RECON ITR Software Manual

SUMURI LLC

RECON ITR 26.1.0

Jun 22, 2026

Table of Contents

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

1 RECON ITR Introduction

Built entirely in Swift, **RECON ITR** is SUMURI's flagship imaging, triage, and reporting solution, purpose-built for macOS investigations. By leveraging native architecture, it delivers exceptional performance and seamless integration, working with the macOS environment rather than attempting to emulate it, ensuring a smooth, efficient experience for modern macOS investigations.

1.1 Native macOS Advantage

RECON ITR is natively developed on macOS using Apple's own libraries and system frameworks. Having been designed in Apple native Swift: - **Zero Emulation**: Runs natively on Apple Silicon (M series Mac) and Intel processors for maximum performance. - **Immediate Support**: Day-one compatibility with new macOS versions and file systems (APFS, local snapshots, Filevault, Time Machine, etc.). - **Precision Parsing**: Accurate interpretation of proprietary Apple Extended Attributes and system metadata that non-native tools often miss or corrupt.

Why Native macOS Matters

Many forensic tools attempt to analyze Mac data from Windows or Linux environments. This often results in incomplete interpretation of Apple metadata, extended attributes, and APFS features.

Because RECON ITR is built natively in Swift using Apple frameworks, it can interpret macOS artifacts exactly as the operating system does.

1.1.1 Licensing

- **License Length:** Each initial purchase of **RECON ITR** includes a one-year license. Licenses may be renewed for up to three years at a time.
- **SaaS Model: RECON ITR** operates under a subscription-based licensing model. When a license expires, the software will no longer function, and access to all imaging and triage features will be disabled until the license is renewed.

1.1.2 Imaging Capabilities

RECON ITR provides a versatile forensic imager available in both bootable and live environments, allowing examiners to adapt to nearly any hardware scenario. - **Supported Acquisitions:** - **APFS Containers:** Block-level acquisition of synthesized APFS containers

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

(required for T2 and Apple Silicon Macs). - **Physical Drives:** Bit-for-bit acquisition of physical disks (supported on pre-T2 Intel Macs and external media). - **Logical Imaging:** Targeted acquisition of specific files, folders, or user directories when full disk imaging is not authorized or technically feasible.

Reminder:

On Macs equipped with a Secure Enclave (T2 Intel Security Chip or Apple Silicon), physical imaging of the internal SSD is not possible due to hardware encryption. Examiners must target the APFS Container or Data Volume.

1.1.3 Triage Capabilities

The tool's on-site triage capability allows investigators to obtain answers from a running Mac within minutes. - **Live Triage:** Rapidly parse and identify critical evidence (User Activity, Chat Logs, Internet History) on a live running system. - **Automated Analysis:** Leverage over 100 built-in plugins to automatically extract artifacts without the need to manually search through the file system - **Field-Ready:** Designed for "on-scene" use, allowing investigators to preview data and make rapid decisions without needing to return to the lab.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

2 Installation and Updating

2.1 Updating the Software

RECON ITR is shipped preinstalled on a high-speed portable Samsung T7 SSD and is ready for immediate use. Before deploying the software in the field, it is recommended to verify that the latest version is installed. The most current version of **RECON ITR,** and available updates, can be found on the **SUMURI** page. The updater utility updates both the Live and Bootable partitions at the same time. During the update process, the drive will be reformatted. All case data and evidence must be removed from the drive prior to updating to prevent accidental data loss.

