

# Atola Insight Forensic Manual

Version: Dec 02 2025

## Quickstart

- [Start imaging](#)

## Introduction

- [About Atola Insight Forensic](#)
- [Workflow](#)

## Unit & extensions

- [Package contents](#)
- [DiskSense 2 unit](#)
- [M.2 SSD extension](#)
- [Apple PCIe SSD extension](#)
- [SAS extension](#)
- [Thunderbolt extension](#)

## Installation & environment setup

- [First use guide](#)
- [Extending subscription offline](#)
- [Hardware and OS requirements](#)
- [DiskSense / HASP connection issues](#)
- [Network database setup](#)
- [Database backup and restore](#)

## Connecting and disconnecting devices

- [Supported drives](#)
- [Working with SATA, USB, IDE drives](#)

# Interface controls & indicators

- [Main window and controls](#)
- [ATA registers: what they mean](#)

# Diagnostics

- [Automatic diagnostics](#)
- [Media scan](#)
- [Track SMART table before and after imaging](#)

# Imaging: Basics

- [Image to a file on a target device](#)
- [Image to a file on an encrypted target](#)
- [Image to 3 targets](#)
- [Image to an E01 file with dual hash](#)
- [Logical imaging to L01 file](#)
- [Clip target drive to source evidence size](#)
- [Artifact search during imaging](#)
- [Split an imaging session to separate targets](#)
- [Image only selected sectors](#)
- [Image a remote drive via iSCSI](#)

# Imaging: Damaged drives & performance

- [Image 3 source drives simultaneously](#)
- [Multipass imaging of damaged drives](#)
- [Image drives with damaged heads](#)
- [Image freezing damaged drives](#)
- [Image a shorted drive](#)
- [Imaging speed](#)
- [Launch a CLI app after imaging](#)
- [Cheat sheet](#)

# Calculating & verifying hash

- [Segmented hashing](#)
- [Verify damaged images with segmented hashing](#)
- [Calculate hash during imaging](#)
- [Calculate dual hash of an existing E01 file](#)

- [Compare source & target to find modified data](#)
- [Hash lists to filter good & bad files](#)

## Unlocking devices

- [Extract/Reset an unknown ATA password](#)
- [Unlock Hitachi drives](#)
- [Unlock Seagate drives](#)
- [Recover damaged Seagate 7200.11 drives](#)

## More features & special capabilities

- [Artifact Finder](#)
- [Disk Editor](#)
- [Locate sectors](#)
- [Lift HPA, DCO, AMA restrictions](#)
- [Multitasking](#)
- [Restore image file to device](#)
- [Wipe multiple drives simultaneously](#)

## Case management

- [Case management system](#)
- [Find and open a case](#)
- [Print reports in a case](#)
- [Change details in a case](#)
- [Export and import cases](#)

## What else?

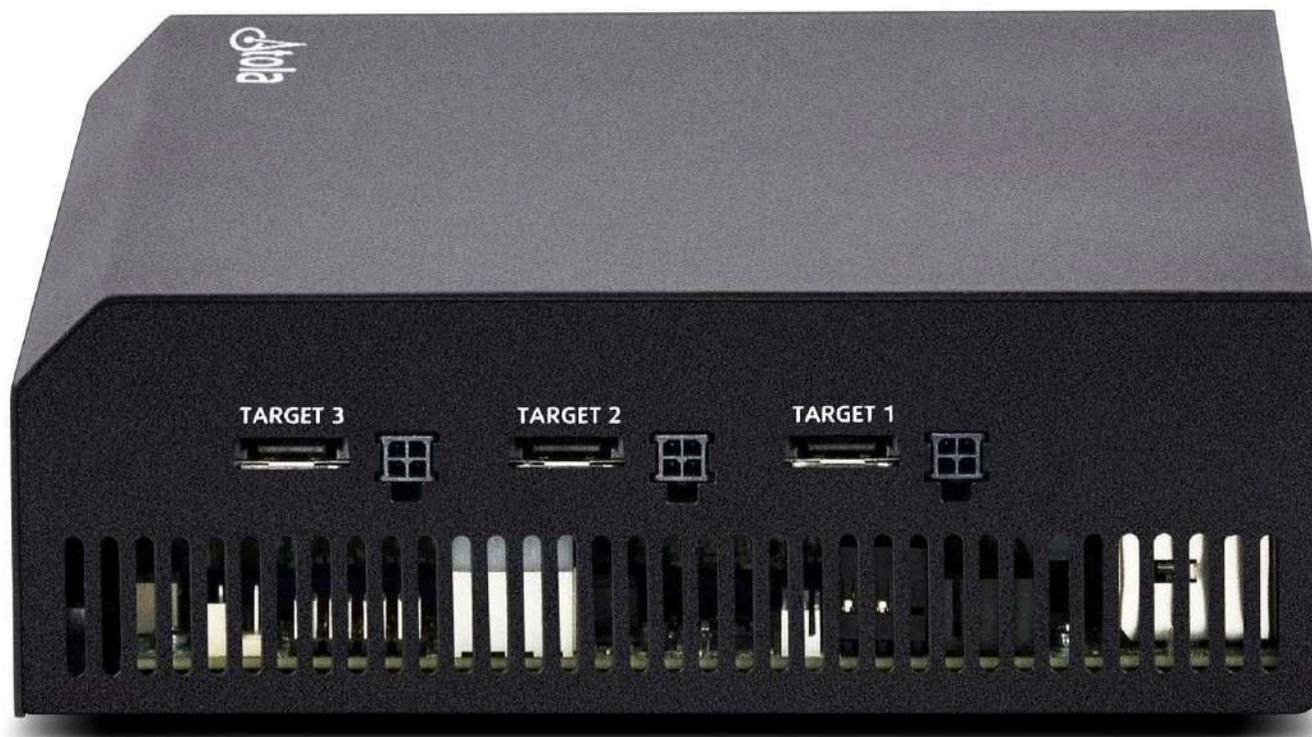
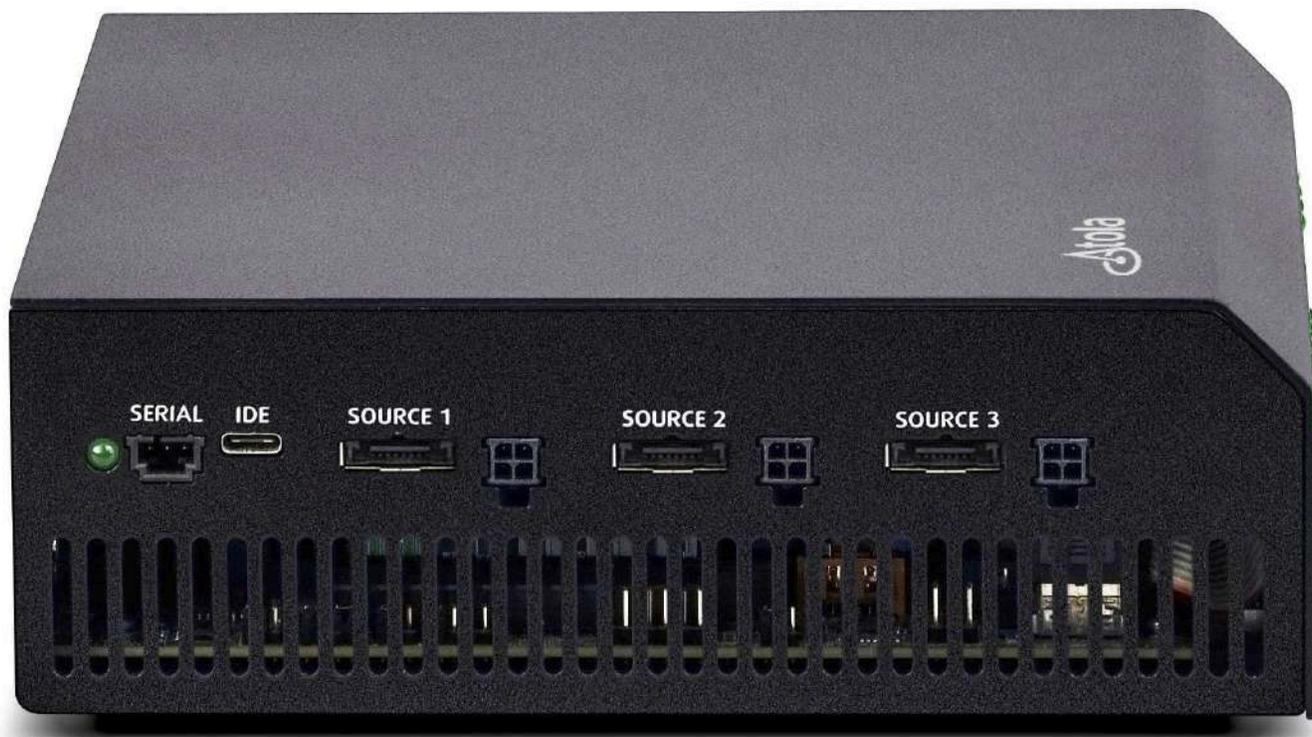
- [FAQ and Troubleshooting](#)

## Quickstart

Assuming you have Atola Insight Forensic software [installed and activated](#), let us start from zero and learn how to image an evidence device safely in Atola Insight Forensic.

**Step 1. Plug the source and target devices into the DiskSense 2 hardware unit.**

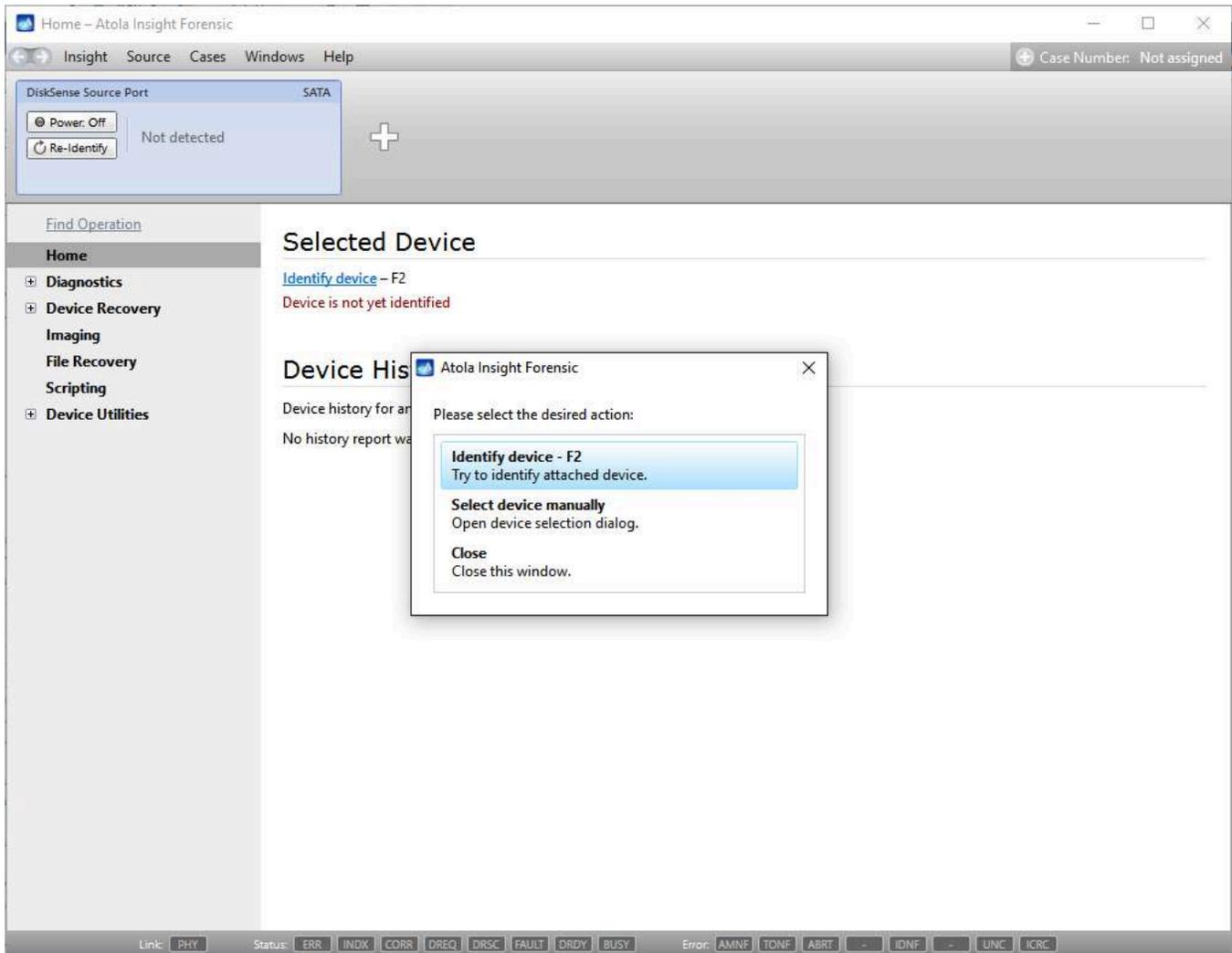
Take two SATA drives that will serve as your source and target devices. Plug them into the SATA source and SATA target ports.



## Step 2. Launch Atola Insight.

Launch already installed Atola Insight Forensic software.

You will see the following window requesting that you select the desired action:



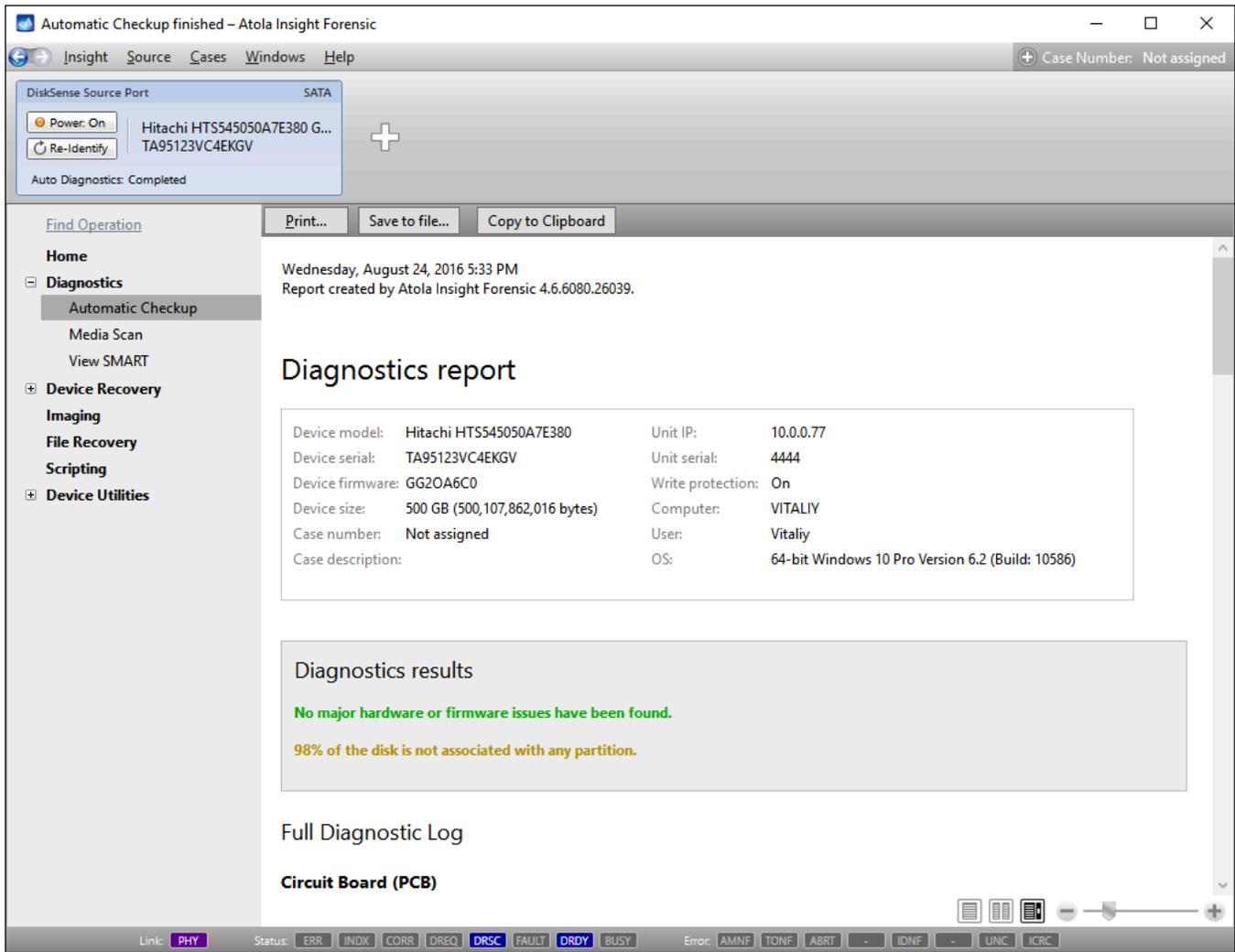
Select **Close** to avoid powering up the source SATA port for now.

### Step 3. Diagnose first before imaging.

Presumably, we know nothing about the source device and its state. Maybe it is a good working drive, or maybe it is not. It may be a damaged one or it may die in a few hours. That is why we should begin with **Automatic Checkup**.

Go to **Diagnostics > Automatic checkup**, and then click the **Start** button.

It will take a couple of minutes to get to the Diagnostics report. In this particular case, we see that the source drive is in good state, and we can safely start imaging it.



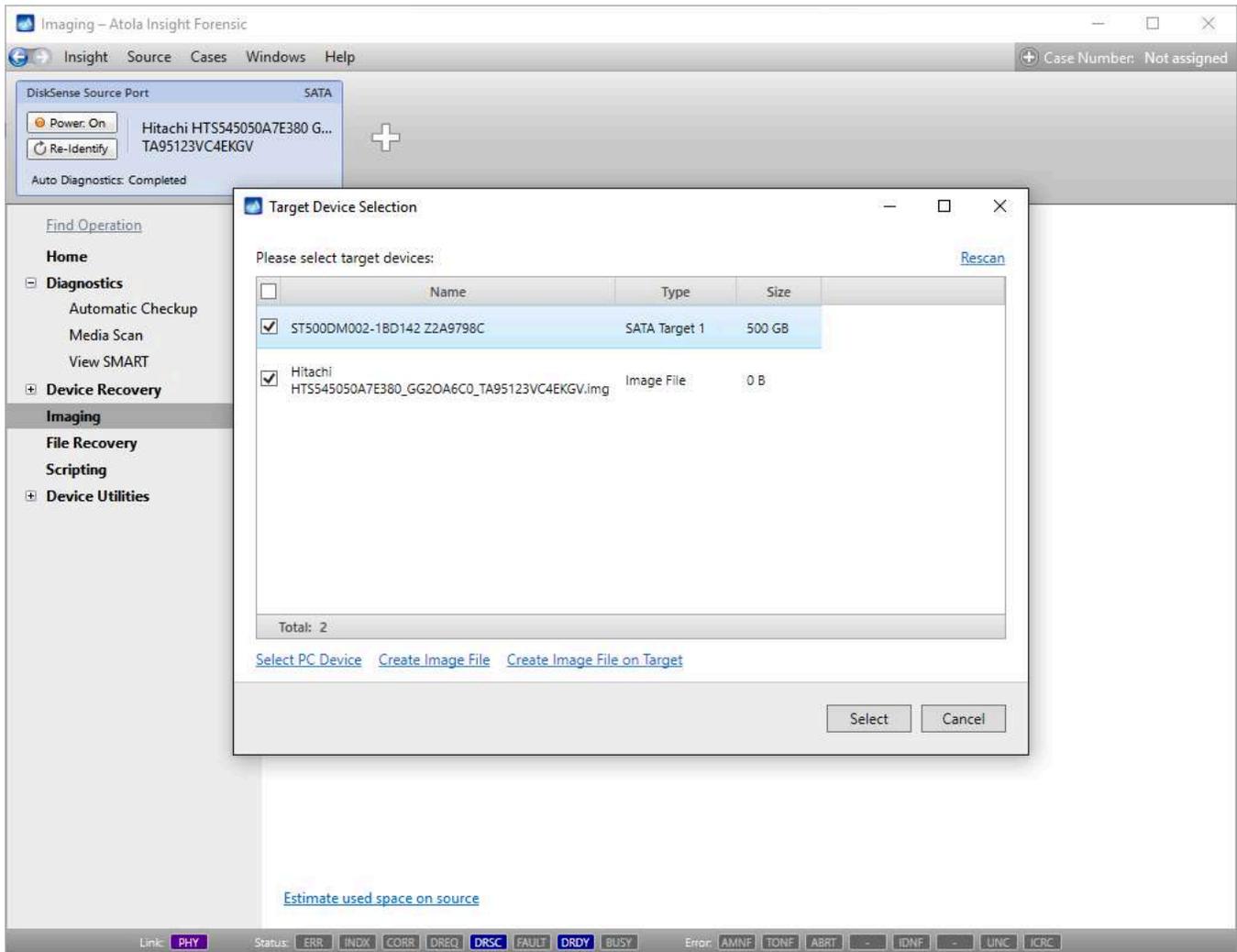
## Step 4. Select the imaging targets.

On the left, click **Imaging** and then **Create New Session**. You will be asked to select the imaging targets, including the following:

- Devices plugged into SATA/USB target ports of the DiskSense system
- Image files

Let us take advantage of imaging into two targets at the same time: SATA target drive and image file.

Click **Create Image File** and then confirm a selected filename. Then select the SATA Target 1 device. In the end, you will get a screen like this:

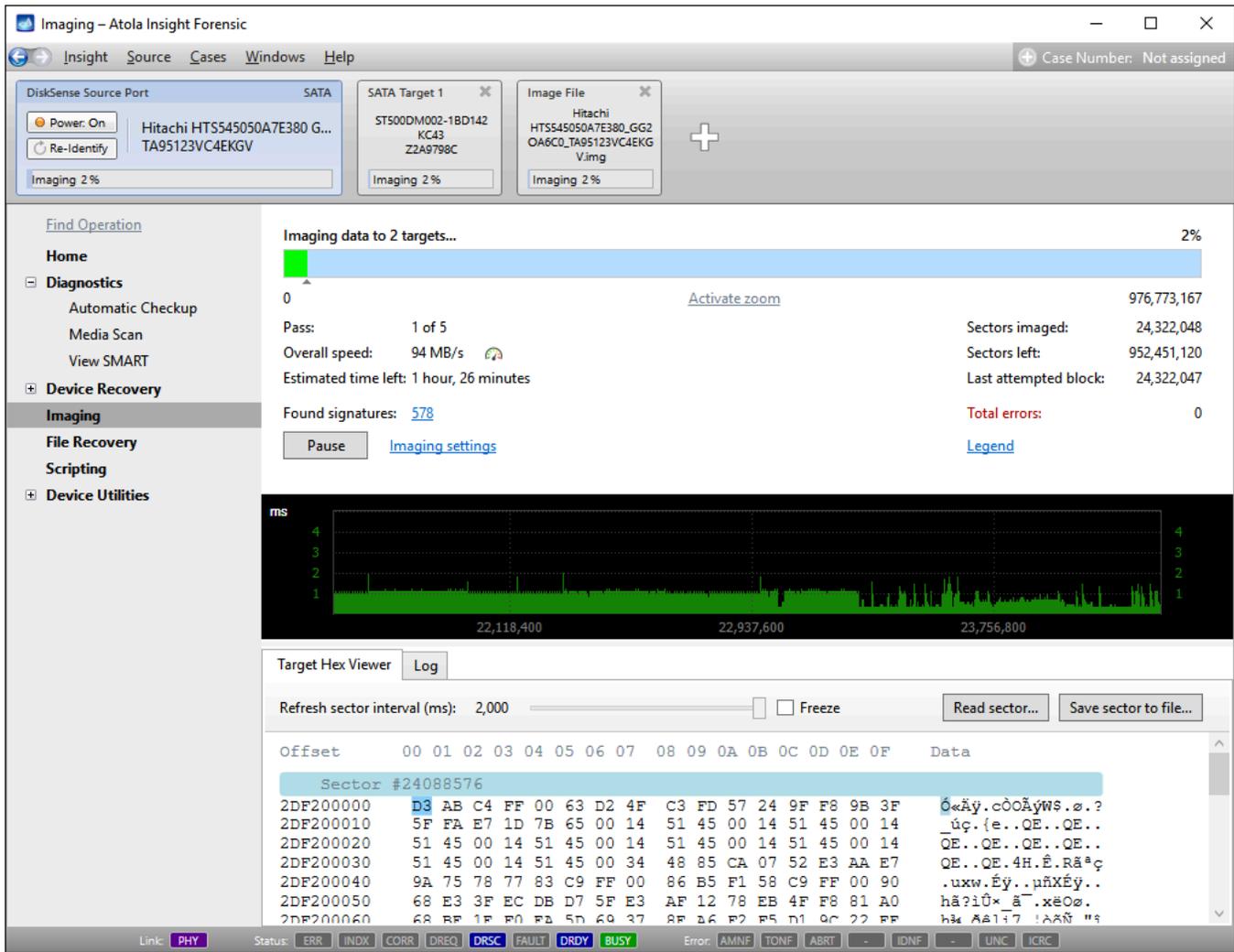


Click the **Select** button to confirm.

## Step 5. Start imaging.

Imaging includes a wide variety of settings for tuning the process. Sometimes it is helpful when dealing with severely damaged evidence drives. However, the default imaging preset works great in most cases.

Here is just one button to click, **Start Imaging**, to get the imaging process running.



## Bonus: Screencasts

Congratulations! You read the quickstart up to this section, and we have an award for you! :-). Here are a number of screencasts explaining specific features of Atola Insight Forensic.

- [Download or watch in high-resolution on Dropbox](#)
- [Watch on Youtube](#)

## Introduction

Atola Insight Forensic is a fast forensic imager with the capacity to perform 3 simultaneous imaging sessions on a wide range of media.

It also offers complex yet highly automated data recovery functions on failing storage devices and provides utilities for accessing hard drives at the lowest level. Its sophisticated software is wrapped in a simple and effective user interface.

Designed for use both in the lab and in the field, Insight is developed by a team of industry renowned data recovery engineers in collaboration with law enforcement agencies and forensic experts from around the globe.

## Atola Insight Forensic system includes:

- Insight Forensic software that runs on Windows PC
- [DiskSense 2 hardware unit](#) - released in July 2021
- Hardware [extensions](#) (optional)

We stand behind our product. If the hardware unit malfunctions, it's covered by our [Lifetime warranty](#) for as long as your subscription is active.

The subscription includes [2-3 software updates in a year](#).

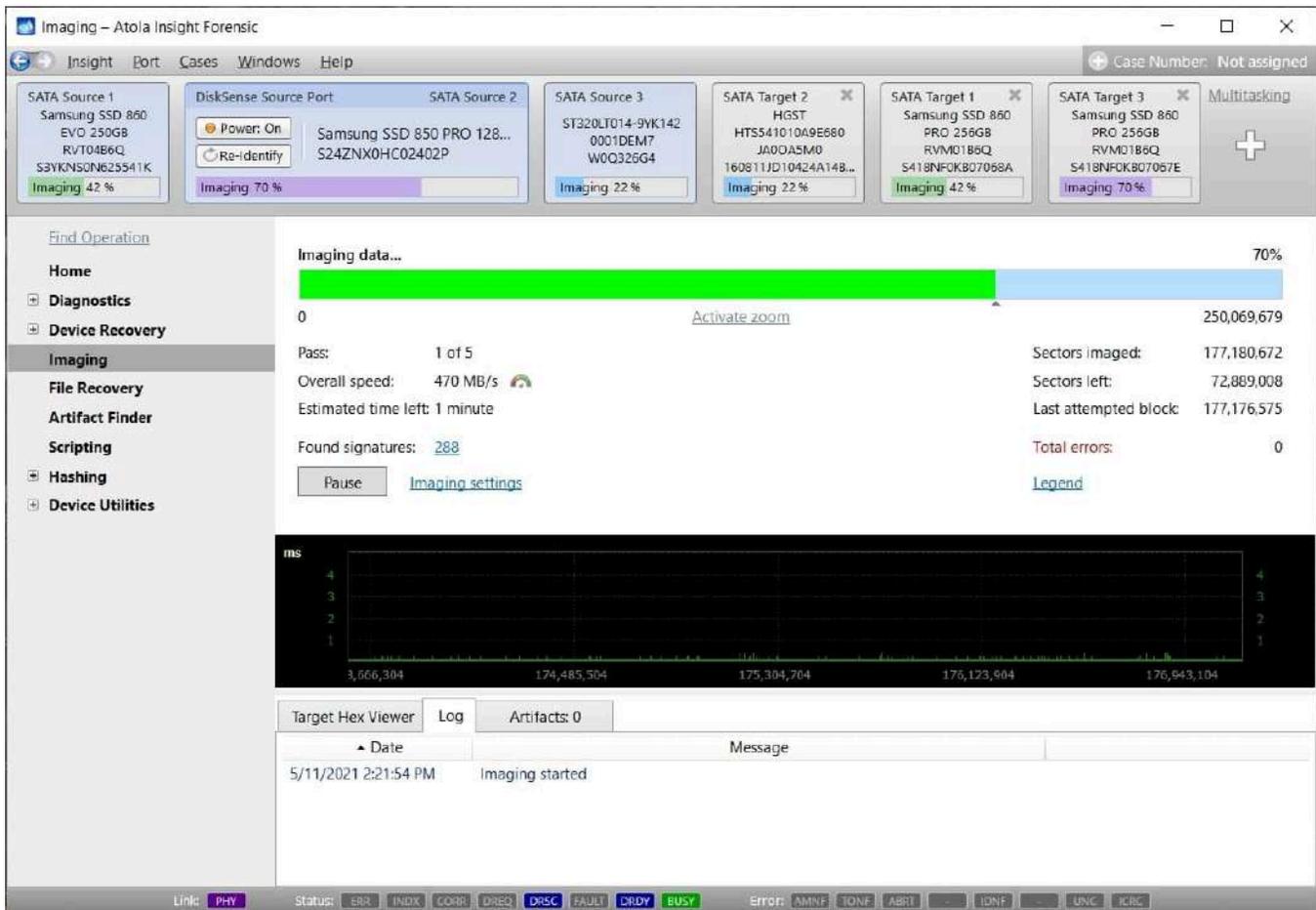
## Parallel imaging

Atola Insight is equipped with [server-grade motherboard and CPU](#) to sustain multiple imaging sessions at the top native speeds of the evidence drives, whether in good or bad condition.



[3D view](#)

- 3 simultaneous imaging sessions + [multitasking](#)
- 2 built-in 10Gb Ethernet ports
- Imaging session speed [up to 500 MB/s](#)
- E01, AFF4 or Raw target images created in the network or on target drives
- Up to [3 targets](#) per imaging session
- Support of SATA, IDE, USB drives
- Via [extensions](#): SAS, M.2 NVMe and PCIe AHCI SSDs, Apple PCIe (2013-2015)
- Built-in hardware write blocker for all source ports
- Remote image acquisition via iSCSI



## Damaged drive support

All features are designed to support damaged media. In cases where other imagers stall or abort on media errors, Atola Insight can acquire a usable image. Types of damage supported: degraded or damaged heads, scratches on platters, logical errors, freezing drives, old drives with worn-out magnetic layer.

- In-depth [automated drive diagnostics](#)
- [Multipass imaging](#) of damaged drives
- Automated imaging of [freezing media](#)
- [Bad sector recovery](#)
- [Segmented hashing](#) for bad drive's image verification
- HDD current monitoring for continuous diagnosis

## Forensic feature set

Forensic data recovery specialists will take advantage of the low-level features listed below.

- Unknown [ATA password extraction](#)
- [Locate sectors](#) - detect which files and partitions they belong to specified drive sectors
- On-the-fly sector-level [Artifact finder](#) based on Intel Hyperscan engine
- Hash calculation (linear and segmented): MD5, SHA1, SHA224, SHA256, SHA384, SHA512
- Wiping methods including DoD 5220.22-M, Secure Erase, NIST 800-88, Pattern Erase
- [Forensic file recovery](#) for NTFS, APFS (with encrypted volumes), XFS, ext4/3/2, exFAT, Btrfs, HFS/HFS+, FAT32, FAT16

The screenshot displays the Atola Insight Forensic software interface. At the top, there are navigation tabs for Insight, Port, Cases, Windows, and Help. A case number is shown as 'Not assigned'. Below this, there are four drive panels: 'DiskSense Source Port' (Samsung SSD 860 PRO 256GB, 93% imaged), 'SATA Source 2' (Samsung SSD 860 EVO 250GB, completed), 'SATA Source 3' (Samsung SSD 850 PRO 128GB, completed), and 'SATA Target 1' (Samsung SSD 860 EVO 250GB, 93% imaged). A 'Multitasking' button is visible.

The main area shows 'Imaging data...' with a progress bar at 93% and a total size of 500,118,191. It also displays 'Pass: 1 of 5', 'Overall speed: 300 MB/s', and 'Estimated time left: 57 seconds'. A 'Found signatures: 201813' is shown with a 'Pause' button and a link to 'Imaging settings'. On the right, statistics include 'Sectors imaged: 466,354,176', 'Sectors left: 33,764,016', 'Last attempted block: 470,354,175', and 'Total errors: 4'. A 'Legend' link is also present.

Below the progress bar is a 'ms' graph showing a flat line at 1ms across three data points: 468,011,264, 468,830,464, and 469,649,664. Below the graph is a 'Target Hex Viewer' and a 'Log' section showing 'Artifacts: 4.6M'.

The artifact search results are displayed in a donut chart and a list:

Artifact Type	Count
Credit cards	170
Emails	1,476,269
GPS (Exif)	0
Keywords	345,083
IP	22,486
MAC	685
Phone numbers	195
Regular expressions	1,193,884
URL	1,579,315

At the bottom, there is a status bar with 'Link: PHY', 'Status: ERR, INDX, CORR, DREQ, DRSC, FAULT, DRDY, BUSY', and 'Error: AMNF, TONF, ABRF, IDNF, UNC, ICRC'.

- [Case management system](#) automatically generates detailed reports
- Comparison of 1 drive against 3 drives or images
- Detection and lifting of [HPA/AMA/DCO restricted areas](#)
- SSD Trim

It is the only forensic hardware tool in the world with unknown ATA password removal, Locate sectors, and Artifact search in the course of imaging.

Other features are helpful for to prepare drives for image acquisition, analysis, testing, or other specific tasks.

# Workflow

## 1. Drive diagnostics

Atola imagers are the only products in both forensic and data recovery industries with the ability to automatically and accurately evaluate a hard drive's health and pinpoint specific problems. Atola Insight automatically diagnoses the drive's PCB, heads, media surface, firmware, and partitions, assesses imaging time, and creates a detailed report. The [Diagnostics module](#) helps you take informed decisions when getting down to imaging.

## 2. ATA password removal

Atola Insight [automatically removes ATA passwords](#) from hard drives in just 2 minutes. This sophisticated feature is executed with one click of a button. Whenever possible, the extracted password is displayed upon its removal.

## 3. Evidence drive imaging

Retrieving every fragment of data from a drive is a crucial to a [forensically sound data acquisition](#). Atola Insight's imaging system allows completely customizing imaging process to handle even damaged or unstable media.

It includes [selective head imaging](#), which enables an individual imaging approach to each one based on the status of specific heads as identified by the Diagnostics module.

Not only does the imaging system cope with damaged drives, but also it runs multi-threaded sector-level analysis in the course of image acquisition:

- artifact search
- file signature detection
- entropy calculation

## 4. Forensic file recovery

Insight's [file recovery module](#) is simple, intuitive, and effective. It integrates seamlessly with the imaging functionality and the Case Management system to retrieve data effectively.

Sector-level analysis with [Artifact Finder](#) and [Locate Sectors](#) helps find forensic artifacts in unallocated and hidden spaces that you could miss.

## Atola Insight Forensic workflow

Atola Insight Forensic covers all phases of the data acquisition process:

1. [Media diagnosis](#)

2. [Media recovery](#) (if needed)
3. [Image creation](#)
4. [File recovery](#)

## 1. Media diagnosis

Whenever you start working on a hard drive, the very first thing we recommend to do is to find out if the drive is damaged in any way, and if so, what is the extent of the damage.

The tool comes with fully automated hard drive diagnosis module. It diagnoses all hard drive components:

- 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 the DiskSense unit.

After diagnostics finishes, the tool will prepare a report and let you know the exact issue with the drive; it will also suggest the next step to be able to retrieve the data.

## 2. Media recovery

Atola Insight Forensic can recover and/or remove unknown HDD passwords (also known as ATA-passwords). For most hard drives the unlocking process is fully automated. Some hard drives (for example, latest 2.5-inch Hitachi hard drives) require a degree of manual interference. Operator can choose whether to display the password or just remove it and unlock the drive. Both security levels (High or Maximum) are supported.

To get the list of the hard drives currently supported by automatic password recovery routine, see [Supported drives](#).

## Manual firmware recovery

If there is firmware damage that cannot be fixed automatically, you will have to proceed with manual firmware recovery procedure. Generally speaking, firmware recovery process includes of the following steps:

1. Full firmware backup
2. Diagnosis
3. Recovery

Backup is a very important part of the process. Make sure you have full firmware backup before you make any change to the firmware area.

Basic diagnostics of the firmware area is done during Automatic Diagnostics process (see [Automatic Diagnostics](#)). More in-depth diagnostics is done during firmware backup process, after which any firmware damage that may exist will become obvious, as damaged modules will have either "Read Failure" or "Bad Checksum" mark. Some of these damaged modules can be recovered by right-clicking them and selecting Recover (module will be re-generated and written to the drive). In some

rare cases, when Atola Insight Forensic cannot regenerate the module, you would have to copy it from a donor drive (you would need to locate a similar hard drive, save that module from that drive into a file, and then copy that file into the bad drive's firmware, replacing the damaged module).

Please note: if after the full firmware backup you find that there are many unreadable firmware modules (more than 10% of total number of modules), it might be a good indication that the head stack is malfunctioning. The best thing to do in this case is to **reconfirm** that the hard drive does not have a head damage before proceeding with firmware recovery attempt. Attempting firmware recovery on a hard drive with internal damage may result in an unrecoverable damage.

### 3. Image creation

Before you proceed with any file recovery attempt, it is very important that you have a sector-by-sector copy of the drive. This is done with the Imaging module available in the software.

For more details, see [Imaging](#).

### 4. File recovery

After you made a copy of the original hard drive, you can start recovering files. File Recovery engine is able to show status of each file in the file browser, such as what percentage of file was imaged without errors. There's also an ability to create lists of files specifying the status of each file. After creation, the list may be presented for a review.

To learn more, see [File Recovery](#).

## Package contents (DiskSense 2)

The DiskSense 2 package includes the following items:

[DiskSense 2 unit](#)



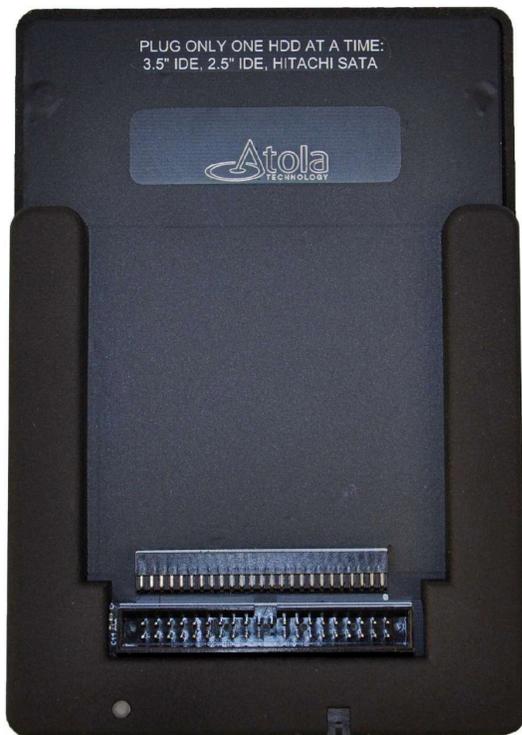
Power supply



7x SATA cables



IDE adapter



USB-C cable



IDE power cable



**IDE interface cable**

**Serial cable RS-232**



**Ethernet cat 7 cable**





USB3 to Ethernet adapter



Flash card reader



## DiskSense 2 Hardware Unit

DiskSense 2 is built to last using the highest quality components including server-grade motherboard and CPU. It is equipped with the fastest, most reliable interface connections available. The hardware is designed to handle damaged media. It includes a built-in oscilloscope for current monitoring and hardware write protection switch for source ports.

See how it compares with the previous version of the unit: [DiskSense 2 vs. DiskSense: What's new?](#)

To ensure reliability and efficiency of our hardware imagers, [we test them on hundreds of storage devices.](#)

# Ports & switches

6 Source ports equipped with Write protection switch:

- 3 SATA 3.0
- USB 3.2
- IDE (via [Atola adapter](#) included in the package)
- Extension slot (for SAS, Thunderbolt, Apple PCIe SSD and M.2 SSD [extension modules](#)):

4 Target ports:

- 3 SATA 3.0
- USB 3.2

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

Other ports: Serial RS232, IDE power, VGA, RS-232, DC IN 24V.

Supported hard drive interfaces: SATA I/II/III, SAS3 (12Gb), USB 2.0/3.0, IDE.

Interfaces supported via extension modules: SAS, NVMe, Apple PCIe, FireWire, Thunderbolt 2 and 3 (2016-2017 models).

Flash card support via card reader attached to any USB port.

## Indicators

Operation LEDs for all ports and write protection LED for sources ports.

IP address display.

Power switch LED.

## Physical / Environmental

- Aluminum case
- Dimensions: 7.9 x 7.9 x 2.6 in (190 x 190 x 63 mm)
- Weight: 3.3 lb (1.5 kg)
- Wide working temperature range: 0°C–50°C (32°F–122°F)
- Power consumption: 60 Watt average, 280 Watt peak
- Supply Voltage: 100 - 240 VAC, 50-60 Hz
- RoHS compliant

## Other specs

- Internal OS: Linux running a custom kernel
- Control interface: Atola Insight Forensic (Windows application)

# DiskSense 2: under the hood



[DiskSense 2 unit in 3D](#)

DiskSense 2 is essentially a small computer running a Linux OS. However, neither normal computer's BIOS, nor basic Linux kernel are suitable for handling of damaged drives because neither of them were designed to properly handle hard drive failures. We have invested significant R&D efforts to build a highly customized and fine-tuned Linux kernel that overcomes these limitations. Additionally, this kernel features:

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



DiskSense 2 also features our proprietary circuitry for ultimate hard drive's power control:

- Current sensor for in-depth drive diagnostics
- Automatic overcurrent and short-circuit protection
- Overvoltage protection

These features are a must when dealing with damaged drives.

For example, low-level control of the SATA, USB and IDE ports allows Atola Insight to deal with drives that do not properly initialize, have many bad sectors, or frequently freeze due to internal mechanical failures.

SATA PHY control allows resetting a frozen drive without a power cycle. This reduces the time while imaging, and the chance of further drive degradation and failure.

Current sensing allows Atola Insight to diagnose a failed drive even if it has electronic or mechanical damage. For more details on how this works, see [Diagnostics](#).

Overcurrent protection detects when a drive draws abnormal current and stops the attached device to prevent further damage.

Overvoltage protection circuit ensures that in the unlikely event of the DiskSense 2 unit malfunction, the attached drives are not damaged in any way.

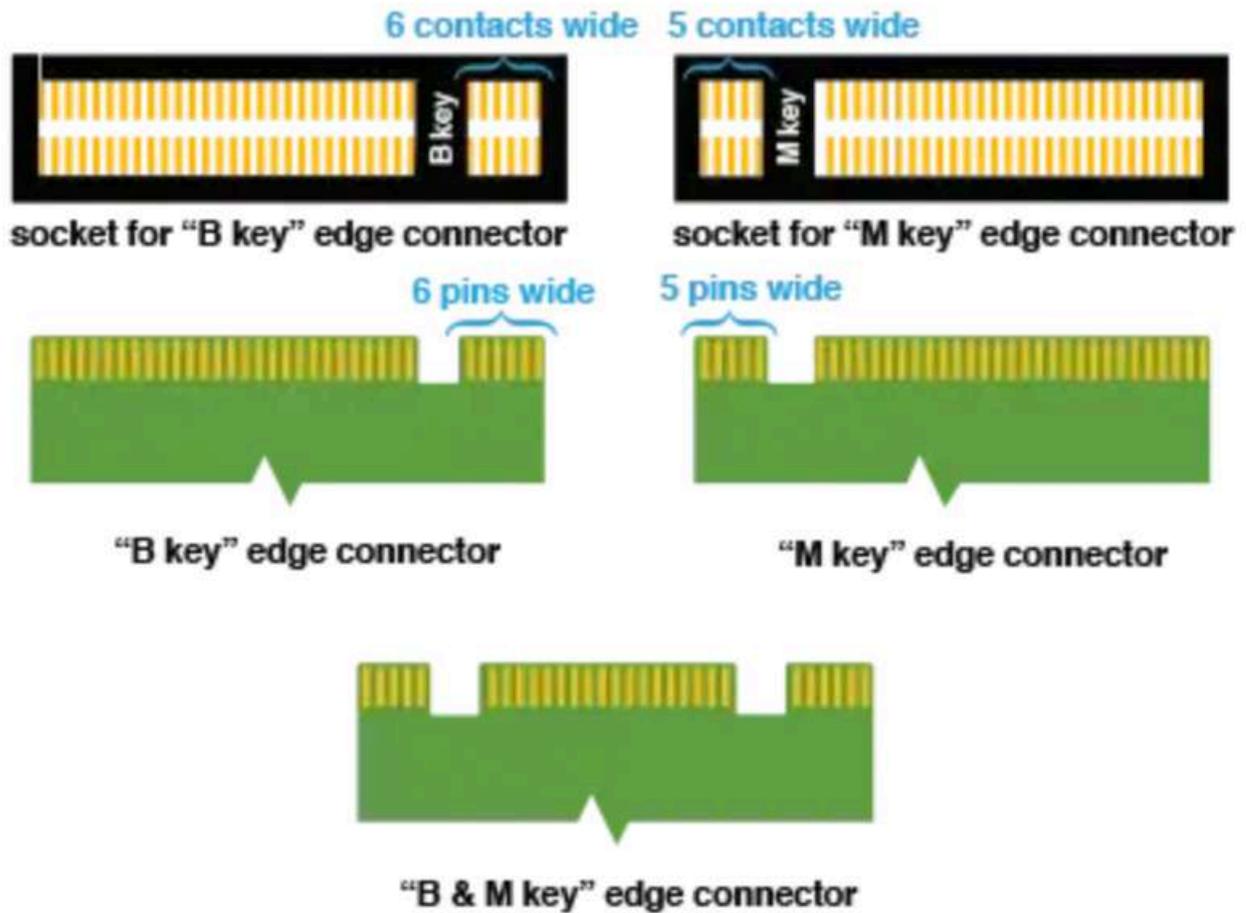
DiskSense 2 unit is fully controlled by Insight software via 10Gbe interface, therefore, you need no Linux experience to operate it.



## M.2 SSD extension module

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

Only B & M key and M key interface drives are supported by this extension module.



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

## Insight Forensic features supported for the M.2 SSD extension

Here are the differences in PCIe NVMe M.2, PCIe AHCI M.2, and SATA M.2 support in Atola Insight Forensic working with the DiskSense 2 hardware unit:

<b>All Insight operations</b>	Partial (see below)	✓	Partial (see below)
<b>Drive hotplug</b>	✓	✓	—
<b>Power management</b>	✓	✓	✓

Supported PCIe NVMe M.2 and PCIe AHCI M.2 features:

- Max read/write speed: 700 MB/s
- Write protection

- Imaging
- Diagnostics, media scan
- Damaged drive support
- Hash calculation and verification
- Wiping
- Device utilities:
  - disk editor
  - media recovery
  - SSD trim
  - compare (with a pattern, image file or drives)
  - and more

Drive hotplug is supported for PCIe NVMe M.2 and SATA M.2 drives, but not for PCIe AHCI M.2 drives.

## Plug and unplug the M.2 SSD extension module

DiskSense 2 has a PCI Express port on its back panel, which is labeled as *EXTENSION*. It is used to connect [Atola hardware extension modules](#) supported by Atola Insight Forensic software.



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

To connect the M.2 SSD extension module to the DiskSense 2 hardware unit, do the following:

1. Power off DiskSense 2.
2. Align the 3 holes on the extension module with the 3 screw holes on the DiskSense 2 back panel. Firmly plug the M.2 SSD extension module all the way into the Extension port and fasten the module with 3 screws.

3. Plug a PCIe NVMe M.2, PCIe AHCI M.2, or SATA M.2 drive into the extension and fasten the drive in place with the black plastic slider.
4. **Optional:** If you plan to work with SATA M.2 drives, connect the plugged extension to one of the SATA ports on DiskSense using a SATA cable. For details, see [Connect and identify a SATA M.2 drive](#) on this page.
5. Power on DiskSense 2.



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

1. Power off DiskSense 2.
2. Disconnect the SATA cable from the extension module (if you were using the cable).
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 DiskSense 2.

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

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

But there are different ways to connect PCIe NVMe M.2 and PCIe AHCI M.2 drives on one hand, and SATA M.2 drives on the other hand to DiskSense 2 using the M.2 SSD extension module.

The easiest way to tell apart NVMe M.2 and PCIe AHCI M.2 drives from SATA M.2 drives – when the extension is connected and DiskSense 2 is powered on – is to look at the LED indicator on the extension module, next to the words "When LED is on, plug SATA source port cable here":

- If the LED is off, the drive connected to the M.2 SSD extension module is either NVMe M.2 or PCIe AHCI M.2. See [Connect and identify an NVMe M.2 or AHCI M.2 drive](#).
- If the LED is on, the drive is SATA M.2. See [Connect and identify a SATA M.2 drive](#).

To define the type of a 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 NVMe M.2 or PCIe AHCI M.2 drive

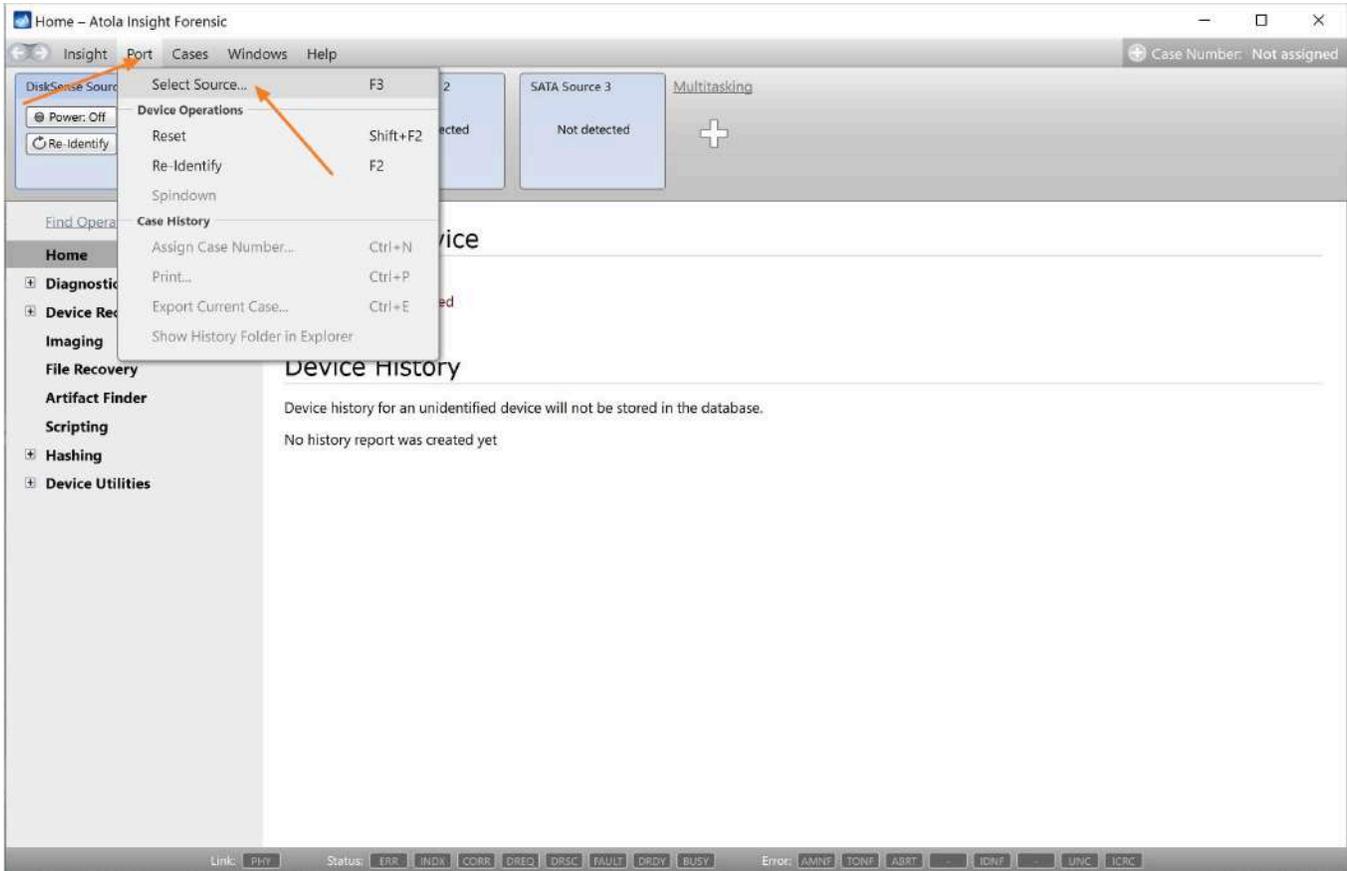
1. Power off the M.2 SSD extension using the SSD PWR button on the extension. LED power indicator on the extension turns off.



2. Plug a PCIe NVMe M.2 or a PCIe AHCI M.2 drive into the extension and fasten the drive in place with the black plastic slider.
3. Power the extension on by pressing the SSD PWR button. The LED power indicator on the extension is on.

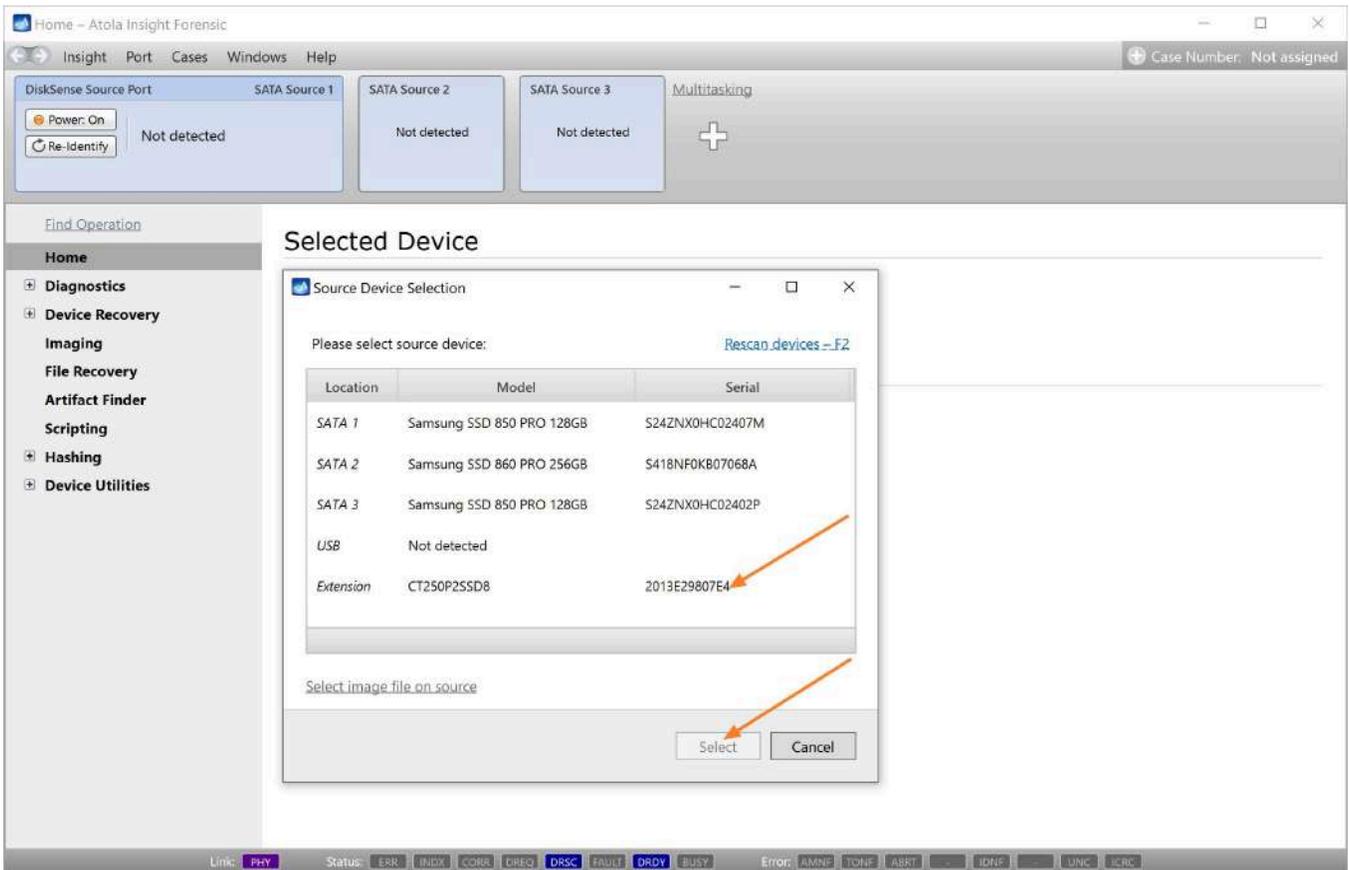


4. In Atola Insight Forensic, go to **Port > Select Source**.

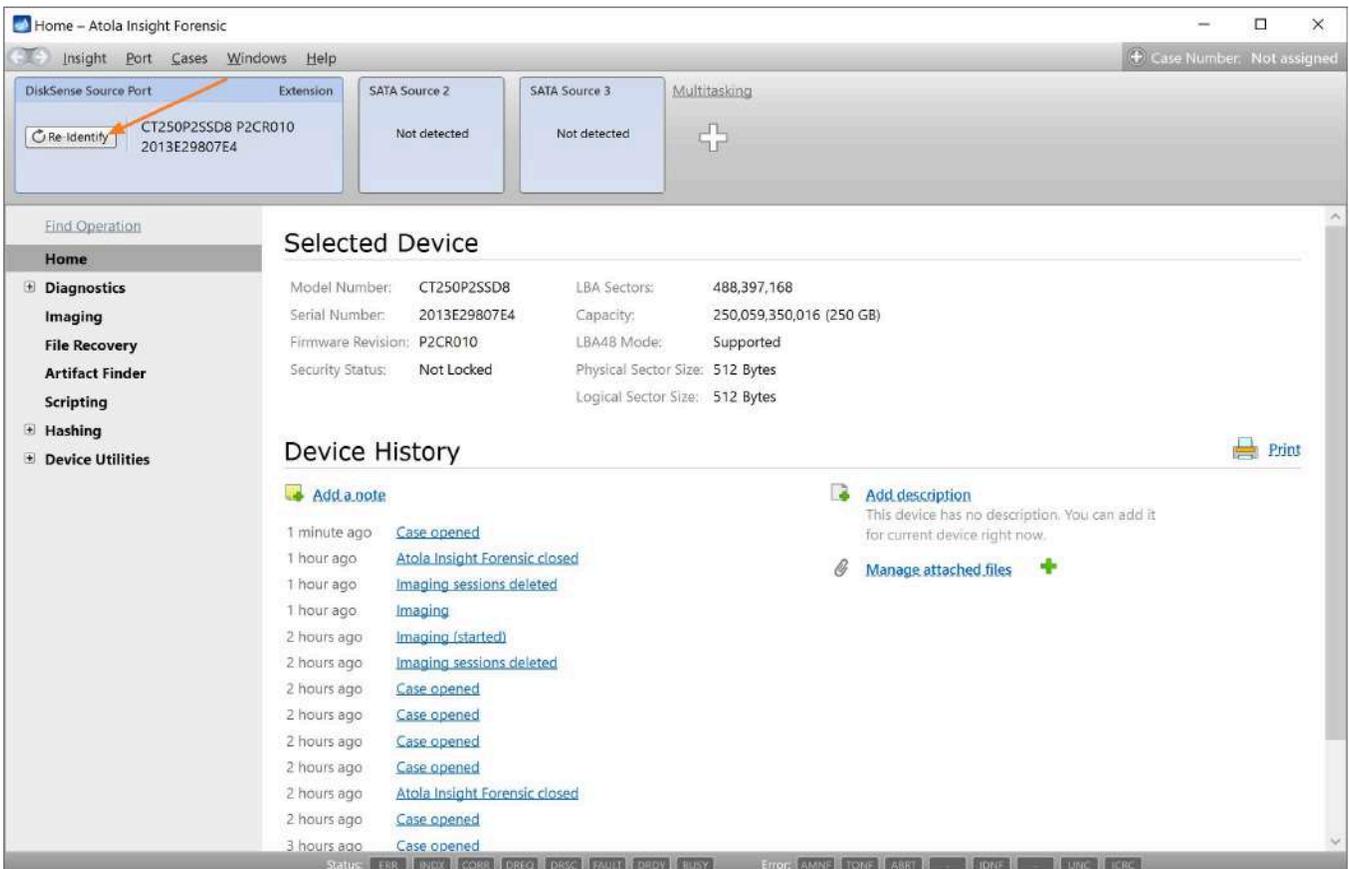


5. In the **Source device selection** window, choose the drive connected to the Extension port, and then click **Select**.

Non-SATA sources can only be opened in the SATA Source 1 port. If you have another device attached to the SATA Source 1 port, the system may suggest powering it off.



6. In the Insight interface, click **Re-identify** to initialize your source drive.



Once the drive is connected and identified, you can proceed to [diagnostics](#), [imaging](#), [hashing](#) or other operations.

## Work with several NVMe M.2 drives in a row

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

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

To replace or remove an NVMe M.2 drive, make sure to power off the M.2 SSD extension module by pressing the SSD PWR button.

## Connect and identify a SATA M.2 drive

When you plug a SATA M.2 drive into the M.2 SSD extension module, DiskSense 2 will light up the LED indicator on the module, next to the words *"When LED is on, plug SATA source port cable here"*.

To connect a SATA M.2 drive to DiskSense 2, do the following steps:

1. Using the SATA cable, connect the M.2 SSD extension module to one of the SATA ports on DiskSense 2.
2. In Atola Insight Forensic software, power off SATA Source port.
3. Plug a SATA M.2 drive into the extension and fasten it in place with the black plastic slider.
4. In Atola Insight Forensic, power on SATA Source port.



## Work with several SATA M.2 drives in a row

For SATA M.2, drive hotplug is supported. You can connect and replace SATA M.2 drives without turning DiskSense 2 off and on again.

For safety reasons, before replacing SATA M.2 drives, the port must be powered off by clicking the Power button on the source port in the Atola Insight Forensic interface.

To define if a particular M.2 drive is SATA type or not, check the markings on it or refer to the manufacturer's specifications.

Also, if your drive belongs to SATA type, DiskSense 2 will light up the LED indicator on the extension module, next to the words "*When LED is on, plug SATA source port cable here*".

## Connect a U.2 NVMe drive using adapter

To use a drive with U.2 interface, attach the drive to DiskSense 2 unit 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 the unit, 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 DiskSense 2 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.



## Apple PCIe SSD extension module

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

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

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

## Insight Forensic features supported for Apple PCIe SSD extension

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

- Imaging at 550 MB/s (33 GB/min)
- Write protection
- Diagnostics, media scan
- Damaged drive support
- Hash calculation and verification
- Wiping
- Device utilities:
  - disk editor
  - media recovery
  - SSD trim
  - compare (with a pattern, image file or drives)
  - and more

# Plug and unplug the Apple PCIe SSD extension module

DiskSense 2 has a PCI Express port on its back panel, which is labeled as *EXTENSION*. It is used to connect [Atola hardware extension modules](#) supported by Atola Insight Forensic software.



The DiskSense 2 hardware unit must be powered off before installing the extension module.

To connect the Apple PCIe SSD extension module to DiskSense 2, do the following:

1. Power off DiskSense 2.
2. Align the screw on the extension module and the top screw hole on the DiskSense 2 back panel. Firmly plug the Apple PCIe SSD extension module all the way into the Extension port and fasten the module with a screw.
3. Plug Apple PCIe SSD drive into the extension and fasten the drive in place with the plastic latch.
4. Power on DiskSense 2.

**Important:** Drive hotplug is not supported yet. DiskSense 2 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 DiskSense 2.
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 fasten the module with a screw.
4. Power on DiskSense 2.

## SAS extension module

Connect SAS drives to Atola DiskSense 2 using the SAS extension module. The main characteristics of the SAS extension module are:

- SAS interface: 6 Gbit/s.
- Max read/write speed: 500 MB/s.
- Imaging at 800 MB/s
- Hotplug for SAS drives is supported.



## Insight Forensic features supported for SAS extension

Atola Insight Forensic supports most operations for a SAS drive plugged into DiskSense 2:

- Write protection
- Current sensing, short circuit and overvoltage protection
- Damaged drive support
- Diagnostics, media scan
- Hash calculation and verification
- Wiping
- Device utilities:
  - disk editor
  - file recovery
  - compare (with a pattern, image file or drives)
  - and more

There are a few functions that are not available for SAS drives:

- Host Protected Area (HPA)
- Device Configuration Overlay (DCO)
- Security features
- SSD Trim
- Firmware recovery

## Plug and unplug the SAS extension module

DiskSense 2 has a PCI Express port on its back panel, which is labeled as *EXTENSION*. It is used to connect [Atola hardware extension modules](#) supported by Atola Insight Forensic software.



The DiskSense 2 hardware unit must be powered off before installing the extension module.

To connect the SAS extension module to the DiskSense 2 hardware unit, do the following:

1. Power off DiskSense 2.
2. Align 3 holes on the extension module and 3 screw holes on the DiskSense 2 back panel. Firmly plug the SAS extension module all the way into the Extension port and fix the module with 3 screws.
3. Power on DiskSense 2.

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

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

# Connect a SAS drive to DiskSense 2 using SAS extension module

1. Plug the mini SAS connector into the extension module.
2. Plug the molex power connector into the SATA 1 source power socket.
3. Plug the SAS connector into the drive.



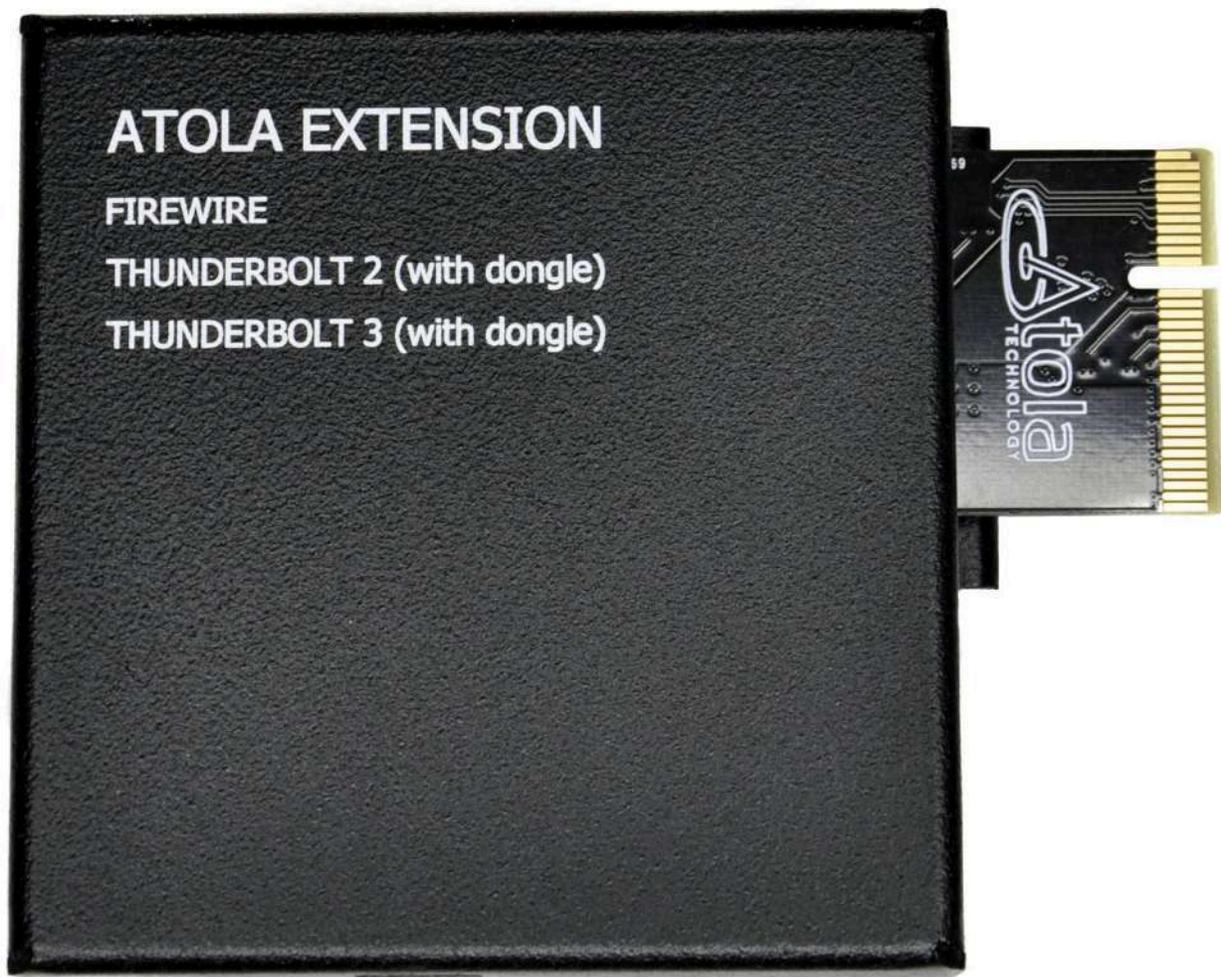
Hotplug for SAS drives is supported. You can connect and disconnect SAS drives without turning DiskSense 2 off and on again.

## Thunderbolt extension module

Thunderbolt extension enables DiskSense 2 to work on MacBooks with the following interfaces:

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

No SSD removal is necessary, the extension allows connecting DiskSense 2 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)



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

## Insight Forensic features supported for Thunderbolt extension

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

- Imaging
- Hash calculation and verification
- Write protection
- Media scan
- Device utilities:
  - file recovery
  - compare (with a pattern, image file or drives)
  - and more

## Plug and unplug the Thunderbolt extension module

DiskSense 2 has a PCI Express port on its back panel, which is labeled as *EXTENSION*. It is used to connect [Atola hardware extension modules](#) supported by Atola Insight Forensic software.



The DiskSense 2 hardware unit must be powered off before installing the extension module.

To connect the Thunderbolt extension module to the DiskSense 2 hardware unit, do the following:

1. Power off DiskSense 2.
2. Align the screw on the extension module with the top screw hole on the DiskSense 2 back panel. Firmly plug the Thunderbolt extension module all the way into the Extension port and fasten the module with a screw.
3. Power on DiskSense 2.

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

1. Power off DiskSense.
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 fasten the module with a screw.
4. Power on DiskSense.

## Connect MacBook using Thunderbolt extension module

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



Then do the following steps:

1. Turn off both MacBook and DiskSense 2.
2. Plug the Thunderbolt extension module into the Extension port and fasten the module with a screw.
3. Connect MacBook to the DiskSense 2 unit with the help of Thunderbolt extension and the FireWire cable. Use the adapters (included) to connect to the MacBooks with Thunderbolt 2 or Thunderbolt 3 interface.



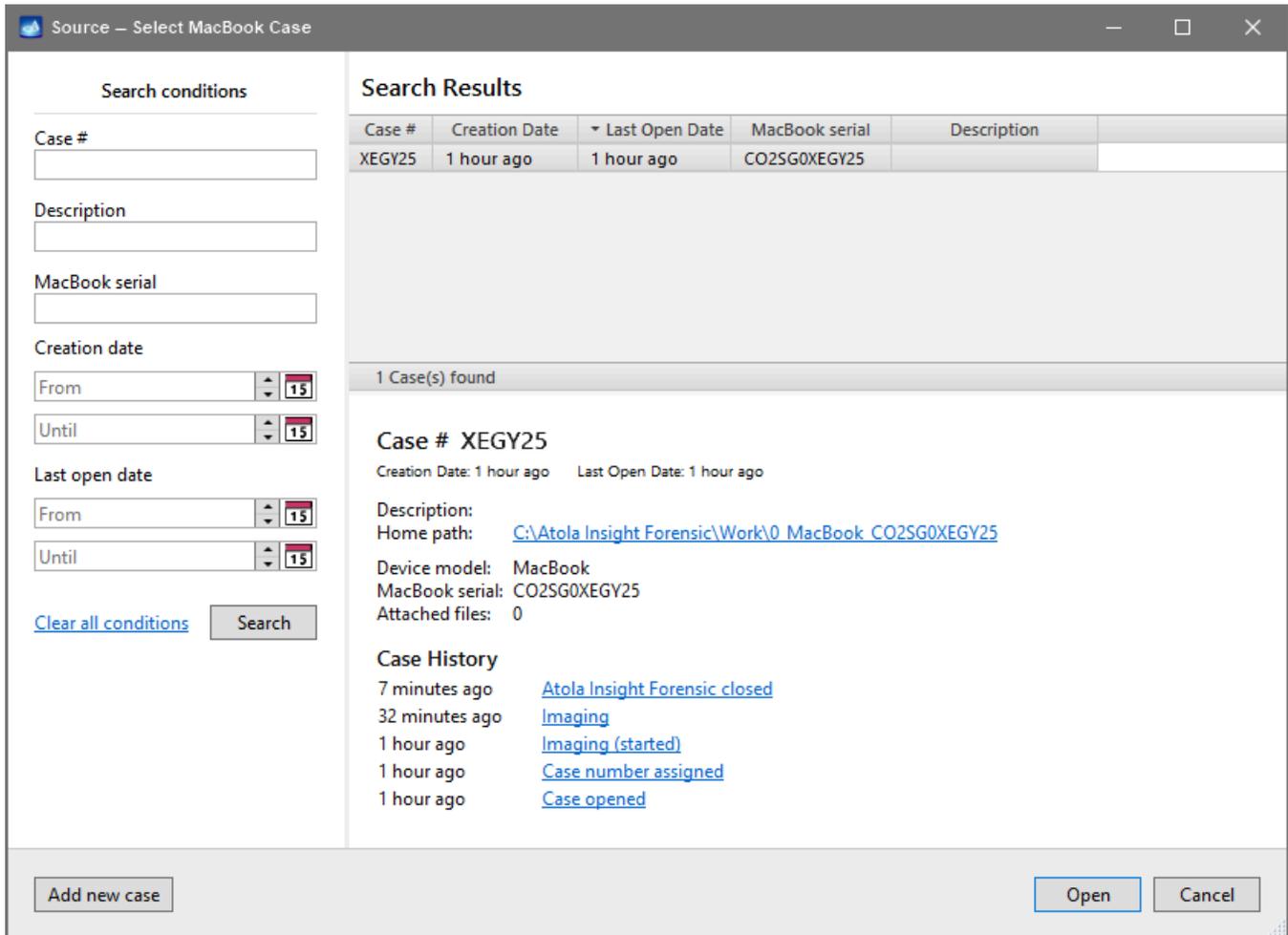
4. Boot MacBook in Target Disk Mode. To do that, start it up while holding down the T key. You should see a Firewire or Thunderbolt icon displayed on the screen, indicating that Target Disk Mode is on.
5. Power on the DiskSense 2 hardware unit.
6. Launch Atola Insight Forensic on your computer.
7. In the pop-up window, select **Identify device**.
8. In the **Source – Select MacBook Case** window, click **Add new case**.

The screenshot shows a software window titled "Source – Select MacBook Case". The window is split into two panes. The left pane, titled "Search conditions", contains several search criteria: "Case #" (text input), "Description" (text input), "MacBook serial" (text input), "Creation date" (with "From" and "Until" date pickers), and "Last open date" (with "From" and "Until" date pickers). Below these are a "Clear all conditions" link and a "Search" button. The right pane, titled "Search Results", is currently empty and shows "0 Case(s) found". At the bottom of the window, there are three buttons: "Add new case" on the left, and "Open" and "Cancel" on the right.

### Select MacBook Case

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

When the MacBook is connected to Insight next time, you can simply select the appropriate case from the table.



**Opening an existing MacBook case from the Select MacBook Case window.**

## First use guide for Atola DiskSense 2

Here's how to install Atola Insight Forensic software and connect Atola DiskSense 2 hardware unit for the first time to start imaging evidence devices.

### Step 1. Download and install Atola Insight Forensic software

Atola Insight Forensic software requires a PC with Windows 10/11 (64-bit). Check [minimum and optimal hardware requirements](#) before installing the software.

1. Go to the [Atola Insight Forensic Downloads page](#) and download the latest version of the full installation package.
2. Run the installer and proceed with setup steps.  
If Windows warns you about an unrecognized app, click Run anyway and allow the app to make changes to your device.

3. **Optional:** If you don't have Microsoft .NET and Microsoft SQL Server on your computer, the installer prompts to install these components.
4. After the installation is finished, reboot your computer. Don't launch Atola Insight Forensic software yet.

## Step 2. Configure your network

DiskSense 2 can be configured to use either a static or dynamic IP address.

- **Direct connection:** If you plan to connect the DiskSense 2 hardware unit directly to your computer, we recommend [using the static IP address](#).
- **Using router:** If you plan to connect the DiskSense 2 hardware unit through a network router or switch, we recommend [using the dynamic IP address](#).

If your computer has no Ethernet port, you can use the USB-to-Ethernet adapter included in the package. Connect it to your computer before configuring a network.

### Use 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 188.  
Default IP addresses of the DiskSense 2 unit are 10.0.0.188 and 192.168.0.188. The IP address of your PC's Ethernet card must be different from that of the DiskSense 2 unit.
  - **Network mask:** 255.0.0.0.  
If your PC and the DiskSense 2 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**.

To use a static IP address, on **Step 3** connect a network cable to the **ETH 1** port of DiskSense 2.

### Use a dynamic IP address

The ETH2 port of DiskSense 2 is set to automatically receive an IP address from your network router (DHCP server).

If you want the unit to use a dynamic IP address, on **Step 3** connect a network cable to the **ETH 2** port of DiskSense 2.

## Step 3. Connect DiskSense 2

1. Before setting up and connecting DiskSense 2, write down or take a photo of the **Device serial number**. It is located on the bottom of the DiskSense 2 unit. You will need the Device serial number on **Step 5** to activate the Atola Insight Forensic software.
2. Plug the power supply cable to the **DC IN** socket on the back of the DiskSense 2 hardware unit.
3. Connect an Ethernet cable to DiskSense 2:

- If you plan to use a **static** IP address, choose the **ETH1** port.
  - If you plan to use a **dynamic** IP address, choose the **ETH2** port.
4. Connect the other end of the Ethernet cable to your PC or router.

## Step 4. Power on DiskSense 2

1. Make sure that there are no USB devices attached to the DiskSense 2 hardware unit.
2. Using the PWR switch on the back panel of DiskSense 2, power on the unit.
3. Wait for the PWR LED on the back of the unit to stop blinking.
4. When booting is finished, the unit's IP address appears on the IP screen on its front panel.

## Step 5. Launch and activate Atola Insight Forensic software

To activate Atola Insight Forensic software, you need the **Device serial number** of the DiskSense 2 hardware unit. It is located on the bottom of the DiskSense 2 unit.

1. Launch Atola Insight Forensic.
2. To prevent blocking communication between the software and DiskSense 2 hardware unit, in your firewall and anti-malware, allow access for *insight.exe*.

There are three options to activate Atola Insight Forensic:

1. [Online activation](#). Choose this option if your computer has an internet connection.
2. [Offline activation](#). Choose this option if your computer does not have an internet connection, but you can use a USB drive.
3. [Offline activation by code](#). Choose this option if your computer does not have an internet connection and you cannot use USB or any other removable drive.

### Online activation

To activate Atola Insight Forensic online, you need to have an internet connection on your computer.

1. In the **Activation dialog**, choose **Online activation** and click **Continue**.
2. Fill out all fields in the **Activation form** and click **Continue**.
3. Atola Insight Forensic confirms that activation has been successfully completed. Click **Finish**.

### Offline activation

To activate Atola Insight Forensic offline, you need another PC with internet connection and a flash memory stick.

1. In the **Activation dialog**, choose **Offline activation** and click **Continue**.
2. Fill out all fields in the **Activation form** and click **Continue**.
3. Save the *Activation\*\*\*\*.aa* file to a USBstick.

4. Using another computer connected to the internet, go to [activation.atola.com](https://activation.atola.com).
5. Click **Choose File** to upload the *Activation\*\*\*\*.aa* file from the USB stick, enter your email and click **Submit**.
6. Atola sends you an email with an Activation response file: *Response\*\*\*\*.ar*. Save this file to your USB stick.
7. In the Insight **Activation dialog**, submit the *Response\*\*\*\*.ar* file from the USB stick and click **Continue**.
8. Atola Insight Forensic confirms that activation has been successfully completed. Click **Finish**.

## Offline activation by code

To activate Atola Insight Forensic offline by code, you need another device with internet connection (PC or mobile).

1. In the **Activation dialog**, choose **Offline activation by code** and click **Continue**.
2. Enter **Device serial number** located on the bottom of the DiskSense 2 unit and click **Continue**.
3. Save the following information from the Insight Activation dialog:
  - o Hasp ID
  - o Insight version
  - o Checksum
4. Using another device connected to the internet, go to the Atola licensing webpage: [activation.atola.com/ActivateByCode](https://activation.atola.com/ActivateByCode).
5. Fill out all the fields on the Atola licensing webpage, including:
  - o Device serial number (from the bottom of the unit).
  - o Hasp ID, Insight version, Checksum (from the Insight Activation dialog).
  - o Your email, phone number, and organization.
6. Click **Submit**. Atola licensing webpage generates an **Activation code** and also sends it to the email address you provided.
7. On your computer, go back to the Insight **Activation dialog**, enter your **Activation code** and click **Continue**.
8. Atola Insight Forensic confirms that activation has been successfully completed. Click **Finish**.

## Run Atola Insight Forensic on several computers

Activation details are stored in the DiskSense 2 unit itself. If you decide to install the Atola Insight Forensic software on another computer, there's no need to reactivate it.

It is permitted to install multiple copies of the software on many computers and use a centralized database for convenience. See [Network database setup](#).

---

## Change or reset an IP address of DiskSense 2

### Change an IP address

To change the IP address of the DiskSense 2 unit, choose one of the following:

- Run Atola Insight Forensic and go to **Insight > Modify DiskSense Unit IP**  
Or,
- Use DS Unit Update Tool, by running the *DSEthernetUpdate.exe* file located in your Atola Insight Forensic folder.

## Reset an IP address

1. Power on the DiskSense 2 hardware unit.
2. While the unit is booting, press and hold the small **IP RESET** button on its back side.
3. Still holding the **IP RESET** button, wait until the **PWR** LED stops blinking.

Now the unit has default IP addresses: *10.0.0.188* and *192.168.0.188*.

The reset procedure does not affect the ETH2 port, because its IP address is auto-assigned by your network router (DHCP server).

## 10Gb network connection

For saving time when imaging to a network folder, we recommend using a 10Gb Ethernet network.

## Extend subscription offline

Atola products come 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](#).

To extend your subscription for another period, you need to [buy](#) and then [reactivate](#) it. You can reactivate your subscription even in a network-free environment.

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.

## Buy subscription

There are two ways to order an Atola Insight Forensic subscription for another period:

- **From a sales representative:** the Atola sales rep or the reseller that sold you the unit. For contact information, see [Where to buy](#).
- **Online** on the [Subscriptions page](#) on the Atola website.

After you have purchased the subscription for another period, you need to **reactivate it**.

# Reactivate subscription

You can reactivate the subscription even if your computer does not have an internet connection. There are different options to reactivate a subscription offline, depending on how you buy it.

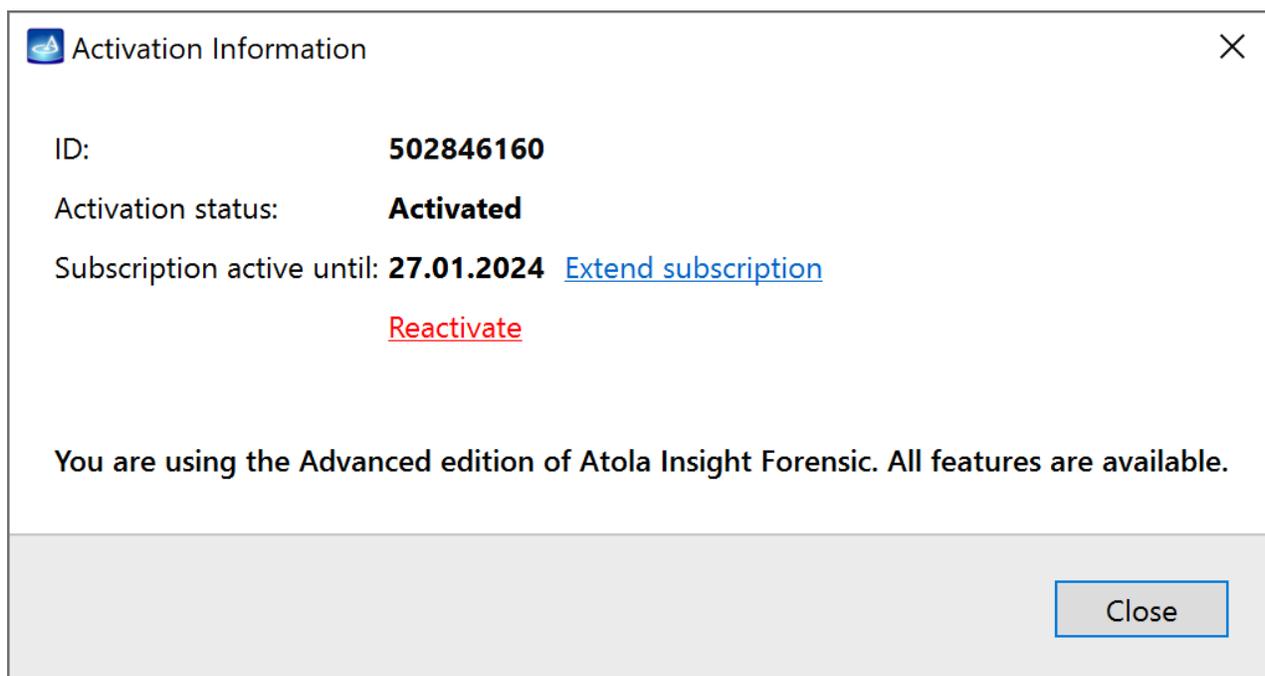
## Offline by code

You will need:

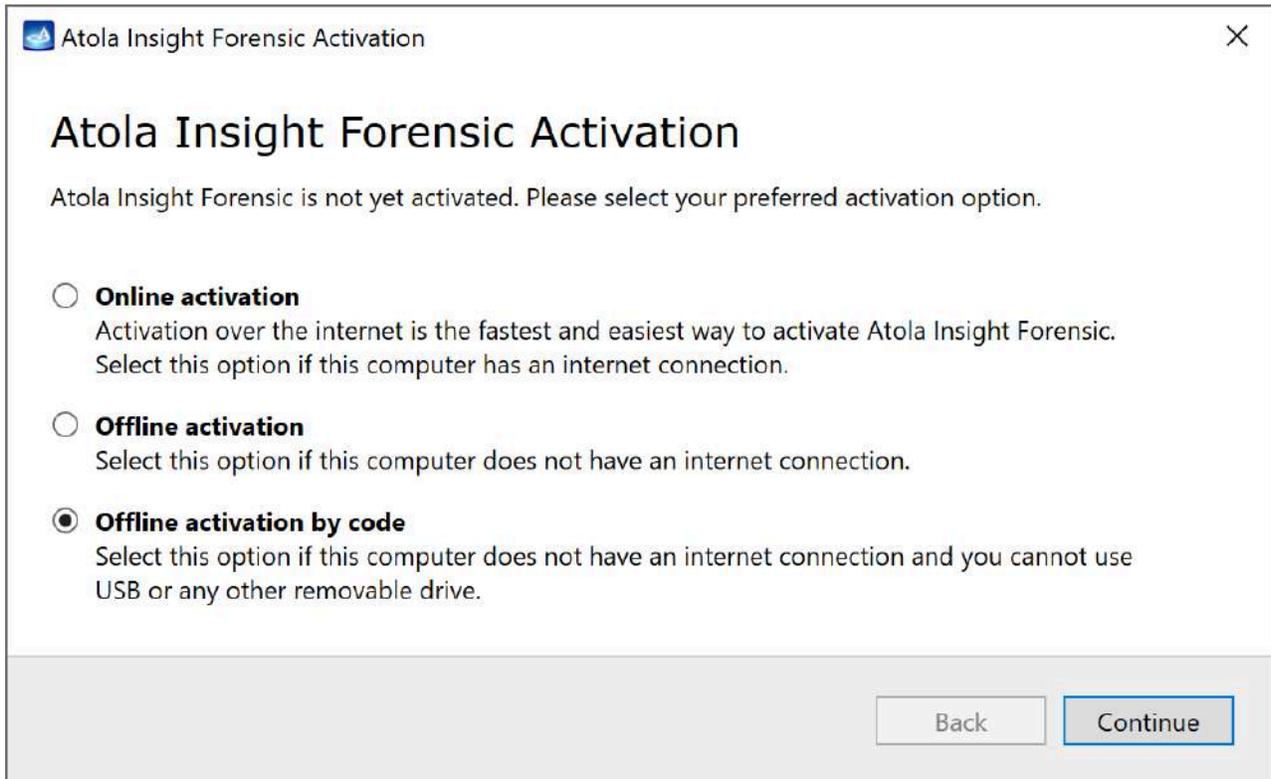
- another device with an internet connection (PC or mobile)
- the **Device serial number** located on the bottom of the DiskSense hardware unit

To activate Insight offline by code, do the following:

1. In Insight Forensic, open the **Help** menu and select **Activation status**.
2. Click the **Reactivate** link.



3. In the **Activation** dialog, choose **Offline activation by code** and click **Continue**.



4. Enter the **Device serial number** located on the bottom of the DiskSense unit and click **Continue**.
5. Save the following information from the Insight Activation dialog:
  - Hasp ID
  - Insight version
  - Checksum
6. Using another device connected to the internet, go to the Atola licensing webpage:  
[activation.atola.com/ActivateByCode](https://activation.atola.com/ActivateByCode).
7. Fill out all the fields on the Atola licensing webpage, including:
  - Device serial number (from the bottom of the unit)
  - Hasp ID, Insight version, Checksum (from the Insight Activation dialog)
  - Your email, phone number, and organization
8. Click **Submit**. The Atola licensing webpage generates an Activation code and also sends it to the email address you provided.
9. On your computer, go back to the Insight Activation dialog, enter your Activation code and click **Continue**.
10. Insight confirms that reactivation has been successfully completed. Click **Finish**.

## Offline with a USB flash drive

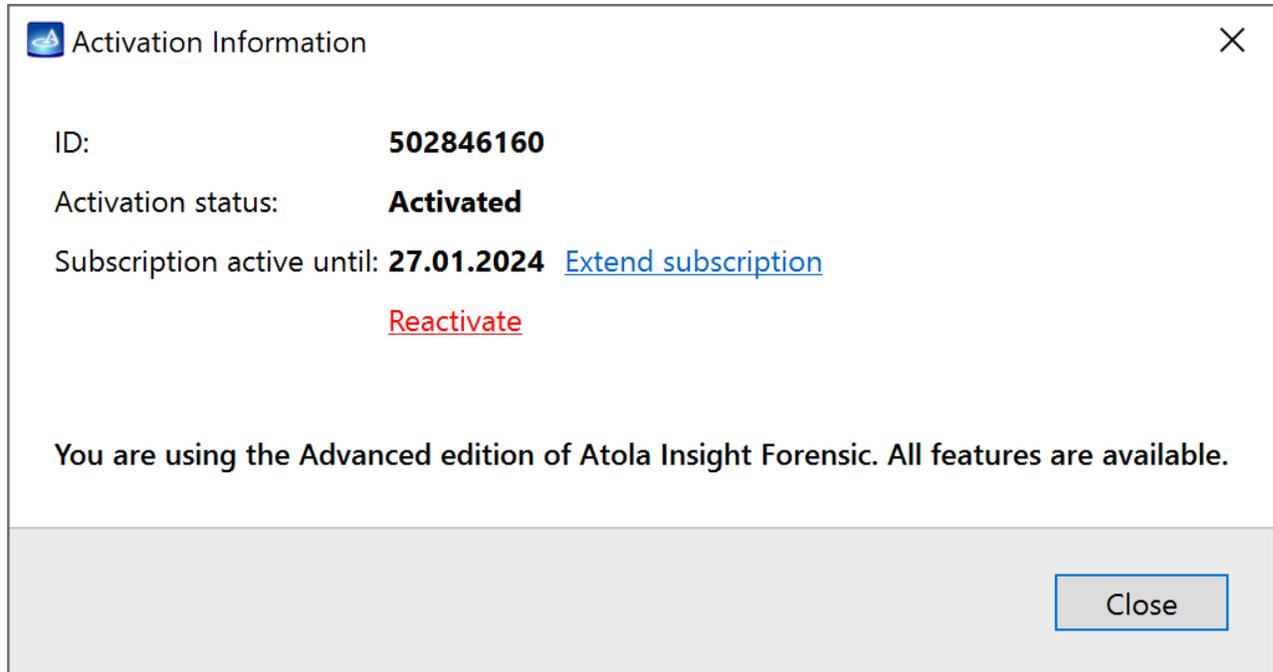
You will need:

- another device with an internet connection (PC or mobile)
- a USB flash drive
- the **Device serial number** located on the bottom of the DiskSense hardware unit

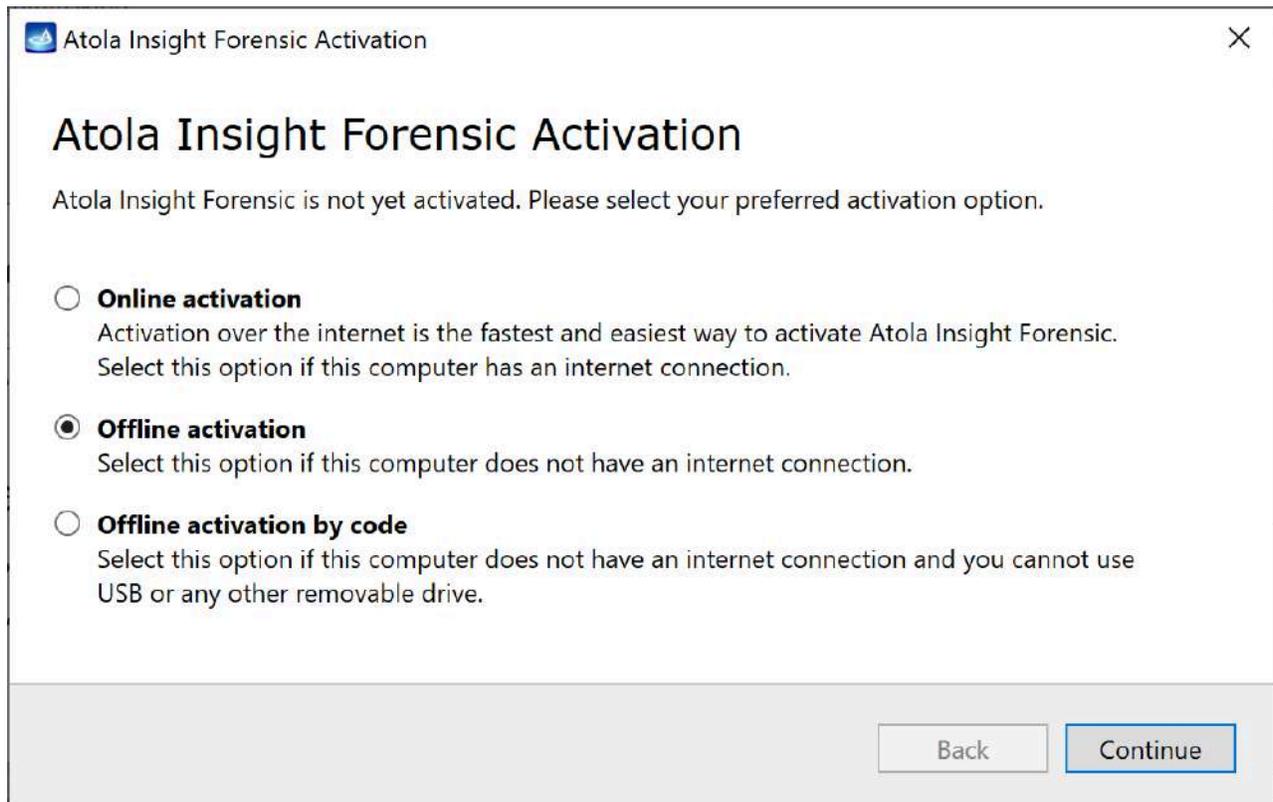
To activate Insight offline with a USB flash drive, do the following:

1. In Insight Forensic, open the **Help** menu and select **Activation status**.

2. Click the **Reactivate** link.

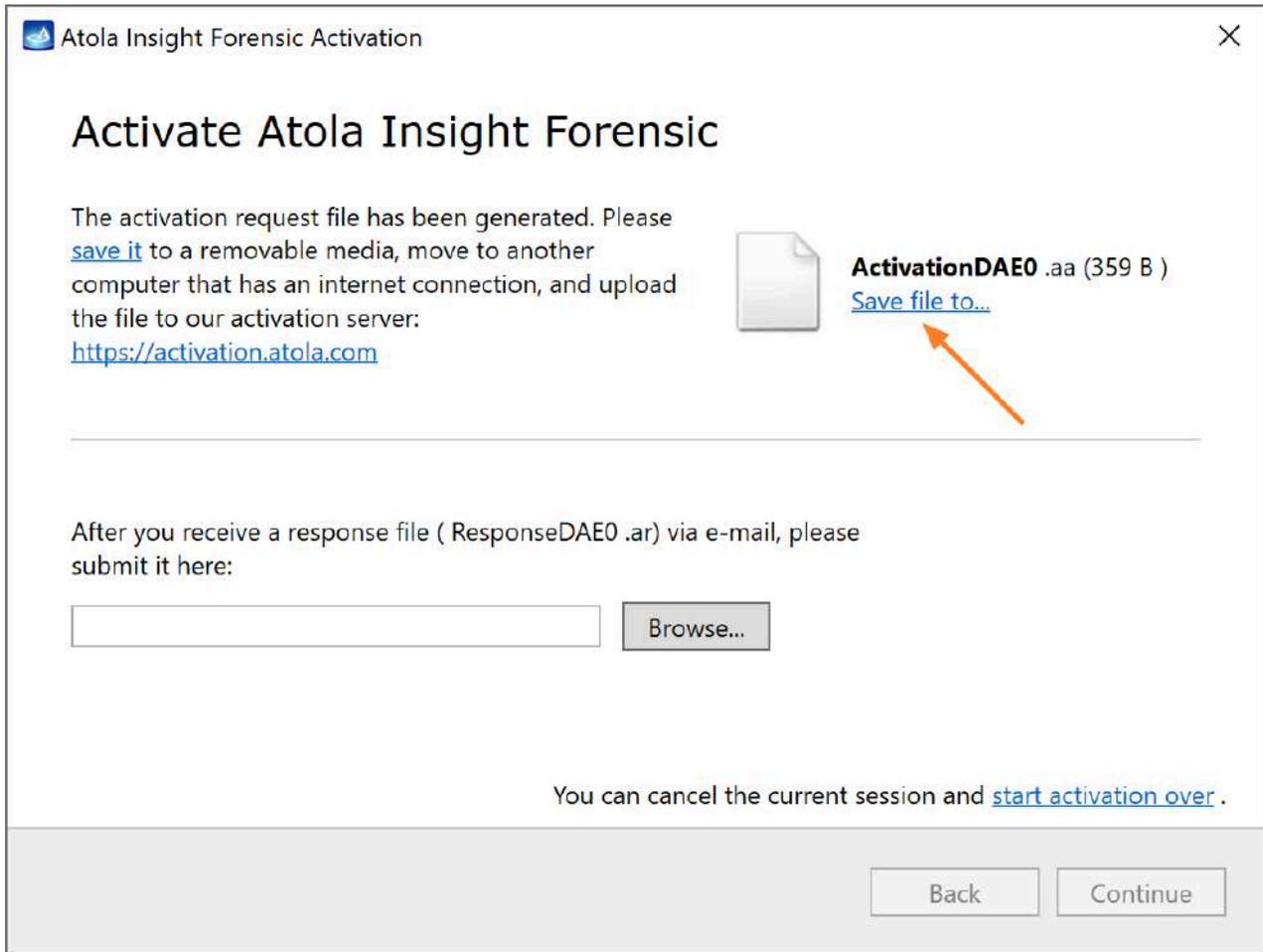


3. In the **Activation** dialog, choose **Offline activation** and click **Continue**.



4. Fill out all fields in the **Activation** form and click **Continue**.

5. Save the *Activation\*\*\*\*.aa* file to a USB stick.



- Using another computer connected to the internet, go to [activation.atola.com](https://activation.atola.com).
- Click **Browse** to upload the *Activation\*\*\*\*.aa* file from the USB stick, enter your email and click **Submit**.

## Atola Licensing

### Software Activation Request

Activation request file

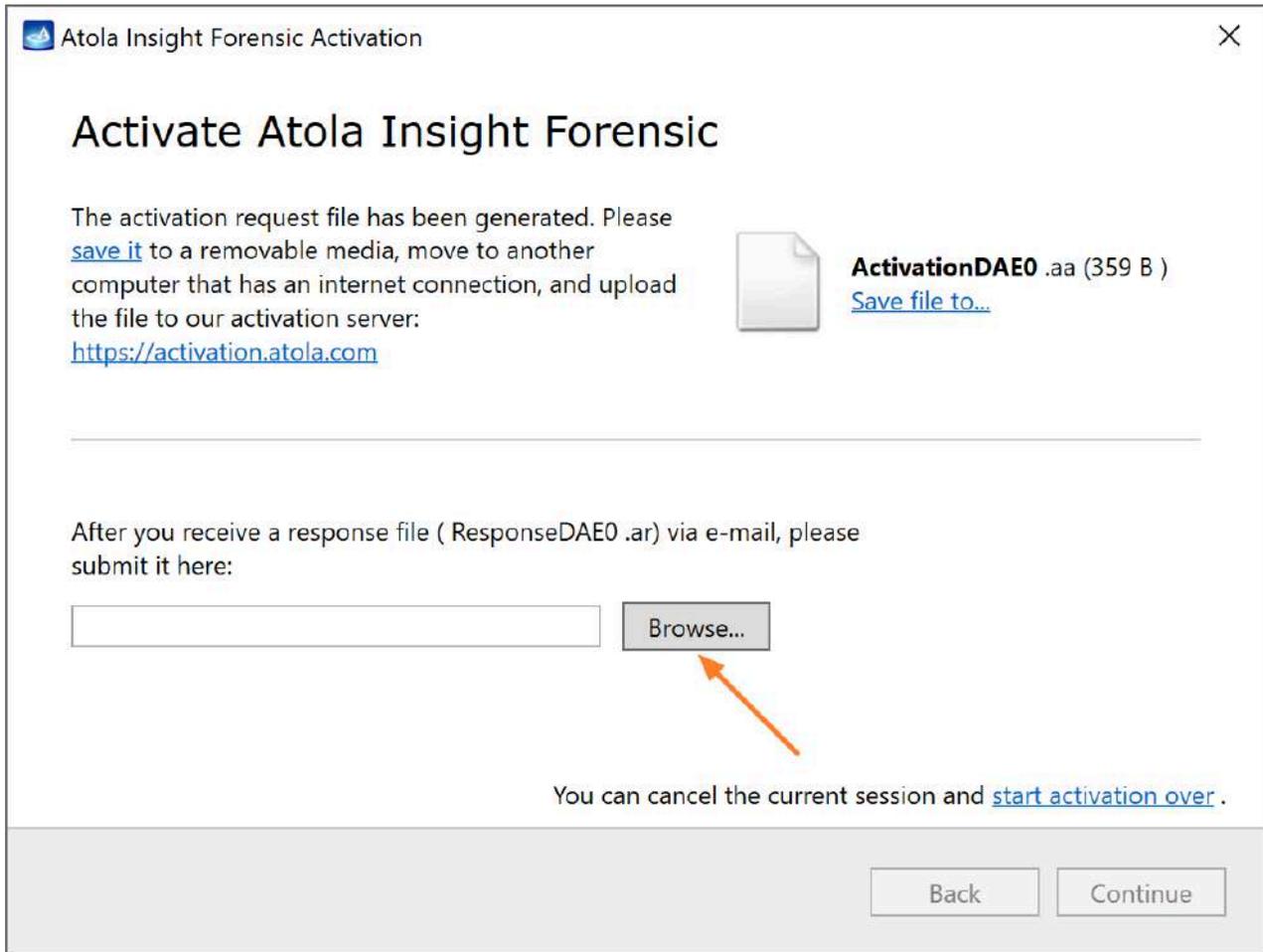
No file selected.

E-mail

Activation Response file will be sent to this e-mail address

**Note:** all fields are required.

- Atola sends you an email with an Activation response file: *Response\*\*\*\*.ar*. Save this file to your USB stick.
- In the Insight **Activation dialog**, submit the *Response\*\*\*\*.ar* file from the USB stick and click **Continue**.

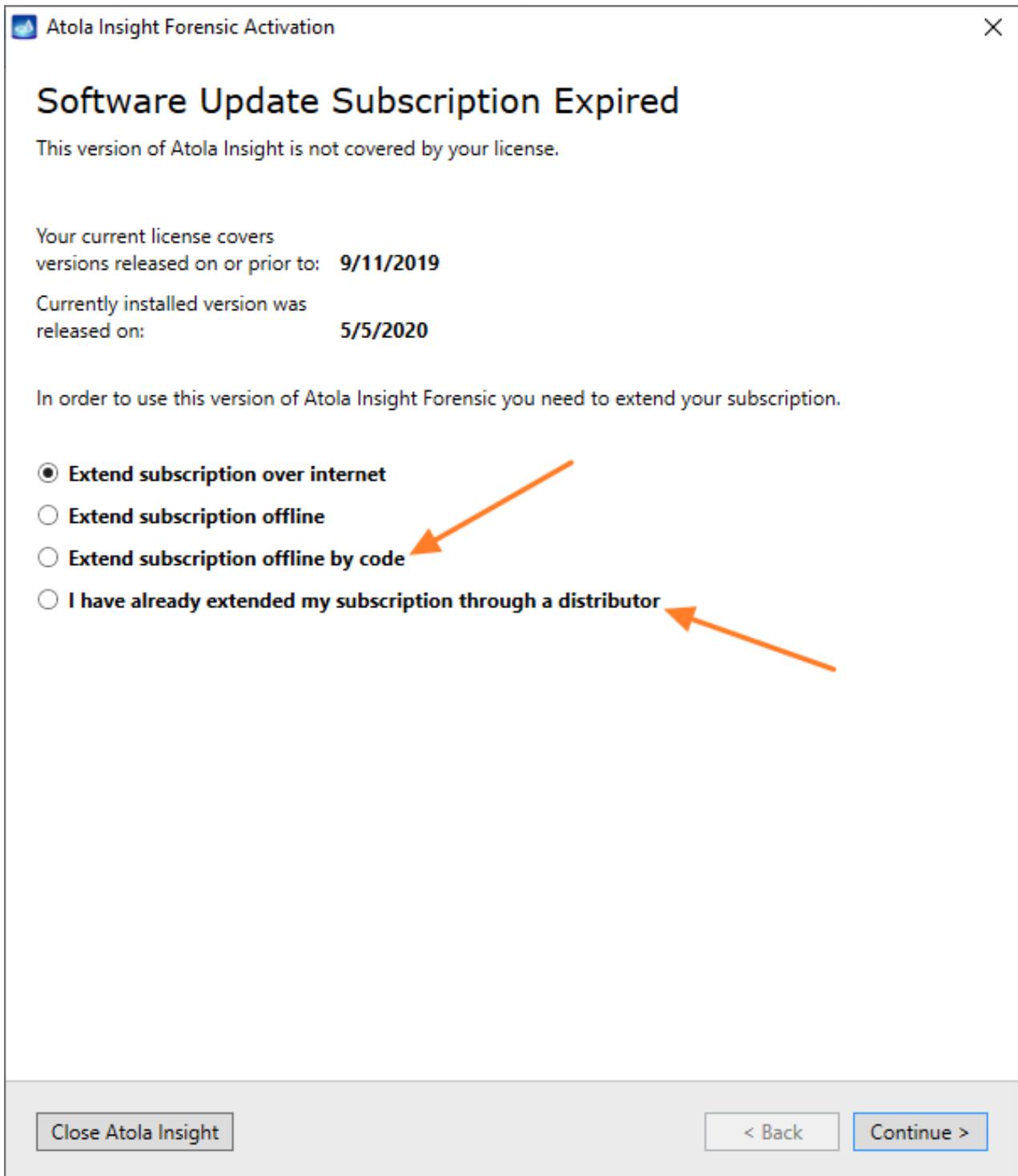


10. Insight confirms that reactivation has been successfully completed. Click **Finish**.

## When Insight software update is not covered by subscription

If your subscription expired but you installed a version of Insight software that is not covered by your expired subscription, you can do one of the following:

- Return to an earlier version of the software and go through the steps outlined earlier in this article to activate the new subscription and update the software to the new version afterward.
- When you launch Insight software you will get the screen below and choose the third or the fourth options, which will then take you through the steps outlined above in this article.



## Hardware and OS requirements

### Minimum hardware specs:

- Intel or AMD dual core CPU

- 8 GB of RAM
- one 1 GBit Ethernet port
- 5 GB of free disk space

## Recommended hardware specs for optimal performance:

- Intel or AMD dual core CPU
- 16 GB of RAM
- one 10 GBit Ethernet port
- 20 GB of free disk space

## Supported OS:

- Windows 10/11 (64 bit)

## DiskSense / HASP connection issues

The DiskSense hardware system includes an internal HASP USB dongle. It contains unique activation and subscription information.

## "Too many connections" and "Cannot locate DiskSense unit" errors

Having more than one DiskSense system in your network may result in HASP-related conflicts. These conflicts usually manifest as *"Too many connections"* or *"Cannot locate DiskSense unit"* errors.

The issue is caused by behavior of the HASP discovery system which by default picks a random HASP dongle on the network. In other words, one Atola Insight Forensic instance may establish the connection with one DiskSense system, however it will "use" the HASP dongle of another (random) system available on the network.

## How to resolve multiple HASP connection issues

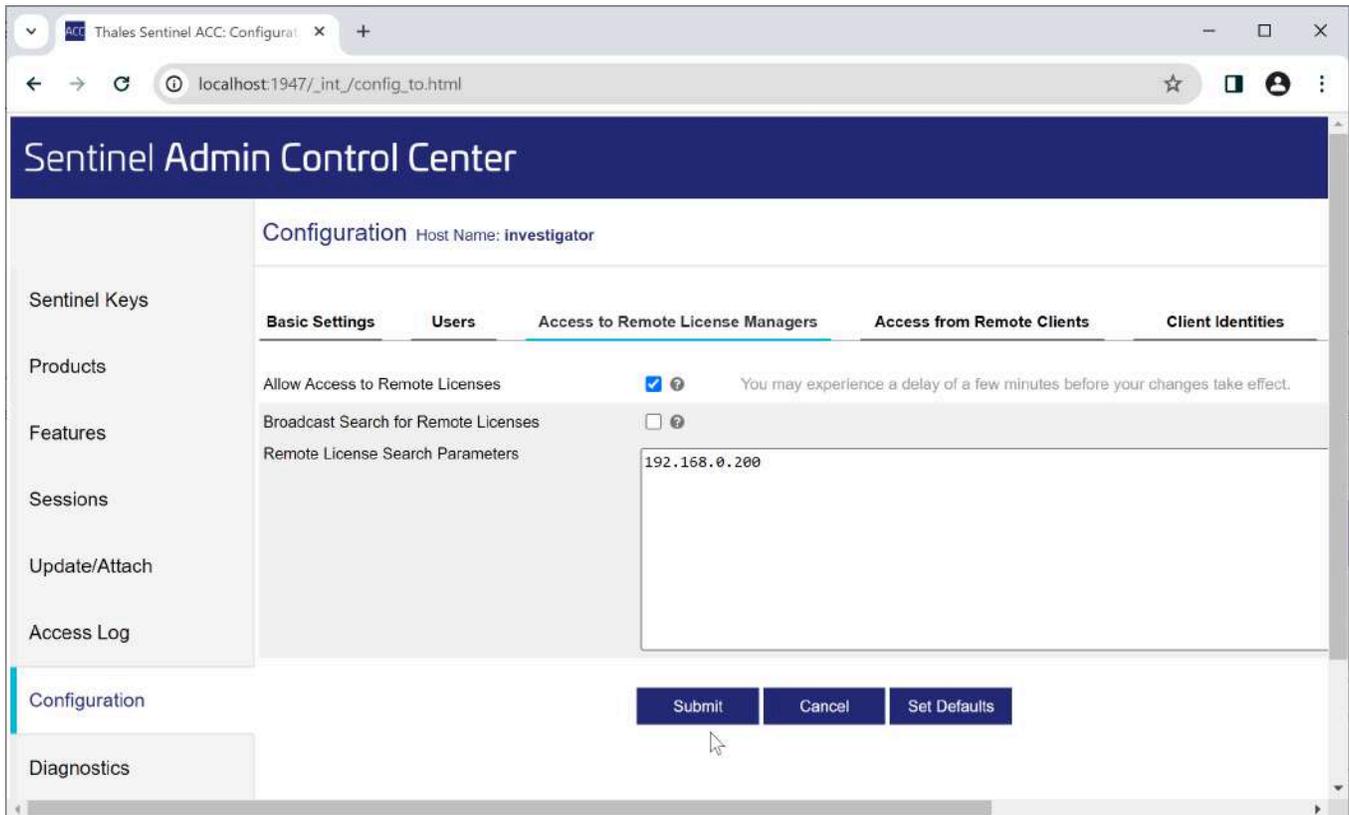
HASP discovery system offers a web administration tool where one can easily set up an IP filter specifying HASP dongle search locations.

1. In Atola Insight Forensic, go to **Insight menu** > **DiskSense Information** and copy the DiskSense unit IP address.
2. In your browser, go to <http://localhost:1947>. The **Sentinel Admin Control Center** page opens.
3. On the left, click **Configuration**.
4. Go to the **Access to Remote License Managers** tab.
5. Clear the **Broadcast Search for Remote Licenses** checkbox.

6. In the **Remote License Search Parameters** field, enter the DiskSense unit IP address specified in Atola Insight Forensic.

7. Click **Submit**.

After you perform the actions, the final screen should look like this (192.168.0.200 is used as an example):



**The Access to Remote License Managers tab with the correct settings.**

## Network database setup

Atola Insight Forensic enables working with remote database shared between many users. Here is the scenario how to setup such a network database and connect different PCs with Atola Insight to it:

1. On the network server PC, pre-install SQL Server 2012-2022.
2. On the user PC, launch Atola Insight Forensic.
3. On the menu bar, go to **Insight > Database Connection Settings**.
  - o Select Server type: Remote.
  - o Specify network server name, select SQL server instance and database names.
  - o Enter SQL server login and password as shown in the picture below:

**Database settings**

Server type: Remote

Computer name: S

SQL server name: SQLEXPRESS [Search](#)

Database name: InsightDB [Search](#)

Authentication: SQL Server Authentication

Username: ss

Password: ●●

Backup directory: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup

**Important:** backup directory is located on the same server as the selected database.

[Check connection](#) [Restore defaults](#) [OK](#) [Cancel](#)

4. Click **OK** and re-launch Atola Insight Forensic on the user PC.
5. It will create the remote database and ask for the Work Folder name:

**Work Folder Setup**

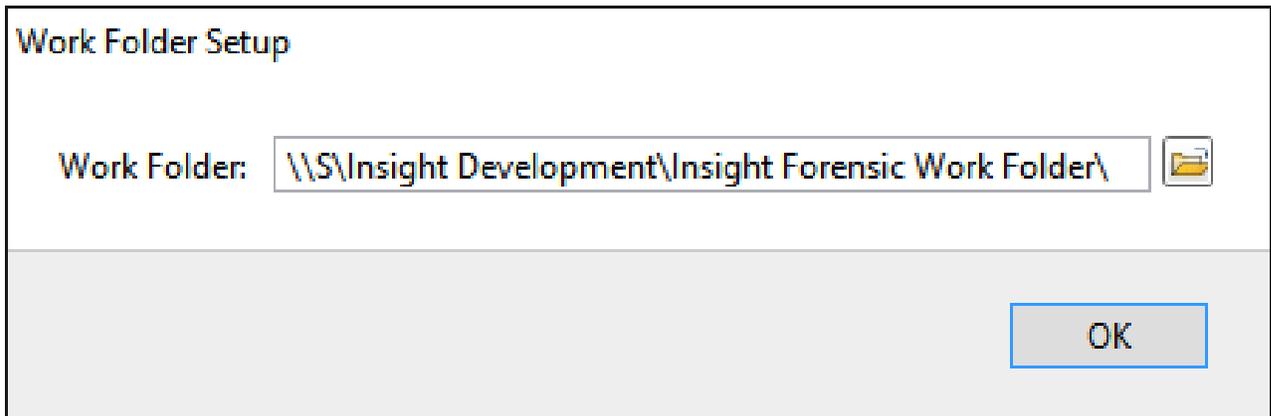
Work Folder: C:\Atola Insight Forensic\Work\ 

[OK](#)

Work Folder is necessary to store large files that do not fit into the database: imaging maps, logs, file recovery

hash lists.

6. Change the **Work Folder** to the shared folder on the network server PC.



Now you have Atola Insight network database prepared for remote use! You can connect Atola Insight Forensic software from the other PCs. Just set up the same database settings as you did in the step 3. No need to specify Work Folder anymore given Atola Insight will load it from the remote SQL server on the network server PC.

The only limitation: Two users will not be able to work on the same case simultaneously.

## Atola Insight Forensic: Database backup and restore

To be able to backup and restore Atola Insight Forensic database, you will need Microsoft SQL Server Management Studio Express. You can download it [here](#).

### Backup

To backup the database, please follow these steps:

1. Launch Microsoft SQL Server Management Studio Express.
2. Establish database connection (with default settings).
3. Select **Databases** folder on the tree.
4. Right-click **AtolaInsightForensic** and select **Tasks > Back Up**.
5. Check the backup destination and change it if desired.
6. Click **OK**.

### Restore

This procedure will work only if you did not move backup file (for example, from another PC). If you are moving the database over to another PC, see [Restore when moving](#).

1. Launch Microsoft SQL Server Management Studio Express.
2. Establish database connection (with default settings).
3. Select **Databases** folder on the tree.
4. Right-click **AtolalnsightForensic** and select **Tasks > Restore > Database**.
5. Select the desired backup file.
6. Click **OK**.

## Move

To move the database from one PC over to another, please follow these steps:

1. Backup your database on the source PC.
2. Copy backup file over to destination PC.
3. Restore the backup file on the destination PC (see [Restore when moving](#) below).

## Restore when moving

1. Launch Microsoft SQL Server Management Studio Express.
2. Establish database connection (with default settings).
3. Right-click **Databases** folder on the tree and select **Restore Database**.
4. In the **To database** field enter *AtolalnsightForensic*.
5. In **Source for restore**, select **From device**.
6. Point to the database backup file.
7. Click **OK**.

## If you only have .mdf and .ldf files

This may happen if your operating system has crashed and you are reinstalling everything from scratch. In this case you would need to copy *AtolalnsightForensic.mdf* and *AtolalnsightForensic\_log.LDF* files from the old hard drive over to the new one. You may find these files in:

- "C:\Users\\*USERNAME\*\AppData\Roaming\Atola\Insight Forensic\", if (localdb)\V11.0 instance is used (default).
- "C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\", if SQLEXPRESS instance is used.

After you have copied the database files, follow these steps:

1. Launch Microsoft SQL Server Management Studio Express.
2. Establish database connection (with default settings).
3. Right-click **Databases** folder on the tree and select **Attach**.
4. Click **Add** and select **AtolalnsightForensic.mdf**.
5. Click **OK**.

# Supported Drives

Atola Insight Forensic supports all 1.8-inch, 2.5-inch, 3.5-inch IDE, SATA and USB hard drives, USB Flash media as well as SD, Compactflash, and Memory Stick cards via a generic USB Card Reader.

To ensure high quality and efficiency of our tools, [we test them on hundreds of storage devices](#).

Atola Insight Forensic can also work with the following drive types using proprietary Atola extension modules:

- SAS drives
- M.2 NVMe/SATA/PCIe SSDs (M interface key only)
- PCIe SSDs from Apple MacBooks (2013 - 2015)
- Soldered Macbook SSDs (up to 2017)

Remote image acquisition can be performed via iSCSI protocol. For that, a drive on another PC has to be exposed as an iSCSI target.

Most functions of Atola Insight Forensic 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).

However, there are three functions that only work with specific hard drive model families:

- Automatic password removal
- Head selection in Imaging and Media Scan
- Full firmware access

## 1. Automatic password removal works for the following HDD models

- SATA and IDE Seagate hard drives (including F3 series) with exception of some models released since 2018
- SATA and IDE Western Digital hard drives with exception of some models released since 2018
- SATA and IDE Toshiba hard drives: MG, MK, MQ, DT families with exception of some models released since 2018
- SATA and IDE Maxtor hard drives
- SATA and IDE Samsung hard drives with exception of old hard drives made prior to 2004 and some latest models
- SATA and IDE Fujitsu hard drives with exception of latest models (MHW and newer)
- The following Hitachi hard drives are supported: HCxxxxxxxA7A3xx, HDxxxxxxxCLA3xx, HTxxxxxxxA9A3xx, HTxxxxxxxA9E3xx, HTxxxxxxxA9E6xx, HTxxxxxxxB9A3xx, HTxxxxxxxG9ATxx, HTxxxxxxxG9SAxx, HTxxxxxxxH9ATxx, HTxxxxxxxH9SAxx, HTxxxxxxxJ9ATxx, HTxxxxxxxJ9SAxx, HTxxxxxxxK9ATxx, HTxxxxxxxK9SAxx, HTxxxxxxxL9SAxx, HTxxxxxxxM9ATxx, HTS72xxxxA7E6xx, HUXxxxxxxxCLA3xx, IC25NxxxATMRxx
- The following Hitachi DK hard drives are supported: DK23DA, DK23EA, DK23FA.
- The following Hitachi Endurastar hard drives are supported: J4K50 (HEJxxxxxxxF9ATxx), N4K50 (HENxxxxxxxF9ATxx).

