Atola TaskForce 2 Manual

Version: Dec 02 2025

Quickstart

Introduction

Unit & extensions

Installation & environment setup

Working with devices

Interface controls & indicators

Diagnostics

Imaging: Basics

Imaging: Damaged drives & performance

RAID reassembly and imaging

Automation

Wipe, hash & special capabilities

Case management

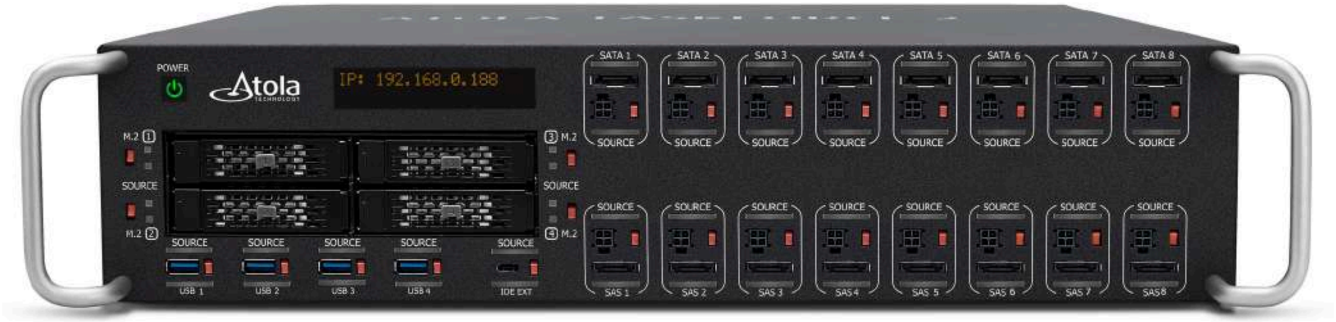
What else?

Quickstart

Learn how to image an evidence drive with Atola TaskForce 2.

Step 1. Start TaskForce 2

1. Press the **Power** button on the front panel of the hardware unit.
2. The following message shows on the small **IP screen** on the front panel: "*Booting 3 min*". Wait until it disappears.
3. Open TaskForce 2 user interface:
   - **Network mode:** If TaskForce 2 is connected to your local network with an Ethernet cable or a Wi-Fi adapter, open a Chrome browser on your PC, tablet or mobile, and enter the IP address displayed on the IP screen in its address bar.
   - **Kiosk mode:** If TaskForce 2 is not connected to the network, plug in a VGA display, mouse & keyboard. The "*Kiosk mode*" message appears on the IP screen.



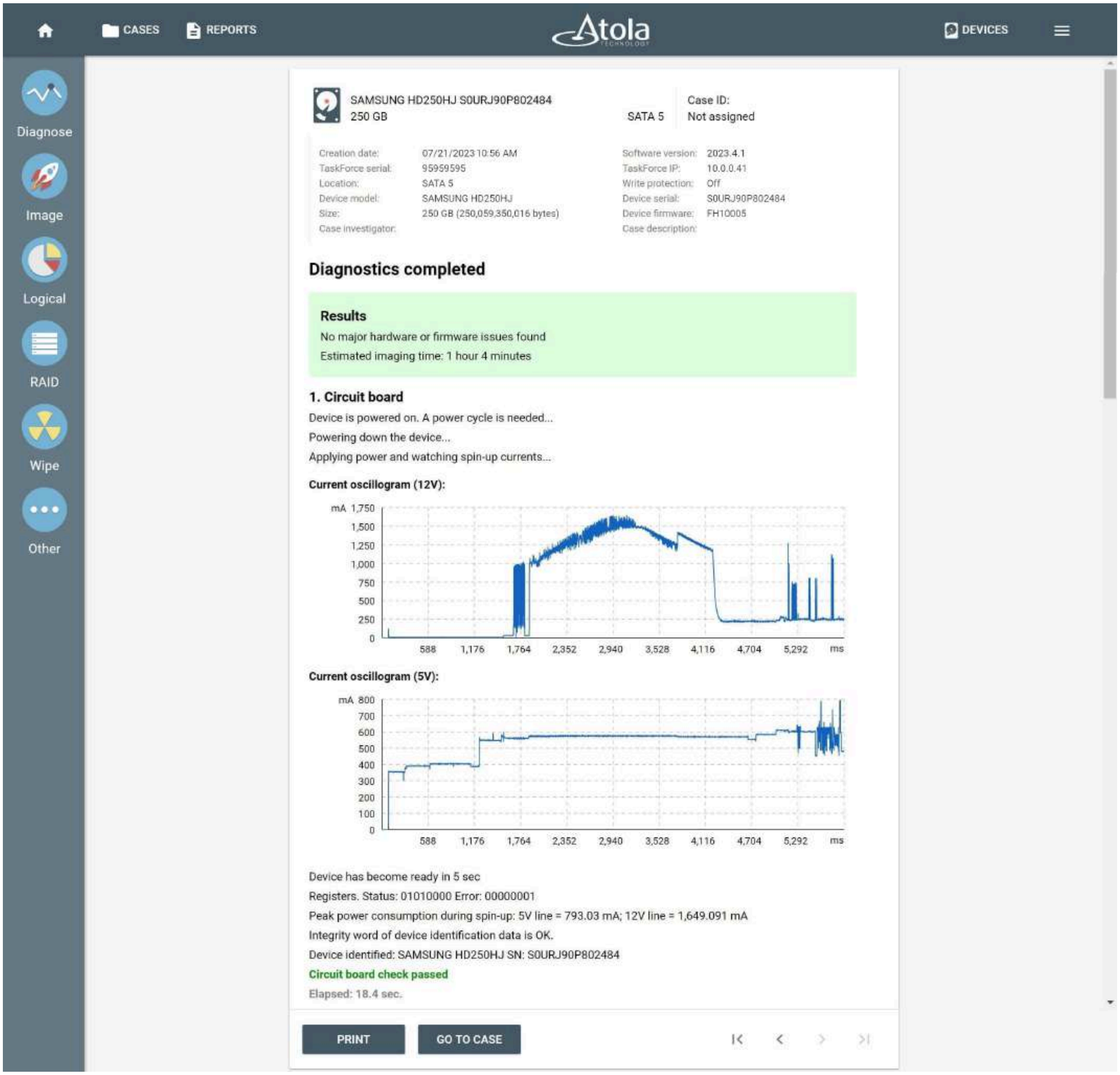
TaskForce 2 shows an IP address required to connect to its user interface.

Step 2. Plug a source drive into TaskForce 2

1. To protect an evidence drive from any alterations, switch one of TaskForce's 26 ports into the Source mode, using the red source/target switch next to this port. The corresponding source indicator lights up signaling that the port is set to the Source mode and is write-protected.
2. Connect your evidence drive to the port switched to the Source mode.

Step 3. Diagnose the source drive

1. In the TaskForce 2 user interface, click **Diagnose**.
2. On the **Select device** panel, find the appropriate category (SATA, SAS, USB, File, IDE, or Extension*), expand it and select your source drive.
3. Click **Start**. The Diagnostics process takes a couple of minutes. If diagnostics results show that the drive is in good condition, proceed to imaging.



SAMSUNG HD250HJ S0URJ90P802484
250 GB

SATA 5

Case ID:
Not assigned

Creation date:	07/21/2023 10:56 AM	Software version:	2023.4.1
TaskForce serial:	95959595	TaskForce IP:	10.0.0.41
Location:	SATA 5	Write protection:	Off
Device model:	SAMSUNG HD250HJ	Device serial:	S0URJ90P802484
Size:	250 GB (250,059,350,016 bytes)	Device firmware:	FH10005
Case investigator:		Case description:	

Diagnostics completed

Results

No major hardware or firmware issues found

Estimated imaging time: 1 hour 4 minutes

1. Circuit board

Device is powered on. A power cycle is needed...

Powering down the device...

Applying power and watching spin-up currents...

Device has become ready in 5 sec

Registers. Status: 01010000 Error: 00000001

Peak power consumption during spin-up: 5V line = 793.03 mA; 12V line = 1,649.091 mA

Integrity word of device identification data is OK.

Device identified: SAMSUNG HD250HJ SN: S0URJ90P802484

Circuit board check passed

Elapsed: 18.4 sec.

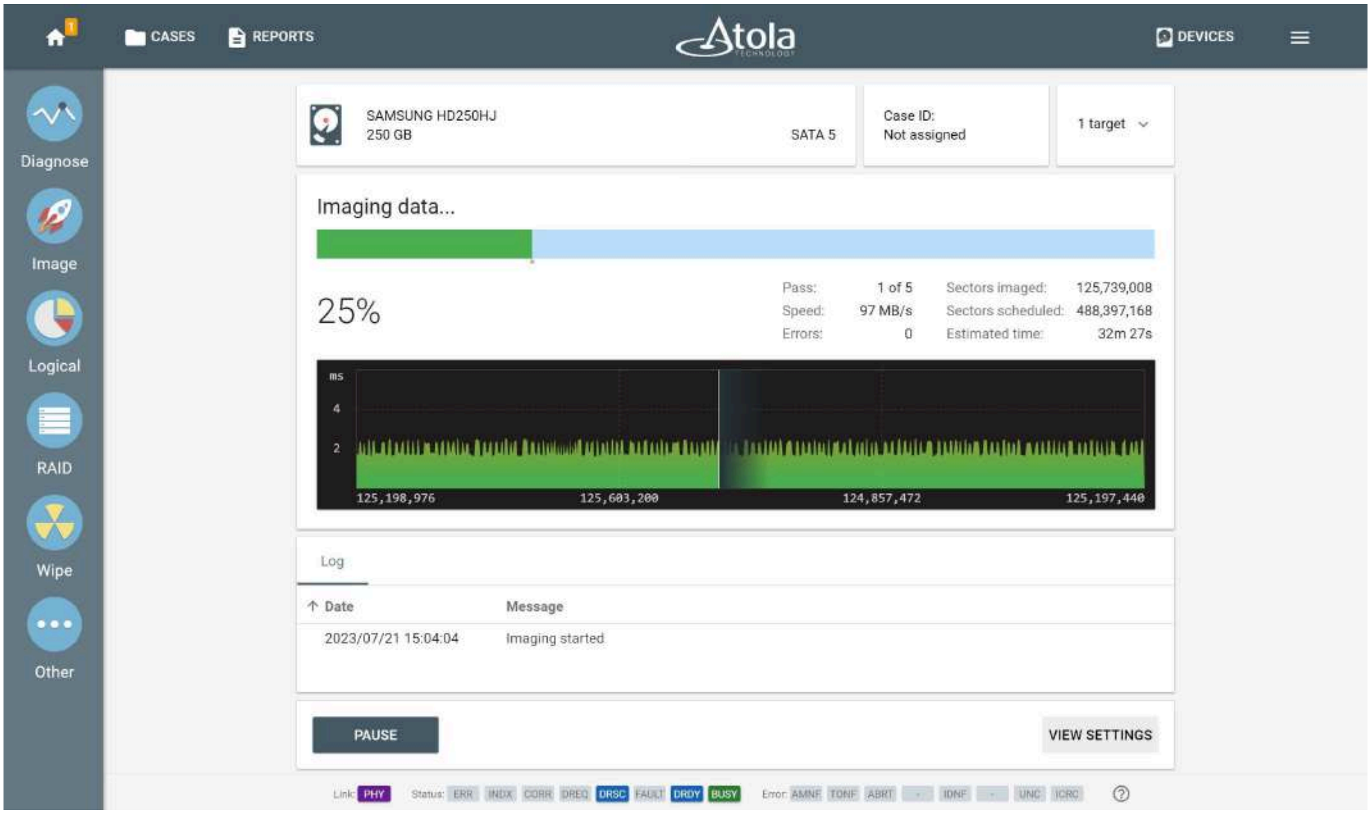
Diagnostics report proves the drive is in good condition.

Step 4. Plug a target drive into the TaskForce 2

1. Switch one of the free ports into the Target mode, using the red source/target switch next to it. The corresponding source indicator turns off.
2. Connect a target drive to the port switched to the Target mode.

Step 5. Start imaging

1. In the TaskForce 2 user interface, click **Image**.
2. On the **Select source device** panel, find the appropriate category (SATA, SAS, USB, File, IDE, or Extension*), expand it and select your source drive.
3. On the **Imaging sessions** page, click **Start new**.
4. On the **Select target devices** panel, find the appropriate category (SATA, SAS, USB, File, IDE, or Extension*), expand it and select your target device or devices. Then click **Continue**.
5. Check the imaging settings and adjust them if needed. The **Settings** page shows:
   - the source drive and the case ID
   - the default settings applied to this imaging session
   - the list of Targets to be involved in this session
6. Click **Start**.



SAMSUNG HD250HJ
250 GB
SATA 5

Case ID:
Not assigned

1 target

Imaging data...

25%

Pass: 1 of 5
Speed: 97 MB/s
Errors: 0
Sectors imaged: 125,739,008
Sectors scheduled: 488,397,168
Estimated time: 32m 27s

Date	Message
2023/07/21 15:04:04	Imaging started

Image acqusition in progress.

Atola TaskForce 2 technical specs

Drive ports

26 drive ports

8 SATA (up to 540 MB/s)

8 SAS/SATA (up to 1000 MB/s)

4 NVMe M.2/U.2/U.3 PCIe 4.0 (up to 6000 MB/s)

4 USB (up to 400 MB/s)

1 IDE (up to 100 MB/s)

1 Extension

Drive port features

Physical source/target switch with LED indication

Hardware write protection in the source mode

Task status LED indication

Full low-level control over drive ports

Reset and SATA PHY control for the best handling of severely damaged hard drives

Drive's power control

Current sensor

Automatic overcurrent protection

Automatic short-circuit protection

Overvoltage protection

Supported drive interfaces

M.2 / U.2 / U.3 NVMe

SATA I/II/III

SAS3 (12 Gb)

USB 2.0/3.x

IDE

Flash cards via a card reader attached to any USB port

Other interfaces supported via Extension modules (see below)

Network

Two 10Gb Ethernet ports for imaging to a network server or NAS.

WiFi 802.11n 150 Mb/s adapter in access point mode. Included in the package.

CPU, motherboard, and RAM

Xeon CPU with 16 cores

Server-grade Supermicro motherboard

16 GB ECC RAM

Extension modules

Apple PCIe

FireWire

Thunderbolt 2 and 3 (2016-2017 models)

M.2 NVMe/PCIe/SATA

Indication

Power LED indicator

Signals that hardware is up and running

Color-coded port LEDs

Indicate that a task is running or finished, a process is OK or there are issues

IP display

OLED (20x2 characters). Shows an IP address to connect to the TaskForce 2 user interface or Kiosk mode

Auxiliary connections

Kiosk mode

VGA port

Two USB ports for connecting a keyboard and mouse

Database

Two DB USB 3.0 ports for connecting a USB flash media as database storage

Serial RS232 port

Fan power port

System SD card slot for boot drive

Power

Power consumption

190 Watt average, 550 Watt peak

Supply voltage

100–240 VAC, 50–60 Hz

Power supply

Internal power supply

IEC 60320 C14 power inlet

Power supply switch on the back panel

Size, weight, and temperature

Aluminum case

Dimensions

17.4 x 14.5 x 3.9 in (442 x 370 x 100 mm)

Required server rack height: 2.5U

Weight

17.2 lb (7.8 kg)

Working temperature

32° – 95°F (0°C – 35°C)

Lifetime warranty

TaskForce 2 hardware is covered by our Lifetime warranty, for as long as your software update subscription is active.

If you have an active subscription, you can request free replacement of a device, component, extension module, or cable, as well as free training and technical support.

Learn more about Lifetime warranty →

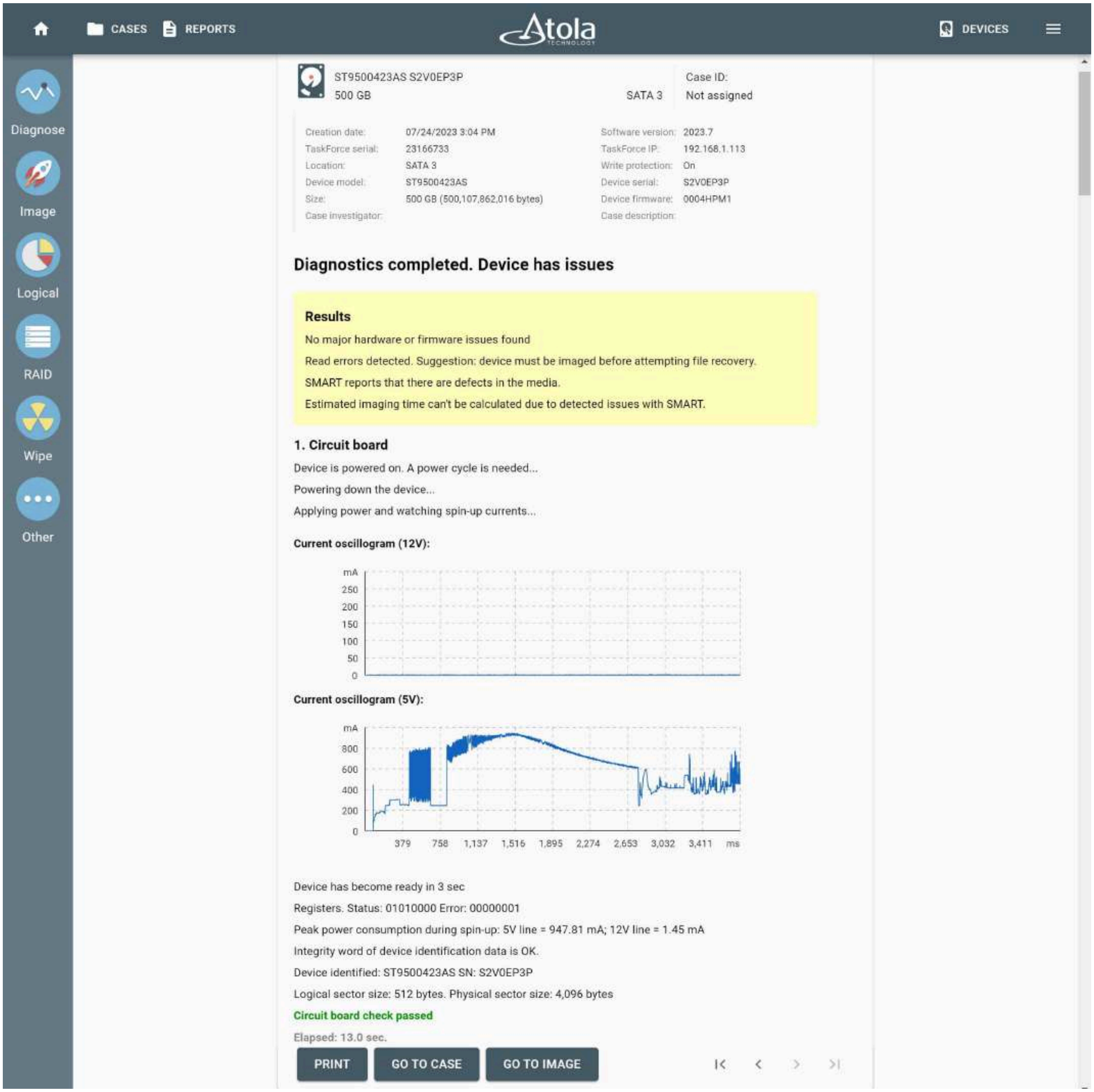
TaskForce workflow

Atola TaskForce provides a complete feature set for a forensically sound evidence acquisition process. Based on our own decade-long experience of working with data storage devices as well as the experience of our clients in digital forensics market we strongly recommend this workflow:

1. Diagnose the drive

TaskForce is equipped with a fully-automated diagnostics module, which diagnoses all drive systems: printed circuit board (PCB), spindle motor, head stack, firmware, and file systems. Diagnostics will work properly even if the drive has burnt parts or damaged head stack – the routine makes use of the current monitor that is embedded into TaskForce unit.

After diagnostics finishes, the tool prepares a report and lets you know the exact issue with the drive; it also suggests the next step to be able to retrieve the data.



ST9500423AS S2V0EP3P
500 GB

SATA 3

Case ID:
Not assigned

Creation date:	07/24/2023 3:04 PM	Software version:	2023.7
TaskForce serial:	23166733	TaskForce IP:	192.168.1.113
Location:	SATA 3	Write protection:	On
Device model:	ST9500423AS	Device serial:	S2V0EP3P
Size:	500 GB (500,107,862,016 bytes)	Device firmware:	0004HPM1
Case investigator:		Case description:	

Diagnostics completed. Device has issues

Results

No major hardware or firmware issues found

Read errors detected. Suggestion: device must be imaged before attempting file recovery.

SMART reports that there are defects in the media.

Estimated imaging time can't be calculated due to detected issues with SMART.

1. Circuit board

Device is powered on. A power cycle is needed...

Powering down the device...

Applying power and watching spin-up currents...

Current oscillogram (12V):

Current oscillogram (5V):

Device has become ready in 3 sec

Registers. Status: 01010000 Error: 00000001

Peak power consumption during spin-up: 5V line = 947.81 mA; 12V line = 1.45 mA

Integrity word of device identification data is OK.

Device identified: ST9500423AS SN: S2V0EP3P

Logical sector size: 512 bytes. Physical sector size: 4,096 bytes

Circuit board check passed

Elapsed: 13.0 sec.

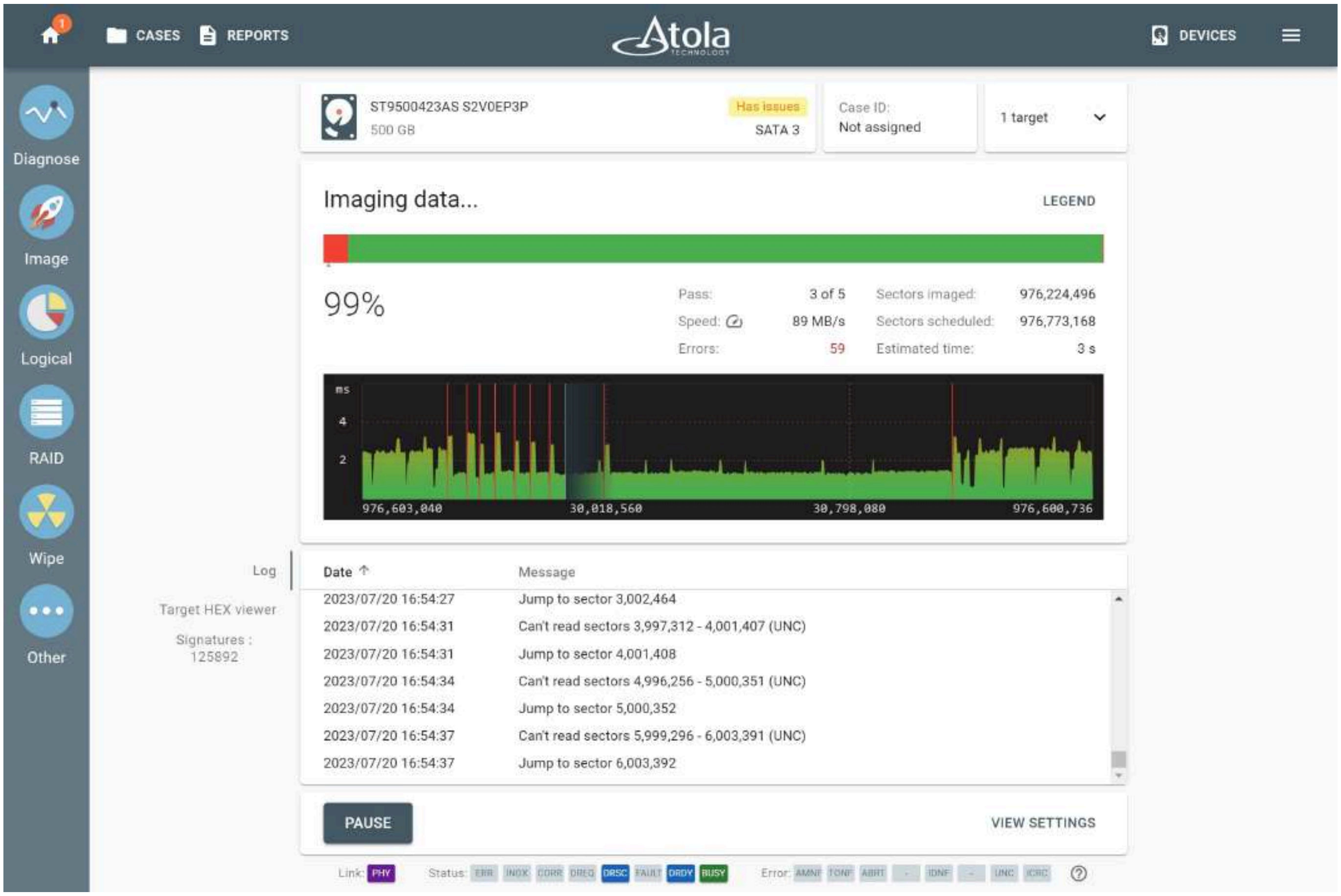
Diagnostics of damaged drive.

2. Get access to the hidden drive areas

Unclip or change HPA, DCO, AMA limitations
TaskForce detects hidden areas on the drive Host Protected Area (HPA), Device Overlay Configuration (DCO), or Accessible Max Address (AMA) and can automatically recover/remove them. To avoid change the state of the drive, HPA reset until power cycle option is available.

3. Image the evidence

To ensure efficient imaging of both good and damaged drives, TaskForce is equipped with a sophisticated and powerful imaging module that creates a bit-to-bit copy of the evidence. Based on the diagnostics report, image drives with default settings or adjust them, should the media be damaged and require special treatment.



ST9500423AS S2V0EP3P
500 GB
SATA 3

Case ID:
Not assigned

1 target

Imaging data...

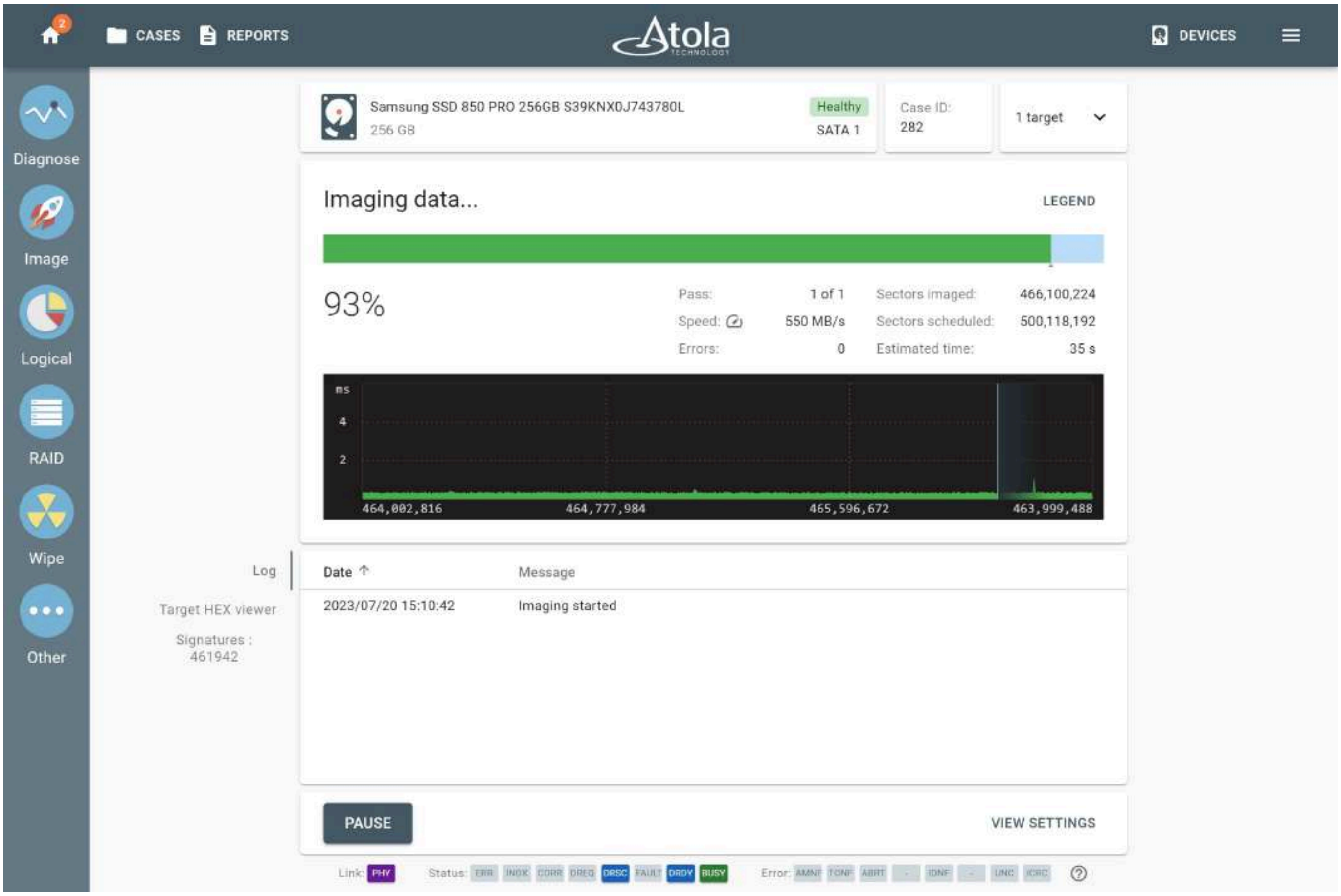
99%

Pass: 3 of 5
Speed: 89 MB/s
Errors: 59
Sectors imaged: 976,224,496
Sectors scheduled: 976,773,168
Estimated time: 3 s

Signatures : 125892

```
Date ↑                 Message
2023/07/20 16:54:27    Jump to sector 3,002,464
2023/07/20 16:54:31    Can't read sectors 3,997,312 - 4,001,407 (UNC)
2023/07/20 16:54:31    Jump to sector 4,001,408
2023/07/20 16:54:34    Can't read sectors 4,996,256 - 5,000,351 (UNC)
2023/07/20 16:54:34    Jump to sector 5,000,352
2023/07/20 16:54:37    Can't read sectors 5,999,296 - 6,003,391 (UNC)
2023/07/20 16:54:37    Jump to sector 6,003,392
```

Imaging damaged drive.



Samsung SSD 850 PRO 256GB S39KNX0J743780L
256 GB
Healthy
SATA 1
Case ID: 282
1 target

Imaging data...

93%

Pass: 1 of 1
Speed: 550 MB/s
Errors: 0
Sectors imaged: 466,100,224
Sectors scheduled: 500,118,192
Estimated time: 35 s

Signatures : 461942

Date ↑	Message
2023/07/20 15:10:42	Imaging started

Imaging good SSD. Speed: 550 MB/s.

4. Calculate hash

To ensure forensically sound evidence acquisition process, remember to calculate hash of the evidence and the image. It is essential way to prove image integrity.

With damaged devices, it is best to calculate hash during imaging (using segmented hashing). This way data on a fragile device is only read once, and less potential damage to the media is caused.

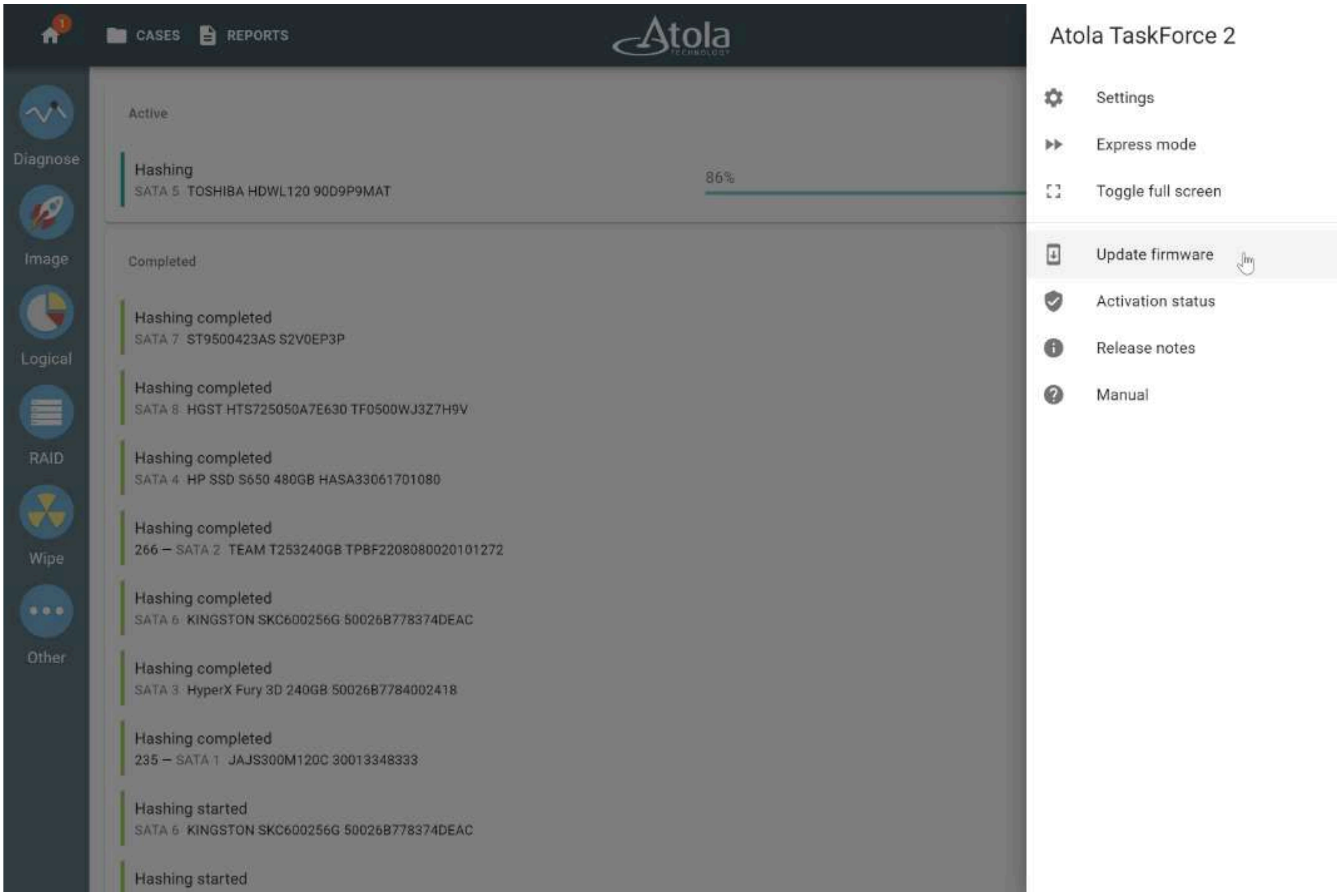
Linear hash can only be calculated by reading data in sectors consecutively in one pass. When it encounters a bad sector, linear hash calulation is discontinued.

Updating TaskForce firmware

Atola TaskForce firmware is updated on regular basis by our team. You can keep track of the updates we make to the firmware in TaskForce changelog.

Updating TaskForce firmware is easy using a remotely connected computer.

1. Plug TaskForce into to your local Ethernet network.
2. Open the Chrome browser on your PC.
3. Download the most recent version of the firmware.
4. Enter TaskForce IP address in the Chrome browser.
5. Go to the **Menu** on the top right.
6. Click **Update firmware**.



Active

Hashing
SATA 5 TOSHIBA HDWL120 90D9P9MAT
86%

Completed

Hashing completed
SATA 7 ST9500423AS S2V0EP3P

Hashing completed
SATA 8 HGST HTS725050A7E630 TF0500WJ3Z7H9V

Hashing completed
SATA 4 HP SSD S650 480GB HASA33061701080

Hashing completed
266 — SATA 2 TEAM T253240GB TPBF2208080020101272

Hashing completed
SATA 6 KINGSTON SKC600256G 50026B778374DEAC

Hashing completed
SATA 3 HyperX Fury 3D 240GB 50026B7784002418

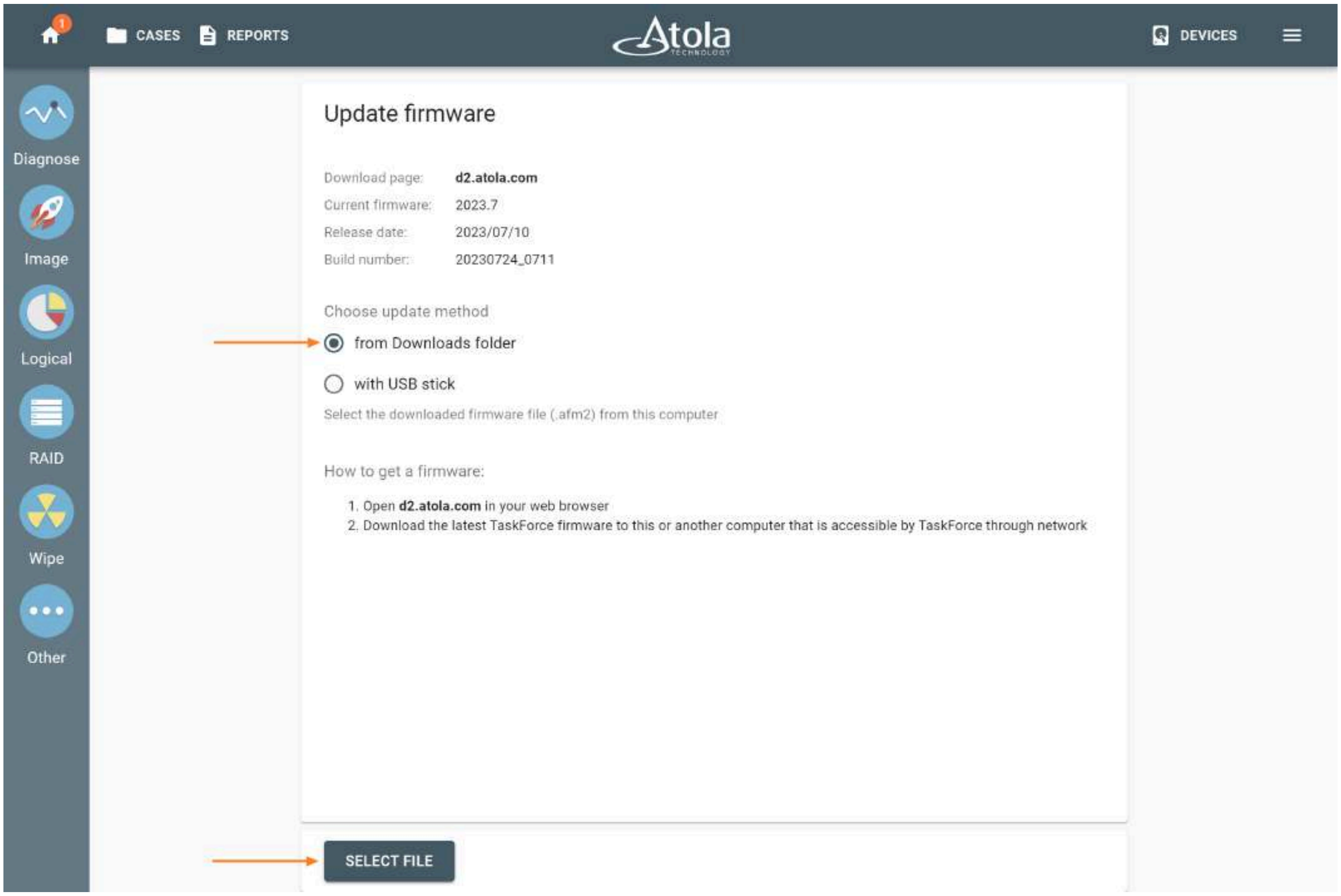
Hashing completed
235 — SATA 1 JAJS300M120C 30013348333

Hashing started
SATA 6 KINGSTON SKC600256G 50026B778374DEAC

Hashing started

The Update firmware command in the TaskForce 2 menu.

7. Choose update method and then click **Select file**.



Update firmware

Download page: **d2.atola.com**

Current firmware: 2023.7

Release date: 2023/07/10

Build number: 20230724_0711

Choose update method

● from Downloads folder

○ with USB stick

Select the downloaded firmware file (.afm2) from this computer

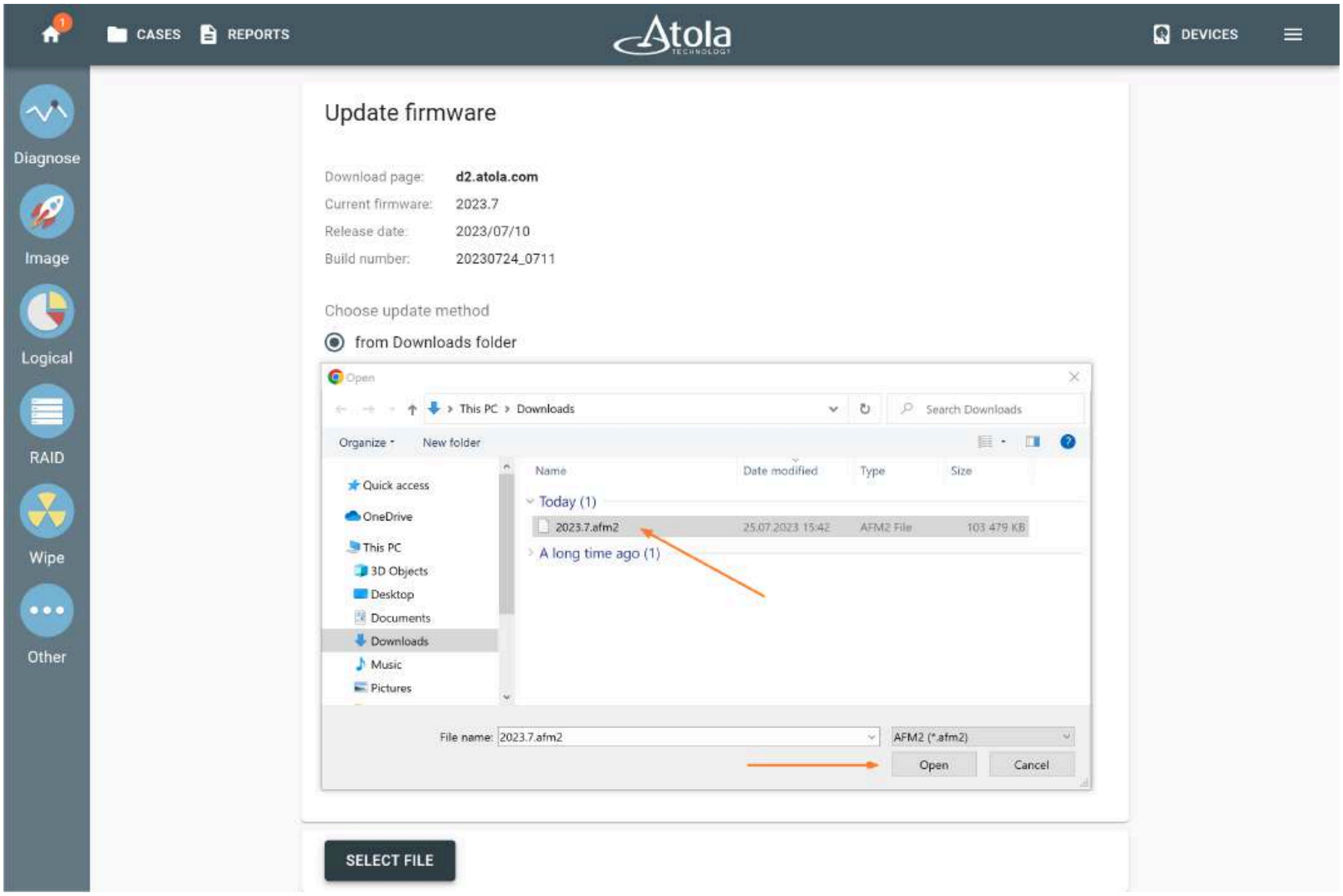
How to get a firmware:

1. Open **d2.atola.com** in your web browser
2. Download the latest TaskForce firmware to this or another computer that is accessible by TaskForce through network

SELECT FILE

Choosing update method on the Update firmware page.

8. In the file selector, select the firmware file and then click **Open**.



Update firmware

Download page: **d2.atola.com**
Current firmware: 2023.7
Release date: 2023/07/10
Build number: 20230724_0711

Choose update method

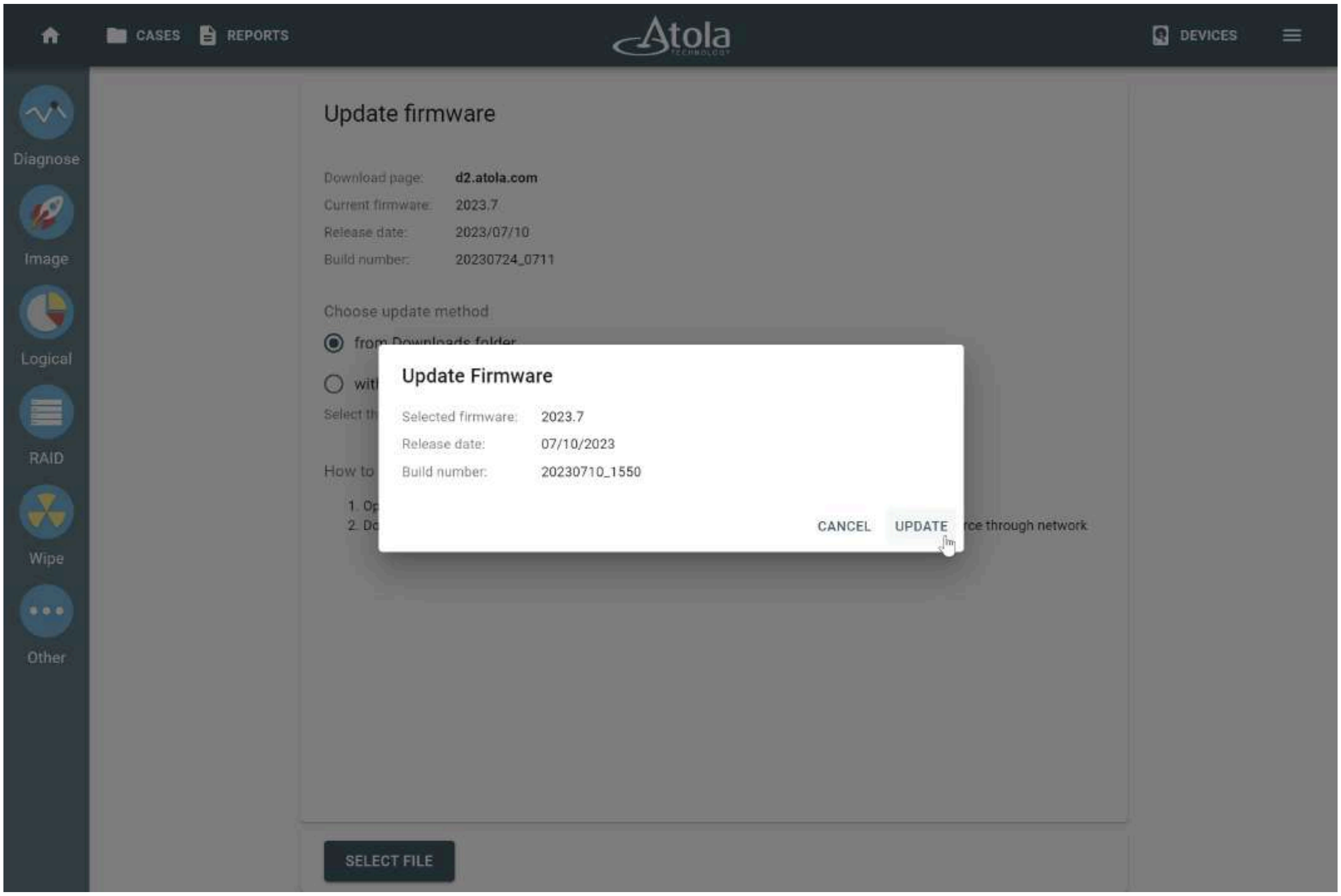
● from Downloads folder

Name	Date modified	Type	Size
2023.7.afm2	25.07.2023 15:42	AFM2 File	103 479 KB

File name: 2023.7.afm2
AFM2 (*.afm2)

Selecting the firmware file.

9. In the Update firmware dialog, click **Update**.



Update firmware

Download page:	d2.atola.com
Current firmware:	2023.7
Release date:	2023/07/10
Build number:	20230724_0711

Choose update method

● from Downloads folder

○ wit

Select th

How to

1. Op
2. Do rce through network

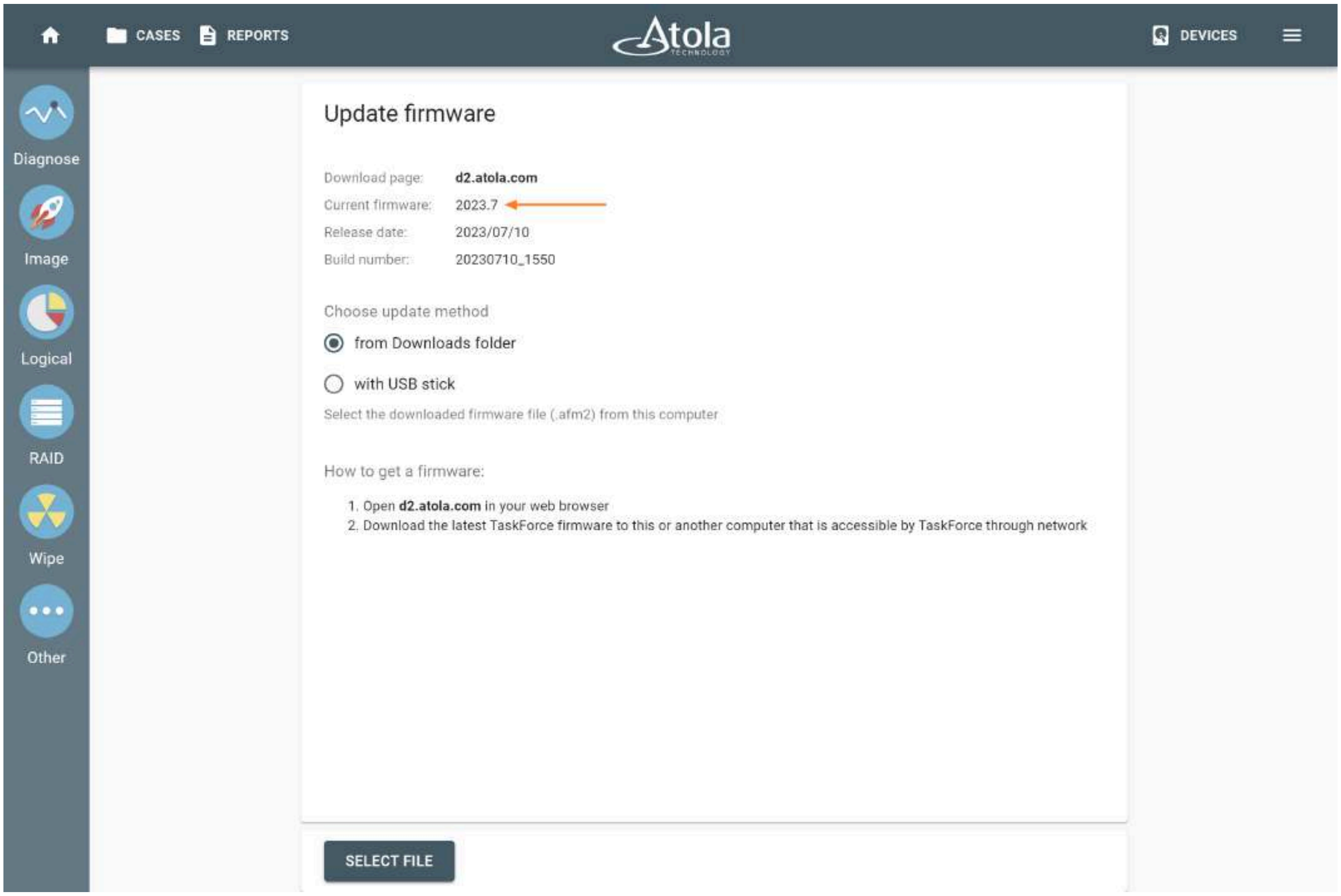
Update Firmware

Selected firmware:	2023.7
Release date:	07/10/2023
Build number:	20230710_1550

The Update button in the Update firmware dialog.

Once the update process is completed, TaskForce software switches to the new version. No TaskForce reboot or Chrome restart is required.

To check the current firmware version, go to **Menu** > **Update firmware**.



Update firmware

Download page: **d2.atola.com**
Current firmware: 2023.7
Release date: 2023/07/10
Build number: 20230710_1550

Choose update method

● from Downloads folder

○ with USB stick

Select the downloaded firmware file (.afm2) from this computer

How to get a firmware:

1. Open **d2.atola.com** in your web browser
2. Download the latest TaskForce firmware to this or another computer that is accessible by TaskForce through network

Check current firmware version.

Package contents (TaskForce 2)

The TaskForce 2 package includes the following items:

TaskForce 2 hardware unit	Power cable

20x SAS/SATA powered cables

2x Ethernet cat 7 cable

Flash card reader

SmartQ™
SMART QUICKLY
Design Patent:
USD949875S

IDE adapter

PLUG ONLY ONE HDD AT A TIME:
3.5" IDE, 2.5" IDE, HITACHI SATA
Atola
TECHNOLOGY

USB-C cable

IDE power cable

IDE interface cable

Quick setup guide

Lifetime warranty

1 Plug

[illegible]

2 Boot

[illegible]

3 Connect. Choose 1 of 3 ways:

- [illegible]
- [illegible]
- [illegible]

4 Activate

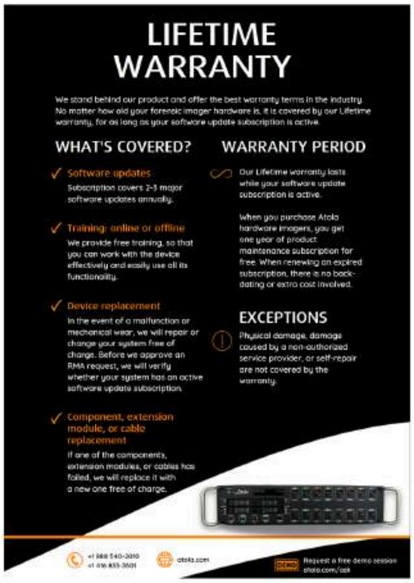
[illegible]

5 Update

[illegible]

Quickstart guide is available at
[illegible]

QUICKSTART



LIFETIME WARRANTY

We stand behind our product and offer the best warranty terms in the industry. No matter how old your forensic imager hardware is, it is covered by our Lifetime warranty, for as long as your software update subscription is active.

WHAT'S COVERED?

✓ Software updates
Subscription covers 2-3 major software updates annually.

✓ Training: online or offline
We provide free training, so that you can work with the device effectively and easily use all its functionality.

✓ Device replacement
In the event of a malfunction or mechanical wear, we will repair or change your system free of charge. Before we approve an RMA request, we will verify whether your system has an active software update subscription.

✓ Component, extension module, or cable replacement
If one of the components, extension modules, or cables has failed, we will replace it with a new one free of charge.

WARRANTY PERIOD

Our Lifetime warranty lasts while your software update subscription is active.

When you purchase Atola hardware imagers, you get one year of product maintenance subscription for free. When renewing an expired subscription, there is no back-dating or extra cost involved.

EXCEPTIONS

Physical damage, damage caused by a non-authorized service provider, or self-repair are not covered by the warranty.

☎ +1 888 540-2010
+1 416 833-3501

atola.com

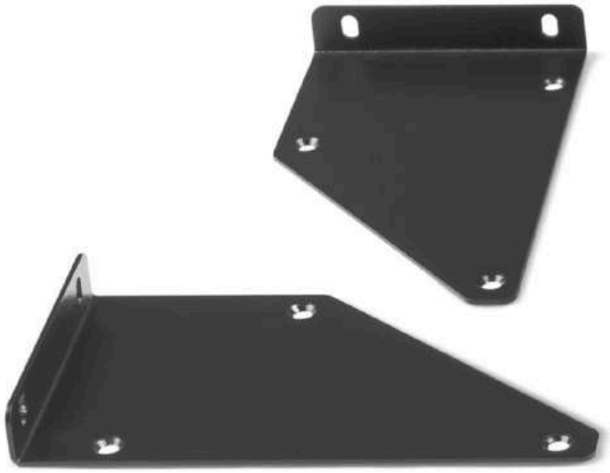
DEMO Request a free demo session
atola.com/ask

USB DB

Wi-Fi adapter

USB-A cable for Wi-Fi adapter

Brackets for server rack

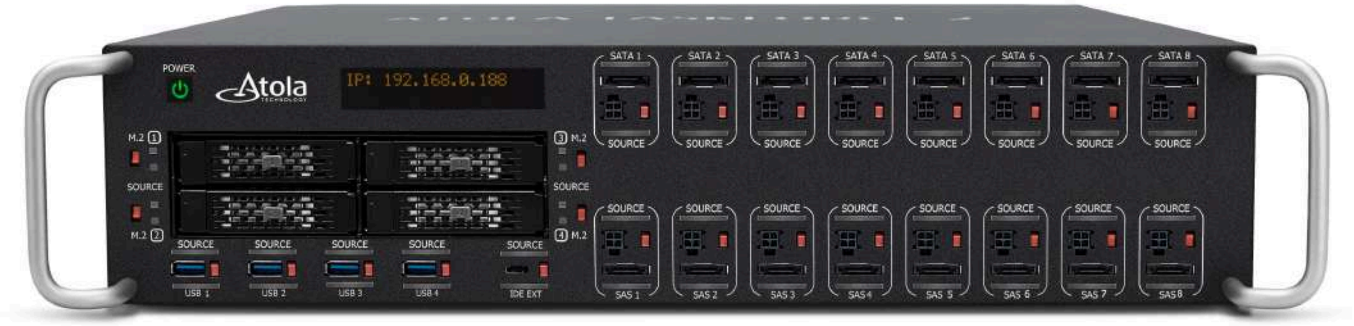


Set of screwdrivers

Forensic hardware unit

To support many simultaneous imaging sessions and other forensic tasks running on its 26 ports at top speeds, TaskForce 2 hardware unit is built on extremely robust, high-capacity components that include a server-grade motherboard, 16-thread Xeon CPU and 16 GB ECC RAM. To ensure the high quality and efficiency of our tools, we test them on hundreds of storage devices.

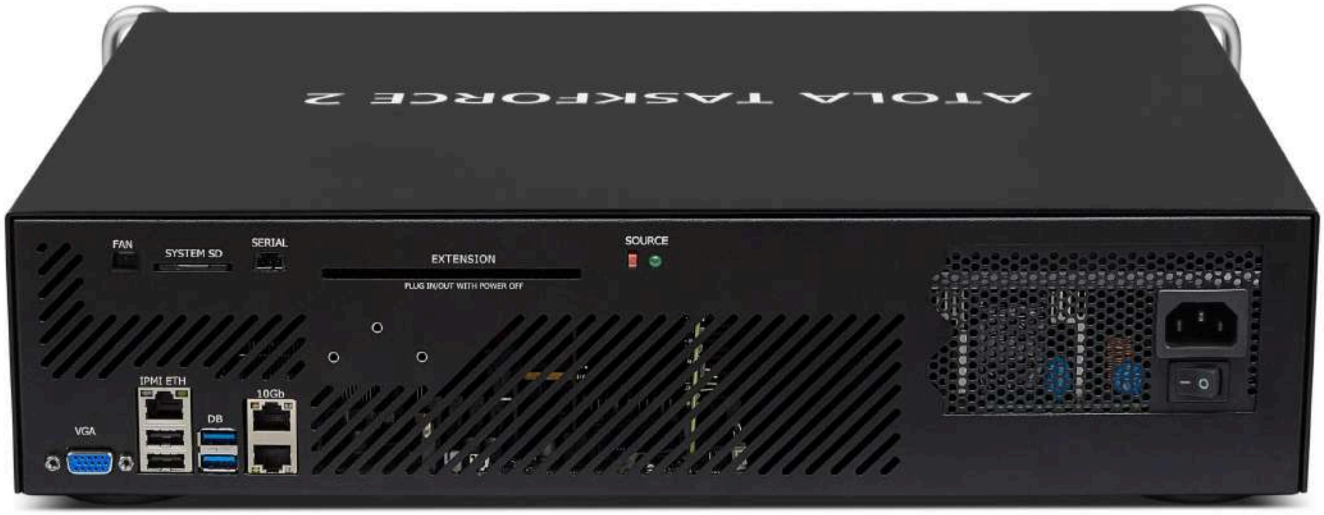
This forensic hardware unit is designed for various types of digital investigations in the lab environment.



Ports, indicators & switches

Ports:

- 8 SATA
- 8 SATA/SAS
- 4 USB 3.0
- 4 NVMe M.2/U.2 PCIe 4.0
- IDE
- Extension slot (for Thunderbolt, Apple PCIe SSD and M.2 SSD extension modules)



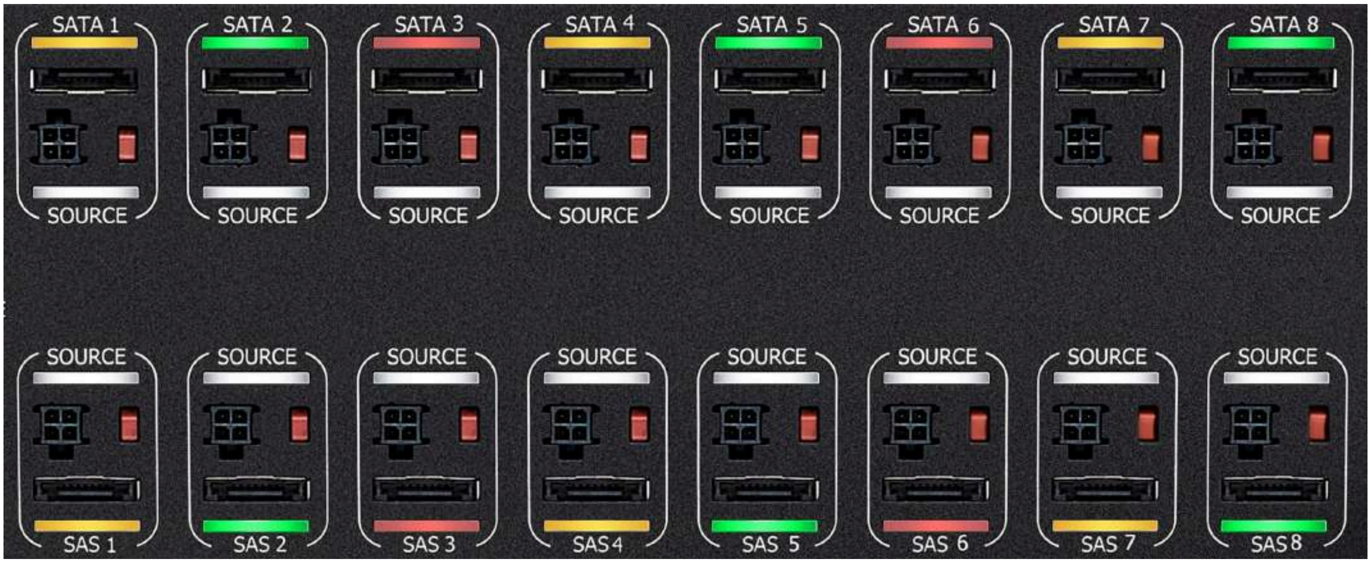
Source/target switch on each of 26 ports enabling hardware write protection in source mode:

- **Source mode:** helps safely connect and with the examined evidence drives to TaskForce 2.
- **Flexible port configuration:** any TaskForce port can serve you as a source or target depending on your needs.

LED indicators: two indicators for each of the 26 ports. One indicator is located next to the port’s source/target switch and lights up when source mode is enabled.

There are plenty of informative LED indicators on the front panel of the unit:

- **Power LED indicator** to signal that hardware is up and running.
- **IP display** to show an IP address you need to connect to the TaskForce 2 control interface using Chrome browser.



- **White LED source/target indicator** on each of the 26 ports.
  - White light: port is in the Source mode, write protection is **on**.
  - No light: port is in the Target mode, write protection is **off**.
- **Color-coded LED indication of each port status**

  Running tasks:

    - Blinking **green** light: the task is running without issues.

  Completed tasks:

    - Still **green** light: the task is completed successfully.
    - Still **yellow** light: the task completed with minor issues or warnings.
    - Still **red** light: the task failed.

  Special statuses:

    - Still **blue** light: the connected drive is in Storage mode.
    - Blinking **blue** light: the task is running on a drive in Storage mode.
    - Blinking **yellow** light: user action required (in Express mode).
    - Blinking **red** light: short circuit.

  Software startup and update:

    - Blinking **blue** LEDs forming a letter A: Taskforce software is booting.
    - Blinking **yellow** LEDs forming a letter A: firmware update in progress.

  You can control LED brightness in TaskForce 2 settings.

Network ports:

- Two 10Gb Ethernet ports handle 26 multiple imaging sessions utilizing two 10Gb network connections
- One IPMI ETH port

Other connections:

- Two USB 3.0 ports for connecting a USB flash media as TaskForce 2 database storage
- Two USB 2.0 ports for keyboard/mouse in the Kiosk mode
- VGA for connecting a monitor in the Kiosk mode
- Auxiliary serial RS232 port
- Auxiliary fan power port

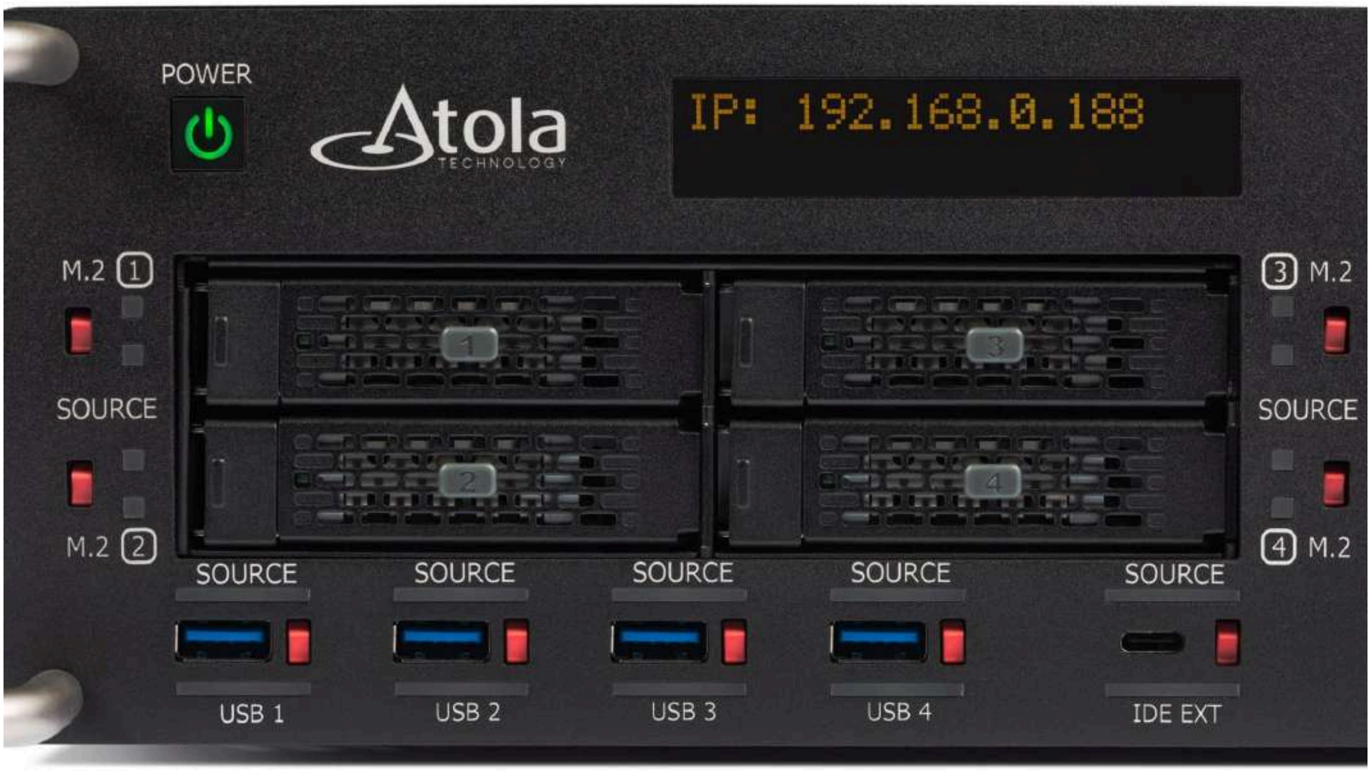
The power socket is located on the back side of the unit.

Supported hard drive interfaces: SATA I/II/III, SAS3 (12Gb), USB 2.0/3.0, IDE, M.2/U.2 PCIe NVMe up to 4.0.

Flash memory cards are supported via a card reader plugged into any USB port of TaskForce 2.

Display

IP display: OLED (20x2 characters)



Physical / Environmental

- Dimensions: 17.4 × 14.5 × 3.9 in (442 × 370 × 100 mm)
- Weight: 17.2 lb (7.8 kg)
- Working temperature range: 32° – 95°F (0°C – 35°C)
- Power consumption: 140 Watt average, 650 Watt peak
- Supply Voltage: 100–240 VAC, 50–60 Hz
- RoHS compliant

Other specs

- Internal OS: Linux running a custom kernel
- Control interface: web-based TaskForce application
- Removable NVMe SSD for internal case management database
- Optional WiFi 802.11n 150 Mb/s adapter in access point mode for easy connectivity (purchased separately)

Inside TaskForce forensic hardware unit

TaskForce 2 forensic hardware unit is essentially a small server-grade computer running Linux. But because neither BIOS nor Linux kernel was designed to handle hard disk failures, Atola engineers have invested a significant amount of research and development efforts to build a highly customized and fine-tuned Linux kernel that fully overcomes these issues and handles damaged media properly. Additionally, this kernel features:

- High-speed DMA data transfers, 500+ MB/s
- Full low-level control over SATA, USB and IDE ports
- Full native SATA support
- Reset and SATA PHY control for best handling of severely damaged hard drives
- All BIOS and standard kernel functions are disabled

TaskForce 2 hardware also features Atola's proprietary circuitry for the ultimate drive's power control:

- Current sensor for in-depth hard disk diagnosis
- Automatic overcurrent and short-circuit protection
- Overvoltage protection

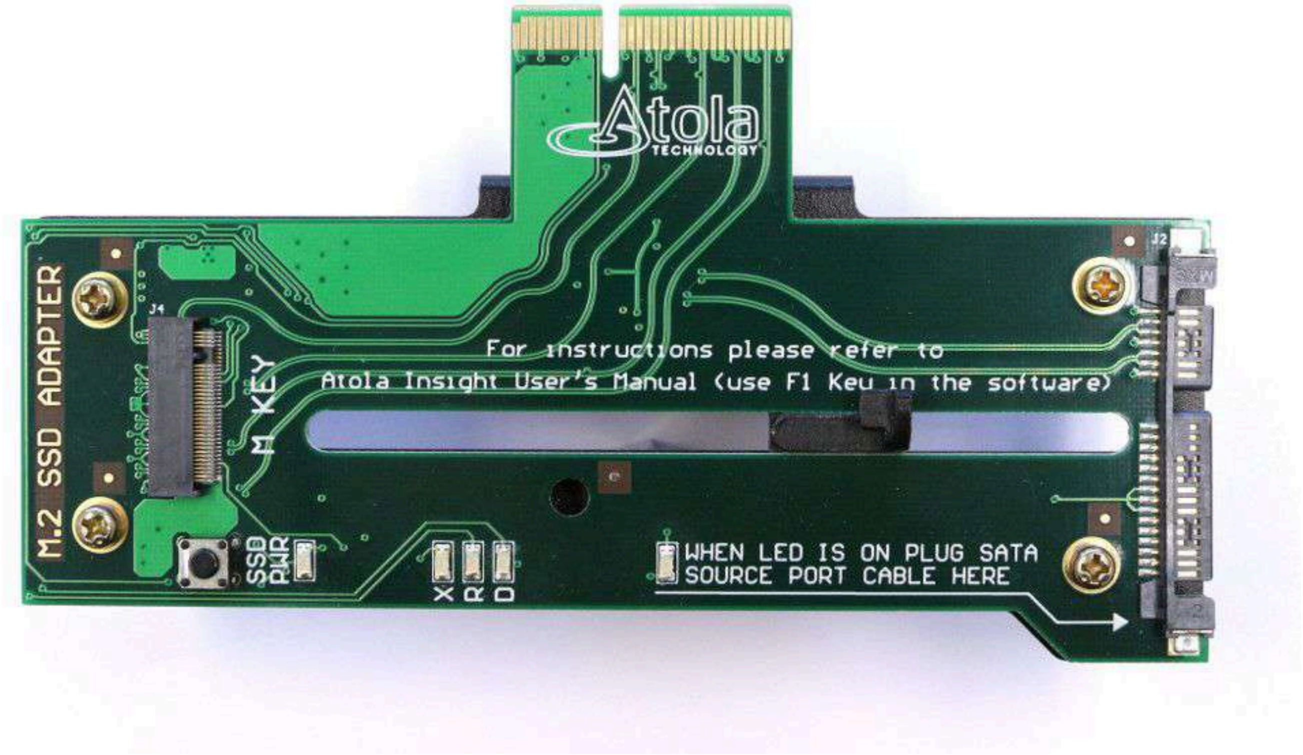
These features are a must for proper handling of damaged drives.

For instance, low-level control of the SATA, SAS, USB and IDE ports allows TaskForce 2 to handle the devices that do not properly initialize, have many bad sectors, or frequently freeze due to internal (mechanical) failures. SATA PHY control allows resetting a frozen hard drive without a power cycle, thus saving time during imaging, and reducing the chances of further hard disk degradation and failure. Current sensing allows TaskForce to diagnose a failed drive even if it has electronic or mechanical damage.

Overcurrent protection detects when the drive draws an abnormal current and stops it to prevent any further damage. An overvoltage protection circuit ensures that in the unlikely event of a hardware malfunction, the attached drives are not damaged in any way.

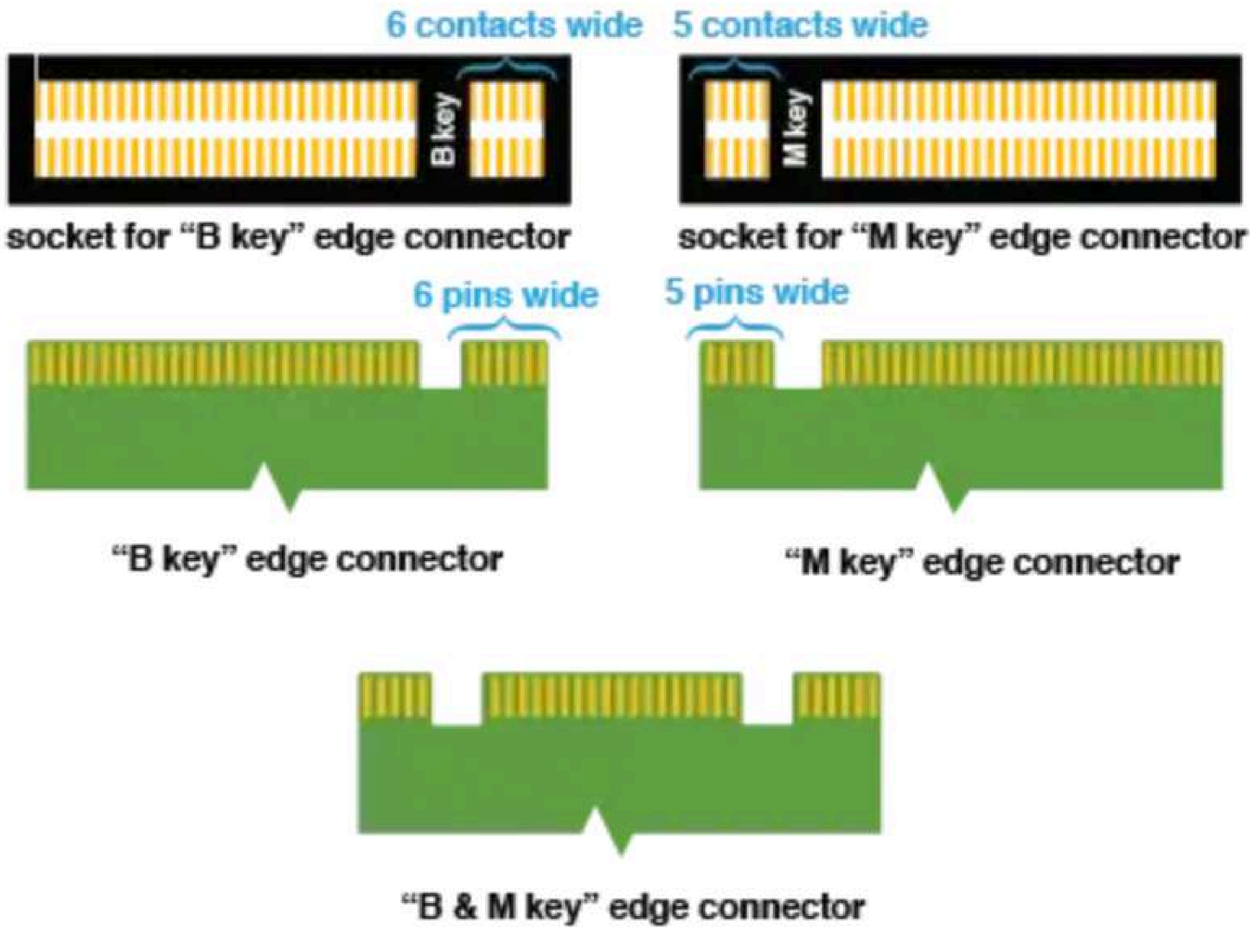
TaskForce 2 forensic hardware unit is fully controlled by the software via Chrome browser, therefore no Linux experience is required to operate it.

M.2 SSD extension module



You can connect M.2 PCIe NVMe and M.2 PCIe AHCI solid state drives to Atola TaskForce 2 using the M.2 SSD extension module.

This extension module supports **only B & M key and M key interface** drives.



M.2 SSD extension module works with Atola DiskSense 2 as well.

TaskForce features supported for the M.2 SSD extension

All standard TaskForce operations and features are supported for the M.2 PCIe NVMe and M.2 PCIe AHCI including:

- Max read/write speed: 4000 MB/s
- Drive hotplug (excluding M.2 PCIe AHCI drives)
- Write protection with the physical source/target switch
- Diagnostics
- Physical and logical imaging
- Hash calculation
- Damaged drive support

Plug and unplug the M.2 SSD extension module

TaskForce hardware unit is equipped with the PCI Express port on its back panel, which is referred to as an Extension port. It is used to plug Atola hardware extension modules supported by Atola TaskForce software.

> **Important:** Do not plug or unplug the extension module when TaskForce is powered on, this can damage the extension module or TaskForce hardware unit. However, you can hotplug M.2 PCIe NVMe drives when the extension module is already connected and fixed in place.

To connect the M.2 SSD extension module to TaskForce, do the following:

1. Power off TaskForce.

2. Align 3 holes on the extension module and 3 screw holes on the Taskforce back panel. Firmly plug the M.2 SSD extension module into the Extension port and fasten the module with 3 screws.
3. Plug an M.2 PCIe NVMe, or M.2 PCIe AHCI, into the extension and fasten the drive in place with the black plastic slider.
4. Power on TaskForce.

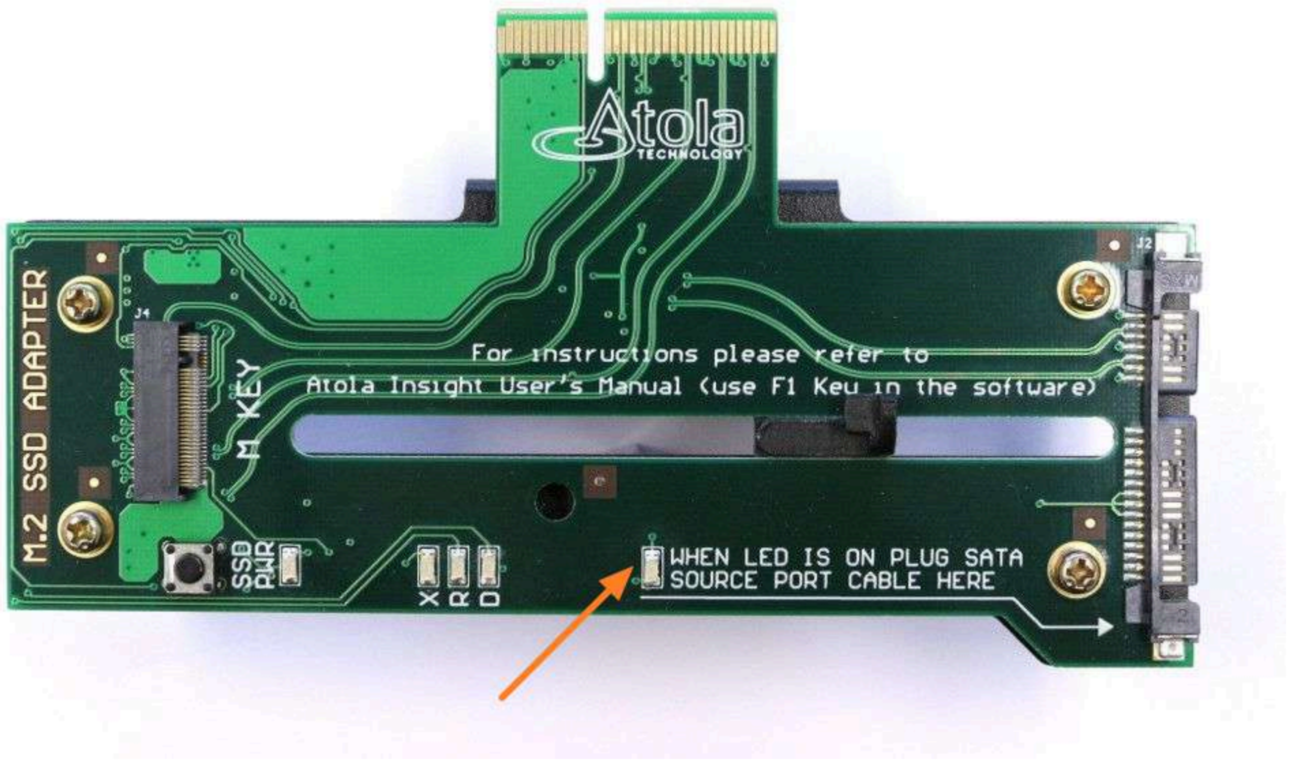
To disconnect the M.2 SSD extension module or replace it with another extension module, do the following steps:

1. Power off TaskForce.
2. Disconnect the SATA cable from the extension module.
3. Release the screws, which hold the module, and unplug it from the Extension port.
4. **Optional:** Plug another extension module into the Extension port and fasten the module with a screw.
5. Power on TaskForce.

Distinguish between M.2 NVMe/M.2 AHCI, and M.2 SATA drives

All solid state drives with M.2 form factor look pretty much the same.

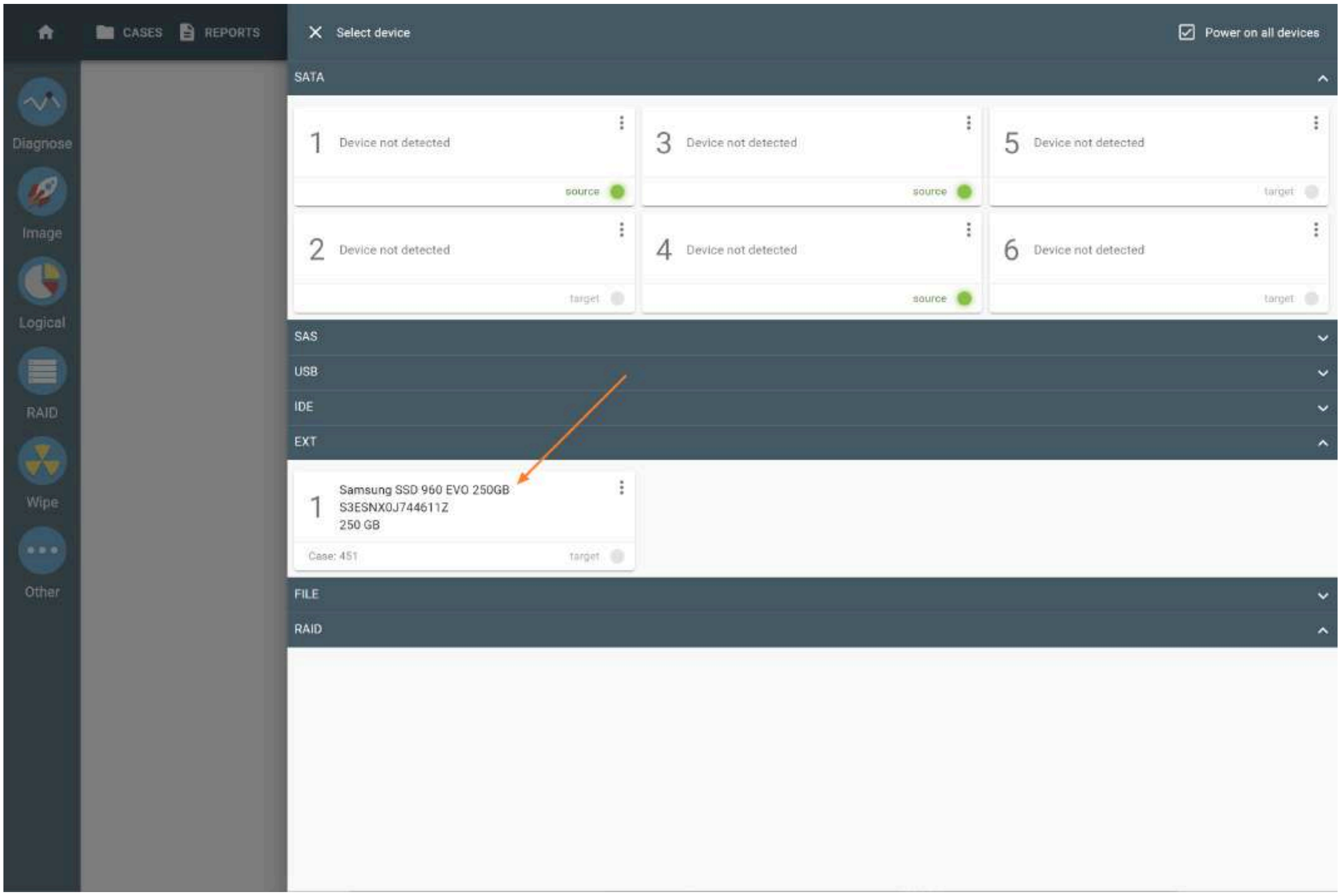
To define the type of the particular M.2 drive before connecting it to TaskForce, check the markings on the drive or refer to the manufacturer’s specifications.



Connect and identify an M.2 NVMe or M.2 AHCI drive

To identify the M.2 PCIe NVMe or M.2 PCIe AHCI drive, TaskForce must be first booted with that particular type of drive connected to the M.2 SSD extension module:

1. Power off TaskForce.
2. Plug an M.2 PCIe NVMe or M.2 PCIe AHCI drive into the extension and fasten the drive with the black plastic slider.
3. Power on TaskForce and wait for the booting to be completed.
4. In the TaskForce main window, click **Devices**.
5. Click the port in the **EXT** section of the **Select device** panel.



NVMe M.2 drive in the EXT section of the Select device panel.

Work consecutively with several M.2 NVMe drives

Drive hotplug is supported for M.2 PCIe NVMe drives, but not for M.2 PCIe AHCI drives. You can plug several M.2 NVMe drives one after another, without turning TaskForce off and on.

To identify the M.2 PCIe NVMe drive, TaskForce must be first booted with that particular type of drive connected to the M.2 SSD extension module. After you boot TaskForce with an M.2 NVMe drive connected to the extension module, the system identifies all other M.2 NVMe drives without rebooting the hardware unit.

To define the type of the particular drive, check the markings on it or refer to the manufacturer’s specifications.

Connect a U.2 NVMe drive using adapter

To use a drive with U.2 interface, attach the drive to TaskForce with the help of a U.2-to-M.2 adapter and a cable (not included in the package).

To connect a U.2 drive to TaskForce, do the following:

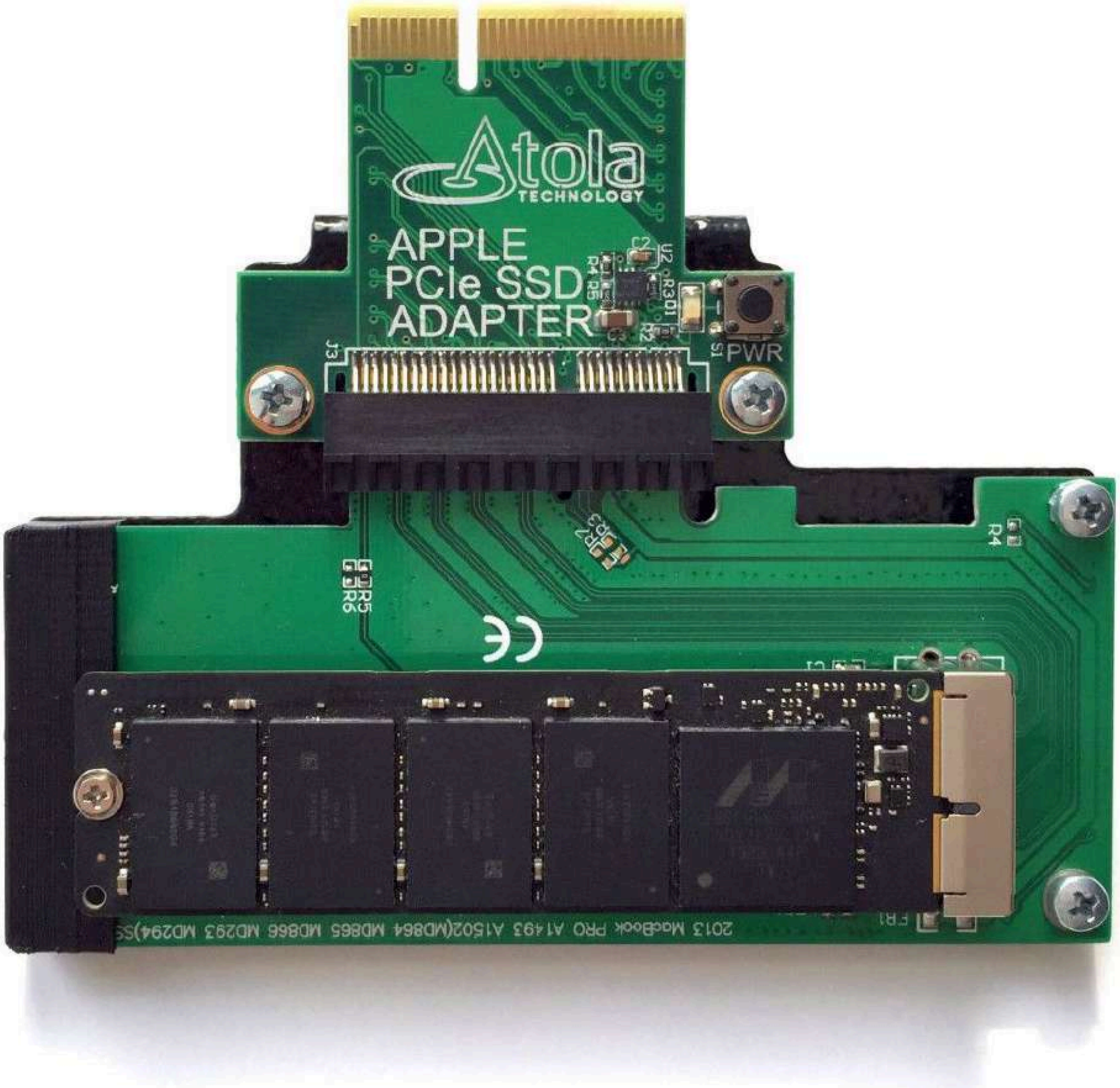
1. Plug the U.2 drive into the U.2-to-M.2 adapter using the cable.
2. Plug the U.2-to-M.2 adapter into the Atola M.2 SSD extension.
3. Plug the extension into TaskForce while the unit is powered off.

> U.2 SSD adapters are available to combine them with the Atola M.2 SSD extension. Please contact your Atola dealer for more information.

Connect and identify an M.2 SATA drive

To connect an M.2 SATA drive to the TaskForce 2, you will need to use one of the SATA ports and an M.2 to SATA SSD adapter. Please contact your Atola dealer for more information on adapters.

Apple PCIe SSD extension module


Atola
TECHNOLOGY
APPLE
PCIe SSD
ADAPTER
PWR
2013 MacBook PRO A1493 A1502(MD864 MD865 MD866 MD293 MD294)SS

Apple PCIe SSD extension lets you connect TaskForce to the PCIe SSDs with the custom proprietary M.2 interface within Apple laptops:

- MacBook Pro, Late 2013-2015
- MacBook Air, 2013-2015

TaskForce Apple PCIe SSD extension module works with Atola DiskSense 2 as well.

TaskForce features supported for Apple PCIe SSD extension

The following TaskForce operations and features are supported for the Apple drives:

- Write protection with the physical source/target switch

- Diagnostics
- Physical and logical imaging
- Hash calculation
- Damaged drive support

Plug and unplug the Apple PCIe SSD extension module

TaskForce hardware unit is equipped with the PCI Express port on its back panel, which is referred to as Extension port. It is used to plug Atola hardware extension modules supported by Atola TaskForce software.

> **Important:** Do not plug or unplug the extension module when TaskForce is turned on, it can damage the extension module or TaskForce hardware unit.

To connect the Apple PCIe SSD extension module to TaskForce, do the following:

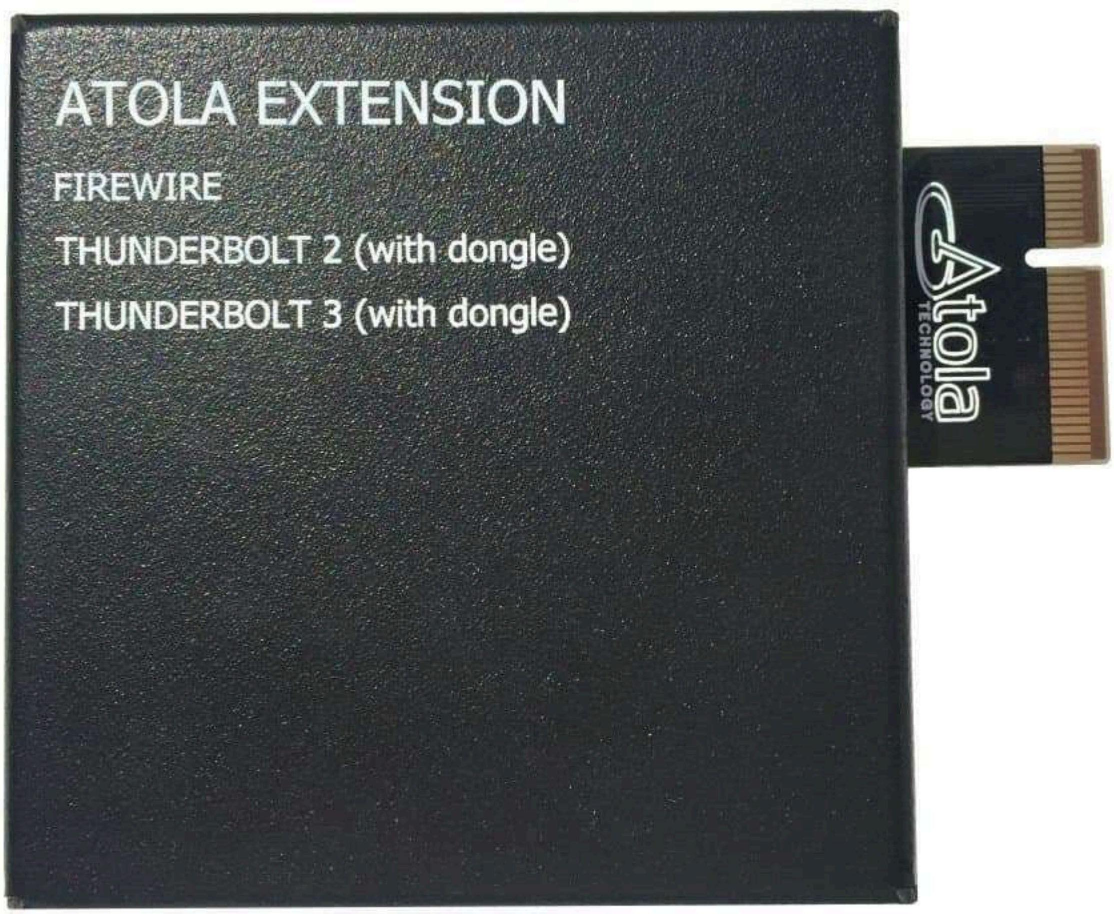
1. Power off TaskForce.
2. Align the screw on the extension module and the top screw hole on the Taskforce back panel. Plug the Apple PCIe SSD extension module into the Extension port and fix the module with a screw.
3. Plug an Apple PCIe SSD drive into the extension and fasten the drive with the black plastic latch.
4. Power on TaskForce.

> **Important:** Drive hotplug is not supported yet. TaskForce must be powered off before installing or replacing Apple PCIe SSDs.

To disconnect the Apple PCIe SSD extension module or replace it with another extension module, do the following steps:

1. Power off TaskForce.
2. Release the screw, which holds the module, and unplug it from the Extension port.
3. **Optional:** Plug another extension module into the Extension port and fix the module with a screw.
4. Power on TaskForce.

Thunderbolt extension module



Thunderbolt extension enables TaskForce to work on MacBooks with the following interfaces:

1. FireWire
2. Thunderbolt 2
3. Thunderbolt 3, 2016-2017 models

No SSD removal is necessary, the extension allows connecting TaskForce directly to a MacBook.

The extension module comes with:

- FireWire cable (comes in white or black color)
- Thunderbolt 2 to FireWire adapter (by Apple)
- Thunderbolt 3 to Thunderbolt 2 adapter (by Apple)

TaskForce Thunderbolt extension module works with Atola DiskSense 2 as well.

TaskForce features supported for Thunderbolt extension

TaskForce supports the following operations and features on MacBooks when connected through Thunderbolt extension:

- Write protection with the physical source/target switch
- Physical and logical imaging
- Hash calculation
- Damaged drive support

Plug and unplug the Thunderbolt extension module

TaskForce hardware unit is equipped with the PCI Express port on its back panel, which is referred to as an Extension port. It is used to plug Atola hardware extension modules supported by Atola TaskForce software.

Important: Do not plug or unplug the extension module when TaskForce is turned on, this can damage the extension module or TaskForce hardware unit.

To connect the Thunderbolt extension module to TaskForce, do the following:

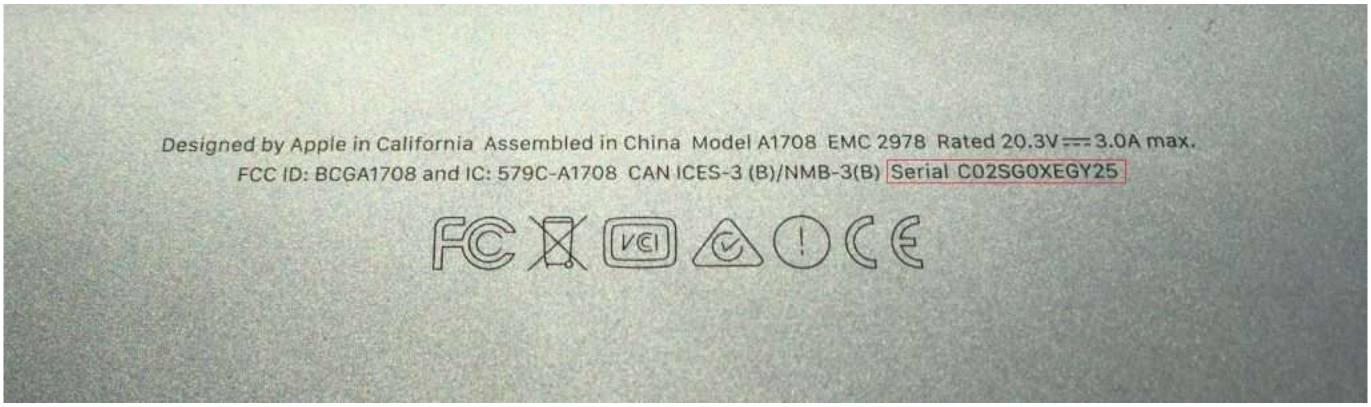
1. Power off TaskForce.
2. Align the screw on the extension module and the top screw hole on the Taskforce back panel. Plug the Thunderbolt extension module into the Extension port and fasten the module with a screw.
3. Power on TaskForce.

To disconnect the Thunderbolt extension module or replace it with another extension module, do the following steps:

1. Power off TaskForce.
2. Release the screw, which holds the module, and unplug it from the Extension port.
3. **Optional:** Plug another extension module into the Extension port and fix the module with a screw.
4. Power on TaskForce.

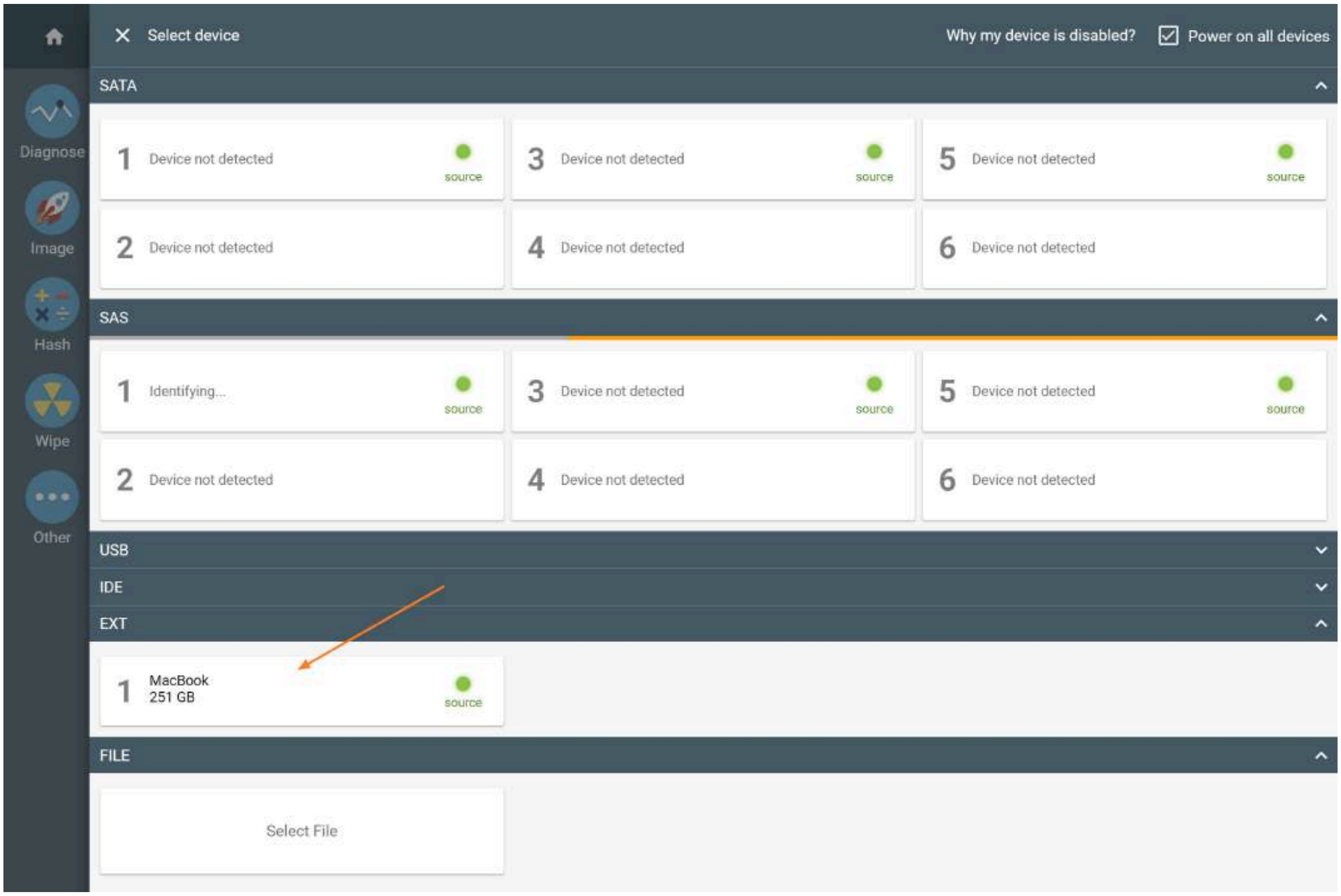
Connect MacBook using Thunderbolt extension module

First, write down or take a photo of the serial number located on the bottom side of the MacBook. It will be needed later.


Designed by Apple in California Assembled in China Model A1708 EMC 2978 Rated 20.3V ⎓ 3.0A max.
FCC ID: BCGA1708 and IC: 579C-A1708 CAN ICES-3 (B)/NMB-3(B) Serial C02SG0XEGY25
VCI

Then do the following steps:

1. Turn off both the MacBook and TaskForce.
2. Plug the Thunderbolt extension module into the Extension port and fasten the module with a screw.
3. Connect the MacBook to TaskForce unit with the help of the Thunderbolt extension and the FireWire cable. Use adapters to connect to the MacBooks with Thunderbolt 2 or Thunderbolt 3 interface.
4. Boot the MacBook in the Target Disk Mode. To do that, start it up while holding down the T key. You should see a Firewire or Thunderbolt icon displayed on screen, signifying that Target Disk Mode is detected and working.
5. Power on TaskForce and wait for the booting to be completed.
6. In the TaskForce main window, open the **Device** panel.
7. Click the port in the **EXT** section of the **Device** panel.



Select device

Why my device is disabled? ☑ Power on all devices

SATA

1 Device not detected ● source

3 Device not detected ● source

5 Device not detected ● source

2 Device not detected

4 Device not detected

6 Device not detected

SAS

1 Identifying... ● source

3 Device not detected ● source

5 Device not detected ● source

2 Device not detected

4 Device not detected

6 Device not detected

USB

IDE

EXT

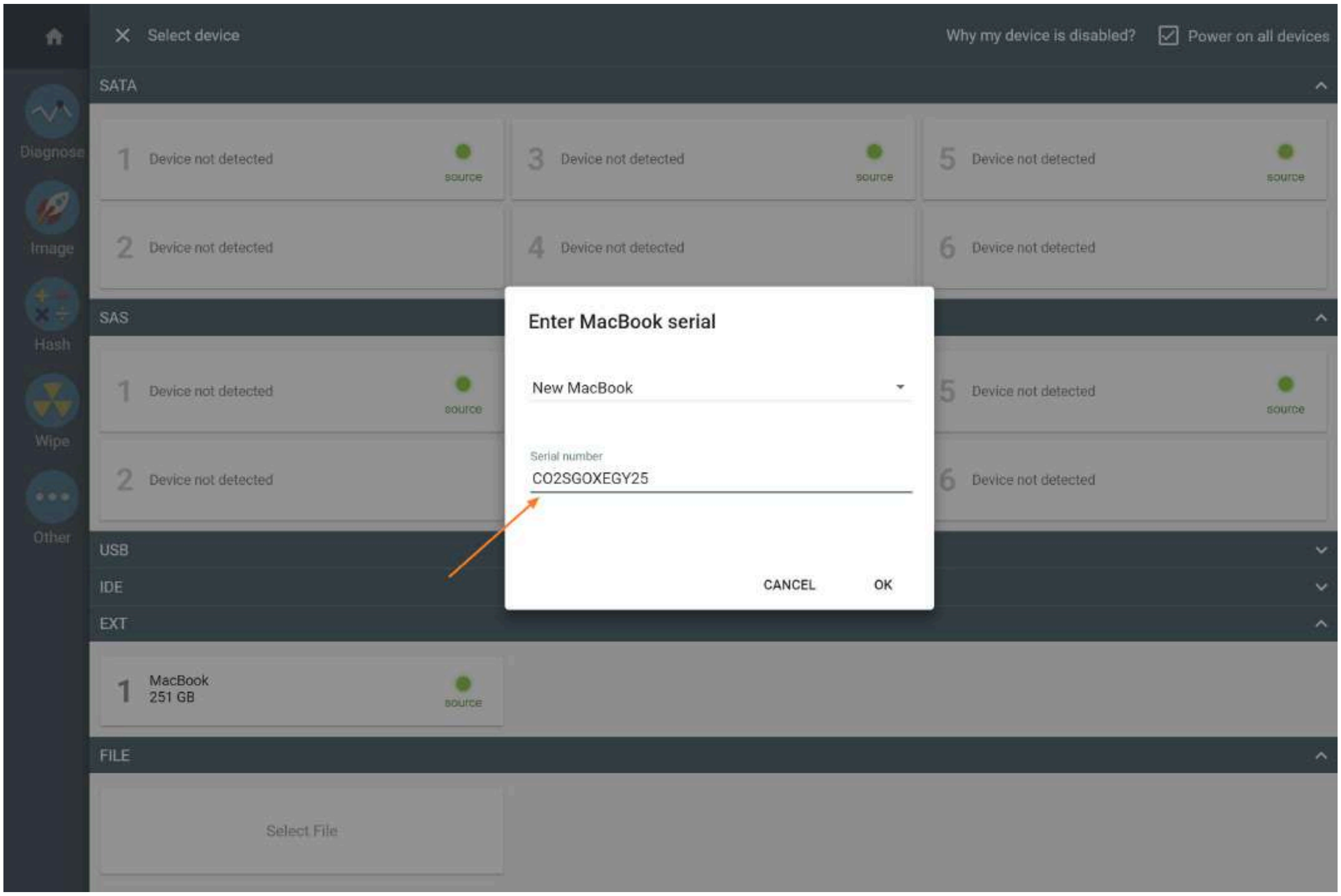
1 MacBook 251 GB ● source

FILE

Select File

MacBook device in the EXT section of the Device panel.

8. If it is the first time this MacBook is identified by TaskForce, in the **Enter MacBook serial** window, enter the serial number located on the bottom side of the MacBook, and then click **OK**.



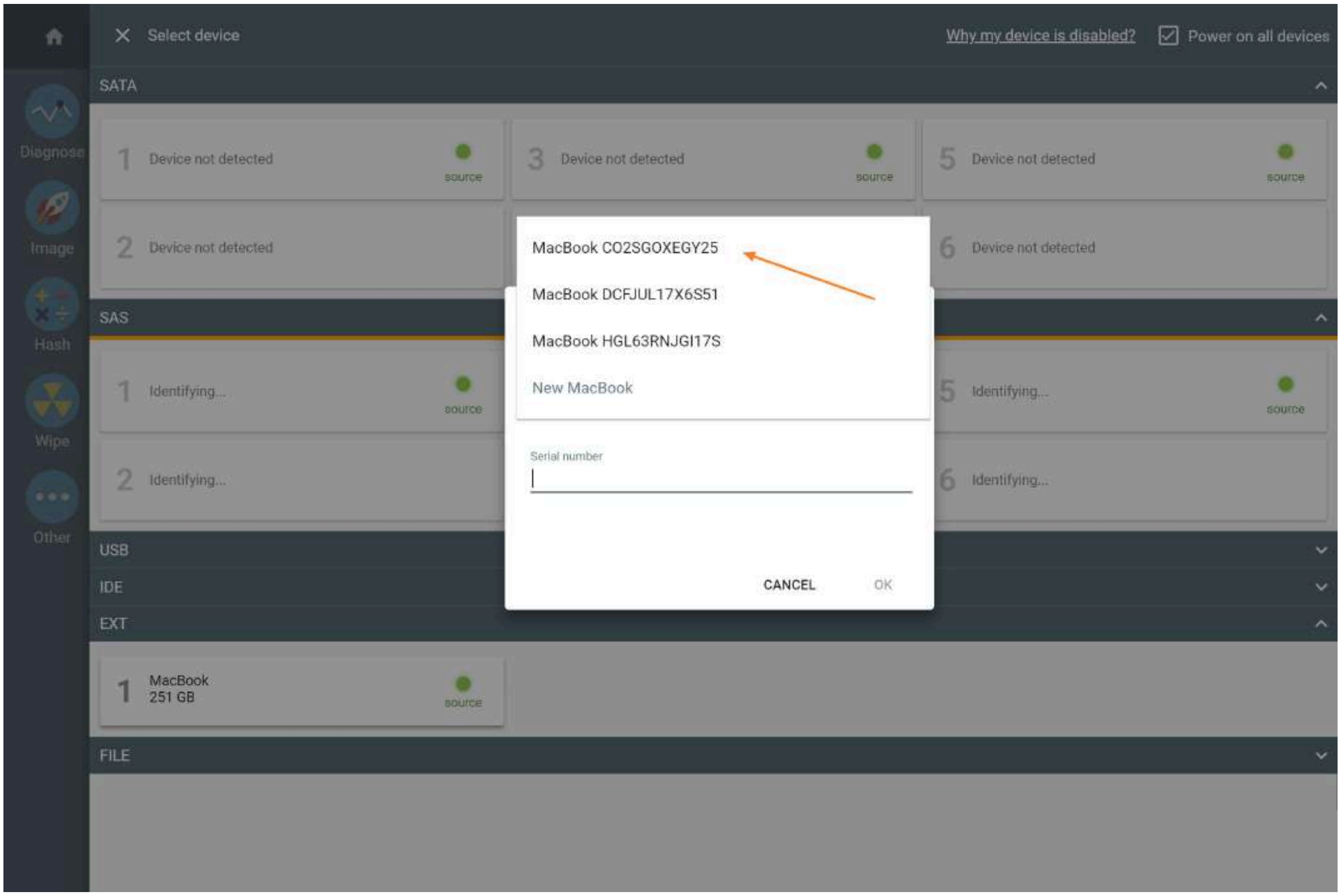
Enter MacBook serial

New MacBook

Serial number: CO2SGOXEGY25

Enter MacBook's serial number.

During the subsequent identifications of the MacBook connected to TaskForce, its serial number can be selected from the drop-down menu in the **Enter MacBook serial** window. TaskForce will look up its case management system and offer the choice of MacBooks with the same drive size.



Select the MacBook with the serial number you have connected to TaskForce.

Extend subscription

Atola TaskForce 2 comes with a complimentary 1-year subscription. It covers regular software updates, includes training and technical support from our in-house team of developers, and secures a lifetime warranty.

Buy subscription

To extend your subscription for another period, you first need to place a purchase order with the reseller that sold you the unit or on the Atola website.

If your subscription has not yet expired, you can still purchase and activate a new one. The new subscription period will commence the day following the current subscription’s expiration date.

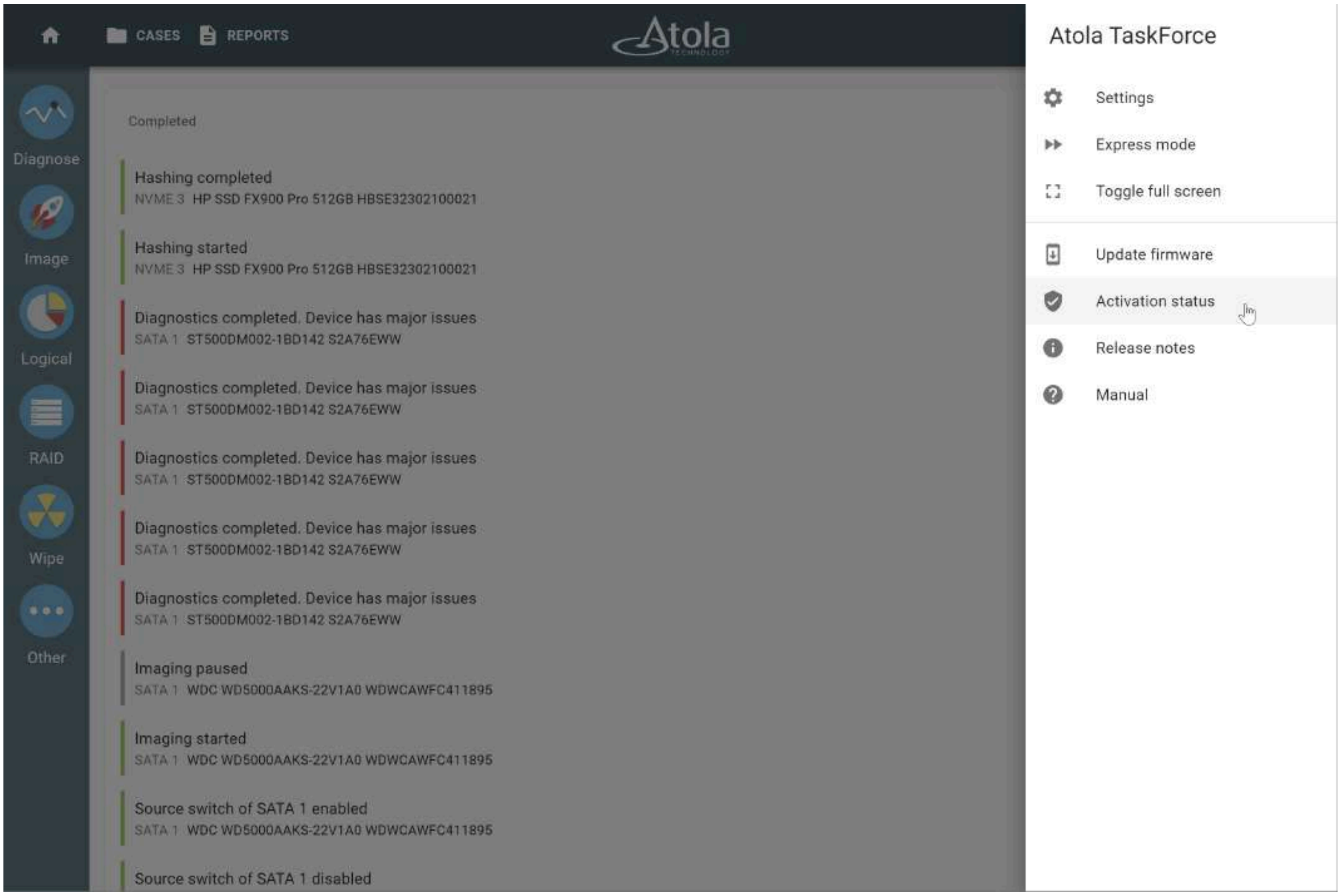
Extend subscription

You will need:

- A device with an internet connection (PC or mobile).
- The serial number located on the bottom side of the TaskForce 2 unit.

After you have purchased a subscription, do the following:

1. On a device with an internet connection, open the TaskForce 2 user interface in your web browser.
2. At the top right, click **Menu** > **Activation status**.



Completed

Hashing completed
NVME 3 HP SSD FX900 Pro 512GB HBSE32302100021

Hashing started
NVME 3 HP SSD FX900 Pro 512GB HBSE32302100021

Diagnostics completed. Device has major issues
SATA 1 ST500DM002-1BD142 S2A76EWW

Diagnostics completed. Device has major issues
SATA 1 ST500DM002-1BD142 S2A76EWW

Diagnostics completed. Device has major issues
SATA 1 ST500DM002-1BD142 S2A76EWW

Diagnostics completed. Device has major issues
SATA 1 ST500DM002-1BD142 S2A76EWW

Diagnostics completed. Device has major issues
SATA 1 ST500DM002-1BD142 S2A76EWW

Imaging paused
SATA 1 WDC WD5000AAKS-22V1A0 WDWCAWFC411895

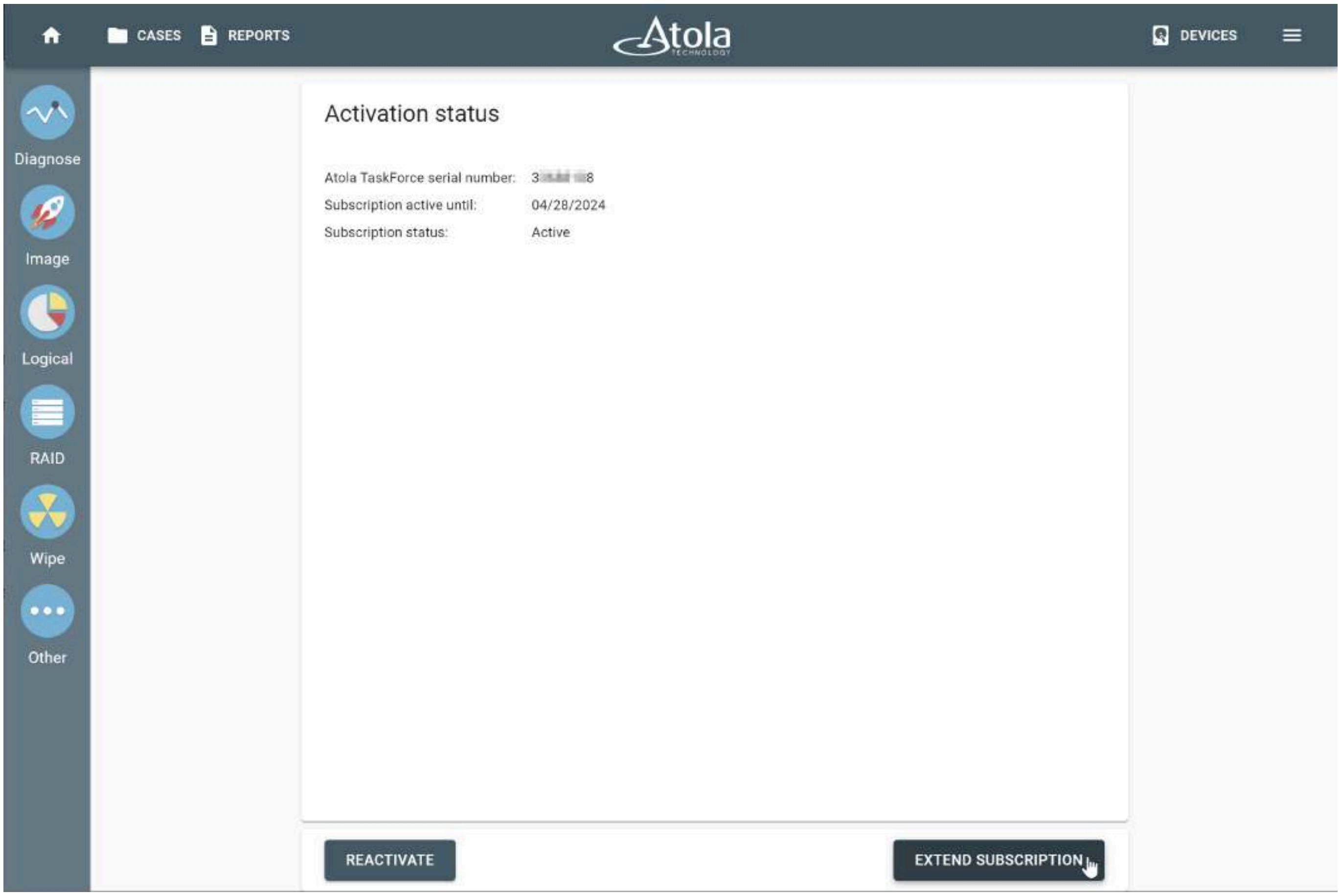
Imaging started
SATA 1 WDC WD5000AAKS-22V1A0 WDWCAWFC411895

Source switch of SATA 1 enabled
SATA 1 WDC WD5000AAKS-22V1A0 WDWCAWFC411895

Source switch of SATA 1 disabled

The Activation status option in the TaskForce Menu.

3. Click **Extend subscription**.

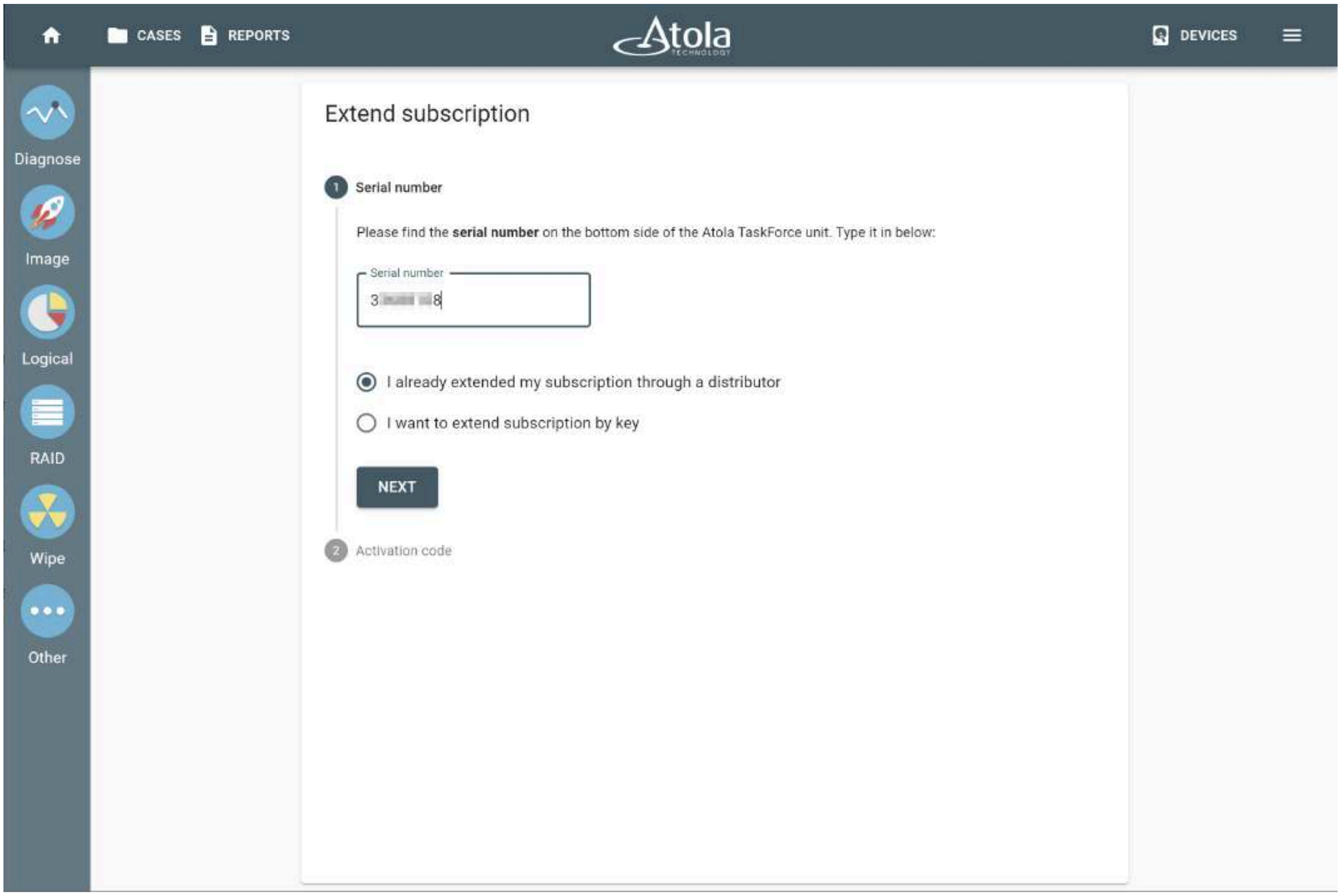


Activation status

Atola TaskForce serial number: 3[redacted]8
Subscription active until: 04/28/2024
Subscription status: Active

The Extend subscription button on the Activation status page.

4. Enter the **serial number** of the TaskForce 2 unit.
5. Select **I already extended my subscription through a distributor**, and then click **Next**.



Extend subscription

1 Serial number

Please find the **serial number** on the bottom side of the Atola TaskForce unit. Type it in below:

Serial number: 3[redacted]8

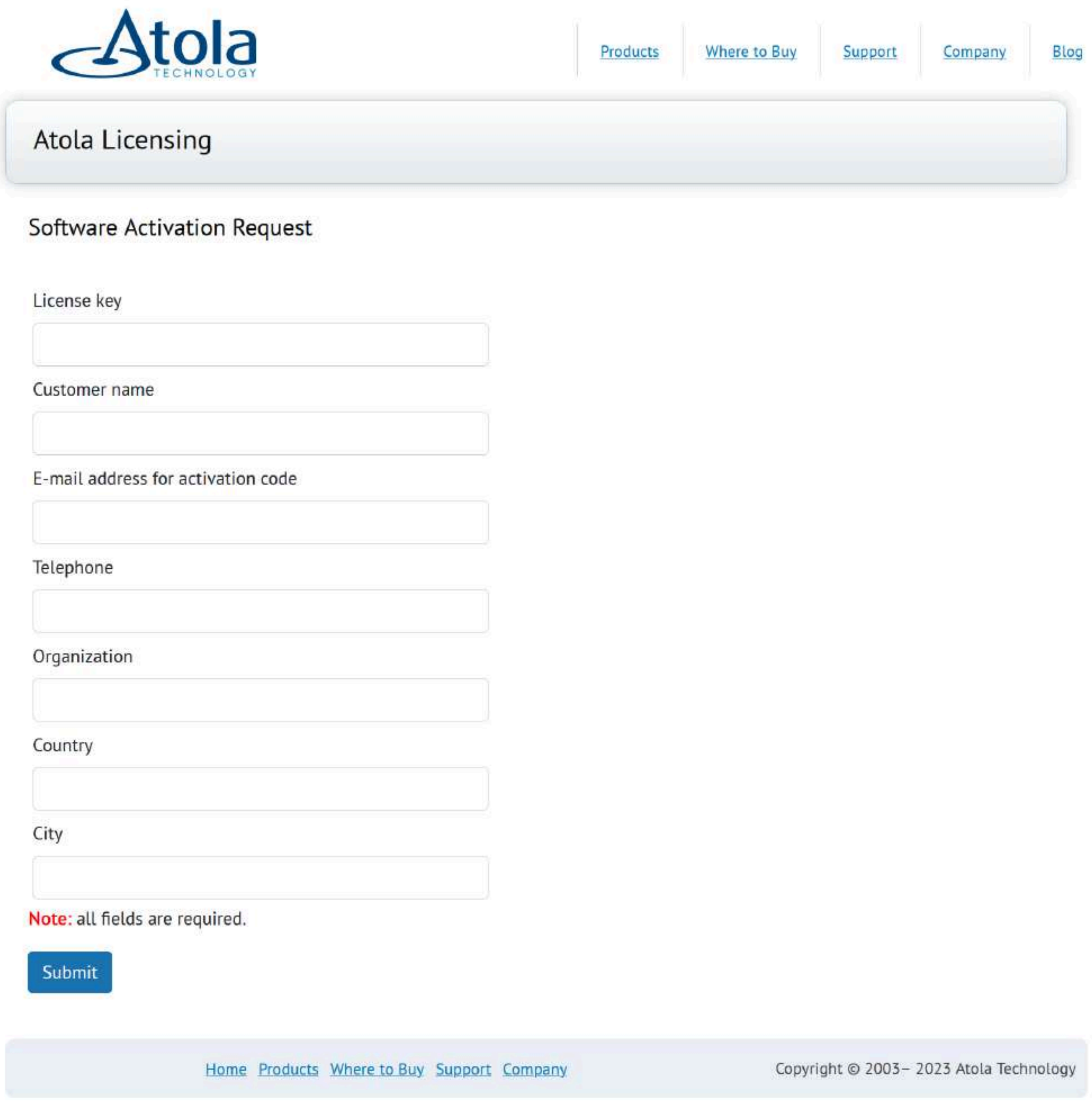
● I already extended my subscription through a distributor

○ I want to extend subscription by key

2 Activation code

The Extend subscription page.

6. Visit the Atola **licensing page**: a.atola.com or scan QR code on the screen.
7. On the Atola **licensing page**, enter the **license key** shown in TaskForce web interface.
8. Fill out all other fields on the Atola licensing webpage, including:
    - Customer name
    - E-mail address for activation code
    - Telephone
    - Organization, country and city



Atola Licensing

Software Activation Request

License key

Customer name

E-mail address for activation code

Telephone

Organization

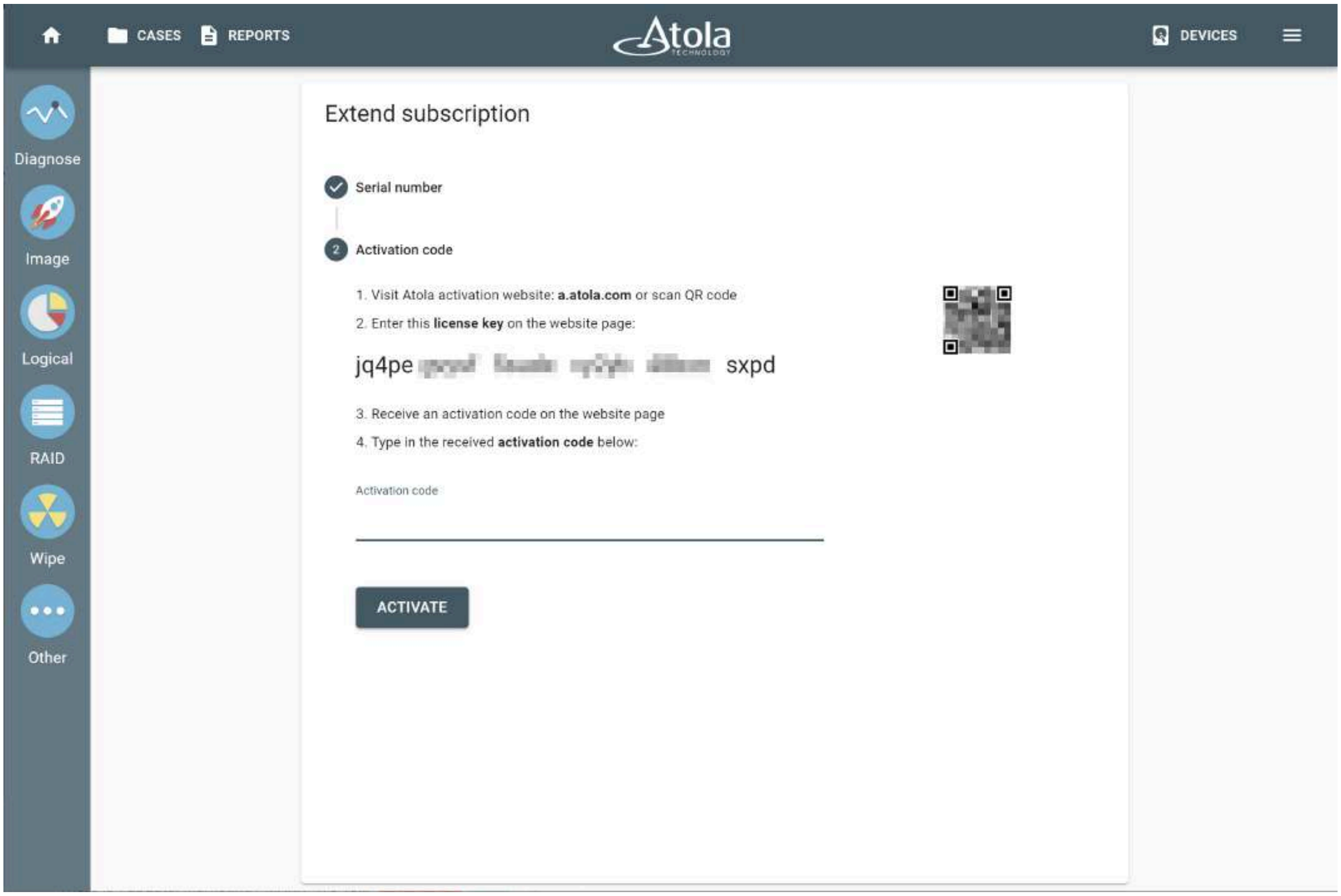
Country

City

Note: all fields are required.

Copyright © 2003– 2023 Atola Technology

9. Click **Submit**. The Atola licensing webpage generates an activation code.
10. Go back to TaskForce 2 user interface and enter the **activation code** in the respective field.



Extend subscription

Serial number

2 Activation code

1. Visit Atola activation website: **a.atola.com** or scan QR code
2. Enter this **license key** on the website page:

jq4pe [redacted] sxpd

3. Receive an activation code on the website page
4. Type in the received **activation code** below:

Activation code

ACTIVATE

Entering the activation code on the Extend subscription page.

11. Click **Activate**. TaskForce 2 confirms that reactivation has been successfully completed.

Connectivity and multi-user access

Atola TaskForce 2 has three connectivity options:

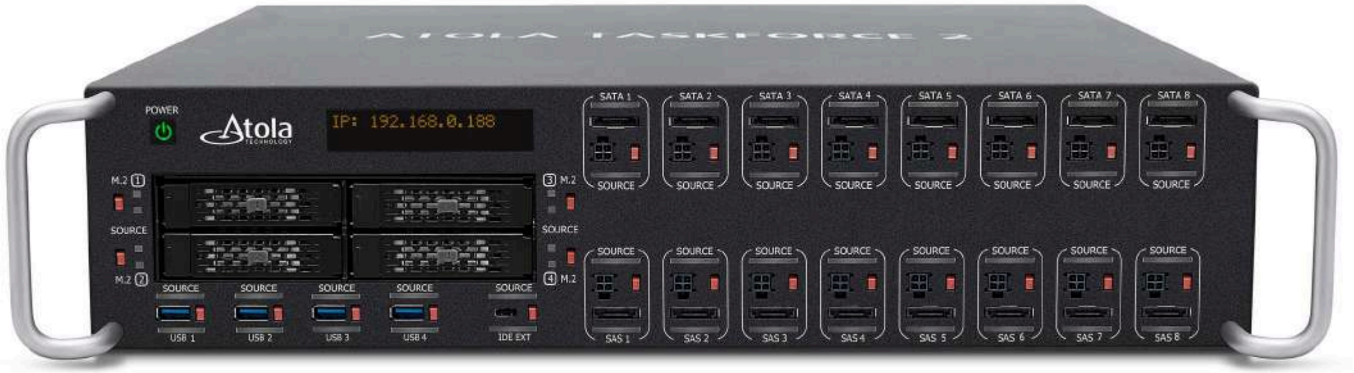
1. 10Gb Ethernet network
2. Kiosk mode
3. Wi-Fi access point (optional)

10Gb Ethernet network

TaskForce is equipped with two 10Gb Ethernet ports. Whenever the system is connected to a local network via one of its Ethernet ports, an IP address will be displayed on the IP screen on the system's front panel.

Supported network features:

- Two 10Gb Ethernet ports
- Dynamic (DHCP) IP / Static IP address
- Settings: DNS nameserver, Default gateway, Jumbo frames
- Secure connection with password-protected network folders
- Support of HTTPS with external organizational and self-signed certificates



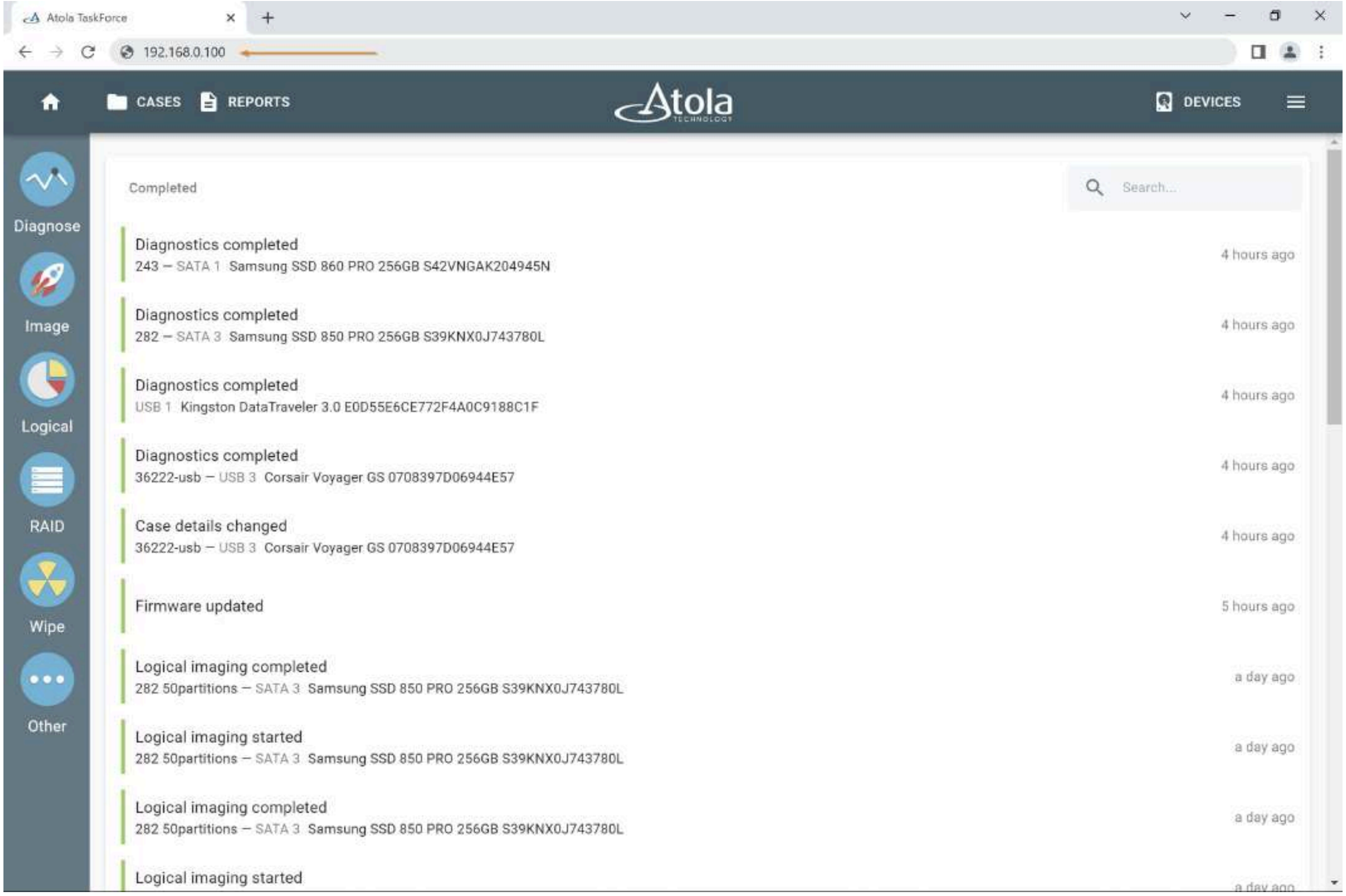
TaskForce 2 shows an IP address required to connect to its user interface

If the system is connected via both Ethernet ports, two IP addresses will be displayed on the screen. These IP addresses are assigned to TaskForce by your DHCP server.

Multi-user access

With the help of these IP addresses, TaskForce can be operated by multiple users simultaneously from their workstations or mobile devices:

- enter either of the IP addresses as shown on the IP screen in Chrome browser on another device within the same local network.



Completed

Diagnostics completed
243 – SATA 1 Samsung SSD 860 PRO 256GB S42VNGAK204945N
4 hours ago

Diagnostics completed
282 – SATA 3 Samsung SSD 850 PRO 256GB S39KNX0J743780L
4 hours ago

Diagnostics completed
USB 1 Kingston DataTraveler 3.0 E0D55E6CE772F4A0C9188C1F
4 hours ago

Diagnostics completed
36222-usb – USB 3 Corsair Voyager GS 0708397D06944E57
4 hours ago

Case details changed
36222-usb – USB 3 Corsair Voyager GS 0708397D06944E57
4 hours ago

Firmware updated
5 hours ago

Logical imaging completed
282 50partitions – SATA 3 Samsung SSD 850 PRO 256GB S39KNX0J743780L
a day ago

Logical imaging started
282 50partitions – SATA 3 Samsung SSD 850 PRO 256GB S39KNX0J743780L
a day ago

Logical imaging completed
282 50partitions – SATA 3 Samsung SSD 850 PRO 256GB S39KNX0J743780L
a day ago

Logical imaging started
a day ago

Enter IP address in Chrome browser

Through the Chrome browser one can remotely track and manage tasks, power devices on and off, open, edit and print cases, etc.

Types of devices that can be used to access TaskForce simultaneously include:

- Desktop PC
- Laptop
- Tablet
- Smartphone

TaskForce software can be opened in the Chrome browser within any OS.

This functionality enables a group of users to work on different assignments using the same tool. This helps utilize TaskForce’s multitasking capabilities to the maximum and track operation progress remotely. The number of users accessing TaskForce simultaneously is unlimited.

Kiosk mode

Use TaskForce without any network connection in the Kiosk mode by plugging a VGA monitor, keyboard, and mouse into respective ports on the **back side** of the TaskForce hardware unit.

Whenever the system is not connected to a network via its 10Gb Ethernet ports, the *Kiosk mode* status is displayed on the IP screen.

Once a monitor is plugged in, it displays the Taskforce user interface, and you can operate the system using a keyboard and mouse.

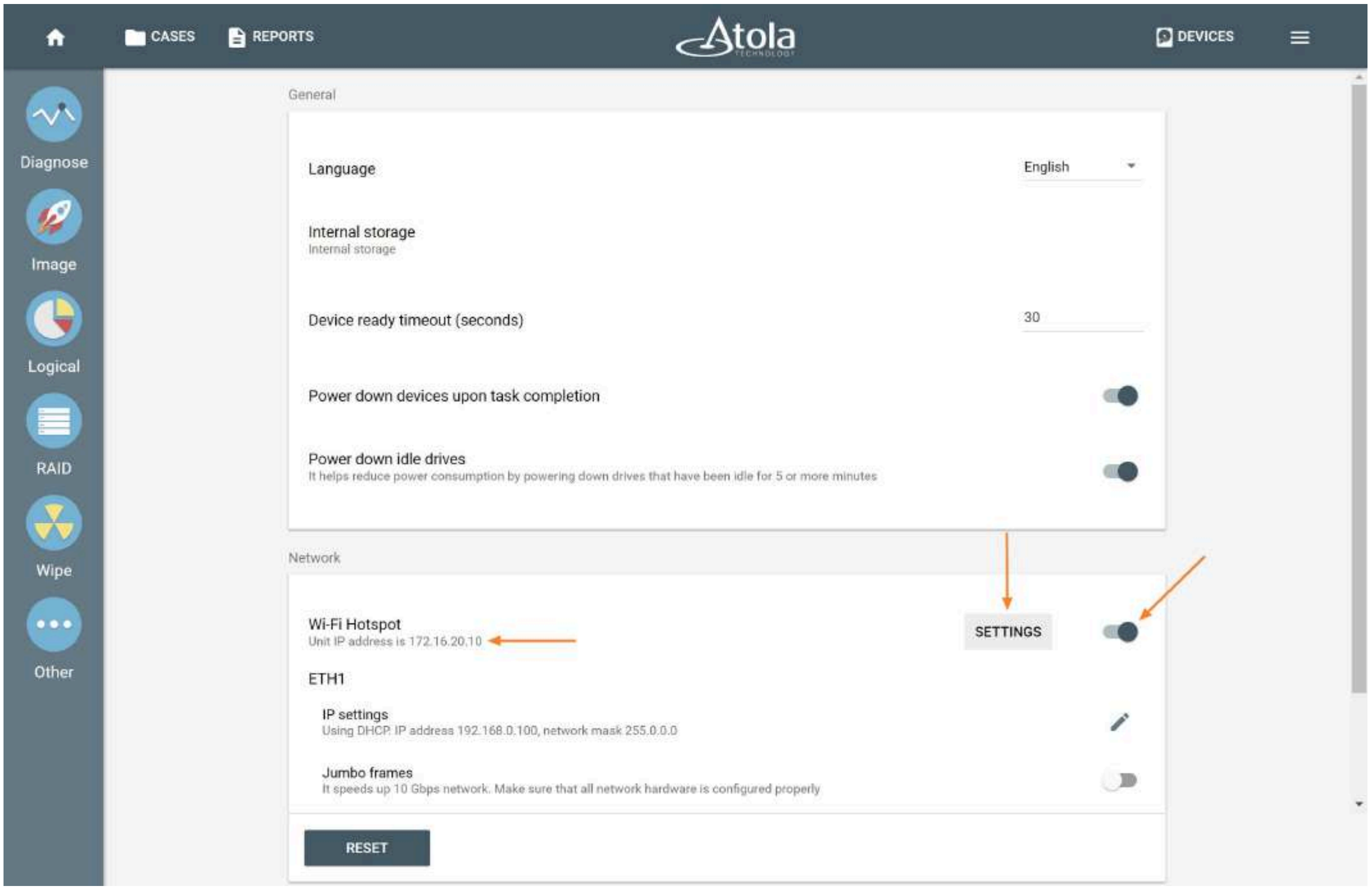
TaskForce 2 in the Kiosk mode.

Wi-Fi access point

The third way to access TaskForce's user interface is via a Wi-Fi 802.11n 150 Mb/s adapter (included in the package). Once the Wi-Fi access point is established, TaskForce can be operated by multiple users simultaneously from their devices connected to the hotspot.

To enable the adapter, follow these steps:

1. Plug the adapter into one of the TaskForce's USB ports.
2. Go to **Menu** in the top right corner of the TaskForce web page.
3. Click **Settings**.
4. Enable **Wi-Fi Hotspot**. An IP address of the hotspot will appear on the unit’s IP screen as well as under the **Wi-Fi Hotspot** category in the **Settings** window.
5. Click **Settings**.



General

Language: English

Internal storage
Internal storage

Device ready timeout (seconds): 30

Power down devices upon task completion

Power down idle drives
It helps reduce power consumption by powering down drives that have been idle for 5 or more minutes

Network

Wi-Fi Hotspot
Unit IP address is 172.16.20.10

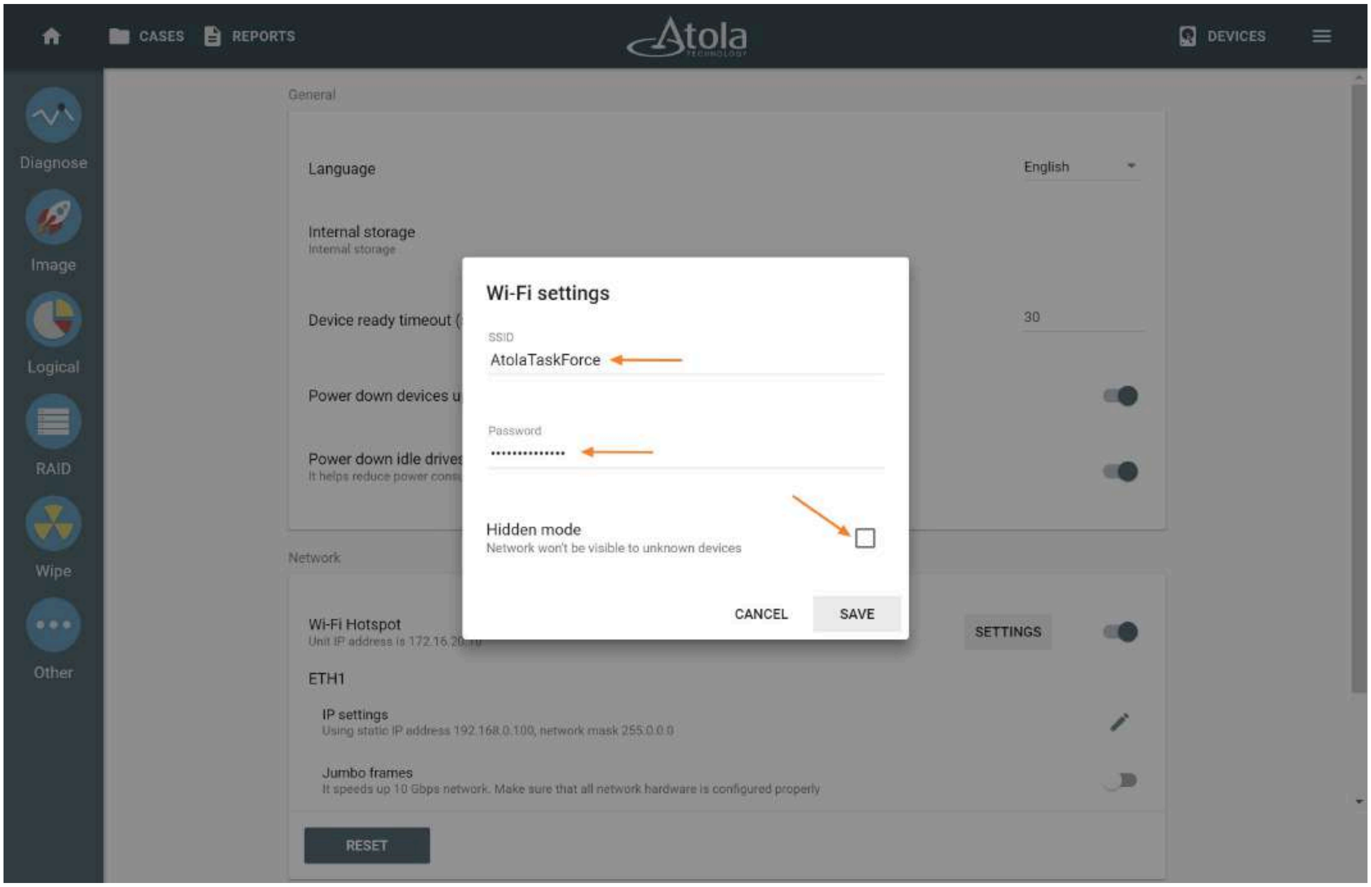
ETH1

IP settings
Using DHCP. IP address 192.168.0.100, network mask 255.0.0.0

Jumbo frames
It speeds up 10 Gbps network. Make sure that all network hardware is configured properly

Enable Wi-Fi Hotspot

5. Enable **Wi-Fi Hotspot**.
6. Set **SSID** and **Password**. To make the network invisible to other devices, select **Hidden mode**. Click **Save**.
7. Use these details to connect to the Hotspot from another device.



General

Language English

Internal storage
Internal storage

Device ready timeout (30

Power down devices u

Power down idle drives
It helps reduce power cons

Network

Wi-Fi Hotspot
Unit IP address is 172.16.20.10

SETTINGS

ETH1

IP settings
Using static IP address 192.168.0.100, network mask 255.0.0.0

Jumbo frames
It speeds up 10 Gbps network. Make sure that all network hardware is configured properly

RESET

Wi-Fi settings

SSID
AtolaTaskForce

Password
••••••••••••••

Hidden mode
Network won't be visible to unknown devices □

CANCEL SAVE

Adjust Wi-Fi settings

8. To open the TaskForce interface, enter the unit's IP address (indicated on the unit's IP screen as well as under the **Wi-Fi Hotspot** category in the **Settings** window, see Step 4) in the Chrome browser of the device connected to the Hotspot.

Use TaskForce with multiple user profiles

For security reasons, you can allow access to Atola TaskForce only for authorized users, protect each user profile with a password, and keep processes, reports, and cases separate and confidential for each user.

Also, you can set up Atola TaskForce to automatically lock its screen after a certain time of inactivity and to prompt a user to log in.

Setting up user roles and profiles is an optimal solution when you want to:

- Share one Atola TaskForce unit with multiple colleagues at the same time.
- Prevent other users from interrupting the processes you started on your TaskForce.
- Prevent your colleagues from seeing each other's cases.
- Temporarily pass your TaskForce to another forensic lab, department, or agency without giving access to your cases.

What others can see and do when you share one TaskForce

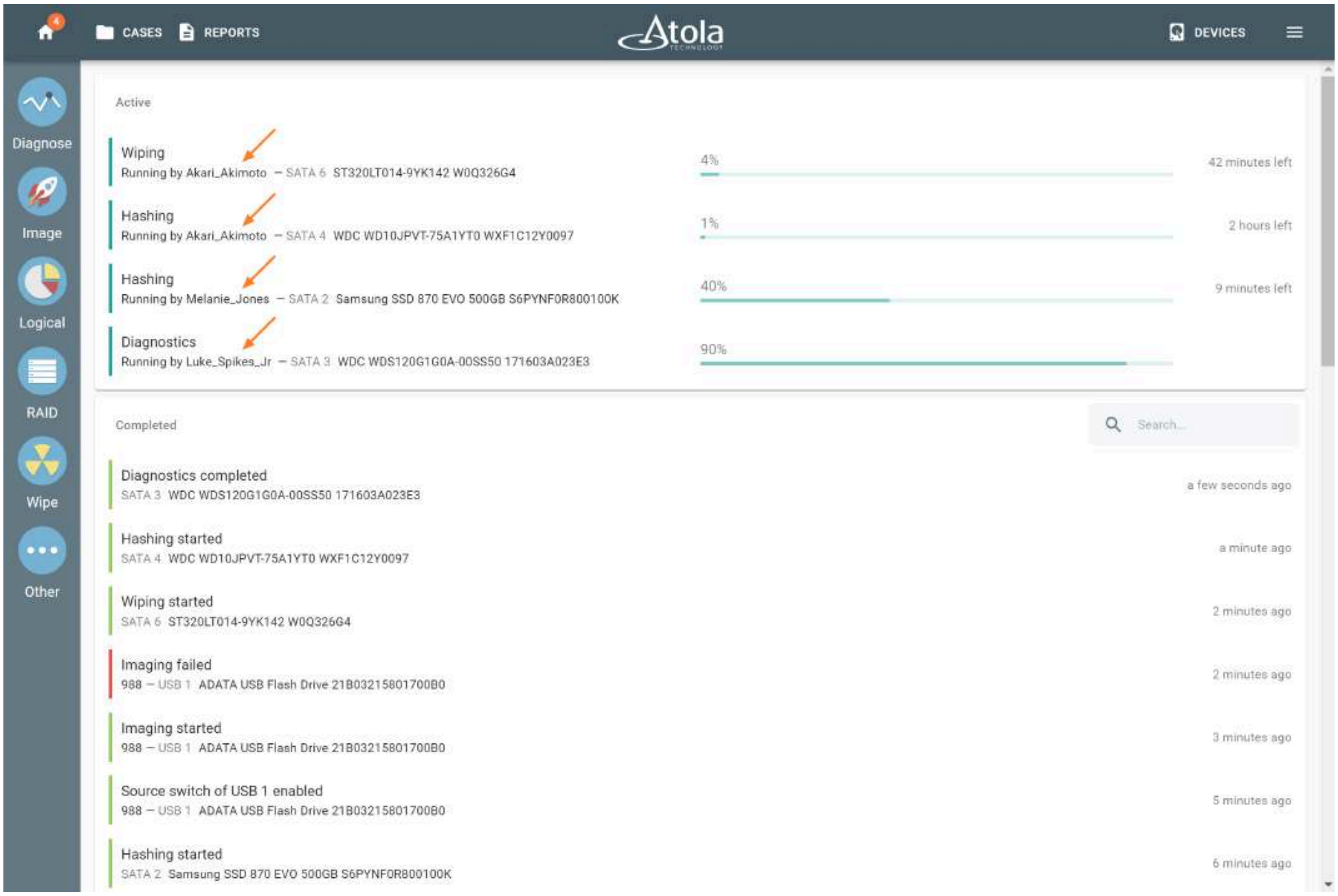
After you enable User management, you become an administrator and can create up to 20 profiles with either *Admin* or *User* roles. These roles have different permissions.

What an Admin can see and do

The first profile that you create after enabling User management has an Admin role. You can have more than one profile with the Admin role on your TaskForce.

As an *Admin*, **you can**:

- See and edit all cases of other users.
- See and stop all processes run by other users.
- See and print all reports created by other users.
- Access and change all TaskForce settings.
- Enable or disable User management.
- Add, edit, or delete other user profiles with either *Admin* or *User* role.
- Change other user's password.
- Set TaskForce to automatically lock the screen after a certain time of inactivity.



Active

Wiping
Running by Akari_Akimoto – SATA 6 ST320LT014-9YK142 W0Q326G4
4%
42 minutes left

Hashing
Running by Akari_Akimoto – SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097
1%
2 hours left

Hashing
Running by Melanie_Jones – SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800100K
40%
9 minutes left

Diagnostics
Running by Luke_Spikes_Jr – SATA 3 WDC WDS120G1G0A-00SS50 171603A023E3
90%

Completed

Diagnostics completed
SATA 3 WDC WDS120G1G0A-00SS50 171603A023E3
a few seconds ago

Hashing started
SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097
a minute ago

Wiping started
SATA 6 ST320LT014-9YK142 W0Q326G4
2 minutes ago

Imaging failed
988 – USB 1 ADATA USB Flash Drive 21B03215801700B0
2 minutes ago

Imaging started
988 – USB 1 ADATA USB Flash Drive 21B03215801700B0
3 minutes ago

Source switch of USB 1 enabled
988 – USB 1 ADATA USB Flash Drive 21B03215801700B0
5 minutes ago

Hashing started
SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800100K
6 minutes ago

Admin sees all processes and cases of other users.

What a User can see and do

A profile with a *User* role is created by *Admin* and has limited access to TaskForce.

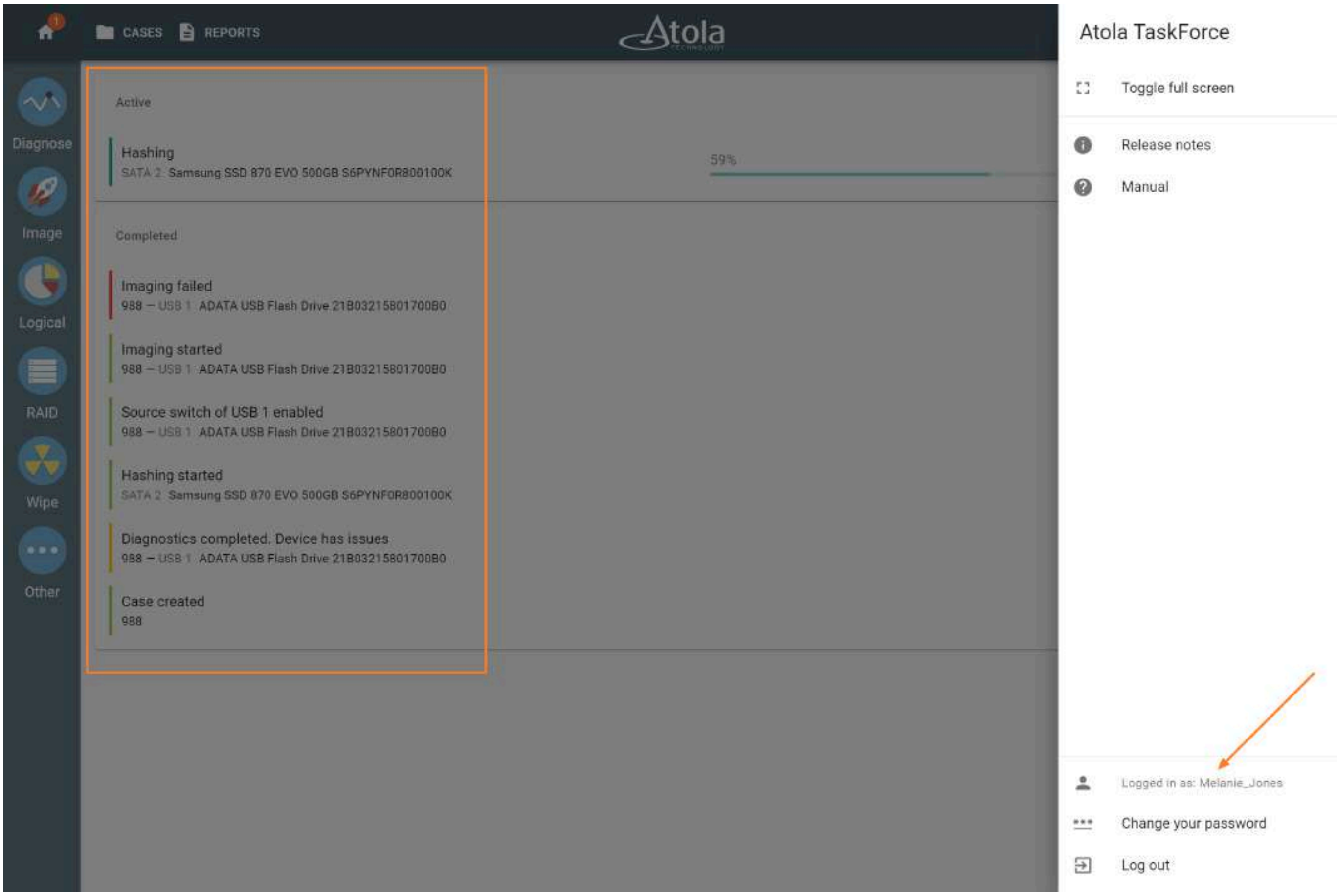
As a *User*, **you can**:

- Log in only to your user profile.
- See and edit only your cases.
- See and print only your reports.
- See, run, and stop only your processes.
- Change only your password.

As a *User*, **you can't**:

- Access somebody else's user profile.
- See and edit other users' cases.
- See and print other users' reports.
- See or interrupt other users' processes.
- Access a device that is being used by another user

- Access and change TaskForce settings.
- Enable or disable User management.
- Add, edit, or delete other user profiles.
- Change other user's password.
- Disable or configure Automatically lock screen feature set by Admin.



Active

Hashing
SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800100K

59%

Completed

Imaging failed
988 — USB 1 ADATA USB Flash Drive 21B03215801700B0

Imaging started
988 — USB 1 ADATA USB Flash Drive 21B03215801700B0

Source switch of USB 1 enabled
988 — USB 1 ADATA USB Flash Drive 21B03215801700B0

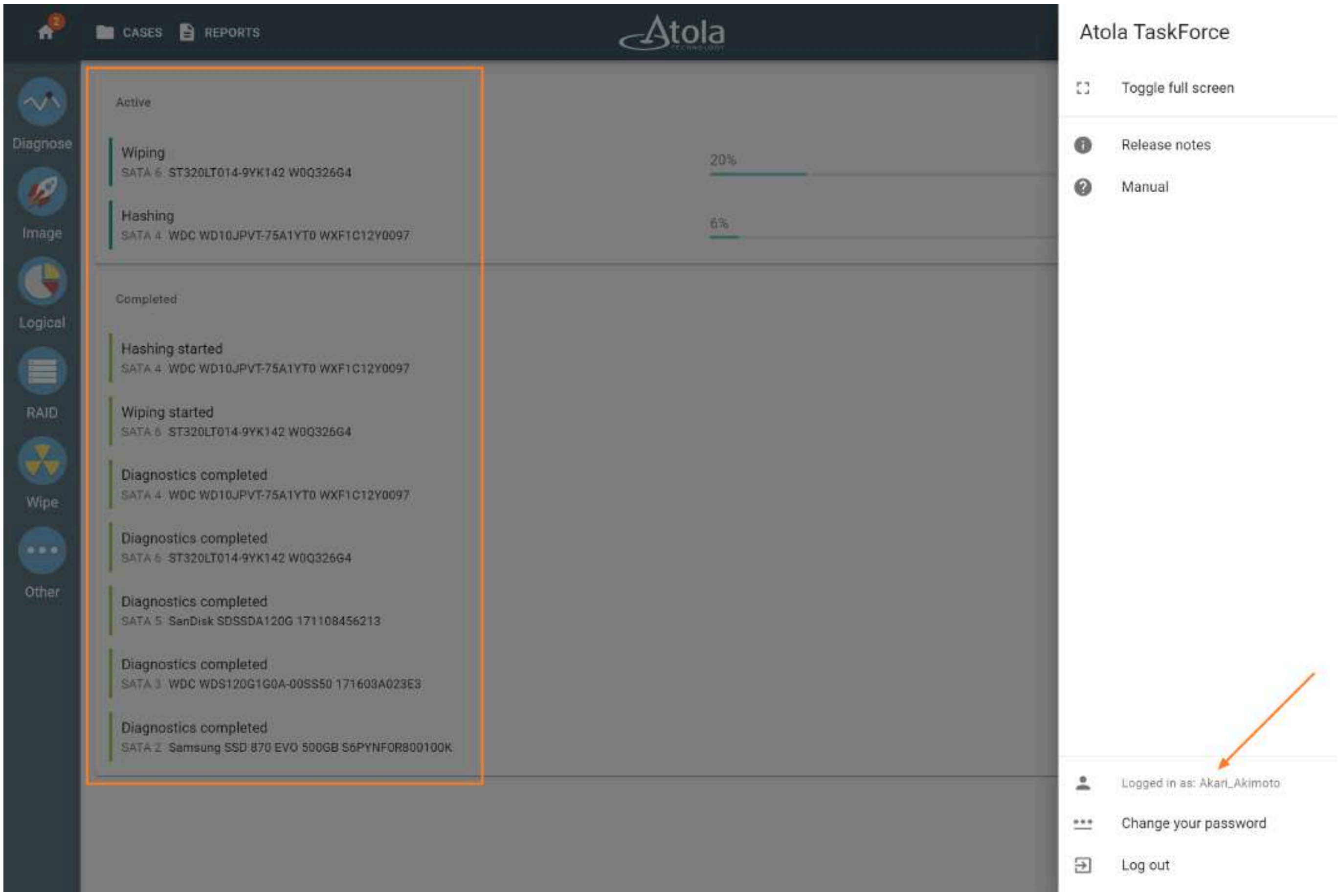
Hashing started
SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800100K

Diagnostics completed. Device has issues
988 — USB 1 ADATA USB Flash Drive 21B03215801700B0

Case created
988

Logged in as: Melanie_Jones

Profiles with a User role see only their cases and processes.



Active

Wiping
SATA 6 ST320LT014-9YK142 W0Q326G4 20%

Hashing
SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097 6%

Completed

Hashing started
SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097

Wiping started
SATA 6 ST320LT014-9YK142 W0Q326G4

Diagnostics completed
SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097

Diagnostics completed
SATA 6 ST320LT014-9YK142 W0Q326G4

Diagnostics completed
SATA 5 SanDisk SDSSDA120G 171108456213

Diagnostics completed
SATA 3 WDC WDS120G1G0A-00SS50 171603A023E3

Diagnostics completed
SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800100K

Logged in as: Akari_Akimoto

Profiles with a User role don’t see each other’s cases and processes.

Enable User management

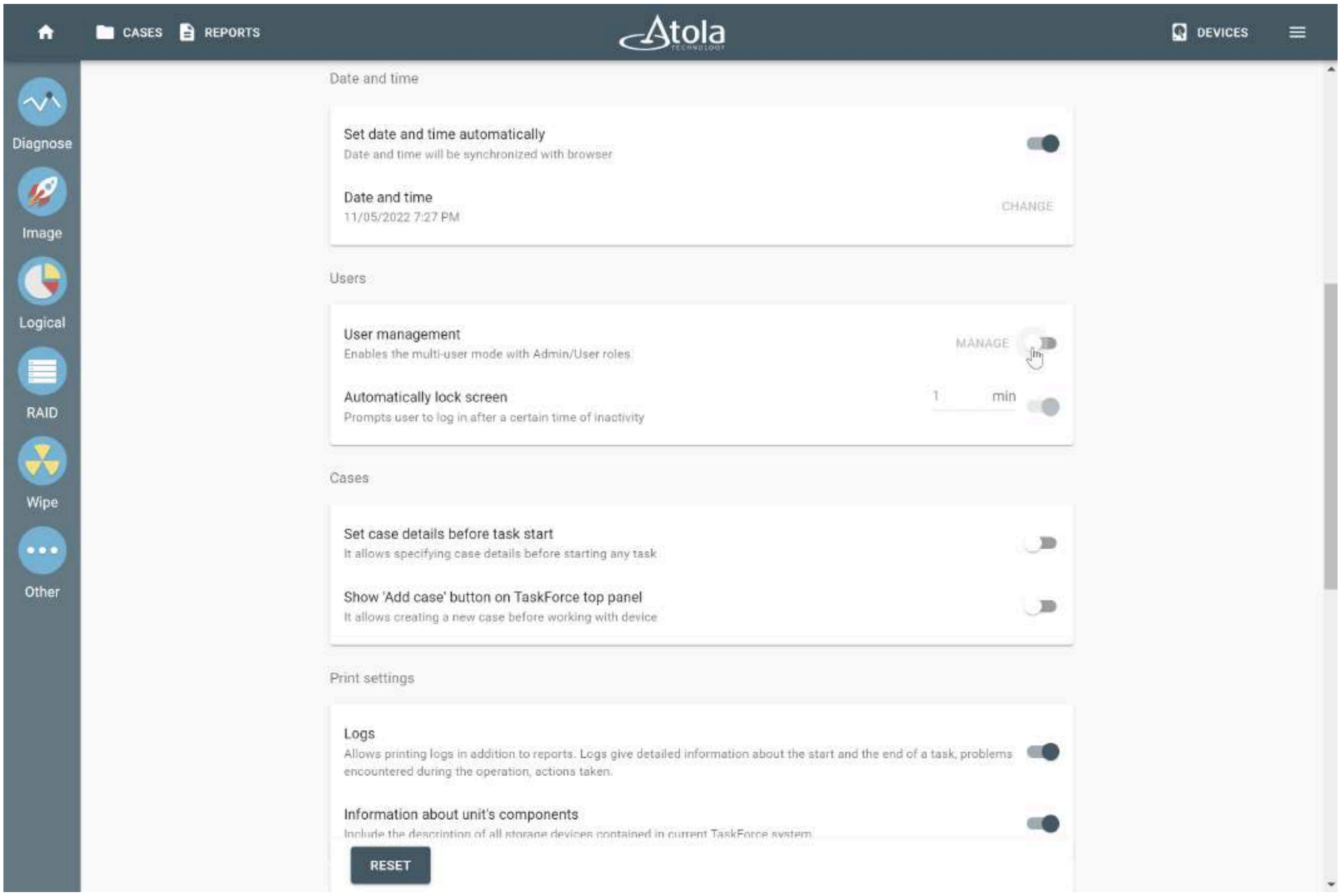
The first profile, what you create after enabling User management, has an *Admin* role.

To enable the multi-user mode in Atola TaskForce, do the following steps:

1. In the Atola TaskForce window, go to **Menu** > **Settings**.
2. In the **Users** section, toggle **User management**.
3. Enter the username and password for the administrator’s profile, and then click **Create**.

Now you can add, edit, or delete other user profiles.

> After you enable User management, Express mode is disabled due to security reasons.



Date and time

Set date and time automatically
Date and time will be synchronized with browser

Date and time
11/05/2022 7:27 PM

Users

User management
Enables the multi-user mode with Admin/User roles

Automatically lock screen
Prompts user to log in after a certain time of inactivity
1 min

Cases

Set case details before task start
It allows specifying case details before starting any task

Show 'Add case' button on TaskForce top panel
It allows creating a new case before working with device

Print settings

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

Information about unit's components
Include the description of all storage devices contained in current TaskForce system

User management toggle in the Users section of the Settings menu.

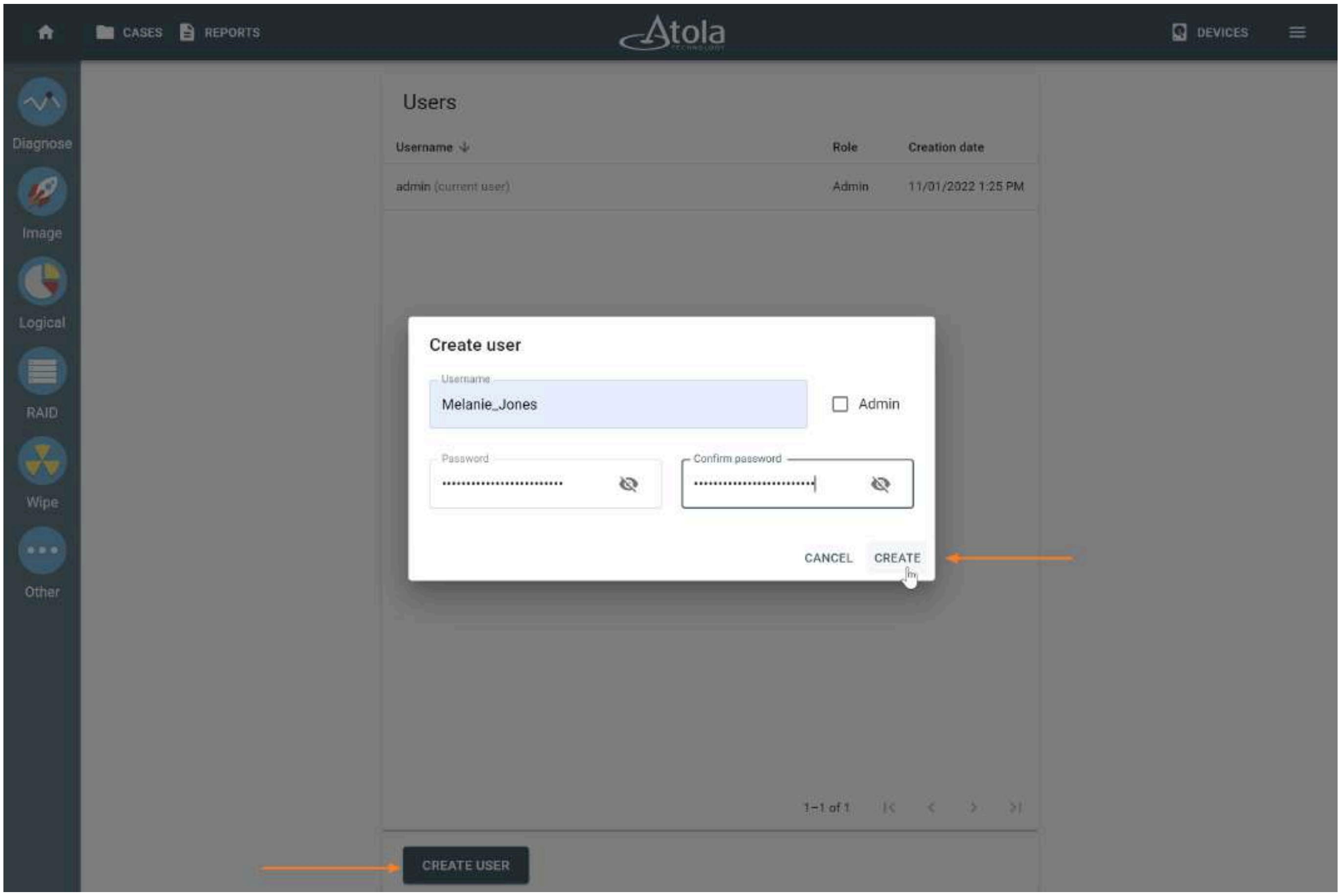
Add, edit, or delete users

Only *Admin* can add, edit, or delete other user profiles with either *Admin* or *User* role.

Add a user

To add a user, do the next steps:

1. Log in to a profile that has the *Admin* role.
2. In the Atola TaskForce window, go to **Menu** > **Settings**.
3. In the **Users** section, click **Manage**.
4. On the **Users page**, click **Create user**.
5. Enter the username and password for a user.
   Optional: To grant this user an *Admin* role, select **Admin** checkbox.
6. Click **Create**.



Users

Username	Role	Creation date
admin (current user)	Admin	11/01/2022 1:25 PM

Create user

Username: Melanie_Jones

□ Admin

Password: ••••••••••••••••••••••••••

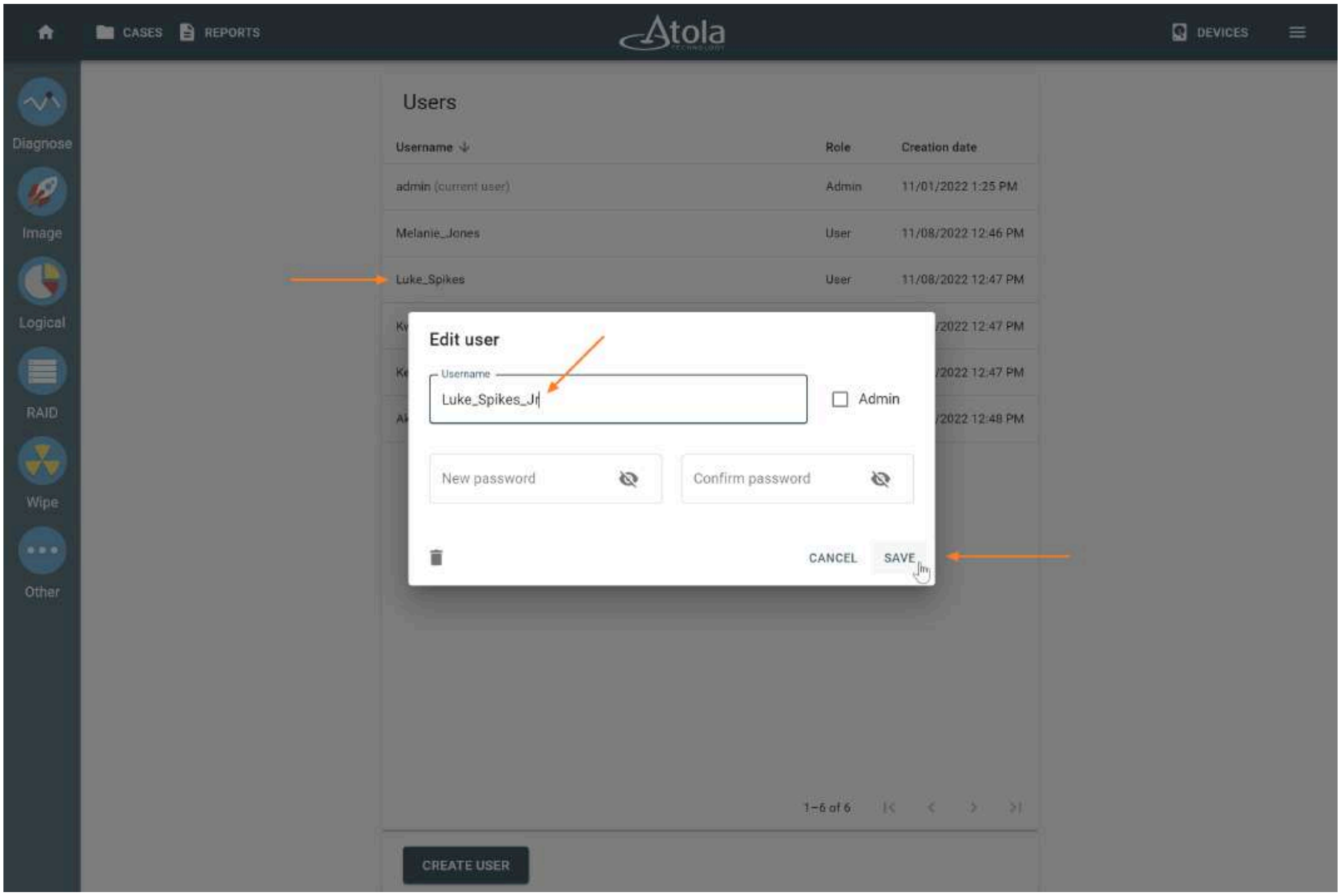
Confirm password: ••••••••••••••••••••••••••

The Create user button and dialog.

Edit a user

To edit a user, do the following:

1. Log in to a profile that has the *Admin* role.
2. In the Atola TaskForce window, go to **Menu** > **Settings**.
3. In the **Users** section, click **Manage**.
4. On the **Users page**, select a user you want to edit.
5. In the **Edit user** dialog, edit the username.
   Optional: To grant this user an *Admin* role, select **Admin** checkbox.
6. Click **Save**.



Users

Username	Role	Creation date
admin (current user)	Admin	11/01/2022 1:25 PM
Melanie_Jones	User	11/08/2022 12:46 PM
Luke_Spikes	User	11/08/2022 12:47 PM
Ky		/2022 12:47 PM
Ke		/2022 12:47 PM
Al		/2022 12:48 PM

Username: Luke_Spikes_Jr

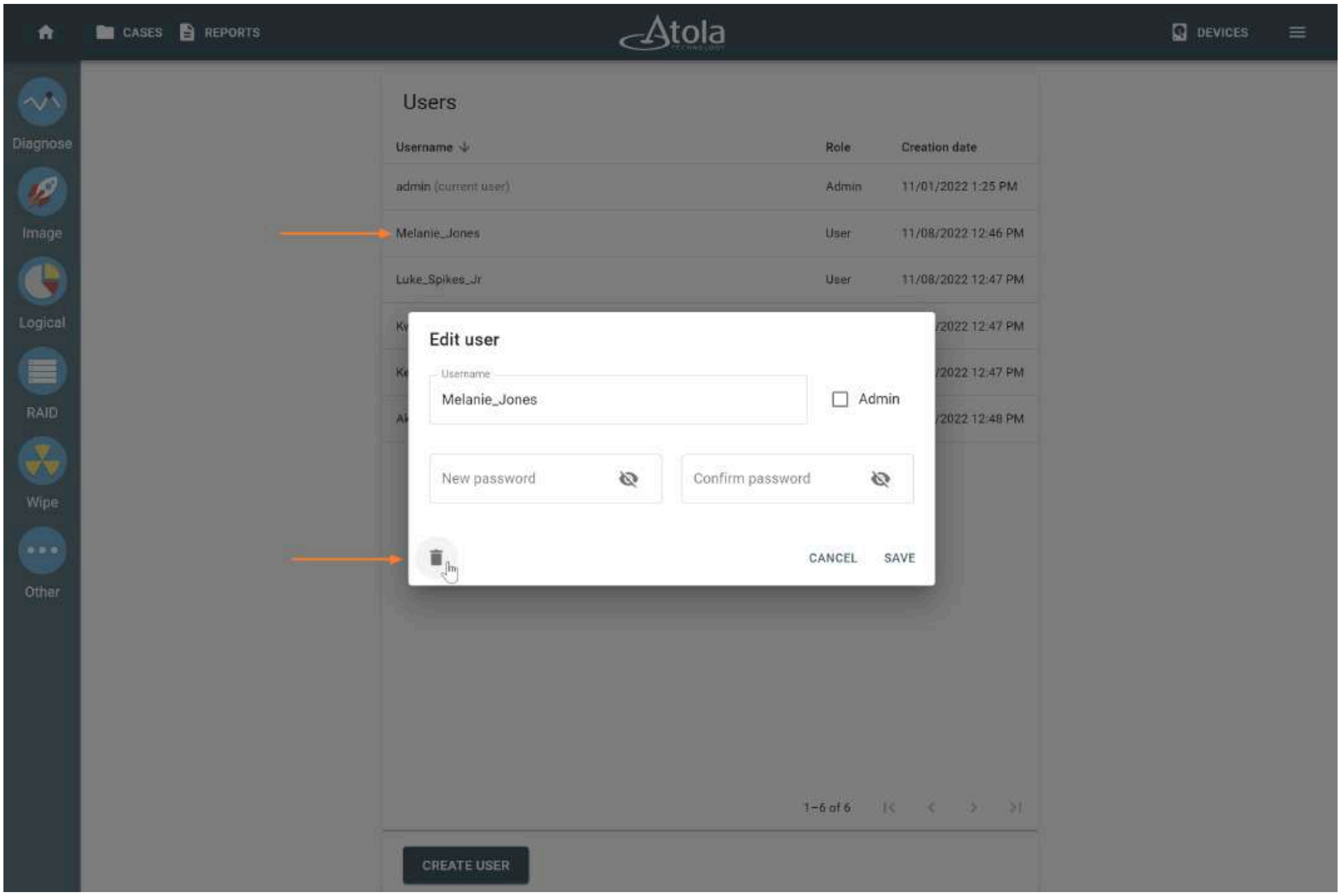
The Edit user dialog.

Delete a user

After deleting a user, you can still access their cases and reports under a profile with the *Admin* role.

To delete a user, do the following steps:

1. Log in to a profile that has the *Admin* role.
2. In the Atola TaskForce window, go to **Menu** > **Settings**.
3. In the **Users** section, click **Manage**.
4. On the **Users page**, select a user you want to delete.
5. In the **Edit user** dialog, click the **Delete** icon.
6. In the confirmation dialog, enter *YES*, and then click **Delete**.



Users

Username ↓	Role	Creation date
admin (current user)	Admin	11/01/2022 1:25 PM
Melanie_Jones	User	11/08/2022 12:46 PM
Luke_Spikes_Jr	User	11/08/2022 12:47 PM
Ky		/2022 12:47 PM
Ke		/2022 12:47 PM
Al		/2022 12:48 PM

Edit user

Username: Melanie_Jones

□ Admin

New password

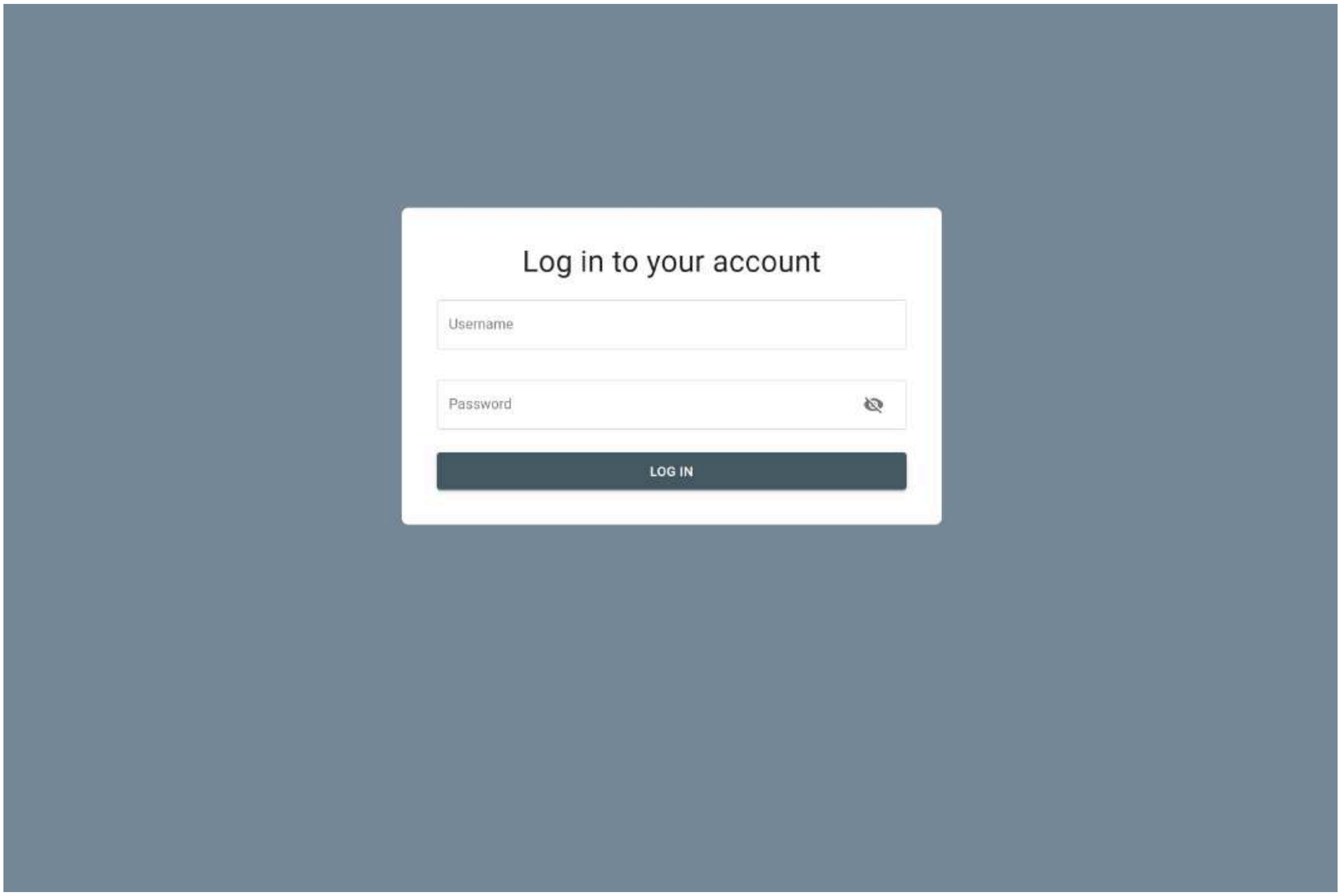
Confirm password

The Delete icon in the Edit user dialog.

Log in and log out

To log out, click **Menu** > **Log out**. Atola TaskForce locks itself and prompts you to enter a username and password. All the processes you started before logging out are still running in the background.

To log in, enter your username and password, and then click **Log in**. Atola TaskForce unlocks itself and shows its Home screen.



Log in to your account

Username

Password

LOG IN

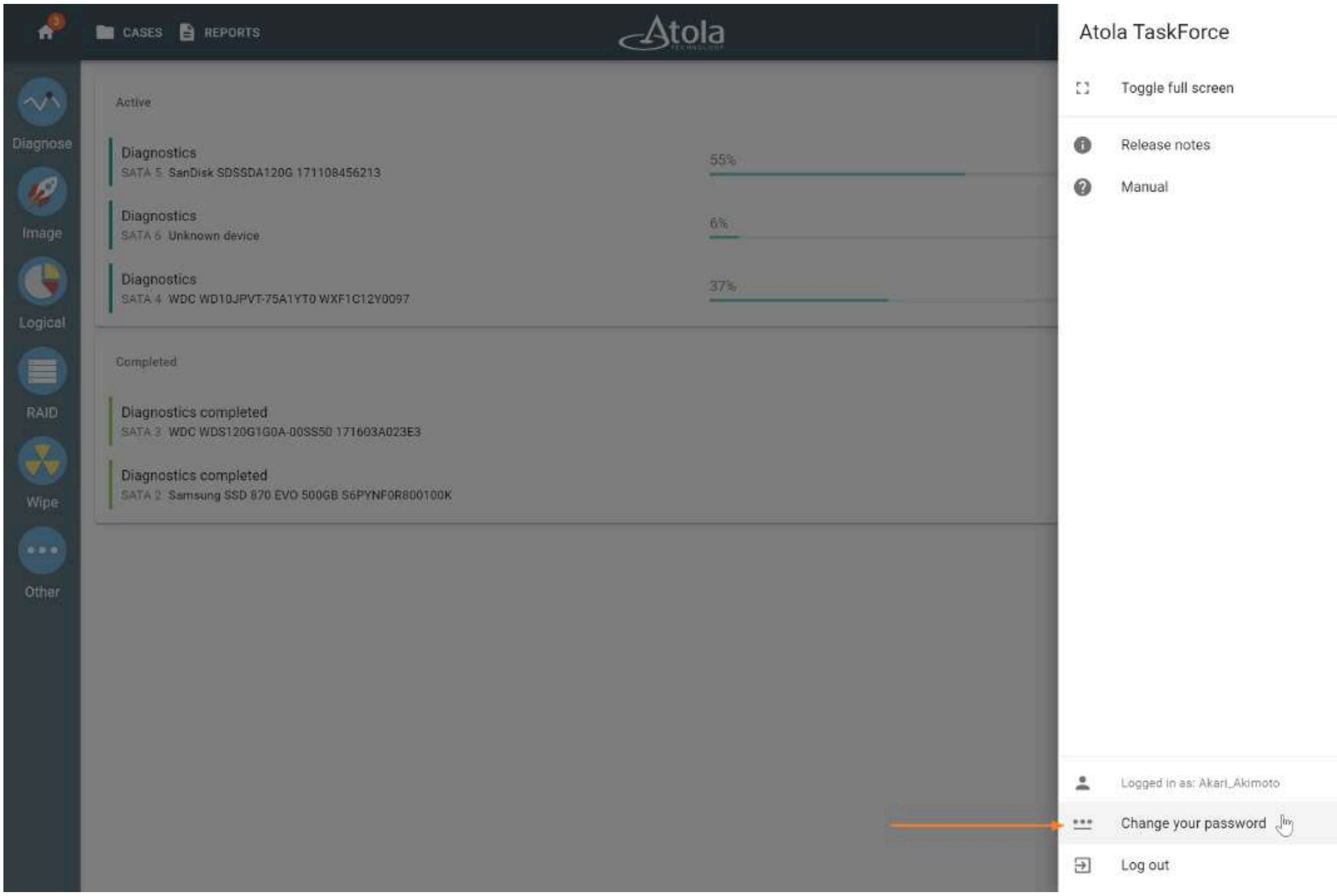
Atola TaskForce is locked and prompts you to enter a username and password.

Change the password

As a *User*, you can change only your password. As an *Admin*, you can change other users' passwords as well.

Change the password for your profile

To change the password for your profile, go to **Menu** > **Change your password**, enter your current and new passwords and click **Save**.



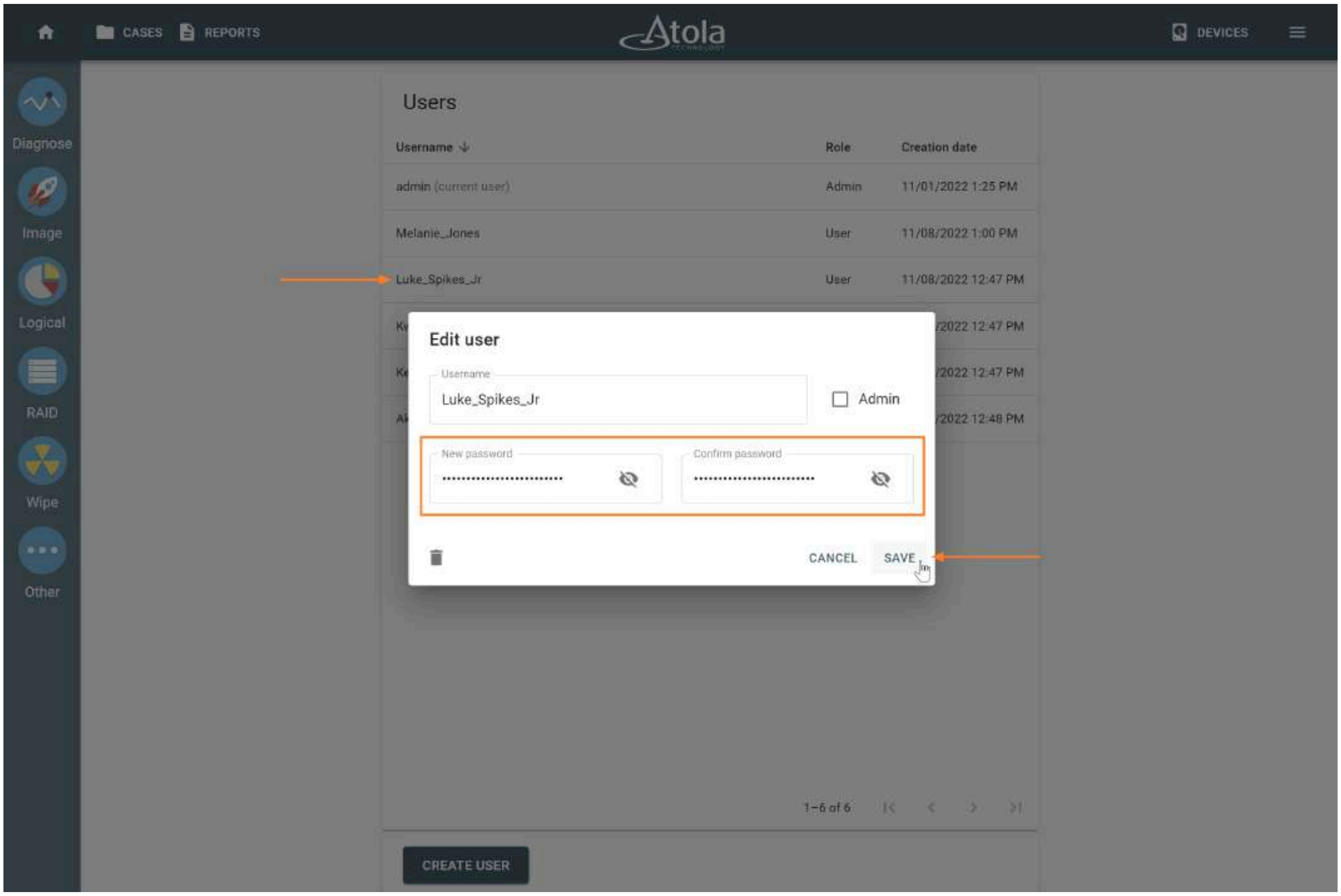
Change your password command in the Menu.

Change the password for another user as an administrator

To change the password for another user, do the following:

1. Log in to a profile that has the *Admin* role.
2. In the Atola TaskForce window, go to **Menu** > **Settings**.
3. In the **Users** section, click **Manage**.
4. On the **Users page**, select a user you want to change the password for.
5. In the **Edit user** dialog, enter a new password, confirm the password, and then click **Save**.

If you forgot or don’t know the password for an administrator profile on your TaskForce, contact Atola Support.



Users

Username ↓	Role	Creation date
admin (current user)	Admin	11/01/2022 1:25 PM
Melanie_Jones	User	11/08/2022 1:00 PM
Luke_Spikes_Jr	User	11/08/2022 12:47 PM
Ky		/2022 12:47 PM
Ke		/2022 12:47 PM
Ak		/2022 12:48 PM

Edit user

Username: Luke_Spikes_Jr

□ Admin

New password: ••••••••••••••••••••••••••

Confirm password: ••••••••••••••••••••••••••

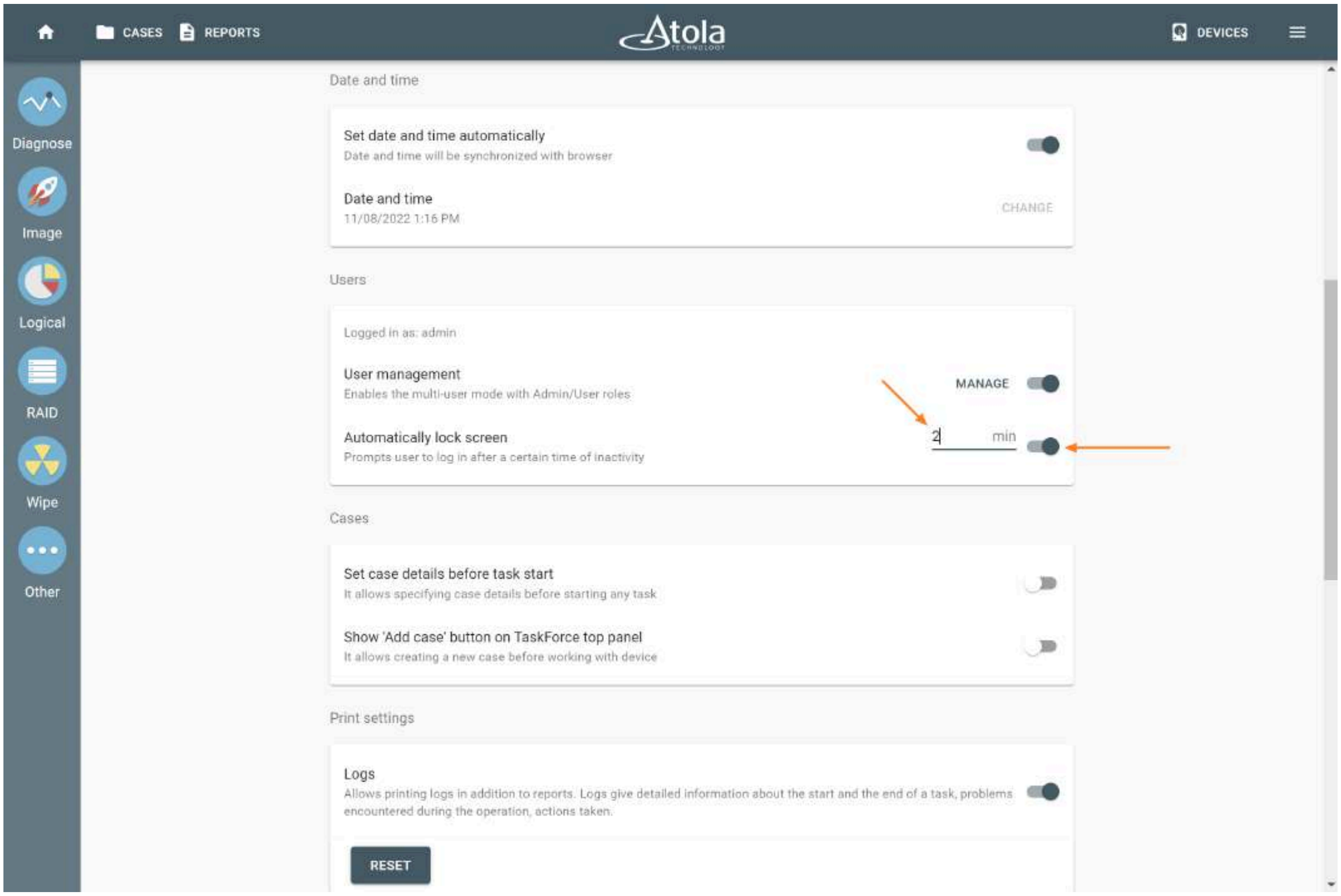
CANCEL SAVE

Changing a user password in the Edit user dialog on the Users page.

Automatically lock screen

As an Admin, you can set up Atola TaskForce to automatically lock its screen after a certain time of inactivity. To enable this feature, log in to a profile with the Admin role and do the next steps:

1. Go to **Menu** > **Settings**.
2. In the **Users** section, toggle **Automatically lock screen**.
3. Enter a time interval in minutes you want TaskForce to wait before automatically locking in.



Date and time

Set date and time automatically
Date and time will be synchronized with browser

Date and time
11/08/2022 1:16 PM

Users

Logged in as: admin

User management
Enables the multi-user mode with Admin/User roles

Automatically lock screen — 2 min
Prompts user to log in after a certain time of inactivity

Cases

Set case details before task start
It allows specifying case details before starting any task

Show 'Add case' button on TaskForce top panel
It allows creating a new case before working with device

Print settings

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

The Automatically lock screen toggle in the Users section of the Settings menu.

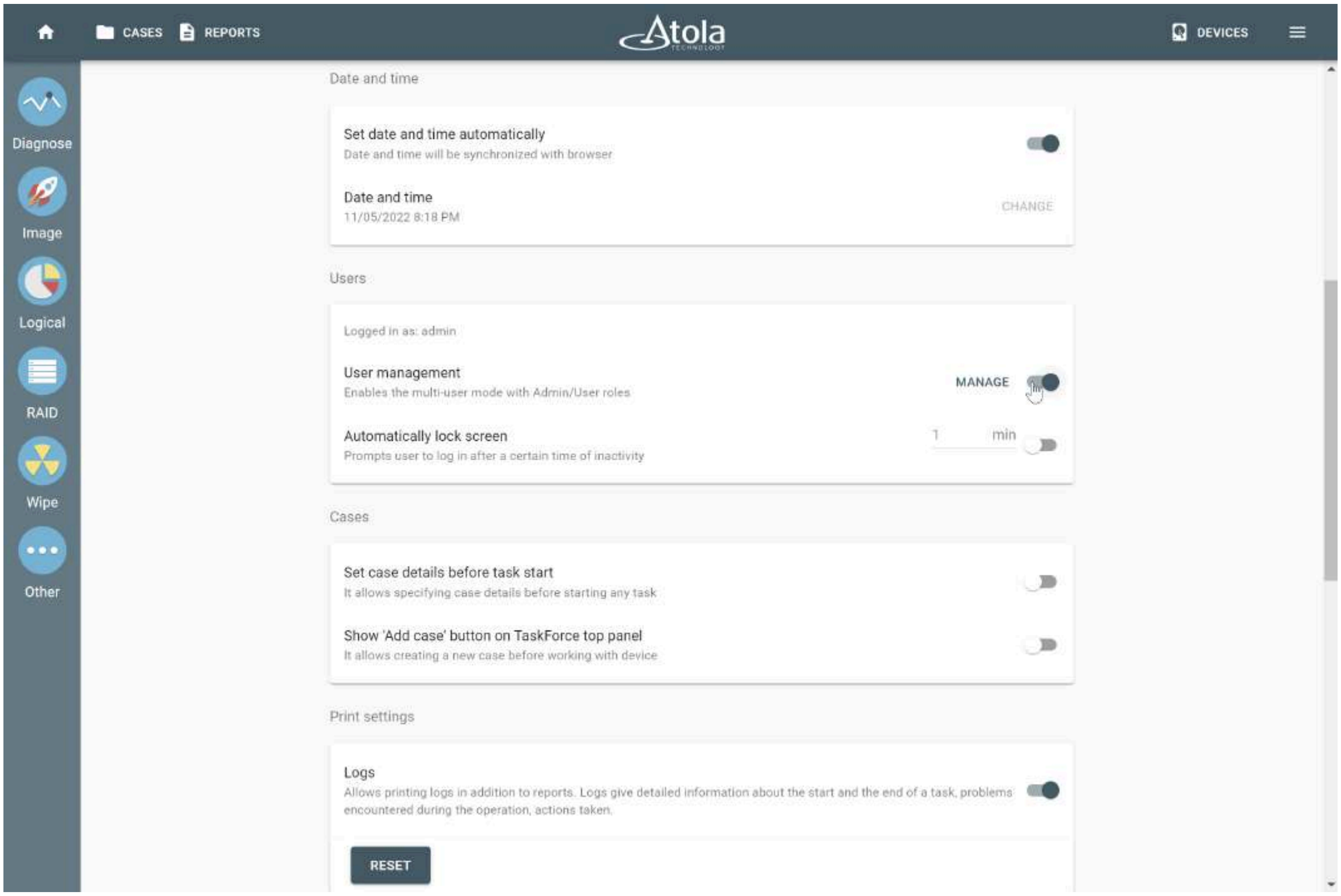
Disable User management and password protection

As an *Admin*, you can disable user management and password protection for your Atola TaskForce.

> If you disable User management, cases and reports will become available to all users of that TaskForce unit.

To disable user management and password protection, do the following steps:

1. Log in to a profile that has the Admin role.
2. Go to **Menu** > **Settings**.
3. In the **Users** section, toggle off **User management**.



Date and time

Set date and time automatically
Date and time will be synchronized with browser

Date and time
11/05/2022 8:18 PM
CHANGE

Users

Logged in as: admin

User management
Enables the multi-user mode with Admin/User roles
MANAGE

Automatically lock screen
Prompts user to log in after a certain time of inactivity
1 min

Cases

Set case details before task start
It allows specifying case details before starting any task

Show 'Add case' button on TaskForce top panel
It allows creating a new case before working with device

Print settings

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

RESET

Toggling off User management.

Maximize 10Gb network throughput

If you image evidence drives to a file on a server or a computer using a local network and want to achieve the best imaging speeds, maximize your network throughput by following these tips.

Set up 10Gb Ethernet network

Atola TaskForce 2 is equipped with two 10Gb Ethernet ports. To fully use this potential and achieve the best imaging speeds, every node in your local network between the TaskForce unit and your computer or server need to support 10Gb connection as well.

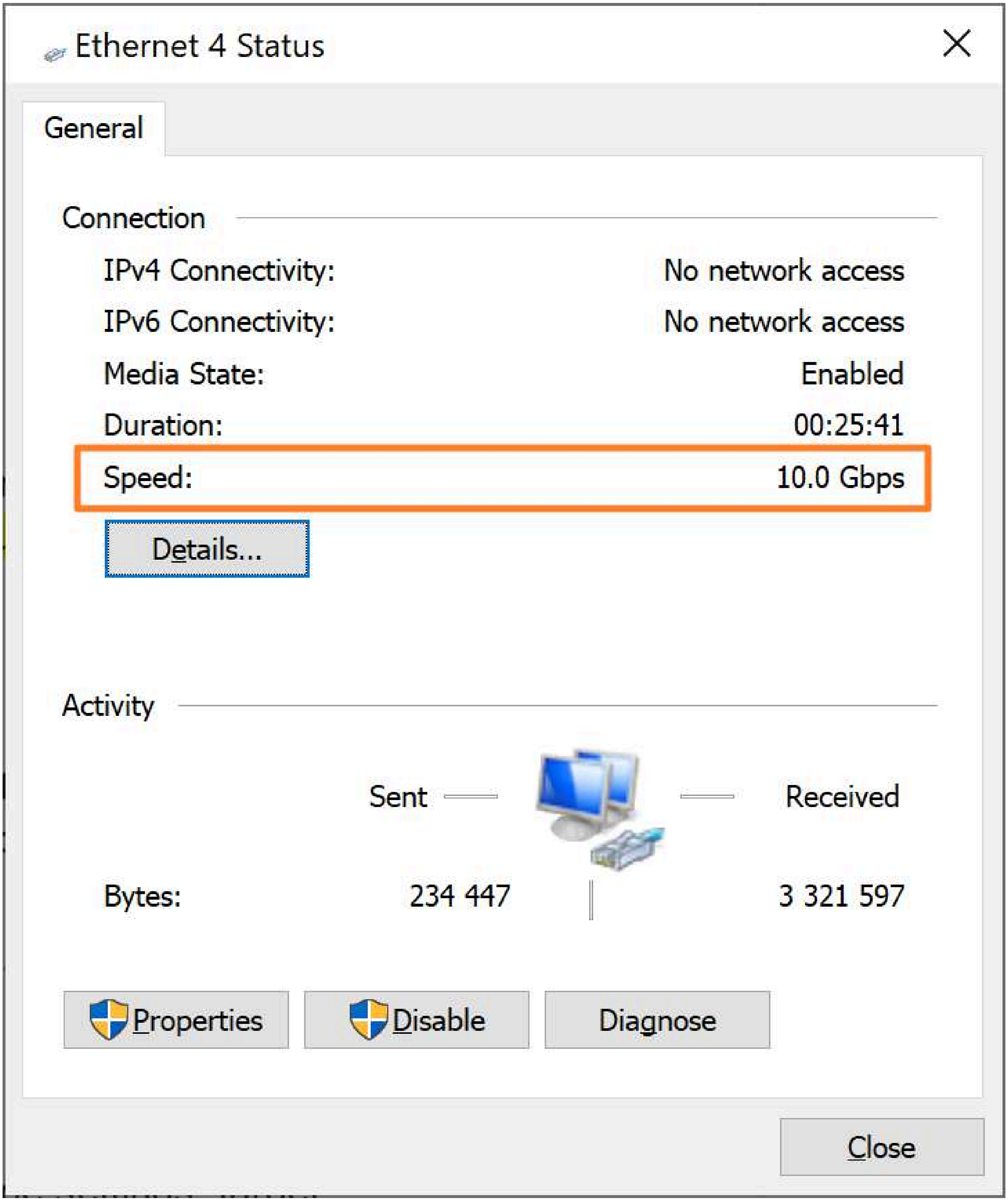
Use 10Gb network adapter

Make sure that a network adapter on your server or your computer supports a 10Gb connection:

- Check vendor specifications for your network adapter.
- Check the network adapter speed in your OS settings.

How to check Ethernet connection speed on Windows 10 and Windows 11

1. Go to **Control panel** > **Network & Internet** > **Network and Sharing Center**.
2. In the **View your active networks** section, click your Ethernet connection.
3. In the **Status** window, check the connection speed. It must be equal to 10 Gbps.



Ethernet 4 Status

General

Connection

IPv4 Connectivity: No network access

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:25:41

Speed: 10.0 Gbps

Activity

Bytes: Sent 234 447 Received 3 321 597

Use 10Gb network cable

Make sure that the network cable you use to connect your TaskForce unit and your local network nodes supports 10Gb connection. It must have Cat6 (with the length of less than 55 meters), Cat6a, Cat7, Cat7a, or Cat8 marking on it.

Use 10Gb router or switch

If your TaskForce unit is connected through a network router or switch, make sure that every such device in your local network in between TaskForce and the target computer or server supports a 10Gb connection:

- Check vendor specifications for your network router or switch.
- Check that the 10Gb network cable is connected to a 10Gb port on your router or switch.

Enable jumbo frames

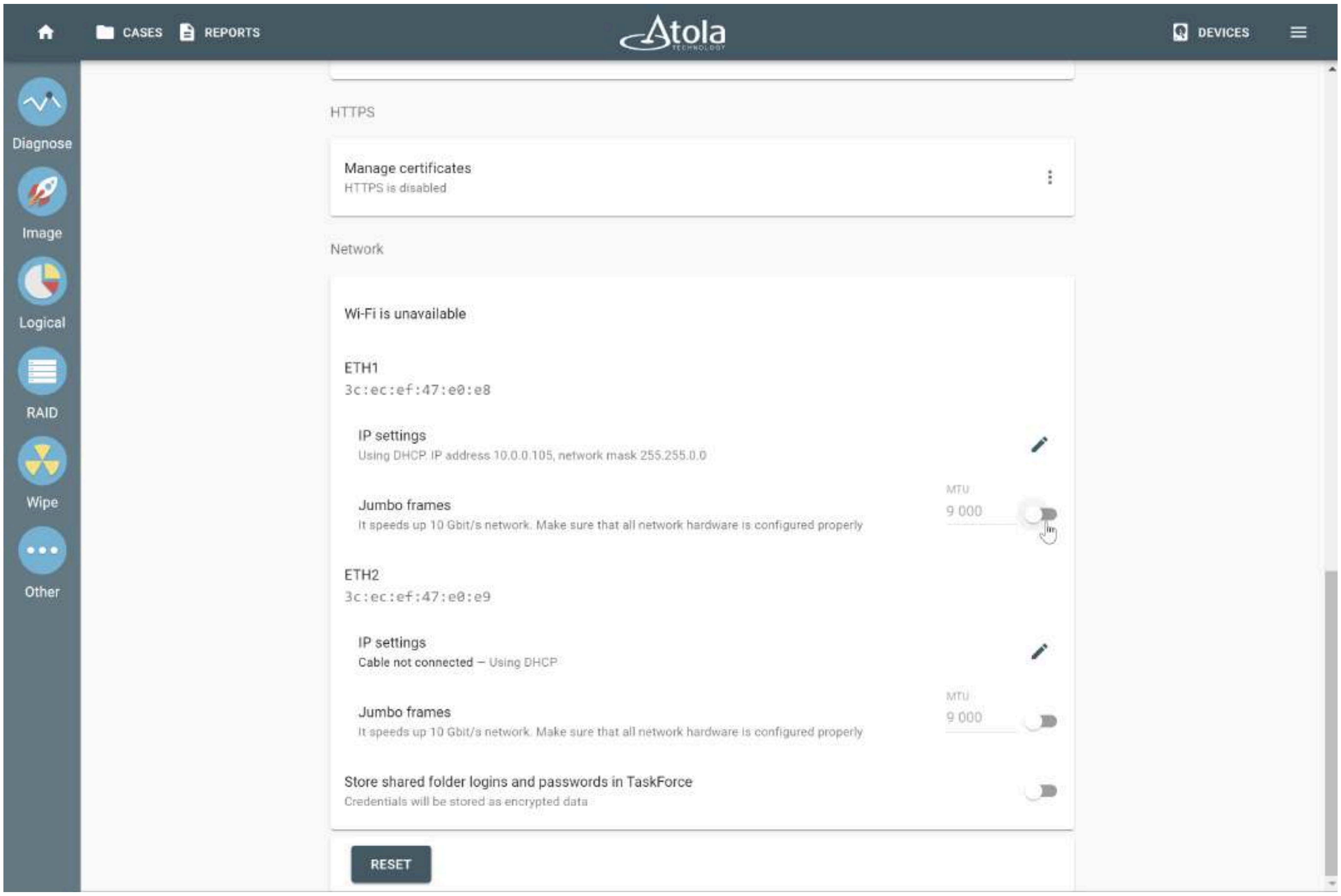
To speed up your 10Gb network, enable jumbo frames on your TaskForce 2, your target device, and every network switch or router in between them.

Jumbo frames increase the efficiency of broadband Ethernet processing because they carry 9000 bytes of payload, which is more than the standard limit of payload.

Enable jumbo frames on TaskForce 2

To enable jumbo frames on your TaskForce unit, do the following:

1. In the Atola TaskForce interface, go to **Menu** > **Settings**.
2. In the **Network** section, toggle Jumbo frames for respective Ethernet port (ETH1 or ETH2). Default MTU (maximum transmission unit) value is set to 9000 bytes, don't change it.



HTTPS

Manage certificates
HTTPS is disabled

Network

Wi-Fi is unavailable

ETH1
3c:ec:ef:47:e0:e8

IP settings
Using DHCP. IP address 10.0.0.105, network mask 255.255.0.0

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU
9 000

ETH2
3c:ec:ef:47:e0:e9

IP settings
Cable not connected — Using DHCP

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU
9 000

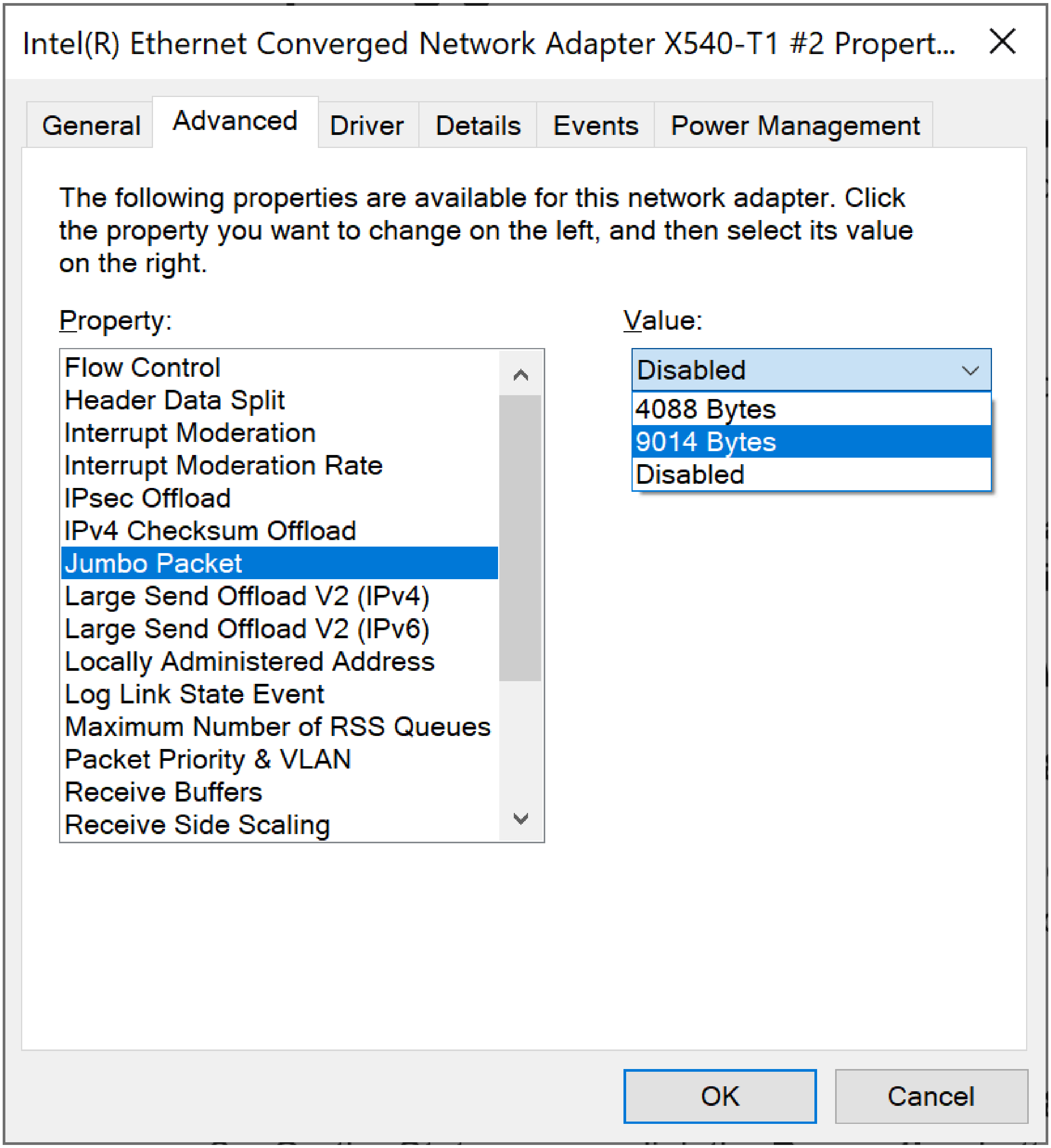
Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data

Jumbo frames toggle on the Settings page in Atola TaskForce.

Enable jumbo frames on a target computer

To enable jumbo frames for 10Gb network adapter on a target computer running Windows 10 or Windows 11, do the next steps:

1. Go to **Control panel** > **Network & Internet** > **Network and Sharing Center**.
2. In the **View your active networks** section, click on your Ethernet connection.
3. In the **Status** window, click **Properties**.
4. In the **Properties** window, click **Configure** and go to the **Advanced** tab.
5. On the **Advanced** tab, select **Jumbo Packet** and change its **Value** to 9014 Bytes.
6. Click **OK**.



Intel(R) Ethernet Converged Network Adapter X540-T1 #2 Propert...

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- Flow Control
- Header Data Split
- Interrupt Moderation
- Interrupt Moderation Rate
- IPsec Offload
- IPv4 Checksum Offload
- Jumbo Packet
- Large Send Offload V2 (IPv4)
- Large Send Offload V2 (IPv6)
- Locally Administered Address
- Log Link State Event
- Maximum Number of RSS Queues
- Packet Priority & VLAN
- Receive Buffers
- Receive Side Scaling

Value:

Disabled

- 4088 Bytes
- 9014 Bytes
- Disabled

Enable jumbo frames on a network router or switch

Jumbo frames need to be enabled on network routers or switches, which connect your TaskForce unit with your target computer or server.

Many 10Gb routers and switches support jumbo frames by default.

For specifications and instructions, refer to a router or switch user guide provided by its manufacturer.

Use Samba version 3.0 or later

Samba is a free software that provides fast shared access to files and printers for all network clients using the SMB/CIFS protocol.

We recommend using Samba version 3.0 or later to speed up the imaging to the files on network-connected drives.

For guidance, refer to the Samba installation guide.

Update OS and drivers

Install the latest OS and driver updates.

Due to various software issues, the local network speed can be lower than expected if the operating system and network drivers are outdated.

Check server use quota

Sometimes, a network administrator can create quotas, which limit server space or throughput for end users.

Check if there is an opportunity to change or lift these quotas to achieve maximum data throughput during imaging.

Use faster target drives

To achieve higher imaging speeds, we recommend using faster destination drives with reading and writing speeds of no less than 600 MB per second.

If you’re using a RAID array as a storage, consider choosing RAID types with faster reading and writing speed, such as RAID 0 and RAID 5.

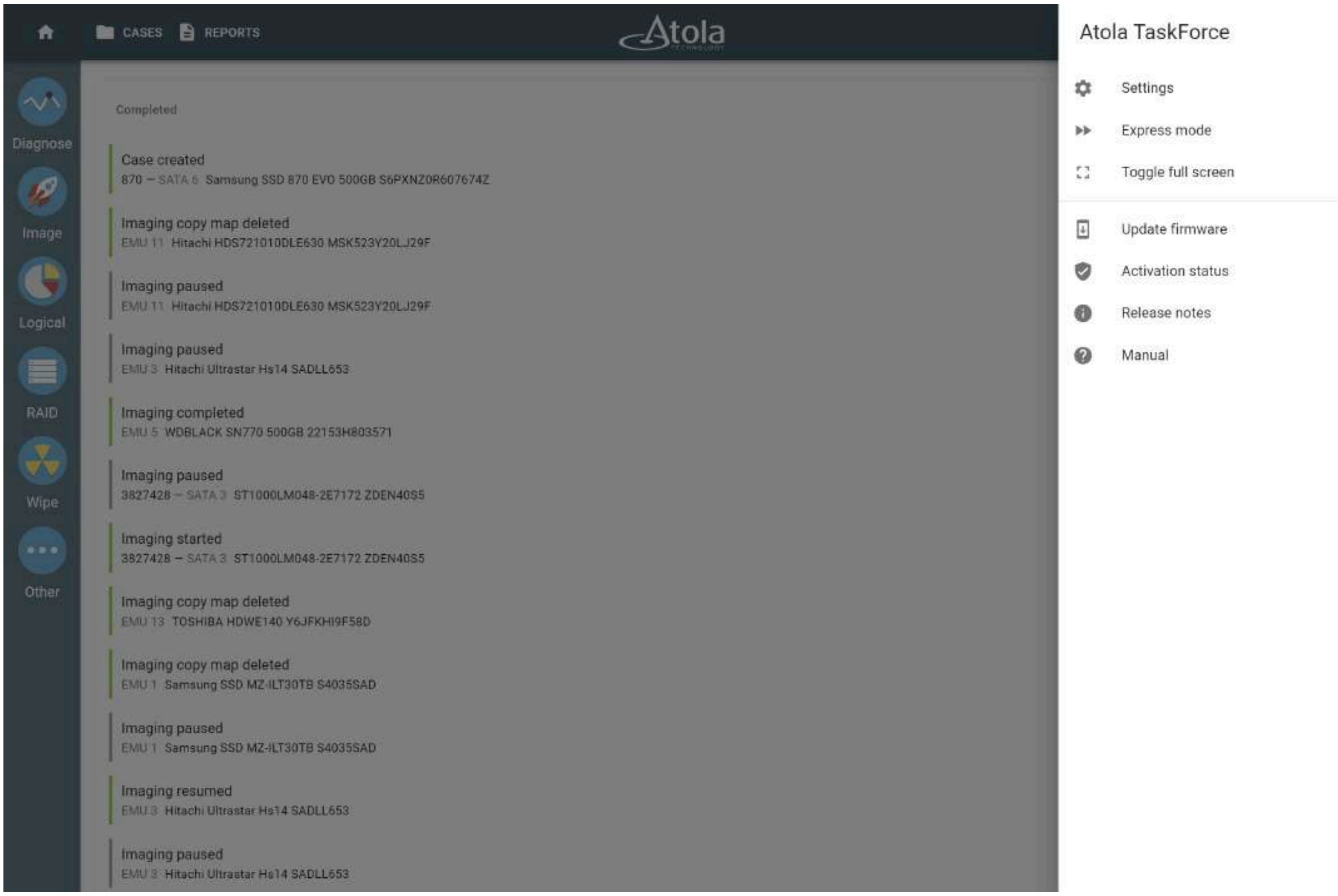
When storing very big files, opt for a large cluster size on your server. The bigger files you want to store, the larger cluster size should be.

Use a static IP address

If you plan to connect TaskForce 2 directly to your computer, we recommend configuring your computer and TaskForce to use a static IP address. Here’s how to do it.

Configure TaskForce 2 for using a static IP address

1. On your computer, open a Chrome browser and in its address bar enter the IP address, displayed on the TaskForce front panel.
2. In the TaskForce interface, go to **Menu** > **Settings**.



Completed

Case created
870 — SATA 6 Samsung SSD 870 EVO 500GB S6PXNZ0R607674Z

Imaging copy map deleted
EMU 11 Hitachi HDS721010DLE630 MSK523Y20LJ29F

Imaging paused
EMU 11 Hitachi HDS721010DLE630 MSK523Y20LJ29F

Imaging paused
EMU 3 Hitachi Ultrastar Hs14 SADLL653

Imaging completed
EMU 5 WDBLACK SN770 500GB 22153H803571

Imaging paused
3827428 — SATA 3 ST1000LM048-2E7172 ZDEN40S5

Imaging started
3827428 — SATA 3 ST1000LM048-2E7172 ZDEN40S5

Imaging copy map deleted
EMU 13 TOSHIBA HDWE140 Y6JFKHI9F58D

Imaging copy map deleted
EMU 1 Samsung SSD MZ-ILT30TB S4035SAD

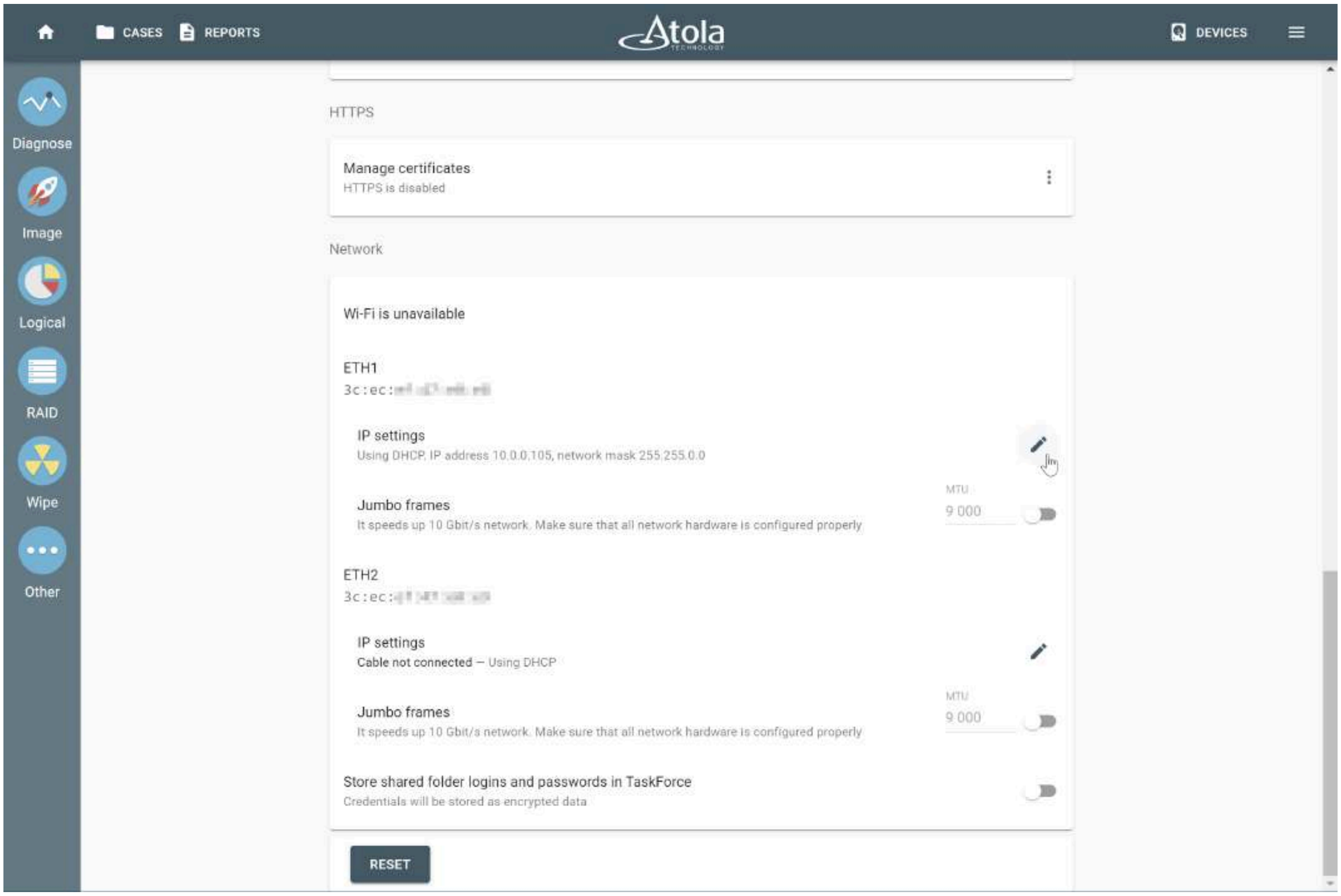
Imaging paused
EMU 1 Samsung SSD MZ-ILT30TB S4035SAD

Imaging resumed
EMU 3 Hitachi Ultrastar Hs14 SADLL653

Imaging paused
EMU 3 Hitachi Ultrastar Hs14 SADLL653

TaskForce system menu.

3. In the **Network** section, find the **IP settings** for the ETH1 or ETH2 port and click the **Edit** icon next to it.



HTTPS

Manage certificates
HTTPS is disabled

Network

Wi-Fi is unavailable

ETH1
3c:ec:[redacted]

IP settings
Using DHCP. IP address 10.0.0.105, network mask 255.255.0.0

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU
9 000

ETH2
3c:ec:[redacted]

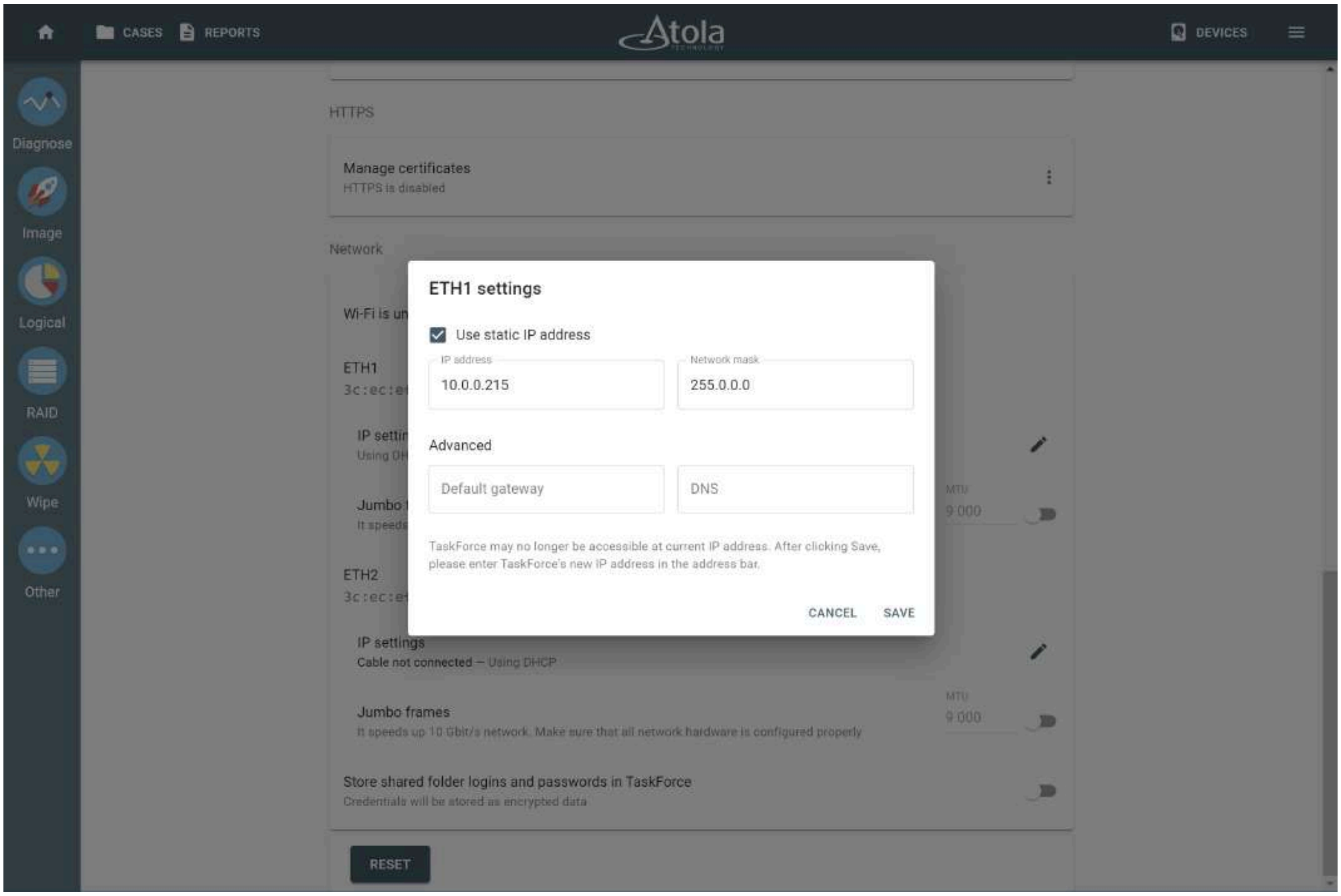
IP settings
Cable not connected — Using DHCP

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU
9 000

Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data

The Edit icon next to IP settings for the ETH 1 port.

4. Enter the following network settings:
   - **IP address:** 10.0.0.XXX, where XXX can be any number from 1 to 254.
     Default static IP addresses of the TaskForce unit are 10.0.0.215 and 192.168.0.215.
     The IP address of your PC's Ethernet card must be different from that of the TaskForce unit.
   - **Network mask:** 255.0.0.0.
     If your PC and the TaskForce unit belong to different subnets, the connection can’t be established.
   - **Default gateway** and **DNS** can be left empty or set to any value.
5. Click **Save**. The new IP address appears on the TaskForce front panel.



HTTPS

Manage certificates
HTTPS is disabled

Network

Wi-Fi is un

ETH1
3c:ec:e

IP settin
Using DH

Jumbo f
It speeds

MTU 9 000

ETH2
3c:ec:e

IP settings
Cable not connected — Using DHCP

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly

MTU 9 000

Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data

ETH1 settings

☑ Use static IP address

IP address: 10.0.0.215

Network mask: 255.0.0.0

Advanced

Default gateway

DNS

TaskForce may no longer be accessible at current IP address. After clicking Save, please enter TaskForce's new IP address in the address bar.

Network settings for the ETH1 port.

Connect TaskForce 2 directly to your computer

To use a static IP address, connect your computer to the ETH1 or ETH2 port of TaskForce 2 with an Ethernet network cable.

If your computer has no Ethernet port, you can use the USB-to-Ethernet adapter (not included in the package). Connect it to your computer before configuring a network.

Configure your computer for using a static IP address

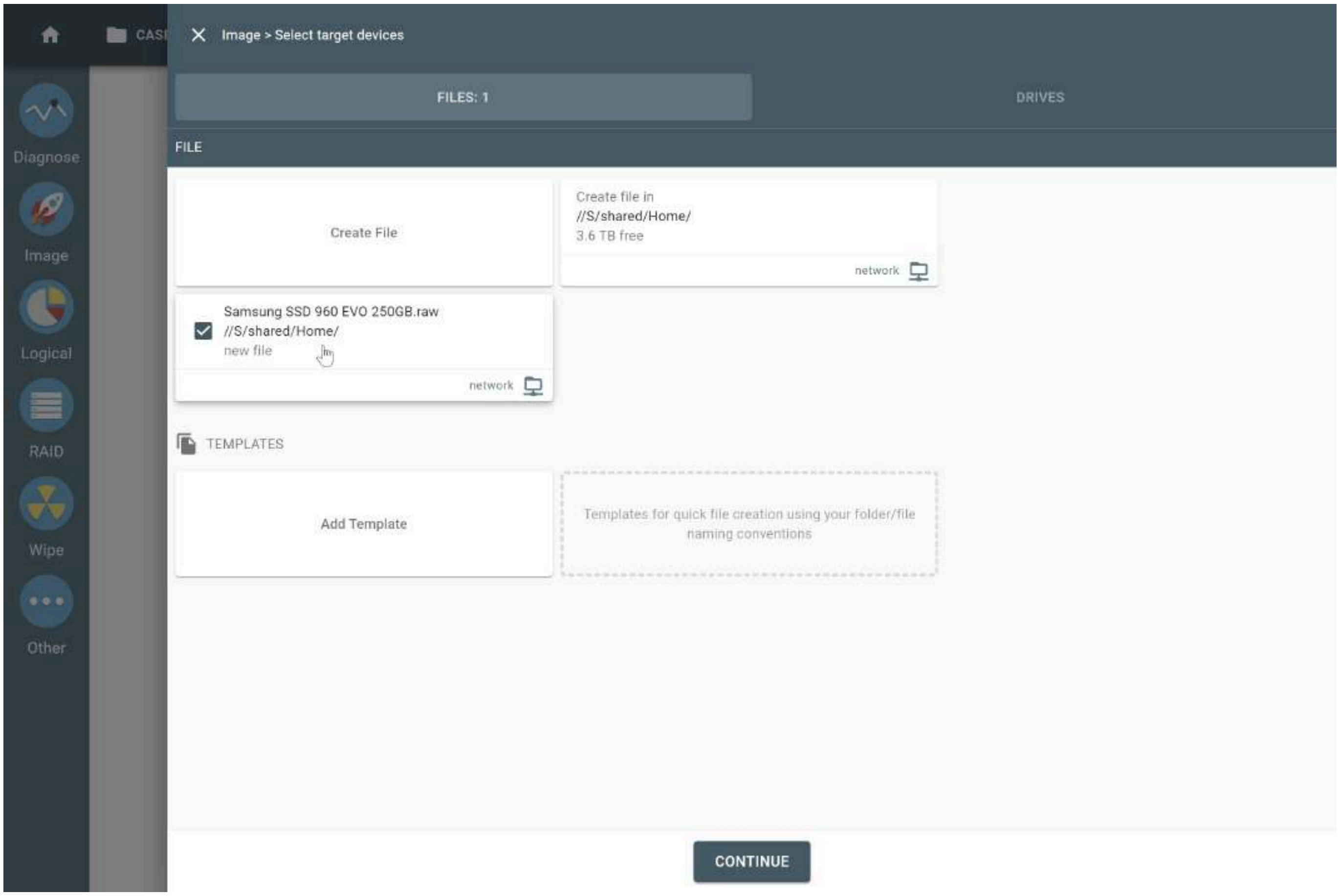
1. In Windows, open **Network Connections**: press *Win+R*, enter *ncpa.cpl* and click **OK**.
2. Right-click your Ethernet adapter, and then select **Properties**.
3. Select **Internet Protocol Version 4**, and then click **Properties**.
4. Enter the following network settings:
    - **IP address:** 10.0.0.*XXX*, where *XXX* can be any number from 1 to 254 except for 215.
      Default static IP addresses of the TaskForce unit are 10.0.0.215 and 192.168.0.215.
      The IP address of your PC's Ethernet card must be different from that of the TaskForce unit.
    - **Network mask**: 255.0.0.0.
      If your PC and the TaskForce unit belong to different subnets, the connection can't be established.
    - **Gateway** and **DNS server** can be left empty or set to any value.
5. Click **OK**.

Jumbo frames for fast imaging to server

In TaskForce 2, Jumbo frames are activated by default to ensure maximum data transfer rates when imaging to a file on your server.

However, if Jumbo frames have been disabled, it is easy to enable them again and experience substantial boost to the speed of imaging!

First, create a file on the server, to which you will be imaging.



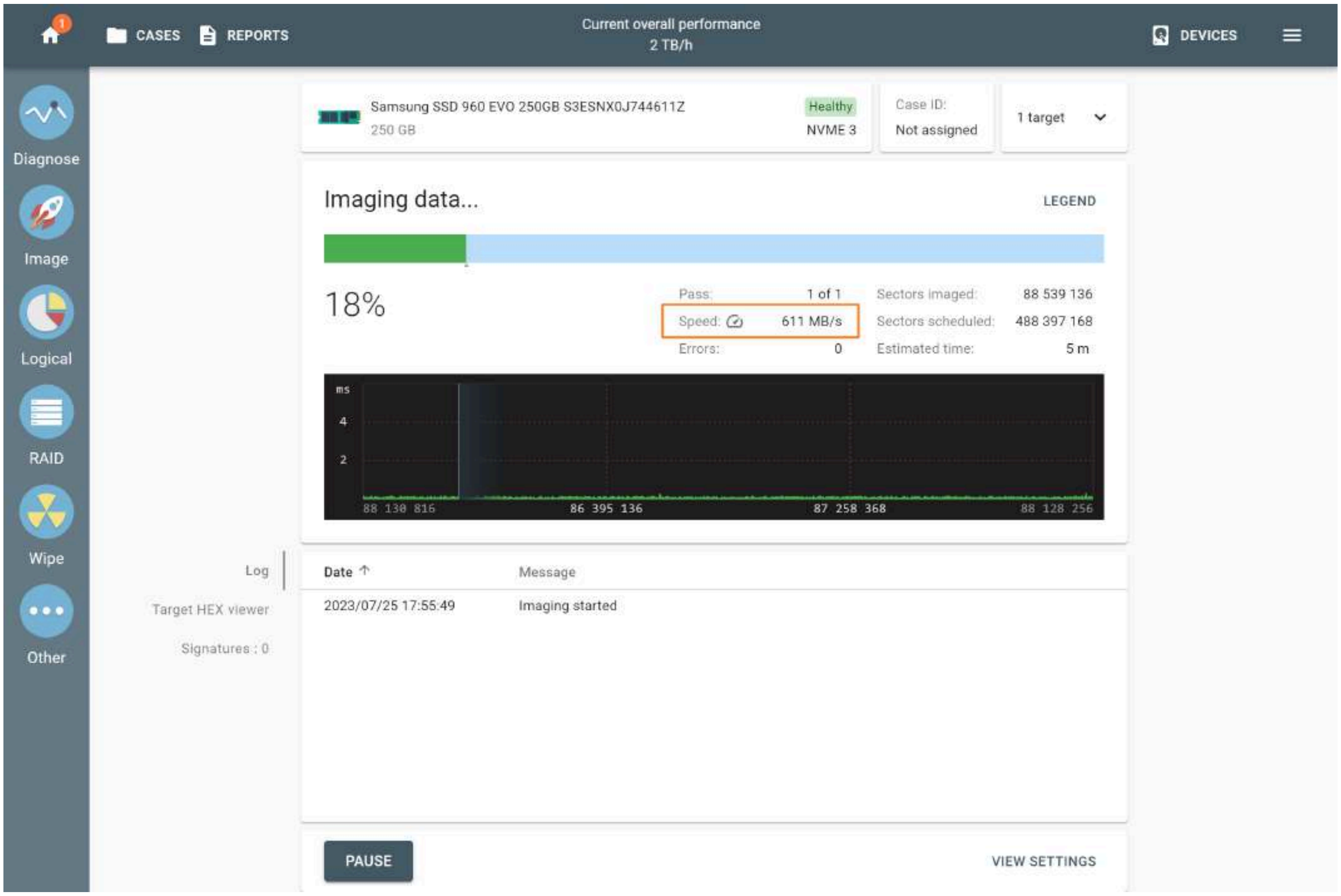
Create file in
//S/shared/Home/
3.6 TB free

☑ Samsung SSD 960 EVO 250GB.raw
//S/shared/Home/
new file

Templates for quick file creation using your folder/file naming conventions

Creating a target file.

When you start to image to your server with Jumbo frame disabled, the data transfer speed will not exceed 700 MB/s. The actual speed will also depend on the configuration and current traffic in the network.



Samsung SSD 960 EVO 250GB S3ESNX0J744611Z
250 GB
Healthy
NVME 3

Case ID:
Not assigned

1 target

Imaging data...

18%

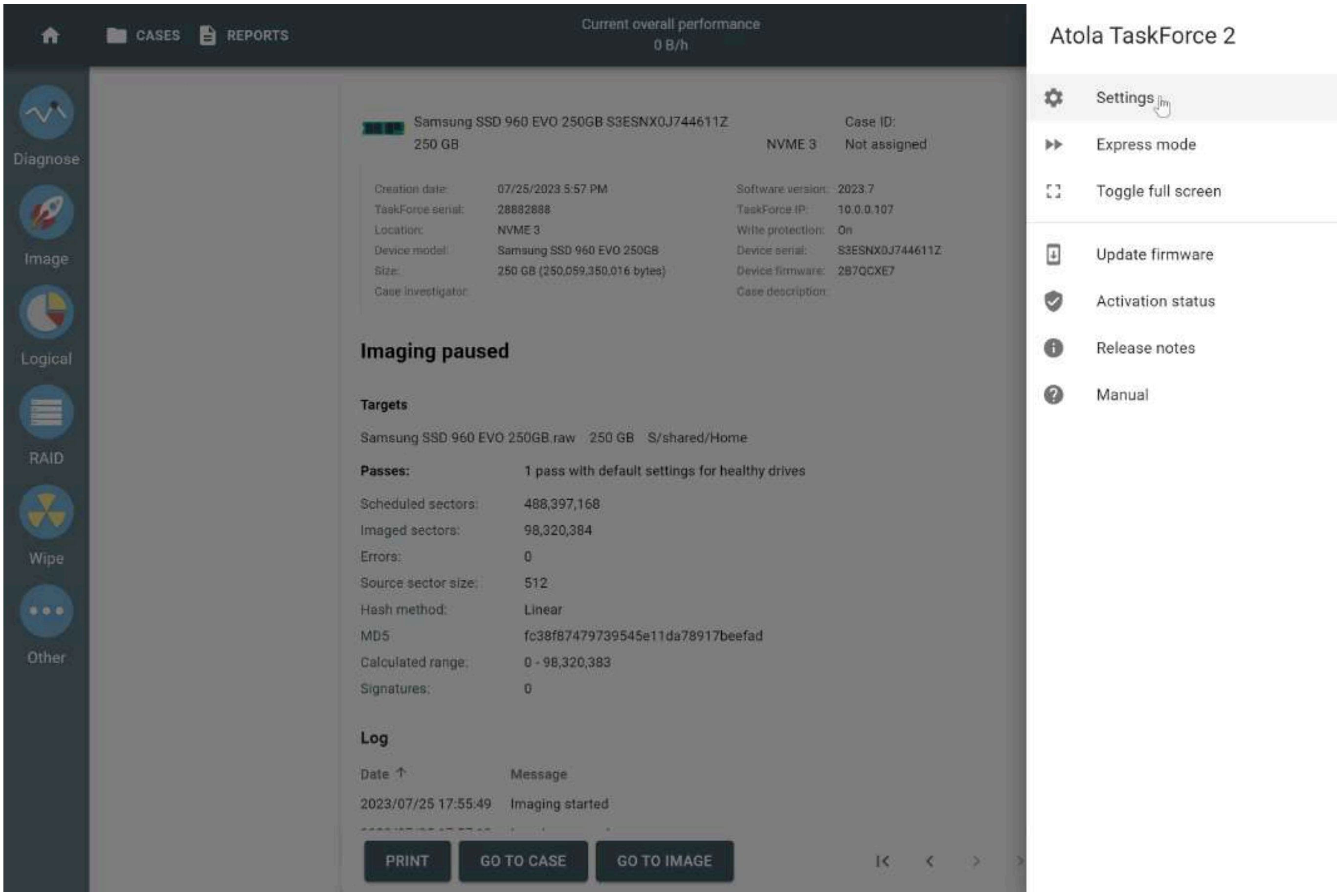
Pass: 1 of 1
Speed: 611 MB/s
Errors: 0
Sectors imaged: 88 539 136
Sectors scheduled: 488 397 168
Estimated time: 5 m

Date	Message
2023/07/25 17:55:49	Imaging started

Speed of imaging without Jumbo frames.

