RECON ITR / RECON IMAGER Manual

SUMURI LLC

RECON ITR 1.3.0 / RECON IMAGER 6.1.1

May 6, 2025

1 RECON ITR Introduction

RECON ITR is SUMURI's premier **forensic imaging, triage, and reporting solution**, built from the ground up for macOS. It is designed to meet the needs of both **beginner** and **advanced forensic examiners**, enabling fast and reliable acquisition and analysis of Mac systems.

Imaging Capabilities

- **RECON ITR** provides a **built-in forensic imager** that allows examiners to swiftly acquire images of:
    - **APFS volumes** and **Synthesized APFS Containers** on modern Macs.
    - **Physical drives** (full disk images) on **pre-T2 Intel Macs**.
- On Macs with a **Secure Enclave** (T2 and Apple Silicon), **physical imaging is not possible**; examiners must target volumes or containers instead.
- **External hard drives** and removable storage devices may also be physically imaged when connected to the Mac.
- For cases where a full forensic image is not necessary, RECON ITR offers a **selective logical imaging option** to capture only relevant files or artifacts.

Triage Capabilities

- **RECON ITR** includes powerful **live triage functionality** for field use.
- Examiners can quickly leverage **hundreds of built-in plugins** to **parse thousands of artifacts** across macOS systems.
- Triage can be performed on a **running live system** or a **mounted drive** connected via **Target Disk Mode (TDM)**or **Share Mode**, depending on Mac hardware.

Native macOS Advantage

Unlike many forensic tools originally built for Windows or Linux:

- **RECON ITR** is **natively developed on macOS**, using **Apple's own libraries** and **system frameworks**.
- This ensures:
    - **Immediate support** for new macOS versions and file systems (such as APFS and Local Snapshots).
    - **Accurate parsing** of proprietary Apple Extended Attributes and system metadata.
    - **Faster and more reliable performance** without relying on reverse engineering.

- Competing tools often depend on **third-party open-source libraries** or **reverse-engineered solutions**, which can lead to:
    - Missed artifacts
    - Inaccurate timestamp interpretations
    - Incomplete imaging results

RECON ITR's native development guarantees that **forensic integrity** and **macOS compatibility** are maintained at the highest level.

Licensing

- Every initial purchase of RECON ITR includes a **one-year standard license**.
- After expiration:
    - **Updates and new version downloads** will no longer be available without renewal.
- **License Renewal Policy**:
    - Licenses older than **three months past expiration** will require **full-price renewal**.
    - Renewals can be purchased for **up to three years** at a time for convenience.

---

2 Installation and Updating

RECON ITR is shipped pre-installed on an external SSD and is ready for immediate use upon receipt. After receiving the device—and after each update—it is strongly recommended to **verify the software** by testing it on **test devices and sample data** before using it in live casework.

2.1 Updating the software

RECON ITR receives frequent updates to equip examiners with the latest features, security improvements, and expanded macOS support.

- Updates can be applied at any time as long as the license is **active**.
- To view the latest available version, visit the official updates page: https://sumuri.com/updates/

2.1.1 Steps to update the software

> ***Important:***
> *Before updating, ensure the software license is active. The license expiration date can be checked within the live RECON ITR application.*

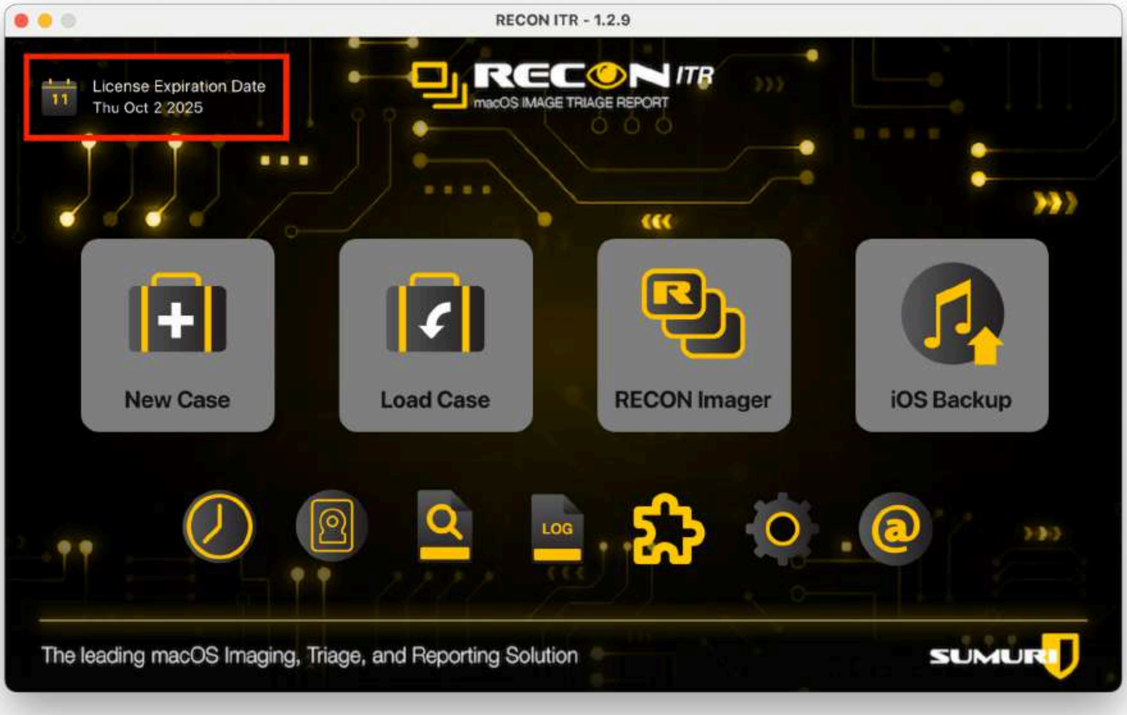
Update Process:

1. **Login** to the Mac with a user account that has **administrative privileges**.
2. **Connect** the RECON ITR SSD to the Mac.
3. **Backup any evidence** stored on the RECON ITR drive—**the drive will be erased** during the update process.
4. **Close the RECON ITR application** if it is running.
5. Visit https://sumuri.com/updates/ and download the latest **RECON ITR / Imager Updater**.
6. Once downloaded, **double-click the DMG** to mount it.
7. In the Finder window that appears, **launch** the **RECON Imager Updater.app**.
8. If prompted with "**This app was downloaded from the Internet. Are you sure you want to open it?**," click **Open**.
9. Ensure **Online Update** is selected in the **Update Type** dropdown.
10. Click **OK** to start the update process.
11. The updater will **download**, **verify**, and **hash** the latest update.
12. When prompted by **SUMURI Imager-Restore**, **enter your administrator credentials**. (This authorizes the application to write to the RECON ITR drive.)
13. After the update completes, a **"Process Succeeded"** message will appear.
14. Click **OK** to finish.

Your RECON ITR drive is now successfully updated and ready for use.

> ***Reminder:***
> *Always verify the updated software using **test devices and test data** before deploying it in live casework.*
>
> ***Offline Updates:***
> *If your agency requires offline updating, please contact us at software@sumuri.com for assistance.*

2.1.2 Finding the expiration date



RECON ITR - 1.2.9

License Expiration Date
Thu Oct 2 2025

RECON ITR
macOS IMAGE TRIAGE REPORT
New Case
Load Case
RECON Imager
iOS Backup
LOG
The leading macOS Imaging, Triage, and Reporting Solution
SUMURI

To find your RECON ITR license expiration date:

1. Connect the RECON ITR SSD to your Mac.
2. Locate the **LIVE partition** (visible on the Desktop or via Finder).
3. Launch the **RECON_ITR.app** from the LIVE partition.
4. If prompted, **enter the Admin password** and click **OK**.
5. The **License Expiration Date** will be displayed in the top left corner of the home screen.
6. For additional details (such as **Days Remaining**), click the **About RECON** button.

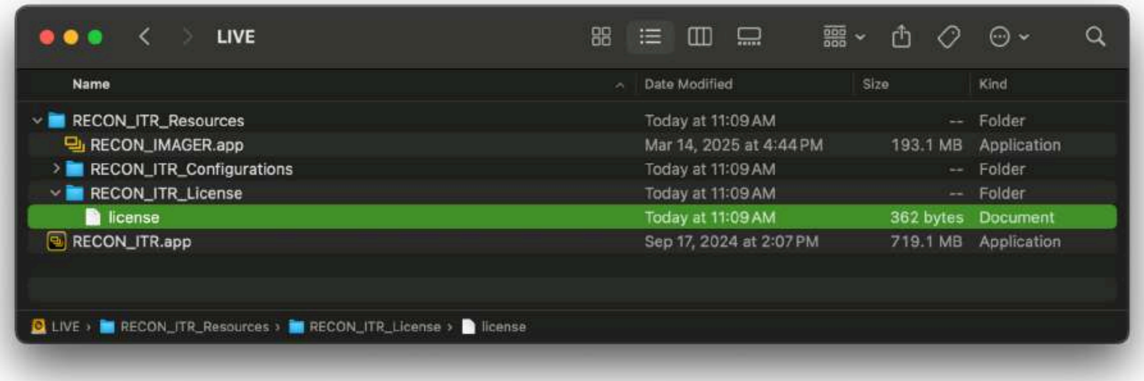
2.1.3 License renewal

- Reminder emails are sent to the registered email address **one week before** and **one week after** license expiration.
- To renew your license:
  - Email sales@sumuri.com.
  - Include the **serial number** of the RECON ITR drive you wish to renew.
- A member of the SUMURI Software team will guide you through the renewal process.

> ***Important:***
> *Licenses must be renewed* ***within three months*** *of expiration to qualify for discounted*

renewal pricing.
*Licenses older than three months past expiration must be renewed at **full price**.*

2.1.4 Updating the license



LIVE

Name	Date Modified	Size	Kind
RECON_ITR_Resources	Today at 11:09 AM	--	Folder
RECON_IMAGER.app	Mar 14, 2025 at 4:44 PM	193.1 MB	Application
RECON_ITR_Configurations	Today at 11:09 AM	--	Folder
RECON_ITR_License	Today at 11:09 AM	--	Folder
license	Today at 11:09 AM	362 bytes	Document
RECON_ITR.app	Sep 17, 2024 at 2:07 PM	719.1 MB	Application

LIVE › RECON_ITR_Resources › RECON_ITR_License › license

After your license renewal is processed:

1. You will receive a **zipped license file** by email from the SUMURI Software team.
2. Connect the RECON ITR SSD to your Mac.
3. **Download and unzip** the license file.
4. **Copy** the file named **license**.
5. Paste the license file into the appropriate locations depending on your RECON ITR version:

Version	Location to Paste License File
All Bootable Imager Modes(High Sierra, Catalina, Sonoma)	Paste into the **root** of each bootable volume. Select **Replace** if prompted.
LIVE Partition (v1.3.0 and earlier)	Paste into the **root** of the LIVE partition. Select **Replace** if prompted.
LIVE Partition (v1.3.0 and later)	Paste into the **RECON_ITR_LICENSE** folder located inside the **RECON_ITR_Resources** folder at the root of the LIVE partition. Select **Replace** if prompted.

Once the new license file is in place, your RECON ITR system will be active and ready for updates.

3 Supported Hardware and macOS

3.1 Triage / Live Imaging

Triage and **live imaging** are performed using the **live RECON ITR application** located on the **LIVE** partition of the RECON ITR SSD.

- The live application is designed for use when the target Mac is **powered on and logged into** a user account.
- **Minimum supported macOS version:**
  ➔ macOS 12 Monterey
- **Currently supported up to:**
  ➔ macOS 15 Sequoia (latest)

Important:

- Full Disk Access must be granted to RECON ITR in order to collect live data effectively.
- Secure Enclave devices (T2 and Apple Silicon Macs) cannot be physically imaged but a block copy of the APFS container or a logical file copy of the APFS data volume can be acquired.

3.2 Boot Imaging

Boot imaging is performed using the **RECON IMAGER application** built into the bootable modes of RECON ITR.

- **RECON IMAGER** is launched when booting the Mac into one of the **bootable imagers**.
- Supported hardware includes:
  - All **Intel-based Macs** (pre-T2 and T2)
  - All **Apple Silicon Macs** (M1, M2, M3, M4 series)

There are currently **three Bootable Imager Modes** available:

Bootable Mode	Primary Use
HIGH SIERRA	Older Intel Macs (pre-T2)
CATALINA	Newer Intel Macs (including T2)

SONOMA	All Apple Silicon Macs and latest Intel Macs

3.2.1 HIGH SIERRA - Bootable Imager

- MacBook (Early 2015) (*)
- MacBook (Late 2008 Aluminum, or Early 2009 or newer) (*)
- MacBook Pro (Mid/Late 2007 or newer) (*)
- MacBook Air (Late 2008 or newer) (*)
- Mac mini (Early 2009 or newer) (*)
- iMac (Mid 2007 or newer) (*)
- Mac Pro (Early 2008 or newer) (*)
- Xserve (Early 2009) (*)
- MacBook (Late 2009 or newer)
- MacBook Pro (Mid 2010 or newer)
- MacBook Air (Late 2010 or newer)
- Mac mini (Mid 2010 or newer)
- iMac (Late 2009 or newer)
- Mac Pro (Mid 2010 or newer)

Note (*): Support for these devices is dependent on the version of macOS installed on the device. Older versions of macOS may require the user to fall back onto other general imaging tools such as **PALADIN**.

3.2.2 CATALINA - Bootable Imager

- MacBook (Early 2015 or newer)
- MacBook Air (Mid 2012 or newer)
- MacBook Pro (Mid 2012 or newer)
- Mac mini (Late 2012 or newer)
- iMac (Late 2012 or newer)
- iMac Pro (2017)
- Mac Pro (Late 2013; Mid 2010 and Mid 2012 models with recommended Metal-capable graphics cards)

3.2.3 SONOMA - Bootable Imager

- MacBook Air (2018 or newer)
- MacBook Pro (2018 or newer)
- Mac mini (2018 or newer)
- iMac (2019 or newer)
- iMac Pro (2017)
- Mac Pro (2019)
- Apple Silicon MacBook Air (2021 or newer)
- Apple Silicon MacBook Pro (2021 or newer)

- Apple Silicon Mac Mini (2021 or newer)
- Apple Silicon iMac (2021 or newer)

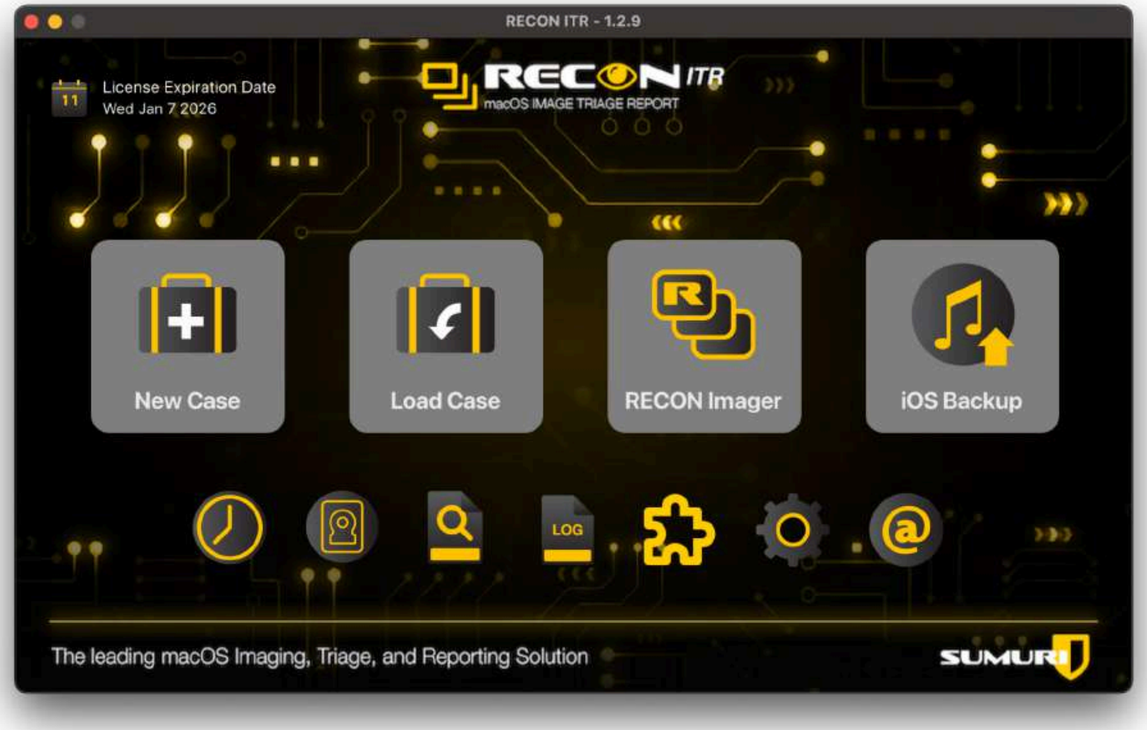
Note:
Support for some older devices (*) depends on the version of macOS installed.
*If the device is too old or incompatible, alternative imaging methods like **PALADIN** may be required.*

4 RECON ITR Main Menu Options

When **RECON ITR** is launched in the **live environment**, the **Main Menu** (splash screen) appears. From here, the examiner can:

- Start a new **macOS triage case**.
- Launch the **RECON IMAGER** to perform live imaging.
- Access additional triage tools and utilities.

The **RECON ITR application** is located on the **LIVE** volume of the RECON ITR SSD.



4.1 New Case

- The **New Case** button allows the examiner to initiate a new live triage session on the current device.
- Triage focuses on parsing and extracting artifacts rather than creating a full forensic image.
- Ideal for **rapid assessment**, especially in **on-scene** situations where speed is critical.

4.2 Load Case

- The **Load Case** button enables loading of **previously completed triage cases**.
- Useful for reviewing, continuing analysis, or generating additional reports from previously gathered triage data.

4.3 RECON Imager

- **RECON IMAGER** is the **forensic imaging tool** built into **RECON ITR**.
- It enables:
    - **Complete disk imaging** (where possible).
    - **Logical imaging** of selected volumes or files.
- This is the same imaging engine used in the bootable imagers.
- The **RECON IMAGER** button launches the imaging interface from the live environment.

4.4 iOS Backup

- The **iOS Backup** tool locates and extracts **local iOS device backups** stored on the Mac.
- Examiners can **export** the backups or **triage** them using RECON ITR's triage capabilities.
- Provides a fast and effective method for analyzing iOS backup data without the device being present.

4.5 File Timeline

- The **File Timeline** tool displays a **chronological view of file activity** on the system.
- It analyzes both:
    - **Apple Extended Metadata** timestamps (e.g., Content Creation, Last Used).
    - **POSIX timestamps** (traditional Unix time attributes).
- Helps reconstruct **user and system activity** based on file interactions.

4.6 Disk Manager

- **Disk Manager** provides an **overview of all disks and partitions** currently connected to the Mac.
- It allows examiners to:
    - **Manually manage disk mounting**.

    - **Control read/write settings**.
    - **Decrypt APFS encrypted volumes** (with password or recovery key).
- Ensures **precise control** over how evidence volumes are accessed and handled.

4.7 File Search

- **File Search** enables **targeted searches** across specific directories based on:
    - **File signatures**
    - **File names**
    - **Keywords**
- Supports creating **search templates** for repetitive use across multiple cases.
- Search results can be **reviewed**, **bookmarked**, and **reported** directly from within RECON ITR.

4.8 Log Collect

- **Log Collect** provides two methods for acquiring **Apple Unified Logs**:
    - **Without administrator password:** Collected as text files.
    - **With administrator password:** Collected as native **.logarchive** files.
- Unified logs can reveal detailed historical information about system and user activity.

4.9 Plugins Viewer

- The **Plugins Viewer** lists all **forensic plugins** available within RECON ITR.
- Plugins are divided into:
    - **General Plugins:** Default plugins included with every RECON ITR installation.
    - **Specialized Plugins:** Custom plugins created for specific agency needs (available by request).
- This section also displays basic **license information**.

4.10 RECON Configuration

- The **RECON Configuration** section allows examiners to set:
    - **Examiner details** (name, phone, email).
    - **Agency information** (agency name, address).
    - **Custom logos** (optional, PNG format).
    - **Preferred date formats** for reports.
- These settings auto-populate during triage and report generation for professional, standardized outputs.

4.11 About RECON

- The **About RECON** section provides important software information including:
    - **License expiration date** and **days remaining**.
    - **Purchase date** and **USB serial number**.

    - Access to the **End User License Agreement (EULA)**.
    - **Change Logs** highlighting recent updates and improvements.
    - A list of known **Exceptions/Known Issues**.
    - Links to **Support Resources** and manuals.

---

5 Supported Plugins

RECON ITR includes **over 150 built-in forensic plugins**.
These plugins may be accessed through:

- **Triage Cases** (New Case)
- **Logical Imaging** (Logical Imager inside RECON Imager)

When selected, RECON ITR will:

- Attempt to **extract artifacts** related to the chosen plugin.
- **Parse** and **generate reports** for the artifacts.

> ***Note:***
> *Some plugins are **volatile** and can **only be executed live** on a running system.*
> *These will not be available when using the Logical Imager.*

The **macOS version** on the target device may impact:

- Which artifacts are detected.
- How much data is available for extraction.

New macOS updates or application changes may alter or deprecate plugin behavior.

5.1 Plugin List

Network & System Artifacts:
Active Networks, Airport Wireless Network, Bluetooth, Bluetooth Logs, Bluetooth Logs Legacy, Connected iOS Devices, Device Information, Disk Utility, Disk Utility Saved List, Installed Hardware, IP Addresses, Logged Users, Login Startup Items, Media Mounted, Mounted Volumes, Network Information, Network Interfaces, Network Logs, Network Mapped, Network Preferences, Quarantine Events, Scheduled Tasks, System Information, System Integrity Protection Status, System Profile, USB Attached Legacy, USB Logs, Wake Reason, Wake Reason Logs

Browser & Internet Artifacts:
Brave Browser, Chromium, Cyberduck, Mozilla Firefox, Google Chrome, Google Drive, Internet Explorer, Opera, Opera Mini, Safari, TorBrowser, UC Browser, Vuze, WireShare, YouTube

Communication & Messaging Artifacts:
Adium, Apple FaceTime, Apple Mail, Apple Mail Extractor, Call History, FaceTime, iCloud, iCloud Logs, Messages, LinkedIn, Nimbuzz, Notifications, Skype, TeamViewer, TextMe, Viber, Voice Mail, Voice Memos, WhatsApp

Cloud Storage & Backup Artifacts:
Dropbox, Free Download Manager, Gigatribe, iOS Backup, Mobile Backups, OneDrive

Virtualization Artifacts:
Parallels, VMWare Fusion, VirtualBox, Virtual Machine Files

Media & Multimedia Artifacts:
Audio, Audio-Video, Camera, Geotags, Images, Music, Photo Booth, Photos, Podcasts, TV, Video, VLC, Weather, YouTube

User Activity & Behavioral Artifacts:
App Compatibility Cache, Application Services, Bash History, Clipboard, Daily Out, Escalate Privileges, Finder, Finder Sidebar, Jump List, Launchpad, Login Banner, Logon Banner, Recent Items, Running Processes, SSH, Spotlight Settings, Startups, Typed Words, Uptime, Window Media Player, Zsh History

File Management Artifacts:
Black Hole, Data Destruction, Deleted Users, Document Files,Exe Files, File Zilla, HFS+ Device Logs, Log Files, Prefetch, Thumb Cache, Trash / Recycle Bin

Security & Encryption Artifacts:
FileVault Status, Keychain

Application & Software Artifacts:
Apple Installed Applications, Maps, Software Updates, Windows Installed Applications, Apple Calendar, Apple Dock, Apple Parallels, Apple Unified USB Logs, Calendar, CleanMyMac 2, Cortana, Daily Out, Dolphin, eMule, Frostwire, Line, Mercury, Outlook 2011, Outlook 2016, Reminders, Remote Desktop, Scheduled Tasks, Stock

File Sharing & Torrent Artifacts:
aMule, BitTorrent, BitTorrent Web, Torrent Files, uTorrent, uTorrentWeb

Miscellaneous Artifacts:
WhereFrom, Printer and Scanner, Screen Time, Screenshot

6 RECON Imager

RECON IMAGER is the built-in imaging application available in two ways:

- From the bootable imager

- From within the RECON ITR application by clicking the **RECON IMAGER** button.

RECON IMAGER allows you to create forensic images of:

- APFS volumes
- Synthesized APFS containers
- Physical drives (Accessible from boot environment only if targeting an internal drive)

Before using RECON IMAGER, it is important to carefully review this manual and the appendices. Additionally, after each installation or update, we strongly recommend verifying functionality by imaging sample data.

Important Hardware Note:
The available imaging options depend on the Mac's hardware.

- Physical imaging is **not possible** on devices with a Secure Enclave (T2 and Apple Silicon M-series chips).
- Physical imaging **is possible** from boot on pre-T2 Intel Macs.

Accessing RECON IMAGER (Live Environment)

To launch RECON IMAGER while the Mac is running normally:

1. Open the **RECON ITR** application.
2. Click the **RECON IMAGER** button on the home screen.

Authentication Levels:

- If RECON ITR was launched **with the administrative password**, you will have full access to Disk Imaging.
- If RECON ITR was launched **without the administrative password**, you can only acquire a logical image of the user's home directory.

Important:
If imaging in a live environment and you have the administrative password, ensure that **Full Disk Access** has been granted to RECON ITR. See the Full Disk Access section in the appendix for detailed instructions.

Accessing RECON IMAGER (Boot Environment)

For Pre-T2 Intel macs, RECON IMAGER must be used in the bootable environment to acquire a physical image of the internal disks.

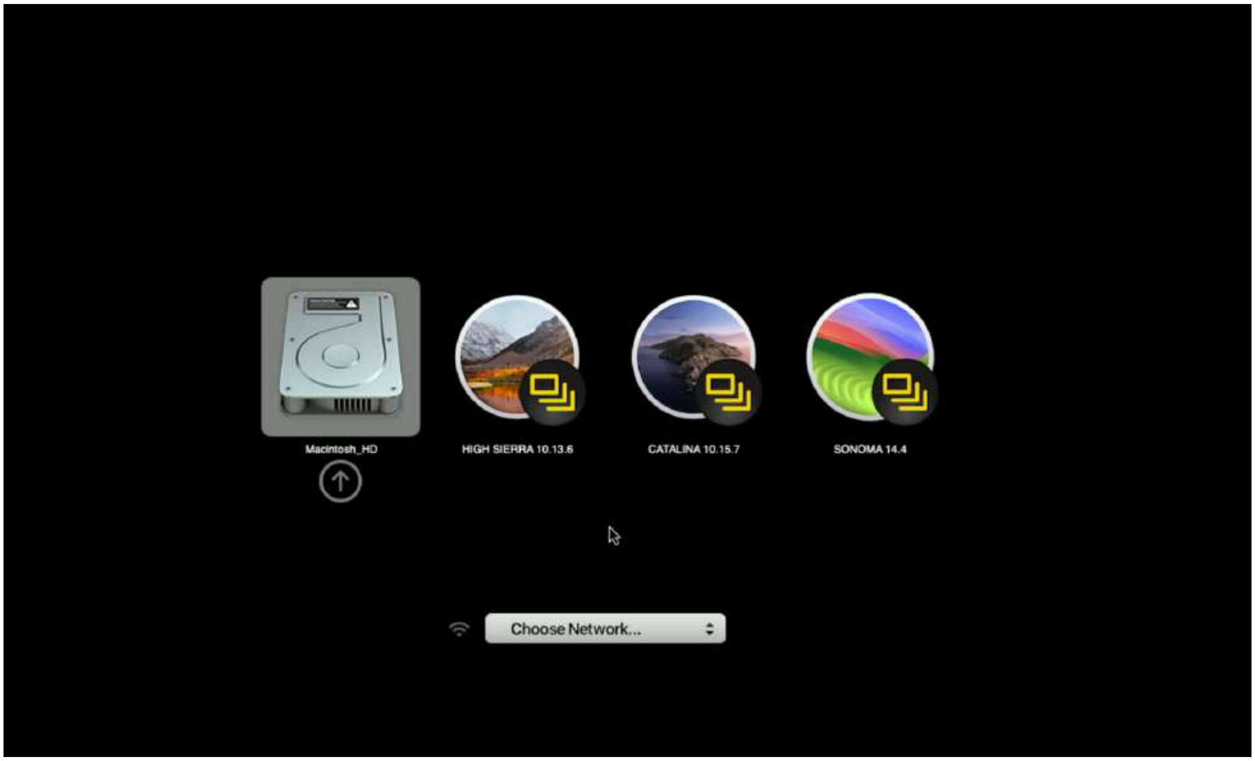
To launch RECON IMAGER from a bootable environment:

1. Start the Mac in Startup Disk Mode.
2. Select the bootable RECON imager as the startup disk.
3. After booting, open RECON IMAGER.

Imaging Capabilities:

- Physical imaging of internal drives: Only possible from the boot environment.
- Physical imaging of external drives: Possible both live and from boot.
- Imaging of APFS Data Volumes and Synthesized APFS Containers: Possible both live and from boot.

6.1 Startup Disk Mode - (Boot Only)



To use a bootable RECON Imager, the Mac must first be started in **Startup Disk Mode**.
Startup Disk Mode allows you to select an external volume, such as a RECON Imager, to boot from. Once in Startup Disk Mode, you can choose and boot into one of the available RECON Imagers. The key combination required to enter Startup Disk Mode depends on the Mac's hardware:

- **Apple Silicon (M-series)** Macs:
  - Press and **hold the Power button** until you see **"Loading startup options..."** on the screen.

- **Intel-based** Macs:
  - Press the **Power button**, then immediately **hold down the Option key** while the Mac starts up.

After selecting the RECON Imager volume, the Mac will boot into the RECON imaging environment.

6.1.1 Choosing a bootable imager

When the Mac is booted into **Startup Options**, you will see a list of available recovery modes along with the RECON Bootable Imagers that the device can use.

The RECON Bootable Imagers that appear will depend on:

- The **model** of the Mac
- The **macOS version** installed on the device

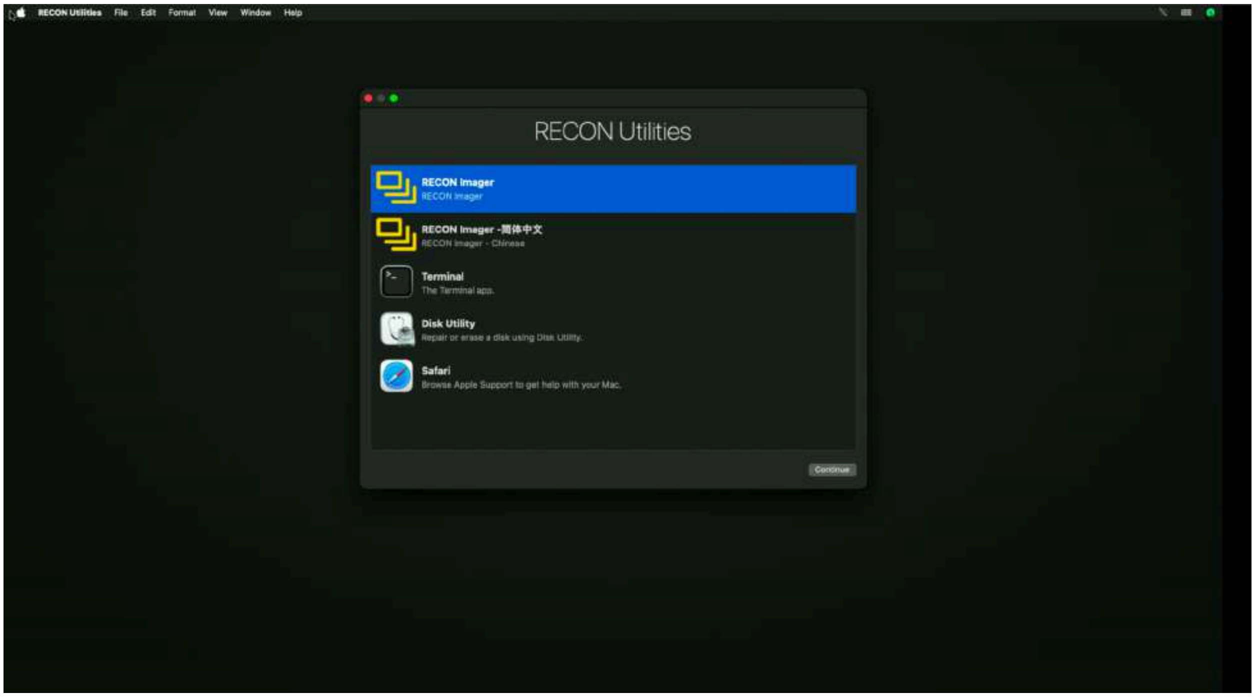
How to Choose the Correct Bootable Imager:

- Apple Silicon Macs (M1, M2, M3, M4, etc.)**:**
  - Always select the SONOMA Bootable Imager.
- Intel Macs**:**
  - If the Mac is running macOS 14 (Sonoma) or newer, select the SONOMA Bootable Imager.
  - If the Mac is running an older version of macOS (macOS 13 Ventura, macOS 12 Monterey, macOS 11 Big Sur, etc.), select the HIGH SIERRA or CATALINA Bootable Imager, whichever is closest to the source macOS version.

Example:

- macOS 12 Monterey (Intel Mac) ➔ Use **CATALINA Bootable Imager**.
- macOS 14 Sonoma (Intel Mac or Apple Silicon) ➔ Use **SONOMA Bootable Imager**.

6.2 RECON Utilities - (Boot Only)



RECON Utilities

RECON Imager
RECON Imager

RECON Imager -简体中文
RECON Imager - Chinese

Terminal
The Terminal app.

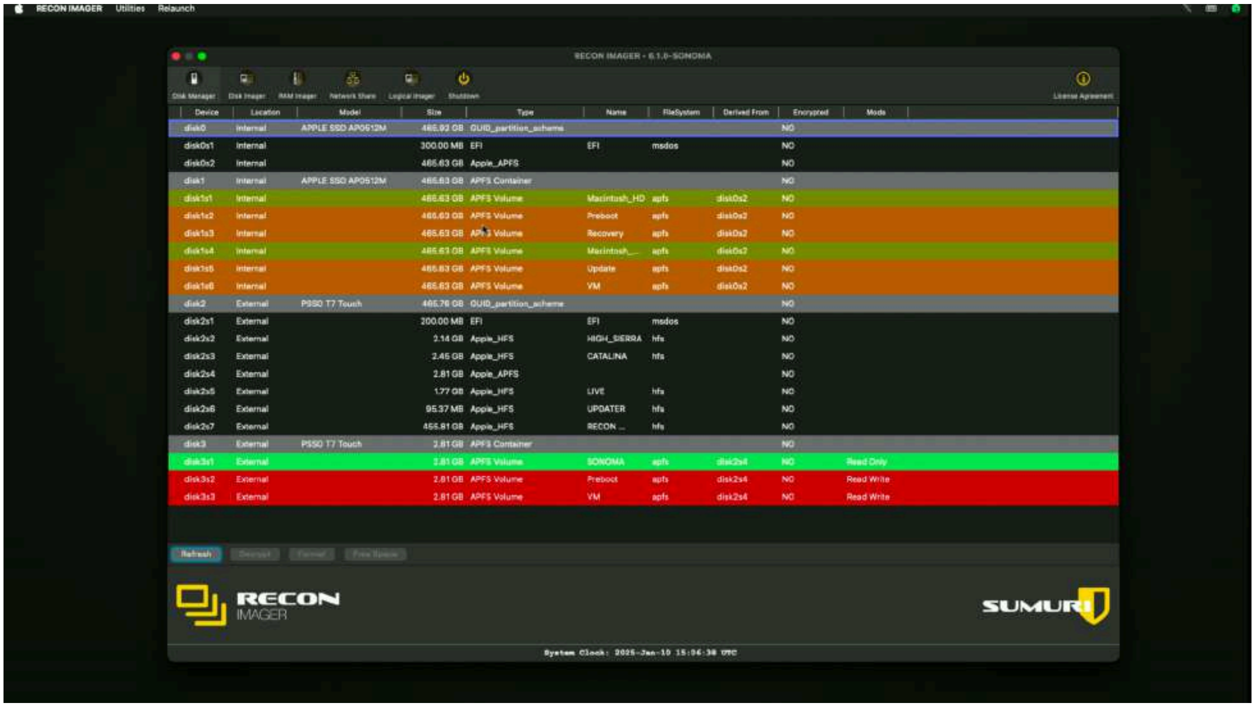
Disk Utility
Repair or erase a disk using Disk Utility.

Safari
Browse Apple Support to get help with your Mac.

After selecting a Bootable Imager, you may be presented with the **RECON Utilities** screen.
This screen displays a list of applications available on the bootable imager. Below are the applications currently included:

- **RECON Imager**
  Launches the RECON Imager application, which allows you to capture images of the booted device.
  - Supports both **physical disk imaging** and **logical user data imaging**.
- **RECON Imager – Chinese**
  Identical to the standard RECON Imager, but with a **Chinese-localized interface**.
- **Terminal**
  Launches Apple's native **Terminal** application.
  - Allows you to execute command-line operations **with root privileges**.
- **Disk Utility**
  Opens Apple's native **Disk Utility** application.
  - Used for viewing, managing, and configuring disks detected on the system.
- **Safari**
  Launches Apple's native **Safari** web browser.
  - Useful for accessing online resources if network access is available.

6.3 Disk Manager - (Boot Only)



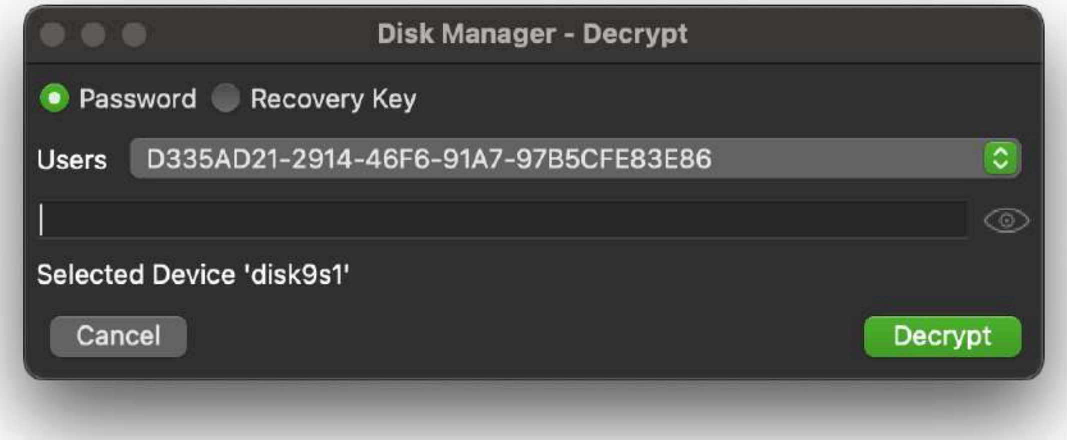
RECON IMAGER - 6.1.0-SONOMA

Device	Location	Model	Size	Type	Name	FileSystem	Derived From	Encrypted	Mode
disk0	Internal	APPLE SSD AP0512M	465.92 GB	GUID_partition_scheme				NO	
disk0s1	Internal		300.00 MB	EFI	EFI	msdos		NO	
disk0s2	Internal		465.63 GB	Apple_APFS				NO	
disk1	Internal	APPLE SSD AP0512M	465.63 GB	APFS Container				NO	
disk1s1	Internal		465.63 GB	APFS Volume	Macintosh_HD	apfs	disk0s2	NO	
disk1s2	Internal		465.63 GB	APFS Volume	Preboot	apfs	disk0s2	NO	
disk1s3	Internal		465.63 GB	APFS Volume	Recovery	apfs	disk0s2	NO	
disk1s4	Internal		465.63 GB	APFS Volume	Macintosh_...	apfs	disk0s2	NO	
disk1s5	Internal		465.63 GB	APFS Volume	Update	apfs	disk0s2	NO	
disk1s6	Internal		465.63 GB	APFS Volume	VM	apfs	disk0s2	NO	
disk2	External	PSSD T7 Touch	465.76 GB	GUID_partition_scheme				NO	
disk2s1	External		200.00 MB	EFI	EFI	msdos		NO	
disk2s2	External		2.14 GB	Apple_HFS	HIGH_SIERRA	hfs		NO	
disk2s3	External		2.45 GB	Apple_HFS	CATALINA	hfs		NO	
disk2s4	External		2.81 GB	Apple_APFS				NO	
disk2s5	External		1.77 GB	Apple_HFS	LIVE	hfs		NO	
disk2s6	External		95.37 MB	Apple_HFS	UPDATER	hfs		NO	
disk2s7	External		455.81 GB	Apple_HFS	RECON ...	hfs		NO	
disk3	External	PSSD T7 Touch	2.81 GB	APFS Container				NO	
disk3s1	External		2.81 GB	APFS Volume	SONOMA	apfs	disk2s4	NO	Read Only
disk3s2	External		2.81 GB	APFS Volume	Preboot	apfs	disk2s4	NO	Read Write
disk3s3	External		2.81 GB	APFS Volume	VM	apfs	disk2s4	NO	Read Write

System Clock: 2025-Jan-10 15:06:38 UTC

The **Disk Manager** in the bootable RECON Imager environment allows you to manage the disks currently detected by the system. Several options are available for managing disks:

- **Refresh**
  - Updates the information displayed in the Disk Manager table.
- **Decrypt**
  - Unlocks encrypted APFS volumes using either:
    - The administrator password, or
    - The FileVault Recovery Key.