2.1.1 Steps to update the software:

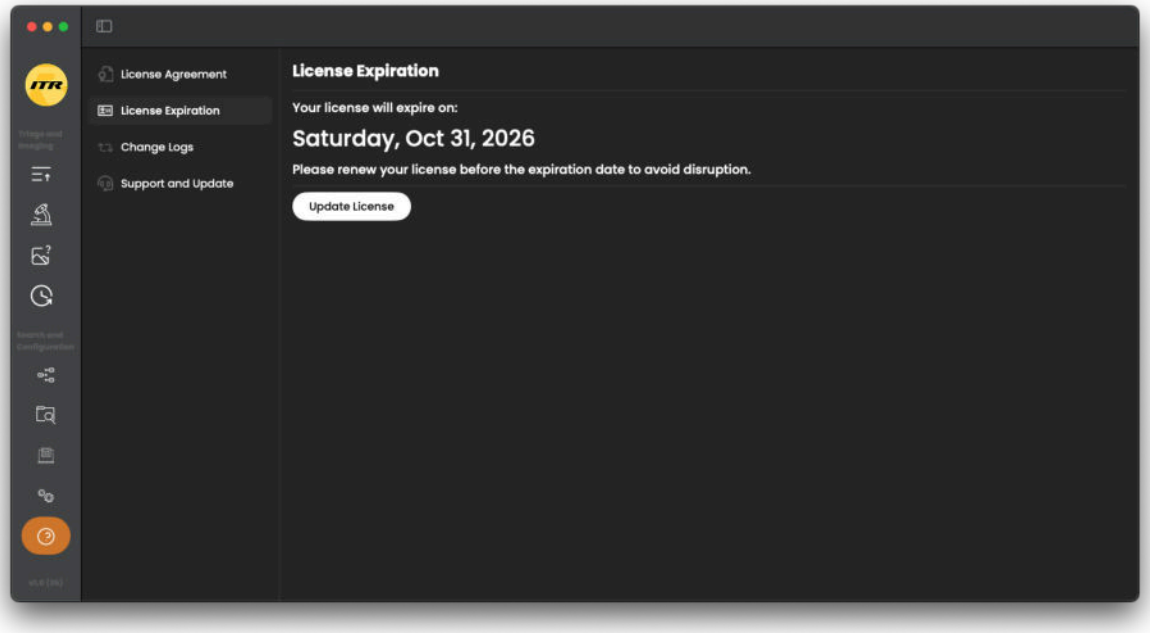
1. Connect the **RECON ITR** SSD to an examiner Mac that has internet access.
2. From the Software Updates page, download the latest **RECON ITR Updater**.
3. Open the downloaded DMG file and drag **RECON ITR Updater** into the Applications folder.
4. Grant Full Disk Access to **RECON ITR Updater**:
    - Open System Settings → Privacy & Security → Full Disk Access
    - Add **RECON ITR Updater**
5. Launch **RECON ITR Updater**.
6. If prompted, select your current license file (.lic).
7. Confirm that Online Update is selected, then click OK.
8. When prompted, enter an administrator password to allow the update to proceed.
9. Once the update completes successfully, the SSD will be updated with the latest software and a confirmation message will be displayed.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Notice:

If your agency is unable to connect the examiner Mac to the internet and requires an offline updater, please contact sumuri.com">Software@sumuri.com for assistance.

2.1.2 Finding the expiration date



To check the expiration date of your license: 1. Launch the **RECON ITR** application. 2. Navigate to the **About RECON** section, located in the bottom-left corner of the main window. 3. A new window will appear. On the left-hand sidebar of this window, select the option labeled **License Expiration**. 4. The main view will now display your license's expiration date.

2.1.3 License renewal

RECON ITR is licensed under an annual SaaS model. The initial purchase includes a one year active license, which is required to operate the application. - **Active License**: You receive unlimited updates and support. - **Expired License**: **RECON ITR** operates on a strict SaaS (Software as a Service) subscription model. An active license is required to launch and operate the application. If your license expires, the software will cease to function immediately, and you will be unable to perform any forensic tasks until the subscription is renewed.

To renew, please contact with your device Serial Number (found in the *System Information*

menu).

2.1.4 Updating the license

After purchasing a renewal, you will receive an email from containing a zipped digital license file (.lic). 1. Connect the **RECON ITR** SSD to the Mac 2. Download and unzip the zipped license file from 3. Ensure the **RECON ITR** application has Full Disk Access 4. Launch the **RECON ITR** application and provide the Administrator Password when prompted 5. Navigate to the **About RECON** section 6. Click on the **License Expiration** tab 7. Click on **Update License** and navigate to the new (.lic) file.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

3 Supported Hardware and macOS

Comprehensive support for the entire Apple ecosystem, ranging from legacy Intel-based systems to the modern Apple Silicon (M-Series) architecture.

3.1 Live Imaging and Triage

Live imaging and Triage are performed using the Live **RECON ITR** application located on the LIVE partition of the SSD. Live imaging and Triage can be performed while the target Mac is powered on and logged into a User or Admin Account. - **System Requirements:** - **Minimum Supported Version:** macOS 14 (Sonoma) - **Supported Processors:** - **Intel:** Intel Core i5, i7, i9, and Xeon processors. - **Apple Silicon:** Native support for **M1, M2, M3, M4, and M5** (including Pro, Max, and Ultra variants).