To boost the speed:

1. Pause the imaging session.
2. Go to the **Menu** at the top right.
3. Click **Settings**.



Samsung SSD 960 EVO 250GB S3ESNX0J744611Z
250 GB NVME 3
Case ID: Not assigned

Creation date:	07/25/2023 5:57 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.107
Location:	NVME 3	Write protection:	On
Device model:	Samsung SSD 960 EVO 250GB	Device serial:	S3ESNX0J744611Z
Size:	250 GB (250,059,350,016 bytes)	Device firmware:	2B7QCXE7
Case investigator:		Case description:	

Imaging paused

Targets

Samsung SSD 960 EVO 250GB.raw 250 GB S/shared/Home

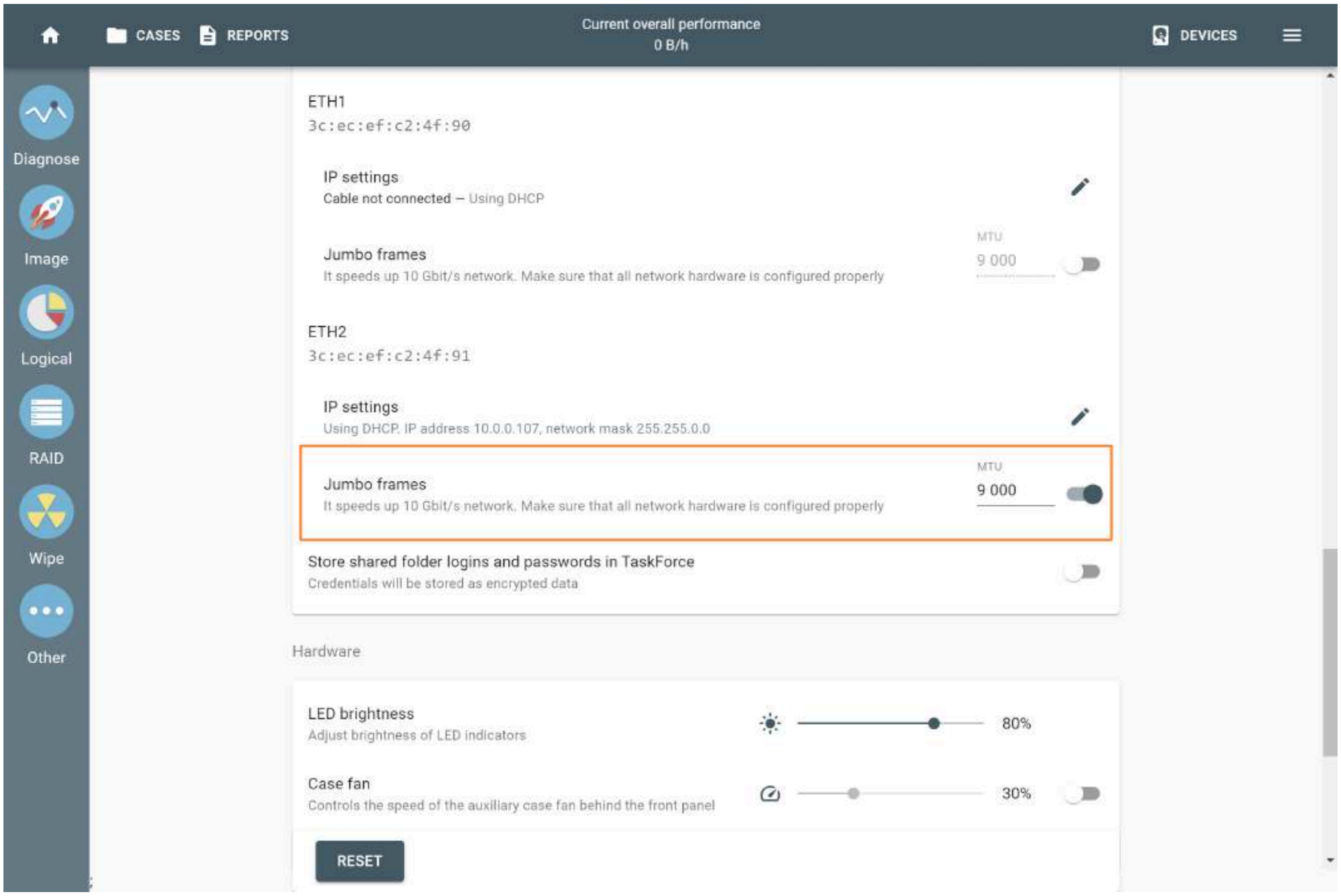
Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	488,397,168
Imaged sectors:	98,320,384
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	fc38f87479739545e11da78917beefad
Calculated range:	0 - 98,320,383
Signatures:	0

Log

Date ↑	Message
2023/07/25 17:55:49	Imaging started

The Settings in the TaskForce Menu.

4. In the **Network** section, enable **Jumbo frames** of the Ethernet port you are using and set **MTU** to 9000.



Current overall performance
0 B/h

ETH1
3c:ec:ef:c2:4f:90

IP settings
Cable not connected — Using DHCP

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU 9 000

ETH2
3c:ec:ef:c2:4f:91

IP settings
Using DHCP. IP address 10.0.0.107, network mask 255.255.0.0

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU 9 000

Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data

Hardware

LED brightness
Adjust brightness of LED indicators
80%

Case fan
Controls the speed of the auxiliary case fan behind the front panel
30%

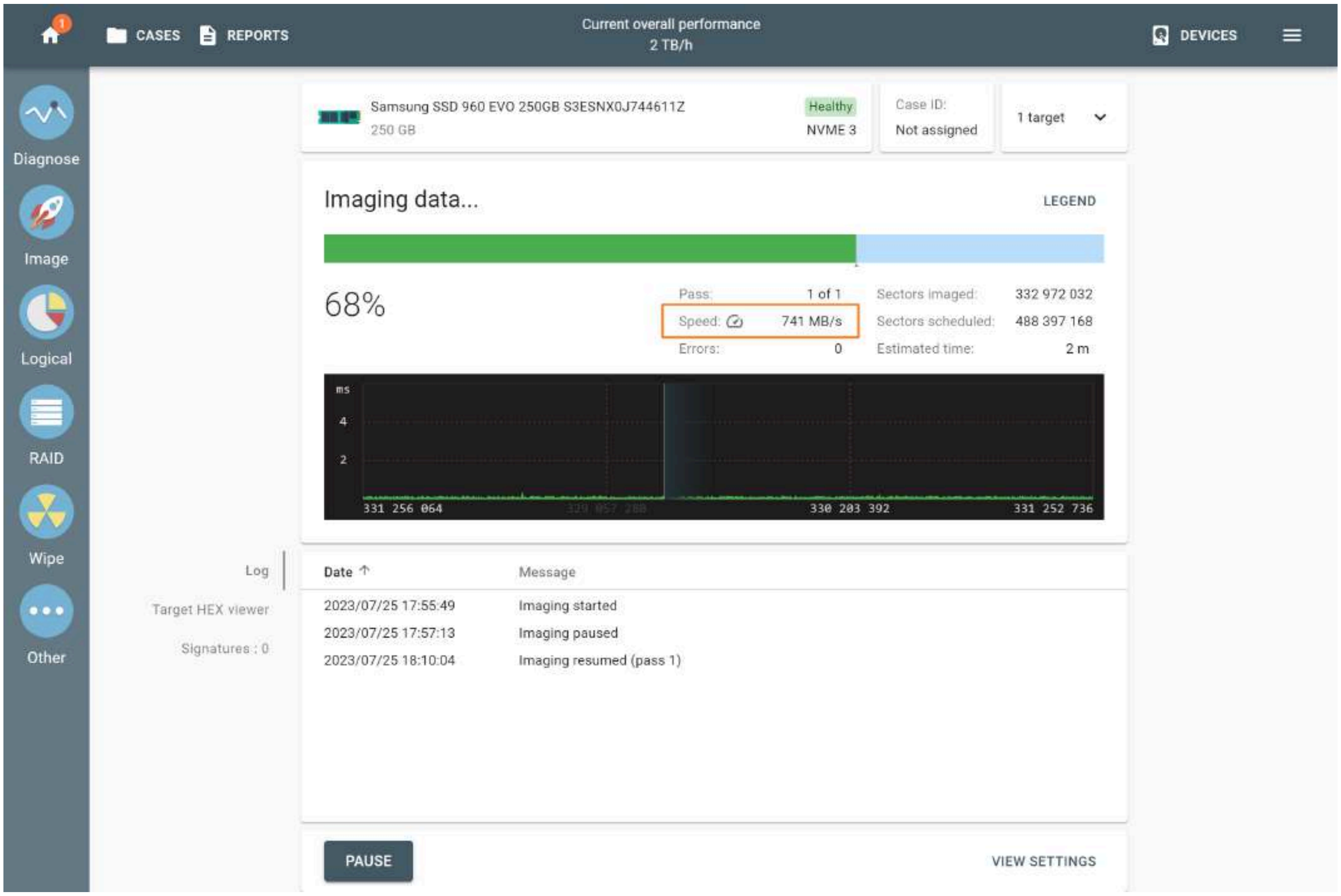
Enabling Jumbo frames.

> For fast imaging of files to your server via 10Gb network, you need to activate Jumbo framework in the settings of the server’s network adapter as well as in the settings of the network switch, should it be necessary (10Gb switches normally have Jumbo framework activated by default).

Then you can return to your imaging session:

1. Go to **Image**.
2. Select the source.
3. Click **Resume**.

This time, the speed is way higher!



Samsung SSD 960 EVO 250GB S3ESNX0J744611Z
250 GB
Healthy
NVME 3
Case ID:
Not assigned
1 target

Imaging data...

68%

Pass:	1 of 1	Sectors imaged:	332 972 032
Speed:	741 MB/s	Sectors scheduled:	488 397 168
Errors:	0	Estimated time:	2 m

Date ↑	Message
2023/07/25 17:55:49	Imaging started
2023/07/25 17:57:13	Imaging paused
2023/07/25 18:10:04	Imaging resumed (pass 1)

Imaging speed with Jumbo frames enabled.

Network setup tips

- Configuring 10Gb network with DHCP-enabled switch
- Getting maximum performance of Ubiquiti network
- Configuring a dynamic IP for TaskForce 2 in a network without router or DHCP-enabled switch
- Accessing Windows Server 2012 shared folder
- Setting up Synology DS218 as storage server

Configuring 10Gb network with DHCP-enabled switch

You need to create or extend network with DHCP-enabled switch with 10Gb connection.

Example. Ubiquiti EdgeSwitch 16 XG: four 10Gb Ethernet ports, twelve 10Gb SFP ports. Approximate price: $600.

This kind of switch supports static IP setup via simple web admin. So you could set the IP addresses you need for each current network device.

How to configure Ubiquiti DHCP server:

1. Connect PC and TaskForce 2 to Ubiquiti switch.
2. Set static IP address of PC to 192.168.1.4.
3. Open a browser and enter 192.168.1.2 (default Ubiquiti switch IP).
4. Log in with default credentials: ubnt (both in name and password fields).
5. Go to **System** > **Advanced Configuration** > **DHCP server** > **Global**.
6. Activate **Admin mode** by checking a necessary checkbox and pressing **Submit** button.

7. Go to **Pool Summary** and press **Add** to make a new address pool.
8. Enter your:
    - pool name
    - network base address (for example, 192.168.1.0)
    - network mask (in most cases, it should be 255.255.255.0)
    - put Default Router Address and DNS

    After creating your pool, you can change it via **Pool configuration** tab.
9. Click **Save configuration** button in the upper right corner of the window and click **Save**.

You can check this Youtube guide for alternative instructions on network setup using Ubiquiti switch.

Getting maximum performance of Ubiquiti EdgeSwitch 16 XG network

To optimize performance using Ubiquiiti EdgeSwitch 16 XG, you need to enable 10Gb with jumbo frames:

1. Go to **Basic** > **Port summary**.
2. Select ports 0/13, 0/14, 0/15, 0/16 and click **Edit**.
3. Change **Maximum Frame Size** to 9014 in **Edit Port** configuration window.

Configuring a dynamic IP for TaskForce 2 in a network without router or DHCP-enabled switch

If there is no hardware in the network that assigns IP address, or if you want to keep a small network with TaskForce 2 and your server/PC connected directly, it is possible to install and setup software DHCP server. The good news is, it does not require any investment. All you need is some time to set it up on any computer in the server network. Follow the instructions from these guides:

- Windows: Free DHCP server.
- Linux: Included DHCP service.

Accessing Windows Server 2012 shared folder

If you want to store a target image file in a Window Server 2012 network folder but it appears missing, please follow these steps:

1. Go to **Control panel**.
2. Enable **Guest** account (**Administrative tools** > **AD users and computers** > **Users**).
3. **Network and sharing center** > **Change advanced sharing settings** > **Turn On network discovery** + **Turn on sharing (file and printers** + **public folders)**.
4. In the shared folder access options, add **Guest** or **Everyone**.

If the shared folder demands restricted access, please follow this guide.

Setting up Synology DS218 as storage server

To set up Synology DS218:

1. Go to **Control panel** > **File services** > **SMB** > **Advanced settings**.
2. Set **Maximum protocol** to SMB3.
3. Go to **Control panel** > **Shared folder**.
4. Click **Create** button and specify network folder details.

If you need to get a guest account working, run the following actions:

1. Go to **Control panel** > **User**.
2. Edit for **Guest** user.
3. Clear the **Disable this account** checkbox.

For more instructions and information about check our Troubleshooting guide and FAQ page.

Configuring TaskForce use with Synology or QNAP NAS as a LAN

Here is a guide to configure your NAS to be used with TaskForce 2 for storage of image files.

This manual is indicative and may vary between models and manufacturers. We have tested this setup on Synology DS218 and QNAP TS-431K.

Table of contents

Setting up a Synology NAS

1. Install drives in the Synology NAS.
2. Use a LAN cable to connect the DiskStation to your switch, router, or hub.
3. Press the power button to turn on your Synology NAS.
4. Install DiskStation Manager (DSM) – Synology's browser-based operating system – on your DiskStation.
5. Follow the instructions to create a RAID volume and a partition with a file system on it.

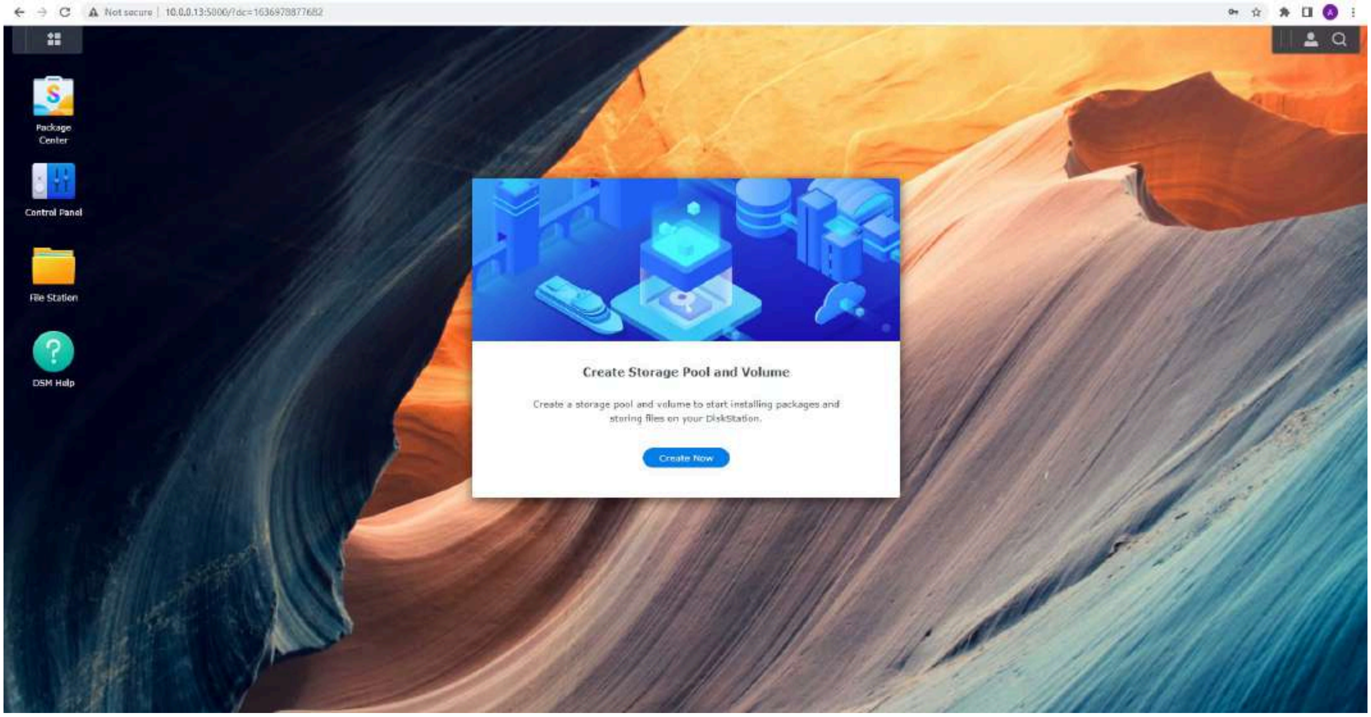
Enabling SMB3 is highly recommended for the best performance:

a. Go to **Control panel** > **File services** > **SMB** > **Advanced settings**.

b. Set **Maximum protocol** to *SMB3*.

c. Go to **Control panel** > **Shared folder**.

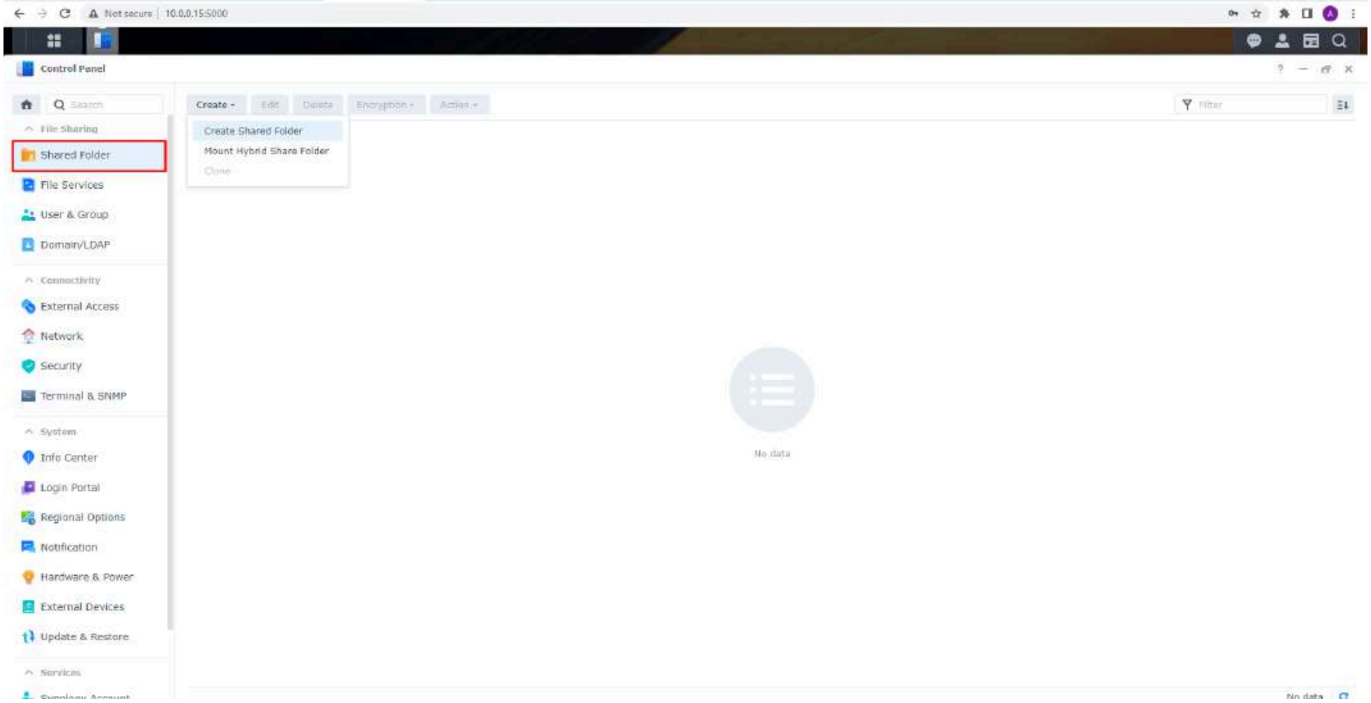
d. Click **Create** and specify network folder details.



Create Storage Pool and Volume

Create a storage pool and volume to start installing packages and storing files on your DiskStation.

6. Create a Shared folder in the new volume:
   Control panel > **File sharing** > **Shared folder** > **Create** > **Create Shared Folder**



7. In the folder creation menu, set the folder name, e.g. *Image Files* and set access options.

Setting up a QNAP NAS

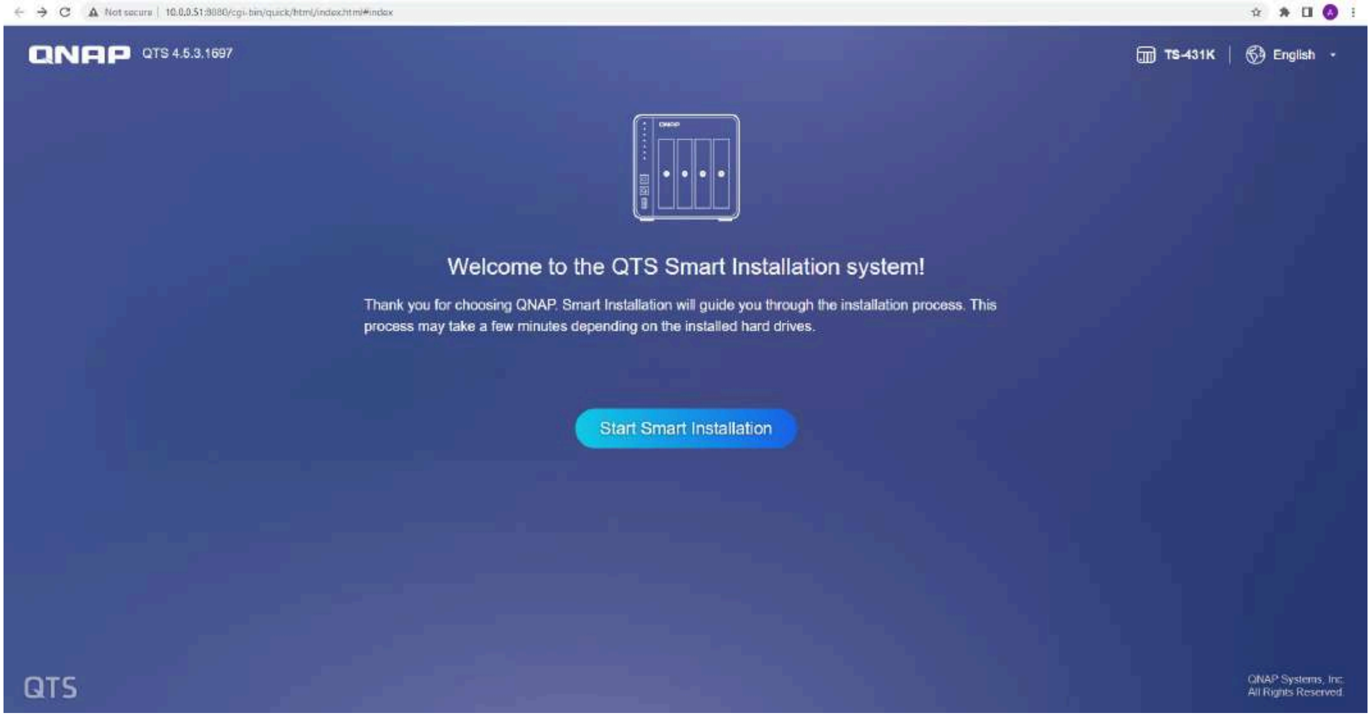
1. Install drives in the QNAP NAS.
2. Use a LAN cable to connect the QNAP to your switch, router, or hub.

3. Press the power button to turn on your QNAP.

4. Install Qfinder Pro for quick find and easy access to QNAP NAS on the same LAN.

5. Find your QNAP using Qfinder Pro and go to its page in the browser.

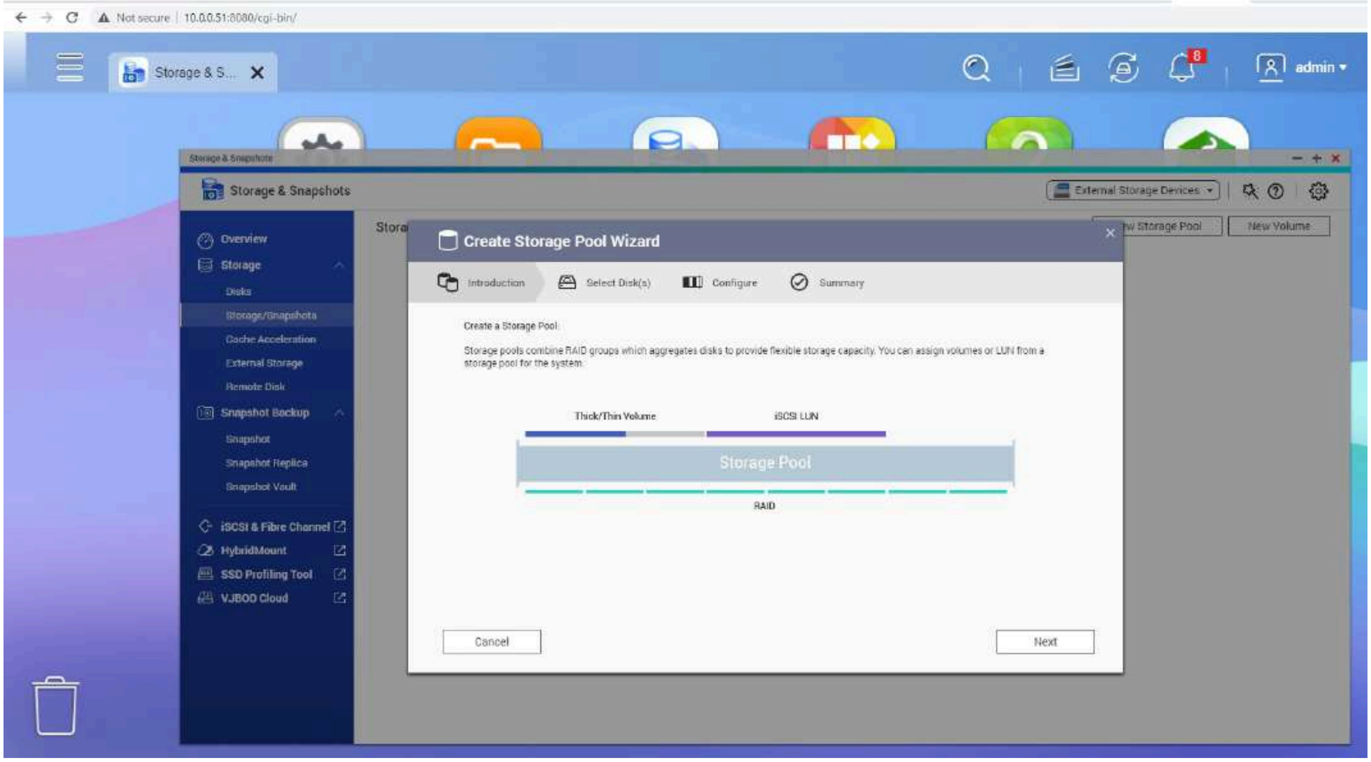
6. Follow instructions to complete Smart Installation.



Welcome to the QTS Smart Installation system!

Thank you for choosing QNAP. Smart Installation will guide you through the installation process. This process may take a few minutes depending on the installed hard drives.

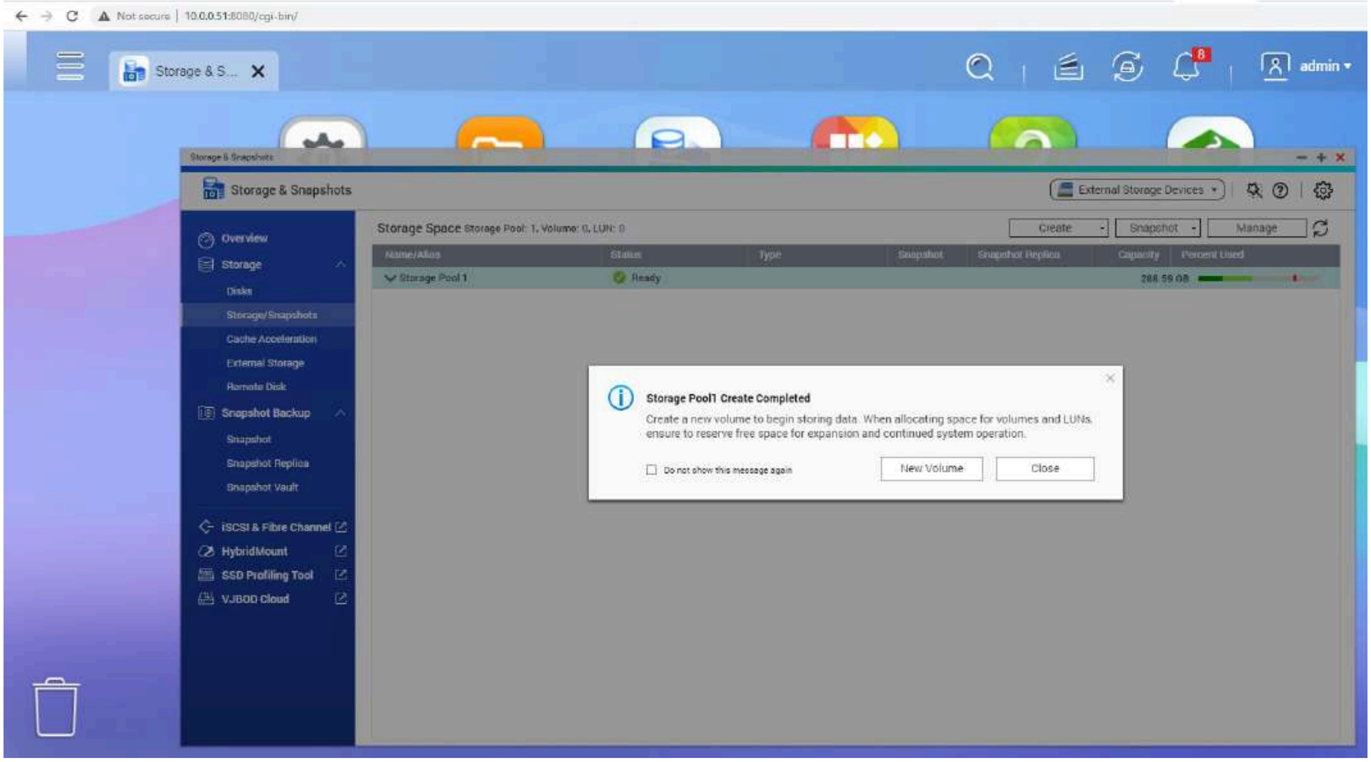
7. Create Storage Pool (RAID):
   a. Storage & Snapshots.
   b. Storage (left menu).
   c. Storage/Snapshots.
   d. New Storage Pool (in the the top right corner).
   e. Follow the instructions to set up the Storage Pool.



Create a Storage Pool:

Storage pools combine RAID groups which aggregates disks to provide flexible storage capacity. You can assign volumes or LUN from a storage pool for the system.

8. In the final stages of setting up the Storage Pool, create a New Volume.



Storage Space Storage Pool: 1, Volume: 0, LUN: 0

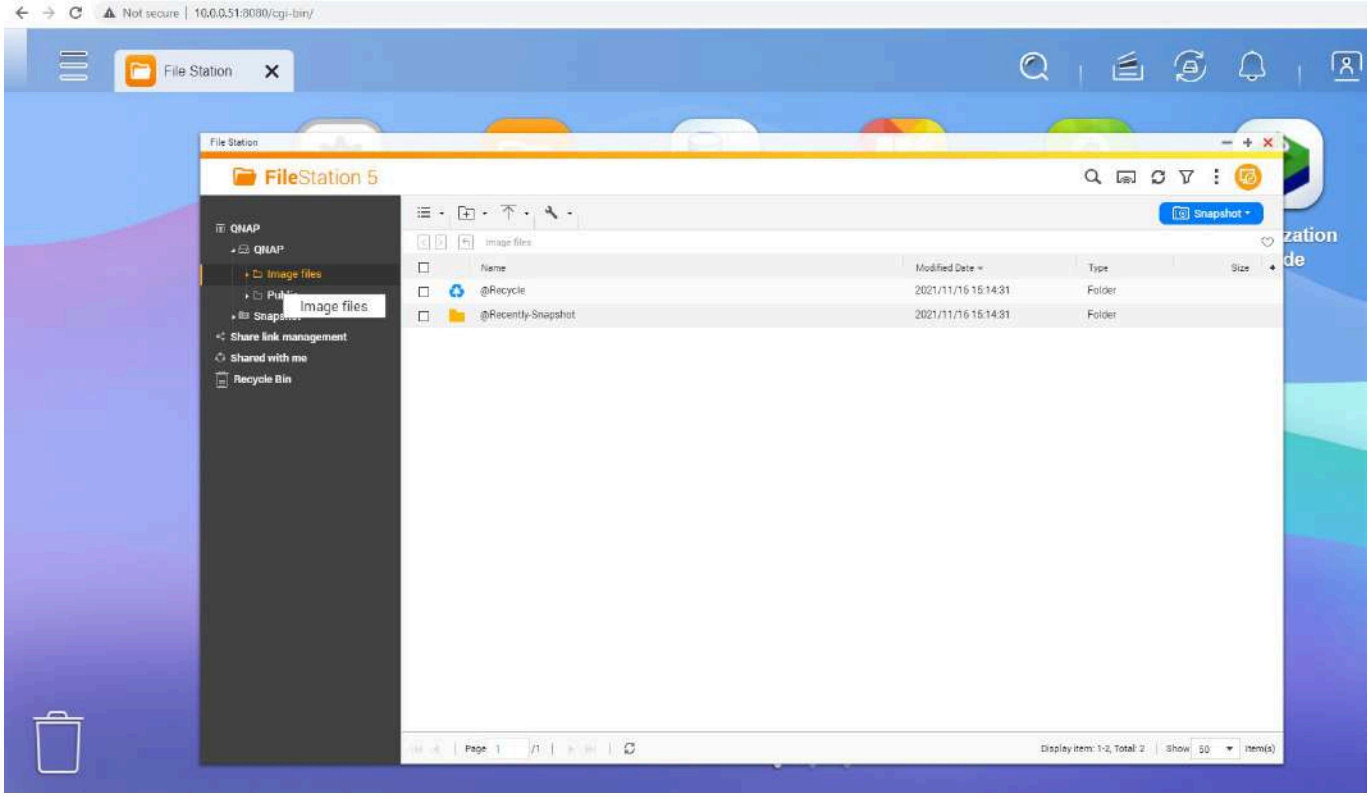
Name/Alias	Status	Type	Snapshot	Snapshot Replica	Capacity	Percent Used
Storage Pool 1	Ready				288.59 GB	

Storage Pool1 Create Completed

Create a new volume to begin storing data. When allocating space for volumes and LUNs, ensure to reserve free space for expansion and continued system operation.

☐ Do not show this message again

9. In the File Station utility, you can find the new volume: QNAP. In it, there is a Shared Folder created by default called *Public*.

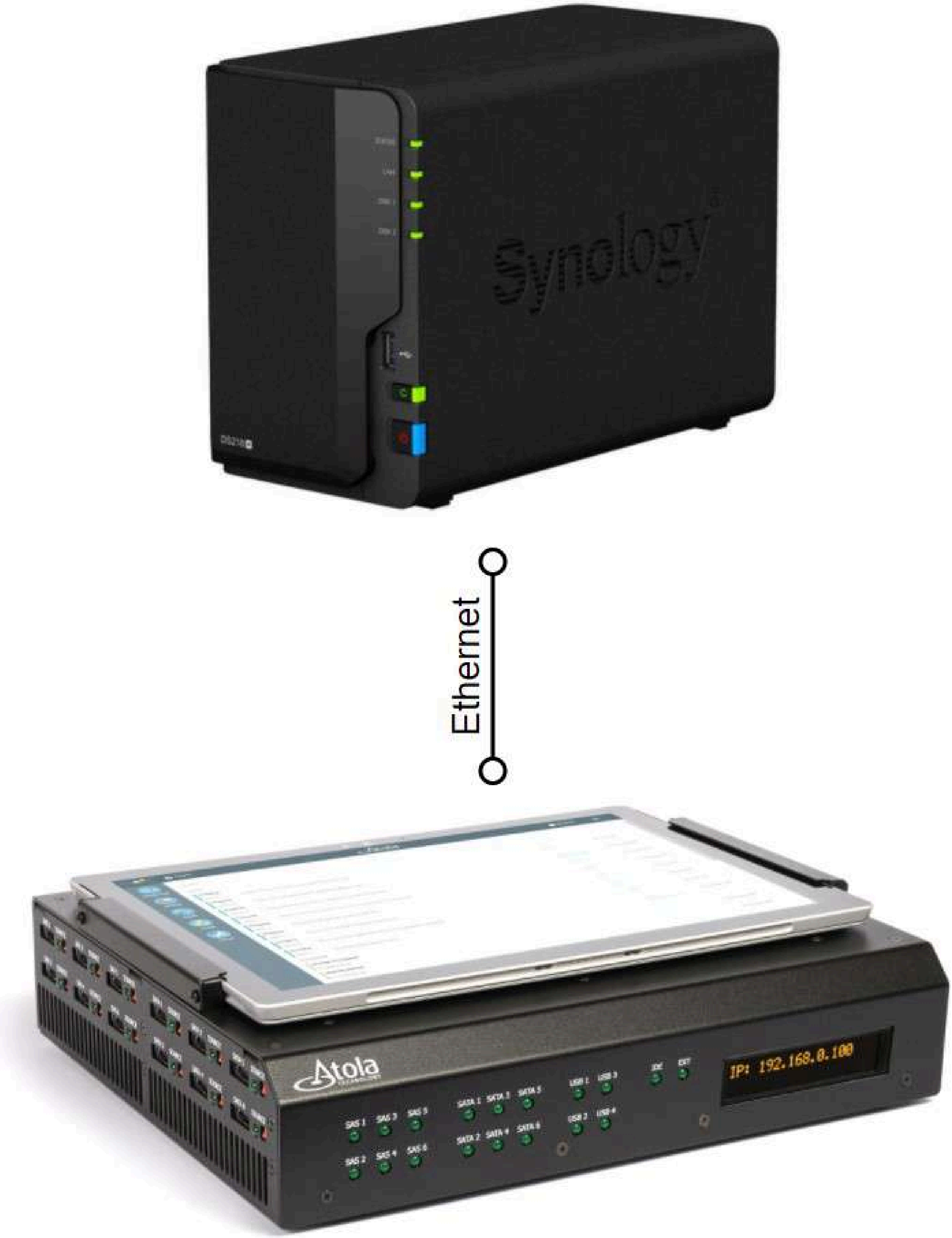


Name	Modified Date	Type	Size
@Recycle	2021/11/16 15:14:31	Folder	
@Recently-Snapshot	2021/11/16 15:14:31	Folder	

Page 1 /1

Display item: 1-2, Total: 2 | Show 50 Item(s)

10. For a Shared Folder with specific access or encoding settings, create a new one by clicking the icon showing a folder with a + and adjust the configuration.

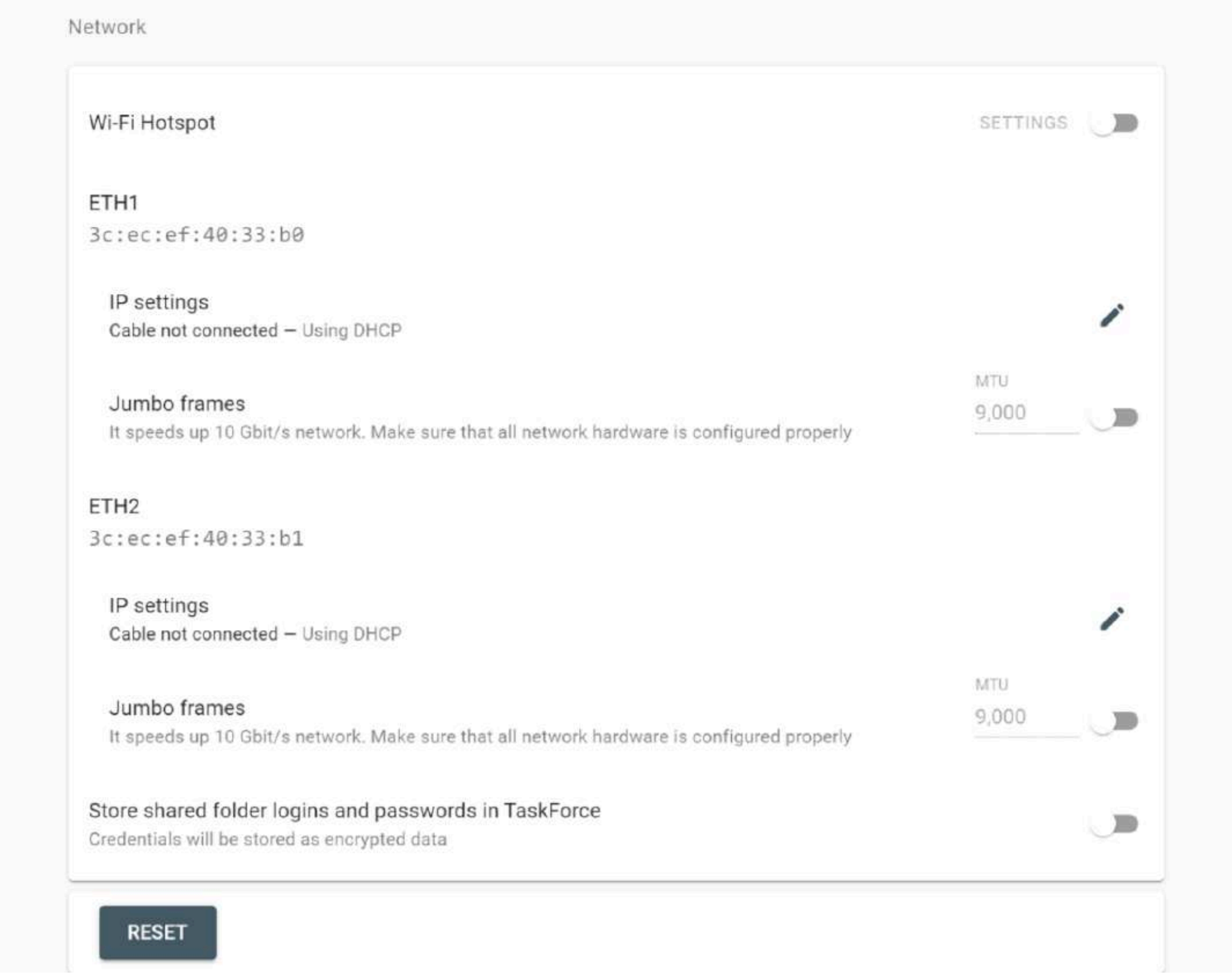


Direct connection with a Static IP:

Since we are not connecting TaskForce and Synology/QNAP NAS to a wider network, it is enough to set up the same Subnet Mask for the NAS and the TaskForce, and configure Static IP addresses that will indicate the same network.

TaskForce 2 configuration

1. Go to **Menu** > **Settings** > **Network section**.
2. Select the Ethernet port through which Synology is connected (e.g. ETH1).
3. Click IP settings's **Edit** icon.



Network

Wi-Fi Hotspot

ETH1
3c:ec:ef:40:33:b0

IP settings
Cable not connected — Using DHCP

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU 9,000

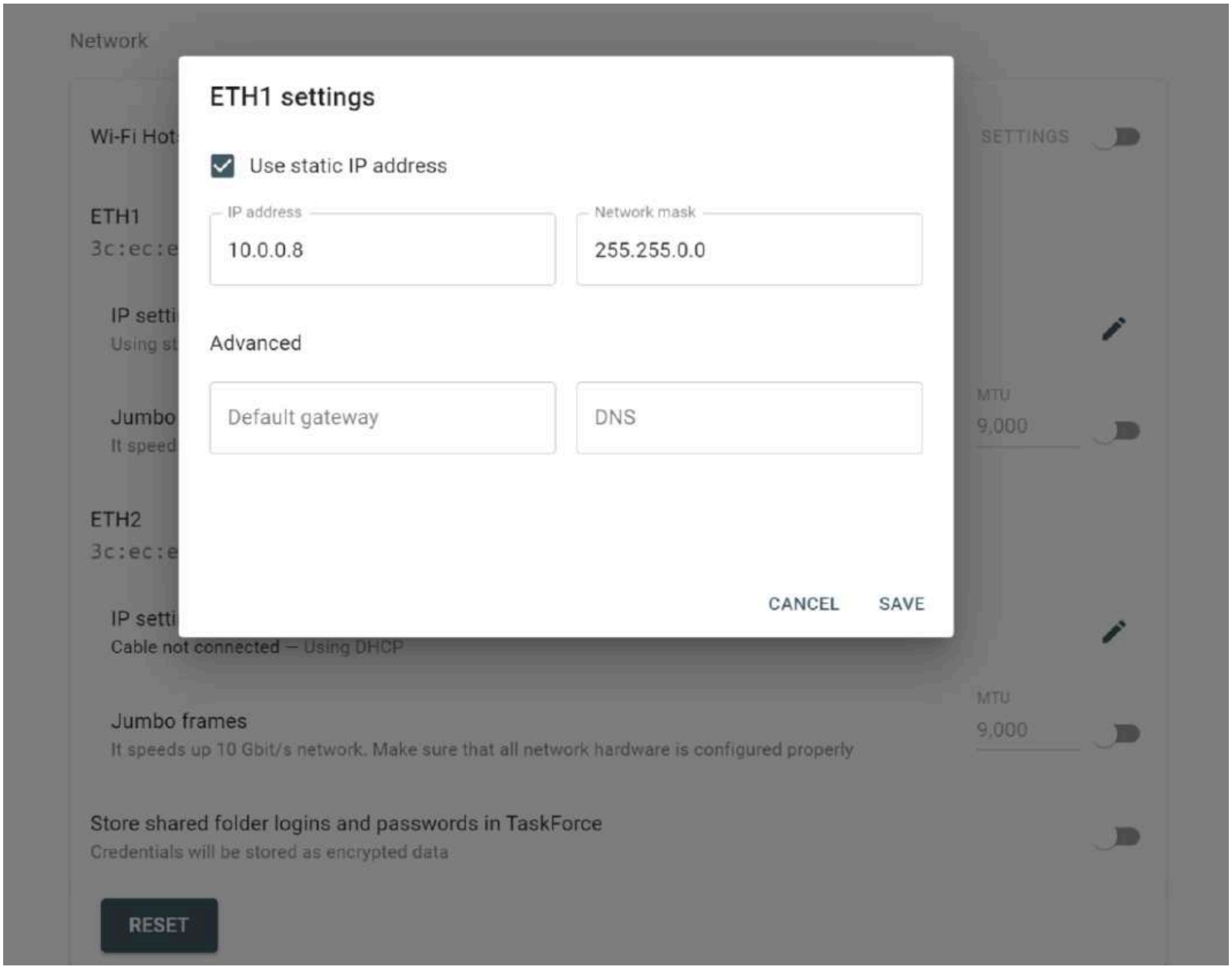
ETH2
3c:ec:ef:40:33:b1

IP settings
Cable not connected — Using DHCP

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU 9,000

Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data

4. In the **ETH settings** dialog, enter the address (e.g. *255.255.0.0*) in the **Subnet Mask** field that is identical to that of Synology.
5. Assign an IP address using the Subnet Mask: the first two bytes of TaskForce's IP must be identical to those of IP Synology (e.g. *10.0.0.15*). This will ensure that both TaskForce and Synology belong to the same network. (e.g. *10.0.0.8*).



ETH1 settings

☑ Use static IP address

IP address: 10.0.0.8

Network mask: 255.255.0.0

Advanced

Default gateway

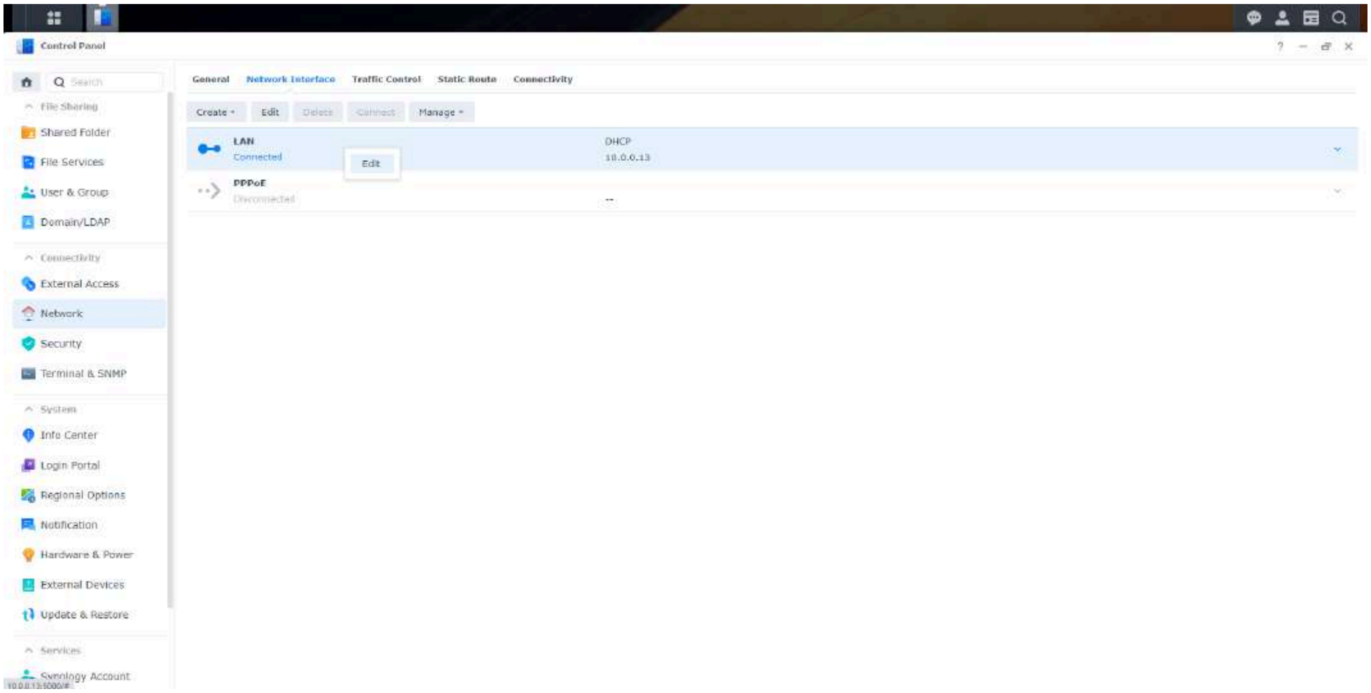
DNS

CANCEL
SAVE
Network
Wi-Fi Hot
SETTINGS
ETH1
3c:ec:e
IP setti
Using st
Jumbo
It speed
MTU
9,000
ETH2
3c:ec:e
IP setti
Cable not connected — Using DHCP
Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly
MTU
9,000
Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data
RESET

6. Click **Save**.

Setting up a Static IP in Synology

1. Go to the **Control panel**.
2. Open **Network interface**.
3. Select the current connection to Synology.
4. Click **Edit**.



LAN Connected DHCP 10.0.0.13

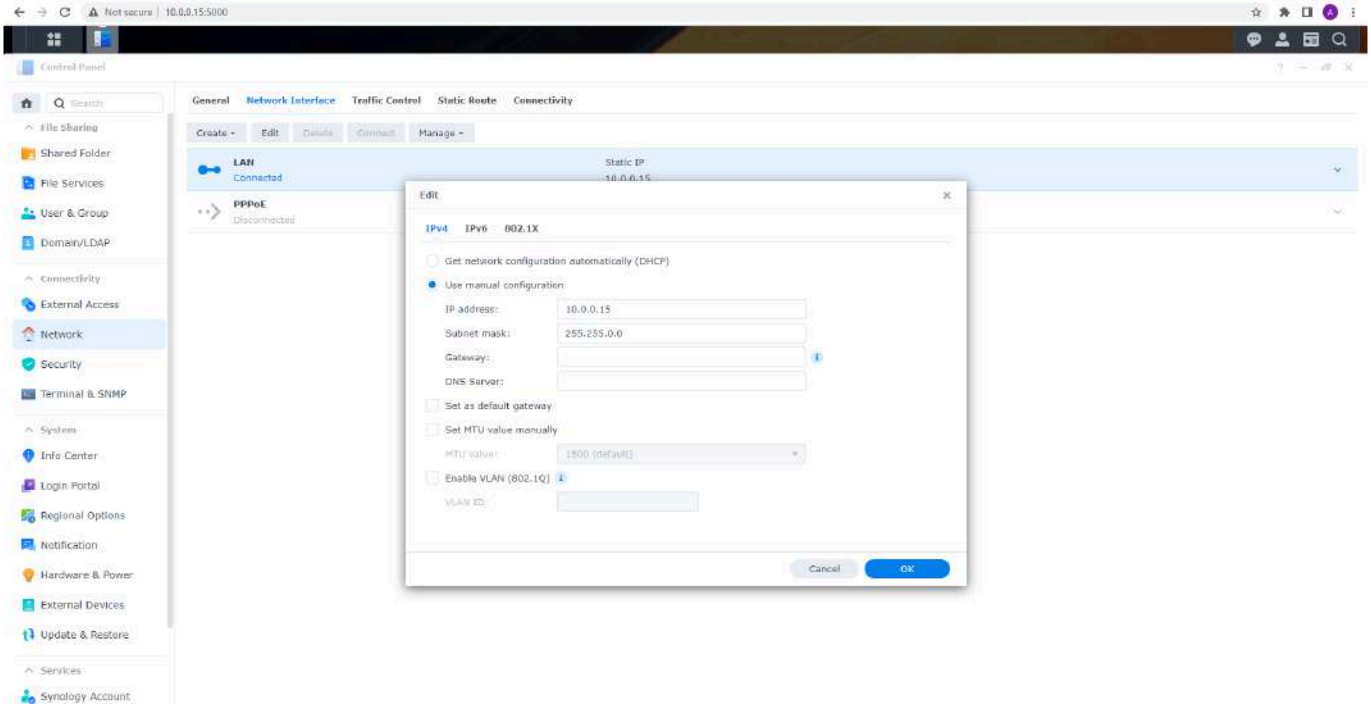
PPPoE Disconnected --

5. On **IPv4** tab, select **Use manual configuration**.

6. Assign **Subnet Mask** (e.g. *255.255.0.0*), which is identical to that of TaskForce.

7. Assign **IP address** (e.g.: *10.0.0.15*).

8. Click **OK**.



LAN Connected Static IP 10.0.0.15

PPPoE Disconnected

○ Get network configuration automatically (DHCP)

● Use manual configuration

IP address: 10.0.0.15

Subnet mask: 255.255.0.0

Gateway:

DNS Server:

□ Set as default gateway

□ Set MTU value manually

MTU value: 1500 (default)

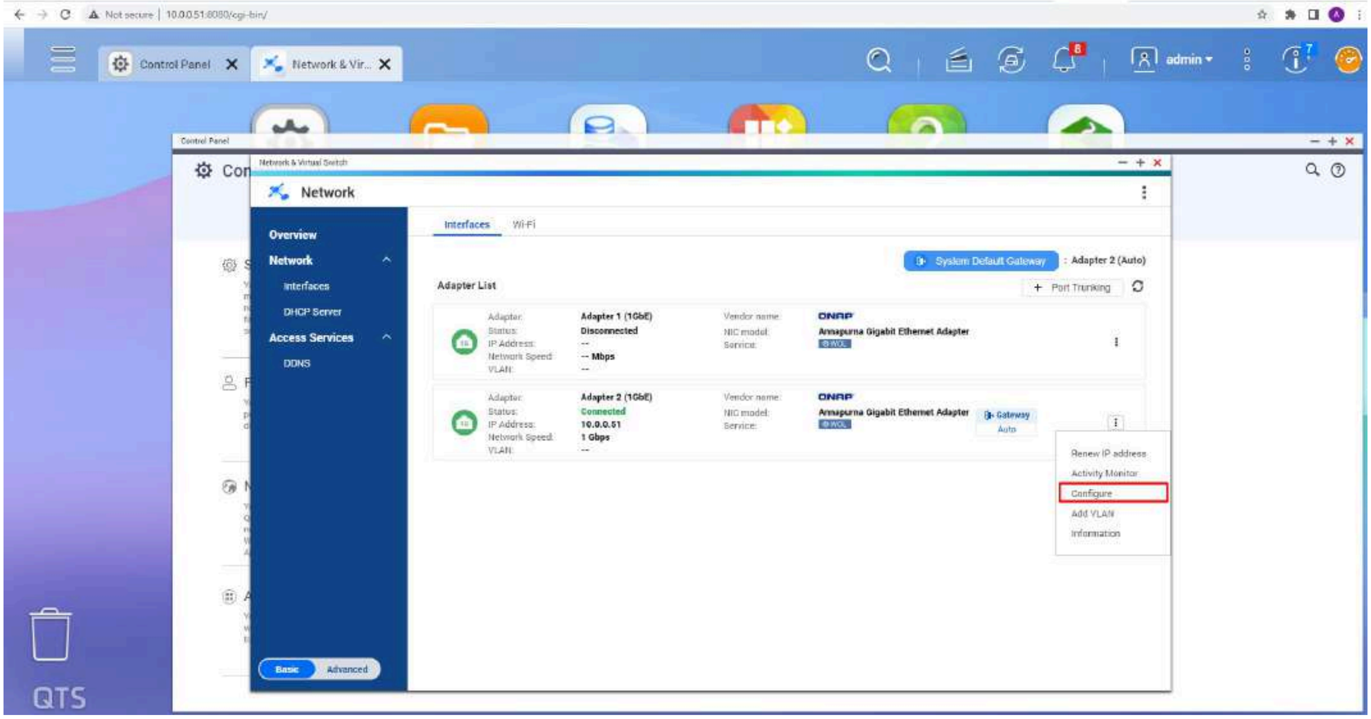
□ Enable VLAN (802.1Q)

VLAN ID:

9. After Synology has changed the settings, it can be disconnected from the current network.

Setting up Static IP in QNAP

1. In the **Control panel**, go to **Network & Virtual Switch**.
2. Select the current connection to QNAP.
3. Open the **Menu**.
4. Click **Configure**.



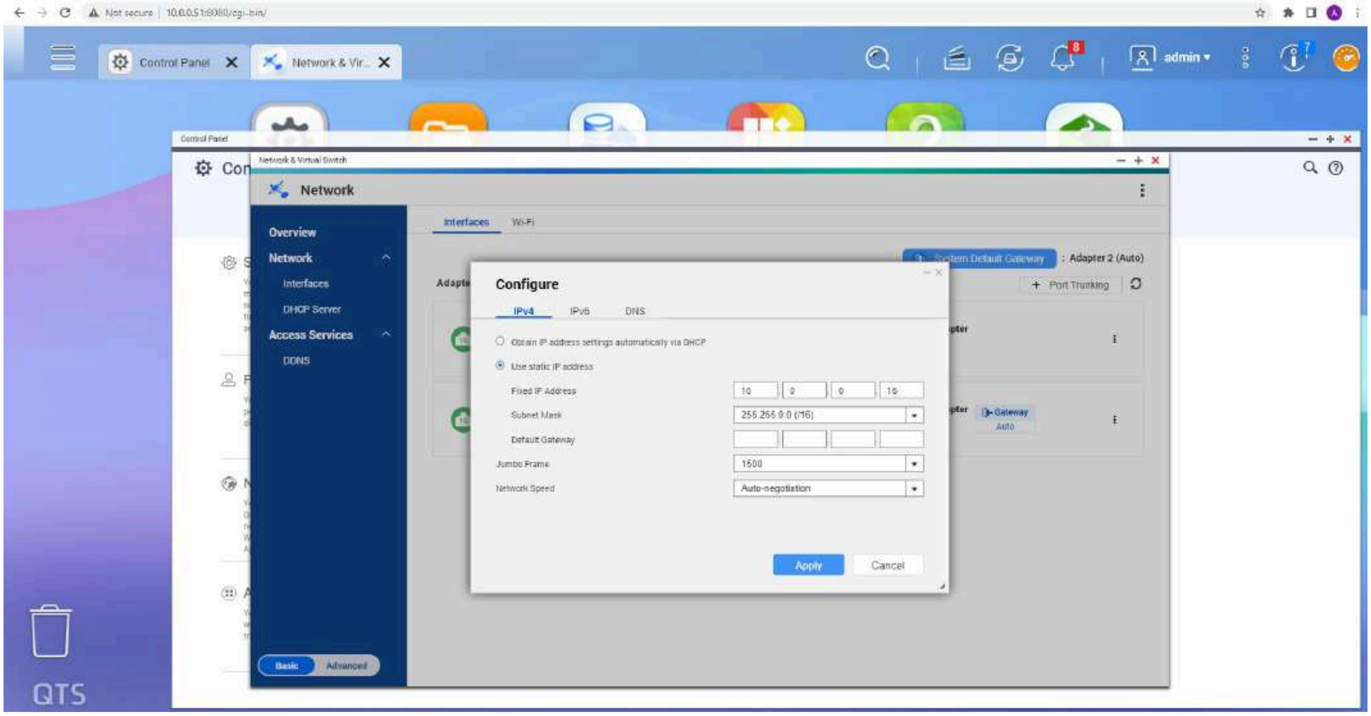
Adapter List

Adapter: Adapter 1 (1GbE)
Status: Disconnected
IP Address: --
Network Speed: -- Mbps
VLAN: --
Vendor name: QNAP
NIC model: Annapurna Gigabit Ethernet Adapter
Service: WOL

Adapter: Adapter 2 (1GbE)
Status: Connected
IP Address: 10.0.0.51
Network Speed: 1 Gbps
VLAN: --
Vendor name: QNAP
NIC model: Annapurna Gigabit Ethernet Adapter
Service: WOL

System Default Gateway : Adapter 2 (Auto)

5. On the **IPv4** tab, select **Use static IP address**.
6. Assign a **Subnet Mask** (e.g. *255.255.0.0*), which is identical to that of TaskForce.
7. Assign an **IP address** (e.g.: *10.0.0.16*).
8. **Gateway** field should be left blank because you are configuring a LAN and connecting to other networks is unnecessary.
9. **Jumbo Frame** and **Network speed** should be left with the default values.
10. Click **Apply**.



Configure

IPv4 IPv6 DNS

○ Obtain IP address settings automatically via DHCP

● Use static IP address

Fixed IP Address: 10 . 0 . 0 . 16

Subnet Mask: 255.255.0.0 (/16)

Default Gateway:

Jumbo Frame: 1500

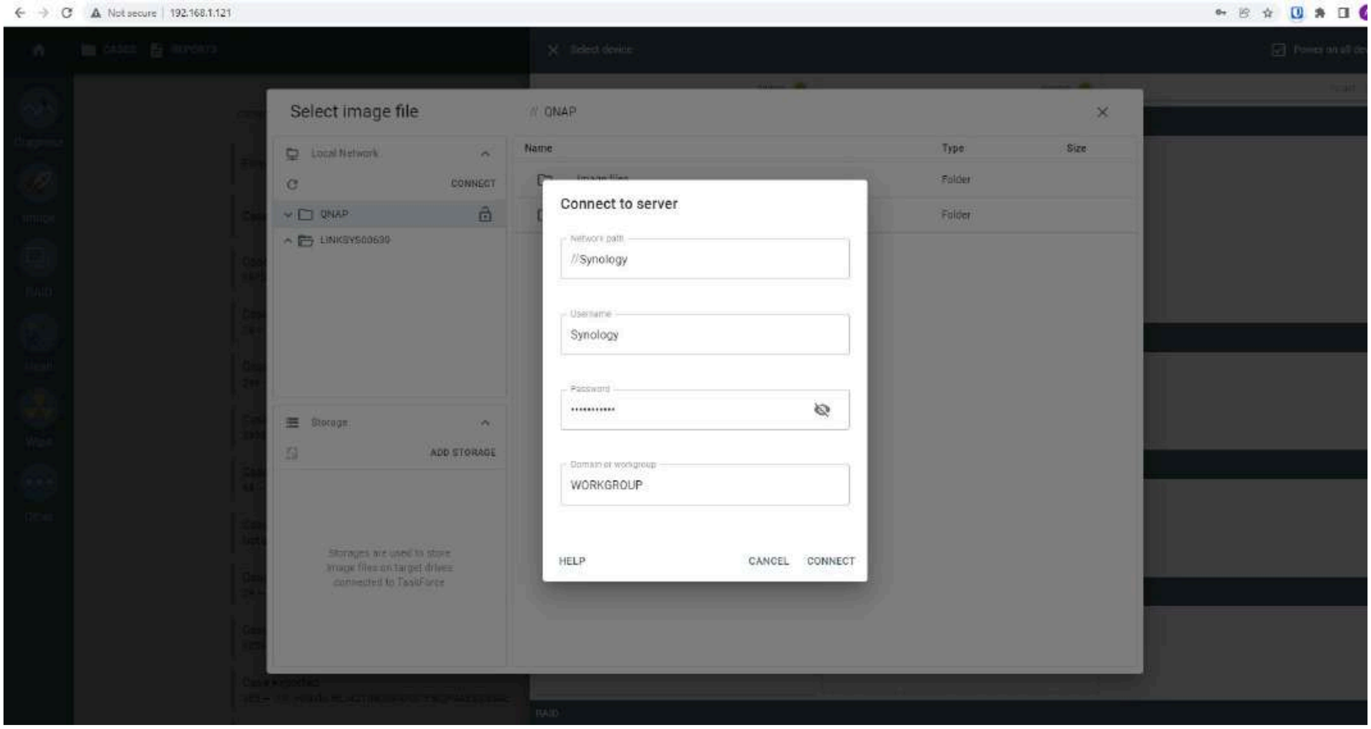
Network Speed: Auto-negotiation

Apply Cancel

11. After the QNAP has changed the settings you can disconnect it from the current network.

Connecting to the Shared Folder in TaskForce 2

1. Connect the Synology/QNAP NAS to TaskForce’s ETH1 port.
2. Click the **Devices** icon in the upper right corner. Go to the **File** section and click **Select File**.
3. Click **Connect**.
4. Enter the Server name, Username, Password.
   If you do not remember the server name, look it up:
   Synology > Control Panel > Info Center > Server name
   QNAP > Control Panel > General Setting > Server name
5. Click **Connect**.



Connect to server

Network path: //Synology

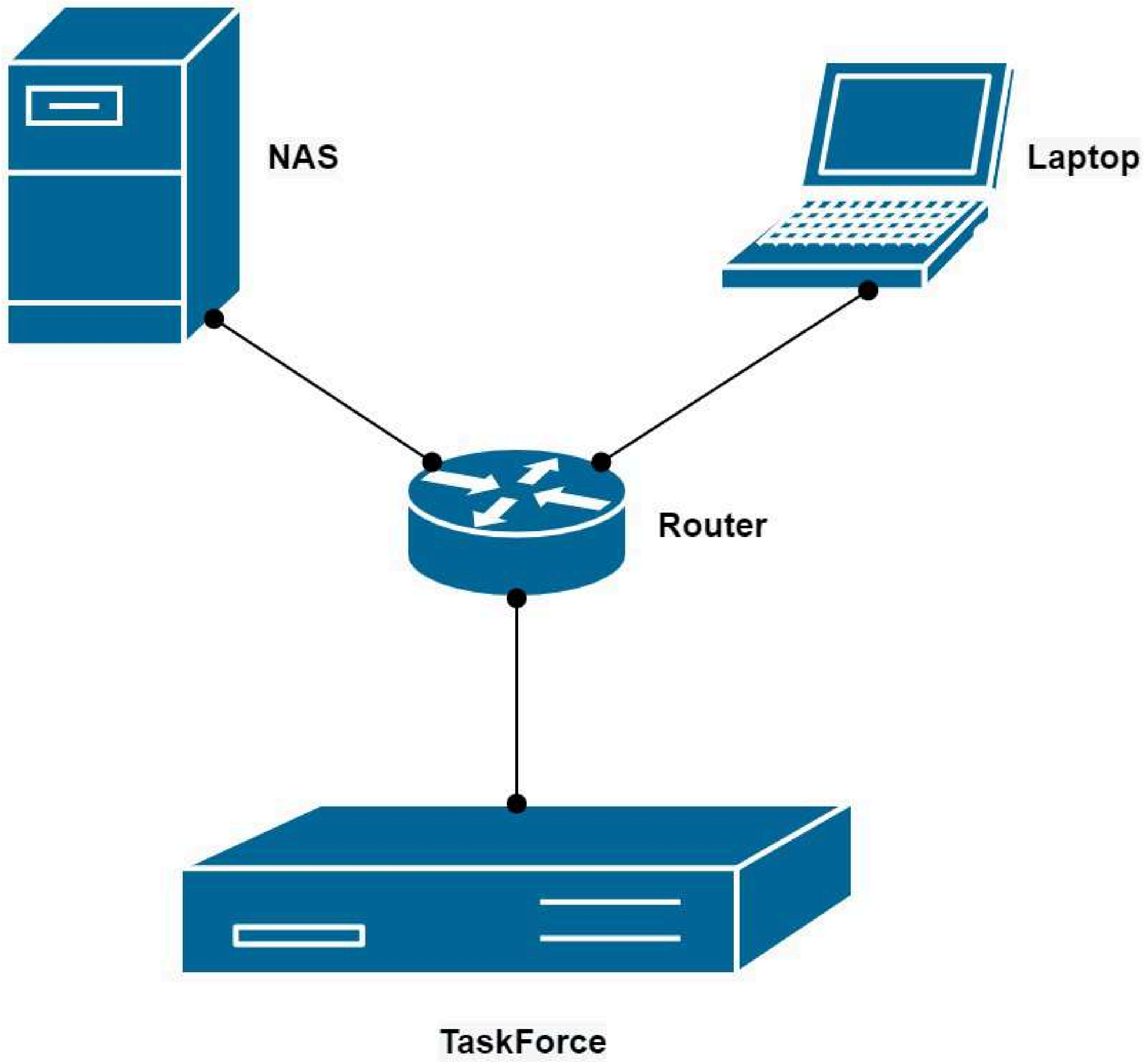
Username: Synology

Password: ••••••••••••

Domain or workgroup: WORKGROUP

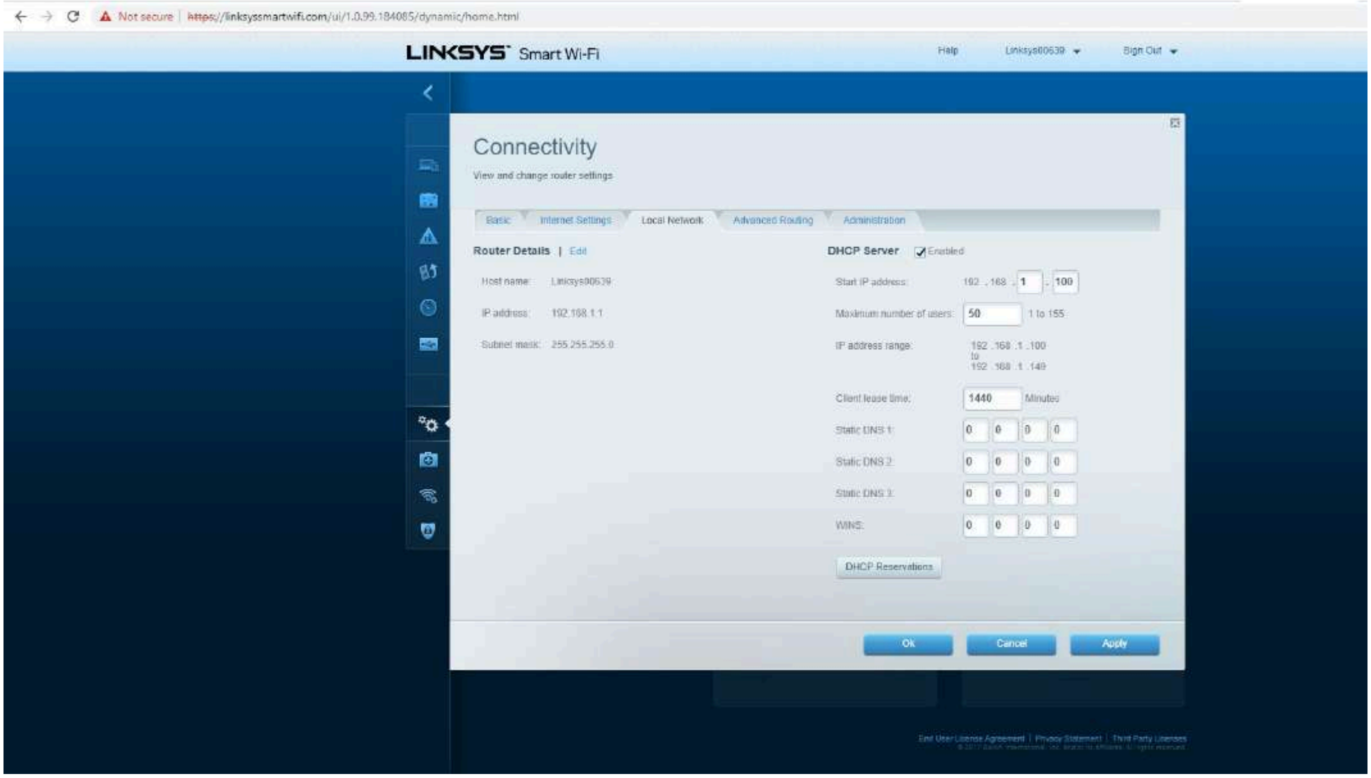
6. TaskForce 2 has connected to Synology and you can open the previously created Shared Folder.

Setting up a LAN using router with DHCP (Dynamic IP)



Setting up router

1. Connect the router directly to your PC or laptop via the Ethernet port.
2. Log in to the web configurator.
3. Turn on the DHCP server in the local network settings.
4. Apply changes.



Connectivity

View and change router settings

Router Details

Host name: Linksys00639

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

DHCP Server ☑ Enabled

Start IP address: 192 . 168 . 1 . 100

Maximum number of users: 50 1 to 155

IP address range: 192 . 168 . 1 . 100 to 192 . 168 . 1 . 149

Client lease time: 1440 Minutes

Static DNS 1: 0 0 0 0

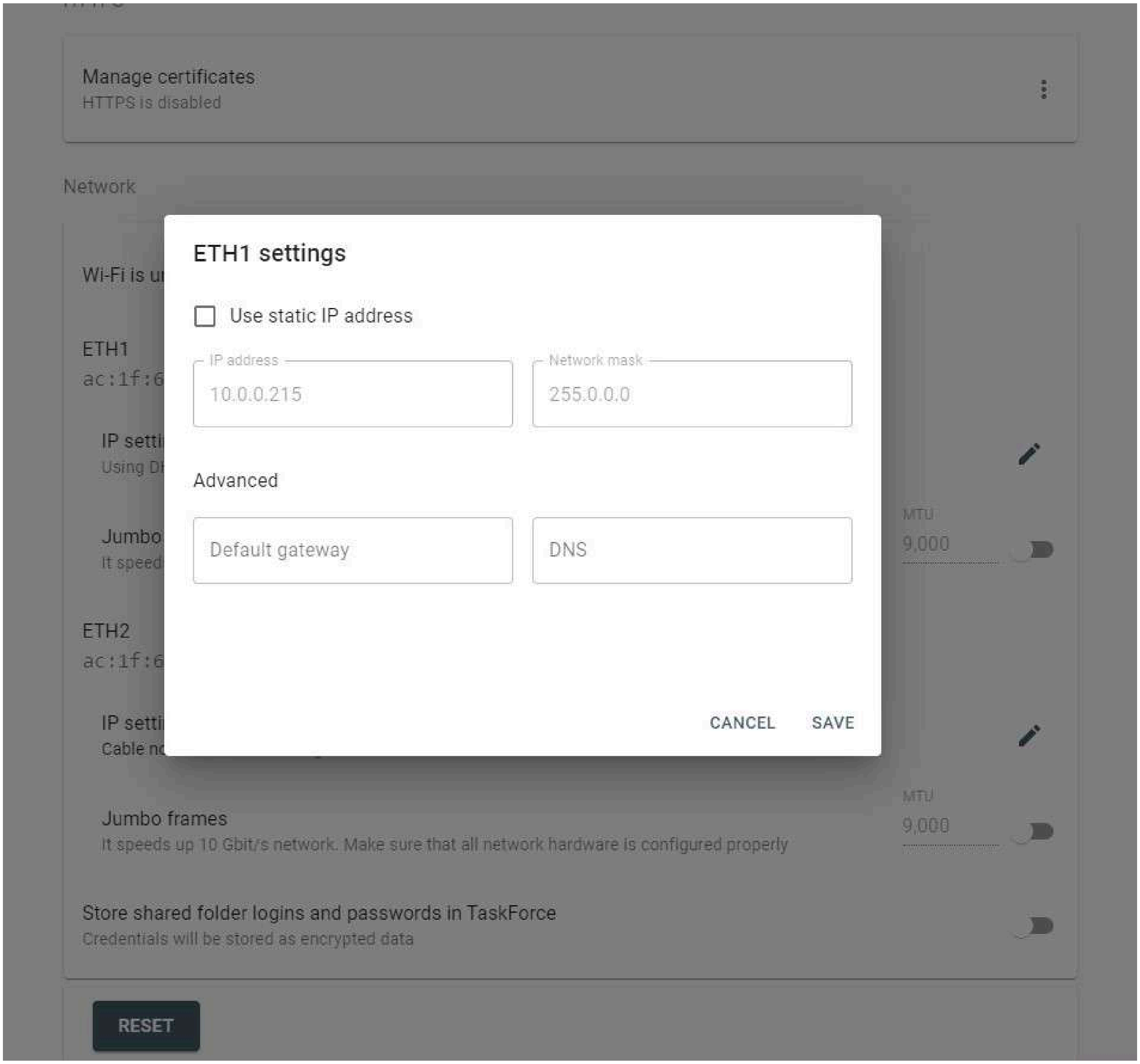
Static DNS 2: 0 0 0 0

Static DNS 3: 0 0 0 0

WINS: 0 0 0 0

Setting up DHCP in TaskForce 2

1. Open **Menu** > **Settings**, go to the **Network** section.
2. Select the Ethernet port to which Synology will be connected. (e.g. ETH1).
3. Click the **Edit** icon to adjust the IP settings.
4. Clear the **Use static IP address** checkbox.
5. Click **Save**.



Manage certificates
HTTPS is disabled

Network

Wi-Fi is ur

ETH1
ac:1f:6

IP setti
Using DI

Jumbo
It speed

MTU 9,000

ETH2
ac:1f:6

IP setti
Cable nc

Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly

MTU 9,000

Store shared folder logins and passwords in TaskForce
Credentials will be stored as encrypted data

RESET

ETH1 settings

□ Use static IP address

IP address: 10.0.0.215

Network mask: 255.0.0.0

Advanced

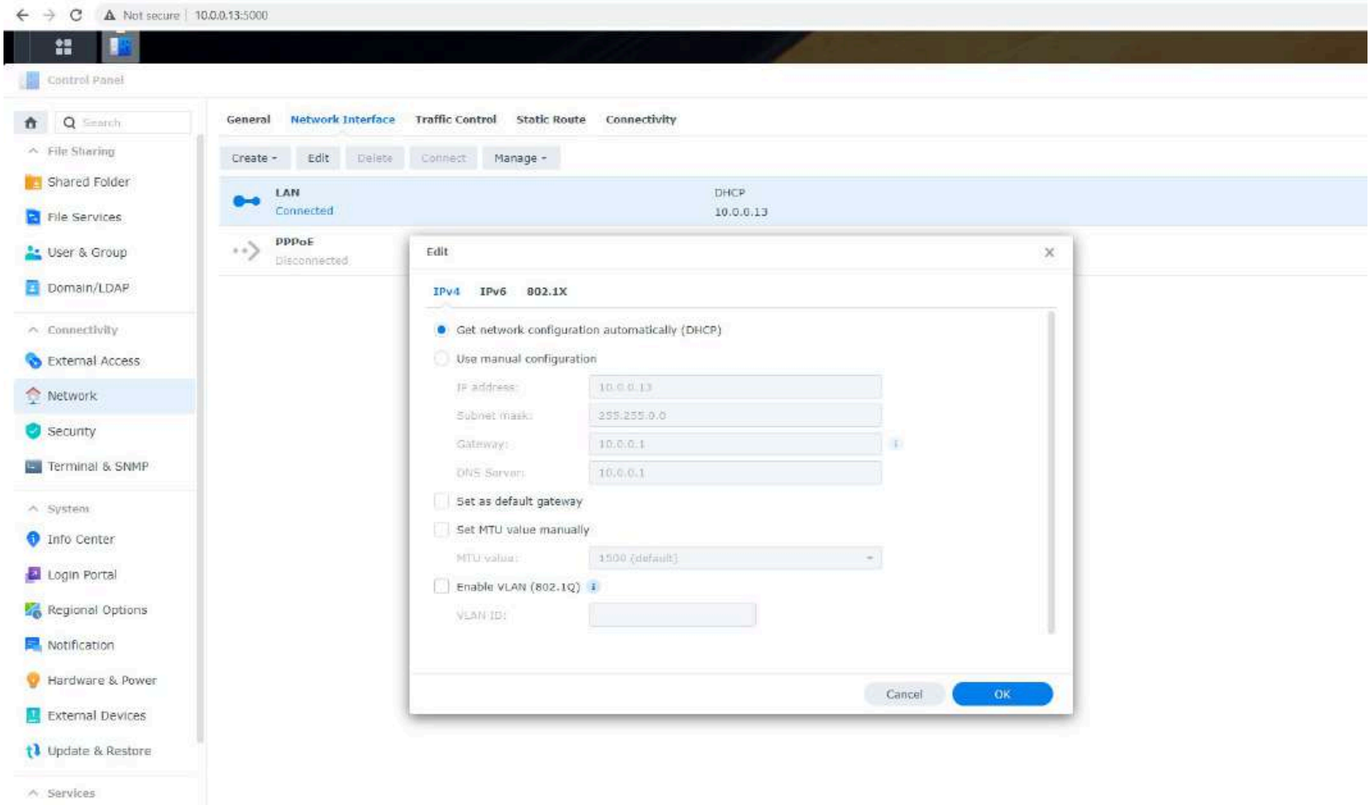
Default gateway

DNS

CANCEL SAVE

Setting up DHCP in Synology

1. Go to **Control panel** > **Network** > **Network interface**.
2. Select the current connection to Synology and click **Edit**.
3. On the **IPv4** tab, select the **Get network configuration automatically (DHCP)** option.



LAN — Connected — DHCP — 10.0.0.13

PPPoE — Disconnected

● Get network configuration automatically (DHCP)

○ Use manual configuration

IP address:	10.0.0.13
Subnet mask:	255.255.0.0
Gateway:	10.0.0.1
DNS Server:	10.0.0.1

□ Set as default gateway

□ Set MTU value manually

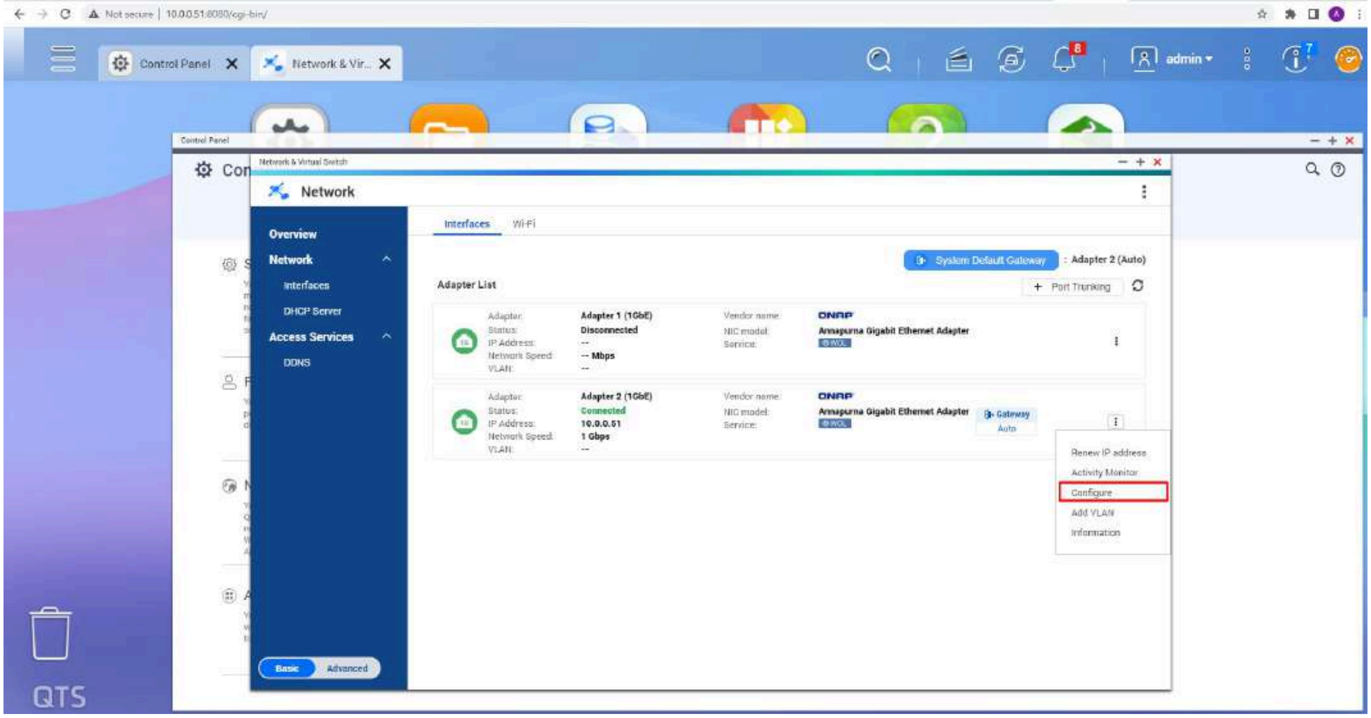
MTU value: 1500 (default)

□ Enable VLAN (802.1Q)

VLAN ID:

Setting up DHCP in QNAP

1. In the **Control panel**, go to the **Network & Virtual Switch**.
2. Select the current connection to QNAP, open the **Menu** and select **Configure**.

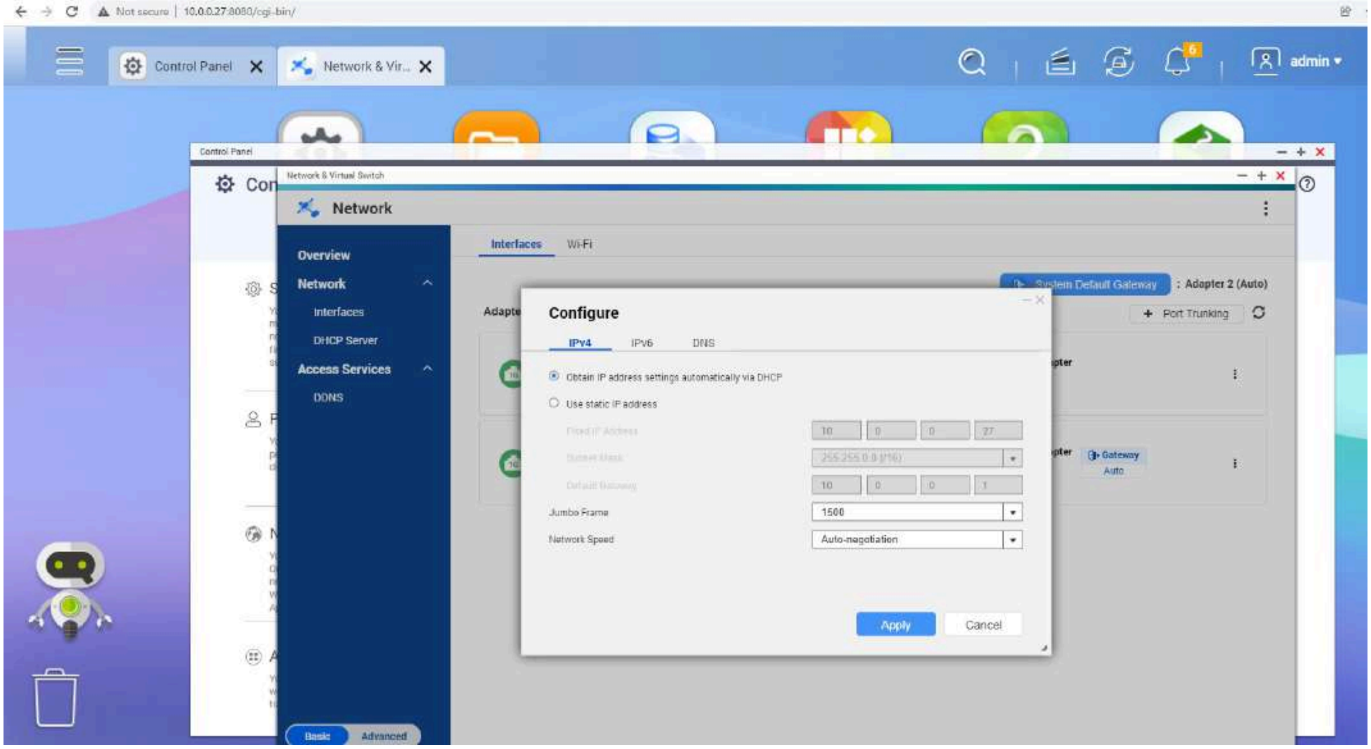


System Default Gateway : Adapter 2 (Auto)

Adapter List

Adapter:	Adapter 1 (1GbE)	Vendor name:	QNAP
Status:	Disconnected	NIC model:	Annapurna Gigabit Ethernet Adapter
IP Address:	--	Service:	WOL
Network Speed:	-- Mbps		
VLAN:	--		
Adapter:	Adapter 2 (1GbE)	Vendor name:	QNAP
Status:	Connected	NIC model:	Annapurna Gigabit Ethernet Adapter
IP Address:	10.0.0.51	Service:	WOL, Gateway Auto
Network Speed:	1 Gbps		
VLAN:	--		

3. On the **IPv4** tab, select **Obtain IP address settings automatically via DHCP**.



Configure

IPv4 IPv6 DNS

● Obtain IP address settings automatically via DHCP

○ Use static IP address

Fixed IP Address: 10 . 0 . 0 . 27

Subnet Mask: 255.255.0.0 (/16)

Default Gateway: 10 . 0 . 0 . 1

Jumbo Frame: 1500

Network Speed: Auto-negotiation

Apply Cancel

Connecting the LAN devices

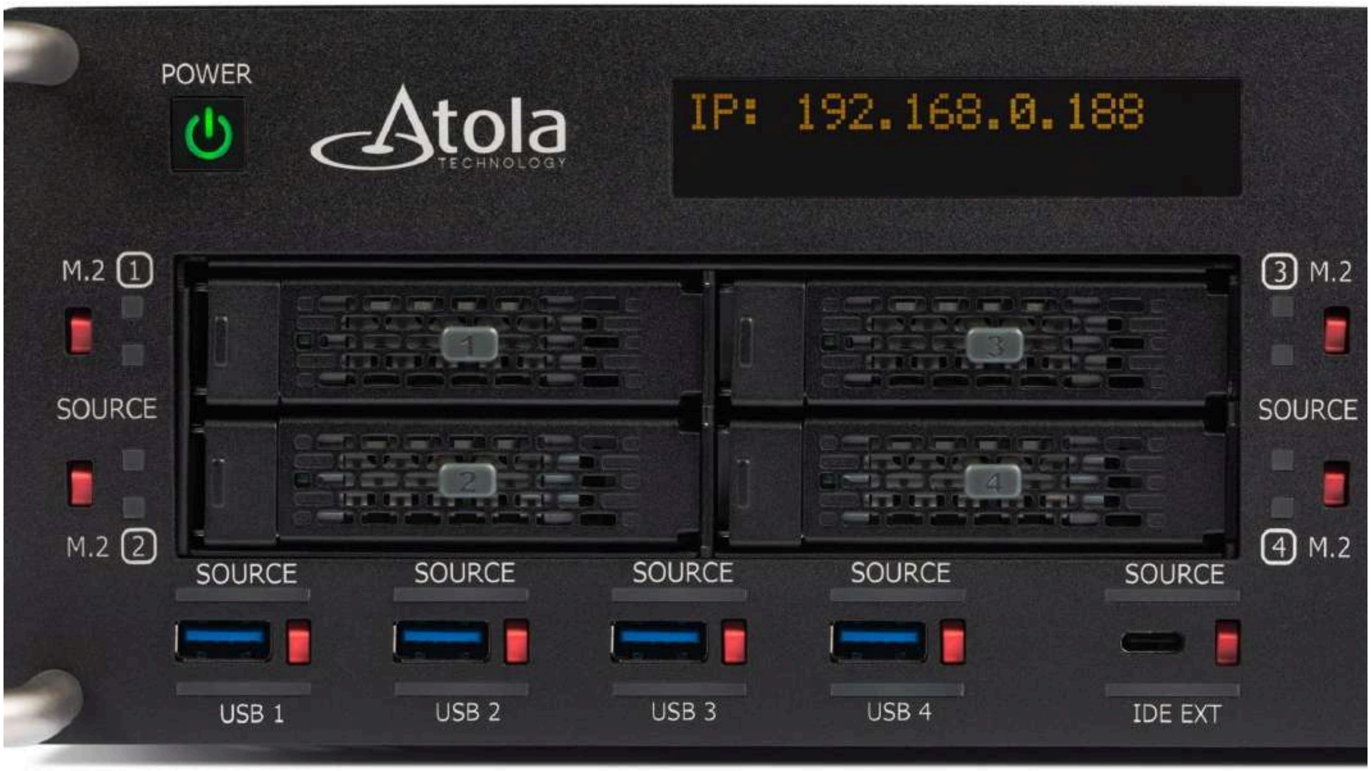
After all the reconfigurations, connect TaskForce 2, NAS and your PC or laptop to the router using Ethernet ports and connect to the Shared Folder as described above.

Connecting drives & starting Atola TaskForce 2

This page provides information about the startup procedure of Atola TaskForce 2, to ensure the safe and effective operation of the unit.

Powering on TaskForce

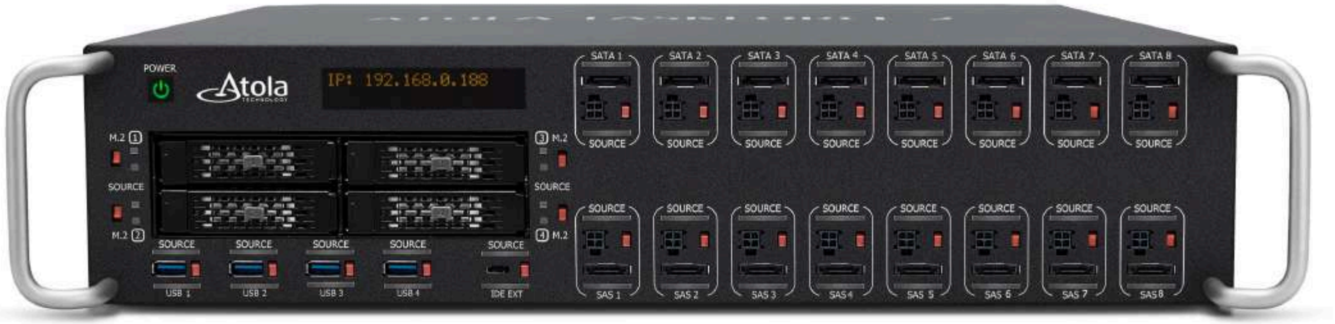
The power button is located on the front panel of the unit. To start TaskForce, press the power button.



Booting

The booting process takes up to 3 minutes.

Once booting is completed, the IP screen on the front panel will display either the "*Kiosk mode*" message or an IP address if the unit is connected to the local network using an Ethernet cable. At this point, the unit is ready for operation.



Connecting drives

TaskForce supports SAS, SATA, USB, NVMe M.2/U.2 PCIe, and IDE drives via its 25 ports, as well as other storage devices via Thunderbolt, Apple PCIe, and M.2 SSD extension modules.

To ensure both TaskForce and the devices connected to it are used properly and safely, read the instructions below.

Connecting M.2 devices

M.2 ports support hotplug to allow for drives to be regularly swapped, without restarting the whole system. To connect an M.2 drive to TaskForce 2, do the following:

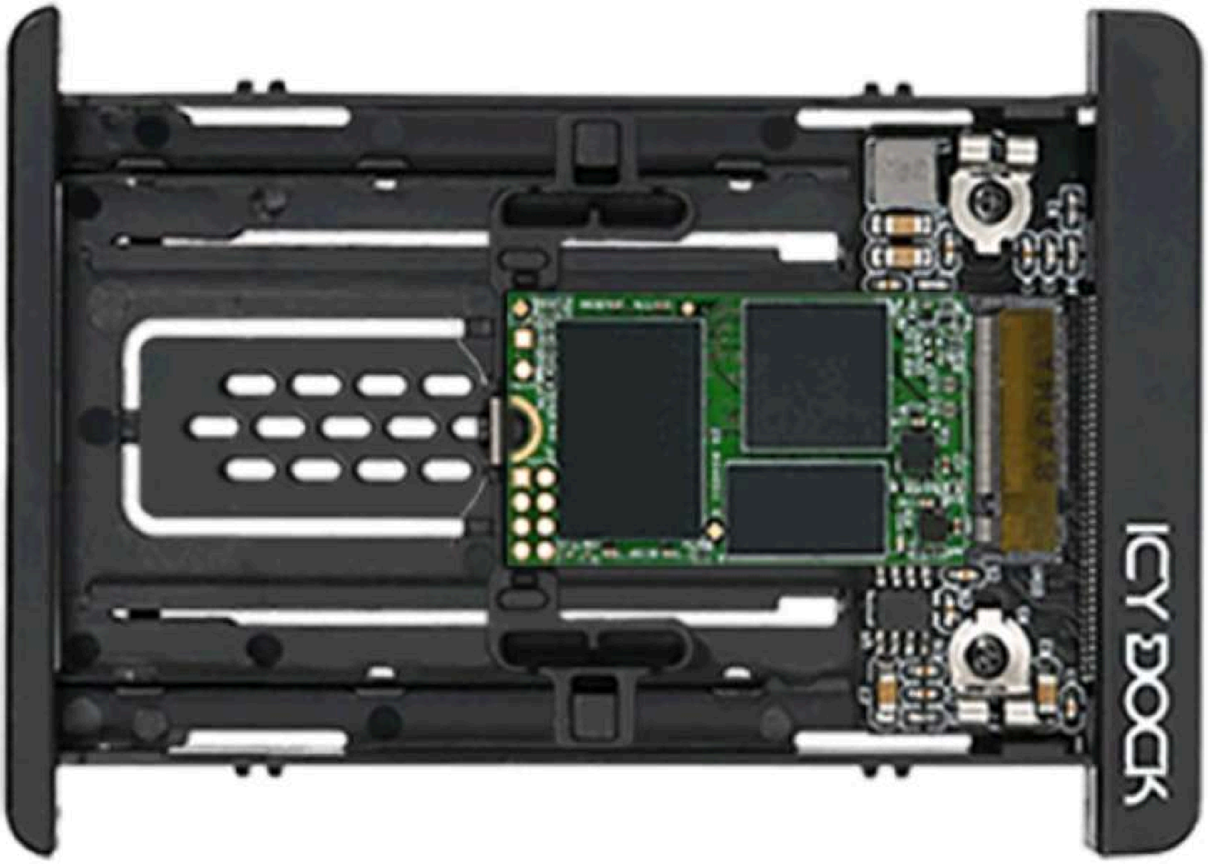
1. Push the tray ejection button located on the left side of an M.2 tray.
2. Pull the M.2 tray out from its bay.

3. Remove the 4 screws at the bottom side of the M.2 tray with a PH1 screwdriver.

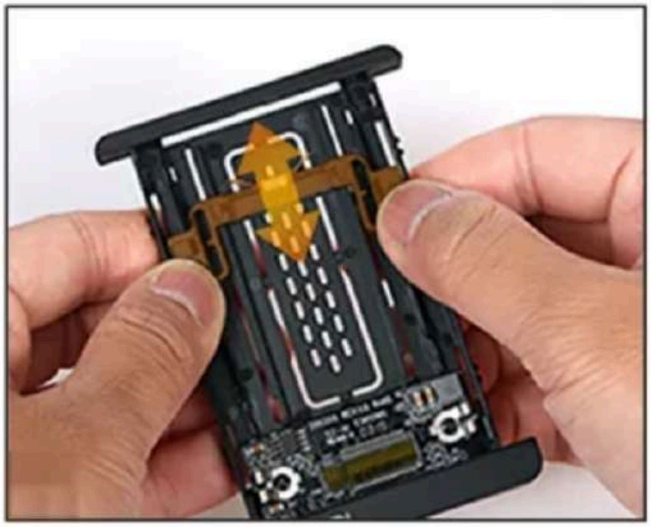
4. Slide the black Icy Dock adapter to the side to remove it out of the tray.

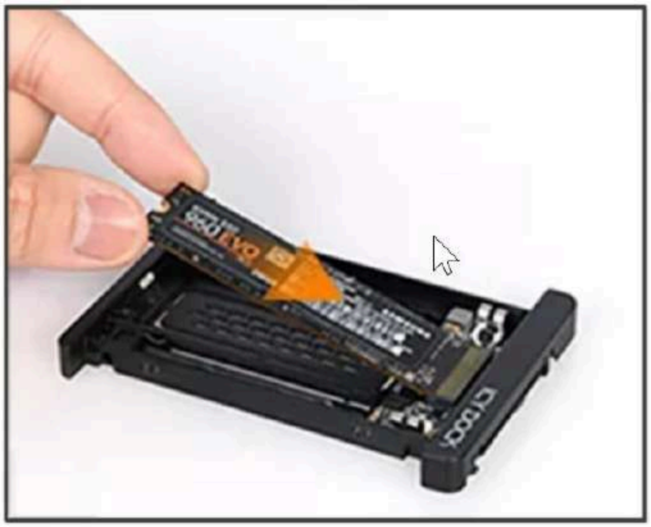
5. Snap off the heatsink of the Icy Dock adapter by pushing it up from the sides.

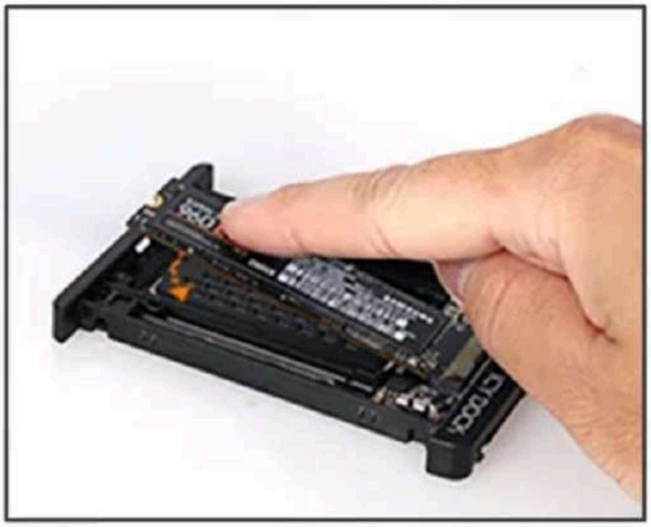
6. An adjustable M.2 locker slides to accommodate all the standard M.2 PCIe NVMe SSD drive lengths, including 2230 (30mm), 2242 (42mm), 2260 (60mm), and 2280 (80mm). Adjust the M.2 locker to the drive length.

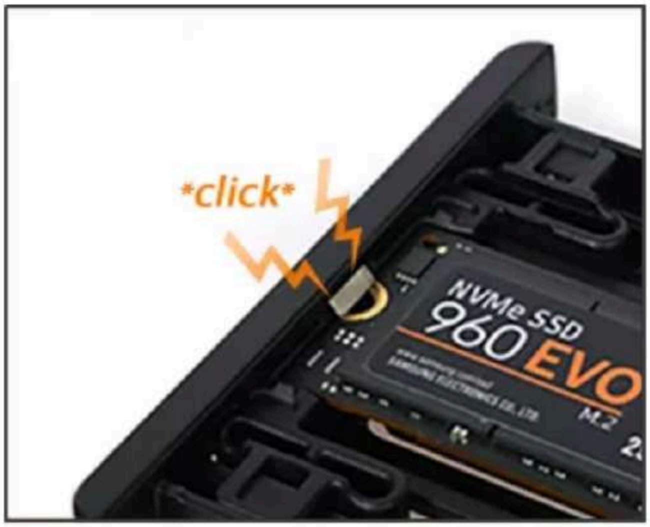


7. Insert the M.2 drive into the M.2 connector and then slightly press the drive down. A spring latch locks the drive with a “click” sound. To release the spring latch, slide the locker open by moving the two plastic levers situated on both sides of the drive.





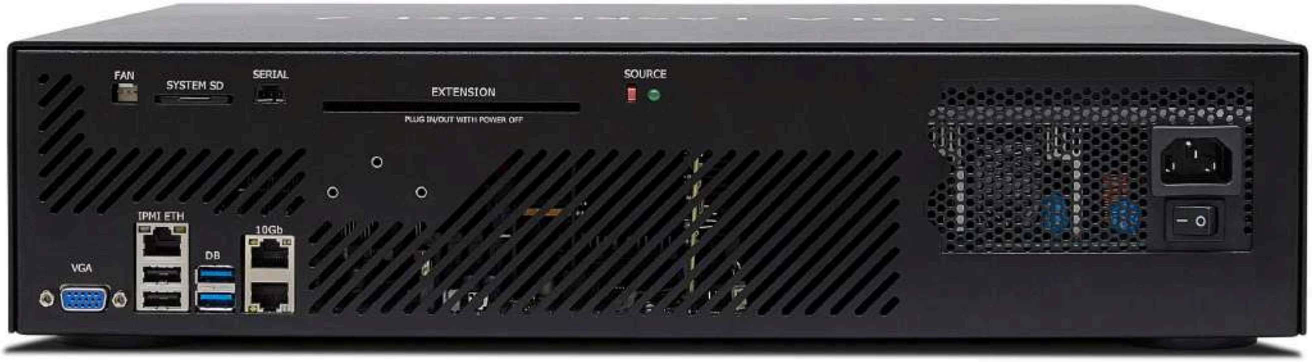




8. Once the drive is plugged into a connector and secured with a latch, snap the heat sink lid on.
9. Slide the Icy Dock adapter back into the M.2 tray.
10. Use at least one screw to secure the adapter onto the tray.
11. **Important:** Make sure that the U.2 connector of the adapter faces the bay and the heatsink with the “Icy Dock” logo faces up.
12. Insert the M.2 tray back into the M.2 bay, make sure it is pushed inside all the way, and then close the lock of the tray.

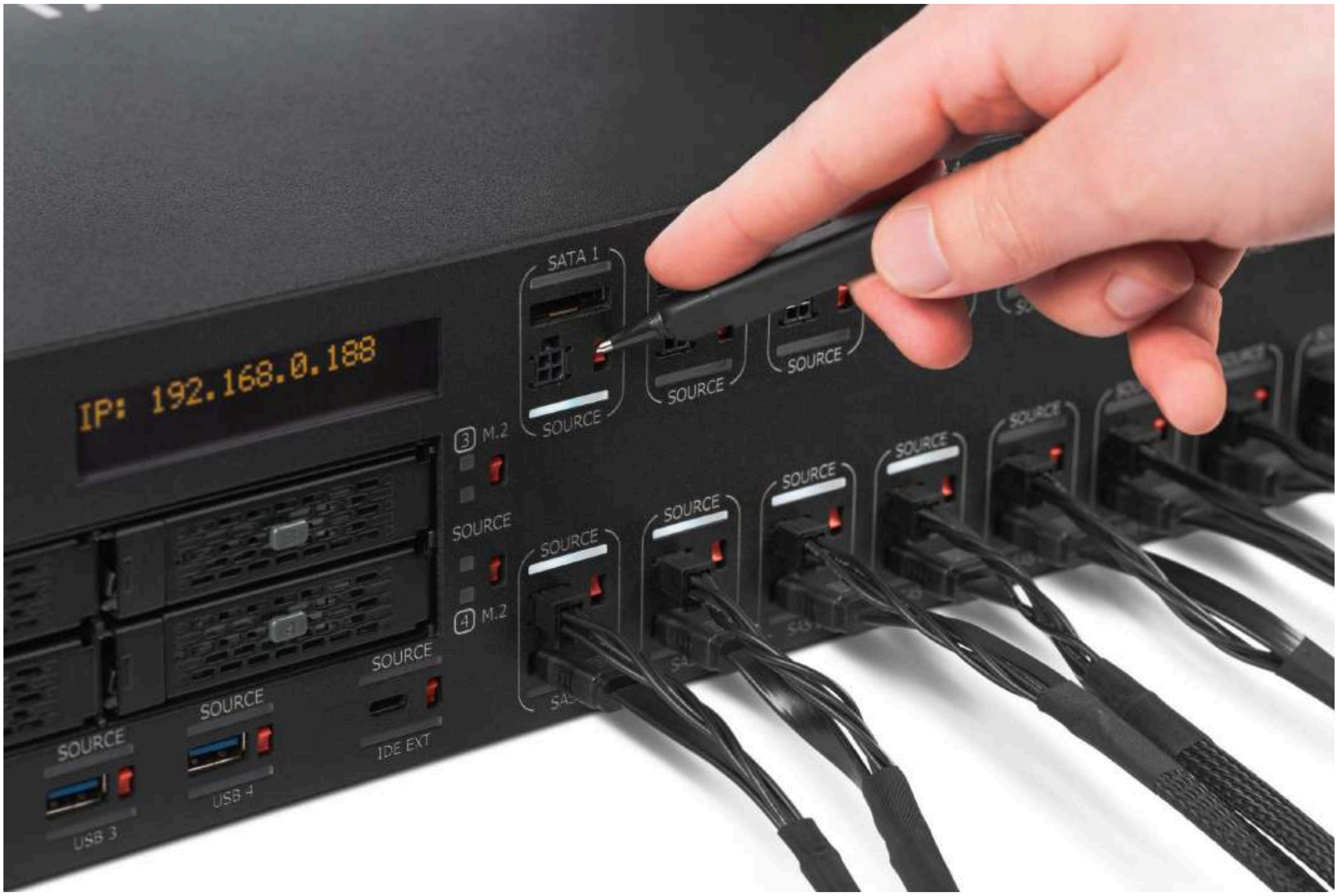
Connecting extensions

Before connecting an extension module, make sure TaskForce is powered off. Plug the extension module into the extension slot located on the back panel of TaskForce and power the unit on.



Hardware write protection

Each port is equipped with an individual Source switch enabling hardware write protection on the port. To make sure data on an evidence drive is not overwritten, check if the port is in the source before connecting the drive.



Connecting SATA & SAS drives

TaskForce has 8 SATA and 8 SATA/SAS ports. When a drive is connected to TaskForce, the port is powered off by default, therefore the device is not immediately identified.

To identify the device, click the **Devices** button in the top panel of the TaskForce interface, and TaskForce will start drive identification process on all ports. The system ensures a sustainable overall power consumption in situations when many drives are plugged in. That's why drives are powered not all at once but sequentially, in a matter of a few seconds.

Powering off TaskForce

To power off the TaskForce hardware unit:

1. In TaskForce window, stop all active tasks.
2. Press the power button on the front panel of the unit for 5 seconds.

Supported Drives

Atola TaskForce 2 supports all 1.8-inch, 2.5-inch, 3.5-inch IDE, SATA, SAS and USB hard drives, USB Flash media as well as SD, Compactflash, and Memory Stick cards via a generic USB Card Reader. Its four ports for NVMe SSDs supporting the following form factors: M.2, U.2, U.3.

TaskForce 2 can also work with the following drive types using proprietary Atola extension modules:

- M.2 NVMe/PCIe/SATA SSDs
- latest Apple SSDs via Thunderbolt extension
- the newest PCIe SSDs from Apple MacBooks (2013 - 2015)

Remote image acquisition can be performed using the iSCSI protocol. To do this, you need to mount a drive on another PC as an iSCSI target.

Most functions of Atola TaskForce 2 will work with any hard drive or flash card with either IDE, SATA-1/2/3 or USB-1/2/3 interface (including those attached via adapters).

To ensure high quality and efficiency of our tools, we test them on hundreds of storage devices.

Head selection works for the following HDD models

- SATA and IDE Seagate hard drives (including F3 series)
- SATA and IDE Western Digital, HGST hard drives with exception of some models released since 2018
- SATA and IDE Hitachi hard drives
- SATA and IDE Toshiba hard drives: MG, MK, MQ, DT, HD families with exception of some models released since 2018

RAID support: unknown configuration detection, reassembly, and imaging

- RAID 0, 1, 5, 6, 10, JBOD
- Hardware RAID controllers: Adaptec, Areca, HP, Dell, LSI, Intel RST, IBM ServeRAID, other generic controllers
- Software RAID: mdadm
- Synology NAS RAID
- File systems: NTFS, exFAT, ext4/3/2, XFS, ZFS, Btrfs, APFS, HFS/HFS+, FAT32/16

TaskForce drive identification

Atola TaskForce is designed to perform multiple processes simultaneously and provide its users with unprecedented flexibility when it comes to a variety of devices and configurations in which they can be used. TaskForce also efficiently communicates how a device is being used and helps a user to handle drives correctly.

Switch between the Source and Target mode

When connecting a drive to the system, make sure the right mode is set on the port: in the source mode, an evidence drive is automatically write-protected. It can only be changed with Source hardware switches.

Source hardware switches.

Initial drive identification

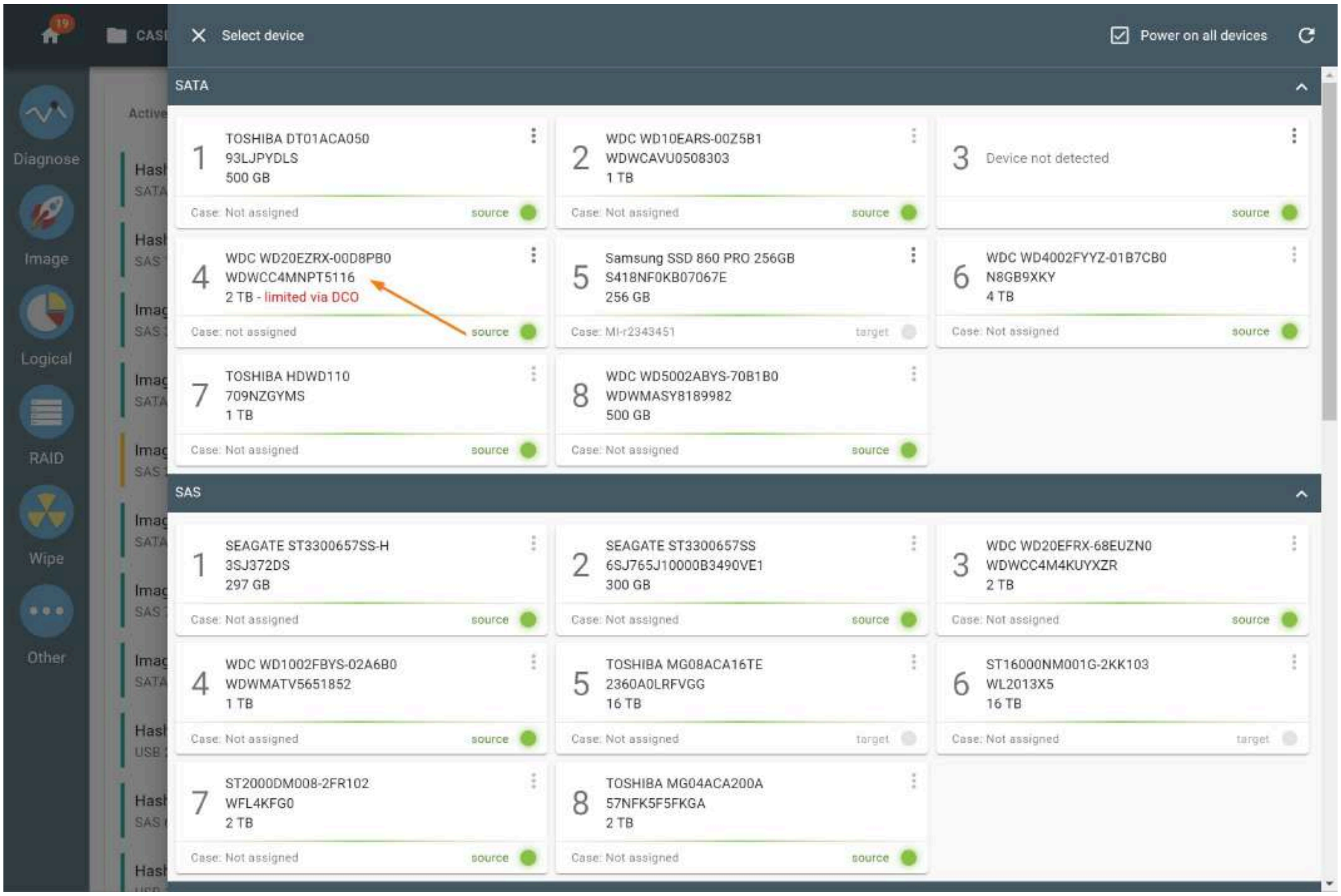
As soon as you choose a particular task or click **Devices** in the top bar, TaskForce starts sequentially supplying power and sending commands to identify all connected devices.

After a connected drive receives power supply and identification commands from the unit, it responds with device info including:

- device model and serial number;
- device capacity;
- limitations of the drive.

Detection of password protection and HPA/DCO/AMA restrictions

TaskForce software also immediately detects whether the drive is locked by an ATA password or the drive's max readable address is limited via HPA/DCO/AMA. The unit indicates these restrictions and notifies a user about those with the red color indication in the device menu.



☑ Power on all devices

SATA

1 TOSHIBA DT01ACA050
93LJPYDLS
500 GB
Case: Not assigned — source

2 WDC WD10EARS-00Z5B1
WDWCAVU0508303
1 TB
Case: Not assigned — source

3 Device not detected
source

4 WDC WD20EZRX-00D8PB0
WDWCC4MNPT5116
2 TB - limited via DCO
Case: not assigned — source

5 Samsung SSD 860 PRO 256GB
S418NF0KB07067E
256 GB
Case: MI-r2343451 — target

6 WDC WD4002FYYZ-01B7CB0
N8GB9XKY
4 TB
Case: Not assigned — source

7 TOSHIBA HDWD110
709NZGYMS
1 TB
Case: Not assigned — source

8 WDC WD5002ABYS-70B1B0
WDWMASY8189982
500 GB
Case: Not assigned — source

SAS

1 SEAGATE ST3300657SS-H
3SJ372DS
297 GB
Case: Not assigned — source

2 SEAGATE ST3300657SS
6SJ765J10000B3490VE1
300 GB
Case: Not assigned — source

3 WDC WD20EFRX-68EUZN0
WDWCC4M4KUYXZR
2 TB
Case: Not assigned — source

4 WDC WD1002FBYS-02A6B0
WDWMATV5651852
1 TB
Case: Not assigned — source

5 TOSHIBA MG08ACA16TE
2360A0LRFVGG
16 TB
Case: Not assigned — target

6 ST16000NM001G-2KK103
WL2013X5
16 TB
Case: Not assigned — target

7 ST2000DM008-2FR102
WFL4KFG0
2 TB
Case: Not assigned — source

8 TOSHIBA MG04ACA200A
57NFK5F5FKGA
2 TB
Case: Not assigned — source

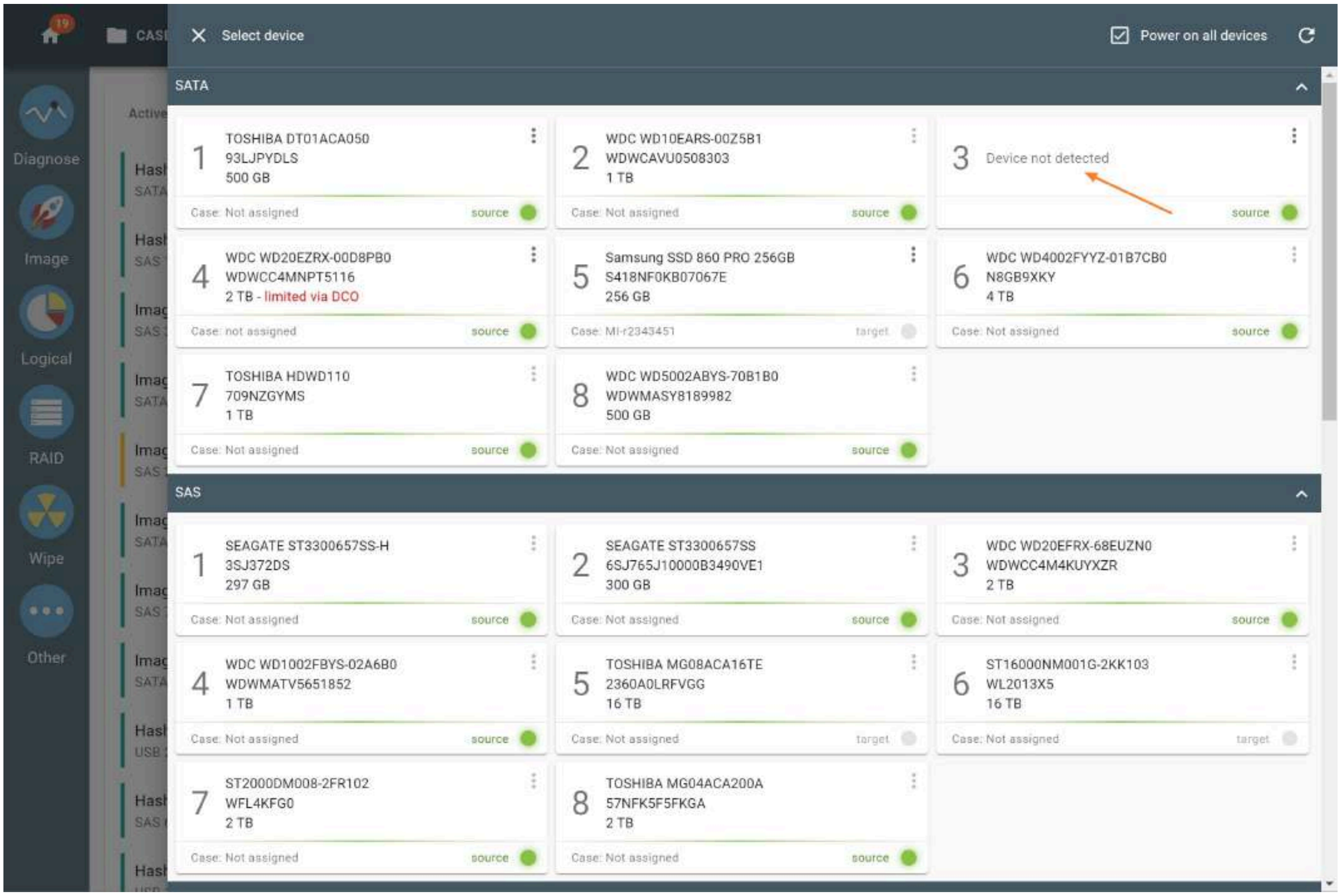
TaskForce detects ATA, HPA/DCO/AMA limitations

These indicators allow a user to make informed decisions on how to proceed with the device, whether unlocking is required to get access to the whole drive space before starting an imaging session.

The 'Device not detected' notification

Notification **Device not detected** may point to one of these issues:

- there is no device on the port;
- the cable is not properly plugged in;
- the device is connected to another port;
- the device is heavily damaged.



SATA

1 TOSHIBA DT01ACA050
93LJPYDLS
500 GB
Case: Not assigned source ●

2 WDC WD10EARS-00Z5B1
WDWCAVU0508303
1 TB
Case: Not assigned source ●

3 Device not detected
source ●

4 WDC WD20EZRX-00D8PB0
WDWCC4MNPT5116
2 TB - limited via DCO
Case: not assigned source ●

5 Samsung SSD 860 PRO 256GB
S418NF0KB07067E
256 GB
Case: MI-r2343451 target ○

6 WDC WD4002FYYZ-01B7CB0
N8GB9XKY
4 TB
Case: Not assigned source ●

7 TOSHIBA HDWD110
709NZGYMS
1 TB
Case: Not assigned source ●

8 WDC WD5002ABYS-70B1B0
WDWMASY8189982
500 GB
Case: Not assigned source ●

SAS

1 SEAGATE ST3300657SS-H
3SJ372DS
297 GB
Case: Not assigned source ●

2 SEAGATE ST3300657SS
6SJ765J10000B3490VE1
300 GB
Case: Not assigned source ●

3 WDC WD20EFRX-68EUZN0
WDWCC4M4KUYXZR
2 TB
Case: Not assigned source ●

4 WDC WD1002FBYS-02A6B0
WDWMATV5651852
1 TB
Case: Not assigned source ●

5 TOSHIBA MG08ACA16TE
2360A0LRFVGG
16 TB
Case: Not assigned target ○

6 ST16000NM001G-2KK103
WL2013X5
16 TB
Case: Not assigned target ○

7 ST2000DM008-2FR102
WFL4KFG0
2 TB
Case: Not assigned source ●

8 TOSHIBA MG04ACA200A
57NFK5F5FKGA
2 TB
Case: Not assigned source ●

Device not detected

Re-identify device

You might want to re-identify a device in one of the following cases:

- A device hasn't been detected from the first try.
- You have connected another device to the drive port.

To re-identify a single device from the **Select device** panel:

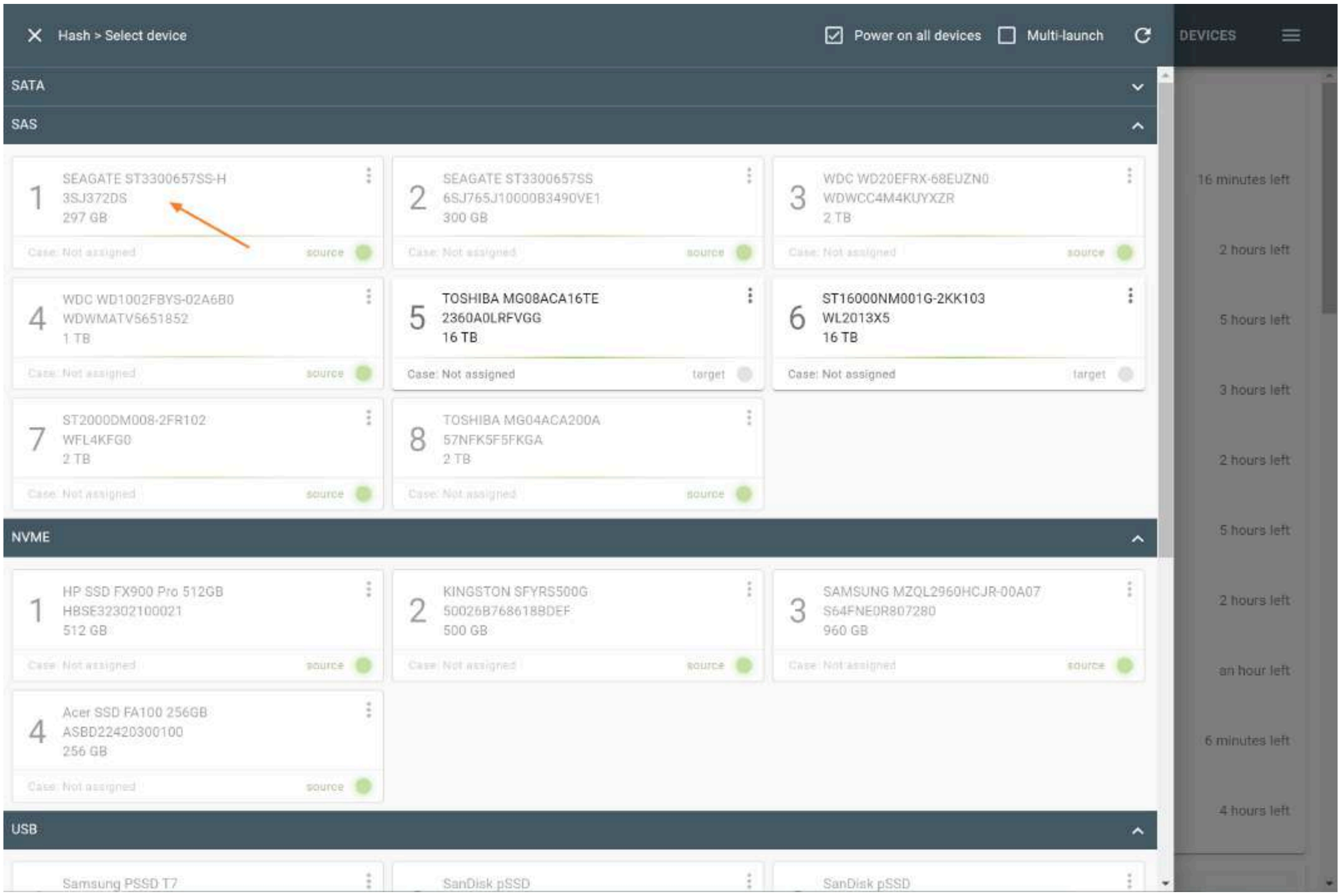
1. In the port with your device, click the **More** icon (the one with three dots).
2. Select Re-identify.

To re-identify all connected devices, use the **Re-identify** button in the top right corner of the **Select device** panel. It affects only the devices in unfolded sections of the panel.

You can also re-identify a single device from its device page by clicking the **Re-identify** button at the bottom.

When the drive port is unavailable

If a source drive is busy with a running operation, the port will be temporarily unavailable for selection when launching other tasks. In such a case, the fonts in the respective box will be a lighter shade of grey, making the port unclickable.



SATA

SAS

1 SEAGATE ST3300657SS-H
3SJ372DS
297 GB
Case: Not assigned — source

2 SEAGATE ST3300657SS
6SJ765J10000B3490VE1
300 GB
Case: Not assigned — source

3 WDC WD20EFRX-68EUZN0
WDWCC4M4KUYXZR
2 TB
Case: Not assigned — source

4 WDC WD1002FBYS-02A6B0
WDWMATV5651852
1 TB
Case: Not assigned — source

5 TOSHIBA MG08ACA16TE
2360A0LRFVGG
16 TB
Case: Not assigned — target

6 ST16000NM001G-2KK103
WL2013X5
16 TB
Case: Not assigned — target

7 ST2000DM008-2FR102
WFL4KFG0
2 TB
Case: Not assigned — source

8 TOSHIBA MG04ACA200A
57NFK5F5FKGA
2 TB
Case: Not assigned — source

NVME

1 HP SSD FX900 Pro 512GB
HBSE32302100021
512 GB
Case: Not assigned — source

2 KINGSTON SFYRS500G
50026B768618BDEF
500 GB
Case: Not assigned — source

3 SAMSUNG MZQL2960HCJR-00A07
S64FNE0R807280
960 GB
Case: Not assigned — source

4 Acer SSD FA100 256GB
ASBD22420300100
256 GB
Case: Not assigned — source

USB

Samsung PSSD T7

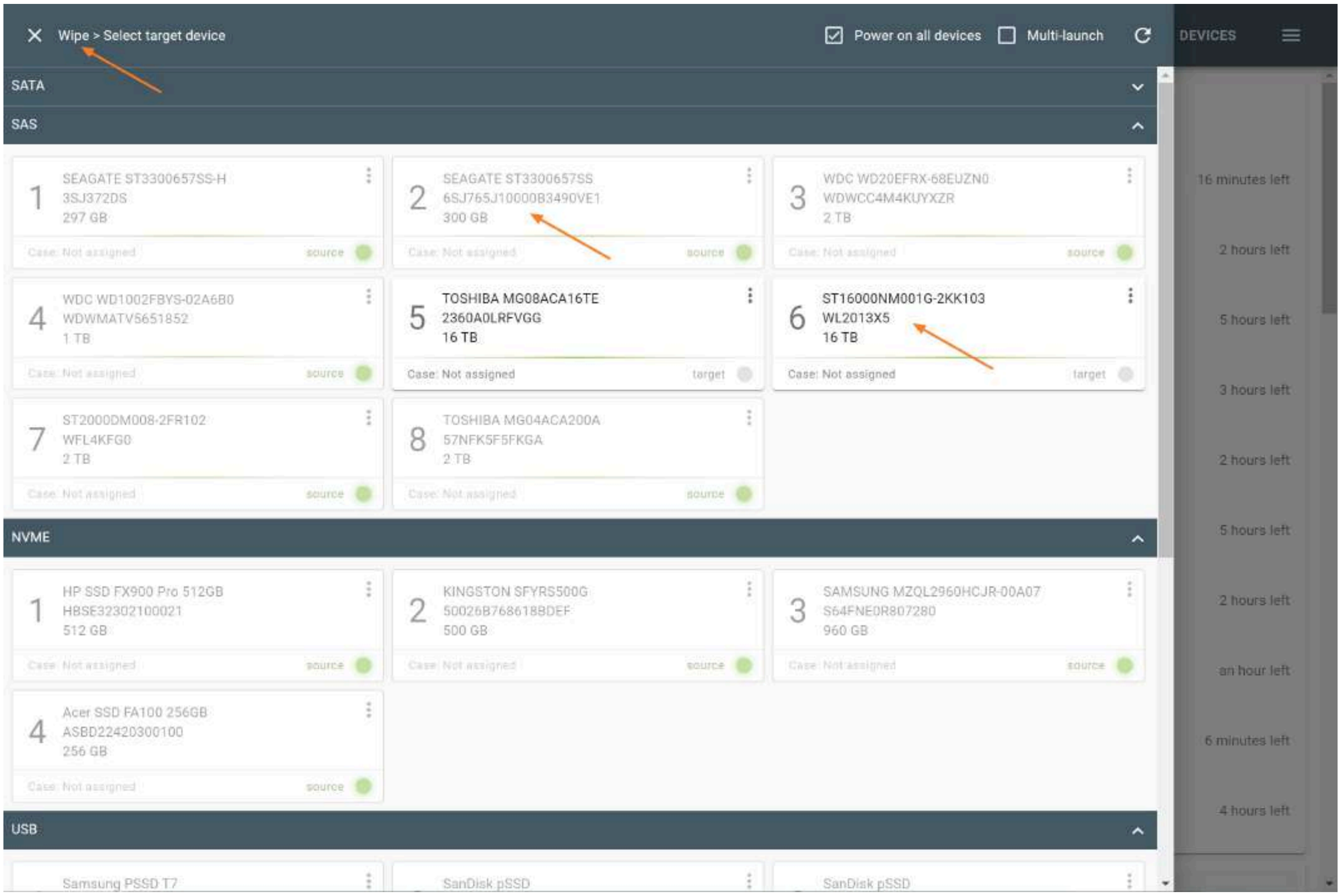
SanDisk pSSD

SanDisk pSSD

16 minutes left
2 hours left
5 hours left
3 hours left
2 hours left
5 hours left
2 hours left
an hour left
6 minutes left
4 hours left

Busy source drive

When selecting a target device for wiping or imaging, source drives are also unavailable to ensure that data on an evidence drive doesn’t get overwritten by mistake.


Wipe > Select target device
☑ Power on all devices
□ Multi-launch
DEVICES
SATA
SAS
1 SEAGATE ST3300657SS-H 3SJ372DS 297 GB Case: Not assigned source
2 SEAGATE ST3300657SS 6SJ765J10000B3490VE1 300 GB Case: Not assigned source
3 WDC WD20EFRX-68EUZN0 WDWCC4M4KUYXZR 2 TB Case: Not assigned source
4 WDC WD1002FBYS-02A6B0 WDWMATV5651852 1 TB Case: Not assigned source
5 TOSHIBA MG08ACA16TE 2360A0LRFVGG 16 TB Case: Not assigned target
6 ST16000NM001G-2KK103 WL2013X5 16 TB Case: Not assigned target
7 ST2000DM008-2FR102 WFL4KFG0 2 TB Case: Not assigned source
8 TOSHIBA MG04ACA200A 57NFK5F5FKGA 2 TB Case: Not assigned source
NVME
1 HP SSD FX900 Pro 512GB HBSE32302100021 512 GB Case: Not assigned source
2 KINGSTON SFYRS500G 50026B768618BDEF 500 GB Case: Not assigned source
3 SAMSUNG MZQL2960HCJR-00A07 S64FNE0R807280 960 GB Case: Not assigned source
4 Acer SSD FA100 256GB ASBD22420300100 256 GB Case: Not assigned source
USB
Samsung PSSD T7
SanDisk pSSD
SanDisk pSSD
16 minutes left
2 hours left
5 hours left
3 hours left
2 hours left
5 hours left
2 hours left
an hour left
6 minutes left
4 hours left

Selecting target device

Add a device to a case

Once a drive is connected to a drive port and identified, you can add it to a new or existing case right from the **Select device** panel:

1. In the port with your device, click the **More** icon (the one with three dots), and then select **Add case**.
2. Choose between **Create new case** or **Select existing case** and click **Next**.
3. Enter details for a new case or select an existing case from a table.

Power off and power on a drive

From the **Select device** panel, you can power off and power on any connected device. To do that, in the port with your device, click the **More** icon (the one with three dots), and then select the **Power on** or **Power off** option.

Power on all devices: if this checkbox at the top right is selected, TaskForce automatically powers on all plugged drives after the sliding panel appears.

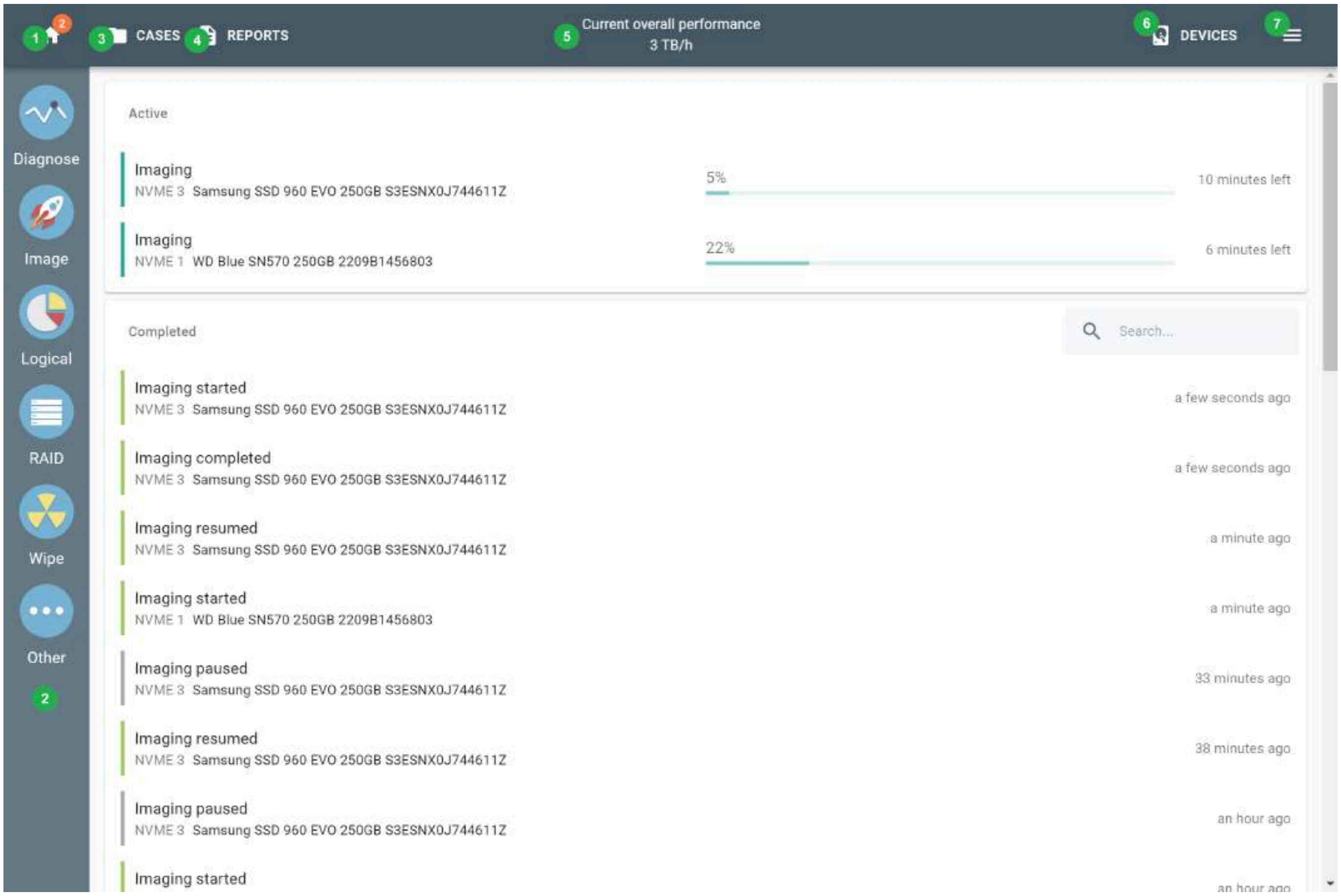
You can also power a device on and off from a device page, by clicking the respective button at the bottom of the page.

When a device is idle for 5 minutes, TaskForce automatically powers it off. This is the setting that you can disable.

However, we recommend powering off a device before disconnecting it from TaskForce.

Atola TaskForce: Main window

This article helps in understanding TaskForce's main window, its controls and buttons and how to use them.



Active

Imaging
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — 5% — 10 minutes left

Imaging
NVME 1 WD Blue SN570 250GB 2209B1456803 — 22% — 6 minutes left

Completed

Imaging started
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — a few seconds ago

Imaging completed
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — a few seconds ago

Imaging resumed
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — a minute ago

Imaging started
NVME 1 WD Blue SN570 250GB 2209B1456803 — a minute ago

Imaging paused
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — 33 minutes ago

Imaging resumed
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — 38 minutes ago

Imaging paused
NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z — an hour ago

Imaging started — an hour ago

An overall view of the TaskForce 2 main window: 1 - Home icon, 2 - Taskbar, 3 - Cases button, 4 - Reports button, 5 - Current overall performance, 6 - Devices button, 7 - Menu.

1. Home icon

The **Home** button brings you back to the **Home screen**. This is where you can check the active and recently completed tasks in the respective sections of the screen.

The number of current active processes is indicated next to the **Home icon** in a small orange circle.

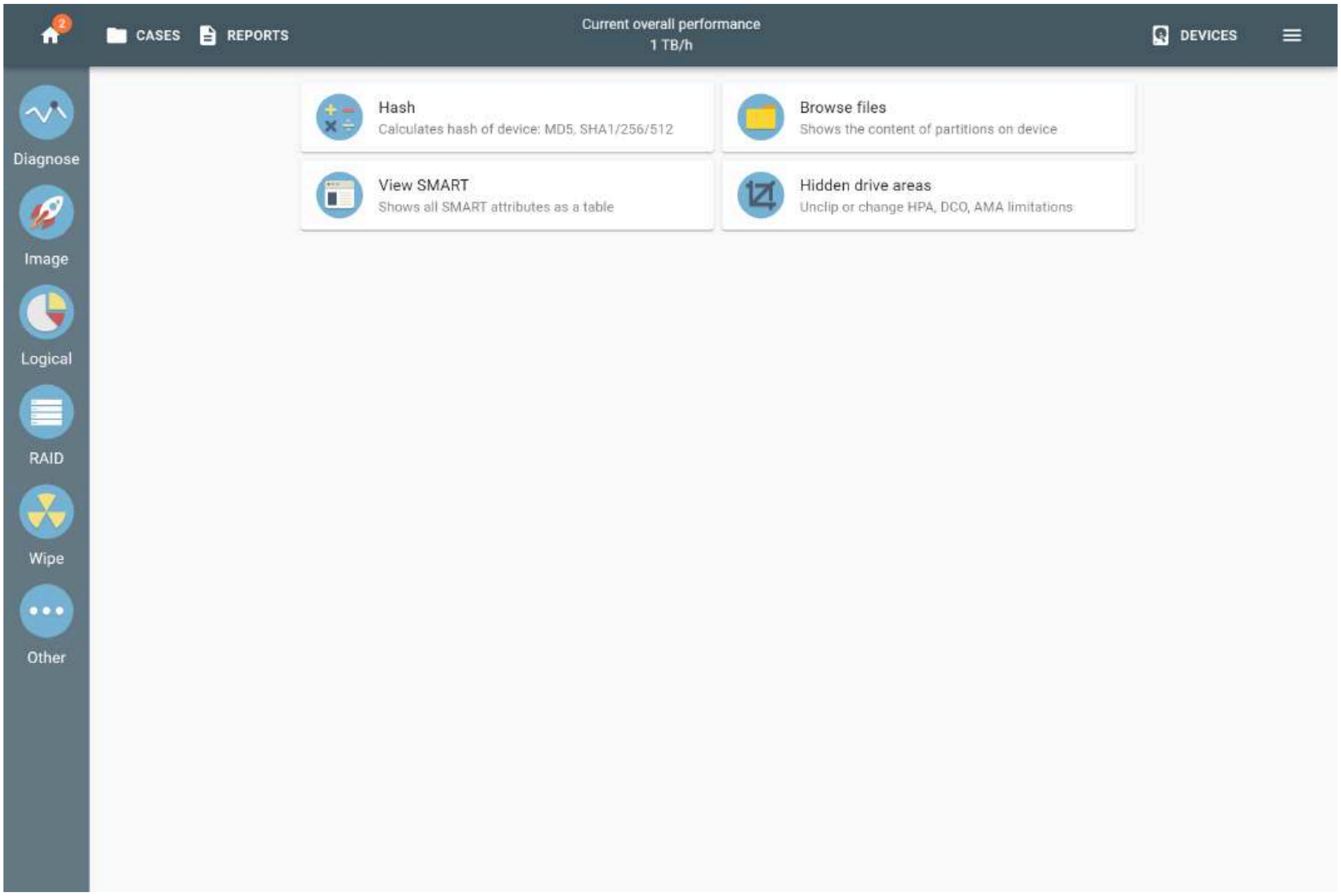
2. Taskbar

The **Taskbar** on the left shows main TaskForce operations:

1. Diagnose
2. Image
3. Logical
4. RAID
5. Wipe

Click the **Other** button in the **Taskbar** to access 4 more important TaskForce operations:

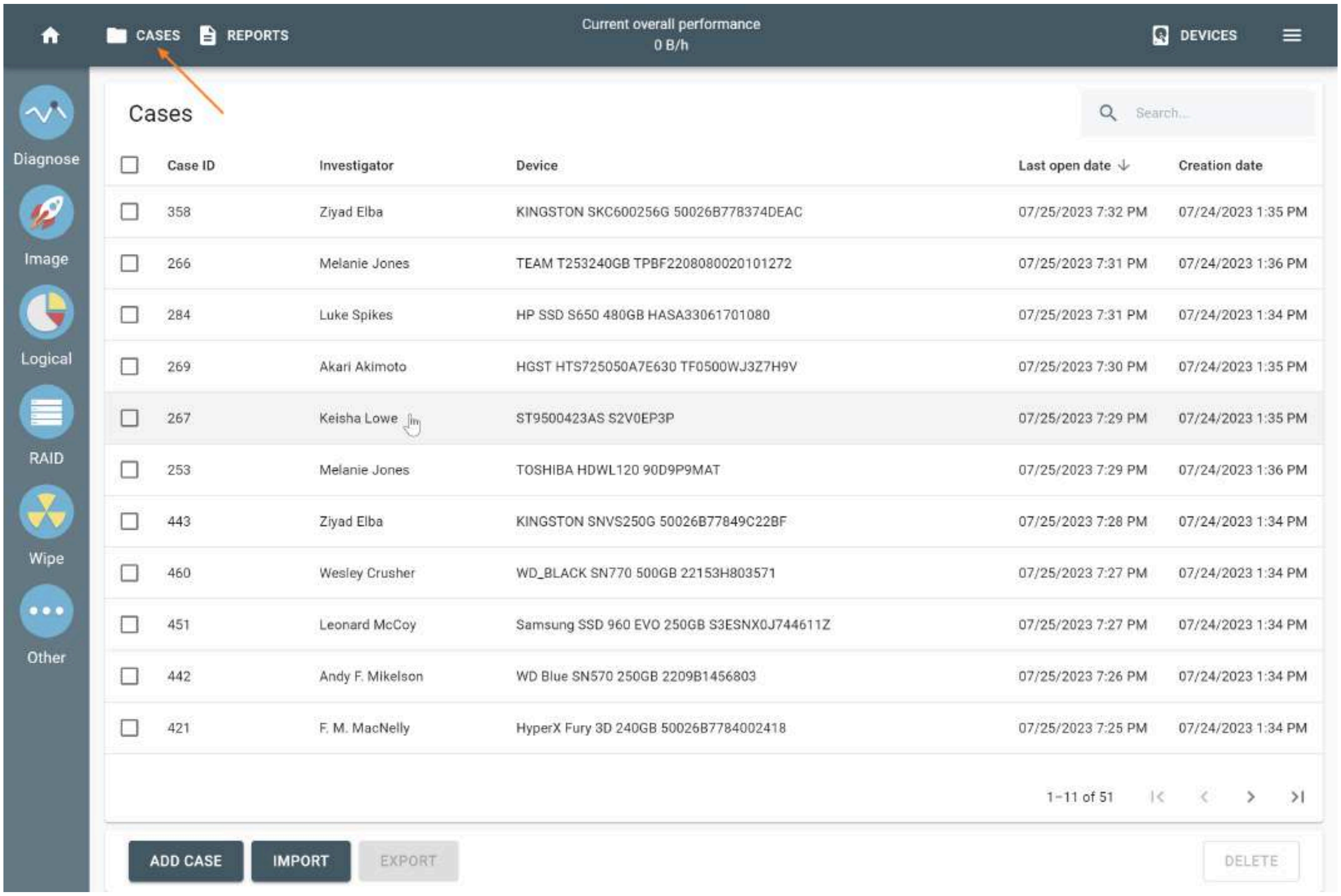
1. Hash: Calculates hash of a device: MD5, SHA-1, SHA-256, SHA-512.
2. View SMART: Shows all SMART attributes as a table.
3. Browse files: Shows the content of partitions on a device.
4. Hidden drive areas: Lets you to unclip or change HPA, DCO, AMA limitations.


2
CASES
REPORTS
Current overall performance
1 TB/h
DEVICES
Diagnose
Image
Logical
RAID
Wipe
Other
Hash
Calculates hash of device: MD5, SHA1/256/512
Browse files
Shows the content of partitions on device
View SMART
Shows all SMART attributes as a table
Hidden drive areas
Unclip or change HPA, DCO, AMA limitations

Section with other tasks: Hash, View SMART, Browse files, Hidden drive areas.

3. Cases

By clicking the **Cases** button in the top panel you get to the **Cases** page with a list of the latest cases. With the help of the **Search bar** you can find a specific case. The cases are available for import and export between different TaskForce units.

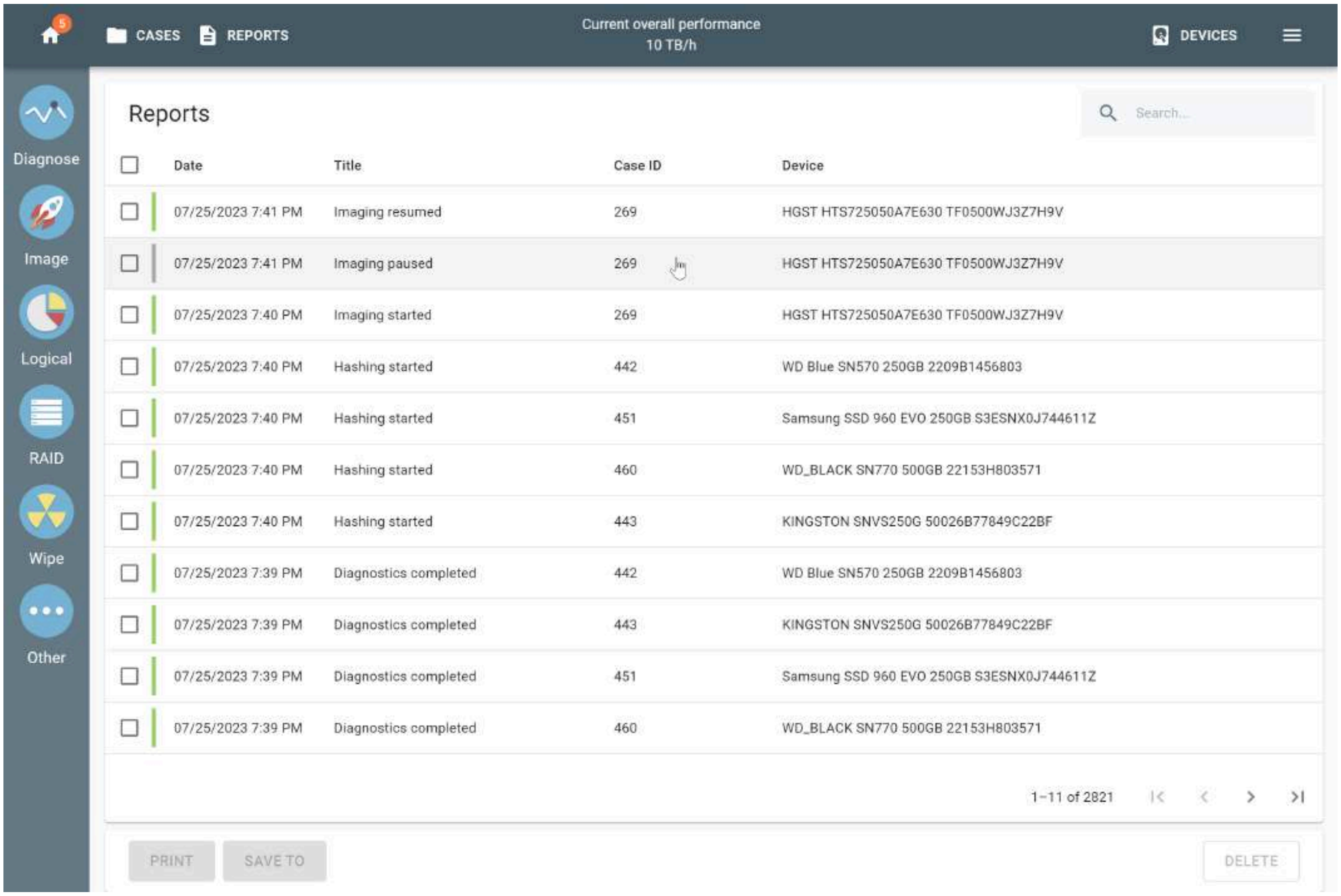


□	Case ID	Investigator	Device	Last open date ↓	Creation date
□	358	Ziyad Elba	KINGSTON SKC600256G 50026B778374DEAC	07/25/2023 7:32 PM	07/24/2023 1:35 PM
□	266	Melanie Jones	TEAM T253240GB TPBF2208080020101272	07/25/2023 7:31 PM	07/24/2023 1:36 PM
□	284	Luke Spikes	HP SSD S650 480GB HASA33061701080	07/25/2023 7:31 PM	07/24/2023 1:34 PM
□	269	Akari Akimoto	HGST HTS725050A7E630 TF0500WJ3Z7H9V	07/25/2023 7:30 PM	07/24/2023 1:35 PM
□	267	Keisha Lowe	ST9500423AS S2V0EP3P	07/25/2023 7:29 PM	07/24/2023 1:35 PM
□	253	Melanie Jones	TOSHIBA HDWL120 90D9P9MAT	07/25/2023 7:29 PM	07/24/2023 1:36 PM
□	443	Ziyad Elba	KINGSTON SNVS250G 50026B77849C22BF	07/25/2023 7:28 PM	07/24/2023 1:34 PM
□	460	Wesley Crusher	WD_BLACK SN770 500GB 22153H803571	07/25/2023 7:27 PM	07/24/2023 1:34 PM
□	451	Leonard McCoy	Samsung SSD 960 EVO 250GB S3ESNX0J744611Z	07/25/2023 7:27 PM	07/24/2023 1:34 PM
□	442	Andy F. Mikelson	WD Blue SN570 250GB 2209B1456803	07/25/2023 7:26 PM	07/24/2023 1:34 PM
□	421	F. M. MacNelly	HyperX Fury 3D 240GB 50026B7784002418	07/25/2023 7:25 PM	07/24/2023 1:34 PM

An overall view of the Cases page with a list of the latest cases.

4. Reports

By clicking the **Reports** button in the top panel you get to the **Reports** page that is equipped with a similar search bar. The reports can be selected and printed directly from this page.



Current overall performance
10 TB/h

Reports

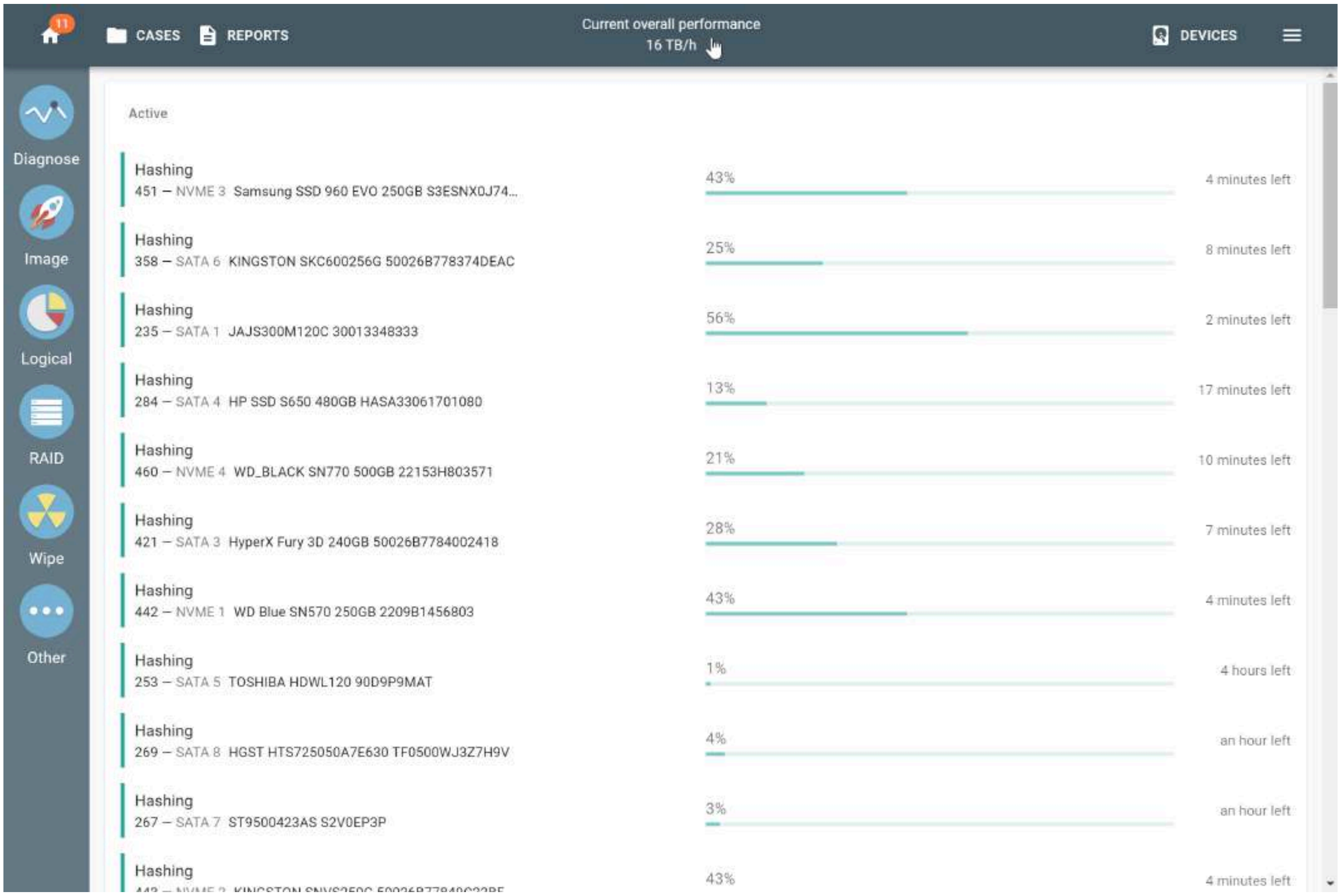
☐	Date	Title	Case ID	Device
☐	07/25/2023 7:41 PM	Imaging resumed	269	HGST HTS725050A7E630 TF0500WJ3Z7H9V
☐	07/25/2023 7:41 PM	Imaging paused	269	HGST HTS725050A7E630 TF0500WJ3Z7H9V
☐	07/25/2023 7:40 PM	Imaging started	269	HGST HTS725050A7E630 TF0500WJ3Z7H9V
☐	07/25/2023 7:40 PM	Hashing started	442	WD Blue SN570 250GB 2209B1456803
☐	07/25/2023 7:40 PM	Hashing started	451	Samsung SSD 960 EVO 250GB S3ESNX0J744611Z
☐	07/25/2023 7:40 PM	Hashing started	460	WD_BLACK SN770 500GB 22153H803571
☐	07/25/2023 7:40 PM	Hashing started	443	KINGSTON SNVS250G 50026B77849C22BF
☐	07/25/2023 7:39 PM	Diagnostics completed	442	WD Blue SN570 250GB 2209B1456803
☐	07/25/2023 7:39 PM	Diagnostics completed	443	KINGSTON SNVS250G 50026B77849C22BF
☐	07/25/2023 7:39 PM	Diagnostics completed	451	Samsung SSD 960 EVO 250GB S3ESNX0J744611Z
☐	07/25/2023 7:39 PM	Diagnostics completed	460	WD_BLACK SN770 500GB 22153H803571

1–11 of 2821

The Reports page with a list of the latest reports.

5. Current overall performance

To check the **Current overall performance**, click Atola logo in the top panel. This lets you to keep track of the unit’s capacity usage. TaskForce allows running processes at 25 TB/hour and more.



Current overall performance
16 TB/h

Active

Hashing
451 – NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J74...
43%
4 minutes left

Hashing
358 – SATA 6 KINGSTON SKC600256G 50026B778374DEAC
25%
8 minutes left

Hashing
235 – SATA 1 JAJS300M120C 30013348333
56%
2 minutes left

Hashing
284 – SATA 4 HP SSD S650 480GB HASA33061701080
13%
17 minutes left

Hashing
460 – NVME 4 WD_BLACK SN770 500GB 22153H803571
21%
10 minutes left

Hashing
421 – SATA 3 HyperX Fury 3D 240GB 50026B7784002418
28%
7 minutes left

Hashing
442 – NVME 1 WD Blue SN570 250GB 2209B1456803
43%
4 minutes left

Hashing
253 – SATA 5 TOSHIBA HDWL120 90D9P9MAT
1%
4 hours left

Hashing
269 – SATA 8 HGST HTS725050A7E630 TF0500WJ3Z7H9V
4%
an hour left

Hashing
267 – SATA 7 ST9500423AS S2V0EP3P
3%
an hour left

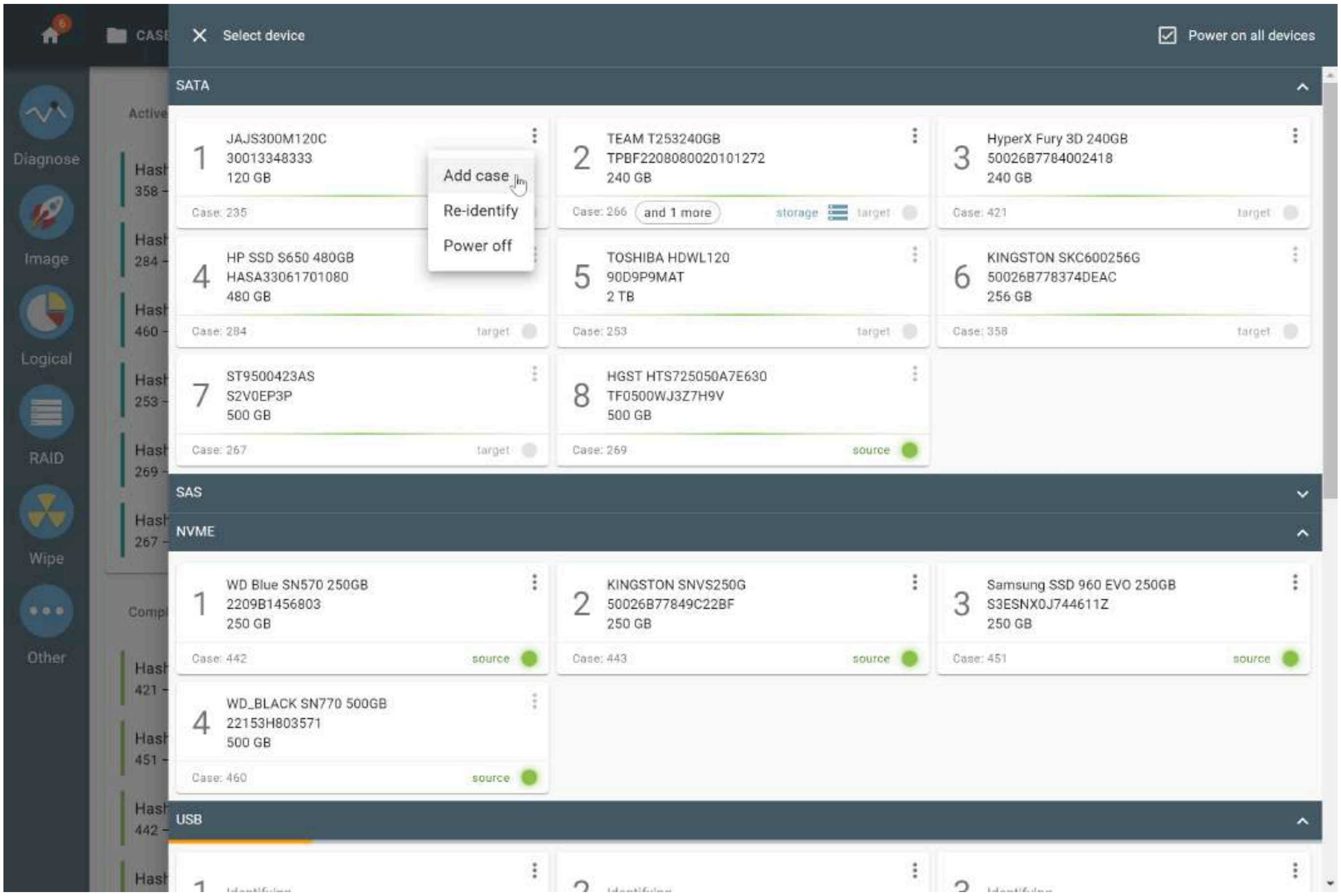
Hashing
443 – NVME 2 KINGSTON SNVS250G 50026B77840C22BE
43%
4 minutes left

Current overall performance shows after you click Atola logo.

6. Devices

Click **Devices** button in the top panel to see all the drives connected to TaskForce to obtain maximum information about each by simply clicking it.

The **Devices** panel provides additional options for working with the drives: add a case for a device, re-identify or power off any device.



SATA

1 JAJS300M120C 30013348333 120 GB — Case: 235

2 TEAM T253240GB TPBF2208080020101272 240 GB — Case: 266 and 1 more — storage — target

3 HyperX Fury 3D 240GB 50026B7784002418 240 GB — Case: 421 — target

4 HP SSD S650 480GB HASA33061701080 480 GB — Case: 284 — target

5 TOSHIBA HDWL120 90D9P9MAT 2 TB — Case: 253 — target

6 KINGSTON SKC600256G 50026B778374DEAC 256 GB — Case: 358 — target

7 ST9500423AS S2V0EP3P 500 GB — Case: 267 — target

8 HGST HTS725050A7E630 TF0500WJ3Z7H9V 500 GB — Case: 269 — source

SAS

NVME

1 WD Blue SN570 250GB 2209B1456803 250 GB — Case: 442 — source

2 KINGSTON SNVS250G 50026B77849C22BF 250 GB — Case: 443 — source

3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z 250 GB — Case: 451 — source

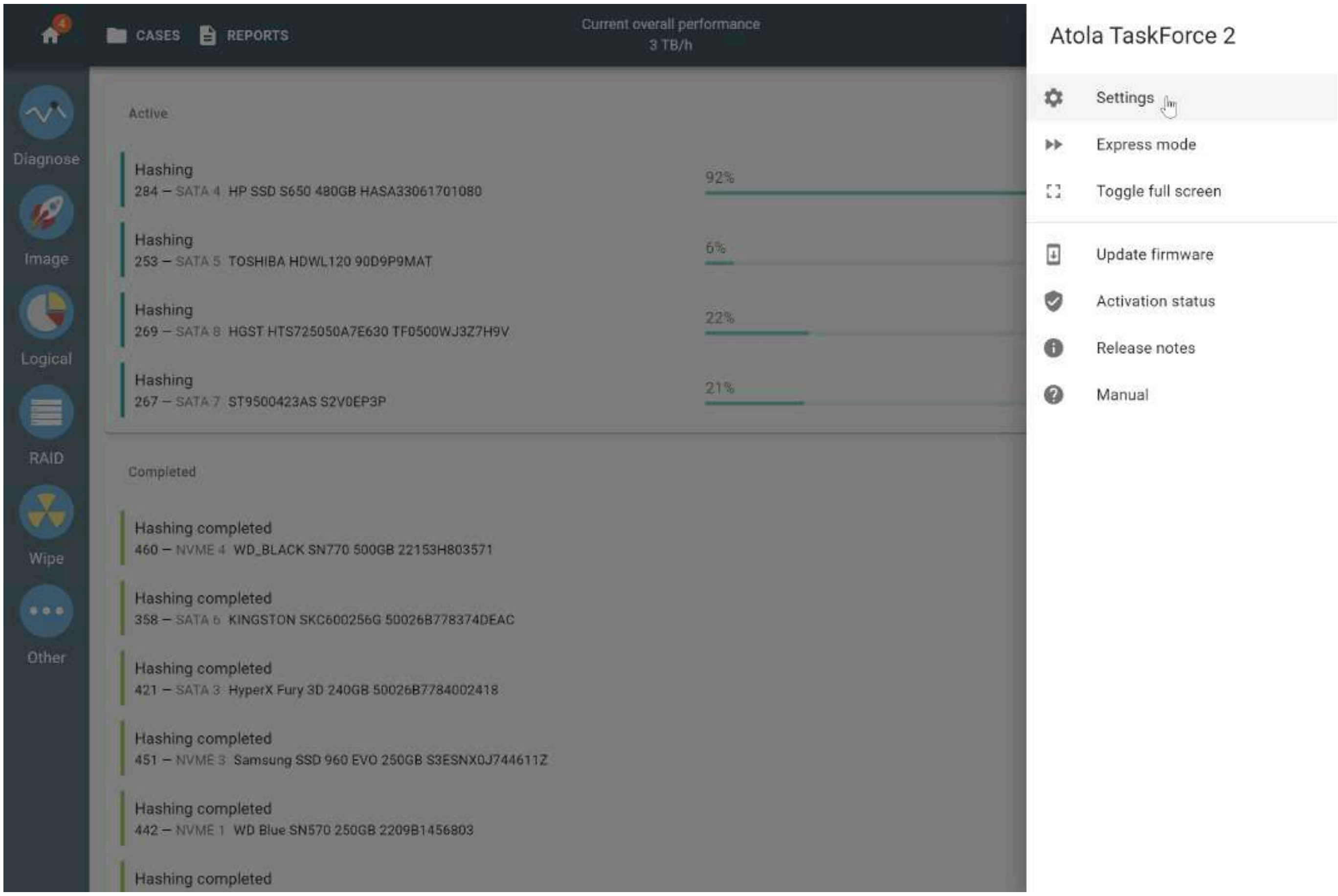
4 WD_BLACK SN770 500GB 22153H803571 500 GB — Case: 460 — source

USB

The Devices panel is expanded and shows all the drives connected to TaskForce.

7. Menu

The **Menu** contains device settings and features that regulate your use of the TaskForce unit.



Current overall performance
3 TB/h

Active

Hashing
284 – SATA 4 HP SSD S650 480GB HASA33061701080 92%

Hashing
253 – SATA 5 TOSHIBA HDWL120 90D9P9MAT 6%

Hashing
269 – SATA 8 HGST HTS725050A7E630 TF0500WJ3Z7H9V 22%

Hashing
267 – SATA 7 ST9500423AS S2V0EP3P 21%

Completed

Hashing completed
460 – NVME 4 WD_BLACK SN770 500GB 22153H803571

Hashing completed
358 – SATA 6 KINGSTON SKC600256G 50026B778374DEAC

Hashing completed
421 – SATA 3 HyperX Fury 3D 240GB 50026B7784002418

Hashing completed
451 – NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z

Hashing completed
442 – NVME 1 WD Blue SN570 250GB 2209B1456803

Hashing completed

The Menu gives access to Atola TaskForce settings, express mode, full screen mode, release notes, and manual.

In **Settings** you can adjust the general, database, network, print, and other settings.

Express mode enables automatic launch of multiple imaging sessions on all ports that are set to source. For more details, see Express mode: self-launching imaging.

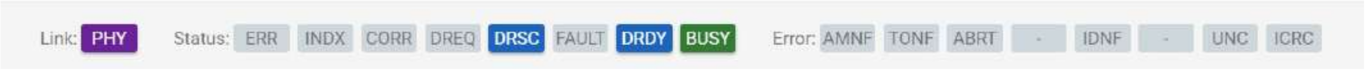
Toggle fullscreen option is handy when working with other programs or files.

In **Update firmware** you can check the current TaskForce firmware, choose update method and perform the firmware update by selecting and downloading the firmware file.

Activation status lets you to look up, reactivate the status, or extend the subscription.

In **Release notes** you can read the information about the most recent Atola TaskForce firmware release and track all updates and enhancements by clicking corresponding links.

ATA registers: what they mean


Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

Link Register

It's only enabled when port powered on, device presence detected and PHY communication established.

Status Register

This register contains hard drive status information. It is updated after every single command sent to the drive.

ERR: means last command failed to execute. In this case the Error register contains more details on the specific error.
INDX: obsolete, used to trigger after each spindle revolution
CORR: obsolete, used to trigger after a bad sector was automatically corrected by ECC
DREQ (Data Request): is asserted when hard drive wants to exchange data with the host controller (in either direction)
DRSC (Device Seek Complete): is obsolete; always asserted on modern hard drives
FAULT (Write Fault): is obsolete
DRDY (Device Ready): is obsolete; always asserted on modern hard drives
BUSY: indicates that the hard drive is busy executing a command OR initializing (after power on or reset)

Error Register

Error register provides more details if the last command failed. This register is only valid when **ERR** bit of the Status Register is asserted.

AMNF: means Address Mark Not Found (usually occurs on failed read attempt)
T0NF (Track 0 Not Found): obsolete
ABRT: command aborted (unsupported command or other failure)
IDNF: sector ID not found (usually occurs on failed read attempt)
UNC: uncorrectable read error; the hard drive was unable to read data even after applying ECC recovery algorithms
ICRC (Interface CRC error): there was CRC error while transferring data between host and the hard drive (usually indicates bad interface cable)

Diagnosing a drive with Atola TaskForce 2

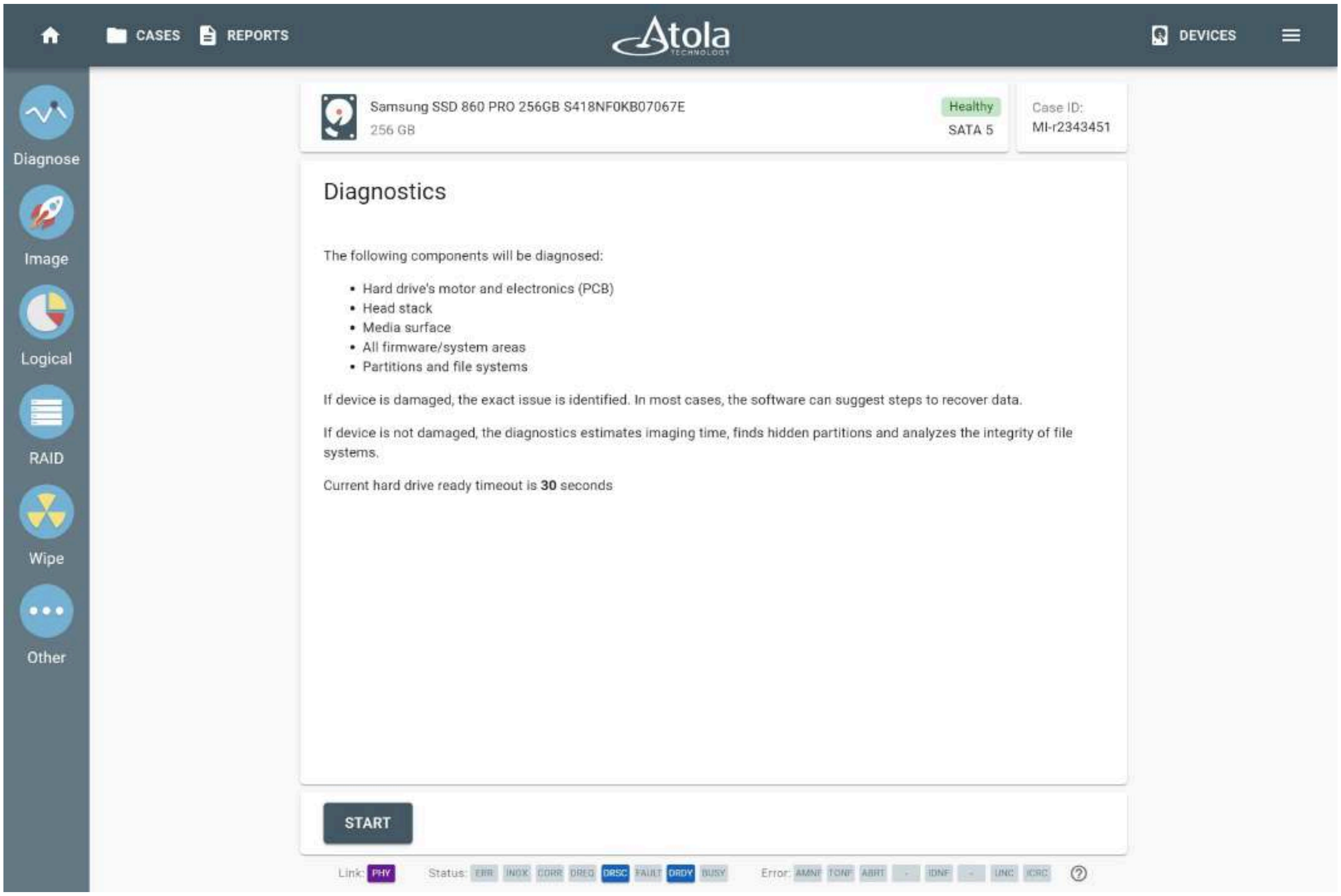
When an evidence drive lands on investigator’s table for the first time, there is always an uncertainty when it comes to the drive's condition. A broken head or scratched surface of the media require different imaging tactics. That’s why it is strongly suggested that before imaging, each drive should first be diagnosed.

TaskForce 2 has Atola's unique diagnostics module which checks all systems of the drive:

- Hard drive's motor and electronics (PCB)
- Head stack
- Media surface
- All firmware/system areas
- Partitions and file systems

At the end the system produces a report which sums up all issues. The process will take only 2-5 minutes.

To start, go to **Diagnose**, select the drive and then click **START**.



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 5
Case ID:
MI-r2343451

Diagnostics

The following components will be diagnosed:

- Hard drive's motor and electronics (PCB)
- Head stack
- Media surface
- All firmware/system areas
- Partitions and file systems

If device is damaged, the exact issue is identified. In most cases, the software can suggest steps to recover data.

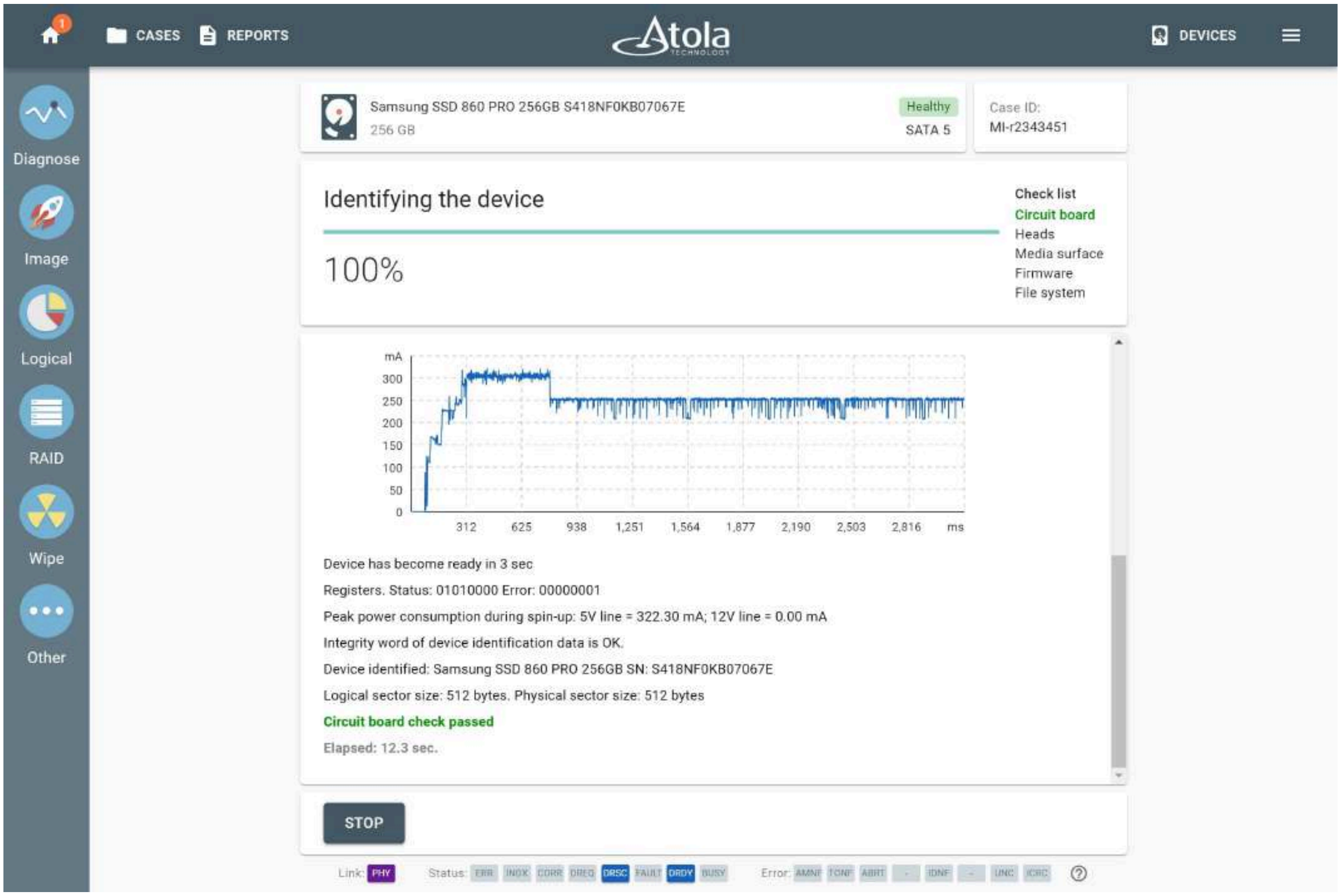
If device is not damaged, the diagnostics estimates imaging time, finds hidden partitions and analyzes the integrity of file systems.

Current hard drive ready timeout is **30** seconds

START
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

Start diagnostics.

First, TaskForce 2 checks the drive's printed circuit board. The system applies power to the device and records and analyzes spin-up current curve. This helps detect most issues with the PCB and the motor. Next, TaskForce 2 analyzes the contents of the hard drive's ATA registers and device identification sector.

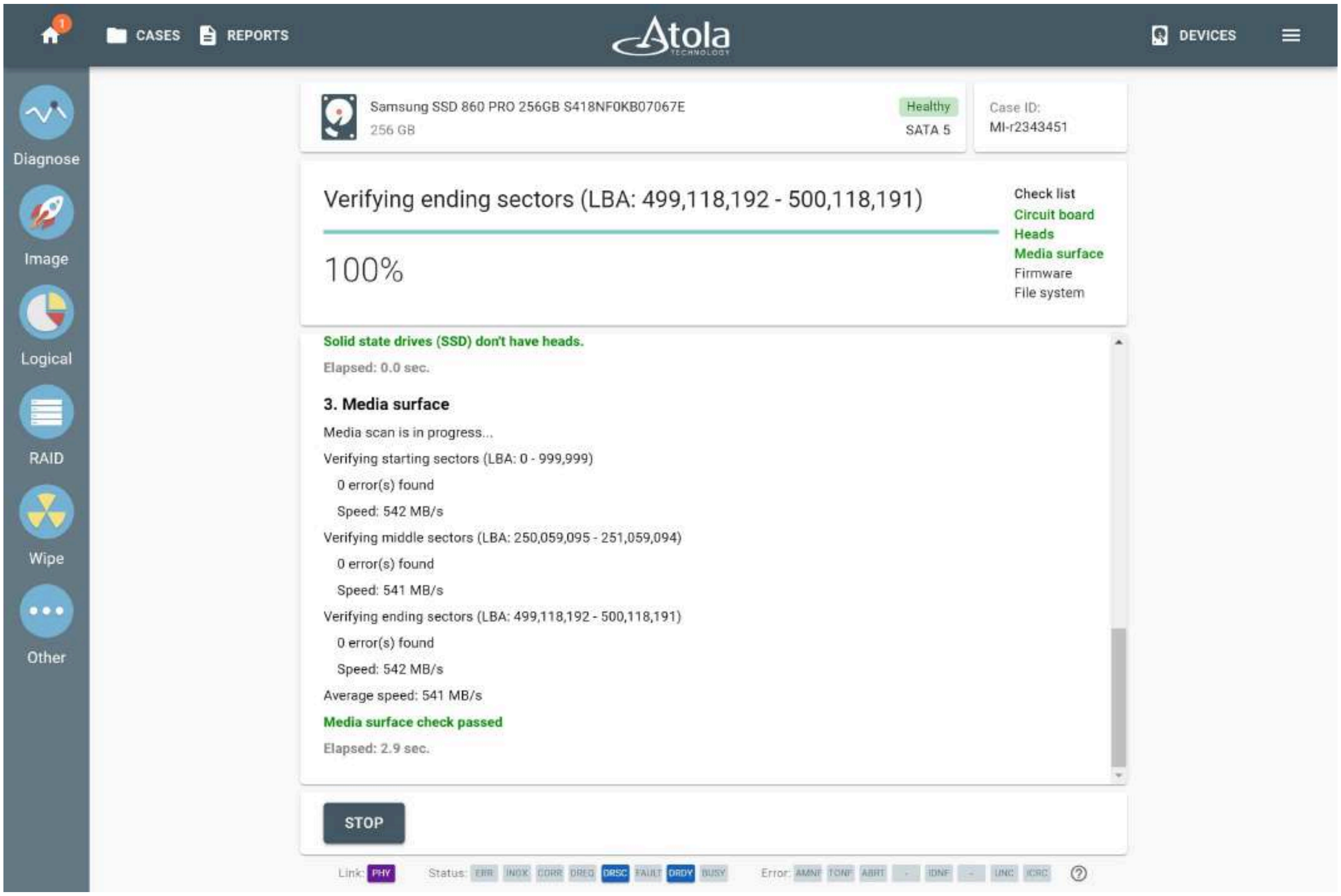


```
Device has become ready in 3 sec
Registers. Status: 01010000 Error: 00000001
Peak power consumption during spin-up: 5V line = 322.30 mA; 12V line = 0.00 mA
Integrity word of device identification data is OK.
Device identified: Samsung SSD 860 PRO 256GB SN: S418NF0KB07067E
Logical sector size: 512 bytes. Physical sector size: 512 bytes
Circuit board check passed
Elapsed: 12.3 sec.
```

Circuit board check.

After that, the head stack is tested. Several factors are taken into consideration when diagnosing heads: media access time for each head, power consumption curves, and internal drive's error reporting systems.

If the head stack looks good, the system performs a short media scan. The purpose of this scan is to verify if there are any bad sectors in the starting, middle and ending sectors of the drive pointing to a damage to the media surface or logical errors.


CASES
REPORTS
Atola
DEVICES
Diagnose
Image
Logical
RAID
Wipe
Other
STOP
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 5

Case ID:
MI-r2343451

Verifying ending sectors (LBA: 499,118,192 - 500,118,191)

100%

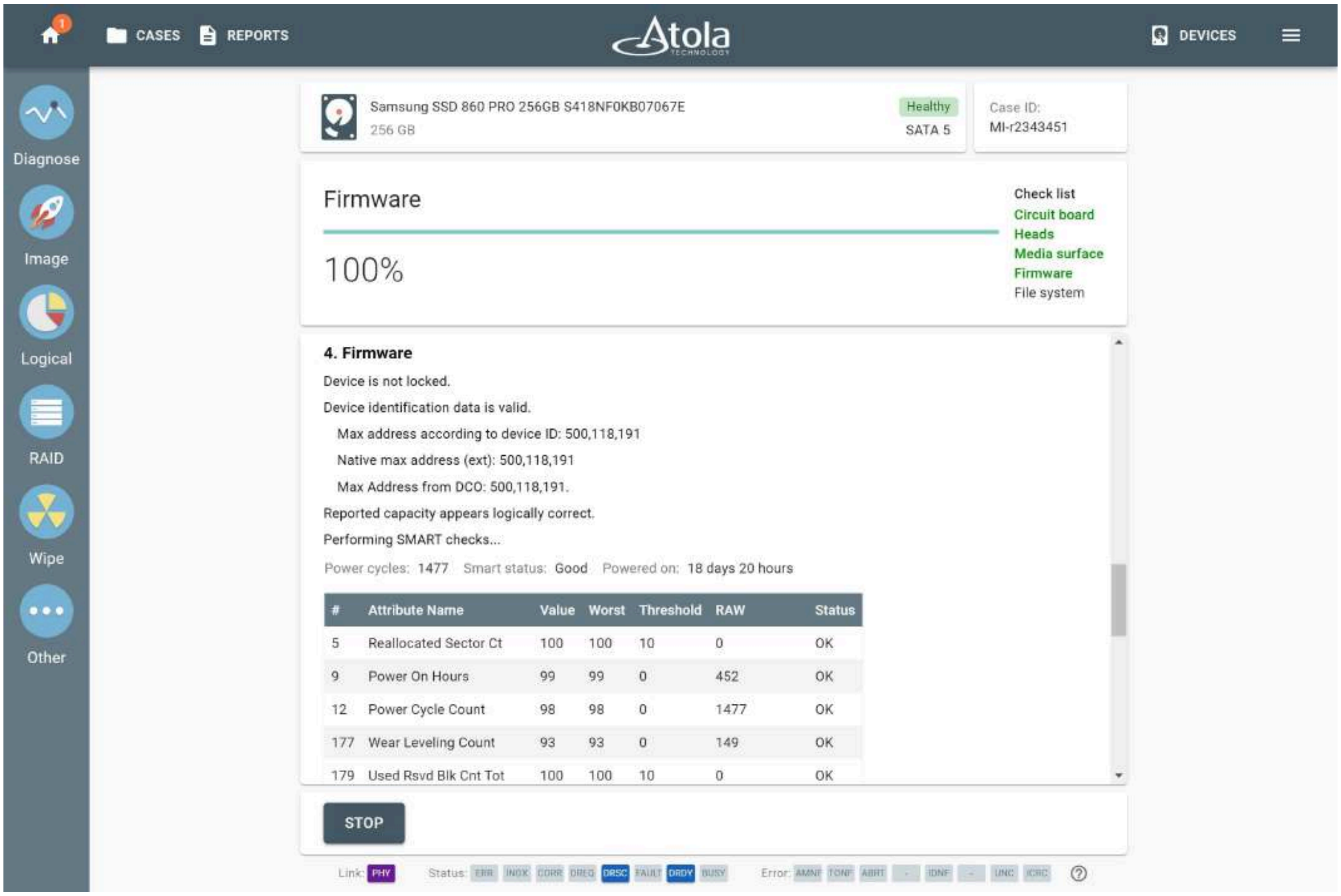
Check list
Circuit board
Heads
Media surface
Firmware
File system

```
Solid state drives (SSD) don't have heads.
Elapsed: 0.0 sec.

3. Media surface
Media scan is in progress...
Verifying starting sectors (LBA: 0 - 999,999)
  0 error(s) found
  Speed: 542 MB/s
Verifying middle sectors (LBA: 250,059,095 - 251,059,094)
  0 error(s) found
  Speed: 541 MB/s
Verifying ending sectors (LBA: 499,118,192 - 500,118,191)
  0 error(s) found
  Speed: 542 MB/s
Average speed: 541 MB/s
Media surface check passed
Elapsed: 2.9 sec.
```

Heads and media surface check.

Next, several firmware tests are performed:



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 5

Case ID:
MI-r2343451

Firmware

100%

Check list
Circuit board
Heads
Media surface
Firmware
File system

4. Firmware

Device is not locked.

Device identification data is valid.

Max address according to device ID: 500,118,191

Native max address (ext): 500,118,191

Max Address from DCO: 500,118,191.

Reported capacity appears logically correct.

Performing SMART checks...

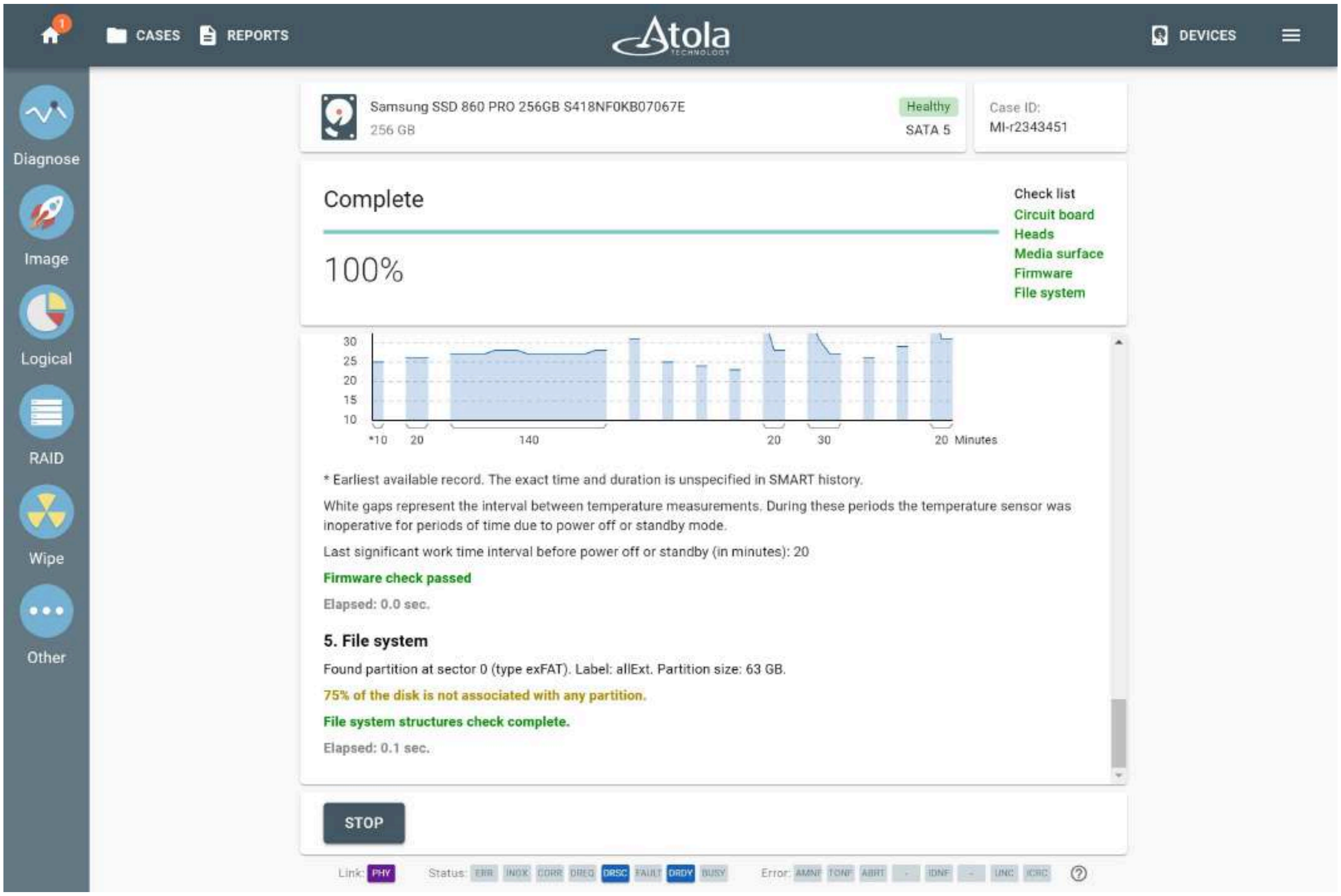
Power cycles: 1477 Smart status: Good Powered on: 18 days 20 hours

#	Attribute Name	Value	Worst	Threshold	RAW	Status
5	Reallocated Sector Ct	100	100	10	0	OK
9	Power On Hours	99	99	0	452	OK
12	Power Cycle Count	98	98	0	1477	OK
177	Wear Leveling Count	93	93	0	149	OK
179	Used Rsvd Blk Cnt Tot	100	100	10	0	OK

STOP
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

Firmware check.

If TaskForce detected no issues by this point, it performs a file system checkup:



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 5
Case ID:
MI-r2343451

Complete

100%

Check list
Circuit board
Heads
Media surface
Firmware
File system

* Earliest available record. The exact time and duration is unspecified in SMART history.

White gaps represent the interval between temperature measurements. During these periods the temperature sensor was inoperative for periods of time due to power off or standby mode.

Last significant work time interval before power off or standby (in minutes): 20

Firmware check passed

Elapsed: 0.0 sec.

5. File system

Found partition at sector 0 (type exFAT). Label: allExt. Partition size: 63 GB.

75% of the disk is not associated with any partition.

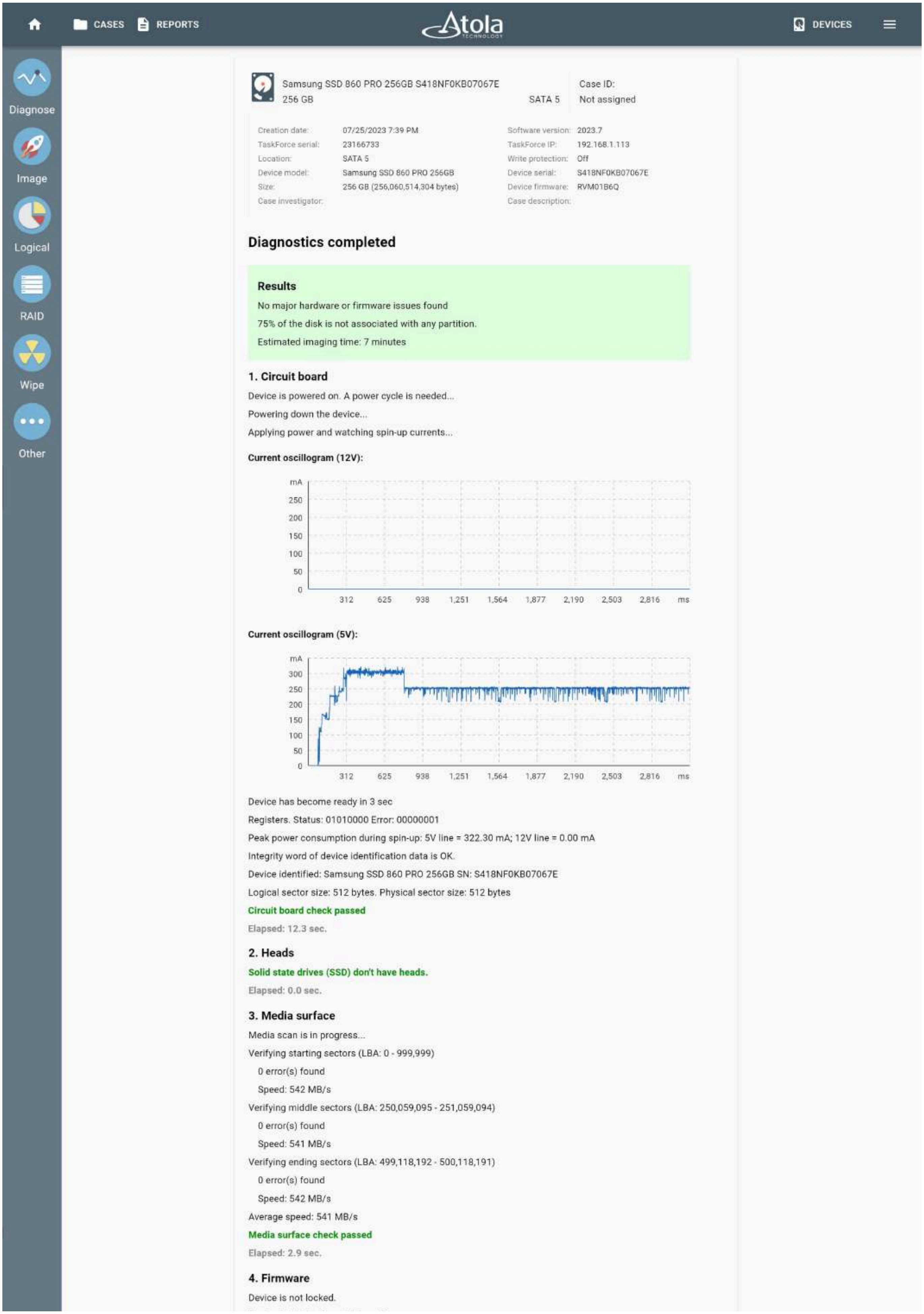
File system structures check complete.

Elapsed: 0.1 sec.

STOP
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

File system check.

After this final stage of diagnostics, TaskForce 2 displays the full report. The **Diagnostics result** message box contains a short summary of all tests. It also provides estimated imaging time for this drive.



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB

SATA 5

Case ID:
Not assigned

Creation date:	07/25/2023 7:39 PM	Software version:	2023.7
TaskForce serial:	23166733	TaskForce IP:	192.168.1.113
Location:	SATA 5	Write protection:	Off
Device model:	Samsung SSD 860 PRO 256GB	Device serial:	S418NF0KB07067E
Size:	256 GB (256,060,514,304 bytes)	Device firmware:	RVM01B6Q
Case investigator:		Case description:	

Diagnostics completed

Results

No major hardware or firmware issues found

75% of the disk is not associated with any partition.

Estimated imaging time: 7 minutes

1. Circuit board

Device is powered on. A power cycle is needed...

Powering down the device...

Applying power and watching spin-up currents...

Current oscillogram (12V):

Current oscillogram (5V):

Device has become ready in 3 sec

Registers. Status: 01010000 Error: 00000001

Peak power consumption during spin-up: 5V line = 322.30 mA; 12V line = 0.00 mA

Integrity word of device identification data is OK.

Device identified: Samsung SSD 860 PRO 256GB SN: S418NF0KB07067E

Logical sector size: 512 bytes. Physical sector size: 512 bytes

Circuit board check passed

Elapsed: 12.3 sec.

2. Heads

Solid state drives (SSD) don't have heads.

Elapsed: 0.0 sec.

3. Media surface

Media scan is in progress...

Verifying starting sectors (LBA: 0 - 999,999)

  0 error(s) found

  Speed: 542 MB/s

Verifying middle sectors (LBA: 250,059,095 - 251,059,094)

  0 error(s) found

  Speed: 541 MB/s

Verifying ending sectors (LBA: 499,118,192 - 500,118,191)

  0 error(s) found

  Speed: 542 MB/s

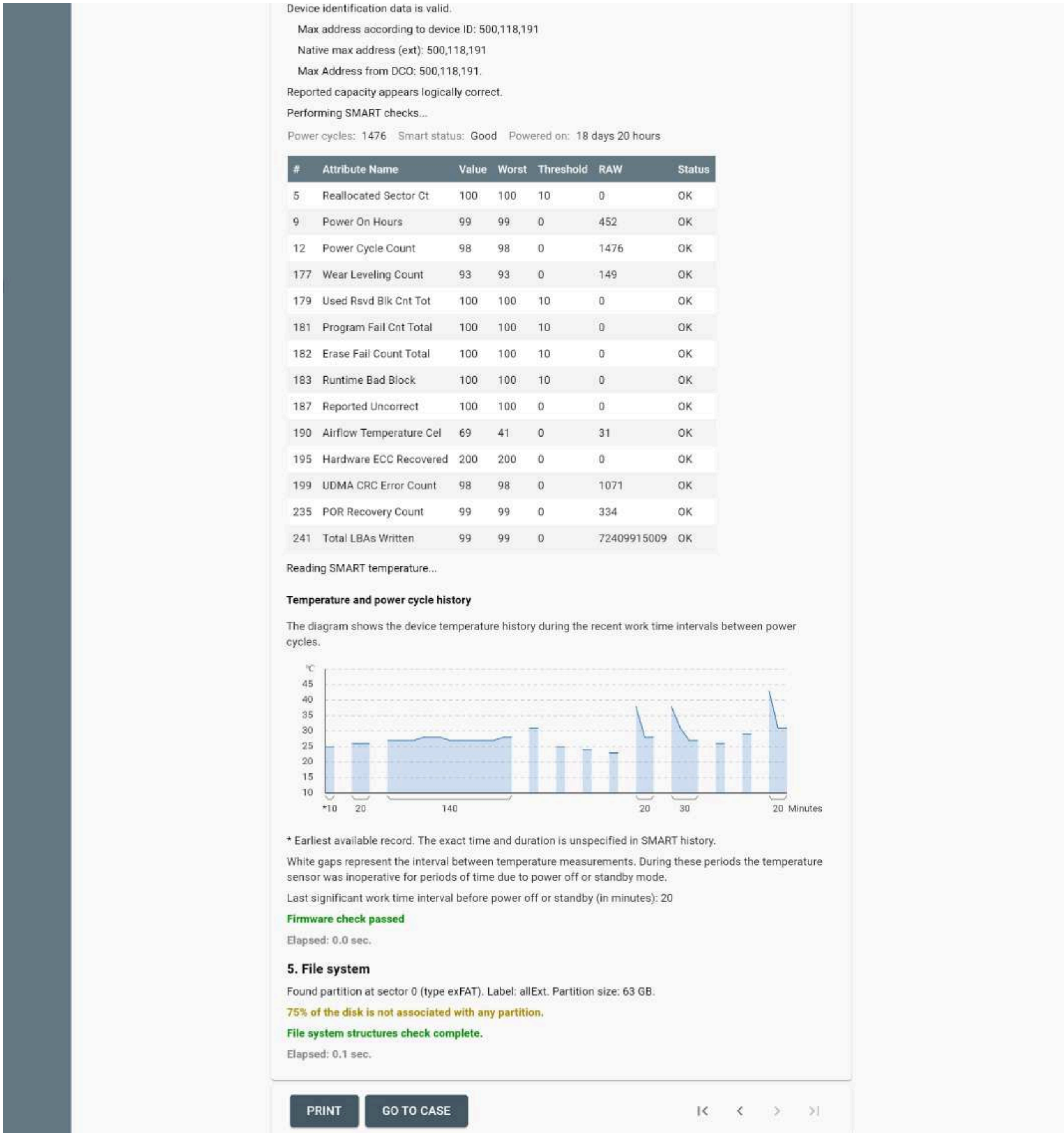
Average speed: 541 MB/s

Media surface check passed

Elapsed: 2.9 sec.

4. Firmware

Device is not locked.



Device identification data is valid.

Max address according to device ID: 500,118,191

Native max address (ext): 500,118,191

Max Address from DCO: 500,118,191.

Reported capacity appears logically correct.

Performing SMART checks...

Power cycles: 1476 Smart status: Good Powered on: 18 days 20 hours

#	Attribute Name	Value	Worst	Threshold	RAW	Status
5	Reallocated Sector Ct	100	100	10	0	OK
9	Power On Hours	99	99	0	452	OK
12	Power Cycle Count	98	98	0	1476	OK
177	Wear Leveling Count	93	93	0	149	OK
179	Used Rsvd Blk Cnt Tot	100	100	10	0	OK
181	Program Fail Cnt Total	100	100	10	0	OK
182	Erase Fail Count Total	100	100	10	0	OK
183	Runtime Bad Block	100	100	10	0	OK
187	Reported Uncorrect	100	100	0	0	OK
190	Airflow Temperature Cel	69	41	0	31	OK
195	Hardware ECC Recovered	200	200	0	0	OK
199	UDMA CRC Error Count	98	98	0	1071	OK
235	POR Recovery Count	99	99	0	334	OK
241	Total LBAs Written	99	99	0	72409915009	OK

Reading SMART temperature...

Temperature and power cycle history

The diagram shows the device temperature history during the recent work time intervals between power cycles.

* Earliest available record. The exact time and duration is unspecified in SMART history.

White gaps represent the interval between temperature measurements. During these periods the temperature sensor was inoperative for periods of time due to power off or standby mode.

Last significant work time interval before power off or standby (in minutes): 20

Firmware check passed

Elapsed: 0.0 sec.

5. File system

Found partition at sector 0 (type exFAT). Label: allExt. Partition size: 63 GB.

75% of the disk is not associated with any partition.

File system structures check complete.

Elapsed: 0.1 sec.

Diagnostics report.

Tracking a drive's SMART table status before and after imaging

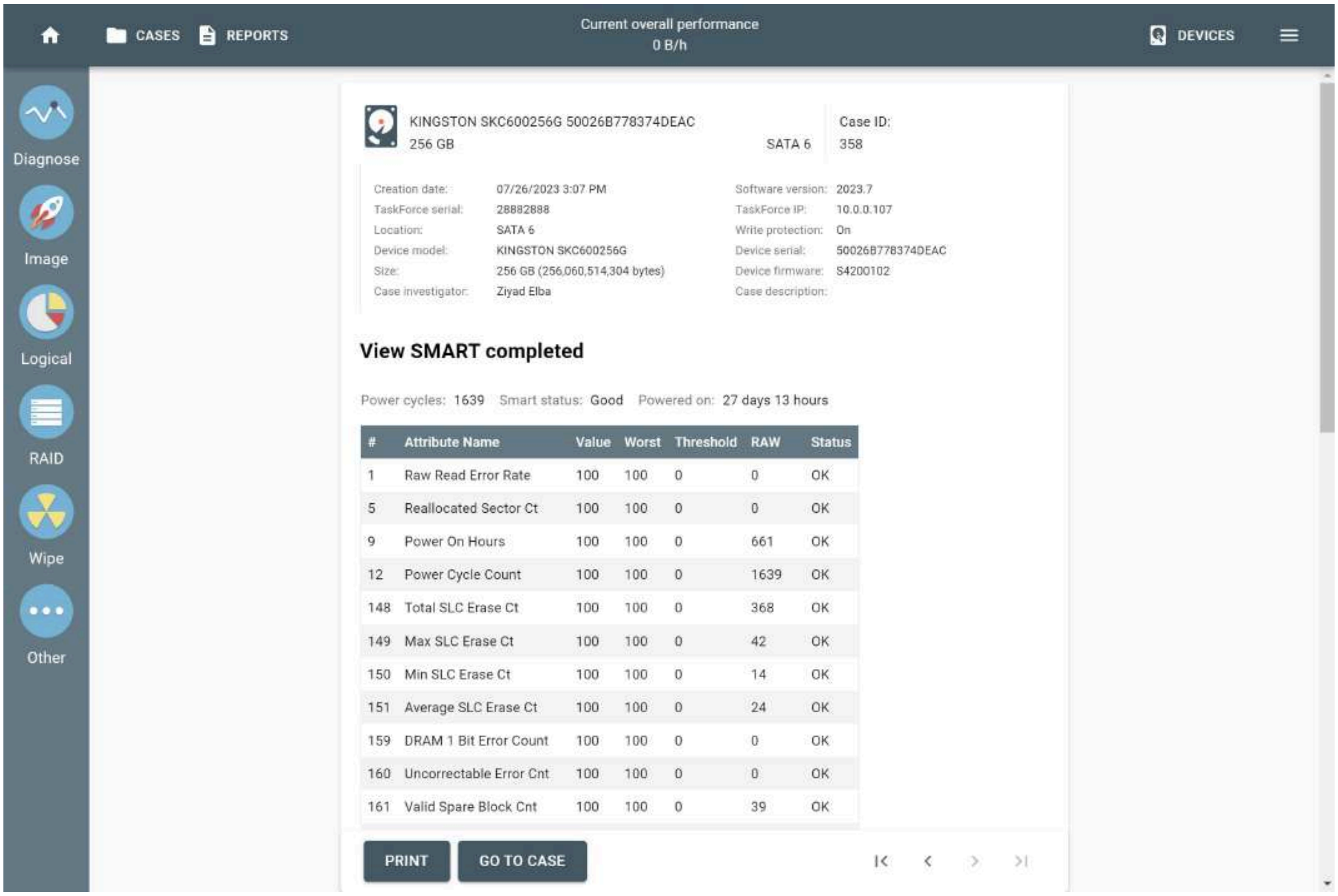
SMART table is a valuable source of information about a hard drive's health. SMART (Self-Monitoring, Analysis and Reporting Technology) provides stats of a drive's operation, thus helping predict its future failure.

Making a definitive conclusion based on the indices in SMART table is not easy: not all parameters are critical, it is usually a combination of bad values of a few parameters that point to a trouble, time factor plays a role too (how fast has the state of the drive been deteriorating).

View SMART table

SMART table is included in the Diagnostics report. If you want to have a look at the current indices:

1. Go to **Other** > **View SMART**.
2. Select the drive.
3. Click **Start**.



KINGSTON SKC600256G 50026B778374DEAC
256 GB
SATA 6
Case ID:
358

Creation date:	07/26/2023 3:07 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.107
Location:	SATA 6	Write protection:	On
Device model:	KINGSTON SKC600256G	Device serial:	50026B778374DEAC
Size:	256 GB (256,060,514,304 bytes)	Device firmware:	S4200102
Case investigator:	Ziyad Elba	Case description:	

View SMART completed

Power cycles: 1639 Smart status: Good Powered on: 27 days 13 hours

#	Attribute Name	Value	Worst	Threshold	RAW	Status
1	Raw Read Error Rate	100	100	0	0	OK
5	Reallocated Sector Ct	100	100	0	0	OK
9	Power On Hours	100	100	0	661	OK
12	Power Cycle Count	100	100	0	1639	OK
148	Total SLC Erase Ct	100	100	0	368	OK
149	Max SLC Erase Ct	100	100	0	42	OK
150	Min SLC Erase Ct	100	100	0	14	OK
151	Average SLC Erase Ct	100	100	0	24	OK
159	DRAM 1 Bit Error Count	100	100	0	0	OK
160	Uncorrectable Error Cnt	100	100	0	0	OK
161	Valid Spare Block Cnt	100	100	0	39	OK

SMART table report.

SMART table attributes may differ depending on the drive manufacturer. The most critical attributes are:

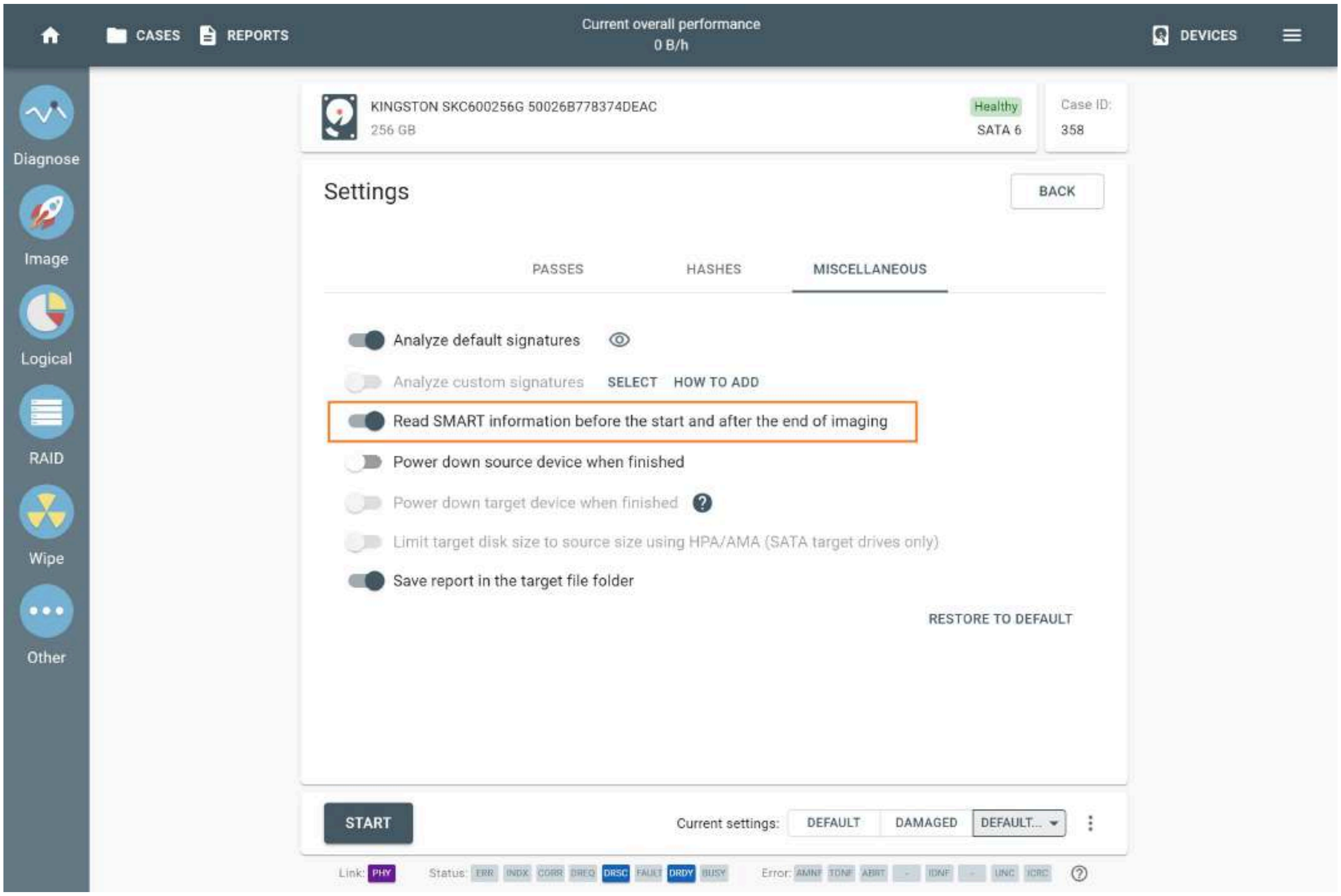
- Reallocated sectors count.
- Current pending sector count.
- Uncorrectable sector count.

When RAW value of any of these attributes is greater than zero, TaskForce highlights it in yellow.

The worse the values, especially in these critical attributes, the more carefully the drive needs to be treated.

Track changes of the SMART table attributes

To keep track of the changes occurring to the attributes of the SMART table, the imaging settings can be easily adjusted to records SMART table indices prior and after each imaging session.



KINGSTON SKC600256G 50026B778374DEAC
256 GB
Healthy
SATA 6
Case ID:
358

Settings

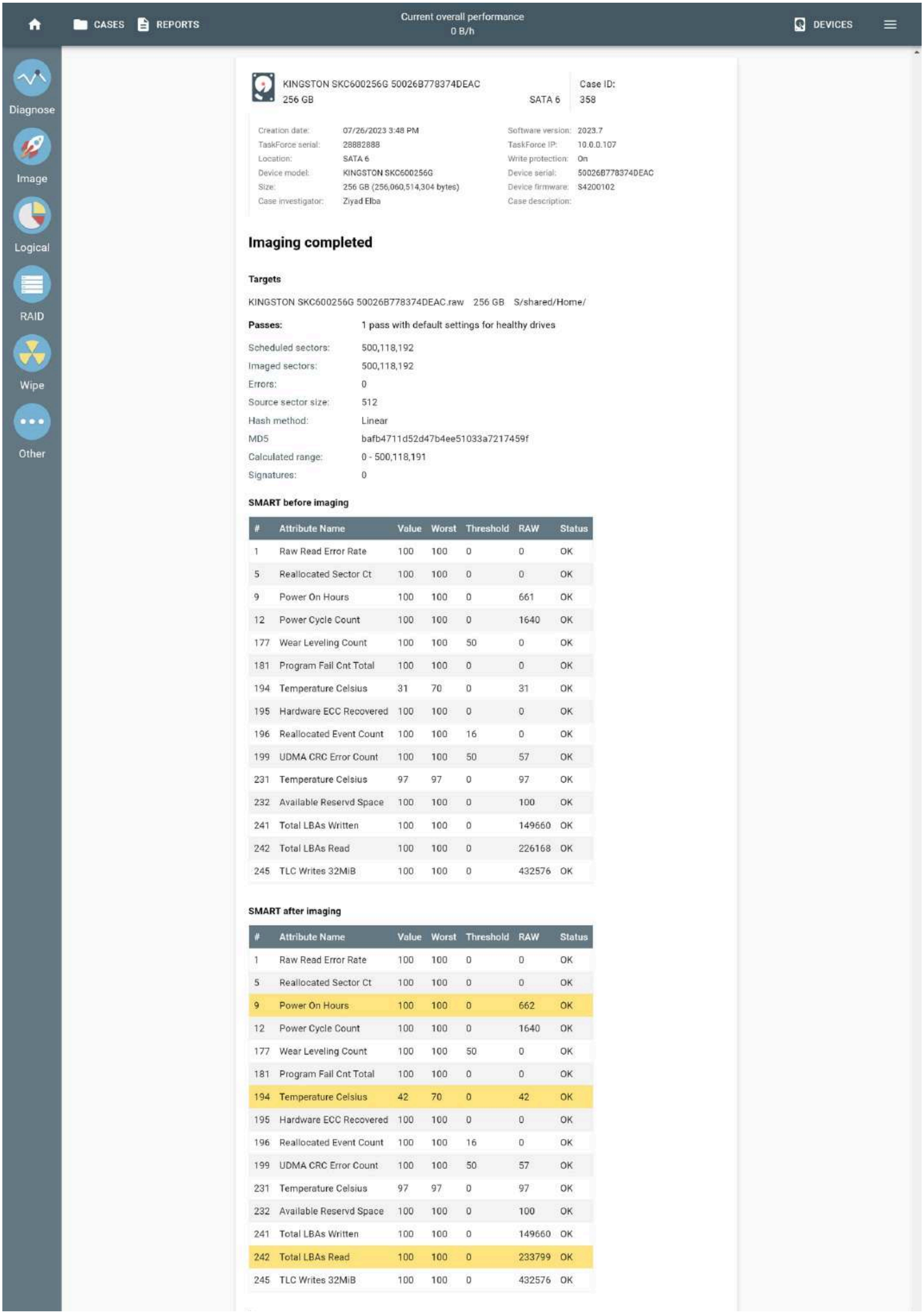
- ● Analyze default signatures
- ○ Analyze custom signatures SELECT HOW TO ADD
- ● Read SMART information before the start and after the end of imaging
- ○ Power down source device when finished
- ○ Power down target device when finished
- ○ Limit target disk size to source size using HPA/AMA (SATA target drives only)
- ● Save report in the target file folder

Current settings: DEFAULT DAMAGED DEFAULT...

Link: PHY Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY Error: AMNF TONF ABRT - IDNF - UNC ICRC

Adjust the imaging settings to keep the record of SMART prior and after the imaging session.

By comparing the two tables, user can evaluate whether the health of a drive has been deteriorating throughout the imaging session and thus assess how quickly its health has been getting worse. Any discrepancies between the two SMART tables will be highlighted in yellow.



Current overall performance
0 B/h

KINGSTON SKC600256G 50026B778374DEAC
256 GB

SATA 6

Case ID:
358

Creation date:	07/26/2023 3:48 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.107
Location:	SATA 6	Write protection:	On
Device model:	KINGSTON SKC600256G	Device serial:	50026B778374DEAC
Size:	256 GB (256,060,514,304 bytes)	Device firmware:	S4200102
Case investigator:	Ziyad Elba	Case description:	

Imaging completed

Targets

KINGSTON SKC600256G 50026B778374DEAC.raw 256 GB S/shared/Home/

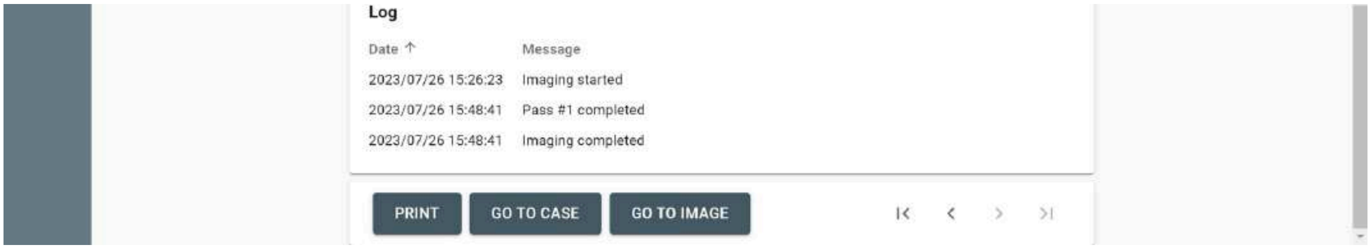
Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	500,118,192
Imaged sectors:	500,118,192
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	bafb4711d52d47b4ee51033a7217459f
Calculated range:	0 - 500,118,191
Signatures:	0

SMART before imaging

#	Attribute Name	Value	Worst	Threshold	RAW	Status
1	Raw Read Error Rate	100	100	0	0	OK
5	Reallocated Sector Ct	100	100	0	0	OK
9	Power On Hours	100	100	0	661	OK
12	Power Cycle Count	100	100	0	1640	OK
177	Wear Leveling Count	100	100	50	0	OK
181	Program Fail Cnt Total	100	100	0	0	OK
194	Temperature Celsius	31	70	0	31	OK
195	Hardware ECC Recovered	100	100	0	0	OK
196	Reallocated Event Count	100	100	16	0	OK
199	UDMA CRC Error Count	100	100	50	57	OK
231	Temperature Celsius	97	97	0	97	OK
232	Available Reservd Space	100	100	0	100	OK
241	Total LBAs Written	100	100	0	149660	OK
242	Total LBAs Read	100	100	0	226168	OK
245	TLC Writes 32MiB	100	100	0	432576	OK

SMART after imaging

#	Attribute Name	Value	Worst	Threshold	RAW	Status
1	Raw Read Error Rate	100	100	0	0	OK
5	Reallocated Sector Ct	100	100	0	0	OK
9	Power On Hours	100	100	0	662	OK
12	Power Cycle Count	100	100	0	1640	OK
177	Wear Leveling Count	100	100	50	0	OK
181	Program Fail Cnt Total	100	100	0	0	OK
194	Temperature Celsius	42	70	0	42	OK
195	Hardware ECC Recovered	100	100	0	0	OK
196	Reallocated Event Count	100	100	16	0	OK
199	UDMA CRC Error Count	100	100	50	57	OK
231	Temperature Celsius	97	97	0	97	OK
232	Available Reservd Space	100	100	0	100	OK
241	Total LBAs Written	100	100	0	149660	OK
242	Total LBAs Read	100	100	0	233799	OK
245	TLC Writes 32MiB	100	100	0	432576	OK



Log

```
Date ↑                Message
2023/07/26 15:26:23   Imaging started
2023/07/26 15:48:41   Pass #1 completed
2023/07/26 15:48:41   Imaging completed
```

How SMART table state changed after image acquisition

Whenever you need to evaluate how the state of the drive has been changing long-term, go to previous imaging sessions and look up SMART table. TaskForce stores this information in its case management system.

Imaging an evidence drive to 5 targets

Atola TaskForce allows imaging to up to 5 targets at a time.

The targets may include:

- E01, AFF4, RAW file on a network server.
- target drive plugged into one of 26 TaskForce ports.

To start an imaging session that includes 5 targets:

1. Go to **Image**.
2. Select a source device.
3. On the **Select target devices** panel:
    a. Switch to the **Drives** tab and select your target drives.

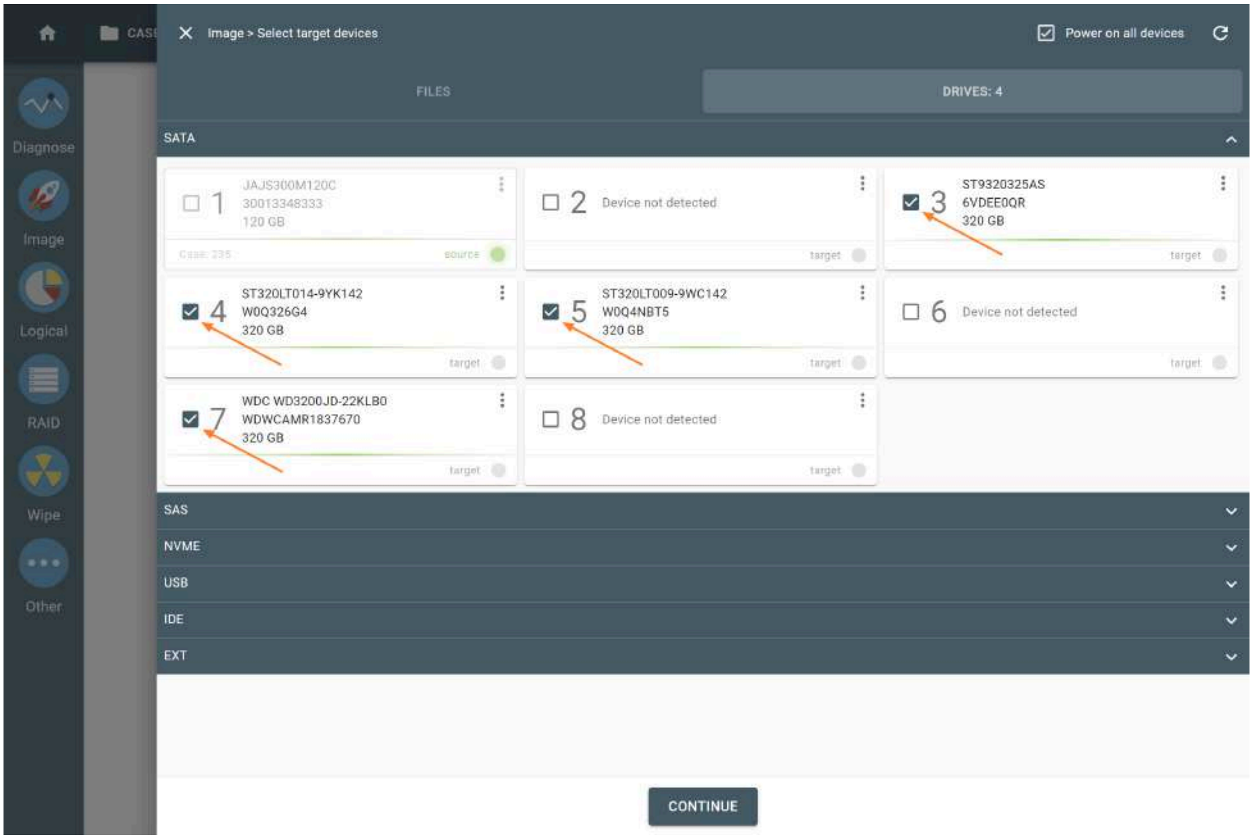


Image > Select target devices

☑ Power on all devices

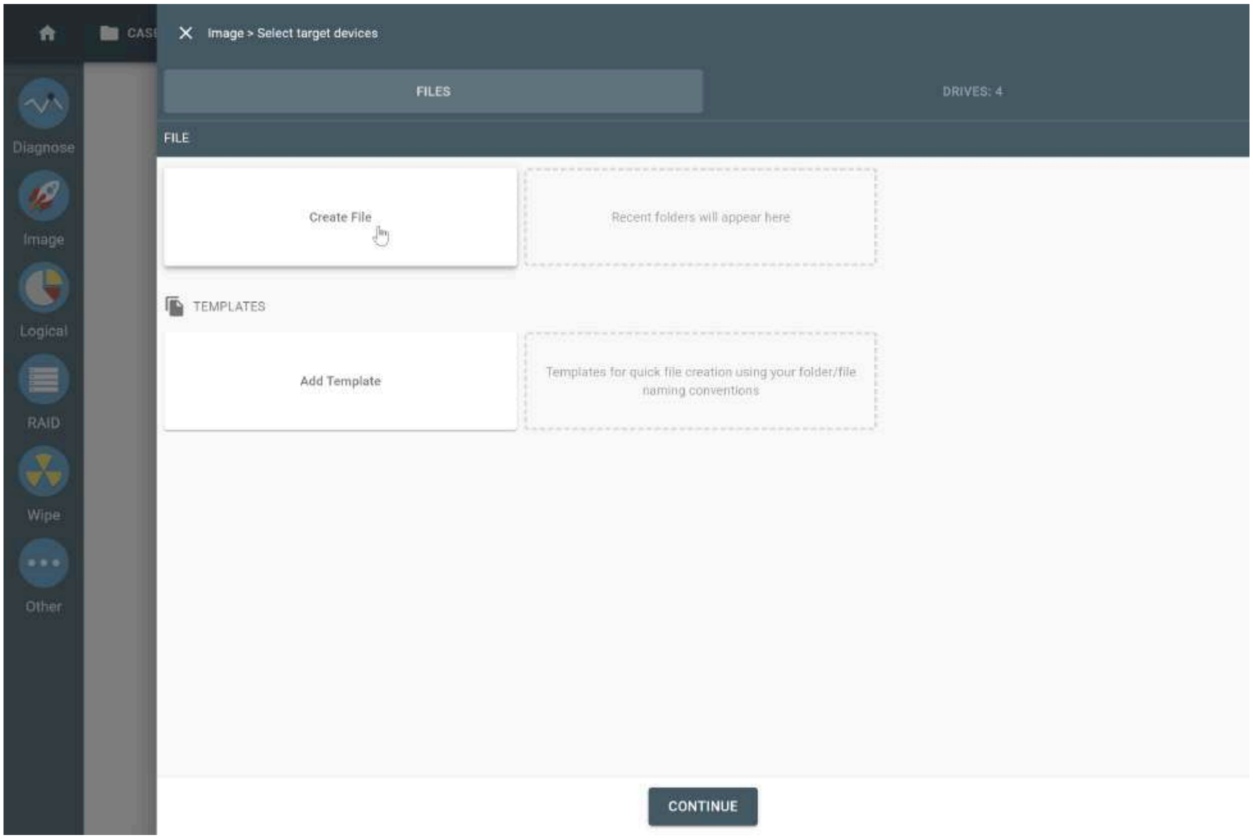
FILES | DRIVES: 4

SATA

□ 1 JAJS300M120C 30013348333 120 GB — Case: 235 — source
□ 2 Device not detected — target
☑ 3 ST9320325AS 6VDEE0QR 320 GB — target
☑ 4 ST320LT014-9YK142 W0Q326G4 320 GB — target
☑ 5 ST320LT009-9WC142 W0Q4NBT5 320 GB — target
□ 6 Device not detected — target
☑ 7 WDC WD3200JD-22KLB0 WDWCAMR1837670 320 GB — target
□ 8 Device not detected — target

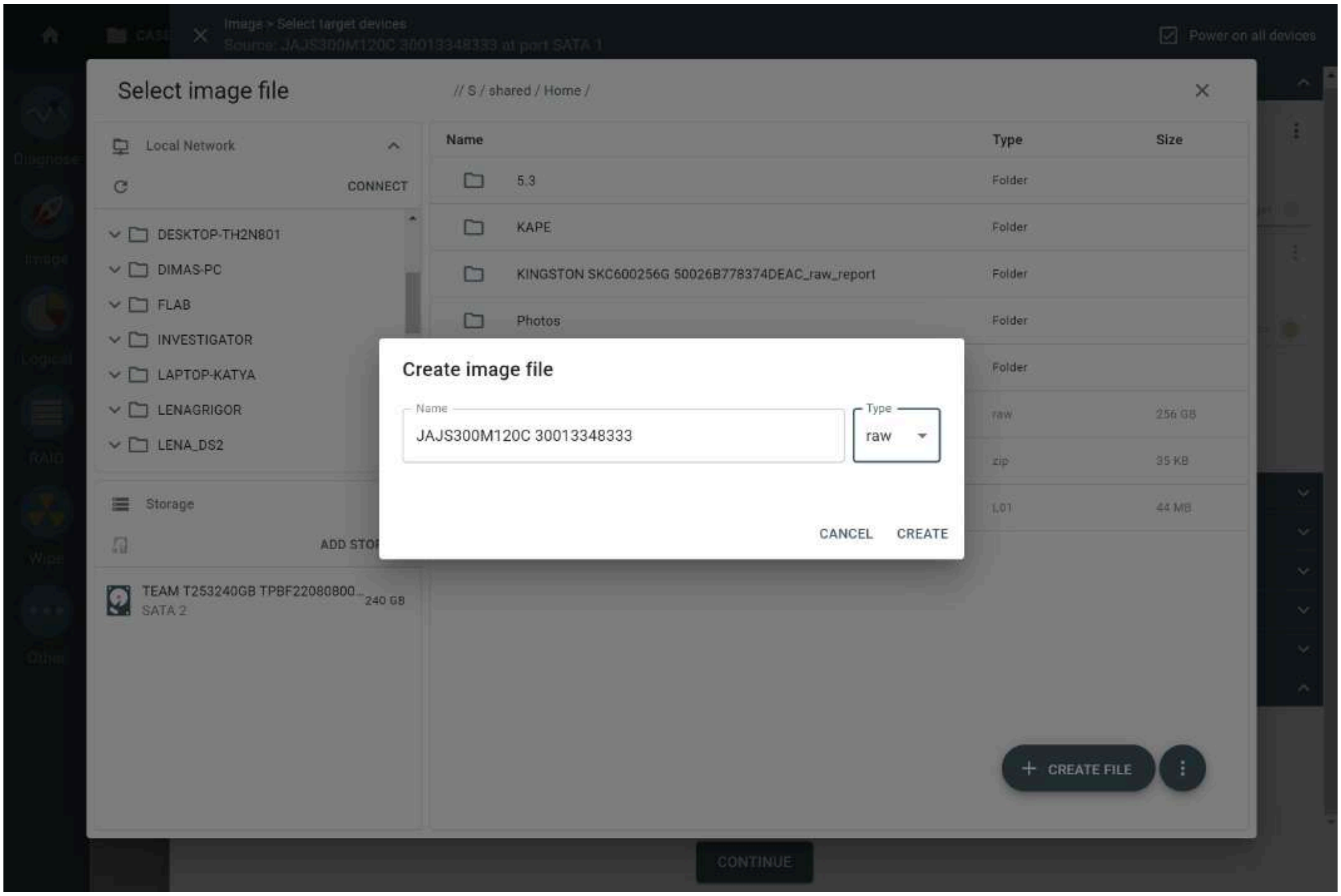
Selecting target devices.

b. Switch to the **Files** tab and click **Create File**.


CASE
Image > Select target devices
FILES
DRIVES: 4
Diagnose
Image
Logical
RAID
Wipe
Other
FILE
Create File
Recent folders will appear here
TEMPLATES
Add Template
Templates for quick file creation using your folder/file naming conventions
CONTINUE

Creating target image file.

4. In the **Select image file** window, open the folder on the server where you want the file to be created and click **Create file**.
5. In the **Create image file** dialog, enter a name for the file, select its type (E01, aff4, dd, img, or raw), and then click **Create**.



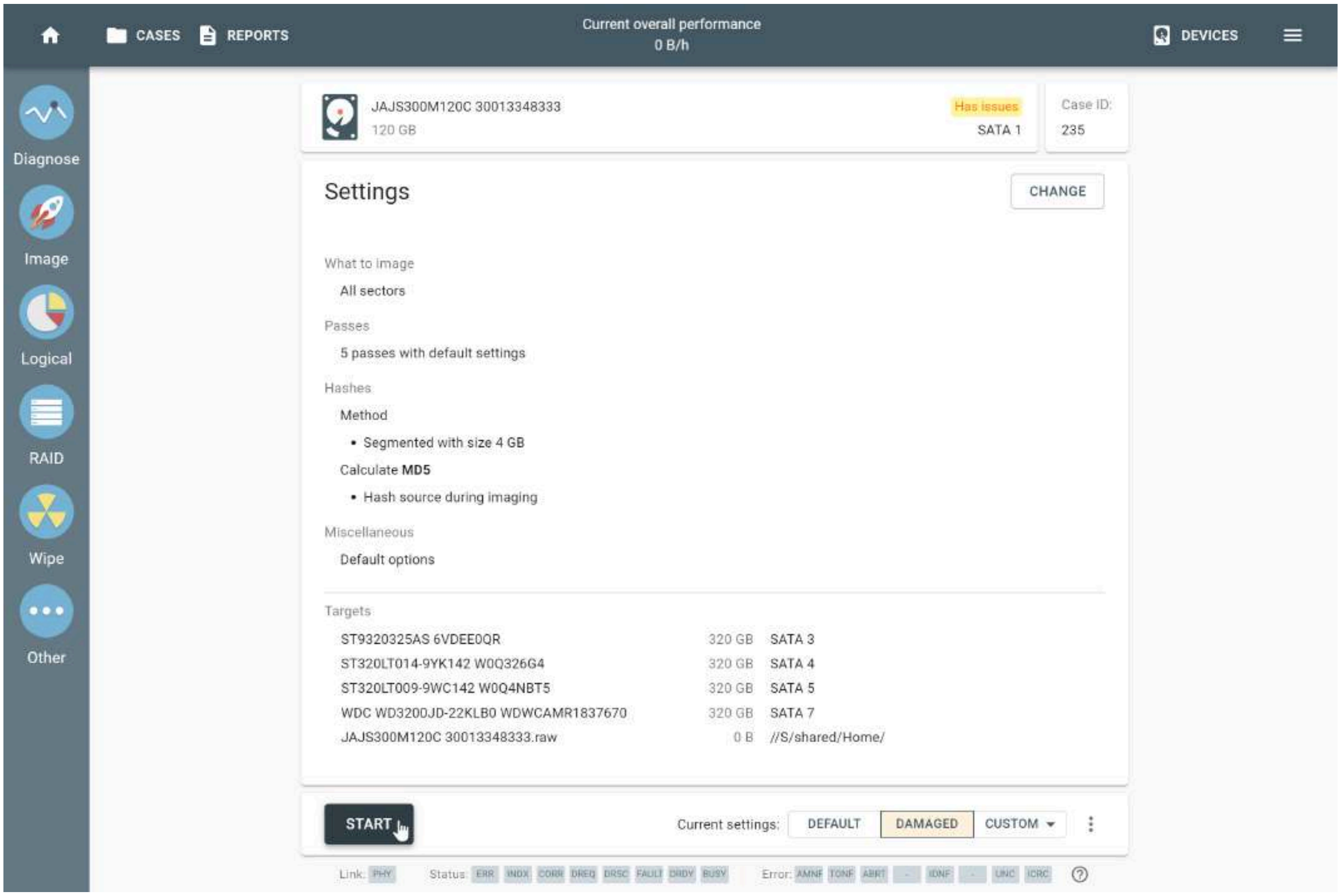
Name	Type	Size
5.3	Folder	
KAPE	Folder	
KINGSTON SKC600256G 50026B778374DEAC_raw_report	Folder	
Photos	Folder	
	Folder	
	raw	256 GB
	zip	35 KB
	L01	44 MB

Name: JAJS300M120C 30013348333

Type: raw

Entering the name of the file.

6. On **Select target devices** panel, click **Continue**.
7. On the imaging settings page, double-check all settings and the targets selected for the imaging session, and then click **Start**.



JAJS300M120C 30013348333
120 GB
SATA 1
Case ID:
235

Settings

What to image
All sectors

Passes
5 passes with default settings

Hashes
Method
- Segmented with size 4 GB

Calculate **MD5**
- Hash source during imaging

Miscellaneous
Default options

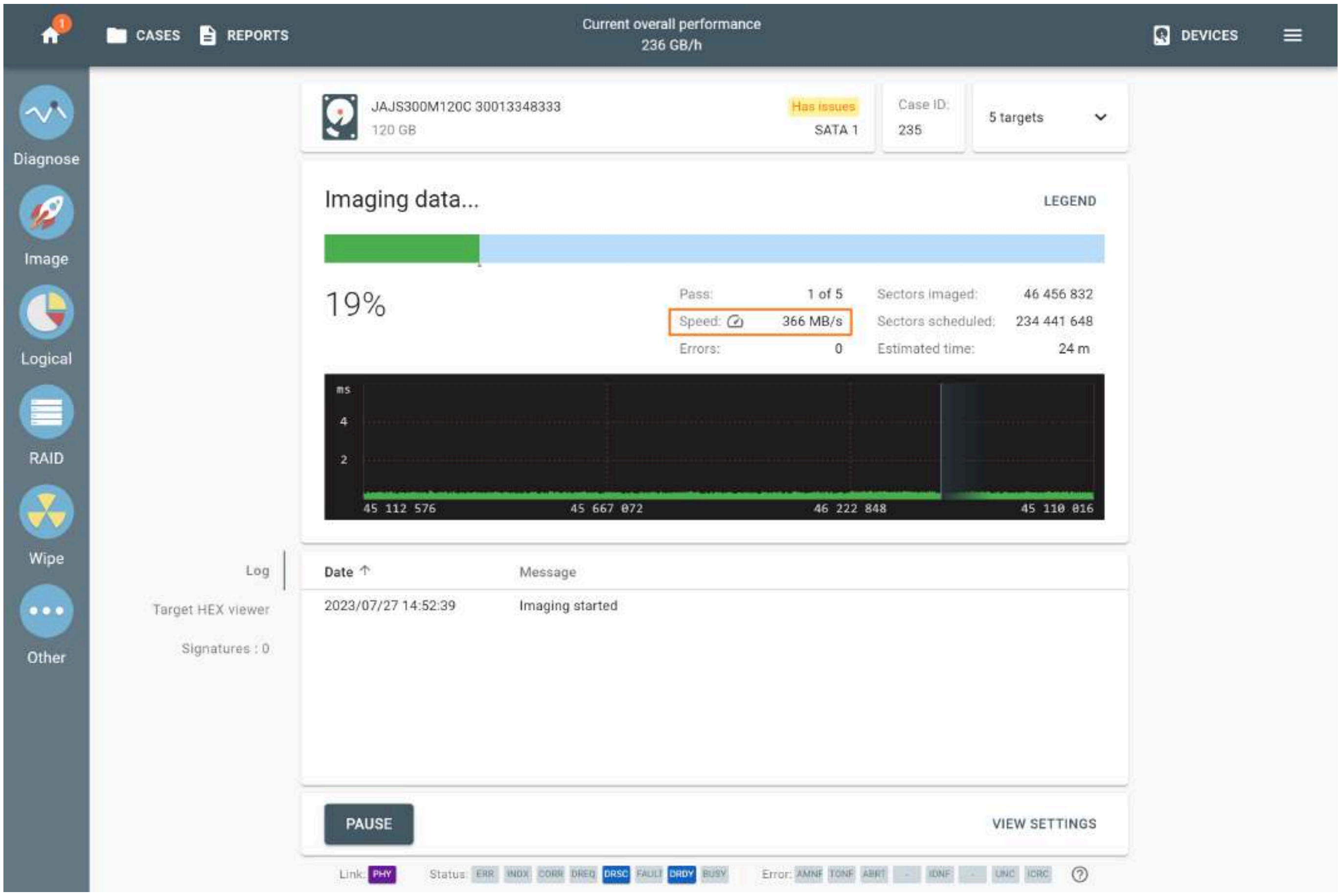
Targets

ST9320325AS 6VDEE0QR	320 GB	SATA 3
ST320LT014-9YK142 W0Q326G4	320 GB	SATA 4
ST320LT009-9WC142 W0Q4NBT5	320 GB	SATA 5
WDC WD3200JD-22KLB0 WDWCAMR1837670	320 GB	SATA 7
JAJS300M120C 30013348333.raw	0 B	//S/shared/Home/

The imaging settings page.

In the imaging page, there are two diagrams that show the progress of imaging. The upper one is called *imaging map bar* and shows imaging progress throughout the whole drive space (all successfully imaged sectors on the source drive are marked green, all damaged ones are marked red). The lower diagram is called *read speed graph* and shows the time TaskForce spent reading sectors on the source drive.

> Overall imaging speed is always limited by the slowest device: either by the read speed of the source or the write speed of the slowest target.



Current overall performance
236 GB/h

JAJS300M120C 30013348333
120 GB
SATA 1
Case ID: 235
5 targets

Imaging data...

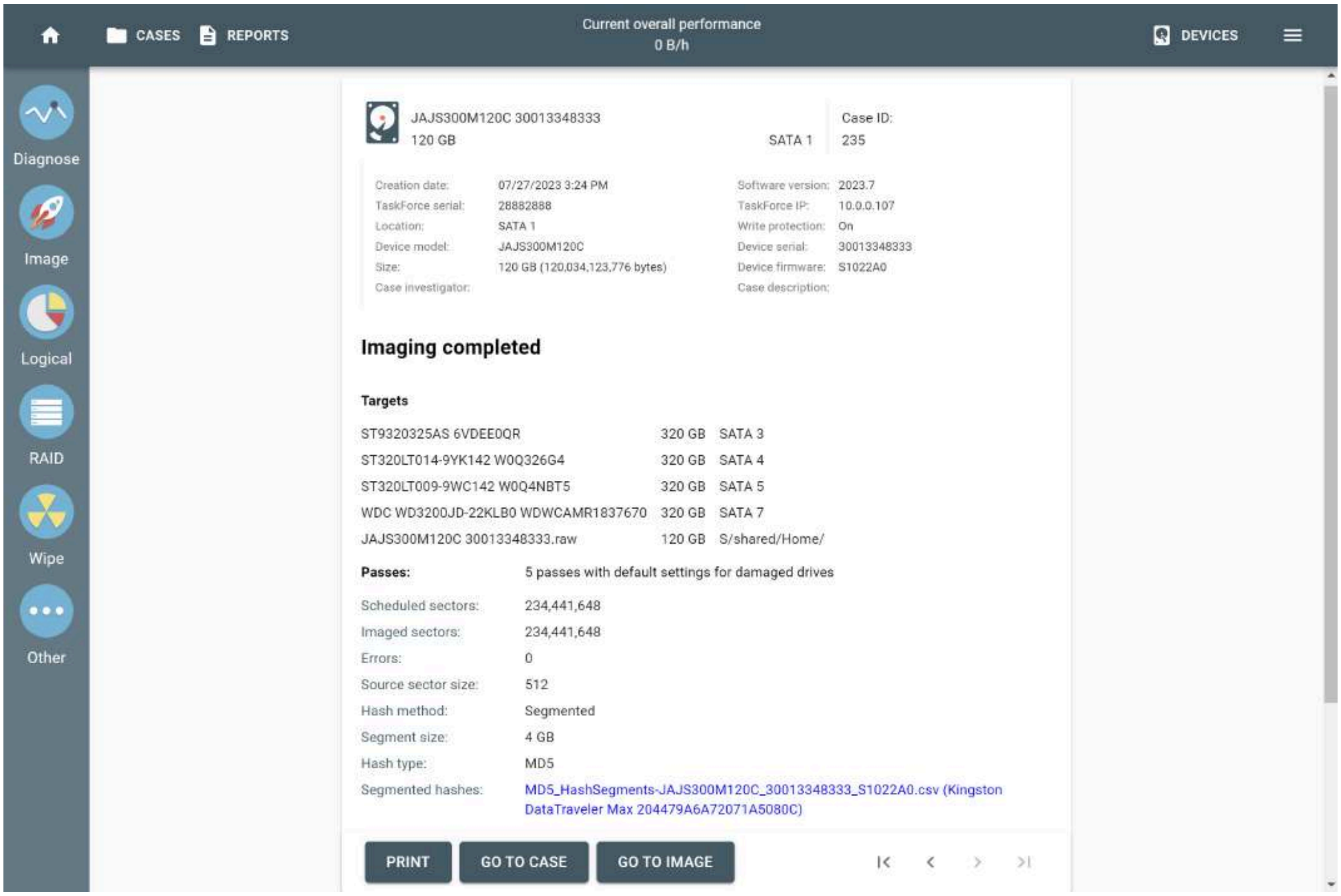
19%

Pass: 1 of 5
Speed: 366 MB/s
Errors: 0
Sectors imaged: 46 456 832
Sectors scheduled: 234 441 648
Estimated time: 24 m

Date ↑	Message
2023/07/27 14:52:39	Imaging started

Imaging in progress.

When imaging is completed, you are redirected to the imaging summary page, where you can review the details of the session including source and target drive details, imaging settings, hash values and the time when imaging session started and when it was completed.



JAJS300M120C 30013348333
120 GB
SATA 1
Case ID:
235

Creation date:	07/27/2023 3:24 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.107
Location:	SATA 1	Write protection:	On
Device model:	JAJS300M120C	Device serial:	30013348333
Size:	120 GB (120,034,123,776 bytes)	Device firmware:	S1022A0
Case investigator:		Case description:	

Imaging completed

Targets

ST9320325AS 6VDEE0QR	320 GB	SATA 3
ST320LT014-9YK142 W0Q326G4	320 GB	SATA 4
ST320LT009-9WC142 W0Q4NBT5	320 GB	SATA 5
WDC WD3200JD-22KLB0 WDWCAMR1837670	320 GB	SATA 7
JAJS300M120C 30013348333.raw	120 GB	S/shared/Home/

Passes:	5 passes with default settings for damaged drives
Scheduled sectors:	234,441,648
Imaged sectors:	234,441,648
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-JAJS300M120C_30013348333_S1022A0.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

The Imaging completed report.

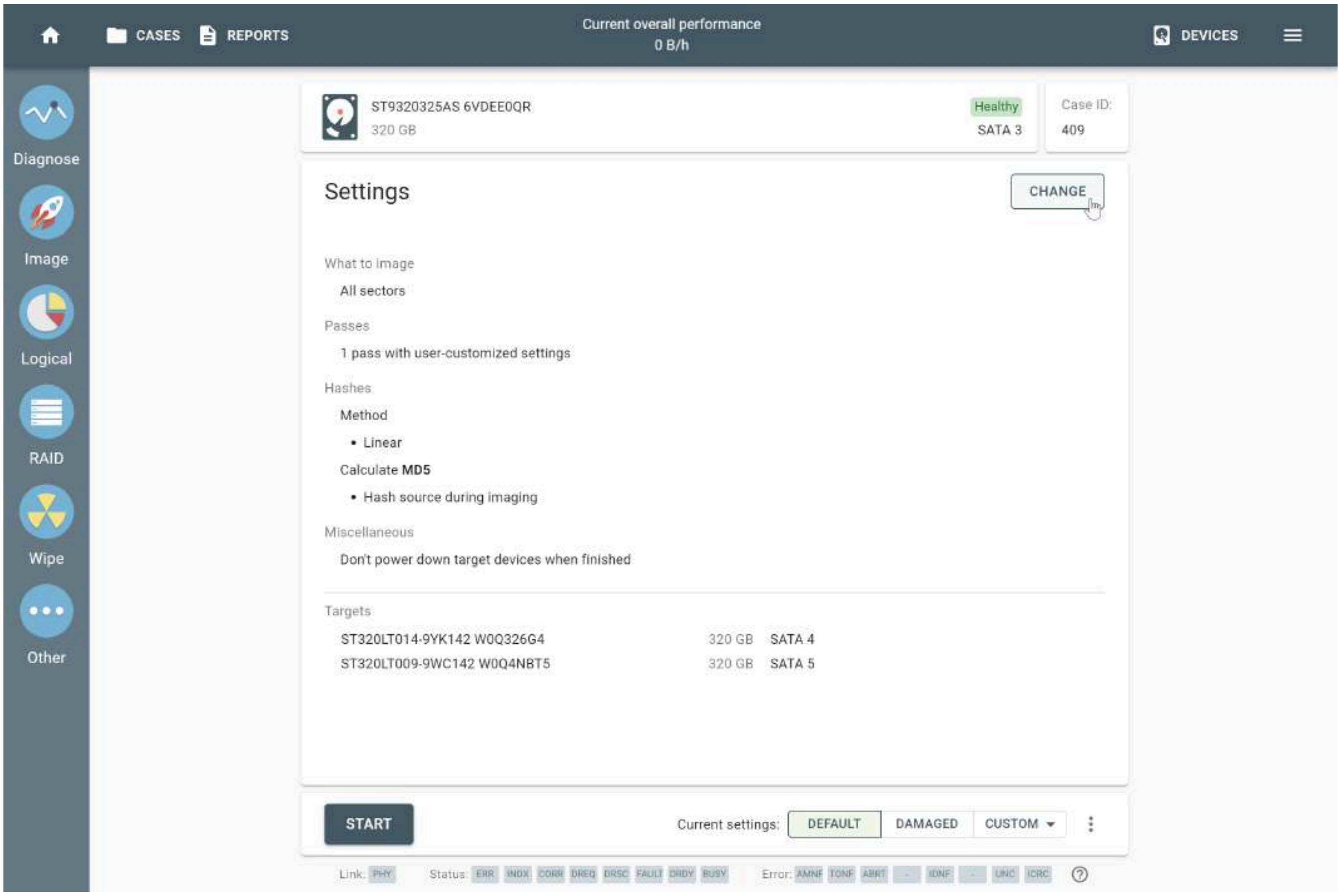
Imaging a drive to two targets with post-hashing

Atola TaskForce's imaging functionality provides many adjustable settings to help forensic examiners follow the guidelines set by their organizations as well as common-sense evidence handling routines.

When you need to create two images of a source drive and verify that both images are identical to the source drive, you will need to calculate the hashes of both targets after imaging. To optimize the process, post-hashing of both target devices is easily configured in imaging settings.