Disk Manager - Decrypt

● Password ○ Recovery Key

Users D335AD21-2914-46F6-91A7-97B5CFE83E86

Selected Device 'disk9s1'

Format

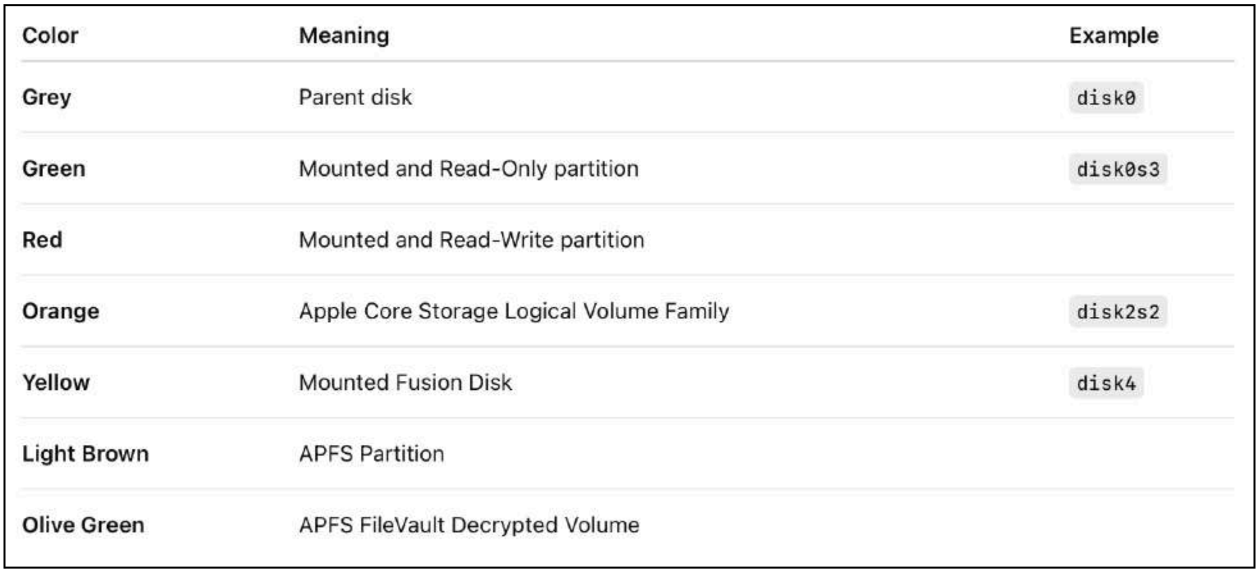
- Formats a drive to either:
  - **APFS** (Apple File System).
  - **HFS+** (macOS Extended).
- Commonly used to prepare a collection drive for imaging.

Free Space

- Displays the amount of free space available on a selected partition.

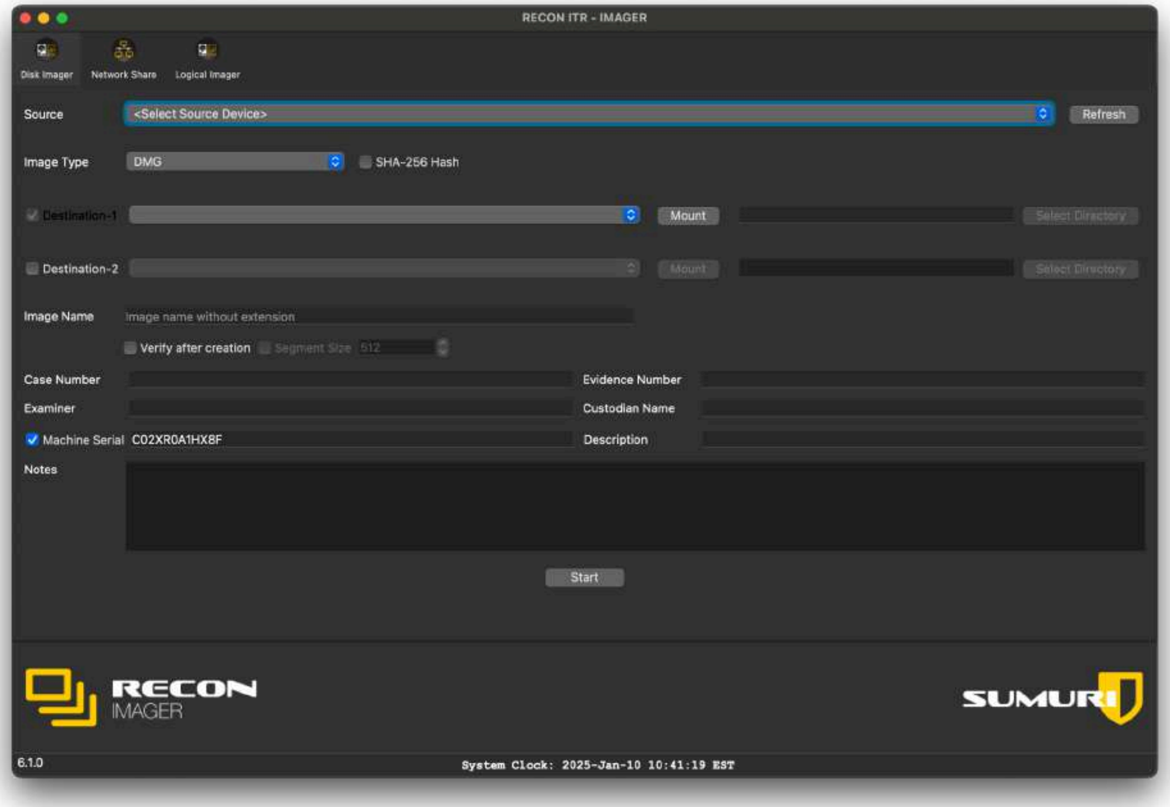
6.3.1 Disk Manager Color Coding

The Disk Manager uses a **color-coded system** to help you quickly identify disk types and statuses:



Color	Meaning	Example
Grey	Parent disk	`disk0`
Green	Mounted and Read-Only partition	`disk0s3`
Red	Mounted and Read-Write partition	
Orange	Apple Core Storage Logical Volume Family	`disk2s2`
Yellow	Mounted Fusion Disk	`disk4`
Light Brown	APFS Partition	
Olive Green	APFS FileVault Decrypted Volume	

6.4 Disk Imager



Source: <Select Source Device>

Image Type: DMG ☐ SHA-256 Hash

☑ Destination-1

☐ Destination-2

Image Name: Image name without extension

☐ Verify after creation ☐ Segment Size 512

Case Number:

Evidence Number:

Examiner:

Custodian Name:

☑ Machine Serial: C02XR0A1HX8F

Description:

Notes:

System Clock: 2025-Jan-10 10:41:19 EST

The **Disk Imager** tab allows you to create forensic images of both **internal** and **external** disks. The ability to acquire a physical image is dependent on the devices hardware:

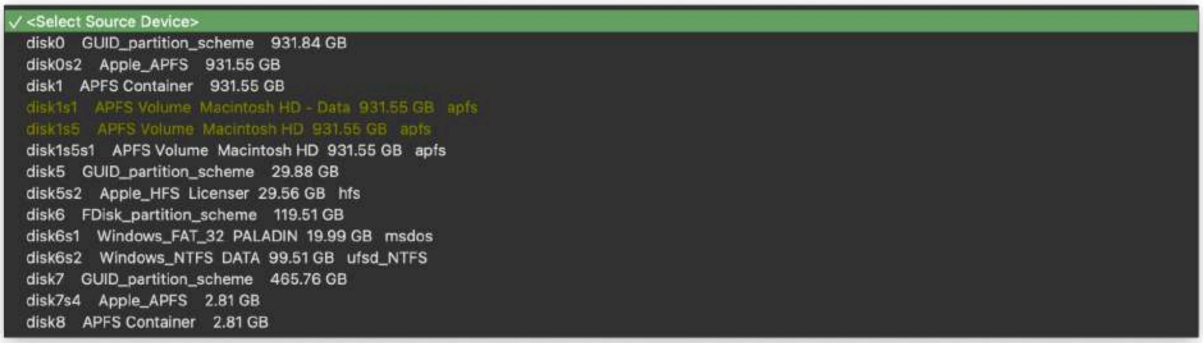
- **Pre-T2 Intel Macs**: Full physical imaging is possible.
- **T2 and Apple Silicon Macs**: Only a block copy of the APFS container or a logical copy of the APFS data volume is supported.

You can access the Disk Imager in two environments:

- **Bootable Imagers** (during boot)
- **Live Environment** (while the Mac is running normally)

Important:
In the **Live Environment**, the Disk Imager will only be available if the **RECON ITR application** was launched **with administrative credentials** (admin password). Without admin credentials, you will not have access to the Disk Imager tab.

6.4.1 Supported Disk Sources



```
✓ <Select Source Device>
  disk0   GUID_partition_scheme   931.84 GB
  disk0s2   Apple_APFS   931.55 GB
  disk1   APFS Container   931.55 GB
  disk1s1   APFS Volume  Macintosh HD - Data  931.55 GB   apfs
  disk1s5   APFS Volume  Macintosh HD  931.55 GB   apfs
  disk1s5s1   APFS Volume  Macintosh HD  931.55 GB   apfs
  disk5   GUID_partition_scheme   29.88 GB
  disk5s2   Apple_HFS  Licenser  29.56 GB   hfs
  disk6   FDisk_partition_scheme   119.51 GB
  disk6s1   Windows_FAT_32  PALADIN  19.99 GB   msdos
  disk6s2   Windows_NTFS  DATA  99.51 GB   ufsd_NTFS
  disk7   GUID_partition_scheme   465.76 GB
  disk7s4   Apple_APFS   2.81 GB
  disk8   APFS Container   2.81 GB
```

The **Source** dropdown menu displays a list of internal and external disks currently connected to the system. To refresh the list of available sources:

- Click the **Refresh** button.
- The disk list will update based on devices currently detected.

Important:
*Disk identifiers (such as `disk0`, `disk1`, etc.) are **not static** and may vary between devices and boot sessions.*

Choosing a Source

The selected source affects:

- The **available image types** (DMG, Logical Folder, E01, Ex01, etc, etc)
- The **available hashing options**

Reminder:
*These are **recommendations only**. Always consult your **agency's guidelines and policies** before choosing a source and an output format.*

Metadata Preservation

When imaging from an **APFS volume**, some file timestamps and metadata may not exactly match the original disk due to the logical acquisition process.
To help preserve evidence integrity:

- RECON IMAGER automatically creates a **CSV** and **SQL database** containing:
    - The **original POSIX timestamps**

  - The **Inode references** of all copied files

⚠️ Critical Warning

Be familiar with imaging **Apple file systems** before proceeding.
Choosing the wrong source or output format may result in an **unusable or incomplete image**.

- Thoroughly review this manual.
- Always follow your agency's approved procedures.

Supported Source Options by Mac Type

Apple Silicon Macs (M1, M2, M3, M4, etc.)

Physical imaging is not possible on Apple Silicon devices. Preferred targets (in order):

1. Synthesized APFS Container (commonly `disk3`)
2. APFS Data Volume (commonly `disk3s5` — *"Macintosh HD - Data"*)

T2 Intel Macs

Physical imaging is not possible on T2-protected devices. Preferred targets (in order):

1. Synthesized APFS Container (commonly `disk1`)
2. APFS Data Volume (commonly `disk1s1` — *"Macintosh HD - Data"*)

Intel Macs (Non-Fusion / Non-T2)

Preferred targets (in order):

1. Physical internal drive (commonly `disk0`)
2. Synthesized APFS Container (commonly `disk1`)
3. APFS Data Volume (commonly `disk1s1` — *"Macintosh HD - Data"*)

Intel Macs (Fusion Drive Systems)

Preferred targets (in order):

1. Synthesized APFS Container (commonly `disk2`)
2. APFS Data Volume (commonly `disk2s1` — *"Macintosh HD - Data"*)
3. Physical internal drives (commonly `disk0` and `disk1`)

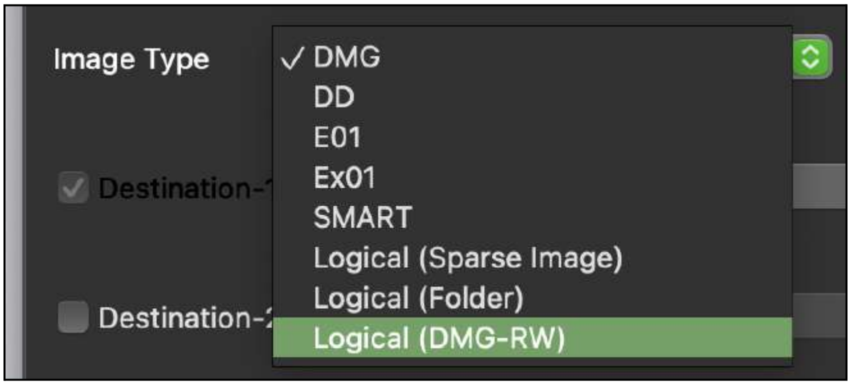
External Drives (any Mac)

Preferred targets (in order):

1. Physical external drive
2. Partition
3. Synthesized APFS Container
4. APFS Data Volume

6.4.2 Image Type Options

In the **Image Type** dropdown menu, you can select the format you want for your forensic image. The list of available formats will vary depending on the selected source.



Supported Image Types

Format	**Description**	**Notes**
DMG	Apple's proprietary fixed-size disk image format.	Widely used in Mac forensics. Mountable in macOS.
Logical (DMG-RW)	Used for logical acquisitions. Initializes a writable DMG before copying data.	Slower imaging times due to initialization.
FS Block Copy - DMG	Used for block-level copies, typically for APFS Containers.	Slower imaging due to initialization.
Raw Output DMG	A raw (bit-by-bit) copy output with a `.dmg` extension instead of `.dd`.	Only available when targeting physical drives.
SparseImage	Apple's dynamically-sized image format that grows/shrinks as needed.	Faster imaging than DMG. Limited Windows tool support.
Logical (SparseImage)	Logical acquisition stored in a SparseImage format.	Mountable on macOS.
FS Block Copy - SparseImage	Block copy of an APFS Container into a SparseImage format.	
E01/EX01	Standard forensic image formats widely supported by forensic tools.	Best for physical imaging on pre-2018 Intel Macs.
DD	Raw forensic image format (bit-by-bit copy).	Only available for physical drives/partitions. Not common for Macs with Secure Enclave.
SMART	Another forensic image format similar to DD.	Rarely used in Mac forensics today.
Logical Folder	Copies selected files or APFS volumes into a standard folder structure (directory).	Only available for logical acquisitions.

Additional Notes:

- **DMG Details:**
  - DMGs must be initialized with a fixed size before imaging begins.
  - Variations in how DMGs are listed (e.g., Logical DMG-RW, FS Block Copy - DMG) reflect **how they are created**, not the final file format.
- **SparseImage Details:**
  - Mountable natively in macOS.
  - Faster to initialize than DMGs.
  - Some **Windows-based forensic tools** may not support SparseImage files. Always verify compatibility with your analysis software.
- **Physical Imaging Limitations:**
  - Due to **Secure Enclave protections** (T2 and Apple Silicon), **physical imaging is no longer possible** on most modern Macs.
  - Formats like **E01**, **DD**, and **SMART** are primarily used only on **older Intel-based Macs** without Secure Enclave protection.

⚠️ Critical Reminders:

- Choose the image type based on your case requirements **and** your **agency's policies**.
- Improper format selection can lead to issues in analysis or evidence acceptance.
- Always verify the expected compatibility of the image with your forensic tools **before acquisition**.

Quick Visual Summary:

Source Type	**Recommended Image Format**
Logical APFS Volume	Logical (DMG-RW) or Logical (SparseImage)
Full APFS Container	FS Block Copy - DMG or FS Block Copy - SparseImage
Physical Disk (older Intel)	DMG (raw output), E01, DD, or SMART

6.4.3 Hashing Options and Source Options

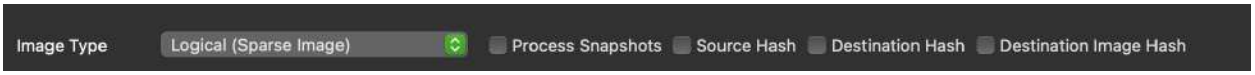


Image Type: Logical (Sparse Image)

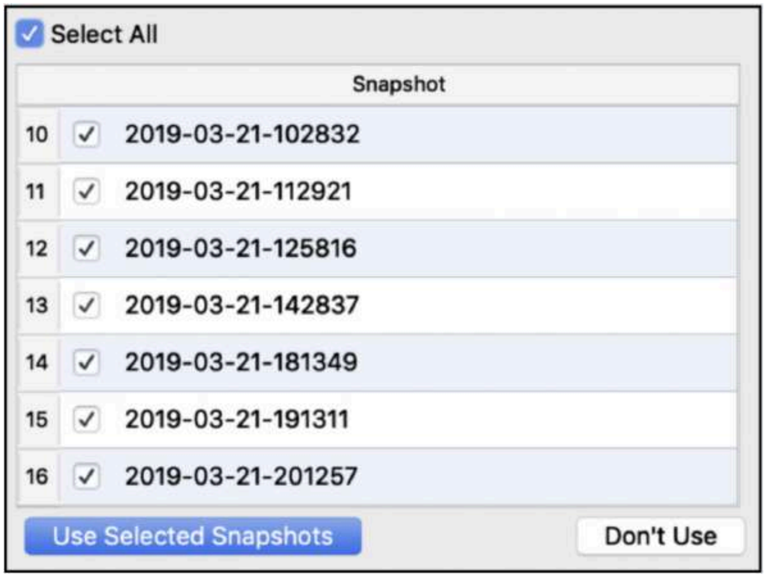
□ Process Snapshots □ Source Hash □ Destination Hash □ Destination Image Hash

Next to the **Image Type** dropdown, you can select various **Hashing Options** by clicking the corresponding checkboxes. The available hashing options depend on the source selected.

6.4.4 Hashing Options

- Destination Image Hash
    - Creates a hash of the final image file.
    - ✅ Available for DMG, SparseImage, E01/EX01, DD, and SMART formats.
    - ❌ Not available for Logical Folder outputs.
- Source Hash
    - Hashes individual files before they are copied into the destination image.
    - Results are saved in:
        1. A SQLite database in the case folder, and
        2. Plain-text CSV files.
    - ➡️ Only available when imaging from a volume source.
- Destination Hash
    - Hashes individual files after they are copied into the destination image.
    - Results are saved in:
        1. A SQLite database in the case folder, and
        2. Plain-text CSV files.
    - ➡️ Only available when imaging from a volume source.
- SHA-256 Hash
    - Enables SHA-256 hashing specifically for physical DD and DMG images.
    - ➡️ Selectable when imaging physical drives or partitions.

- Process Snapshots
  - Compares the live APFS Data volume to available local snapshots.
  - Identifies files that have been edited, modified, or deleted.
  - ➡️ Only available if:
    1. APFS Data volume is selected as the source.
    2. SparseImage is selected as the output format.
  - How to Use Snapshots:
    1. When prompted, a list of local snapshots will appear.
    2. Check the box next to the snapshots you want to analyze.
    3. Click Use Selected Snapshots.



		Snapshot
10	☑	2019-03-21-102832
11	☑	2019-03-21-112921
12	☑	2019-03-21-125816
13	☑	2019-03-21-142837
14	☑	2019-03-21-181349
15	☑	2019-03-21-191311
16	☑	2019-03-21-201257

⚡ Quick Notes:

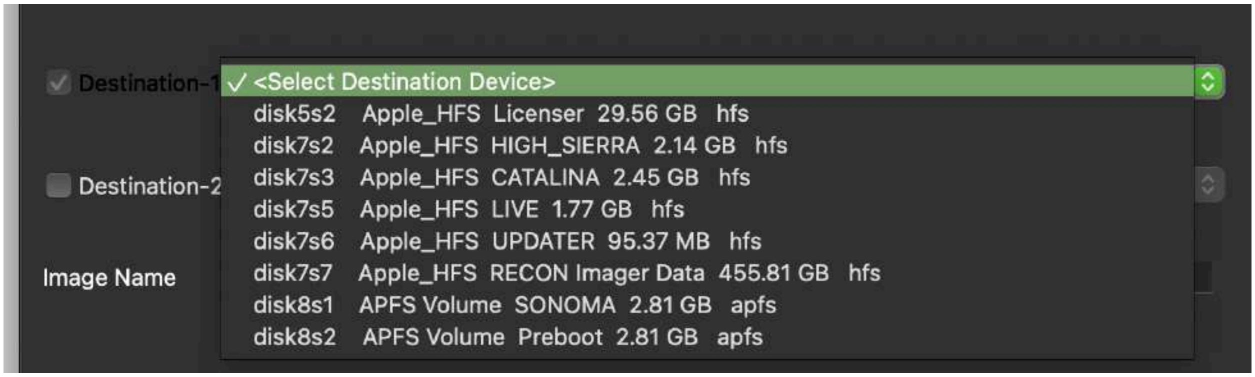
- Source Hash and Destination Hash are different:
  - Source = Before copying
  - Destination = After copying

If working with snapshots, only SparseImage format supports them.

Additional Imaging Options

- **Compression Level**
  (Available for **E01/EX01** and **SMART (.S01)** image formats)
  - **None**: No compression. Fastest imaging.
  - **Fast**: Minimal compression. Good balance between speed and size.
  - **Best**: Maximum compression. Slower imaging process.
- **Segment Size**
  - Allows supported image types to be split into segments.
  - ➡️ Only available for **E01/EX01** and **SMART (.S01)** formats.
  - ❌ Not available for DMG, SparseImage, Logical Folder, or Block Copy formats.
- **How to set Segment Size:**
  - Check the **Segment Size** box.
  - Enter the desired size (in MB).
- **Verify After Creation**
  - Performs a verification hash (MD5 and SHA-1) on the **output image** after acquisition.
  - A summary window will display the results at the end of imaging.
  - Full details are also saved in the logs inside the image output folder.

6.4.5 Destination Drive Formats



```
✓ <Select Destination Device>
disk5s2   Apple_HFS  Licenser  29.56 GB   hfs
disk7s2   Apple_HFS  HIGH_SIERRA  2.14 GB   hfs
disk7s3   Apple_HFS  CATALINA  2.45 GB   hfs
disk7s5   Apple_HFS  LIVE  1.77 GB   hfs
disk7s6   Apple_HFS  UPDATER  95.37 MB   hfs
disk7s7   Apple_HFS  RECON Imager Data  455.81 GB   hfs
disk8s1   APFS Volume  SONOMA  2.81 GB   apfs
disk8s2   APFS Volume  Preboot  2.81 GB   apfs
```

To select a destination drive for imaging:

1. Click the **Select Destination Device** dropdown next to **Destination-1**.
2. Choose the disk where you would like RECON Imager to save the forensic image.

The destination can be either:

- The **"**Imager Data**"** partition on the RECON ITR drive, or
- A separate external destination drive.

Recommended Destination Drive Size

- Choose a destination drive that is at least **25% larger** than the internal drive or source volume you are imaging.

Recommended File System Formats

When preparing your destination drive, we recommend formatting it with one of the following file systems:

- **HFS+ (macOS Extended Journaled)**
  - ✅ Fully supported and highly recommended.
  - ✅ Most stable across all macOS versions.
  - ✅ Widely accepted by forensic tools.
- **APFS (Apple File System)**
  - ✅ Supported.
  - ⚠️ Native to newer versions of macOS.
  - May require additional drivers for access on non-macOS systems.

Important:
ExFAT is NOT supported as a destination file system for writing forensic images. ExFAT lacks key features such as journaling and metadata preservation, making it unsuitable for forensic evidence handling.

If you need to transfer or access the forensic image on a Windows system later:

- First save the image to an **HFS+** or **APFS** drive.
- After acquisition, **manually transfer** the image to an **ExFAT** or **NTFS** drive if absolutely necessary for transport or access.

Better Alternative:
Install third-party drivers such as **Paragon Mac Toolkit** or other **macOS FUSE drivers** on the Windows system. These drivers allow Windows to **read HFS+ and APFS** drives natively, preserving forensic integrity without requiring file system conversion.

Mounting and Saving the Image

- You **do not need** to manually mount the destination drive before starting imaging.
- RECON ITR will **automatically mount** the selected destination during the imaging process.
- By default, RECON Imager saves images inside a new **case folder** at the root of the destination drive.

To change the default location:

1. Click **Mount**.
2. Click **Select Directory**.
3. Navigate to the desired folder where you want the image to be saved.

Writing to Multiple Destinations

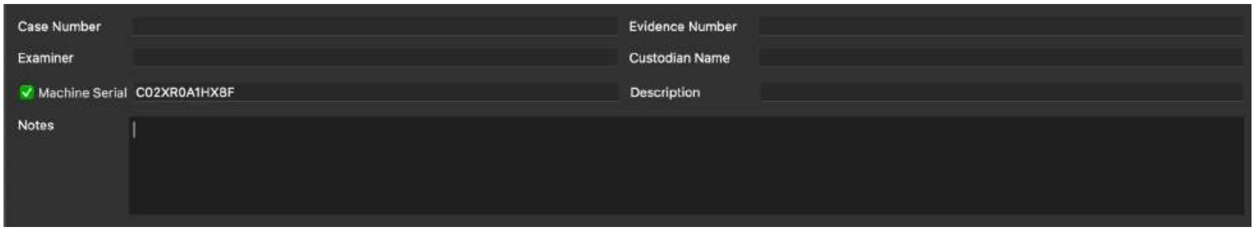
To simultaneously create two copies of the image:

1. Check the box next to **Destination-2**.
2. Select a second destination drive.
3. RECON Imager will write the image to both locations during acquisition.

⚡ Quick Tips:

- Always format your destination drive properly before beginning imaging.
- Confirm there is enough free space — the imaging process will fail if the destination fills up.
- Using two destinations helps meet evidence duplication requirements and strengthens your chain of custody.

6.4.6 Case Details



Case Number		Evidence Number	
Examiner		Custodian Name	
☑ Machine Serial	C02XR0A1HX8F	Description	
Notes			

At the bottom of the **Disk Imager** screen, you can enter **Case Details** for the acquisition. These details will be saved in a file called **Complete.txt**, which is automatically generated alongside your forensic image when imaging is complete.

The **Complete.txt** file records:

- The entered Case Details
- Imaging start and end times
- Imaging settings and summary details

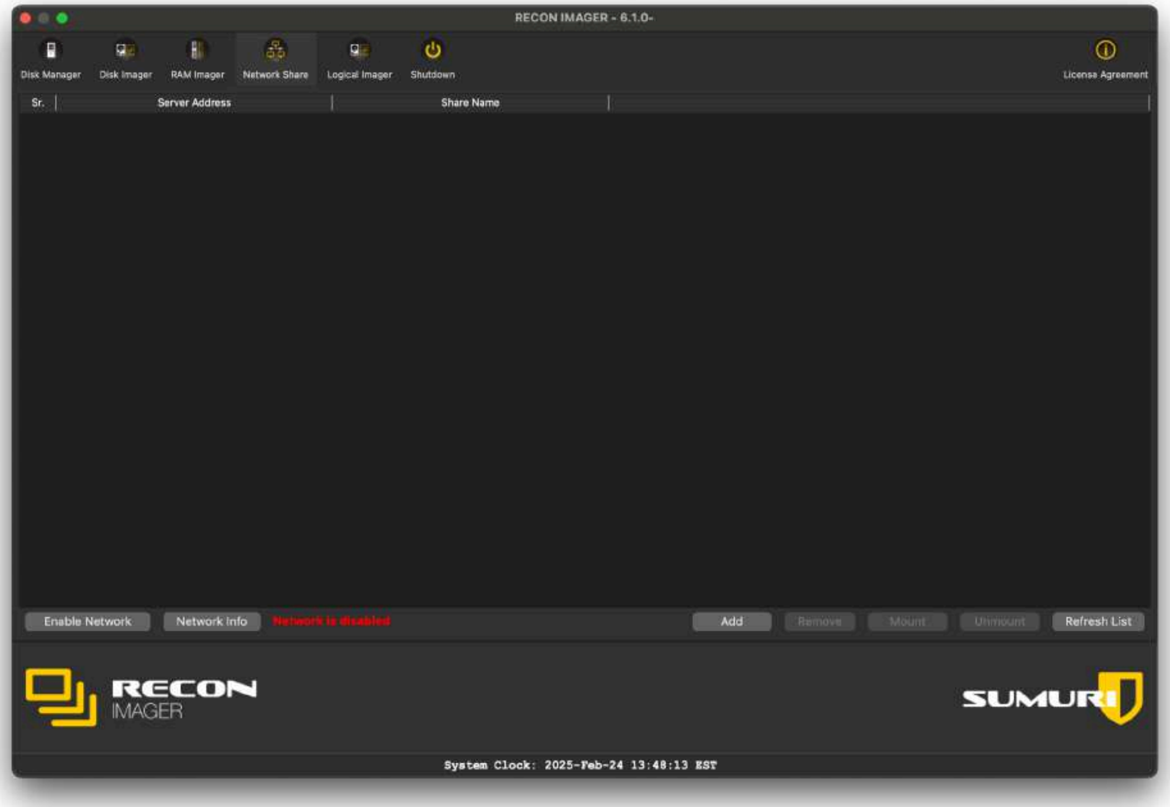
Available Case Detail Fields

Field	**Description**
Image Name *(Required)*	The name assigned to the output image file. **This field must be filled in** to proceed.
Case Number *(Optional)*	Enter the case number associated with the investigation, if applicable.
Examiner *(Optional)*	Enter the name of the examiner performing the acquisition.
Machine Serial*(Optional/Autofill)*	The Mac's serial number will automatically populate this field. ➔ You can **exclude** the serial number by unchecking the box next to "Machine Serial."
Evidence Number *(Optional)*	Enter an evidence tag or number if applicable.
Custodian Name *(Optional)*	Enter the name of the custodian or owner of the device.
Description *(Optional)*	Provide a brief description of the device being imaged (e.g., "MacBook Pro 14-inch, 2023").
Notes *(Optional)*	Add any additional notes relevant to the acquisition or case context.

⚡ Quick Tips:

- **Always complete at least the Image Name** field to ensure proper identification of your evidence.
- Case Number, Examiner, and Evidence Number fields help strengthen chain of custody documentation.
- Notes are a good place to log any special considerations (e.g., device condition, encryption status, startup behavior).

6.5 Network Share



Sr.	Server Address	Share Name

Network is disabled

System Clock: 2025-Feb-24 13:48:13 EST

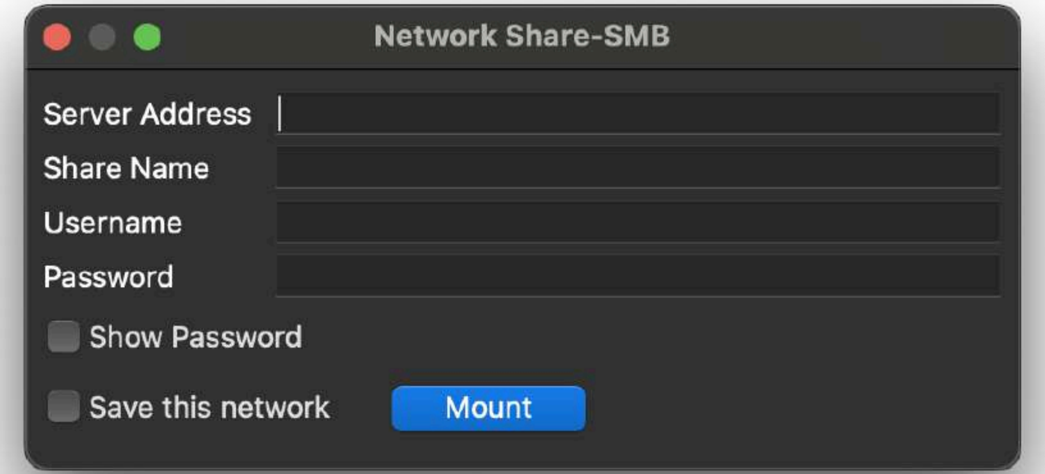
The **Network Share** option within the Imager allows you to add and configure an **SMB (SAMBA) network connection**. This enables you to send forensic images directly to a network destination.

Using Network Share (Bootable Environment)

In the bootable environment, you must first **connect to the network** by clicking **Enable Network**. Once the network is enabled, you can configure SMB network connections through the Network Share interface.

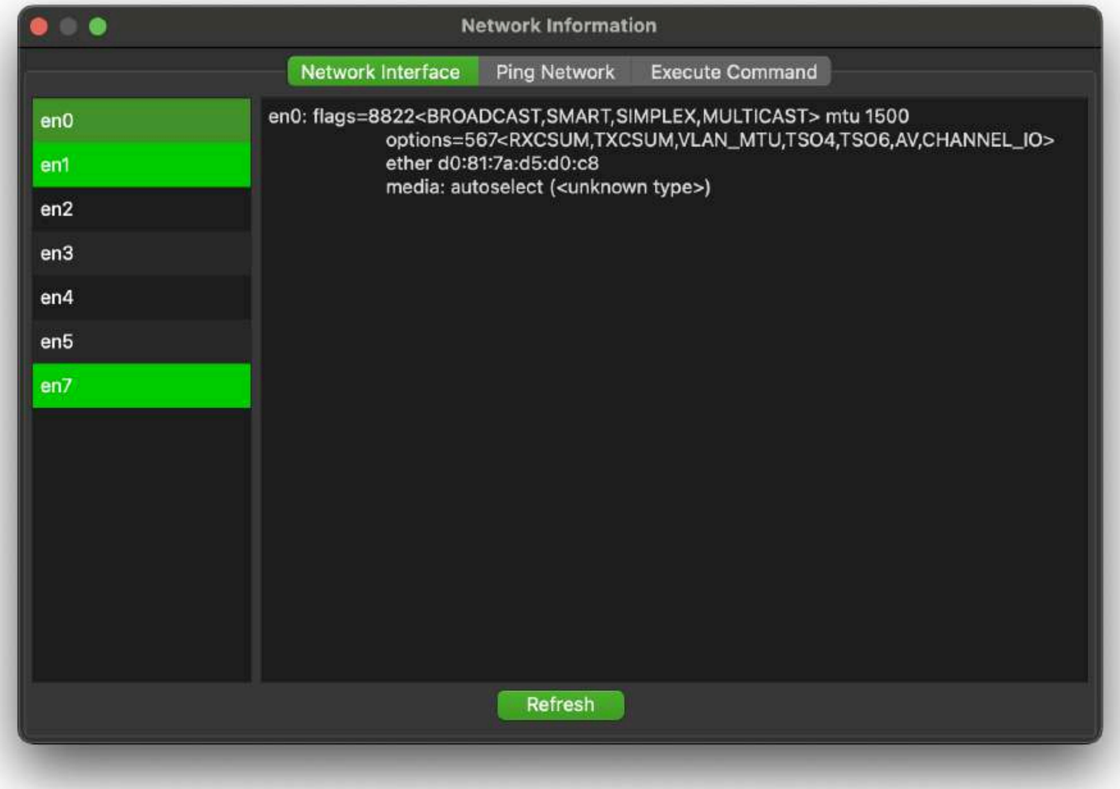
Network Share Functions

Action	Description
Add	Add a new network connection.
Remove	Remove the selected network connection.
Mount	Connect to the selected network share.
Unmount	Disconnect from the selected network share.
Refresh List	Update the list of available network connections.



Adding a Network Connection

1. Click **Add**.
2. Enter your **SAMBA network settings** and **credentials**.
3. (Optional) Check **Save this network** if you want RECON Imager to remember the connection for future use.
4. After entering the settings, click **Mount**.
5. Once mounted, your network share will appear as a **Destination** option when selecting where to save your forensic image.



```
en0: flags=8822<BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
        options=567<RXCSUM,TXCSUM,VLAN_MTU,TSO4,TSO6,AV,CHANNEL_IO>
        ether d0:81:7a:d5:d0:c8
        media: autoselect (<unknown type>)
```

Additional Network Tools (Bootable Environment Only)

At the bottom of the **Network Share** tab, you will also see a **Network Info** button. The following tools are available:

Tool	**Description**
Network Interface	Displays information about active network connections (IP addresses, interfaces, etc.).
Ping Network	Tests if a specific network address is reachable. ➔ Enter a network address and click **Ping**.
Execute Command	Allows you to enter and run a single Terminal command. ➔ Results are displayed immediately below.

⚡ Quick Tips:

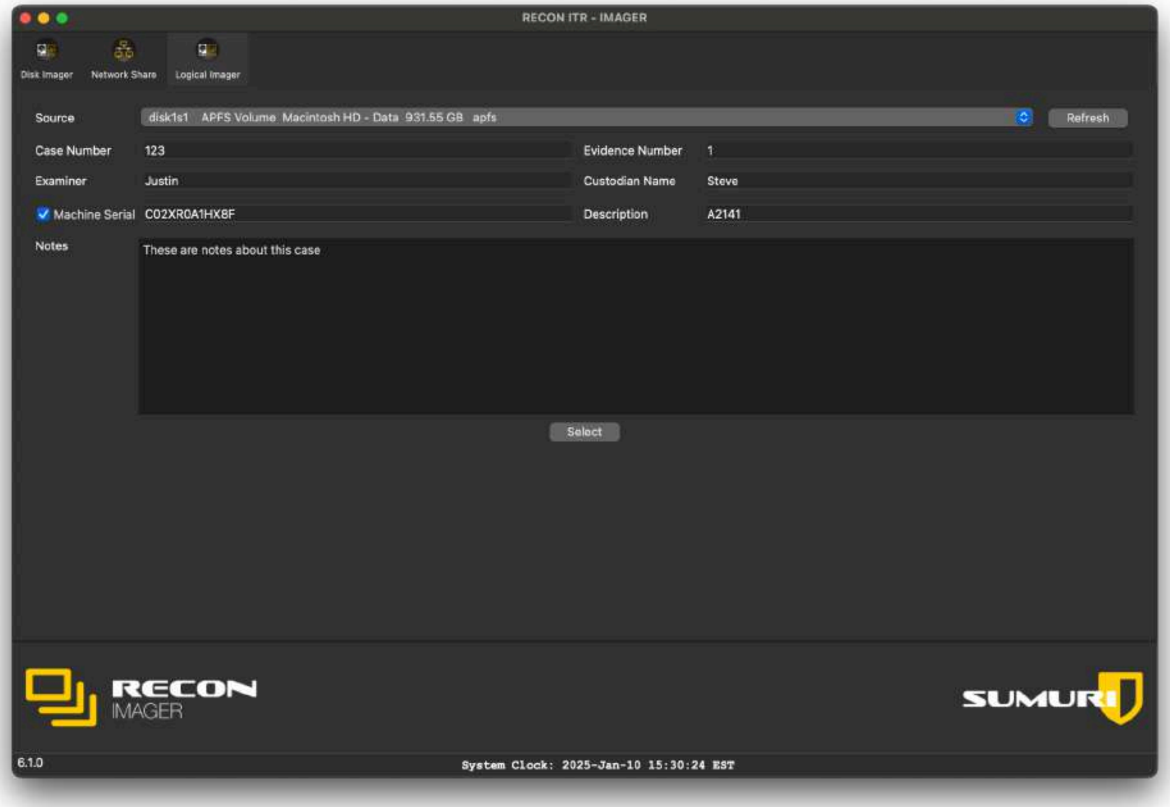
- Always verify that you are properly connected to the network **before imaging** to avoid incomplete transfers.
- Use **Ping Network** to troubleshoot basic connectivity issues.
- Mount the network share **before** starting the imaging process to ensure it appears as an available destination.