Please note that due to the wide variety of firmware revisions released by hard drive manufacturers, it is impossible to guarantee that the password removal will always work. Hence, password removal may fail on a small percentage of hard drives.

## 2. 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

## 3. Full firmware access (HDD only)

- Western Digital hard drives: all IDE and SATA models are supported with exception of latest models released since 2018
- Fujitsu hard drives: all IDE and SATA models are supported
- Samsung hard drives: all IDE and SATA models are supported with exception of old hard drives made prior to 2004
- The following Hitachi hard drives are supported: A7A3, A9A3, A9E3, A9E6, ALA6, ATCS, ATDA, ATMR, AVER, AVV2, AVVA, AVVN, B9A3, CLA3, DADA, DARA, DBCA, DCXA, DHEA, DJNA, DJSA, DKLA, DLA3, DLAT, DPTA, DTCA, DTLA, DTTA, G9AT, G9SA, H9AT, H9SA, J9AT, J9SA, K9AT, K9SA, L9SA, M9AT, PLA3, PLAT, VLAT
- Toshiba hard drives supported: DT family only

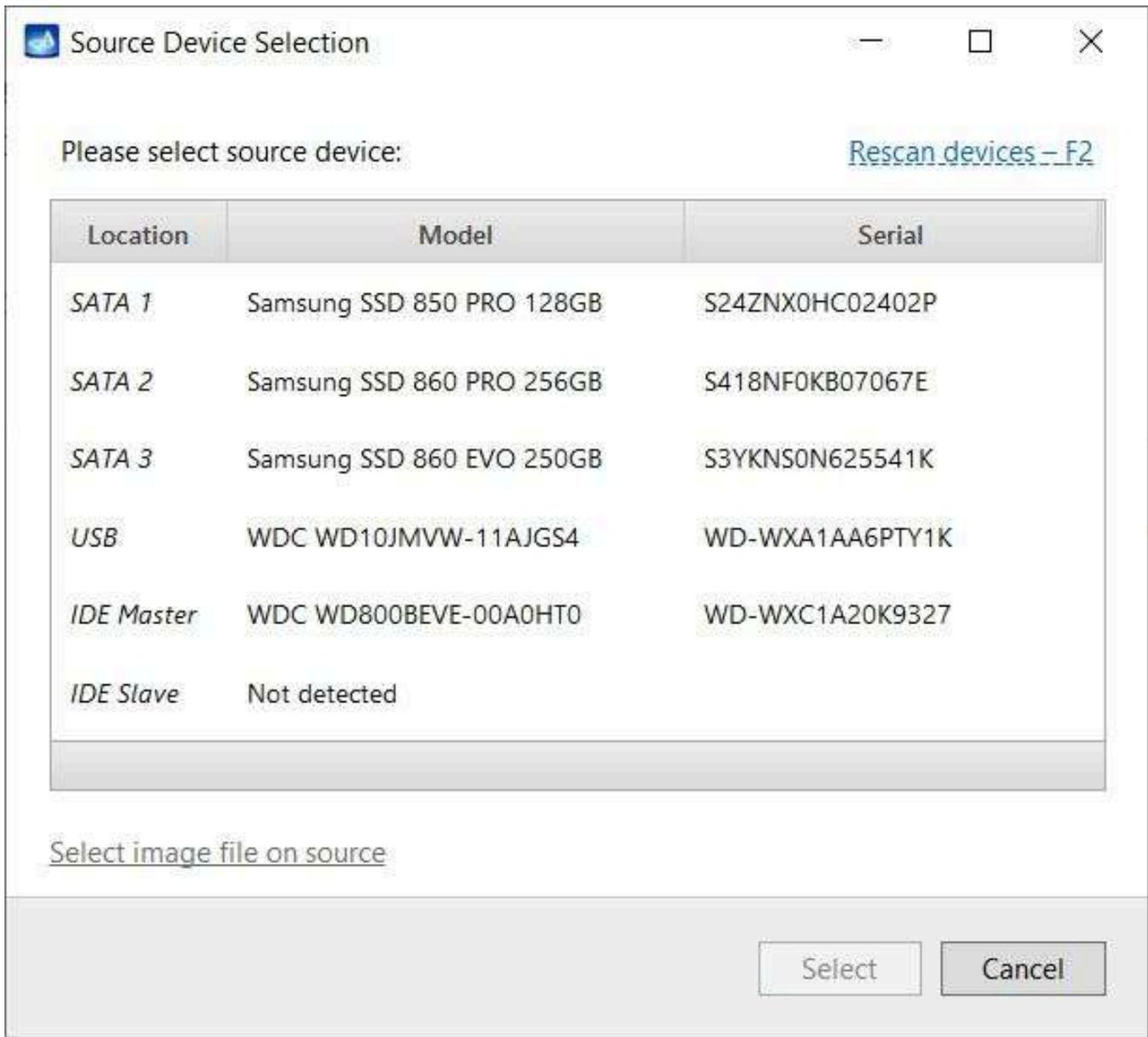
## Working with SATA, USB, IDE drives

The purpose of this page is to provide information on Atola Insight Forensic start up procedure.

## Begin with source drive selection

The **Source Device Selection** dialog is available from the menu bar (**Source > Select Source**) or via **F3** shortcut key:

SATA 1, IDE, USB Source and Extension share the same first source port in the UI, while SATA2 and SATA3 have distinct UI ports.



### Source device selection

At this point you can select the port you'd like to work with (SATA, USB, IDE Master, IDE Slave).

After you select the device, Atola Insight Forensic switches to the main application window.

## Attaching and detaching drives

You can attach and remove drives at any time without restarting the software or hardware unit.

When replacing drives, Atola Insight Forensic detects the change automatically. However, if you'd like to manually re-identify a hard drive, you can do one of the following:

- Use the Source Port **Re-Identify** button or press F2.
- Use **Source > Select Source** menu item.

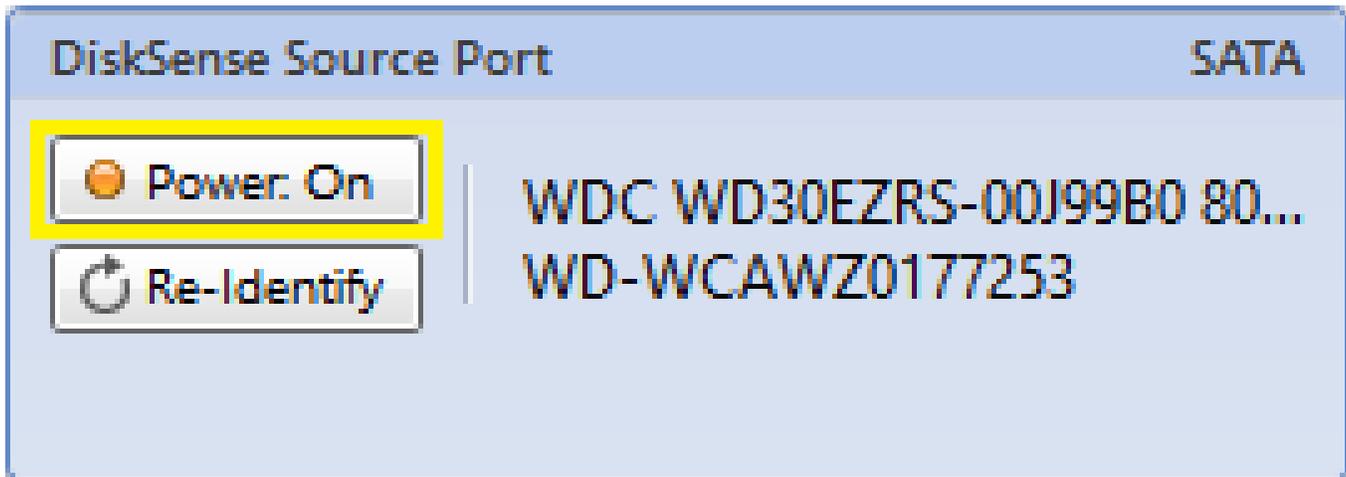
Select Source...	F3
<b>Device Operations</b>	
Reset	Shift+F2
Re-Identify	F2
Spindown	
<b>Case History</b>	
Assign Case Number...	Ctrl+N
Print...	Ctrl+P
Export Current Case...	Ctrl+E
Show History Folder in Explorer	

#### Source device menu

The difference is that re-identification works only when the attached drive can return at least some identification data. When the hard drive has significant damage (for example, a burnt PCB) and therefore won't return identification data, Atola Insight Forensic will fail to automatically recognize such hard drive.

In this case you would have to use **Source > Select Source** menu item to manually select the device. Atola Insight Forensic will still be able to diagnose a hard drive that is "completely dead" by relying on the current sampling.

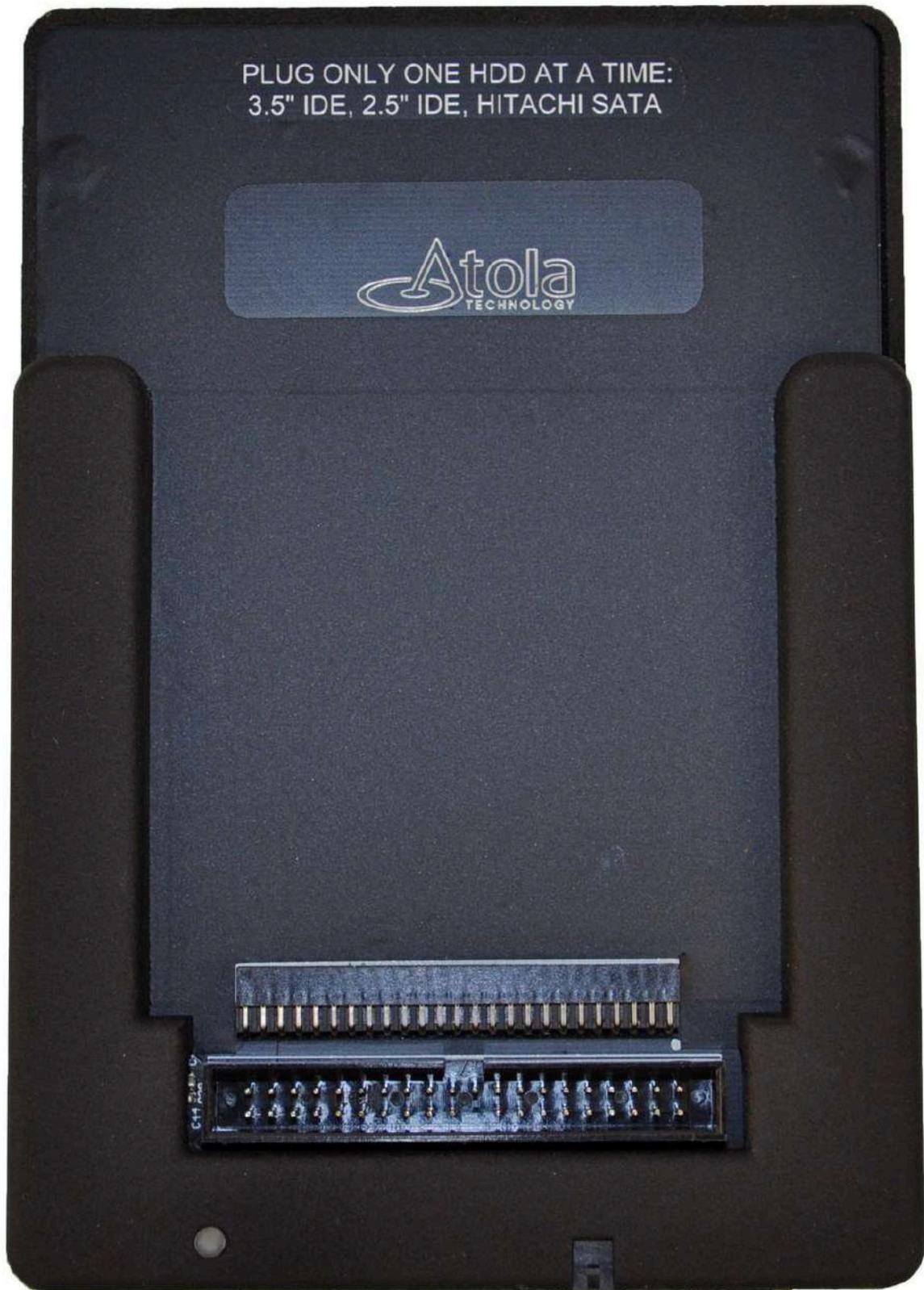
Before disconnecting hard drives from the unit, we recommend to use the **Power Off** button in Atola Insight Forensic software to properly shut down the drive:



**Source power button**

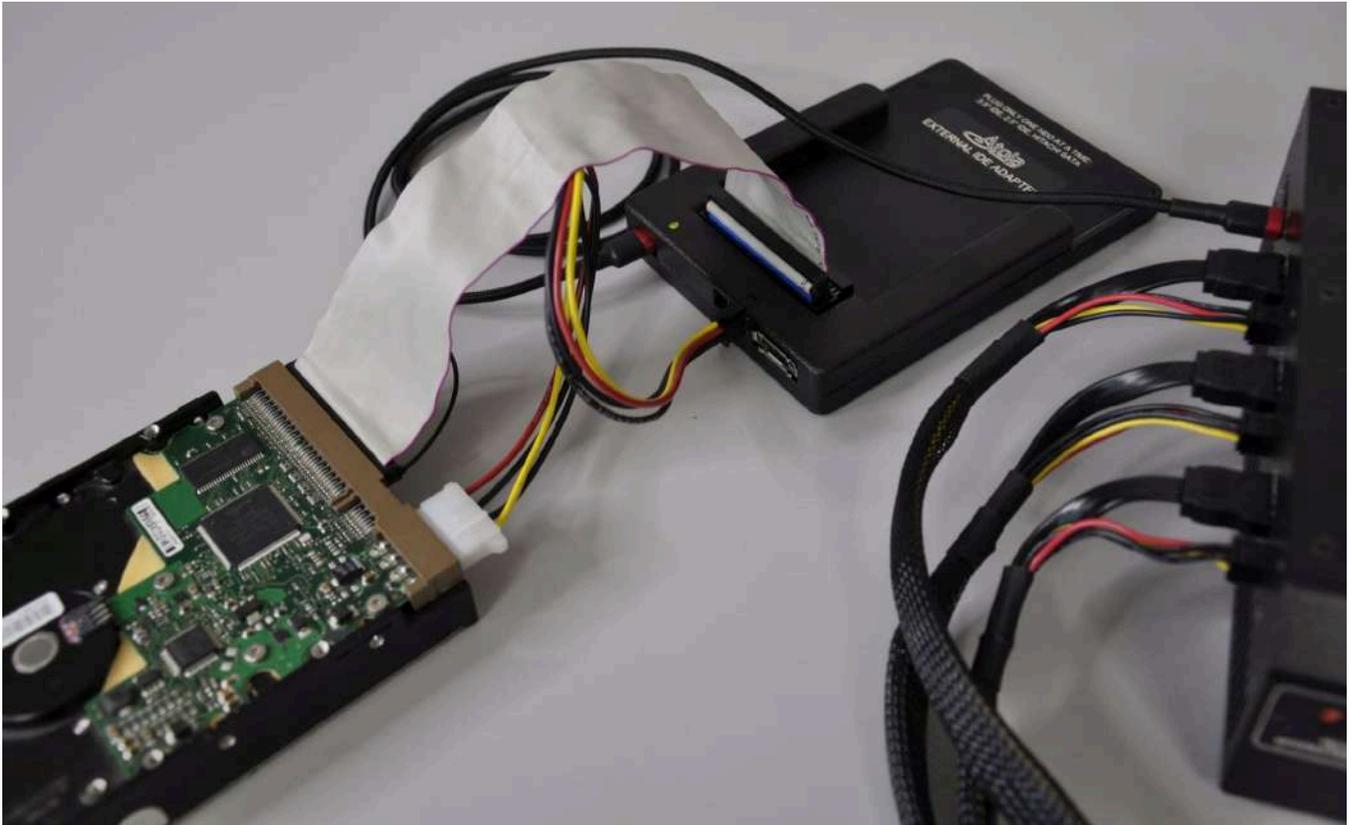
## Working with IDE drives

The only way to connect an IDE drive to DiskSense 2 unit is Atola External IDE adapter, which is included in the product package.



The adapter plugs straight into the IDE (USB-C) port located on the front side of the DiskSense unit.

## 3.5-inch IDE drive connection



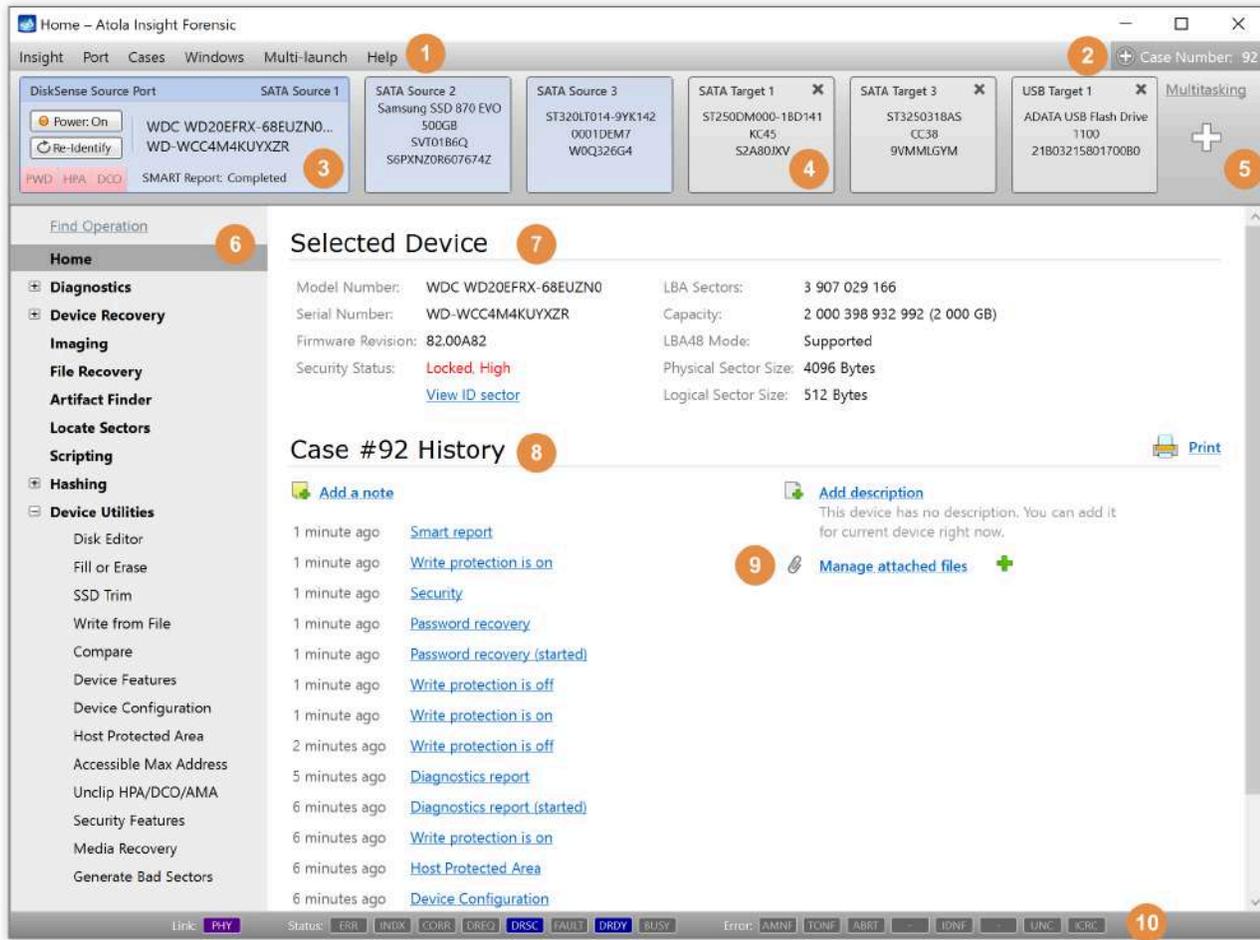
## 2.5-inch IDE drive connection



## Main window and controls

This page provides information on basic Atola Insight Forensic controls:

1. [Menu bar](#)
2. [Case panel](#)
3. [Source port controls and indicators](#)
4. [Target port controls and indicators](#)
5. [Plus icon](#)
6. [Sidebar](#)
7. [Selected device information](#)
8. [Case history](#)
9. [Attached files](#)
10. [ATA Registers bar](#)



## 1. Menu bar

The Menu bar contains Insight Forensic commands grouped in six menus:

- [Insight](#)
- [Port](#)
- [Cases](#)
- [Windows](#)
- [Multi-launch](#)
- [Help](#)

## Insight menu

- **Change DiskSense Unit:** Lets you switch between the different DiskSense hardware units connected to your local network or PC.
- **Modify DiscSense Unit IP:** Configures a network address and hostname of the DiskSense hardware unit.
- **DiskSense Information:** Shows unit's serial number, firmware version, IP and MAC address, as well as network speed. Keyboard shortcut: *Ctrl+D*.

- **Manage SSH Root Password:** Lets you remotely access the device's operating system for additional maintenance.
- **Preferences:** Configures system settings, such as work folder path, system language, case management and file recovery settings etc. Keyboard shortcut: *Ctrl+Q*.
- **Database Connection Settings:** Sets up server path and database name, authentication method and credentials, as well as the path for backups.

## Port menu

- **Select Source:** Allows choosing another source device (SATA/IDE/USB). For details, see [Working with SATA, USB, IDE drives](#). Keyboard shortcut: *F3*.
- **Reset:** Resets a hard drive's interface. Keyboard shortcut: *Shift+F2*.
- **Re-Identify:** Should be used after you replace the drive. Keyboard shortcut: *F2*.
- **Spindown:** Sends the 'Spindown Immediate' ATA command to the drive.
- **Detect All Devices:** Sends identification commands to all devices connected to the DiskSense 2 hardware unit and displays all detected devices on the Device panel. Keyboard shortcut: *F6*.
- **Assign Case Number:** Allows assigning a specific number to the open case. Keyboard shortcut: *Ctrl+N*.
- **Print:** Prints or saves to a file the whole case history. For details, see [Printing reports in a case](#). Keyboard shortcut: *Ctrl+P*.
- **Export Current Case:** Saves the entire case history into a single file. Keyboard shortcut: *Ctrl+E*.
- **Show History Folder in Explorer:** Opens the file folder of the current case in Windows Explorer.

## Cases menu

- **Search/Open:** Lets you find a case according to specific criteria and open it. For details, see [Finding and opening a case](#). Keyboard shortcut: *Ctrl+O*.
- **Export:** Brings the window with all available cases, in which you can select cases and export them to a defined folder. For guidance, see [Exporting and importing cases](#).
- **Import:** Imports a case from another computer into the Insight Forensic database. For guidance, see [Exporting and importing cases](#). Keyboard shortcut: *Ctrl+I*.

## Windows menu

- **Current Oscilloscope:** Helps to keep track of hard drive power consumption levels and can be especially useful for damaged hard drive diagnostics. Keyboard shortcut: *Ctrl+U*.
- **Terminal:** Helps in accessing the firmware area of certain hard drive models for manual firmware recovery. Keyboard shortcut: *Ctrl+K*.

## Multi-launch menu

This menu lets you quickly launch the following operations on multiple devices at once:

- [Automatic Checkup](#) (drive diagnostics)
- [Fill or Erase](#)
- SSD Trim
- [Artifact Finder](#)
- Calculate Hash
- [Locate Sectors](#)

## Help menu

- **Manual:** Opens a single-page user manual for Insight Forensic in your web browser. Keyboard shortcut: *F1*.
- **Keyboard Shortcuts:** Opens a PDF file with a list of all keyboard shortcuts used in Insight Forensic.
- **Send Feedback:** Redirects to a [contact form](#) on the Atola Technology website.
- **Extend Subscription:** Provides variants of extending your software subscription for another period, either [offline](#) or online.
- **Activation Status:** Shows information about your current subscription: subscription ID, activation status, subscription due date.
- **About:** Provides information about your current Insight Forensic firmware version and the serial number of your DiskSense 2 hardware unit.

## 2. Case panel

This panel shows the current case number. To [add or change the case number](#) and description, click the small plus icon.

## 3. Source port controls and indicators

The source port consists of several parts:

- **Power button:** Allows to manually apply power to the hard drive attached to the DiskSense 2 unit.
  - When power is on, a single button click sends a spin-down command first and then performs power-off.
  - When power is on, you can click the button a second time during spin-down to instantly power the device off.
- **Re-Identify button:** Used when you replace the hard drive.
- **HDD model, firmware, and serial number:** Hard drive identification info.
- **Device interface type:** Can be SATA, USB, or IDE.
- **DCO tag:** Indicates whether Device Configuration Overlay (DCO) is activated.
- **HPA tag:** Indicates whether the Host Protection Area (HPA) is activated.
- **PWD tag:** Indicates if the hard drive is locked with an ATA password.

## Source port context (right-click) menu

- **Select Source:** Allows choosing another source device (SATA/IDE/USB). For more information, see [Working with SATA, USB, IDE drives](#).
- **Select source file:** Allows choosing a raw image file located on a source device.
- **Reset:** Resets a hard drive's interface.
- **Re-identify:** Should be used after you replace the drive.
- **Spindown:** Sends 'Spindown Immediate' ATA command to the drive.
- **Current Oscilloscope:** Brings up the oscilloscope window.
- **Terminal:** Brings up RS-232/serial terminal window.
- **Assign Case Number:** Allows assigning a specific number to the open case.
- **Print:** Prints or saves the whole case history to a file. For details, see [Printing reports in a case](#).
- **Export:** Saves the entire case history into a single file.
- **Import:** Imports case history from a previously exported file.

## 4. Target port controls and indicators

The Target port has all the features of the Source port. The Target port allows to work with one of the following:

- A device attached to the hardware target port (SATA or USB).
- Image file: Raw, E01, AFF4.

## Target port context (right-click) menu

Along with the commands that are identical to the ones in the [Source port context menu](#), the Target port context menu has an additional one:

- **Remove port:** Powers down the selected port and removes it from the Device panel.

## 5. Plus icon

To start another operation, add another target drive port for:

- SATA device
- USB device
- Image file
- Image file on target
- Multiple devices of any type

**Detect All Devices:** Sends identification commands to all devices connected to the DiskSense 2 hardware unit and displays all detected devices on the Device panel.

## 6. Sidebar

This sidebar helps to navigate through operations and different software modules of Insight Forensic.

## 7. Selected device information

Selected Device			
Model Number:	WDC WD20EFRX-68EUZN0	LBA Sectors:	3 907 029 166
Serial Number:	WD-WCC4M4KUYXZR	Capacity:	2 000 398 932 992 (2 000 GB)
Firmware Revision:	82.00A82	LBA48 Mode:	Supported
Security Status:	Locked, High <a href="#">View ID sector</a>	Physical Sector Size:	4096 Bytes
		Logical Sector Size:	512 Bytes

Shows detailed information about the device currently attached to the selected port:

- Model number
- Serial number
- Firmware version
- Security status
- Number of LBA sectors
- Device capacity
- LBA48 mode support
- Physical and logical sector size

The **View ID Sector** link will open the full information on the ID sector returned by the hard drive.

## 8. Case history

# Case #92 History

---

 [Add a note](#)

- 1 minute ago [Smart report](#)
- 1 minute ago [Write protection is on](#)
- 1 minute ago [Security](#)
- 1 minute ago [Password recovery](#)
- 1 minute ago [Password recovery \(started\)](#)
- 1 minute ago [Write protection is off](#)
- 1 minute ago [Write protection is on](#)
- 2 minutes ago [Write protection is off](#)
- 5 minutes ago [Diagnostics report](#)
- 6 minutes ago [Diagnostics report \(started\)](#)

Lists all actions that were done to the selected device. To get a detailed report on an action, click on its name.

## 9. Attached files



[Manage attached files](#)



example-hash-list.txt



ISO-17025.pdf



Package contents.xlsx

Insight Forensic lets you attach files to the case. Whenever you attach a picture, a thumbnail is added to the Home screen.

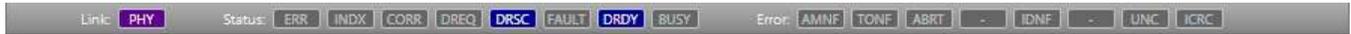
To attach an image or file to the current case, click the green plus icon. For details, see [Add a document or an image to the case](#).

## 10. ATA Registers bar



Displays raw contents of Link, Status, and Error ATA registers in real time. To learn more about each register, see [ATA registers: what they mean](#).

## ATA registers: what they mean



### Link Register

**PHY:** It's only enabled when port powered on, device presence detected and physical layer 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)

**TONF (Track 0 Not Found):** obsolete

**ABRT:** command aborted (unsupported command or other failure)

**IDNF:** sector ID not found (usually occurs on failed read attempt)

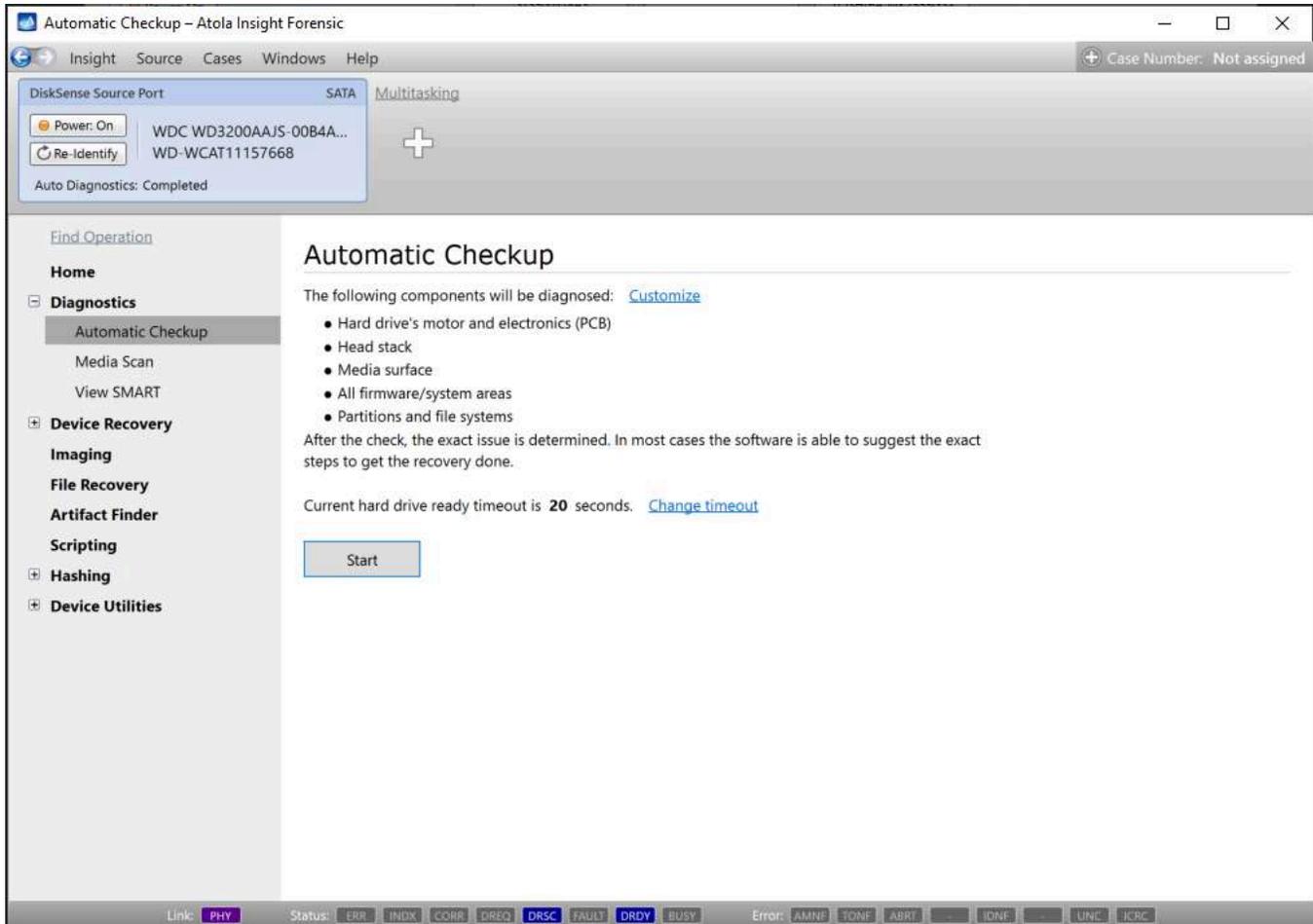
**UNC:** uncorrectable read error; the hard drive was unable to read data even after applying ECC recovery algorithms

**ICRC (Interface CRC error):** there was CRC error while transferring data between host and the hard drive (usually indicates bad interface cable)

## Automatic Diagnostics

Automatic Checkup feature diagnoses the following hard drive components:

- Electronics (circuit board)
- Motor
- Heads
- Media surface
- Firmware area
- Partitions and file systems



## One-button start of Diagnostics

First, hard drive's **electronics** (printed circuit board or PCB) is diagnosed. The system applies power to the device and records and analyzes spin-up current curve. This allows to detect most issues with the PCB and the motor.

Then, the contents of the hard drive's **ATA registers** and **device identification sector** are being analyzed.

Diagnosics in progress... - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: On WDC WD3200AAJS-00B4A...  
 Re-Identify WD-WCAT11157668

Auto Diagnostics: 20 %

Find Operation

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

- Imaging
- File Recovery
- Artifact Finder
- Scripting

Hashing

Device Utilities

## Checking Circuit Board (PCB)

Done

Stop

Check list

- Circuit Board
- Heads
- Media Surface
- Firmware
- File System

### Circuit Board (PCB)

Device is powered on. A power cycle is needed...  
 Applying power and watching spin-up currents...  
 Selected Interface: SATA

**Current oscillogram (12V):**

**Current oscillogram (5V):**

Device has become ready in 7 sec.  
 Registers: 0101 0000 0000 0000 0000 A0A0 5050 Alt: 5050  
 Peak power consumption during spin-up: 5V line = 791,21 mA; 12V line = 1022,42 mA  
 Integrity word of device identification data is ok.  
 Device has been identified: WDC WD3200AAJS-00B4A0 SN: WD-WCAT11157668  
 Logical sector size: 512 bytes, Physical sector size: 512 bytes  
 Elapsed: 26,8 sec.

**Circuit board check passed**

Link: PHY Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY Error: AMNF TDNF ABRT IDNF LUNC ICRC

## Measuring hard drive's currents

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 hard drive's error reporting systems.

Diagnosics in progress... - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: On WDC WD3200AAJS-00B4A...  
 Re-Identify WD-WCAT11157668

Auto Diagnostics 40 %

Find Operation

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

Imaging

File Recovery

Artifact Finder

Scripting

Hashing

Device Utilities

## Checking Heads

Done

Stop

Check list

- Circuit Board
- Heads
- Media Surface
- Firmware
- File System

**Heads**

Detecting device family  
 All device identification checks have passed.  
 Detected 2 heads: 0 1  
 Performing media access timing verification separately for each head.  
 Using the following LBA ranges for this test: Outer: 0 - 475 479, Middle: 312 333 484 - 312 808 963, Inner: 624 666 968 - 625 142 447.

**Head #0 speed graph:**

**Head #1 speed graph:**

Head #	Speed	Sectors processed	Freeze count	Read Errors	Head status
0	84 MB/s	718 260	0	0	OK
1	85 MB/s	708 179	0	0	OK

Media access timing verification shows no damage to the head stack.  
 Elapsed: 10,6 sec.

**Head stack check passed**

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

## Head stack test

If head stack looks good, the system performs a short **media scan**. The purpose of this scan is to find out how many "bad sectors" (if any) there are on the surface:

Diagnosics in progress... - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: On WDC WD3200AAJS-00B4A...  
 Re-Identify WD-WCAT11157668

Auto Diagnostics: 60 %

Find Operation

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

Imaging

File Recovery

Artifact Finder

Scripting

Hashing

Device Utilities

## Checking Media Surface

Done

Stop

Check list

- Circuit Board
- Heads
- Media Surface**
- Firmware
- File System

Head #	Speed	Sectors processed	Freeze count	Read Errors	Head status
0	84 MB/s	718 260	0	0	OK
1	85 MB/s	708 179	0	0	OK

Media access timing verification shows no damage to the head stack.  
 Elapsed: 10,6 sec.

**Head stack check passed**

**Media Surface**

Media scan is running...

Verifying starting sectors (LBA: 0-600 064)  
 0 error(s) found  
 Speed: 129 MB/s

Verifying middle sectors (LBA: 312 571 223-313 171 287)  
 0 error(s) found  
 Speed: 113 MB/s

Verifying ending sectors (LBA: 624 542 383-625 142 447)  
 0 error(s) found  
 Speed: 64 MB/s

Average speed: 102 MB/s  
 Elapsed: 10,8 sec.

**Media surface check passed**

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

## Checking media surface for bad sectors

Then, several firmware tests are performed:

Diagnosics in progress... - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: On WDC WD3200AAJS-00B4A...  
 Re-Identify WD-WCAT11157668

Auto Diagnostics: 80 %

Find Operation

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

Imaging

File Recovery

Artifact Finder

Scripting

Hashing

Device Utilities

## Checking Firmware

Done

Stop

Check list

- Circuit Board
- Heads
- Media Surface
- Firmware**
- File System

### Firmware

Device is not locked.  
 Device identification data is valid.  
 Max Address according to device ID: 625 142 447  
 Native Max Address Ext: 625 142 447  
 Max Address from DCO: 625 142 447  
 Reported capacity appears logically correct.  
 Performing SMART checks...  
 Power cycles: 6908 Power on time: 455 days 10 hours SMART Status: Good

#	Attribute Name	Value	Worst	Threshold	RAW
1	Read error rate	200	200	51	130
3	Spin up time	151	148	21	3 441
4	Number of spin-up times	94	94	0	6 977
5	Reallocated sectors count	200	200	140	0
7	Seek error rate	200	200	0	0
9	Power-on time	86	86	0	10 930
10	Spin-up retries	100	100	0	0
11	Calibration retries	100	100	0	0
12	Power Cycles	94	94	0	6 908
192	Power-off retract count	199	199	0	1 320
193	Load/unload cycle count	198	198	0	6 976
194	HDA Temperature	109	92	0	34
196	Reallocate event count	200	200	0	0
197	Current pending sectors	200	199	0	0
198	Offline scan UNC sectors	200	200	0	0
199	Ultra ATA CRC Error Rate	200	200	0	84
200	Write error rate at preamp	200	200	0	0

### Temperature and power cycle history

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

\* Earliest available record. The exact time and duration is unspecified in SMART history.  
 Last significant work time interval before power off or standby (in minutes): 94  
 White gaps indicate the discontinuity in temperature measurements. They show that temperature sensor was inoperative for periods of time due to power off or standby mode.  
 Elapsed: 0,3 sec.

**Firmware check passed**

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

## Firmware checks

If no issues found up to this point, a file systems checkup is performed:

Diagnosics in progress... - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: On WDC WD3200AAJS-00B4A...  
 Re-Identify WD-WCAT11157668

Auto Diagnostics: 100 %

Find Operation

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

Imaging

File Recovery

Artifact Finder

Scripting

Hashing

Device Utilities

### Checking File System Structures

Complete

Stop

Check list

- Circuit Board
- Heads
- Media Surface
- Firmware
- File System**

#### Temperature and power cycle history

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

\* Earliest available record. The exact time and duration is unspecified in SMART history.  
 Last significant work time interval before power off or standby (in minutes): 94  
 White gaps indicate the discontinuity in temperature measurements. They show that temperature sensor was inoperative for periods of time due to power off or standby mode.  
 Elapsed: 0,3 sec.

**Firmware check passed**

#### File System Structures

Found partition at sector 2048 (type exFAT). Label: Atola Volume. Size: 320 GB.  
 Elapsed: 0,7 sec.

**Partitions and file systems look fine.**

Link: PHY Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY Error: AMHF TONE ABRT IDNF LINC JCRC

## Short analysis of filesystems

After all tests are done, Atola Insight Forensic will display the full report. The **Diagnostics** result message box contains a short summary of all tests:

Automatic Checkup finished – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: On WDC WD3200AAJS-00B4A...  
 Re-Identify WD-WCAT11157668

Auto Diagnostics: Completed

Print... Save to file... Copy to Clipboard

воскресенье, 14 февраля 2021 г. 19:05  
 Report created by Atola Insight Forensic 4.17.7634.14614.

## Diagnostics report

Device model:	WDC WD3200AAJS-00B4A0	Unit IP:	10.0.0.155
Device serial:	WD-WCAT11157668	Unit serial:	yulias
Device firmware:	01.03A01	Write protection:	On
Device size:	320 GB (320 072 933 376 bytes)	Computer:	DESKTOP-KNTLFF5
Case number:	Not assigned	User:	HP
Case description:		OS:	64-bit Windows 10 Home Version 6.2 (Build: 18363)

### Diagnostics results

**No major hardware or firmware issues have been found.**

**Estimated imaging time: 51 minutes**

### Full Diagnostic Log

#### Circuit Board (PCB)

Device is powered on. A power cycle is needed...  
 Applying power and watching spin-up currents...  
 Selected Interface: SATA

#### Current oscillogram (12V):

mA

0 250 500 750 1000

0 1 306 2 613 3 920 5 227 6 534 ms

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

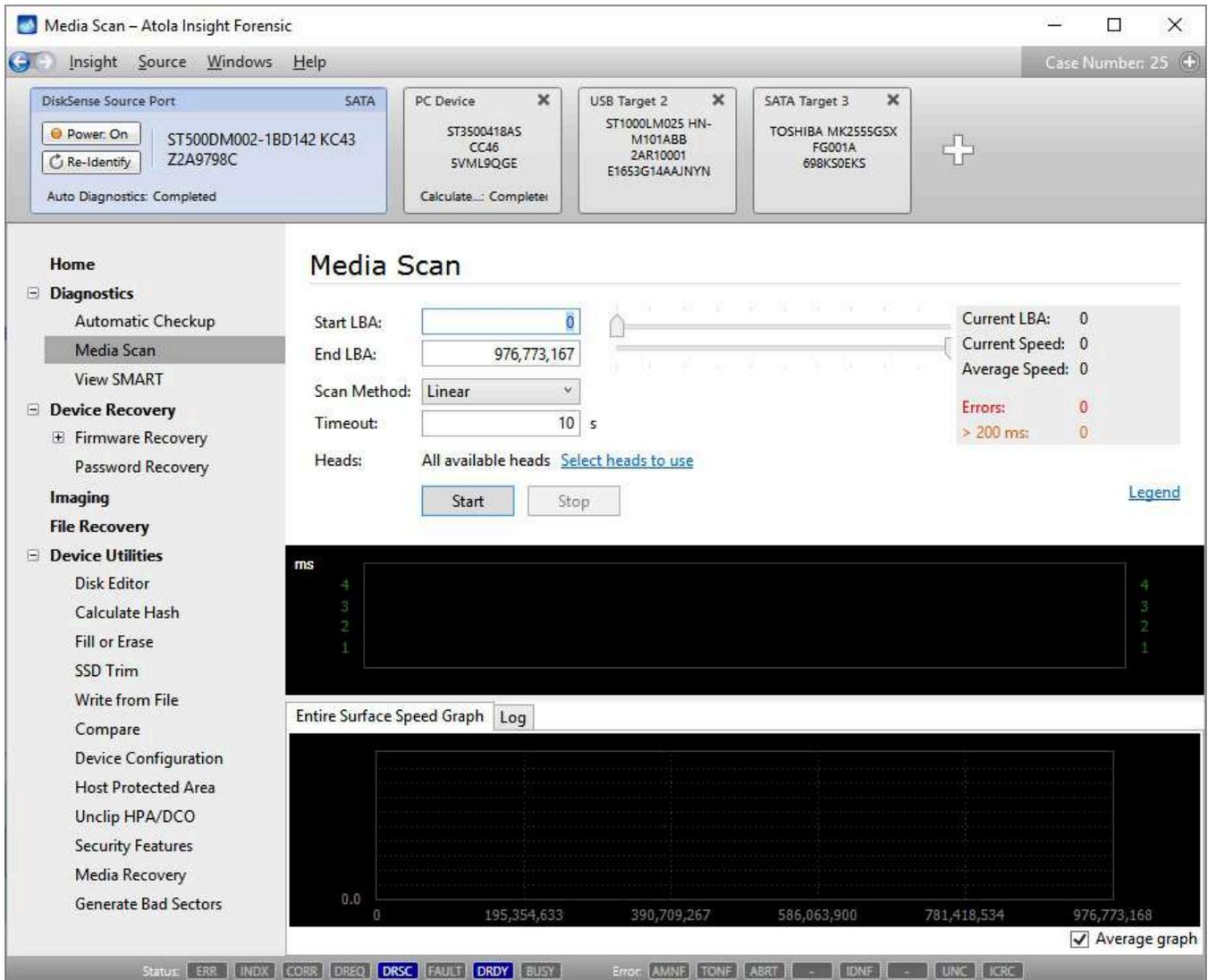
## Final diagnosis

## Media Scan

Media scan can help detect two kind of hard drive damage:

- Head stack damage
- Read errors ("bad sectors")

Media scan can also be used to determine general condition of the hard drive's surface.

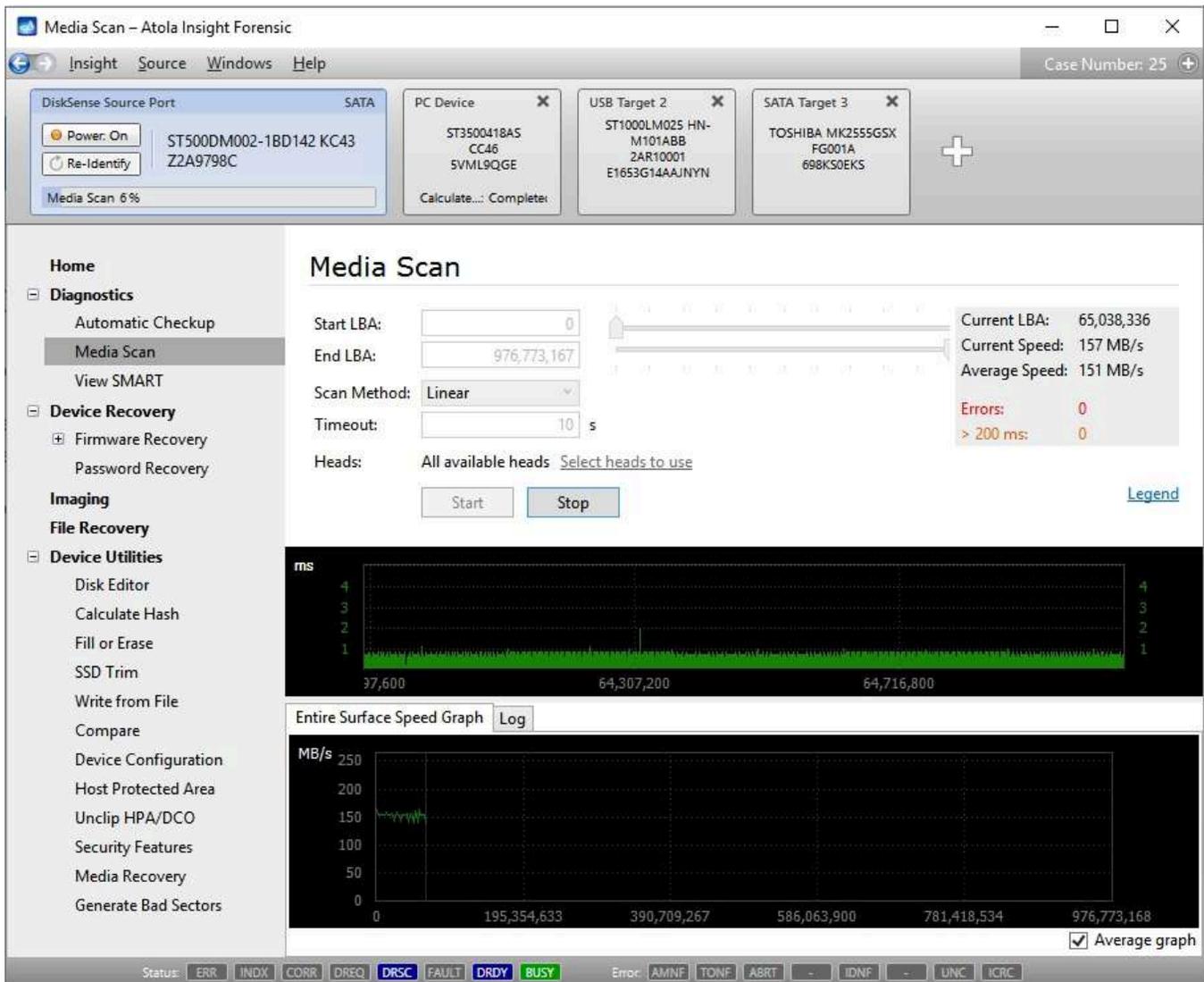


There are three methods of scanning:

- Linear — from start LBA to end LBA.
- Backward — from end LBA to start LBA (in reverse).
- Fast — from start LBA to end LBA. Please note that in this mode the software skips large numbers of sectors; this mode is to be used only to get a quick overview of the entire surface.

Let's scan a good hard drive and see what we get.

# Good hard drive



## Drive without bad sectors

There are two graphs; the top graph represents single block read time (one block is 2048 sectors which equals to 1 megabyte), and the bottom graph represents read speed for the entire surface.

Now let's have a look at some graphs taken from damaged hard drives.

# Unstable hard drive

The screenshot shows the Atola Insight Forensic Media Scan interface. The top bar displays the case number 22 and navigation options. Below the top bar, there are four device selection boxes: DiskSense Source Port (SATA), PC Device, USB Target 2, and SATA Target 1. The DiskSense Source Port box is selected and shows a WDC WD5000AAKS-00V1A0... drive with a media scan progress bar at 57%. The main area is titled "Media Scan" and contains a progress bar with Start LBA (0) and End LBA (976,773,167). The scan method is set to Linear, and the timeout is 10 seconds. The current LBA is 562,092,032, with a current speed of 105 MB/s and an average speed of 114 MB/s. The error statistics show 5 errors and 9 errors greater than 200 ms. A speed graph below the progress bar shows read times in milliseconds, with a peak of 90 ms. The log below the graph shows several read errors, including "Block (256 sectors) read time > 200 ms" and "Cannot read block of data" (Error: UNC).

**Media Scan**

Start LBA: 0  
End LBA: 976,773,167  
Scan Method: Linear  
Timeout: 10 s  
Heads: Not available

Current LBA: 562,092,032  
Current Speed: 105 MB/s  
Average Speed: 114 MB/s  
Errors: 5  
> 200 ms: 9

ms

Date	Message
3/29/2014 12:41:34 PM	Block (256 sectors) read time > 200 ms at: 500,066,304
3/29/2014 12:42:02 PM	Block (256 sectors) read time > 200 ms at: 500,494,336
3/29/2014 12:42:24 PM	Cannot read block of data at 500,600,832 - 500,602,879 (Error: UNC)
3/29/2014 12:42:29 PM	Block (256 sectors) read time > 200 ms at: 500,617,216
3/29/2014 12:42:34 PM	Block (256 sectors) read time > 200 ms at: 500,635,648
3/29/2014 12:42:41 PM	Cannot read block of data at 500,668,416 - 500,670,463 (Error: UNC)
3/29/2014 12:51:14 PM	Block (256 sectors) read time > 200 ms at: 559,011,840

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

We call such hard drives "unstable". They usually do not have read errors, but at the same time media access times are very high and change sporadically. In most cases it is possible to create a clean image of such drive.

# Hard drive with damaged head

The screenshot shows the Atola Insight Forensic Media Scan interface. The top bar indicates the case number is 24. The main window displays the scan progress for a SATA drive (WDC WD30EZRS-00J99B0 80...). The scan is currently at 0% completion. The interface shows the following settings:

- Start LBA: 0
- End LBA: 5,860,533,167
- Scan Method: Linear
- Timeout: 10 s
- Heads: Head 0, Head 1, Head 2, Head 3, Head 4, Head 5, Head 6, Head 7 (all checked)
- Do not use head map:

The scan progress bar shows the current LBA is 2,395,856, with a current speed of 396 KB/s and an average speed of 114 MB/s. The error statistics are:

- Errors: 48
- > 200 ms: 9

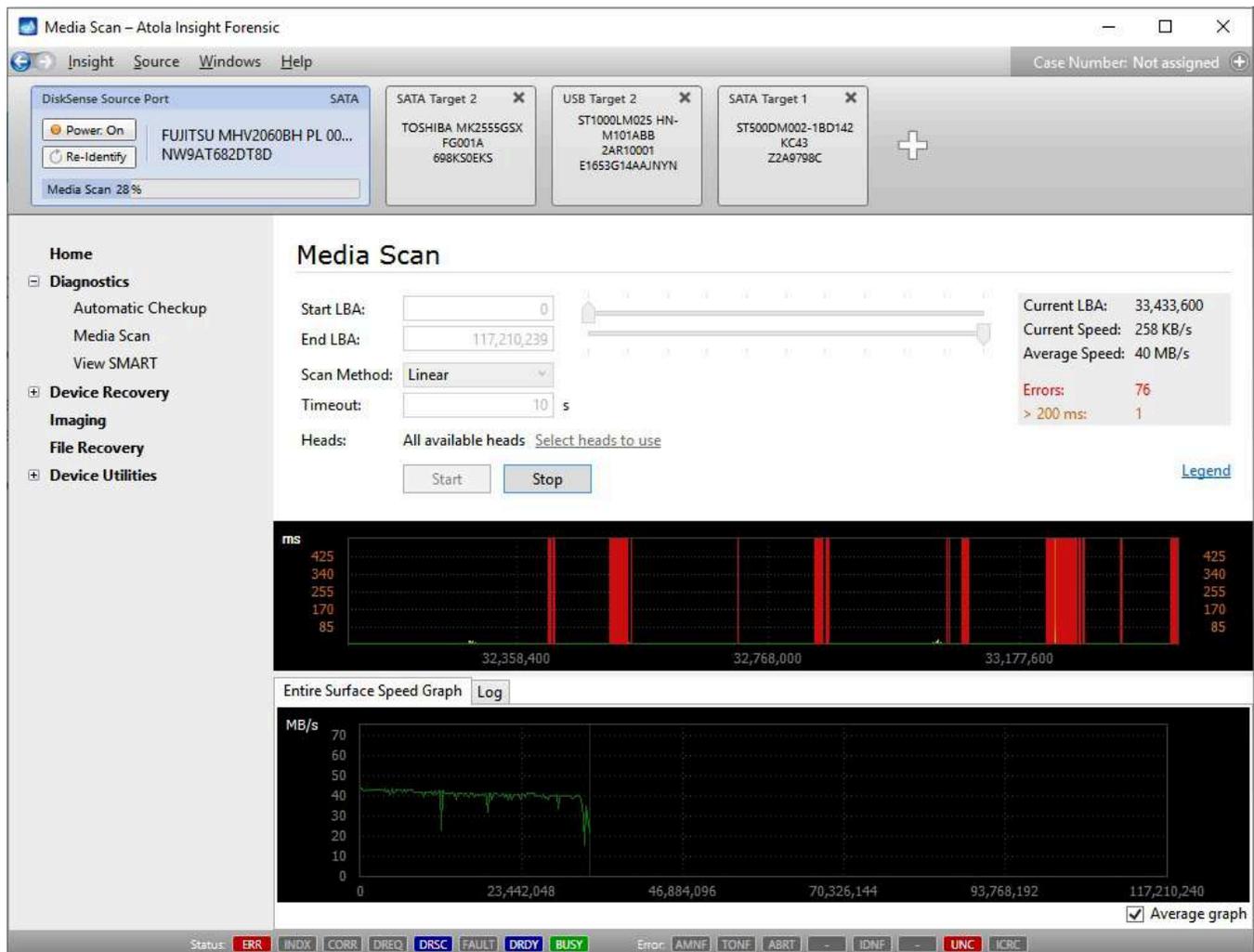
The interface also shows a legend for Head #6 and a graph of the entire surface speed. The graph shows a significant increase in delay (ms) for Head 6, indicating damage. The log shows the following errors:

Date	Message
3/29/2014 3:37:03 PM	Cannot read block of data at 2,367,184 - 2,369,231 Head: 6 (Error: UNC)
3/29/2014 3:37:05 PM	Block (256 sectors) read time > 200 ms at: 2,369,232 Head: 6
3/29/2014 3:37:08 PM	Cannot read block of data at 2,371,280 - 2,373,327 Head: 6 (Error: UNC)
3/29/2014 3:37:16 PM	Cannot read block of data at 2,393,808 - 2,395,855 Head: 6 (Error: UNC)
3/29/2014 3:37:18 PM	Cannot read block of data at 2,395,856 - 2,397,903 Head: 6 (Error: UNC)

The status bar at the bottom shows the status as ERR, INDX, CORR, DREQ, DRSC, FAULT, DRDY, BUSY, Error: AMNF, TONF, ABRT, IDNF, UNC, ICRC.

You can observe patterns of delays which indicate head damage. However, please note that although the head is damaged, it can still read *some* sectors without errors, therefore it is possible to create a relatively good image of such hard drive by imaging data off good heads first, and then off the bad head.

# Read errors



Read errors are displayed as vertical red bars. Please note that when scanning, Atola Insight Forensic shows the entire block as bad even when only one sector in that block is damaged.

## Tracking SMART table status before/after imaging

Being able to evaluate the drive's state before it has exhausted its resources can make all the difference between a case won or a case lost in a court of law.

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

To view SMART table of a drive:

1. In the sidebar, go to **Diagnostics > View SMART**.
2. Click **Read SMART**.

View SMART – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 78345

DiskSense Source Port: SATA Multitasking

Power: On Re-Identify Hitachi HTS545032B9SA00 P... 091130PBP301Q6E630HM

SMART Report: Completed

Find Operation

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART**

Device Recovery

Imaging

File Recovery

Scripting

Hashing

Device Utilities

## View SMART

Read SMART  Show raw values in HEX

SMART RETURN STATUS: Good

#	Attribute Name	Value	Worst	Threshold	RAW	Status
1	Read error rate	93	93	62	524,311	OK
2	Throughput performance	100	100	40	0	OK
3	Spin up time	149	149	33	90,194,313,218	OK
4	Number of spin-up times	97	97	0	5,827	OK
5	Reallocated sectors count	78	78	5	0	OK
7	Seek error rate	100	100	67	0	OK
8	Seek performance	100	100	40	0	OK
9	Power-on time	65	65	0	15,424	OK
10	Spin-up retries	100	100	60	0	OK
12	Power Cycles	97	97	0	5,621	OK
191	G-Sensor trigger rate	100	100	0	0	OK
192	Power-off retract count	99	99	0	357	OK
193	Load/unload cycle count	84	84	0	162,112	OK
194	HDA Temperature	239	239	0	214,747,971,607	OK
196	Reallocate event count	100	100	0	222	OK
197	Current pending sectors	83	83	0	1,221	OK
198	Offline scan UNC sectors	100	100	0	0	OK
199	Ultra ATA CRC Error Rate	200	200	0	0	OK
223	Load retry count	100	100	0	0	OK

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

## Hitachi drive with 1221 pending sectors

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, Insight highlights it in yellow.

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

## Compare SMART tables

To keep track of the changes occurring to the attributes of the SMART table, Insight records SMART table indices prior and after each imaging session.

To open both SMART tables for side-by-side comparison:

1. After the imaging is completed, check the **Imaging Results**.
2. In **SMART data** line, click the **View** link.

The screenshot shows the 'Imaging Results' window in Atola Insight Forensic. The window title is 'Imaging Results - Atola Insight Forensic'. The interface includes a navigation menu on the left with options like 'Home', 'Diagnostics', 'Device Recovery', 'Imaging', 'File Recovery', 'Scripting', 'Hashing', and 'Device Utilities'. The main content area displays the following information:

- Imaging Results** (with a 'Back to sessions' link)
- SATA Target 1: Hitachi HDS721010DLE630 / MSK523Y20LJ29F
- Buttons: Resume, Analyze target image
- Sectors scheduled: 625,142,448
- Sectors imaged: 625,130,818 (with links for 'Export imaged sectors' and 'Export non-imaged sectors')
- Errors: 11,630 (with a link for 'Export sectors with errors')
- Copy range: All sectors
- Start sector in range: 0
- End sector in range: 625,142,447
- SMART data: [View](#) (indicated by a red arrow)
- File signatures: [659,850](#)

Below the statistics is a 'Log' section with a table of events:

Date	Message
9/13/2017 9:59:51 AM	Imaging started
9/13/2017 9:59:56 AM	Cannot read block of data at 311,296 - 315,391 (Timeout)
9/13/2017 9:59:58 AM	Cannot read block of data at 1,311,296 - 1,315,391 (Timeout)
9/13/2017 10:00:00 AM	Cannot read block of data at 2,327,680 - 2,331,775 (Timeout)
9/13/2017 10:00:17 AM	Cannot read block of data at 5,560,000 - 5,564,095 (Timeout)
9/13/2017 10:00:22 AM	Cannot read block of data at 7,010,560 - 7,014,655 (Timeout)
9/13/2017 10:02:05 AM	Cannot read block of data at 23,530,304 - 23,534,399 (Timeout)
9/13/2017 10:02:07 AM	Cannot read block of data at 24,530,304 - 24,534,399 (Timeout)
9/13/2017 10:02:25 AM	Cannot read block of data at 26,857,408 - 26,861,503 (Timeout)
9/13/2017 10:02:31 AM	Cannot read block of data at 28,299,776 - 28,303,871 (Timeout)

The status bar at the bottom shows various indicators: Link: PHY, Status: ERR, INDX, CORR, DREQ, DRSC, FAULT, DRDY, BUSY, Error: AMNF, TONF, ABRT, IDNF, UNC, ICRC.

By comparing the two tables, operator 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.

Before Imaging						After Imaging							
SMART RETURN STATUS: Good						SMART RETURN STATUS: Threshold exceeded							
#	Attribute Name	Value	Worst	Threshold	RAW	Status	#	Attribute Name	Value	Worst	Threshold	RAW	Status
1	Read error rate	93	93	62	524,311	OK	1	Read error rate	44	44	62	1,582,759,936	FAIL
2	Throughput performance	100	100	40	0	OK	2	Throughput performance	100	100	40	0	OK
3	Spin up time	149	149	33	90,194,313,218	OK	3	Spin up time	144	144	33	90,194,313,218	OK
4	Number of spin-up times	97	97	0	5,827	OK	4	Number of spin-up times	97	97	0	5,838	OK
5	Reallocated sectors count	78	78	5	0	OK	5	Reallocated sectors count	1	1	5	0	FAIL
7	Seek error rate	100	100	67	0	OK	7	Seek error rate	100	100	67	0	OK
8	Seek performance	100	100	40	0	OK	8	Seek performance	100	100	40	0	OK
9	Power-on time	65	65	0	15,424	OK	9	Power-on time	65	65	0	15,444	OK
10	Spin-up retries	100	100	60	0	OK	10	Spin-up retries	100	100	60	0	OK
12	Power Cycles	97	97	0	5,621	OK	12	Power Cycles	97	97	0	5,632	OK
191	G-Sensor trigger rate	100	100	0	0	OK	191	G-Sensor trigger rate	100	100	0	0	OK
192	Power-off retract count	99	99	0	357	OK	192	Power-off retract count	99	99	0	367	OK
193	Load/unload cycle count	84	84	0	162,112	OK	193	Load/unload cycle count	84	84	0	162,124	OK
194	HDA Temperature	239	239	0	214,747,971,607	OK	194	HDA Temperature	171	171	0	214,747,971,616	OK
196	Reallocate event count	100	100	0	222	OK	196	Reallocate event count	79	79	0	1,359	OK
197	Current pending sectors	83	83	0	1,221	OK	197	Current pending sectors	19	19	0	4,005	OK
198	Offline scan UNC sectors	100	100	0	0	OK	198	Offline scan UNC sectors	100	100	0	0	OK
199	Ultra ATA CRC Error Rate	200	200	0	0	OK	199	Ultra ATA CRC Error Rate	200	200	0	0	OK
223	Load retry count	100	100	0	0	OK	223	Load retry count	100	100	0	0	OK

## How SMART table state changed after image acquisition

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

## Image to a file on a target device

Atola Insight Forensic with DiskSense 2 hardware unit supports imaging to a file on a target device. You can save a bit-by-bit image of a source device to a file on a target device in one of the following formats:

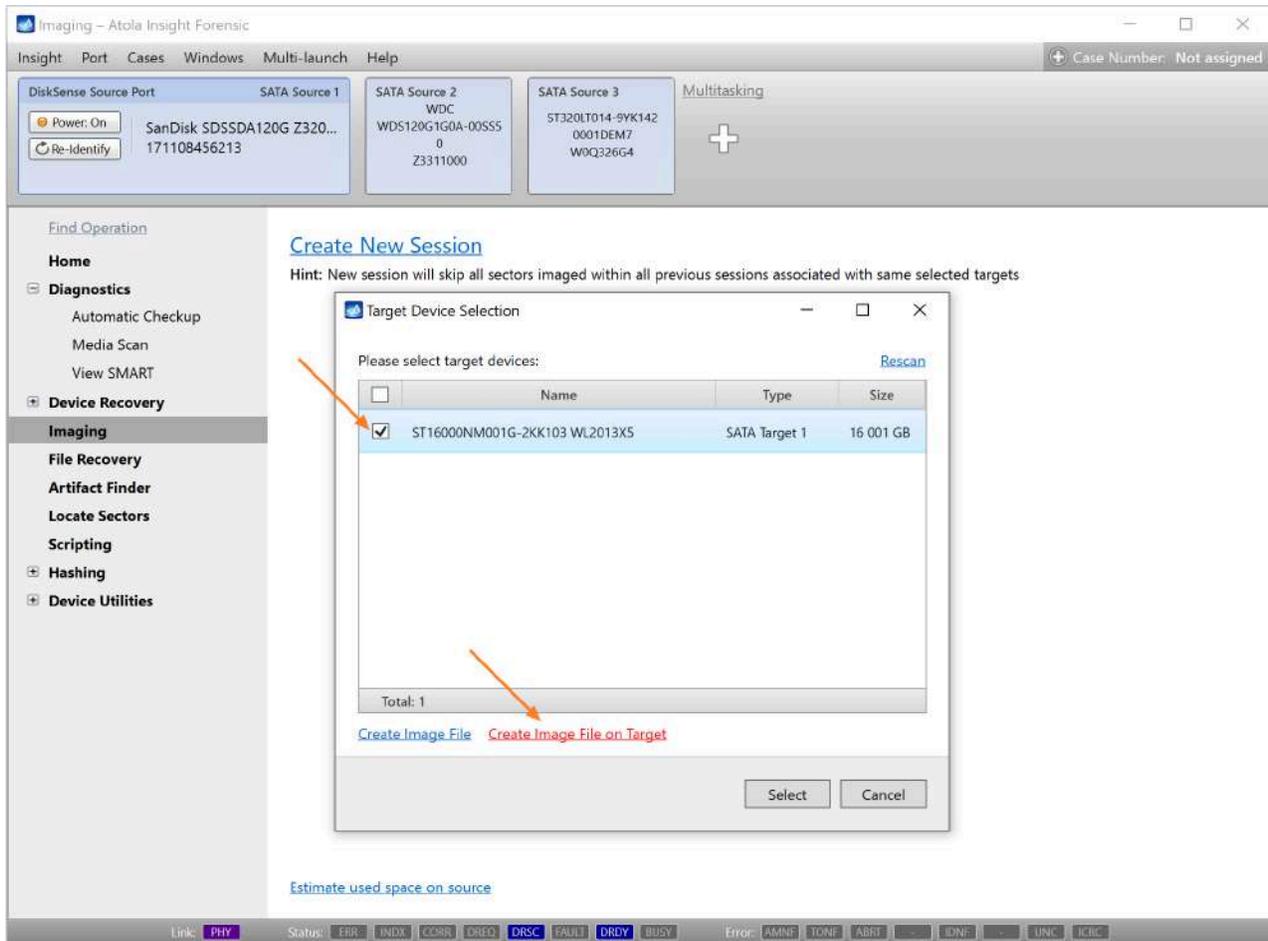
- Raw image file (growing)
- Preallocated raw image file
- E01 file

In order to create an image file on a target device, Atola Insight Forensic formats that device and creates a single exFAT partition with 32 MB cluster size.

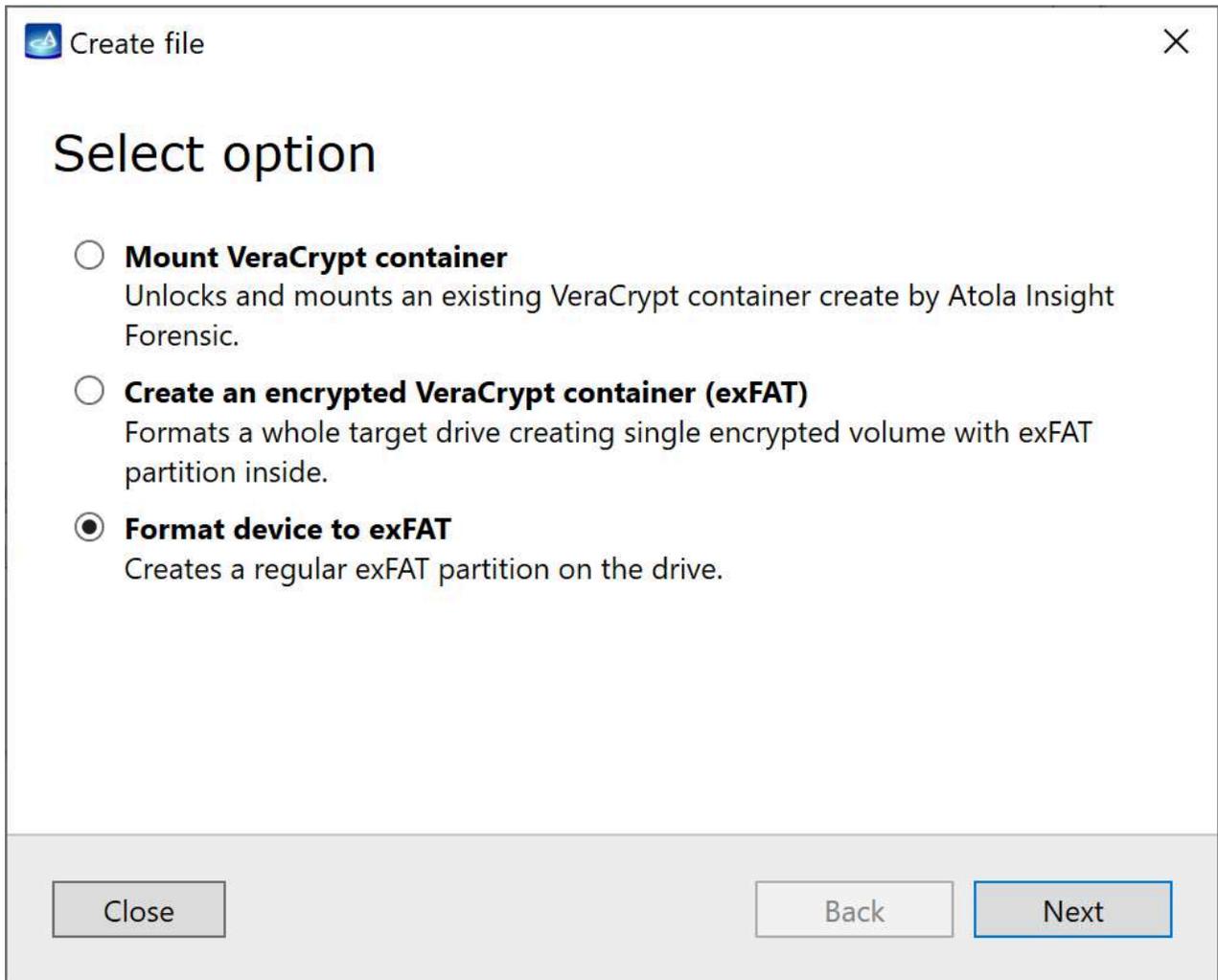
To image a source device to an image file on a target device, do the following:

1. Connect source and target devices to DiskSense 2 hardware unit.
2. In the sidebar, go to **Imaging**.
3. Click **Create New Session**.

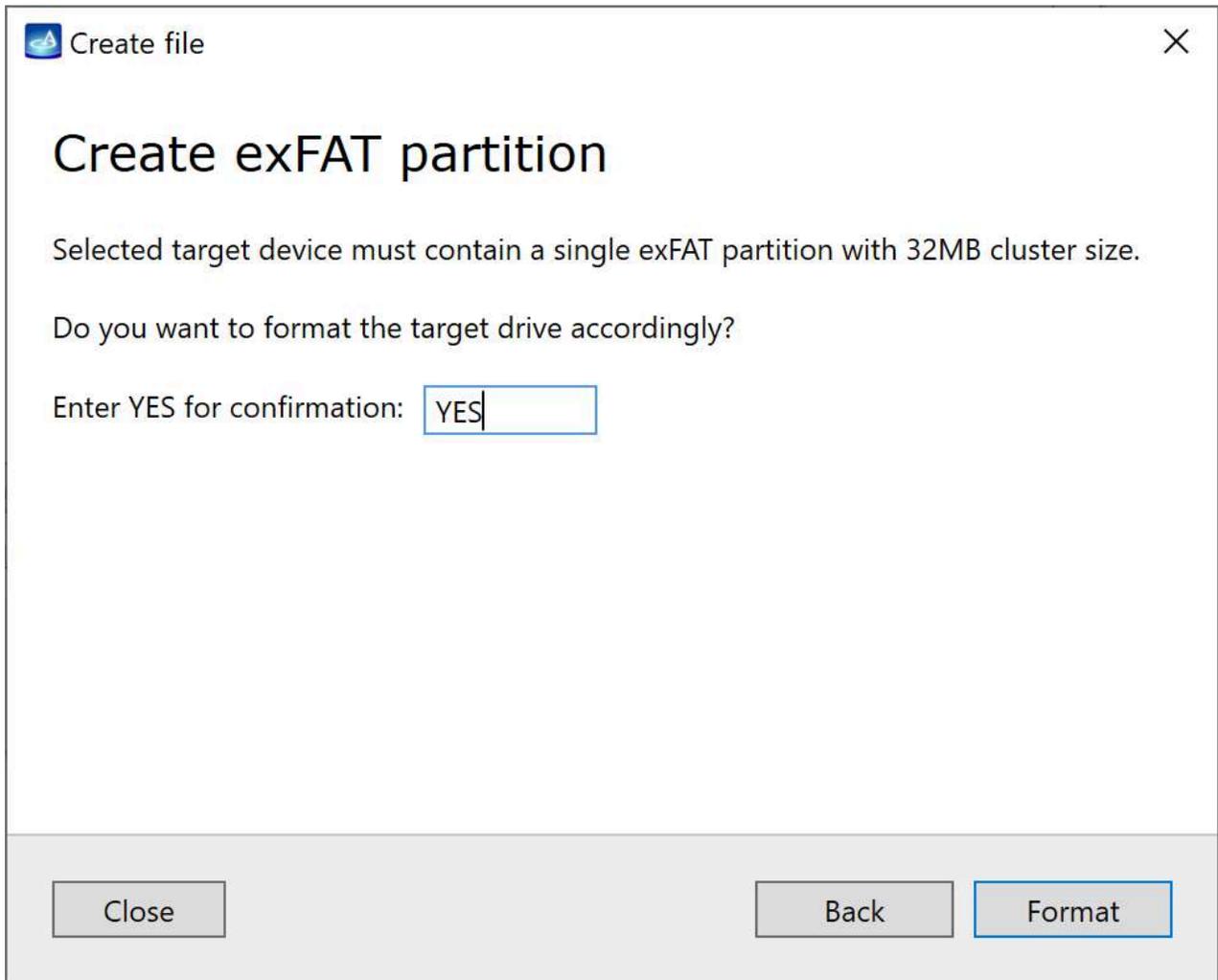
4. In the Target Device Selection dialog, select target device and then click **Create Image File on Target** link.



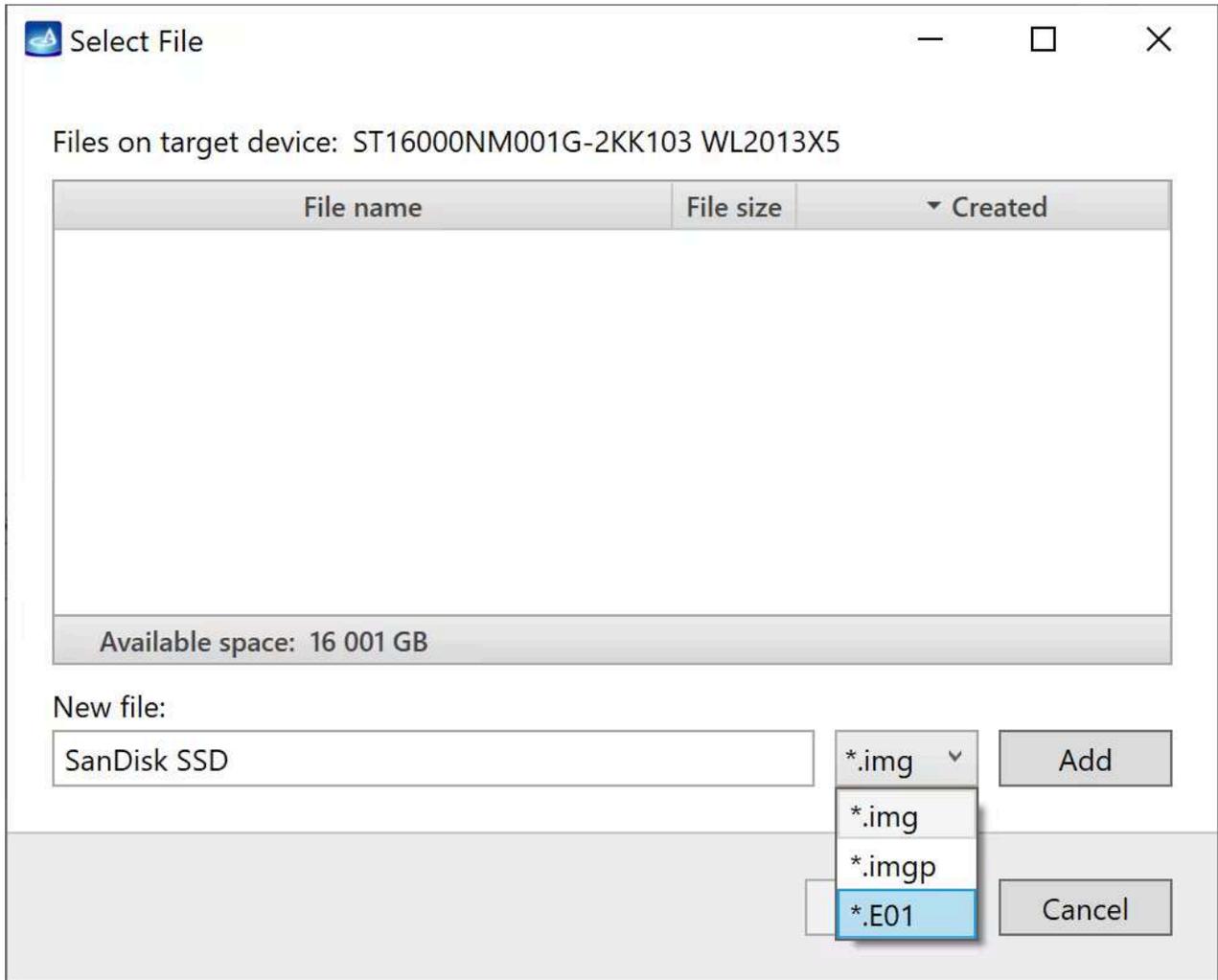
5. In the Create file dialog, select **Format device to exFAT** and then click **Next**.



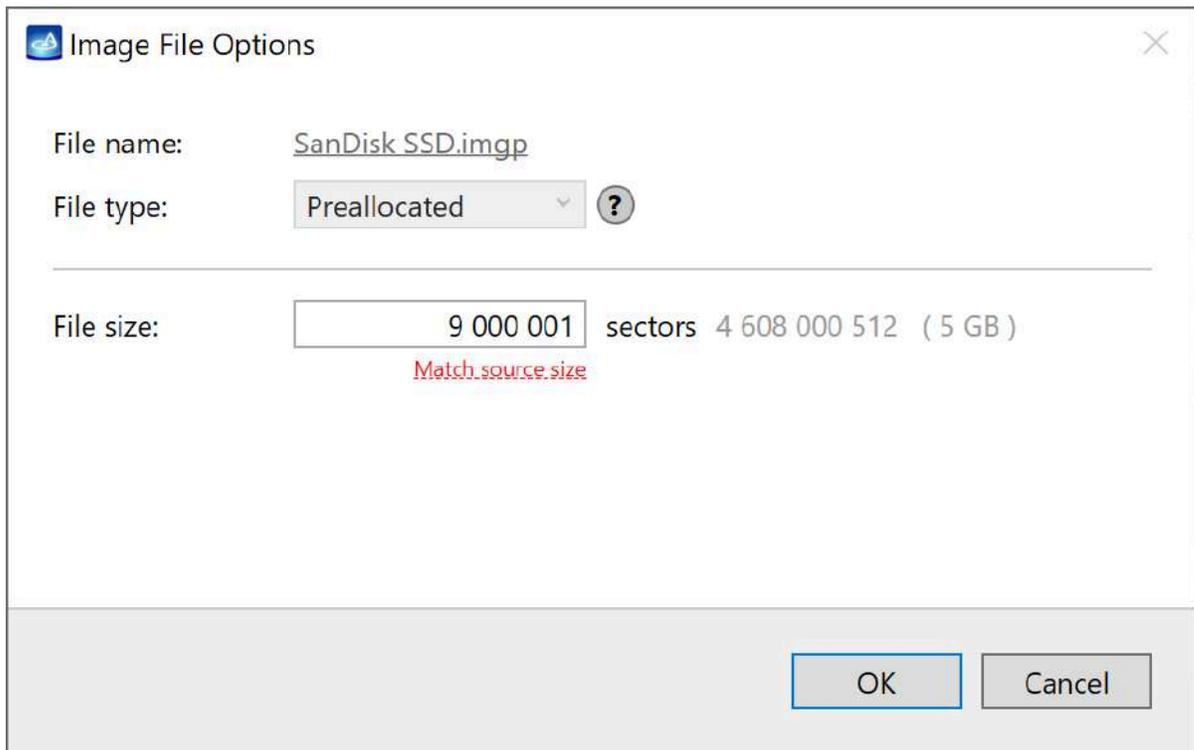
6. To confirm formatting of the target device, enter **YES** and then click **Format**. On the target device, Atola Insight Forensic creates a regular exFAT partition with 32 MB cluster size.



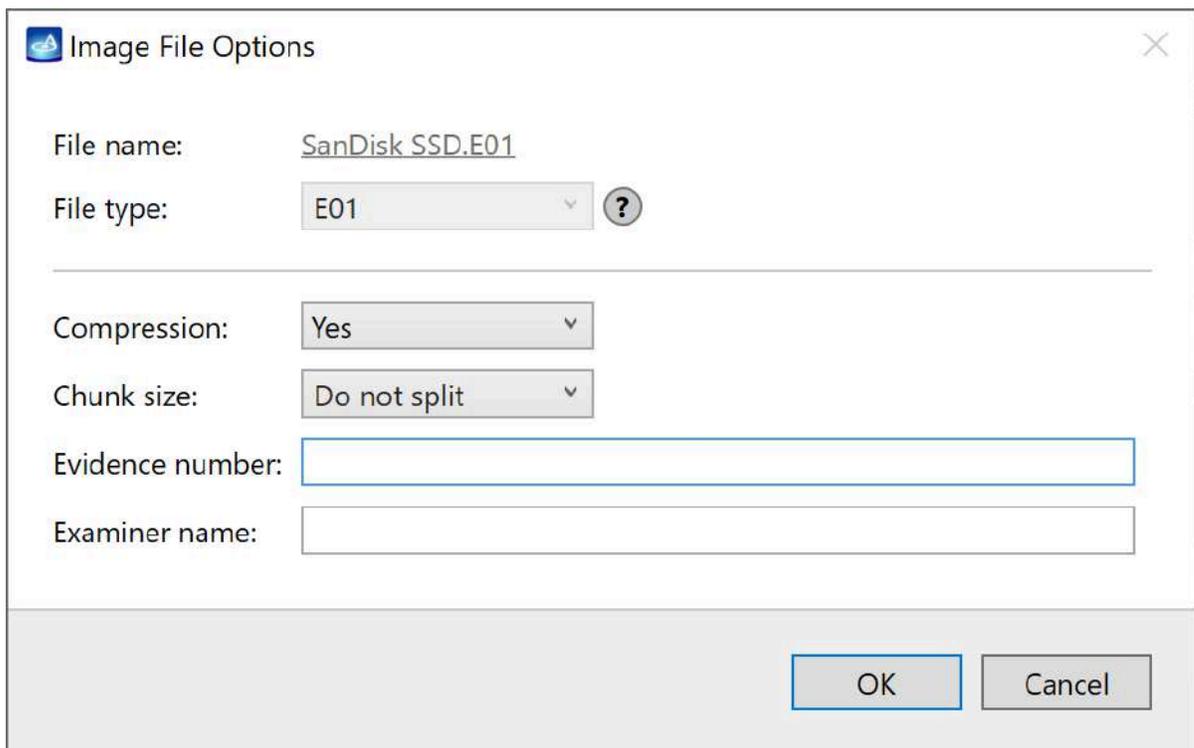
7. In the **Select File** dialog, enter filename in the **New file** field, select file extension and then click **Add**.



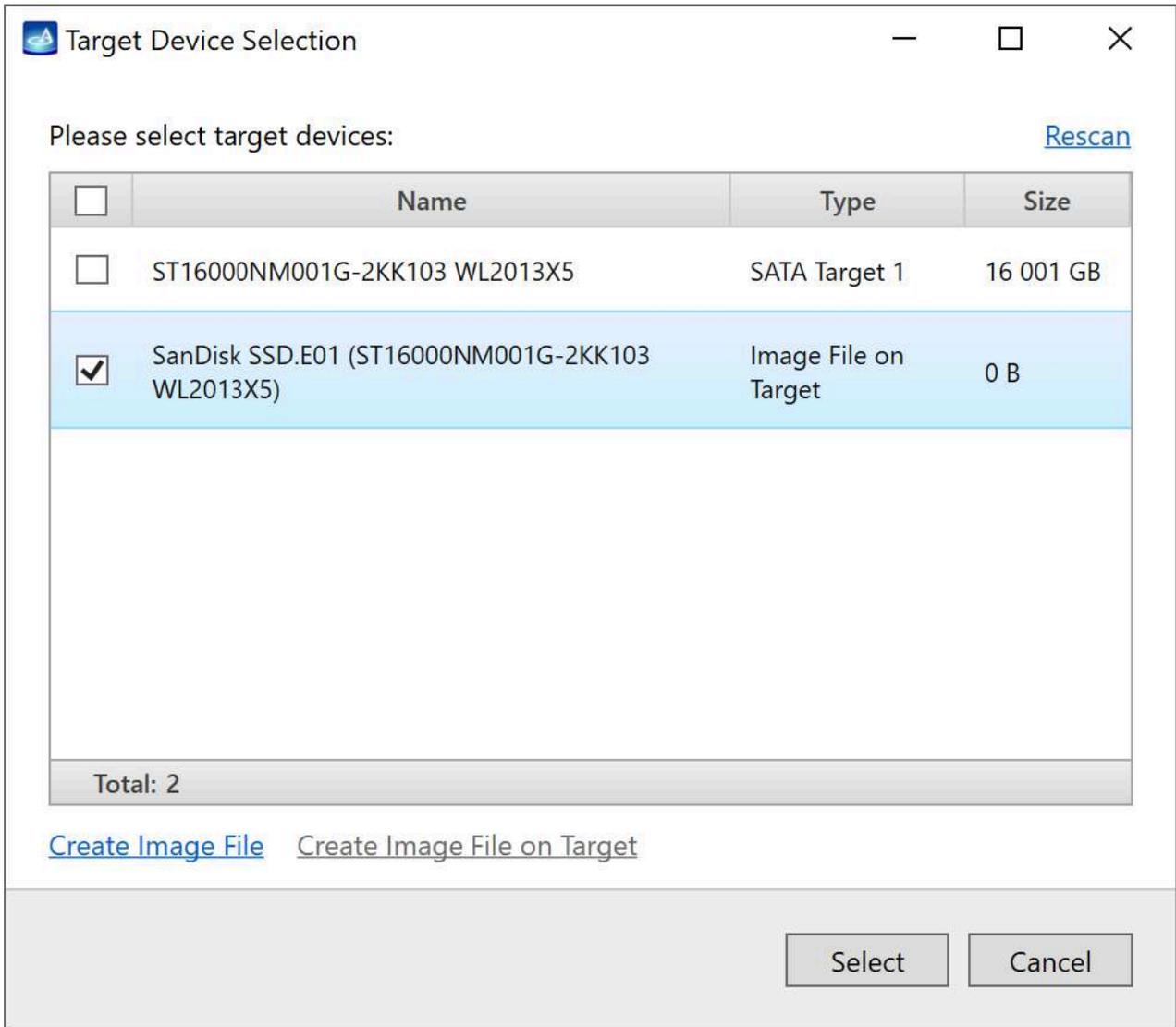
- For Preallocated raw image file (\*.imgp) you can configure file size to match source device size.



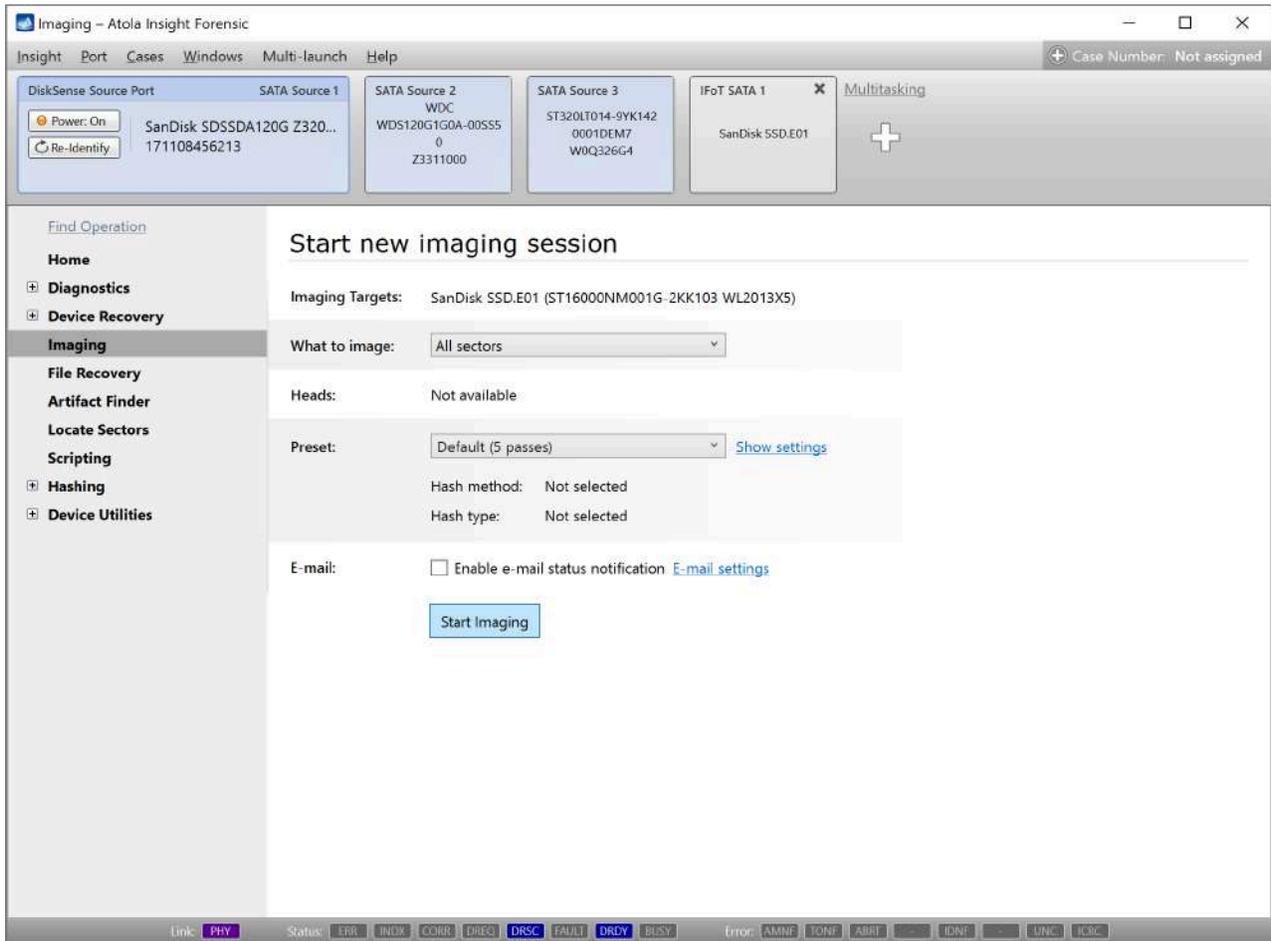
- o For E01 file you can configure compression and chunk size, enter evidence number and examiner name.



8. In the **Target Device Selection** dialog, choose your image file and then click **Select**.



9. Specify the settings for this imaging session and then click **Start Imaging**.



Atola Insight Forensic begins imaging data into the file on the selected target device.

Imaging – Atola Insight Forensic

Insight Port Cases Windows Multi-launch Help Case Number: Not assigned

DiskSense Source Port SATA Source 1  
 Power: On Re-Identify SanDisk SDSSDA120G Z320... 171108456213  
 Imaging 73%

SATA Source 2 WDC WDS120G1G0A-00SS5 0 Z3311000

SATA Source 3 ST320LT014-9YK142 0001DEM7 W0Q326G4

IFoT SATA 1 SanDisk SSD.E01  
 Imaging 73%

Multitasking

Find Operation

- Home
- Diagnosics
- Device Recovery
- Imaging**
- File Recovery
- Artifact Finder
- Locate Sectors
- Scripting
- Hashing
- Device Utilities

Imaging data... 73%

0 9 000 000

Pass: 1 of 5 Sectors imaged: 6 606 848

Overall speed: 83 MB/s Sectors left: 2 393 153

Estimated time left: 15 seconds Last attempted block: 6 606 847

Found signatures: 0 Total errors: 0

Pause Imaging settings Legend Cheat sheet

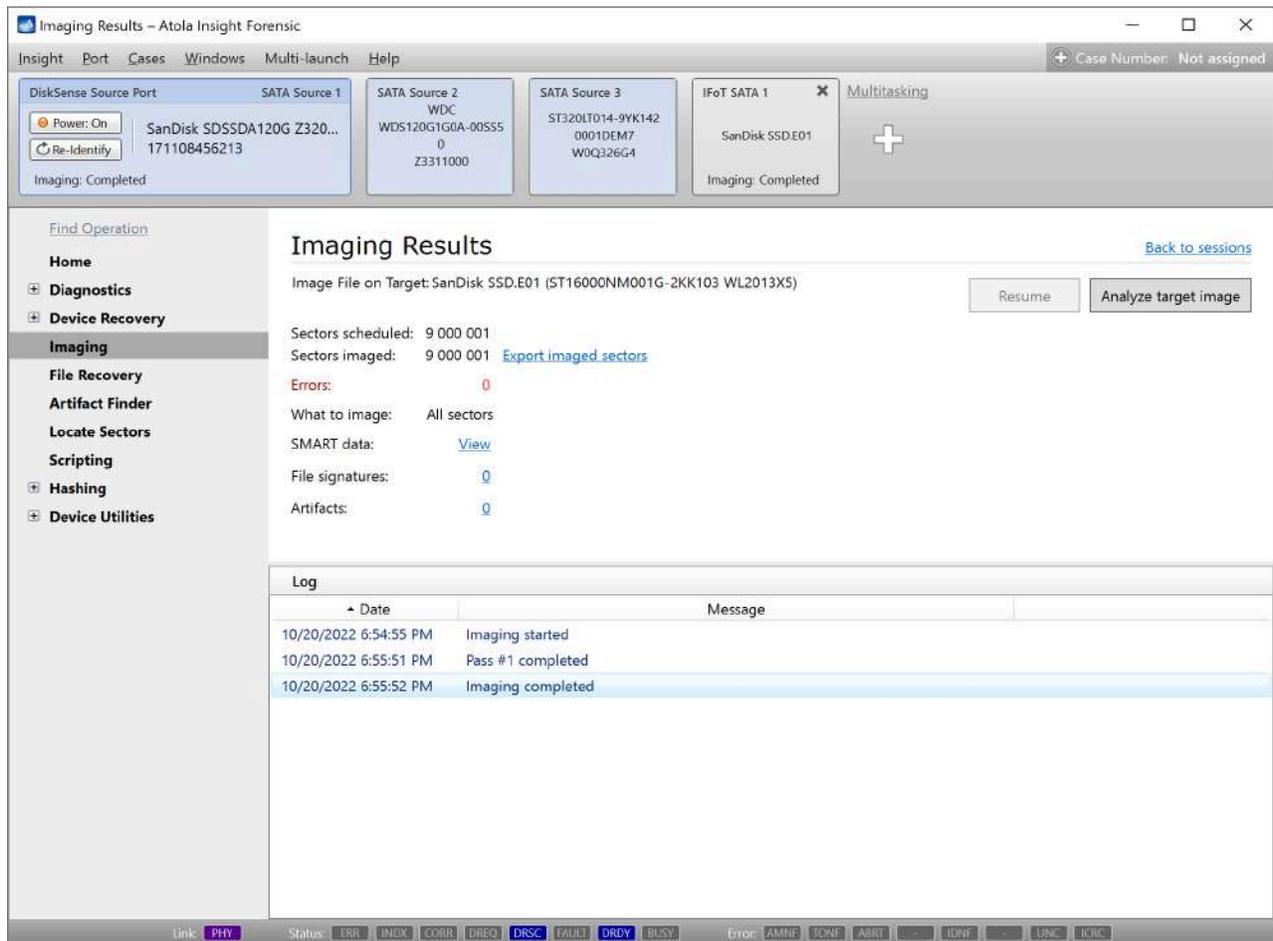
ms

Target Hex Viewer Log Artifacts: 0 Entropy

Date	Message
10/20/2022 6:54:55 PM	Imaging started

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

After the imaging is completed, check the Imaging Results.



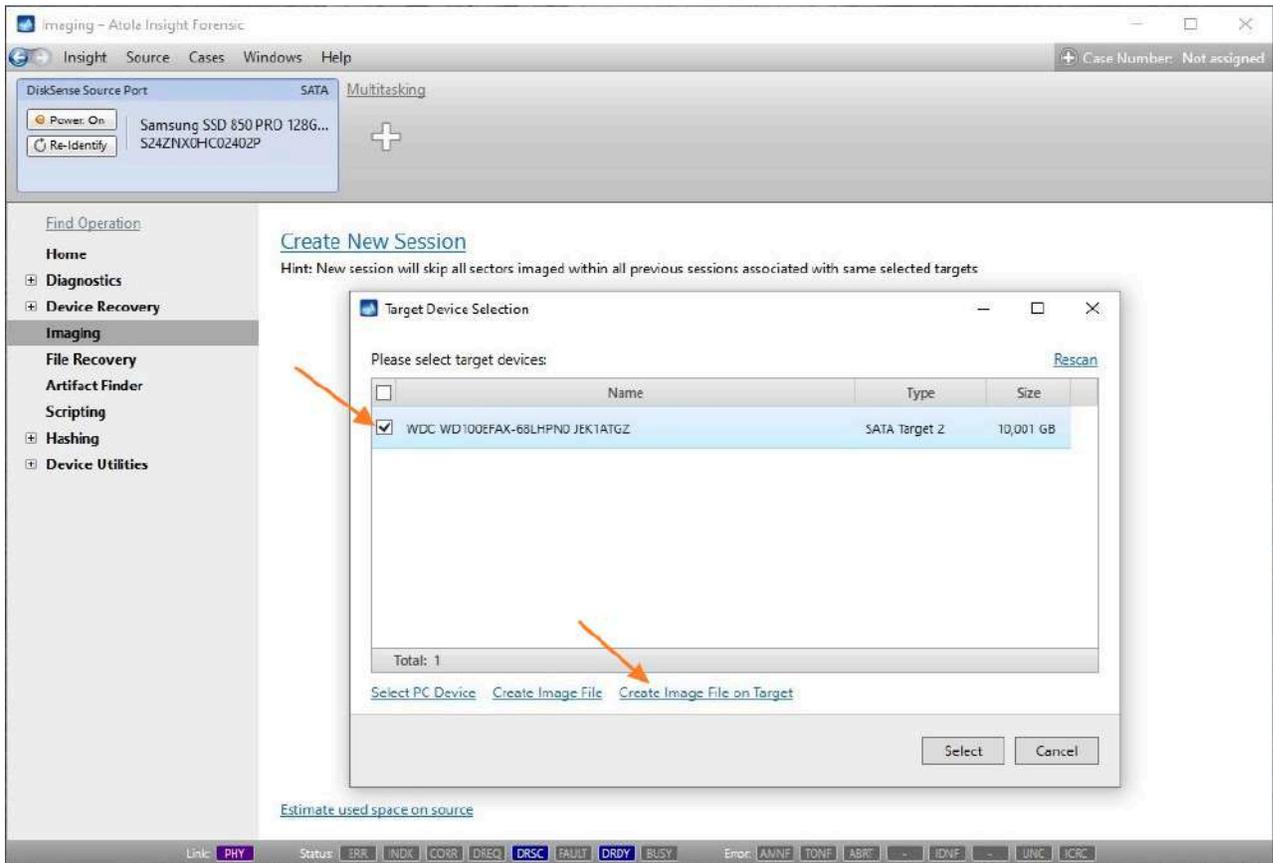
## Imaging into a file on an encrypted target

Atola Insight Forensic supports imaging into a file on an encrypted target drive, using VeraCrypt for data encryption.

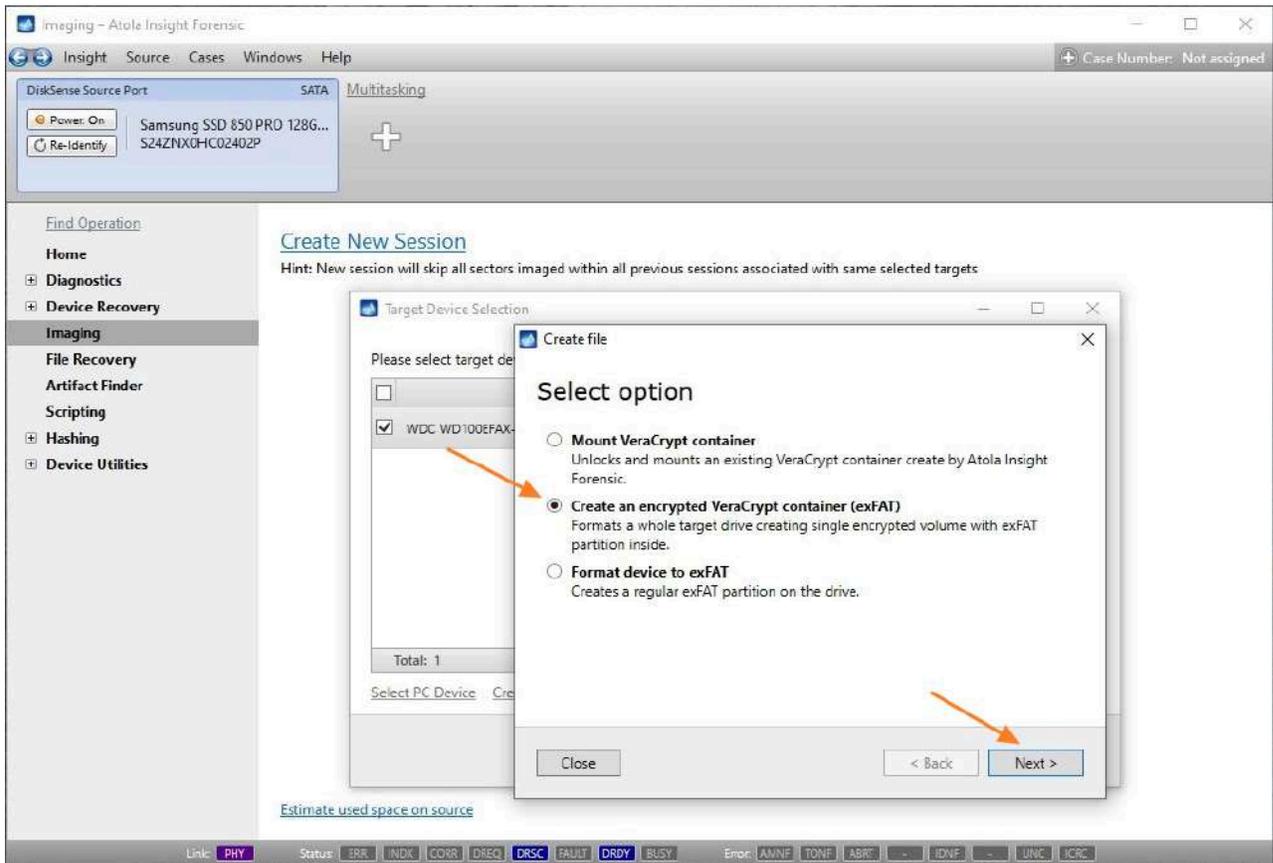
## Create an encrypted target volume

After your source drive is identified by the system perform these steps:

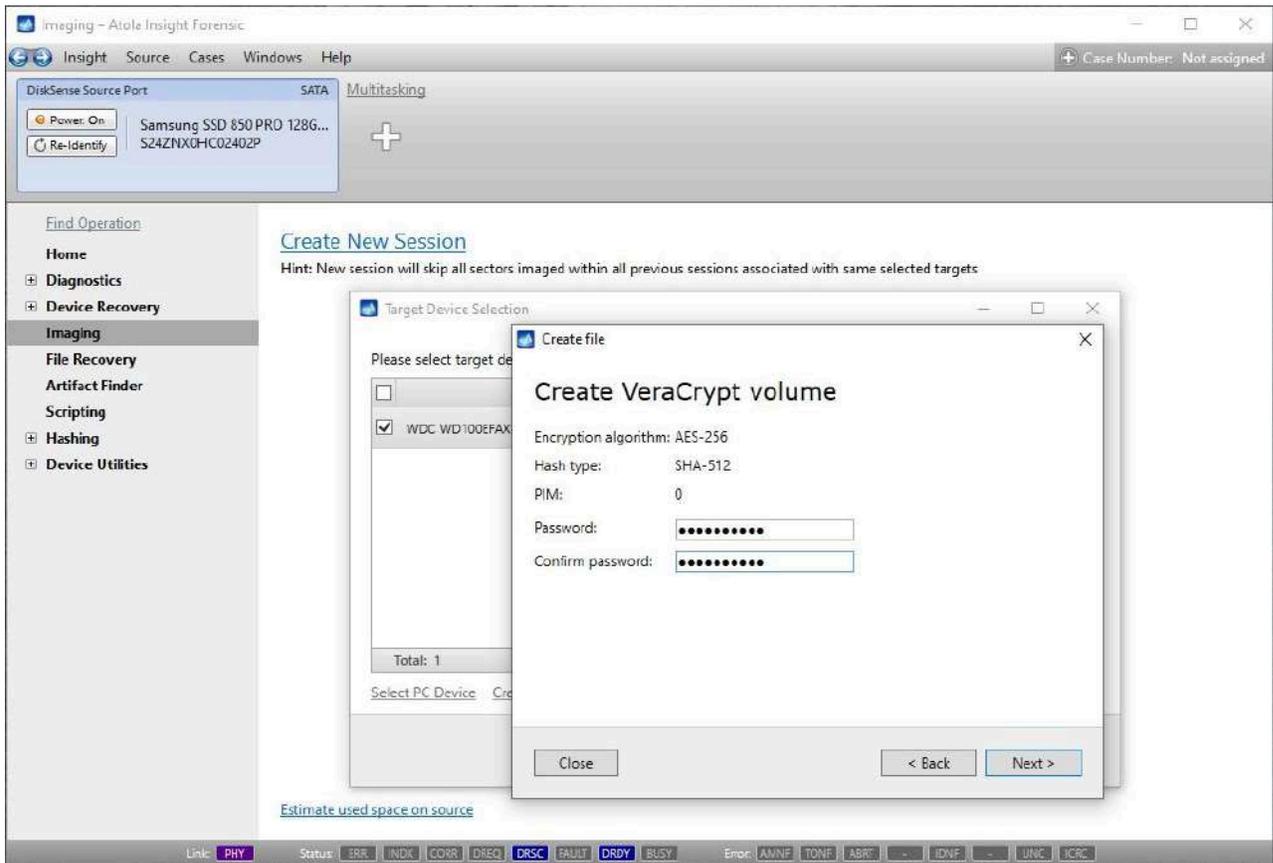
1. In the sidebar, go to **Imaging**.
2. Click **Create New Session**.
3. In the **Target Device Selection** dialog, select target device and then click **Create Image File on Target** link.



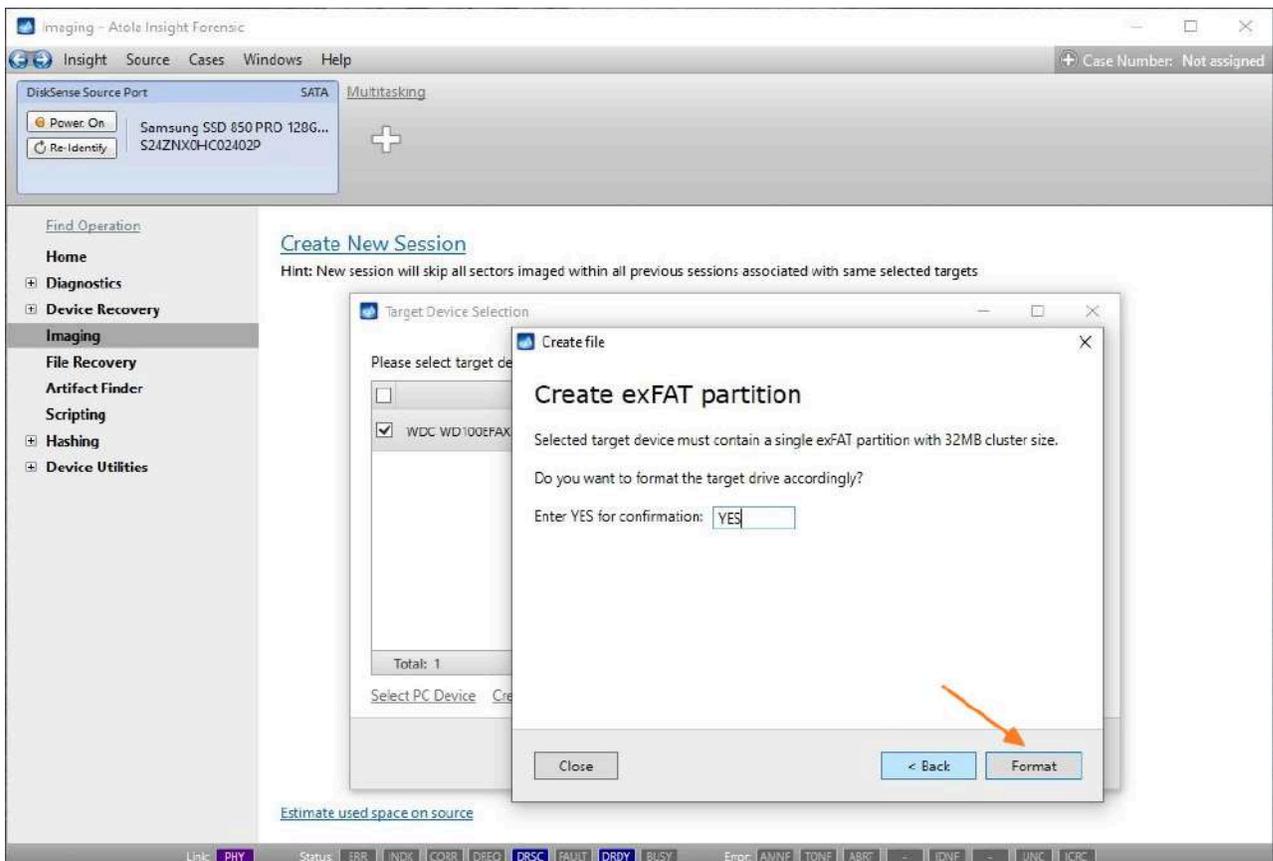
4. In the Create file dialog, select Create an encrypted VeraCrypt container (exFAT) and click Next.



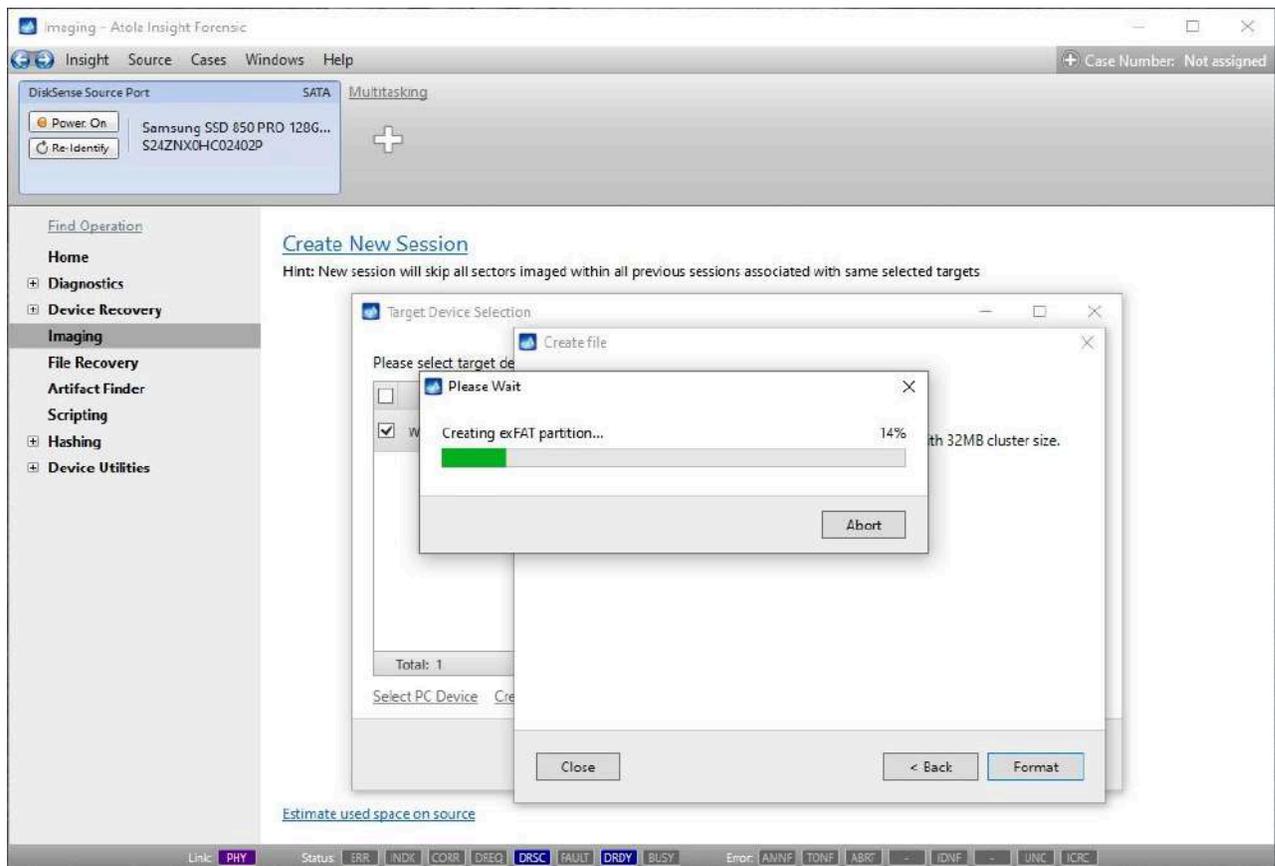
5. To complete the creation of a VeraCrypt volume, enter the password and click **Next**.



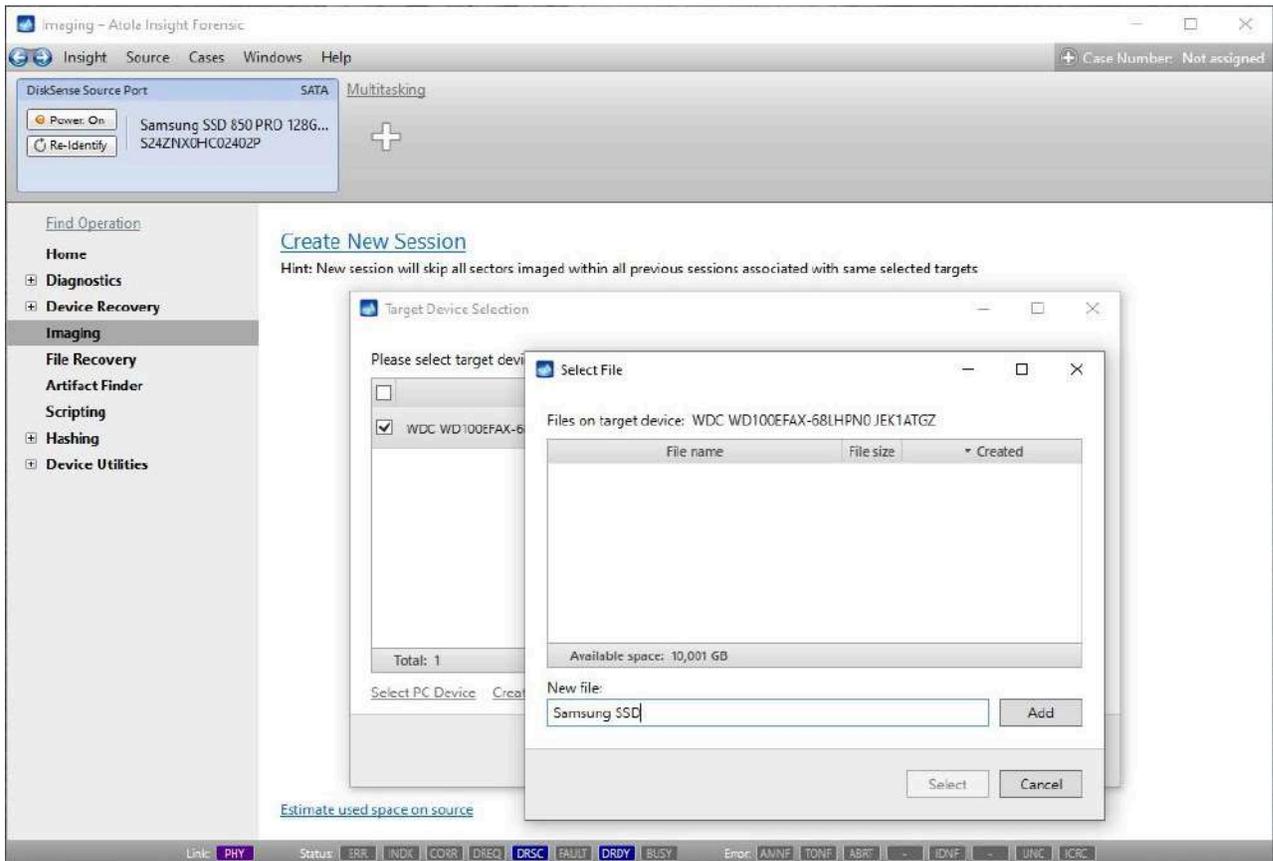
6. To confirm formatting the drive to create the encrypted partition, enter YES and then click **Format**.



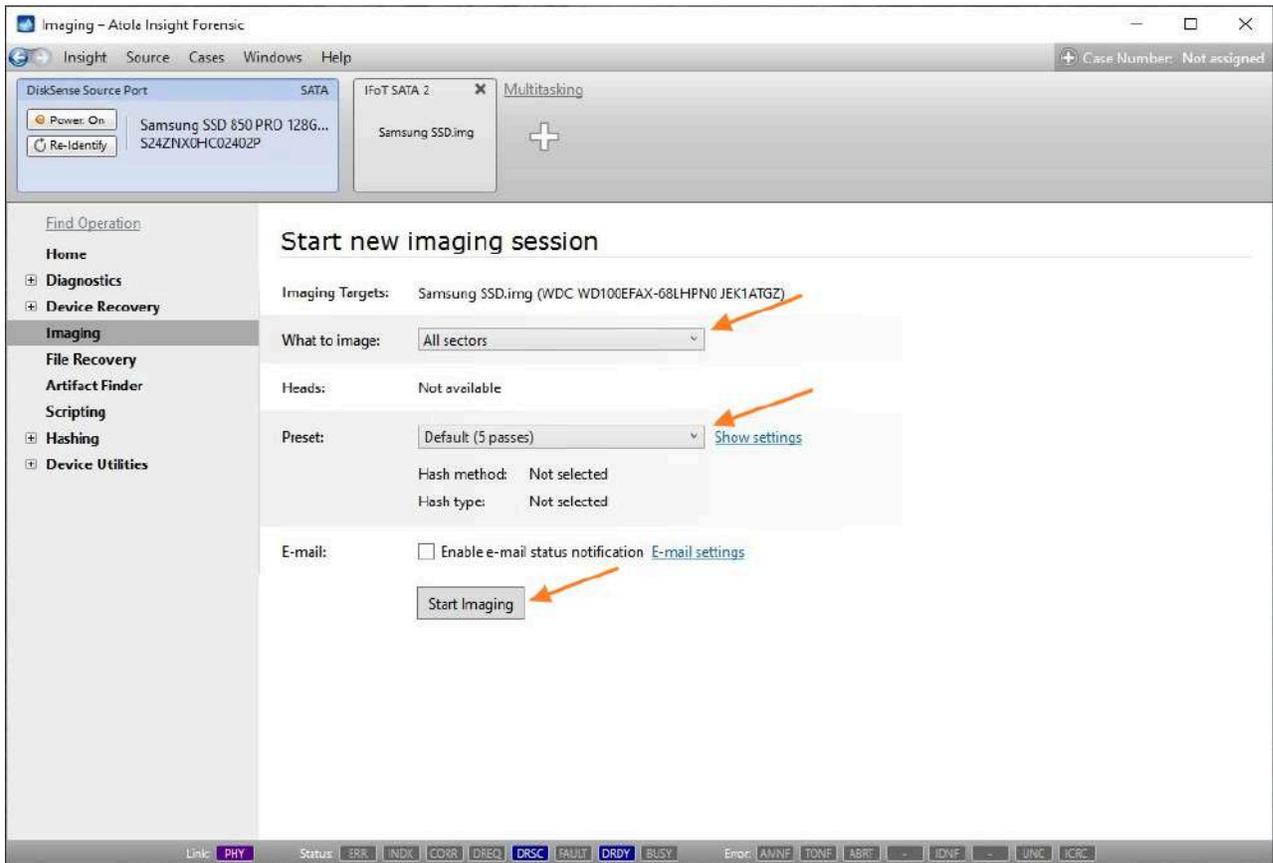
Formatting takes a few seconds.