Here's how to do it:

1. Go to **Image**.
2. Select Source and Target devices.
3. TaskForce 2 redirects you to the page with the summary of current imaging settings. By default, hashing of source drive during imaging is enabled.
4. To adjust the imaging settings, click **Change**.


CASES
REPORTS
Current overall performance
0 B/h
DEVICES
Diagnose
Image
Logical
RAID
Wipe
Other
CHANGE
START
DAMAGED
CUSTOM
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

ST9320325AS 6VDEE0QR
320 GB
Healthy
SATA 3

Case ID:
409

Settings

What to image
All sectors

Passes
1 pass with user-customized settings

Hashes
Method
- Linear

Calculate **MD5**
- Hash source during imaging

Miscellaneous
Don't power down target devices when finished

Targets

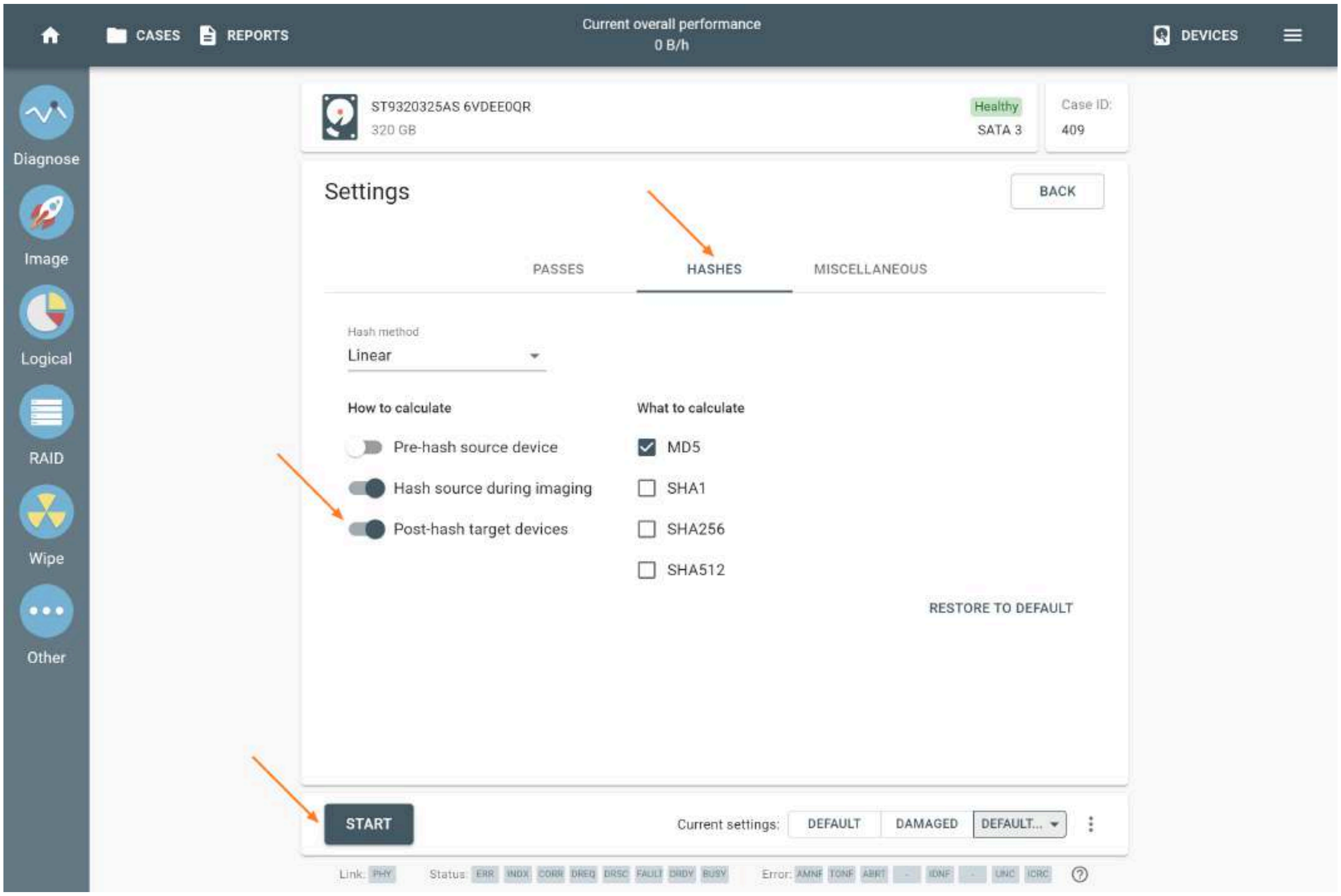
ST320LT014-9YK142 W0Q326G4	320 GB	SATA 4
ST320LT009-9WC142 W0Q4NBT5	320 GB	SATA 5

Current settings: DEFAULT

Changing default imaging settings.

5. In the imaging settings, open the **Hashes** tab and toggle **Post-hash target devices**.

6. To proceed with imaging, click **Start**.



ST9320325AS 6VDEE0QR
320 GB
Healthy
SATA 3
Case ID: 409

Settings

Hash method: Linear

How to calculate

- ○ Pre-hash source device
- ● Hash source during imaging
- ● Post-hash target devices

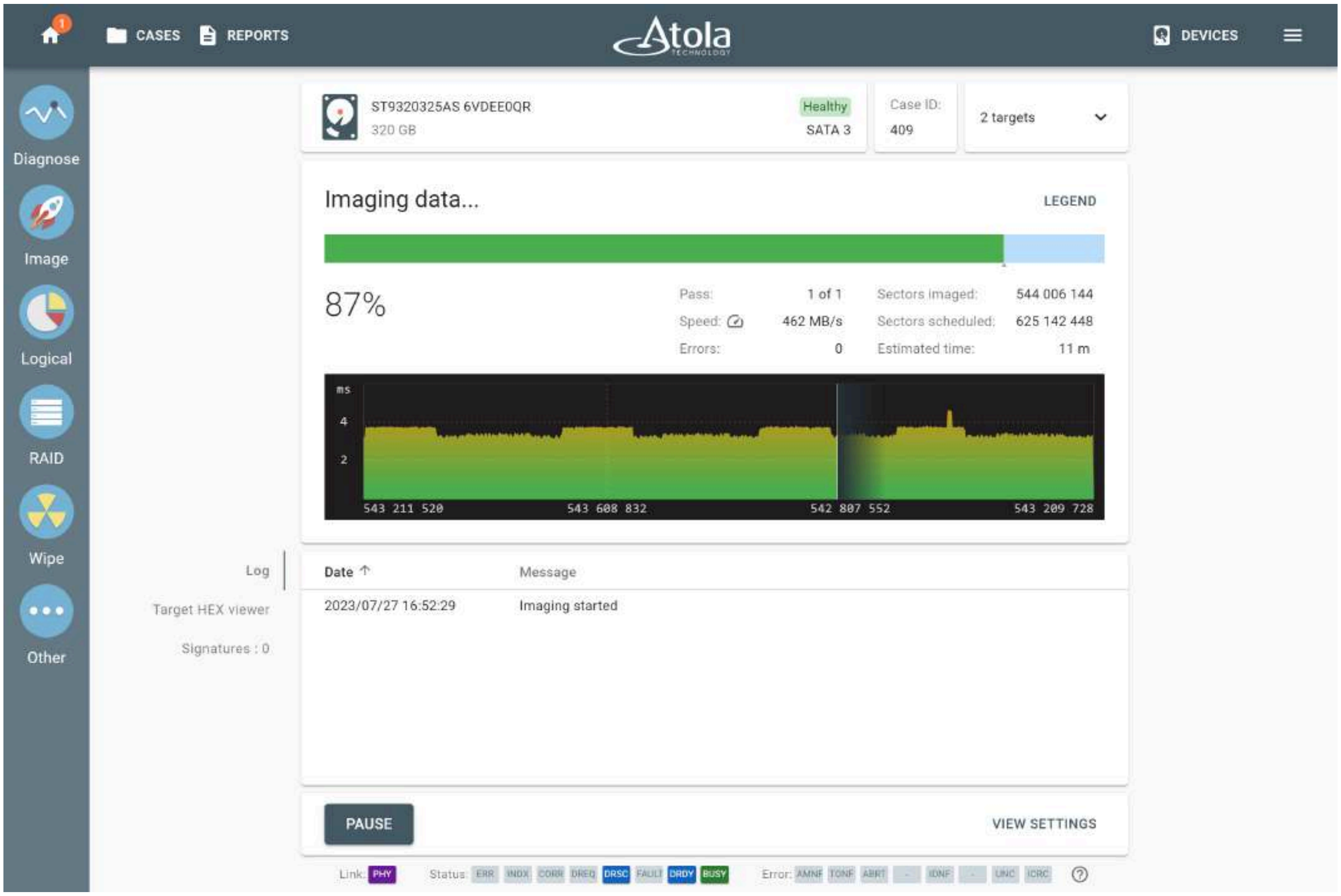
What to calculate

- ☑ MD5
- □ SHA1
- □ SHA256
- □ SHA512

Current settings: DEFAULT

Enabling post-hashing of targets.

Hashing of source drive during imaging is a preferred option because it only requires the data on the evidence drive to be read once, for both imaging and hash calculation. This ensures both a forensically sound process and minimal impact to potentially unstable media. Hashing during imaging does not slow down imaging process.



ST9320325AS 6VDEE0QR
320 GB
Healthy
SATA 3
Case ID: 409
2 targets

Imaging data...

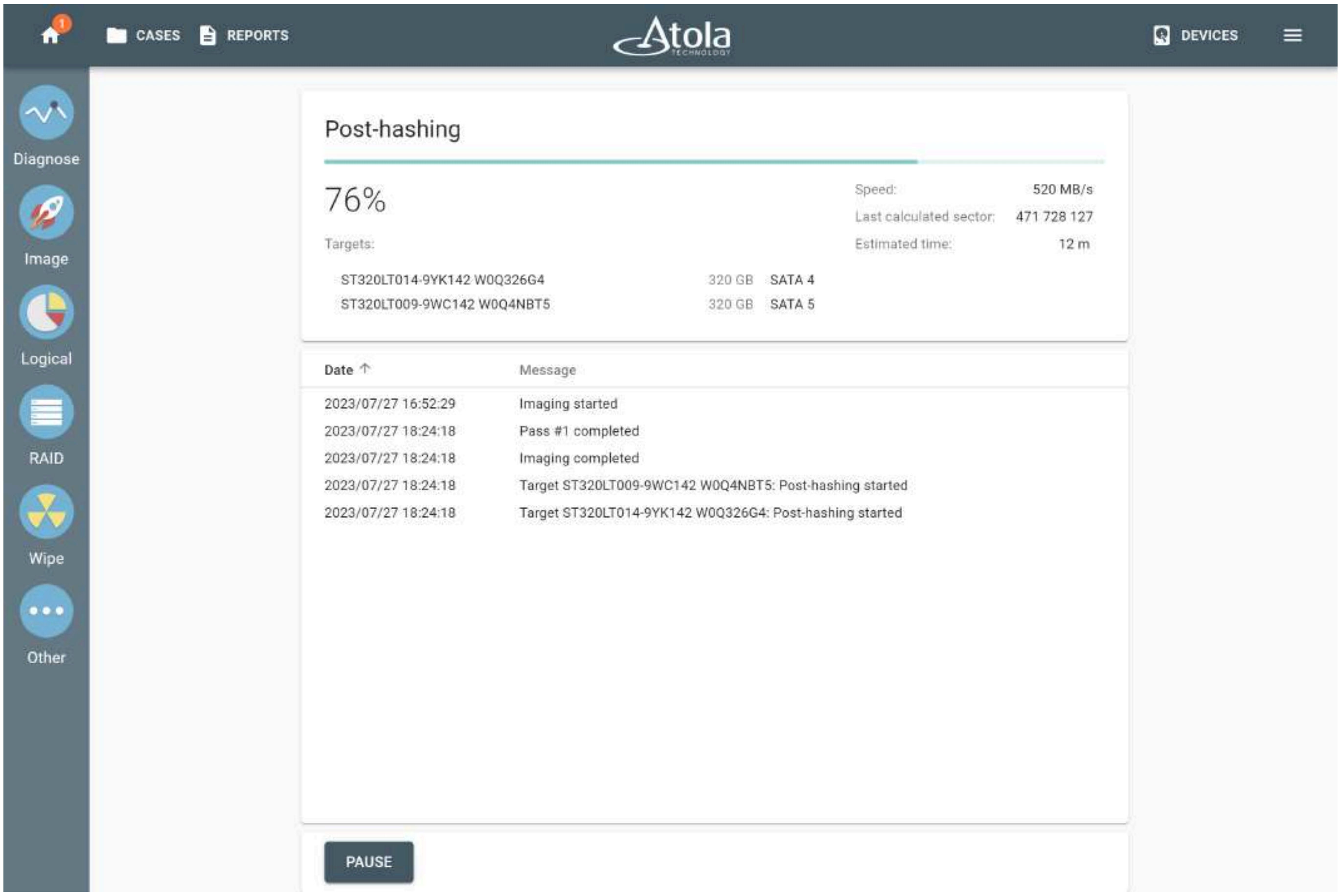
87%

Pass: 1 of 1
Speed: 462 MB/s
Errors: 0
Sectors imaged: 544 006 144
Sectors scheduled: 625 142 448
Estimated time: 11 m

Date	Message
2023/07/27 16:52:29	Imaging started

Imaging progress.

Once imaging is completed, post-hashing begins immediately on both target devices:



Post-hashing

76%

Speed: 520 MB/s
Last calculated sector: 471 728 127
Estimated time: 12 m

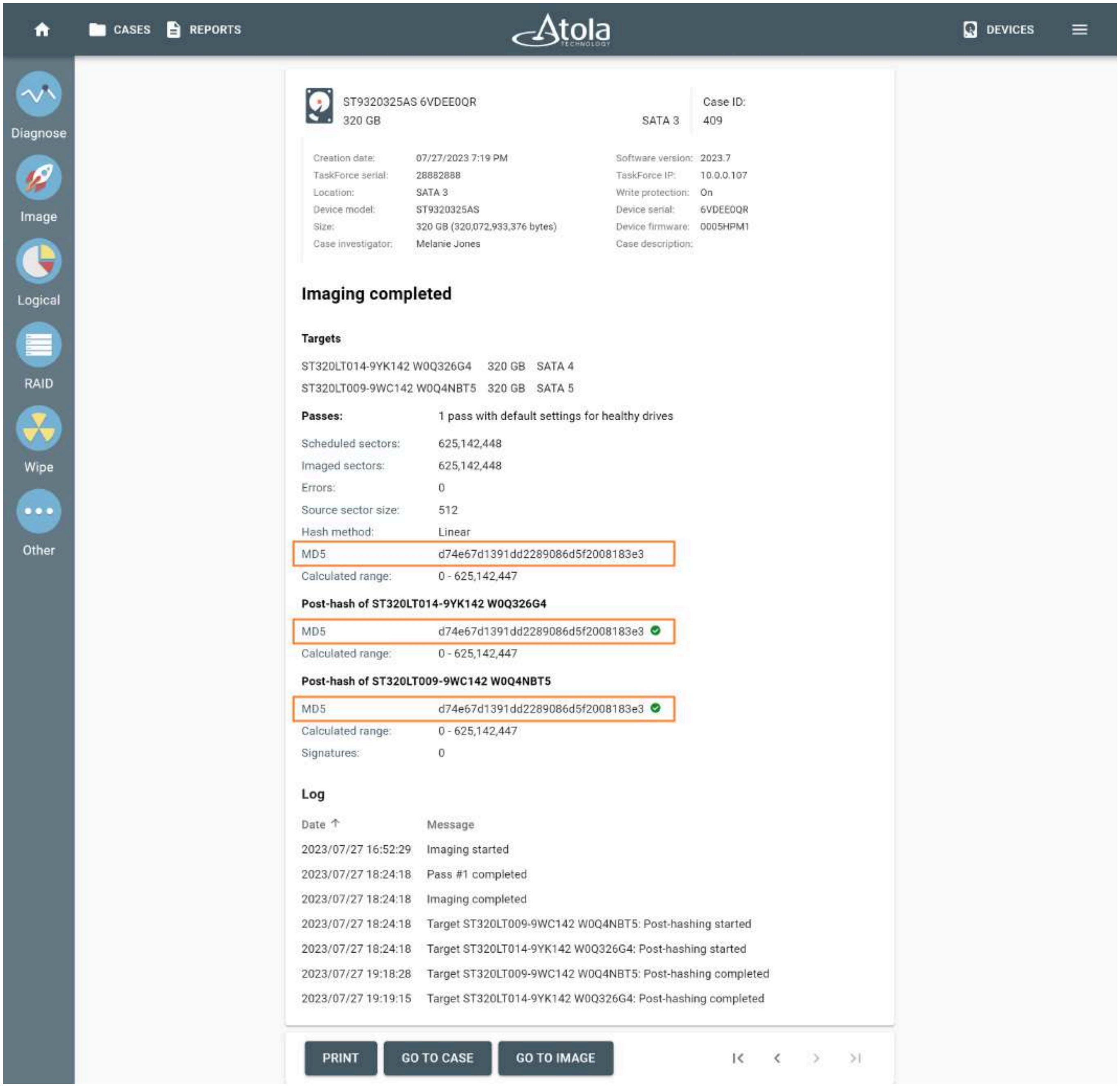
Targets:

ST320LT014-9YK142 W0Q326G4	320 GB	SATA 4
ST320LT009-9WC142 W0Q4NBT5	320 GB	SATA 5

Date	Message
2023/07/27 16:52:29	Imaging started
2023/07/27 18:24:18	Pass #1 completed
2023/07/27 18:24:18	Imaging completed
2023/07/27 18:24:18	Target ST320LT009-9WC142 W0Q4NBT5: Post-hashing started
2023/07/27 18:24:18	Target ST320LT014-9YK142 W0Q326G4: Post-hashing started

Post-hashing in progress.

In the end, TaskForce 2 produces a report that documents hashes of both source and target devices:



ST9320325AS 6VDEE0QR
320 GB
SATA 3

Case ID:
409

Creation date:	07/27/2023 7:19 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.107
Location:	SATA 3	Write protection:	On
Device model:	ST9320325AS	Device serial:	6VDEE0QR
Size:	320 GB (320,072,933,376 bytes)	Device firmware:	0005HPM1
Case investigator:	Melanie Jones	Case description:	

Imaging completed

Targets

ST320LT014-9YK142 W0Q326G4 320 GB SATA 4
ST320LT009-9WC142 W0Q4NBT5 320 GB SATA 5

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	625,142,448
Imaged sectors:	625,142,448
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	d74e67d1391dd2289086d5f2008183e3
Calculated range:	0 - 625,142,447

Post-hash of ST320LT014-9YK142 W0Q326G4

MD5	d74e67d1391dd2289086d5f2008183e3 ✓
Calculated range:	0 - 625,142,447

Post-hash of ST320LT009-9WC142 W0Q4NBT5

MD5	d74e67d1391dd2289086d5f2008183e3 ✓
Calculated range:	0 - 625,142,447
Signatures:	0

Log

Date ↑	Message
2023/07/27 16:52:29	Imaging started
2023/07/27 18:24:18	Pass #1 completed
2023/07/27 18:24:18	Imaging completed
2023/07/27 18:24:18	Target ST320LT009-9WC142 W0Q4NBT5: Post-hashing started
2023/07/27 18:24:18	Target ST320LT014-9YK142 W0Q326G4: Post-hashing started
2023/07/27 19:18:28	Target ST320LT009-9WC142 W0Q4NBT5: Post-hashing completed
2023/07/27 19:19:15	Target ST320LT014-9YK142 W0Q326G4: Post-hashing completed

Imaging report with source and target hashes.

Imaging to an E01 file with dual hash

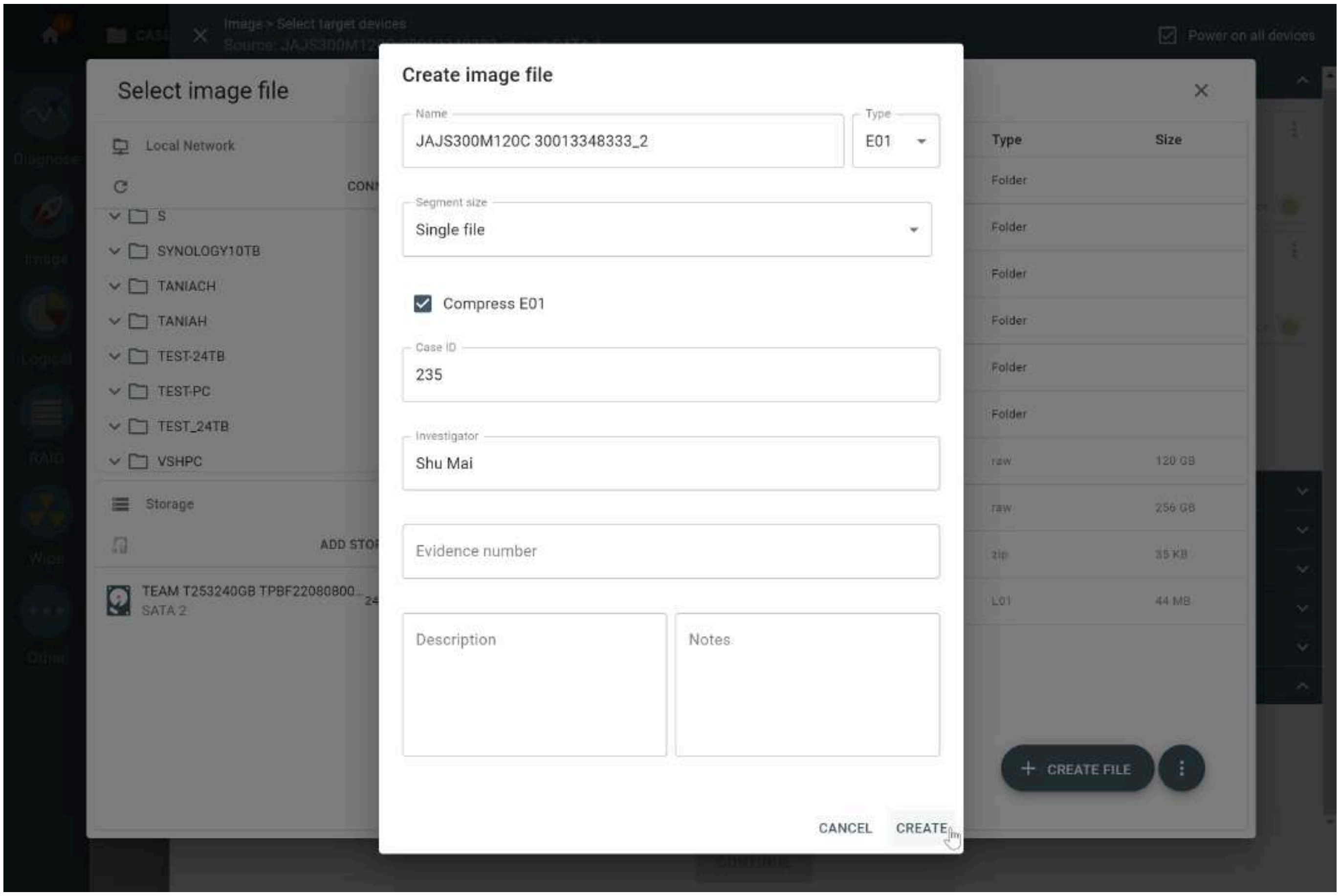
E01 file format is the de facto standard format for forensic examiners to store images due to its ability to store not only a copy of the evidence drive, but also case and evidence details. E01 file can also store both MD5 and SHA1 hash values calculated during imaging.

To image a source evidence drive to an E01 file, you have to create a new target file.

Creating a new E01 file

1. Go to **Image**.
2. Select the source evidence drive.

3. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.
4. In the file selector, find the folder to store the image and click **Create file**.
5. In the **Create image file** dialog, select the E01 file type.
6. Fill in E01 file information, and then click **Create**.
7. On the **Select target devices** panel, click **Continue**.



Create image file

Name: JAJS300M120C 30013348333_2

Type: E01

Segment size: Single file

☑ Compress E01

Case ID: 235

Investigator: Shu Mai

Evidence number

Description

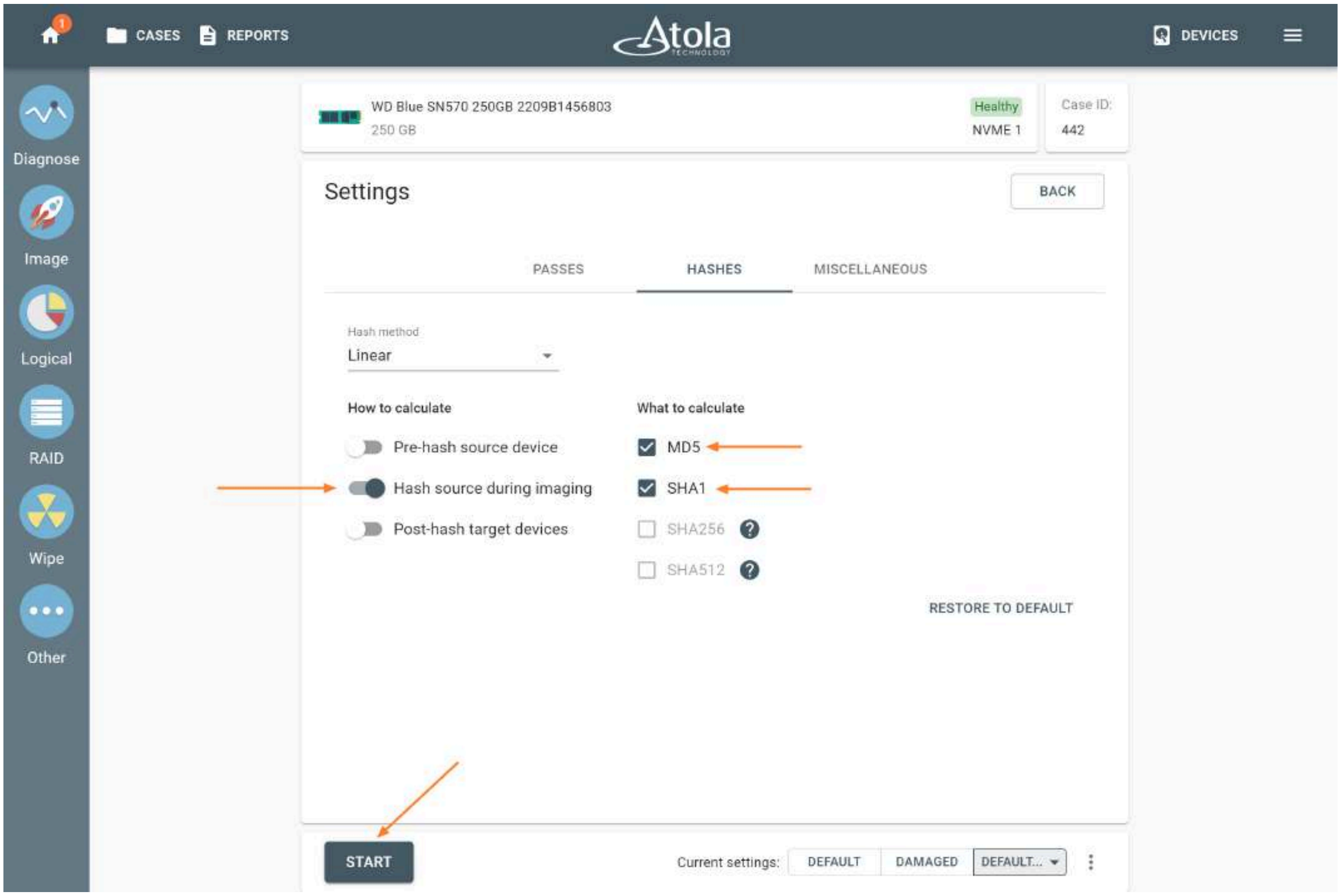
Notes

CANCEL CREATE

Creating an E01 file.

Enable dual-hash and start imaging

1. Once you have selected the source drive and created the target file, you end up on the **Settings** summary page. To adjust the imaging settings, click **Change**.
2. On the **Hashes** tab, make sure that **Hash source during imaging** is selected, also select both MD5 and SHA1 hash types.
3. To proceed with imaging, click **Start**.



WD Blue SN570 250GB 2209B1456803
250 GB
Healthy
NVME 1
Case ID: 442

Settings

Hash method: Linear

How to calculate

- ○ Pre-hash source device
- ● Hash source during imaging
- ○ Post-hash target devices

What to calculate

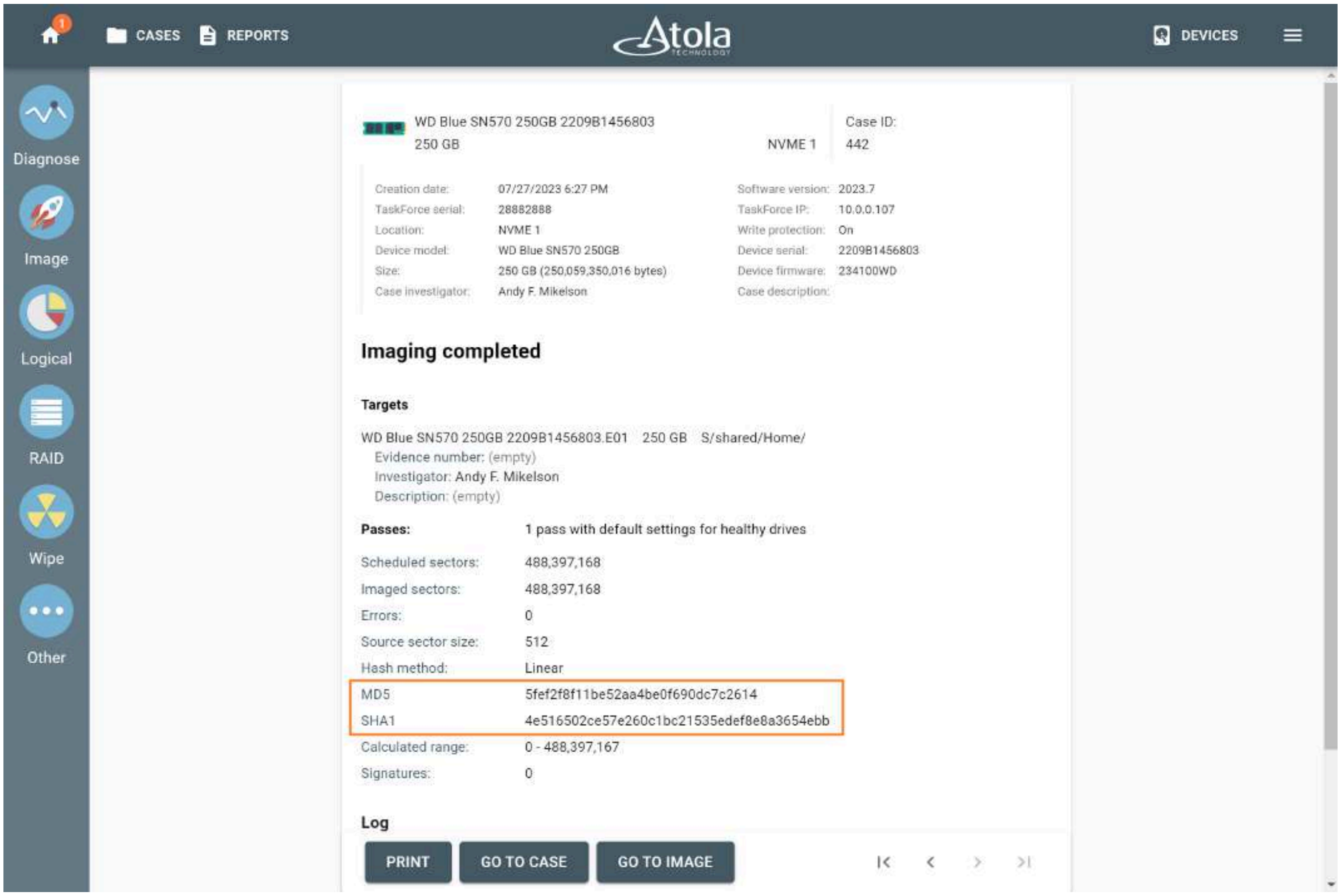
- ☑ MD5
- ☑ SHA1
- □ SHA256
- □ SHA512

Current settings:

Adjusting imaging settings.

The report and the E01 file

Upon completion of imaging, you can see both MD5 and SHA1 hash values indicated in the **Imaging completed** report.



WD Blue SN570 250GB 2209B1456803
250 GB

NVME 1

Case ID:
442

Creation date:	07/27/2023 6:27 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.107
Location:	NVME 1	Write protection:	On
Device model:	WD Blue SN570 250GB	Device serial:	2209B1456803
Size:	250 GB (250,059,350,016 bytes)	Device firmware:	234100WD
Case investigator:	Andy F. Mikelson	Case description:	

Imaging completed

Targets

WD Blue SN570 250GB 2209B1456803.E01 250 GB S/shared/Home/
Evidence number: (empty)
Investigator: Andy F. Mikelson
Description: (empty)

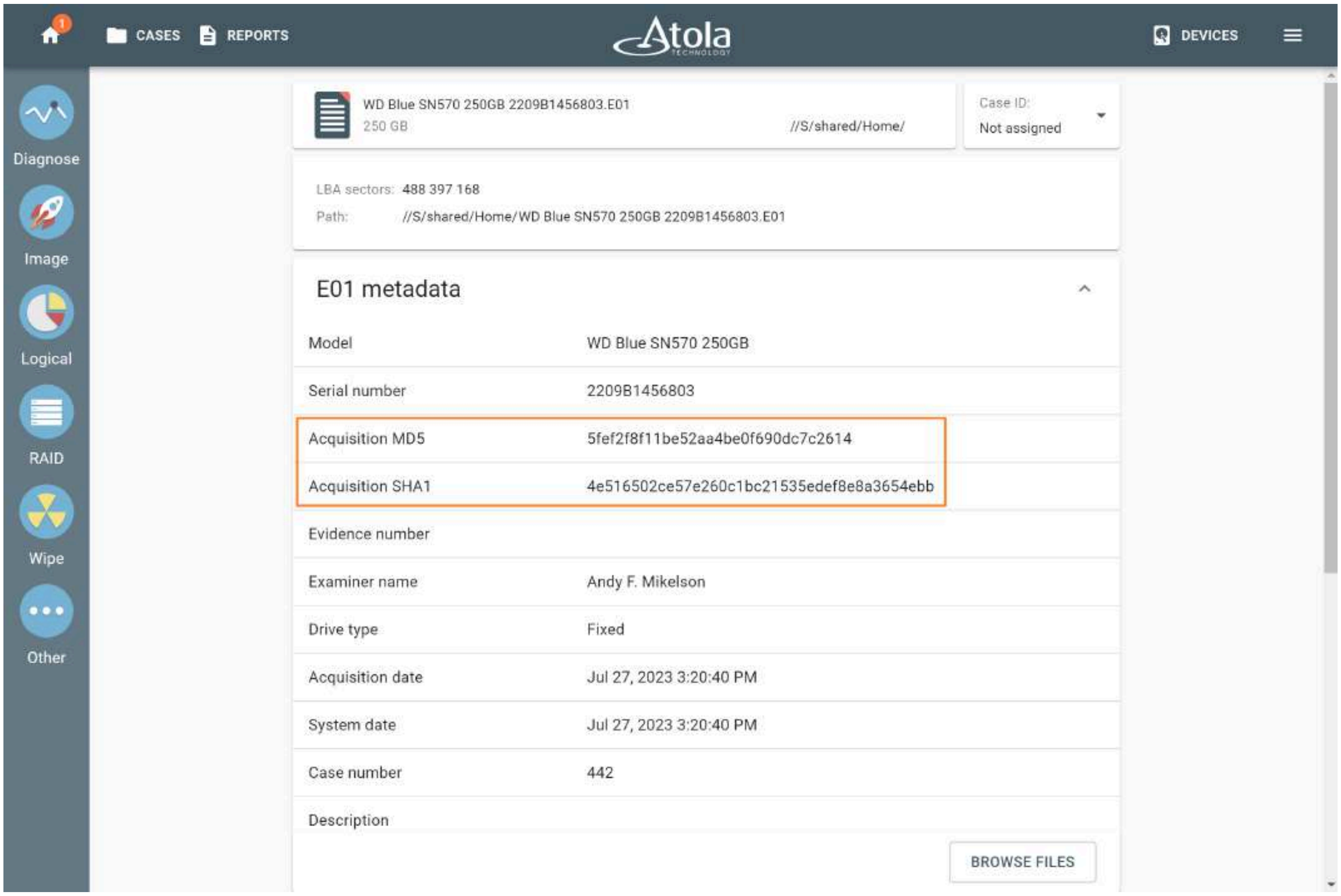
Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	488,397,168
Imaged sectors:	488,397,168
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	5fef2f8f11be52aa4be0f690dc7c2614
SHA1	4e516502ce57e260c1bc21535edef8e8a3654ebb
Calculated range:	0 - 488,397,167
Signatures:	0

Log

Imaging report.

It is also possible to look up the information of the created E01 file. To do that, perform the following actions:

1. Click **Devices** at the top right.
2. Expand the **File** section and click **Select file**.
3. Choose your file. TaskForce 2 opens the file information page with all the metadata of the E01 file. The MD5 and SHA hash values are listed there, too.



WD Blue SN570 250GB 2209B1456803.E01
250 GB
//S/shared/Home/

Case ID:
Not assigned

LBA sectors: 488 397 168
Path: //S/shared/Home/WD Blue SN570 250GB 2209B1456803.E01

E01 metadata

Model	WD Blue SN570 250GB
Serial number	2209B1456803
Acquisition MD5	5fef2f8f11be52aa4be0f690dc7c2614
Acquisition SHA1	4e516502ce57e260c1bc21535edef8e8a3654ebb
Evidence number	
Examiner name	Andy F. Mikelson
Drive type	Fixed
Acquisition date	Jul 27, 2023 3:20:40 PM
System date	Jul 27, 2023 3:20:40 PM
Case number	442
Description	

E01 file with calculated MD5 and SHA1 hashes.

Imaging to a compressed E01 file on a target drive

In TaskForce 2, you can image source drives to target files on a storage device connected directly to one of the imager's drive ports. E01, AFF4, and RAW file formats are supported. E01 and AFF4 files can be compressed.

To create multiple target images on a directly connected drive, first, you need to set this device to the Storage mode.

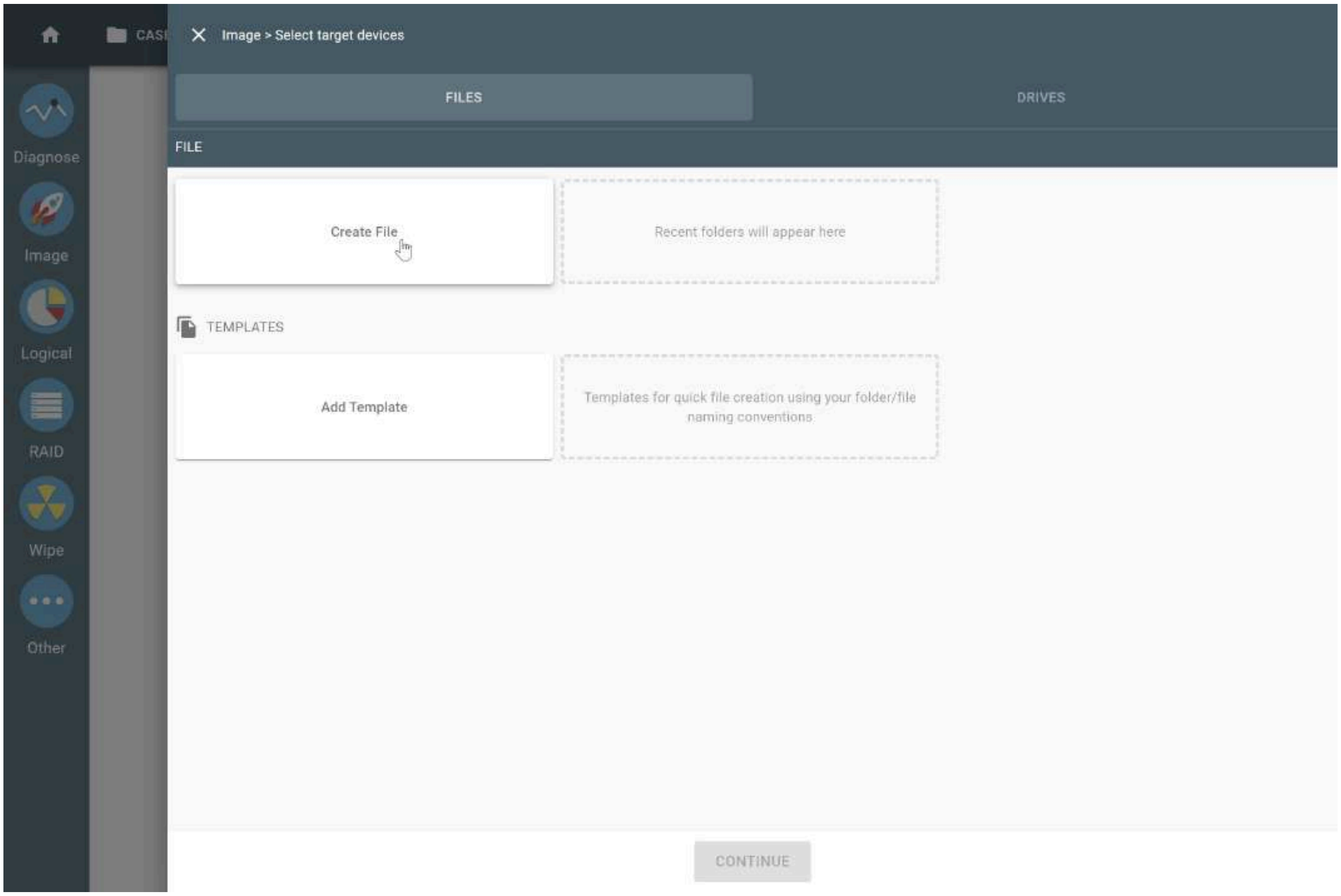
If a drive is already in the Storage mode, plug it into one of the TaskForce drive ports and use it to store target image files without additional formatting. You can image several evidence devices to target files on storage **simultaneously**.

The drive in the Storage mode is marked with a special blue icon on the **Select target devices** panel. A LED status indicator of the respective drive port on the TaskForce 2 front panel also turns blue.

Set a device to the Storage mode

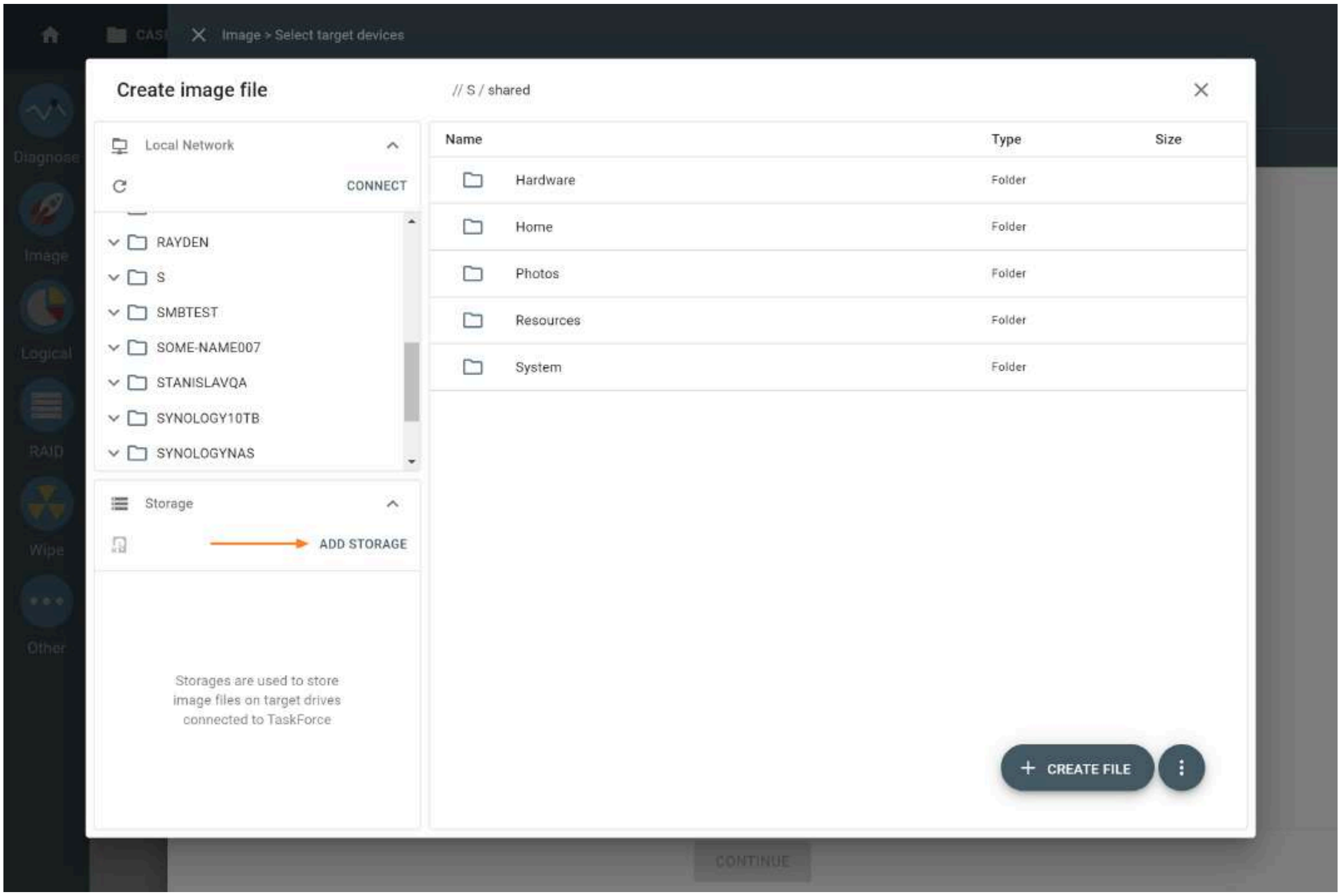
To set a target device to the Storage mode:

1. Go to **Image**.
2. Select the source evidence drive.
3. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.


CASE
Image > Select target devices
FILES
DRIVES
FILE
Create File
Recent folders will appear here
TEMPLATES
Add Template
Templates for quick file creation using your folder/file naming conventions
CONTINUE
Diagnose
Image
Logical
RAID
Wipe
Other

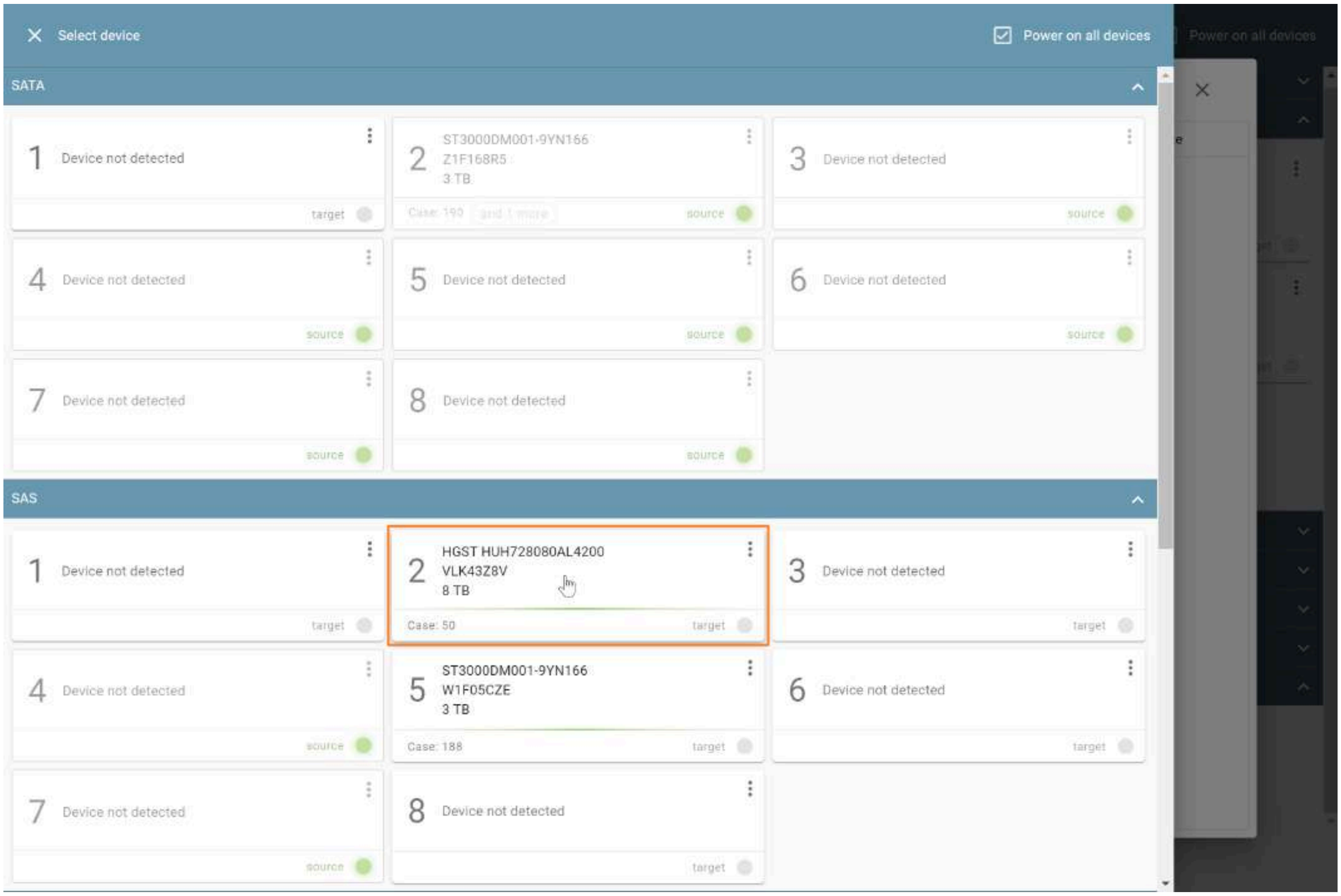
Selecting a target file.

4. In the **Select image file** window, click **Add storage**.



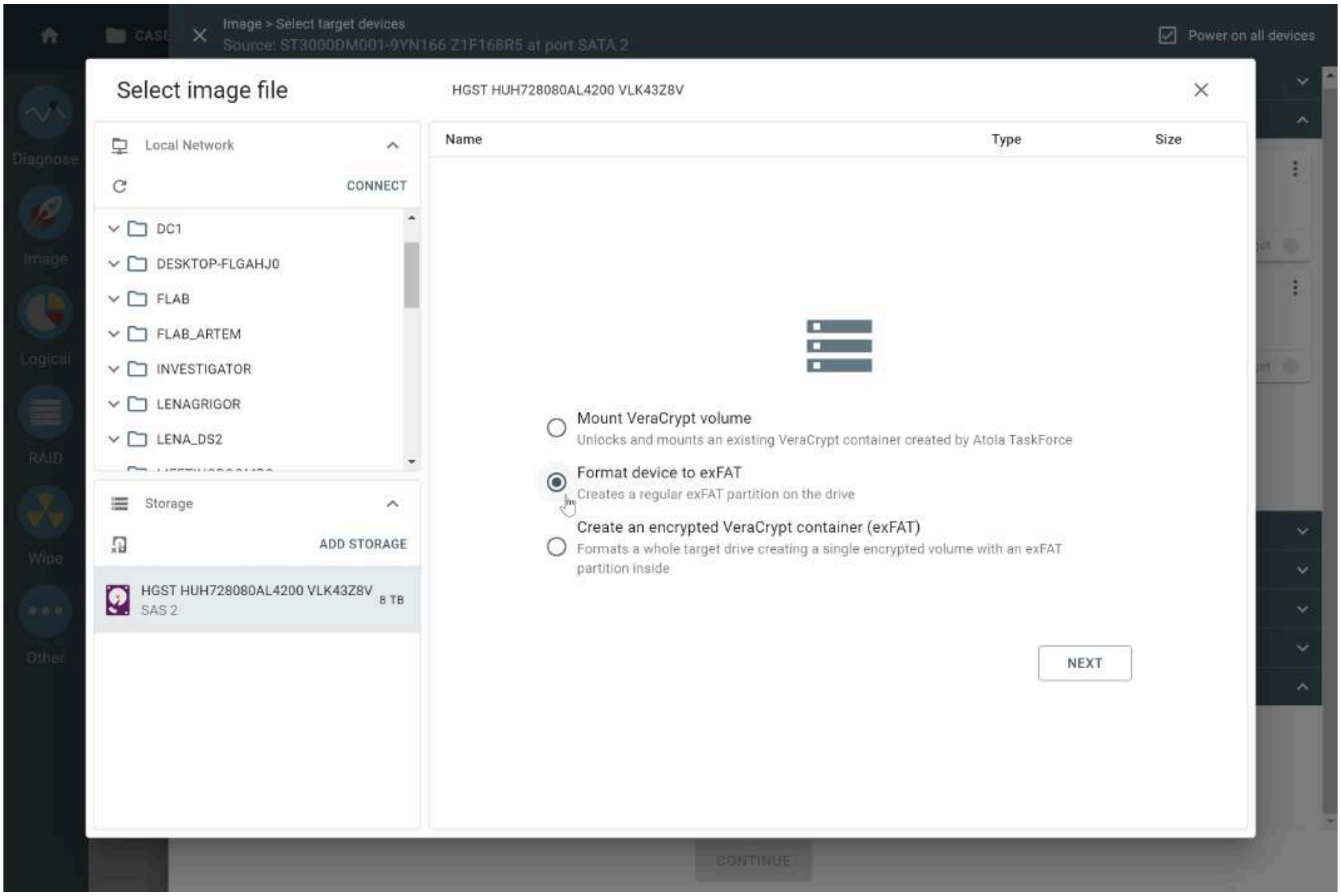
Adding a storage drive.

5. On the **Select device** panel, choose the drive you want to use in the Storage mode. TaskForce 2 uses a lighter shade of blue to indicate that a storage drive is being configured.



Selecting a storage drive.

6. If TaskForce 2 cannot find the appropriate exFAT partition on the selected drive, it offers you to format the device accordingly. In that case, select **Format device to exFAT** and click **Next**.



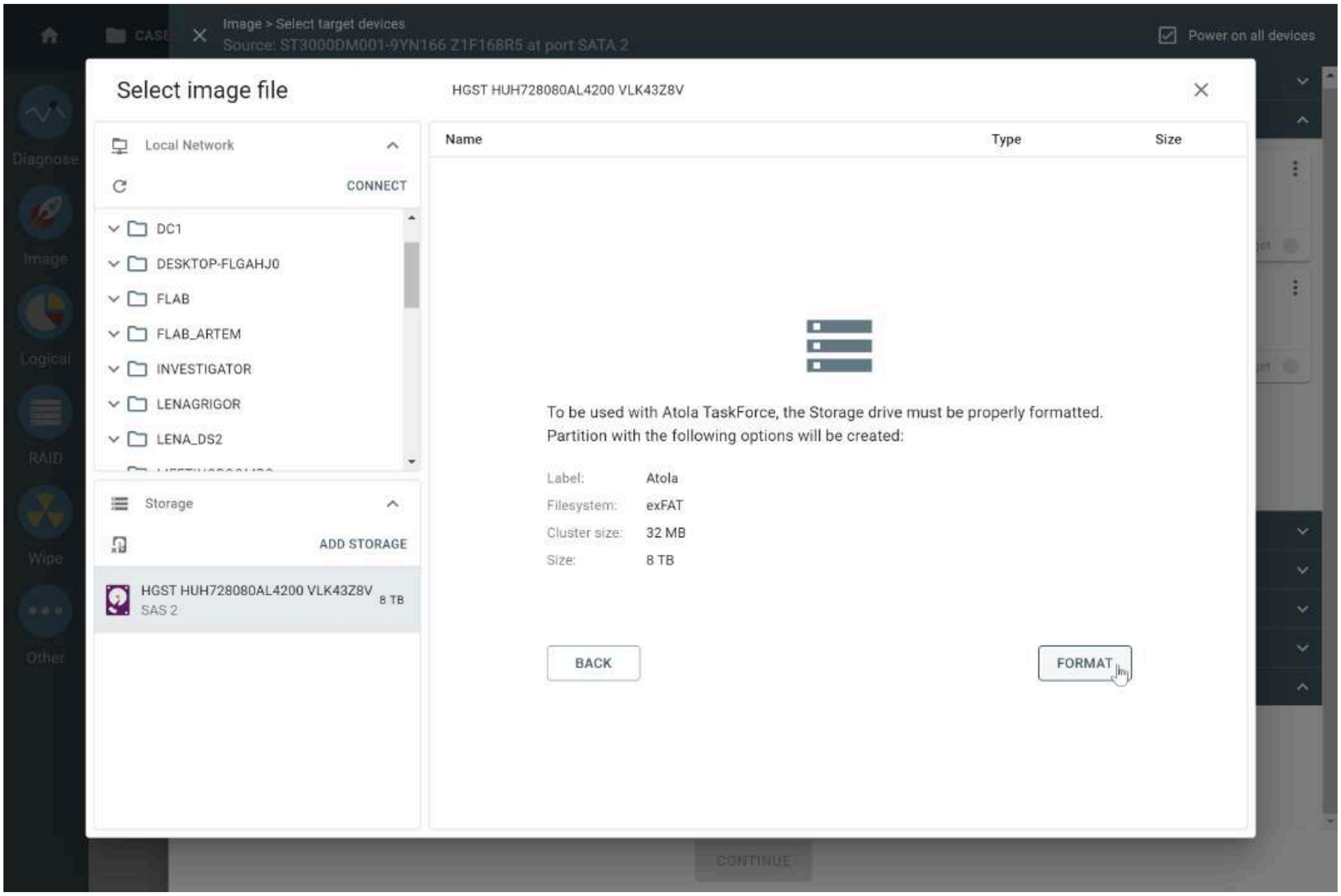
○ Mount VeraCrypt volume
Unlocks and mounts an existing VeraCrypt container created by Atola TaskForce

● Format device to exFAT
Creates a regular exFAT partition on the drive

○ Create an encrypted VeraCrypt container (exFAT)
Formats a whole target drive creating a single encrypted volume with an exFAT partition inside

Formatting the target to exFAT.

7. To launch target device formatting to exFat with a large cluster size (32 MB), click **Format** and enter *YES* for confirmation. This cluster size enables faster imaging to this drive.



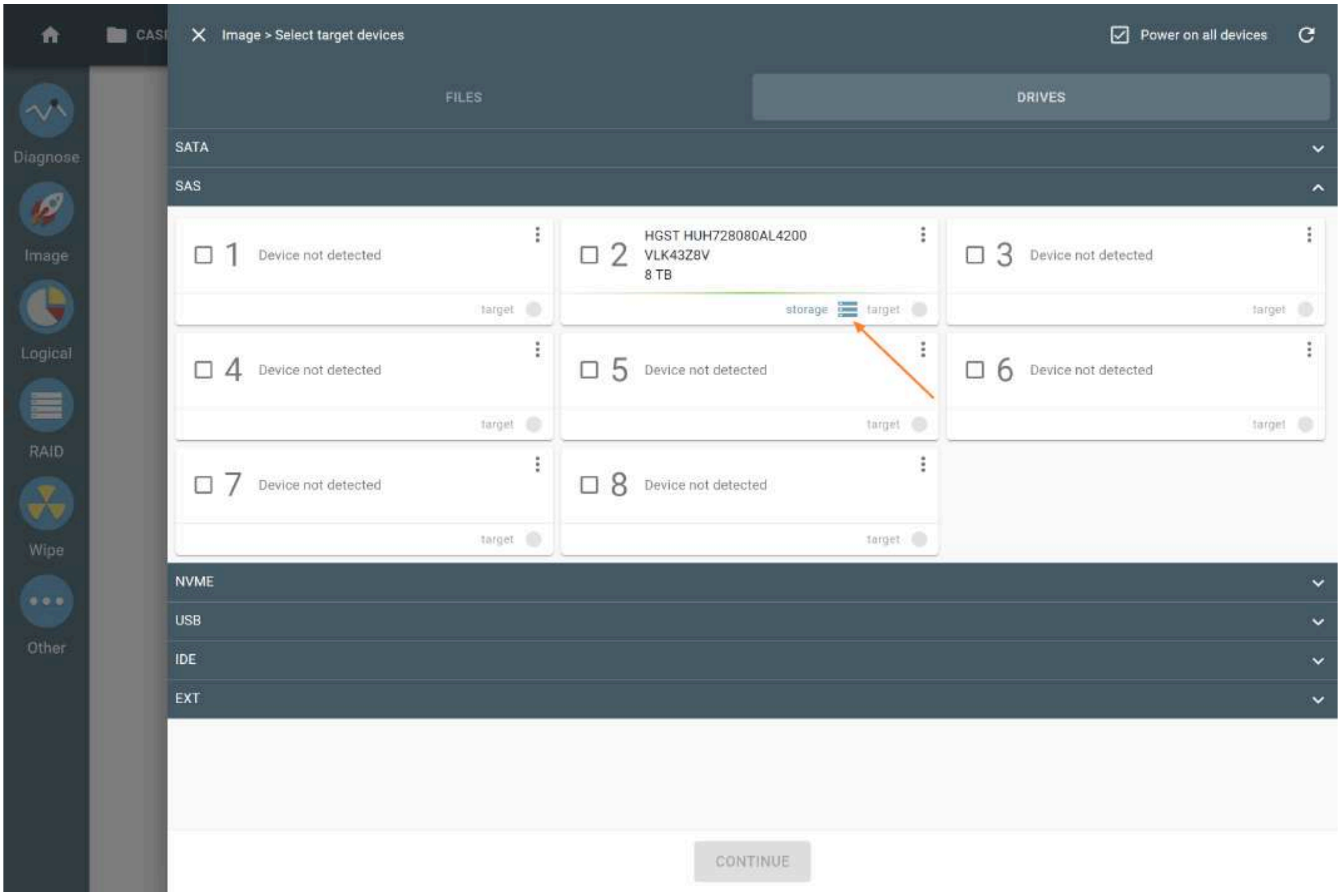
To be used with Atola TaskForce, the Storage drive must be properly formatted.
Partition with the following options will be created:

Label: Atola
Filesystem: exFAT
Cluster size: 32 MB
Size: 8 TB

Formatting the target to exFAT.

Once the target device is formatted, TaskForce 2 perceives it as a Storage target and you can proceed to create a compressed E01 image file on the storage device.

The drive in the Storage mode is marked with a special blue icon on the **Select target devices** panel. A LED status indicator of the respecting drive port on the TaskForce 2 front panel also turns blue.



A drive in the Storage mode.

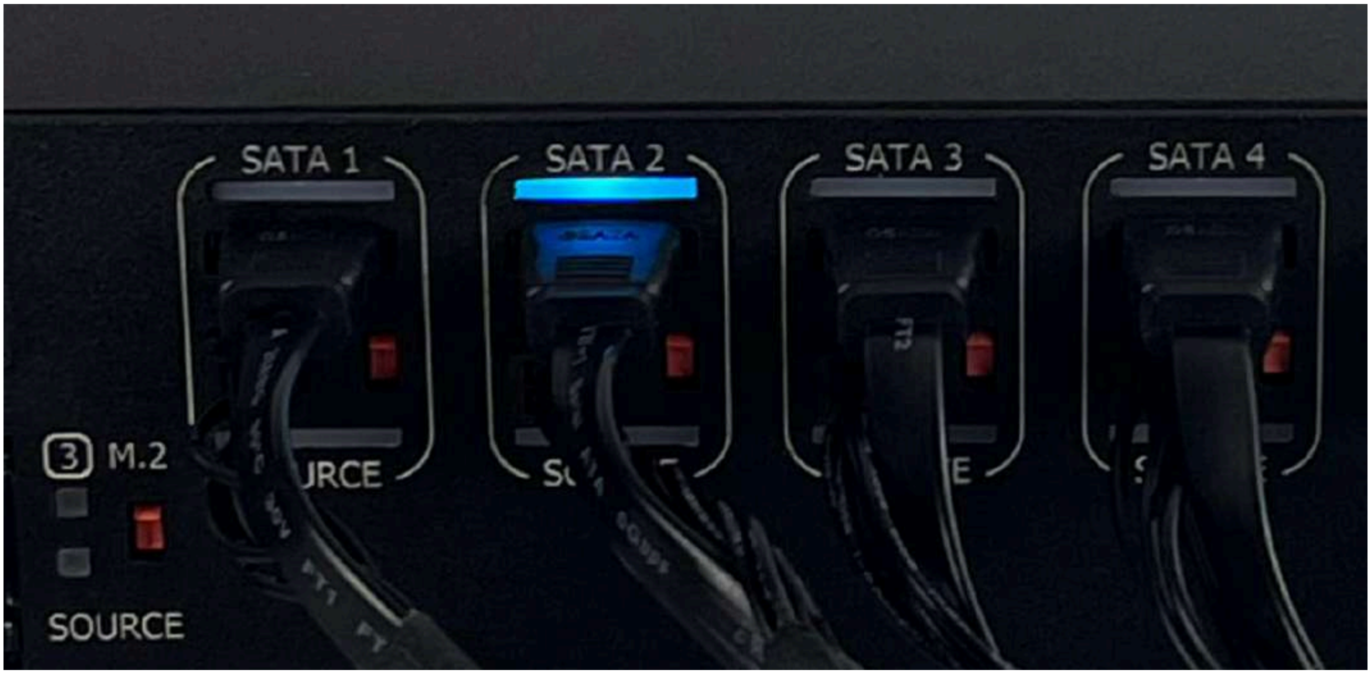
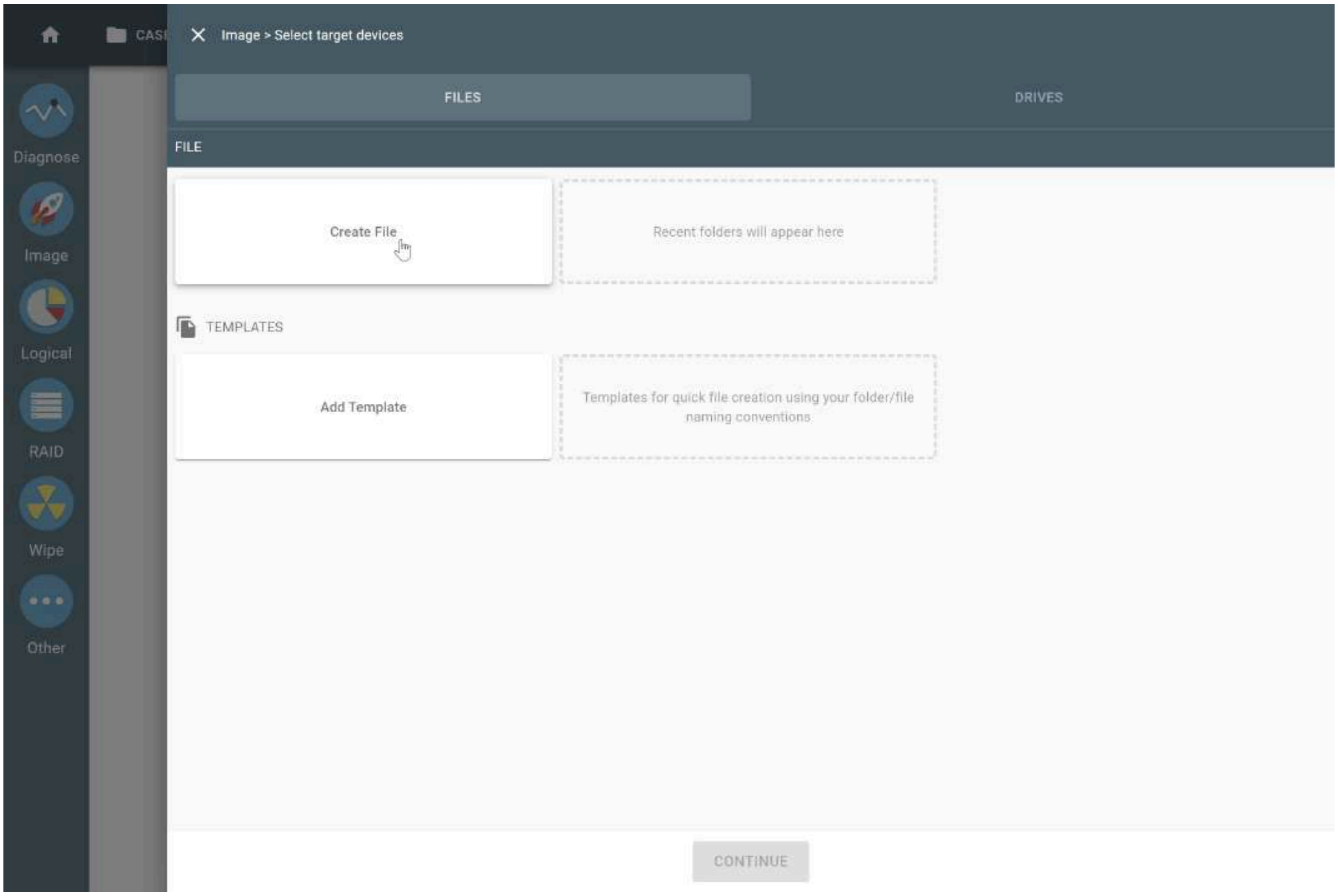


Image to a Storage drive

If you already have a drive configured as a Storage, you can plug it into one of the TaskForce drive ports and use it to store target image files without additional formatting:

1. Go to **Image**.
2. Select the source evidence drive.
3. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.


CASE
Image > Select target devices
FILES
DRIVES
FILE
Create File
Recent folders will appear here
TEMPLATES
Add Template
Templates for quick file creation using your folder/file naming conventions
Diagnose
Image
Logical
RAID
Wipe
Other
CONTINUE

Selecting a target file.

4. On the bottom left in the **Select image file** window, select your Storage drive. Then proceed to create a target image file.

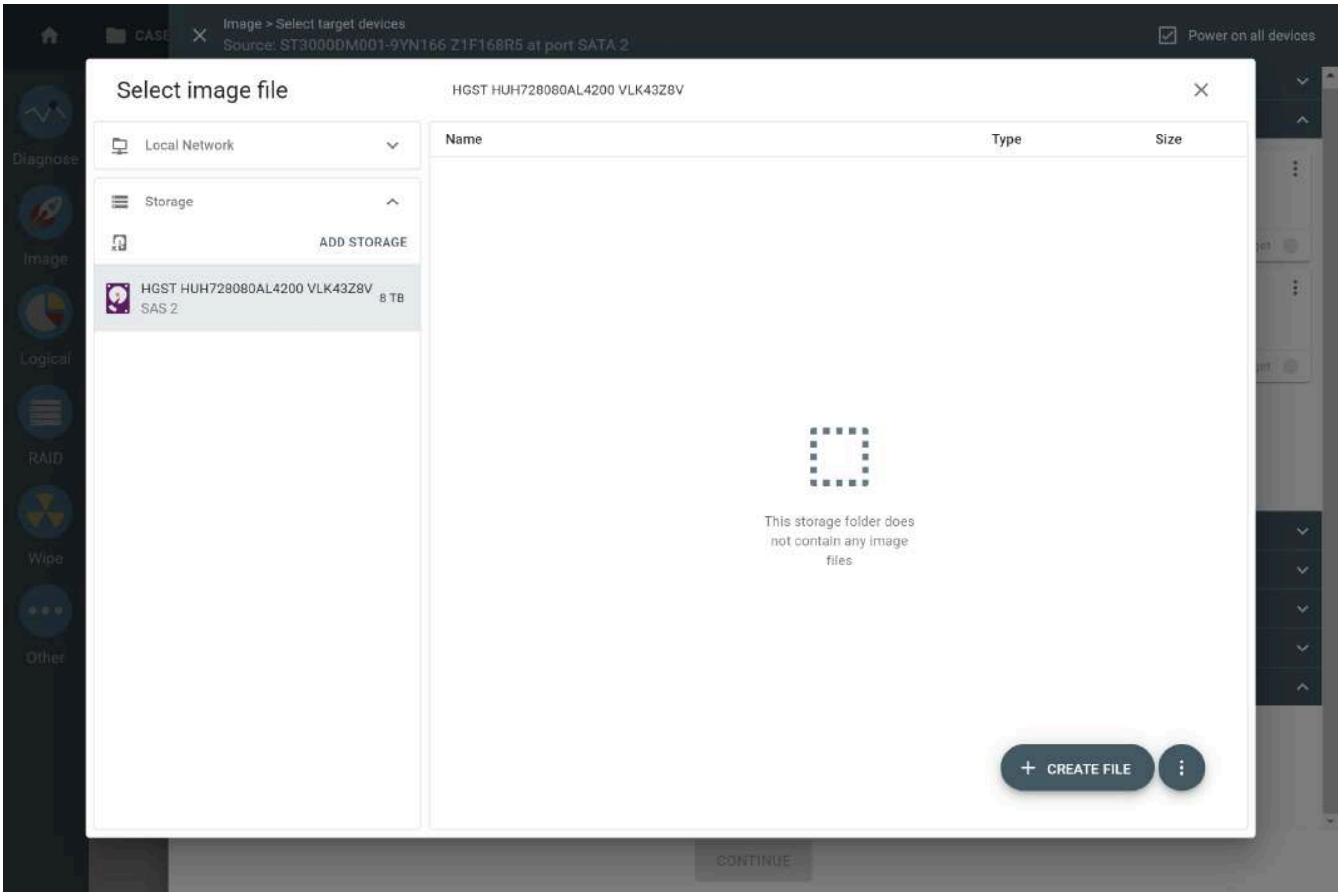


Image > Select target devices
Source: ST3000DM001-9YN166 Z1F168R5 at port SATA 2
Power on all devices
CASE
Diagnose
Image
Logical
RAID
Wipe
Other
Select image file
HGST HUH728080AL4200 VLK43Z8V
Local Network
Storage
ADD STORAGE
HGST HUH728080AL4200 VLK43Z8V
SAS 2
8 TB
Name
Type
Size
This storage folder does not contain any image files
CREATE FILE
CONTINUE

Selecting a target file.

Create a compressed E01 image file

To proceed with creating a compressed E01 image file on the storage device, do the following:

1. In the **Select image file** window, select the storage drive and then click **+ Create file**.

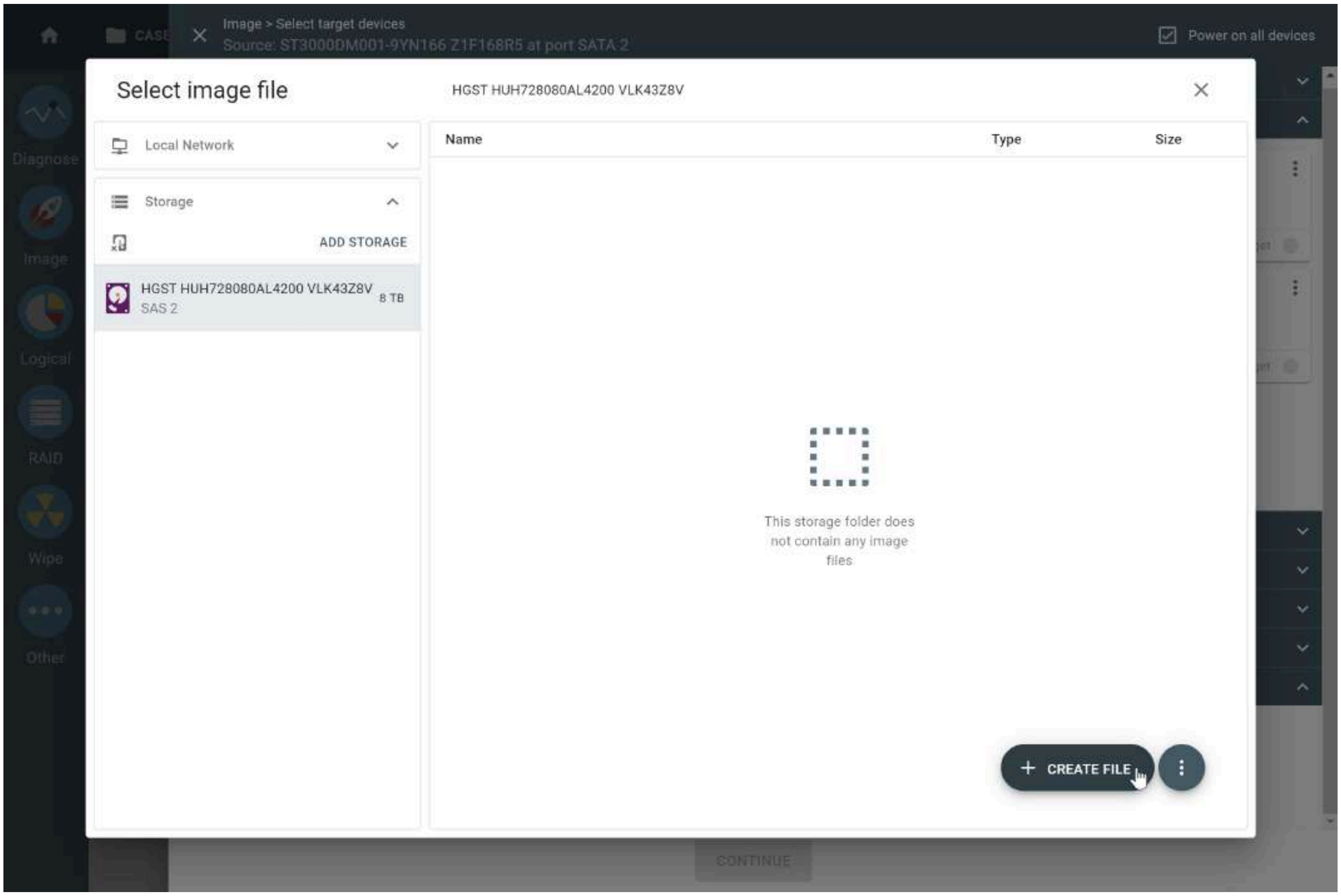
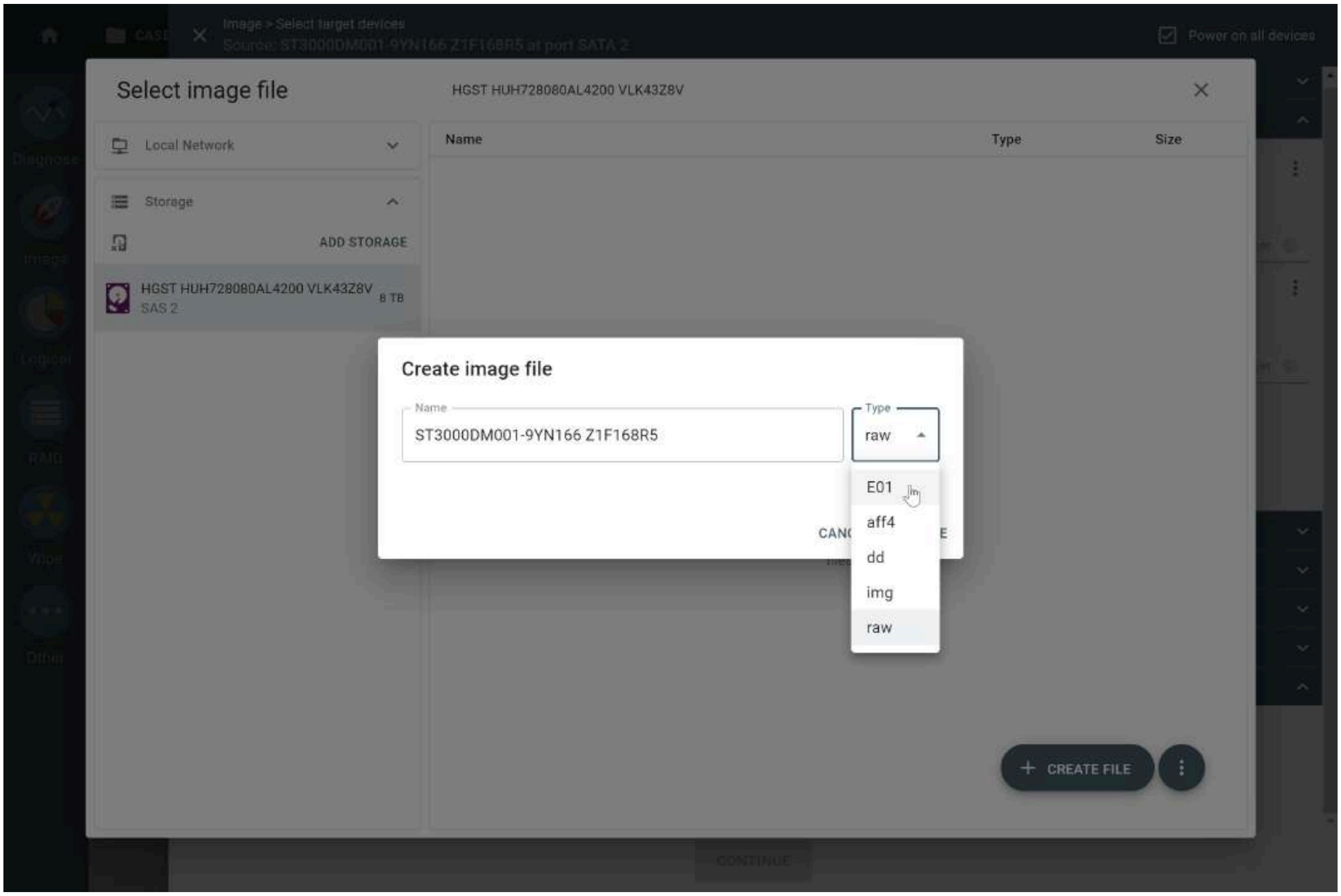


Image > Select target devices
Source: ST3000DM001-9YN166 Z1F168R5 at port SATA 2
Power on all devices
Diagnose
Image
Logical
RAID
Wipe
Other
Select image file
HGST HUH728080AL4200 VLK43Z8V
Local Network
Storage
ADD STORAGE
HGST HUH728080AL4200 VLK43Z8V
SAS 2
8 TB
Name
Type
Size
This storage folder does not contain any image files
CREATE FILE
CONTINUE

Adding a new file.

2. In the **Create image file** dialog, enter the file name and select the E01 file type.

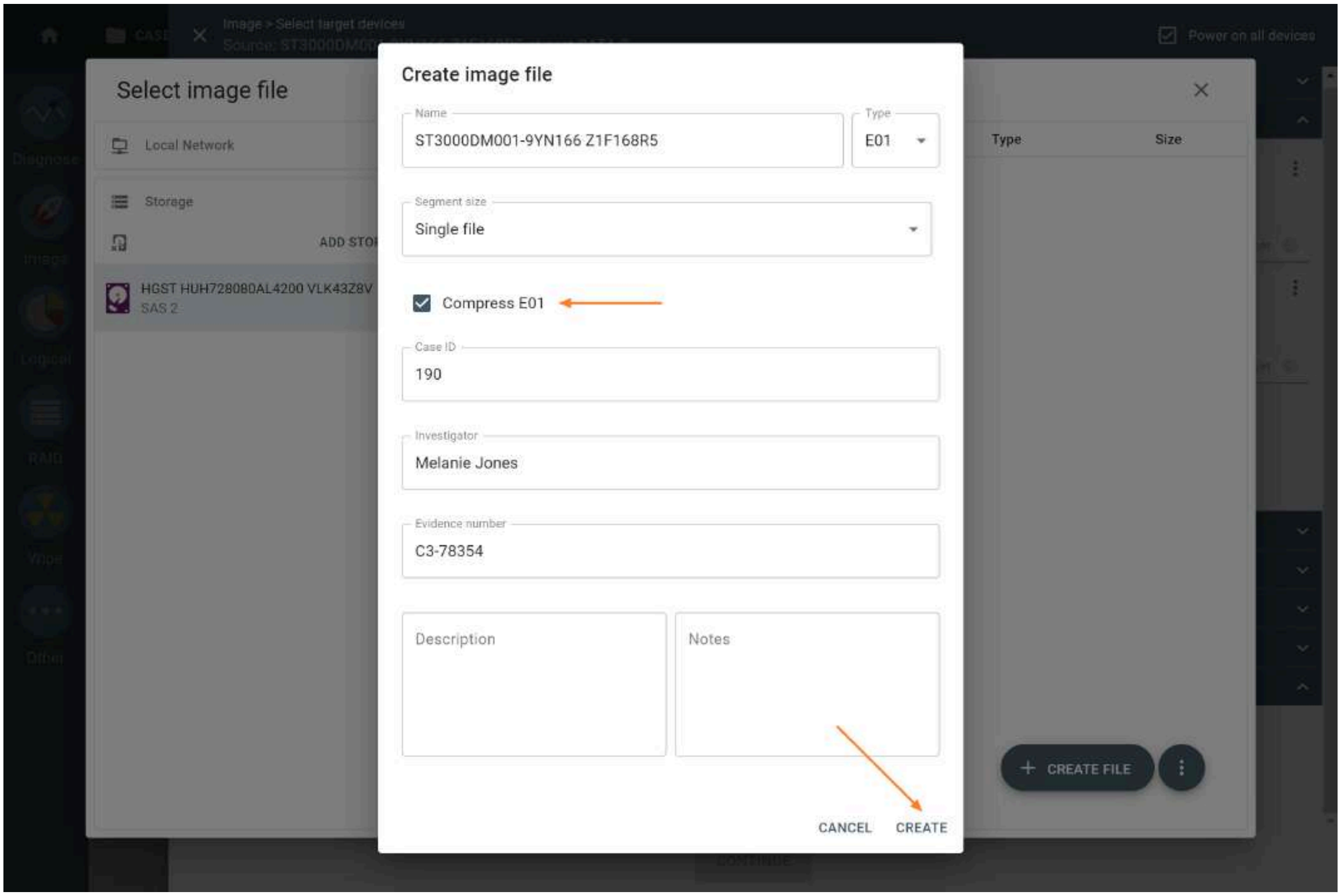


Name: ST3000DM001-9YN166 Z1F168R5

Type: raw

Creating an image file.

3. Select the **Compress E01** option.
4. Fill out other file details, and then click **Create**.



Create image file

Name: ST3000DM001-9YN166 Z1F168R5

Type: E01

Segment size: Single file

☑ Compress E01

Case ID: 190

Investigator: Melanie Jones

Evidence number: C3-78354

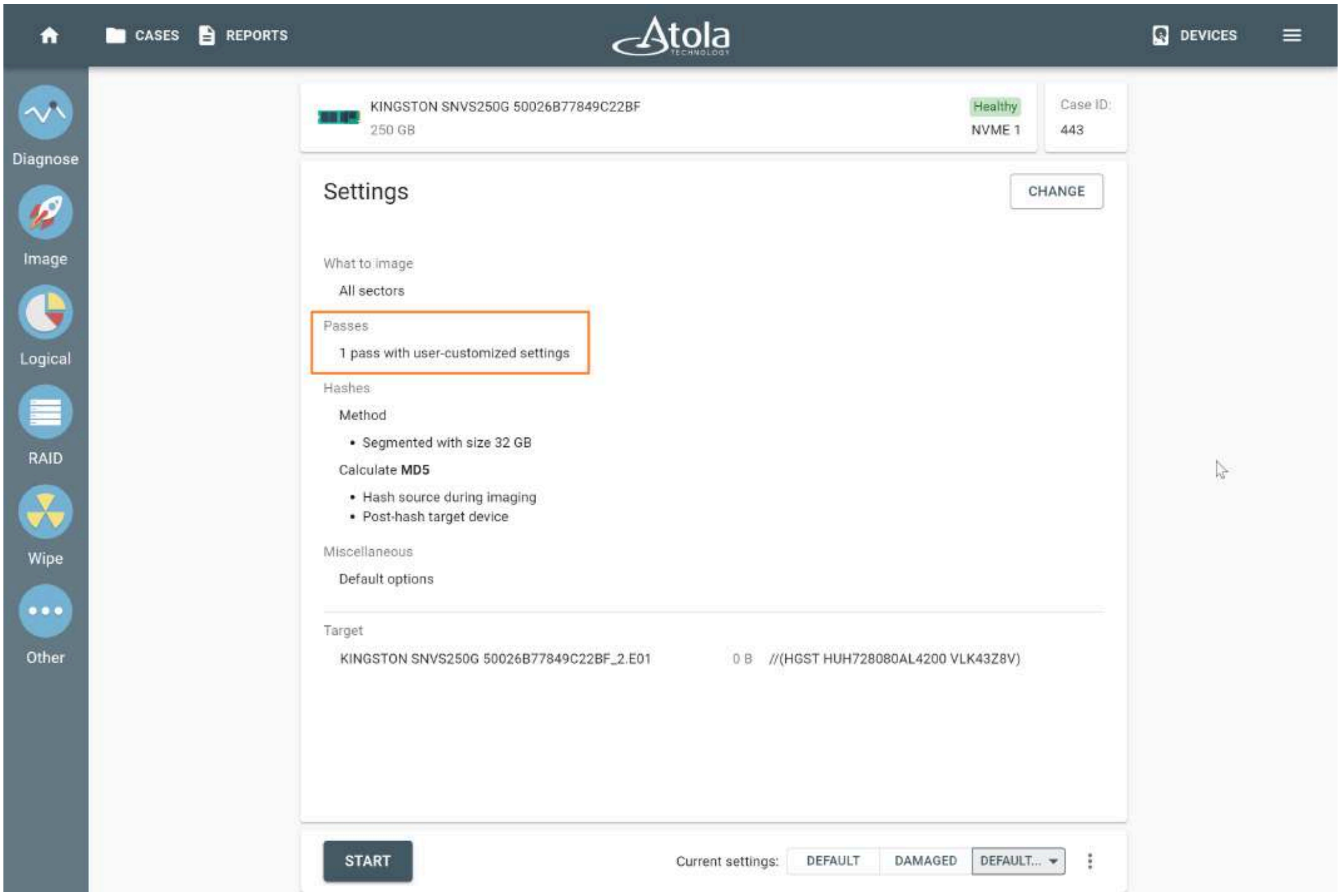
Description

Notes

Configuring the compressed E01 file.

5. Check your imaging settings and click **Start** to proceed with imaging.

When you select the **Compress E01** option in the imaging settings, the multipass imaging system or reverse imaging option cannot be applied to such an imaging session. However, other fine-tuning options remain available including advanced hashing options (pre-hash, post-hash, segmented hashing, etc.) and selective imaging.



KINGSTON SNVS250G 50026B77849C22BF
250 GB
Healthy
NVME 1
Case ID:
443

Settings

What to image
All sectors

Passes
1 pass with user-customized settings

Hashes
Method
- Segmented with size 32 GB

Calculate **MD5**
- Hash source during imaging
- Post-hash target device

Miscellaneous
Default options

Target
KINGSTON SNVS250G 50026B77849C22BF_2.E01 0 B //(HGST HUH728080AL4200 VLK43Z8V)

Current settings:

The imaging settings screen.

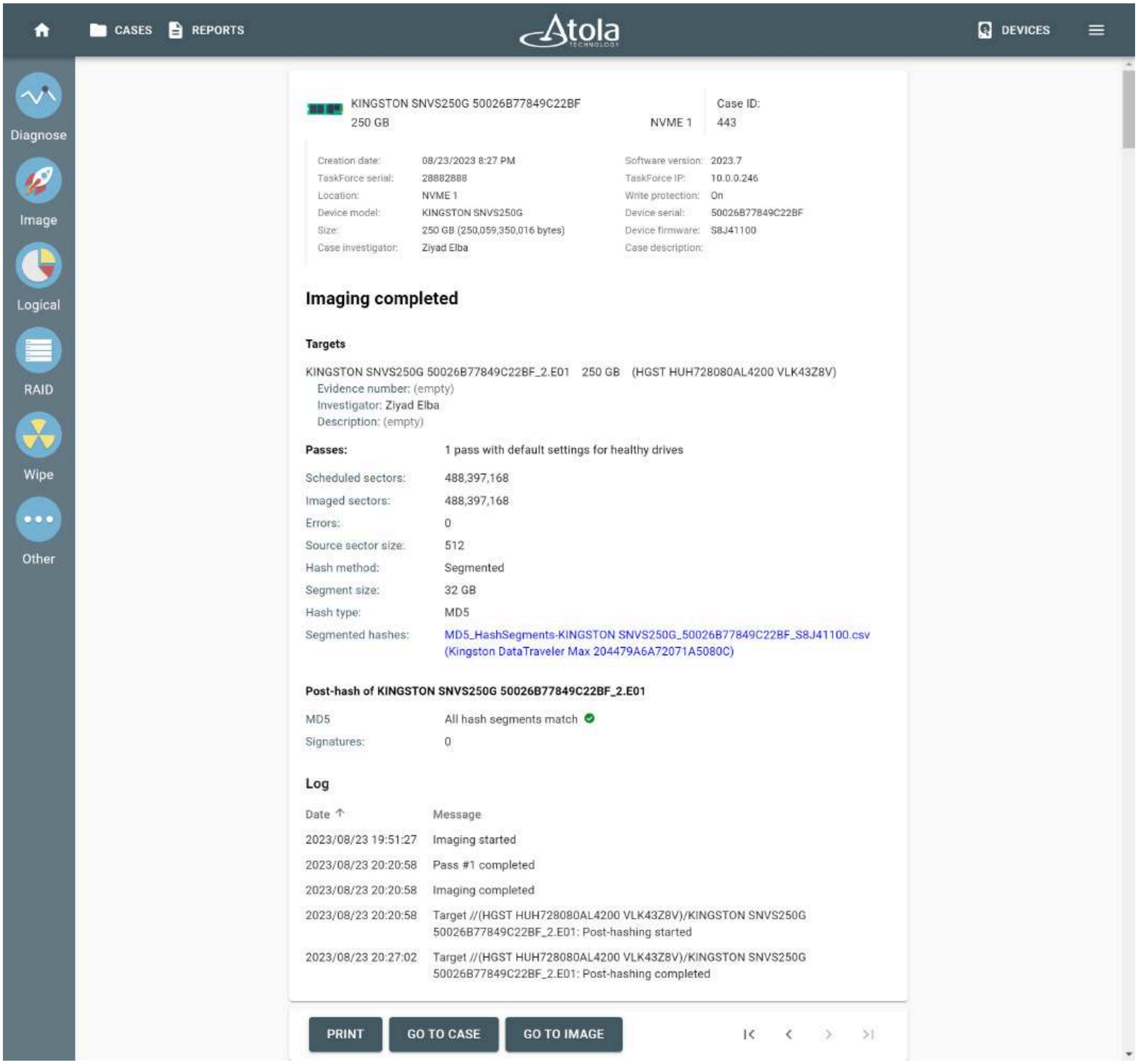
Image several devices to a Storage drive in parallel

You can run multiple imaging sessions to E01/AFF4/RAW files on a Storage drive simultaneously.

To do that, follow the steps described in the Image to a Storage drive section and then Create a compressed E01 image file for each evidence device.

Imaging completed report

The **Imaging completed** report provides all the time stamps, hash values, and hash verification result. To look up the settings of the imaging session, you can also see the **Imaging started** report in the case management system.



KINGSTON SNVS250G 50026B77849C22BF
250 GB
NVME 1
Case ID:
443

Creation date:	08/23/2023 8:27 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	NVME 1	Write protection:	On
Device model:	KINGSTON SNVS250G	Device serial:	50026B77849C22BF
Size:	250 GB (250,059,350,016 bytes)	Device firmware:	S8J41100
Case investigator:	Ziyad Elba	Case description:	

Imaging completed

Targets

KINGSTON SNVS250G 50026B77849C22BF_2.E01 250 GB (HGST HUH728080AL4200 VLK43Z8V)
Evidence number: (empty)
Investigator: Ziyad Elba
Description: (empty)

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	488,397,168
Imaged sectors:	488,397,168
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	32 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-KINGSTON SNVS250G_50026B77849C22BF_S8J41100.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

Post-hash of KINGSTON SNVS250G 50026B77849C22BF_2.E01

MD5	All hash segments match ✓
Signatures:	0

Log

```
Date ↑                 Message
2023/08/23 19:51:27    Imaging started
2023/08/23 20:20:58    Pass #1 completed
2023/08/23 20:20:58    Imaging completed
2023/08/23 20:20:58    Target //(HGST HUH728080AL4200 VLK43Z8V)/KINGSTON SNVS250G
                       50026B77849C22BF_2.E01: Post-hashing started
2023/08/23 20:27:02    Target //(HGST HUH728080AL4200 VLK43Z8V)/KINGSTON SNVS250G
                       50026B77849C22BF_2.E01: Post-hashing completed
```

The Imaging completed report.

Imaging to an AFF4 file

Atola TaskForce 2 supports performing an image acquisition of an evidence device to an AFF4 forensic file.

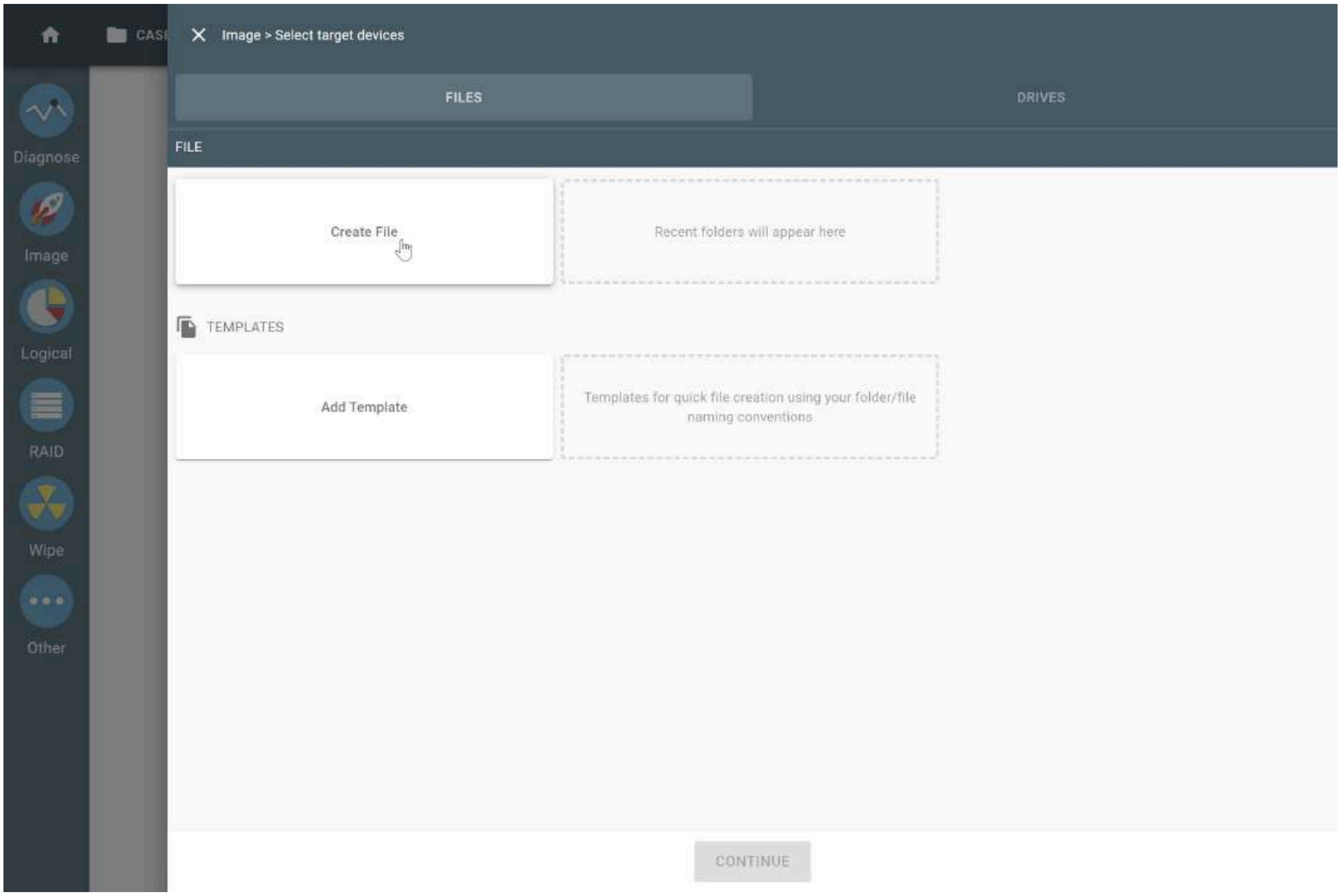
AFF4 is a highly optimized open-source forensic file format used for the storage of digital evidence and data. It offers a wide range of benefits:

- Is an open-source format: you can describe it in a court.
- Supports multipass imaging.
- Offers fast compression methods: Snappy and LZ4.
- Supports block hashes.
- Stores binary zeroes as spans similar to sparse files.
- Is vendor-neutral.

AFF4's block hashes are calculated for small segments of data on the drive and are stored in a table inside AFF4 metadata. There is a Block map hash that represents a single SHA-512 hash value for all the individual block hashes based on Merkle tree model. This is great for imaging of damaged drives to a file using TaskForce's multipass imaging algorithms.

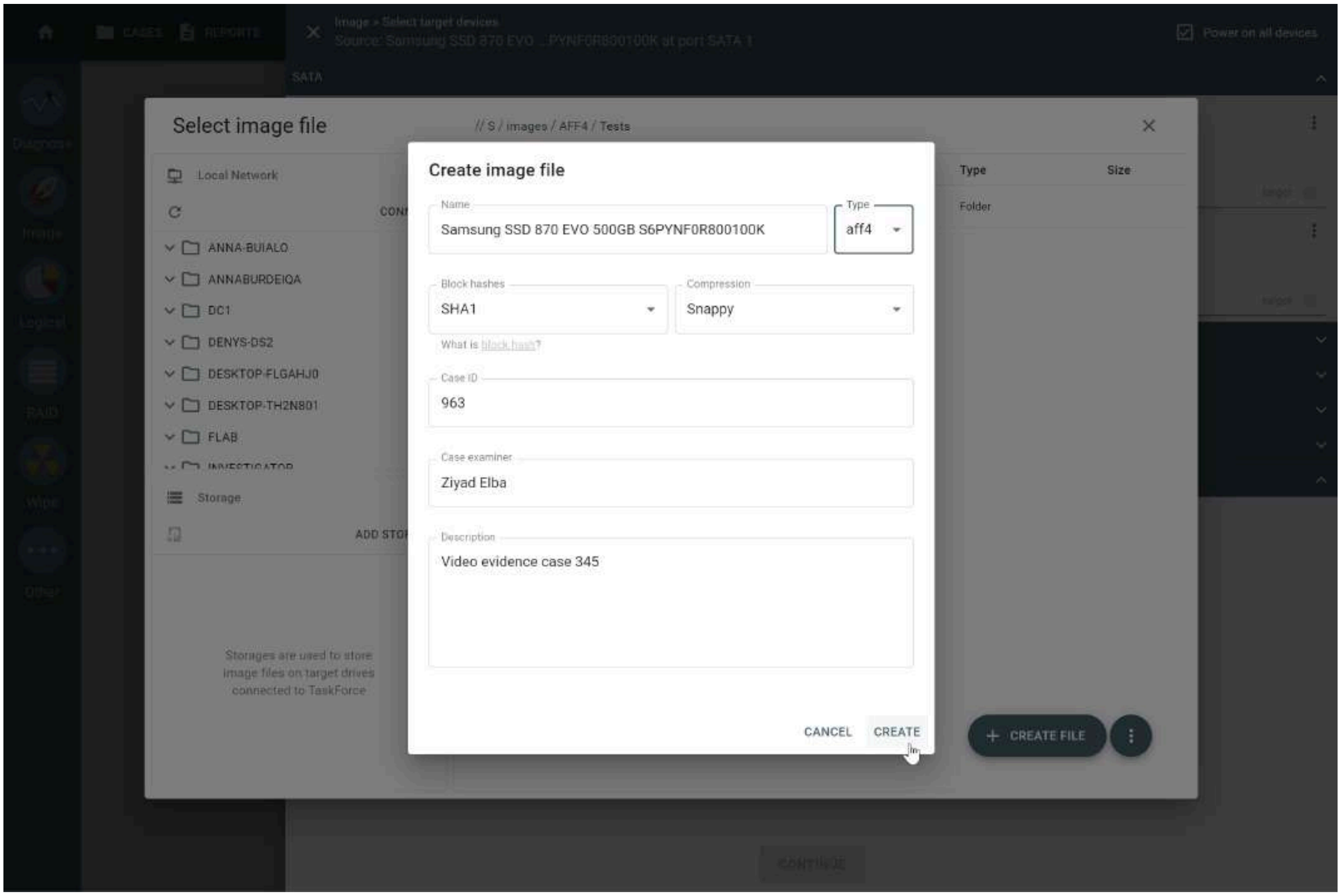
Create an AFF4 file as an imaging target

1. In the TaskForce main window, click **Image**.
2. Select a source device.
3. **Optional:** On the **Imaging sessions** page, click **Start new**.
4. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.


CASE
Image > Select target devices
FILES
DRIVES
FILE
Create File
Recent folders will appear here
TEMPLATES
Add Template
Templates for quick file creation using your folder/file naming conventions
Diagnose
Image
Logical
RAID
Wipe
Other
CONTINUE

Creating a file as an imaging target.

5. Choose a folder for your file. You can save a file:
    - on a computer or server in your local network or
    - on a storage device connected to your TaskForce.
6. After selecting a folder, click **Create file**.
7. In the **Create image file** dialog, change file **Type** to AFF4.
8. Define hashing type and compression algorithm for your target AFF4 file:
    - Block hashes: choose from MD5, SHA1, MD5 + SHA1, SHA256, or SHA512
    - Compression: choose from LZ4, Snappy, or Not compressed.
9. Enter other case details and then click **Create**.



Create image file

Name: Samsung SSD 870 EVO 500GB S6PYNF0R800100K

Type: aff4

Block hashes: SHA1

Compression: Snappy

What is block hash?

Case ID: 963

Case examiner: Ziyad Elba

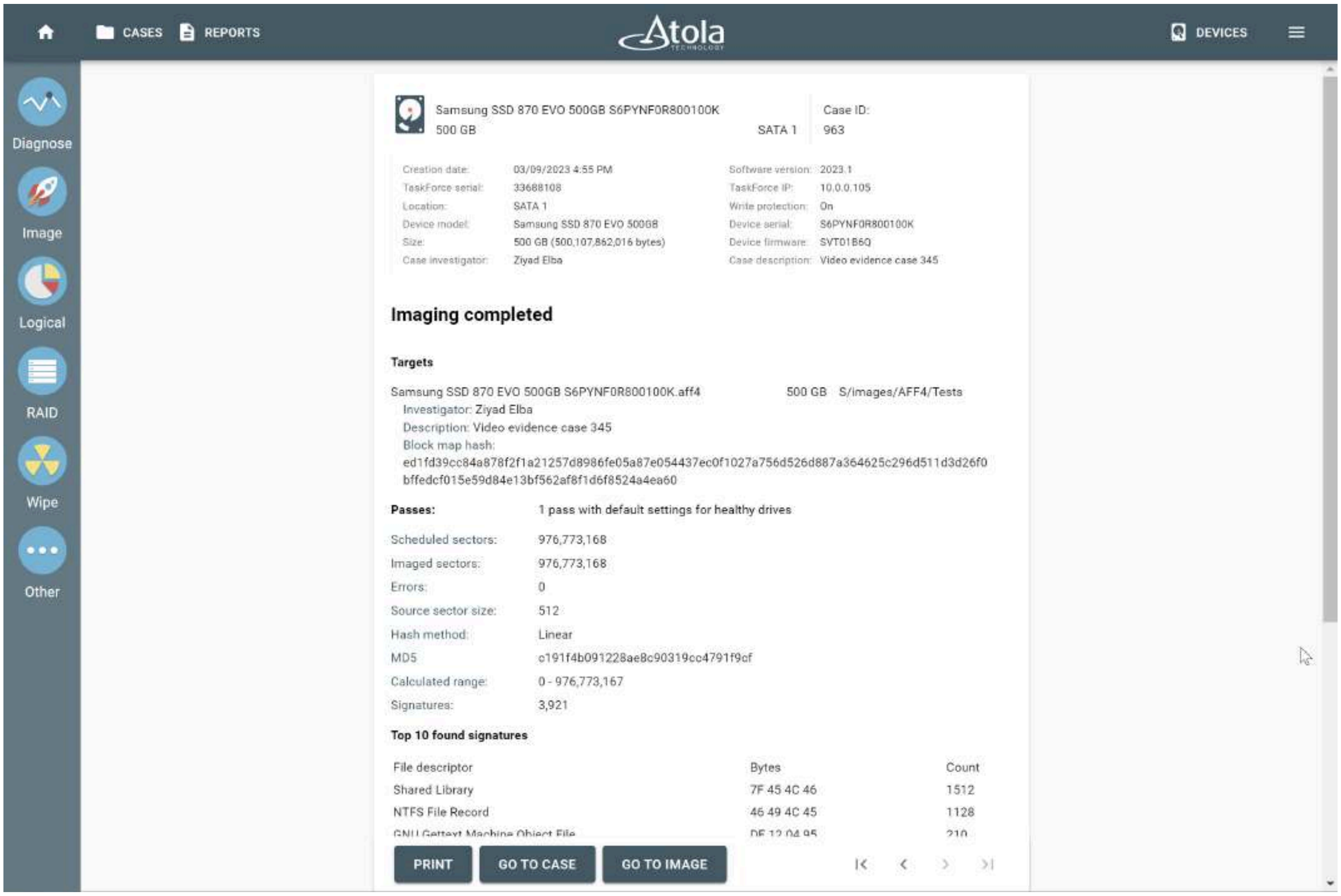
Description: Video evidence case 345

Storages are used to store image files on target drives connected to TaskForce

The settings for AFF4 target image file.

10. Click **Continue**.
11. Check imaging settings, change them if needed, and then click **Start**.

TaskForce 2 starts imaging your evidence device to an AFF4 target file. After imaging is finished, the system shows an **Imaging completed** report.



Samsung SSD 870 EVO 500GB S6PYNF0R800100K
500 GB SATA 1

Case ID:
963

Creation date:	03/09/2023 4:55 PM	Software version:	2023.1
TaskForce serial:	33688108	TaskForce IP:	10.0.0.105
Location:	SATA 1	Write protection:	On
Device model:	Samsung SSD 870 EVO 500GB	Device serial:	S6PYNF0R800100K
Size:	500 GB (500,107,862,016 bytes)	Device firmware:	SVT01B6Q
Case investigator:	Ziyad Elba	Case description:	Video evidence case 345

Imaging completed

Targets

Samsung SSD 870 EVO 500GB S6PYNF0R800100K.aff4 500 GB S/images/AFF4/Tests
Investigator: Ziyad Elba
Description: Video evidence case 345
Block map hash:
ed1fd39cc84a878f2f1a21257d8986fe05a87e054437ec0f1027a756d526d887a364625c296d511d3d26f0
bffedcf015e59d84e13bf562af8f1d6f8524a4ea60

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	976,773,168
Imaged sectors:	976,773,168
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	c191f4b091228ae8c90319cc4791f9cf
Calculated range:	0 - 976,773,167
Signatures:	3,921

Top 10 found signatures

File descriptor	Bytes	Count
Shared Library	7F 45 4C 46	1512
NTFS File Record	46 49 4C 45	1128
GNU Gettext Machine Object File	DE 12 04 95	210

The Imaging completed report with an AFF4 file as a target.

Image a remote drive using the iSCSI protocol

Some devices can't be plugged directly into the TaskForce hardware unit for imaging. These could be drives soldered into a motherboard, servers that can't be turned off, or devices you have legal access to but lack the right to seize.

To image such devices remotely with TaskForce, use the iSCSI network protocol.

To set up an iSCSI target correctly and expose a physical or logical drive via iSCSI on a network, you can utilize a Python script provided by Atola that automatically creates iSCSI targets for all drives except for a boot device.

Automatically create iSCSI targets

To expose a physical or logical drive via iSCSI on a network, you need first set up the iSCSI target correctly. To help you with that, Atola engineers created a Python script named **iscsi-targets**, which automatically creates iSCSI targets for all drives except the boot device.

Download iscsi-targets from GitHub →

Features of the 'iscsi-targets' script

- Automatically creates iSCSI targets for all drives except the boot device.
- Ensures that the iSCSI Qualified Name (IQN) of every iSCSI target includes the drive model and serial number. When you add such an iSCSI target in Atola imagers as a source drive, the imager's software automatically extracts the model and serial number from the IQN into the case details.
- Lets you specify a block device as a script argument to create an iSCSI target only for that device.

What you need to run the ‘iscsi-targets’ script

The script runs on **Linux only**. It was tested on various distributions such as Ubuntu, Fedora, CentOS, and RHEL, including DFIR boot environments like Paladin, Caine, and Tsurugi.

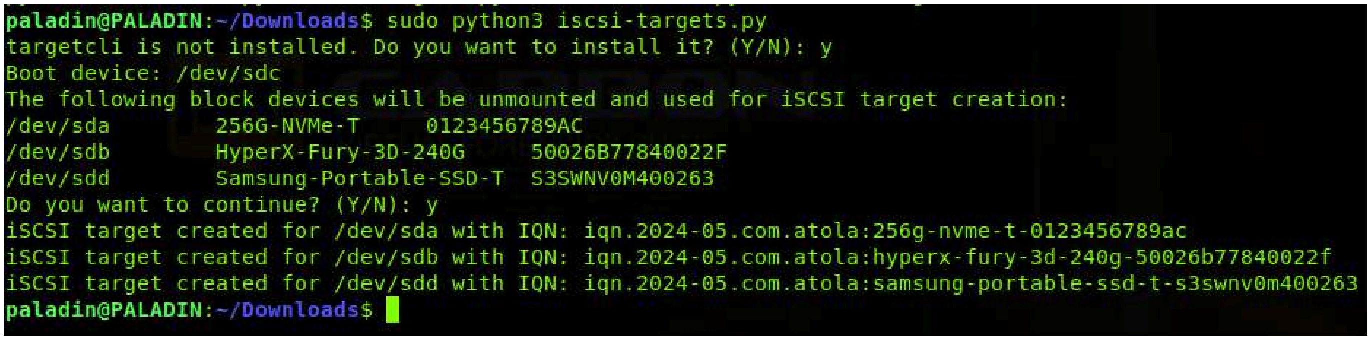
1. **Python 3.6 or higher** must be installed.
2. On the first run, the script automatically checks for and installs two required dependencies:
   - *targetcli*
   - *python3-rtslib*

How to use the ‘iscsi-targets’ script

Here are some examples of using the ‘iscsi-targets’ script.

1. Create iSCSI targets for **all drives** except the boot device:
   `sudo python3 iscsi-targets.py`
2. Create a **single iSCSI target** for the specified /dev/sdb1 partition:
   `sudo python3 iscsi-targets.py /dev/sdb1`

The example below shows the first run of iscsi-targets.py on Paladin. It has added 3 iSCSI targets for SATA and USB drives.



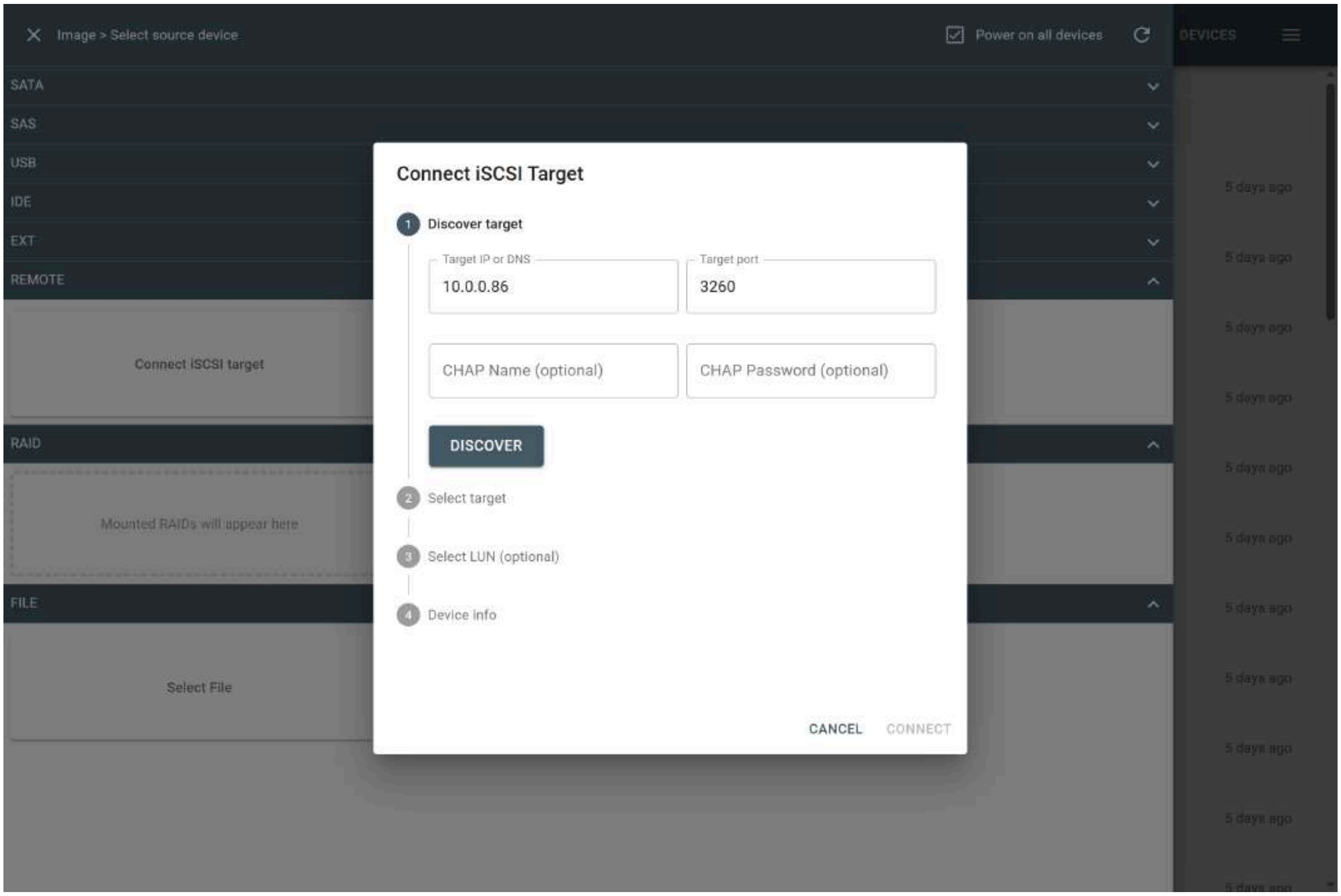
```
paladin@PALADIN:~/Downloads$ sudo python3 iscsi-targets.py
targetcli is not installed. Do you want to install it? (Y/N): y
Boot device: /dev/sdc
The following block devices will be unmounted and used for iSCSI target creation:
/dev/sda        256G-NVMe-T     0123456789AC
/dev/sdb        HyperX-Fury-3D-240G     50026B77840022F
/dev/sdd        Samsung-Portable-SSD-T  S3SWNV0M400263
Do you want to continue? (Y/N): y
iSCSI target created for /dev/sda with IQN: iqn.2024-05.com.atola:256g-nvme-t-0123456789ac
iSCSI target created for /dev/sdb with IQN: iqn.2024-05.com.atola:hyperx-fury-3d-240g-50026b77840022f
iSCSI target created for /dev/sdd with IQN: iqn.2024-05.com.atola:samsung-portable-ssd-t-s3swnv0m400263
paladin@PALADIN:~/Downloads$
```

Automated iSCSI target creation in Paladin.

Image remote drives in parallel using iSCSI

To image a remote drive in TaskForce using the iSCSI protocol, follow these steps:

1. Expose a physical or logical drive via iSCSI on a network.
2. In the TaskForce window, click **Image**.
3. Scroll down to the **Remote** section and click **Connect iSCSI target**.
4. Enter **Target IP or DNS** and **Target port**. If needed, also enter a username and password for remote authentication.
5. Click **Discover**.

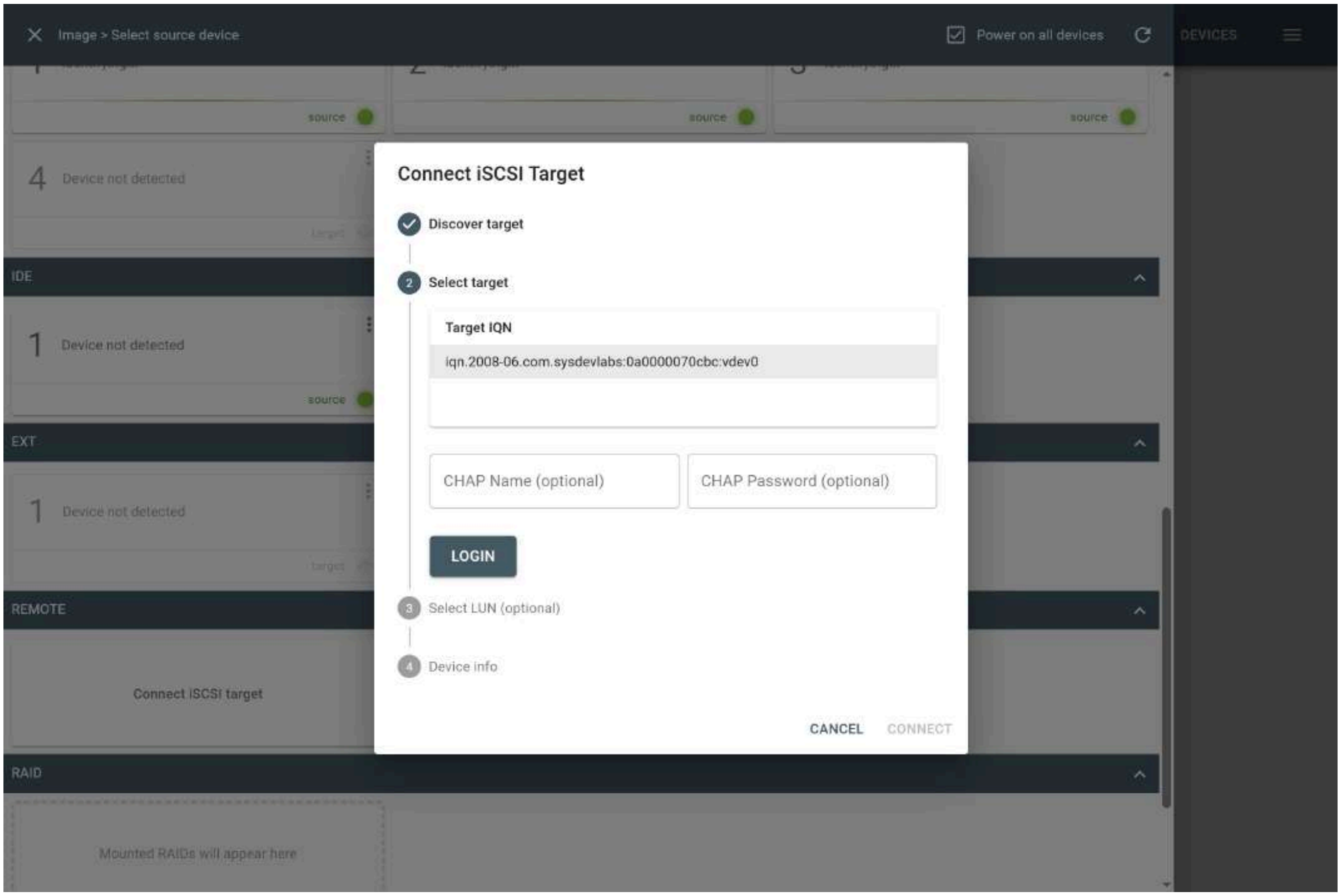


Target IP or DNS: 10.0.0.86

Target port: 3260

Discovering the iSCSI target.

6. TaskForce searches for and lists all iSCSI devices available at the IP address and port you provided. Select your iSCSI target, enter a username and password if required and click **Login**.



Connect iSCSI Target

Discover target

2 Select target

Target IQN

iqn.2008-06.com.sysdevlabs:0a0000070cbc:vdev0

CHAP Name (optional)

CHAP Password (optional)

Selecting the iSCSI target.

7. **Optional:** Select the LUN if multiple devices are exposed.
8. Enter or correct the device model and serial number.
9. Click **Connect**.
10. TaskForce opens the selected iSCSI device as a source. You can now image this device as usual.

Templates for target image files

If you image evidence devices to target files on a network server or storage drive, you can benefit from highly customizable and flexible target file templates.

Thanks to configurable variables, such as the current date, case ID, device serial number, and more, a template lets you create complex subfolder paths and file names with a couple of clicks, according to your internal naming conventions.

Additionally, you can set up other target parameters, such as file type, compression, hashing method, and autofill repeating case details, such as case number, investigator name, or location.

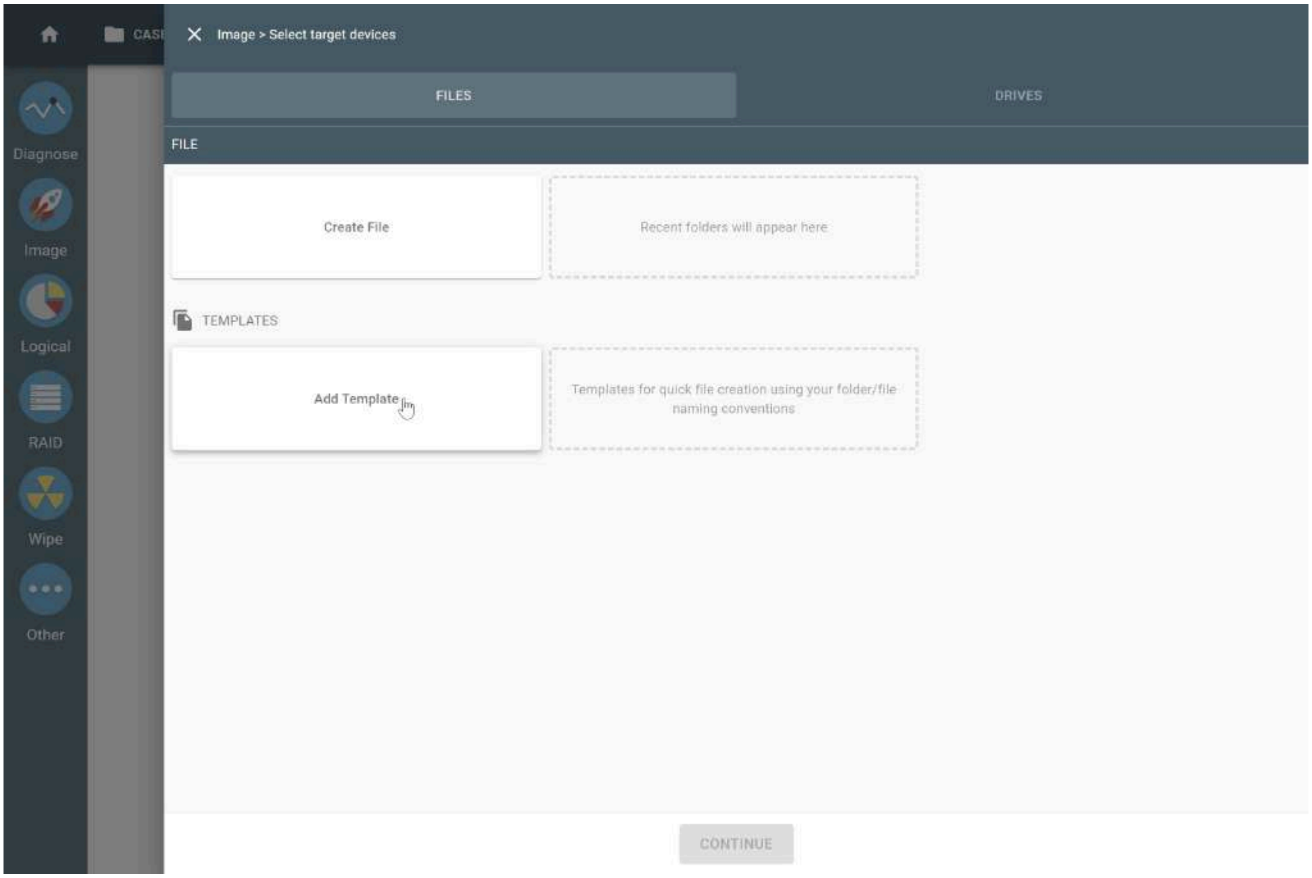
Once created, a template for a target image file can be applied with a single click.

You can use templates when performing physical or logical imaging, as well as in Express mode.

Create template

To configure a template for target image files, do the following:

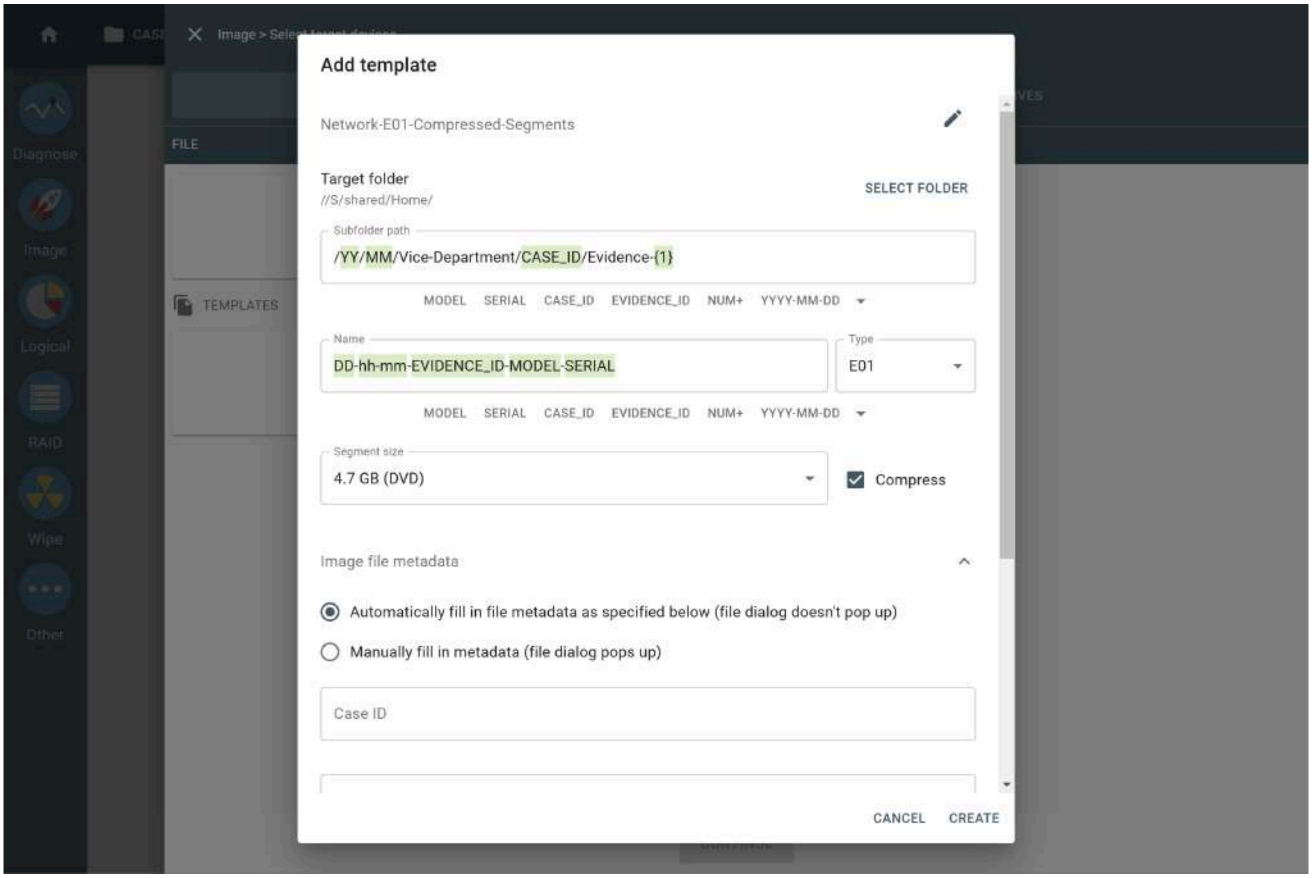
1. On the Taskbar, click **Image** and select your Source device.
2. On the **Select target devices** panel, switch to the **Files** tab and in the **Templates** section click **Add Template**.



CASE
Image > Select target devices
FILES
DRIVES
FILE
Create File
Recent folders will appear here
TEMPLATES
Add Template
Templates for quick file creation using your folder/file naming conventions
CONTINUE
Diagnose
Image
Logical
RAID
Wipe
Other

Adding a template from the 'Select target device' panel.

3. The **Add template** dialog opens.



Add template

Network-E01-Compressed-Segments

Target folder
//S/shared/Home/
SELECT FOLDER

Subfolder path: /YY/MM/Vice-Department/CASE_ID/Evidence-{1}

MODEL SERIAL CASE_ID EVIDENCE_ID NUM+ YYYY-MM-DD

Name: DD-hh-mm-EVIDENCE_ID-MODEL-SERIAL
Type: E01

MODEL SERIAL CASE_ID EVIDENCE_ID NUM+ YYYY-MM-DD

Segment size: 4.7 GB (DVD)
☑ Compress

Image file metadata

● Automatically fill in file metadata as specified below (file dialog doesn't pop up)

○ Manually fill in metadata (file dialog pops up)

Case ID

CANCEL CREATE

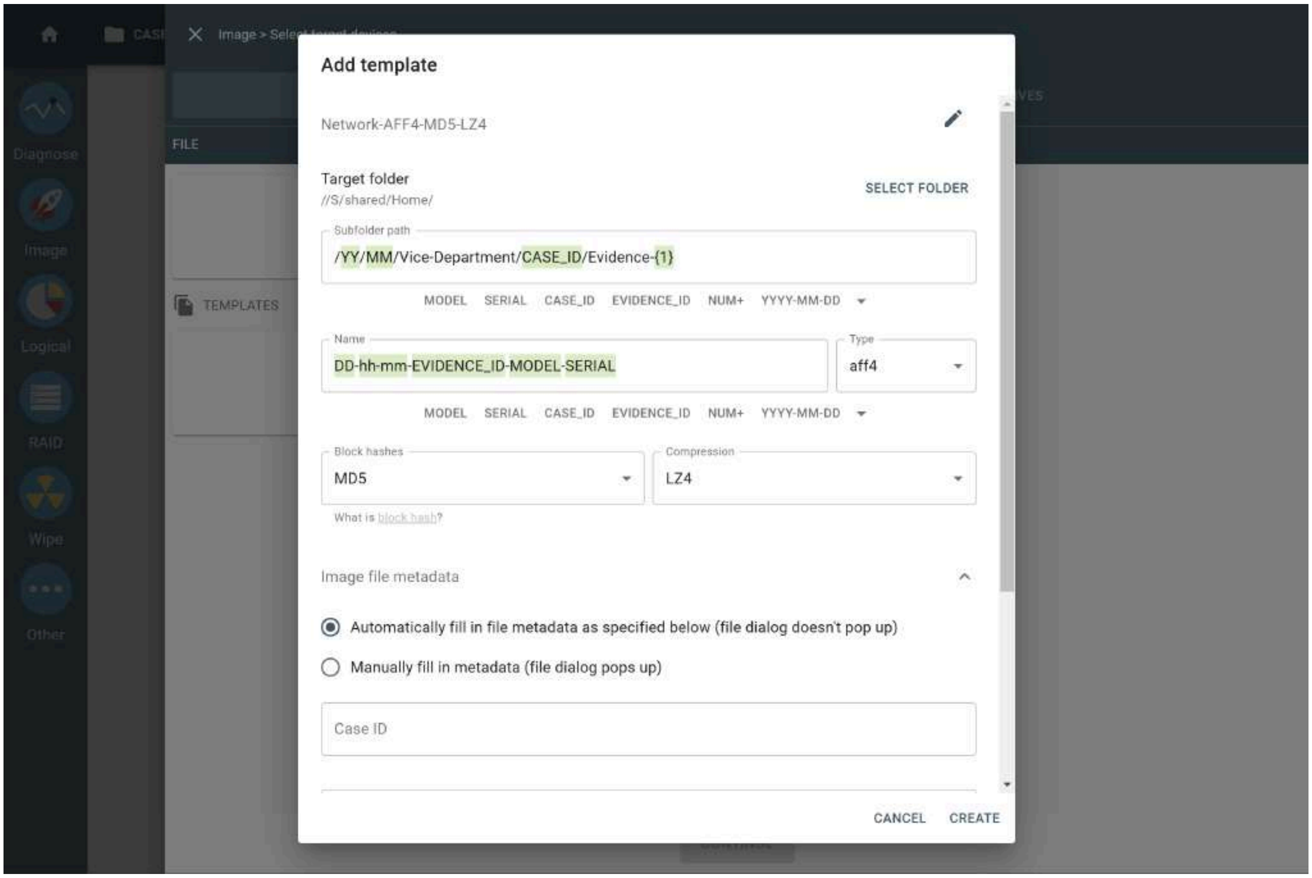
The 'Add template' dialog.

4. To edit the template's name, click the **Pencil** icon next to it.
5. Specify a **Target folder** by clicking **Select folder** and choosing the desired location.
6. Set up a **Subfolder path** and **Name** template for your target files using constants (such as department name) and available variables:
    a. Year: YY (two-digit format) or YYYY (four-digit format).
    b. Month: MM (two-digit format).
    c. Day: DD (two-digit format).
    d. Current time: hh-mm (24-hour format).
    e. Case ID: CASE_ID (as specified in the TaskForce case system).
    f. Evidence ID: EVIDENCE_ID.
    g. Drive model: MODEL (acquired automatically by TaskForce during identification).
    h. Drive serial number: SERIAL (acquired automatically by TaskForce during identification).
    i. Ordinal number variable: {NUM+} (increments from the number you specify in curly brackets if the file or folder with the same name already exists).

   Variables are highlighted with pale green for better visibility.

   To create **nested folders** in the specified Target folder, use the forward slash symbol (/) in the **Subfolder path** field.

7. Select the target file **Type**: E01, AFF4, IMG, DD, or RAW.



Add template

Network-AFF4-MD5-LZ4

Target folder
//S/shared/Home/

SELECT FOLDER

Subfolder path: /YY/MM/Vice-Department/CASE_ID/Evidence-{1}

MODEL SERIAL CASE_ID EVIDENCE_ID NUM+ YYYY-MM-DD

Name: DD-hh-mm-EVIDENCE_ID-MODEL-SERIAL

Type: aff4

MODEL SERIAL CASE_ID EVIDENCE_ID NUM+ YYYY-MM-DD

Block hashes: MD5

Compression: LZ4

What is block hash?

Image file metadata

● Automatically fill in file metadata as specified below (file dialog doesn't pop up)

○ Manually fill in metadata (file dialog pops up)

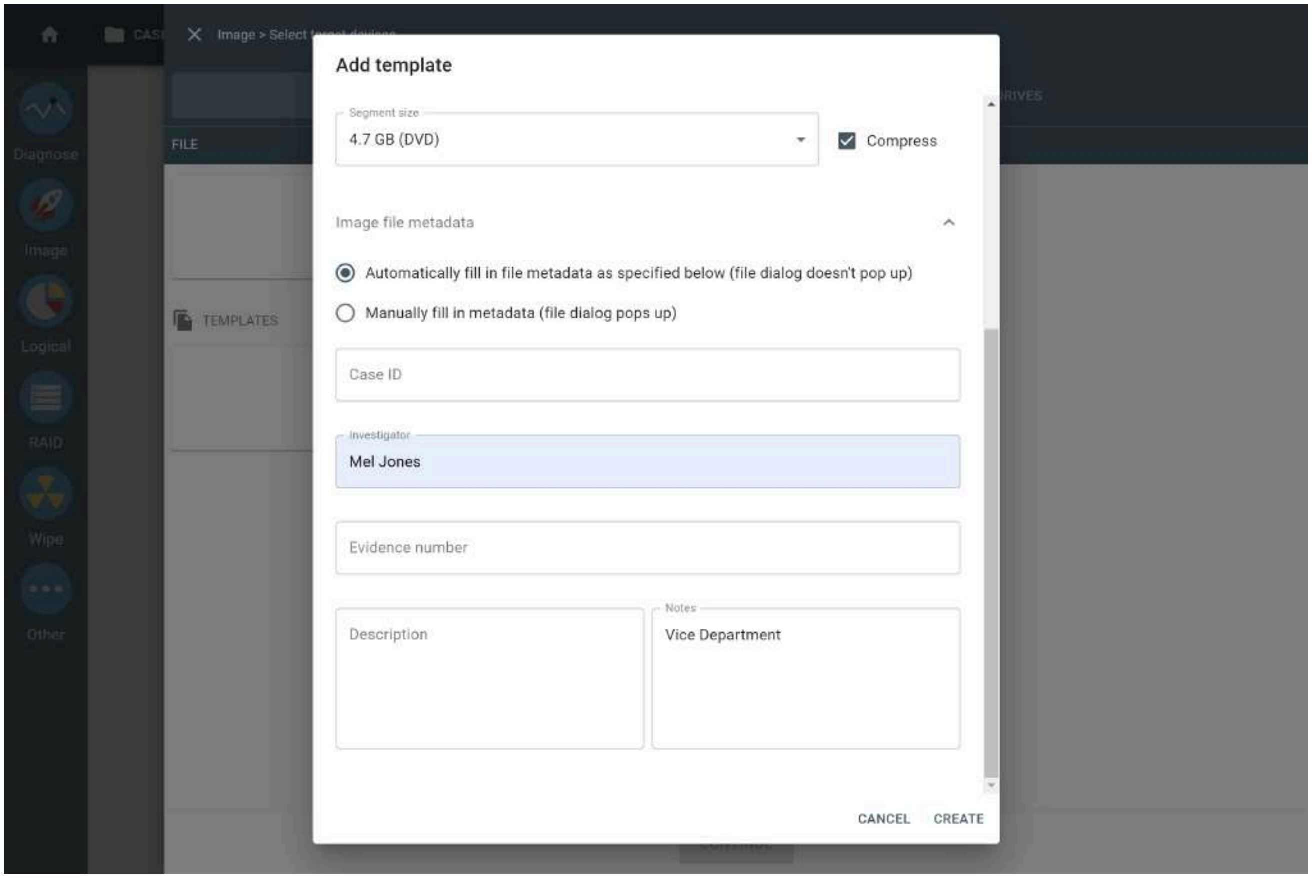
Case ID

CANCEL CREATE

Selecting target file type for a template.

8. **Optional:** Configure additional parameters of a target file:
   - For **E01** files: **Segment size** and **Compression**.
   - For **AFF4** files: method for **Block hashes** (MD5, SHA1, MD5 + SHA1, SHA256, SHA512) and **Compression** algorithm (LZ4 or Snappy).
9. Choose how to fill in file metadata: automatically (default) or manually.

   If you choose **Automatically**, specify the values for Case ID, Investigator’s name, Evidence number, Description, or Notes.


Add template

Segment size: 4.7 GB (DVD)

☑ Compress

Image file metadata

● Automatically fill in file metadata as specified below (file dialog doesn't pop up)

○ Manually fill in metadata (file dialog pops up)

Case ID

Investigator: Mel Jones

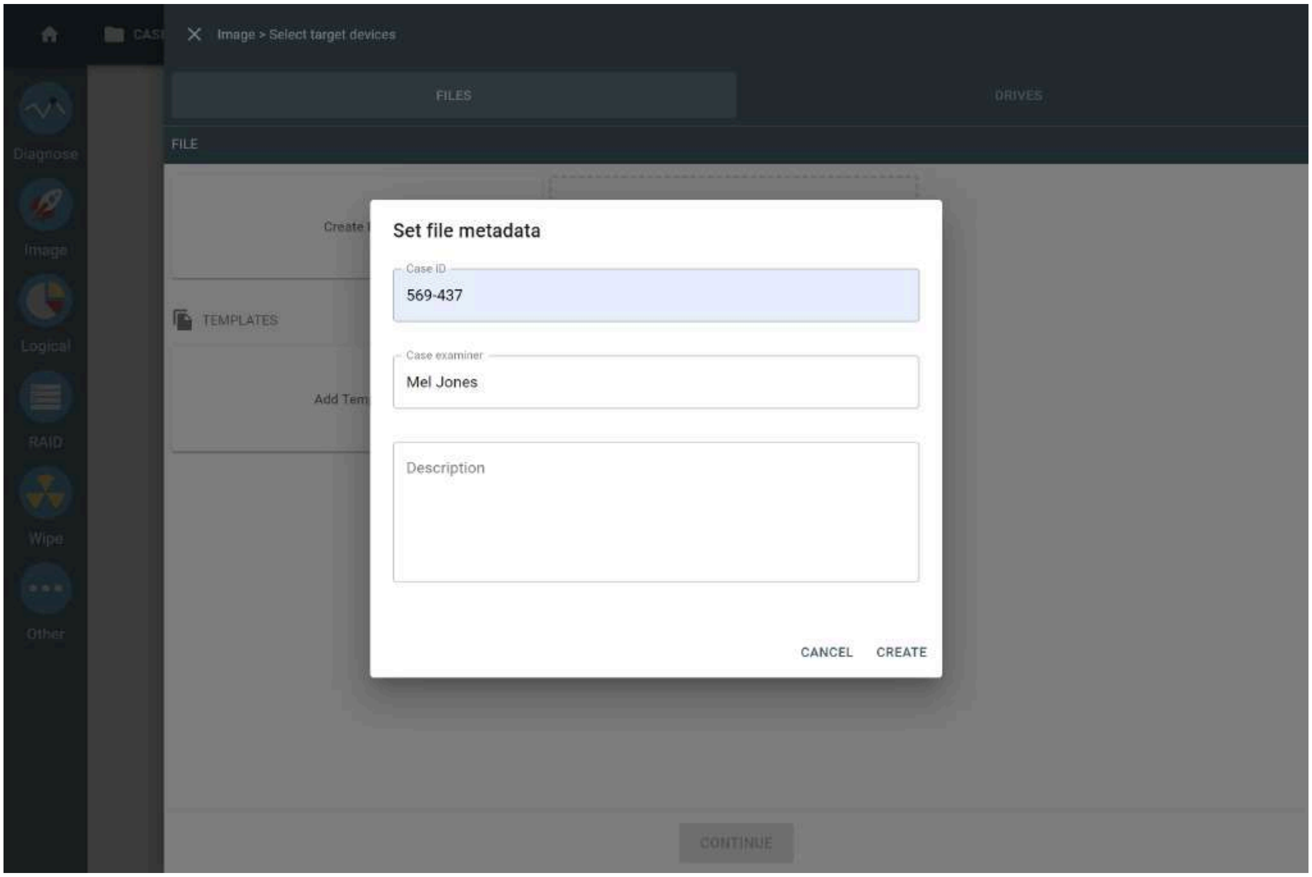
Evidence number

Description

Notes: Vice Department

Option to fill in file metadata automatically.

If you choose **Manually**, TaskForce will ask you to enter file metadata whenever you create a target file using the template.



Set file metadata

Case ID: 569-437

Case examiner: Mel Jones

Description

CANCEL CREATE

The 'Set file metadata' dialog.

10. When all the parameters of the template are set, click **Create**.

Use template

To create a target image file using an existing template, after selecting a Source device, simply click your template on the **Select target devices** panel.

After that, TaskForce creates the required subfolder(s) and adds a file with the specified parameters as an imaging target.

The target file appears on the **Files** tab of the **Select target devices** panel.

Then you can proceed to the Imaging settings screen by clicking **Continue**.

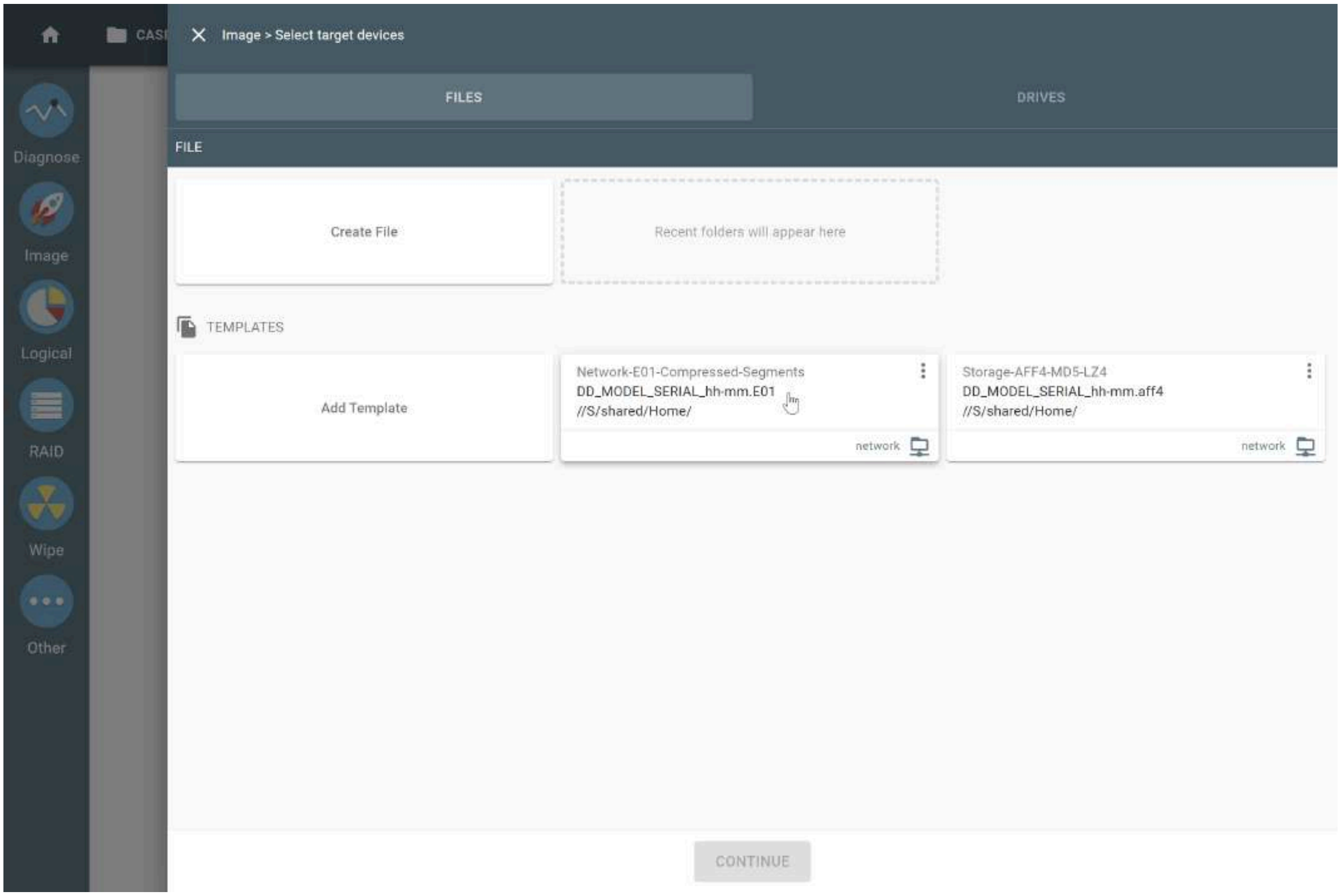


Image > Select target devices

Create File

Recent folders will appear here

TEMPLATES

Add Template

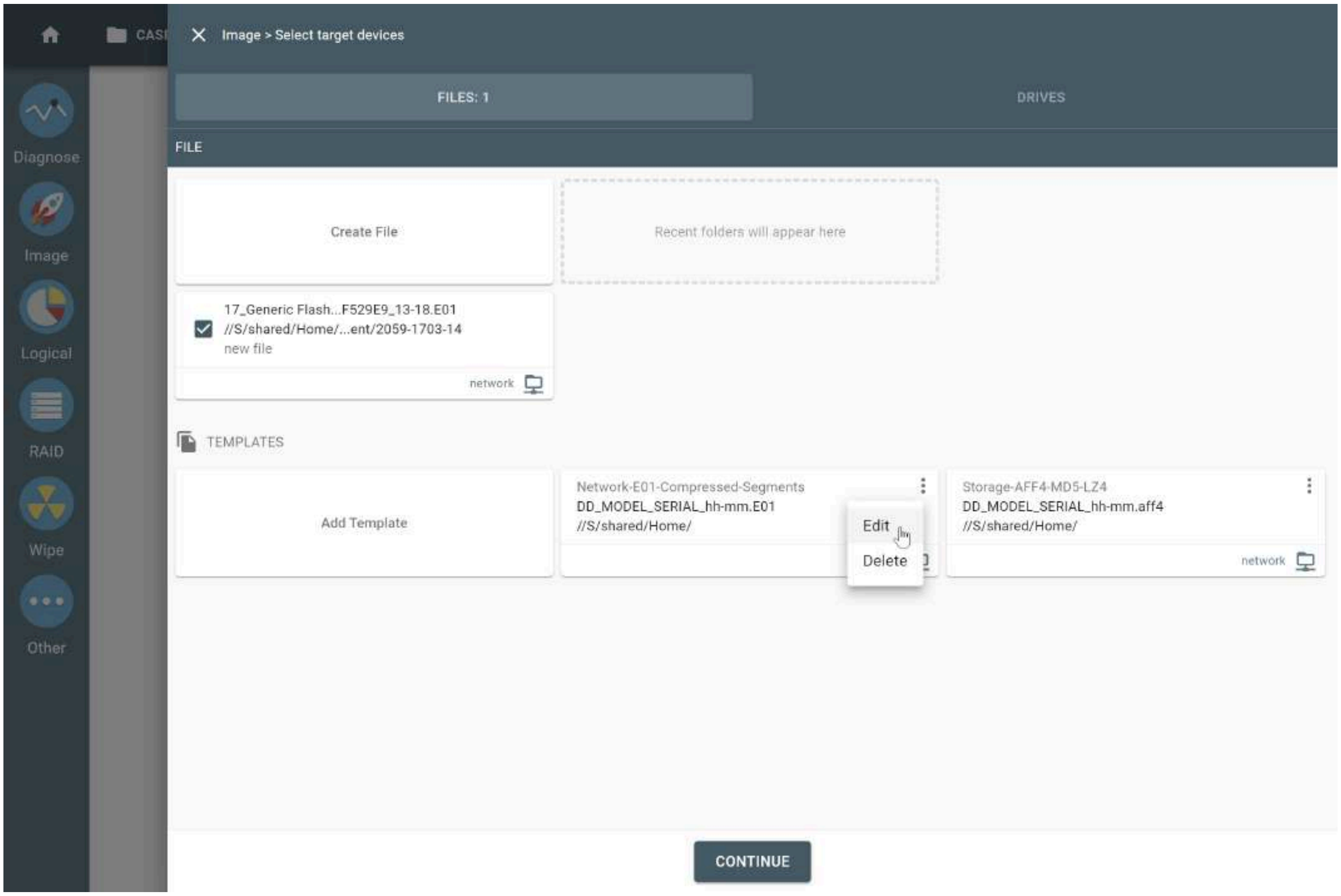
Network-E01-Compressed-Segments
DD_MODEL_SERIAL_hh-mm.E01
//S/shared/Home/
network

Storage-AFF4-MD5-LZ4
DD_MODEL_SERIAL_hh-mm.aff4
//S/shared/Home/
network

A template for target image files on the 'Select target device' panel.

Edit or delete template

To edit or delete a template for target image files, use the **three-dots icon** next to the template's name on the **Select target devices** panel.


CASE
Image > Select target devices
FILES: 1
DRIVES
FILE
Create File
Recent folders will appear here
17_Generic Flash...F529E9_13-18.E01
//S/shared/Home/...ent/2059-1703-14
new file
network
TEMPLATES
Add Template
Network-E01-Compressed-Segments
DD_MODEL_SERIAL_hh-mm.E01
//S/shared/Home/
Edit
Delete
Storage-AFF4-MD5-LZ4
DD_MODEL_SERIAL_hh-mm.aff4
//S/shared/Home/
network
CONTINUE
Diagnose
Image
Logical
RAID
Wipe
Other

Editing or deleting a template for target image files.

Accessing password-protected servers

Accessing password-protected servers allows saving image files on such servers, imaging or calculating hash of the files located there, etc.

To create an image file on a password-protected server:

1. In the TaskForce main window, click **Image**.
2. Select a source device.
3. **Optional:** On the **Imaging sessions** page, click **Start new**.
4. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.
5. In the **Select image file** window, choose the server from the list. If the server does not appear in the list, click **Refresh** icon to search for all available directories. If the server still does not appear in the list, click **Connect**.

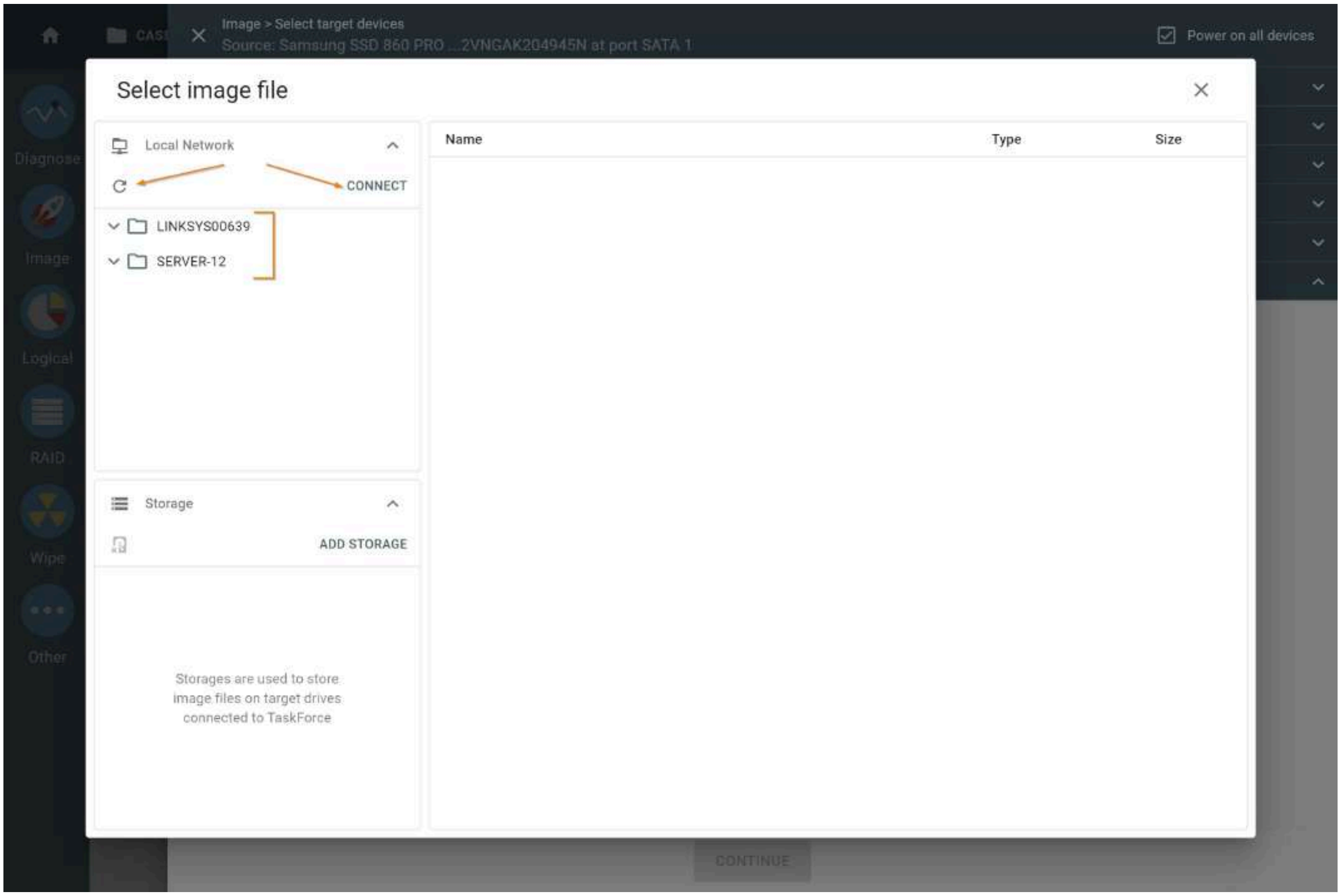


Image > Select target devices
Source: Samsung SSD 860 PRO ...2VNGAK204945N at port SATA 1
Power on all devices
Select image file
Local Network
CONNECT
LINKSYS00639
SERVER-12
Storage
ADD STORAGE
Storages are used to store image files on target drives connected to TaskForce
Name
Type
Size
Diagnose
Image
Logical
RAID
Wipe
Other
CONTINUE

Selecting a server from the list.

6. The **Connect to server** dialog opens. Enter the name of the server and fill out login details, including domain or workgroup, and then click **Connect**. To learn these details, contact your network administrator.

TaskForce supports NTLM protocol, which is enabled by default in Active Directory and Windows.

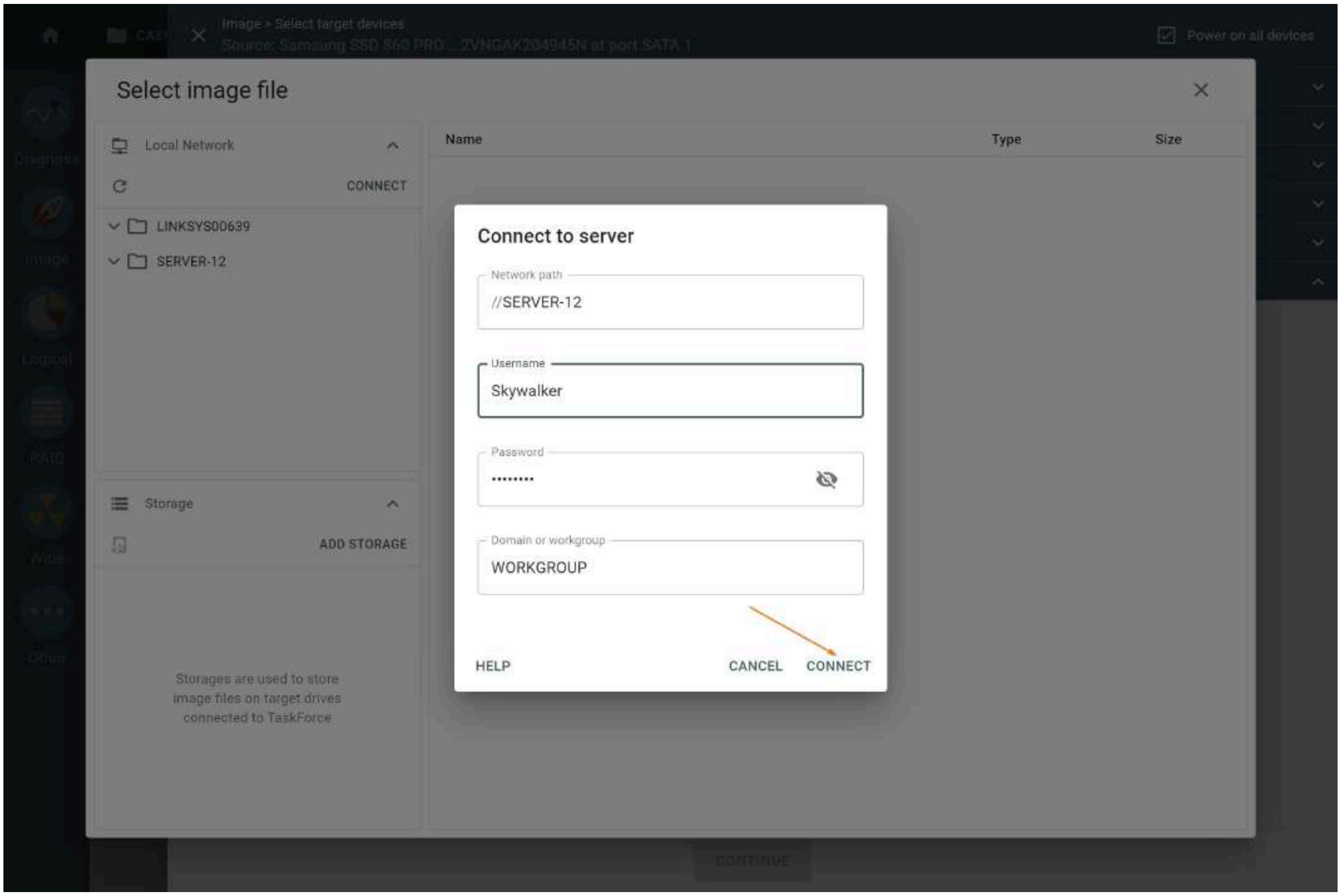


Image > Select target devices
Source: Samsung SSD 860 PRO ...2VNGAK204945N at port SATA 1
Power on all devices
Select image file
Local Network
CONNECT
LINKSYS00639
SERVER-12
Storage
ADD STORAGE
Storages are used to store image files on target drives connected to TaskForce
Name
Type
Size
HELP
CANCEL
CONNECT
CONTINUE

Connect to server

Network path: //SERVER-12

Username: Skywalker

Password: ••••••••

Domain or workgroup: WORKGROUP

Entering server and login details.

7. Go to the folder on the server where you need to store your image and click the **Plus** icon in the right bottom corner of the window.

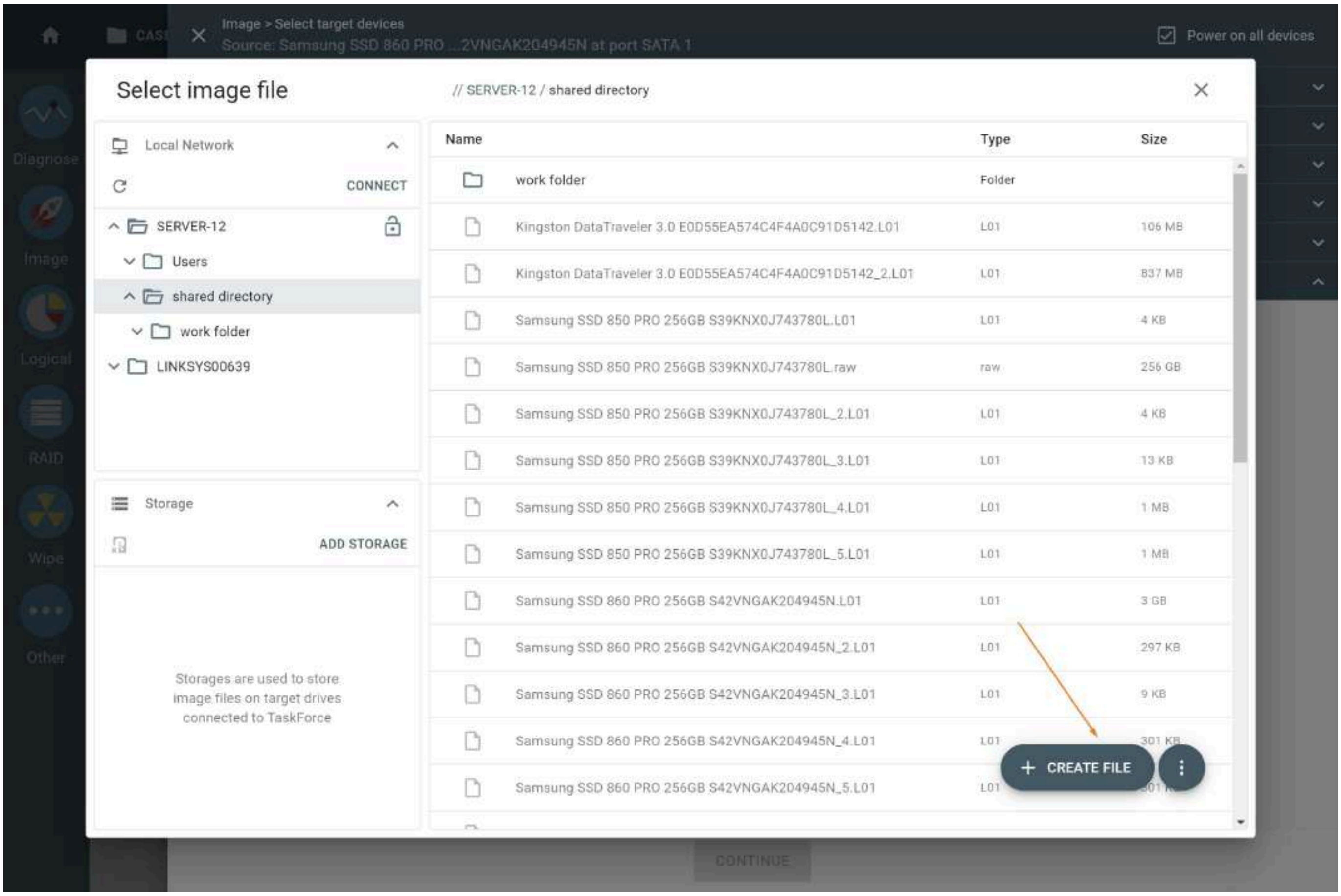


Image > Select target devices
Source: Samsung SSD 860 PRO ...2VNGAK204945N at port SATA 1
Power on all devices
Diagnose
Image
Logical
RAID
Wipe
Other
Select image file
// SERVER-12 / shared directory
Local Network
CONNECT
SERVER-12
Users
shared directory
work folder
LINKSYS00639
Storage
ADD STORAGE
Storages are used to store image files on target drives connected to TaskForce
CREATE FILE
CONTINUE

Name	Type	Size
work folder	Folder	
Kingston DataTraveler 3.0 E0D55EA574C4F4A0C91D5142.L01	L01	106 MB
Kingston DataTraveler 3.0 E0D55EA574C4F4A0C91D5142_2.L01	L01	837 MB
Samsung SSD 850 PRO 256GB S39KNX0J743780L.L01	L01	4 KB
Samsung SSD 850 PRO 256GB S39KNX0J743780L.raw	raw	256 GB
Samsung SSD 850 PRO 256GB S39KNX0J743780L_2.L01	L01	4 KB
Samsung SSD 850 PRO 256GB S39KNX0J743780L_3.L01	L01	13 KB
Samsung SSD 850 PRO 256GB S39KNX0J743780L_4.L01	L01	1 MB
Samsung SSD 850 PRO 256GB S39KNX0J743780L_5.L01	L01	1 MB
Samsung SSD 860 PRO 256GB S42VNGAK204945N.L01	L01	3 GB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_2.L01	L01	297 KB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_3.L01	L01	9 KB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_4.L01	L01	301 KB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_5.L01	L01	301 K

Creating a new file in the directory.

8. Enter the name of the new image file and select the format. Click **Create**.

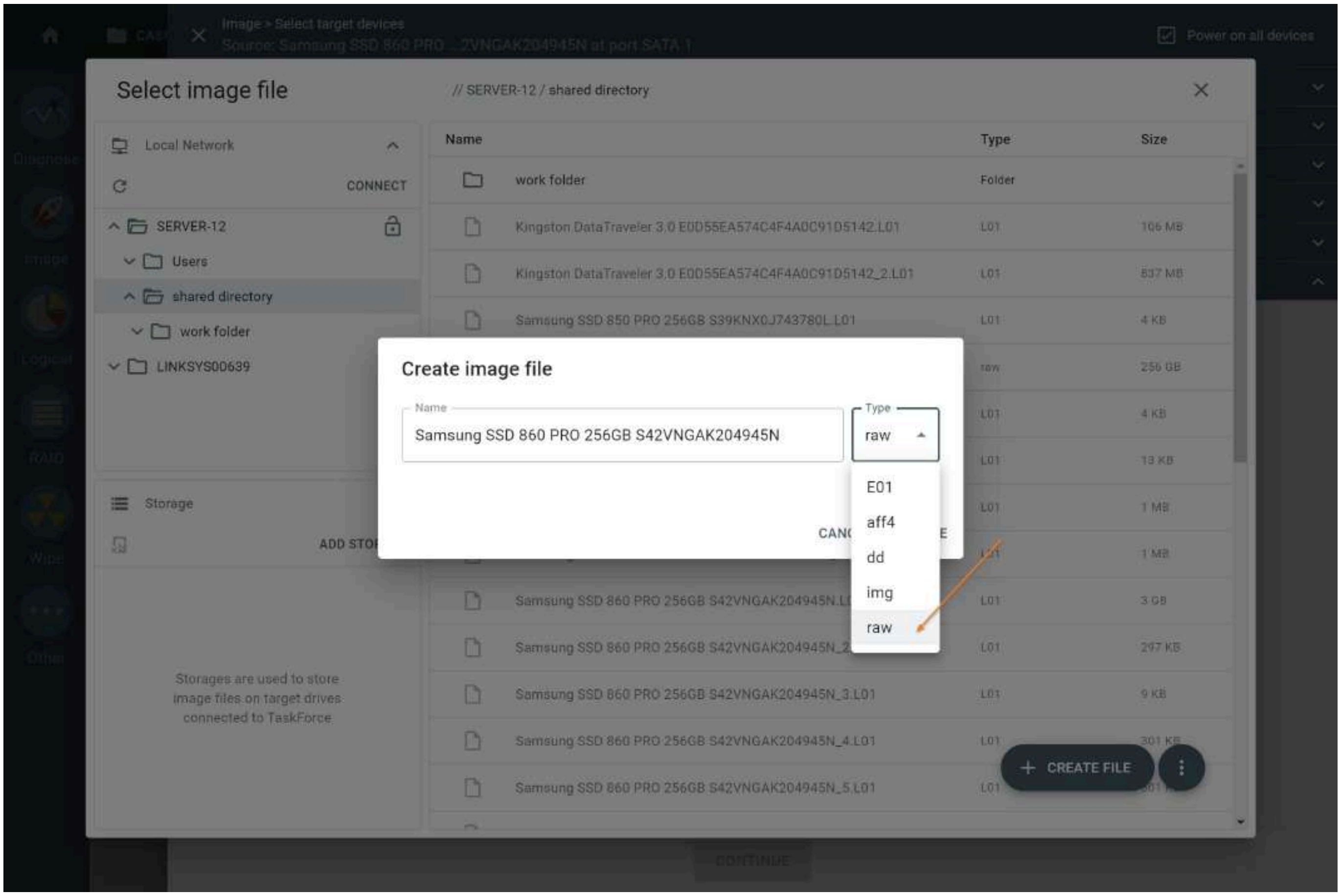


Image > Select target devices
Source: Samsung SSD 860 PRO ...2VNGAK204945N at port SATA 1
Power on all devices
Select image file
// SERVER-12 / shared directory
Local Network
CONNECT
SERVER-12
Users
shared directory
work folder
LINKSYS00639
Storage
ADD STOR
Storages are used to store image files on target drives connected to TaskForce
CANC
E
CREATE FILE
CONTINUE

Name	Type	Size
work folder	Folder	
Kingston DataTraveler 3.0 E0D55EA574C4F4A0C91D5142.L01	L01	106 MB
Kingston DataTraveler 3.0 E0D55EA574C4F4A0C91D5142_2.L01	L01	837 MB
Samsung SSD 850 PRO 256GB S39KNX0J743780L.L01	L01	4 KB
	raw	256 GB
	L01	4 KB
	L01	13 KB
	L01	1 MB
	L01	1 MB
Samsung SSD 860 PRO 256GB S42VNGAK204945N.L	L01	3 GB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_2	L01	297 KB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_3.L01	L01	9 KB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_4.L01	L01	301 KB
Samsung SSD 860 PRO 256GB S42VNGAK204945N_5.L01	L01	301 KB

Create image file

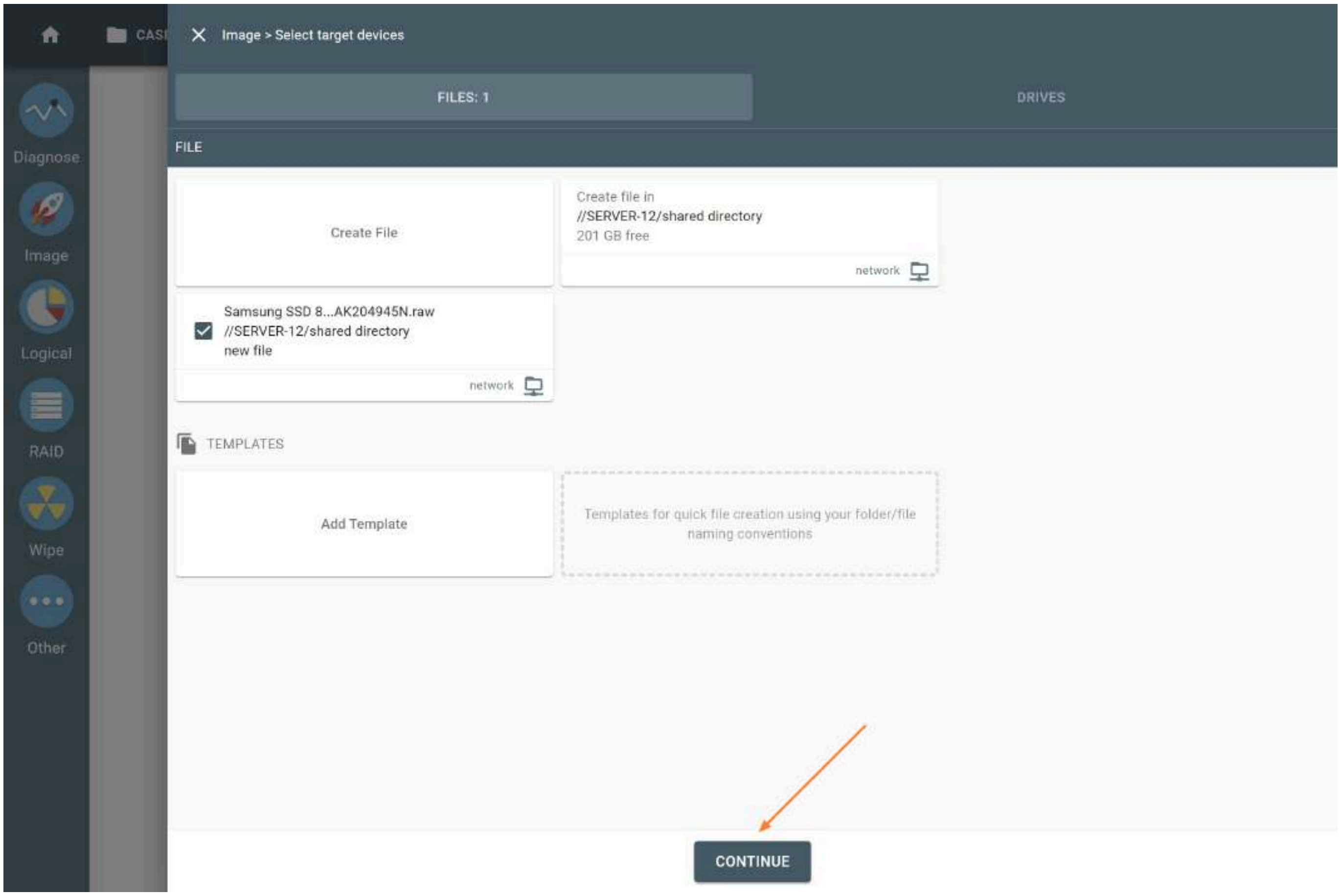
Name: Samsung SSD 860 PRO 256GB S42VNGAK204945N

Type: raw

- E01
- aff4
- dd
- img
- raw

Entering the name and selecting the format of the new image file.

9. On the **Select target devices** panel, click **Continue**.



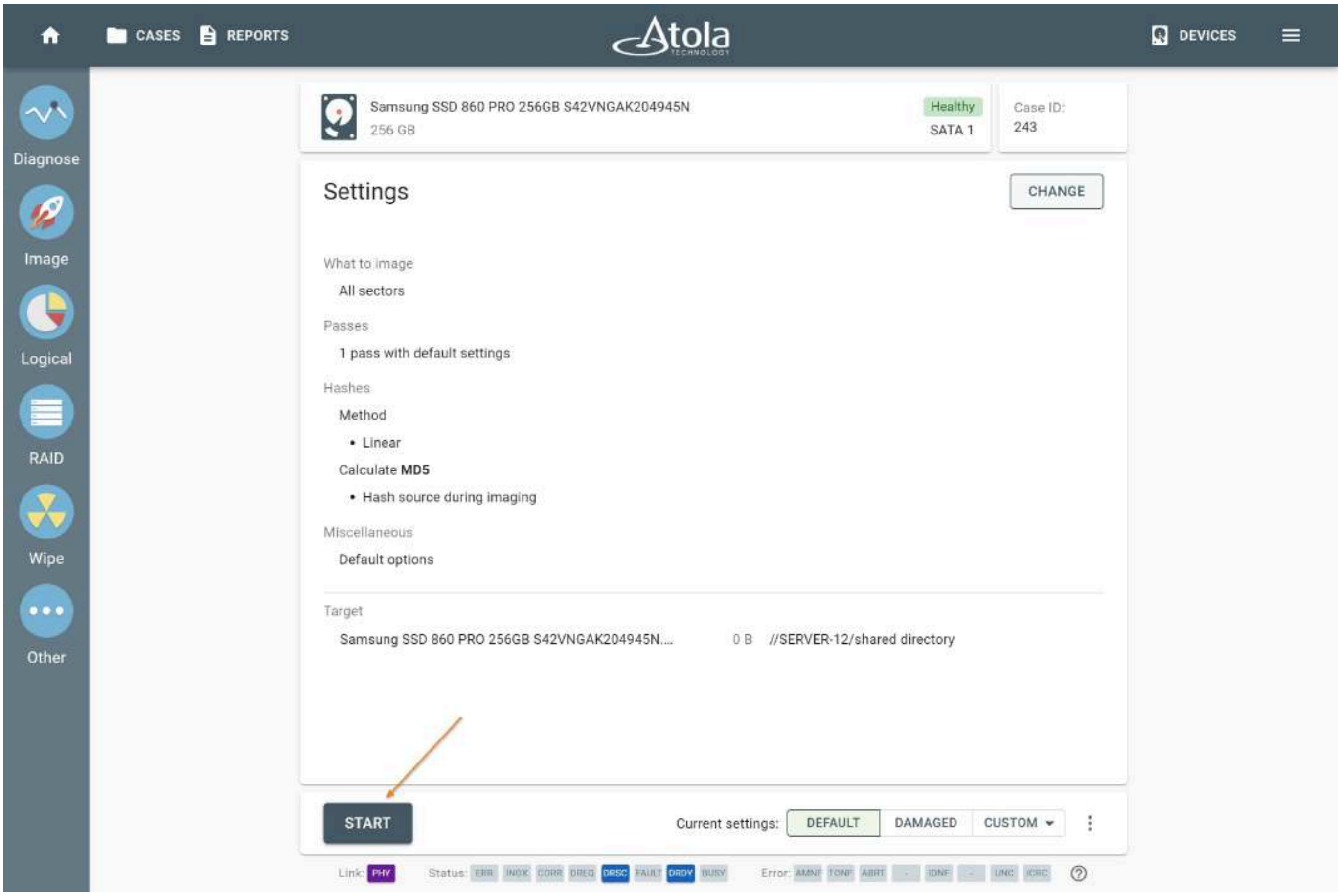
Create file in
//SERVER-12/shared directory
201 GB free

☑ Samsung SSD 8...AK204945N.raw
//SERVER-12/shared directory
new file

Templates for quick file creation using your folder/file naming conventions

The Continue button on the Select target devices panel.

10. Check your imaging settings and click **Start** to proceed with imaging.



Samsung SSD 860 PRO 256GB S42VNGAK204945N
256 GB
Healthy
SATA 1
Case ID:
243

Settings

What to image
All sectors

Passes
1 pass with default settings

Hashes
Method
- Linear

Calculate **MD5**
- Hash source during imaging

Miscellaneous
Default options

Target
Samsung SSD 860 PRO 256GB S42VNGAK204945N... 0 B //SERVER-12/shared directory

Current settings: DEFAULT

The Start button on the Imaging settings page.

Imaging to a file on an encrypted drive with TaskForce 2

With Atola TaskForce 2 it is possible to image into files on an encrypted target drive using VeraCrypt for data encryption. Multiple target drives can be encrypted for the same or different sessions.

Create encrypted storage

To image into files on an encrypted target drive, connect the source drive to a port in the *Source* mode and take these steps:

1. In the TaskForce main window, click **Image**.
2. Select a source device.
3. **Optional:** On the **Imaging sessions** page, click **Start new**.
4. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.
5. In the **Select image file** window, click **Add storage**.

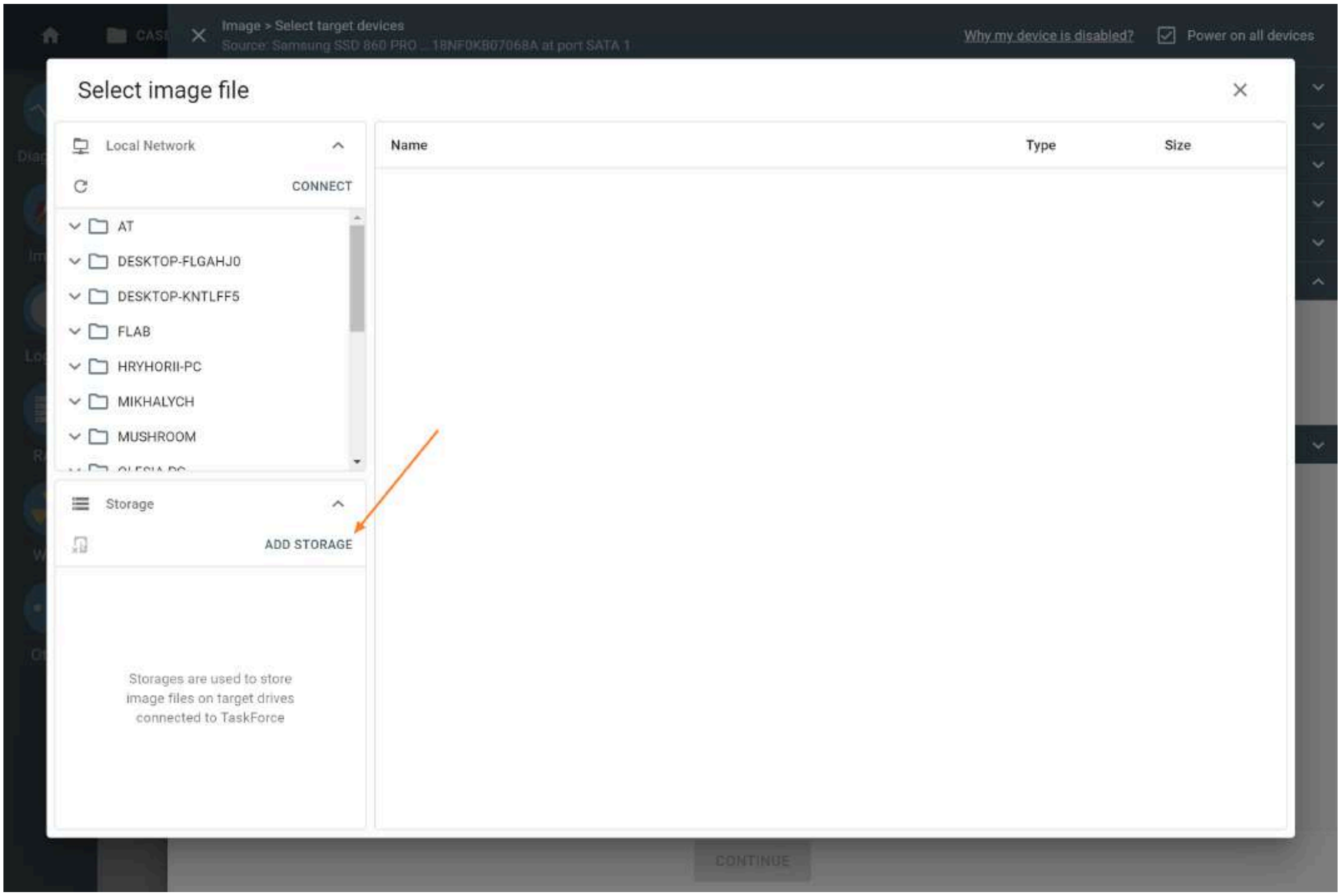
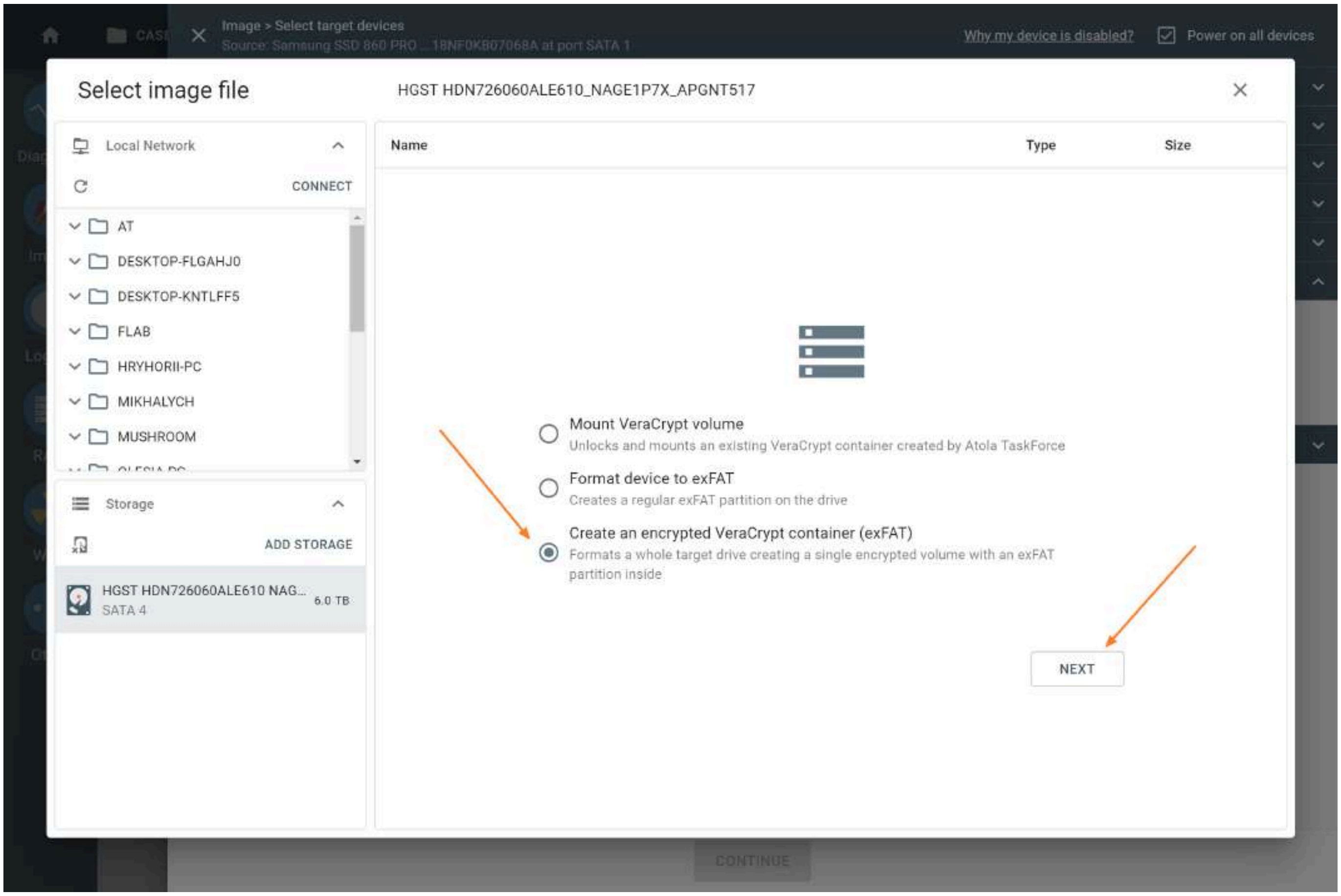


Image > Select target devices
Source: Samsung SSD 860 PRO ...18NF0KB07068A at port SATA 1
Why my device is disabled?
☑ Power on all devices
Select image file
Local Network
CONNECT
AT
DESKTOP-FLGAHJ0
DESKTOP-KNTLFF5
FLAB
HRYHORII-PC
MIKHALYCH
MUSHROOM
Storage
ADD STORAGE
Storages are used to store image files on target drives connected to TaskForce
Name
Type
Size
CONTINUE

6. On the **Select device** panel, switch to the **Drives** tab and choose the drive connected to a port in the *Target* mode.

7. Select **Create an encrypted VeraCrypt container (exFAT)** and click **Next**.



Select image file

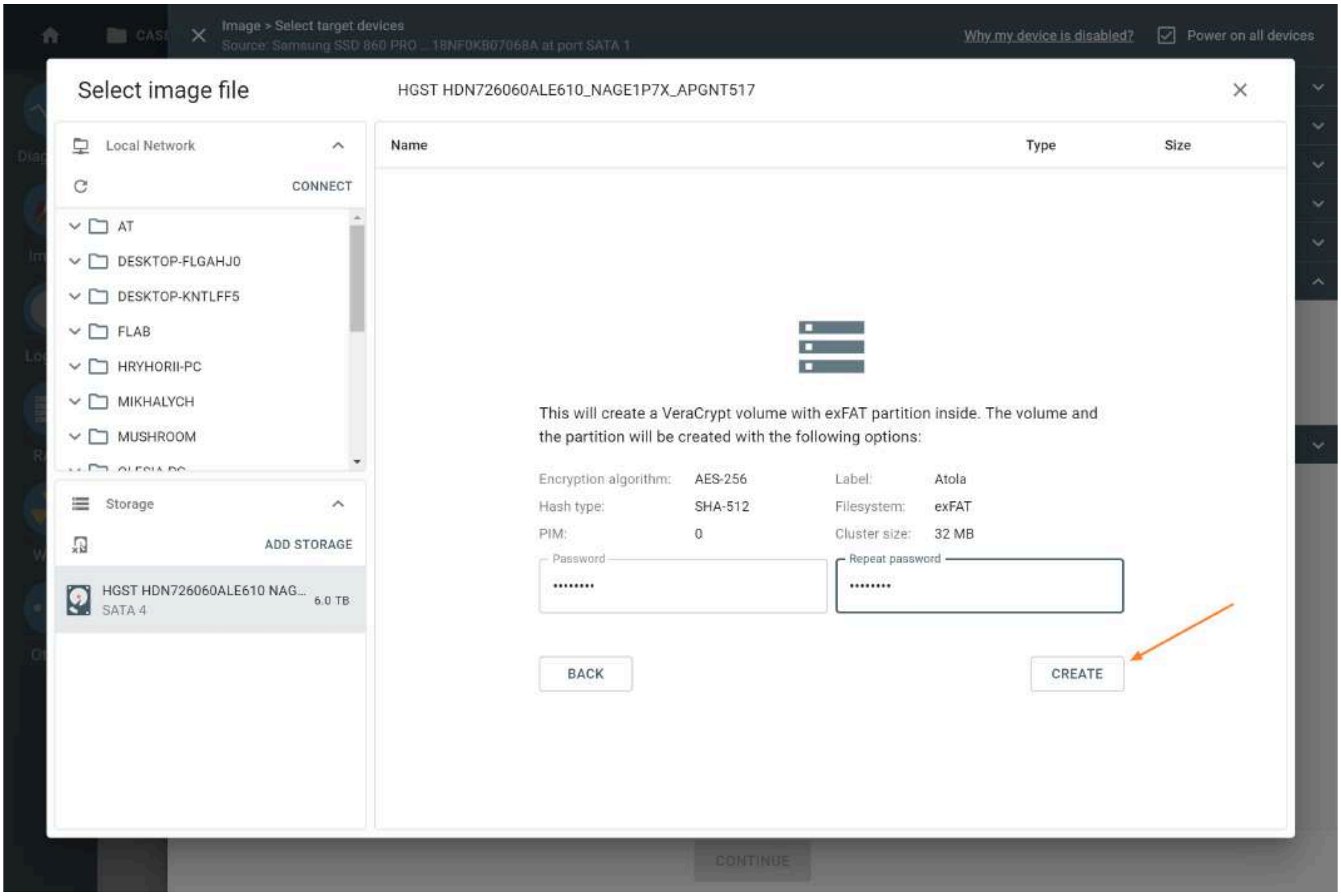
HGST HDN726060ALE610_NAGE1P7X_APGNT517

○ Mount VeraCrypt volume
Unlocks and mounts an existing VeraCrypt container created by Atola TaskForce

○ Format device to exFAT
Creates a regular exFAT partition on the drive

● Create an encrypted VeraCrypt container (exFAT)
Formats a whole target drive creating a single encrypted volume with an exFAT partition inside

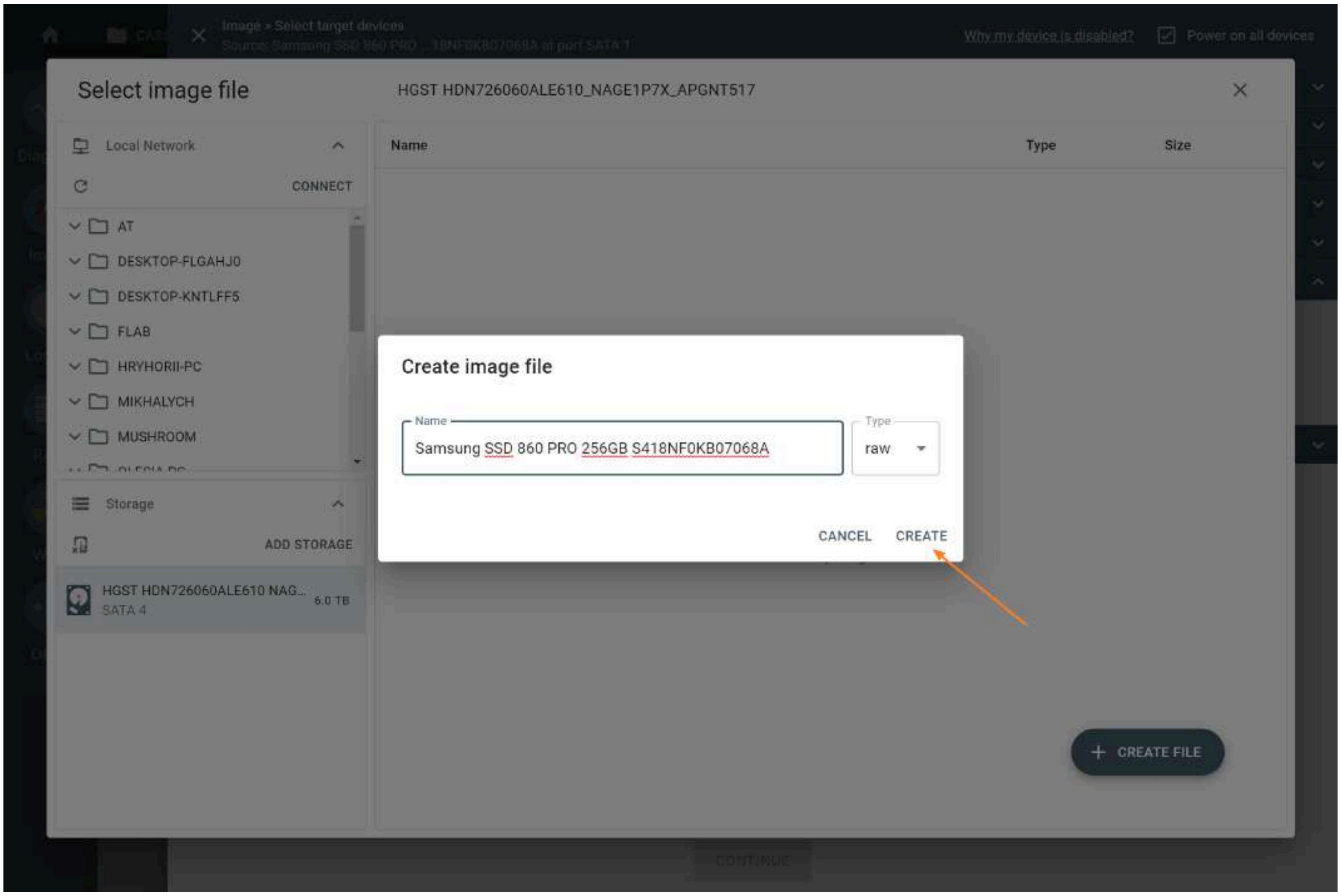
8. Enter and confirm the password for the encrypted volume on the drive. Then click **Create**.



This will create a VeraCrypt volume with exFAT partition inside. The volume and the partition will be created with the following options:

Encryption algorithm: AES-256
Hash type: SHA-512
PIM: 0
Label: Atola
Filesystem: exFAT
Cluster size: 32 MB
Password: ••••••••
Repeat password: ••••••••

9. Confirm the formatting of the device by entering *YES* and clicking **OK**. After this step, the formatting takes a few seconds.
10. Click + **Create file**.
11. Enter the name of the image file and choose the file format (E01, raw, img or dd). Then click **Create**.



Create image file

Name: Samsung SSD 860 PRO 256GB S418NF0KB07068A

Type: raw

12. Once you have created the file, you may add more image files in the same or a different folder.

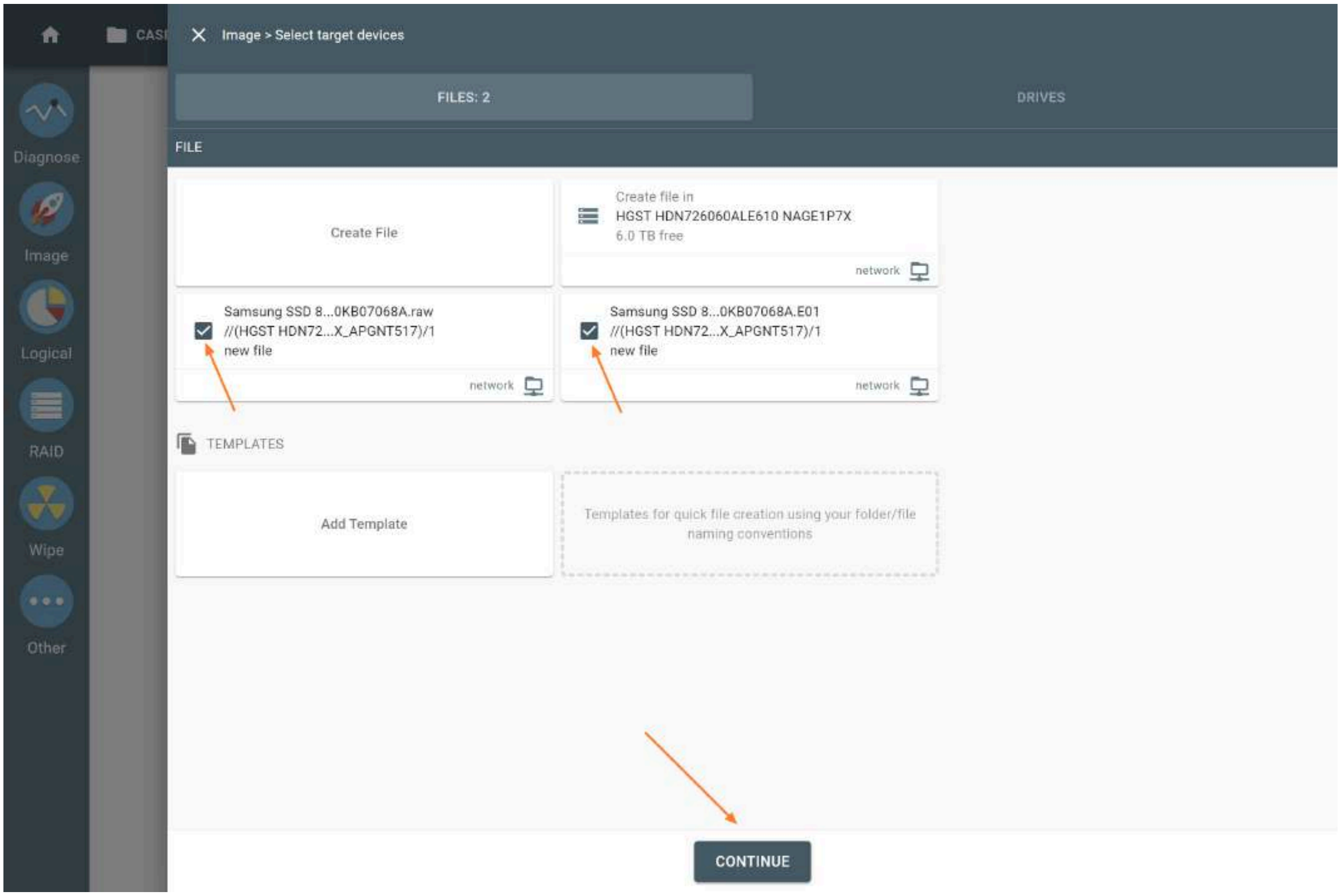


Image > Select target devices

Create file in
HGST HDN726060ALE610 NAGE1P7X
6.0 TB free

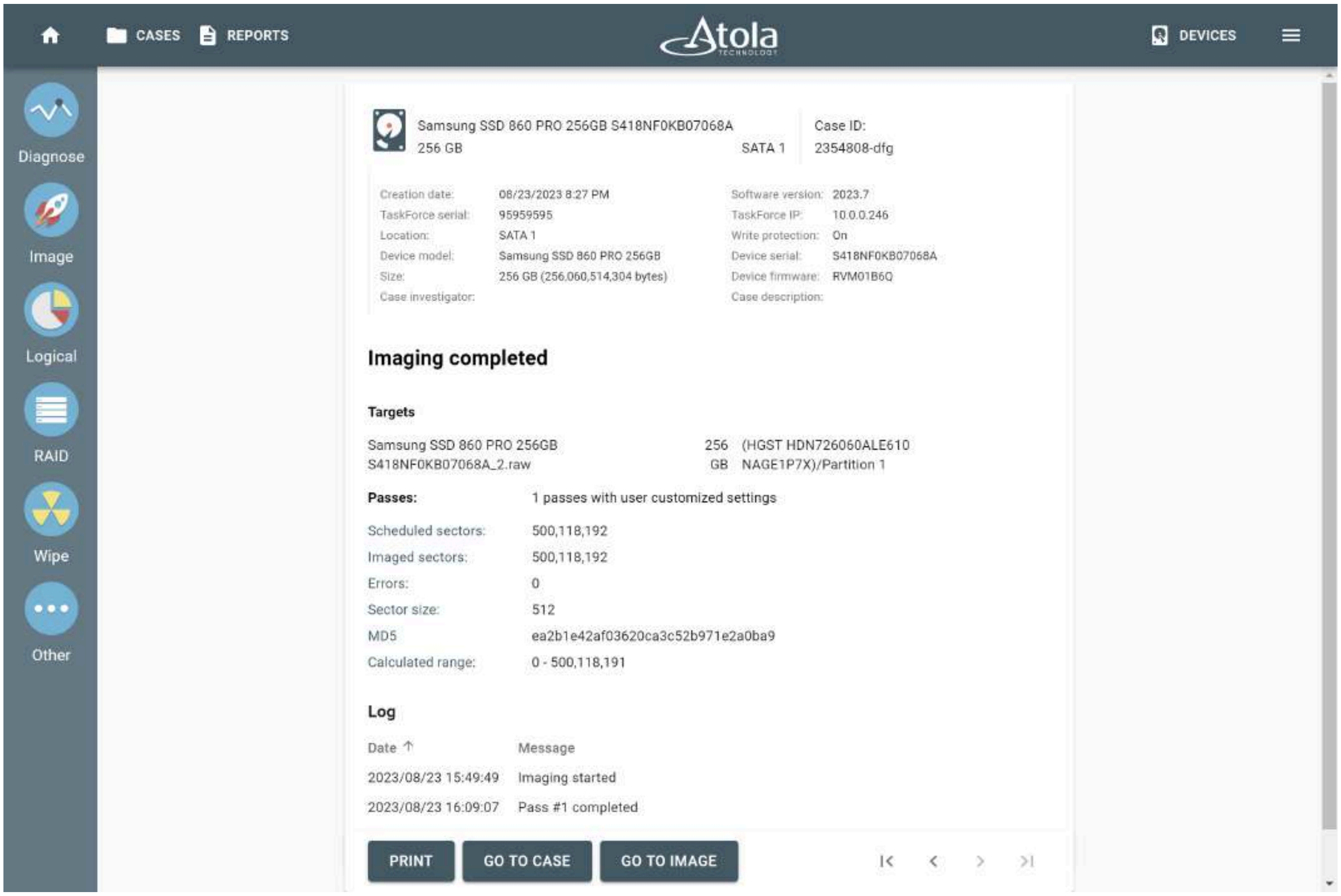
☑ Samsung SSD 8...0KB07068A.raw
//(HGST HDN72...X_APGNT517)/1
new file

☑ Samsung SSD 8...0KB07068A.E01
//(HGST HDN72...X_APGNT517)/1
new file

Templates for quick file creation using your folder/file naming conventions

After you click **Continue**, TaskForce 2 images the evidence into the file on your encrypted target.

Upon completion of the imaging session, check the **Imaging completed** report.



Samsung SSD 860 PRO 256GB S418NF0KB07068A
256 GB SATA 1

Case ID:
2354808-dfg

Creation date:	08/23/2023 8:27 PM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	Samsung SSD 860 PRO 256GB	Device serial:	S418NF0KB07068A
Size:	256 GB (256,060,514,304 bytes)	Device firmware:	RVM01B6Q
Case investigator:		Case description:	

Imaging completed

Targets

Samsung SSD 860 PRO 256GB S418NF0KB07068A_2.raw 256 GB (HGST HDN726060ALE610 NAGE1P7X)/Partition 1

Passes:	1 passes with user customized settings
Scheduled sectors:	500,118,192
Imaged sectors:	500,118,192
Errors:	0
Sector size:	512
MD5	ea2b1e42af03620ca3c52b971e2a0ba9
Calculated range:	0 - 500,118,191

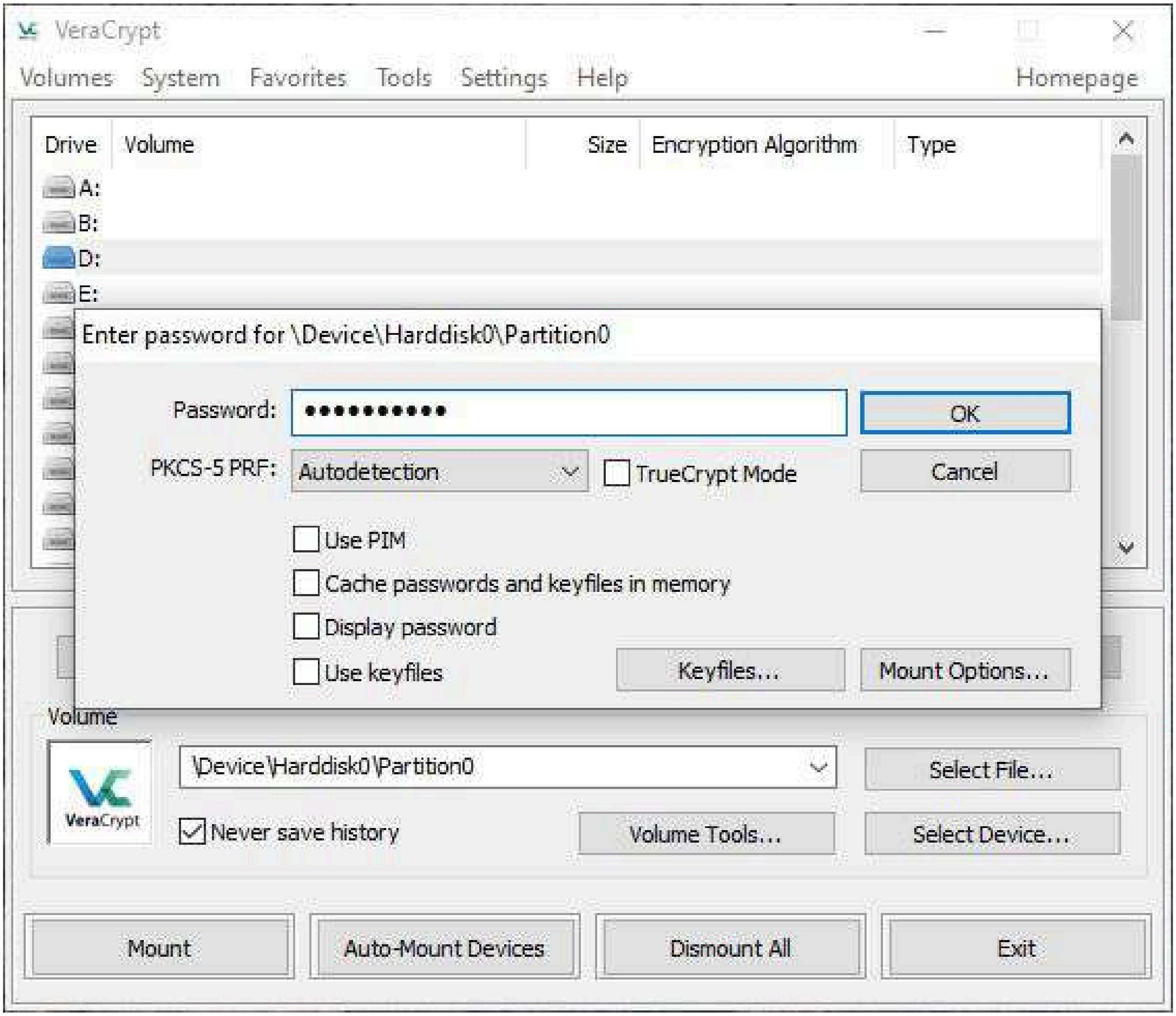
Log

Date ↑	Message
2023/08/23 15:49:49	Imaging started
2023/08/23 16:09:07	Pass #1 completed

Extract data from an encrypted volume

To find the VeraCrypt volume and the imaged file, do the following:

1. Plug the target drive into your computer.
2. Use VeraCrypt software to safely access encrypted data from your drive.
3. Select the drive label (A, B, C, etc.) on which you want the volume to be mounted.
4. Click **Select device**.
5. In the pop-up window, select your encrypted volume.
6. Click **Mount**. Now you can view the partition name, size and encryption algorithm.
7. Use the password set prior to the imaging session to get access to the encrypted volume.



Enter password for \Device\Harddisk0\Partition0

Password: ●●●●●●●●●●●

PKCS-5 PRF: Autodetection

□ TrueCrypt Mode

□ Use PIM

□ Cache passwords and keyfiles in memory

□ Display password

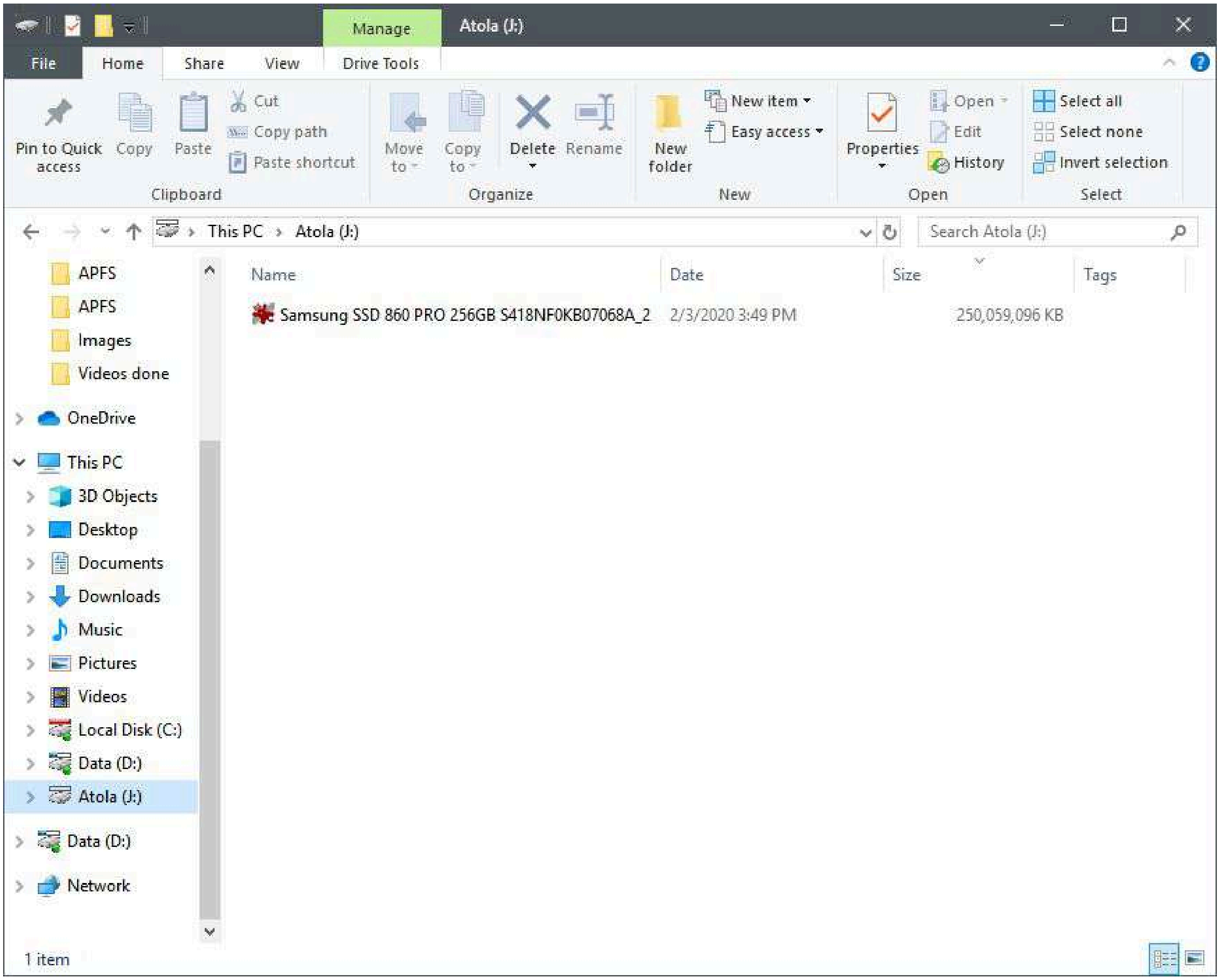
□ Use keyfiles

Volume

\Device\Harddisk0\Partition0

☑ Never save history

After you enter the password, the volume is mounted and you can access it from Windows Explorer and use the image for subsequent operations.

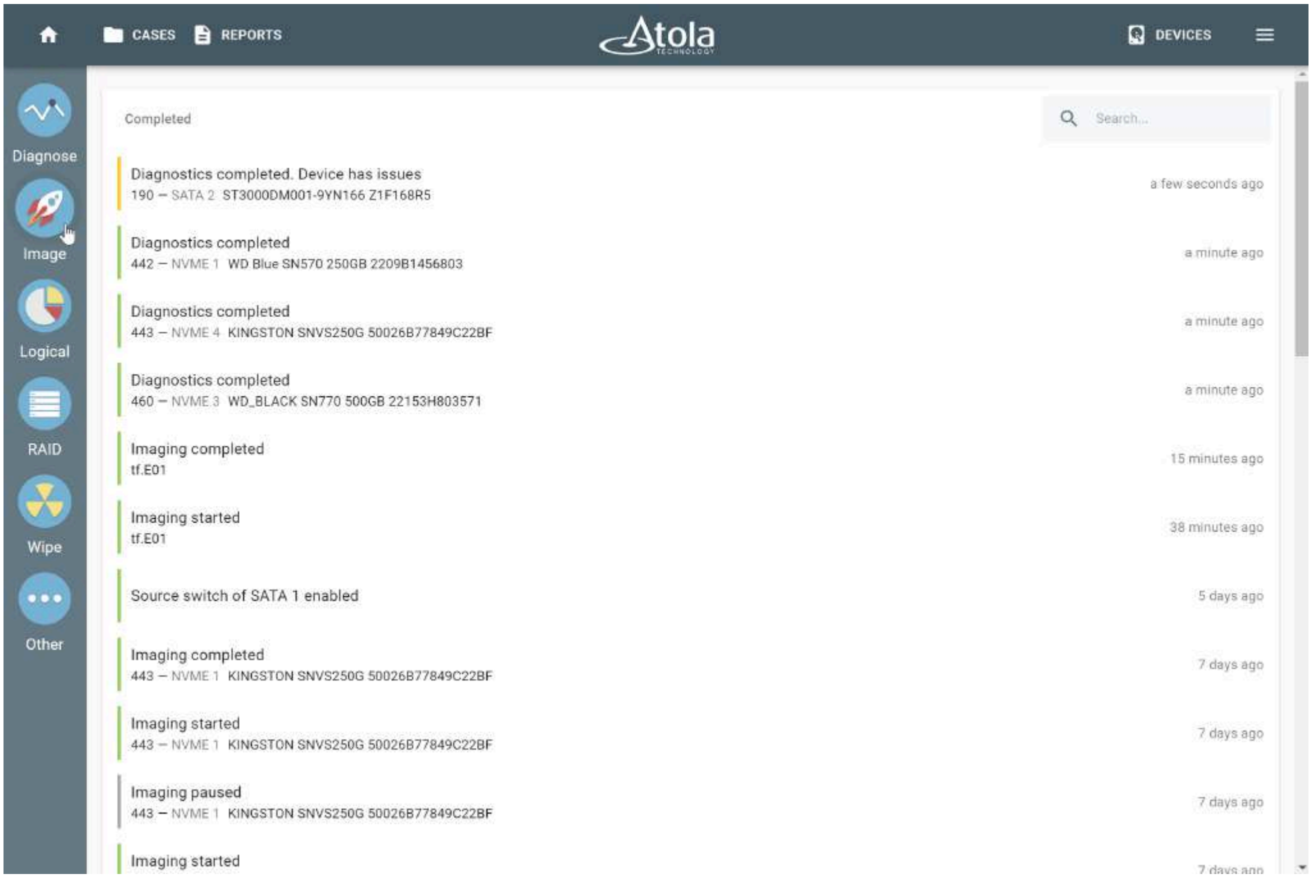


Name	Date	Size	Tags
Samsung SSD 860 PRO 256GB S418NF0KB07068A_2	2/3/2020 3:49 PM	250,059,096 KB	

Restore E01, AFF4, RAW image file to drive

To restore data from an image file to a drive using Atola TaskForce 2, follow these steps:

1. In the TaskForce main window, click **Image**.

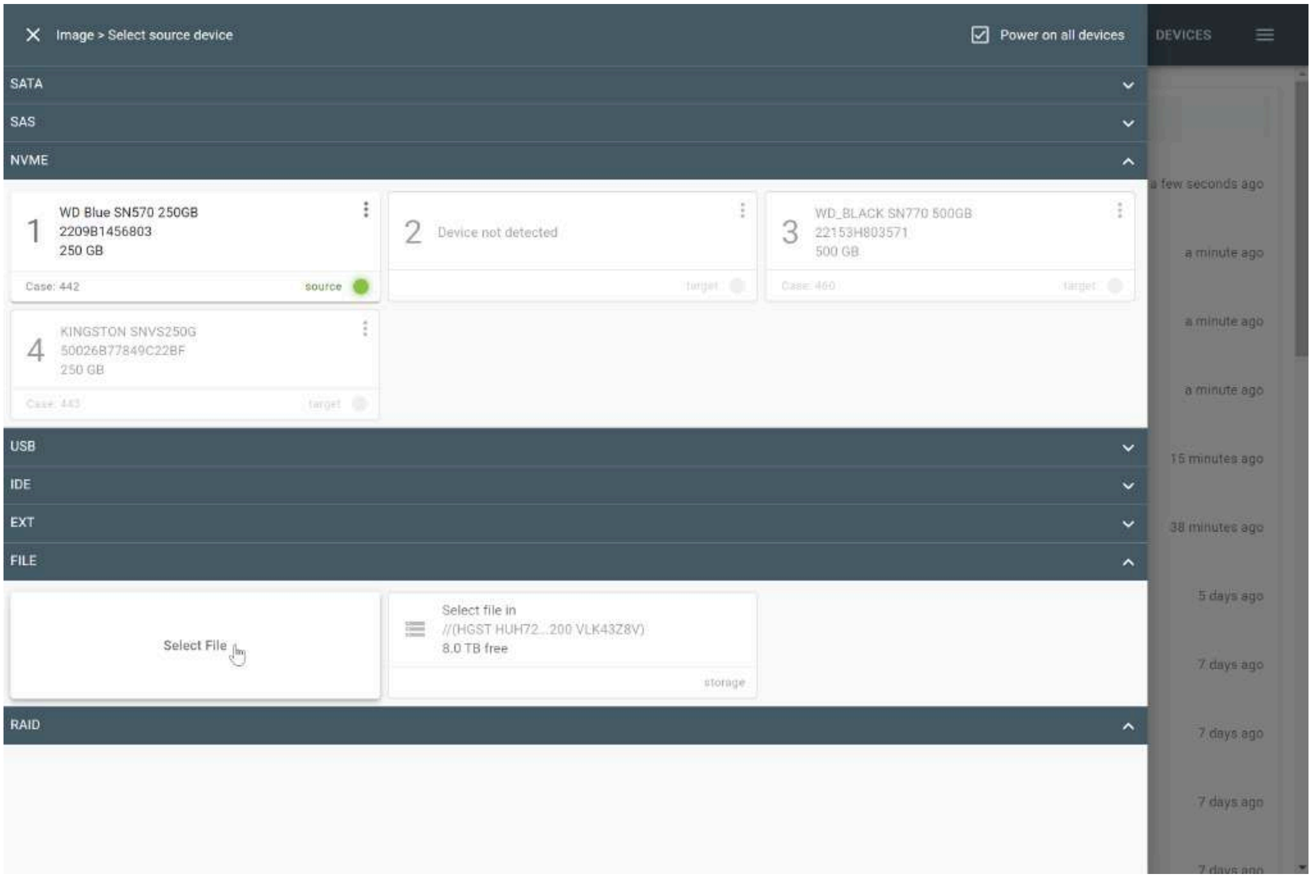


Completed

Search...

Diagnostics completed. Device has issues 190 — SATA 2 ST3000DM001-9YN166 Z1F168R5	a few seconds ago
Diagnostics completed 442 — NVME 1 WD Blue SN570 250GB 2209B1456803	a minute ago
Diagnostics completed 443 — NVME 4 KINGSTON SNVS250G 50026B77849C22BF	a minute ago
Diagnostics completed 460 — NVME 3 WD_BLACK SN770 500GB 22153H803571	a minute ago
Imaging completed tf.E01	15 minutes ago
Imaging started tf.E01	38 minutes ago
Source switch of SATA 1 enabled	5 days ago
Imaging completed 443 — NVME 1 KINGSTON SNVS250G 50026B77849C22BF	7 days ago
Imaging started 443 — NVME 1 KINGSTON SNVS250G 50026B77849C22BF	7 days ago
Imaging paused 443 — NVME 1 KINGSTON SNVS250G 50026B77849C22BF	7 days ago
Imaging started	7 days ago

2. On the **Select source device** panel, expand the **File** section and then click **Select file**.



1 WD Blue SN570 250GB 2209B1456803 250 GB — Case: 442 — source

2 Device not detected — target

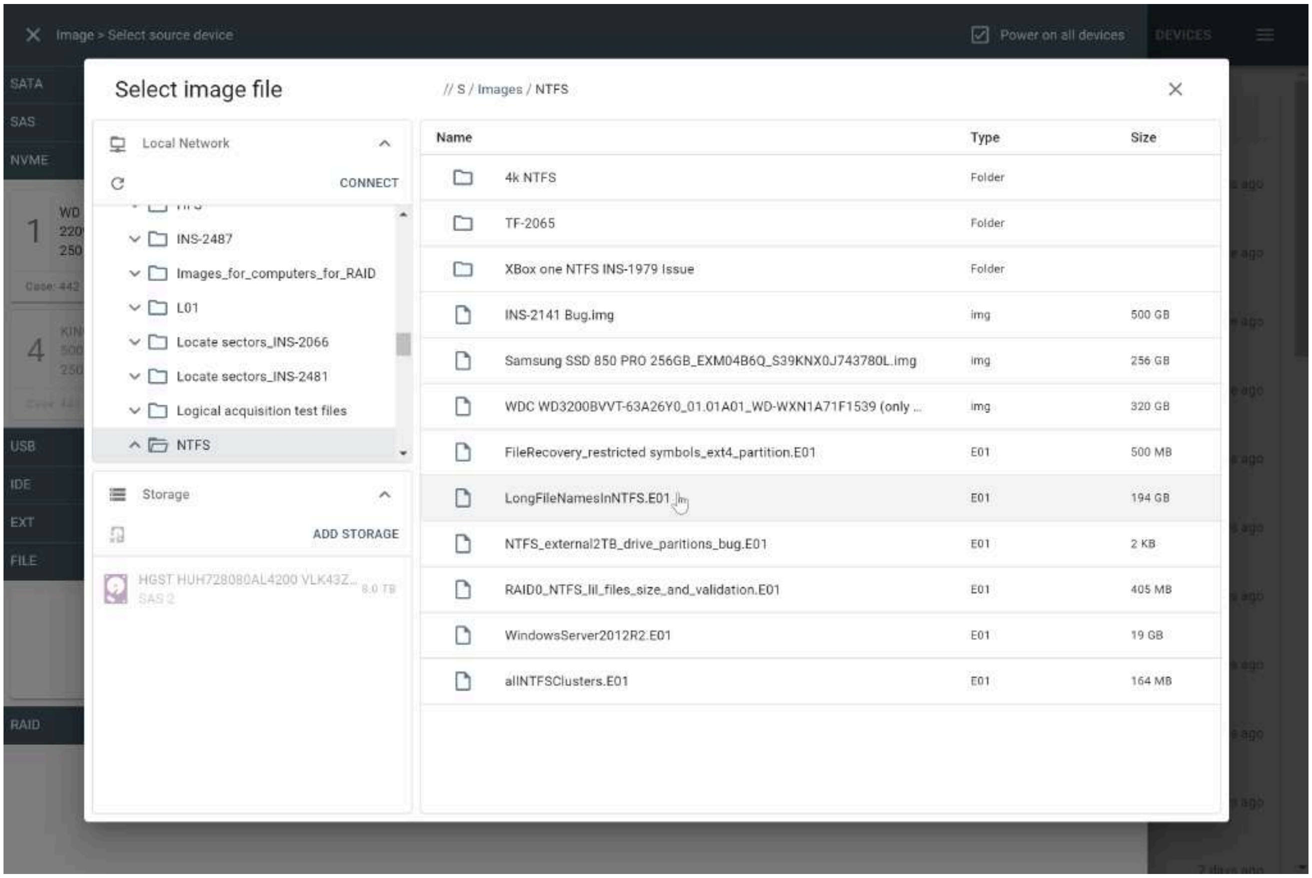
3 WD_BLACK SN770 500GB 22153H803571 500 GB — Case: 460 — target

4 KINGSTON SNVS250G 50026B77849C22BF 250 GB — Case: 443 — target

Select File

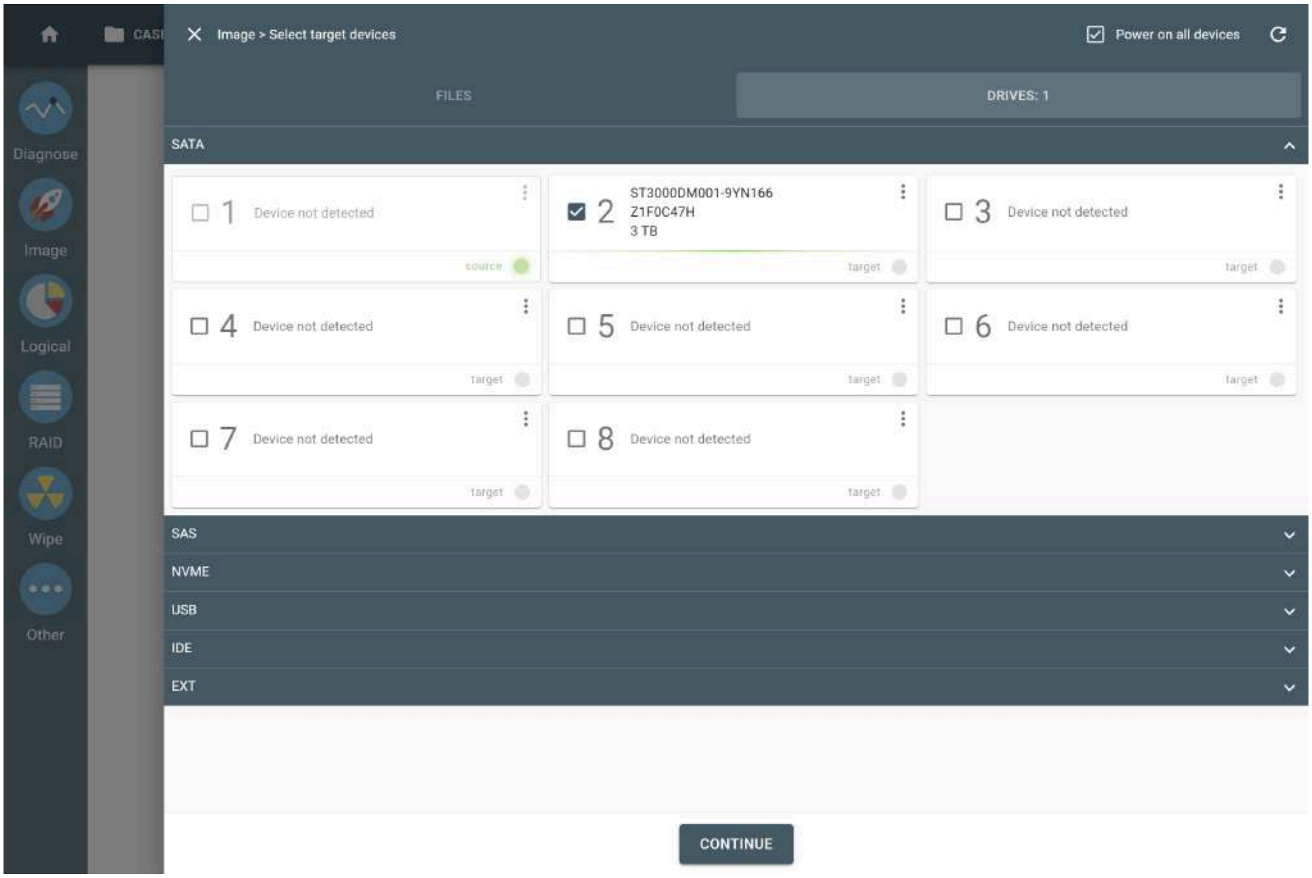
Select file in //(HGST HUH72...200 VLK43Z8V) 8.0 TB free — storage

3. Select the E01, AFF4 or RAW file you are planning to restore.



Name	Type	Size
4k NTFS	Folder	
TF-2065	Folder	
XBox one NTFS INS-1979 Issue	Folder	
INS-2141 Bug.img	img	500 GB
Samsung SSD 850 PRO 256GB_EXM04B6Q_S39KNX0J743780L.img	img	256 GB
WDC WD3200BVVT-63A26Y0_01.01A01_WD-WXN1A71F1539 (only ...	img	320 GB
FileRecovery_restricted symbols_ext4_partition.E01	E01	500 MB
LongFileNamesInNTFS.E01	E01	194 GB
NTFS_external2TB_drive_paritions_bug.E01	E01	2 KB
RAID0_NTFS_lil_files_size_and_validation.E01	E01	405 MB
WindowsServer2012R2.E01	E01	19 GB
allNTFSClusters.E01	E01	164 MB

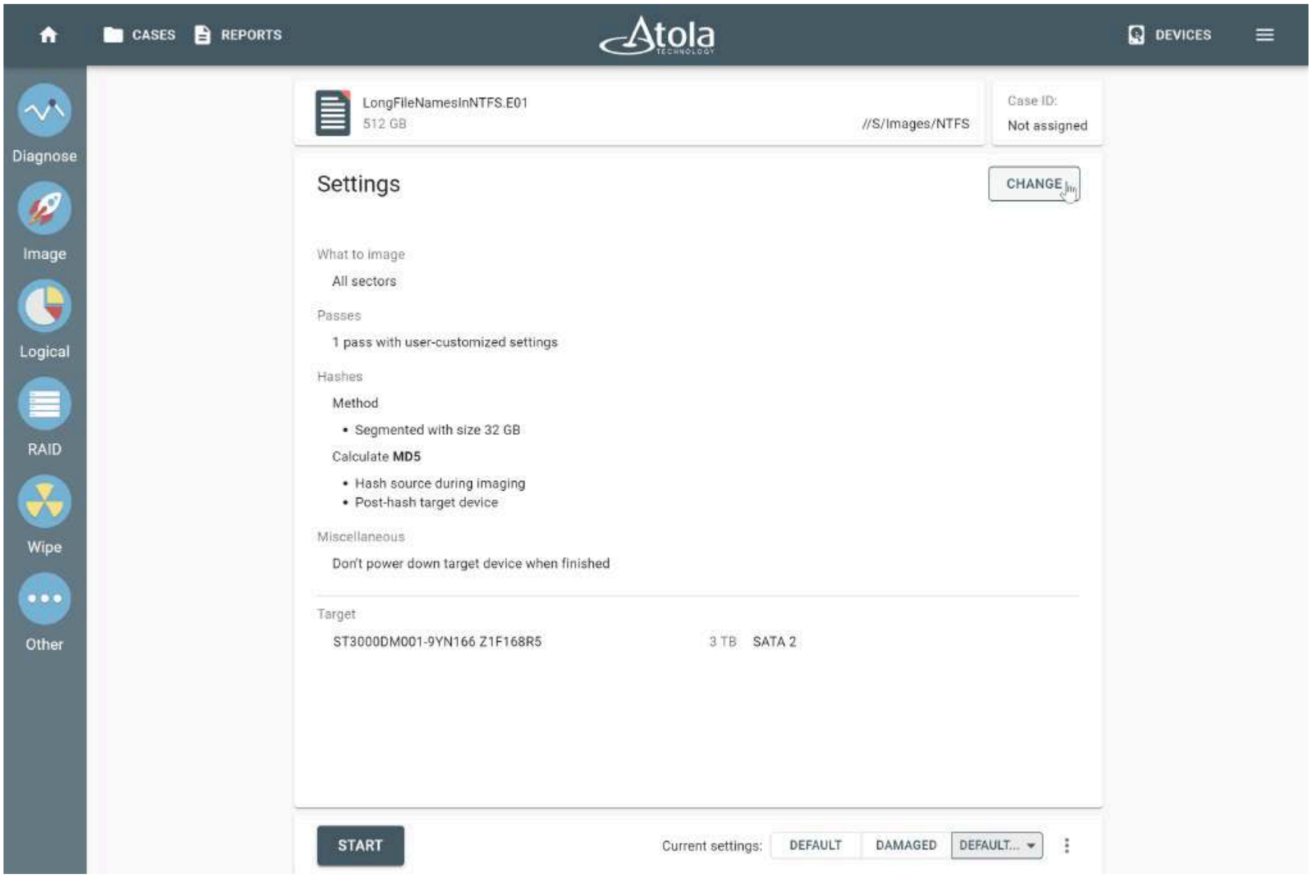
4. Select the target drive and click **Continue**.



☐ 1 Device not detected — source
☑ 2 ST3000DM001-9YN166 Z1F0C47H 3 TB — target
☐ 3 Device not detected — target
☐ 4 Device not detected — target
☐ 5 Device not detected — target
☐ 6 Device not detected — target
☐ 7 Device not detected — target
☐ 8 Device not detected — target

> If your target drive is larger than the size of the image, the hash values of the target drive will not be identical to that of the image file. With TaskForce 2, you can limit a SATA target drive's capacity via Host Protected Area (HPA) or Accessible Max Address (AMA). Applying the HPA or AMA will set a new max address in the drive’s firmware, which will make the sectors beyond the required capacity inaccessible. This will make the hashing process straightforward and the hashes will match.

To limit SATA target drive's capacity via HPA or AMA, go to the imaging **Settings** and click the **Change** button.



LongFileNamesInNTFS.E01
512 GB
//S/Images/NTFS
Case ID:
Not assigned

Settings

What to image
All sectors

Passes
1 pass with user-customized settings

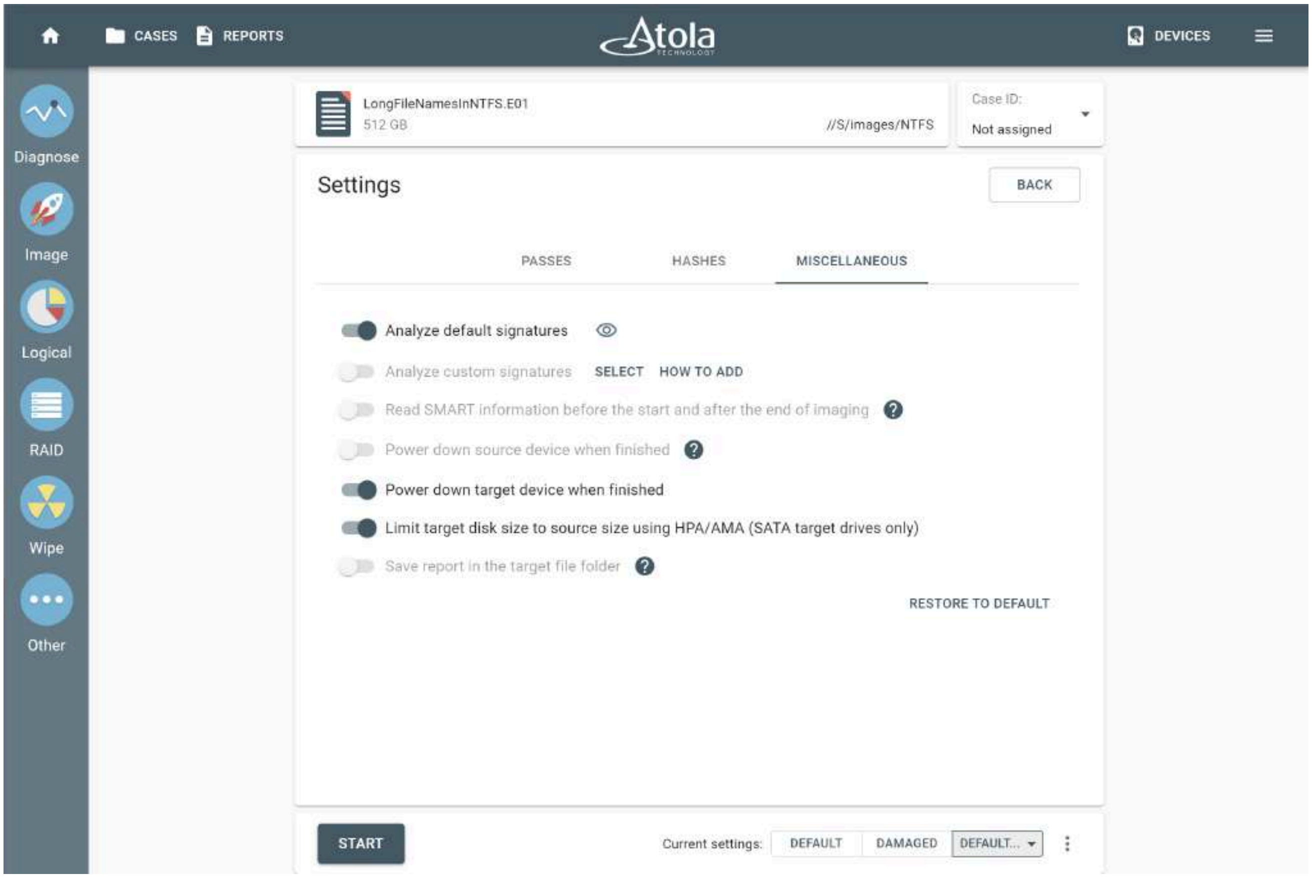
Hashes
Method
- Segmented with size 32 GB

Calculate **MD5**
- Hash source during imaging
- Post-hash target device

Miscellaneous
Don't power down target device when finished

Target
ST3000DM001-9YN166 Z1F168R5 3 TB SATA 2

Go to the **Miscellaneous** tab and enable the **Limit target disk size to source size using HPA/AMA** option.

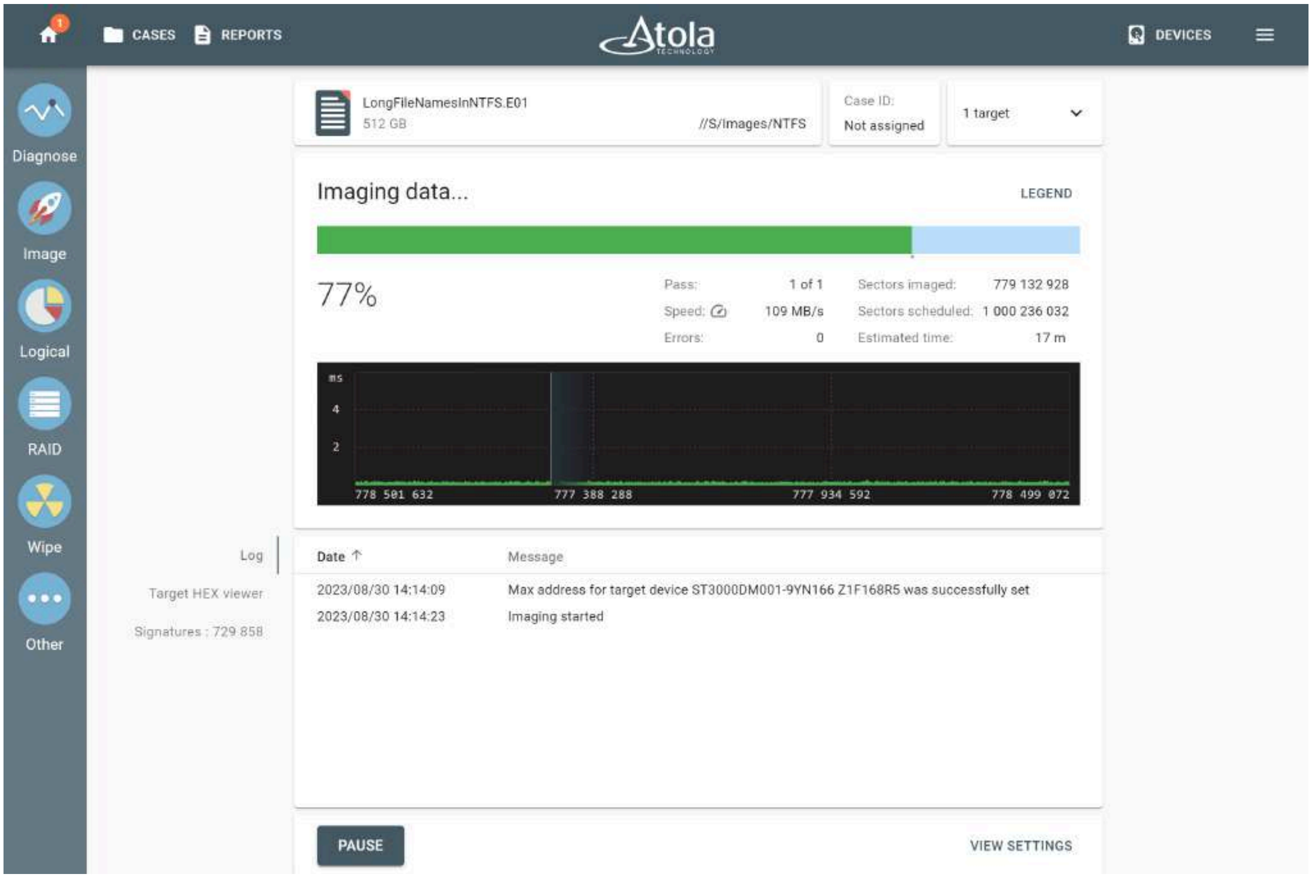


LongFileNamesInNTFS.E01
512 GB
//S/Images/NTFS
Case ID:
Not assigned

Settings

- ● Analyze default signatures
- ○ Analyze custom signatures SELECT HOW TO ADD
- ○ Read SMART information before the start and after the end of imaging
- ○ Power down source device when finished
- ● Power down target device when finished
- ● Limit target disk size to source size using HPA/AMA (SATA target drives only)
- ○ Save report in the target file folder

5. Click **Start** for the imaging to begin.



LongFileNamesInNTFS.E01
512 GB
//S/Images/NTFS

Case ID:
Not assigned

1 target

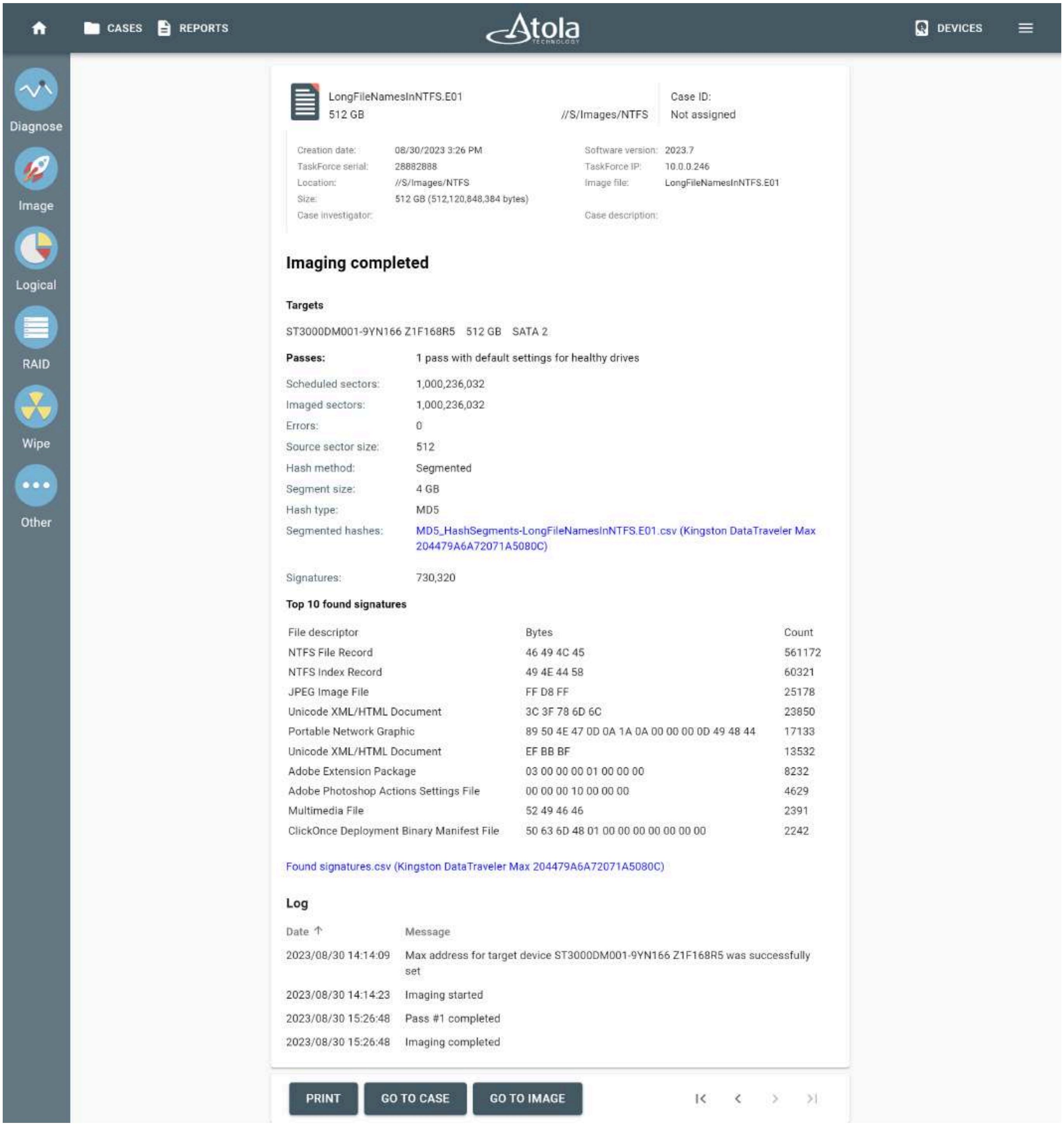
Imaging data...

77%

Pass: 1 of 1
Speed: 109 MB/s
Errors: 0
Sectors imaged: 779 132 928
Sectors scheduled: 1 000 236 032
Estimated time: 17 m

```
Date ↑                 Message
2023/08/30 14:14:09    Max address for target device ST3000DM001-9YN166 Z1F168R5 was successfully set
2023/08/30 14:14:23    Imaging started
```

TaskForce 2 automatically creates detailed reports for every session. The imaging report lists all the details of the source, the target, the imaging settings and timestamps including the setting of the new max address of the target drive. This makes such data extraction from a file transparent and forensically sound.



LongFileNamesInNTFS.E01
512 GB
//S/Images/NTFS

Case ID:
Not assigned

Creation date:	08/30/2023 3:26 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	//S/Images/NTFS	Image file:	LongFileNamesInNTFS.E01
Size:	512 GB (512,120,848,384 bytes)		
Case investigator:		Case description:	

Imaging completed

Targets

ST3000DM001-9YN166 Z1F168R5   512 GB   SATA 2

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	1,000,236,032
Imaged sectors:	1,000,236,032
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-LongFileNamesInNTFS.E01.csv (Kingston DataTraveler Max 204479A6A72071A5080C)
Signatures:	730,320

Top 10 found signatures

File descriptor	Bytes	Count
NTFS File Record	46 49 4C 45	561172
NTFS Index Record	49 4E 44 58	60321
JPEG Image File	FF D8 FF	25178
Unicode XML/HTML Document	3C 3F 78 6D 6C	23850
Portable Network Graphic	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44	17133
Unicode XML/HTML Document	EF BB BF	13532
Adobe Extension Package	03 00 00 00 01 00 00 00	8232
Adobe Photoshop Actions Settings File	00 00 00 10 00 00 00	4629
Multimedia File	52 49 46 46	2391
ClickOnce Deployment Binary Manifest File	50 63 6D 48 01 00 00 00 00 00 00 00	2242

Found signatures.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

Log

Date ↑	Message
2023/08/30 14:14:09	Max address for target device ST3000DM001-9YN166 Z1F168R5 was successfully set
2023/08/30 14:14:23	Imaging started
2023/08/30 15:26:48	Pass #1 completed
2023/08/30 15:26:48	Imaging completed

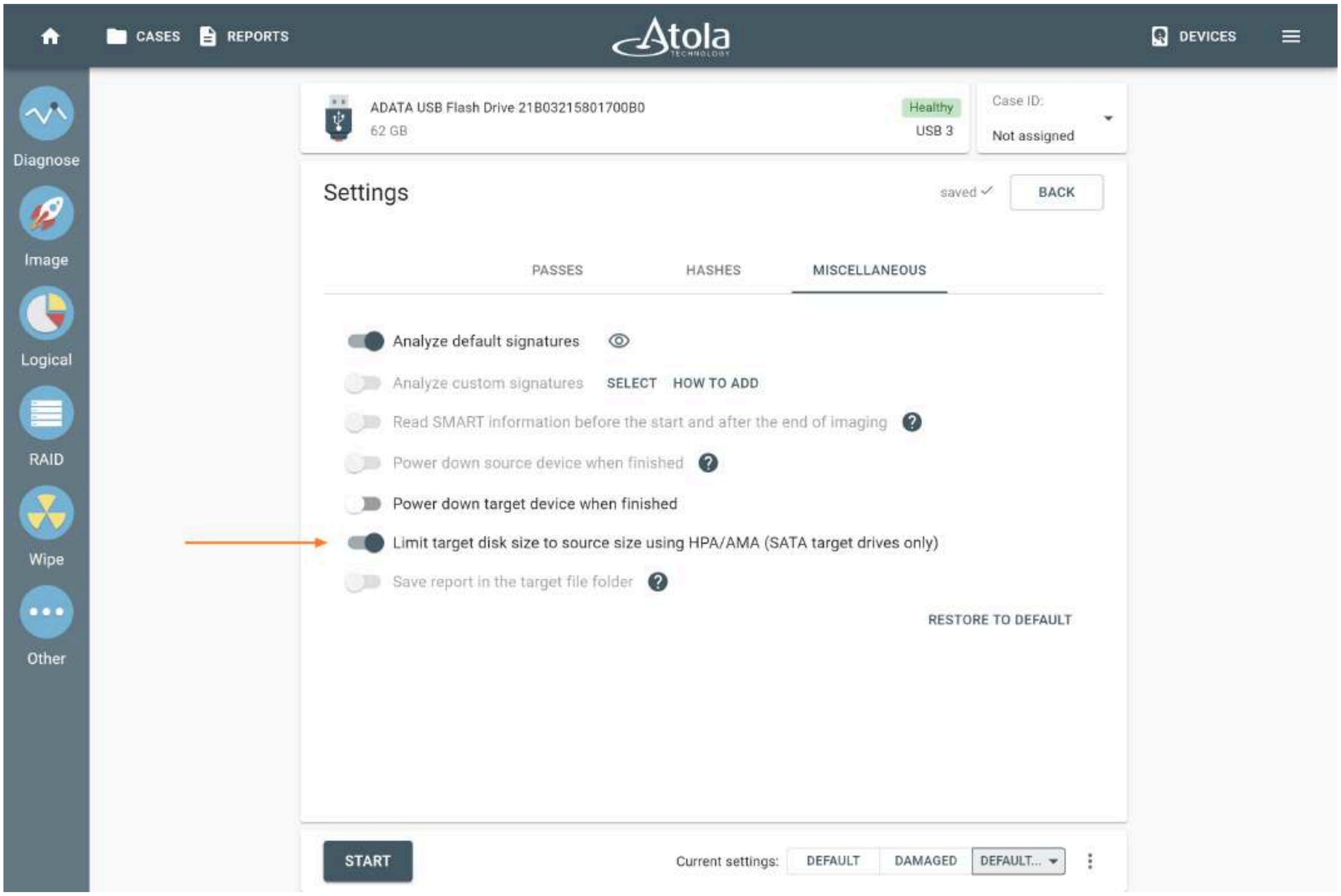
Clip target drive to source evidence size

When you image data from an evidence drive, but the target drive is larger than that of the source, the hash values for the source and for the target drives will not be identical. This will happen even if there is no data in the remaining space of the target.