Important: - While not strictly required for the application to launch, granting **Full Disk Access** is strongly recommended. Enabling this permission allows **RECON ITR** to access protected macOS user artifacts such as Messages, and Photos. - **Secure Enclave Devices** (T2 and Apple Silicon) cannot be physically imaged as they utilize the Secure Enclave which incorporates hardware level encryption. Instead, a block-level copy of the APFS container or a logical acquisition of the Data volume is required.

3.2 Boot Imaging

Boot imaging is performed by booting the target Mac directly to the **RECON ITR** SSD. This ensures the internal data volume is not mounted writable by the host OS.

3.2.1 RECON BOOTABLE - Bootable Imager

This is the primary bootable imaging environment for **RECON ITR**. It is fully optimized for Apple Silicon architecture and supports the latest file system features. - **Apple Silicon Models (M1, M2, M3, M4, M5) (Pro, Max and Ultra):** - MacBook Air - MacBook Pro - Mac mini - Mac Studio - iMac - Mac Pro - **Intel Models:** - MacBook Air (Retina, 2018 or newer) - MacBook Pro (2018 or newer) - Mac mini (2018 or newer) - iMac (2019 or newer) - iMac Pro (2017) - Mac Pro (2019)

LEGACY INTEL - Bootable Imager

The LEGACY INTEL boot mode is designed primarily for T2 Intel Macs that are not compatible with the v26 RECON ITR application. This environment runs RECON Imager v7.0.0 and provides full imaging support for T2 Intel devices where the current Imager version

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

is not supported. Some support for older, non-T2 Intel Macs is also available through this boot mode.

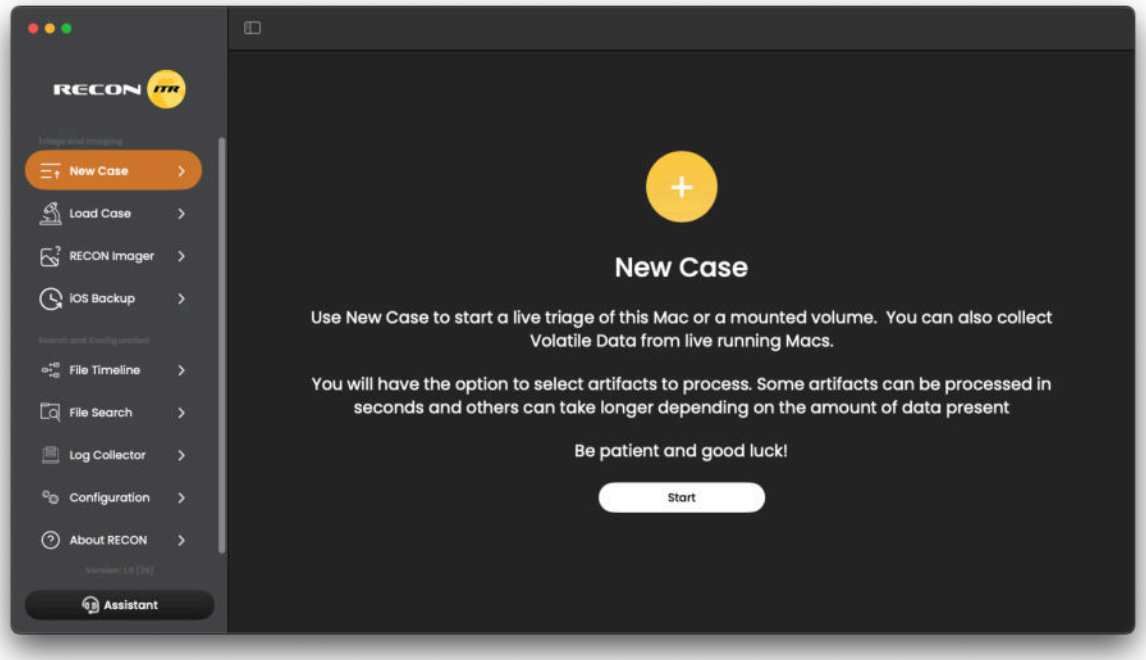
Notice:

If you are imaging a Mac manufactured before 2017, it is recommended that you use Paladin to acquire the image. Paladin is included free with RECON ITR and is designed for imaging pre-T2 Intel-based Macs, WIndows, and Linux devices

If you need the 7.0 Imager Manual for the Legacy Bootable Imagers, please reach out to sumuri.com">Software@sumuri.com

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

4 RECON ITR Splash Screen Options



Upon launching **RECON ITR** in the live environment, you are presented with the dashboard interface. The sidebar layout allows for seamless navigation between modules without returning to a central home screen, enabling you to keep multiple forensic tools active simultaneously. The Dashboard is divided into two main areas: - **The Sidebar (Left)**: Permanent navigation to all forensic modules and utilities. - **The Workspace (Right)**: The active window for the selected module.

4.1 Navigation Sidebar

The sidebar acts as the command center for **RECON ITR**, organized into two categories to streamline the examiner's workflow.

4.1.1 Triage and Imaging:

- **New Case**: The starting point for triage investigations. Initiates the Case Creation Wizard for live triage and volatile data collection.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

- **Load Case**: Opens previously created triage cases for review, reporting, or continued analysis.
- **RECON Imager**: Opens the dedicated forensic imaging engine for Logical, Container, or Physical (where supported) acquisition.
- **iOS Backup**: Scans the local system for locally saved iOS backups to extract or triage mobile data using the built-in iLEAPP module.

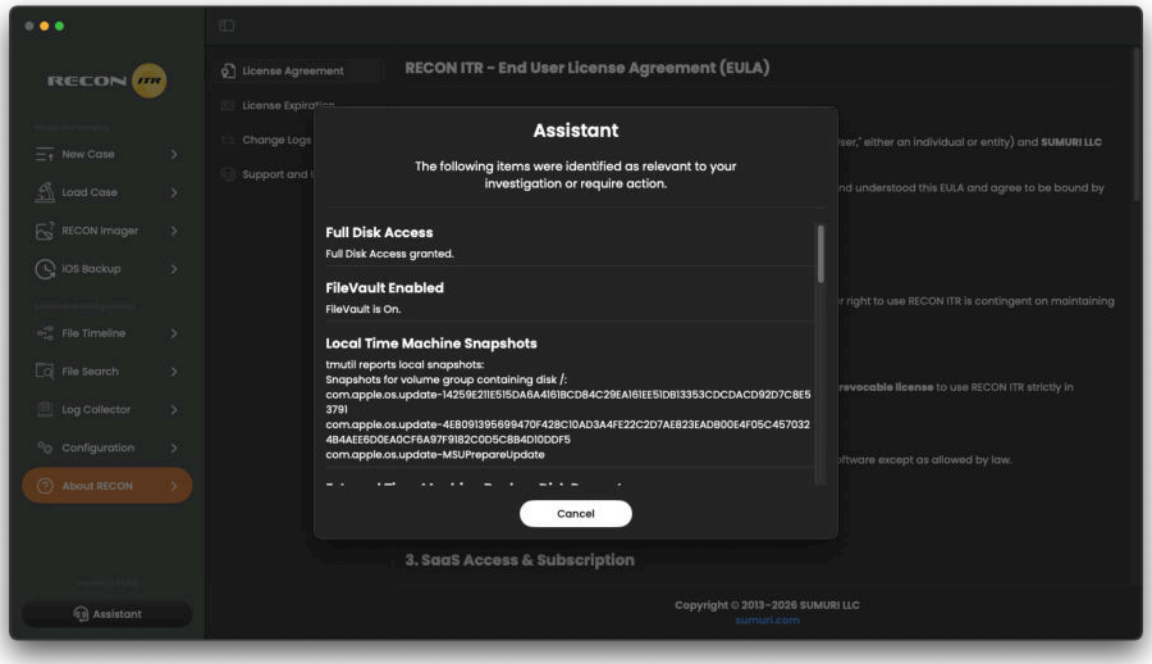
4.1.2 Search and Configuration:

- **File Timeline:** Creates a chronological view of file system activity using Apple Extended Attribute timestamps. Examiners may generate reports documenting bookmarked file system activity.
- **File Search:** Performs targeted searches across selected directories using user-defined file signatures, keywords, or filenames. Reports may be generated from bookmarked search results.
- **Log Collector**: Collects Apple Unified Logs (as either text or .logarchive format) for system analysis.
- **Configuration:** Customizes examiner details, agency logos, and global software settings.
- **About RECON:** Displays current EULA, license status, and change logs. Through

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

this window, you may update your license file.