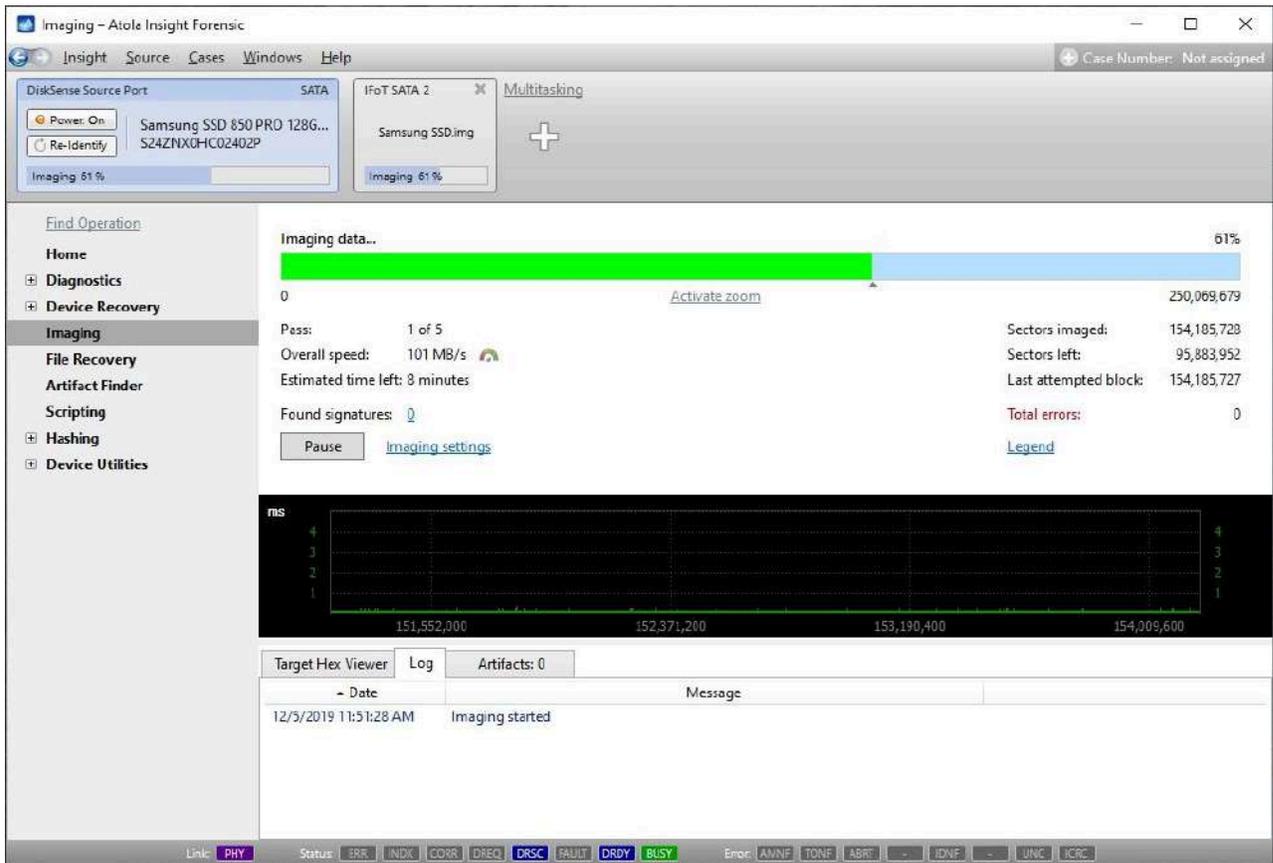
7. Enter a name for a new image file, click **Add** and then click **Select**.



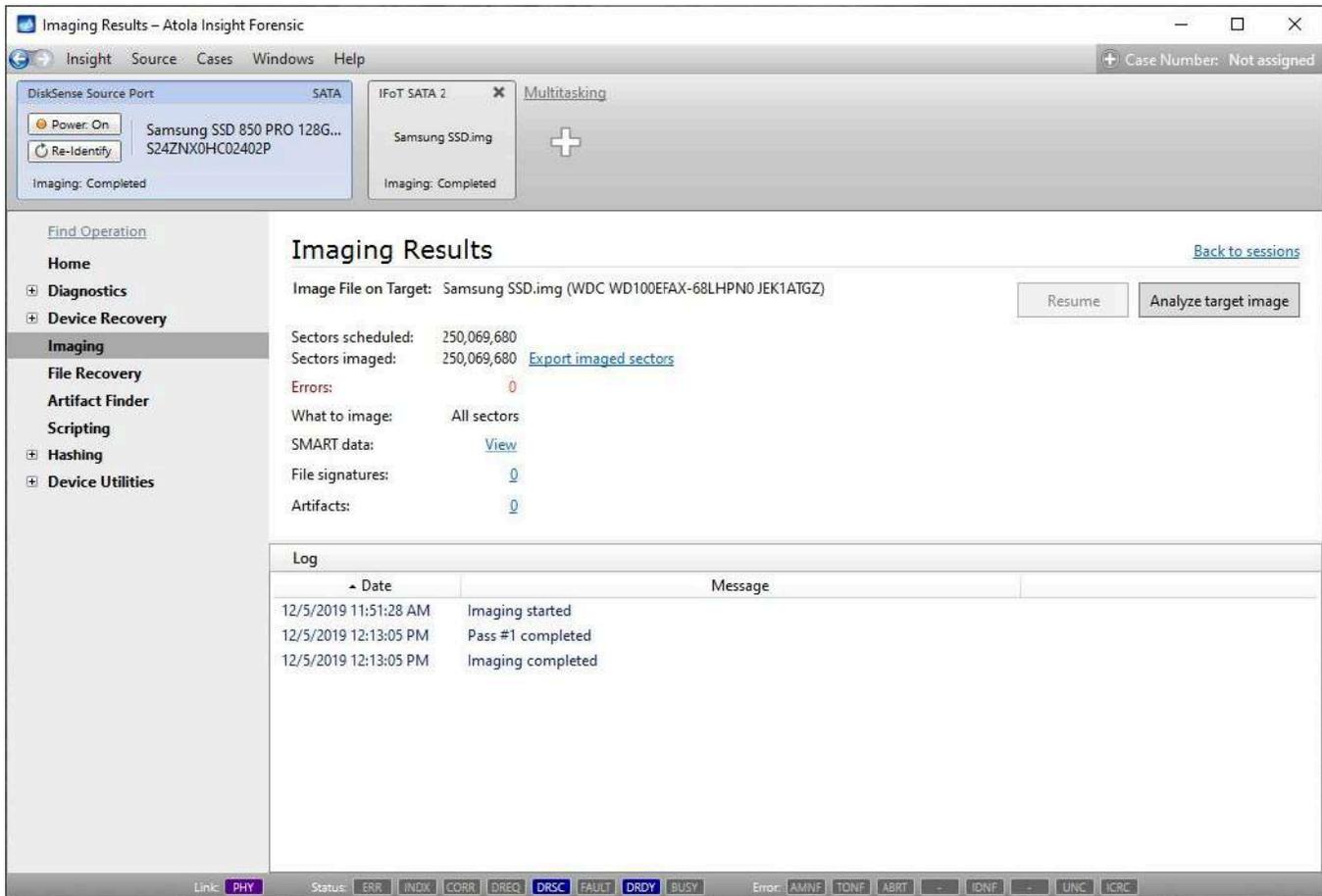
8. Specify the settings for this imaging session and click the **Start Imaging** button.



After you click the **Start Imaging** button, Insight begins imaging data into the file on your encrypted target.

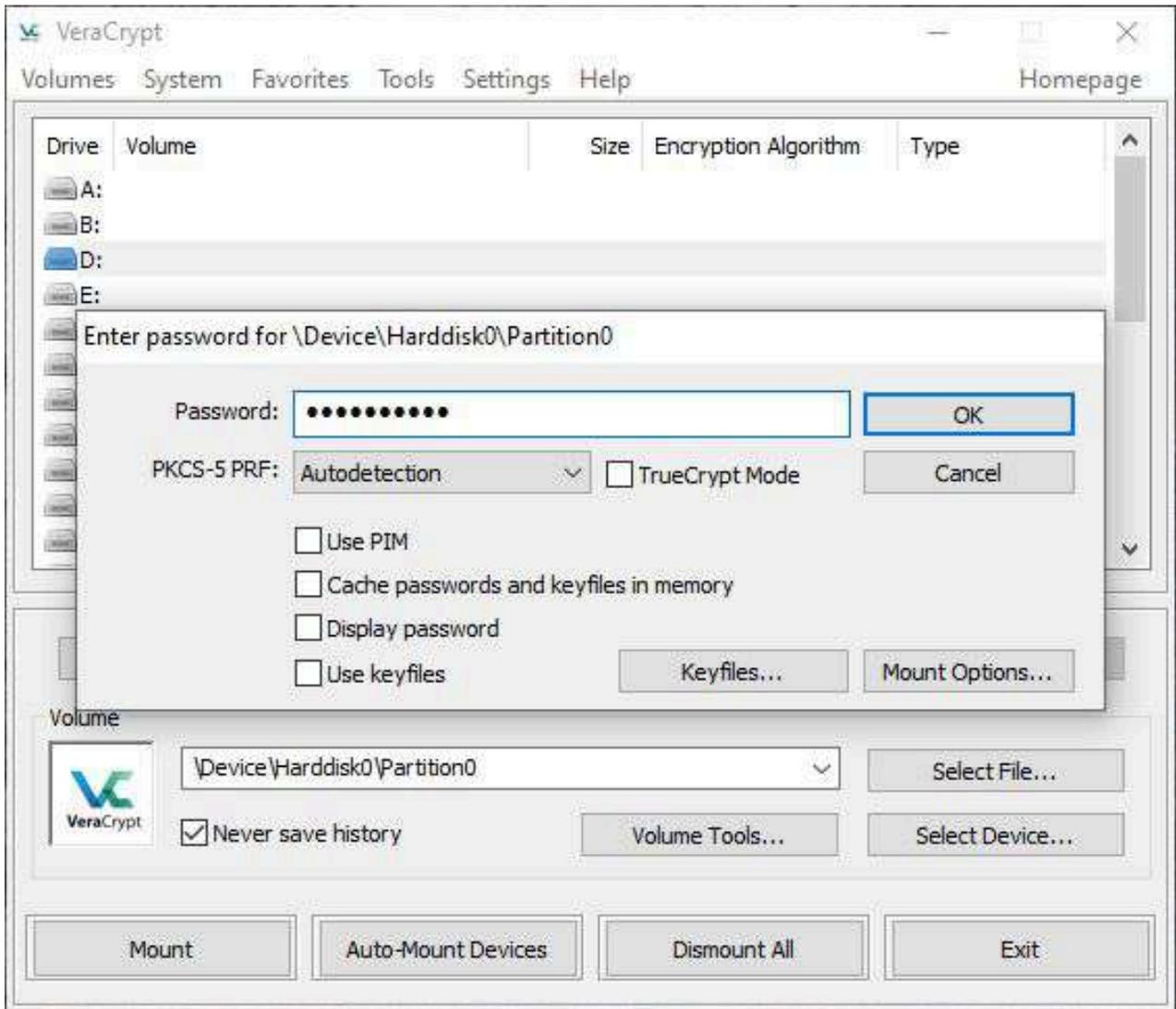


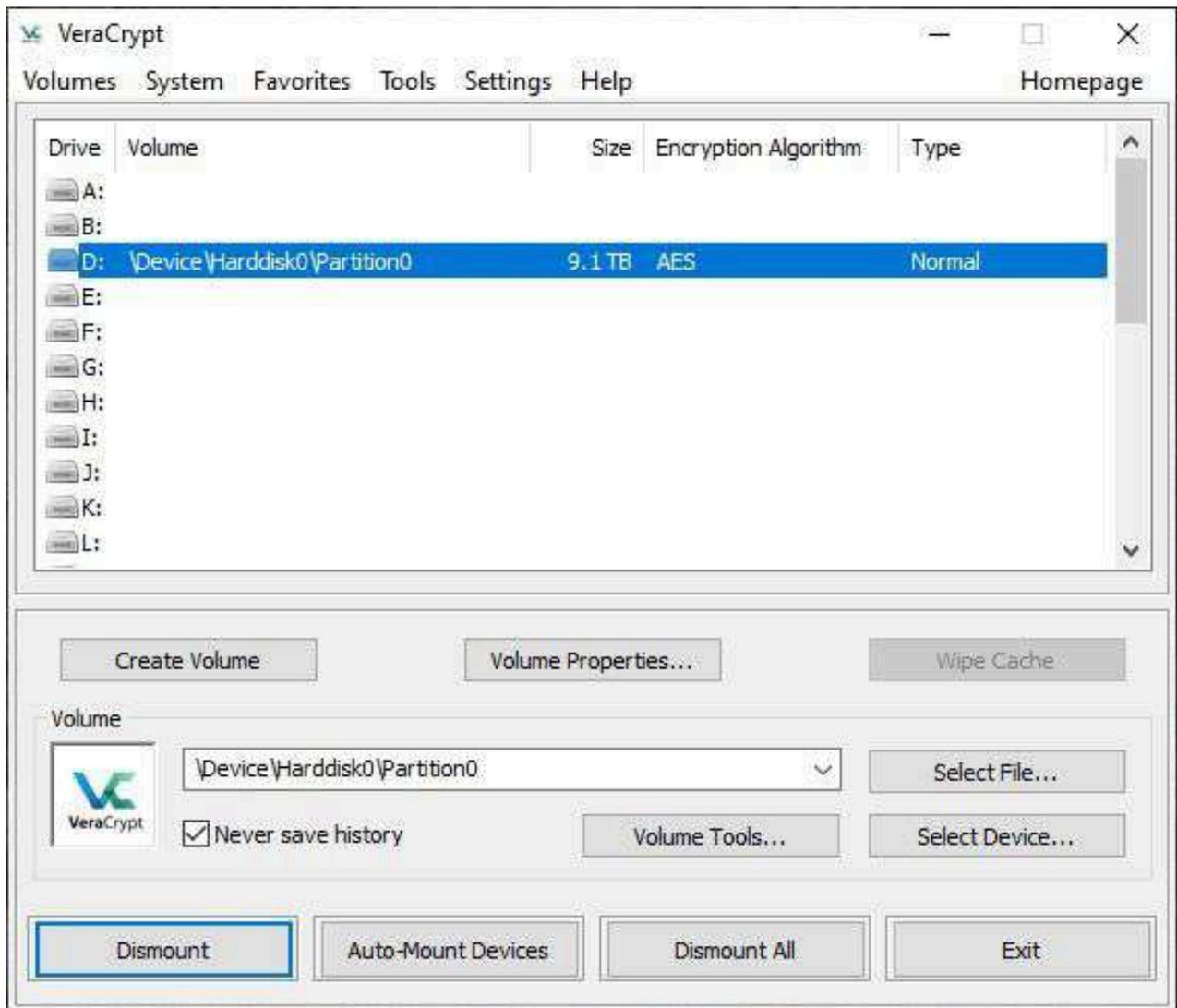
Upon completion of the imaging session, check the **Imaging results** screen.



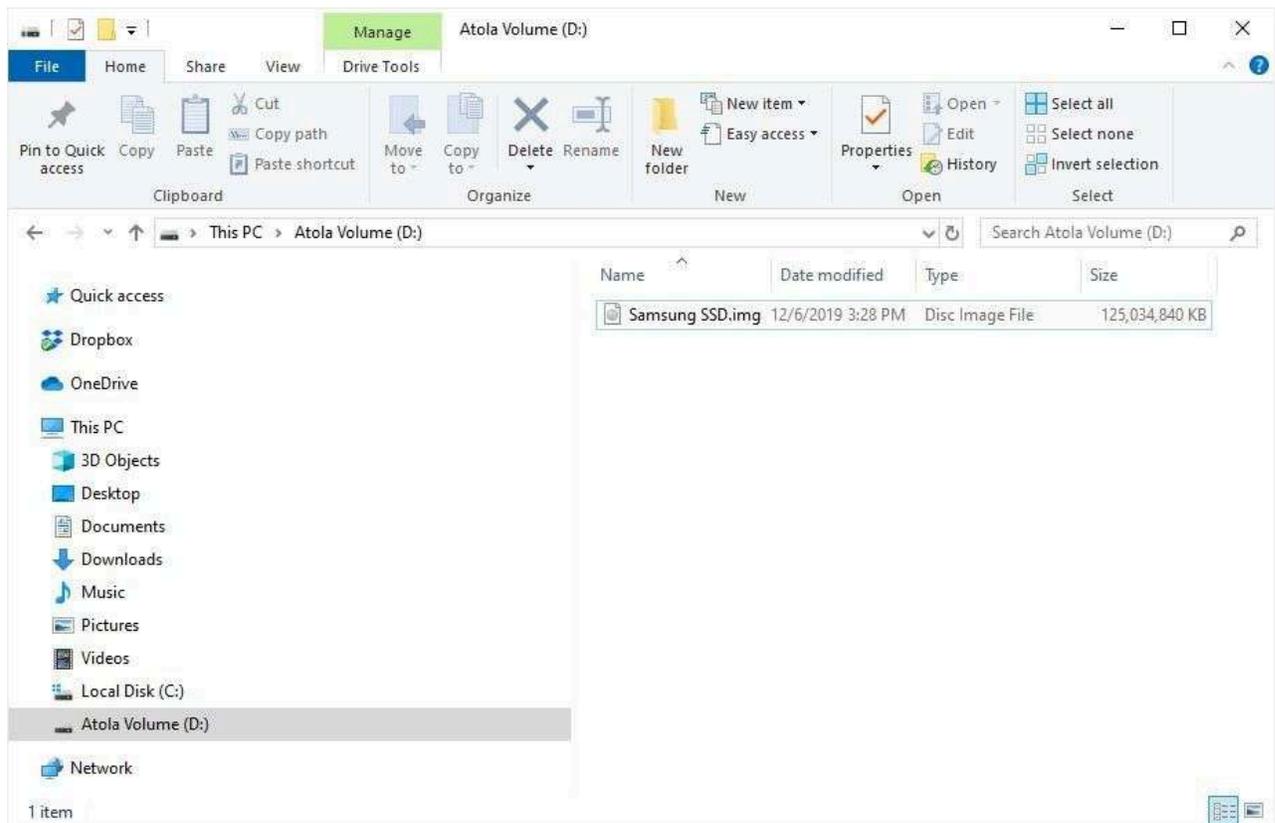
## Extract data from your encrypted VeraCrypt volume

1. To find the VeraCrypt volume and the imaged file, 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 the **Select device** button.
5. In the pop-up window, select your encrypted volume.
6. Click the **Mount** button. Now you can view the partition name, size and encryption algorithm.
7. To get access to the encrypted volume, use the password set prior to the imaging session.





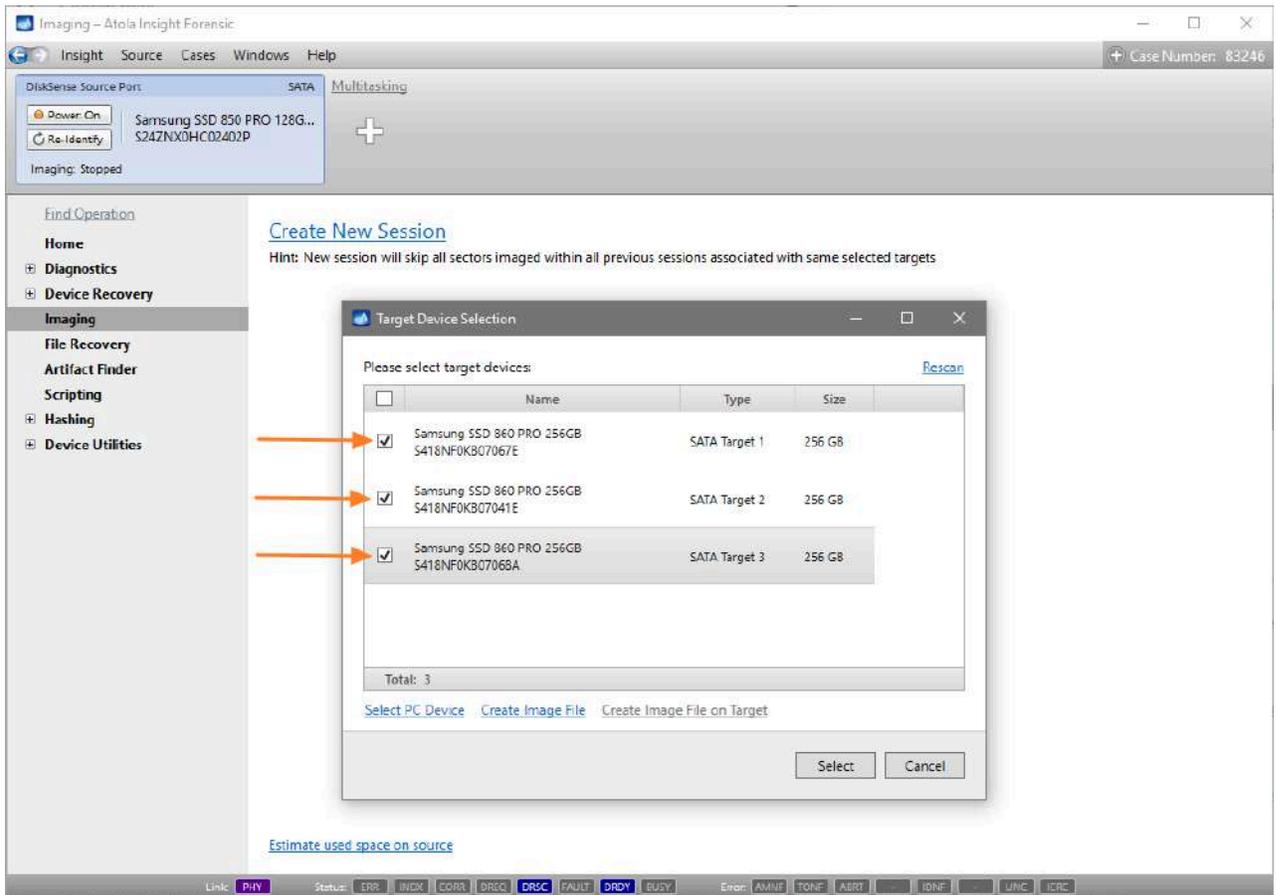
8. Once you have entered the password, the volume will be mounted and you can access it from Windows Explorer and use the image for subsequent operations.



## Imaging an evidence drive to 3 targets

If you need to create multiple images of a drive for different purposes, with Insight you can image to three targets simultaneously. The targets can be of different types: another drive, an E01/AFF4/RAW file located on a server/workstation.

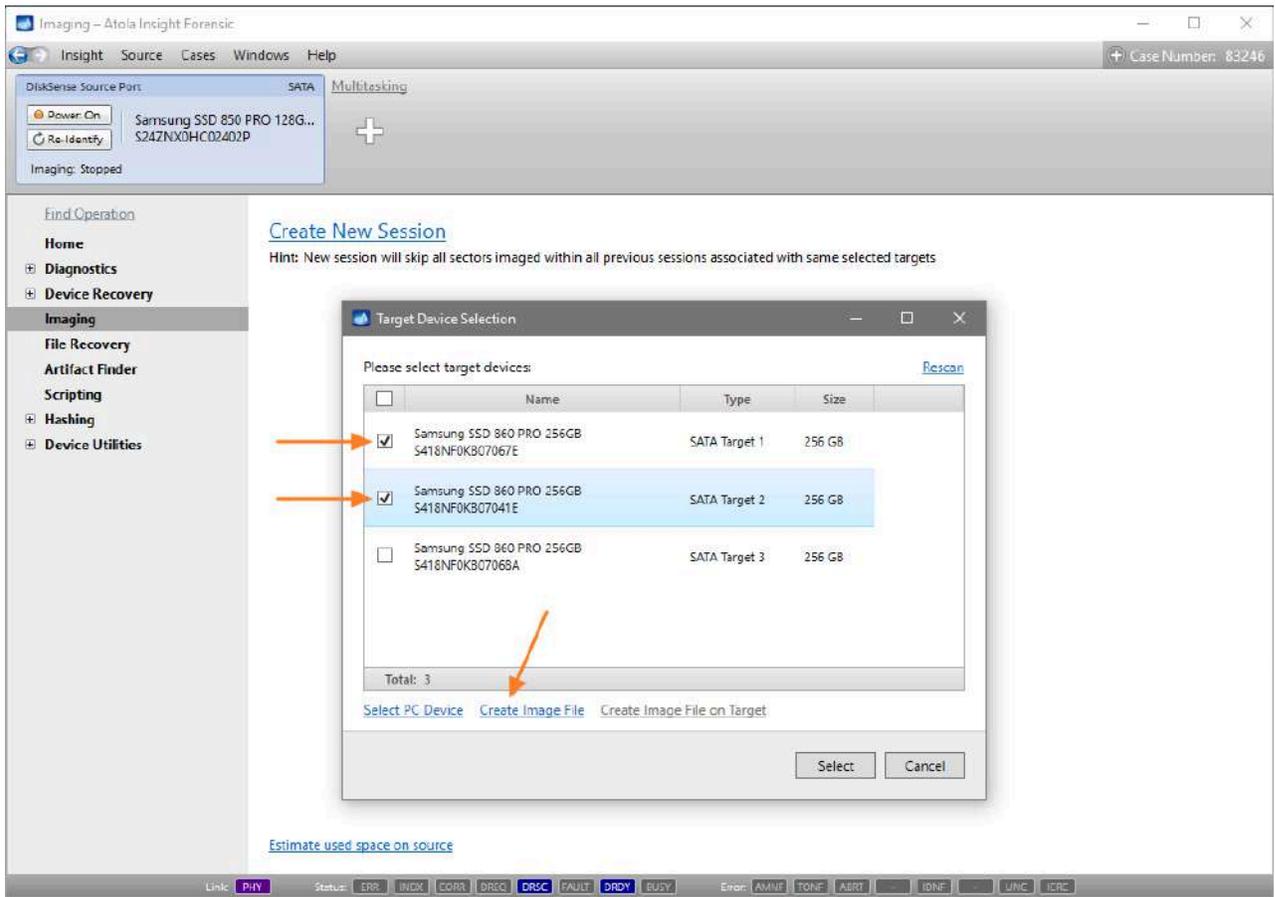
1. In the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. In the **Target Device Selection** dialog, select the target drives you want to image to and click the **Select** button.



## Selecting target drives.

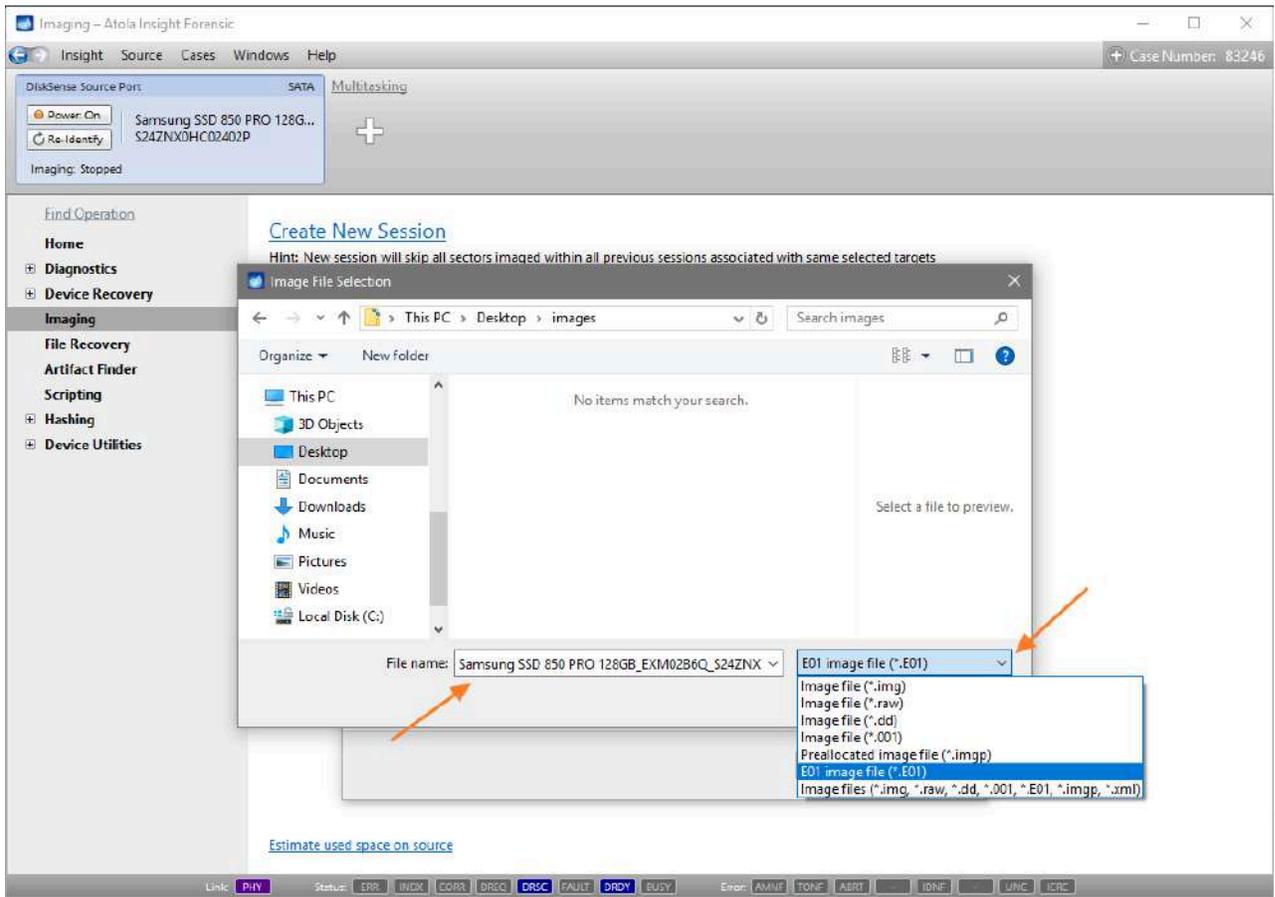
If one of the targets has to be a file, follow these steps:

1. In the Target Device Selection dialog, click the Create Image File link.



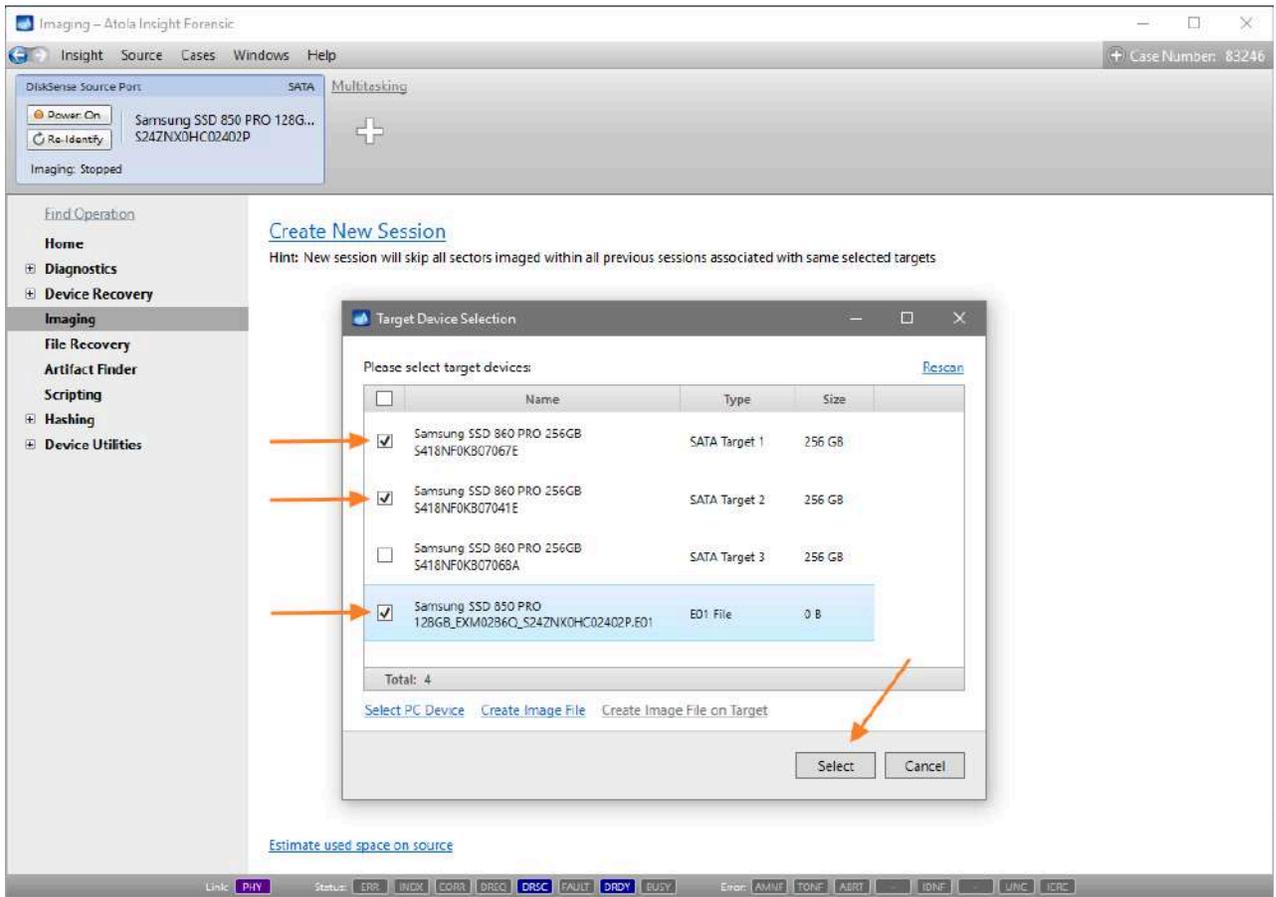
## The Create Image File link in the Target Device Selection dialog.

2. Select file location, name and format, then click Open.



## Selecting target file.

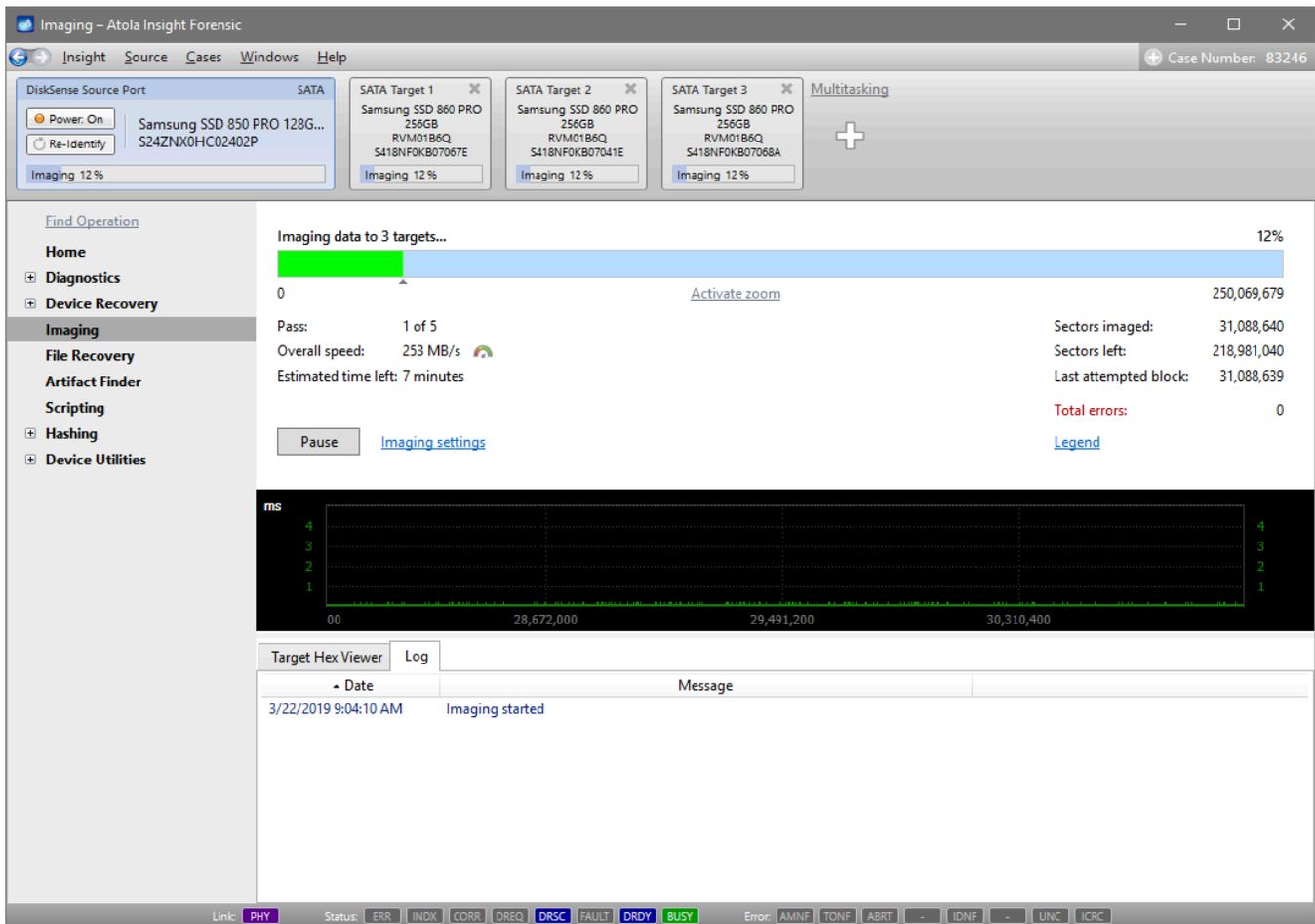
3. Once you have selected all targets, click the **Select** button.



### Selecting multiple files as imaging targets.

4. Double-check the imaging settings and click the **Start Imaging** button.

The speed of this imaging session will depend on the slowest of the devices involved in it: either on the read speed of the source drive or the write speed of the targets you have selected.



Imaging data to 3 target files.

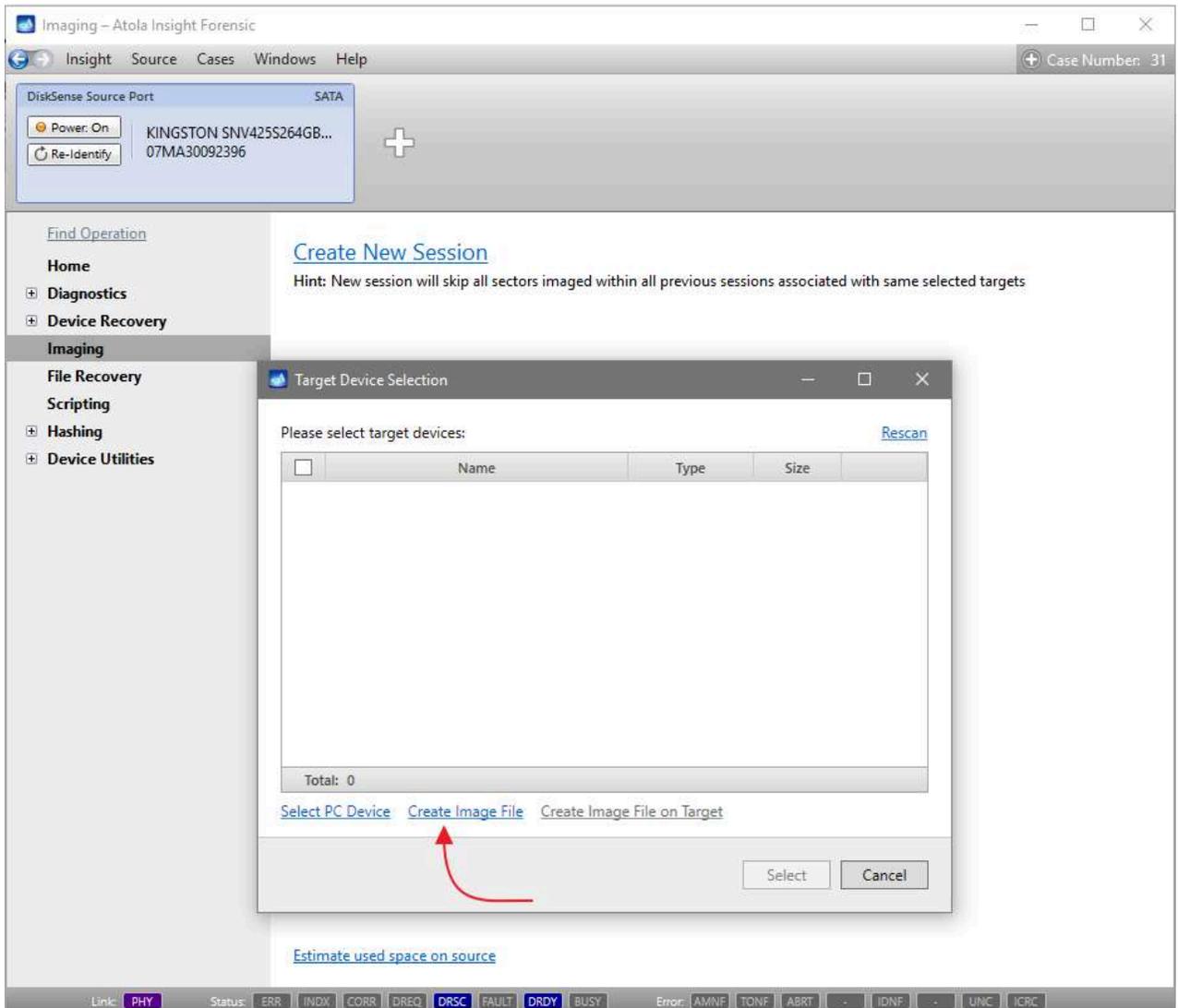
## Imaging to an E01 File with MD5 and SHA-1 Hashes

In recent years, E01 file format has become the de facto standard format for forensic purposes due to its ability to store not only a physical or logical copy of a source drive, but also case and evidence details. E01 file can also contain both MD5 and SHA-1 hashes. And it is considered a good practice among forensic specialists to calculate both hashes while imaging the evidence so that they are included in the E01 file.

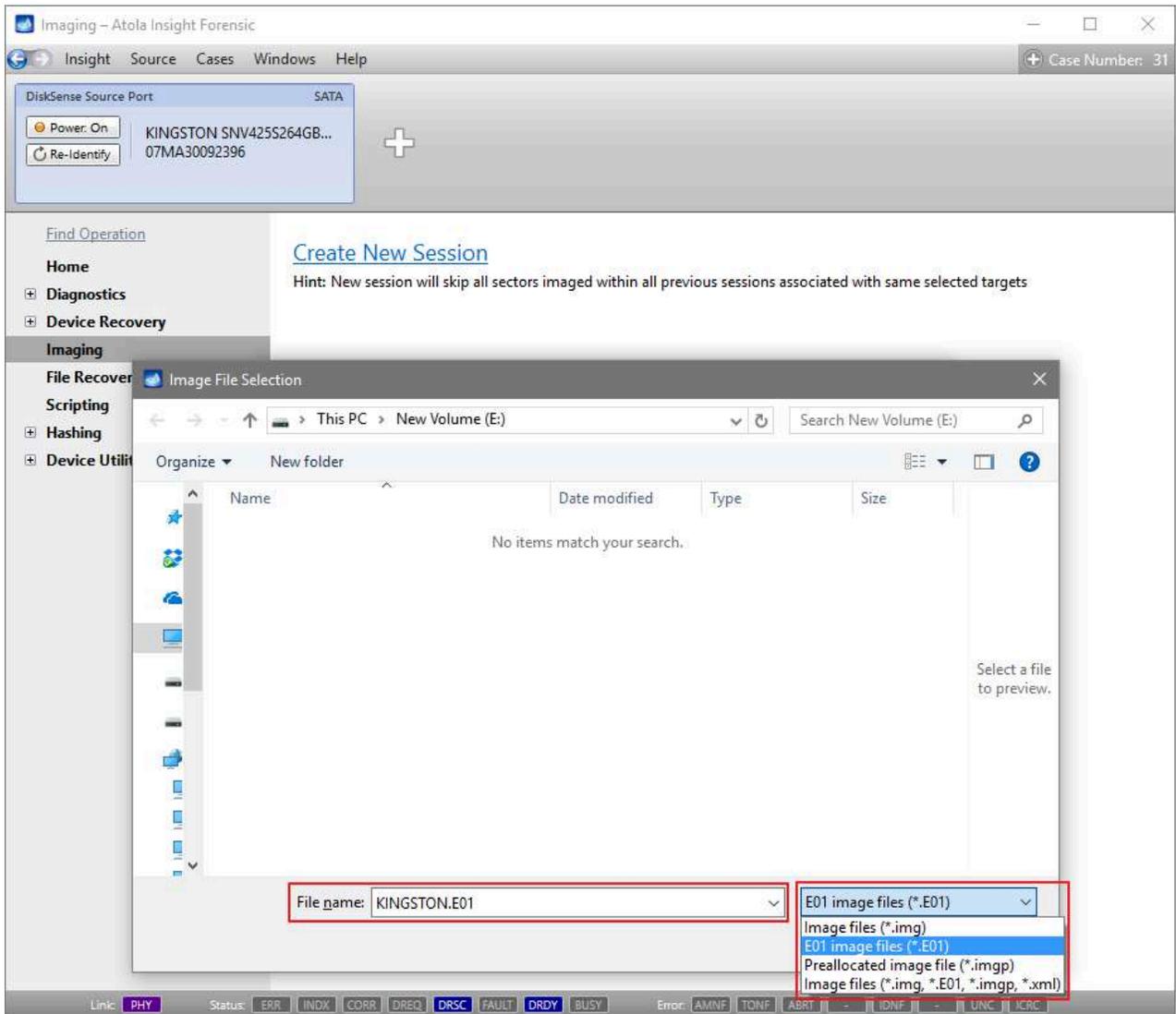
To image a source evidence drive to an E01 file, you have to add a new target file.

### Select a new E01 file

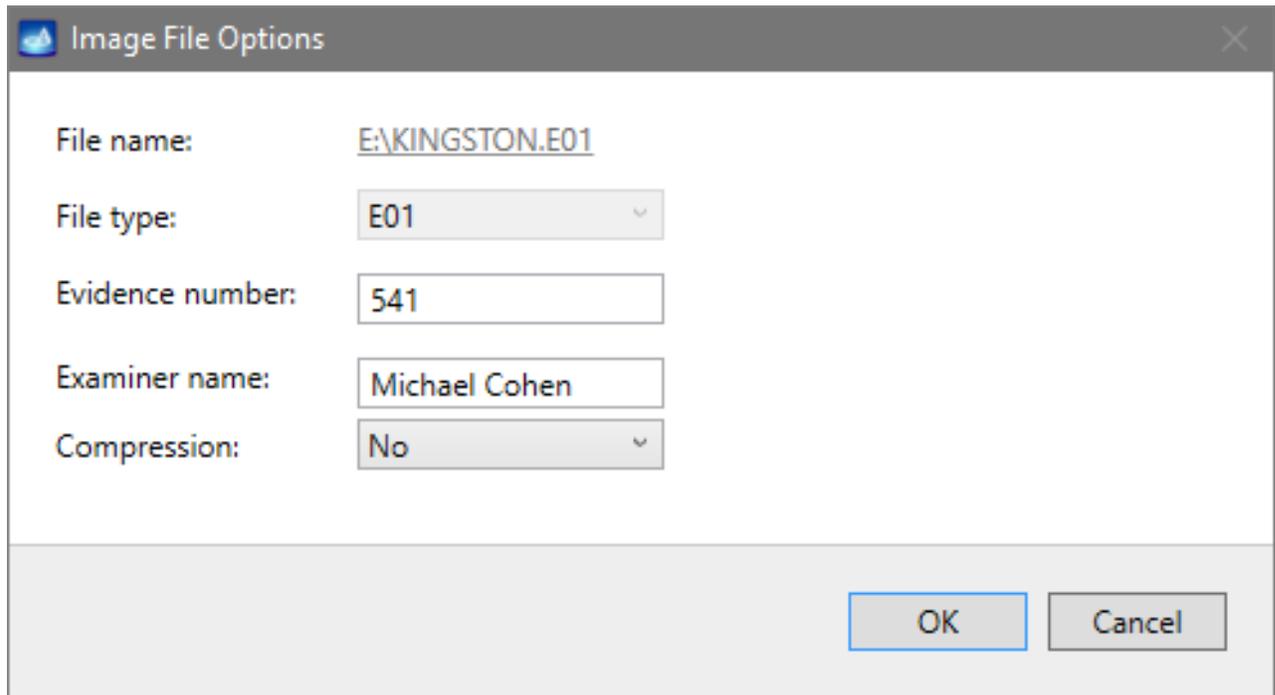
1. In the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. In the **Target Device Selection** dialog, click the **Create Image File** link.



4. In the **Image File Selection** dialog, select E01 file extension in the drop-down menu to create an image file with this extension and enter the name you prefer in the **File Name** field.



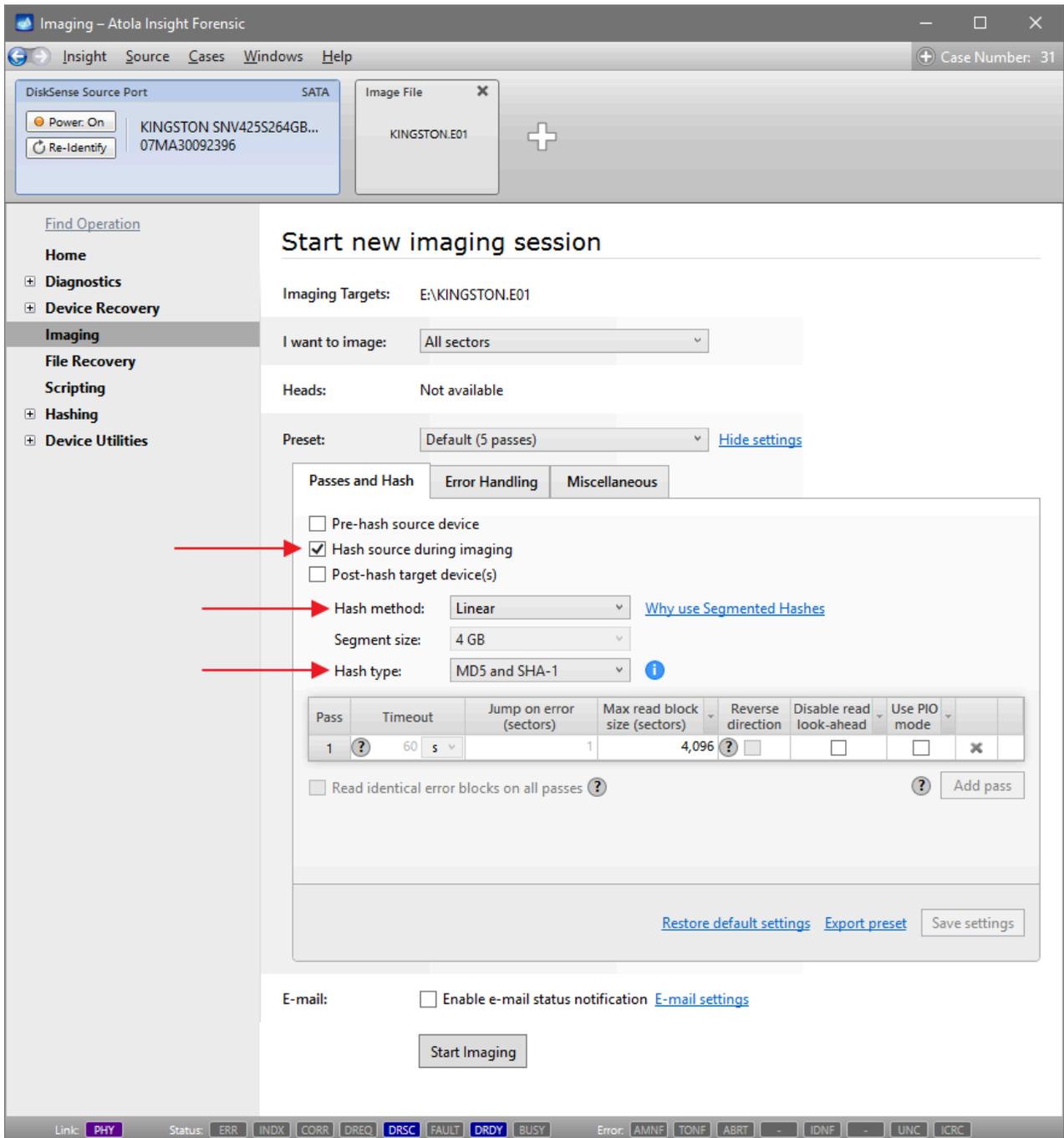
5. In the **Image File Options** dialog, fill out all the relevant fields. You can also do it later on the **Home** page of the file when it is created.



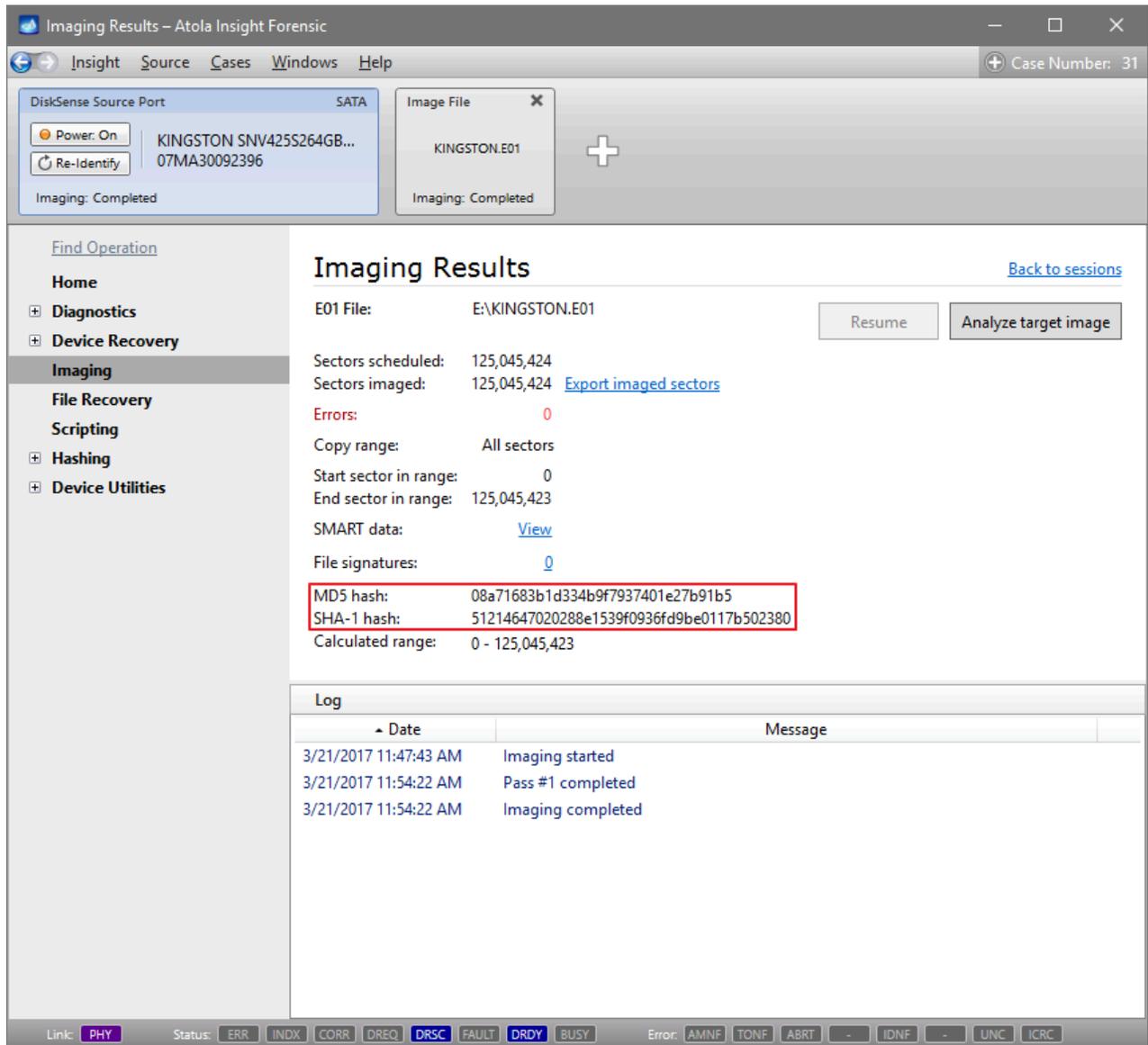
6. In the **Target Device Selection** window, click the **Select** button.
7. Insight creates an E01 file with current 0 bytes capacity. Its final capacity will be defined by the amount of imaged data it contains plus the metadata.

## Calculate the hashes during imaging

1. In the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. In **Preset** line, click the **Show settings** link.
4. On the **Passes and Hash** tab, select the **Hash source during imaging** option.
5. In the **Hash method** list, select **Linear**.
6. In the **Hash type** list, select **MD5 and SHA-1**.
7. Click **Start imaging**.



8. Upon completion of imaging, on the **Imaging Results** page, Insight features both MD5 and SHA-1 hashes.



### Calculated MD5 and SHA1 hashes

## Logical imaging

The logical imaging module in Atola Insight Forensic creates an L01 file with a forensically sound logical copy of folders and files you've selected manually or using built-in include and exclude filters.

The resulting L01 file also includes unaltered metadata, such as file attributes and creation dates, as well as hashes calculated during the imaging process. An L01 file can be compressed to save storage space.

Once the logical imaging process is complete, Insight also generates a comprehensive report with details about the source, target, number of imaged files and bytes and more.

# Key features of logical imaging

- Smart include and exclude filters
- L01 format for target image file
- Compression of L01 image file
- Up to 3 parallel logical imaging sessions
- Pause and resume option for each imaging session
- Supported source drive types: SATA, USB, IDE, NVMe, SAS, MacBook
- Supported image file located on a source drive: RAW, E01, AFF4
- Supported file systems: NTFS, APFS, XFS, ext4/3/2, exFAT, Btrfs, HFS/HFS+, FAT32, FAT16

## Logical imaging workflow

To create a logical image of your source device, follow these steps:

1. [Select your source device and go to Logical imaging.](#)
2. [Select partitions, folders or files to image.](#)
3. [Apply smart filters, if needed.](#)
4. [Create a target file.](#)
5. [Optional: Pause and resume the imaging process.](#)
6. [View the logical imaging report.](#)

## Select source device

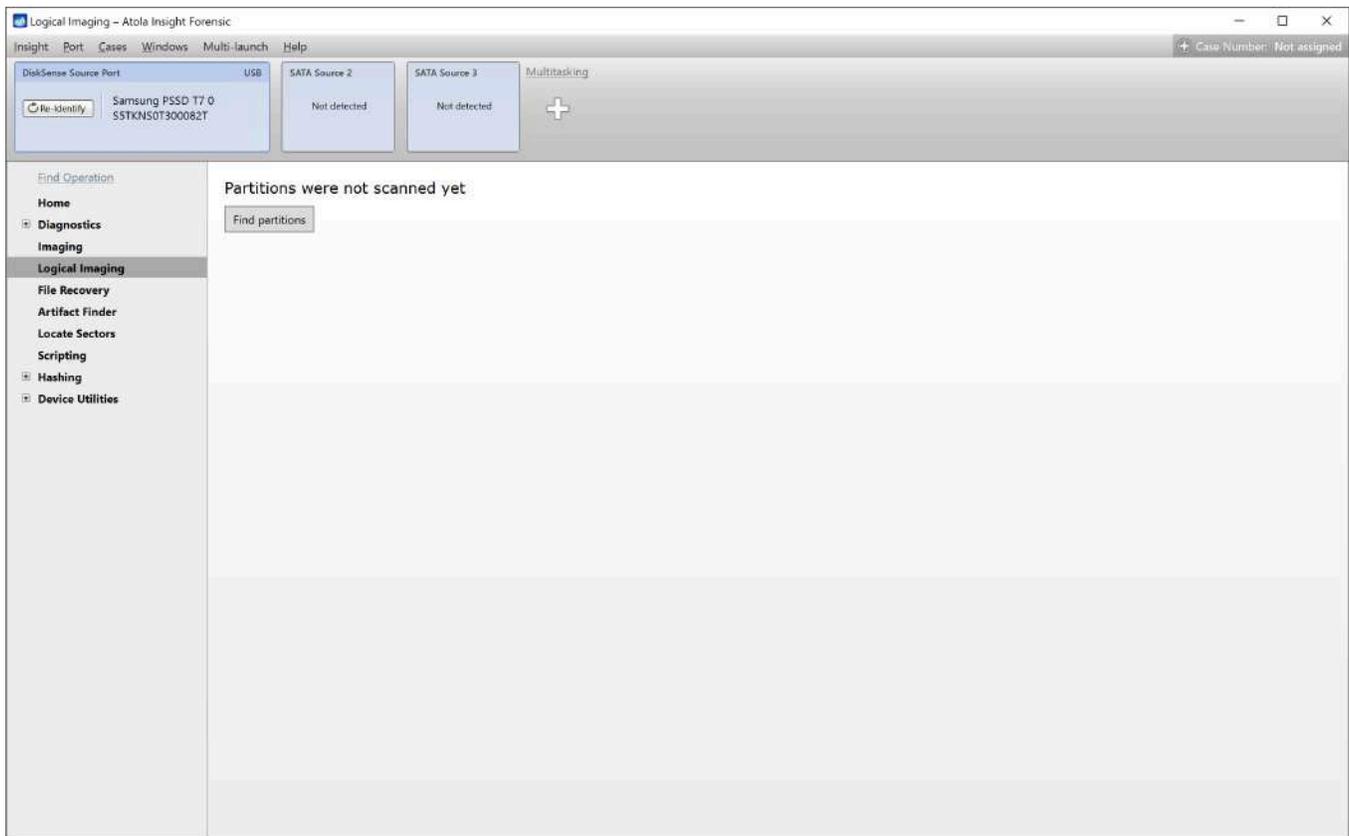
As a source for logical imaging, you can use:

- **Physical drives**, connected directly or via extension modules
  - SATA
  - USB
  - IDE
  - NVMe via [M.2 extension module](#)
  - SAS via [SAS extension module](#)
  - MacBook drives via [Apple PCIe SSD](#) or [Thunderbolt](#) extension modules
- **Image files** from a Source drive
  - RAW
  - E01
  - AFF4

To launch the Logical imaging module:

1. On the Devices panel, select the source drive or file.

2. On the Sidebar, click **Logical imaging**.
3. Click the **Find partitions** button.

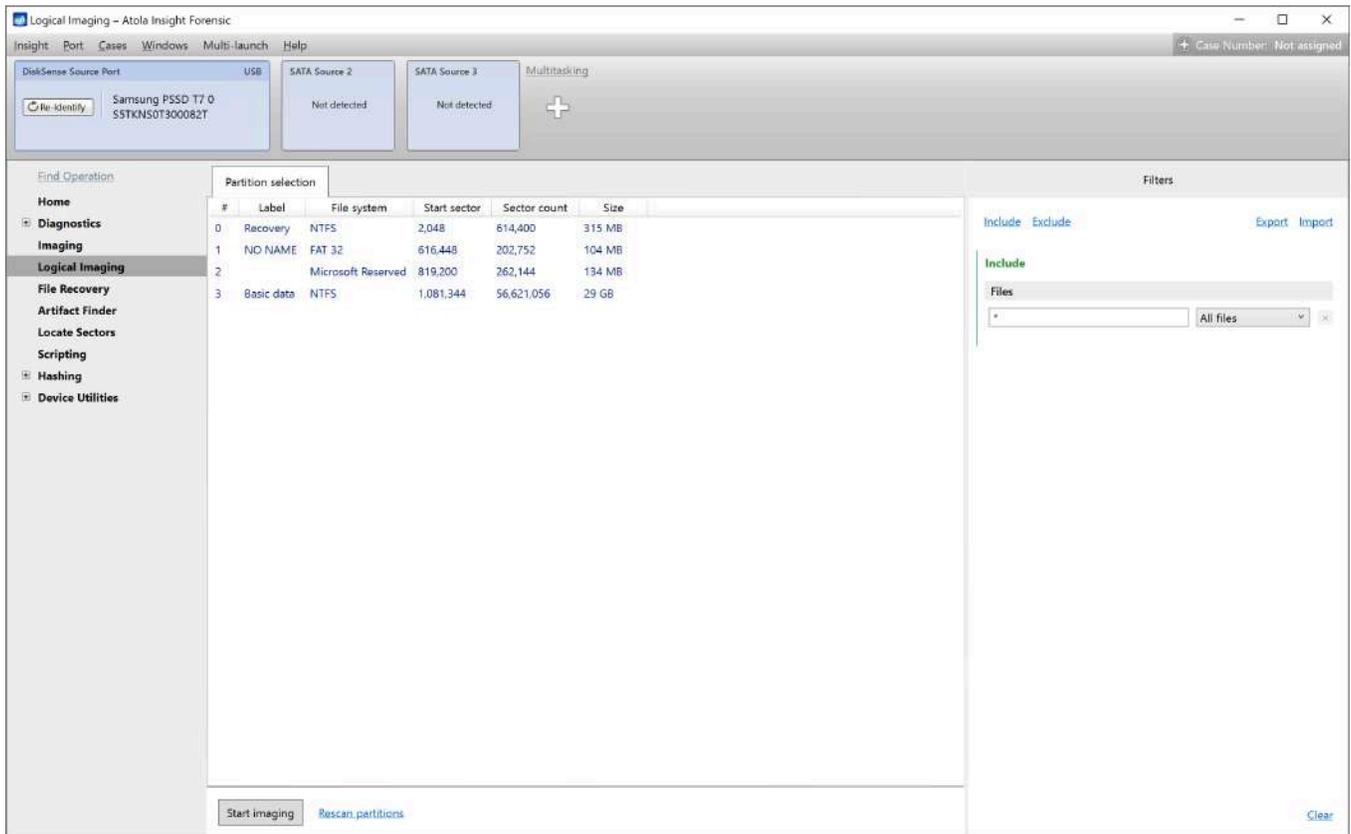


The 'Find partitions' button in the Logical imaging section.

## Select partitions, folders or files to image

After scanning partitions on the source device, Insight displays their list on the **Partition selection** tab.

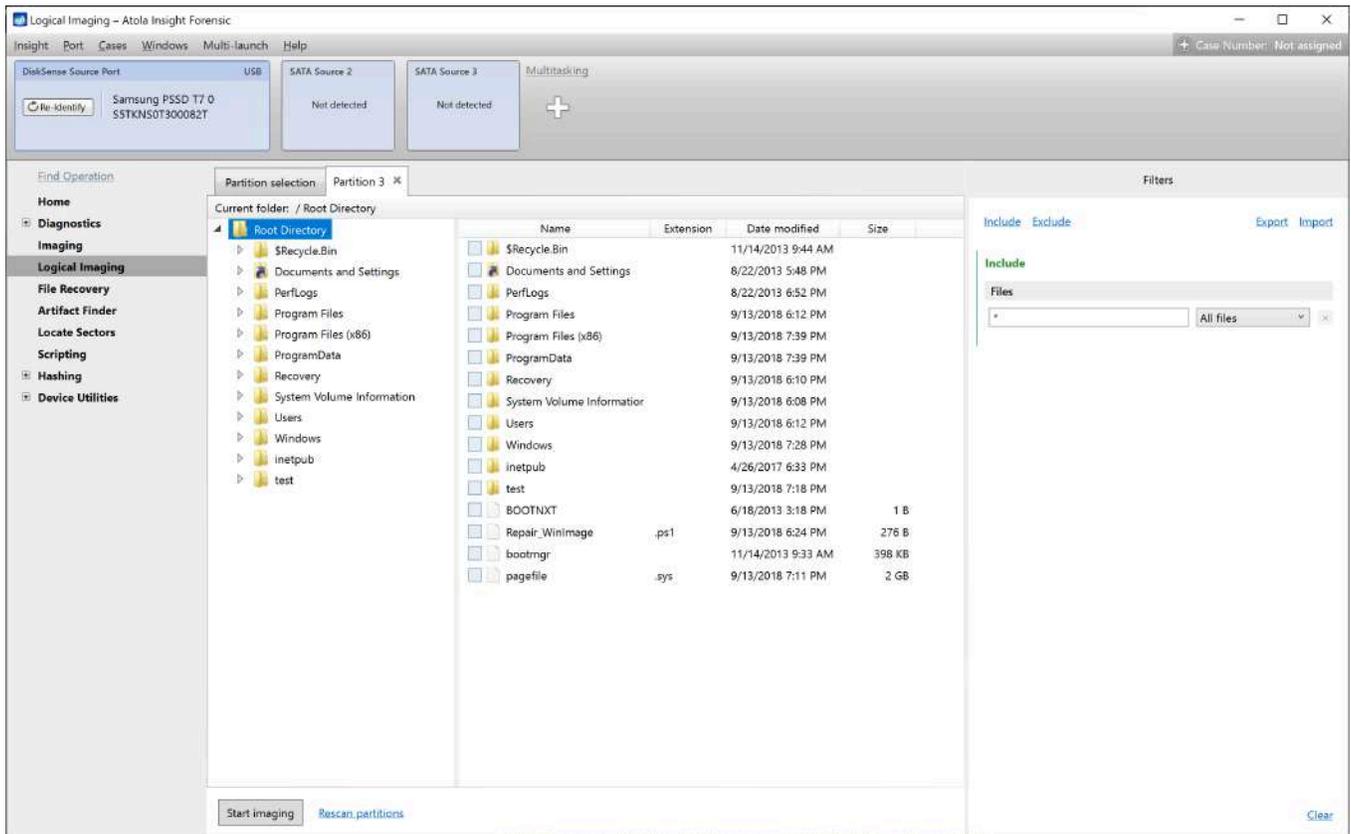
By default, Insight images all files from all partitions.



**The list of the available partitions.**

## Preview, select or deselect partition

To preview the partition contents, double-click its name on the **Partition selection** tab. The separate **Partition** tab opens, displaying the partition folder structure and file list.

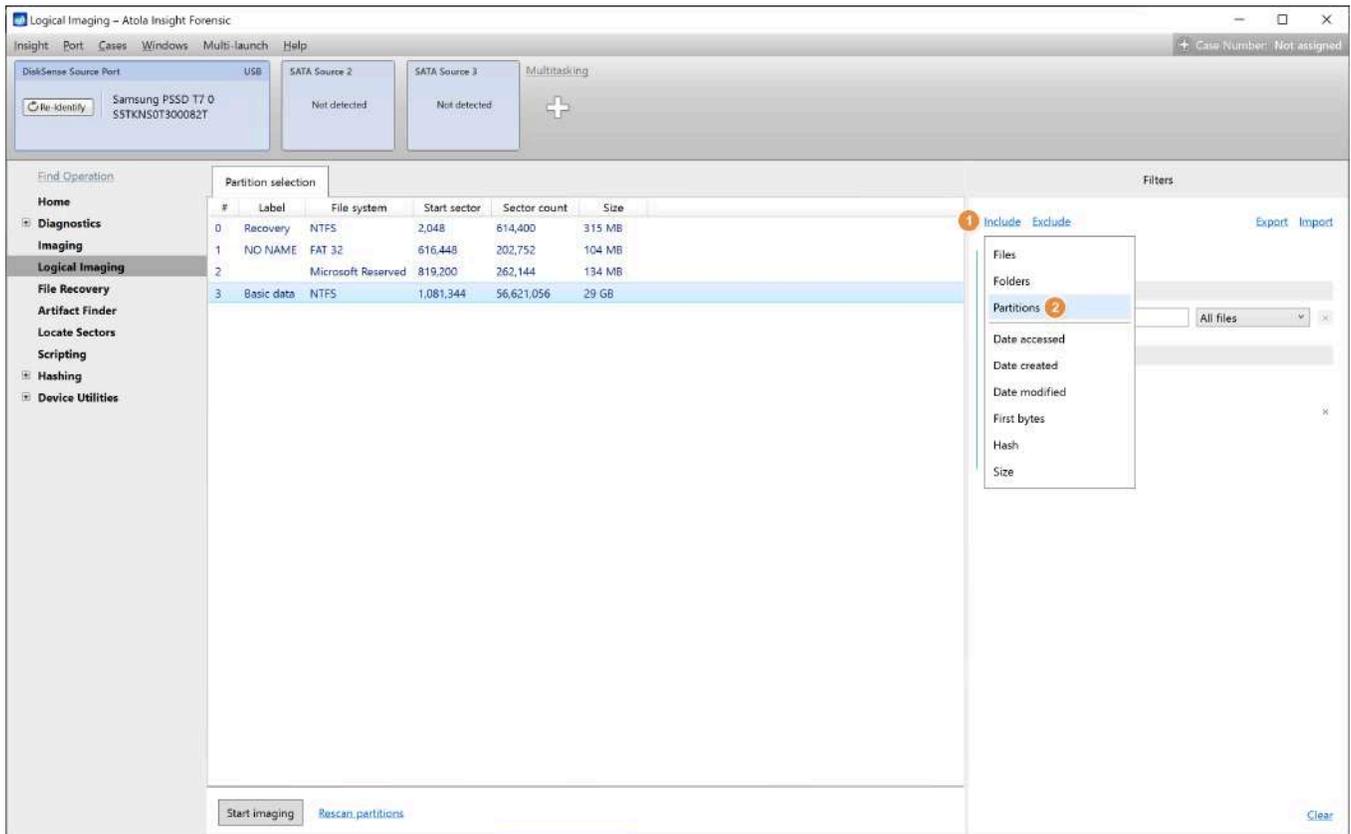


### The partition preview, displaying the folder structure and file list.

**Important:** By default, all files from all partitions are selected for logical imaging.

To exclude a partition:

1. On the **Filters** panel, click the **Include** link at the top.
2. Select **Partitions** from the list.
3. Clear the checkboxes next to the partitions you want to exclude.



## The partitions filter.

To include a partition again, select the checkbox.

Your selection is saved automatically.

## Filters

[Include](#) [Exclude](#)

[Export](#) [Import](#)

### Include

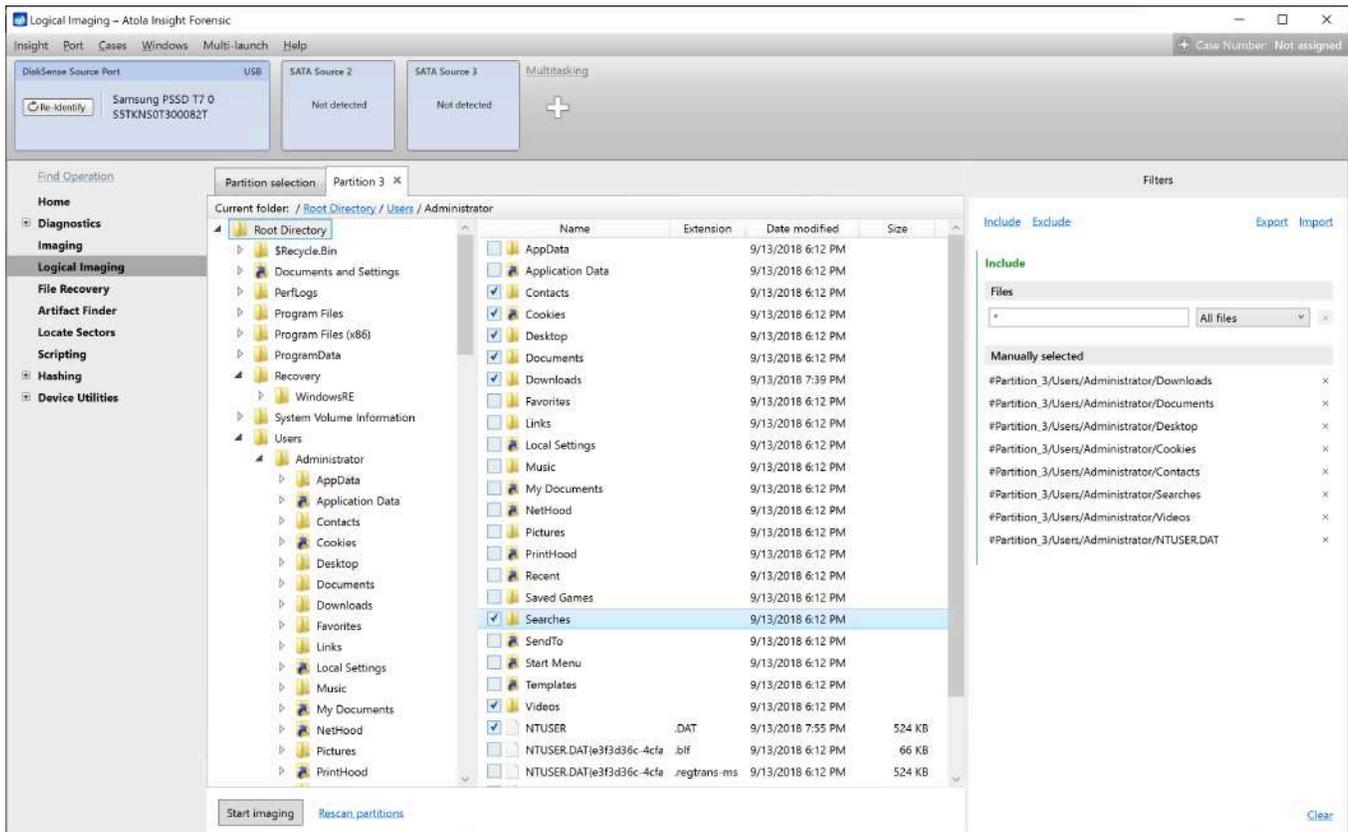
#### Files

#### Partitions

- Partition 0
- Partition 1
- Partition 2
- Partition 3

## Preview folder, manually include or exclude folders and files

The **Partition** tab displays the partition folder structure and the file list.



## Manually selecting folders and files for logical imaging.

- To preview a folder's contents, click the folder name in the folder tree.
- To manually include a folder or file for imaging, click the checkbox next to its name. The folder or file appears on the Filters panel on the right as manually selected.
- To manually exclude a folder or file from the selection, clear its checkbox or use the x icon on the Filters panel on the right. The folder or file disappears from the panel.
- To deselect all the selected folders and files, click the Clear link at the bottom of the Filters panel.

## Use smart filters and presets for selecting folders or files

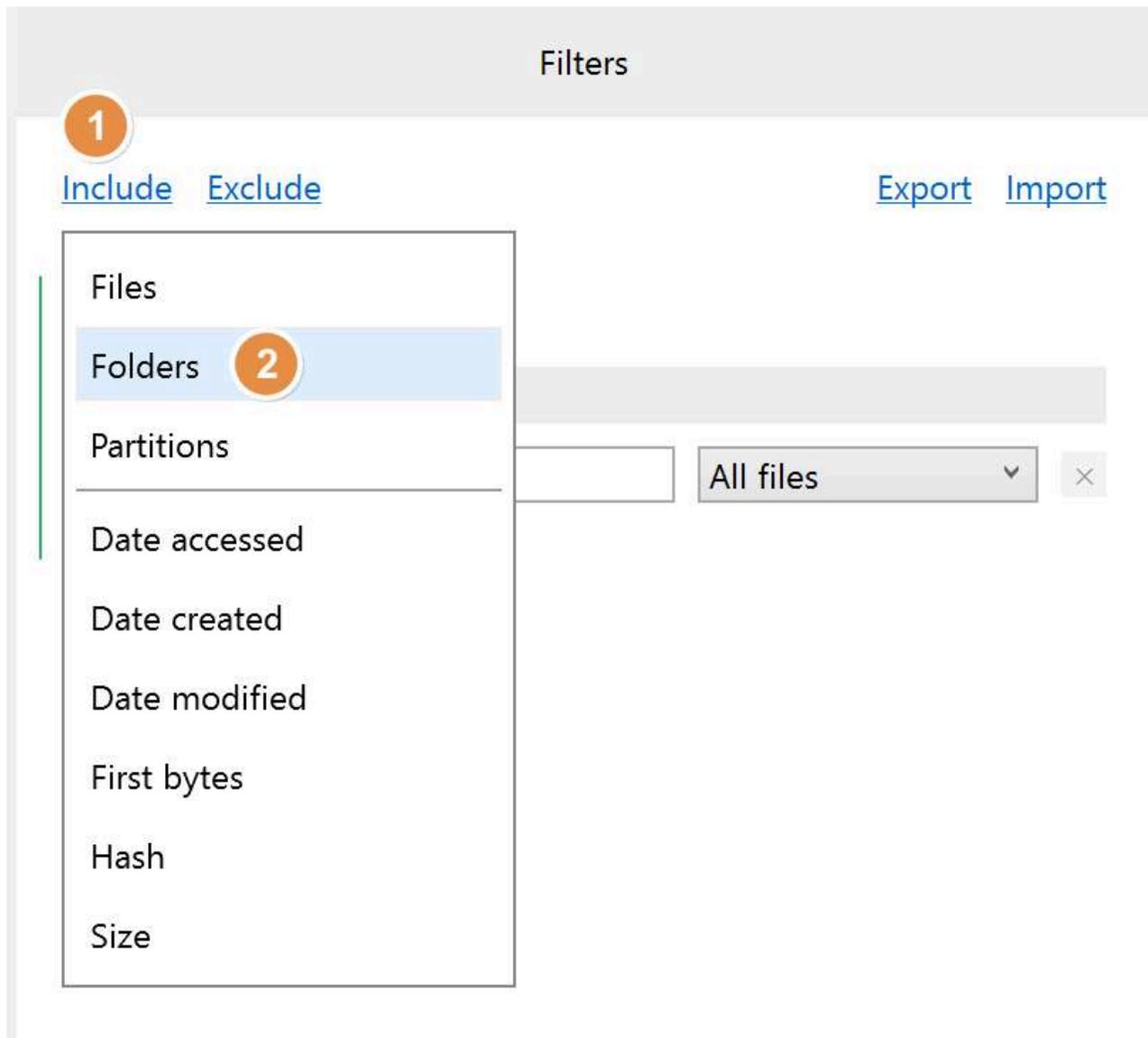
By default, Insight images all files from all partitions.

On the Filters panel, you can automatically include or exclude folders and files for imaging by applying the built-in smart filters or custom filtering presets.

### Filtering folders and files

To automatically include or exclude specific files or folders:

1. On the Filters panel, click the Include or Exclude link at the top.
2. Select Folders or Files from the list that appears.



3. The respective section on the **Filters** panel appears. In that section, select one of the predefined options from the list:

a. For folders:

- OS folders
- User folders
- Custom folders – Filter folders using user-defined patterns with wildcard support. Use wildcards to match multiple folders at once (for example, `*/temp` for all temp subdirectories, or `backup_202?_*` for dated backup folders).

## Filters

[Include](#) [Exclude](#) [Export](#) [Import](#)

**Include**

### Files

All files ▼ ×

### Folders

OS folders ▼ ×

Custom folders

OS folders

User folders

b. For files:

- Archives
- Audio
- Databases
- Documents
- Emails
- Financial
- Pictures
- Security keys
- Videos
- Virtual machines
- Custom files – Filter files using user-defined patterns with wildcard support. Use wildcards to match multiple files at once (for example, `*.log` for all log files, `report_*.pdf` for numbered reports, or `data_202?_*.csv` for yearly data files).

**Filters**

[Include](#)   [Exclude](#) [Export](#)   [Import](#)

**Include**

**Files**

Documents ▼

- All files
- Custom files
- Archives
- Audio
- Databases
- Documents**
- Emails
- Financial
- Pictures
- Security keys
- Videos
- Virtual machines

## Additional filtering parameters

You can also include or exclude specific files or folders meeting one or more of the following parameters:

- Date accessed
- Date created
- Date modified
- First bytes
- Hash
- Size

To apply additional filtering parameters, do the following:

1. On the **Filters** panel, click the **Include** or **Exclude** link at the top.
2. Select an additional filtering parameter from the list that appears.
3. The respective section on the **Filters** panel appears. In that section, enter a value for a filtering parameter.

## Filters

[Include](#)[Exclude](#)[Export](#)[Import](#)

### Include

**Files**

All files ▼

×

**Date accessed**

9/1/2025

▲  
▼

9/17/2025

▲  
▼

×

**Date created**

8/1/2025

▲  
▼

9/17/2025

▲  
▼

×

**First bytes**

×

**Hash**

MD5 ▼

×

**Size**

2

Bytes ▼

1000

MByte: ▼

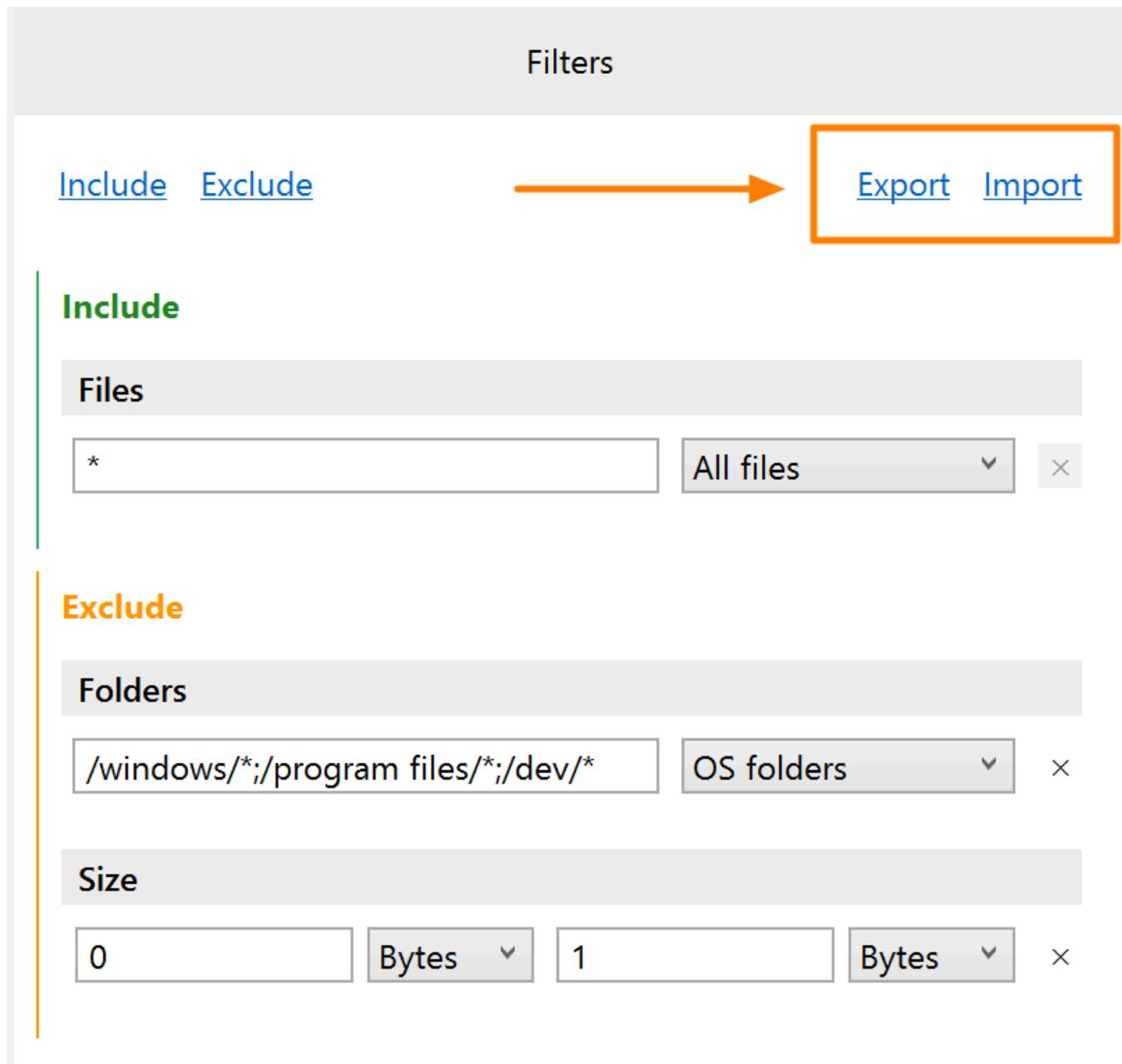
×

## 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 in JSON format:

1. On the **Filters** panel, click the **Export** link at the top.
2. Enter the name for your preset and click **Save**.

To apply an existing filter preset, use the **Import** link at the top of the **Filters** panel.



The screenshot shows the 'Filters' panel with the following elements:

- Filters** (Panel Title)
- [Include](#) [Exclude](#) (Navigation Links)
- [Export](#) [Import](#) (Action Links, highlighted with an orange box and arrow)
- Include** (Section Header)
- Files** (Section Header)
- (Dropdown)  (Remove)
- Exclude** (Section Header)
- Folders** (Section Header)
- (Dropdown)  (Remove)
- Size** (Section Header)
- (Dropdown)   (Dropdown)  (Remove)

## Create a target file

1. Once you have adjusted the logical imaging parameters, click the **Start imaging** button at the bottom.

2. The **Create Logical Image File** dialog opens.

**Create Logical Image File (.L01)**

Destination: **Folder** Target Drive

File: \\10.0.0.11\shared\Home\Samsung PSSD T7 0 S5TKNS0T300082T.L01 [Change](#)

Digest type: MD5+SHA1  Compress L01

Case ID: 389-2025-09-03

Examiner: William J. Carpenter

Evidence number: 28779-389

Description: Red Samsung SSD T7, found in the room #01, in the black box under the table.

Notes:

File settings can only be modified when creating a new image file

Create Cancel

3. Select the **Destination** for the target L01 file:

- **Folder** – For a folder on the local PC or remote network drive.
- **Target Drive** – For a storage device, directly connected to the DiskSense 2 hardware unit.

4. Change the file name if necessary.

5. Select the hashing method (Digest type): MD5, SHA1 or MD5+SHA1.

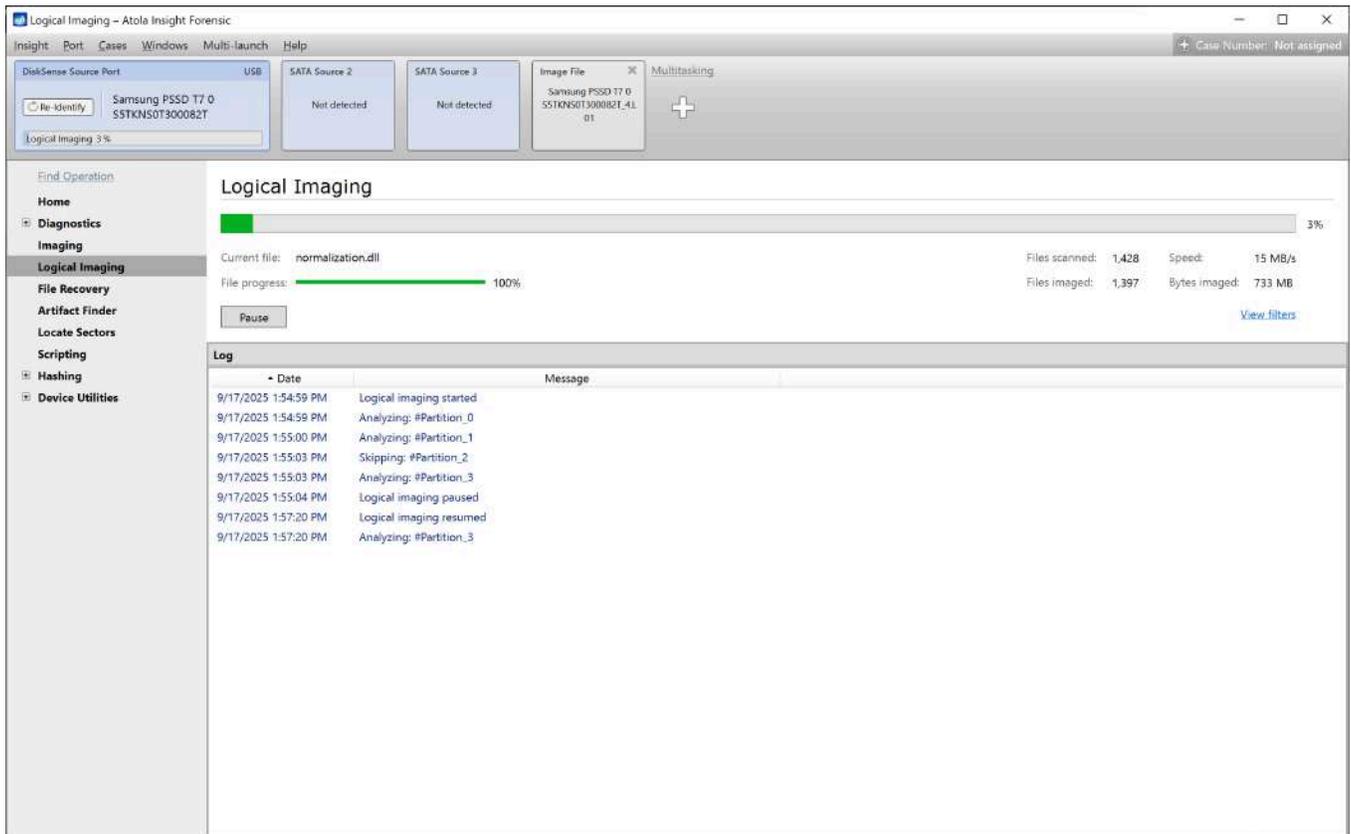
6. Enable or disable compression for the L01.

7. Fill in other details: Case ID, Examiner name, Evidence number, Description and Notes.

8. Click **Create**.

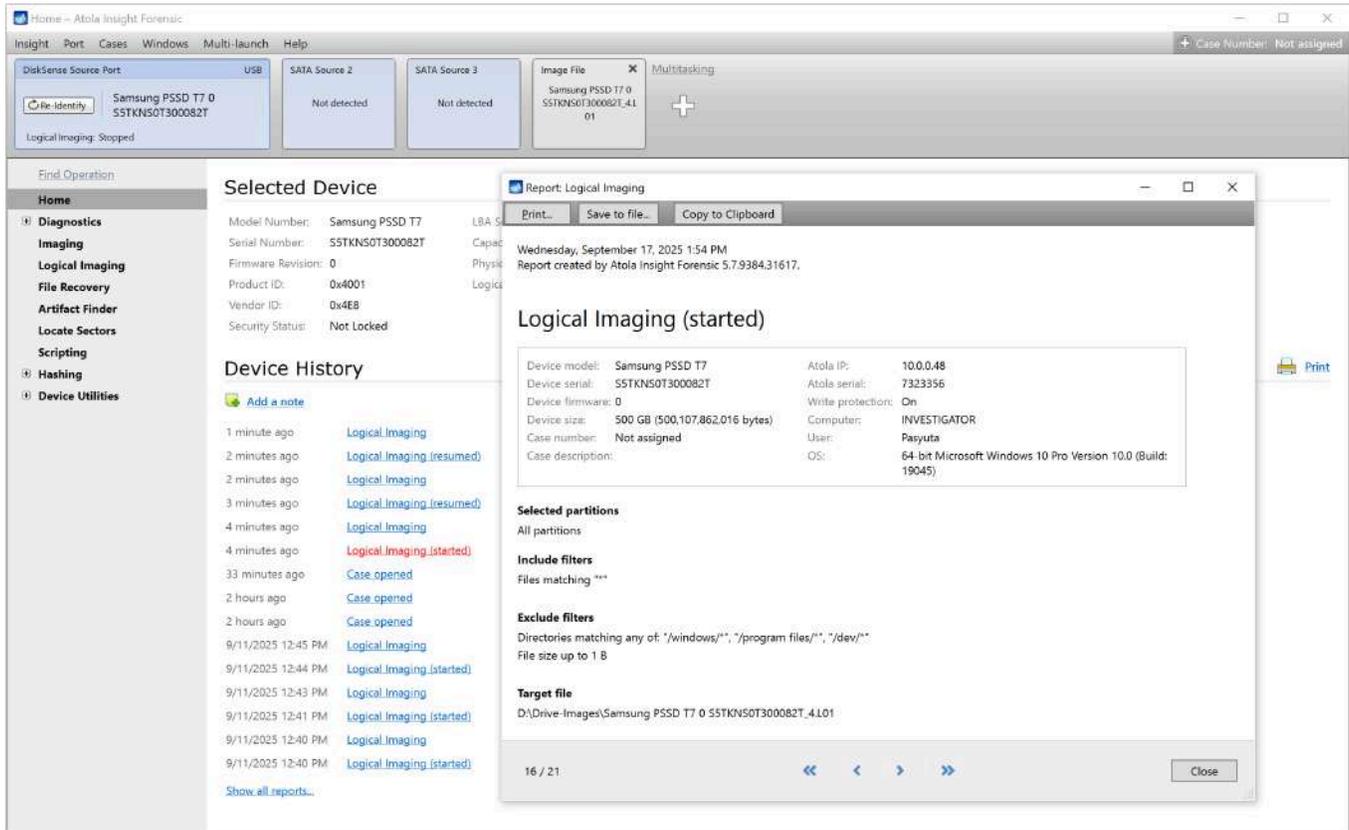
## Logical imaging process. Pause and resume

The logical imaging process starts immediately when you click **Create** in the **Create Logical Image File** dialog.



### The Logical imaging progress screen.

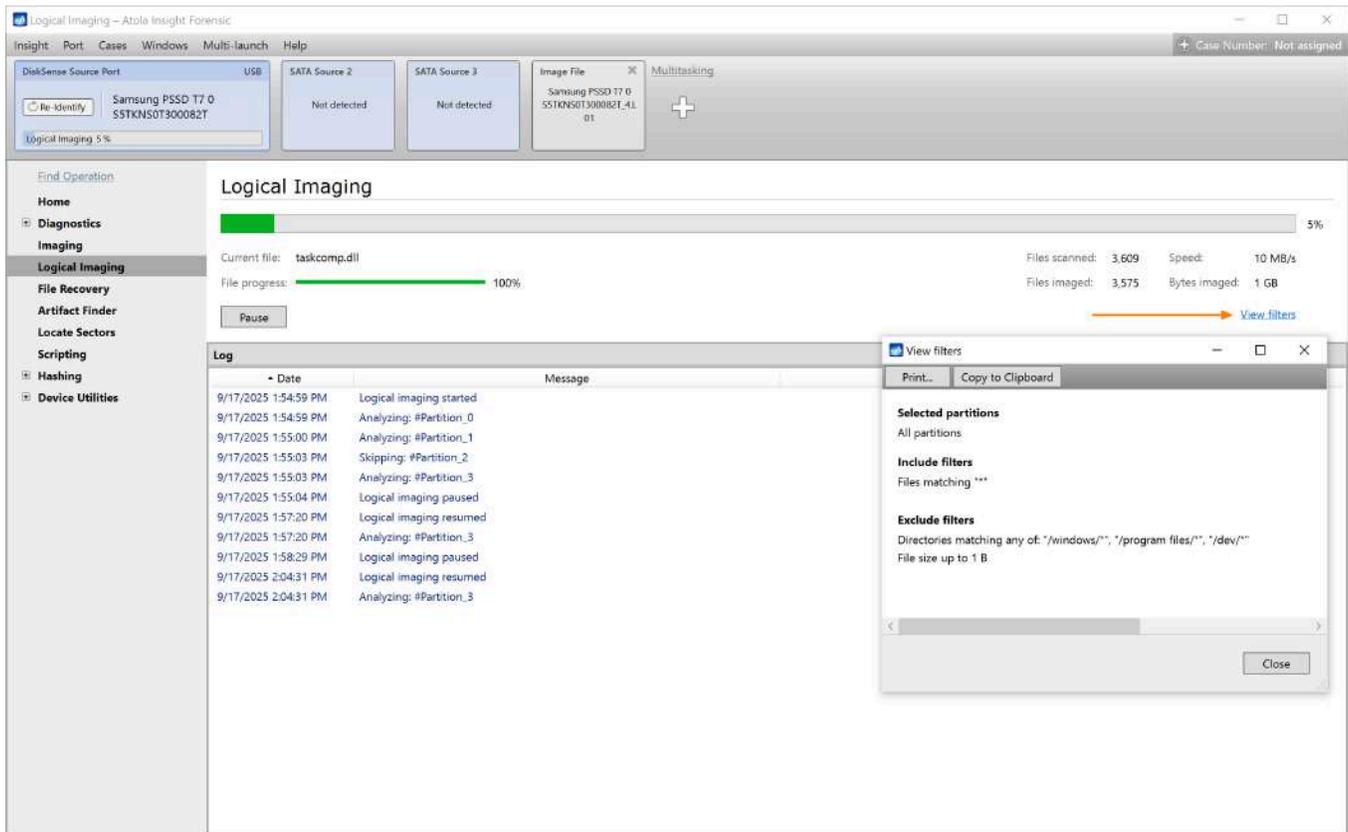
Once imaging is launched, Insight creates a **Logical imaging (started)** report. It contains all details about the imaging source and target(s), as well as information about the include or exclude filters. You can find this report on the device **Home** screen, in the **Device history** section.



## The 'Logical Imaging (started)' report.

During the imaging process, you can track the progress of individual files.

To check the filtering parameters of the running session, click the **View filters** link on the right.



## The 'View filters' option.

## Pause and Resume

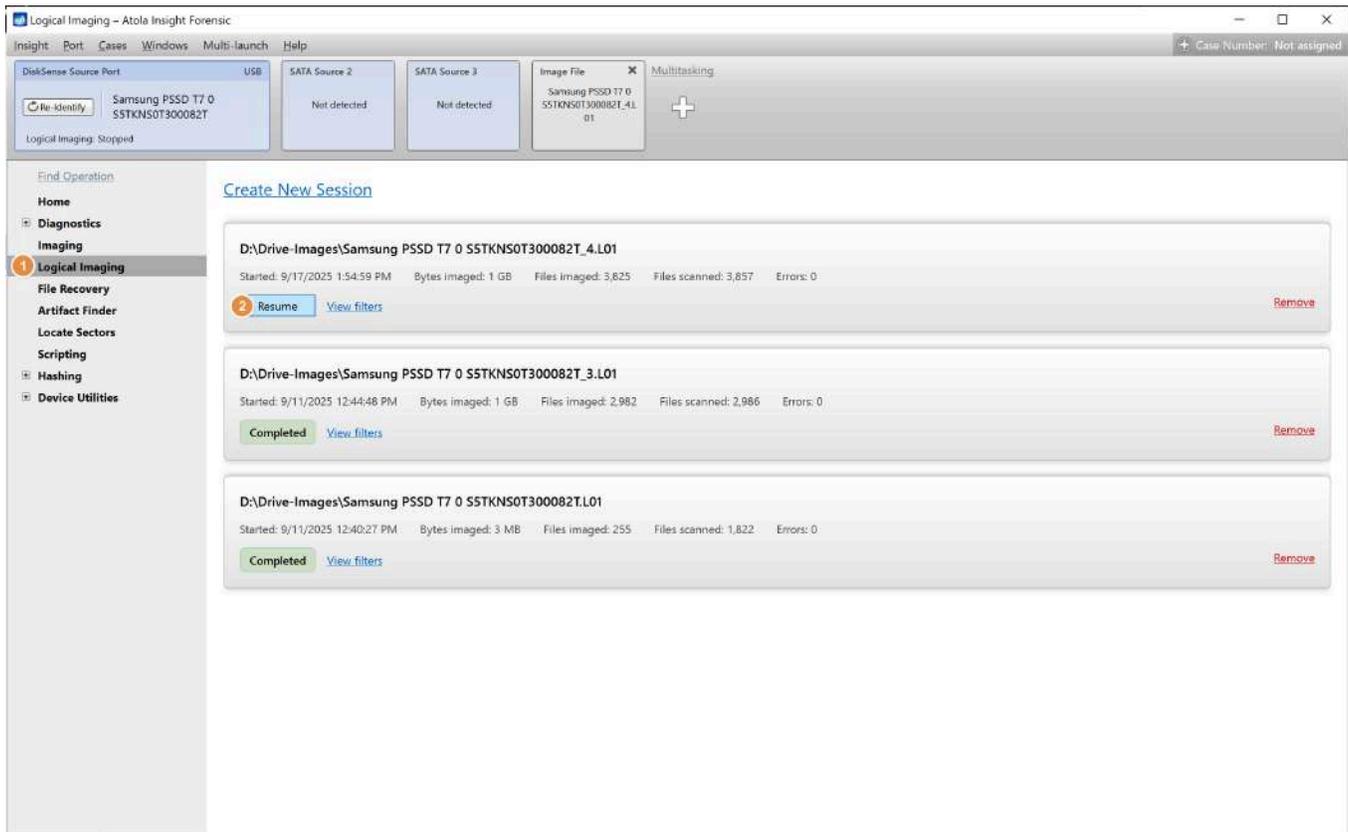
Insight lets you pause any logical imaging session and resume it later.

This feature could be helpful when you need to:

- Turn off your equipment and leave the lab for a night, or
- Continue a logical imaging process at a different location

**Pause:** While the logical imaging process is running, click the **Pause** button on the left.

**Resume:** In the Sidebar, click **Logical**, find your paused session and click the **Resume** button.



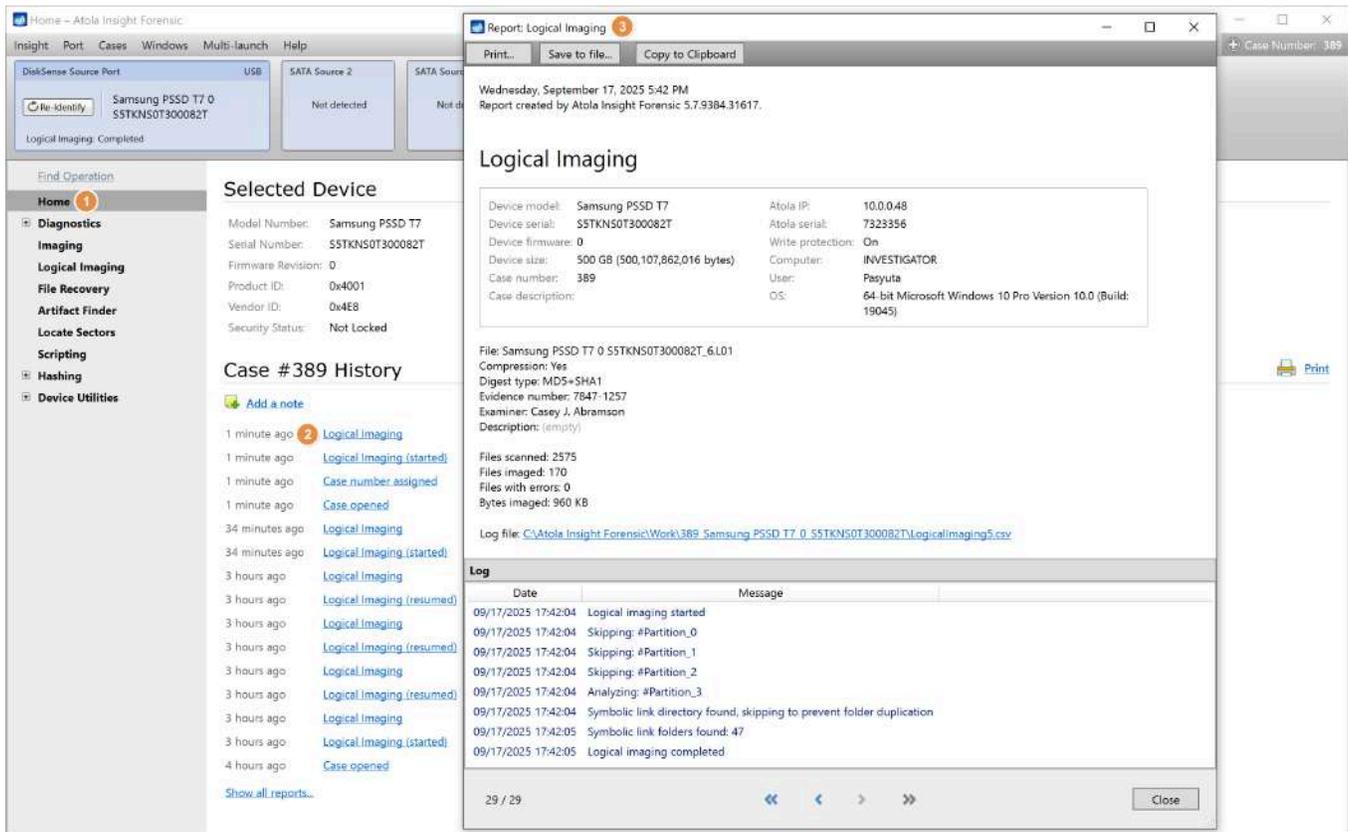
**Resuming the paused logical imaging session.**

## Logical imaging report

After the logical imaging process is completed, Insight generates a comprehensive report with all the details of the imaged data:

- The number of scanned and imaged files
- The volume of imaged data
- Timestamps
- and more

You can find the **Logical imaging** report on the device **Home** screen, in the **Device history** section.



The Logical imaging report.

## Clip target drive to source evidence device size

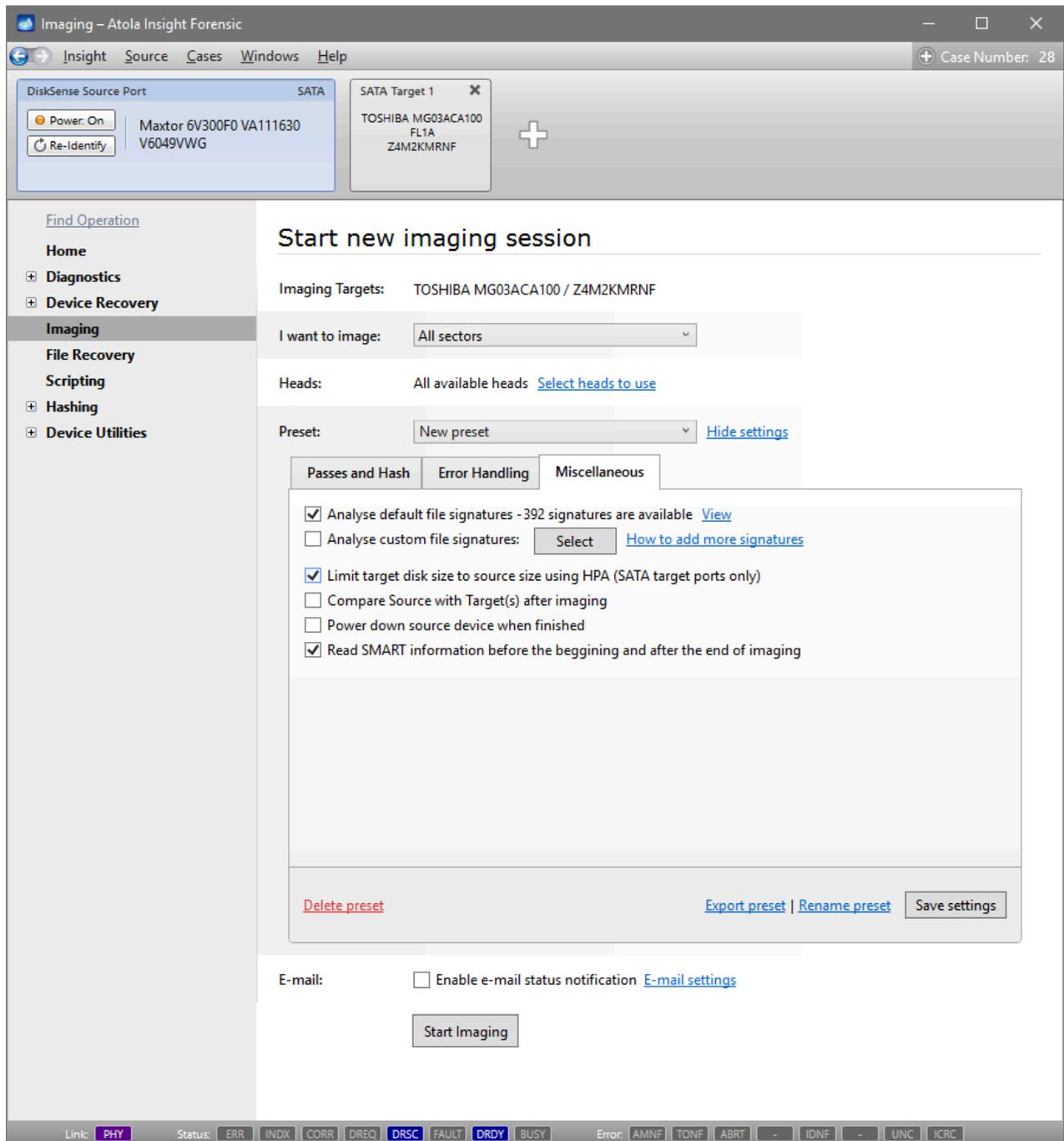
When you image data from a drive involved in an investigation case, and the target drive will be holding a 1:1 clone of evidence data, in many cases it is critical that the target drive's capacity is identical to that of the source drive. Should there be a difference in size between the source and the target devices, their hashes will be different too.

However, if your SATA target drive has a larger capacity, you can limit its size to that of the source drive using Host Protected Area (HPA). It will make the sectors beyond this limit inaccessible to the hashing tools as well as the end user.

Enabling HPA is an option available only for SATA target drives.

To clip target drive to source evidence device size, do the following:

1. In the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. In the **Preset** line, click the **Show settings** link.
4. On the **Miscellaneous** tab, select the **Limit target disk size to source size using HPA (SATA target ports only)** option.



## Enabling HPA restriction for target

5. Click the **Start Imaging** button.
6. To indicate that HPA has been enabled on the target drive, Insight displays an **HPA** tag on the target drive port.

Home – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 28

SATA Source  
Maxtor 6V300F0  
VA111630  
V6049VWG

DiskSense Target Port  
SATA Target 1 X  
Power: On  
Re-Identify  
TOSHIBA MG03ACA100 FL1A  
Z4M2KMRNF  
HPA

Find Operation

Home

- Diagnosics
- File Recovery
- Scripting
- Hashing
- Device Utilities

### Selected Device

Model Number:	TOSHIBA MG03ACA100	LBA Sectors:	586,114,704
Serial Number:	Z4M2KMRNF	Capacity:	300,090,728,448 (300 GB)
Firmware Revision:	FL1A	LBA48 Mode:	Supported
Security Status:	Not Locked	Physical Sector Size:	512 Bytes

[View ID sector](#)

### Case #28 History

[Add a note](#)

- 1 hour ago [Imaging target](#)
- 2 hours ago [Imaging \(started\)](#)
- 2 hours ago [Host Protected Area](#)
- 2 hours ago [ID sector saved](#)
- 2 hours ago [Case opened](#)
- 2 hours ago [Atola Insight Forensic closed](#)
- 2 hours ago [Compare](#)
- 2 hours ago [Compare \(started\)](#)
- 2 hours ago [Diagnostics report](#)
- 2 hours ago [ID sector saved](#)
- 2 hours ago [Case opened](#)
- 2 hours ago [Diagnostics report \(started\)](#)

[Show all reports...](#)

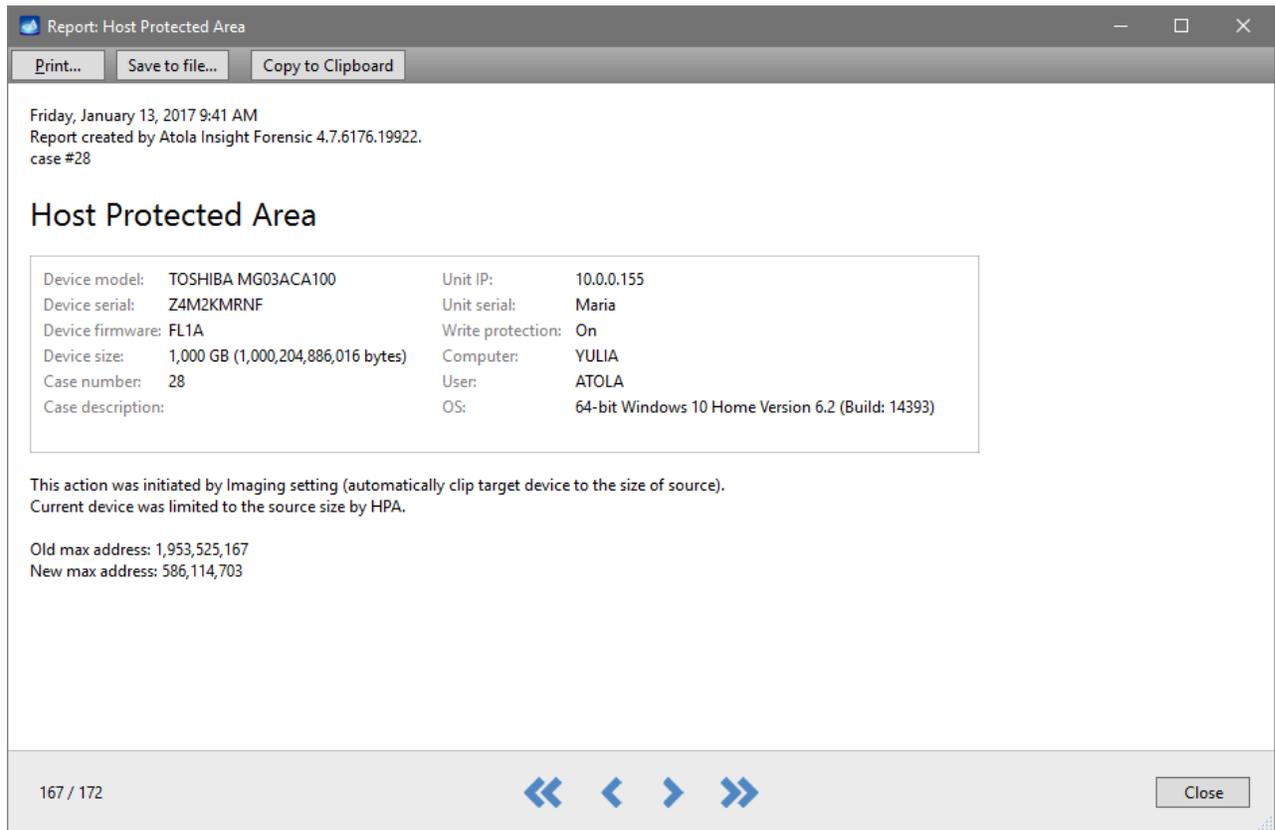
[Add description](#)  
This device has no description. You can add it for current device right now.

[Manage attached files](#) +

Print

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

7. In the **Case History**, Insight creates a report with the information about the time when HPA was enabled, a detailed device description and how this action was initiated. The report also indicates the initial max address as well as the current one.



To make sure that source and target are identical after enabling HPA, calculate hashes on both drives.

## Artifacts search

Imaging is a time-consuming part of the evidence acquisition process, especially when dealing with damaged drives.

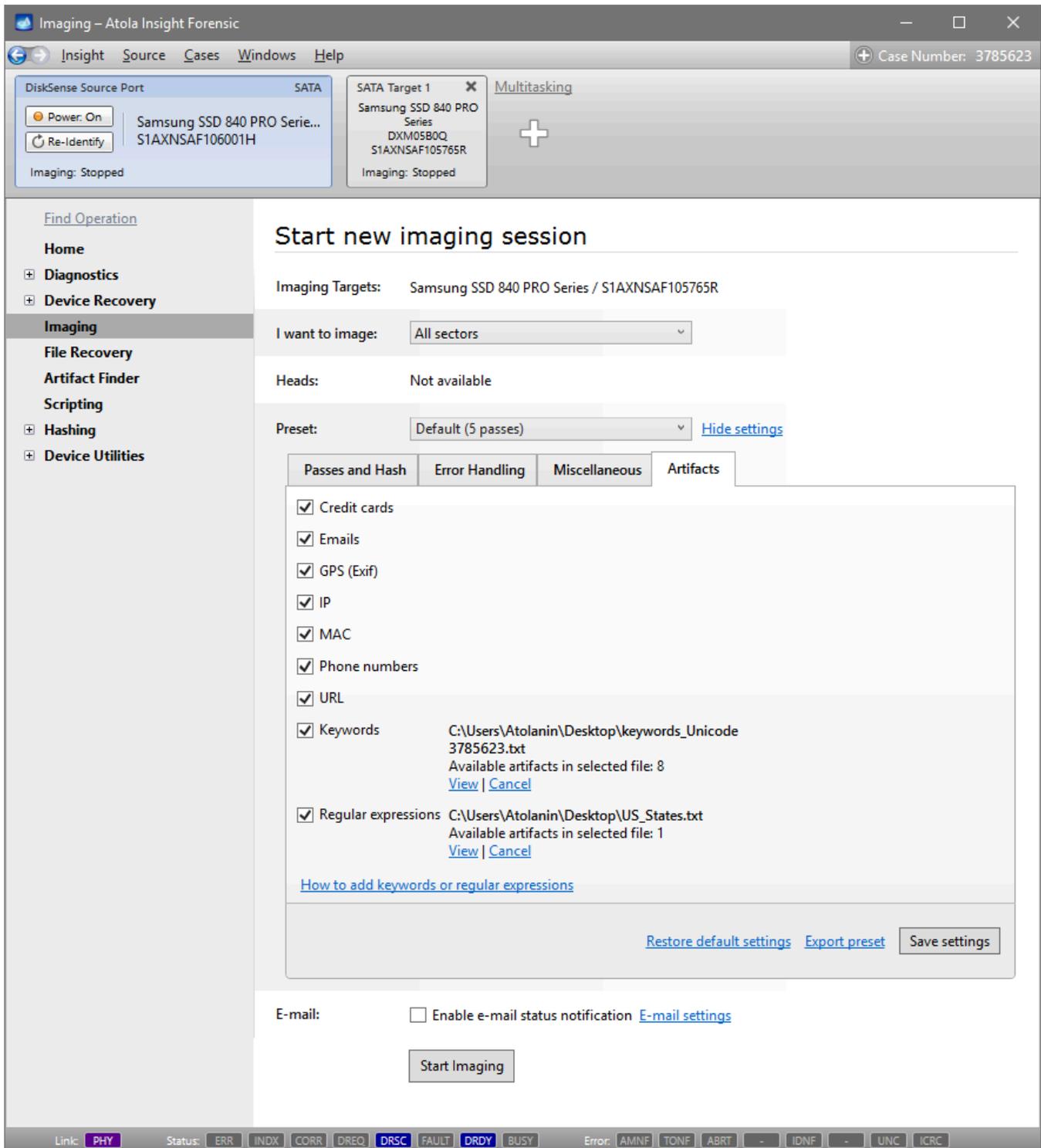
Even though Atola Insight Forensic is the fastest forensic imaging tool in the world (there is literally no penalty on a drive speed when you image it with Insight!), we want to help expedite forensic process even further. The **artifact search** feature allows analysis of data from an evidence device in the course of imaging.

Unlike most forensic analysis tools that parse the file structure, Insight does sector-level parsing, which allows getting data even from the spaces of the drive that are not associated with any file (e.g. remnants of previously deleted documents), thus providing you with clues that are omitted by most analysis tools. Artifact finder uses Intel Hyperscan engine, which makes it the fastest possible tool for primary data analysis.

## Artifacts settings

1. On the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. In the **Target Device Selection** dialog, select target device.