To avoid it, you can limit your SATA target drive's capacity using Host Protected Area (HPA) or Accessible Max Address (AMA). It will make the sectors beyond this limit inaccessible to the hashing tools or the end user. In TaskForce, it only takes one quick adjustment to the imaging settings:

1. In the TaskForce main window, click **Image**.

2. Select a source and target device.
3. On the **Imaging sessions** page, click **Start new**.
4. On the **Settings** page, click **Change**.
5. On the **Miscellaneous** tab, toggle the **Limit target disk size to source size using HPA/AMA (SATA target ports only)** option.



ADATA USB Flash Drive 21B03215801700B0
62 GB
Healthy
USB 3
Case ID:
Not assigned

Settings
saved ✓ BACK

PASSES HASHES MISCELLANEOUS

● Analyze default signatures
○ Analyze custom signatures SELECT HOW TO ADD
○ Read SMART information before the start and after the end of imaging ?
○ Power down source device when finished ?
○ Power down target device when finished
● Limit target disk size to source size using HPA/AMA (SATA target drives only)
○ Save report in the target file folder ?

RESTORE TO DEFAULT

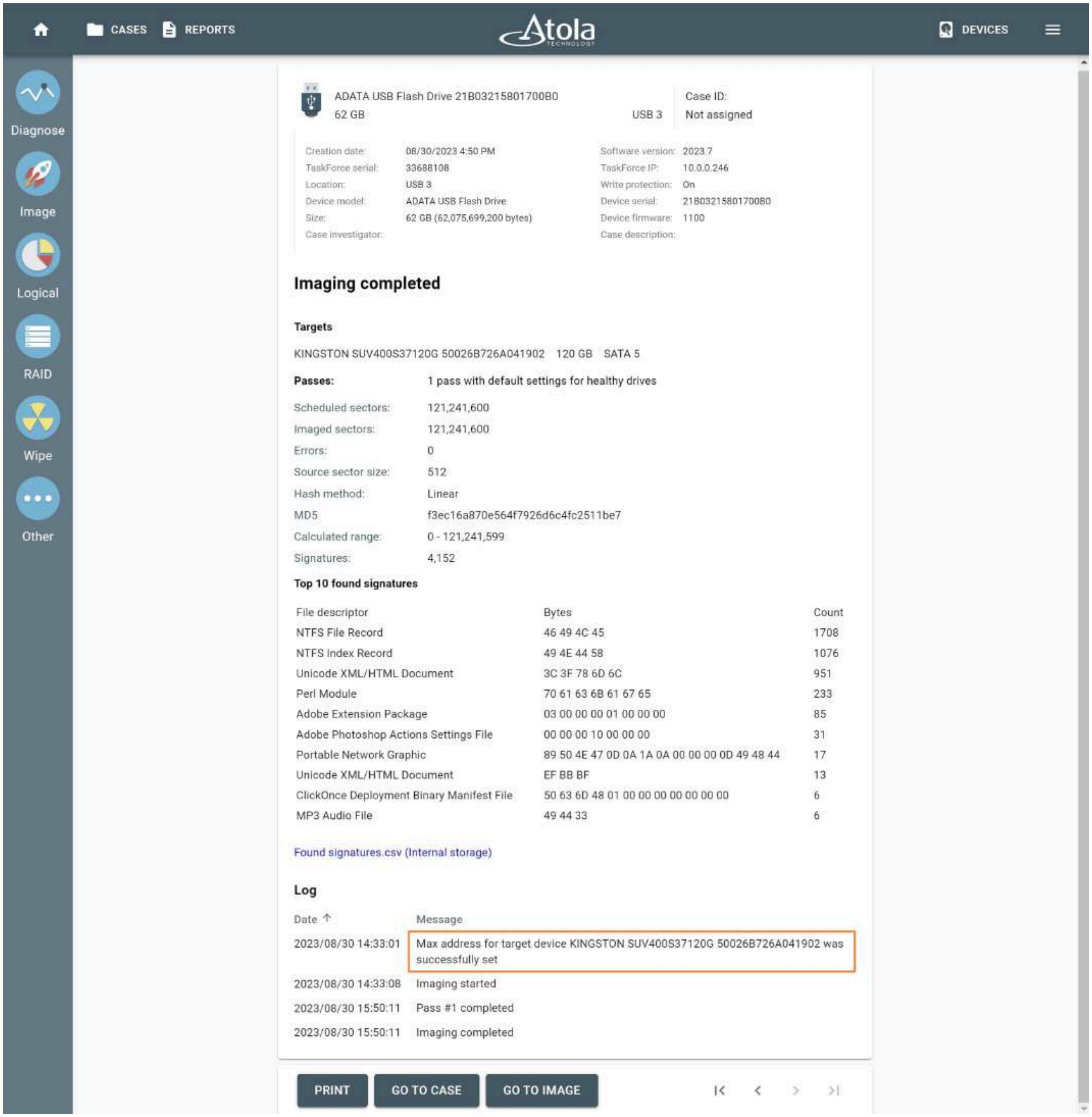
START
Current settings: DEFAULT DAMAGED DEFAULT...

Enabling HPA/AMA restriction for target.

You can now proceed with the imaging process by clicking the **Start** button.

Before the imaging starts, TaskForce 2 looks up the size of the evidence drive and limits the space of the target using HPA/AMA to make its capacity identical to that of the evidence drive.

When imaging is complete, the report will contain information about the time when HPA/AMA was enabled.



ADATA USB Flash Drive 21B03215801700B0
62 GB
USB 3

Case ID:
Not assigned

Creation date:	08/30/2023 4:50 PM	Software version:	2023.7
TaskForce serial:	33688108	TaskForce IP:	10.0.0.246
Location:	USB 3	Write protection:	On
Device model:	ADATA USB Flash Drive	Device serial:	21B03215801700B0
Size:	62 GB (62,075,699,200 bytes)	Device firmware:	1100
Case investigator:		Case description:	

Imaging completed

Targets

KINGSTON SUV400S37120G 50026B726A041902 120 GB SATA 5

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	121,241,600
Imaged sectors:	121,241,600
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	f3ec16a870e564f7926d6c4fc2511be7
Calculated range:	0 - 121,241,599
Signatures:	4,152

Top 10 found signatures

File descriptor	Bytes	Count
NTFS File Record	46 49 4C 45	1708
NTFS Index Record	49 4E 44 58	1076
Unicode XML/HTML Document	3C 3F 78 6D 6C	951
Perl Module	70 61 63 6B 61 67 65	233
Adobe Extension Package	03 00 00 00 01 00 00 00	85
Adobe Photoshop Actions Settings File	00 00 00 10 00 00 00	31
Portable Network Graphic	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44	17
Unicode XML/HTML Document	EF BB BF	13
ClickOnce Deployment Binary Manifest File	50 63 6D 48 01 00 00 00 00 00 00	6
MP3 Audio File	49 44 33	6

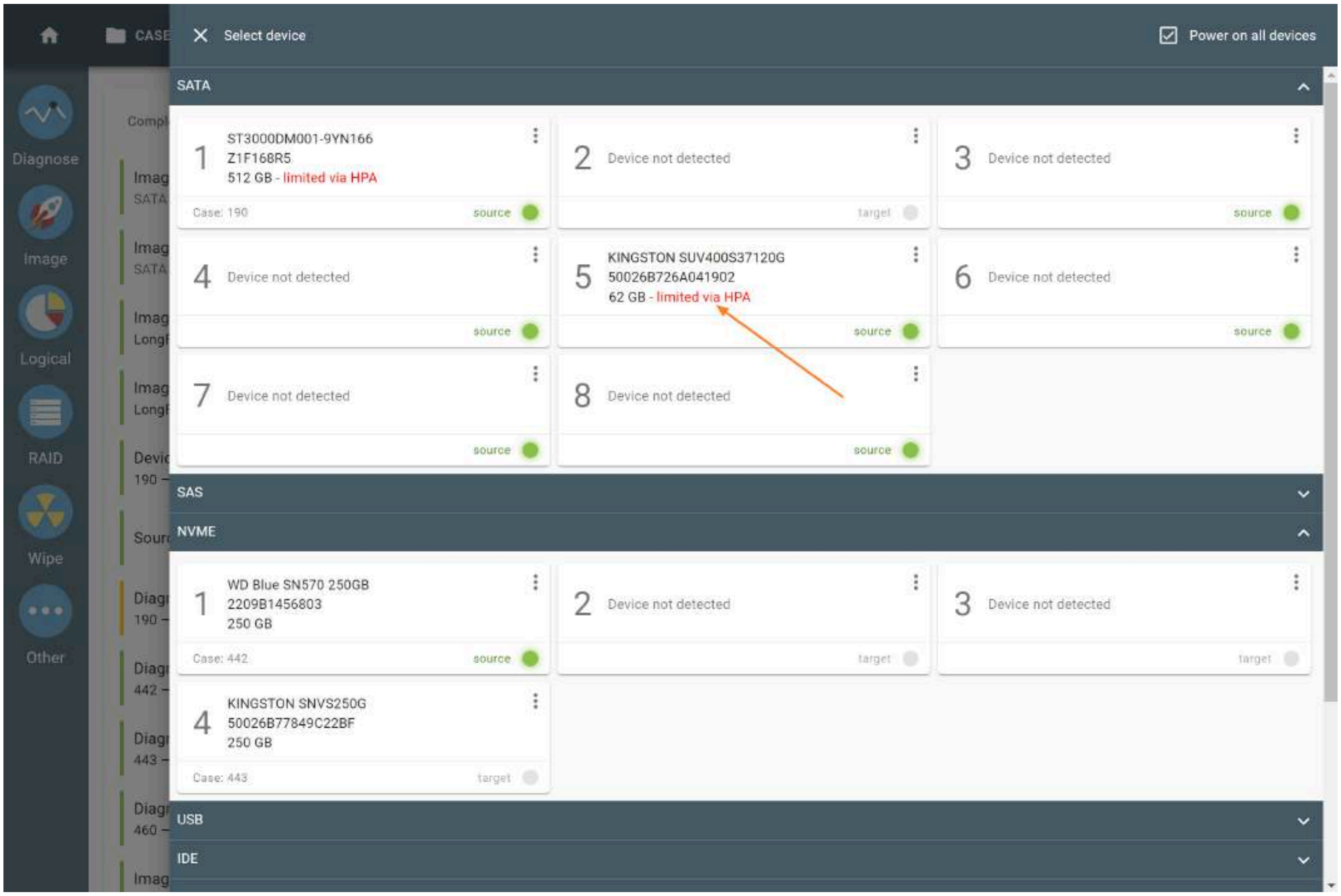
Found signatures.csv (Internal storage)

Log

Date ↑	Message
2023/08/30 14:33:01	Max address for target device KINGSTON SUV400S37120G 50026B726A041902 was successfully set
2023/08/30 14:33:08	Imaging started
2023/08/30 15:50:11	Pass #1 completed
2023/08/30 15:50:11	Imaging completed

The Imaging report indicates the change to the target drive capacity.

The target disk's port in Devices menu now contains an HPA/AMA indicator, thus informing you that HPA/AMA has been enabled on this drive.



SATA

1 ST3000DM001-9YN166
Z1F168R5
512 GB - limited via HPA
Case: 190 source ●

2 Device not detected target ○

3 Device not detected source ●

4 Device not detected source ●

5 KINGSTON SUV400S37120G
50026B726A041902
62 GB - limited via HPA
source ●

6 Device not detected source ●

7 Device not detected source ●

8 Device not detected source ●

NVME

1 WD Blue SN570 250GB
2209B1456803
250 GB
Case: 442 source ●

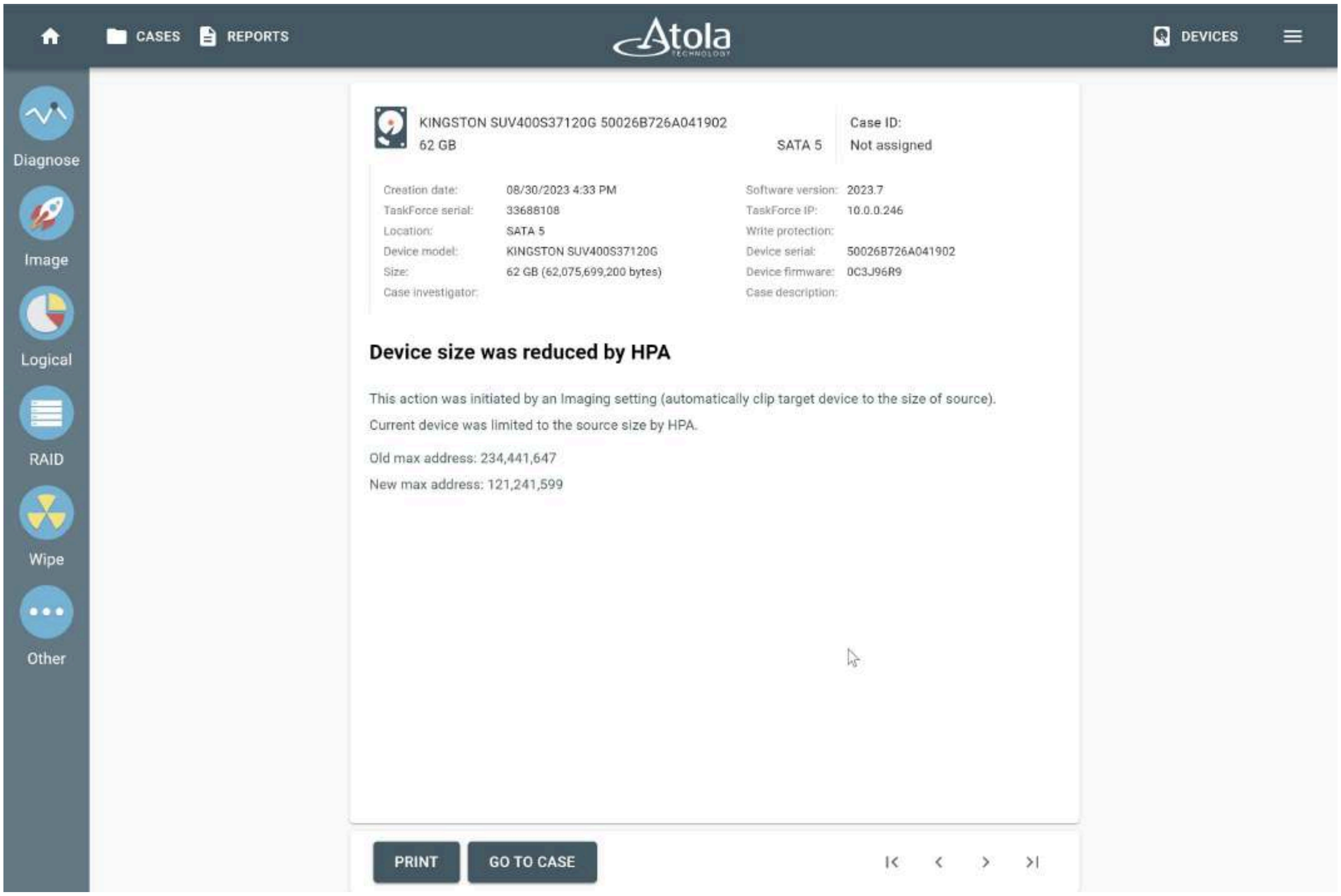
2 Device not detected target ○

3 Device not detected target ○

4 KINGSTON SNVS250G
50026B77849C22BF
250 GB
Case: 443 target ○

The HPA indicator in the port of the Device menu.

There will also be a report created in the case management system, which indicates the old (native) and the new (as set by HPA/AMA) max address.



KINGSTON SUV400S37120G 50026B726A041902
62 GB
SATA 5
Case ID:
Not assigned

Creation date: 08/30/2023 4:33 PM
TaskForce serial: 33688108
Location: SATA 5
Device model: KINGSTON SUV400S37120G
Size: 62 GB (62,075,699,200 bytes)
Case investigator:

Software version: 2023.7
TaskForce IP: 10.0.0.246
Write protection:
Device serial: 50026B726A041902
Device firmware: 0C3J96R9
Case description:

Device size was reduced by HPA

This action was initiated by an Imaging setting (automatically clip target device to the size of source).
Current device was limited to the source size by HPA.

Old max address: 234,441,647
New max address: 121,241,599

The report about HPA activation.

Now you can calculate hash on both drives to make sure the hash values are identical.

> Enabling HPA/AMA is an option available only for SATA target drives.

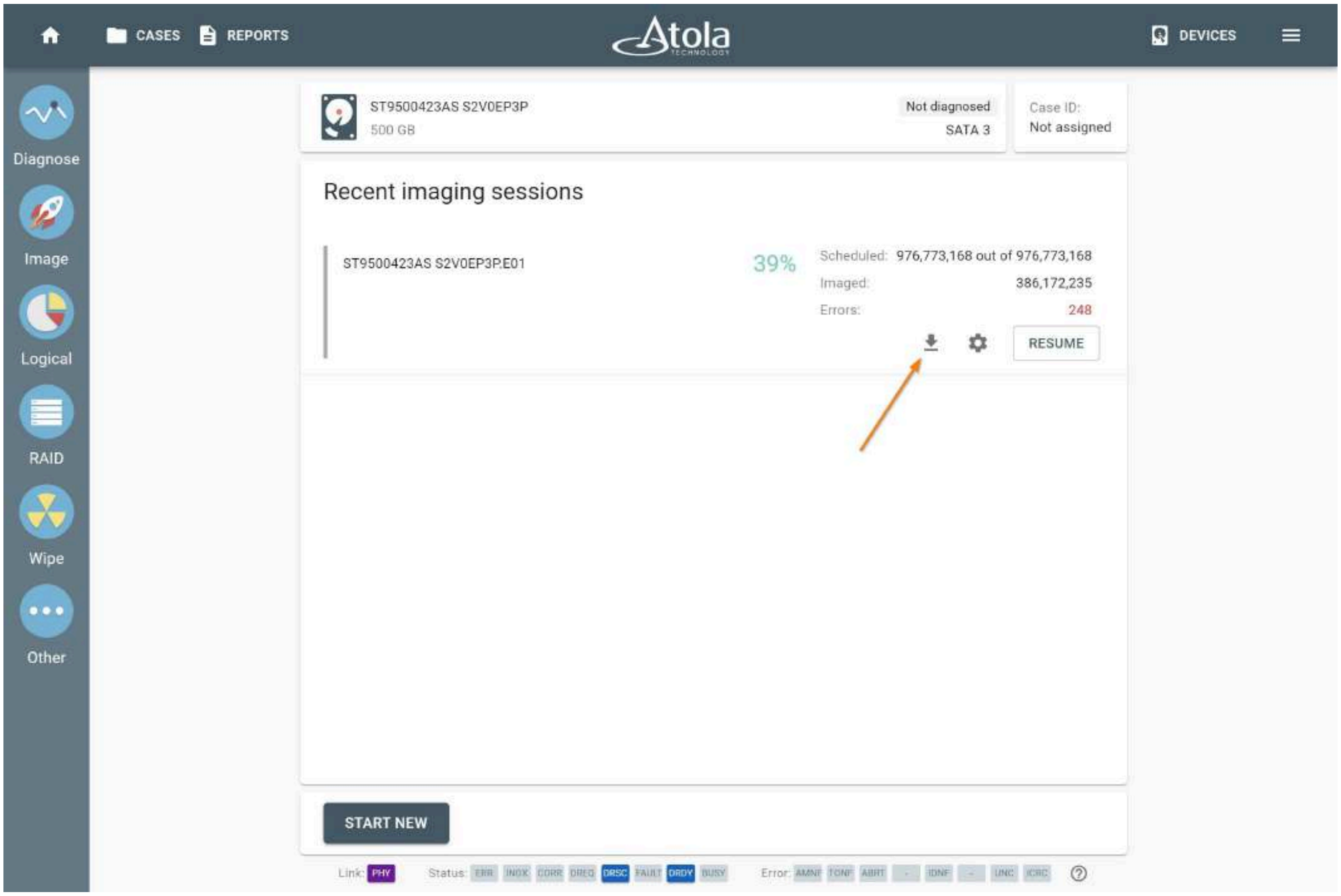
To learn how to unclip HPA/AMA, read Unclip or change HPA, DCO, AMA limitations in our manual.

Exporting sector lists from an imaging session

When an imaging session is completed or paused, it is possible to see its summary in the **Imaging sessions summary** page. Now there is also a possibility to export lists which would clearly indicate which of the sectors on the source drive have been successfully imaged, which have not (if any), and which of the sectors contained errors.

To export such list:

1. Go to **Image** and select the source drive.
2. In the session summary, click the **Export** icon.



ST9500423AS S2V0EP3P
500 GB
Not diagnosed
SATA 3
Case ID:
Not assigned

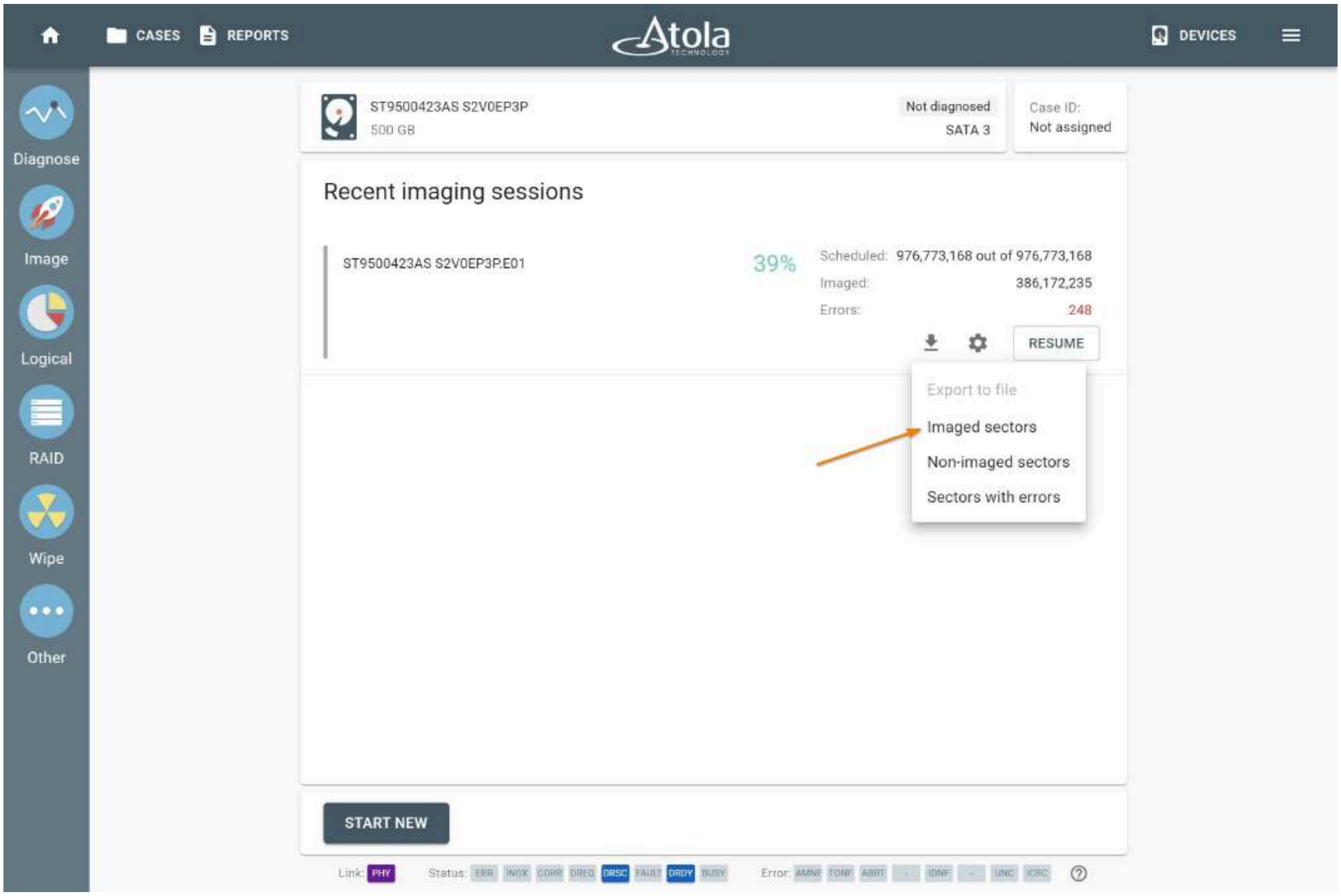
Recent imaging sessions

ST9500423AS S2V0EP3P.E01
39%
Scheduled: 976,773,168 out of 976,773,168
Imaged: 386,172,235
Errors: 248

RESUME
START NEW
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

The Export icon in the session summary.

3. Select the sectors you are interested in (for example, **Imaged sectors**).


CASES
REPORTS
Atola
TECHNOLOGY
DEVICES
Diagnose
Image
Logical
RAID
Wipe
Other
START NEW
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF T0NF ABRT - IDNF - UNC ICRC

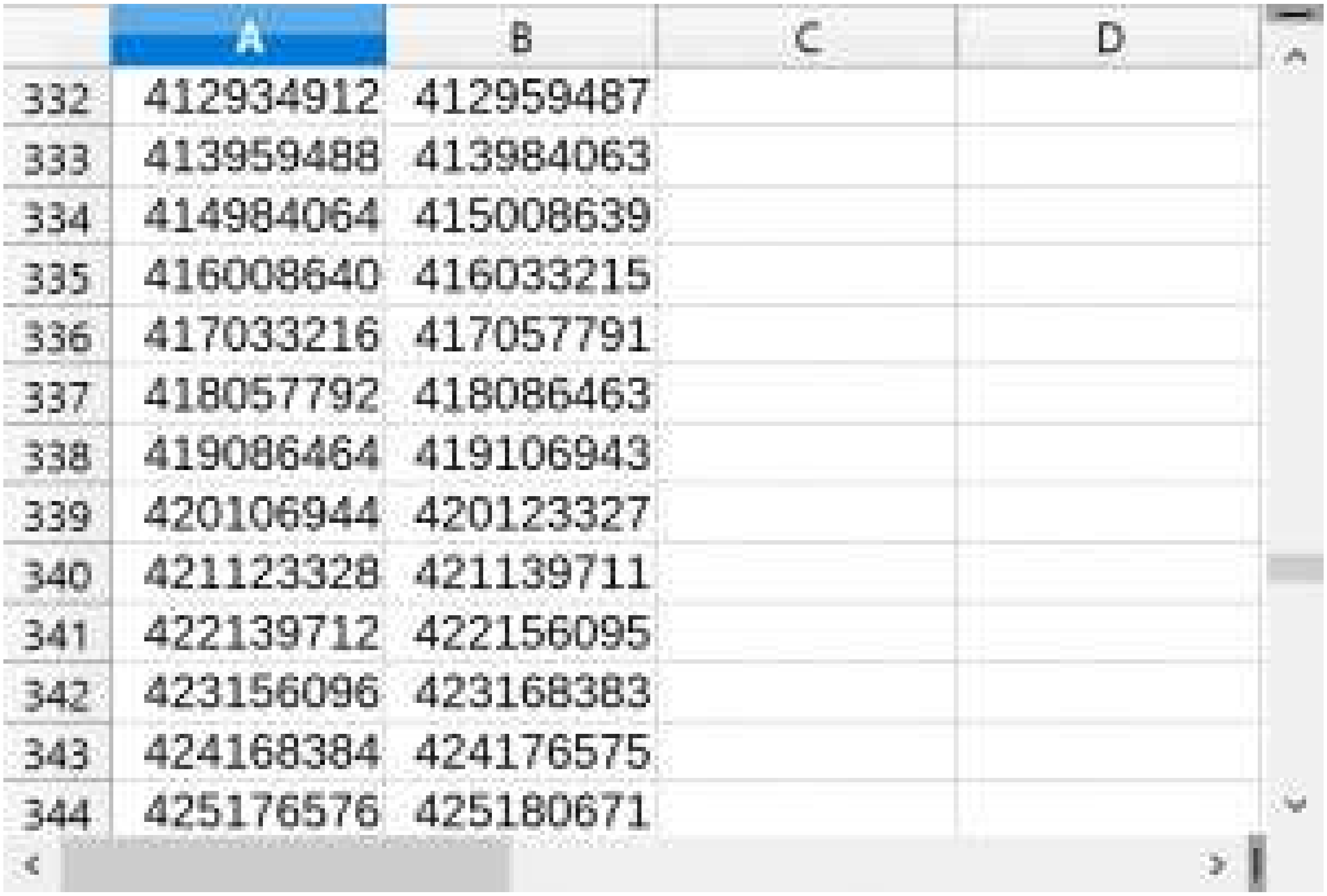
ST9500423AS S2V0EP3P
500 GB
Not diagnosed
SATA 3
Case ID:
Not assigned

Recent imaging sessions

ST9500423AS S2V0EP3P.E01
39%
Scheduled: 976,773,168 out of 976,773,168
Imaged: 386,172,235
Errors: 248

Selecting the type of sectors.

4. Save the downloaded .csv file. This file shows the ranges of imaged sectors:



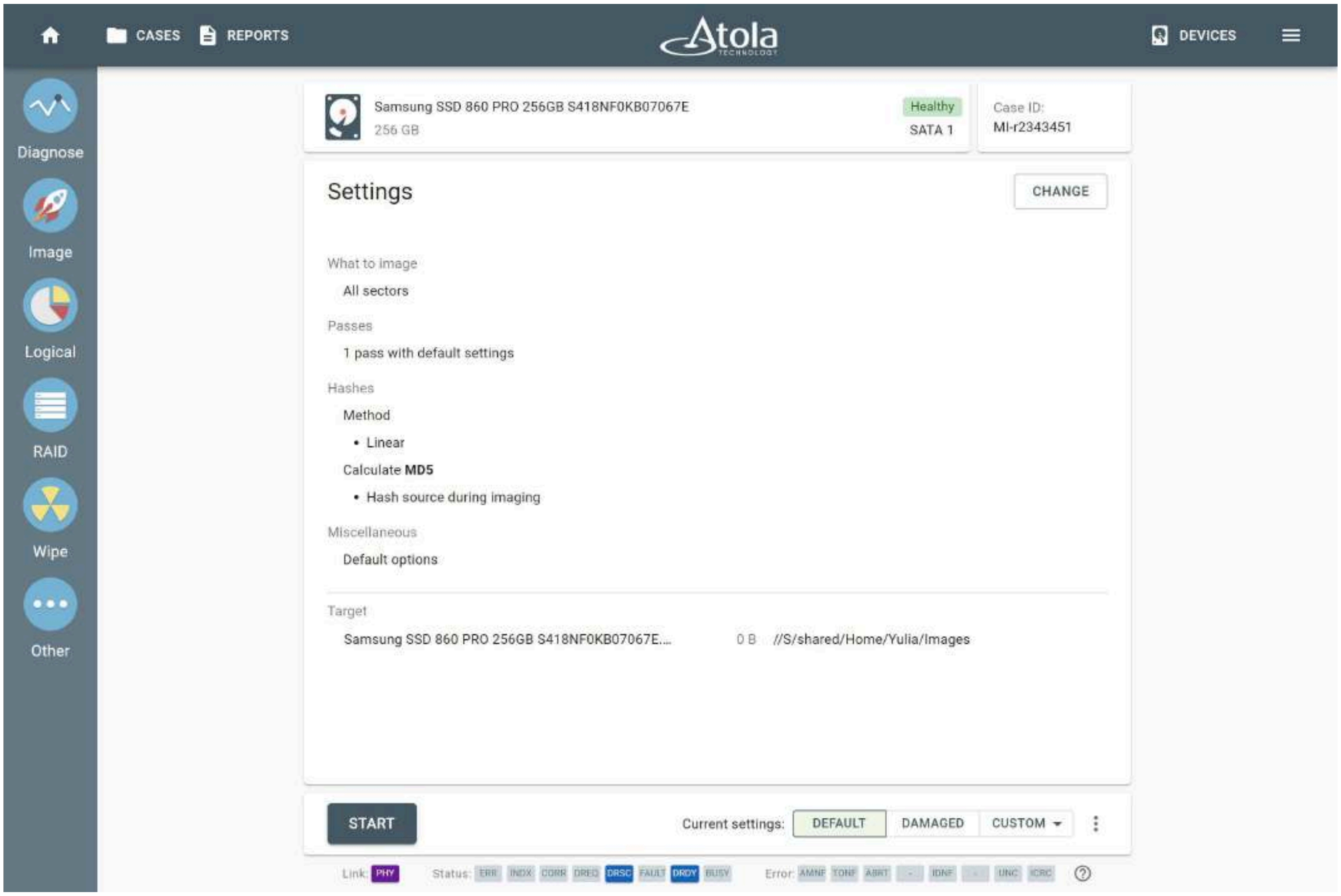
	A	B	C	D
332	412934912	412959487		
333	413959488	413984063		
334	414984064	415008639		
335	416008640	416033215		
336	417033216	417057791		
337	418057792	418086463		
338	419086464	419106943		
339	420106944	420123327		
340	421123328	421139711		
341	422139712	422156095		
342	423156096	423168383		
343	424168384	424176575		
344	425176576	425180671		

Should an imaging session be completed, the list of non-imaged sectors will be blank.

Imaging presets

For examiners who need to ensure they are using specific imaging settings for certain types of drives or cases, TaskForce 2 allows creating different presets for easy, one-click switching to a specific imaging routine. Presets also allow these specific imaging settings to be shared with colleagues who use another TaskForce 2 by exporting presets from one device and importing them onto another one.

TaskForce 2 has two presets called *Default* and *Damaged* recommended for healthy and faulty drives respectively.



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 1

Case ID:
MI-r2343451

Settings

What to image
All sectors

Passes
1 pass with default settings

Hashes
Method
- Linear

Calculate **MD5**
- Hash source during imaging

Miscellaneous
Default options

Target
Samsung SSD 860 PRO 256GB S418NF0KB07067E... 0 B //S/shared/Home/Yulia/Images

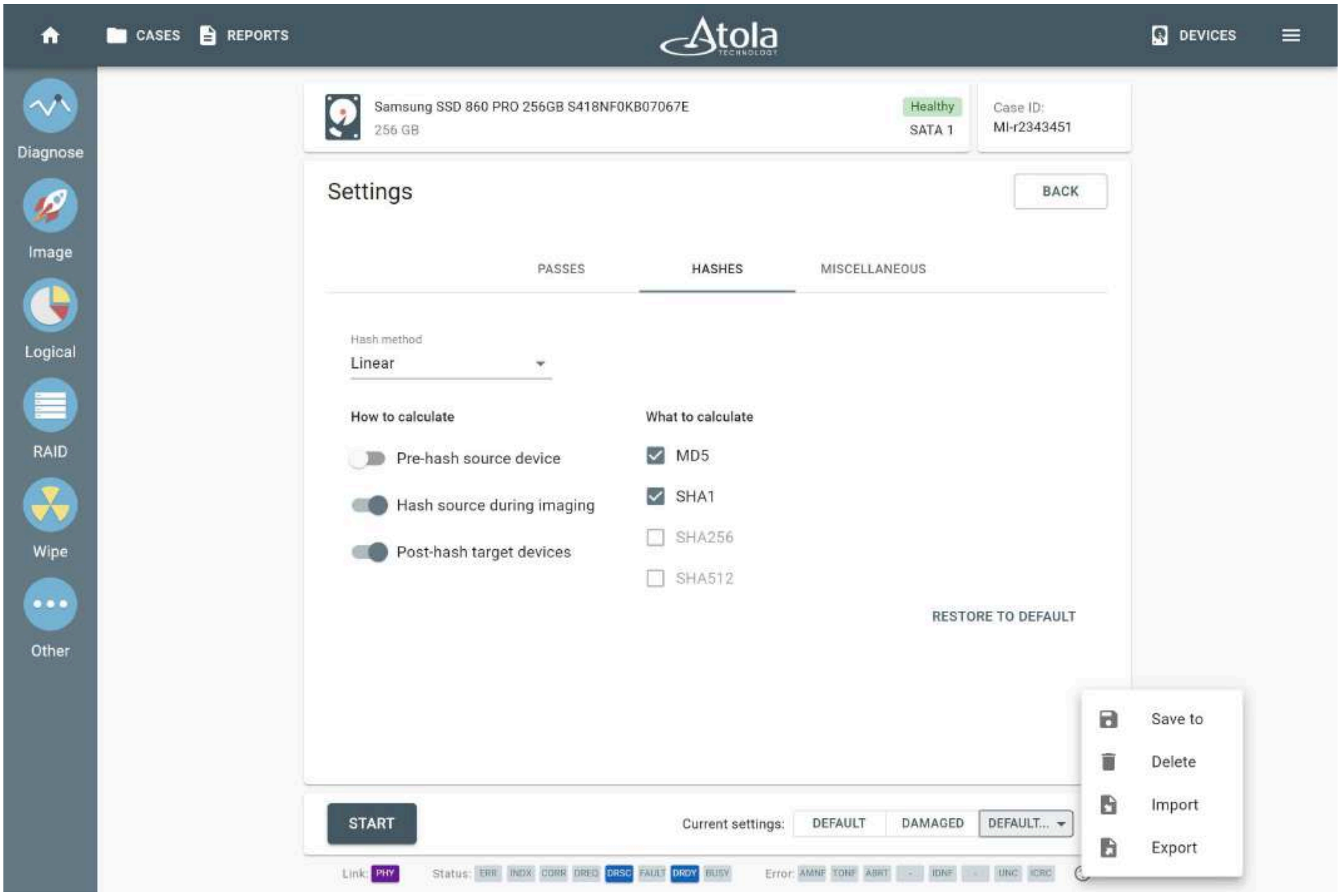
Current settings: DEFAULT

Default presets.

Manage custom presets

To create a custom preset:

1. Go to **Image** and select source and target devices.
2. On the **Imaging settings** page, click **Change**.
3. Change the imaging settings.
4. Click the three-dot icon in the bottom right corner and choose **Save to**.
5. In the dialog window, enter the name of the preset and click **Save**.



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 1

Case ID:
MI-r2343451

Settings

Hash method
Linear

How to calculate

- Pre-hash source device (off)
- Hash source during imaging (on)
- Post-hash target devices (on)

What to calculate

- ☑ MD5
- ☑ SHA1
- ☐ SHA256
- ☐ SHA512

Current settings: DEFAULT DAMAGED DEFAULT...

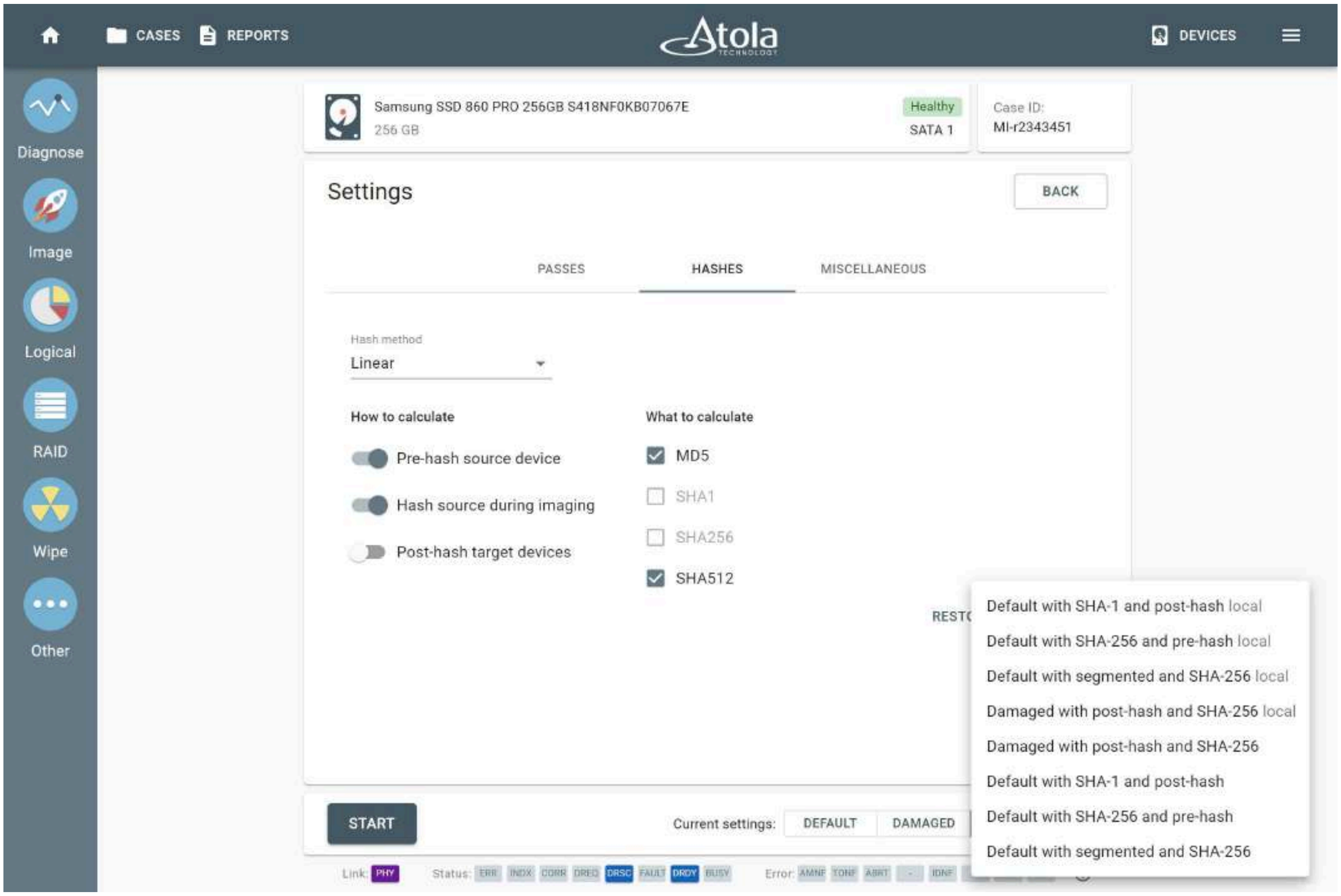
Saving a preset.

Once you have saved a preset, they are stored in TaskForce's work folder and can be used by other operators using the same imager. They can find the presets you created under the **Custom** button.

The Chrome browser of the user who created a preset, saves a copy of the preset locally. When this user opens the **Custom** menu, both presets are displayed:

- one is the preset saved in TaskForce's work folder,
- another one is the local copy.

If one becomes redundant, it can be easily deleted.



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB
Healthy
SATA 1

Case ID:
MI-r2343451

Settings

Hash method: Linear

How to calculate
- ● Pre-hash source device
- ● Hash source during imaging
- ○ Post-hash target devices

What to calculate
- ☑ MD5
- ☐ SHA1
- ☐ SHA256
- ☑ SHA512

Current settings:

- Default with SHA-1 and post-hash local
- Default with SHA-256 and pre-hash local
- Default with segmented and SHA-256 local
- Damaged with post-hash and SHA-256 local
- Damaged with post-hash and SHA-256
- Default with SHA-1 and post-hash
- Default with SHA-256 and pre-hash
- Default with segmented and SHA-256

All custom presets.

To delete a preset:

1. Select the preset in the **Custom** menu.
2. Go to the three-dot menu in the bottom-right corner and click **Delete**.

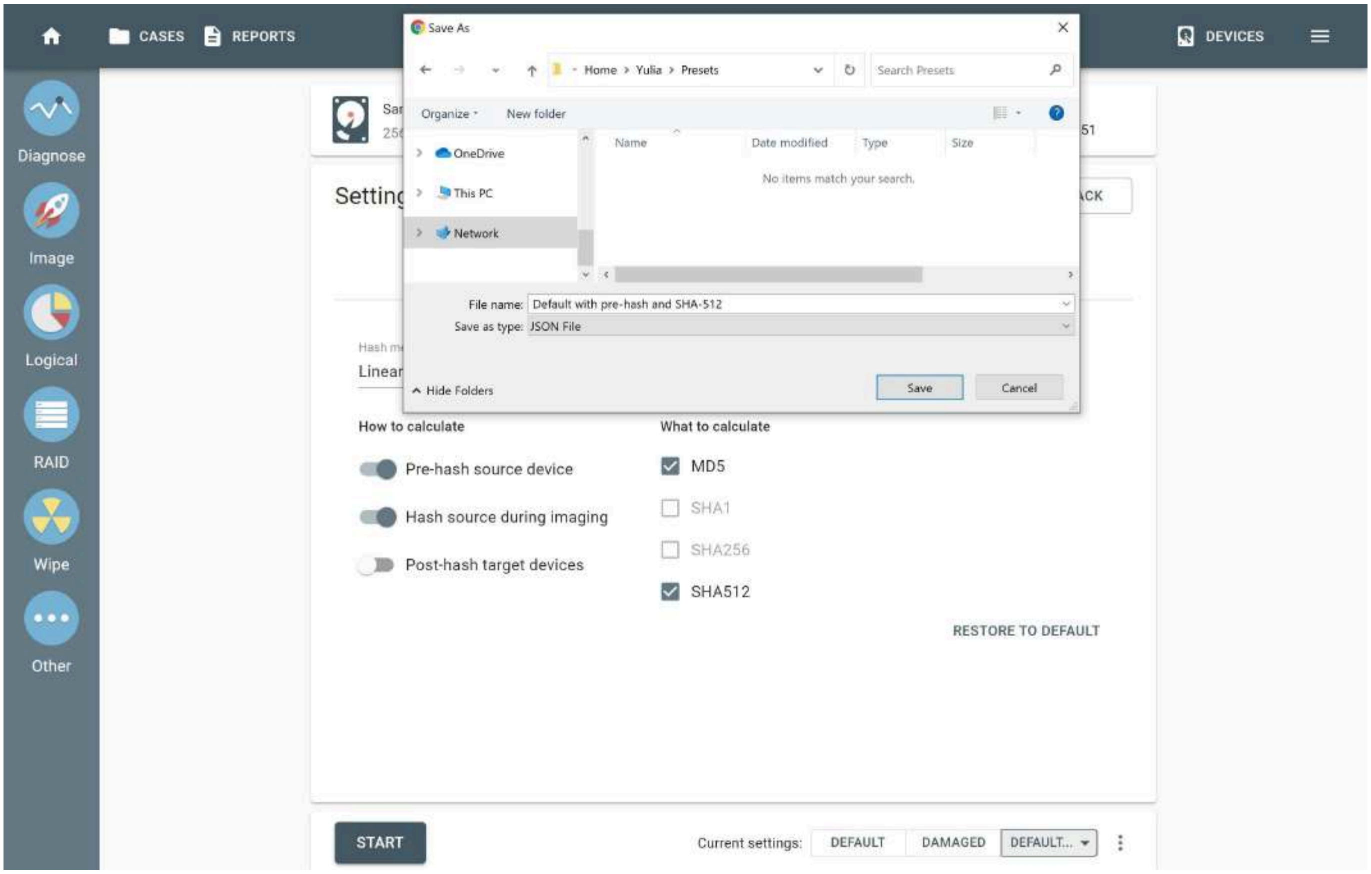
Share presets with another TaskForce

Once you have created your custom presets, you can share them with colleagues who use another TaskForce imager.

To export a preset:

1. Select the preset from the **Custom** menu.
2. Click the three-dot icon.
3. Click **Export**.

The preset will be downloaded in .json format.



File name: Default with pre-hash and SHA-512

Save as type: JSON File

How to calculate

- ● Pre-hash source device
- ● Hash source during imaging
- ○ Post-hash target devices

What to calculate

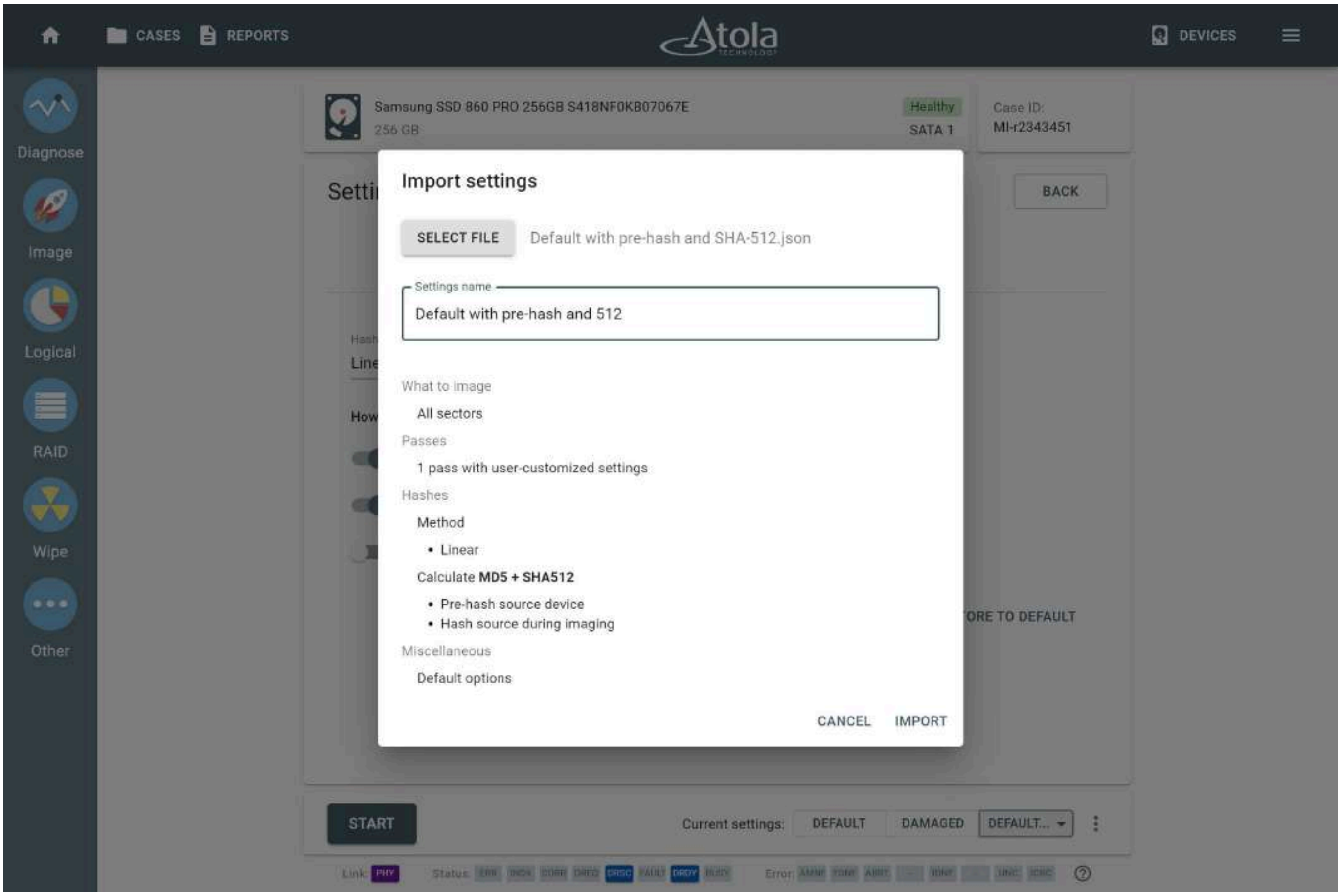
- ☑ MD5
- □ SHA1
- □ SHA256
- ☑ SHA512

Current settings: DEFAULT DAMAGED DEFAULT...

Exporting a preset.

To import a preset:

1. Click the three-dot icon.
2. Click **Import**.
3. In the **Import settings** window, click **Select file**.
4. Find the file in the file selector and click **Open**.
5. Double-check the preset and click **Import**.



Import settings

SELECT FILE Default with pre-hash and SHA-512.json

Settings name: Default with pre-hash and 512

What to image
All sectors

Passes
1 pass with user-customized settings

Hashes
Method
- Linear

Calculate **MD5 + SHA512**
- Pre-hash source device
- Hash source during imaging

Miscellaneous
Default options

CANCEL IMPORT

Importing a preset.

After this import, the preset can be found in the **Custom** menu.

Imaging a drive with a damaged head

The diagnostics module, selective head imaging and multipass imaging algorithm allow Atola TaskForce 2 to handle a drive with damaged heads gently and effectively. All these techniques help minimize the risk of losing more data on the working part of the head stack.

Diagnose first

The built-in diagnostics module of TaskForce 2 automatically checks all major subsystems of the evidence drive: circuit board, heads, media surface, firmware and file system.

A diagnostics report provides detailed information about the heads. In addition, it offers recommendations for the optimal imaging strategy for your damaged hard drive.

Diagnostics completed

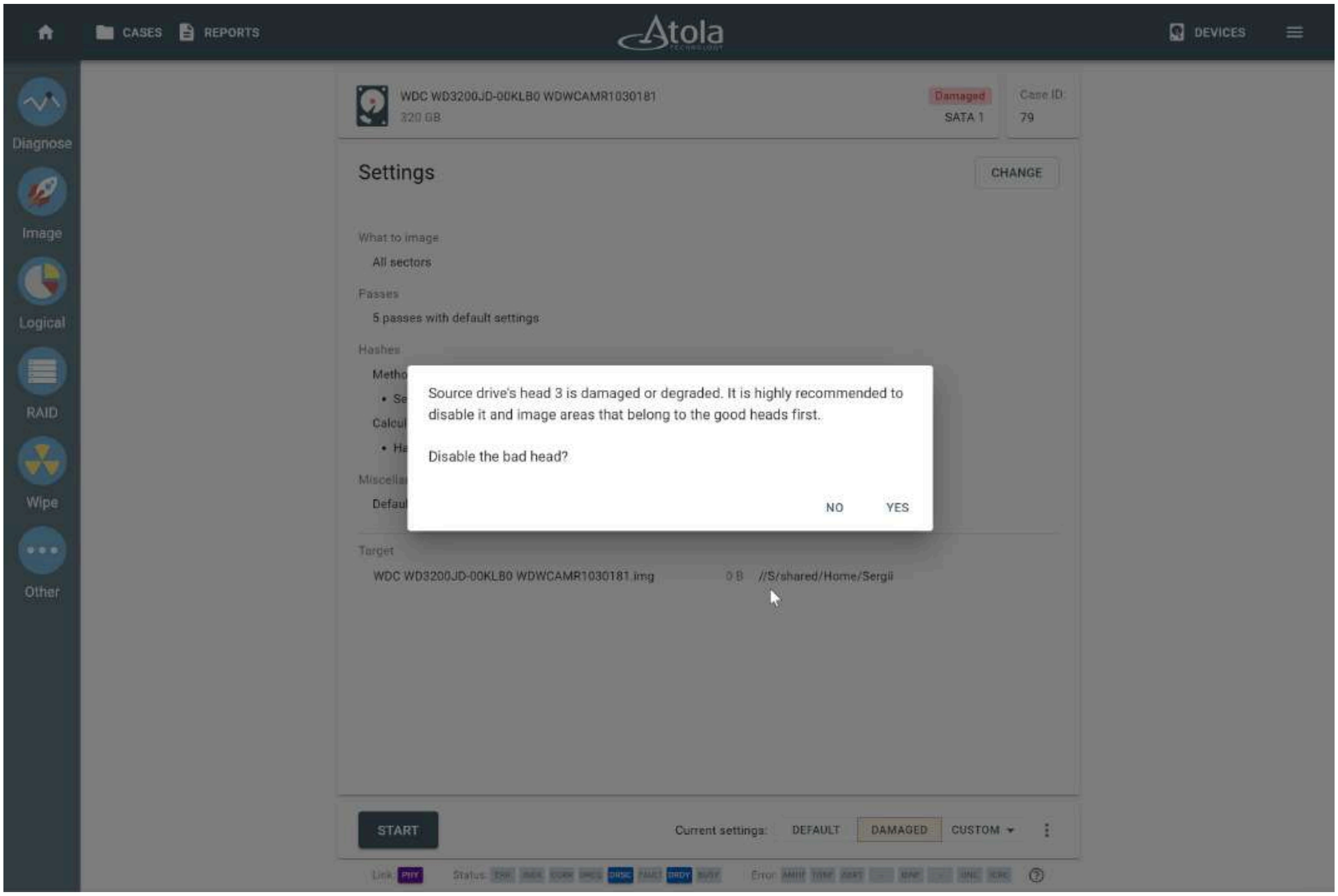
PDF

The above diagnostics report informs the operator that the drive’s hardware has major issues and points to defects in the media and a damaged head (Head#3). The report contains a recommendation to disable the damaged head in the imaging settings.

Selective head imaging

Atola engineers recommend that the good heads are imaged first. To do that:

1. Go to **Image**.
2. Select your source and target devices.
3. Click **Continue**.
4. If a head was identified as damaged during the diagnostics, at this stage TaskForce 2 shows a dialog prompting you to disable the damaged head. To confirm that the head should be automatically disabled for the subsequent imaging session, click **YES**.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
Damaged
SATA 1
Case ID: 79

Settings

What to image
All sectors

Passes
5 passes with default settings

Source drive's head 3 is damaged or degraded. It is highly recommended to disable it and image areas that belong to the good heads first.

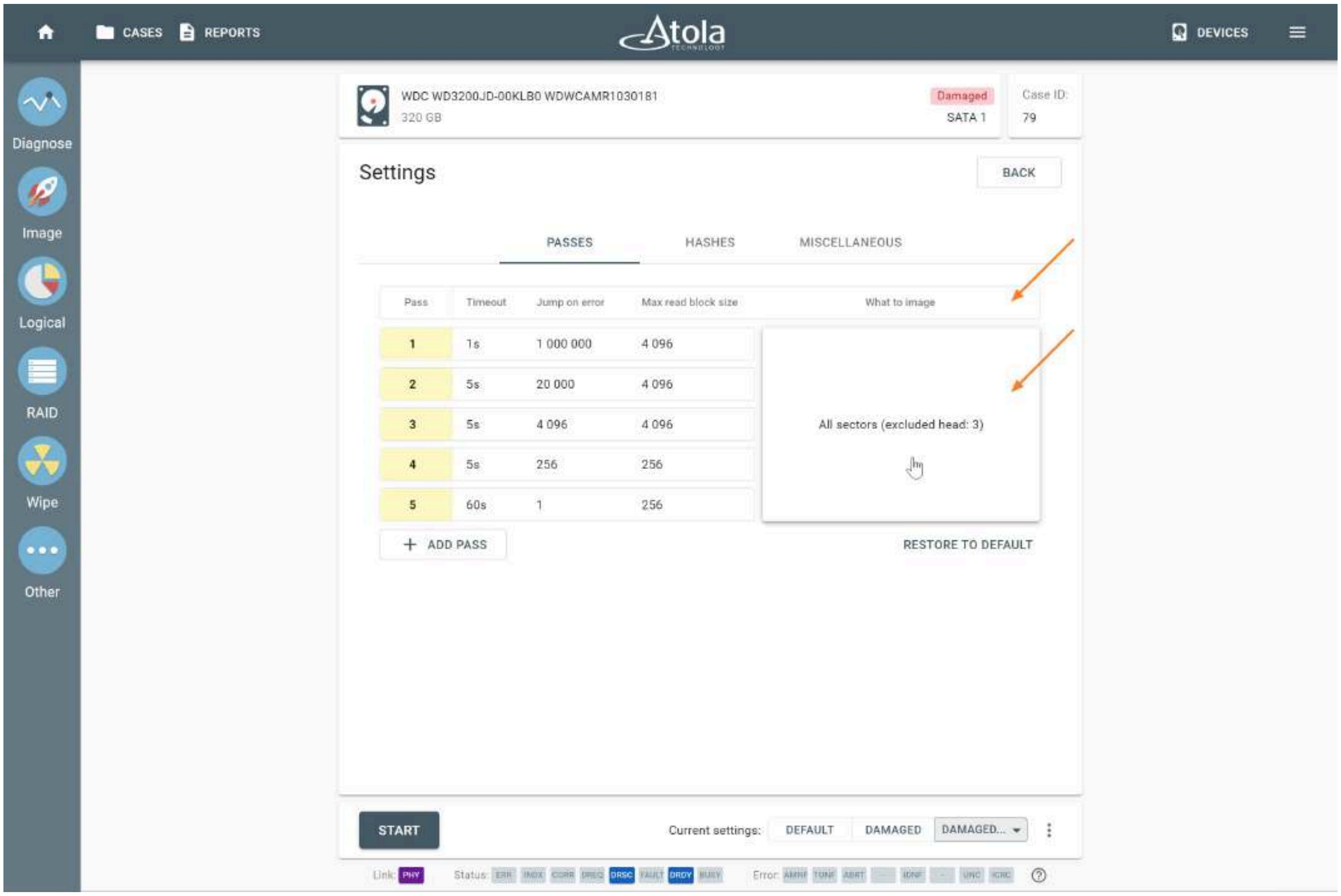
Disable the bad head?

Target
WDC WD3200JD-00KLB0 WDWCAMR1030181.img 0 B //S/shared/Home/Sergii

Current settings: DAMAGED

Alternatively, the damaged head can be disabled in the imaging settings:

1. On the **Imaging settings** page, click **Change** to adjust the settings for your imaging session.
2. In **What to image** section, click on **All sectors** to configure the selective imaging.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
Damaged
SATA 1
Case ID: 79

Settings

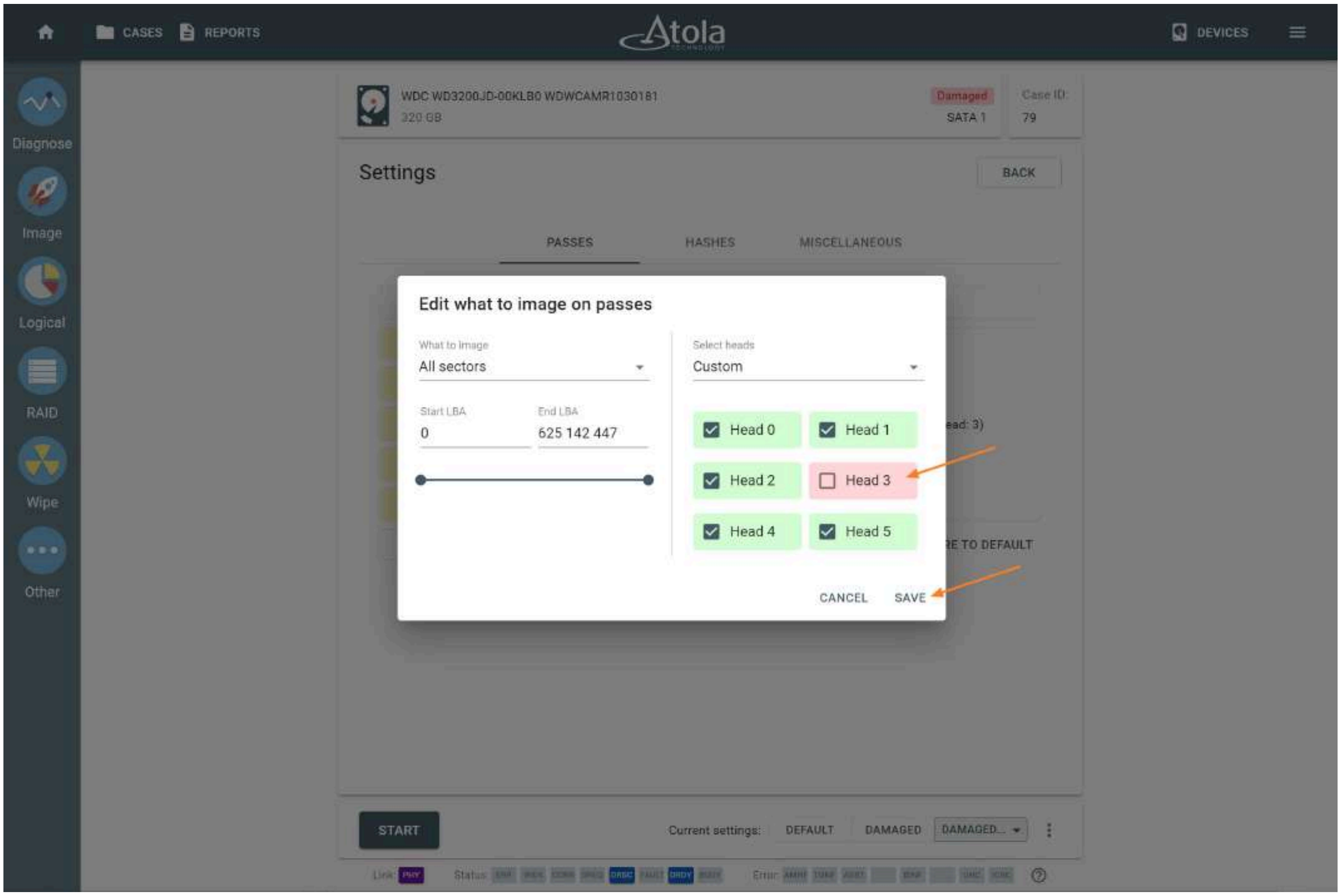
BACK

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	All sectors (excluded head: 3)
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

Current settings: DEFAULT DAMAGED DAMAGED...

3. Unselect the damaged head and click **Save**.

4. To launch your imaging session, click **Start**.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
Damaged
SATA 1
Case ID:
79

Settings

Edit what to image on passes

What to image: All sectors

Start LBA: 0

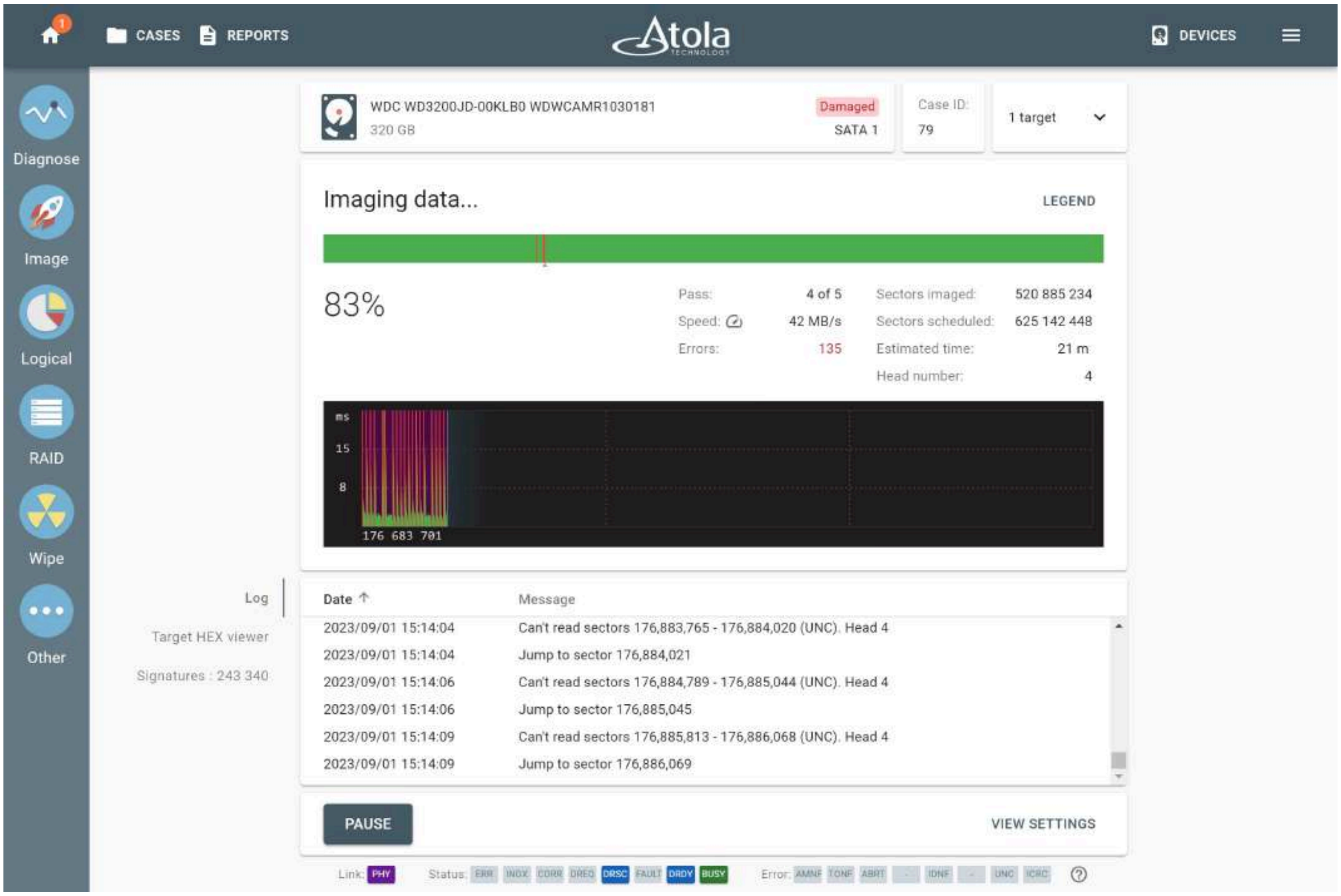
End LBA: 625 142 447

Select heads: Custom

☑ Head 0 ☑ Head 1
☑ Head 2 □ Head 3
☑ Head 4 ☑ Head 5

Multipass imaging algorithm

As you can see in the screenshot below, some errors were found in the course of imaging on the space of the drive that is read with the Head#4. It is common for a drive with a bad head to also contain errors on the platters that are read with other heads.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
SATA 1
Case ID: 79

Imaging data...

83%

Pass: 4 of 5
Speed: 42 MB/s
Errors: 135
Sectors imaged: 520 885 234
Sectors scheduled: 625 142 448
Estimated time: 21 m
Head number: 4

Signatures : 243 340

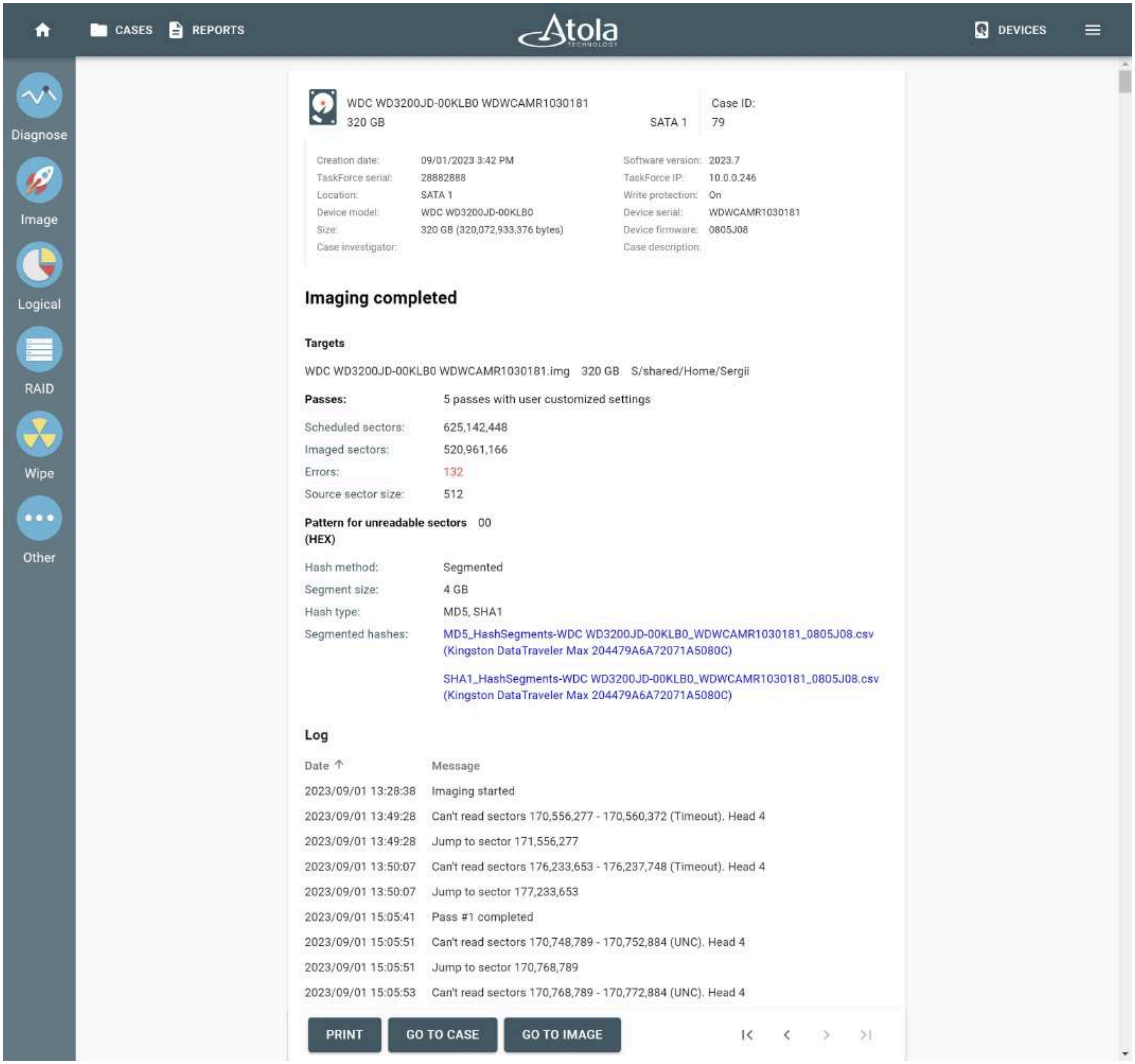
```
Date ↑                Message
2023/09/01 15:14:04   Can't read sectors 176,883,765 - 176,884,020 (UNC). Head 4
2023/09/01 15:14:04   Jump to sector 176,884,021
2023/09/01 15:14:06   Can't read sectors 176,884,789 - 176,885,044 (UNC). Head 4
2023/09/01 15:14:06   Jump to sector 176,885,045
2023/09/01 15:14:09   Can't read sectors 176,885,813 - 176,886,068 (UNC). Head 4
2023/09/01 15:14:09   Jump to sector 176,886,069
```

TaskForce 2 uses its multipass imaging algorithm when encountering a bad sector that belongs to a good head. It allows handling errors and retrieving data from some of the bad sectors. For as long as it is possible to read data from the sector or block of sectors within the specified pass timeout, TaskForce 2 will be able to image this data.

Having completed imaging from the good heads, the system pauses the session and produces a detailed imaging report with a log of all actions performed during the imaging session.

TaskForce 2 allows editing settings of all unstarted imaging passes, adding or removing passes, etc. So if later you think you may be able to retrieve important data with Head#4, you can add another pass and configure the settings of the new pass accordingly.

TaskForce 2 automatically inserts and launches an additional imaging pass after you click **Resume** on the pause session. The new pass will include all non-imaged sectors.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
SATA 1
Case ID:
79

Creation date:	09/01/2023 3:42 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	WDC WD3200JD-00KLB0	Device serial:	WDWCAMR1030181
Size:	320 GB (320,072,933,376 bytes)	Device firmware:	0805J08
Case investigator:		Case description:	

Imaging completed

Targets

WDC WD3200JD-00KLB0 WDWCAMR1030181.img 320 GB S/shared/Home/Sergii

Passes:	5 passes with user customized settings
Scheduled sectors:	625,142,448
Imaged sectors:	520,961,166
Errors:	132
Source sector size:	512
Pattern for unreadable sectors (HEX)	00
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5, SHA1
Segmented hashes:	MD5_HashSegments-WDC WD3200JD-00KLB0_WDWCAMR1030181_0805J08.csv (Kingston DataTraveler Max 204479A6A72071A5080C) SHA1_HashSegments-WDC WD3200JD-00KLB0_WDWCAMR1030181_0805J08.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

Log

```
Date ↑               Message
2023/09/01 13:28:38  Imaging started
2023/09/01 13:49:28  Can't read sectors 170,556,277 - 170,560,372 (Timeout). Head 4
2023/09/01 13:49:28  Jump to sector 171,556,277
2023/09/01 13:50:07  Can't read sectors 176,233,653 - 176,237,748 (Timeout). Head 4
2023/09/01 13:50:07  Jump to sector 177,233,653
2023/09/01 15:05:41  Pass #1 completed
2023/09/01 15:05:51  Can't read sectors 170,748,789 - 170,752,884 (UNC). Head 4
2023/09/01 15:05:51  Jump to sector 170,768,789
2023/09/01 15:05:53  Can't read sectors 170,768,789 - 170,772,884 (UNC). Head 4
```

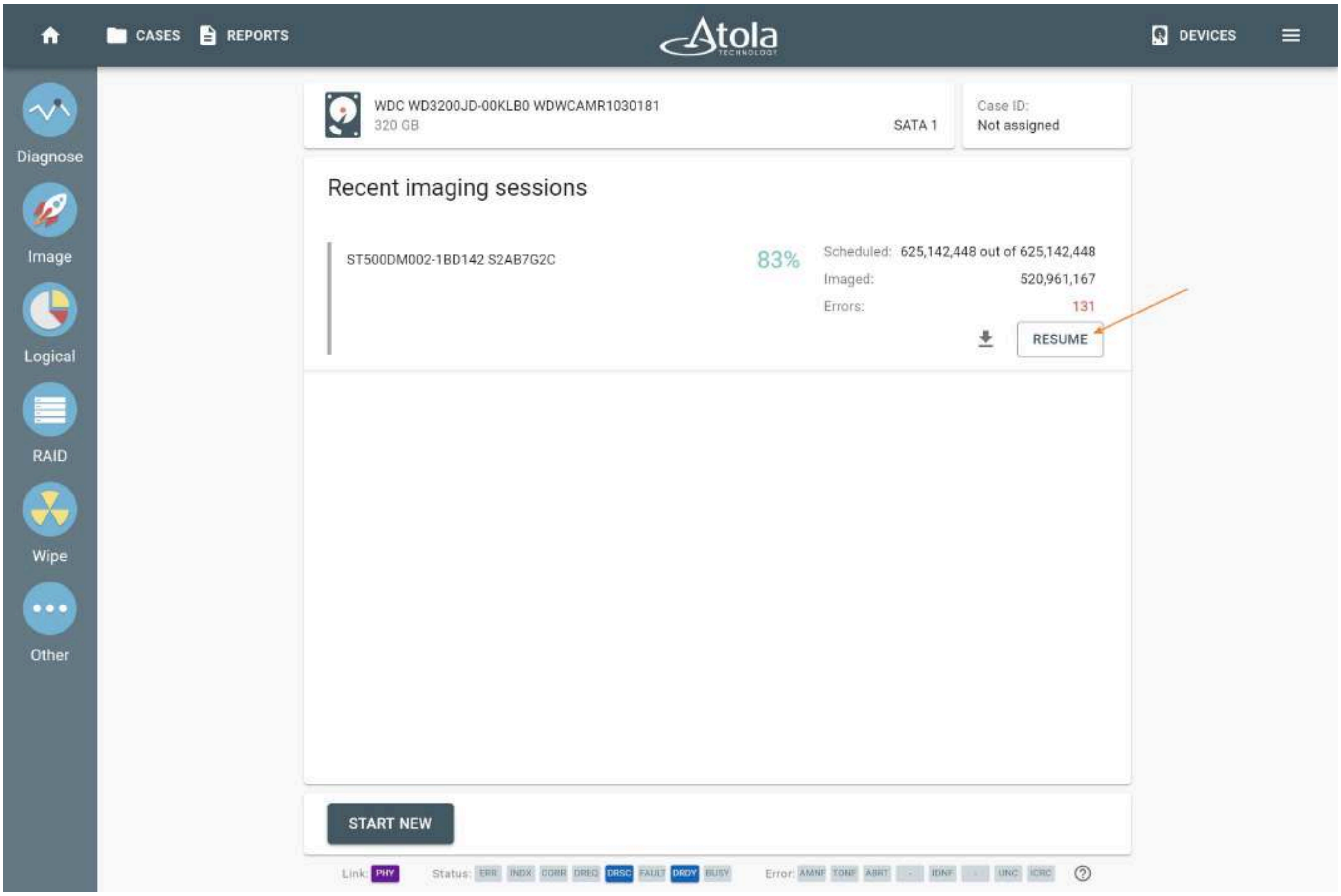
TaskForce 2 automatically creates reports for every single action applied to each device connected to it. The reports are stored in the case management system.

Working with a bad head

After you successfully retrieved data from the good heads, you have two options:

- To replace the head stack before you get down to imaging of the remaining data. You should be aware of the risk, however, that data on the drive can become unreadable due to head stack replacement.
- To attempt imaging data with the *Degraded* or *Damaged* head.

To image the unselected bad head, simply click **Resume**.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
SATA 1

Case ID:
Not assigned

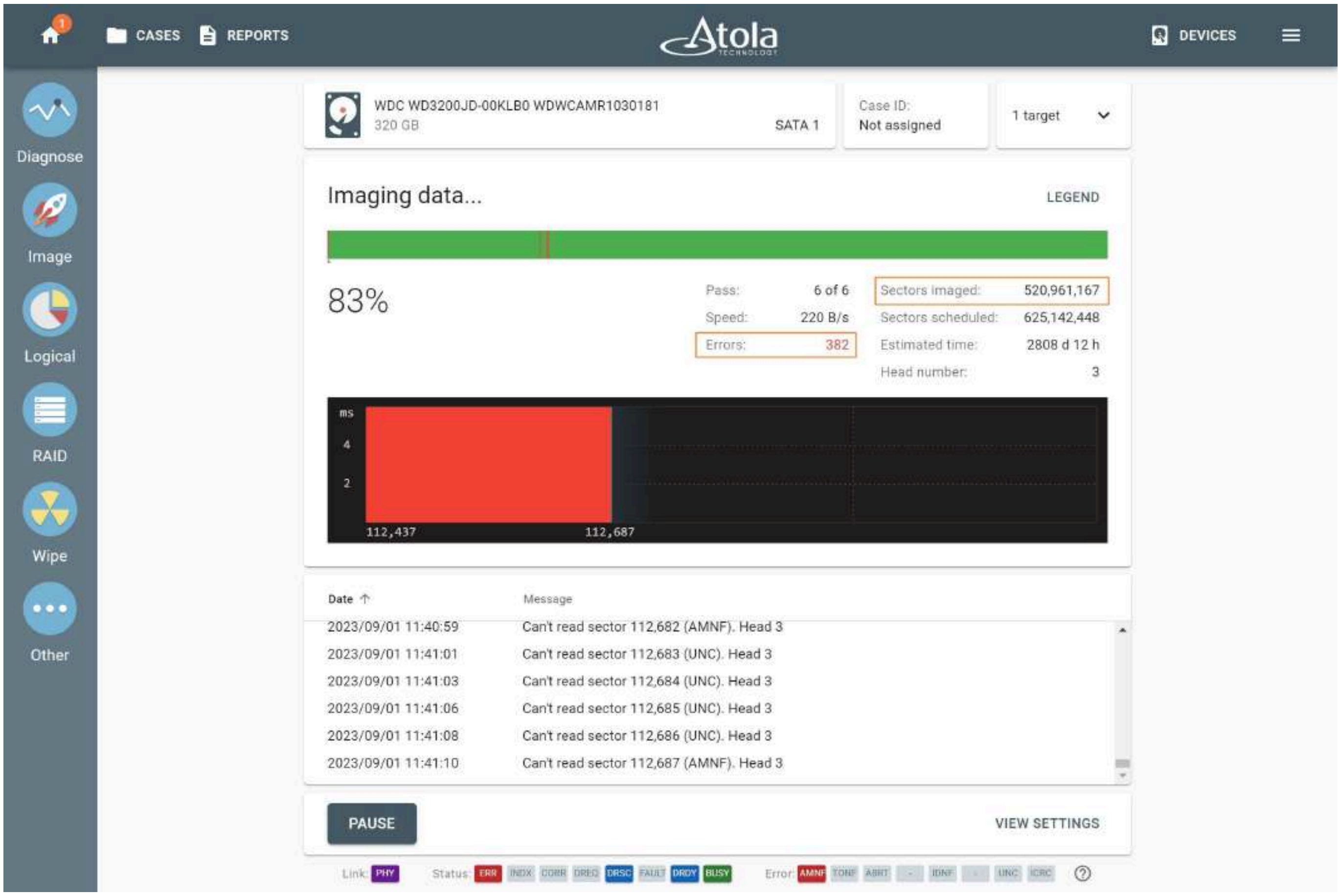
Recent imaging sessions

ST500DM002-1BD142 S2AB7G2C

83%

Scheduled: 625,142,448 out of 625,142,448
Imaged: 520,961,167
Errors: 131

TaskForce 2 resumes the imaging session to focus on the area that belongs to the damaged head.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
SATA 1

Case ID: Not assigned

1 target

Imaging data...

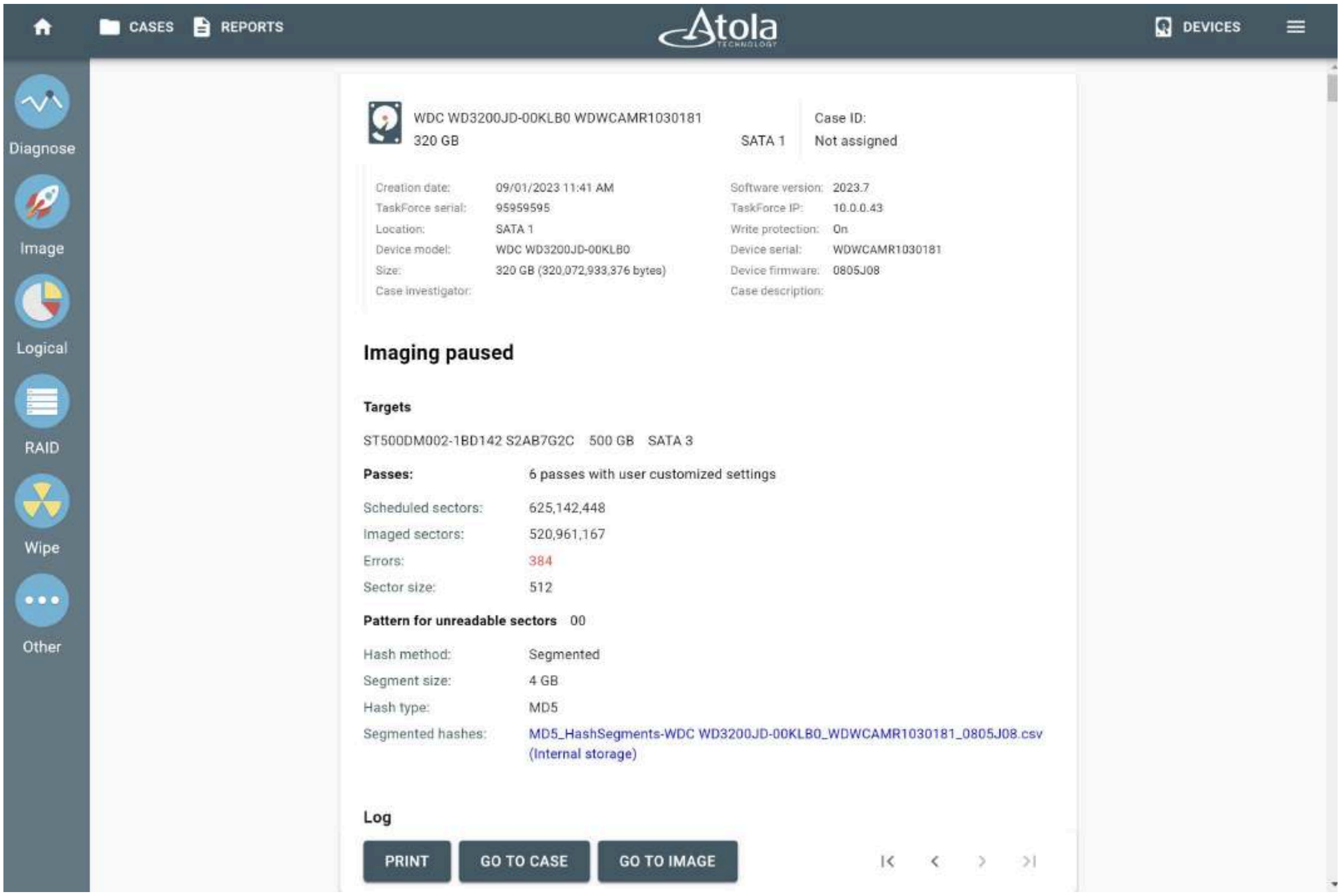
83%

Pass: 6 of 6
Speed: 220 B/s
Errors: 382

Sectors imaged: 520,961,167
Sectors scheduled: 625,142,448
Estimated time: 2808 d 12 h
Head number: 3

```
Date                  Message
2023/09/01 11:40:59   Can't read sector 112,682 (AMNF). Head 3
2023/09/01 11:41:01   Can't read sector 112,683 (UNC). Head 3
2023/09/01 11:41:03   Can't read sector 112,684 (UNC). Head 3
2023/09/01 11:41:06   Can't read sector 112,685 (UNC). Head 3
2023/09/01 11:41:08   Can't read sector 112,686 (UNC). Head 3
2023/09/01 11:41:10   Can't read sector 112,687 (AMNF). Head 3
```

If the number of errors keeps growing, while the number of the imaged sectors remains unchanged, pause your imaging session and power down the drive because the head seems to be completely inoperable.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
SATA 1

Case ID:
Not assigned

Creation date:	09/01/2023 11:41 AM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.43
Location:	SATA 1	Write protection:	On
Device model:	WDC WD3200JD-00KLB0	Device serial:	WDWCAMR1030181
Size:	320 GB (320,072,933,376 bytes)	Device firmware:	0805J08
Case investigator:		Case description:	

Imaging paused

Targets

ST500DM002-1BD142 S2AB7G2C 500 GB SATA 3

Passes:	6 passes with user customized settings
Scheduled sectors:	625,142,448
Imaged sectors:	520,961,167
Errors:	384
Sector size:	512

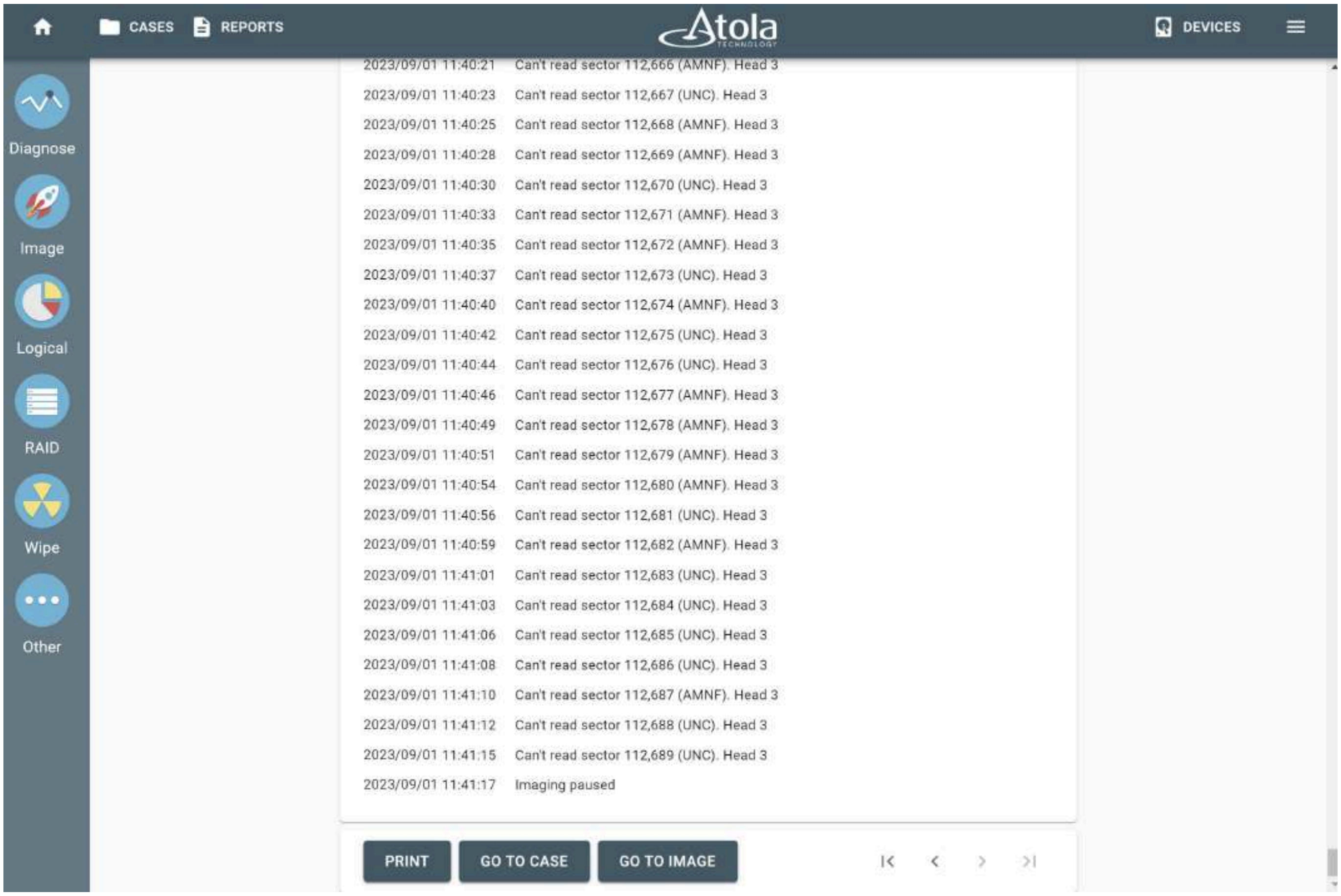
Pattern for unreadable sectors 00

Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-WDC WD3200JD-00KLB0_WDWCAMR1030181_0805J08.csv (Internal storage)

Log

In the **Imaging report** above, you can see that TaskForce 2 imaged 520,961,167 sectors out of 625,142,448, having extracted as much data from good heads as was possible with the default settings.

For more details scroll the report down to check the **Log**:



```
2023/09/01 11:40:21   Can't read sector 112,666 (AMNF). Head 3
2023/09/01 11:40:23   Can't read sector 112,667 (UNC). Head 3
2023/09/01 11:40:25   Can't read sector 112,668 (AMNF). Head 3
2023/09/01 11:40:28   Can't read sector 112,669 (AMNF). Head 3
2023/09/01 11:40:30   Can't read sector 112,670 (UNC). Head 3
2023/09/01 11:40:33   Can't read sector 112,671 (AMNF). Head 3
2023/09/01 11:40:35   Can't read sector 112,672 (AMNF). Head 3
2023/09/01 11:40:37   Can't read sector 112,673 (UNC). Head 3
2023/09/01 11:40:40   Can't read sector 112,674 (AMNF). Head 3
2023/09/01 11:40:42   Can't read sector 112,675 (UNC). Head 3
2023/09/01 11:40:44   Can't read sector 112,676 (UNC). Head 3
2023/09/01 11:40:46   Can't read sector 112,677 (AMNF). Head 3
2023/09/01 11:40:49   Can't read sector 112,678 (AMNF). Head 3
2023/09/01 11:40:51   Can't read sector 112,679 (AMNF). Head 3
2023/09/01 11:40:54   Can't read sector 112,680 (AMNF). Head 3
2023/09/01 11:40:56   Can't read sector 112,681 (UNC). Head 3
2023/09/01 11:40:59   Can't read sector 112,682 (AMNF). Head 3
2023/09/01 11:41:01   Can't read sector 112,683 (UNC). Head 3
2023/09/01 11:41:03   Can't read sector 112,684 (UNC). Head 3
2023/09/01 11:41:06   Can't read sector 112,685 (UNC). Head 3
2023/09/01 11:41:08   Can't read sector 112,686 (UNC). Head 3
2023/09/01 11:41:10   Can't read sector 112,687 (AMNF). Head 3
2023/09/01 11:41:12   Can't read sector 112,688 (UNC). Head 3
2023/09/01 11:41:15   Can't read sector 112,689 (UNC). Head 3
2023/09/01 11:41:17   Imaging paused
```

Multipass imaging of damaged drives

Damaged media require a sophisticated imaging approach to balance out thorough data extraction with forensic units' need for expediency and careful treatment of damaged media.

Atola TaskForce has a complex imaging functionality that lets you image even physically damaged drives while avoiding causing further drive damage. You can use a predefined setting for imaging a damaged drive, or fine-tune all imaging parameters yourself.

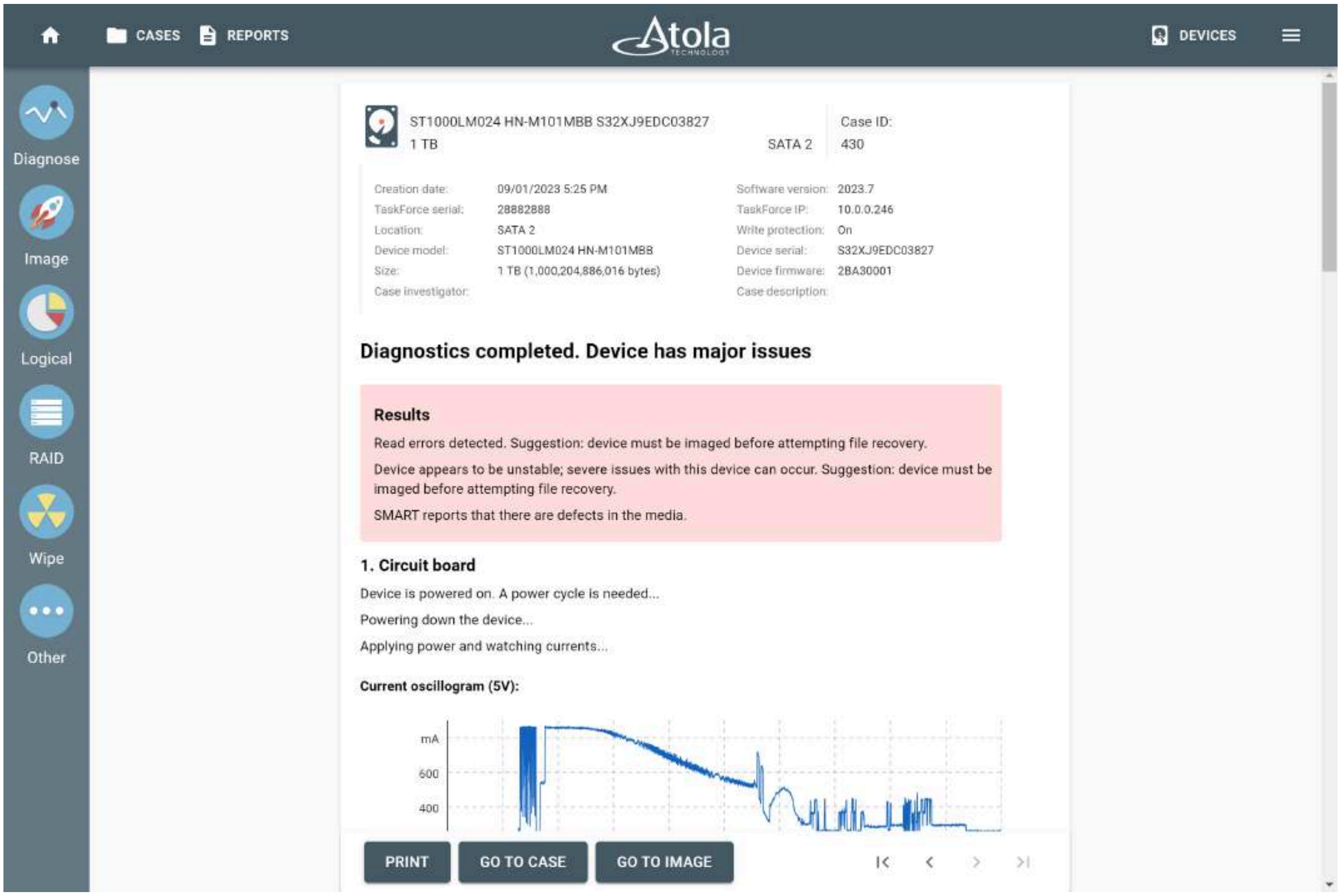
Diagnose first

Before imaging any evidence device, we strongly recommend diagnosing it.

To image an evidence drive without causing further damage to it, TaskForce is equipped with an automatic diagnostics module that evaluates the state of the drive, identifies specific errors and their location, and recommends the best approach for data acquisition.

The detailed diagnostics report contains detailed recommendations on how to acquire data from this particular drive, based on its condition.

> If Automatic Checkup detects a damaged or degraded head, disable the head in the imaging settings for the initial imaging session. For details, see Imaging drives with damaged heads.



ST1000LM024 HN-M101MBB S32XJ9EDC03827
1 TB
SATA 2
Case ID:
430

Creation date:	09/01/2023 5:25 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 2	Write protection:	On
Device model:	ST1000LM024 HN-M101MBB	Device serial:	S32XJ9EDC03827
Size:	1 TB (1,000,204,886,016 bytes)	Device firmware:	2BA30001
Case investigator:		Case description:	

Diagnostics completed. Device has major issues

Results

Read errors detected. Suggestion: device must be imaged before attempting file recovery.

Device appears to be unstable; severe issues with this device can occur. Suggestion: device must be imaged before attempting file recovery.

SMART reports that there are defects in the media.

1. Circuit board

Device is powered on. A power cycle is needed...

Powering down the device...

Applying power and watching currents...

Current oscillogram (5V):

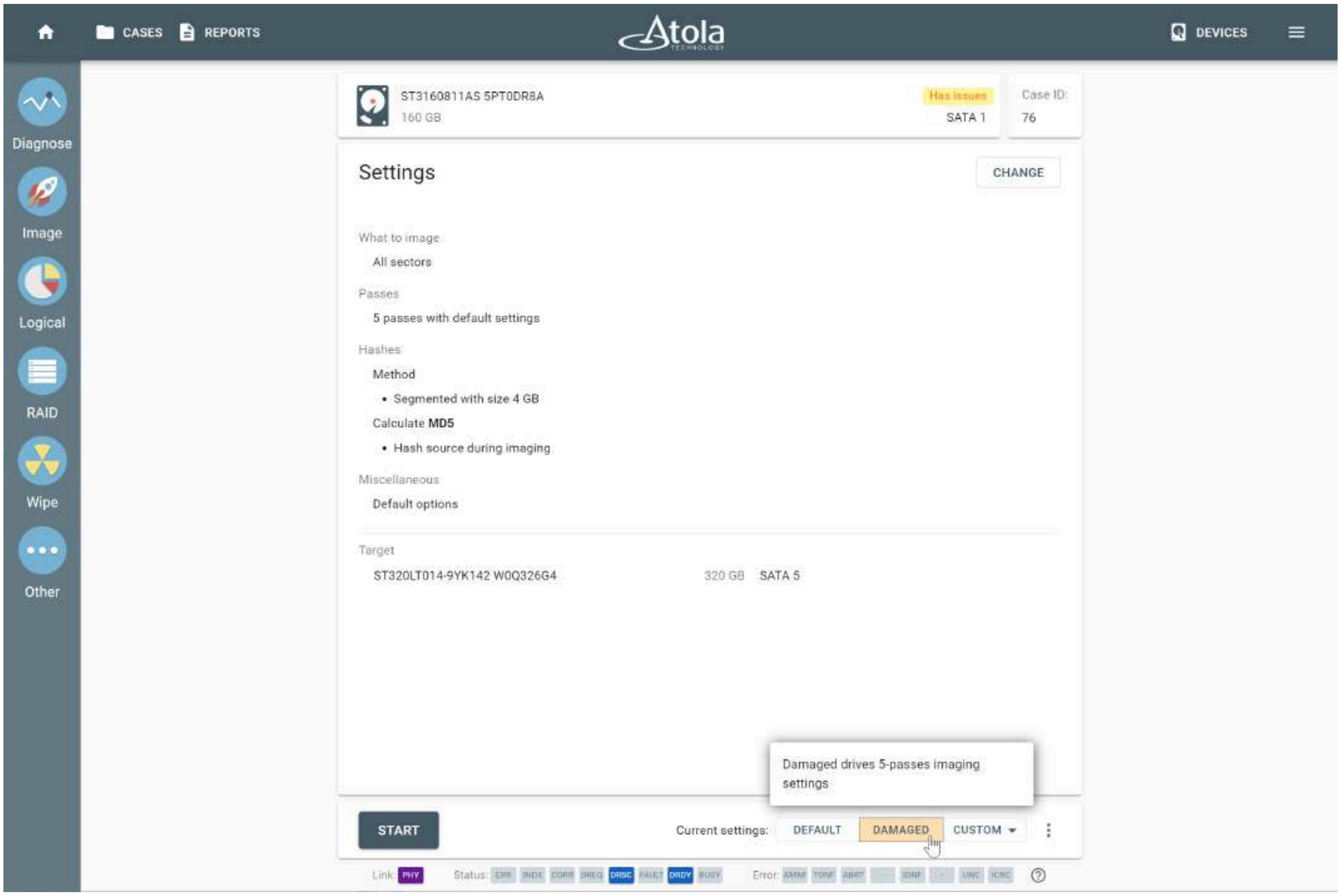
The diagnostics report for a damaged device.

Preset for imaging damaged drives

If a device has issues or is damaged, TaskForce shows the respective tag next to it and suggests using the *Damaged* preset, designed specifically for imaging faulty drives.

In this case, the *Damaged* preset is automatically selected on the **Imaging settings** screen.

The default preset for bad drives is based on our decades-long experience in the data recovery market to overcome most types of damage to the drives. That's why we suggest that you use the *Damaged* preset for bad drives unless a particular drive requires a specific imaging approach.



ST3160811AS 5PT0DR8A
160 GB
SATA 1

Case ID:
76

Settings

What to image
All sectors

Passes
5 passes with default settings

Hashes
Method
- Segmented with size 4 GB

Calculate **MD5**
- Hash source during imaging

Miscellaneous
Default options

Target
ST320LT014-9YK142 W0Q326G4 320 GB SATA 5

Damaged drives 5-passes imaging settings

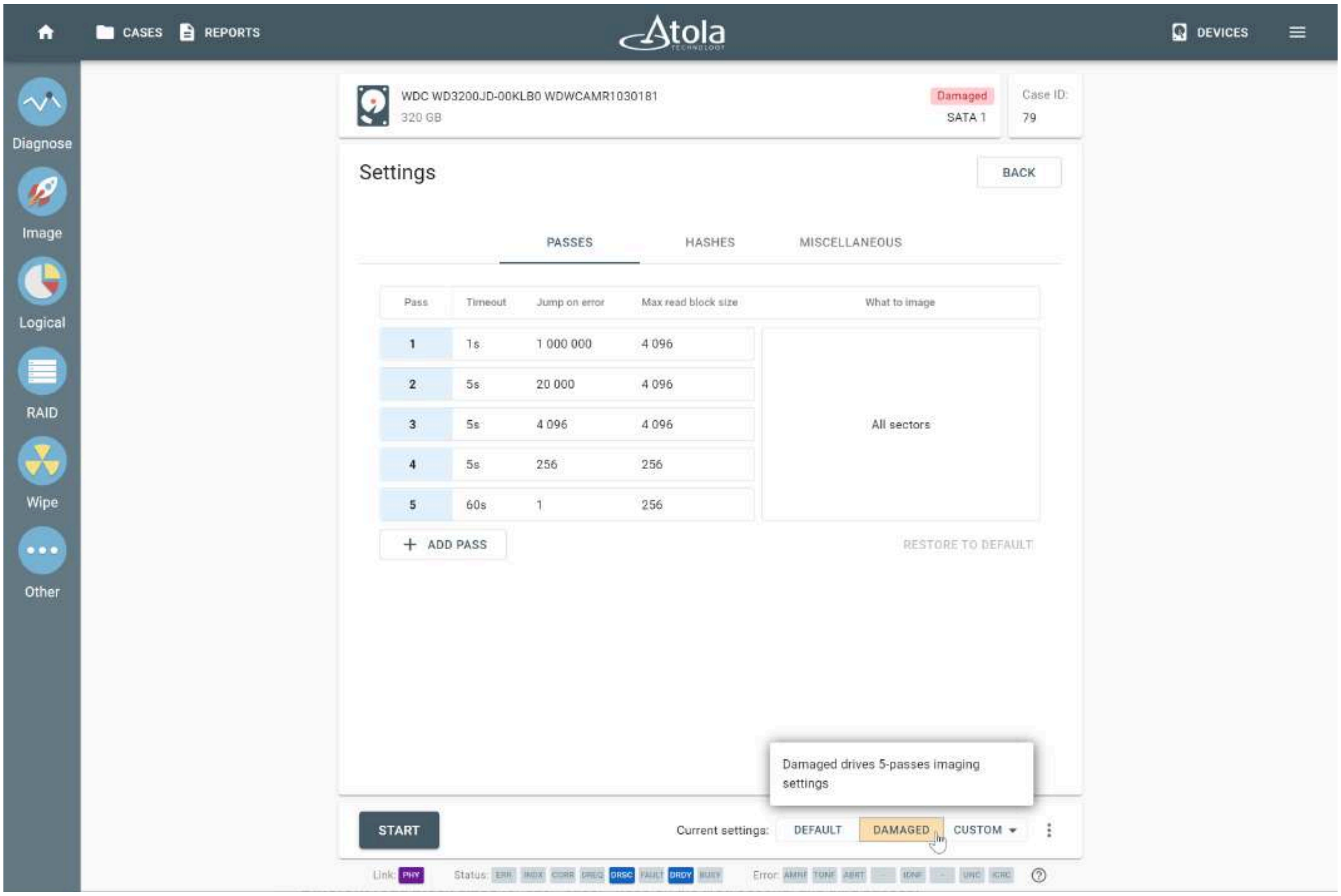
Current settings: DAMAGED

The Damaged preset is selected on the Imaging settings screen.

To thoroughly retrieve maximum data from an unstable drive in a forensically sound way, the preset for damaged hard drives has several major differences from default imaging settings:

- **Number of passes**: 5 passes for damaged drives instead of 1 pass for good drives.
- **Different timeouts for each pass**: 1 second on the first pass, 5 seconds on the second, third, and fourth passes, and 60 seconds on the last fifth pass.
- **Jump on errors**: from 1,000,000 sectors on the first pass to only 1 sector jump on the last pass.
- **Different read block sizes for each pass**: 4,096 on the first, second, and third passes, 256 for the fourth and fifth passes.
- **Segmented hashing** with 4 GB segments instead of linear hashing used by default for good drives.

If you use an E01 file as a target along with a linear hashing method, multiple passes aren’t available. In such a case, we recommend using an AFF4 or RAW file format instead.



WDC WD3200JD-00KLB0 WDWCAMR1030181
320 GB
Damaged
SATA 1
Case ID: 79

Settings

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	All sectors
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

Damaged drives 5-passes imaging settings

START
Current settings: DEFAULT DAMAGED CUSTOM
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

The Damaged preset for imaging faulty drives.

Pass is a single complete cycle of reading blocks from a source device and writing them to a target device, beginning from a start sector and finishing at an end sector (as specified in the **What to image** field).

Timeout is a max time for a single read block attempt during this pass.

Jump on errors is a number of consecutive sectors that TaskForce will skip if it can’t read a block from a source device.

Max read block size is a maximum number of sectors that TaskForce reads from a source device at a time.

Segmented hashing is a process of calculating hashes for a series of corresponding LBA ranges of the image. For more details, see Segmented hashing for data verification.

Multipass algorithm for imaging damaged drives

To approach bad drives in the most gentle way possible, TaskForce uses its special multipass imaging system.

Most forensic imagers can only do linear imaging, which dramatically slows down the imaging process whenever a bad sector is encountered, and, as a result, the drive may freeze. To speed up the imaging of damaged media and maximize the amount of successfully retrieved data, TaskForce has a special imaging algorithm that includes a deliberate timeout and block size control.

Timeouts and block size control

Using a small block size pays off when you need to thoroughly retrieve maximum data from an unstable drive, but it also significantly slows down the imaging process. What’s worse, such an imaging approach may cause further damage to the media.

That's why TaskForce's multipass imaging engine uses **large blocks with short timeouts** on the **first few passes**, scheduling reads inside slow areas for later and then using the **smallest block size on the last pass** when very few sectors are left to be read. TaskForce handles block size automatically, to provide the best possible results in the shortest time.

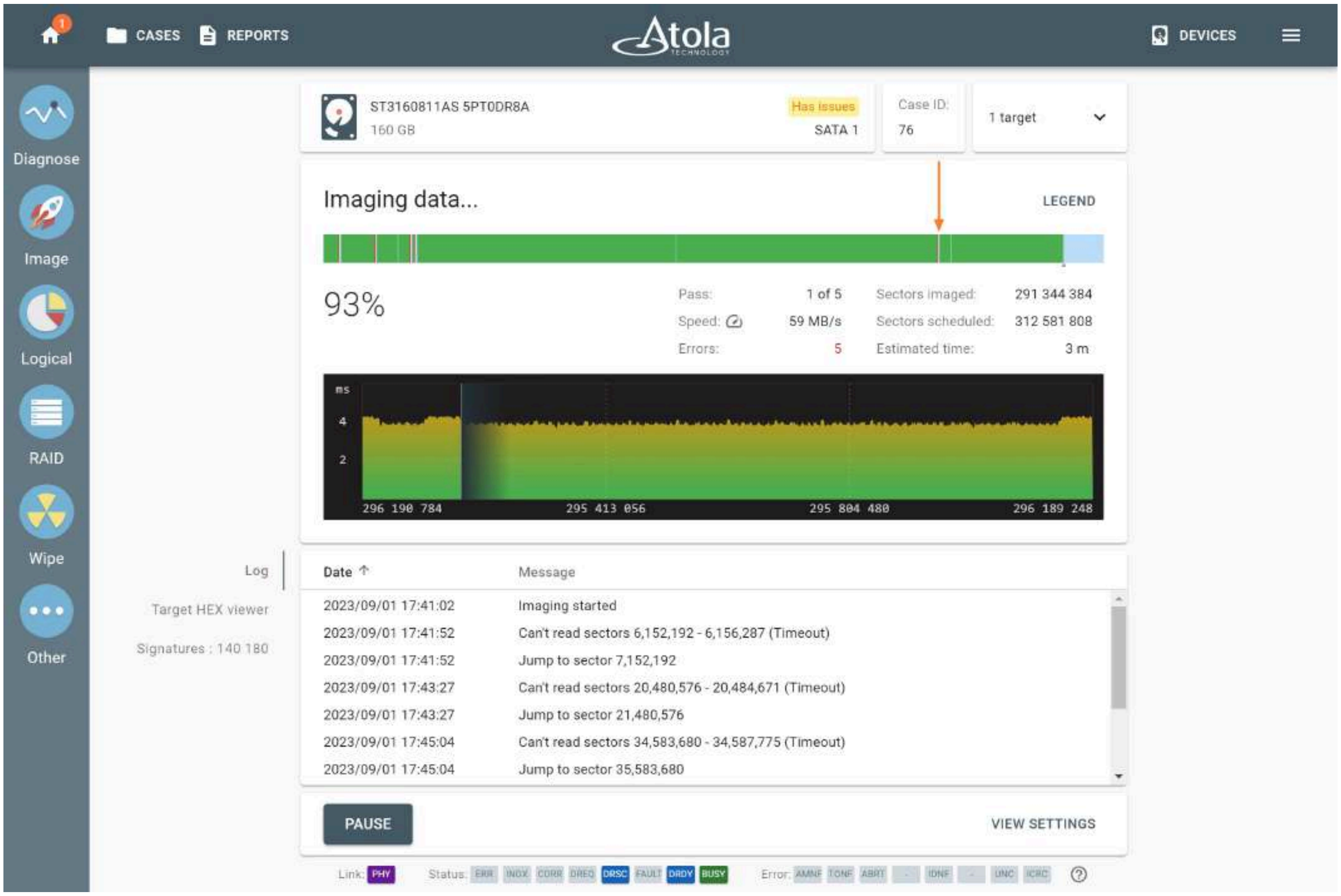
This technique helps achieve imaging max speeds in good areas of the drive. At the same time, it lets you approach bad areas in the most delicate way possible and retrieve as much data as possible.

First pass

On the first pass, TaskForce allows a 1-second **Timeout** per block, and the **Max read block size** is set to 4096 sectors. This allows smooth sequential imaging of all healthy modern drives.

But when imaging damaged media, these settings let TaskForce skip any areas that slow down the process and perform **Jump on error** by 1,000,000 sectors at a time.

This way all the good areas of the drive are imaged at top speed, while forcing TaskForce to return to the problematic areas on the following passes, narrowing down the bad areas and allowing more time to retrieve the data within them.



ST3160811AS 5PT0DR8A
160 GB
Has issues
SATA 1
Case ID: 76
1 target

Imaging data...

93%

Pass: 1 of 5
Speed: 59 MB/s
Errors: 5
Sectors imaged: 291 344 384
Sectors scheduled: 312 581 808
Estimated time: 3 m

Signatures : 140 180

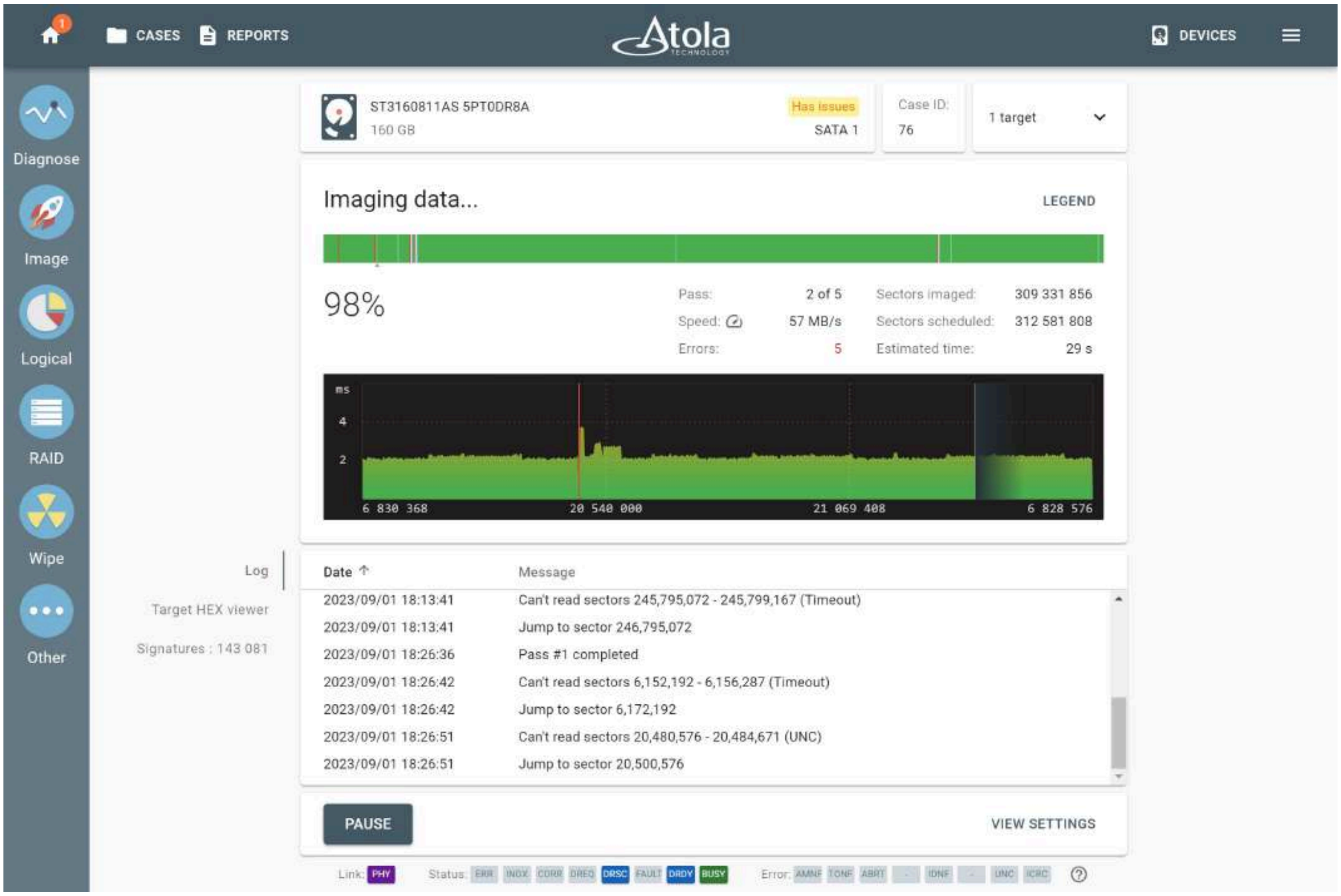
Date ↑	Message
2023/09/01 17:41:02	Imaging started
2023/09/01 17:41:52	Can't read sectors 6,152,192 - 6,156,287 (Timeout)
2023/09/01 17:41:52	Jump to sector 7,152,192
2023/09/01 17:43:27	Can't read sectors 20,480,576 - 20,484,671 (Timeout)
2023/09/01 17:43:27	Jump to sector 21,480,576
2023/09/01 17:45:04	Can't read sectors 34,583,680 - 34,587,775 (Timeout)
2023/09/01 17:45:04	Jump to sector 35,583,680

Link: PHY Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY Error: AMNF TONF ABRT - IDNF - UNC ICRC

Imaging the first pass. Empty areas where errors were encountered and jumps were performed.

Second and third passes

While the **Max read block size** remains the same during the second and the third passes, the **Jump on error** is set to 20,000 sectors and 4,096 sectors respectively, and slightly longer, 5-second **Timeouts** are allowed for attempted reading of the blocks.



ST3160811AS 5PT0DR8A
160 GB
Has issues
SATA 1

Case ID: 76

1 target

Imaging data...

98%

Pass: 2 of 5
Speed: 57 MB/s
Errors: 5
Sectors imaged: 309 331 856
Sectors scheduled: 312 581 808
Estimated time: 29 s

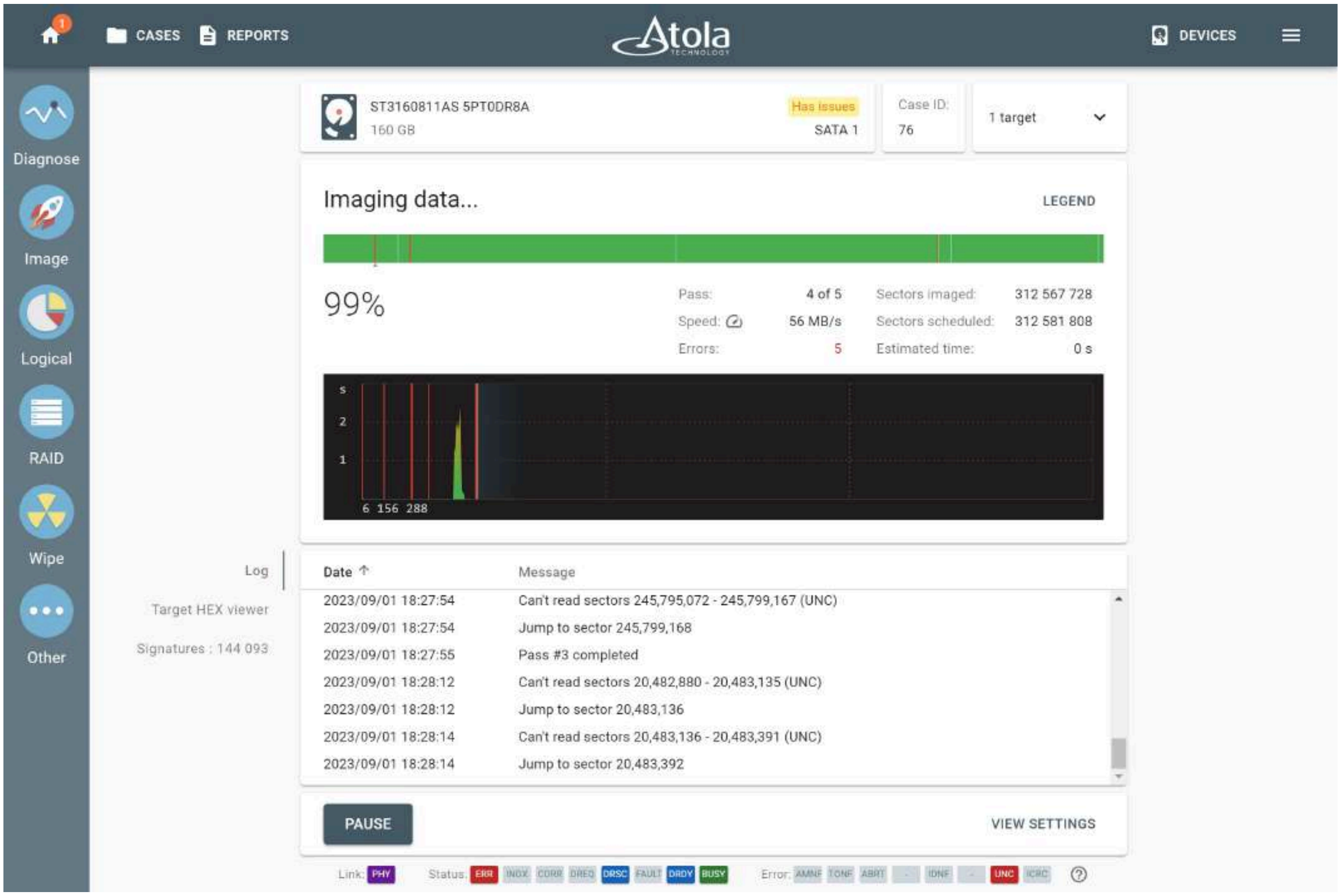
Signatures : 143 081

```
Date          Message
2023/09/01 18:13:41   Can't read sectors 245,795,072 - 245,799,167 (Timeout)
2023/09/01 18:13:41   Jump to sector 246,795,072
2023/09/01 18:26:36   Pass #1 completed
2023/09/01 18:26:42   Can't read sectors 6,152,192 - 6,156,287 (Timeout)
2023/09/01 18:26:42   Jump to sector 6,172,192
2023/09/01 18:26:51   Can't read sectors 20,480,576 - 20,484,671 (UNC)
2023/09/01 18:26:51   Jump to sector 20,500,576
```

Empty areas start filling up with data, as the jumps become smaller.

Fourth pass

On the fourth pass, both **Jump on error** and **Max read block size** are reduced to 256 sectors to try reading problematic zones in a more granular way.



ST3160811AS 5PT0DR8A
160 GB

Has issues
SATA 1

Case ID: 76

1 target

Imaging data...

99%

Pass: 4 of 5
Speed: 56 MB/s
Errors: 5
Sectors imaged: 312 567 728
Sectors scheduled: 312 581 808
Estimated time: 0 s

Signatures : 144 093

```
Date                  Message
2023/09/01 18:27:54   Can't read sectors 245,795,072 - 245,799,167 (UNC)
2023/09/01 18:27:54   Jump to sector 245,799,168
2023/09/01 18:27:55   Pass #3 completed
2023/09/01 18:28:12   Can't read sectors 20,482,880 - 20,483,135 (UNC)
2023/09/01 18:28:12   Jump to sector 20,483,136
2023/09/01 18:28:14   Can't read sectors 20,483,136 - 20,483,391 (UNC)
2023/09/01 18:28:14   Jump to sector 20,483,392
```

The amount of data retrieved is already 99%.

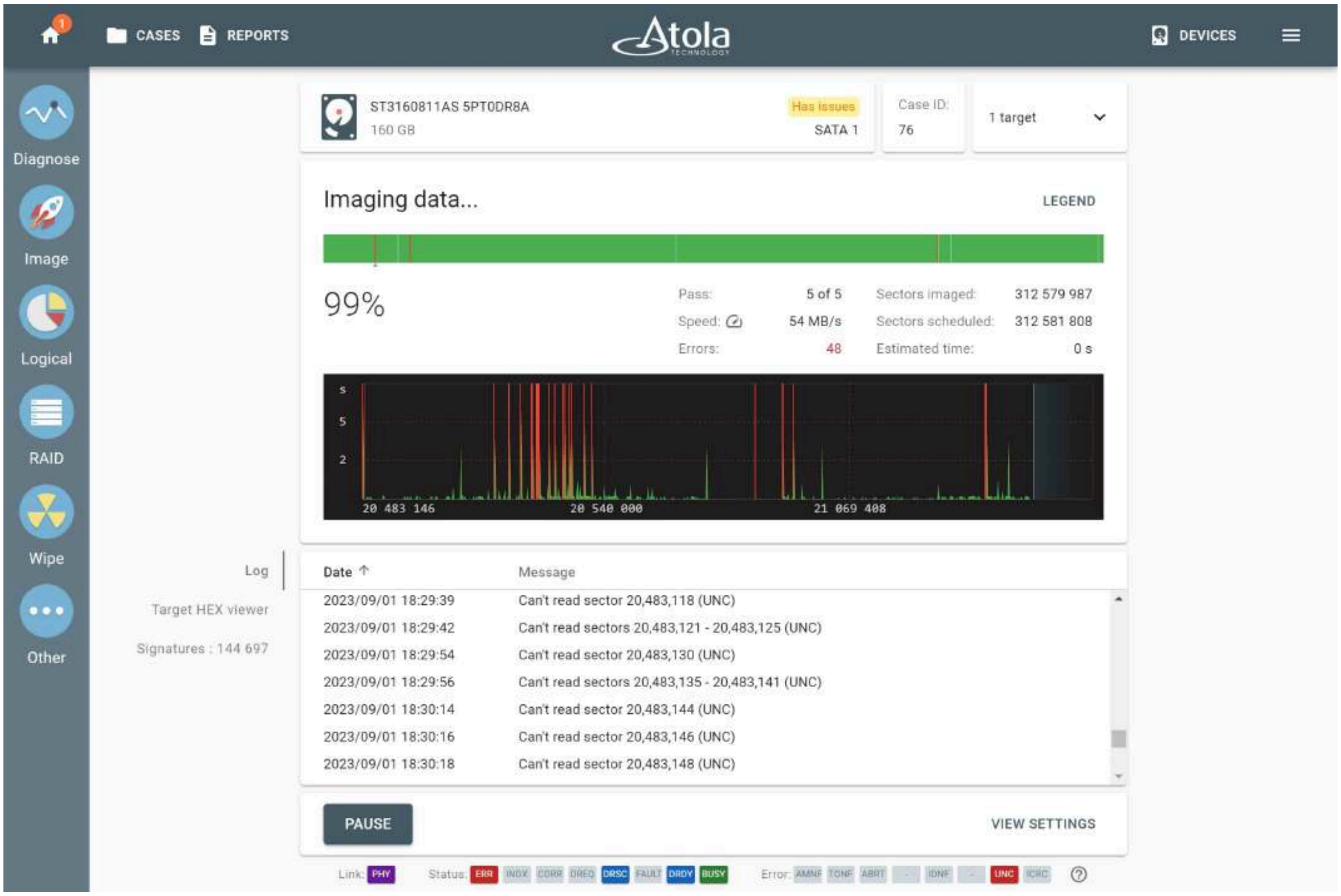
Fifth pass

On the fifth pass, TaskForce allocates 60-second **Timeouts** to read the **Maximum block size** of 256 with just 1-sector **Jump on error**. It is the last and the most thorough attempt to retrieve data from the remaining bad areas of the drive.

The last pass has a unique feature that is not used during previous passes: an internal sector-by-sector auto-reread procedure for an error block. It is defined by an unchangeable Jump size = 1 sector.

How the imaging engine works on the last pass:

- It reads a block using the Max Block Size pass setting (256 by default).
- If the reading is successful, it proceeds to the next non-imaged block.
- If a read error occurs, the engine re-reads the whole error block sector by sector.



ST3160811AS 5PT0DR8A
160 GB
Has issues
SATA 1

Case ID: 76

1 target

Imaging data...

99%

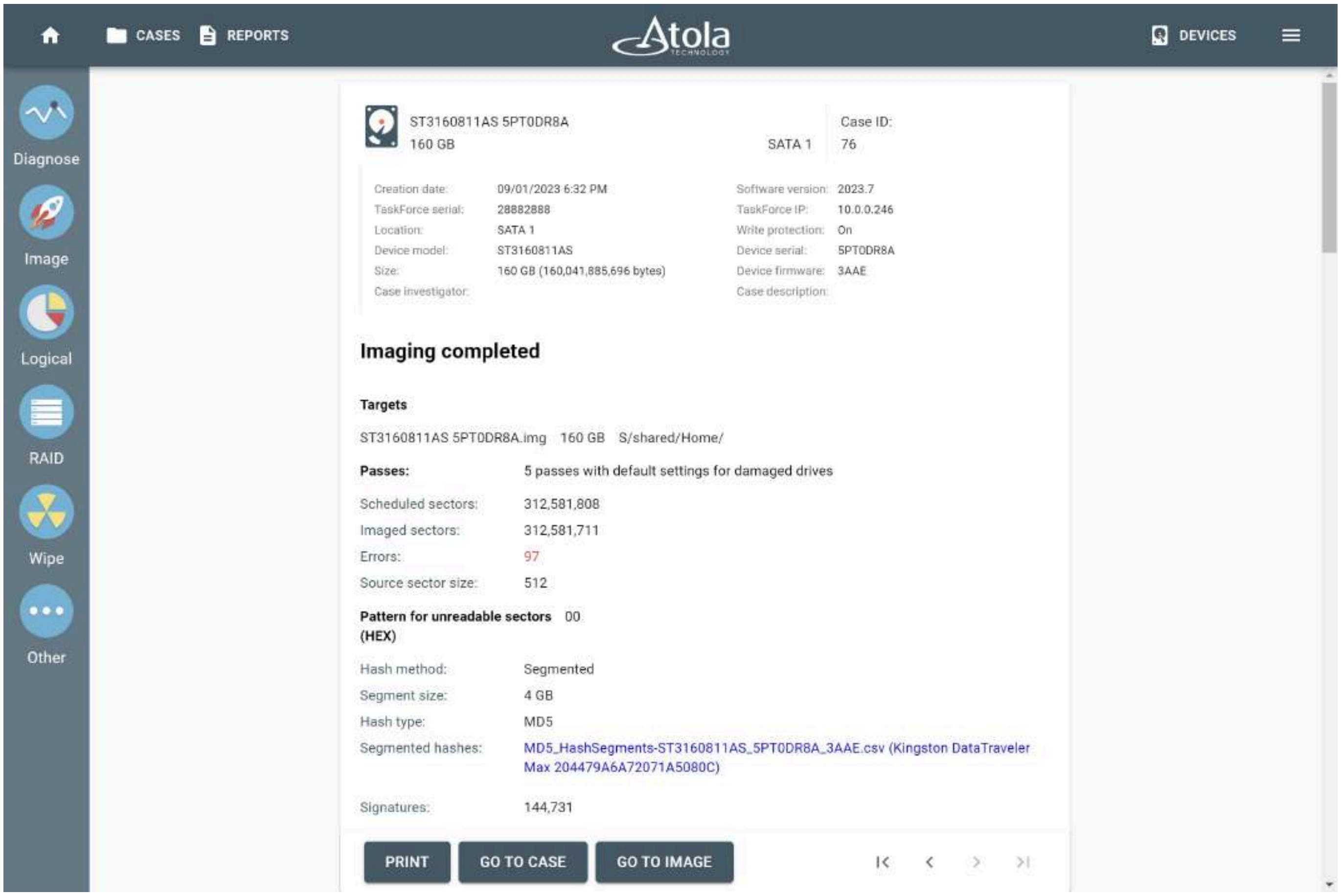
Pass: 5 of 5
Speed: 54 MB/s
Errors: 48
Sectors imaged: 312 579 987
Sectors scheduled: 312 581 808
Estimated time: 0 s

Log
Target HEX viewer
Signatures : 144 697

Date ↑	Message
2023/09/01 18:29:39	Can't read sector 20,483,118 (UNC)
2023/09/01 18:29:42	Can't read sectors 20,483,121 - 20,483,125 (UNC)
2023/09/01 18:29:54	Can't read sector 20,483,130 (UNC)
2023/09/01 18:29:56	Can't read sectors 20,483,135 - 20,483,141 (UNC)
2023/09/01 18:30:14	Can't read sector 20,483,144 (UNC)
2023/09/01 18:30:16	Can't read sector 20,483,146 (UNC)
2023/09/01 18:30:18	Can't read sector 20,483,148 (UNC)

On the fifth pass TaskForce attempts to read the data for the last time.

After the final pass, the **Imaging Results** report will indicate the eventual number of errors on the drive and other detailed statistics.



ST3160811AS 5PT0DR8A
160 GB
SATA 1
Case ID:
76

Creation date:	09/01/2023 6:32 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	ST3160811AS	Device serial:	5PT0DR8A
Size:	160 GB (160,041,885,696 bytes)	Device firmware:	3AAE
Case investigator:		Case description:	

Imaging completed

Targets

ST3160811AS 5PT0DR8A.img 160 GB S/shared/Home/

Passes:	5 passes with default settings for damaged drives
Scheduled sectors:	312,581,808
Imaged sectors:	312,581,711
Errors:	97
Source sector size:	512
Pattern for unreadable sectors (HEX)	00
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-ST3160811AS_5PT0DR8A_3AAE.csv (Kingston DataTraveler Max 204479A6A72071A5080C)
Signatures:	144,731

The Imaging Results report shows the number of errors on the drive.

Customize imaging settings for each pass

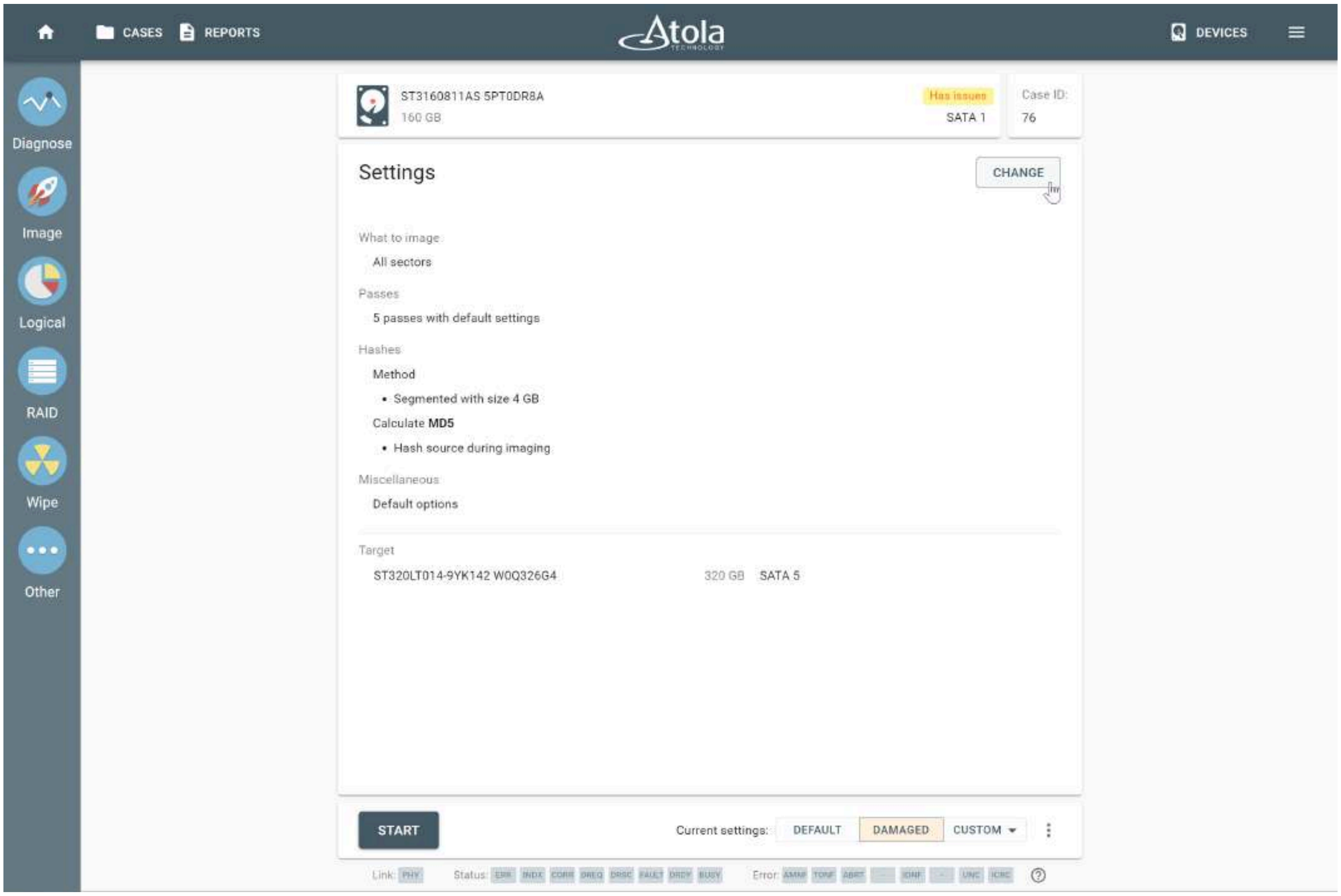
To cope with a severely damaged drive, you can adjust the following parameters of any imaging pass:

- Timeout
- Jump on error
- Max read block address
- Start and end LBA
- Image in reverse direction
- Disable read look-ahead

Also, you can add or delete an imaging pass.

To customize settings for a certain imaging pass, do the following:

1. On the **Imaging settings** page, click **Change**.


CASES
REPORTS
Atola
DEVICES
Diagnose
Image
Logical
RAID
Wipe
Other

ST3160811AS 5PT0DR8A
160 GB
Has issues
SATA 1
Case ID:
76

Settings

CHANGE

What to image

All sectors

Passes

5 passes with default settings

Hashes

Method

- Segmented with size 4 GB

Calculate **MD5**

- Hash source during imaging

Miscellaneous

Default options

Target

ST320LT014-9YK142 W0Q326G4 320 GB SATA 5

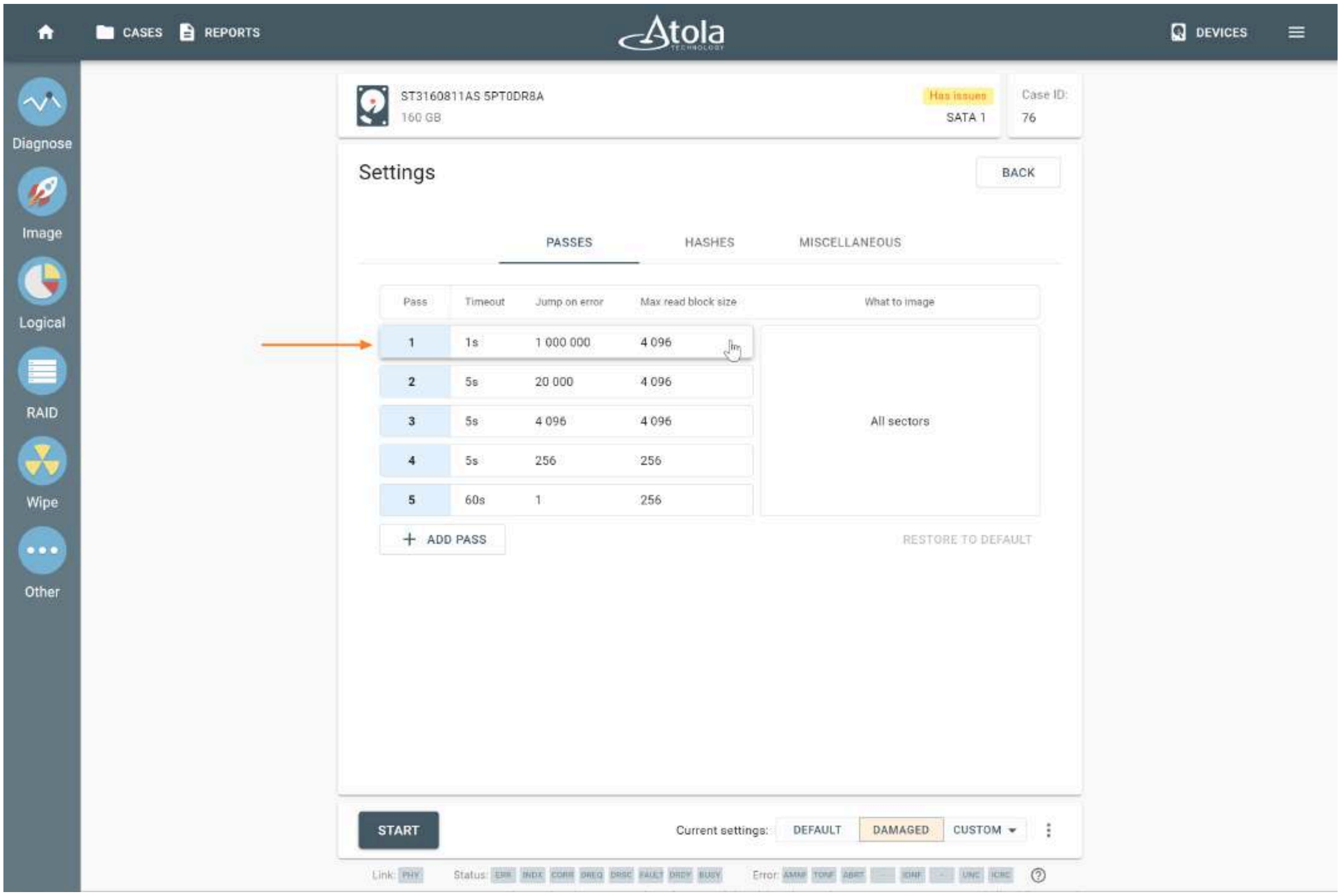
START

Current settings: DEFAULT DAMAGED CUSTOM

Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

The Change button on the Imaging settings page.

2. Click the pass you want to change.



ST3160811AS 5PT0DR8A
160 GB

Has issues
SATA 1

Case ID:
76

Settings

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	All sectors
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

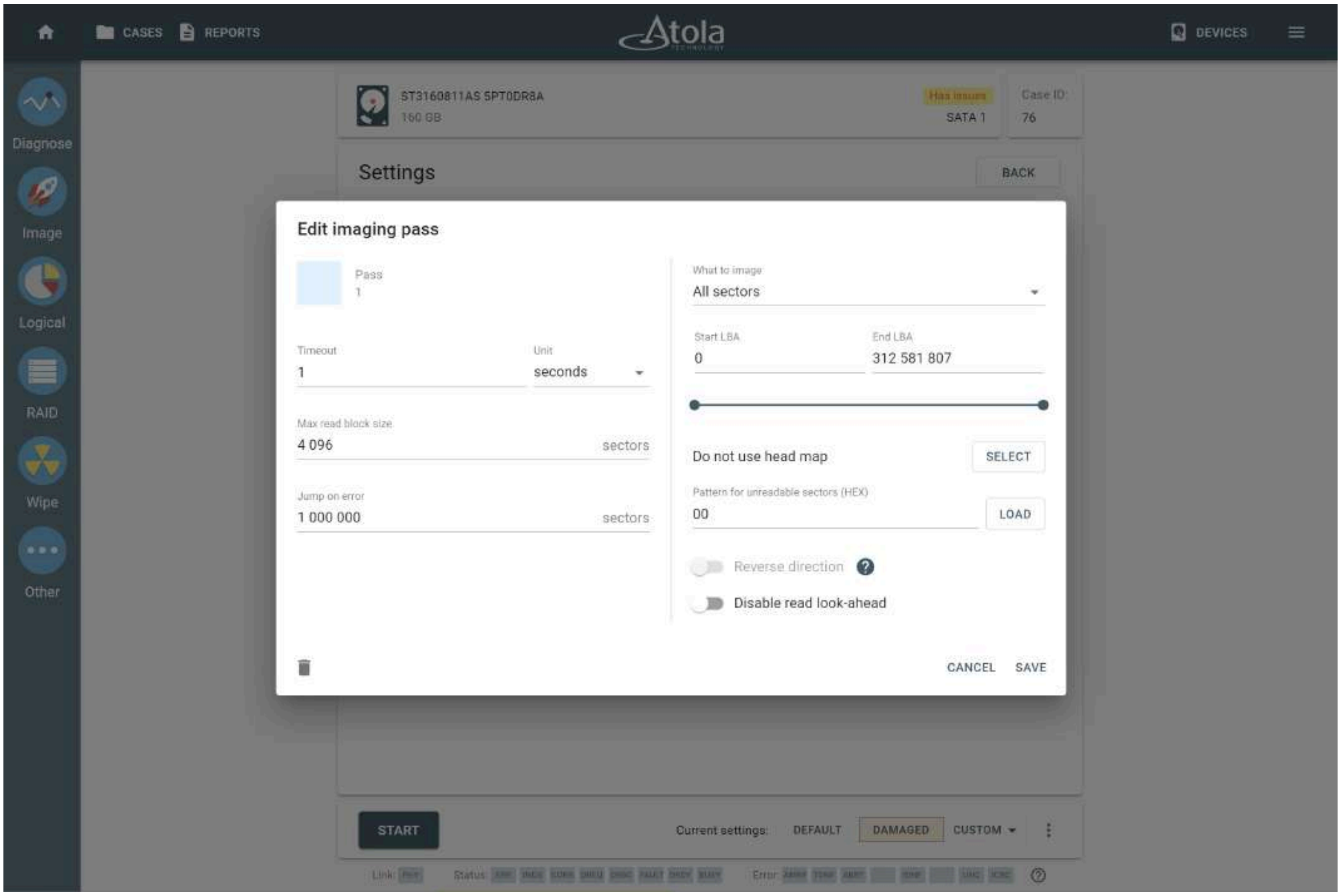
Current settings: DEFAULT DAMAGED CUSTOM

Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

An imaging pass is highlighted on the Imaging settings page.

3. In the **Edit imaging pass** window, enter new settings or toggle the options you need.

4. Click Save.



ST3160811AS 5PT0DR8A
160 GB
SATA 1
Case ID: 76

Settings

Edit imaging pass

Pass
1

Timeout: 1
Unit: seconds

Max read block size: 4 096 sectors

Jump on error: 1 000 000 sectors

What to image: All sectors

Start LBA: 0
End LBA: 312 581 807

Do not use head map

Pattern for unreadable sectors (HEX): 00

Reverse direction

Disable read look-ahead

Current settings: DAMAGED

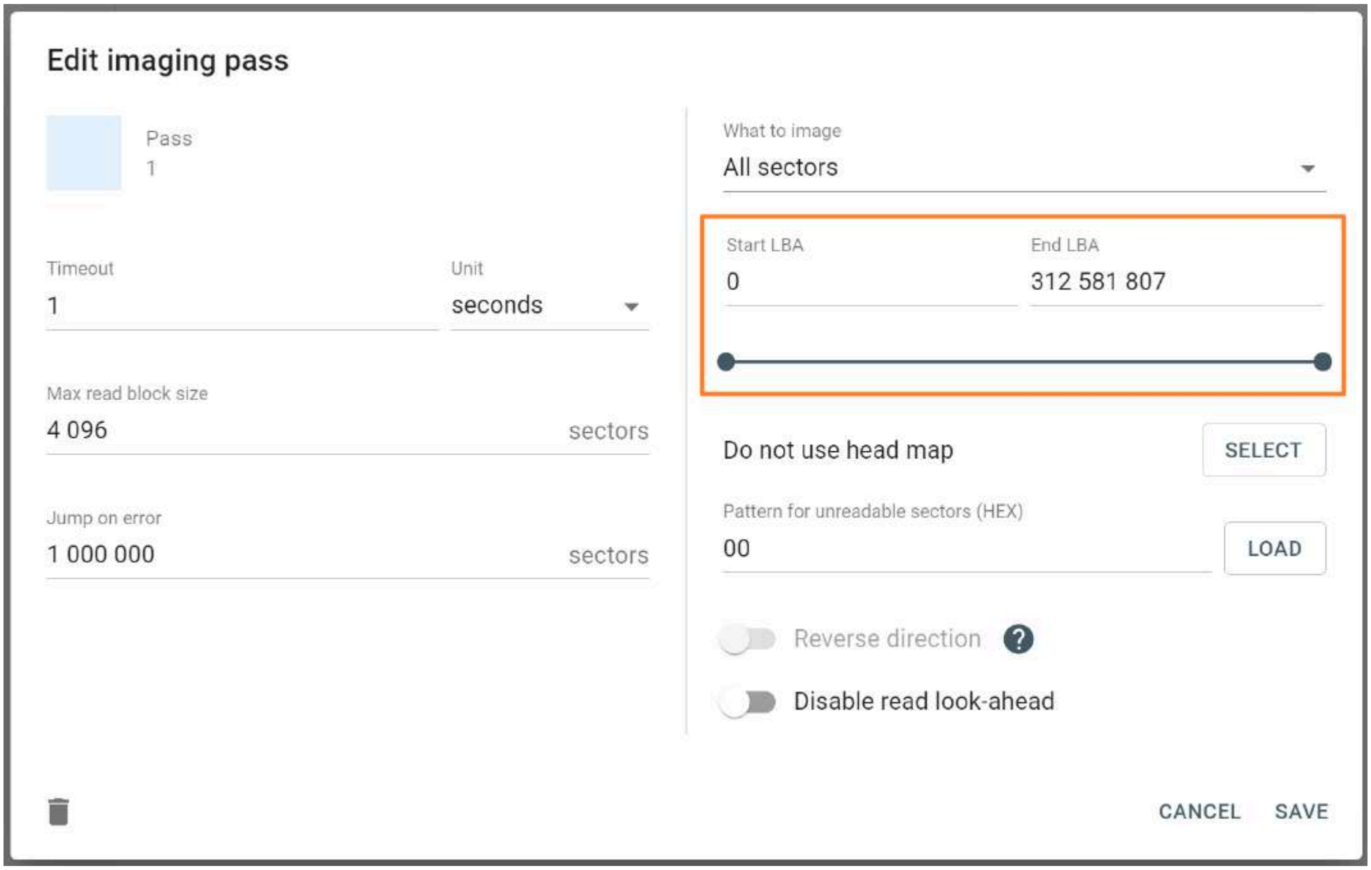
The Edit imaging pass window shows the current settings for the first pass.

Start and End LBA

For each pass, you can define the starting and ending sectors by entering logical block addresses in the respective fields (**Start LBA**, **End LBA**) or by dragging markers of the slider below.

Alternatively, you can select **All sectors with data** in the **What to image** field. It makes TaskForce search for all known partitions and image only the sectors that contain data. This option is a good use when you are facing a lack of time to take a full image.

Currently supported partitions: NTFS, ext4/3/2, exFAT, XFS, ZFS, Btrfs, APFS (with encrypted volumes), HFS/HFS+, FAT32/16.



Edit imaging pass

Pass
1

Timeout
1

Unit
seconds

Max read block size
4 096 sectors

Jump on error
1 000 000 sectors

What to image
All sectors

Start LBA
0

End LBA
312 581 807

Do not use head map

Pattern for unreadable sectors (HEX)
00

Reverse direction

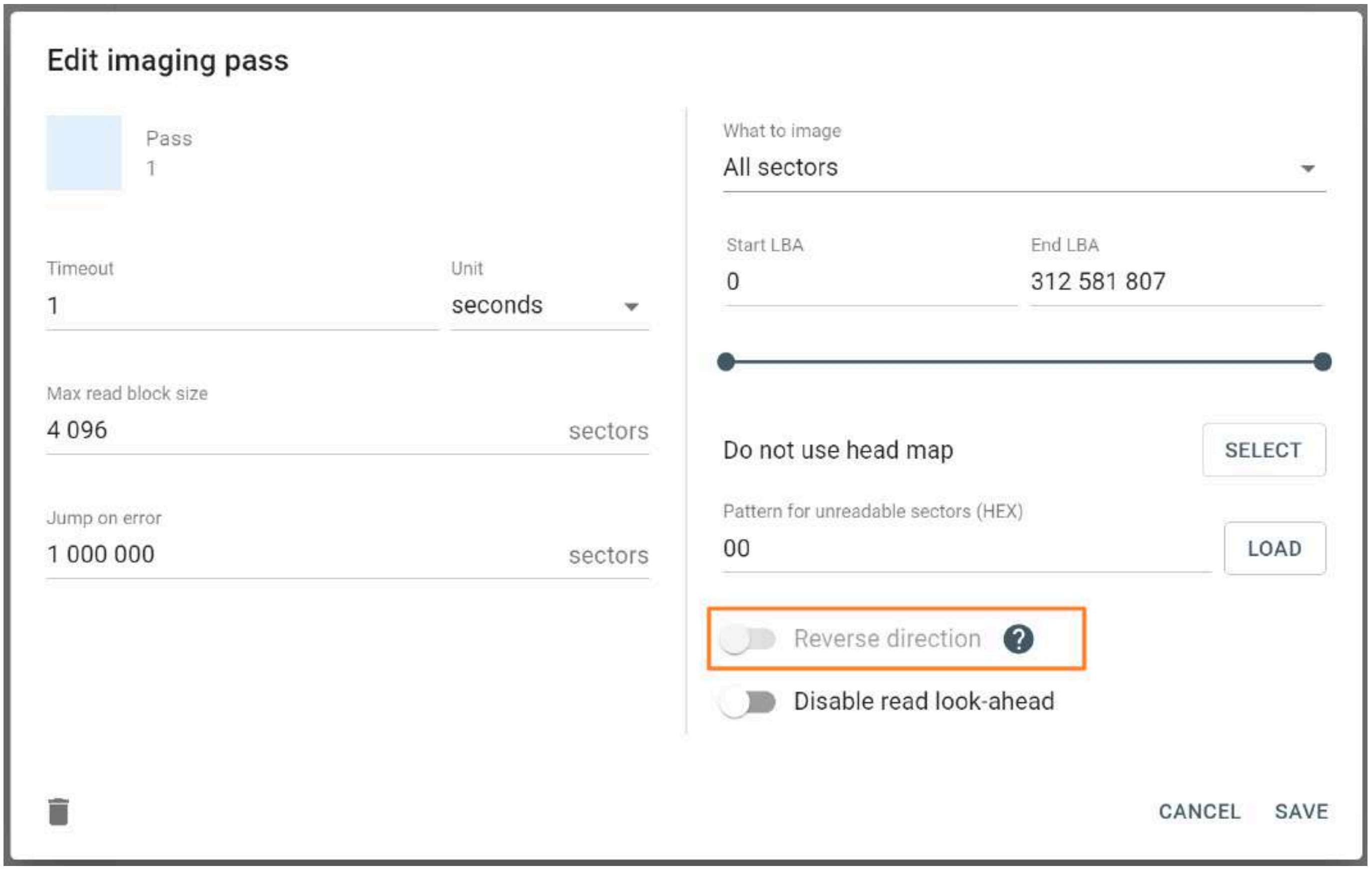
Disable read look-ahead

Image in reverse direction

With this function selected, TaskForce approaches skipped areas of the drive from the other side on any selected pass. That means the imaging engine reads a source drive backward and reaches the damaged areas from the opposite direction.

This way, the imaging module can retrieve more data from a drive before entering a damaged zone, which needs to be concentrated on during the following passes. But the speed decreases due to auto disabling of the drive's cache.

Hint: It is one of the best options we recommend you enable to get more data from a severely damaged drive.



Edit imaging pass

Pass
1

Timeout
1

Unit
seconds

Max read block size
4 096 sectors

Jump on error
1 000 000 sectors

What to image
All sectors

Start LBA
0

End LBA
312 581 807

Do not use head map

Pattern for unreadable sectors (HEX)
00

Reverse direction

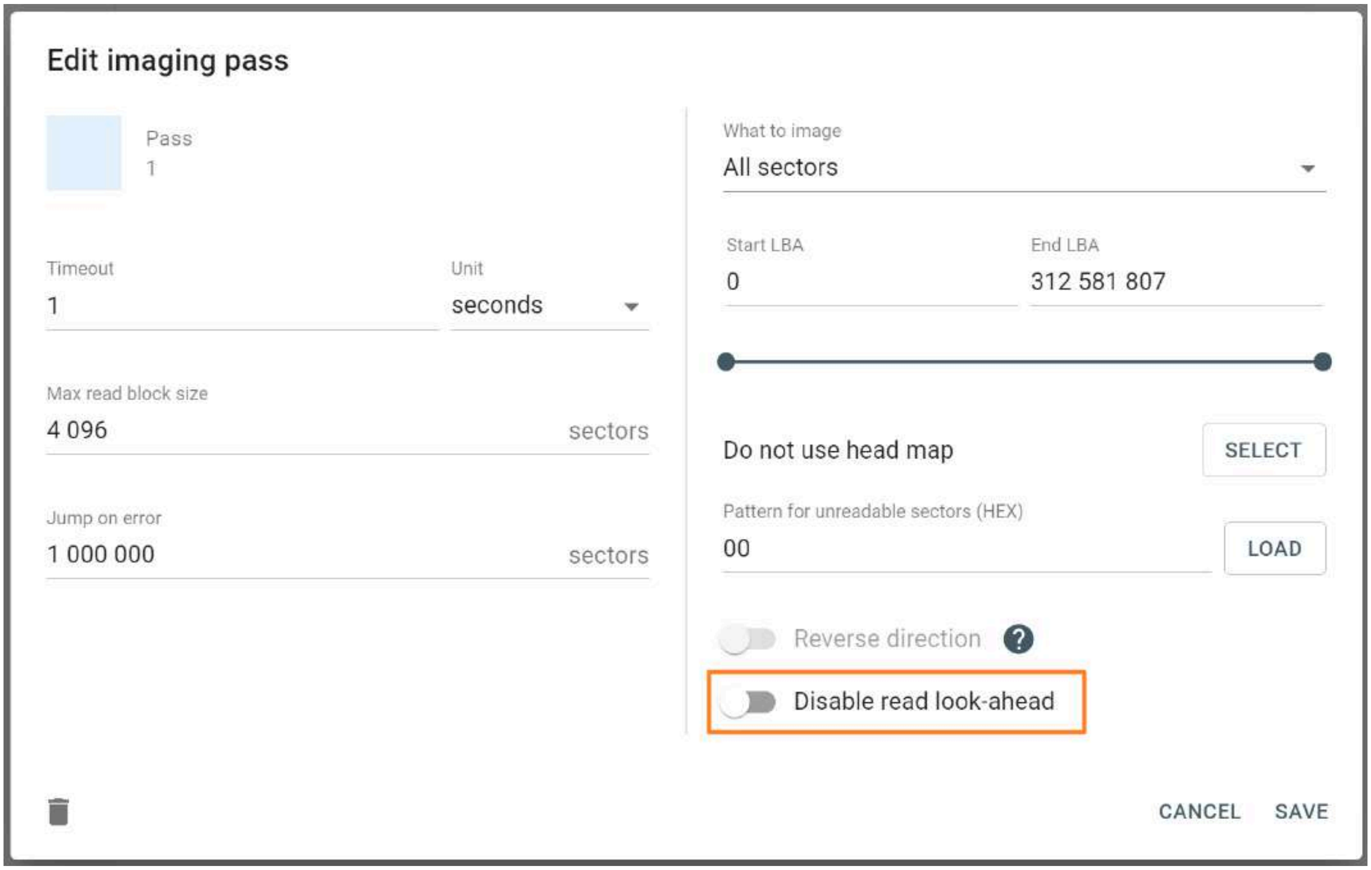
Disable read look-ahead

Disable the read look-ahead mode

Most contemporary hard drives have a read look-ahead functionality, which makes the drive read more blocks sequentially than requested by software.

In good drives, this functionality helps the drive operate faster by reading more data and caching it.

But with bad drives, the read look-ahead feature leads to bad areas being addressed more often. This slows down the process and may lead to a complete freeze of the drive. In such cases, we recommend disabling the read look-ahead option.



Edit imaging pass

Pass 1

Timeout: 1

Unit: seconds

Max read block size: 4 096 sectors

Jump on error: 1 000 000 sectors

What to image: All sectors

Start LBA: 0

End LBA: 312 581 807

Do not use head map

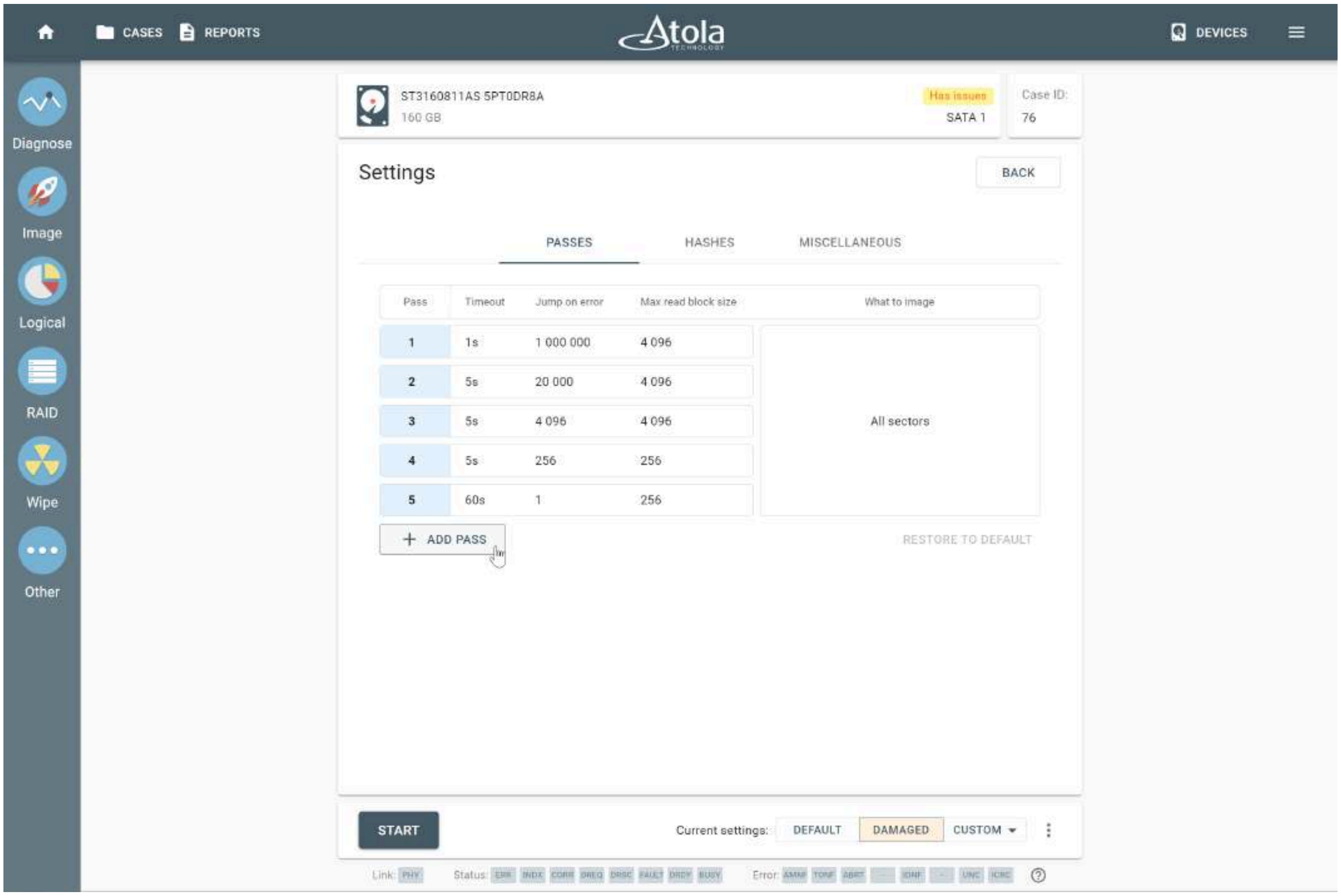
Pattern for unreadable sectors (HEX): 00

Add a pass

You can add new passes even when an imaging session is not yet started or when it's paused.

To add a new pass to an imaging session, do the following:

1. On the **Imaging settings** page, click **Change**.
2. Click **Add pass**.



Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	All sectors
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

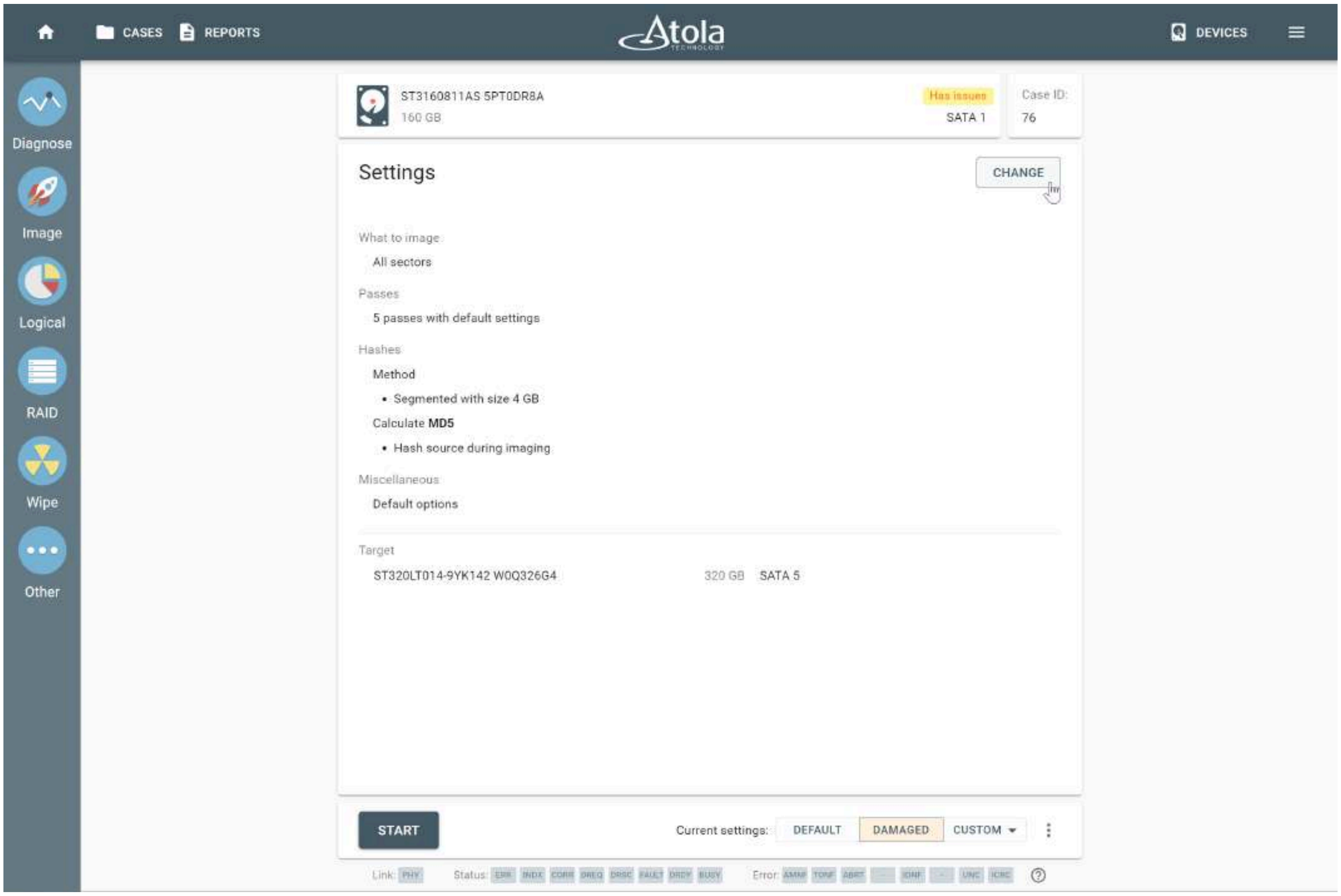
Adding a pass.

3. Adjust the settings for the new pass.
4. Click **Save**.

Delete a pass

You can delete any pass that has not been started yet. To delete an imaging pass, do the following:

1. On the **Imaging settings** page, click **Change**.



ST3160811AS 5PT0DR8A
160 GB
Has issues
SATA 1
Case ID:
76

Settings

What to image
All sectors

Passes
5 passes with default settings

Hashes
Method
- Segmented with size 4 GB

Calculate **MD5**
- Hash source during imaging

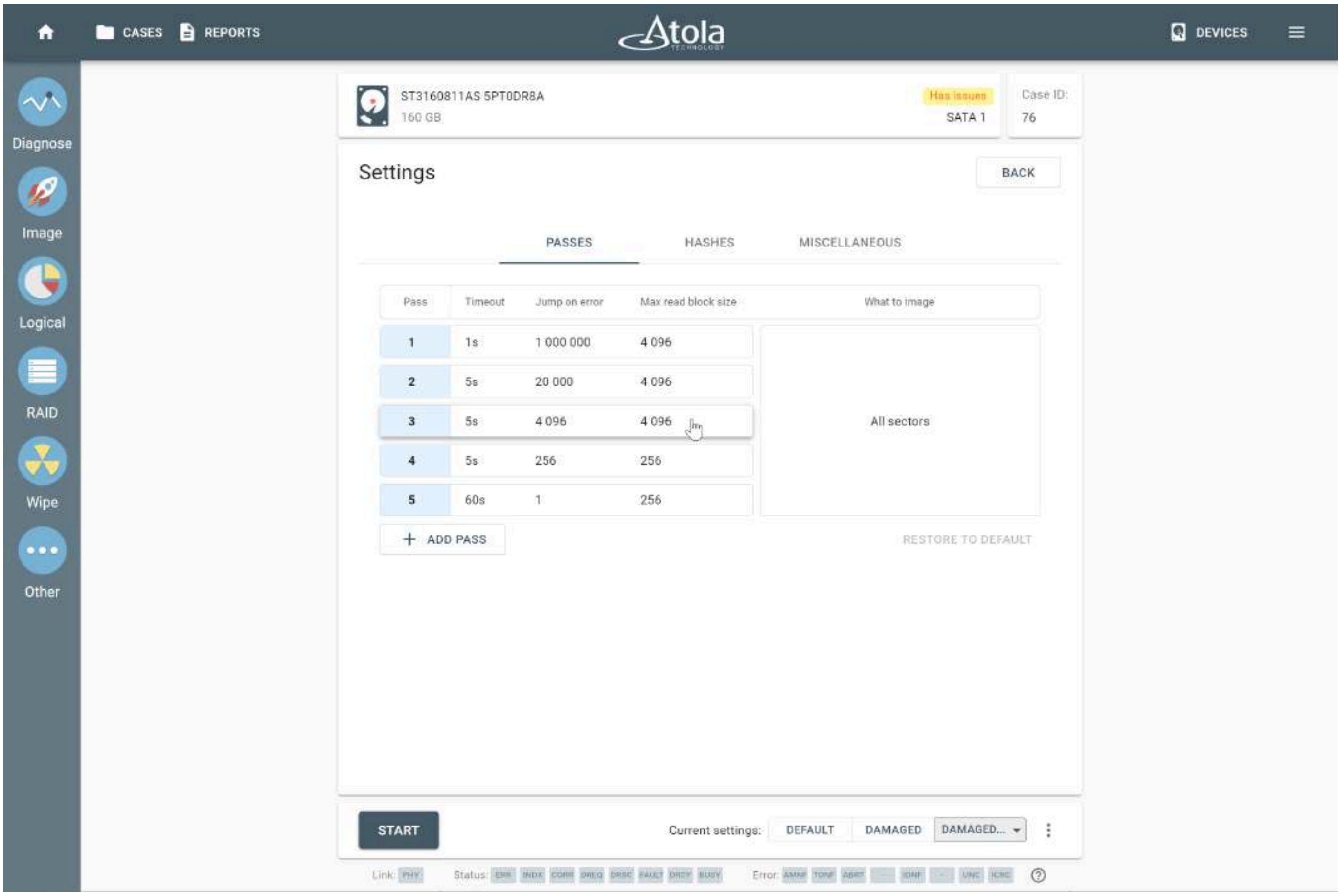
Miscellaneous
Default options

Target
ST320LT014-9YK142 W0Q326G4 320 GB SATA 5

Current settings: DAMAGED

The Change button on the Imaging settings page.

2. Click the pass you want to delete.



ST3160811AS 5PT0DR8A
160 GB

Has issues
SATA 1

Case ID: 76

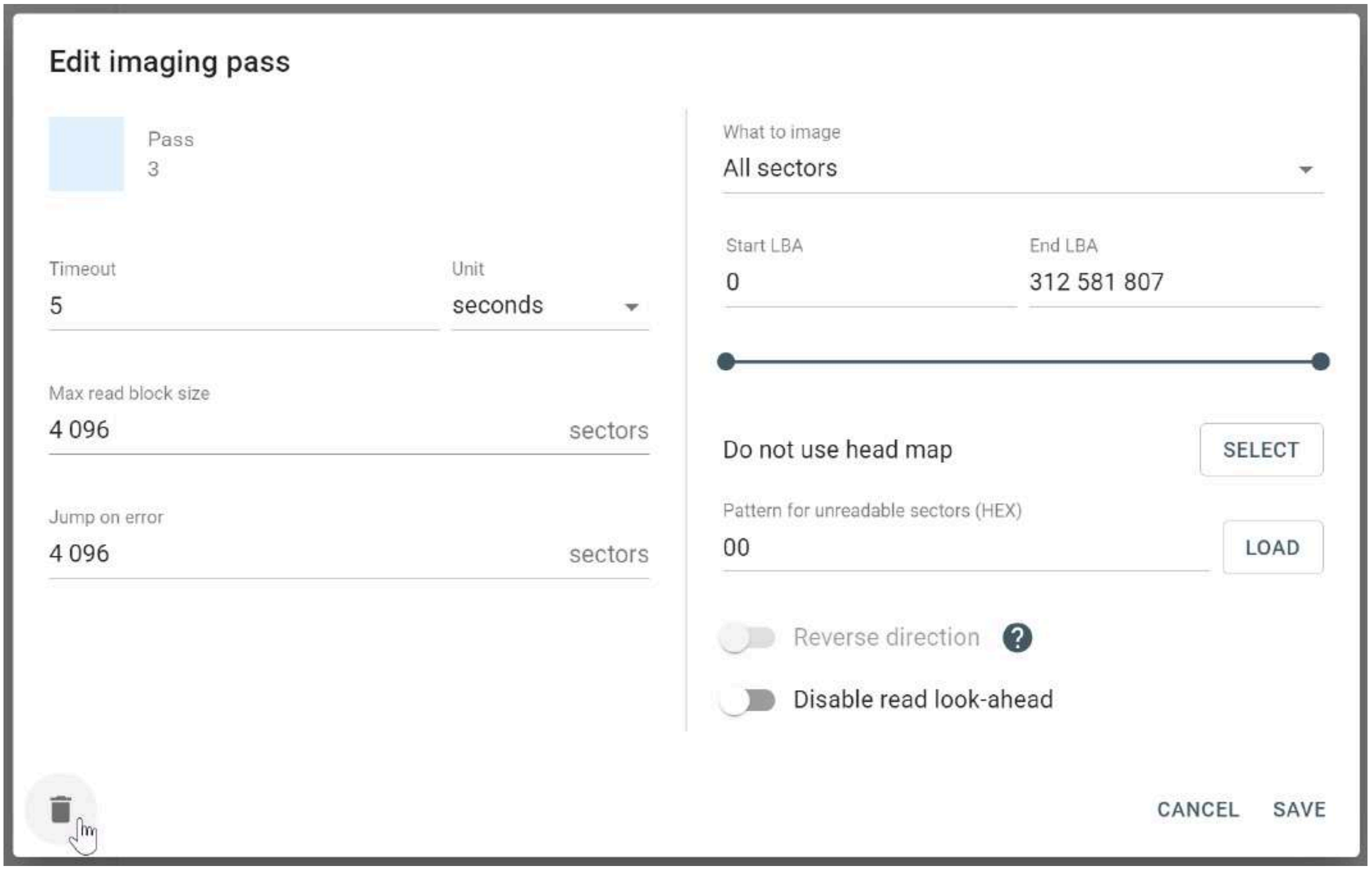
Settings

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	All sectors
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

Current settings: DAMAGED...

An imaging pass is highlighted on the Imaging settings page.

3. In the **Edit imaging pass** window, click the **Delete** icon and confirm the deletion.



Edit imaging pass

Pass 3

Timeout: 5

Unit: seconds

Max read block size: 4 096 sectors

Jump on error: 4 096 sectors

What to image: All sectors

Start LBA: 0

End LBA: 312 581 807

Do not use head map

Pattern for unreadable sectors (HEX): 00

Reverse direction

Disable read look-ahead

Imaging freezing drives

The core part of the imaging process is based on reading a source drive by sending multiple **Read sectors** commands and handling the drive's response at the low native I/O level.

When a drive receives and runs a **Read sectors** command but is unable to read any data from that sector. So it goes into **Retry** mode, trying to get data from the damaged area again and again.

After a certain number of tries, it gives up on a particular command and returns an error with timeout.

In TaskForce, you can detect a freezing drive during diagnostics or during imaging.

Freeze detection and handling during imaging

Imagine that the drive is unable to read data from the damaged sectors and goes into a long-lasting retry mode before it gives up on a particular sector and returns an error.

If TaskForce simply waited for each **Read sectors** command to be completed:

- it would take ages to get an image of a drive with numerous errors;
- it could cause the drive to slip into complete freeze;
- in the worst-case scenario, further damage could be caused to the data on the drive.

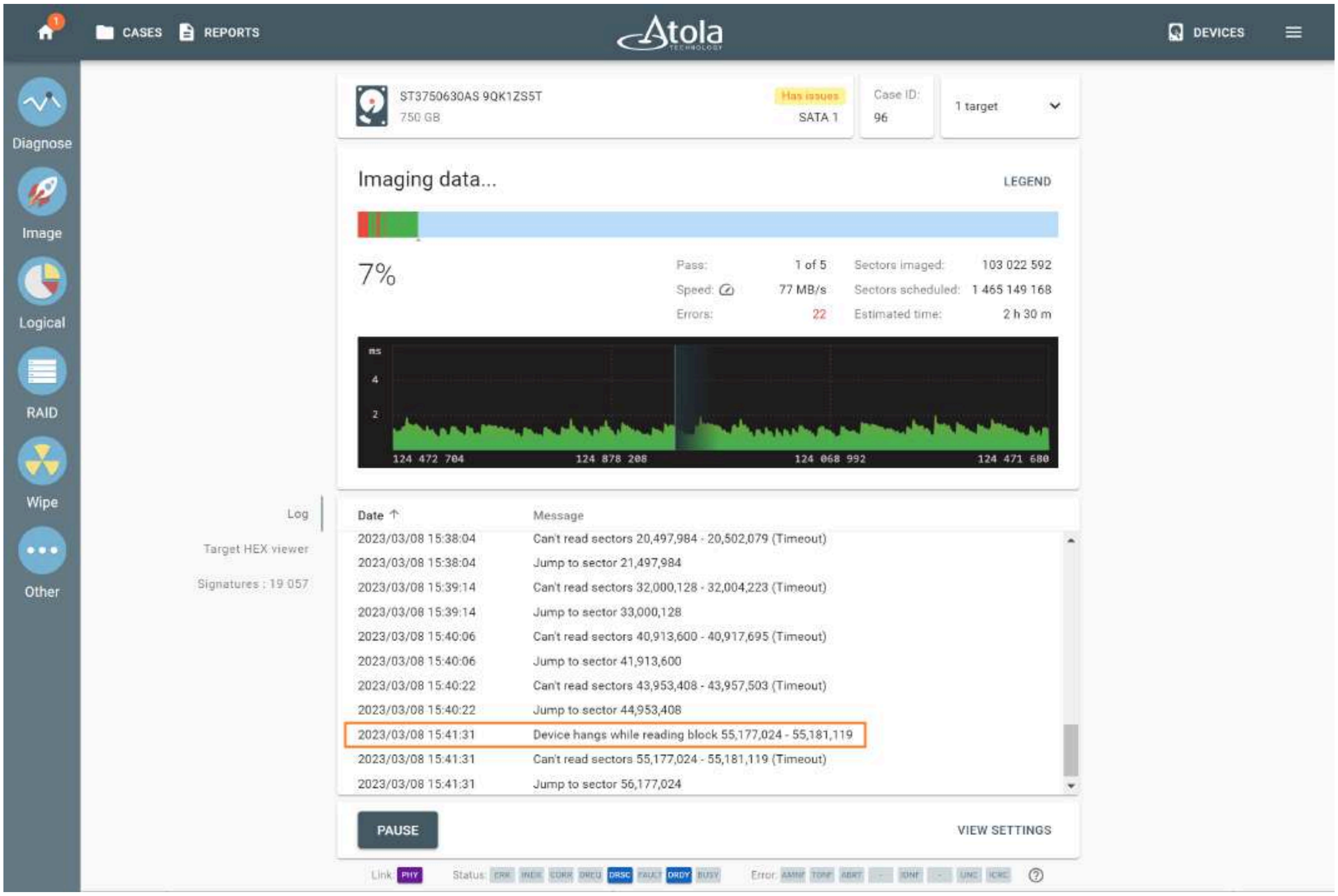
The Reset command

To avoid causing further damage to the data on the drive and long waiting periods, TaskForce issues a **Reset** command whenever a drive attempts to read a block of sectors longer than allowed by the pre-configured timeout.

Reset is a device interface operation, using which TaskForce stops the previously sent **Read sectors** (or any other) command and then continues imaging from the next planned block on the drive.

If the device is still running the Read Sectors command, even after the first **Reset** attempt, TaskForce waits 3 seconds and performs the second **Reset** command. At the moment of the second **Reset**, a new entry appears in the imaging **Log** reading

```
Device hangs while reading block X – Y.
```



ST3750630AS 9QK1ZS5T
750 GB
Has issues
SATA 1
Case ID: 96
1 target

Imaging data...

7%

Pass:	1 of 5	Sectors imaged:	103 022 592
Speed:	77 MB/s	Sectors scheduled:	1 465 149 168
Errors:	22	Estimated time:	2 h 30 m

Signatures : 19 057

Date ↑	Message
2023/03/08 15:38:04	Can't read sectors 20,497,984 - 20,502,079 (Timeout)
2023/03/08 15:38:04	Jump to sector 21,497,984
2023/03/08 15:39:14	Can't read sectors 32,000,128 - 32,004,223 (Timeout)
2023/03/08 15:39:14	Jump to sector 33,000,128
2023/03/08 15:40:06	Can't read sectors 40,913,600 - 40,917,695 (Timeout)
2023/03/08 15:40:06	Jump to sector 41,913,600
2023/03/08 15:40:22	Can't read sectors 43,953,408 - 43,957,503 (Timeout)
2023/03/08 15:40:22	Jump to sector 44,953,408
2023/03/08 15:41:31	Device hangs while reading block 55,177,024 - 55,181,119
2023/03/08 15:41:31	Can't read sectors 55,177,024 - 55,181,119 (Timeout)
2023/03/08 15:41:31	Jump to sector 56,177,024

Log entry: Device hangs while reading block X – Y.

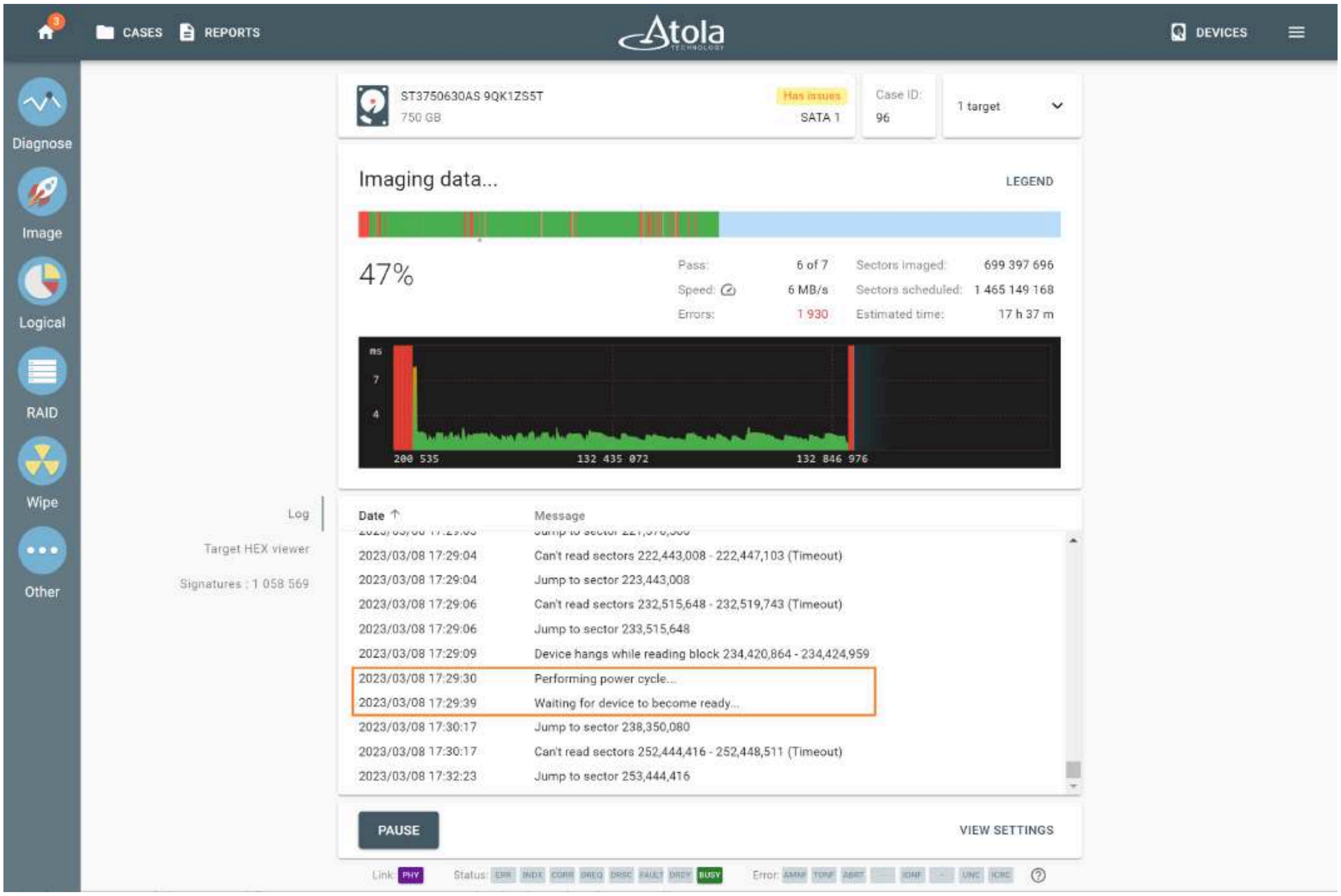
Performing a power cycle

If 20 seconds after the second **Reset** command the drive still tries to read the bad block, TaskForce performs the **Power cycle** command by forcibly cutting power to the drive for 5 seconds.

At this point, TaskForce adds two entries to the imaging **Log**:

`Performing power cycle...` (when the power is cut off) and

`Waiting for the device to become ready…` (when the power is switched back on).



ST3750630AS 9QK1ZS5T
750 GB
Has issues
SATA 1

Case ID: 96

1 target

Signatures : 1 058 569

47%

Pass: 6 of 7
Speed: 6 MB/s
Errors: 1 930
Sectors imaged: 699 397 696
Sectors scheduled: 1 465 149 168
Estimated time: 17 h 37 m

```
Date ↑                 Message
2023/03/08 17:29:04    Can't read sectors 222,443,008 - 222,447,103 (Timeout)
2023/03/08 17:29:04    Jump to sector 223,443,008
2023/03/08 17:29:06    Can't read sectors 232,515,648 - 232,519,743 (Timeout)
2023/03/08 17:29:06    Jump to sector 233,515,648
2023/03/08 17:29:09    Device hangs while reading block 234,420,864 - 234,424,959
2023/03/08 17:29:30    Performing power cycle...
2023/03/08 17:29:39    Waiting for device to become ready...
2023/03/08 17:30:17    Jump to sector 238,350,080
2023/03/08 17:30:17    Can't read sectors 252,444,416 - 252,448,511 (Timeout)
2023/03/08 17:32:23    Jump to sector 253,444,416
```

Log entry: Performing power cycle.

After a successful power cycle

In case the first **Power cycle** command is successful, and the drive become ready to accept the next command, there will be a final log entry for this problematic block of sectors saying:

```
Cannot read block of data at X – Y (Timeout).
```

And then TaskForce continues imaging from the next planned block.

After an unsuccessful power cycle

If the first **Power cycle** command is ineffective, and the drive is still in **Busy** state and can't run the next command, TaskForce makes the second **Power cycle**.

If the second **Power cycle** does not help either, imaging is terminated. It can be resumed afterward, and TaskForce will continue to image all remaining sectors.

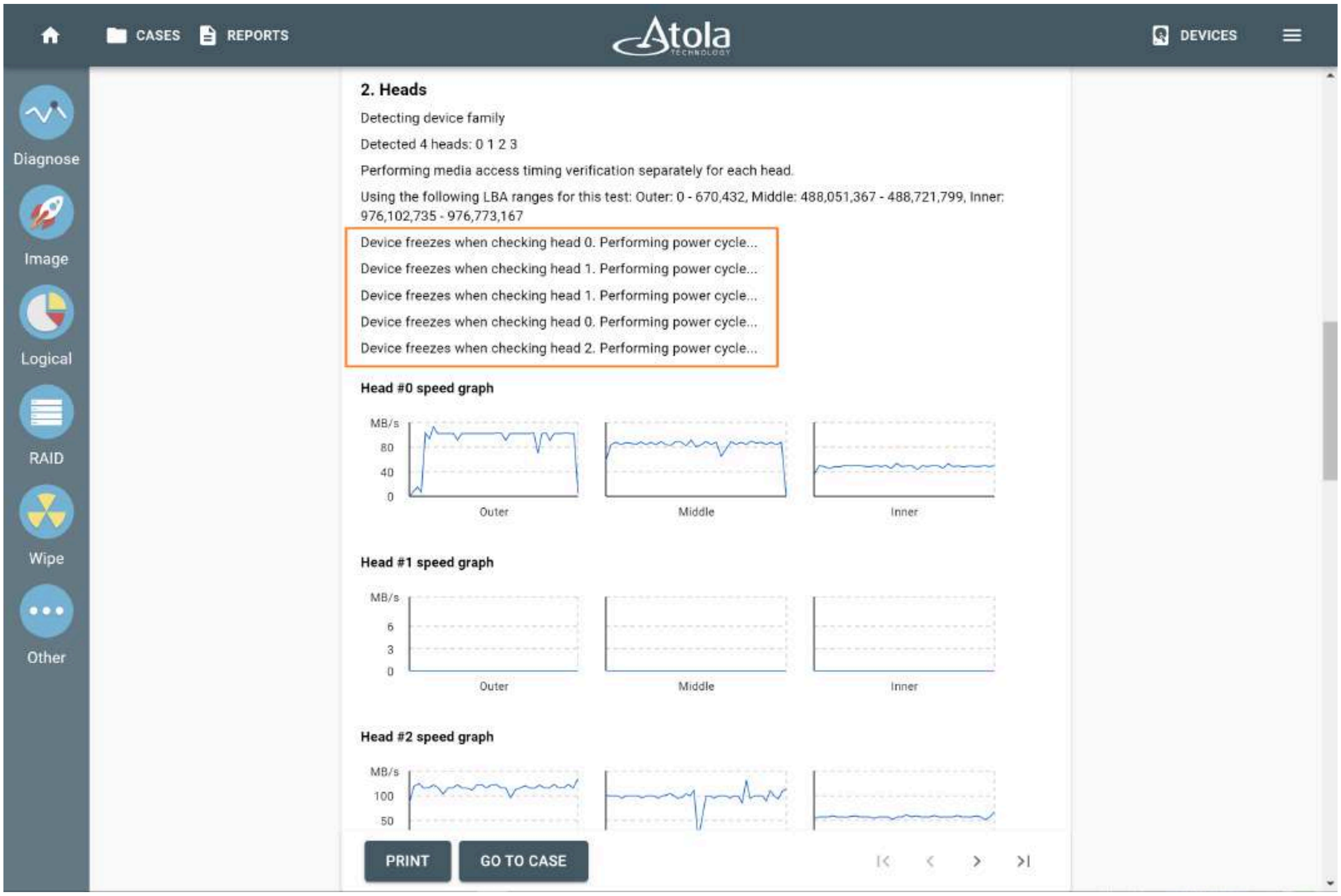
Freeze detection during diagnostics

TaskForce diagnostics module automatically checks the status of each head (for HDDs) and the condition of the media surface by reading several hundreds of thousands of sectors from the starting/outer, middle, and ending/inner part of the head or drive.

If a drive freezes, unable to read certain sectors, it may or may not be detected during diagnostics because not all sectors of the drive are being read at this stage.

If an HDD has a damaged head causing it to enter a busy state, a diagnostics report notifies you about that with the line

```
Device freezes when checking head N. Performing power cycle...
```



2. Heads

Detecting device family

Detected 4 heads: 0 1 2 3

Performing media access timing verification separately for each head.

Using the following LBA ranges for this test: Outer: 0 - 670,432, Middle: 488,051,367 - 488,721,799, Inner: 976,102,735 - 976,773,167

Device freezes when checking head 0. Performing power cycle...

Device freezes when checking head 1. Performing power cycle...

Device freezes when checking head 1. Performing power cycle...

Device freezes when checking head 0. Performing power cycle...

Device freezes when checking head 2. Performing power cycle...

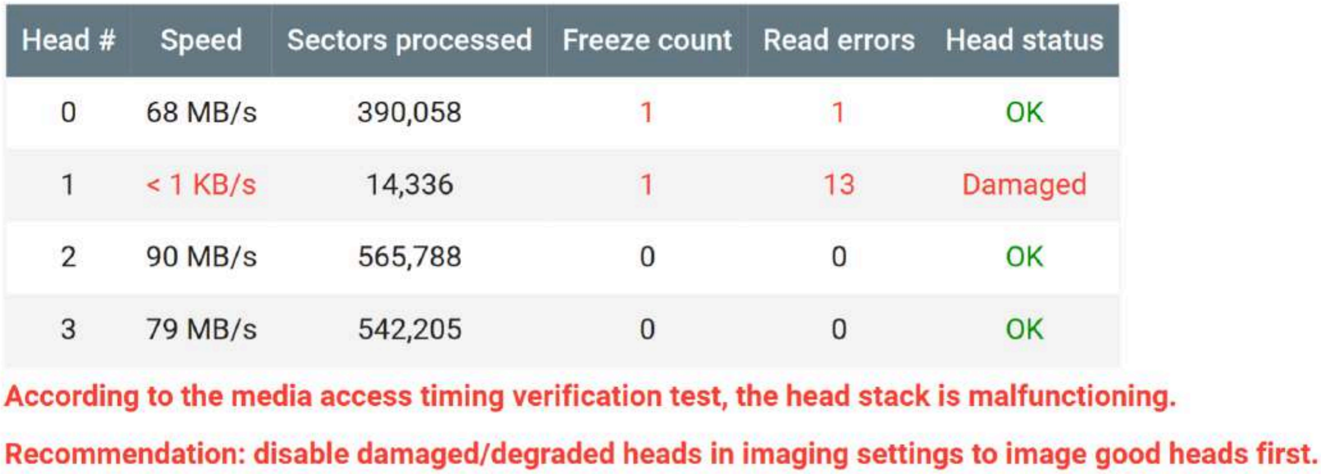
Head #0 speed graph

Head #1 speed graph

Head #2 speed graph

Notification "Device freezes when checking head N" in the diagnostics report.

Also, the diagnostics report shows a table with a freeze count and the number of read errors for each HDD head:

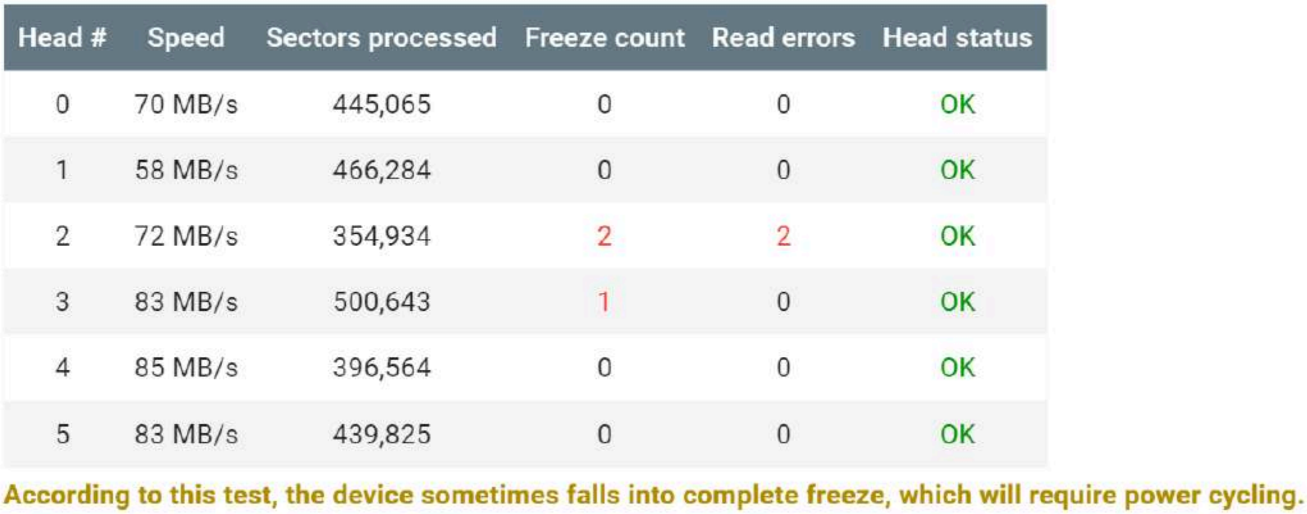


Head #	Speed	Sectors processed	Freeze count	Read errors	Head status
0	68 MB/s	390,058	1	1	OK
1	< 1 KB/s	14,336	1	13	Damaged
2	90 MB/s	565,788	0	0	OK
3	79 MB/s	542,205	0	0	OK

According to the media access timing verification test, the head stack is malfunctioning.

Recommendation: disable damaged/degraded heads in imaging settings to image good heads first.

A table with a freeze count for a drive with a damaged head.



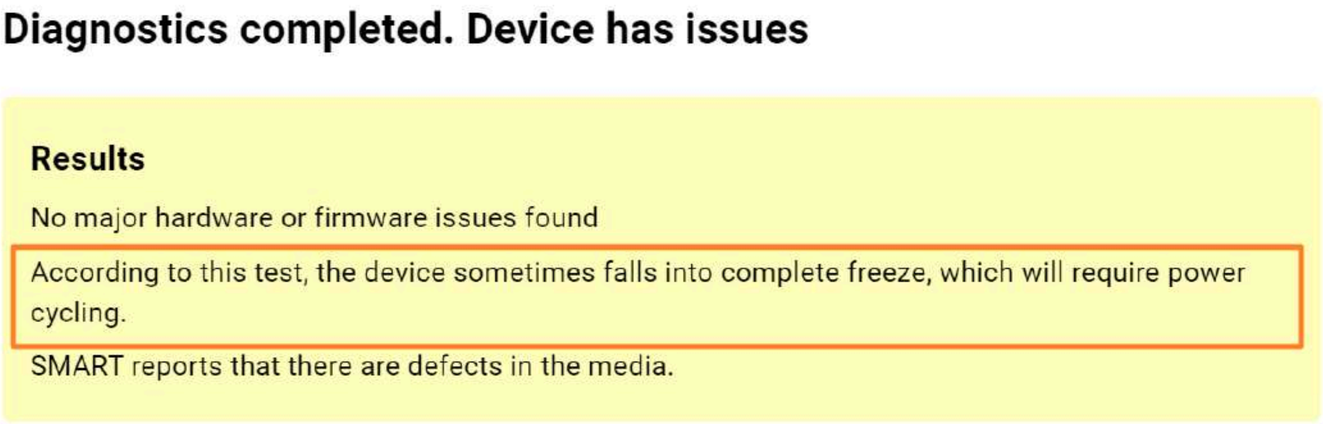
Head #	Speed	Sectors processed	Freeze count	Read errors	Head status
0	70 MB/s	445,065	0	0	OK
1	58 MB/s	466,284	0	0	OK
2	72 MB/s	354,934	2	2	OK
3	83 MB/s	500,643	1	0	OK
4	85 MB/s	396,564	0	0	OK
5	83 MB/s	439,825	0	0	OK

According to this test, the device sometimes falls into complete freeze, which will require power cycling.

A table with a freeze count for a drive with good heads.

If the heads status is OK, but some freezes were detected during diagnostics, the result of the diagnostics show the following line:

```
According to this test, the device sometimes falls into complete freeze, which will require power cycling.
```



Diagnostics completed. Device has issues

Results

No major hardware or firmware issues found

According to this test, the device sometimes falls into complete freeze, which will require power cycling.

SMART reports that there are defects in the media.

The Diagnostics results notifying that the device sometimes falls into complete freeze.

Imaging a shorted hard drive

Atola TaskForce has built-in short circuit protection and can detect shorted hard drives. In most cases, a drive has become shorted after experiencing overvoltage, either due to a power supply failure or as a result of a user error. Here is what happens to a drive in these scenarios and how to fix this.

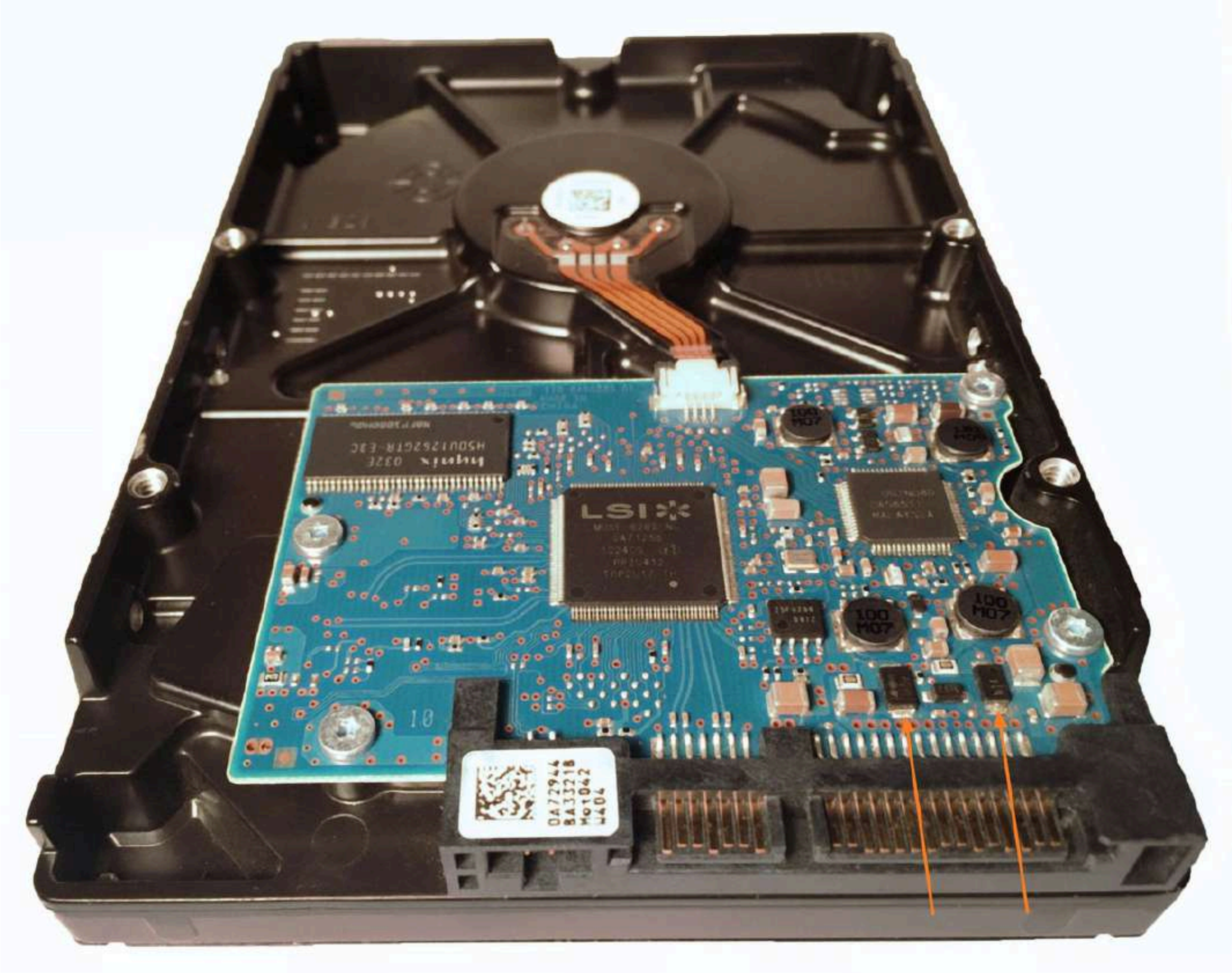
How drives become shorted

Most drives are equipped with two TVS diodes to protect the circuit from overvoltage. One diode is located on the 5V rail and another on the 12V rail.

If the drive experiences an overvoltage, the diodes convert the excess electrical power into heat energy and warm up, thus protecting the drive's circuit. Similarly, in the case of reverse polarity, the diode warms up as it conducts the current in the opposite direction.

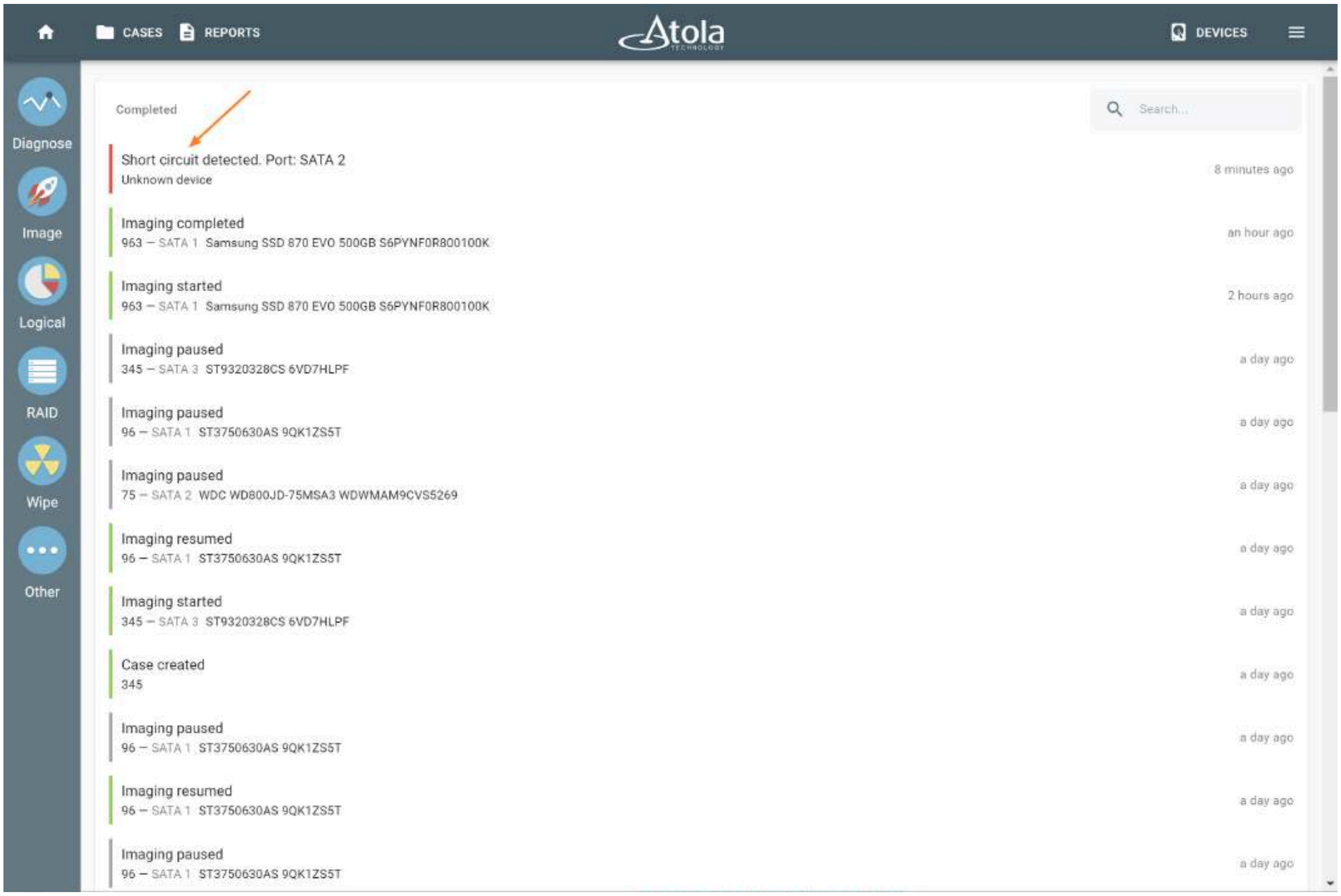
If the overvoltage or reverse polarity event is short and the dissipated energy is not too high, the diodes can recover and continue working. However, if the dissipated energy is too high, the diodes will "sacrifice" themselves and get shorted.

When the drive is subsequently powered, the shorted diodes create a low resistance connection between two nodes, known as a short circuit. This is exactly what happens to a drive when its TVS diodes are shorted.



Detect a shorted drive

When you connect a shorted drive to Atola TaskForce, the **Home screen** shows a short circuit alert to notify the operator about the detected issue.



Completed

Short circuit detected. Port: SATA 2
Unknown device
8 minutes ago

Imaging completed
963 — SATA 1 Samsung SSD 870 EVO 500GB S6PYNF0R800100K
an hour ago

Imaging started
963 — SATA 1 Samsung SSD 870 EVO 500GB S6PYNF0R800100K
2 hours ago

Imaging paused
345 — SATA 3 ST9320328CS 6VD7HLPF
a day ago

Imaging paused
96 — SATA 1 ST3750630AS 9QK1ZS5T
a day ago

Imaging paused
75 — SATA 2 WDC WD800JD-75MSA3 WDWMAM9CVS5269
a day ago

Imaging resumed
96 — SATA 1 ST3750630AS 9QK1ZS5T
a day ago

Imaging started
345 — SATA 3 ST9320328CS 6VD7HLPF
a day ago

Case created
345
a day ago

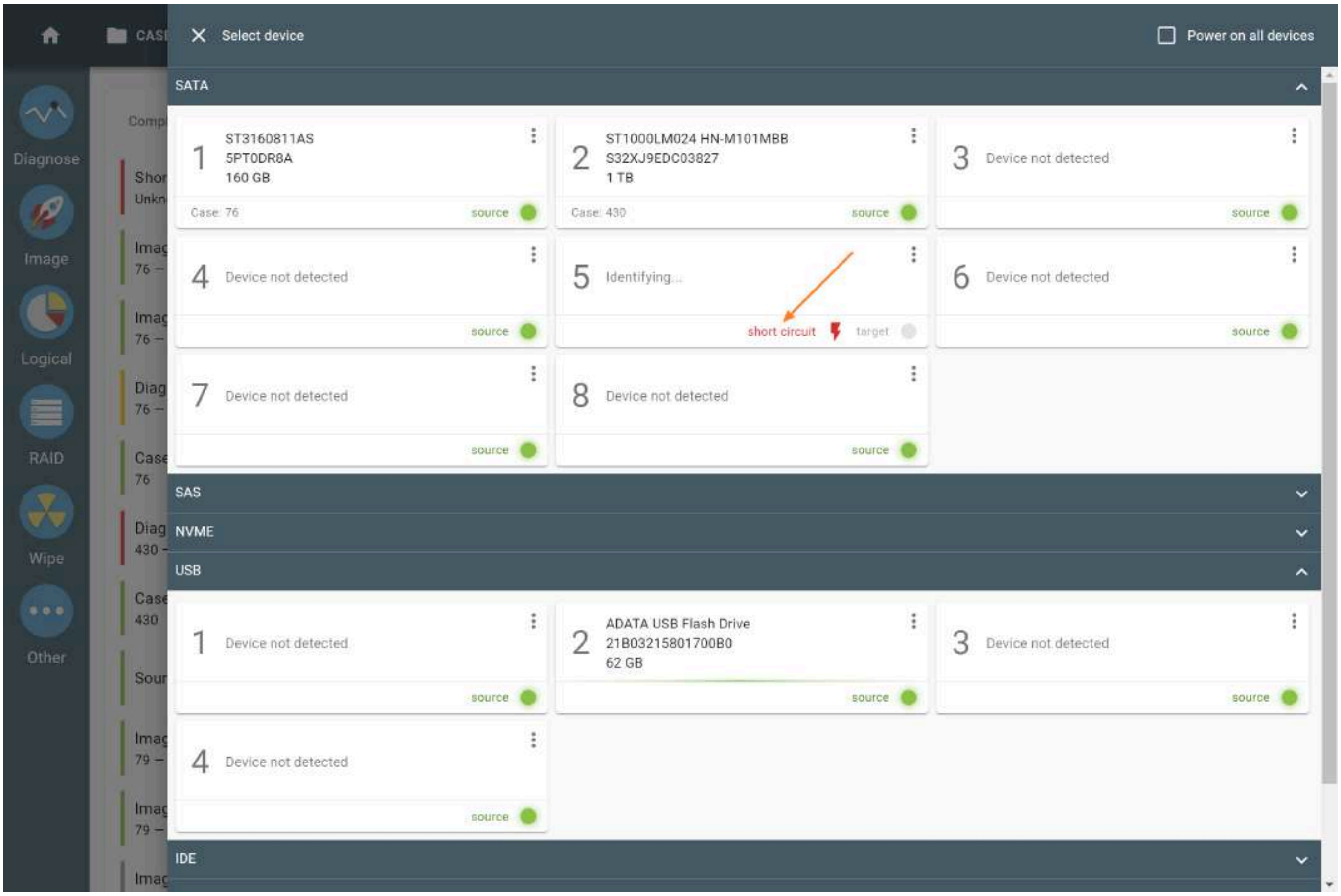
Imaging paused
96 — SATA 1 ST3750630AS 9QK1ZS5T
a day ago

Imaging resumed
96 — SATA 1 ST3750630AS 9QK1ZS5T
a day ago

Imaging paused
96 — SATA 1 ST3750630AS 9QK1ZS5T
a day ago

The Home screen with a short circuit alert.

On the **Select device** panel, TaskForce marks the port to which a shorted drive is connected with the **Short circuit** tag and icon.



SATA

1 ST3160811AS 5PT0DR8A 160 GB — Case: 76 — source

2 ST1000LM024 HN-M101MBB S32XJ9EDC03827 1 TB — Case: 430 — source

3 Device not detected — source

4 Device not detected — source

5 Identifying... — short circuit — target

6 Device not detected — source

7 Device not detected — source

8 Device not detected — source

USB

1 Device not detected — source

2 ADATA USB Flash Drive 21B03215801700B0 62 GB — source

3 Device not detected — source

4 Device not detected — source

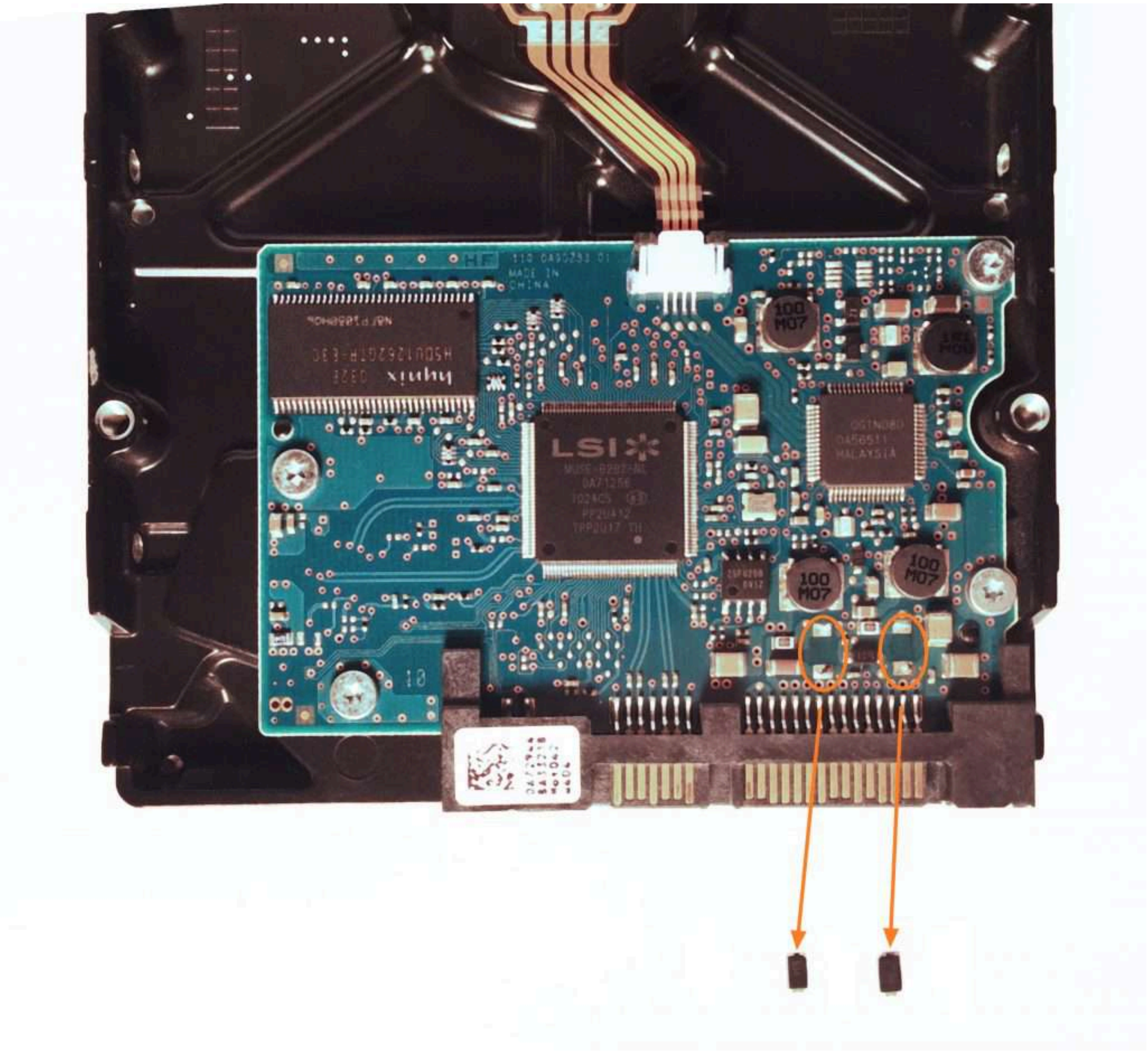
The Short circuit tag and icon on the Select device panel.

A drive with a shorted TVS diode cannot be identified, diagnosed, or imaged with TaskForce, until you replace or remove the diode.

Image a shorted drive

If you need to image a shorted drive but do not have new TVS diodes on hand to replace the shorted ones, you can image the drive using Atola TaskForce after removing the diodes. This process is safe because Atola TaskForce has short circuit and overvoltage protection, which guards both the imager and the drives connected to it against circuit failures.

To remove the diodes, heat the area of the drive where they are located with a hot fan (such as in a hot air soldering station) and then gently remove them with tweezers.



Once the diodes have been detached, you can plug the drive into Atola TaskForce and proceed with imaging data from it.

Express mode: self-launching imaging on 25 drive ports

Self-launching imaging mode is a perfect solution when it comes to processing large amounts of data under time pressure, while still allowing gentle treatment of damaged media.

Express mode enables the automatic launch of multiple imaging sessions with predefined settings on all drive ports set to source, except the Extension port (25 in total). Once an examiner plugs drives into TaskForce 2, imaging sessions start automatically. Drive images are saved as a RAW, E01, or AFF4 file in a specified folder on the local server. Two 10Gb Ethernet ports of TaskForce 2 enable high data throughput.

Additionally, there is the option to group ports in Express mode and assign different imaging settings for each group. TaskForce 2 can be set to automatically diagnose all source drives before imaging and proceed only if diagnostics show no issues.

In this article, you will learn how to:

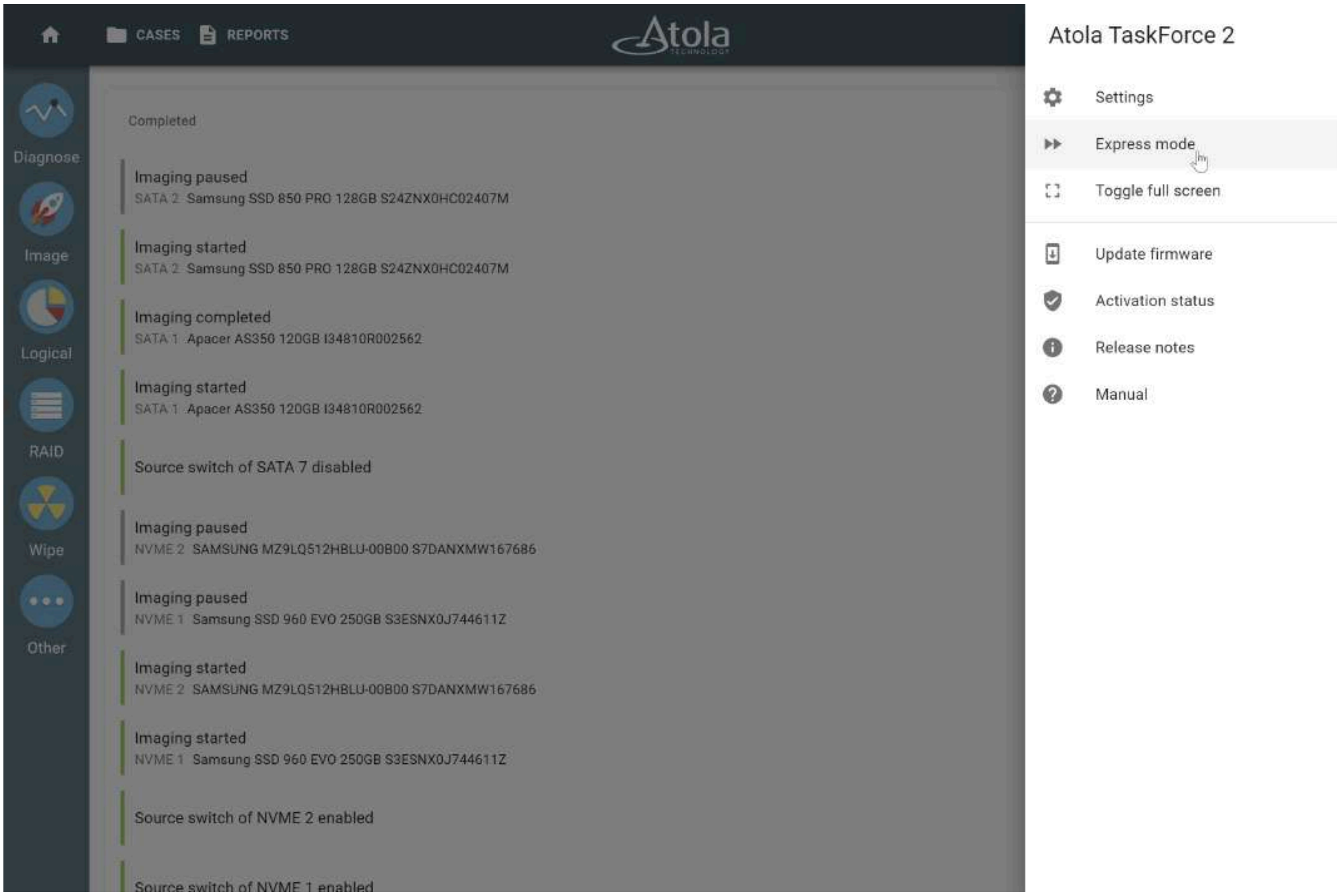
- Configure Express mode
- Activate Express mode
- Image drives in Express mode

- Deactivate Express mode

Configure Express mode

Before activating Express mode, you need to configure it first: specify the target folder, file image format, and other imaging details.

To open the Express mode settings page, click the **Menu** in the top right and select **Express mode**.



Completed

Imaging paused
SATA 2 Samsung SSD 850 PRO 128GB S24ZNX0HC02407M

Imaging started
SATA 2 Samsung SSD 850 PRO 128GB S24ZNX0HC02407M

Imaging completed
SATA 1 Apacer AS350 120GB I34810R002562

Imaging started
SATA 1 Apacer AS350 120GB I34810R002562

Source switch of SATA 7 disabled

Imaging paused
NVME 2 SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686

Imaging paused
NVME 1 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z

Imaging started
NVME 2 SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686

Imaging started
NVME 1 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z

Source switch of NVME 2 enabled

Source switch of NVME 1 enabled

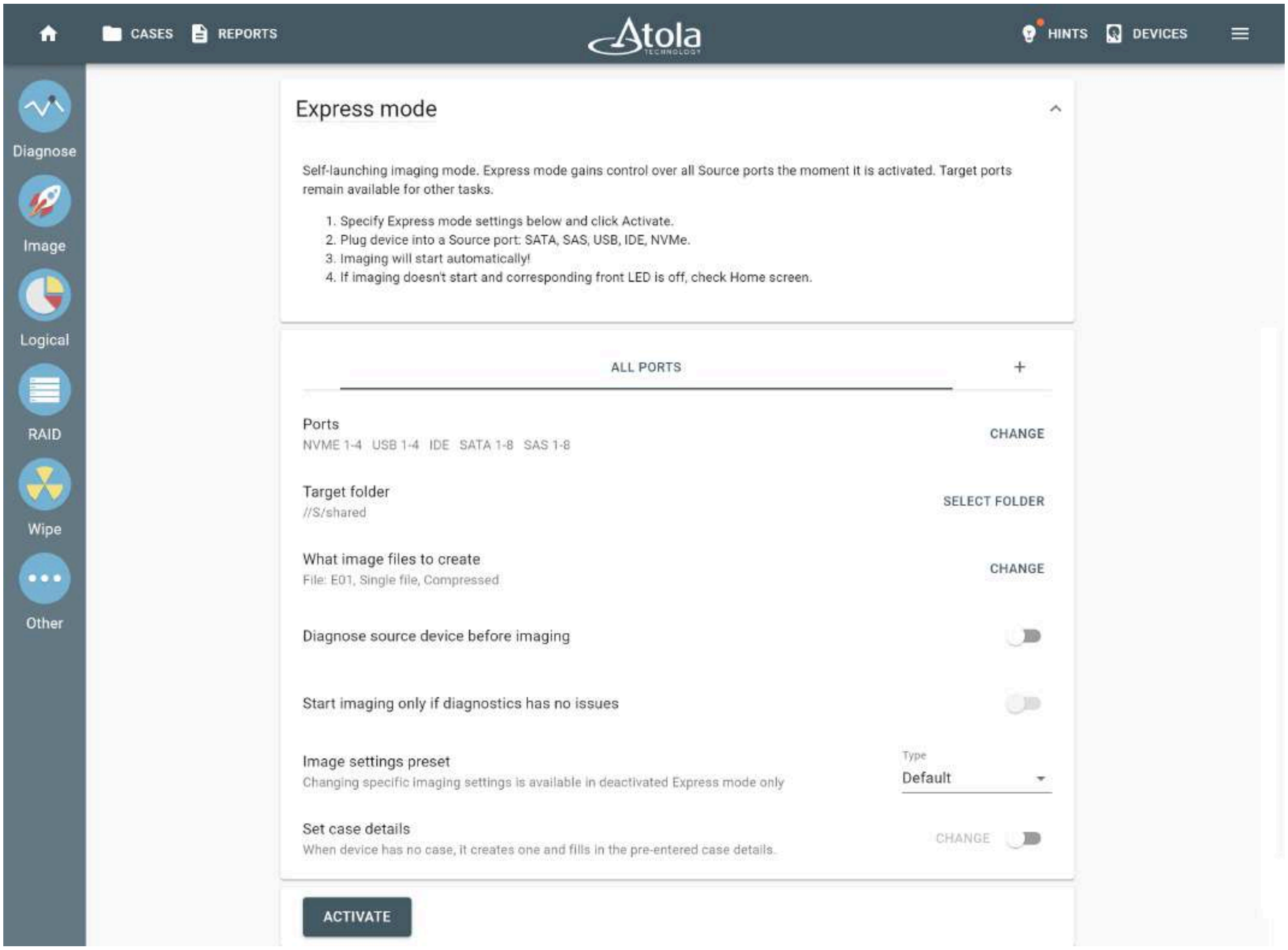
Choosing Express mode from the Menu.

TaskForce 2 can process 25 self-launching imaging sessions in Express mode on almost all of its ports, except for the Extension slot. The ports that can be used for imaging in Express mode are:

- 4 NVMe M.2/U.2
- 8 SATA
- 8 SATA/SAS
- 4 USB
- 1 IDE

When activated, Express mode controls all source ports, leaving target ones available for other tasks. If a port is switched from target to source, it also becomes available for imaging in Express mode.

By default, Express mode settings are applied to all drive ports set to source. However, you can combine any number of TaskForce ports into a custom group with specific imaging parameters for Express mode. See Port groups for details.



Express mode

Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

ALL PORTS +

Ports
NVME 1-4 USB 1-4 IDE SATA 1-8 SAS 1-8 — CHANGE

Target folder
//S/shared — SELECT FOLDER

What image files to create
File: E01, Single file, Compressed — CHANGE

Diagnose source device before imaging

Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only — Type: Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details. — CHANGE

ACTIVATE

Express mode settings.

Port groups

In cases where different types of drives require different approaches to image acquisition, you can assign specific imaging settings for certain groups of drive ports in Express mode.

For example, to balance image acquisition time, you can image new NVMe drives to your faster server and older/smaller SATA drives to slower storage. Or image healthy drives to the “Good” network folder and faulty ones to the “Bad” network folder to treat them differently later.

In Express mode, for each custom group of drive ports, you can specify:

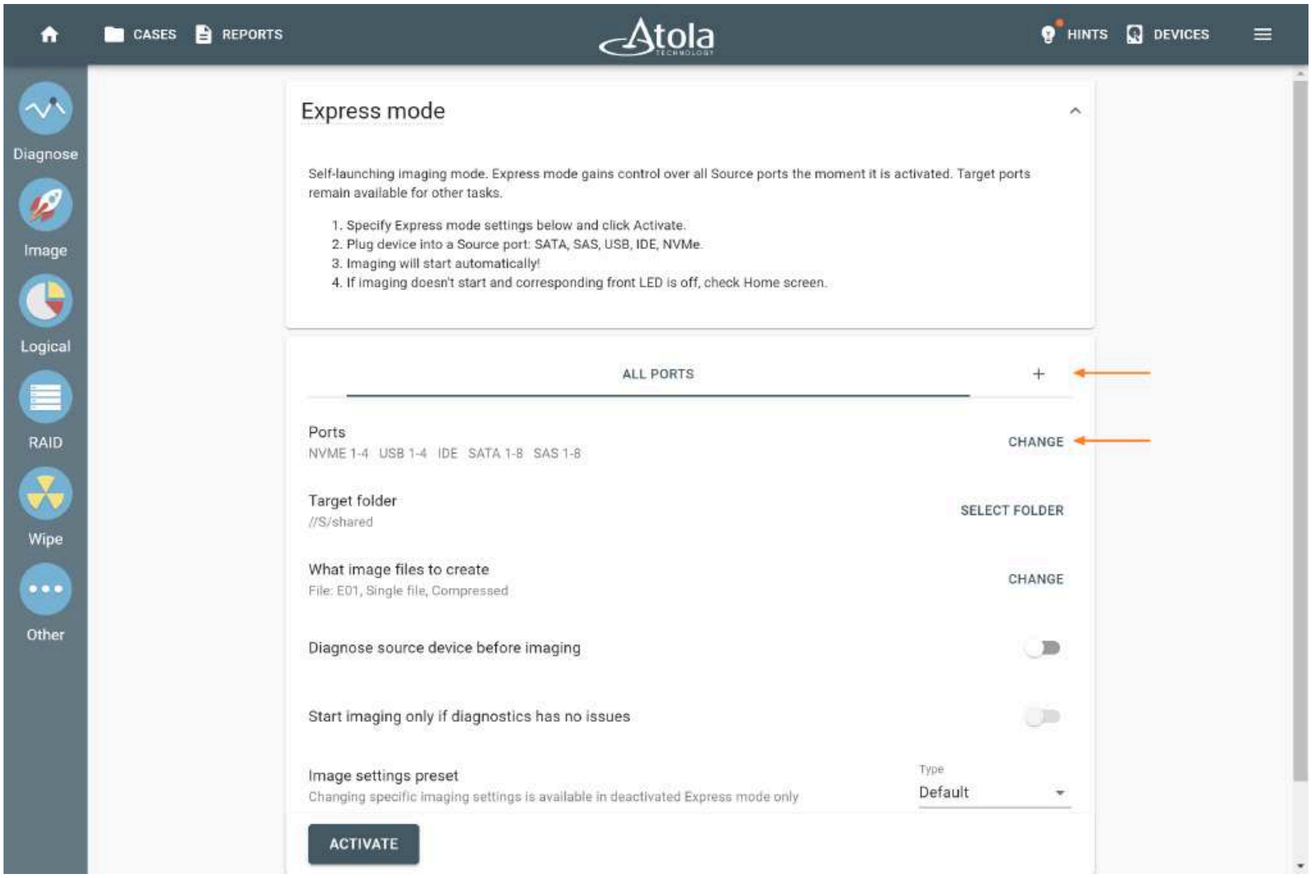
- Network folder where to save an image file
- Which image file format to use
- Which type of hash to calculate
- Whether to diagnose the source device before imaging
- How to fill in case report fields: Case ID, Organization, Investigator

Add a new group of ports

By default, Express mode settings are applied to all drive ports set to source. Thus, the group tab on the Express mode settings page is named **All ports**. All the ports included in the group are listed in the **Ports** section.

To add a new group of ports:

1. Next to the **All ports** group tab, click the **Plus** icon.



Express mode

Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

ALL PORTS +

Ports
NVME 1-4 USB 1-4 IDE SATA 1-8 SAS 1-8
CHANGE

Target folder
//S/shared
SELECT FOLDER

What image files to create
File: E01, Single file, Compressed
CHANGE

Diagnose source device before imaging

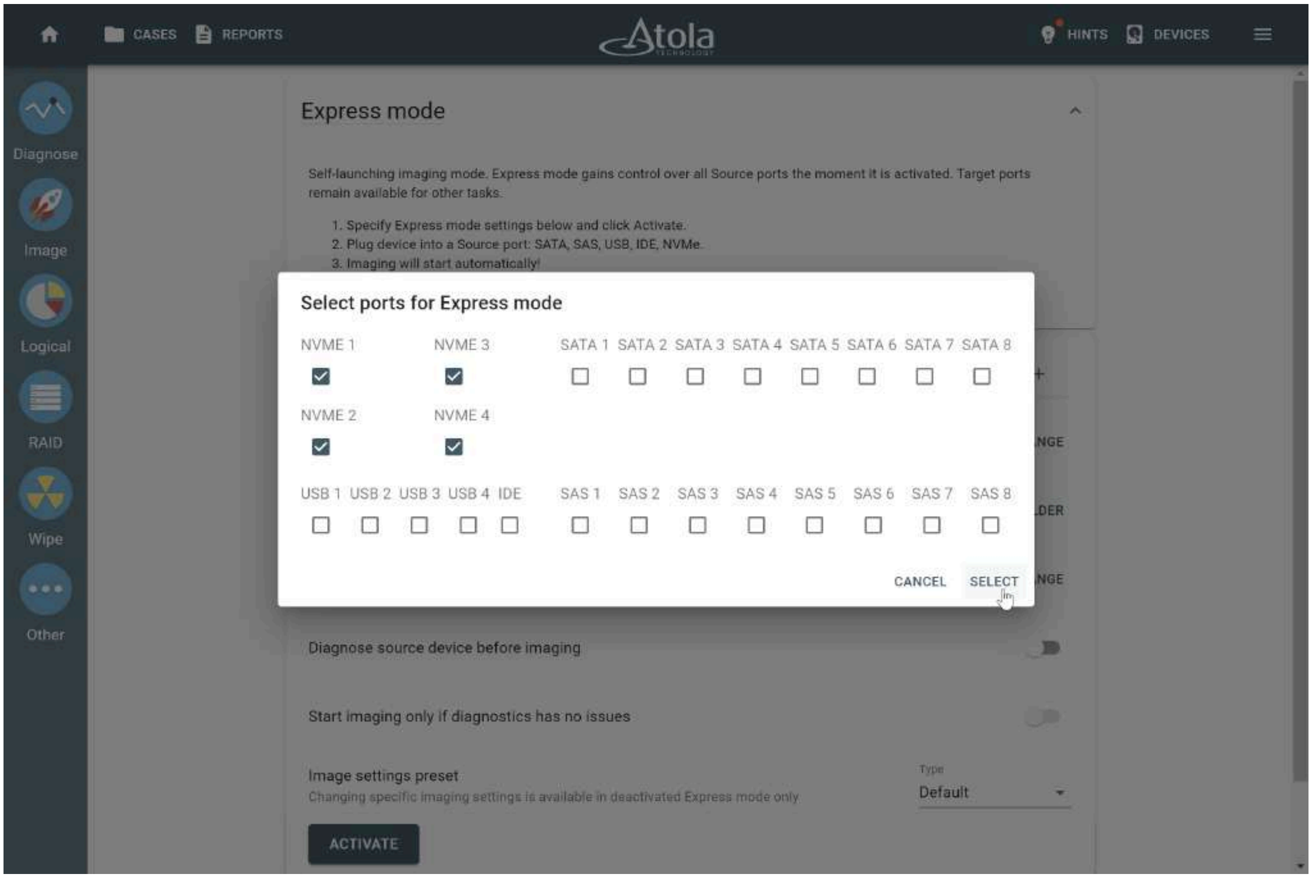
Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only
Type
Default

ACTIVATE

The All ports group tab and the Plus icon.

2. In the dialog window, select ports for the new group.



Express mode

Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!

Select ports for Express mode

NVME 1	NVME 3	SATA 1	SATA 2	SATA 3	SATA 4	SATA 5	SATA 6	SATA 7	SATA 8
☑	☑	□	□	□	□	□	□	□	□
NVME 2	NVME 4								
☑	☑								

USB 1	USB 2	USB 3	USB 4	IDE	SAS 1	SAS 2	SAS 3	SAS 4	SAS 5	SAS 6	SAS 7	SAS 8
□	□	□	□	□	□	□	□	□	□	□	□	□

CANCEL SELECT

Diagnose source device before imaging

Start imaging only if diagnostics has no issues

Image settings preset

Changing specific imaging settings is available in deactivated Express mode only

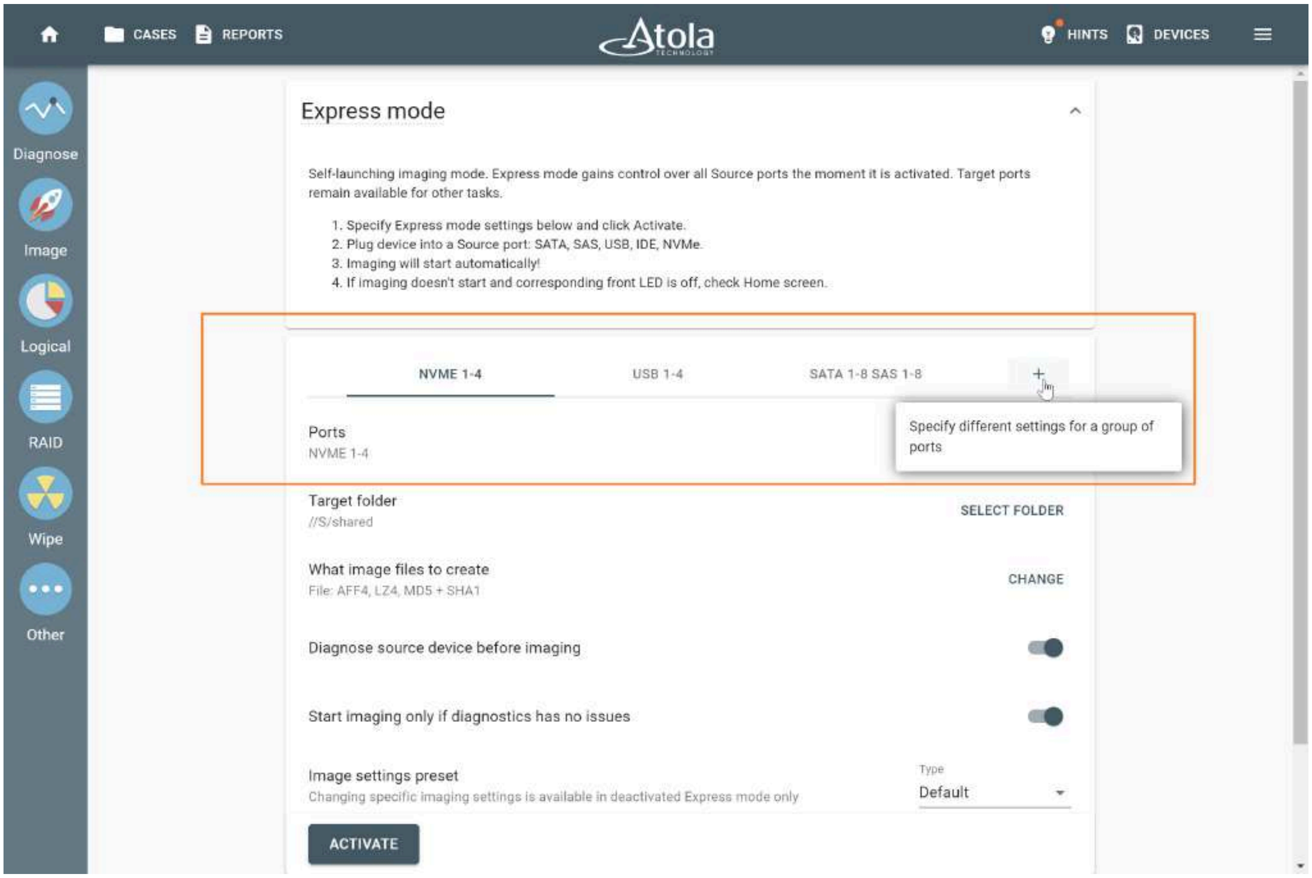
Type: Default

ACTIVATE

Selecting ports for the new group.

3. Click **Select**.

To avoid confusion and accidental mistakes, TaskForce excludes selected ports from any existing groups and adds them to the new one.



Express mode

Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

NVME 1-4 | USB 1-4 | SATA 1-8 SAS 1-8 | +

Specify different settings for a group of ports

Ports
NVME 1-4

Target folder
//S/shared
SELECT FOLDER

What image files to create
File: AFF4, LZ4, MD5 + SHA1
CHANGE

Diagnose source device before imaging

Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only
Type
Default

ACTIVATE

Several port groups in the Express mode settings.

4. The group name changes to clearly show port types and numbers included in it, for example, "**NVME 1-4**" or "**SATA 1-8 SAS 1-8**". Switch between port groups by clicking the tab with the group name.

Now you can proceed with assigning different imaging settings in Express mode to different port groups.

Change a port group

To change the drive ports included in an existing port group:

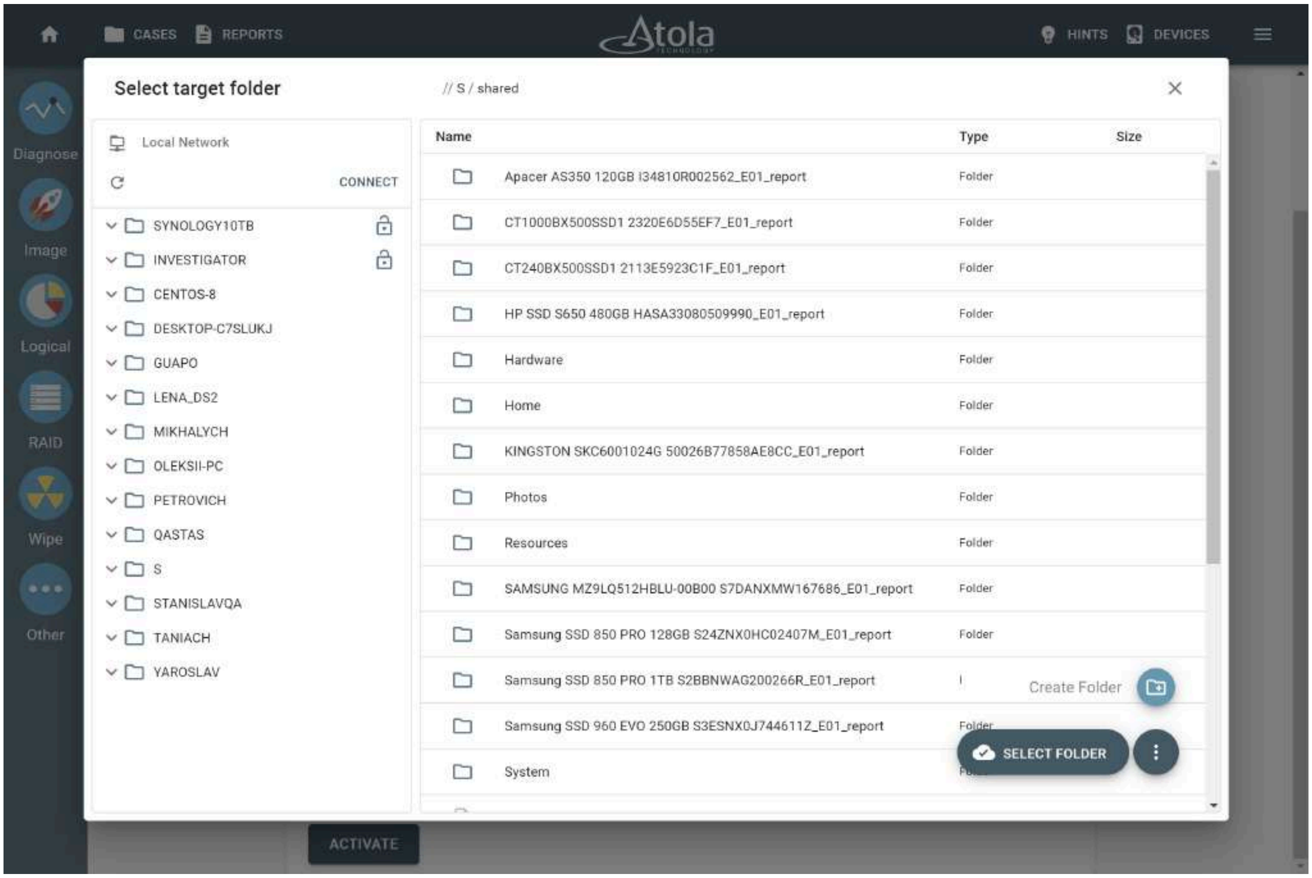
1. On the Express mode settings page, switch to the port group you want to change by clicking on the tab with its name.
2. On the right, click **Change**.
3. In the dialog window, select the drive ports you want to include in the group or deselect the drive ports you want to exclude.
4. Click **Select**.
5. The group name changes to clearly show port types and numbers included in it.

Target folder

In Express mode, TaskForce 2 stores drive images on a local server.

To activate Express mode, you need to specify a target folder on a local network to store drive images:

1. On the Express mode settings page, find the **Target folder** section and click **Select folder**.
2. In the **Select target folder** window, go to the existing folder and click the **Select folder** button. To create a new folder, click the icon with three dots and select **Create folder**.



Select target folder

// S / shared

- SYNOLOGY10TB
- INVESTIGATOR
- CENTOS-8
- DESKTOP-C7SLUKJ
- GUAPO
- LENA_DS2
- MIKHALYCH
- OLEKSII-PC
- PETROVICH
- QASTAS
- S
- STANISLAVQA
- TANIACH
- YAROSLAV

Name	Type	Size
Apacer AS350 120GB I34810R002562_E01_report	Folder	
CT1000BX500SSD1 2320E6D55EF7_E01_report	Folder	
CT240BX500SSD1 2113E5923C1F_E01_report	Folder	
HP SSD S650 480GB HASA33080509990_E01_report	Folder	
Hardware	Folder	
Home	Folder	
KINGSTON SKC6001024G 50026B77858AE8CC_E01_report	Folder	
Photos	Folder	
Resources	Folder	
SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686_E01_report	Folder	
Samsung SSD 850 PRO 128GB S24ZNX0HC02407M_E01_report	Folder	
Samsung SSD 850 PRO 1TB S2BBNWAG200266R_E01_report		
Samsung SSD 960 EVO 250GB S3ESNX0J744611Z_E01_report	Folder	
System	Fo	

The 'Select target folder' window.

What image files to create: type, compression, hash, templates and more

To set up the parameters of a target image file, such as file type, compression method, segment size, and hash type, on the Express mode settings page, find the **What image file to create** section and click **Change**.

Configuration dialog appears.

On the **File** tab of this dialog, configure the target image file.

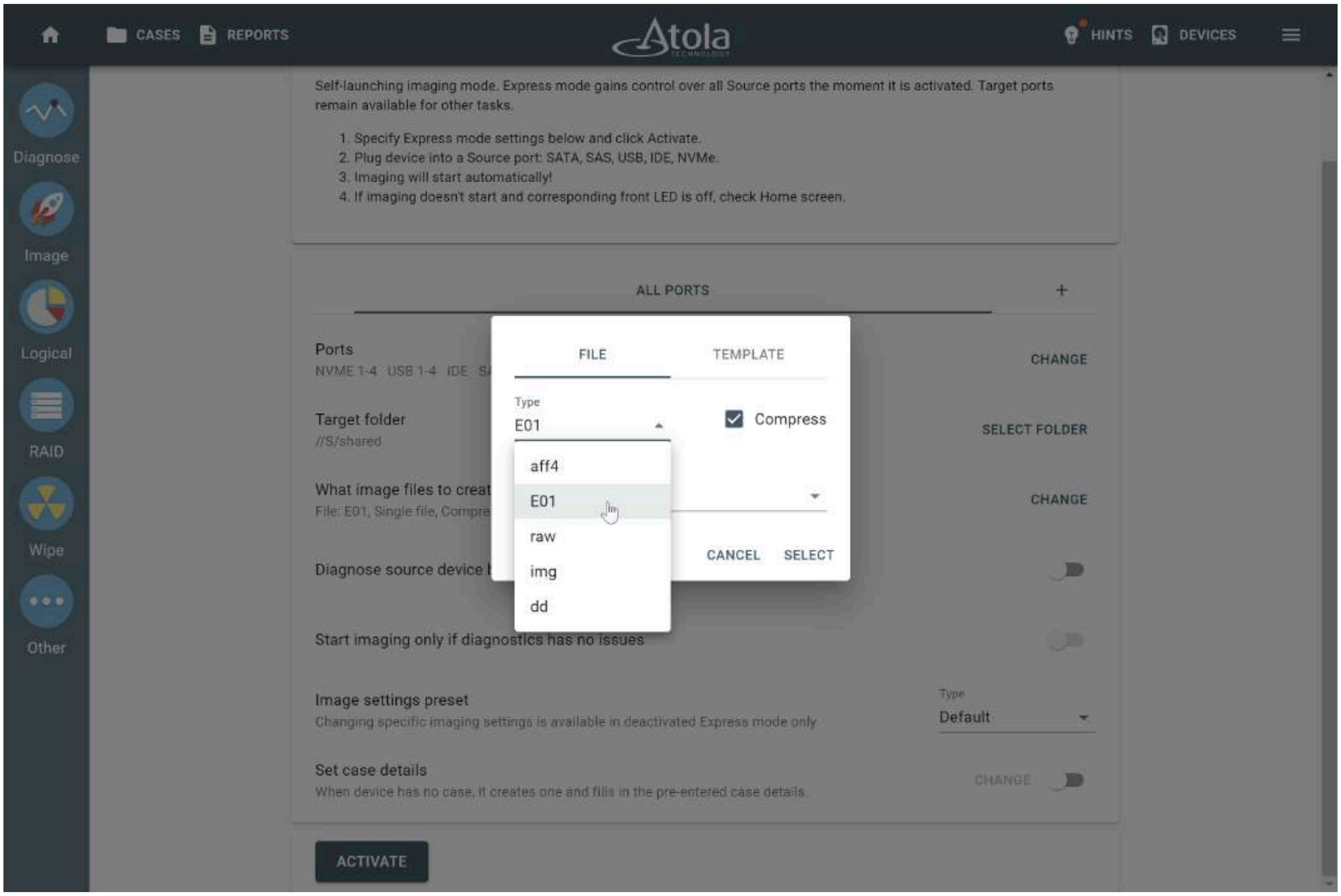
On the **Template** tab, you can also create the templates for image file names.