6.6 Logical Imager

The **Logical Imager** allows you to create a **targeted forensic image** of **selected files or directories** instead of capturing an entire disk. This is useful for situations where a **full physical image** is not required or not possible. Using the Logical Imager, you can:

- Select the **APFS Data Volume** from the **Source** dropdown.
- Target specific files, folders, or plugins for collection.

6.6.1 Creating a Logical Imager Case



Source: disk1s1 APFS Volume Macintosh HD - Data 931.55 GB apfs

Case Number: 123

Evidence Number: 1

Examiner: Justin

Custodian Name: Steve

☑ Machine Serial: C02XR0A1HX8F

Description: A2141

Notes: These are notes about this case

System Clock: 2025-Jan-10 15:30:24 EST

When setting up a Logical Imager case, you can enter the following Case Details:

Field	Description
Case Number *(Optional)*	Enter the case number associated with the investigation.
Examiner *(Optional)*	Enter the name of the examiner performing the acquisition.
Machine Serial *(Optional/Autofill)*	The Mac's serial number will automatically populate this field. ➔ You can exclude it by deselecting the checkbox next to "Machine Serial."
Evidence Number *(Optional)*	Enter the evidence tag or number for the device, if applicable.
Custodian Name *(Optional)*	Enter the name of the custodian or device owner.

Description *(Optional)*	Provide a brief description of the device (e.g., "MacBook Air M2, 2022").
Notes *(Optional)*	Add any relevant notes about the case or acquisition context.

Important for Bootable Environment Use

If you are using the Logical Imager in the **bootable environment**:

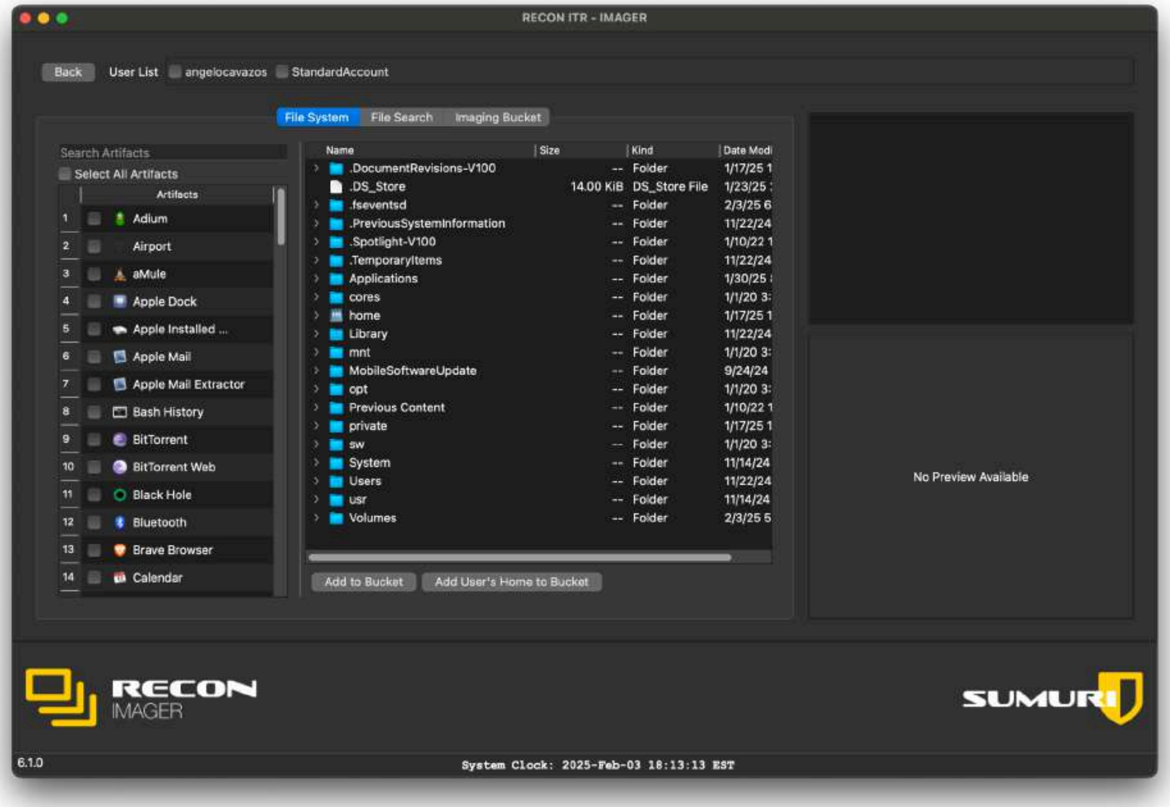
- **You must decrypt FileVault** on the selected source volume using the **Disk Manager**.
- If FileVault encryption remains active, a **warning** will appear notifying you that FileVault is still enabled.

Decrypting FileVault ensures that all targeted files and metadata can be properly accessed and imaged.

⚡ Quick Tips:

- Always double-check if FileVault is active before beginning a logical acquisition.
- Logical Imager is ideal for live environments when imaging only specific user data (e.g., Documents, Downloads, Desktop).
- Proper Case Detail entry strengthens your evidence documentation, even during partial acquisitions.

6.6.2 File System View



	Artifacts
1	Adium
2	Airport
3	aMule
4	Apple Dock
5	Apple Installed ...
6	Apple Mail
7	Apple Mail Extractor
8	Bash History
9	BitTorrent
10	BitTorrent Web
11	Black Hole
12	Bluetooth
13	Brave Browser
14	Calendar

Name	Size	Kind	Date Modi
.DocumentRevisions-V100	--	Folder	1/17/25 1
.DS_Store	14.00 KiB	DS_Store File	1/23/25
.fseventsd	--	Folder	2/3/25 6
.PreviousSystemInformation	--	Folder	11/22/24
.Spotlight-V100	--	Folder	1/10/22 1
.TemporaryItems	--	Folder	11/22/24
Applications	--	Folder	1/30/25
cores	--	Folder	1/1/20 3:
home	--	Folder	1/17/25 1
Library	--	Folder	11/22/24
mnt	--	Folder	1/1/20 3:
MobileSoftwareUpdate	--	Folder	9/24/24
opt	--	Folder	1/1/20 3:
Previous Content	--	Folder	1/10/22 1
private	--	Folder	1/17/25 1
sw	--	Folder	1/1/20 3:
System	--	Folder	11/14/24
Users	--	Folder	11/22/24
usr	--	Folder	11/14/24
Volumes	--	Folder	2/3/25 5

System Clock: 2025-Feb-03 18:13:13 EST

The **File System View** in RECON ITR is divided into several sections, providing forensic examiners with powerful tools to:

- Select artifacts for imaging
- Select specific files or directories
- View detailed file information
- Image user home directories

Each section of the File System View is designed to streamline targeted acquisitions.

6.6.2.1 Artifacts Panel (Far Left)

The **Artifacts Panel** is the **far-left** section of the File System View. It displays a list of artifacts available for logical imaging. When an artifact is selected:

- RECON IMAGER locates known directories associated with the application.
- Relevant **SQLite databases** and **plist files** containing application data are automatically retrieved.
- These files are copied into the forensic image.

Artifact Panel Options:

- **Select All Artifacts**:
  - Check this box to include **all available artifacts** in the logical imaging selection.
- **Search Artifacts**:
  - Use the search field to quickly find specific artifacts by name.

> **Tip:** Artifacts include data from common apps like Safari, Mail, Notes, Messages, and more.

6.6.2.2 File Navigation Table (Center)

The central table displays the **root** of the selected **APFS Data Volume** and allows you to manually navigate through its folder structure.

To add a file or folder to the imaging set:

1. Click on the desired file or folder.
2. Click **Add To Bucket**.
3. The item will now appear in the **Imaging Bucket**, ready for acquisition.

> **Note:** Only files and folders added to the Imaging Bucket will be included in the logical image.

6.6.2.3 File Details and Preview (Far Right)

The **far-right panel** shows detailed attributes of any selected file, including:

- File Name
- File Path
- Timestamps (Created, Modified, Accessed)
- Size
- Permissions

If the selected file is a media file (e.g., images or videos), RECON ITR provides an in-panel **live preview** for quick validation.

6.6.2.4 Imaging User Profiles

You can also target and image entire user home directories. To add a user's home folder to the Imaging Bucket**:**

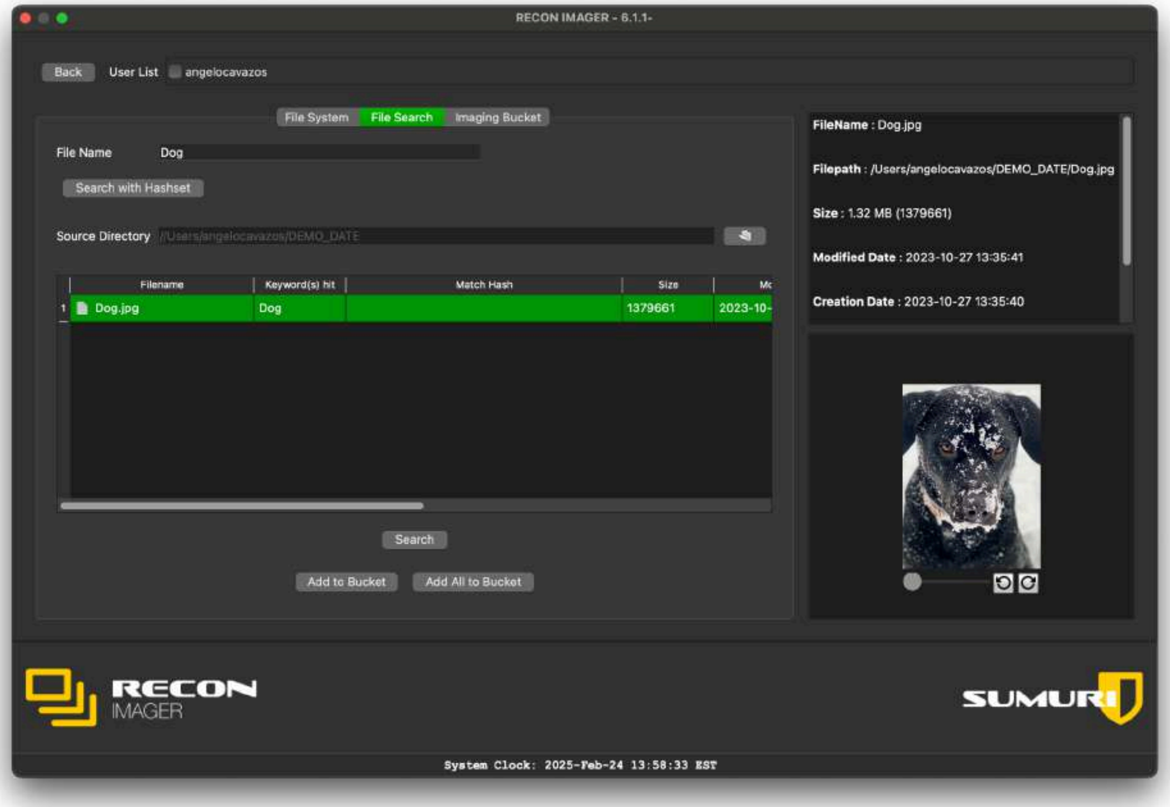
1. In the **User List** at the top of the screen, check the box next to the user profile you want to collect.
2. Click **Add User's Home to Bucket**.
3. The full home directory path will be added to the Imaging Bucket for acquisition.

Tip: Imaging user profiles ensures you collect common locations like Desktop, Documents, Downloads, and Library data.

⚡ Quick Tips:

- Combine artifact selection **and** file system selection for a thorough targeted collection.
- Preview file metadata before adding large directories to avoid unnecessary imaging.
- Always verify the Imaging Bucket before starting the logical acquisition.

6.6.3 File Search



User List □ angelocavazos

File Name: Dog

Source Directory: //Users/angelocavazos/DEMO_DATE

	Filename	Keyword(s) hit	Match Hash	Size	Mc
1	Dog.jpg	Dog		1379661	2023-10-

FileName : Dog.jpg

Filepath : /Users/angelocavazos/DEMO_DATE/Dog.jpg

Size : 1.32 MB (1379661)

Modified Date : 2023-10-27 13:35:41

Creation Date : 2023-10-27 13:35:40

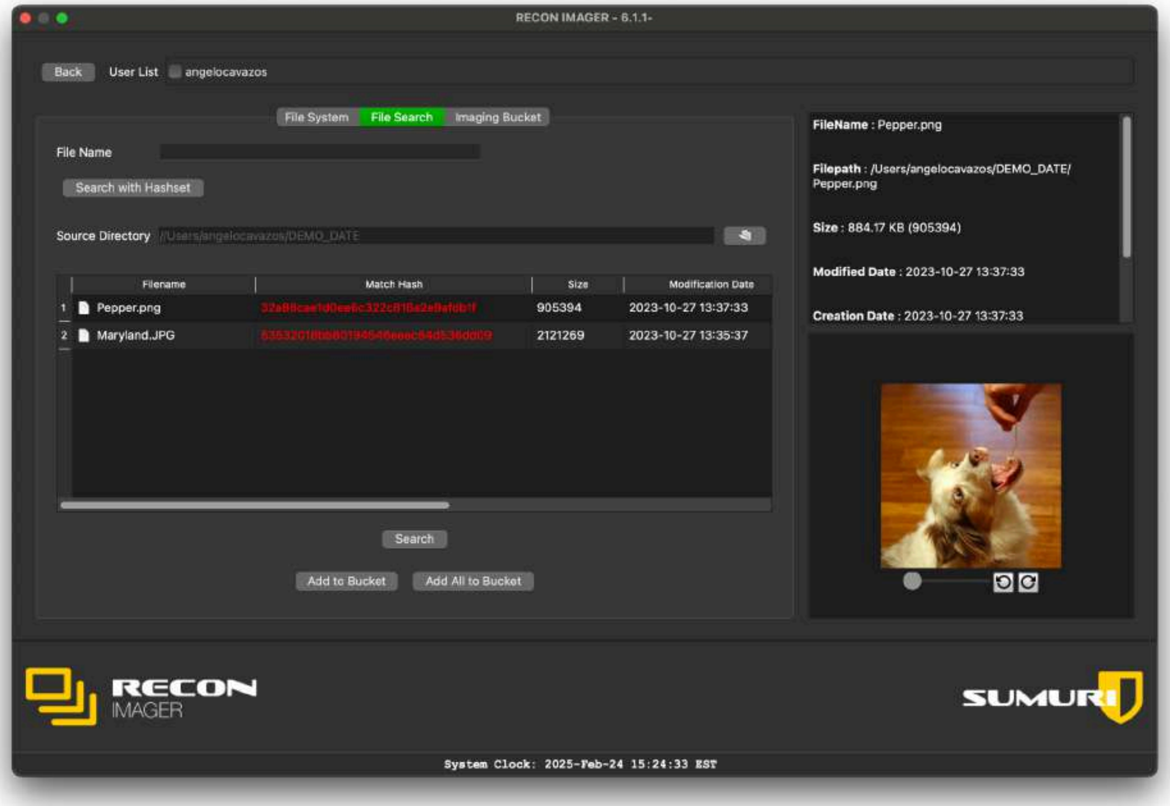
System Clock: 2025-Feb-24 13:58:33 EST

The **File Search** tab allows you to search a selected directory for files by:

- **Name** (filename or extension).
- **Hash value** (using a loaded hashset).

Files found through File Search can be added to the **Imaging Bucket**, which contains the list of all files and paths that will be imaged.

6.6.4 Key Areas of the File Search Tab



Source Directory: //Users/angelocavazos/DEMO_DATE

	Filename	Match Hash	Size	Modification Date
1	Pepper.png	32a88cae1d0ee6c322c816a2e8afdb1f	905394	2023-10-27 13:37:33
2	Maryland.JPG	63532018bb80194646eeec64d536dd09	2121269	2023-10-27 13:35:37

FileName : Pepper.png

Filepath : /Users/angelocavazos/DEMO_DATE/Pepper.png

Size : 884.17 KB (905394)

Modified Date : 2023-10-27 13:37:33

Creation Date : 2023-10-27 13:37:33

System Clock: 2025-Feb-24 15:24:33 EST

Area	Description
File Search Tab	Allows you to search for files or folders by name or extension. ➔ Highlight results and add selected items to the Imaging Bucket.
Search with Hashset	Allows you to load a CSV or SQLite hashset. ➔ RECON ITR will search for files matching loaded hash values and allow targeted extraction.
Add to Bucket	Adds a **selected file or folder** from the search results into the Imaging Bucket.
Add All to Bucket	Adds **all files/folders** from the search results into the Imaging Bucket in one action.

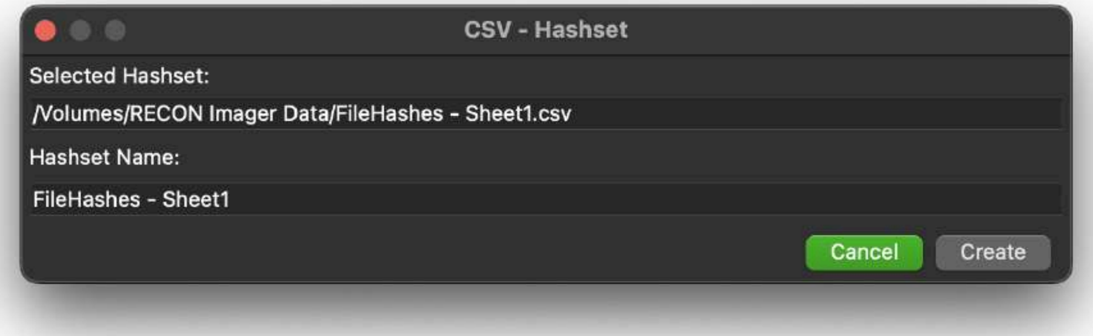
6.6.4.1 To Search With Hashset:

To perform a file search using a hashset:

1. **Select the Source Directory**
    - ○ Click the folder icon next to **Source Directory**.

- Use the Finder window to choose where the search should begin (e.g., APFS Data volume or specific user folder).

2. **Enable Hashset Search**
   - Click **Search with Hashset**.
3. **Import the Hashset**
   - Click **Import**.
   - Choose the hashset file format:
     - **CSV** (Comma-Separated Values) file, or
     - **SQLite** database file.
   - Navigate to and select your hashset file.



CSV - Hashset

Selected Hashset:

/Volumes/RECON Imager Data/FileHashes - Sheet1.csv

Hashset Name:

FileHashes - Sheet1

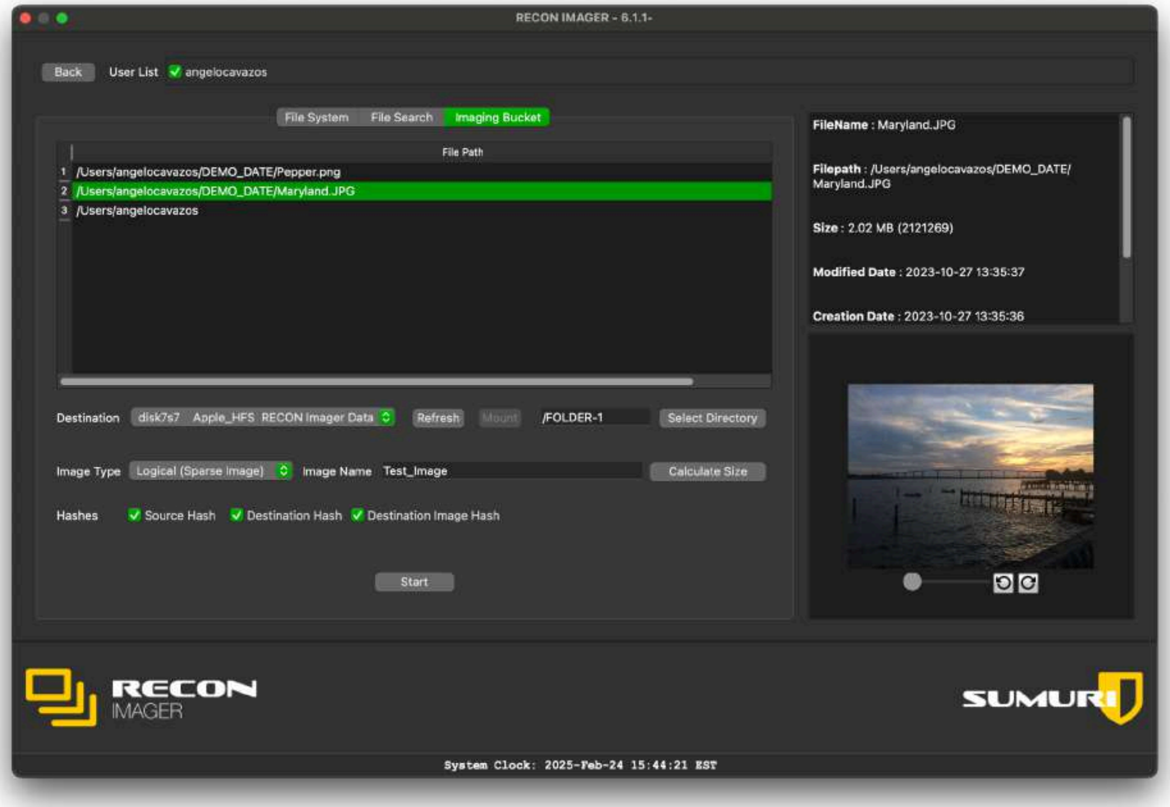
4. **Verify Hashset Information**
   - After importing, verify that the hashset data is displayed correctly.
   - Click **Create** to load the hashset.
5. **Select the Hashset**
   - In the list of available hashsets, select the one you want to use.
   - Click **OK** to confirm.
6. **Run the Search**
   - Click **Search**.
   - RECON ITR will locate and display files that match the hash values from the loaded hashset.
7. **Add Matches to the Imaging Bucket**
   - Individually select matches and click **Add to Bucket**, or
   - Click **Add All to Bucket** to add all matches at once.

⚡ Quick Tips:

- Always ensure the correct **Source Directory** is selected before starting a hashset search.

- Verify your imported hashset format — column headers and hash types must match expectations (especially for CSV imports).
- Use **Add All to Bucket** carefully if your hashset is large, as this can quickly fill your Imaging Bucket with many files.

6.6.4 Imaging Bucket



User List ☑ angelocavazos

	File Path
1	/Users/angelocavazos/DEMO_DATE/Pepper.png
2	/Users/angelocavazos/DEMO_DATE/Maryland.JPG
3	/Users/angelocavazos

FileName : Maryland.JPG

Filepath : /Users/angelocavazos/DEMO_DATE/ Maryland.JPG

Size : 2.02 MB (2121269)

Modified Date : 2023-10-27 13:35:37

Creation Date : 2023-10-27 13:35:36

Destination disk7s7 Apple_HFS RECON Imager Data /FOLDER-1

Image Type Logical (Sparse Image) Image Name Test_Image

Hashes ☑ Source Hash ☑ Destination Hash ☑ Destination Image Hash

System Clock: 2025-Feb-24 15:44:21 EST

The **Imaging Bucket** contains a list of file and directory paths selected for logical imaging.
This feature generates a targeted forensic image of the selected **files, directories, and artifacts**.

> ***Important:***
> *Artifacts selected from the **File System View do not appear** in the Imaging Bucket but **will still be included** in the imaging process if selected.*

6.6.6 Key Areas of the Imaging Bucket

Area	Description
File Path Table	Lists the individual files and folders added for logical imaging. ➔ To remove a file: right-click the entry and choose either **Remove** (selected file) or **Remove All** (clear the entire bucket).
Destination	Dropdown list to select the drive where you want to save the logical image. ➔ For more details, see Destination Drive Formats.
Refresh	Updates the list of available disks shown in the Destination dropdown.
Mount	If the selected destination drive is not currently mounted, this button will mount it automatically.
Image Type	Allows you to select the output format. ➔ Only **Logical Image** formats are available here (e.g., Logical DMG, SparseImage, Logical Folder). ➔ For more details, see Logical Image Types.
Image Name	The name that will be assigned to the created logical image file.
Calculate Size	Estimates the total size of the selected files and folders in the Imaging Bucket.
Hashes	Select hashing options for the logical image. ➔ For more details on available hashing options, see Hashing Options and Source Options.

⚡ Quick Tips:

- Always **calculate the size** of your Imaging Bucket before starting to ensure the destination drive has enough space.
- Use **Remove** and **Remove All** carefully — there is no undo option.
- Confirm your **Image Name** is unique and descriptive for easy tracking later.

6.7 Shutdown - (Boot Only)

When using the **bootable RECON Imager**, you will see a **Shut Down** button available on the interface. It is recommended to use this **Shut Down** button to properly power off the device after a successful imaging session. Clicking **Shut Down** will:

- Safely close all running processes,
- Unmount any mounted volumes, and
- Cleanly power down the Mac.

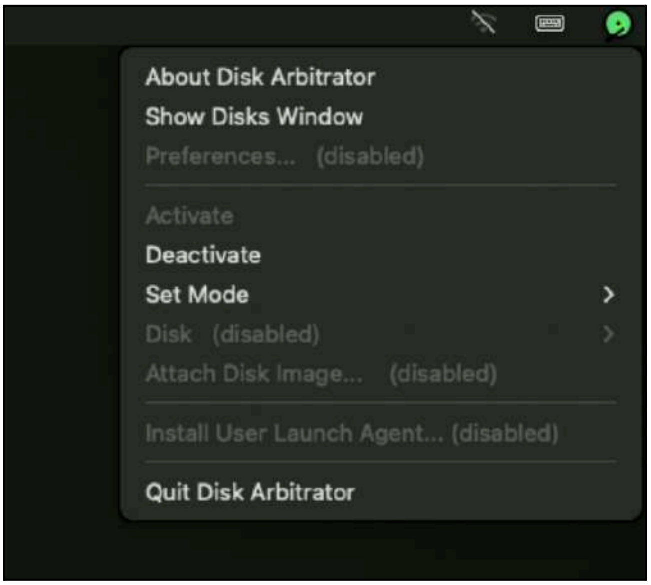
6.8 License Agreement - (Boot Only)

When using the bootable RECON Imager, you may also see a **License Agreement** button. Clicking the **License Agreement** button will allow you to:

- View the current End User License Agreement (EULA), and
- Review the changelog for recent updates and improvements to the RECON Imager software.

> ***Note:***
> *It is important to review the EULA to understand the usage rights, restrictions, and responsibilities associated with using RECON Imager.*

6.9 Disk Arbitrator - (Boot Only)



6.9.1 Disk Arbitrator – (Boot Only)

The **bootable RECON Imager** includes a built-in **Disk Arbitrator** tool.
Disk Arbitrator controls how volumes are mounted, overriding the macOS system's default disk handling behavior to help maintain evidence integrity.

6.9.2 Key Details About Disk Arbitrator

- **Supported Macs**:
    - ✅ Disk Arbitrator is **supported** when imaging **Intel-based Macs**.
    - ❌ Disk Arbitrator is **not supported** when imaging **Apple Silicon (M1, M2, M3, etc.)** Macs.
- **Default Behavior**:
    - Disk Arbitrator is **enabled by default** when the bootable imager loads.
- **Accessing Disk Arbitrator**:
    - Click the **green disk icon** located in the **top-right corner** of the system bar.
    - From here, you can **enable** or **disable** Disk Arbitrator as needed.

6.9.3 When to Disable Disk Arbitrator

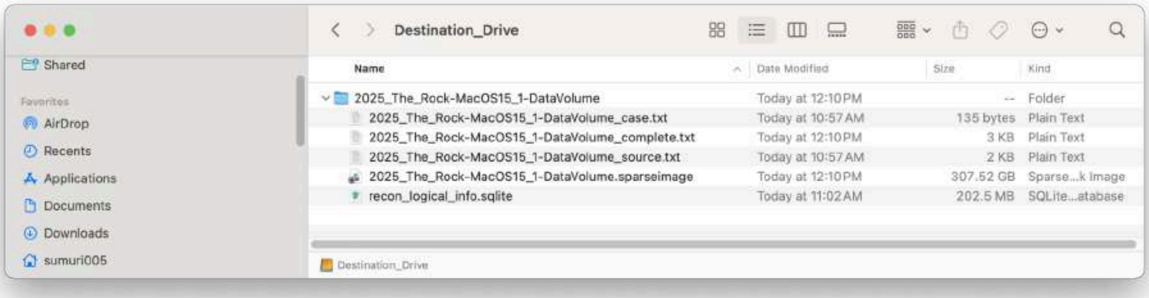
- **Disable Disk Arbitrator only when imaging an APFS Container**.
  - This is necessary because the **Apple Software Restore (ASR)** command used for container imaging requires Disk Arbitrator to be turned off.
- **No need to disable** Disk Arbitrator when imaging:
  - A **physical drive** (e.g., `disk0`)
  - An **individual APFS volume** (e.g., `disk1s1`)

Reminder:
Always verify whether you are imaging a **container** or a **volume** before adjusting Disk Arbitrator settings.

⚡ Quick Tips:

- Leave Disk Arbitrator **enabled** for most imaging tasks to ensure volumes are safely controlled and mounted read-only.
- Only **disable it temporarily** if you are performing an **ASR-based block copy** of an APFS Container.

6.10 Imager Case Folder



Destination_Drive

Name	Date Modified	Size	Kind
2025_The_Rock-MacOS15_1-DataVolume	Today at 12:10 PM	--	Folder
2025_The_Rock-MacOS15_1-DataVolume_case.txt	Today at 10:57 AM	135 bytes	Plain Text
2025_The_Rock-MacOS15_1-DataVolume_complete.txt	Today at 12:10 PM	3 KB	Plain Text
2025_The_Rock-MacOS15_1-DataVolume_source.txt	Today at 10:57 AM	2 KB	Plain Text
2025_The_Rock-MacOS15_1-DataVolume.sparseimage	Today at 12:10 PM	307.52 GB	Sparse...k Image
recon_logical_info.sqlite	Today at 11:02 AM	202.5 MB	SQLite...atabase

Destination_Drive

Once RECON Imager has successfully completed imaging, an **Imager Case folder** will be created on the selected **destination drive**.

- If a **specific directory** was not selected during setup, the case folder will be placed in the **root** of the destination drive.
- If a directory was selected, the case folder will be created in that chosen location.

6.10.1 Files and Directories Created in an Imager Case

File / Folder	Description
Case.txt	Stores the **Case Details** entered during case setup, including Case Name, Examiner Name, Custodian Name, and other metadata.
Complete.txt	Logs the **acquisition details**, including: - Imaging start and end times - Targeted source information - Destination drive information - MD5 and SHA-1 hashes if "Destination Image Hash" was selected.
Source.txt	Contains **detailed information** about the source disk or volume that was imaged (e.g., drive identifiers, disk type, file system).
Files_Hashes *(Folder)*	Contains a series of **CSV files** listing individual file **Source Hashes** and **Destination Hashes**. ➔ Only appears if a **logical image** was performed and file hashing options were enabled. ➔ Number of CSV files depends on how many files were included in the logical image.
Files_Hashes_SQLite	An **SQLite database** that stores individual file hashes for Source Hash and Destination Hash. ➔ Only appears if a **logical image** was performed and file hashing was selected.
Recon_logical_info.sqlite	An **SQLite database** created during logical acquisitions to preserve the **original timestamps and inode references** of the collected files. ➔ RECON LAB reads this database to display original file metadata when loading a RECON Logical Image.

Forensic Image File

- Within the Imager Case folder, you will also find the forensic image file created during acquisition (e.g., `.dmg`, `.sparseimage`, `.e01`).
- The image file will be **locked** to prevent accidental access or deletion.

Important:
Locking the image protects the integrity of the forensic evidence while preserving chain of custody.

⚡ Quick Tips:

- Always verify that the **Complete.txt** file exists and matches your expected imaging parameters before closing your case.
- RECON LAB will automatically reference **Recon_logical_info.sqlite** to display correct timestamps if the image is loaded as a RECON Logical Image.

7 Imaging Guidelines

> ***Important:***
> *Before following any of the imaging guides below, always refer to your agency's **policies**, **procedures**, and **legal requirements** for imaging Mac systems.*

The following instructions are intended to serve as a **general baseline** for using RECON Imager. These guides provide helpful workflows, but **should not** replace your agency's approved protocols or case-specific instructions.

Use the following guides as a **general reference**, adapting steps as needed to meet your agency's standards and the specific circumstances of your investigation.

7.1 Bootable Imaging

Bootable imaging refers to shutting down a Mac, powering it on, and changing its **Startup Disk** to a **bootable RECON Imager** device. This allows acquisition of a forensic image outside of the live operating system environment.

> **Important:**
> If **FileVault** is enabled on the target device, you must provide either the **admin password** or the **FileVault Recovery Key** to capture a **decrypted image**.

7.1.1 Pre-Imaging Preparation

Before beginning:

- ✅ Ensure the **RECON Imager software** is updated to the latest version.
- ✅ Verify functionality on a **test system** before using on evidence devices.
- ✅ Confirm the **target Mac** (the device to be imaged) is **shut down**.

7.1.2 Bootable Imaging Procedure

1. Connect Devices
    - Connect the **RECON ITR drive** to the target Mac.
    - Connect a **separate destination drive** if needed for storing the forensic image.
2. Modify Startup Security Settings (If Required)
    - **Only required for Intel Macs with T2 Security Chip**:
        - Boot into **Recovery Mode**.
        - Open **Startup Security Utility** and lower the security settings (allow booting from external media).
          ➔ For detailed instructions, see Startup Security Utility.
        - After adjusting settings, **shut down** the Mac.
    - Apple Silicon Macs (M1, M2, M3, etc.):
        - No changes to security settings are required.
        - Boot directly into Startup Options as described below.
3. Boot into Startup Options
    - **Apple Silicon Macs**:
        - Press and **hold the Power button** until you see **"Loading startup options…"**.
    - **Intel Macs**:
        - Press the **Power button**, then immediately **hold the Option key** while the device starts up.
4. Select Bootable RECON Imager
    - Choose the appropriate **RECON Bootable Imager** from the Startup Options menu.
      ➔ For help choosing the correct imager, see Choosing a Bootable Imager.
    5. Troubleshooting:
        - If the bootable RECON Imager does not appear, double-check the **Startup Security settings**(Intel T2 Macs only).
        - If the Mac boots into **Internet Recovery Mode**, this usually indicates the device still has restricted startup settings (Intel T2 Macs only).
6. Launch RECON Utilities
    - From the **RECON Utilities window**, select the **RECON Imager** application and click **Continue**.
7. Check FileVault Status
    - When the **Disk Manager** screen loads:
        - Check if the target volume shows active **FileVault** encryption (look under the **Encrypted** column).
        - If FileVault is enabled:
            1. Select the encrypted volume.
            2. Click **Decrypt**.
            3. Enter an **Admin password** or the **FileVault Recovery Key**. ➔ For full instructions, see FileVault Decryption.
8. Start Imaging

- ○ Click the **Disk Imager** tab.

9. Select Source Disk
   - ○ In the **Source** dropdown, select the volume, container, or drive you wish to image.
     ➔ For guidance, see Supported Disk Sources.
10. Select Image Format
    - ○ In the **Image Type** dropdown, choose your preferred forensic image format.
      ➔ For options, see Image Type Options.
11. Configure Hashing (Optional)
    - ○ Select any desired hashing options (e.g., Destination Image Hash, Source Hash).
      ➔ For more details, see Hashing Options and Source Options.
12. Select Destination Drive
    - ○ Use the **Destination-1** dropdown to select the destination drive.
      ➔ For instructions, see Destination Drive Formats.
13. Enter Case Details
    - ○ Enter a **required Image Name**.
    - ○ Optionally, fill out the **Case Number**, **Examiner**, **Evidence Number**, **Custodian Name**, **Description**, and **Notes** fields.
14. Start Imaging Process
    - ○ After verifying all selections, click **Start**.
    - ○ A confirmation window will appear — click **Yes** to begin the imaging process.

7.1.2 ⚡ Quick Tips:

- 7.2 Intel T2 Macs ➔ Lower startup security settings before booting from RECON Imager.
- 7.3 Apple Silicon Macs ➔ No startup security changes required.
- 7.4 Always decrypt FileVault volumes if needed before imaging.
- 7.5 Always double-check destination drive free space and case detail entry.

7.2 Live Imaging with Admin Credentials

Disk images can also be captured **live** when logged in with a **user account that has administrative privileges**.

> **Important:**
> Live imaging requires that the RECON ITR application is granted **Full Disk Access** to properly image all available data.

7.2.1 Pre-Imaging Preparation

Before starting:

- ✅ Ensure the **RECON ITR software** is updated to the latest version.
- ✅ Verify RECON ITR functionality with **test data** on a non-evidence machine.
- ✅ Confirm you are logged in to a **user account with administrative privileges**.

7.2.2 Live Imaging Procedure

1. **Connect Devices**
    - Connect the **RECON ITR drive** to the Mac.
    - Connect a **separate destination drive** if needed for storing the forensic image.
2. **Adjust Power Settings**
    - Change the Mac's **energy and power settings** to prevent the system from sleeping or shutting down during imaging.
      ➔ For instructions, see Energy and Power Settings.
3. **Grant Full Disk Access**
    - Give the **RECON_ITR.app Full Disk Access** via:
      System Settings ➔ Privacy & Security ➔ Full Disk Access. ➔ For detailed steps, see Full Disk Access.
4. **Launch RECON ITR**
    - Open the **RECON ITR** application.
    - When prompted, enter the **admin password** and click **OK**.
5. **Open RECON Imager**

    - On the RECON ITR splash screen, click the **RECON Imager** button.
6. **Select Source Disk**
    - When the **Disk Imager** screen loads:
        - Click the **Source** dropdown.
        - Select the source drive, container, or volume to image.
          ➔ For more information, see Supported Disk Sources.
7. **Select Image Format**
    - Choose the desired format from the **Image Type** dropdown.
      ➔ For more details, see Image Type Options.
8. **Configure Hashing (Optional)**
    - If needed, select hashing options (Destination Image Hash, Source Hash, etc.).
      ➔ For more information, see Hashing Options and Source Options.
9. **Select Destination Drive**
    - Choose the drive where the image will be written using the **Destination-1** dropdown.
      ➔ For destination setup, see Destination Drive Formats.
10. **Enter Case Details**
    - Enter the required **Image Name**.
    - Optionally, complete the fields for **Case Number**, **Examiner**, **Evidence Number**, **Custodian Name**, **Description**, and **Notes**.
11. **Start Imaging Process**
    - Review and verify all settings.
    - Click **Start**.
    - Confirm your choices by clicking **Yes** when prompted to begin the imaging process.

⚡ Quick Tips:

- Without Full Disk Access, RECON ITR will not be able to image the full disk — you will be limited to partial user data.
- Always double-check power settings to prevent sleep or shutdown during long imaging operations.
- Record the admin account used for live imaging in your case notes for transparency.