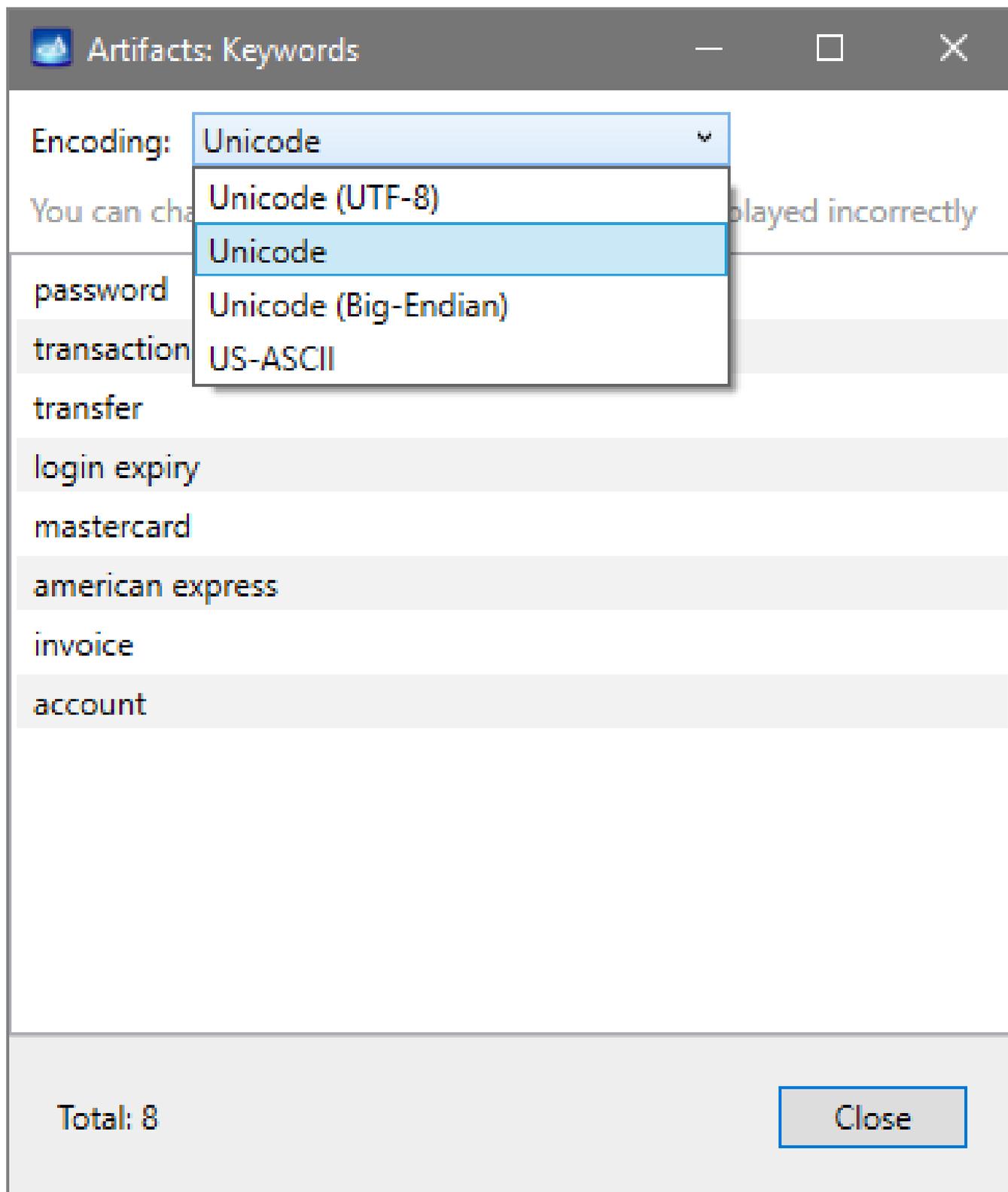
4. Open the Artifacts tab.



In this tab it is possible to view, select or deselect the artifacts you want to be searched in the course of imaging.

For each of these artifacts we have not only applied well-known algorithms including the Luhn formula used to validate credit card numbers, but also applied our own smart filters to eliminate false results (for example, if there are two slashes near the number that has preliminarily been identified as a credit card number, that will eliminate it from the search results, as it is likely to be a part of a URL).

Keywords and regular expressions can be added to the search parameters in a txt file with one artifact per line. Next to the **Keywords** category on the **Artifacts** tab, click the **View** link before imaging and make sure the keywords are displayed correctly. Keyword encoding can be adjusted to **Unicode**, **Unicode (UTF-8)**, **Unicode (Big-Endian)** or **US-ASCII**.



The screenshot shows a window titled "Artifacts: Keywords" with a standard Windows-style title bar (minimize, maximize, close buttons). The main content area displays a list of keywords: "password", "transaction", "transfer", "login expiry", "mastercard", "american express", "invoice", and "account". Each keyword is on a separate line with a light gray background. A dropdown menu is open over the "Encoding:" label, showing five options: "Unicode" (selected), "Unicode (UTF-8)", "Unicode", "Unicode (Big-Endian)", and "US-ASCII". At the bottom left, it says "Total: 8". At the bottom right, there is a "Close" button.

Artifacts: Keywords

Encoding: Unicode

You can change the encoding of the keywords displayed incorrectly

password

transaction

transfer

login expiry

mastercard

american express

invoice

account

Total: 8

Close

A few of the artifacts are selected by default, namely: *GPS, MAC, Phone numbers, URL*. You can adjust these default settings and click the **Save settings** button. This will affect all future imaging sessions (including those on new source drives) unless you re-adjust the settings or restore the default settings by clicking the corresponding link. The paths to the files with keywords and regular expressions will also remain saved, although should any changes be made to the txt files in the saved directory, the changes will be uploaded at the start of each imaging session.

It is advisable that no more than 4 artifacts are selected at a time, otherwise imaging will slow down considerably. Also, keywords consisting of less than 4 symbols or regular expressions consisting of less than 6 symbols; large number of keywords (more than 2000) or regular expressions (more than 10) may also slow down imaging process. This is due to the large number of results such search parameters are capable of producing.

Once you have ticked the boxes next to the artifacts you would like to be searched for, click the **Start Imaging** button.

## Browse through the artifacts in the course of imaging

Once imaging has begun, go to the **Artifacts** tab in the bottom part of Insight window and watch the selected artifacts being found: the numbers of artifacts and the corresponding diagram change on the go.

To see the artifacts in a list, press on any of the categories or the diagram.

**Imaging data...** 86%

0 1,000,215,215

Pass: 2 of 5  
Overall speed: 170 MB/s  
Estimated time left: 6 minutes

Sectors imaged: 868,214,224  
Sectors left: 132,000,992  
Last attempted block: 554,653,599

Found signatures: [305587](#) Total errors: **149**

Pause [Imaging settings](#) [Legend](#)

**Artifacts: 2.7M**

Category	Count
Credit cards	1350
Emails	76350
GPS (Exif)	0
Keywords	8040
IP	11791
MAC	38237
Phone numbers	1134
Regular expressions	0
URL	2529233

In the table, each artifact is assigned an **Id** number, each found **Value** is shown in the context (including 20 bytes before and 20 bytes after the artifact in grey color), the **LBA** and the **Offset** are also displayed in the table to help locate the artifact.

There are many options to help find, sort, filter and view the artifacts: it is possible to view one or a few categories of artifacts in one list, use the **Search** bar to find a specific value (search examples are provided in the bottom right corner of the window), filter results for unique values by clicking the **Show unique artifacts** link.

Artifacts				
Search artifacts by value or LBA				Search
<input checked="" type="checkbox"/> Credit cards <input checked="" type="checkbox"/> Emails <input checked="" type="checkbox"/> GPS (Exif) <input checked="" type="checkbox"/> Keywords <input checked="" type="checkbox"/> IP <input checked="" type="checkbox"/> MAC <input checked="" type="checkbox"/> Phone numbers <a href="#">Show only unique artifacts</a>				
<input checked="" type="checkbox"/> Regular expressions <input checked="" type="checkbox"/> URL				
Found artifacts: 2,709,917			Page: 114 / 96783	◀◀ ▶▶
Id	Type	Value	Lba	Offset
3165	Emails	00.08U0">1"00.ID: <20592.1022586929.1@example.c	722,477	1D6
3166	Emails	: "Allison Dunlap" <xxx@example.com>.To: yyy@exa	722,479	059
3167	Emails	xx@example.com>.To: yyy@example.com.Subject: 644	722,479	06E
3168	Emails	Delivery Subsystem <xxx@example.com>.To: yyy@.0c	722,479	199
3169	Emails	...à.Return-Path: <barry@python.org>.Delivered-	722,483	124
3170	Emails	...à<Return-Path: <sender@example.net>.Delivery	722,486	0AC
3171	Emails	22..!³np0.X2MÀ!-IDà.4B66B890.4070408@teconcept.d	722,486	1EE
3172	URL	IesÈ0 XÉ.lon0ÀW atà.http://sf.net/proj.kis/mime1	722,512	066
3173	URL	or ROT13... ..à.See http://ucsub.colorado.edu/~k	723,253	185
3174	URL	or ROT13... ..à.See http://ucsub.colorado.edu/~k	723,257	0A1
3175	URL	or ROT13... ..à.See http://ucsub.colorado.edu/~k	723,260	18D
3176	Emails	d..A.là. Wirzenius <liw@iki.fi>..#.>èGerrit Ho..	723,471	1E9
3177	Emails	: Paul Kippes <k..à.p@gmail.com>..import unittes	726,873	05C
3178	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,088	04C
3179	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,097	020
3180	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,102	15A
3181	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,106	0EB
3182	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,109	0C1
3183	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,112	121
3184	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,115	10A
3185	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,119	1C5
3186	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,124	0B9
3187	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,129	061
3188	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,132	082
3189	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,135	088
3190	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,138	0B4
3191	URL	etic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,145	078
3192	URL	ic ..@6c.0s"0à.at http://www2.hursley.ibm.com/	727,151	003

The latter option is quite valuable as it helps identify the values most frequently occurring on the drive: to sort the results click **Count** in the table header.

Artifacts

Search artifacts by value or LBA Search

Credit cards  Emails  GPS (Exif)  Keywords  IP  MAC  Phone numbers [Show all artifacts](#)

Regular expressions  URL

Found artifacts: 2,709,917 Page: 1 / 4780 ◀◀ ◀ ▶ ▶▶

Type	Value	Count
URL	http://i.imgur.com	120,940
URL	http://www.w3.org	116,161
URL	http://ns.adobe.com	105,172
URL	http://news.google.com	103,661
URL	http://www.reddit.com	94,406
URL	http://swcdn.apple.com	81,780
URL	http://www.apple.com	80,799
URL	http://appldnld.apple.com	71,512
URL	https://swdist.apple.com	64,662

View sector Export to CSV [Search examples](#)

To promptly find the sector where an artifact is located, you can double click the artifact you would like to examine more thoroughly.

Artifacts

Search artifacts by value or LBA Search

Credit cards
  Emails
  GPS (Exif)
  Keywords
  IP
  MAC
  Phone numbers
 [Show only unique artifacts](#)

Regular expressions
  URL

Found artifacts: 2,709,917 Page: 114 / 96783

Id	Type	Value	Lba	Offset
3165	Emails	08.0808".>1"0à.ID: <20592.1022586929.1@example.c	722,477	1D6
3166	Emails	: "Allison Dunlap" <xxx@example.com>.To: yyy@exa	722,479	059
3167	Emails	xx@example.com>.To: yyy@example.com.Subject: 644:	722,479	06E
3168	Emails	Delivery Subsystem <xxx@example.com>.To: yyy8.0ç	722,479	199
3169	Emails	...à.Return-Path: <barry@python.org>.Delivered-	722,483	124

Sector View

1 sector(s) read starting from 0xB0633.

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Data
Sector #722483																	
160C6600	BD	80	62	09	62	79	A2	22	67	5F	64	1A	29	E0	06	53	¼.b.byç"q_d.)à.S
160C6610	4D	54	50	0A	09	69	64	20	41	32	33	32	41	44	30	33	MTP..id A232AD03
160C6620	44	45	33	41	3B	39	6F	FE	9E	33	35	F7	1F	DB	1F	A4	DE3A;9op.35÷.Û.¼
160C6630	15	7F	17	DF	1F	3A	5E	F7	19	CB	C6	53	61	74	6E	37	...ß.:^÷.ËÆSatn7
160C6640	F2	80	59	30	33	E7	3A	33	30	20	55	54	43	A7	1B	6B	ò.Y03ç:30 UTC\$.k
160C6650	8F	BE	19	49	6D	C0	4B	61	6E	63	4F	9B	1F	4E	47	80	.¼.ImÅKancO..NG.
160C6660	20	6C	ED	50	72	69	6F	72	69	74	79	3A	20	33	20	28	liPriority: 3 (
160C6670	18	16	40	17	29	C0	3D	4D	53	4D	38	1E	F1	20	31	22	..@.)Å=MSM8.ñ 1"
160C6680	A9	BF	0A	86	2D	49	44	A3	FF	86	3A	44	F4	3F	94	21	©ç..-ID&y.:Dô?!.!
160C6690	E6	6D	69	78	65	64	3B	A2	7C	85	40	01	3D	E0	00	36	æmixed;ç .@.=à.6
160C66A0	37	62	64	32	62	37	61	35	2E	66	39	39	66	37	22	3A	7bd2b7a5.f99f7":
160C66B0	44	F0	07	3A	C3	F0	06	E4	2D	2D	0A	0A	06	00	00	00	Dò.:Åð.ä--.....
160C66C0	00	00	00	00	00	2E	00	00	00	03	C1	D1	00	00	00	00	.....ÅÑ....
160C66D0	00	11	00	63	00	6F	00	6D	00	2E	00	61	00	70	00	70	...c.o.m...a.p.p
160C66E0	00	6C	00	65	00	2E	00	64	00	65	00	63	00	6D	00	70	.l.e...d.e.c.m.p
160C66F0	00	66	00	73	00	00	00	10	00	00	00	00	00	00	00	00	.f.s.....
160C6700	00	00	02	6E	66	70	6D	63	07	00	00	00	07	F3	03	00	...nfpmc.....
160C6710	00	00	00	00	E0	1E	52	65	74	75	72	6E	2D	50	61	74	....à.Return-Pat
160C6720	68	3A	20	3C	62	61	72	72	79	40	70	79	74	68	6F	6E	h: <barry@python
160C6730	2E	6F	72	67	3E	0A	44	65	6C	69	76	65	72	65	64	2D	.org>.Delivered-
160C6740	54	6F	3A	20	38	20	F6	E5	0A	52	65	63	65	F3	40	1B	To: 8 0à.Receó@.
160C6750	64	E7	79	20	6D	61	69	6C	2E	38	1D	E0	0D	20	28	50	dçy mail.8.à. (P
160C6760	6F	73	74	66	69	78	2C	20	66	72	6F	6D	20	75	73	65	ostfix, from use
160C6770	72	69	64	20	38	38	39	29	0A	09	00	09	E0	12	43	32	rid 889)....à.C2
160C6780	42	46	30	44	33	37	43	36	3B	20	54	75	65	2C	20	31	BF0D37C6; Tue, 1
160C6790	31	20	53	65	70	20	32	30	30	31	20	30	30	3A	30	35	1 Sep 2001 00:05
160C67A0	00	03	E0	43	20	2D	30	34	30	30	20	28	45	44	54	29	..àç -0400 (EDT)
160C67B0	0A	4D	49	4D	45	2D	56	65	72	73	69	6F	6E	3A	20	31	.MIME-Version: 1
160C67C0	2E	30	0A	43	6F	6E	74	65	6E	74	2D	54	79	70	65	3A	.0.Content-Type:
160C67D0	20	6D	75	6C	74	69	70	61	72	74	2F	6D	69	78	65	64	multipart/mixed
160C67E0	3B	20	62	6F	75	6E	64	61	72	79	3D	22	68	39	30	56	; boundary="h90V
160C67F0	49	49	49	4B	6D	78	22	38	35	E0	11	72	61	6E	73	66	IIKmx"85à.ransf

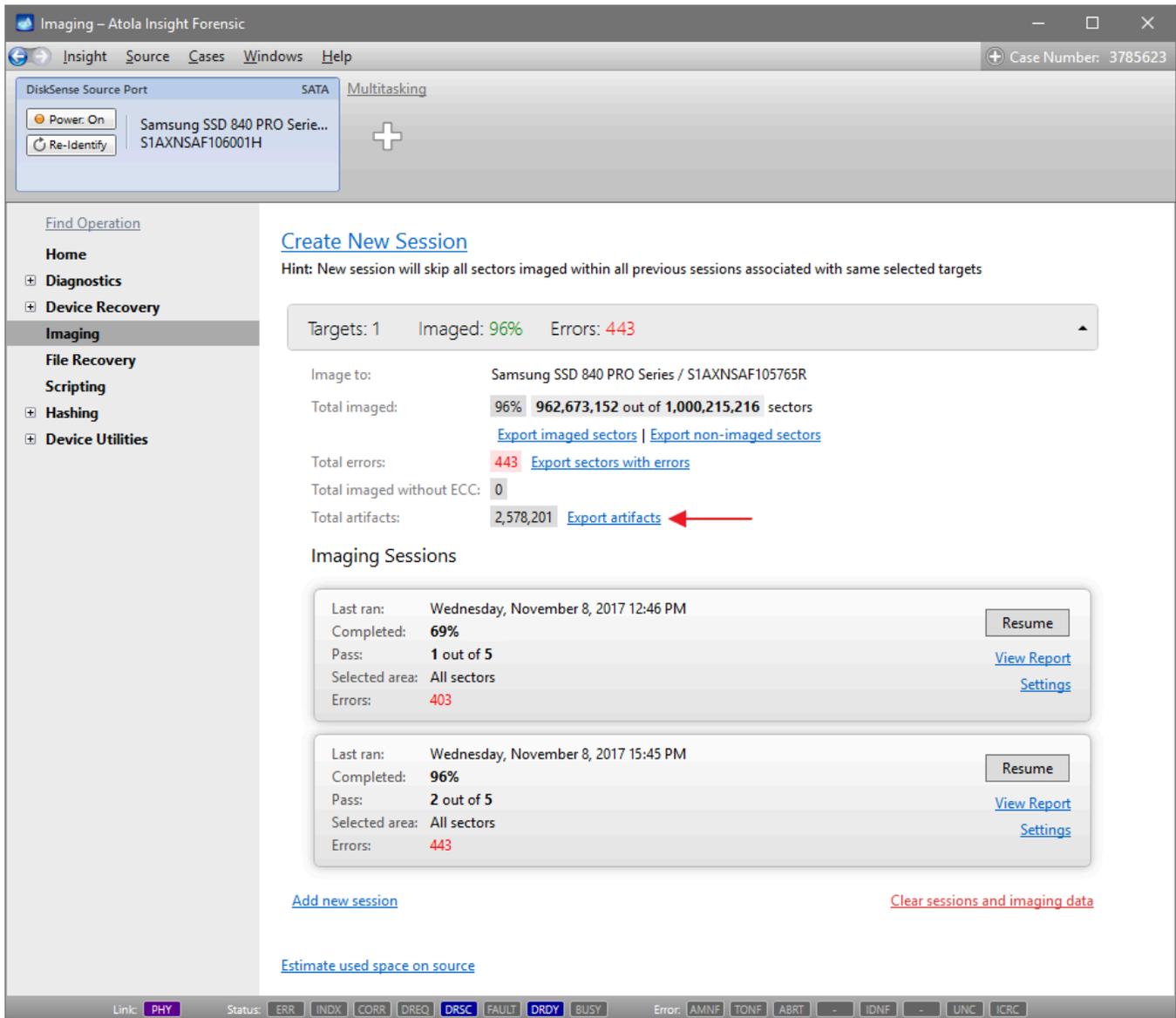
Save to file... Close

# Export artifacts

The **Export to CSV** button is disabled during imaging. You can wait until imaging is completed or pause it, make an export and restart imaging, should it be necessary to start analyzing the current artifact search output with an external tool:

1. **Pause** imaging.
2. On the **Imaging results** screen, click the **Artifacts** link.
3. On the **Artifacts** screen, select the artifacts you would like to be exported (for example, one or multiple artifact categories, unique artifacts or only those fitting certain search criteria).
4. Click the **Export to CSV file** button.
5. Select the path for the file and click **Export**.
6. Once the export is completed (which normally takes no longer than a few seconds), restart imaging.

Now, in the **Imaging** category on the **Sidebar**, there is the **Export artifact** link. If the source drive was imaged in multiple sessions, and artifact lists were created during different imaging sessions, by clicking this link you can download a merged list of artifacts from multiple imaging sessions.



## Split an imaging session to separate targets

While a multi-target imaging is paused, one or more targets may become unavailable. The drive may be taken and used by another technician or broken, or the server with the image file may become unavailable.

To finish the imaging to the remaining target as fast as possible and start analyzing the evidence, you can split imaging sessions.

## Split an interrupted multi-target imaging session

1. Connect the source device to the DiskSense unit.

2. In the sidebar, click **Imaging** and find the interrupted imaging session to several targets. If not all target drives and image files are available, it is impossible to simply resume imaging.
3. To split the interrupted imaging session into separate ones, one per each target, click the **Split all sessions to separate targets** link. Insight splits the session.

Imaging – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 0275

DiskSense Source Port SATA Multitasking

Power: On WDC WDS120G1G0A-00SS50...  
Re-Identify 171710A0035D

Find Operation

Home

⊕ Diagnostics

⊕ Device Recovery

**Imaging**

File Recovery

Scripting

⊕ Hashing

⊕ Device Utilities

### Create New Session

Hint: New session will skip all sectors imaged within all previous sessions associated with same selected targets

Targets: 3 Imaged: 90% Errors: 0

Image to:

- WDC WDS120G1G0A-00SS50 / 171710A0077B
- C:\Users\Atolanin\Desktop\WDC WDS120G1G0A-00SS50\_Z3311000\_171710A0035D.img
- Samsung SSD 850 PRO 128GB / S24ZNX0HC02402P

Total imaged: 90% 211,124,224 out of 234,441,648 sectors  
[Export imaged sectors](#) | [Export non-imaged sectors](#)

Total errors: 0

Total imaged without ECC: 0

#### Imaging Sessions

Last ran: Friday, July 14, 2017 1:55 PM

Completed: 90% [Resume](#)

Pass: 1 out of 5 [View Report](#)

Selected area: All sectors [Settings](#)

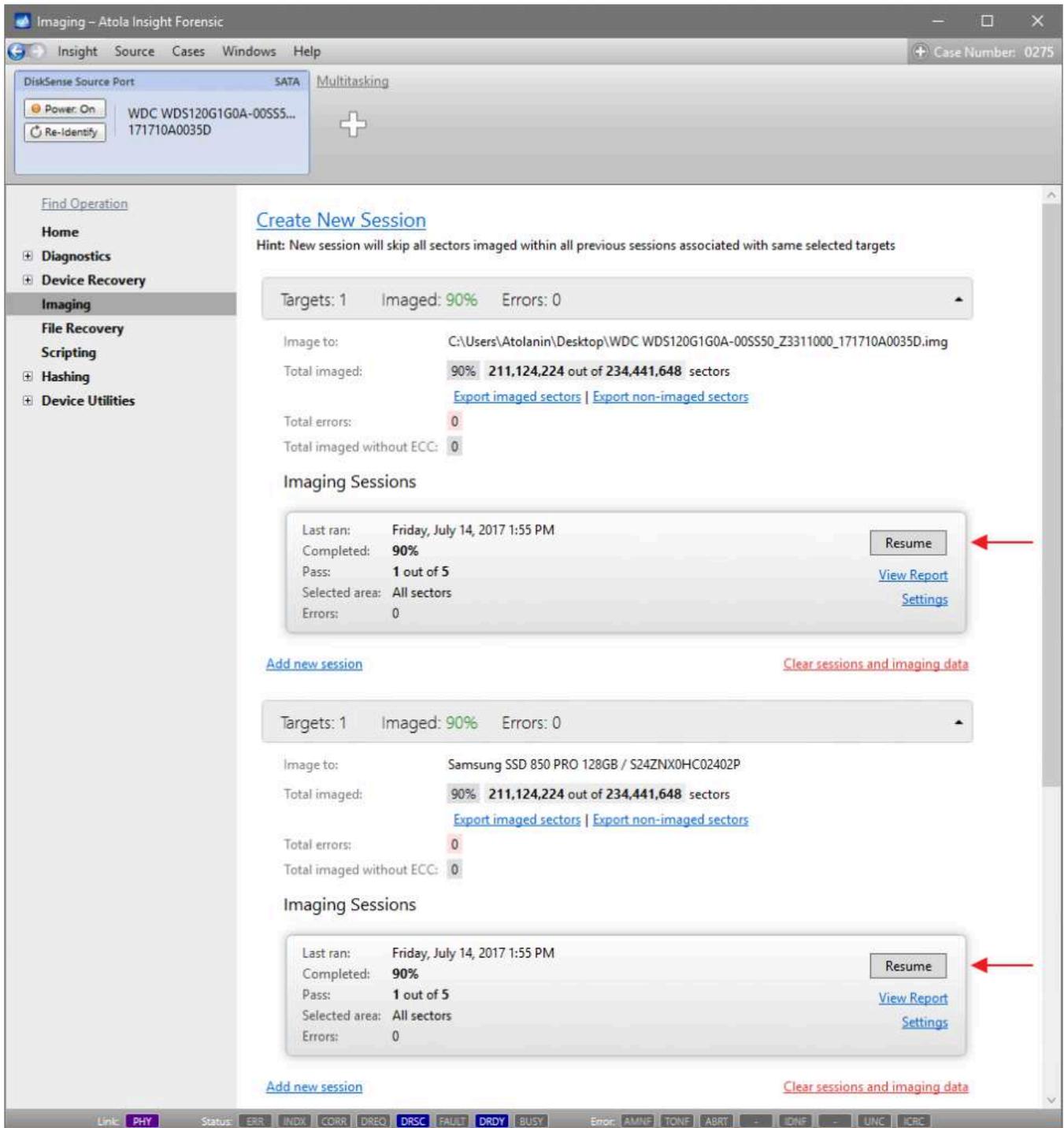
Errors: 0

[Add new session](#) [Split all sessions to separate targets](#) [Clear sessions and imaging data](#)

[Estimate used space on source](#)

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

4. To resume imaging to each separate target, click **Resume** in each target's **Imaging Session**.



5. The resumed imaging session skips all the sectors imaged to the target during the previous session.

Imaging – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 0275

DiskSense Source Port SATA

Power: On Re-Identify WDC WDS120G1G0A-00SS5... 171710A0035D Imaging 97%

SATA Target 1 WDC WDS120G1G0A-00SS50 Z3311000 171710A0077B Imaging 97%

Multitasking

Find Operation

- Home
- Diagnosics
- Device Recovery
- Imaging**
- File Recovery
- Scripting
- Hashing
- Device Utilities

Imaging data... 97%

0 234,441,647 [Activate zoom](#)

Pass: 1 of 5 Sectors imaged: 228,335,616

Overall speed: 221 MB/s Sectors left: 6,106,032

Estimated time left: 33 seconds Last attempted block: 228,335,615

Found signatures: 0 Total errors: 0

Pause [Imaging settings](#) [Legend](#)

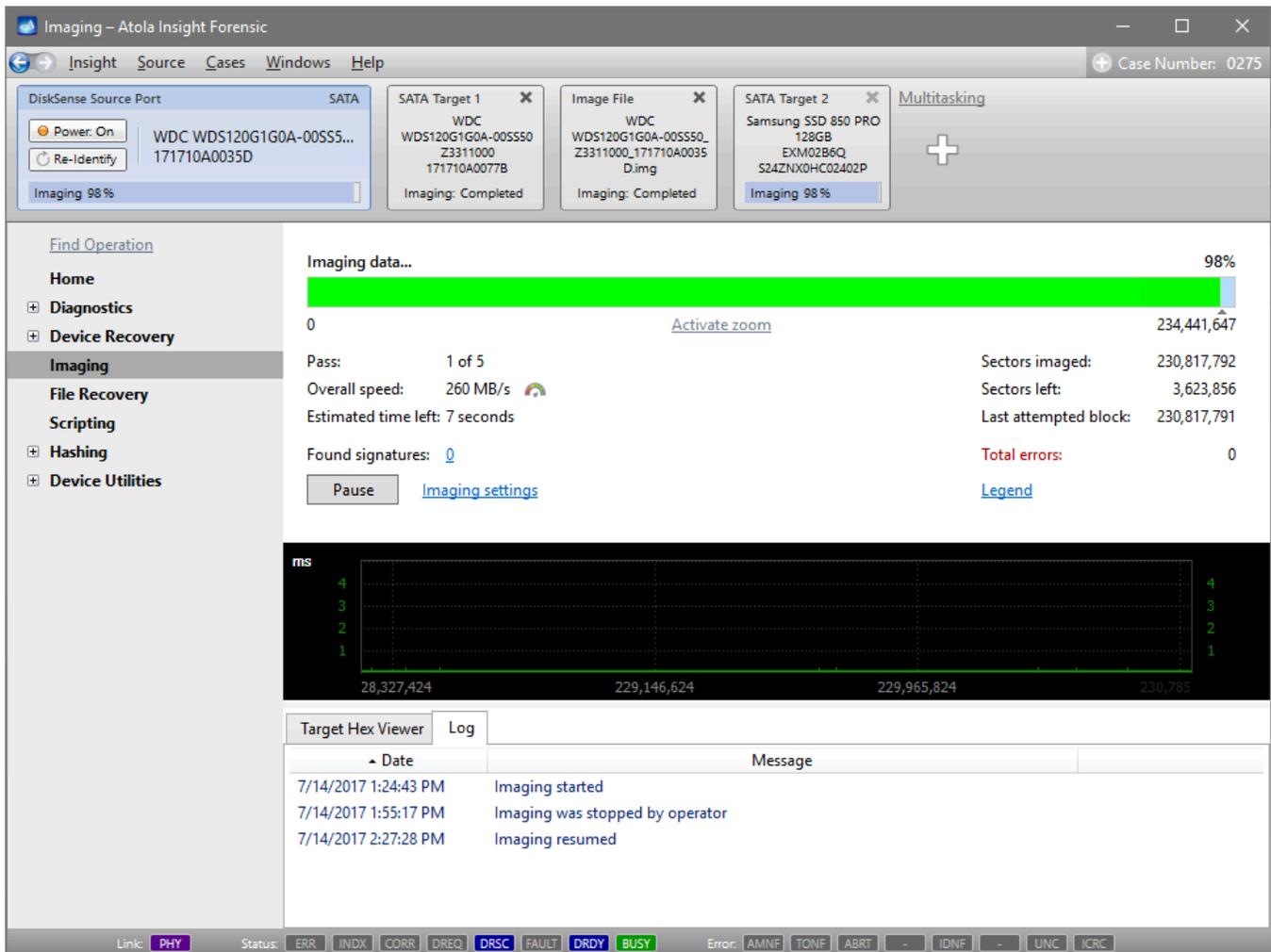
ms

Target Hex Viewer Log

Date	Message
7/14/2017 1:24:43 PM	Imaging started
7/14/2017 1:55:17 PM	Imaging was stopped by operator
7/14/2017 2:16:17 PM	Imaging resumed

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

This way you can complete the imaging to all targets at different times, as they become available.



If a target becomes unavailable during imaging, the process automatically stops, and you can try to either resume the imaging to all targets, or split imaging sessions should it be necessary.

## Imaging only selected sectors

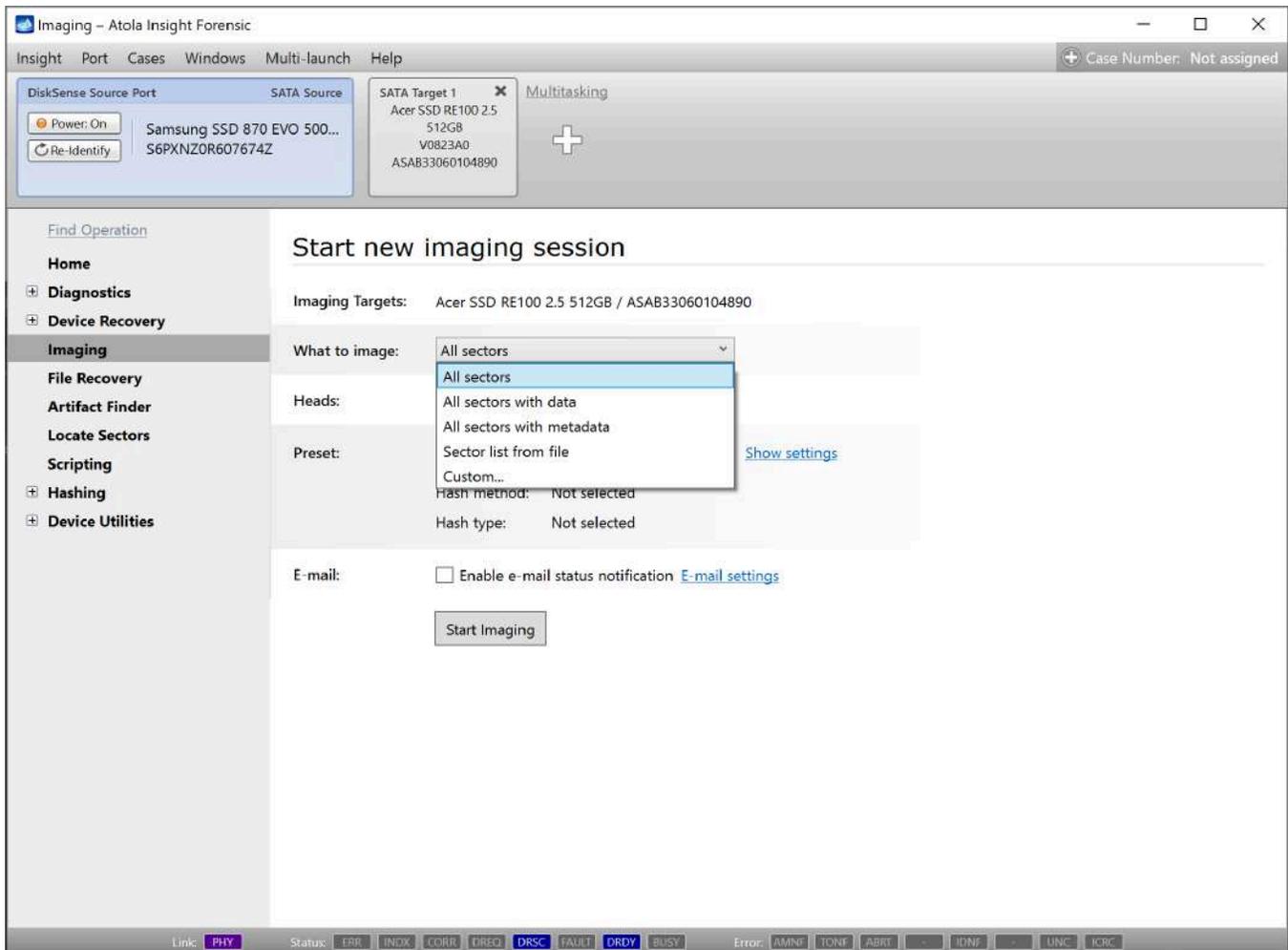
While physical imaging involves sector-for-sector copying of the whole evidence drive from the first LBA to the last one, selective acquisition implies bit-for-bit copying of the file structure.

The selective acquisition is handy when time is limited and you need to quickly start working with the file structure. At the same time, the image of only selected sectors does not include remaining fragments of previously deleted files, which makes this imaging method incomplete. On top of that, the hash values of the source and the target drives as a result of such imaging will not be identical. For these reasons, it may be preferable to use a physical image.

This guide will show how Atola Insight Forensic's flexible imaging functionality enables users to perform selective imaging. As for image verification, this guide will demonstrate how segmented hashing can help you verify such an image.

# All sectors

By default, Insight Forensic is set to image **all sectors** of a drive. With this option selected in the **What to image** list on the imaging setting screen, the system will create a full physical copy of a source drive.

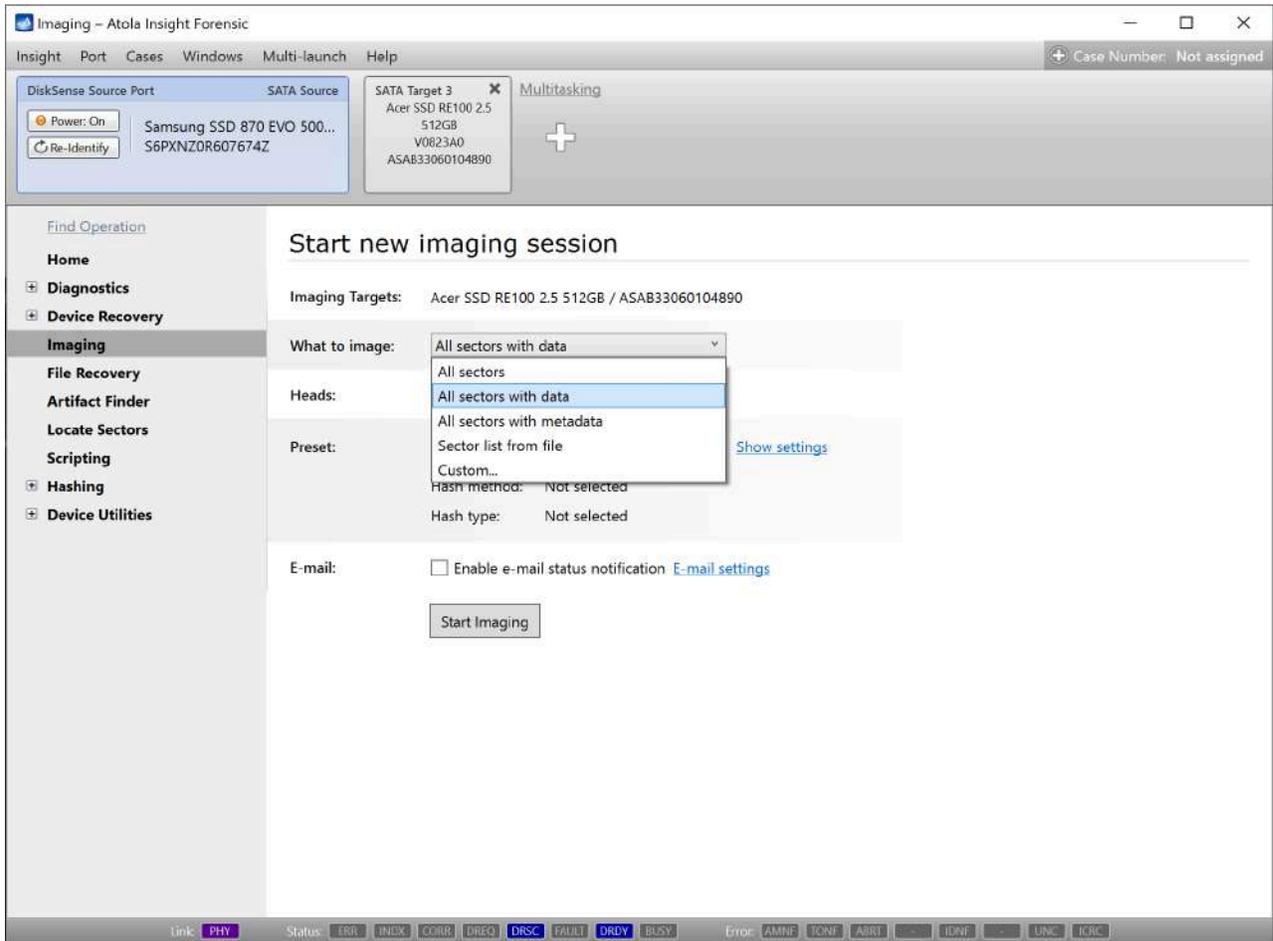


**The All sectors option selected in the What to image list.**

# All sectors with data

To image the whole system structure of the drive including folders and files, while omitting the areas with no data or fragments of previously deleted files, do the following:

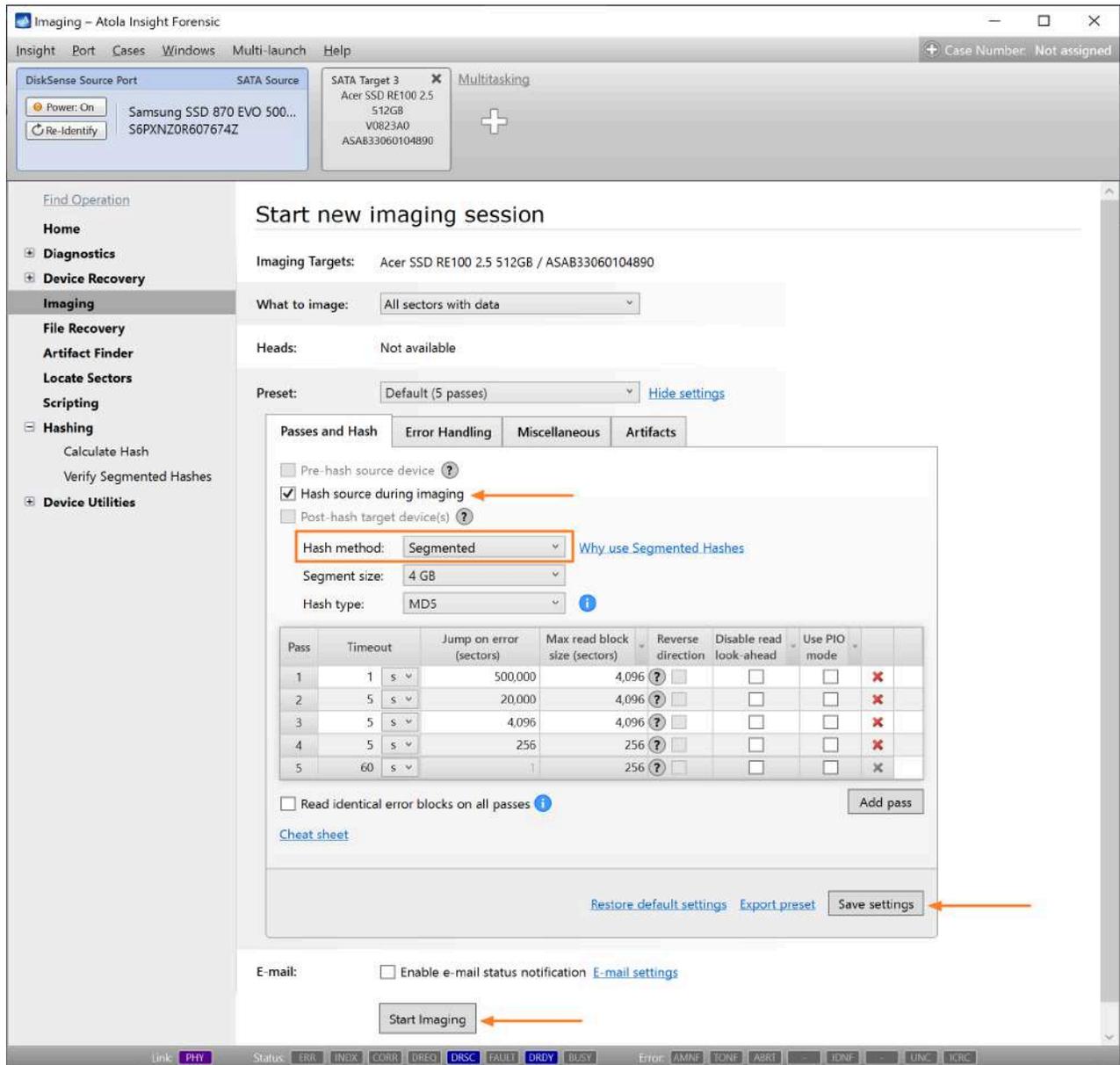
1. Go to Imaging > Create New Session.
2. In the **What to image** list, select **All sectors with data**.



### The All sectors with data option selected in the What to image list.

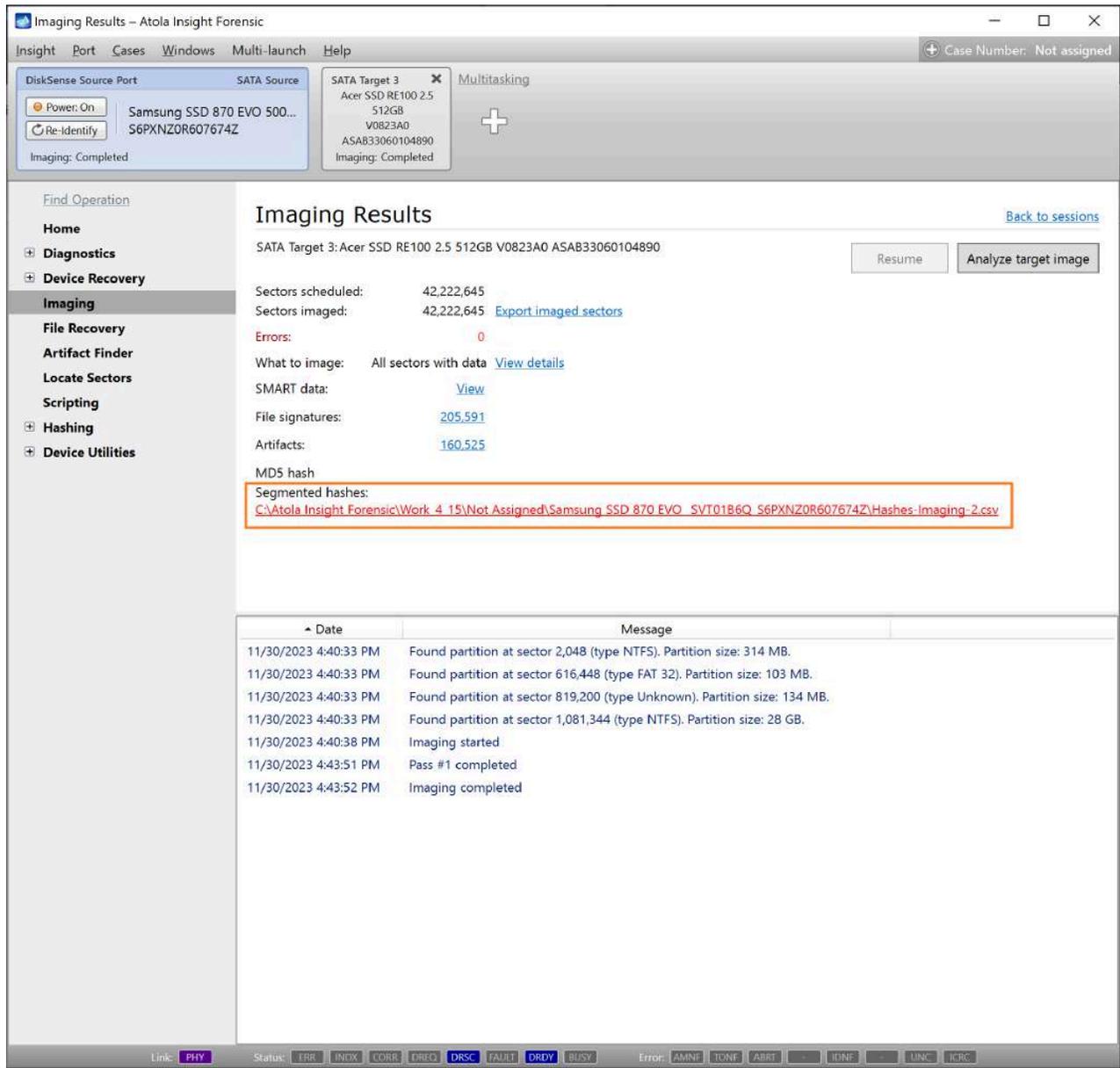
3. Recommended: Enable [segmented hashing](#) for an imaging session:
  - a. In the **Preset** section, click the **Show settings** link.
  - b. On the **Passes and Hash** tab, enable **Hash source during imaging**.
  - c. Set the **Hash method** to **Segmented**.

Otherwise, if you use the linear hashing method, the hash values of the source and the target drives, as a result of imaging only sectors with data, will not be identical.



### Enabling segmented hashing in the imaging settings.

- Adjust other imaging settings as needed and click **Start imaging**.
- When you choose to image all sectors with data, the imaging log adds a message about the partitions Insight has been able to find. A link to the file with segmented hashes is included in the **Imaging Results** report.



The Imaging Results report with messages about partitions found during imaging all sectors with data.

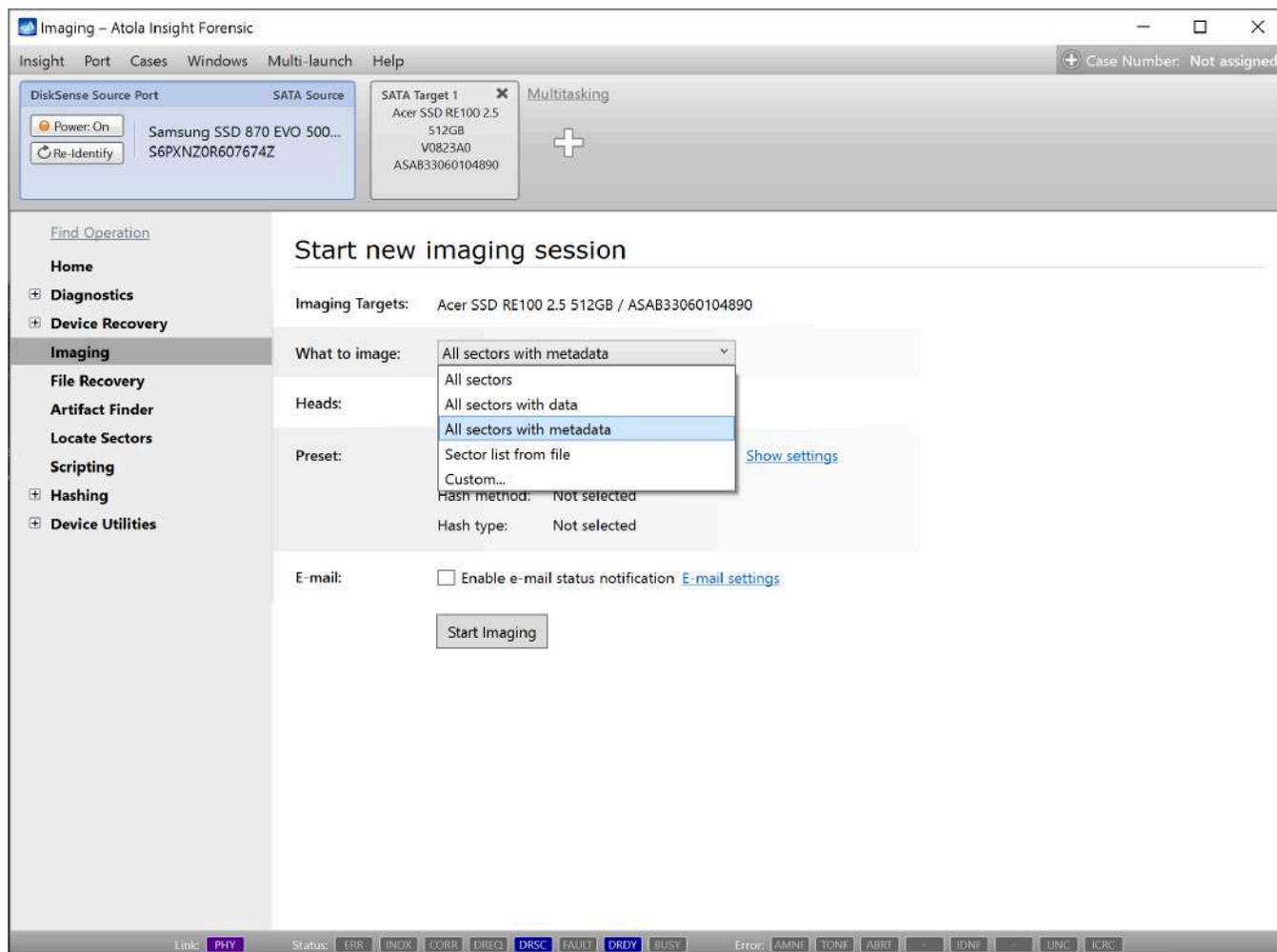
## All sectors with metadata

To image only the system structure of a drive without data within its files (for example, MFT in NTFS), do the following:

1. Go to Imaging > Create New Session.
2. In the What to image list, select All sectors with metadata.
3. Adjust other imaging settings as needed and click Start imaging.

Imaged metadata can be used later to browse through files and select the ones to be imaged in full. For more details, watch this video guide: [Benefits of imaging metadata.](#)

When choosing to image all sectors with metadata, the imaging log adds a message about the partitions that Insight has been able to find.

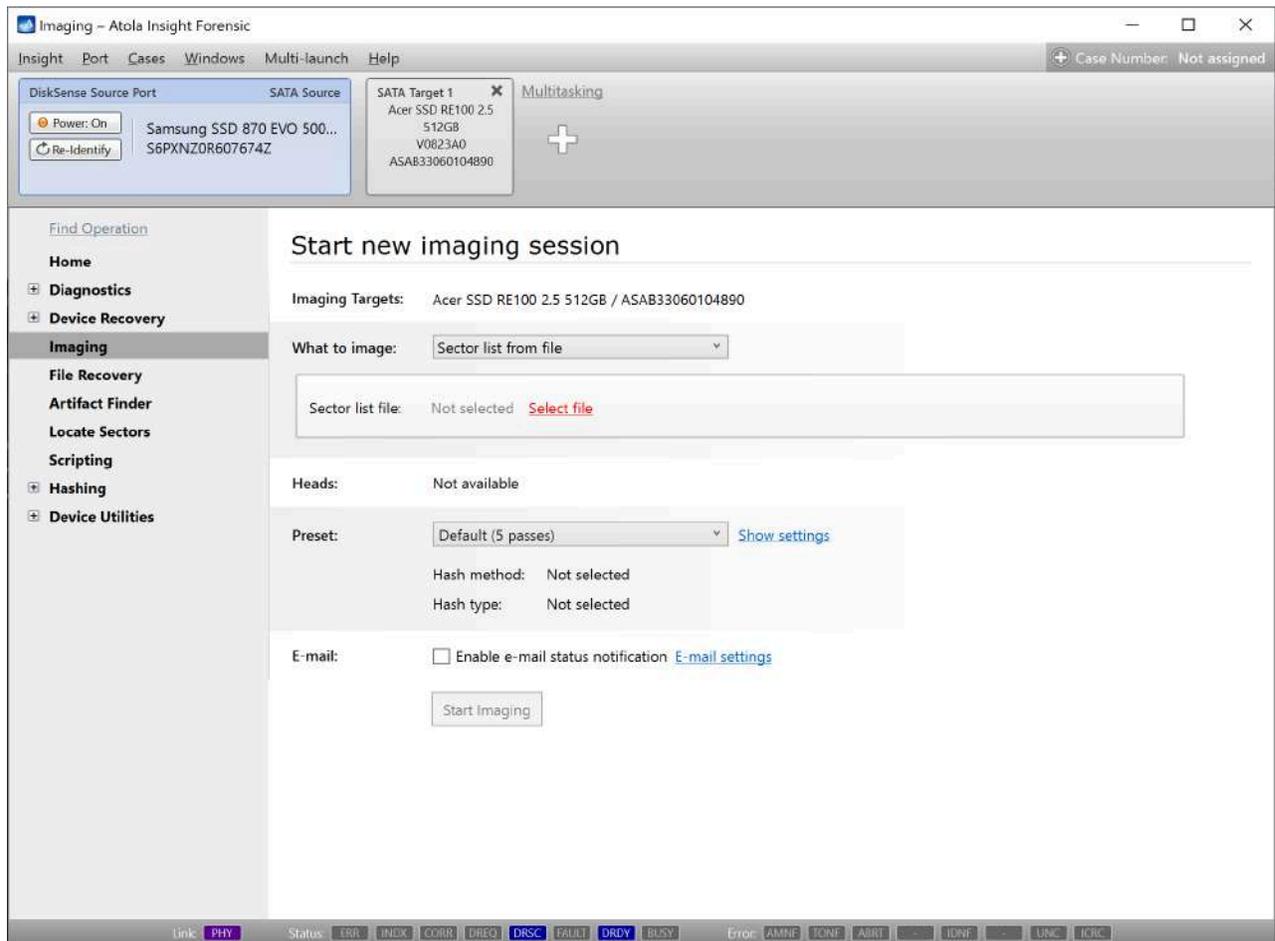


**The All sectors with metadata option selected in the What to image list.**

## Sector list from file

If you have a text or a CSV file with a list of sectors you want to image, you can select the relevant option in the imaging settings, and Insight Forensic will image only the sectors specified in the file you provided:

1. Go to **Imaging > Create New Session**.
2. In the **What to image** list, select **Sector list from file**.
3. Click the **Select file** link and choose a file with a list of sectors.
4. Adjust other imaging settings as needed and click **Start imaging**.

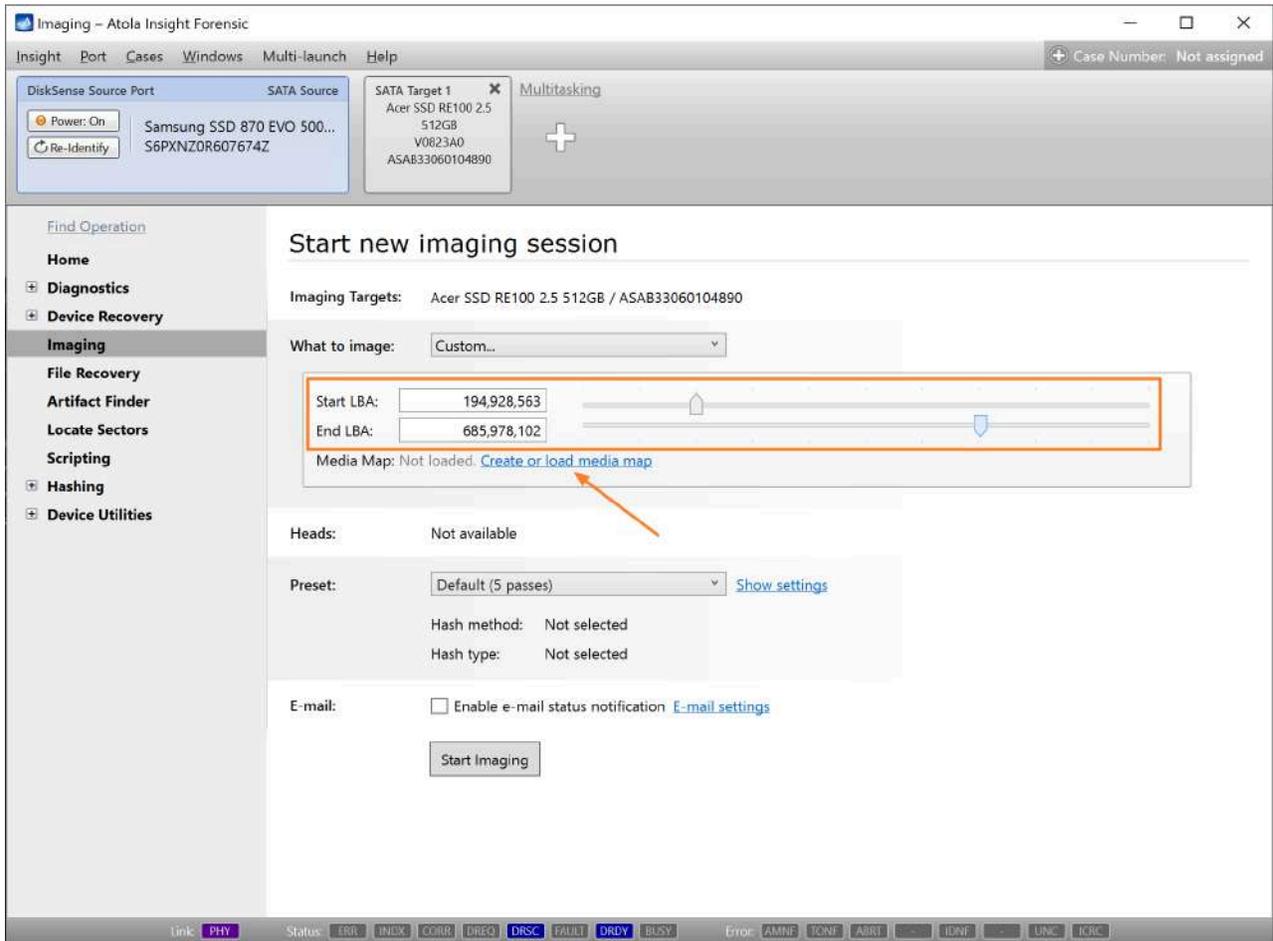


**Selecting a file with a sector list to image in the imaging settings.**

## Custom sector selection

In Insight Forensic, you can fine-tune sector ranges you want to image, specifying start and end LBA, including or excluding certain partitions or sector ranges, or customizing imaging ranges for each partition. Here's how to do it:

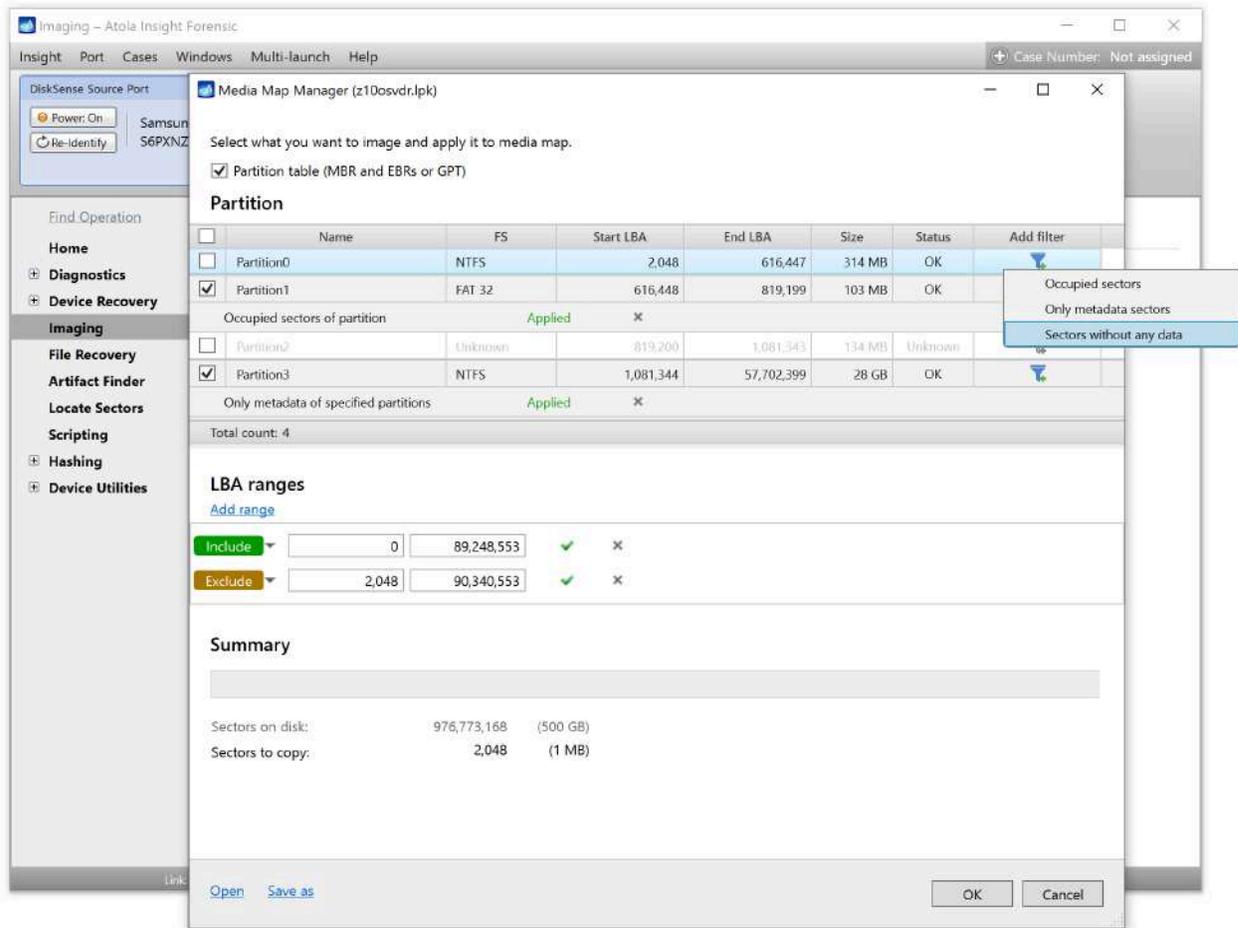
1. Go to **Imaging > Create New Session**.
2. In the **What to image** list, select **Custom**.
3. **Optional:** To adjust Start and End LBA, enter values in the respective fields or use sliders.
4. Click the **Create or load media map** link.



### The Create or load media map link on the imaging settings screen.

5. The **Media Map Manager** window opens. Here are various options to customize the sector ranges for imaging:

- In the **Partition** section, you can select partitions to be imaged. Also, you can add a filter for each partition to specify which sectors to image:
  - occupied sectors,
  - only metadata sectors, or
  - sectors without any data.
- In the **LBA ranges** section, you can add custom sector ranges you want to image, as well as exclude certain sector ranges from imaging. Click the **Add range** link, choose the **Include or Exclude** option from a list and enter the start and end LBA for a range.
- As you adjust sector range settings, the **Summary** section immediately updates information about the number of sectors scheduled for copying and their total size.



### Adjusting sector ranges for imaging in the Media Map Manager window.

6. After adjusting sector ranges, click **OK**.
7. Back on the **Start new imaging session** screen, adjust other imaging settings as needed and click **Start imaging**.

## Analyze data from the imaged sector ranges

Once imaging of the selected sector ranges is complete, you can view the structure of the resulting image you have obtained:

1. On the Imaging results screen, click **Analyze target image**.

Imaging Results – Atola Insight Forensic

Insight Port Cases Windows Multi-launch Help Case Number: Not assigned

DiskSense Source Port SATA Source

Power: On Re-Identify Samsung SSD 870 EVO 500... S6PXNZ0R607674Z Imaging: Completed

SATA Target 1 x Multitasking

Acer SSD RE100 2.5 512GB V0823A0 ASAB33060104890 Imaging: Completed

Find Operation

Home

Diagnostics

Device Recovery

Imaging

File Recovery

Artifact Finder

Locate Sectors

Scripting

Hashing

Device Utilities

## Imaging Results

[Back to sessions](#)

SATA Target 1: Acer SSD RE100 2.5 512GB V0823A0 ASAB33060104890

Resume Analyze target image

Sectors scheduled: 42,222,645

Sectors imaged: 42,222,645 [Export imaged sectors](#)

Errors: 0

What to image: All sectors with data [View details](#)

SMART data: [View](#)

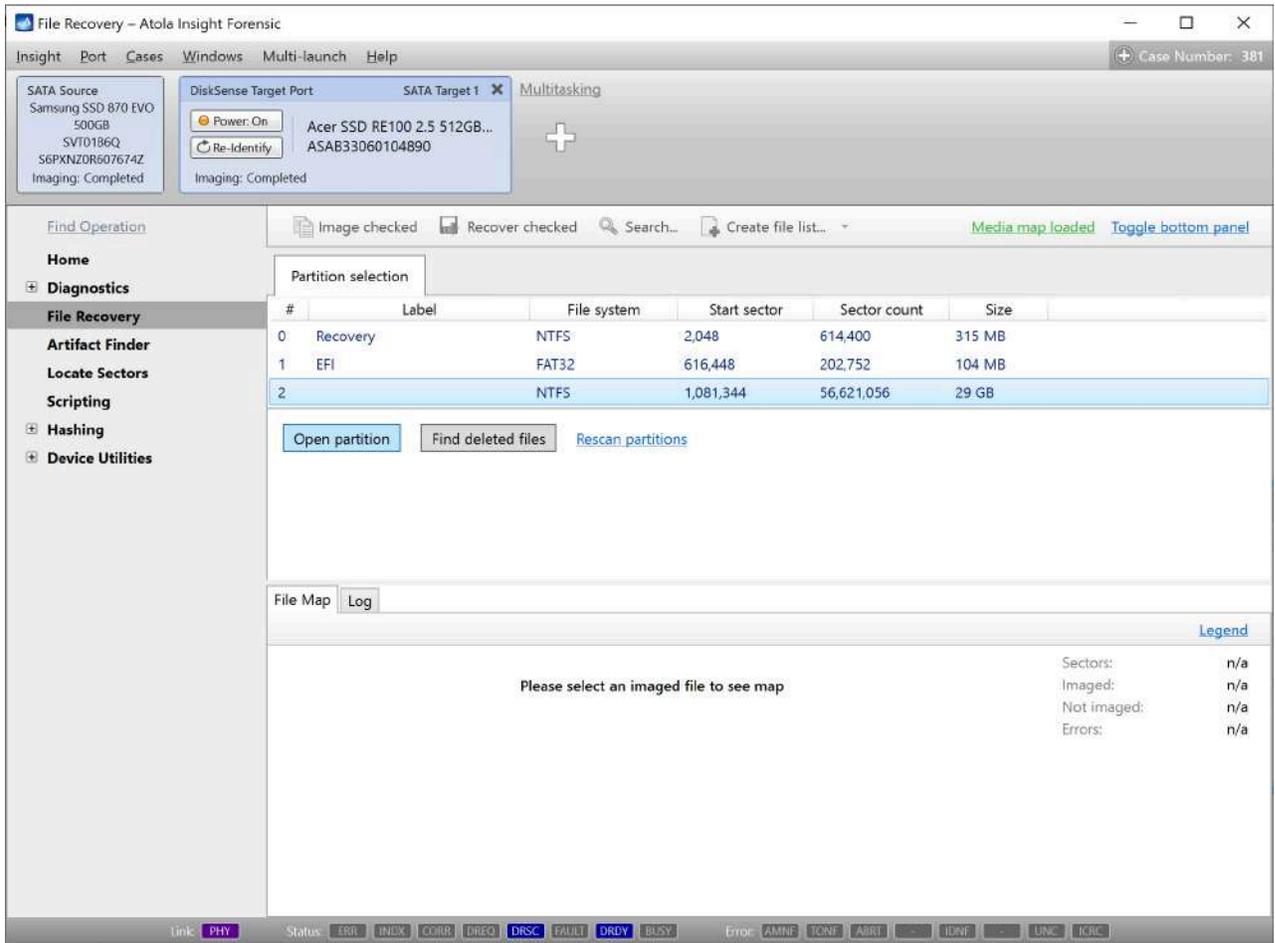
File signatures: 205,591

Artifacts: 160,525

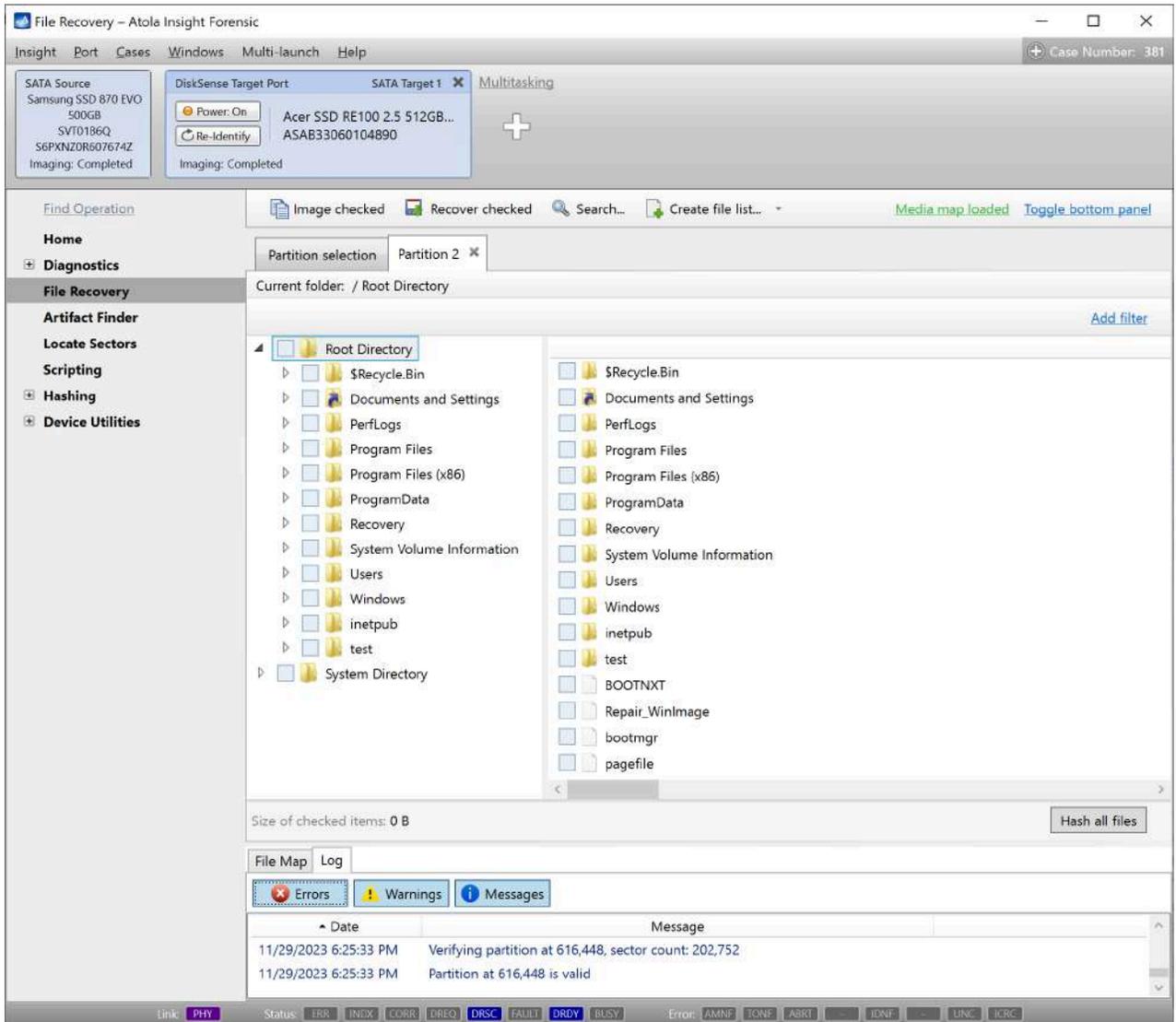
Date	Message
11/29/2023 6:20:30 PM	Found partition at sector 2,048 (type NTFS). Partition size: 314 MB.
11/29/2023 6:20:30 PM	Found partition at sector 616,448 (type FAT 32). Partition size: 103 MB.
11/29/2023 6:20:30 PM	Found partition at sector 819,200 (type Unknown). Partition size: 134 MB.
11/29/2023 6:20:30 PM	Found partition at sector 1,081,344 (type NTFS). Partition size: 28 GB.
11/29/2023 6:20:36 PM	Imaging started
11/29/2023 6:23:50 PM	Pass #1 completed
11/29/2023 6:23:51 PM	Imaging completed

Link: PHY Status: ERR, INDX, CORR, DREQ, DRSC, FAULT, DRDY, BUSY Error: AMNF, TONF, ABBT, LUNF, LUNC, ICRC

2. The Target port opens. Click the **Scan partitions** button.
3. Select any of the imaged partitions you want to preview and click the **Open partition** button.



4. Browse through the imaged folders and files.



## Image a remote drive using the iSCSI protocol

The iSCSI network protocol lets you access devices remotely. With its help, you can also image drives that can't be plugged into the DiskSense 2 hardware unit. These could be drives soldered into a motherboard, servers that can't be turned off, or devices you have legal access to but not the right to seize.

Up to 3 remote network drives can be imaged in parallel via iSCSI.

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, first, you need to set up an iSCSI target correctly. To help you with that, Atola engineers created a Python script named `iscsi-targets`, that automatically creates iSCSI targets for all drives except for a boot device.

[Download iscsi-targets from GitHub →](#)

## Features of the 'iscsi-targets' script

- Automatically creates iSCSI targets for all drives except for a 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 pulls the drive model and serial number from IQN into a case.
- Lets you specify a block device as a script argument to create an iSCSI target only for it.

## What you need to run the 'iscsi-targets' script

The script runs on **Linux only**. It was tested on various flavors of Linux like Ubuntu, Fedora, CentOS, and RHEL, including DFIR boot images: Paladin, Caine, and Tsurugi.

1. **Python 3.6+** must be installed.
2. The script will also check for and install two dependencies the first time it is run:
  - `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 for a 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.

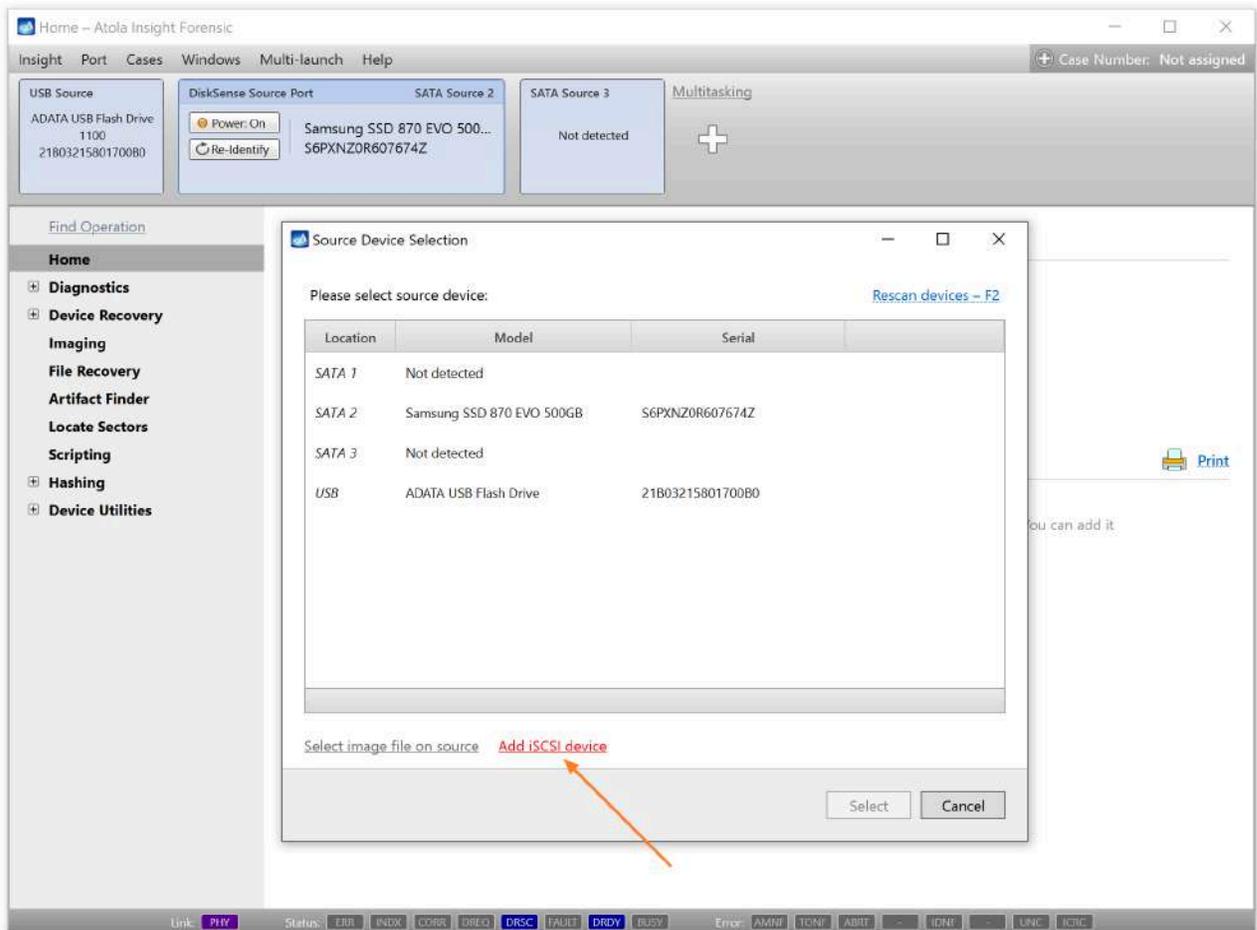
```
paladin@PALADIN:~/Downloads$ sudo python3 iscsi-targets.py
targetcli is not installed. Do you want to install it? (Y/N): y
Boot device: /dev/sdc
The following block devices will be unmounted and used for iSCSI target creation:
/dev/sda      256G-NVMe-T      0123456789AC
/dev/sdb      HyperX-Fury-3D-240G      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.

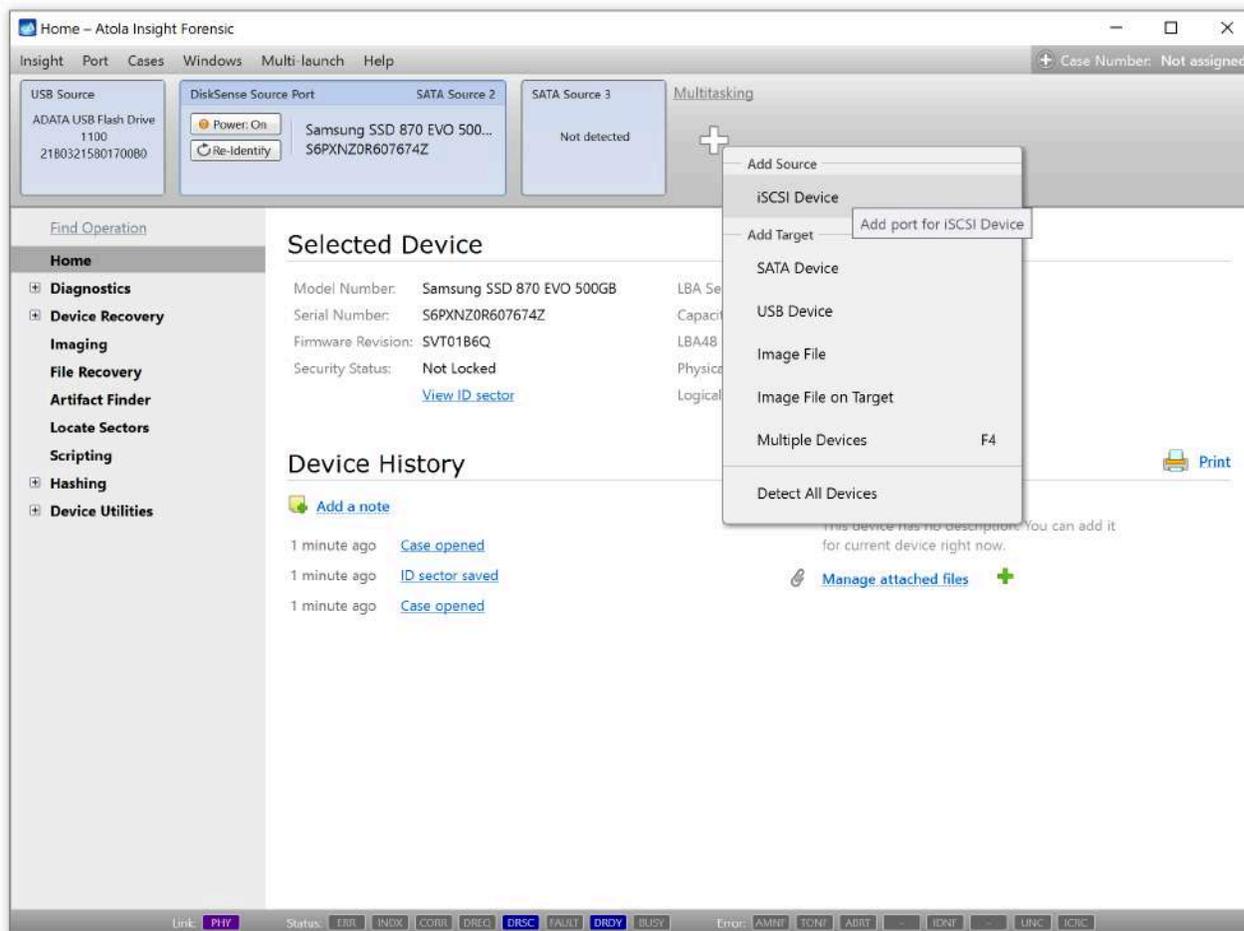
## Image up to 3 remote drives in parallel using iSCSI

Here's how to image a remote drive in Insight Forensic using the iSCSI protocol:

1. Expose a physical or logical drive via iSCSI on a network.
2. Go to **Port > Select Source** and then click the **Add iSCSI device** link.



Alternatively, click the **Plus** icon at the top and in the **Add Source** menu select **iSCSI Device**.



3. Enter the IP address and Port of a remote storage device. If needed, also enter a user name and password for remote authentication.

Open iSCSI target

Connection Favorites

IP: 10.0.0.197 Port: 3260

Discovery authentication (optional)

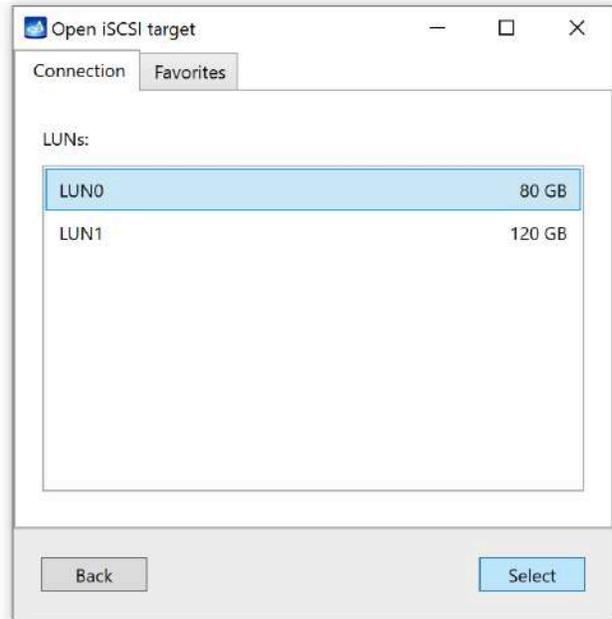
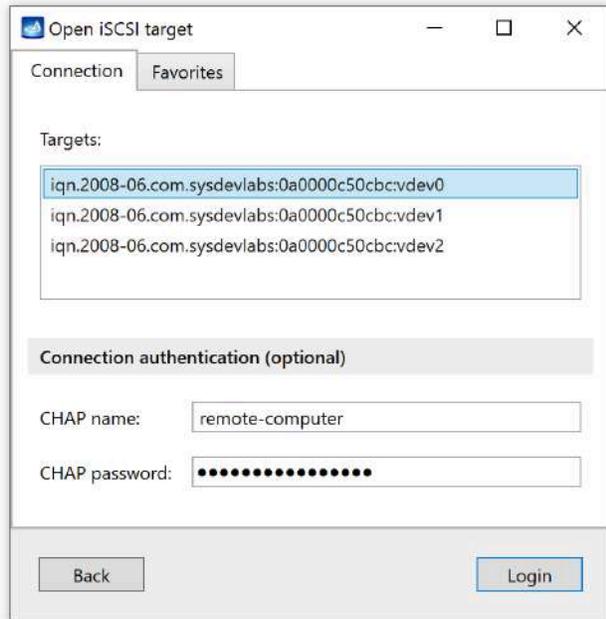
CHAP name: remote-computer

CHAP password: ●●●●●●●●●●●●●●●●

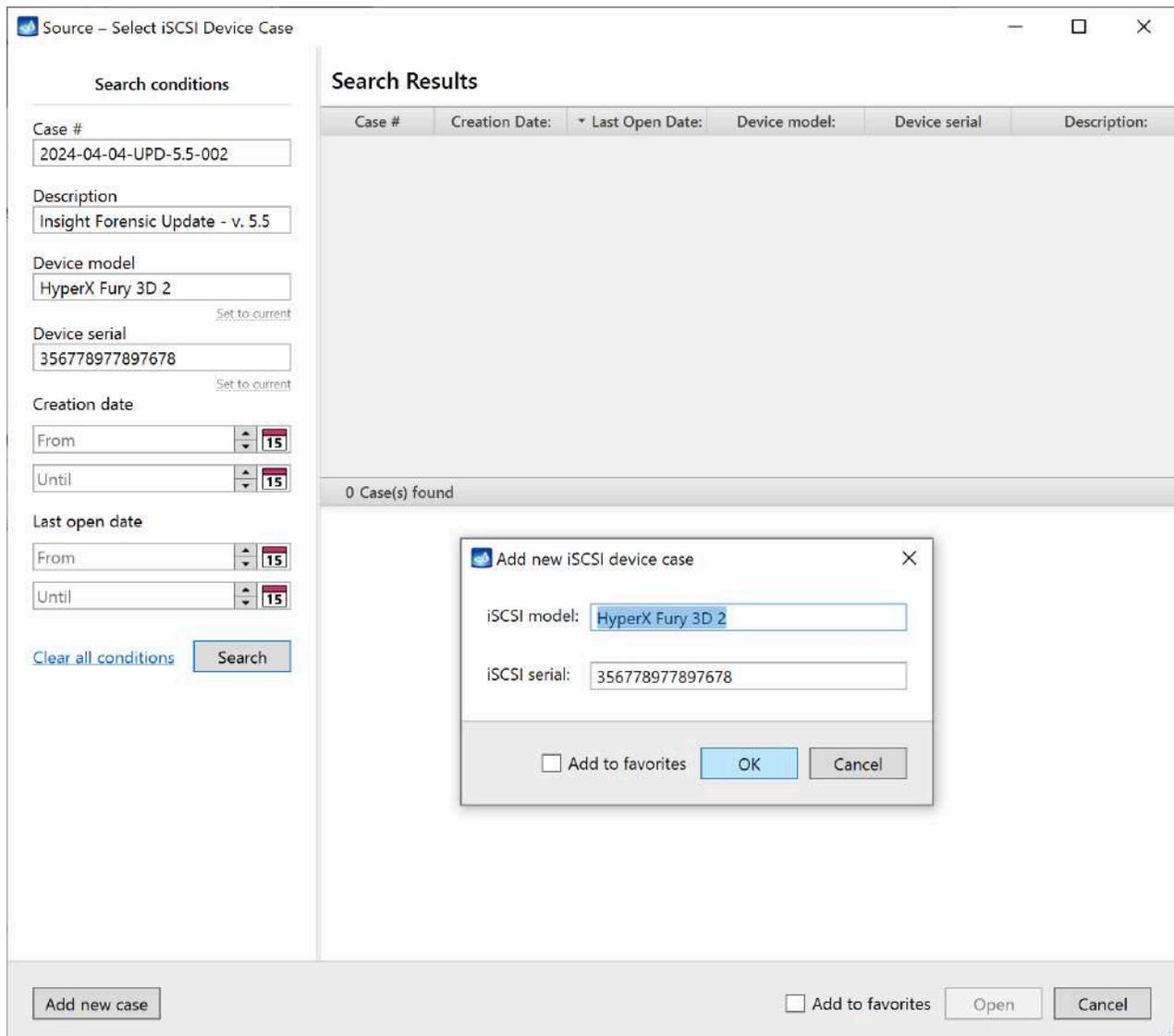
Discover

4. Click **Discover**.

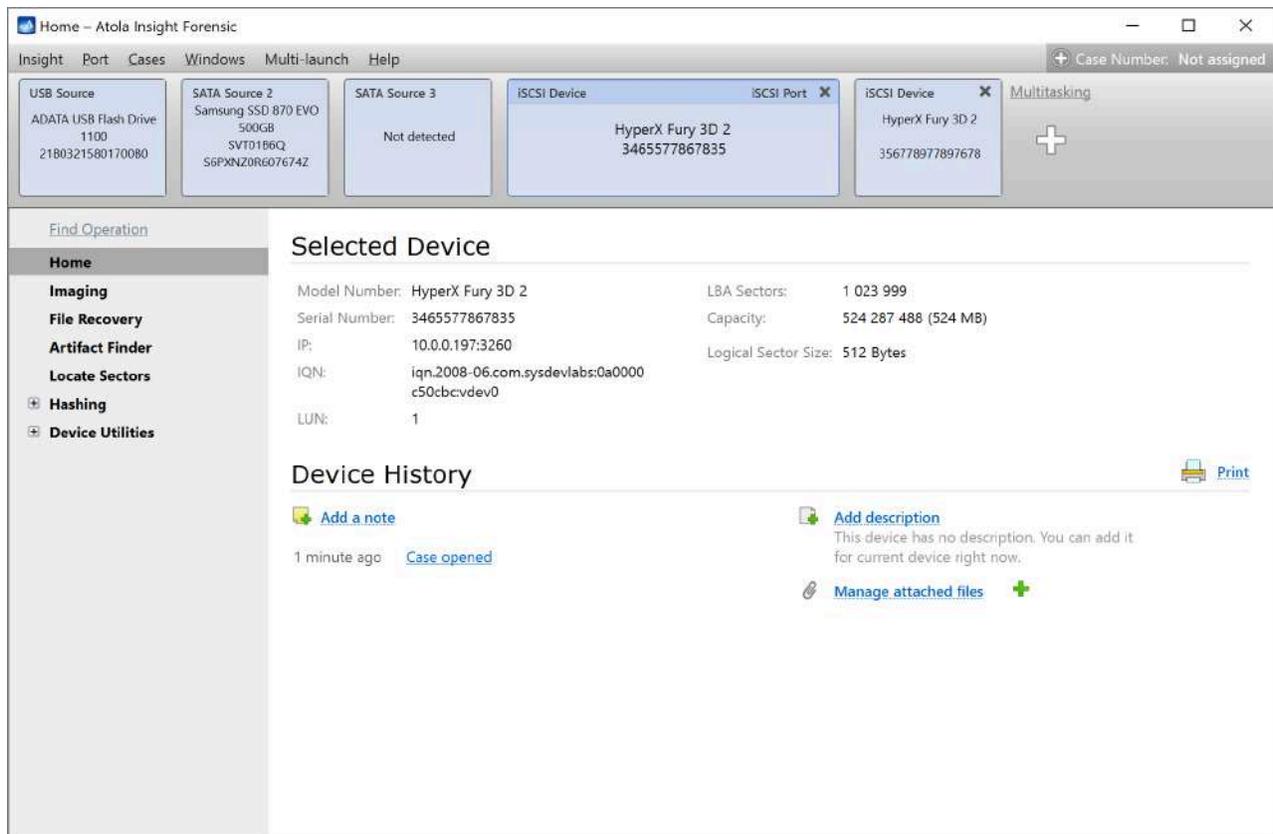
5. Insight Forensic searches and shows all the iSCSI devices available at the IP and port address you provided. Select your device.



6. Create a new case for an iSCSI device or select an existing one.



7. Insight Forensic opens the selected iSCSI device as a separate port.



Now, you can image this device as usual or launch other operations, such as:

- [File recovery](#)
- [Artifact finder](#)
- [Locate sectors](#)
- [Calculate hash](#)
- [Disk editor](#) (in read-only mode)

## Parallel imaging of three SATA drives

With DiskSense 2, Atola Insight Forensic is able to sustain 3 parallel imaging sessions.

The upgraded hardware unit is equipped with 3 SATA source ports. They can be imaged up to 3 targets each: to the 4 target ports (3 SATA and 1 USB) or to a file on the local server or host computer using the two built-in 10Gb Ethernet ports.

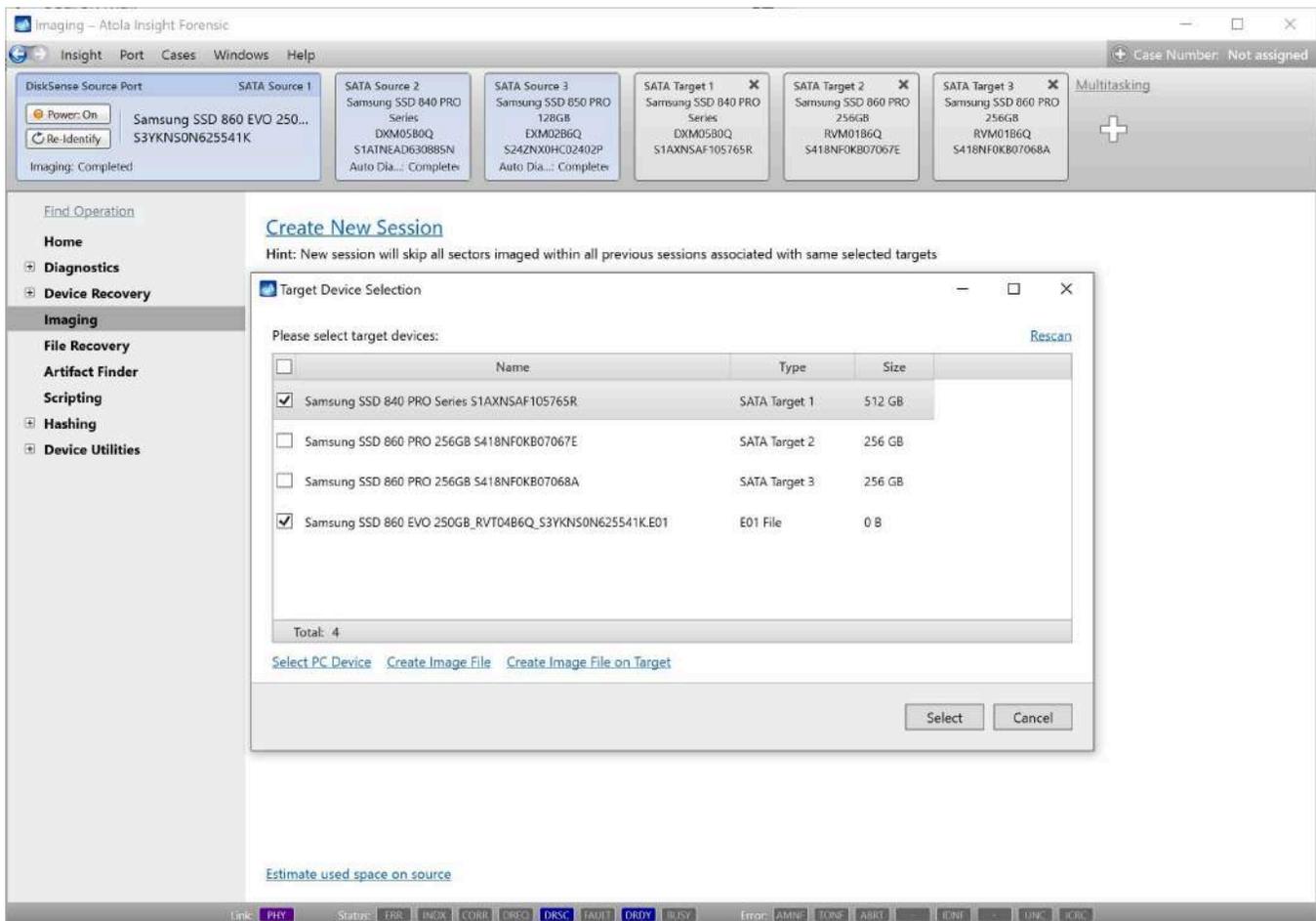
To be able to sustain such throughput of data, DiskSense has been enhanced with server-grade motherboard and CPU. And the addition of [ECC RAM](#) makes data transfer more reliable than ever.

To launch multiple imaging sessions in the interface:

1. Select the source port in the port selection panel.

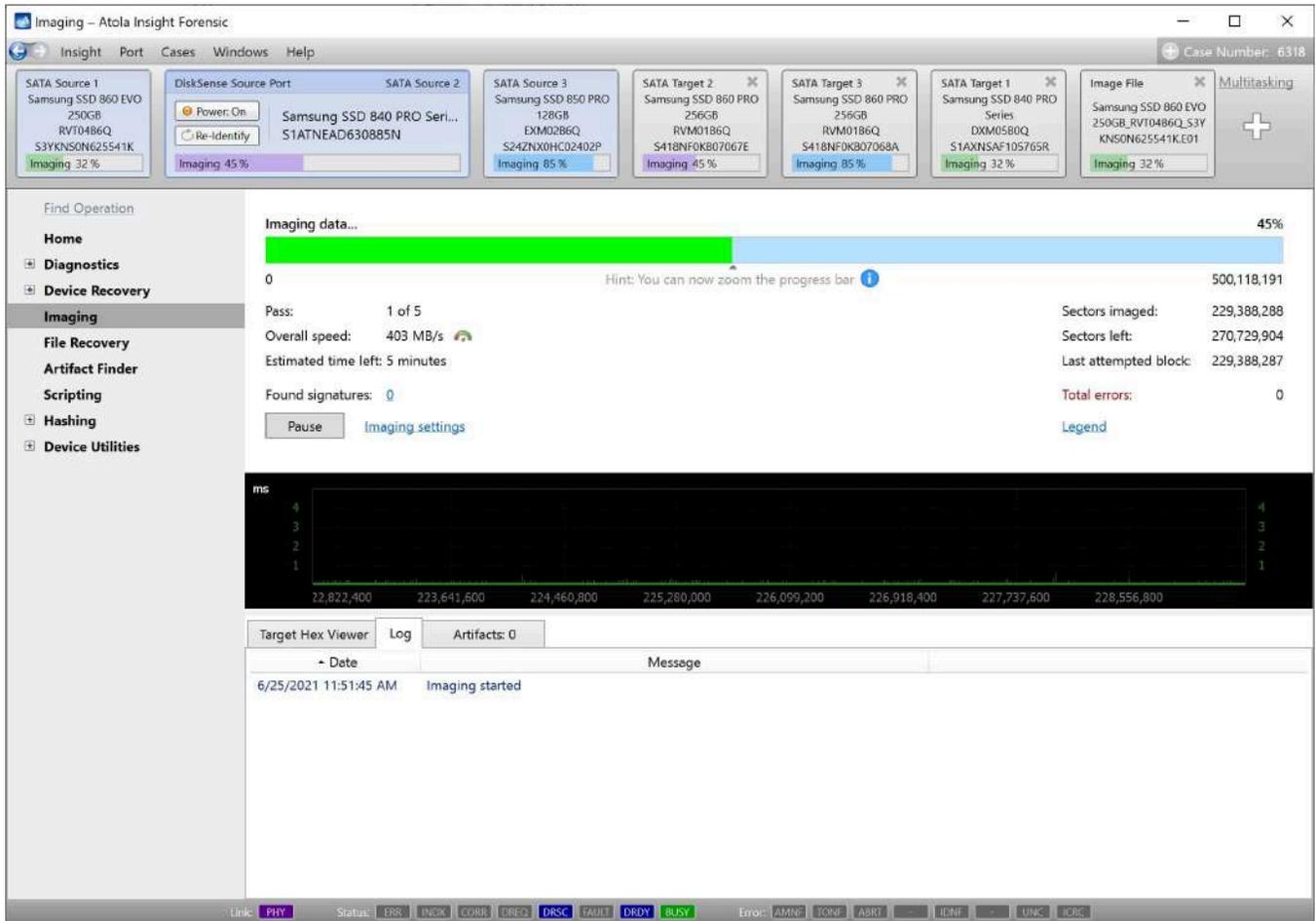


2. Click **Imaging** and then **Create New Session**.
3. Select the target or a few.
4. Click **Start imaging**.



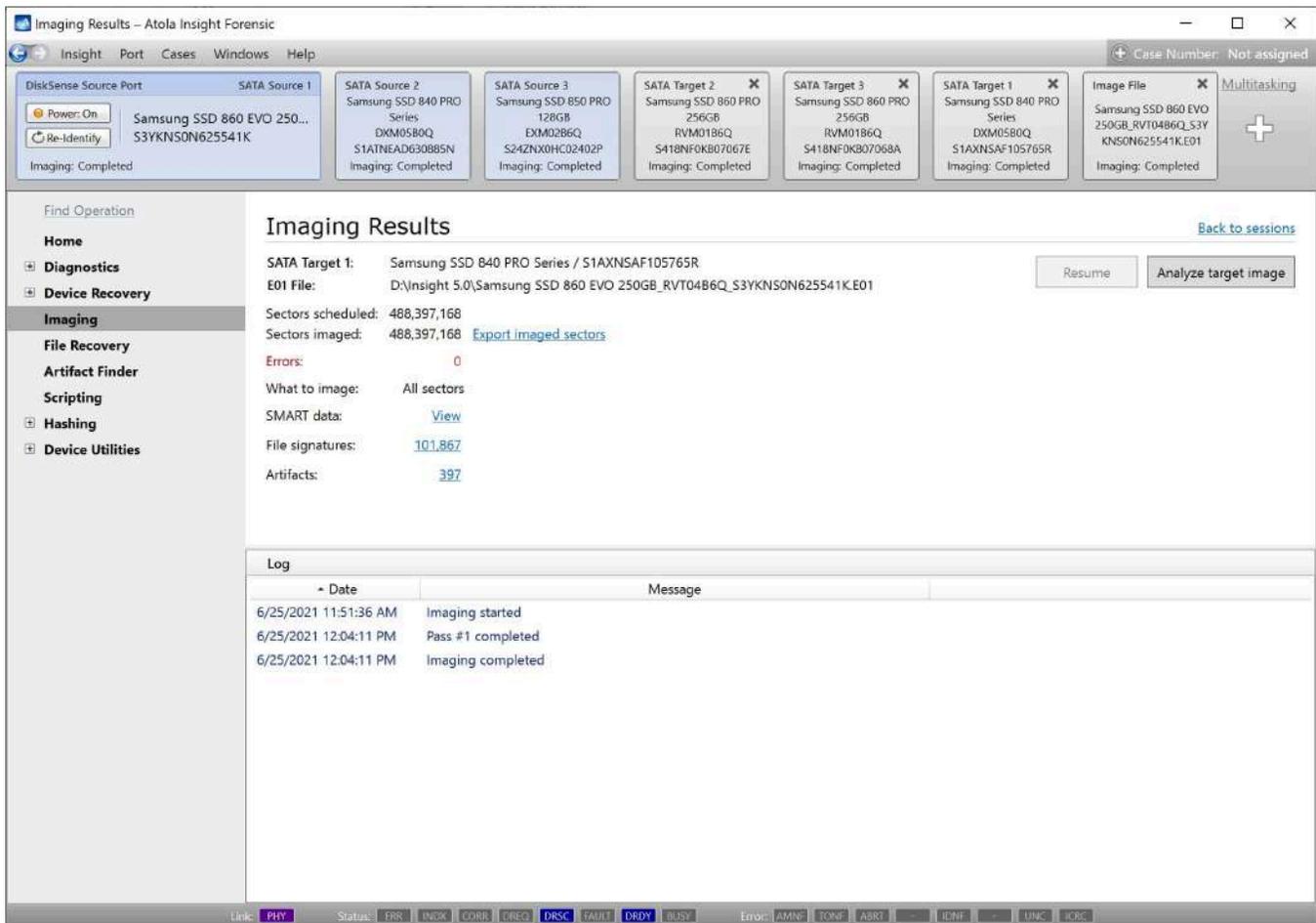
Move on to the next source by selecting another Source port in the port selection panel and repeat the steps to launch thesecond and the third sessions.

The server-grade hardware within DiskSense 2 allows sustaining each imaging session at the rate of 500 MB/s (if the type and condition of the drives allow) as well as your network configuration (if some of the targets are located there).



Once all the sessions are running, you can track the imaging progress by switching between the Source ports.

Upon completion of the imaging sessions, you can look up the **Imaging results** pages. The reports for all sessions are automatically saved in the [Case management system](#).



## Multipass imaging of damaged hard drives

Physically damaged drives require a complex imaging approach to retrieve as much data as possible while approaching the bad areas in the most gentle way possible.

Atola Insight Forensic has a complex imaging functionality, which allows imaging of even physically damaged drives, avoiding their further deterioration.

## Diagnose first

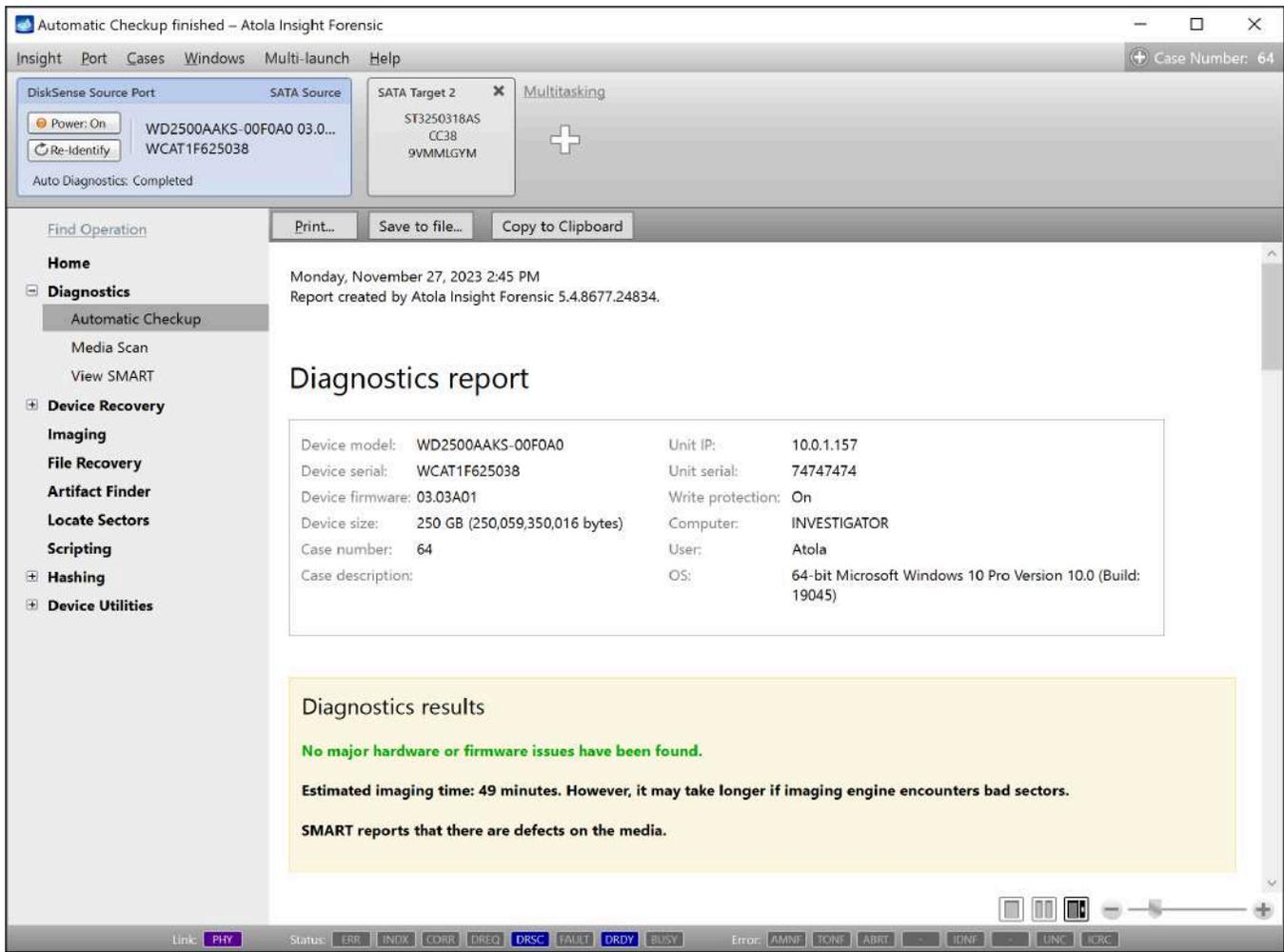
Whenever you start working on a drive, the very first thing we recommend to do is to find out if the drive is damaged in any way, and if so, what is the extent of the damage.

Insight Forensic comes with a fully automated [diagnostics module](#). It diagnoses all drive components and data on it:

- printed circuit board (PCB),
- spindle motor,
- head stack,
- firmware,
- and file systems.

Diagnostics works properly even if the drive has burnt parts or damaged head stack—the routine makes use of the current monitor that is embedded into the DiskSense unit.

After diagnostics, Insight Forensic generates a detailed report, which lists the exact issue with the drive and suggests the best approach for data acquisition.



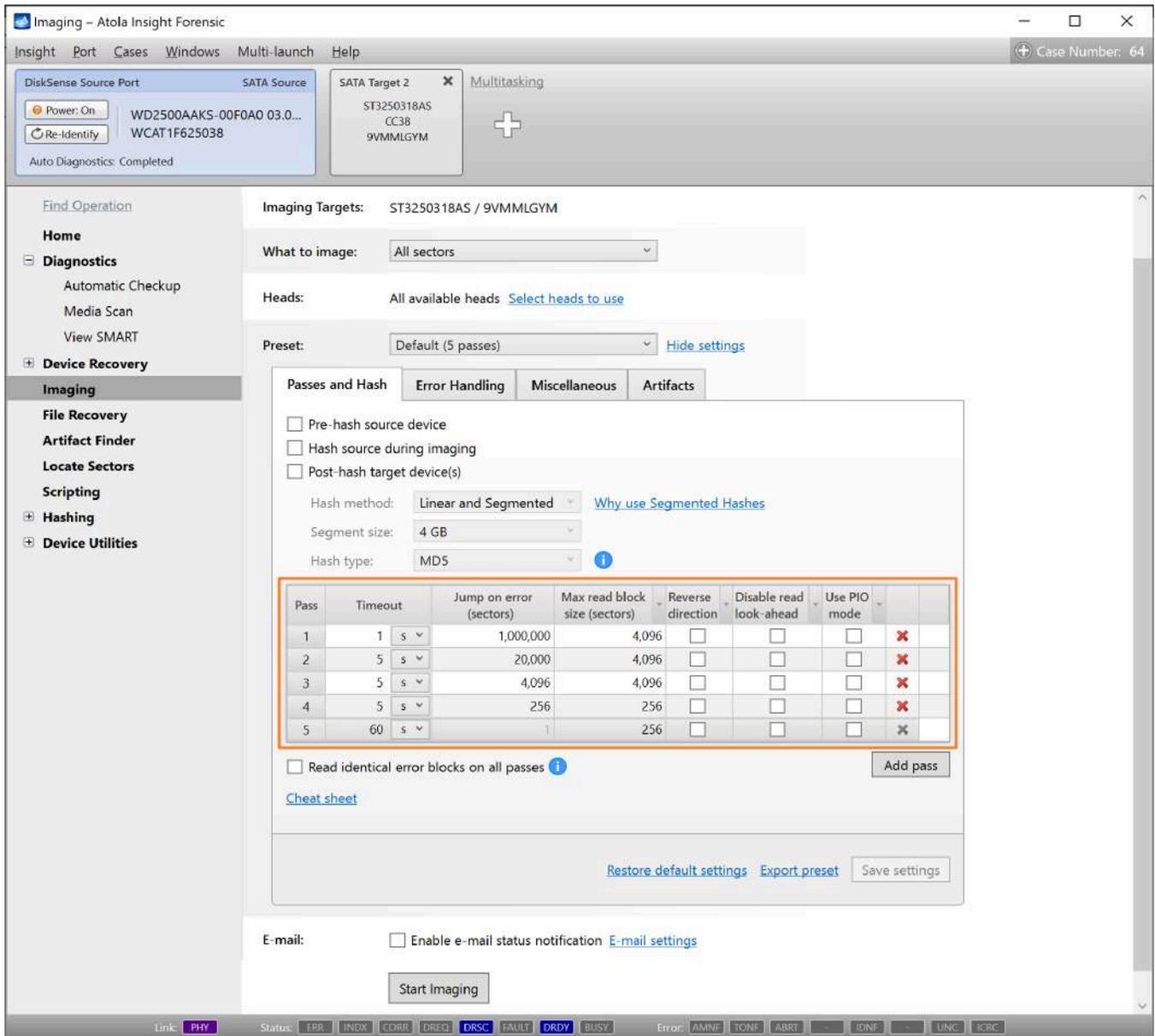
A diagnostics report of a damaged drive.

## Default settings for imaging damaged drives

Most imagers have a linear imaging process. Whenever such an imager encounters a bad sector on a drive, the process slows down drastically. This often causes the drive to freeze.

Insight Forensic operates using a special multipass imaging algorithm that applies a non-linear approach and allows speeding up the imaging of damaged drives while maximizing the amount of successfully retrieved data.

The default settings of the passes are based on our decades-long experience in the data recovery market to fit the majority of problematic drives. Therefore, it is advisable to follow them, unless a particular drive requires specific settings.



## Default imaging settings for damaged drives with 5 passes.

Let's clarify the terms used on the imaging settings screen:

- **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 the maximum time for a single read block attempt during this pass.
- **Jump on errors (sectors)** is the number of consecutive sectors that Insight Forensic will skip if it can't read a block from a source device.
- **Max read block size (sectors)** is the maximum number of sectors that Insight Forensic reads from a source device at a time.
- **Reverse direction:** when enabled for a particular pass, 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. However, the speed decreases due to the automatic disabling of the drive's cache.

- **Disable read look-ahead** turns off a read look-ahead functionality, which makes the drive read more blocks sequentially than requested by the software. In good drives, this functionality helps the drive operate faster by reading more data and caching it. 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.
- **Use PIO mode** enables reading sectors using PIO commands (READ SECTORS EXT, READ SECTORS) instead of DMA commands. This can help in extremely rare cases of damaged drives.

## Multipass algorithm for imaging damaged drives

To ensure thorough data extraction and avoid causing further damage to media, Insight Forensic applies the multipass imaging algorithm with deliberate timeout and block size control. Here's how the algorithm works.

### Timeouts and block size control

Using a small block size pays off when you need to retrieve the maximum data from an unstable drive. This approach also significantly slows down the imaging process. It may also increase the possibility of causing further damage to the media.

That's why Insight's multipass imaging engine uses **large blocks with short timeouts** on the first few passes. It schedules reads inside slow areas for later and then uses the **smallest block size on the last pass** when very few sectors are left to be read.

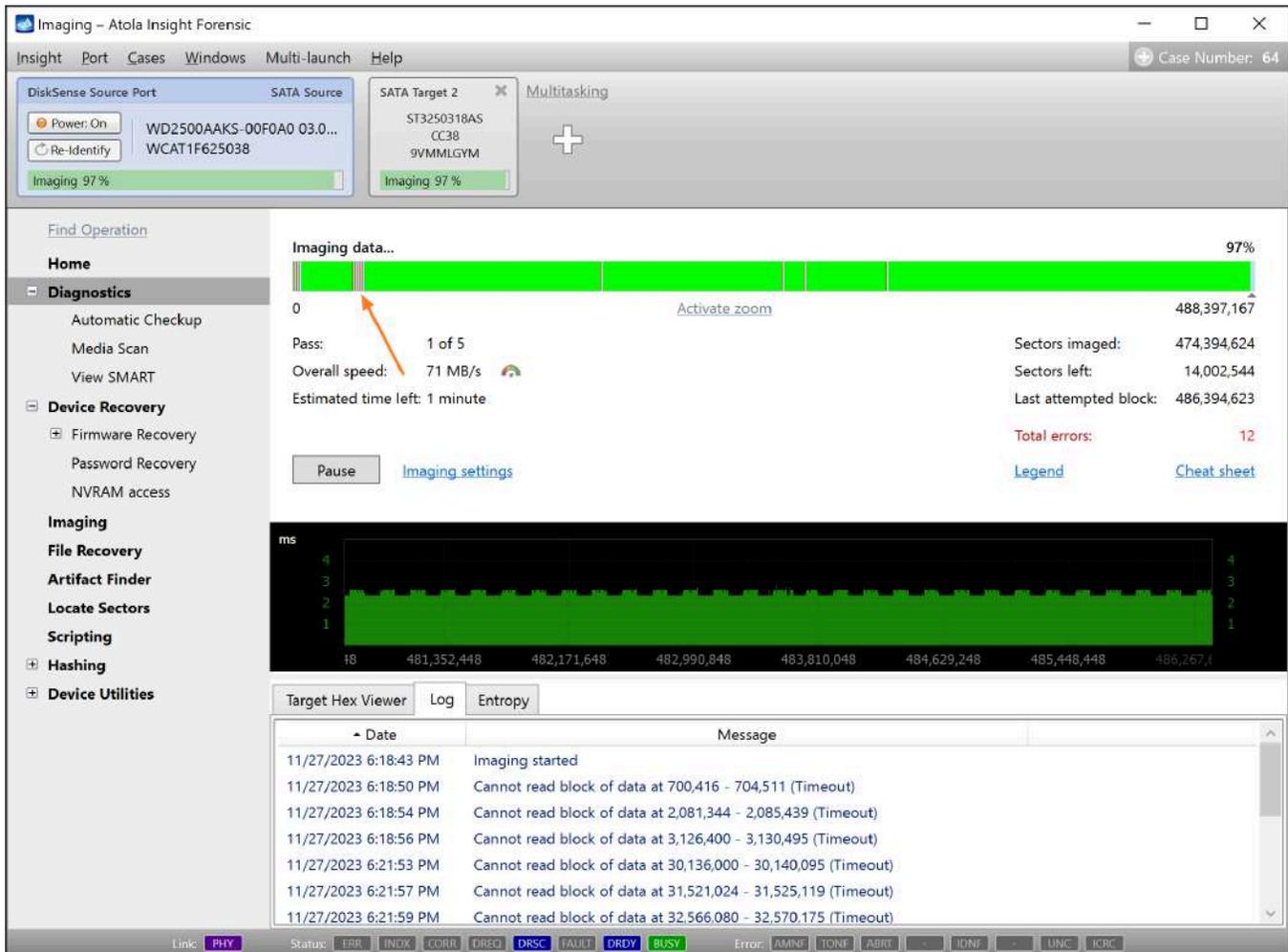
Insight Forensic handles block sizes automatically to provide the best possible results in the shortest amount of time.

### First pass

On the first pass, Insight has a 1-second **Timeout** per block, and the **Max read block size** is set to 4096 sectors. The default settings of the first pass allow smooth sequential imaging of all modern drives in good condition.

But when you need to image a drive with bad sectors, these settings make Insight skip any areas that slow down the reading: it performs **Jump on error** by 1,000,000 sectors at a time.

These settings ensure imaging data from the healthy areas of the drive at top speed while making Insight return to the problematic areas during the following passes. Atola Insight Forensic splits such areas into smaller pieces and allows more time for reading the data within them.



**Insight performs Jump on error by 1,000,000 sectors on the first pass.**

## 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. Insight allows slightly longer, 5-second **Timeouts** for attempted reading of the blocks. As the jumps become smaller, empty areas start filling up with data.

The screenshot displays the Atola Insight Forensic software interface during the second imaging pass. The top menu bar includes 'Insight', 'Port', 'Cases', 'Windows', 'Multi-launch', and 'Help'. The source and target configuration shows 'DiskSense Source Port' (SATA Source) and 'SATA Target 2' (ST3250318AS CC38 9VMMMLGYM), both at 99% imaging progress. The central area shows 'Imaging data...' at 99% completion, with a progress bar and a summary of statistics: 488,397,167 sectors imaged, 3,528,512 sectors left, and an overall speed of 71 MB/s. A performance graph below shows the read speed in ms over time. The log window at the bottom lists several error messages, including 'Pass #1 completed', 'Error block 700,416 - 704,511 was skipped', and 'Cannot read block of data at 30,541,024 - 30,545,119 (Error: UNC)'. The status bar at the bottom indicates the device is 'BUSY' and shows various error codes like 'ERR', 'INDX', 'CORR', 'DREQ', 'DRSC', 'FAULT', 'DRDY', 'BUSY', 'AMNF', 'TONF', 'ABRT', 'IDNF', 'UNC', and 'ICRC'.

The second imaging pass.

## Fourth pass

On the fourth pass, to try reading problematic zones in a more granular way, both Jump on error and Max read block size are yet again reduced, this time to 256 sectors.

The screenshot shows the Atola Insight Forensic interface during the fourth imaging pass. The progress bar at the top indicates 99% completion. The 'Imaging data...' section shows 488,397,167 sectors imaged, with 57,344 sectors left. The overall speed is 70 MB/s, and the estimated time left is 0 seconds. The log window shows the following messages:

Date	Message
11/27/2023 7:17:11 PM	Pass #3 completed
11/27/2023 7:17:13 PM	Cannot read block of data at 700,416 - 700,671 (Error: UNC)
11/27/2023 7:17:16 PM	Cannot read block of data at 2,081,344 - 2,081,599 (Error: UNC)
11/27/2023 7:17:18 PM	Cannot read block of data at 2,933,088 - 2,933,343 (Error: UNC)
11/27/2023 7:17:20 PM	Cannot read block of data at 3,126,400 - 3,126,655 (Error: UNC)
11/27/2023 7:17:22 PM	Cannot read block of data at 30,138,560 - 30,138,815 (Error: UNC)
11/27/2023 7:17:25 PM	Cannot read block of data at 30,542,048 - 30,542,303 (Error: UNC)

The status bar at the bottom shows the link as PHY, status as ERR, INDX, CORR, DREQ, DRSC, FAULT, DRDY, and BUSY. Error codes include AMNF, TONF, ABRF, IDNF, UNC, and ICRC.

### The fourth imaging pass.

## Fifth pass

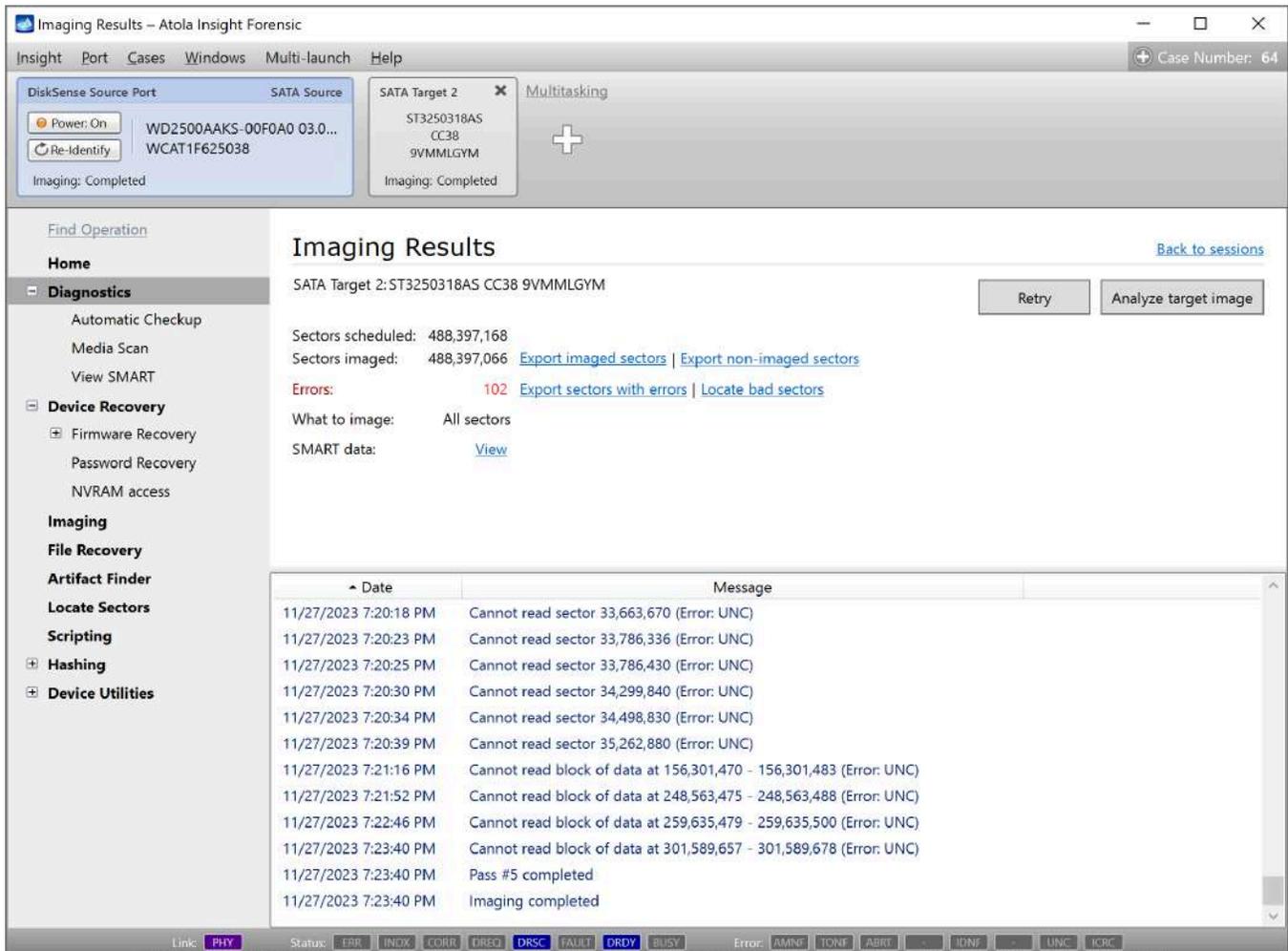
On the fifth pass, Insight allocates 60-second Timeouts to read the Maximum block size of 256 with just 1-sector Jump on error. It is the last and the most scrupulous attempt to read the remaining problematic areas of the drive.

The screenshot displays the Atola Insight Forensic software interface during the fifth imaging pass. The top menu bar includes 'Insight', 'Port', 'Cases', 'Windows', 'Multi-launch', and 'Help'. The 'Case Number' is 64. The source is 'DiskSense Source Port' (SATA Source) and the target is 'SATA Target 2'. Both are at 99% imaging progress. The central area shows 'Imaging data...' with a progress bar at 99%. The overall speed is 64 MB/s, and the estimated time left is 0 seconds. The diagnostics sidebar on the left includes sections for Home, Diagnostics, Device Recovery, Imaging, File Recovery, Artifact Finder, Locate Sectors, Scripting, Hashing, and Device Utilities. The central data display shows 'Pass: 5 of 5' and 'Overall speed: 64 MB/s'. A performance graph below shows activity over time. The log window at the bottom shows several 'Cannot read' errors (UNC).

Target Hex Viewer	Log	Entropy														
<table border="1"> <thead> <tr> <th>Date</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>11/27/2023 7:20:30 PM</td> <td>Cannot read sector 34,299,840 (Error: UNC)</td> </tr> <tr> <td>11/27/2023 7:20:34 PM</td> <td>Cannot read sector 34,498,830 (Error: UNC)</td> </tr> <tr> <td>11/27/2023 7:20:39 PM</td> <td>Cannot read sector 35,262,880 (Error: UNC)</td> </tr> <tr> <td>11/27/2023 7:20:56 PM</td> <td>Cannot read block of data at 156,301,470 - 156,301,483 (Error: UNC)</td> </tr> <tr> <td>11/27/2023 7:21:52 PM</td> <td>Cannot read block of data at 248,563,475 - 248,563,488 (Error: UNC)</td> </tr> <tr> <td>11/27/2023 7:21:57 PM</td> <td>Cannot read block of data at 259,635,479 - 259,635,500 (Error: UNC)</td> </tr> </tbody> </table>			Date	Message	11/27/2023 7:20:30 PM	Cannot read sector 34,299,840 (Error: UNC)	11/27/2023 7:20:34 PM	Cannot read sector 34,498,830 (Error: UNC)	11/27/2023 7:20:39 PM	Cannot read sector 35,262,880 (Error: UNC)	11/27/2023 7:20:56 PM	Cannot read block of data at 156,301,470 - 156,301,483 (Error: UNC)	11/27/2023 7:21:52 PM	Cannot read block of data at 248,563,475 - 248,563,488 (Error: UNC)	11/27/2023 7:21:57 PM	Cannot read block of data at 259,635,479 - 259,635,500 (Error: UNC)
Date	Message															
11/27/2023 7:20:30 PM	Cannot read sector 34,299,840 (Error: UNC)															
11/27/2023 7:20:34 PM	Cannot read sector 34,498,830 (Error: UNC)															
11/27/2023 7:20:39 PM	Cannot read sector 35,262,880 (Error: UNC)															
11/27/2023 7:20:56 PM	Cannot read block of data at 156,301,470 - 156,301,483 (Error: UNC)															
11/27/2023 7:21:52 PM	Cannot read block of data at 248,563,475 - 248,563,488 (Error: UNC)															
11/27/2023 7:21:57 PM	Cannot read block of data at 259,635,479 - 259,635,500 (Error: UNC)															

### The fifth imaging pass.

After the final pass, the Imaging Results report will show the eventual number of errors on the drive and other detailed statistics.



**The Imaging results report.**

## Customize imaging settings for each pass

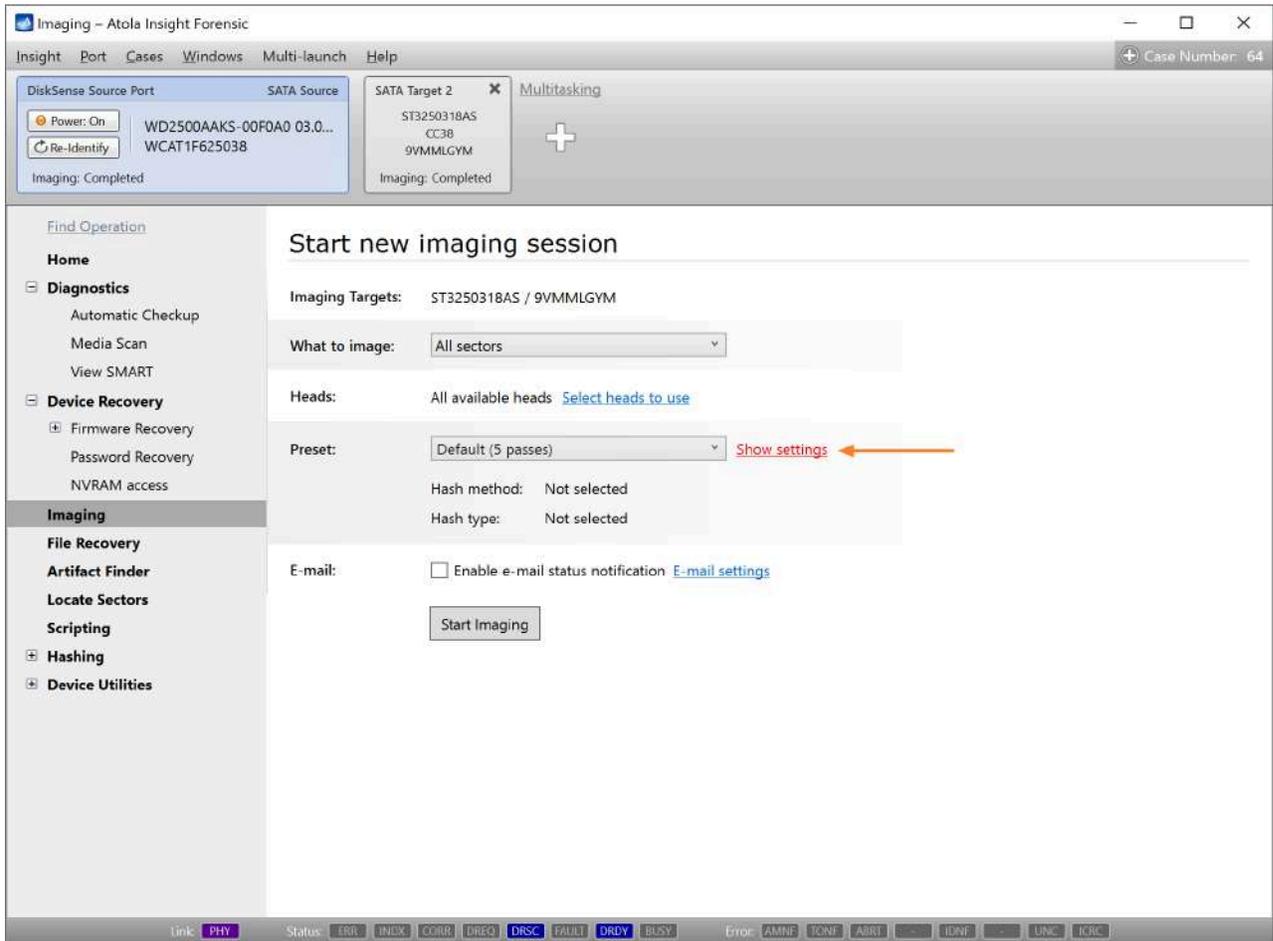
If a particular drive has some unusual damage and requires a specific imaging approach, you can customize the following settings for each pass:

- Timeout
- Jump on error
- Max read block address
- Start and end LBA
- Image in reverse direction
- Disable read look-ahead
- Use PIO mode

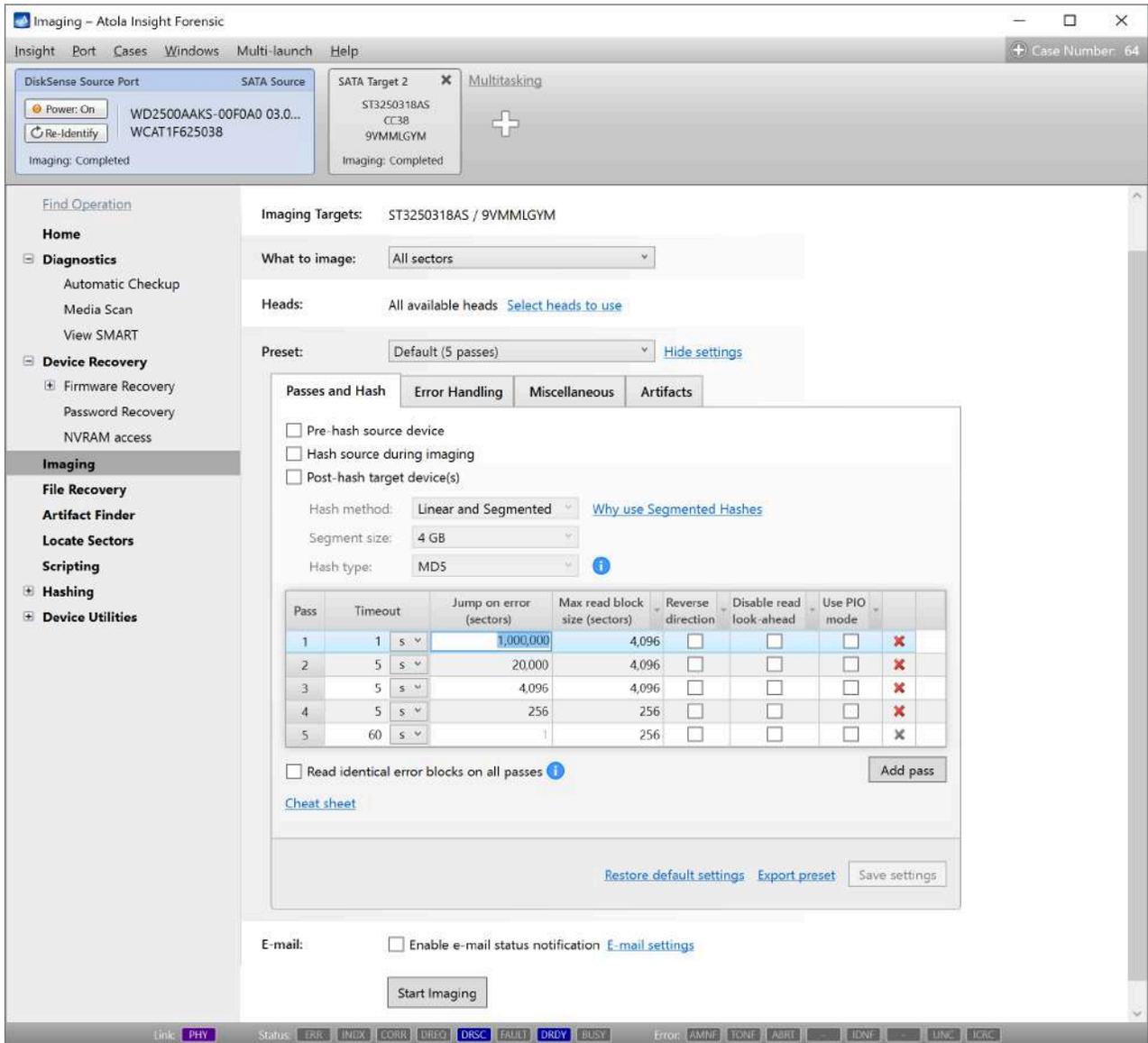
On top of that, you can add passes with customized imaging parameters or remove passes.

To change settings for a certain imaging pass, add or remove passes:

1. In the Insight sidebar, click **Imaging**, and then **Create New Session**.
2. On the **Start new imaging session** screen, in the **Preset** section, click the **Show settings** link.



3. To adjust a particular parameter, click on a respective field and enter a new value.



4. Optional: Adding or removing passes. After you expand the Imaging settings section:

- a. To add another pass, click the **Add pass** button.
- b. To remove a pass, click the **X** icon next to the respective pass.

Preset: Default (5 passes) [Hide settings](#)

**Passes and Hash** | Error Handling | Miscellaneous | Artifacts

Pre-hash source device  
 Hash source during imaging  
 Post-hash target device(s)

Hash method: Linear and Segmented [Why use Segmented Hashes](#)  
Segment size: 4 GB  
Hash type: MD5 ⓘ

Pass	Timeout	Jump on error (sectors)	Max read block size (sectors)	Reverse direction	Disable read look-ahead	Use PIO mode		
1	1 s	500,000	4,096	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	5 s	20,000	4,096	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	5 s	4,096	4,096	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	5 s	256	256	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	60 s	1	256	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Read identical error blocks on all passes ⓘ Add pass

[Cheat sheet](#)

[Restore default settings](#) [Export preset](#) Save settings

5. Click Save settings.

Preset: Default (5 passes) [Hide settings](#)

**Passes and Hash** | Error Handling | Miscellaneous | Artifacts

Pre-hash source device  
 Hash source during imaging  
 Post-hash target device(s)

Hash method: Linear and Segmented [Why use Segmented Hashes](#)  
Segment size: 4 GB  
Hash type: MD5 ⓘ

Pass	Timeout	Jump on error (sectors)	Max read block size (sectors)	Reverse direction	Disable read look-ahead	Use PIO mode		
1	1 s	500,000	4,096	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	5 s	20,000	4,096	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	5 s	4,096	4,096	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	5 s	256	256	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	60 s	1	256	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Read identical error blocks on all passes ⓘ Add pass

[Cheat sheet](#)

[Restore default settings](#) [Export preset](#) Save settings

# Imaging drives with damaged heads

Hard drives with physical damage require a complex imaging approach. This guide will explain how to retrieve data with the minimal risk of data loss on a drive with a damaged head stack.

## Diagnose first

The built-in Automatic Checkup module of Atola Insight Forensic automatically checks all major subsystems of the evidence drive: circuit board, heads, media surface, firmware and file system.

To run diagnostics, in the sidebar, go to **Diagnostics > Automatic Checkup** and click **Start**.

A diagnostics report provides detailed information about the heads. In addition, it offers recommendations for the optimal imaging strategy for your damaged hard drive.

If an **Automatic Checkup report** indicates that there is a problem with the heads, look at the status of each head.

Automatic Checkup finished – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 28

DiskSense Source Port: SATA

Power: On ST9500420AS 0003SDM1  
Re-Identify 5VJ9SYLT

Auto Diagnostics: Completed

Find Operation

Home

Diagnosics

Automatic Checkup

Media Scan

View SMART

Device Recovery

Imaging

File Recovery

Scripting

Hashing

Device Utilities

Print... Save to file... Copy to Clipboard

### Heads

Identifying the device  
Detecting device family  
All device identification checks have passed.  
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 - 600,000, Middle: 488,086,583 - 488,686,583, Inner: 976,023,167 - 976,773,167.

**Head #0 speed graph:**

**Head #1 speed graph:**

**Head #2 speed graph:**

**Head #3 speed graph:**

Head #	Speed	Sectors processed	Freeze count	Read Errors	Head status
0	74 MB/s	447,483	0	0	OK
1	78 MB/s	411,561	0	0	OK
2	5 MB/s	317,871	3	95	Degraded
3	74 MB/s	543,849	0	0	OK

Some sectors failed to read despite verify command succeeded.

Elapsed: 91.2 sec.

According to the media access timing verification test, one or more heads are degraded or their state is unknown.

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

## Head problem found during Diagnostics.

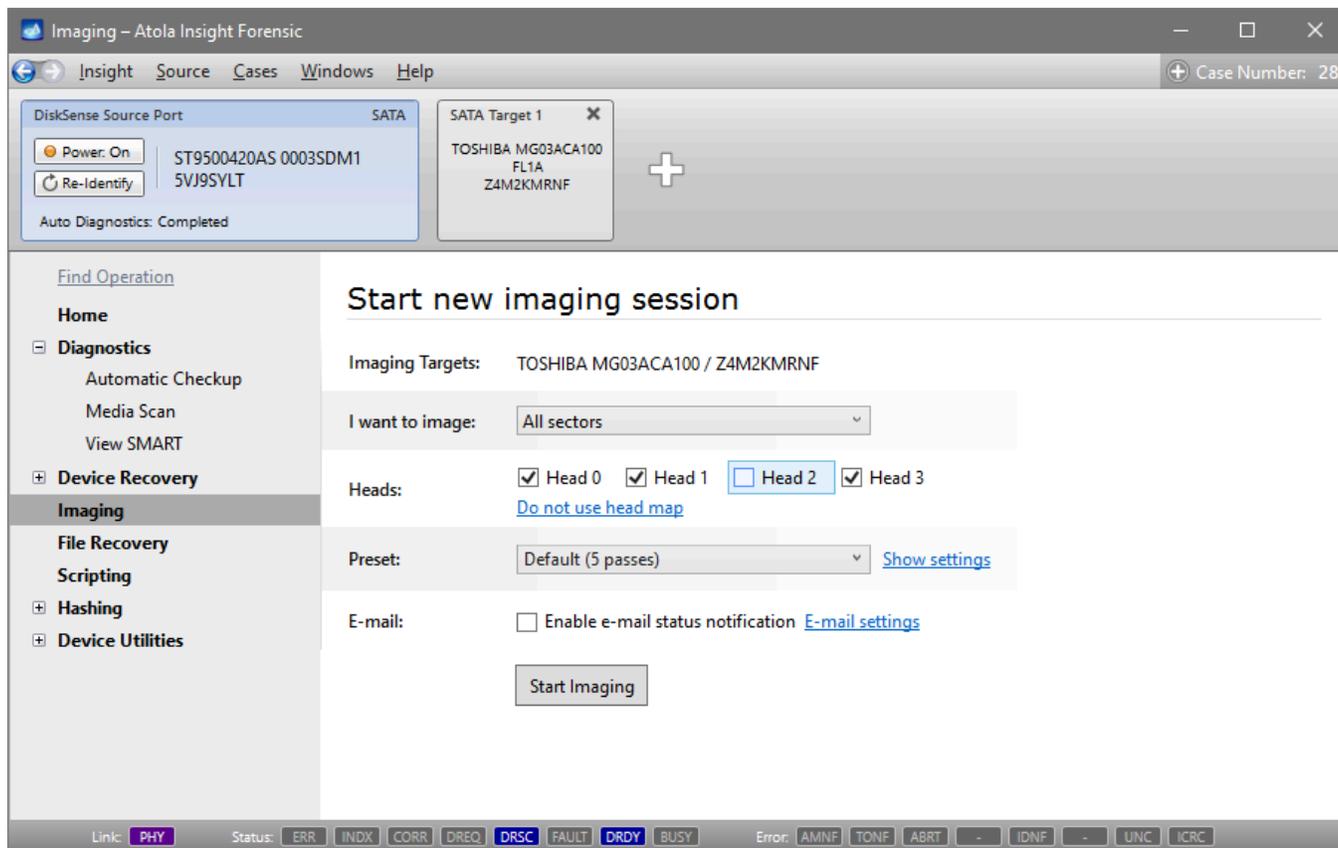
If the status of a head or multiple heads is *Degraded* or *Damaged*, the drive will not be able to read all the data. What's worse, even more sectors may soon become unavailable due to incorrect functioning of the drive's hardware.

## Image good heads

We recommend that you start by imaging the heads, whose status is OK, as soon as possible. To do that:

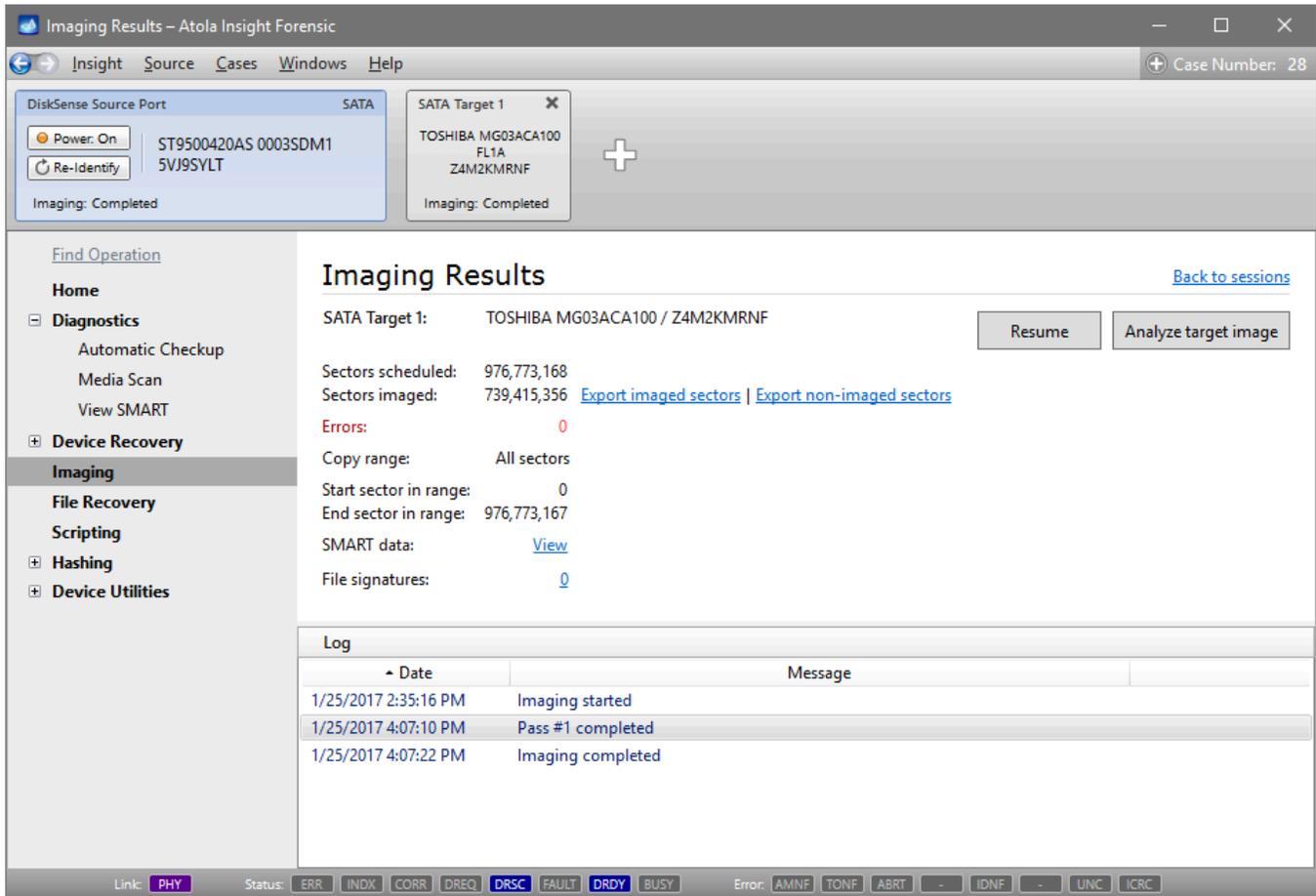
1. In the sidebar, go to **Imaging** and click the **Create New Session** link.
2. Choose the target device or file and click **Select**.

3. On the **Start new imaging session** screen, find the **Heads** section and unselect the damaged head.
4. Click **Start Imaging**.



### Unselect degraded head.

As a result, you get as much data from the drive's viable heads as possible before even beginning to work with the damaged head. This way the risk of losing data on the working part of the head stack is minimized.



### Imaging result with 3 good heads.

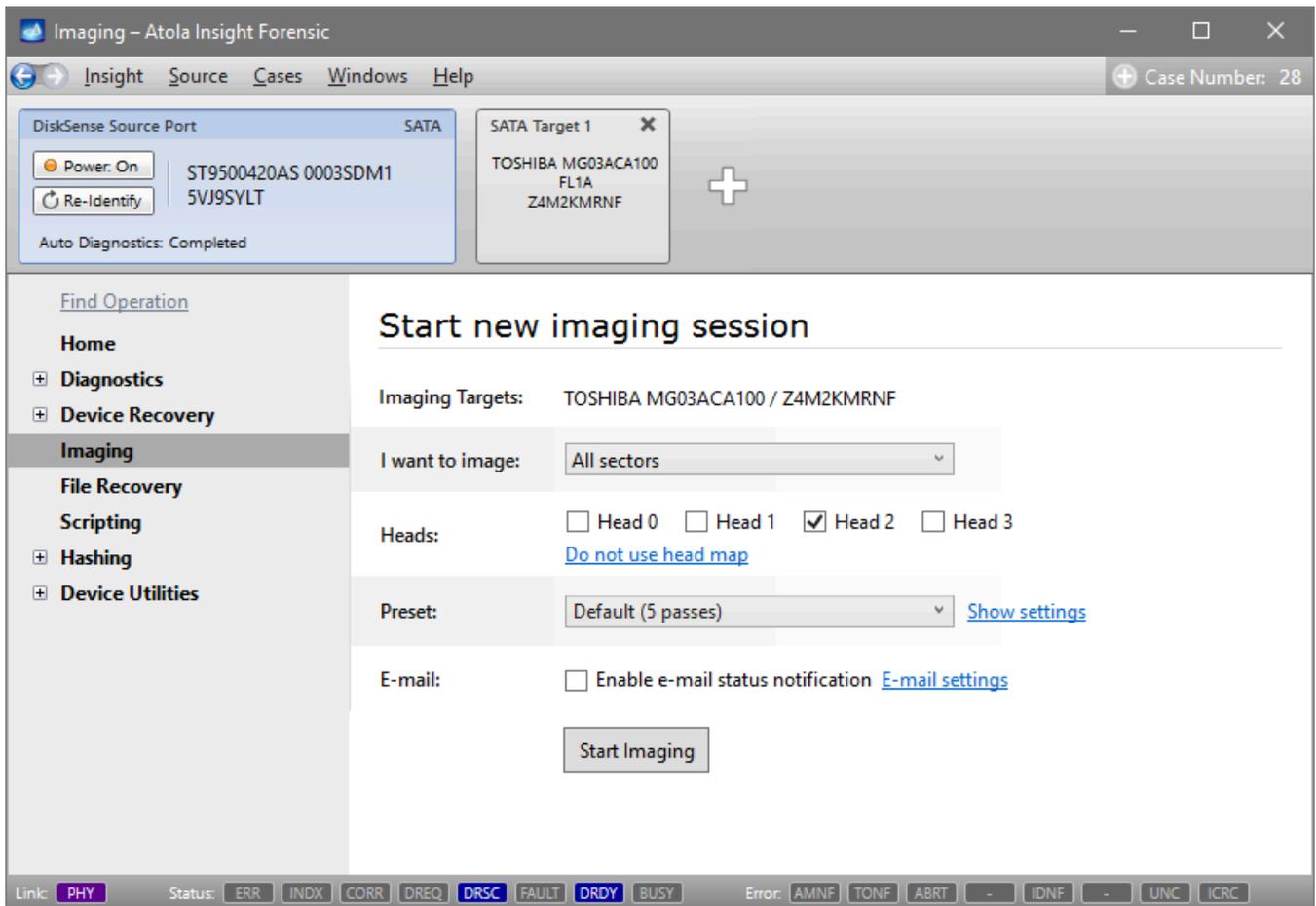
Now that this data has been successfully retrieved, you have two options:

- To have the head stack replaced before imaging the remaining data. However, there is a risk that as a result of head stack replacement, data on the drive can become unreadable.
- To attempt imaging data from the *Degraded* or *Damaged* head.

## Image damaged or degraded heads

Insight’s sophisticated functionality lets users retrieve maximum data even from severely damaged drives. To image damaged or degraded heads, do the following:

1. In the sidebar, go to **Imaging** and click the **Create New Session** link.
2. Choose the target device or file and click **Select**.
3. On the **Start new imaging session** screen, go to the **Heads** line, unselect all the working heads and leave only the **Degraded/Damaged** one(s).
4. Click **Start Imaging**.



**Unselect 3 working heads.**

Imaging – Atola Insight Forensic

Case Number: 28

DiskSense Source Port: SATA  
 ST9500420AS 0003SDM1  
 5VJ9SYLT  
 Auto Diagnostics: Completed

SATA Target 1  
 TOSHIBA MG03ACA100  
 FL1A  
 Z4M2KMRNF

Find Operation

Home

- Diagnosics
  - Automatic Checkup
  - Media Scan
  - View SMART
- Device Recovery
- Imaging**
- File Recovery
- Scripting
- Hashing
- Device Utilities

Imaging data... 24%

0 976,773,167

Pass: 3 of 5 Sectors imaged: 238,754,365

Overall speed: 10 MB/s [Why the speed is so slow?](#) Sectors left: 738,018,803

Estimated time left: 10 hours, 26 minutes Last attempted block: 20,611,820

Found signatures: [216398](#) Total errors: **3,156**

Pause [Imaging settings](#) [Legend](#)

Hint: Move your mouse over the graph to see head number

ms

4 4

3 3

2 2

1 1

13,882,786 17,247,395

Log

Date	Message
1/24/2017 1:04:49 PM	Error block 19,370,105 - 19,374,200 was skipped
1/24/2017 1:04:50 PM	Cannot read block of data at 19,374,201 - 19,468,408 Head: 2 (Error: ABRT)
1/24/2017 1:04:50 PM	Error block 19,676,557 - 19,680,652 was skipped
1/24/2017 1:04:50 PM	Cannot read block of data at 19,468,409 - 19,472,404 Head: 2 (Error: ABRT)
1/24/2017 1:04:50 PM	Error block 19,676,557 - 19,680,652 was skipped
1/24/2017 1:04:51 PM	Cannot read block of data at 19,680,653 - 19,758,476 Head: 2 (Error: ABRT)
1/24/2017 1:04:51 PM	Error block 20,203,069 - 20,207,164 was skipped
1/24/2017 1:04:51 PM	Cannot read block of data at 19,758,477 - 19,778,856 Head: 2 (Error: ABRT)
1/24/2017 1:04:51 PM	Error block 20,203,069 - 20,207,164 was skipped
1/24/2017 1:04:52 PM	Cannot read block of data at 20,207,165 - 20,301,372 Head: 2 (Error: ABRT)
1/24/2017 1:04:52 PM	Error block 20,509,521 - 20,513,616 was skipped
1/24/2017 1:04:52 PM	Cannot read block of data at 20,301,373 - 20,305,368 Head: 2 (Error: ABRT)
1/24/2017 1:04:52 PM	Error block 20,509,521 - 20,513,616 was skipped
1/24/2017 1:04:53 PM	Cannot read block of data at 20,513,617 - 20,607,824 Head: 2 (Error: ABRT)
1/24/2017 1:04:53 PM	Error block 21,036,033 - 21,040,128 was skipped
1/24/2017 1:04:54 PM	Cannot read block of data at 20,607,825 - 20,611,820 Head: 2 (Error: ABRT)
1/24/2017 1:04:54 PM	Performing power cycle after 300 consecutive errors...
1/24/2017 1:05:00 PM	Waiting for device to become ready...
1/24/2017 1:05:06 PM	Error block 21,036,033 - 21,040,128 was skipped

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

### Imaging degraded head.

Now that you have an image of the source evidence including the data copied from the damaged head, you can take the risk and get the head stack fixed. Afterward, you can start a new session to complete the initially created image with data from previously unreadable sectors.

## Imaging freezing damaged drives

When Atola Insight Forensic performs imaging, it can succeed even with the drives that freeze.

### Why do damaged drives freeze?

When a drive receives and runs a **Read sectors** command, and comes across a physically or logically damaged sector, the device 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.

However, often the drive is unable to read data from the damaged sectors, and the **Retry** mode can last for a very long time before the drive decides to give up on a particular sector and return an error with a timeout.

### How does Insight handle freezing drives?

If Insight 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.

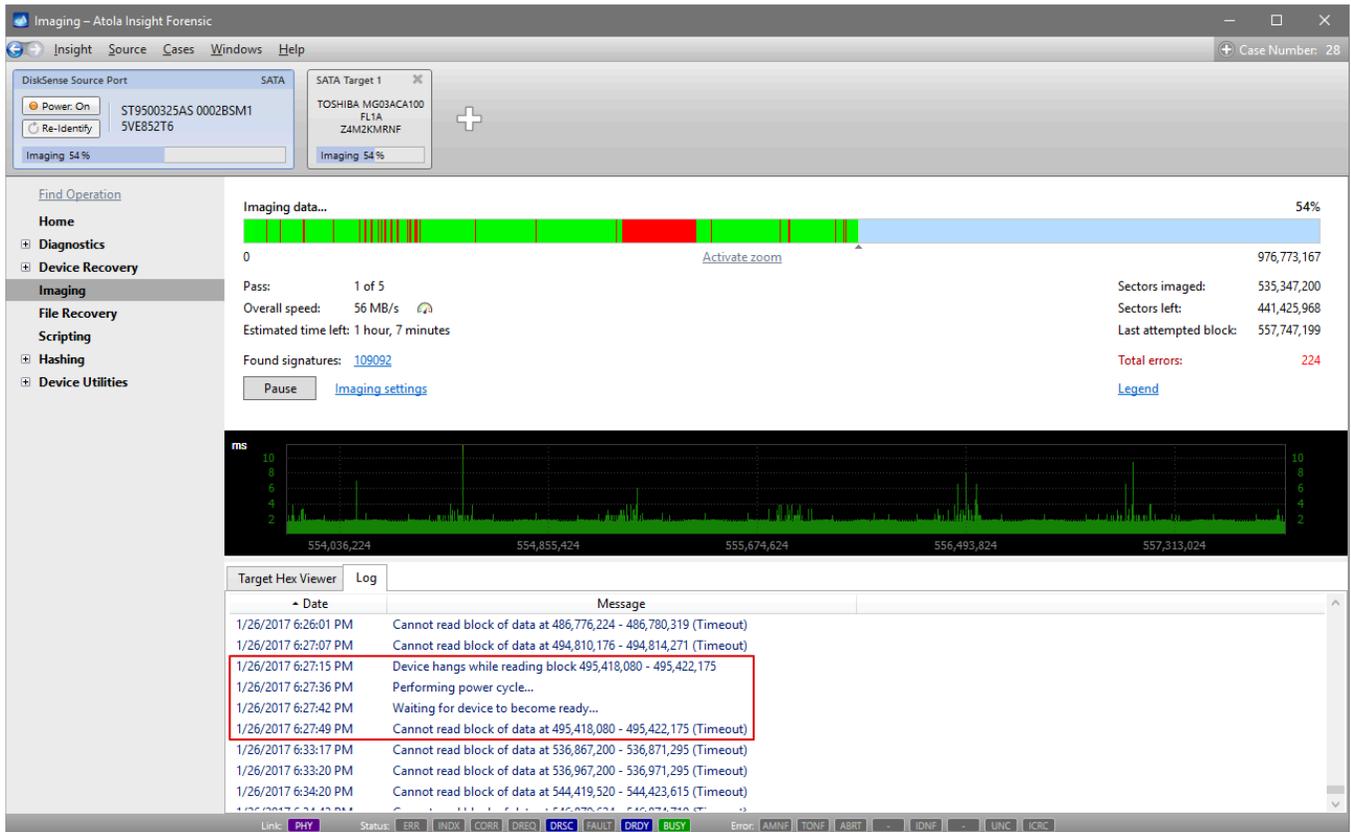
### The Reset command

To avoid causing further damage to the data on the drive and long waiting periods, Insight issues the **Reset** command whenever a drive attempts to read a block of sectors for longer than allowed by the pre-configured timeout.

**Reset** is a device interface operation, using which Insight (the *host*) 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, Insight will wait 3 seconds and perform the second **Reset** command. At the moment of the second **Reset**, a new entry will appear in the imaging **Log** reading