Selected parameters apply to an active port group only. Here are the details about each parameter.

Image file type

In Express mode, drive images can be saved as RAW, E01, or AFF4 files.

To change the target image file type for a specific group of ports, select it from the **Type** list on the **File** tab.



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

Ports
NVME 1-4 USB 1-4 IDE S

Type
E01

☑ Compress

Target folder
//S/shared

What image files to creat
File: E01, Single file, Compre

Diagnose source device

Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only
Type
Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details.

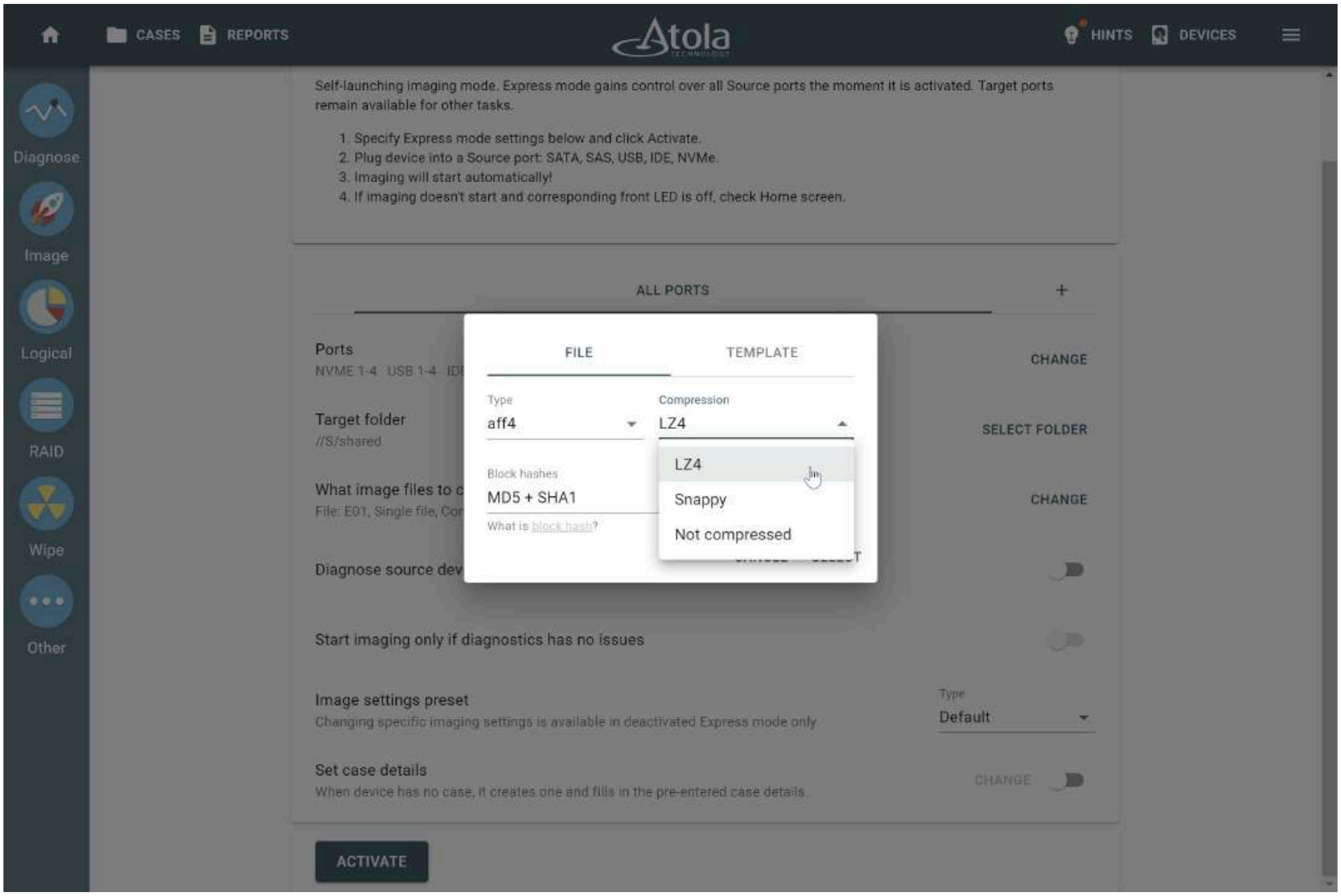
Selecting target image file type.

Compression

TaskForce 2 supports the default compression method for the E01 file format and LZ4 or Snappy compression methods for the AFF4 file format.

Choose the compression method from the respective list on the **File** tab. The **Not compressed** option is also available for both E01 and AFF4.

The RAW file format does not support compression.



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

Ports
NVME 1-4 USB 1-4 IDE

Target folder
//S/shared

What image files to c
File: E01, Single file, Cor

Type: aff4

Compression: LZ4

- LZ4
- Snappy
- Not compressed

Block hashes: MD5 + SHA1

What is block hash?

Diagnose source dev

Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only

Type: Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details.

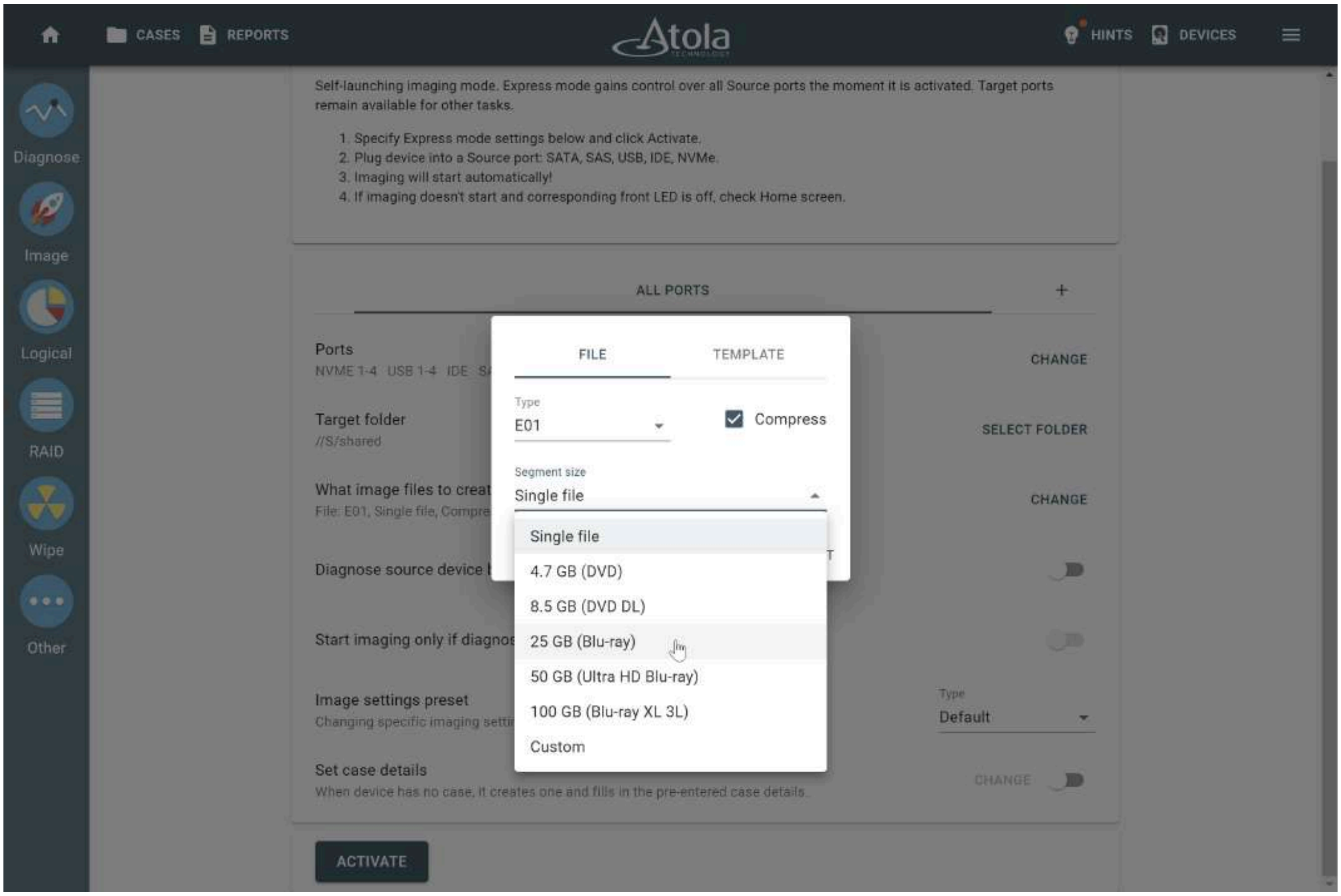
Selecting the compression method for a target image file.

Segment size

For the E01 file format, TaskForce 2 can split the target image into segments of predefined size. Each segment is stored in a specified folder as a separate file.

The **Segment size** list becomes available on the **File** tab when the E01 file type is selected. You can choose the segment size from the following options:

- Single file
- 4.7 GB (DVD)
- 8.5 GB (DVD DL)
- 25 GB (Blu-ray)
- 50 GB (Ultra HD Blu-ray)
- 100 GB (Blu-ray XL 3L)
- Custom (enter the segment size you want)



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

Ports
NVME 1-4 USB 1-4 IDE SA

Target folder
//S/shared

What image files to creat
File: E01, Single file, Compre

Diagnose source device b

Start imaging only if diagnos

Image settings preset
Changing specific imaging setti

Type: Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details.

Type: E01

☑ Compress

Segment size: Single file

- Single file
- 4.7 GB (DVD)
- 8.5 GB (DVD DL)
- 25 GB (Blu-ray)
- 50 GB (Ultra HD Blu-ray)
- 100 GB (Blu-ray XL 3L)
- Custom

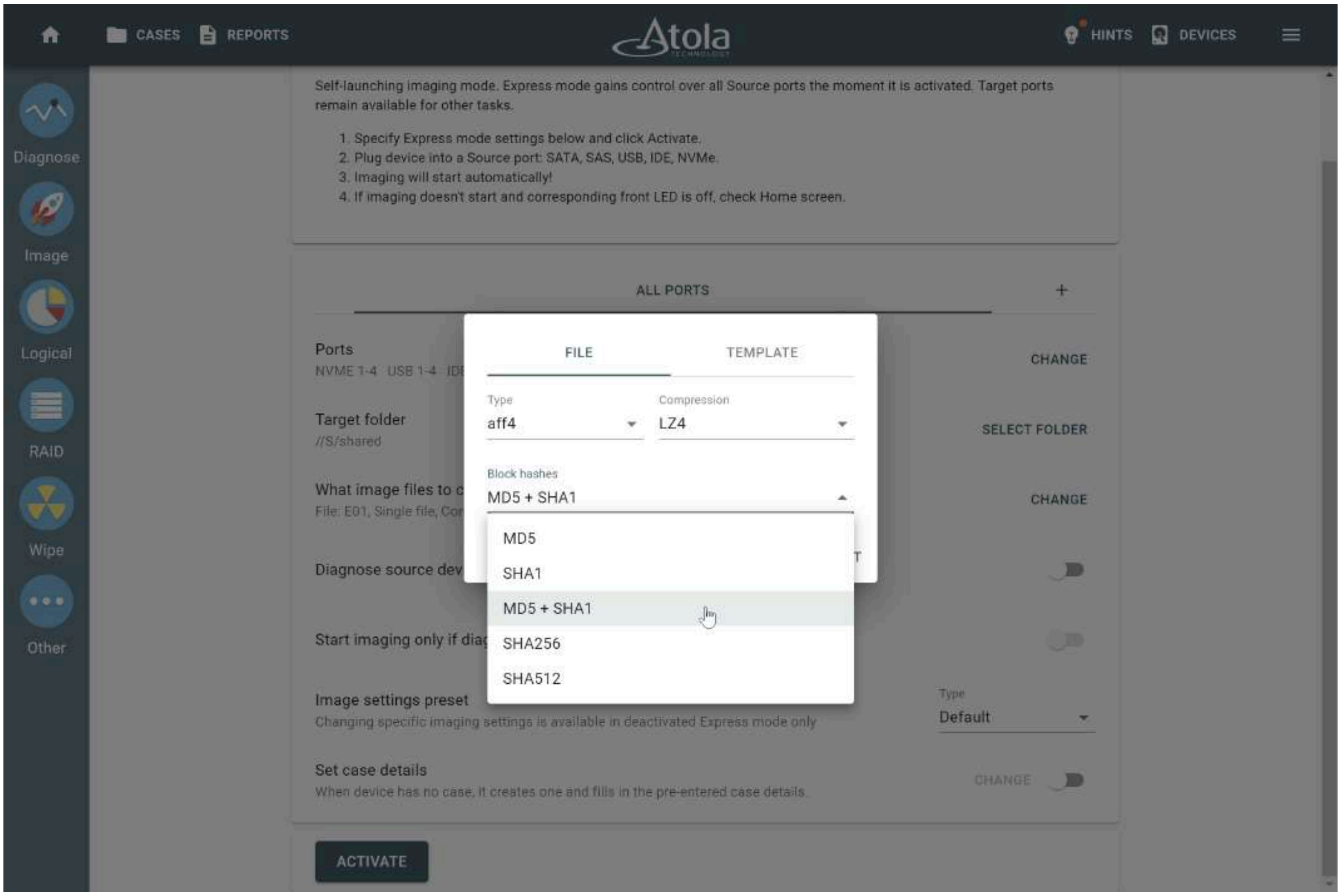
Selecting the segment size for a target image file.

Hash type

For AFF4 file format, TaskForce 2 can calculate built-in block hashes during the imaging process in the Express mode.

To select the hash type you want to calculate, use the **Block hash** list on the **File** tab. The available hashing options for the AFF4 file format are:

- MD5
- SHA1
- MD5+SHA1
- SHA256
- SHA512



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

Ports
NVME 1-4 USB 1-4 IDE

Target folder
//S/shared

What image files to c
File: E01, Single file, Cor

Diagnose source dev

Start imaging only if diag

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only

Type: Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details.

Type: aff4

Compression: LZ4

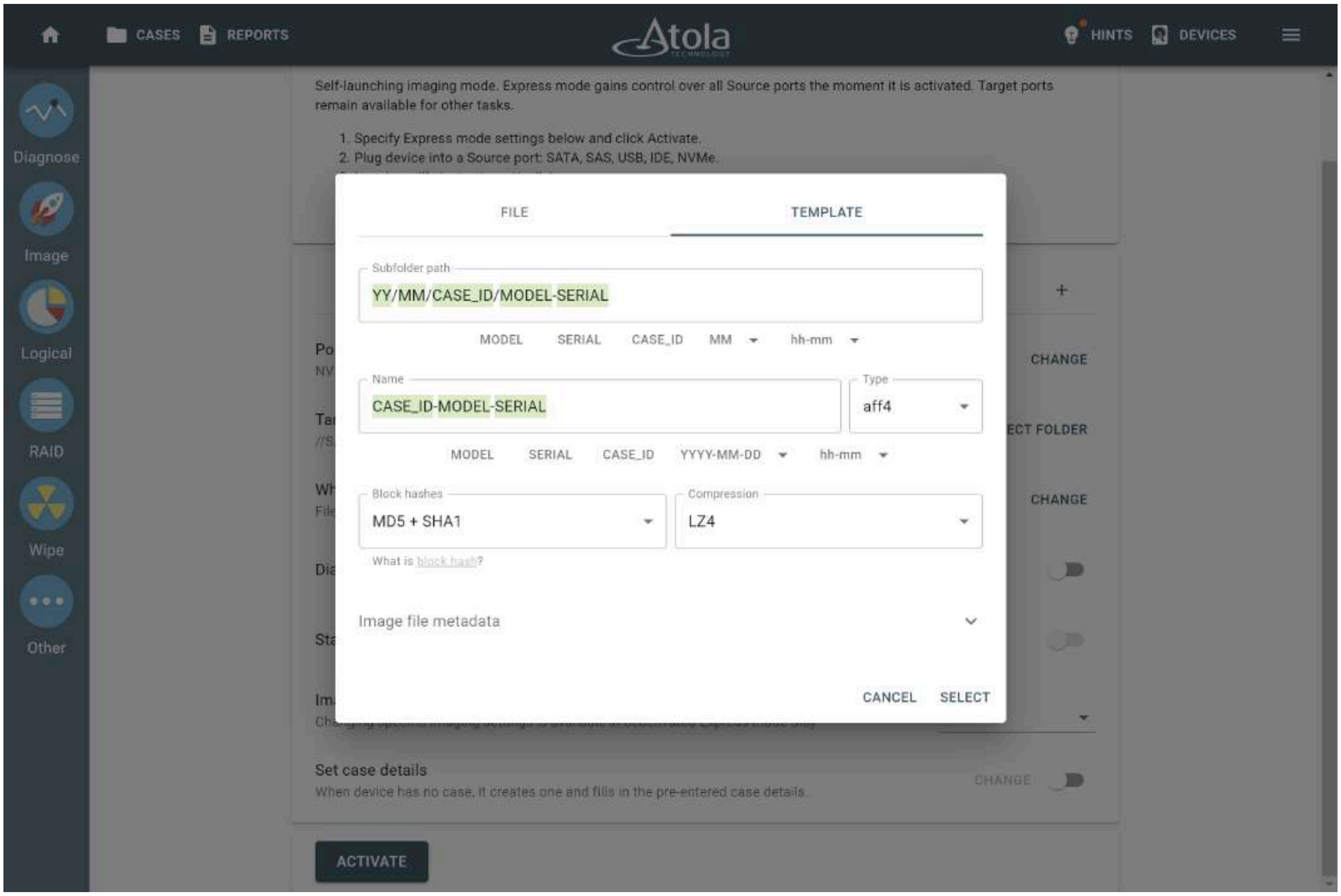
Block hashes: MD5 + SHA1

- MD5
- SHA1
- MD5 + SHA1
- SHA256
- SHA512

Selecting the hash type for a target image file.

Create template for image file names

To create a template for naming target subfolders and files according to your organization rules, find the **What image file to create** section, click **Change**, and switch to the **Template** tab. For details, see Target file templates.



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.

Subfolder path: YY/MM/CASE_ID/MODEL-SERIAL

Name: CASE_ID-MODEL-SERIAL

Type: aff4

Block hashes: MD5 + SHA1

Compression: LZ4

What is block hash?

Image file metadata

Set case details

When device has no case, it creates one and fills in the pre-entered case details.

Creating a template for a target image files names in Express mode.

Diagnose before imaging and Start imaging only if diagnostics has no issues

As essential as imaging speed is, the proper treatment of evidence drives remains a priority. That's why we recommend that diagnostics is always performed as soon as a drive is connected to TaskForce 2 for the first time.

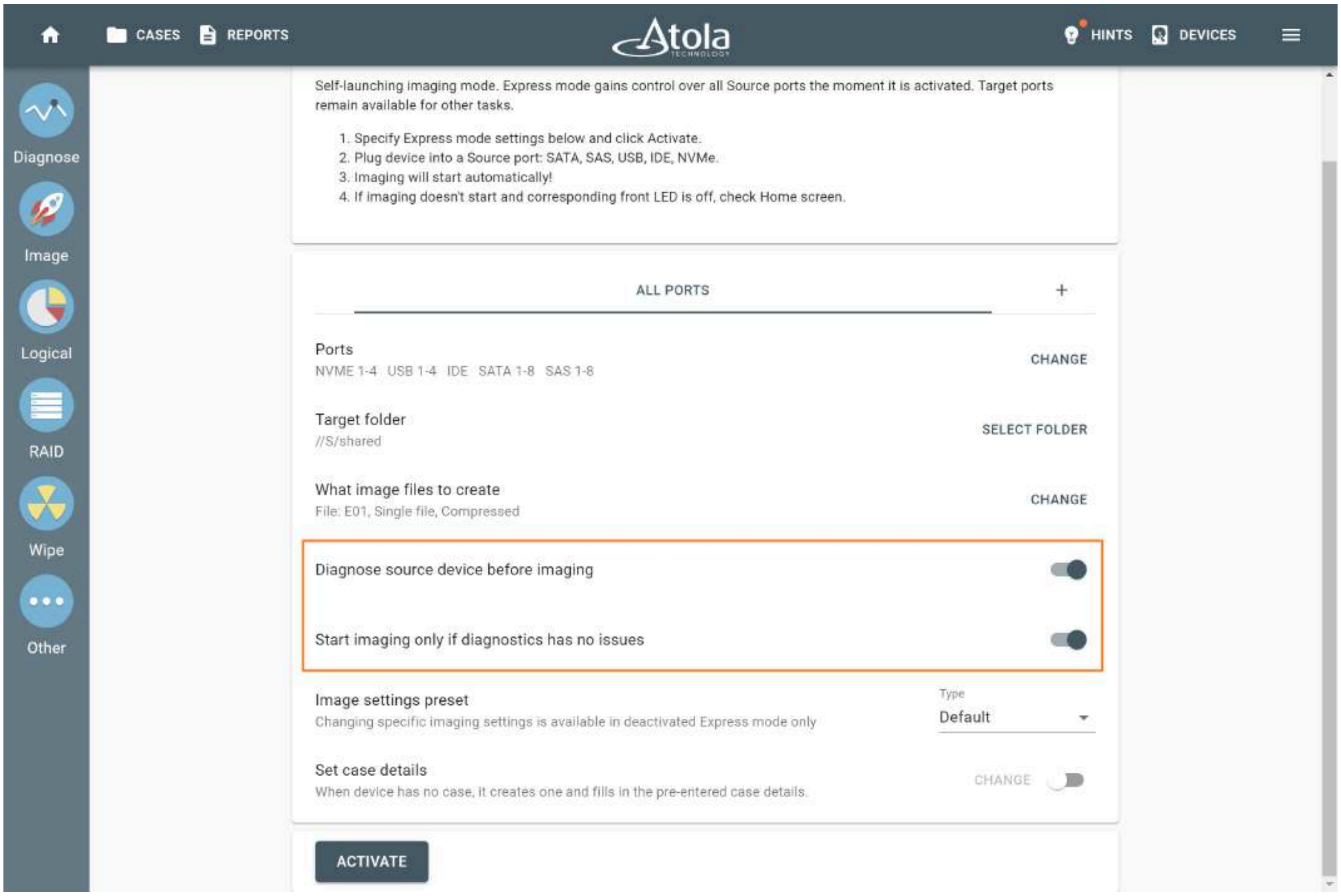
To enable the automatic launch of imaging of the healthy devices and avoid potential deterioration of drives in a shaky condition, the Express mode settings have two handy options:

- select **Diagnose source drive before imaging** so that diagnostics start automatically,
- then select **Start imaging only if diagnostics has no issues**.

When enabled in Express mode, Atola's signature automated diagnostics module checks all drive systems:

- hard drive's motor and electronics (PCB),
- head stack,
- media surface,
- all firmware/system areas,
- partitions and file systems.

For more information about TaskForce's diagnostics module, see Diagnosing a drive with Atola TaskForce 2.



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

Ports
NVME 1-4 USB 1-4 IDE SATA 1-8 SAS 1-8

Target folder
//S/shared

What image files to create
File: E01, Single file, Compressed

Diagnose source device before imaging

Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only
Type: Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details.

Diagnostics options for Express mode.

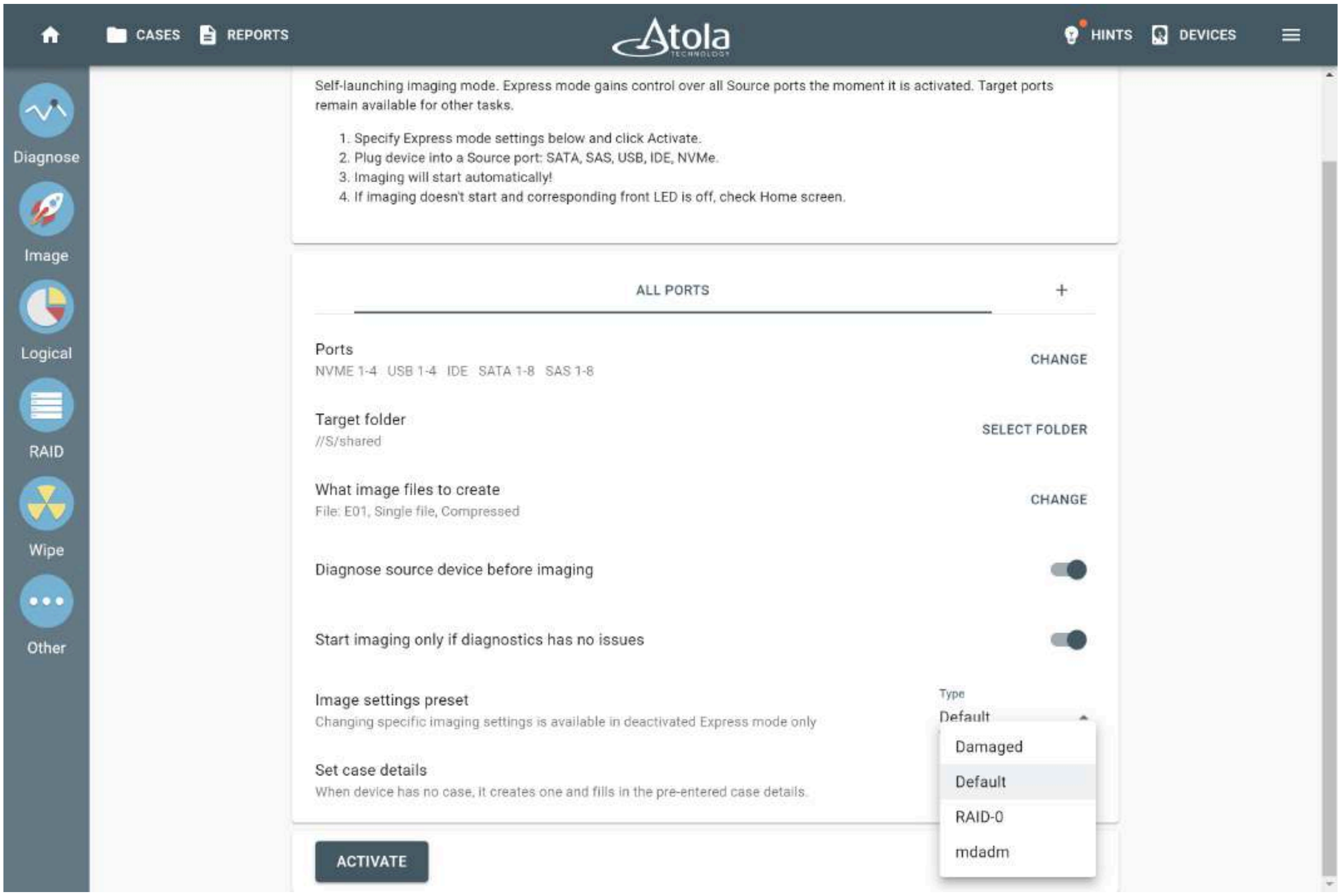
Imaging presets

To ensure that all imaging sessions in Express mode fit your organization's demands and procedures, in Express mode you can use one of the preconfigured imaging presets.

TaskForce 2 has two built-in imaging presets, *Default* and *Damaged*, for good and bad drives respectively, but you can also create and configure your own preset. For guidance, see Imaging presets.

To select an imaging preset for Express mode, use the **Type** list in the **Imaging settings preset** section.

Changing the imaging preset is available only when Express mode is deactivated.



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

Ports
NVME 1-4 USB 1-4 IDE SATA 1-8 SAS 1-8

Target folder
//S/shared

What image files to create
File: E01, Single file, Compressed

Diagnose source device before imaging

Start imaging only if diagnostics has no issues

Image settings preset
Changing specific imaging settings is available in deactivated Express mode only

Type
Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details.

The 'Type' list in the 'Imaging settings preset' section.

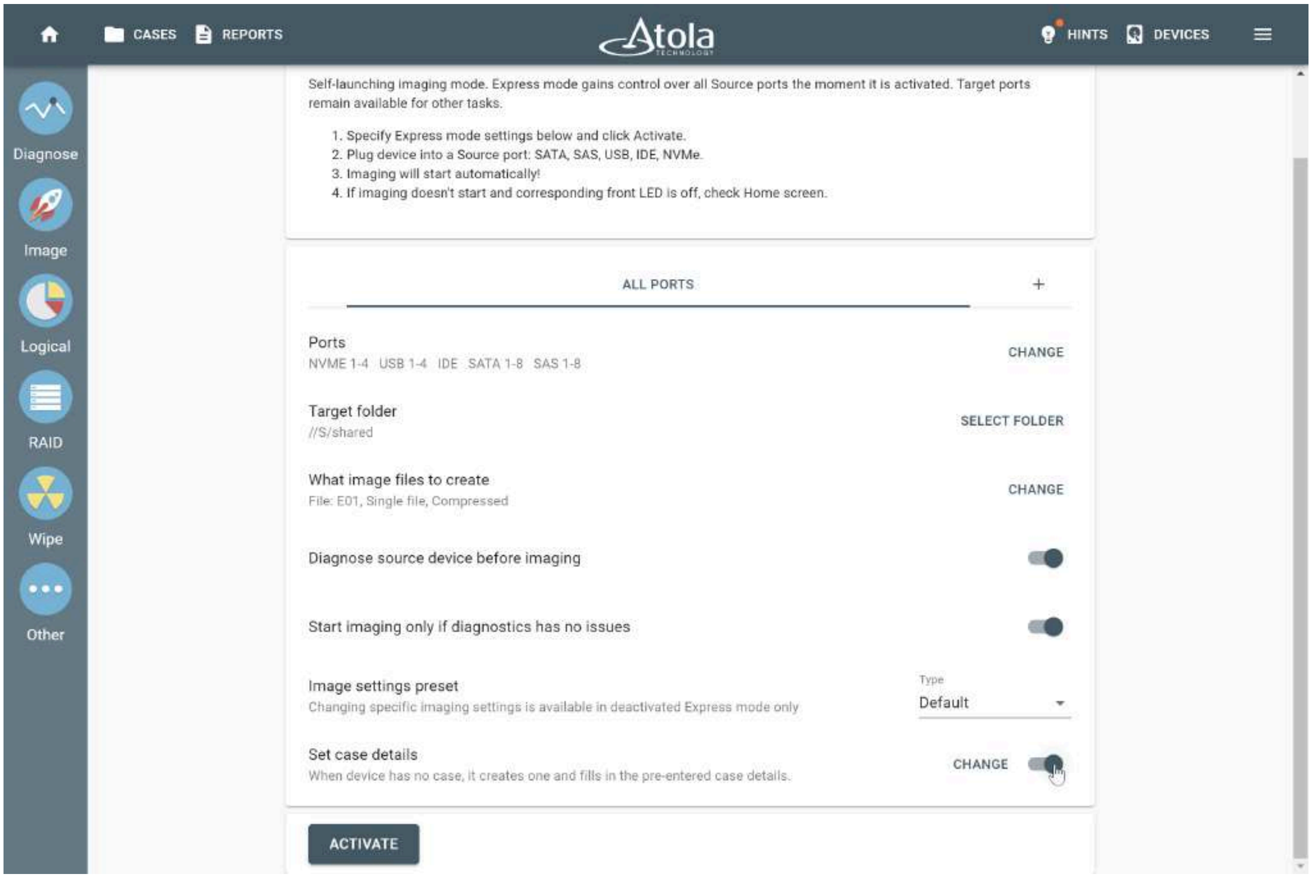
Set case details

To streamline your acquisition workflow in the Express mode, you can pre-fill case details for each evidence drive using predefined information:

- Case ID
- Investigator’s name
- Organization
- Location
- Description

To enter predefined case details for Express mode and allow filling them up:

1. On the Express mode settings page, go to the **Set case details** section and toggle this option on.



Self-launching imaging mode. Express mode gains control over all Source ports the moment it is activated. Target ports remain available for other tasks.

1. Specify Express mode settings below and click Activate.
2. Plug device into a Source port: SATA, SAS, USB, IDE, NVMe.
3. Imaging will start automatically!
4. If imaging doesn't start and corresponding front LED is off, check Home screen.

ALL PORTS +

Ports
NVME 1-4 USB 1-4 IDE SATA 1-8 SAS 1-8 — CHANGE

Target folder
//S/shared — SELECT FOLDER

What image files to create
File: E01, Single file, Compressed — CHANGE

Diagnose source device before imaging

Start imaging only if diagnostics has no issues

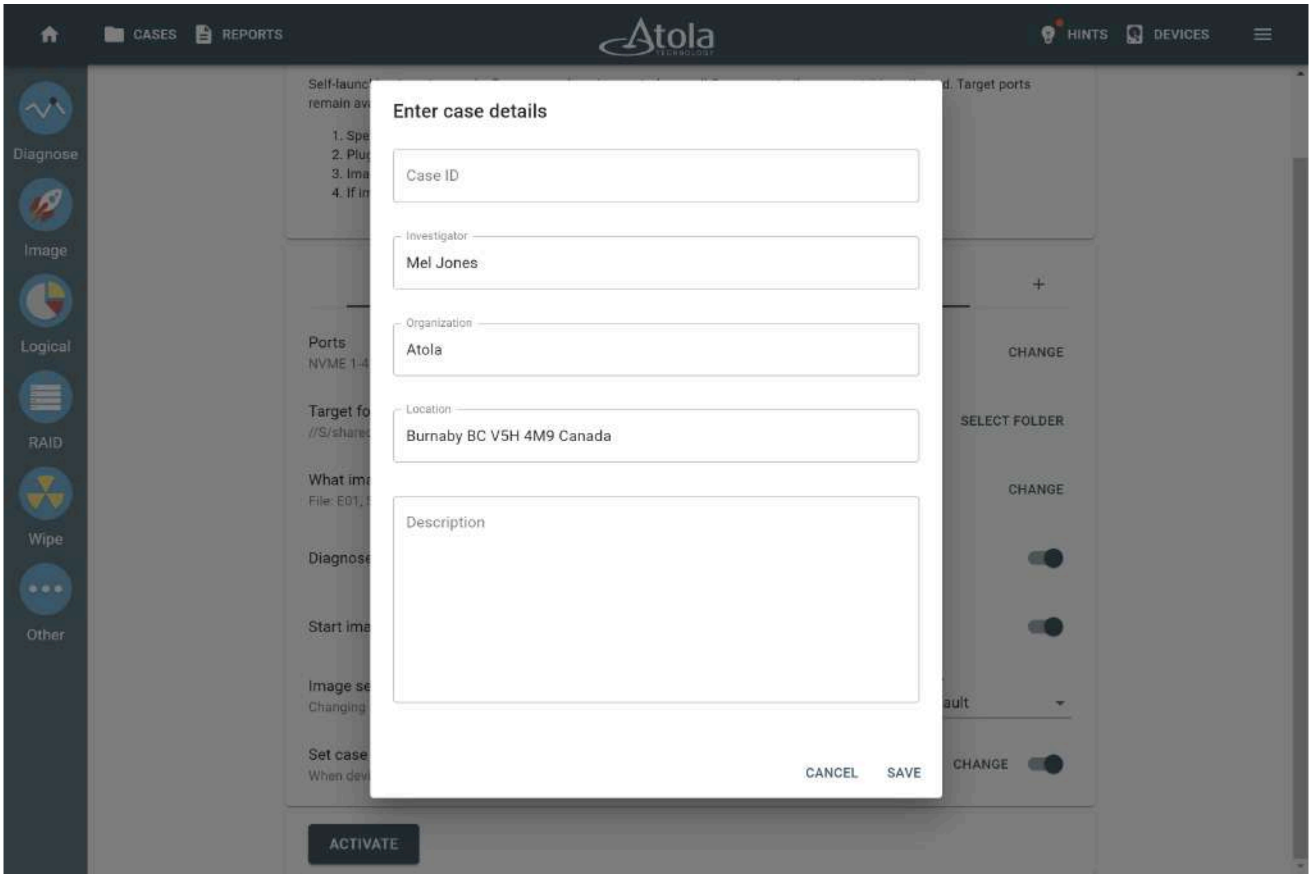
Image settings preset
Changing specific imaging settings is available in deactivated Express mode only
Type: Default

Set case details
When device has no case, it creates one and fills in the pre-entered case details. — CHANGE

ACTIVATE

2. Click **Change**.

3. In the dialog window, enter case details and click **Save**.



Enter case details

Case ID

Investigator: Mel Jones

Organization: Atola

Location: Burnaby BC V5H 4M9 Canada

Description

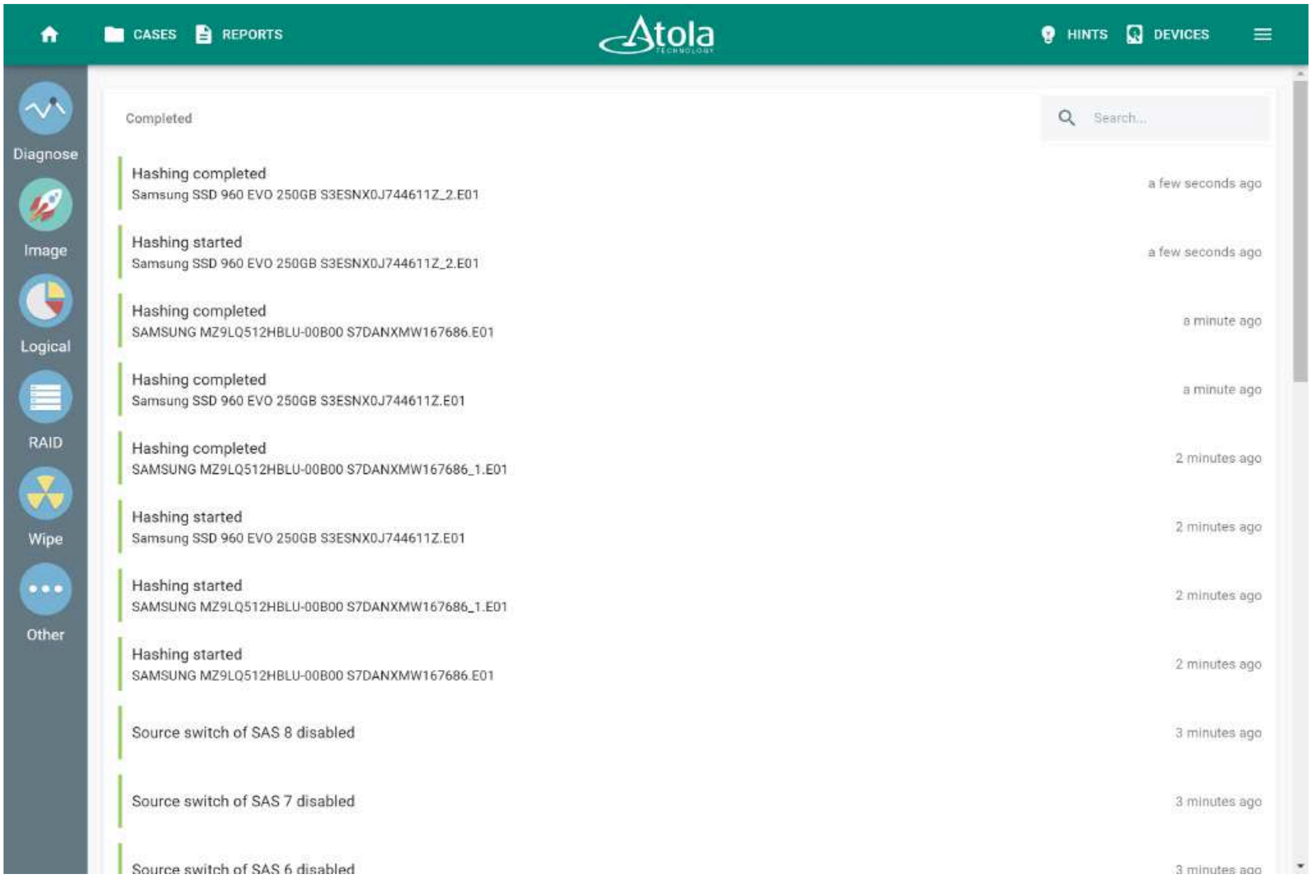
Activate Express mode

Once Express mode settings are specified, click the **Activate** button and connect your evidence drives for an immediate start of imaging.

If any drives are already connected to the source ports, TaskForce starts to image those devices immediately using Express mode settings once you click **Activate**.

To indicate that TaskForce now operates in Express mode:

1. In the user interface, the color of the top panel and the Image icon on the left changes.



Completed

Hashing completed Samsung SSD 960 EVO 250GB S3ESNX0J744611Z_2.E01	a few seconds ago
Hashing started Samsung SSD 960 EVO 250GB S3ESNX0J744611Z_2.E01	a few seconds ago
Hashing completed SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686.E01	a minute ago
Hashing completed Samsung SSD 960 EVO 250GB S3ESNX0J744611Z.E01	a minute ago
Hashing completed SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686_1.E01	2 minutes ago
Hashing started Samsung SSD 960 EVO 250GB S3ESNX0J744611Z.E01	2 minutes ago
Hashing started SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686_1.E01	2 minutes ago
Hashing started SAMSUNG MZ9LQ512HBLU-00B00 S7DANXMW167686.E01	2 minutes ago
Source switch of SAS 8 disabled	3 minutes ago
Source switch of SAS 7 disabled	3 minutes ago
Source switch of SAS 6 disabled	3 minutes ago

2. On the TaskForce’s IP screen, the message “Express mode” appears.

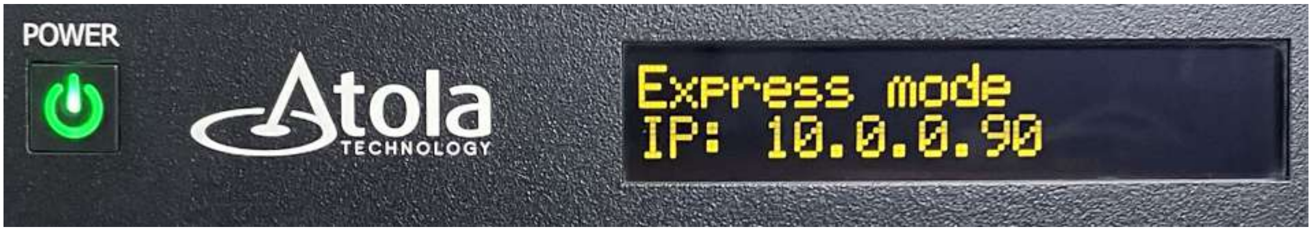


Image drives in Express mode

Plug drives

Once all settings are configured and Express mode is activated, simply plug in the drives one by one and watch the imaging sessions start automatically.

Control imaging status in Express mode

- **Home screen:** All diagnostics and imaging processes launched in Express mode appear on the Home screen. Click any process to see its details.
- **LED indicators** on the TaskForce front panel:
  - Blinking green - everything is OK, the process is running smoothly.
  - Yellow - user action required.
- **IP screen:** TaskForce 2 keeps the user updated by displaying the number of user actions required on the IP screen on the front panel of the unit.

User action required

When TaskForce 2 detects an issue with an imaging session, the **User action required** notification appears on the Home screen for the user to make a decision.

The number of user actions required is also displayed on the IP screen on the front panel of the hardware unit.

TaskForce prompts for user to take action if:

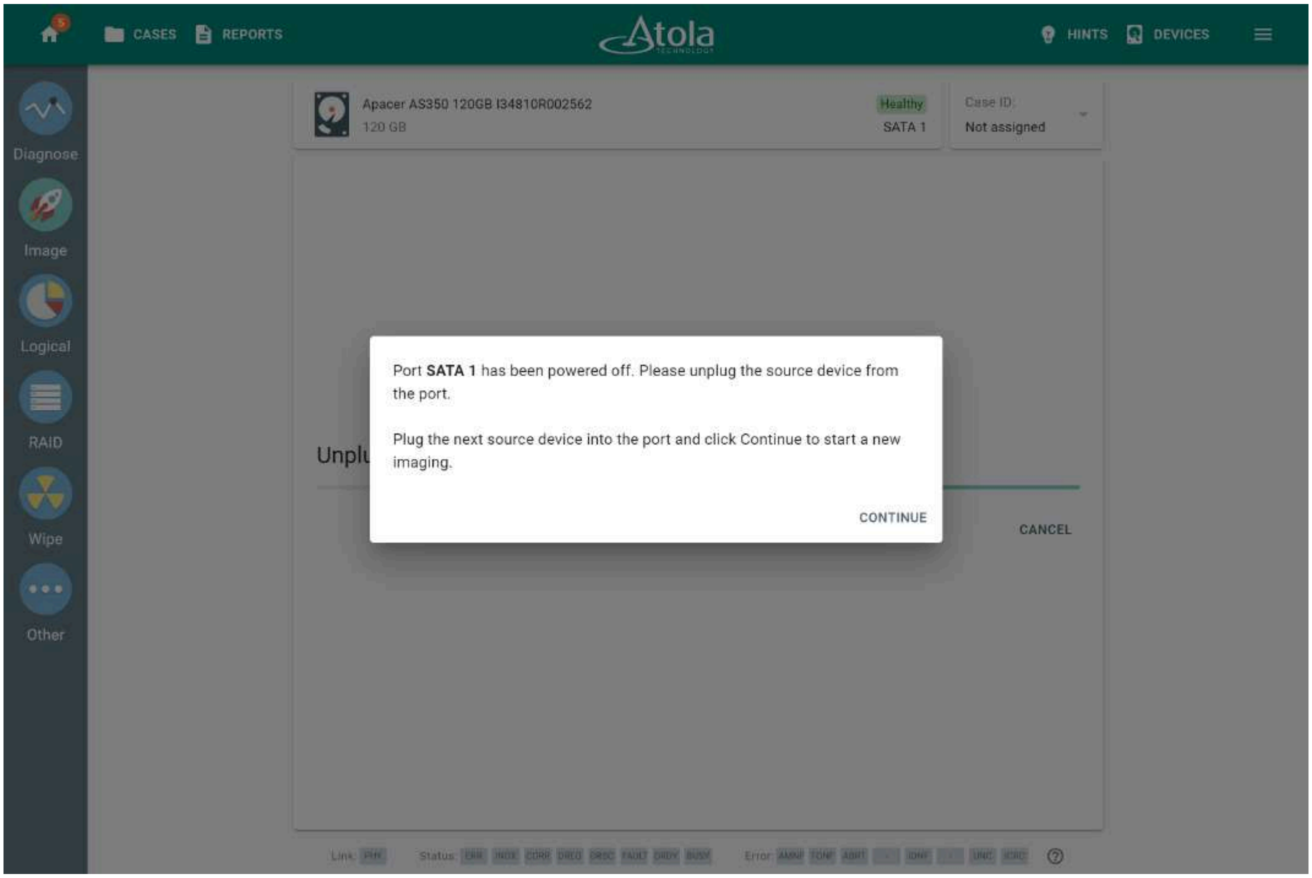
- Diagnostics detect any issues with a device.
- A user pauses the imaging process.
- Imaging finishes.
- A source device has already been imaged, fully or partially.
- A source device has been formatted as storage.

Pause and resume imaging session

As in standard imaging mode, in Express mode you can pause any imaging session and then resume it later.

To pause an imaging session in Express mode:

1. On the Home screen, click on the running imaging process you want to pause.
2. On the imaging details page, click the **Pause** button at the bottom.
3. Confirm pausing the imaging process.
4. TaskForce shows the notification that the port has been powered off.
5. **Optional:** Unplug your evidence drive from the port.
6. **Optional:** Plug the next drive or do not plug any.
7. In the dialog, click **Continue**.



Apacer AS350 120GB I34810R002562
120 GB

Healthy
SATA 1

Case ID:
Not assigned

Port **SATA 1** has been powered off. Please unplug the source device from the port.

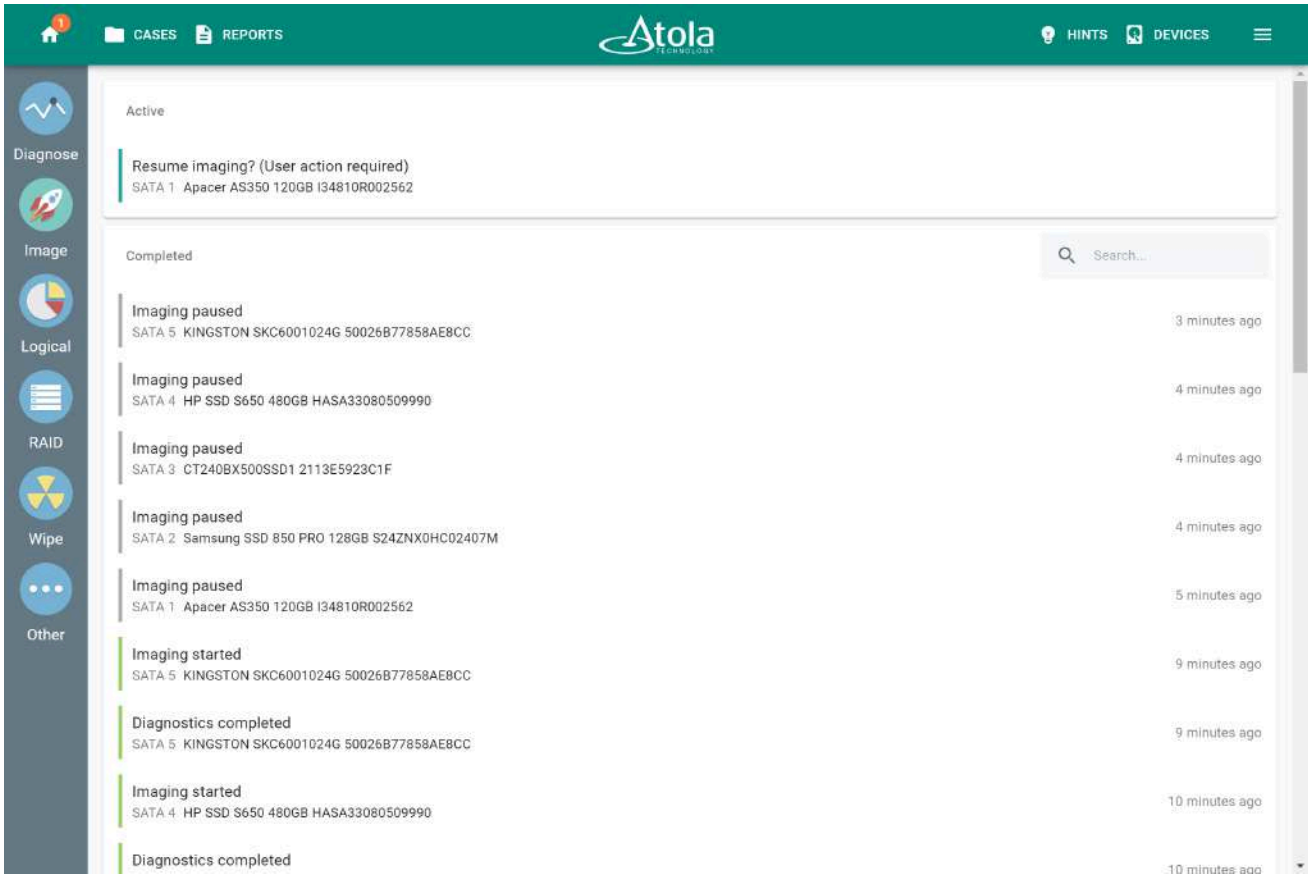
Plug the next source device into the port and click Continue to start a new imaging.

CONTINUE

Once the imaging process is paused, TaskForce creates an **Imaging paused report** available either from the **Home screen** or from the **Reports** page.

To resume the paused imaging session in Express mode:

1. On the Home screen, click the paused session.
2. In the dialog, click **Resume**.



Active

Resume imaging? (User action required)
SATA 1 Apacer AS350 120GB I34810R002562

Completed

Imaging paused
SATA 5 KINGSTON SKC6001024G 50026B77858AE8CC
3 minutes ago

Imaging paused
SATA 4 HP SSD S650 480GB HASA33080509990
4 minutes ago

Imaging paused
SATA 3 CT240BX500SSD1 2113E5923C1F
4 minutes ago

Imaging paused
SATA 2 Samsung SSD 850 PRO 128GB S24ZNX0HC02407M
4 minutes ago

Imaging paused
SATA 1 Apacer AS350 120GB I34810R002562
5 minutes ago

Imaging started
SATA 5 KINGSTON SKC6001024G 50026B77858AE8CC
9 minutes ago

Diagnostics completed
SATA 5 KINGSTON SKC6001024G 50026B77858AE8CC
9 minutes ago

Imaging started
SATA 4 HP SSD S650 480GB HASA33080509990
10 minutes ago

Diagnostics completed
10 minutes ago

Check imaging reports

Once the imaging process is started, paused, resumed, or completed in Express mode, TaskForce creates the respective report.

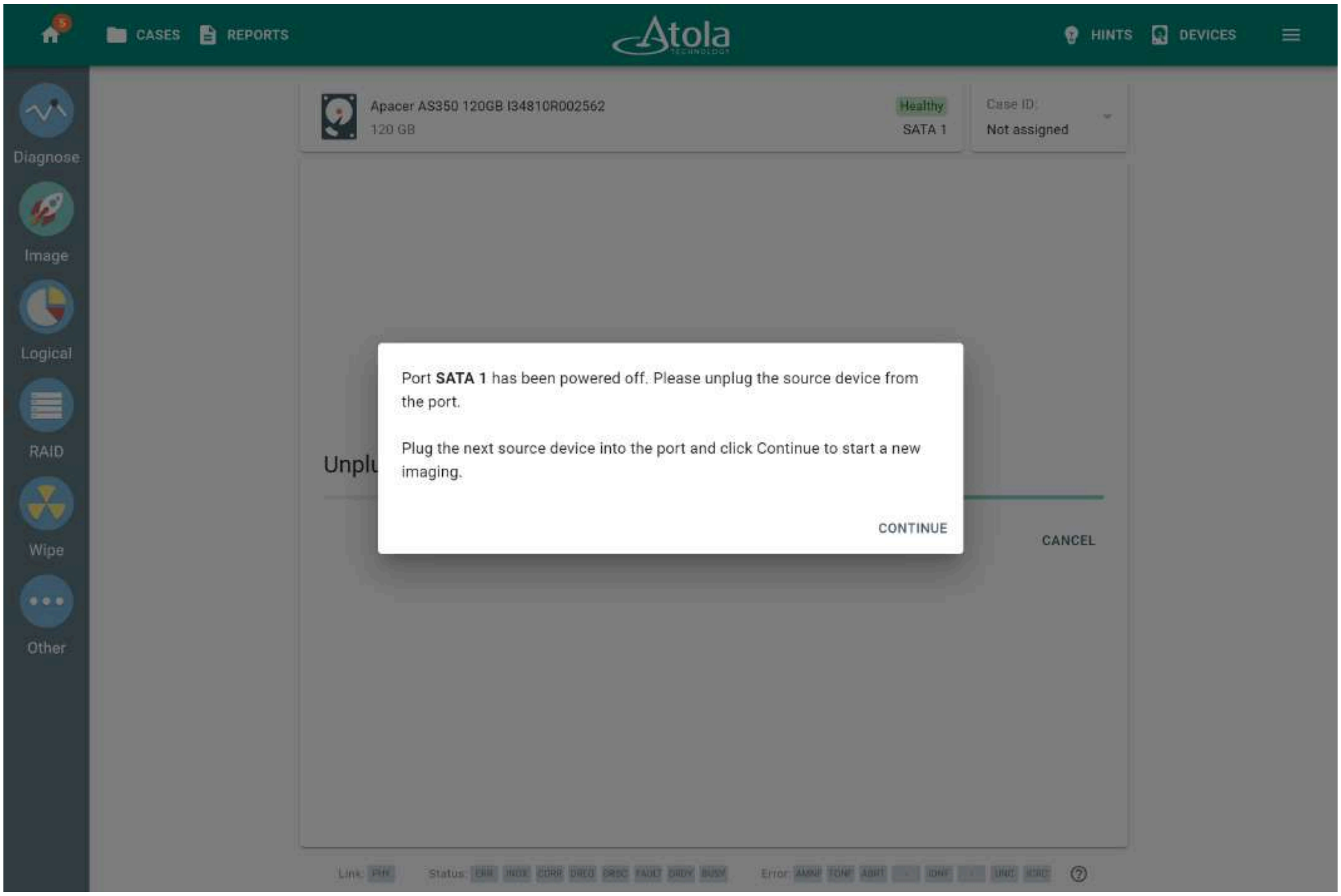
Reports contain the various details of the session in its current stage including source and target drive details, imaging settings, hash values, the time when the imaging session started, when it was completed and more.

Reports are available either from the **Home screen** or from the **Reports** page.

Change drives

Once an imaging session in Express mode is completed, TaskForce powers the respective port off and prompts a user to plug in the next evidence device.

To start a new imaging session, plug in the next source device and click **Continue** in the dialog.



Port **SATA 1** has been powered off. Please unplug the source device from the port.

Plug the next source device into the port and click Continue to start a new imaging.

CONTINUE

Deactivate Express mode

To deactivate Express mode:

1. Click the **Menu** in the top right and select **Express mode**.
2. On the bottom of the Express mode settings page, click **Deactivate**.

To show that Express mode is deactivated, TaskForce changes the color of the top panel and the Image icon on the left back to normal. The message “Express mode” on the IP screen also disappears.

Logical imaging

The **Logical imaging** module saves you time and storage space by copying only selected files and folders from an individual physical drive, image file, or RAID array in a forensically sound manner, without altering the original content of a source device and its metadata.

As a result of logical imaging, you get an image file in L01 or ZIP format, which contains only the data you selected manually or using include/exclude filters. L01 image will also include MD5/SHA1 hashes of the files.

After the logical imaging process is completed, TaskForce 2 generates a comprehensive report with the details about the source, target, number of imaged files and bytes and more.

Key features of logical imaging in TaskForce 2

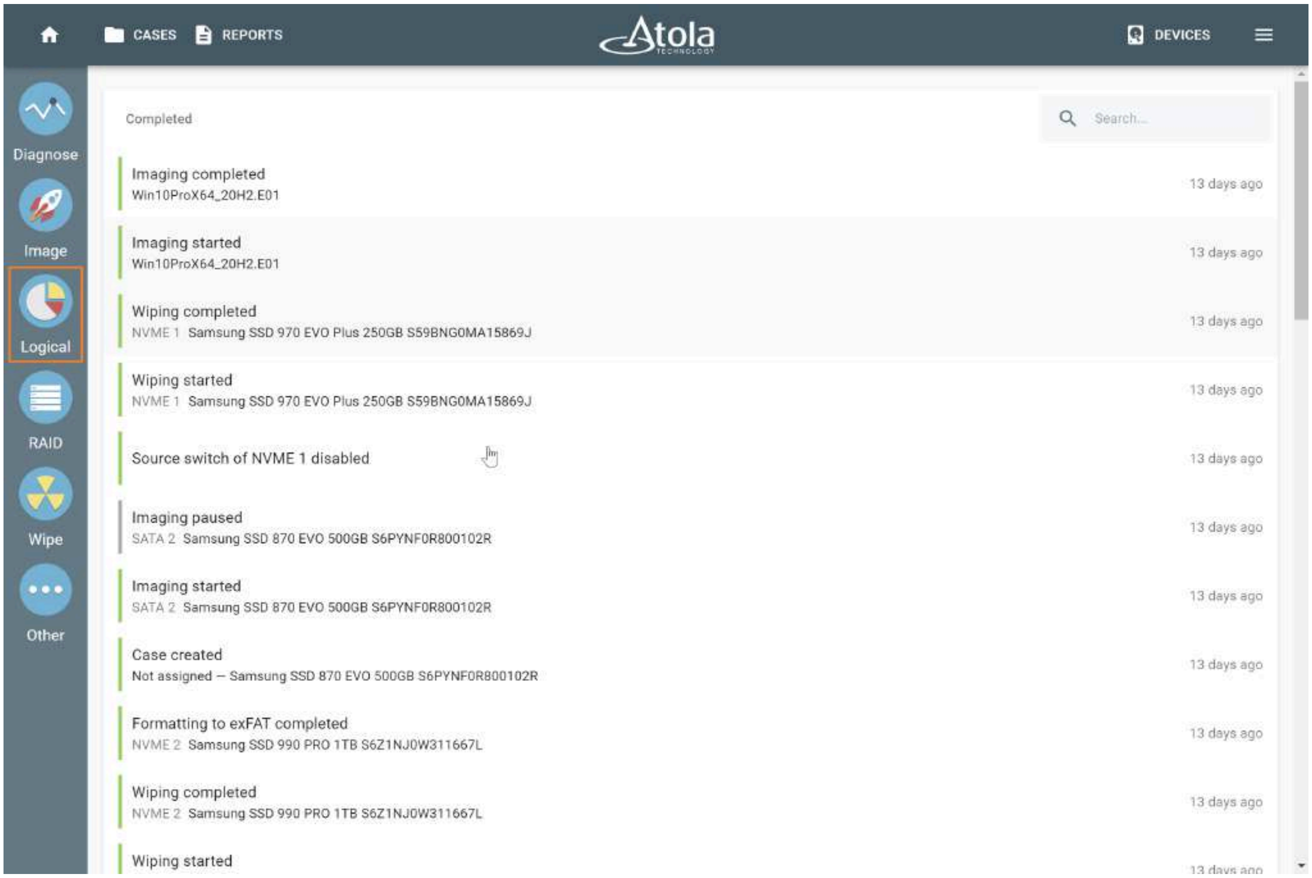
- 25+ parallel logical imaging sessions.
- Pause/Resume for each session.
- L01 or ZIP target images created in a network folder or on a storage drive.

- Compression of a target file is available.
- Supported file systems: NTFS, ext4/3/2, exFAT, XFS, ZFS, Btrfs, APFS (with encrypted volumes), HFS/HFS+, FAT32/16.
- Smart include/exclude filters.

Start logical imaging

There are two ways to start the Logical imaging module in TaskForce 2.

- **From the Homescreen:** On the Taskbar, click the Logical icon.



Completed

Imaging completed
Win10ProX64_20H2.E01
13 days ago

Imaging started
Win10ProX64_20H2.E01
13 days ago

Wiping completed
NVME 1 Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
13 days ago

Wiping started
NVME 1 Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
13 days ago

Source switch of NVME 1 disabled
13 days ago

Imaging paused
SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800102R
13 days ago

Imaging started
SATA 2 Samsung SSD 870 EVO 500GB S6PYNF0R800102R
13 days ago

Case created
Not assigned — Samsung SSD 870 EVO 500GB S6PYNF0R800102R
13 days ago

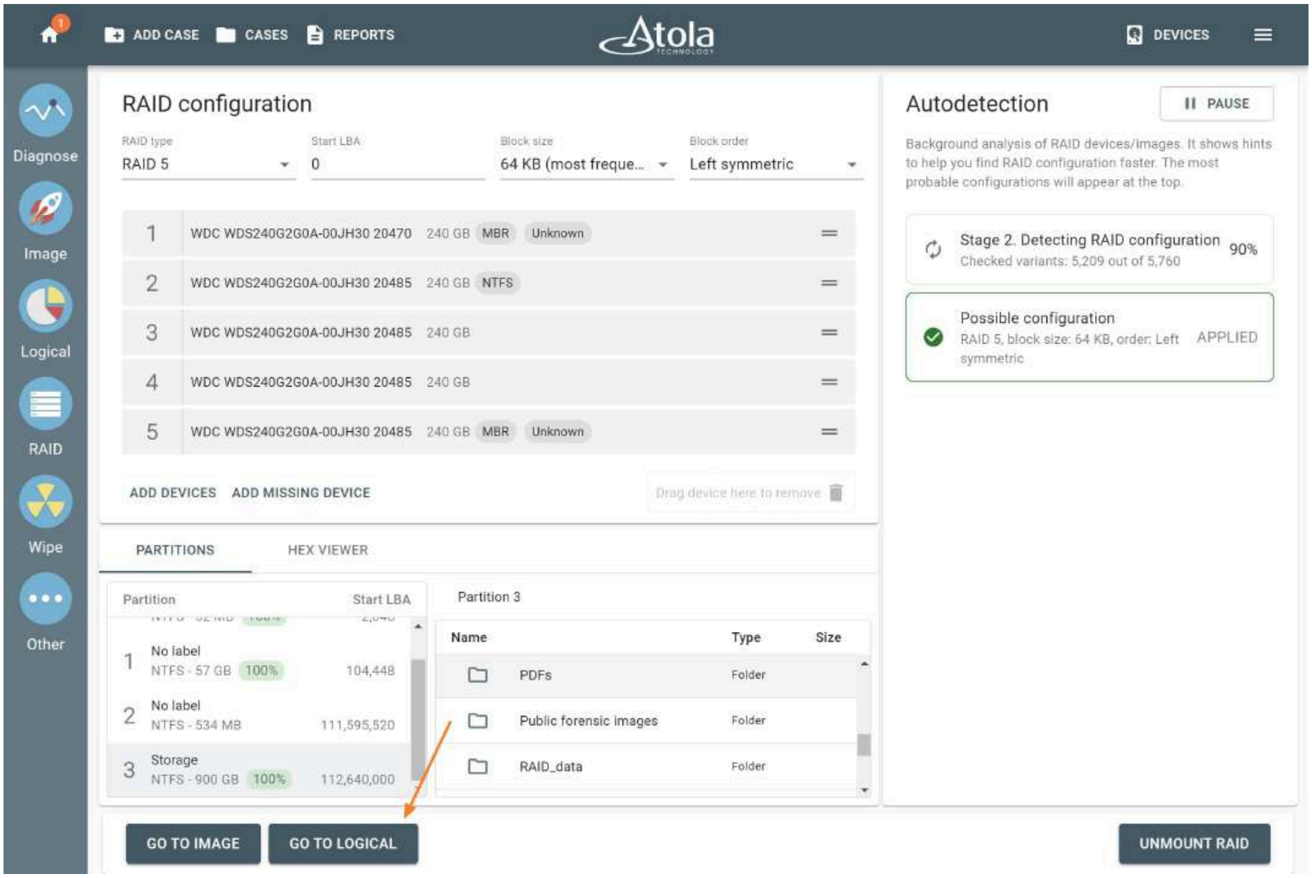
Formatting to exFAT completed
NVME 2 Samsung SSD 990 PRO 1TB S6Z1NJ0W311667L
13 days ago

Wiping completed
NVME 2 Samsung SSD 990 PRO 1TB S6Z1NJ0W311667L
13 days ago

Wiping started
13 days ago

The Logical icon in the Taskbar.

- **From the RAID module:** On the RAID Configuration page, click the Go to logical button. For details, see Logical imaging of a RAID array.



RAID configuration

RAID type	Start LBA	Block size	Block order
RAID 5	0	64 KB (most freque...	Left symmetric

1	WDC WDS240G2G0A-00JH30 20470	240 GB	MBR	Unknown
2	WDC WDS240G2G0A-00JH30 20485	240 GB	NTFS	
3	WDC WDS240G2G0A-00JH30 20485	240 GB		
4	WDC WDS240G2G0A-00JH30 20485	240 GB		
5	WDC WDS240G2G0A-00JH30 20485	240 GB	MBR	Unknown

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 90%
Checked variants: 5,209 out of 5,760

Possible configuration
RAID 5, block size: 64 KB, order: Left symmetric APPLIED

	Partition	Start LBA
1	No label NTFS - 57 GB 100%	104,448
2	No label NTFS - 534 MB	111,595,520
3	Storage NTFS - 900 GB 100%	112,640,000

Partition 3

Name	Type	Size
PDFs	Folder	
Public forensic images	Folder	
RAID_data	Folder	

The Go to Logical button on the RAID configuration page.

Logical imaging workflow in TaskForce 2

Once you started the Logical imaging module, follow these steps to create a logical image of your source device:

1. Select your source device.
2. Select partitions, folders, or files to image.
3. Apply smart filters, if needed.
4. Select target file.
5. Optional: Pause and resume the imaging process.
6. View the logical imaging report.

Let's see in detail how to perform each step.

Select source device

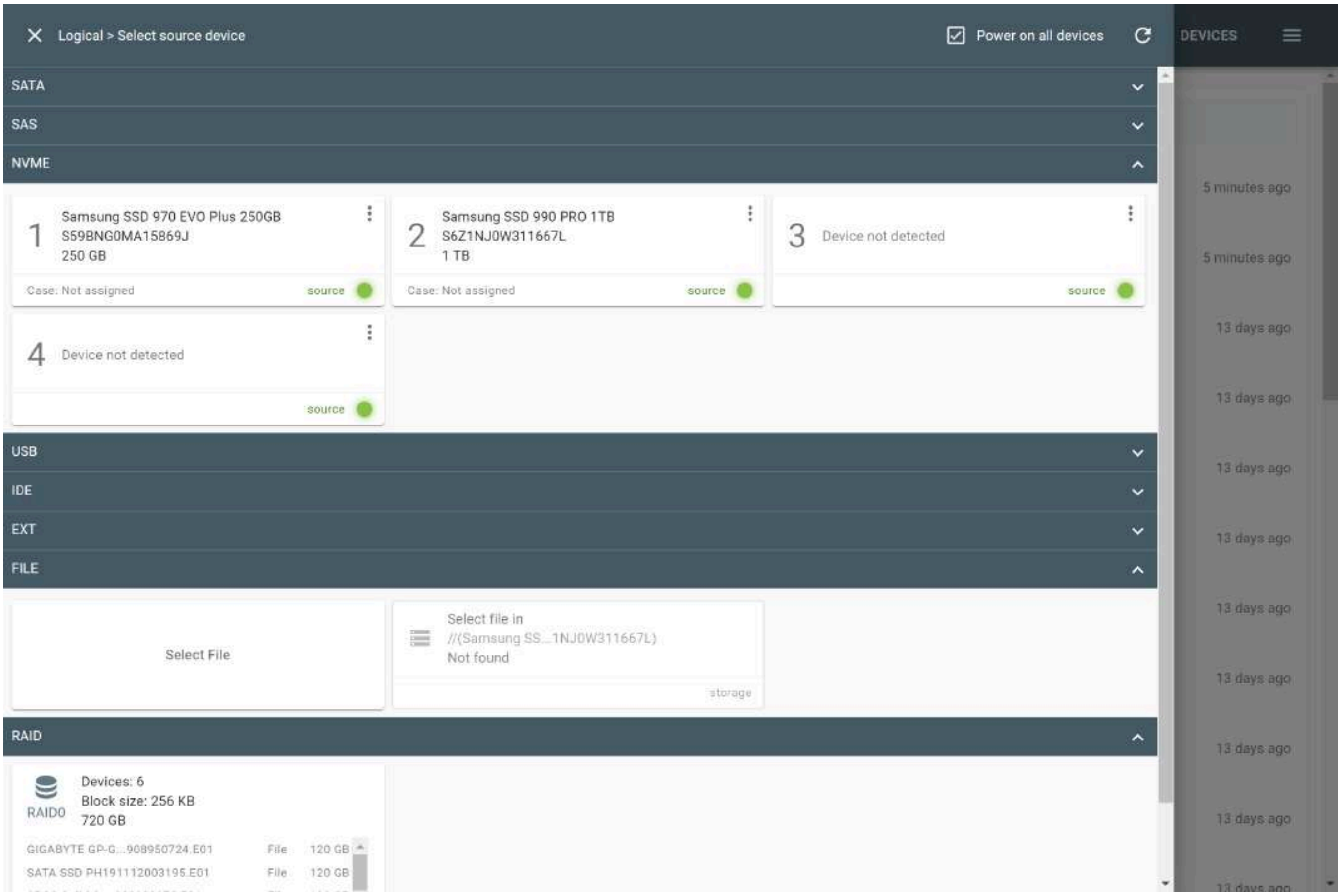
After clicking the Logical icon on the Taskbar, select your source device.

TaskForce 2 supports the following source types:

1. Individual physical drive:
   - SATA,
   - SAS,
   - NVMe,
   - USB,
   - IDE,
   - drives with M.2 interface within Apple laptops using the Apple PCIe SSD extension module,
   - Apple MacBooks with FireWire, Thunderbolt 2, and Thunderbolt 3 interfaces using the Thunderbolt extension module.

2. Image files:
    - IMG, RAW, DD
    - E01
    - AFF4
3. Reassembled RAID arrays.

File systems, supported by the Logical imaging module, are NTFS, ext4/3/2, exFAT, XFS, ZFS, Btrfs, APFS (with encrypted volumes), HFS/HFS+, FAT32/16.



☑ Power on all devices

1 Samsung SSD 970 EVO Plus 250GB
S59BNG0MA15869J
250 GB
Case: Not assigned source

2 Samsung SSD 990 PRO 1TB
S6Z1NJ0W311667L
1 TB
Case: Not assigned source

3 Device not detected
source

4 Device not detected
source

Select File

Select file in
//(Samsung SS...1NJ0W311667L)
Not found
storage

RAID0
Devices: 6
Block size: 256 KB
720 GB

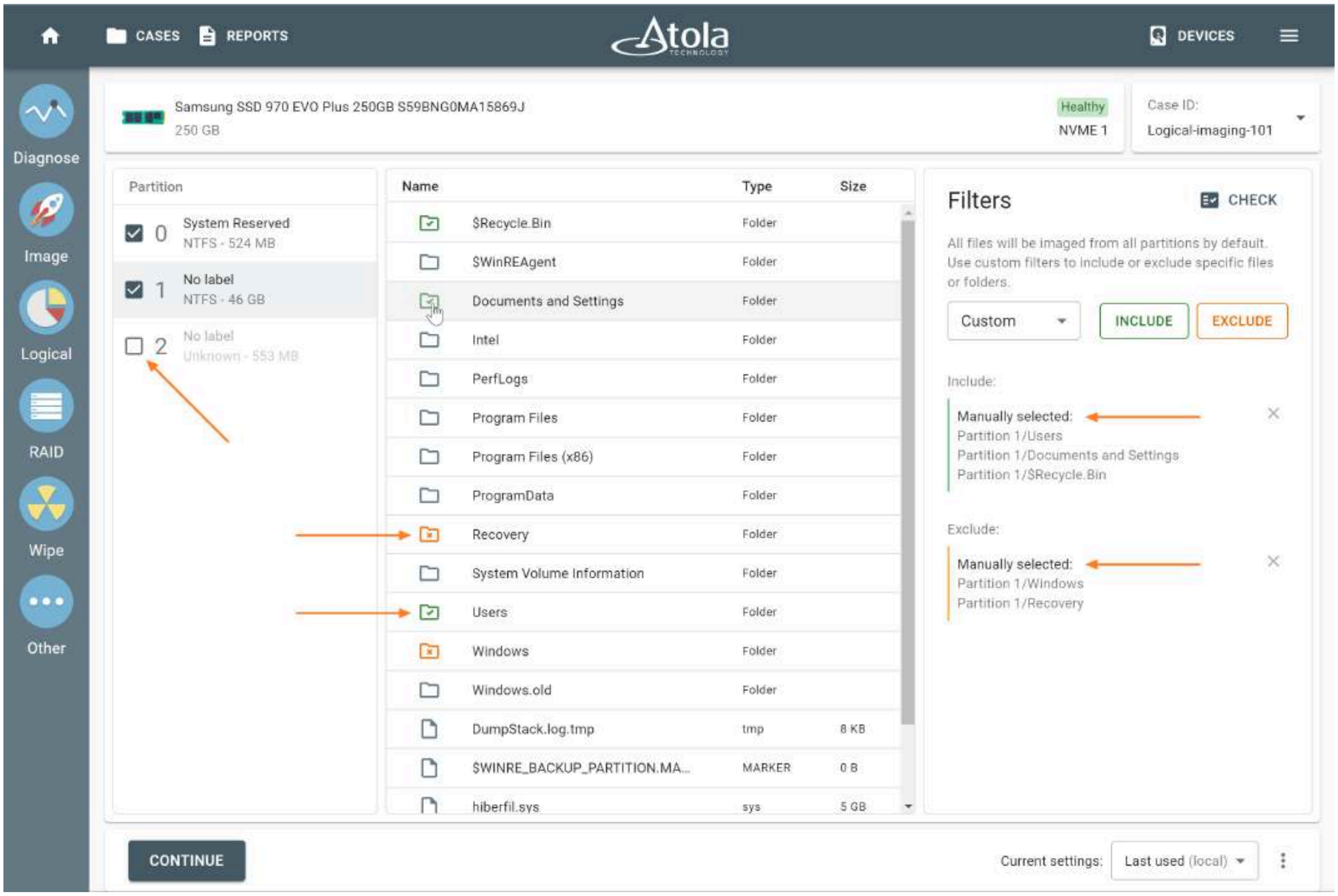
GIGABYTE GP-G...908950724.E01	File	120 GB
SATA SSD PH191112003195.E01	File	120 GB

Selecting a source device for logical imaging.

Select partitions, folders, or files to image

After you select your source device for logical imaging, TaskForce takes you to the Logical imaging page. Here you can preview the content of available partitions and folders, apply smart filters or use presets with predefined filtering settings.

Your source device and its case ID are shown at the top of the page.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
250 GB
Healthy
NVME 1
Case ID: Logical-imaging-101

Partition	
☑ 0	System Reserved NTFS - 524 MB
☑ 1	No label NTFS - 46 GB
□ 2	No label Unknown - 553 MB

Name	Type	Size
$Recycle.Bin	Folder	
$WinREAgent	Folder	
Documents and Settings	Folder	
Intel	Folder	
PerfLogs	Folder	
Program Files	Folder	
Program Files (x86)	Folder	
ProgramData	Folder	
Recovery	Folder	
System Volume Information	Folder	
Users	Folder	
Windows	Folder	
Windows.old	Folder	
DumpStack.log.tmp	tmp	8 KB
$WINRE_BACKUP_PARTITION.MA...	MARKER	0 B
hiberfil.sys	sys	5 GB

Filters

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

Custom

Include:

Manually selected:
Partition 1/Users
Partition 1/Documents and Settings
Partition 1/$Recycle.Bin

Exclude:

Manually selected:
Partition 1/Windows
Partition 1/Recovery

Current settings: Last used (local)

Selecting partitions, folders, and files for logical imaging.

Preview, select, or deselect partition

The **Partition** section on the left lists all the partitions available on your source device.

- **To preview** the partition contents, click on its name.
- By default, all partitions are selected for imaging.
- **To exclude** a partition, clear the checkbox next to it.
- **To include** a partition again, select the checkbox.

Preview folder, manually include or exclude folders and files

Folders and files of the selected partition are shown in the middle section. By default, TaskForce images all files from all partitions.

- **To preview a folder's** contents, click on the folder name.
- To manually **include** a folder or file for imaging, click on its icon once. The icon turns green. The folder or file appears in the Filters section on the right as manually included.
- To manually **exclude** a folder or file, click on its icon twice. The icon turns orange. The folder or file appears in the Filters section on the right as manually excluded.

Use smart filters and presets for selecting folders or files

Automatically include or exclude folders and files for imaging by using the built-in smart filters or custom filtering presets.

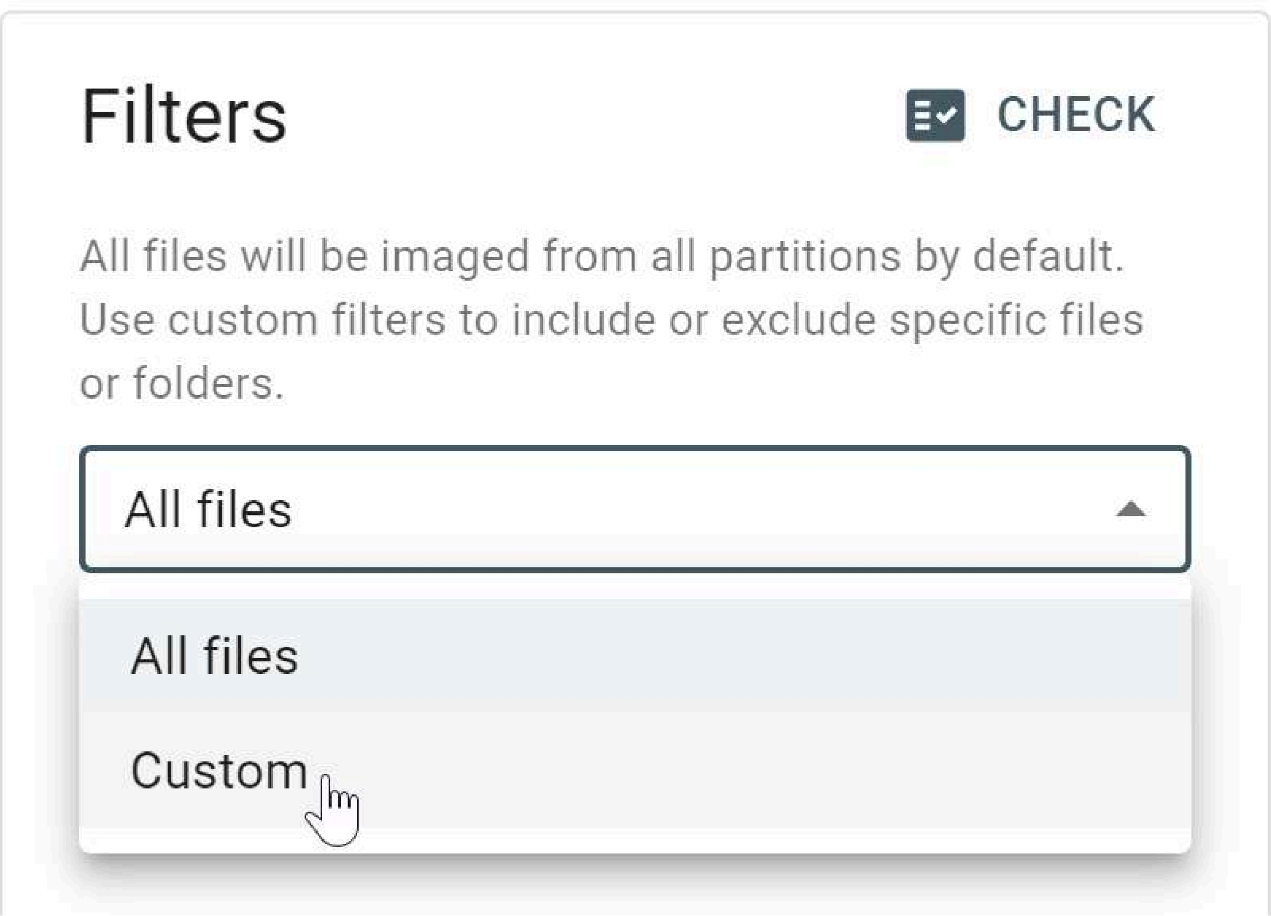
The **Filters** section on the right provides flexible options for fine-tuning your selection of folders and files for imaging.

By default, TaskForce images all files from all partitions.

Apply filters

Use smart filters to automatically include or exclude specific files or folders:

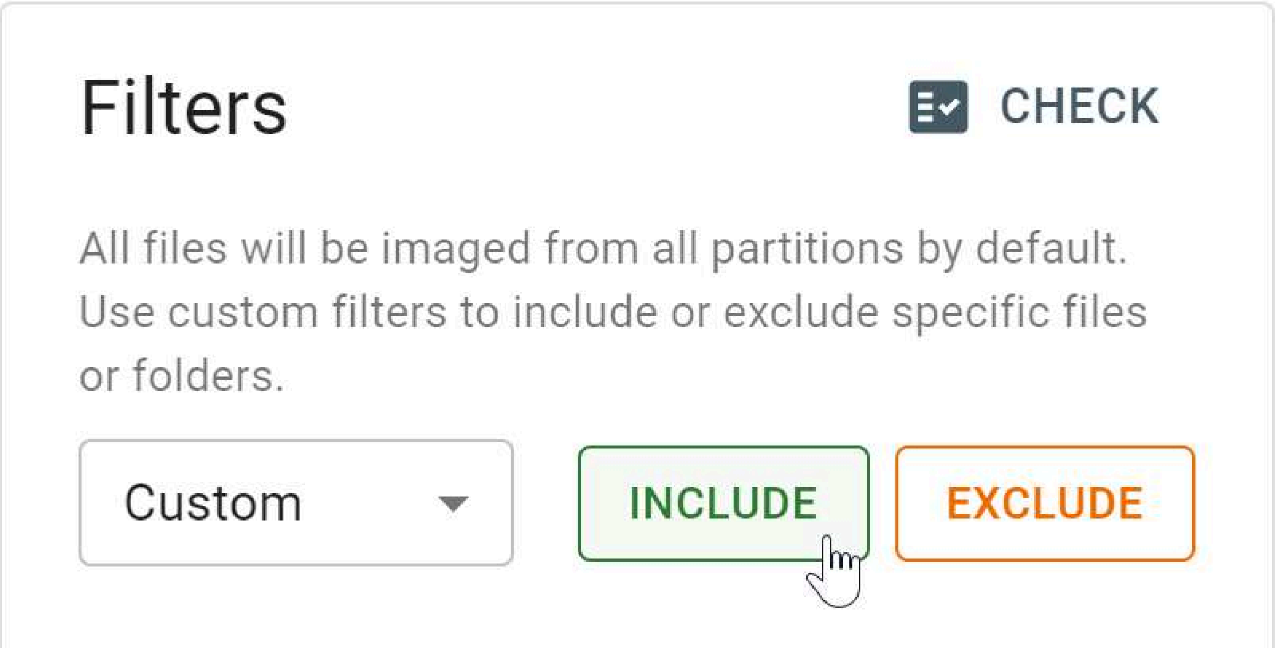
1. In the **Filters** section, select the **Custom** option from the list.



Filters

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

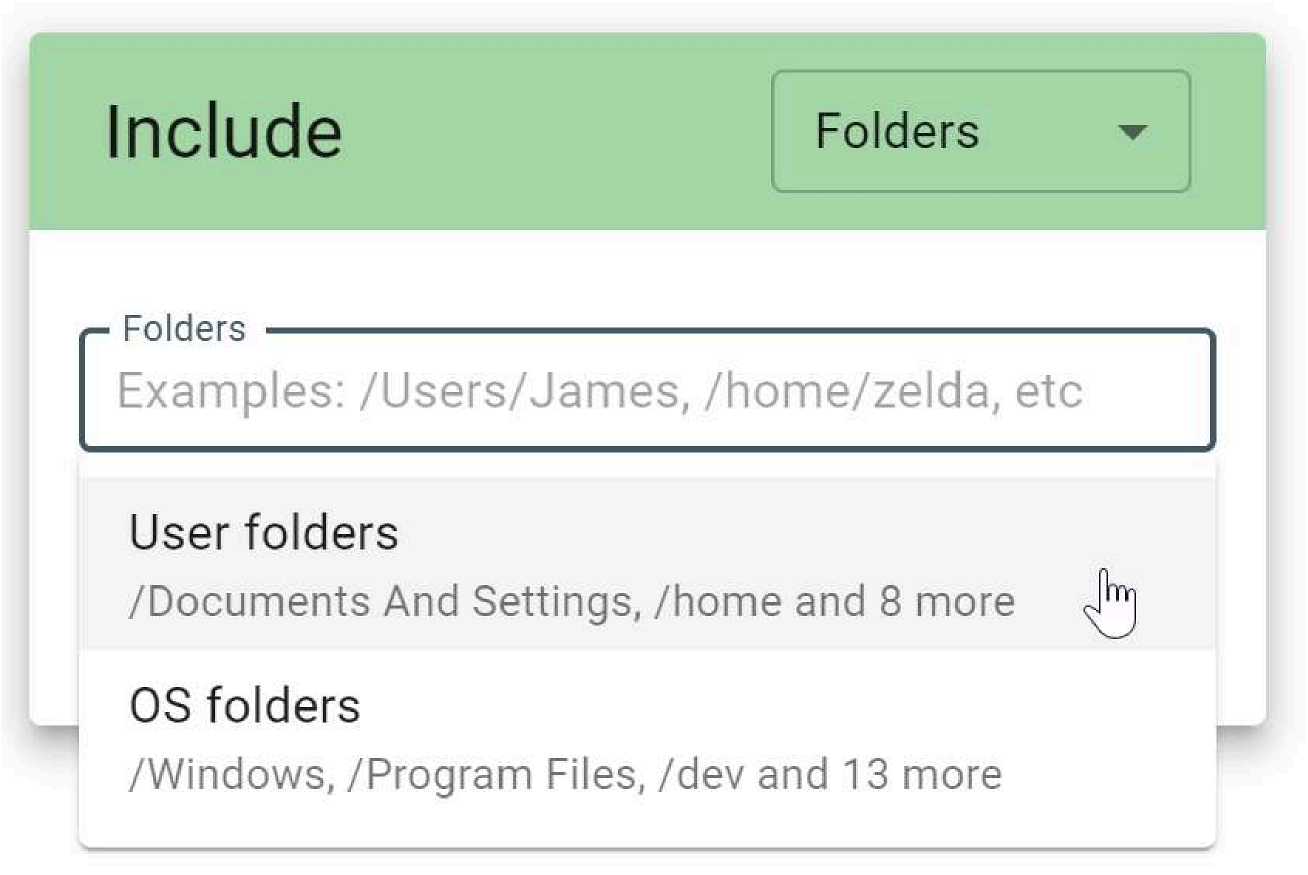
2. Click the **Include** or **Exclude** button. The respective dialog appears.



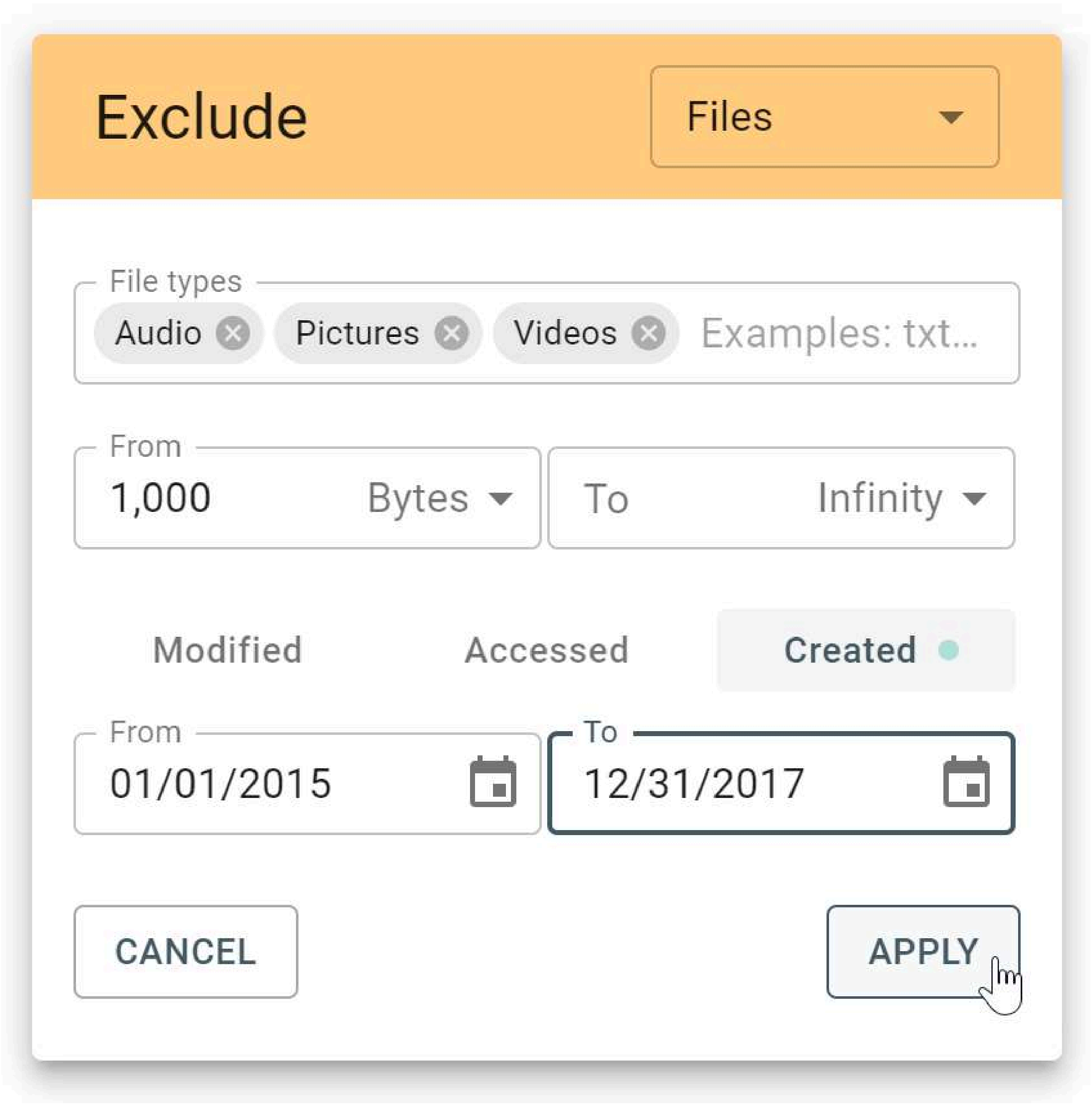
Filters

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

3. Automatically include or exclude folders:
   a. In the respective dialog, select the **Folders** option from the list at the top.
   b. Click in the **Folders** field.
   c. Select one of the predefined options: **User folders** or **OS folders**.
   d. Or enter the folder paths, separated by commas.
   e. Click **Apply**.


Include
Folders
Folders
Examples: /Users/James, /home/zelda, etc
User folders
/Documents And Settings, /home and 8 more
OS folders
/Windows, /Program Files, /dev and 13 more

4. Automatically include or exclude files:
   a. In the respective dialog, select the **Files** option from the list at the top.
   b. Specify **File types** by selecting predefined options from the list: archives, audio, databases, documents, emails, financial, pictures, security keys, video, and virtual machines. You can enter file extensions yourself as well.
   c. Enter file size range: from 1 byte to infinity.
   d. Narrow down time spans: when files were modified, accessed, or created.
   e. Click **Apply**.



Exclude

Files

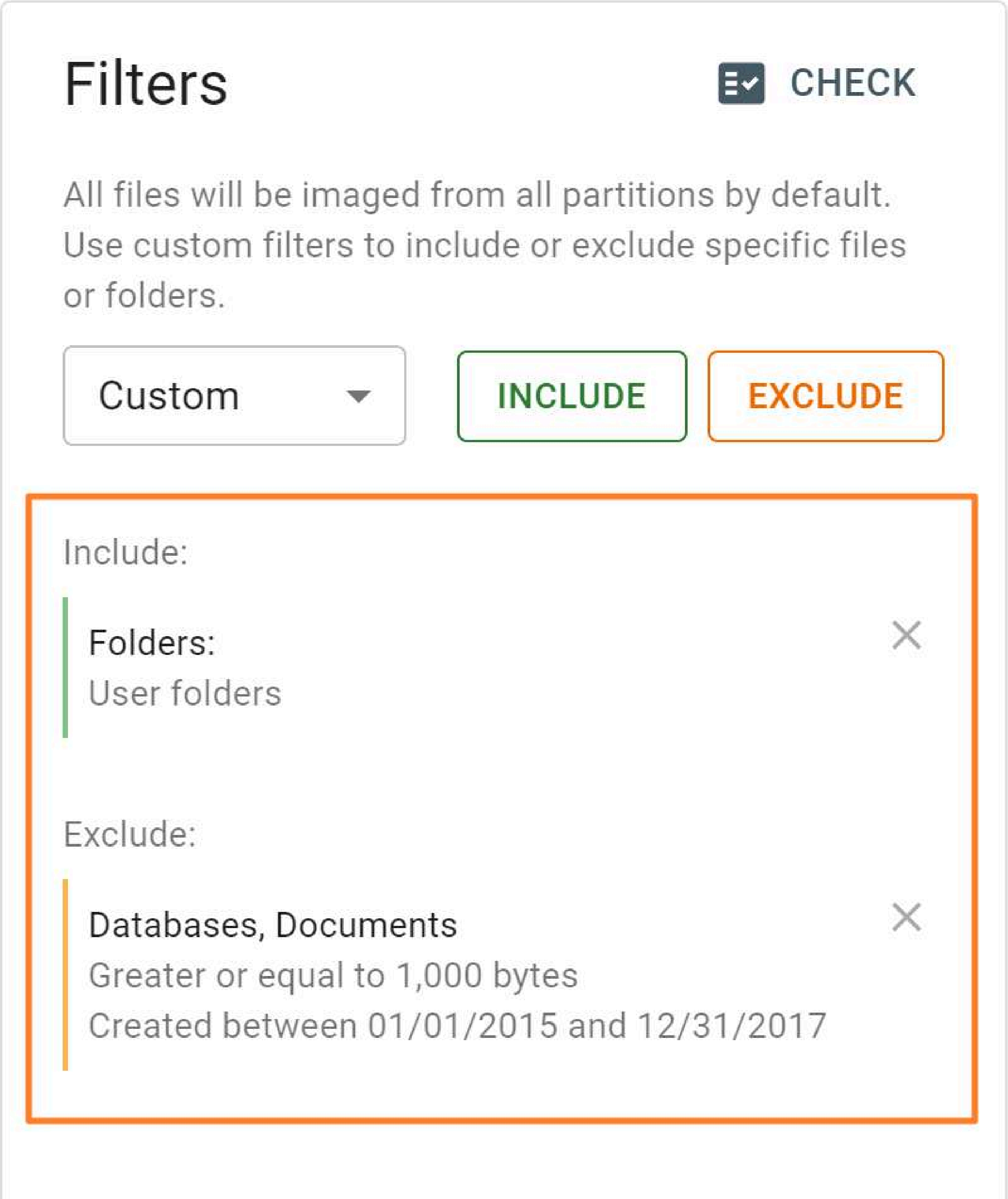
File types: Audio, Pictures, Videos

From 1,000 Bytes To Infinity

Created

From 01/01/2015 To 12/31/2017

All applied Include or Exclude filters appear in the Filters section.



Filters

CHECK

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

Custom

INCLUDE

EXCLUDE

Include:

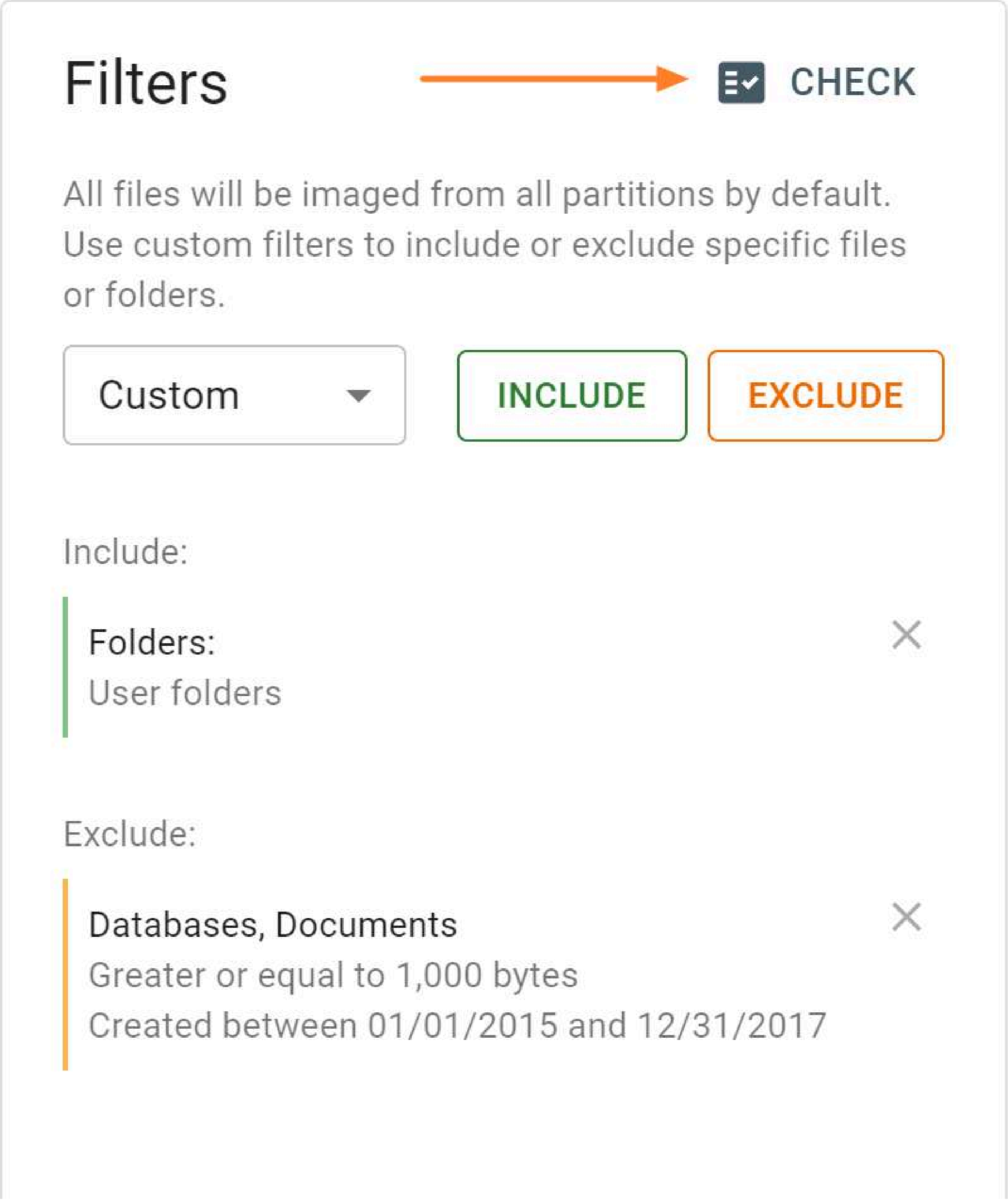
Folders:
User folders

Exclude:

Databases, Documents
Greater or equal to 1,000 bytes
Created between 01/01/2015 and 12/31/2017

Check filters before imaging

To test your filtering settings before imaging and get a list of files that match the selected filters, click **Check** at the top of the Filters section:



All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

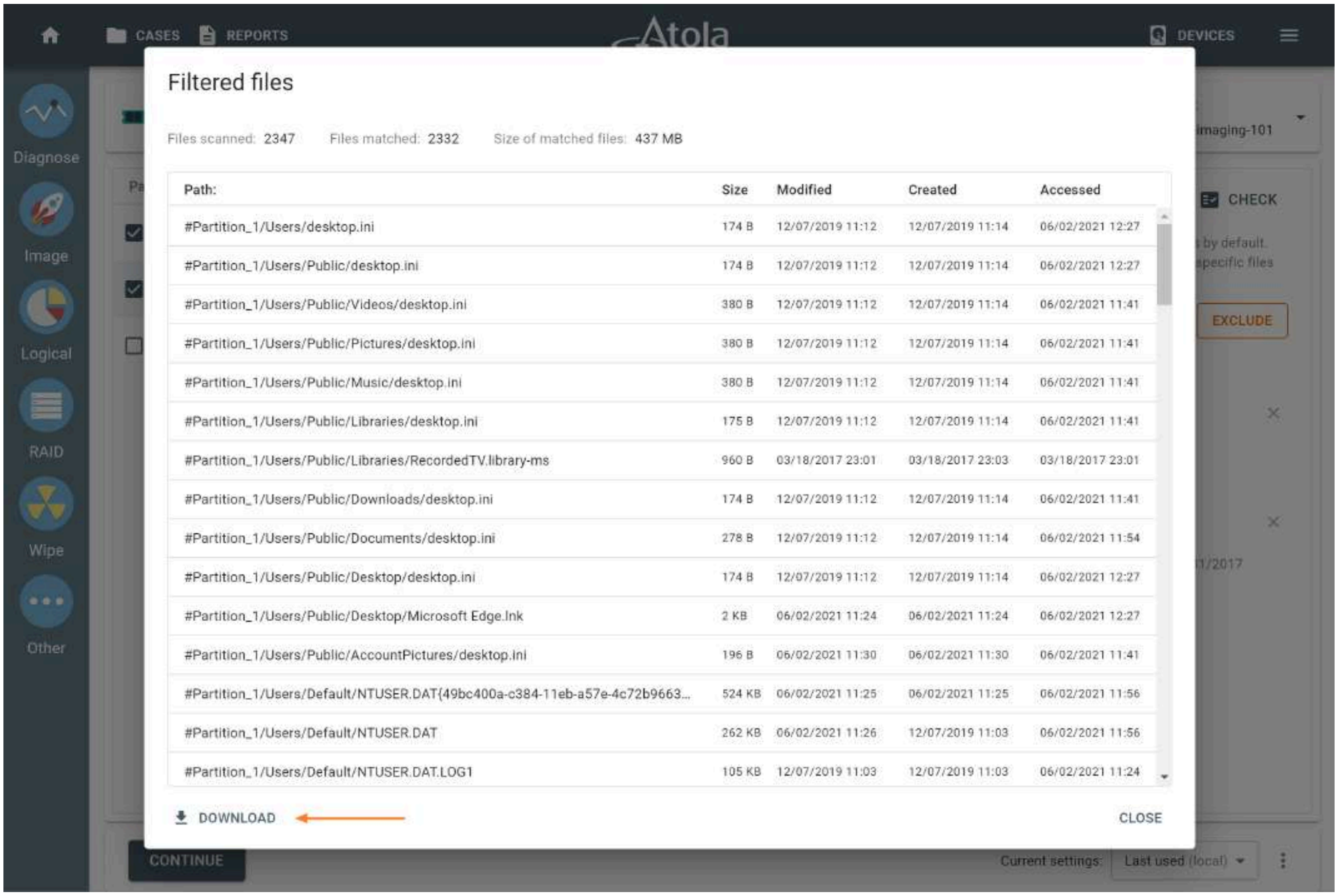
Include:

Folders:
User folders

Exclude:

Databases, Documents
Greater or equal to 1,000 bytes
Created between 01/01/2015 and 12/31/2017

TaskForce scans the selected partition(s) and lists all files matching the filtering criteria. You can download this file list in CSV format by clicking the **Download** button at the bottom.



Filtered files

Files scanned: 2347 Files matched: 2332 Size of matched files: 437 MB

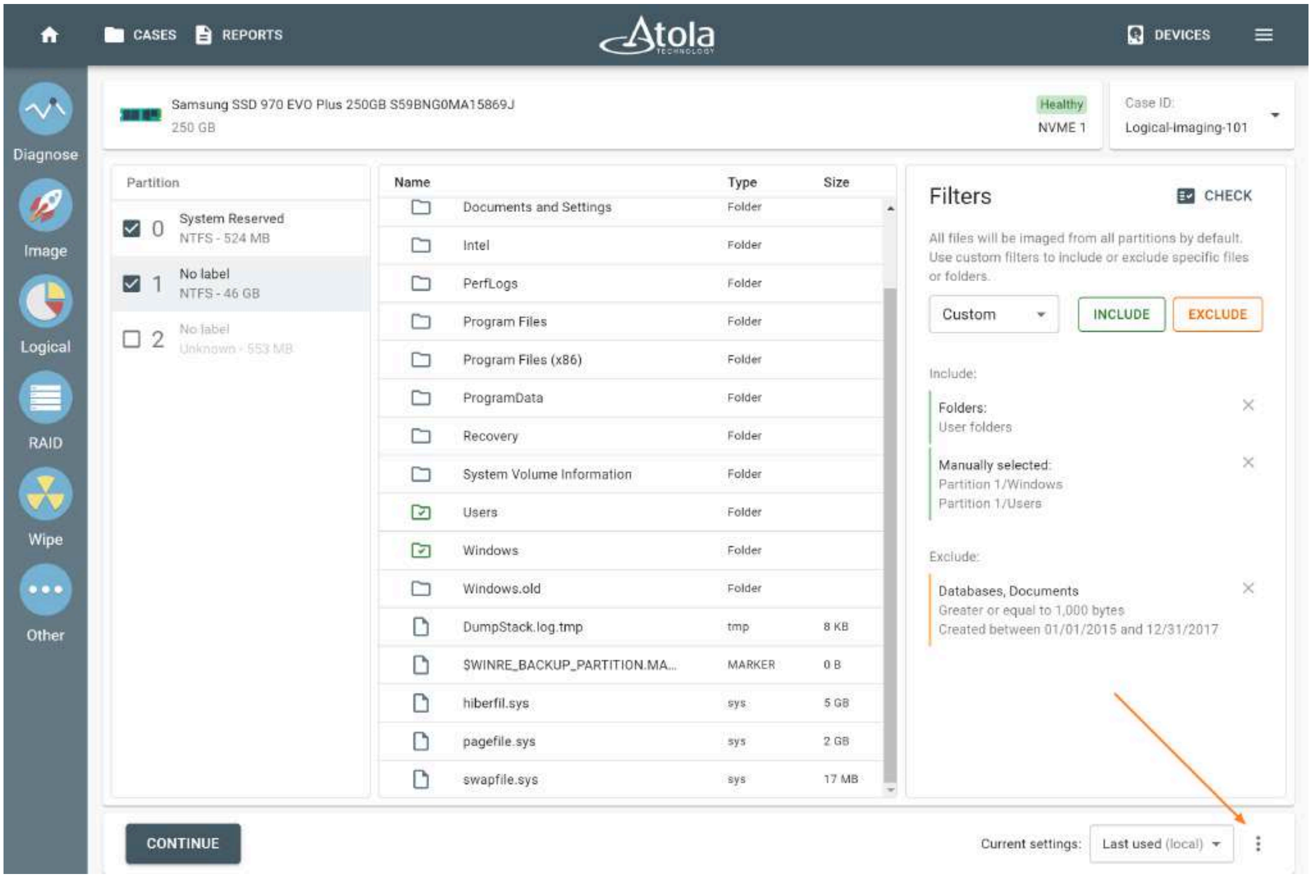
Path:	Size	Modified	Created	Accessed
#Partition_1/Users/desktop.ini	174 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 12:27
#Partition_1/Users/Public/desktop.ini	174 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 12:27
#Partition_1/Users/Public/Videos/desktop.ini	380 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 11:41
#Partition_1/Users/Public/Pictures/desktop.ini	380 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 11:41
#Partition_1/Users/Public/Music/desktop.ini	380 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 11:41
#Partition_1/Users/Public/Libraries/desktop.ini	175 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 11:41
#Partition_1/Users/Public/Libraries/RecordedTV.library-ms	960 B	03/18/2017 23:01	03/18/2017 23:03	03/18/2017 23:01
#Partition_1/Users/Public/Downloads/desktop.ini	174 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 11:41
#Partition_1/Users/Public/Documents/desktop.ini	278 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 11:54
#Partition_1/Users/Public/Desktop/desktop.ini	174 B	12/07/2019 11:12	12/07/2019 11:14	06/02/2021 12:27
#Partition_1/Users/Public/Desktop/Microsoft Edge.lnk	2 KB	06/02/2021 11:24	06/02/2021 11:24	06/02/2021 12:27
#Partition_1/Users/Public/AccountPictures/desktop.ini	196 B	06/02/2021 11:30	06/02/2021 11:30	06/02/2021 11:41
#Partition_1/Users/Default/NTUSER.DAT{49bc400a-c384-11eb-a57e-4c72b9663...	524 KB	06/02/2021 11:25	06/02/2021 11:25	06/02/2021 11:56
#Partition_1/Users/Default/NTUSER.DAT	262 KB	06/02/2021 11:26	12/07/2019 11:03	06/02/2021 11:56
#Partition_1/Users/Default/NTUSER.DAT.LOG1	105 KB	12/07/2019 11:03	12/07/2019 11:03	06/02/2021 11:24

Downloading the list of files matching the filtering criteria.

Save filtering settings as a preset

To reuse your filtering settings later or share them with your colleague, save them as a logical imaging preset:

1. In the bottom right corner of the Logical imaging page, click the **More** icon with three dots.
2. Select **Save to**.
3. Enter the name for your preset and click **Save**.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
250 GB

Healthy
NVME 1

Case ID:
Logical-imaging-101

Partition	
☑ 0	System Reserved NTFS - 524 MB
☑ 1	No label NTFS - 46 GB
□ 2	No label Unknown - 553 MB

Name	Type	Size
Documents and Settings	Folder	
Intel	Folder	
PerfLogs	Folder	
Program Files	Folder	
Program Files (x86)	Folder	
ProgramData	Folder	
Recovery	Folder	
System Volume Information	Folder	
☑ Users	Folder	
☑ Windows	Folder	
Windows.old	Folder	
DumpStack.log.tmp	tmp	8 KB
$WINRE_BACKUP_PARTITION.MA...	MARKER	0 B
hiberfil.sys	sys	5 GB
pagefile.sys	sys	2 GB
swapfile.sys	sys	17 MB

Filters

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

Custom

Include:

Folders:
User folders

Manually selected:
Partition 1/Windows
Partition 1/Users

Exclude:

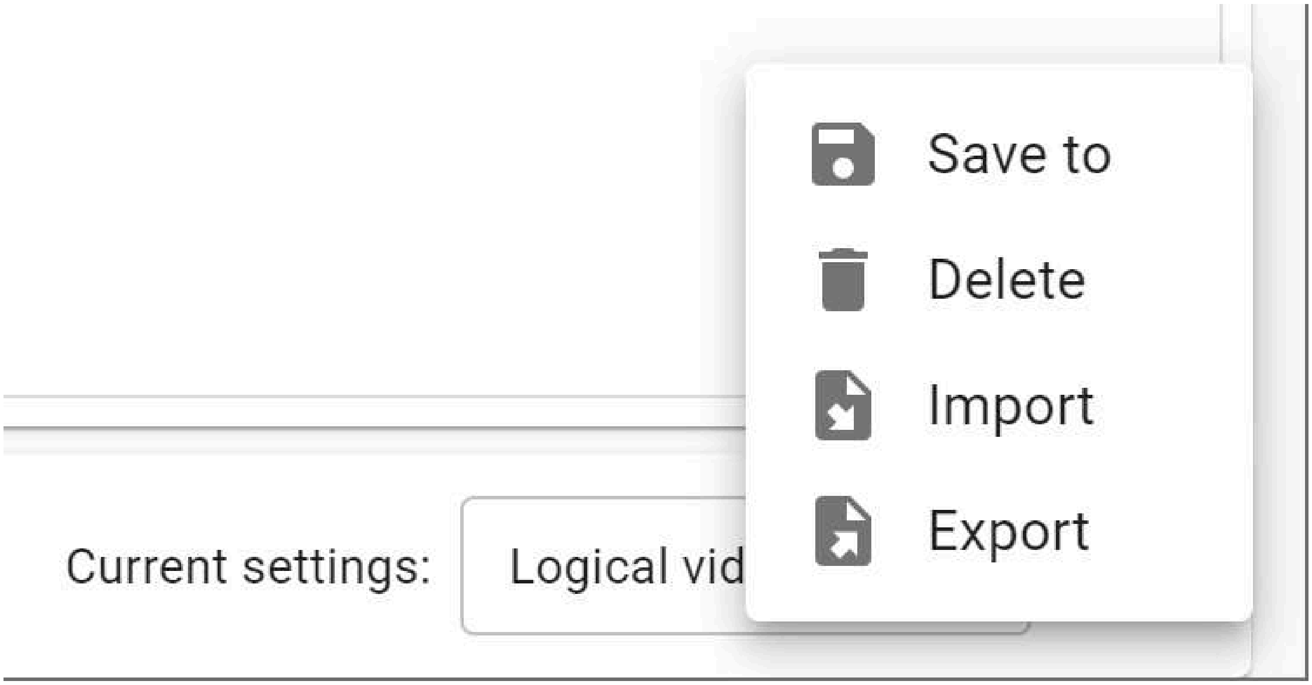
Databases, Documents
Greater or equal to 1,000 bytes
Created between 01/01/2015 and 12/31/2017

Current settings: Last used (local)

Saving a logical imaging preset.

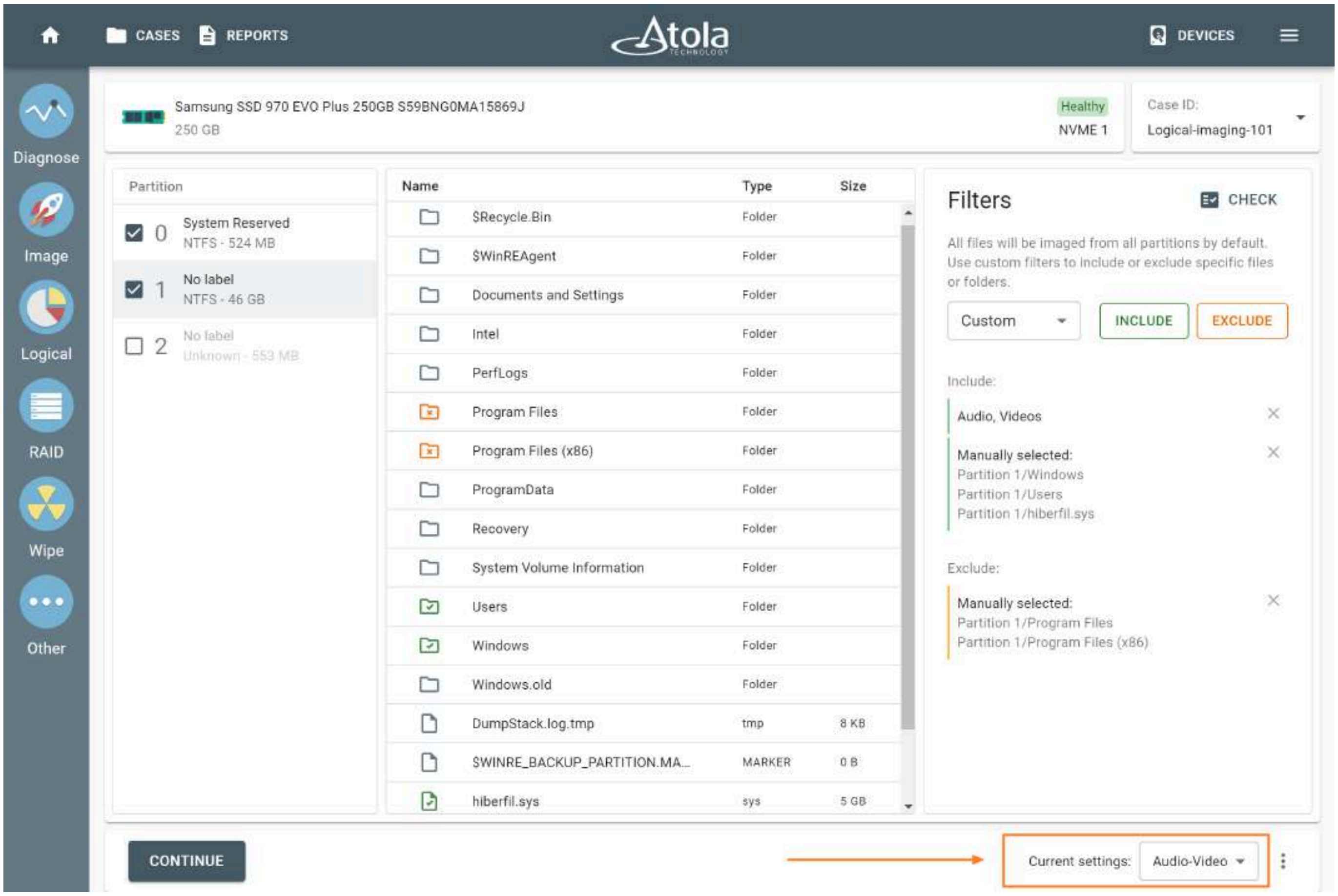
From the same three-dots menu, you can also:

- **Export** a preset to use it on another computer.
- **Import** a preset created on another computer.
- **Delete** a preset.



Current settings: Logical vid

To switch between presets, use the **Current settings** list on the bottom right of the logical imaging page.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
250 GB

Healthy
NVME 1

Case ID:
Logical-imaging-101

	Partition	
☑	0	System Reserved NTFS - 524 MB
☑	1	No label NTFS - 46 GB
□	2	No label Unknown - 553 MB

Name	Type	Size
$Recycle.Bin	Folder	
$WinREAgent	Folder	
Documents and Settings	Folder	
Intel	Folder	
PerfLogs	Folder	
Program Files	Folder	
Program Files (x86)	Folder	
ProgramData	Folder	
Recovery	Folder	
System Volume Information	Folder	
Users	Folder	
Windows	Folder	
Windows.old	Folder	
DumpStack.log.tmp	tmp	8 KB
$WINRE_BACKUP_PARTITION.MA...	MARKER	0 B
hiberfil.sys	sys	5 GB

Filters

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

Custom

Include:

Audio, Videos

Manually selected:
Partition 1/Windows
Partition 1/Users
Partition 1/hiberfil.sys

Exclude:

Manually selected:
Partition 1/Program Files
Partition 1/Program Files (x86)

Current settings: Audio-Video

Selecting a preset from the Current settings list.

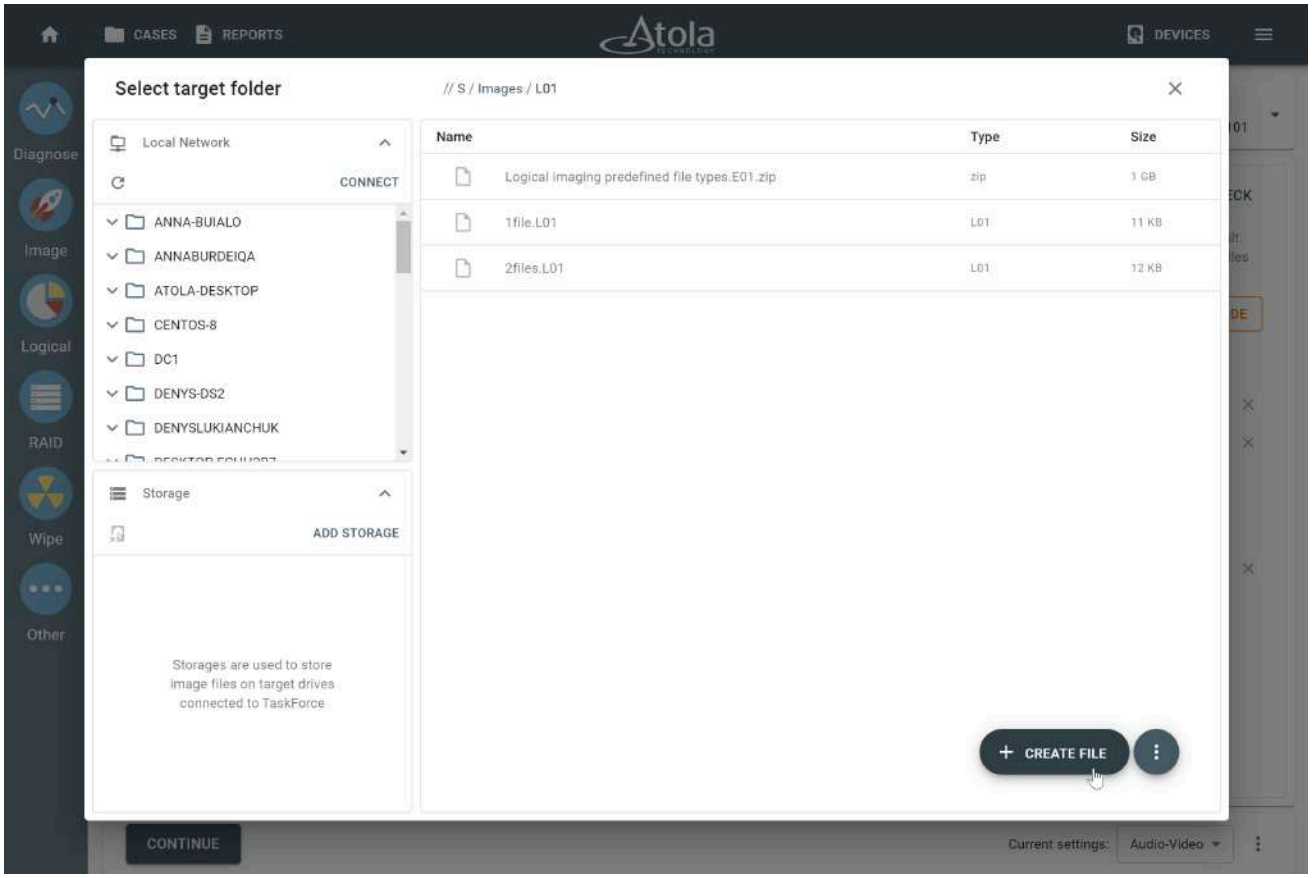
Select target file

Once you have adjusted the logical imaging parameters, click **Continue**.

TaskForce takes you to the **Select target folder** window.

The target file in L01 or ZIP format (with or without compression) can be created either on a network drive or on a storage device connected directly to the TaskForce hardware unit:

1. Select the folder for your target file and click **Create file**.

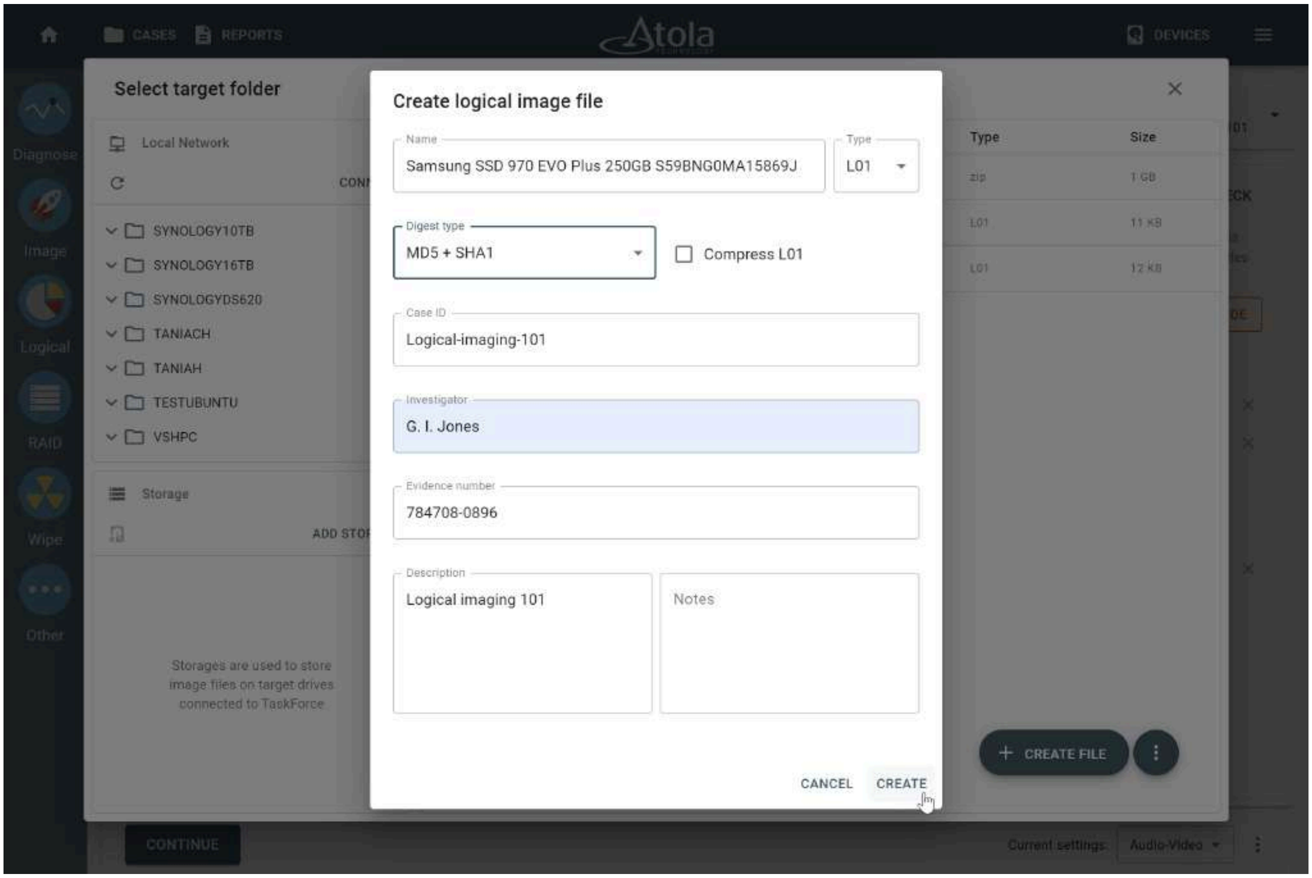


Name	Type	Size
Logical imaging predefined file types.E01.zip	zip	1 GB
1file.L01	L01	11 KB
2files.L01	L01	12 KB

The Select target folder window.

2. Adjust the settings of the target file:
    a. Name.
    b. File type: L01 or ZIP.
    c. Hashing method (Digest type): MD5, SHA1, or MD5+SHA1.
    d. Compression.
    e. Case ID and details.

3. Click **Create** to start the imaging process.



Storages are used to store image files on target drives connected to TaskForce.

Type	Size
zip	1 GB
L01	11 KB
L01	12 KB

Create logical image file

- Name: Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
- Type: L01
- Digest type: MD5 + SHA1
- □ Compress L01
- Case ID: Logical-imaging-101
- Investigator: G. I. Jones
- Evidence number: 784708-0896
- Description: Logical imaging 101
- Notes

Creating logical imaging file.

How to set a drive to Storage mode

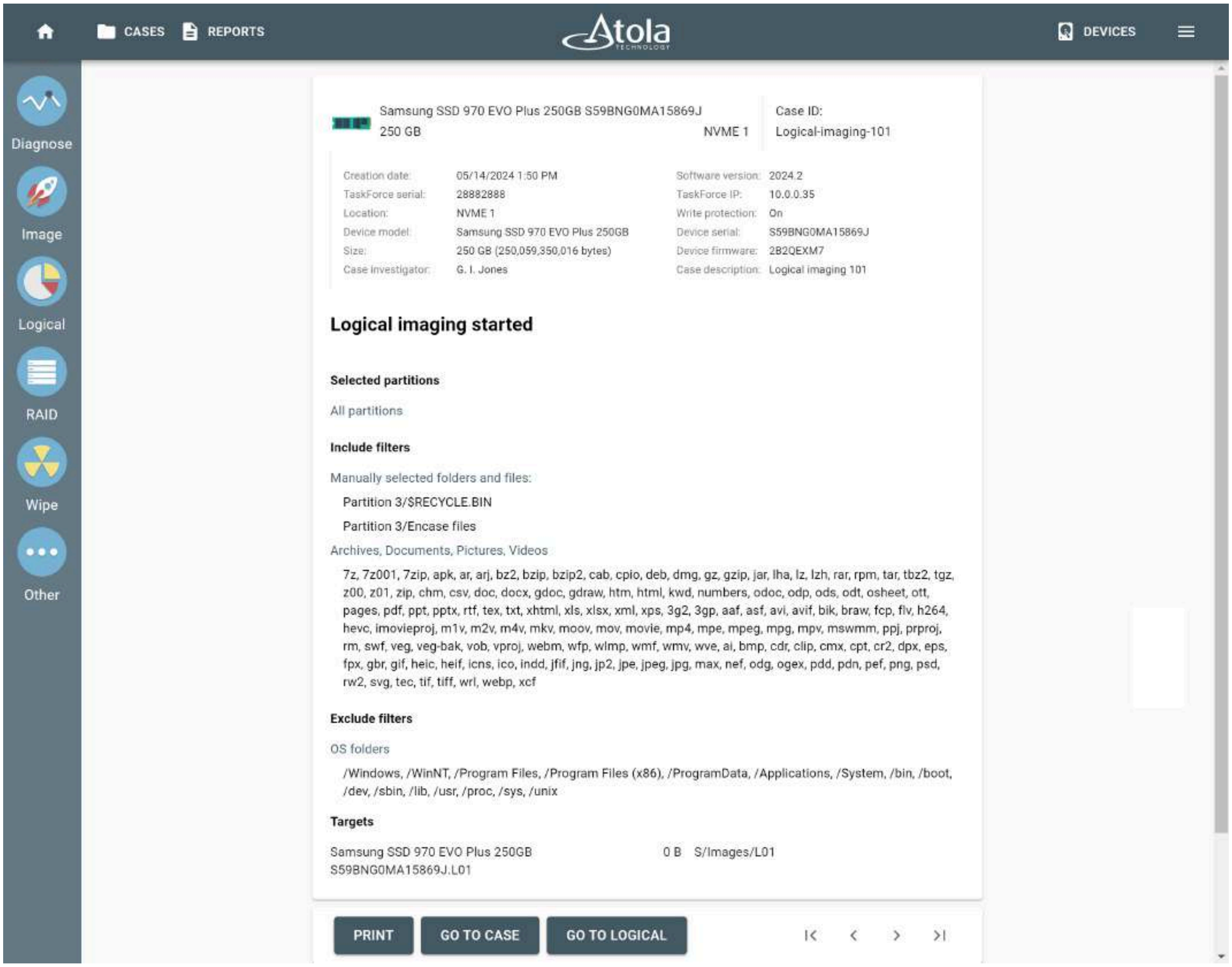
To create a target file on a drive connected directly to the TaskForce, you must first add this drive as a storage device:

1. In the **Select image file** window, click **Add storage**.
2. On the **Select device** panel, choose the drive you want to use in Storage mode. TaskForce uses a lighter shade of blue to indicate that a storage drive is being configured.
3. If TaskForce cannot find the appropriate exFAT partition on the selected drive, it offers you to format the device accordingly. In that case, select the **Format device to exFAT** option and click **Next**.
4. To launch target device formatting to exFat with a large cluster size (32 MB), click **Format** and enter *YES* for confirmation. This cluster size enables faster imaging to this drive.
5. Once the target device is formatted, TaskForce perceives it as a Storage target.

Logical imaging process. Pause and resume

The logical imaging process starts immediately when you click Create in the Create logical image file dialog.

Once imaging is launched, TaskForce creates a **Logical imaging started** report. It contains all details about the imaging source and target(s), as well as information about the include or exclude filters. You can find this report on the Home screen, on the Case page, or the Reports page.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
250 GB NVME 1

Case ID:
Logical-imaging-101

Creation date:	05/14/2024 1:50 PM	Software version:	2024.2
TaskForce serial:	28882888	TaskForce IP:	10.0.0.35
Location:	NVME 1	Write protection:	On
Device model:	Samsung SSD 970 EVO Plus 250GB	Device serial:	S59BNG0MA15869J
Size:	250 GB (250,059,350,016 bytes)	Device firmware:	2B2QEXM7
Case investigator:	G. I. Jones	Case description:	Logical imaging 101

Logical imaging started

Selected partitions

All partitions

Include filters

Manually selected folders and files:

Partition 3/$RECYCLE.BIN

Partition 3/Encase files

Archives, Documents, Pictures, Videos

7z, 7z001, 7zip, apk, ar, arj, bz2, bzip, bzip2, cab, cpio, deb, dmg, gz, gzip, jar, lha, lz, lzh, rar, rpm, tar, tbz2, tgz, z00, z01, zip, chm, csv, doc, docx, gdoc, gdraw, htm, html, kwd, numbers, odoc, odp, ods, odt, osheet, ott, pages, pdf, ppt, pptx, rtf, tex, txt, xhtml, xls, xlsx, xml, xps, 3g2, 3gp, aaf, asf, avi, avif, bik, braw, fcp, flv, h264, hevc, imovieproj, m1v, m2v, m4v, mkv, moov, mov, movie, mp4, mpe, mpeg, mpg, mpv, mswmm, ppj, prproj, rm, swf, veg, veg-bak, vob, vproj, webm, wfp, wlmp, wmf, wmv, wve, ai, bmp, cdr, clip, cmx, cpt, cr2, dpx, eps, fpx, gbr, gif, heic, heif, icns, ico, indd, jfif, jng, jp2, jpe, jpeg, jpg, max, nef, odg, ogex, pdd, pdn, pef, png, psd, rw2, svg, tec, tif, tiff, wrl, webp, xcf

Exclude filters

OS folders

/Windows, /WinNT, /Program Files, /Program Files (x86), /ProgramData, /Applications, /System, /bin, /boot, /dev, /sbin, /lib, /usr, /proc, /sys, /unix

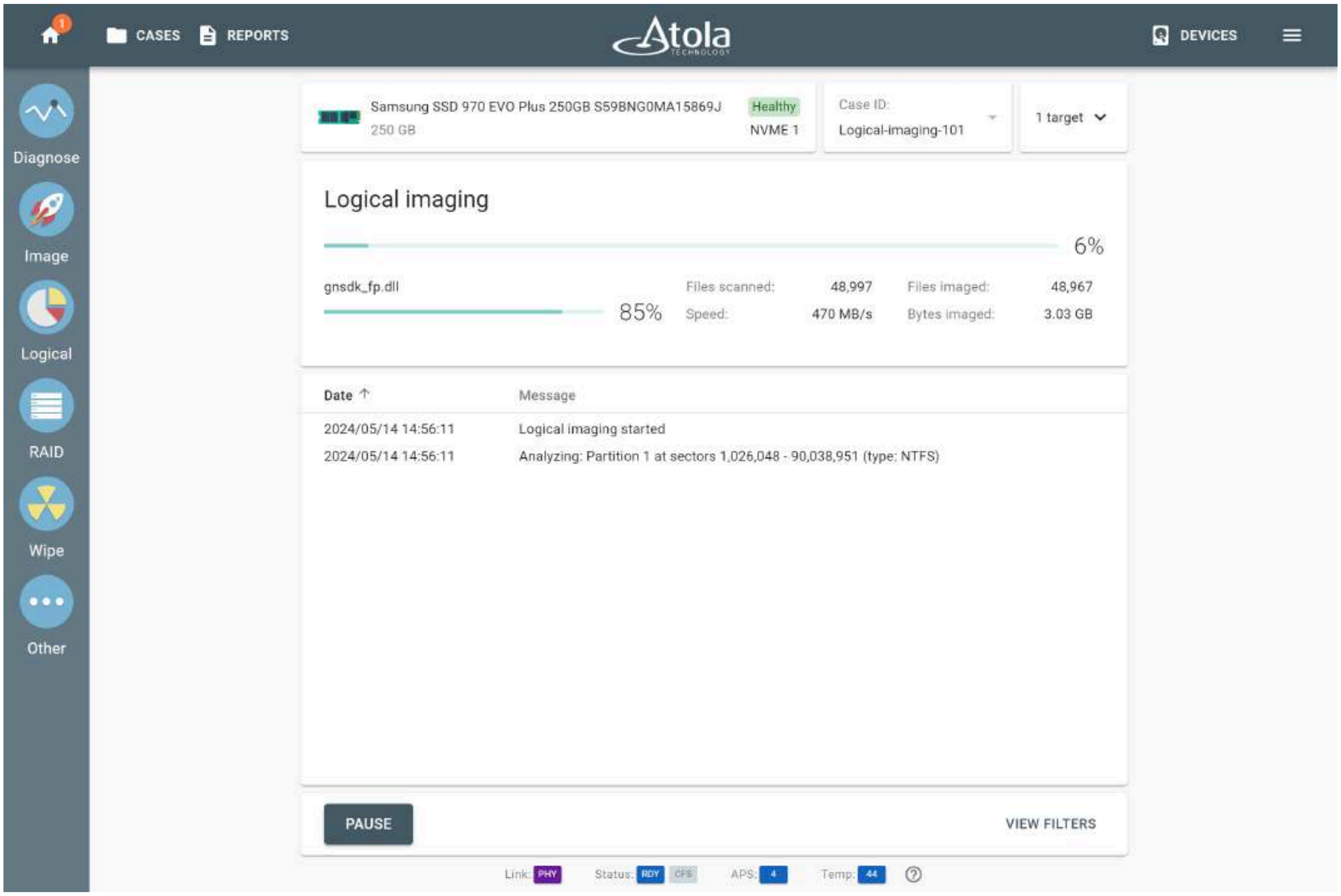
Targets

Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J.L01	0 B	S/Images/L01

A Logical imaging started report.

During the imaging process, you can track the progress of individual files.

To check the filtering parameters of this running session, click **View filters** at the bottom of the page.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J Healthy
250 GB NVME 1

Case ID: Logical-imaging-101

1 target

Logical imaging

6%

gnsdk_fp.dll 85%

Files scanned: 48,997
Speed: 470 MB/s
Files imaged: 48,967
Bytes imaged: 3.03 GB

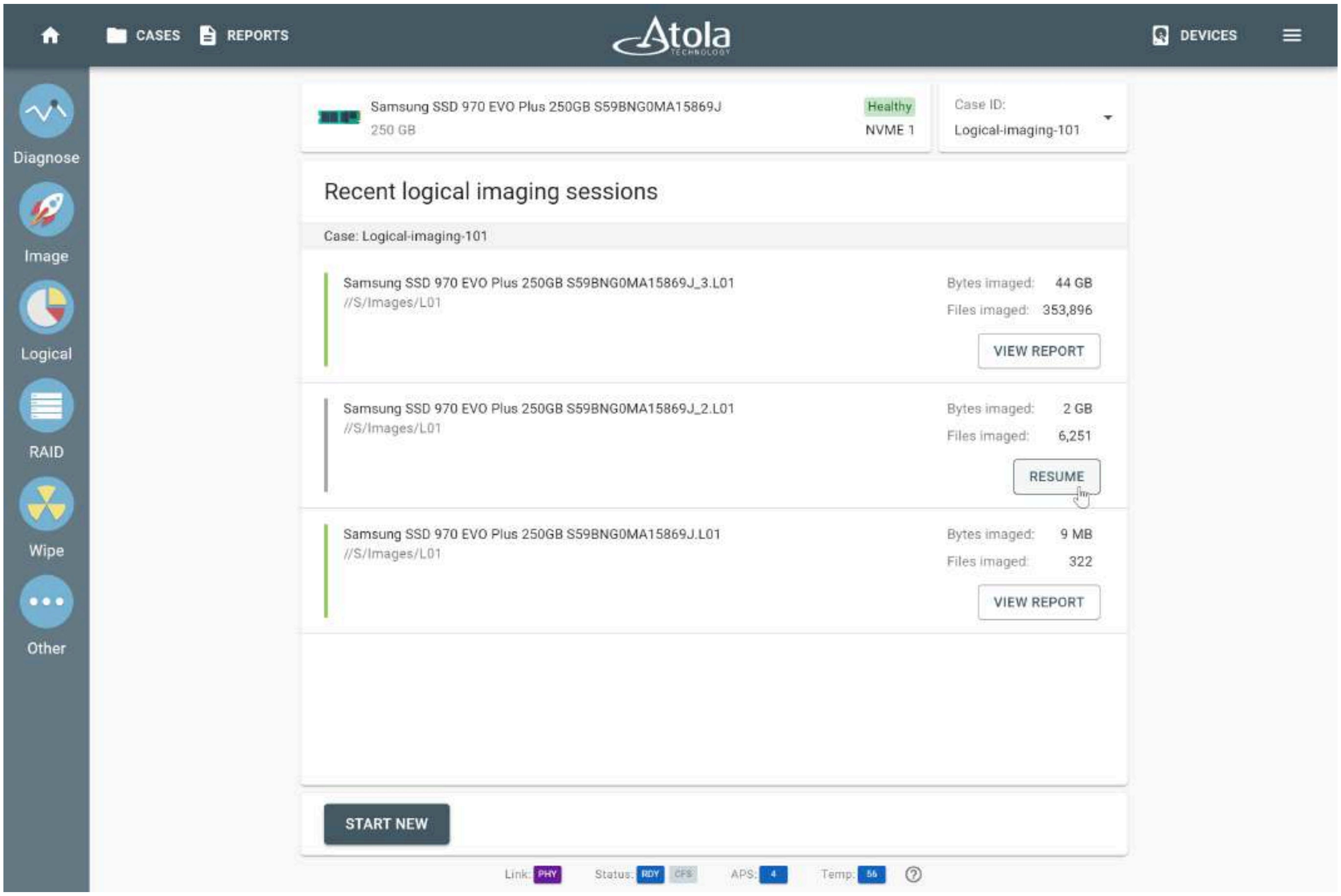
Date	Message
2024/05/14 14:56:11	Logical imaging started
2024/05/14 14:56:11	Analyzing: Partition 1 at sectors 1,026,048 - 90,038,951 (type: NTFS)

The logical imaging process.

Pause and Resume

TaskForce lets you pause any logical imaging session and resume it later:

1. While the logical imaging process is running, click the **Pause** button at the bottom of the page.
2. To resume a session, click **Logical** on the Taskbar and then select your source device.
3. On the **Recent logical imaging sessions** page, click **Resume** next to your session.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J Healthy
250 GB NVME 1

Case ID: Logical-imaging-101

Recent logical imaging sessions

Case: Logical-imaging-101

Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J_3.L01
//S/Images/L01
Bytes imaged: 44 GB
Files imaged: 353,896

Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J_2.L01
//S/Images/L01
Bytes imaged: 2 GB
Files imaged: 6,251

Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J.L01
//S/Images/L01
Bytes imaged: 9 MB
Files imaged: 322

Resuming the logical imaging session.

Use cases of Pause/Resume

When you have to temporarily power off your TaskForce:

1. Pause logical data acquisition.
2. Turn off the TaskForce.
3. Power it on later.
4. Resume the logical imaging session exactly from the very "pause" moment.

When you want your colleague to continue imaging on another TaskForce:

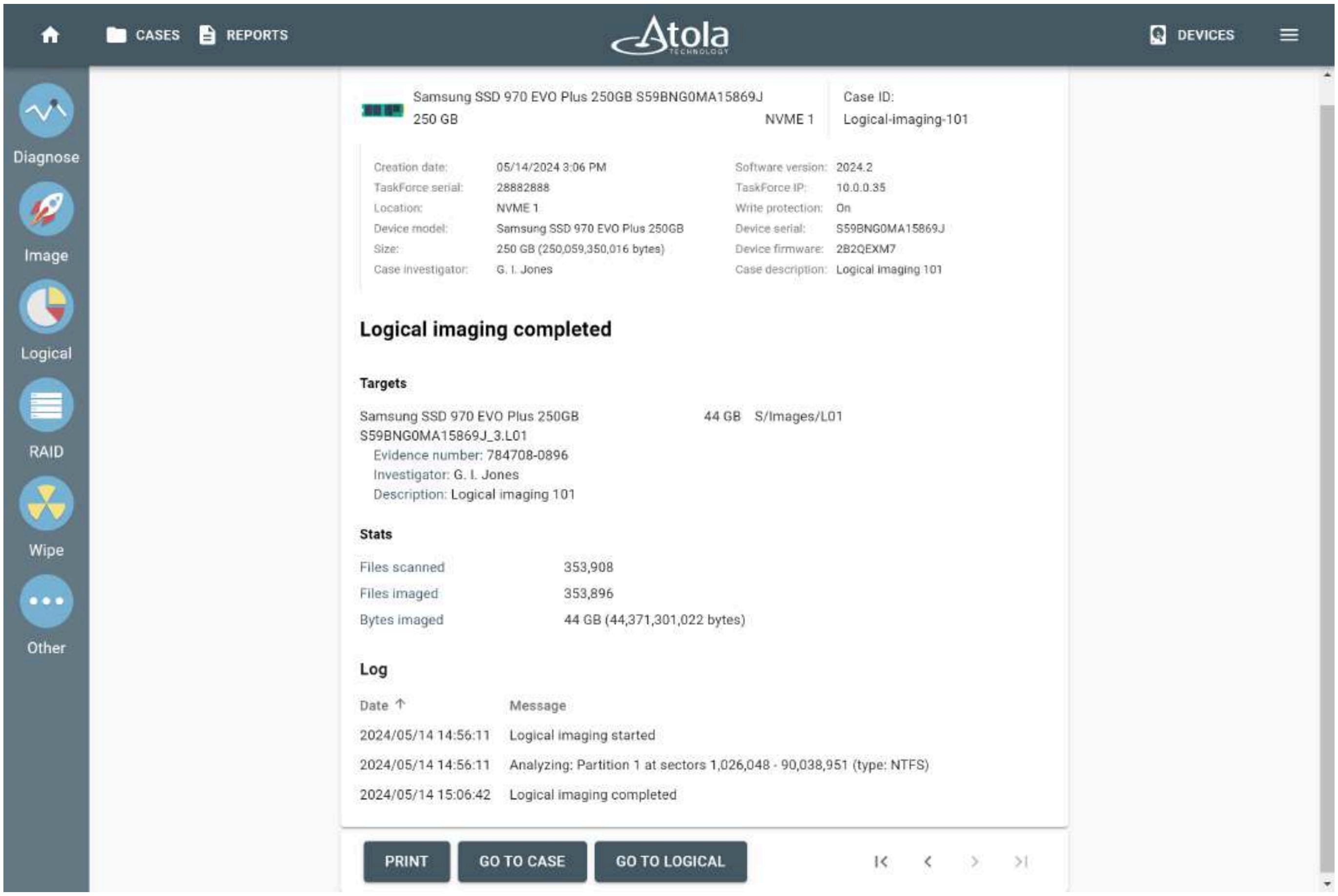
1. Pause logical data acquisition.
2. Export the case.
3. Transfer the source drive and the exported case to a different location that has another TaskForce.
4. Import the case.
5. Resume the logical imaging session.

Logical imaging completed report

After the logical imaging process is completed, TaskForce 2 generates a comprehensive report with all the details of the imaged data:

- The number of scanned and imaged files
- The volume of imaged data
- Time stamps
- and more

You can find this report on the **Home screen**, on the **Case** page, or on the **Reports** page.



Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J
250 GB NVME 1

Case ID:
Logical-imaging-101

Creation date:	05/14/2024 3:06 PM	Software version:	2024.2
TaskForce serial:	28882888	TaskForce IP:	10.0.0.35
Location:	NVME 1	Write protection:	On
Device model:	Samsung SSD 970 EVO Plus 250GB	Device serial:	S59BNG0MA15869J
Size:	250 GB (250,059,350,016 bytes)	Device firmware:	2B2QEXM7
Case investigator:	G. I. Jones	Case description:	Logical imaging 101

Logical imaging completed

Targets

Samsung SSD 970 EVO Plus 250GB S59BNG0MA15869J_3.L01 44 GB S/Images/L01
Evidence number: 784708-0896
Investigator: G. I. Jones
Description: Logical imaging 101

Stats

Files scanned	353,908
Files imaged	353,896
Bytes imaged	44 GB (44,371,301,022 bytes)

Log

Date ↑	Message
2024/05/14 14:56:11	Logical imaging started
2024/05/14 14:56:11	Analyzing: Partition 1 at sectors 1,026,048 - 90,038,951 (type: NTFS)
2024/05/14 15:06:42	Logical imaging completed

The 'Logical imaging completed' report.

Imaging only sectors with data

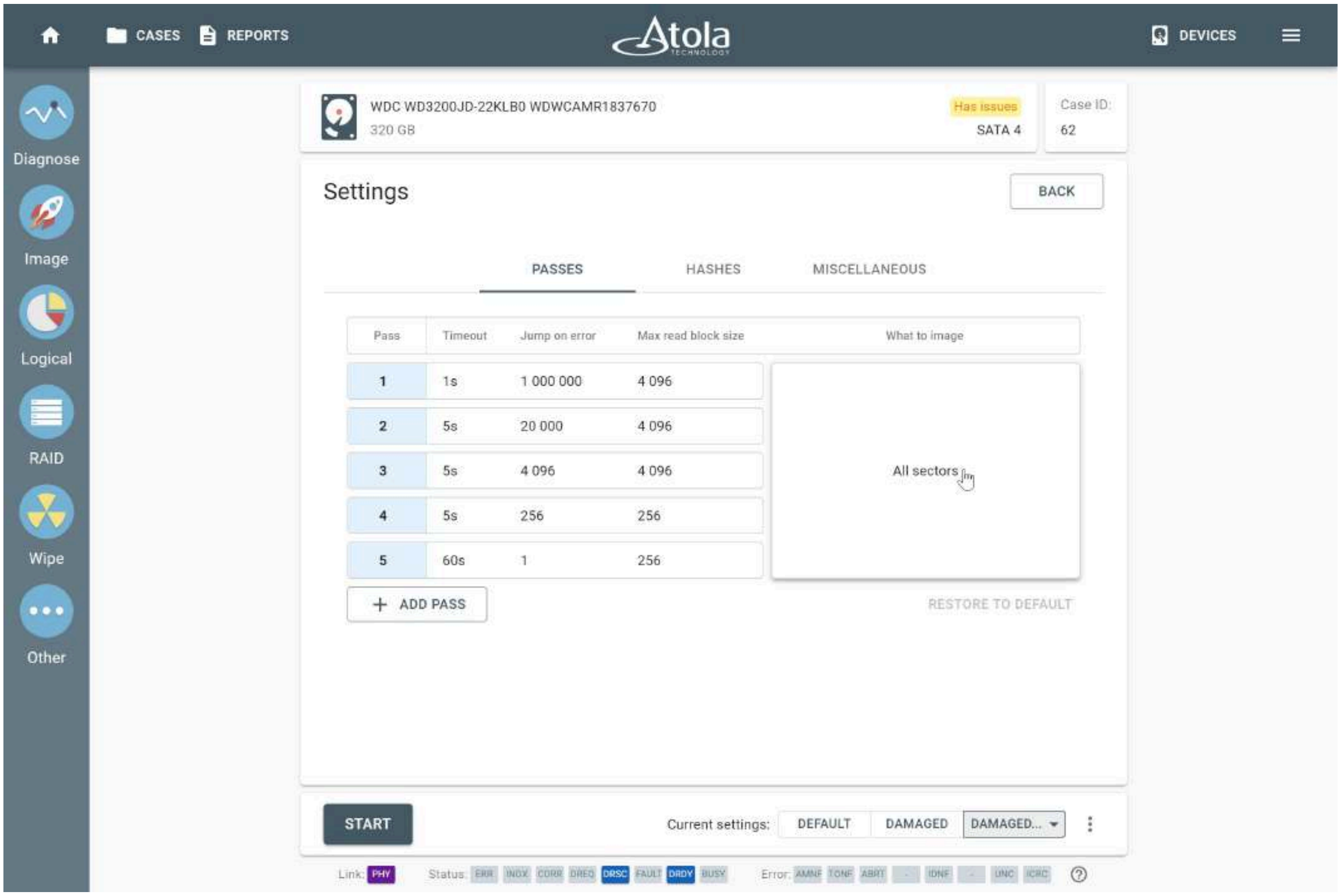
Capacity of an average drive is constantly growing, and selective imaging becomes a way out for many investigators to keep their backlogs smaller.

We at Atola have developed selective imaging functionality to make it possible to image only sectors containing data.

The feature is supported in these file systems: NTFS, APFS, XFS, ext2/3/4, HFS, HFS+, ExFAT, FAT16, FAT32.

To image only sectors with data, do the following:

1. On the **Imaging settings** page, click **Change** to adjust imaging settings.
2. On the **Passes** tab, click on the value in the **What to image** column.



WDC WD3200JD-22KLB0 WDWCAMR1837670
320 GB
SATA 4
Case ID: 62

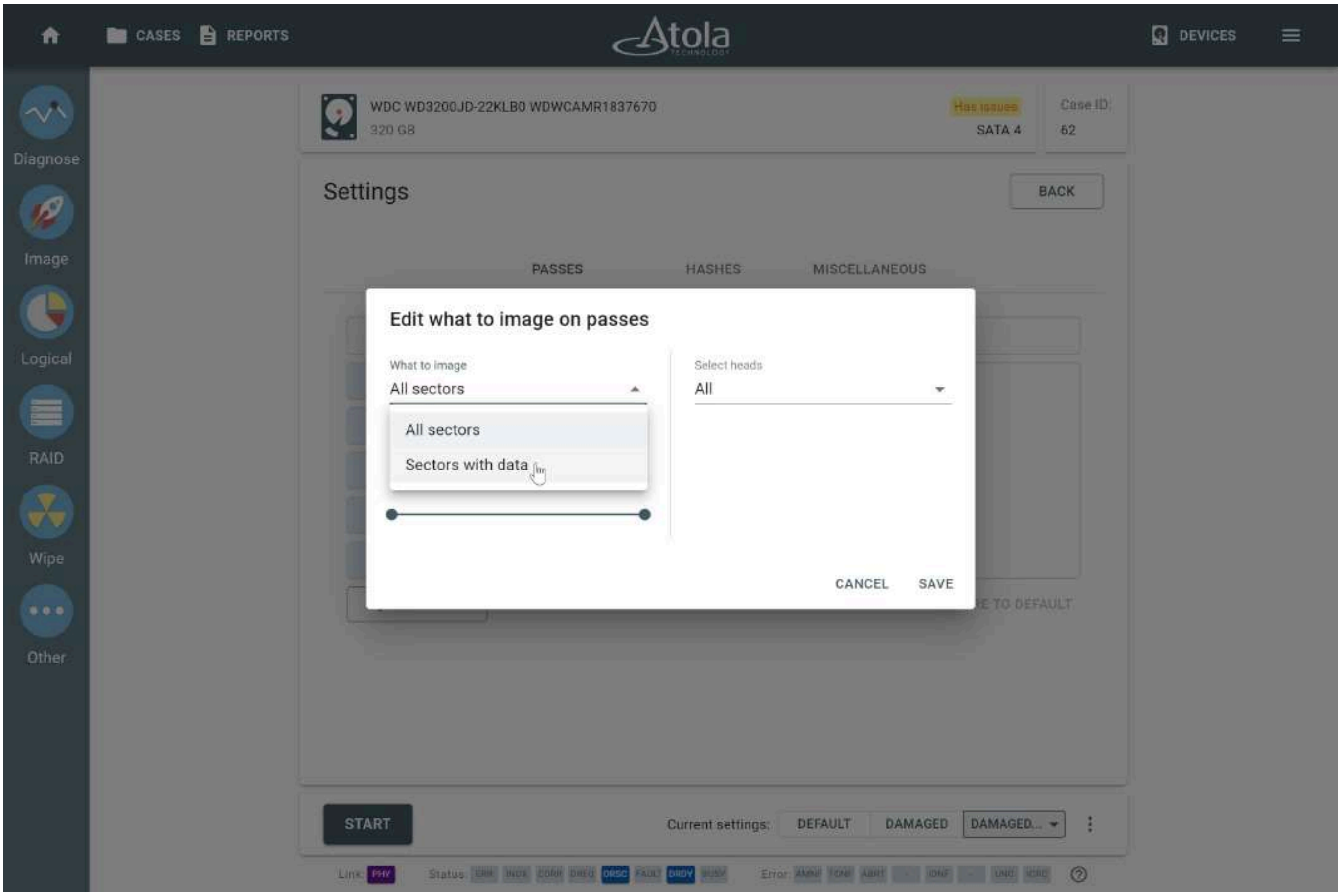
Settings

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	All sectors
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

Current settings: DAMAGED...

The value in the What to image column.

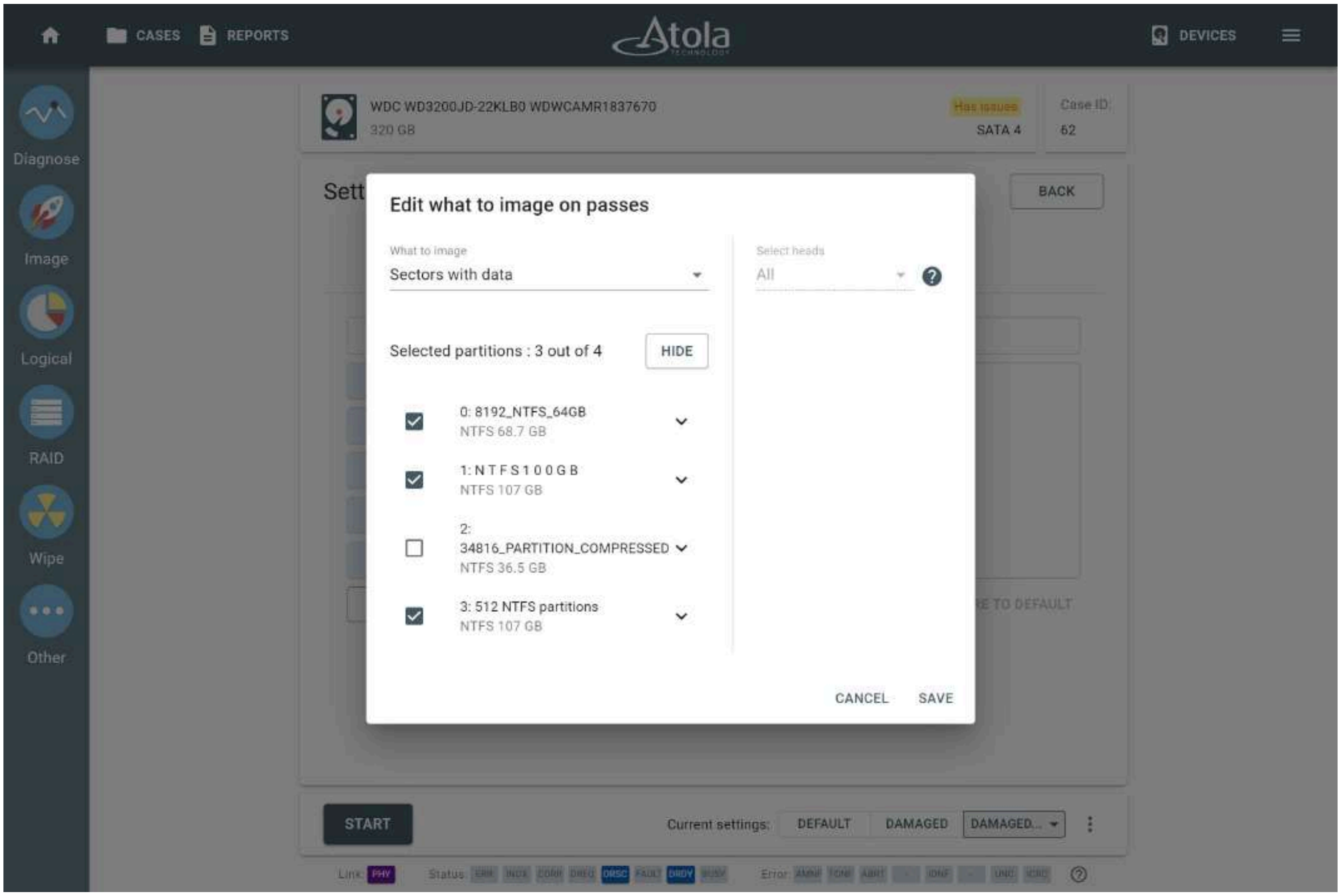
3. In the **Edit what to image on passes** dialog, select **Sectors with data**.



Selecting the Sectors with data option.

4. To preview the partitions on the source drive, click **Show**.

> Imaging individual partitions is possible: just unselect the partitions you do not want to image. The imaging report will document this setting and indicate, which of the partitions have been imaged and the sector ranges in which the partitions were located.



Edit what to image on passes

What to image: Sectors with data

Select heads: All

Selected partitions : 3 out of 4

☑ 0: 8192_NTFS_64GB
NTFS 68.7 GB

☑ 1: N T F S 1 0 0 G B
NTFS 107 GB

☐ 2: 34816_PARTITION_COMPRESSED
NTFS 36.5 GB

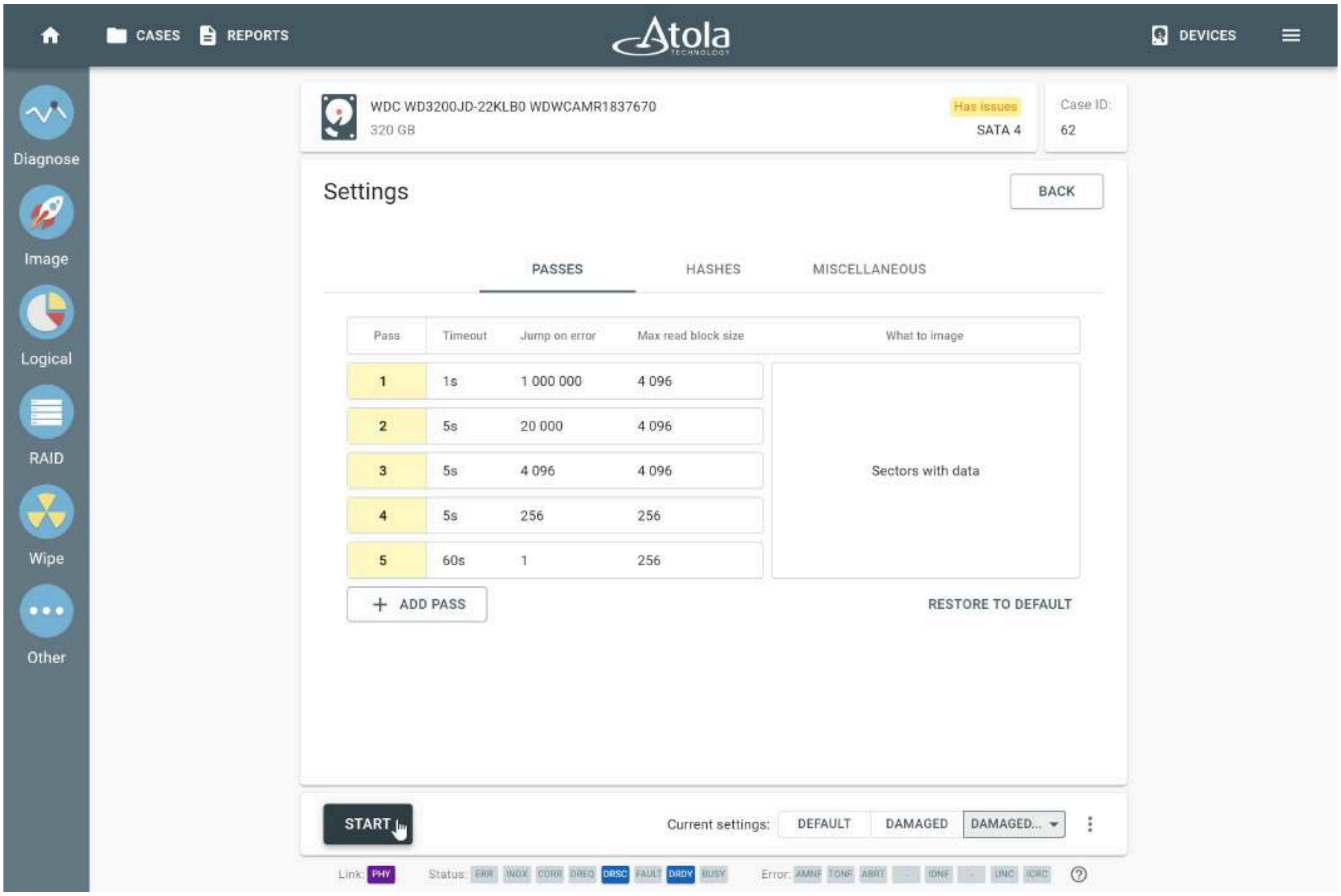
☑ 3: 512 NTFS partitions
NTFS 107 GB

Current settings: DAMAGED...

Partitions preview.

5. In the **Edit what to image on passes** dialog, click **Save**.

6. To proceed with imaging, click **Start**.



WDC WD3200JD-22KLB0 WDWCAMR1837670
320 GB
Has issues
SATA 4
Case ID:
62

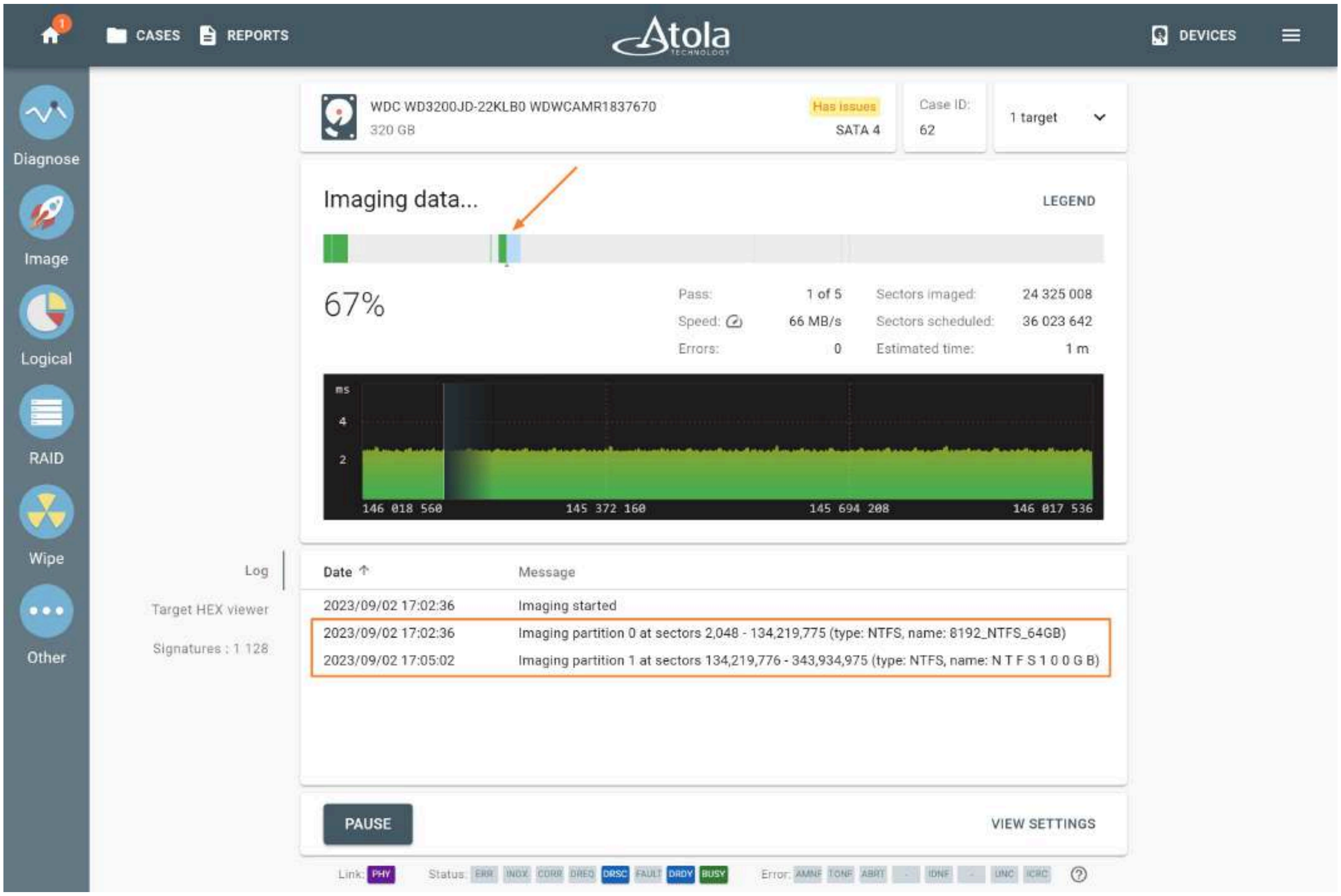
Settings

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1 000 000	4 096	Sectors with data
2	5s	20 000	4 096	
3	5s	4 096	4 096	
4	5s	256	256	
5	60s	1	256	

+ ADD PASS
RESTORE TO DEFAULT
START
Current settings:
DEFAULT
DAMAGED
DAMAGED...
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

The Start button on the Imaging settings page.

You can see the partitions being imaged in the imaging log. In the imaging bar, the blue areas represent the sectors that are planned to be imaged. These are the sectors that belong to the drive's partitions and contain data.



WDC WD3200JD-22KLB0 WDWCAMR1837670
320 GB
SATA 4
Case ID: 62
1 target

Imaging data...

67%

Pass: 1 of 5
Speed: 66 MB/s
Errors: 0
Sectors imaged: 24 325 008
Sectors scheduled: 36 023 642
Estimated time: 1 m

```
Date                 Message
2023/09/02 17:02:36  Imaging started
2023/09/02 17:02:36  Imaging partition 0 at sectors 2,048 - 134,219,775 (type: NTFS, name: 8192_NTFS_64GB)
2023/09/02 17:05:02  Imaging partition 1 at sectors 134,219,776 - 343,934,975 (type: NTFS, name: N T F S 1 0 0 G B)
```

Information about the partitions imaged in the log.

Imaging cheat sheet

When source drive is damaged

Use these imaging settings and follow the recommendations to cope with severely damaged drives.

Optimal target types for damaged source device

AFF4 image, RAW image file, or target drive plugged into the unit. Best to use segmented hashing with linear hashing disabled.

E01 is a linear format. It limits the use of TaskForce's advanced imaging features, e.g. reverse imaging or manual jumps.

Segmented hashes

Imaging with linear hash: one MD5/SHA1 hash.

Imaging with segmented hashes: many hashes of corresponding LBA ranges of the image.

The sum of these LBA ranges represents the entire image, though not necessarily in sequential order. You can still prove that the entire image has not been modified by verifying all hashes in a set.

Damaged head

If Diagnostics detects a damaged or degraded head, disable the head in the imaging settings for the initial imaging session.

Read more here: Imaging a drive with a damaged head.

Damaged SATA drive on SAS port

TaskForce's SATA module and ports have more in-depth support of damaged SATA drives than the SAS subsystem. For instance, SAS doesn't allow sending so-called vendor ATA commands that TaskForce uses in SATA to detect heads.

To be most effective against damaged SATA drives, it is best to connect them to SATA ports.

USB drive read errors

Use high-quality short USB3 cables. Longer or lower-quality USB3 cables can produce read errors during imaging.

Reverse direction

Imaging pass setting.

When enabled, the imaging engine reads a drive backwards.

Pros:

- disables Read Look-Ahead effect
- reaches damaged areas from the opposite direction

Cons:

- speed decreases due to auto disabling of drive's cache

Manually skip bad sectors

If TaskForce can’t read a block from a source device, it will automatically skip sectors and try to image them on later passes. When the imaging process seems to be stuck, you can move the imaging cursor manually by clicking another area on the top progress bar.
Manual sector jumps work only if linear hashing is disabled. You can use segmented hashing instead.

Disable read look-ahead

Imaging pass setting.

When enabled, a source device switches off its read-cache. Disabling read look-ahead decreases speed; but, it can be helpful against damaged drives.

Last imaging pass is too slow

Reduce a max time for a single read block attempt:

1. Pause imaging.

2. Add a new pass.
3. Change its Timeout setting to 500 ms (milliseconds).
4. Use the Go to pass button to switch to the newly added pass.

How imaging works on the last pass

The last pass has a unique feature which does not occur during previous passes: internal auto-reread procedure for error block sector-by-sector. It is defined by an unchangeable Jump size = 1 sector.

How imaging engine works on the last pass:

1. It reads block using Max Block Size pass setting (256 by default)
2. If reading is successful -> proceed to a next non-imaged block
3. If a read error occurs -> re-read the whole error block sector by sector.
4. If a read error occurs and ReadLong setting is enabled -> re-read using ReadLong command.

Faster imaging

If you want to speed up image acquisition, follow these hints.

Diagnose source before imaging

How it is useful:

1. Make sure the drive is in good condition or learn about the type of damage to make an informed decision about your following steps.
2. Prioritize the drive. Diagnostics report tells you if there is any data at all.
3. Use imaging time estimation.

Use faster targets

Good options:

- target SSD
- target NAS
- network server with RAID

When imaging a network, 10Gbit network connection is highly recommended.

When to use Logical imaging

- Time-constrained scenarios
- Large capacity drives (e.g., 10TB and above) or RAID arrays
- When specific files are of interest, not the entire drive

Image output format will be L01 or zip.

Change the timeout for a single read block attempt on-the-fly

You can read the data from your source device with a different timeout by adding another pass to your imaging session when it’s paused:

1. Pause the currently running imaging, using the **Pause** button.
2. Click **Image** and select your Source device.
3. On the Recent imaging sessions page, find your paused session and click the **Edit imaging settings** icon next to it.
4. In the Imaging settings dialog, click **Add pass**.
5. Click on the new pass, edit the **Timeout** value and **Save** it.
6. Select the new pass, click **Go to Pass** and **Apply**.
7. Next to your paused session, click the **Resume** button.

Important: The resumed imaging session will complement the data imaged prior to the pause with only the sectors that were not yet copied.

Express mode

Express mode is ideal for processing large amounts of data quickly. It automatically starts an imaging session for a newly inserted drive:

1. In the TaskForce window, go to system **Menu** > **Express mode**.
2. Specify Express mode **Settings** and click **Activate**.
3. Plug devices into Source ports: SATA, SAS, USB, IDE.
4. Imaging will start automatically.
5. If imaging doesn't start and the corresponding front LED is off, check the Home screen.

Integrate TaskForce into your workflow via Web API

Web API helps external software to communicate with TaskForce. Another software may control TaskForce this way. To put it simply, there are simple operations in TaskForce Web API that any external software can run:

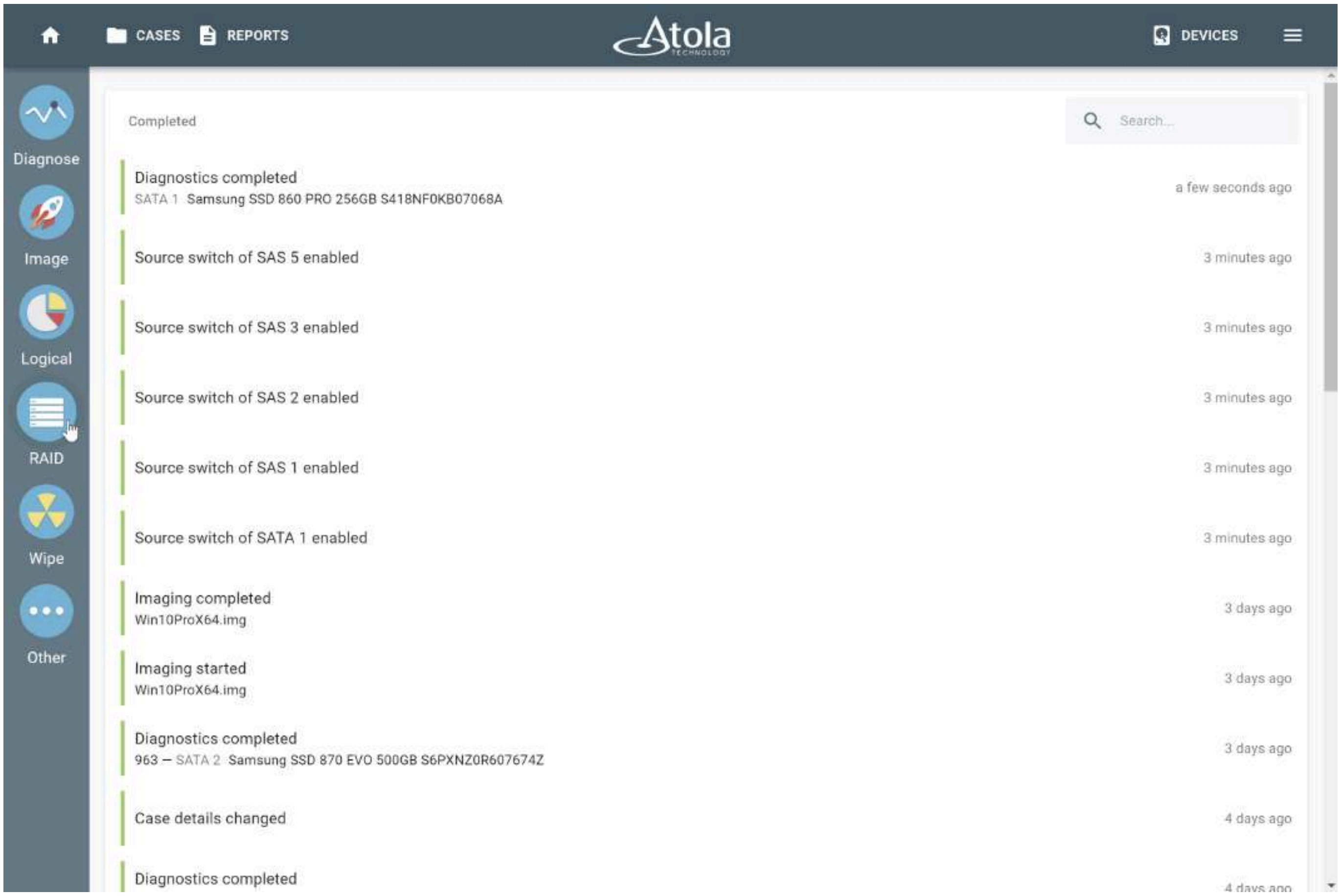
- Get available Source drives
- Optionally: diagnose drives
- Start imaging
- Check task status
- Stop running task (if necessary)
- Download created report

RAID 0 imaging

Atola TaskForce 2 can automatically detect a RAID 0 configuration, assemble and image such RAID array.

Assembling a RAID 0 with unknown configuration

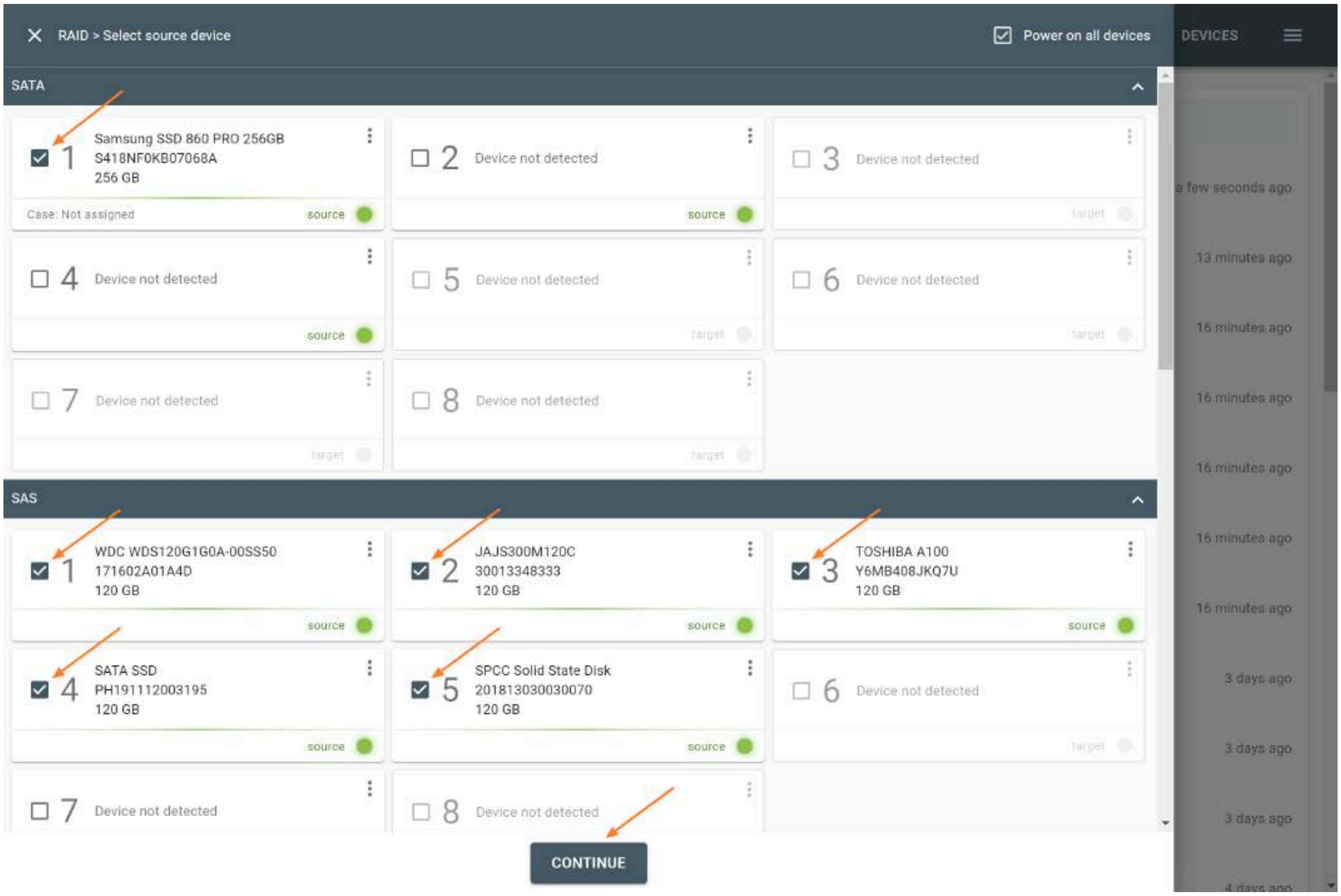
1. Connect the drives to the TaskForce hardware unit's ports that are switched to the Source mode.
2. On the left in the TaskForce main window, click **RAID**.



Completed

Diagnostics completed SATA 1 Samsung SSD 860 PRO 256GB S418NF0KB07068A	a few seconds ago
Source switch of SAS 5 enabled	3 minutes ago
Source switch of SAS 3 enabled	3 minutes ago
Source switch of SAS 2 enabled	3 minutes ago
Source switch of SAS 1 enabled	3 minutes ago
Source switch of SATA 1 enabled	3 minutes ago
Imaging completed Win10ProX64.img	3 days ago
Imaging started Win10ProX64.img	3 days ago
Diagnostics completed 963 — SATA 2 Samsung SSD 870 EVO 500GB S6PXNZ0R607674Z	3 days ago
Case details changed	4 days ago
Diagnostics completed	4 days ago

3. On the **Select source device** panel, select the drives that make up a RAID array and click **Continue**.



Selecting source RAID drives.

You can see key RAID configuration parameters at the top of the page:

- Order of drives/images
- RAID type
- Start LBA
- Block size
- Block order

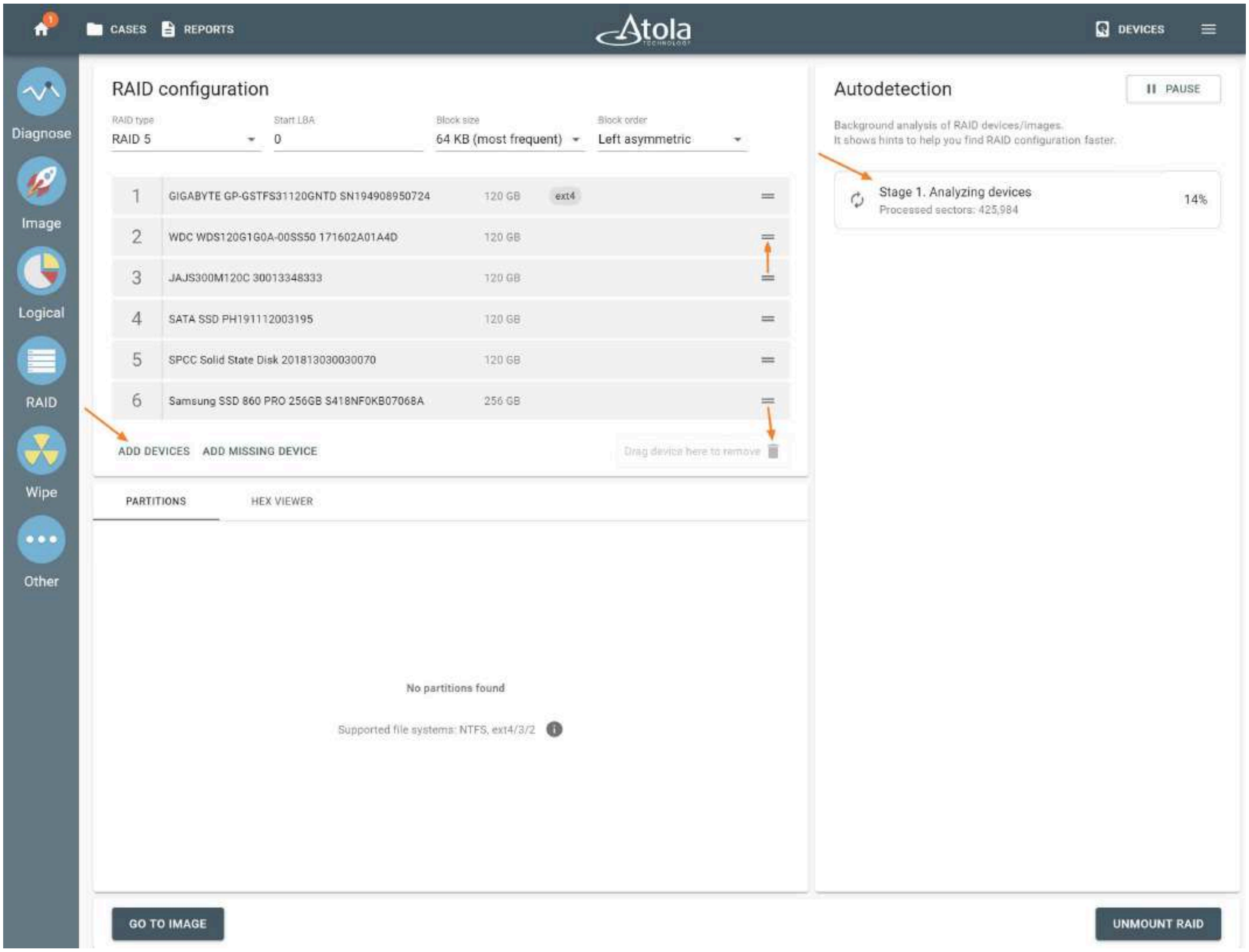
Before you enter other values either manually or by applying Autodetection module results, the most commonly used values are displayed in the given fields.

The **Autodetection module** starts running immediately.

RAID 0 autodetection

Stage 1: TaskForce 2 is reading data on the drives to identify the RAID type.

To change the order of drives in the array, simply drag a drive to its new position. To remove a device from the current array, grab it and put it into the bin.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most frequent)
Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD SN194908950724	120 GB	ext4
2	WDC WDS120G1G0A-00SS50 171602A01A4D	120 GB	
3	JAJS300M120C 30013348333	120 GB	
4	SATA SSD PH191112003195	120 GB	
5	SPCC Solid State Disk 201813030030070	120 GB	
6	Samsung SSD 860 PRO 256GB S418NF0KB07068A	256 GB	

No partitions found

Supported file systems: NTFS, ext4/3/2

Autodetection

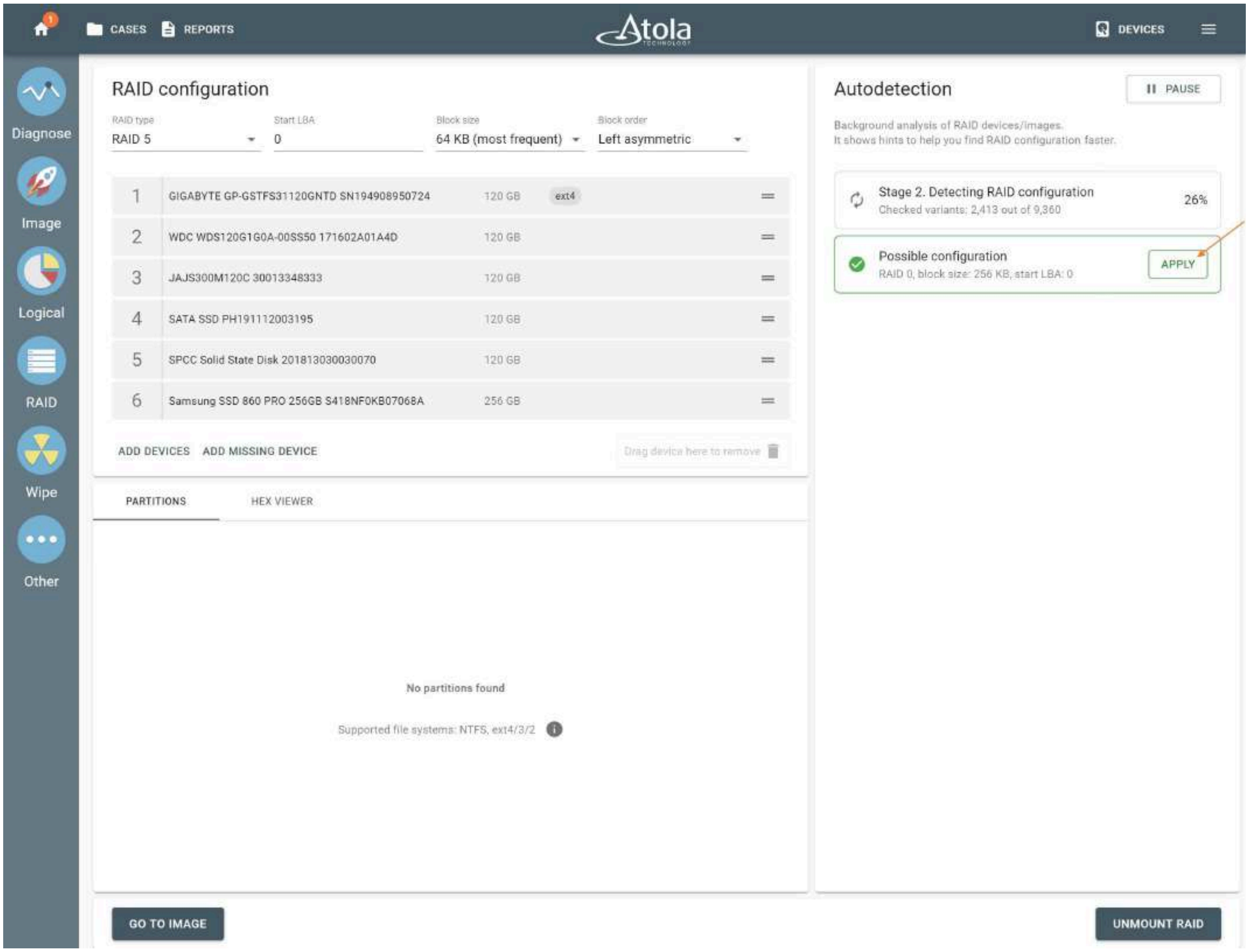
Background analysis of RAID devices/images.
It shows hints to help you find RAID configuration faster.

Stage 1. Analyzing devices
Processed sectors: 425,984
14%

Analyzing devices.

Stage 2: TaskForce 2 goes through thousands of possible variants of RAID parameters.

Click **Apply** as soon as a **Possible configuration** tile appears.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most frequent)
Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD SN194908950724	120 GB	ext4
2	WDC WDS120G1G0A-00SS50 171602A01A4D	120 GB	
3	JAJS300M120C 30013348333	120 GB	
4	SATA SSD PH191112003195	120 GB	
5	SPCC Solid State Disk 201813030030070	120 GB	
6	Samsung SSD 860 PRO 256GB S418NF0KB07068A	256 GB	

No partitions found

Supported file systems: NTFS, ext4/3/2

Autodetection

Background analysis of RAID devices/images.
It shows hints to help you find RAID configuration faster.

Stage 2. Detecting RAID configuration 26%
Checked variants: 2,413 out of 9,360

Possible configuration
RAID 0, block size: 256 KB, start LBA: 0

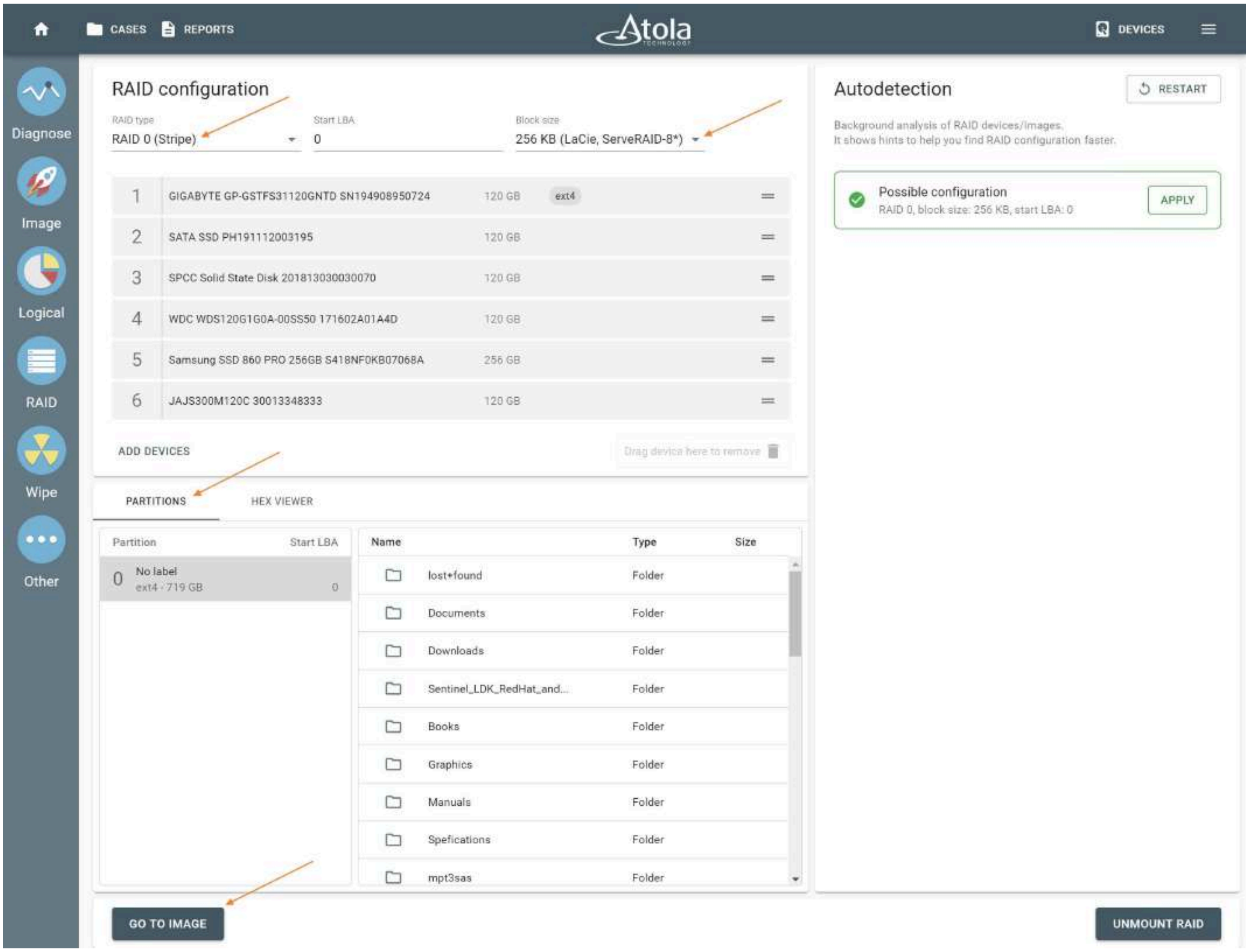
Possible RAID configuration.

After you click **Apply**, TaskForce 2 automatically applies the suggested configuration and checks the file system for partitions. At the bottom of the screen, a preview of the partitions is available.

Observing files and folders in the preview confirms the detected RAID 0 configuration is correct.

Imaging RAID 0 array

1. After RAID configuration is successfully applied, click **Go to Image** to proceed with imaging.



RAID configuration

RAID type: RAID 0 (Stripe)
Start LBA: 0
Block size: 256 KB (LaCie, ServeRAID-8*)

1	GIGABYTE GP-GSTFS31120GNTD SN194908950724	120 GB	ext4
2	SATA SSD PH191112003195	120 GB	
3	SPCC Solid State Disk 201813030030070	120 GB	
4	WDC WDS120G1G0A-00SS50 171602A01A4D	120 GB	
5	Samsung SSD 860 PRO 256GB S418NF0KB07068A	256 GB	
6	JAJS300M120C 30013348333	120 GB	

ADD DEVICES
Drag device here to remove

PARTITIONS HEX VIEWER

Partition	Start LBA
0 No label ext4 · 719 GB	0

Name	Type	Size
lost+found	Folder	
Documents	Folder	
Downloads	Folder	
Sentinel_LDK_RedHat_and...	Folder	
Books	Folder	
Graphics	Folder	
Manuals	Folder	
Spefications	Folder	
mpt3sas	Folder	

GO TO IMAGE

Autodetection

RESTART

Background analysis of RAID devices/images.
It shows hints to help you find RAID configuration faster.

Possible configuration
RAID 0, block size: 256 KB, start LBA: 0

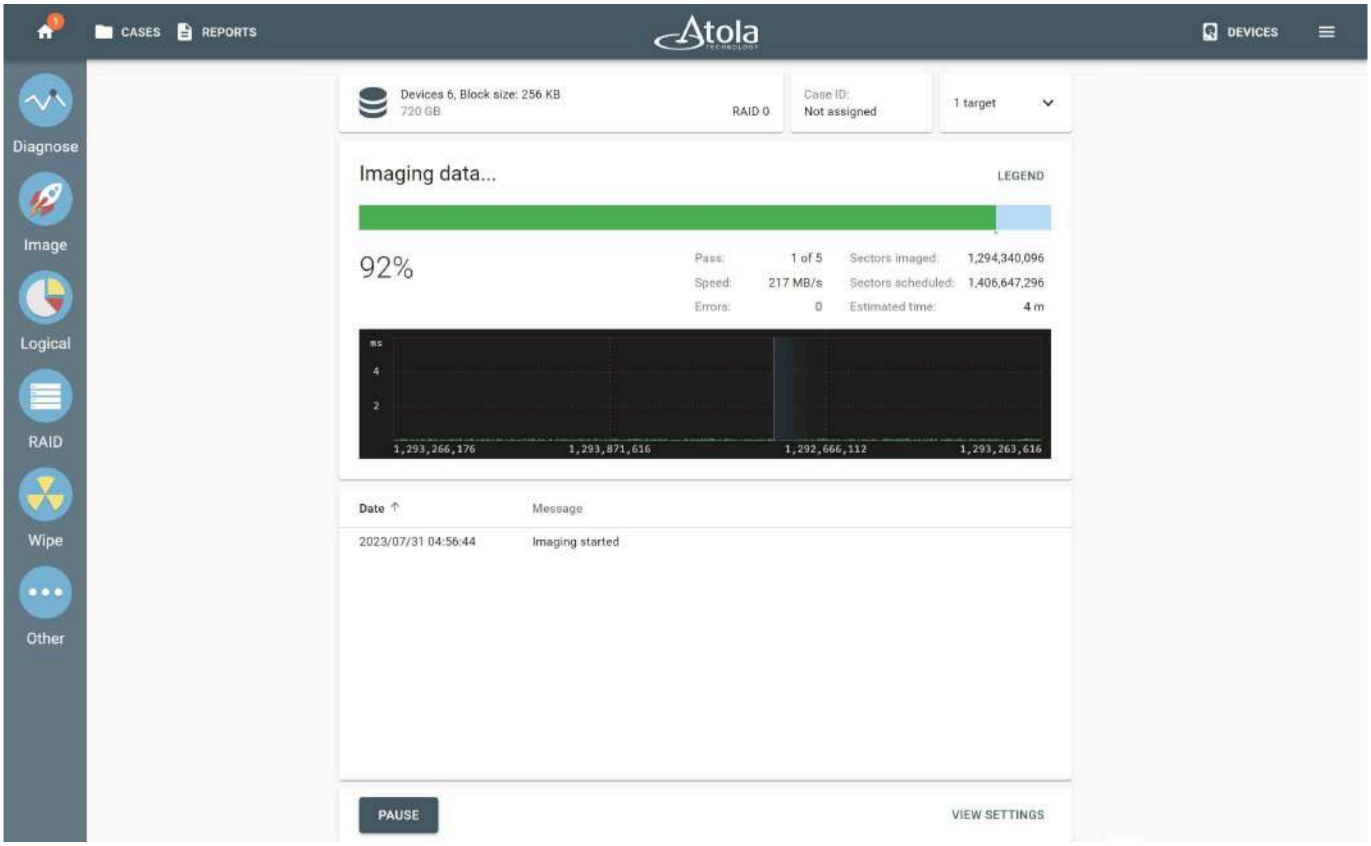
APPLY

UNMOUNT RAID

The Go to image button.

2. Select your target device or network folder and click **Continue**.
3. To launch your imaging session, click **Start**.

RAID imaging may take much longer than imaging a drive. You can optimize the imaging speed by using a fast target or a high-speed server.



Devices 6, Block size: 256 KB
720 GB
RAID 0

Case ID: Not assigned

1 target

Imaging data...

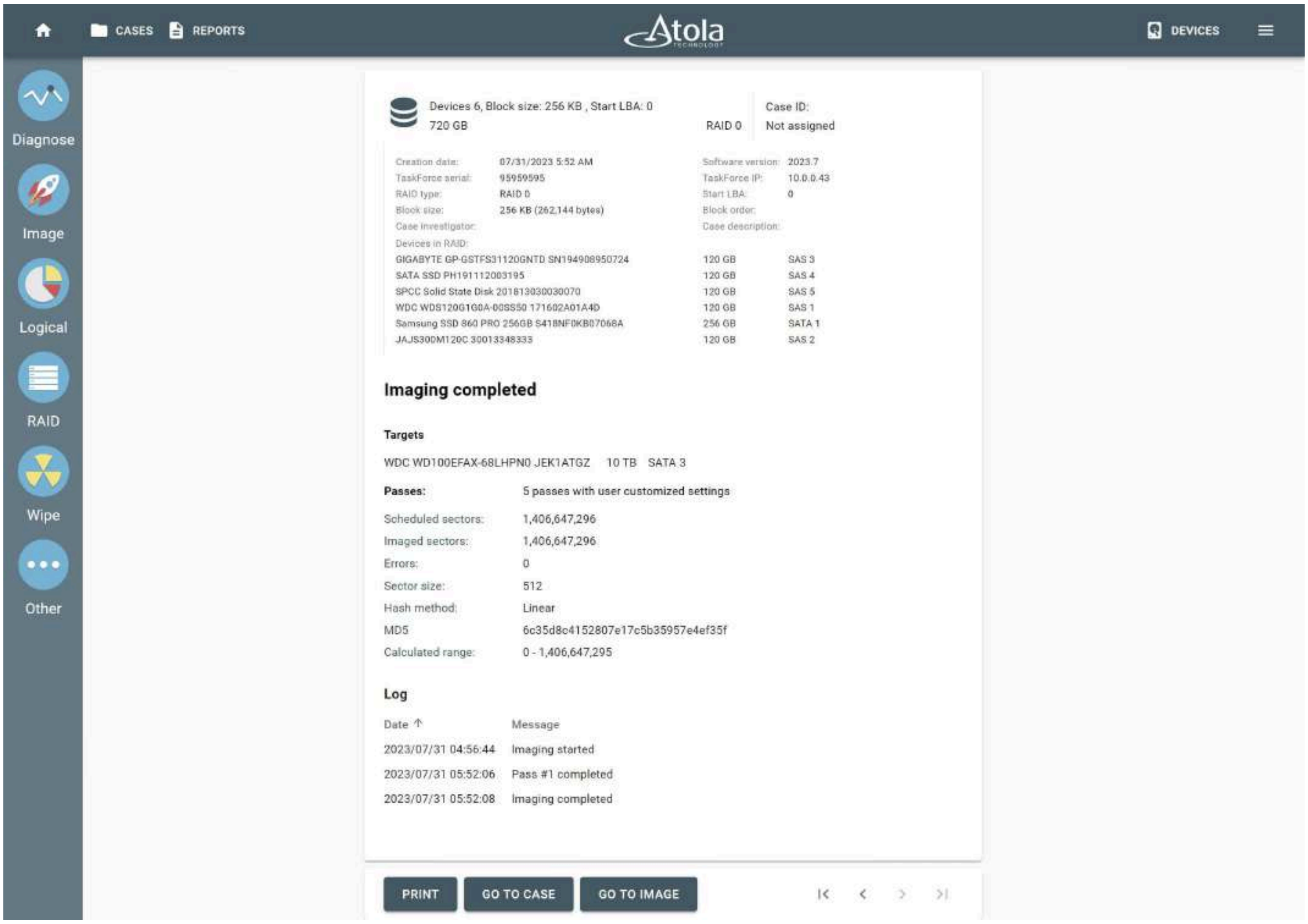
92%

Pass: 1 of 5
Speed: 217 MB/s
Errors: 0
Sectors imaged: 1,294,340,096
Sectors scheduled: 1,406,647,296
Estimated time: 4 m

Date	Message
2023/07/31 04:56:44	Imaging started

How to make raid image.

TaskForce 2 automatically generates reports for every session. The **Imaging completed** report will contain all RAID details as well as timestamps.



Devices 6, Block size: 256 KB , Start LBA: 0
720 GB
RAID 0
Case ID:
Not assigned

Creation date:	07/31/2023 5:52 AM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.43
RAID type:	RAID 0	Start LBA:	0
Block size:	256 KB (262,144 bytes)	Block order:	
Case investigator:		Case description:	

Devices in RAID:

GIGABYTE GP-GSTFS31120GNTD SN194908950724	120 GB	SAS 3
SATA SSD PH191112003195	120 GB	SAS 4
SPCC Solid State Disk 201813030030070	120 GB	SAS 5
WDC WDS120G1G0A-00SS50 171602A01A4D	120 GB	SAS 1
Samsung SSD 860 PRO 256GB S418NF0KB07068A	256 GB	SATA 1
JAJS300M120C 30013348333	120 GB	SAS 2

Imaging completed

Targets

WDC WD100EFAX-68LHPN0 JEK1ATGZ 10 TB SATA 3

Passes:	5 passes with user customized settings
Scheduled sectors:	1,406,647,296
Imaged sectors:	1,406,647,296
Errors:	0
Sector size:	512
Hash method:	Linear
MD5	6c35d8c4152807e17c5b35957e4ef35f
Calculated range:	0 - 1,406,647,295

Log

Date ↑	Message
2023/07/31 04:56:44	Imaging started
2023/07/31 05:52:06	Pass #1 completed
2023/07/31 05:52:08	Imaging completed

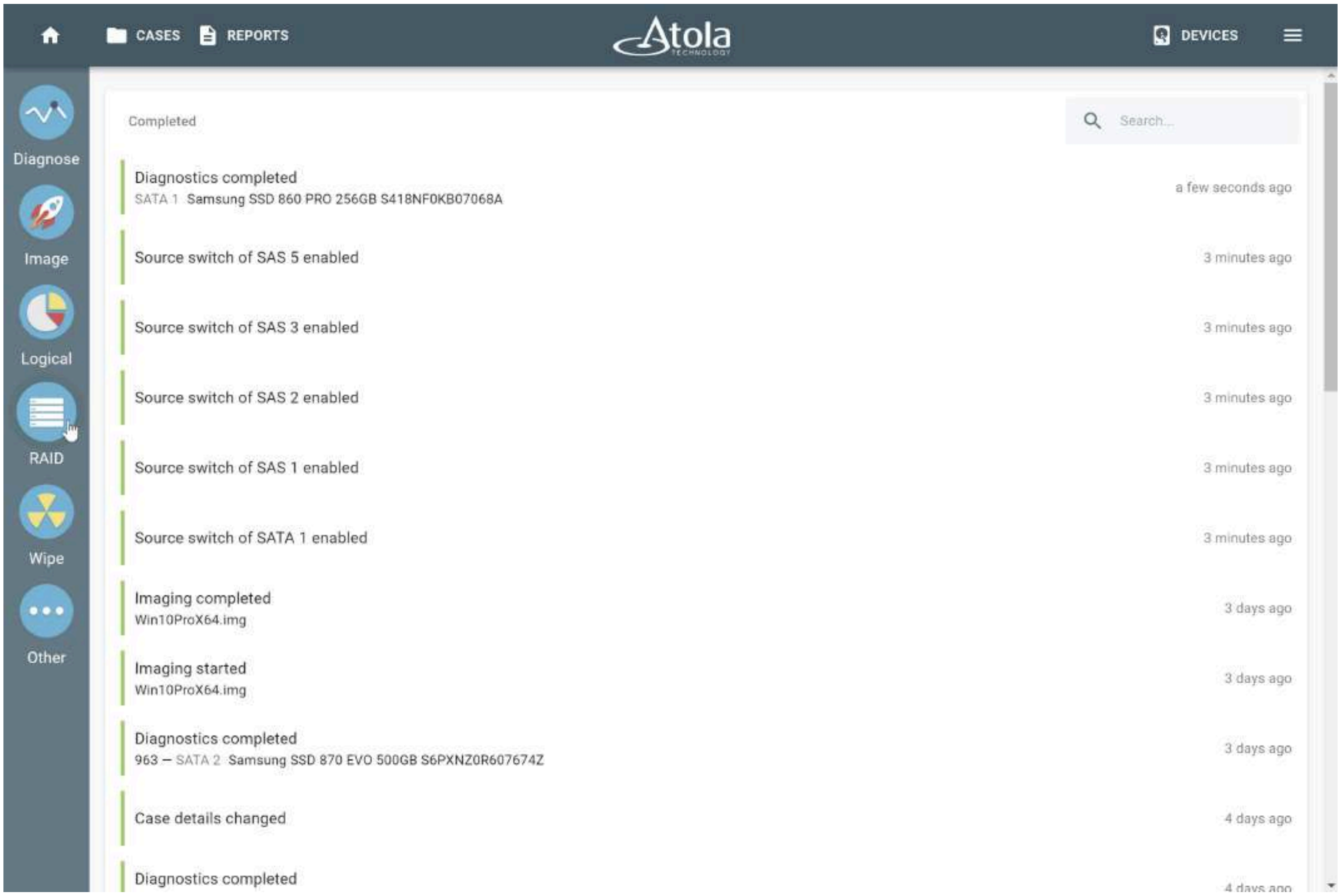
The Imaging completed report.

RAID 5 forensics: Automated reassembly and imaging

TaskForce 2 is equipped with configuration autodetection module that makes assembling and imaging a RAID 5 array with an unknown configuration fast and easy.

Autodetection of RAID 5 configuration

1. Connect the drives to the TaskForce hardware unit's ports that are switched to the Source mode.
2. On the left in the TaskForce main window, click **RAID**.



Completed

Diagnostics completed
SATA 1 Samsung SSD 860 PRO 256GB S418NF0KB07068A — a few seconds ago

Source switch of SAS 5 enabled — 3 minutes ago

Source switch of SAS 3 enabled — 3 minutes ago

Source switch of SAS 2 enabled — 3 minutes ago

Source switch of SAS 1 enabled — 3 minutes ago

Source switch of SATA 1 enabled — 3 minutes ago

Imaging completed
Win10ProX64.img — 3 days ago

Imaging started
Win10ProX64.img — 3 days ago

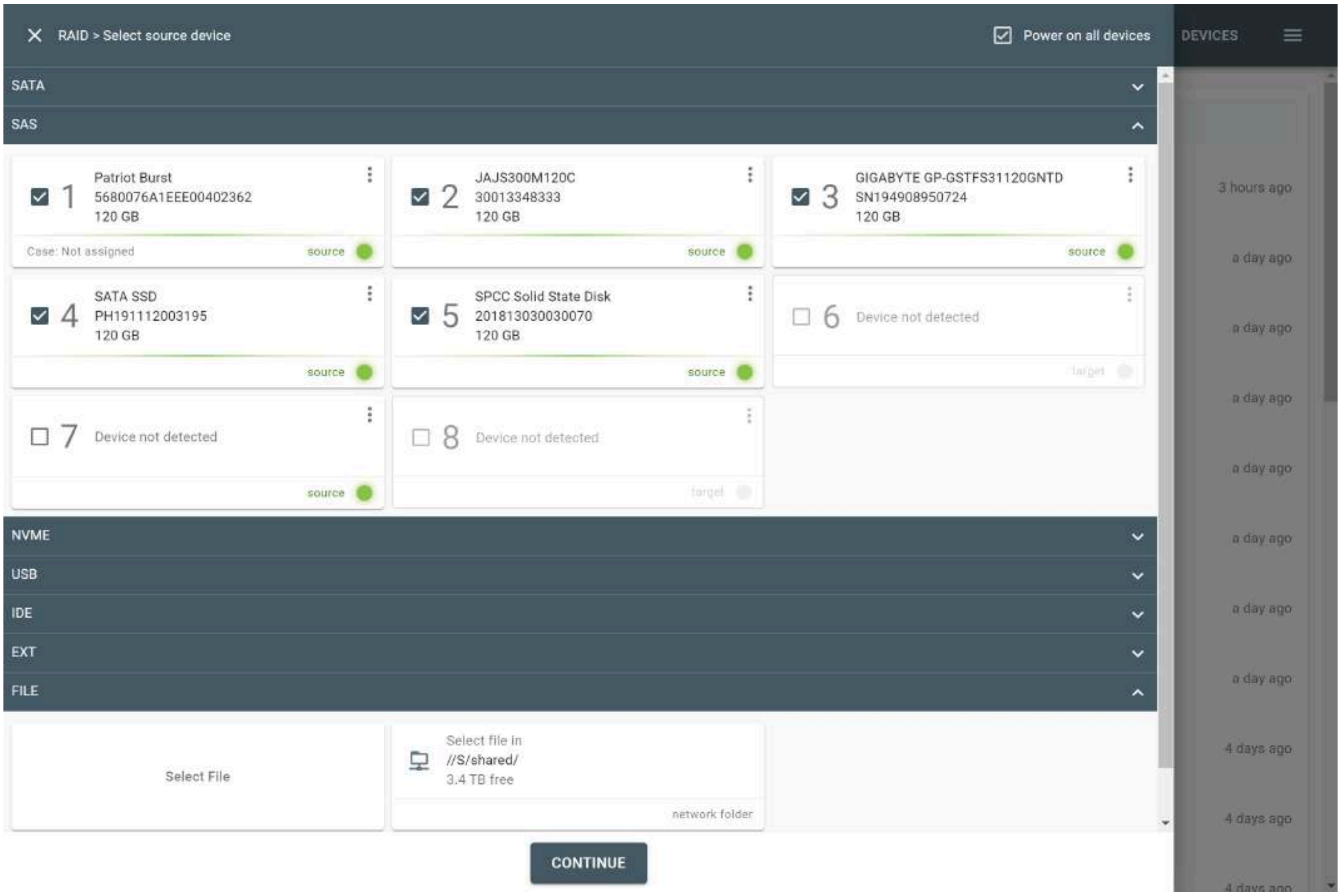
Diagnostics completed
963 — SATA 2 Samsung SSD 870 EVO 500GB S6PXNZ0R607674Z — 3 days ago

Case details changed — 4 days ago

Diagnostics completed — 4 days ago

Initiating work with RAID.

3. On the **Select source device** panel, select the drives that make up a RAID array and click **Continue**.



Selecting the drives that make up a RAID.

To assemble a RAID from images instead of drives or to use a combination of drives and images, on the **Select source device** panel, expand the **File** section and click **Select file**. Then browse and select images.

After you selected the drives that make up a RAID array, TaskForce 2 redirects you to the RAID configuration screen. It consists of three parts:

- The selected devices (and/or image files) are shown in the top **RAID configuration** part.
- The **RAID Partitions** viewer below it provides a preview of partitions and files within them, once RAID has been successfully assembled.
- The **Autodetection** module in the right-hand part of the screen immediately starts running and produces an output of RAID configuration suggestions.

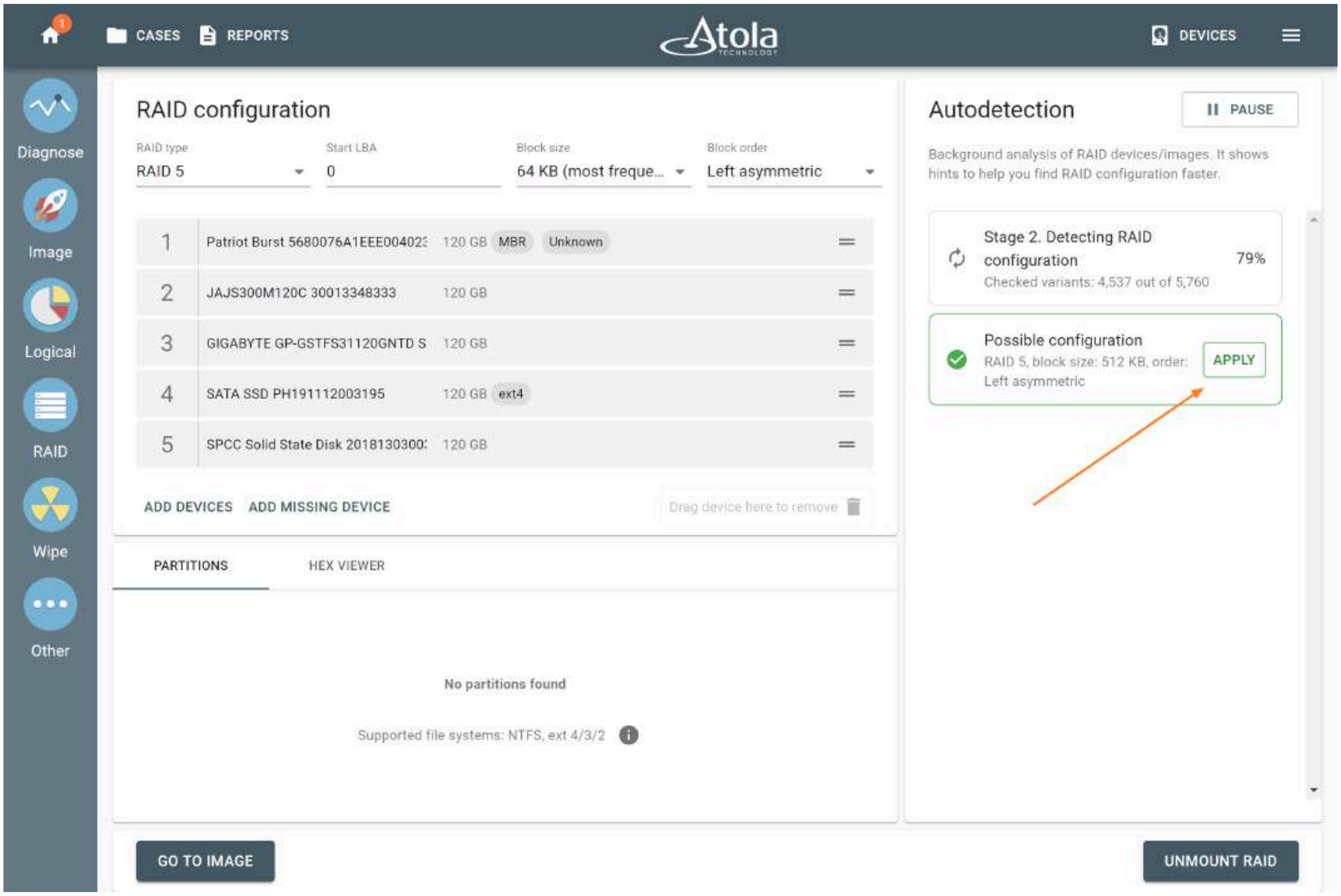
Autodetection module reads data from all the selected devices and/or images to detect these RAID parameters:

- Order of drives/images.
- RAID type.
- Start LBA.
- Block size.
- Block order.

Should the configuration be known, these parameters can also be set manually by the operator.

The time required for configuration detection can vary from a few seconds to a few hours depending on the numbers of drives involved, RAID volume and type, and how metadata is distributed on the drives in the RAID. In certain cases, Autodetection may produce several configuration suggestions, which can be applied one by one to find the exact match. TaskForce's Autodetection is based on heuristics algorithms that help speed up the variant check.

4. Click the **Apply** button to apply the configuration suggested by the Autodetection module.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left asymmetric

1	Patriot Burst 5680076A1EEE00402	120 GB	MBR	Unknown
2	JAJS300M120C 30013348333	120 GB		
3	GIGABYTE GP-GSTFS31120GNTD S	120 GB		
4	SATA SSD PH191112003195	120 GB	ext4	
5	SPCC Solid State Disk 201813030	120 GB		

No partitions found

Supported file systems: NTFS, ext 4/3/2

Autodetection

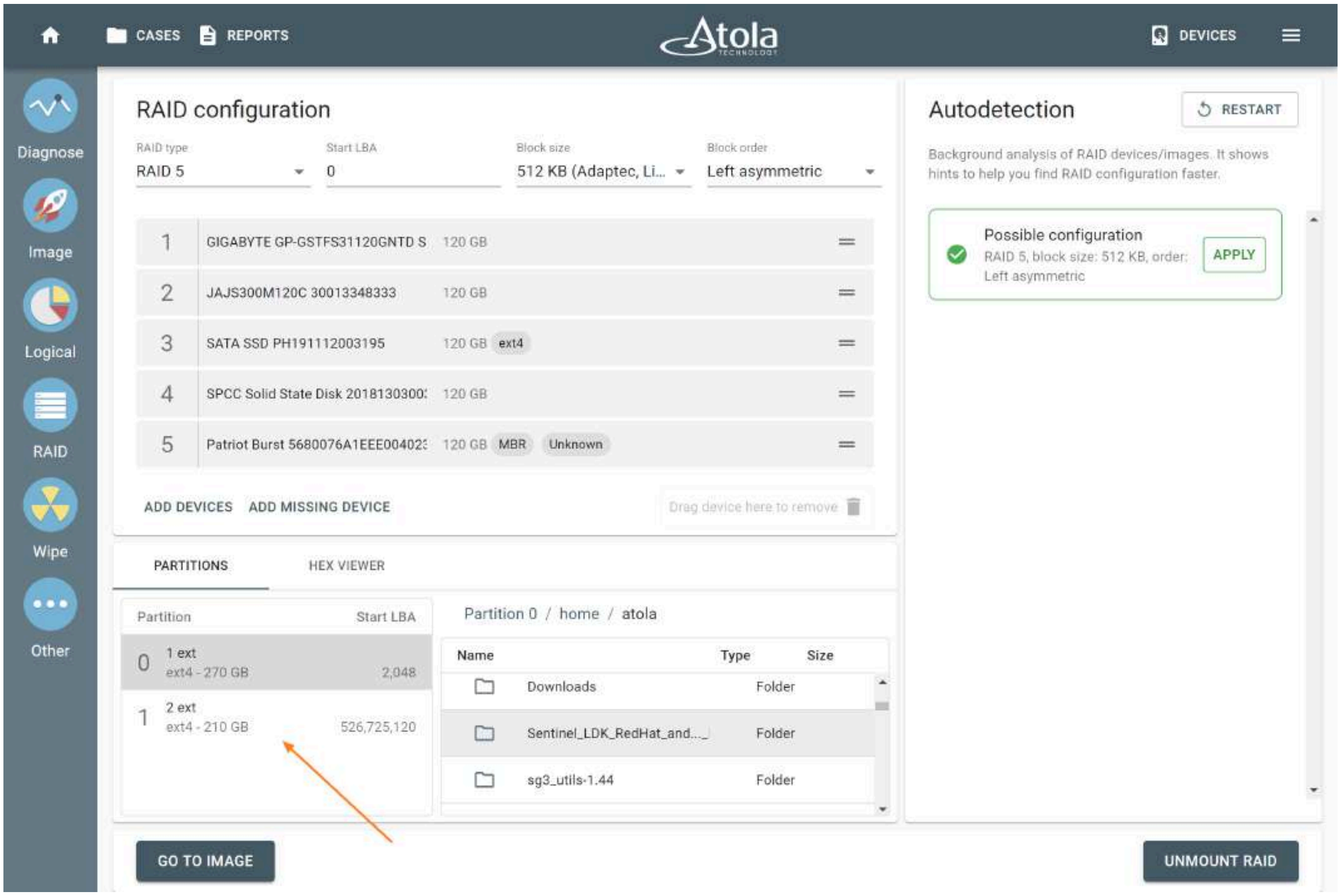
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster.

Stage 2. Detecting RAID configuration 79%
Checked variants: 4,537 out of 5,760

Possible configuration
RAID 5, block size: 512 KB, order: Left asymmetric

Autodetection module searching for possible RAID configurations.

If the suggested configuration matches the RAID native configuration, partitions of the RAID will be displayed and a preview of data within the partition will be enabled.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 512 KB (Adaptec, Li...
Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD S	120 GB	
2	JAJS300M120C 30013348333	120 GB	
3	SATA SSD PH191112003195	120 GB	ext4
4	SPCC Solid State Disk 201813030O:	120 GB	
5	Patriot Burst 5680076A1EEE00402:	120 GB	MBR Unknown

	Partition	Start LBA
0	1 ext ext4 - 270 GB	2,048
1	2 ext ext4 - 210 GB	526,725,120

Partition 0 / home / atola

Name	Type	Size
Downloads	Folder	
Sentinel_LDK_RedHat_and..._	Folder	
sg3_utils-1.44	Folder	

Autodetection

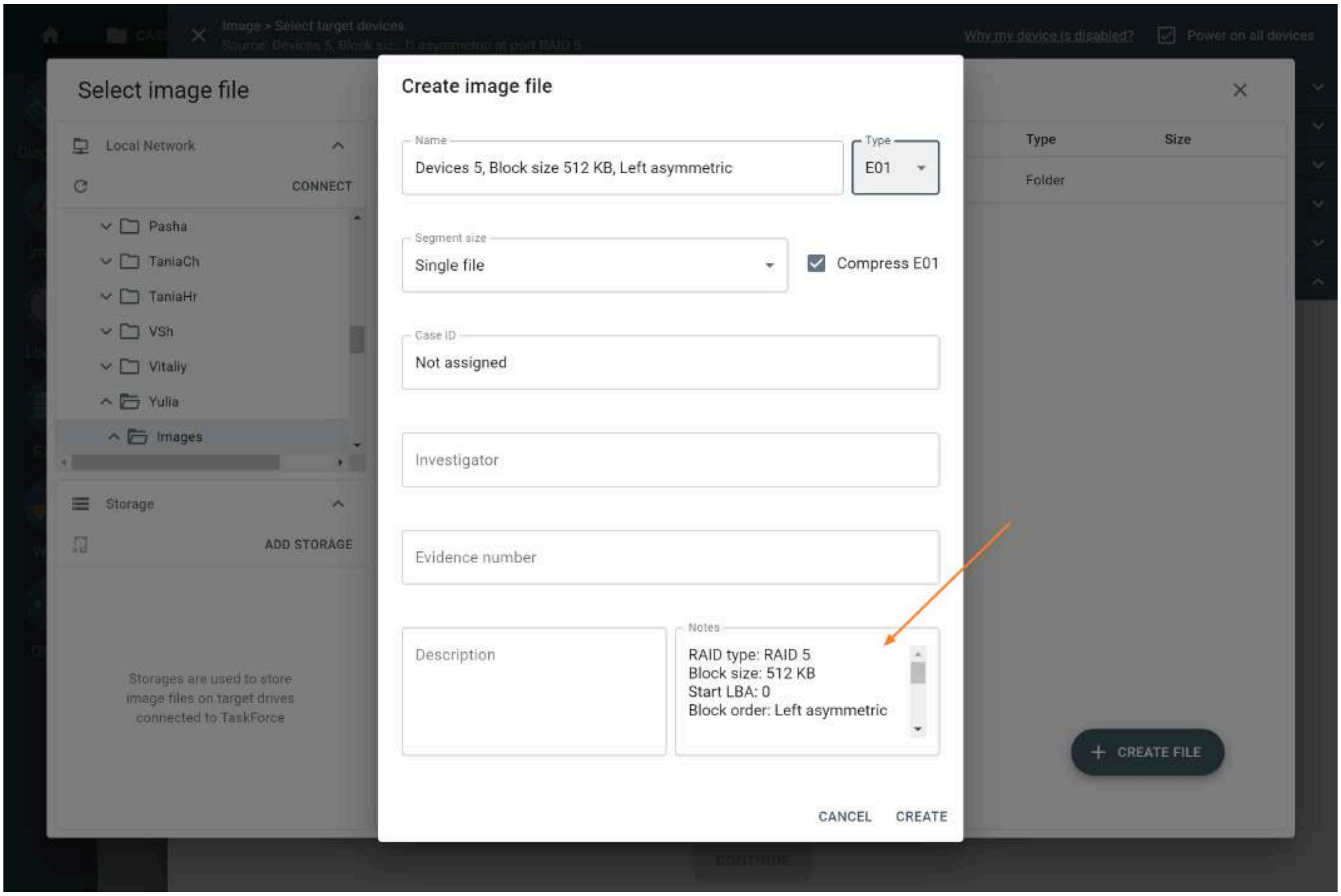
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster.

Possible configuration
RAID 5, block size: 512 KB, order: Left asymmetric

Detected RAID 5 configuration applied

Imaging selected partitions of RAID 5

1. To adjust the imaging settings and define the target for the image, in the left bottom corner of the screen, click **Go to image**.
2. Select the target for the imaging session. Both a local server and a target device in Storage mode can be used for imaging of a RAID array.
3. Click **Create file**.
4. In the **Create image file** dialog, fill out the image details and click **Create**.



Create image file

Name: Devices 5, Block size 512 KB, Left asymmetric

Type: E01

Segment size: Single file

☑ Compress E01

Case ID: Not assigned

Investigator

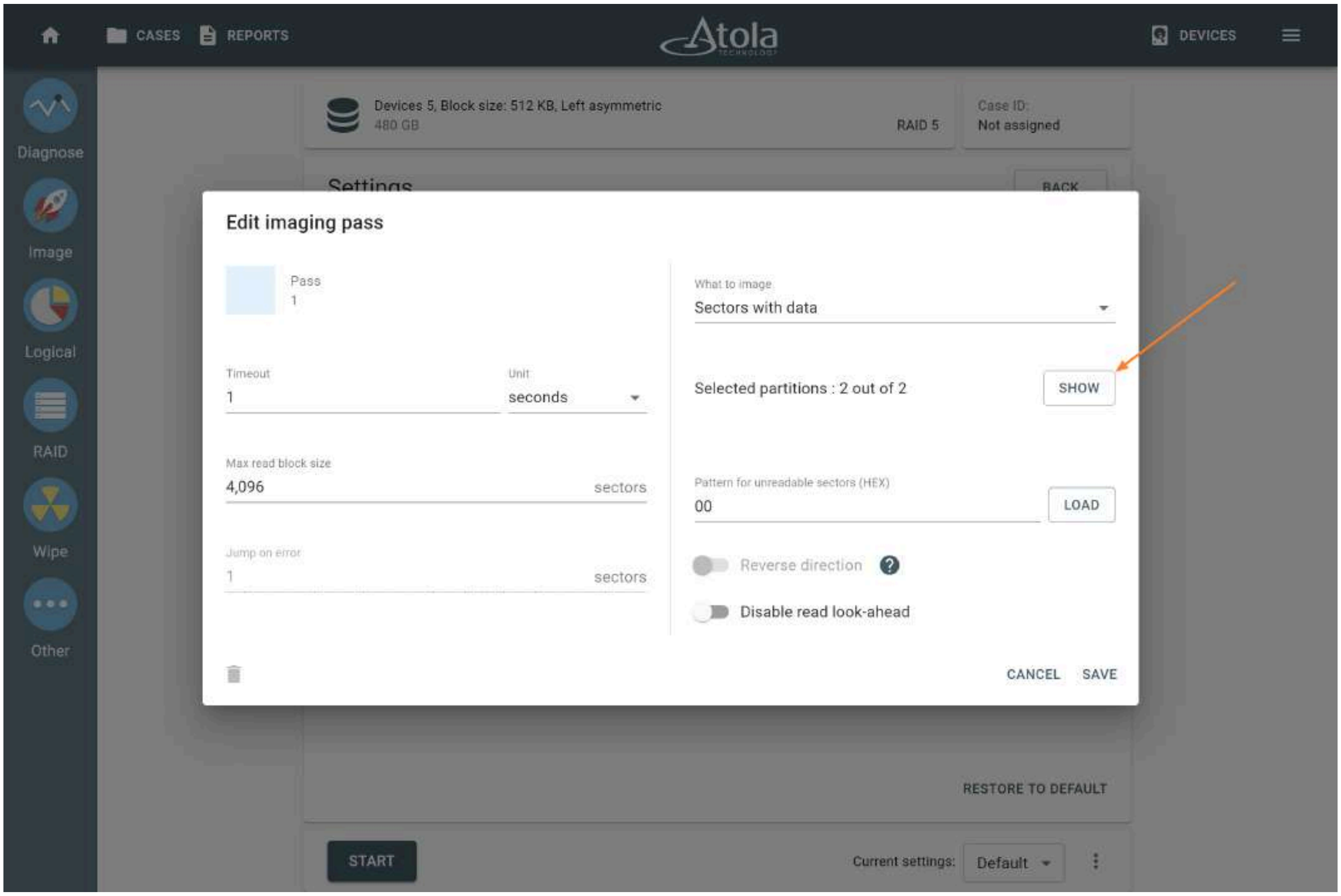
Evidence number

Description

Notes:
RAID type: RAID 5
Block size: 512 KB
Start LBA: 0
Block order: Left asymmetric

Imaging RAID. E01 details.

5. On the **Settings** page, click **Change** and then click the settings of an imaging pass.



Devices 5, Block size: 512 KB, Left asymmetric
480 GB
RAID 5

Case ID:
Not assigned

Edit imaging pass

Pass
1

Timeout: 1
Unit: seconds

Max read block size: 4,096 sectors

Jump on error: 1 sectors

What to image: Sectors with data

Selected partitions : 2 out of 2

Pattern for unreadable sectors (HEX): 00

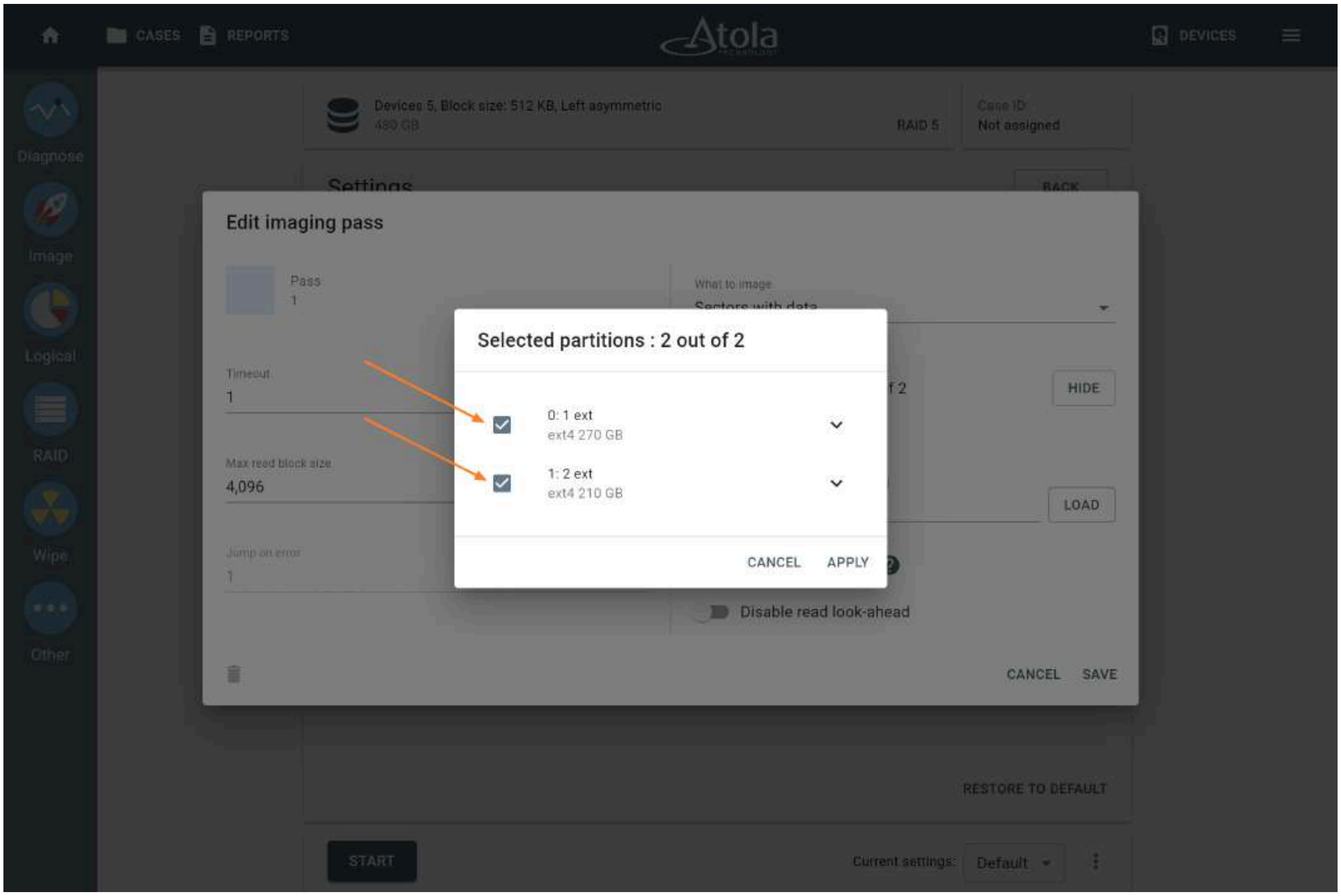
Reverse direction

Disable read look-ahead

Current settings: Default

Imaging settings.

6. In **Edit imaging pass** dialog, select the individual partitions to be imaged if selective imaging is required and click **Save**.



Devices 5, Block size: 512 KB, Left asymmetric
480 GB
RAID 5

Case ID: Not assigned

Edit imaging pass

Pass: 1

Timeout: 1

Max read block size: 4,096

Jump on error: 1

What to image: Sectors with data

Selected partitions : 2 out of 2

☑ 0: 1 ext
ext4 270 GB

☑ 1: 2 ext
ext4 210 GB

CANCEL APPLY

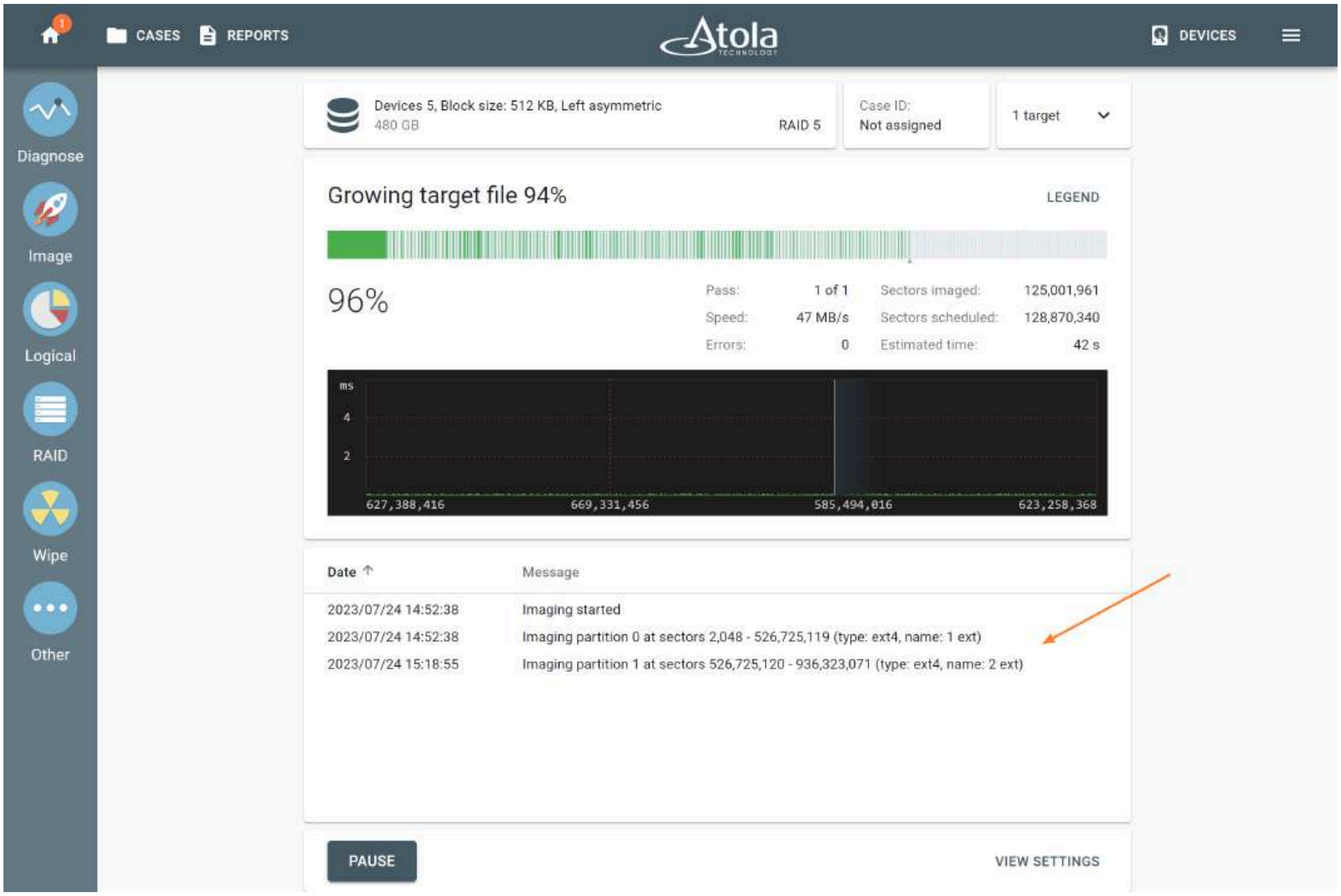
Disable read look-ahead

Current settings: Default

Selecting partitions in imaging settings

7. To launch the imaging session, click **Start**.

TaskForce 2 will be imaging RAID 5 array or its partitions as configured in the imaging settings.



Devices 5, Block size: 512 KB, Left asymmetric
480 GB
RAID 5

Case ID:
Not assigned

1 target

Growing target file 94%

96%

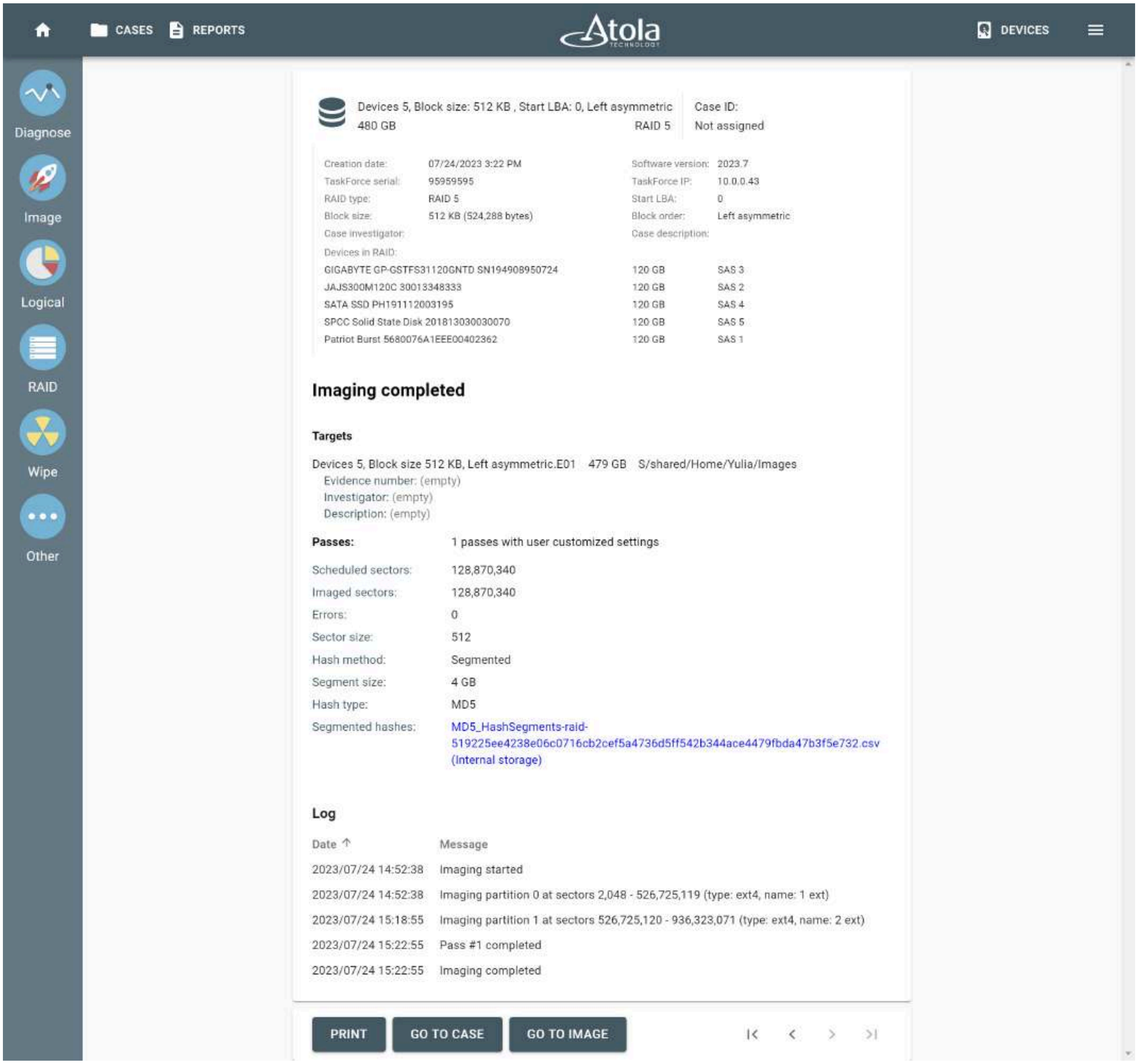
Pass: 1 of 1
Speed: 47 MB/s
Errors: 0

Sectors imaged: 125,001,961
Sectors scheduled: 128,870,340
Estimated time: 42 s

Date ↑	Message
2023/07/24 14:52:38	Imaging started
2023/07/24 14:52:38	Imaging partition 0 at sectors 2,048 - 526,725,119 (type: ext4, name: 1 ext)
2023/07/24 15:18:55	Imaging partition 1 at sectors 526,725,120 - 936,323,071 (type: ext4, name: 2 ext)

Imaging RAID 5 in progress

At the end of the imaging session, TaskForce 2 produces an **Imaging completed** report with all the details of the source drives, the RAID configuration, the target, the partition, the timestamps, etc.



Devices 5, Block size: 512 KB , Start LBA: 0, Left asymmetric
480 GB RAID 5

Case ID:
Not assigned

Creation date:	07/24/2023 3:22 PM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.43
RAID type:	RAID 5	Start LBA:	0
Block size:	512 KB (524,288 bytes)	Block order:	Left asymmetric
Case investigator:		Case description:	

Devices in RAID:

GIGABYTE GP-GSTFS31120GNTD SN194908950724	120 GB	SAS 3
JAJS300M120C 30013348333	120 GB	SAS 2
SATA SSD PH191112003195	120 GB	SAS 4
SPCC Solid State Disk 201813030030070	120 GB	SAS 5
Patriot Burst 5680076A1EEE00402362	120 GB	SAS 1

Imaging completed

Targets

Devices 5, Block size 512 KB, Left asymmetric.E01 479 GB S/shared/Home/Yulia/Images
Evidence number: (empty)
Investigator: (empty)
Description: (empty)

Passes:	1 passes with user customized settings
Scheduled sectors:	128,870,340
Imaged sectors:	128,870,340
Errors:	0
Sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-raid-519225ee4238e06c0716cb2cef5a4736d5ff542b344ace4479fbda47b3f5e732.csv (Internal storage)

Log

Date ↑	Message
2023/07/24 14:52:38	Imaging started
2023/07/24 14:52:38	Imaging partition 0 at sectors 2,048 - 526,725,119 (type: ext4, name: 1 ext)
2023/07/24 15:18:55	Imaging partition 1 at sectors 526,725,120 - 936,323,071 (type: ext4, name: 2 ext)
2023/07/24 15:22:55	Pass #1 completed
2023/07/24 15:22:55	Imaging completed

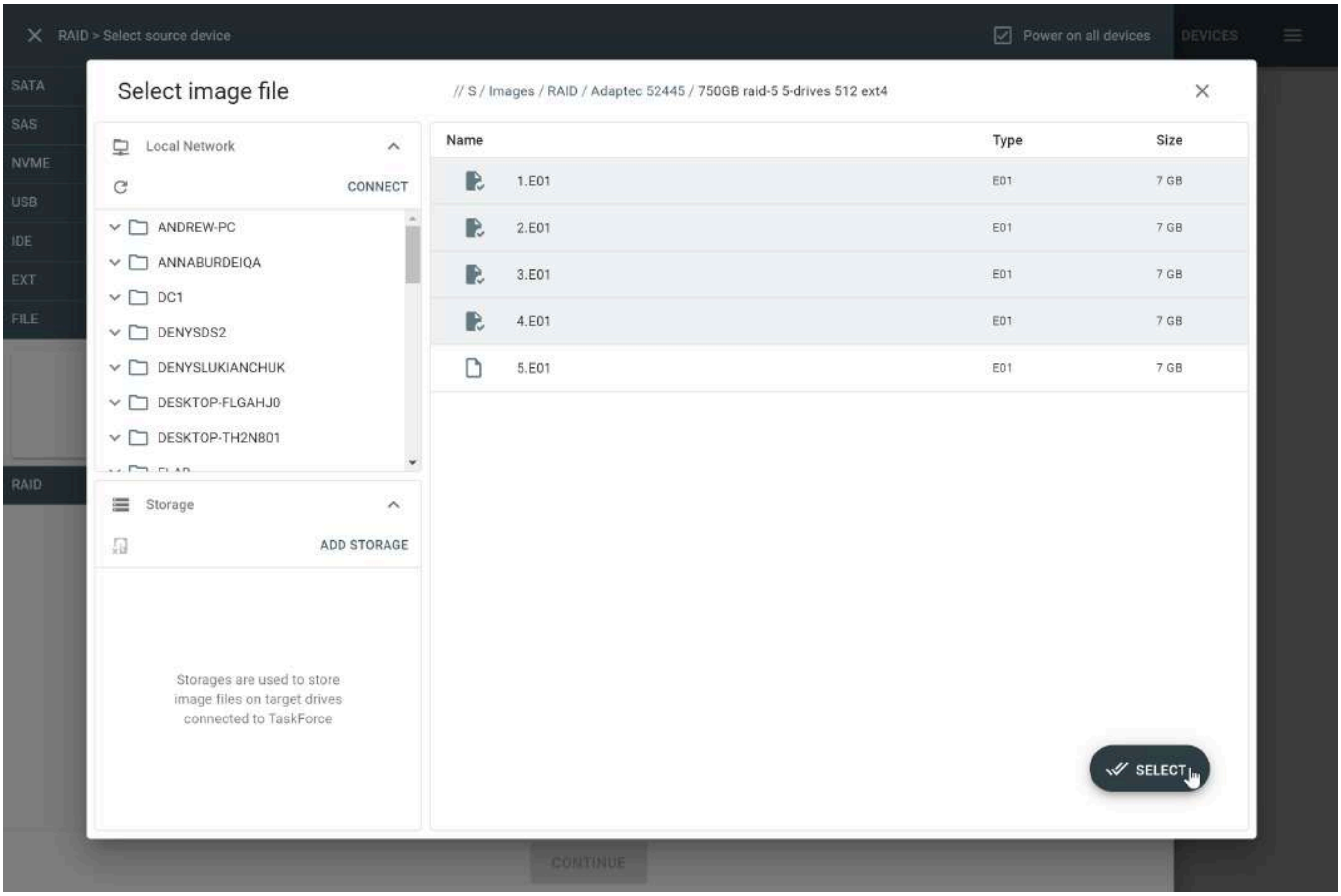
RAID 5 forensics. Imaging report

Reassembling RAID 5 with a missing drive from image files

Imagine you have image files that are created from source RAID 5 drives. If one of RAID 5 drives was missing or heavily damaged, one image file is missing or incomplete, too. TaskForce 2 uses RAID 5 redundancy to create a full image of the RAID even in such cases.