7.3 Live Imaging with Logged in User (No Admin Credentials)

If the target Mac already has a user logged in and the **admin password is unknown**, you can still capture an image of that **logged-in user's home directory**.

> **Important:**
> This method only allows imaging of the user's accessible data, not full disk acquisition.

7.3.1 Pre-Imaging Preparation

Before beginning:

- ✅ Ensure the **RECON ITR software** is updated to the latest version.
- ✅ Verify functionality with **test data** on a non-evidence system.
- ✅ Confirm that the user is **already logged in** on the target Mac.

7.3.2 Live Imaging Procedure (No Admin Access)

1. Connect Devices
   - Connect the **RECON ITR drive** to the Mac.
   - Connect a **separate destination drive** if needed for saving the forensic image.
2. Adjust Power Settings
   - Modify the Mac’s **energy and power settings** to prevent sleep or shutdown during imaging.
     ➔ For instructions, see Energy and Power Settings.
3. Launch RECON ITR
   - Open the **RECON ITR** application.
   - When prompted for the **Admin Password**, click **Skip**, then click **Continue**.
4. Access RECON Imager
   - On the RECON ITR splash screen, click the **RECON Imager** button.
5. Switch to Logical Imager
   - Click the **Logical Imager** tab.
6. Select Source Volume
   - From the **Source** dropdown, select the **APFS Data Volume**.
7. Enter Case Details (Optional)
   - Optionally fill out **Case Number**, **Examiner**, **Evidence Number**, **Custodian Name**, **Description**, and **Notes**.
8. Select the User’s Home Directory
   - In the **User List** at the top of the Logical Imager screen:
     - Check the box next to the logged-in user's name.
     - Click **Add User’s Home to Bucket** (button at the bottom middle).
     - This action adds the user’s home directory path to the **Imaging Bucket**.
9. Configure Imaging Bucket
   - Click the **Imaging Bucket** tab.
   - Confirm that the user's home directory path has been added.
10. Select Destination Drive

- From the **Destination-1** dropdown, choose the drive where you want to save the logical image.
  ➔ For drive preparation details, see Destination Drive Formats.

11. Enter Image Name
    - Enter the required **Image Name** for the logical image file.
12. Configure Hashing (Optional)
    - If needed, select the hashing options you want to apply (e.g., Source Hash, Destination Hash).
      ➔ For options, see Hashing Options and Source Options.
13. Start Imaging Process
    - Review all selections carefully.
    - Click **Start**.
    - Confirm your choices by clicking **Yes** when prompted to begin the imaging process.

⚡ Quick Tips:

- Without admin access, you can only capture data from the logged-in user's profile — not system-wide data.
- Always double-check power settings to ensure the Mac stays awake during acquisition.
- Confirm that the correct **user profile** is selected before starting.

7.4 Imaging in Target Disk Mode

Target Disk Mode (TDM) allows any **Intel Mac** to be mounted as an external disk on another Mac. This method can be used to capture forensic images of Intel-based Macs, whether or not they have a **T2 Security Chip**.

> ***Important:***
> *Always verify your procedures against your agency's guidelines and policies before proceeding.*

7.4.1 Pre-Imaging Preparation

Before starting:

- ✅ Ensure the **RECON Imager software** is updated to the latest version.
- ✅ Verify functionality with **test data** on a non-evidence system.
- ✅ Confirm the **examiner Mac** (the Mac running RECON ITR) has administrative access.

7.4.2 Target Mac Setup (Mac to Be Imaged)

1. **Boot into Target Disk Mode**
   - Power on the Intel Mac while **holding down the T key**.
   - Continue holding until you see **symbols** on the screen (e.g., Thunderbolt, USB 3.1) indicating supported connection types.
2. **Connect Devices**
   - Connect the **Target Mac** to the **Examiner Mac** using a compatible cable (Thunderbolt, USB-C, or FireWire depending on model).
   - Connect the **RECON ITR drive** and a **destination drive** (if needed) into the **Examiner Mac**.

Note:
Target Disk Mode is available only on **Intel Macs**.
Apple Silicon Macs (M1, M2, M3, etc.) do not support traditional Target Disk Mode, but use a different "Share Disk" feature.

7.4.3 Examiner Mac Setup (Mac Running RECON ITR)

3. **Adjust Power Settings**
   - Change the **Energy and Power Settings** to prevent the Examiner Mac from sleeping during the imaging process.
     ➔ See Energy and Power Settings.
4. **Grant Full Disk Access**
   - Provide **Full Disk Access** to the **RECON_ITR.app** via:
     System Settings ➔ Privacy & Security ➔ Full Disk Access.
     ➔ See Full Disk Access for detailed instructions.
5. **Launch RECON ITR**
   - Open the **RECON ITR** application.
   - When prompted, enter the **admin password** and click **OK**.
6. **Access RECON Imager**
   - On the RECON ITR splash screen, click the **RECON Imager** button.

7.4.4 Imaging Process

7. **Select Source Disk**
    - In the **Disk Imager** screen, click the **Source** dropdown.
    - Select the disk representing the **mounted Target Disk Mode device**.
8. **Select Image Format**
    - Choose the desired forensic image format from the **Image Type** dropdown.
      ➔ For format details, see Image Type Options.
9. **Configure Hashing (Optional)**
    - If needed, select hashing options (Destination Image Hash, Source Hash, etc.).
      ➔ See Hashing Options and Source Options.
10. **Select Destination Drive**
    - Use the **Destination-1** dropdown to choose the drive where the image will be written.
      ➔ See Destination Drive Formats.
11. **Enter Case Details**
    - Enter the **required Image Name**.
    - Optionally fill out the **Case Number**, **Examiner**, **Evidence Number**, **Custodian Name**, **Description**, and **Notes** fields.
12. **Start Imaging Process**
    - Verify all settings carefully.
    - Click **Start**.
    - Confirm by clicking **Yes** when prompted to begin the imaging process.

⚡ Quick Tips:

- Always use a **high-speed connection** (Thunderbolt or USB 3.1) for faster imaging.
- Carefully verify the mounted Target Disk Mode disk to avoid selecting the Examiner Mac's internal drive by mistake.
- TDM disks typically mount under a different name or identifier than internal volumes.

7.5 Imaging in Share Disk Mode

Share Disk Mode is a feature available on **Apple Silicon Macs** that allows one Mac's internal storage to be shared with another Mac over a direct USB-C or Thunderbolt connection.

> ***Important:***
> ***Share Disk Mode should be used as a last resort.***
> *It is **not recommended** for standard forensic imaging because:*
>
> - *It was **not designed** for transferring large amounts of data.*
> - *It is **much slower** compared to other imaging methods (bootable imaging, live imaging, etc.).*

Always use bootable imaging or other direct methods when possible. Reserve Share Disk Mode for situations where no other imaging method is available.

7.5.1 Pre-Imaging Preparation

Before beginning:

- ✅ Ensure the **RECON Imager software** is updated to the latest version.
- ✅ Verify RECON Imager functionality using **test data** on a non-evidence system.

7.5.2 Setup Process

1. **Connect the Devices**
   - Connect the **Examiner Mac** and the **Target Mac** (Apple Silicon) using a **USB-C** or **Thunderbolt** cable.
2. **Prepare the Target Mac**
   - Ensure the Target Mac is **shut down**.
   - Press and **hold the Power button** until you see **"Loading startup options…"**.
   - Click **Options**, then click **Continue**.
   - Select the **Startup Disk** (you may be prompted to unlock it with a password).
   - From the **Utilities** dropdown menu, select **Share Disk**.
   - Select the disk you want to share, then click **Start Sharing**.

7.5.3 Setup on the Examiner Mac

3. **Connect RECON Devices**
   - Connect the **RECON ITR drive** to the Examiner Mac.
   - Connect a **destination drive** if needed for saving the forensic image.
4. **Adjust Power Settings**
   - Configure the Examiner Mac's **Energy and Power Settings** to prevent sleep or shutdown.
     ➔ See Energy and Power Settings for instructions.
5. **Grant Full Disk Access**
   - Give the **RECON_ITR.app Full Disk Access** through:
     System Settings ➔ Privacy & Security ➔ Full Disk Access.
     ➔ See Full Disk Access for detailed setup.
6. **Launch RECON ITR**
   - Open the **RECON ITR** application.
   - When prompted, enter the **admin password** and click **OK**.
7. **Open RECON Imager**
   - On the RECON ITR splash screen, click the **RECON Imager** button.

7.5.4 Imaging Process

8. **Select Source Disk**
   - In the **Disk Imager** screen, click the **Source** dropdown.
   - Select the disk that was mounted through Share Disk Mode (it will appear as an external disk).
9. **Select Image Format**
   - Choose your preferred forensic image format from the **Image Type** dropdown.
     ➔ See Image Type Options.
10. **Configure Hashing (Optional)**
    - Select any desired hashing options (e.g., Destination Image Hash, Source Hash).
      ➔ See Hashing Options and Source Options.
11. **Select Destination Drive**
    - Use the **Destination-1** dropdown to select where the image will be saved.
      ➔ See Destination Drive Formats.
12. **Enter Case Details**
    - Enter the required **Image Name**.
    - Optionally fill out the **Case Number**, **Examiner**, **Evidence Number**, **Custodian Name**, **Description**, and **Notes** fields.
13. **Start Imaging Process**
    - Carefully review all settings.
    - Click **Start**.
    - Confirm by clicking **Yes** when prompted to begin the imaging process.

⚡ Quick Tips:

- Expect **slower transfer speeds** in Share Disk Mode compared to direct imaging methods.
- Always document in your case notes when Share Disk Mode was used and why it was necessary.
- Monitor the Examiner Mac and Target Mac throughout the imaging process to ensure stable connectivity.

8 Live Triage

Live Triage allows you to quickly review artifacts from a **running device** or a device connected through **Target Disk Mode (TDM)**. This process is designed to provide **fast access** to critical information — but it **does not replace** a **full forensic acquisition** and **full analysis**.

> **Important:**
> **Triage is intended for rapid assessment only.** It provides a quick view of selected artifacts to help guide investigative decisions, but it is **not a substitute for full forensic imaging, evidence preservation, or comprehensive analysis**.

When a plugin is selected and a triage scan is run:

- A **table of parsed artifacts** will be displayed for immediate review.
- A **report** can be generated documenting the artifacts found.

8.0.1 Triage Options

- **New Case**:
  ➔ Click the **New Case** button on the RECON ITR splash screen to start a new triage session.
- **Load Case**:
  ➔ Use the **Load Case** button to reopen and review a previously saved triage session.

8.1 Prerequisites

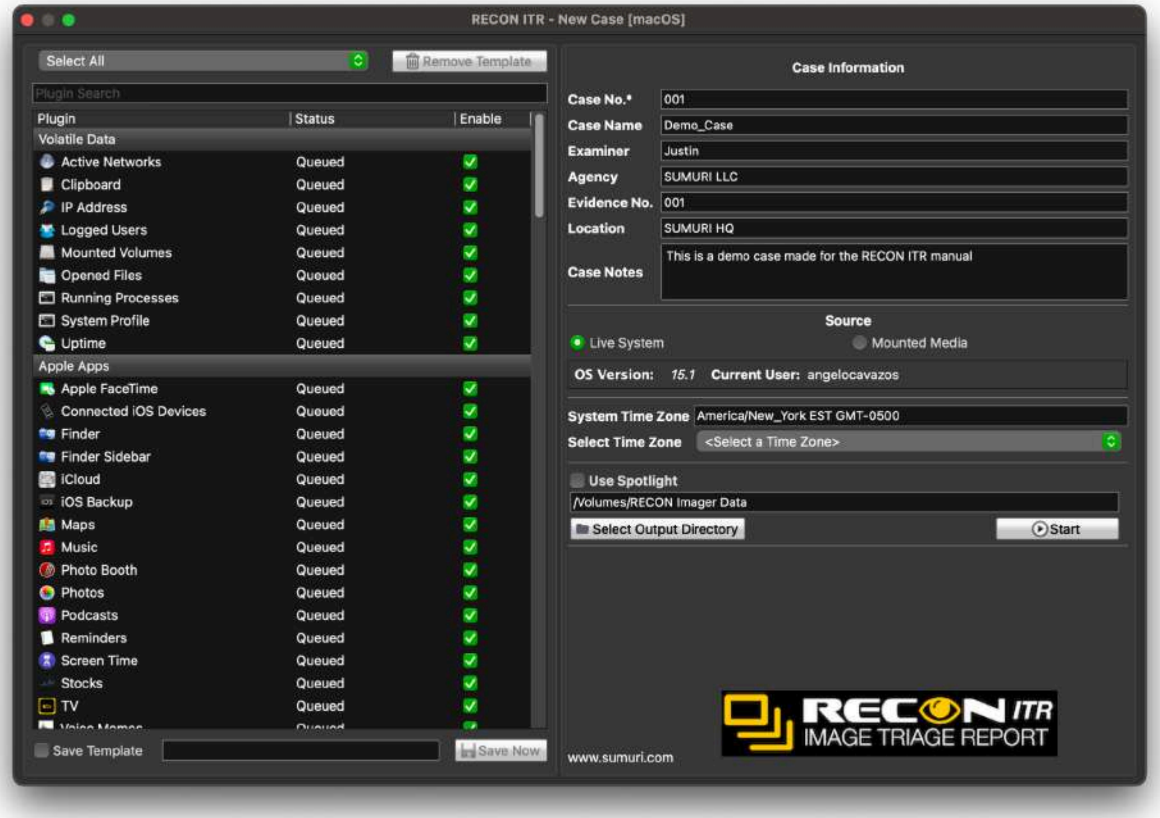
Before performing Live Triage, ensure the following:

Requirement	Description
Full Disk Access	Grant **RECON ITR Full Disk Access** through **System Settings ➔ Privacy & Security ➔ Full Disk Access**.
Device Compatibility	Confirm the target device **meets the minimum system requirements** to run RECON ITR.
Sufficient Storage	Ensure there is a **destination drive** or location large enough to store **case files**. ➔ Set this using the **Select Output Directory** button.
Administrator Access	For best results, log in with a **user account that has Administrator privileges**. This ensures the maximum amount of artifact data can be accessed.

⚡ Quick Reminders:

- Use Triage to **quickly gather answers** when time is critical (e.g., assessing user activity, confirming artifact presence).
- Always plan to perform a **full forensic image and full analysis** if evidence needs to be preserved, presented in court, or fully examined.
- Document triage sessions separately from full forensic examinations to maintain clear case integrity.

8.2 Creating a Triage Case



Plugin	Status	Enable
Volatile Data		
Active Networks	Queued	✓
Clipboard	Queued	✓
IP Address	Queued	✓
Logged Users	Queued	✓
Mounted Volumes	Queued	✓
Opened Files	Queued	✓
Running Processes	Queued	✓
System Profile	Queued	✓
Uptime	Queued	✓
Apple Apps		
Apple FaceTime	Queued	✓
Connected iOS Devices	Queued	✓
Finder	Queued	✓
Finder Sidebar	Queued	✓
iCloud	Queued	✓
iOS Backup	Queued	✓
Maps	Queued	✓
Music	Queued	✓
Photo Booth	Queued	✓
Photos	Queued	✓
Podcasts	Queued	✓
Reminders	Queued	✓
Screen Time	Queued	✓
Stocks	Queued	✓
TV	Queued	✓
Voice Memos	Queued	✓

Case Information

Case No.* 001
Case Name Demo_Case
Examiner Justin
Agency SUMURI LLC
Evidence No. 001
Location SUMURI HQ
Case Notes This is a demo case made for the RECON ITR manual

Source

● Live System ○ Mounted Media

OS Version: 15.1 Current User: angelocavazos

System Time Zone America/New_York EST GMT-0500
Select Time Zone <Select a Time Zone>

□ Use Spotlight
/Volumes/RECON Imager Data

Creating a **new case** is the first and most important step when triaging a live device.

To start a Triage session:

- Click the **New Case** button on the RECON ITR splash screen.
- This will open the **Triage Case Setup** window.

In the Triage Case Setup window, you can:

- Select which **plugins** you would like to run.
- Enter **case details**.
- Configure the **source**, **time zone**, and **output directory**.

8.2.1 Selecting Plugins

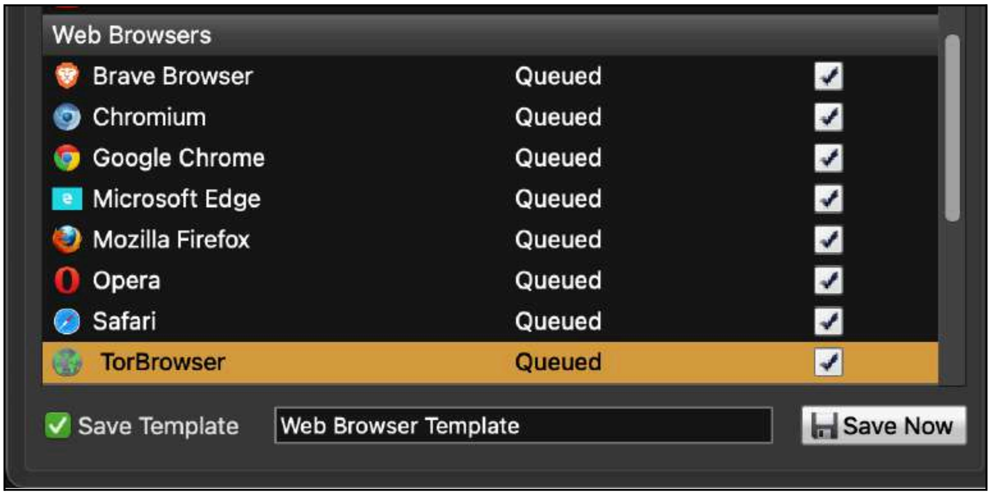
In the Plugins panel:

- Click the checkbox under the **Enable** column next to each plugin you wish to run.

- RECON ITR will parse the live system (or connected device) and extract forensic artifacts related to the selected plugins.
- Parsed artifact data will be displayed in structured, easy-to-read tables.

Tip:
Selecting only necessary plugins can speed up triage and reduce case file size.

8.2.2 Creating a template



Web Browsers		
Brave Browser	Queued	☑
Chromium	Queued	☑
Google Chrome	Queued	☑
Microsoft Edge	Queued	☑
Mozilla Firefox	Queued	☑
Opera	Queued	☑
Safari	Queued	☑
TorBrowser	Queued	☑

☑ Save Template: Web Browser Template

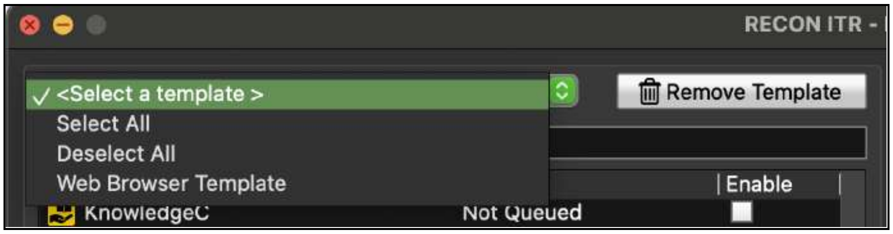
Templates are useful when you frequently need to run the same set of plugins across multiple devices.

To create a template:

1. Select the desired plugins by checking the boxes under the **Enable** column.
2. Check the **Save Template** box at the bottom right of the Triage Setup window.
3. Enter a name for your template in the text box.
4. Click **Save Now**.

After saving:

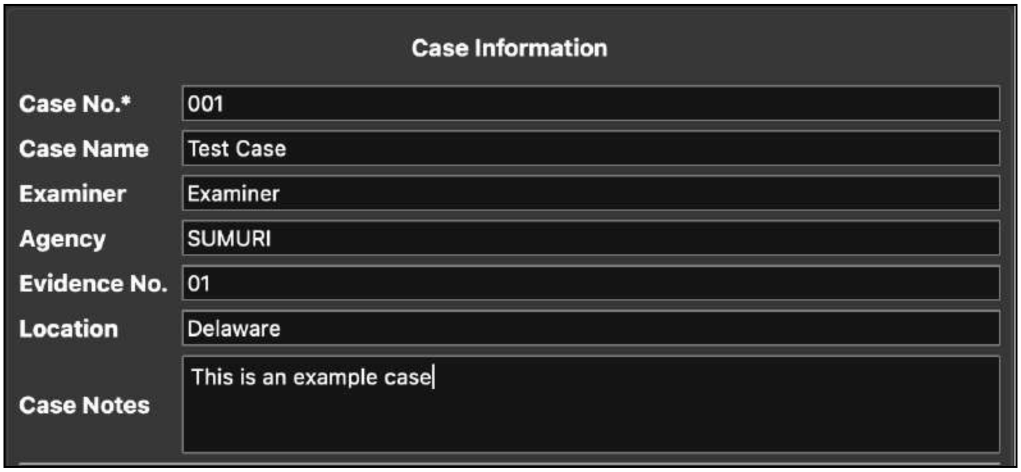
- Your template will appear at the top of the window under the **Select a Template** dropdown.
- Selecting a saved template will automatically re-select all plugins included when the template was created.



KnowledgeC Not Queued □

Tip:
Templates improve efficiency by standardizing your triage plugin selection.

8.2.3 Case Information



Case Information

Case No.*	001
Case Name	Test Case
Examiner	Examiner
Agency	SUMURI
Evidence No.	01
Location	Delaware
Case Notes	This is an example case

Case Information contains important details that will be saved with the triage case and displayed whenever the case is loaded. Completing these fields helps maintain proper organization, chain of custody, and documentation standards for your investigations.

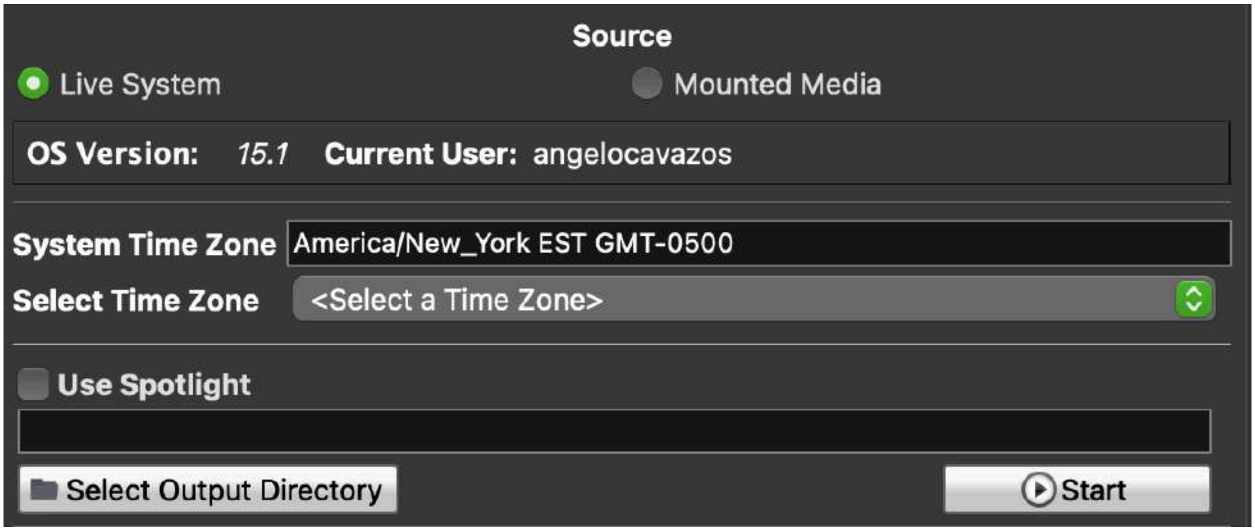
Field	**Description**
Case No. *(Required)*	A unique identifier for the case. **This field must be completed** before starting triage.
Case Name *(Optional)*	A descriptive name for the case (e.g., "Suspect Laptop 04/25/2025").
Examiner *(Optional)*	The name of the person conducting the triage. ➔ This value can be pre-set through the **Configuration** tab.
Agency *(Optional)*	The name of the agency or organization performing the triage. ➔ This value can also be pre-set through the **Configuration** tab.
Evidence No.*(Optional)*	An evidence number assigned to the device, if applicable.
Location *(Optional)*	The physical location where the device was obtained or examined.
Case Notes *(Optional)*	Any relevant notes or context regarding the device, the triage purpose, or examiner observations.

Reminder:

*Only the **Case No.** field is required to begin the triage process.*

All other fields are optional but highly recommended for complete documentation.

8.2.4 Source



Source

● Live System ○ Mounted Media

OS Version: 15.1 Current User: angelocavazos

System Time Zone America/New_York EST GMT-0500

Select Time Zone <Select a Time Zone>

□ Use Spotlight

In the **Source** section, select the device you want to triage:

- **Live System**
  ➔ Select this option if you are triaging the Mac where **RECON ITR** is currently running.
- **Mounted Media**
  ➔ Select this option if you are triaging a device connected through **Target Disk Mode (TDM)**.

Time Zone Selection

- By default, artifact timestamps will use the **system time zone** of the examiner Mac.
- To change the time zone:
  - Use the **Select a Time Zone** dropdown menu.
  - Choose the appropriate time zone for the device under investigation.

Tip:
Adjust the time zone if the device was seized from a different geographic location.

Spotlight Toggle Option

You also have the option to **toggle Spotlight indexing**:

- **Enable Spotlight Search**:
    - RECON ITR will utilize the **Spotlight indices** already present on the volume to locate files and artifacts.
    - **This method is faster** because it leverages the system's existing index.
- **Disable Spotlight Search**:
    - RECON ITR will perform a **live, non-indexed search** across the volume.
    - **This method is slower**, but it can be **more thorough**, especially if the Spotlight index is incomplete, corrupted, or missing certain data.

Tip:
If speed is critical and you trust the device's index, enable Spotlight.
If completeness is more important (e.g., during a high-priority triage), disable Spotlight for a deeper live search.

Output Directory

- Set the **output directory** where the case folder will be saved by clicking **Select Output Directory**.
- All parsed artifacts, triage reports, and logs will be saved in this location.

Note:
You must navigate to this same directory if you later want to **reload the case** using the **Load Case** option.

8.2.5 Starting the Triage Process

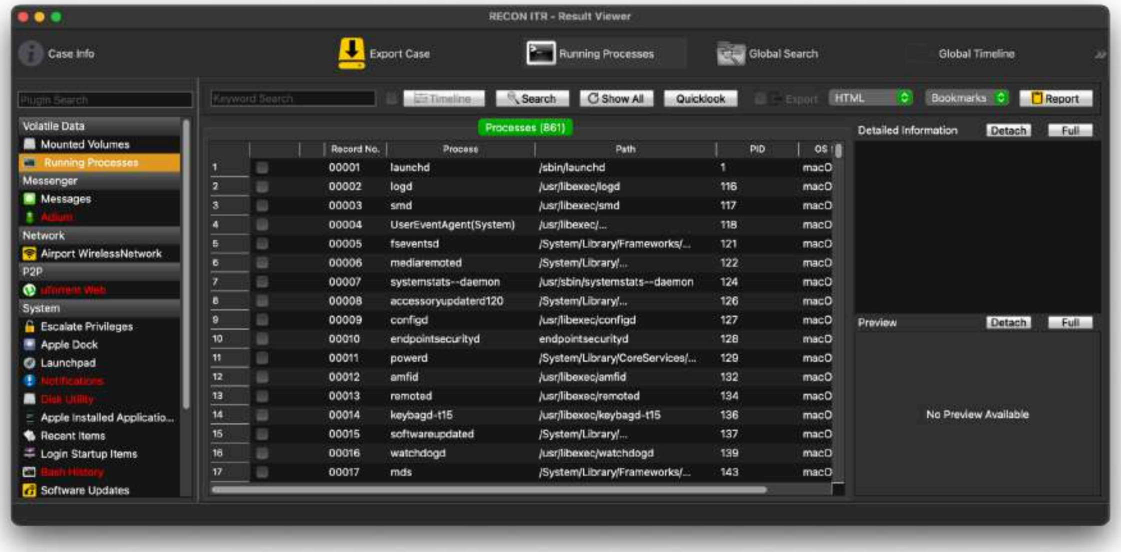
Once all selections are made:

- Confirm that the **Source**, **Time Zone**, **Spotlight Toggle**, and **Output Directory** are correctly set.
- Click **Start** to begin the triage process.

The **duration** of the triage will vary depending on:

- System hardware performance.
- Number and type of selected artifacts.
- Whether Spotlight indexing is utilized or bypassed.

8.3 Plugin Result Viewer



			Record No.	Process	Path	PID	OS
1			00001	launchd	/sbin/launchd	1	macO
2			00002	logd	/usr/libexec/logd	116	macO
3			00003	smd	/usr/libexec/smd	117	macO
4			00004	UserEventAgent(System)	/usr/libexec/...	118	macO
5			00005	fseventsd	/System/Library/Frameworks/...	121	macO
6			00006	mediaremoted	/System/Library/...	122	macO
7			00007	systemstats--daemon	/usr/sbin/systemstats--daemon	124	macO
8			00008	accessoryupdaterd120	/System/Library/...	126	macO
9			00009	configd	/usr/libexec/configd	127	macO
10			00010	endpointsecurityd	endpointsecurityd	128	macO
11			00011	powerd	/System/Library/CoreServices/...	129	macO
12			00012	amfid	/usr/libexec/amfid	132	macO
13			00013	remoted	/usr/libexec/remoted	134	macO
14			00014	keybagd-t15	/usr/libexec/keybagd-t15	136	macO
15			00015	softwareupdated	/System/Library/...	137	macO
16			00016	watchdogd	/usr/libexec/watchdogd	139	macO
17			00017	mds	/System/Library/Frameworks/...	143	macO

After triaging the selected device, the **Result Viewer** screen will appear. This interface enables examiners to:

- Navigate through the selected plugins.
- Review parsed forensic artifacts.
- Create reports based on collected data.

8.3.1 Overview

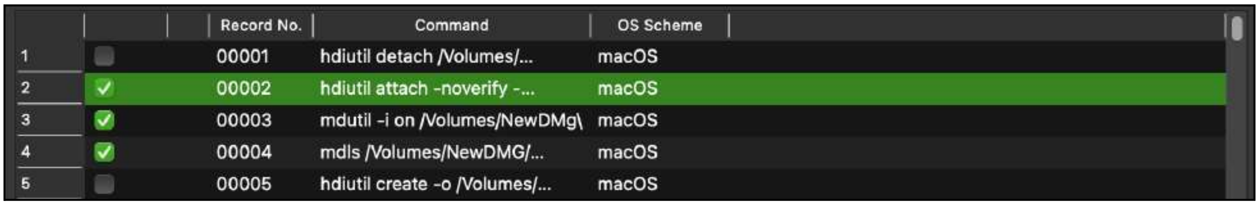
- On the **left side** of the Result Viewer, a list of all **executed plugins** is displayed.
- **Plugins highlighted in red** indicate that no relevant artifacts were found for that plugin or application during triage.

When a plugin is selected:

- A **table of parsed artifact records** will appear in the results window.
- Some plugins may have **multiple artifact tabs** — each tab contains different types of parsed records related to the application.
- If no artifacts are found for a specific plugin or artifact type, the table may appear **empty**.

> ***Reminder:***
> *The absence of parsed artifacts may simply indicate that the application was not used or data was not available.*

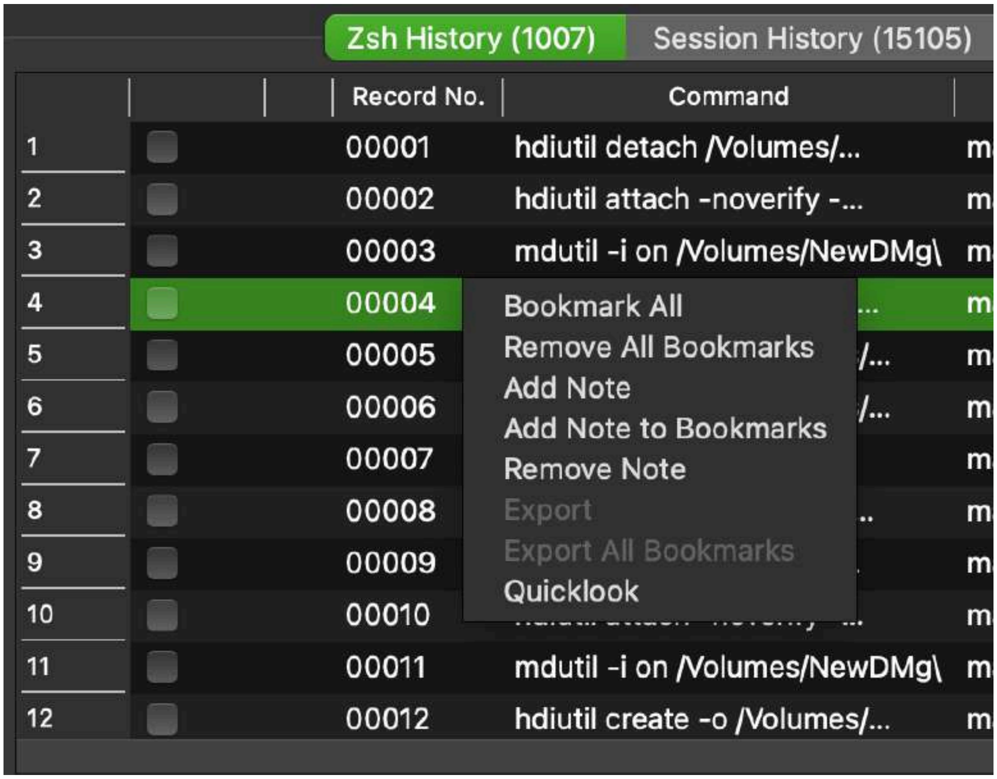
8.3.2 Bookmarking



			Record No.	Command	OS Scheme
1	□		00001	hdiutil detach /Volumes/...	macOS
2	☑		00002	hdiutil attach -noverify -...	macOS
3	☑		00003	mdutil -i on /Volumes/NewDMg\	macOS
4	☑		00004	mdls /Volumes/NewDMG/...	macOS
5	□		00005	hdiutil create -o /Volumes/...	macOS

Bookmarking allows examiners to mark artifacts of interest for reporting or exporting at a later time.

- **To bookmark a record**: Click the checkbox next to the item.
- **To unbookmark a record**: Click the checkbox again to remove the bookmark.



			Record No.	Command	
1	□		00001	hdiutil detach /Volumes/...	m
2	□		00002	hdiutil attach -noverify -...	m
3	□		00003	mdutil -i on /Volumes/NewDMg\	m
4	□		00004	...	m
5	□		00005	/...	m
6	□		00006	/...	m
7	□		00007		m
8	□		00008	..	m
9	□		00009	.	m
10	□		00010	-...	m
11	□		00011	mdutil -i on /Volumes/NewDMg\	m
12	□		00012	hdiutil create -o /Volumes/...	m

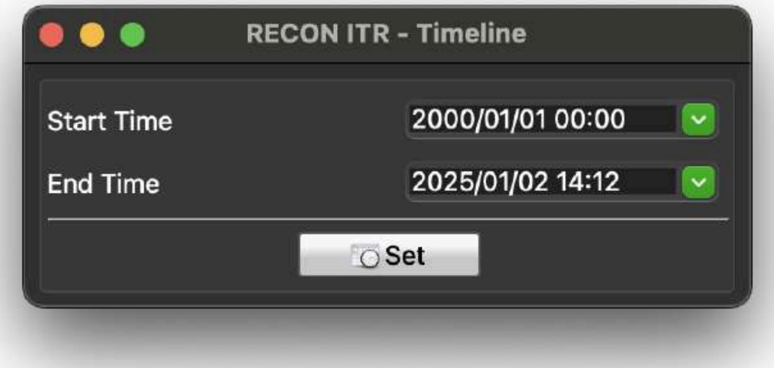
Right-click a record for additional bookmarking and note options:

Option	**Description**
Bookmark All	Bookmark every record in the active table.
Remove All Bookmarks	Remove bookmarks from all records in the active table.
Add Note	Attach a note to the selected record.
Add Note to Bookmarks	Attach the same note to all currently bookmarked records.
Remove Note	Delete a note attached to a record.
Export	Export the selected file or artifact.
Export All Bookmarks	Export all files that have been bookmarked.
QuickLook	Preview selected media files using Apple's native QuickLook feature.

> ***Tip:***
> *Bookmarking helps organize artifacts during review and simplifies creating focused reports later.*

8.3.3 Timeline

The **Timeline** feature enables examiners to filter records by a specific date range — if the selected plugin's artifact table contains date fields.



Start Time 2000/01/01 00:00

End Time 2025/01/02 14:12

- If the plugin supports Timeline filtering, the **Timeline checkbox** will be active.
- If not, the Timeline option will be **disabled**.

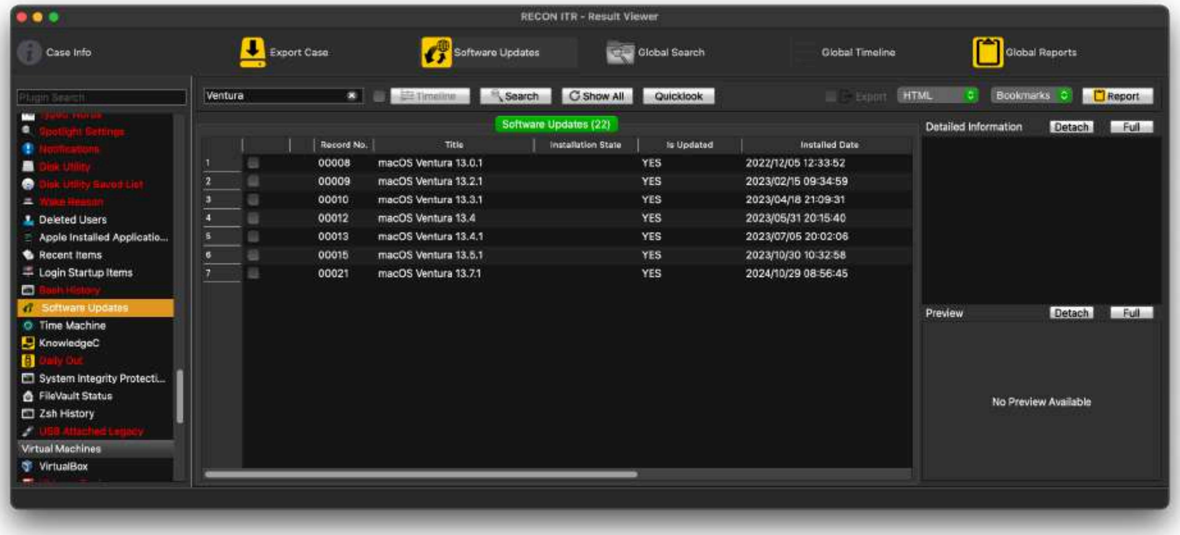
To use the Timeline filter:

1. Click the checkbox next to **Timeline** to enable it.
2. Click the **Timeline** button.
3. Enter a **Start Time** (beginning date of the filter).
4. Enter an **End Time** (ending date of the filter).
5. Click **Set** to apply the date range.

The table will then display **only the records** that fall within the selected date range.

8.3.4 Search

The **Search** feature allows you to find specific keywords within the active plugin's table.



			Record No.	Title	Installation State	Is Updated	Installed Date
1	□		00008	macOS Ventura 13.0.1		YES	2022/12/05 12:33:52
2	□		00009	macOS Ventura 13.2.1		YES	2023/02/15 09:34:59
3	□		00010	macOS Ventura 13.3.1		YES	2023/04/18 21:09:31
4	□		00012	macOS Ventura 13.4		YES	2023/05/31 20:15:40
5	□		00013	macOS Ventura 13.4.1		YES	2023/07/05 20:02:06
6	□		00015	macOS Ventura 13.5.1		YES	2023/10/30 10:32:58
7	□		00021	macOS Ventura 13.7.1		YES	2024/10/29 08:56:45

To search for keywords:

1. Enter the desired keyword into the **Keyword Search** text box.
2. Click **Search**.
3. All matching values containing the keyword will be displayed.