4.1.3 Assistant



Located at the bottom of the sidebar, the **Assistant** provides integrated, context-aware support to guide examiners through workflows or answer questions about the software's capabilities. The assistant may provide critical information that may be important to your case. This can include notifications such as: - Status of Full Disk Access - FileVault Status - Local Time Machine Snapshots - Status of connected External Time Machine Backup Drives - Locally saved iOS Backups - iCloud Account Status

This can be useful for getting a quick glance of what could impact or be useful in your investigation.

5 Supported Plugins

RECON ITR includes over 100 built-in plugins designed to parse artifacts from both Apple-native and widely used third-party applications. These plugins can be accessed through the following workflows: - **Triage Case** (New Case / Load Case) - **Logical Imaging** (**RECON Imager**)

When a plugin is selected during New Case or Load Case, **RECON ITR** attempts to extract relevant artifacts and parse the underlying data into examiner-readable reports. When a plugin is selected through Logical Imaging (**RECON Imager**), **RECON ITR** attempts to acquire all forensic artifacts associated with the selected plugin and store them in a logical image. Important Notes: - **Volatile Data**: Some plugins (such as Running Processes or Active Network Connections) are volatile and can only be executed on a live running system. These will not be available or effective when triaging a mounted external drive. These artifacts may also not be collected through the Logical Imager. - **macOS Version**: The macOS version on the target device impacts which artifacts are detected and how much data is available. New macOS updates may alter or deprecate specific plugin behaviors.

5.1 Plugin List

Below is the comprehensive list of supported plugins, categorized by function.

5.1.1 Advanced Analysis

Audio, Basic Information, CCleaner, CleanMyMac2, Document Files, iOS Backups, Keychain, Online Accounts, Opened Files, Spoliation

5.1.2 Apple / Native Apps

Apple Calendar, Apple Dock, Apple Mail, Connected iOS Devices, Contacts, Facetime, Finder and Recent Items, Finder Sidebar, iCloud, iCloud Logs, Maps, Music, Notes, Photo Booth,

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Photos, Podcasts, Reminders, Screen Time, Stocks, Voice Memos

5.1.3 Email & Messaging

Messages, Thunderbird, Viber

5.1.4 Files & Downloads

FileZilla, Cyberduck, Free Download Manager

5.1.5 Images

Geotags, Images

5.1.6 Logs & System Activity

Network Logs, Utmpx

5.1.7 Networks

Active Networks, Apple Wireless Networks, Bluetooth, IP Address, Network Interfaces, Network Preferences, SSH

5.1.8 Online Storage

Dropbox, Google Drive, OneDrive

5.1.9 P2P (File Sharing)

aMule, Bitlord, Bittorrent Web, eMule, Folx, Qbittorrent, Torrent Files, Transmission, uTorrent Web

5.1.10 System

Bash History, Clipboard, Connected Devices, Deleted Users, Printers and Scanners, Escalate Privileges, Installed Applications, Installed Hardware, Text Replacements, KnowledgeC, Logged Users, Auto Start, Microsoft 365, Notifications, Quarantine Events, Running Processes, SavedState, Software Updates, Spotlight Settings, System Profiles, TCC, Time

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Machine, Trash Recyclebin, Typed Words, Uptime, Wake Reasons, WhereFroms, Zsh History