To reassemble a RAID from image files:

1. On the left in the TaskForce main window, click **RAID**.
2. On the **Select source device** panel, expand the **File** section and click **Select file**.
3. In the **Select image file** window, find the directory with the images you want to use and select the files. Then click **Select**.

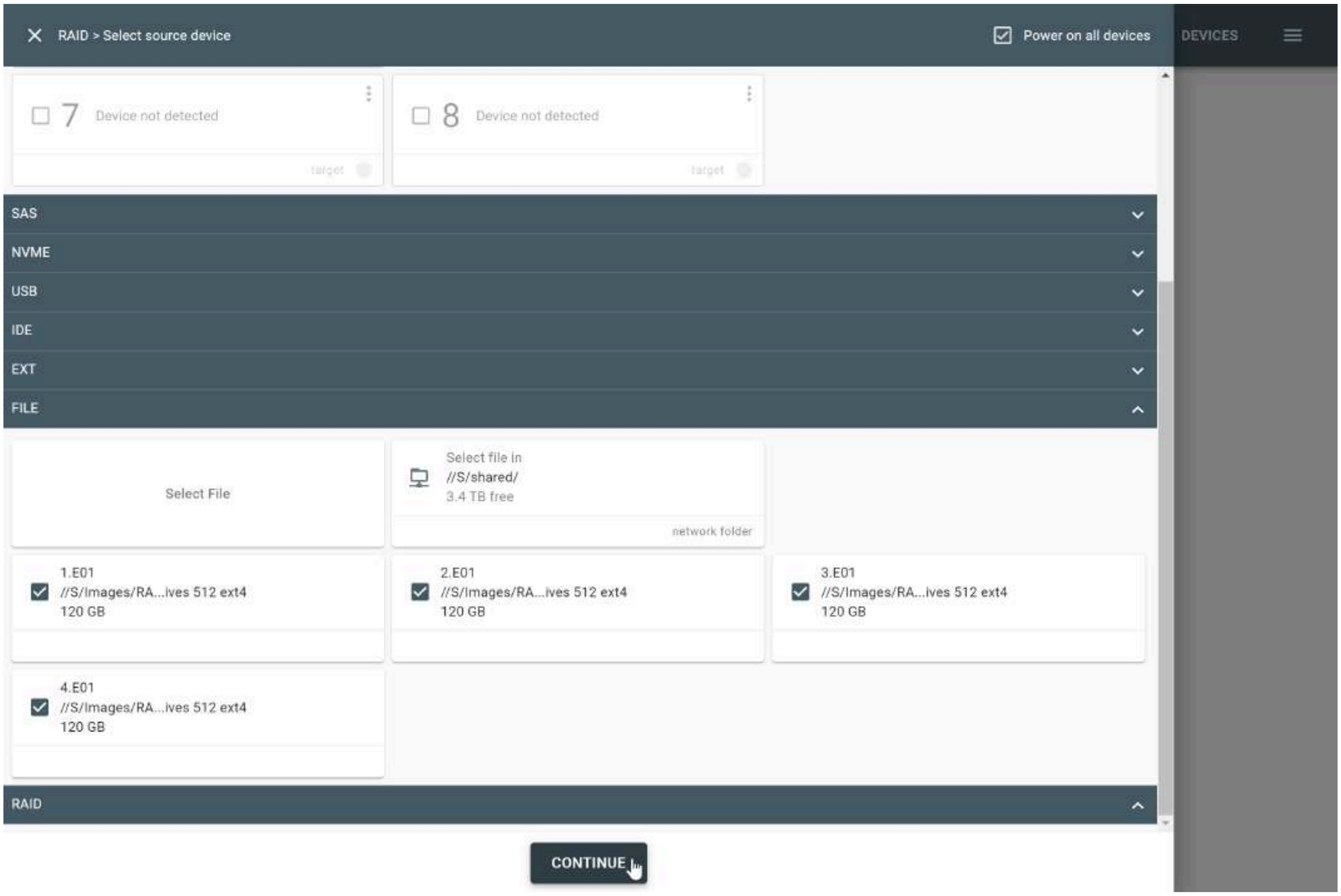


// S / Images / RAID / Adaptec 52445 / 750GB raid-5 5-drives 512 ext4

Name	Type	Size
1.E01	E01	7 GB
2.E01	E01	7 GB
3.E01	E01	7 GB
4.E01	E01	7 GB
5.E01	E01	7 GB

Selecting RAID 5 image files.

5. On the **Select source device** panel, check source image files and then click **Continue**.



☑ 1.E01
//S/Images/RA...ives 512 ext4
120 GB

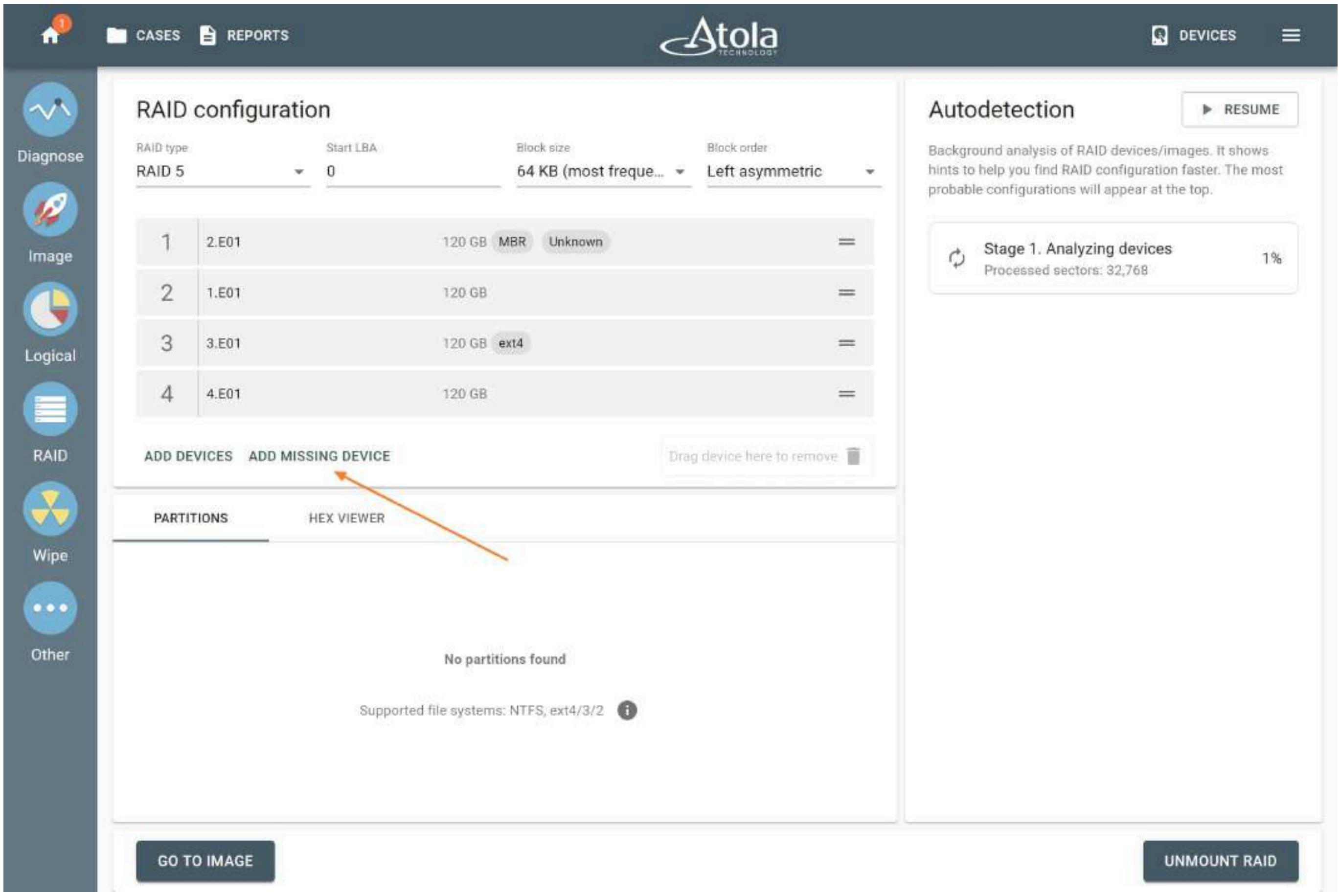
☑ 2.E01
//S/Images/RA...ives 512 ext4
120 GB

☑ 3.E01
//S/Images/RA...ives 512 ext4
120 GB

☑ 4.E01
//S/Images/RA...ives 512 ext4
120 GB

Selecting RAID 5 image files.

6. Autodetection module starts running automatically to find a suitable RAID configuration. You know that there is an image file missing from the selection (it may have been lost or damaged), so click **Add missing device** underneath the list of image files.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left asymmetric

1	2.E01	120 GB	MBR Unknown
2	1.E01	120 GB	
3	3.E01	120 GB	ext4
4	4.E01	120 GB	

Drag device here to remove

No partitions found

Supported file systems: NTFS, ext4/3/2

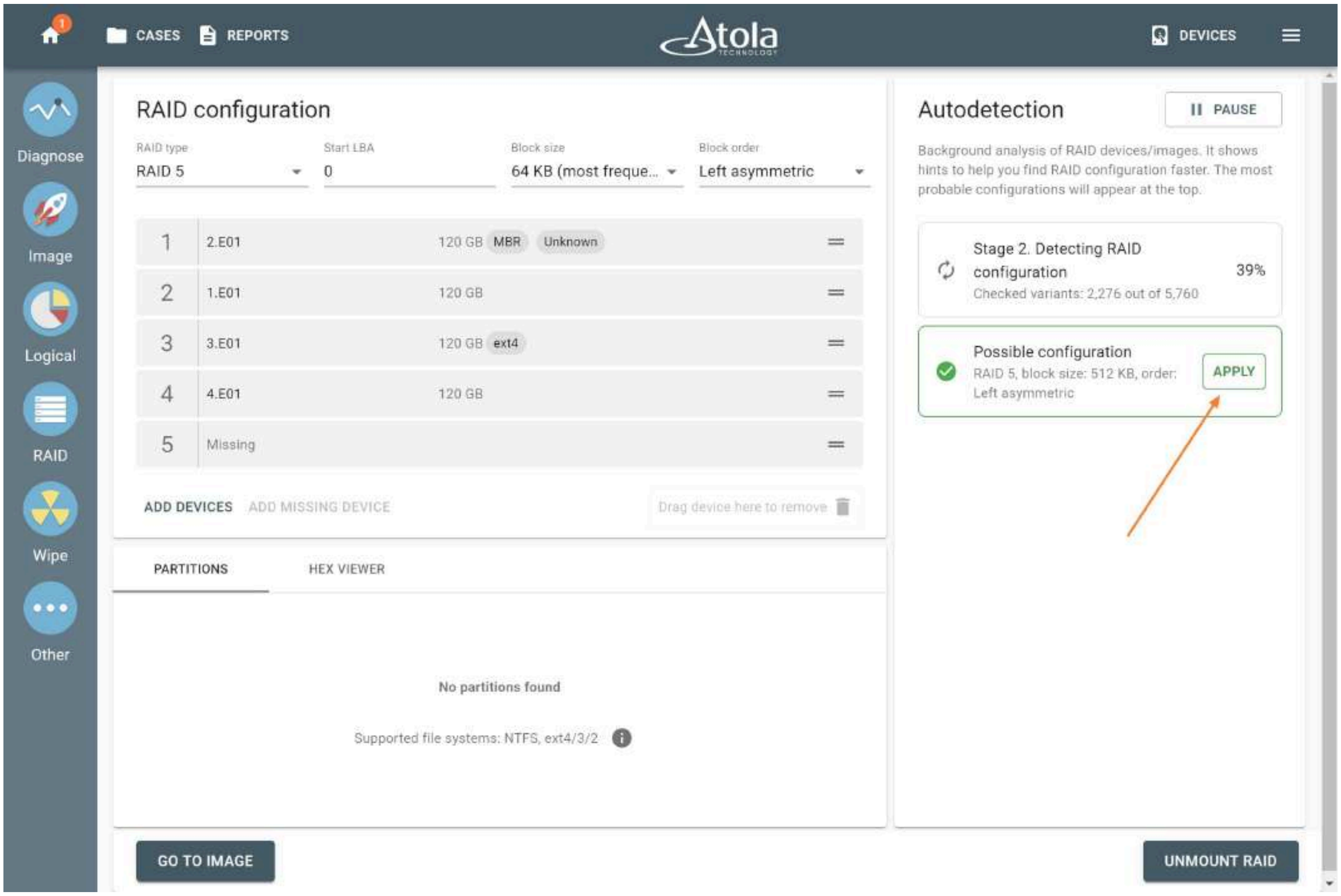
Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 1%
Processed sectors: 32,768

Adding missing RAID 5 drive.

7. Autodetection will recommence when a new image file or device is added. If the RAID is type 5, TaskForce 2 will be able to identify the right configuration and reassemble the RAID by using the redundancy. When a possible configuration is found, click **Apply**.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left asymmetric

1	2.E01	120 GB	MBR Unknown
2	1.E01	120 GB	
3	3.E01	120 GB	ext4
4	4.E01	120 GB	
5	Missing		

Drag device here to remove

No partitions found

Supported file systems: NTFS, ext4/3/2

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

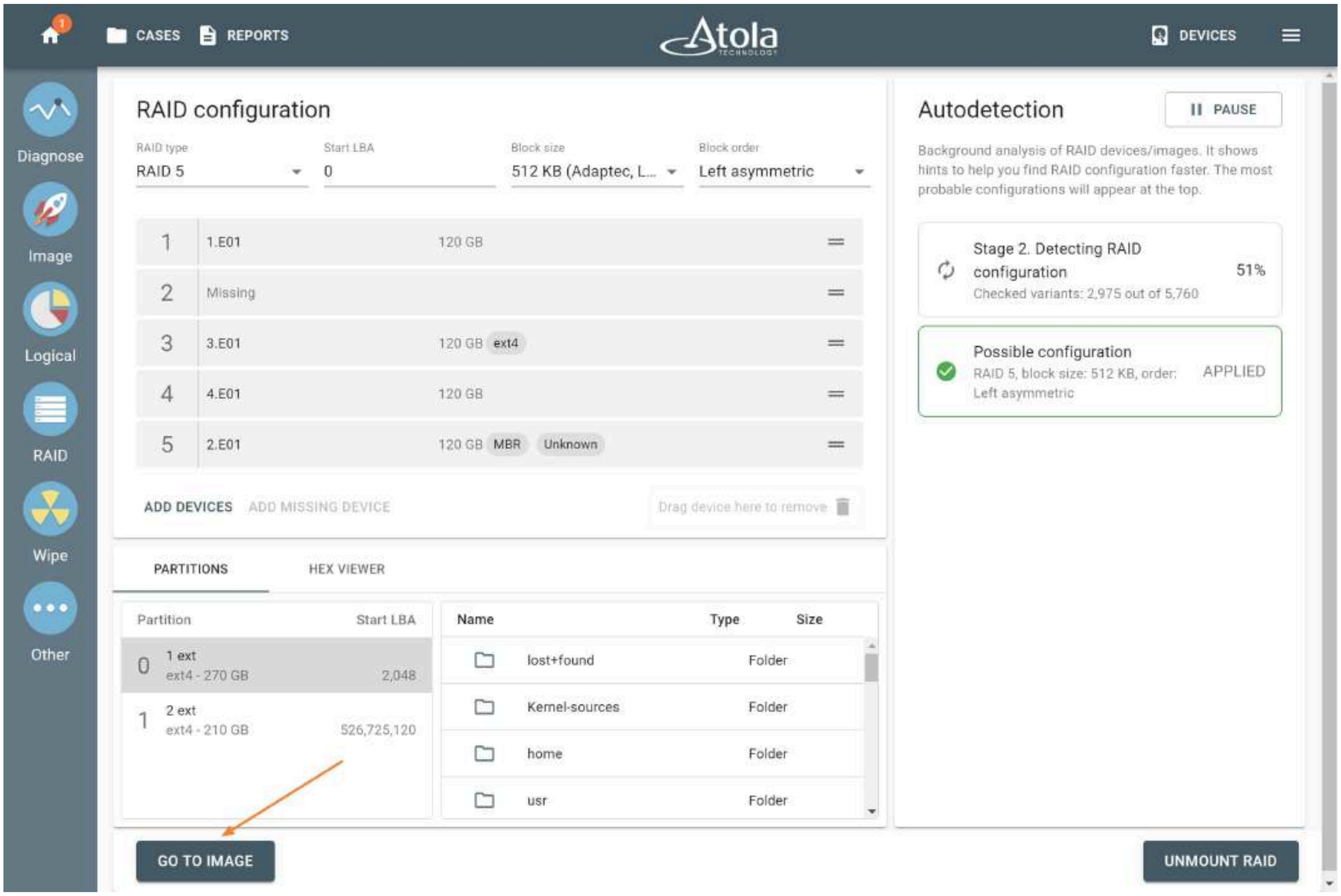
Stage 2. Detecting RAID configuration 39%
Checked variants: 2,276 out of 5,760

Possible configuration
RAID 5, block size: 512 KB, order: Left asymmetric

Applying the found RAID configuration.

The configuration application automatically changes the order of the drives/images, the detected RAID type, block size and order is applied automatically, too. In the bottom part of the screen, the found partitions are available for preview.

8. To proceed with imaging, click the **Go to image** button and follow the instruction in subsequent screens to select the target and adjust imaging settings.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 512 KB (Adaptec, L...
Block order: Left asymmetric

1	1.E01	120 GB	
2	Missing		
3	3.E01	120 GB	ext4
4	4.E01	120 GB	
5	2.E01	120 GB	MBR Unknown

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 51%
Checked variants: 2,975 out of 5,760

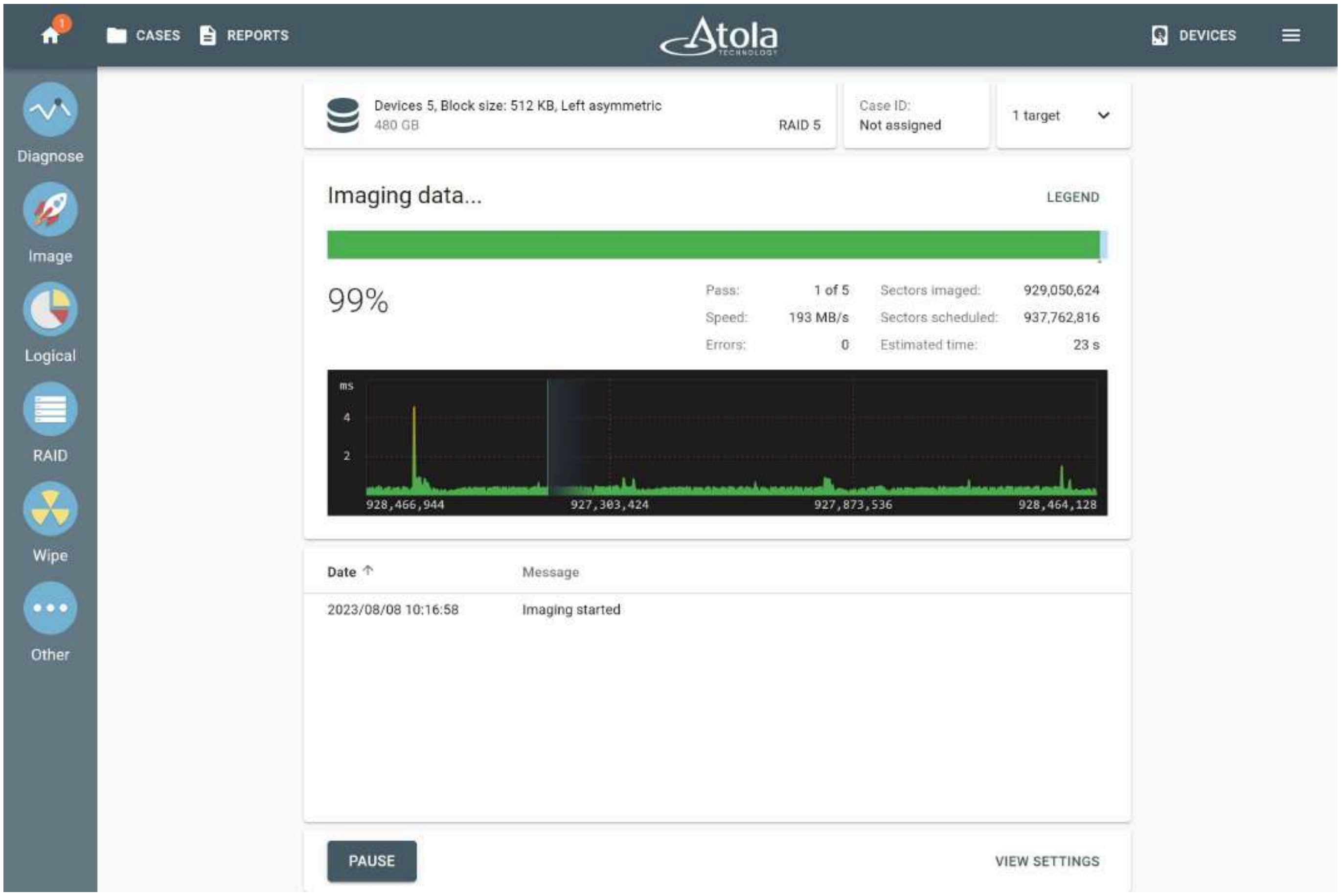
Possible configuration APPLIED
RAID 5, block size: 512 KB, order: Left asymmetric

	Partition	Start LBA
0	1 ext ext4 - 270 GB	2,048
1	2 ext ext4 - 210 GB	526,725,120

Name	Type	Size
lost+found	Folder	
Kernel-sources	Folder	
home	Folder	
usr	Folder	

Preview the found partitions and proceed to image

During the imaging, TaskForce 2 takes advantage of the redundancy to create an image of the RAID despite one of the devices is missing.



Devices 5, Block size: 512 KB, Left asymmetric
480 GB
RAID 5

Case ID:
Not assigned

1 target

Imaging data...

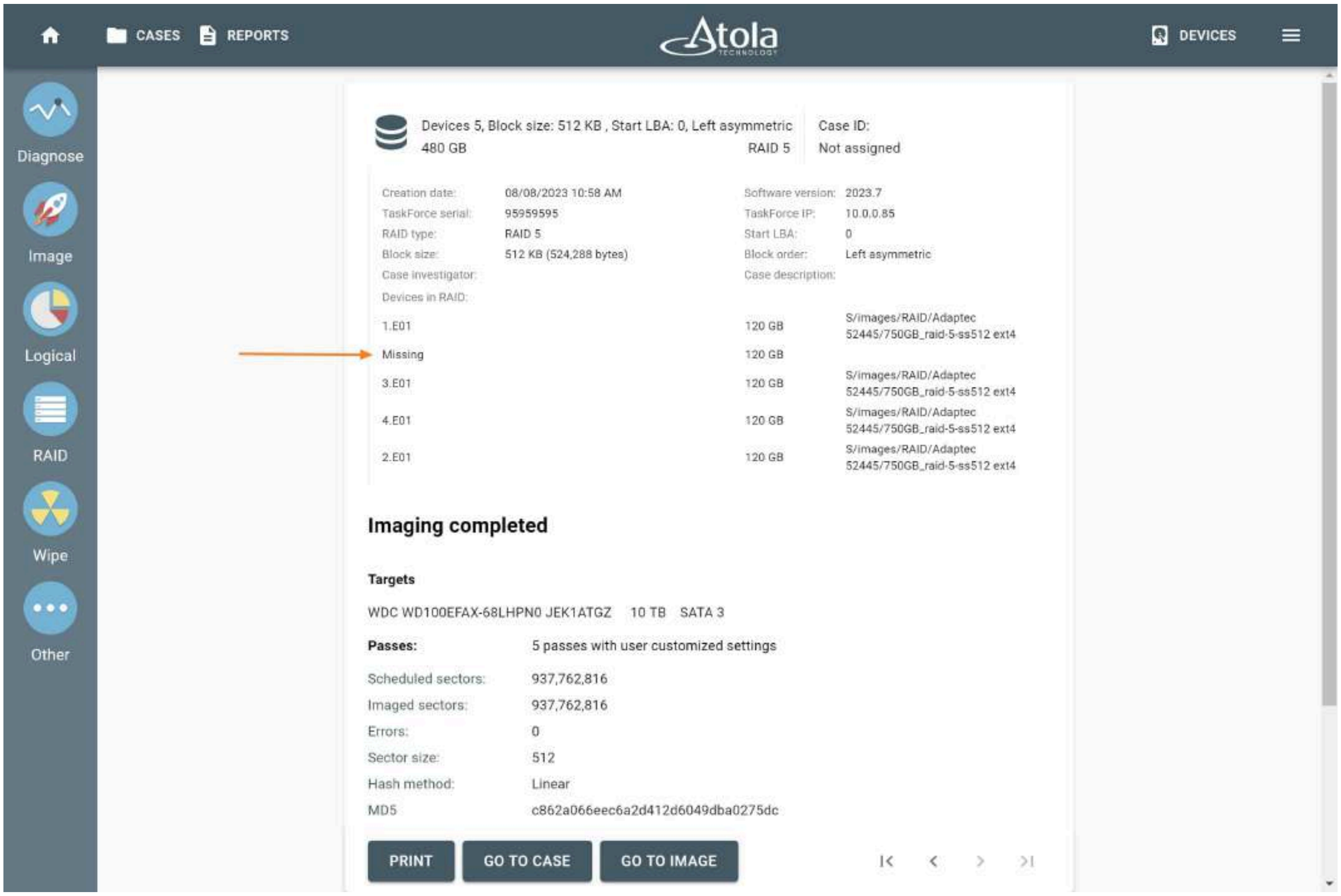
99%

Pass:	1 of 5	Sectors imaged:	929,050,624
Speed:	193 MB/s	Sectors scheduled:	937,762,816
Errors:	0	Estimated time:	23 s

Date ↑	Message
2023/08/08 10:16:58	Imaging started

Imaging RAID 5 with a missing drive.

The imaging report clearly indicates which of the devices that make up the RAID array was missing. Other RAID parameters, such as type, block size and order are also clearly reflected in the report.



Devices 5, Block size: 512 KB , Start LBA: 0, Left asymmetric
480 GB RAID 5

Case ID:
Not assigned

Creation date:	08/08/2023 10:58 AM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.85
RAID type:	RAID 5	Start LBA:	0
Block size:	512 KB (524,288 bytes)	Block order:	Left asymmetric
Case investigator:		Case description:	

Devices in RAID:

1.E01	120 GB	S/images/RAID/Adaptec 52445/750GB_raid-5-ss512 ext4
Missing	120 GB	
3.E01	120 GB	S/images/RAID/Adaptec 52445/750GB_raid-5-ss512 ext4
4.E01	120 GB	S/images/RAID/Adaptec 52445/750GB_raid-5-ss512 ext4
2.E01	120 GB	S/images/RAID/Adaptec 52445/750GB_raid-5-ss512 ext4

Imaging completed

Targets

WDC WD100EFAX-68LHPN0 JEK1ATGZ 10 TB SATA 3

Passes:	5 passes with user customized settings
Scheduled sectors:	937,762,816
Imaged sectors:	937,762,816
Errors:	0
Sector size:	512
Hash method:	Linear
MD5	c862a066eec6a2d412d6049dba0275dc

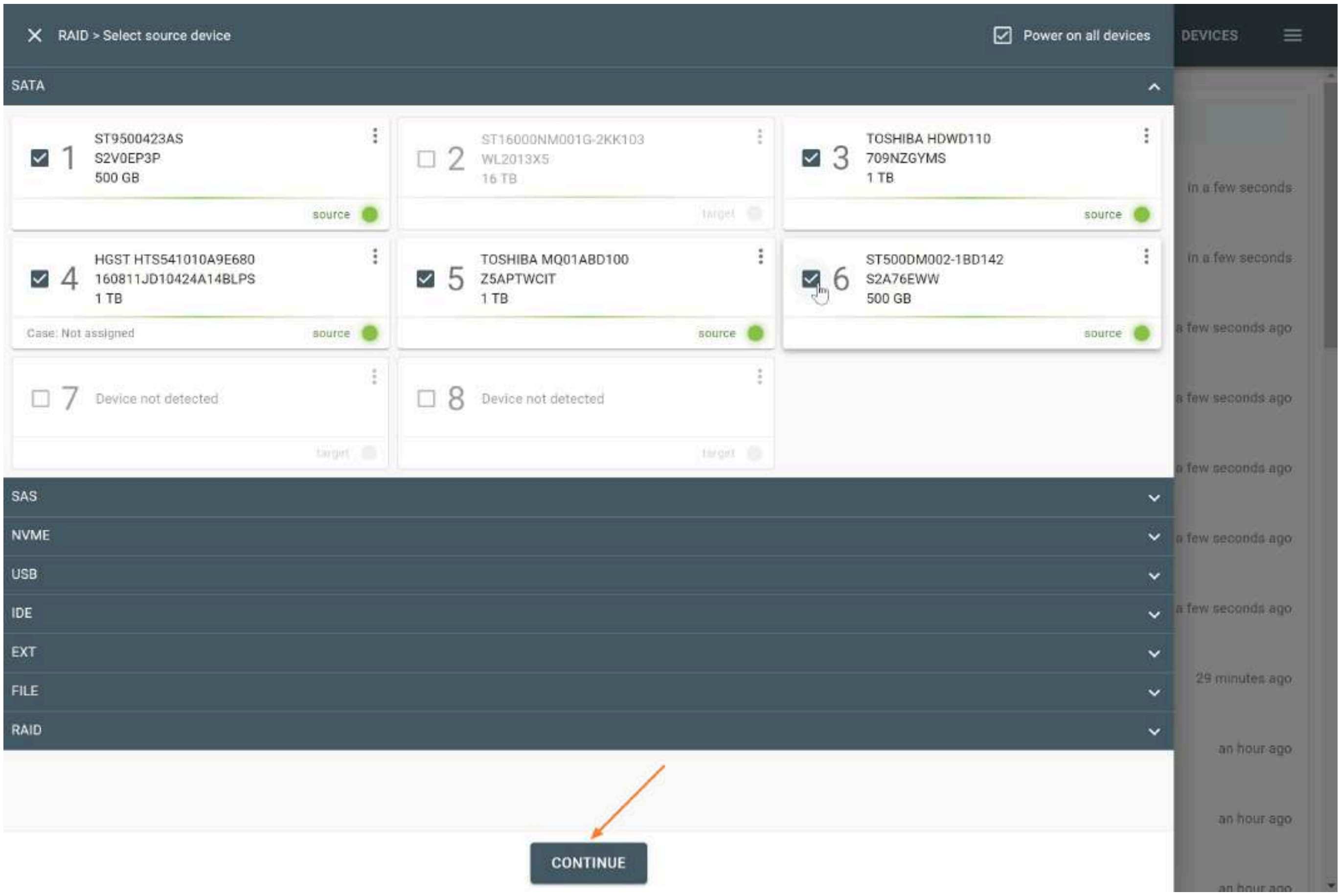
Imaging report clearly indicates the missing device in RAID 5.

Imaging RAID 5 array with 2 damaged drives

Even if a RAID 5 array contains errors, Atola TaskForce 2 is able to detect its parameters and image such RAID.

Reassemble RAID 5

1. Connect the drives to the ports of the TaskForce 2 hardware unit. Make sure the ports are in *Source mode*.
2. On the left in the TaskForce main window, click **RAID**.
3. Select the drives that make up the RAID array.
4. Click **Continue**.



☑ 1 ST9500423AS S2V0EP3P 500 GB source

□ 2 ST16000NM001G-2KK103 WL2013X5 16 TB target

☑ 3 TOSHIBA HDWD110 709NZGYMS 1 TB source

☑ 4 HGST HTS541010A9E680 160811JD10424A14BLPS 1 TB Case: Not assigned source

☑ 5 TOSHIBA MQ01ABD100 Z5APTWCIT 1 TB source

☑ 6 ST500DM002-1BD142 S2A76EWW 500 GB source

□ 7 Device not detected target

□ 8 Device not detected target

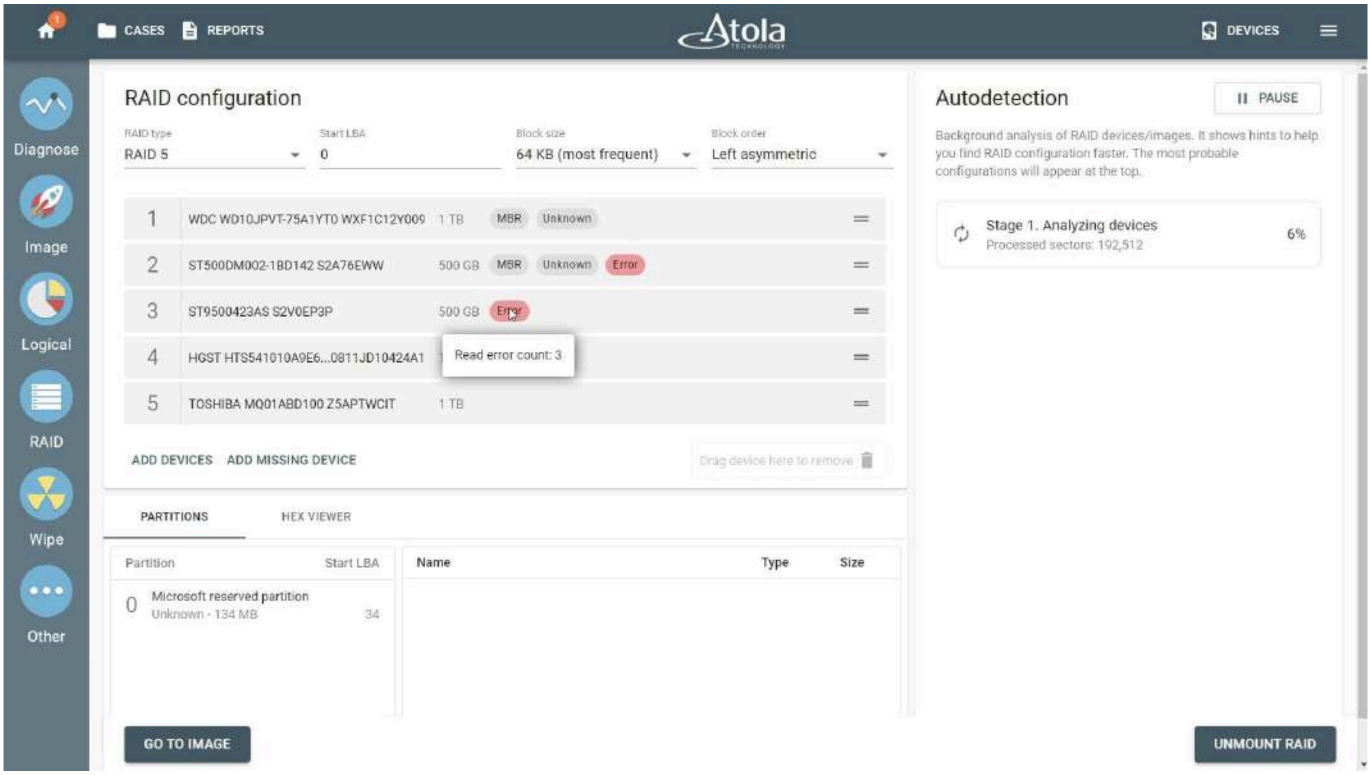
Selecting RAID members

Detecting errors

The TaskForce 2 autodetection module starts running immediately, after you select the RAID devices.

Stage 1: TaskForce 2 reads data on the drives to identify RAID type. If it runs across an error, TaskForce 2 displays error tags next to the respective RAID member.

To see the number of errors encountered on a RAID member, simply hover the cursor over the error tag.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most frequent)
Block order: Left asymmetric

1	WDC WD10JPVT-75A1YT0 WXF1C12Y009	1 TB	MBR Unknown
2	ST500DM002-1BD142 S2A76EWW	500 GB	MBR Unknown Error
3	ST9500423AS S2V0EP3P	500 GB	Error
4	HGST HTS541010A9E6...0811JD10424A1	1 TB	
5	TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB	

Read error count: 3

Partition	Start LBA
0 Microsoft reserved partition Unknown - 134 MB	34

Name	Type	Size

Autodetection

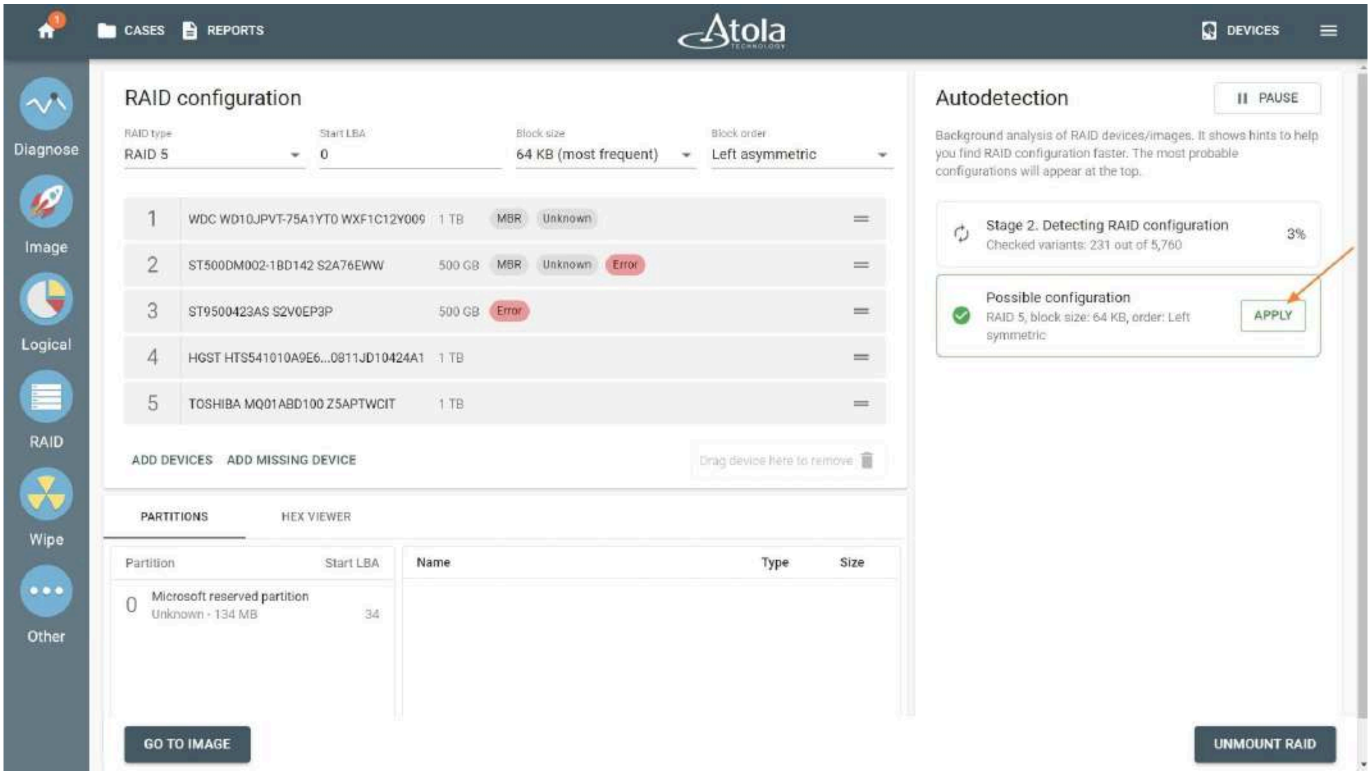
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 6%
Processed sectors: 192,512

Error tags

Stage 2: TaskForce 2 goes through thousands of possible RAID configurations to identify a suitable one.

Once the configuration is detected, click the **Apply** button.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most frequent)
Block order: Left asymmetric

1	WDC WD10JPVT-75A1YT0 WXF1C12Y009	1 TB	MBR Unknown
2	ST500DM002-1BD142 S2A76EWW	500 GB	MBR Unknown Error
3	ST9500423AS S2V0EP3P	500 GB	Error
4	HGST HTS541010A9E6...0811JD10424A1	1 TB	
5	TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB	

Partition	Start LBA
0 Microsoft reserved partition Unknown - 134 MB	34

Name	Type	Size

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 3%
Checked variants: 231 out of 5,760

Possible configuration
RAID 5, block size: 64 KB, order: Left symmetric

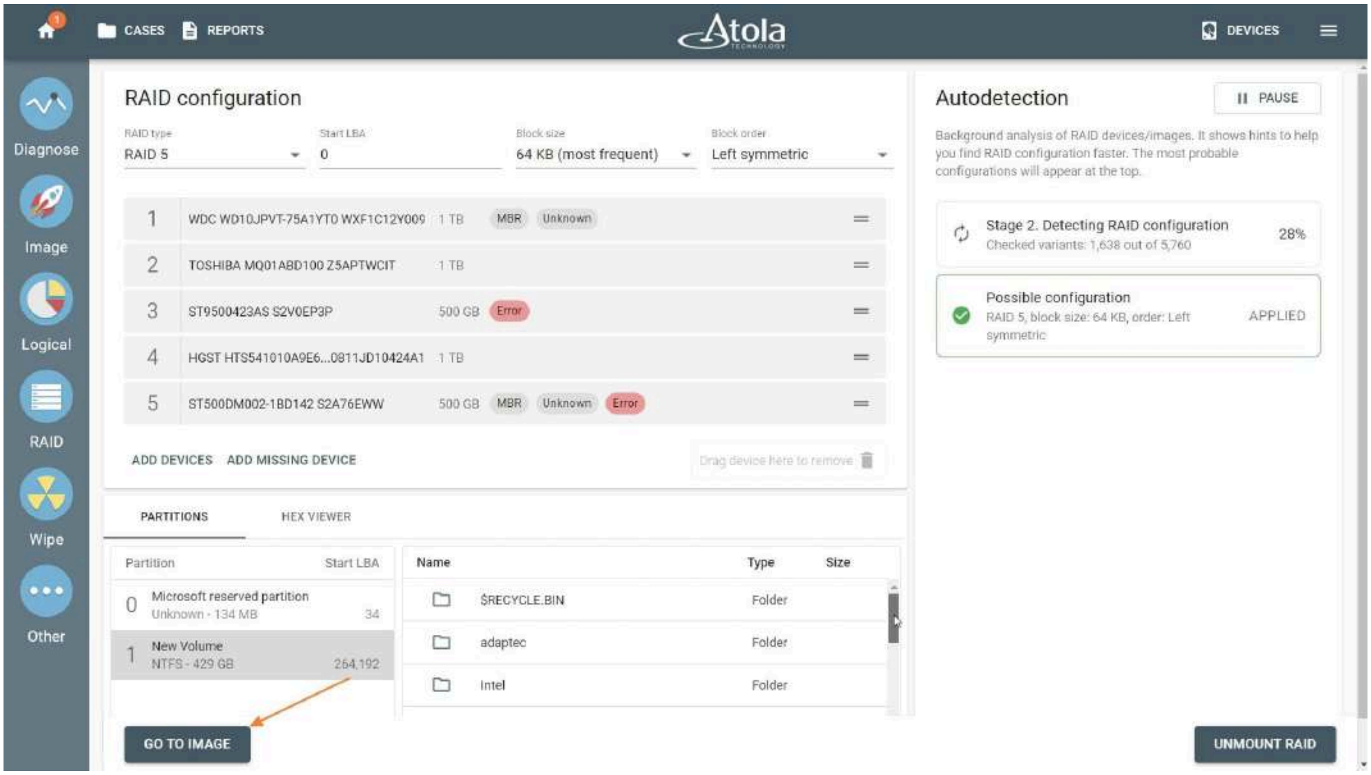
Applying the suggested RAID configuration

After you click **Apply**, TaskForce 2 automatically applies the suggested configuration and checks the file system for partitions.

Despite read errors, TaskForce 2 can mount the partitions for preview by rebuilding the data in the bad sectors using data redundancy inherent to this RAID type.

Imaging RAID 5 array with errors

1. After RAID configuration is successfully applied, click the **Go to image** button to proceed with imaging.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most frequent)
Block order: Left symmetric

1	WDC WD10JPVT-75A1YT0 WXF1C12Y009	1 TB	MBR	Unknown	
2	TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB			
3	ST9500423AS S2V0EP3P	500 GB	Error		
4	HGST HTS541010A9E6...0811JD10424A1	1 TB			
5	ST500DM002-1BD142 S2A76EWW	500 GB	MBR	Unknown	Error

Partition		Start LBA
0	Microsoft reserved partition Unknown - 134 MB	34
1	New Volume NTFS - 429 GB	264,192

Name	Type	Size
$RECYCLE.BIN	Folder	
adaptec	Folder	
Intel	Folder	

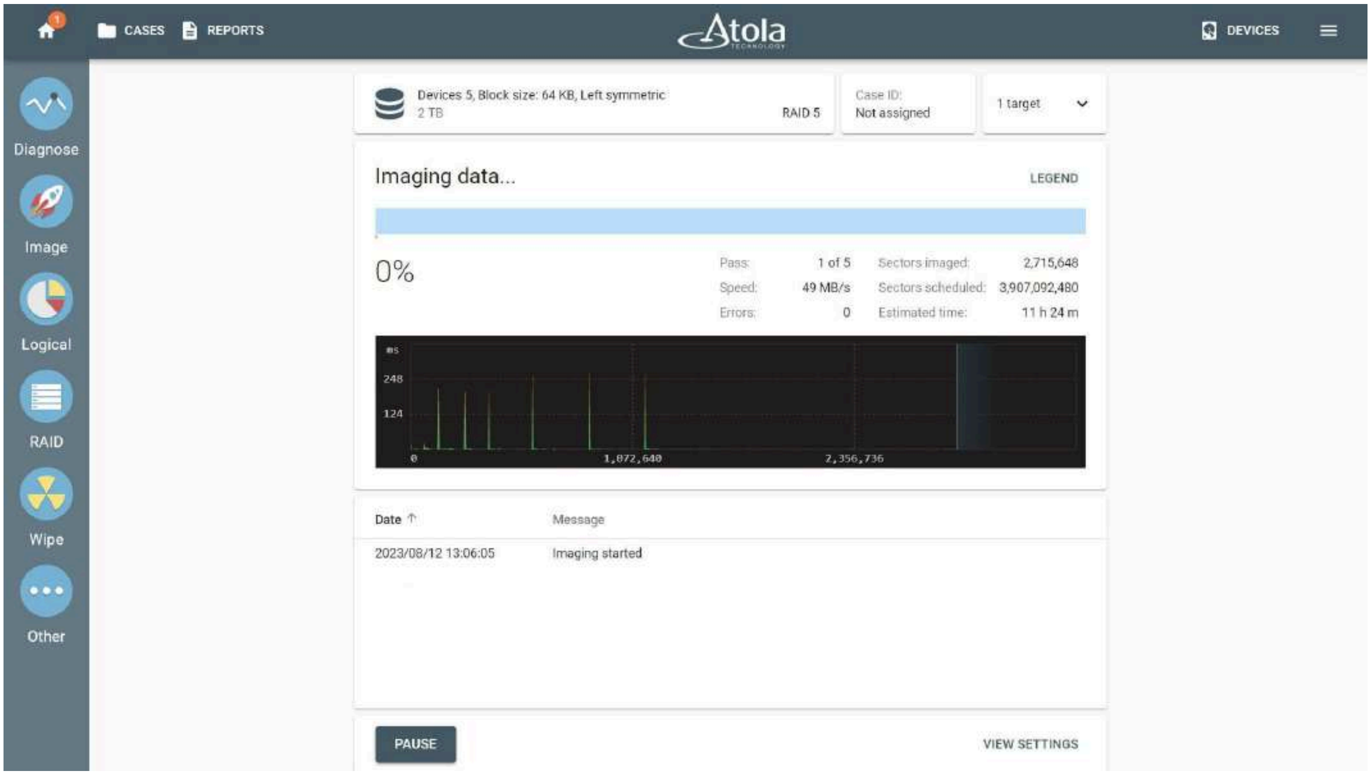
Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 28%
Checked variants: 1,638 out of 5,760

Possible configuration APPLIED
RAID 5, block size: 64 KB, order: Left symmetric

2. Select your target device or folder and click **Continue**.
3. To launch your imaging session, click **Start**.
4. When the TaskForce system encounters an error, it automatically reconstructs the missing data, using the data in the parity blocks on the remaining RAID members.



Devices 5, Block size: 64 KB, Left symmetric
2 TB
RAID 5

Case ID:
Not assigned

1 target

Imaging data...

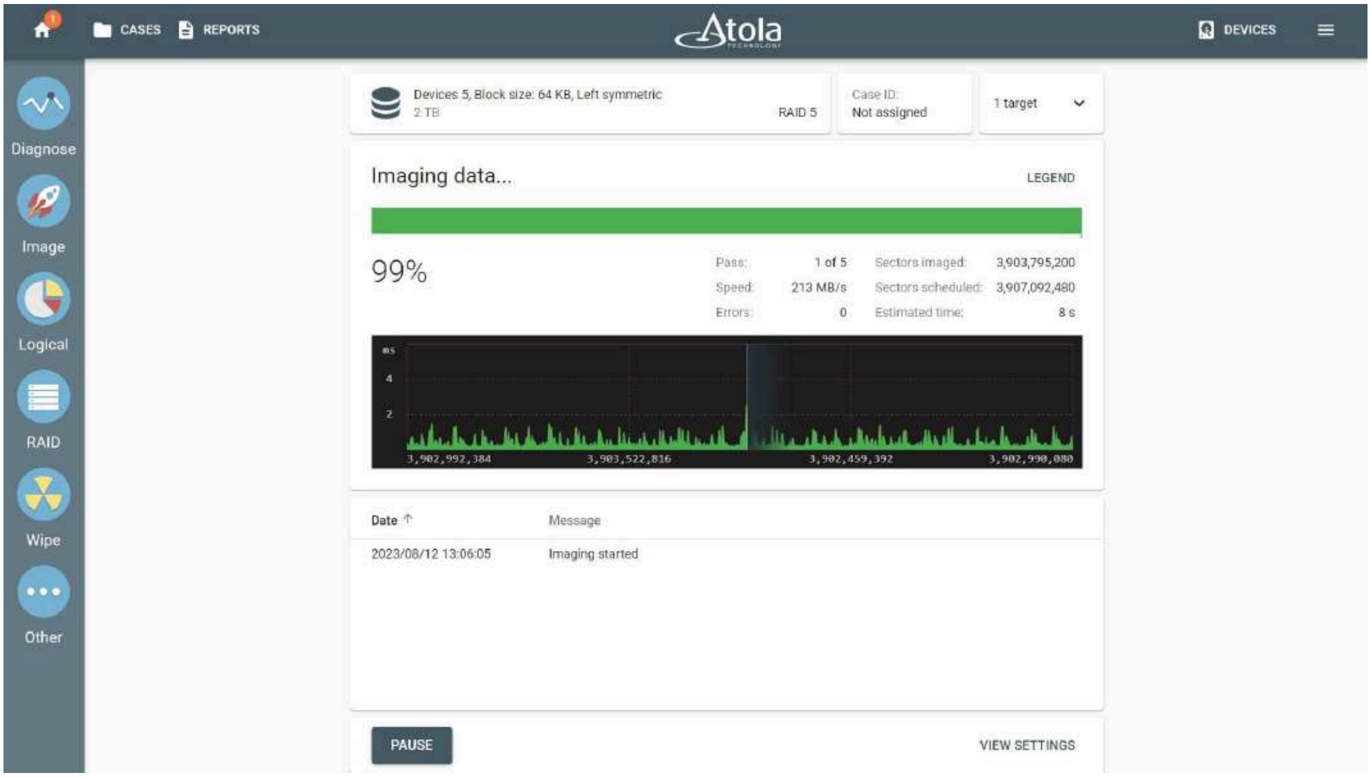
0%

Pass:	1 of 5	Sectors imaged:	2,715,648
Speed:	49 MB/s	Sectors scheduled:	3,907,092,480
Errors:	0	Estimated time:	11 h 24 m

Date ↑	Message
2023/08/12 13:06:05	Imaging started

Coping with errors.

Thus TaskForce 2 can recover the full image. No operator involvement is necessary.



Devices 5, Block size: 64 KB, Left symmetric
2 TB
RAID 5

Case ID:
Not assigned

1 target

Imaging data...

99%

Pass:	1 of 5	Sectors imaged:	3,903,795,200
Speed:	213 MB/s	Sectors scheduled:	3,907,092,480
Errors:	0	Estimated time:	8 s

Date ↑	Message
2023/08/12 13:06:05	Imaging started

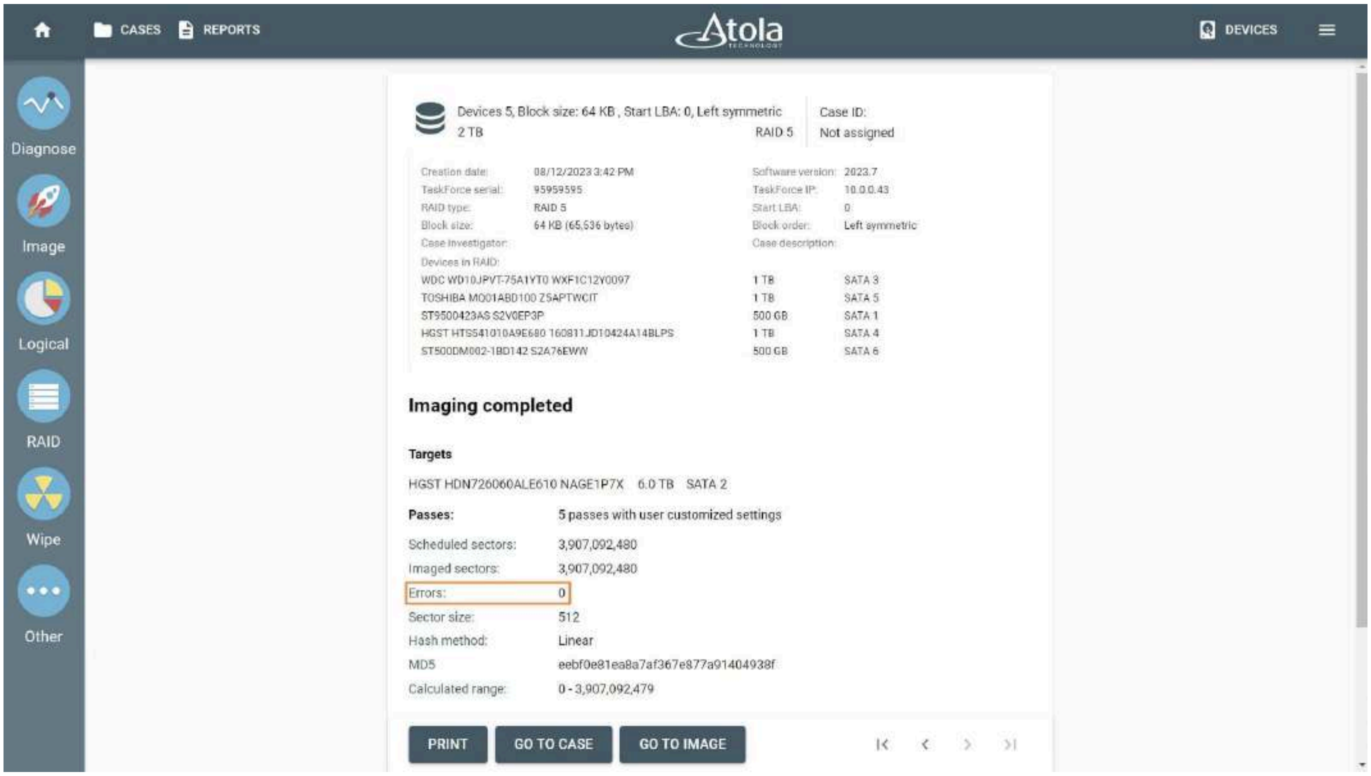
Imaging RAID 5 array.

> In case 2 drives of the RAID 5 array contain errors in the same sector, TaskForce 2 can still recover the data from those, using the multipass imaging system.

Imaging report

TaskForce 2 automatically generates the **Imaging completed** report with all RAID details and timestamps.

TaskForce 2 managed to successfully reconstruct and image all the data. That is why the number of errors in the **Imaging completed** report is zero.



Devices 5, Block size: 64 KB , Start LBA: 0, Left symmetric
2 TB
RAID 5

Case ID:
Not assigned

Creation date:	08/12/2023 3:42 PM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.43
RAID type:	RAID 5	Start LBA:	0
Block size:	64 KB (65,536 bytes)	Block order:	Left symmetric
Case investigator:		Case description:	

Devices in RAID:

WDC WD10JPVT-75A1YT0 WXF1C12Y0097	1 TB	SATA 3
TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB	SATA 5
ST9500423AS S2V0EP3P	500 GB	SATA 1
HGST HTS541010A9E680 160811JD10424A14BLPS	1 TB	SATA 4
ST500DM002-1BD142 S2A76EWW	500 GB	SATA 6

Imaging completed

Targets

HGST HDN726060ALE610 NAGE1P7X 6.0 TB SATA 2

Passes:	5 passes with user customized settings
Scheduled sectors:	3,907,092,480
Imaged sectors:	3,907,092,480
Errors:	0
Sector size:	512
Hash method:	Linear
MD5	eebf0e81ea8a7af367e877a91404938f
Calculated range:	0 - 3,907,092,479

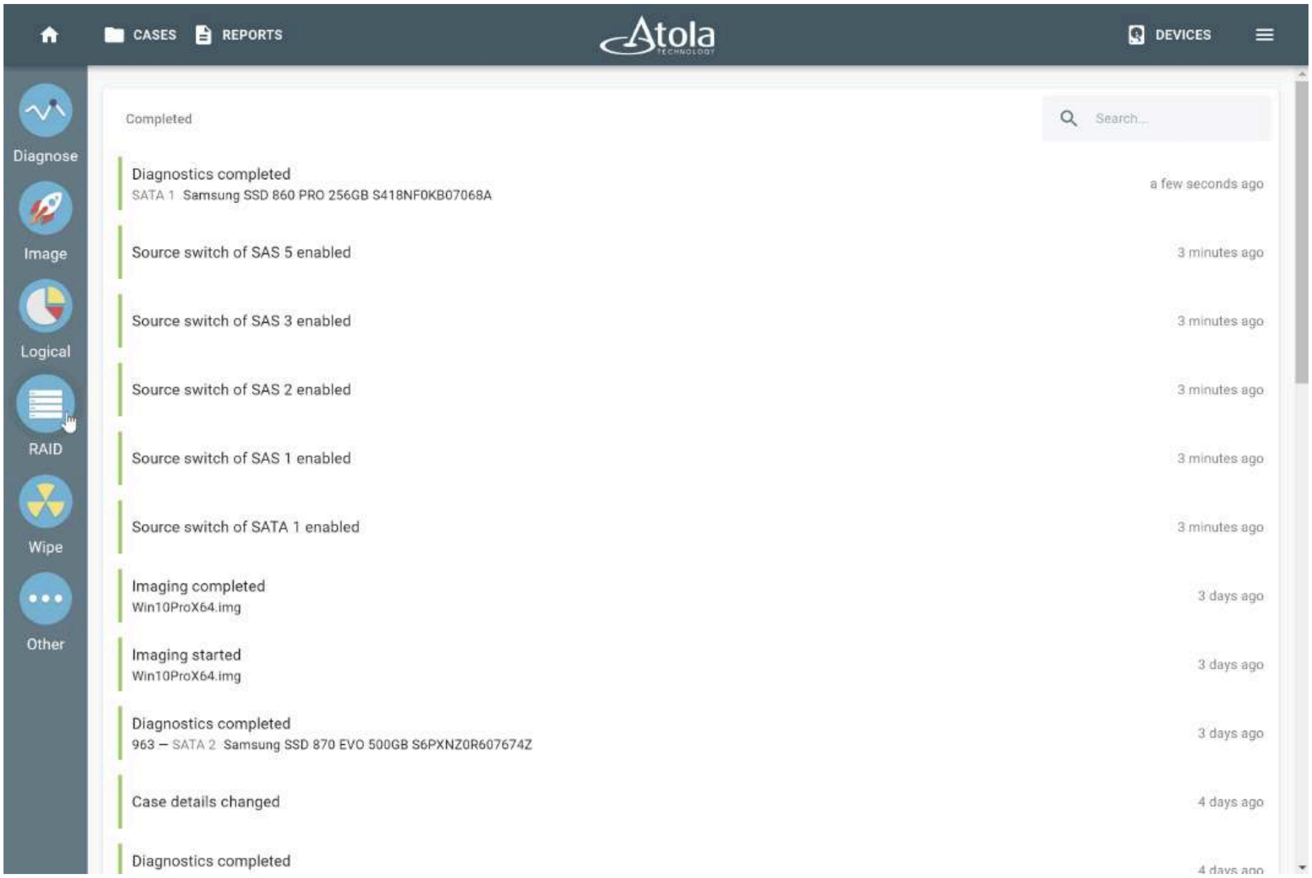
Imaging report.

RAID 6 with unknown configuration

Atola TaskForce 2 lets you automatically detect all parameters of a RAID 6 array, preview its contents, and then create its full physical image or perform logical imaging of only selected partitions, folders, and files.

To reassemble and image a RAID 6 array with an unknown configuration, do the following:

1. On the left in the TaskForce main window, click **RAID**.



Completed

Diagnostics completed
SATA 1 Samsung SSD 860 PRO 256GB S418NF0KB07068A — a few seconds ago

Source switch of SAS 5 enabled — 3 minutes ago

Source switch of SAS 3 enabled — 3 minutes ago

Source switch of SAS 2 enabled — 3 minutes ago

Source switch of SAS 1 enabled — 3 minutes ago

Source switch of SATA 1 enabled — 3 minutes ago

Imaging completed
Win10ProX64.img — 3 days ago

Imaging started
Win10ProX64.img — 3 days ago

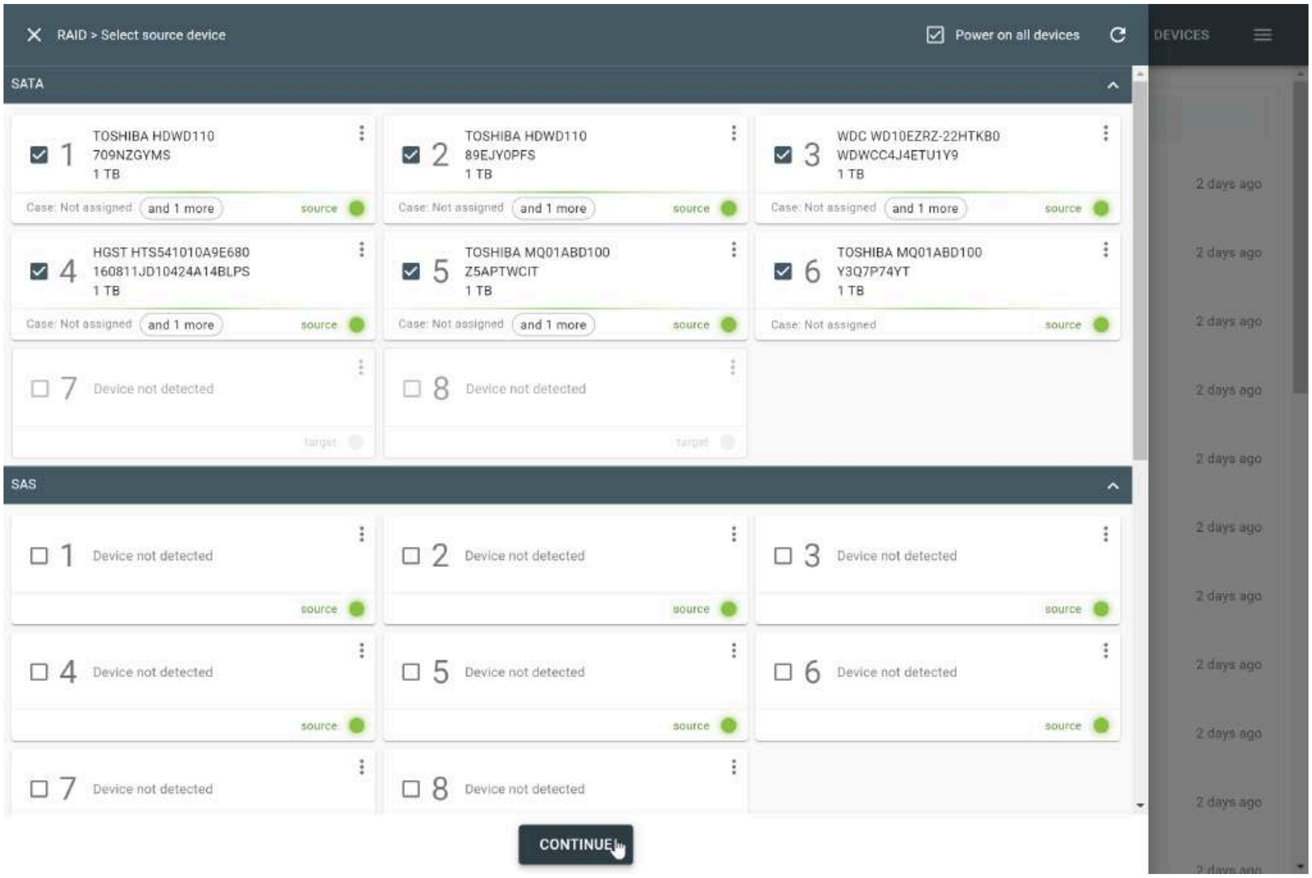
Diagnostics completed
963 — SATA 2 Samsung SSD 870 EVO 500GB S6PXNZ0R607674Z — 3 days ago

Case details changed — 4 days ago

Diagnostics completed — 4 days ago

Initiating work with RAID.

2. On the **Select source device** panel, select the devices that make up a RAID array. They can be physical drives of all supported types, connected to the TaskForce 2 hardware unit, image files (raw, E01 or AFF4 image files), or a combination of both.



SATA

☑ 1 TOSHIBA HDWD110 709NZGYMS 1 TB — Case: Not assigned, and 1 more — source

☑ 2 TOSHIBA HDWD110 89EJY0PFS 1 TB — Case: Not assigned, and 1 more — source

☑ 3 WDC WD10EZRZ-22HTKB0 WDWCC4J4ETU1Y9 1 TB — Case: Not assigned, and 1 more — source

☑ 4 HGST HTS541010A9E680 160811JD10424A14BLPS 1 TB — Case: Not assigned, and 1 more — source

☑ 5 TOSHIBA MQ01ABD100 Z5APTWCIT 1 TB — Case: Not assigned, and 1 more — source

☑ 6 TOSHIBA MQ01ABD100 Y3Q7P74YT 1 TB — Case: Not assigned — source

□ 7 Device not detected — target

□ 8 Device not detected — target

SAS

□ 1 Device not detected — source

□ 2 Device not detected — source

□ 3 Device not detected — source

□ 4 Device not detected — source

□ 5 Device not detected — source

□ 6 Device not detected — source

□ 7 Device not detected

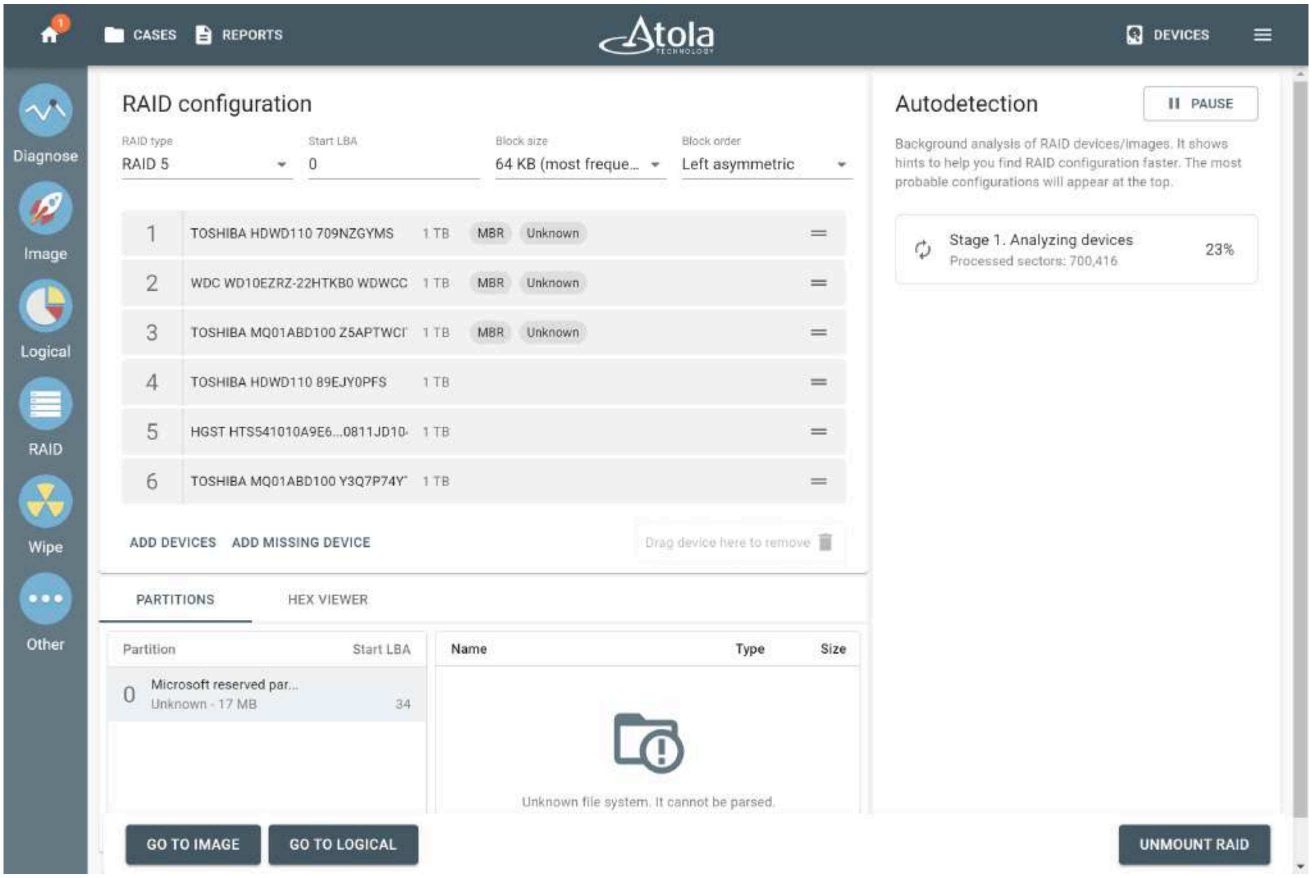
□ 8 Device not detected

2 days ago

Selecting RAID members.

3. Once all the RAID members are selected, click **Continue**.

4. TaskForce 2 redirects you to the **RAID configuration** screen and immediately starts the **Autodetection** module.



RAID configuration

RAID type	Start LBA	Block size	Block order
RAID 5	0	64 KB (most freque...	Left asymmetric

1	TOSHIBA HDWD110 709NZGYMS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown
3	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB	MBR	Unknown
4	TOSHIBA HDWD110 89EJY0PFS	1 TB		
5	HGST HTS541010A9E6...0811JD10	1 TB		
6	TOSHIBA MQ01ABD100 Y3Q7P74Y	1 TB		

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 23%
Processed sectors: 700,416

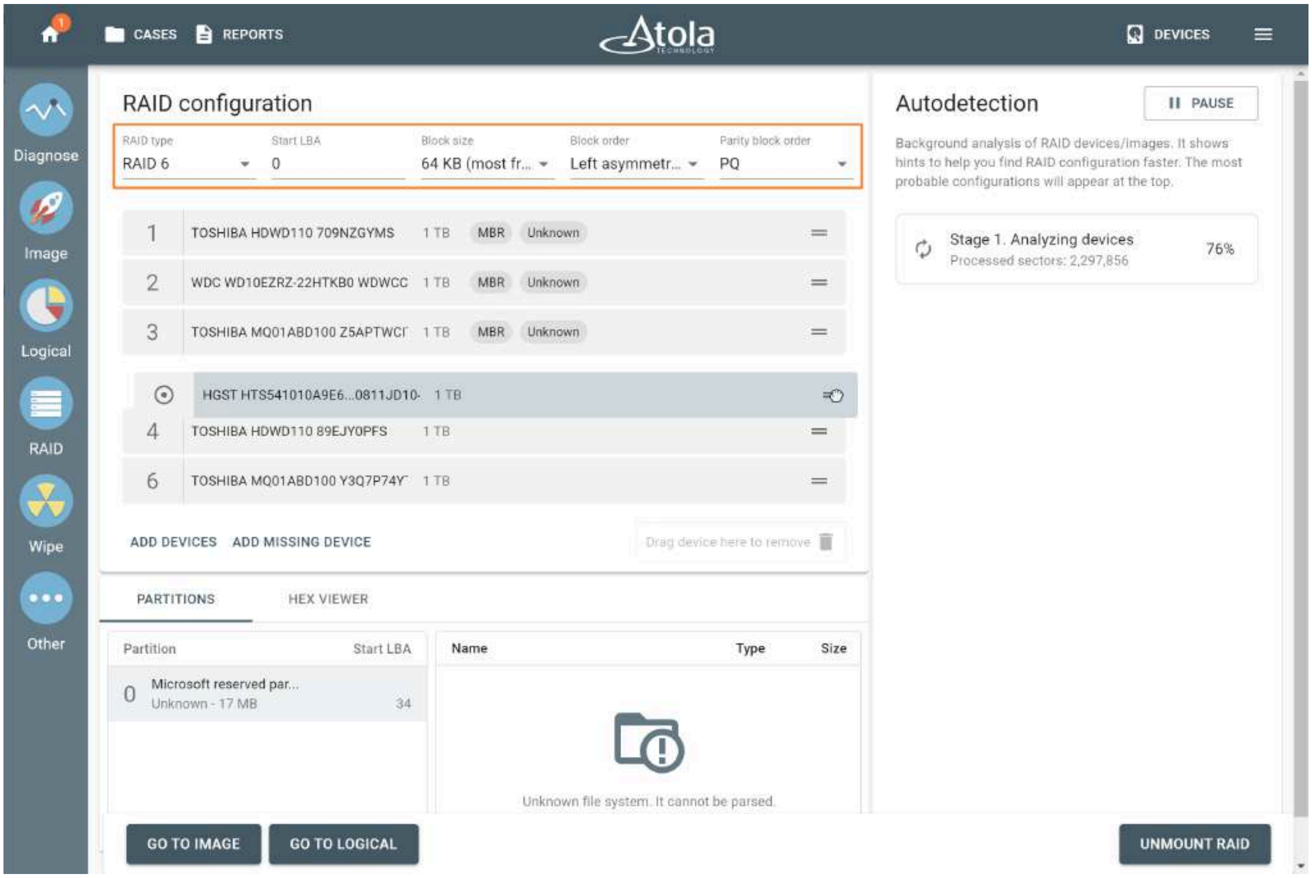
Partition		Start LBA
0	Microsoft reserved par... Unknown - 17 MB	34

Name	Type	Size

Unknown file system. It cannot be parsed.

The RAID configuration screen in Atola TaskForce 2.

5. **Optional:** If you know some of the RAID parameters, such as *RAID type*, *Start LBA*, *Block size*, and *Block order*, you can select them manually from the lists at the top of the **RAID configuration** section. To change the device order, drag the devices up or down, as needed.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	64 KB (most fr...	Left asymmetr...	PQ

1	TOSHIBA HDWD110 709NZGYMS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown
3	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB	MBR	Unknown
	HGST HTS541010A9E6...0811JD10	1 TB		
4	TOSHIBA HDWD110 89EJY0PFS	1 TB		
6	TOSHIBA MQ01ABD100 Y3Q7P74Y	1 TB		

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 76%
Processed sectors: 2,297,856

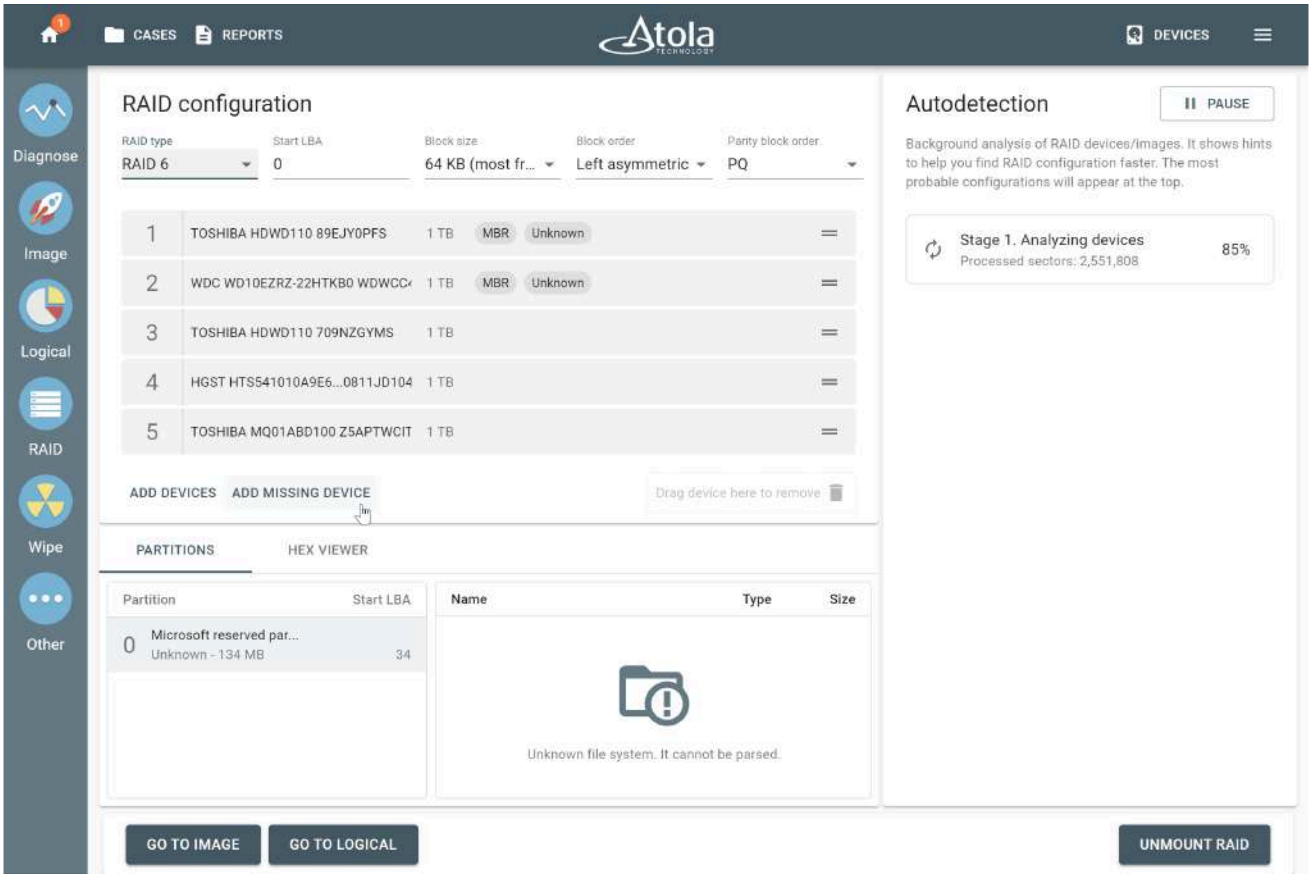
Partition	Start LBA
0 Microsoft reserved par... Unknown - 17 MB	34

Name	Type	Size

Unknown file system. It cannot be parsed.

Lists with RAID parameters for manual selection.

6. **Optional:** If you know that one or two RAID members are missing, choose *RAID 6* from the **RAID type** list and then click the **Add missing device** button once or twice respectively. For details, see RAID 6 with two missing devices.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	64 KB (most fr...	Left asymmetric	PQ

1	TOSHIBA HDWD110 89EJY0PFS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC‹	1 TB	MBR	Unknown
3	TOSHIBA HDWD110 709NZGYMS	1 TB		
4	HGST HTS541010A9E6...0811JD104	1 TB		
5	TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB		

Partition		Start LBA
0	Microsoft reserved par... Unknown - 134 MB	34

Name	Type	Size

Unknown file system. It cannot be parsed.

Autodetection

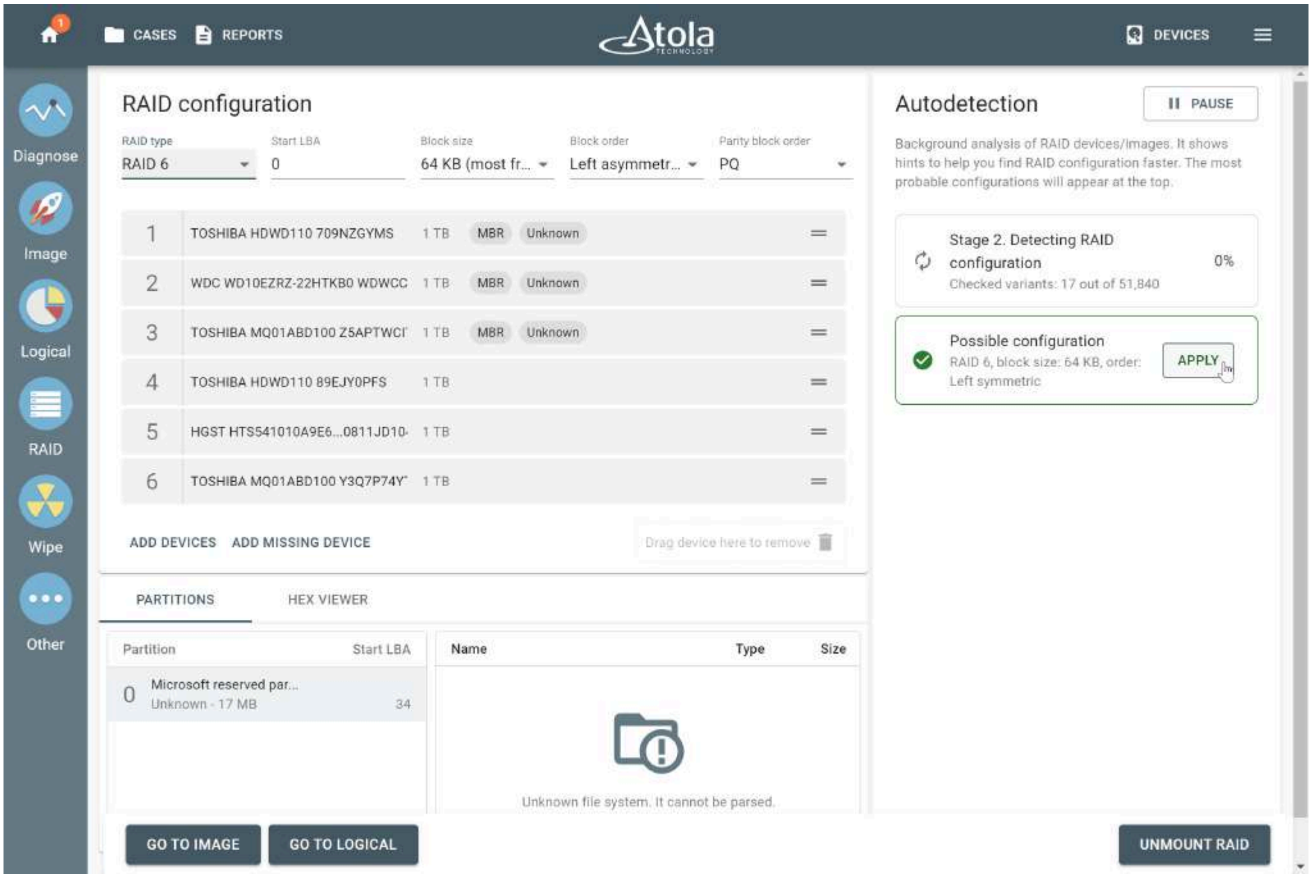
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 85%
Processed sectors: 2,551,808

Adding a missing device to a RAID.

7. Wait for a couple of minutes while the module is checking thousands of variants to find a possible RAID configuration. The Autodetection progress is displayed on the right side of the screen. To learn more about our heuristic RAID autodetection algorithm, see How autodetection of an unknown RAID works.

8. Once TaskForce 2 has detected a possible configuration, click **Apply**. TaskForce 2 automatically changes the order of the devices, applies the detected RAID type and other parameters, and then parses and verifies the file system of an array.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	64 KB (most fr...	Left asymmetr...	PQ

1	TOSHIBA HDWD110 709NZGYMS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown
3	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB	MBR	Unknown
4	TOSHIBA HDWD110 89EJY0PFS	1 TB		
5	HGST HTS541010A9E6...0811JD10	1 TB		
6	TOSHIBA MQ01ABD100 Y3Q7P74Y	1 TB		

Partition	Start LBA
0 Microsoft reserved par... Unknown · 17 MB	34

Name	Type	Size

Unknown file system. It cannot be parsed.

Autodetection

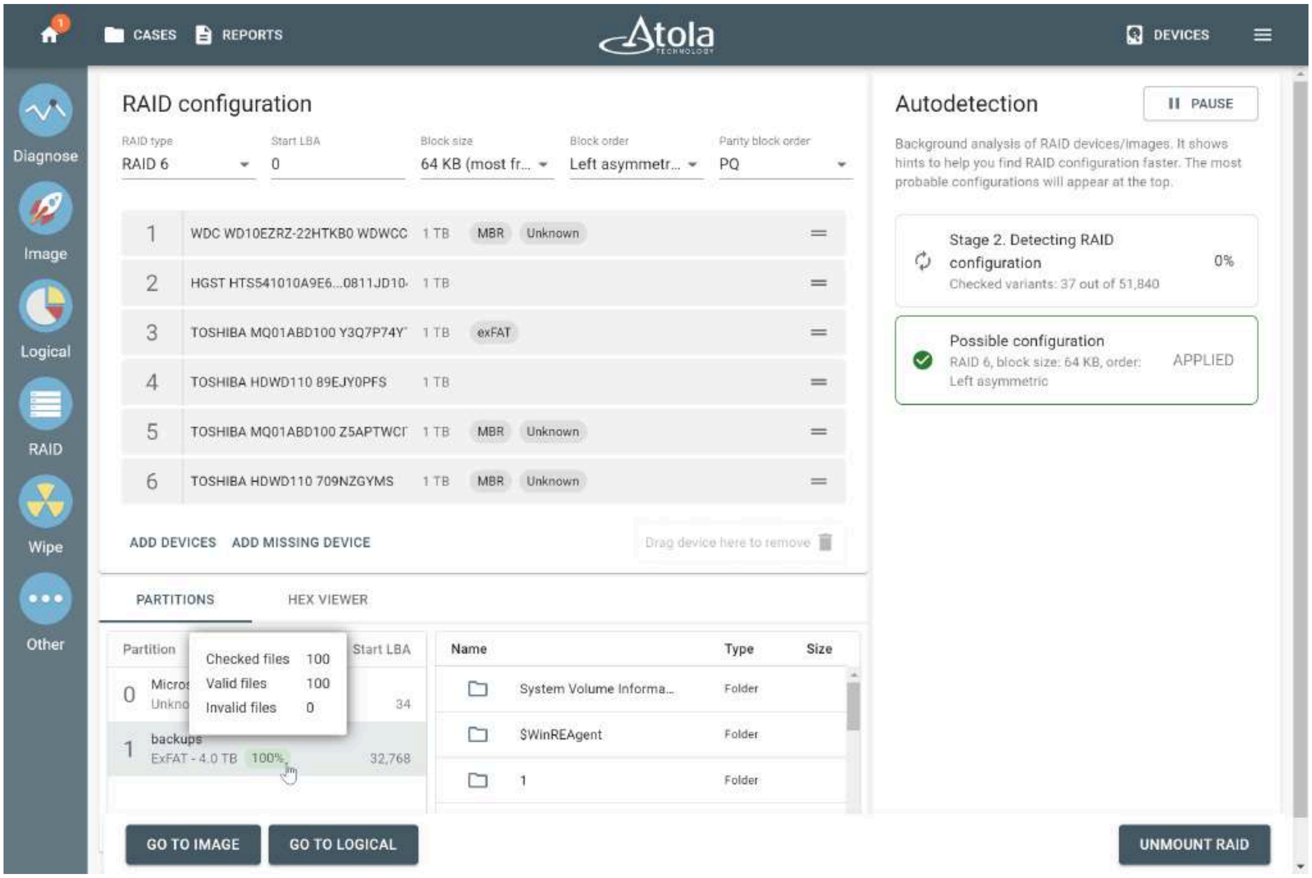
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 0%
Checked variants: 17 out of 51,840

Possible configuration
RAID 6, block size: 64 KB, order: Left symmetric

Applying a possible RAID configuration.

9. To make sure that the suggested RAID configuration is resulting in tangible data, check the **Partitions** section at the bottom left and preview the contents of a reassembled RAID, including partitions, folders, and files. To help you decide whether the applied configuration is valid or not, TaskForce 2 displays a small tag with the accuracy percentage next to the partition. In some cases, TaskForce will suggest alternative configurations, and you can try to improve the accuracy percentage by applying these alternative configurations.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	64 KB (most fr...	Left asymmetr...	PQ

1	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown
2	HGST HTS541010A9E6...0811JD10·	1 TB		
3	TOSHIBA MQ01ABD100 Y3Q7P74Y'	1 TB	exFAT	
4	TOSHIBA HDWD110 89EJY0PFS	1 TB		
5	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB	MBR	Unknown
6	TOSHIBA HDWD110 709NZGYMS	1 TB	MBR	Unknown

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 0%
Checked variants: 37 out of 51,840

Possible configuration APPLIED
RAID 6, block size: 64 KB, order: Left asymmetric

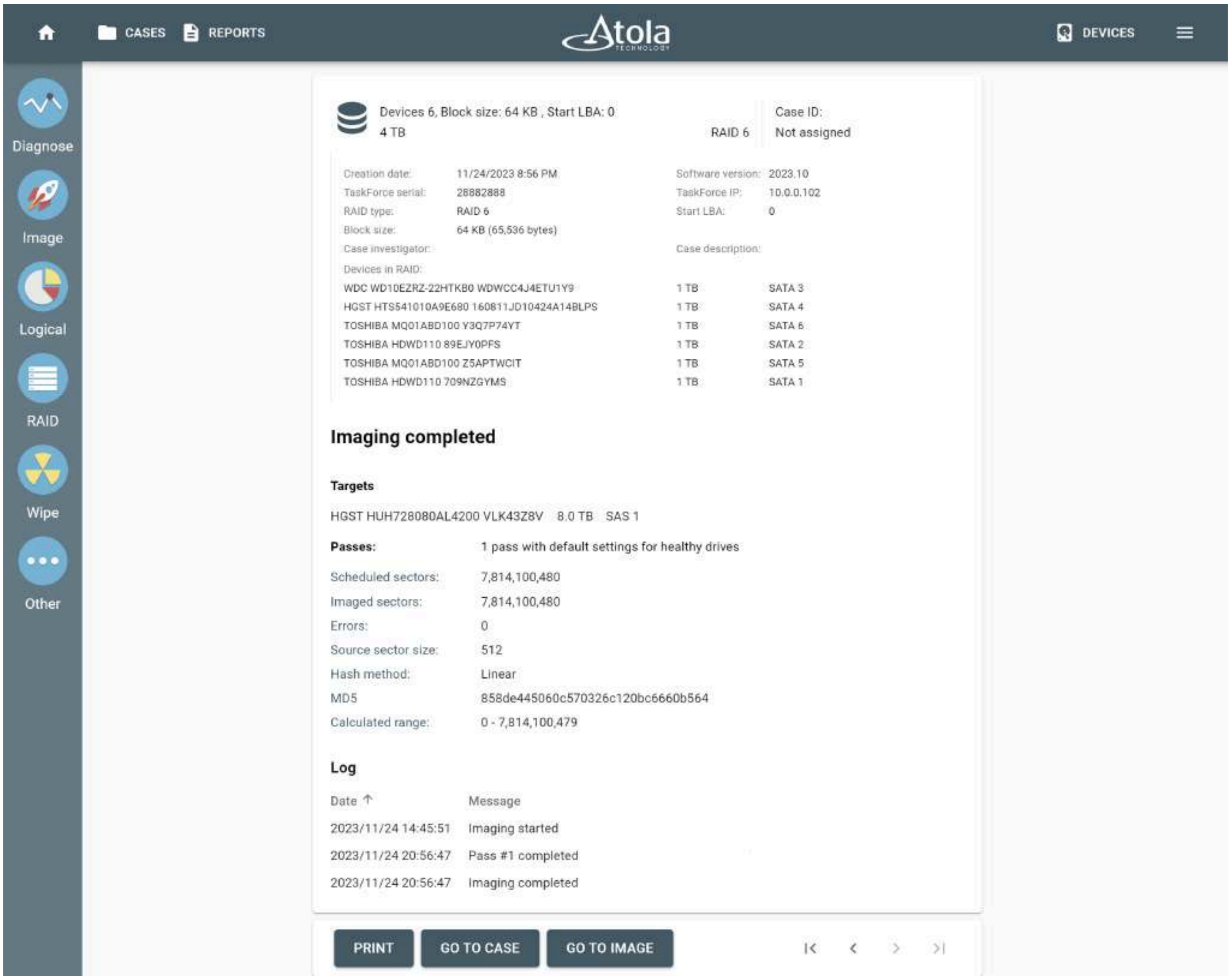
Partition		Start LBA
0	Micros Unkno	34
1	backups ExFAT - 4.0 TB 100%	32,768

Checked files	100
Valid files	100
Invalid files	0

Name	Type	Size
System Volume Informa...	Folder	
$WinREAgent	Folder	
1	Folder	

The preview of the RAID contents.

10. Click **Go to image** to acquire a full bit-by-bit copy of the array to E01, AFF4, or raw image. Or click **Go to logical** to copy only selected partitions, folders, or files to L01 or ZIP.
11. After imaging is finished, TaskForce 2 automatically generates an **Imaging completed** report. It includes all the details of the source drives, the RAID configuration, the target, the partition, the timestamps and more.



Devices 6, Block size: 64 KB , Start LBA: 0
4 TB

RAID 6

Case ID:
Not assigned

Creation date:	11/24/2023 8:56 PM	Software version:	2023.10
TaskForce serial:	28882888	TaskForce IP:	10.0.0.102
RAID type:	RAID 6	Start LBA:	0
Block size:	64 KB (65,536 bytes)		
Case investigator:		Case description:	

Devices in RAID:

WDC WD10EZRZ-22HTKB0 WDWCC4J4ETU1Y9	1 TB	SATA 3
HGST HTS541010A9E680 160811JD10424A14BLPS	1 TB	SATA 4
TOSHIBA MQ01ABD100 Y3Q7P74YT	1 TB	SATA 6
TOSHIBA HDWD110 89EJY0PFS	1 TB	SATA 2
TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB	SATA 5
TOSHIBA HDWD110 709NZGYMS	1 TB	SATA 1

Imaging completed

Targets

HGST HUH728080AL4200 VLK43Z8V 8.0 TB SAS 1

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	7,814,100,480
Imaged sectors:	7,814,100,480
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	858de445060c570326c120bc6660b564
Calculated range:	0 - 7,814,100,479

Log

Date ↑	Message
2023/11/24 14:45:51	Imaging started
2023/11/24 20:56:47	Pass #1 completed
2023/11/24 20:56:47	Imaging completed

The Imaging completed report.

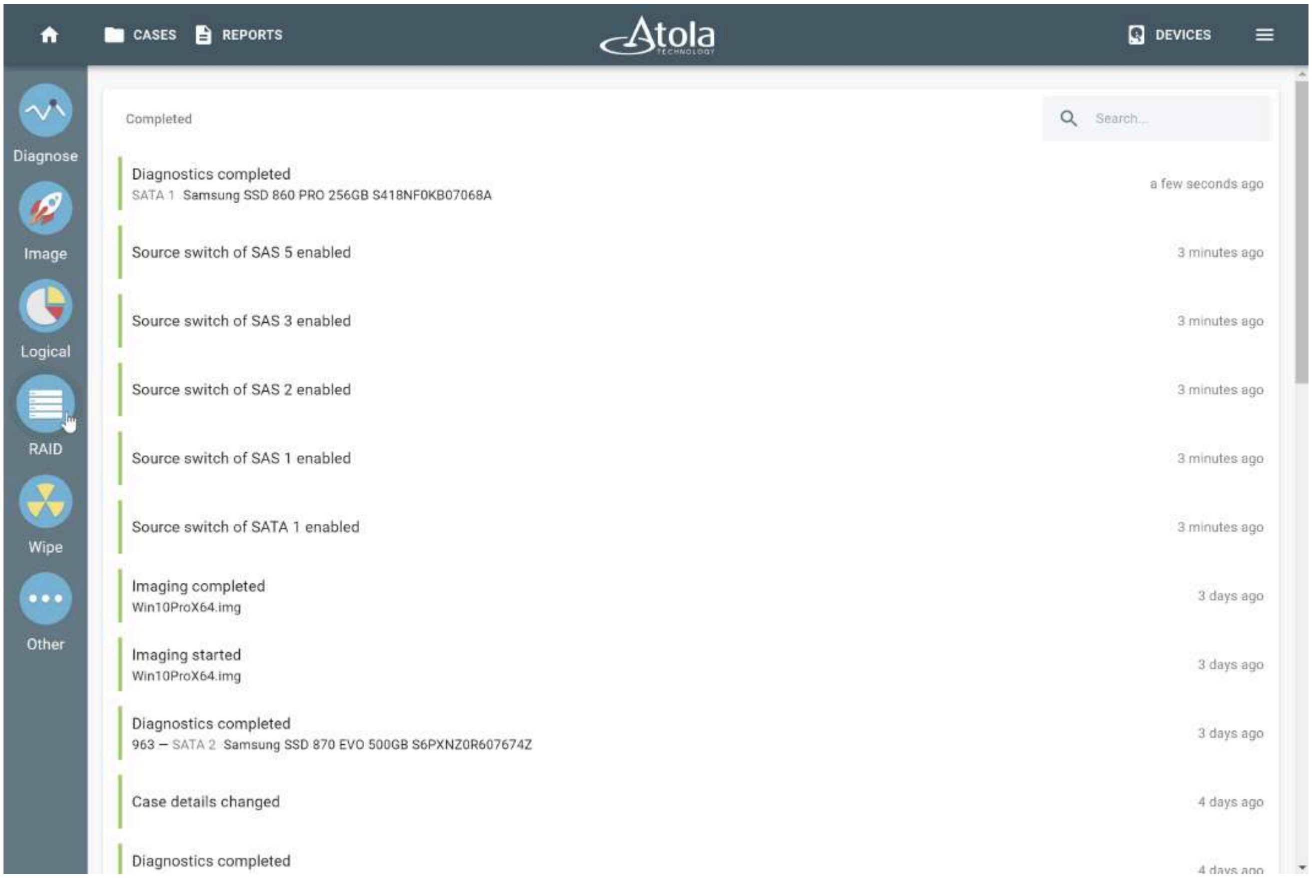
RAID 6 with two missing devices

Even if two of the devices in a RAID 6 array are damaged or missing, Atola TaskForce 2 can rebuild and image a RAID of this type, taking advantage of its extra redundancy. To accomplish that, TaskForce 2 uses both types of parity blocks, XOR parity and Reed-Solomon parity, distributed across all the devices in a RAID 6 array.

TaskForce 2 automatically detects all parameters of a RAID 6 array with two missing devices, reassembles the array, and enables a preview of its contents. Once the RAID is reassembled, you can acquire its full physical image or perform logical imaging of only selected partitions, folders, and files.

To rebuild and image a RAID 6 array with one or two missing devices, do the following:

1. In the Taskbar, click **RAID**.



Completed

Diagnostics completed
SATA 1 Samsung SSD 860 PRO 256GB S418NF0KB07068A — a few seconds ago

Source switch of SAS 5 enabled — 3 minutes ago

Source switch of SAS 3 enabled — 3 minutes ago

Source switch of SAS 2 enabled — 3 minutes ago

Source switch of SAS 1 enabled — 3 minutes ago

Source switch of SATA 1 enabled — 3 minutes ago

Imaging completed
Win10ProX64.img — 3 days ago

Imaging started
Win10ProX64.img — 3 days ago

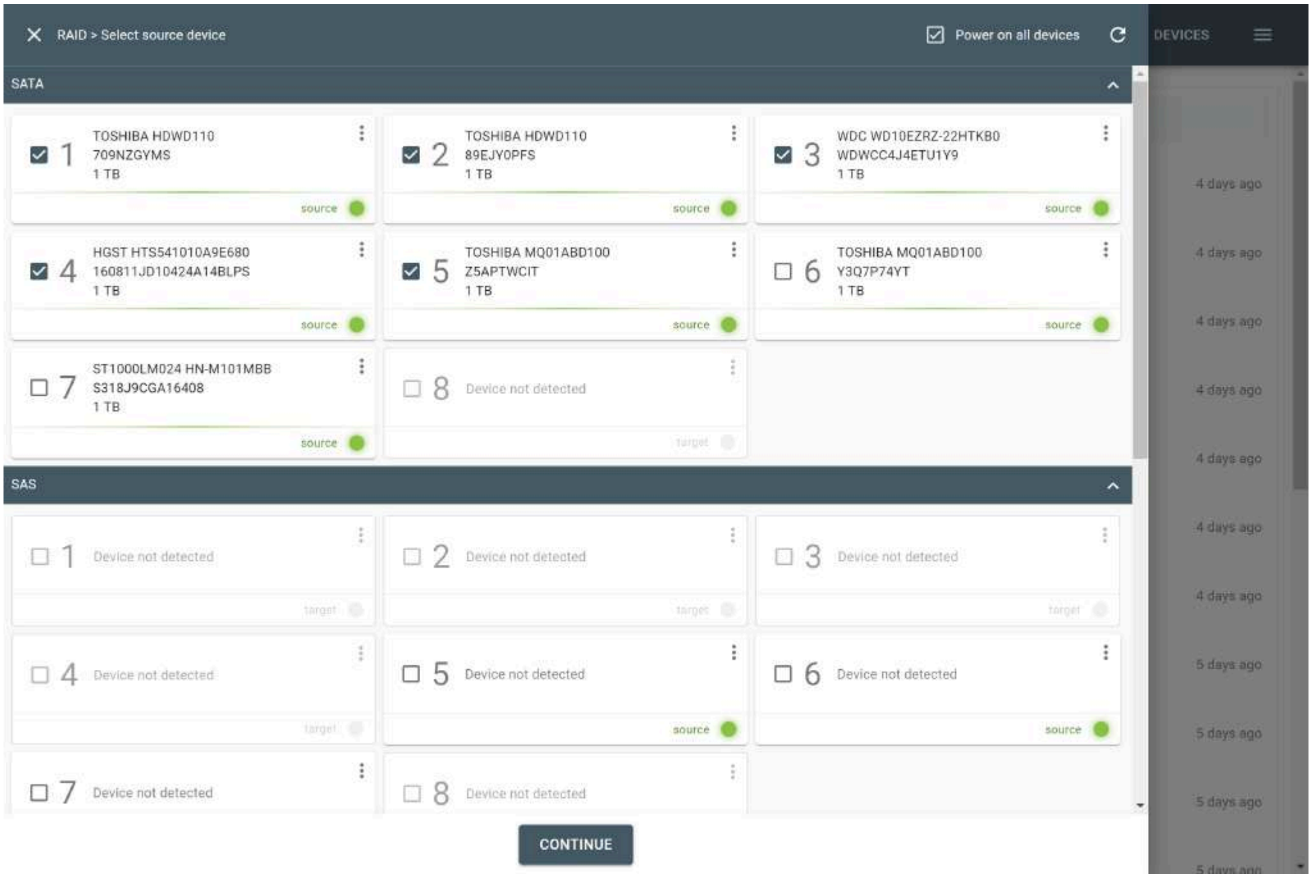
Diagnostics completed
963 — SATA 2 Samsung SSD 870 EVO 500GB S6PXNZ0R607674Z — 3 days ago

Case details changed — 4 days ago

Diagnostics completed — 4 days ago

Initiating work with RAID.

2. On the **Select source device** panel, select the devices that make up a RAID array. They can be physical drives of all supported types, connected to the TaskForce 2 hardware unit, image files (raw, E01 or AFF4 image files), or a combination of both.



SATA

☑ 1 TOSHIBA HDWD110 709NZGYMS 1 TB — source ●

☑ 2 TOSHIBA HDWD110 89EJY0PFS 1 TB — source ●

☑ 3 WDC WD10EZRZ-22HTKB0 WDWCC4J4ETU1Y9 1 TB — source ●

☑ 4 HGST HTS541010A9E680 160811JD10424A14BLPS 1 TB — source ●

☑ 5 TOSHIBA MQ01ABD100 Z5APTWCIT 1 TB — source ●

□ 6 TOSHIBA MQ01ABD100 Y3Q7P74YT 1 TB — source ●

□ 7 ST1000LM024 HN-M101MBB S318J9CGA16408 1 TB — source ●

□ 8 Device not detected — target ○

SAS

□ 1 Device not detected — target ○

□ 2 Device not detected — target ○

□ 3 Device not detected — target ○

□ 4 Device not detected — target ○

□ 5 Device not detected — source ●

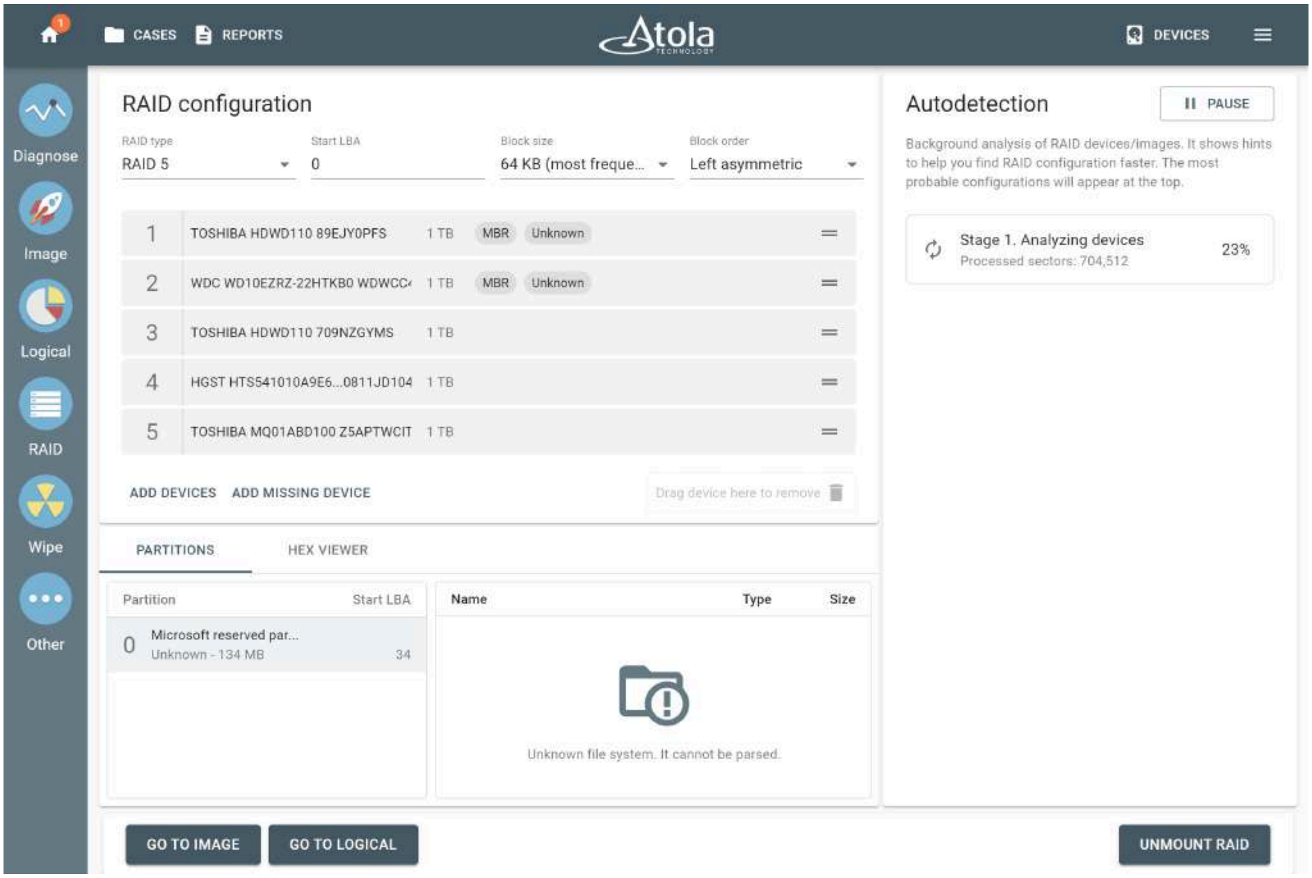
□ 6 Device not detected — source ●

□ 7 Device not detected

□ 8 Device not detected

Selecting RAID members.

3. Once the available RAID members are selected, click **Continue**.
4. TaskForce 2 redirects you to the RAID reassembly screen and immediately starts the **Autodetection** process to find the suitable configuration.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left asymmetric

1	TOSHIBA HDWD110 89EJY0PFS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC‹	1 TB	MBR	Unknown
3	TOSHIBA HDWD110 709NZGYMS	1 TB		
4	HGST HTS541010A9E6...0811JD104	1 TB		
5	TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB		

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 23%
Processed sectors: 704,512

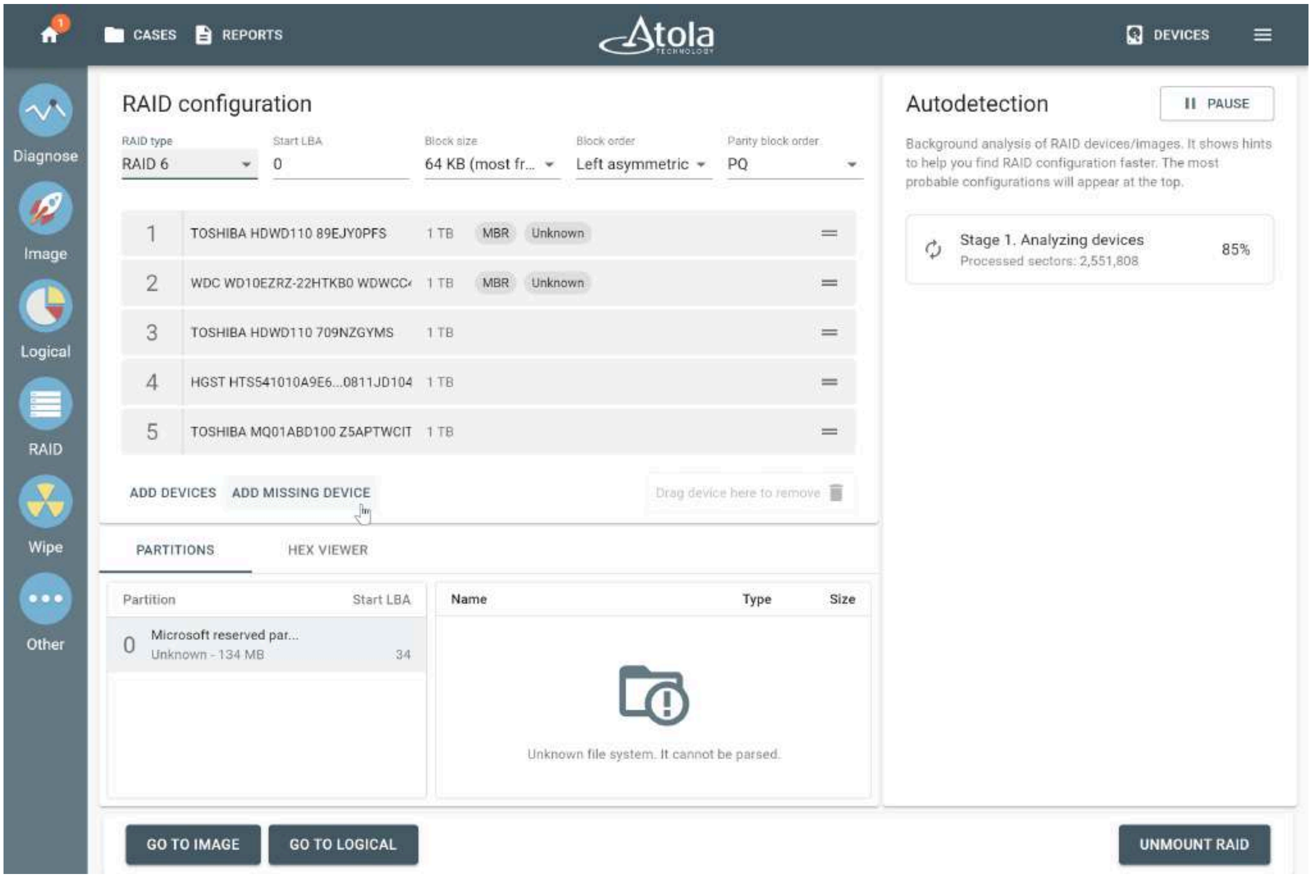
Partition		Start LBA
0	Microsoft reserved par... Unknown - 134 MB	34

Name	Type	Size

Unknown file system. It cannot be parsed.

The RAID configuration screen in Atola TaskForce 2.

5. Since you know that one or two RAID members are missing, select *RAID 6* from the **RAID type** list and click the **Add missing device** button once or twice respectively. When checking variants of possible RAID configuration, TaskForce 2 will take into account that there are missing RAID members.



RAID configuration

RAID type: RAID 6
Start LBA: 0
Block size: 64 KB (most fr...
Block order: Left asymmetric
Parity block order: PQ

1	TOSHIBA HDWD110 89EJY0PFS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC‹	1 TB	MBR	Unknown
3	TOSHIBA HDWD110 709NZGYMS	1 TB		
4	HGST HTS541010A9E6...0811JD104	1 TB		
5	TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB		

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices
Processed sectors: 2,551,808
85%

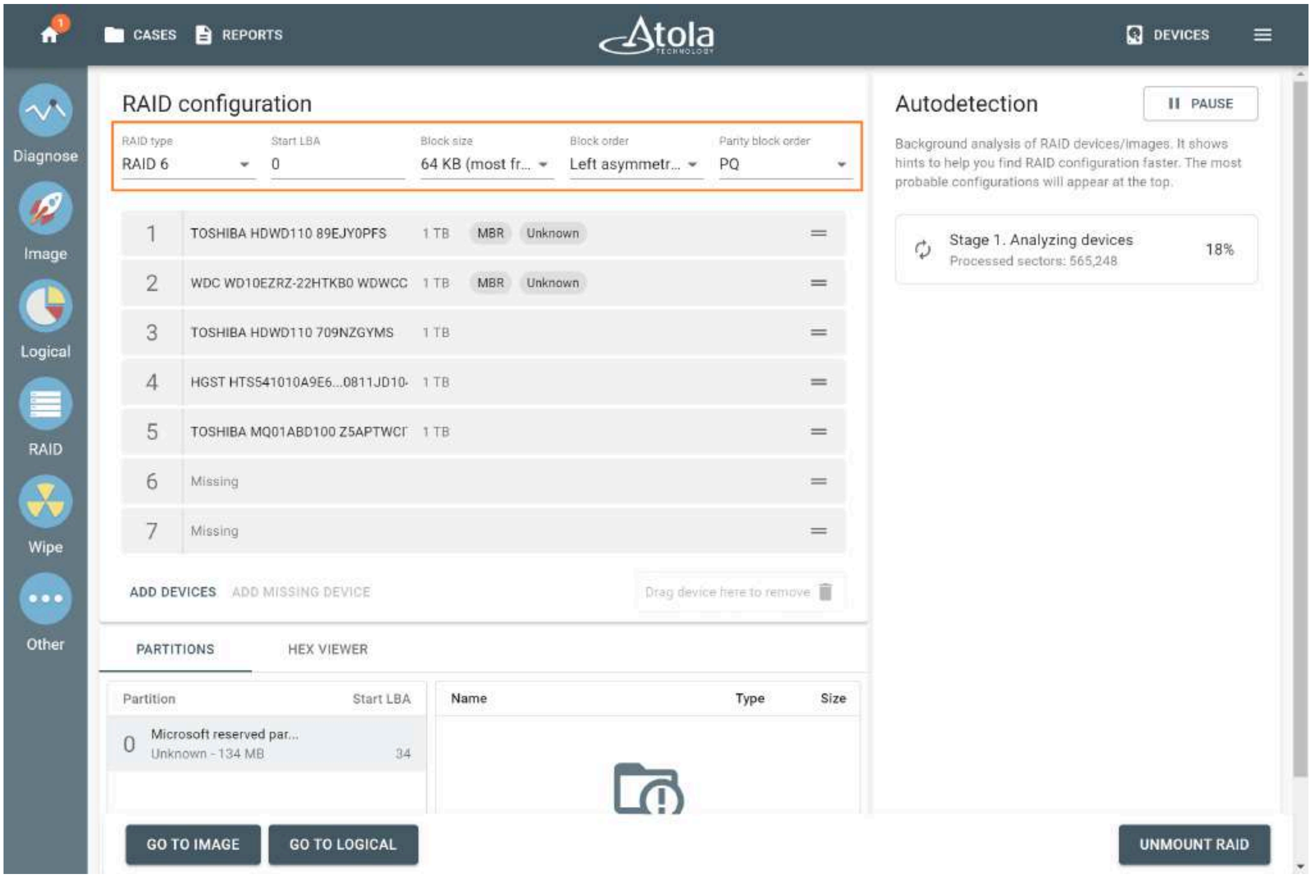
Partition	Start LBA
0 Microsoft reserved par... Unknown - 134 MB	34

Name	Type	Size

Unknown file system. It cannot be parsed.

Adding a missing device to a RAID.

6. **Optional:** If you know some of the RAID parameters, such as *RAID type*, *Start LBA*, *Block size*, *Block order*, *Parity block order*, you can select them manually from the lists at the top of the **RAID configuration** section.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	64 KB (most fr...	Left asymmetr...	PQ

1	TOSHIBA HDWD110 89EJY0PFS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown
3	TOSHIBA HDWD110 709NZGYMS	1 TB		
4	HGST HTS541010A9E6...0811JD10-	1 TB		
5	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB		
6	Missing			
7	Missing			

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 18%
Processed sectors: 565,248

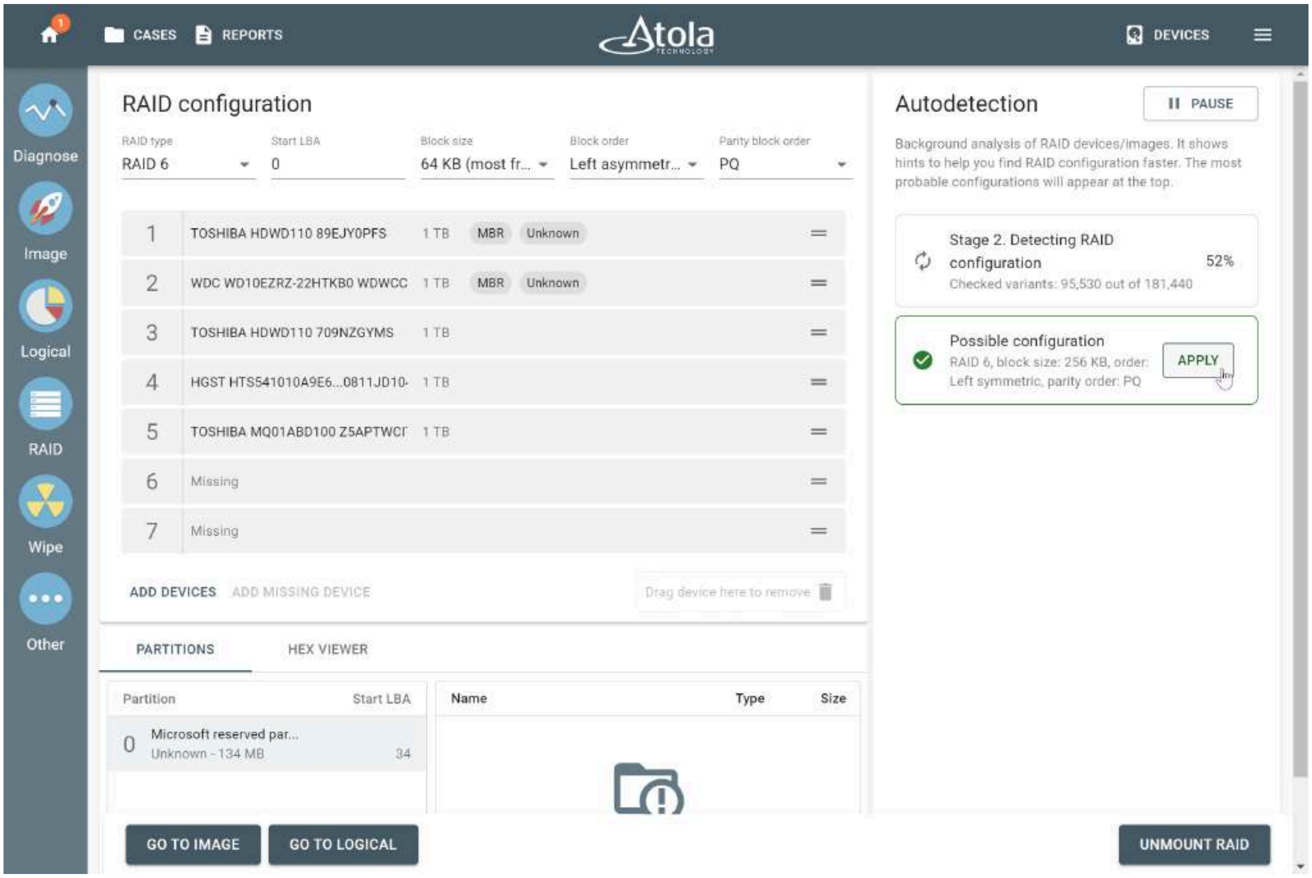
	Partition	Start LBA
0	Microsoft reserved par... Unknown - 134 MB	34

Name	Type	Size

Lists with RAID parameters for manual selection.

7. Wait while the module is checking thousands of variants to find a possible RAID configuration. Autodetection progress is displayed on the right side of the screen. To learn more about our heuristic RAID autodetection algorithm, see How autodetection of an unknown RAID works.

8. Once TaskForce 2 has detected a possible configuration with two missing devices, click **Apply**. TaskForce 2 automatically changes the order of the devices, applies the detected RAID type and other parameters, and then parses and verifies the file systems of an array.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	64 KB (most fr...	Left asymmetr...	PQ

1	TOSHIBA HDWD110 89EJY0PFS	1 TB	MBR	Unknown
2	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown
3	TOSHIBA HDWD110 709NZGYMS	1 TB		
4	HGST HTS541010A9E6...0811JD10-	1 TB		
5	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB		
6	Missing			
7	Missing			

Partition		Start LBA
0	Microsoft reserved par... Unknown - 134 MB	34

Name	Type	Size

Autodetection

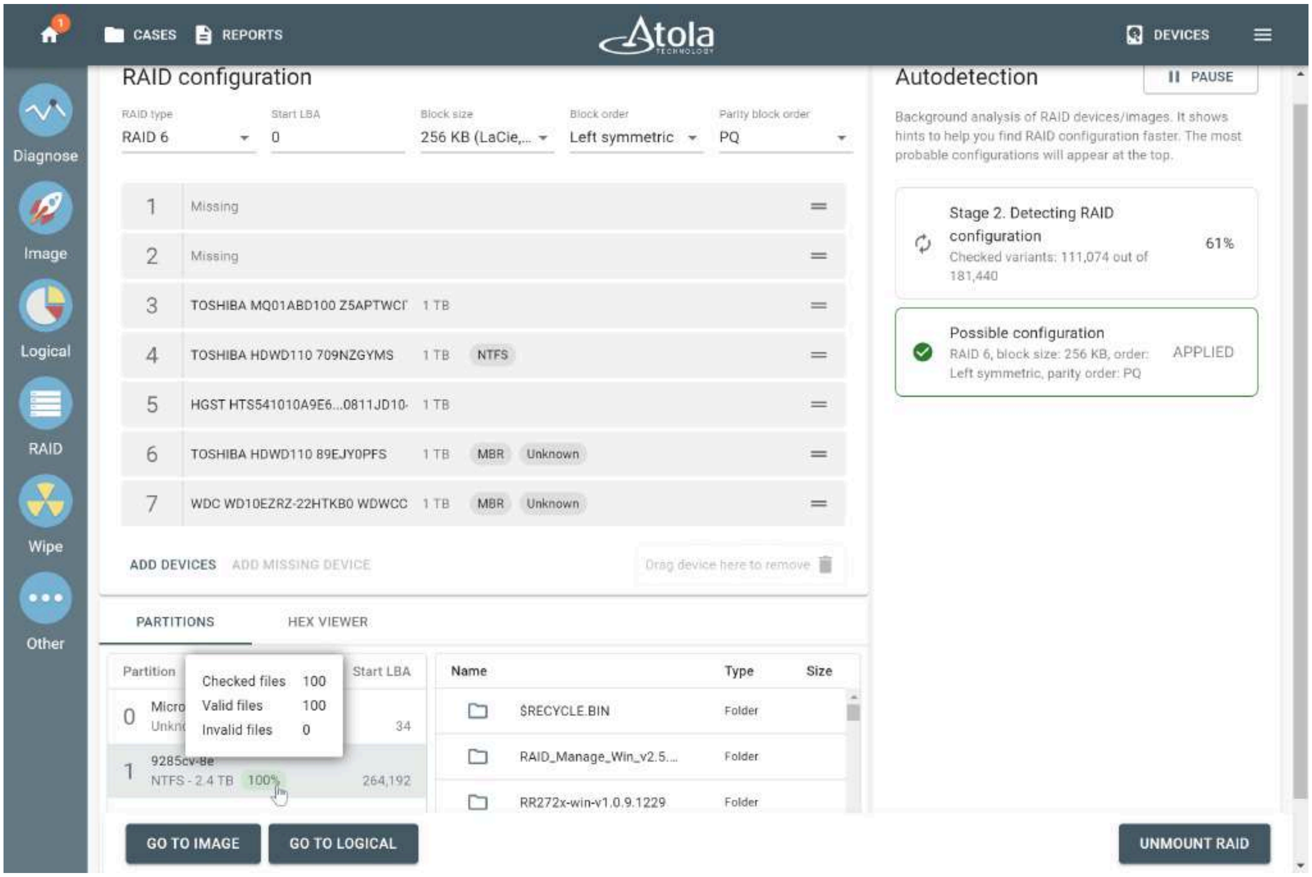
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 52%
Checked variants: 95,530 out of 181,440

Possible configuration
RAID 6, block size: 256 KB, order: Left symmetric, parity order: PQ

Applying a possible RAID configuration.

9. To make sure that the suggested RAID configuration is correct, check the **Partitions** section at the bottom left and preview the contents of the reassembled RAID, including partitions, folders, and files. To help you decide whether the applied configuration is valid or not, TaskForce 2 displays a small tag with the accuracy percentage near the partition.



RAID configuration

RAID type	Start LBA	Block size	Block order	Parity block order
RAID 6	0	256 KB (LaCie,...	Left symmetric	PQ

1	Missing			
2	Missing			
3	TOSHIBA MQ01ABD100 Z5APTWCI	1 TB		
4	TOSHIBA HDWD110 709NZGYMS	1 TB	NTFS	
5	HGST HTS541010A9E6...0811JD10	1 TB		
6	TOSHIBA HDWD110 89EJY0PFS	1 TB	MBR	Unknown
7	WDC WD10EZRZ-22HTKB0 WDWCC	1 TB	MBR	Unknown

Partition		Start LBA
0	Micro Unkn	34
1	9285cv-8e NTFS - 2.4 TB 100%	264,192

Checked files	100
Valid files	100
Invalid files	0

Name	Type	Size
$RECYCLE.BIN	Folder	
RAID_Manage_Win_v2.5....	Folder	
RR272x-win-v1.0.9.1229	Folder	

Autodetection

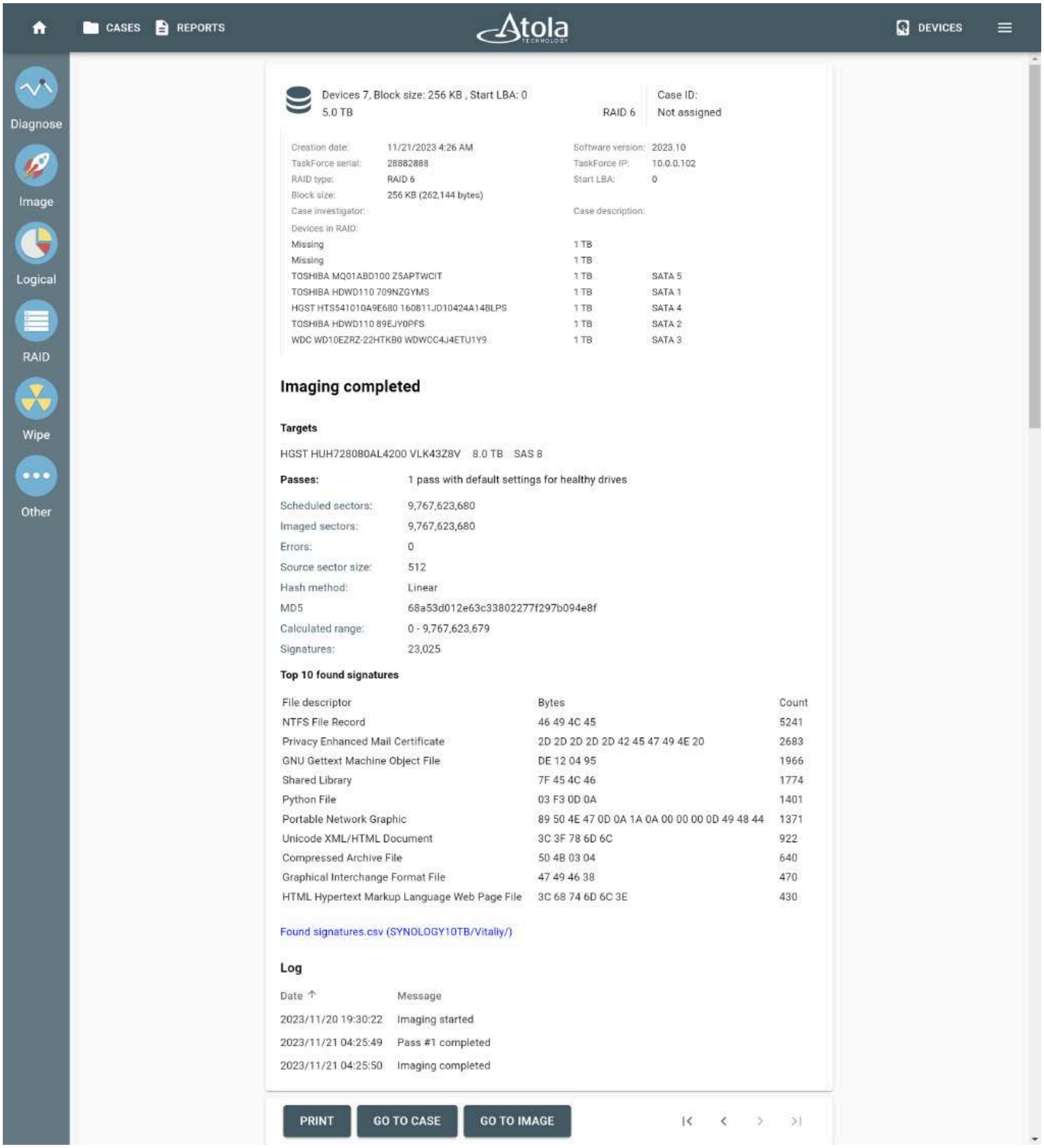
Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration
Checked variants: 111,074 out of 181,440
61%

Possible configuration
RAID 6, block size: 256 KB, order: Left symmetric, parity order: PQ
APPLIED

The preview of the RAID contents.

10. Click **Go to image** to acquire a full bit-by-bit copy of the array or **Go to logical** to copy only selected partitions, folders, or files.
11. After imaging is finished, TaskForce 2 automatically generates an **Imaging completed** report. It includes all the details of the source drives, the RAID configuration, the target image, the timestamps and more.



Devices 7, Block size: 256 KB , Start LBA: 0
5.0 TB

RAID 6

Case ID:
Not assigned

Creation date:	11/21/2023 4:26 AM	Software version:	2023.10
TaskForce serial:	28882888	TaskForce IP:	10.0.0.102
RAID type:	RAID 6	Start LBA:	0
Block size:	256 KB (262,144 bytes)		
Case investigator:		Case description:	

Devices in RAID:

Missing	1 TB	
Missing	1 TB	
TOSHIBA MQ01ABD100 Z5APTWCIT	1 TB	SATA 5
TOSHIBA HDWD110 709NZGYMS	1 TB	SATA 1
HGST HTS541010A9E680 160811JD10424A14BLPS	1 TB	SATA 4
TOSHIBA HDWD110 89EJY0PFS	1 TB	SATA 2
WDC WD10EZRZ-22HTKB0 WDWCC4J4ETU1Y9	1 TB	SATA 3

Imaging completed

Targets

HGST HUH728080AL4200 VLK43Z8V 8.0 TB SAS 8

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	9,767,623,680
Imaged sectors:	9,767,623,680
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	68a53d012e63c33802277f297b094e8f
Calculated range:	0 - 9,767,623,679
Signatures:	23,025

Top 10 found signatures

File descriptor	Bytes	Count
NTFS File Record	46 49 4C 45	5241
Privacy Enhanced Mail Certificate	2D 2D 2D 2D 2D 42 45 47 49 4E 20	2683
GNU Gettext Machine Object File	DE 12 04 95	1966
Shared Library	7F 45 4C 46	1774
Python File	03 F3 0D 0A	1401
Portable Network Graphic	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44	1371
Unicode XML/HTML Document	3C 3F 78 6D 6C	922
Compressed Archive File	50 4B 03 04	640
Graphical Interchange Format File	47 49 46 38	470
HTML Hypertext Markup Language Web Page File	3C 68 74 6D 6C 3E	430

Found signatures.csv (SYNOLOGY10TB/Vitaliy/)

Log

Date ↑	Message
2023/11/20 19:30:22	Imaging started
2023/11/21 04:25:49	Pass #1 completed
2023/11/21 04:25:50	Imaging completed

The Imaging completed report.

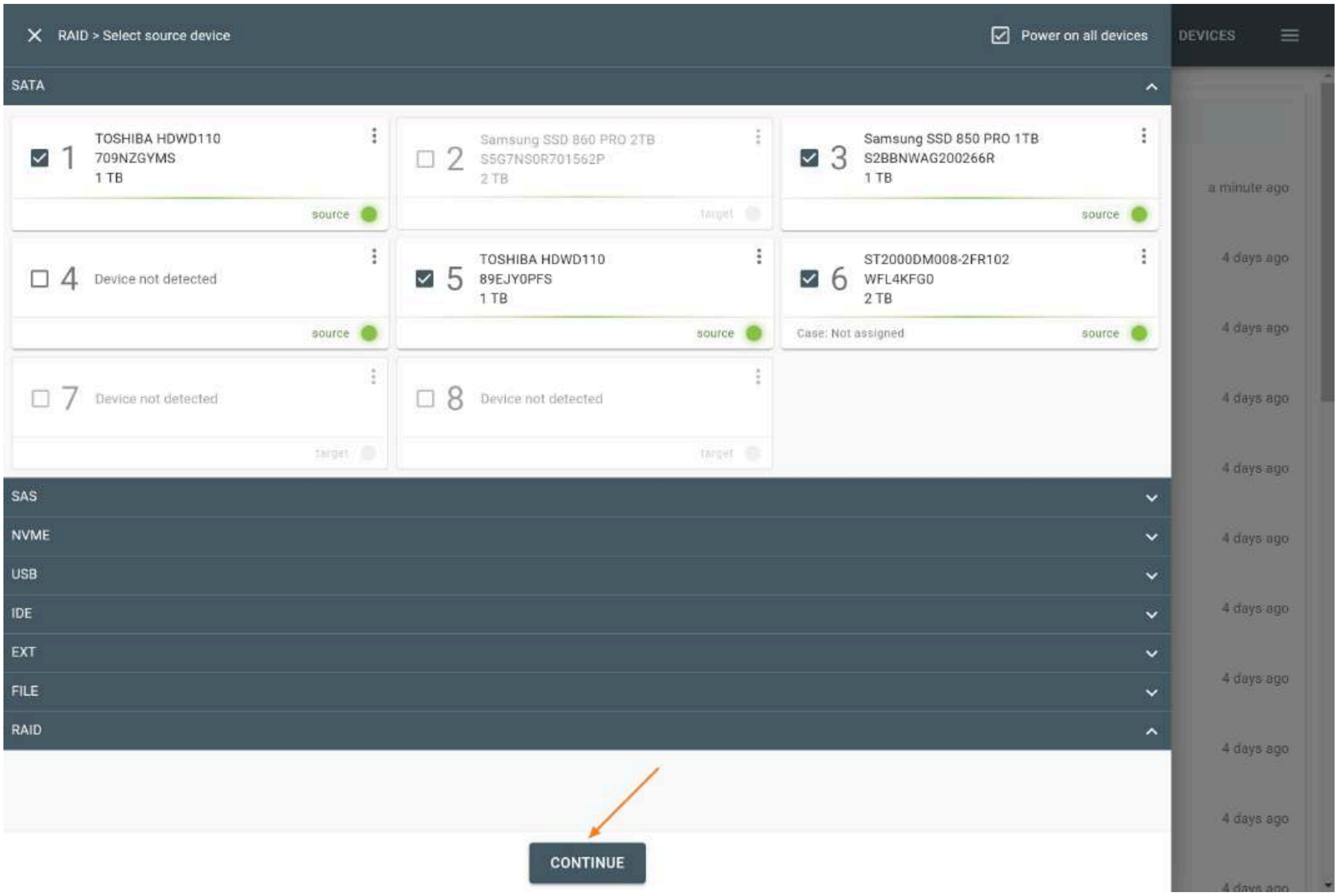
RAID 10: reassembly and imaging

RAID 10 arrays combine mirroring and striping techniques. This helps these arrays have higher performance and better resiliency against data loss or corruption. TaskForce 2 uses both of these advantages: it images data faster from a RAID 10 compared to other RAID types and rebuilds the image using the data redundancy in case of disk failure.

TaskForce's configuration autodetection module will help identifying the type and other parameters of a RAID 10, should there be a lack of information about the given RAID and its configuration.

To mount an unknown RAID 10 and image it:

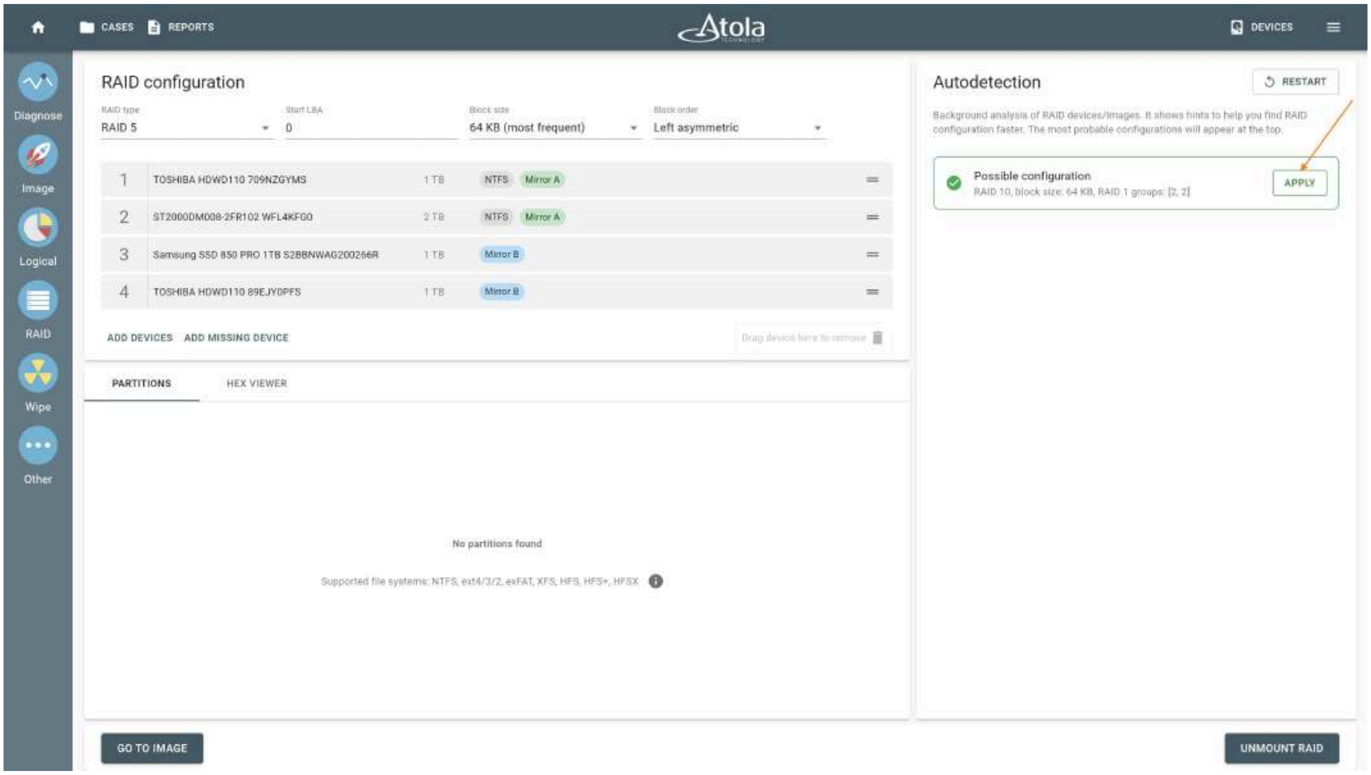
1. On the left in the TaskForce main window, click **RAID**.
2. Select the drives that make up the RAID array and click **Continue**.


RAID > Select source device
☑ Power on all devices
DEVICES
SATA
☑ 1 TOSHIBA HDWD110 709NZGYMS 1 TB source
□ 2 Samsung SSD 860 PRO 2TB S5G7NS0R701562P 2 TB target
☑ 3 Samsung SSD 850 PRO 1TB S2BBNWAG200266R 1 TB source
□ 4 Device not detected source
☑ 5 TOSHIBA HDWD110 89EJY0PFS 1 TB source
☑ 6 ST2000DM008-2FR102 WFL4KFG0 2 TB Case: Not assigned source
□ 7 Device not detected target
□ 8 Device not detected target
SAS
NVME
USB
IDE
EXT
FILE
RAID
CONTINUE
a minute ago
4 days ago

RAID 10. Selecting RAID members.

3. When the autodetection module (in the right part of the screen) comes up with a suggestion of RAID configuration, click **Apply**.

> In rare cases, there can be more than one suggestion. Try them out one by one by clicking **Apply** next to each suggestion.
> If you know the type and parameters of the RAID, you can enter them manually in the drop-downs.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most frequent)
Block order: Left asymmetric

1	TOSHIBA HDWD110 709NZGYMS	1 TB	NTFS Mirror A
2	ST2000DM008-2FR102 WFL4KFG0	2 TB	NTFS Mirror A
3	Samsung SSD 850 PRO 1TB S2BBNWAG200266R	1 TB	Mirror B
4	TOSHIBA HDWD110 89EJY0PFS	1 TB	Mirror B

No partitions found

Supported file systems: NTFS, ext4/3/2, exFAT, XFS, HFS, HFS+, HFSX

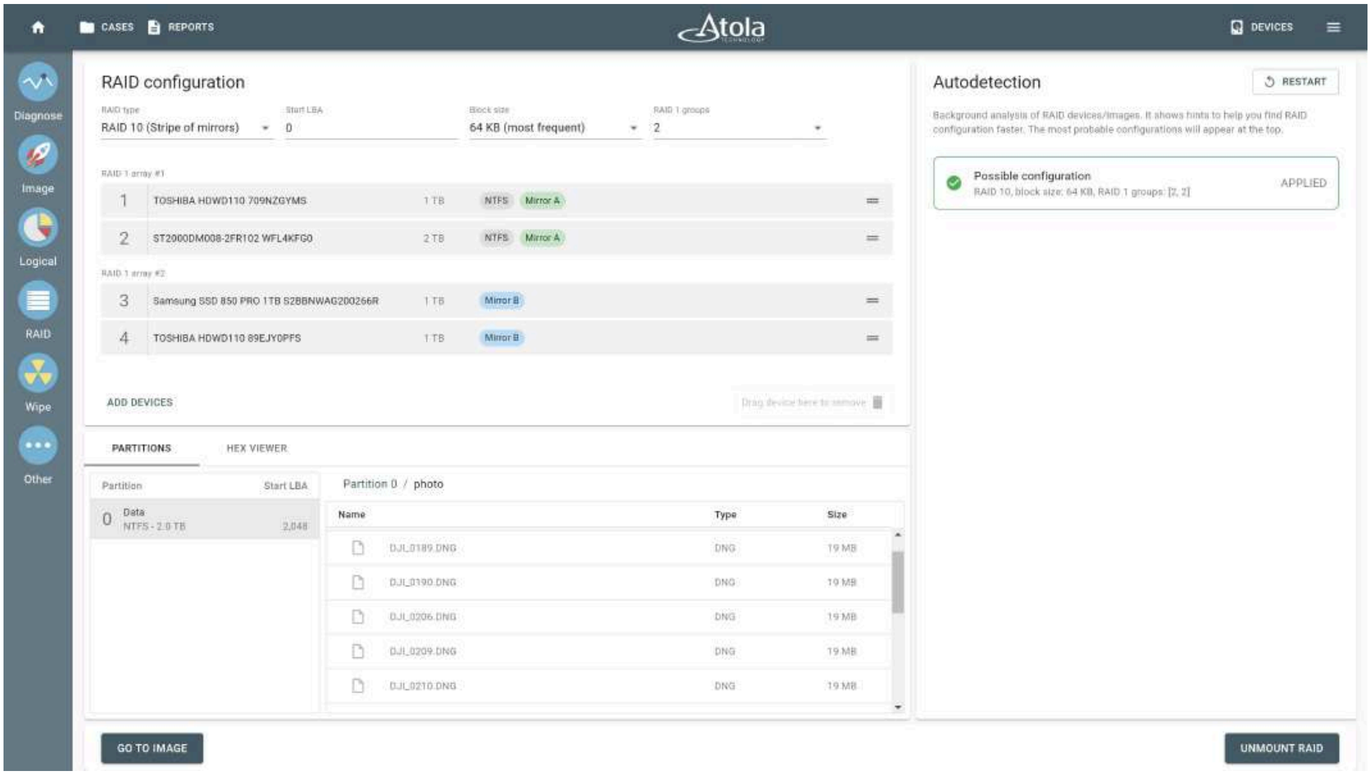
Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Possible configuration
RAID 10, block size: 64 KB, RAID 1 groups: [2, 2]

RAID 10. Applying the detected configuration.

4. TaskForce 2 arranges the drives into respective groups and applies other RAID settings to mount the partitions, which you can browse through in the Partition preview below.



RAID configuration

RAID type: RAID 10 (Stripe of mirrors)
Start LBA: 0
Block size: 64 KB (most frequent)
RAID 1 groups: 2

RAID 1 array #1

1	TOSHIBA HDWD110 709NZGYMS	1 TB	NTFS Mirror A
2	ST2000DM008-2FR102 WFL4KFG0	2 TB	NTFS Mirror A

RAID 1 array #2

3	Samsung SSD 850 PRO 1TB S2BBNWAG200266R	1 TB	Mirror B
4	TOSHIBA HDWD110 89EJY0PFS	1 TB	Mirror B

Partition	Start LBA
0 Data NTFS - 2.0 TB	2,048

Partition 0 / photo

Name	Type	Size
DJI_0189.DNG	DNG	19 MB
DJI_0190.DNG	DNG	19 MB
DJI_0206.DNG	DNG	19 MB
DJI_0209.DNG	DNG	19 MB
DJI_0210.DNG	DNG	19 MB

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Possible configuration
RAID 10, block size: 64 KB, RAID 1 groups: [2, 2]

RAID 10. Previewing the partitions.

5. Click the **Go to image** button and select the target.

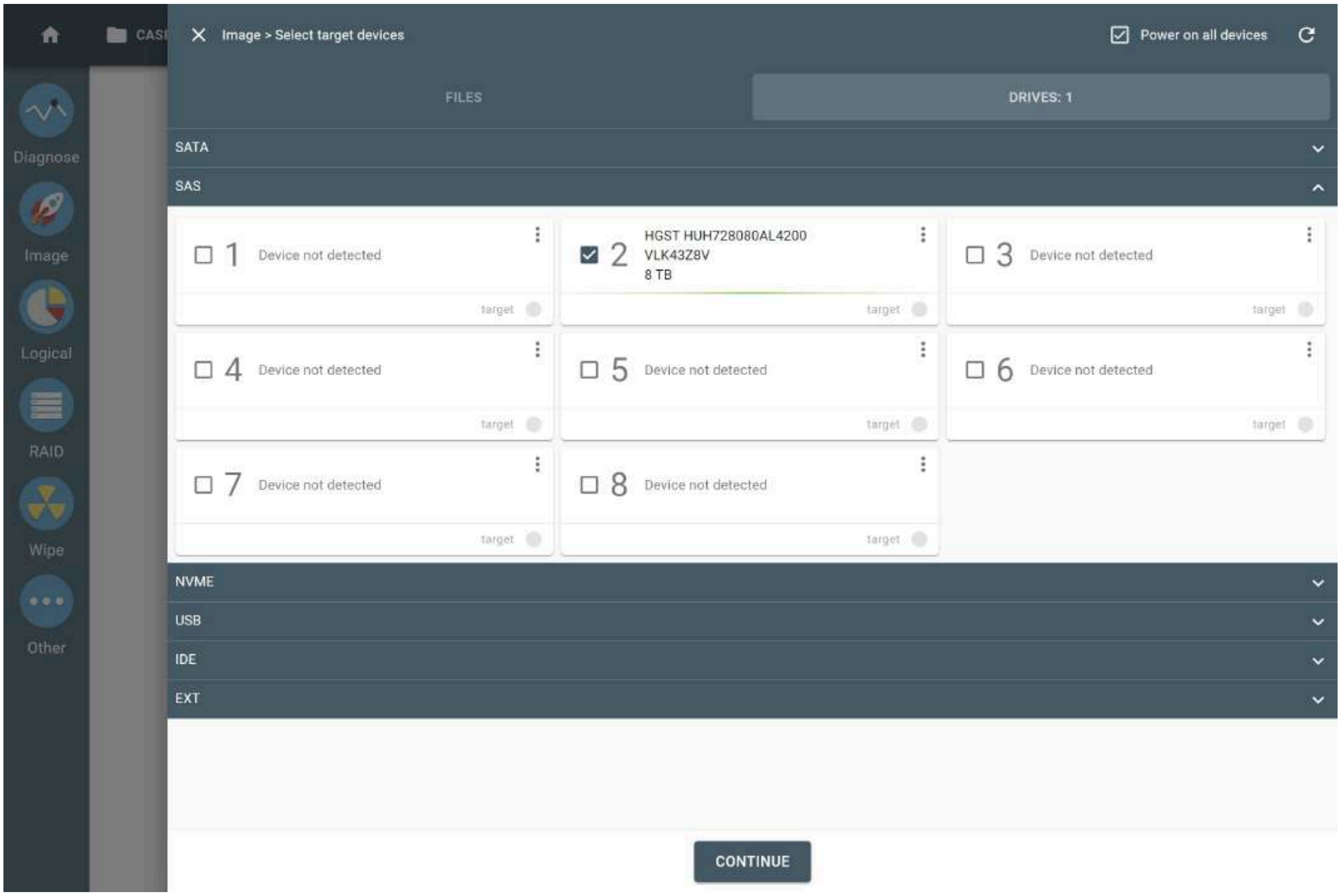


Image > Select target devices

☑ Power on all devices

SAS

□ 1 Device not detected

☑ 2 HGST HUH728080AL4200
VLK43Z8V
8 TB

□ 3 Device not detected

□ 4 Device not detected

□ 5 Device not detected

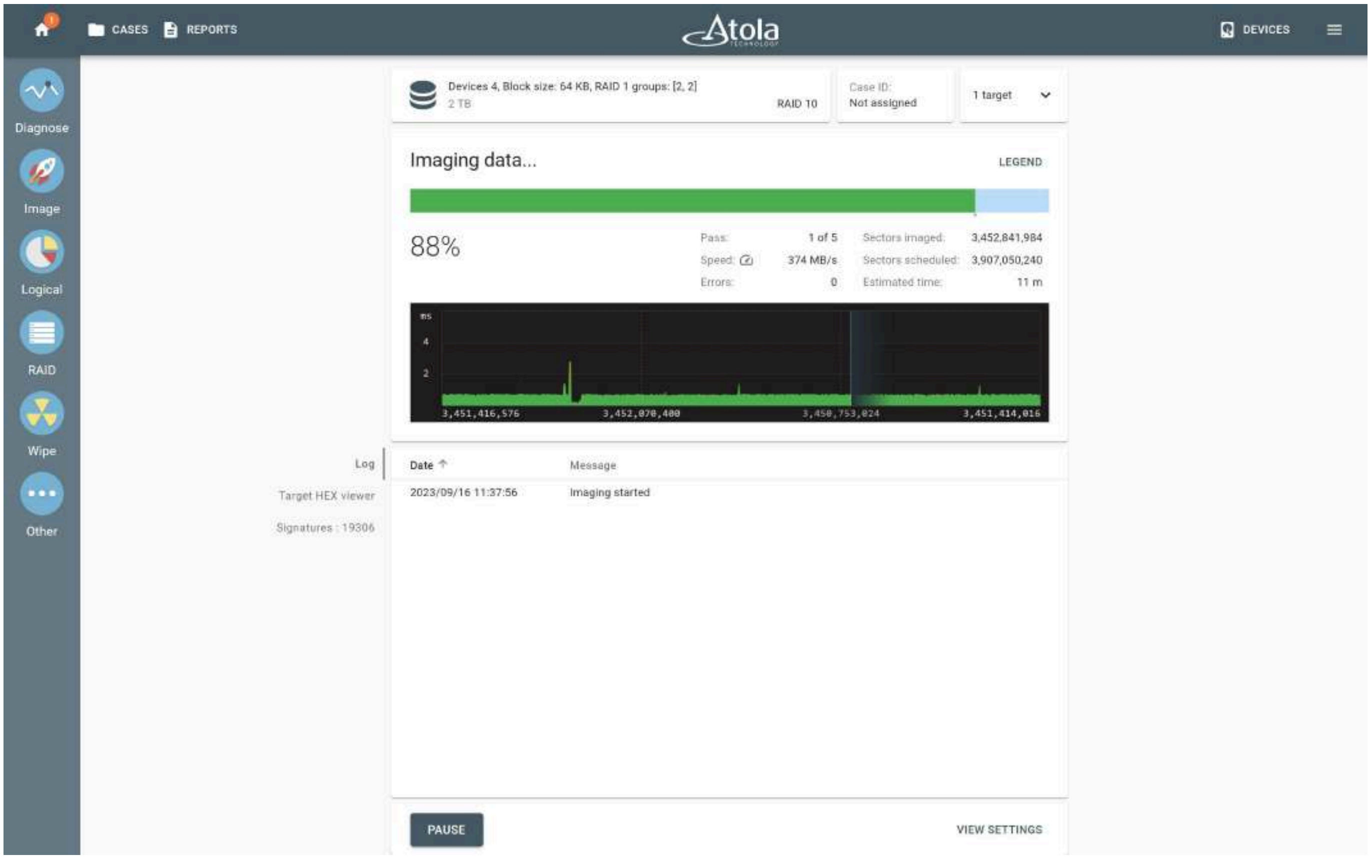
□ 6 Device not detected

□ 7 Device not detected

□ 8 Device not detected

RAID 10. Selecting target.

6. Check the settings. Please note that you can choose to image only part of the data (only one of the partitions).



Devices 4, Block size: 64 KB, RAID 1 groups: [2, 2]
2 TB
RAID 10

Case ID:
Not assigned

1 target

Imaging data...

88%

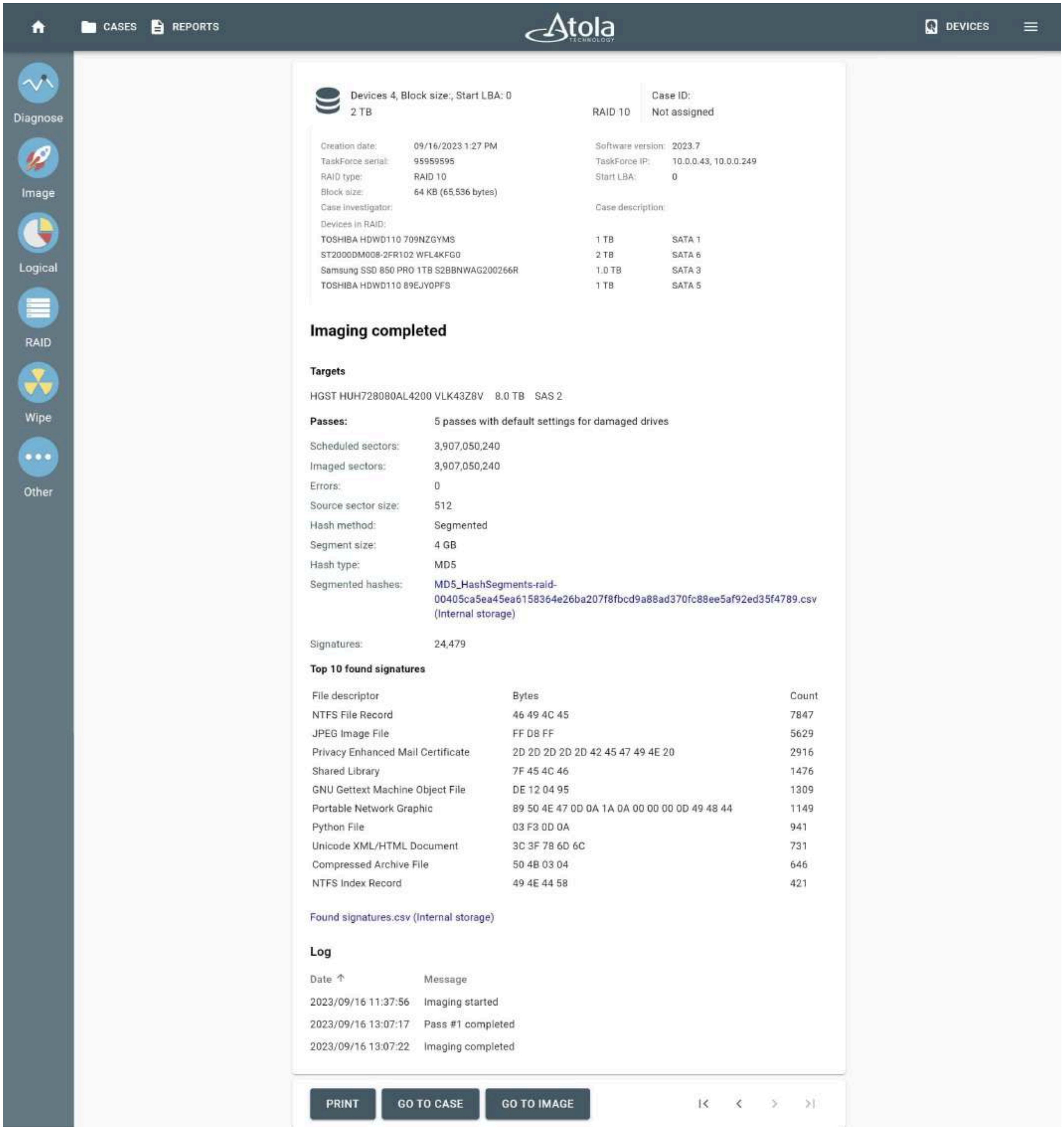
Pass:	1 of 5	Sectors imaged:	3,452,841,984
Speed:	374 MB/s	Sectors scheduled:	3,907,050,240
Errors:	0	Estimated time:	11 m

Signatures : 19306

Date ↑	Message
2023/09/16 11:37:56	Imaging started

RAID 10. Imaging.

7. The automatically generated **Imaging report** contains the details of the RAID and its members, the target, hashes, signatures found as well as the timestamps.



Devices 4, Block size:, Start LBA: 0
2 TB
RAID 10
Case ID:
Not assigned

Creation date:	09/16/2023 1:27 PM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.43, 10.0.0.249
RAID type:	RAID 10	Start LBA:	0
Block size:	64 KB (65,536 bytes)		
Case investigator:		Case description:	

Devices in RAID:

TOSHIBA HDWD110 709NZGYMS	1 TB	SATA 1
ST2000DM008-2FR102 WFL4KFG0	2 TB	SATA 6
Samsung SSD 850 PRO 1TB S2BBNWAG200266R	1.0 TB	SATA 3
TOSHIBA HDWD110 89EJY0PFS	1 TB	SATA 5

Imaging completed

Targets

HGST HUH728080AL4200 VLK43Z8V 8.0 TB SAS 2

Passes:	5 passes with default settings for damaged drives
Scheduled sectors:	3,907,050,240
Imaged sectors:	3,907,050,240
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-raid-00405ca5ea45ea6158364e26ba207f8fbcd9a88ad370fc88ee5af92ed35f4789.csv (Internal storage)
Signatures:	24,479

Top 10 found signatures

File descriptor	Bytes	Count
NTFS File Record	46 49 4C 45	7847
JPEG Image File	FF D8 FF	5629
Privacy Enhanced Mail Certificate	2D 2D 2D 2D 2D 42 45 47 49 4E 20	2916
Shared Library	7F 45 4C 46	1476
GNU Gettext Machine Object File	DE 12 04 95	1309
Portable Network Graphic	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44	1149
Python File	03 F3 0D 0A	941
Unicode XML/HTML Document	3C 3F 78 6D 6C	731
Compressed Archive File	50 4B 03 04	646
NTFS Index Record	49 4E 44 58	421

Found signatures.csv (Internal storage)

Log

Date ↑	Message
2023/09/16 11:37:56	Imaging started
2023/09/16 13:07:17	Pass #1 completed
2023/09/16 13:07:22	Imaging completed

RAID 10. Imaging report.

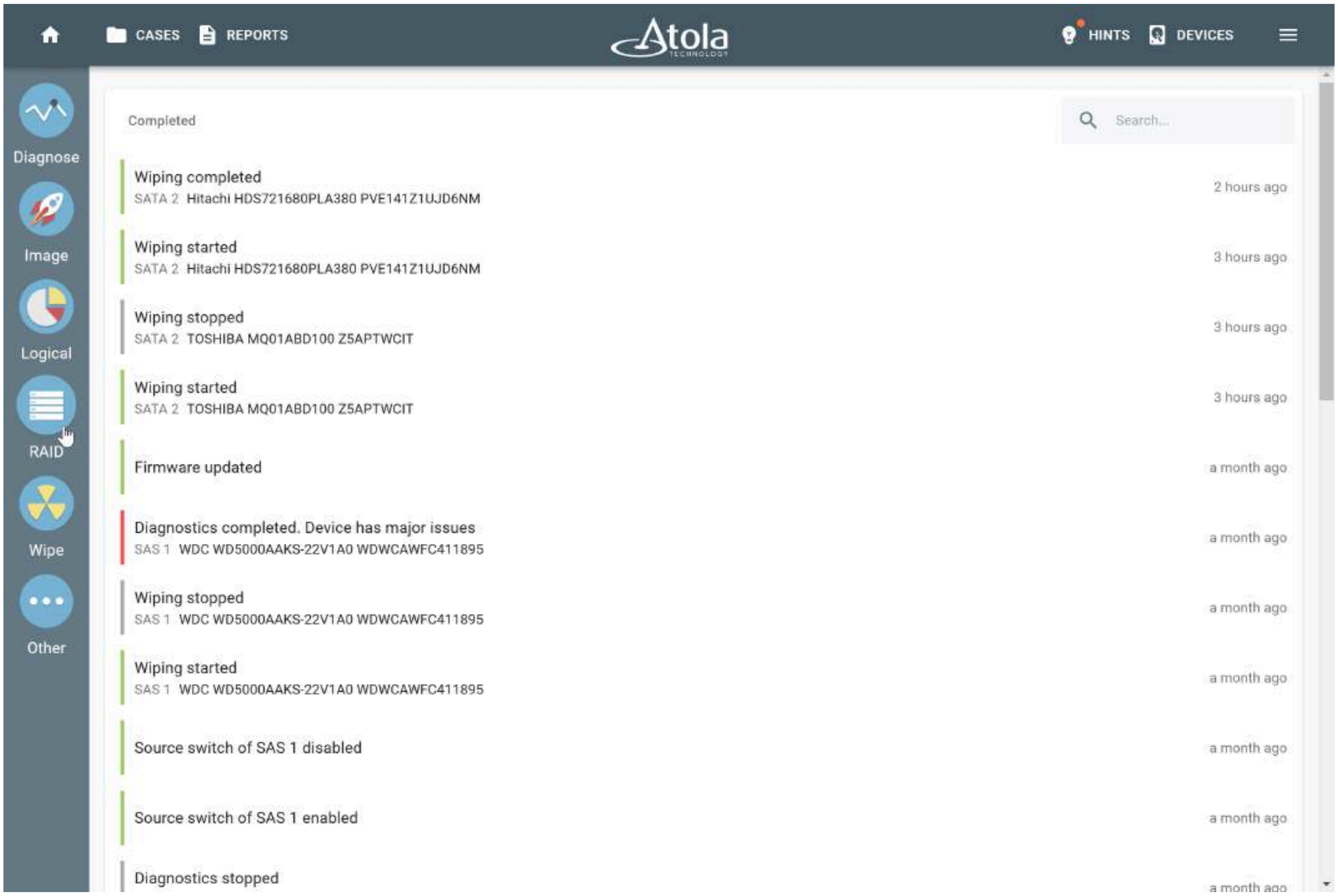
Synology NAS RAID auto reassembly

Synology NAS RAID is a popular network storage solution. It has a complex structure and can include several RAIDs combined via LVM (Logical volume manager) and SHR RAID management system.

Atola TaskForce 2 can automatically detect the configuration of a Synology NAS RAID array and perform immediate forensic RAID reconstruction.

To automatically reassemble and then image a Synology NAS RAID array with an unknown configuration, do the following:

1. On the left in the TaskForce main window, click **RAID**.



Completed

Wiping completed
SATA 2 Hitachi HDS721680PLA380 PVE141Z1UJD6NM
2 hours ago

Wiping started
SATA 2 Hitachi HDS721680PLA380 PVE141Z1UJD6NM
3 hours ago

Wiping stopped
SATA 2 TOSHIBA MQ01ABD100 Z5APTWCIT
3 hours ago

Wiping started
SATA 2 TOSHIBA MQ01ABD100 Z5APTWCIT
3 hours ago

Firmware updated
a month ago

Diagnostics completed. Device has major issues
SAS 1 WDC WD5000AAKS-22V1A0 WDWCAWFC411895
a month ago

Wiping stopped
SAS 1 WDC WD5000AAKS-22V1A0 WDWCAWFC411895
a month ago

Wiping started
SAS 1 WDC WD5000AAKS-22V1A0 WDWCAWFC411895
a month ago

Source switch of SAS 1 disabled
a month ago

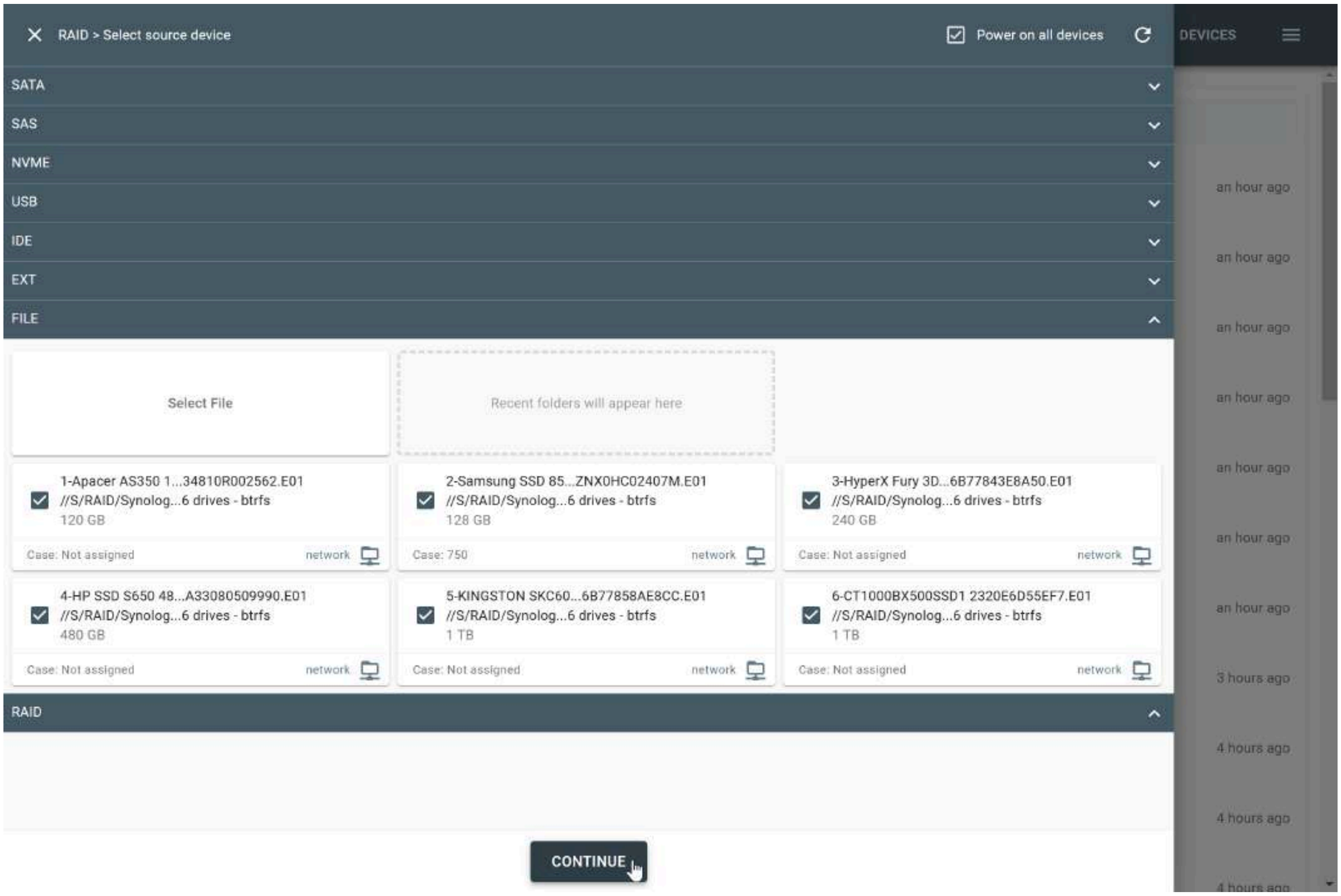
Source switch of SAS 1 enabled
a month ago

Diagnostics stopped
a month ago

Initiating work with RAID.

2. On the **Select source device** panel, select the devices that make up a RAID array.

   They can be physical drives of all supported types, connected to the TaskForce 2 hardware unit, image files (raw, E01 or AFF4 image files), or a combination of both.



☑ 1-Apacer AS350 1...34810R002562.E01
//S/RAID/Synolog...6 drives - btrfs
120 GB
Case: Not assigned network

☑ 2-Samsung SSD 85...ZNX0HC02407M.E01
//S/RAID/Synolog...6 drives - btrfs
128 GB
Case: 750 network

☑ 3-HyperX Fury 3D...6B77843E8A50.E01
//S/RAID/Synolog...6 drives - btrfs
240 GB
Case: Not assigned network

☑ 4-HP SSD S650 48...A33080509990.E01
//S/RAID/Synolog...6 drives - btrfs
480 GB
Case: Not assigned network

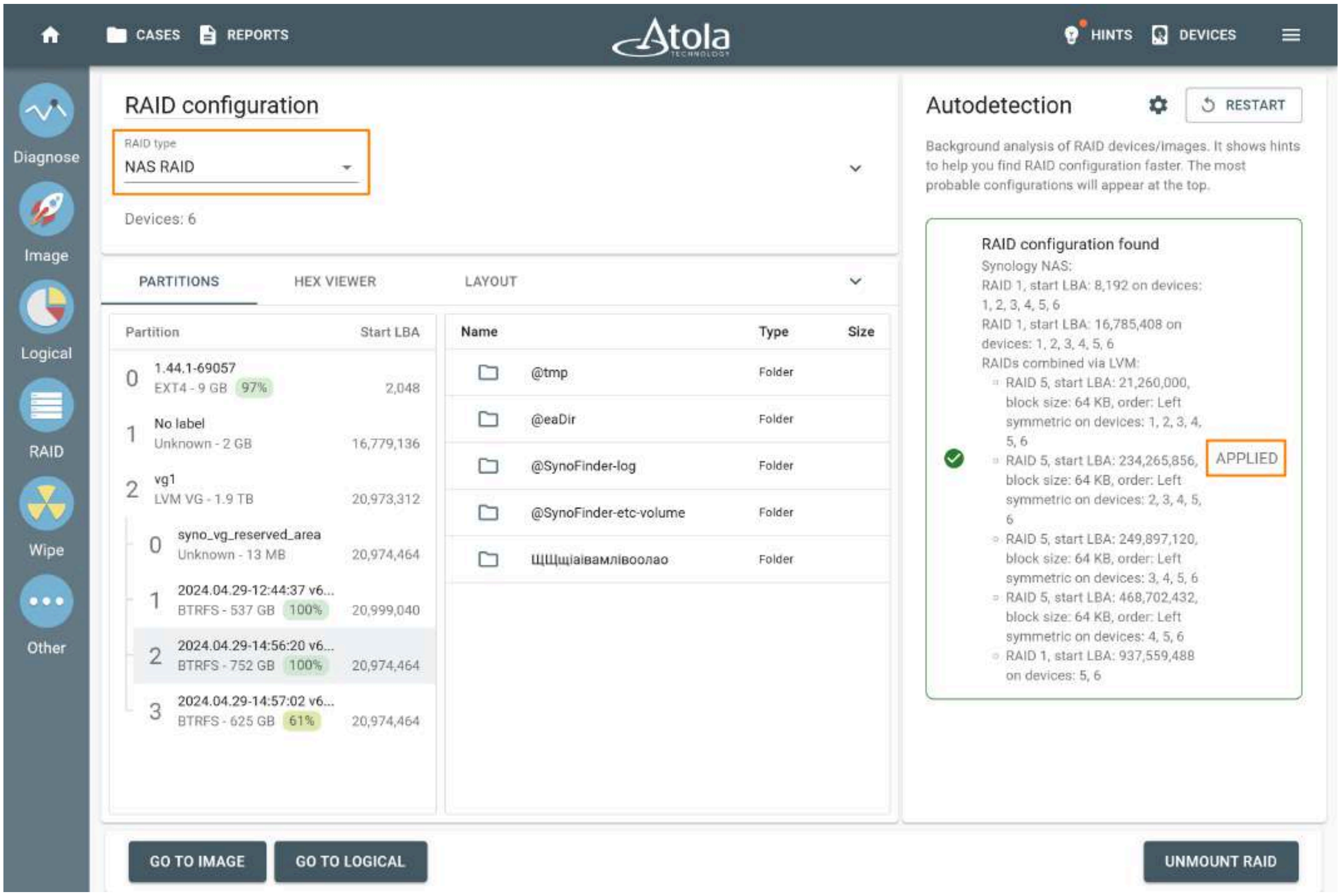
☑ 5-KINGSTON SKC60...6B77858AE8CC.E01
//S/RAID/Synolog...6 drives - btrfs
1 TB
Case: Not assigned network

☑ 6-CT1000BX500SSD1 2320E6D55EF7.E01
//S/RAID/Synolog...6 drives - btrfs
1 TB
Case: Not assigned network

Selecting RAID members.

3. Once all the RAID members are selected, click **Continue**.
4. TaskForce redirects you to the **RAID configuration** screen and immediately starts the **Autodetection** module.

   Despite the complexity of the Synology NAS RAID structure, the autodetection module instantly identifies the array by detecting controller metadata and applies the RAID configuration.



RAID configuration

RAID type: NAS RAID

Devices: 6

Partition		Start LBA
0	1.44.1-69057 EXT4 - 9 GB 97%	2,048
1	No label Unknown - 2 GB	16,779,136
2	vg1 LVM VG - 1.9 TB	20,973,312
0	syno_vg_reserved_area Unknown - 13 MB	20,974,464
1	2024.04.29-12:44:37 v6... BTRFS - 537 GB 100%	20,999,040
2	2024.04.29-14:56:20 v6... BTRFS - 752 GB 100%	20,974,464
3	2024.04.29-14:57:02 v6... BTRFS - 625 GB 61%	20,974,464

Name	Type	Size
@tmp	Folder	
@eaDir	Folder	
@SynoFinder-log	Folder	
@SynoFinder-etc-volume	Folder	
ЩЩщіавамлівоолао	Folder	

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

✓ RAID configuration found

Synology NAS:

RAID 1, start LBA: 8,192 on devices: 1, 2, 3, 4, 5, 6

RAID 1, start LBA: 16,785,408 on devices: 1, 2, 3, 4, 5, 6

RAIDs combined via LVM:

- RAID 5, start LBA: 21,260,000, block size: 64 KB, order: Left symmetric on devices: 1, 2, 3, 4, 5, 6
- RAID 5, start LBA: 234,265,856, block size: 64 KB, order: Left symmetric on devices: 2, 3, 4, 5, 6 APPLIED
- RAID 5, start LBA: 249,897,120, block size: 64 KB, order: Left symmetric on devices: 3, 4, 5, 6
- RAID 5, start LBA: 468,702,432, block size: 64 KB, order: Left symmetric on devices: 4, 5, 6
- RAID 1, start LBA: 937,559,488 on devices: 5, 6

Synology NAS RAID configuration found and applied.

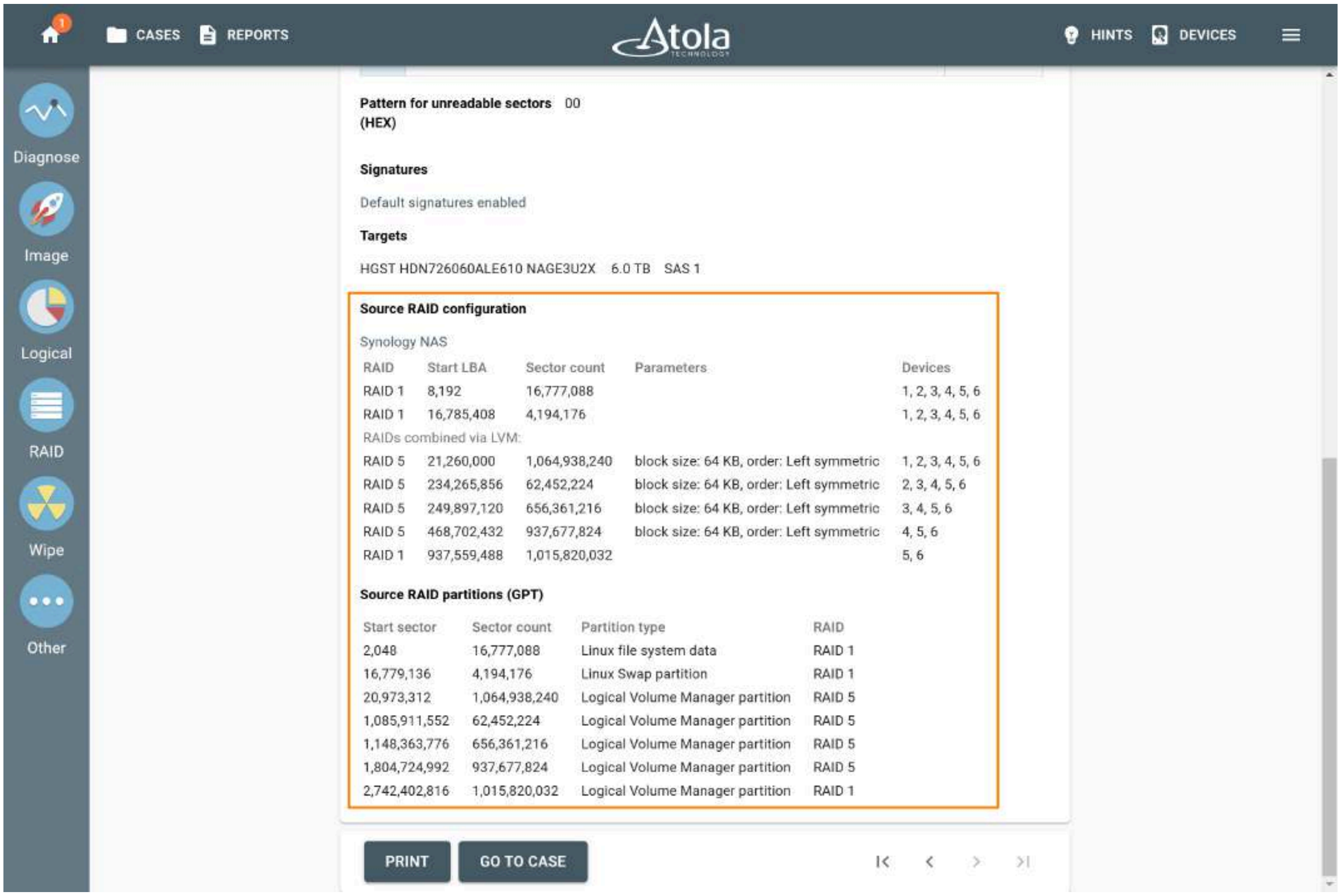
If the Synology NAS RAID configuration wasn't immediately found and the Autodetection process is still running, there are two possible reasons:

a. One or more selected devices aren't part of this Synology NAS RAID array.

b. One or more devices of the array are missing.

In this case, stop the Autodetection module, go back to Step 2 and try selecting different devices that make up a RAID array.

5. Once the RAID configuration is found, proceed with imaging the assembled RAID:
   - Click **Go to image** to acquire a full bit-by-bit copy of the array to E01, AFF4, or raw image.
   - Or click **Go to logical** to copy only selected partitions, folders, or files to L01 or ZIP.
6. At the start of the imaging process, TaskForce creates an **Imaging started** report with detailed information about Synology NAS RAID configuration and partitions.



Pattern for unreadable sectors (HEX) 00

Signatures

Default signatures enabled

Targets

HGST HDN726060ALE610 NAGE3U2X 6.0 TB SAS 1

Source RAID configuration

Synology NAS

RAID	Start LBA	Sector count	Parameters	Devices
RAID 1	8,192	16,777,088		1, 2, 3, 4, 5, 6
RAID 1	16,785,408	4,194,176		1, 2, 3, 4, 5, 6
RAIDs combined via LVM:				
RAID 5	21,260,000	1,064,938,240	block size: 64 KB, order: Left symmetric	1, 2, 3, 4, 5, 6
RAID 5	234,265,856	62,452,224	block size: 64 KB, order: Left symmetric	2, 3, 4, 5, 6
RAID 5	249,897,120	656,361,216	block size: 64 KB, order: Left symmetric	3, 4, 5, 6
RAID 5	468,702,432	937,677,824	block size: 64 KB, order: Left symmetric	4, 5, 6
RAID 1	937,559,488	1,015,820,032		5, 6

Source RAID partitions (GPT)

Start sector	Sector count	Partition type	RAID
2,048	16,777,088	Linux file system data	RAID 1
16,779,136	4,194,176	Linux Swap partition	RAID 1
20,973,312	1,064,938,240	Logical Volume Manager partition	RAID 5
1,085,911,552	62,452,224	Logical Volume Manager partition	RAID 5
1,148,363,776	656,361,216	Logical Volume Manager partition	RAID 5
1,804,724,992	937,677,824	Logical Volume Manager partition	RAID 5
2,742,402,816	1,015,820,032	Logical Volume Manager partition	RAID 1

The 'Imaging started' report.

7. After the imaging is finished, TaskForce generates an **Imaging completed** report. It includes all the details of the source devices in a RAID, the target(s), the number of imaged sectors, the timestamps and more.

Instant forensic RAID reconstruction: Linux mdadm

Atola TaskForce 2 can automatically detect configuration of software RAID created with mdadm in Linux and perform immediate forensic RAID reconstruction.

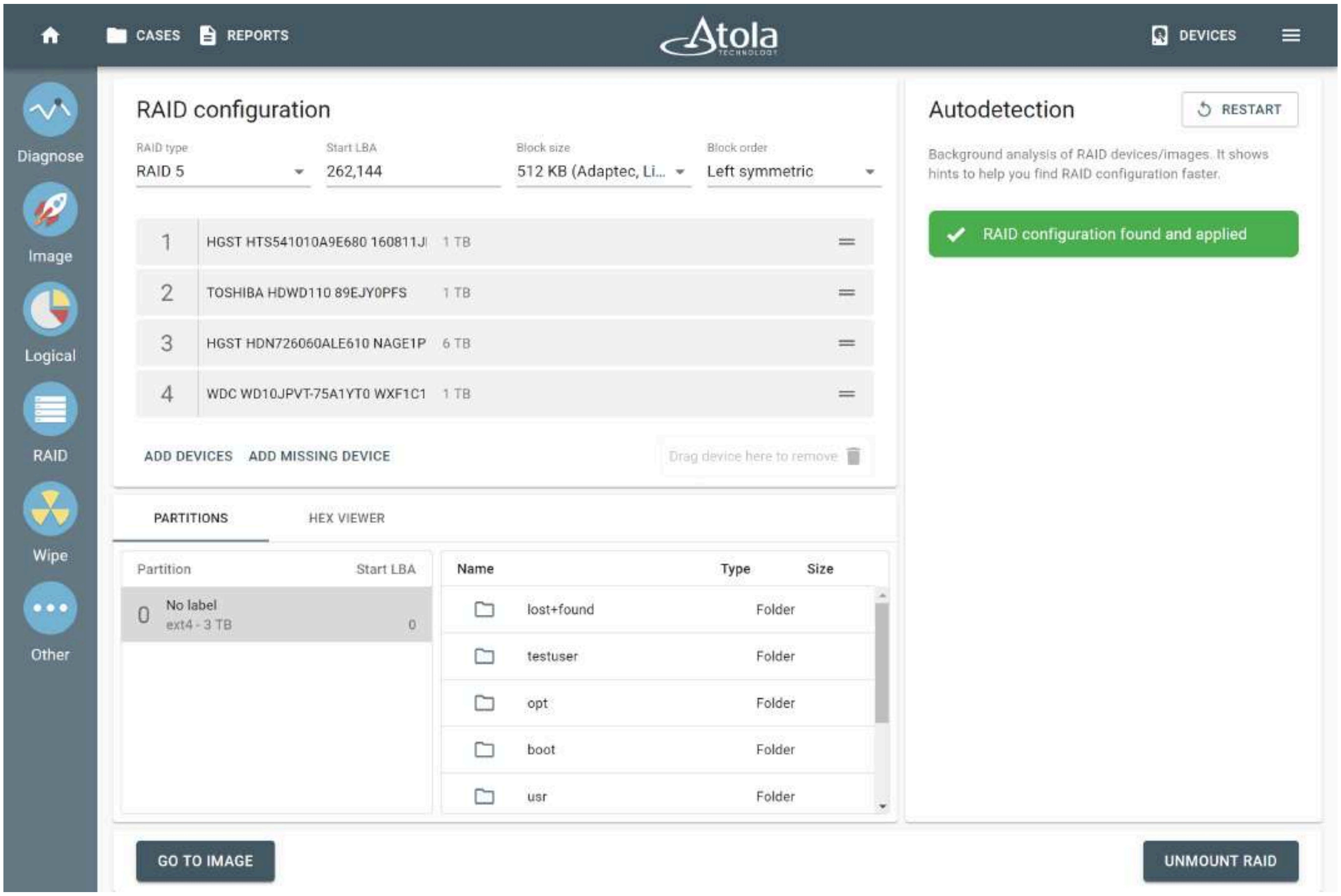
Autodetection of the mdadm-created software RAID

1. Connect the drives to ports in Source mode.
2. On the left in the TaskForce main window, click **RAID**.
3. Select the drives that make up a RAID array and click **Continue**.

Autodetection module has instantly recognized and applied the RAID configuration. TaskForce 2 automatically identifies mdadm-created RAID arrays with great precision by detecting controller metadata.

This RAID’s Start LBA is different from 0. TaskForce’s autodetection module is trained to detect this parameter for different types of RAID arrays and mdadm versions.

A partition is displayed in the bottom part of the screen, confirming that the applied configuration is correct.



RAID configuration

RAID type: RAID 5

Start LBA: 262,144

Block size: 512 KB (Adaptec, Li...

Block order: Left symmetric

1	HGST HTS541010A9E680 160811J	1 TB
2	TOSHIBA HDWD110 89EJY0PFS	1 TB
3	HGST HDN726060ALE610 NAGE1P	6 TB
4	WDC WD10JPVT-75A1YT0 WXF1C1	1 TB

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster.

✓ RAID configuration found and applied

Partition	Start LBA
0 No label ext4 - 3 TB	0

Name	Type	Size
lost+found	Folder	
testuser	Folder	
opt	Folder	
boot	Folder	
usr	Folder	

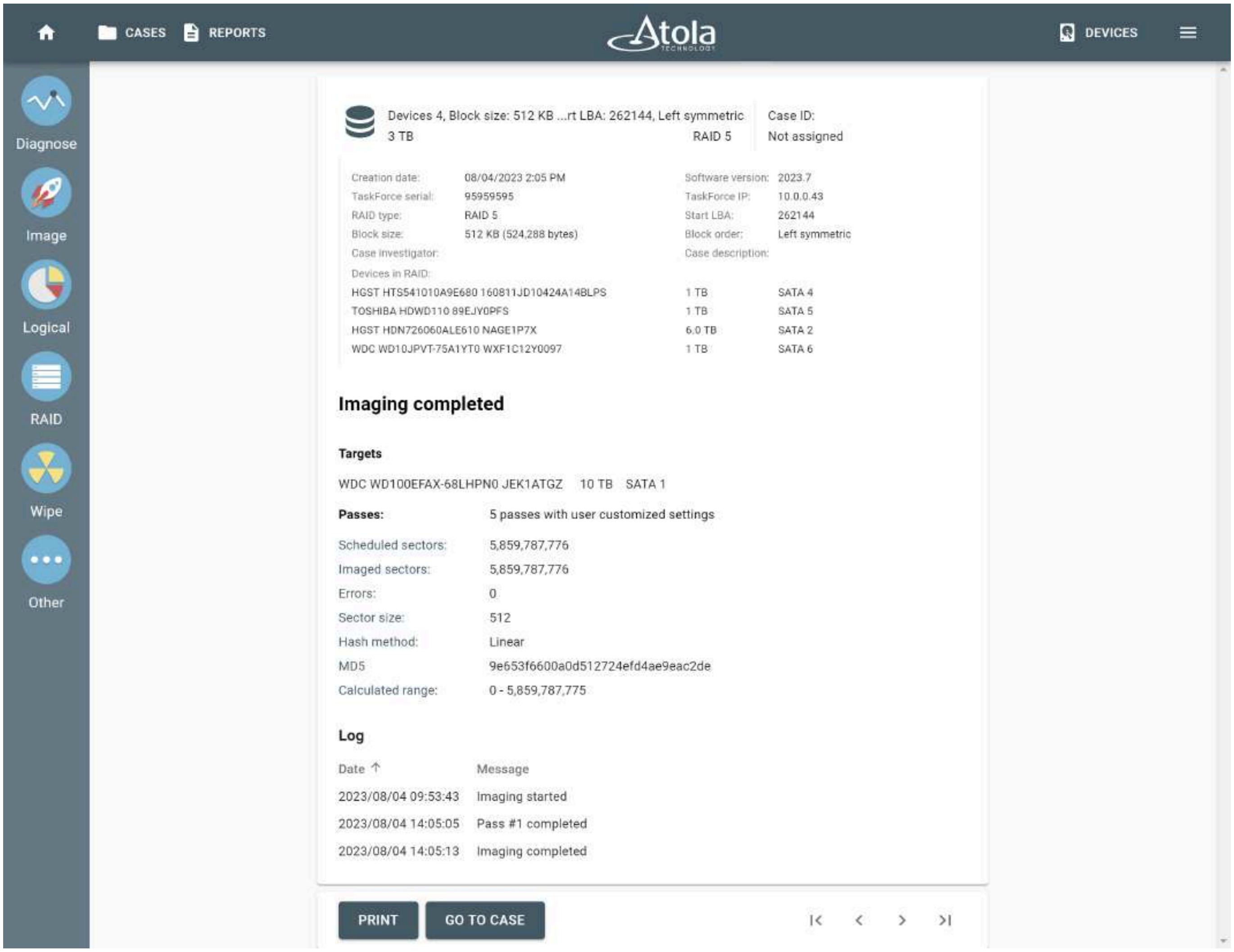
Forensic RAID reconstruction.

Imaging the mdadm-created RAID array

1. To proceed with imaging the assembled RAID, click the **Go to image** button.
2. Select the target and click **Continue**.
3. Click **Start** and confirm the overwriting of data on the target.

The imaging session runs as fast as the target speed allows.

The imaging report contains all the RAID details and timestamps.



Devices 4, Block size: 512 KB ...rt LBA: 262144, Left symmetric
3 TB RAID 5

Case ID:
Not assigned

Creation date:	08/04/2023 2:05 PM	Software version:	2023.7
TaskForce serial:	95959595	TaskForce IP:	10.0.0.43
RAID type:	RAID 5	Start LBA:	262144
Block size:	512 KB (524,288 bytes)	Block order:	Left symmetric
Case investigator:		Case description:	

Devices in RAID:

HGST HTS541010A9E680 160811JD10424A14BLPS	1 TB	SATA 4
TOSHIBA HDWD110 89EJY0PFS	1 TB	SATA 5
HGST HDN726060ALE610 NAGE1P7X	6.0 TB	SATA 2
WDC WD10JPVT-75A1YT0 WXF1C12Y0097	1 TB	SATA 6

Imaging completed

Targets

WDC WD100EFAX-68LHPN0 JEK1ATGZ 10 TB SATA 1

Passes:	5 passes with user customized settings
Scheduled sectors:	5,859,787,776
Imaged sectors:	5,859,787,776
Errors:	0
Sector size:	512
Hash method:	Linear
MD5	9e653f6600a0d512724efd4ae9eac2de
Calculated range:	0 - 5,859,787,775

Log

Date ↑	Message
2023/08/04 09:53:43	Imaging started
2023/08/04 14:05:05	Pass #1 completed
2023/08/04 14:05:13	Imaging completed

Imaging report for an mdadm-created RAID.

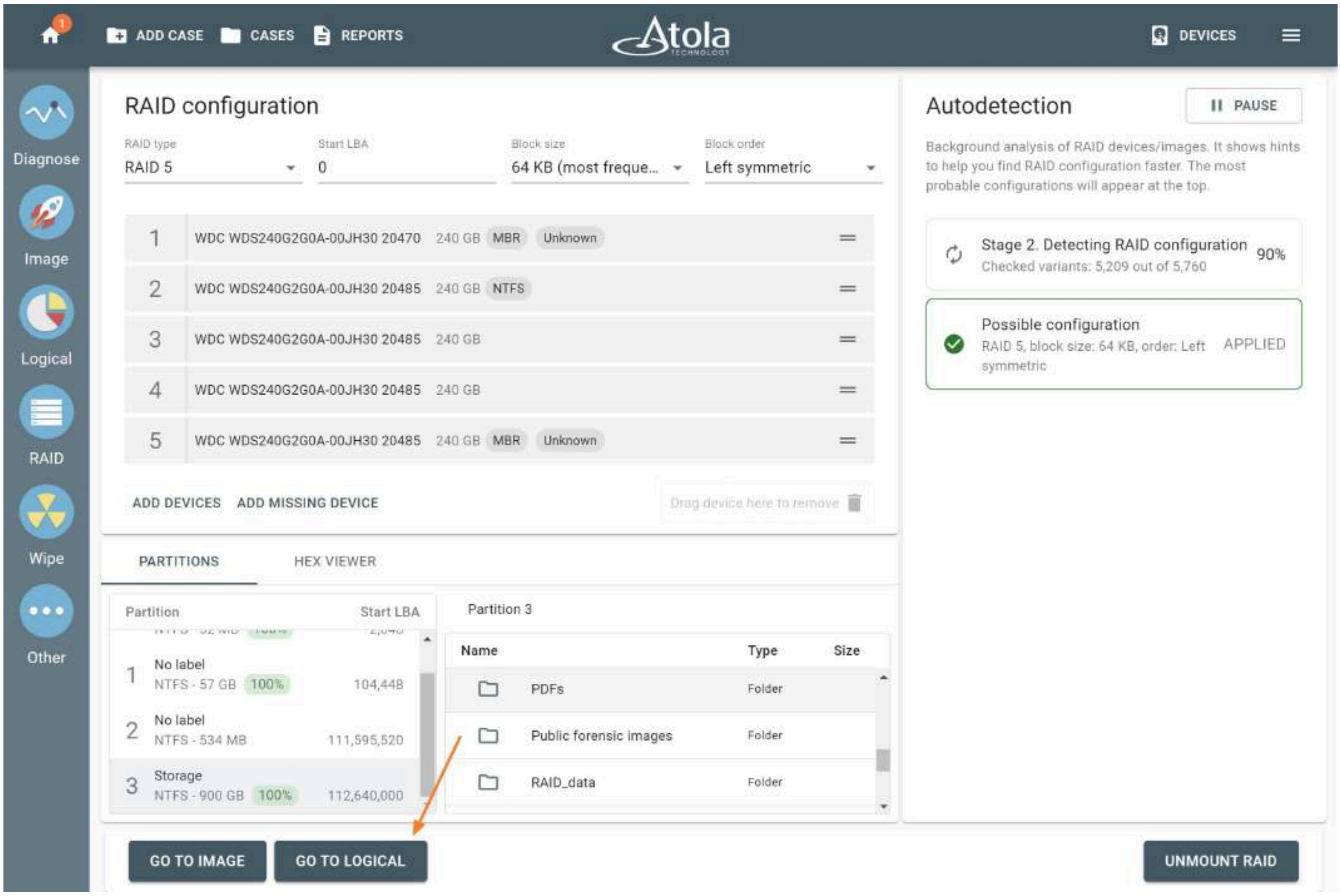
Logical imaging of a RAID array

Imaging of a RAID can potentially take too long. When you are under time constrains, TaskForce's logical imaging module helps you focus on imaging only the data that can make an immediate impact.

Once a RAID has been reassembled, you have a preview of the RAID's contents in the RAID module. This helps you decide which files or folders you want to image immediately.

Create logical image of a RAID array

1. On the **RAID Configuration** page, click the **Go to logical** button.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left symmetric

1	WDC WDS240G2G0A-00JH30 20470	240 GB	MBR	Unknown
2	WDC WDS240G2G0A-00JH30 20485	240 GB	NTFS	
3	WDC WDS240G2G0A-00JH30 20485	240 GB		
4	WDC WDS240G2G0A-00JH30 20485	240 GB		
5	WDC WDS240G2G0A-00JH30 20485	240 GB	MBR	Unknown

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 2. Detecting RAID configuration 90%
Checked variants: 5,209 out of 5,760

Possible configuration
RAID 5, block size: 64 KB, order: Left symmetric APPLIED

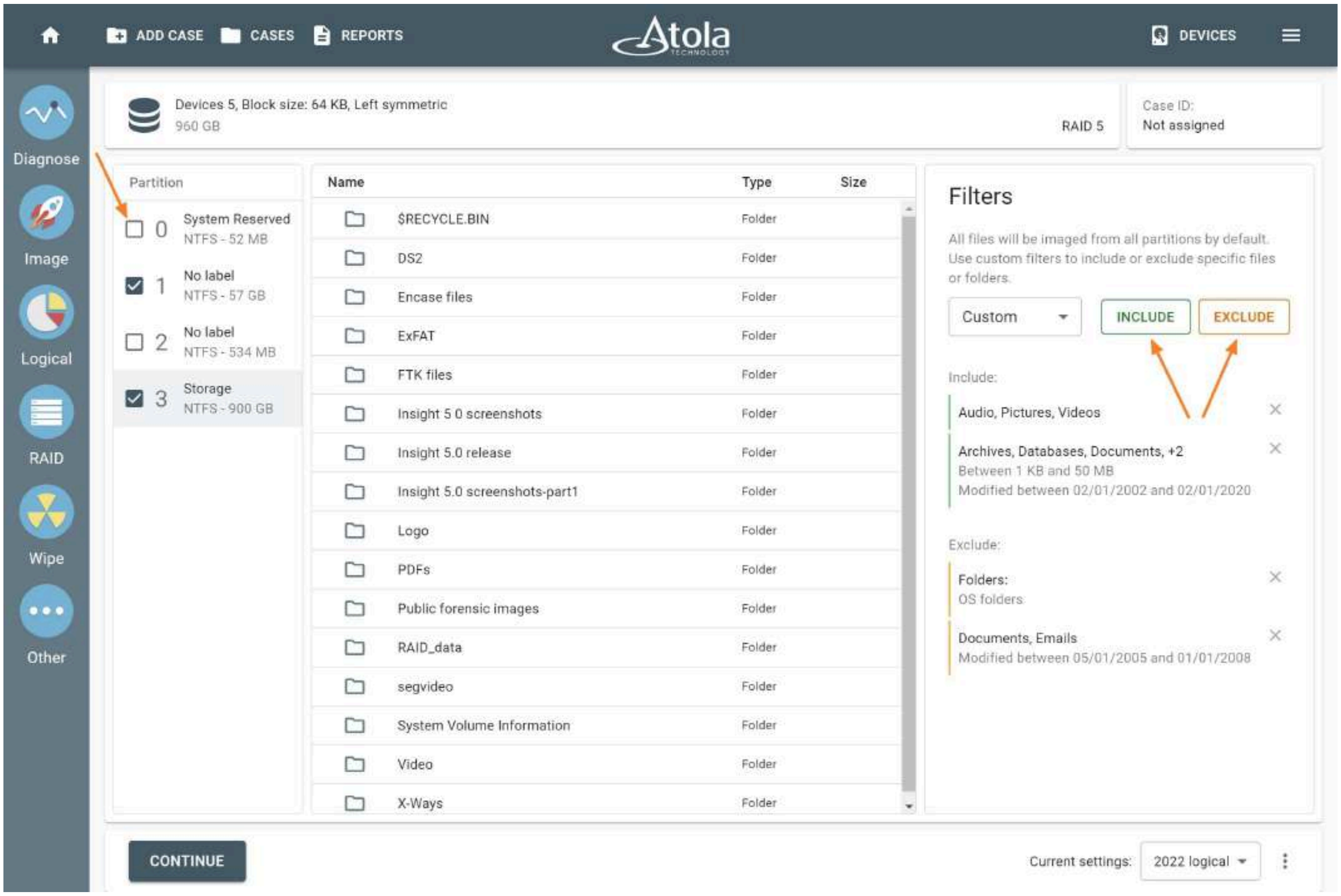
Partition	Start LBA
1 No label NTFS - 57 GB 100%	104,448
2 No label NTFS - 534 MB	111,595,520
3 Storage NTFS - 900 GB 100%	112,640,000

Partition 3

Name	Type	Size
PDFs	Folder	
Public forensic images	Folder	
RAID_data	Folder	

The suggested RAID configuration applied, partitions preview shows partitions.

2. In the **Logical imaging** module, adjust your selection if needed.



Devices 5, Block size: 64 KB, Left symmetric
960 GB
RAID 5

Case ID:
Not assigned

Partition		
□	0	System Reserved NTFS - 52 MB
☑	1	No label NTFS - 57 GB
□	2	No label NTFS - 534 MB
☑	3	Storage NTFS - 900 GB

Name	Type	Size
$RECYCLE.BIN	Folder	
DS2	Folder	
Encase files	Folder	
ExFAT	Folder	
FTK files	Folder	
Insight 5 0 screenshots	Folder	
Insight 5.0 release	Folder	
Insight 5.0 screenshots-part1	Folder	
Logo	Folder	
PDFs	Folder	
Public forensic images	Folder	
RAID_data	Folder	
segvideo	Folder	
System Volume Information	Folder	
Video	Folder	
X-Ways	Folder	

Filters

All files will be imaged from all partitions by default. Use custom filters to include or exclude specific files or folders.

Custom

Include:

Audio, Pictures, Videos ×

Archives, Databases, Documents, +2 ×
Between 1 KB and 50 MB
Modified between 02/01/2002 and 02/01/2020

Exclude:

Folders: ×
OS folders

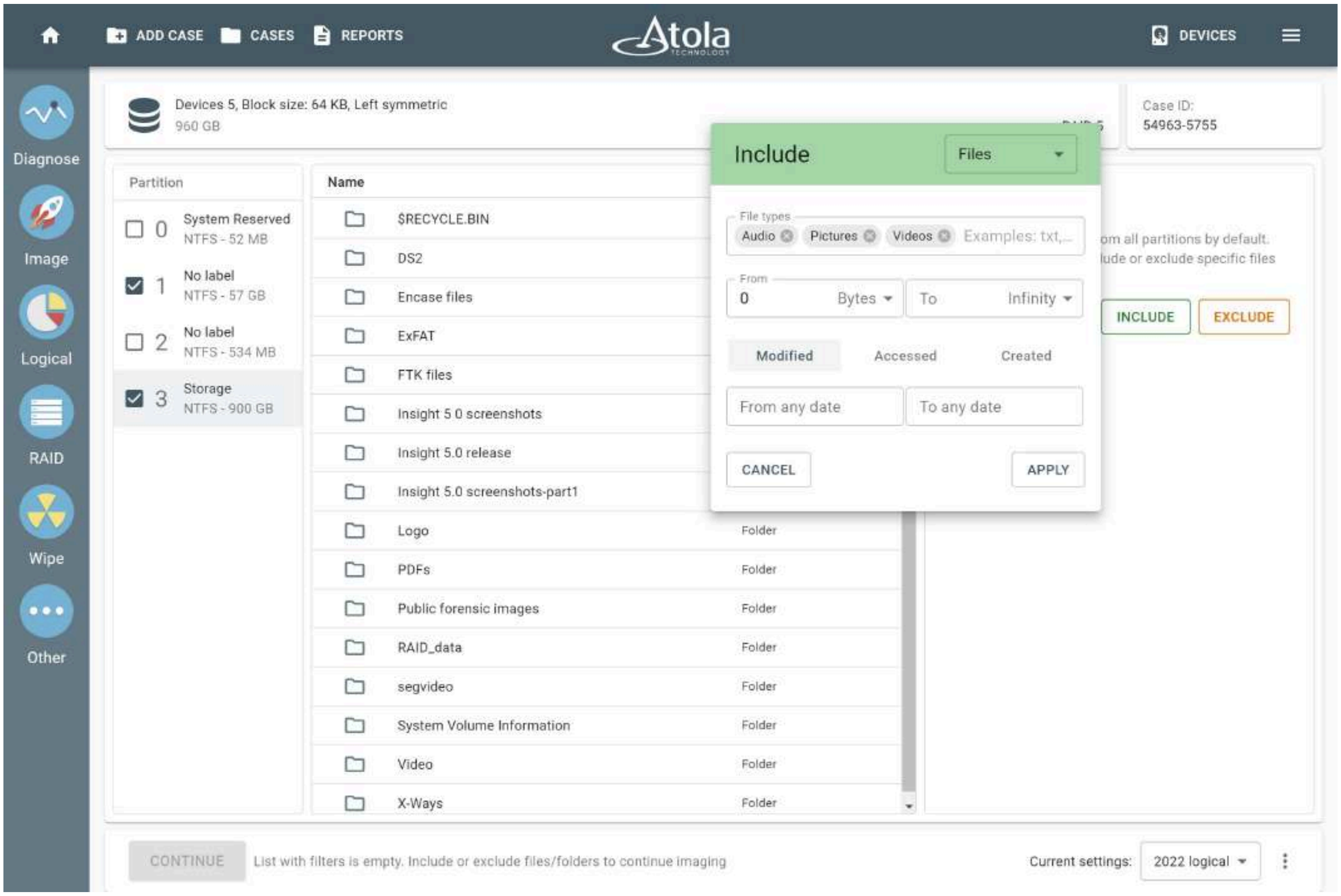
Documents, Emails ×
Modified between 05/01/2005 and 01/01/2008

Current settings: 2022 logical

Specify the partitions, files and folders to included or excluded in the imaging.

By default, logical imaging is set to image all files from a drive or a RAID. To fine-tune your selection, include or exclude what you need:

- All or selected partitions.
- Manually selected files or folders.
- Specified file types: archives, emails, documents, databases, financial, virtual machine, audio, video, pictures, security keys.
- Folder types: only user or only OS folders.
- Time spans: when files were accessed, created, modified.
- File size: from 1 byte to infinity.



Devices 5, Block size: 64 KB, Left symmetric
960 GB

Case ID:
54963-5755

Partition	
□ 0	System Reserved NTFS - 52 MB
☑ 1	No label NTFS - 57 GB
□ 2	No label NTFS - 534 MB
☑ 3	Storage NTFS - 900 GB

Name	
$RECYCLE.BIN	
DS2	
Encase files	
ExFAT	
FTK files	
Insight 5 0 screenshots	
Insight 5.0 release	
Insight 5.0 screenshots-part1	
Logo	Folder
PDFs	Folder
Public forensic images	Folder
RAID_data	Folder
segvideo	Folder
System Volume Information	Folder
Video	Folder
X-Ways	Folder

Include — Files

File types: Audio ⊗ Pictures ⊗ Videos ⊗ Examples: txt,...

From: 0 Bytes — To Infinity

Modified | Accessed | Created

From any date — To any date

CANCEL — APPLY

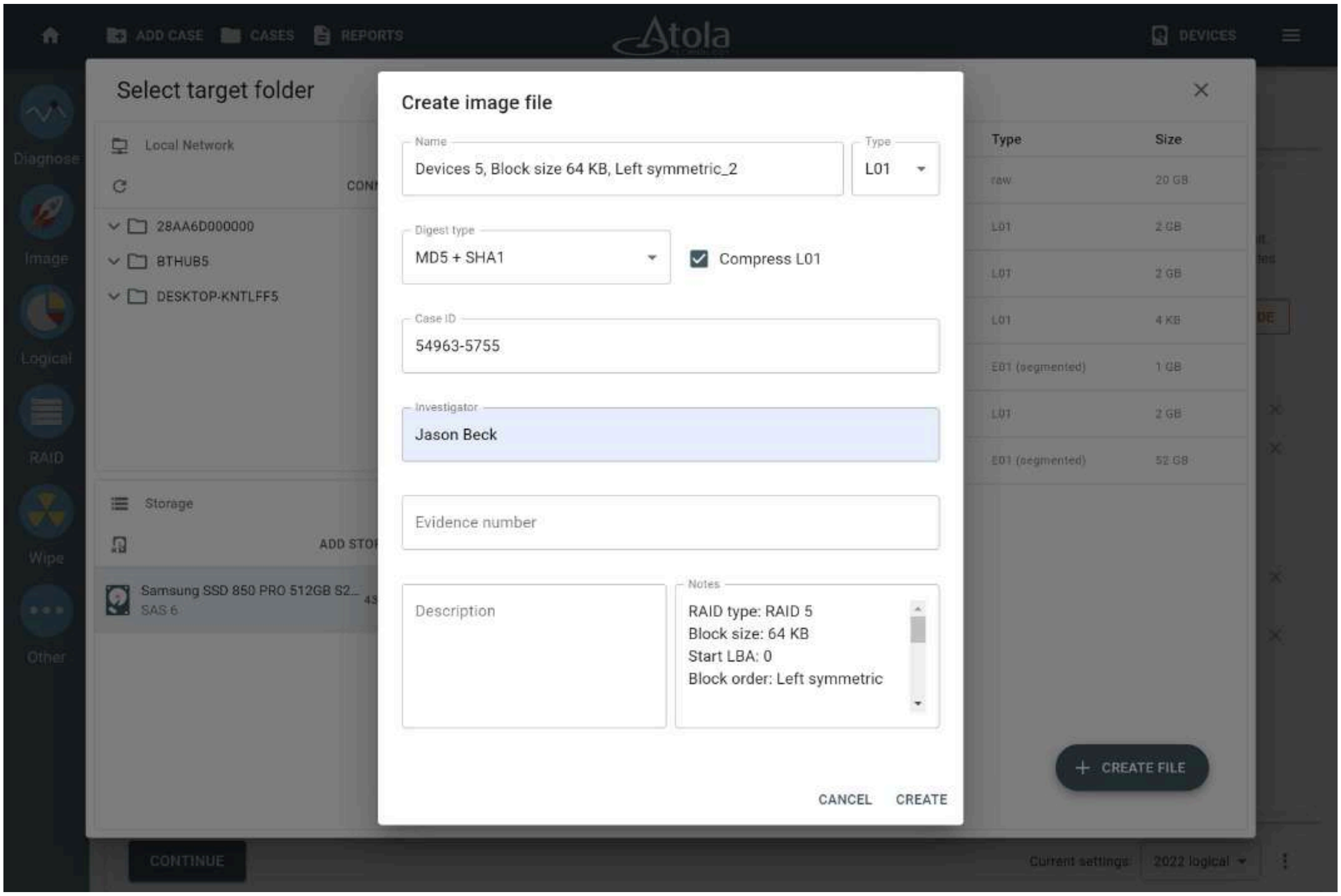
...om all partitions by default.
...lude or exclude specific files

List with filters is empty. Include or exclude files/folders to continue imaging

Current settings: 2022 logical

Multiple search parameters allow you to fine-tune your selection.

3. Once you have adjusted the logical imaging parameters, click **Continue**.
4. Select the Target for your L01 file and click **Create file**.
5. Adjust the settings of the L01 file and click **Create** to start the imaging session.



Create image file

Name: Devices 5, Block size 64 KB, Left symmetric_2

Type: L01

Digest type: MD5 + SHA1

☑ Compress L01

Case ID: 54963-5755

Investigator: Jason Beck

Evidence number

Description

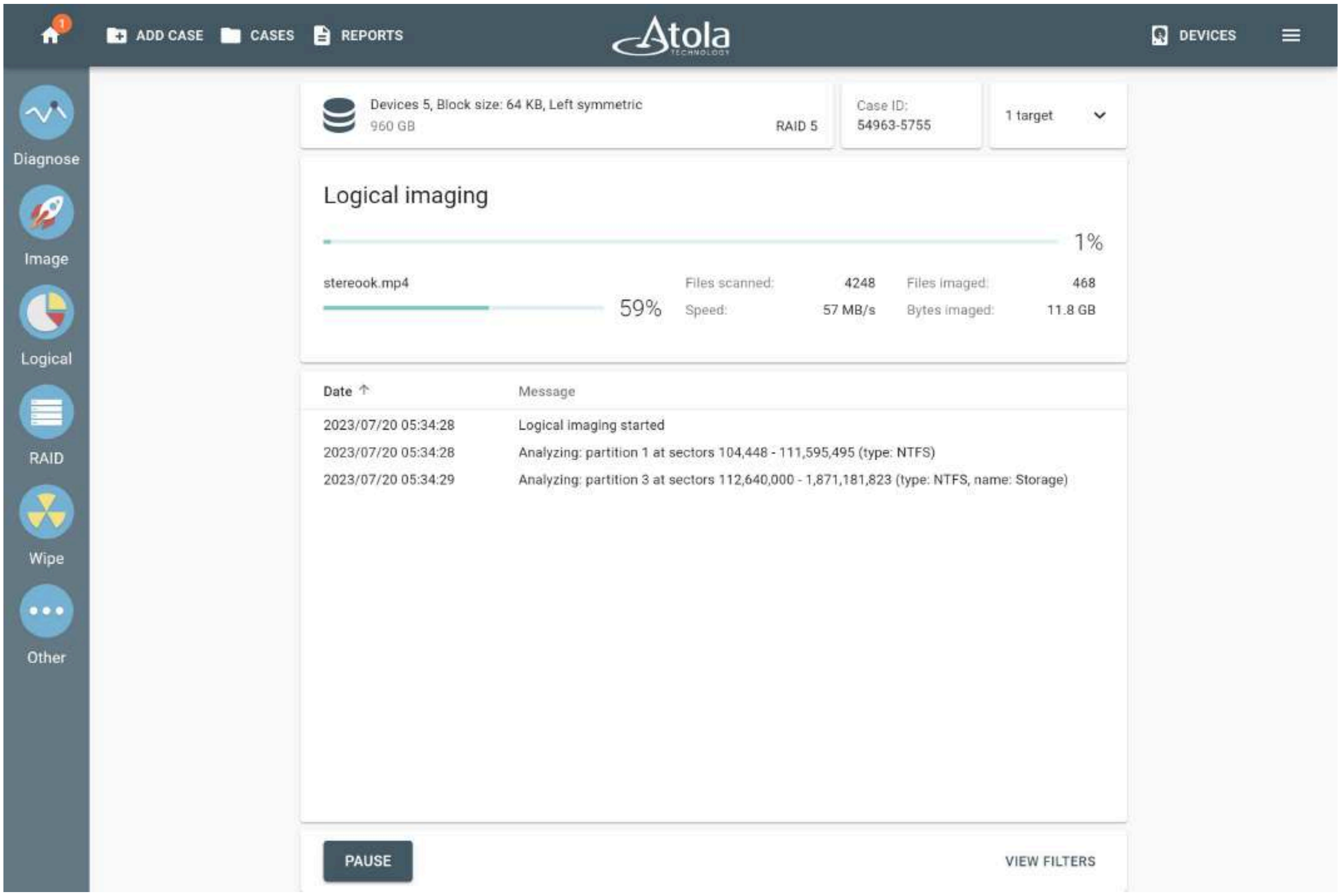
Notes:
RAID type: RAID 5
Block size: 64 KB
Start LBA: 0
Block order: Left symmetric

CANCEL CREATE

Type	Size
raw	20 GB
L01	2 GB
L01	2 GB
L01	4 KB
E01 (segmented)	1 GB
L01	2 GB
E01 (segmented)	52 GB

Settings of an L01 file.

When the imaging is running, you can track the progress of imaging of the individual files. As for the overall imaging progress, the upper graph indicates the amount of imaged data as related to the whole space of the RAID volume, not to the selected volume.



Devices 5, Block size: 64 KB, Left symmetric
960 GB
RAID 5

Case ID:
54963-5755

1 target

Logical imaging

1%

stereook.mp4 59%

Files scanned: 4248
Files imaged: 468
Speed: 57 MB/s
Bytes imaged: 11.8 GB

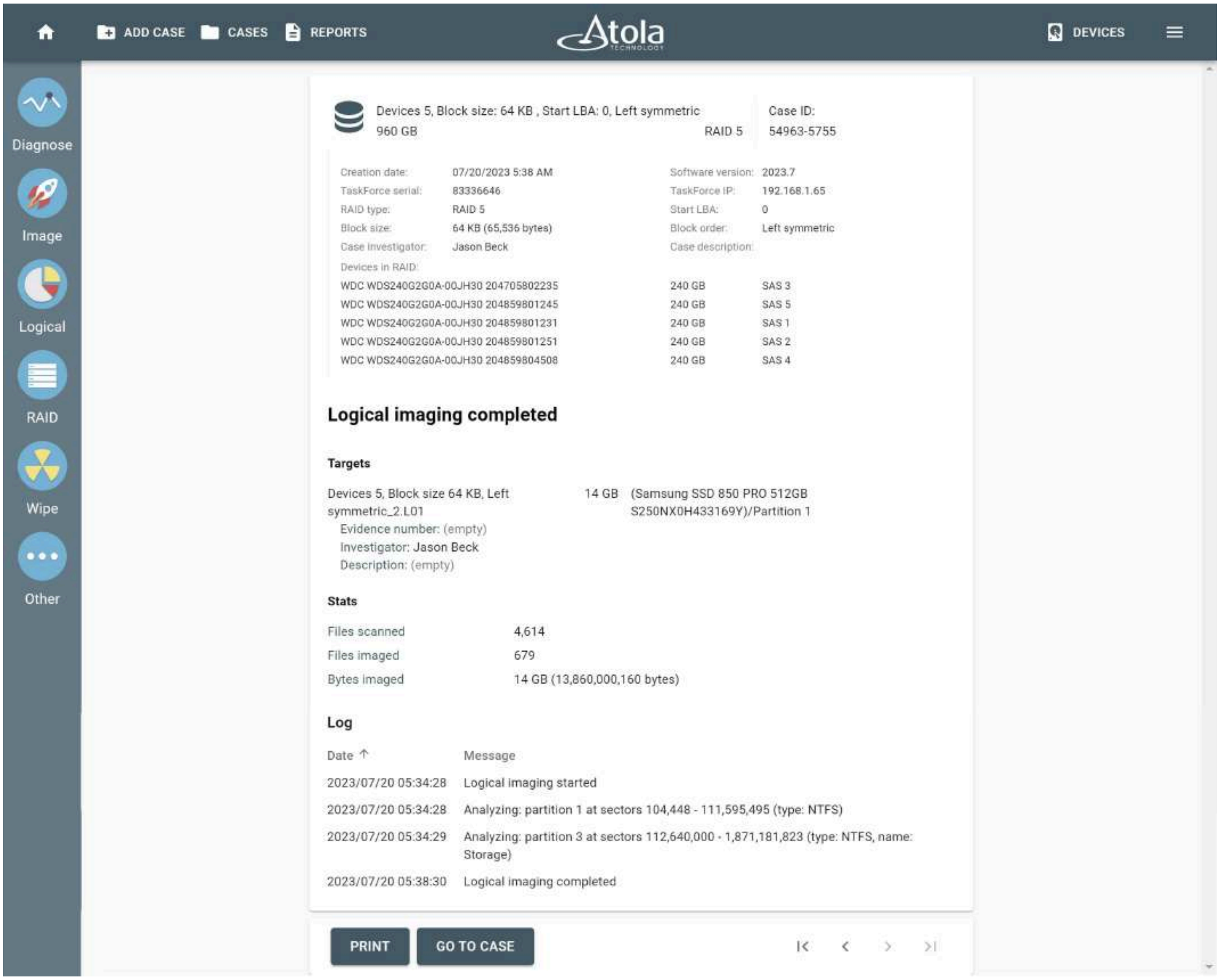
Date ↑	Message
2023/07/20 05:34:28	Logical imaging started
2023/07/20 05:34:28	Analyzing: partition 1 at sectors 104,448 - 111,595,495 (type: NTFS)
2023/07/20 05:34:29	Analyzing: partition 3 at sectors 112,640,000 - 1,871,181,823 (type: NTFS, name: Storage)

Logical imaging of a RAID array.

Imaging report

TaskForce 2 generates the **Imaging completed** report with all the details of the imaged selection from this RAID:

- The number of scanned and imaged files
- The volume of imaged data
- Time stamps



Devices 5, Block size: 64 KB , Start LBA: 0, Left symmetric
960 GB
RAID 5
Case ID:
54963-5755

Creation date:	07/20/2023 5:38 AM	Software version:	2023.7
TaskForce serial:	83336646	TaskForce IP:	192.168.1.65
RAID type:	RAID 5	Start LBA:	0
Block size:	64 KB (65,536 bytes)	Block order:	Left symmetric
Case investigator:	Jason Beck	Case description:	

Devices in RAID:

WDC WDS240G2G0A-00JH30 204705802235	240 GB	SAS 3
WDC WDS240G2G0A-00JH30 204859801245	240 GB	SAS 5
WDC WDS240G2G0A-00JH30 204859801231	240 GB	SAS 1
WDC WDS240G2G0A-00JH30 204859801251	240 GB	SAS 2
WDC WDS240G2G0A-00JH30 204859804508	240 GB	SAS 4

Logical imaging completed

Targets

Devices 5, Block size 64 KB, Left symmetric_2.L01 14 GB (Samsung SSD 850 PRO 512GB S250NX0H433169Y)/Partition 1
Evidence number: (empty)
Investigator: Jason Beck
Description: (empty)

Stats

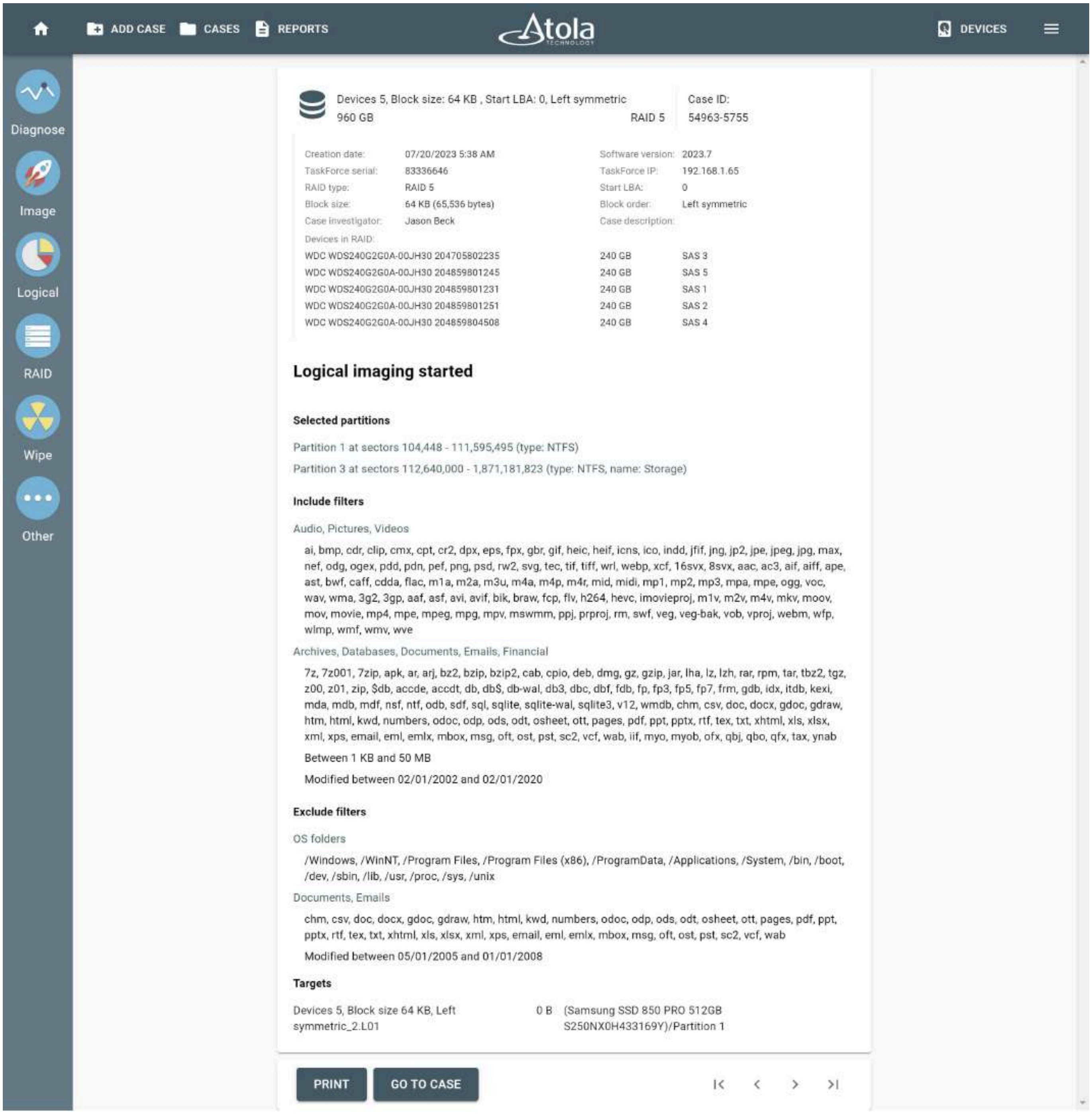
Files scanned	4,614
Files imaged	679
Bytes imaged	14 GB (13,860,000,160 bytes)

Log

Date ↑	Message
2023/07/20 05:34:28	Logical imaging started
2023/07/20 05:34:28	Analyzing: partition 1 at sectors 104,448 - 111,595,495 (type: NTFS)
2023/07/20 05:34:29	Analyzing: partition 3 at sectors 112,640,000 - 1,871,181,823 (type: NTFS, name: Storage)
2023/07/20 05:38:30	Logical imaging completed

Imaging completed report of a logical imaging session

Imaging started report is created the moment the imaging launched: it is a detailed report of all the settings including the elements selected for this acquisition (partitions, files and folders).



Devices 5, Block size: 64 KB , Start LBA: 0, Left symmetric
960 GB RAID 5

Case ID:
54963-5755

Creation date:	07/20/2023 5:38 AM	Software version:	2023.7
TaskForce serial:	83336646	TaskForce IP:	192.168.1.65
RAID type:	RAID 5	Start LBA:	0
Block size:	64 KB (65,536 bytes)	Block order:	Left symmetric
Case investigator:	Jason Beck	Case description:	

Devices in RAID:

WDC WDS240G2G0A-00JH30 204705802235	240 GB	SAS 3
WDC WDS240G2G0A-00JH30 204859801245	240 GB	SAS 5
WDC WDS240G2G0A-00JH30 204859801231	240 GB	SAS 1
WDC WDS240G2G0A-00JH30 204859801251	240 GB	SAS 2
WDC WDS240G2G0A-00JH30 204859804508	240 GB	SAS 4

Logical imaging started

Selected partitions

Partition 1 at sectors 104,448 - 111,595,495 (type: NTFS)

Partition 3 at sectors 112,640,000 - 1,871,181,823 (type: NTFS, name: Storage)

Include filters

Audio, Pictures, Videos

ai, bmp, cdr, clip, cmx, cpt, cr2, dpx, eps, fpx, gbr, gif, heic, heif, icns, ico, indd, jfif, jng, jp2, jpe, jpeg, jpg, max, nef, odg, ogex, pdd, pdn, pef, png, psd, rw2, svg, tec, tif, tiff, wrl, webp, xcf, 16svx, 8svx, aac, ac3, aif, aiff, ape, ast, bwf, caff, cdda, flac, m1a, m2a, m3u, m4a, m4p, m4r, mid, midi, mp1, mp2, mp3, mpa, mpe, ogg, voc, wav, wma, 3g2, 3gp, aaf, asf, avi, avif, bik, braw, fcp, flv, h264, hevc, imovieproj, m1v, m2v, m4v, mkv, moov, mov, movie, mp4, mpe, mpeg, mpg, mpv, mswmm, ppj, prproj, rm, swf, veg, veg-bak, vob, vproj, webm, wfp, wlmp, wmf, wmv, wve

Archives, Databases, Documents, Emails, Financial

7z, 7z001, 7zip, apk, ar, arj, bz2, bzip, bzip2, cab, cpio, deb, dmg, gz, gzip, jar, lha, lz, lzh, rar, rpm, tar, tbz2, tgz, z00, z01, zip, $db, accde, accdt, db, db$, db-wal, db3, dbc, dbf, fdb, fp, fp3, fp5, fp7, frm, gdb, idx, itdb, kexi, mda, mdb, mdf, nsf, ntf, odb, sdf, sql, sqlite, sqlite-wal, sqlite3, v12, wmdb, chm, csv, doc, docx, gdoc, gdraw, htm, html, kwd, numbers, odoc, odp, ods, odt, osheet, ott, pages, pdf, ppt, pptx, rtf, tex, txt, xhtml, xls, xlsx, xml, xps, email, eml, emlx, mbox, msg, oft, ost, pst, sc2, vcf, wab, iif, myo, myob, ofx, qbj, qbo, qfx, tax, ynab

Between 1 KB and 50 MB

Modified between 02/01/2002 and 02/01/2020

Exclude filters

OS folders

/Windows, /WinNT, /Program Files, /Program Files (x86), /ProgramData, /Applications, /System, /bin, /boot, /dev, /sbin, /lib, /usr, /proc, /sys, /unix

Documents, Emails

chm, csv, doc, docx, gdoc, gdraw, htm, html, kwd, numbers, odoc, odp, ods, odt, osheet, ott, pages, pdf, ppt, pptx, rtf, tex, txt, xhtml, xls, xlsx, xml, xps, email, eml, emlx, mbox, msg, oft, ost, pst, sc2, vcf, wab

Modified between 05/01/2005 and 01/01/2008

Targets

Devices 5, Block size 64 KB, Left symmetric_2.L01	0 B	(Samsung SSD 850 PRO 512GB S250NX0H433169Y)/Partition 1

Imaging started report of a logical imaging session.

Imaging selected partitions of a RAID array

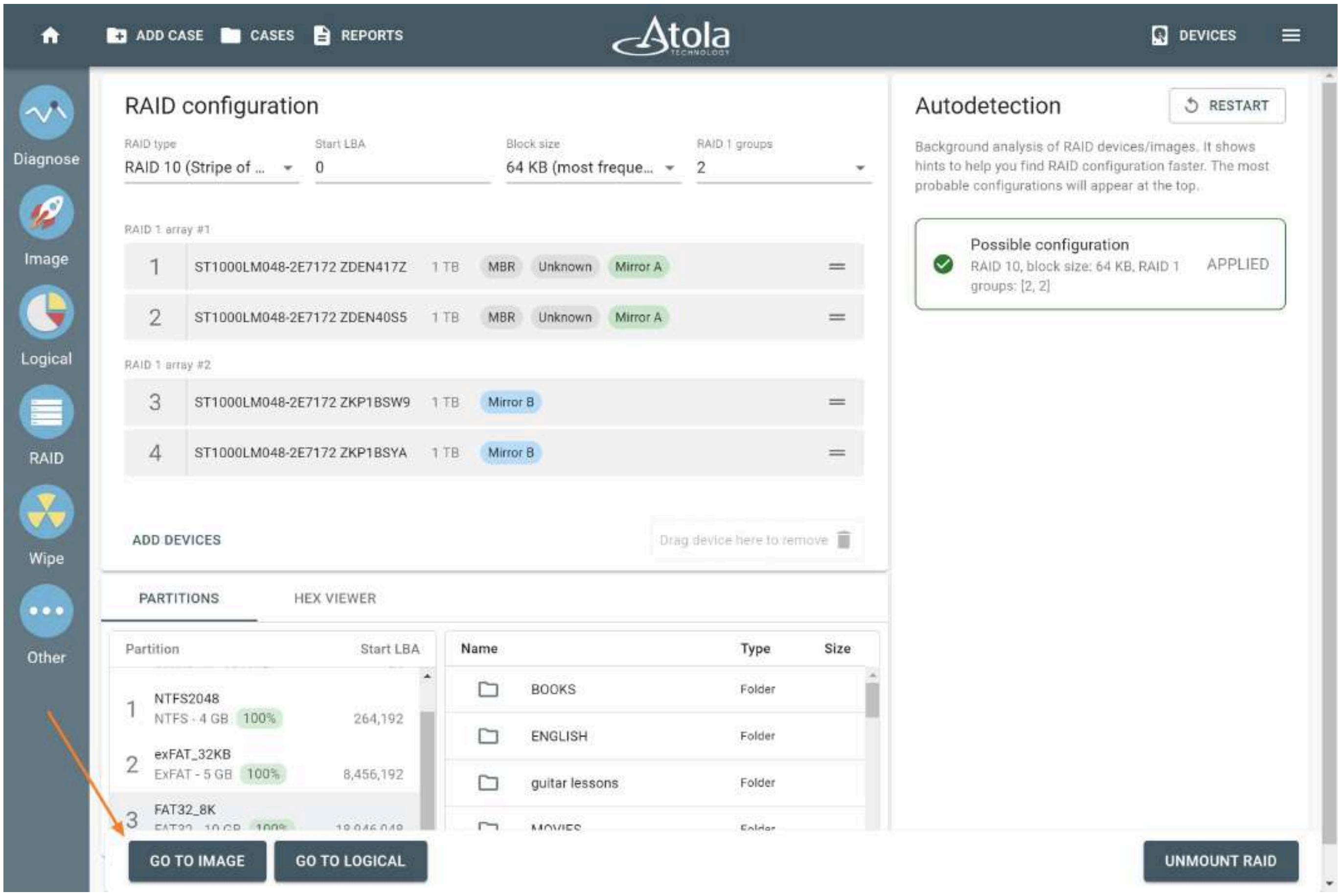
With Atola TaskForce 2, you can image individual partitions of an assembled RAID array to avoid imaging excessive amounts of data.

Once the RAID array has been reassembled, you can preview the contents of its partitions. It helps you conclude which of the partitions may contain the critical evidence and which are irrelevant.

Image selected partitions

To image only selected partitions of an assembled RAID array, do the following:

1. On the **RAID configuration** page, click **Go to image**.



RAID configuration

RAID type: RAID 10 (Stripe of ...
Start LBA: 0
Block size: 64 KB (most freque...
RAID 1 groups: 2

RAID 1 array #1

1	ST1000LM048-2E7172 ZDEN417Z	1 TB	MBR	Unknown	Mirror A
2	ST1000LM048-2E7172 ZDEN40S5	1 TB	MBR	Unknown	Mirror A

RAID 1 array #2

3	ST1000LM048-2E7172 ZKP1BSW9	1 TB	Mirror B
4	ST1000LM048-2E7172 ZKP1BSYA	1 TB	Mirror B

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

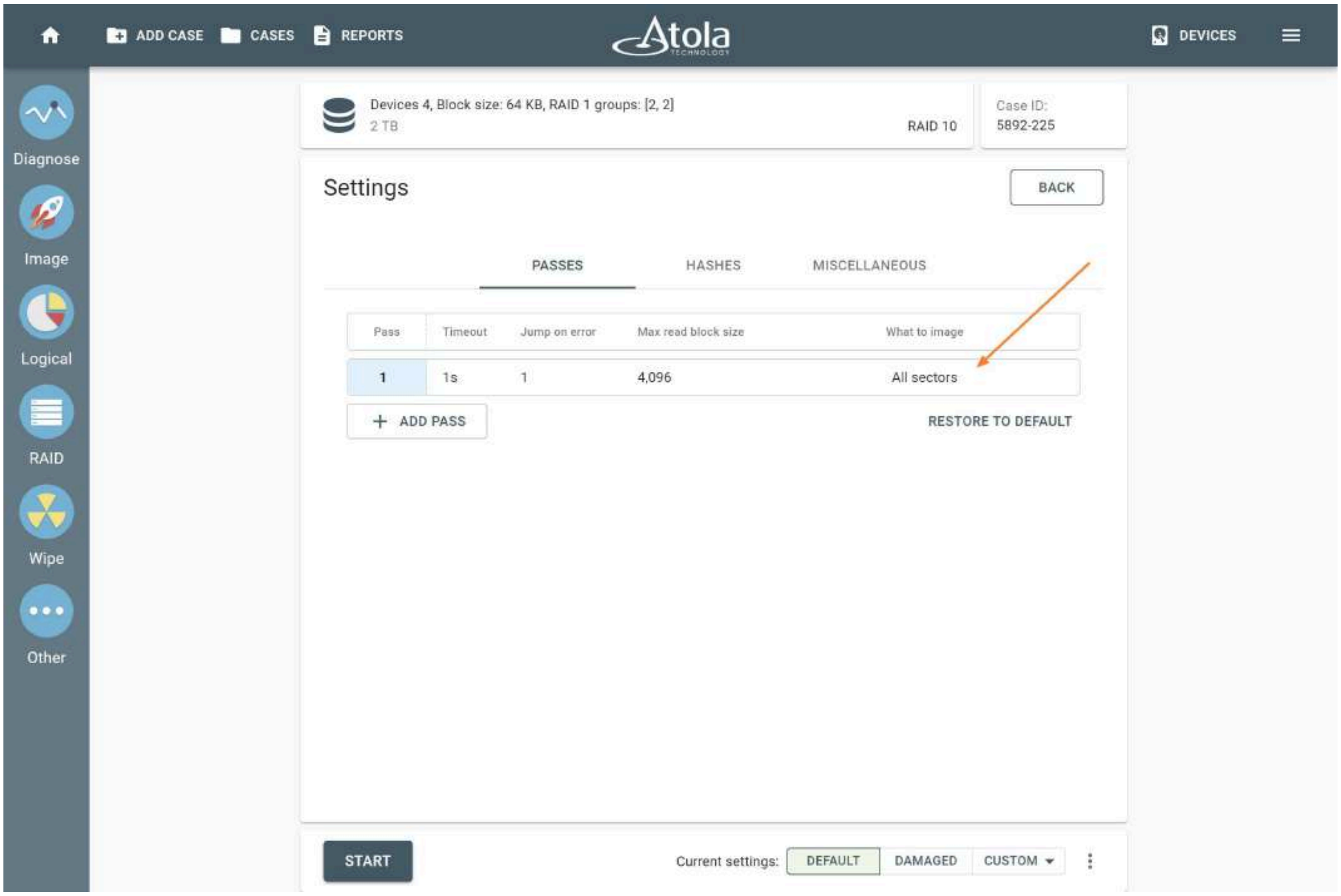
Possible configuration
RAID 10, block size: 64 KB, RAID 1 groups: [2, 2]
APPLIED

Partition		Start LBA
1	NTFS2048 NTFS - 4 GB 100%	264,192
2	exFAT_32KB ExFAT - 5 GB 100%	8,456,192
3	FAT32_8K FAT32 - 10 GB 100%	18,946,048

Name	Type	Size
BOOKS	Folder	
ENGLISH	Folder	
guitar lessons	Folder	
MOVIES	Folder	

The suggested RAID configuration applied, partitions preview shows partitions.

2. Select your target device and click **Continue**.
3. On the imaging **Settings** page, click the imaging pass to adjust the imaging range.



Devices 4, Block size: 64 KB, RAID 1 groups: [2, 2]
2 TB
RAID 10

Case ID:
5892-225

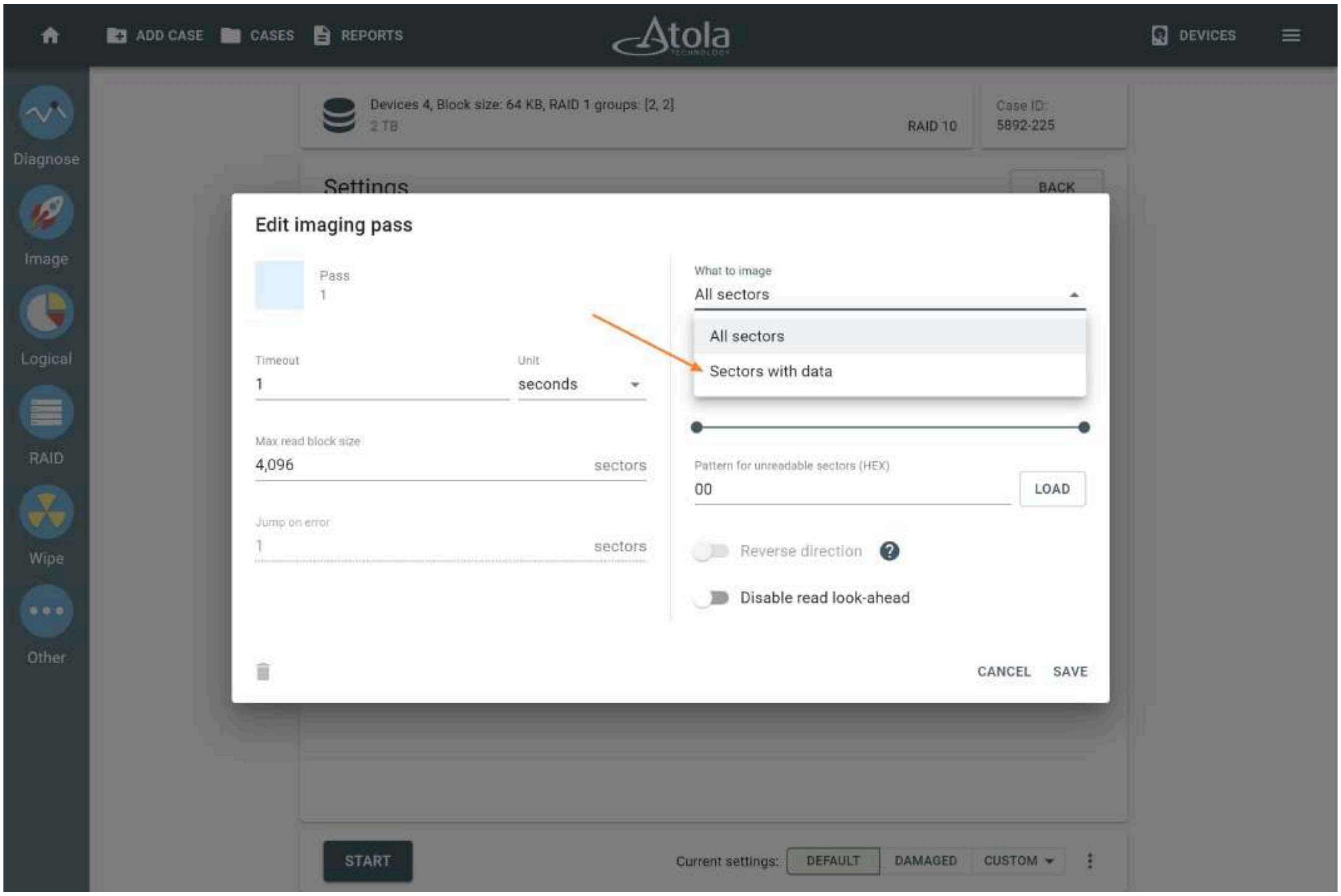
Settings

Pass	Timeout	Jump on error	Max read block size	What to image
1	1s	1	4,096	All sectors

Current settings: DEFAULT

The suggested RAID configuration applied, partitions preview shows partitions.

4. In the **Edit imaging pass** dialog, click on the **What to image** and select **Sectors with data**.



Devices 4, Block size: 64 KB, RAID 1 groups: [2, 2]
2 TB
RAID 10

Case ID:
5892-225

Edit imaging pass

Pass
1

Timeout
1

Unit
seconds

Max read block size
4,096 sectors

Jump on error
1 sectors

What to image
All sectors

Pattern for unreadable sectors (HEX)
00

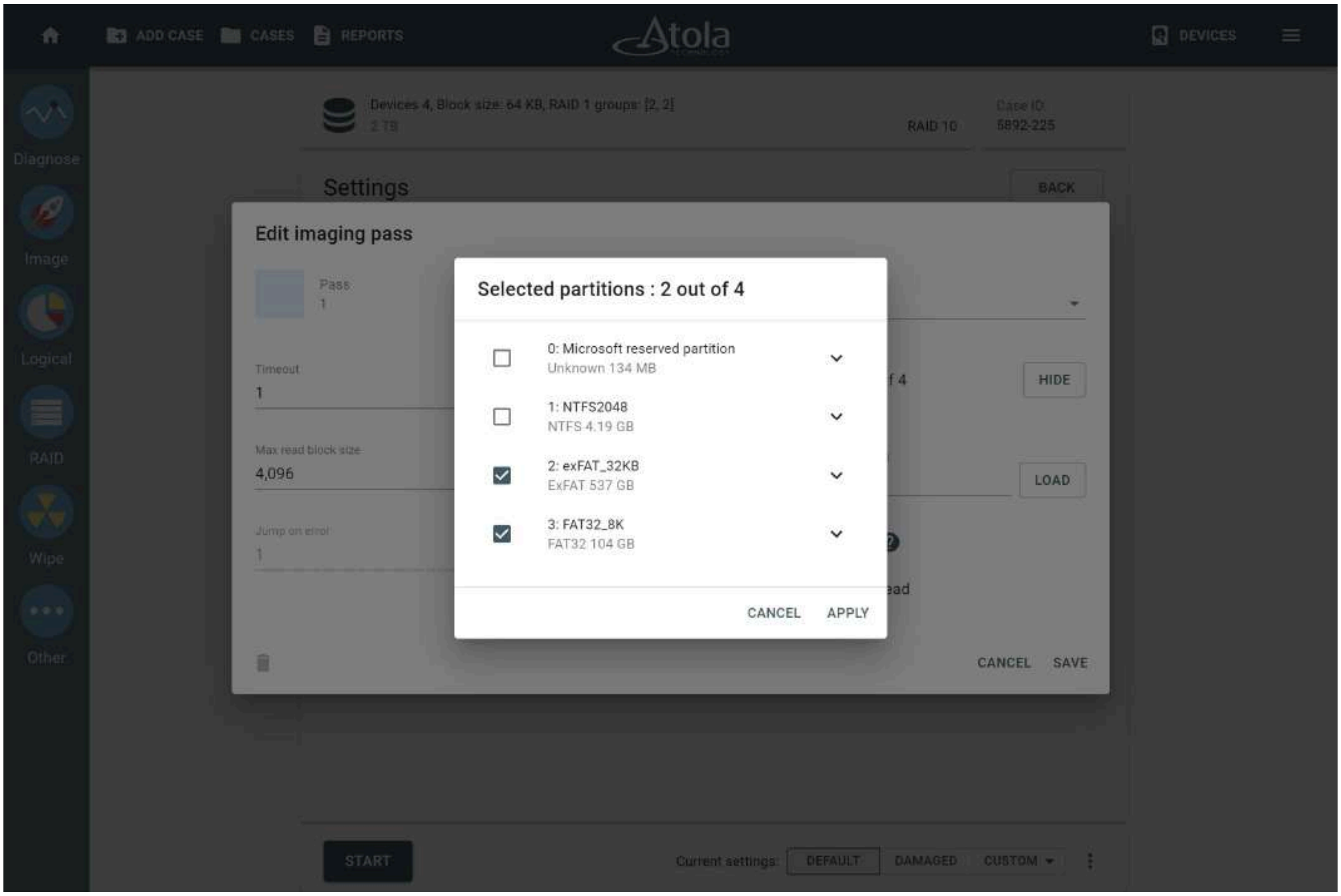
Reverse direction

Disable read look-ahead

Current settings: DEFAULT

Selecting only sectors with data from the What to image list.

5. Unselect the partitions you do not need and click **Apply**. Then click **Save** to keep this change.



Timeout: 1

Max read block size: 4,096

Jump on error: 1

Selected partitions : 2 out of 4

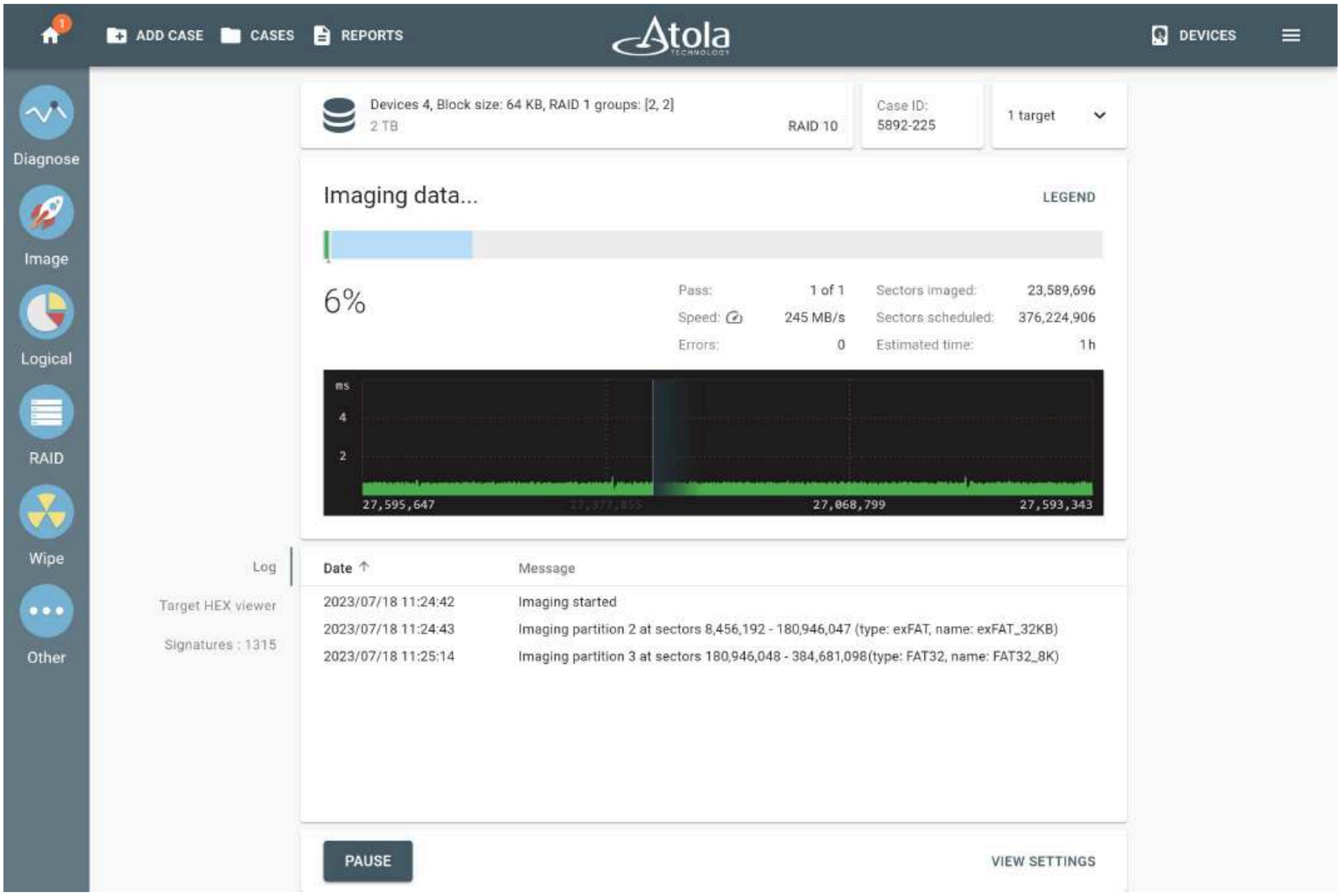
- ☐ 0: Microsoft reserved partition — Unknown 134 MB
- ☐ 1: NTFS2048 — NTFS 4.19 GB
- ☑ 2: exFAT_32KB — ExFAT 537 GB
- ☑ 3: FAT32_8K — FAT32 104 GB

CANCEL APPLY

Select partitions for imaging

> The selective imaging does not linear hashing of the imaged range, segmeted hashing is suggested for such imaging.

6. To launch your imaging session, click **Start**.



Devices 4, Block size: 64 KB, RAID 1 groups: [2, 2]
2 TB
RAID 10

Case ID:
5892-225

1 target

Imaging data...