> ***Tip:***
> *Searches apply only to the currently selected plugin and currently displayed table.*

8.3.5 Show All

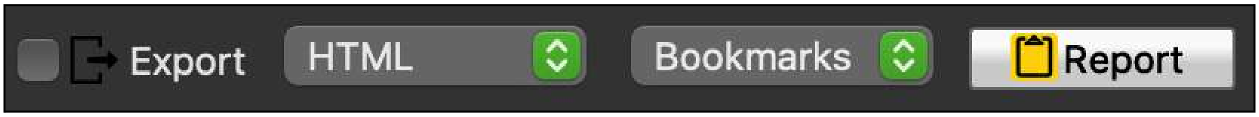
- Clicking the **Show All** button will **clear all active filters** and **redisplay all records**.
- This action removes any filters set by **Timeline** or **Search** functions.

8.3.6 QuickLook

- The **QuickLook** button opens the currently selected record (typically a media file) using **Apple's native QuickLook** viewer.
- This is useful for previewing files such as images, documents, videos, and other supported media types without leaving RECON ITR.

8.3.7 Export and Report

Reports can be generated for any plugin that has parsed artifact records.



To create a report:

1. Navigate to the desired plugin in the Result Viewer.
2. In the top-right corner, locate the **Report Options**.

If you wish to export associated files:

- Check the **Export** checkbox before generating the report.

Choose your desired report file format:

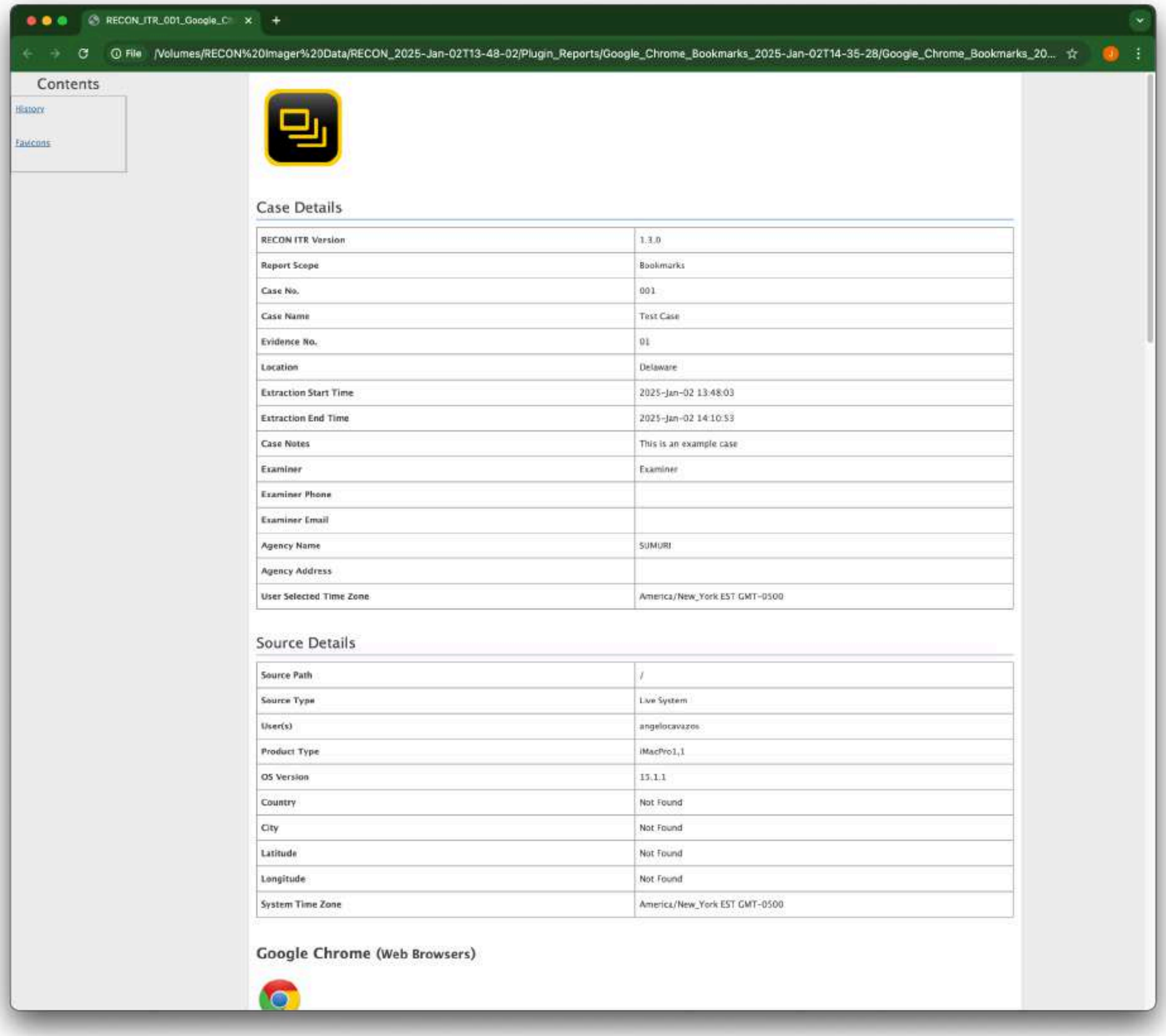
Format	Description
HTML	Opens in any web browser for easy viewing.
PDF	Creates a Portable Document Format file.
CSV	Creates a Comma-Separated Values spreadsheet.
XML	Creates an Extensible Markup Language file, useful for importing into other forensic tools.
KML	Creates a Keyhole Markup Language file for artifacts with location data (e.g., mapping coordinates).

Select what content to include in the report:

Option	Description
Bookmarks	Includes only bookmarked records from the selected plugin.
Full Plugin	Includes **all** records from the selected plugin.
Screen Items	Includes **only the records currently displayed** in the Results Window (after any active filters).

To finalize:

- Click **Report**.
- A pop-up will ask if you want to open the report immediately.
  - Click **Yes** to view the report now.
  - Click **No** to return to the Result Viewer.



RECON_ITR_001_Google_C
File /Volumes/RECON%20Imager%20Data/RECON_2025-Jan-02T13-48-02/Plugin_Reports/Google_Chrome_Bookmarks_2025-Jan-02T14-35-28/Google_Chrome_Bookmarks_20...
Contents
History
Favicons

Case Details

RECON ITR Version	1.3.0
Report Scope	Bookmarks
Case No.	001
Case Name	Test Case
Evidence No.	01
Location	Delaware
Extraction Start Time	2025-Jan-02 13:48:03
Extraction End Time	2025-Jan-02 14:10:53
Case Notes	This is an example case
Examiner	Examiner
Examiner Phone	
Examiner Email	
Agency Name	SUMURI
Agency Address	
User Selected Time Zone	America/New_York EST GMT-0500

Source Details

Source Path	/
Source Type	Live System
User(s)	angelocavazos
Product Type	iMacPro1,1
OS Version	15.1.1
Country	Not Found
City	Not Found
Latitude	Not Found
Longitude	Not Found
System Time Zone	America/New_York EST GMT-0500

Google Chrome (Web Browsers)

8.4 Global Search

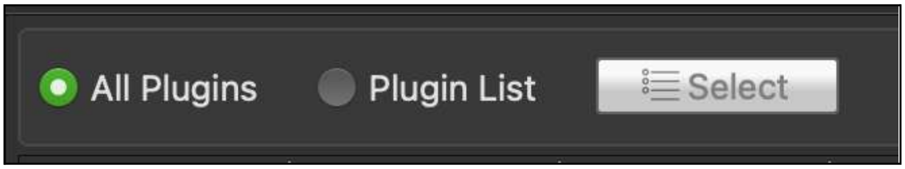
The **Global Search** feature allows you to perform a **keyword search** across multiple selected plugins at once. This can be helpful for quickly identifying artifacts of interest across different data sources without manually reviewing each plugin individually.

8.4.1 Overview

- To access Global Search:
  - Click the **Global Search** button located on the **top menu bar** of RECON ITR.
- Global Search enables you to:
  - Choose which plugins to search.
  - Enter one or more keywords.
  - Bookmark or export search results.

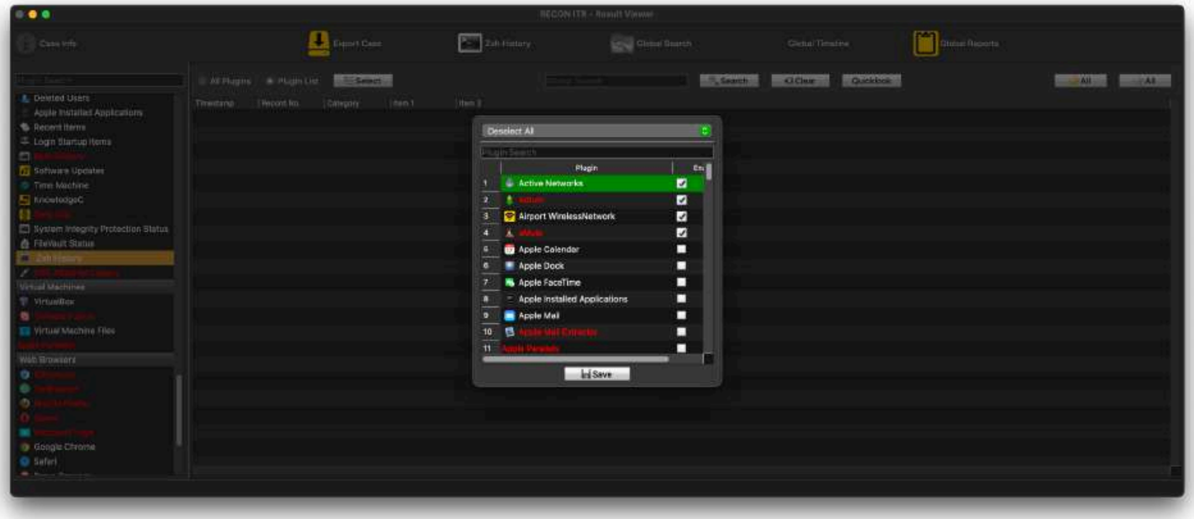
8.4.2 Plugin List

The **Plugin List** determines **which plugins** will be included in the Global Search.



You have two options:

- **Search All Plugins**:
  1. Click the **All Plugins** radio button in the top-left corner to search across **every available plugin**.
- **Search Specific Plugins**:
  1. Click the **Plugin List** radio button.
  2. Click **Select** to open the plugin selection window.
  3. Click **Enable** next to each plugin you want to include in the search.



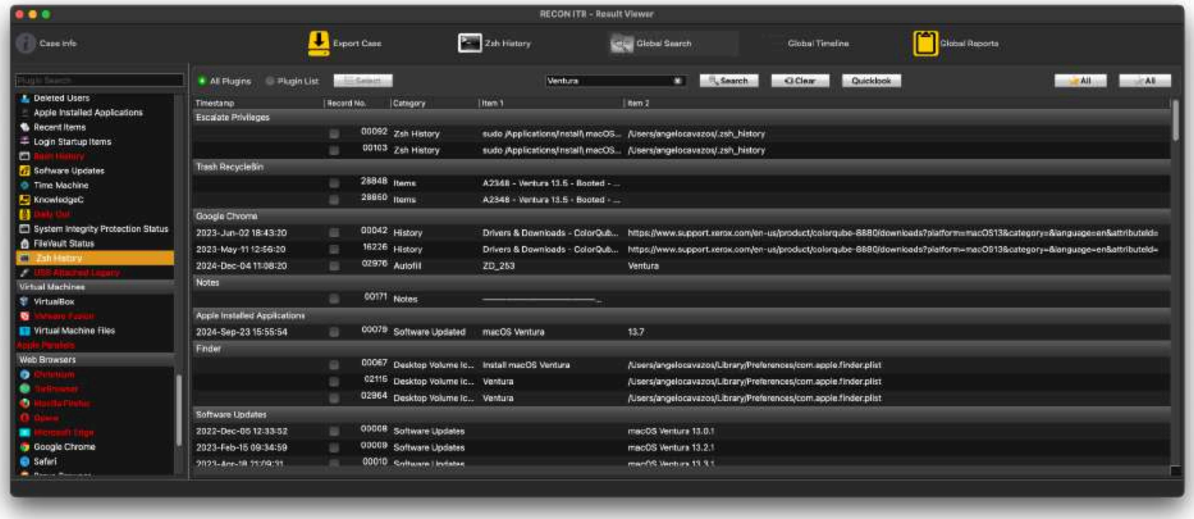
	Plugin	En
1	Active Networks	☑
2	[illegible]	☑
3	Airport WirelessNetwork	☑
4	[illegible]	☑
5	Apple Calendar	□
6	Apple Dock	□
7	Apple FaceTime	□
8	Apple Installed Applications	□
9	Apple Mail	□
10	Apple Mail Extractor	□
11	[illegible]	□

Tip:
Narrowing the plugin list can speed up search performance and focus results on specific artifact types.

8.4.3 Keyword Search

To perform a Global Search:

1. Enter the desired keyword into the **Global Search** text box.
2. Click the **Search** button.
3. RECON ITR will search the selected plugins for any records containing the entered keyword.



Timestamp	Record No.	Category	Item 1	Item 2
Escalate Privileges				
	00092	Zsh History	sudo /Applications/Install\ macOS...	/Users/angelocavazos/.zsh_history
	00103	Zsh History	sudo /Applications/Install\ macOS...	/Users/angelocavazos/.zsh_history
Trash RecycleBin				
	28848	Items	A2348 - Ventura 13.5 - Booted - ...	
	28850	Items	A2348 - Ventura 13.5 - Booted - ...	
Google Chrome				
2023-Jun-02 18:43:20	00042	History	Drivers & Downloads - ColorQub...	https://www.support.xerox.com/en-us/product/colorqube-8880/downloads?platform=macOS13&category=&language=en&attributeId=
2023-May-11 12:56:20	16226	History	Drivers & Downloads - ColorQub...	https://www.support.xerox.com/en-us/product/colorqube-8880/downloads?platform=macOS13&category=&language=en&attributeId=
2024-Dec-04 11:08:20	02976	Autofill	ZD_253	Ventura
Notes				
	00171	Notes	——————————_	
Apple Installed Applications				
2024-Sep-23 15:55:54	00079	Software Updated	macOS Ventura	13.7
Finder				
	00067	Desktop Volume Ic...	Install macOS Ventura	/Users/angelocavazos/Library/Preferences/com.apple.finder.plist
	02115	Desktop Volume Ic...	Ventura	/Users/angelocavazos/Library/Preferences/com.apple.finder.plist
	02964	Desktop Volume Ic...	Ventura	/Users/angelocavazos/Library/Preferences/com.apple.finder.plist
Software Updates				
2022-Dec-05 12:33:52	00008	Software Updates		macOS Ventura 13.0.1
2023-Feb-15 09:34:59	00009	Software Updates		macOS Ventura 13.2.1
2023-Apr-18 11:09:31	00010	Software Updates		macOS Ventura 13.3.1

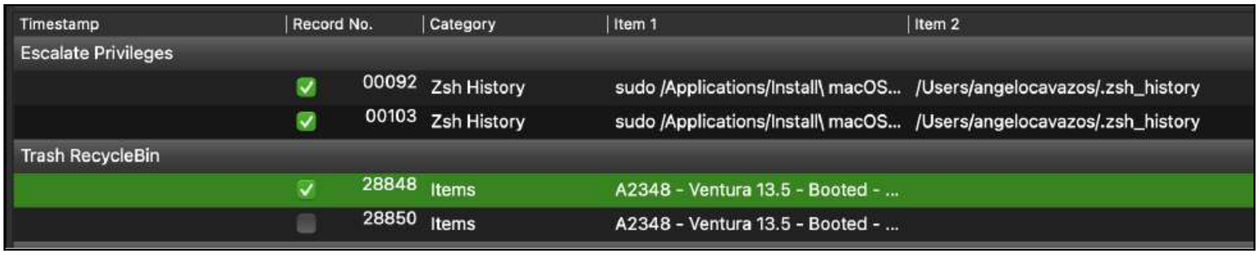
Additional Options:

- **Clear**:
➔ Click the **Clear** button next to Search to reset the search field and remove current results.
- **QuickLook**:
➔ Highlight a record, then click the **QuickLook** button to preview the selected file using Apple's native QuickLook.

Note:
Searching only applies to the currently selected plugin list and will not affect unselected plugins.

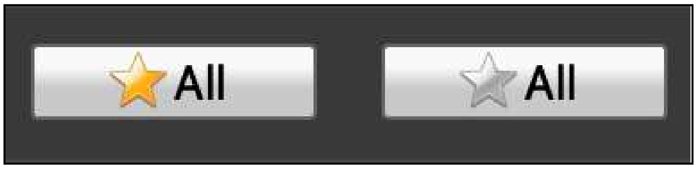
8.4.4 Bookmarking

Bookmarking search results allows you to easily save important records for later reporting or exporting.



Timestamp	Record No.	Category	Item 1	Item 2
Escalate Privileges				
	☑ 00092	Zsh History	sudo /Applications/Install\ macOS...	/Users/angelocavazos/.zsh_history
	☑ 00103	Zsh History	sudo /Applications/Install\ macOS...	/Users/angelocavazos/.zsh_history
Trash RecycleBin				
	☑ 28848	Items	A2348 - Ventura 13.5 - Booted - ...	
	□ 28850	Items	A2348 - Ventura 13.5 - Booted - ...	

- **To bookmark an individual record**:
  ➔ Click the **checkbox** next to the item you want to bookmark.
- **To bookmark all currently shown records**:
  ➔ Click the **gold star button** labeled "**All**".
- **To remove all bookmarks**:
  ➔ Click the **gray star button** labeled "**All**".



Tip:
Bookmarking during Global Search helps streamline the creation of focused reports based on keyword hits.

8.4.5 Report

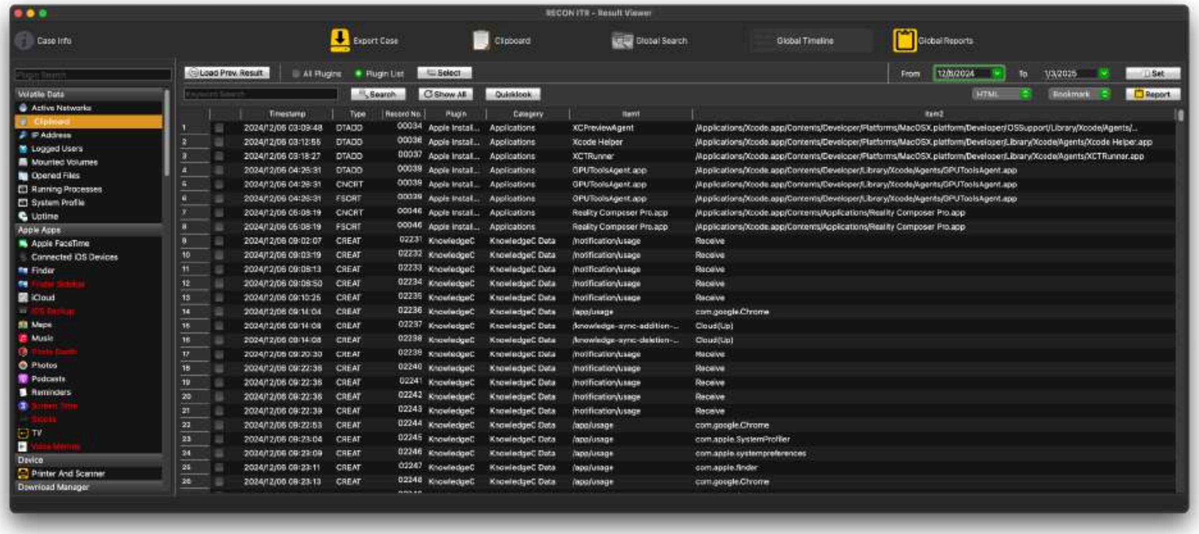
To generate a report based on bookmarked Global Search results:

1. Click the **Global Reports** button.
2. A new window will open, allowing you to configure and generate your report. ➔ For detailed instructions, see the Global Report section.

8.5 Global Timeline

The **Global Timeline** feature allows you to view artifact records containing **date fields** from multiple plugins in a **single table view**. This is useful for identifying patterns, sequences of events, or suspicious activities across different applications and data sources.

8.5.1 Overview



From 12/6/2024 To 1/3/2025

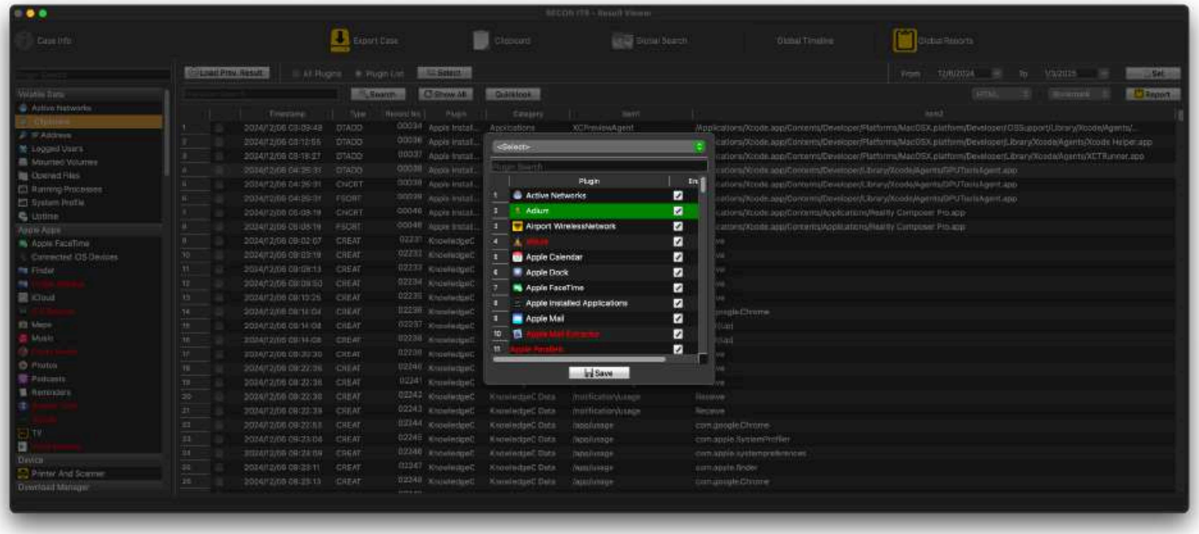
		Timestamp	Type	Record No.	Plugin	Category	Item1	Item2
1	□	2024/12/06 03:09:48	DTADD	00034	Apple Install...	Applications	XCPreviewAgent	/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/OSSupport/Library/Xcode/Agents/...
2	□	2024/12/06 03:12:56	DTADD	00036	Apple Install...	Applications	Xcode Helper	/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/Library/Xcode/Agents/Xcode Helper.app
3	□	2024/12/06 03:18:27	DTADD	00037	Apple Install...	Applications	XCTRunner	/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/Library/Xcode/Agents/XCTRunner.app
4	□	2024/12/06 04:26:31	DTADD	00038	Apple Install...	Applications	GPUToolsAgent.app	/Applications/Xcode.app/Contents/Developer/Library/Xcode/Agents/GPUToolsAgent.app
5	□	2024/12/06 04:26:31	CNCRT	00039	Apple Install...	Applications	GPUToolsAgent.app	/Applications/Xcode.app/Contents/Developer/Library/Xcode/Agents/GPUToolsAgent.app
6	□	2024/12/06 04:26:31	FSCRT	00039	Apple Install...	Applications	GPUToolsAgent.app	/Applications/Xcode.app/Contents/Developer/Library/Xcode/Agents/GPUToolsAgent.app
7	□	2024/12/06 05:08:19	CNCRT	00046	Apple Install...	Applications	Reality Composer Pro.app	/Applications/Xcode.app/Contents/Applications/Reality Composer Pro.app
8	□	2024/12/06 05:08:19	FSCRT	00046	Apple Install...	Applications	Reality Composer Pro.app	/Applications/Xcode.app/Contents/Applications/Reality Composer Pro.app
9	□	2024/12/06 09:02:07	CREAT	02231	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
10	□	2024/12/06 09:03:19	CREAT	02232	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
11	□	2024/12/06 09:08:13	CREAT	02233	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
12	□	2024/12/06 09:08:50	CREAT	02234	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
13	□	2024/12/06 09:10:25	CREAT	02235	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
14	□	2024/12/06 09:14:04	CREAT	02236	KnowledgeC	KnowledgeC Data	/app/usage	com.google.Chrome
15	□	2024/12/06 09:14:08	CREAT	02237	KnowledgeC	KnowledgeC Data	/knowledge-sync-addition-...	Cloud(Up)
16	□	2024/12/06 09:14:08	CREAT	02238	KnowledgeC	KnowledgeC Data	/knowledge-sync-deletion-...	Cloud(Up)
17	□	2024/12/06 09:20:30	CREAT	02239	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
18	□	2024/12/06 09:22:36	CREAT	02240	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
19	□	2024/12/06 09:22:36	CREAT	02241	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
20	□	2024/12/06 09:22:36	CREAT	02242	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
21	□	2024/12/06 09:22:39	CREAT	02243	KnowledgeC	KnowledgeC Data	/notification/usage	Receive
22	□	2024/12/06 09:22:53	CREAT	02244	KnowledgeC	KnowledgeC Data	/app/usage	com.google.Chrome
23	□	2024/12/06 09:23:04	CREAT	02245	KnowledgeC	KnowledgeC Data	/app/usage	com.apple.SystemProfiler
24	□	2024/12/06 09:23:09	CREAT	02246	KnowledgeC	KnowledgeC Data	/app/usage	com.apple.systempreferences
25	□	2024/12/06 09:23:11	CREAT	02247	KnowledgeC	KnowledgeC Data	/app/usage	com.apple.finder
26	□	2024/12/06 09:23:13	CREAT	02248	KnowledgeC	KnowledgeC Data	/app/usage	com.google.Chrome

- Global Timeline compiles and displays records with associated dates from the selected plugins.
- You can narrow the displayed data by applying **date ranges** and **keyword filters**.
- Records of interest can be **bookmarked** and **exported into a report** for documentation or further analysis.

Important:
Global Timeline is an excellent tool for identifying chronological sequences but does not replace full artifact review.

8.5.2 Plugin Selection

Before performing a Global Timeline search, you must first select which plugins to include.



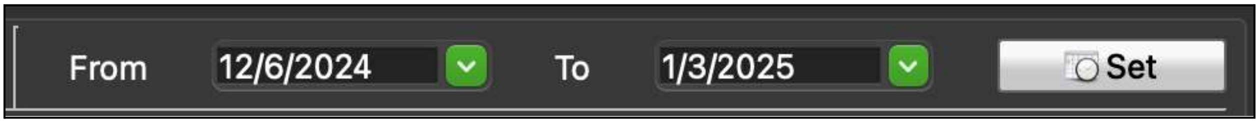
	Plugin	En
1	Active Networks	☑
2	Adium	☑
3	Airport WirelessNetwork	☑
4	[illegible]	☑
5	Apple Calendar	☑
6	Apple Dock	☑
7	Apple FaceTime	☑
8	Apple Installed Applications	☑
9	Apple Mail	☑
10	[illegible]	☑
11	[illegible]	☑

You have two options:

- **All Plugins**:
  ➔ Click the **All Plugins** radio button to include every plugin with date-based records.
- **Select Specific Plugins**:
  1. Click the **Plugin List** radio button.
  2. Click **Select**.
  3. In the selection window:
     - Click the **Enable** checkbox next to each desired plugin.
     - Use the **Plugin Search** text box to quickly find specific plugins by name.
     - Use the **Select** dropdown to **Select All** or **Deselect All** plugins quickly.
  4. After making your selections, click **Save**.

> ***Tip:***
> *Limiting the number of plugins can speed up timeline loading and make focused analysis easier.*

8.5.3 Date Selection

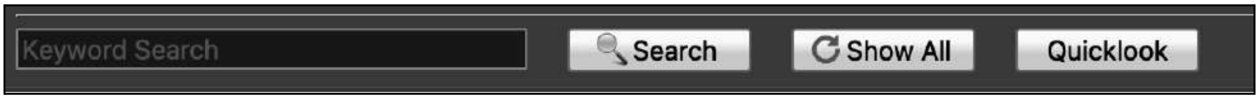


To narrow the timeline to specific periods of interest:

- **From**:
  ➔ Select the **start date**.
  ➔ RECON ITR will show only records occurring **on or after** this date.
- **To**:
  ➔ Select the **end date**.
  ➔ No records after this date will be displayed.
- **Set**:
  ➔ Click **Set** after choosing your dates to apply the date range filter.

  Note:
  Filtering by date is useful when focusing on events tied to known timeframes (e.g., incident dates, user activity windows).

8.5.4 Record Search



You can further refine results using a **keyword search**.

To perform a keyword search:

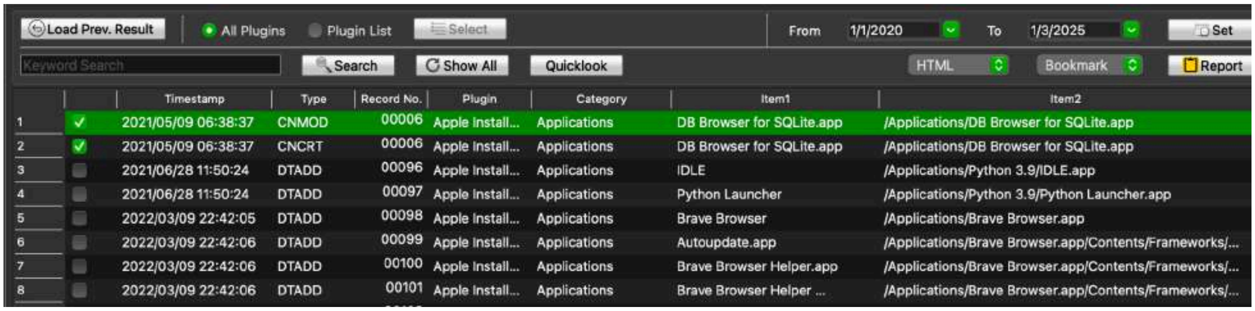
1. Enter the keyword into the **Keyword Search** text box.
2. Click **Search**.

This will search across all visible records within the current date and plugin filters.

Additional Options:

Button	Description
Search	Executes a search on displayed records for the entered keyword.
Show All	Clears all filters and displays all available records.
QuickLook	Previews the selected file or artifact using Apple's native QuickLook, if supported.

8.5.5 Bookmarking



		Timestamp	Type	Record No.	Plugin	Category	Item1	Item2
1	☑	2021/05/09 06:38:37	CNMOD	00006	Apple Install...	Applications	DB Browser for SQLite.app	/Applications/DB Browser for SQLite.app
2	☑	2021/05/09 06:38:37	CNCRT	00006	Apple Install...	Applications	DB Browser for SQLite.app	/Applications/DB Browser for SQLite.app
3	□	2021/06/28 11:50:24	DTADD	00096	Apple Install...	Applications	IDLE	/Applications/Python 3.9/IDLE.app
4	□	2021/06/28 11:50:24	DTADD	00097	Apple Install...	Applications	Python Launcher	/Applications/Python 3.9/Python Launcher.app
5	□	2022/03/09 22:42:05	DTADD	00098	Apple Install...	Applications	Brave Browser	/Applications/Brave Browser.app
6	□	2022/03/09 22:42:06	DTADD	00099	Apple Install...	Applications	Autoupdate.app	/Applications/Brave Browser.app/Contents/Frameworks/...
7	□	2022/03/09 22:42:06	DTADD	00100	Apple Install...	Applications	Brave Browser Helper.app	/Applications/Brave Browser.app/Contents/Frameworks/...
8	□	2022/03/09 22:42:06	DTADD	00101	Apple Install...	Applications	Brave Browser Helper ...	/Applications/Brave Browser.app/Contents/Frameworks/...

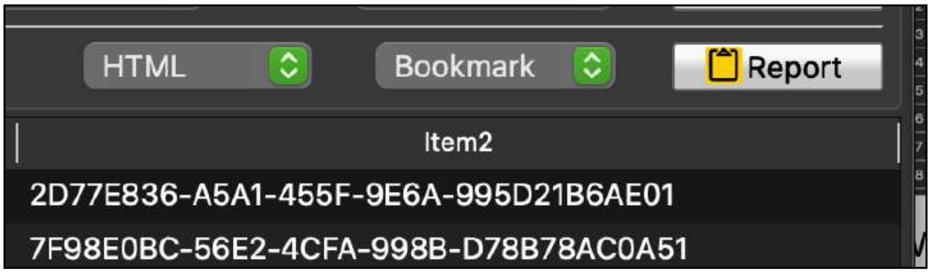
When reviewing Global Timeline results, you can bookmark important records for reporting.

- **To bookmark an individual record**:
  ➔ Click the **checkbox** next to the record.
- **Right-click a record** for additional options:

Option	Description
Bookmark All	Bookmarks all currently shown records.
Remove All Bookmarks	Clears all bookmarks currently set in Global Timeline.
QuickLook	Previews the selected file if it is a supported media file.

> ***Tip:***
> *Bookmarking saves time when generating focused reports based only on key findings.*

8.5.6 Report



Item2

2D77E836-A5A1-455F-9E6A-995D21B6AE01

7F98E0BC-56E2-4CFA-998B-D78B78AC0A51

Reports can be generated from the Global Timeline view based on bookmarked or full results.

To generate a report:

1. Choose the **report file format**:

Format	Description
HTML	Opens in a web browser.
PDF	Portable Document Format, easy for sharing.
CSV	Comma-Separated Value spreadsheet.
XML	Extensible Markup Language for importing into other tools.

2. Choose the **report scope**:

Scope	Description
Bookmark	Includes only bookmarked records.

Full	Includes all records from the Global Timeline view.
Screen Items	Includes only records currently displayed (filtered view).

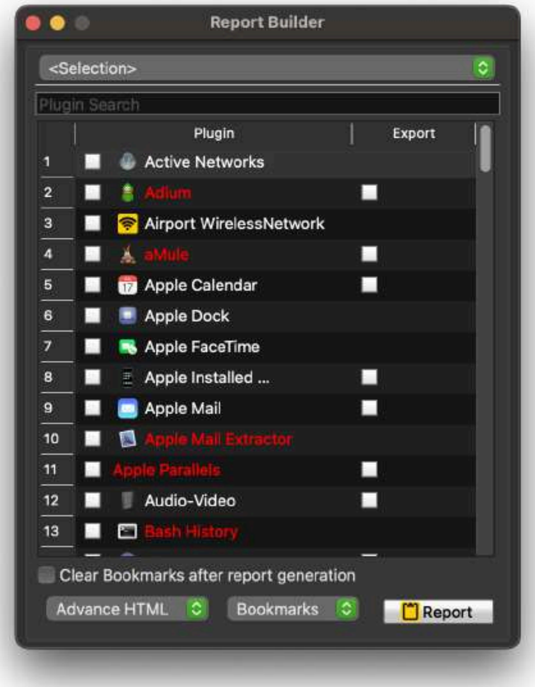
3. Click the **Report** button to generate the report.
    - After report generation, a prompt will ask if you want to **open the report immediately**.
        - Click **Yes** to view now.
        - Click **No** to view it later from the **GlobalTimeline folder** within the RECON ITR case directory.

8.6 Global Reports

The **Global Reports** feature allows you to generate customized forensic reports based on artifacts and files **bookmarked** during Global Search, Global Timeline, or Plugin Result Viewer sessions.

8.6.1 Overview

- To access Global Reports:
    - Click the **Global Reports** button from the triage screen.



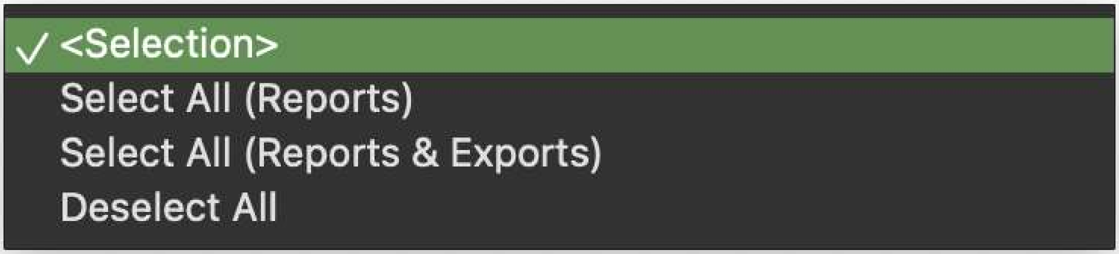
	Plugin	Export
1	□ Active Networks	
2	□ Adium	□
3	□ Airport WirelessNetwork	
4	□ aMule	□
5	□ Apple Calendar	□
6	□ Apple Dock	
7	□ Apple FaceTime	
8	□ Apple Installed ...	□
9	□ Apple Mail	□
10	□ Apple Mail Extractor	
11	□ Apple Parallels	□
12	□ Audio-Video	□
13	□ Bash History	

□ Clear Bookmarks after report generation

This opens the **Report Builder**, where you can:

- Select which plugins and artifacts to include.
- Choose to export associated files.
- Customize the report format and content scope.

8.6.2 Selection Options

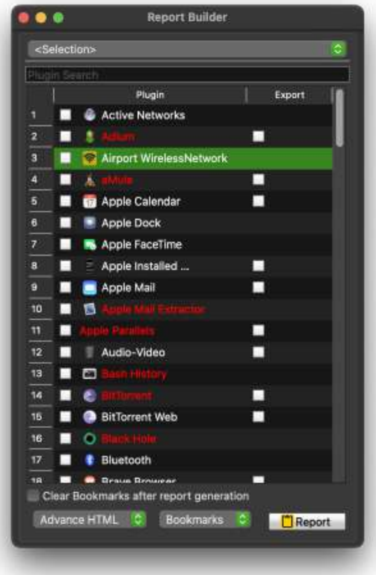


In the Report Builder, you can quickly select which plugins and exports to include using the **Selection Dropdown** options:

Option	**Description**
Select All (Reports)	Adds **all plugins** to the report without exporting associated files.
Select All (Reports & Exports)	Adds **all plugins** and also exports all bookmarked files linked to the artifacts.
Deselect All	Clears all selections for both reporting and file export.

You may also **manually select** individual plugins in the Plugin table:

- The **Plugin** checkbox includes that plugin’s artifacts in the report.
- The **Export** checkbox (available only for plugins with exportable files) includes associated files in the exported data.



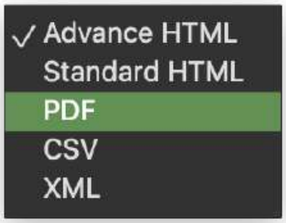
	Plugin	Export
1	□ Active Networks	
2	□ Adium	□
3	□ Airport WirelessNetwork	
4	□ aMule	□
5	□ Apple Calendar	□
6	□ Apple Dock	
7	□ Apple FaceTime	
8	□ Apple Installed ...	□
9	□ Apple Mail	□
10	□ Apple Mail Extractor	
11	□ Apple Parallels	□
12	□ Audio-Video	□
13	□ Bash History	
14	□ BitTorrent	□
15	□ BitTorrent Web	□
16	□ Black Hole	
17	□ Bluetooth	
18	□ Brave Browser	□

□ Clear Bookmarks after report generation

Tip:
Manually selecting plugins and exports gives you more control over the scope and size of your final report.

8.6.3 Export Formats

Before generating the report, you can choose the desired report format.



Click the **Advance HTML** dropdown to view available formats:

Format	**Description**
Advance HTML	An enhanced HTML report with additional navigation features, viewable in any web browser.
Standard HTML	A simpler HTML report, also viewable in any web browser.
PDF	A Portable Document Format report, ideal for formal sharing and printing.
CSV	A Comma-Separated Values file, easily opened in spreadsheet software like Excel.
XML	An Extensible Markup Language file for data exchange or import into other forensic tools.