```
Device hangs while reading block X - Y.
```



**Power cycle due to the source device falling into freeze.**

## Performing a power cycle

If 20 seconds after the second **Reset**, the drive still tries to read the bad block, Insight performs a **Power cycle** by forcibly cutting power to the drive for 5 seconds.

At this point, Insight 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).

## After a successful power cycle

If the first **Power cycle** command is successful, and the drive becomes ready to receive another 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 Insight 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 a **Busy** state and can't run another command, Insight makes one or more additional power cycles.

In Insight's default settings, the **Max consecutive Power Cycles** option is set to *five*. If all five Power cycles are unsuccessful, imaging is terminated. It can be resumed afterward, and Insight will continue to image all remaining sectors.

While users can change the default maximum numbers of Resets and Power cycles, this number is based on our decades-long experience and balances the need for data retrieving with the risk of further data loss.

## Features with the 'until power cycle' option

If prior to imaging you apply the **Change Max Address temporarily (until power cycle)** option, the Power cycles performed in the course of imaging do not affect it. The Host Protected Area remains accessible throughout the imaging process. Insight temporarily removes the HPA max address restriction after each imaging-related Power cycle.

The same is true for the **Reset Password until power cycle** option. Insight keeps the password reset throughout the imaging process, without regard to the applied Power cycles.

## Imaging a shorted hard drive

Every once in a while forensic examiners come across hard drives that get shorted. 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 drive in these scenarios and how to fix this.

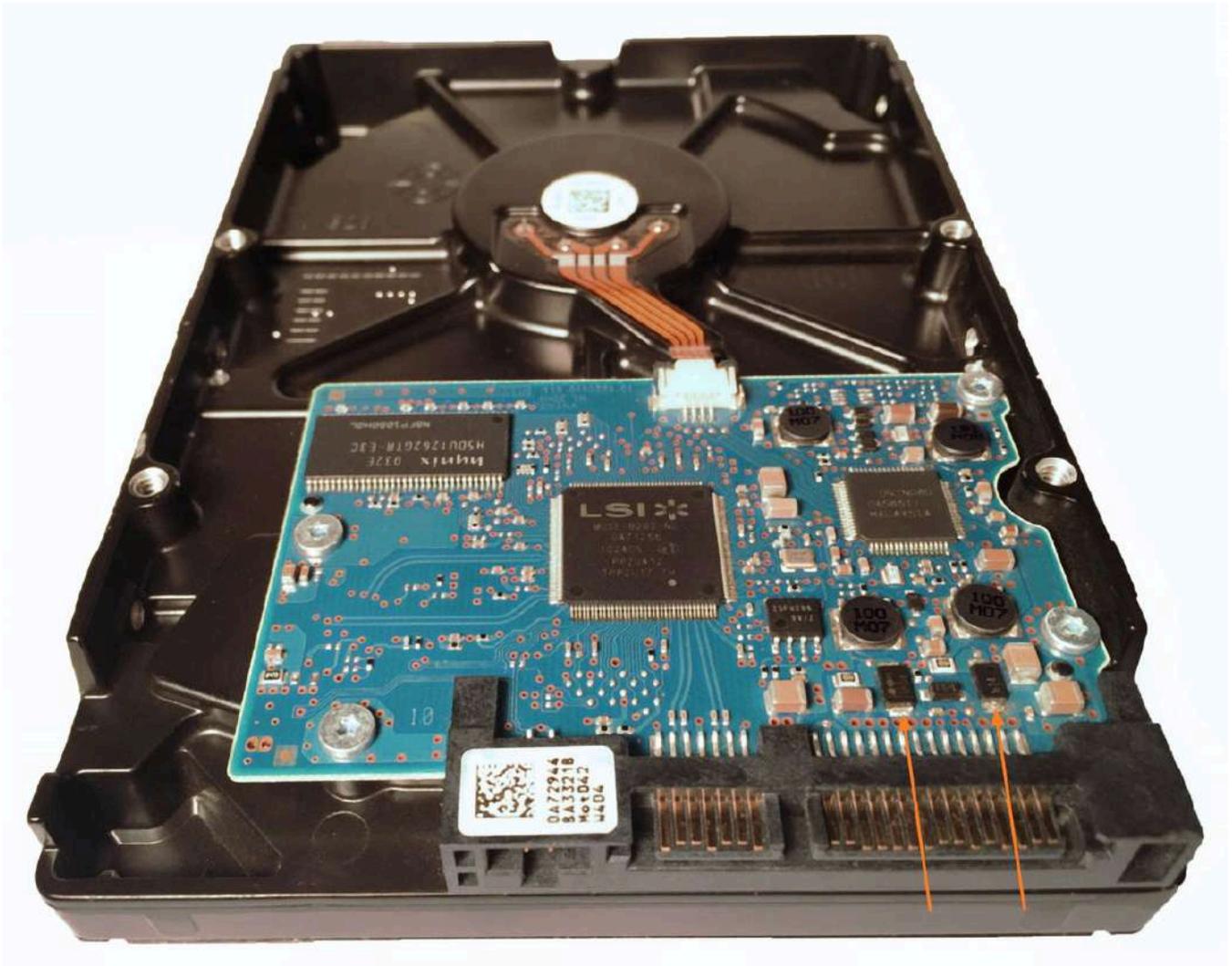
## How drives become shorted

Most drives have two TVS diodes: one on the 5V rail and another one on the 12V rail.

If a drive experiences an overvoltage, its 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.

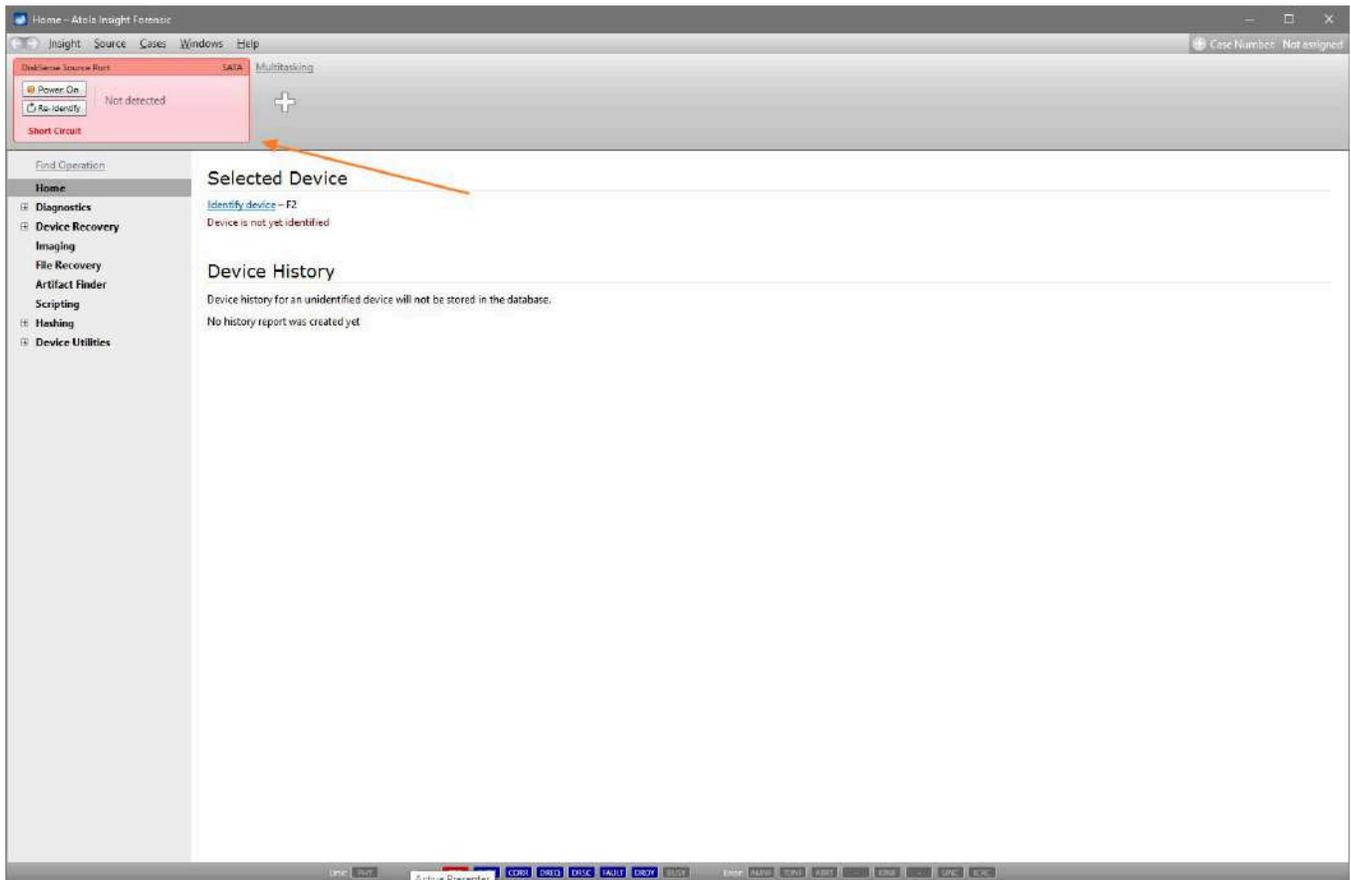
If the overvoltage or reverse polarity event is short and the dissipated energy is not too high, the diodes can recover and continue working. However, if the dissipated energy is too high, the diodes will "sacrifice" themselves and get shorted.

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.



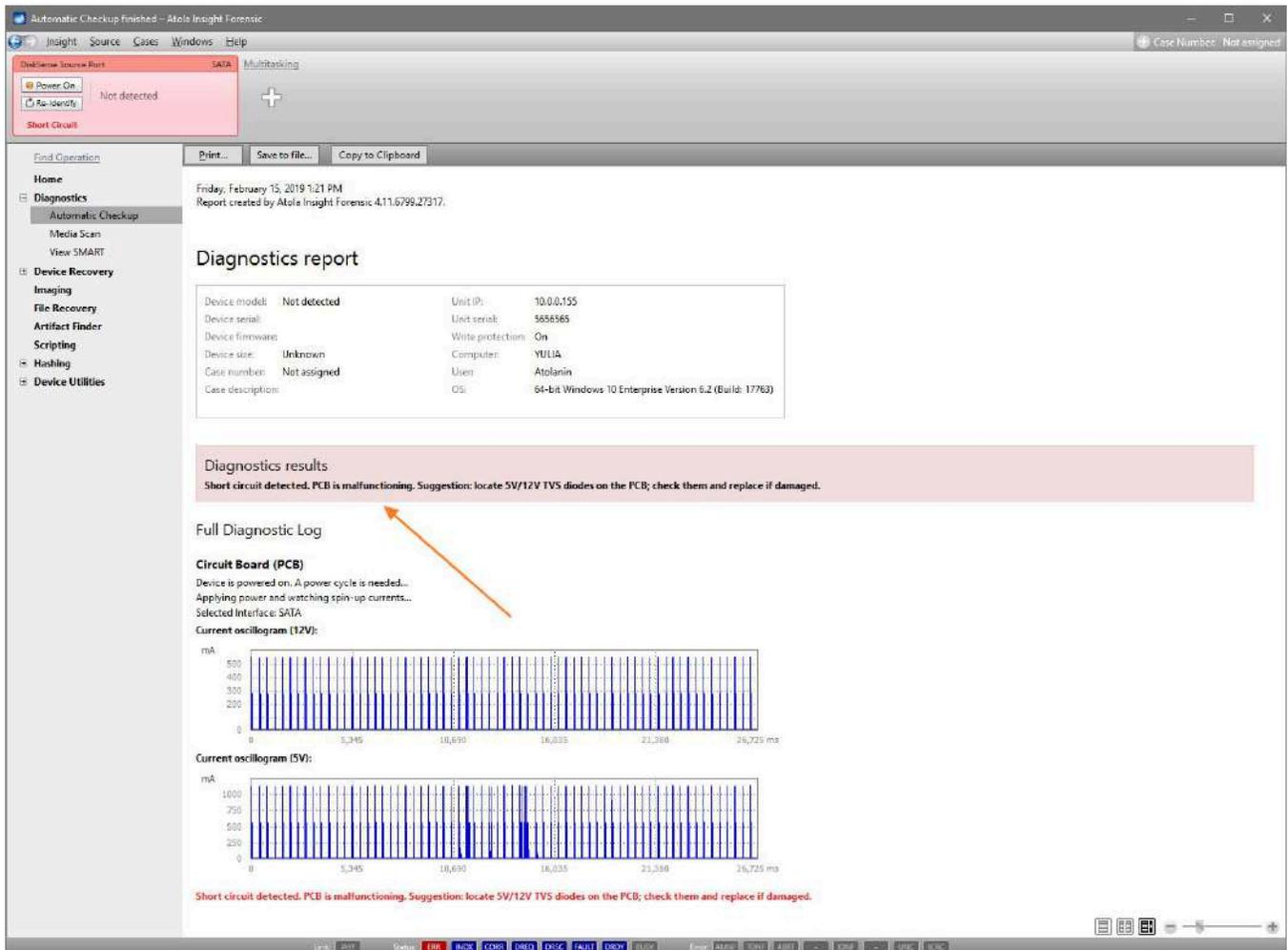
## Detect a shorted drive

If you try to connect a shorted drive to Atola Insight Forensic, the Source window will have a short circuit alert to notify the operator about the detected issue.



### Short circuit alert.

A drive with a shorted TVS diode cannot be identified or imaged. You can try to run diagnostics on the drive, although it cannot be properly diagnosed and the report will suggest that the TVS diodes should be replaced.



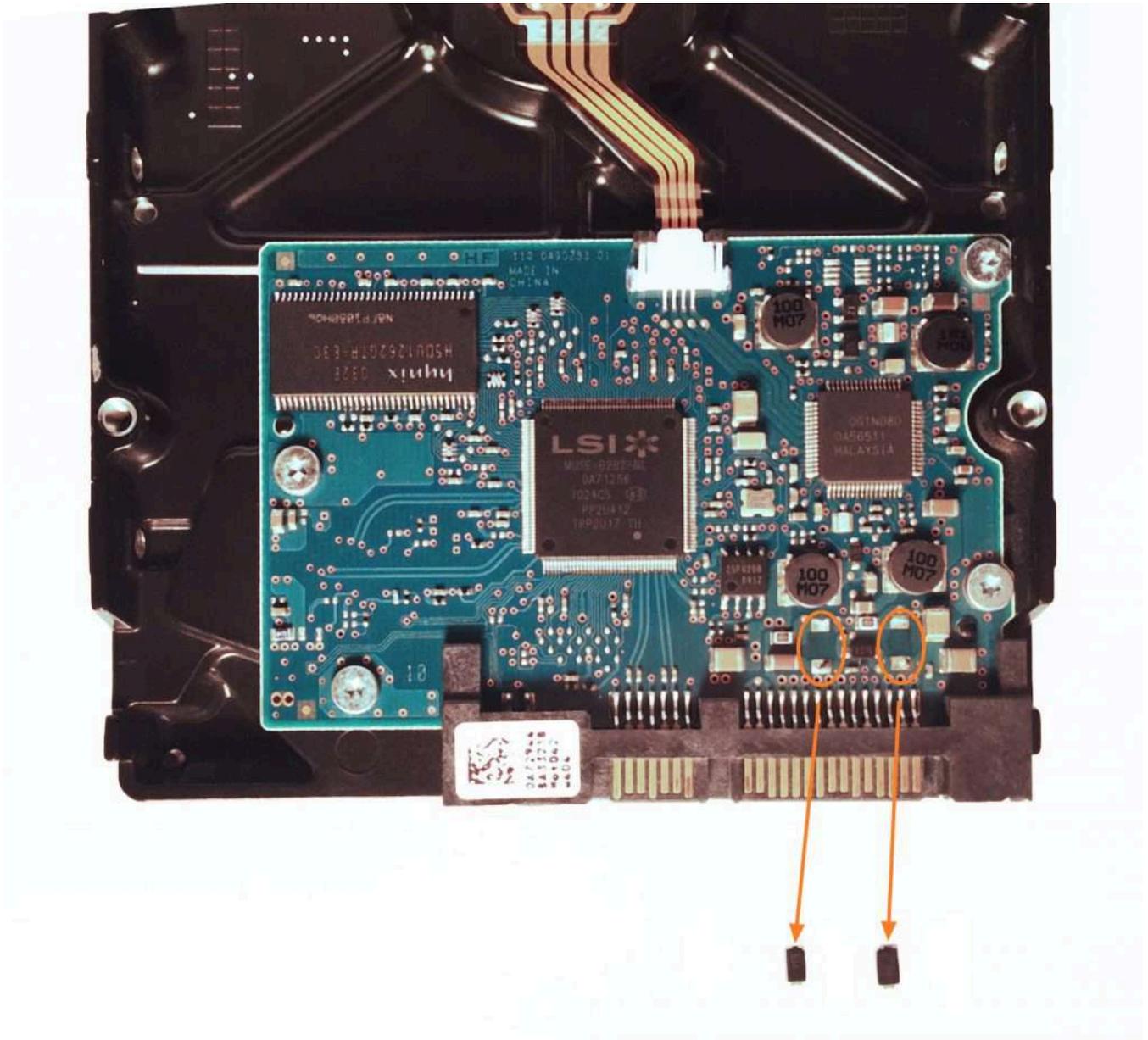
**Diagnostics report of a shorted drive.**

## Image a shorted drive

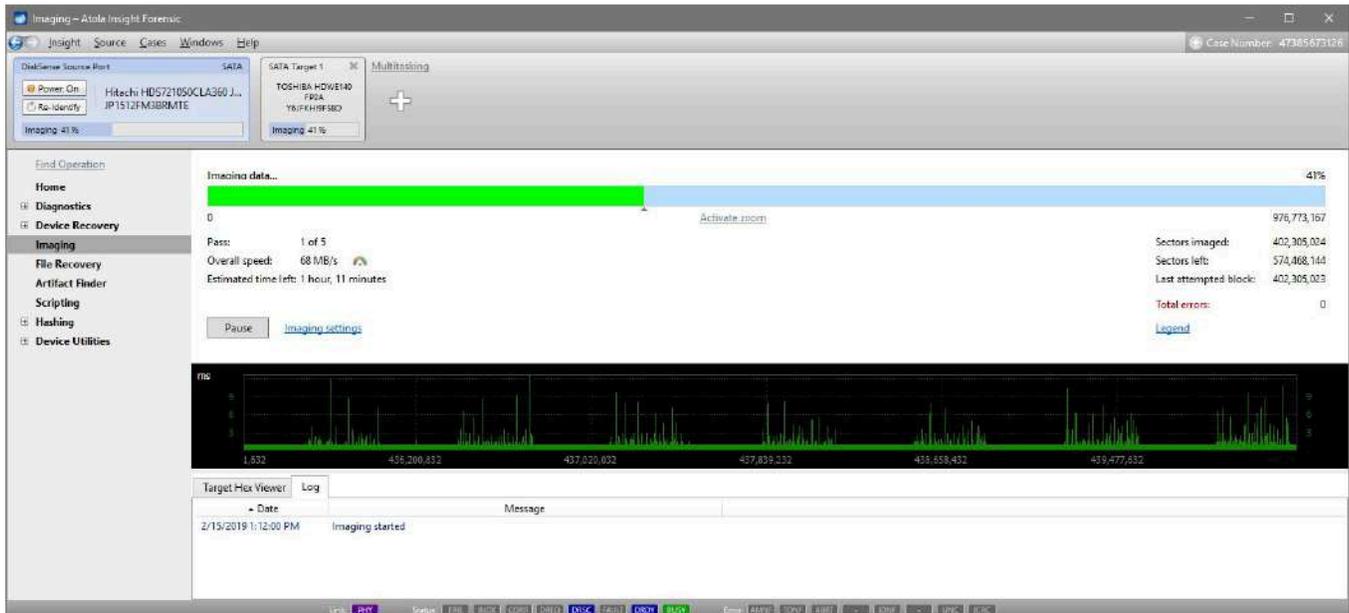
If you need to image a shorted drive but do not have new TVS diodes on hand to replace the shorted ones, you can image the drive using Insight after removing the diodes.

This process is safe because Insight 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 Insight and proceed with imaging data from its platters.



**Imaging a drive with detached TVS diodes.**

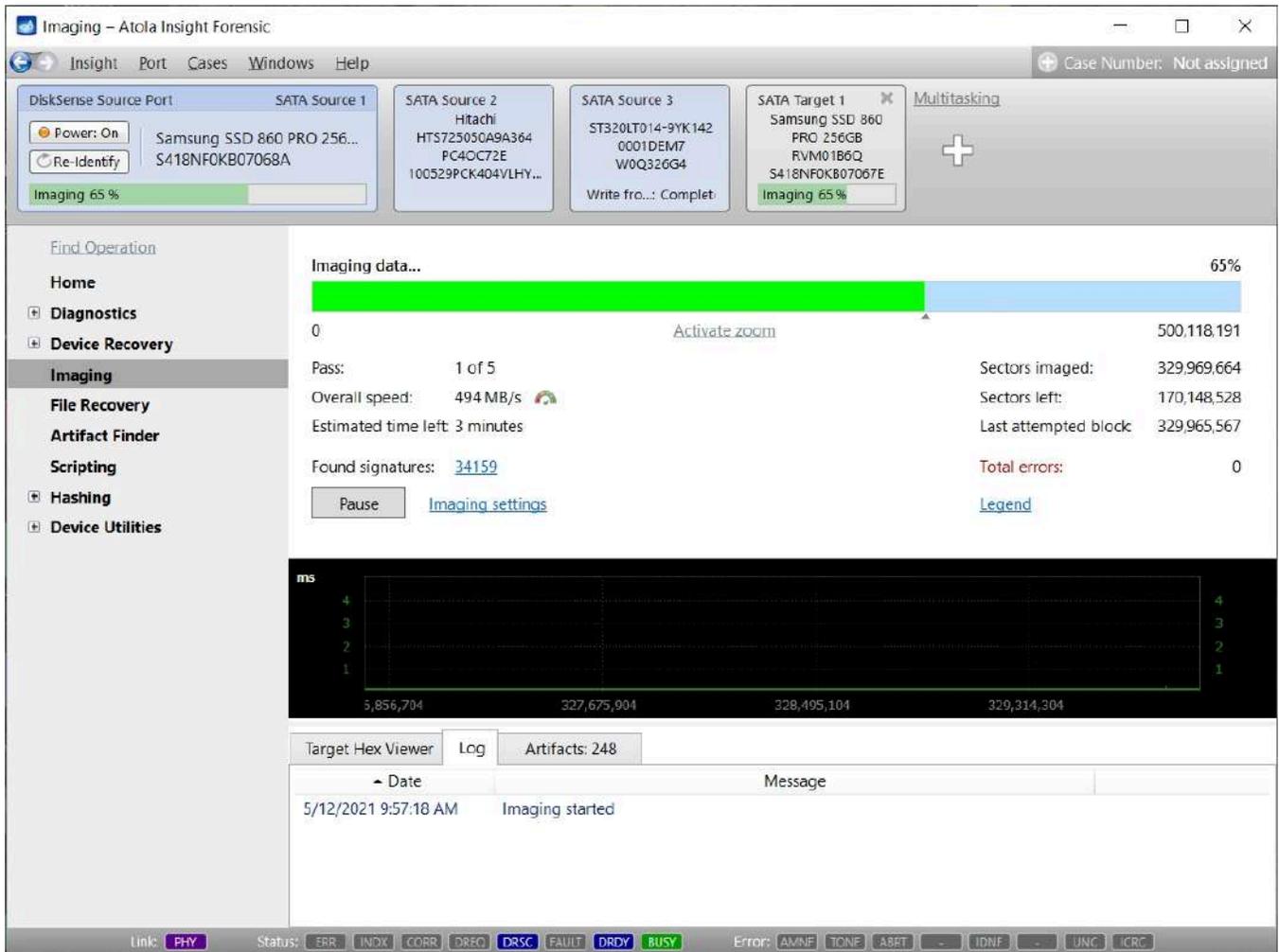
## Imaging speed

To evaluate Atola Insight Forensic's imaging performance, we imaged a few popular models of HDDs, SSDs and USB flash drives and cross-checked the speed with [userbenchmark.com](http://userbenchmark.com), where you can find detailed info on the minimum, average and maximum read and write speed of almost every data storage device in the market.

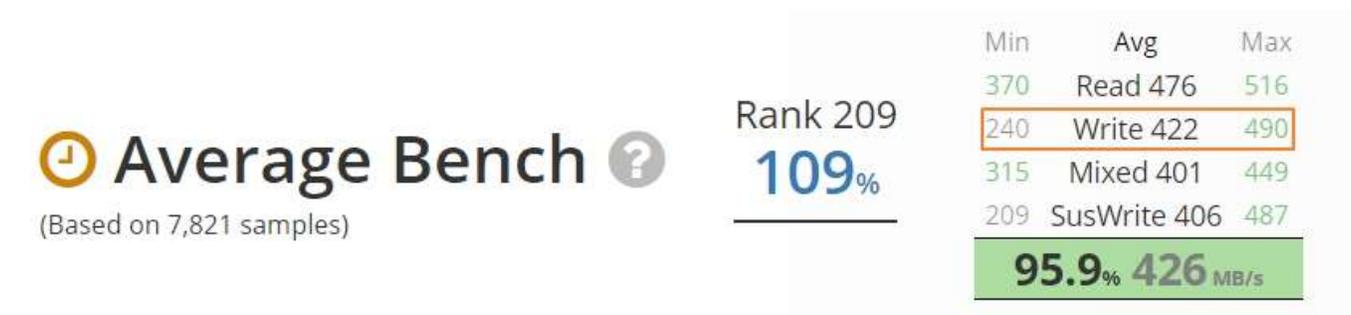
**NB** Imaging speed is always limited by the speed of the slowest of the devices participating in an imaging session. Therefore, the slowest of the two speeds (either the read speed of the source or the write speed of the target) will define the speed at which [forensic imaging process](#) is running.

## Samsung 860 PRO 256GB

We start with popular Samsung 860 PRO SSDs for both source and target. Both drives are not damaged but are rather worn out because we have been using them for imaging speed demonstrations at trade shows for a few years now. Insight images such SSDs at 494 MB/s (it is the write speed of the target drive that is defines the imaging speed in this case).

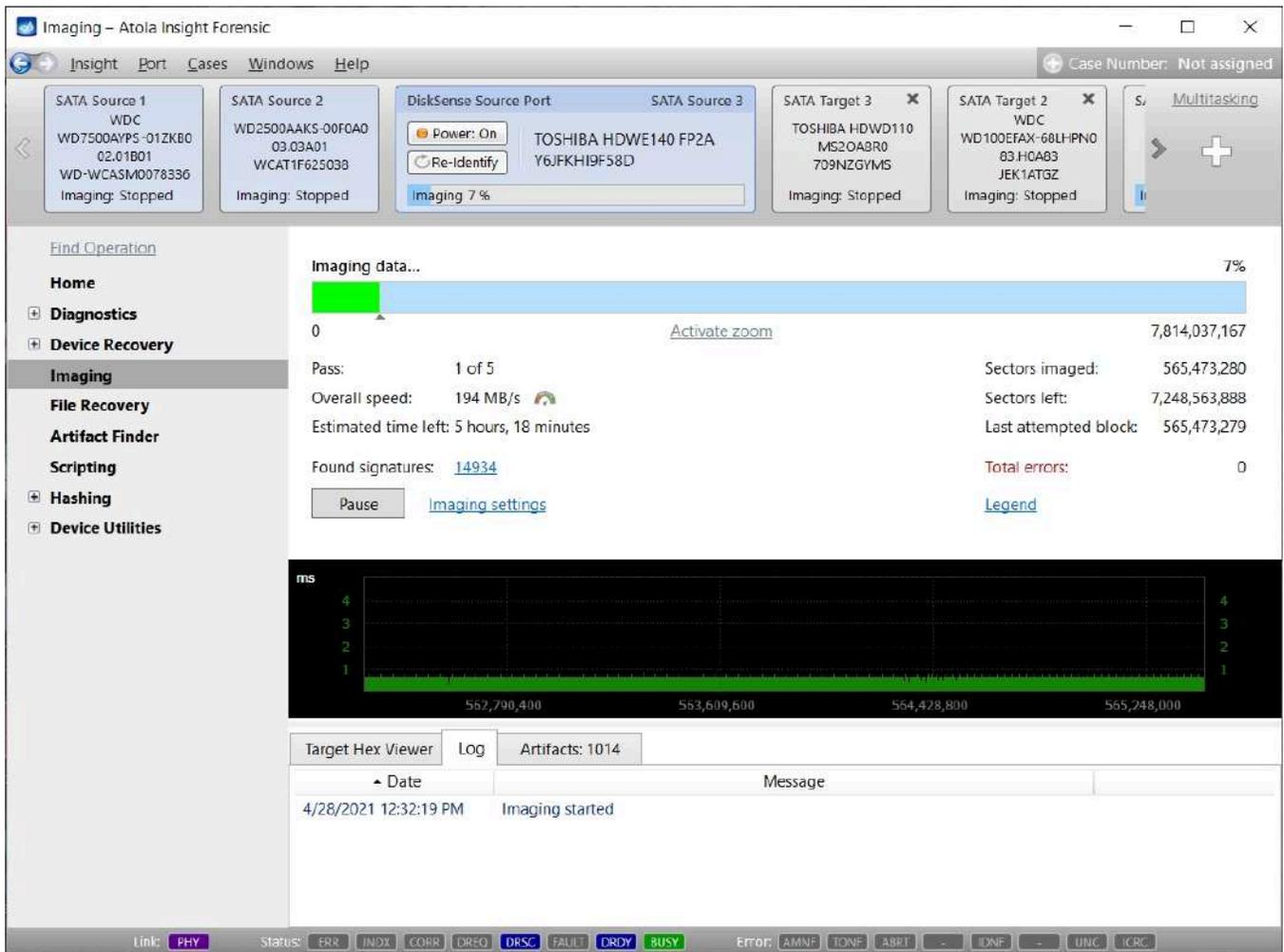


At userbenchmark.com, the [256GB Samsung 860 Pro's](#) maximum write speed in sequential mode (sectors read and written to in sequential order) is 490 MB/s, less than the speed demonstrated by Atola Insight.



## Toshiba X300 4TB

When Insight images a 4TB Toshiba X300 (an HDD with SATA interface), it achieves the speed of 194 MB/s.



How does this speed compare to the one at userbenchmark.com? The [website quotes 184 MB/s](#) of max read speed. Insight's speed substantially exceeded the benchmark speed based on almost 19 thousand samples!

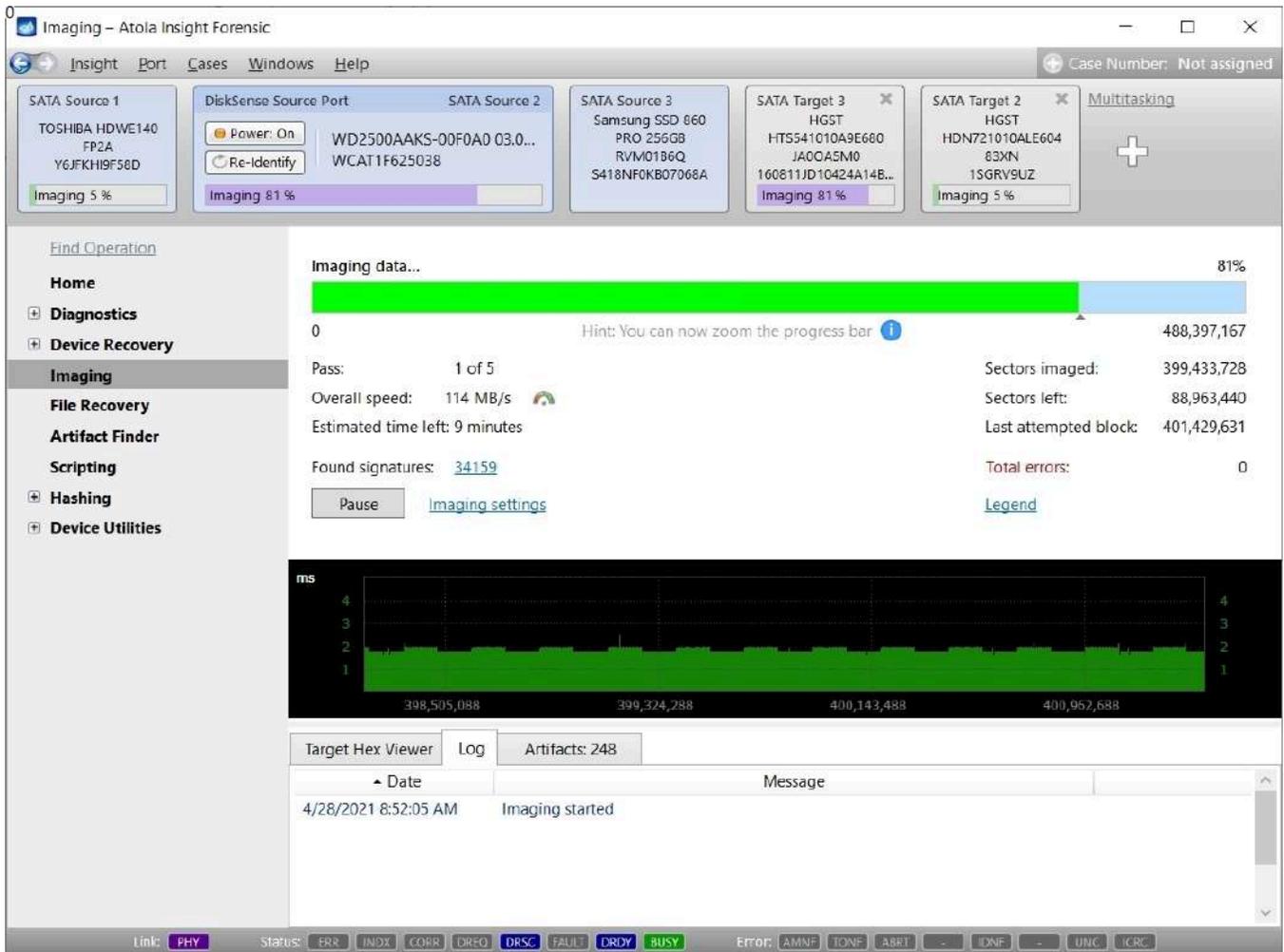
**Average Bench**   
 (Based on 18,849 samples)

Rank 45  
**86.6%**

Min	Avg	Max
96.1	Read 152	184
95.8	Write 149	180
42	Mixed 63.3	71.8
95.6	SusWrite 149	185
<b>93.5%</b>		<b>128 MB/s</b>

## Western Digital's Blue 250 GB (2008)

Insight's speed of imaging a Western Digital's Blue 250 GB constituted 114 MB/s.



At userbenchmark.com the same drive's [max read speed is 114 MB/s](#). Again Insight achieved the top speed based on over 8000 samples.

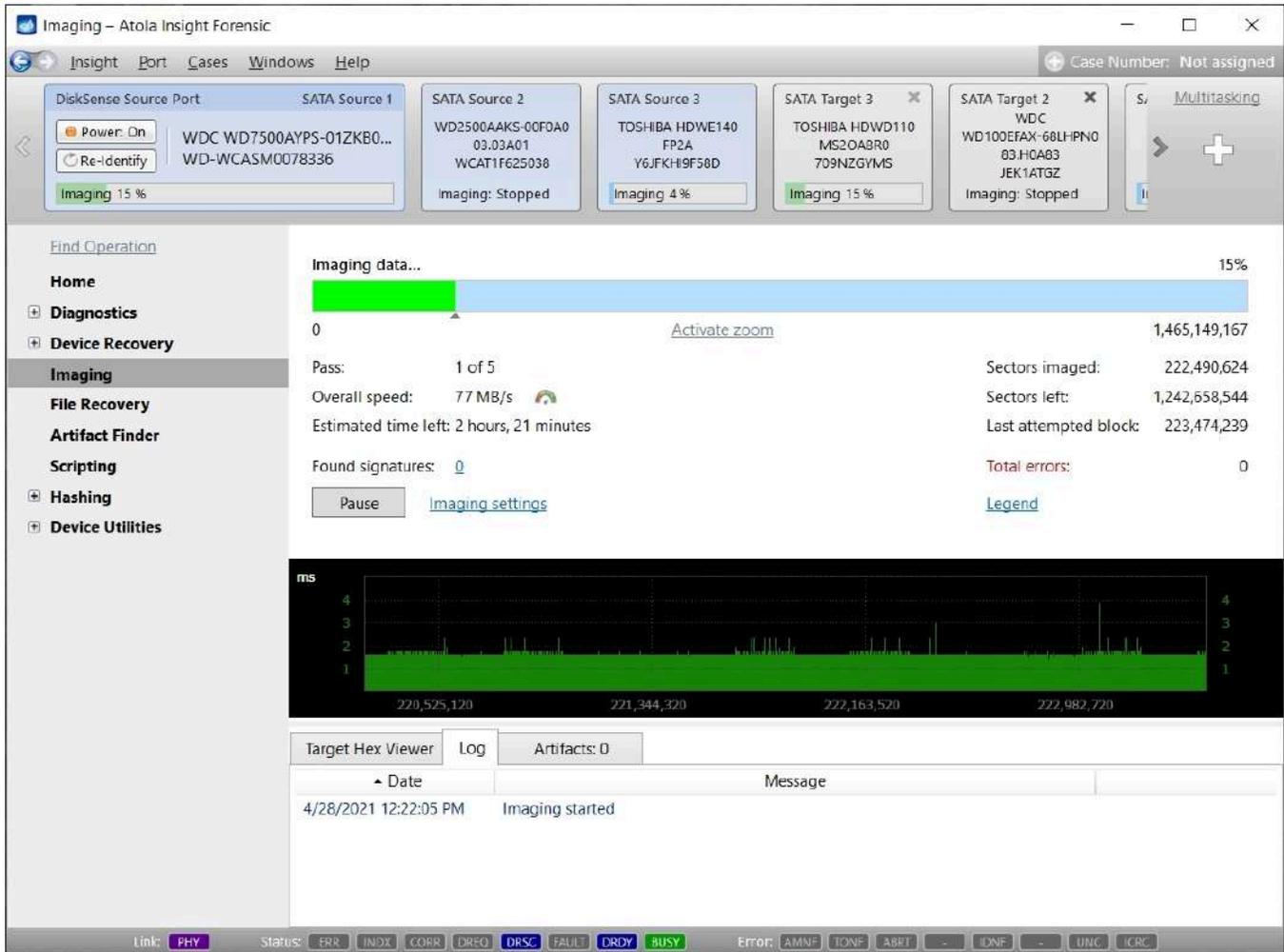
 **Average Bench**   
 (Based on 8,692 samples)

Rank 432  
**44%**

	Min	Avg	Max
Read	45.9	80	114
Write	38.7	77	112
Mixed	34.8	54.4	69.3
SusWrite	33.4	73	110
<b>Average</b>	<b>52.4%</b>	<b>71.1</b>	<b>MB/s</b>

## Western Digital WD7500AYPS 750GB

Insight reaches 77 Mb/s when reading WD7500AYPS 750GB drive.



The same drive at userbenchmark.com achieved the [maximum read speed of 76.3 MB/s](#). Again Insight has exceeded this value.

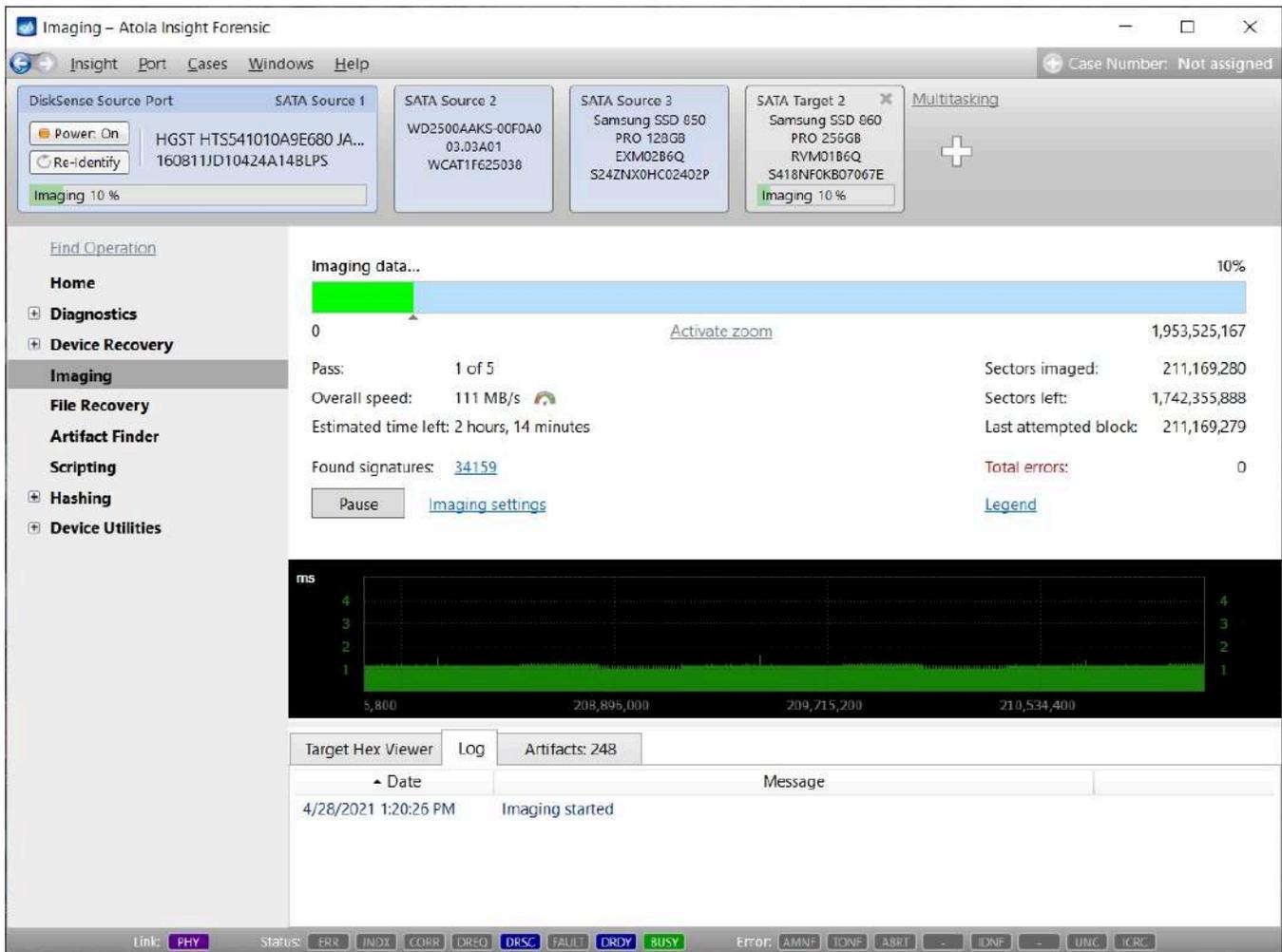
**Average Bench** ?  
 (Based on 172 samples)

Rank 615  
**34.3%**

	Min	Avg	Max
Read	38.4	61.3	76.3
Write	36.7	58.2	74.9
Mixed	23.7	48.2	70.2
SusWrite	38.3	57.9	74.4
		<b>41.8%</b>	<b>56.4 MB/s</b>

## HGST HTS41010A9E680 1TB

When imaging this HGST 1TB SAS hard drive, Insight achieves 111 MB/s.

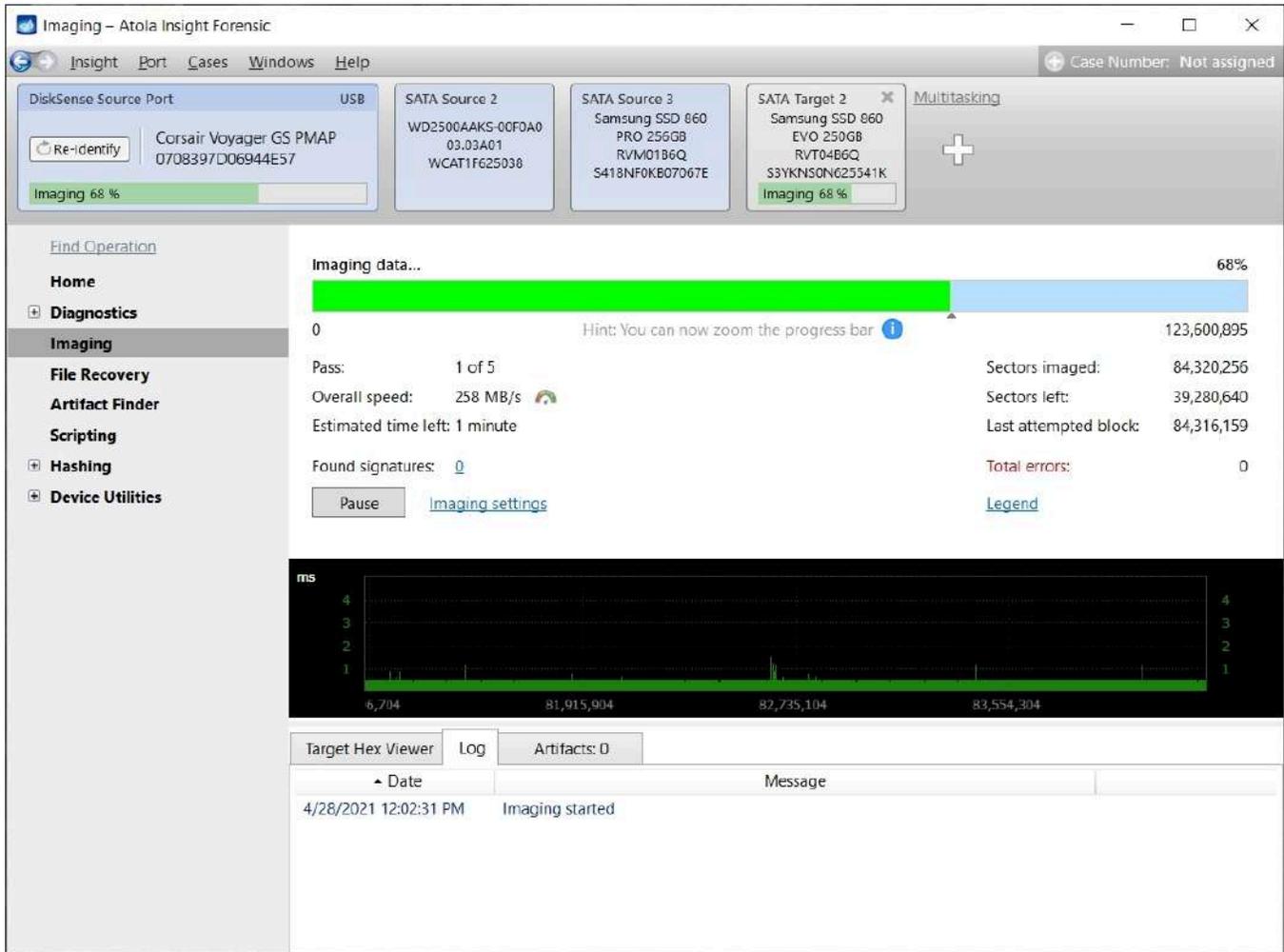


And it is a much higher speed than that of userbenchmark.com ([104 MB/s max read speed](#)).



## Corsair Voyager 3.0 64GB

Next, we image Corsair Voyager 3.0 64GB USB, and Insight reached the speed of 258 MB/s.



The [max read speed constituted 281 MB/s](#) as registered by the contributors of userbenchmark.com. Insight imaged it below the max speed but still substantially above the average.



Please note that here we imaged devices that were in overall good health. Imaging may be considerably slower when dealing with a damaged drive, and the speed heavily depends on the type and degree of such damage.

Here are links to the userbenchmark.com pages with the devices mentioned above for your reference (please note that the screenshots in this article were made in May 2021, the indices you find at these links may change over time):

Samsung 850 Pro 256GB <https://ssd.userbenchmark.com/Samsung-850-Pro-256GB/Rating/2385>

Samsung 850 Pro 128GB <https://ssd.userbenchmark.com/Samsung-850-Pro-128GB/Rating/3483>

Toshiba X300 4TB <https://hdd.userbenchmark.com/Toshiba-X300-4TB/Rating/3592>

WD Blue WD2500AAKS 250GB <https://hdd.userbenchmark.com/SpeedTest/2143/WDC-WD2500AAKS-00L6A0>

WD WD7500AYPS-01ZKB0 750GB <https://hdd.userbenchmark.com/SpeedTest/7309/WDC-WD7500AYPS-01ZKB0>

HGST Travelstar 5K1000 2.5" 1TB <https://hdd.userbenchmark.com/SpeedTest/72/HGST-HTS541010A9E680>

Corsair Voyager GT 3.0 64GB <https://usb.userbenchmark.com/SpeedTest/5886/Corsair-Voyager-GT-30>

## Launch a command-line interface app after imaging

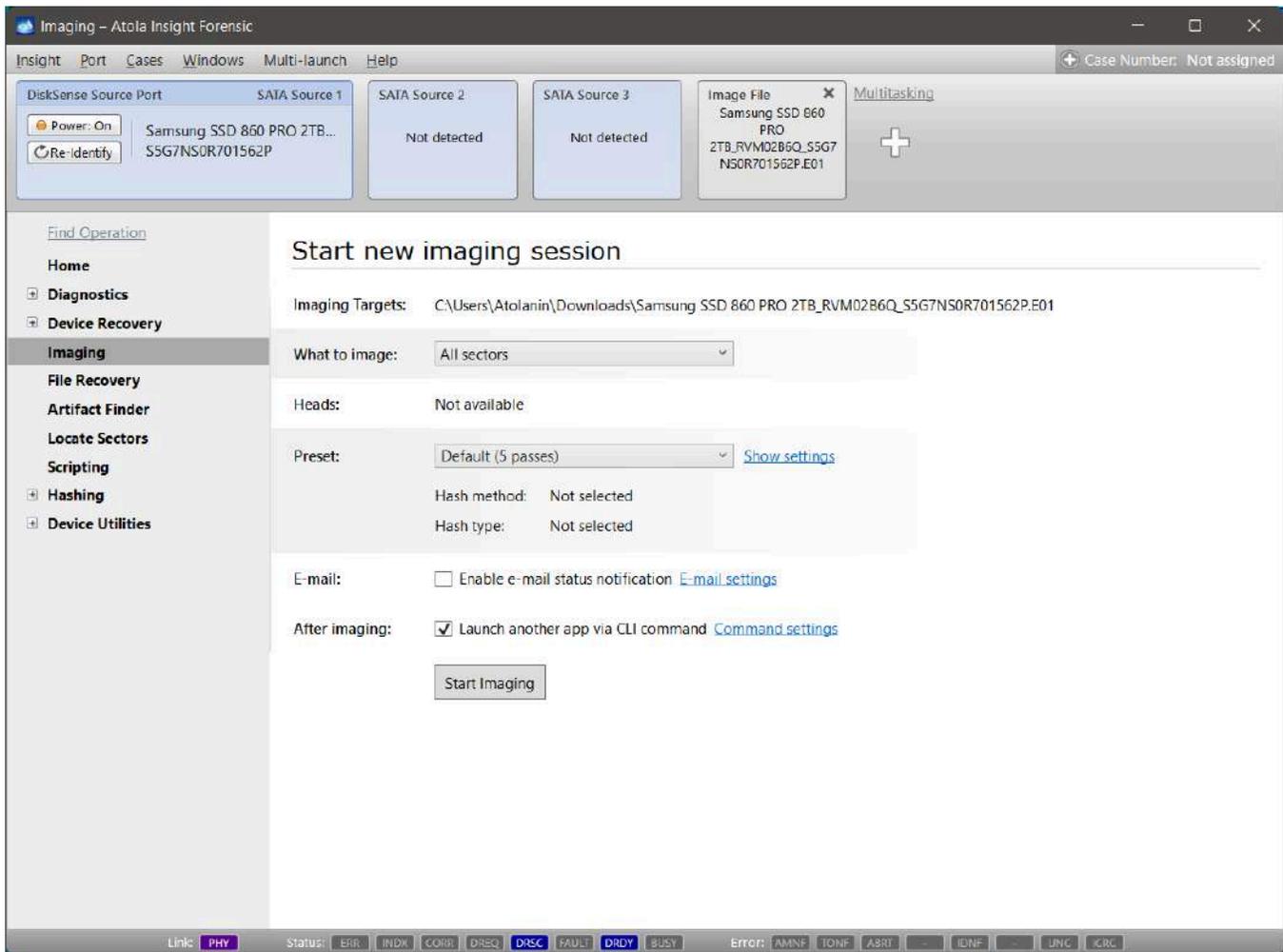
To include an imaging process in your automated workflow, you can tell Atola Insight Forensic to launch another application after imaging using command-line interface (CLI). It can be a single CLI command with custom arguments or even a chain of commands contained in a BAT file.

## How to launch a CLI app after imaging

If you want to launch not one, but a chain of custom CLI commands after imaging, you need to save them as the BAT file beforehand.

To launch a command-line interface app after imaging, do the following:

1. Connect your source and target devices to Atola DiskSense 2 hardware unit.
2. Click on the port with your source device.
3. Go to **Imaging** > **Create new session**, and then select your target device.
4. On the **Start new imaging session** screen, find the **After imaging** section, and then select **Launch another app via CLI command**.



5. To specify that CLI app to launch, click **Command settings**.

6. In the **Application** field, enter the path to the executable file of your application or to your BAT file.

7. In the **Arguments** field, enter command-line arguments for your application.

Atola Insight Forensics assists in specifying default arguments of Autopsy, X-Ways, Forensic Explorer, and OSFMount.

Atola Insight Forensic saves the path to the resulting target image file as a variable and can pass this variable to your CLI app:

- %1 - full path to the first target image file
- %2 - full path to the second target image file
- %3 - full path to the third target image file

We recommend using %1 in double quotes due to possible spaces in the file path.



8. **Optional:** To see the possible result of running your application with specified arguments, click **Test command**.
9. After entering the application path and arguments, click **OK**.
10. Click **Start imaging**.

The imaging starts. When it is completed, Atola Insight Forensic launches the specified CLI app against the resulting image and records all the command-line interface commands it runs.

The message that a CLI app has been launched shows in the imaging log.

Imaging Results – Atola Insight Forensic

Insight Port Cases Windows Multi-launch Help Case Number: Not assigned

DiskSense Source Port: USB ST9320320AS B503 55X0HH7Q Re-Identify Imaging: Completed

SATA Source 2: Not detected

SATA Source 3: Not detected

Multitasking

Find Operation

- Home
- Diagnosics
- Imaging**
- File Recovery
- Artifact Finder
- Locate Sectors
- Scripting
- Hashing
- Device Utilities

### Imaging Results

[Back to sessions](#)

Image File: D:\Image-files\ST9320320AS\_B503\_55X0HH7Q\_02.imgp Resume Analyze target image

Sectors scheduled: 848 249

Sectors imaged: 848 249 [Export imaged sectors](#)

Errors: 0

What to image: All sectors with data [View details](#)

File signatures: 4 165

Artifacts: 41 260

CLI app launch after imaging: [Result](#) ←

#### Log

Date	Message
12/15/2022 3:13:13 PM	Found partition at sector 34 (type Unknown). Partition size: 16 MB.
12/15/2022 3:13:13 PM	Found partition at sector 32 768 (type NTFS). Partition size: 320 GB.
12/15/2022 3:13:15 PM	Imaging started
12/15/2022 3:13:27 PM	Pass #1 completed
12/15/2022 3:13:28 PM	Imaging completed
12/15/2022 3:13:31 PM	CLI command has been executed.

The report about the results of launching your custom CLI app appears on the **Imaging results** screen. To view the report and the text output from your CLI app, click on the **Result** link.

```
after-imaging-app-4e40c781-919b-49ae-a245-7726c2c92ba8 - Notepad
File Edit Format View Help
C:\Program Files\Atola Insight Forensic_5_3>"C:\Program Files\OSFMount\OSFMount.com" -a -t file -f "D:\Image-files
\ST9320320AS_BS03_5SX0HH7Q.imgp" -v 2 -m Z:
Creating device...
Created device 3: Z: -> D:\Image-files\ST9320320AS_BS03_5SX0HH7Q.imgp
Notifying applications...
Done.

C:\Program Files\Atola Insight Forensic_5_3>"D:\KAPE\kape.exe" --tsource Z: --tdest D:\Temp3 --target
BrowserCache,Chrome,ChromeExtensions,ChromeFileSystem,Edge,EdgeChromium,Firefox,InternetExplorer,Opera,PuffinSecureBrowser
KAPE version 1.1.0.1 Author: Eric Zimmerman (kape@kroll.com)

KAPE directory: D:\KAPE
Command line: --tsource Z: --tdest D:\Temp3 --target
BrowserCache,Chrome,ChromeExtensions,ChromeFileSystem,Edge,EdgeChromium,Firefox,InternetExplorer,Opera,PuffinSecureBrowser

System info: Machine name: INVESTIGATOR, 64-bit: True, User: Pasyuta OS: Windows10 (10.0.19044)

Using Target operations
    Creating target destination directory 'D:\Temp3'
Found 10 targets. Expanding targets to file list...
Found 14573 files in 1,598 seconds. Beginning copy...

Copied 14573 out of 14573 files in 62,6285 seconds. See '*_CopyLog.csv' in 'D:\Temp3' for copy details

Total execution time: 62,6479 seconds

*****
* A new version of KAPE is available! Please use Get-KAPEUpdate.ps1 *
* to get the latest version, 1.2.0.0, from the server. *
*****

C:\Program Files\Atola Insight Forensic_5_3>"C:\Program Files\OSFMount\OSFMount.com" -d -m Z:
Notifying applications...
Flushing file buffers...
Locking volume...
Dismounting filesystem...
Removing device...
Removing mountpoint...
Done.
```

## Imaging Cheat Sheet

### When source drive is damaged

Use these imaging settings and follow the recommendations to cope with severely damaged drives.

#### 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

### **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 Insight's advanced imaging features, e.g. reverse imaging or manual jumps.

### **USB drive read errors**

Use high-quality short USB3 cables. Longer or lower-quality USB3 cables can produce read errors during imaging.

### **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.

### **Effective error handling rule**

For particularly unstable drives, go to Error Handling tab and add a rule:

- Consecutive errors: 10
- Action: Change imaging direction

### **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 Automatic Checkup detects a damaged or degraded head, disable the head in the imaging settings for the initial imaging session.

Read more here: [Imaging Drives with Damaged Heads](#)

## Last imaging pass explained

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 to network, 10Gbit network connection is highly recommended.

### All sectors with metadata

All files contain file data and metadata. Partitions store metadata in specific structures, e.g MFT for NTFS. Metadata includes file name, access/modification datetimes, size, etc.

Imaging all sectors with metadata allows opening the full directory tree including files, without data within them.

Then you can open File Recovery and create an imaging session for specific files you need.

Example: pictures, videos, documents.

### Disable Artifact Finder

If artifact search has been enabled and the output is too large, it may slow down imaging. Try this:

1. Pause imaging
2. Add a new imaging session
3. Disable some or all Artifacts
4. Resume the session

### Change imaging pass timeout on-the-fly

Changing timeout is available only when you create a new session:

1. Pause the currently running imaging ('Pause' button)
2. Click 'Add New Session' link
3. Open imaging settings and change timeout of the last pass
4. Resume the imaging session

Important: The resumed imaging session will complement the data imaged prior to the pause with only the sectors that were not yet copied.

### Use Media Map Manager

When imaging selected files, speed can be low due to a high fragmentation of sectors which belong to the files.

1. Select files and click 'Image checked'
2. Click 'Edit this map'
3. View the fragmented blocks in LBA ranges
4. Click 'Add range'

5. New LBA range will appear at the end of the list
6. Change Start and End LBA of the new range to include most of LBA ranges above

## Segmented Hashing

Segmented hashing is no longer a new hashing concept. It was introduced by Atola Technology in November 2016 and has since been successfully utilized by thousands of investigators. Segmented hashing enables the hashing of damaged source drives and prevents losing a target image if part of the data gets corrupted. This hashing method can be used during multipass imaging of damaged drives.

## How is segmented hashing different from regular hashing?

With regular hashing, you get a single hash for the entire image.

With segmented hashing, you end up with 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.

Segmented hashes are saved in a CSV file in this format:

*Hash,start LBA,end LBA*

Example:

```
75c92419e86ce82734ef3bbb781e6602 ,0,8388608  
e2c7fc5264bae820e46c50b0502236d3 ,8388609,16777216  
42718e48b5adb59563c98727cbce0619 ,16777217,25165824  
... And so on until the last LBA.
```

## Segmented hashes for multipass imaging

Conventional hashing methods don't work when imaging an evidence device in a non-linear way, which means no proper hash calculation is possible when imaging damaged evidence drives.

Segmented hashing allows the use of multiple passes and more efficient handling of damaged drives while hashing all the good areas. Hashes are calculated only for the imaged areas, while all bad sectors are excluded from the calculation.

## Better resiliency

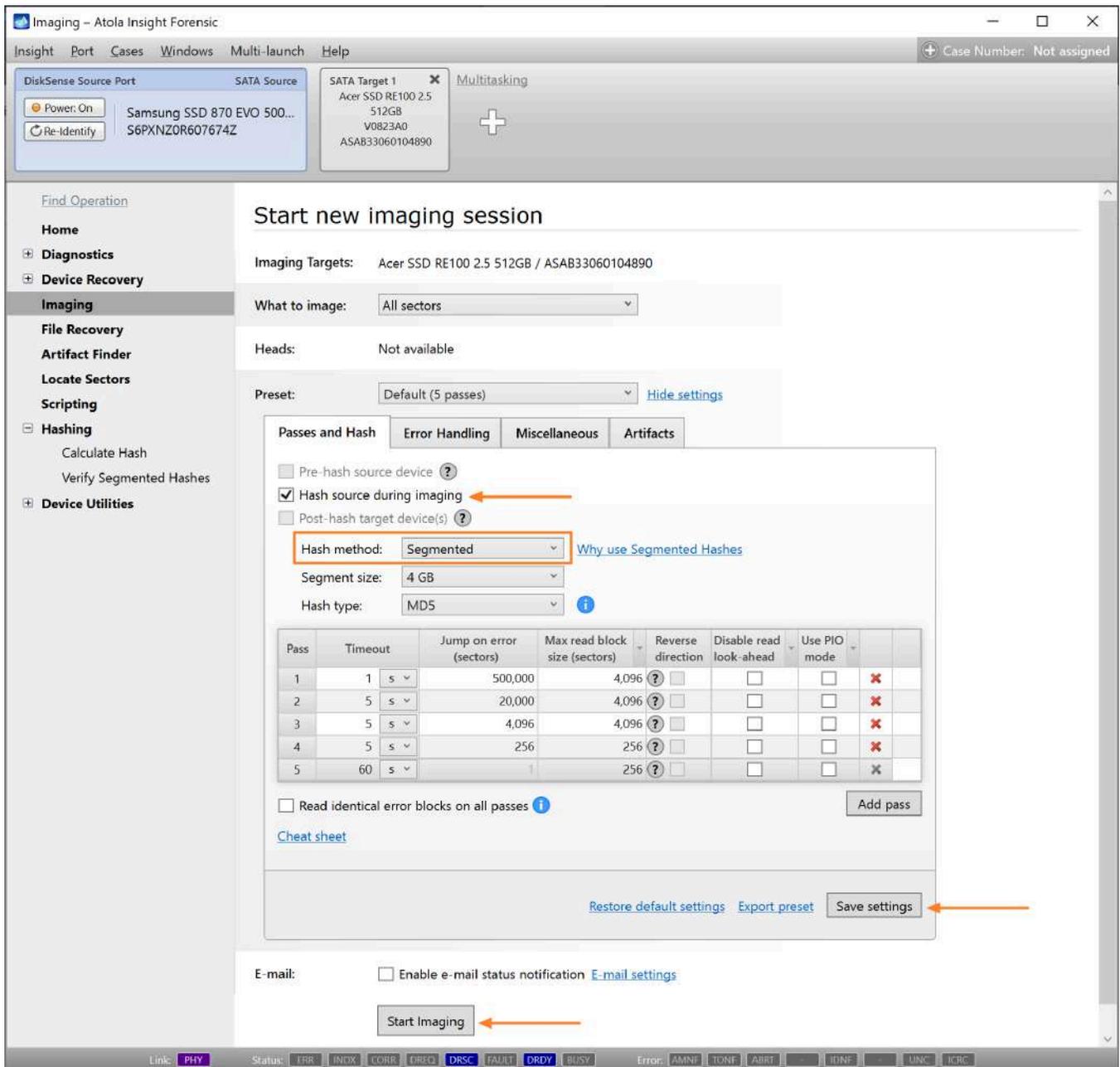
Another reason to use segmented hashes is to ensure better resiliency against data corruption in the image.

If your acquired evidence image gets damaged in the future, with a regular linear hash you will get a hash mismatch upon verification, and the entire image will become useless. With segmented hashes, only the hash for one segment in the set will become invalid.

## Image with segmented hashing

To enable segmented hashing for an imaging session, do the following:

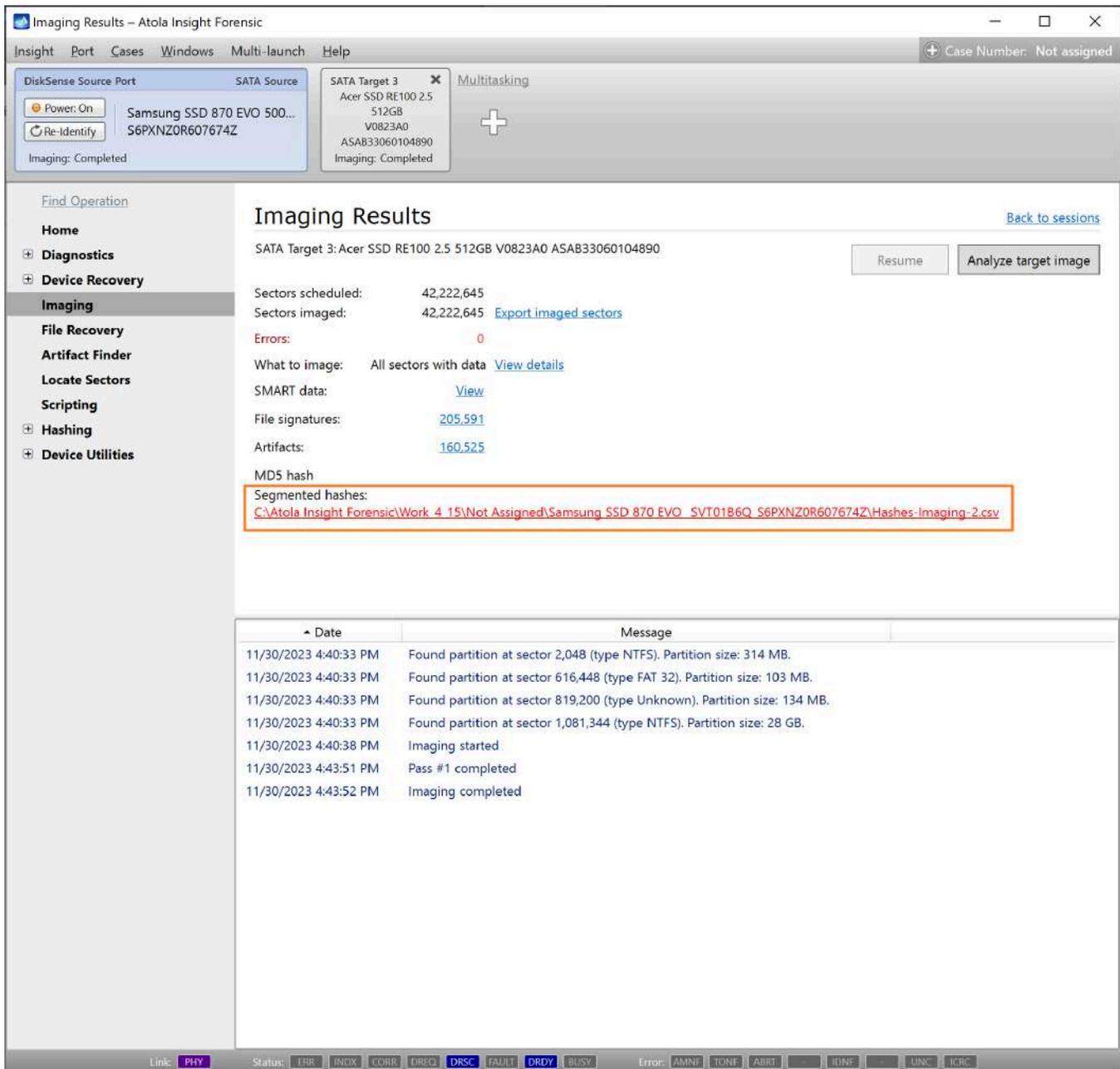
1. Go to **Imaging > Create New Session**.
2. In the **Preset** section, click the **Show settings** link.
3. On the **Passes and Hash** tab, enable **Hash source during imaging**.
4. Set the **Hash method** to **Segmented**.
5. Adjust other imaging parameters as needed and click **Save settings**.
6. Click **Start imaging**.



Segmented hashes are saved in a CSV file in "*Hash,start LBA,end LBA*" format:

	A	B	C
1	f7bf70a5334d2c89a446a8e19d51a1a0	0	8388607
2	6dee83f1113df428376a527e05aa1025	8388608	16777215
3	bd545f75d2105b70ebf8bf77e6646cbf	16777216	25165823
4	4b37dc251e944ffe07f55541c4bc2e87	25165824	33554431
5	cd8132c1a6519cf86581b87d1739468f	33554432	41943039
6	3ac718b7bf24a1e2e2c8e4f7e8f958fa	41943040	50331647
7	bd46b112052cbca1c11e11c0bc002bec	50331648	58720255
8	f5202708a3403fc12f0bcaacd94c2068	58720256	67108863
9	45a0fdd5d10a3bad3052b699dde12b48	67108864	75497471
10	8352fd4e1b91518746a25a9f1ea86040	75497472	83886079
11	757969d60ff8f2b98ed846dd2cc592fa	83886080	92274687
12	9ad7e94836a35b9b8bbc5fb53464cbdf	92274688	100663295
13	4c7241d3fc54e7b92c0e68b434c46d04	100663296	109051903
14	53ad24d1f14a680867b4c522c298124b	109051904	117440511
15	42bad2c897a8545c51a799944570c7b0	117440512	125829119
16	e71763cb053b96b0295fb8c482e86b32	125829120	134217727
17	144d2c8bd01f1faf80509bb33e04193e	134217728	142606335
18	c5193c7b808fcb7239c0ef2fcf5b672c	142606336	150994943
19	d068ad53d97ab03f6ad17d0c1412e70a	150994944	159383551
20	3dd6266ae3154dff290a3845495bccd7	159383552	167772159
21	004294e4fdab1a07b0bcbf78b8f4a67b	167772160	176160767
22	46b5d924925e8d150eaf6d3055e01dc1	176160768	184549375
23	3f0c00c4e931807eca7b5ad5eef2e1e5	184549376	192937983
24	d36b480b5cbd0c16fb53f1a23db4dc5f	192937984	201326591
25	045f7a61c38479f497c7e570572ebf19	201326592	209715199
26	95c625def63c33608e0dae9db3e59b8f	209715200	218103807
27	6d3c5057c90b5c0cf50cac80f77035be	218103808	226492415
28	98aaad3e787bd5d0bbec576825b33209	226492416	234441647
29			

A link to the file with segmented hashes is included in the Imaging Results report.



## Verifying images of damaged drives with segmented hashing

Unlike the conventional linear hashing, segmented hashing produces not a single hash, but a list of hashes of corresponding LBA ranges of the image saved into a CSV file in this format:

*Hash, start LBA, end LBA*

By validating all hashes on the list, you can prove that the entire image has not been modified. For more information about this hashing method, see [Segmented Hashing](#).

While this method of hashing has a number of benefits for forensic specialists, among its strongest advantages is its applicability to damaged drives.

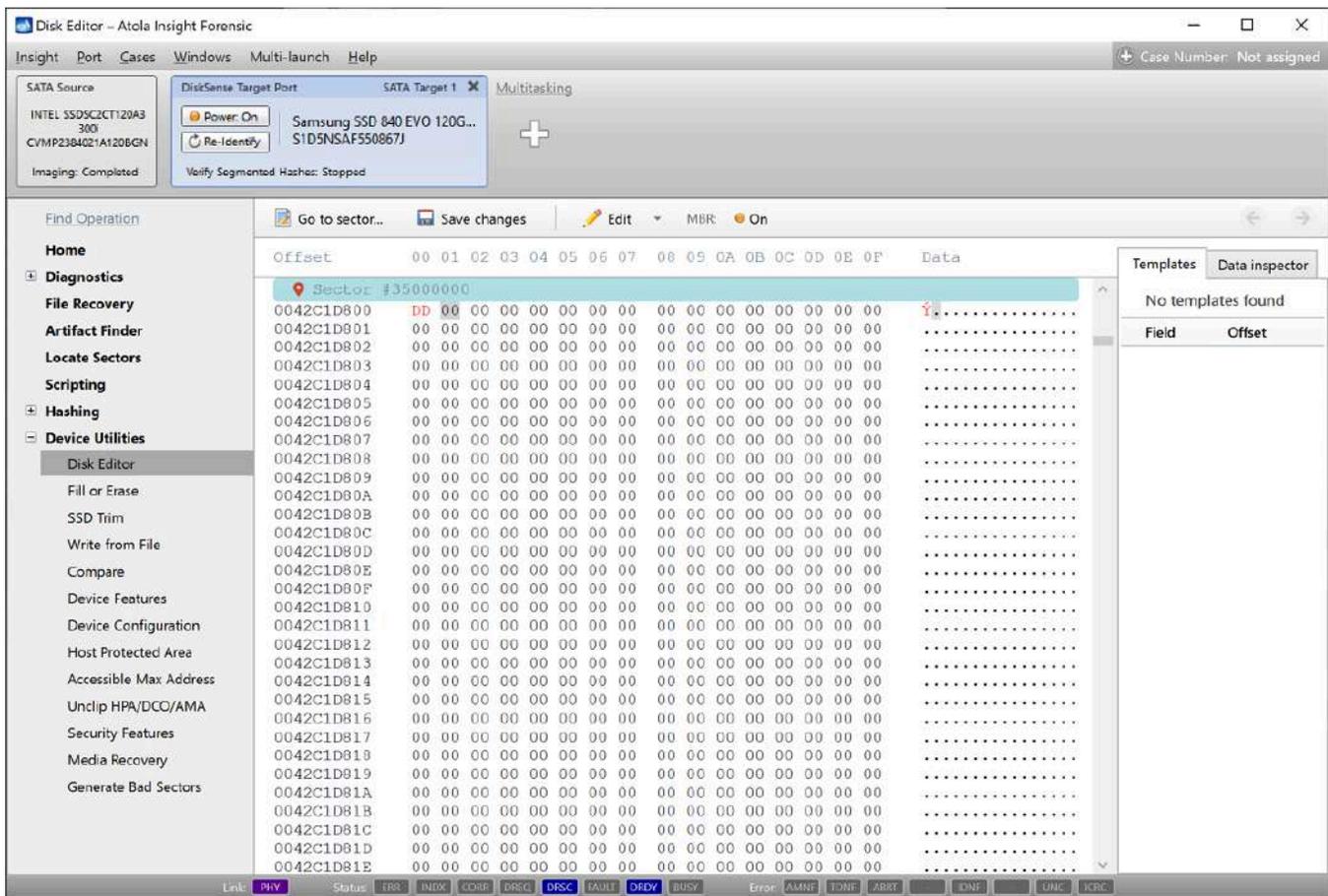
For one, this non-linear hashing method allows calculating hashes of the good areas of evidence media, while bad areas that are impossible to read and image, are left out of the calculation.

Secondly, if your 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, whereas with segmented hashes only the hash of the damaged segment will become invalid. For example, in the case of a 4TB hard drive, if the default 4GB segment size is applied, one invalid hash will account for only 0.1% of the drive, while the remaining 99.9% of hashes can still be verified.

## Verifying segmented hashes

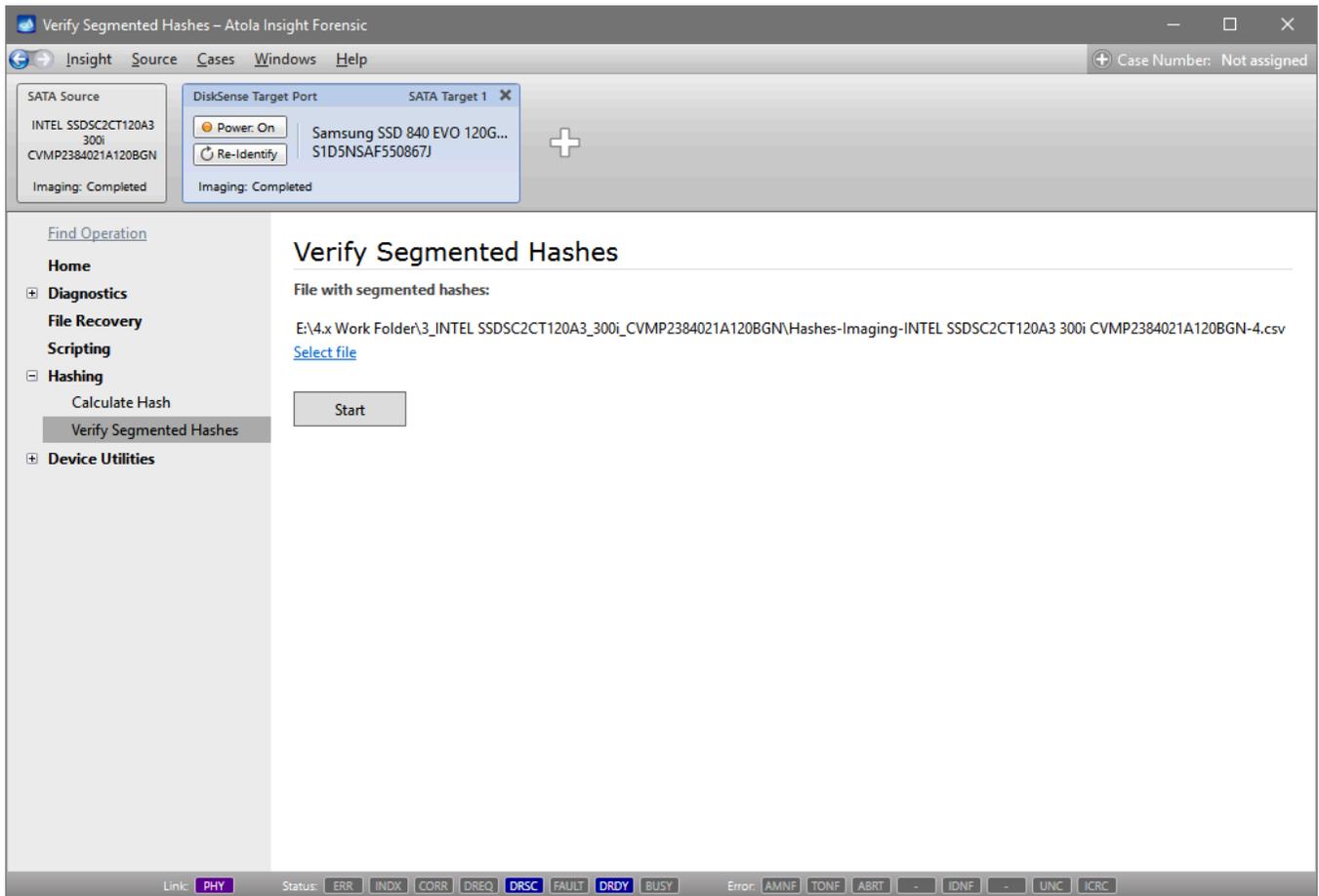
For instance, you have imaged a source drive and calculated its segmented hashes, the CSV file is stored on your computer. Now let's simulate a change of the evidence image to see how Segmented hashing helps us identify the areas, whose integrity has not been compromised.

**Step 1.** In the top **Device panel**, select the target image. In the sidebar, go to **Device Utilities > Disk Editor**. Click **Go to sector** and enter *35,000,000*. Change one byte in this sector and click **Save changes**.



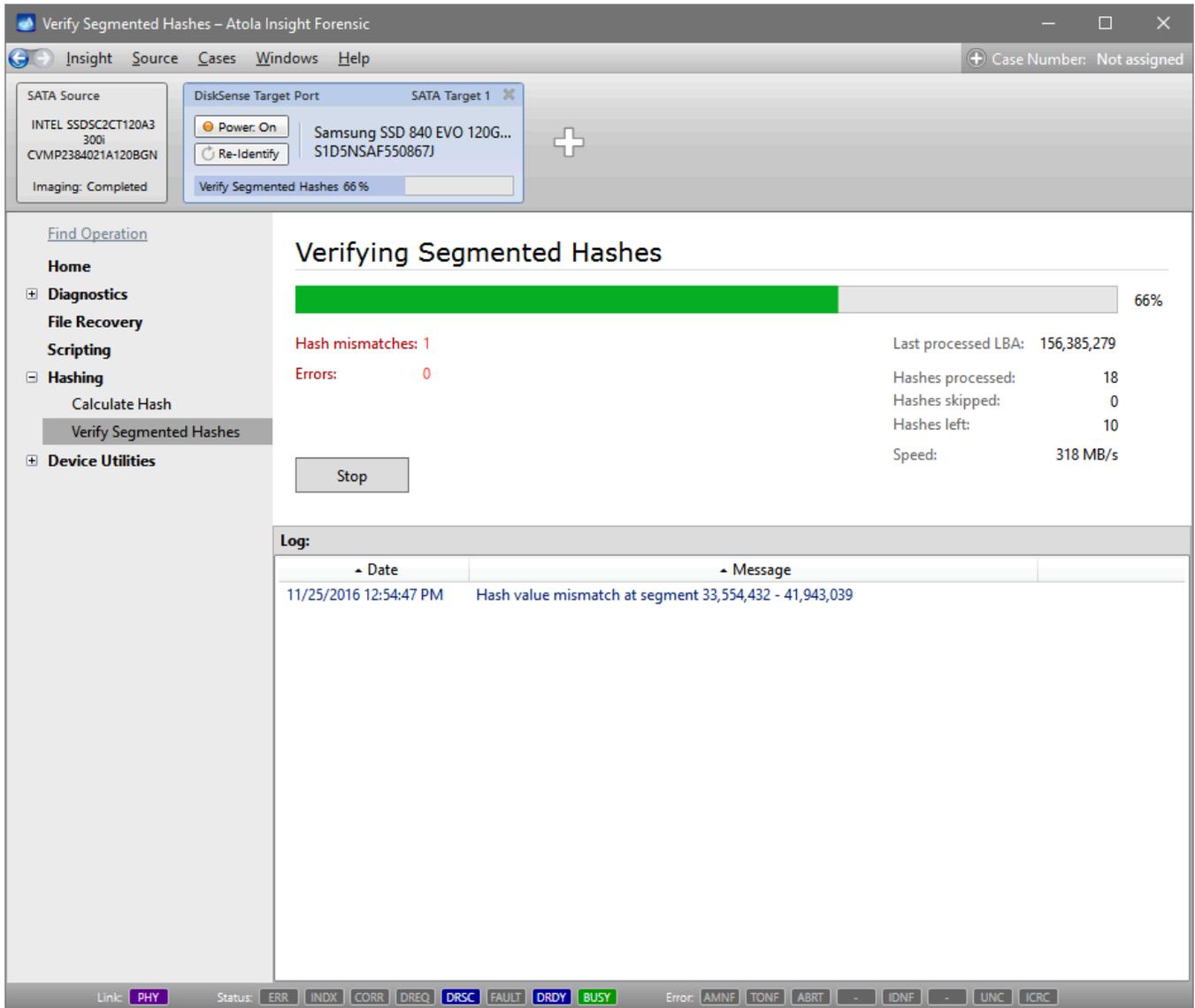
### Changing one byte in Disk Editor

**Step 2.** In the sidebar, go to **Hashing > Verify Segmented Hashes**. This is an automated way to verify the segmented hashes in an existing CSV file against the target image. Select the file with segmented hashes calculated during imaging and click **Start**.



## Hash verification

**Step 3.** Hash verification is in progress. Here we see 18 segmented hashes checked. Hash for the interval that includes sector 35,000,000 is invalid.



### Segmented hash verification in progress

Step 4. Hash verification finishes with the proper case report automatically created, also in CSV format.

Report: Verify Segmented Hashes

Print... Save to file... Copy to Clipboard

Friday, November 25, 2016 12:59 PM  
Report created by Atola Insight Forensic 4.7.6173.21925.

## Verify Segmented Hashes

Device model:	Samsung SSD 840 EVO 120GB	Unit IP:	10.0.0.77
Device serial:	S1D5NSAF550867J	Unit serial:	4444
Device firmware:	EXT0BB6Q	Write protection:	On
Device size:	120 GB (120,034,123,776 bytes)	Computer:	VITALIY
Case number:	Not assigned	User:	Vitaliy
Case description:		OS:	64-bit Windows 10 Pro Version 6.2 (Build: 10586)

Last processed LBA: 234,441,647

Hashes processed: 28  
Hashes skipped: 0

Hashes in file: 28  
Hashes left: 0

Hash mismatches: 1  
Errors: 0

Segmented hashes: [E:\4.x Work Folder\Not Assigned\Samsung SSD 840 EVO 120GB EXT0BB6Q S1D5NSAF550867J\Hashes-Imaging-INTEL SSDSC2CT120A3 300i CVMP2384021A120BGN-40.csv](#)

Log file: [E:\4.x Work Folder\Not Assigned\Samsung SSD 840 EVO 120GB EXT0BB6Q S1D5NSAF550867J\VerifyMultipleSegments1.csv](#)

### Log

Date	Message
11/25/2016 12:54:47	Hash value mismatch at segment 33,554,432 - 41,943,039

9 / 9

Close

### Segmented hash verification report

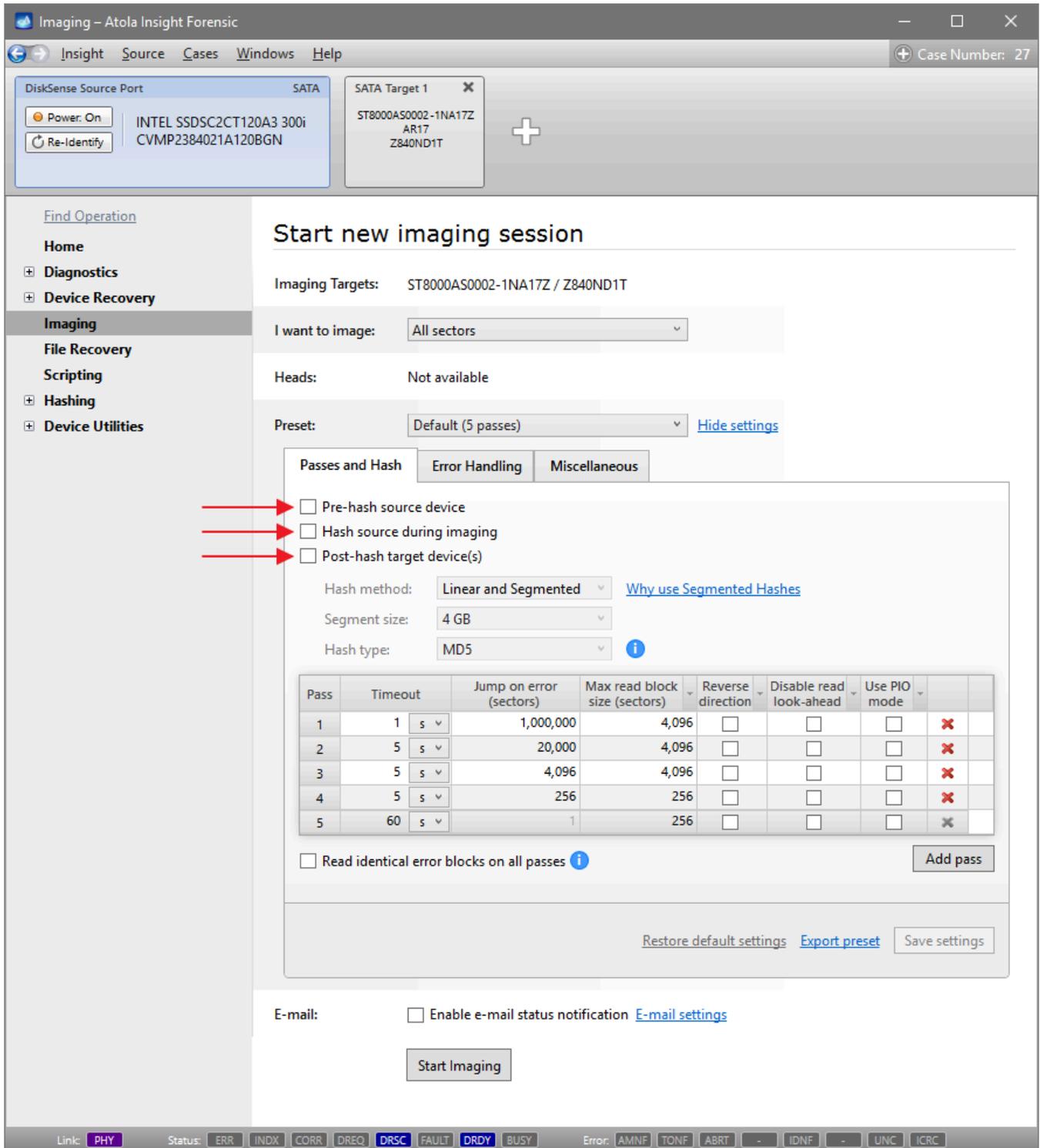
This is how segmented hashing helps you avoid the whole image being compromised when a small area of the evidence target is damaged.

## Calculating hash during imaging

Atola Insight Forensic supports hash calculation of both source and target devices in conjunction with imaging. We have developed highly flexible functionality to help optimize evidence acquisition process to fit one's internal procedures as well as avoid causing further damage to fragile media.

To view the hashing options:

1. In the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. Select the target device or file.
4. In **Preset** line, click the **Show settings** link.
5. In the upper part of the **Passes and Hash** tab there are three checkboxes:
  - o Pre-hash source device.
  - o Hash source during imaging.
  - o Post-hash target device(s).



## Imaging results with segmented hashes

Multiselect is available, which allows an operator to use all three of these options.

However, **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.

On the contrary, **Hash source during imaging** is the most appropriate way to calculate the hash of a fragile source evidence drive. In this case, Insight 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. Therefore ticking **Hash source during imaging** checkbox and selecting **Linear** or combined **Linear and Segmented** option in the **Hashing method** list leads the number of passes to be limited to one. When dealing with a damaged drive, we strongly recommend using **Segmented hashing**, as this method supports multipass imaging and handling of bad sectors and provides better resiliency against data corruption. For more details, see [Segmented hashing](#).

**Post-hash target device(s)** option allows to properly record the calculated hash in the case. Since this operation does not require reading the source drive, it is safe to use this option while imaging either good or damaged drives.

**Imaging Results**

SATA Target 1: ST8000AS0002-1NA17Z / Z840ND1T

Sectors scheduled: 976,773,168  
Sectors imaged: 976,773,165 [Export imaged sectors](#) | [Export non-imaged sectors](#)

Errors: [Export sectors with errors](#)

Copy range: All sectors  
Start sector in range: 0  
End sector in range: 976,773,167  
SMART data: [View](#)  
File signatures: [0](#)

MD5 hash: 02250b77fbc87294055e61e1a39a2927  
Calculated range: 0 - 976,773,167  
Segmented hashes: [C:\Atola Insight Forensic\Work\672\\_WDC\\_WD5000AAKX-001C40\\_15.01H15\\_WD-WMAVU2595458\Hashes-Imaging-WDC\\_WD5000AAKX-001C40\\_15.01H15\\_WD-WMAVU2595458-0.csv](#)

Post-hash for ST8000AS0002-1NA17Z AR17 Z840ND1T  
MD5 hash: 02250b77fbc87294055e61e1a39a2927  
Calculated range: 0 - 976,773,167  
Segmented hashes: [C:\Atola Insight Forensic\Work\Not Assigned\ST8000AS0002-1NA17Z AR17 Z840ND1T\Hashes-ST8000AS0002-1NA17Z AR17 Z840ND1T-2.csv](#)

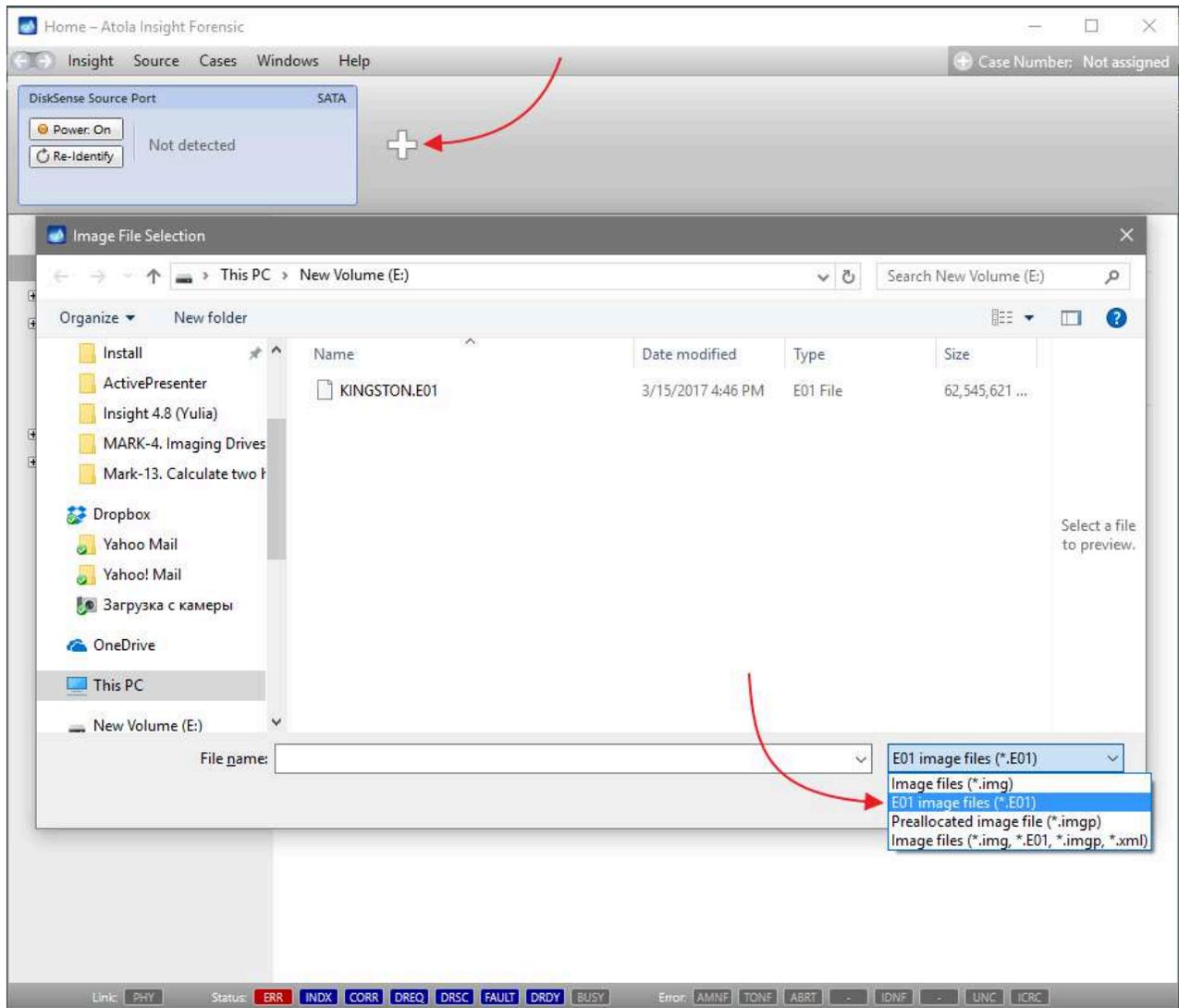
Date	Message
4/7/2017 2:43:28 PM	Imaging started
4/7/2017 3:01:38 PM	Cannot read block of data at 259,000,000 - 259,000,002 (Error: UNC)
4/7/2017 4:03:32 PM	Pass #1 completed
4/7/2017 4:05:32 PM	Imaging completed

## Calculating MD5 and SHA1 hashes of an existing E01 file

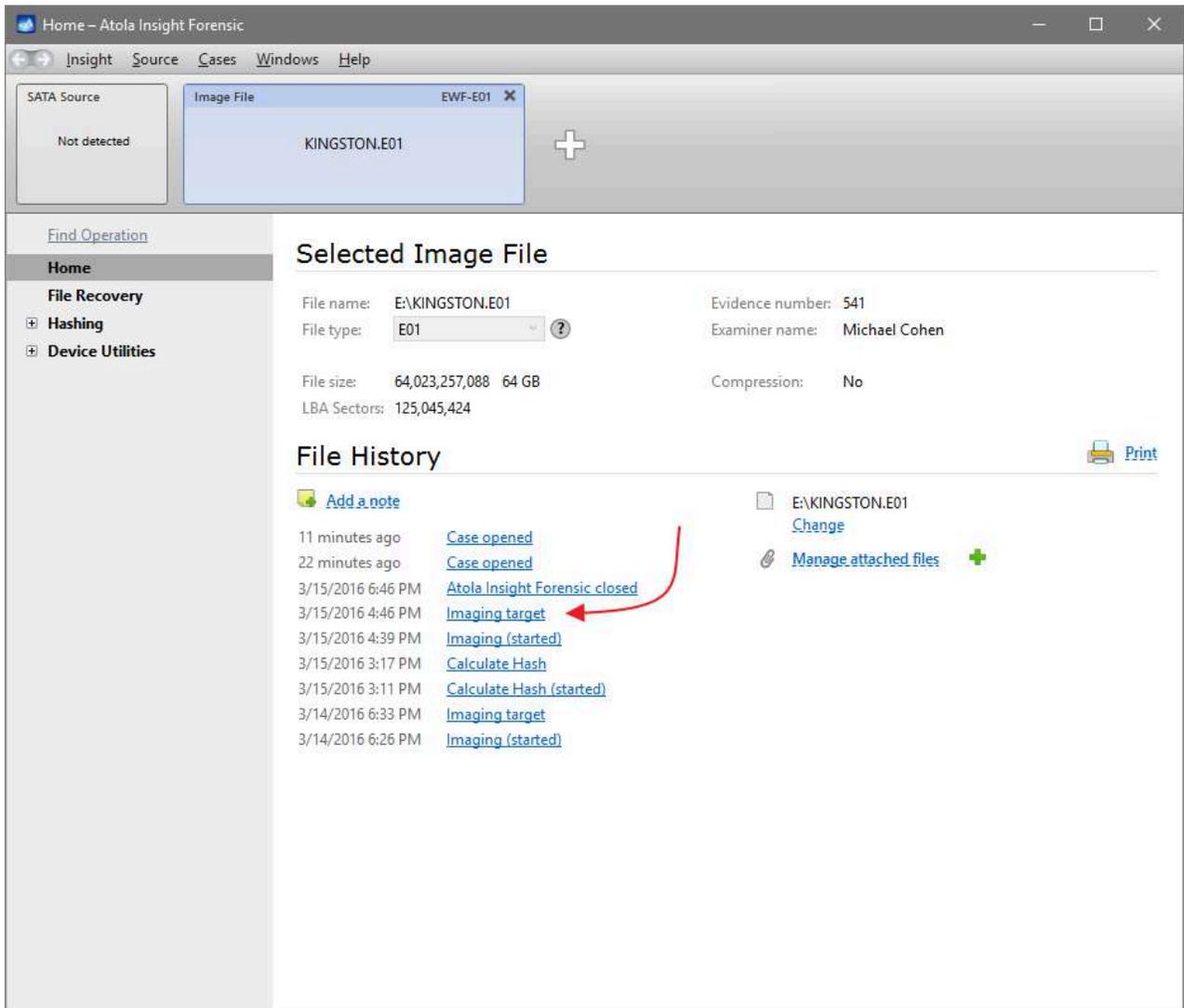
Over the years, E01 file format has become a popular format for forensic purposes due to its ability to store not only the physical or logical copy of the source drive, but also case and evidence details. E01 file can also contain both MD5 and SHA-1 hashes. And it is considered a good practice among forensic specialists to calculate both hashes while imaging the evidence so that they are included in the E01 file.

To view the hash calculated for an E01 file with Atola Insight Forensic, do the following:

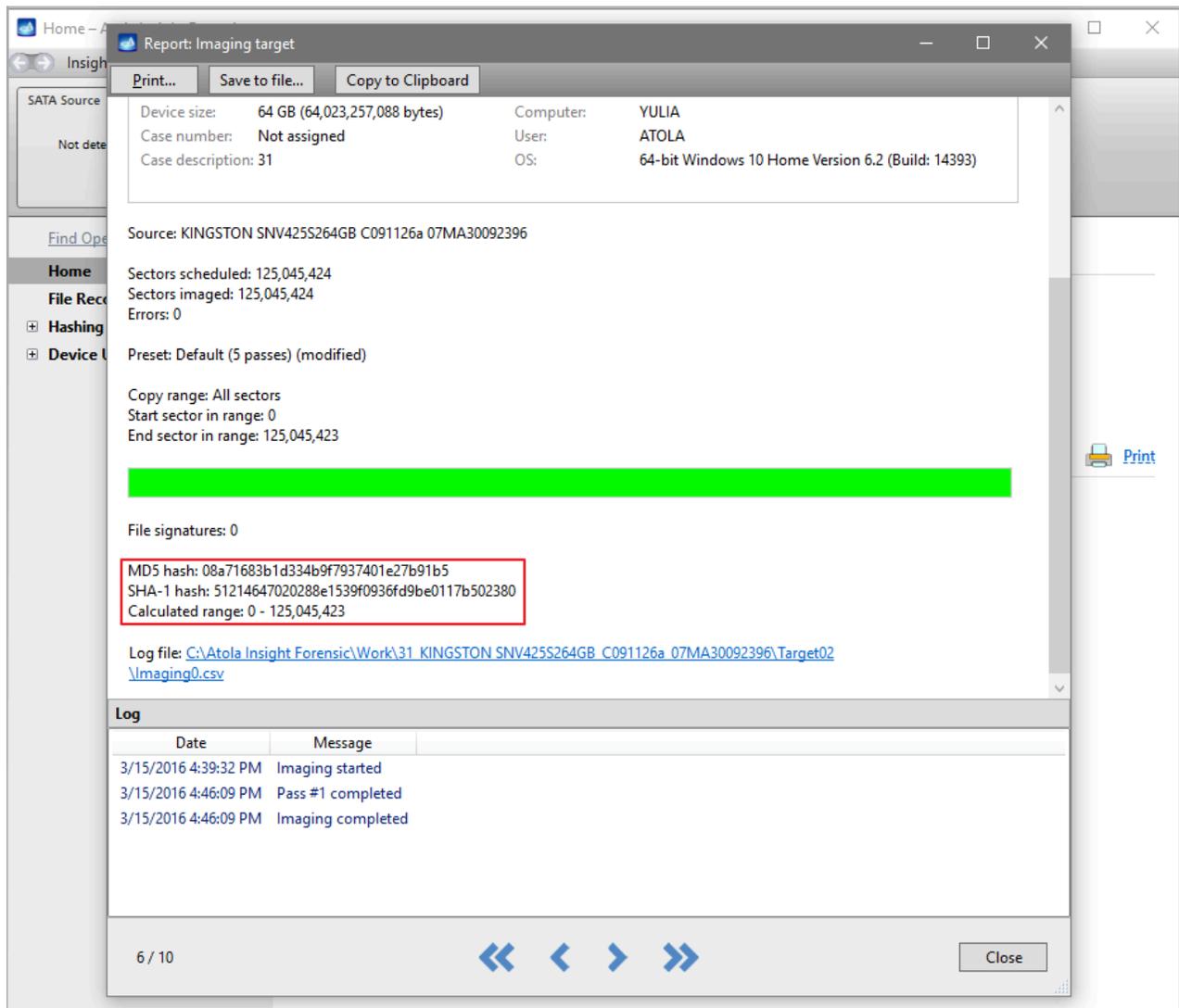
1. To open the file, press the **Plus** icon on the **Device panel** and then select the **E01 image files (\*.E01)** file extension in the drop-down menu to view existing files with this extension.



2. On the **Home** screen, look through the **File History** and click on the **Imaging target** link.

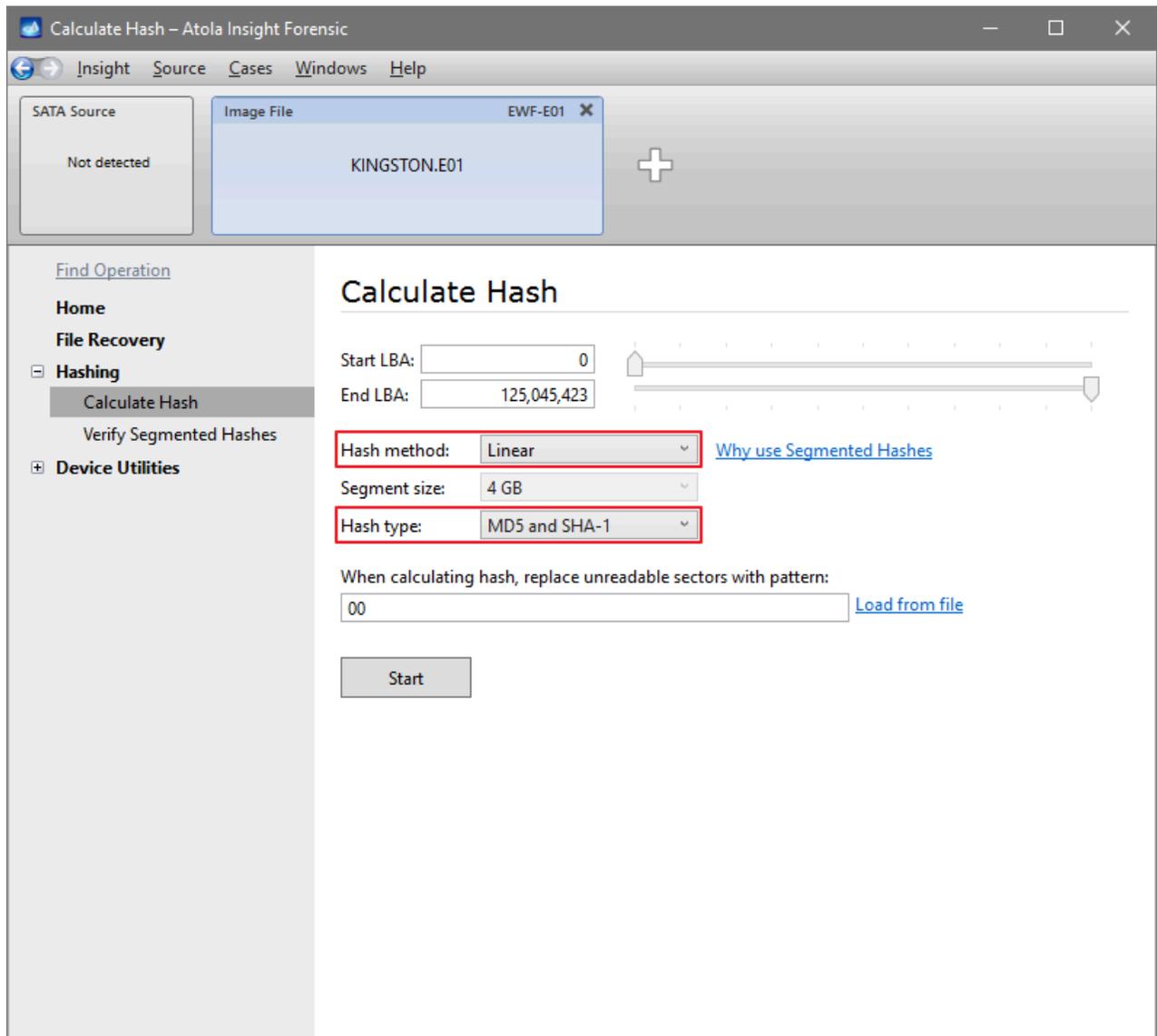


3. The **Imaging target** report opens. At the bottom the are both hashes calculated during the imaging session.



Leave this window open or save the report as a pdf file to compare the hash with the newly calculated one later.

4. In the sidebar, go to **Hashing > Calculate Hash**.
5. In the **Hash method** list, select **Linear**.
6. In the **Hash type** list, select **MD5 and SHA-1**.
7. Click **Start**.



8. Once the hashes are calculated, you can make sure that the two sets of hashes are identical.

The screenshot shows the 'Calculated Hash' window in Atola Insight Forensic. The window title is 'Calculated Hash - Atola Insight Forensic'. The interface includes a menu bar with 'Insight', 'Source', 'Cases', 'Windows', and 'Help'. On the left, there are tabs for 'SATA Source' (Not detected) and 'Image File' (KINGSTON.E01, EWF-E01). The 'Image File' tab shows 'Calculate Hash: Completed'. The main area displays the 'Calculated Hash' results for the 'KINGSTON.E01' image file. The hash method is 'Linear'. The calculated hashes are:

Hash method:	Linear
MD5	08a71683b1d334b9f7937401e27b91b5
SHA-1	51214647020288e1539f0936fd9be0117b502380

Additional information shown includes:

- Calculated range: 0 - 125,045,423
- Selected range: 0 - 125,045,423
- Sectors calculated: 125,045,424
- Errors: 0

An 'Error Log' section is visible at the bottom, with columns for 'Date' and 'Message'.

## Compare source and target to find modified data

So you have a Source evidence drive and its image on a different device, and you have a record that their hash values were identical in the past.

Imaging Results – Atola Insight Forensic

Case Number: 27

DiskSense Source Port: SATA

Power: On  
Re-Identify

INTEL SSDSC2CT120A3 300i  
CVMP2384021A120BGN

Post-Hashing Targets: Completed

SATA Target 1

INTEL SSDSC2CT120A3 300i  
CVMP3024006W120BGN

Calculate...: Complete

Find Operation

Home

- Diagnosics
- Device Recovery
- Imaging**
- File Recovery
- Scripting
- Hashing
- Device Utilities

## Imaging Results

[Back to sessions](#)

SATA Target 1: INTEL SSDSC2CT120A3 / CVMP3024006W120BGN Resume Analyze target image

Sectors scheduled: 234,441,648  
Sectors imaged: 234,441,648 [Export imaged sectors](#)

Errors: 0

Copy range: All sectors

Start sector in range: 0  
End sector in range: 234,441,647

SMART data: [View](#)

File signatures: [400,434](#)

MD5 hash: 1ffb74753e98207a48e194da1226bd8a  
Calculated range: 0 - 234,441,647

Post-hash for INTEL SSDSC2CT120A3 300i CVMP3024006W120BGN

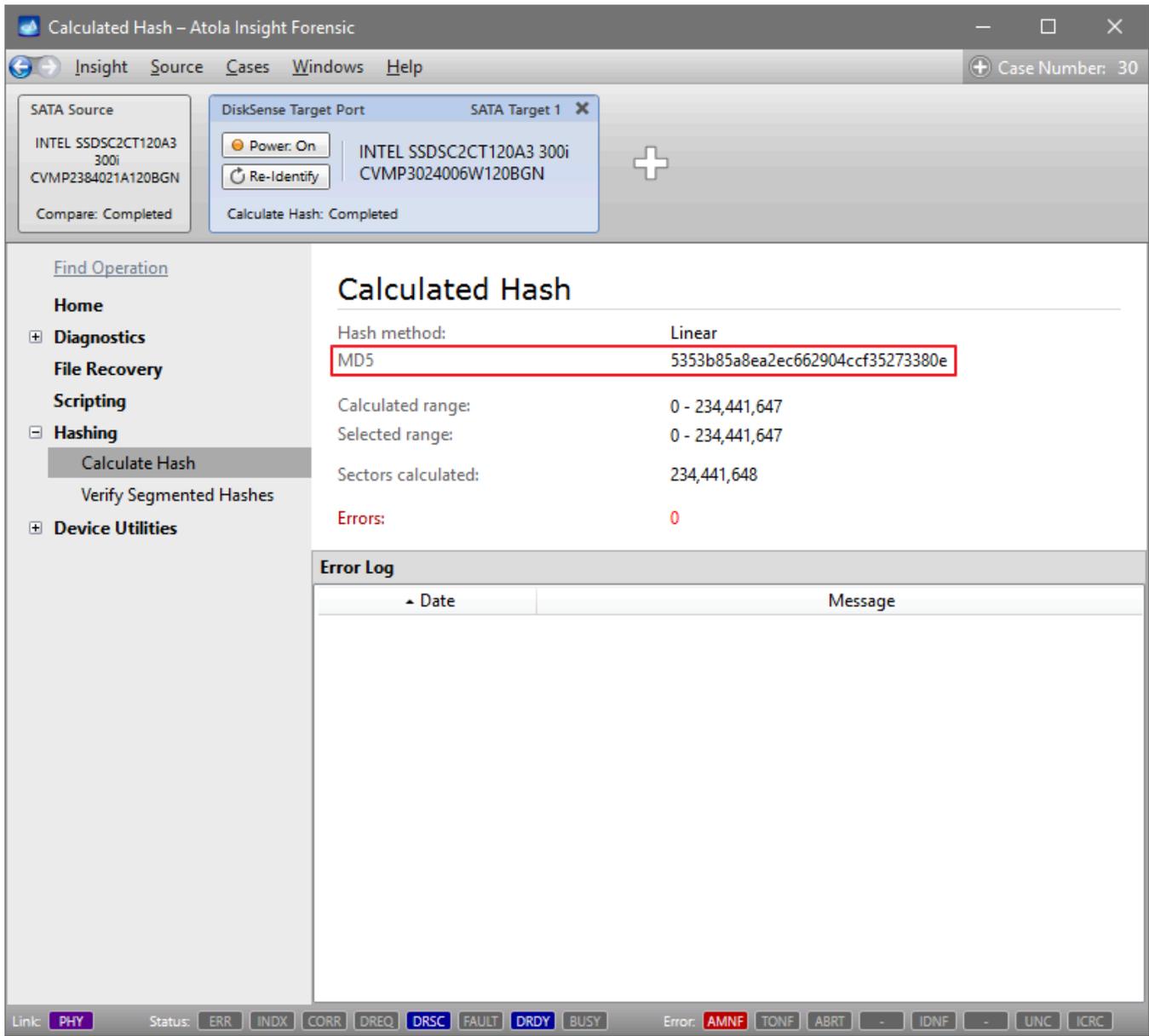
MD5 hash: 1ffb74753e98207a48e194da1226bd8a  
Calculated range: 0 - 234,441,647

Log

Date	Message
4/10/2015 4:44:57 PM	Imaging started
4/10/2015 4:51:10 PM	Pass #1 completed
4/10/2015 4:51:11 PM	Imaging completed

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

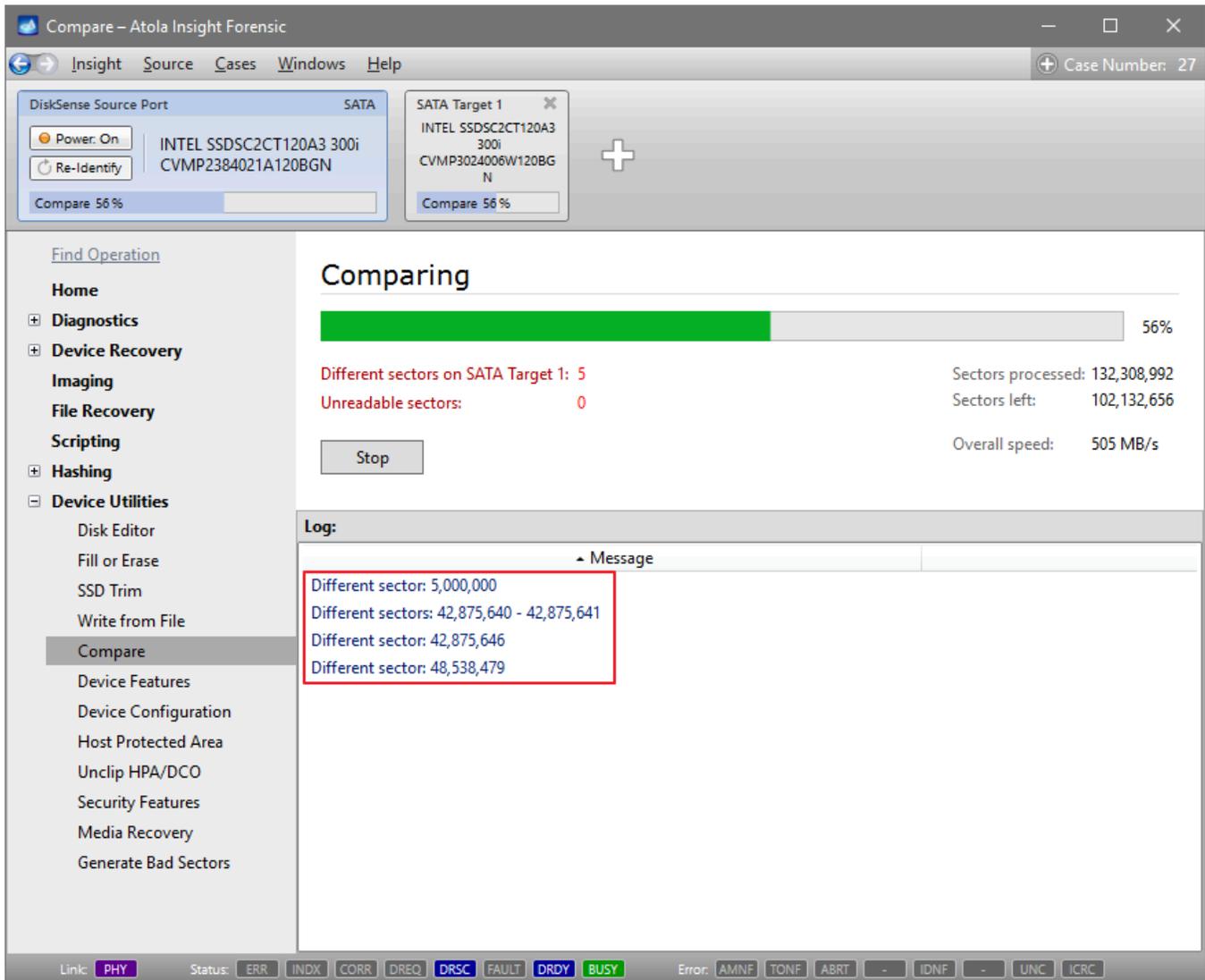
If you get a different hash value when you calculate the hash of the target now, it could be due to hardware failure, or because the device containing your image was used by a third party.



To understand how substantial these changes are, you may want to locate the sectors that have been modified.

1. In the sidebar, go to **Disk Utilities > Compare**.
2. Make sure that the whole range of sectors of the drive and radio button next to the **Device on DiskSense Target Port** option is selected.
3. Click **Compare**.

Insight's high-performance compare function compares the source and the target and helps you identify and locate the modified sectors:



## Hash lists to filter good & bad files

To quickly detect and mark known "good" or "bad" files in Atola Insight Forensic, you can [import lists of hashes](#) of known white or black files:

- **White hash** belongs to a known good file created by known software.
- **Black hash** indicates a known bad file, which could be malware, a hacking script, a hidden illicit data file and more.

You can then use the imported hash lists in the **File Recovery** module to analyze each calculated file hash and [filter files](#) based on which hash list they belong to.

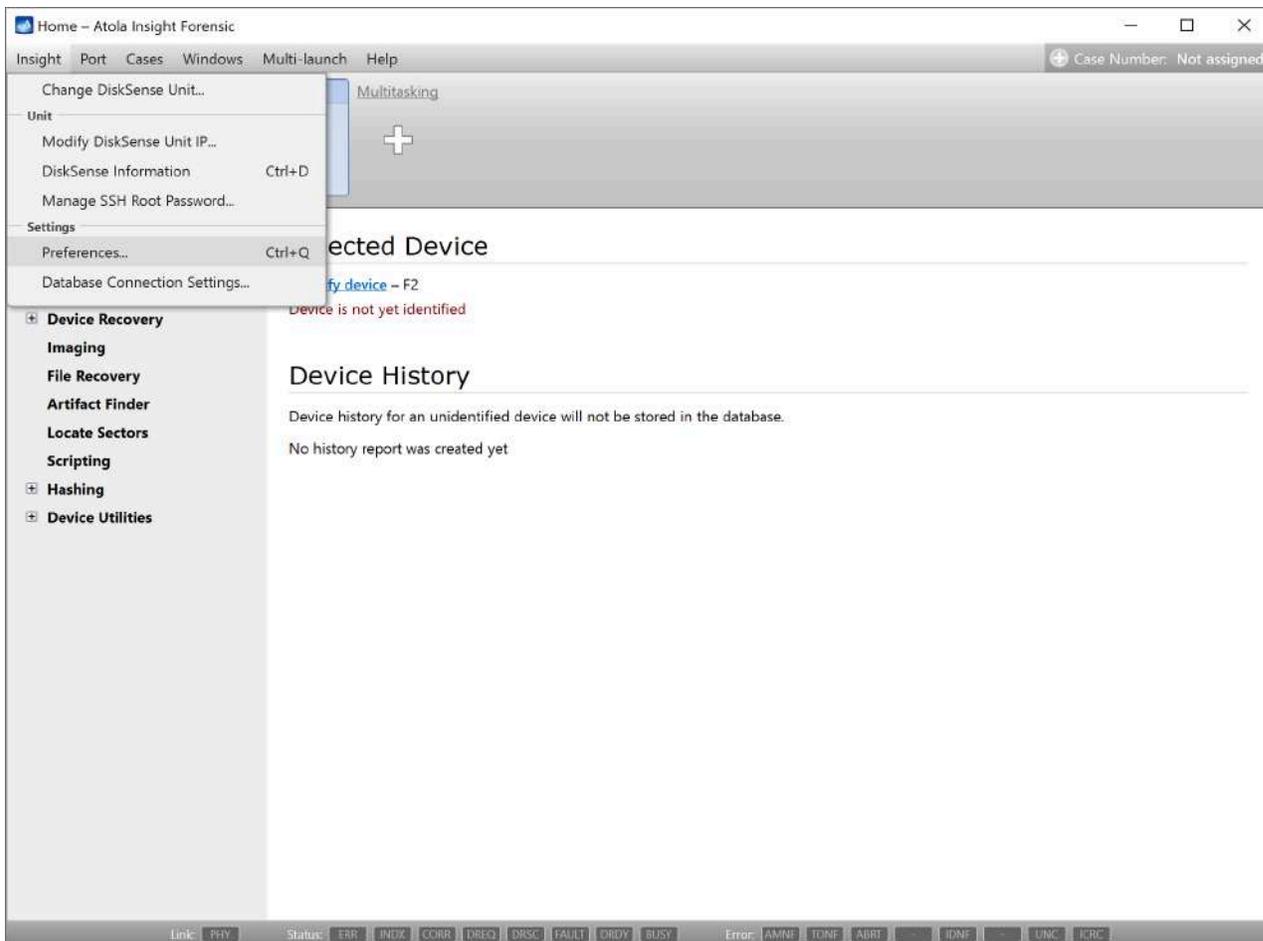
## Add a hash list

To import a hash list from a file, do the following:

1. Prepare a CSV or text file with a hash list, with one hash per line. For example, a file with two MD5 hashes looks like this:

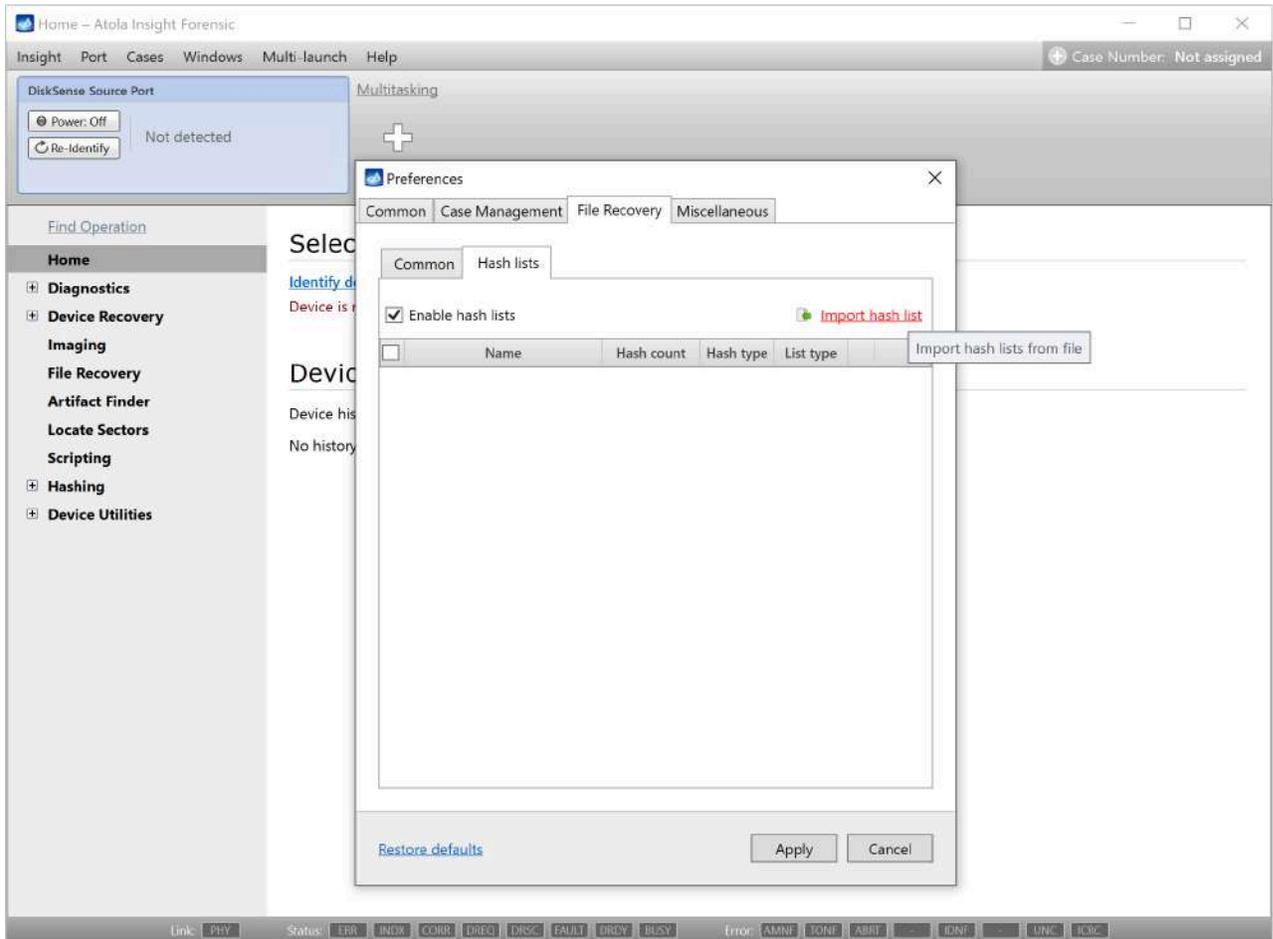
```
1777f831255b7f6fa5869acddc2e2c93
f6e0fcac265d3e139dd510be0eecb0b1
```

2. In the Insight Forensic menu bar, select **Insight > Preferences** or press **Ctrl + Q**.



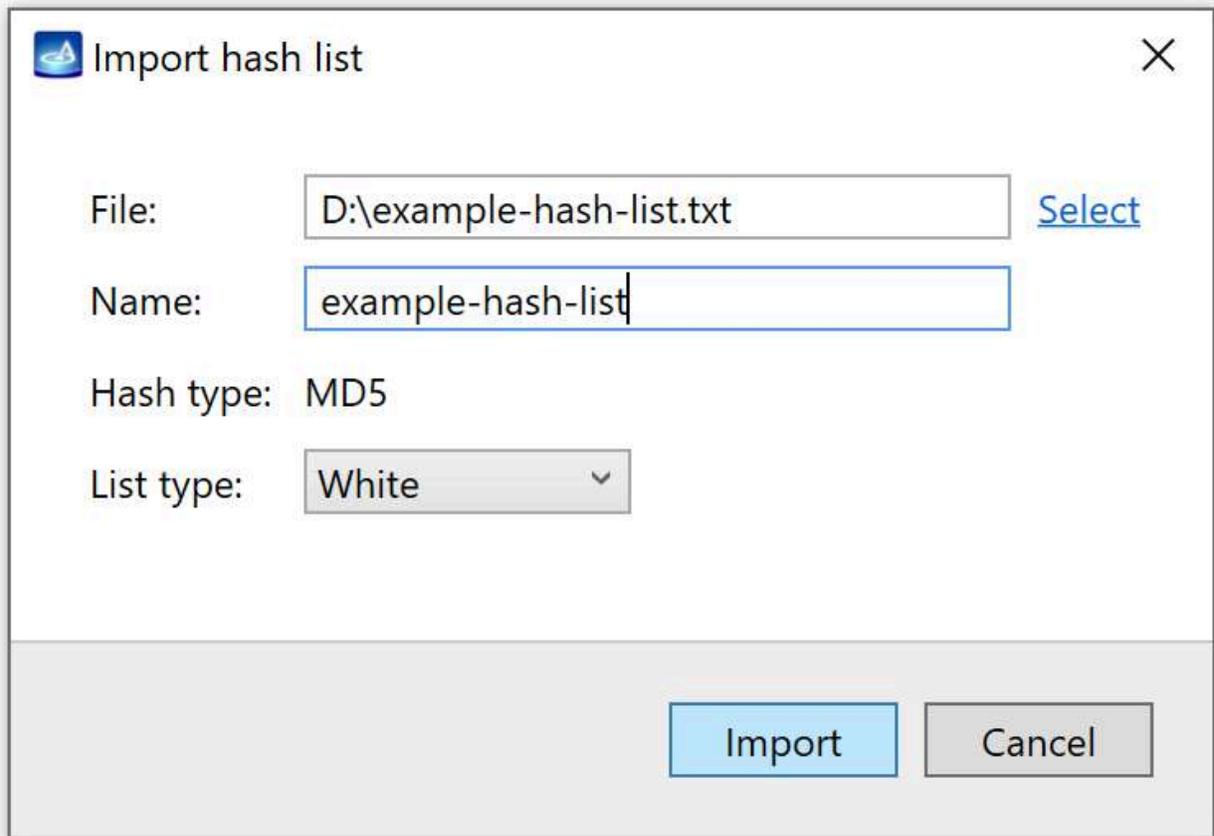
3. In the **Preferences** window, go to the **File Recovery** tab.

4. On the **Hash lists** subtab, click the **Import hash list** link.



5. In the **Import hash list** dialog, select the file with hashes, enter the hash list name, and select hash list type:

- **White** for hashes that belong to the known good files.
- **Black** for hashes of the known bad files, such as malware, hacking scripts, hidden illicit data files and more.



6. Click **Import**.

7. Click **Apply**.

## Filter files using hash lists

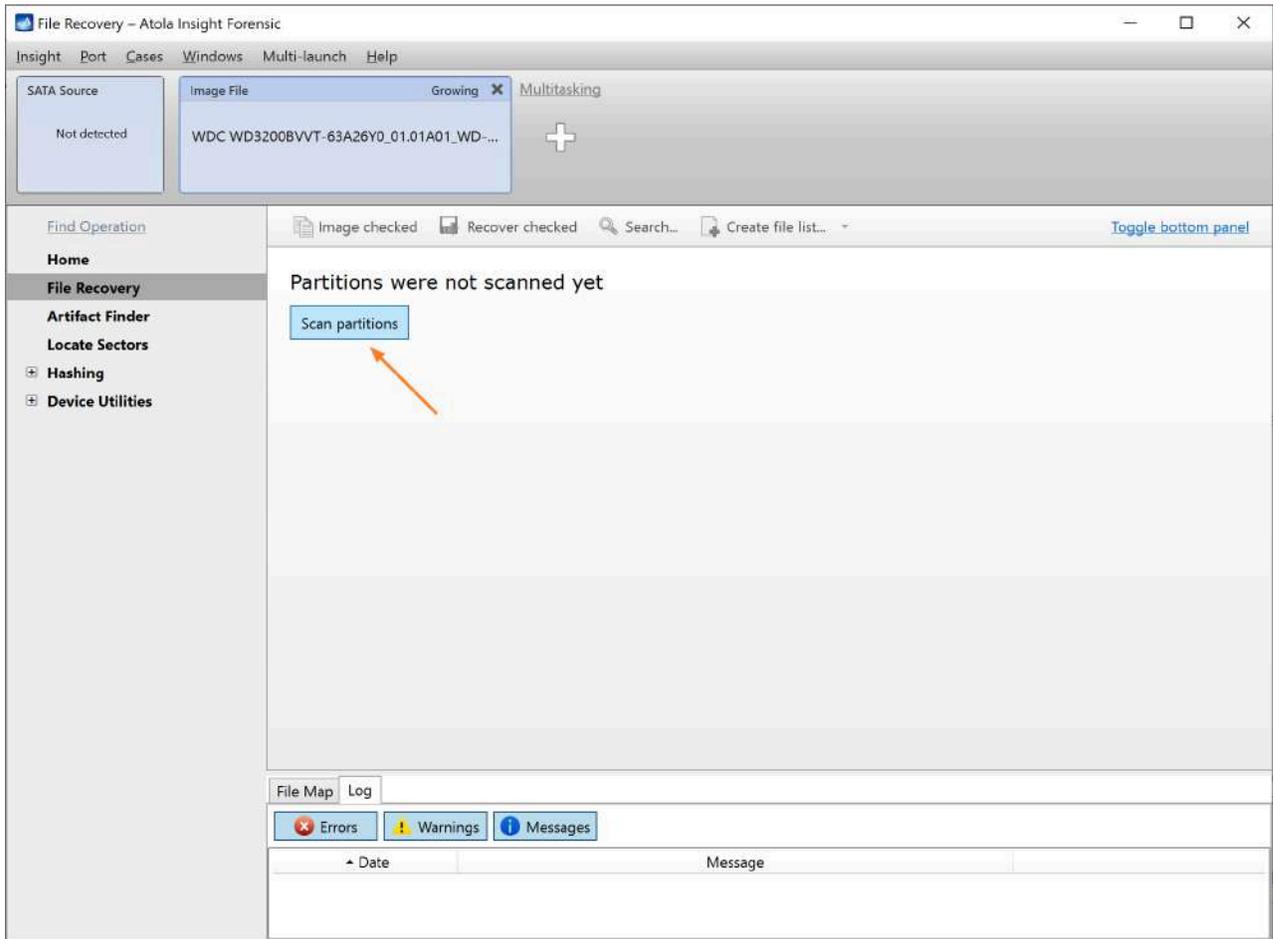
Once imaging of an evidence drive is finished, you can open its copy in the **File Recovery** module for a quick analysis. If the file hash belongs to the previously imported white or black hash list, Insight Forensic displays special marks on the left of file hash values:

- ✓ Checkmarks for the files found in the white hash list.
- ⚠ Warning triangles for the files found in the black hash list.

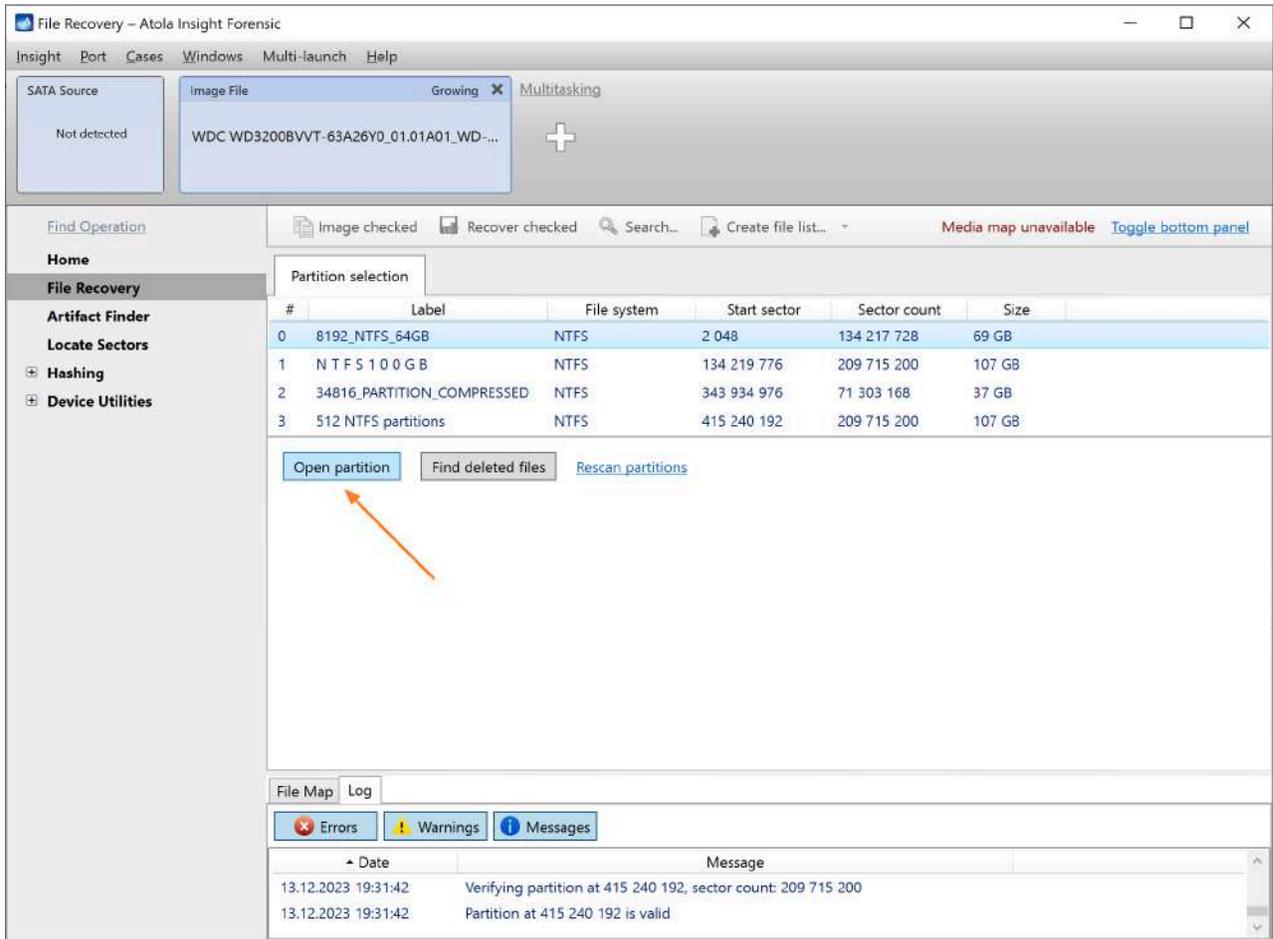
Name	Extension	Date modified	Size	Copied	MD5
<input type="checkbox"/>  \$RECYCLE.BIN		16.11.2018 16:05			
<input type="checkbox"/>  Insight_Firmware		16.11.2018 16:11			
<input type="checkbox"/>  Insight_Installatio		16.11.2018 16:12			
<input type="checkbox"/>  System Volume Ir		16.11.2018 16:01			
<input type="checkbox"/>  01Visa-UTF8	.txt	21.06.2017 12:56	19 B	—	✓ 191ba891b984d35391eb3552df2241c6
<input type="checkbox"/>  02Visa-ASCII	.dat	21.06.2017 12:59	19 B	—	✓ 97f85bdad254887254d60b55fd40ba1d
<input type="checkbox"/>  03Visa-UTF16BE	.dat	21.06.2017 13:01	40 B	—	✓ fa407fab41d382bcd756379132c471ee
<input type="checkbox"/>  04MC-UTF16LE	.dat	21.06.2017 13:02	40 B	—	⚠ 8a1dae71dfe6acb7a294f73714bf41f6
<input type="checkbox"/>  05MC-UTF8	.txt	21.06.2017 13:06	19 B	—	⚠ c59a757f679f3136d9361751ac2ab10c
<input type="checkbox"/>  06AE-UTF16	.dat	21.06.2017 13:06	38 B	—	⚠ f489e89d0dbeadac39ed044821995a0d
<input type="checkbox"/>  07AE-ASCII	.dat	21.06.2017 13:08	17 B	—	2654e55186eedde1b24c57e53f71bd0a
<input type="checkbox"/>  08AE-UTF16LE	.dat	21.06.2017 13:04	36 B	—	2da6b90c460b601fe5a1b30092fbd87c

The File Recovery engine can filter files on a target device based on the imported white and black hash lists. To display only the files, which have either white or black hashes, do the following:

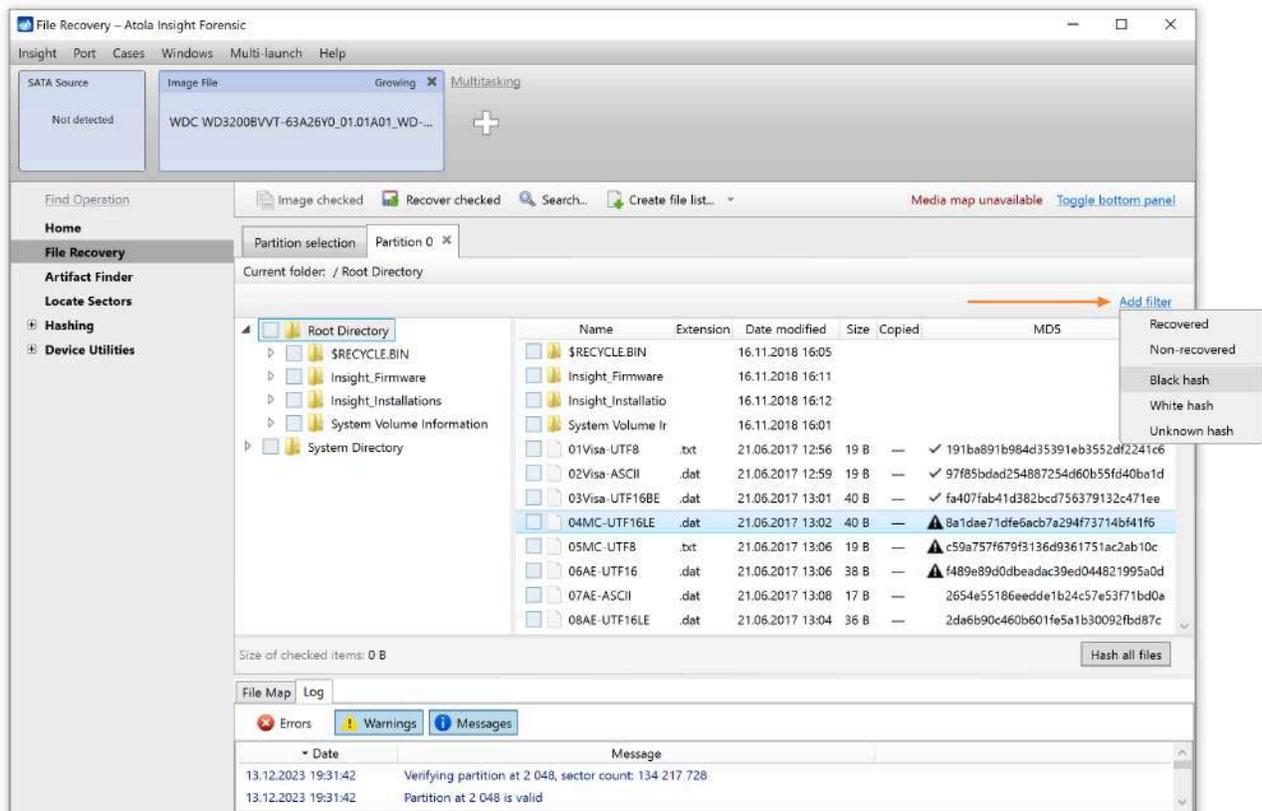
1. Select the **Target** port.
2. In the sidebar, click **File Recovery**.
3. Click the **Scan partitions** button.



4. On the **Partition selection** tab, choose the partition you want to examine and click **Open partition**.

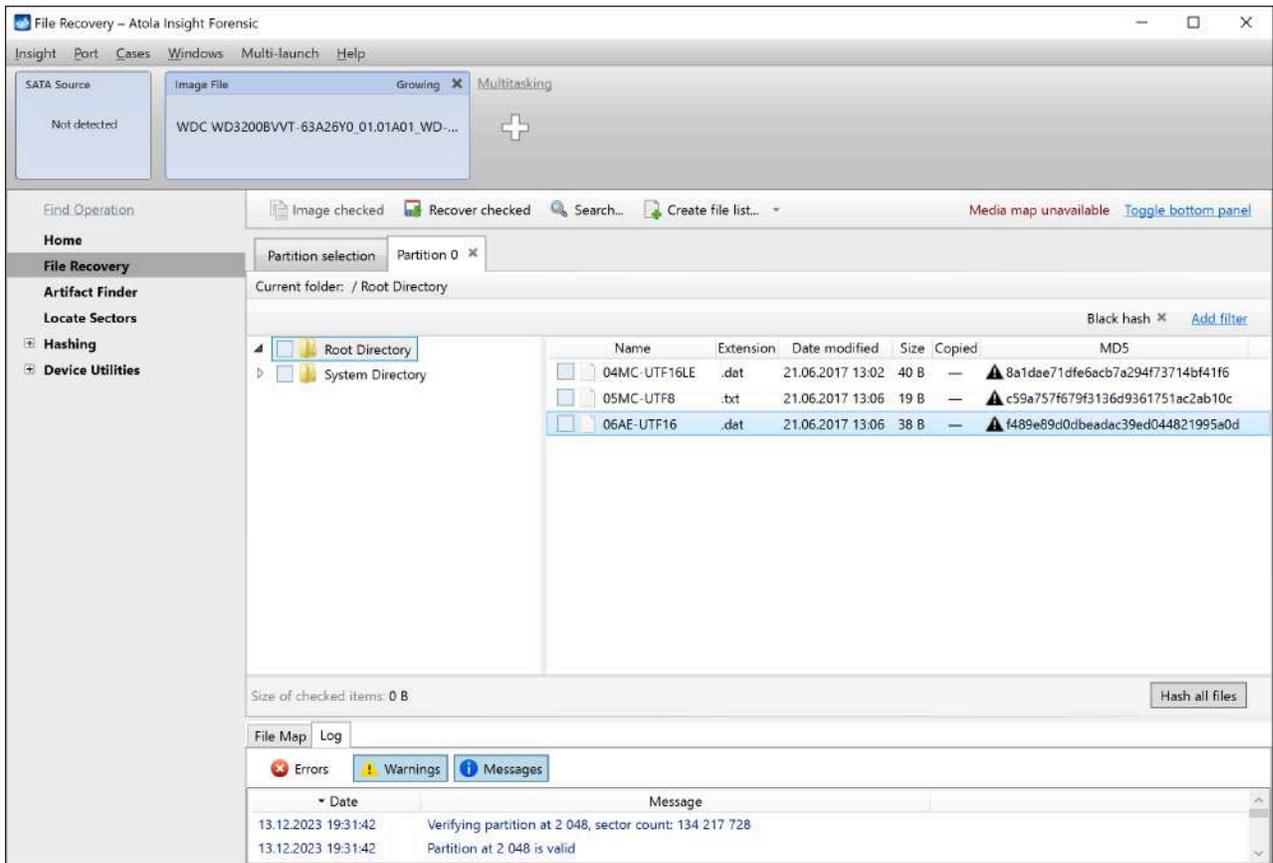


5. On the top right of the **Partition** tab, click the **Add filter** link.



6. Select either **Black hash** or **White hash**.

7. Insight Forensic compares every calculated file hash against the selected hash list and displays only the files whose hashes are found in this list.

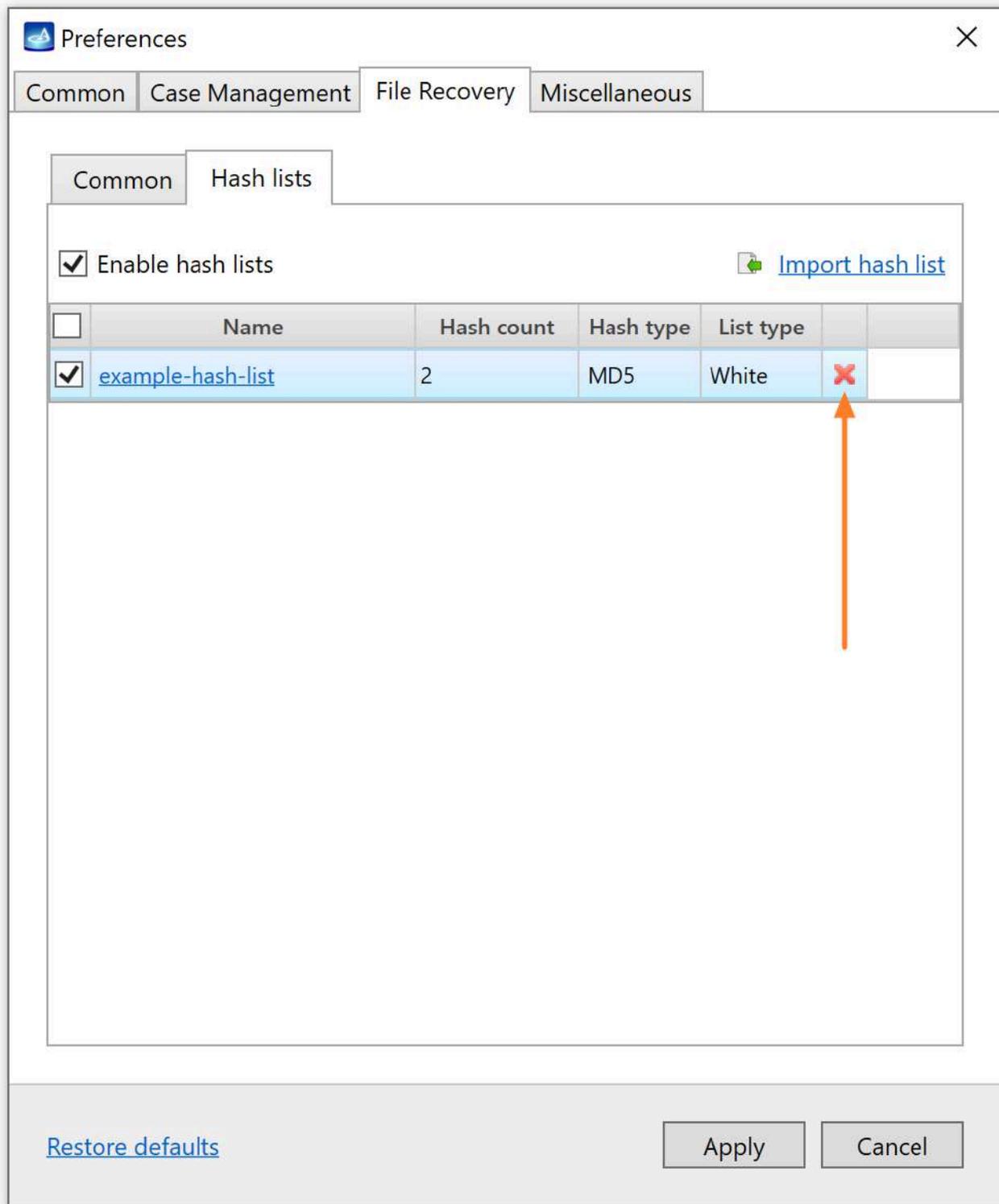


To learn more about file extraction capabilities for both good and damaged drives, see [File Recovery](#).

## Delete a hash list

To delete an existing hash list from Insight Forensic, do the following:

1. In the Insight Forensic menu, select **Insight > Preferences** or press **Ctrl + Q**.
2. In the **Preferences** window, go to the **File Recovery** tab, and then to the **Hash lists** subtab.
3. Select the hash list you want to delete, click the **Delete** icon and confirm your decision.



## Extracting and resetting an unknown ATA password

Atola Insight Forensic can recover and/or remove unknown HDD passwords (also known as ATA passwords). For most hard drives the unlocking process is fully automated.

Automatic ATA password recovery is supported for many Seagate, WD, Toshiba, Hitachi, Samsung, Fujitsu, Maxtor SATA and IDE drives. For the full list of the hard drives supported by the feature, see [Supported drives](#).

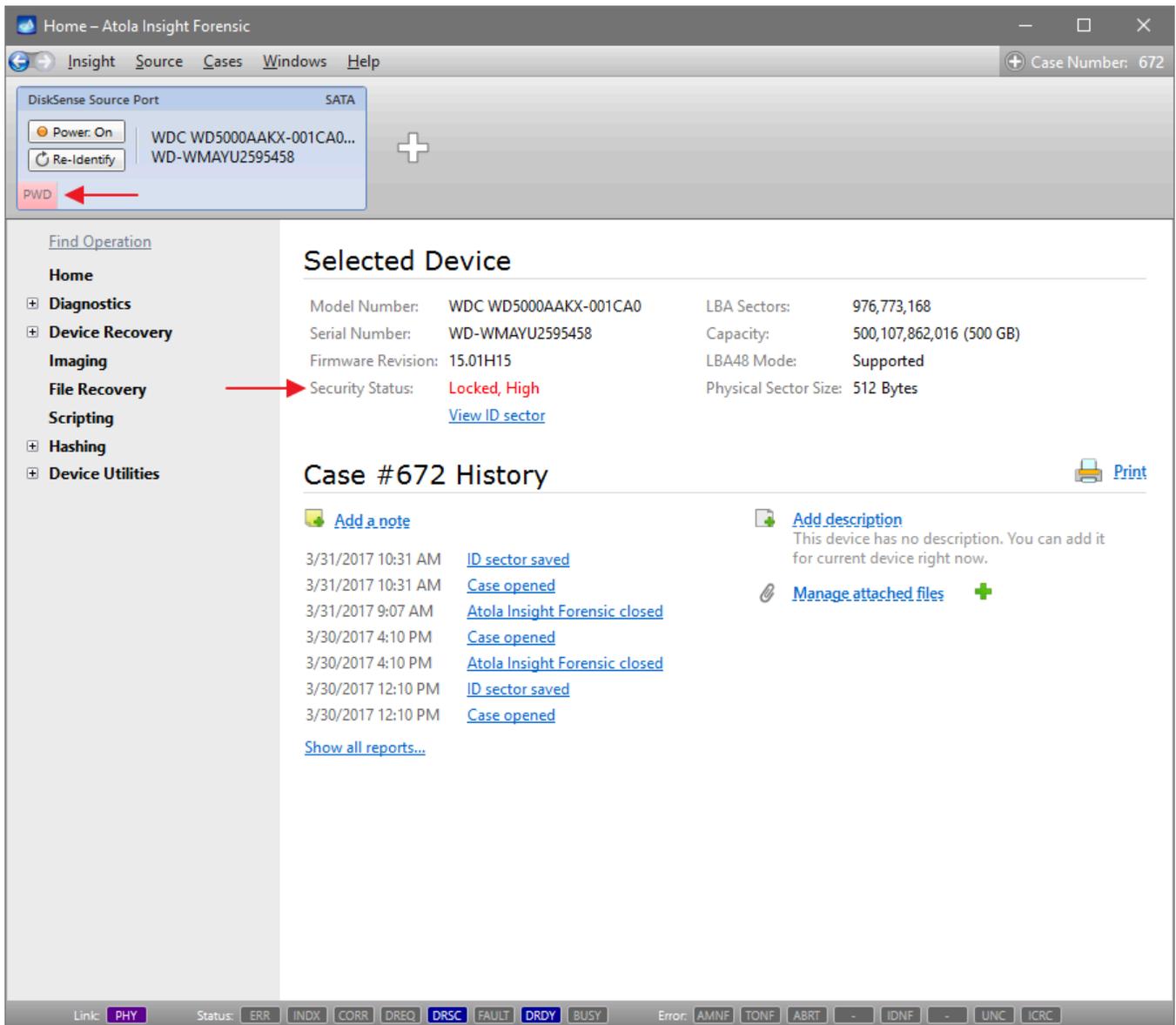
This guide is applicable to all supported Samsung, Toshiba and Western Digital hard drives.

- To unlock a Seagate drive, [connect the device to the Serial port](#) of the DiskSense unit and then follow the steps described in this guide.
- Hitachi drives require the use of the password extraction adapter. For more information, see [Hitachi HDDs: Remove an unknown password](#).

## Detect an ATA password

When a device is connected and identified as locked with an ATA password, there is a corresponding **PWD** indicator displayed in the port, and **Security Status** in the Home page says *Locked, High* or *Locked, Maximum*.

High and maximum are password protection levels that the operator who locked the device selected. Although information about it may be relevant to the investigator, both security levels are supported by Insight password recovery functionality, therefore this information is not important for the purpose of this guide.



### Source device locked with ATA password

To perform a complete Diagnostics, Insight needs to have a hard drive unlocked. Therefore we suggest that when dealing with a locked device, password recovery is performed before running the **Automatic Checkup**.

Automatic Checkup finished – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 672

DiskSense Source Port SATA

Power: Off WDC WD5000AAKX-001CA0...  
Re-Identify WD-WMAYU2595458

PWD Auto Diagnostics: Completed

**Note:** Currently attached device is locked. Most actions will fail until the device is unlocked. [Go to Password Recovery](#)

Print... Save to file... Copy to Clipboard

Thursday, April 6, 2017 2:19 PM  
Report created by Atola Insight Forensic 4.8.6255.23495.  
case #28

### Diagnostics report

Device model:	WDC WD5000AAKX-001CA0	Unit IP:	10.0.0.155
Device serial:	WD-WMAYU2595458	Unit serial:	67331143
Device firmware:	15.01H15	Write protection:	On
Device size:	500 GB (500,107,862,016 bytes)	Computer:	YULIA
Case number:	672	User:	ATOLA
Case description:		OS:	64-bit Windows 10 Home Version 6.2 (Build: 14393)

**Diagnostics results**

The device is locked with ATA password and therefore the diagnostics cannot continue. Please remove the lock and re-run the diagnostics.

**Full Diagnostic Log**

**Circuit Board (PCB)**

Device is powered on. A power cycle is needed...  
Applying power and watching spin-up currents...  
Selected Interface: SATA

**Current oscillogram (12V):**

mA

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

### Diagnostics showing password lock

## Extract password, Reset password and Reset password until power cycle

There are 3 options of dealing with a locked hard drive:

- To extract and display password without unlocking the device.
- To reset password only until power cycle.
- To permanently unlock the device.

## Extract and display password

This option does not require to switch off the write protection on the source port.

To display the password without unlocking the device, do these steps:

1. In the sidebar, go to **Device Recovery > Password Recovery**.
2. Click **Extract**.

## Reset password only until power cycle

When you reset password only until power cycle, write protection stays enabled on the source port, and no changes can be made to the drive.

To work with the data on the drive without permanently resetting the password, do the following:

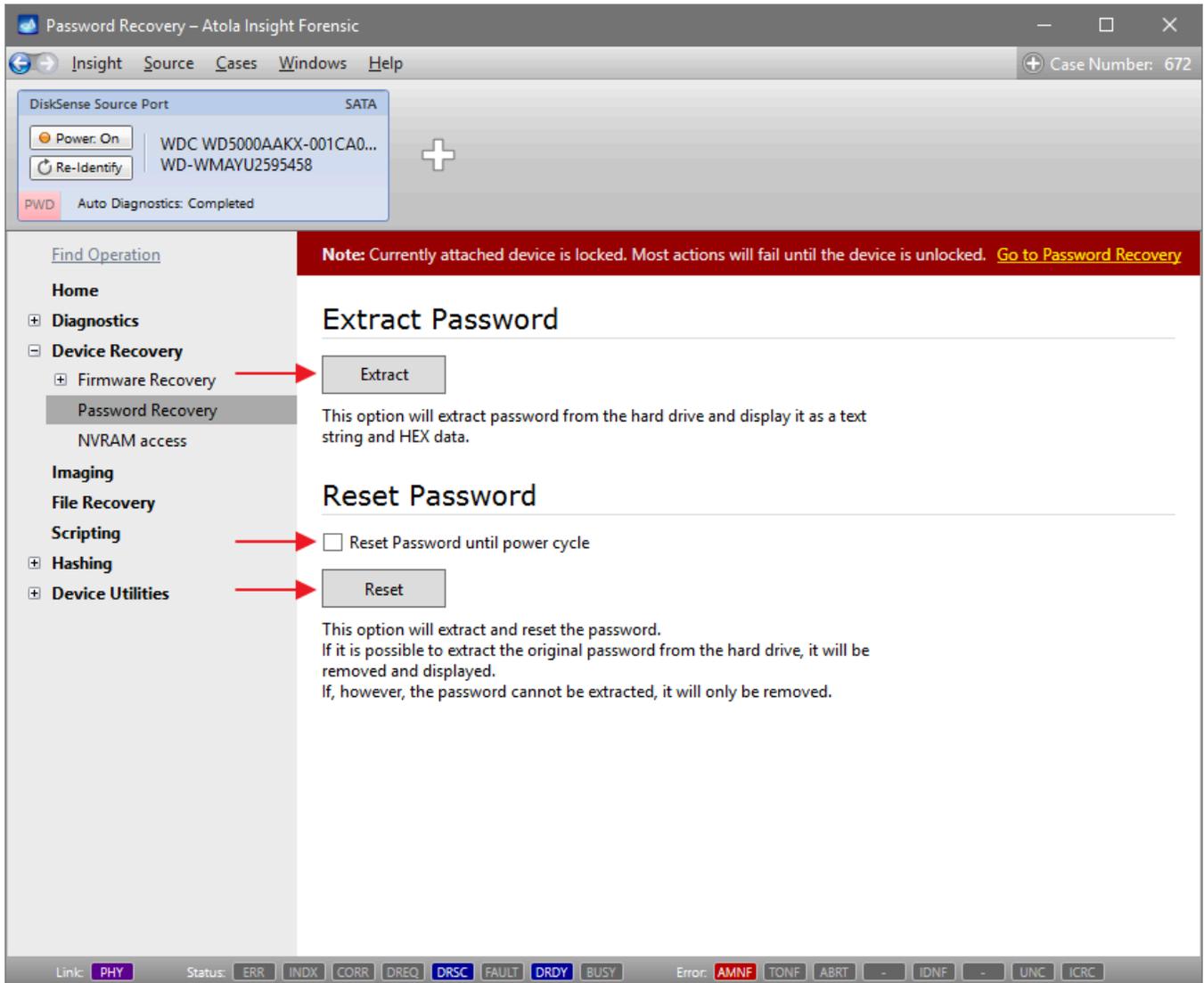
1. In the sidebar, go to **Device Recovery > Password Recovery**.
2. Select **Reset Password until power cycle**.
3. Click **Reset**.

If the **Reset Password until power cycle** option is selected, no power cycles that are executed in the course of automatic checkup, imaging, or other operations will affect the temporary unlocked status of the device. Only a deliberate power cycle, such as turning off and on the Power switch, will change the Security status of the drive back to Locked.

## Permanently reset password

To permanently reset password and unlock the device, do next steps:

1. Turn off the **Write protection switch** on the front panel of the DiskSense hardware unit.
2. In the sidebar, go to **Device Recovery > Password Recovery**.
3. Click **Reset**.



## Unknown password recovery

## Hitachi HDDs: Remove an unknown password

DISCLAIMER: BY FOLLOWING THESE INSTRUCTIONS YOU ACKNOWLEDGE THAT NO ONE IS RESPONSIBLE FOR ANY DAMAGE THAT CAN BE DONE TO THE HARD DRIVE OR OTHER DEVICES OR EQUIPMENT DURING THIS PROCEDURE.

PLEASE MAKE SURE THAT YOUR PC AND ATOLA DISKSENSE 2 UNIT ARE PLUGGED VIA A UPS (Uninterruptible Power Supply). PLEASE ALSO MAKE SURE YOU DO NOT HAVE ANY OTHER PROGRAMS RUNNING. INTERRUPTION OF THE UNLOCKING PROCESS MAY RENDER THE HARD DRIVE INOPERABLE.

BEFORE YOU PROCEED WITH UNLOCKING, PLEASE LOOK THROUGH FOLLOWING INFORMATION. IF YOU ARE NOT COMFORTABLE WITH THE PROVIDED INFORMATION, PLEASE DO NOT PROCEED.





4. Use a T4 screwdriver to remove four screws as shown below:



5. Put a piece of paper between the circuit board and the hard drive assembly:



6. Do not remove paper; proceed with unlocking.

7. Remove the paper and then put all screws back:



8. Continue with the unlocking process.

## 2.5-inch SATA hard drives (old models)

The following actions can only be performed if your SATA drive is attached to DiskSense 2 unit via Atola External IDE Adapter.

1. Connect Atola External IDE Adapter to the IDE (USB-C) port located on the left side of DiskSense 2 unit.
2. Connect the source Hitachi HDD to Atola External IDE Adapter.
3. Place the hard drive as shown on the picture (no need to disconnect any cables):



4. Use a T4 screwdriver to remove two screws as shown below:



5. Put a piece of paper between the circuit board and the hard drive assembly:



6. Do not remove paper; proceed with unlocking.

7. Remove the paper and then put all screws back:



8. Continue with the unlocking process.

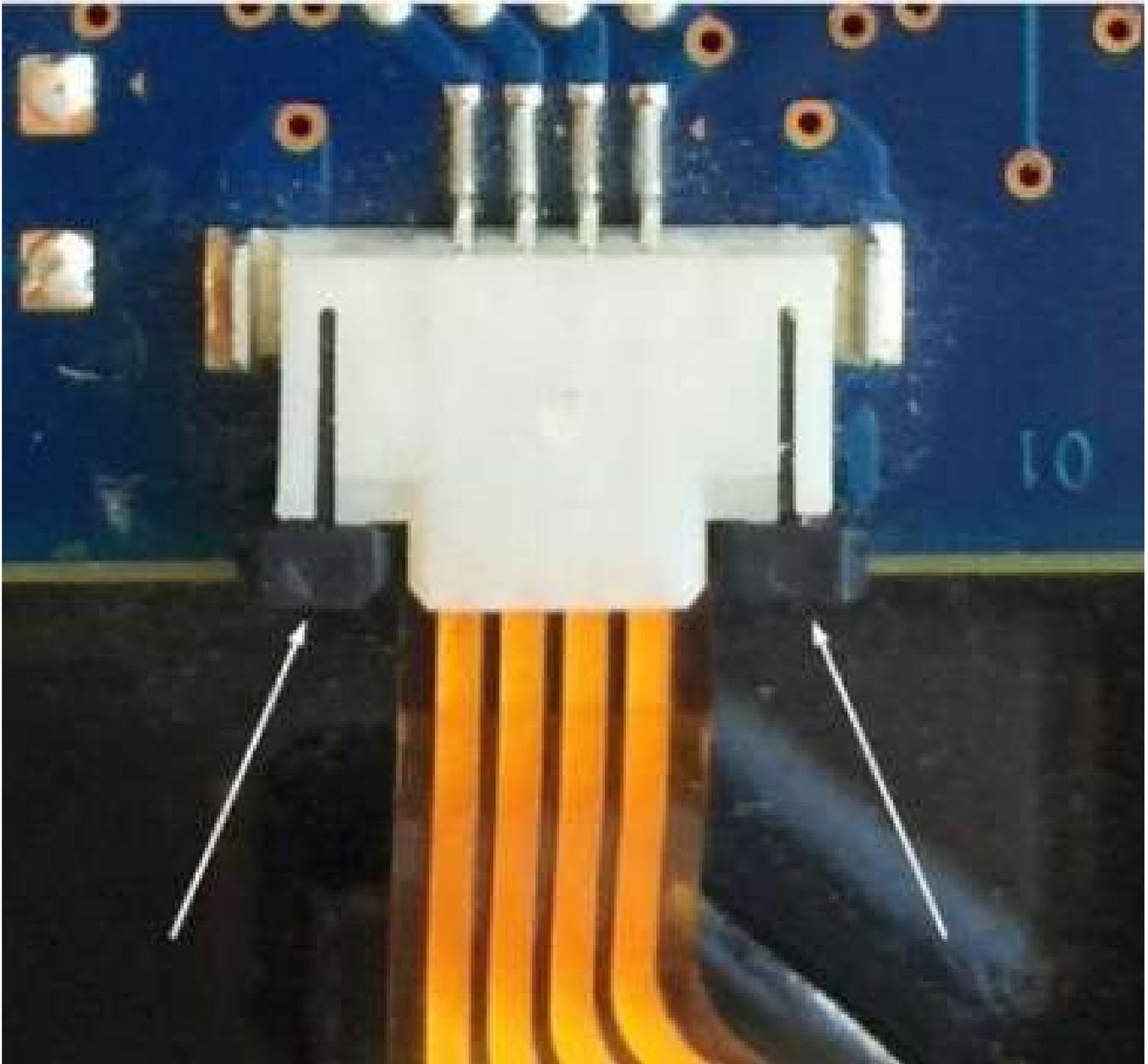
## 3.5-inch SATA hard drives

The following actions can only be performed if your SATA drive is attached to DiskSense 2 unit via Atola External IDE Adapter.

1. Place the hard drive as shown on the picture (no need to disconnect any cables):

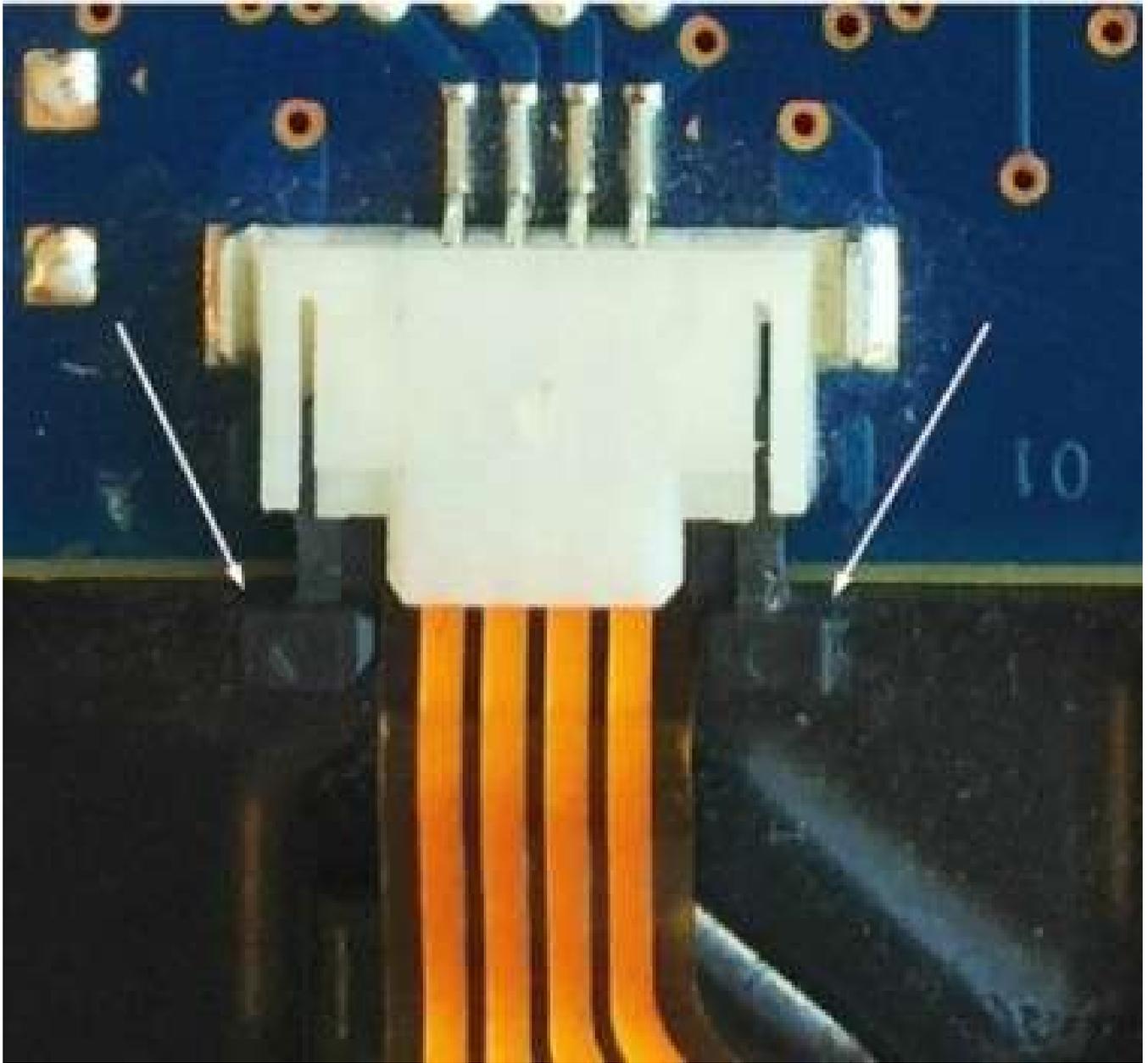


You may see the orange cable connected to the PCB being fastened by the latch.

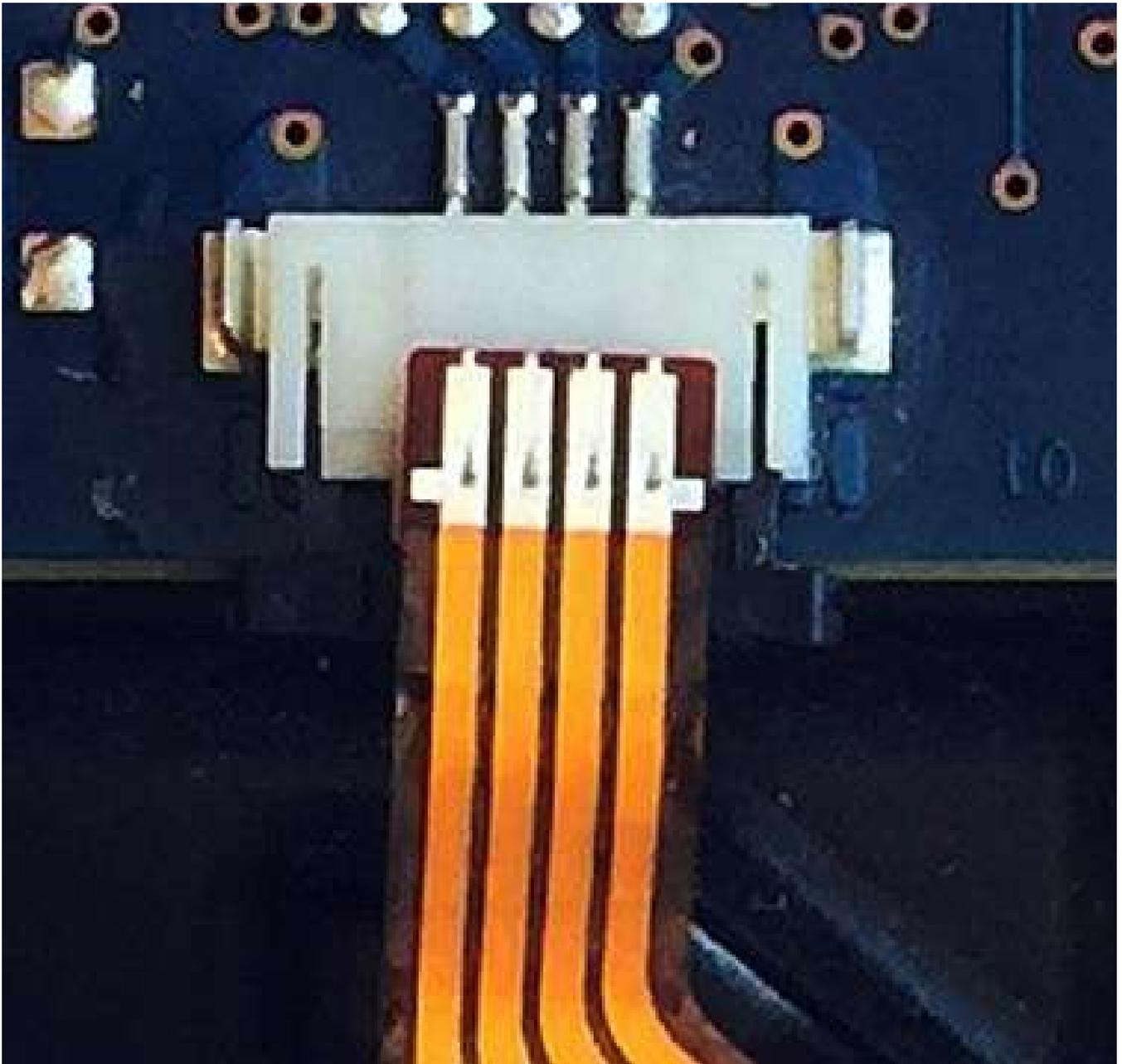


2. **Important:** Power off the drive.

3. Unlock the latch as it is shown below:



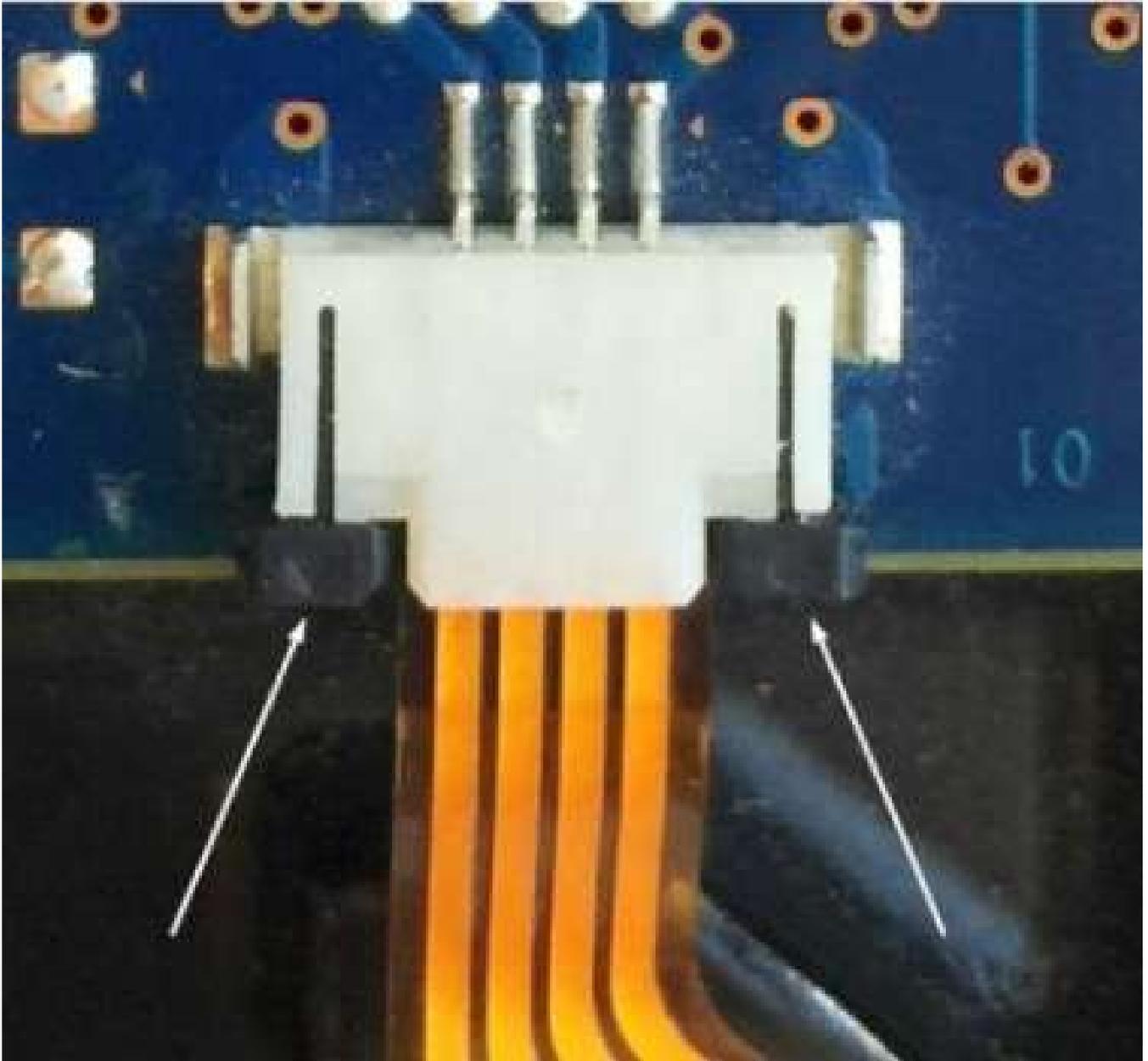
4. Disconnect the cable.



5. Proceed following Atola Insight instructions.

6. **Important:** Power off the drive.

7. Plug the orange connector into the PCB socket and fasten it with the latch.



8. Follow Atola Insight instructions.

## 2.5-inch IDE hard drives

1. Connect your 2.5-inch IDE drive to the DiskSense 2 unit using the Atola External IDE Adapter:



2. Install a jumper between pins A and C (on the adapter).
3. Attach the hard drive back to the DiskSense 2 unit and proceed with unlocking.
4. Remove the jumper:



5. Plug the hard drive back to the DiskSense 2 unit and continue with unlocking.

## 3.5-inch IDE hard drives

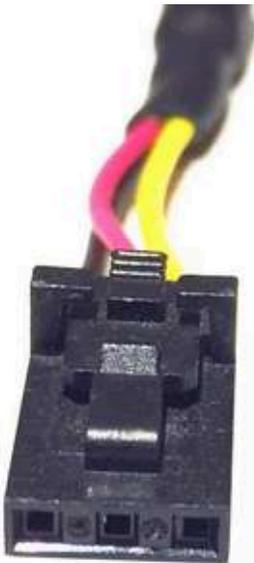
1. Connect your 3.5-inch IDE drive to the DiskSense 2 unit using the Atola External IDE Adapter:



## Unlocking Seagate drives

If you need to extract or reset an unknown password or perform drive recovery on a Seagate hard drive, use a **Serial cable** to connect the drive to the DiskSense unit.

Take a minute to familiarize yourself with the Serial cable's three connectors. On one side of the cable, there are two connectors. Both are **2-pin RX-TX** (receive-transmit) connectors. The slightly larger one has **2.5-mm** pin pitch and is used for **IDE** drives. The smaller one has **2-mm** pin pitch and is used for **SATA** drives.



**3-pin TX-RX-GND  
connector**



**2.5-mm RX-TX  
connector**



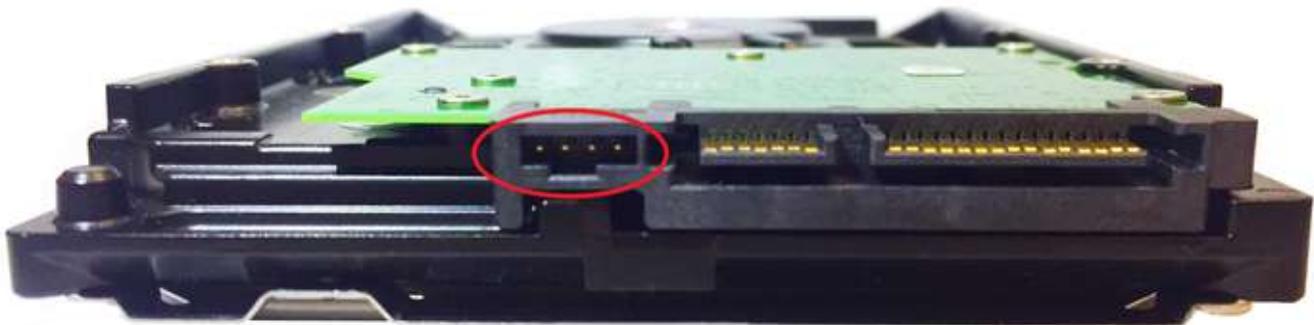
**2-mm RX-TX  
connector**

On the opposite side of the Serial cable, there is a **3-pin TX-RX-GND** (transmit-receive-grounding) connector. This connector is inserted in the **Serial port** on the back side of the DiskSense unit.



## Connecting 3.5-inch and 2.5-inch Seagate SATA drives

When you look at a Seagate SATA drive (either 3.5-inch or 2.5-inch), there is a 4-pin jumper block right next to the SATA port.





Connect the 2-mm RX-TX end of the serial cable to the two jumper pins located closest to the SATA port so that the red RX (receive) wire is connected to the pin closer to the SATA port.

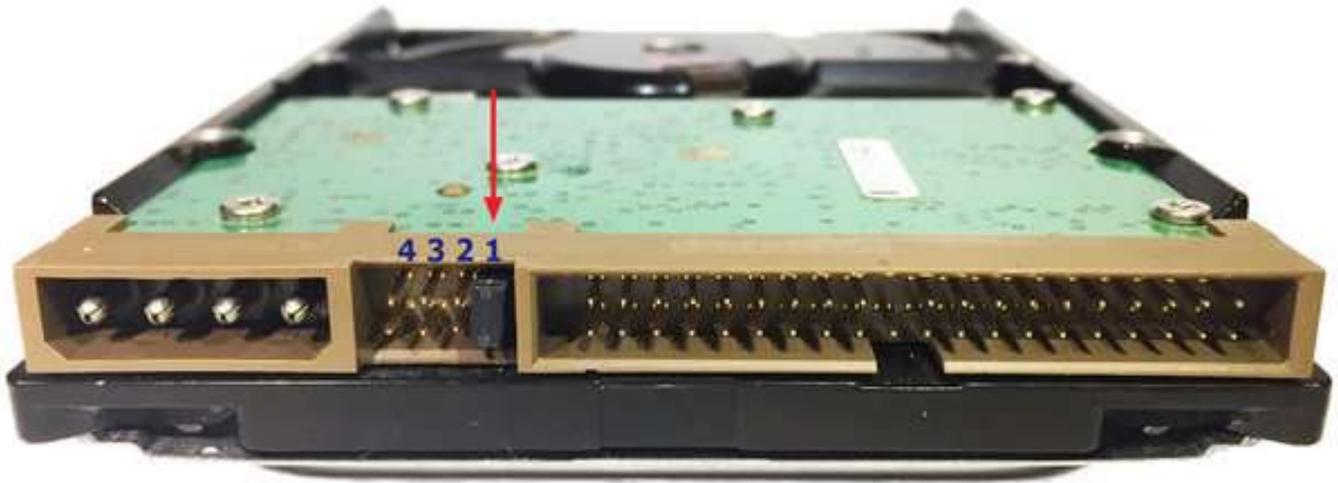




## Connecting 3.5-inch Seagate IDE drives

Desktop IDE drives have an **8-pin jumper block** between IDE port and Power port. For the purpose of this manual, we shall call the pair of pins located closest to the IDE port and used for Master/Slave settings the **first pair** of pins. The next, second pair of pins is usually used for Cable Select settings. The **third pair** of pins is the one we will connect the **Serial cable** to.

Please note that IDE hard drives must be set to **Master mode** for password extraction and reset or drive recovery. To use the drive in Master mode, place a jumper on the **first pair** of pins (closest to the IDE port), as shown in the picture below.



Attach the 2.5-mm RX-TX connector to the **third** pair of jumper pins, as shown in the picture below. Make sure that red RX (receive) wire is facing down and the black TX (transmit) wire is facing up. The **second** pair and the **fourth** pair of pins must be left open.



## Connecting 2.5-inch Seagate IDE drives

Similar to desktop hard drives, laptop Seagate hard drives also must be set to Master mode to perform password extraction and reset or drive recovery. Master mode on a 2.5-inch device is set by removing all jumpers.



There is a Atola external IDE adapter included in the package with the DiskSense 2 unit.

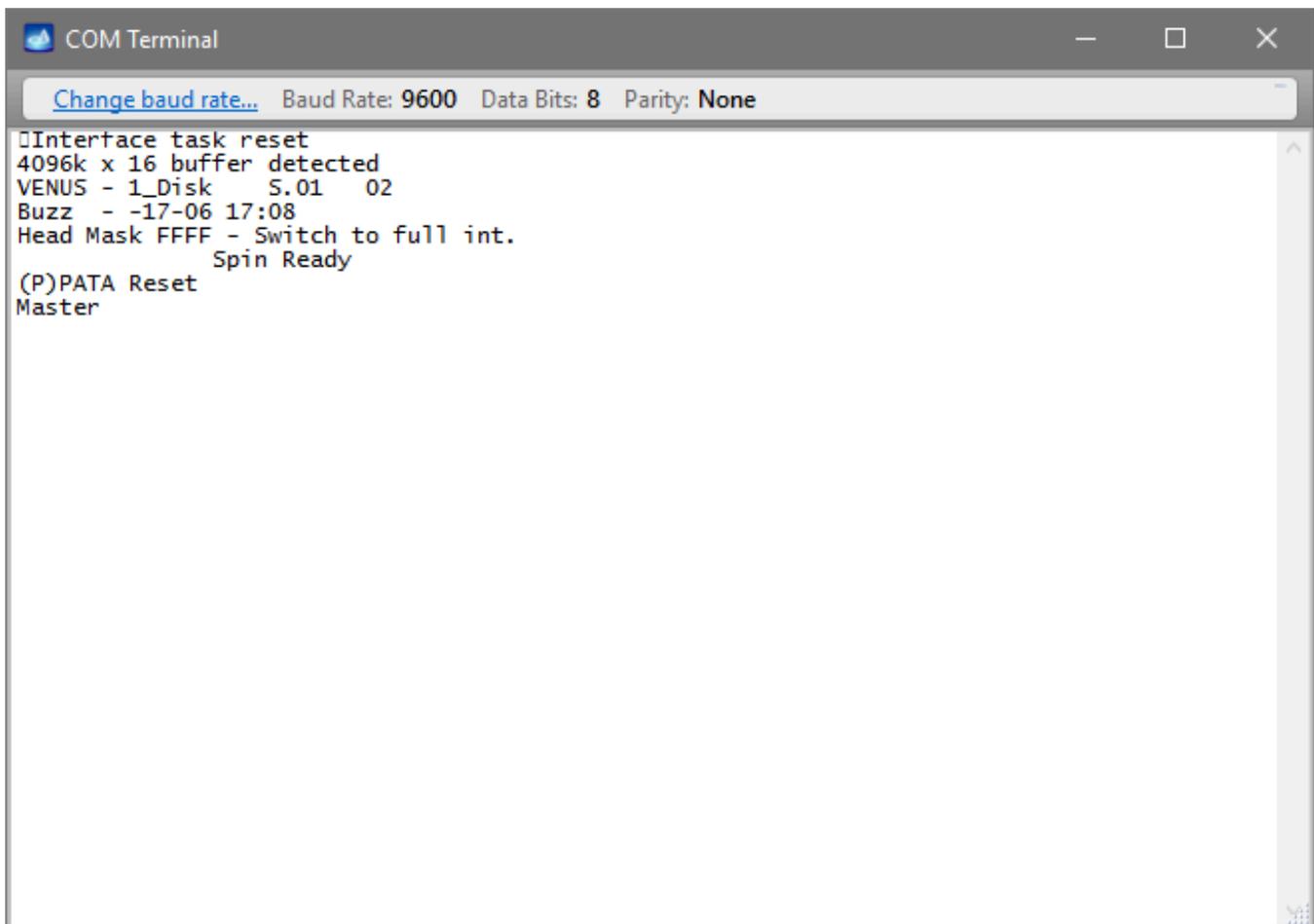
Use the adapter to connect the drive to IDE interface cable and IDE power cable. Then attach the 2.5-mm RX-TX connector to the left pins vertically, as shown in the picture below. Make sure that the black TX (transmit) wire is connected to the upper pin and red RX (receive) wire is connected to the lower pin.



# Configuring the Baud rate

Once the Seagate hard drive is connected to the unit, follow these instructions to configure the **Baud rate** of Seagate Terminal, which allows you to use an extensive set of commands on a Seagate drive:

1. If there is only one source drive connected to the DiskSense unit, it will automatically be identified and displayed in the **Source disk port**. However, if there are multiple hard drives connected to the DiskSense unit as Source drives, go to **Source** category of the top level menu, click on **Select Source** and choose the Seagate drive.
2. Power down the selected drive.
3. In the **Windows** category of the top level menu click on **Terminal** and in the **COM Port Settings** window select the **Baud rate** compatible with the drive. *Please note that for Seagate 7200.10 and older Baud rate will be 9600; for 7200.11 and newer Baud rate will be 38400 (Atola Insight Forensic will suggest the baud rate by setting a default value in the Terminal window for the drive connected to it).*
4. Then click OK. But do not close the **Terminal** window just yet.
5. Power on the drive again. There must be a valid output in the **Terminal** window (see the picture below).



The screenshot shows a window titled "COM Terminal" with a status bar at the top displaying "Change baud rate...", "Baud Rate: 9600", "Data Bits: 8", and "Parity: None". The main area contains the following text output:

```
□Interface task reset
4096k x 16 buffer detected
VENUS - 1_Disk   S.01  02
Buzz - -17-06 17:08
Head Mask FFFF - Switch to full int.
                Spin Ready
(P)PATA Reset
Master
```

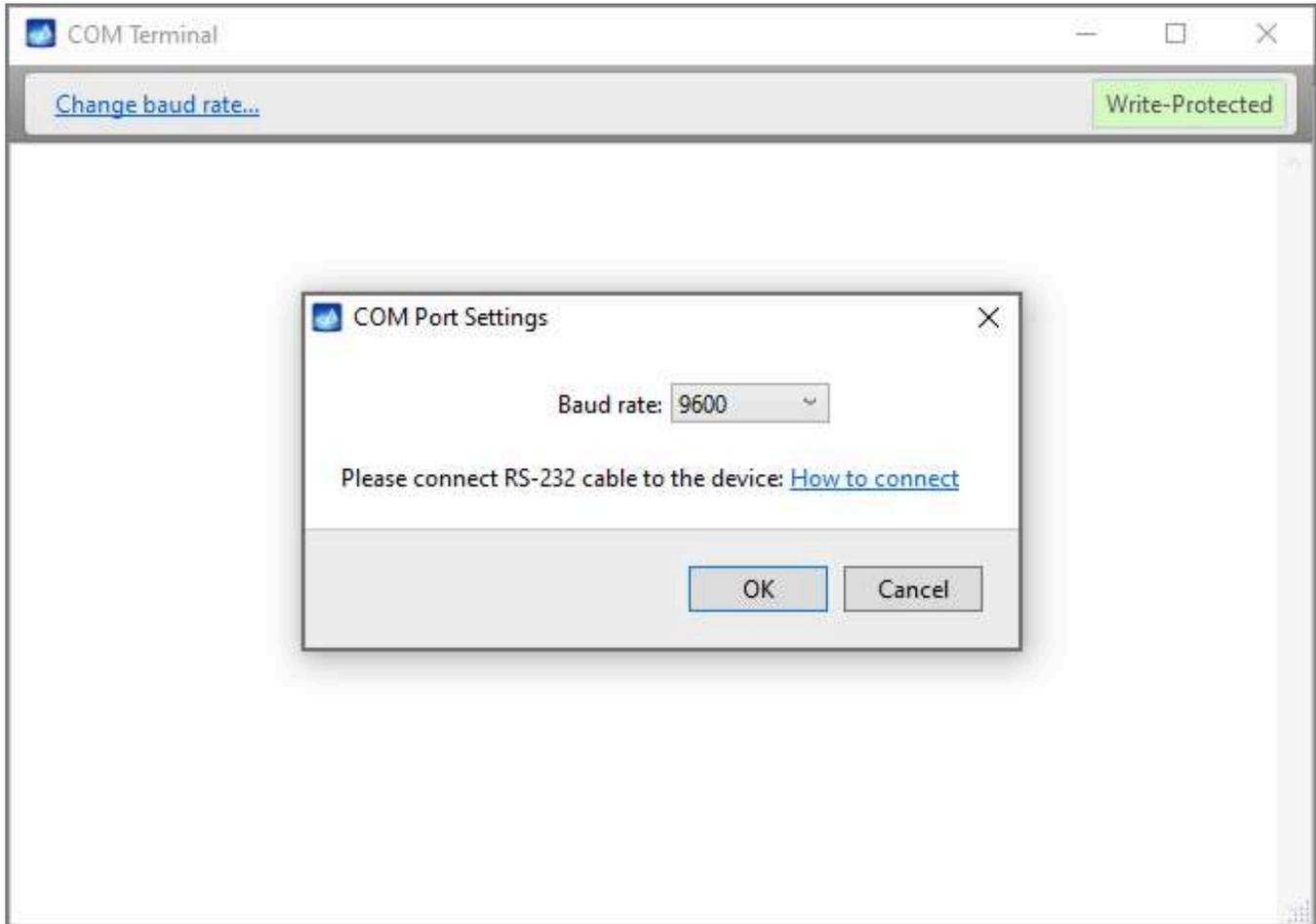
Should there be no output in the Terminal window or should it consist of random symbols, try to change the Baud rate until you get a good response.

Now proceed with [password extraction](#) or send Seagate Terminal commands to the drive.

## Recovering Seagate 7200.11 hard drives

First of all, please connect the hard drive's serial port to DiskSense unit by following instructions on the [Serial Port Connection](#) page.

Open the Terminal window, select the DiskSense COM port (usually the one that is displayed by default is the correct one). 38400 is the proper speed for 7200.11 hard drives:



### COM terminal connection

Once everything is set up, click OK. Make sure that you have attached everything correctly by applying power to the drive (you should see a meaningful output in the terminal window).

Note: if you make an mistake while entering commands, you will get the following message:

---

Invalid Diag Cmd Parameter

---

In this case simply re-enter the command and double-check that you are entering everything exactly as shown in this manual.

Once everything is ready and you have powered on the drive, you should see the following (or very similar) output in the terminal window:

---

```
Rst 0x20M
```

```
(P) SATA Reset
```

---

At this point press CTRL+Z. You should receive the command prompt:

```
F3 T>
```

---

## Fixing zero capacity problem

1. Type the following: m0,2,2,0,0,0,22 and then press ENTER.
2. At this point the drive will stop responding for a while.
3. After some time (1-5 minutes) you will get several messages from the drive similar to these:

---

```
Max Wr Retries = 00, Max Rd Retries = 00, Max ECC T-Level = 00, Max Certify Rewrite Retries = 0000  
User Partition Format Successful - Elapsed Time 0 mins 00 secs
```

4. Wait some more time until you see the command prompt again:

---

```
F3 T>
```

5. Type the following: /2 and then press ENTER. You will see the following output:

---

```
F3 T>/2  
F3 2>
```

6. Type capital Z and press ENTER:

---

```
F3 2>Z  
Spin Down Complete  
Elapsed Time 10.543 secs  
F3 2>
```

7. At this point you have to re-power the drive. The procedure is complete.

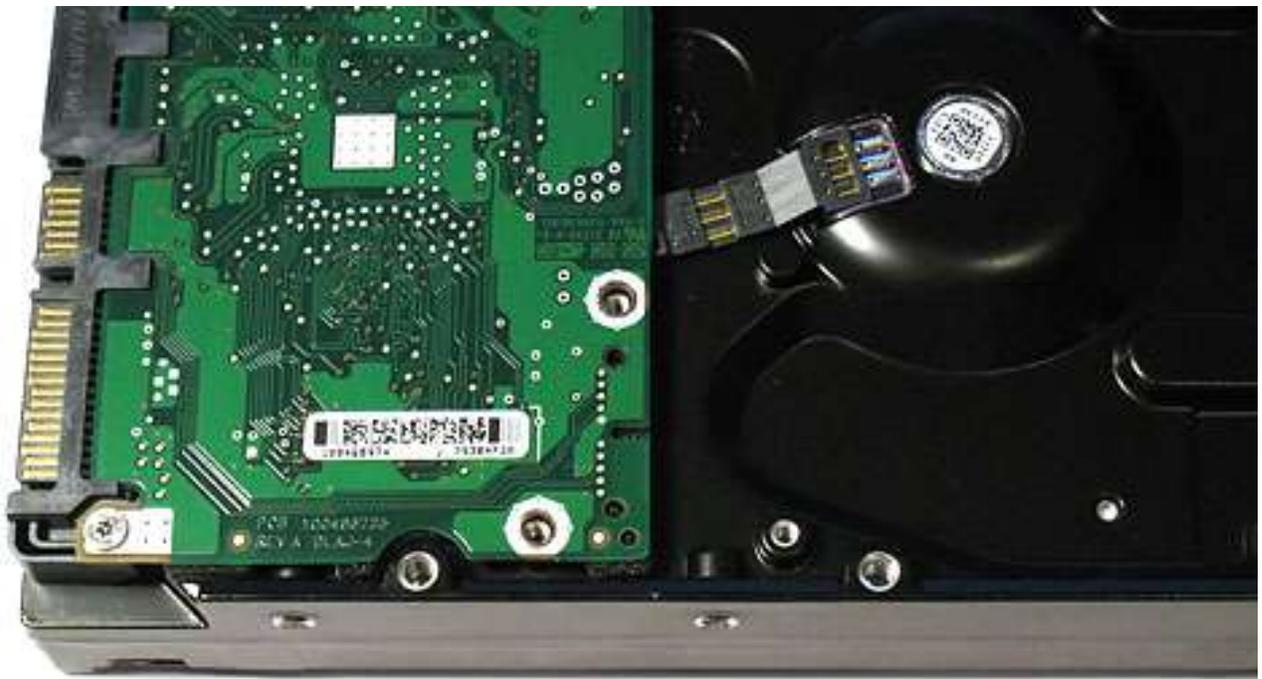
# Fixing HDD always BUSY problem

This problem is also known as "LED:000000CC problem". This is because when you apply power, you will usually see the following output:

```
Rst 0x10M  
LED:000000CC FAddr:0025BF67
```

To fix this issue, please follow these steps:

1. Power off the drive
2. Remove two screws as shown on the picture below (you will need a Torx T6 screwdriver):



3. Put a piece of paper as shown on the picture below (the goal is to separate spindle motor contacts from the pcb):



4. If you detached any cables from the drive, this is the right time to attach them back.

5. Apply power to the drive (with screws removed and paper inserted) and wait for the drive to become ready (usually no more than one minute)

6. You will see the following (or very similar) output in the terminal:

```
Rst 0x20M
```

7. Press CTRL+Z. You will get the command prompt:

```
F3 T>
```

8. Type the following: /2 and then press ENTER. You will see the following output:

```
F3 T>/2  
F3 2>
```

9. Type capital Z and press ENTER:

```
F3 2>Z
Spin Down Complete
Elapsed Time 0.132 msec
F3 2>
```

10. Now remove the paper, put all screws back and tighten them (do not power off the drive!):



11. Type capital U and press ENTER:

```
F3 2>U
Spin Up Complete
Elapsed Time 6.604 secs
F3 2>
```

12. Type the following: /1 and then press ENTER. You will see the following output:

```
F3 2>/1
F3 1>
```

13. Type the following: N1 (capital N and one) and then press ENTER. You will see the following output:

```
F3 1>N1
```

```
F3 1>
```

---

14. Re-power the drive (press Power Off button on the DiskSense unit; wait 10-15 seconds; press Power On button) and wait until it initializes:

---

```
Rst 0x20M
```

```
(P) SATA Reset
```

---

15. Press CTRL+Z. You will get the command prompt:

---

```
F3 T>
```

---

16. Type the following: i4,1,22 and then press ENTER. You will see the following output:

---