6%

Pass:	1 of 1	Sectors imaged:	23,589,696
Speed:	245 MB/s	Sectors scheduled:	376,224,906
Errors:	0	Estimated time:	1 h

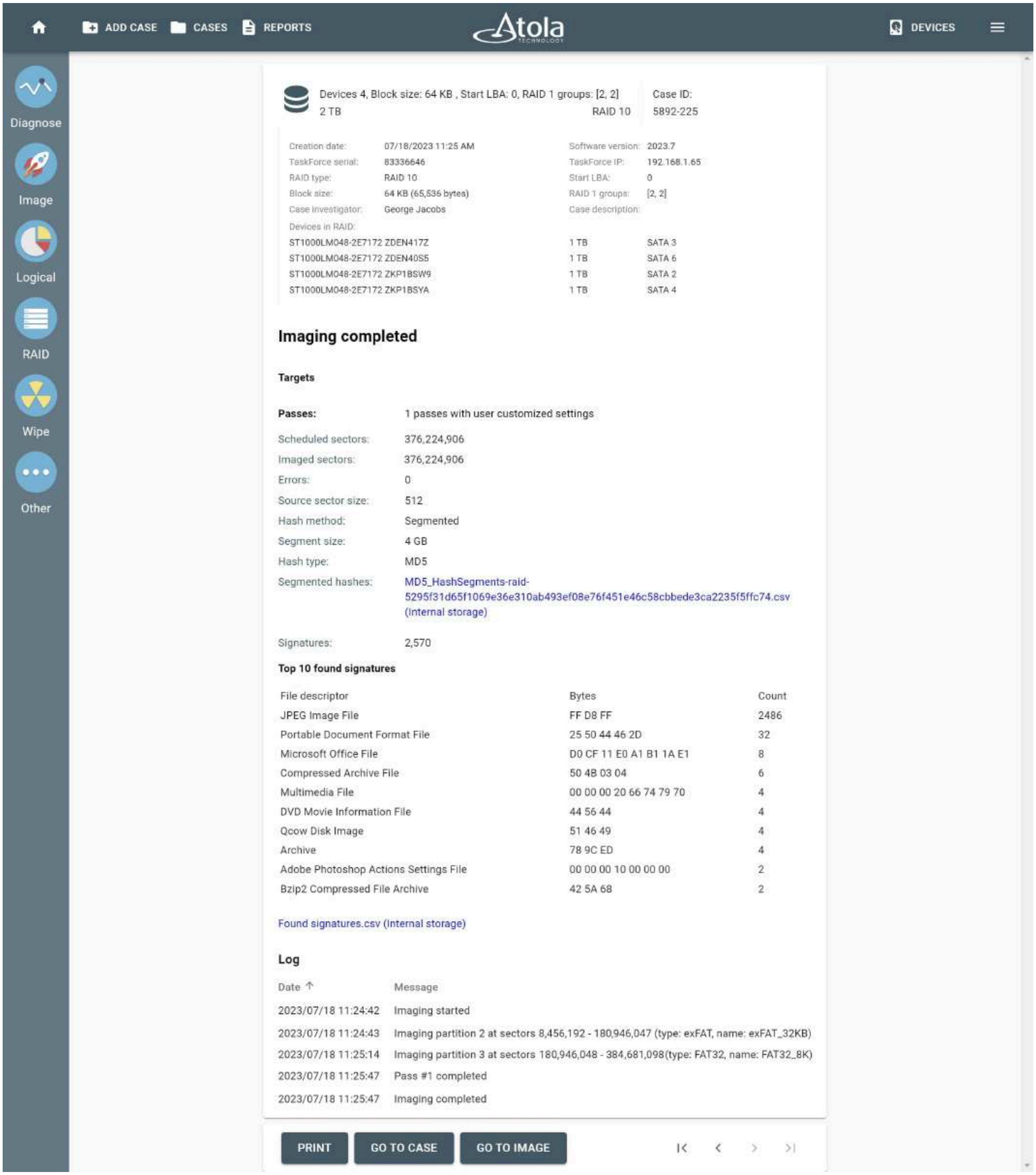
Date ↑	Message
2023/07/18 11:24:42	Imaging started
2023/07/18 11:24:43	Imaging partition 2 at sectors 8,456,192 - 180,946,047 (type: exFAT, name: exFAT_32KB)
2023/07/18 11:25:14	Imaging partition 3 at sectors 180,946,048 - 384,681,098(type: FAT32, name: FAT32_8K)

The suggested RAID configuration applied, partitions preview shows partitions

Imaging report

TaskForce 2 generates the **Imaging completed** report with all the details of the RAID:

- The imaged range.
- Time stamps.
- A link to the file with the segmented hash, calculated for the imaged range.



Devices 4, Block size: 64 KB , Start LBA: 0, RAID 1 groups: [2, 2]
2 TB
RAID 10

Case ID:
5892-225

Creation date:	07/18/2023 11:25 AM	Software version:	2023.7
TaskForce serial:	83336646	TaskForce IP:	192.168.1.65
RAID type:	RAID 10	Start LBA:	0
Block size:	64 KB (65,536 bytes)	RAID 1 groups:	[2, 2]
Case investigator:	George Jacobs	Case description:	
Devices in RAID:			
ST1000LM048-2E7172 ZDEN417Z		1 TB	SATA 3
ST1000LM048-2E7172 ZDEN40S5		1 TB	SATA 6
ST1000LM048-2E7172 ZKP1BSW9		1 TB	SATA 2
ST1000LM048-2E7172 ZKP1BSYA		1 TB	SATA 4

Imaging completed

Targets

Passes:	1 passes with user customized settings
Scheduled sectors:	376,224,906
Imaged sectors:	376,224,906
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5
Segmented hashes:	MD5_HashSegments-raid-5295f31d65f1069e36e310ab493ef08e76f451e46c58cbbede3ca2235f5ffc74.csv (Internal storage)
Signatures:	2,570

Top 10 found signatures

File descriptor	Bytes	Count
JPEG Image File	FF D8 FF	2486
Portable Document Format File	25 50 44 46 2D	32
Microsoft Office File	D0 CF 11 E0 A1 B1 1A E1	8
Compressed Archive File	50 4B 03 04	6
Multimedia File	00 00 00 20 66 74 79 70	4
DVD Movie Information File	44 56 44	4
Qcow Disk Image	51 46 49	4
Archive	78 9C ED	4
Adobe Photoshop Actions Settings File	00 00 00 10 00 00 00	2
Bzip2 Compressed File Archive	42 5A 68	2

Found signatures.csv (Internal storage)

Log

```
Date ↑               Message
2023/07/18 11:24:42  Imaging started
2023/07/18 11:24:43  Imaging partition 2 at sectors 8,456,192 - 180,946,047 (type: exFAT, name: exFAT_32KB)
2023/07/18 11:25:14  Imaging partition 3 at sectors 180,946,048 - 384,681,098(type: FAT32, name: FAT32_8K)
2023/07/18 11:25:47  Pass #1 completed
2023/07/18 11:25:47  Imaging completed
```

The Imaging completed report

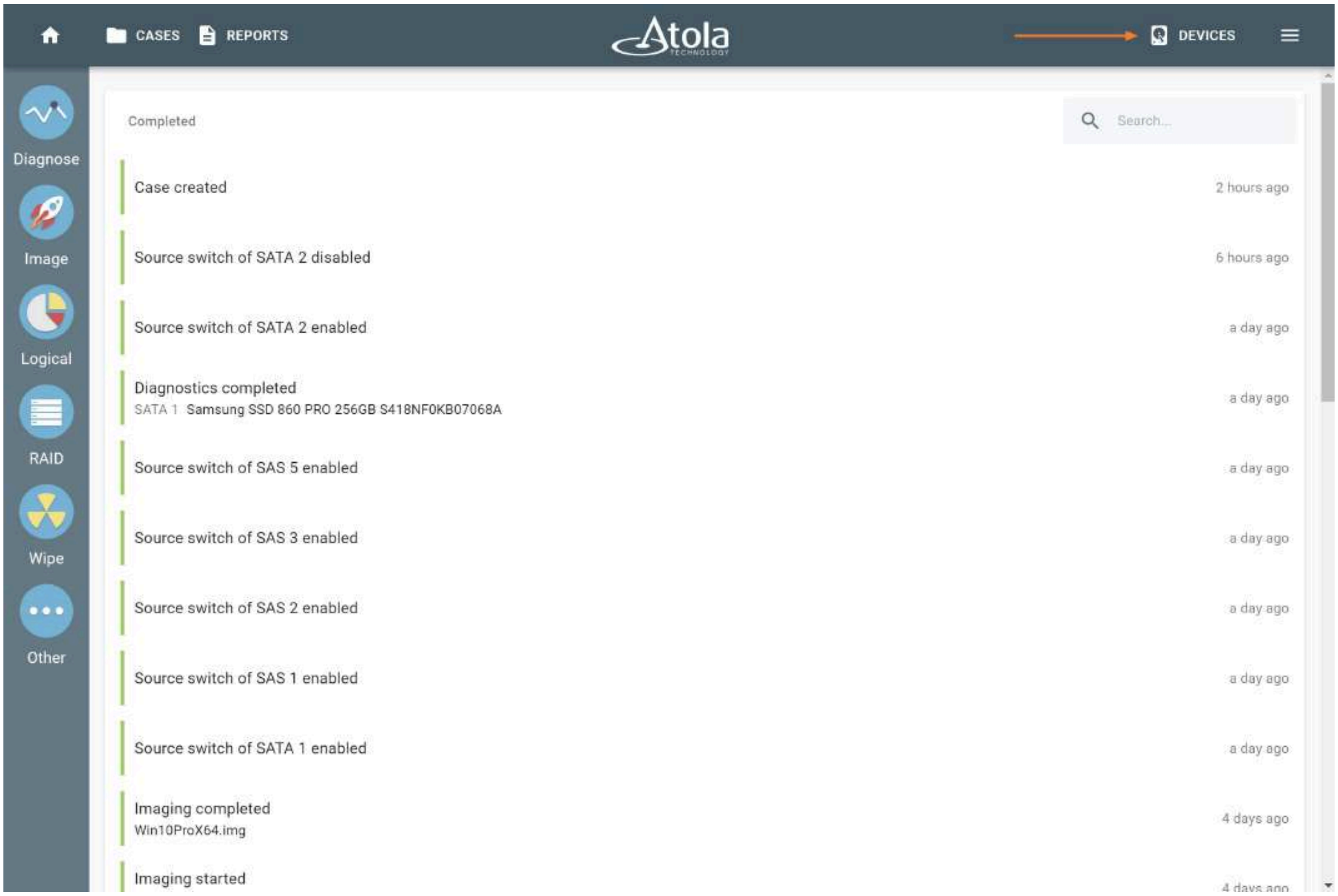
How to unmount an assembled RAID

After you selected specific drives or images as RAID participants, they constitute virtual RAID array and become unavailable for individual tasks. For instance, you cannot recalculate hash of one of such drives.

To use the individual drives that are a part of a mounted RAID array, you need to unmount the RAID first.

Follow these steps:

1. At the top right, click **Devices**.



Completed

Case created 2 hours ago

Source switch of SATA 2 disabled 6 hours ago

Source switch of SATA 2 enabled a day ago

Diagnostics completed
SATA 1 Samsung SSD 860 PRO 256GB S418NF0KB07068A a day ago

Source switch of SAS 5 enabled a day ago

Source switch of SAS 3 enabled a day ago

Source switch of SAS 2 enabled a day ago

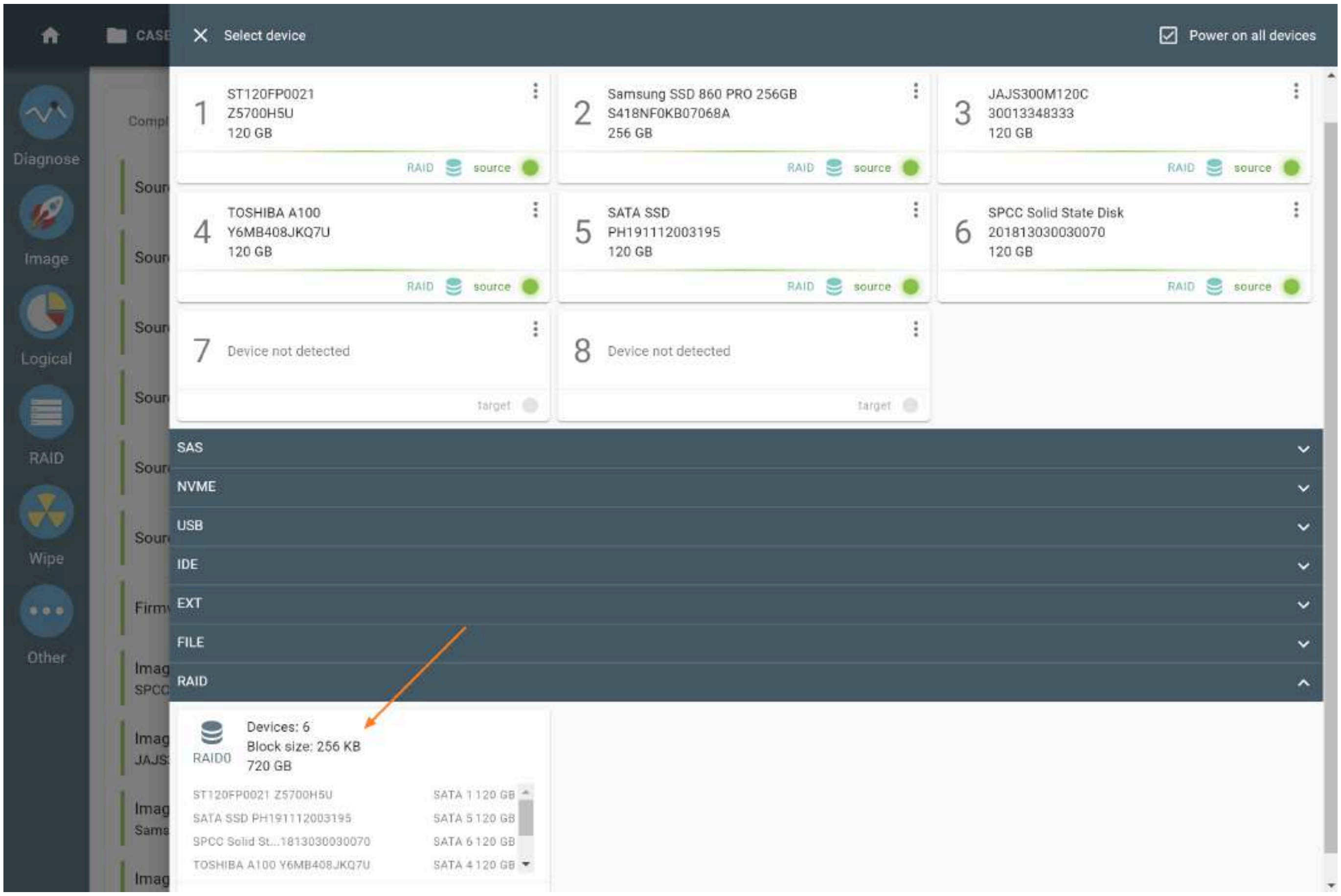
Source switch of SAS 1 enabled a day ago

Source switch of SATA 1 enabled a day ago

Imaging completed
Win10ProX64.img 4 days ago

Imaging started 4 days ago

2. Scroll down to the bottom of the **Devices** panel and in the **RAID** section select the currently connected and mounted RAID.



1 ST120FP0021 Z5700H5U 120 GB — RAID source

2 Samsung SSD 860 PRO 256GB S418NF0KB07068A 256 GB — RAID source

3 JAJS300M120C 30013348333 120 GB — RAID source

4 TOSHIBA A100 Y6MB408JKQ7U 120 GB — RAID source

5 SATA SSD PH191112003195 120 GB — RAID source

6 SPCC Solid State Disk 201813030030070 120 GB — RAID source

7 Device not detected — target

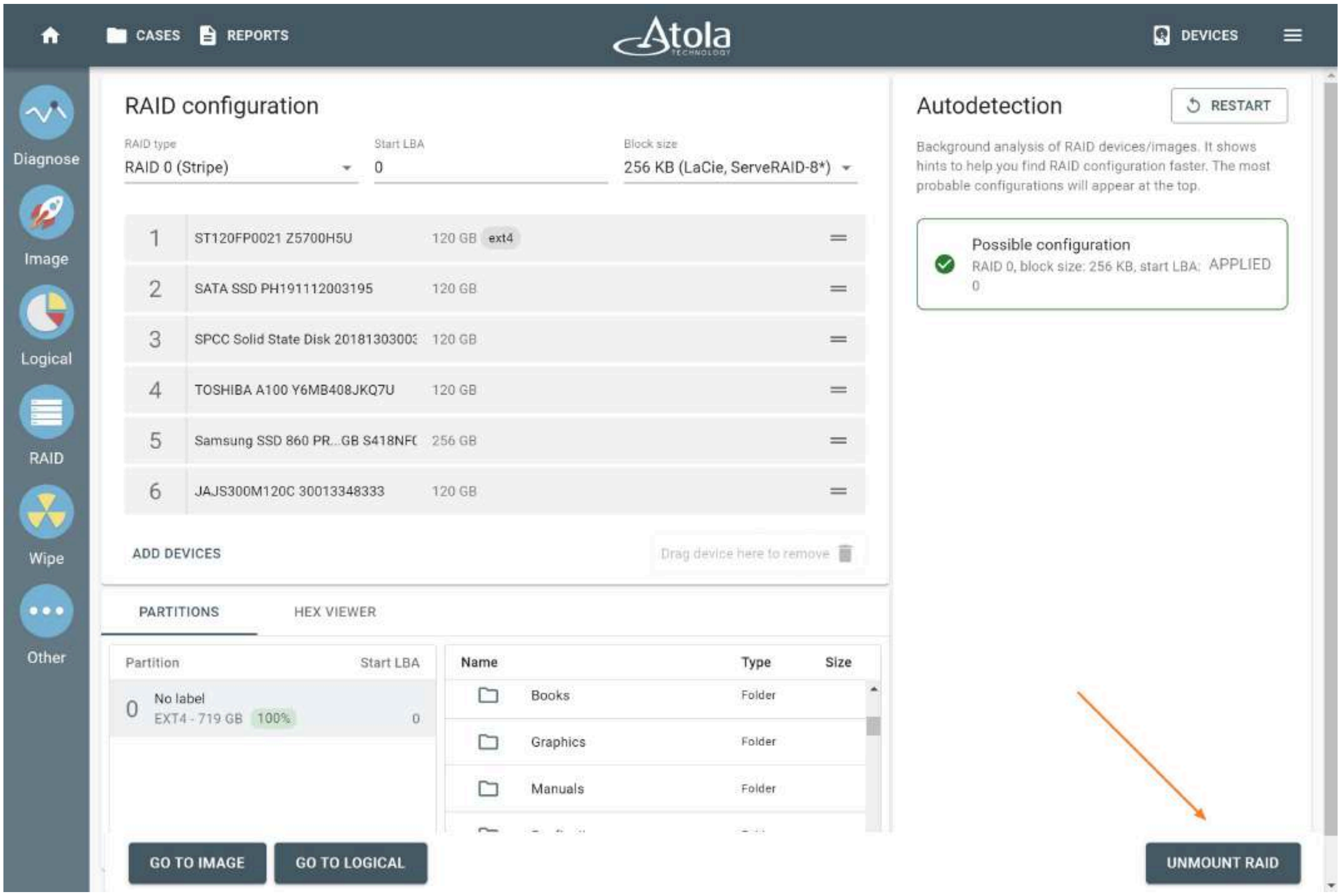
8 Device not detected — target

RAID0 — Devices: 6, Block size: 256 KB, 720 GB

```
ST120FP0021 Z5700H5U              SATA 1 120 GB
SATA SSD PH191112003195           SATA 5 120 GB
SPCC Solid St...1813030030070     SATA 6 120 GB
TOSHIBA A100 Y6MB408JKQ7U         SATA 4 120 GB
```

Assembled RAID array.

3. At the bottom of the **RAID configuration** page, click the **Unmount RAID** button.



RAID configuration

RAID type: RAID 0 (Stripe)
Start LBA: 0
Block size: 256 KB (LaCie, ServeRAID-8*)

1	ST120FP0021 Z5700H5U	120 GB ext4
2	SATA SSD PH191112003195	120 GB
3	SPCC Solid State Disk 2018130300:	120 GB
4	TOSHIBA A100 Y6MB408JKQ7U	120 GB
5	Samsung SSD 860 PR...GB S418NF(	256 GB
6	JAJS300M120C 30013348333	120 GB

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Possible configuration
RAID 0, block size: 256 KB, start LBA: 0 APPLIED

Partition	Start LBA
0 No label EXT4 - 719 GB 100%	0

Name	Type	Size
Books	Folder	
Graphics	Folder	
Manuals	Folder	

Unmount RAID with a single click.

Now you can proceed with other sessions, using any of the drives connected to TaskForce 2.

Supported RAID types and parameters

RAID stands for "*redundant array of independent disks*" or "*redundant array of inexpensive disks*". It is a technology of data storage that combines two or more physical disk drives into one or more logical units (**arrays**). This approach improves data storage reliability, performance, or both.

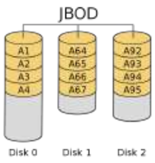
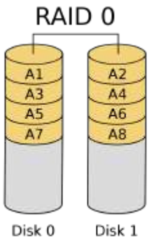
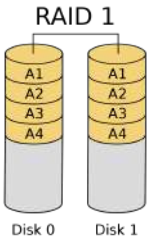
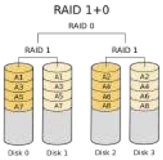
The data can be distributed across physical drives of a RAID array using different standardized methods, which are called **RAID types** or **RAID levels**.

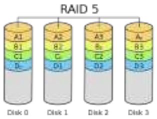
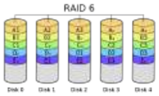
Atola TaskForce can reassemble and image the following RAID types:

- JBOD
- RAID 0 (Stripe)
- RAID 1 (Mirror)
- RAID 10 (Stripe of mirrors)
- RAID 5 (Distributed parity)
- RAID 6 (Dual parity)

This article covers currently supported RAID types and their parameters in more detail.

RAID types comparison

RAID type and method	Scheme of data distribution	Description	Common usage	Performance	Fault tolerance	Capacity	Minimum number of disks
JBOD: Spanning	 JBOD A1 A2 A3 A4 A64 A65 A66 A67 A92 A93 A94 A95 Disk 0 Disk 1 Disk 2	Multiple physical drives are spanned, or concatenated, together to form a single logical disk with no redundancy.	Increasing capacity. Cost-effective storage with no performance or security benefits.	No benefits. Array performance equals the performance of each drive depending on data location.	Very low. Redundancy is not provided. If one drive fails, a failure is typically isolated to this drive.	Array capacity is the sum of the capacities of its members.	2
RAID 0: Striping	 RAID 0 A1 A3 A5 A7 A2 A4 A6 A8 Disk 0 Disk 1	Data is split ('striped') evenly across the drives forming a logical array, without parity or mirroring.	Improving reading and writing speed.	The highest read and write speed because data is striped across all disks, and the controller can read and write several drives in parallel with no delay due to parity calculation.	Very low. If one drive fails, data is lost.	Volume is the sum of the capacities of the drives in the set. No overhead is provided by parity blocks.	2
RAID 1: Mirroring	 RAID 1 A1 A2 A3 A4 A1 A2 A3 A4 Disk 0 Disk 1	Mirroring without parity or striping. Data is written identically to two or more drives, producing a "mirrored set" of drives.	Standart app servers; applications that require higher fault tolerance, than storage capacity or performance.	High read speed: the controller can read several drives in parallel. Lower compared to RAID 0 write speed: all data must be written to two disks.	High. If one drive fails, data is restored from the "mirror" drive(s).	Storage capacity is reduced by 1/2 as all data is written twice.	2
RAID 10 (1+0): Striping and mirroring	 RAID 1+0 RAID 0 RAID 1 RAID 1 A1 A3 A5 A7 A1 A3 A5 A7 A2 A4 A6 A8 A2 A4 A6 A8 Disk 0 Disk 1 Disk 2 Disk 3	Striped set from a series of mirrored drives. Data is shared between disks and duplicated.	Highly utilized database, email, web servers.	High read speed similar to RAID 1 due to improved read rates through simultaneous disk reads.Moderate to high write speed because data is mirrored across pairs, but the striping allows for higher write speeds compared to just RAID 1.	Very high fault tolerance. The array can sustain multiple drive losses so long as no mirror loses all its drives.	Storage capacity is reduced by 1/2 as all data is written twice.	4

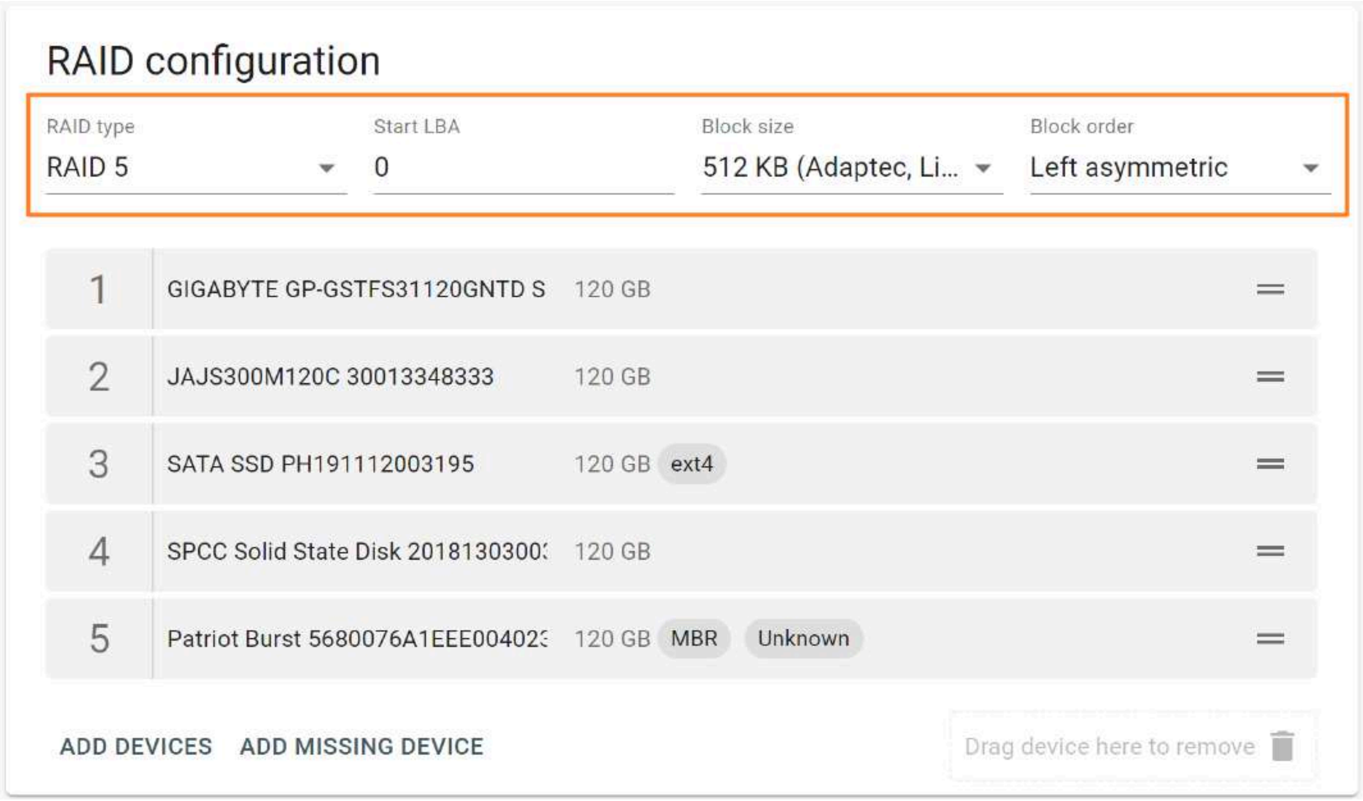
RAID type and method	Scheme of data distribution	Description	Common usage	Performance	Fault tolerance	Capacity	Minimum number of disks
RAID 5: Striping and parity	 RAID 5 A1 A2 A3 Ap B1 B2 Bp B3 C1 Cp C2 C3 Dp D1 D2 D3 Disk 0 Disk 1 Disk 2 Disk 3	Data is split ('striped') evenly across the drives with added distributed parity.	Normal file storage and app servers.	High read speed but slightly lower than RAID 0 because of the overhead from parity calculations and distribution across all disks. Moderate write speed due to the need for parity calculations and writing both data and parity information.	High. If one drive fails, data can still be calculated from the distributed parity.	Due to parity blocks, storage capacity equals the smallest drive capacity multiplied by (N−1) drives.	3
RAID 6: Striping and double parity		Data is split ('striped') evenly across the drives with two distributed parity blocks, instead of one.	Large file storage and app servers.	High read speed similar to RAID 5, but can be slightly slower due to additional parity calculations. Write speed is lower than RAID 5 because it requires two parity blocks to be written.	Very high fault tolerance due to double parity. Data can still be calculated even if two drives fail.	Due to dual parity blocks, storage capacity equals the smallest drive capacity multiplied by (N−2) drives.	4

RAID parameters

Each individual RAID is defined by a combination of several main parameters:

- RAID type (or RAID level)
- Number of devices
- Device order
- Start LBA (or Disk offset)
- Block size
- Block order
- Parity block order
- File system

To identify RAID type and exact parameters, TaskForce automatically checks up to 200,000,000 RAID parameter combinations. However, if you know the exact RAID configuration, you can enter it manually.



RAID configuration

RAID type: RAID 5

Start LBA: 0

Block size: 512 KB (Adaptec, Li...

Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD S	120 GB
2	JAJS300M120C 30013348333	120 GB
3	SATA SSD PH191112003195	120 GB ext4
4	SPCC Solid State Disk 2018130300:	120 GB
5	Patriot Burst 5680076A1EEE00402:	120 GB MBR Unknown

Depending on the RAID type, different sets of parameters can be applied:

Number of devices	✓	✓	✓	✓	✓ + missing	✓ + missing
Device order	✓	✓	✓	✓	✓	✓
Start LBA	✓	✓	✓	✓	✓	✓
Block size	–	✓	–	✓	✓	✓
RAID 1 groups	–	–	–	✓	–	–
Block order	–	–	–	–	✓	✓
Parity block order/type	–	–	–	–	–	✓

Here's what each of the RAID parameters means.

RAID type (or RAID level)

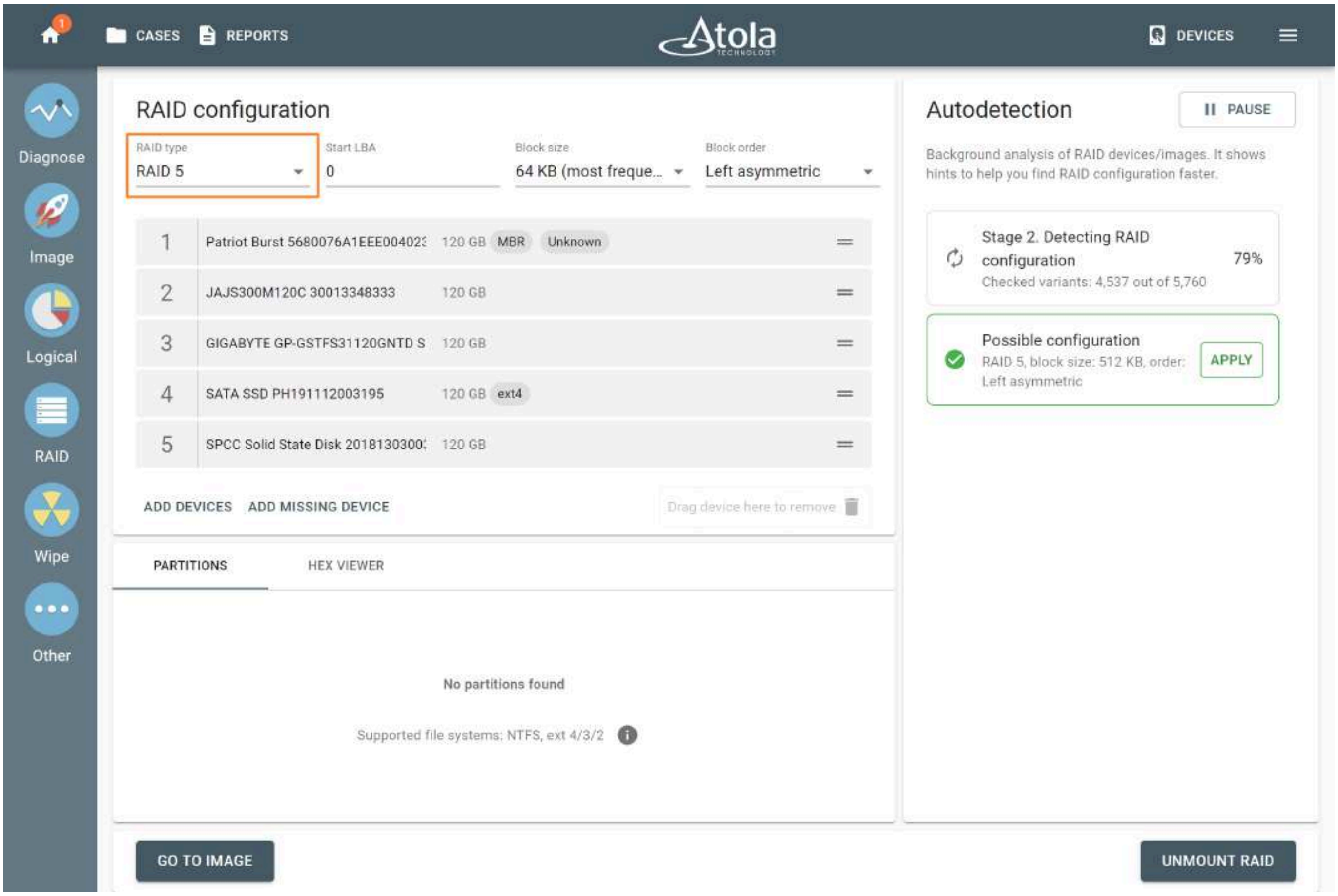
RAID type is defined by the method in which data is distributed across physical drives combining the array. TaskForce currently supports the following RAID types:

- JBOD
- RAID 0 (Stripe)
- RAID 1 (Mirror)
- RAID 10 (Stripe of mirrors)
- RAID 5 (Distributed parity)

- RAID 6 (Dual parity)

In TaskForce, the RAID type can be automatically identified by the **Autodetection** module along with other parameters.

However, if you know the RAID type, you can select it manually from the **RAID type** list in the **RAID configuration** section.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left asymmetric

1 Patriot Burst 5680076A1EEE00402: 120 GB MBR Unknown
2 JAJS300M120C 30013348333 120 GB
3 GIGABYTE GP-GSTFS31120GNTD S 120 GB
4 SATA SSD PH191112003195 120 GB ext4
5 SPCC Solid State Disk 2018130300: 120 GB

No partitions found

Supported file systems: NTFS, ext 4/3/2

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster.

Stage 2. Detecting RAID configuration 79%
Checked variants: 4,537 out of 5,760

Possible configuration
RAID 5, block size: 512 KB, order: Left asymmetric

The RAID type list in the RAID configuration section.

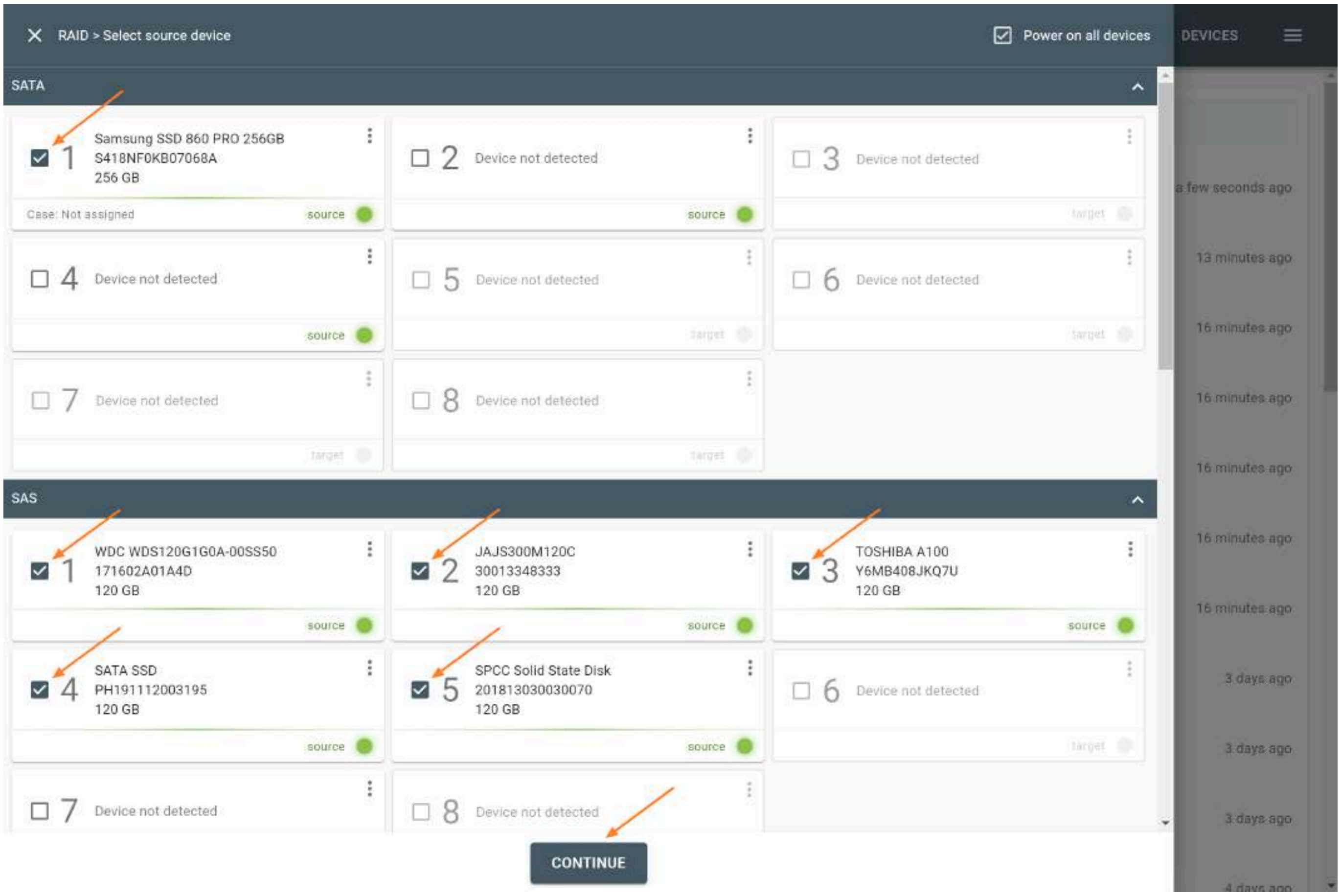
Number of devices

Applies to: all supported RAID types.

The minimum number of disks needed to build a RAID array is:

- two for JBOD, RAID 0, and RAID 1,
- three for RAID 5,
- four for RAID 10 and RAID 6.

The actual number of RAID members is determined by you when you select in the TaskForce RAID module physical disks (SATA/SAS/USB drives) or their images (raw, E01 or AFF4 image files) as Sources that make up a RAID array.



RAID > Select source device

☑ Power on all devices

DEVICES

SATA

☑ 1 Samsung SSD 860 PRO 256GB
S418NF0KB07068A
256 GB
Case: Not assigned source

□ 2 Device not detected
source

□ 3 Device not detected
target

□ 4 Device not detected
source

□ 5 Device not detected
target

□ 6 Device not detected
target

□ 7 Device not detected
target

□ 8 Device not detected
target

SAS

☑ 1 WDC WDS120G1G0A-00SS50
171602A01A4D
120 GB
source

☑ 2 JAJS300M120C
30013348333
120 GB
source

☑ 3 TOSHIBA A100
Y6MB408JKQ7U
120 GB
source

☑ 4 SATA SSD
PH191112003195
120 GB
source

☑ 5 SPCC Solid State Disk
201813030030070
120 GB
source

□ 6 Device not detected
target

□ 7 Device not detected

□ 8 Device not detected

CONTINUE

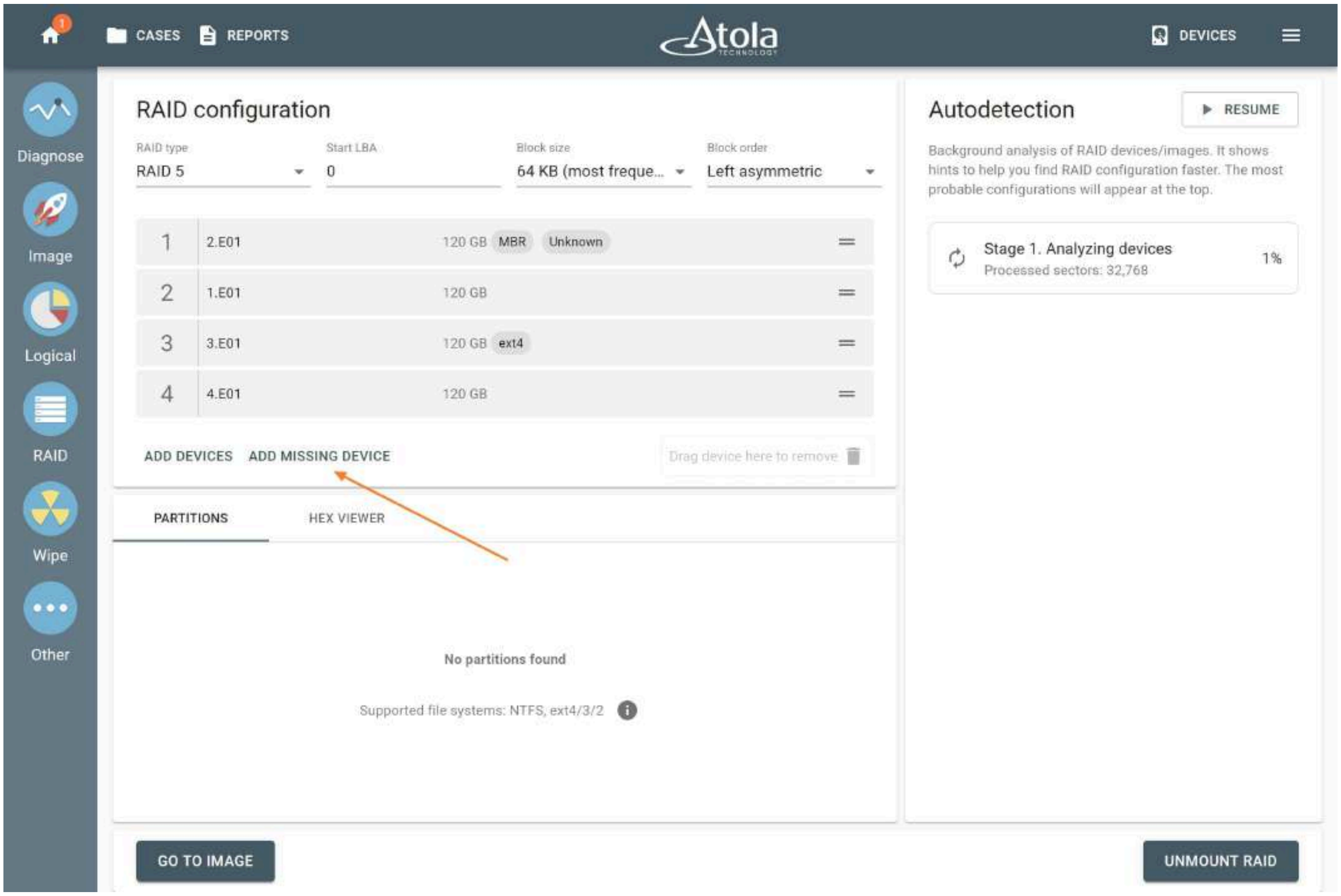
a few seconds ago
13 minutes ago
16 minutes ago
16 minutes ago
16 minutes ago
16 minutes ago
16 minutes ago
3 days ago
3 days ago
3 days ago
4 days ago

Selecting source RAID drives.

Missing RAID members. For the RAID types that use redundancy (parity blocks), TaskForce can reassemble an array and create its image even with a missing device:

- with **one missing** device for RAID 5 that uses distributed parity,
- with **two missing** devices for RAID 6 that uses double distributed parity.

See RAID 5 with a missing drive for more details.



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 64 KB (most freque...
Block order: Left asymmetric

1	2.E01	120 GB	MBR Unknown
2	1.E01	120 GB	
3	3.E01	120 GB	ext4
4	4.E01	120 GB	

No partitions found

Supported file systems: NTFS, ext4/3/2

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster. The most probable configurations will appear at the top.

Stage 1. Analyzing devices 1%
Processed sectors: 32,768

Adding missing RAID 5 drive.

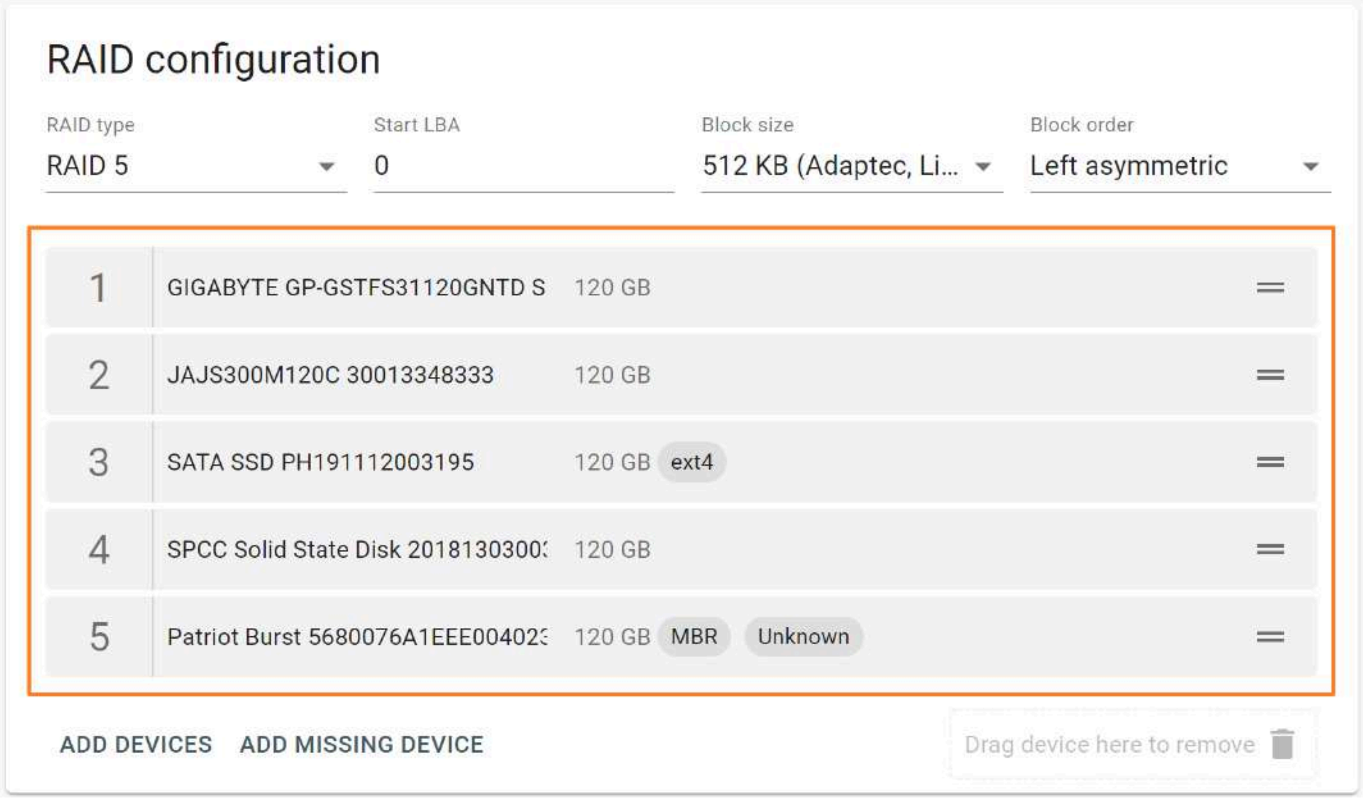
Device order

Applies to: all supported RAID types.

The drive order is the order in which physical devices (or their images) follow each other within a logical array (think pages within a book). That order is defined by a RAID controller during the setup of an array. To reassemble and image a RAID array, you need to determine which of its members go first, second, third and so on.

In TaskForce, the drive order can be automatically detected by the Autodetection module along with other parameters.

However, if you know the drive order, arrange the RAID members manually by dragging them up or down in the **RAID configuration** section of the TaskForce RAID module.



RAID configuration

RAID type: RAID 5

Start LBA: 0

Block size: 512 KB (Adaptec, Li...

Block order: Left asymmetric

1 GIGABYTE GP-GSTFS31120GNTD S 120 GB

2 JAJS300M120C 30013348333 120 GB

3 SATA SSD PH191112003195 120 GB ext4

4 SPCC Solid State Disk 2018130300: 120 GB

5 Patriot Burst 5680076A1EEE00402: 120 GB MBR Unknown

Start LBA (or Disk offset)

Applies to: all supported RAID types.

LBA stands for Logical Block Address. It is a scheme used for addressing a particular area on a storage device in a linear way using sequential integer numbers, starting from zero: 0, 1, 2, 3... Thanks to LBA a single drive or a RAID controller identifies the exact location of bytes it needs to read from or write to.

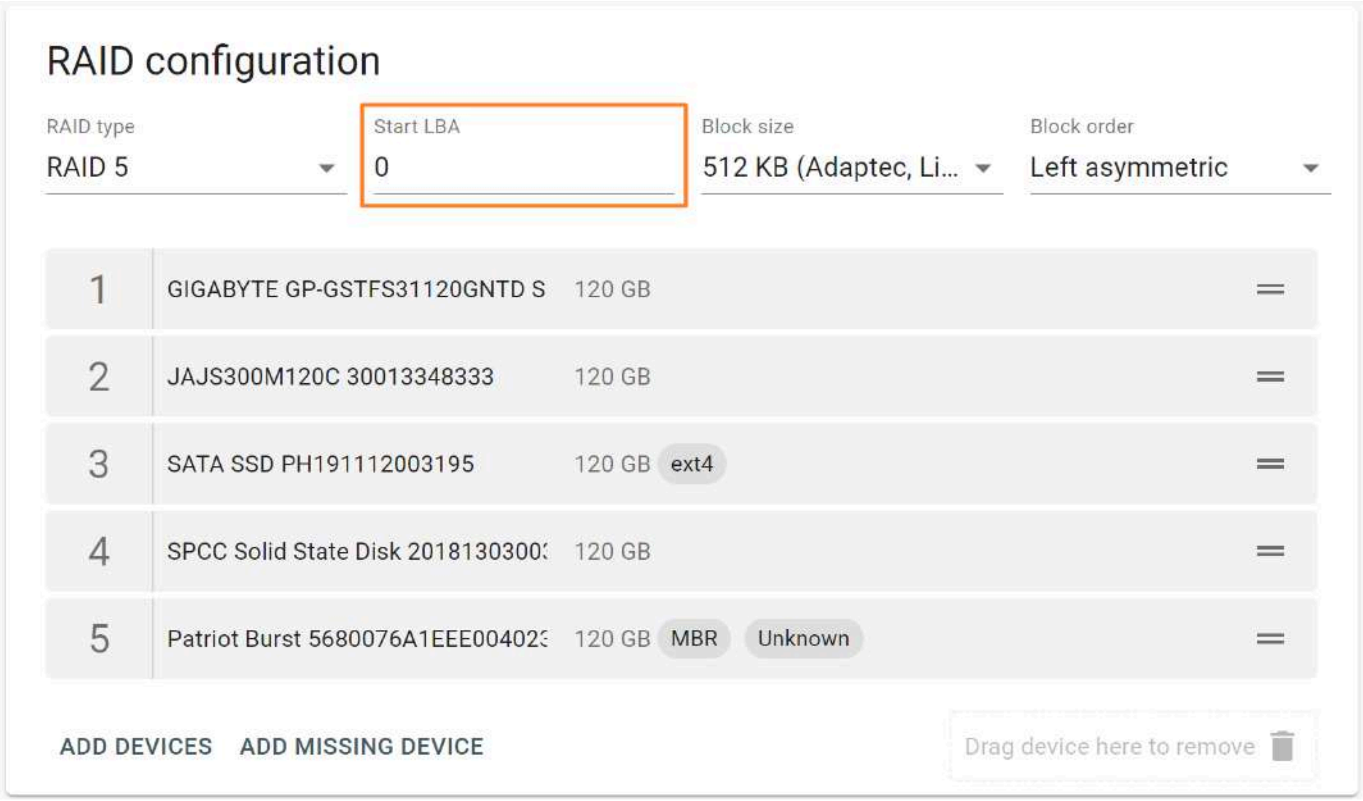
When we talk about RAIDs, **Start LBA**, also known as **Device offset**, refers to an address of a logical block on each physical RAID member where user data begins. **Start LBA** of each member of the same RAID is identical.

If RAID's Start LBA is 0, RAID blocks (chunks) start from the first logical block on each drive in an array, without any offset (it is the most common case).

If RAID's Start LBA is greater than 0, a space created by this offset is skipped. RAID blocks start from the specified Start LBA on each drive in an array. Typically, the skipped space can be used to store RAID metadata (data about data).

In some cases, TaskForce can identify RAID's Start LBA during autodetection using a heuristic algorithm.

If you know Start LBA, you can enter it in the **Start LBA** field of the **RAID configuration section**.



RAID configuration

RAID type: RAID 5

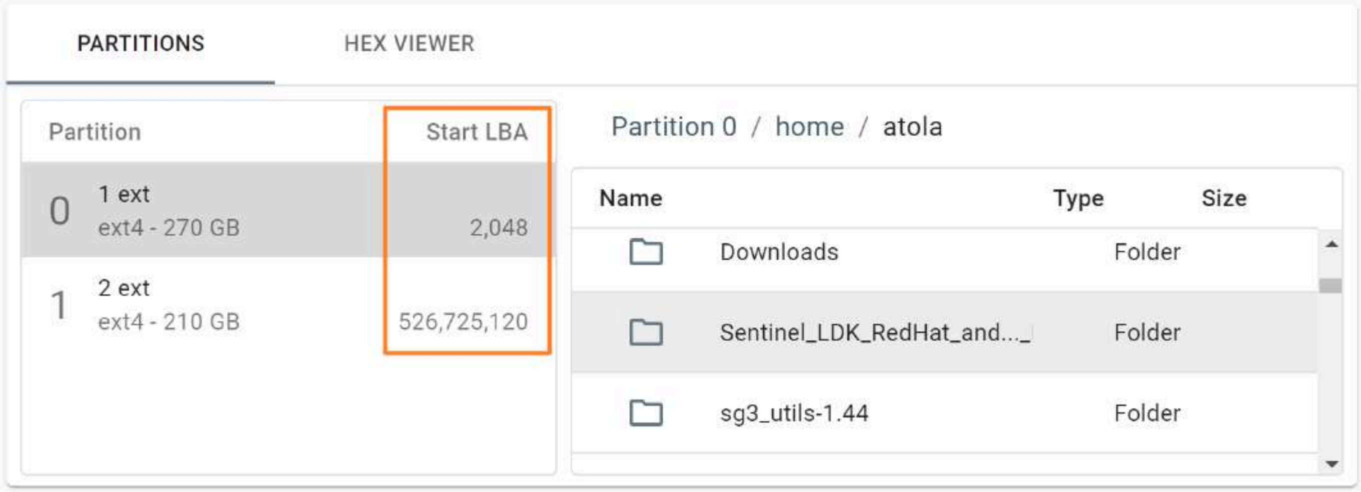
Start LBA: 0

Block size: 512 KB (Adaptec, Li...

Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD S	120 GB	
2	JAJS300M120C 30013348333	120 GB	
3	SATA SSD PH191112003195	120 GB	ext4
4	SPCC Solid State Disk 2018130300:	120 GB	
5	Patriot Burst 5680076A1EEE00402:	120 GB	MBR Unknown

When we talk about logical partitions, Start LBA refers to the logical block address where a particular partition starts in an already assembled RAID array. In this case, Start LBA of each partition is different.



Partition		Start LBA
0	1 ext ext4 - 270 GB	2,048
1	2 ext ext4 - 210 GB	526,725,120

Partition 0 / home / atola

Name	Type	Size
Downloads	Folder	
Sentinel_LDK_RedHat_and..._	Folder	
sg3_utils-1.44	Folder	

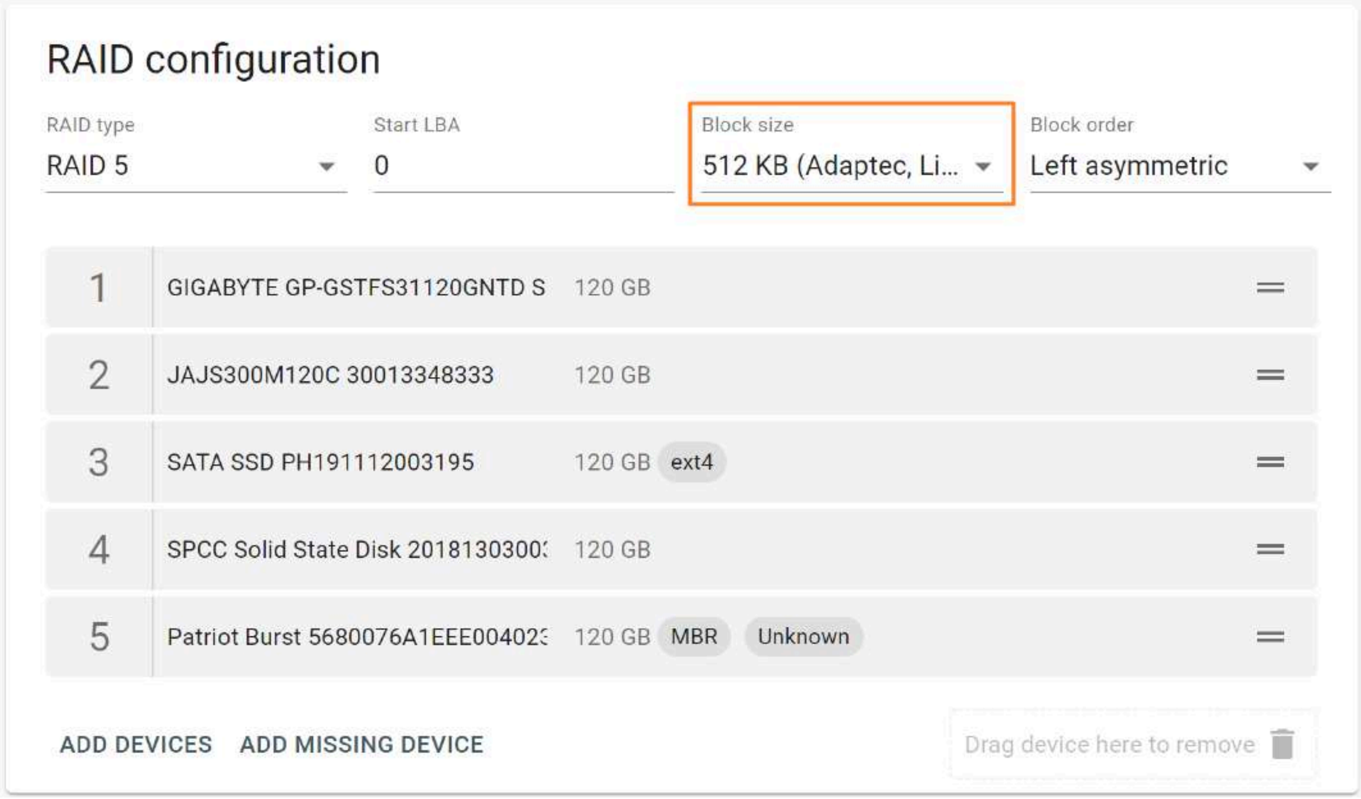
Block size

Applies to: RAID 0, RAID 10, RAID 5, RAID 6 (types that use striping method).

Some RAID types use striping method for distributing data across physical drives: data is split into consecutive logical blocks (also called “stripes” or “chunks”), which are stored on different physical storage devices.

The **Block size** parameter in TaskForce RAID module refers to the size of these logical blocks (or “stripes”) measured in bytes. TaskForce supports RAID block sizes from 512 bytes to 1 megabyte and can detect that parameter automatically using a heuristic algorithm. The most frequently used block size is 64 kilobytes.

If you know the block size of a RAID, you can select it manually from the **Block size** list in the **RAID configuration** section.



RAID configuration

RAID type: RAID 5

Start LBA: 0

Block size: 512 KB (Adaptec, Li...

Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD S	120 GB		
2	JAJS300M120C 30013348333	120 GB		
3	SATA SSD PH191112003195	120 GB	ext4	
4	SPCC Solid State Disk 2018130300:	120 GB		
5	Patriot Burst 5680076A1EEE00402:	120 GB	MBR	Unknown

Block order

Applies to: RAID 5, RAID 6 (types that use block-level striping with distributed parity).

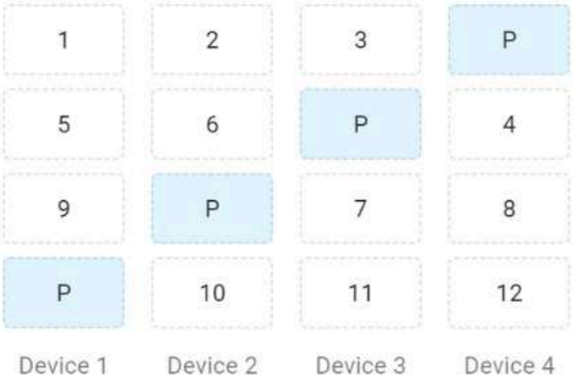
The **Block order** parameter defines the layout (or pattern), in which RAID logical blocks ("stripes") are distributed among the devices in the array. It is the sequence of writing data and parity blocks across the RAID members and depends on:

1. The direction of data blocks writing: left to right or right to left on the disk array.
2. The placement of the parity blocks: at the beginning or the end of the stripe.
3. The location of the first block of a stripe relative to the parity of the previous stripe.

For RAID 5, the Block order parameter can be:

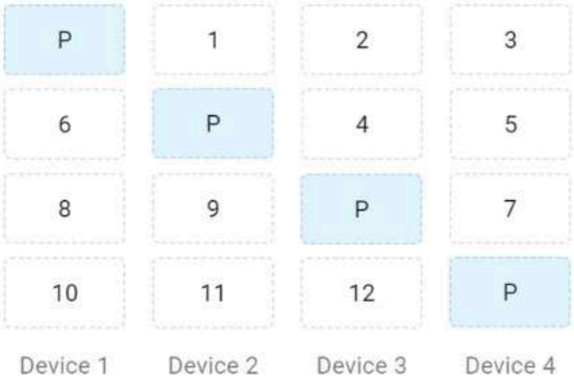
- **Left symmetric.** This is the default RAID 5 layout under Linux.
- **Left asymmetric.** This is the 'standard' RAID 5 layout.
- **Right symmetric.**
- **Right asymmetric.**

Left symmetric



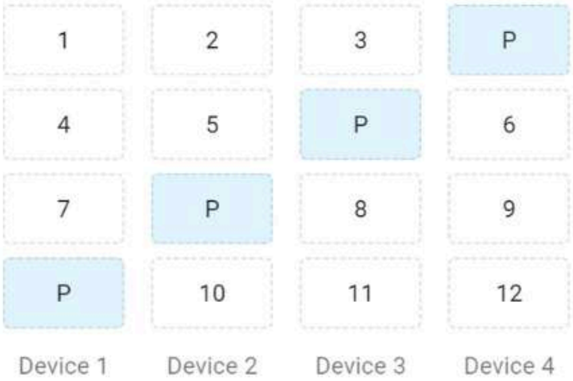
Device 1	Device 2	Device 3	Device 4
1	2	3	P
5	6	P	4
9	P	7	8
P	10	11	12

Right symmetric



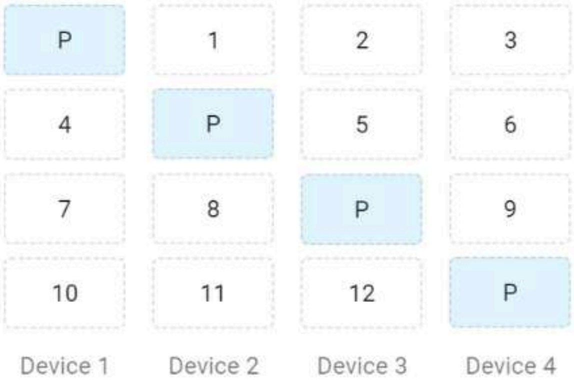
Device 1	Device 2	Device 3	Device 4
P	1	2	3
6	P	4	5
8	9	P	7
10	11	12	P

Left asymmetric



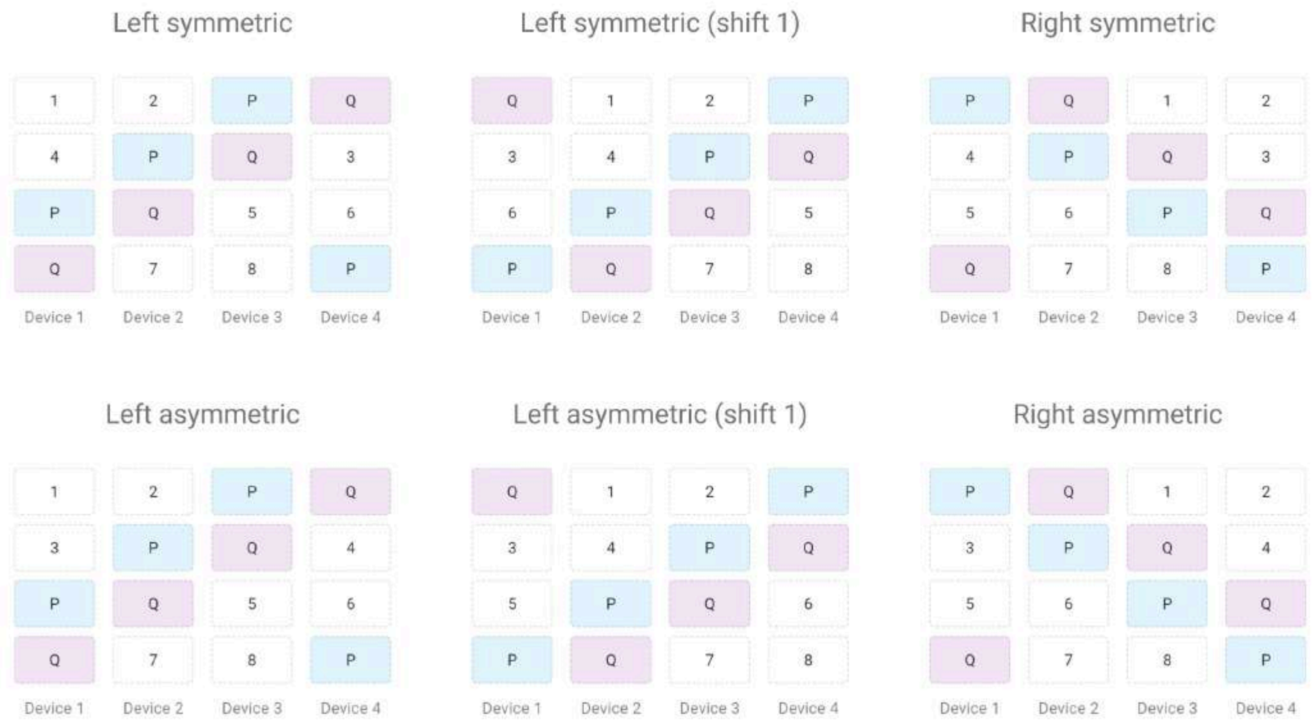
Device 1	Device 2	Device 3	Device 4
1	2	3	P
4	5	P	6
7	P	8	9
P	10	11	12

Right asymmetric



Device 1	Device 2	Device 3	Device 4
P	1	2	3
4	P	5	6
7	8	P	9
10	11	12	P

For RAID 6, the Block order parameter can be following:



Left symmetric

Device 1	Device 2	Device 3	Device 4
1	2	P	Q
4	P	Q	3
P	Q	5	6
Q	7	8	P

Left symmetric (shift 1)

Device 1	Device 2	Device 3	Device 4
Q	1	2	P
3	4	P	Q
6	P	Q	5
P	Q	7	8

Right symmetric

Device 1	Device 2	Device 3	Device 4
P	Q	1	2
4	P	Q	3
5	6	P	Q
Q	7	8	P

Left asymmetric

Device 1	Device 2	Device 3	Device 4
1	2	P	Q
3	P	Q	4
P	Q	5	6
Q	7	8	P

Left asymmetric (shift 1)

Device 1	Device 2	Device 3	Device 4
Q	1	2	P
3	4	P	Q
5	P	Q	6
P	Q	7	8

Right asymmetric

Device 1	Device 2	Device 3	Device 4
P	Q	1	2
3	P	Q	4
5	6	P	Q
Q	7	8	P

Parity block order

Applies to: RAID 6.

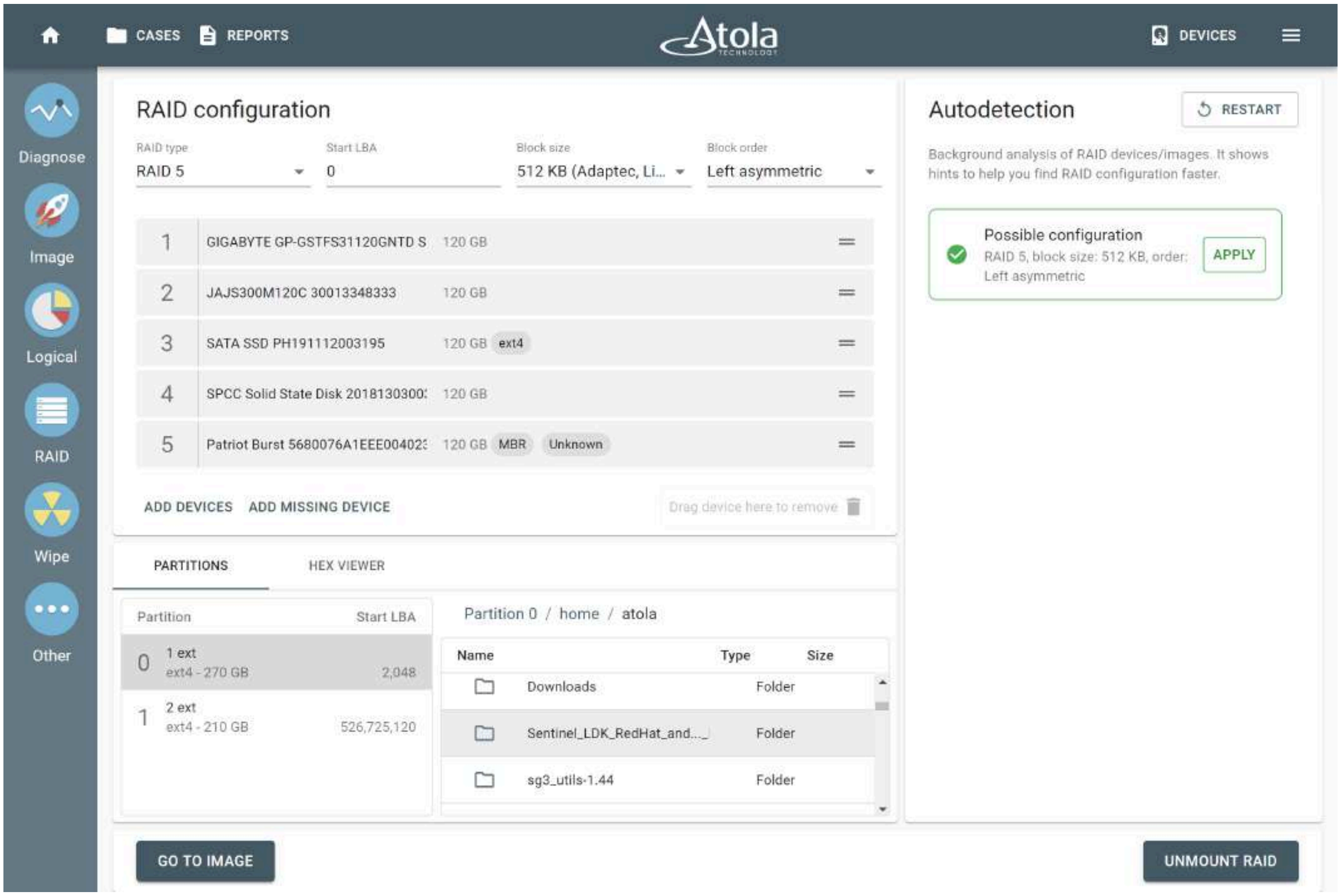
Unlike RAID 5, RAID 6 uses not one, but two types of parity blocks. The **Parity block** order parameter defines, which parity block type comes first and which follows:

- **PQ:** XOR parity block comes first, Reed-Solomon parity block comes second.
- **QP:** Reed-Solomon parity block comes first, XOR parity block comes second.

File system

After reassembling RAID using other parameters, TaskForce automatically identifies its file system and shows a preview of its partitions, folders, and files.

Currently supported file systems are: .



RAID configuration

RAID type: RAID 5
Start LBA: 0
Block size: 512 KB (Adaptec, Li...
Block order: Left asymmetric

1	GIGABYTE GP-GSTFS31120GNTD S	120 GB	
2	JAJS300M120C 30013348333	120 GB	
3	SATA SSD PH191112003195	120 GB	ext4
4	SPCC Solid State Disk 2018130300:	120 GB	
5	Patriot Burst 5680076A1EEE00402:	120 GB	MBR Unknown

Autodetection

Background analysis of RAID devices/images. It shows hints to help you find RAID configuration faster.

Possible configuration
RAID 5, block size: 512 KB, order: Left asymmetric

	Partition	Start LBA
0	1 ext ext4 - 270 GB	2,048
1	2 ext ext4 - 210 GB	526,725,120

Partition 0 / home / atola

Name	Type	Size
Downloads	Folder	
Sentinel_LDK_RedHat_and..._	Folder	
sg3_utils-1.44	Folder	

The preview of the RAID file system with partitions, folders, and files.

JBOD

JBOD is an abbreviation of "*Just a Bunch Of Drives*" and refers to a method for **concatenation** (or **spanning**) of multiple physical drives into a single logical disk with no redundancy. Data is written consecutively, from the beginning to the end of the first drive, and then spans to the second, the third and so on.

JBOD provides cost-effective storage with no performance or security benefits. It needs at least 2 drives to function. Array capacity is the sum of the capacities of its members.

If one drive fails, all data stored across the entire array may be compromised or lost, as JBOD does not implement any form of redundancy or fault tolerance.

JBOD advantages:

- Increasing capacity.
- Cost-effective storage.

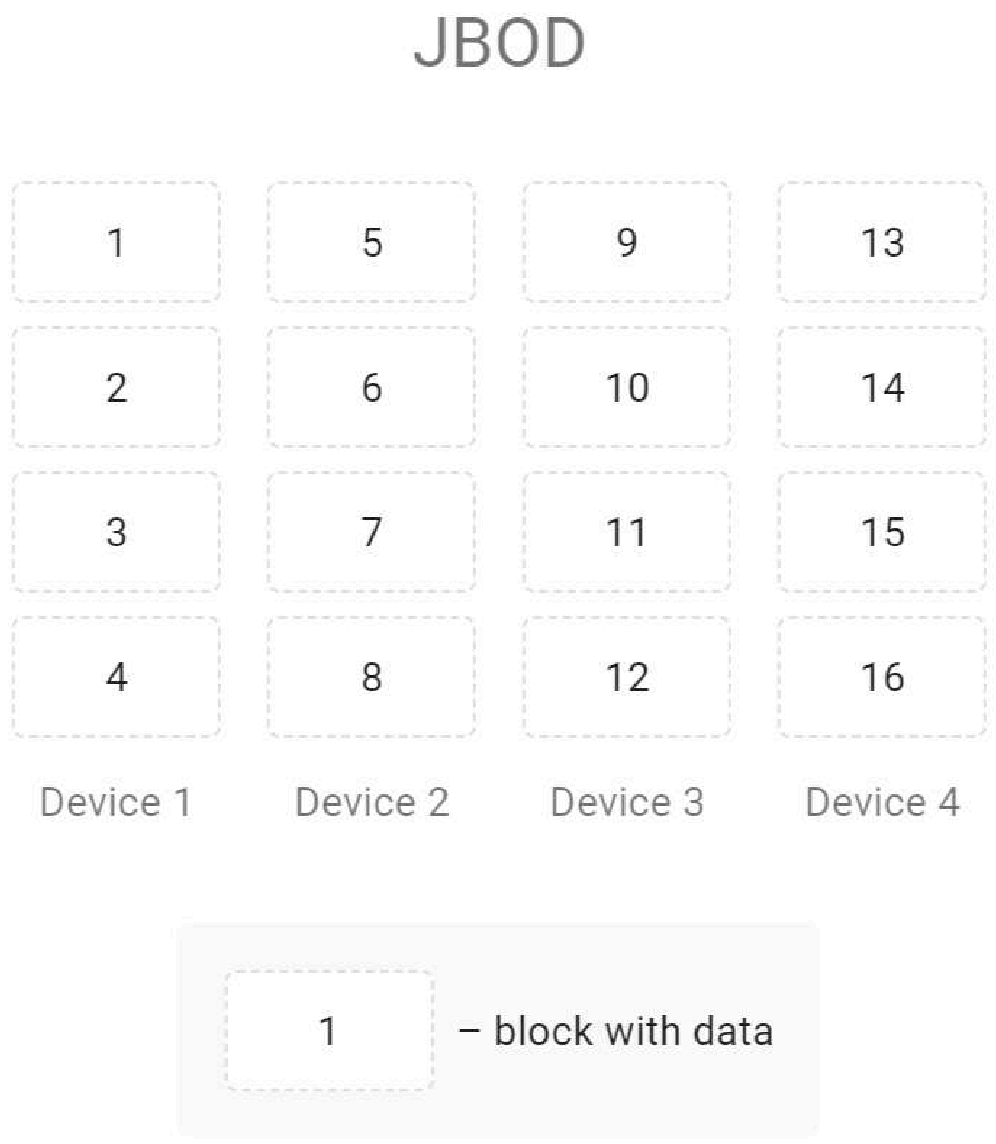
JBOD disadvantages:

- No performance benefits.
- Redundancy is not provided.

JBOD parameters

When reassembling JBOD in Atola TaskForce, the following parameters are available for manual selection:

- Device order
- Start LBA



Device 1	Device 2	Device 3	Device 4
1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

RAID 0 (Stripe)

In RAID 0, data is evenly distributed into stripes across two or more drives, forming a logical array, without parity or mirroring. RAID 0 provides higher reading and writing speed, as it can read and write multiple drives in parallel. As RAID 0 does not use mirroring or parity blocks, there’s no redundancy and fault tolerance: if one drive fails, data is lost.

RAID 0 needs at least 2 drives to function. Array volume is the sum of the capacities of the drives in the set, there’s no overhead provided by parity blocks.

RAID 0 advantages:

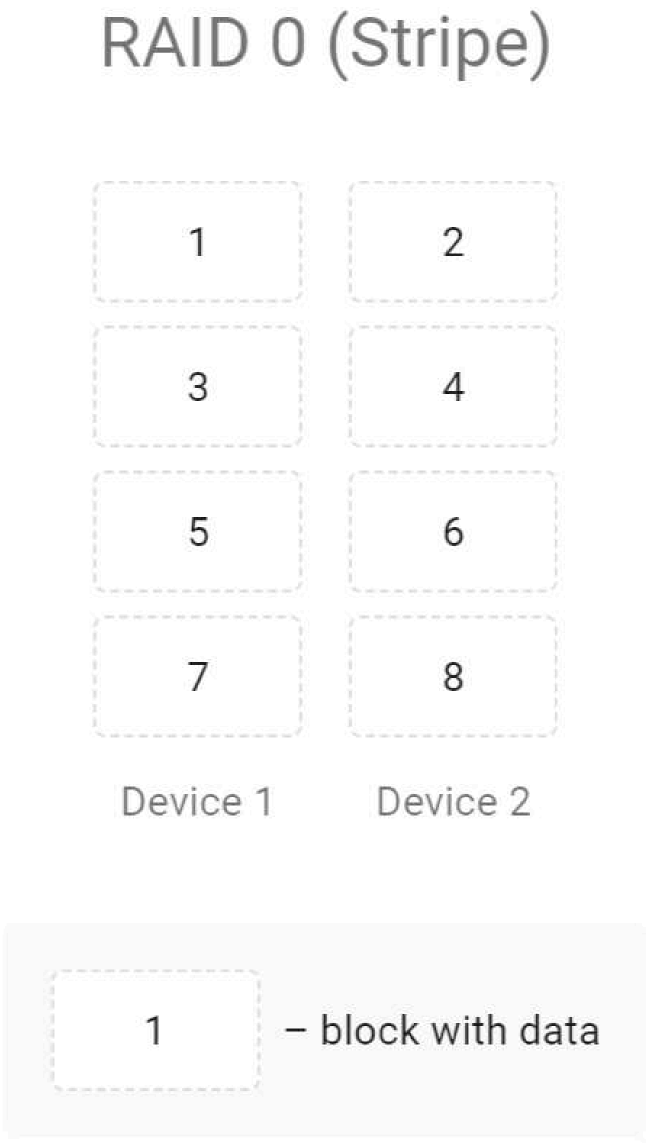
- Highest reading and writing speed.
- No overhead provided by parity blocks.
- Maximum capacity: sum of all RAID members.

RAID 0 disadvantages:

- No fault tolerance: if one drive fails, data is lost.

RAID 0 parameters

When reassembling RAID 0 in Atola TaskForce, the following parameters are available for manual selection:



- Device order
- Start LBA
- Block size

See also

- Imaging RAID 0 with unknown configuration

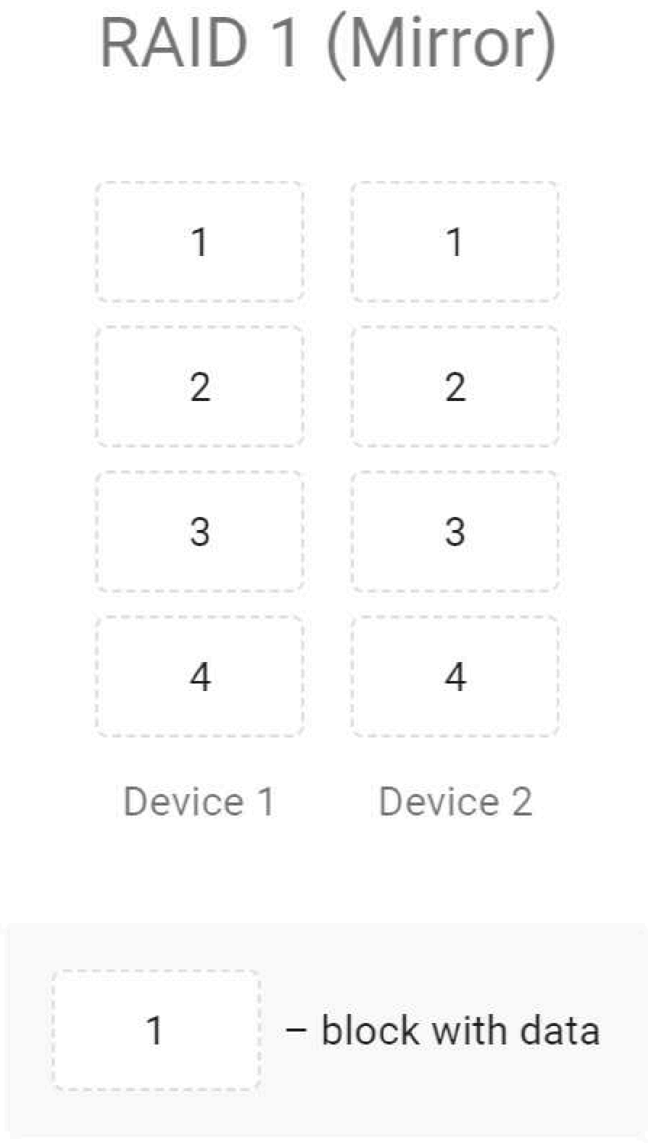
RAID 1 (Mirror)

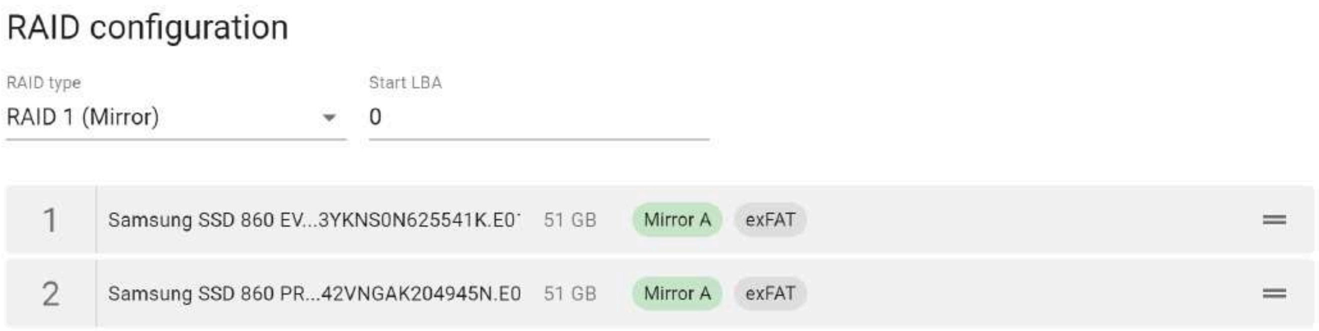
RAID 1 creates an exact copy of the drive's data (“mirror”) on another drive or drives. Thus RAID 1 usually consists of mirrored drives which are exact copies of each other. No spanning, striping, or parity is being used. The capacity of the array is limited to the size of the smallest member drive.

If one member drive fails, data is restored by copying from the mirror drive. Because of that RAID 1 can still work even if only one member drive is in good condition.

RAID 1 reads multiple drives in parallel, increasing overall reading performance. But writing speed is lower, as it takes additional time to duplicate data on the mirror drive.

When TaskForce detects a mirrored pair of devices (drives or image files), it labels both of them with the “Mirror” tag.





RAID configuration

RAID type: RAID 1 (Mirror)

Start LBA: 0

1	Samsung SSD 860 EV...3YKNS0N625541K.E0'	51 GB	Mirror A	exFAT
2	Samsung SSD 860 PR...42VNGAK204945N.E0	51 GB	Mirror A	exFAT

RAID 1 advantages:

- Improved reading speed.
- High fault tolerance. Data can be restored from the “mirror” drive.
- Simplest RAID storage system.

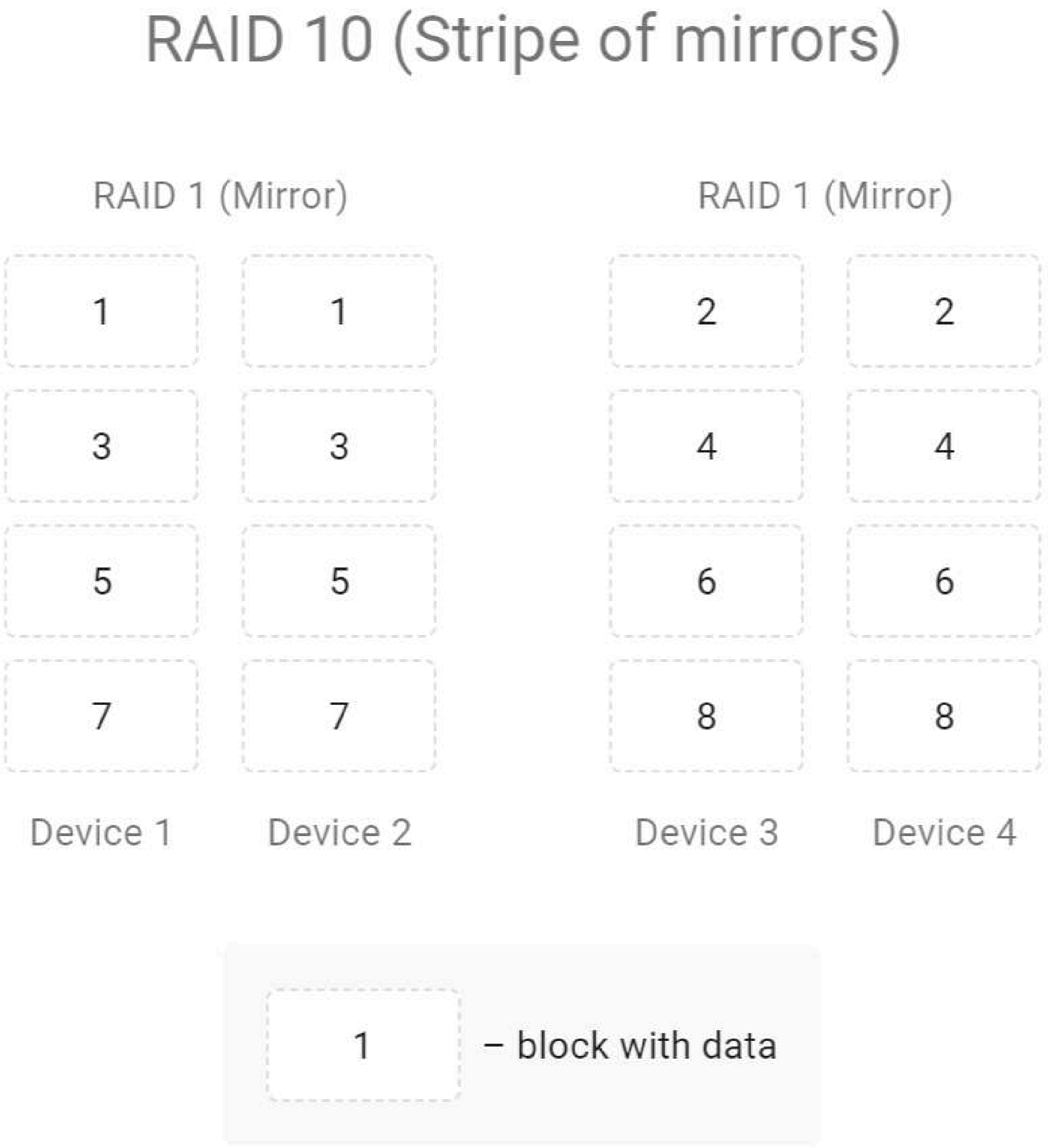
RAID 1 disadvantages:

- Storage capacity is limited to the size of the smallest member drive.
- Writing speed is lower due to data duplication.

RAID 1 parameters

When reassembling RAID 1 in Atola TaskForce, the following parameters are available for manual selection:

- Device order
- Start LBA



RAID 10 (Stripe of mirrors)

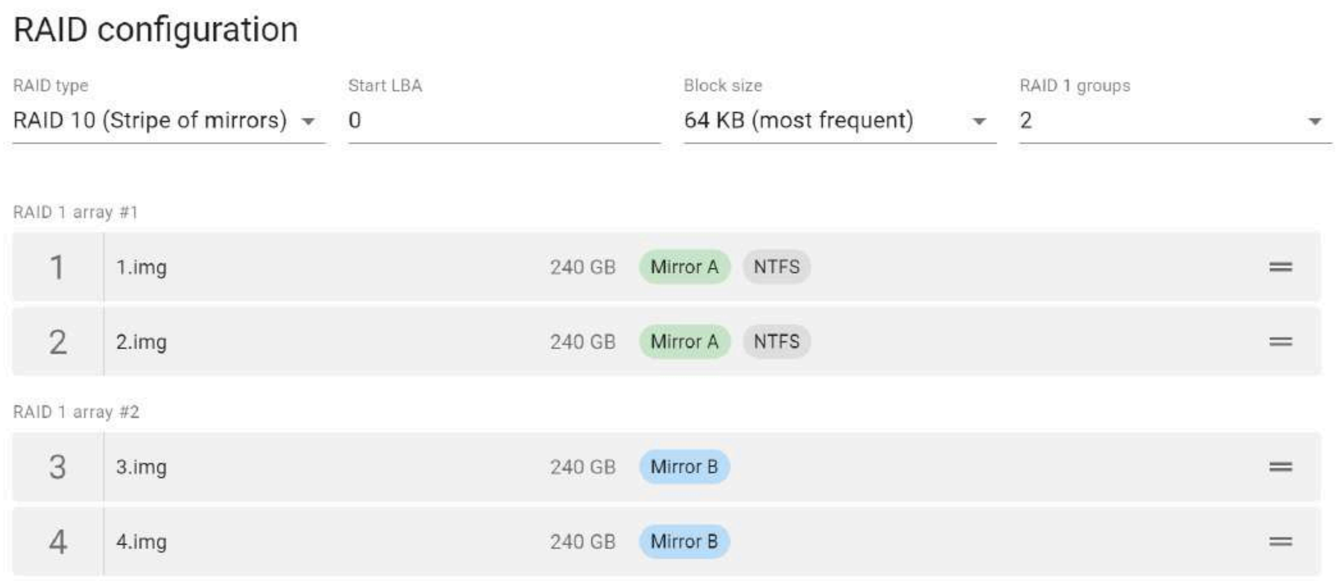
RAID 10 is called “stripe of mirrors” as it combines RAID 1 (“mirroring”) and RAID 0 (“striping”) methods within a single logical array. Data is shared between drives and duplicated. It is a RAID 0 array consisting of mirrors and thus requires a minimum of four drives: two for striping and two for storing mirrored data of each drive.

High read and write performance is achieved by striping RAID 1 mirrored segments.

If one member drive fails, data is restored by copying from the mirror drive. The overall storage capacity is reduced by 1/2 as all data is written twice.

RAID 10 typical use is highly loaded databases, email, or web servers.

When TaskForce detects a mirrored pair of devices (drives or image files), it labels both of them with the “Mirror” tag.



RAID configuration

RAID type: RAID 10 (Stripe of mirrors)

Start LBA: 0

Block size: 64 KB (most frequent)

RAID 1 groups: 2

RAID 1 array #1

1	1.img	240 GB	Mirror A NTFS
2	2.img	240 GB	Mirror A NTFS

RAID 1 array #2

3	3.img	240 GB	Mirror B
4	4.img	240 GB	Mirror B

RAID 10 advantages:

- High reading and writing speed.
- High fault tolerance. Data can be restored from the “mirror” drive.

RAID 10 disadvantages:

- Storage capacity is reduced by 1/2 as all data is written twice.
- Limited scalability.

RAID 10 parameters

When reassembling RAID 10 in Atola TaskForce, the following parameters are available for manual selection:

- Device order
- Start LBA
- Block size
- RAID 1 groups

See also

- Reassembly and imaging of RAID 10

RAID 5 (Distributed parity)

In RAID 5, data in the form of block-level stripes is evenly distributed across at least 3 drives, along with parity information which is used to restore data.

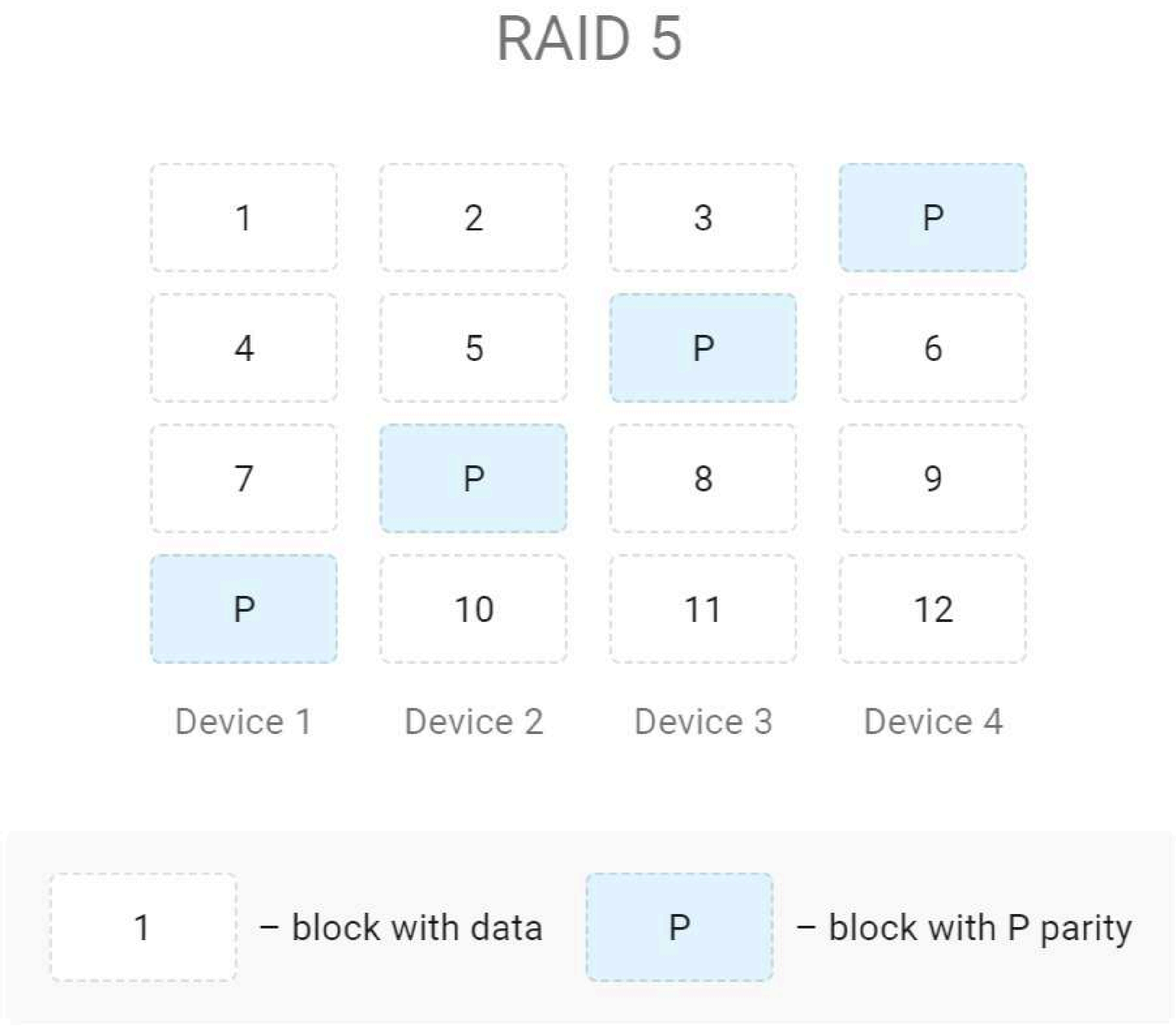
RAID 5 can still operate without one of its members. If one drive fails, its data is calculated from the parity blocks distributed across other members. Atola TaskForce can detect the parameters of the RAID 5 array with two damaged drives and successfully image such RAIDs regardless of errors.

The storage capacity of RAID 5 is reduced due to parity blocks.

Reading and writing speed is high since RAID 5 can read from and write to all array members in parallel.

RAID 5 is typically used for file servers, database servers, and application servers.

RAID 5 can have different layouts, or block orders, depending on the pattern in which RAID 5 data blocks (“stripes”) and parity blocks are distributed among the devices in the array. The layout is defined by:



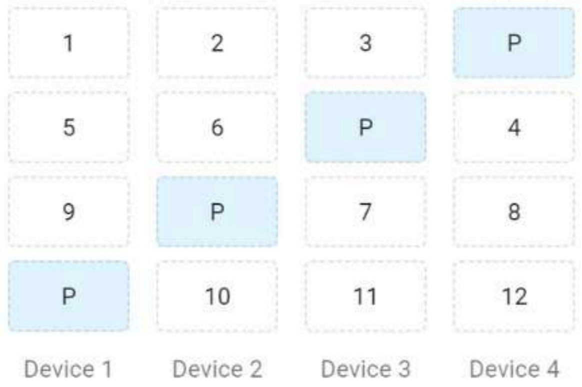
Device 1	Device 2	Device 3	Device 4
1	2	3	P
4	5	P	6
7	P	8	9
P	10	11	12

1. The direction of data blocks writing: left to right or right to left on the disk array.
2. The placement of the parity blocks: at the beginning or end of a stripe.
3. The location of the first block of a stripe relative to the parity of the previous stripe.

There are four RAID 5 layouts (or block orders):

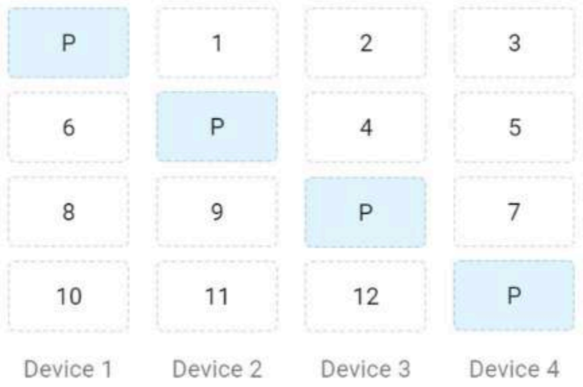
1. Left symmetric.
2. Right symmetric.
3. Left asymmetric.
4. Right asymmetric.

Left symmetric



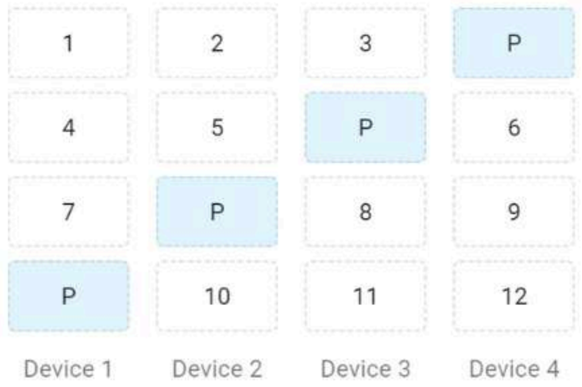
Device 1	Device 2	Device 3	Device 4
1	2	3	P
5	6	P	4
9	P	7	8
P	10	11	12

Right symmetric



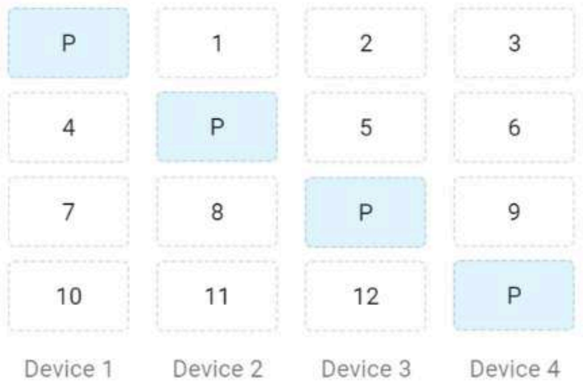
Device 1	Device 2	Device 3	Device 4
P	1	2	3
6	P	4	5
8	9	P	7
10	11	12	P

Left asymmetric



Device 1	Device 2	Device 3	Device 4
1	2	3	P
4	5	P	6
7	P	8	9
P	10	11	12

Right asymmetric



Device 1	Device 2	Device 3	Device 4
P	1	2	3
4	P	5	6
7	8	P	9
10	11	12	P

RAID 5 advantages:

- High read speed but slightly lower than RAID 0 because of the overhead from parity calculations and distribution across all disks.
- High fault tolerance. Data from one failed drive can be restored using parity information, stored on other array members.

RAID 5 disadvantages:

- Storage capacity is reduced due to parity blocks. Space efficiency is described by formula: *1 − 1/n*, where *n* is the number of devices in an array. For instance, for RAID 5 consisting of 5 drives with total capacity of 1 TB, available space will be reduced by 1/5 (or 200 MB), to 800 MB.
- Moderate write speed due to the need for parity calculations and writing both data and parity information.

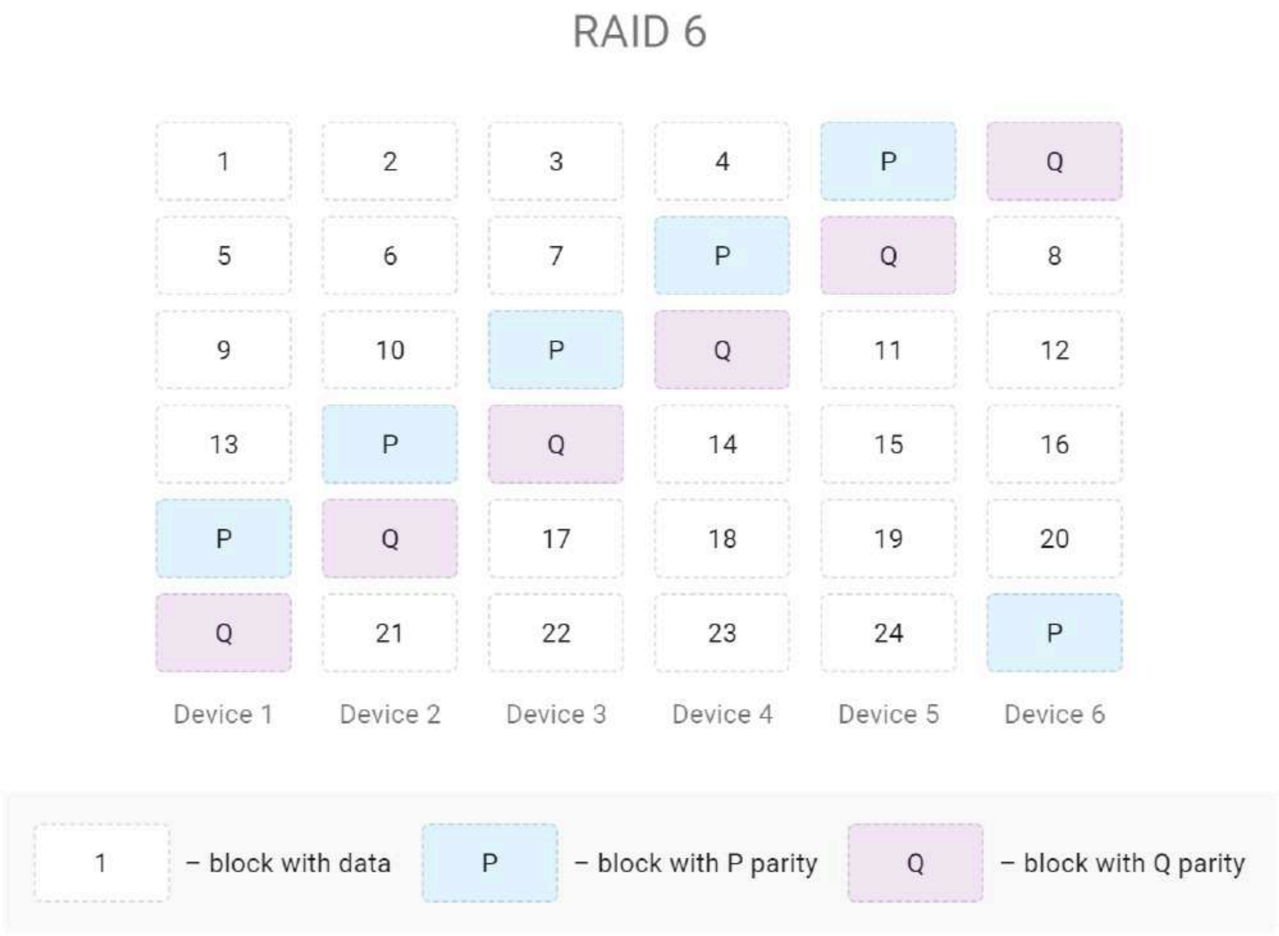
RAID 5 parameters

When reassembling RAID 5 in Atola TaskForce, the following parameters are available for manual selection:

- Device order
- Start LBA
- Block size
- Block order

See also

- RAID 5 with unknown configuration
- RAID 5 with a missing drive
- Imaging RAID 5 array with 2 damaged drives



RAID 6

Device 1	Device 2	Device 3	Device 4	Device 5	Device 6
1	2	3	4	P	Q
5	6	7	P	Q	8
9	10	P	Q	11	12
13	P	Q	14	15	16
P	Q	17	18	19	20
Q	21	22	23	24	P

1 – block with data P – block with P parity Q – block with Q parity

RAID 6 (Dual parity)

RAID 6 uses block-level striping (data is shared between drives) with two parity blocks, instead of one, distributed across all member disks. This gives extra redundancy to an array: RAID 6 can read and write data even if two drives fail at the same time.

This RAID type needs at least 4 drives to function. Storage capacity is reduced because of the dual parity scheme.

RAID 6 is typically used for large file storage, file servers, database servers, app servers.

Thanks to RAID 6 extra redundancy coming from two parity block types, TaskForce can rebuild a RAID 6 array even if two of its members are missing or damaged.

RAID 6 can have different layouts, or block orders, depending on the pattern in which RAID 6 data blocks (“stripes”) and parity blocks are distributed among the devices in the array. The layout is defined by:

1. The direction of data blocks writing: left to right or right to left on the disk array.
2. The placement of the parity blocks: at the beginning or end of the stripe.
3. Parity block order.
4. The location of the first block of a stripe relative to the parity of the previous stripe.

RAID 6 advantages:

- Very high data fault tolerance.
- Data can be restored even if two drives fail.

- High reading speed similar to RAID 5, but can be slightly slower due to additional parity calculations.

RAID 6 disadvantages:

- Storage capacity is reduced because of the dual parity scheme.
- Reduced writing speed due to the usage of two types of parity blocks.
- Minimum 4 drives needed.

RAID 6 parameters

When reassembling RAID 6 in Atola TaskForce, the following parameters are available for manual selection:

- Device order
- Start LBA
- Block size
- Block order
- Parity block order

RAID read and write speeds

The different RAID levels offer various trade-offs in terms of read and write speed, redundancy, and storage efficiency. Below is a comparison of RAID 0, 1, 10, 5, and 6 regarding their read and write speeds.

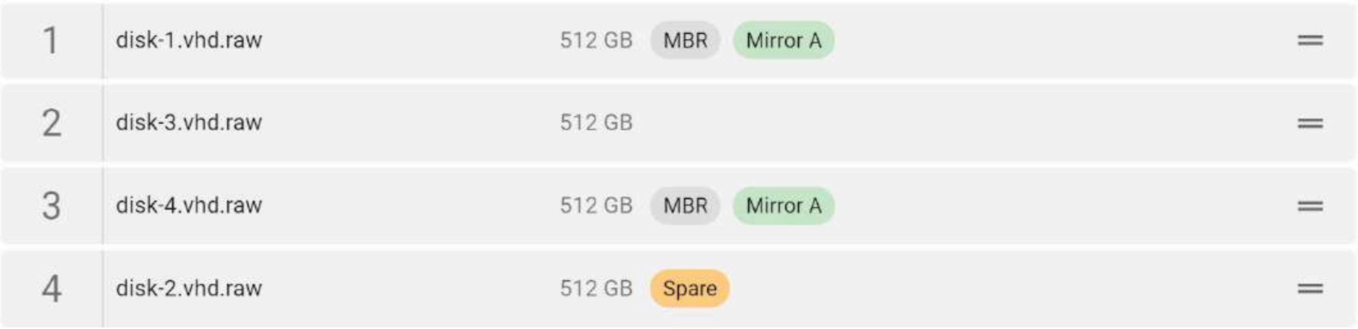
RAID type	Read Speed	Write Speed
RAID 0	**Highest** because data is striped across all disks, allowing simultaneous reads.	**Highest** because data is striped, allowing simultaneous writes. No parity calculation delay.
RAID 1	**High** because data can be read from either of the mirrored disks, potentially doubling the read rate compared to a single disk.	**Lower** than RAID 0 because all data must be written to two disks, causing a slight overhead.
RAID 10	**High**, similar to RAID 1 because it combines striping and mirroring, offering improved read rates through simultaneous disk reads.	**Moderate to High** because data is mirrored across pairs, but the striping allows for higher write speeds compared to just RAID 1.
RAID 5	**High** but slightly lower than RAID 0 because of the overhead from parity calculations and distribution across all disks.	**Moderate** due to the need for parity calculations and writing both data and parity information, which introduces some overhead.
RAID 6	**High**, similar to RAID 5, but can be slightly slower due to additional parity calculations.	**Lower** than RAID 5 because it requires two parity blocks to be written, further increasing the overhead compared to RAID 5.

Key Points:

- **RAID 0** offers the best performance both in reads and writes but no redundancy.
- **RAID 1** provides good read performance and redundancy at the cost of available capacity.
- **RAID 10** combines the benefits of RAID 0 and RAID 1, offering a good balance of speed and redundancy.
- **RAID 5 and RAID 6** offer a good balance between storage efficiency, read speed, and redundancy, with RAID 6 providing higher fault tolerance at the cost of write speed due to additional parity calculations.

RAID tags and what they mean

When reassembling a RAID in TaskForce 2, start by selecting the drives and/or images it consists of. The system reads the first 3 million sectors of each RAID member, analyzes the data and compares the members against each other. TaskForce 2 then labels the RAID members with appropriate tags to help you identify the condition, relation and possible position.



1	disk-1.vhd.raw	512 GB	MBR Mirror A
2	disk-3.vhd.raw	512 GB	
3	disk-4.vhd.raw	512 GB	MBR Mirror A
4	disk-2.vhd.raw	512 GB	Spare

Spare

The **Spare** tag informs you that 99.95% of the drive's initial 3M sectors are filled with zeros.

A spare (aka hot spare) drive in RAID arrays is used as a standby drive reserved to replace a RAID member in case it fails: in this situation the RAID controller uses redundancy data to reconstruct the data from the failed disk to the spare one. Spare drives are used in RAID 1, RAID 5 and RAID 6.

Mirror

With the **Mirror** tag, TaskForce 2 informs you that 99.5% out of the analyzed 3M sectors are identical to the same sectors on a different RAID member. It works as a hint that you are dealing with a RAID 1, RAID 10 or RAID 50.

MBR

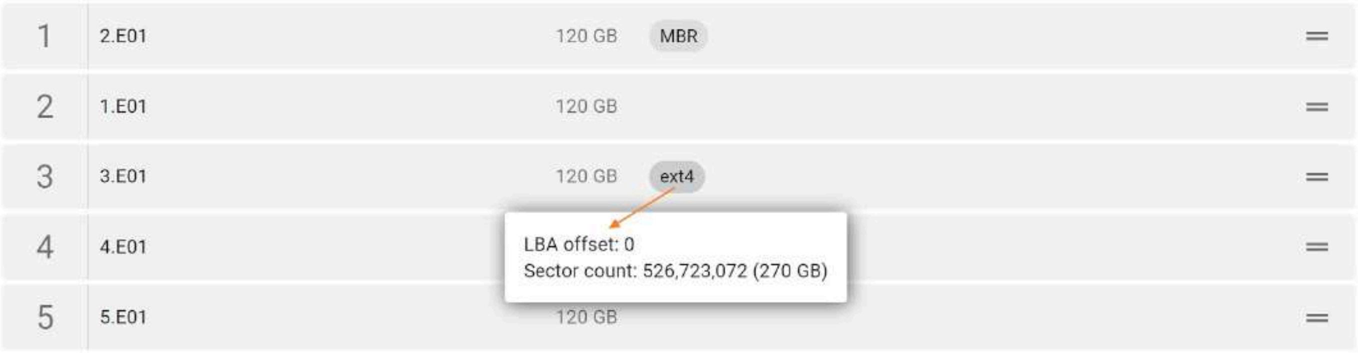
MBR (Master Boot Record) points to the drive(s) that contain an MBR. Therefore, it is likely that the drive with detected MBR can be placed first in the given array.

File system tags

The initial 3M sectors of each drive/image are analyzed to identify a boot sector of any known file system. When a partition boot sector is detected, the corresponding file system tag is added. To see LBA offset and sector count of the partition, hover mouse cursor over the tag.

Supported file system tags: NTFS, ext4/3/2, APFS, HFS, HFS+, exFAT, FAT32, FAT16, XFS.

Additionally, **Unknown** tag may appear if the file system identification is not supported yet.

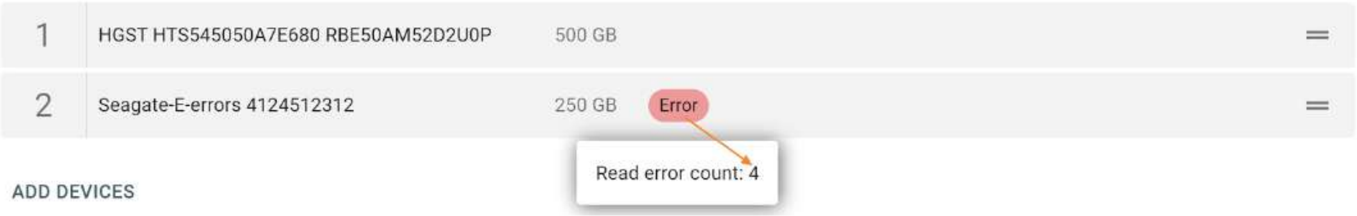


1	2.E01	120 GB	MBR
2	1.E01	120 GB	
3	3.E01	120 GB	ext4
4	4.E01		
5	5.E01	120 GB	

LBA offset: 0
Sector count: 526,723,072 (270 GB)

Error

The **Error** tag informs you whether there are read errors encountered in the process of RAID autodetection. To see the exact number of encountered errors, hover mouse over the **Error** tag to get the tooltip.



1	HGST HTS545050A7E680 RBE50AM52D2U0P	500 GB	
2	Seagate-E-errors 4124512312	250 GB	Error

Read error count: 4

RAID cheat sheet

When RAID Autodetection finds nothing

Follow these tips if the automatic RAID reassembly module doesn't detect a RAID configuration.

If you know the RAID configuration

If you know the exact RAID configuration, skip waiting for Autodetection to complete and manually select the RAID parameters instead.

If you only know the device order

If you know the exact order of the RAID members, select them in the correct sequence: the RAID Autodetection module prioritizes the device order specified by the user.

If you know the RAID offset (Start LBA)

If you're aware of a specific disk offset for the RAID members, specify the LBA in the Autodetection module's settings (look for the gear icon). This will enable the Autodetection to identify a suitable RAID configuration in cases where it previously failed.

Synology NAS RAID detection

If you are certain the devices belong to a Synology NAS RAID but the RAID configuration isn’t detected right away and Autodetection is still running, consider the following possibilities:

- One or more selected devices may not be part of this RAID array.
- One or more devices could be missing from the array.

To resolve this, stop the Autodetection process and try selecting a different combination of drives that belong to the RAID array.

Multiple configurations found

If the Autodetection module suggests multiple possible RAID configurations, the best match will always appear first.

Additionally, pay attention to the small tags displaying the accuracy percentage next to the RAID partitions — the higher the percentage, the better the match.

Parity order in RAID 6

For RAID 6, the 'Parity Order' parameter is only relevant when a device is missing.

Handling RAID 5 / RAID 6 with missing devices

If you know that a device is missing from your RAID 5 or RAID 6, click ‘Add missing device’ to speed up the Autodetection process.

For RAID 6, you can specify up to two missing devices.

Exclude ‘Spare’ devices

RAID members marked with the ‘Spare’ tag most likely contain only zeroes. It's recommended to remove these devices from the list by dragging them to the bin icon.

RAID configuration not detected

If the Autodetection module is unable to find a valid RAID configuration, try adjusting the parameters manually.

To help you evaluate the validity of the applied configuration, TaskForce displays a small evaluate the validity of next to each partition.

If a file system is not currently supported, an Unknown tag may appear next to the corresponding RAID member.

Tricky cases

RAID member s tagged with ‘Error’

If a RAID member is marked with an **Error** tag:

- Image that drive first, then attempt to reassemble the RAID using the acquired image.
- For **RAID 5** or **RAID 6**, remove the device with ‘Error’ from the list, then click ‘Add missing device’. TaskForce will use redundancy to rebuild the RAID.
- If it’s **RAID 10**, remove the faulty from the list. TaskForce will automatically use the mirrored copy to rebuild the array.

Imaging RAID takes too long

RAID capacity can exceed dozens of terabytes, making full physical imaging a time-consuming process.

To speed up access to critical data, start with logical imaging using smart filters to extract only the files of interest. Your can perform a full physical imaging later by clicking the ‘Go to image’ button.

Not enough drive ports for all RAID members

If you’re dealing with a large array and don't have enough drive ports for all RAID members:

1. image some of the drives to image files.
2. Go to **RAID** > **Select source device** > **Files** > **Select files** and use these image files instead of physical drives.

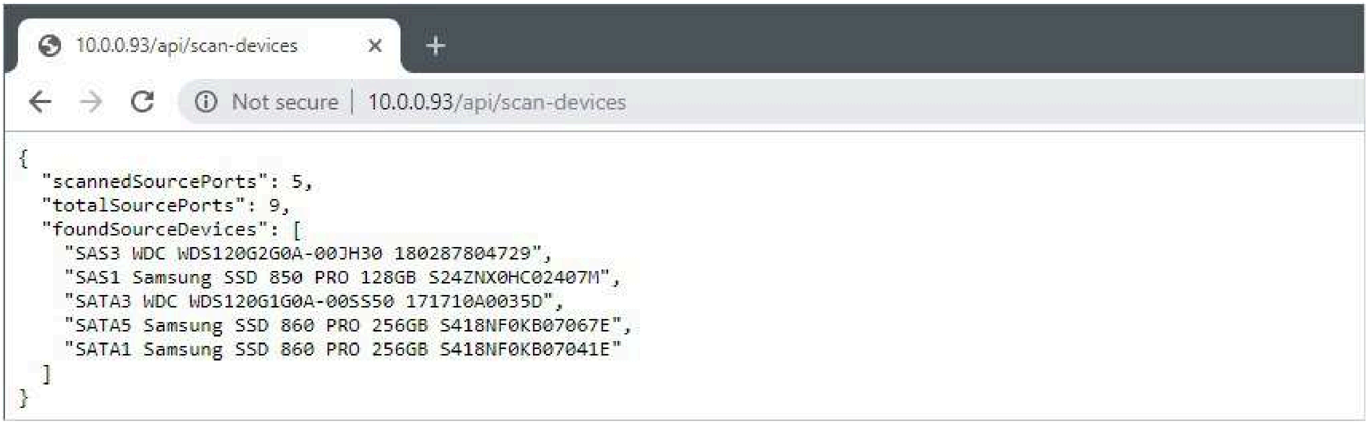
Using Web API in a browser

Web API is built into TaskForce 2, and it helps optimize your workflow in many ways.

Web API is extremely handy as it allows you to use it in scripts, via CLI tools like curl, and simply by typing commands in the browser address bar.

Here's how to use Web API in a browser:

1. Scan devices plugged to all source ports. The command powers up all ports and returns the list of drive on each port in Source mode as well as the model and the serial number of the drive on each port.

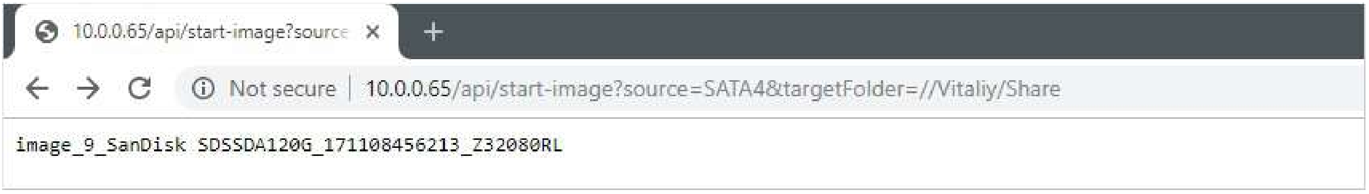


```
10.0.0.93/api/scan-devices
```

```
{
  "scannedSourcePorts": 5,
  "totalSourcePorts": 9,
  "foundSourceDevices": [
    "SAS3 WDC WDS120G2G0A-00JH30 180287804729",
    "SAS1 Samsung SSD 850 PRO 128GB S24ZNX0HC02407M",
    "SATA3 WDC WDS120G1G0A-00SS50 171710A0035D",
    "SATA5 Samsung SSD 860 PRO 256GB S418NF0KB07067E",
    "SATA1 Samsung SSD 860 PRO 256GB S418NF0KB07041E"
  ]
}
```

Devices identification.

2. Start imaging a source drive plugged into TaskForce 2 SATA 4 port.

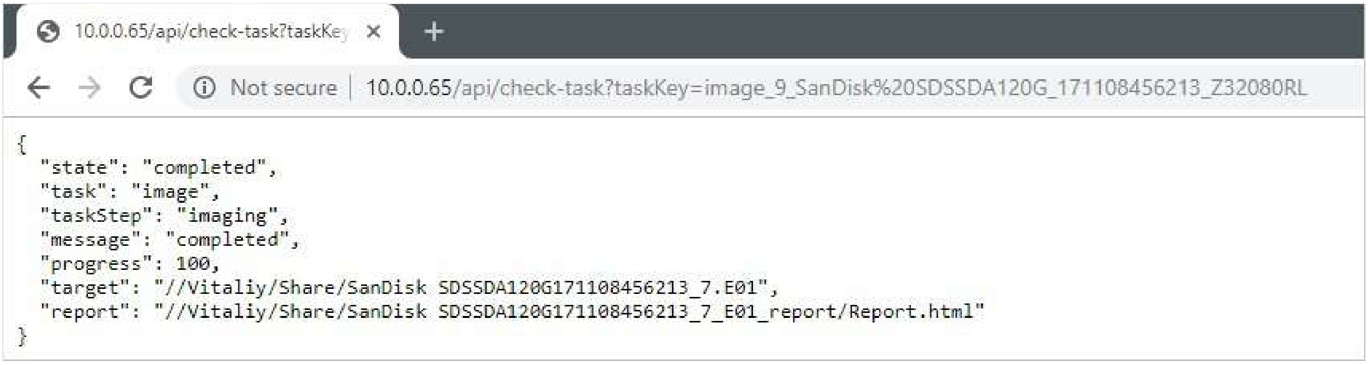


```
10.0.0.65/api/start-image?source=SATA4&targetFolder=//Vitaliy/Share
```

```
image_9_SanDisk SDSSDA120G_171108456213_Z32080RL
```

Start imaging.

3. Track imaging session status using task key received in response to the command above.


10.0.0.65/api/check-task?taskKey
Not secure
10.0.0.65/api/check-task?taskKey=image_9_SanDisk%20SDSSDA120G_171108456213_Z32080RL

```
{
  "state": "completed",
  "task": "image",
  "taskStep": "imaging",
  "message": "completed",
  "progress": 100,
  "target": "//Vitaliy/Share/SanDisk SDSSDA120G171108456213_7.E01",
  "report": "//Vitaliy/Share/SanDisk SDSSDA120G171108456213_7_E01_report/Report.html"
}
```

Check task status.

For more information about these and other commands, see API specification that we made available to public.

Instantly starting 16 imaging sessions using Web API

Imagine you have 16 TaskForce SATA and SAS ports switched to Source mode and source drives plugged into them. Now you can instantly launch 16 imaging sessions simply starting the script.

Python script utilizes **/start-image** API request and prints task keys of all launched imaging sessions.

```
import sys

if sys.version_info[0] < 3:
    raise Exception("Please use Python 3 to run this script")

import urllib.request

ports = ["SATA1", "SATA2", "SATA3", "SATA4", "SATA5", "SATA6", "SATA7", "SATA8",
         "SAS1", "SAS2", "SAS3", "SAS4", "SAS5", "SAS6", "SAS7", "SAS8"]
tasks = []
errors = {}

for port in ports:
    try:
        res = urllib.request.urlopen("http://10.0.0.4/api/start-image?source=%s&targetFolder=//Vitaliy/Share" % (port))
        tasks.append(res.read().decode('utf-8'))
    except urllib.error.HTTPError as e:
        errors[port] = e.read()

print("IDs of started imaging tasks:")
print('\n'.join(tasks))
```

The script works in any operating system. To run, perform the following actions:

1. Save the script into image16.py file.
2. Replace **10.0.0.4** with IP address of your TaskForce 2.
3. Replace **//Vitaliy/Share** with your shared network folder path.
4. Execute the script in the console: `python image16.py` .

For more information about these and other commands, see API specification that we made available to public.

Autostart image analysis when imaging is completed

With TaskForce 2, you can track the status of the started imaging sessions using **/check-task** API request. It reports the imaging progress enabling you (or your code) to notice when the task gets completed. Once this notification is received, it makes perfect sense to automatically start the forensic analysis of the target image.

Powershell script below shows how one can create this kind of automation flow:

1. Start imaging a source drive on TaskForce SATA port 4 to the target folder **\\Vitaliy\Share**.
2. Wait for imaging completion using **/check-task**.
3. Launch Autopsy Ingest via command-line when the target image is ready.

> Important: Instead of Autopsy, you are free to use any Magnet Forensics products, X-Ways Forensics, or any other forensic analysis toolkit that supports console launch with arguments.

```
try {
    $r = Invoke-WebRequest "http://10.0.0.65/api/start-image?source=SATA4&targetFolder=\\Vitaliy\Share"
}
catch {
    Write-Output "$($_.Exception.Message)"
    exit $_.Exception.Response.StatusCode
}

$taskKey = $r.Content
do {
    $check = (Invoke-WebRequest "http://10.0.0.65/api/check-task?taskKey=$taskKey").Content | ConvertFrom-Json
    Start-Sleep -s 1
} while ($check.state -eq "progress")

$windowsPath = "C:\Share\" + ($check.target -replace '[\/]', '\' | Split-Path -leaf)
$caseName = "Case123"
$autopsyArguments = '" --createCase --caseName="' + $caseName + ' --caseBaseDir="C:\Work\Cases"'
                  + ' --addDataSource --dataSourcePath="' + $windowsPath + '" --runIngest --generateReports'

Start-Process -FilePath "C:\Program Files\Autopsy\bin\autopsy64.exe" -ArgumentList $autopsyArguments
```

The script works in Windows with Powershell. To run it, please perform the following actions:

1. Install Autopsy.
2. Create C:\Share folder.
3. Save the script into image.ps1 file.
4. Replace **10.0.0.65** with IP address of your TaskForce 2.
5. Replace **\\Vitaliy\Share** with your shared network folder path.
6. Execute the script in the console: `powershell -ExecutionPolicy ByPass -File image.ps1`.

> Autopsy Ingest v4.11 does not work with network file paths from the command line. That’s why this example shows a shared folder located at PC where PowerShell script is executed. Therefore \\Vitaliy\Share points to C:\Share folder.

For more information about these and other commands, see API specification that we made available to public.

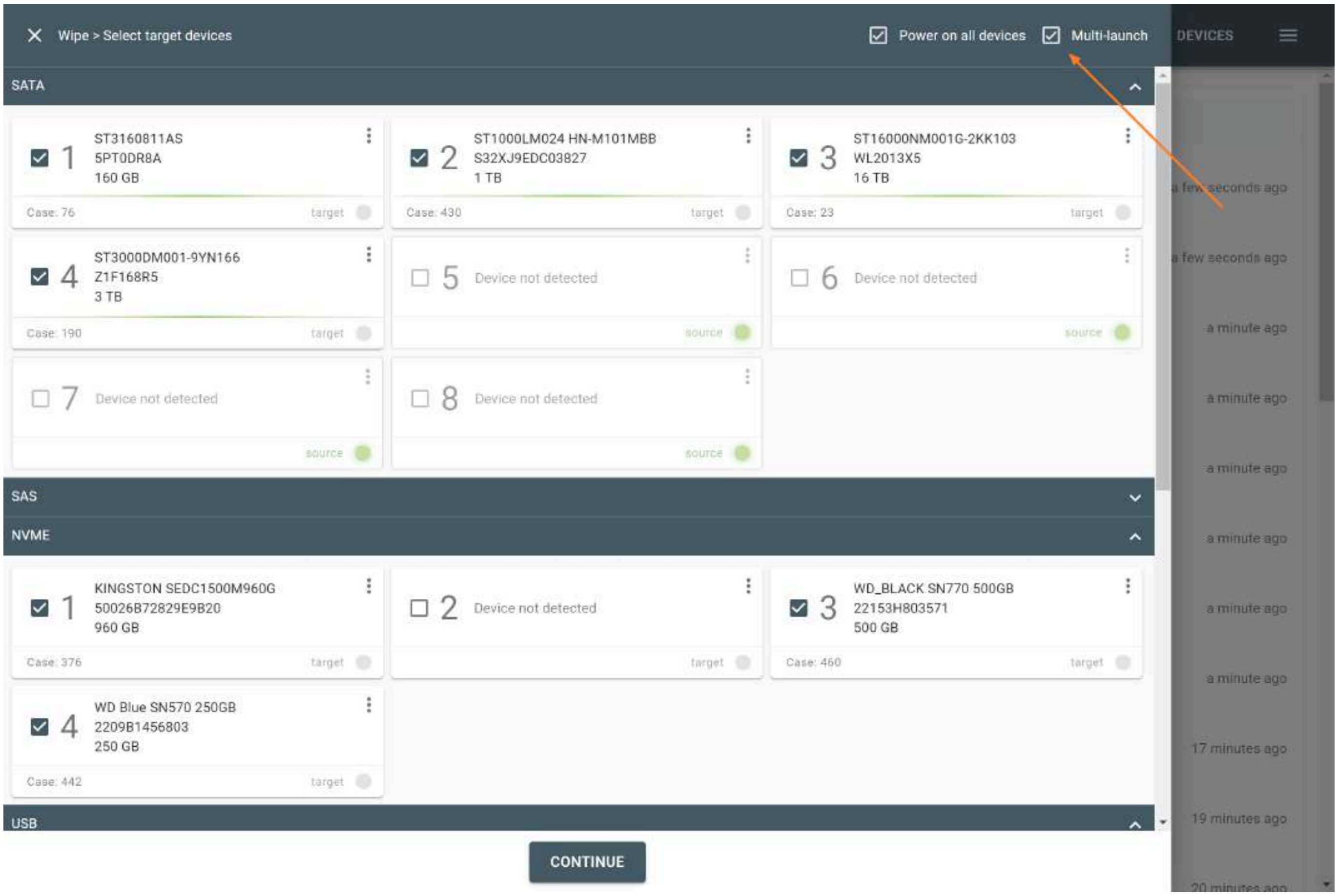
Multi-launch of single-device operations

To wipe a bunch of target drives for subsequent imaging sessions or verify hash values on multiple drives in your archive, use multi-launch functionality in TaskForce 2.

The function is currently supported for single-drive tasks: Wiping, Diagnostics, Hashing.

To wipe multiple drives:

1. On the left, click **Wipe**.
2. On the **Select target devices** panel, enable **Multi-launch** and select the drives.



Wipe > Select target devices

☑ Power on all devices ☑ Multi-launch

SATA

☑ 1 ST3160811AS 5PT0DR8A 160 GB — Case: 76 — target

☑ 2 ST1000LM024 HN-M101MBB S32XJ9EDC03827 1 TB — Case: 430 — target

☑ 3 ST16000NM001G-2KK103 WL2013X5 16 TB — Case: 23 — target

☑ 4 ST3000DM001-9YN166 Z1F168R5 3 TB — Case: 190 — target

□ 5 Device not detected — source

□ 6 Device not detected — source

□ 7 Device not detected — source

□ 8 Device not detected — source

SAS

NVME

☑ 1 KINGSTON SEDC1500M960G 50026B72829E9B20 960 GB — Case: 376 — target

□ 2 Device not detected — target

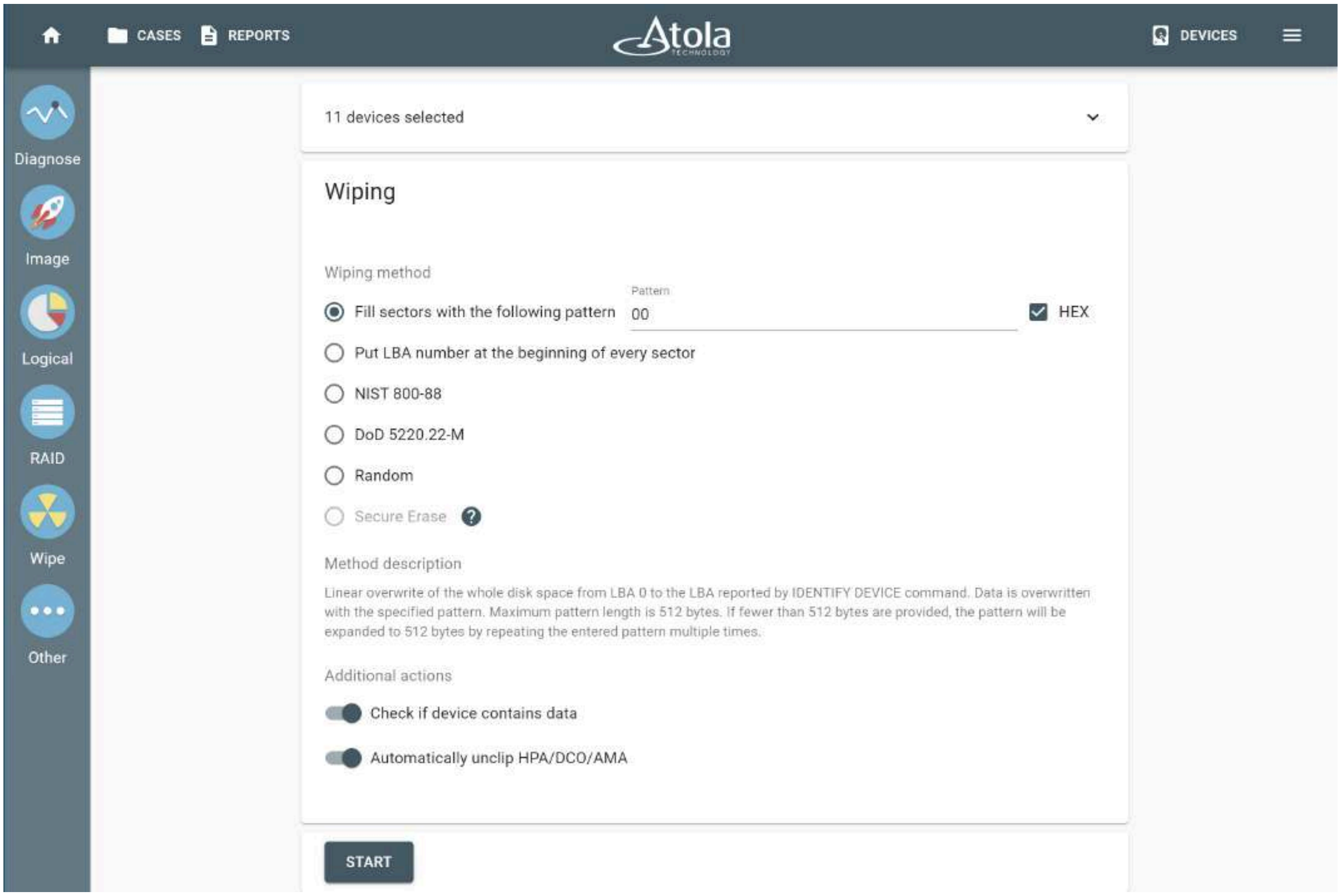
☑ 3 WD_BLACK SN770 500GB 22153H803571 500 GB — Case: 460 — target

☑ 4 WD Blue SN570 250GB 2209B1456803 250 GB — Case: 442 — target

USB

The Multi-launch option.

3. On the wiping settings page, adjust the sessions parameters. They will be applied to all the currently selected drives. If you wish to double-check the list of selected devices, click the top panel with the number of selected drives. The drop-down provides info about the drives, their health status and case ID.



11 devices selected

Wiping

Wiping method

● Fill sectors with the following pattern   Pattern: 00   ☑ HEX

○ Put LBA number at the beginning of every sector

○ NIST 800-88

○ DoD 5220.22-M

○ Random

○ Secure Erase

Method description

Linear overwrite of the whole disk space from LBA 0 to the LBA reported by IDENTIFY DEVICE command. Data is overwritten with the specified pattern. Maximum pattern length is 512 bytes. If fewer than 512 bytes are provided, the pattern will be expanded to 512 bytes by repeating the entered pattern multiple times.

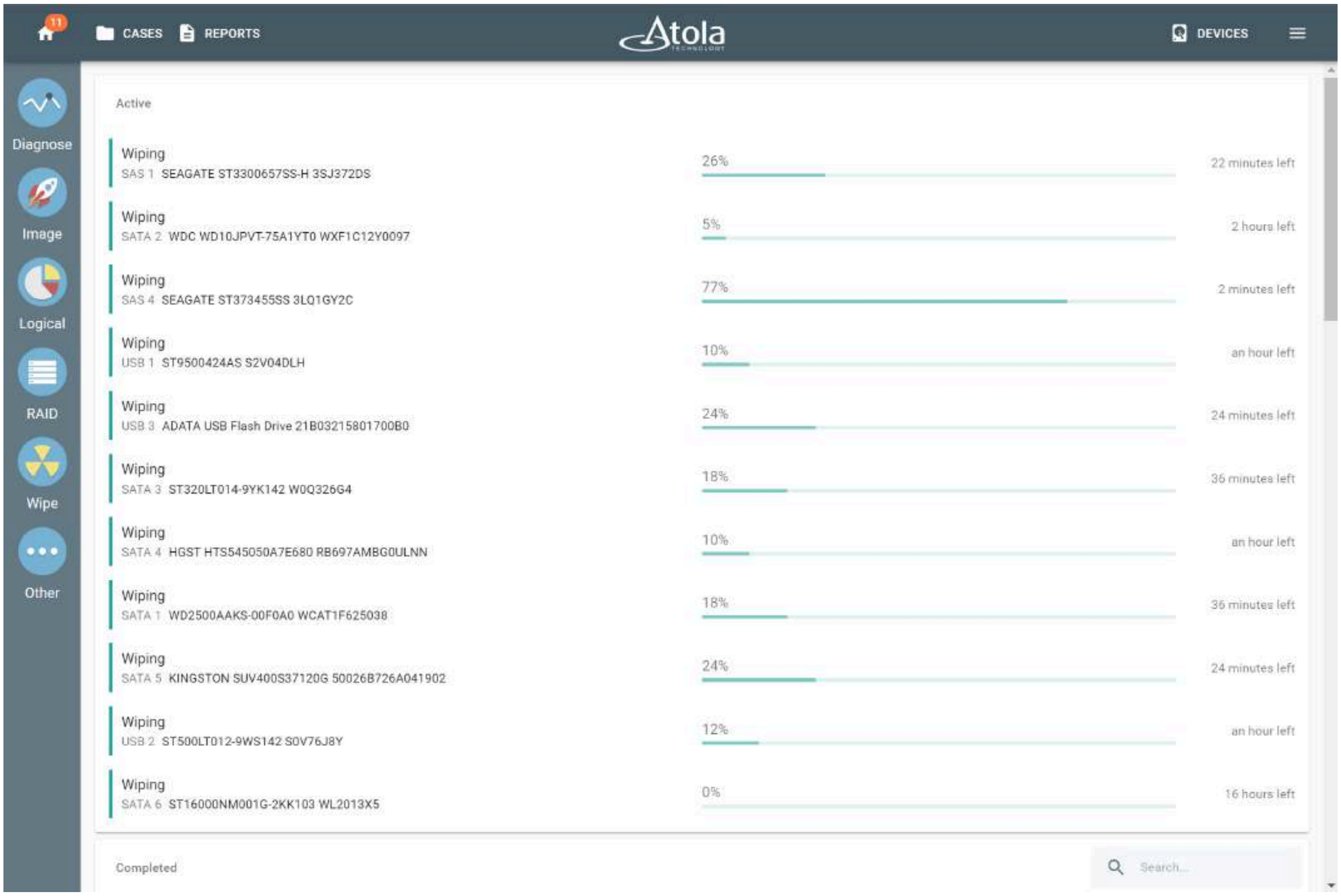
Additional actions

Check if device contains data: on

Automatically unclip HPA/DCO/AMA: on

The Settings page.

4. Click **Start**.



Active

Wiping SAS 1 SEAGATE ST3300657SS-H 3SJ372DS	26%	22 minutes left
Wiping SATA 2 WDC WD10JPVT-75A1YT0 WXF1C12Y0097	5%	2 hours left
Wiping SAS 4 SEAGATE ST373455SS 3LQ1GY2C	77%	2 minutes left
Wiping USB 1 ST9500424AS S2V04DLH	10%	an hour left
Wiping USB 3 ADATA USB Flash Drive 21B03215801700B0	24%	24 minutes left
Wiping SATA 3 ST320LT014-9YK142 W0Q326G4	18%	36 minutes left
Wiping SATA 4 HGST HTS545050A7E680 RB697AMBG0ULNN	10%	an hour left
Wiping SATA 1 WD2500AAKS-00F0A0 WCAT1F625038	18%	36 minutes left
Wiping SATA 5 KINGSTON SUV400S37120G 50026B726A041902	24%	24 minutes left
Wiping USB 2 ST500LT012-9WS142 S0V76J8Y	12%	an hour left
Wiping SATA 6 ST16000NM001G-2KK103 WL2013X5	0%	16 hours left

Completed

Multiple sessions initiated via multi-launch.

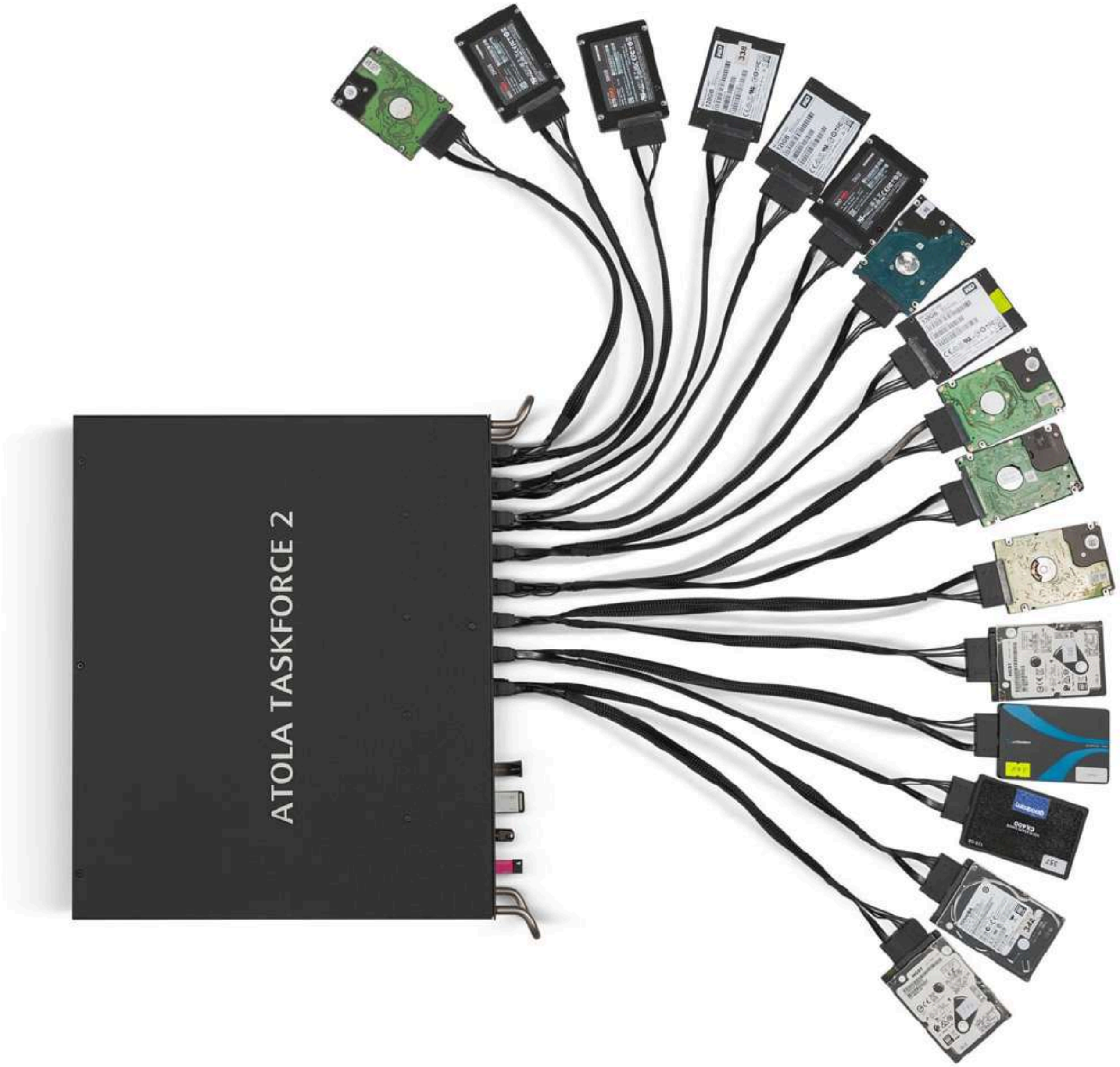
When the **Check if device contains data** option is enabled, TaskForce 2 scans all selected devices. If any data may be overwritten, the imager will warn you.

The procedure is the same for other single-drive processes. When hashing, multi-launch can be applied to both the devices plugged into the system and the locally stored image files.

The case management system automatically saves separate reports into the individual cases.

Wiping 26 drives simultaneously

With TaskForce 2, Atola introduced the fastest and most capable imaging engine to the forensic market. While the cumulative imaging speed in TaskForce 2 constitutes 25 TB/h, the engine can wipe up to 26 drives connected to it and achieve an overall performance of up to 100 TB/h.



Multiple drives connected to Atola TaskForce 2

TaskForce’s task-oriented and efficient user interface is designed to enable the launch of every operation in just a couple of clicks and expedite work with multiple evidence drives.

TaskForce 2 has 26 ports:

- 4 NVMe M.2/U.2 PCIe 4.0,
- 8 SATA,
- 8 SAS/SATA,
- 4 USB,
- 1 IDE,
- 1 Extension slot for Atola Thunderbolt, Apple PCIe SSD and M.2 NVMe/PCIe/SATA SSD extension modules,

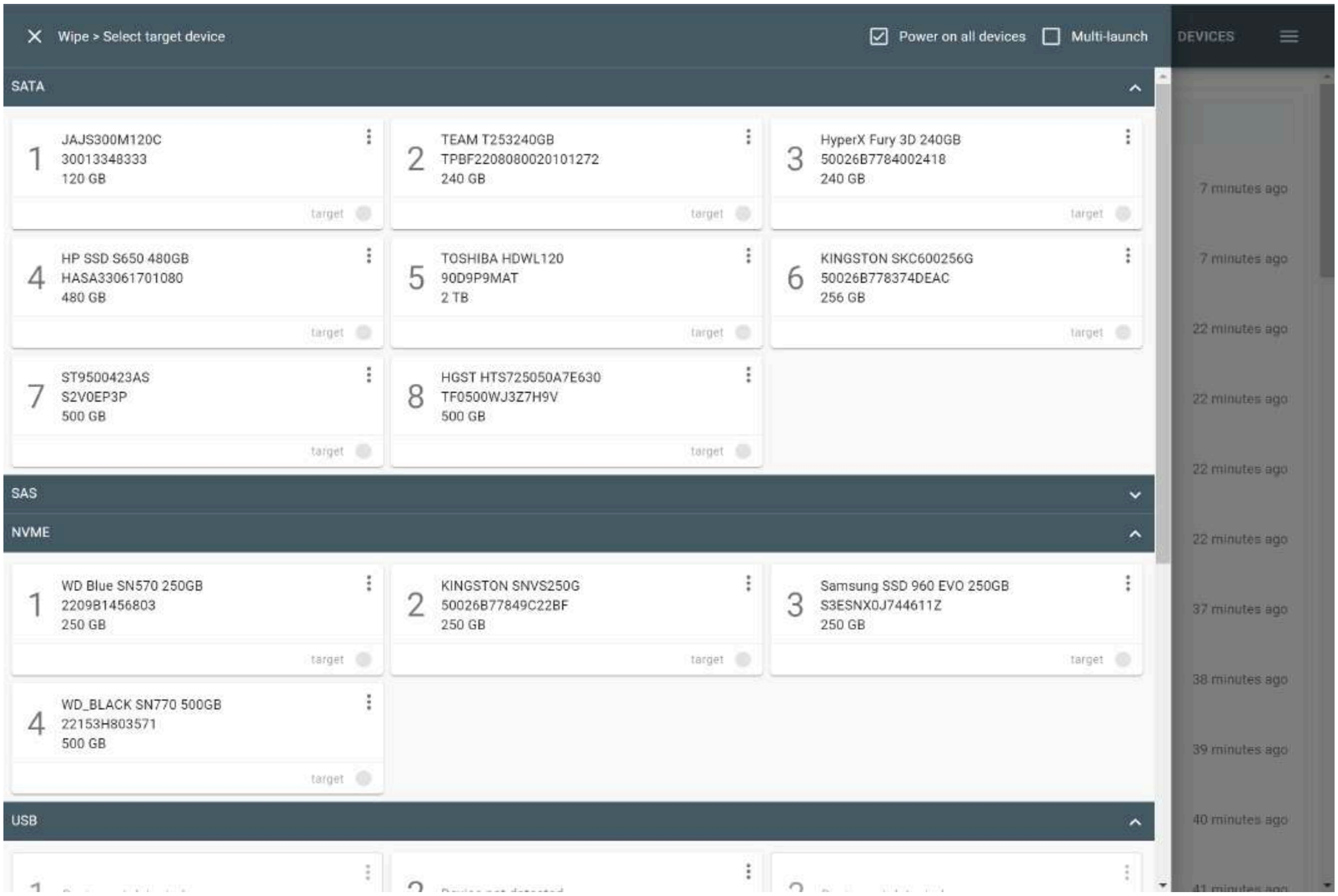
Each port can be used for simultaneous wiping sessions.

TaskForce 2 can wipe 26 devices simultaneously at their top native speeds using the standard wiping method.

Launch multiple wiping sessions

To perform multiple wiping sessions:

1. Connect the drives to TaskForce.
2. Switch the ports, to which the drives are connected, to Target mode by using the individual Source switches on each port.
3. In the TaskForce user interface, click the **Wipe** icon on the left.
4. On the **Select target device** panel, select a drive.
   To launch the wiping process for multiple drives simultaneously, tick the **Multi-launch** box at the top right, and select the drives you want to wipe.



Wipe > Select target device

☑ Power on all devices □ Multi-launch

SATA

1 JAJS300M120C
30013348333
120 GB
target ○

2 TEAM T253240GB
TPBF2208080020101272
240 GB
target ○

3 HyperX Fury 3D 240GB
50026B7784002418
240 GB
target ○

4 HP SSD S650 480GB
HASA33061701080
480 GB
target ○

5 TOSHIBA HDWL120
90D9P9MAT
2 TB
target ○

6 KINGSTON SKC600256G
50026B778374DEAC
256 GB
target ○

7 ST9500423AS
S2V0EP3P
500 GB
target ○

8 HGST HTS725050A7E630
TF0500WJ3Z7H9V
500 GB
target ○

SAS

NVME

1 WD Blue SN570 250GB
2209B1456803
250 GB
target ○

2 KINGSTON SNVS250G
50026B77849C22BF
250 GB
target ○

3 Samsung SSD 960 EVO 250GB
S3ESNX0J744611Z
250 GB
target ○

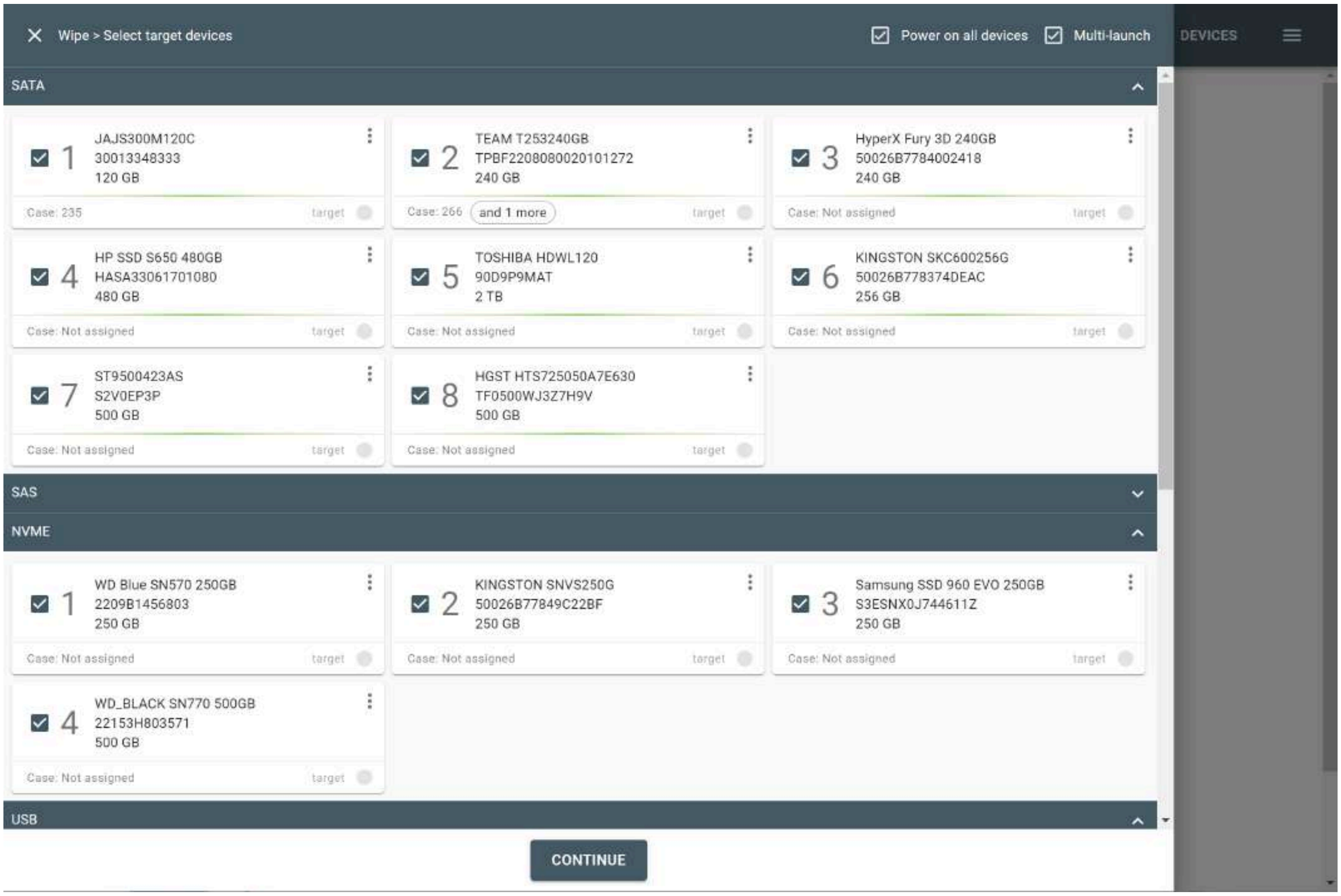
4 WD_BLACK SN770 500GB
22153H803571
500 GB
target ○

USB

1

2 Device not detected

3



SATA

☑ 1 JAJS300M120C
30013348333
120 GB
Case: 235 target

☑ 2 TEAM T253240GB
TPBF2208080020101272
240 GB
Case: 266 and 1 more target

☑ 3 HyperX Fury 3D 240GB
50026B7784002418
240 GB
Case: Not assigned target

☑ 4 HP SSD S650 480GB
HASA33061701080
480 GB
Case: Not assigned target

☑ 5 TOSHIBA HDWL120
90D9P9MAT
2 TB
Case: Not assigned target

☑ 6 KINGSTON SKC600256G
50026B778374DEAC
256 GB
Case: Not assigned target

☑ 7 ST9500423AS
S2V0EP3P
500 GB
Case: Not assigned target

☑ 8 HGST HTS725050A7E630
TF0500WJ3Z7H9V
500 GB
Case: Not assigned target

NVME

☑ 1 WD Blue SN570 250GB
2209B1456803
250 GB
Case: Not assigned target

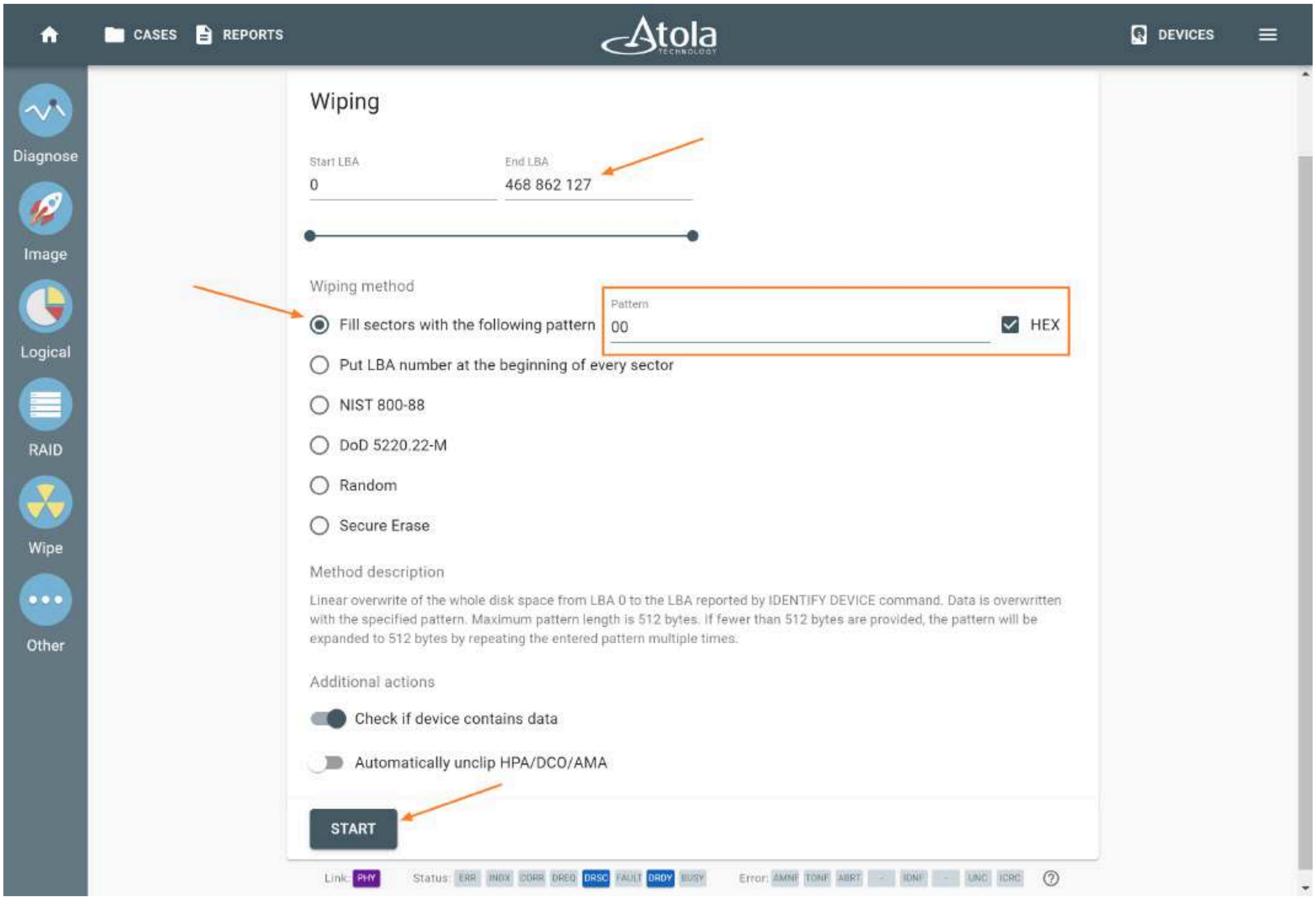
☑ 2 KINGSTON SNVS250G
50026B77849C22BF
250 GB
Case: Not assigned target

☑ 3 Samsung SSD 960 EVO 250GB
S3ESNX0J744611Z
250 GB
Case: Not assigned target

☑ 4 WD_BLACK SN770 500GB
22153H803571
500 GB
Case: Not assigned target

5. Adjust wiping settings:
   - the range of sectors to be wiped
   - wiping method
   - enter a pattern and select its format (HEX/ASCII)

6. Click **Start**.



Wiping

Start LBA: 0

End LBA: 468 862 127

Wiping method

- ● Fill sectors with the following pattern — Pattern: 00 ☑ HEX
- ○ Put LBA number at the beginning of every sector
- ○ NIST 800-88
- ○ DoD 5220.22-M
- ○ Random
- ○ Secure Erase

Method description

Linear overwrite of the whole disk space from LBA 0 to the LBA reported by IDENTIFY DEVICE command. Data is overwritten with the specified pattern. Maximum pattern length is 512 bytes. If fewer than 512 bytes are provided, the pattern will be expanded to 512 bytes by repeating the entered pattern multiple times.

Additional actions

- Check if device contains data (on)
- Automatically unclip HPA/DCO/AMA (off)

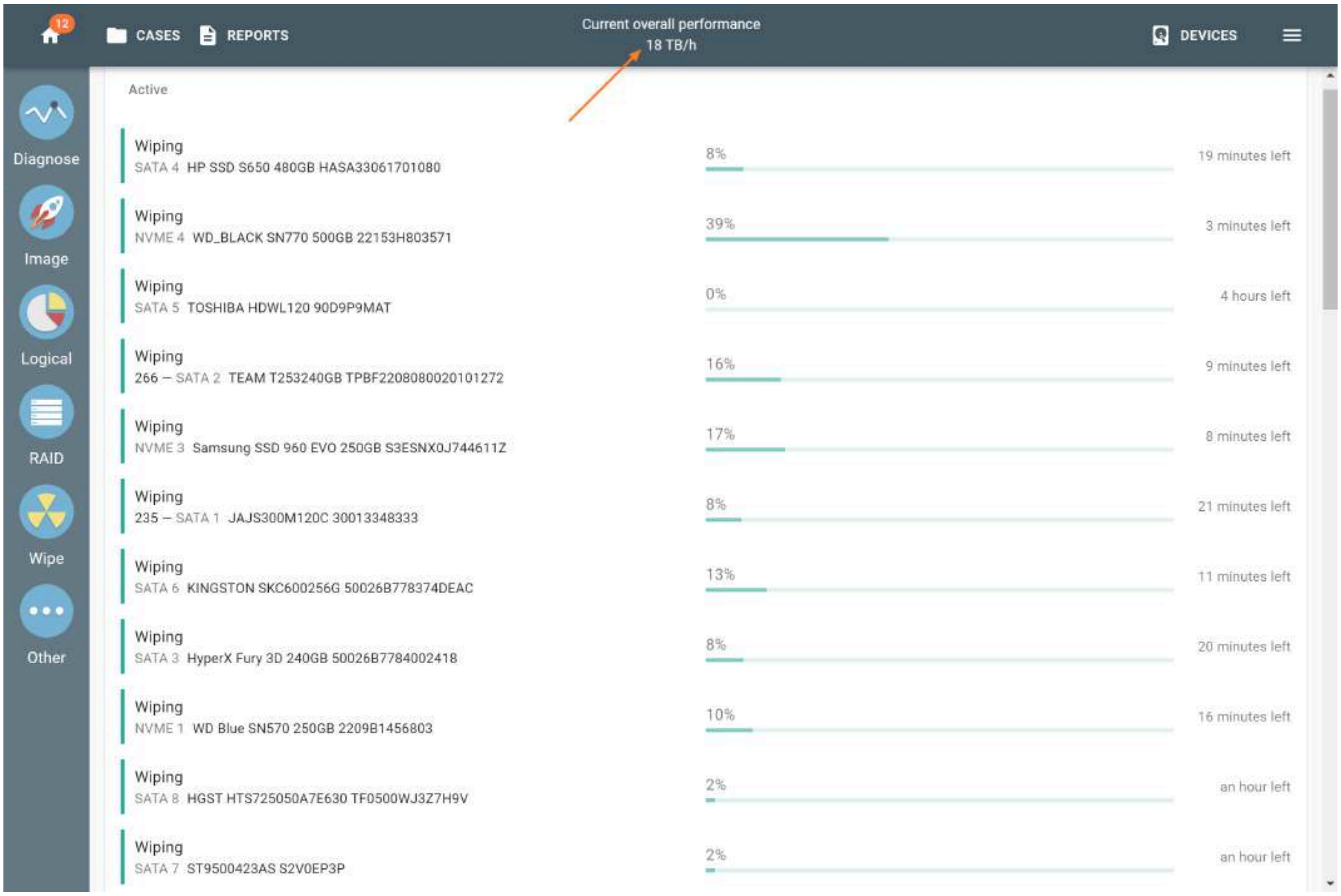
Link: PHY Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY Error: AMNF TONF ABRT - IDNF - UNC ICRC

Wiping is consecutively launched for each device.

Track the wiping progress

Once the operations have started, track the progress of all tasks on the **Home screen**. It displays the percentage of wiped drive area and the time left until the end of the planned session. To see more details on the progress of an individual wiping session, click on that session.

To reveal the current overall wiping speed, click the Atola logo in the center of the top bar. In this case, we were able to achieve 18 TB/h. This high-speed wiping capability allows a forensic expert to prepare target drives for imaging in minimal time.



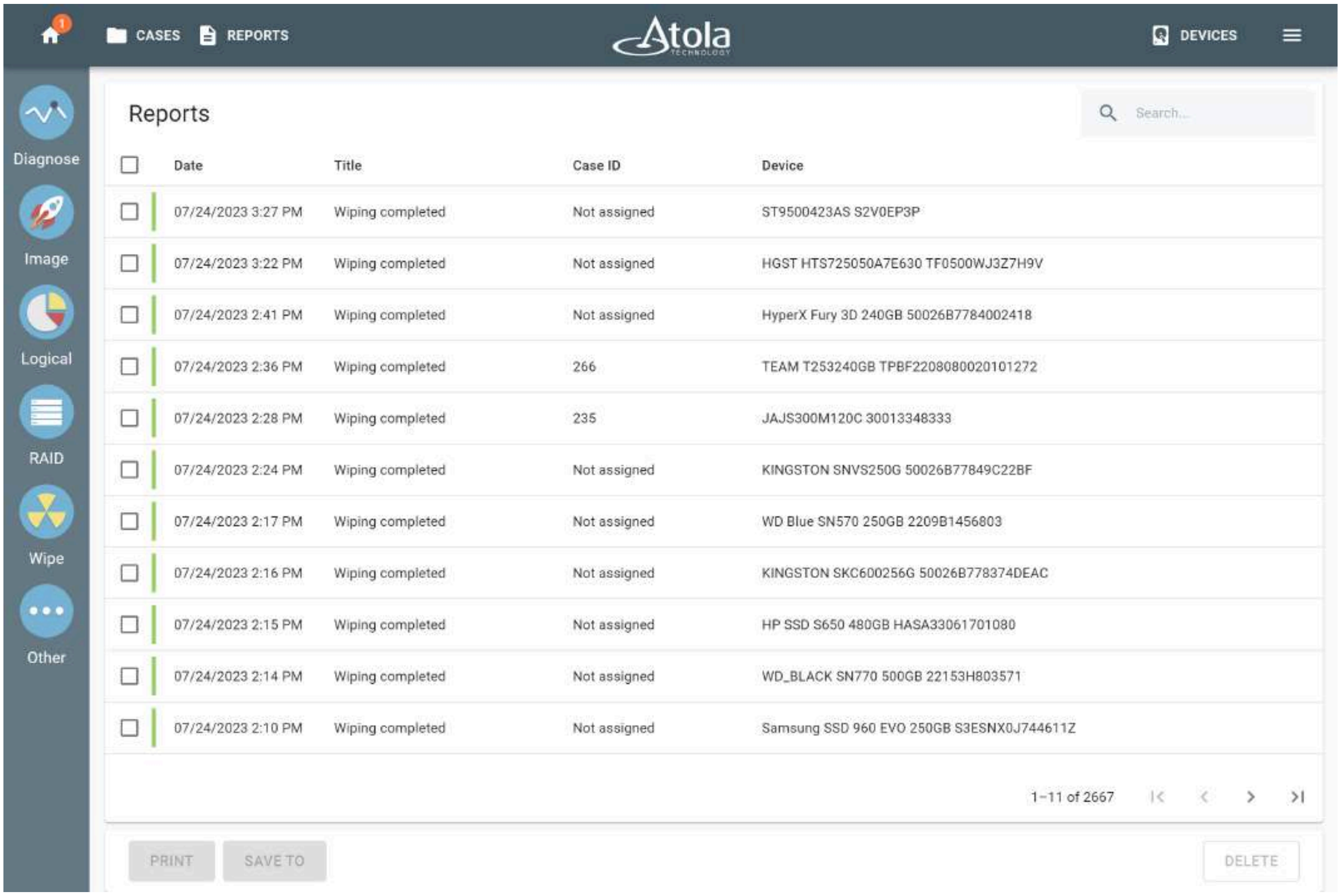
Current overall performance
18 TB/h

Active

Wiping SATA 4 HP SSD S650 480GB HASA33061701080	8%	19 minutes left
Wiping NVME 4 WD_BLACK SN770 500GB 22153H803571	39%	3 minutes left
Wiping SATA 5 TOSHIBA HDWL120 90D9P9MAT	0%	4 hours left
Wiping 266 – SATA 2 TEAM T253240GB TPBF2208080020101272	16%	9 minutes left
Wiping NVME 3 Samsung SSD 960 EVO 250GB S3ESNX0J744611Z	17%	8 minutes left
Wiping 235 – SATA 1 JAJS300M120C 30013348333	8%	21 minutes left
Wiping SATA 6 KINGSTON SKC600256G 50026B778374DEAC	13%	11 minutes left
Wiping SATA 3 HyperX Fury 3D 240GB 50026B7784002418	8%	20 minutes left
Wiping NVME 1 WD Blue SN570 250GB 2209B1456803	10%	16 minutes left
Wiping SATA 8 HGST HTS725050A7E630 TF0500WJ3Z7H9V	2%	an hour left
Wiping SATA 7 ST9500423AS S2V0EP3P	2%	an hour left

> A wiping session can take longer if a different wiping method is selected. E.g. the NIST 800-88 method implies not only wiping but also rereading of the wiped range. The DoD 5220.22-M method wipes the same range three times.

To ensure maximum transparency and effectiveness, TaskForce 2 documents every operation by creating detailed reports and logs. Click **Reports** at the top and find the report in the list or use the **Search bar** at the top of the page.



Reports

☐	Date	Title	Case ID	Device
☐	07/24/2023 3:27 PM	Wiping completed	Not assigned	ST9500423AS S2V0EP3P
☐	07/24/2023 3:22 PM	Wiping completed	Not assigned	HGST HTS725050A7E630 TF0500WJ3Z7H9V
☐	07/24/2023 2:41 PM	Wiping completed	Not assigned	HyperX Fury 3D 240GB 50026B7784002418
☐	07/24/2023 2:36 PM	Wiping completed	266	TEAM T253240GB TPBF2208080020101272
☐	07/24/2023 2:28 PM	Wiping completed	235	JAJS300M120C 30013348333
☐	07/24/2023 2:24 PM	Wiping completed	Not assigned	KINGSTON SNVS250G 50026B77849C22BF
☐	07/24/2023 2:17 PM	Wiping completed	Not assigned	WD Blue SN570 250GB 2209B1456803
☐	07/24/2023 2:16 PM	Wiping completed	Not assigned	KINGSTON SKC600256G 50026B778374DEAC
☐	07/24/2023 2:15 PM	Wiping completed	Not assigned	HP SSD S650 480GB HASA33061701080
☐	07/24/2023 2:14 PM	Wiping completed	Not assigned	WD_BLACK SN770 500GB 22153H803571
☐	07/24/2023 2:10 PM	Wiping completed	Not assigned	Samsung SSD 960 EVO 250GB S3ESNX0J744611Z

1–11 of 2667

How TaskForce verifies that wiping is successful

To verify that wiping is successful, TaskForce applies the following algorithm:

1. One hundred sectors, evenly spaced across the wiping range, are filled with the verification ASCII pattern '*AtolaTechnology*'.
2. The whole drive or a selected range of sectors on it is wiped by applying the method selected by the user ('*Fill sectors with the following pattern*' by default).
3. Finally, TaskForce reads the hundred sectors that were filled during the first step and makes sure that none of them contains the pattern '*AtolaTechnology*'.

Unclip or change HPA, DCO, AMA limitations

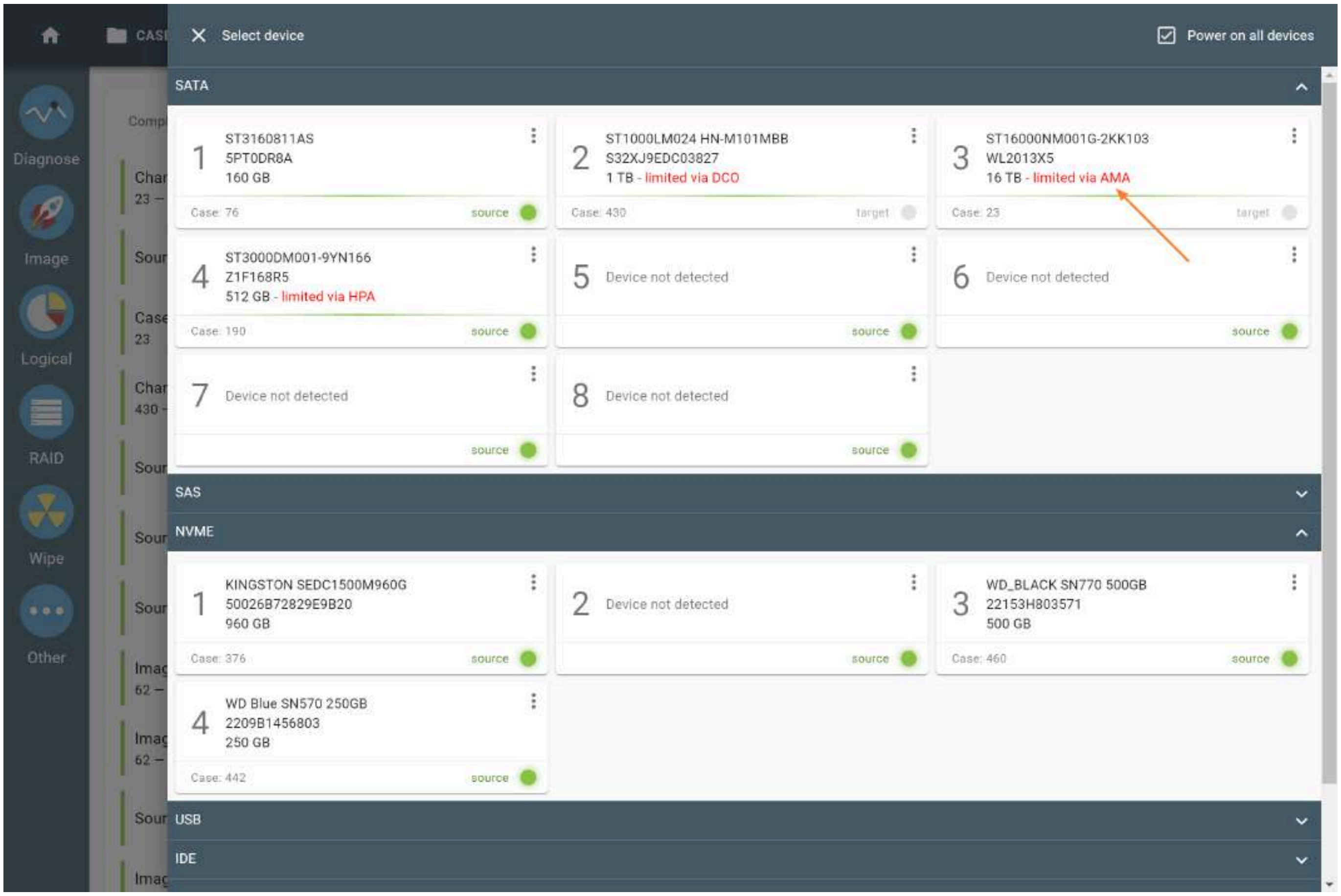
DCO (device configuration overlay), HPA (host protected area), or AMA (accessible max address) features were created by hard drive manufacturers as hidden areas reserved for storing vendor utilities or simply to make a drive appear to have a certain number of sectors (smaller than the actual drive capacity).

But it is many years ago that end users learned to modify and write to these areas of hard drives with the help of open source and freely available tools. For digital forensics specialists, it means that without the ability to identify such hidden areas of a drive and image the full physical image including data in these areas, the evidence they get may be incomplete and lead to inaccurate investigative conclusions.

Atola TaskForce 2 helps you detect, unclip, or change HPA, DCO, AMA limitations.

Detect DCO, HPA, or AMA limitations

When you connect a hard drive to the TaskForce 2 unit, in addition to the standard *Identify device* command, TaskForce software automatically sends two commands to look up the drive size as set in drive’s firmware: *Read native max address* and *Device configuration identify*. If drive size has been limited by DCO, HPA, or AMA, TaskForce 2 will draw your attention to these changes by adding the note in red color in the device menu.



SATA

1 ST3160811AS
5PT0DR8A
160 GB
Case: 76 — source

2 ST1000LM024 HN-M101MBB
S32XJ9EDC03827
1 TB - limited via DCO
Case: 430 — target

3 ST16000NM001G-2KK103
WL2013X5
16 TB - limited via AMA
Case: 23 — target

4 ST3000DM001-9YN166
Z1F168R5
512 GB - limited via HPA
Case: 190 — source

5 Device not detected — source

6 Device not detected — source

7 Device not detected — source

8 Device not detected — source

NVME

1 KINGSTON SEDC1500M960G
50026B72829E9B20
960 GB
Case: 376 — source

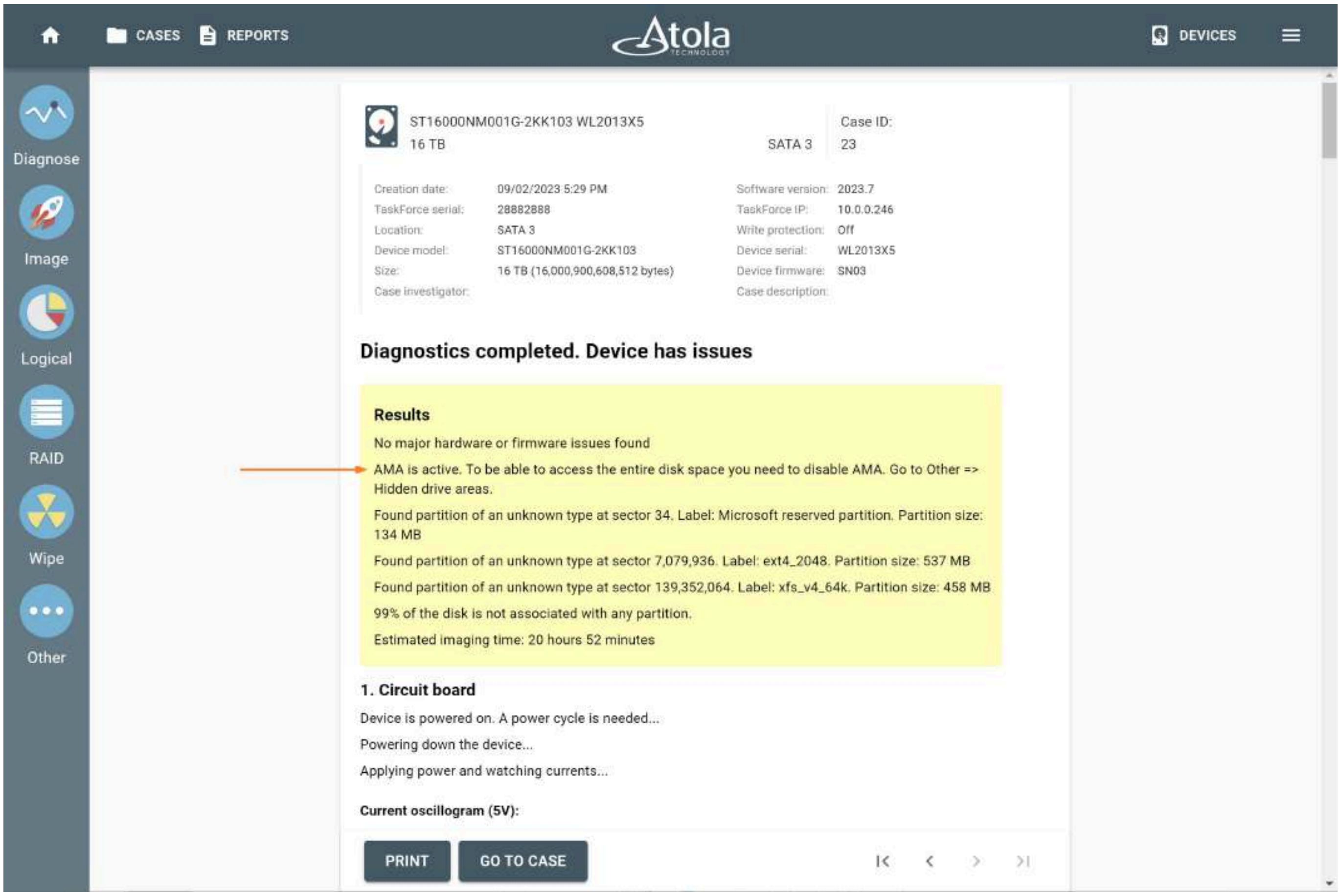
2 Device not detected — source

3 WD_BLACK SN770 500GB
22153H803571
500 GB
Case: 460 — source

4 WD Blue SN570 250GB
2209B1456803
250 GB
Case: 442 — source

Notification about HPA, DCO, and AMA in device menu.

To get more details about the modifications that have been made to the drive’s firmware, run **Diagnose** and see the **Firmware** section of the **Diagnostics report**.



ST16000NM001G-2KK103 WL2013X5
16 TB
SATA 3
Case ID:
23

Creation date:	09/02/2023 5:29 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 3	Write protection:	Off
Device model:	ST16000NM001G-2KK103	Device serial:	WL2013X5
Size:	16 TB (16,000,900,608,512 bytes)	Device firmware:	SN03
Case investigator:		Case description:	

Diagnostics completed. Device has issues

Results

No major hardware or firmware issues found

AMA is active. To be able to access the entire disk space you need to disable AMA. Go to Other => Hidden drive areas.

Found partition of an unknown type at sector 34. Label: Microsoft reserved partition. Partition size: 134 MB

Found partition of an unknown type at sector 7,079,936. Label: ext4_2048. Partition size: 537 MB

Found partition of an unknown type at sector 139,352,064. Label: xfs_v4_64k. Partition size: 458 MB

99% of the disk is not associated with any partition.

Estimated imaging time: 20 hours 52 minutes

1. Circuit board

Device is powered on. A power cycle is needed...

Powering down the device...

Applying power and watching currents...

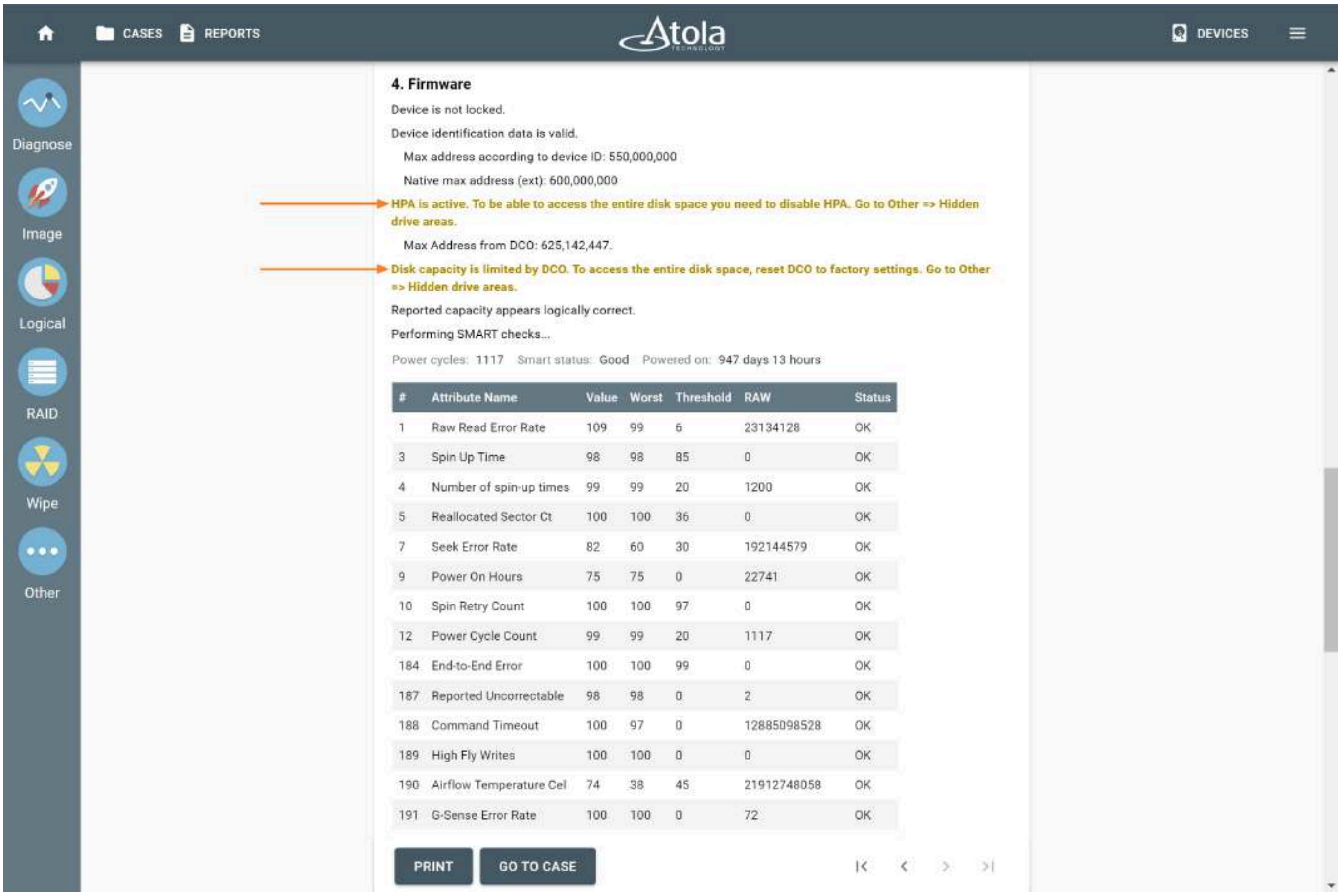
Current oscillogram (5V):

AMA limitation is indicated in the Diagnostics summary.

There you will see three lines indicating the drive's Max Address according to different records in the drive's firmware:

1. The *Max Address according to device ID* line shows the max address from the ID sector, affected by DCO and HPA/AMA restrictions if those are applied.
2. *Native Max Address* indicates max address ignoring HPA/AMA limitation that may have been enabled, yet affected by DCO restriction.
3. *Max Address from DCO* is the line that gives you the actual drive size.

A **Diagnostics report** of a drive that does not have HPA/AMA or DCO activated will have the same value in all three lines.



4. Firmware

Device is not locked.

Device identification data is valid.

Max address according to device ID: 550,000,000

Native max address (ext): 600,000,000

HPA is active. To be able to access the entire disk space you need to disable HPA. Go to Other => Hidden drive areas.

Max Address from DCO: 625,142,447.

Disk capacity is limited by DCO. To access the entire disk space, reset DCO to factory settings. Go to Other => Hidden drive areas.

Reported capacity appears logically correct.

Performing SMART checks...

Power cycles: 1117 Smart status: Good Powered on: 947 days 13 hours

#	Attribute Name	Value	Worst	Threshold	RAW	Status
1	Raw Read Error Rate	109	99	6	23134128	OK
3	Spin Up Time	98	98	85	0	OK
4	Number of spin-up times	99	99	20	1200	OK
5	Reallocated Sector Ct	100	100	36	0	OK
7	Seek Error Rate	82	60	30	192144579	OK
9	Power On Hours	75	75	0	22741	OK
10	Spin Retry Count	100	100	97	0	OK
12	Power Cycle Count	99	99	20	1117	OK
184	End-to-End Error	100	100	99	0	OK
187	Reported Uncorrectable	98	98	0	2	OK
188	Command Timeout	100	97	0	12885098528	OK
189	High Fly Writes	100	100	0	0	OK
190	Airflow Temperature Cel	74	38	45	21912748058	OK
191	G-Sense Error Rate	100	100	0	72	OK

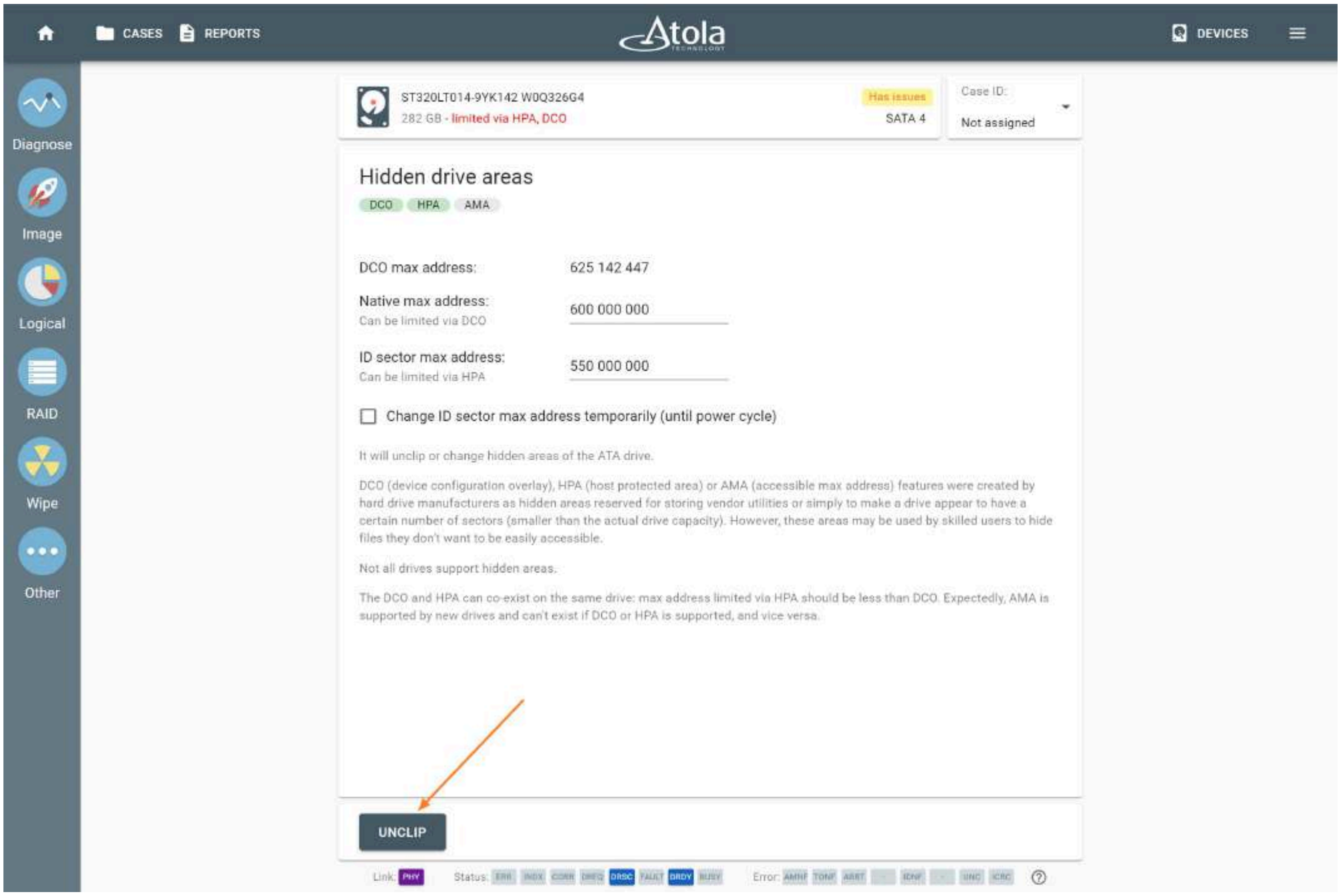
HPA and DCO restriction details in the Firmware section of the Diagnostics report.

Unclip HPA, DCO, AMA limitations

To disable HPA, DCO, AMA limitations that have been applied to the drive’s firmware:

1. On the left, click **Other** and then **Hidden drive areas**.
2. Select device.
3. Click **Unclip**.

The drive needs to be in the Target mode (use the Source/Target switch on the unit to perform this operation), as **Unclip HPA, DCO, AMA limitations** implies making changes to the drive's firmware, and that is not possible when the drive is in the Source mode.



ST320LT014-9YK142 W0Q326G4
282 GB - limited via HPA, DCO

Has issues
SATA 4

Case ID:
Not assigned

Hidden drive areas

DCO max address: 625 142 447

Native max address: 600 000 000
Can be limited via DCO

ID sector max address: 550 000 000
Can be limited via HPA

☐ Change ID sector max address temporarily (until power cycle)

It will unclip or change hidden areas of the ATA drive.

DCO (device configuration overlay), HPA (host protected area) or AMA (accessible max address) features were created by hard drive manufacturers as hidden areas reserved for storing vendor utilities or simply to make a drive appear to have a certain number of sectors (smaller than the actual drive capacity). However, these areas may be used by skilled users to hide files they don't want to be easily accessible.

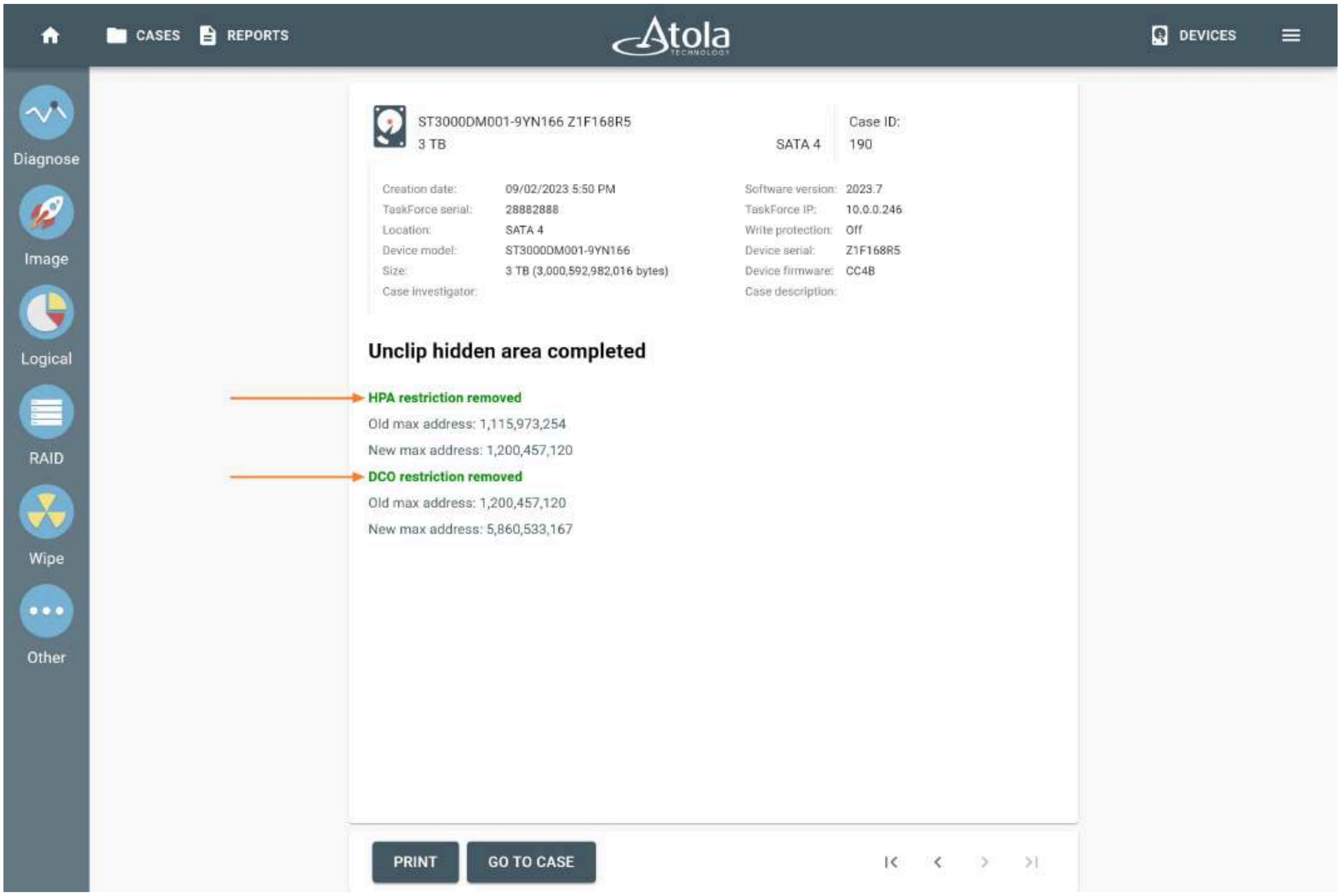
Not all drives support hidden areas.

The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO. Expectedly, AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

UNCLIP
Link: PHY
Status: ERR INDX CORR DRQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT IDNF UNC ICRC

Remove HPA and DCO by clicking the Unclip button.

TaskForce 2 lifts HPA/AMA and DCO restrictions in a matter of seconds and enables access to all data on the drive.



ST3000DM001-9YN166 Z1F168R5
3 TB
SATA 4
Case ID:
190

Creation date:	09/02/2023 5:50 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 4	Write protection:	Off
Device model:	ST3000DM001-9YN166	Device serial:	Z1F168R5
Size:	3 TB (3,000,592,982,016 bytes)	Device firmware:	CC4B
Case investigator:		Case description:	

Unclip hidden area completed

HPA restriction removed
Old max address: 1,115,973,254
New max address: 1,200,457,120
DCO restriction removed
Old max address: 1,200,457,120
New max address: 5,860,533,167

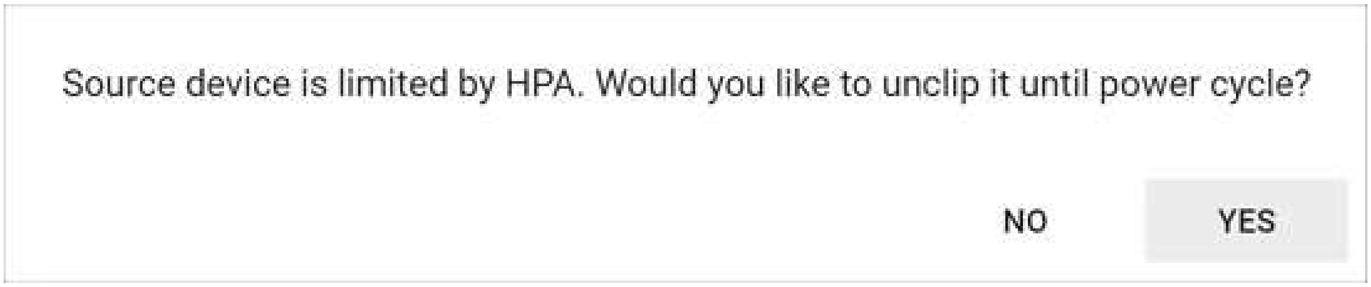
HPA and DCO unclip report.

Unclip HPA temporarily (until power cycle)

To ensure the forensically sound process, it can be necessary to avoid making any changes to the drive. Therefore it is prohibited to disable HPA and DCO restrictions and access data in the hidden areas. With TaskForce 2 it is possible to lift HPA restriction until the next power cycle. This helps avoid permanent changes to the drive.

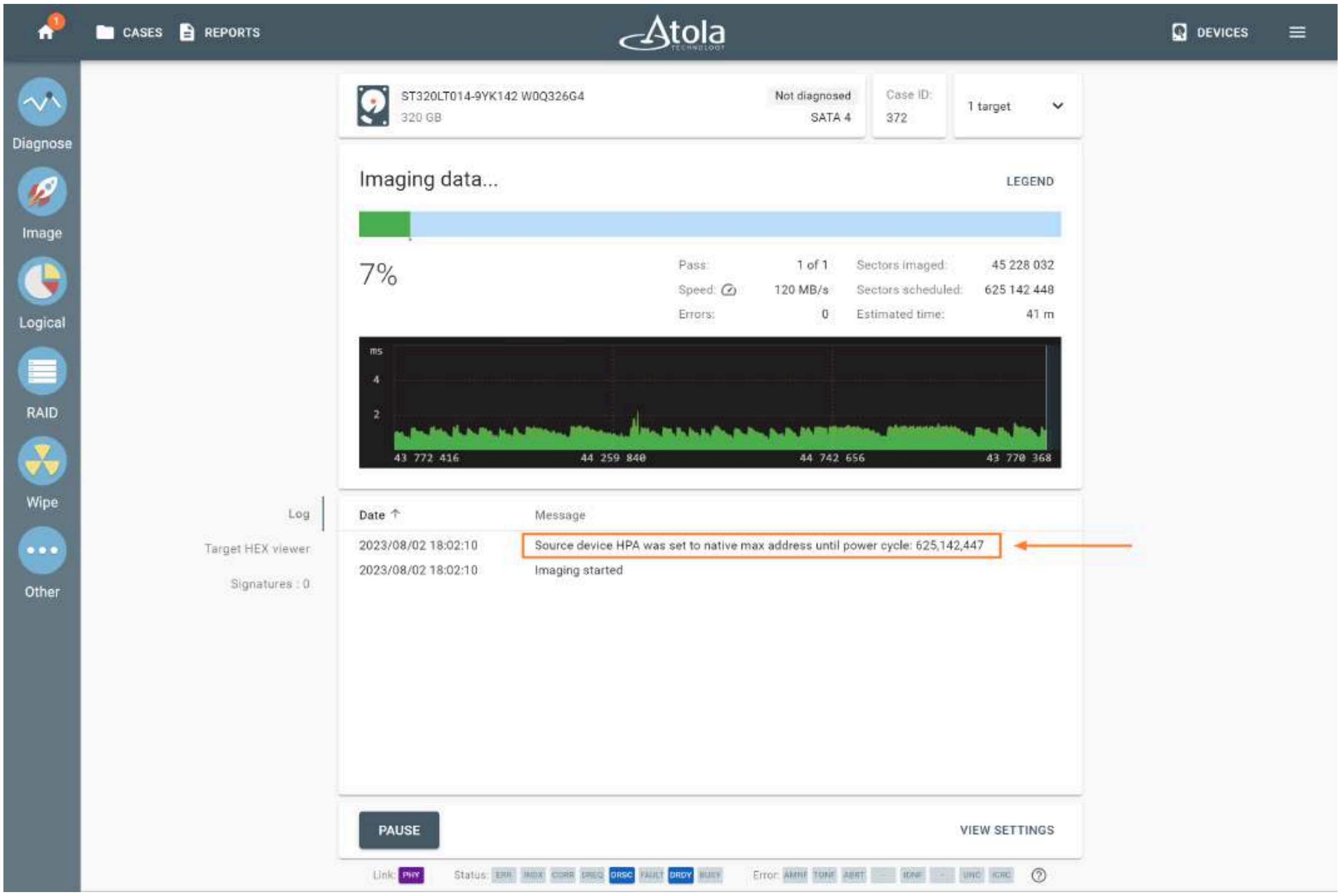
To unclip HPA on the source drive until power cycle before imaging:

1. Go to **Image**.
2. Select source device.
3. Select target devices and click **Continue**.
4. In **Confirmation** dialog, suggesting you unclip the drive until power cycle, click **Yes**.


Source device is limited by HPA. Would you like to unclip it until power cycle?

This will allow temporary access to the data in HPA-protected area, but as soon as you power off or unplug the drive, the HPA will be back again.

After you confirm unclipping HPA until power cycle, the imaging process starts and the following message appears in the imaging log: *Source device HPA was set to native max address until power cycle*.



ST320LT014-9YK142 W0Q326G4
320 GB
Not diagnosed
SATA 4
Case ID: 372
1 target

Imaging data...

7%

Pass:	1 of 1	Sectors imaged:	45 228 032
Speed:	120 MB/s	Sectors scheduled:	625 142 448
Errors:	0	Estimated time:	41 m

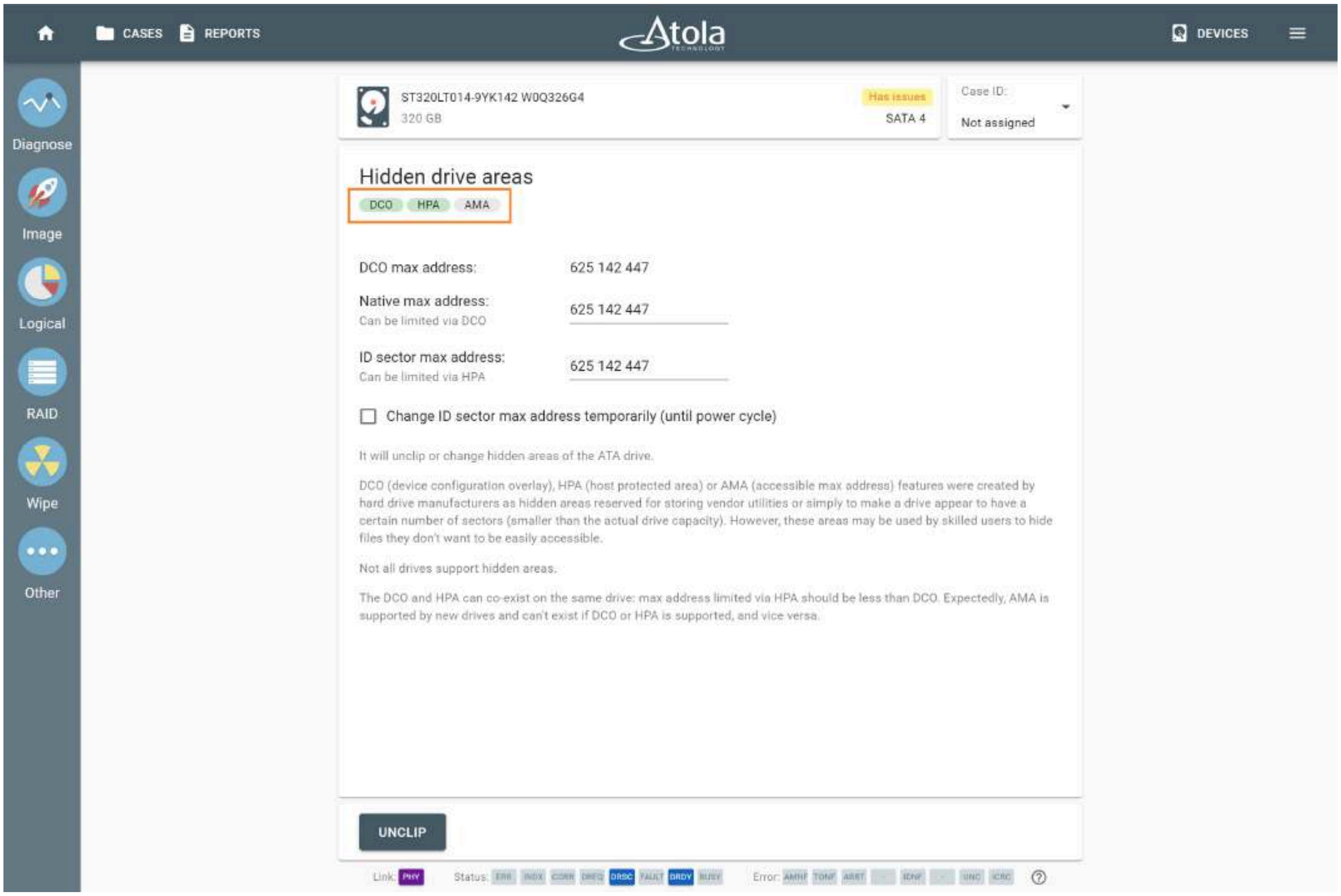
Date ↑	Message
2023/08/02 18:02:10	Source device HPA was set to native max address until power cycle: 625,142,447
2023/08/02 18:02:10	Imaging started

The message in the imaging log informs that source device HPA was set to native max address until power cycle.

If a drive freezes in the course of imaging TaskForce forcibly performs power cycles to continue imaging the drive. However, such power cycles will not affect the temporarily disabled HPA. TaskForce will be temporarily removing HPA max address restriction after each power cycle performed during imaging. The HPA-protected area will remain accessible throughout the imaging process.

Set or change HPA, DCO, AMA limitations

Not all drives support hidden areas. Limitation type supported by the particular drive will be shown in green on the **Hidden drive areas** page.



ST320LT014-9YK142 W0Q326G4
320 GB
SATA 4

Case ID:
Not assigned

Hidden drive areas

DCO max address: 625 142 447

Native max address: 625 142 447
Can be limited via DCO

ID sector max address: 625 142 447
Can be limited via HPA

☐ Change ID sector max address temporarily (until power cycle)

It will unclip or change hidden areas of the ATA drive.

DCO (device configuration overlay), HPA (host protected area) or AMA (accessible max address) features were created by hard drive manufacturers as hidden areas reserved for storing vendor utilities or simply to make a drive appear to have a certain number of sectors (smaller than the actual drive capacity). However, these areas may be used by skilled users to hide files they don't want to be easily accessible.

Not all drives support hidden areas.

The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO. Expectedly, AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

The drive supports DCO and HPA limitations, but does not support AMA.

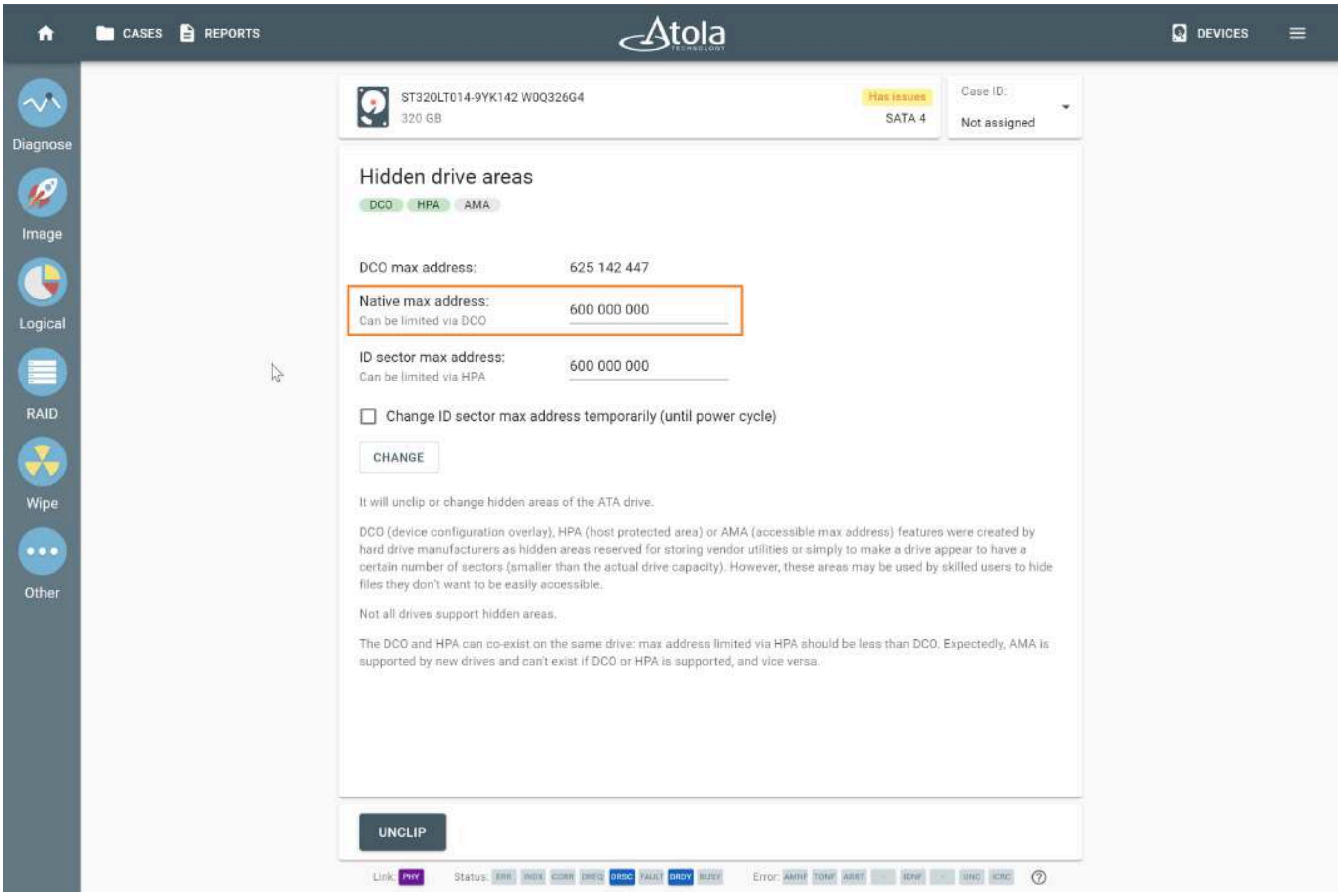
The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO.

Expectedly, AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

If your target device is larger than your source device, but you need hash values for the source and for the target devices to be identical, see Clip target drive to source evidence size.

To set or change DCO limitation:

1. Make sure that the drive is in the Target mode.
2. On the left, click **Other** and then **Hidden drive areas**.
3. Select device.
4. Enter new **Native max address**. Notice that **ID sector max address** changes accordingly.
5. Click **Change**.



ST320LT014-9YK142 W0Q326G4
320 GB

Case ID: Not assigned

Hidden drive areas

DCO max address: 625 142 447

Native max address: 600 000 000
Can be limited via DCO

ID sector max address: 600 000 000
Can be limited via HPA

☐ Change ID sector max address temporarily (until power cycle)

It will unclip or change hidden areas of the ATA drive.

DCO (device configuration overlay), HPA (host protected area) or AMA (accessible max address) features were created by hard drive manufacturers as hidden areas reserved for storing vendor utilities or simply to make a drive appear to have a certain number of sectors (smaller than the actual drive capacity). However, these areas may be used by skilled users to hide files they don't want to be easily accessible.

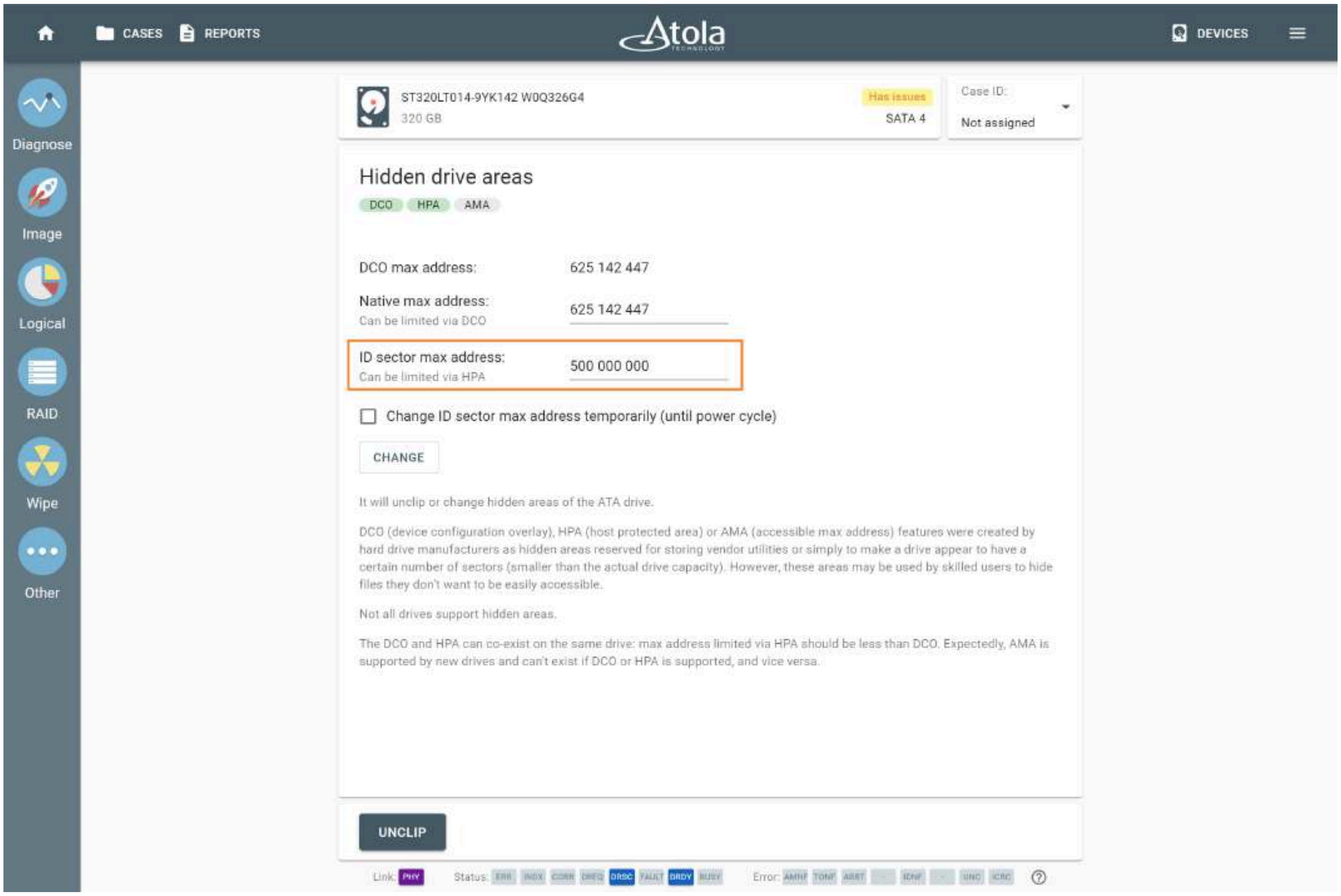
Not all drives support hidden areas.

The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO. Expectedly, AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

Setting new DCO limitation.

To set or change HPA limitation:

1. Make sure that the drive is in the Target mode.
2. On the left, click **Other** and then **Hidden drive areas**.
3. Select device.
4. Enter new **ID sector max address**.
5. **Optional:** Check **Change ID sector max address temporarily (until power cycle)** if needed.
6. Click **Change**.



ST320LT014-9YK142 W0Q326G4
320 GB

Case ID:
Not assigned

Hidden drive areas

DCO max address: 625 142 447

Native max address: 625 142 447
Can be limited via DCO

ID sector max address: 500 000 000
Can be limited via HPA

☐ Change ID sector max address temporarily (until power cycle)

It will unclip or change hidden areas of the ATA drive.

DCO (device configuration overlay), HPA (host protected area) or AMA (accessible max address) features were created by hard drive manufacturers as hidden areas reserved for storing vendor utilities or simply to make a drive appear to have a certain number of sectors (smaller than the actual drive capacity). However, these areas may be used by skilled users to hide files they don't want to be easily accessible.

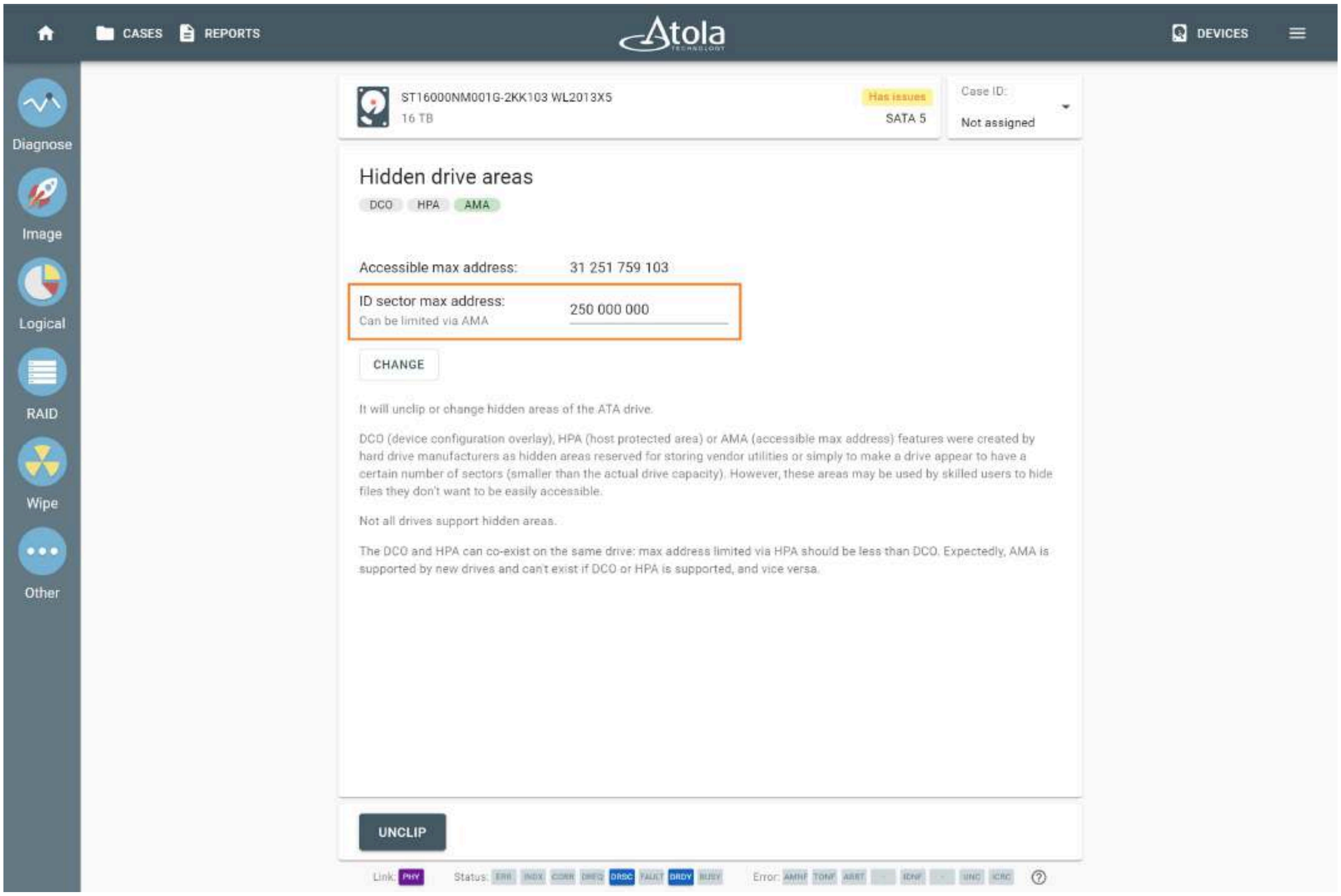
Not all drives support hidden areas.

The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO. Expectedly, AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

Setting new HPA limitation.

To set or change AMA limitation:

1. Make sure that the drive is in the Target mode.
2. On the left, click **Other** and then **Hidden drive areas**.
3. Select device.
4. Enter new **ID sector max address**.
5. Click **Change**.



ST16000NM001G-2KK103 WL2013X5
16 TB

Has issues
SATA 5

Case ID:
Not assigned

Hidden drive areas

Accessible max address: 31 251 759 103

ID sector max address: 250 000 000
Can be limited via AMA

It will unclip or change hidden areas of the ATA drive.

DCO (device configuration overlay), HPA (host protected area) or AMA (accessible max address) features were created by hard drive manufacturers as hidden areas reserved for storing vendor utilities or simply to make a drive appear to have a certain number of sectors (smaller than the actual drive capacity). However, these areas may be used by skilled users to hide files they don't want to be easily accessible.

Not all drives support hidden areas.

The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO. Expectedly, AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

UNCLIP
Link: PHY
Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY
Error: AMNF TONF ABRT - IDNF - UNC ICRC

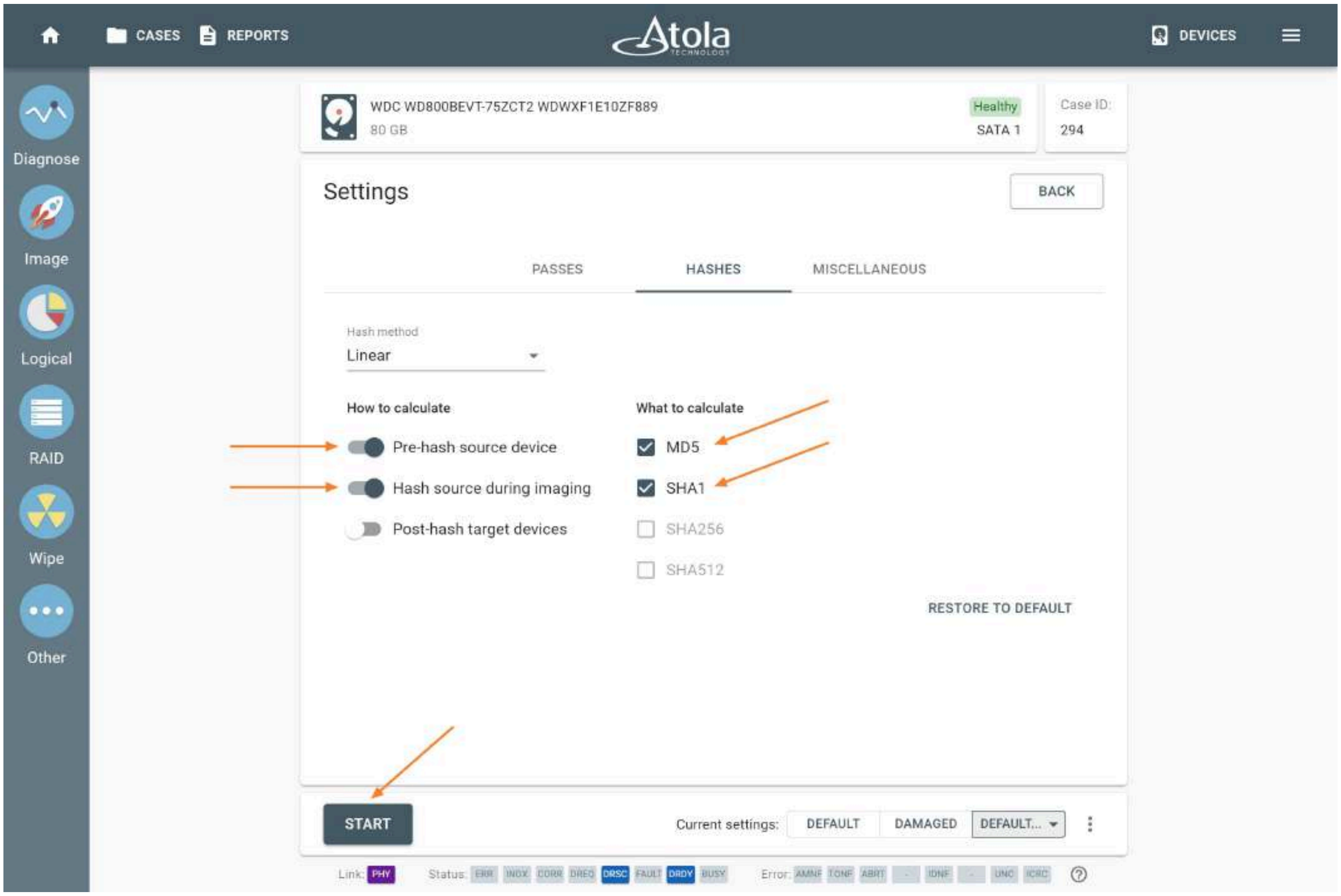
Setting new AMA limitation.

Calculating hash during imaging

Atola TaskForce 2 supports hash calculation of both the evidence drive and the image in conjunction with imaging. We have developed highly flexible functionality to help optimize evidence acquisition process to fit one’s internal procedures, while avoiding further damage to fragile media.

To calculate hash of both the evidence and the image:

1. On the left, click **Image**.
2. Select the source and target device.
3. On the imaging **Settings** page, click **Change**.
4. On the **Hashes** tab, toggle one or several options how you want to calculate hash:
    - Pre-hash source device
    - Hash source during imaging
    - Post-hash target device



WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
80 GB
Healthy
SATA 1
Case ID: 294

Settings

Hash method
Linear

How to calculate
- ● Pre-hash source device
- ● Hash source during imaging
- ○ Post-hash target devices

What to calculate
- ☑ MD5
- ☑ SHA1
- □ SHA256
- □ SHA512

Current settings: DEFAULT DAMAGED DEFAULT...

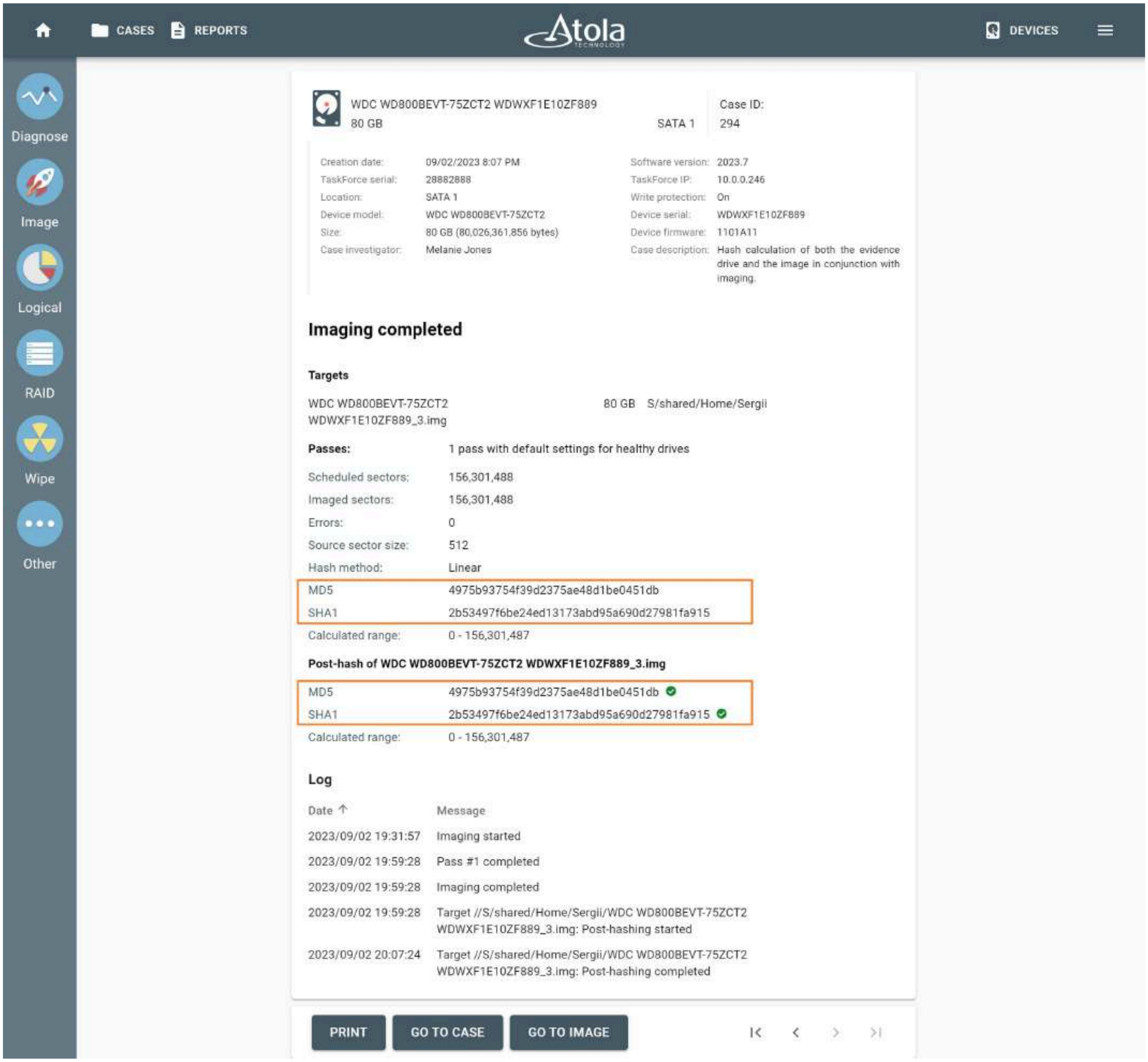
Selecting hash methods.

Pre-hash source drive option must be used with caution: although pre-hashing can be required by an investigator's internal procedures, when dealing with drives that have been diagnosed with hardware failure, this operation may cause further damage to the drive before essential data is imaged.

Hash source during imaging is the most appropriate way to calculate the hash of a fragile source evidence drive. In this case, TaskForce 2 only needs to read the data on the drive once to both image and calculate the hash, thus minimally using the drive's hardware.

Linear hash can only be calculated by reading data in sectors consecutively in one pass. When it encounters a bad sector, linear hash calulation is discontinued. For bad drives we recommend using Segmented hashing.

Post-hash target device option lets you to properly record the calculated hash in the case.



WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
80 GB

SATA 1

Case ID:
294

Creation date:	09/02/2023 8:07 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	WDC WD800BEVT-75ZCT2	Device serial:	WDWXF1E10ZF889
Size:	80 GB (80,026,361,856 bytes)	Device firmware:	1101A11
Case investigator:	Melanie Jones	Case description:	Hash calculation of both the evidence drive and the image in conjunction with imaging.

Imaging completed

Targets

WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889_3.img 80 GB S/shared/Home/Sergii

Passes:	1 pass with default settings for healthy drives
Scheduled sectors:	156,301,488
Imaged sectors:	156,301,488
Errors:	0
Source sector size:	512
Hash method:	Linear
MD5	4975b93754f39d2375ae48d1be0451db
SHA1	2b53497f6be24ed13173abd95a690d27981fa915
Calculated range:	0 - 156,301,487

Post-hash of WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889_3.img

MD5	4975b93754f39d2375ae48d1be0451db ✓
SHA1	2b53497f6be24ed13173abd95a690d27981fa915 ✓
Calculated range:	0 - 156,301,487

Log

Date ↑	Message
2023/09/02 19:31:57	Imaging started
2023/09/02 19:59:28	Pass #1 completed
2023/09/02 19:59:28	Imaging completed
2023/09/02 19:59:28	Target //S/shared/Home/Sergii/WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889_3.img: Post-hashing started
2023/09/02 20:07:24	Target //S/shared/Home/Sergii/WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889_3.img: Post-hashing completed

Imaging results with hash values for both hash during imaging and post-hash.

Calculating dual hash of an existing E01 file

Some source evidence drives and their images can be involved in a long-running investigation case and wait to be presented in court for months or years on end. Data stored on such drives and their image files may eventually get corrupt. Therefore it may be critical for an investigator to ensure the integrity of data on such devices or image files before resuming to work with them or presenting them in court.

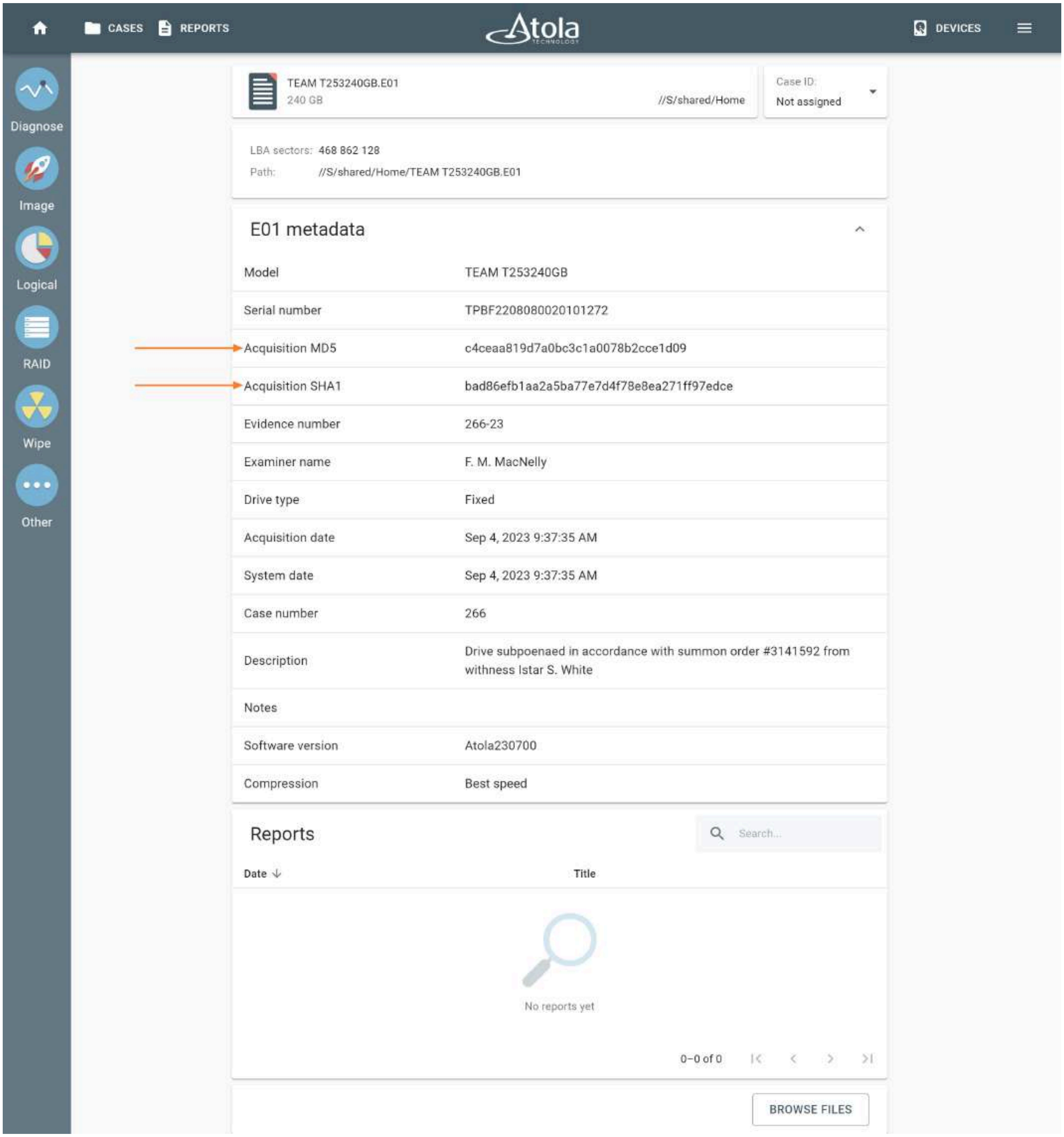
Over the years, E01 file format has become a popular format for forensic purposes due to its ability to store not both the image of the drive, but also case and evidence details. E01 file can also contain both MD5 and SHA-1 hash values.

View the previously calculated hash

To view the previously calculated hash calculated for an E01 file with Atola TaskForce, open the imaging report in the case management system. It contains the hash values calculated during imaging.

Alternatively, you can look up the metadata stored in the E01 file itself:

1. At the top, click **Devices**.
2. Expand the **File** category and click **Select file**.
3. Select the E01 file in the file browser.



TEAM T253240GB.E01
240 GB
//S/shared/Home

Case ID:
Not assigned

LBA sectors: 468 862 128
Path: //S/shared/Home/TEAM T253240GB.E01

E01 metadata

Model	TEAM T253240GB
Serial number	TPBF2208080020101272
Acquisition MD5	c4ceaa819d7a0bc3c1a0078b2cce1d09
Acquisition SHA1	bad86efb1aa2a5ba77e7d4f78e8ea271ff97edce
Evidence number	266-23
Examiner name	F. M. MacNelly
Drive type	Fixed
Acquisition date	Sep 4, 2023 9:37:35 AM
System date	Sep 4, 2023 9:37:35 AM
Case number	266
Description	Drive subpoenaed in accordance with summon order #3141592 from withness Istar S. White
Notes	
Software version	Atola230700
Compression	Best speed

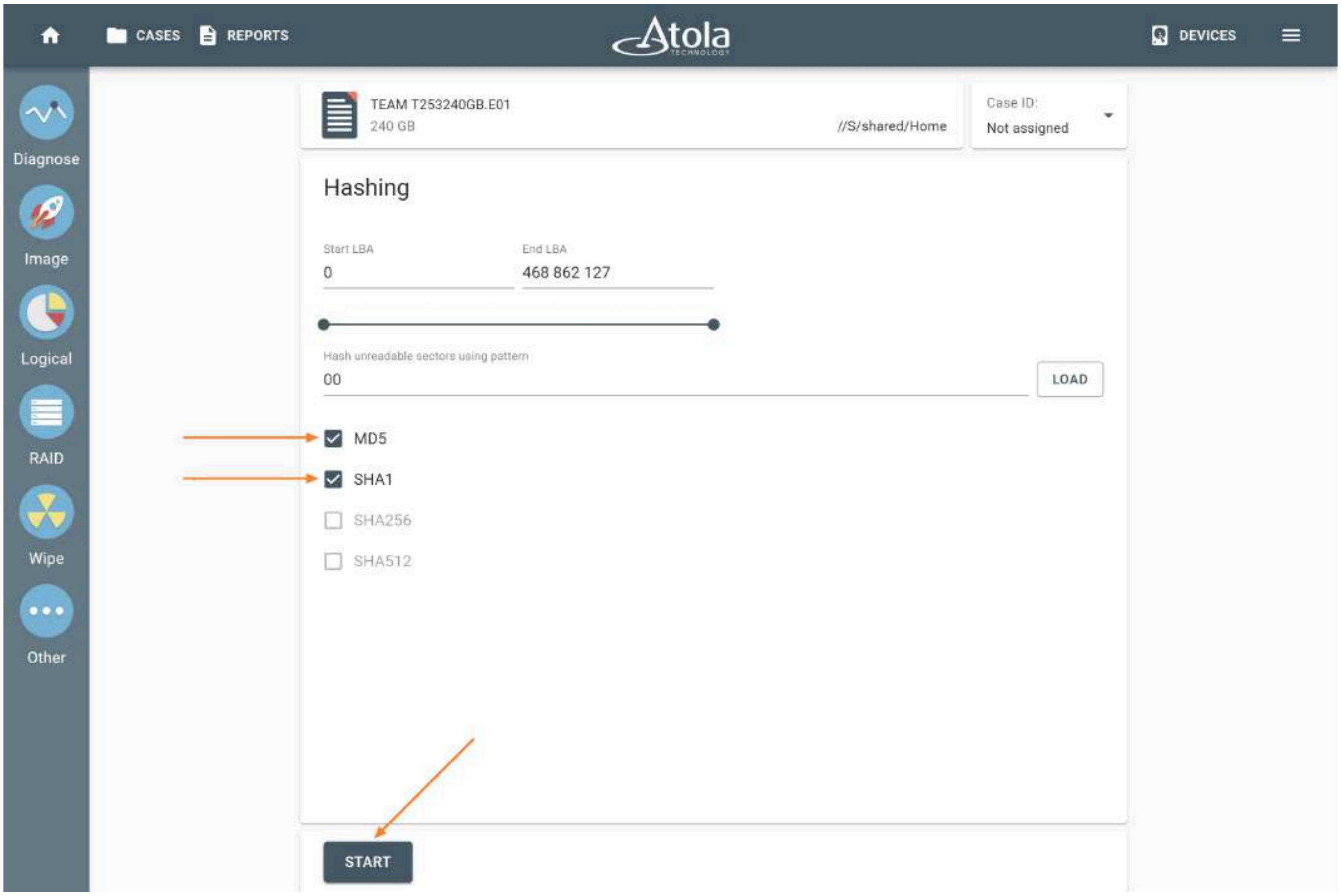
Reports

Hash calculated during imaging stored in E01 file's metadata.

Recalculate the hash for an E01 file

To ensure the integrity of the data in the file, you can recalculate its hash.

1. On the left, click **Other**, and then **Hash**.
2. To choose the file for which you want to calculate hash, expand the **File** category and click **Select file**.
3. Select the E01 file in the file browser.
4. Adjust hashing settings. Make sure to select the same hashing types (MD5, SHA1, etc.)
5. Click **Start**.



TEAM T253240GB.E01
240 GB
//S/shared/Home

Case ID:
Not assigned

Hashing

Start LBA
0

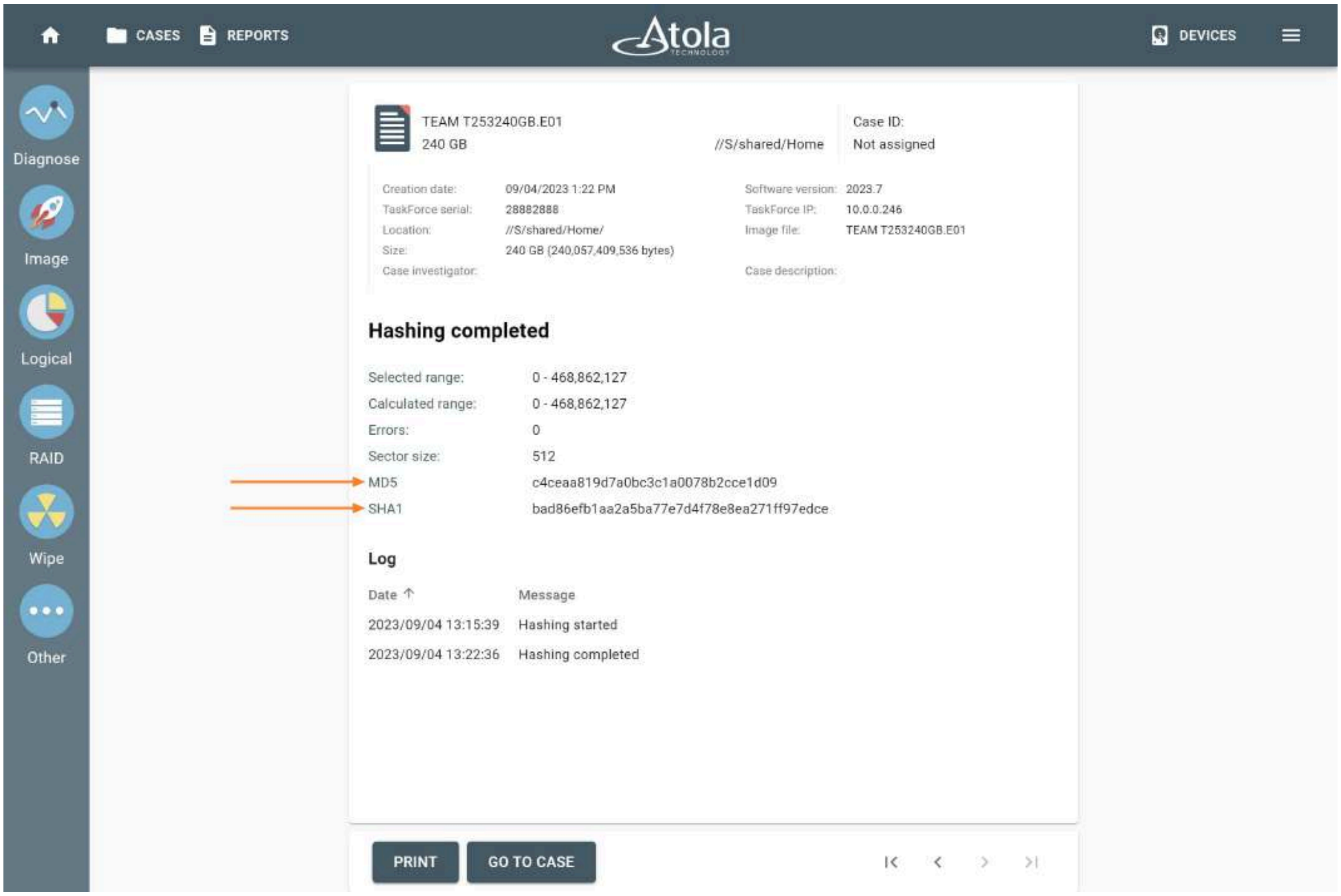
End LBA
468 862 127

Hash unreadable sectors using pattern
00

☑ MD5
☑ SHA1
☐ SHA256
☐ SHA512

Starting hash calculation.

When the hash calculation is completed, you can make sure that the two sets of hashes are identical.



TEAM T253240GB.E01
240 GB
//S/shared/Home

Case ID:
Not assigned

Creation date:	09/04/2023 1:22 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	//S/shared/Home/	Image file:	TEAM T253240GB.E01
Size:	240 GB (240,057,409,536 bytes)		
Case investigator:		Case description:	

Hashing completed

Selected range:	0 - 468,862,127
Calculated range:	0 - 468,862,127
Errors:	0
Sector size:	512
MD5	c4ceaa819d7a0bc3c1a0078b2cce1d09
SHA1	bad86efb1aa2a5ba77e7d4f78e8ea271ff97edce

Log

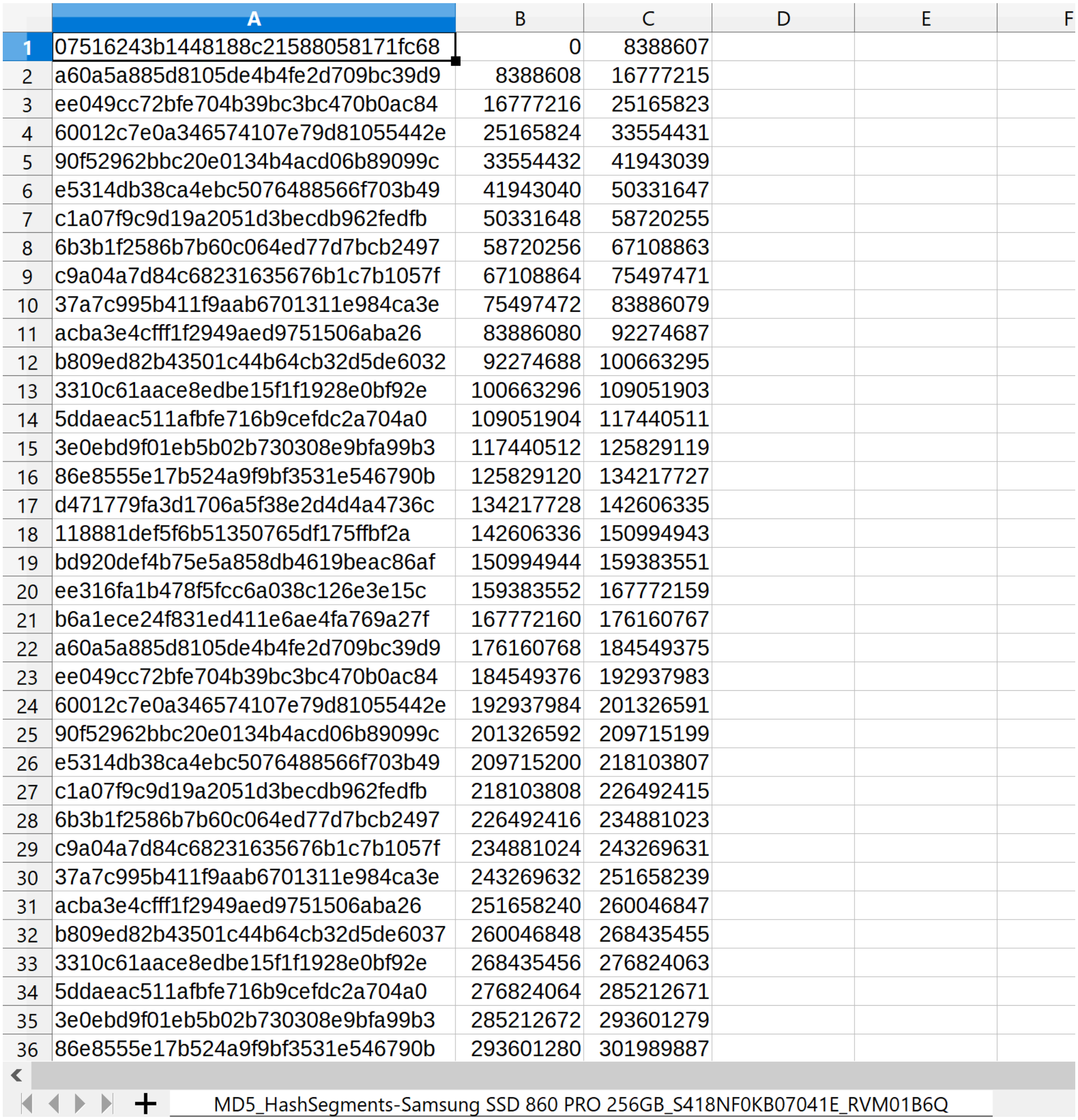
Date ↑	Message
2023/09/04 13:15:39	Hashing started
2023/09/04 13:22:36	Hashing completed

Comparing the calculated hash values to the ones calculated during imaging.

Segmented hashing for data verification

Segmented hashing allows verifying data, imaged from damaged media. The image can be verified even if data gets corrupt over time.