8.6.4 Bookmarking Options

Before generating the final report, select the **scope** of the content to include:

Option	**Description**
Bookmarks	Includes only **bookmarked records** from the selected plugins. ➔ If the **Export** checkbox was selected, only bookmarked files will be exported.
Full Plugin	Includes **all records** from the selected plugins, regardless of bookmark status. ➔ All available files for exportable artifacts will be exported along with the report.

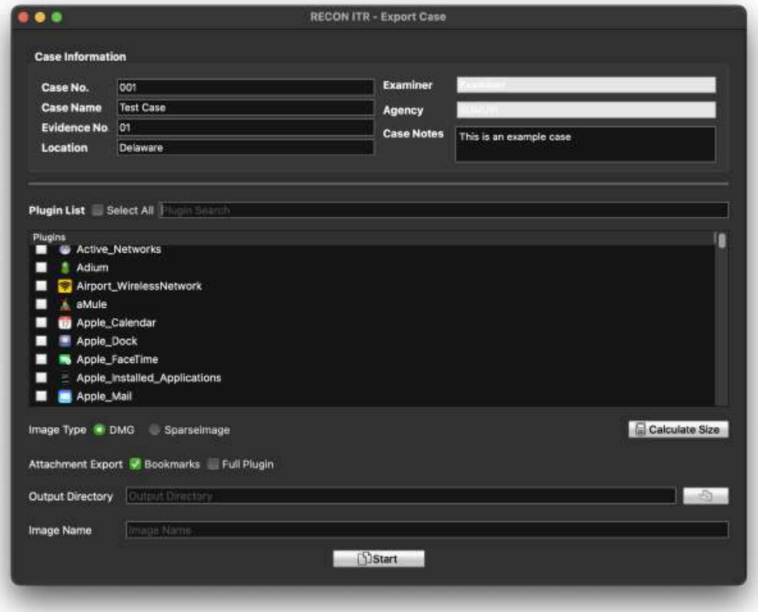
Tip:
*Using the **Bookmarks** option creates a more focused report highlighting only items of interest.*
*Using the **Full Plugin** option creates a complete record of all parsed artifacts.*

8.7 Export Case

The **Export Case** feature allows examiners to export **files found within parsed artifacts** during triage into a forensic image format.

> ***Important:***
> *This is **not** a full forensic image of the entire device.*
> *Only files discovered during triage and selected for export will be included.*

8.7.1 Overview



RECON ITR - Export Case

Case Information

Case No. 001
Case Name Test Case
Evidence No 01
Location Delaware
Case Notes This is an example case

Plugin List □ Select All

Plugins
□ Active_Networks
□ Adium
□ Airport_WirelessNetwork
□ aMule
□ Apple_Calendar
□ Apple_Dock
□ Apple_FaceTime
□ Apple_Installed_Applications
□ Apple_Mail

Image Type ● DMG ○ SparseImage

Attachment Export ☑ Bookmarks □ Full Plugin

- Exporting a case creates an image containing **only the extracted files** from selected plugins during triage.
- This can be useful for preserving specific artifacts without performing a full device acquisition.

> ***Reminder:***
> *Use full forensic imaging procedures if complete evidence preservation is required.*

8.7.2 Case Information

Case Information refers to the details stored in the **Complete.txt** file.

This file is created at the end of the export process and includes:

- Case metadata provided during initial setup.
- Details about the artifacts exported.
- Summary of selected export options.

8.7.3 Exporting a Case

To export a triage case:

1. **Select Artifacts to Export**
    - In the **Plugin List** table:
        - Check the box next to each artifact/plugin you wish to include.
        - Or use the **Select All** checkbox to select all available plugins.
2. **Choose Image Type**
    - Select the format for the export image:

Image Type	**Description**
SparseImage	Faster creation using Apple’s dynamic image format. ➔ Best suited for use within macOS environments. ➔ Limited compatibility outside macOS.
DMG	Apple-native Disk Image format. ➔ Slightly slower to create. ➔ Broad compatibility across macOS and forensic tools on other platforms.

3. **Select Export Scope**

- Decide what content to include using the **Attachment Export** options:

Option	**Description**
Bookmarks	Exports only files that were bookmarked during triage.
Full Plugin	Exports all files associated with the selected plugins, regardless of bookmark status.

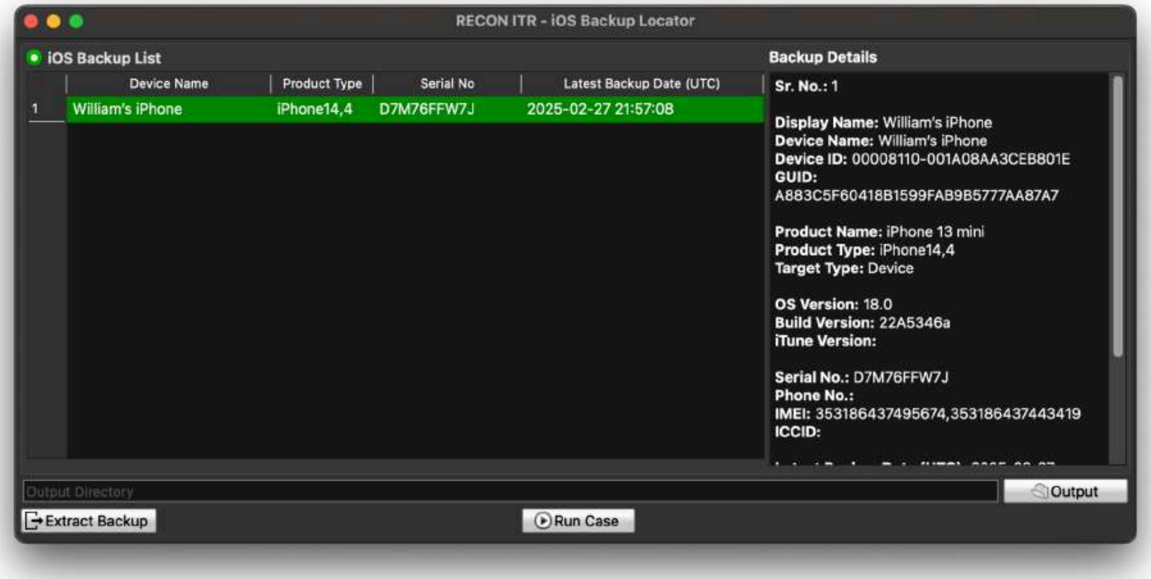
4. **Set Output Details**

- **Output Directory**:
  ➔ Specify the folder where the exported image will be saved.
- **Image Name**:
  ➔ Enter the name to assign to the resulting export image.

5. **Start the Export**

- Review your selections carefully.
- Begin the export process to create the forensic image with the selected artifacts and files.

9 iOS Backup



	Device Name	Product Type	Serial No	Latest Backup Date (UTC)
1	William's iPhone	iPhone14,4	D7M76FFW7J	2025-02-27 21:57:08

Sr. No.: 1

Display Name: William's iPhone
Device Name: William's iPhone
Device ID: 00008110-001A08AA3CEB801E
GUID:
A883C5F60418B1599FAB9B5777AA87A7

Product Name: iPhone 13 mini
Product Type: iPhone14,4
Target Type: Device

OS Version: 18.0
Build Version: 22A5346a
iTune Version:

Serial No.: D7M76FFW7J
Phone No.:
IMEI: 353186437495674,353186437443419
ICCID:

The **iOS Backup** tool built into **RECON ITR** is designed to **locate, acquire, extract, and triage locally stored iOS backups** saved on a Mac.

- To access the iOS Backup tool:
    - Click the **iOS Backup** button from the **RECON ITR splash screen**.

The **iOS Backup Locator** will:

- Search for any iOS backups stored in the user's default backup location: `/MobileSync/Backup`
- Display a **list of available iOS backups** in a table format.
- Show **Backup Details** for the selected backup, including device information such as:
    - Device Name
    - Device Serial Number
    - Backup Date and Time
    - Backup Size

Once a backup is located, RECON ITR offers two main options:

Option	Description
Extract Backup	Copies the iOS backup files to a selected destination for preservation or offline analysis.
Triage Backup	Parses the backup and creates a triage case to review user data, application artifacts, and other forensic evidence contained within the backup.

Important:
Extracting or triaging an iOS backup only processes ***data already stored on the Mac*** *— it does* ***not*** *create a new backup from a connected iOS device.*

9.1 Extracting Backup

Extracting an iOS backup copies the selected backup to a destination of your choice for analysis or preservation.

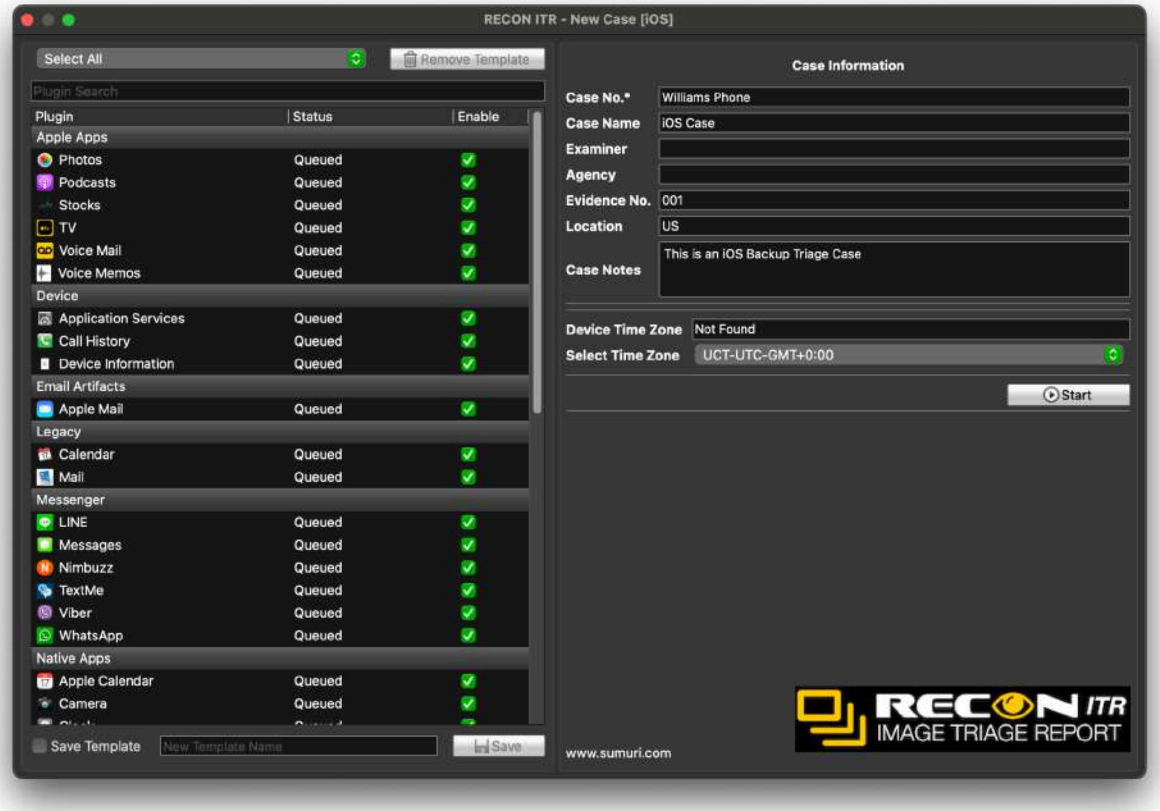
To extract an iOS backup:

1. Select the desired **iOS Backup record** from the iOS Backup Locator table.
2. Click the **Output** button:
    - A Finder window will open.
    - Navigate to the destination folder where you want the backup to be saved.
3. Click **Extract Backup** to start the extraction process.

- After extraction is complete, an **Extraction Completed** window will appear, confirming success.

> ***Note:***
> *Extraction preserves the original backup file structure for later review or triage analysis.*

9.2 Triage the Backup



Plugin	Status	Enable
Apple Apps		
Photos	Queued	☑
Podcasts	Queued	☑
Stocks	Queued	☑
TV	Queued	☑
Voice Mail	Queued	☑
Voice Memos	Queued	☑
Device		
Application Services	Queued	☑
Call History	Queued	☑
Device Information	Queued	☑
Email Artifacts		
Apple Mail	Queued	☑
Legacy		
Calendar	Queued	☑
Mail	Queued	☑
Messenger		
LINE	Queued	☑
Messages	Queued	☑
Nimbuzz	Queued	☑
TextMe	Queued	☑
Viber	Queued	☑
WhatsApp	Queued	☑
Native Apps		
Apple Calendar	Queued	☑
Camera	Queued	☑

Case Information

Case No.*	Williams Phone
Case Name	iOS Case
Examiner	
Agency	
Evidence No.	001
Location	US
Case Notes	This is an iOS Backup Triage Case
Device Time Zone	Not Found
Select Time Zone	UCT-UTC-GMT+0:00

In addition to extraction, you can also **analyze** an iOS backup by creating a **Triage Case** directly from the backup.

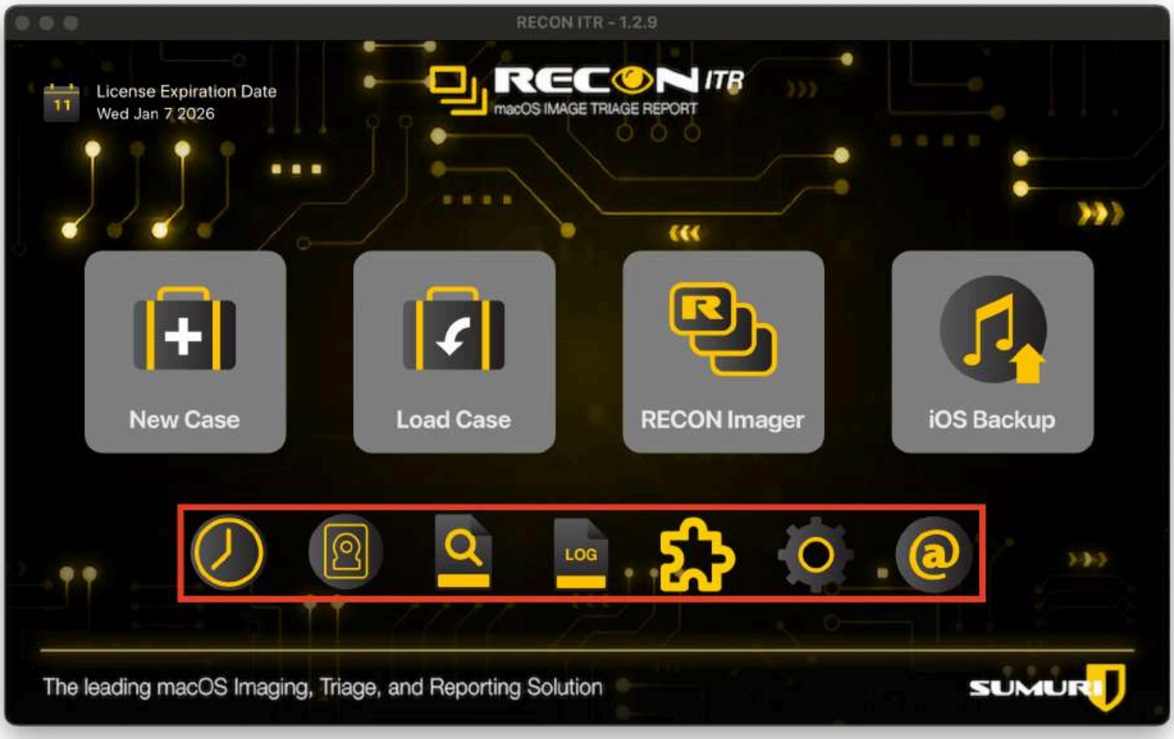
To triage an iOS backup:

1. Select the desired **iOS Backup record** from the iOS Backup Locator table.
2. Click the **Output** button:
    - A Finder window will open.
    - Navigate to the destination folder where you want the triage case to be saved.
3. Click **Run Case**.

- You will then be prompted to **enter Triage Case details** (e.g., Case Number, Examiner Name, etc.).
- Once complete, RECON ITR will begin parsing the backup and generating a triage case.

For additional information on case creation and review, refer to the Live Triage section.

10 Triage Tools



Triage Tools are a set of built-in utilities in **RECON ITR** designed to assist examiners in **quickly finding files of interest** during live triage.

- These tools focus on identifying potential evidence without requiring full imaging.
- Triage Tools can be found at the **bottom of the RECON ITR home screen**.

10.1 File Timeline

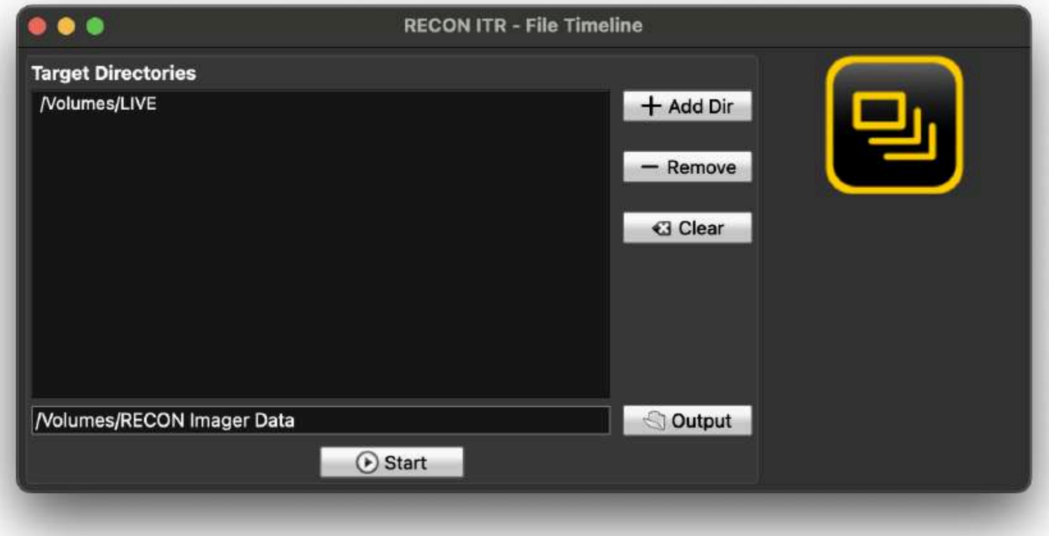
10.1.1 Overview

The **File Timeline** tool in RECON ITR allows examiners to:

- Compare multiple timestamps across files and directories.
- Create an **event-based timeline** of file activity.

This tool is especially useful for reconstructing **user activity** and **event sequences** across different locations on the system.

10.1.2 Selecting Target Directory



Target Directories: /Volumes/LIVE

/Volumes/RECON Imager Data

Target Directories define where file metadata will be pulled from for timeline creation.

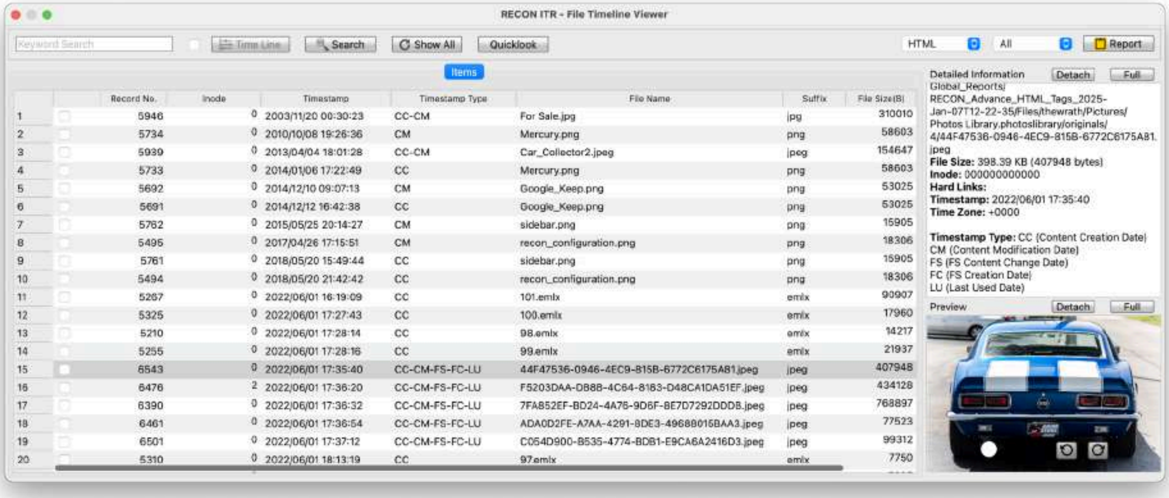
Available Options:

Button	Description
Add Dir	Select a directory from which files will be included in the timeline.
Remove	Remove the currently selected directory from the list.
Clear	Remove all directories from the list.
Output	Choose the destination directory where the generated timeline evidence will be saved.
Start	Begin the timeline generation process based on the selected directories.

Tip:

Selecting smaller, focused directories (e.g., User Documents, Downloads) can speed up timeline generation and provide more relevant results.

10.1.3 Timeline Viewer



		Record No.	Inode	Timestamp	Timestamp Type	File Name	Suffix	File Size(B)
1	□	5946	0	2003/11/20 00:30:23	CC-CM	For Sale.jpg	jpg	310010
2	□	5734	0	2010/10/08 19:26:36	CM	Mercury.png	png	58603
3	□	5939	0	2013/04/04 18:01:28	CC-CM	Car_Collector2.jpeg	jpeg	154647
4	□	5733	0	2014/01/06 17:22:49	CC	Mercury.png	png	58603
5	□	5692	0	2014/12/10 09:07:13	CM	Google_Keep.png	png	53025
6	□	5691	0	2014/12/12 16:42:38	CC	Google_Keep.png	png	53025
7	□	5762	0	2015/05/25 20:14:27	CM	sidebar.png	png	15905
8	□	5495	0	2017/04/26 17:15:51	CM	recon_configuration.png	png	18306
9	□	5761	0	2018/05/20 15:49:44	CC	sidebar.png	png	15905
10	□	5494	0	2018/05/20 21:42:42	CC	recon_configuration.png	png	18306
11	□	5267	0	2022/06/01 16:19:09	CC	101.emlx	emlx	90907
12	□	5325	0	2022/06/01 17:27:43	CC	100.emlx	emlx	17960
13	□	5210	0	2022/06/01 17:28:14	CC	98.emlx	emlx	14217
14	□	5255	0	2022/06/01 17:28:16	CC	99.emlx	emlx	21937
15	□	6543	0	2022/06/01 17:35:40	CC-CM-FS-FC-LU	44F47536-0946-4EC9-815B-6772C6175A81.jpeg	jpeg	407948
16	□	6476	2	2022/06/01 17:36:20	CC-CM-FS-FC-LU	F5203DAA-D888-4C64-8183-D48CA1DA51EF.jpeg	jpeg	434128
17	□	6390	0	2022/06/01 17:36:32	CC-CM-FS-FC-LU	7FA852EF-BD24-4A76-9D6F-8E7D7292DDD8.jpeg	jpeg	768897
18	□	6461	0	2022/06/01 17:36:54	CC-CM-FS-FC-LU	ADA0D2FE-A7AA-4291-8DE3-49688015BAA3.jpeg	jpeg	77523
19	□	6501	0	2022/06/01 17:37:12	CC-CM-FS-FC-LU	C054D900-B535-4774-BDB1-E9CA6A2416D3.jpeg	jpeg	99312
20	□	5310	0	2022/06/01 18:13:19	CC	97.emlx	emlx	7750

Detailed Information

Global_Reports/
RECON_Advance_HTML_Tags_2025-Jan-07T12-22-35/Files/thewrath/Pictures/Photos Library.photoslibrary/originals/4/44F47536-0946-4EC9-815B-6772C6175A81.jpeg
File Size: 398.39 KB (407948 bytes)
Inode: 000000000000
Hard Links:
Timestamp: 2022/06/01 17:35:40
Time Zone: +0000

Timestamp Type: CC (Content Creation Date)
CM (Content Modification Date)
FS (FS Content Change Date)
FC (FS Creation Date)
LU (Last Used Date)

Once timeline generation completes, the **Timeline Viewer** will open.

Key columns displayed include:

Column	Description
Record No	The UUID assigned by RECON ITR to each record.
Inode	File system inode number associated with the file.
Timestamp	The date and time of the recorded event.
Timestamp Type	The event type based on Apple Extended Metadata: • CC: Content Creation • CM: Content Modification • FS: File System Content Change • FC: File System Creation • LU: Last Used
File Name	The name of the file.
Suffix	The file's extension (e.g., .docx, .jpg).
File Size (B)	File size in bytes.

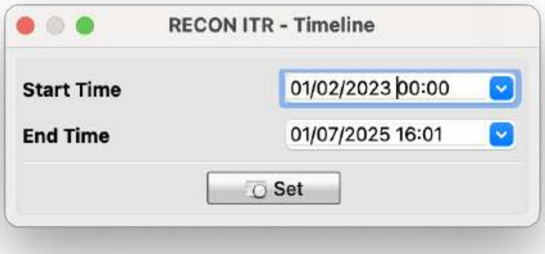
Other Viewer Features:

- **Detailed Information Panel** (right side):
  ➔ Displays detailed metadata for the selected record.
- **QuickLook Preview** (bottom right):
  ➔ If the file is a media file, a native QuickLook preview will be shown.
- **Detach View**:
  ➔ Opens the Detailed Information panel in a separate window for easier review.

Bookmarking Records:

- You can mark records of interest by checking the box at the beginning of the row.
- Bookmarked records can later be included in generated reports for easier reference.

10.1.4 Timeline Options



Start Time 01/02/2023 00:00

End Time 01/07/2025 16:01

To narrow focus to specific events, you can **enable Timeline Filtering**:

- **Start Time**:
  ➔ Show only events that occurred **on or after** this selected date and time.
- **End Time**:
  ➔ Show only events that occurred **on or before** this selected date and time.

Default Settings:

- **Start Time**: Earliest possible date in dataset.
- **End Time**: Current system date and time.

To apply a filter:

1. Enable the **Timeline** checkbox.
2. Set your desired **Start Time** and **End Time**.
3. Click **Set**.

The Timeline Viewer will update to display only the records within the selected range.

10.1.5 Generating a Report

To create a report from your timeline findings:

1. **Select the Report Format**
   Use the dropdown menu to choose a file format:

Format	Description
HTML	Opens in a standard web browser.
PDF	Portable Document Format for easy sharing or printing.
CSV	Comma-Separated Value file for spreadsheets.
XML	Extensible Markup Language for importing into forensic tools.

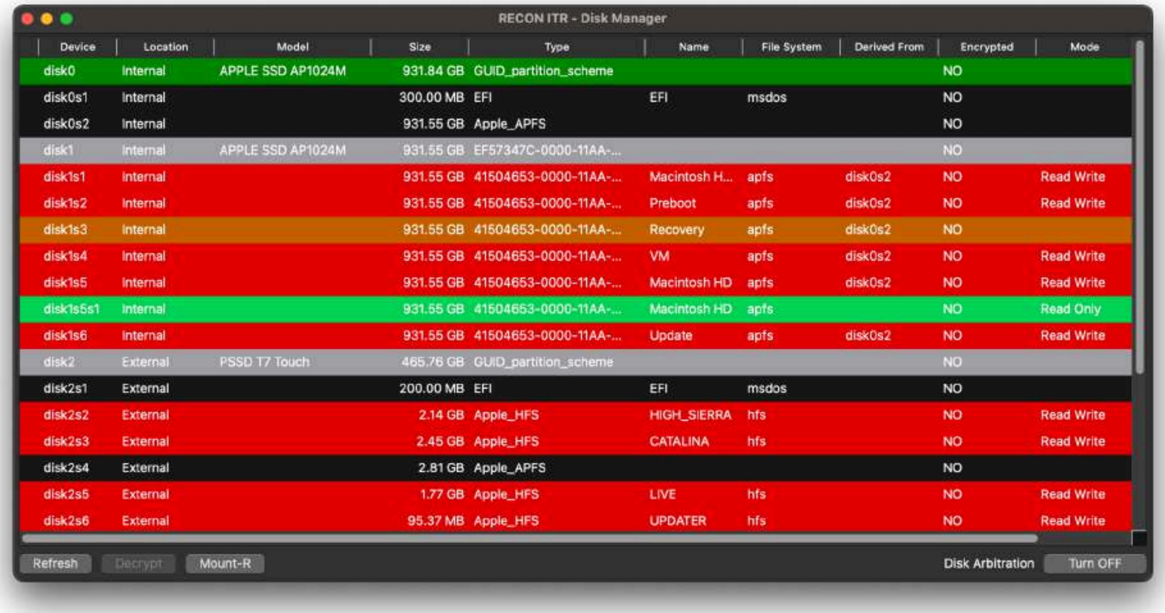
2. **Choose the Report Source**
   Define which records to include:

Option	Description
All	Includes all timestamps and records in the timeline.
Bookmarks	Includes only bookmarked records.
Screen Items	Includes only currently displayed records, factoring in any filters.

3. **Generate the Report**
   - Click **Report**.
   - Confirm by selecting **YES** if you would like to open the report immediately.

Note:
*Reports are saved inside a new directory located within the **Output** folder selected during timeline setup.*

10.2 Disk Manager



RECON ITR - Disk Manager

Device	Location	Model	Size	Type	Name	File System	Derived From	Encrypted	Mode
disk0	Internal	APPLE SSD AP1024M	931.84 GB	GUID_partition_scheme				NO	
disk0s1	Internal		300.00 MB	EFI	EFI	msdos		NO	
disk0s2	Internal		931.55 GB	Apple_APFS				NO	
disk1	Internal	APPLE SSD AP1024M	931.55 GB	EF57347C-0000-11AA-...				NO	
disk1s1	Internal		931.55 GB	41504653-0000-11AA-...	Macintosh H...	apfs	disk0s2	NO	Read Write
disk1s2	Internal		931.55 GB	41504653-0000-11AA-...	Preboot	apfs	disk0s2	NO	Read Write
disk1s3	Internal		931.55 GB	41504653-0000-11AA-...	Recovery	apfs	disk0s2	NO	
disk1s4	Internal		931.55 GB	41504653-0000-11AA-...	VM	apfs	disk0s2	NO	Read Write
disk1s5	Internal		931.55 GB	41504653-0000-11AA-...	Macintosh HD	apfs	disk0s2	NO	Read Write
disk1s5s1	Internal		931.55 GB	41504653-0000-11AA-...	Macintosh HD	apfs		NO	Read Only
disk1s6	Internal		931.55 GB	41504653-0000-11AA-...	Update	apfs	disk0s2	NO	Read Write
disk2	External	PSSD T7 Touch	465.76 GB	GUID_partition_scheme				NO	
disk2s1	External		200.00 MB	EFI	EFI	msdos		NO	
disk2s2	External		2.14 GB	Apple_HFS	HIGH_SIERRA	hfs		NO	Read Write
disk2s3	External		2.45 GB	Apple_HFS	CATALINA	hfs		NO	Read Write
disk2s4	External		2.81 GB	Apple_APFS				NO	
disk2s5	External		1.77 GB	Apple_HFS	LIVE	hfs		NO	Read Write
disk2s6	External		95.37 MB	Apple_HFS	UPDATER	hfs		NO	Read Write

The **Disk Manager** provides an overview of all disks currently connected to the system and allows examiners to **manually manage disk mounting** using **Disk Arbitration**.

Manual disk control is critical during forensic triage to:

- Prevent macOS from automatically mounting and altering connected evidence disks.
- Ensure disks can be mounted safely as **read-only** when needed.

Column Descriptions

Each connected disk and partition is listed with the following details:

Column	Description
Device	Identifies the disk and partition (e.g., `disk0s2`).
Location	Indicates whether the drive is **internal** or **external**.
Model	Lists the hardware model of the physical drive.
Size	Displays the size of the disk or partition.

Type	Shows the disk or volume type.
Name	Displays the volume name (e.g., "Macintosh HD").
File System	Indicates the file system format (e.g., APFS, HFS+).
Derived From	Identifies parent disks for virtualized or synthesized volumes.
Encrypted	Shows if the volume is encrypted (**YES** for active encryption like FileVault, **NO** for unencrypted).
Mode	Displays the disk's current mount status (e.g., **Read-Only** or **Read-Write**).

Color Scheme for Disk Identification

RECON ITR uses color coding to visually distinguish disk types and statuses:

Color	**Meaning**
Grey	Parent disk (e.g., `disk0`).
Green	Mounted **Read-Only** (e.g., `disk1s5s1`).
Red	Mounted **Read-Write**.
Orange	Apple Core Storage Logical Volume Family.
Yellow	Mounted Fusion Disk.
Light Brown	APFS Partitions.
Olive Green	APFS FileVault Decrypted Volumes.

Tip:
Always verify disk status (especially Read-Only vs Read-Write) before interacting with potential evidence drives.

10.2.1 Disk Arbitration (Live)

Disk Arbitration allows manual control of how external drives are mounted when connected to the system.

- To activate Disk Arbitration:
  - Click the **Disk Arbitration** button until it displays **TURN ON**.

When Disk Arbitration is enabled:

- **Automatic mounting is disabled**.
- Drives must be manually mounted through RECON ITR, providing better control and minimizing risk of evidence alteration.

10.2.1.1 Disk Management Options

Option	Description
Refresh	Updates the Disk Manager table to display the latest connected disks and partitions.
Decrypt	Allows decryption of an APFS volume by entering a password (e.g., FileVault decryption).
Mount-R	Manually mounts a selected disk or volume in Read-Only mode to protect its contents.

Important:

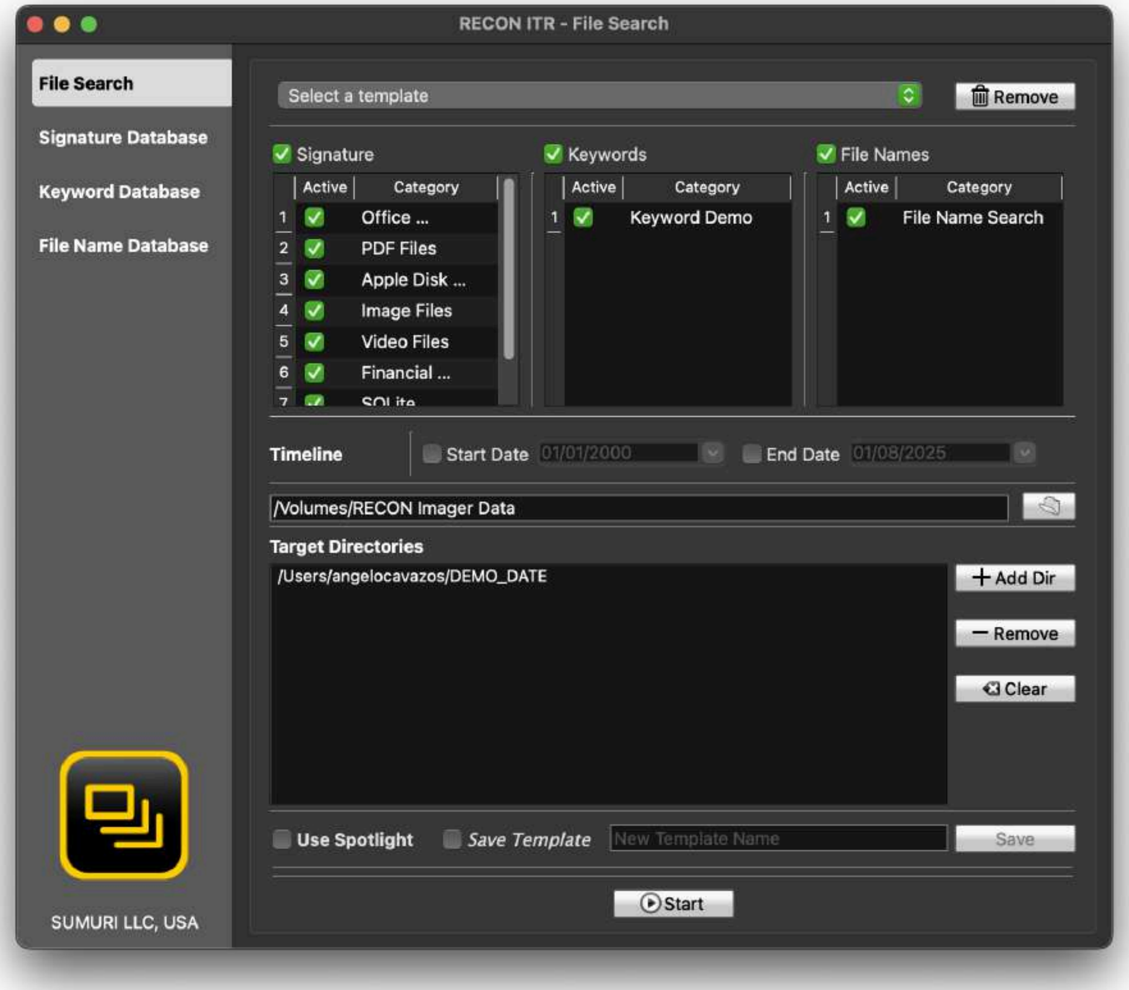
Always verify that sensitive evidence volumes are mounted Read-Only before performing any forensic activities.

10.3 File Search

The **File Search** feature allows examiners to scan directories for files that meet **specific search criteria**. Identified files can then be reviewed, bookmarked, exported, and included in a customizable report. Three types of search criteria are available:

Criteria	Description
Signature	Searches for files based on their file signature or header.
Keywords	Finds files containing specific keywords.
File Names	Locates files based on file names or extensions

10.3.1 Overview



☑ Signature

	Active	Category
1	☑	Office ...
2	☑	PDF Files
3	☑	Apple Disk ...
4	☑	Image Files
5	☑	Video Files
6	☑	Financial ...
7	☑	SQLite

☑ Keywords

	Active	Category
1	☑	Keyword Demo

☑ File Names

	Active	Category
1	☑	File Name Search

Timeline □ Start Date 01/01/2000 □ End Date 01/08/2025

/Volumes/RECON Imager Data

Target Directories

/Users/angelocavazos/DEMO_DATE

□ Use Spotlight □ *Save Template* New Template Name

Enabling Search Criteria:

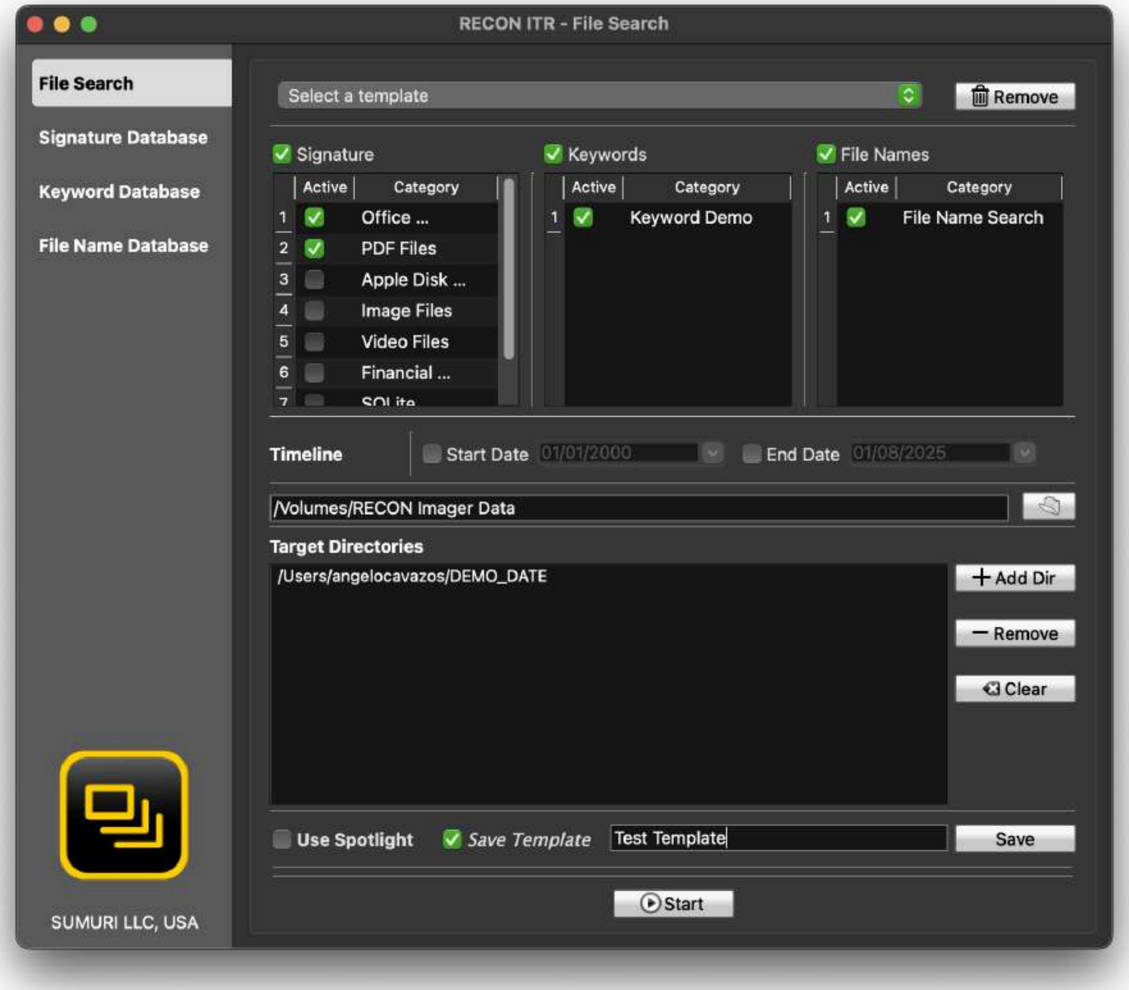
- Check the box next to the search type you want to use (**Signature**, **Keywords**, or **File Names**).
- Within the enabled criteria, activate specific **categories** by checking the box under the **Active** column.