```
F3 T>i4,1,22
```

```
F3 T>
```

---

17. At this point do not re-power the drive, scroll to the top of this page and go through **Fixing zero capacity problem** starting from step 1.

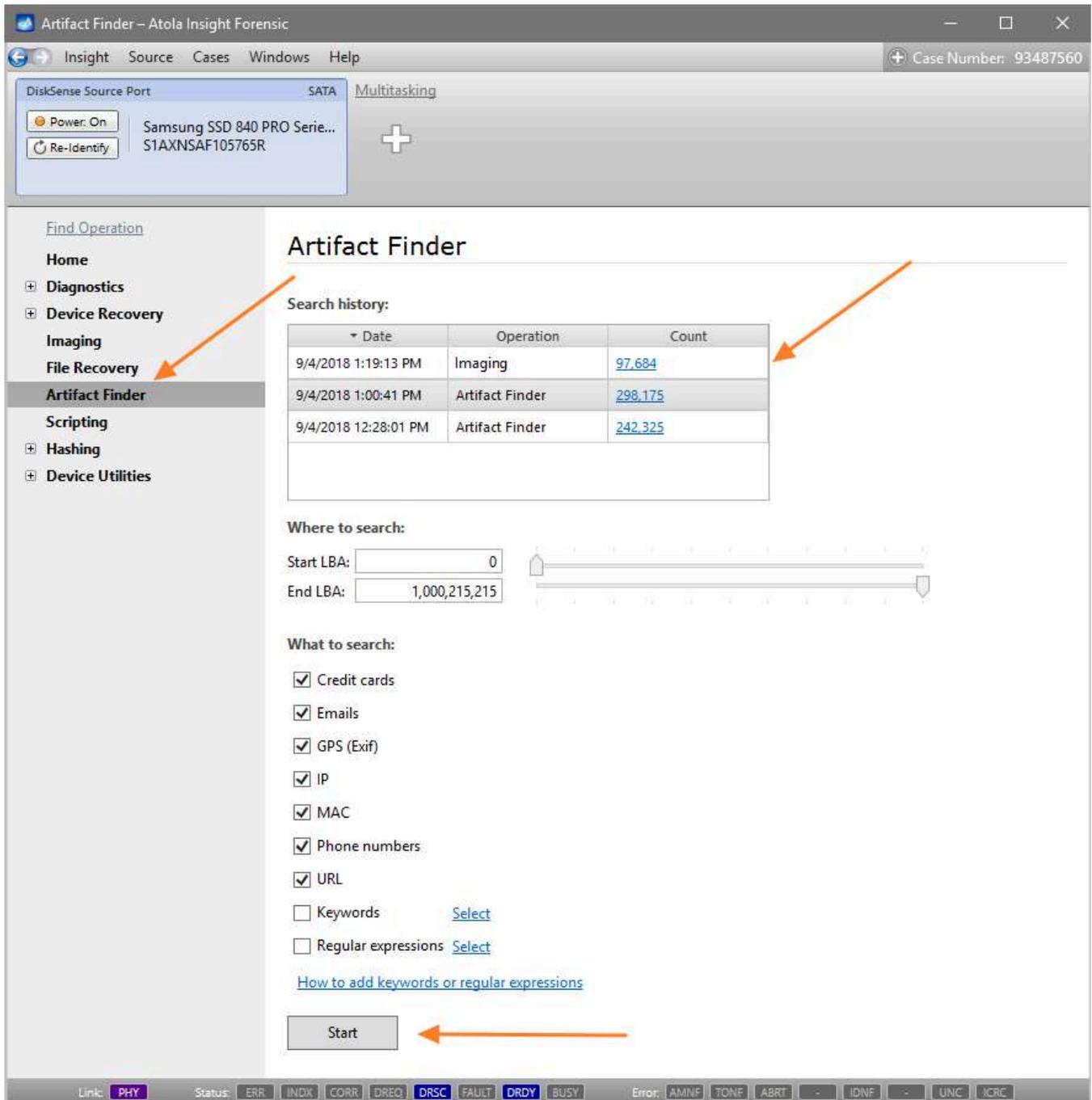
## Artifacts Finder

Insight's Artifact Finder feature allows early analysis of data by reading and parsing it on an evidence drive or its images. Unlike most forensic analysis tools that parse the file structure, Insight does sector-level parsing, which allows getting data even from the spaces of the drive that are not associated with any file (e.g. remnants of previously deleted documents), thus providing you with clues that are omitted by most analysis tools. Artifact finder uses Intel Hyperscan engine, which makes it the fastest possible tool for primary data analysis.

Insight supports multiple simultaneous artifact searches on both source and target drives.

## Search for artifacts

On the Sidebar, go to Artifacts Finder. In the upper part of the window there is a table with previous artifact searches performed on the current drive including those carried out during imaging. If you want to perform another search, select the artifacts that need to be found.

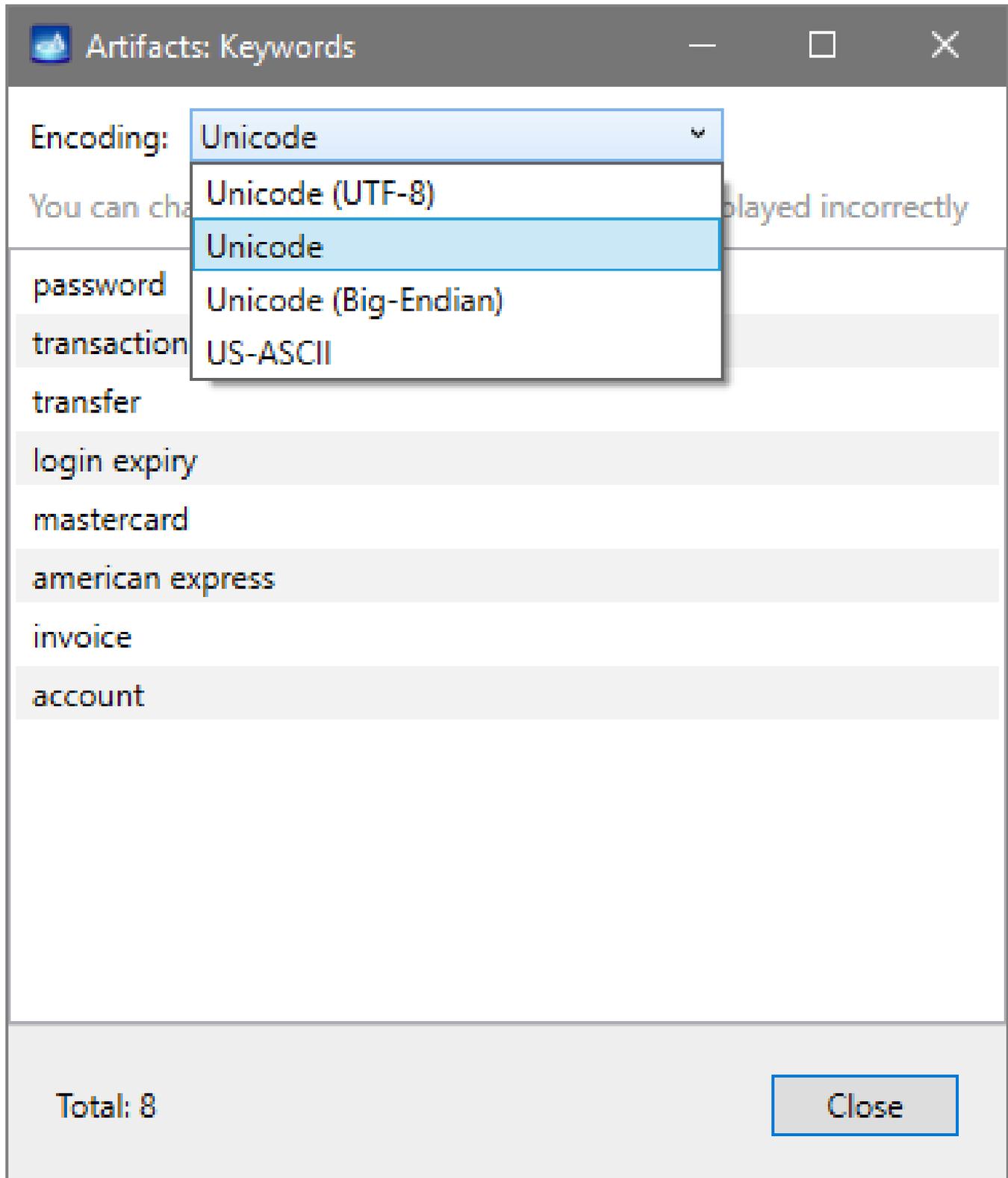


The artifacts include:

1. Credit cards
2. Emails
3. GPS coordinates
4. IP
5. MAC
6. Phone numbers
7. URL
8. Keywords
9. Regular expressions

For each of the artifacts, not only widely known filter algorithms were applied for proper result filtering (such as the Luhn formula used to validate credit card numbers), but there have also been custom smart filters applied to eliminate false results (e.g. two slashes next a number that has preliminarily been identified as a credit card number, will eliminate it from the search results, as it is likely to be a part of a URL).

Keywords and regular expressions can be added to the search parameters in a txt file with one artifact per line. Keyword encoding can be adjusted to *Unicode*, *Unicode (UTF-8)*, *Unicode (Big-Endian)* or *US-ASCII*.



The screenshot shows a window titled "Artifacts: Keywords" with a search results list and an encoding dropdown menu. The search results list contains the following keywords: password, transaction, transfer, login expiry, mastercard, american express, invoice, and account. The encoding dropdown menu is open, showing the following options: Unicode, Unicode (UTF-8), Unicode, Unicode (Big-Endian), and US-ASCII. The "Unicode" option is currently selected. At the bottom of the window, there is a "Total: 8" label and a "Close" button.

Encoding:	Unicode
You can cha	Unicode (UTF-8)
password	Unicode
transaction	Unicode (Big-Endian)
transfer	US-ASCII
login expiry	
mastercard	
american express	
invoice	
account	

Total: 8

Close

# Browse through the found artifacts

As the Artifact Finder is still running, you can look at the progress in the Artifacts tab below the progress bar and click the diagram to see the list of found artifacts. If you only want to look at a certain category, click it in the list or in the diagram.

The screenshot shows the Atola Insight Forensic interface. At the top, a progress bar indicates the Artifact Finder is 68% complete. Below this, a summary shows 163,478 artifacts found in 5 minutes, with a speed of 473 MB/s. A donut chart displays the distribution of artifact categories, with URL being the most frequent at 160,766. An orange arrow points to the URL category in the legend.

Category	Count
Credit cards	10
Emails	1,986
GPS (Exif)	0
IP	586
MAC	68
Phone numbers	62
URL	160,766

In the table, each artifact is given an **Id** number, each found **Value** is shown in the context (including 20 bytes before and 20 bytes after the artifact in grey color), the **LBA** and the **offset** are also displayed in the table to help locate the artifact.

Artifacts

Search artifacts by value or LBA

Credit cards
  Emails
  GPS (Exif)
  IP
  MAC
  Phone numbers
  URL
 [Show unique artifacts](#)

Found artifacts: 160,766 Page: 1 / 6,699

Id	Type	Value	Lba	Offset
1	URL	DTD PLIST 1.0//EN" http://www.apple.com/DTDs/PropertyList-1	6,720	05D
2	URL	DTD PLIST 1.0//EN" http://www.apple.com/DTDs/PropertyList-1	6,784	05D
3	URL	<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-synt	7,640	133
4	URL	about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmp	7,640	18A
5	URL	/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:	7,640	185
6	URL	0/mm/" xmlns:stref="http://ns.adobe.com/xap/1.0/sType/Resou	7,640	1E3
7	URL	lash.upgrade.url": "http://get.adobe.com/flashplayer/",.	19,506	0E7
8	URL	s.src = "http://1.yimg.com/d/lib/3pm/cs_0.2.js	19,511	182
9	URL	<head><meta c	88,420	15F
41	URL	Transitional//EN" http://www.w3.org/TR/xhtml1/DTD/xhtml1	92,165	140
42	URL	ml:lang="en" xmlns="http://www.w3.org/1999/xhtml" xmlns:w	92,165	19E
43	URL	9/xhtml" xmlns:web="http://schemas.live.com/web/"><head><meta c	92,165	1C7
44	URL	gle -->...<!-- Site: http://www.ehow.com/ -->...<!-- SectionH	95,015	1D8
45	URL	.....f...f..... http://www.ehow.com/ -->...<!-- Copy and	95,016	041
46	URL	script><script src="http://a1.interclick.com/getInPageJS.aspx?a=	95,111	01F
47	URL	><noscript><A HREF="http://ad.yieldmanager.com/clk?3,e3ytjdEKgjAYh	95,111	088
54	URL	DTD HTML 4.01//EN" http://www.w3.org/TR/html4/strict.dtd	120,223	114

[Search examples](#)

There are many options to help find, sort, filter and view the artifacts. It is possible to view one or a few categories of artifacts in one list, use the **Search** bar to find a specific value (search examples are provided in the bottom right corner of the window), filter results for unique values by clicking the **Show unique artifacts** link. It helps identify the values most frequently occurring on the drive: to sort the results click **Count** in the table header.

Artifacts

Search artifacts by value or LBA Search

Credit cards  Emails  GPS (Exif)  Keywords  IP  MAC  Phone numbers [Show all artifacts](#)

Regular expressions  URL

Found artifacts: 2,709,917 Page: 1 / 4780 ◀◀ ◀ ▶ ▶▶

Type	Value	Count
URL	http://i.imgur.com	120,940
URL	http://www.w3.org	116,161
URL	http://ns.adobe.com	105,172
URL	http://news.google.com	103,661
URL	http://www.reddit.com	94,406
URL	http://swcdn.apple.com	81,780
URL	http://www.apple.com	80,799
URL	http://appldnld.apple.com	71,512
URL	https://swdist.apple.com	64,662

View sector Export to CSV [Search examples](#)

Click an artifact in the list to see the sector where it is located. It allows you to see the context, in which this artifact is placed.

Artifact search is in progress – Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 93487560

DiskSense Source Port SATA Multitasking

Power: On Samsung SSD 840 PRO Serie... S1AXNSAF105765R

Re-Identify

Artifact Finder 11 %

Find Operation

Home

Diagnostics

Device Recovery

Imaging

File Recovery

Artifact Finder

Scripting

Hashing

Device Utilities

### Finding artifacts

68%

Artifacts found: 163,478 Last processed LBA: 687,388,607

Time left: 5 minutes Speed: 473 MB/s

Stop

Error Log Hex Viewer Artifacts

Refresh sector interval (ms): 2,000  Freeze Read sector... Save sector to file...

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Data
Sector #6720																	
00348000	3C	3F	78	6D	6C	20	76	65	72	73	69	6F	6E	3D	22	31	<?xml version="1
00348010	2E	30	22	20	65	6E	63	6F	64	69	6E	67	3D	22	55	54	.0" encoding="UT
00348020	46	2D	38	22	3F	3E	0A	3C	21	44	4F	43	54	59	50	45	F-8"?>.<!DOCTYPE
00348030	20	70	6C	69	73	74	20	50	55	42	4C	49	43	20	22	2D	plist PUBLIC "
00348040	2F	2F	41	70	70	6C	65	2F	2F	44	54	44	20	50	4C	49	//Apple//DTD PLI
00348050	53	54	20	31	2E	30	2F	2F	45	4E	22	20	22	68	74	74	ST 1.0//EN" "htt
00348060	70	3A	2F	2F	77	77	77	2E	61	70	70	6C	65	2E	63	6F	p://www.apple.co
00348070	6D	2F	44	54	44	73	2F	50	72	6F	70	65	72	74	79	4C	m/DTDs/PropertyL
00348080	69	73	74	2D	31	2E	30	2E	64	74	64	22	3E	0A	3C	70	ist-1.0.dtd">.<p
00348090	6C	69	73	74	20	76	65	72	73	69	6F	6E	3D	22	31	2E	list version="1.
003480A0	30	22	3E	0A	3C	64	69	63	74	3E	0A	09	3C	6B	65	79	0">.<dict>.<key
003480B0	3E	36	30	31	41	45	31	42	36	2D	42	46	30	37	2D	34	>601AE1B6-BF07-4
003480C0	46	41	43	2D	42	36	30	44	2D	35	37	42	33	38	44	36	FAC-B60D-57B38D6
003480D0	39	35	45	44	46	3C	2F	6B	65	79	3E	0A	09	3C	64	69	95EDF</key>.<di
003480E0	63	74	3E	0A	09	09	3C	6B	65	79	3E	70	61	72	74	69	ct>.<key>parti
003480F0	61	6C	50	61	74	68	3C	2F	6B	65	79	3E	0A	09	09	3C	alPath</key>.<st
00348100	73	74	72	69	6E	67	3E	3C	2F	73	74	72	69	6E	67	3E	string></string>
00348110	0A	09	09	3C	6B	65	79	3E	70	6F	6C	69	63	79	53	65	...<key>policySe
00348120	61	72	63	68	3C	2F	6B	65	79	3E	0A	09	09	3C	69	6E	arch</key>.<in
00348130	74	65	67	65	72	3E	33	3C	2F	69	6E	74	65	67	65	72	teger>3</integer
00348140	3E	0A	09	3C	2F	64	69	63	74	3E	0A	3C	2F	64	69	63	>.<.</dict>.</dic
00348150	74	3E	0A	3C	2F	70	6C	69	73	74	3E	0A	00	00	00	00	t>.</plist>.....
00348160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00348170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00348180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

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

## Export the list of found artifacts

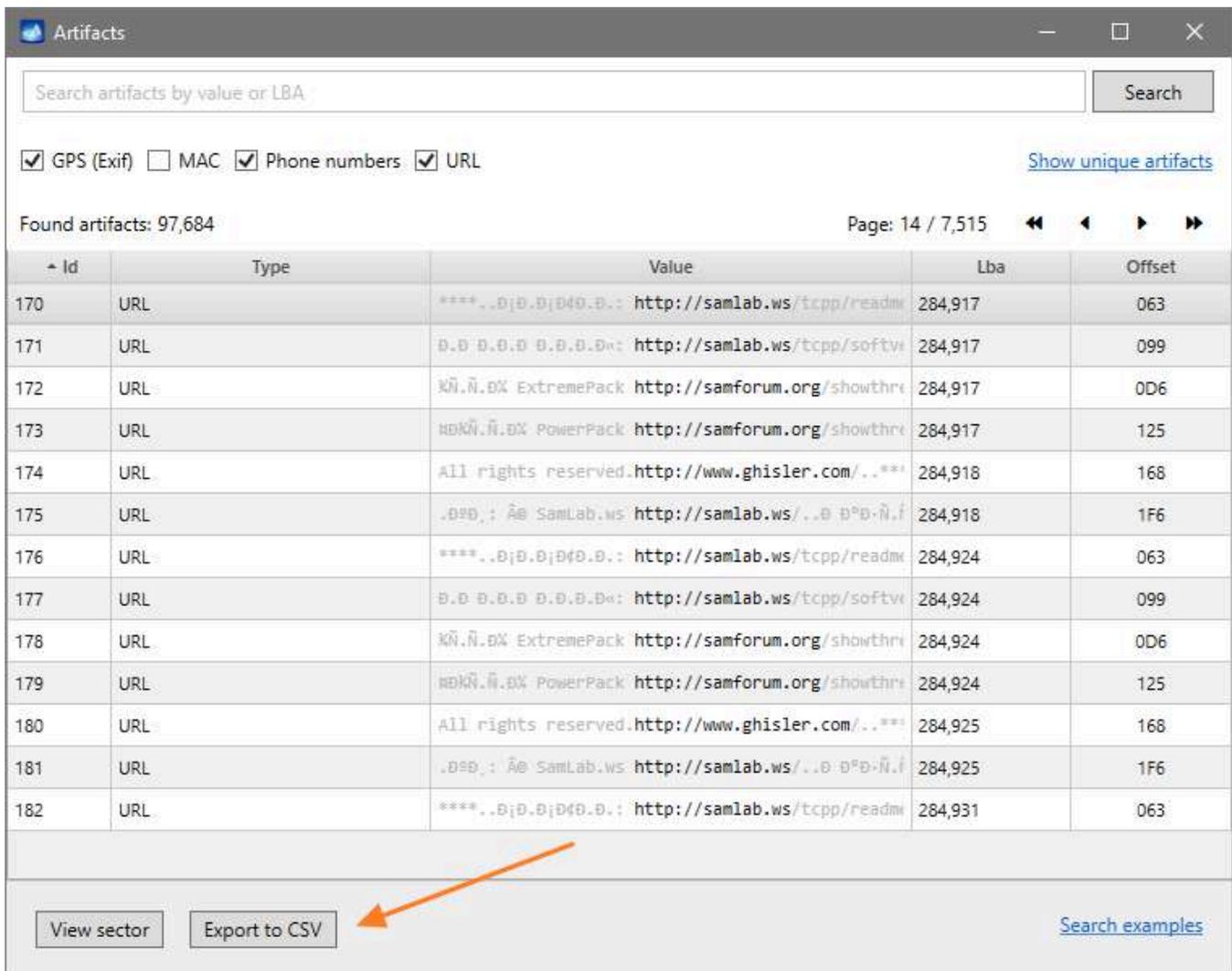
During the search, the **Export to CSV** button is disabled. You can wait until the process is completed or, should it be necessary to start analyzing the current search output with an external tool, stop it, make an export and restart the search from scratch or from the last LBA analyzed during the previous session.

To make an export:

1. Click the link with the number of artifacts found during this search.
2. On the **Artifacts** screen, select the artifacts to be exported (e.g. one or multiple artifact categories, unique artifacts or

only those fitting certain search criteria), and then click the **Export to CSV file** button.

3. Select the path for the file and click **Export**.



The screenshot shows the 'Artifacts' window with a search bar and filters. The search results table is as follows:

Id	Type	Value	Lba	Offset
170	URL	****. .BjB.BjDfB.B.: http://samlab.ws/tcpp/readm	284,917	063
171	URL	B.B B.B.B B.B.B.B: http://samlab.ws/tcpp/softv	284,917	099
172	URL	кН.Н.ВX ExtremePack http://samforum.org/showthr	284,917	0D6
173	URL	кВкН.Н.ВX PowerPack http://samforum.org/showthr	284,917	125
174	URL	All rights reserved.http://www.ghisler.com/..**	284,918	168
175	URL	.B%B,: ÅB SamLab.ws http://samlab.ws/..B B°B·Н.í	284,918	1F6
176	URL	****. .BjB.BjDfB.B.: http://samlab.ws/tcpp/readm	284,924	063
177	URL	B.B B.B.B B.B.B.B: http://samlab.ws/tcpp/softv	284,924	099
178	URL	кН.Н.ВX ExtremePack http://samforum.org/showthr	284,924	0D6
179	URL	кВкН.Н.ВX PowerPack http://samforum.org/showthr	284,924	125
180	URL	All rights reserved.http://www.ghisler.com/..**	284,925	168
181	URL	.B%B,: ÅB SamLab.ws http://samlab.ws/..B B°B·Н.í	284,925	1F6
182	URL	****. .BjB.BjDfB.B.: http://samlab.ws/tcpp/readm	284,931	063

At the bottom of the interface, there are two buttons: 'View sector' and 'Export to CSV'. An orange arrow points to the 'Export to CSV' button.

## Analyze device data on the byte level

Atola Insight Forensic lets you delve deeper than the device partitions, folders, or files and analyze the drive contents on the level of individual bytes.

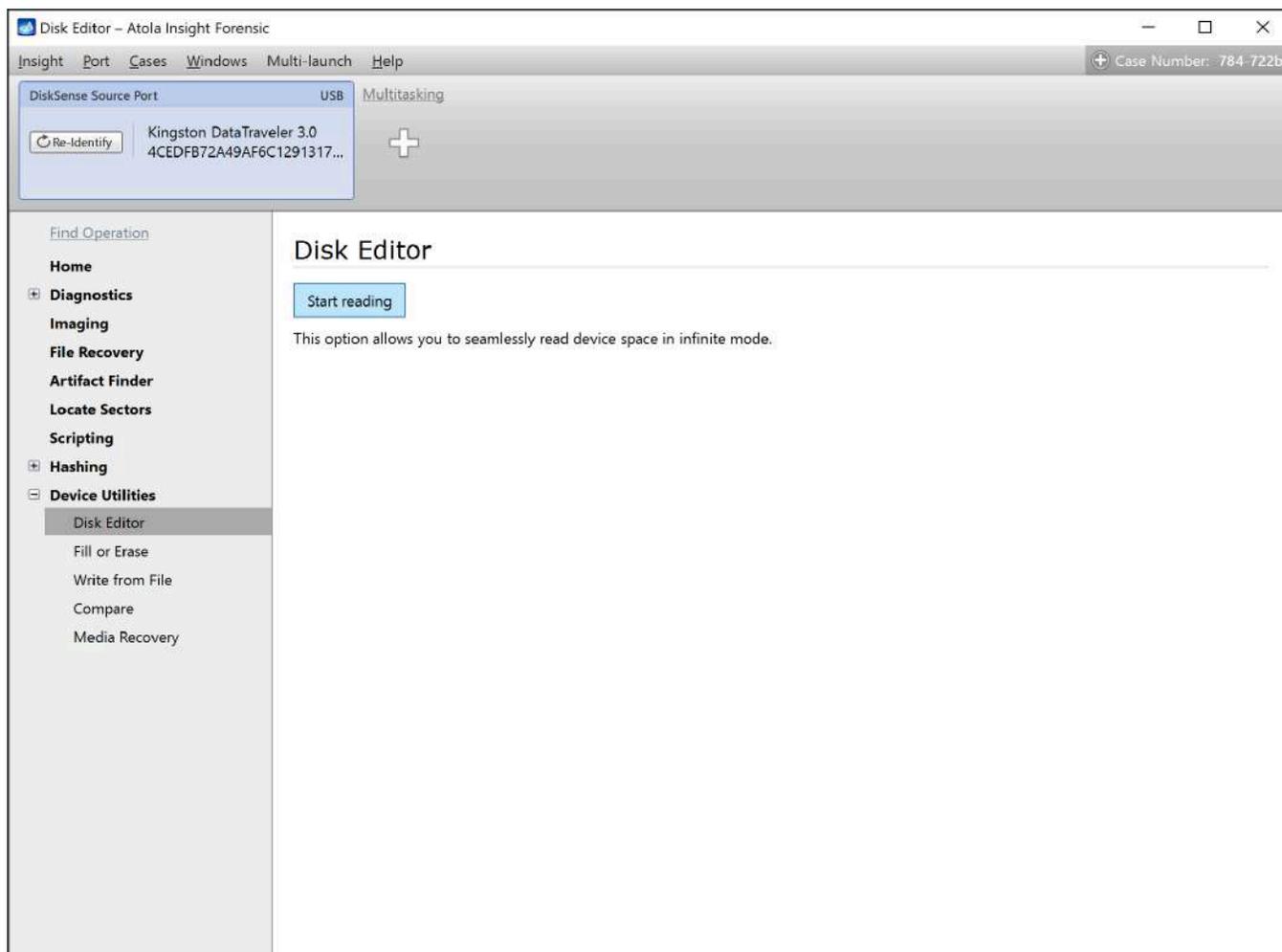
The specialized Disk Editor module makes it possible to find, read, or edit individual bytes, identify the exact location of specific sectors, automatically detect file system structures using built-in templates, search for hex strings, and convert hex values to decimal or binary format on the fly.

# Launch Disk Editor

To launch the Disk Editor module:

1. In the sidebar, go to **Device Utilities > Disk Editor**.
2. Click **Start reading**.

To prevent possible damage to an unstable media, Disk Editor won't start reading device contents without your command.



**Launching the Disk Editor module.**

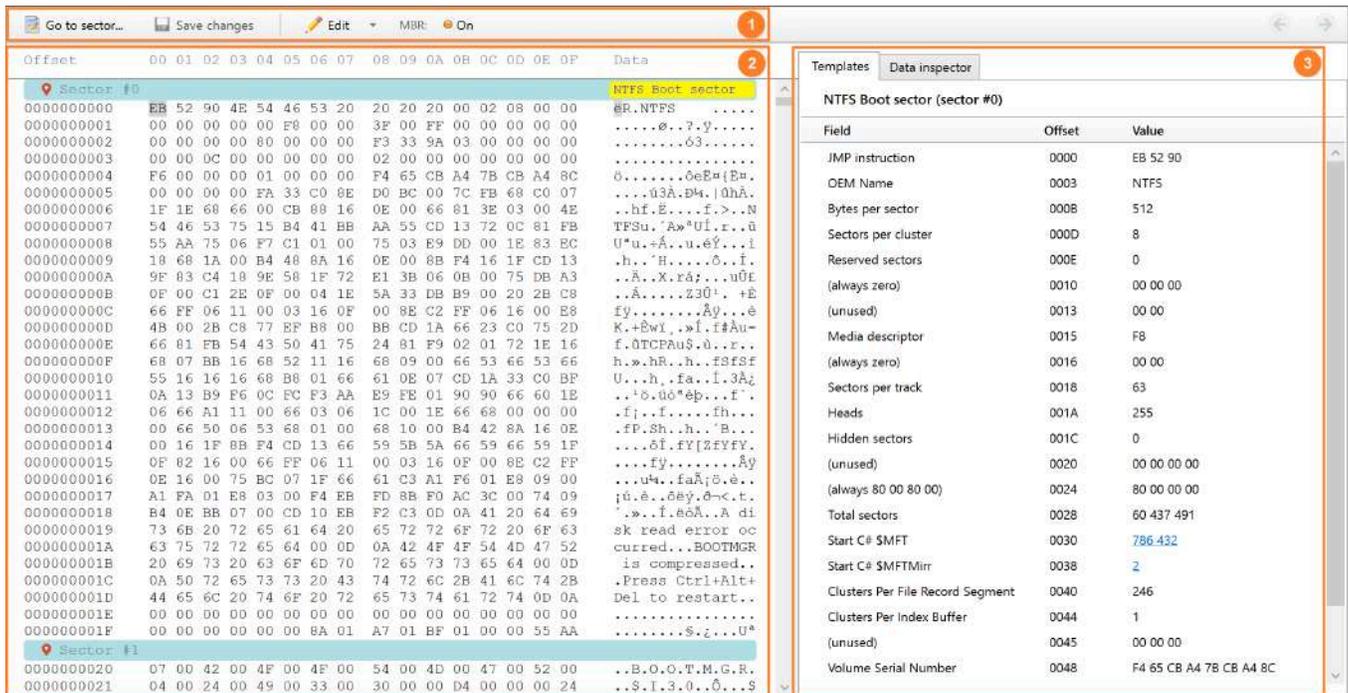
## Disk Editor screen explained

The Disk Editor screen consists of three main areas:

1. **Toolbar** provides quick access to frequently used commands, like **Go to sector** or **Save changes**.
2. **Hex viewer** shows byte-level contents of a device in the hexadecimal format:

- Left column contains hexadecimal offset values, meaning how far the byte array is from the starting sector of the drive.
- Central column presents individual bytes in the hexadecimal format.
- Right column shows corresponding values in the ASCII format.

3. **Templates and Data inspector** tabs are used to display sector metadata in a human-readable form, search for hex strings, and convert hex values to alternative formats.



**Three main areas of the Disk Editor screen: 1 - Toolbar, 2 - Hex viewer, 3 - Templates and Data inspector tabs.**

## Read sectors using Hex viewer

Insight Forensic seamlessly reads device space in infinite mode: bytes are loaded automatically as you scroll the hex viewer up or down.

To quickly jump to a certain position, click the **Go to sector** button on the toolbar or press **Ctrl+G**. Two more convenient shortcuts:

- **Ctrl+Home** immediately brings you to the first sector of a drive,
- **Ctrl+End** gets you to the last sector.

To select a single byte, click it in the central column of the Hex viewer. To select multiple bytes, click the first byte of the sequence and drag a cursor to the last byte. Insight also highlights the corresponding ASCII values in the right column.

To save selection to a file, in the toolbar, go to **Edit > Save selection to file** or press **Ctrl+Shift+S**.

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Data
	Sector #0																NTFS Boot sector
000000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS .....
000000001	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	00	00	00	.....ø...?.ÿ.....
000000002	00	00	00	00	80	00	00	00	F3	33	9A	03	00	00	00	00	.....ó3.....
000000003	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00	.....
000000004	F6	00	00	00	01	00	00	00	F4	65	CB	A4	7B	CB	A4	8C	ø.....ðeËª(Ëª.
000000005	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	...ú3À.Ð¼.  úhÀ.
000000006	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë....f.>..N
000000007	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A»ªUÍ.r.ú
000000008	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ...î
000000009	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'H.....ò..í.
00000000A	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	..Ä..x.rá;...uÛ£
00000000B	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È
00000000C	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....Äÿ...è
00000000D	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwí. »Í.f#Äu-
00000000E	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.úTCPAU\$.ù..r..
00000000F	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.»hR..h..fSfSf
000000010	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h..fa..Í.3À¿
000000011	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..¹ò.úóªép...f'.
000000012	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.fj..f.....fh...
000000013	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..`B...
000000014	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	....ðÍ.fY[ZfYfY.

**Locate sector:** To find the exact location of a specific sector, click on the sector number with a red pin. Insight detects which files and partitions the sector belongs to and shows the detailed information about the location.

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Data
00633493BE	7F	D0	0F	AB	50	05	F9	E6	E6	35	48	04	A0	3D	EB	F1	.Ð.«P.ùæª5H. =ëñ
00633493BF	F1	79	70	FC	7B	EF	FB	F1	57	AF	A4	AA	54	B5	67	3B	ñÿpü{iúñWªªTug;
	Sector #52012190																
00633493C0	CE	6C	EC	D6	8F	5B	93	CD	E8	DC	3A	37	12	C2	97	85	îliö. [. íeù:7.Á..
00633493C1	36	DB	02	9D	E6	31	90	5F	CB	4B	22	FC	C3	33	7C	23	6Û..æ1. ÈK"úÃ3 #
00633493C2												9C	0A	69	B3	CA	T.;£.?.6.ý...iªÈ
00633493C3												1F	4B	A9	B6	2D	ÙeÁª;Ûµ..J .K@¶-
00633493C4												3D	C1	78	3A	86	HUU .JðZÒ.ª=Áx:.
00633493C5												A5	DD	6C	3E	D1	.xSÀ © .Ä."ýÝ1>Ñ
00633493C6												21	BA	7A	EC	CA	-g. ß.6n5Û.!ºziÈ
00633493C7												AA	77	6B	6C	E0	.ð1.Yò`\$s6ñªwklà
00633493C8												3E	1F	29	94	77	a;yòª.\$i@2J>.) .w
00633493C9												F9	5A	52	A6	A7	ý ¶£HJÈAxH.ùZR S
00633493CA												3B	C8	82	77	50	Z.ä.ª.ðñZª;È.wP
00633493CB												B6	28	8D	45	BA	?0E»2bçEª.S¶(.Eª
00633493CC												8B	82	5F	54	E6	.pMøÈª GÈ#...Tæ
00633493CD												A1	3F	BB	A2	24	BÄ.ðu1.è.ÄÛ;?ªç\$
00633493CE												05	3D	7D	91	1B	.Nclª?y..àL.=) ..
00633493CF												59	E8	BD	4F	EA	»{Z...9v+ÍVYèªOè
00633493D0												AC	C0	16	CA	1E	?1+ªj .hòø.-À.È.
00633493D1												DD	B2	B3	4C	C8	Ðv..M"£úÑæ2ÝªªLÈ
00633493D2												88	29	D4	1B	86	Ñ¶úÍ=E's."`.)ò..
00633493D3												EC	DD	EC	29	EB	Se+.í¶LÈª-íÝi)è
00633493D4												20	AF	35	36	2D	+.(÷im.ª)k.ª56-
00633493D5												AB	9C	02	BD	A5	41 44 DB 22 1D 65 FF 57 E5 1F 6B
00633493D6												35	46	2F	9F	F6	BA 13 9C 5C 41 CC E1 33 51 9D 11

**Location information**

Sector: 52 012 190

Location: File

Path: \Movies\IMDB-Top250\

FileName: Godfather II.avi

Partition: Kingston

Size: 3 GB

Created Date: 09.08.2011 19:05:00

Access Date: 15.04.2023 19:07:45

Modify Date: 10.08.2011 20:41:22

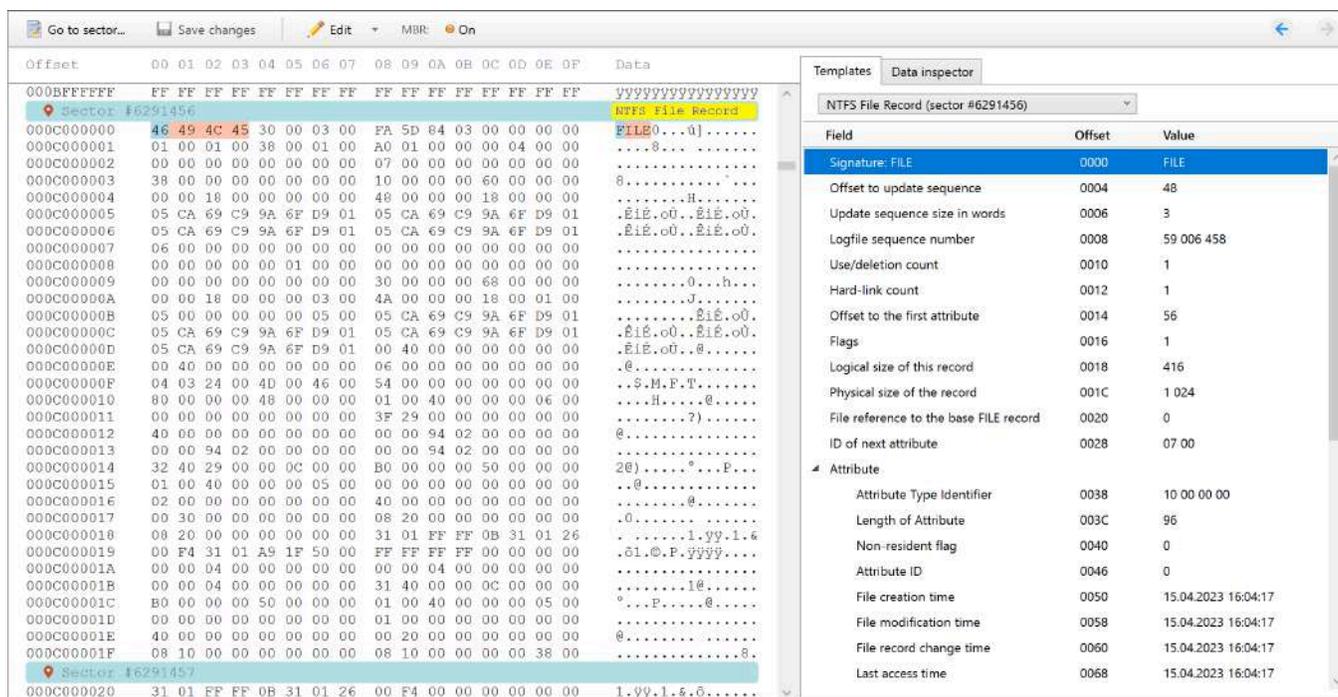
Close

# Examine file system structures

After you launch Disk Editor, it detects file system structures automatically and shows known metadata in a human-readable form on the **Templates** tab.

When you click a field in the **Templates** tab, Insight highlights the corresponding byte sequence in the **Hex viewer**.

Navigate through file system structures using a drop-down list at the top of the **Templates** tab or Back and Forward arrow buttons in the top right corner of the Disk Editor screen.



**The Templates tab contains file system metadata in a human-readable form.**

Supported metadata structures:

## Edit sector contents

As its name suggests, Disk Editor lets you modify any sector contents. You can edit individual bytes directly in the Hex viewer or paste the previously saved byte sequence from a file.

To edit a byte directly, select it in the Hex viewer and enter a new value. You can use standard **Copy** (*Ctrl+C*) and **Paste** (*Ctrl+V*) commands as well.

To paste the previously saved byte sequence from a file, in the toolbar, select **Edit > Paste from file** or press *Ctrl+Shift+V*.

Modified bytes are colored red.

To revert the last changes, use standard **Undo** (*Ctrl+Z*) and **Redo** (*Ctrl+Y*) commands in the **Edit** menu.

To write modified data, click **Save changes** on the toolbar or press *Ctrl+S*.

**MBR On/Off** button on the toolbar is used in data recovery cases. It swaps the last two bytes of MBR sector #0 to disable partition scanning by Windows.

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Data
000000017F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
<b>Sector #12</b>																	
0000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000181	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000182	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000183	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000184	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000185	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000186	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000187	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000188	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000189	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000018A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000018B	00	41	74	6F	6C	61	20	49	6E	73	69	67	68	74	00	00	.Atola Insight.
000000018C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000018D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000018E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000018F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000191	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000193	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

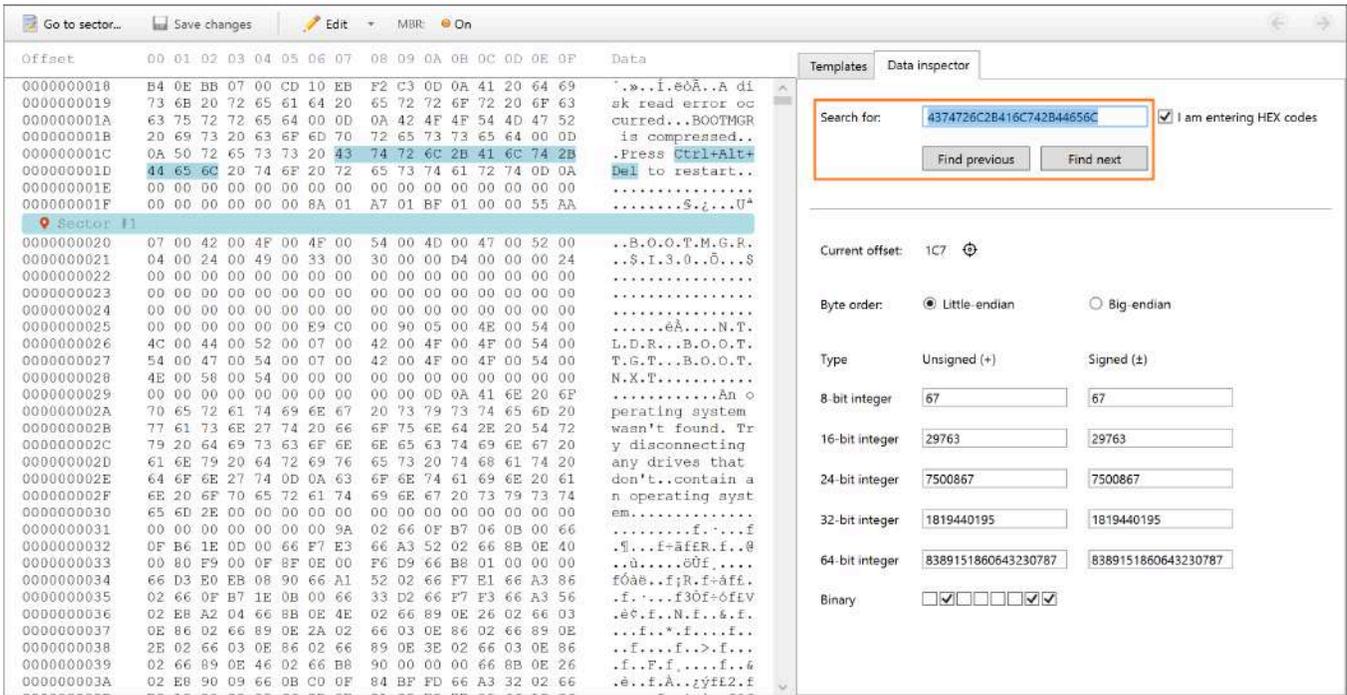
## Search for a string or byte sequence

To quickly find a certain byte sequence, go to the **Data inspector** tab or press *Ctrl+F* shortcut and enter a string you are searching for.

If you search the data in the hexadecimal format, select the **I am entering HEX code** option.

Insight highlights the found string in the Hex viewer.

Use **Find previous** and **Find next** buttons to cycle through found byte sequences.



Searching for a hex string in the Disk Editor module.

## Interpret bytes with Data inspector

Understand bytes quicker thanks to the Data inspector feature. It converts hex value to decimal (8-, 16-, 24-, 32-bit integer) or binary format on the fly.

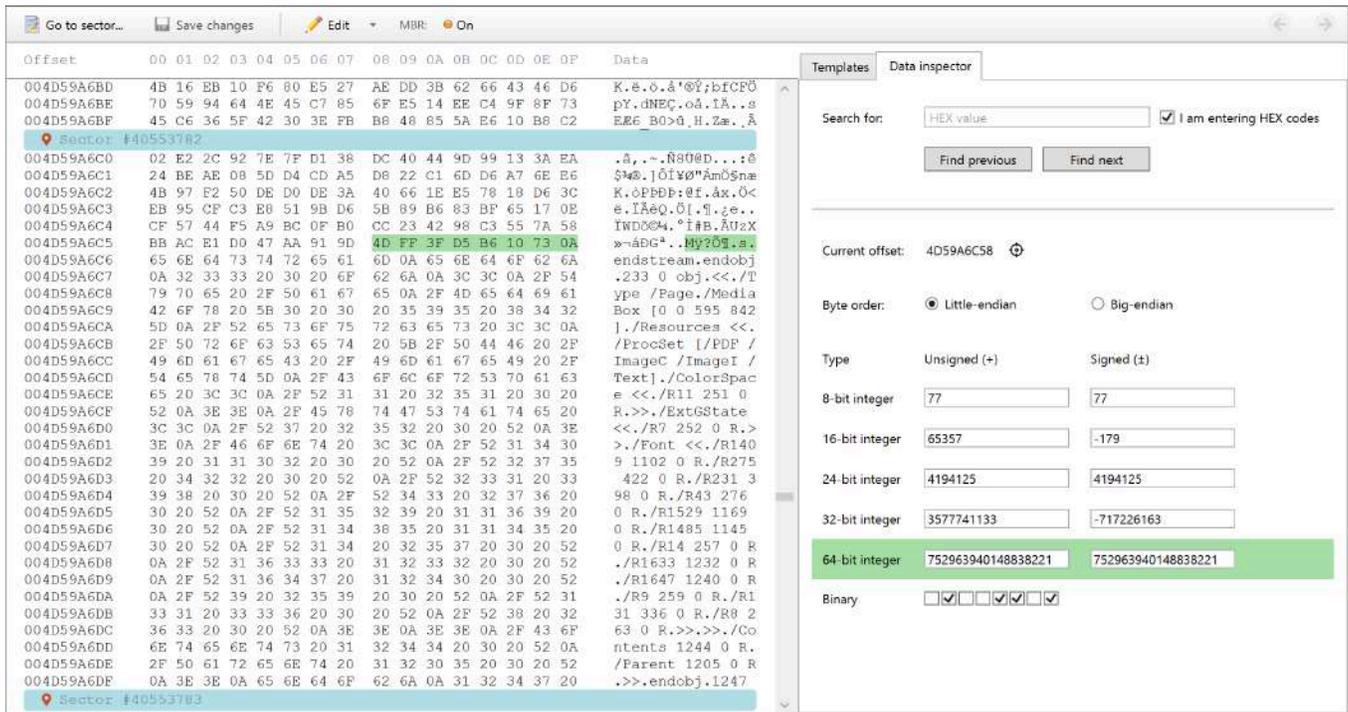
Change bytes by entering new values in the respective fields or by selecting or deselecting bits in the Binary format.

**Current offset:** shows the selected byte position relative to the first sector of the device.

**Byte order:** switches byte order between Little-endian and Big-endian modes.

**8-, 16-, 24-, 32-bit integer:** shows selected byte(s) in the respective decimal format.

**Binary:** shows the first selected byte in the binary format.



**Data inspector feature in the Disk Editor module.**

## Disk Editor keyboard shortcuts

### Navigation and search

Go to sector	Ctrl+G
Scroll one screen up	Page Up
Scroll one screen down	Page Down
Jump to the first sector	Ctrl+Home
Jump to the last sector	Ctrl+End
Find a string	Ctrl+F

### Editing

Undo	Ctrl+Z
Redo	Ctrl+Y
Copy	Ctrl+C
Paste	Ctrl+V
Save selection to file	Ctrl+Shift+S
Paste from file	Ctrl+Shift+V
Save changes	Ctrl+S

## Locate sectors

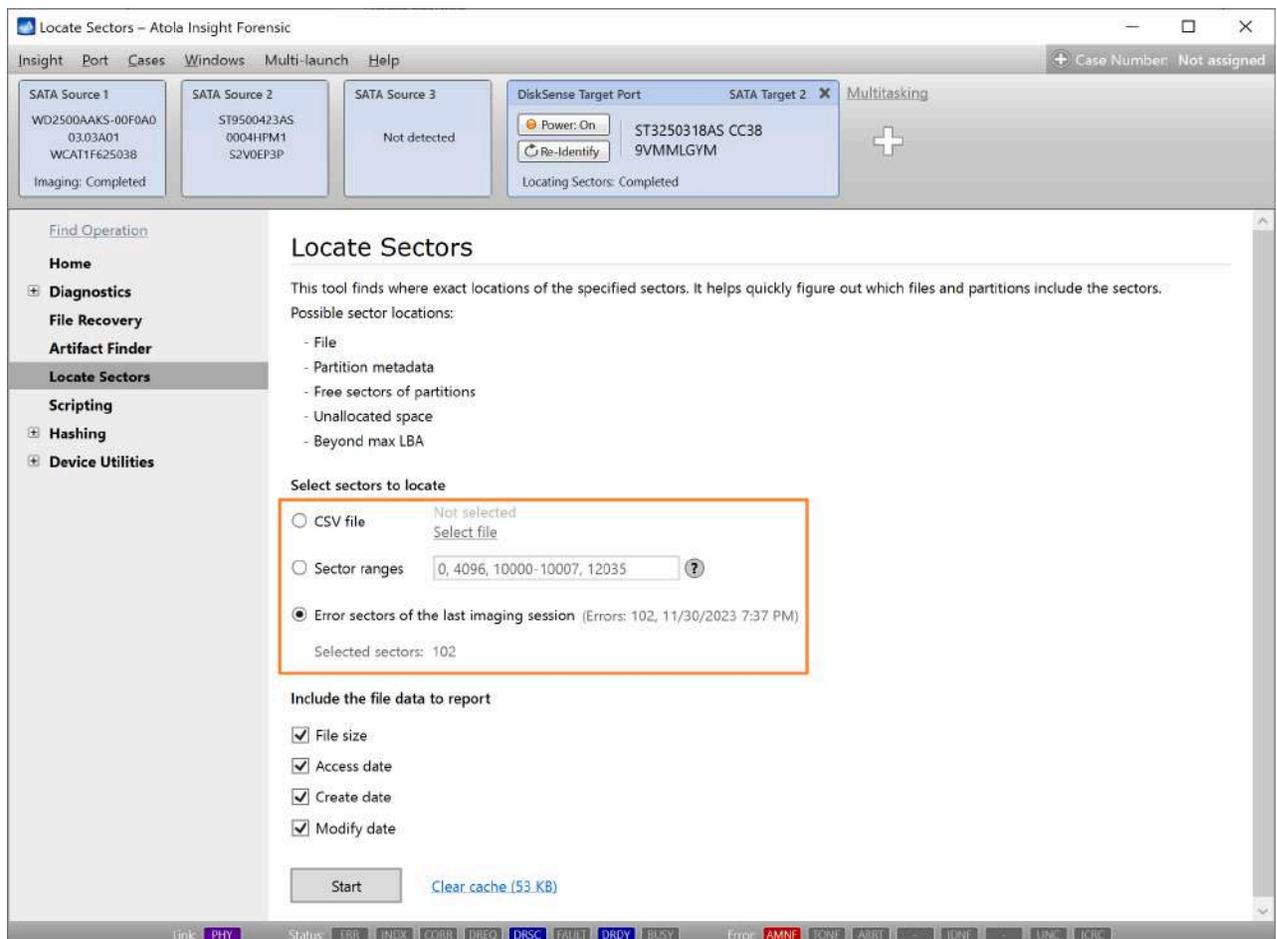
The [Locate Sectors](#) functionality helps find the exact location of specific sectors to detect which files and partitions they belong to.

You can launch the **Locate sectors** operation from the Sidebar. Alternatively, select it as an option to identify bad sectors belonging to the file system when you get the **Imaging Results** report which contains errors.

## How to quickly locate sectors

To run **Locate sectors** as a separate operation, follow these steps:

1. In the Sidebar, click **Locate Sectors**.
2. Select sectors to locate, using one of the following options:
  - **CSV file:** select a CSV file, which contains comma-separated sector ranges.
  - **Sector ranges:** enter comma-separated individual sector numbers (for example: *501, 607*) or sector ranges (for example: *1000-2000*).
  - **Error sectors of the last imaging session:** this option is available if you are locating sectors on a target that contain an image of a drive that had bad sectors.



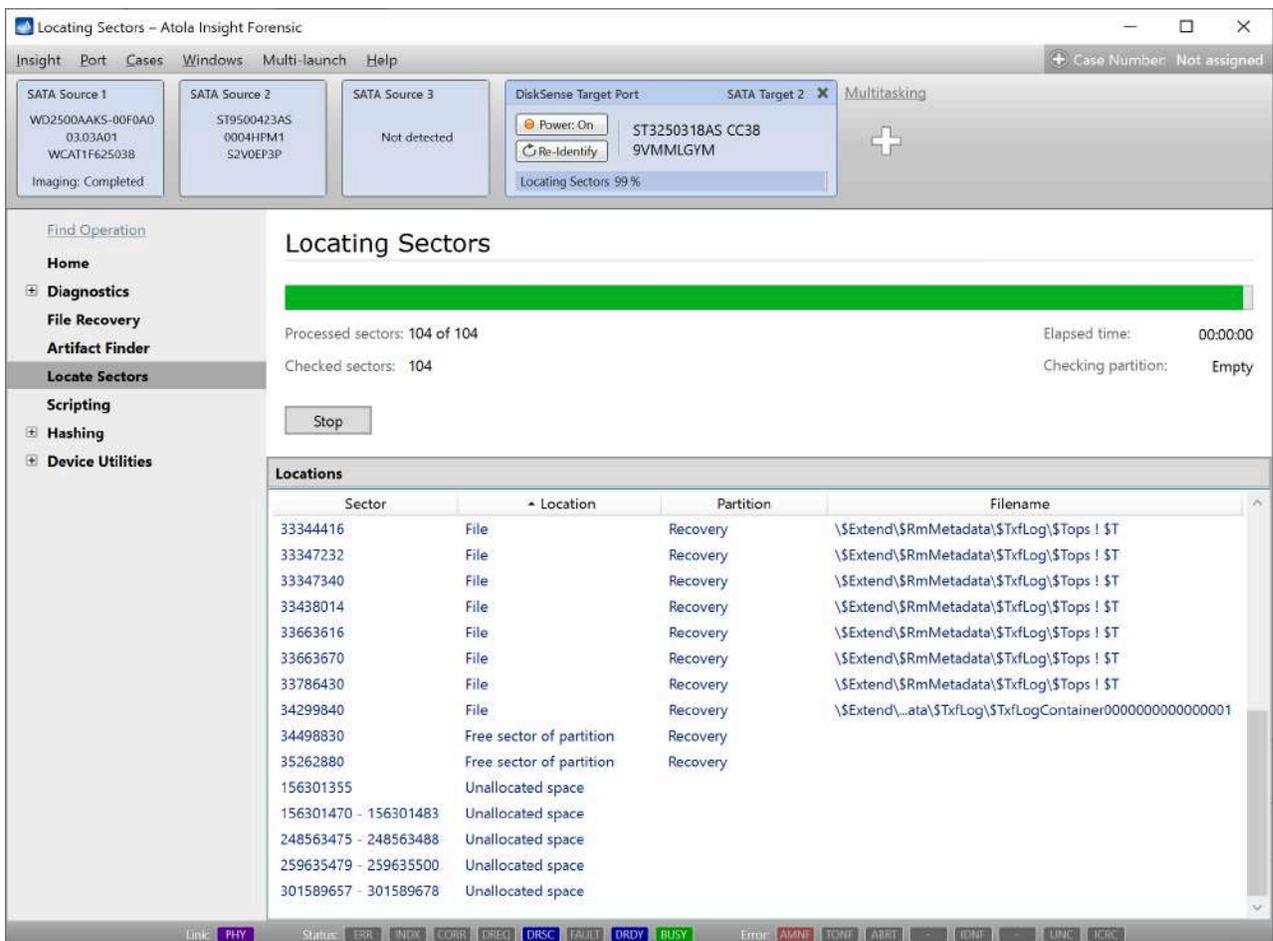
3. Select the file data you'd like to see in the report:

- File size
- Access date
- Create date
- Modify date

4. **Optional:** Insight caches files to speed up the analysis of the sector location. If the cache takes too much space in your Insight work folder, click the **Clear cache** link at the bottom.



5. Click the **Start** button. Insight immediately begins locating the sectors.



6. After processing all the scheduled sectors, Insight generates a report listing where the sectors have landed in relation to individual files and the file system as a whole.

**Located Sectors**

Elapsed time: 00:00:00

Processed sectors: 104 of 104

Files: 97

Free sectors of partitions: 2

Unallocated space: 5

Partition metadata: 0

Beyond max LBA: 0

Not supported file system: 0

Not valid file system: 0

Encrypted file system: 0

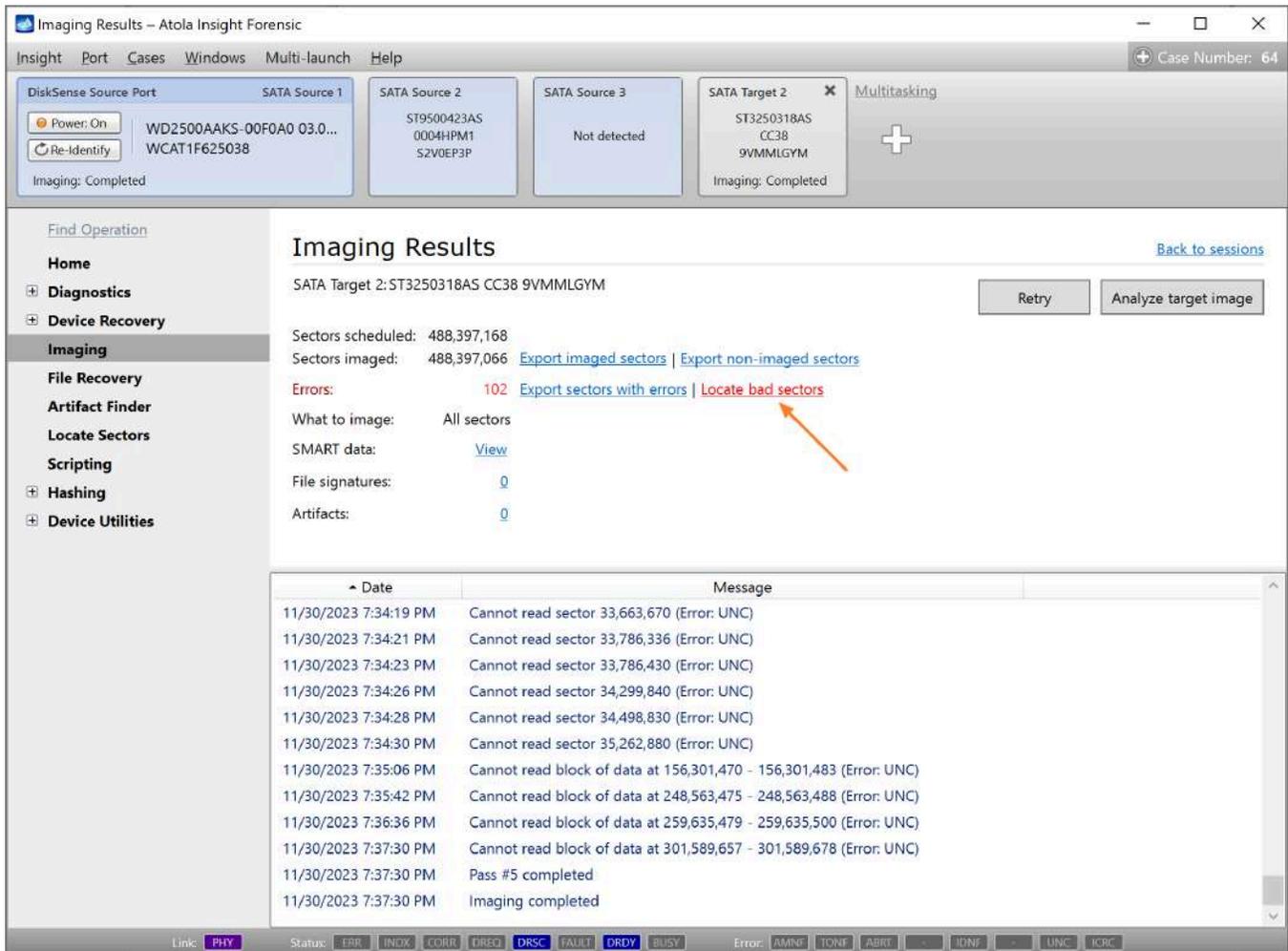
**Results:** [C:\Atola Insight Forensic\Work 4 15\Not Assigned\ST3250318AS\\_CC38\\_9VMMLGYM\LocateSectorslog0.csv](C:\Atola Insight Forensic\Work 4 15\Not Assigned\ST3250318AS_CC38_9VMMLGYM\LocateSectorslog0.csv)

Sector	Location	Partition	Filename
33786430	File	Recovery	\\$Extend\\$\RmMetadata\\$\TxfLog\\$\Tops ! \$T
34299840	File	Recovery	\\$Extend\...ata\\$\TxfLog\\$\TxfLogContainer0000000000000001
34498830	Free sector of partition	Recovery	
35262880	Free sector of partition	Recovery	
156301355	Unallocated space		
156301470 - 156301483	Unallocated space		
248563475 - 248563488	Unallocated space		
259635479 - 259635500	Unallocated space		
301589657 - 301589678	Unallocated space		

## Locate bad sectors in the Imaging Results report

After an imaging session is completed, Insight generates the **Imaging Results** report. If Insight runs across bad sectors, it reflects them in the report and the operator is offered a few options for working with bad sectors.

To detect which files and partitions these bad sectors belong to, launch the [Locate sectors](#) operation by clicking the **Locate bad sectors** link.

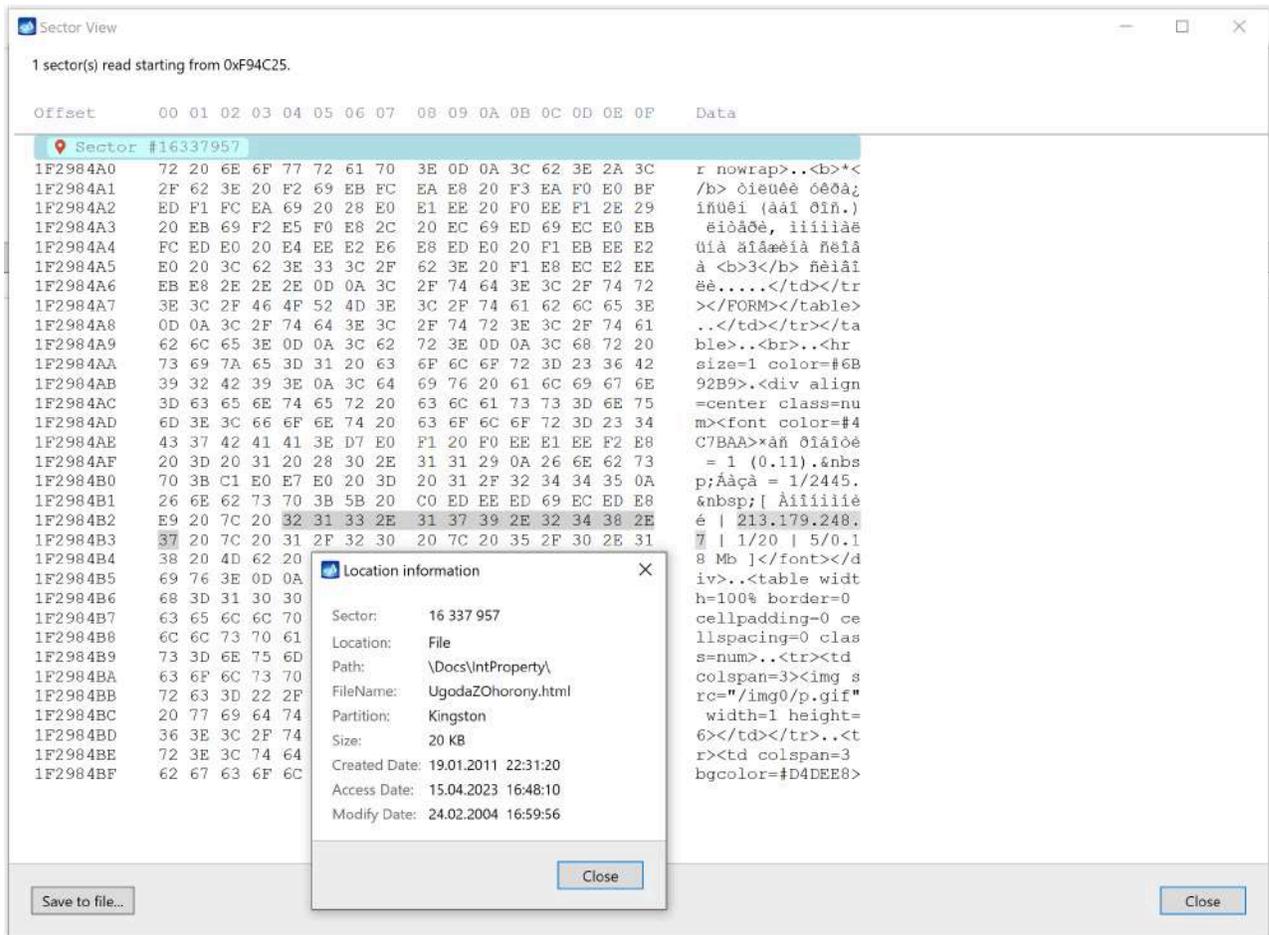


## Locate sectors in the HEX viewer

The HEX viewer is integrated into a few modules of Insight: [Artifact Finder](#), [Disk Editor](#) and File Signatures.

To use the HEX viewer for analyzing to which file on the drive a found artifact belongs, do the following:

1. In the Sidebar, click **Artifact Finder**.
2. Set the parameters of your search and start the process. For guidance, see [Search for artifacts](#).
3. Whether the search is ongoing or finished, you can start examining the output of the found artifacts in the table: filter, sort, and search for individual artifacts.
4. By double-clicking on an artifact, you open the **Hex viewer** window/tab, which shows the artifact within the sector where it was found.
5. To find the file to which this sector belongs, click the red pin icon next to the sector number.



Similarly, you can look up how a signature encountered during imaging relates to the file system.

If the imaging has been completed: look up the signature list in the imaging report and then on an individual signature, this will open the HEX viewer window. By clicking the red pin icon in the sector view, you will see which file the found signature belongs to.

If the artifact does not belong to a file, it may be remnants of the data of a file deleted by the user.

## Unclip or change HPA, DCO, or AMA restrictions

HPA (host protected area), DCO (device configuration overlay), and 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). Sometimes they use it for refurbished drives.

But it was 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 Insight Forensic can detect, unclip, or change HPA, DCO, and AMA limitations.

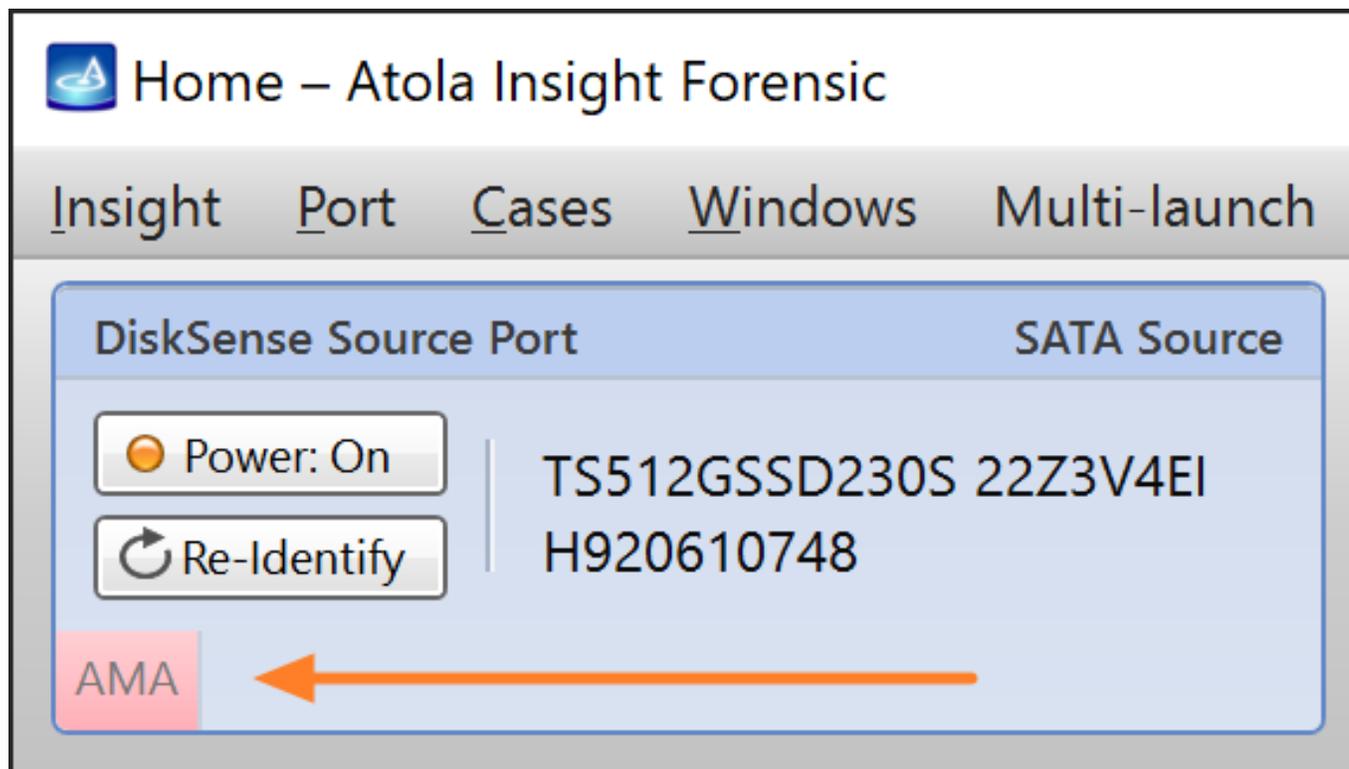
The DCO and HPA can co-exist on the same drive: max address limited via HPA should be less than DCO.

AMA is supported by new drives and can't exist if DCO or HPA is supported, and vice versa.

## Detect HPA, DCO, or AMA restrictions

When you connect a hard drive to the DiskSense unit, in addition to the standard **Identify device** command, Atola Insight Forensic automatically sends commands to look up the drive size as set in the drive's firmware.

If drive size is limited by HPA, DCO, or AMA, Insight draws attention to these changes by adding corresponding red indicators to the DiskSense Source Port.



The screenshot shows the Atola Insight Forensic software interface. At the top, there is a navigation bar with the following items: **Insight**, **Port**, **Cases**, **Windows**, and **Multi-launch**. Below this, a panel titled **DiskSense Source Port** is visible. On the left side of this panel, there are two buttons: **Power: On** (with a power icon) and **Re-Identify** (with a refresh icon). To the right of these buttons, the drive's model and serial numbers are displayed: **TS512GSSD230S 22Z3V4EI** and **H920610748**. In the bottom-left corner of the panel, there is a red box labeled **AMA**. A large orange arrow points from the **AMA** box towards the drive information, indicating that the drive is affected by AMA restrictions.



# Home – Atola Insight Forensic

Insight Port Cases Windows Multi-launch

DiskSense Source Port

SATA Source

Power: On

Re-Identify

ST1000LM024 HN-M101M...  
S32XJ9EDC03827

HPA DCO



To get more details about the modifications that have been made to the drive's firmware, run **Automatic Checkup**.

Automatic Checkup finished – Atola Insight Forensic

Insight Port Cases Windows Multi-launch Help Case Number: 308

DiskSense Source Port SATA Source Multitasking

Power: On TS512GSSD230S 22Z3V4EI  
Re-Identify H920610748

AMA Auto Diagnostics: Completed

Find Operation Print... Save to file... Copy to Clipboard

Home

Diagnosics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

Imaging

File Recovery

Artifact Finder

Locate Sectors

Scripting

Hashing

Device Utilities

Monday, April 15, 2024 3:26 PM  
Report created by Atola Insight Forensic 5.5.8852.26130.

### Diagnostics report

Device model:	TS512GSSD230S	Unit IP:	10.0.1.157
Device serial:	H920610748	Unit serial:	74747474
Device firmware:	22Z3V4EI	Write protection:	On
Device size:	512 GB (512,110,080,512 bytes)	Computer:	INVESTIGATOR
Case number:	308	User:	Pasyuta
Case description:		OS:	64-bit Microsoft Windows 10 Pro Version 10.0 (Build: 19045)

#### Diagnostics results

No major hardware or firmware issues have been found.

AMA is active. To access the entire space, disable AMA.

Estimated imaging time: 16 minutes

Full Diagnostic Log

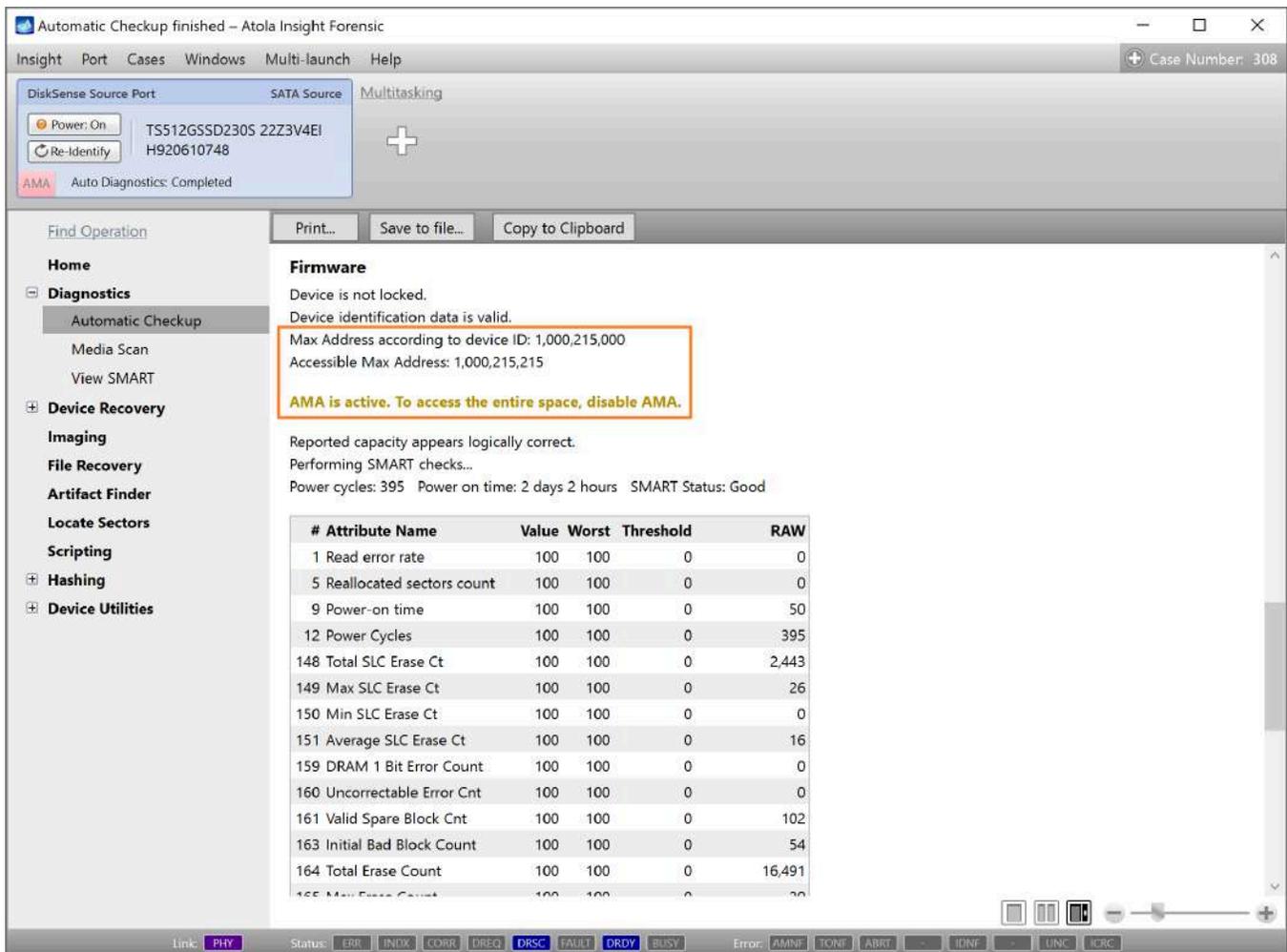
Link: PHY Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY Error: AMNF TONF ABRF IDNF UNC ICRC

## AMA limitation is indicated in the Diagnostics results.

In the **Firmware** section of the **Diagnostics report**, there are two (for AMA) or three (for HPA and DCO) of the following lines, indicating the drive's Max Address according to different records in the drive's firmware:

- 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.
- **Accessible Max Address** indicates max address ignoring AMA limitation that may have been enabled.
- **Native Max Address** indicates max address ignoring HPA limitation that may have been enabled, yet affected by DCO restriction.
- **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, DCO, or AMA activated will have the same value in all these lines.



The screenshot shows the 'Automatic Checkup finished' window in Atola Insight Forensic. The 'Diagnostics' section is expanded to 'Automatic Checkup', and the 'Firmware' section is selected. The firmware report includes the following information:

- Device is not locked.
- Device identification data is valid.
- Max Address according to device ID: 1,000,215,000
- Accessible Max Address: 1,000,215,215
- AMA is active. To access the entire space, disable AMA.**
- Reported capacity appears logically correct.
- Performing SMART checks...
- Power cycles: 395 Power on time: 2 days 2 hours SMART Status: Good

#	Attribute Name	Value	Worst	Threshold	RAW
1	Read error rate	100	100	0	0
5	Reallocated sectors count	100	100	0	0
9	Power-on time	100	100	0	50
12	Power Cycles	100	100	0	395
148	Total SLC Erase Ct	100	100	0	2,443
149	Max SLC Erase Ct	100	100	0	26
150	Min SLC Erase Ct	100	100	0	0
151	Average SLC Erase Ct	100	100	0	16
159	DRAM 1 Bit Error Count	100	100	0	0
160	Uncorrectable Error Cnt	100	100	0	0
161	Valid Spare Block Cnt	100	100	0	102
163	Initial Bad Block Count	100	100	0	54
164	Total Erase Count	100	100	0	16,491
165	Max Erase Count	100	100	0	20

## AMA restriction details in the Firmware section of the Diagnostics report.

Automatic Checkup finished – Atola Insight Forensic

Insight Port Cases Windows Multi-launch Help Case Number: Not assigned

DiskSense Source Port SATA Source Multitasking

Power: On ST1000LM024 HN-M101M...  
Re-Identify S32XJ9EDC03827

HPA DCO Auto Diagnostics: Completed

Find Operation

Home

Diagnostics

- Automatic Checkup
- Media Scan
- View SMART

Device Recovery

Imaging

File Recovery

Artifact Finder

Locate Sectors

Scripting

Hashing

Device Utilities

Print... Save to file... Copy to Clipboard

**Firmware**

Device is not locked.  
Device identification data is valid.

Max Address according to device ID: 1,953,525,000  
Native Max Address Ext: 1,953,525,100

**HPA is active. To be able to access the entire surface you need to disable HPA.**

Max Address from DCO: 1,953,525,167

**Disk capacity is limited by DCO. To be able to access the entire surface you need to reset the DCO to factory settings.**

Reported capacity appears logically correct.  
Performing SMART checks...

**SMART reports that there are defects on the media.**

Power cycles: 5277 Power on time: 124 days 20 hours SMART Status: Good

#	Attribute Name	Value	Worst	Threshold	RAW
1	Read error rate	100	100	51	32,760
2	Throughput performance	252	252	0	0
3	Spin up time	93	88	25	2,146
4	Number of spin-up times	71	71	0	29,456
5	Reallocated sectors count	252	252	10	0
7	Seek error rate	252	252	51	0
8	Seek performance	252	252	15	0
9	Power-on time	100	100	0	2,996

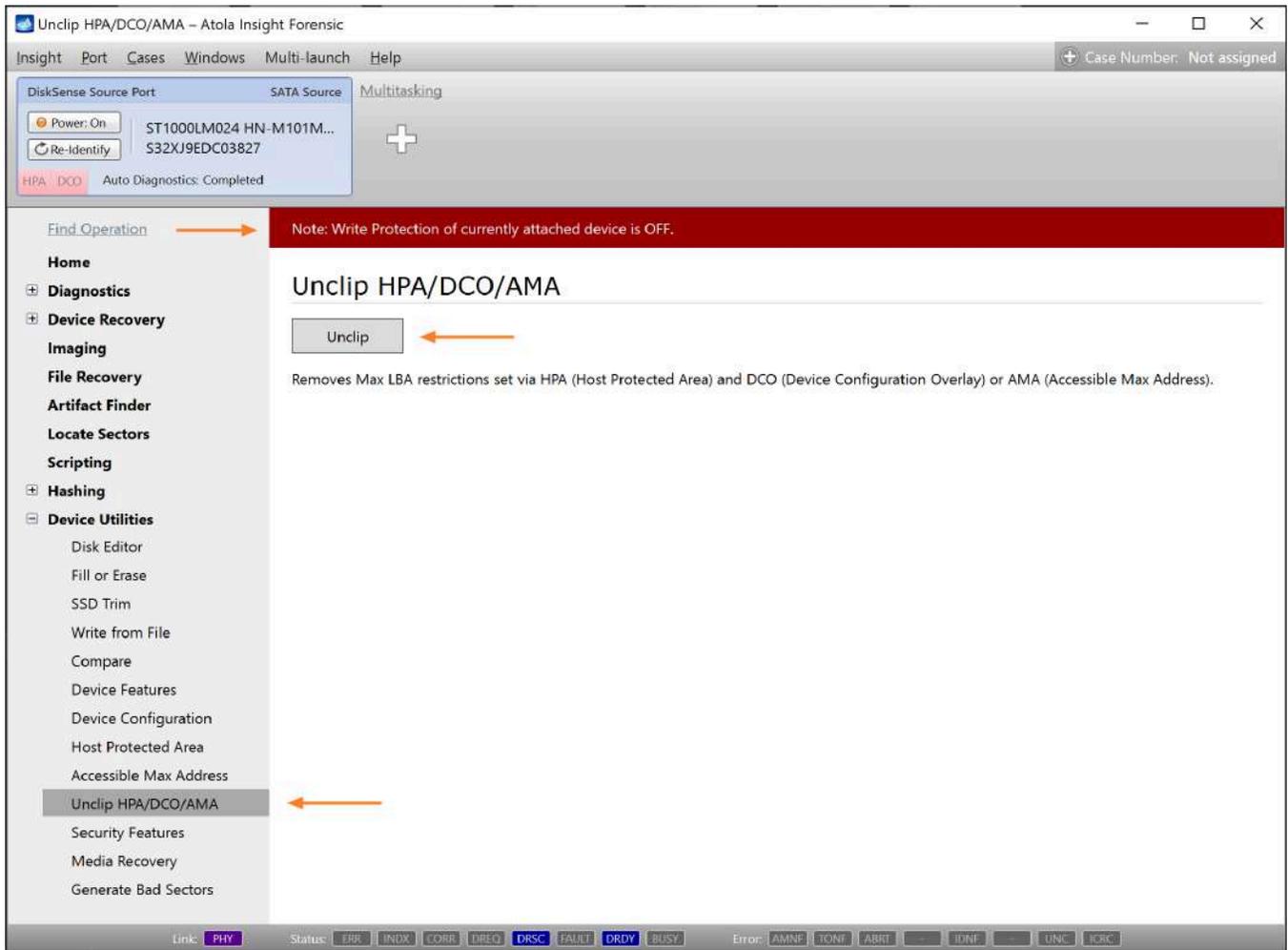
Link: PHY Status: EPR INDX CORE DREQ DRSC FAULT DRDY BUSY Error: AMNF TOM ABRT UNF UNC ICRC

**HPA and DCO restriction details in the Firmware section of the Diagnostics report.**

## Unclip HPA/DCO/AMA restrictions

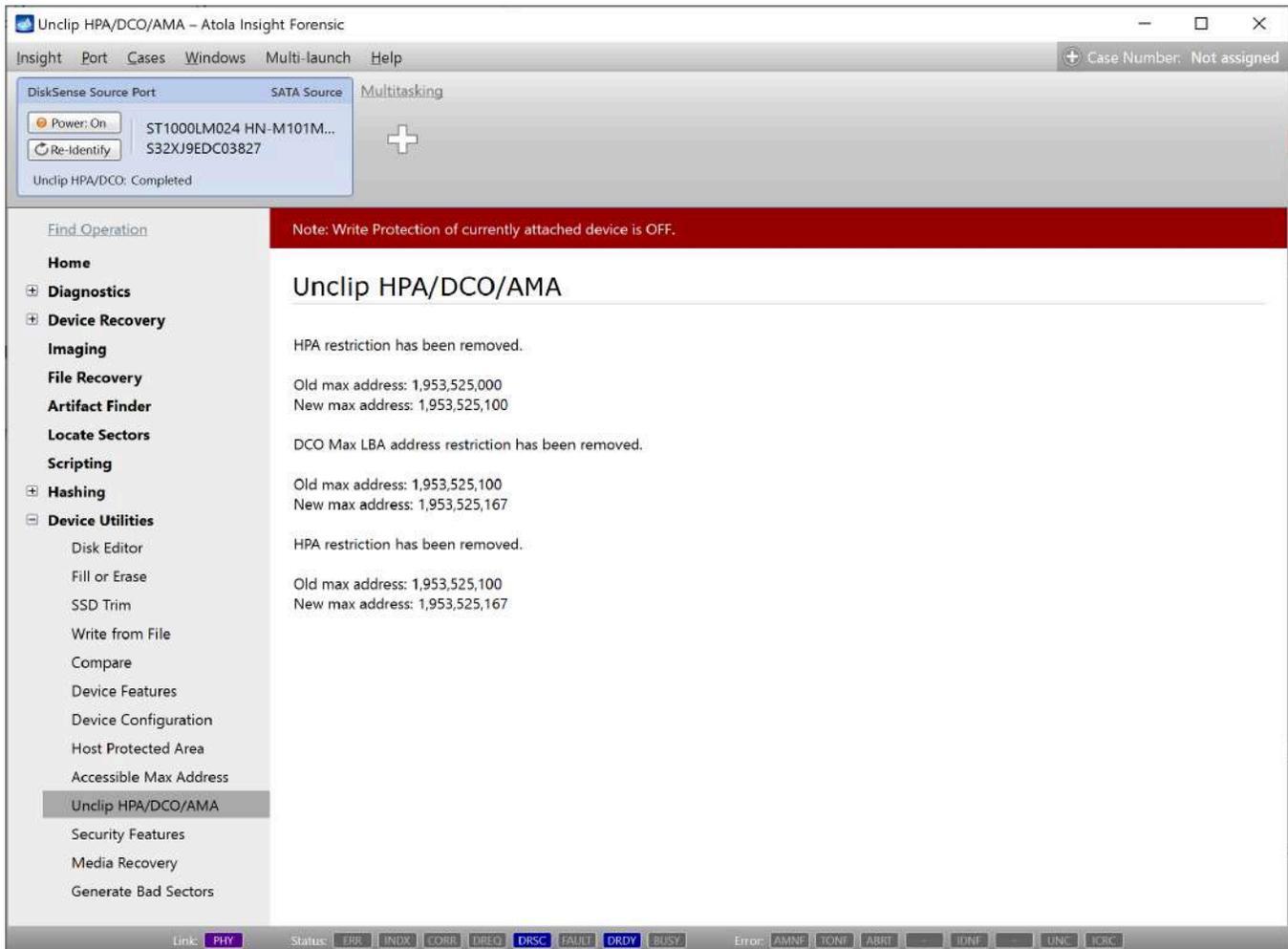
To lift any restrictions that have been applied to the drive's firmware:

- Disable **Write protection** using the physical switch situated on the front panel of the DiskSense unit. The respective LED indicator turns off. Unclipping HPA/DCO/AMA implies making changes to the drive's firmware, and Write protection won't let perform such changes.
- Go to **Device Utilities > Unclip HPA/DCO/AMA**.
- Click the **Unclip** button.



## Unclipping HPA/DCO/AMA.

Insight Forensic lifts HPA, DCO, or AMA restrictions in a matter of seconds and enables access to all data on the drive.



**HPA and DCO restrictions have been removed.**

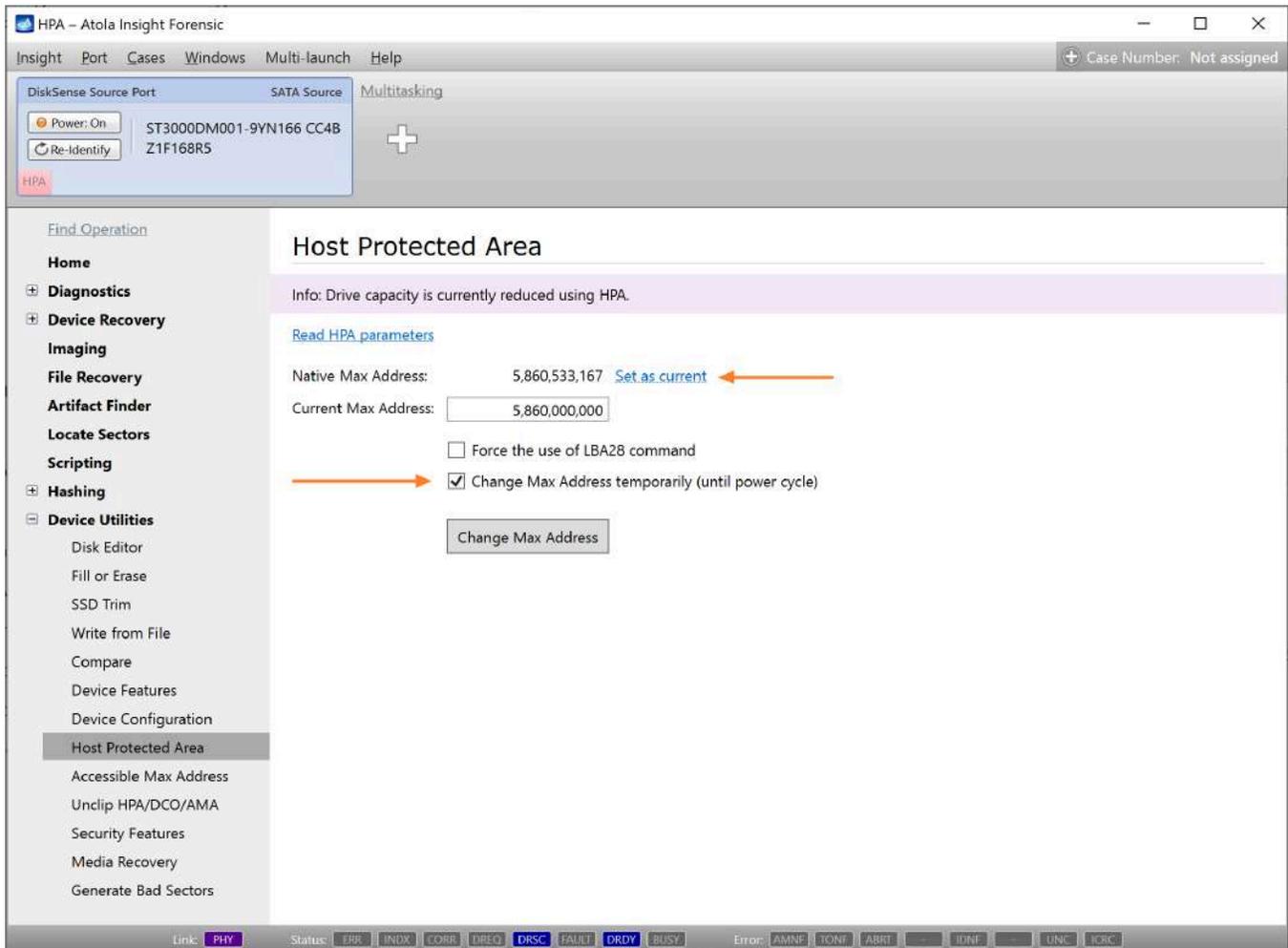
## Change HPA max address temporarily (until power cycle)

To ensure a 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 Insight Forensic 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 the next power cycle before imaging:

1. In the sidebar, go to **Device Utilities > Host Protected Area**.
2. Click the **Read HPA parameters** link.
3. Click **Set as current** to automatically change the **Current Max Address** value to that of the **Native Max Address**.
4. Select the **Change Max Address temporarily (until power cycle)** option.
5. Click the **Change Max Address** button.



### Changing HPA max address until power cycle.

This will allow access to the data in the area previously protected by HPA, yet as soon as you power off or detach the drive, the HPA will be in place again.

If the drive contains damaged areas and Insight needs to perform power cycles during imaging, such power cycles will not affect the temporarily disabled HPA: Insight will temporarily remove the HPA max address restriction after each imaging-related power cycle, and HPA will remain accessible throughout the imaging process.

For more information about imaging of freezing drives, see [Imaging freezing damaged drives](#).

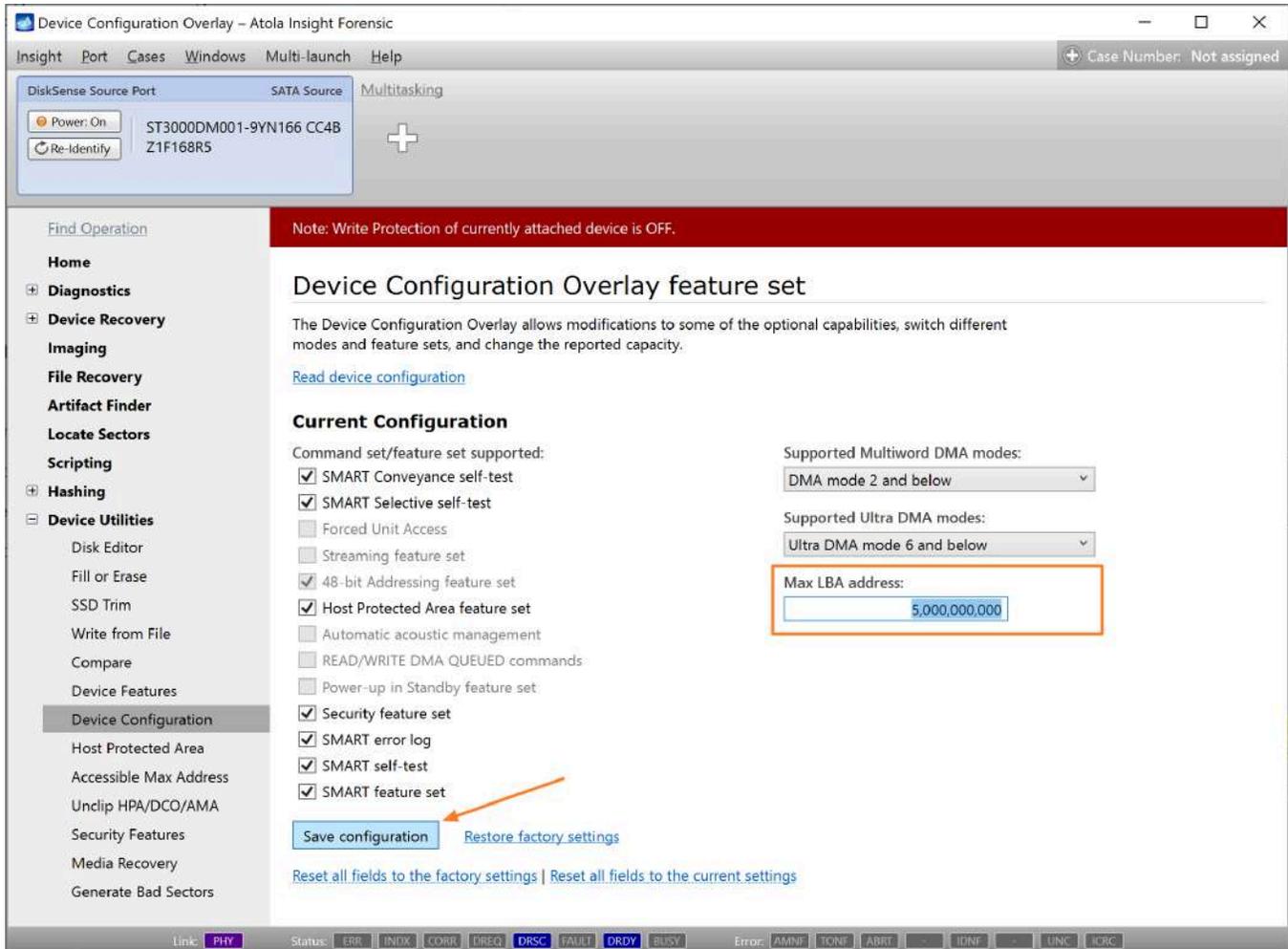
## Set or change HPA, DCO, and AMA restrictions

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. 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 restriction:

1. Disable **Write protection** using the physical switch situated on the front panel of the DiskSense unit. The respective LED indicator turns off.
2. Go to **Device Utilities > Device Configuration**.
3. Click the **Read device configuration** link.
4. Enter a new **Max LBA address**.
5. Click **Save configuration**.

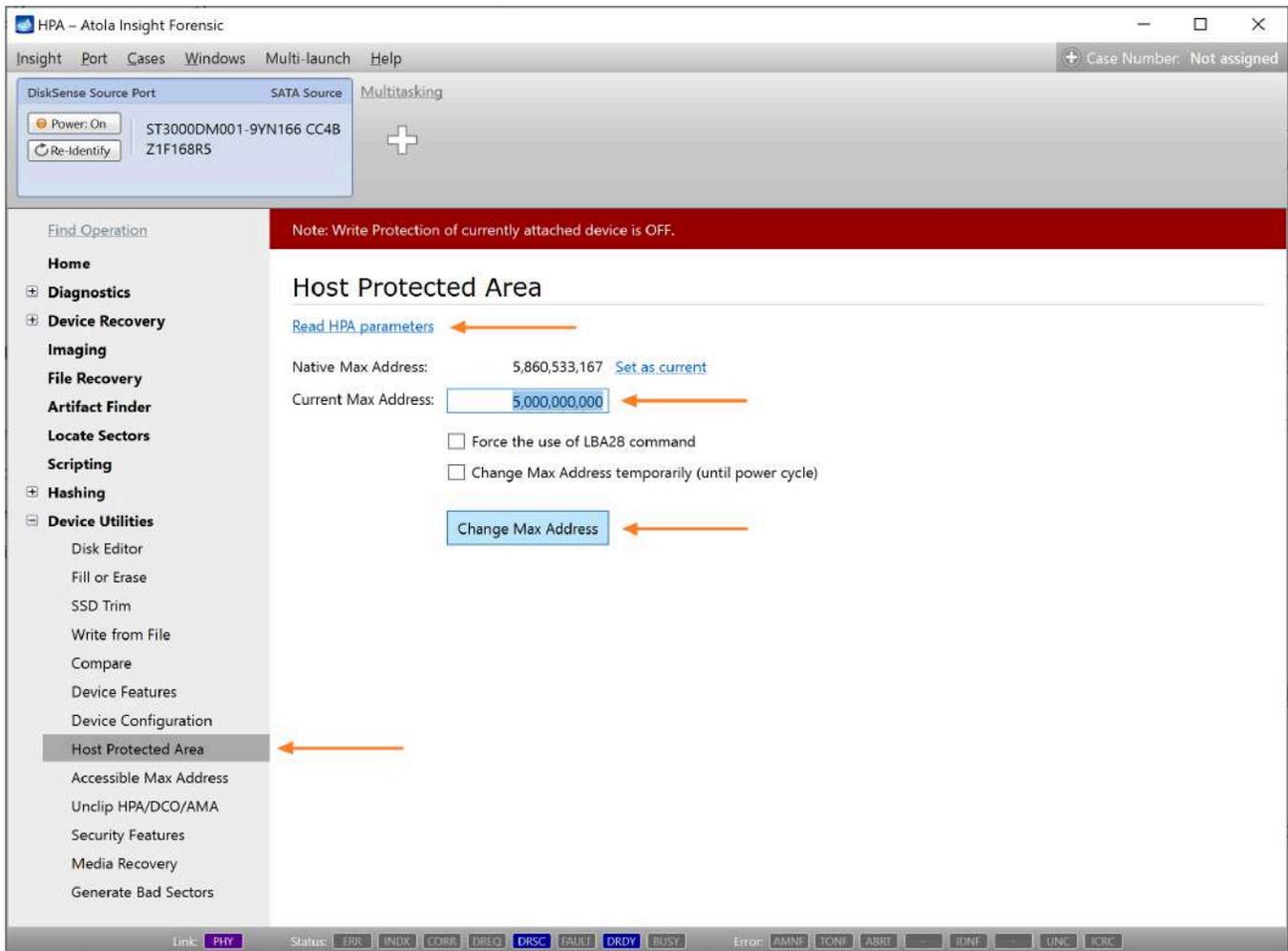


### Setting a new Max LBA address using DCO.

## To set or change HPA restriction:

1. Disable **Write protection** using the physical switch situated on the front panel of the DiskSense unit. The respective LED indicator turns off.
2. Go to **Device Utilities > Host Protected Area**.
3. Click the **Read HPA parameters** link.

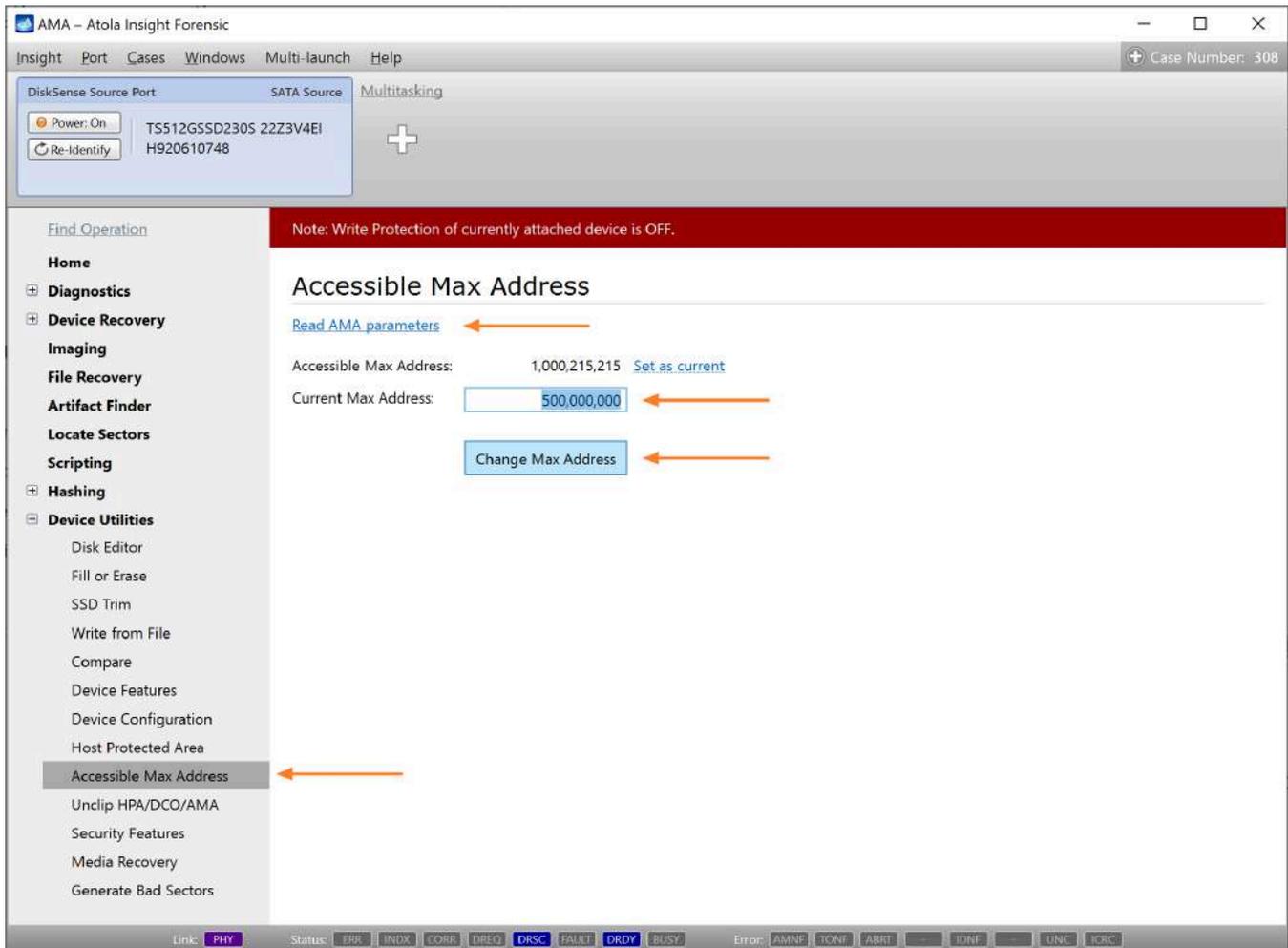
4. Enter a new **Current Max Address**. The max address limited via HPA should be less than the Max LBA address set using DCO.
5. **Optional**: Check the **Change Max Address temporarily (until power cycle)** option if needed.
6. Click the **Change Max Address** button.



### Setting a new HPA restriction.

### To set or change AMA restriction:

1. Disable **Write protection** using the physical switch situated on the front panel of the DiskSense unit. The respective LED indicator turns off.
2. Go to **Device Utilities > Accessible Max Address**.
3. Click the **Read AMA parameters** link.
4. Enter a new **Current Max Address**.
5. Click the **Change Max Address** button.



### Setting a new AMA restriction.

## Multitasking in Atola Insight Forensic

With each passing year, speed becomes a yet bigger issue for forensic specialists: while the capacity of hard drives grows exponentially, their speed does not keep up. A common 4TB drive's speed constitutes up to 200 MB/s or 12 GB/min, which translates to more than 5 hours of imaging. And it may take prohibitive amounts of time to image a drive with damaged zones. Therefore, the ability to simultaneously run different operations on several devices is more vital than ever.

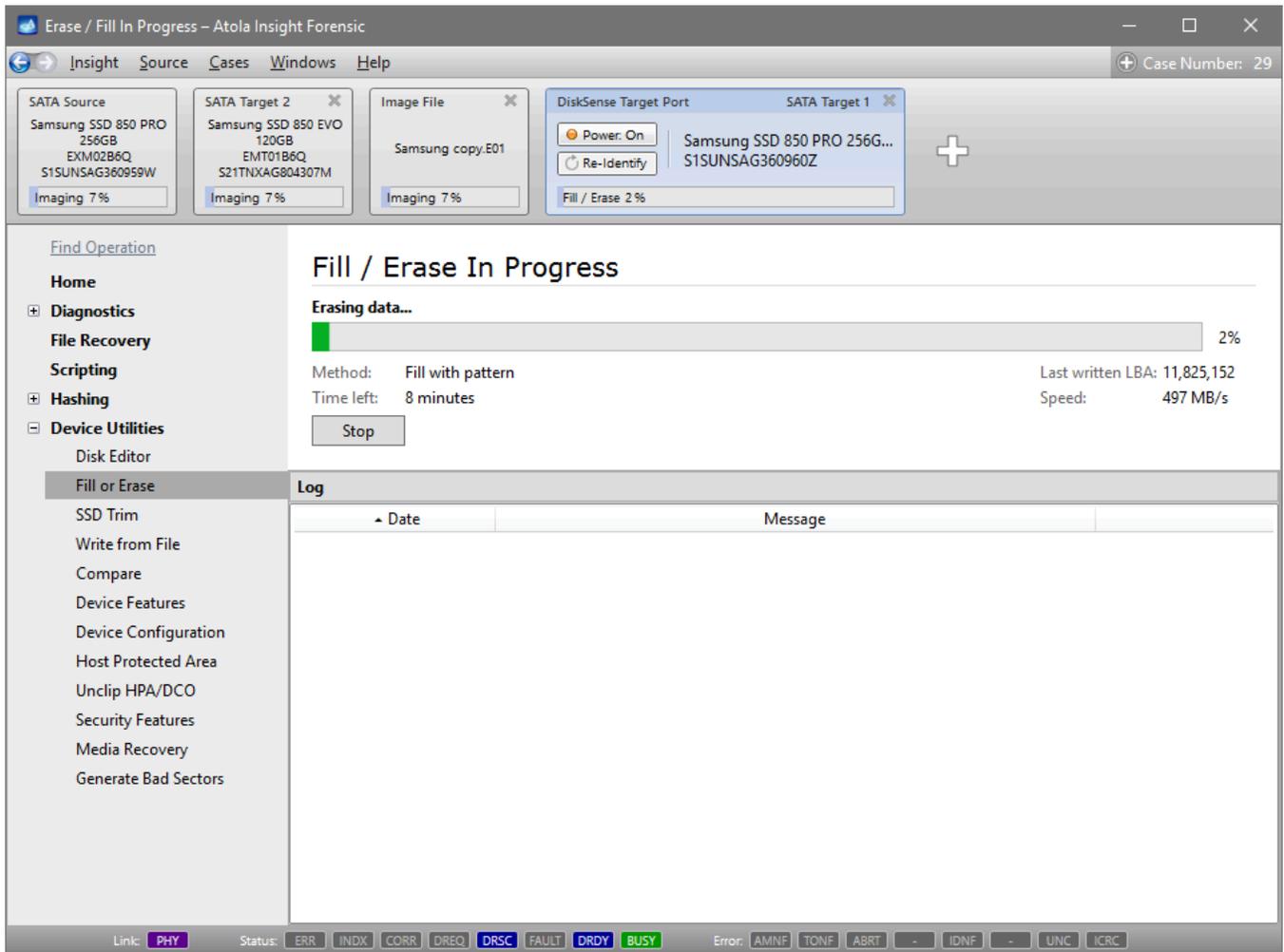
To provide users with greater productivity, Atola Insight Forensic's high-capacity multi-core CPU supports **up to 15 concurrent tasks**, that can be assigned to different drives or image files.

You can start [Imaging](#) process from a Source drive to one or multiple Target drives and/or image files. Then you can click on the **Plus** icon and open another target drive to start another operation.

The screenshot shows the Atola Insight Forensic interface. At the top, there are three panels: 'DiskSense Source Port' (SATA), 'SATA Target 2' (Samsung SSD 850 EVO), and 'Image File' (Samsung copy.E01). A red arrow points to a plus sign icon to the right of the 'Image File' panel. Below these panels is a progress bar for 'Imaging data to 2 targets...' at 2% completion. The progress bar shows a green bar starting at 0 and extending to 500,118,191. Below the progress bar, there are statistics: Pass: 1 of 5, Overall speed: 118 MB/s, Estimated time left: 35 minutes, Sectors imaged: 12,980,224, Sectors left: 487,137,968, Last attempted block: 12,980,223, Found signatures: 224988, and Total errors: 0. There are buttons for 'Pause' and 'Imaging settings', and a 'Legend' link. Below the statistics is a 'Target Hex Viewer' with a 'Log' tab. The log shows a message: '2/8/2017 5:57:39 PM Imaging started'. At the bottom, there is a status bar with 'Link: PHY' and 'Status: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY'. The 'Error' section shows: AMNF TONF ABRT - IDNF - UNC ICRC.

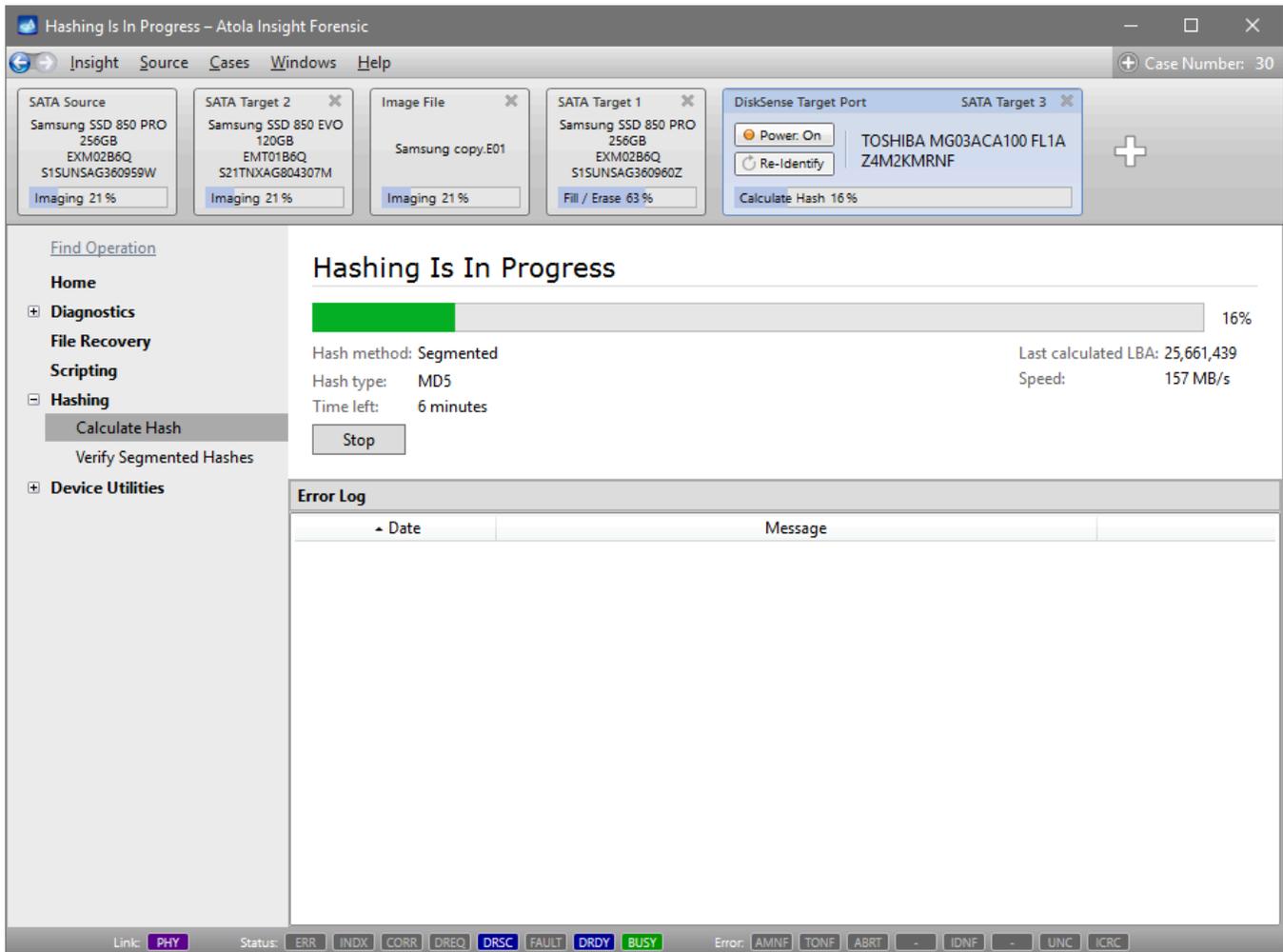
## How to add more device operations

For example, you can launch [Fill/Erase](#) on this Target drive to get it ready for the next imaging session:



### Additional wiping task being executed in parallel

It is also possible to [Calculate Hash](#) on yet another Target drive:



## Hash calculation being executed in parallel

Other long-running operations you can perform simultaneously include:

- [Automatic Checkup](#)
- [Artifact Finder](#)
- [Locate Sectors](#)
- [Verifying Segmented Hashes](#)
- Scripting (e.g. search files, files types, words, phrases or patterns, specific information type like email address, telephone, address, GPS coordinates etc.)
- Comparing data on drive with a pattern
- [Media Scan](#)

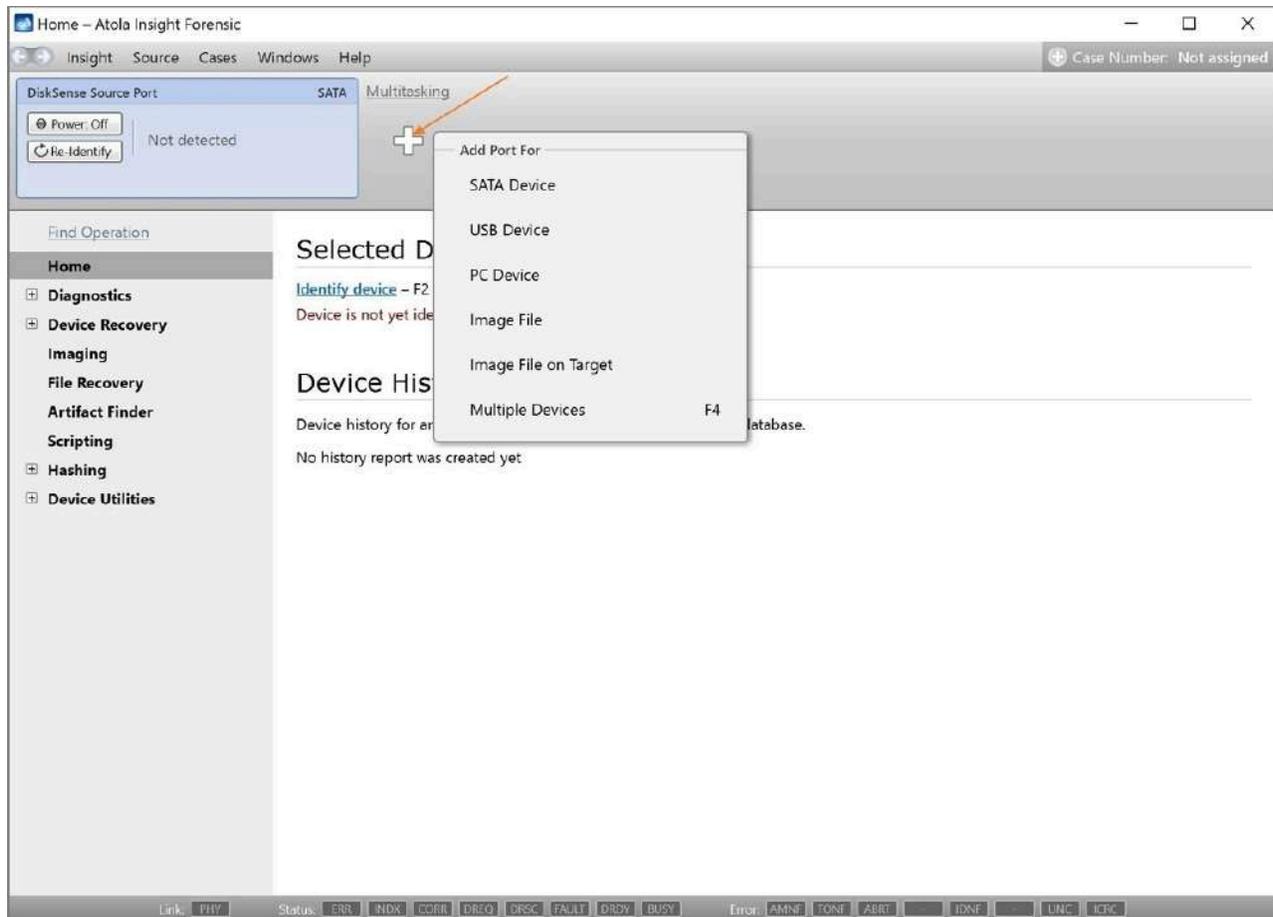
## Restore image file to device

*Writing from image file to device* allows to promptly copy data from the chosen container to the target device.

# Getting devices ready

To start extracting data from the file, follow these steps:

1. On the **Device** panel, click the **Plus** button and select port for the target you intend to use:



2. Choose your target device and click **Select**:

Home - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: Not assigned

DiskSense Source Port SATA Multitasking

Power: Off  
Re-Identify Not detected

Find Operation

Home

- Diagnosics
- Device Recovery
  - Imaging
  - File Recovery
  - Artifact Finder
  - Scripting
- Hashing
- Device Utilities

### Selected Device

[Identify device](#) - F2  
Device is not yet identified

Target Device Selection

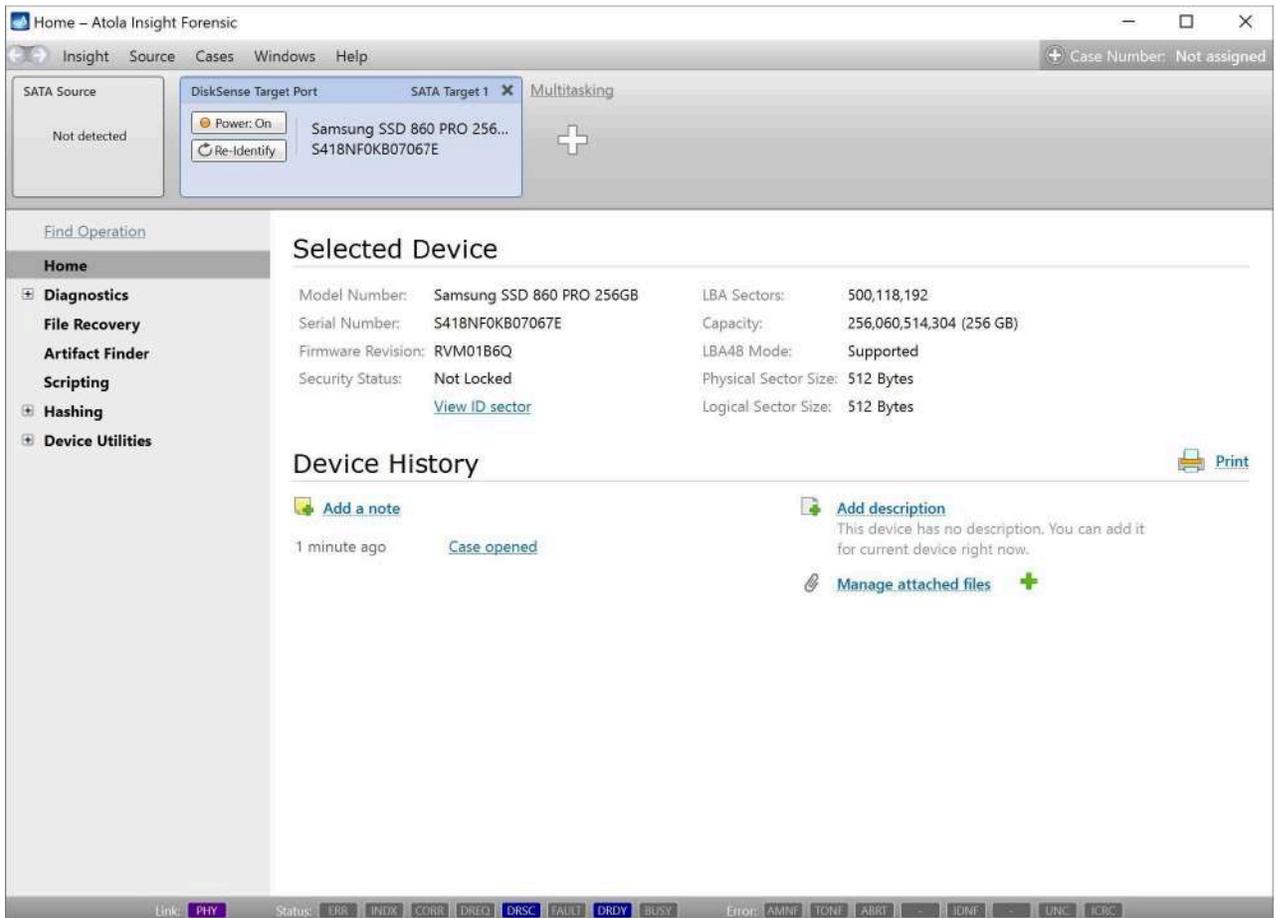
Please select target device: [Rescan](#)

Name	Type	Size
Samsung SSD 860 PRO 256GB S418NF0KB07067E	SATA Target 1	256 GB

Total: 1

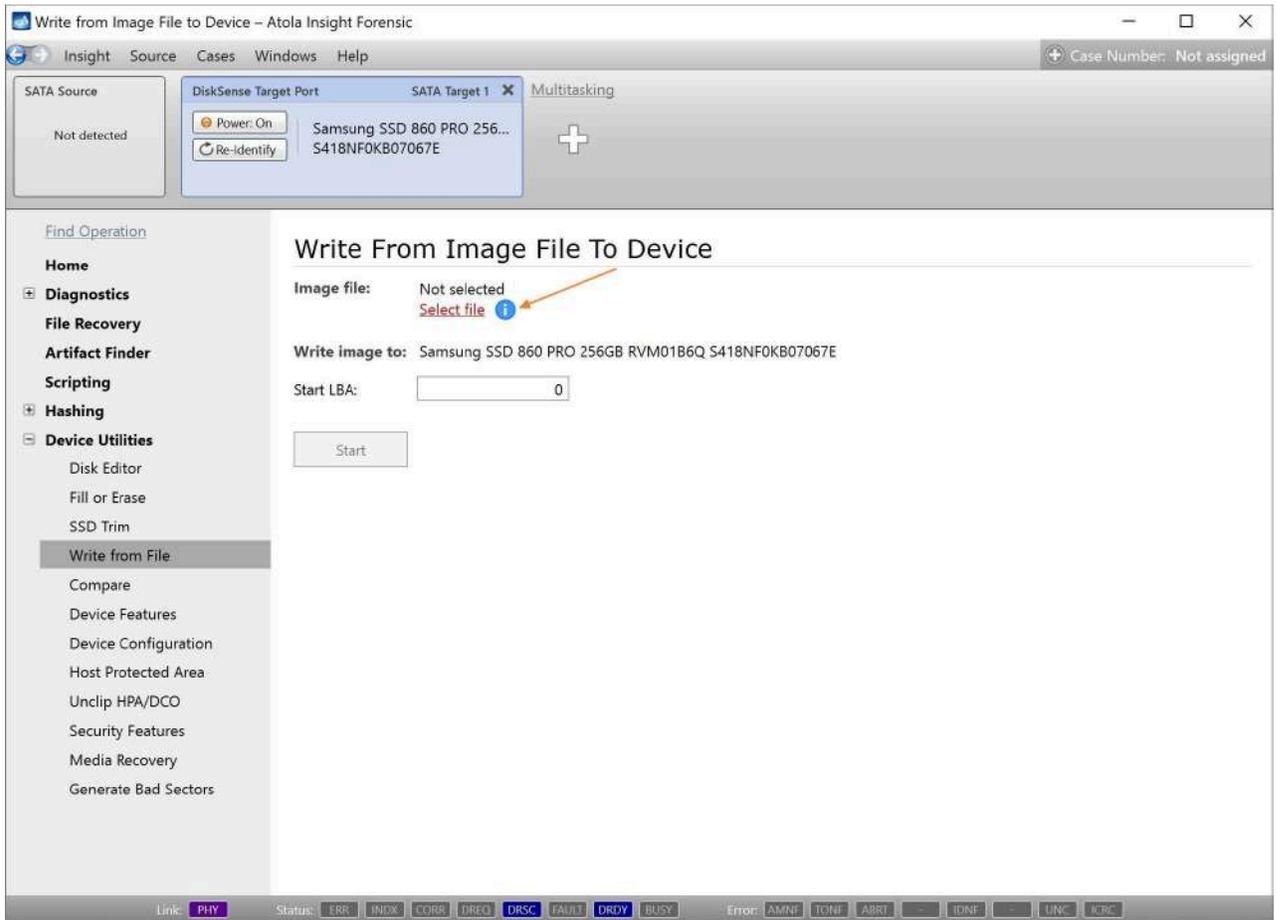
Select Cancel

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

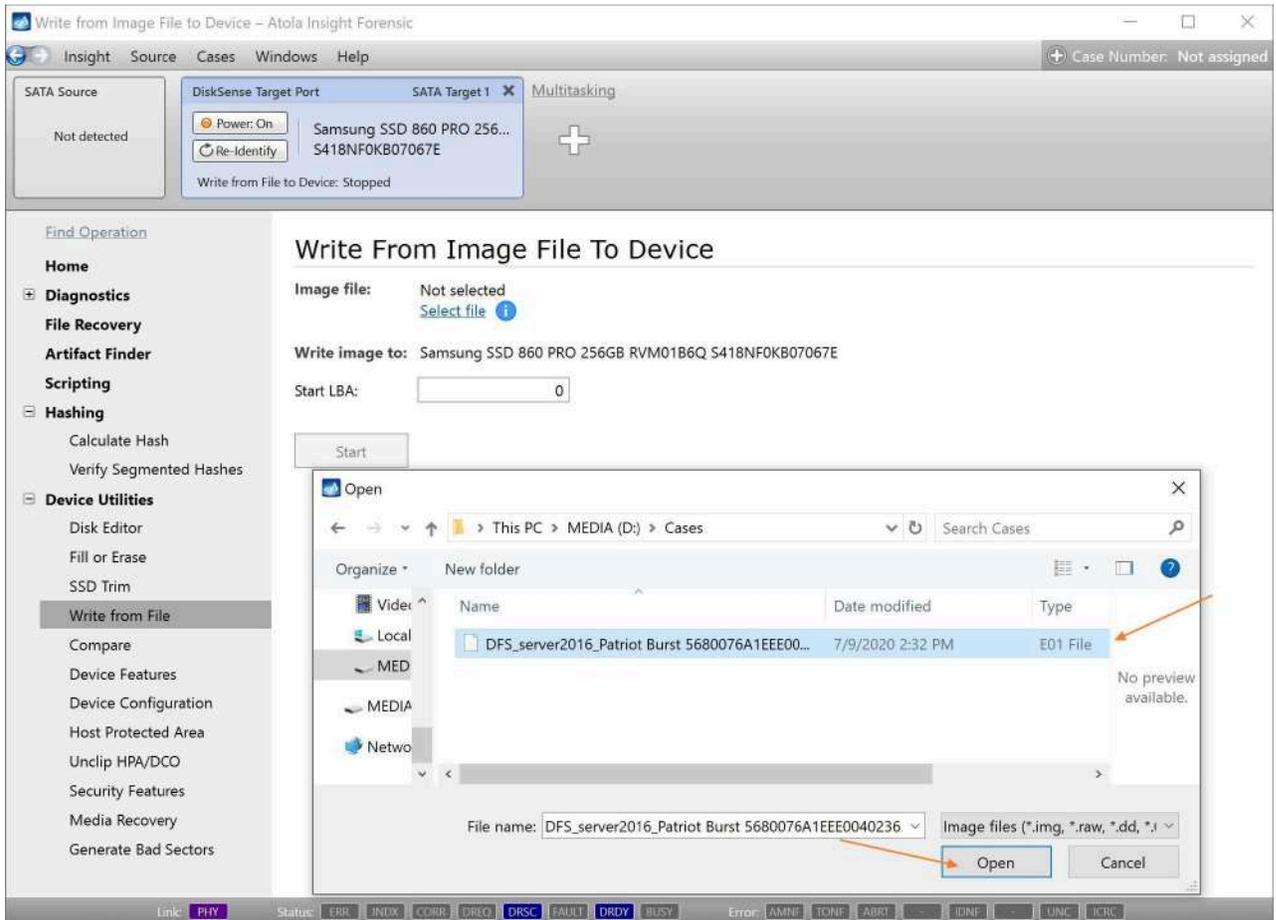


3. In the sidebar, go to **Device Utilities > Write from file**.

4. To locate the file you're planning to image, click the **Select file** link. You can work with E01/AFF4/Raw image files, split image files and more.

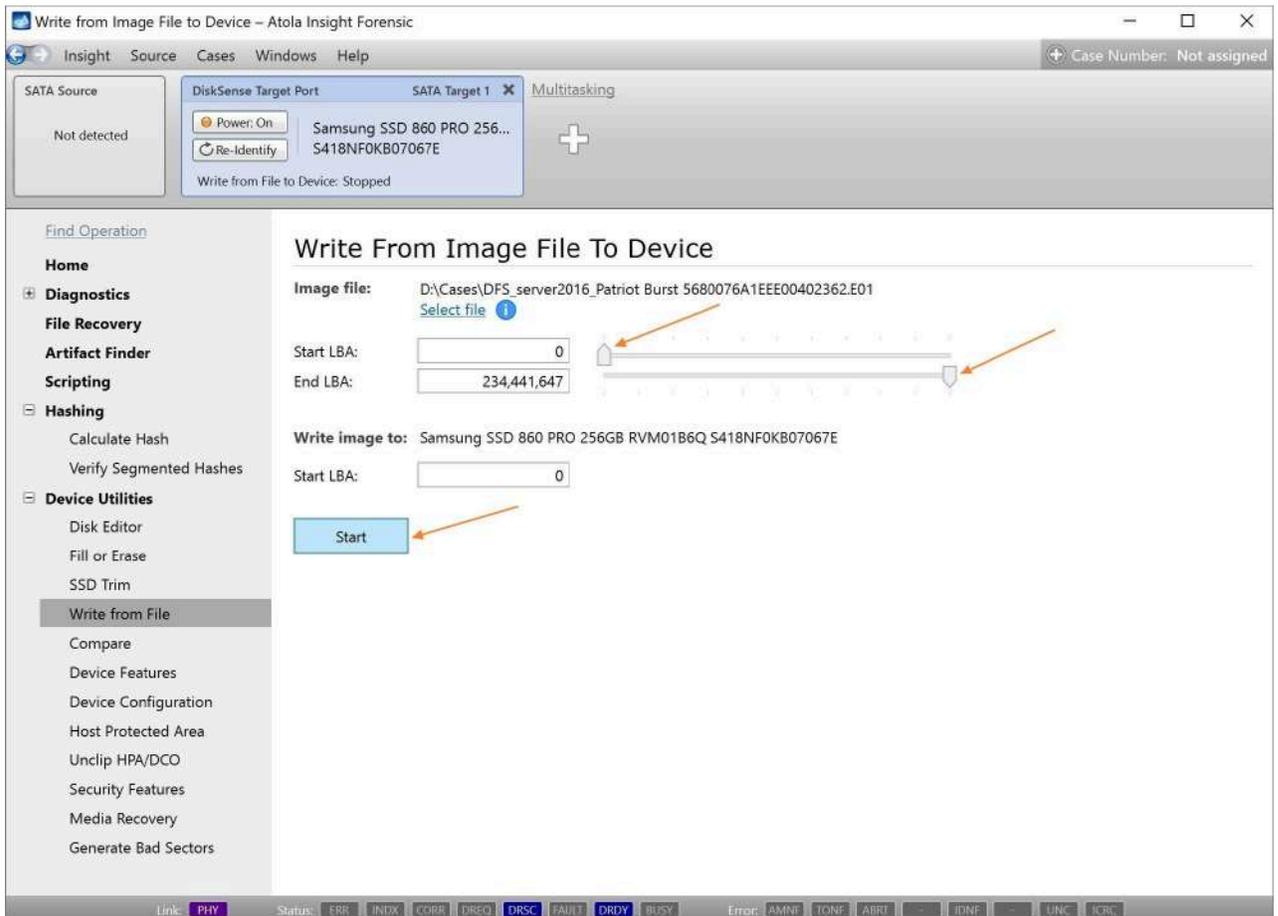


5. Having selected your image file, click the **Open** button:



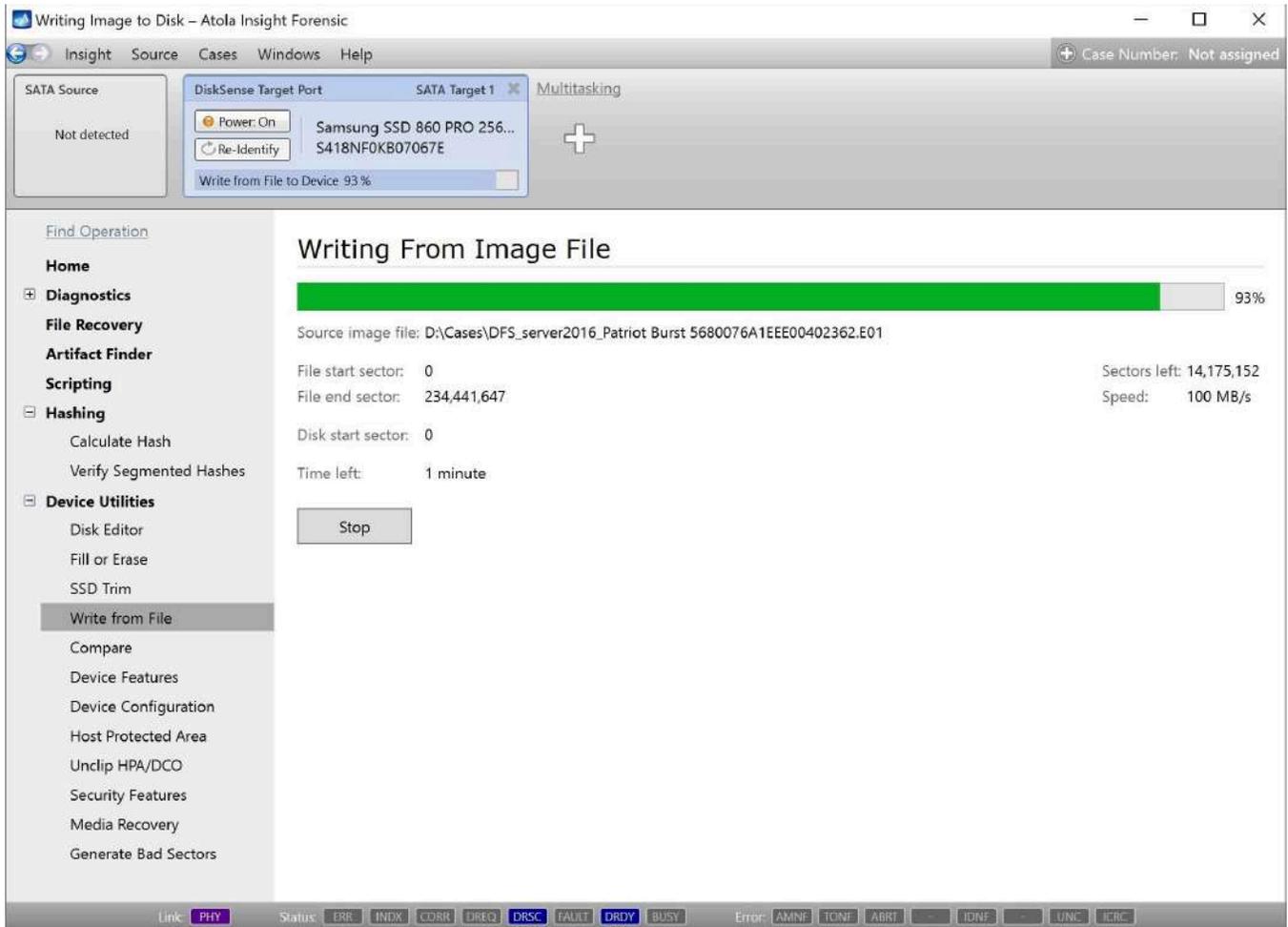
6. **Optional:** If you want to copy a certain range of data from the file, adjust start and end LBA.

7. To launch your imaging session, click the **Start** button.

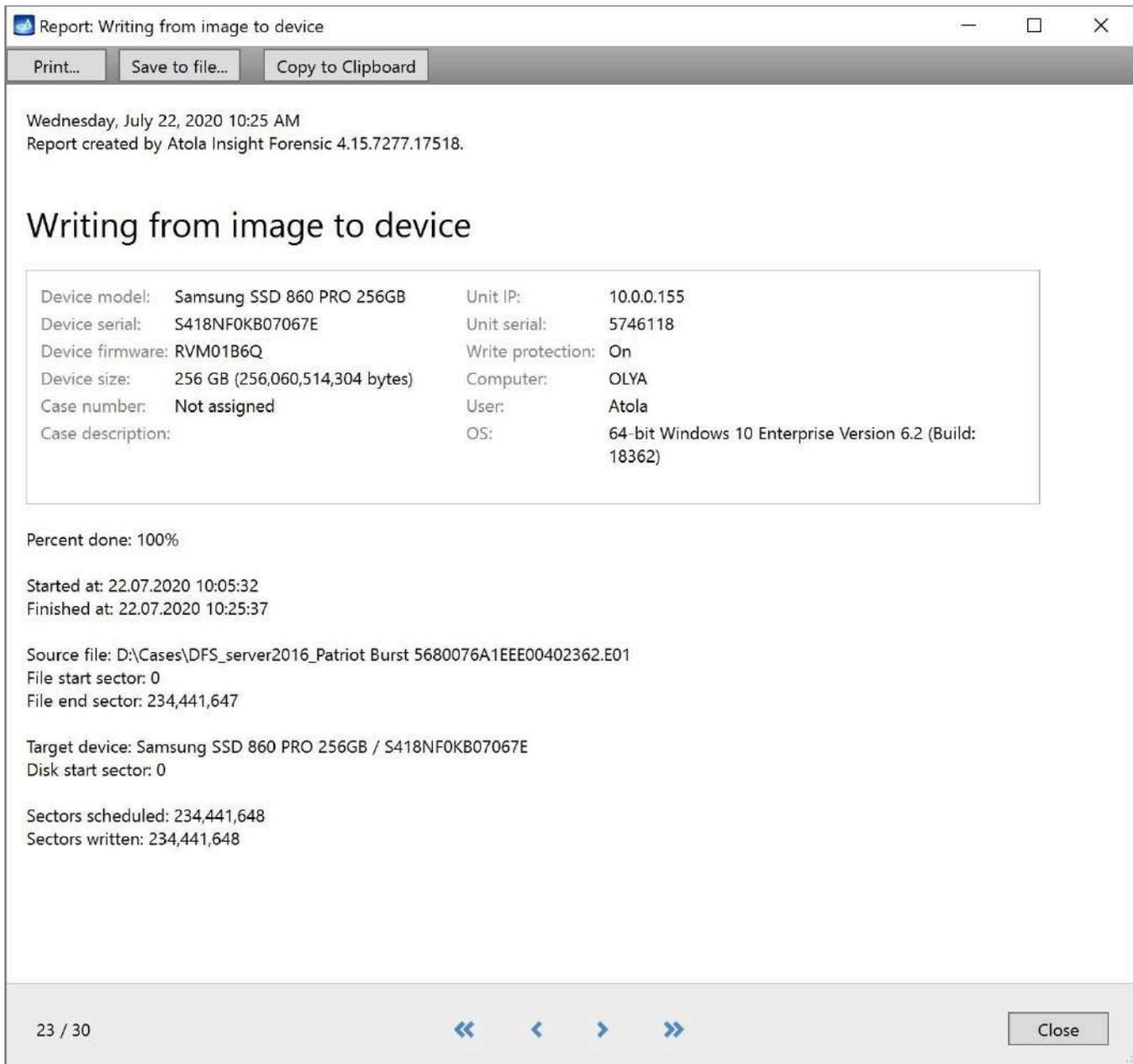


Insight Forensic provides you with all the essential details on the target you are going to use. The system notifies you if your target contains data. To confirm the intention to overwrite the data, enter *YES* in the pop-up window.

Depending on your bandwidth, writing from file to target device may require more time than drive-to-drive imaging. Insight will help you track the progress of your session and indicate the estimated time left.



Insight Forensic automatically creates reports for every session. You can find reports in the [Case management system](#).



## Wiping multiple drives simultaneously

Erasing data on destination drives guarantees accuracy of the imaged data and helps verify that the drive has no errors. In the course, all sectors are overwritten with the help of selected pattern or method.

When you need to prepare multiple hard drives for imaging, Insight's multitasking capabilities enable you to do so much faster by launching Erase/Fill on multiple drives simultaneously, including those connected to the source port.

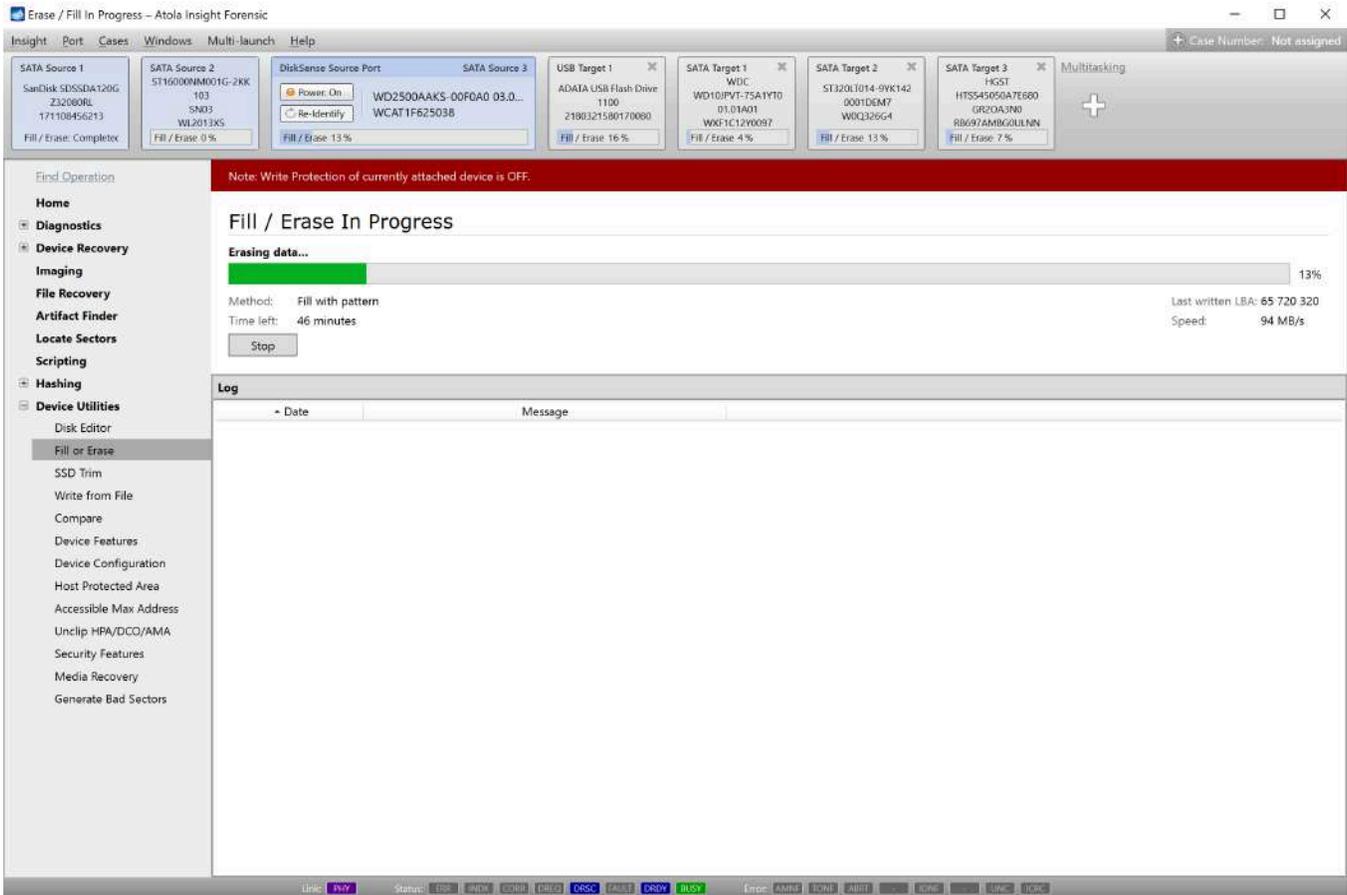


To wipe the drive connected to the source port, remember to switch off write protection on the hardware unit so that the LED indicator near the switch is off and there is a notification in the Atola Insight Forensic window saying *Note: Write protection of currently attached device is OFF.*

Then follow these steps:

1. In the Menu bar, go to **Multi-launch > Fill or Erase.**
2. Select all devices you want to fill or erase and then click **Continue.**
3. Select Fill method among the wide range of options and then click **Start Fill / Erase** button.
4. To confirm that you want to erase data on the selected devices, type **YES** in the **Confirmation** dialog and then click **OK.**

By following these steps, you can wipe data from three source drives and four target drives, all at the same time, as shown in the picture below.



This ability to perform Fill/Erase on multiple drives makes Insight exceptionally useful for forensic units dealing with many cases, where evidence acquisition is an ongoing activity.

## Case Management system

Insight's Case Management system records every step of data acquisition process: every operation is automatically added to the case from the moment a device is identified including date, time, media map and hash values. When a hard drive is imaged, its media map is recorded detailing all the sectors that have been skipped. Case notes can be added at any time to log information such as the case technician or owner of the hard drive.

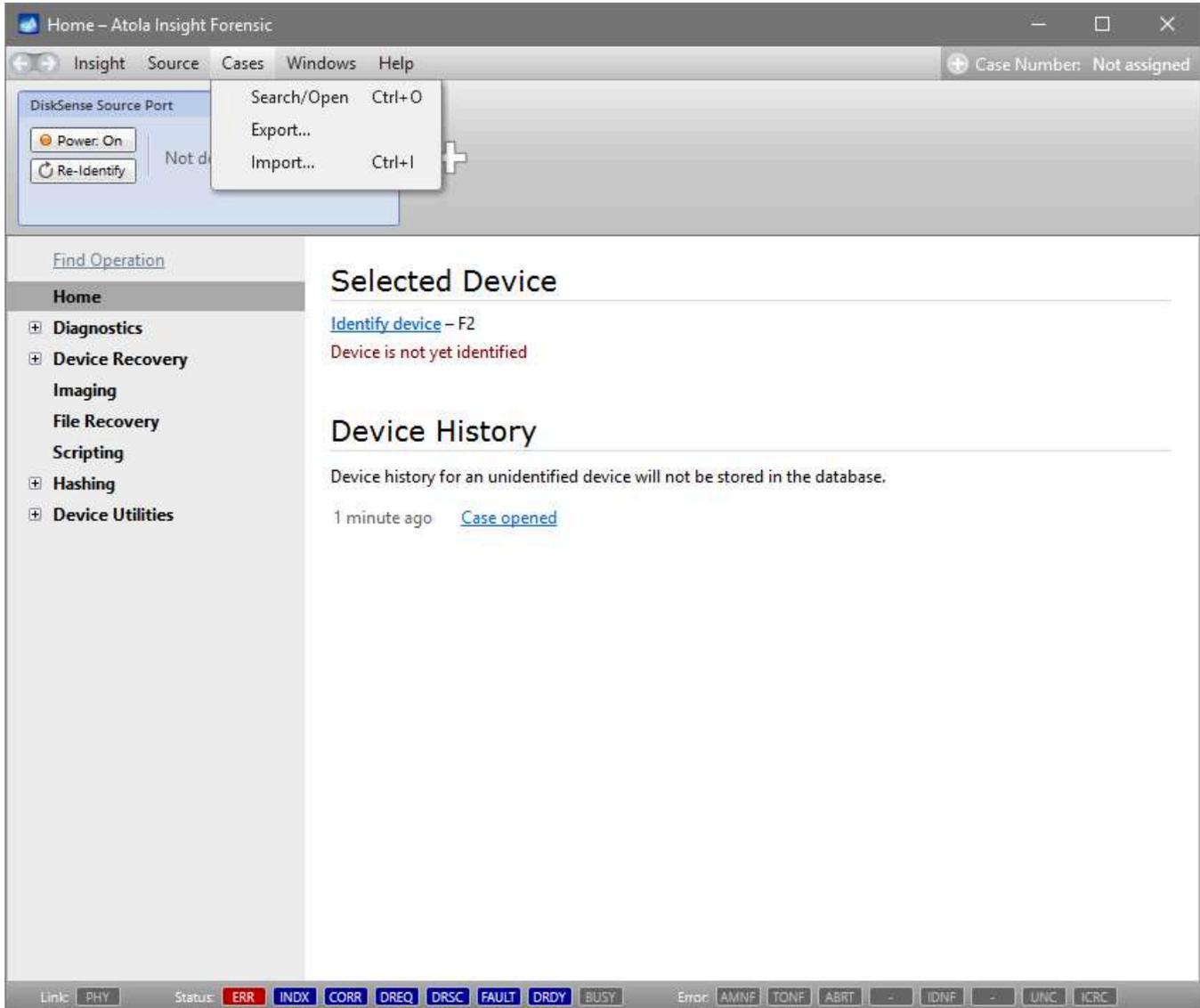
Whenever an operator connects a hard drive to DiskSense unit, Atola Insight Forensic makes an automatic database lookup and retrieves all past records associated with that particular hard drive. New entries will be added seamlessly to the database. You do not need to enable Case Management or take any additional actions for it to start functioning; it is fully embedded into Atola Insight Forensic and works at all times.

Case number can be assigned and changed at any time. The system also allows browsing through all cases and records within the cases, without corresponding devices being connected to the unit.

## Finding and opening a case

Insight's Case Management system records every step of data acquisition process saving them into reports grouped by cases.

To view the whole list of cases and their devices, go to **Cases > Search/Open** in the Menu bar or press **Ctrl + O**.



### Search/Open case

In the **Search and Open Case** window you will see the list of all the devices that have ever been connected and identified by your Insight.

It is possible to search for cases using multiple criteria and sort the results ascending or descending in any of the columns.

You can store multiple devices under the same case number to keep track of all devices related to a certain case.

Once a device is selected, you get a preview of the case including device details:

- when the case was created (i.e. the device was connected to the unit and identified by Insight for the first time),

- last time it was opened,
- the device model,
- serial number and
- description.

**Search conditions**

Case #

Description

Device model

Device serial

Creation date

Last open date

From

Until

[Clear all conditions](#)

**Search Results**

Case #	Creation Date	Last Open Date	Device Model	Device Serial	Description
3123	12/27/2016 10:31 AM	3/3/2017 9:26 AM	SAMSUNG HD502HJ	S20BJ90Z336612	Examiner: Roy Little
7122	12/27/2016 4:06 PM	3/1/2017 11:26 AM	WDC WD3200BEVT-26A23T0	WD-WXD1A11L6835	Examiner: Paul Allan
1233	12/27/2016 4:27 PM	3/3/2017 8:48 AM	TOSHIBA MG03ACA100	Z4M2KMRF	Examiner: Brad Olsen
3123	12/27/2016 4:27 PM	3/3/2017 9:26 AM	TOSHIBA MG03ACA100	Z4M2KMRF	Examiner: John Locke
9123	12/27/2016 4:51 PM	3/3/2017 1:04 PM	ST3500320AS	9QM6V2ZN	Examiner: Jerry King
5612	12/28/2016 4:18 PM	3/7/2017 11:49 AM	HUS153014VLS300	JFYELDJC	Examiner: Ken Beck
1266	12/28/2016 4:53 PM	3/8/2017 9:30 AM	ST500DM002-1BD142	Z2A9798C	Examiner: Paul Allan
6128	12/28/2016 5:54 PM	3/8/2017 1:05 PM	ST3500320AS	9QM6V2ZN	Examiner: Jody Bass
0126	12/28/2016 6:48 PM	3/8/2017 2:20 PM	WDC WD3200AAKX-221CA0	WD-WCAYUX169716	Examiner: Pat Cortez
0127	12/29/2016 2:57 PM	3/9/2017 8:29 AM	WDC WD10EALX-009BA0	WD-WCATR5198628	Examiner: Levi Myers
1240	12/29/2016 3:38 PM	3/28/2017 2:02 PM	TOSHIBA MK5056GSY	608XTJ2GT	Examiner: Elijah Day
6712	12/29/2016 3:44 PM	3/28/2017 3:23 PM	ST2000VM002-9UY166	5YD87CA6	Examiner: Rick Maher
8124	12/29/2016 3:47 PM	4/11/2017 1:21 PM	WDC WD20EARS-00MVWB0	WD-WCAZA3287142	Examiner: Ken Beck
9128	12/29/2016 4:09 PM	4/11/2017 1:24 PM	WDC WD5000AAKS-00V1A0	WD-WCAWF221506i	Examiner: Jerry Clay
7125	12/29/2016 4:27 PM	4/12/2017 7:51 PM	WDC WD1600JD-00GBB0	WD-WMAES463017	Examiner: Neil Price
1221	12/29/2016 4:38 PM	4/12/2017 7:51 PM	Hitachi HTS723225L9A360	090307FC1K00NEGTRJ	Examiner: John Rich
0128	12/29/2016 4:46 PM	4/12/2017 7:51 PM	Maxtor 6B200M0	B41SFHDH	Examiner: Seth Bary
1239	12/29/2016 4:55 PM	4/12/2017 7:51 PM	ST9500420AS	5VJ9SYLT	Examiner: John Haas
0012	12/29/2016 5:57 PM	4/12/2017 7:53 PM	Hitachi HTS545050A7E380	TA95123VC4EKGV	Examiner: John Haas

19 Case(s) found

**Case # 1221**

Creation Date: 12/29/2016 4:38 PM Last Open Date: 14 hours ago

Description: Examiner: John Rich  
Home path: [C:\Atola Insight Forensic\Work\1221 Hitachi HTS723225L9A360 FCDOC60A 090307FC1K00NEGTRJBH](#)

Device model: Hitachi HTS723225L9A360  
Device serial: 090307FC1K00NEGTRJBH  
Firmware revision: FCDOC60A

Attached files: 2

**Case History**

4/12/2017 7:51 PM [Case opened](#)  
3/9/2017 11:52 AM [Case opened](#)  
3/8/2017 8:03 PM [Imaging](#)  
3/8/2017 6:49 PM [Imaging \(started\)](#)  
3/8/2017 6:48 PM [Case opened](#)  
12/29/2016 4:43 PM [Media Scan](#)  
12/29/2016 4:38 PM [Media Scan \(started\)](#)  
12/29/2016 4:38 PM [Write protection is on](#)  
12/29/2016 4:38 PM [ID sector saved](#)  
12/29/2016 4:38 PM [Case opened](#)  
[Show all reports...](#)

## Case search filters

The case opens as a separate port on the Device panel of the Insight window.

The screenshot shows the Atola Insight Forensic software interface. At the top, there is a menu bar with 'Insight', 'Source', 'Cases', 'Windows', and 'Help'. A 'Case Number: 1221' is displayed in the top right corner. Below the menu bar, there is a 'SATA Source' section with 'Not detected' and a 'Case' window containing the device ID: 'Hitachi HTS723225L9A360 FCDOC60A 090307FC1K00NEGTRJBH'. The main content area is divided into two sections: 'Selected Device' and 'Case #1221 History'. The 'Selected Device' section displays the following information:

The following information was retrieved from the database:

Model Number:	Hitachi HTS723225L9A360	LBA Sectors:	488,397,168
Serial Number:	090307FC1K00NEGTRJBH	Capacity:	250,059,350,016 (250 GB)
Firmware Revision:	FCDOC60A		
Security Status:	Not Locked		

The 'Case #1221 History' section shows a list of events with timestamps and actions:

4/12/2017 7:57 PM	<a href="#">Case opened</a>
3/9/2017 11:52 AM	<a href="#">Case opened</a>
3/8/2017 8:03 PM	<a href="#">Imaging</a>
3/8/2017 6:49 PM	<a href="#">Imaging (started)</a>
3/8/2017 6:48 PM	<a href="#">Case opened</a>
3/8/2017 6:48 PM	<a href="#">Media Scan</a>
12/29/2016 4:43 PM	<a href="#">Media Scan (started)</a>
12/29/2016 4:38 PM	<a href="#">Write protection is on</a>
12/29/2016 4:38 PM	<a href="#">ID sector saved</a>
12/29/2016 4:38 PM	<a href="#">Case opened</a>

On the right side of the 'Case #1221 History' section, there is a 'Print' link and a 'Manage attached files' section. The 'Manage attached files' section shows two files: 'Hard drive details.gif' and 'Incident report 04.12.2017.jpg'. The 'Incident report 04.12.2017.jpg' file is highlighted with a green plus sign, indicating it is selected for printing.

## Print reports from a case

Insight's Case Management system includes flexible printing functionality.

To print a report, click the **Print** link on the case's Home screen.

The screenshot shows the Atola Insight Forensic software interface. At the top, there's a navigation bar with 'Insight', 'Source', 'Cases', 'Windows', and 'Help'. A 'Case Number: 4165' is displayed in the top right. Below this, there's a 'SATA Source' section with 'Not detected' and a 'Case' window showing 'ST8000AS0002-1NA17Z AR17 Z840ND1T'. The main content area is divided into a left sidebar with 'Home' and 'Imaging' sections, and a main panel. The main panel has a 'Selected Device' section with details: Model Number: ST8000AS0002-1NA17Z, LBA Sectors: 15,628,053,168, Serial Number: Z840ND1T, Capacity: 8,001,563,222,016 (8,002 GB), Firmware Revision: AR17, Security Status: Not Locked. Below this is the 'Case #4165 History' section, which includes a 'Print' button with a printer icon and a red arrow pointing to it. The history list shows various operations with timestamps and links, such as 'Imaging', 'Imaging (started)', 'Calculate Hash', 'Calculate Hash (started)', 'ID sector saved', 'Case opened', 'Write protection is on', 'Unclip HPA/DCO', 'Write protection is off', and 'ID sector saved'. To the right of the history list, there's a 'Manage attached files' section with a plus sign, showing three files: 'Hard drive details ST8000AS0002.gif', 'Incident report 04.18.2017.jpg', and 'seagate.JPG'.

### Print link

In the **Print Case History** window you get all the reports listed, sortable by date or by reported operation. It is possible to select just some of the reports or select all reports in the case by ticking the check box in the header of the list. Below there are all pictures attached to the case, which you can also select to be printed.

At the top of the **Print Case History** window there are four check boxes with report listing and printing settings (click on the **Case Management** arrow to view all check boxes):

- **Insert page break after every report on print.**
- **Also show miscellaneous reports** hides/displays all reports of seemingly minor importance, yet essential to some forensic specialists in accordance with their internal procedures.

- Also print CSV logs allows the printed version of the reports to include operation logs saved in CSV format.
- Also print segmented hashes also enables segmented hash saved in CSV files to be included in the printed version of the reports.

It is possible to print or save the selected reports and pictures in a PDF, HTML or RTF file by clicking **Save to file** or **Print** buttons.

The screenshot shows the 'Print Case History' dialog box in the Atola Insight Forensic application. The dialog box is titled 'Print Case History' and shows details for Case # 4165, created on Friday, March 3, 2017. A red box highlights the 'Print Case History' settings, which include:

- Insert page break after every report on print
- Case Management
- Also show miscellaneous reports
- Also print CSV logs
- Also print segmented hashes

Below the settings, there are two tables of reports and pictures. The first table, 'Report', has columns for 'Date' and 'Report'. The second table, 'Picture', has columns for 'Date' and 'Picture'. Red arrows point to the checkboxes for 'Imaging' and 'Hard drive details ST8000AS0002.gif' in the report list.

<input checked="" type="checkbox"/>	Date	Report
<input checked="" type="checkbox"/>	4/25/2017 5:40:47 PM	<a href="#">Imaging</a>
<input checked="" type="checkbox"/>	4/25/2017 4:46:10 PM	<a href="#">Imaging</a>
<input checked="" type="checkbox"/>	4/25/2017 2:01:28 PM	<a href="#">Imaging</a>
<input checked="" type="checkbox"/>	4/25/2017 2:00:12 PM	<a href="#">Imaging</a>
<input checked="" type="checkbox"/>	4/25/2017 1:59:10 PM	<a href="#">Imaging</a>
<input checked="" type="checkbox"/>	4/11/2017 1:27:25 PM	<a href="#">Fill or Erase</a>
<input checked="" type="checkbox"/>	4/10/2017 4:26:20 PM	<a href="#">Unclip HPA/DCO</a>
<input checked="" type="checkbox"/>	4/10/2017 4:26:09 PM	<a href="#">Imaging target</a>
<input checked="" type="checkbox"/>	4/10/2017 4:21:41 PM	<a href="#">Host Protected Area</a>
<input checked="" type="checkbox"/>	4/7/2017 4:48:44 PM	<a href="#">Imaging target</a>
<input checked="" type="checkbox"/>	4/7/2017 4:48:39 PM	<a href="#">Calculate Hash</a>
<input checked="" type="checkbox"/>	4/7/2017 2:06:55 PM	<a href="#">Imaging target</a>
<input checked="" type="checkbox"/>	4/7/2017 2:06:54 PM	<a href="#">Calculate Hash</a>
<input checked="" type="checkbox"/>	4/7/2017 1:32:36 PM	<a href="#">Imaging target</a>
<input checked="" type="checkbox"/>	4/7/2017 1:32:32 PM	<a href="#">Calculate Hash</a>
Total: 55		Selected: 55

<input type="checkbox"/>	Date	Picture
<input checked="" type="checkbox"/>	4/20/2017 10:27:25 AM	<a href="#">Hard drive details ST8000AS0002.gif</a>
<input type="checkbox"/>	4/20/2017 10:24:29 AM	<a href="#">Incident report 04.18.2017.jpg</a>
<input type="checkbox"/>	4/20/2017 10:23:23 AM	<a href="#">seagate.JPG</a>
Total: 3		Selected: 1

At the bottom of the dialog box, there are buttons for 'Change Case Details', 'Save to file...', 'Print', and 'Close'.

### Print options

If you have selected the two later options, this is how the log and the segmented hashes will be displayed in the report:

Friday, April 7, 2017 4:48 PM  
Report created by Atola Insight Forensic 4.8.6255.23495.  
case #4165

## Imaging target

Device model:	ST8000AS0002-1NA17Z	Unit IP:	10.0.0.155
Device serial:	Z840ND1T	Unit serial:	67331143
Device firmware:	AR17	Write protection:	On
Device size:	8,002 GB (8,001,563,222,016 bytes)	Computer:	YULIA
Case number:	Not assigned	User:	ATOLA
Case description:		OS:	64-bit Windows 10 Home Version 6.2 (Build: 14393)

Source: WDC WD5000AAKX-001CA0 15.01H15 WD-WMAYU2595458

Sectors scheduled: 976,773,168  
Sectors imaged: 976,773,165  
Errors: 3

Preset: Default (5 passes) (modified)

Copy range: All sectors  
Start sector in range: 0  
End sector in range: 976,773,167



File signatures: 0

MD5 hash: 02250b7ffbc87294055e61e1a39a2927

Calculated range: 0 - 976,773,167

Segmented hashes: [C:\Atola Insight Forensic\Work\672\\_WDC WD5000AAKX-001CA0\\_15.01H15\\_WD-WMAYU2595458\Hashes-Imaging-WDC WD5000AAKX-001CA0\\_15.01H15\\_WD-WMAYU2595458-0.csv](C:\Atola Insight Forensic\Work\672_WDC WD5000AAKX-001CA0_15.01H15_WD-WMAYU2595458\Hashes-Imaging-WDC WD5000AAKX-001CA0_15.01H15_WD-WMAYU2595458-0.csv)

Post-hash for ST8000AS0002-1NA17Z AR17 Z840ND1T

MD5 hash: 02250b7ffbc87294055e61e1a39a2927

Calculated range: 0 - 976,773,167

Segmented hashes: [C:\Atola Insight Forensic\Work\4165\\_ST8000AS0002-1NA17Z\\_AR17\\_Z840ND1T\Hashes-ST8000AS0002-1NA17Z\\_AR17\\_Z840ND1T-2.csv](C:\Atola Insight Forensic\Work\4165_ST8000AS0002-1NA17Z_AR17_Z840ND1T\Hashes-ST8000AS0002-1NA17Z_AR17_Z840ND1T-2.csv)

Log file: [C:\Atola Insight Forensic\Work\0037\\_WDC WD5000AAKX-001CA0\\_15.01H15\\_WD-WMAYU2595458\Target02\Imaging0.csv](C:\Atola Insight Forensic\Work\0037_WDC WD5000AAKX-001CA0_15.01H15_WD-WMAYU2595458\Target02\Imaging0.csv)

Date	Message
4/7/2017 2:43:28 PM	Imaging started
4/7/2017 3:01:38 PM	Cannot read block of data at 269,000,000 - 269,000,002 (Error: UNC)
4/7/2017 4:03:32 PM	Pass #1 completed
4/7/2017 4:03:32 PM	Imaging completed

Segmented hashes: [C:\Atola Insight Forensic\Work\0037\\_WDC WD5000AAKX-001CA0\\_15.01H15\\_WD-WMAYU2595458\Hashes-Imaging-WDC WD5000AAKX-001CA0\\_15.01H15\\_WD-WMAYU2595458-0.csv](C:\Atola Insight Forensic\Work\0037_WDC WD5000AAKX-001CA0_15.01H15_WD-WMAYU2595458\Hashes-Imaging-WDC WD5000AAKX-001CA0_15.01H15_WD-WMAYU2595458-0.csv)