Segmented hashing produces a CSV file in the following format:



	A	B	C	D	E	F
1	07516243b1448188c21588058171fc68	0	8388607			
2	a60a5a885d8105de4b4fe2d709bc39d9	8388608	16777215			
3	ee049cc72bfe704b39bc3bc470b0ac84	16777216	25165823			
4	60012c7e0a346574107e79d81055442e	25165824	33554431			
5	90f52962bbc20e0134b4acd06b89099c	33554432	41943039			
6	e5314db38ca4ebc5076488566f703b49	41943040	50331647			
7	c1a07f9c9d19a2051d3becdb962fedfb	50331648	58720255			
8	6b3b1f2586b7b60c064ed77d7bcb2497	58720256	67108863			
9	c9a04a7d84c68231635676b1c7b1057f	67108864	75497471			
10	37a7c995b411f9aab6701311e984ca3e	75497472	83886079			
11	acba3e4cfff1f2949aed9751506aba26	83886080	92274687			
12	b809ed82b43501c44b64cb32d5de6032	92274688	100663295			
13	3310c61aace8edbe15f1f1928e0bf92e	100663296	109051903			
14	5ddaeac511afbfe716b9cefdc2a704a0	109051904	117440511			
15	3e0ebd9f01eb5b02b730308e9bfa99b3	117440512	125829119			
16	86e8555e17b524a9f9bf3531e546790b	125829120	134217727			
17	d471779fa3d1706a5f38e2d4d4a4736c	134217728	142606335			
18	118881def5f6b51350765df175ffbf2a	142606336	150994943			
19	bd920def4b75e5a858db4619beac86af	150994944	159383551			
20	ee316fa1b478f5fcc6a038c126e3e15c	159383552	167772159			
21	b6a1ece24f831ed411e6ae4fa769a27f	167772160	176160767			
22	a60a5a885d8105de4b4fe2d709bc39d9	176160768	184549375			
23	ee049cc72bfe704b39bc3bc470b0ac84	184549376	192937983			
24	60012c7e0a346574107e79d81055442e	192937984	201326591			
25	90f52962bbc20e0134b4acd06b89099c	201326592	209715199			
26	e5314db38ca4ebc5076488566f703b49	209715200	218103807			
27	c1a07f9c9d19a2051d3becdb962fedfb	218103808	226492415			
28	6b3b1f2586b7b60c064ed77d7bcb2497	226492416	234881023			
29	c9a04a7d84c68231635676b1c7b1057f	234881024	243269631			
30	37a7c995b411f9aab6701311e984ca3e	243269632	251658239			
31	acba3e4cfff1f2949aed9751506aba26	251658240	260046847			
32	b809ed82b43501c44b64cb32d5de6037	260046848	268435455			
33	3310c61aace8edbe15f1f1928e0bf92e	268435456	276824063			
34	5ddaeac511afbfe716b9cefdc2a704a0	276824064	285212671			
35	3e0ebd9f01eb5b02b730308e9bfa99b3	285212672	293601279			
36	86e8555e17b524a9f9bf3531e546790b	293601280	301989887			

+
MD5_HashSegments-Samsung SSD 860 PRO 256GB_S418NF0KB07041E_RVM01B6Q

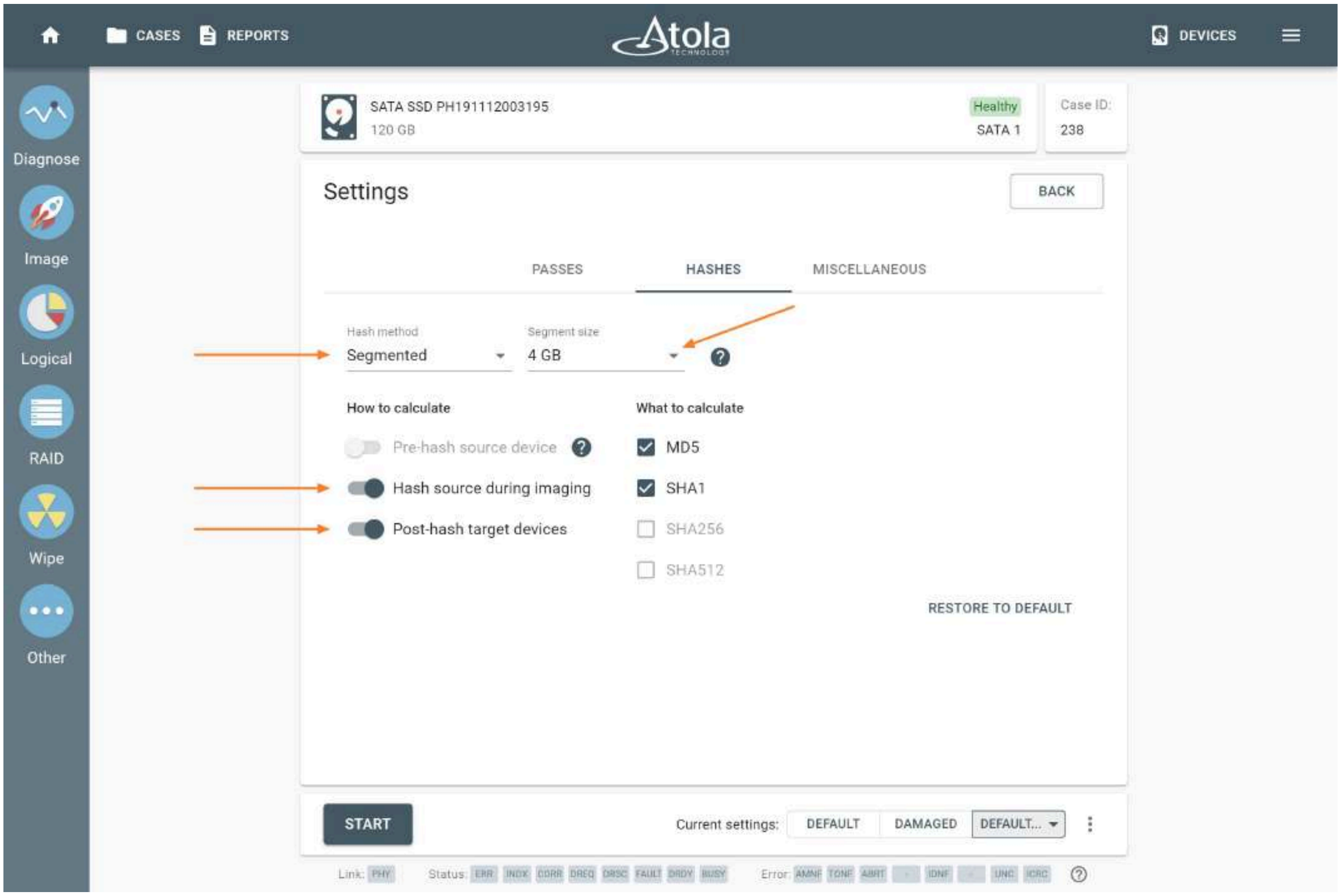
Segmented hashing vs regular hashing

With conventional hashing method you get a single hash for the entire image, while segmented hashing allows getting many hashes of corresponding LBA ranges of the image. The sum LBA ranges represents the entire image.

Verifying all hashes in a set allows you to prove that the entire image has not been modified.

Segmented hashing and post-hashing of the target for immediate image verification

1. Go to the imaging **Settings**.
2. On the **Hashes** tab, select **Segmented** hashing method.
3. To obtain both sets of hashes for the evidence drive and the image, toggle **Post-hash target devices**.



SATA SSD PH191112003195
120 GB
SATA 1
Case ID: 238

Settings

Hash method: Segmented
Segment size: 4 GB

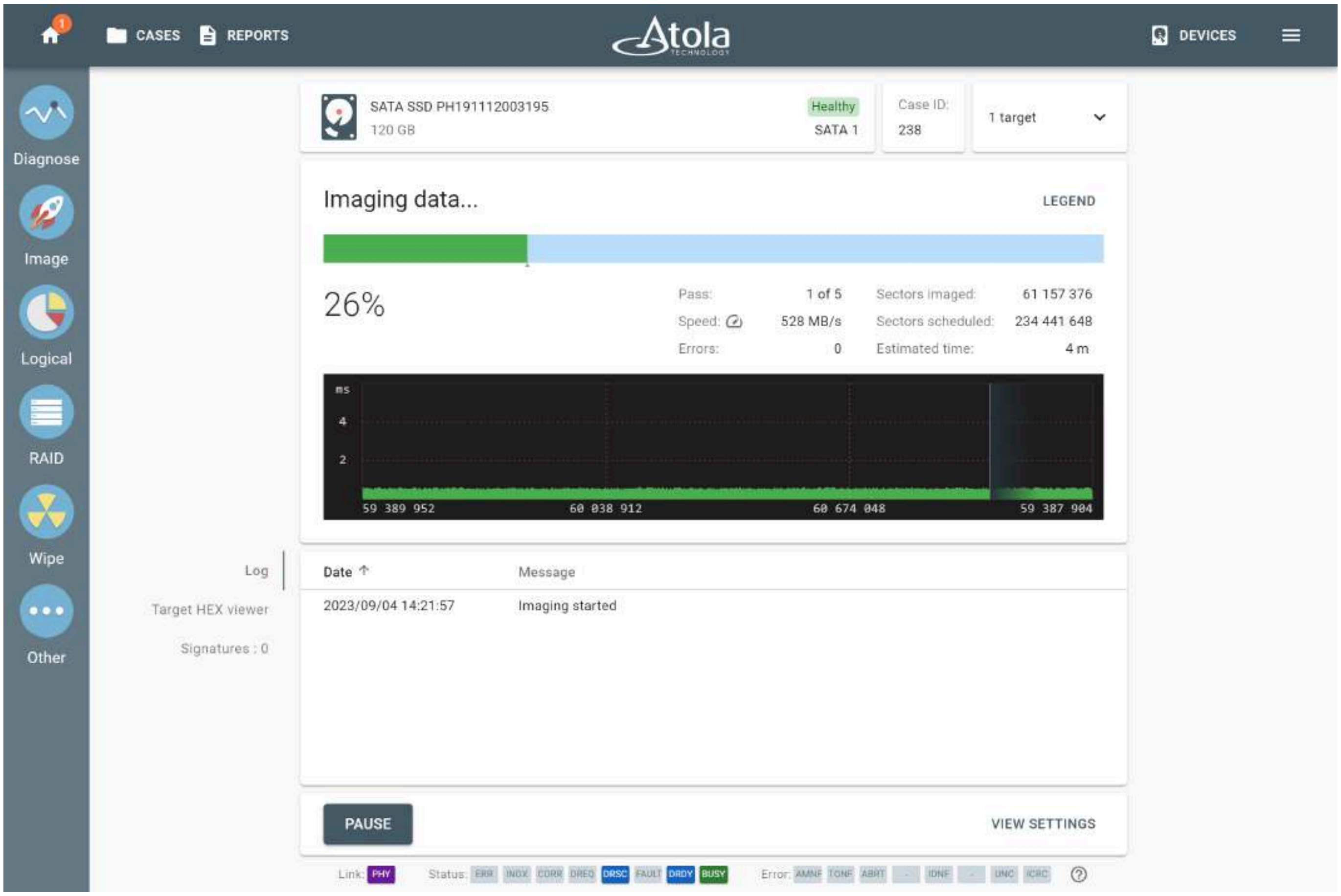
How to calculate
- ○ Pre-hash source device
- ● Hash source during imaging
- ● Post-hash target devices

What to calculate
- ☑ MD5
- ☑ SHA1
- □ SHA256
- □ SHA512

Current settings: DEFAULT...

Selecting hashing method.

Hashing while imaging does not slow down the imaging session:



SATA SSD PH191112003195
120 GB
Healthy
SATA 1
Case ID: 238
1 target

Imaging data...

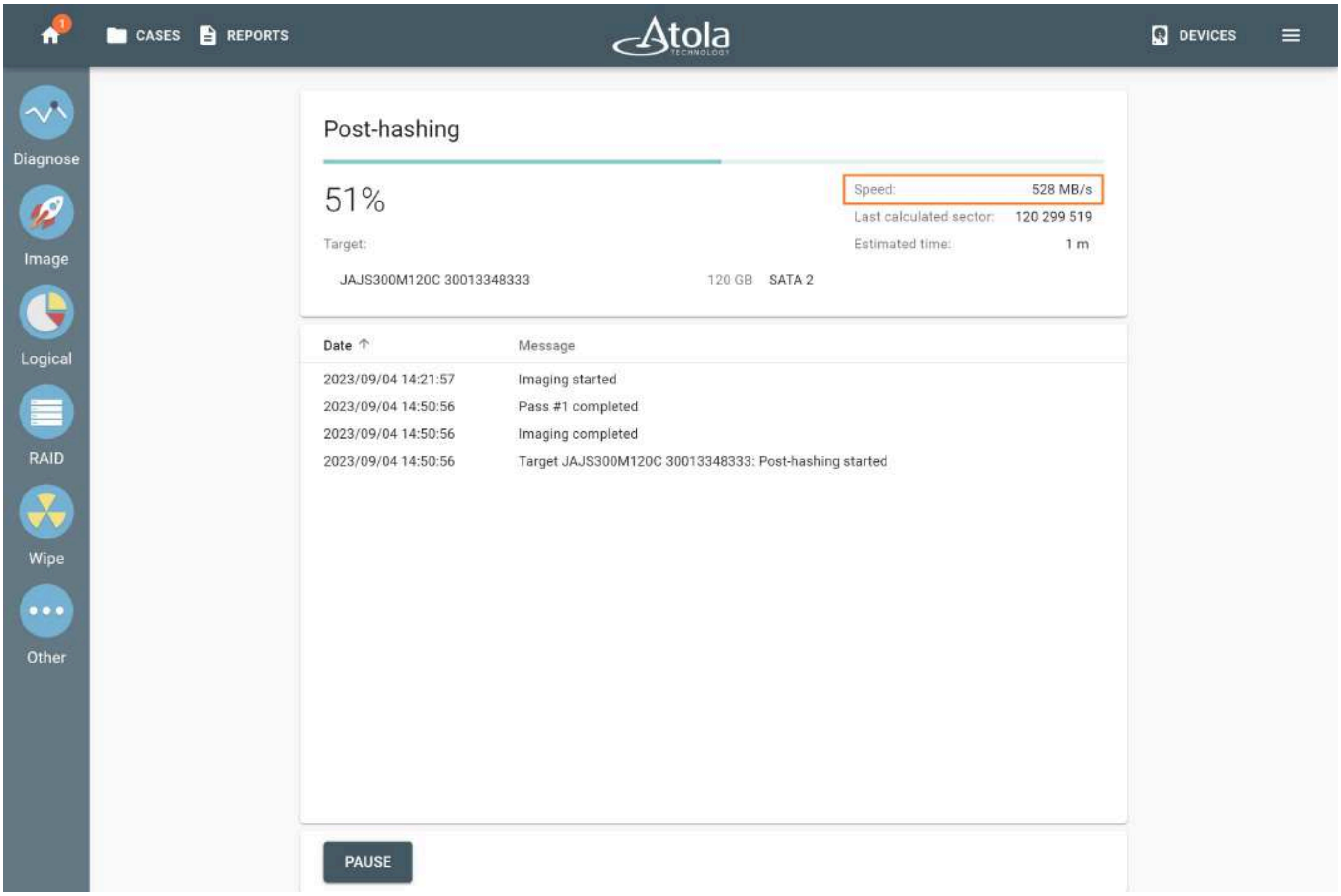
26%

Pass: 1 of 5
Speed: 528 MB/s
Errors: 0
Sectors imaged: 61 157 376
Sectors scheduled: 234 441 648
Estimated time: 4 m

Date	Message
2023/09/04 14:21:57	Imaging started

TaskForce 2 imaging session.

Post-hashing will commence as soon as the imaging session is completed:



Post-hashing

51%

Speed: 528 MB/s
Last calculated sector: 120 299 519
Estimated time: 1 m

Target:

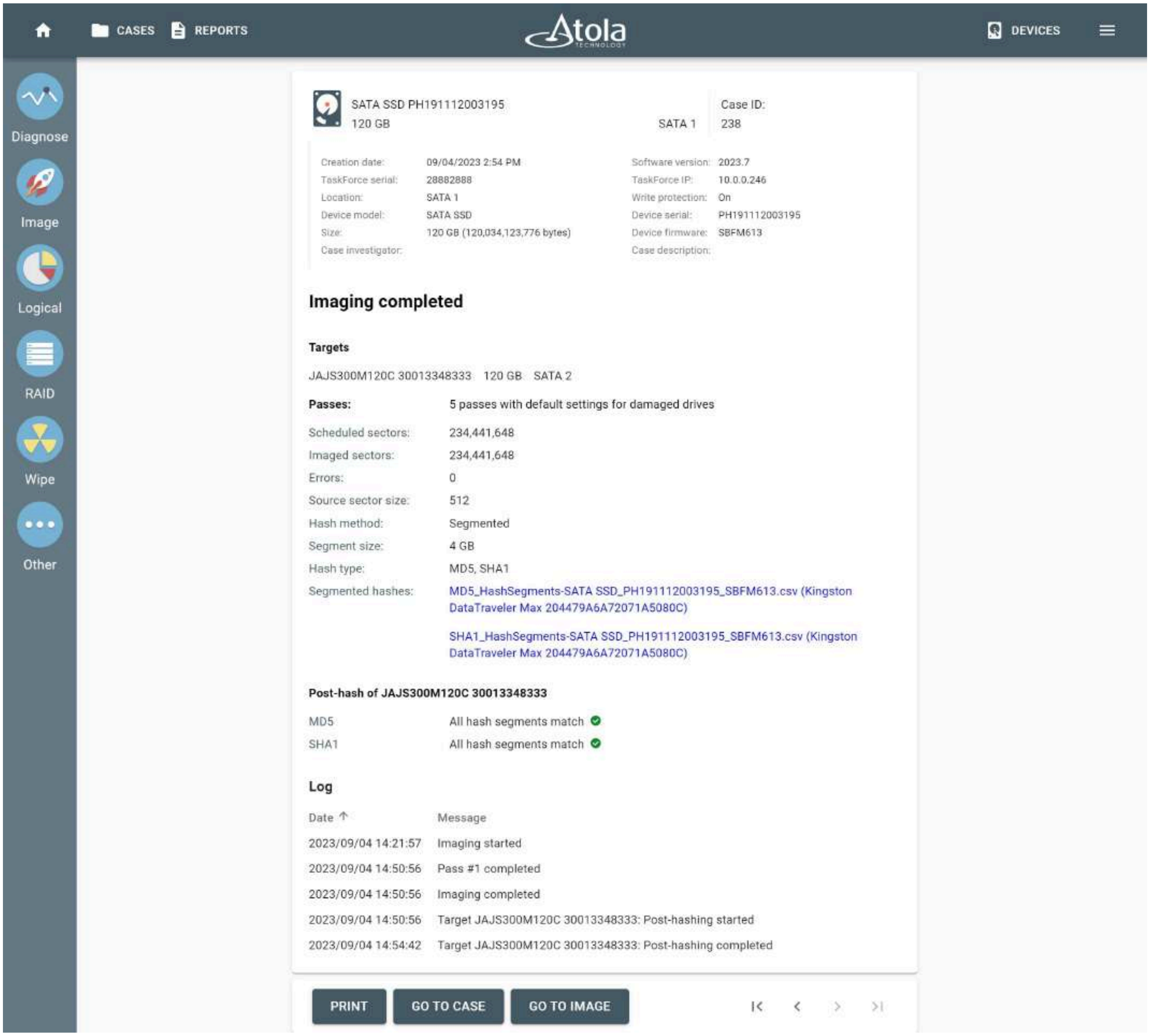
JAJS300M120C 30013348333 120 GB SATA 2

Date ↑	Message
2023/09/04 14:21:57	Imaging started
2023/09/04 14:50:56	Pass #1 completed
2023/09/04 14:50:56	Imaging completed
2023/09/04 14:50:56	Target JAJS300M120C 30013348333: Post-hashing started

Atola TaskForce 2: Post-hashing.

In the **Imaging completed** report you can see imaging results with the link to the file with segmented hashes.

In case you select the post-hashing of the target, you also get the results of cross-checking between the hash sets of the evidence drive and the image.



SATA SSD PH191112003195
120 GB

SATA 1

Case ID:
238

Creation date:	09/04/2023 2:54 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	SATA SSD	Device serial:	PH191112003195
Size:	120 GB (120,034,123,776 bytes)	Device firmware:	SBFM613
Case investigator:		Case description:	

Imaging completed

Targets

JAJS300M120C 30013348333   120 GB   SATA 2

Passes:	5 passes with default settings for damaged drives
Scheduled sectors:	234,441,648
Imaged sectors:	234,441,648
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5, SHA1
Segmented hashes:	MD5_HashSegments-SATA SSD_PH191112003195_SBFM613.csv (Kingston DataTraveler Max 204479A6A72071A5080C) SHA1_HashSegments-SATA SSD_PH191112003195_SBFM613.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

Post-hash of JAJS300M120C 30013348333

MD5	All hash segments match ✓
SHA1	All hash segments match ✓

Log

Date ↑	Message
2023/09/04 14:21:57	Imaging started
2023/09/04 14:50:56	Pass #1 completed
2023/09/04 14:50:56	Imaging completed
2023/09/04 14:50:56	Target JAJS300M120C 30013348333: Post-hashing started
2023/09/04 14:54:42	Target JAJS300M120C 30013348333: Post-hashing completed

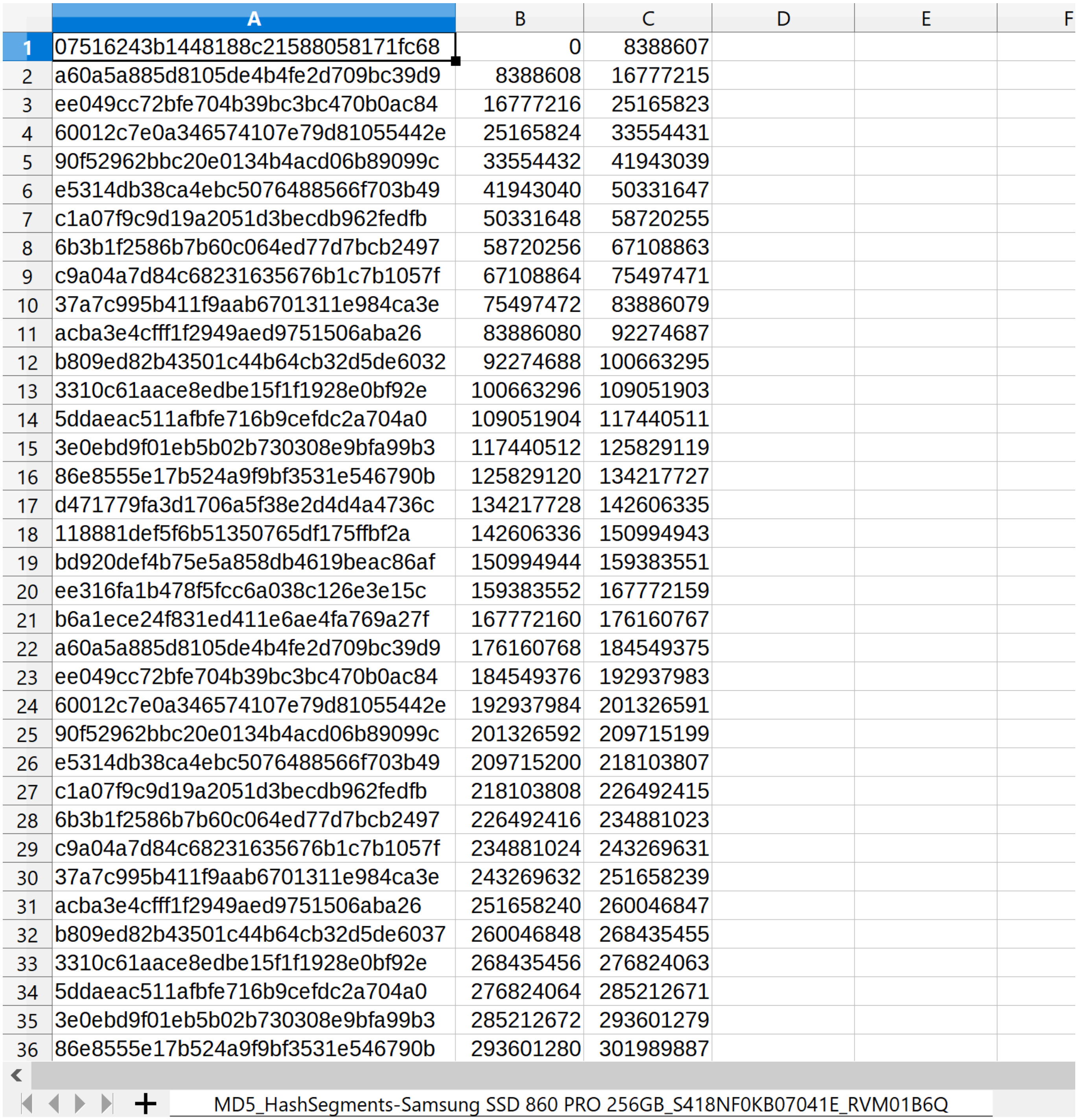
Atola forensic imager: Imaging results

Verify damaged images with segmented hashing

Segmented hashing is a non-linear hashing method that allows hashing damaged drives. Hashes are calculated only for the good areas of evidence media, while bad areas, that are impossible to read and image, are left out of the calculation.

In Atola TaskForce 2, the segmented hashing module produces a list of hashes of corresponding LBA ranges of the image. Then hashes are saved into a CSV file in the following format: *Hash, start LBA, end LBA*.

The sum of the LBA ranges represents the entire image. By verifying all hashes in a set you can prove that the entire image has not been modified.



	A	B	C	D	E	F
1	07516243b1448188c21588058171fc68	0	8388607			
2	a60a5a885d8105de4b4fe2d709bc39d9	8388608	16777215			
3	ee049cc72bfe704b39bc3bc470b0ac84	16777216	25165823			
4	60012c7e0a346574107e79d81055442e	25165824	33554431			
5	90f52962bbc20e0134b4acd06b89099c	33554432	41943039			
6	e5314db38ca4ebc5076488566f703b49	41943040	50331647			
7	c1a07f9c9d19a2051d3becdb962fedfb	50331648	58720255			
8	6b3b1f2586b7b60c064ed77d7bcb2497	58720256	67108863			
9	c9a04a7d84c68231635676b1c7b1057f	67108864	75497471			
10	37a7c995b411f9aab6701311e984ca3e	75497472	83886079			
11	acba3e4cfff1f2949aed9751506aba26	83886080	92274687			
12	b809ed82b43501c44b64cb32d5de6032	92274688	100663295			
13	3310c61aace8edbe15f1f1928e0bf92e	100663296	109051903			
14	5ddaeac511afbfe716b9cefdc2a704a0	109051904	117440511			
15	3e0ebd9f01eb5b02b730308e9bfa99b3	117440512	125829119			
16	86e8555e17b524a9f9bf3531e546790b	125829120	134217727			
17	d471779fa3d1706a5f38e2d4d4a4736c	134217728	142606335			
18	118881def5f6b51350765df175ffbf2a	142606336	150994943			
19	bd920def4b75e5a858db4619beac86af	150994944	159383551			
20	ee316fa1b478f5fcc6a038c126e3e15c	159383552	167772159			
21	b6a1ece24f831ed411e6ae4fa769a27f	167772160	176160767			
22	a60a5a885d8105de4b4fe2d709bc39d9	176160768	184549375			
23	ee049cc72bfe704b39bc3bc470b0ac84	184549376	192937983			
24	60012c7e0a346574107e79d81055442e	192937984	201326591			
25	90f52962bbc20e0134b4acd06b89099c	201326592	209715199			
26	e5314db38ca4ebc5076488566f703b49	209715200	218103807			
27	c1a07f9c9d19a2051d3becdb962fedfb	218103808	226492415			
28	6b3b1f2586b7b60c064ed77d7bcb2497	226492416	234881023			
29	c9a04a7d84c68231635676b1c7b1057f	234881024	243269631			
30	37a7c995b411f9aab6701311e984ca3e	243269632	251658239			
31	acba3e4cfff1f2949aed9751506aba26	251658240	260046847			
32	b809ed82b43501c44b64cb32d5de6037	260046848	268435455			
33	3310c61aace8edbe15f1f1928e0bf92e	268435456	276824063			
34	5ddaeac511afbfe716b9cefdc2a704a0	276824064	285212671			
35	3e0ebd9f01eb5b02b730308e9bfa99b3	285212672	293601279			
36	86e8555e17b524a9f9bf3531e546790b	293601280	301989887			

MD5_HashSegments-Samsung SSD 860 PRO 256GB_S418NF0KB07041E_RVM01B6Q

Benefits of segmented hashing

With the conventional **linear hashing** method you get a single hash for the entire image. As the linear hashing stops upon encountering the first bad sector, it is impossible to calculate hash for the entire space of the source evidence drive.

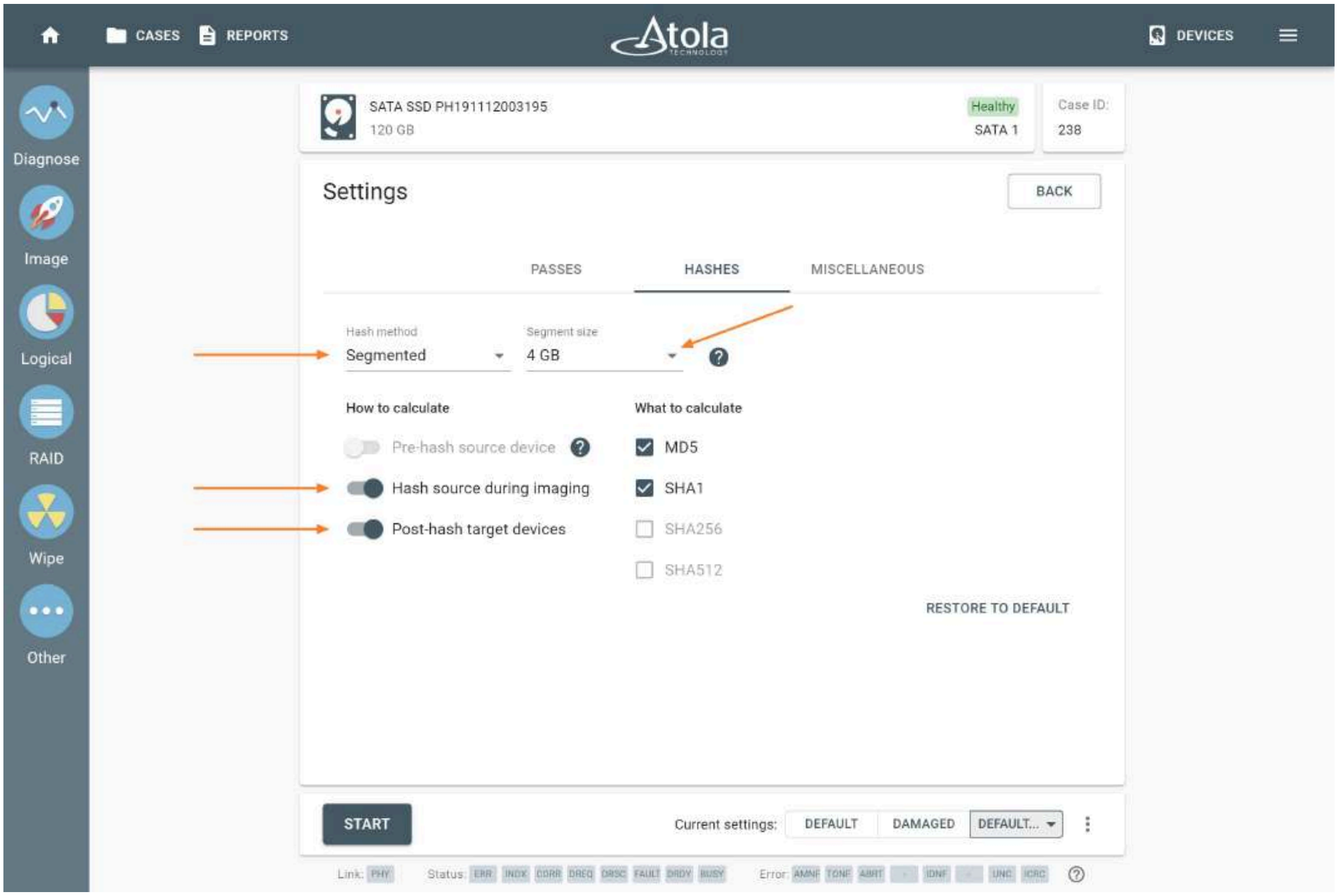
With **segmented hashing**, hashing can be performed during the multipass imaging of a damaged drive. Hashes are calculated only for the successfully imaged areas, while all bad sectors are excluded from the calculation.

If an acquired evidence image is damaged at some point in the future, with the regular linear hashes you will get a hash mismatch upon verification, and the entire image becomes useless. With segmented hashes only the hash of the damaged segment will become invalid.

Calculate segmented hashes of a source and target devices

To calculate segmented hashes of a damaged drive during imaging and post-hash the target for immediate image verification, do the following:

1. Go to the imaging **Settings**.
2. On the **Hashes** tab, select **Segmented hashing** method and specify **Segment size**.
3. To obtain both sets of hashes for the evidence drive and the image, toggle **Post-hash target devices**.



SATA SSD PH191112003195
120 GB
Healthy
SATA 1
Case ID: 238

Settings

Hash method: Segmented
Segment size: 4 GB

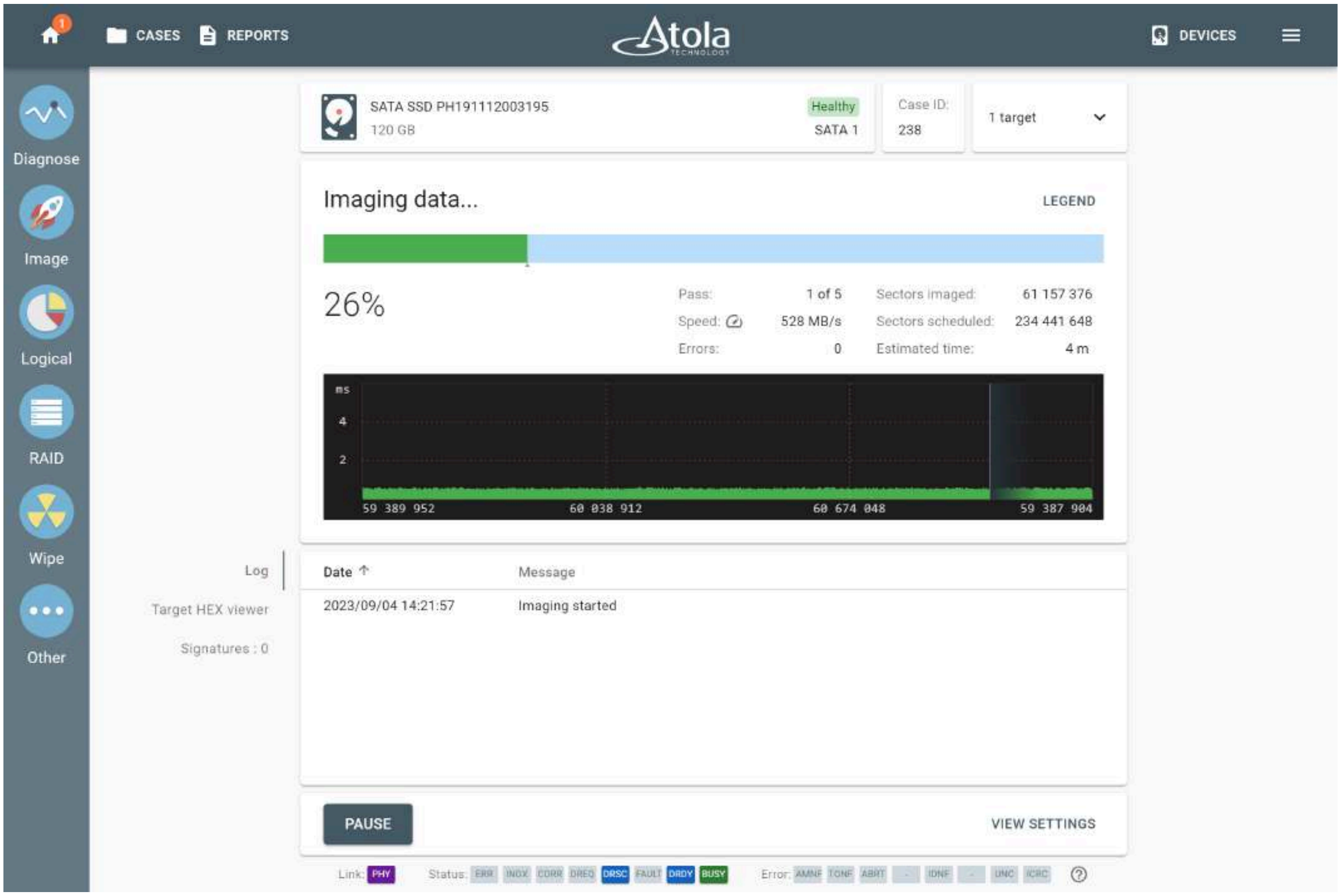
How to calculate
Pre-hash source device: off
Hash source during imaging: on
Post-hash target devices: on

What to calculate
☑ MD5
☑ SHA1
☐ SHA256
☐ SHA512

Current settings: DEFAULT | DAMAGED | DEFAULT...

Selecting hashing method.

Hashing while imaging does not slow down the imaging session:



SATA SSD PH191112003195
120 GB
Healthy
SATA 1

Case ID: 238

1 target

Imaging data...

26%

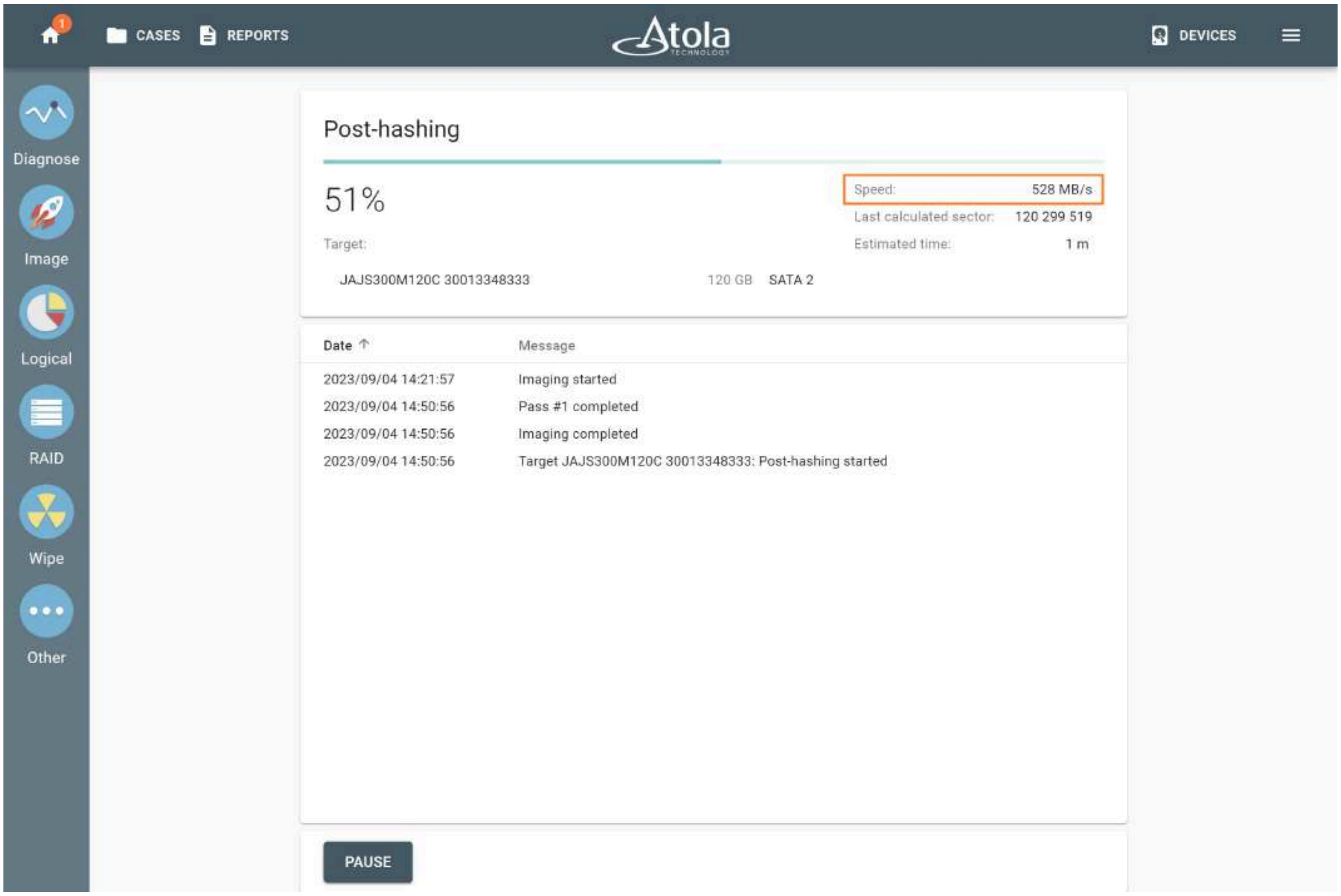
Pass: 1 of 5
Speed: 528 MB/s
Errors: 0
Sectors imaged: 61 157 376
Sectors scheduled: 234 441 648
Estimated time: 4 m

Log
Target HEX viewer
Signatures : 0

```
Date                 Message
2023/09/04 14:21:57  Imaging started
```

TaskForce 2 imaging session.

Post-hashing commences as soon as the imaging session is completed:



Post-hashing

51%

Speed:	528 MB/s
Last calculated sector:	120 299 519
Estimated time:	1 m

Target:

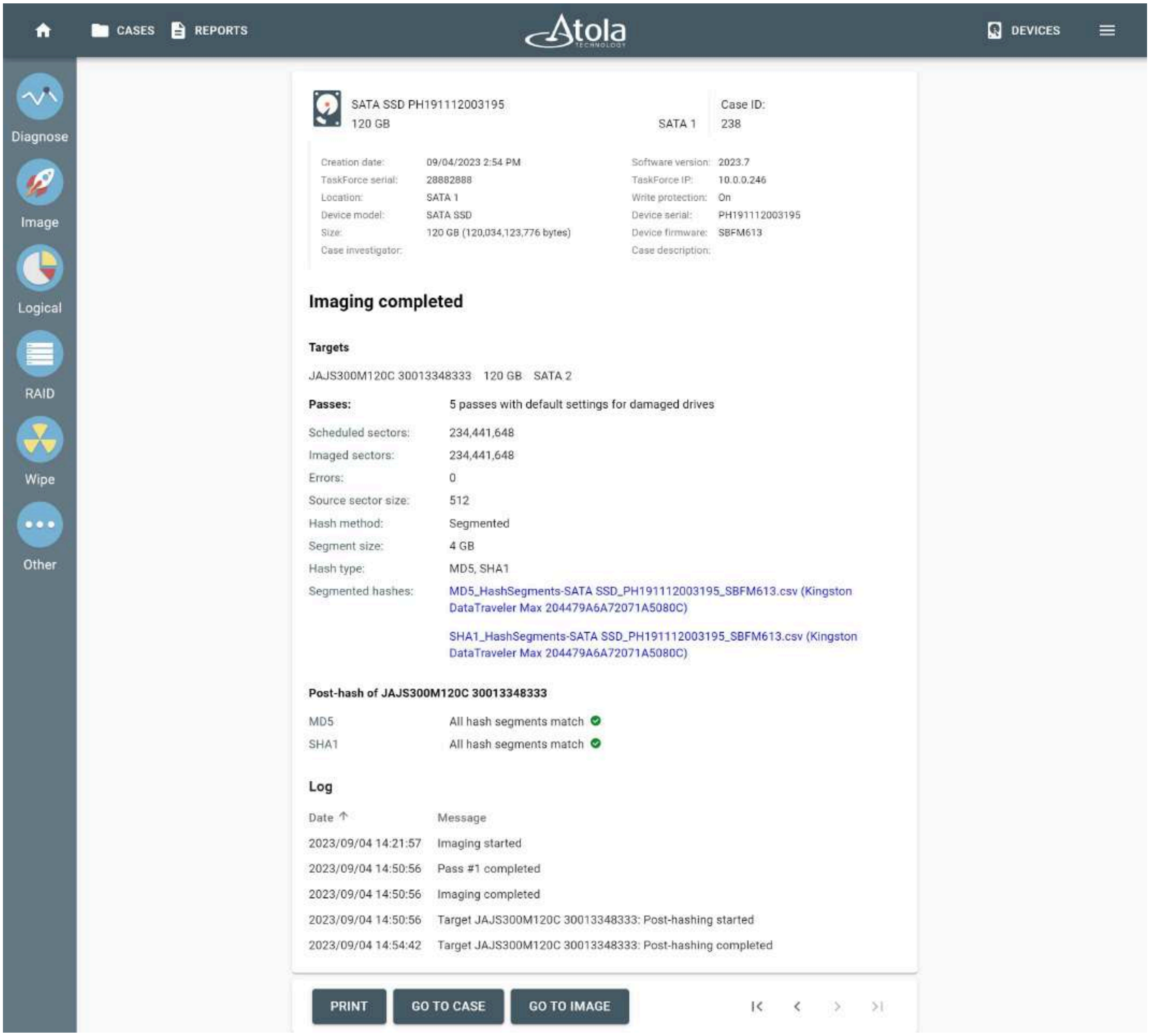
JAJS300M120C 30013348333 120 GB SATA 2

```
Date ↑                 Message
2023/09/04 14:21:57    Imaging started
2023/09/04 14:50:56    Pass #1 completed
2023/09/04 14:50:56    Imaging completed
2023/09/04 14:50:56    Target JAJS300M120C 30013348333: Post-hashing started
```

Atola TaskForce 2: Post-hashing.

In the **Imaging completed** report, you can see imaging results with the link to the file with segmented hashes.

In case you select the post-hashing of the target, you also get the results of cross-checking between the hash sets of the evidence drive and the image.



SATA SSD PH191112003195
120 GB
SATA 1
Case ID:
238

Creation date:	09/04/2023 2:54 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	SATA SSD	Device serial:	PH191112003195
Size:	120 GB (120,034,123,776 bytes)	Device firmware:	SBFM613
Case investigator:		Case description:	

Imaging completed

Targets

JAJS300M120C 30013348333 120 GB SATA 2

Passes:	5 passes with default settings for damaged drives
Scheduled sectors:	234,441,648
Imaged sectors:	234,441,648
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5, SHA1
Segmented hashes:	MD5_HashSegments-SATA SSD_PH191112003195_SBFM613.csv (Kingston DataTraveler Max 204479A6A72071A5080C) SHA1_HashSegments-SATA SSD_PH191112003195_SBFM613.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

Post-hash of JAJS300M120C 30013348333

MD5	All hash segments match ✓
SHA1	All hash segments match ✓

Log

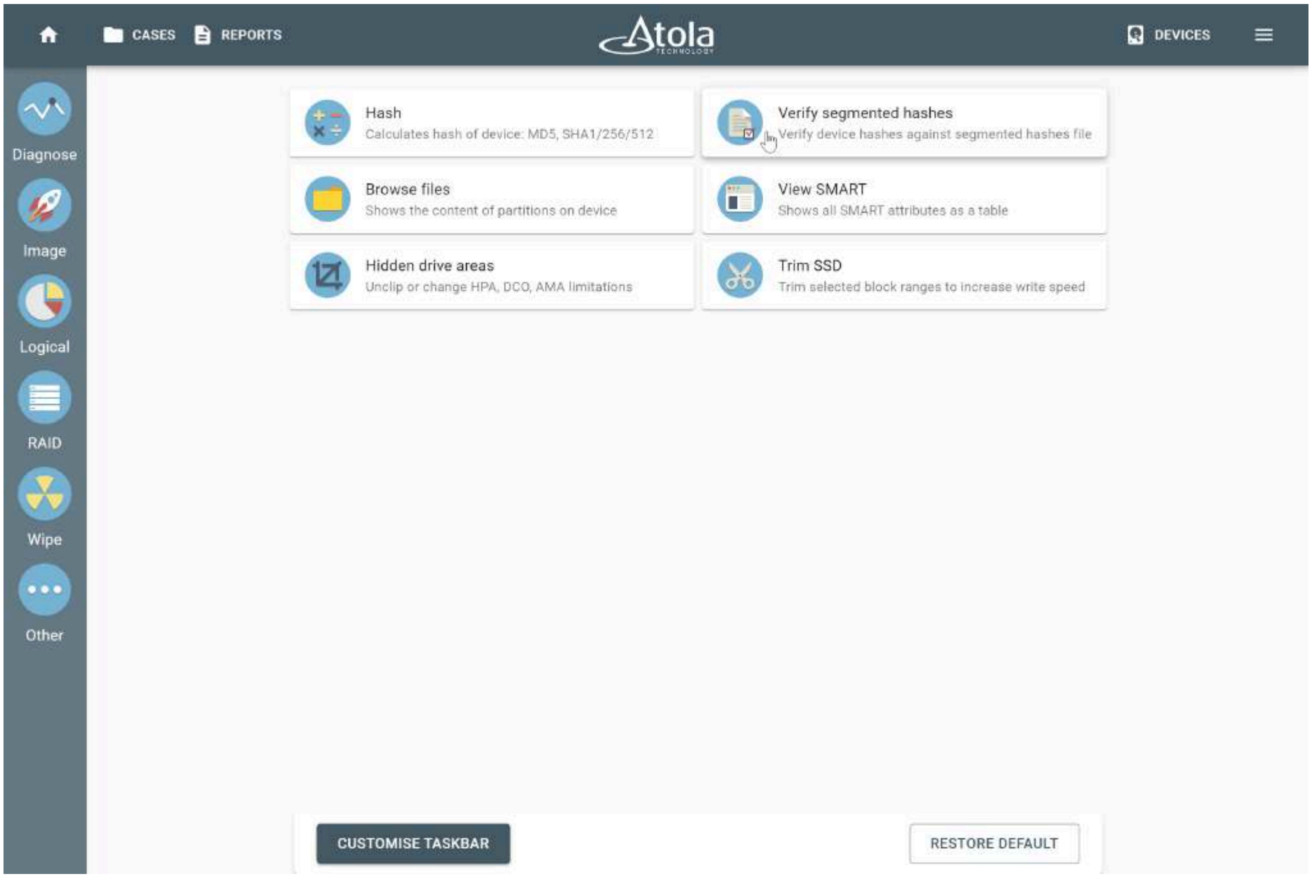
```
Date ↑               Message
2023/09/04 14:21:57  Imaging started
2023/09/04 14:50:56  Pass #1 completed
2023/09/04 14:50:56  Imaging completed
2023/09/04 14:50:56  Target JAJS300M120C 30013348333: Post-hashing started
2023/09/04 14:54:42  Target JAJS300M120C 30013348333: Post-hashing completed
```

Atola TaskForce 2: Imaging results.

Verify an image of a drive with segmented hashing

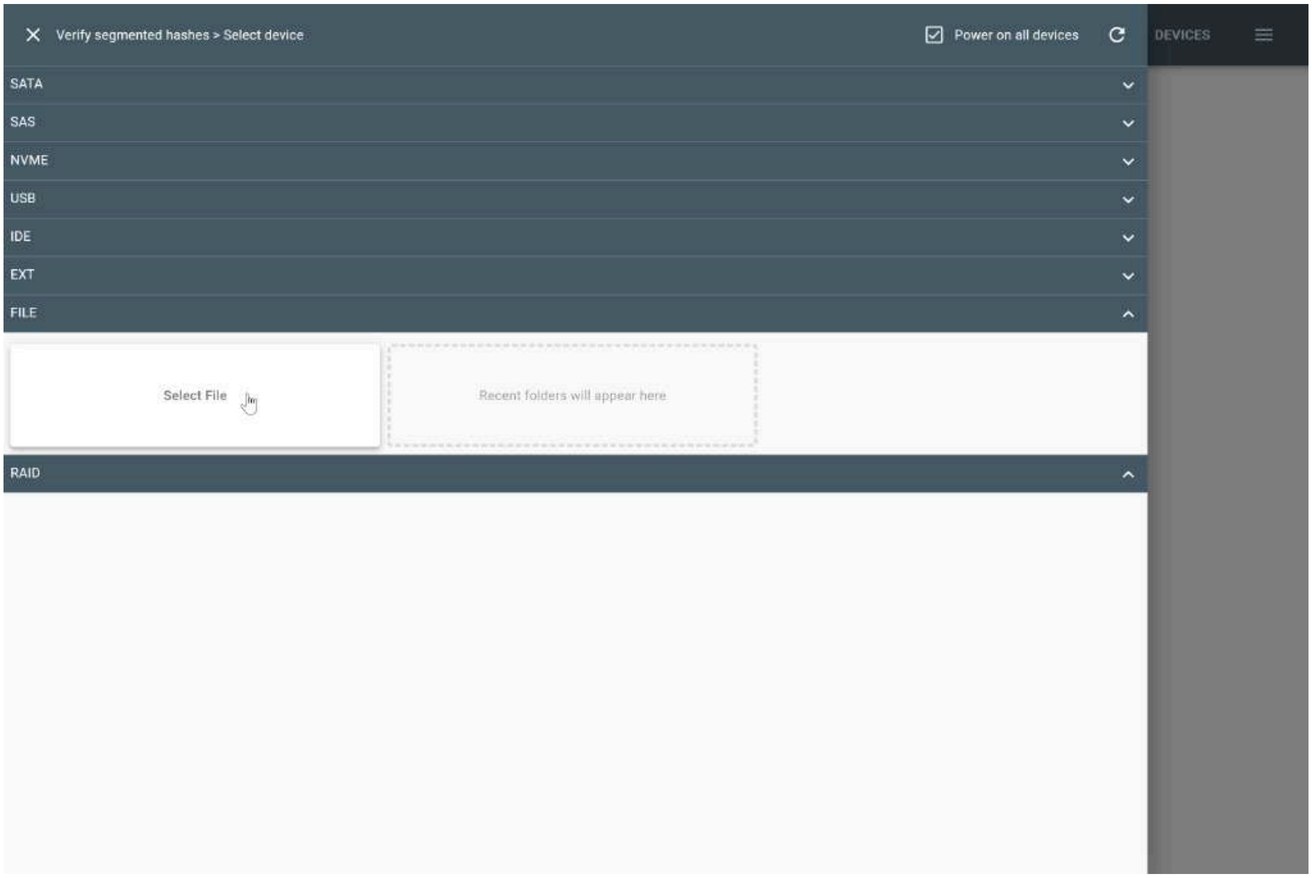
To verify an acquired image file of an evidence drive with segmented hashing, do the following:

1. In the TaskForce window, go to **Other** > **Verify segmented hashes**.


CASES
REPORTS
Atola
DEVICES
Diagnose
Image
Logical
RAID
Wipe
Other
Hash
Calculates hash of device: MD5, SHA1/256/512
Verify segmented hashes
Verify device hashes against segmented hashes file
Browse files
Shows the content of partitions on device
View SMART
Shows all SMART attributes as a table
Hidden drive areas
Unclip or change HPA, DCO, AMA limitations
Trim SSD
Trim selected block ranges to increase write speed
CUSTOMISE TASKBAR
RESTORE DEFAULT

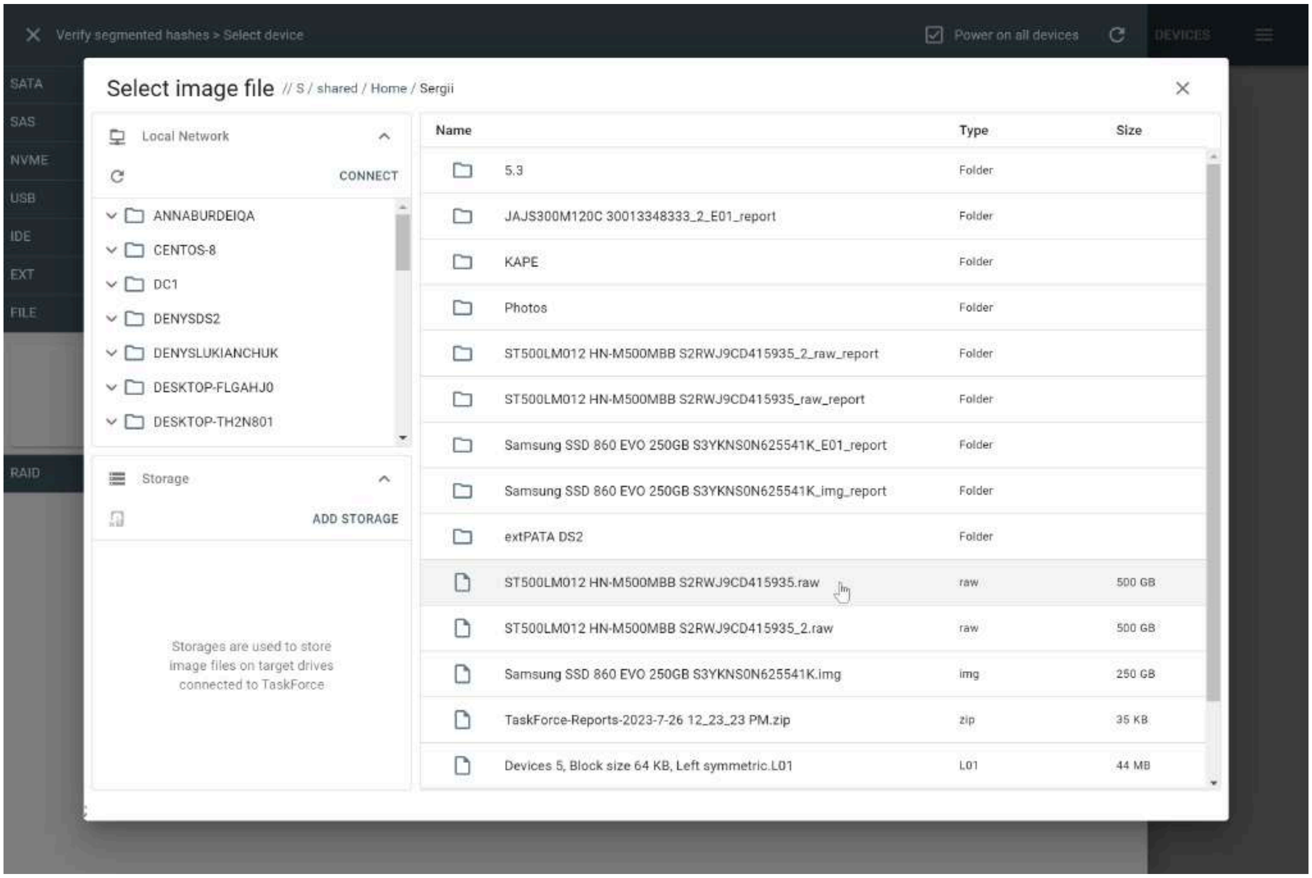
The Verify segmented hashed command on the Other page.

2. The **Select device** panel opens. Expand the **File** section and click **Select file**.


Verify segmented hashes > Select device
☑ Power on all devices
DEVICES
SATA
SAS
NVME
USB
IDE
EXT
FILE
Select File
Recent folders will appear here
RAID

The Select device panel.

3. Select an image file you want to verify. The E01, AFF4 and Raw formats are supported.

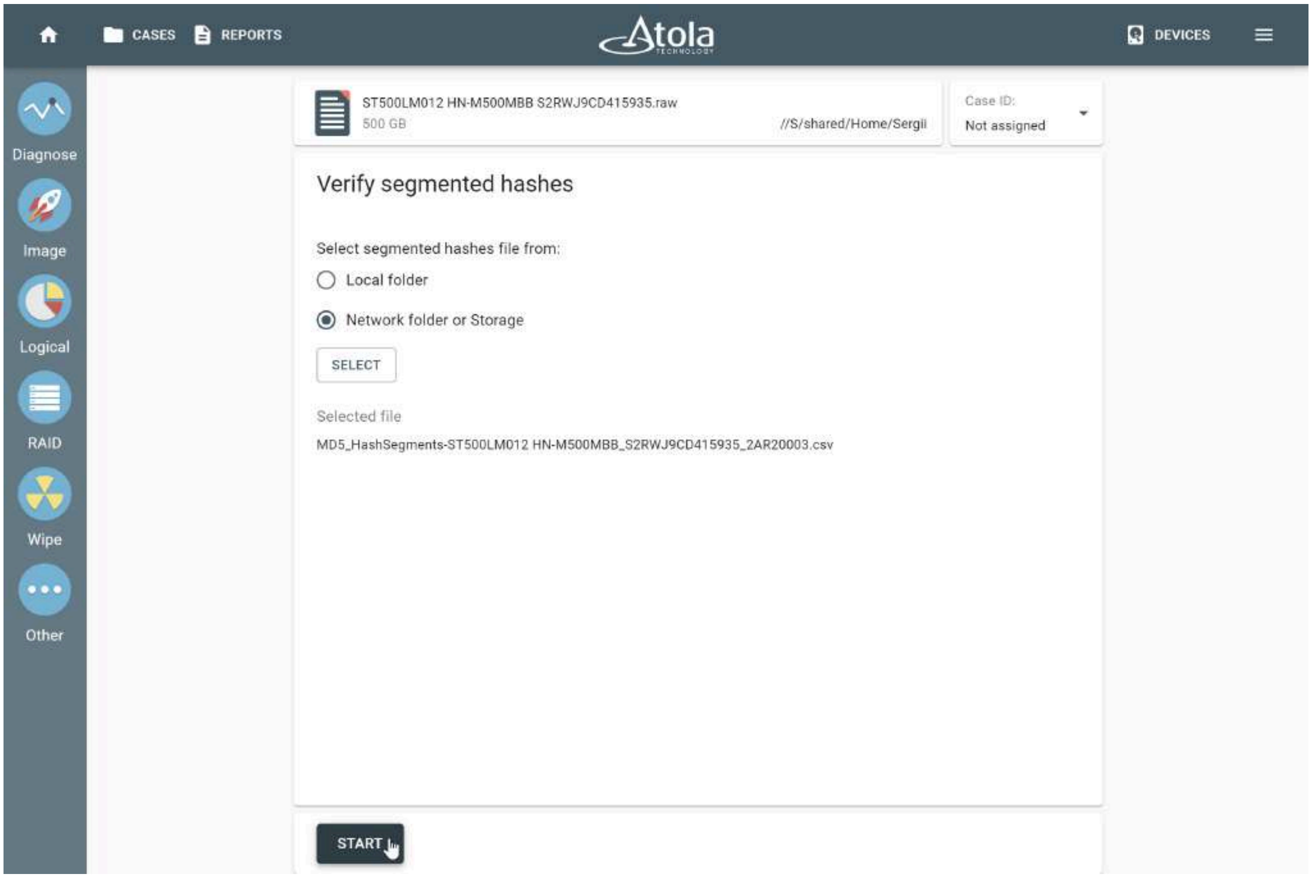


Storages are used to store image files on target drives connected to TaskForce

Name	Type	Size
5.3	Folder	
JAJS300M120C 30013348333_2_E01_report	Folder	
KAPE	Folder	
Photos	Folder	
ST500LM012 HN-M500MBB S2RWJ9CD415935_2_raw_report	Folder	
ST500LM012 HN-M500MBB S2RWJ9CD415935_raw_report	Folder	
Samsung SSD 860 EVO 250GB S3YKNS0N625541K_E01_report	Folder	
Samsung SSD 860 EVO 250GB S3YKNS0N625541K_img_report	Folder	
extPATA DS2	Folder	
ST500LM012 HN-M500MBB S2RWJ9CD415935.raw	raw	500 GB
ST500LM012 HN-M500MBB S2RWJ9CD415935_2.raw	raw	500 GB
Samsung SSD 860 EVO 250GB S3YKNS0N625541K.img	img	250 GB
TaskForce-Reports-2023-7-26 12_23_23 PM.zip	zip	35 KB
Devices 5, Block size 64 KB, Left symmetric.L01	L01	44 MB

Selecting an image file to verify segmented hashes.

4. Select the CSV file with segmented hashes that relates to your image file:
    a. Choose either **Local folder** or **Network folder or Storage**.
    b. Click **Select**.
    c. Find and select a CSV file with segmented hashes.
5. Click **Start**.



ST500LM012 HN-M500MBB S2RWJ9CD415935.raw
500 GB
//S/shared/Home/Sergii

Case ID:
Not assigned

Verify segmented hashes

Select segmented hashes file from:

○ Local folder

● Network folder or Storage

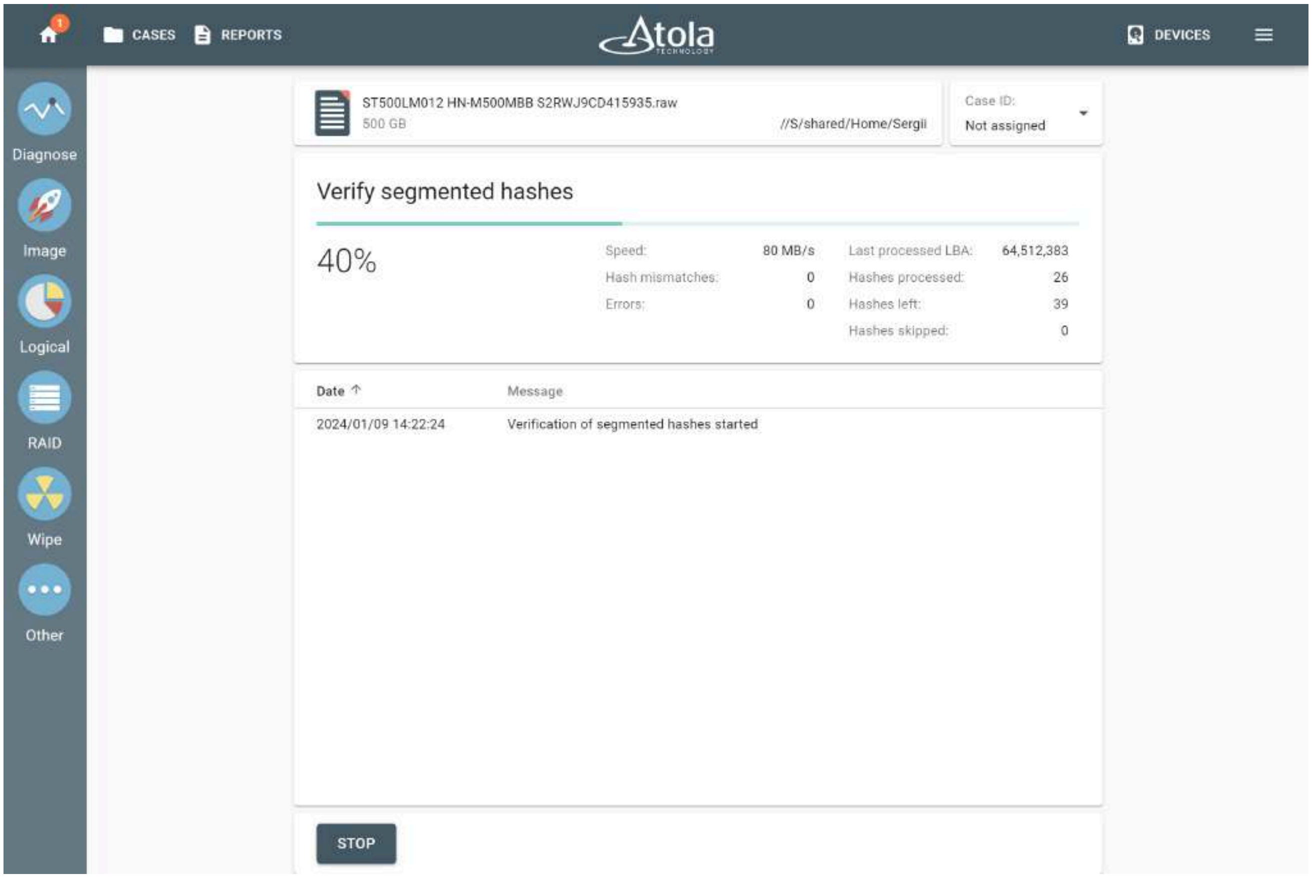
SELECT

Selected file
MD5_HashSegments-ST500LM012 HN-M500MBB_S2RWJ9CD415935_2AR20003.csv

START

Selecting a CSV file with a list of segmented hashes.

6. TaskForce 2 starts the data verification process.



ST500LM012 HN-M500MBB S2RWJ9CD415935.raw
500 GB
//S/shared/Home/Sergii

Case ID:
Not assigned

Verify segmented hashes

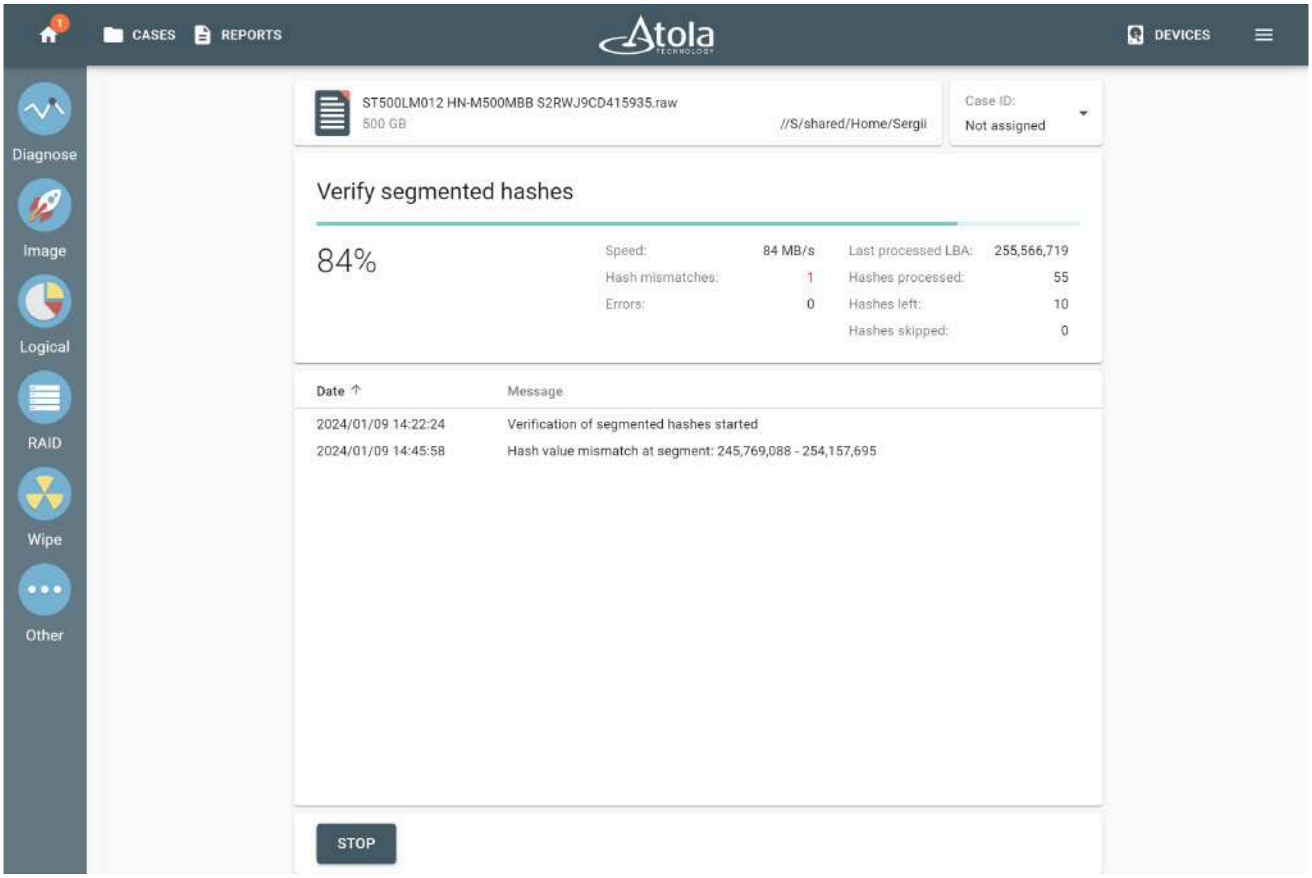
40%

Speed:	80 MB/s	Last processed LBA:	64,512,383
Hash mismatches:	0	Hashes processed:	26
Errors:	0	Hashes left:	39
		Hashes skipped:	0

Date ↑	Message
2024/01/09 14:22:24	Verification of segmented hashes started

The process of verifying segmented hashes.

7. If TaskForce encounters a hash value mismatch, it is reflected in the **Hash mismatches** counter and in the event log, with *Start and End LBA* of the respective segment.



ST500LM012 HN-M500MBB S2RWJ9CD415935.raw
500 GB
//S/shared/Home/Sergii

Case ID:
Not assigned

Verify segmented hashes

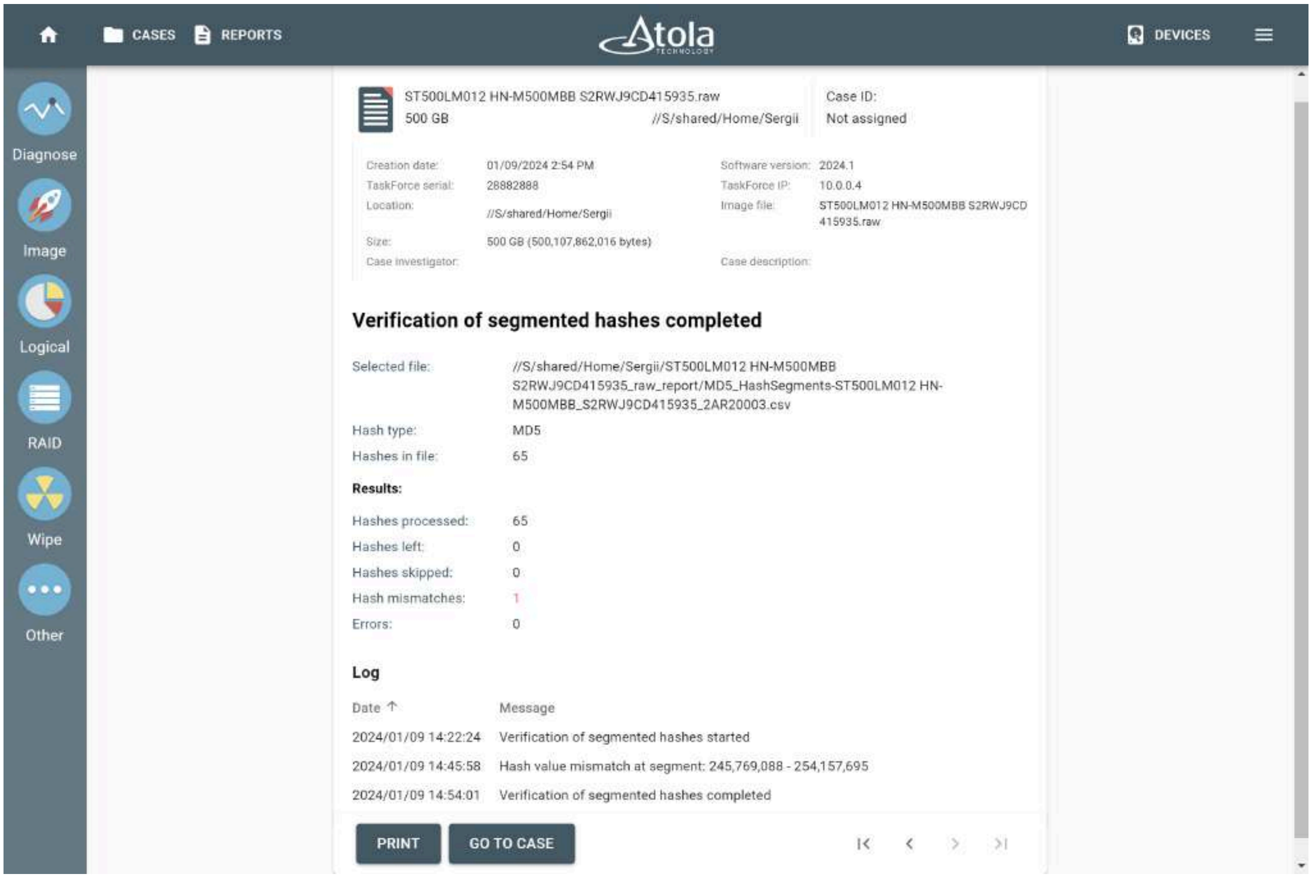
84%

Speed: 84 MB/s
Hash mismatches: 1
Errors: 0
Last processed LBA: 255,566,719
Hashes processed: 55
Hashes left: 10
Hashes skipped: 0

Date ↑	Message
2024/01/09 14:22:24	Verification of segmented hashes started
2024/01/09 14:45:58	Hash value mismatch at segment: 245,769,088 - 254,157,695

Hashes of one of the segments do not match.

8. Once verification of segmented hashes is completed, TaskForce 2 generates a detailed report about its results. The report contains information about the verified image and the file with its segmented hashes, hash type, number of processed hashes and found mismatches if any.



ST500LM012 HN-M500MBB S2RWJ9CD415935.raw
500 GB //S/shared/Home/Sergii

Case ID:
Not assigned

Creation date: 01/09/2024 2:54 PM
TaskForce serial: 28882888
Location: //S/shared/Home/Sergii
Size: 500 GB (500,107,862,016 bytes)
Case investigator:

Software version: 2024.1
TaskForce IP: 10.0.0.4
Image file: ST500LM012 HN-M500MBB S2RWJ9CD415935.raw
Case description:

Verification of segmented hashes completed

Selected file: //S/shared/Home/Sergii/ST500LM012 HN-M500MBB S2RWJ9CD415935_raw_report/MD5_HashSegments-ST500LM012 HN-M500MBB_S2RWJ9CD415935_2AR20003.csv

Hash type: MD5

Hashes in file: 65

Results:

Hashes processed: 65

Hashes left: 0

Hashes skipped: 0

Hash mismatches: 1

Errors: 0

Log

```
Date ↑               Message
2024/01/09 14:22:24  Verification of segmented hashes started
2024/01/09 14:45:58  Hash value mismatch at segment: 245,769,088 - 254,157,695
2024/01/09 14:54:01  Verification of segmented hashes completed
```

The report about completed verification of segmented hashes.

Case management system and report types

TaskForce's case management system records every step of the data acquisition process: every operation is automatically added to the case from the moment a device is identified including date, time, imaging map and hash values. When a hard drive is imaged, its imaging map is recorded detailing all the sectors that have been skipped.

Whenever an operator connects a hard drive to the TaskForce 2, the system makes an automatic database lookup and retrieves all past records associated with that particular hard drive. New entries will be added seamlessly to the database. You do not need to enable case management or take any additional actions for it to start functioning; it is fully embedded into TaskForce 2 and works at all times.

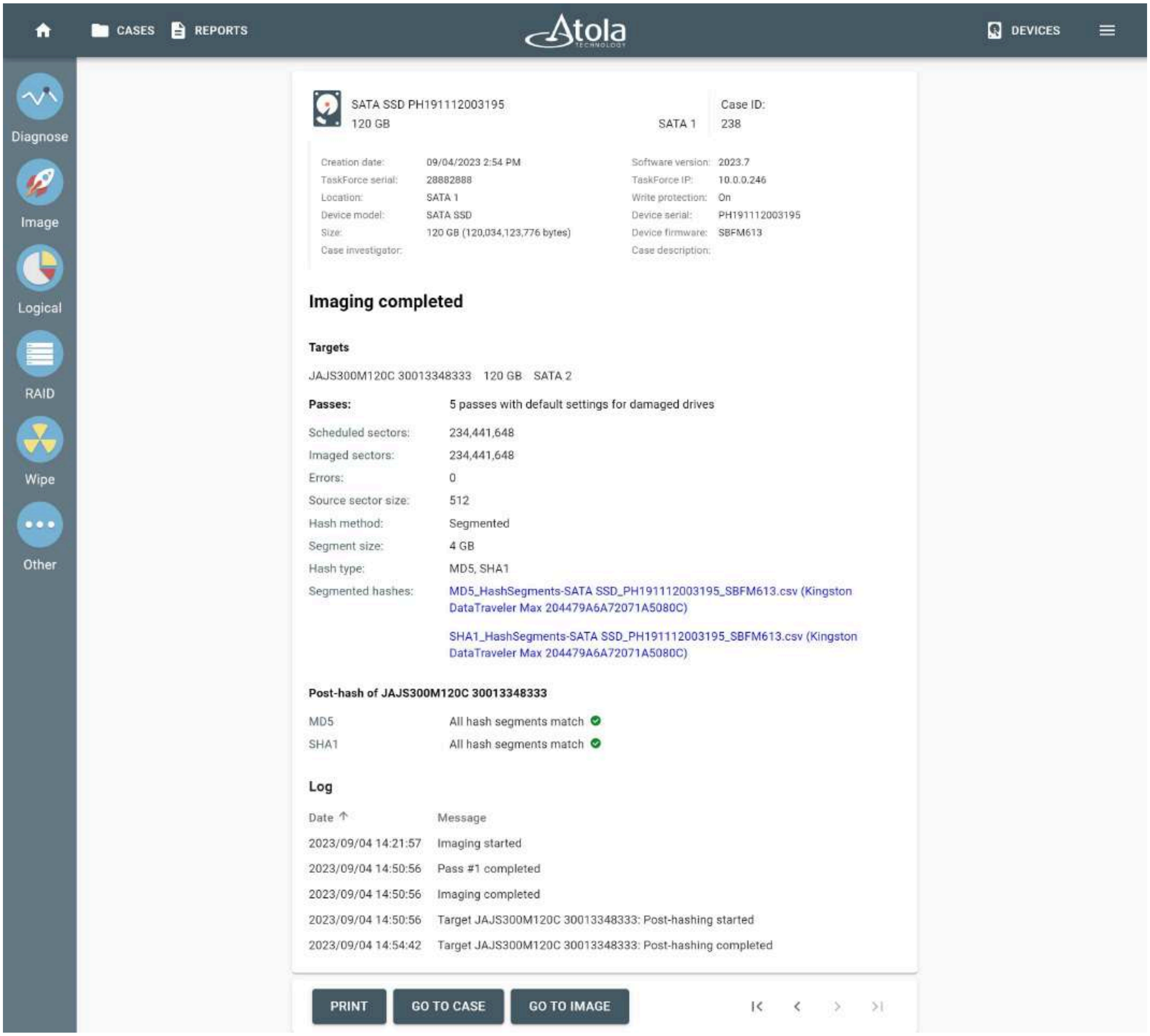
Case number can be assigned and changed at any time. The system also allows browsing through all cases and reports, without corresponding devices being connected to the unit.

Report types and formats

There are two types of reports in TaskForce 2:

1. Device reports are created every time an action is taken to the drive: drive identification, imaging, hashing, wiping and other operations related to the drive are documented in these reports.
2. Non-device reports are created to register any changes made to the cases: case opening, case details change, case import and export.

All reports have these key elements: a header that provides device and case details, an action summary and task details (task settings, task log, etc.).



SATA SSD PH191112003195
120 GB

SATA 1

Case ID:
238

Creation date:	09/04/2023 2:54 PM	Software version:	2023.7
TaskForce serial:	28882888	TaskForce IP:	10.0.0.246
Location:	SATA 1	Write protection:	On
Device model:	SATA SSD	Device serial:	PH191112003195
Size:	120 GB (120,034,123,776 bytes)	Device firmware:	SBFM613
Case investigator:		Case description:	

Imaging completed

Targets

JAJS300M120C 30013348333   120 GB   SATA 2

Passes:	5 passes with default settings for damaged drives
Scheduled sectors:	234,441,648
Imaged sectors:	234,441,648
Errors:	0
Source sector size:	512
Hash method:	Segmented
Segment size:	4 GB
Hash type:	MD5, SHA1
Segmented hashes:	MD5_HashSegments-SATA SSD_PH191112003195_SBFM613.csv (Kingston DataTraveler Max 204479A6A72071A5080C) SHA1_HashSegments-SATA SSD_PH191112003195_SBFM613.csv (Kingston DataTraveler Max 204479A6A72071A5080C)

Post-hash of JAJS300M120C 30013348333

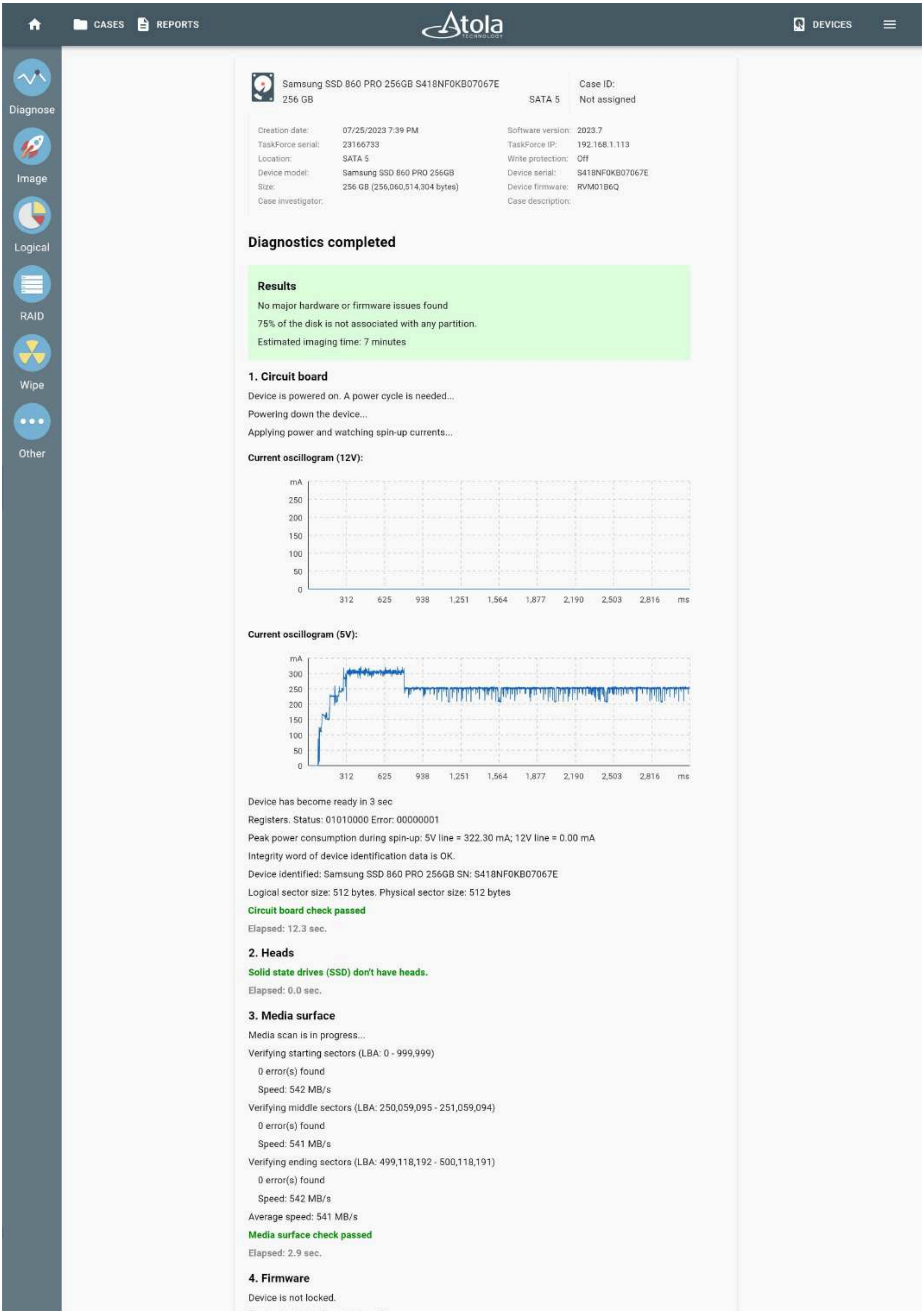
MD5	All hash segments match ✓
SHA1	All hash segments match ✓

Log

Date ↑	Message
2023/09/04 14:21:57	Imaging started
2023/09/04 14:50:56	Pass #1 completed
2023/09/04 14:50:56	Imaging completed
2023/09/04 14:50:56	Target JAJS300M120C 30013348333: Post-hashing started
2023/09/04 14:54:42	Target JAJS300M120C 30013348333: Post-hashing completed

Imaging report in Atola TaskForce 2.

A diagnostics report contains even more details: it lists the checkup results for all subsystems of a drive and includes oscillograms, SMART table, etc.



Samsung SSD 860 PRO 256GB S418NF0KB07067E
256 GB SATA 5

Case ID:
Not assigned

Creation date:	07/25/2023 7:39 PM	Software version:	2023.7
TaskForce serial:	23166733	TaskForce IP:	192.168.1.113
Location:	SATA 5	Write protection:	Off
Device model:	Samsung SSD 860 PRO 256GB	Device serial:	S418NF0KB07067E
Size:	256 GB (256,060,514,304 bytes)	Device firmware:	RVM01B6Q
Case investigator:		Case description:	

Diagnostics completed

Results

No major hardware or firmware issues found

75% of the disk is not associated with any partition.

Estimated imaging time: 7 minutes

1. Circuit board

Device is powered on. A power cycle is needed...

Powering down the device...

Applying power and watching spin-up currents...

Current oscillogram (12V):

Current oscillogram (5V):

Device has become ready in 3 sec

Registers. Status: 01010000 Error: 00000001

Peak power consumption during spin-up: 5V line = 322.30 mA; 12V line = 0.00 mA

Integrity word of device identification data is OK.

Device identified: Samsung SSD 860 PRO 256GB SN: S418NF0KB07067E

Logical sector size: 512 bytes. Physical sector size: 512 bytes

Circuit board check passed

Elapsed: 12.3 sec.

2. Heads

Solid state drives (SSD) don't have heads.

Elapsed: 0.0 sec.

3. Media surface

Media scan is in progress...

Verifying starting sectors (LBA: 0 - 999,999)

0 error(s) found

Speed: 542 MB/s

Verifying middle sectors (LBA: 250,059,095 - 251,059,094)

0 error(s) found

Speed: 541 MB/s

Verifying ending sectors (LBA: 499,118,192 - 500,118,191)

0 error(s) found

Speed: 542 MB/s

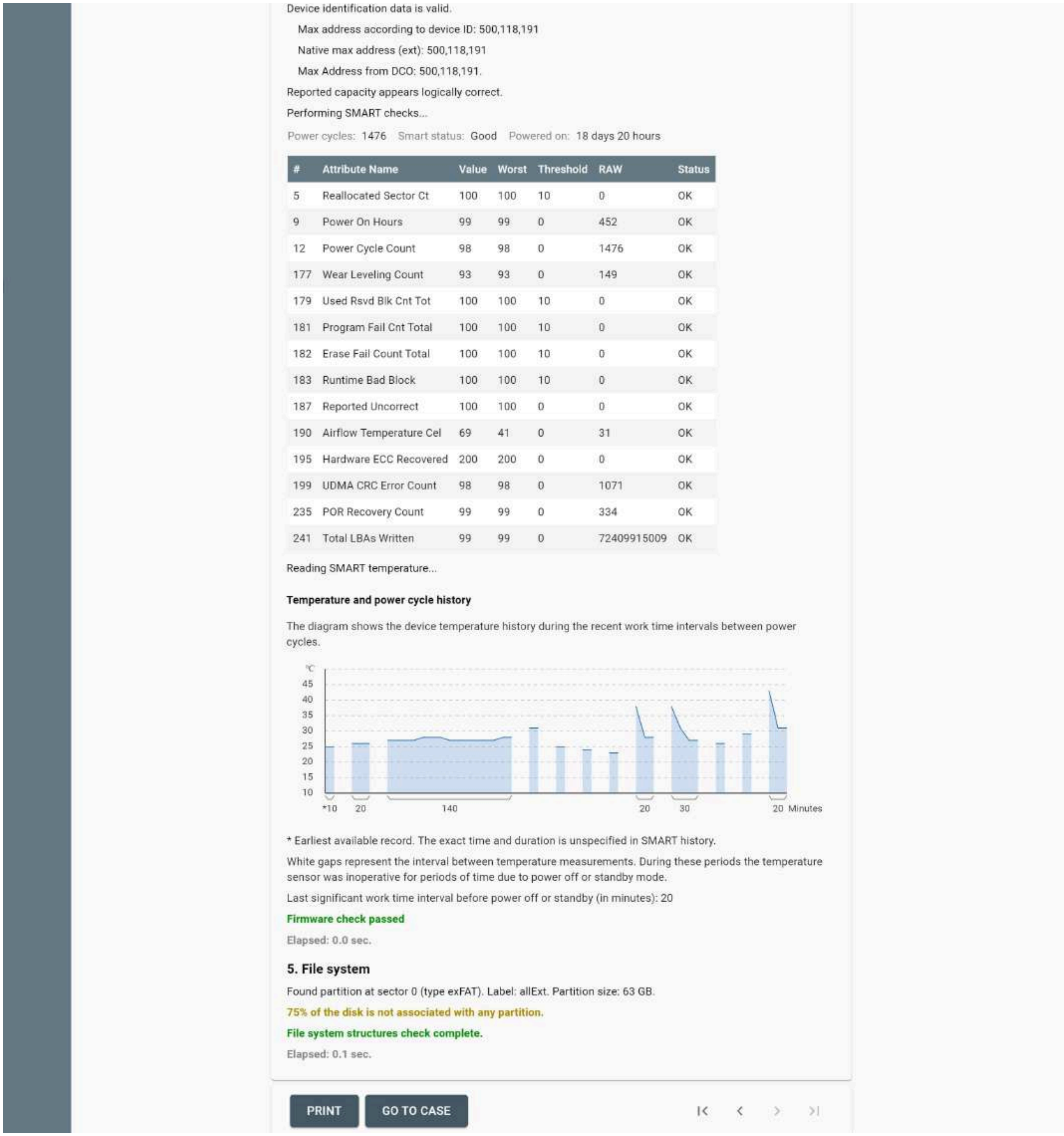
Average speed: 541 MB/s

Media surface check passed

Elapsed: 2.9 sec.

4. Firmware

Device is not locked.



Device identification data is valid.

Max address according to device ID: 500,118,191

Native max address (ext): 500,118,191

Max Address from DCO: 500,118,191.

Reported capacity appears logically correct.

Performing SMART checks...

Power cycles: 1476 Smart status: Good Powered on: 18 days 20 hours

#	Attribute Name	Value	Worst	Threshold	RAW	Status
5	Reallocated Sector Ct	100	100	10	0	OK
9	Power On Hours	99	99	0	452	OK
12	Power Cycle Count	98	98	0	1476	OK
177	Wear Leveling Count	93	93	0	149	OK
179	Used Rsvd Blk Cnt Tot	100	100	10	0	OK
181	Program Fail Cnt Total	100	100	10	0	OK
182	Erase Fail Count Total	100	100	10	0	OK
183	Runtime Bad Block	100	100	10	0	OK
187	Reported Uncorrect	100	100	0	0	OK
190	Airflow Temperature Cel	69	41	0	31	OK
195	Hardware ECC Recovered	200	200	0	0	OK
199	UDMA CRC Error Count	98	98	0	1071	OK
235	POR Recovery Count	99	99	0	334	OK
241	Total LBAs Written	99	99	0	72409915009	OK

Reading SMART temperature...

Temperature and power cycle history

The diagram shows the device temperature history during the recent work time intervals between power cycles.

* Earliest available record. The exact time and duration is unspecified in SMART history.

White gaps represent the interval between temperature measurements. During these periods the temperature sensor was inoperative for periods of time due to power off or standby mode.

Last significant work time interval before power off or standby (in minutes): 20

Firmware check passed

Elapsed: 0.0 sec.

5. File system

Found partition at sector 0 (type exFAT). Label: allExt. Partition size: 63 GB.

75% of the disk is not associated with any partition.

File system structures check complete.

Elapsed: 0.1 sec.

Diagnostics report in Atola TaskForce 2.

Add a case

When you identify a device in Atola TaskForce 2 for the first time, the system automatically creates a new case for that device and records every single operation performed with the device or with the case itself. To know more about how it works, see Case management system and report types.

Until you specify case details, **Case ID** shows in the TaskForce interface as *Not assigned*.

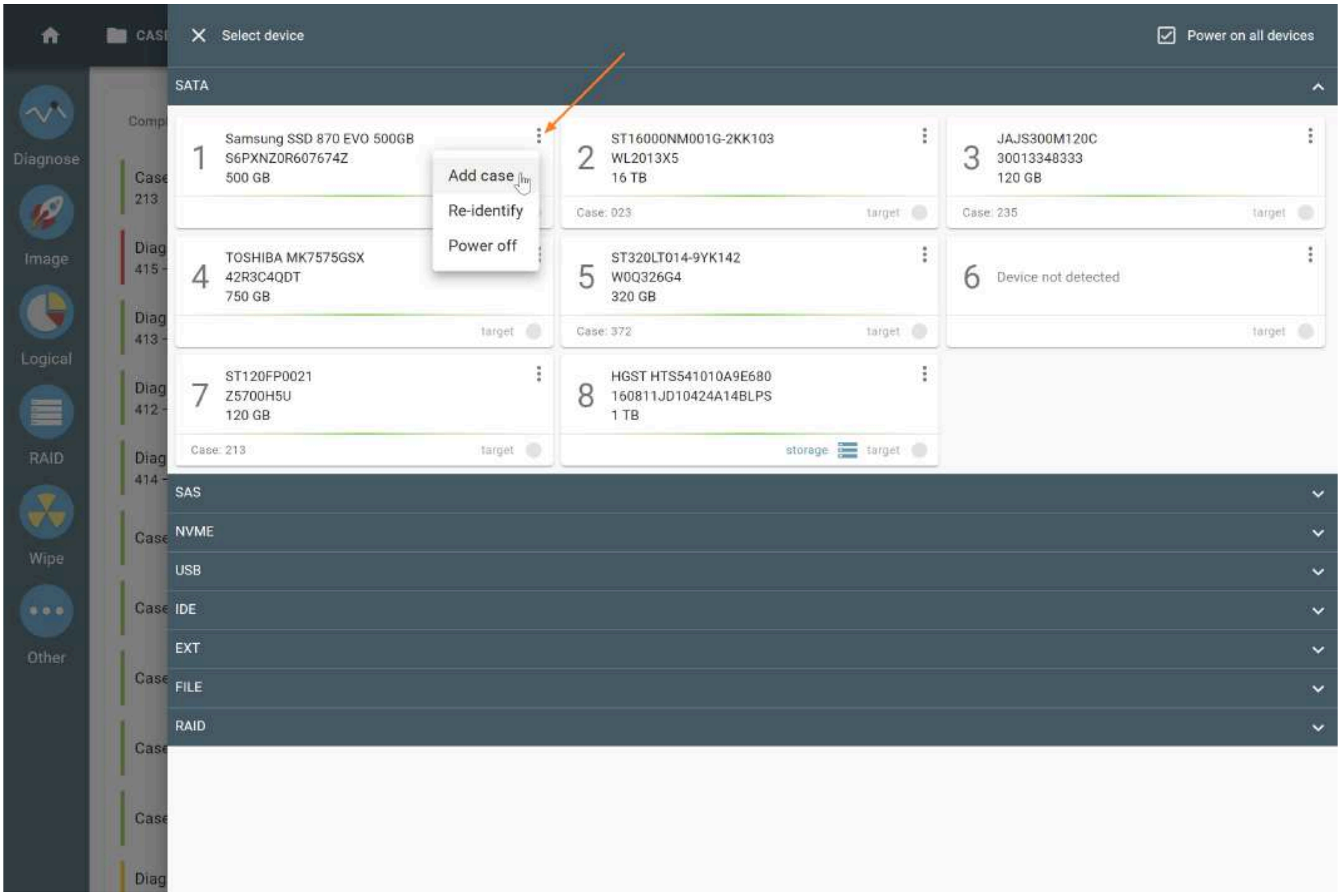
To distinguish and search your cases by a case number, investigator’s name, and case description, you can add a case and enter these case details. Also, you can set TaskForce 2 to remind you to enter case details before starting any task.

There are several ways to create a new case in TaskForce 2:

- From the **Devices** menu.
- From the **Cases** page.
- From the **Device** page.

Add a case from the Devices menu

1. Connect a device to TaskForce 2.
2. In the TaskForce main window, click **Devices**.
3. In the **Select device** panel, in the port with your device, click **More** icon, and then select **Add case**.



1 Samsung SSD 870 EVO 500GB S6PXNZ0R607674Z 500 GB

2 ST16000NM001G-2KK103 WL2013X5 16 TB — Case: 023 — target

3 JAJS300M120C 30013348333 120 GB — Case: 235 — target

4 TOSHIBA MK7575GSX 42R3C4QDT 750 GB — target

5 ST320LT014-9YK142 W0Q326G4 320 GB — Case: 372 — target

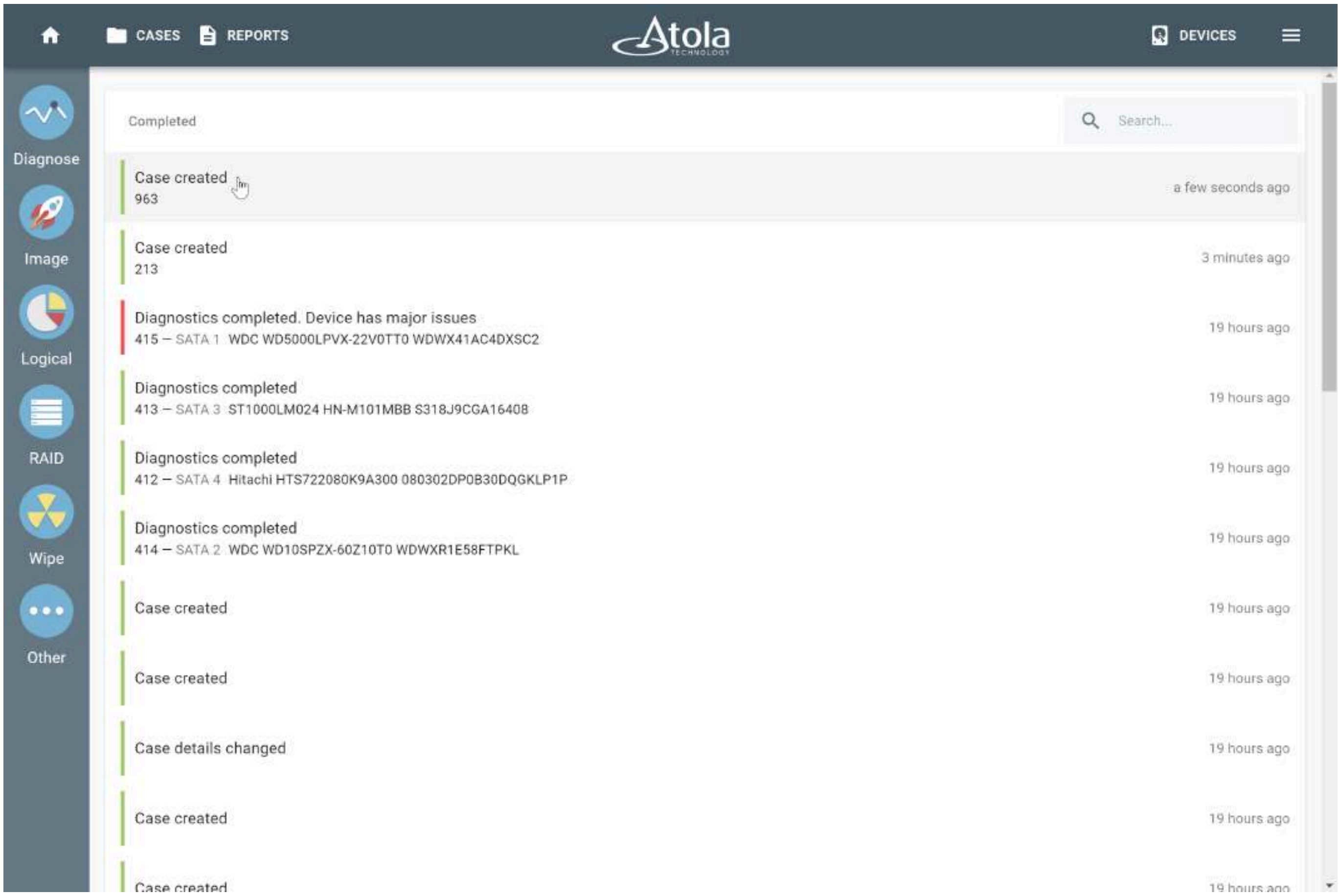
6 Device not detected — target

7 ST120FP0021 Z5700H5U 120 GB — Case: 213 — target

8 HGST HTS541010A9E680 160811JD10424A14BLPS 1 TB — storage — target

Adding a device to a new case from the Devices menu.

4. Enter case details and click **Continue**. TaskForce 2 creates a new case and adds your device to it. The **Case created** report appears on the Home screen and on the **Reports** page.



Completed

Case created
963
a few seconds ago

Case created
213
3 minutes ago

Diagnostics completed. Device has major issues
415 – SATA 1 WDC WD5000LPVX-22V0TT0 WDWX41AC4DXSC2
19 hours ago

Diagnostics completed
413 – SATA 3 ST1000LM024 HN-M101MBB S318J9CGA16408
19 hours ago

Diagnostics completed
412 – SATA 4 Hitachi HTS722080K9A300 080302DP0B30DQGKLP1P
19 hours ago

Diagnostics completed
414 – SATA 2 WDC WD10SPZX-60Z10T0 WDWXR1E58FTPKL
19 hours ago

Case created
19 hours ago

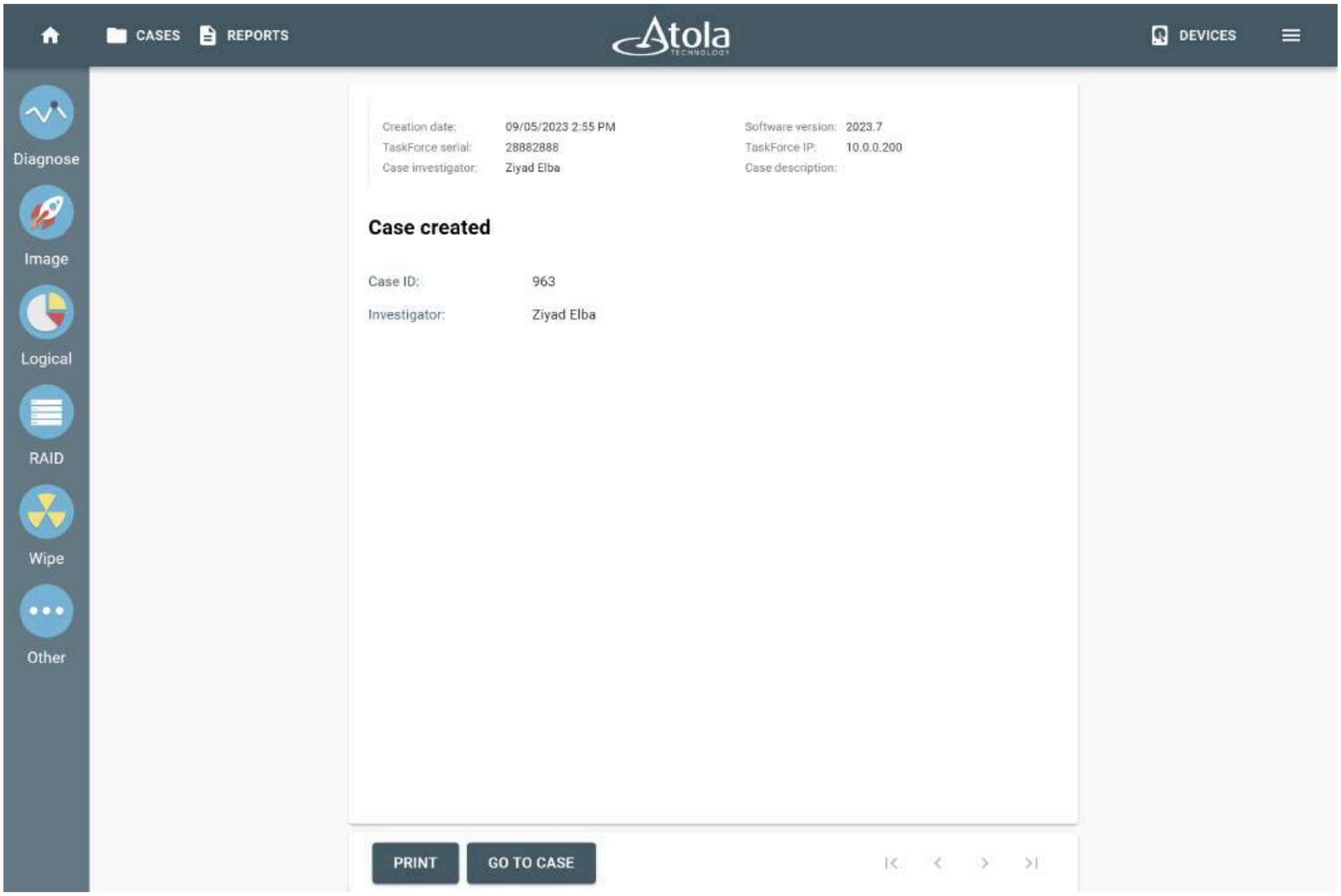
Case created
19 hours ago

Case details changed
19 hours ago

Case created
19 hours ago

Case created
19 hours ago

The Case created report on the Home screen.



Creation date: 09/05/2023 2:55 PM
TaskForce serial: 28882888
Case investigator: Ziyad Elba
Software version: 2023.7
TaskForce IP: 10.0.0.200
Case description:

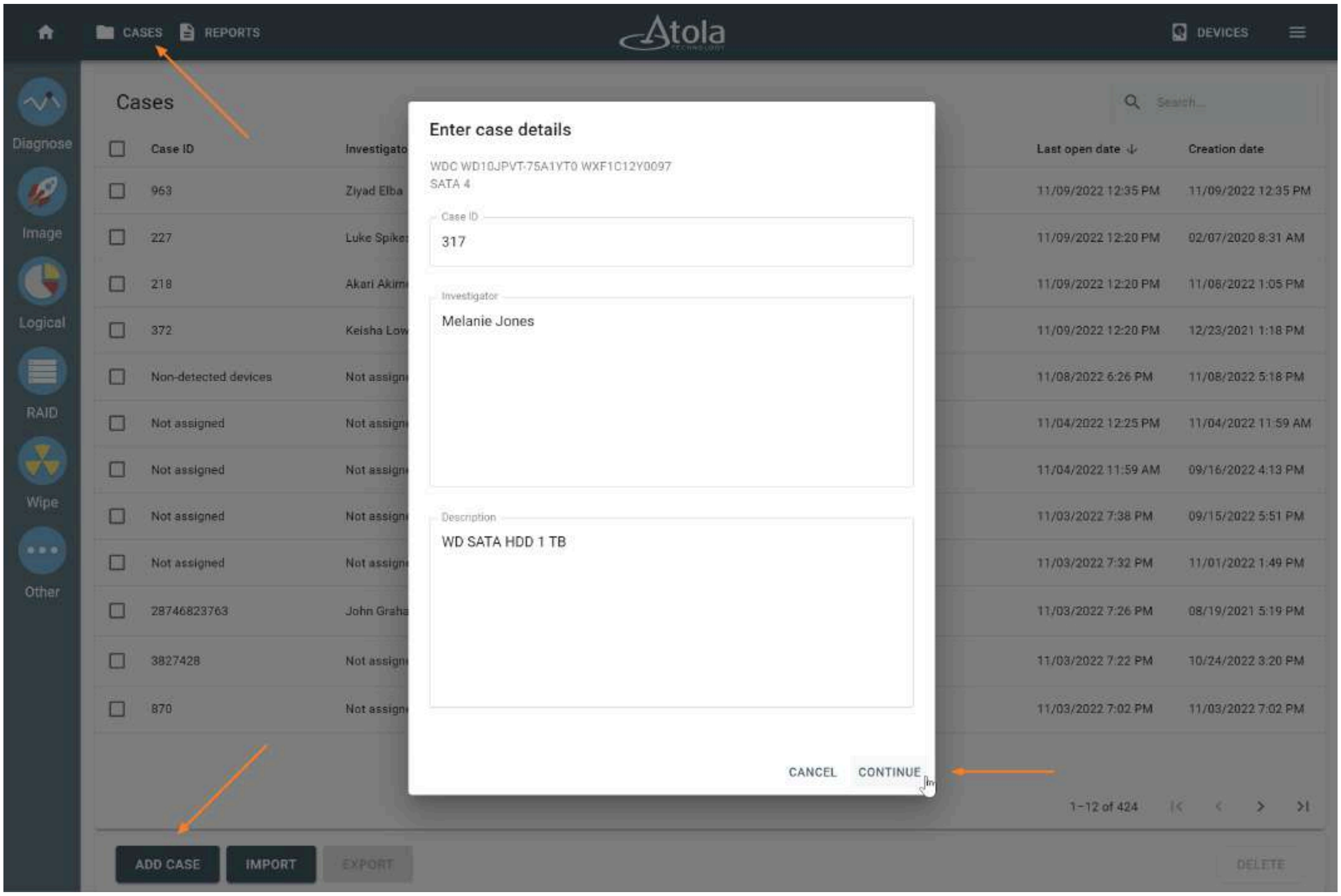
Case created

Case ID: 963
Investigator: Ziyad Elba

Case created report details.

Add a case from the Cases page

1. Connect a device to TaskForce 2.
2. In the TaskForce main window, click **Cases**.
3. On the **Cases** page, click **Add case**.
4. In the **Select device** panel, click on your device.
5. Enter case details and click **Continue**. TaskForce 2 creates a new case and adds your device to it. The **Case created** report appears on the Home screen and on the **Reports** page.



Cases

	Case ID	Investigato	Last open date ↓	Creation date
□	963	Ziyad Elba	11/09/2022 12:35 PM	11/09/2022 12:35 PM
□	227	Luke Spike	11/09/2022 12:20 PM	02/07/2020 8:31 AM
□	218	Akari Akim	11/09/2022 12:20 PM	11/08/2022 1:05 PM
□	372	Keisha Low	11/09/2022 12:20 PM	12/23/2021 1:18 PM
□	Non-detected devices	Not assign	11/08/2022 6:26 PM	11/08/2022 5:18 PM
□	Not assigned	Not assign	11/04/2022 12:25 PM	11/04/2022 11:59 AM
□	Not assigned	Not assign	11/04/2022 11:59 AM	09/16/2022 4:13 PM
□	Not assigned	Not assign	11/03/2022 7:38 PM	09/15/2022 5:51 PM
□	Not assigned	Not assign	11/03/2022 7:32 PM	11/01/2022 1:49 PM
□	28746823763	John Graha	11/03/2022 7:26 PM	08/19/2021 5:19 PM
□	3827428	Not assign	11/03/2022 7:22 PM	10/24/2022 3:20 PM
□	870	Not assign	11/03/2022 7:02 PM	11/03/2022 7:02 PM

Enter case details

WDC WD10JPVT-75A1YT0 WXF1C12Y0097
SATA 4

Case ID: 317

Investigator: Melanie Jones

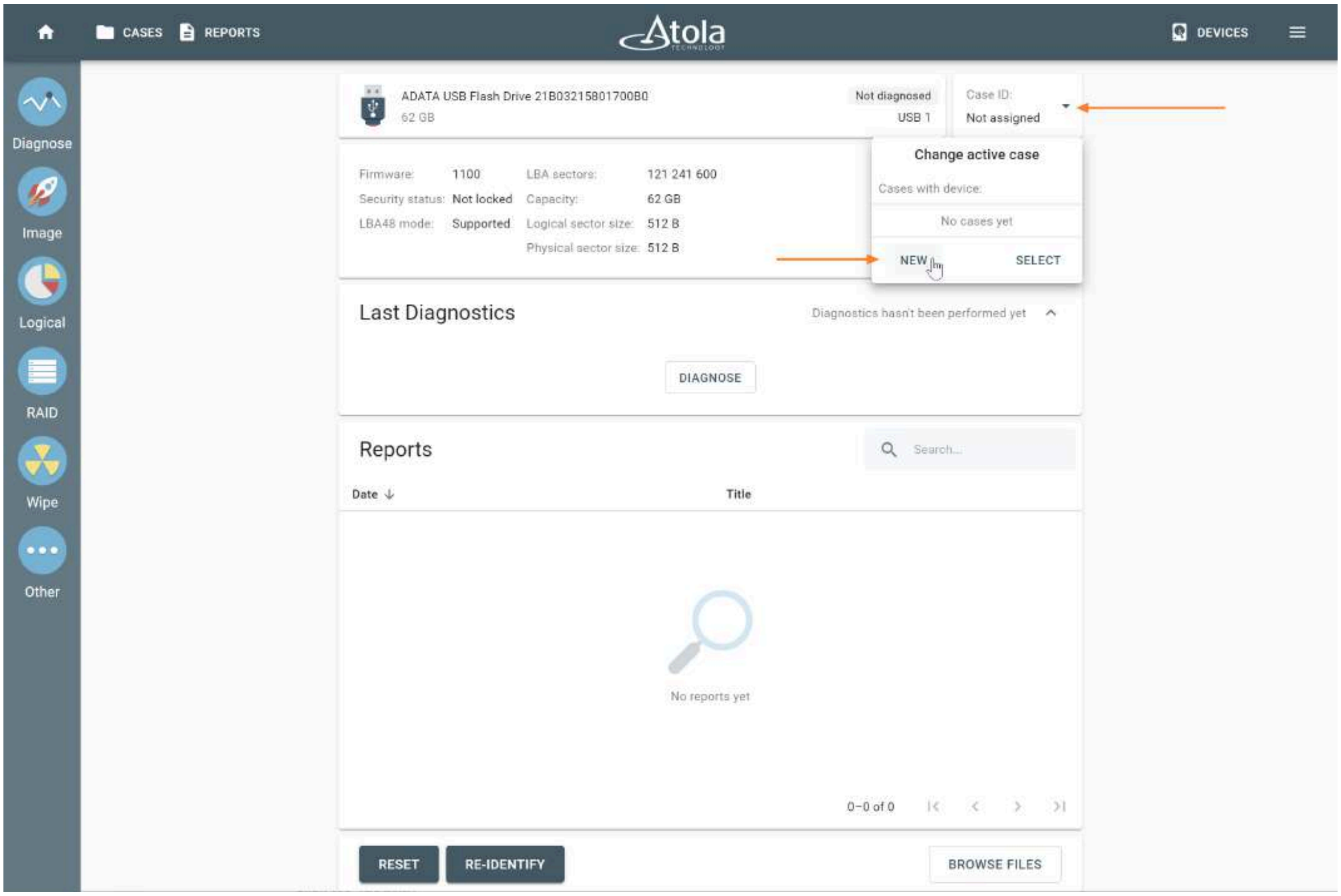
Description: WD SATA HDD 1 TB

CANCEL CONTINUE

The Enter case details dialog.

Add a case from the Device page

1. Connect a device to TaskForce 2.
2. In the TaskForce main window, click **Devices**.
3. In the **Select device** panel, click on the port with your device. TaskForce 2 takes you to the **Device** page.
4. **Optional:** If TaskForce 2 hasn't identified your device yet, then, on the **Device** page, click **Re-identify**.
5. In **Case ID** pane, open the drop-down menu, and then click **New**.



ADATA USB Flash Drive 21B03215801700B0
62 GB
Not diagnosed
USB 1
Case ID:
Not assigned

Firmware: 1100
Security status: Not locked
LBA48 mode: Supported
LBA sectors: 121 241 600
Capacity: 62 GB
Logical sector size: 512 B
Physical sector size: 512 B

Change active case menu is opened on the Device page.

6. Enter case details and click **Continue**. TaskForce 2 creates a new case and adds your device to it. The **Case created** report appears on the Home screen and on the **Reports** page.

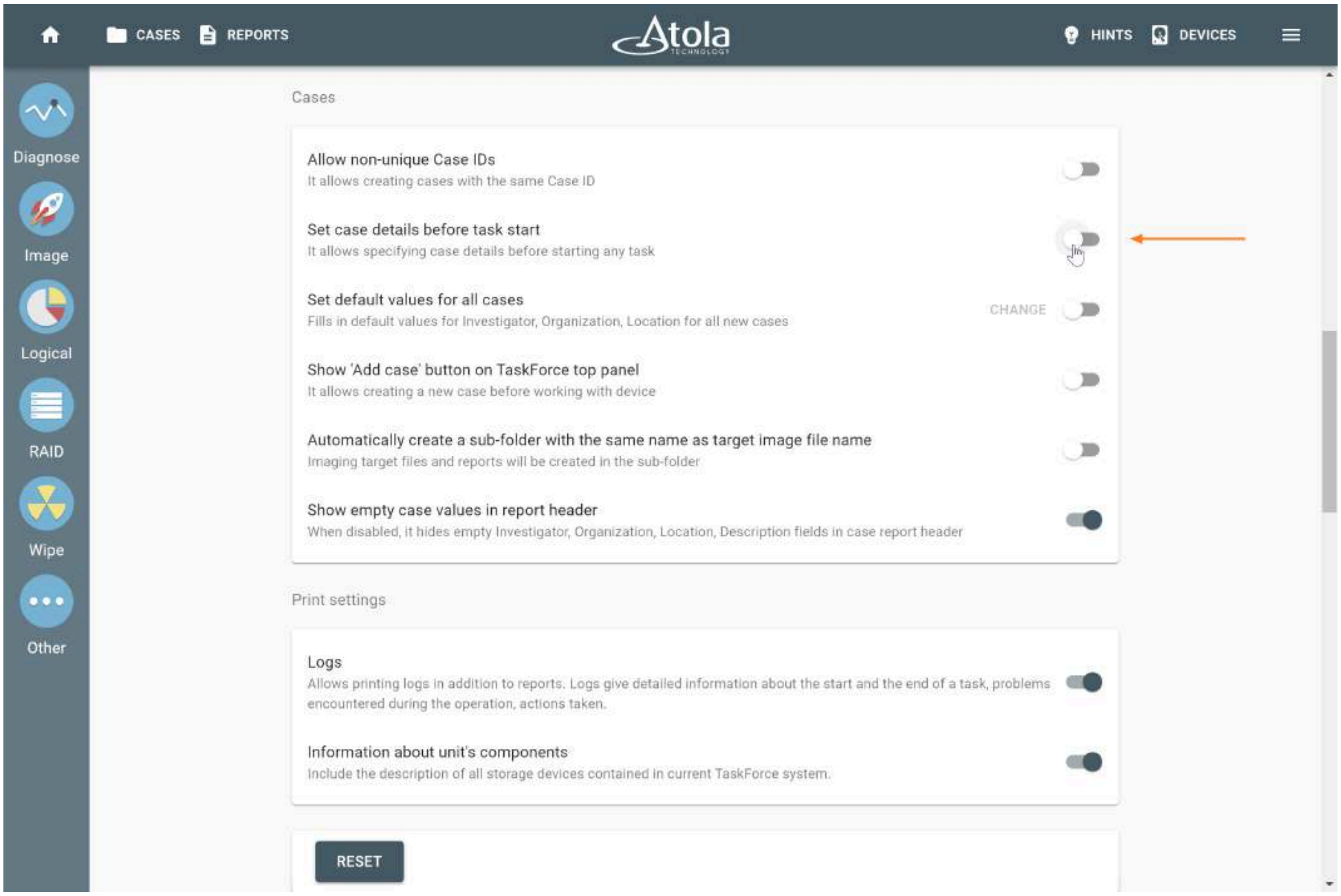
Enter case details before starting any task

Entering case details before performing any operation with a device helps you to keep your cases organized and searchable. TaskForce 2 can be set to request that you enter case details before starting any task.

To enable this feature, do the following:

1. In the TaskForce main window, go to the **Menu** > **Settings**.
2. In the **Cases** section, toggle **Set case details before task start**.

Now, TaskForce 2 will ask you to enter case details before performing any operation with a device.



Cases

Allow non-unique Case IDs
It allows creating cases with the same Case ID

Set case details before task start
It allows specifying case details before starting any task

Set default values for all cases
Fills in default values for Investigator, Organization, Location for all new cases

Show 'Add case' button on TaskForce top panel
It allows creating a new case before working with device

Automatically create a sub-folder with the same name as target image file name
Imaging target files and reports will be created in the sub-folder

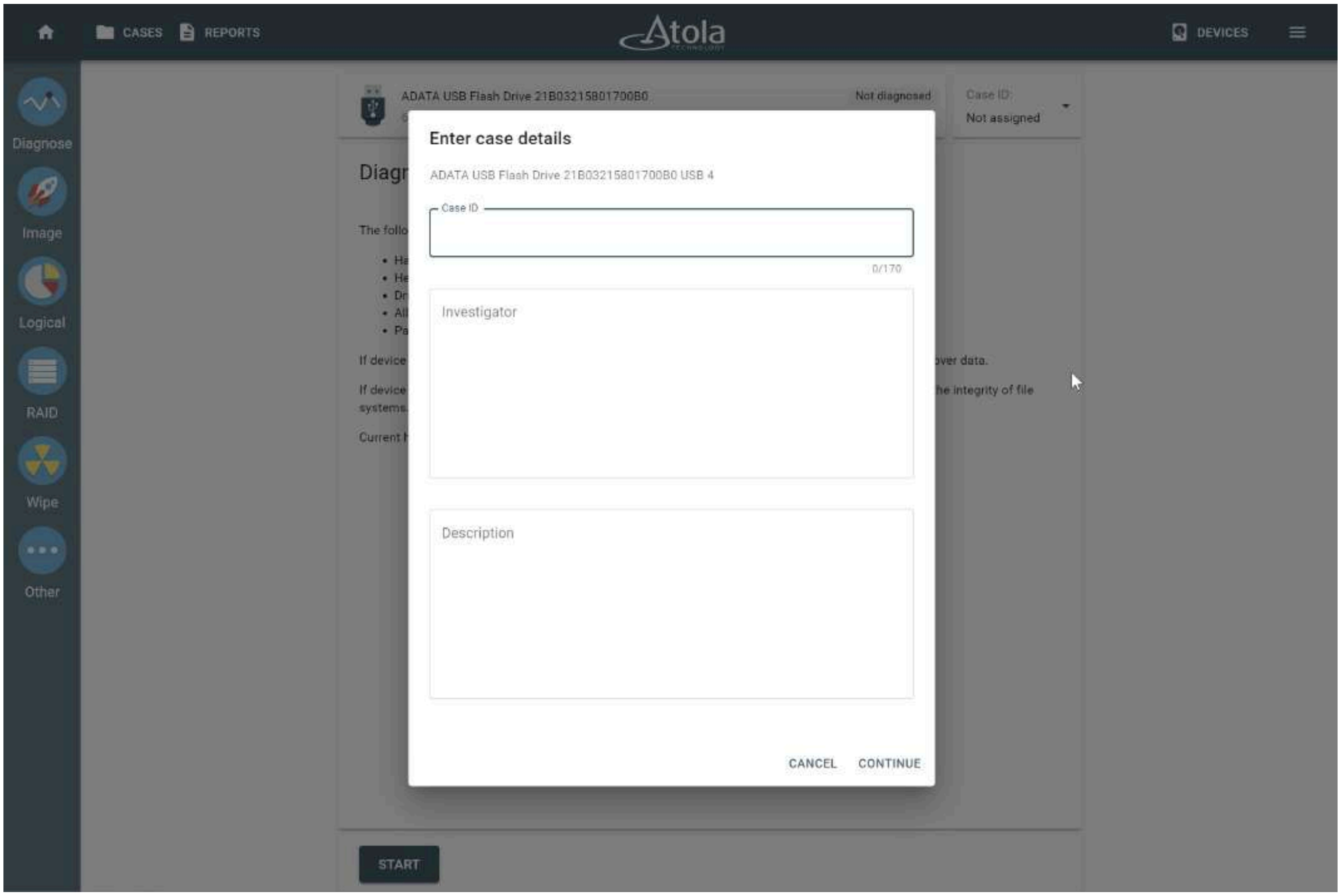
Show empty case values in report header
When disabled, it hides empty Investigator, Organization, Location, Description fields in case report header

Print settings

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

Information about unit's components
Include the description of all storage devices contained in current TaskForce system.

The Set case details before task start toggle on the Settings page.

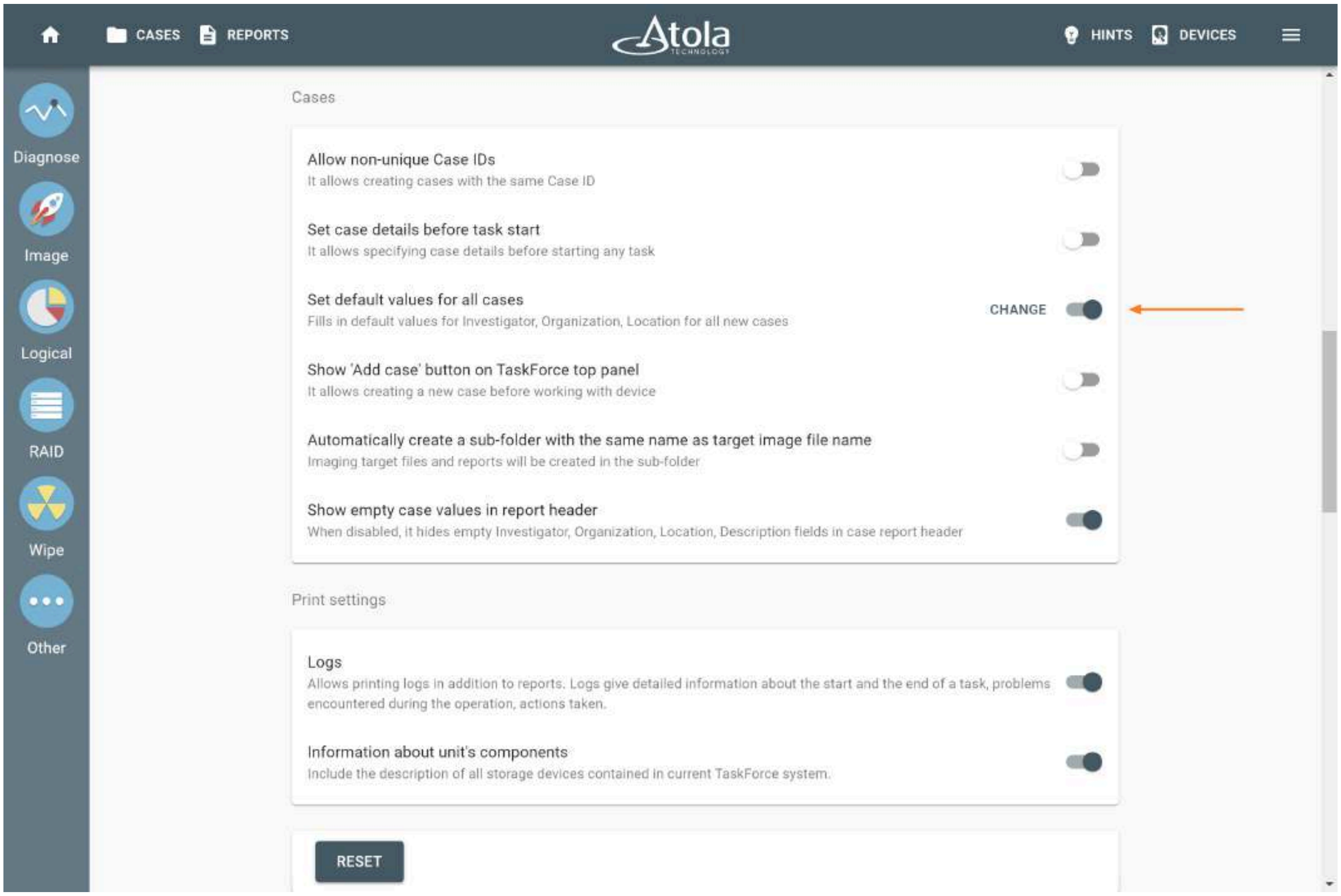


Atola TaskForce 2 asks a user to enter case details before starting diagnostics.

Set default values for all cases

If *Investigator*, *Organization*, or *Location* are the same for all or majority of your cases, set them as default for all new cases, and TaskForce will fill those fields automatically every time you create a new case:

1. At the top right, go to **Menu** > **Settings**.
2. On the Settings page, scroll down to the **Cases** section.
3. Toggle on **Set default values for all cases**.



Cases

Allow non-unique Case IDs
It allows creating cases with the same Case ID

Set case details before task start
It allows specifying case details before starting any task

Set default values for all cases
Fills in default values for Investigator, Organization, Location for all new cases
CHANGE

Show 'Add case' button on TaskForce top panel
It allows creating a new case before working with device

Automatically create a sub-folder with the same name as target image file name
Imaging target files and reports will be created in the sub-folder

Show empty case values in report header
When disabled, it hides empty Investigator, Organization, Location, Description fields in case report header

Print settings

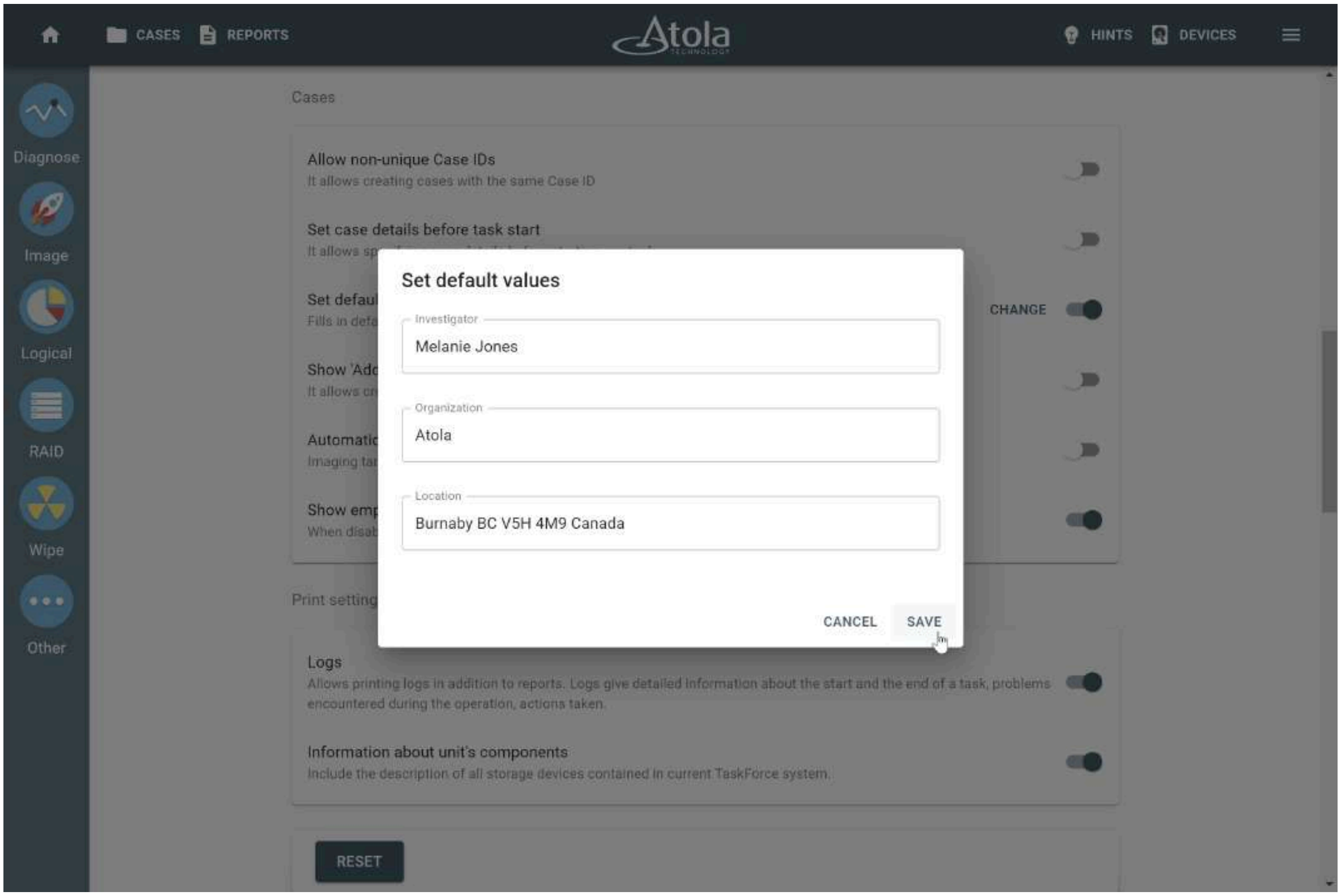
Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

Information about unit's components
Include the description of all storage devices contained in current TaskForce system.

RESET

The 'Set default values for all cases' toggle on the Settings page.

4. Next to the toggle, click **Change**.
5. Fill in the default values for *Investigator*, *Organization*, or *Location* and click **Save**.



Cases

Allow non-unique Case IDs
It allows creating cases with the same Case ID

Set case details before task start
It allows sp

Set defaul
Fills in defa

Show 'Add
It allows cr

Automatic
Imaging ta

Show emp
When disab

Set default values

Investigator: Melanie Jones

Organization: Atola

Location: Burnaby BC V5H 4M9 Canada

Print setting

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

Information about unit's components
Include the description of all storage devices contained in current TaskForce system.

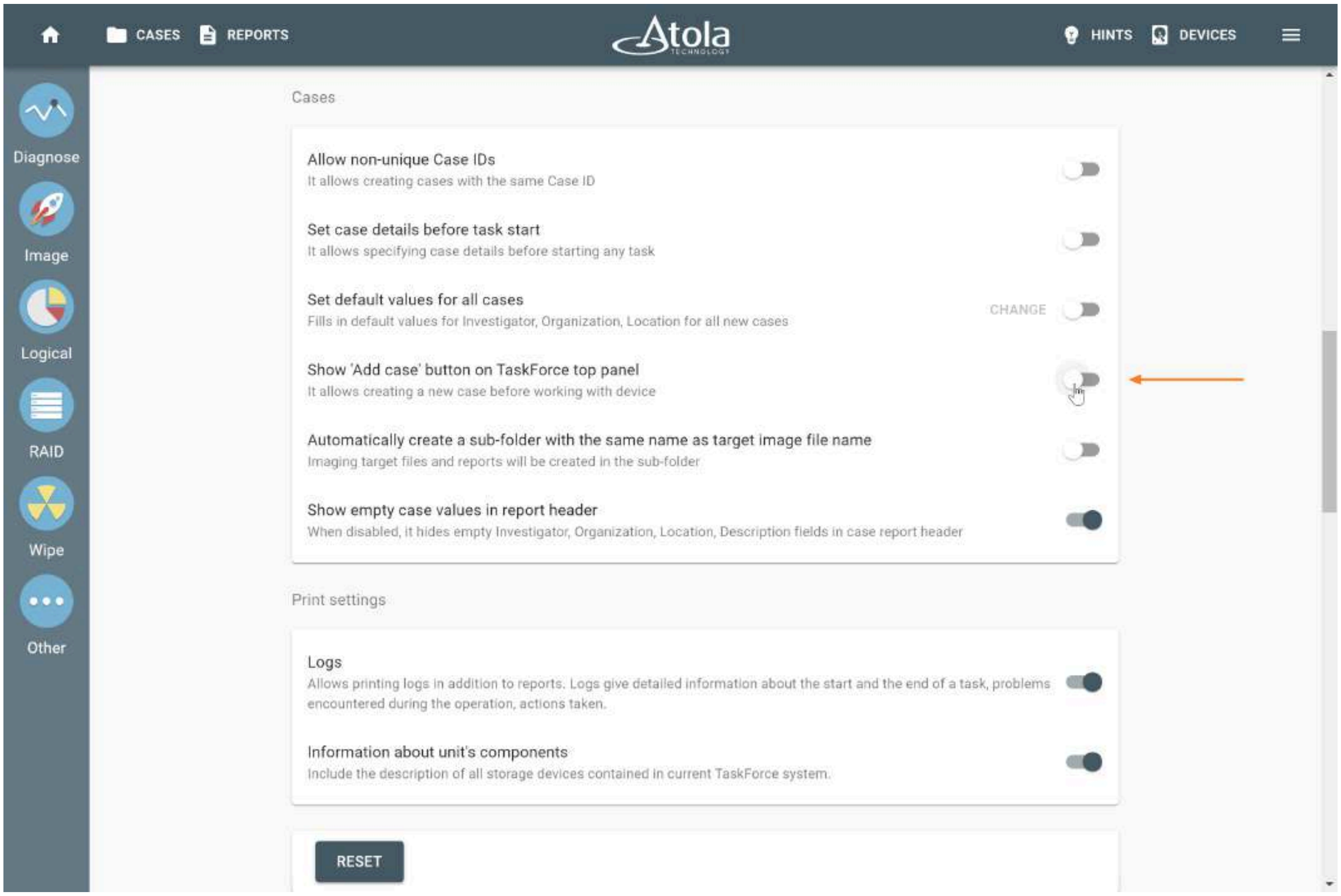
The 'Set default values' dialog.

Show 'Add case' button

You can add cases right from the TaskForce Home screen before working with the device. To do that, set TaskForce 2 to show **Add case** button in the top panel:

1. In the TaskForce main window, go to the **Menu** > **Settings**.
2. In the **Cases** section, toggle **Show 'Add case' button on TaskForce top panel**.

Now, TaskForce 2 shows the **Add case** button in the top panel.



Cases

Allow non-unique Case IDs
It allows creating cases with the same Case ID

Set case details before task start
It allows specifying case details before starting any task

Set default values for all cases
Fills in default values for Investigator, Organization, Location for all new cases

CHANGE

Show 'Add case' button on TaskForce top panel
It allows creating a new case before working with device

Automatically create a sub-folder with the same name as target image file name
Imaging target files and reports will be created in the sub-folder

Show empty case values in report header
When disabled, it hides empty Investigator, Organization, Location, Description fields in case report header

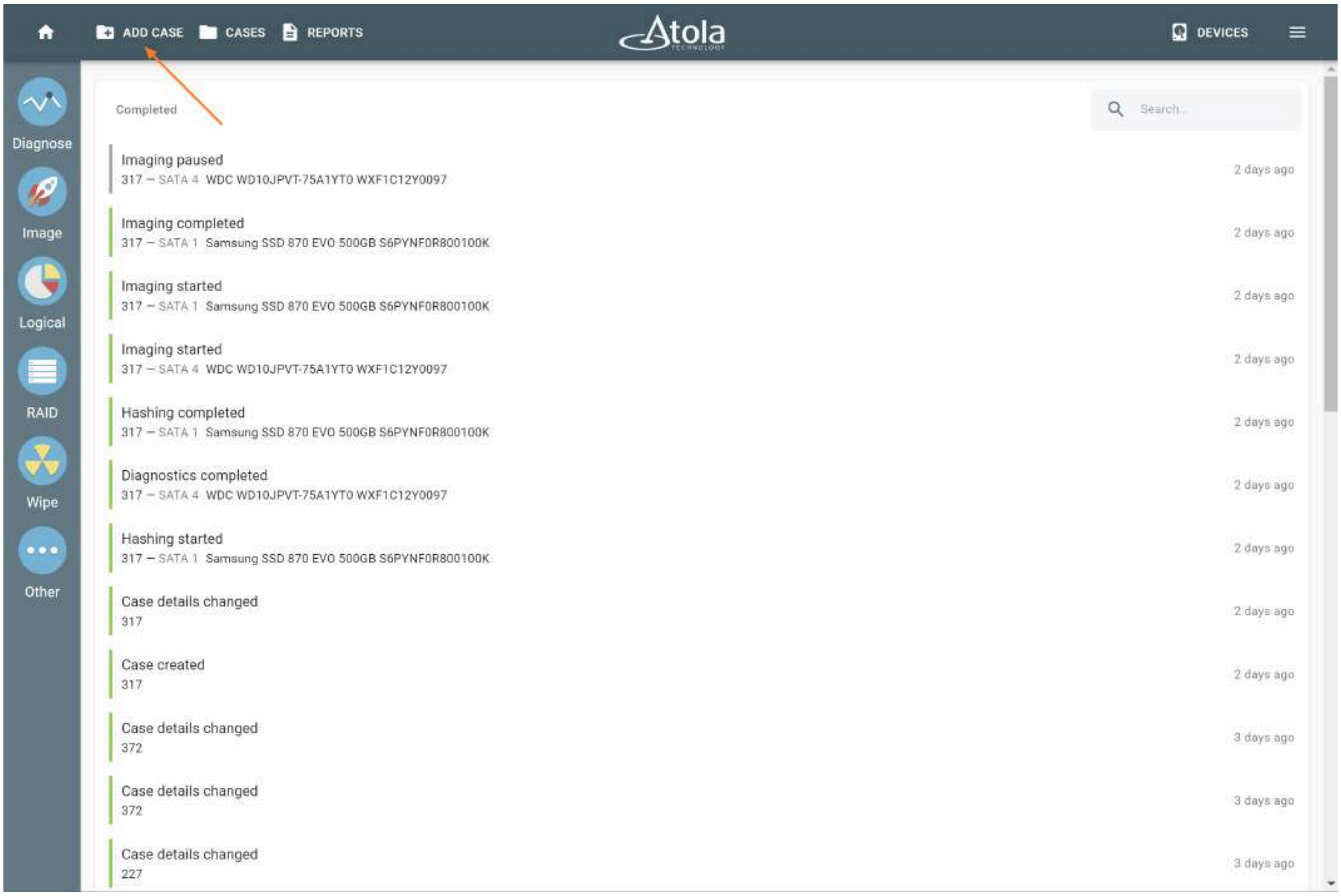
Print settings

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

Information about unit's components
Include the description of all storage devices contained in current TaskForce system.

RESET

The toggle in the Cases section on the Settings page.



Imaging paused
317 – SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097 2 days ago

Imaging completed
317 – SATA 1 Samsung SSD 870 EVO 500GB S6PYNF0R800100K 2 days ago

Imaging started
317 – SATA 1 Samsung SSD 870 EVO 500GB S6PYNF0R800100K 2 days ago

Imaging started
317 – SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097 2 days ago

Hashing completed
317 – SATA 1 Samsung SSD 870 EVO 500GB S6PYNF0R800100K 2 days ago

Diagnostics completed
317 – SATA 4 WDC WD10JPVT-75A1YT0 WXF1C12Y0097 2 days ago

Hashing started
317 – SATA 1 Samsung SSD 870 EVO 500GB S6PYNF0R800100K 2 days ago

Case details changed
317 2 days ago

Case created
317 2 days ago

Case details changed
372 3 days ago

Case details changed
372 3 days ago

Case details changed
227 3 days ago

The Add case button in the Atola TaskForce 2 main window.

Add one device to several cases

In Atola TaskForce, you can include the same device in several new or existing cases using the Case management system. When a device is added to more than one case, TaskForce keeps the tasks and reports, which are associated with each case, separate.

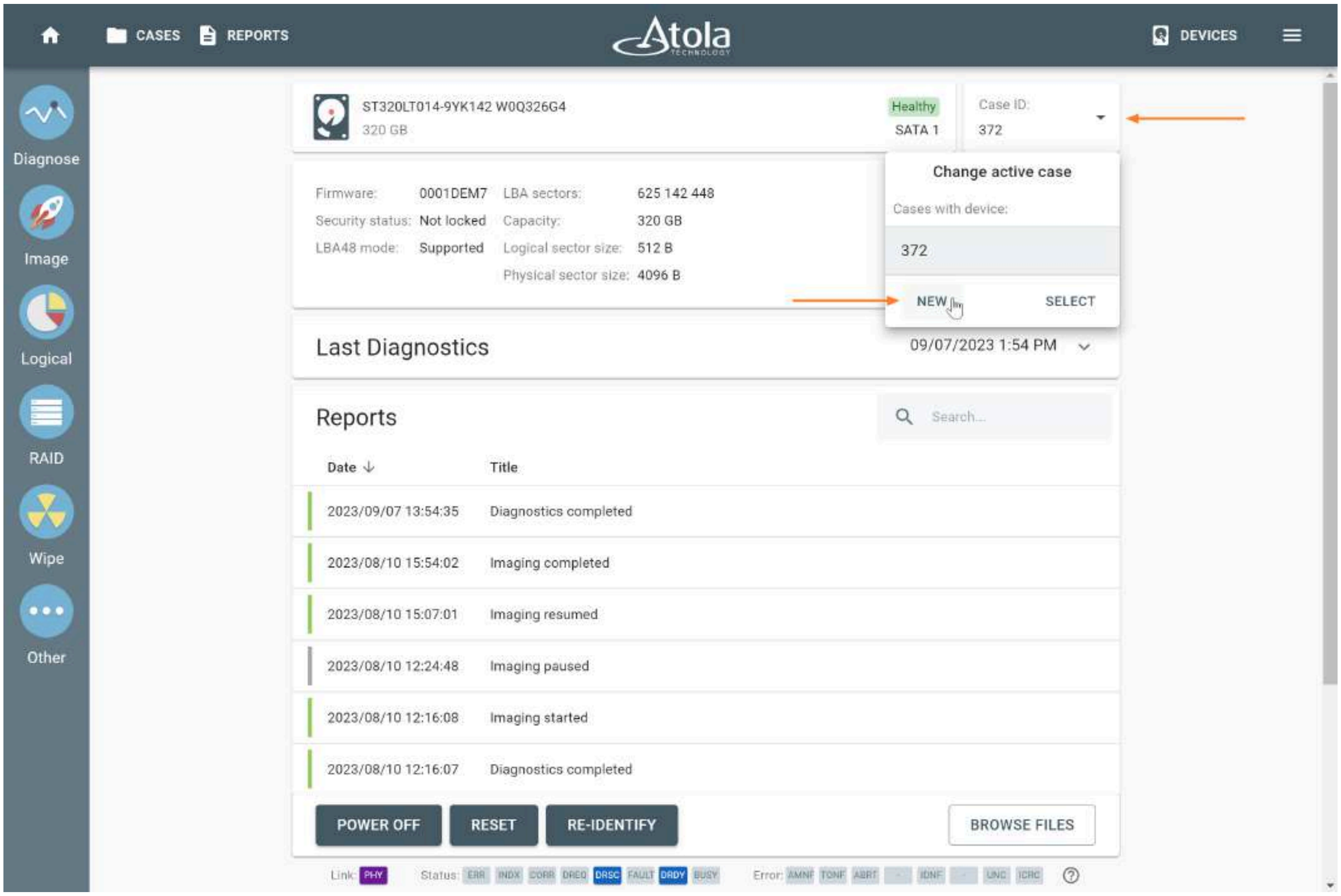
Add a device to another new case

To add your device to several new cases, do the following:

1. Connect a device to TaskForce and identify it.
2. Add first new case and include your device to it. For guidance, see Add a case.

After you have added your device to the first case, do the following steps:

3. In the TaskForce user interface, click **Devices**.
4. In the **Select device** window, click on the port with your device. TaskForce takes you to the **Device** page.
5. In **Case ID** pane, open the drop-down menu, and then click **New**.



ST320LT014-9YK142 W0Q326G4
320 GB
Healthy
SATA 1
Case ID: 372

Firmware:	0001DEM7	LBA sectors:	625 142 448
Security status:	Not locked	Capacity:	320 GB
LBA48 mode:	Supported	Logical sector size:	512 B
		Physical sector size:	4096 B

Cases with device:
372

Last Diagnostics 09/07/2023 1:54 PM

Reports

Date ↓	Title
2023/09/07 13:54:35	Diagnostics completed
2023/08/10 15:54:02	Imaging completed
2023/08/10 15:07:01	Imaging resumed
2023/08/10 12:24:48	Imaging paused
2023/08/10 12:16:08	Imaging started
2023/08/10 12:16:07	Diagnostics completed

The New button in the Change active case menu on the Device page.

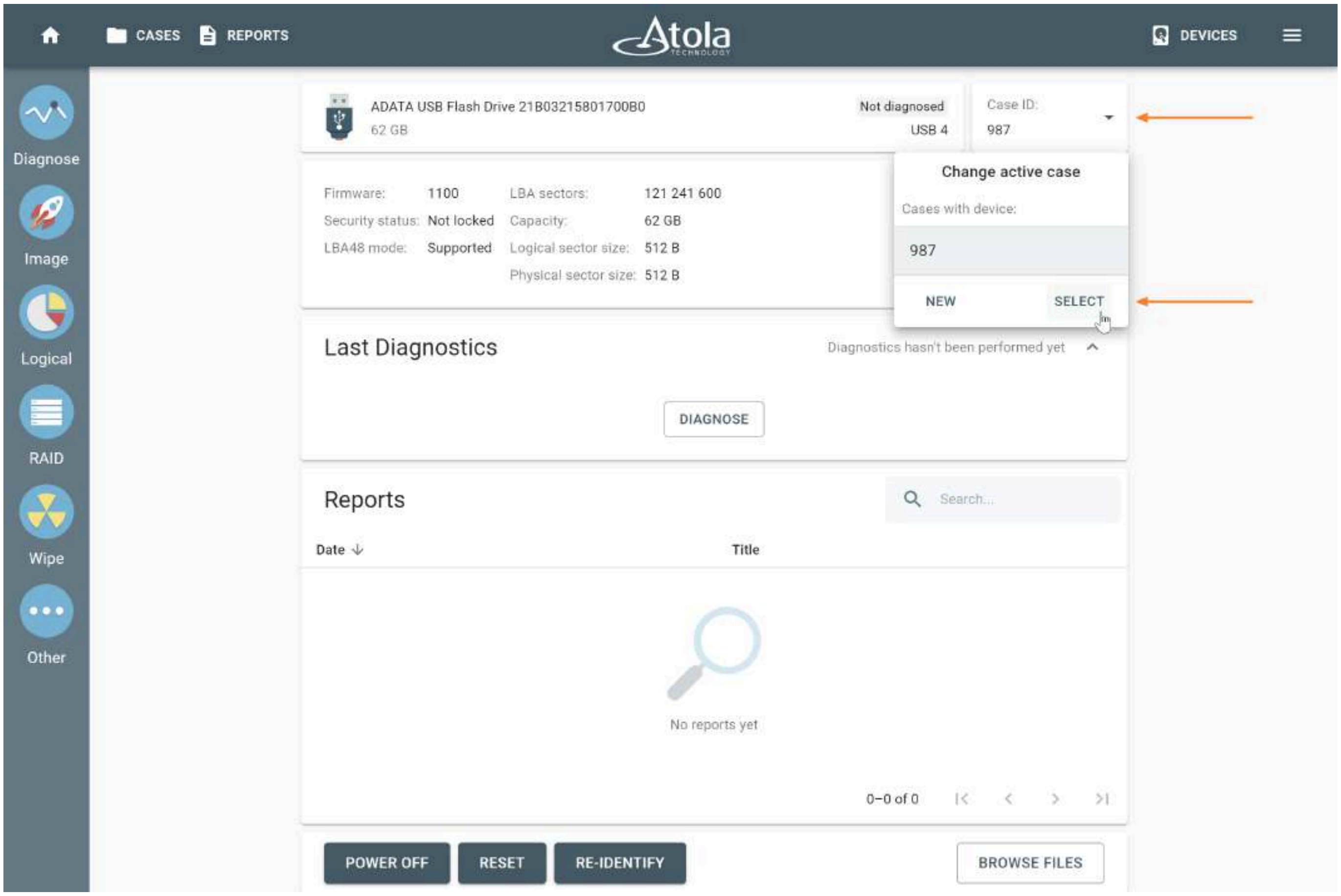
6. Enter case details and click **Continue**.

TaskForce creates another new case and adds your device to it. The **Case created** report appears on the Home screen and on the **Reports** page.

Add a device to another existing case

When you already added your device to one case and want to add that device to another existing case, do the following:

1. Connect a device to TaskForce.
2. In the TaskForce user interface, click **Devices**.
3. In the **Select device** window, click on the port with your device. TaskForce takes you to the **Device** page.
4. **Optional:** If TaskForce hasn't identified your device yet, then, on the **Device** page, click **Re-identify**.
5. In **Case ID** pane, open the drop-down menu, and then click **Select**.



ADATA USB Flash Drive 21B03215801700B0
62 GB

Not diagnosed
USB 4

Case ID: 987

Cases with device: 987

Firmware:	1100	LBA sectors:	121 241 600
Security status:	Not locked	Capacity:	62 GB
LBA48 mode:	Supported	Logical sector size:	512 B
		Physical sector size:	512 B

Last Diagnostics

Diagnostics hasn't been performed yet

Reports

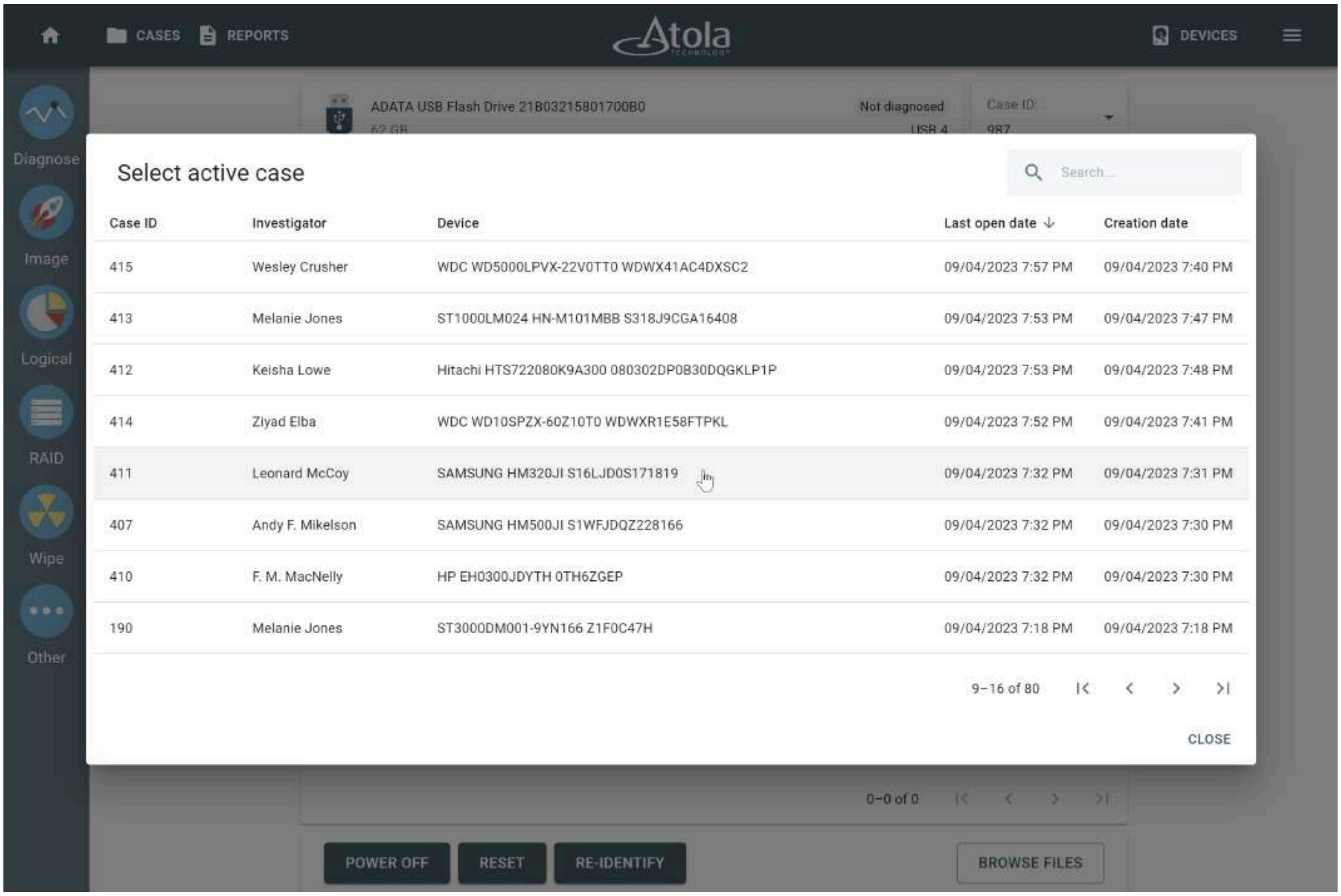
Date ↓	Title

No reports yet

0–0 of 0

The Select button in the Change active case drop-down menu on the Device page.

6. In the **Select active case** window, chose your existing case. If needed, use the **Search** field to find it. TaskForce adds your device to the selected case.



Select active case

Search...

Case ID	Investigator	Device	Last open date ↓	Creation date
415	Wesley Crusher	WDC WD5000LPVX-22V0TT0 WDWX41AC4DXSC2	09/04/2023 7:57 PM	09/04/2023 7:40 PM
413	Melanie Jones	ST1000LM024 HN-M101MBB S318J9CGA16408	09/04/2023 7:53 PM	09/04/2023 7:47 PM
412	Keisha Lowe	Hitachi HTS722080K9A300 080302DP0B30DQGKLP1P	09/04/2023 7:53 PM	09/04/2023 7:48 PM
414	Ziyad Elba	WDC WD10SPZX-60Z10T0 WDWXR1E58FTPKL	09/04/2023 7:52 PM	09/04/2023 7:41 PM
411	Leonard McCoy	SAMSUNG HM320JI S16LJD0S171819	09/04/2023 7:32 PM	09/04/2023 7:31 PM
407	Andy F. Mikelson	SAMSUNG HM500JI S1WFJDQZ228166	09/04/2023 7:32 PM	09/04/2023 7:30 PM
410	F. M. MacNelly	HP EH0300JDYTH 0TH6ZGEP	09/04/2023 7:32 PM	09/04/2023 7:30 PM
190	Melanie Jones	ST3000DM001-9YN166 Z1F0C47H	09/04/2023 7:18 PM	09/04/2023 7:18 PM

9–16 of 80 |< < > >|

CLOSE

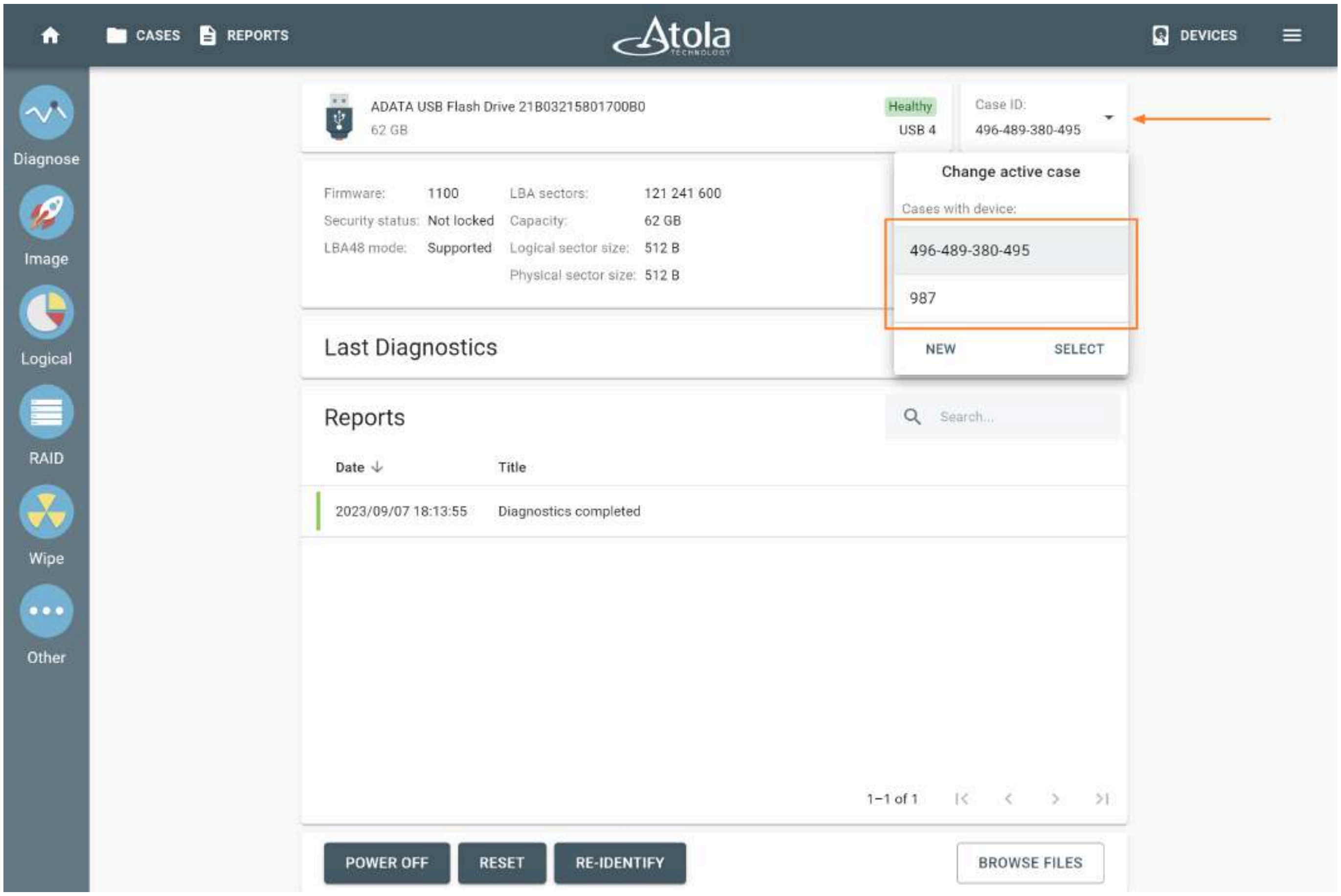
List of all your cases in the Select active case window.

Switch between cases on the Device page

When a device is added to more than one case, TaskForce keeps reports, which are associated with each case, separate.

To switch between cases on the **Device** page:

1. In **Case ID** pane, open the drop-down menu.
2. Click on the case you want to make active. TaskForce shows reports, associated with selected case.



ADATA USB Flash Drive 21B03215801700B0
62 GB
Healthy
USB 4
Case ID: 496-489-380-495

Cases with device:
496-489-380-495
987

Firmware: 1100
Security status: Not locked
LBA48 mode: Supported
LBA sectors: 121 241 600
Capacity: 62 GB
Logical sector size: 512 B
Physical sector size: 512 B

Last Diagnostics

Reports

Date ↓	Title
2023/09/07 18:13:55	Diagnostics completed

1–1 of 1

List of all cases associated with the device in the Case ID pane.

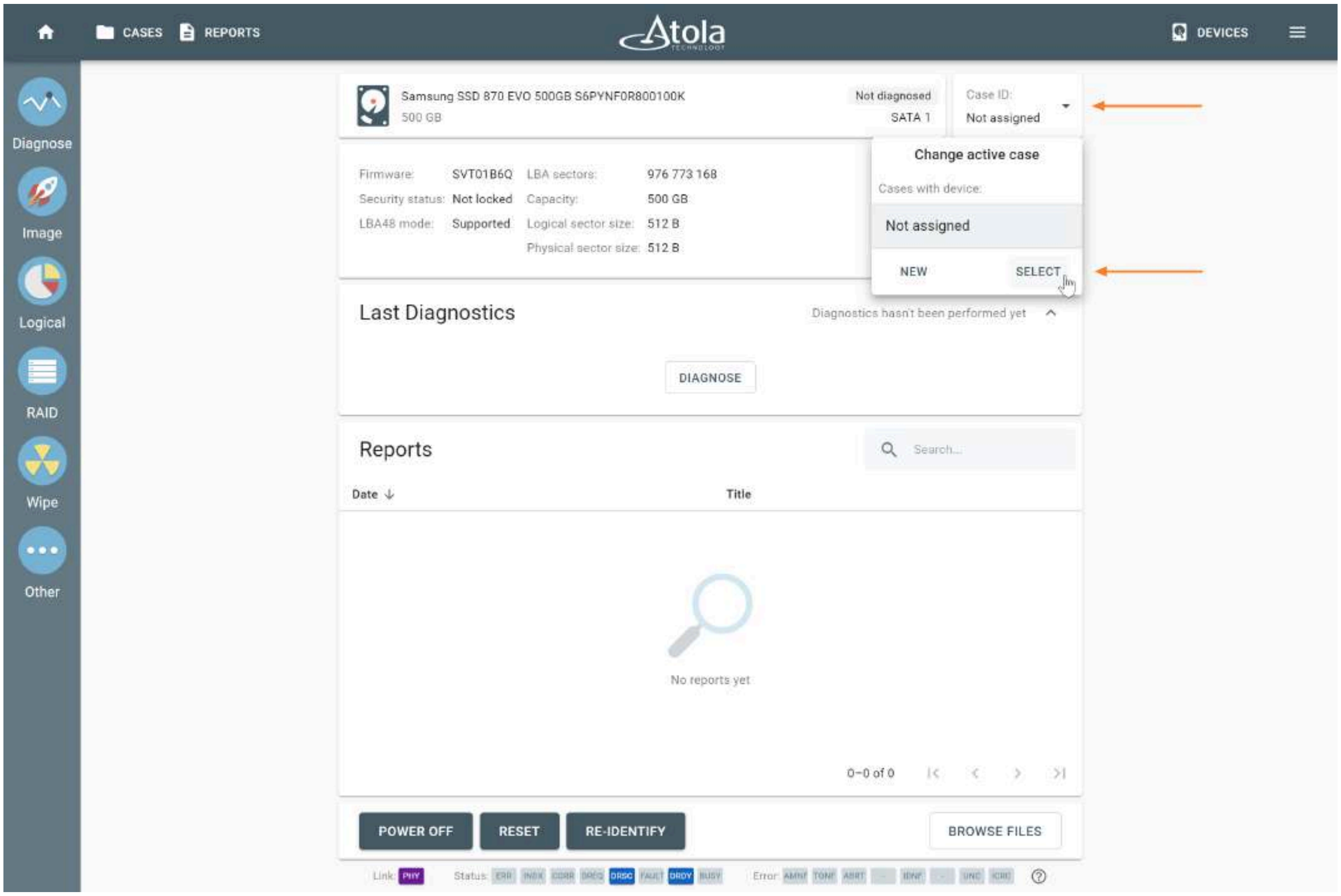
Add several devices to one case

In Atola TaskForce 2, you can have a forensic case that contains more than one device. TaskForce 2 lets you add several devices either to a new or an existing forensic case.

To add several devices to a new case, you need to create a case first. For guidance, see Add a case.

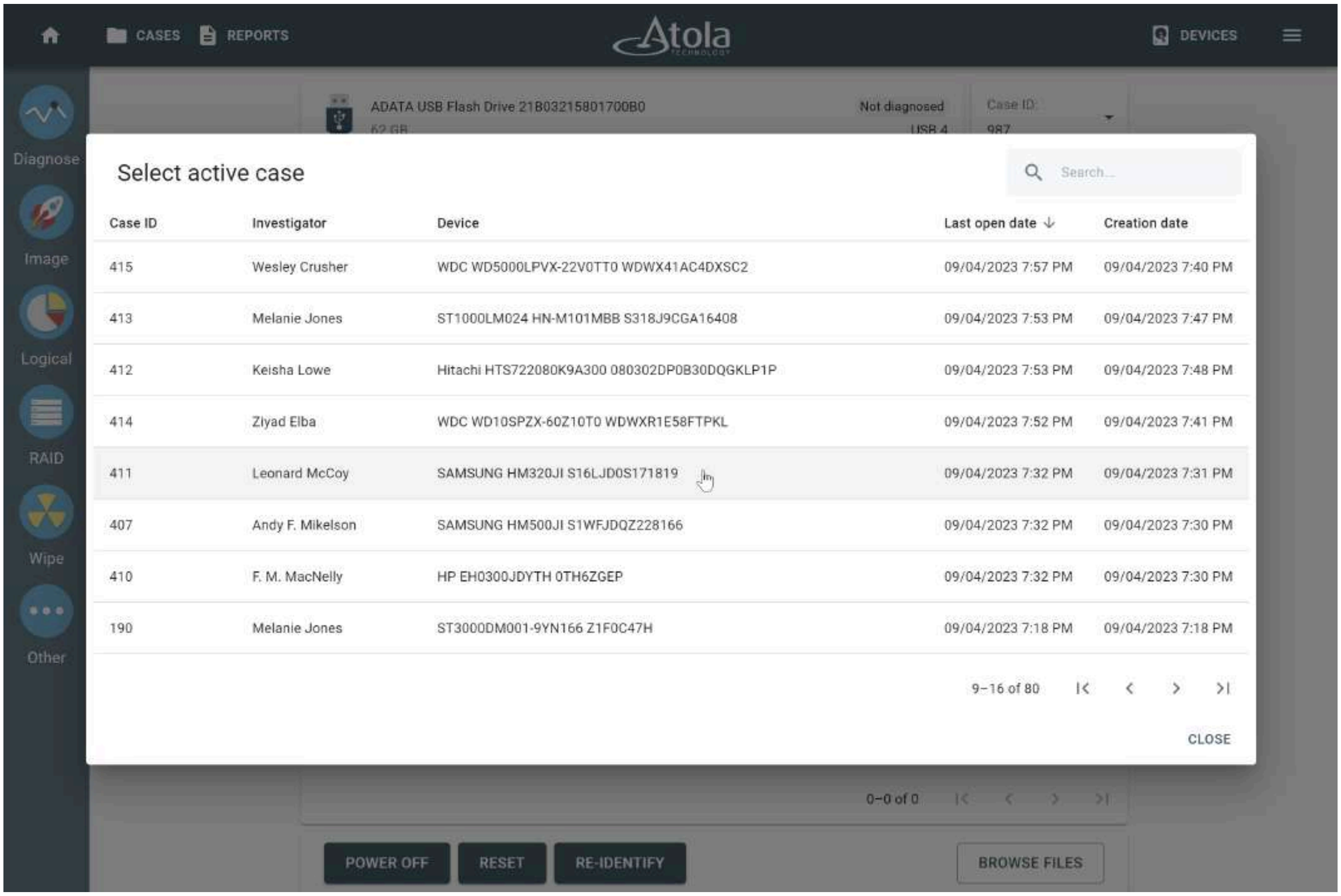
To add another device to an existing case, do the following:

1. Connect a device to TaskForce 2.
2. In the TaskForce user interface, click **Devices**.
3. In the **Select device** window, click on the port with your device. TaskForce takes you to the **Device** page.
4. **Optional:** If TaskForce hasn't identified your device yet, then, on the **Device** page, click **Re-identify**.
5. In **Case ID** pane, open the drop-down menu, and then click **Select**.



Change active case menu is opened on the Device page.

6. In the **Select active case** window, choose your existing case. If needed, use the **Search** field to find it.

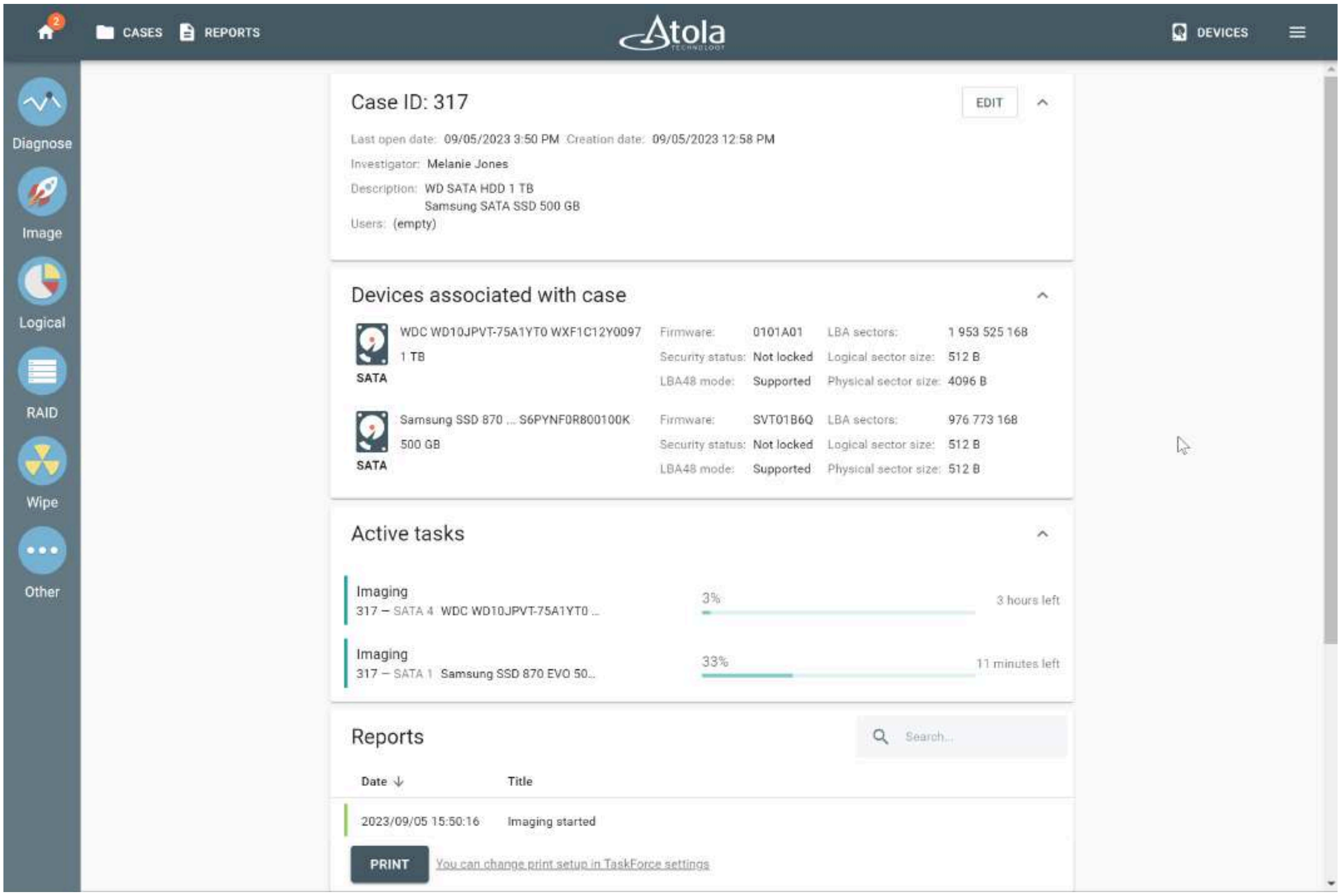


Select active case

Case ID	Investigator	Device	Last open date ↓	Creation date
415	Wesley Crusher	WDC WD5000LPVX-22V0TT0 WDWX41AC4DXSC2	09/04/2023 7:57 PM	09/04/2023 7:40 PM
413	Melanie Jones	ST1000LM024 HN-M101MBB S318J9CGA16408	09/04/2023 7:53 PM	09/04/2023 7:47 PM
412	Keisha Lowe	Hitachi HTS722080K9A300 080302DP0B30DQGKLP1P	09/04/2023 7:53 PM	09/04/2023 7:48 PM
414	Ziyad Elba	WDC WD10SPZX-60Z10T0 WDWXR1E58FTPKL	09/04/2023 7:52 PM	09/04/2023 7:41 PM
411	Leonard McCoy	SAMSUNG HM320JI S16LJD0S171819	09/04/2023 7:32 PM	09/04/2023 7:31 PM
407	Andy F. Mikelson	SAMSUNG HM500JI S1WFJDQZ228166	09/04/2023 7:32 PM	09/04/2023 7:30 PM
410	F. M. MacNelly	HP EH0300JDYTH 0TH6ZGEP	09/04/2023 7:32 PM	09/04/2023 7:30 PM
190	Melanie Jones	ST3000DM001-9YN166 Z1F0C47H	09/04/2023 7:18 PM	09/04/2023 7:18 PM

List of all your cases in the Select active case window.

Now, when you open your case, the **Case details** page lists all devices associated with the case. The **Case details** page also contains active tasks and reports for each device included in the case.



Case ID: 317

Last open date: 09/05/2023 3:50 PM Creation date: 09/05/2023 12:58 PM

Investigator: Melanie Jones

Description: WD SATA HDD 1 TB
Samsung SATA SSD 500 GB

Users: (empty)

Devices associated with case

SATA	WDC WD10JPVT-75A1YT0 WXF1C12Y0097 1 TB	Firmware: Security status: LBA48 mode:	0101A01 Not locked Supported	LBA sectors: Logical sector size: Physical sector size:	1 953 525 168 512 B 4096 B
SATA	Samsung SSD 870 ... S6PYNF0R800100K 500 GB	Firmware: Security status: LBA48 mode:	SVT01B6Q Not locked Supported	LBA sectors: Logical sector size: Physical sector size:	976 773 168 512 B 512 B

Active tasks

Imaging 317 – SATA 4 WDC WD10JPVT-75A1YT0 ...	3%	3 hours left
Imaging 317 – SATA 1 Samsung SSD 870 EVO 50...	33%	11 minutes left

Reports

Date ↓	Title
2023/09/05 15:50:16	Imaging started

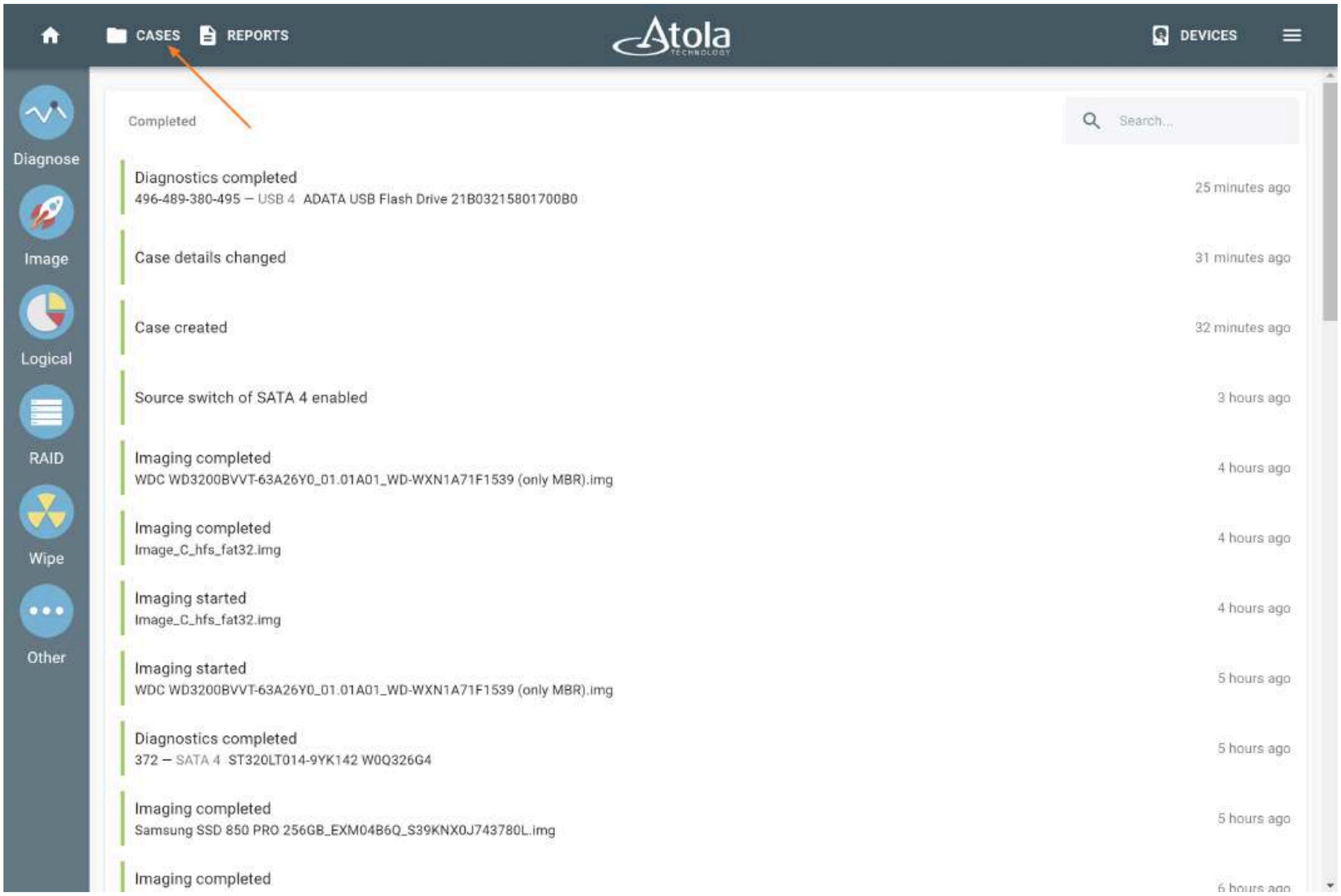
You can change print setup in TaskForce settings

All devices, active tasks, and reports associated with the case.

Find and edit cases

Atola TaskForce 2 automatically creates reports for every single action applied to each drive connected to it. Whether it is a source drive or a target drive, any action, be it imaging, wiping or physically switching write protection on or off, will be documented and stored in the system.

To find a case, click **Cases** in the top left corner, it will redirect you to the case management system.



Completed

Diagnostics completed
496-489-380-495 — USB 4 ADATA USB Flash Drive 21B03215801700B0
25 minutes ago

Case details changed
31 minutes ago

Case created
32 minutes ago

Source switch of SATA 4 enabled
3 hours ago

Imaging completed
WDC WD3200BVVT-63A26Y0_01.01A01_WD-WXN1A71F1539 (only MBR).img
4 hours ago

Imaging completed
Image_C_hfs_fat32.img
4 hours ago

Imaging started
Image_C_hfs_fat32.img
4 hours ago

Imaging started
WDC WD3200BVVT-63A26Y0_01.01A01_WD-WXN1A71F1539 (only MBR).img
5 hours ago

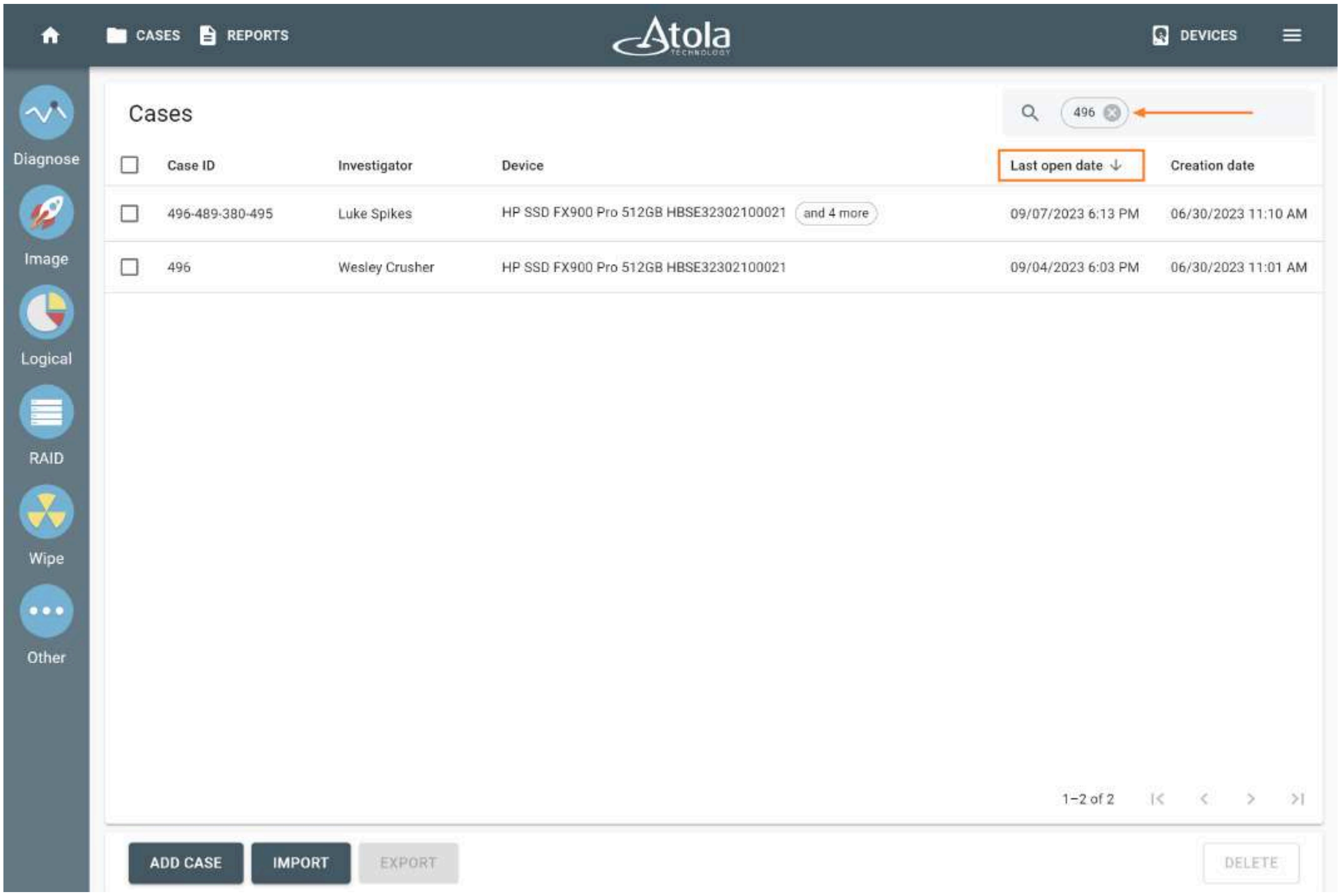
Diagnostics completed
372 — SATA 4 ST320LT014-9YK142 W0Q326G4
5 hours ago

Imaging completed
Samsung SSD 850 PRO 256GB_EXM04B6Q_S39KNX0J743780L.img
5 hours ago

Imaging completed
6 hours ago

Opening case management system.

Search for a specific case or device in the Search bar (by case ID, investigator's name or device details) and sort results by any column.



Cases

□	Case ID	Investigator	Device	Last open date ↓	Creation date
□	496-489-380-495	Luke Spikes	HP SSD FX900 Pro 512GB HBSE32302100021 and 4 more	09/07/2023 6:13 PM	06/30/2023 11:10 AM
□	496	Wesley Crusher	HP SSD FX900 Pro 512GB HBSE32302100021	09/04/2023 6:03 PM	06/30/2023 11:01 AM

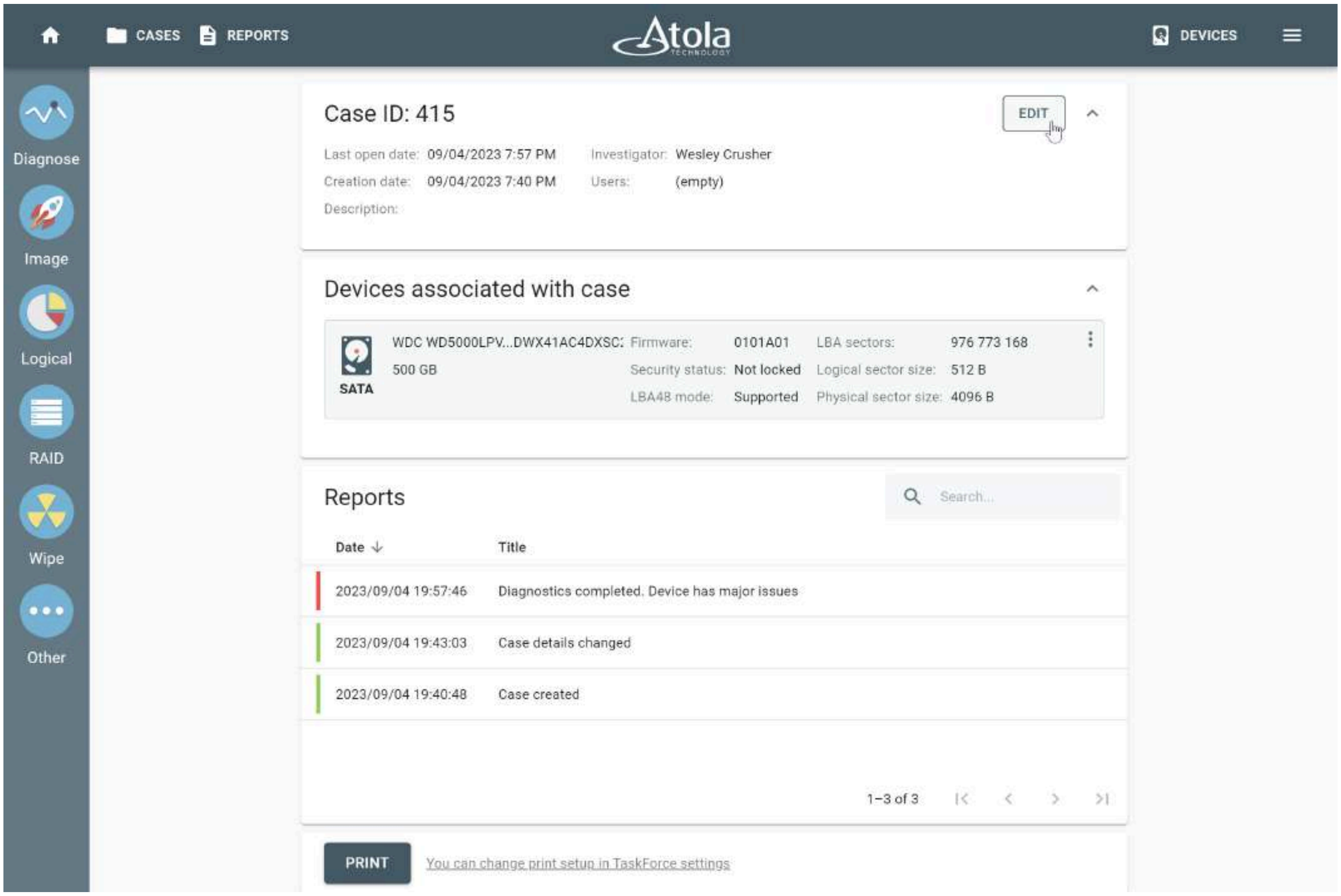
Searching and sorting cases in the list.

To open a case, click the respective line in the list.

A case page contains case details, information about the devices associated with the case (name, serial number, capacity etc.), as well as reports for all tasks applied to the device.

Edit case details

To change case details, click **Edit** at the top of a case page.



Case ID: 415

Last open date: 09/04/2023 7:57 PM Investigator: Wesley Crusher

Creation date: 09/04/2023 7:40 PM Users: (empty)

Description:

Devices associated with case

SATA

WDC WD5000LPV...DWX41AC4DXSC: Firmware: 0101A01 LBA sectors: 976 773 168

500 GB Security status: Not locked Logical sector size: 512 B

LBA48 mode: Supported Physical sector size: 4096 B

Reports

Search...

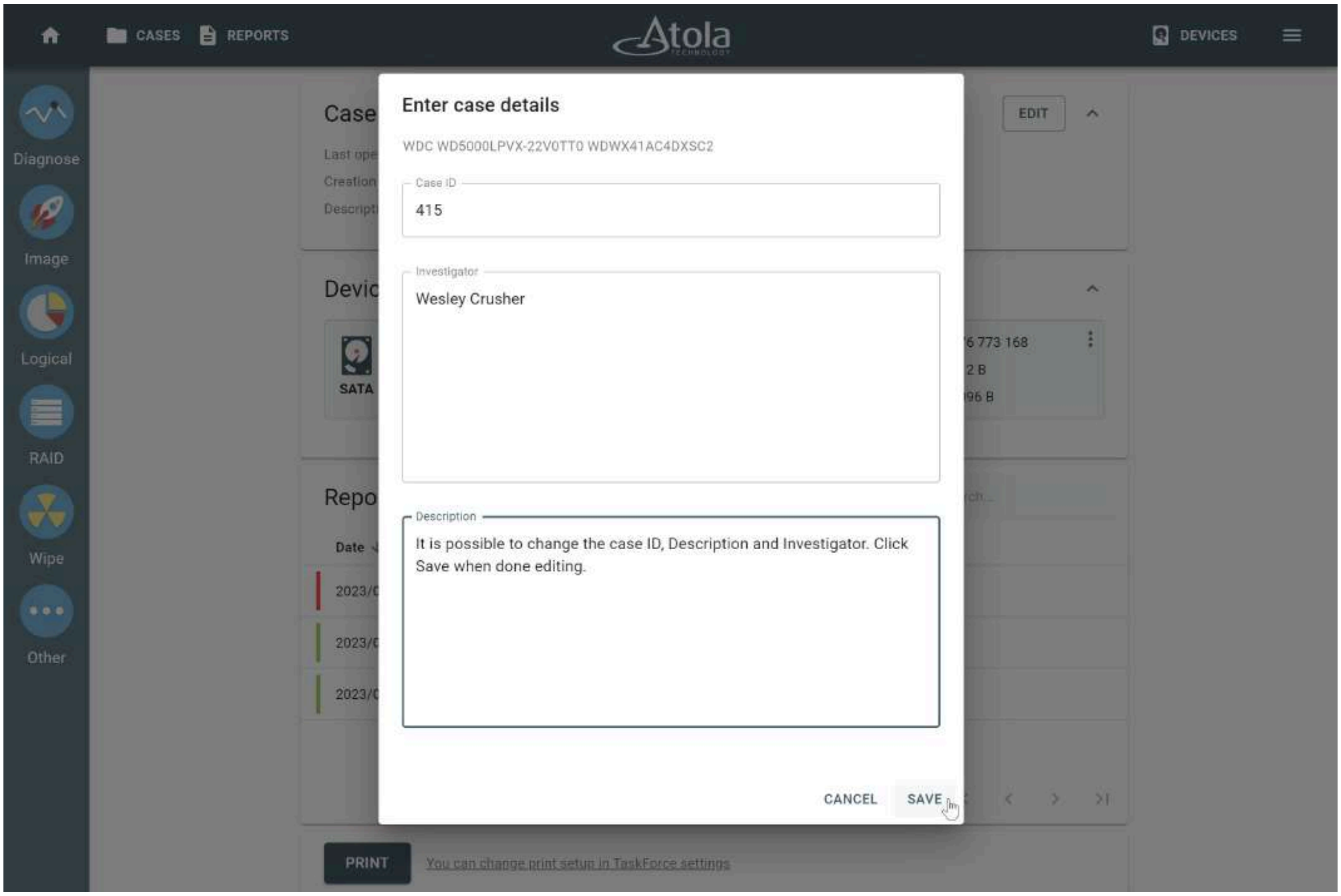
Date ↓	Title
2023/09/04 19:57:46	Diagnostics completed. Device has major issues
2023/09/04 19:43:03	Case details changed
2023/09/04 19:40:48	Case created

1–3 of 3

You can change print setup in TaskForce settings

Case page

It is possible to change the case ID, Description and Investigator. Click **Save** when done editing.



Enter case details

WDC WD5000LPVX-22V0TT0 WDWX41AC4DXSC2

Case ID: 415

Investigator: Wesley Crusher

Description: It is possible to change the case ID, Description and Investigator. Click Save when done editing.

You can change print setup in TaskForce settings

Changing case details.

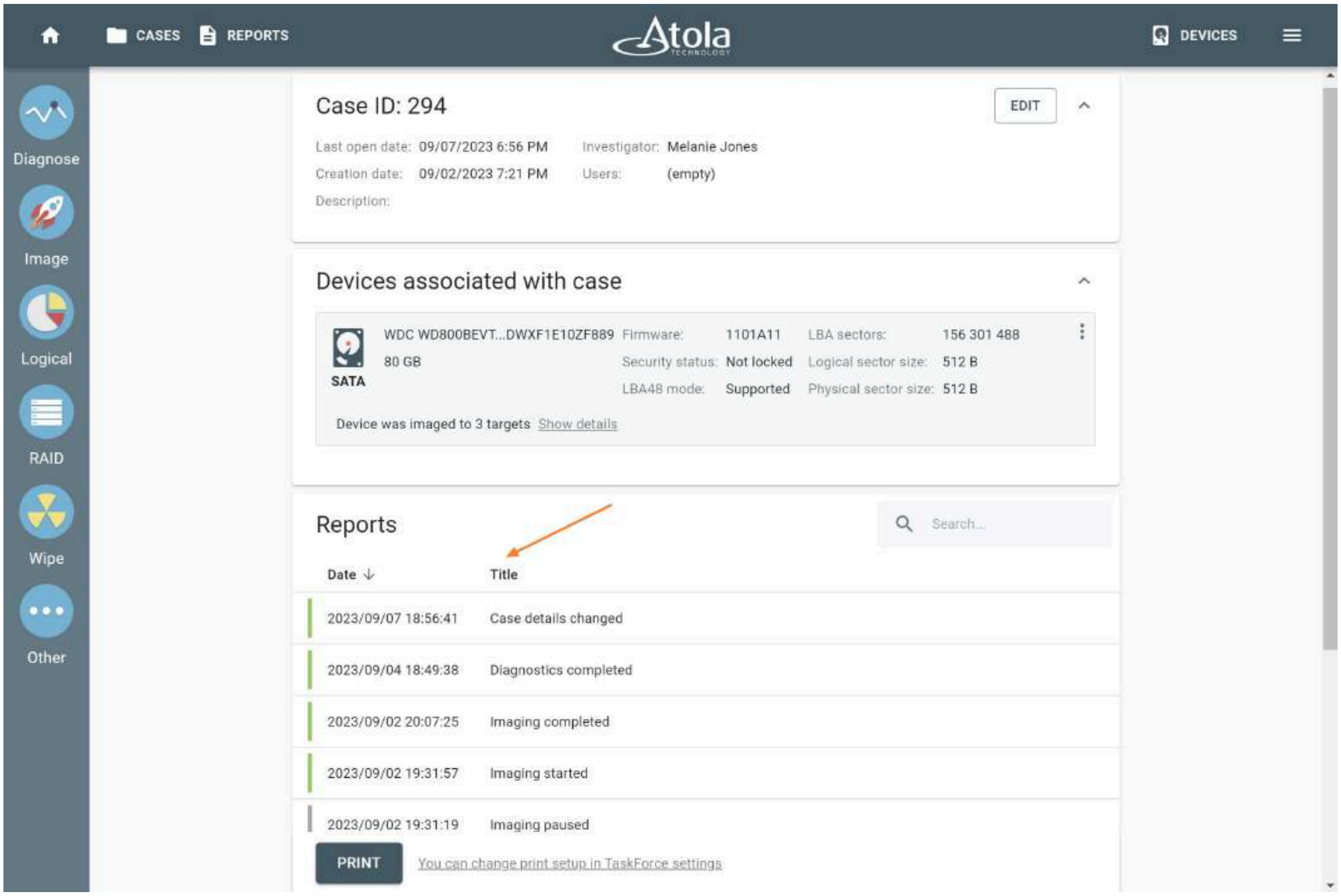
Finding reports

Atola TaskForce 2 automatically creates reports for every single action applied to each drive connected to it. The system also allows browsing through all cases and reports, without corresponding devices being connected to the unit. The reports are listed and can be easily retrieved in different parts of TaskForce 2 software.

1. Via case page

All reports related to the case are listed at the bottom of the case page. Scroll down and turn pages to view all the reports, sort them by date or by title, use the search bar to look for specific reports by their titles.

To open a report, click the respective line.



Case ID: 294

Last open date: 09/07/2023 6:56 PM Investigator: Melanie Jones
Creation date: 09/02/2023 7:21 PM Users: (empty)
Description:

Devices associated with case

WDC WD800BEVT...DWXF1E10ZF889
80 GB
SATA

Firmware:	1101A11	LBA sectors:	156 301 488
Security status:	Not locked	Logical sector size:	512 B
LBA48 mode:	Supported	Physical sector size:	512 B

Device was imaged to 3 targets Show details

Reports

Search...

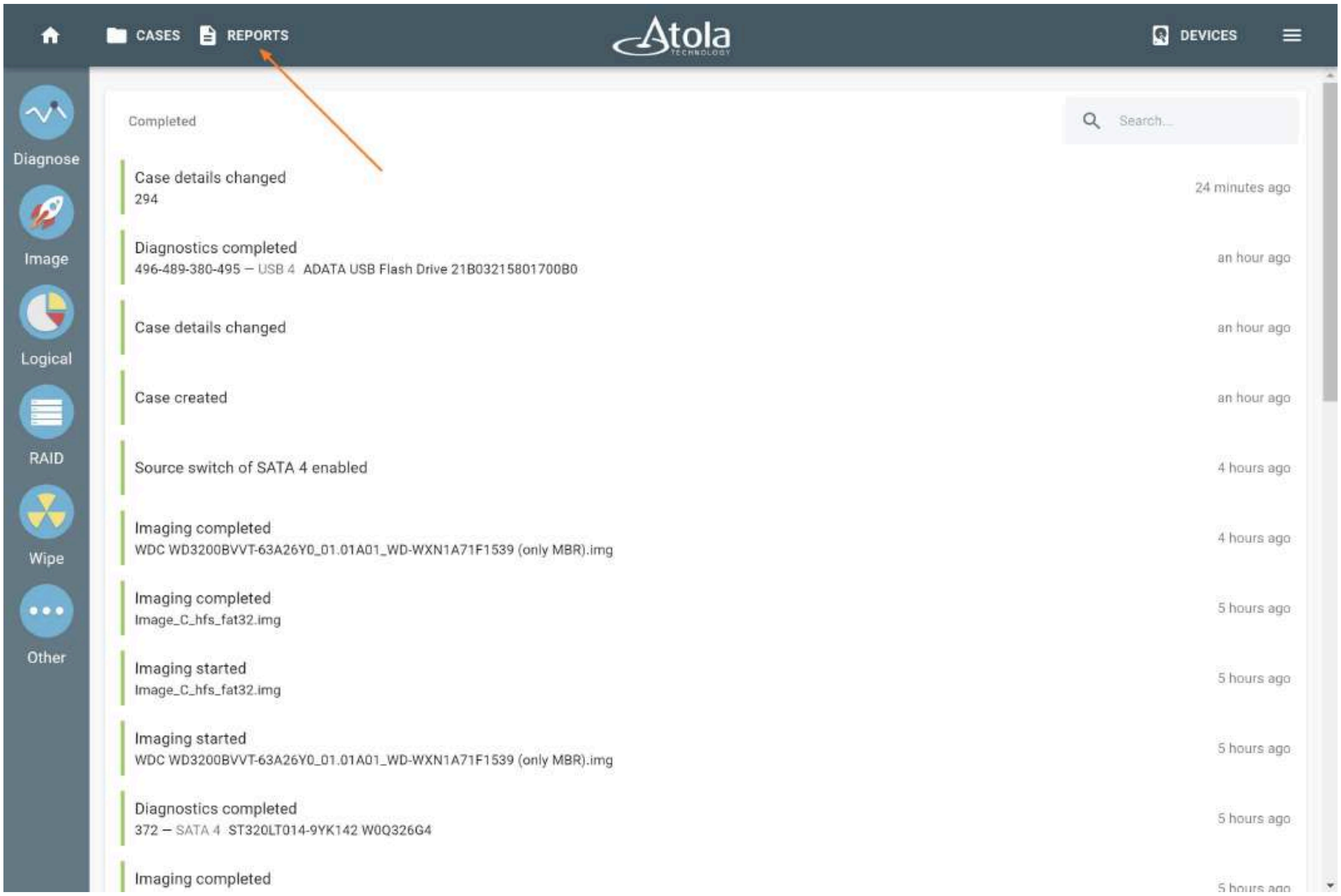
Date ↓	Title
2023/09/07 18:56:41	Case details changed
2023/09/04 18:49:38	Diagnostics completed
2023/09/02 20:07:25	Imaging completed
2023/09/02 19:31:57	Imaging started
2023/09/02 19:31:19	Imaging paused

PRINT You can change print setup in TaskForce settings

Case page with reports.

2. Via Reports page

If you need to search among all existing reports, click **Reports** at the top.



Completed

Case details changed
294
24 minutes ago

Diagnostics completed
496-489-380-495 — USB 4 ADATA USB Flash Drive 21B03215801700B0
an hour ago

Case details changed
an hour ago

Case created
an hour ago

Source switch of SATA 4 enabled
4 hours ago

Imaging completed
WDC WD3200BVVT-63A26Y0_01.01A01_WD-WXN1A71F1539 (only MBR).img
4 hours ago

Imaging completed
Image_C_hfs_fat32.img
5 hours ago

Imaging started
Image_C_hfs_fat32.img
5 hours ago

Imaging started
WDC WD3200BVVT-63A26Y0_01.01A01_WD-WXN1A71F1539 (only MBR).img
5 hours ago

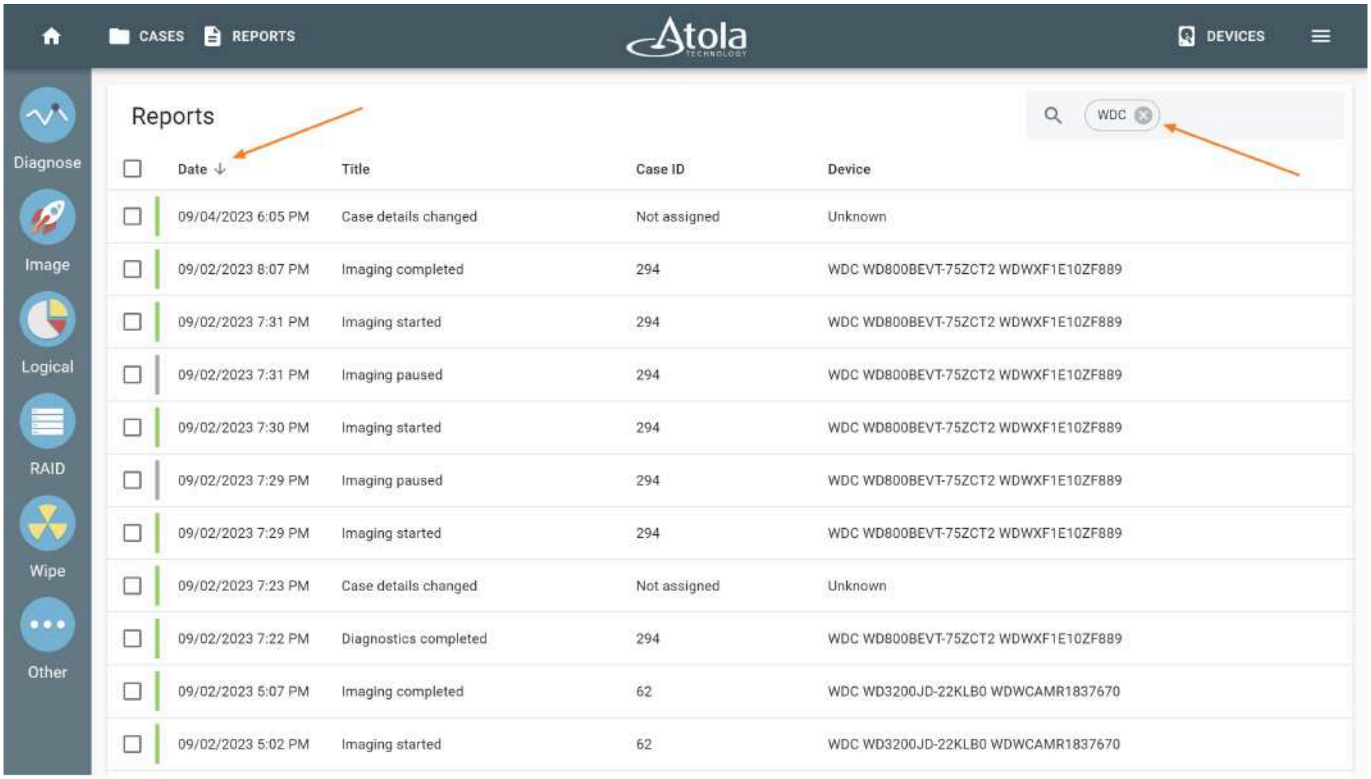
Diagnostics completed
372 — SATA 4 ST320LT014-9YK142 W0Q326G4
5 hours ago

Imaging completed
5 hours ago

The Reports button.

This will redirect you to the page with all existing report that can be filtered by date, title, case ID or device details. Search for a specific report by entering report title or drive details.

Open the report you need by clicking it in the list.



Reports

☐	Date ↓	Title	Case ID	Device
☐	09/04/2023 6:05 PM	Case details changed	Not assigned	Unknown
☐	09/02/2023 8:07 PM	Imaging completed	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 7:31 PM	Imaging started	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 7:31 PM	Imaging paused	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 7:30 PM	Imaging started	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 7:29 PM	Imaging paused	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 7:29 PM	Imaging started	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 7:23 PM	Case details changed	Not assigned	Unknown
☐	09/02/2023 7:22 PM	Diagnostics completed	294	WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
☐	09/02/2023 5:07 PM	Imaging completed	62	WDC WD3200JD-22KLB0 WDWCAMR1837670
☐	09/02/2023 5:02 PM	Imaging started	62	WDC WD3200JD-22KLB0 WDWCAMR1837670

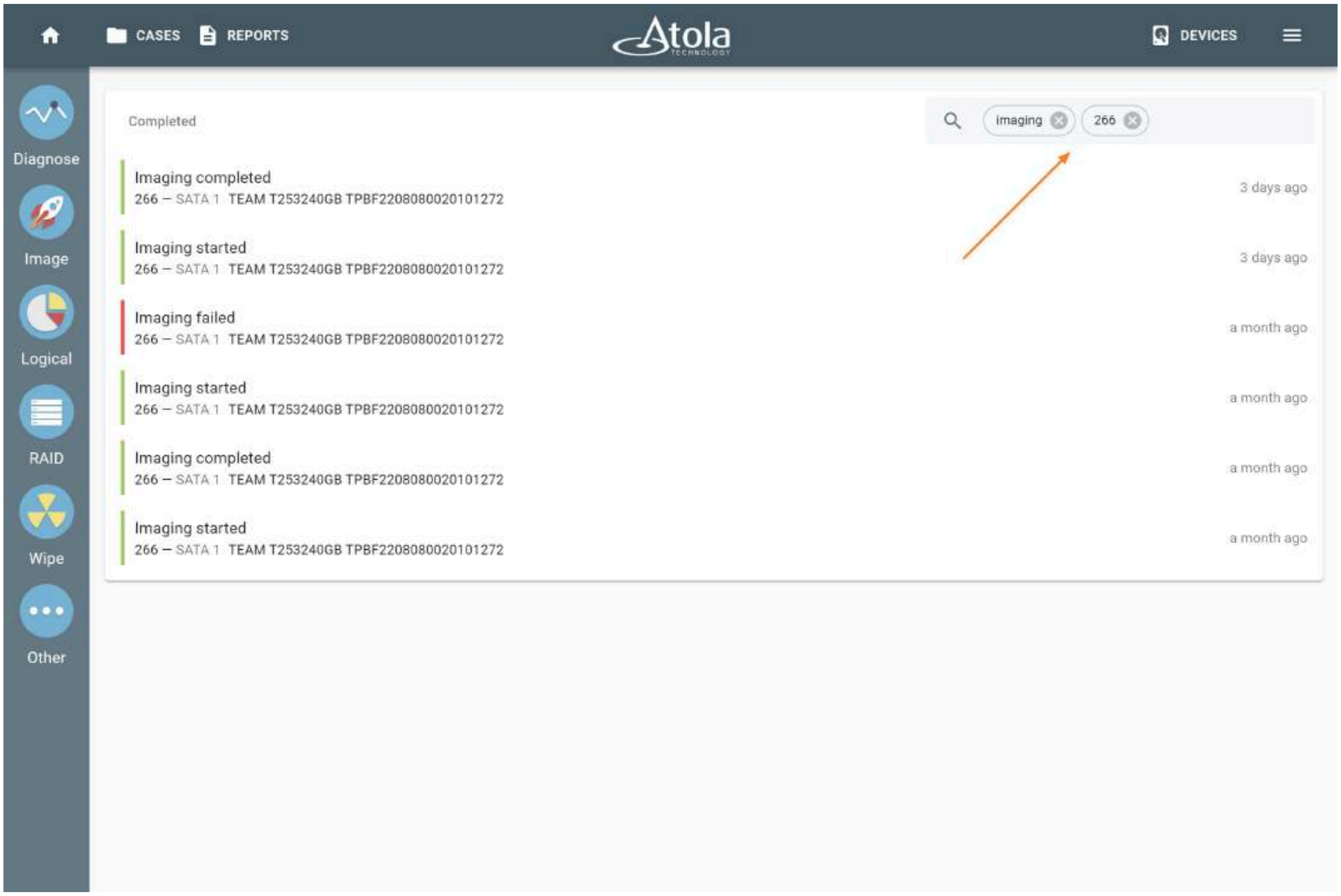
The Reports page.

3. Via Home screen

Similarly, recent reports can also be found on the **Home screen** underneath the **Active** tasks.

On the **Home screen** you can look up active and completed tasks and view reports for all completed tasks.

Quickly find specific reports by entering filters in the search field.



Completed

imaging 266

Imaging completed
266 – SATA 1 TEAM T253240GB TPBF2208080020101272
3 days ago

Imaging started
266 – SATA 1 TEAM T253240GB TPBF2208080020101272
3 days ago

Imaging failed
266 – SATA 1 TEAM T253240GB TPBF2208080020101272
a month ago

Imaging started
266 – SATA 1 TEAM T253240GB TPBF2208080020101272
a month ago

Imaging completed
266 – SATA 1 TEAM T253240GB TPBF2208080020101272
a month ago

Imaging started
266 – SATA 1 TEAM T253240GB TPBF2208080020101272
a month ago

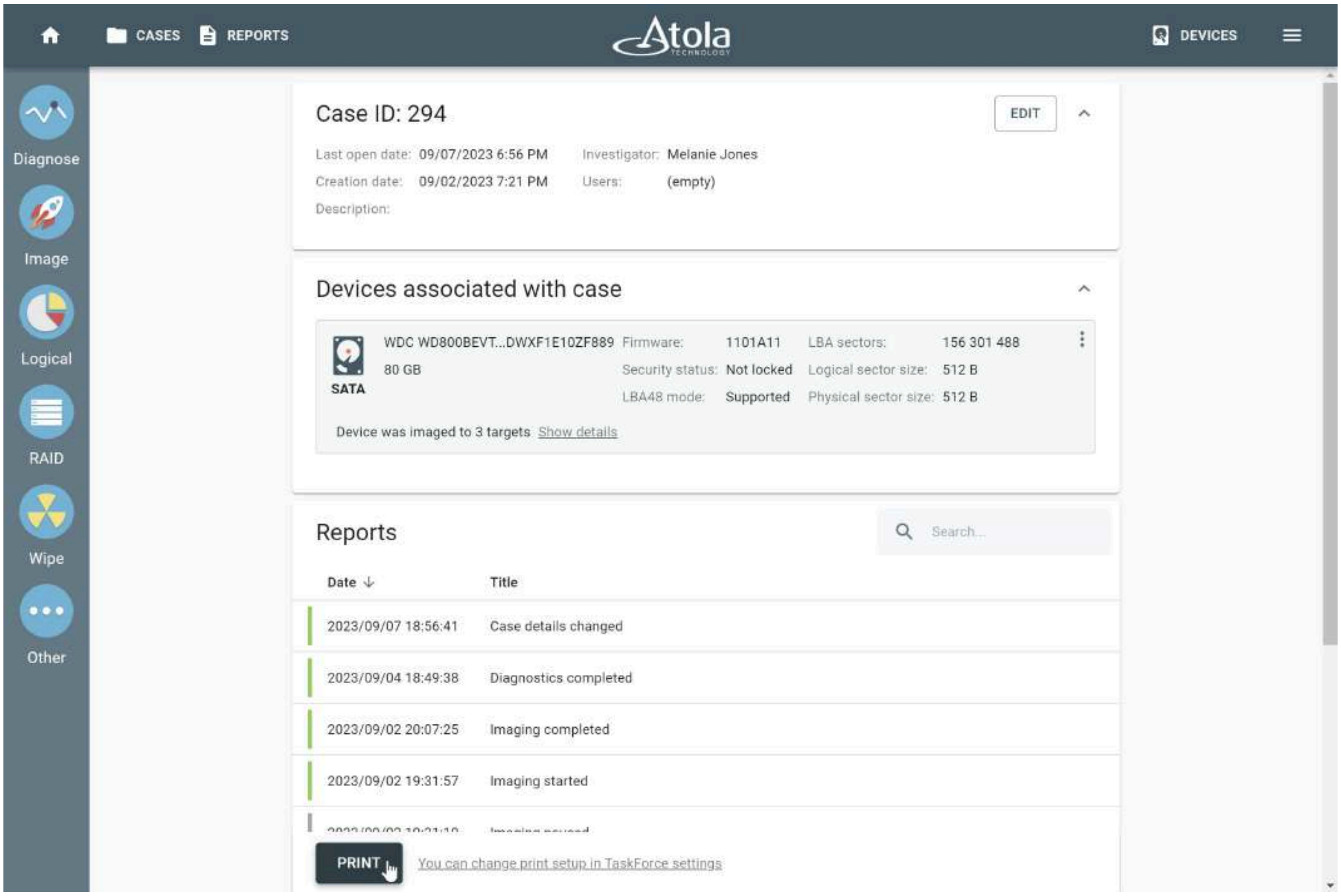
Finding reports on the Home screen.

Printing reports from a case

When you work on an investigation and want to have complete information about the evidence drive and all operations that have been taken to diagnose, image, calculate hash, etc., you can address Atola TaskForce’s case management system to print out all reports concerning your evidence.

To do that:

1. At the bottom of the case page, click **Print**.



Case ID: 294

Last open date: 09/07/2023 6:56 PM Investigator: Melanie Jones
Creation date: 09/02/2023 7:21 PM Users: (empty)
Description:

Devices associated with case

WDC WD800BEVT...DWXF1E10ZF889 80 GB
Firmware: 1101A11
Security status: Not locked
LBA48 mode: Supported
LBA sectors: 156 301 488
Logical sector size: 512 B
Physical sector size: 512 B

Device was imaged to 3 targets Show details

Reports

Search...

Date ↓	Title
2023/09/07 18:56:41	Case details changed
2023/09/04 18:49:38	Diagnostics completed
2023/09/02 20:07:25	Imaging completed
2023/09/02 19:31:57	Imaging started
2023/09/02 19:21:10	Imaging paused

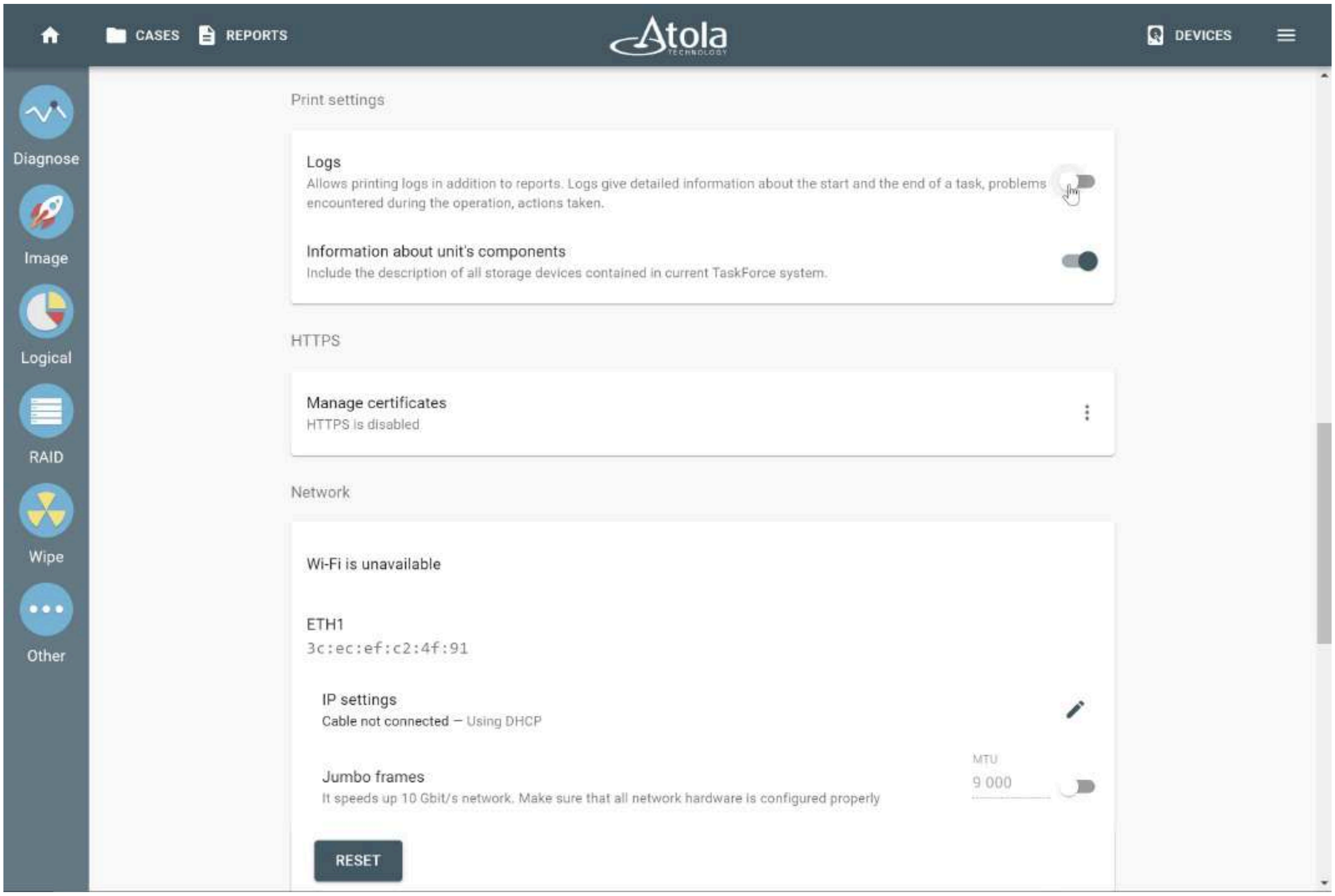
You can change print setup in TaskForce settings

The Print button an the bottom on the case page.

2. **Optional:** If you want the printed reports to include logs, go to the the **Menu** > **Settings**, scroll down to the **Print settings** section and toggle **Logs**.

> Logs are parts of the reports that give detailed information about the start and the end of a task, problems encountered during the operation (for example, inability to read a sector within the time allocated for the operation), actions taken (for example, jumps from a bad sector, completed pass of imaging, performed resets and power cycles etc.)

3. **Optional:** If you want the printed reports to include the description of all storage devices contained in current TaskForce system, go to the the **Menu** > **Settings**, scroll down to the **Print settings** section and toggle **Information about unit's components**.



Print settings

Logs
Allows printing logs in addition to reports. Logs give detailed information about the start and the end of a task, problems encountered during the operation, actions taken.

Information about unit's components
Include the description of all storage devices contained in current TaskForce system.

HTTPS

Manage certificates
HTTPS is disabled

Network

Wi-Fi is unavailable

ETH1
3c:ec:ef:c2:4f:91

IP settings
Cable not connected — Using DHCP

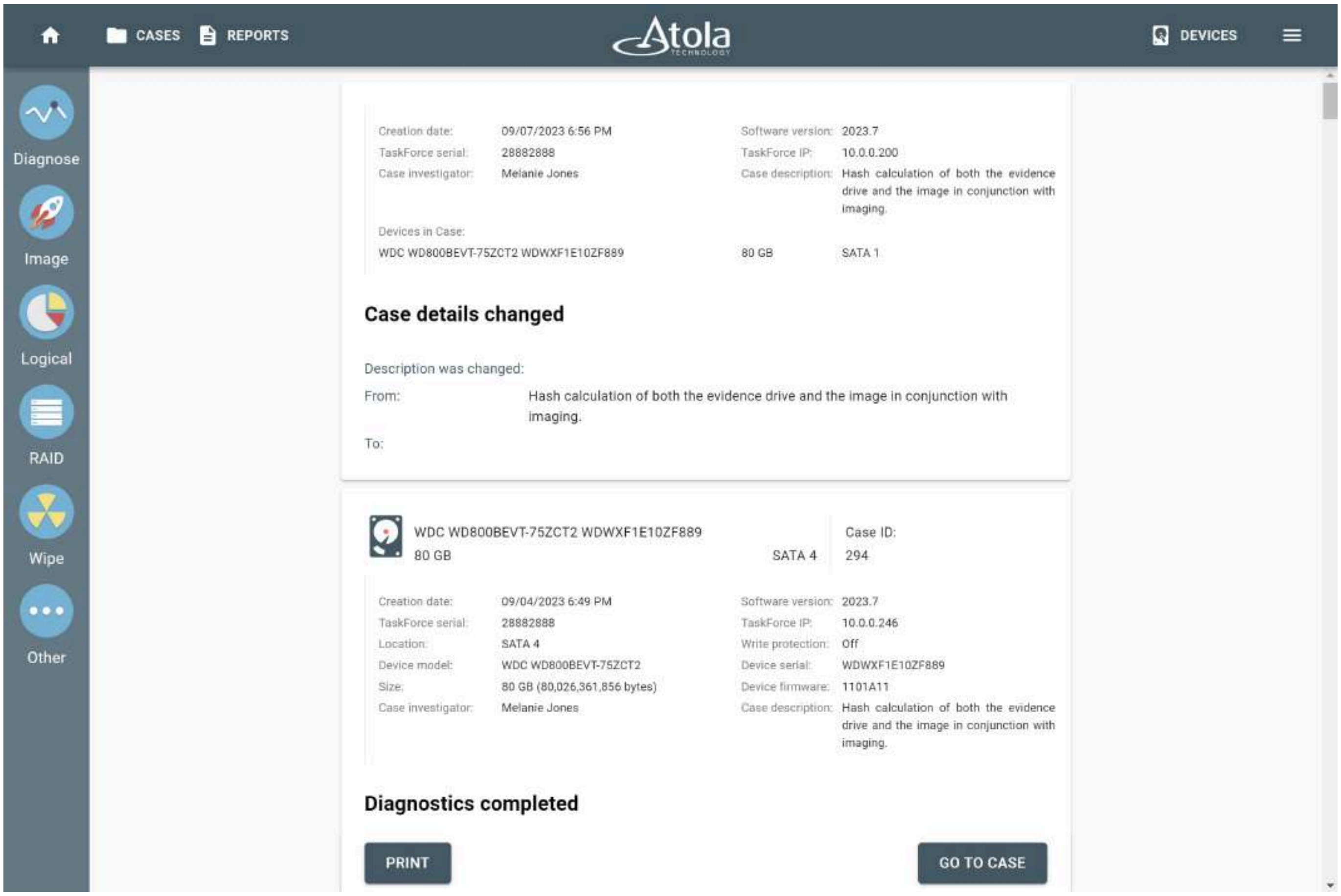
Jumbo frames
It speeds up 10 Gbit/s network. Make sure that all network hardware is configured properly

MTU
9 000

RESET

The Logs toggle in the Print settings section.

4. After you click **Print** on the case page, TaskForce takes you to a page with full reports. There they are arranged in same the order, in which they were listed on the case page (either by date or by title).



Creation date: 09/07/2023 6:56 PM
Software version: 2023.7
TaskForce serial: 28882888
TaskForce IP: 10.0.0.200
Case investigator: Melanie Jones
Case description: Hash calculation of both the evidence drive and the image in conjunction with imaging.

Devices in Case:
WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889 80 GB SATA 1

Case details changed

Description was changed:
From: Hash calculation of both the evidence drive and the image in conjunction with imaging.
To:

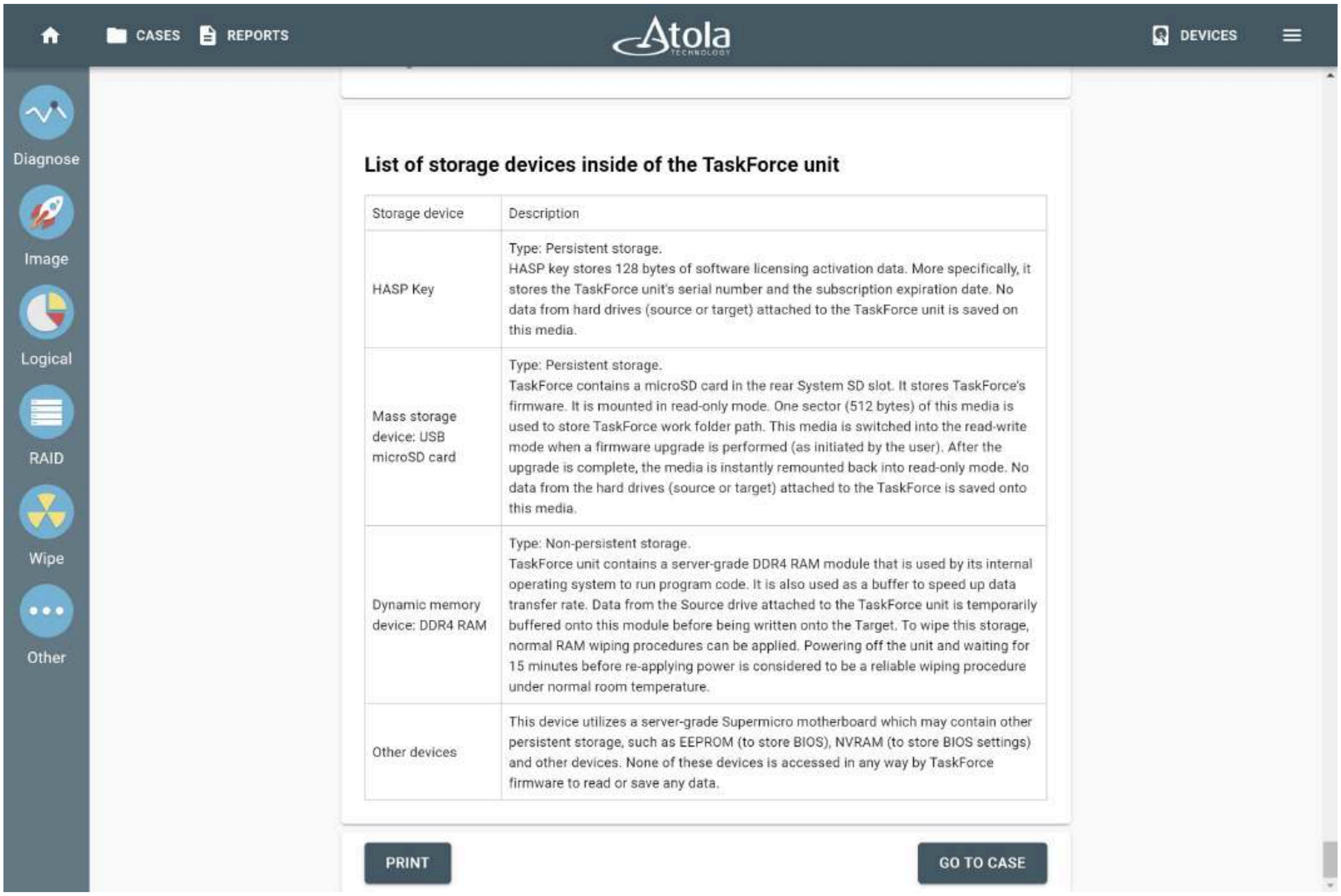
WDC WD800BEVT-75ZCT2 WDWXF1E10ZF889
80 GB SATA 4
Case ID: 294

Creation date: 09/04/2023 6:49 PM
Software version: 2023.7
TaskForce serial: 28882888
TaskForce IP: 10.0.0.246
Location: SATA 4
Write protection: Off
Device model: WDC WD800BEVT-75ZCT2
Device serial: WDWXF1E10ZF889
Size: 80 GB (80,026,361,856 bytes)
Device firmware: 1101A11
Case investigator: Melanie Jones
Case description: Hash calculation of both the evidence drive and the image in conjunction with imaging.

Diagnostics completed

Generated reports.

If you selected the **Information about unit's components**, the last report generated will include the description of all storage devices contained in current TaskForce system.



List of storage devices inside of the TaskForce unit

Storage device	Description
HASP Key	Type: Persistent storage. HASP key stores 128 bytes of software licensing activation data. More specifically, it stores the TaskForce unit's serial number and the subscription expiration date. No data from hard drives (source or target) attached to the TaskForce unit is saved on this media.
Mass storage device: USB microSD card	Type: Persistent storage. TaskForce contains a microSD card in the rear System SD slot. It stores TaskForce's firmware. It is mounted in read-only mode. One sector (512 bytes) of this media is used to store TaskForce work folder path. This media is switched into the read-write mode when a firmware upgrade is performed (as initiated by the user). After the upgrade is complete, the media is instantly remounted back into read-only mode. No data from the hard drives (source or target) attached to the TaskForce is saved onto this media.
Dynamic memory device: DDR4 RAM	Type: Non-persistent storage. TaskForce unit contains a server-grade DDR4 RAM module that is used by its internal operating system to run program code. It is also used as a buffer to speed up data transfer rate. Data from the Source drive attached to the TaskForce unit is temporarily buffered onto this module before being written onto the Target. To wipe this storage, normal RAM wiping procedures can be applied. Powering off the unit and waiting for 15 minutes before re-applying power is considered to be a reliable wiping procedure under normal room temperature.
Other devices	This device utilizes a server-grade Supermicro motherboard which may contain other persistent storage, such as EEPROM (to store BIOS), NVRAM (to store BIOS settings) and other devices. None of these devices is accessed in any way by TaskForce firmware to read or save any data.

Generated report listing all storage devices contained in current TaskForce unit.

On this page, there is another **Print** button. After clicking it you can configure printing settings.

Each report will be printed on a new page.

FAQ and Troubleshooting

- Imaging
- RAID configuration autodetection & imaging
- Performance
- Connectivity
- Wiping
- Case management & reports
- Subscription

Imaging

How do I clone a drive and create multiple identical copies?

TaskForce 2 is perfectly suited for cloning! Here is how to clone into 4 SATA drives and 1 RAW file simultaneously.

When you need to create multiple copies, simply:

1. Go to **Image**.
2. Select a source device.
3. Select up to 5 targets (SATA, USB, SAS or RAW, E01 files) and click **Continue**.
4. Click **Start**.

What's more, TaskForce 2 has 26 ports in total including IDE and Extension ports in combination with huge overhead capacity to handle many imaging sessions or other operations concurrently. So if you start a 1-to-5 cloning, you still have at least 20 ports left for additional cloning/imaging sessions to run simultaneously. TaskForce is designed to minimize the imaging time.

How do I image to an E01 or a RAW file?

When selecting targets in the slide-out panel, click the **Select file** tile. It only works if TaskForce 2 is connected to a network and with an accessible network folder.

How can I create an E01 image?

To image a source evidence drive to an E01 file, you have to create a new target file:

1. Go to **Image**.
2. Select the source evidence drive.
3. On the **Select target devices** panel, switch to the **Files** tab and click **Create file**.
4. In the file selector, find the folder to store the image and click **Create file**.
5. In the **Create image file** dialog, select the E01 file type.
6. Fill in the E01 file information, and then click **Create**.
7. On the **Select target devices** panel, click **Continue**.

Is there a way to delete an imaging session and start imaging all over again?

When you select source and target drives previously used in an imaging session, TaskForce 2 will indicate the progress status of the previous session, and you will be allowed to resume it.

To start a new imaging session with the same source and target, you will need to delete the previous one:

1. Go to **Image**.
2. Select the source drive.

How do I set up an automated launch of AXIOM after imaging?

You cannot launch third-party software from TaskForce 2 itself. However, with Magnet AUTOMATE, TaskForce can be integrated into a workflow with Magnet AXIOM. The Atola team closely cooperates with Magnet's developers to support and enhance this integration. See how it works.

Another option is a folder monitor/watchdog. Use an app that tracks when a new image file appears in a specific folder. After that, such an app can launch Magnet AXIOM against the newly created image. There are many watchdog tools on the web.

Why does a healthy drive appear to have many bad sectors during imaging?

The issue is likely caused by a loose port connection, leading to read errors and even drive identification issues.

To completely reset the physical link, unplug the cable from both the port and the storage device, wait for a full minute and plug it snugly back in.

It could also be cable wear-out. Swap cables between the "working" and "non-working" ports and see how it goes. If certain cables repeatedly cause issues, put them aside.

Why does TaskForce not open the 'Imaging Settings' page when I click 'Continue' upon selecting targets?

The issue must have been caused by the browser cache.

1. Go to Chrome browser settings.
2. Open the **Clear browsing data** option.
3. Clear all the data after selecting the **All time** range.

Please note that TaskForce works properly only with the Chrome browser.

How do I increase the speed when I image to the network?

When imaging to the network, there are two potential bottlenecks:

1. Network performance

It can be enhanced with a 10Gb connection. Another important thing: Jumbo frames should be enabled in the TaskForce settings, on the target computer/NAS network card, and on all network switches/routers in between.

2. Write speed of the target network drive

It can be more difficult to improve, especially if you are imaging several drives to the same network location. This leads to a situation where 8 source SSDs are read at 500 MB/s speed, but the total writing capability of the target network drive limits the speed to just 400 MB/s. Distributed between 8 sessions, the speed becomes too low (400/8=50 MB/s per session).

3. On the **Select target devices** panel, select the target and click **Continue**.
4. Right-click the imaging session.
5. In the context menu, click **Allow imaging map deletion**. A **Trash** icon appears in each imaging progress status tile.
6. To delete the previous imaging session, click the **Trash** icon. Now you can start a new session to the same target.

To disable imaging map deletion, click the imaging session again and select the option in the context menu.

Why does imaging to a NAS end up with a write error?

Possible causes and solutions:

- Maximum file size limitation by the proprietary NAS file system or OS.
- Minimum free space limitation in the NAS setting.
- Network folder permissions.
- Replace the Ethernet cable. Use Cat6 (with a length of less than 55 meters), Cat6a, Cat7, Cat7a, or Cat8 marking on it.

How do I restore a 520-byte sector-sized image to a drive?

TaskForce performs imaging and restores images in sector-to-sector mode. In the process, TaskForce does not convert logical data alignment depending on sector size, which keeps things simple and explicable.

If you have an image of a drive with a sector size of 520 bytes and you want to restore it to another drive, you must use a target SAS drive with a sector size of 520 bytes.

If the SAS drive's sector size is other than 520, you can reformat it in Linux using the sg_format utility: https://linux.die.net/man/8/sg_format

Then perform imaging to the target SAS drive by selecting the image file as a source.

The best solutions to achieve top speeds with target network locations:

- A RAID consisting of SSDs.
- A NAS combined with a 10Gb switch. For example, Ubiquiti EdgeSwitch 16 XG.
- A network server with many drives and great writing performance.

What is Storage mode?

TaskForce treats a target drive as a destination for sector-to-sector imaging unless you set it to Storage mode.

When the target drive is in Storage mode, it can only be used as a container for image files (E01, AFF4, or Raw). The software protects you from accidentally using a Storage drive for sector-to-sector imaging.

Storage mode features:

- You must format a target drive into Storage mode using TaskForce beforehand.
- When formatting in Storage mode, TaskForce creates a single exFAT partition with a large cluster size for the best imaging performance.
- TaskForce will automatically mount the target device formatted as a Storage when you plug it into TaskForce the next time.
- It's safe and works simpler than it seems. Format once and use it many times.

On top of that, you can select a VeraCrypt container instead of a simple exFAT partition to store image files in an encrypted form.

How can I image a SCSI drive?

Take advantage of USB ports and SCSI-to-USB adapters. There are a number of these on the market:

- Microtech XpressSCSI USB to SCSI adapter
- Belkin USB to SCSI Adapter
- Shuttle eUSCSI Bridge
- Castlewood ORB SCSI to USB adapter

RAID configuration autodetection & imaging

Can TaskForce 2 identify a RAID’s configuration if I include drives that are not RAID members (the drives are not marked properly)?

Normally, TaskForce 2 can identify the type of an unknown RAID within a minute. TaskForce reads data from the initial 3 million sectors of each drive and searches for the correct relation between the RAID members.

With an odd drive, the module will need more time to identify the configuration.

- In the case of RAID 1 or 10, detected mirrors will be arranged into groups, the odd drive will be placed separately, and partitions will be mounted successfully.

Can I select E01 images of drives for RAID reassembly?

You can select any combination of image files and/or drives constituting a RAID. See examples:

- 3 drives + 2 AFF4 files
- 5 E01 image files
- 2 raw files + 1 missing member

- If it is a JBOD, the partitions will likely be identified, and the order of the drives will be correct, with the odd drive placed at the end.
- As for RAID 0 or 5, TaskForce won't reassemble such an array: data from the odd drive is taken into account when TaskForce combines data from all members.

NB: The autodetection module attempts to identify the configuration from scratch each time you remove or add a drive. Try removing a drive that seems odd. Normally, RAID members are drives of the same capacity and usually of the same type, made by the same manufacturer, etc.

How do I manually reassemble a RAID knowing configuration parameters?

If you are sure you know all the RAID parameters, you can rebuild the RAID manually, ignoring the autodetection process.

This is the only way to rebuild and image a RAID array when the TaskForce RAID module does not recognize partitions because they are either encrypted or unsupported (for example, ReiserFS).

To rebuild a RAID manually, follow the steps below:

1. Select all RAID members (drives or their images).
2. Specify the following settings manually from the drop-down menus:
   a. RAID type (or RAID level)
   b. Start LBA (it is an offset for all RAID members)
   c. Block size
   d. Block order (only for RAID 5 and RAID 6)
   e. Device order (use the two-line button to drag and drop)
3. Click the **Go to Image** button.

Can I image a RAID array that contains a damaged drive?

The RAID assembly module requires good, readable drives to find a configuration. When one of the RAID's drives is damaged, it's best to image the drive first and attempt the reassembly using the image.

However, if the configuration is known and no search is required, you can try to mount the RAID even with a malfunctioning device. In this case, specify the configuration manually and proceed with imaging. TaskForce's multipass imaging engine handles RAID arrays with such issues effectively.

If you are dealing with a RAID 5, RAID 6, or RAID 1, TaskForce will use the RAID's redundancy when encountering internal read errors.

When one of the drives in a RAID 5 array is seriously damaged, you can add a virtual **Missing device** instead of the damaged device. Next, it is possible to reassemble and image the RAID 5 array from the remaining healthy drives and 1 "stub" device. TaskForce reconstructs data from such arrays on the fly during imaging.

Write error at the 16TB threshold occurs when imaging an assembled RAID. What should I do?

Check the file system of your target folder for maximum file limits. For example, these file systems are limited to the 16TB threshold:

- ext4
- NTFS
- Btrfs in some Synology NAS

To handle larger files in NTFS, you can reformat an NTFS partition to use a larger cluster size. By increasing the cluster size to 64 kilobytes (KB), you can create files up to 256 TB size-wise.

Performance

How to reach 25 TB/h?

TaskForce 2 was designed as an ultimate multitasking tool with a huge overhead capacity. Given that most imaged devices are HDDs, whose data transfer rate is 200 - 220 MB/s at best, it is not frequently that TaskForce will reach the limits of its capacity.

Our QA team achieves a speed of 25 TB/hour with this specific setup:

- imaging 8 SAS ports to 8 SATA ports (all SSD drives)
- imaging 2 NVMe ports to 2 NVMe ports
- imaging 1 USB ports to 1 USB ports (all SSD drives)
- imaging 2 USB ports to network files (10Gb connection)
- imaging the IDE port (with an IDE drive attached) to a network file (10Gb connection)

Instead of cloning, target drives can be formatted as Storage for E01/AFF4/RAW image files.

In most cases, you deal with HDDs as source devices, and they are half as fast as SSDs, which creates a bottleneck.

Performance when imaging to a remote USB drive (write cache + exFAT)

There are two ways to boost imaging performance:

1. Format the target drive to exFAT. It works faster than NTFS.
2. Enable Windows write cache:
   a. Go to **Device Manager**.
   b. In the **Disk Drives** category, select your drive.
   c. On the **Policies** tab, switch to **Better performance**.
   d. Confirm the reboot of the PC.

Important: When the last imaging session completes, use **Eject Removable media** icon in the system tray to guarantee cache-flushing of the last portions of written data. Here is an article explaining how it works.

Another potential performance bottleneck is network bandwidth. To achieve maximum throughput, connect ETH1 port to a network or NAS, and ETH2 port to another network or NAS. It will give you 20Gb/s of throughput. It also depends on your network hardware and setup.

To learn about network throughput optimization, read the official TaskForce manual:

- Jumbo frames for fast imaging to server
- Network setup

Connectivity

How to connect TaskForce to a fiber optic network?

Option 1. Use a 10GBASE-T RJ45 Copper Ethernet to 10G SFP+ Fiber Media Converter.

This device converts signals from your TaskForce’s 10 Gbit Ethernet ports to a fiber optic SFP+ connection, enabling high-speed network capabilities.

Option 2. Connect through a switch with SFP+ ports.

Integrating a network switch that has SFP+ ports can bridge TaskForce with fiber optic networks. Ensure that the switch supports 10 Gbit speeds to match TaskForce's capabilities.

Important considerations:

- Ensure that the SFP+ module is compatible with your switch brand (e.g., Cisco, Juniper).
- Use cables shorter than 55 meters with SFP+ modules; otherwise, these modules might not function properly.

How do I extend my server network with a DHCP-enabled switch?

Here is an example of a switch that supports static IP setup via simple web admin. To set the IP addresses for each current server network node:

Ubiquiti EdgeSwitch 16 XG
Four 10Gb Ethernet ports, twelve 10Gb SFP ports

To configure a Ubiquiti DHCP server:

1. Connect PC and TaskForce to Ubiquiti switch.
2. Set static IP address of PC to *192.168.1.4*.
3. Open a browser and enter *192.168.1.2* (default Ubiquiti switch IP).
4. Log in with default credentials: *ubnt* (both name and password).
5. Go to **System** > **Advanced Configuration** > **DHCP server** > **Global**.
6. Activate **Admin mode** by checking the required checkbox and clicking the **Submit** button.
7. Go to **Pool Summary** and click **Add** to make a new address pool.
8. Enter your:
   - pool name
   - network base address (192.168.1.0, for example)
   - network mask (255.255.255.0)

How do I setup Synology DS218?

1. Go to **Control panel** > **File services** > **SMB** > **Advanced settings**.
2. Set **Maximum protocol** to *SMB3*.
3. Go to **Control panel** > **Shared folder**.
4. Click the **Create** button and specify network folder details.

If you need to get a guest account working, perform the following actions:

1. Go to **Control panel** > **User**.
2. Edit the **Guest** user.
3. Clear the **Disable this account** checkbox.

How do I set up my network shared folder?

Follow these steps to setup Windows network folder:

1. Go to **Settings** > **Network & Internet** > **Status** > **Sharing Options**.
2. Open **Private (current profile)** section.
3. Select **Turn on network discovery**.
4. Select **Turn on file and printer discovery**.
5. Open **Guest** or **Public** section.
6. Repeat steps 3 and 4 for **Guest** or **Public** section.
7. Open **All Networks** section.
8. Select **Turn on sharing** so anyone with network access can read and write files in the **Public** folders.
9. Select **Turn off password protected sharing**.
10. Click **Save changes**.

If the above has not fixed the issue, edit the folder share permissions:

1. Open the **Computer Management** window (press **Win** button and type in **Computer Management**).
2. Expand **System Tools** > **Shared Folders** and click **Shares** in the left-side tree.
3. Right-click the shared folder in the central pane and click **Properties**.
4. Select the **Share Permissions** tab.
5. Click **Add** to assign permissions to the shared folder for a user group.
6. In the dialog box, type *Everyone* and click **OK**.

- put **Default Router Address** and **DNS**

After creating your pool, you can change it via **Pool configuration** tab.

9. Click the **Save configuration** button in the upper right corner of the window and then **Save**.

Alternatively, there is a tutorial on Youtube.

To enable 10Gb with jumbo frames:

1. Go to **Basic** > **Port summary**.
2. Select ports *0/13, 0/14, 0/15* and *0/16* and click **Edit**.
3. In the **Edit Port configuration** window, change **Maximum Frame Size** to *9014*.

Why does an IP address not show despite an Ethernet cable being plugged into the unit?

Usually, your network router is responsible for assigning IP addresses to other computers or devices in the same network.

Make sure your router has DHCP support and it is enabled.

There is no DHCP server on our internal lab network. How do I assign a static IP address to TaskForce?

1. In TaskForce, click the menu button in the top right corner.
2. Click **Settings**.
3. In the **Network** section, find IP settings for both 10Gb Ethernet cards.
4. Click the pencil button to see **Use static IP** checkbox.

Atola TaskForce demo video includes a basic explanation of the network settings. Here's a Youtube video on that.

How do I connect TaskForce 2 to a network domain?

TaskForce 2 does not require a preliminary setup for working in a domain. Instead, your flow would be:

1. In the left-side taskbar, click the **Image** icon.
2. In the left slideout panel, select the source.
3. To select the target, in the **File** section, click **Select file**.
4. In the file manager's **Local network** section, click the **Connect** button.
5. A new dialog appears with the **Domain** field.

The entered server will remain in the **Local Network** section list.

Additionally, in Web API, there's a *targetFolderDomain* parameter of */start-image* command that may be of use.

7. Select **Full control** permission (**Read & Write** permissions) for the user group you have just added.
8. Click **OK**.

We strongly recommend using the latest OS versions. It is crucial for reaching high network transfer speeds.

How do I set up the Windows Server share?

In **Control panel**:

1. Enable the **Guest** account (**Administrative tools** > **Add users and computers** > **Users**).
2. Next, go to **Network and sharing center** and choose **Change advanced sharing settings**.
3. Select **Turn On network discovery** and **Turn on sharing (file and printers + public folders)**.
4. In the shared folder access options, add **Guest** or **Everyone**.

If the shared folder demands restricted access, please follow this guide.

TaskForce booting does not get completed. What should I do?

To ensure TaskForce boots correctly, reset the device:

1. Power off TaskForce.
2. Detach all devices and cables from the system (including PSU cable, Extension module, SATA cables, USB devices/cables, etc.). So the TaskForce should be just by itself with nothing attached to it at all.
3. Give it 3-5 minutes to fully reset. There are a few internal circuits that need up to a minute to fully reset after powering off, but we recommend waiting at least 5 minutes to be sure.
4. Plug only the power cable back in (no network/USB/SATA cables, etc.).
5. Power TaskForce on and wait for 3-4 minutes.

How to see the syslog for more information about the issue I am facing?

To download the TaskForce logs:

1. Connect TaskForce to the network so that you can access it from your PC.
2. An IP address is shown on the IP screen on the front panel of the unit. Let's say, it is *10.0.0.33*.
3. On your PC, open the Chrome browser and enter *http://10.0.0.33/syslog*.
4. Click *Save*.
5. This will download the logs to your PC's *Downloads* folder.

Wiping

How does SSD Trim work and does it wipe a drive completely?

SSD Trim doesn't instantly wipe sectors (NAND memory cells) of a drive. It instructs SSD's firmware which sectors can be wiped by marking them as '*dirty*'.

The time of erasure of '*dirty*' sectors depends on the SSD manufacturer and firmware. For instance, recent Samsung SSDs have a so-called foreground garbage collection. It wipes any erased file almost immediately thanks to a TRIM command proactively executed by the operating system. In older SSDs, trimmed sectors can remain intact for minutes or even hours.

The most secure way to erase an SSD entirely is using one of the following methods:

- **Secure Erase** - for SATA drives
- **Format NVM** or **Sanitize** - for NVMe drives

The drive's internal implementation of these commands is vendor-specific. In most drives, it ensures full erasure of an SSD including non-addressable areas.

Case management & reports

Can all reports listed on the main page be sorted, managed, or deleted?

Yes, they can be filtered, sorted, exported, and deleted. The quickest way to perform a search is by using the **Search** field above the reports on the main page. Entering the task name (**Image, Diagnose, Wipe**) and/or device model/serial helps get a more specific output.

To sort, export, or delete reports, you can go to **Reports** in the top menu, where all case reports are shown in a table view. **Save to** helps download the selected reports in a single ZIP file. There is also a **Delete** button in the bottom right corner for your needs.

Can reports only be exported in PDF, can I export them in RTF format instead?

It should be possible to save a page into RTF. For example, in this Chrome AddOn you can select the reports and click **Print**. It will generate a single page with all selected reports, which can be exported to .RTF file.

Subscription

How do I activate my unit in a network-free environment?

There is a single way to perform TaskForce 2 activation or subscription extension:

1. Enter the TaskForce 2 serial number. It can be found at the bottom of the unit.
2. TaskForce 2 generates a license key (Internet connection is not required).
3. You find an Internet-connected PC and visit the website: a.atola.com.
4. You enter the license key and several other details.

Why does Internet Explorer rename TaskForce's .AFM2 firmware file to a ZIP file?

Internet Explorer identifies an AFM2 file as a ZIP file and automatically renames it to ZIP. Read this article about the reason Explorer does this. This issue only occurs in the Internet Explorer.

We suggest using other popular browsers, such as Chrome or Firefox.

5. The website generates a TaskForce activation code.
6. You write the code down or take a photo, and then enter it in the TaskForce activation screen.

Warning: file_get_contents(troubleshooting.html): failed to open stream: No such file or directory in **/home/atola/public_html/products/taskforce/manual/one.html** on line **81**
File is not found: troubleshooting.html