Search Logic:

- If multiple criteria are enabled, RECON ITR performs an **OR search**.
- A file only needs to satisfy **one** selected criterion to appear in the results.

> ***Tip:***
> *You can fine-tune or broaden search parameters by enabling or disabling specific criteria and categories.*

10.3.2 Creating A Template



☑ Signature

	Active	Category
1	☑	Office ...
2	☑	PDF Files
3	☐	Apple Disk ...
4	☐	Image Files
5	☐	Video Files
6	☐	Financial ...
7	☐	SQLite

☑ Keywords

	Active	Category
1	☑	Keyword Demo

☑ File Names

	Active	Category
1	☑	File Name Search

Timeline ☐ Start Date 01/01/2000 ☐ End Date 01/08/2025

/Volumes/RECON Imager Data

Target Directories

/Users/angelocavazos/DEMO_DATE

☐ Use Spotlight ☑ *Save Template* Test Template

Templates allow you to **save sets of search criteria** for reuse across multiple cases.

To create a template:

1. Select the criteria you want to include.
2. Check the **Save Template** box.
3. Enter a template name in the text box.
4. Click **Save**.

- Saved templates are stored locally and can be loaded later through the **Select a Template** dropdown menu.

- Using templates ensures **consistency and efficiency** when searching across multiple devices.

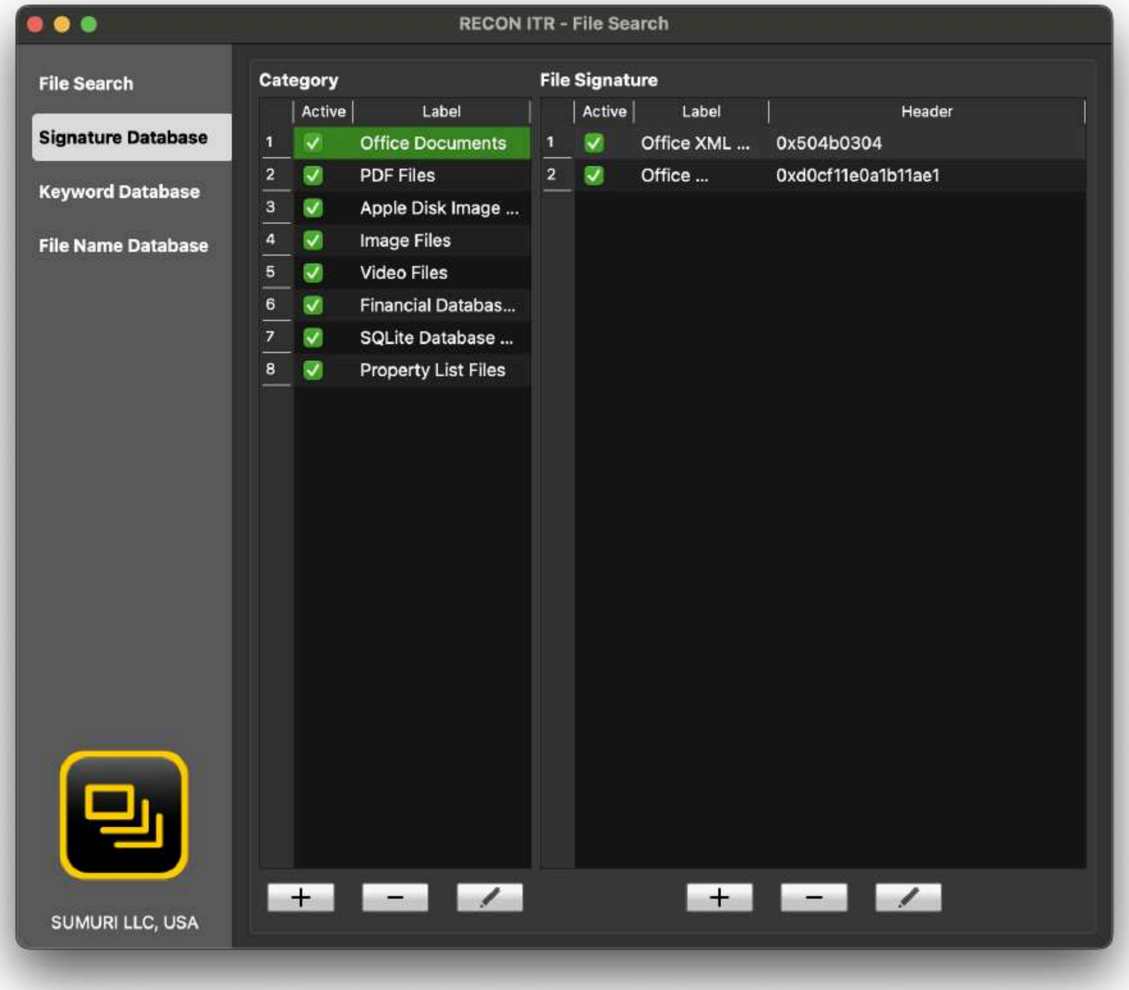
10.3.3 File Search Options

The **File Search** window provides several additional options:

Option	**Description**
Start Date	Set the earliest "Date Added" for files to include.
End Date	Set the latest "Date Added" for files to include.
Destination Directory	Choose where the case data and reports will be saved.
Target Directory	Select which directories will be searched.
Use Spotlight	Utilize macOS Spotlight indexing for faster searches (optional).
Add Dir	Add a directory to the Target Directories list.
Remove	Remove the selected directory from the list.
Clear	Clear all directories from the list.
Start	Begin the File Search based on the selected criteria and options.

> ***Note:***
> *Using Spotlight can make searches faster but may miss some non-indexed files.*

10.3.4 Signature Database



Category

	Active	Label
1	✓	Office Documents
2	✓	PDF Files
3	✓	Apple Disk Image ...
4	✓	Image Files
5	✓	Video Files
6	✓	Financial Databas...
7	✓	SQLite Database ...
8	✓	Property List Files

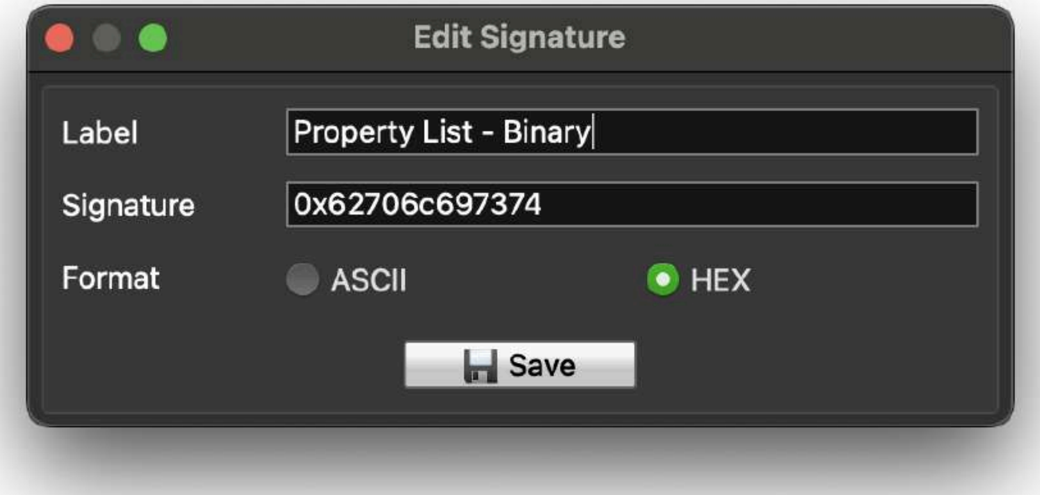
File Signature

	Active	Label	Header
1	✓	Office XML ...	0x504b0304
2	✓	Office ...	0xd0cf11e0a1b11ae1

The **Signature Database** allows you to customize file signature searches.

Category Management:

Option	Description
(+) Symbol	Create a new signature category.
(-) Symbol	Remove the selected category.
Pencil Icon	Edit the category name.



Edit Signature

Label: Property List - Binary

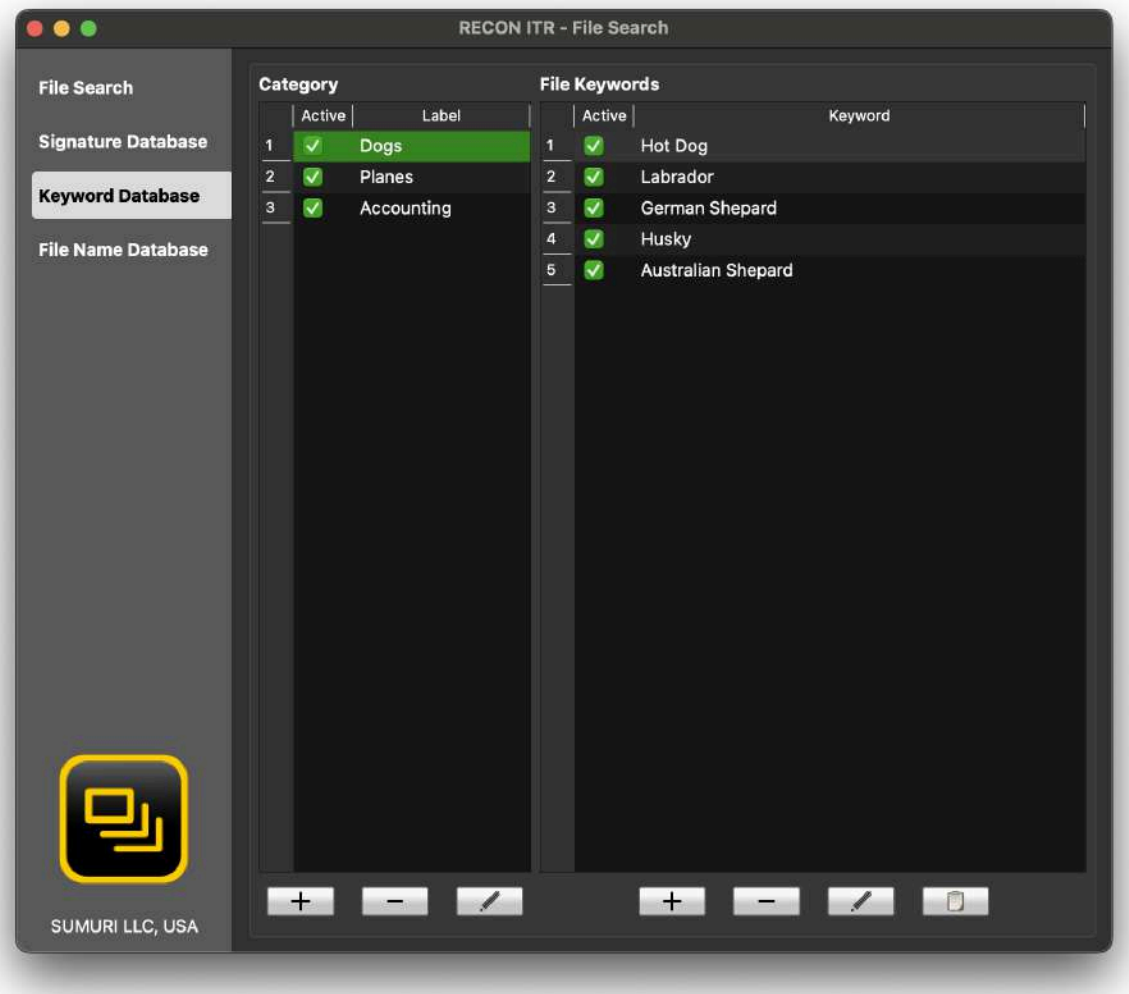
Signature: 0x62706c697374

Format: ○ ASCII ● HEX

Adding Signatures within a Category:

Option	Description
(+) Symbol	Add a new file signature to the category.
Label	Set the display name for the signature.
Signature	Enter the file header or magic number.
Format	Specify the format for header matching.
(-) Symbol	Remove the selected signature.
Pencil Icon	Edit the properties of the selected signature.

10.3.5 Keyword Database



Category

	Active	Label
1	☑	Dogs
2	☑	Planes
3	☑	Accounting

File Keywords

	Active	Keyword
1	☑	Hot Dog
2	☑	Labrador
3	☑	German Shepard
4	☑	Husky
5	☑	Australian Shepard

The **Keyword Database** allows you to manage keyword lists.

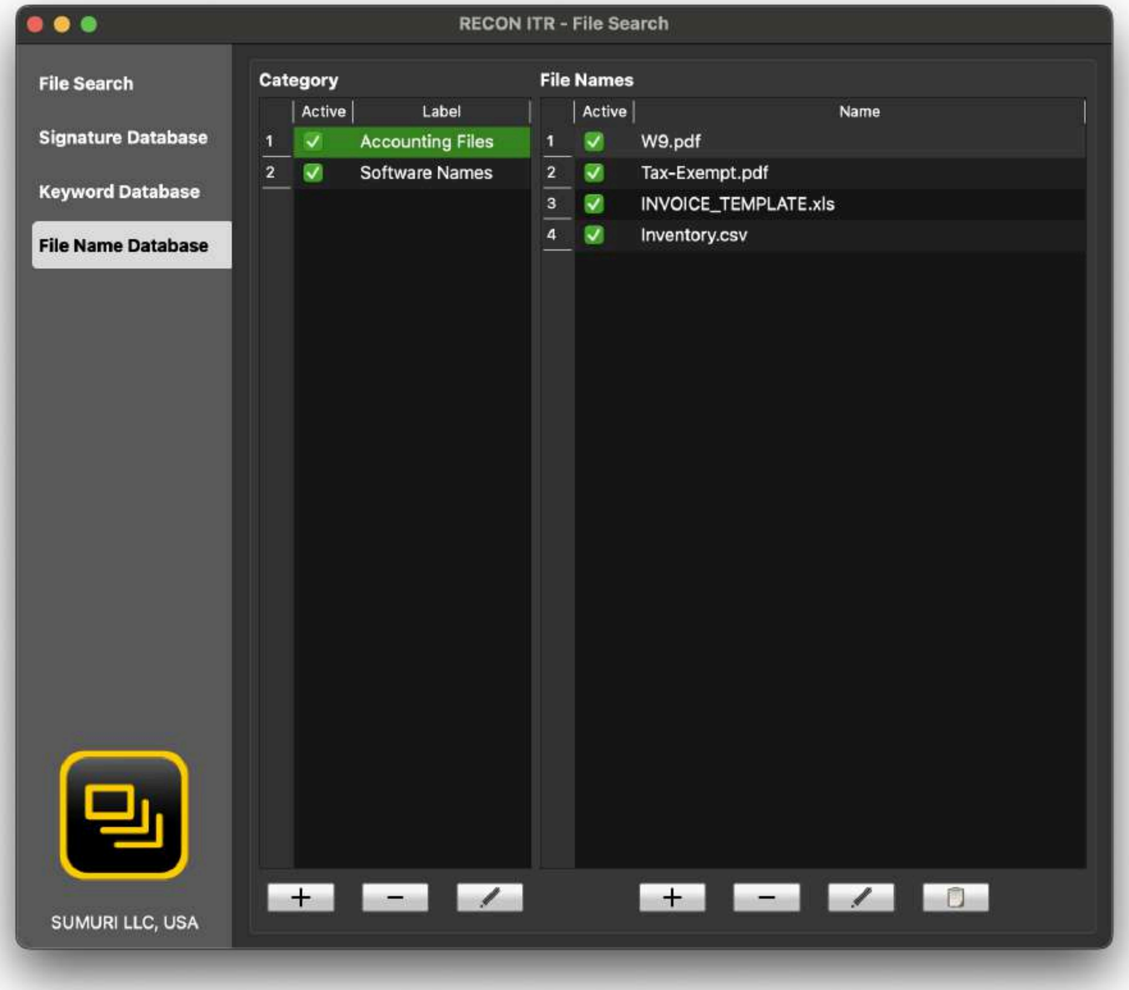
Category Management:

Option	Description
(+) Symbol	Create a new keyword category.
(-) Symbol	Remove the selected category.
Pencil Icon	Rename an existing category.

Keyword Management:

Option	Description
(+) Symbol	Add a new keyword.
(-) Symbol	Remove the selected keyword.
Pencil Icon	Edit the selected keyword.
Paste Icon	Paste text from clipboard and split into multiple keywords based on new lines.

10.3.6 File Name Database



Category

	Active	Label
1	✓	Accounting Files
2	✓	Software Names

File Names

	Active	Name
1	✓	W9.pdf
2	✓	Tax-Exempt.pdf
3	✓	INVOICE_TEMPLATE.xls
4	✓	Inventory.csv

The **File Name Database** allows you to manage lists of file names for targeted searches.

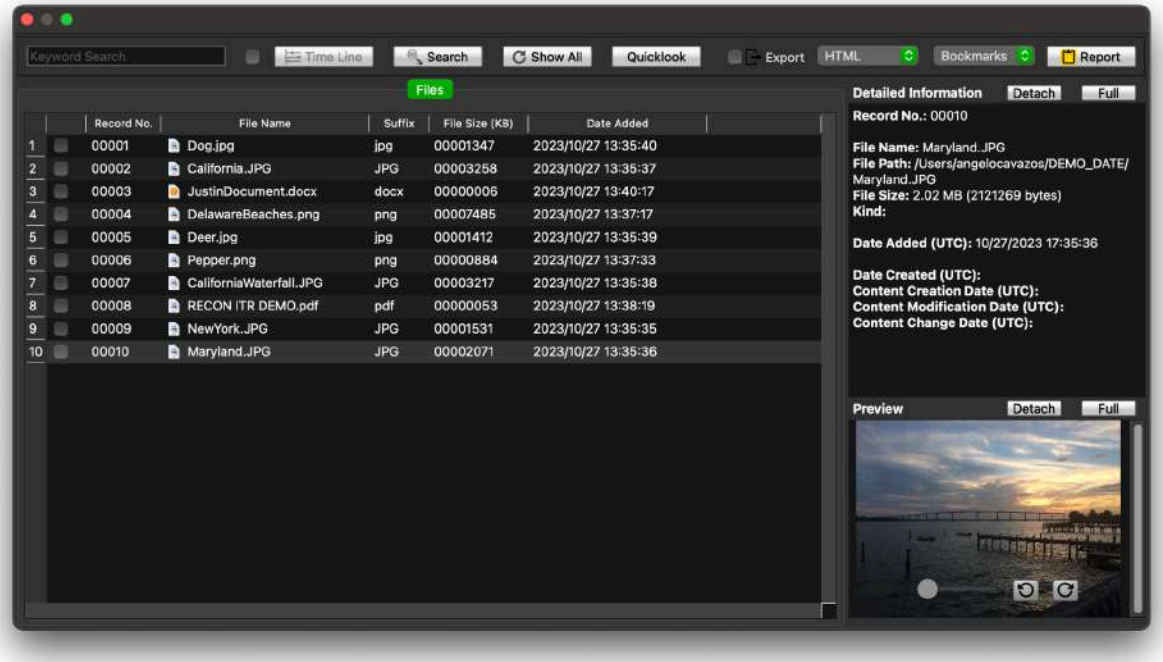
Category Management:

Option	**Description**
(+) Symbol	Create a new file name category.
(-) Symbol	Remove the selected category.
Pencil Icon	Rename an existing category.

File Name Management:

Option	**Description**
(+) Symbol	Add a new file name.
(-) Symbol	Remove the selected file name.
Pencil Icon	Edit the selected file name.
Paste Icon	Paste multiple file names from clipboard text (split by new lines).

10.3.7 Reviewing Results



		Record No.	File Name	Suffix	File Size (KB)	Date Added
1		00001	Dog.jpg	jpg	00001347	2023/10/27 13:35:40
2		00002	California.JPG	JPG	00003258	2023/10/27 13:35:37
3		00003	JustinDocument.docx	docx	00000006	2023/10/27 13:40:17
4		00004	DelawareBeaches.png	png	00007485	2023/10/27 13:37:17
5		00005	Deer.jpg	jpg	00001412	2023/10/27 13:35:39
6		00006	Pepper.png	png	00000884	2023/10/27 13:37:33
7		00007	CaliforniaWaterfall.JPG	JPG	00003217	2023/10/27 13:35:38
8		00008	RECON ITR DEMO.pdf	pdf	00000053	2023/10/27 13:38:19
9		00009	NewYork.JPG	JPG	00001531	2023/10/27 13:35:35
10		00010	Maryland.JPG	JPG	00002071	2023/10/27 13:35:36

Detailed Information

Record No.: 00010

File Name: Maryland.JPG
File Path: /Users/angelocavazos/DEMO_DATE/Maryland.JPG
File Size: 2.02 MB (2121269 bytes)
Kind:

Date Added (UTC): 10/27/2023 17:35:36

Date Created (UTC):
Content Creation Date (UTC):
Content Modification Date (UTC):
Content Change Date (UTC):

After the File Search completes, the **Results Window** will appear showing matched files.

Results Columns:

Column	Description
Record No.	Unique UUID assigned to each file.
File Name	Name of the located file.
Suffix	File extension (e.g., `.jpg`, `.pdf`).
File Size (KB)	File size in kilobytes.
Date Added	UTC timestamp showing when the file was added to the directory.

Record Interaction Options:

- **Time Line**:
  ➔ Filter results based on Date Added.
- **Search**:
  ➔ Search within displayed results using a keyword.

- **Show All**:
  ➔ Clear all filters to view all located files.
- **QuickLook**:
  ➔ Preview media files directly using Apple's QuickLook.

Bookmarking:

- Click the checkbox next to a record to bookmark it.
- Bookmarked files are easily included when generating detailed reports.

10.3.7.1 Generating the Report

After reviewing and bookmarking your results:

1. Export Files (Optional)

- Check the **Export** box if you want to save identified files along with the report.

2. Select Report Format

Format	Description
HTML	Standard web browser report.
PDF	Formal, portable document format.
CSV	Spreadsheet-friendly format for data sorting.
XML	Structured data format for import into other tools.

3. Select Report Content

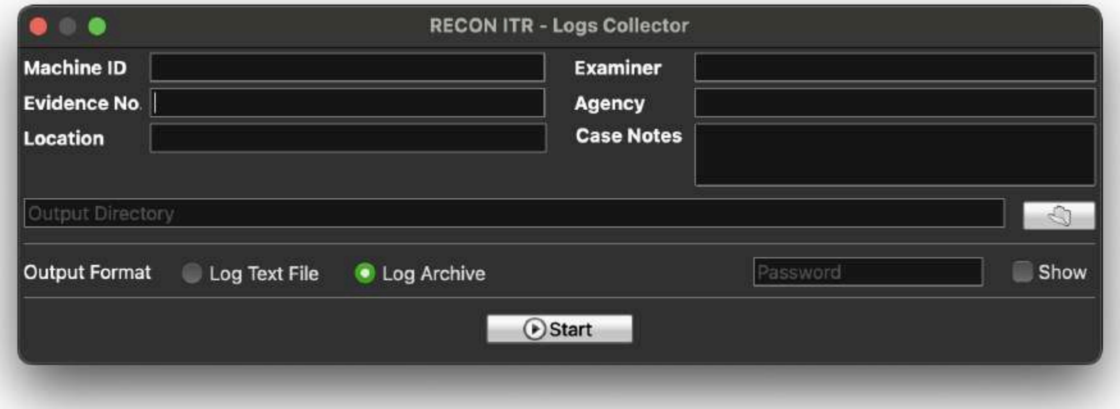
Option	Description
Bookmarks	Includes only bookmarked items.
Full	Includes all search results.
Screen Items	Includes only currently displayed items (after any filters applied).

4. Generate the Report

- Click **Report**.
- Confirm by clicking **YES** if you want to open the report immediately.

The final report and any exported files are saved within the specified destination directory.

10.4 Log Collect



The **Log Collect** tool in RECON ITR allows you to capture Unified Logs from the Mac where RECON ITR is currently running. Unified Logs provide detailed, timestamped records of system activity, application behavior, and security events, making them a valuable source of forensic information.

Log Collection Options

When collecting logs, the following fields and settings are available:

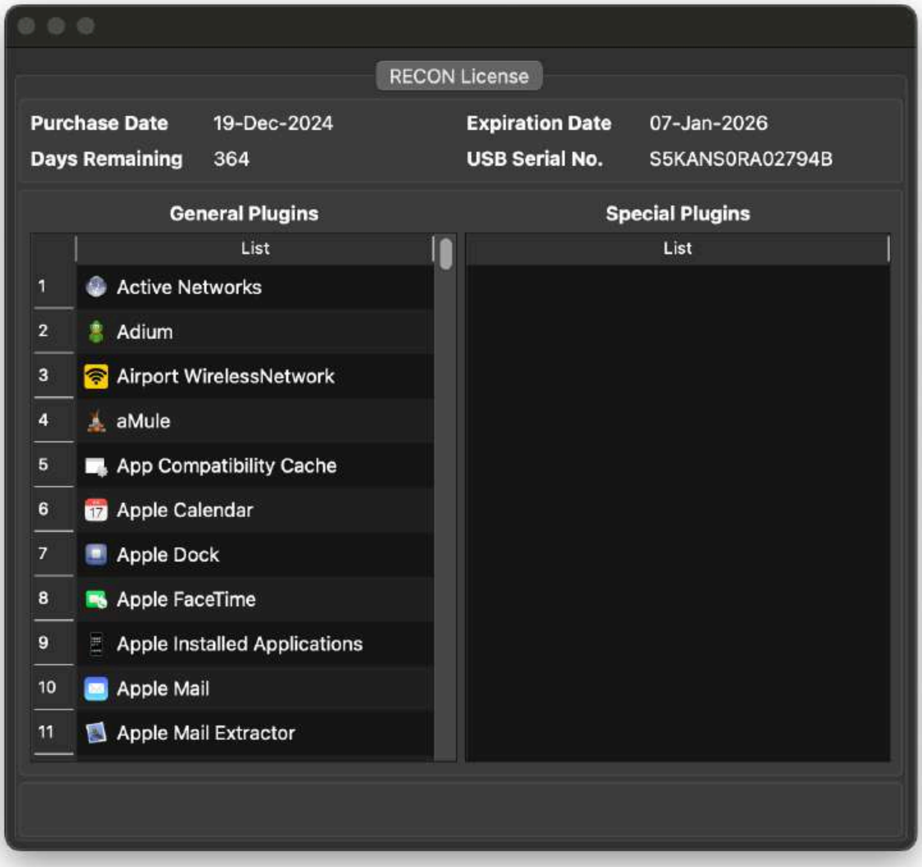
Field	Description
Machine ID *(Required)*	A required field used to identify the device being examined.
Evidence No *(Optional)*	An optional field for entering an associated evidence number.
Location *(Optional)*	An optional field for recording the device's location at the time of examination.
Examiner	Auto-populated from the Configuration tab. Identifies the examiner performing the collection.
Agency	Auto-populated from the Configuration tab. Identifies the agency performing the examination.

Case Notes*(Optional)*	An optional field for entering any additional relevant notes.
Output Directory	Select the destination where the collected logs will be saved.
Output Format	Choose the desired format for the collected logs:
➔ Log Text File	Collects logs as a standard `.txt` file. **No admin password required**.
➔ Log Archive	Collects logs in Apple's native `.logarchive` format, preserving full metadata and structure. **Requires the admin password** of the currently logged-in user.
Password	Enter the **admin password** only if collecting logs in **logarchive format**. (Not required for text file collection.)

Important:

- ***Logarchive format*** *provides a* ***more complete and structured forensic log set*** *but requires administrator credentials.*
- ***Text file output*** *is a simpler option that does* ***not require admin privileges****, but some system-level log detail may be lost.*

10.5 Plugins Viewer



Purchase Date 19-Dec-2024
Days Remaining 364
Expiration Date 07-Jan-2026
USB Serial No. S5KANS0RA02794B

	List
1	Active Networks
2	Adium
3	Airport WirelessNetwork
4	aMule
5	App Compatibility Cache
6	Apple Calendar
7	Apple Dock
8	Apple FaceTime
9	Apple Installed Applications
10	Apple Mail
11	Apple Mail Extractor

The **Plugins Viewer** provides a list of plugins currently supported in your installed version of **RECON ITR**.

Plugins are separated into two categories:

Category	Description
General Plugins	Default plugins included with all versions of RECON ITR.
Specialized Plugins	Custom plugins developed specifically for an agency's request. ➔ If you are interested in specialized plugins, please contact us at **hello@sumuri.com**.

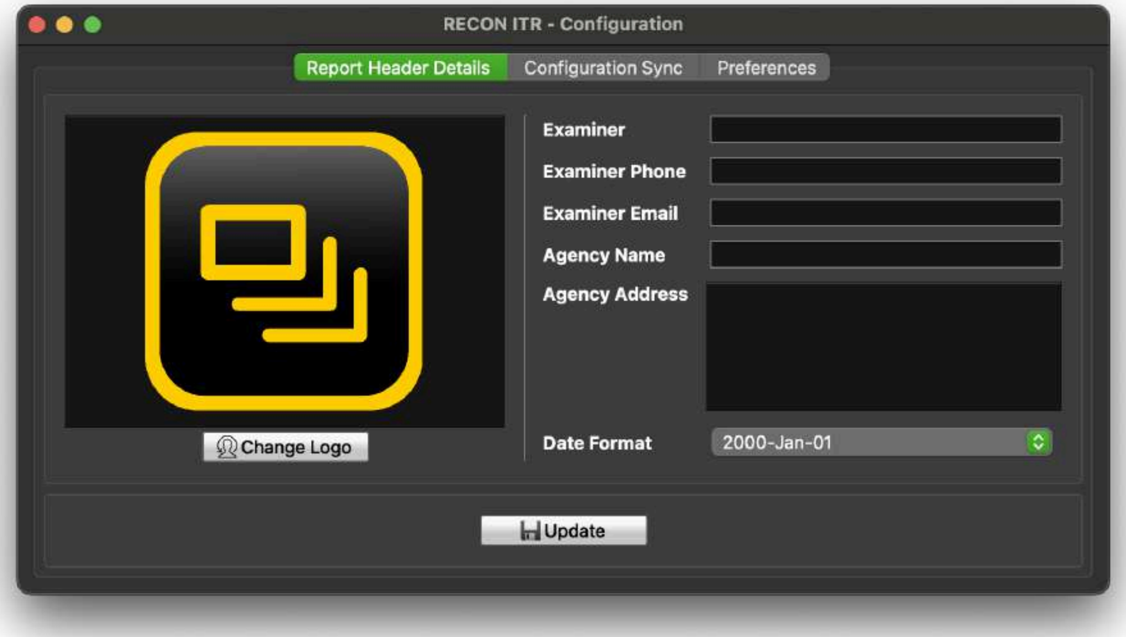
Additional Information Available in Plugins Viewer

The **Plugins Viewer** window also displays **license and system information** related to your RECON ITR installation:

Field	Description
Purchase Date	The date your RECON ITR software license was purchased.
Days Remaining	The number of days left before your license expires.
Expiration Date	The exact date when your current license will expire.
USB Serial Number	The serial number identifies the USB drive or hardware device on which the RECON ITR license is activated.

> ***Tip:***
> *Keeping track of your license expiration ensures you have uninterrupted access to updates and support.*

10.6 Configuration



The **Configuration** section in RECON ITR allows you to **customize agency and examiner details** that will be automatically populated when:

- Setting up triage cases
- Generating reports
- Collecting logs or evidence

Note:
All fields are **optional** and may be left blank if desired.

Available Configuration Fields

Field	Description
Examiner	Name of the examiner conducting triage or analysis.
Examiner Phone	Contact phone number for the examiner.
Examiner Email	Email address of the examiner.

Agency Name	Name of the agency or organization performing the investigation.
Agency Address	Physical address of the agency.

Custom Logo

- You can **replace the default RECON ITR logo** with your agency's specific logo.
- To change the logo:
    1. Click the **Change Logo** button.
    2. Navigate to and select the desired logo file.
    3. The logo file must be in **PNG format**.

Tip:
Using an agency-specific logo can personalize reports for internal or court presentation purposes.

Date Format Configuration

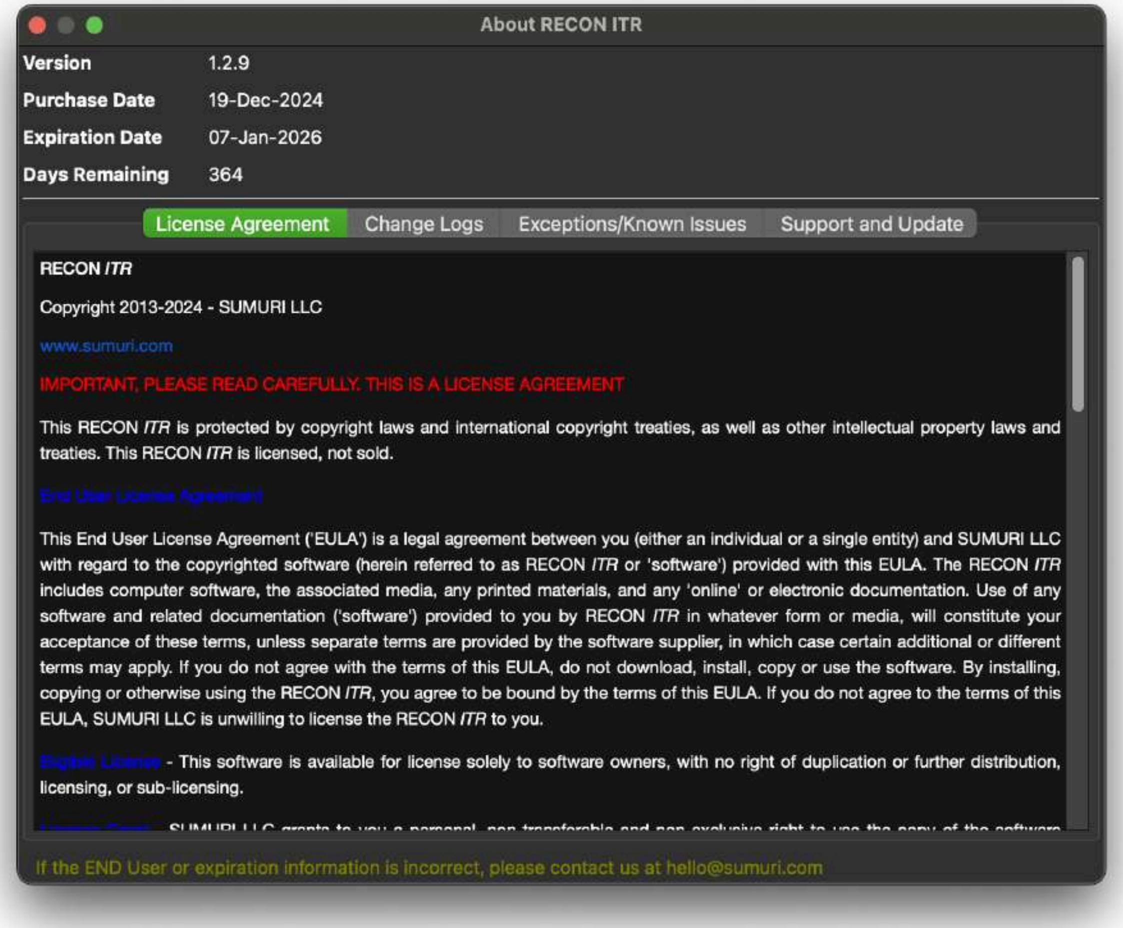
- The **Date Format** option allows you to customize how dates are displayed throughout RECON ITR, including:
    - Triage case data
    - Reports
    - Log collections
- Adjusting the date format ensures compatibility with your agency’s documentation or legal standards.

Tip:
Updating the configuration settings before starting cases improves report consistency and saves time.

10.7 About RECON

The **About RECON** section provides essential information about your **RECON ITR software installation**, including:

- License status
- Access to the End User License Agreement (EULA)
- Software change logs
- Known issues
- Support and update resources



Version	1.2.9
Purchase Date	19-Dec-2024
Expiration Date	07-Jan-2026
Days Remaining	364

RECON *ITR*

Copyright 2013-2024 - SUMURI LLC

www.sumuri.com

IMPORTANT, PLEASE READ CAREFULLY. THIS IS A LICENSE AGREEMENT

This RECON *ITR* is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This RECON *ITR* is licensed, not sold.

End User License Agreement

This End User License Agreement ('EULA') is a legal agreement between you (either an individual or a single entity) and SUMURI LLC with regard to the copyrighted software (herein referred to as RECON *ITR* or 'software') provided with this EULA. The RECON *ITR* includes computer software, the associated media, any printed materials, and any 'online' or electronic documentation. Use of any software and related documentation ('software') provided to you by RECON *ITR* in whatever form or media, will constitute your acceptance of these terms, unless separate terms are provided by the software supplier, in which case certain additional or different terms may apply. If you do not agree with the terms of this EULA, do not download, install, copy or use the software. By installing, copying or otherwise using the RECON *ITR*, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, SUMURI LLC is unwilling to license the RECON *ITR* to you.

Eligible License - This software is available for license solely to software owners, with no right of duplication or further distribution, licensing, or sub-licensing.

- SUMURI LLC grants to you a personal, non-transferable and non-exclusive right to use the copy of the software

If the END User or expiration information is incorrect, please contact us at hello@sumuri.com

10.7.1 Overview

Use the **About RECON** section to:

- Verify license details
- Review updates and improvements
- Understand known limitations
- Find support and update instructions

10.7.2 License Information

At the top of the **About RECON** window, you'll find your current license details:

Field	**Description**
Purchase Date	The date the RECON ITR software was purchased.
Days Remaining	The number of days remaining before the active license expires.
Expiration Date	The date when the software license will expire.
USB Serial Number	The serial number of the USB device to which RECON ITR is licensed.

> ***Tip:***
> *Regularly checking your license information helps avoid interruptions in access to updates and support.*

10.7.3 Additional Tabs in the About RECON Window

Tab	**Description**
License Agreement	View the current **End User License Agreement (EULA)** for RECON ITR.
Change Logs	Review a list of recent **software updates**, enhancements, and bug fixes.
Exceptions/Known Issues	Find a summary of **known issues** or limitations in the current release.

Support and Update	Access user manuals, support contact information, and update instructions.

> ***Note:***
> *Keeping track of known issues and reviewing change logs can help you plan triage and imaging strategies more effectively.*

---

11 Appendix

11.1 Apple Extended Attributes

Apple Extended Attributes are a form of **specialized metadata** created within macOS to enable advanced file indexing and searching through utilities like **Spotlight**.