```
6d4bc0dcb6d4173561d02acae8022309,0,8388607
a98c409f5229faaffe3646e731ad5c94,8388608,16777215
c9a5a6878d97b48cc965c1e41859f034,16777216,25165823
c9a5a6878d97b48cc965c1e41859f034,25165824,33554431
c9a5a6878d97b48cc965c1e41859f034,33554432,41943039
c9a5a6878d97b48cc965c1e41859f034,41943040,50331647
c9a5a6878d97b48cc965c1e41859f034,50331648,58720255
```

**Printing report having logs and segmented hashes included**

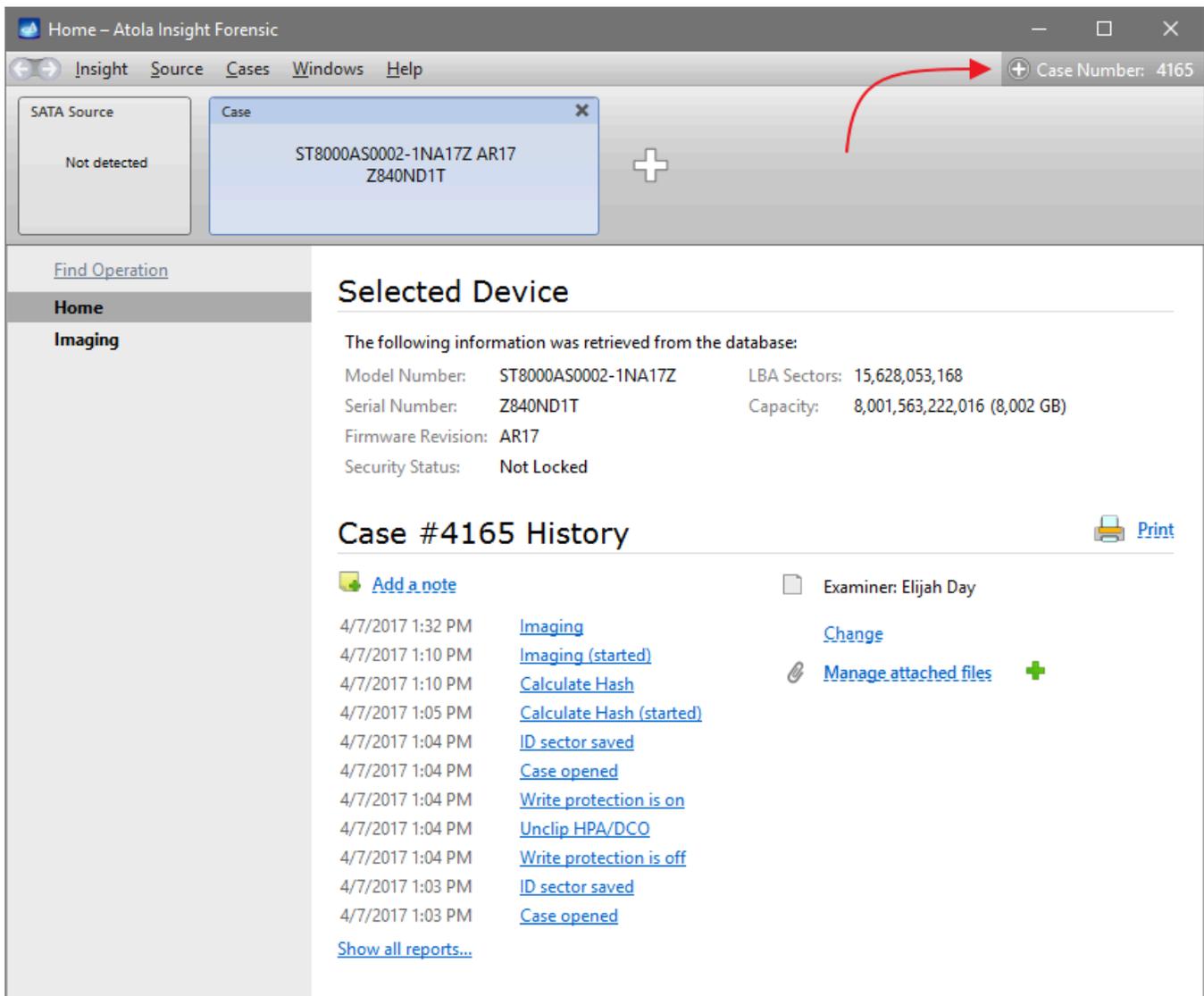
## Changing details in a case

Insight's case management system helps users efficiently keep track of drive-related information.

Even if a drive has already been used for a while, its imaging and hashing have already been performed, it is still possible to open its case and make adjustments to the case details.

## Add or change the case number and description

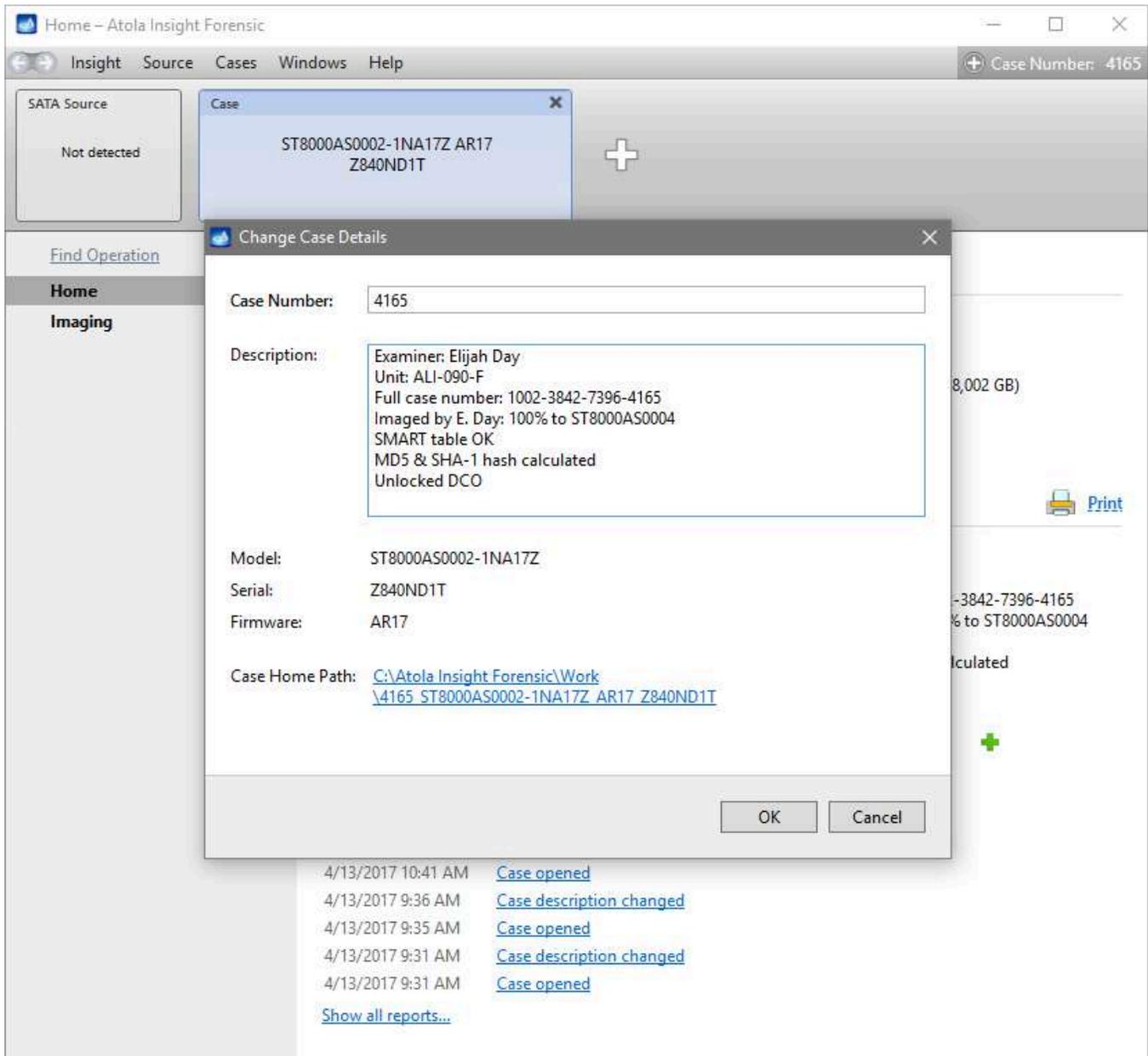
1. In the top right, click the **Plus** icon next to the **Case Number**.



The screenshot shows the Atola Insight Forensic application window. The title bar reads "Home - Atola Insight Forensic". The menu bar includes "Insight", "Source", "Cases", "Windows", and "Help". In the top right corner, there is a "Case Number: 4165" label with a plus icon to its left. A red arrow points to this plus icon. Below the menu bar, there is a "SATA Source" section with "Not detected" and a "Case" section with the ID "ST8000AS0002-1NA17Z AR17 Z840ND1T" and a plus icon to its right. The main content area is divided into two columns. The left column has a "Find Operation" section with "Home" and "Imaging" options. The right column has a "Selected Device" section with the following information: "The following information was retrieved from the database:", "Model Number: ST8000AS0002-1NA17Z", "Serial Number: Z840ND1T", "Firmware Revision: AR17", "Security Status: Not Locked", "LBA Sectors: 15,628,053,168", and "Capacity: 8,001,563,222,016 (8,002 GB)". Below this is a "Case #4165 History" section with a "Print" button. The history list includes: "Add a note", "4/7/2017 1:32 PM Imaging", "4/7/2017 1:10 PM Imaging (started)", "4/7/2017 1:10 PM Calculate Hash", "4/7/2017 1:05 PM Calculate Hash (started)", "4/7/2017 1:04 PM ID sector saved", "4/7/2017 1:04 PM Case opened", "4/7/2017 1:04 PM Write protection is on", "4/7/2017 1:04 PM Unclip HPA/DCO", "4/7/2017 1:04 PM Write protection is off", "4/7/2017 1:03 PM ID sector saved", and "4/7/2017 1:03 PM Case opened". There is also a "Show all reports..." link. On the right side of the history section, there is an "Examiner: Elijah Day" field with a "Change" link and a "Manage attached files" link with a plus icon.

**The Plus icon next to the Case Number.**

2. Enter or change the **Case Number** and **Description**.



### Changing case details.

1. Click **OK**. The description appears next to the **Case History**.  
For quick changes, you can also click the **Change** link right below the description.

The screenshot displays the Atola Insight Forensic software interface. At the top, the window title is "Home - Atola Insight Forensic". The navigation menu includes "Insight", "Source", "Cases", "Windows", and "Help". A "Case Number: 4165" is displayed in the top right corner. On the left, there is a "SATA Source" section with "Not detected" and a "Case" section with "ST8000AS0002-1NA17Z AR17 Z840ND1T". The main content area is divided into two sections: "Selected Device" and "Case #4165 History".

**Selected Device**

The following information was retrieved from the database:

Model Number:	ST8000AS0002-1NA17Z	LBA Sectors:	15,628,053,168
Serial Number:	Z840ND1T	Capacity:	8,001,563,222,016 (8,002 GB)
Firmware Revision:	AR17		
Security Status:	Not Locked		

**Case #4165 History**

[Add a note](#)

- 4/7/2017 1:32 PM [Imaging](#)
- 4/7/2017 1:10 PM [Imaging \(started\)](#)
- 4/7/2017 1:10 PM [Calculate Hash](#)
- 4/7/2017 1:05 PM [Calculate Hash \(started\)](#)
- 4/7/2017 1:04 PM [ID sector saved](#)
- 4/7/2017 1:04 PM [Case opened](#)
- 4/7/2017 1:04 PM [Write protection is on](#)
- 4/7/2017 1:04 PM [Unclip HPA/DCO](#)
- 4/7/2017 1:04 PM [Write protection is off](#)
- 4/7/2017 1:03 PM [ID sector saved](#)
- 4/7/2017 1:03 PM [Case opened](#)

[Show all reports...](#)

[Print](#)

[Add a note](#)

Examiner: Elijah Day  
Unit: ALI-090-F  
Full case number: 1002-3842-7396-4165  
Imaged by E. Day: 100% to ST8000AS0004  
SMART table OK  
MD5 & SHA-1 hash calculated  
Unlocked DCO

[Change](#)

[Manage attached files](#)

### Case description added

## Add a document or an image to the case

1. On the case Home screen, in the Case history section, click the green Plus icon.

The screenshot displays the Atola Insight Forensic software interface. At the top, the window title is "Home - Atola Insight Forensic". The main menu includes "Insight", "Source", "Cases", "Windows", and "Help". A "Case Number: 4165" is displayed in the top right corner. Below the menu, there are two panels: "SATA Source" (Not detected) and "Case" (ST8000AS0002-1NA17Z AR17 Z840ND1T). The "Selected Device" section provides the following information:

The following information was retrieved from the database:

Model Number:	ST8000AS0002-1NA17Z	LBA Sectors:	15,628,053,168
Serial Number:	Z840ND1T	Capacity:	8,001,563,222,016 (8,002 GB)
Firmware Revision:	AR17		
Security Status:	Not Locked		

The "Case #4165 History" section shows a list of operations performed on 4/7/2017:

- 4/7/2017 1:32 PM [Imaging](#)
- 4/7/2017 1:10 PM [Imaging \(started\)](#)
- 4/7/2017 1:10 PM [Calculate Hash](#)
- 4/7/2017 1:05 PM [Calculate Hash \(started\)](#)
- 4/7/2017 1:04 PM [ID sector saved](#)
- 4/7/2017 1:04 PM [Case opened](#)
- 4/7/2017 1:04 PM [Write protection is on](#)
- 4/7/2017 1:04 PM [Unclip HPA/DCO](#)
- 4/7/2017 1:04 PM [Write protection is off](#)
- 4/7/2017 1:03 PM [ID sector saved](#)
- 4/7/2017 1:03 PM [Case opened](#)

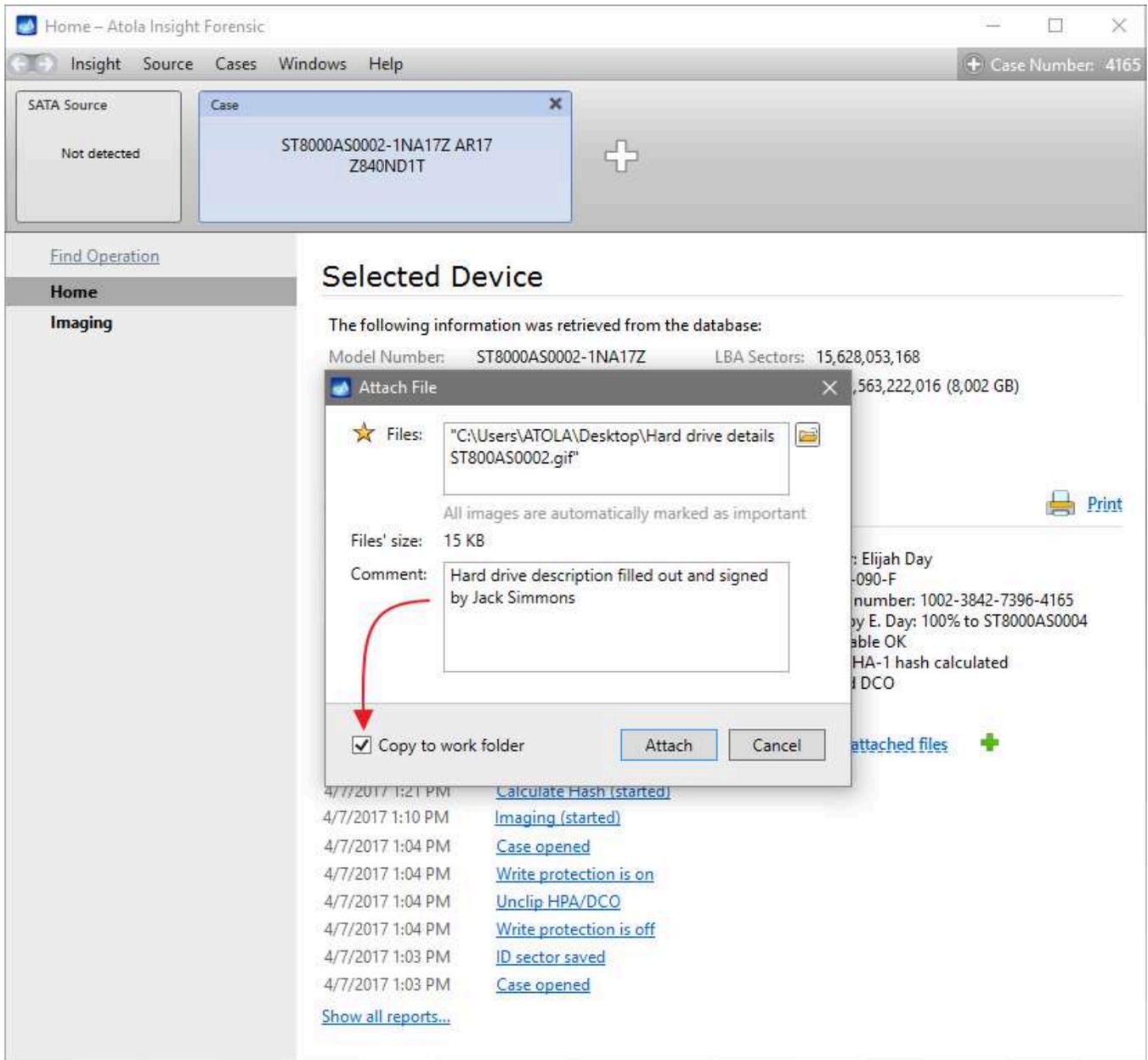
Additional case details include:

- Examiner: Elijah Day
- Unit: ALI-090-F
- Full case number: 1002-3842-7396-4165
- Imaged by E. Day: 100% to ST8000AS0004
- SMART table OK
- MD5 & SHA-1 hash calculated
- Unlocked DCO

A red arrow points to the "Manage attached files" link, which has a green plus sign next to it.

### Adding a file to the case.

2. In the **Attach File** dialog, enter the path to a file and leave a comment in the corresponding field.
3. **Optional:** Select **Copy to work folder** to copy the file to the same folder where any other related files are located, for example, tables with segmented hashes, logs, imaging maps, file signature lists and more.



**The Attach file dialog.**

4. Click **Attach**. All the uploaded files appear on the case **Home** screen below the description.

## View or remove the attached files

To view all the attached files, change their details, or remove them from the case, click the **Manage attached files** link.

The screenshot displays the Atola Insight Forensic software interface. At the top, the window title is "Home - Atola Insight Forensic". The main menu includes "Insight", "Source", "Cases", "Windows", and "Help". A "Case Number: 4165" is displayed in the top right corner. On the left, there is a "SATA Source" section with "Not detected" and a "Case" window showing "ST8000AS0002-1NA17Z AR17 Z840ND1T".

The main content area is divided into two sections:

- Selected Device:** This section provides details retrieved from the database:
  - Model Number: ST8000AS0002-1NA17Z
  - Serial Number: Z840ND1T
  - Firmware Revision: AR17
  - Security Status: Not Locked
  - LBA Sectors: 15,628,053,168
  - Capacity: 8,001,563,222,016 (8,002 GB)
- Case #4165 History:** This section shows a list of operations performed on the device, including "Imaging", "Calculate Hash", "ID sector saved", "Case opened", "Write protection is on", "Unclip HPA/DCO", and "Write protection is off". It also includes a "Manage attached files" section with a red arrow pointing to a list of files:
  - Hard drive details ST800AS0002.gif
  - Incident report 04.18.2017.jpg
  - seagate.JPG

The **Attached files** window contains the list of files including

- an icon representing the file type,
- the name,
- the folder where the file is located,
- the date when the file was attached to the case and
- the comment added by the user.

To edit the **Comment** or copy the file to the case folder, right-click a file and select **Edit**.

To remove the file from the case, select the file and click **Remove**.

Home - Atola Insight Forensic

Insight Source Cases Windows Help Case Number: 4165

SATA Source: Not detected

Case: ST8000AS0002-1NA17Z AR17 Z840ND1T

Find Operation

Home

Imaging

### Selected Device

The following information was retrieved from the database:

Model Number: ST8000AS0002-1NA17Z LBA Sectors: 15,628,053,168  
 Serial Number: Z840ND1T Capacity: 8,001,563,222,016 (8,002 GB)  
 Firmware Revision: AR17  
 Security Status: Not Locked

### Case #4165 History

Print

#### Attached Files

<input type="checkbox"/>	Icon	Name	Directory	Attached at	Comment
<input type="checkbox"/>	★	Hard drive details ST8000AS0002-1NA17Z AR17 Z840ND1T.gif	C:\Atola Insight Forensic\Work\4165_ST8000AS0002-1NA17Z_AR17_Z840ND1T\AttachedFiles	4/20/2017 10:27:25 AM	Hard drive description fi...
<input type="checkbox"/>	★	Incident report 04.18.2017.jpg	C:\Users\ATOLA\Desktop	4/20/2017 10:24:29 AM	Incident report signed by...
<input type="checkbox"/>	★	seagate.JPG	C:\Users\ATOLA\Desktop	4/20/2017 10:23:23 AM	photo of the hard drive

Total: 3 Selected: 0

Remove Add file Close

Show all reports...

seagate.JPG

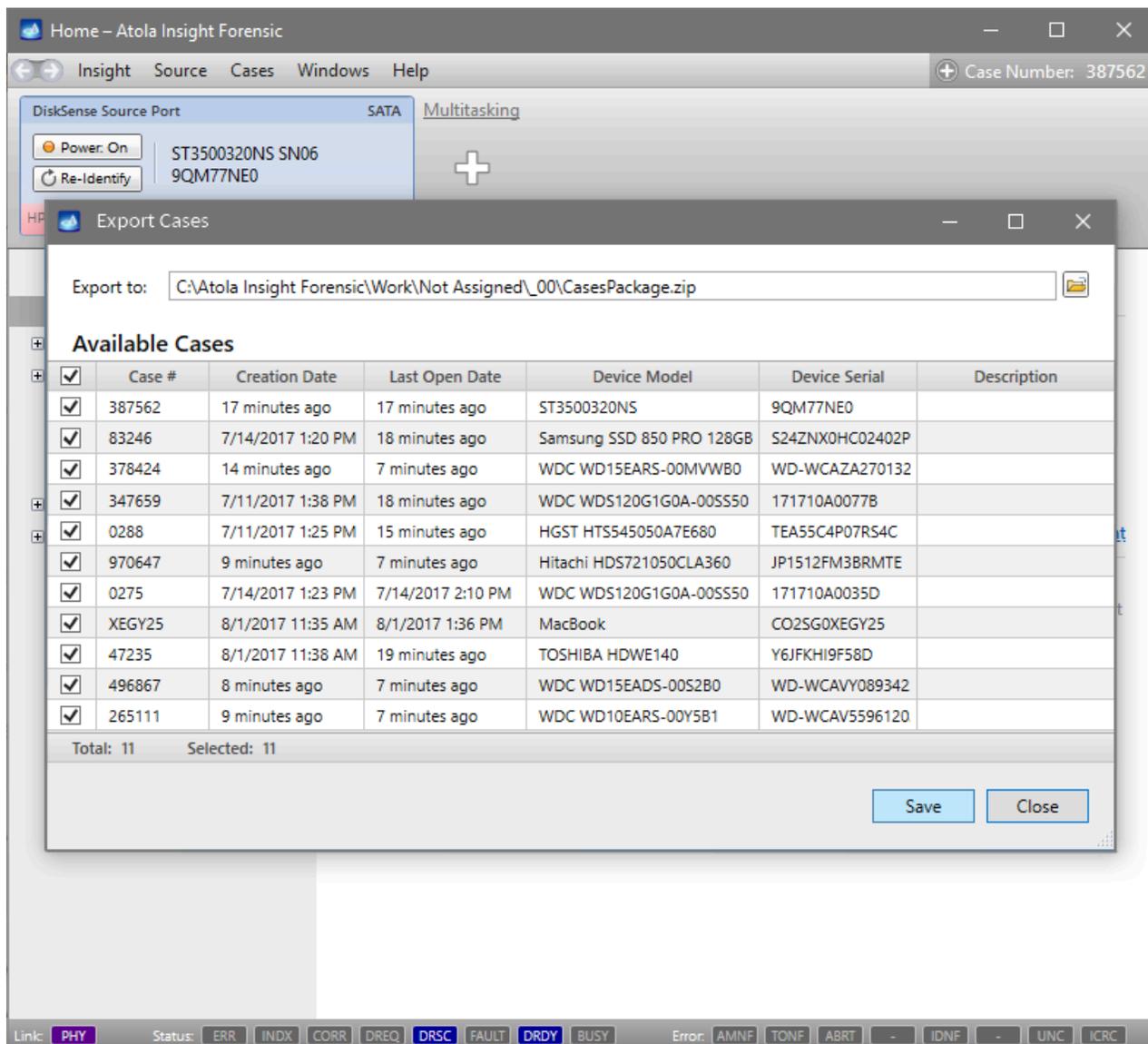
## Exporting and importing cases from one computer to another

It is possible to transfer all or some of the cases stored in one Insight's case management system to another one. The only requirement is that both computers have the same version of Insight installed.

## Export cases

Whenever cases need to be transferred from one computer to another one, start by exporting the cases.

1. In the Menu bar, go to **Cases > Export**.
2. In the **Export Cases** window, select the folder where the cases should be stored.
3. Select the cases you want to export and click the **Save** button.



### Export selected cases

4. Insight saves cases as a package in a zip file with the default name *Cases.Package.zip*. Later you can copy this file to a different computer.
5. Once a case is exported, Insight adds a record about it to the case's history.

The screenshot shows the Atola Insight Forensic application window. The top menu bar includes 'Insight', 'Source', 'Cases', 'Windows', and 'Help'. A 'Case Number: 9578059' is displayed in the top right. A 'SATA Source' window shows 'ST3500320NS SN06 9QM77NE0' and 'Auto Dia...: Complete'. A 'Case' window shows 'WDC WD15EARS-00MVWB0 51.0AB51' and 'WD-WCAZA2701320'. The main area is titled 'Selected Device' and contains the following information:

The following information was retrieved from the database:

Model Number:	WDC WD15EARS-00MVWB0	LBA Sectors:	2,930,277,168
Serial Number:	WD-WCAZA2701320	Capacity:	1,500,301,910,016 (1,500 GB)
Firmware Revision:	51.0AB51	LBA48 Mode:	Supported
Security Status:	Not Locked	Physical Sector Size:	512 Bytes

Below this is the 'Case #9578059 History' section, which includes a 'Print' icon and a list of events:

- 1 minute ago [Case opened](#)
- 8/31/2017 5:16 PM [Case exported](#)
- 8/31/2017 5:13 PM [Case number assigned](#)
- 8/31/2017 5:13 PM [Case opened](#)
- 8/31/2017 5:05 PM [ID sector saved](#)
- 8/31/2017 5:05 PM [Case opened](#)

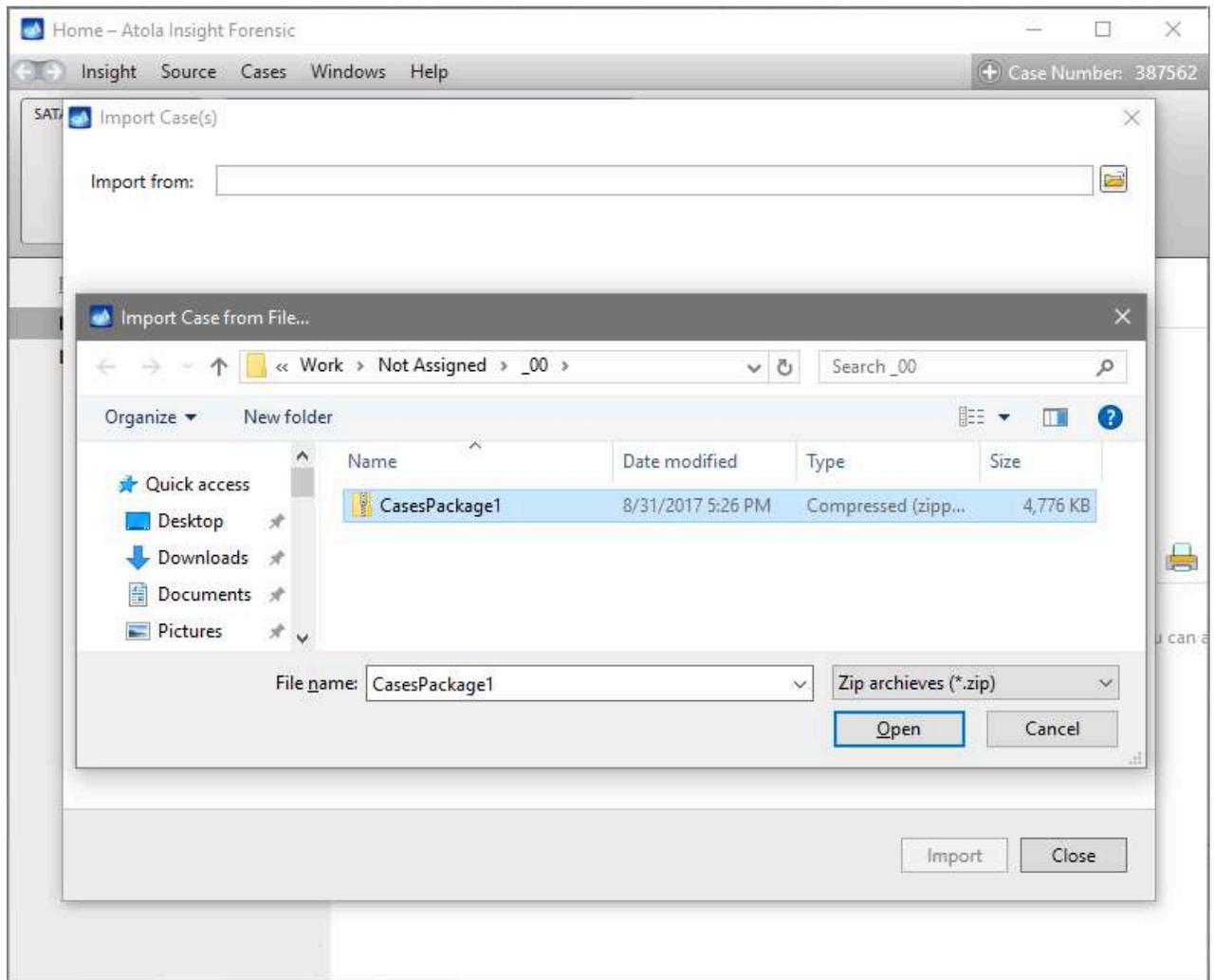
Additional actions include 'Add a note', 'Add description' (with a note: 'This device has no description. You can add it for current device right now.'), and 'Manage attached files'.

## Case export report

## Import cases

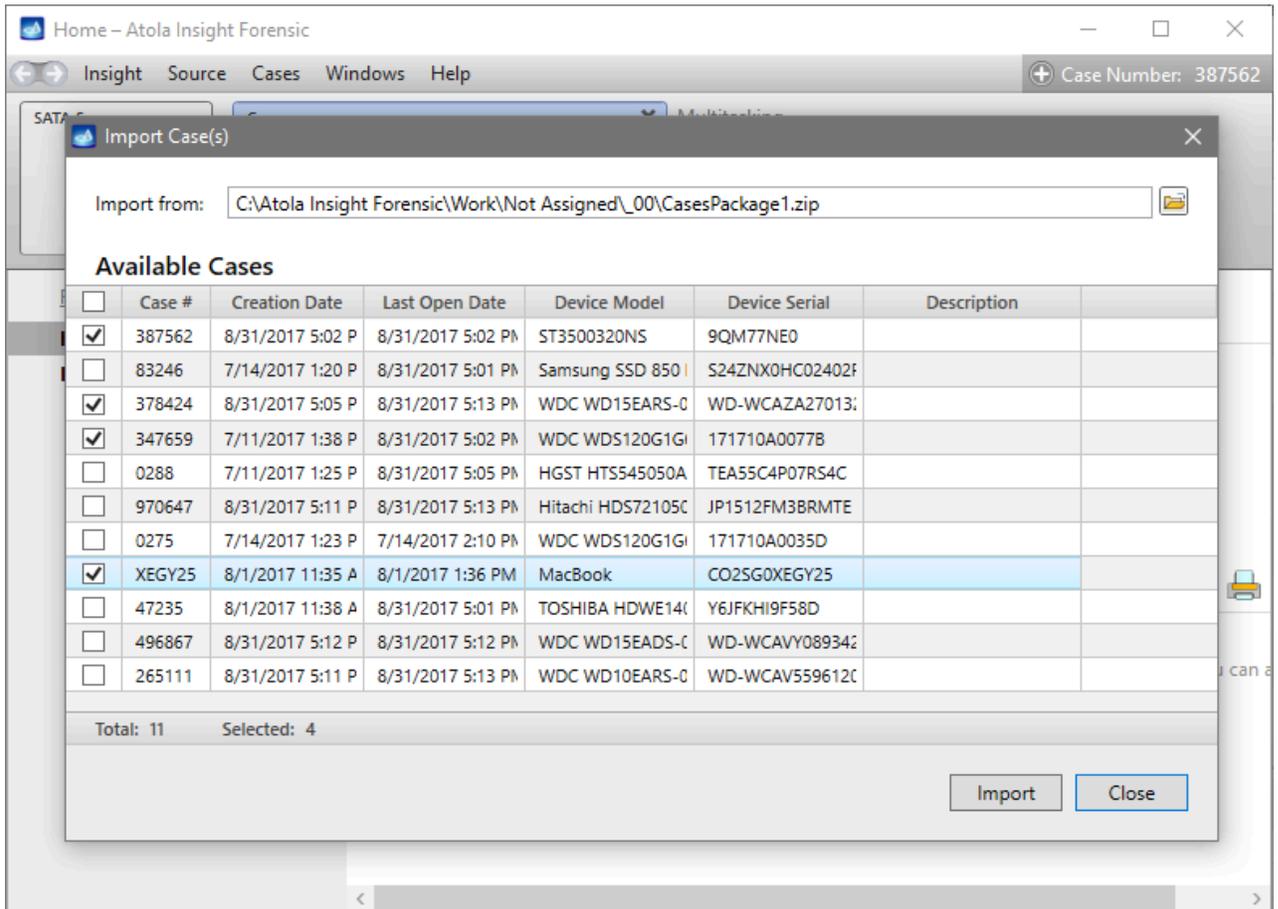
To import cases from a zip file into Insight on a different computer, do the following:

1. In the Menu bar, go to **Cases > Import** or press **Ctrl + I**.
2. Click the **Browse** icon and open the zip file with saves cases.



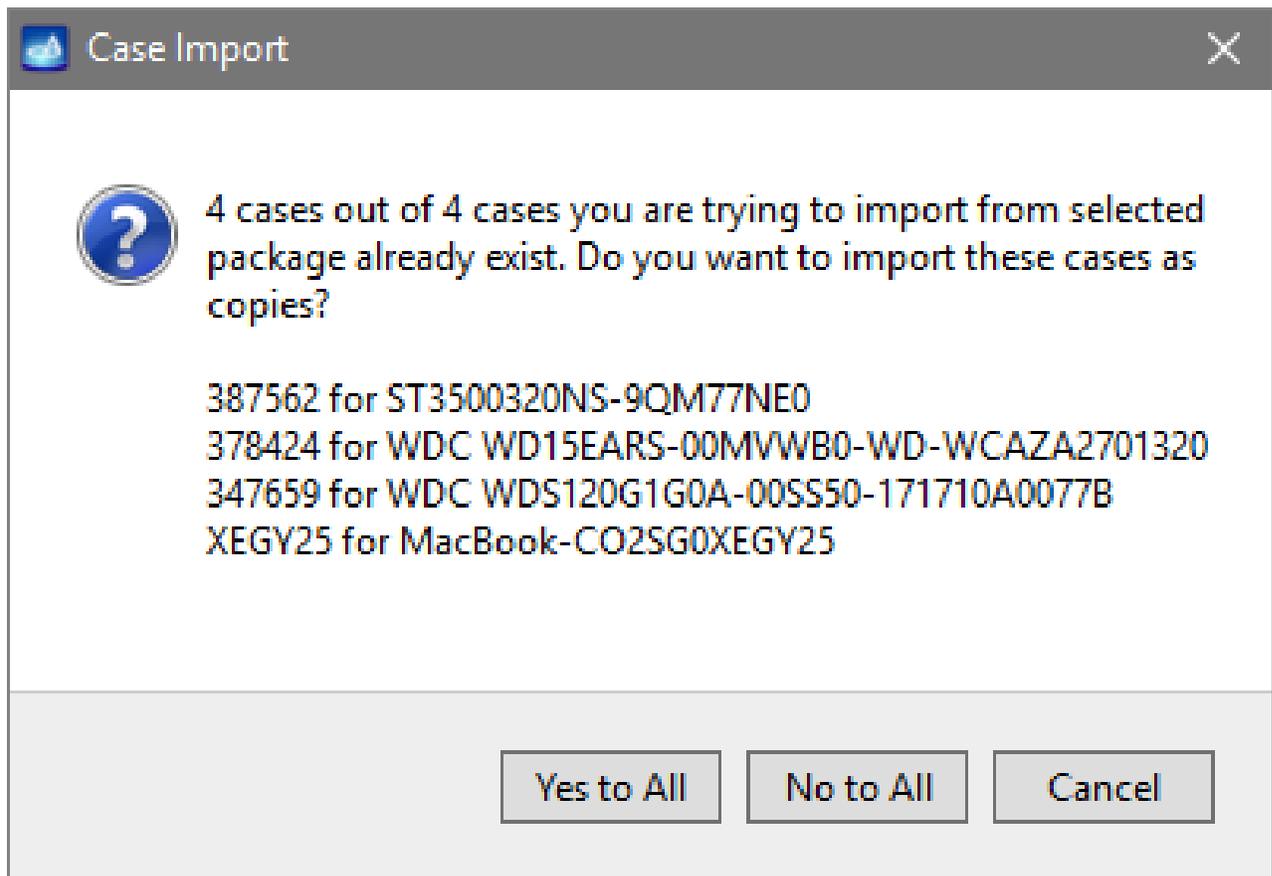
### Importing cases

3. Select some or all of the cases in the table and click the Import button.



### Importing cases selectively

If there is a match between existing case numbers and the imported ones, Insight will prompt you to either cancel the import or save the case that causes the conflict as a copy.



### Ways to resolve import conflicts

## FAQ and Troubleshooting

- ▶ General
- ▶ Hardware unit and installation
- ▶ Connectivity
- ▶ Drive ports
- ▶ Imaging
- ▶ Performance
- ▶ Damaged media & File recovery
- ▶ Diagnostics
- ▶ Hashing
- ▶ Fill/Erase

- Case Management
- Device Recovery

## General

### What is the advantage of using Atola Insight Forensic compared to other forensic imagers?

We produce the only solution that is specifically designed to support damaged media. Here is how it stands out:

Our users usually start with **automatic diagnostics** of an evidence drive. It takes a couple of minutes but saves a lot of time and energy. It detects drive issues such as PCB instability, problems with the motor, a short circuit, firmware errors, degraded or even non-working heads, and physical media surface damage. Based on the results, you can decide on the next steps for handling the evidence drive.

Even if you work with a severely damaged source device, the imaging engine enables you to:

- disable damaged heads
- automatically overcome much more serious problems than the so-called 'software bad sectors'
- track drive state before, during and after imaging
- have every imaging event logged in a forensically sound manner

Atola Insight has file recovery integrated with imaging. By browsing the target image directory tree, you can always see which source file sectors are bad sectors or even were read with the ReadLong ATA command (without ECC).

Last but not least, Atola Insight Forensic can clear any unknown ATA password from the hard disk drive in just a minute.

### What are the PC requirements for Atola Insight Forensic?

Atola Insight Forensic software requires a Windows PC. More details are available in the [Atola Insight Forensic Manual](#)

### Does Insight utilize BIOS and/or operating system functions in the hardware unit to image data?

[Insight's hardware](#) runs a Linux OS with a highly-customized and fine-tuned kernel that allows the blocking of all BIOS and standard Linux I/O operations to enable the lowest-level control of SATA, USB and IDE ports.

### Does Insight image mobile phones, tablets, IoT devices, etc.?

Atola products are designed to handle HDDs, SSDs and other detachable media. We have never developed our systems to support mobile devices like phones or tablets. This approach allows us to be the best at handling the media we focus on and progress quickly in developing high-performance imaging and innovative features for our customers.

### Does Insight repair damaged drives?

Insight can handle damaged drives with varying degrees of success depending on the severity and type of damage, including:

- Degraded or damaged heads
- Drive freezing after a read attempt
- Scratches on the media surface

## What are the advantages of Atola Insight Forensic compared to software data recovery tools?

There are many advantages. Let's take *ddrescue*, for example. Here are some of the functions that Atola Insight Forensic provides but *ddrescue* lacks:

1. For Insight, we have developed a functionality that specifically helps [image freezing damaged drives](#).
2. Insight's diagnostics function identifies damaged heads, while advanced imaging settings allow [head selection](#) to perform imaging in a fast and, most importantly, careful manner to avoid causing further damage to the evidence drive.
3. Insight can [image to multiple targets](#) at the same time, including both hard drives and files.
4. Forensic procedures require [hash calculation](#) to be a part of the acquisition process. Insight has a very flexible hash calculation functionality: it can simultaneously calculate MD5 and SHA hashes of the source before, during or after imaging, and the target drive's hash can be calculated in conjunction with imaging or as a separate action. Additionally, Insight has the [segmented hashing](#) feature, which can verify an image of a damaged drive—something that is impossible with a standard linear hashing.
5. Built-in write protection.
6. Insight's in-depth [diagnostics](#) help identify the drive status and, based on that, the right way to handle the drive for successful data acquisition.
7. Insight's [overcurrent protection](#) detects when a hard drive draws an abnormal current and stops the hard drive to prevent any further damage to the system and the drive.
8. Insight's automatic password removal function can [extract an unknown ATA password](#) and unlock the drive in less than two minutes with just a few mouse clicks.
9. [Locate Sectors](#) finds the exact location of specific sectors and detects which files and partitions they belong to. On top of that, it gives you a list of files that were impacted by bad sectors.

- Firmware issues
- Magnetic layer wear
- Bad sectors (ECC errors)

Insight is equipped with various functionality for damaged media:

- [Automatic checkup](#) to identify the damage
- Complex [multipass imaging algorithms](#)
- [Disabling damaged heads](#) for faster and safer imaging
- Control of [read look-ahead and other device features](#)
- Calculation of [segmented hashes](#) for image verification
- [Reset and power cycle commands](#) for imaging freezing drives
- Overcurrent and [short-circuit protection](#)
- [Bad sector recovery](#) for sectors with damaged ECC fields

However, the system does not perform drive repair. We advise that a drive's hardware-related problems be referred to data recovery labs.

## Is Atola planning to discontinue the support for DiskSense units (manufactured between 2014 and 2021)?

Atola Insight Forensic is in high demand and has a strong user base. We are not planning to discontinue either of these imaging systems. We have several years' worth of exciting new features planned for both systems.

DiskSense hardware units (the first generation of hardware for Atola Insight Forensic imager) will continue to be supported in the foreseeable future and will include the same features as the new, higher-capacity DiskSense 2 hardware units.

We at Atola stand by our products. Remember that your system is covered by a [lifetime warranty](#) for as long as you keep your subscription active. The subscription's other benefits include software updates and fast and effective support from our team of engineers who develop the software and know all the ins and outs of the product.

These are just some of the key features that Insight offers. For more details, see the [full product overview](#).

## Hardware unit and installation

### Why does my DiskSense hardware unit not boot?

It is very likely that there is a USB device plugged into the unit, which is preventing it from booting properly. Try detaching all USB cables and restarting the hardware unit. If that has not worked, follow these steps to fully reset:

1. Power the hardware unit off.
2. Detach any cables and devices (including PSU cable, Extension module, all SATA cables and any USB devices or cables).
3. Leave it powered off for 3-5 minutes to reset fully. A few internal circuits need up to a minute to fully reset, but waiting a bit longer may help.
4. Plug in only the power cable (do not connect network, USB, or SATA cables yet).
5. Power the system on and check the **PWR** LED on the back side of the unit after 15 seconds.

### The previous boot attempt was interrupted and now the unit does not boot. What should I do?

Connect a monitor directly to the unit's HDMI or VGA port. If you see a BIOS message saying *Would you like to restore Fastboot on the next boot? (Y/N)*, it is likely that the previous boot was interrupted at a specific stage.

The most straightforward solution here is to plug a USB keyboard into one of the USB ports and press the *N* key. After the unit has booted successfully, please restart it again to make sure the next boot cycle is smooth.

### Why does Windows 10 (32-bit) show a hardlock.sys error during installation?

It looks like a HASP dongle run-time installation issue. You can install the newest run-time by following an alternative procedure:

1. Download the new HASP run-time version from [this page](#).
2. Unzip it.
3. Temporarily disable firewall and antivirus.
4. Run Command Prompt as Administrator and change the folder to the one containing the downloaded file (from step 1).
5. Execute the following commands:

```
haspdinst.exe -r -fr -kp -fss -purge  
haspdinst.exe -i -fi -kp -fss
```
6. Launch Atola Insight Forensic.

### Windows crashes with a blue screen when launching Atola Insight Forensic. How can I fix this?

Microsoft updated Windows 10 (October 2020), and it broke the support of the HASP run-time v6.60.

The issue was fixed in Atola Insight Forensic version 4.17. For software versions 4.16 and older, please download and install the newest run-time following these steps:

1. [Download](#) the newest HASP run-time version.
2. Unzip it.
3. Run and install *HASPUserSetup.exe*.
4. Launch Atola Insight Forensic.

## Insight software is stuck in the 'Searching for the DiskSense unit' window. How can I solve this issue?

It appears that your unit's HASP is not detected. Please check if you can still ping the DiskSense unit's IP address from Windows PC. Then try the following steps:

1. Open <http://localhost:1947> in a web browser.
2. Click **Configuration** in the left menu.
3. Click **Access to Remote License Managers**.
4. Enable the following two options:
  - **Broadcast Search for Remote Licenses**
  - **Aggressive Search for Remote Licenses**
5. Wait a minute.

The **Remote License Search Parameters** field must be either empty or contain the DiskSense unit's IP address (the latter is preferable).

## How to fix an error "To run this application you must install .NET" (Insight 5.1–5.3 versions only)?

Atola Insight Forensic versions 5.1–5.3 are based on .NET 5. To resolve this issue, install the latest version of .NET 5 64-bit Desktop Runtime:

[Download .NET Desktop 5.0.17](#)

## Connectivity

### How do I reset the IP address of the hardware unit?

You can reset the DiskSense unit's IP address by holding the small **IP RST** button on the back. You should keep holding the button until the **PWR** LED stops blinking. Then the unit's IP address will be reset to *192.168.0.188* and *10.0.0.188*.

### How to change the hardware unit's IP address?

The system has been designed to work in the most commonly used networks and has the IP addresses *10.0.0.188*, *172.16.0.188*, *192.168.0.188*, *169.254.0.188*.

If your network uses one of these subnets (*10.0.0.\**, *172.16.0.\**, *192.168.0.\**, *169.254.0.\**), and the IP address ending in *188* is free, you can simply connect the unit to

### I am able to ping the Insight's hardware unit but cannot connect to it. Why?

Here are the possible reasons:

- The unit has two Ethernet ports, but only the **ETH1** port can be used to interact with the Insight software. Make sure the Ethernet cable is connected to the DiskSense unit's **ETH1** port.
- Firewall or anti-malware software may be blocking communication (while ping might work, other ports could be filtered). Try disabling the firewall or anti-malware software and restart the Insight software.
- IP address conflict. Please double-check the IP address of your PC's Ethernet card. The fourth digit in it must be different from that of the DiskSense unit. For example, if the DiskSense unit's IP address is *192.168.0.188*, then the PC's IP

the network. Then run the Insight software, select the default unit IP ending in *188*, and click **Insight > Modify DiskSense Unit IP**.

If your network has a different subnet address, follow these steps:

1. Connect your PC to the DiskSense unit with an Ethernet cable.
2. Go to **Settings > Network & Internet > Change adapter options**.
3. Find the Ethernet connection with the unit, right-click it and click **Properties**.
4. Find **Internet Protocol Version 4 (TCP/IPv4)** in the list, select it and click the **Properties** button.
5. Select the **Use the following IP address** option, enter *192.168.0.5* and click **OK**.
6. Disable other Ethernet and Wi-Fi connections to avoid IP conflicts.
7. Change the IP address to the one you need.
8. If your PC and the unit belong to different subnets, the connection will be lost. Re-enable the connection in **Network and Internet**.
9. Connect the DiskSense unit to your network with an Ethernet cable and run Atola Insight Forensic.

## I connected the DiskSense unit directly to my PC's second Ethernet card, but I cannot ping it or connect to it. What should I do?

First and foremost, check whether you can ping the unit when it is connected directly via your second Ethernet adapter.

1. If ping attempts are unsuccessful, double-check the IP address of the Ethernet adapter. It should be in the same subnetwork as the unit. The default unit IP addresses (if unchanged) are:  
*192.168.0.188, 10.0.0.188*.
2. Check if you have another network connection and its IP address.
3. If another connection exists, assign a static IP address from a different subnet to the Ethernet adapter.

address should be different—such as *192.168.0.100*.

- The HASP drivers have not been installed correctly. To verify this, visit the [localhost:1947](http://localhost:1947) page. (It may take up to 5 minutes for the HASP keys to appear after powering on the unit.) There is a HASP dongle inside the unit that the Atola Insight software connects to. If you do not see any HASP keys in the list, this indicates the problem. Rerun the installation and make sure to click OK in all pop-up windows as one of them should be the HASP installation. This step will only succeed if a HASP key appears in the web browser.
- The router or switch your unit is connected to may not be configured correctly, especially if it is a Wi-Fi router. Try connecting the unit directly to your PC using an Ethernet connection. You can use the USB-to-Ethernet adapter included in the package.

If these steps prove ineffective, try updating your PC's Windows installation.

## How can I prevent connection losses when I use a USB-to-Ethernet adapter (NIC)?

Certain platforms may experience issues with these adapters, especially after large amounts of data have been transferred.

This may be a USB-related issue, for example, a memory leak in the USB driver that builds up after several days of high-speed transfers.

Try replacing the adapter with a similar one:

- [ASIX AX88179 chipset](#)
- [aRTL8153 chipset](#)

Examples:

- Other network card's IP address on your PC: *192.168.0.5* — set the IP address to *10.0.0.200*.
- Other network card's IP address on your PC: *10.0.0.5* — set the IP address to *192.168.0.5*.

4. Connect to the DiskSense unit by specifying its address in Atola Insight Forensic:

- *10.0.0.188* — if you set *10.0.0.200* as the second Ethernet adapter's IP address
- *192.168.0.188* — if you set *192.168.0.5* as the second Ethernet adapter's IP address

## Drive ports

### **The USB flash drive or USB port is not working. What could be the issue?**

It's very unlikely that your DiskSense system is faulty. Also, keep in mind that all USB ports are native to the motherboard, with no adapters in between. Nevertheless, let's run diagnostics to determine what is working and what is not:

1. Remove all USB flash drives.
2. Power-cycle the DiskSense system to reset USB ports to their initial state.
3. Take a new USB flash stick which is good and working.
4. Plug it into the **USB Target** port.
5. Press **F4** and wait until target device scanning is complete.
6. Plug the same USB flash drive into the **USB Source** port.
7. Press **F3** and wait until source device scanning is complete.

This is a reliable test for checking USB ports. It would be great if you can run the scenario several times using different USB flash drives. Note that the second step (power-cycling the DiskSense system) is essential for accurate test results.

## Imaging

### Does write protection work only for SATA source drives?

Write protection works for all source ports: SATA, IDE, USB and extensions.

### How do I image an NVMe drive?

Use the [M.2 extension module](#).

### How do I image a drive soldered into a laptop?

You can add up to 3 remote network drives simultaneously and image them in parallel using the iSCSI protocol.

To image a remote device via the iSCSI protocol, follow these steps:

1. Expose a physical or logical drive via iSCSI on a network. For that task, you can use our [Python script](#) that automatically creates iSCSI targets for all drives except the boot device.
2. In Insight, go to **Source > Select Source**.
3. In the Source Device Selection window, click the **Add iSCSI device link** and follow the instructions.

Insight also supports imaging of specific models of MacBooks Pro and Air released in 2016-2017. Here is a manual article on [how to image them using a Thunderbolt extension](#).

### How do I create or format an NTFS partition on a target drive?

Insight supports creating exFAT partitions (including encrypted ones) on target drives for subsequent imaging to files stored on them. However, creation or formatting of NTFS partitions is not supported.

### How do I ensure that *Target HEX Viewer* does not save any data to persistent storage?

Here is how **Target HEX Viewer** works internally. It has two modes:

1. **Automatic refresh** is performed when **Freeze** checkbox is inactive. Every time a block of data is imaged, one sector from this block is sent to the Windows software via Ethernet. Insight's software receives the sector and displays it in the **Target HEX Viewer** wiping the previous one. Thus, it performs an automatic refresh on-the-fly and does not save any data to persistent storage (e.g., a hard drive).
2. **Manual Read Sectors** can only be run by clicking on the **Read Sector...** button. This initiates the reading of a specified sector from one of the target devices. The read sector resides only in RAM temporarily while it is displayed in the **Target HEX Viewer**. Similarly to the **Automatic refresh**, no data is saved to any persistent storage during manual read sectors.

## Why could the mapped network drive be unavailable during Image File selection?

The shared folder mapped as a network drive on the local PC is unavailable. This issue occurs in Windows 10 and is caused by [Microsoft's native components](#) we use to select files.

Microsoft [explains this with UAC being enabled and suggests editing the Windows registry](#) as a workaround.

Note that the mapped network drive is just a shortcut for the longer network path. Always select the **Network** part of the tree view and choose the same network folder. Insight will remember the last selected path and open it when you select another image file.

## How do I image into split (segmented) raw files?

Segmented imaging into RAW files is supported. You can split the image into segments (chunks) on the home page of the target image port. Follow these step-by-step instructions:

1. In the sidebar, click **Imaging**.
2. Click **Create New Session**.
3. In the **Target device selection** window, click **Create image file**.
4. Click the **Select** button.
5. On the top port panel, select the **Image file** port.
6. Click **Edit file options**.
7. Change **Chunk size** to a preferred value in the combo box.
8. On the top port panel, select the **Source** port.
9. Click the **Start Imaging** button.

## Will an E01 file created by Insight open in Encase?

E01 files may fail to open in Encase typically due to a file handle held by Insight. It can manifest itself in CRC errors during Encase verification. To resolve this, close the E01 file's port in the Insight's top panel before opening the file in Encase.

Note that Encase caches unsuccessful verification results for the E01 file (or E01 file with the same metadata). Therefore, you may need to clear the cache or start a new case in the EnCase application.

## How to solve an issue with the max path length / folder length?

Make sure that the path length does not exceed the [limit set in Windows API](#).

Atola Insight supports file paths up to 32,767 characters in length.

If you are unable to move the files using Windows Explorer, you can use the `subst` command to shorten the file path. Follow these steps to resolve the issue:

1. Substitute the folder that has a long file path with a drive letter to shorten the overall character count for the files contained in the folder.
2. Copy or move the files to a different folder with a shorter path that does not exceed the Windows path length limit.
3. Delete the mapped folder.

## Why does the artifact finder not find artifacts in files (.pdf, .pst, .docx, etc.)?

Artifact finder performs a low-level, sector-by-sector search without parsing file structure or interpreting specific file formats (.pdf, .pst, .docx).

Instead, Insight's search engine detects keywords, IP addresses, URLs, and other artifacts in raw drive space. This way, it complements the traditional analysis via Magnet AXIOM, X-Ways Forensics, etc.

## What is the difference between a standard IMG and a preallocated IMGP image file?

An IMGP file's contents are identical to those of an IMG file: it is the same raw bit-for-bit source copy. The only difference is that Insight preallocates space within an IMGP file, filling it with zeros until the last LBA, so that the IMGP file is the same size as the source even before imaging begins.

An IMGP file is used to preallocate space on the target media. Our customers use it when storing image files on a remote server for the entire organization. This ensures that, as the image file grows to its final size, there will be no risk of running out of space.

To mount it to any other forensic software, one can just change IMGP target file image extension to .img, .dd, .raw or any other file extensions they want.

To continue working with an IMGP file in Insight after changing its extension, change the image file extension back to .imgp.

## When should I use *All sectors with data* and *All sectors with metadata* imaging options?

These options define the scope of imaging.

**All sectors with data** is used to image only the sectors belonging to files of all detected partitions. The exception is partitions that Insight cannot parse (rare types, e.g. UFS, ReiserFS), which will be imaged in their entirety.

**All sectors with metadata** results in a complete directory tree with files without the file data. Partitions store metadata in specific structures (e.g. \$MFT for NTFS). Metadata includes file name, access/modification timestamps, attributes and the exact sector numbers of the corresponding file data.

[This screencast](#) explains how to make use of metadata imaging.

Another benefit of Insight's artifact search is that it scans the entire drive, including unallocated space. It helps find evidence at the sector level, where other tools could miss it.

## Why does a USB drive imaging produce read errors?

To rule out cable issues, consider using short, high-quality USB 3.0 cables. Longer or lower-quality USB 3.0 cables may cause read errors during acquisition.

# Performance

## How do I achieve the best performance when imaging to the network?

To avoid potential bottlenecks, make sure of the following:

- You are using a [10Gbit Ethernet adapter](#).
- All the network cables are 5e category or higher.
- The network switch supports 10Gbit Ethernet and is configured correctly (if Insight is not connected directly to a PC).
- For maximum performance, connect Insight directly to the PC's Ethernet adapter without intermediate network switches.

Other factors that could affect transfer speeds are network adapter drivers, motherboard drivers, antivirus software and so on. However, following the guidelines above is sufficient for most cases.

## Does Insight always image at the max speeds listed on this website?

The [max speeds](#) have been [lab-tested for accuracy on modern storage devices](#).

However, actual imaging speed depends on the native performance of the devices involved. During the drive-to-drive imaging, the slower device will determine the actual data transfer rate because one drive can only receive data as fast as the other can send it, and vice versa. When imaging to or from the network, another potential bottleneck is the bandwidth.

## How much does data transfer speed vary during imaging?

Insight can reach speeds of up to 500 MB/sec, but speeds may drop to as low as 50 MB/sec (3 GB per minute) when working with older or slower HDD models.

## How do I verify the data transfer rate from Insight to the network?

Follow these steps:

1. Launch Atola Insight Forensic software.
2. Connect a fast SSD (e.g. Samsung 860 PRO/EVO or any other that can image at 500+ MB/sec) to the SATA Source port of the DiskSense unit.
3. Go to **Imaging** and select the **Imaging to File** option.
4. In the file selection dialog, enter *null* file name. This special file name will make Insight read the source at the highest possible speed and skip writing, so that target write speed does not affect the measurement, while data is still transferred through Ethernet.
5. Start imaging.

If everything is working properly, the speeds will be between 50 MB/s and 500 MB/sec, depending on the native speed of the source drive.

# Damaged media & File recovery

## You claim that Atola Insight Forensic is capable of imaging even bad drives. What does a bad drive mean?

By bad drives, we imply various types of drive issues, namely:

- Scratches on the media surface
- Magnetic layer wear-out
- Degraded or even non-working head
- Drive freeze after reading attempt
- Firmware issues
- Bad sectors
- Short circuit on PCB

## How exactly does the Atola Insight imaging process handle damaged drives?

We have two goals here when dealing with severely damaged source drives:

1. Get as much data as possible.
2. Decrease the number of failed read attempts to finish imaging with a still-alive evidence drive.

Atola Insight Forensic uses a fast imaging map, thereby enabling us to run the whole process in multiple passes. The tool uses large blocks with short time-outs on the first few passes and then smaller blocks with longer time-outs on the last pass to image the tough areas. This provides the best possible results in the shortest amount of time.

Atola Insight's ability to disable damaged heads can save your evidence! Other imagers may cause further damage to the media during such imaging.

Imagine having seven out of eight good heads. You can image data with all of them except the damaged one. Afterward, you can begin analysis of 87% of the acquired data and at the same time try to replace the damaged head. A physical head swap is always a risky endeavor.

## How do I identify which of the imaged files contains bad sectors?

1. Select the target device or image file.  
Alternatively, on the **Imaging results** screen, click the **Analyze target image** button.
2. Go to **File Recovery** and open the partition.
3. Click **Create file list** and select **All files**.
4. Select **Files that were partially imaged** and click **Create** for the list to be saved in a .CSV file.

***NB** If the imaging session was interrupted or the range of sectors scheduled for the session did not cover the whole partition (and therefore some of the files), the list of partially imaged files may contain both files with bad sectors and those not covered by the imaging session.*

## How do I find where the bad sectors are located within a file?

When imaging, Insight automatically creates a **Media Map** that reflects the status of all sectors imaged during a given session, namely:

- imaged sectors
- unimaged sectors (with errors or those beyond the imaged range)
- sectors imaged without ECC

To look up the Media Map:

1. In the **Imaging results** screen, click the **Analyze target image** button. Or select the target device or file.
2. Go to **File Recovery** and open the partition.
3. By clicking the individual files, look up an individual **File Map** and see which of the sectors have or have not been successfully imaged.

The imaging engine contains multiple automatic rules. For example, it resets or power-cycles the device when a source drive freezes. It can apply a reverse imaging direction in particular cases. A helpful feature when working with damaged evidence is that two imaging reports are generated: one before and one after the process. Both include not only the imaging information but also SMART tables, thus enabling you to see what happened to the source drive during the process.

Learn more in these articles:

- [Multipass imaging of damaged drives](#)
- [Imaging drives with damaged heads](#)
- [Imaging freezing damaged drives](#)
- [Imaging a shorted drive](#)

## Does Insight support damaged SSD drives?

Atola Insight Forensic does support damaged SSDs. It can automatically diagnose SSDs and generate a detailed, well-structured report. Insight's imaging process can retrieve all readable data from solid-state drives using multipass and read error recovery subsystems. It's fair to say you receive pretty much the same functionality as with standard HDDs. The only exception: unknown password removal and firmware recovery are not supported for SSDs.

In addition to that, Insight Forensic supports custom PCIe SSDs from Apple MacBooks. It works fast via a proprietary [Atola extension](#).

## Can Atola imagers acquire evidence from damaged SSDs?

As is true with any type of media, the degree of damage will inform how we can help with data recovery from a specific device. SSD failures fall into three major categories: logical errors, hardware issues, and firmware failure.

Atola imagers may be able to image data from an SSD with logical errors or hardware issues (e.g. NAND flash wear-out) using our multipass imaging system. A good

## When encountering bad sectors on the source drive during imaging, how does Insight handle the corresponding sectors on the target drive?

Such sectors can be either left alone (skipped) or filled with a pattern. The default pattern used to fill unreadable sectors is `00`. However, you can enter any other pattern or load a pattern (of any length) from a file. To use this option:

1. Go to **Imaging > Create New Session**.
2. Select your target device.
3. On the imaging settings screen, in the **Preset** section, click the **Show settings** link.
4. On the **Error handling** tab, select the **Fill unreadable sectors with the following pattern (HEX)** option.
5. Leave the default pattern as it is or enter/upload a new one.
6. To make this new pattern the default one, click the **Save settings** button. Otherwise, simply click the **Start imaging** button.

## How do I compare the files on a source and a target using their hashes?

To compare the files on the two devices:

1. Select the **Source** device.
2. In the sidebar, go to **File Recovery**.
3. Click **Hash all files**.
4. If the hash column is missing, enable it in **Preferences > File Recovery**.
5. Select all files.
6. Click **Create file list** and select **All files**.
7. Select the **Show file hash** option.
8. Repeat steps 1-5 for the target drive.

predictor of success can be the [Media Scan](#) stage of the diagnostics process.

## What is the success rate of File recovery?

You can recover up to 100% of files imaged with Insight only if the internal file system structure has been successfully imaged. Follow these steps:

1. Select an acquired image on the **Target** port.
2. Go to **File Recovery**.
3. Try to open all the imaged partitions.
4. If partitions do not open, use dedicated DR software to recover the files (e.g. R-Studio).
5. If the partitions do open, you have two options:
  - o Select and recover all files. Then use the **Create file list** button to generate a list of partially imaged files.
  - o Alternatively, manually select all files with **100%** values in the **Copied** column. Some hints for you:
    - By sorting the files in the **Copied** column you can group 100% of imaged files from a specific directory.
    - Selection of multiple objects is available.

## Can you recover data from a deleted file?

Even if a user deletes a file from a computer or even the Recycle Bin, it does not mean that all file data has been erased from the drive. While the record of the file in the filesystem has been removed, the data from the file remain in the sectors to which it had been recorded.

However, over time, the old data may be overwritten with new files and their data. Therefore the more the drive is being used, the lower the likelihood that data from a deleted file remains intact.

Here is how Insight can help retrieve this data

In the end, you get two complete file lists and can compare them using third-party software, for example [Compare++](#).

## How do I use black and white hash lists to filter data?

Watch [this screencast about using hash lists in Insight](#).

For the full step-by-step guidance, see [Hash lists to filter good & bad files](#).

Also, you can find [two use cases in White/Black hash lists](#) section in our blog.

## When should I use the reverse imaging option, and is there a downside to it?

Normally, reverse imaging is beneficial when there is a spot/scratch resulting in a number of bad sectors on the surface area. Reverse imaging (from the inner to the outer tracks) on one of the imaging passes helps you narrow down the bad area faster. It also allows you to get more data from the good areas of the drive before entering the damaged zone and digging into it to retrieve data.

As for the downsides, reverse imaging leads to a speed decrease because HDD's heads have to make additional moves to perform it, and caching is impossible.

## How do I change timeout in the imaging settings on-the-fly?

Changing timeout is only possible when you are creating a new session. Here is how to work around it:

1. Pause the current imaging session by clicking the **Pause** button.
2. Click the **Add New Session** link.
3. Open imaging settings and change timeout of the following pass(es).

***NB** The new imaging session will complement the previous one and will only attempt to retrieve data from the sectors that have not yet been copied.*

If you know any details from the file contents, search for keywords or other artifacts in Insight's [Artifact Finder](#). Unlike most other forensic analysis tools, Insight's Artifact Finder parses data not on the file system level but on the sector level. This gives you the advantage of finding data from deleted files.

The File Recovery module can recover deleted files in these file systems: NTFS (all versions), FAT16, FAT32, HFS, HFS+, HFSX.

Modern SSDs wipe the sectors belonging to the deleted files at the command of an operating system (Windows, Linux, macOS) shortly after the files have been deleted:

1. The operating system sends the Trim command to the sectors belonging to the deleted files.
2. The SSD controller decides when to wipe them.
3. The trimmed sectors are replaced by new ones from the over-provisioning zone.
4. Trimmed sectors are then shortly used for new data.

This means that SSDs provide a much lower chance of recovering such data from deleted files.

## Does Insight support mounting of a damaged APFS partition?

Partition search in Insight is quite advanced; it is more than just looking into MBR/GPT records and involves our unique heuristic algorithm.

It means that Insight should be able to find a partition, and the partition should not be damaged. For cases of damaged partitions, our customers use forensic software that performs file carving or DR software (e.g. R-Studio).

The only [File Recovery functionality](#) that works when there is missing data is the ability to find deleted files in several partition types including NTFS, HFS, FAT.

Some imaging pass settings can be adjusted on the fly—for example, enabling reverse imaging for the next pass.

## How do I look up a drive's G-List with Insight?

Firmware recovery has not been our focus for many years now; therefore, Insight has limited firmware recovery functionality. While some models may provide information about the G-List (see [3. Full firmware access](#)), the G-List is not a kind of information you automatically see on the screen. You would need to manually find the G-List among firmware modules, which requires a certain level of data recovery knowledge.

## Can I turn off bad sector reallocation (or clear the G-List) for a Seagate drive?

Unfortunately, Insight does not handle bad sector reallocation automatically. You may find more info on [data recovery forums](#) by searching for:

- your Seagate drive model
- G-List cleaning
- bad sector reallocation

Here is the information about [terminal commands for modern Seagate drives](#).

## What should I do if Insight can't identify a Seagate drive and shows an inaccurate device capacity?

Zero-capacity typically implies firmware issues, which may be corrected via the serial port in the case of Seagate drives. Atola Insight Forensic enables you to take advantage of a [serial connection](#).

We do not have many guides about fixing specific Seagate issues, which would require extensive knowledge of the Seagate terminal command system. But [here is another article in the manual that may be helpful](#).

# Diagnostics

## How does diagnostics work, and how accurate is it?

The automatic diagnostic function applies a sophisticated system that analyzes electrical currents as they enter and leave the hard drive, examines the hard drive's responsiveness to low-level commands and incorporates firmware information (if it is accessible). Our studies have shown that this approach is accurate in pinpointing malfunctions in at least 95% of cases.

## How do I analyze electrical currents from the oscilloscope if I received no training?

Some data from the oscilloscope is straightforward to understand (for example, when HDD power fails, the lines go flat). Users can learn to understand more complex oscilloscope information by seeking advice from other data recovery technicians, seeking professional training, or simply by gaining experience in the field.

While current monitoring technology plays an important role in Insight's operation, no specific skills are required because the system performs current analysis automatically.

## How does Insight detect the capacity of hybrid drives?

There are [two types of hybrid drives](#).

1. *Dual-drive hybrid systems*. In this case, Insight shows the total capacity, which is the sum of the volumes of both drives. All sectors are addressable and readable.
2. *Solid-state hybrid drive (SSHD)*. For such drives, Insight detects and displays only the capacity of the HDD because the internal SSD is designed to be inaccessible without a chip-off procedure. Hybrid drives of this type use NAND memory (small SSD) for cache. The cached data resides in both the HDD and the NAND chip. What is cached

## Can RAID arrays be diagnosed as a single HDD?

Insight can diagnose only the drives that are directly connected to the hardware unit. Hard drives from RAID arrays must be diagnosed and recovered individually.

[Atola TaskForce](#) is capable of automatically assembling RAID drives into a single virtual device even when the RAID configuration is unknown.

## Why is there a difference in the quantity of errors and performance between Media Scan and Imaging?

The short explanation: Imaging uses different commands and a different level of reading thoroughness than Media Scan.

Imaging reads data and sends it over a data cable (SATA, PATA, USB). At the same time, Media Scan utilizes a low-level Verify command that checks a block of sectors for an error with no data transfer involved.

The two operations are not equally thorough. Media Scan verifies the drive surface block by block (2048 sectors per block). It does not dig in searching for specific bad sectors in a 2048-sector error block.

As opposed to that, the imaging engine has a goal to image as much data as possible. The [multipass system](#) is used during imaging.

However, if linear hashing is enabled, imaging switches to one pass with a 4096-sector block size by default using this algorithm:

1. Read 4096 sectors.
2. If a read error occurs, re-read the sector range using a 256-sector block.
3. Read the first 256 of 4096 sectors.
4. If there is a read error, re-read the 256-sector range sector by sector.
5. Read the first sector of the 256 (within the original 4096).

and how it is cached depends on the drive model and firmware algorithms.

## Hashing

### How do I calculate a hash during imaging, and do I need to use both linear and segmented hashing

Hashing is disabled in the default settings. Select the **Hash source during imaging** option in the **Default (5 passes)** preset.

Here are the guides on [calculating linear hash during imaging](#) and [segmented hashing](#).

Segmented hashing is the only tried-and-tested way to verify an image of a damaged source drive. A segmented hash can be calculated during multipass imaging, which lets you retrieve more data while covering all imaged intervals with a set of hashes,—an ability that has proven crucial for our customers in court.

Besides, with segmented hashing, the image remains usable even if some of the data gets corrupted over time (due to human error, buggy software, hardware issues or power loss): it allows you to identify the segment of data that was corrupted and continue using the good parts of the image

### Do courts of law accept segmented hashing as a valid way of verifying data?

Yes, [segmented hashing](#) has been a principle that forensic examiners successfully follow in their work. This principle is well laid out in academic works and is also widely used in cryptography and secure data modification. Meanwhile, in digital forensics, several vendors who support AFF4 image files have adopted the same principle. Among them are X-Ways, Magnet Axion, GetData Forensic Explorer, Encase Forensic, etc.

Most importantly, with the forensic examiner's proper understanding of the concept and ability to demonstrate it to the court, segmented hashing is as good a

### How does hashing work in parallel with imaging?

When Insight images and calculates hash in parallel, here is how our imaging engine works:

1. Read *block A* from the source to RAM.
2. Hash *block A* + Write *block A* to the target + Read *block B* from the source - all these three actions execute in parallel.
3. Hash *block B* + Write *block B* to the target + Read *block C* from the source...
4. and so on

Two important rules:

- If *read* block fails with an error/timeout, the block is replaced by an unreadable pattern (it can be set by the user).
- If *write* block fails, Insight stops imaging and reverts the *hash* state one block backwards.

verification method as any.

## Fill/Erase

### Why do I need to wipe/erase the target before imaging data onto it?

Certain forensic evidence acquisition or data recovery scenarios require the target hard drive to be wiped/erased prior to imaging. It ensures that the software being used to recover files won't extract old data that was previously on the destination HDD.

### How does *write verification* work in Fill/Erase?

Here is how the algorithm works during the wiping process in Insight:

1. 100 individual sectors selected evenly across the range are filled with the verification pattern *Atola Insight*.
2. The whole drive or a selected range of sectors on it are wiped applying the method selected by the user (*Erase with pattern* by default).
3. The 100 sectors filled with *Atola Insight* during the first step are read to ensure that none of them contains the pattern.

### 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 the SSD's firmware which sectors can be wiped by marking them as '*dirty*'.

Time of erasure of '*dirty*' sectors depends on the SSD manufacturer and firmware. For instance, recent Samsung SSDs have what is 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 the full erasure of an SSD, including non-addressable areas.

## Case Management

### How do I change the path to the Work Folder?

To change the path to the **Work Folder**, go to **Insight > Preferences > Work folder path**, change the directory and click the **Apply** button.

### How do I add notes to the case history after a case was closed?

The quickest and easiest way is to open case history **Cases > Search/Open** and click **Add note**.

## How do I free up storage space in the Work folder?

Depending on the features and settings you use, Insight saves different kinds of data in its **Work Folder**.

- Make sure to disable an on-the-fly artifact search in the imaging settings. Storage space is consumed most aggressively when [artifact search](#) is enabled. When artifact search is enabled in the imaging settings, you may be gathering and storing substantial amounts of data.
- The same goes for [File Signatures](#). Disabling this setting results in much less data being stored, yet it may accumulate and become considerable over time. This setting can be disabled in the Miscellaneous tab of the imaging settings.
- Last but not least, if you no longer need the results of a previously performed artifact search, you can delete all *ArtifactFinder* subfolders to free up space. *ArtifactFinder* subfolders are located at paths similar to this: `C:\Atola Insight Forensic\Work\02_ST1500DM003\ArtifactFinder`, where:
  - `C:\Atola Insight Forensic\Work` - work folder path
  - `\02_ST1500DM003` - device case subfolder

## After I changed the Work folder, how do I move files from the previously created cases to the new folder?

This can be done manually:

1. In the top right corner, click the **Case Number** button.
2. The **Change Case Details** window opens. The **Case Home Path** in it indicates the directory where case files will be moved.
3. Click **OK**. The **Case Home Path** has now been changed in the database and all case files have been moved to the new case folder.

## How do I copy Insight database to another PC?

Yes, it is possible: go to **Cases > Export** and select **All cases**. A single file will be generated, which can later be imported via **Cases > Import**.

## Why are some cases missing in the Search window after database setup?

Most likely, you selected either an incorrect Work Folder or SQL Server.

Insight's database consists of SQL Server data and Work folder files. Large files like imaging maps, file signatures, artifacts and report logs are saved in the Work folder, while the case information, including report data, is stored on the SQL Server.

Two Insight settings refer to that:

- Work folder
- Database connection settings

`\\networkpath\Atola` is the work folder we need. First of all, it must be specified in **Insight > Preferences > Work folder path setting**.

1. Open **Insight > Database Connection Settings**.
2. Select server type: **Remote** (in some cases, it can be **Local**).
3. Enter the **Computer name** from the work folder's network path.
4. Click the **Search** link next to the **SQL server name** field.
5. Select one of the found SQL servers.
6. Click the **Search** link next to the **Database name** field.
7. Select one of the found databases.
8. Click **OK**.
9. Restart Atola Insight Forensic software.
10. Check **Cases > Search/Open** for your cases.

## How can I tell who worked with the drive if I am working on a previously created case?

You can open any operation performed with a hard drive by clicking on the corresponding link in the case history. In the report header, you can see which computer was used, and thus deduce which user worked on this phase of the case.

## Can two hard drives share the same case number if they are related?

Yes, it is possible to assign the same case number to multiple hard drives. It helps keep track of hard drives related to the same investigation.

If cases do not appear, try different combinations of the database name, the SQL server name, and the computer name.

## Device Recovery

### I don't seem to be able to unlock an SSD or a USB drive with Insight. What could be the issue?

Insight supports unlocking passwords of a limited range of drives. While we would like to provide you with maximum support, it is impossible due to the firmware of different drive families being very vendor-specific. Please check the [list of supported drives](#).

We have primarily developed this functionality for hard drives, but extending this functionality to SSDs or USBs would require a prohibitive amount of work to support the huge range of firmware types and controllers. Unfortunately, this functionality has not been the focus of our attention.

### How do I decrypt a BitLocker volume in Insight?

For the time being, Insight supports only the [decryption of APFS partitions](#) with a known password or recovery key.

### I'm having trouble unlocking the Seagate drive connected to the Serial COM port (RS-232). What could help?

First and foremost, we recommend double-checking that the serial cable connection and selected baud rate are correct. Here is the easiest way:

1. Power off the Seagate drive.
2. Connect cables.
3. In Insight, open **Windows > Terminal**.
4. Select baud rate: 38400 (most likely for modern drives)
5. Power on the Seagate drive.

As for BitLocker partitions, Insight detects BitLocker volumes and displays their GUID and type during imaging and diagnostics. While imaging, Insight immediately adds a log record with the start LBA of a BitLocker volume when encountering it.

## **Password removal: How do hard drives become locked with ATA passwords?**

ATA password can be set through the computer's BIOS. In addition, specialized utilities—both commercial and freeware—can set or modify ATA passwords. Examples include commercial tools like Insight, as well as free utilities such as hdparm (Linux) and Victoria HDD (Windows). These tools communicate directly with the drive's firmware, allowing users to set, change, or remove ATA passwords outside of the BIOS environment.

## **Password removal: For which hard drives is password removal supported?**

Automatic password removal is supported for at least 50% of hard drives available on the market. For details about specific models, see [Supported drives](#).

## **Can Atola imagers retrieve data from water-damaged hard drives?**

Depending on many factors, the impact on the drive can vary considerably. The kind of contact (which can range from sprinkles to complete submergence), the duration of such impact and even the composition of the water (if there is residue in the form of salts) all matter.

Additionally, the disk might have been damaged before the drowning, so water may not be the only problem.

Therefore, we recommend that you bring such drives to a cleanroom. At the cleanroom, engineers will perform drying, the initial damage assessment, repair, and cleaning. When drying, it's better to keep the temperature at a reasonable level, such as 100-200 degrees Celsius. Do not heat the PCB to the point where the solder or plastic starts to melt.

## **Firmware recovery: Which hard drive models does the Insight support firmware recovery for?**

There are two ways in which Insight provides firmware recovery: by automatically repairing firmware and by providing direct access to firmware files for manual repair.

Different sets of hard drive models are supported for each of these approaches due to differences in the firmware design by the hard drive manufacturers. For a complete and up-to-date list of supported hard drive models for firmware recovery, see [Supported drives](#).

## **Firmware recovery: How common is firmware corruption in modern hard drives?**

Less than 10% of data recovery cases with modern hard drives involve firmware corruption. Occasionally, a manufacturer will release a hard drive with flawed firmware, and data recovery labs will see a spike in firmware recovery jobs for a period of time.

## **Firmware recovery: What is the difference between firmware files stored on the HDD platter and those stored in ROM/EEPROM/NVRAM?**

This depends on the HDD manufacturer and hard drive model. Each hard drive has its own specifications for where firmware data is stored.