This metadata is **critical to forensic investigations** because:

- It often contains information **not stored in traditional file system structures**.
- It is **invisible to most Windows-based forensic tools** unless specialized macOS tools are used.
- **POSIX timestamps** are often **overwritten or supplemented** by **Apple Extended Attributes**, meaning relying solely on standard file timestamps can produce **inaccurate results**.

11.1.1 Why Apple Extended Attributes Matter

Point	Description
Visibility	Apple Extended Attributes are **not natively visible** on Windows systems without specialized tools.
Limitations in Windows Tools	Most Windows forensic tools **ignore** or **partially display** Apple Extended Attributes.
Timestamps	macOS uses Extended Attributes for **file creation and modification times**, often replacing traditional POSIX timestamps.
Accuracy	Without properly processing Extended Attributes, examiners risk **misinterpreting timelines** and **file activity**.

11.1.2 RECON ITR and Extended Attributes

- **RECON ITR** and **RECON IMAGER** are **natively designed** to recognize, preserve, and document Apple Extended Attributes during imaging and triage.
- When paired with **RECON LAB**, investigators gain **the most comprehensive view** of Apple Extended Metadata available in forensic tools.

> **Key Advantage:**
> Using RECON IMAGER and RECON LAB together ensures investigators can:
>
> - **View correct macOS timestamps**
> - **Preserve full metadata**
> - **Avoid timeline reconstruction errors**

11.2 APFS

Apple File System (APFS) is Apple's proprietary file system used across its major platforms, including **macOS**, **iOS**, **watchOS**, and **tvOS**.

11.2.1 Key Points About APFS

Point	Description
Native Support	Fully supported starting with **macOS High Sierra (10.13)** and later versions.
Partial Support	Limited support available in **macOS Sierra (10.12)**.
Windows Support	**No native support** for APFS in Windows operating systems. Any APFS access in Windows forensic tools relies on **reverse-engineered, non-native implementations**, which may be incomplete or unreliable.

> ***Important:***
> *Analysts must be cautious when using Windows-based tools to process APFS volumes due to potential limitations or inaccuracies.*

11.2.2 RECON ITR and APFS

- **RECON ITR** is developed **natively on macOS** to fully support APFS and other Mac file systems without relying on reverse-engineering.
- APFS volumes and containers are processed **correctly and reliably** within RECON ITR.

Supported Imaging Options:

Imaging Type	Description
Logical Copies of APFS Volumes	Creates logical forensic images of individual APFS volumes. These logical images can be imported into any forensic tool that supports adding directories or files (including many Windows-based forensic tools).
Block Copies of Synthesized APFS Containers	Captures a block-level forensic image of an entire synthesized APFS container (common in macOS installations).

> ***Tip:***
> *Using RECON ITR ensures that APFS structures and metadata are preserved **natively and accurately**, avoiding the risks associated with non-native processing.*

11.3 Core Storage

Core Storage is Apple's version of **Logical Volume Management (LVM)**, introduced to provide **flexibility** in how physical storage devices are presented and managed within macOS.

11.3.1 Key Points About Core Storage

Point	Description
Purpose	Allows one or more physical disks to be combined and presented as a **single logical disk**.
First Introduced	Originally used by Apple to support **Fusion Drives** (combining SSDs and HDDs into a single logical volume).
Other Uses	Core Storage can also be utilized even when a **single physical disk** is present, especially for systems formatted with **macOS Extended (HFS+)** file systems.

11.3.2 Core Storage and RECON ITR

- **RECON IMAGER** fully recognizes both:
  - Traditional physical disks
  - **Core Storage virtualized disks** (logical volumes created by macOS)
- In most forensic imaging scenarios:
  - You will typically target and image the **Core Storage virtualized disk** that is **derived from** the Core Storage volume or volumes.
  - This ensures the **logical view of the filesystem** is accurately captured for analysis.

> ***Tip:***
> *Always verify which disk is the* ***"derived" virtual disk*** *to ensure you are imaging the complete logical volume as seen by the operating system.*

11.4 Disk Arbitrator

Disk Arbitrator is a feature integrated into **RECON ITR** to control how disks are mounted during forensic imaging and triage.

It **overrides macOS's default Disk Arbitration behavior**, which normally:

- **Automatically mounts** internal and external volumes.
- **Assigns** read/write access and a mount point immediately upon detection.

By using Disk Arbitrator:

- **Automatic mounting is blocked**.
- Volumes can only be mounted **manually through the RECON ITR interface**.
- This ensures that disks are **protected** and **not altered** by the operating system.

11.4.1 Behavior on Intel Macs

Environment	Disk Arbitrator Behavior (Intel Macs)
Live Environment	Disk Arbitrator can be manually turned **ON or OFF** by the examiner through the **Disk Manager**.
Bootable Environment	Disk Arbitrator is **enabled by default**. A **visible control icon** (blue/green disk) appears at the top-right system bar, allowing the examiner to manually **disable** it if necessary (e.g., during ASR imaging of APFS Containers).

Key Points:

- Full Disk Arbitration control and user interface are available.
- Examiners have **manual control** at any time while imaging Intel-based Macs.

11.4.2 Behavior on Apple Silicon Macs

Environment	Disk Arbitrator Behavior (Apple Silicon Macs)
Live Environment	Disk Arbitrator operates similarly to Intel Macs. It can be manually enabled through the **Disk Manager**.
Bootable Environment	**Disk Arbitrator is not visible** and **direct manual control is not currently available**. However, RECON ITR still **prevents automatic mounting** of evidence drives **internally**, behind the scenes.

Key Points:

- While the **Disk Arbitrator application** is **not visible** on Apple Silicon during boot imaging, **RECON ITR automatically controls mounting behavior internally**.
- Examiners do **not need to manually manage** Disk Arbitrator during boot imaging on Silicon Macs.
- Drives are still **protected from automatic mount and alteration** during bootable triage.

11.4.3 Important Differences Summary

Feature	Intel Macs	Apple Silicon Macs
Disk Arbitrator Visible?	**Yes** (Manual Control Available)	**No** (Control Handled Internally)
Manual Enable/Disable	Yes (via System Bar Icon)	No (Automatic Protection Only)
Protection Against Auto-Mounting	Yes	Yes
Special Handling During Boot Imaging	Prompt to disable manually if needed	No manual action needed

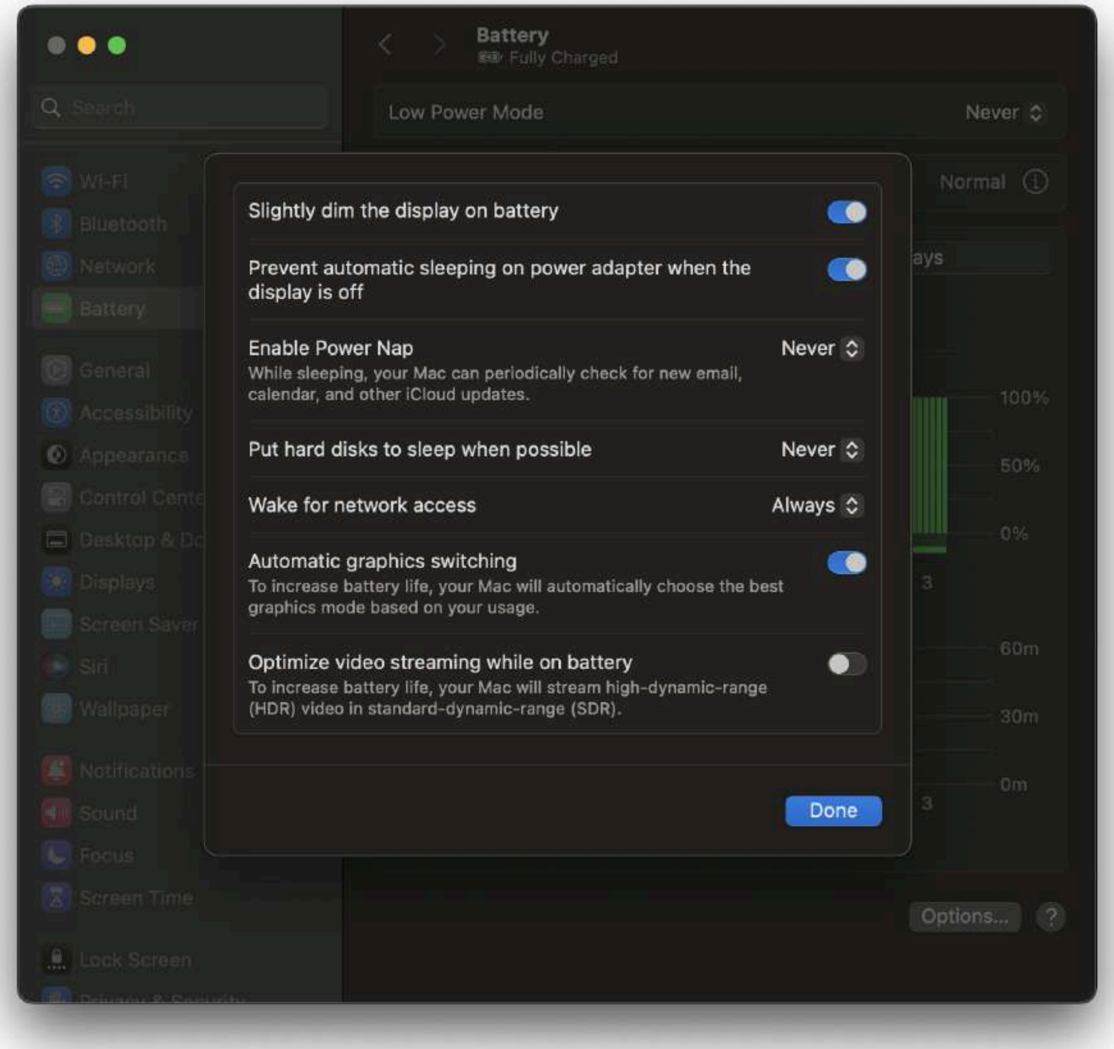
---

11.4.4 Practical Examiner Guidance

- **On Intel Macs:**
  ➔ Use the Disk Arbitrator toggle in the system bar to manually enable/disable as needed.
- **On Apple Silicon Macs:**
  ➔ Trust RECON ITR to automatically prevent auto-mounting during boot triage.
  ➔ You will **not** see a Disk Arbitrator control icon during boot imaging.

Tip:
Always verify disk mount status (read-only vs. read-write) through the Disk Manager before imaging, regardless of platform.

11.5 Energy and Power Settings



Low Power Mode: Never

Slightly dim the display on battery ●

Prevent automatic sleeping on power adapter when the display is off ●

Enable Power Nap: Never
While sleeping, your Mac can periodically check for new email, calendar, and other iCloud updates.

Put hard disks to sleep when possible: Never

Wake for network access: Always

Automatic graphics switching ●
To increase battery life, your Mac will automatically choose the best graphics mode based on your usage.

Optimize video streaming while on battery ○
To increase battery life, your Mac will stream high-dynamic-range (HDR) video in standard-dynamic-range (SDR).

The **Energy and Power Settings** on a Mac determine:

- How long the device stays logged in while idle
- When the screen turns off
- When hard disks go to sleep

11.5.1 Why Adjust Energy Settings?

When using RECON ITR for imaging or triage:

- It is **critical** to ensure that the device **remains active**.
- Allowing the device to **fall asleep** could interrupt imaging, triage, or evidence collection.

Recommendation:
Before starting any imaging or triage process, **adjust the Energy and Power Settings** to **prevent the Mac from sleeping**.

Disabling Sleep Settings on Macs Without a Battery (e.g., iMac, Mac mini, Mac Studio)

To prevent sleep:

1. Click the **Apple icon** in the top-left system toolbar.
2. Select **System Settings**.
3. Navigate to **Energy**.
4. **Disable** the option **Put hard disks to sleep when possible**.

11.5.3 Disabling Sleep Settings on MacBooks (Laptops with Batteries)

To prevent sleep:

1. Click the **Apple icon** in the top-left system toolbar.
2. Select **System Settings**.
3. Navigate to **Battery**.
4. In the **Battery** settings window, click on **Options** (bottom right corner).
5. Under **Put hard disks to sleep when possible**, set the option to **Never**.

Important Tip:

- On macOS Ventura (13) and later, these settings may vary slightly depending on the Mac model.
- Always verify that **display sleep**, **computer sleep**, and **hard disk sleep** are properly disabled for uninterrupted imaging or triage.

11.6 Firmware Password

Firmware Passwords are a security feature available **only on Intel-based Macs** to prevent unauthorized booting from external devices or alternate startup volumes.

When enabled, a Firmware Password:

- Blocks access to Startup Options without entering the password.
- Prevents booting the Mac from any source other than the installed internal macOS.

11.6.1 Key Points About Firmware Passwords (Intel Macs Only)

Point	Description
Purpose	Prevents unauthorized booting or external access by locking Startup Options.
Availability	**Only available on Intel-based Macs**.
Management	Set or removed through **macOS Recovery Mode**.
Behavior at Boot	Pressing **ALT/OPTION** during startup will display a **lock icon** if a Firmware Password is active.
Access Requirements	The **Firmware Password PIN or passcode** must be entered to access any external boot media (including RECON Imagers).

11.6.2 Important Examiner Guidance

- Before attempting to boot an Intel Mac, always check for a possible **Firmware Password**.
- If you see a **lock screen** instead of available startup disks when holding **ALT/OPTION**, a Firmware Password is present.
- Without the correct password:
  - You cannot boot to Recovery.
  - You cannot boot to an external device (such as a RECON Imager).
  - You cannot modify startup settings.

11.6.3 Firmware Passwords on Apple Silicon Macs

- **Apple Silicon Macs (M1, M2, M3, M4) do not use traditional Firmware Passwords**.
- Instead, startup security is managed through the **Secure Enclave** and **Startup Security Utility** settings.
- Protection on Apple Silicon focuses on:
  - Requiring administrative authentication to change startup security settings.
  - Using Activation Lock tied to the user's Apple ID.

Note:
You will not encounter a Firmware Password lock screen on Apple Silicon devices.

11.6.4 Removal of Firmware Passwords (Intel Macs)

- **Apple Certified Technicians** can remove a Firmware Password with proper authorization.
- Law enforcement may contact Apple Legal for assistance when required under applicable laws.

Important:
Firmware Passwords are hardware-level protections and **must not be confused** with standard macOS login passwords.

11.7 FileVault

FileVault is Apple’s proprietary **full-volume encryption** feature, designed to encrypt both the **System** and **Data APFS Volumes** on a Mac.

11.7.1 Key Behavior of FileVault

Point	Description
When Logged In	If the user is **logged in**, the APFS Data Volume is **unlocked** and can be imaged.
When Logged Out or Powered Off	If the device is **powered off** or the user is **logged out**, FileVault **relocks** the volume, encrypting the data.
Unlocking FileVault	To access or image the locked volume, you must provide either: ➔ The **administrator account password**, or ➔ The **FileVault recovery key**.

11.7.2 Imaging Considerations with FileVault

Situation	Action
Device is Logged In	Imaging can proceed normally; the volume is decrypted during the session.
Device is Logged Out or Off	FileVault must be unlocked before imaging can occur.

- **FileVault must be unlocked** before imaging either:
    - The **APFS Data Volume**, or
    - The **Synthesized APFS Container**.

11.7.3 Unlocking FileVault in RECON Imager

When booted into a RECON Imager environment:

1. Open the **Disk Manager** tab.
2. Select the encrypted volume.
3. Click the **Decrypt** button.
4. Provide either:
   - The **administrator password**, or
   - The **FileVault recovery key**.

Once decrypted, imaging of the APFS volume can proceed.

11.7.4 Special Note for Non-T2 Intel Macs

- On **non-T2 Intel Macs**, if neither the password nor the recovery key is known:
  - The **physical disk can still be imaged** in its **encrypted** state.
  - The encrypted image can later be **processed and decrypted** using **RECON LAB** if the password or recovery key becomes available.

> ***Important:***
> *Imaging an encrypted disk without credentials captures the encrypted data exactly as stored* ***— not decrypted content****.*

11.8 Fusion Drives

Fusion Drives are a hybrid storage solution developed by Apple that **combines two or more physical disks** into a **single logical volume** presented to the user.

Originally, a Fusion Drive consisted of:

- A **smaller, faster SSD** (solid-state drive) for performance.
- A **larger, slower spinning HDD** (hard disk drive) for cost-effective storage.

However, it is important to note that:

- On some systems, **both components may be SSDs**.

11.8.1 Traditional Forensic Imaging vs. RECON IMAGER

Approach	Process
Traditional Forensic Tools (e.g., PALADIN)	Examiners are taught to image **each physical disk separately**. To reconstruct the logical Fusion volume, both disk images must be manually mounted together on a Mac, and then re-imaged.
RECON IMAGER	Core Storage technology automatically **"marries" the physical disks** into a **single logical volume** during triage or imaging. Examiners can directly image the **single Core Storage disk**, eliminating the need for manual reconstruction.

11.8.2 How RECON IMAGER Handles Fusion Drives

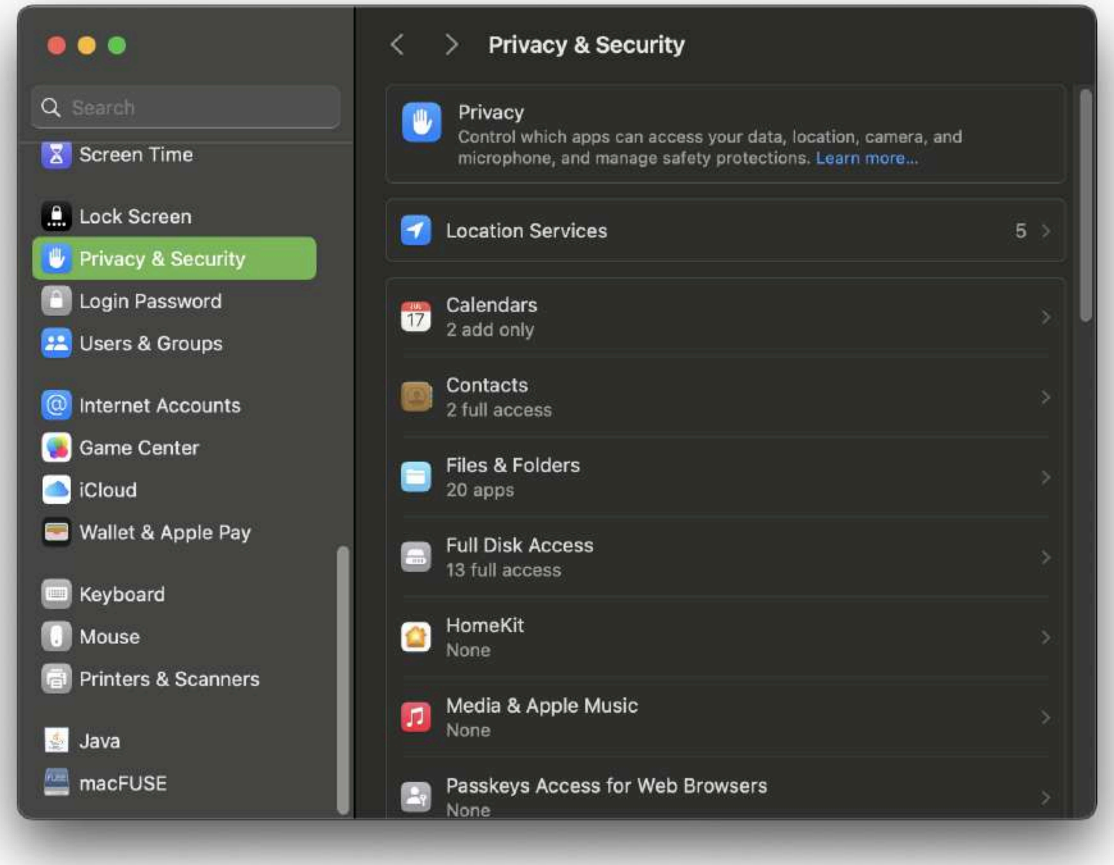
- RECON IMAGER recognizes the Core Storage **virtualized disk** created by macOS.
- Imaging the **Core Storage logical volume** allows the examiner to:
  - **Capture the complete Fusion Drive** in one forensic image.
  - **Preserve file and directory structures** correctly.
  - **Easily load the resulting image** into most forensic analysis tools.

> ***Tip:***
> *Imaging the "parent" physical disks individually is* ***not necessary*** *when using RECON IMAGER unless specifically required by case policy.*

11.8.3 Transition from Core Storage to APFS

- **Core Storage** was the technology behind Fusion Drives on earlier macOS versions.
- As of **macOS 10.13 High Sierra** and later:
    - Fusion Drives are **managed under APFS** instead of Core Storage.
    - Imaging APFS-managed Fusion Drives is handled natively by RECON IMAGER’s APFS support.

11.9 Full Disk Access



Privacy & Security

Privacy
Control which apps can access your data, location, camera, and microphone, and manage safety protections. Learn more...

Location Services 5

Calendars
2 add only

Contacts
2 full access

Files & Folders
20 apps

Full Disk Access
13 full access

HomeKit
None

Media & Apple Music
None

Passkeys Access for Web Browsers
None

Full Disk Access is a **macOS security feature** that allows designated applications to access files and directories that would otherwise be **restricted** — including critical system areas, user files, and private data.

Granting **Full Disk Access** to **RECON ITR** is:

- **Essential** when using the **Live Imaging** or **Live Triage** features.
- **Not required** when using **bootable imaging** environments (since those environments bypass macOS user permissions).

11.9.1 Why Full Disk Access is Important

Without Full Disk Access:

- The RECON ITR live application may not be able to fully access all user data, system artifacts, or application data.
- Triage results and live images could be incomplete or missing critical evidence.

Granting Full Disk Access ensures:

- **Complete and thorough** forensic triage.
- **Proper acquisition** of files and system information during live imaging.

11.9.2 Requirements

- **Administrative credentials** are **required** to grant Full Disk Access to RECON ITR.

11.9.3 How to Grant Full Disk Access to RECON ITR

1. Launch the **System Settings** application (➔ System Settings).
2. Click **Privacy & Security** in the sidebar.
3. Scroll down and click on **Full Disk Access**.
4. Click the **+** (Add) button.
5. Navigate to and select the **RECON ITR application**.
6. Confirm by entering your **administrator username and password** if prompted.

11.10 Local Time Machine Snapshots

Time Machine is the native backup utility in macOS, allowing users to create regular system and file backups to an external or network disk, referred to as the **Time Machine disk**.

11.10.1 How Local Time Machine Snapshots Work

- When the designated **Time Machine disk** is **not connected**, macOS will still attempt to create backups.
- These backups are temporarily stored **locally on the Mac's internal storage**.
- In **APFS-formatted** volumes, these temporary backups are known as **Local Time Machine Snapshots**.
- They are sometimes simply referred to as **APFS Snapshots**.

11.10.2 Key Points About Local Time Machine Snapshots

Feature	Description
Storage Location	Stored locally within the APFS file system on the internal drive.
Purpose	Ensures that backup points are still created even when the external backup drive is unavailable.
Automatic Management	macOS automatically manages local snapshots, deleting older snapshots when free disk space becomes limited.
Forensic Value	Local Time Machine Snapshots can retain data that has been deleted or modified from the active file system, providing valuable historical evidence.

> ***Tip:***
> *Examining Local Time Machine Snapshots can reveal historical states of files and directories that no longer exist on the active live volume.*

11.11 Secure Enclave

The **Secure Enclave** is a critical security component in modern Macs, responsible for managing encryption keys and ensuring data remains protected at rest.

11.11.1 Key History and Function

- The **Secure Enclave** was first introduced in the **iMac Pro**, released on **December 14, 2017**, through the use of the **Apple T2 Security Chip**.
- In Intel-based Macs with a T2 chip, the Secure Enclave operated as a **co-processor** alongside the Intel CPU.
- Key functions of the T2 chip and Secure Enclave included:
    - **Encrypting the internal storage drive.**
    - **Managing Touch ID data** and other sensitive information.
    - **Securing the boot process** and enforcing system integrity.

11.11.2 Hardware-Based Encryption

- During manufacturing, a unique **hardware UUID** (Universally Unique Identifier) is **permanently fused** into the Secure Enclave.
- This UUID is:
    - **Used to derive encryption keys** for the device's storage.
    - **Inaccessible** to the operating system, applications, or users.

11.11.3 Transition to Apple Silicon

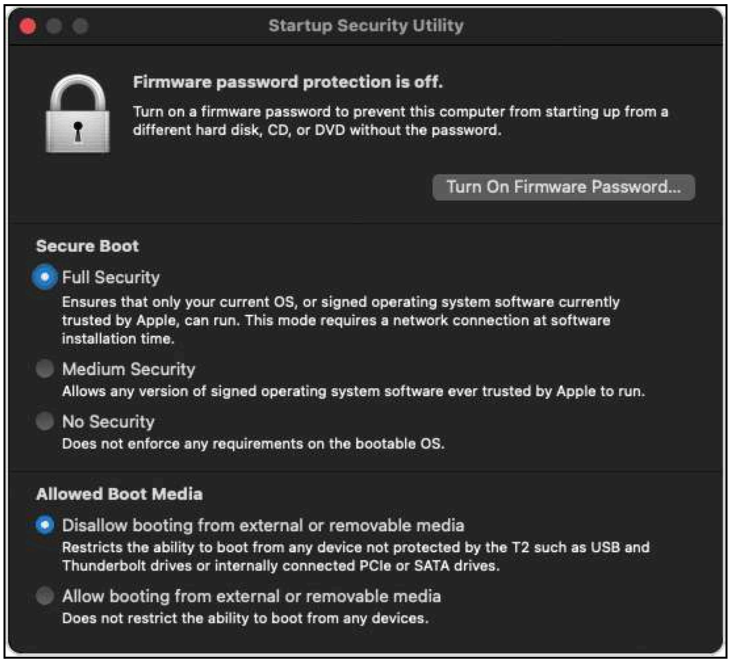
- Starting in **2020** with the release of **Apple Silicon M1 Macs**, the Secure Enclave was **integrated directly** into the main **System on a Chip (SoC)**.
- Although the hardware implementation changed, the core responsibilities of the Secure Enclave **remain the same**:
    - Key management
    - Encryption enforcement
    - System security

11.11.4 Forensic Imaging Considerations

Point	Description
Physical Imaging	**Not possible** on devices with a Secure Enclave (T2 Intel Macs and Apple Silicon Macs).
Supported Imaging Targets	Examiners must image either: - The **APFS Data Volume**, or - The **Synthesized APFS Container**.
Authentication Required	Imaging typically requires: - The **administrator password**, or - The **FileVault recovery key**.

> ***Important:***
> *Without credentials, only an encrypted physical image can be captured — and it cannot be decrypted without the associated authentication data.*

11.12 Startup Security Utility



Firmware password protection is off.

Turn on a firmware password to prevent this computer from starting up from a different hard disk, CD, or DVD without the password.

Secure Boot

● Full Security
Ensures that only your current OS, or signed operating system software currently trusted by Apple, can run. This mode requires a network connection at software installation time.

○ Medium Security
Allows any version of signed operating system software ever trusted by Apple to run.

○ No Security
Does not enforce any requirements on the bootable OS.

Allowed Boot Media

● Disallow booting from external or removable media
Restricts the ability to boot from any device not protected by the T2 such as USB and Thunderbolt drives or internally connected PCIe or SATA drives.

○ Allow booting from external or removable media
Does not restrict the ability to boot from any devices.

Startup Security settings control **whether a Mac can boot from external devices** and **enforce operating system trust**.
Examiners must understand these settings when preparing a Mac for bootable imaging with RECON ITR.

11.12.1 Important Platform Differences

Mac Type	How Startup Security is Managed
Intel Macs with T2 Chip	Managed through the **Startup Security Utility** in Recovery Mode. (Settings often need to be lowered.)
Apple Silicon Macs (M1, M2, M3, M4)	Managed through **Security Policy settings** in RecoveryOS. (**No changes are required** for booting RECON ITR.)

> ***Important:***
> ***Startup Security Utility** is **only present on Intel T2 Macs**.*
> *On Apple Silicon Macs, **no Security Policy modification is needed** to boot from RECON ITR.*

11.12.2 Booting RECON ITR on Apple Silicon Macs

- By default, **Apple Silicon Macs allow booting external drives** like RECON ITR as long as the examiner manually selects the external disk at startup.
- There is **no need** to lower or modify the Security Policy settings for imaging purposes.

Steps to Boot from RECON ITR (Apple Silicon):

1. Ensure the device is **completely powered down**.
2. Press and **hold the Power button** until you see **"Loading startup options…"**.
3. Release the button and wait for the **Startup Options** screen.
4. Select the external RECON ITR drive.
5. Boot into the RECON environment.

> **Note:**
> If a device has been specially hardened with a custom Security Policy that restricts external booting (rare), additional steps may be needed.
> In most default scenarios, no changes are required.

11.12.3 Lowering Startup Security on Intel T2 Macs

Intel Macs equipped with a T2 chip typically **require lowering security settings** to allow external booting.

Steps:

1. Ensure the device is **powered down**.
2. Press the **Power** button, then immediately hold **Command (⌘) + R** to boot into **Recovery Mode**.
3. Log in with the **administrator password** (if prompted).
4. In the menubar, select **Utilities ➔ Startup Security Utility**.
5. Authenticate by clicking **Enter macOS Password** (if prompted).
6. Under **Secure Boot**, select **No Security**.
7. Under **Allowed Boot Media**, select **Allow booting from external or removable media**.
8. Close the window.
9. From the Apple menu (), select **Shut Down**.
10. Boot again and select the RECON drive.

11.12.4 Summary

Mac Platform	Booting RECON ITR	Security Settings Changes Required?
Apple Silicon (M1, M2, M3, M4)	Select external boot device manually	**No** (Default settings allow booting)
Intel T2 Mac	Lower security settings using Startup Security Utility	**Yes** (Set to No Security + Allow External Boot)

> ***Tip:***
> *Always check if the device is locked with a **Firmware Password** or **Activation Lock** as these can still restrict access regardless of security settings.*

11.13 Target Disk Mode (TDM) & Share Mode

Target Disk Mode (TDM) and **Share Mode** are macOS features that allow one Mac to behave like an external drive, making it accessible from another Mac.

These modes are useful for:

- **Transferring large amounts of data** between devices.
- **Performing forensic imaging** using RECON ITR.

When a Mac is connected via TDM or Share Mode:

- It will appear as a **separate disk** in the RECON ITR Imager interface.
- The examiner can then target the disk for imaging as if it were an attached external drive.

11.13.1 Platform Support

Mode	Supported on	Description
Target Disk Mode (TDM)	**Intel Macs only**	Directly mounts the Mac's internal storage as an external drive over Thunderbolt or USB-C.
Share Mode	**Apple Silicon Macs only**	Shares the Mac's internal volume over the network as an **SMB server**.

11.13.2 Connecting Intel Macs via Target Disk Mode (TDM)

Steps:

1. Connect the **examiner Mac** and the **target Mac** using a **Thunderbolt** or **USB-C** cable.
2. Power off the target Mac (the one you want to image).
3. **Press and hold the T key**, then press the **Power button**.
4. Continue holding **T** until you see the **Target Disk Mode** symbol (e.g., Thunderbolt, USB).
5. On the examiner Mac, the target Mac's internal drive should now **mount as an external disk**.

You can now use RECON ITR to image the mounted drive.

11.13.3 Connecting Apple Silicon Macs via Share Mode

Steps:

1. Connect the **examiner Mac** and the **target Mac** using a **Thunderbolt** or **USB-C** cable.
2. Shut down the target Mac (the one you want to image).
3. **Press and hold the Power button** on the target Mac until **Startup Options** appear.
4. Click **Options**, then click **Continue** to enter RecoveryOS.
5. In the **Mac Utilities** window:
    - Click **Utilities** in the menubar.
    - Select **Share Disk** from the dropdown menu.

6. Choose the volume you want to share.
7. Click **Start**.

On the examiner Mac:

- Open **Finder ➔ Network** section.
- You should see the target Mac's shared disk appear as a **network share**.
- RECON ITR can then target the shared volume for imaging.

11.13.4 Important Reminders

Point	**Target Disk Mode (TDM)**	**Share Mode**
Mac Type	Intel Macs only	Apple Silicon Macs only
Connection Type	Thunderbolt or USB-C	Thunderbolt or USB-C (appears over SMB network)
Visibility	Mounts as a direct disk	Appears as a network disk
Imaging Support	Direct block-level access	SMB share-level access (slower than TDM)

> ***Note:***
> *Share Mode is generally **slower** than Target Disk Mode and **not recommended** for large-scale imaging unless no other option is available.*

---

12 Glossary

Term	Definition
APFS	Apple’s modern file system, introduced with macOS High Sierra (10.13), replacing HFS+ as the primary file system for Macs.
Apple Extended Attributes	Special metadata stored in APFS volumes, used by Spotlight and other macOS features to store information beyond standard POSIX attributes.
FileVault	Apple’s volume encryption system that protects disk data by encrypting the contents of the internal drive.
File Signature	A unique pattern (usually located at the start of a file) that identifies a file’s type and format.
Fusion Drive	A hybrid storage configuration combining a Solid State Drive (SSD) and Hard Disk Drive (HDD) to balance speed and capacity.
HFS+	Apple’s legacy file system, also known as Mac OS Extended, used before the introduction of APFS.
Plugins	Individual forensic modules within RECON ITR designed to extract data from specific applications, artifacts, or processes.
Recovery Mode	A special macOS startup mode used for system troubleshooting, disk repair, OS reinstallation, and accessing tools like Startup Security Utility.
REGEX	A pattern-matching syntax (Regular Expression) used for advanced text searching, extraction, and manipulation.
Secure Enclave	A dedicated security processor that manages encryption keys, authentication data, and sensitive operations on Macs with T2 or Apple Silicon chips.
SMB (Samba)	A network file-sharing protocol allowing files and printers to be shared between different operating systems, including macOS and Windows.
Target Disk Mode (TDM)	A macOS feature that allows an Intel Mac to function as an external drive when connected to another Mac via Thunderbolt or USB-C.
Share Mode (Target Share Mode)	A macOS feature on Apple Silicon Macs that shares the internal storage over the network as an SMB server, allowing access from another Mac.

Time Machine Backup	macOS’s built-in backup solution that automatically saves regular snapshots of system files and user data to external or network storage.

13 Terms and Conditions

RECON ITR/IMAGER

http://www.sumuri.com

IMPORTANT, PLEASE READ CAREFULLY. THIS IS A LICENSE AGREEMENT

This **RECON ITR/IMAGER** is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This **RECON ITR/IMAGER** is licensed, not sold.

End User License Agreement

This End User License Agreement (**‘EULA’**) is a legal agreement between you (either an individual or a single entity) and **SUMURI LLC** ( ) with regard to the copyrighted software (herein referred to as **RECON ITR/IMAGER** or ‘software’) provided with this **EULA**. The **RECON ITR/IMAGER** includes computer software, the associated media, any printed materials, and any ‘online’ or electronic documentation. Use of any software and related documentation (‘software’) provided to you by **RECON ITR/IMAGER** in whatever form or media, will constitute your acceptance of these terms, unless separate terms are provided by the software supplier, in which case certain additional or different terms may apply. If you do not agree with the terms of this **EULA**, do not download, install, copy or use the software. By installing, copying or otherwise using the **RECON ITR/IMAGER**, you agree to be bound by the terms of this **EULA**. If you do not agree to the terms of this **EULA**, **SUMURI LLC** is unwilling to license the **RECON ITR/IMAGER** to you.

Eligible License – This software is available for license solely to software owners, with no right of duplication or further distribution, licensing, or sub-licensing.

License Grant – SUMURI LLC grants to you a personal, non-transferable and non-exclusive right to use the copy of the software provided with this **EULA**. You agree you will not copy or duplicate the software. You agree that you may not copy the written materials accompanying the software. Modifying, translating, renting, copying, transferring or assigning all or part of the software, or any rights granted hereunder, to any other persons and removing any proprietary notices, labels or marks from the software is strictly prohibited. Furthermore, you hereby agree not to create derivative works based on the software. You may not transfer this software.

Copyright – The software is licensed, not sold. You acknowledge that no title to the intellectual property in the software is transferred to you. You further acknowledge that title and full ownership rights to the Software will remain the exclusive property of **SUMURI LLC** and/or its suppliers, and you will not acquire any rights to the software, except as expressly set forth above. All copies of the software will contain the same proprietary notices as contained in or on the software. All title and copyrights in and to the **RECON ITR/IMAGER** (including but not limited to any images, photographs, animations, video, audio, music, text and "applets," incorporated into the **RECON ITR/IMAGER**), the accompanying printed materials, and any copies of the **RECON ITR/IMAGER**, are owned by **SUMURI LLC**. The **RECON ITR/IMAGER** is protected by copyright laws and international treaty provisions. You may not copy the printed materials accompanying the **RECON ITR/IMAGER**.

Reverse Engineering – You agree that you will not attempt, and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, modify, translate or disassemble the software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder to **SUMURI LLC**.

Disclaimer of Warranty – The software is provided 'AS IS' without warranty of any kind. **SUMURI LLC** and its suppliers disclaim and make no express or implied warranties and specifically disclaim the warranties of merchantability, fitness for a particular purpose and non-infringement of third-party rights. The entire risk as to the quality and performance of the software is with you. Neither **SUMURI LLC** nor its suppliers warrant that the functions contained in the software will meet your requirements or that the operation of the software will be uninterrupted or error-free. **SUMURI LLC** is not obligated to provide any updates to the software for any user who does not have a software maintenance subscription.

Limitation of Liability – **SUMURI LLC's** entire liability and your exclusive remedy under this EULA shall not exceed the price paid for the software, if any. In no event shall **SUMURI LLC** or its suppliers be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the use or inability to use the software, even if **SUMURI LLC** or its supplier has been advised of the possibility of such damages, or any claim by a third party.

Rental – You may not loan, rent, or lease the software.

Transfer – You may not transfer the software to a third party without written consent from **SUMURI LLC** and written acceptance of the terms of this Agreement by the transferee. Your license is automatically terminated if you transfer the software without the written consent of **SUMURI LLC**. You are to ensure that the software is not made available in any form to anyone not subject to this Agreement. A transfer fee of $150 USD will be charged to transfer the software (not applicable to transfers associated with orders from distributors, or resellers or intra-company transfers).

Upgrades – If the software is an upgrade from an earlier release or previously released version, you now may use that upgraded product only in accordance with this **EULA**. If the **RECON ITR/IMAGER** is an upgrade of a software program which you licensed as a single product, the **RECON ITR/IMAGER** may be used only as part of that single product package and may not be separated for use on more than one computer.

OEM Product Support – Product support for the **RECON ITR/IMAGER** is provided by **SUMURI LLC**. For product support, please call **SUMURI LLC**. Should you have any questions concerning this, please refer to the address provided in the documentation.

No Liability for Consequential Damages – In no event shall **SUMURI LLC** or its suppliers be liable for any damages whatsoever (including, without limitation, incidental, direct, indirect, special and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use or inability to use this **'SUMURI LLC'** product, even if **SUMURI LLC** has been advised of the possibility of such damages. Because some states/countries do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Indemnification By You – If you distribute the software in violation of this Agreement, you agree to indemnify, hold harmless and defend **SUMURI LLC** and its suppliers from and against any claims or lawsuits, including attorney's fees that arise or result from the use or distribution of the software in violation of this Agreement.

Jurisdiction – This agreement shall be governed in all respects by US federal laws and regulations, except as to copyright and trademark matters, which are covered by U.S. laws and international treaties. The US federal court or board having the authority to decide disputes where the US Government is a party, shall have exclusive jurisdiction concerning all matters pertaining to this Agreement, and both parties agree to submit to such jurisdiction, with venue before such applicable US federal court or board. The parties consent to the exclusive jurisdiction and venue of the federal and state courts located in the State of Delaware, USA, in any action arising out of or relating to this Agreement. The parties waive any other venue to which either party might be entitled by domicile or otherwise.