5.1.11 Video & Media

Video

5.1.12 Virtual Machines & Remote Desktop

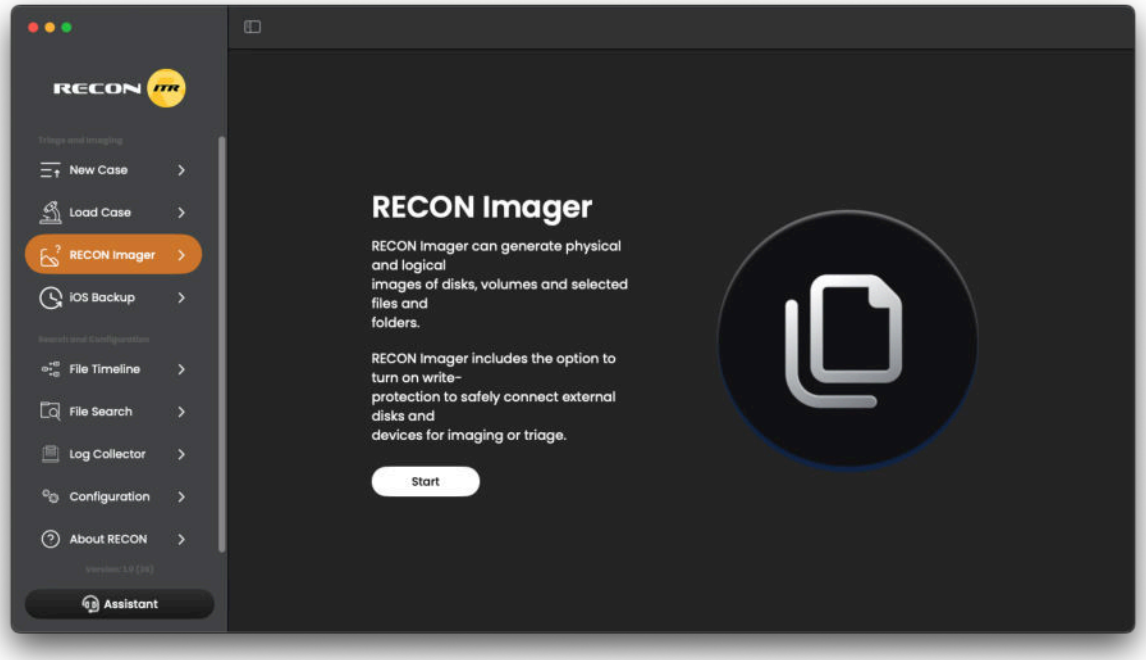
Parallels, TeamViewer, VirtualBox, Virtual Machine Files, VMware Fusion

5.1.13 Web Browsers

Brave, Chromium, Google Chrome, Microsoft Edge, Mozilla Firefox, Opera, Safari, Tor Browser

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

6 RECON Imager



RECON Imager is the built-in imaging application and can be accessed in the following ways: - From the bootable imager RECON Bootable - 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 (internal drives are accessible only from the boot environment) - Physical partitions

Before using **RECON Imager**, carefully review this manual and the associated appendices. After each installation or update, it is strongly recommended that you verify functionality by imaging sample data.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Notice:

Physical imaging is not supported on devices with a Secure Enclave (T2 and Apple Silicon M-series chips), but is supported on pre-T2 Intel Macs and external drives.

6.1 Accessing RECON Imager (Live Environment)

To launch **RECON Imager** while the Mac is running normally: 1. Plug **RECON ITR** SSD into the target Mac 2. Provide **RECON ITR** full Disk Access through System Settings (*Recommended*) 3. Open the LIVE Partition and launch the **RECON ITR** application 4. When prompted, provide the administrator password or press on Skip if being launched by a regular user account 5. Click on the **RECON Imager** button on the Home Screen then press on Start

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

Full Disk Access: - When using **RECON ITR** in a live environment, it is strongly recommended to grant the application Full Disk Access if the administrator password is available. Full Disk Access allows **RECON ITR** to access protected areas of the file system that would otherwise be inaccessible.

Full Disk Access **can only be granted using an administrator account** and cannot be enabled with a standard user password.

6.2 Accessing RECON Imager (Boot Environment)

To launch the **Imager** from a bootable environment: 1. Start the Mac into Startup Disk Mode 2. Select **RECON Bootable** as the Startup Disk 3. After the device has booted to the **RECON Bootable Imager**, open **RECON IMAGER**

Imaging Capabilities: - Acquisitions of the Synthesized APFS Container and APFS Data Volume supported on Apple Silicon and T2 Intel Devices - Physical acquisitions supported on Pre-T2 Intel Macs and external physical drives and partitions

** Notice:** If the target device is not compatible with the RECON Bootable Imager, the LEGACY SILICON or LEGACY INTEL boot modes may be selected instead. These environments run RECON Imager v7.0.0 and provide imaging support for devices where the

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

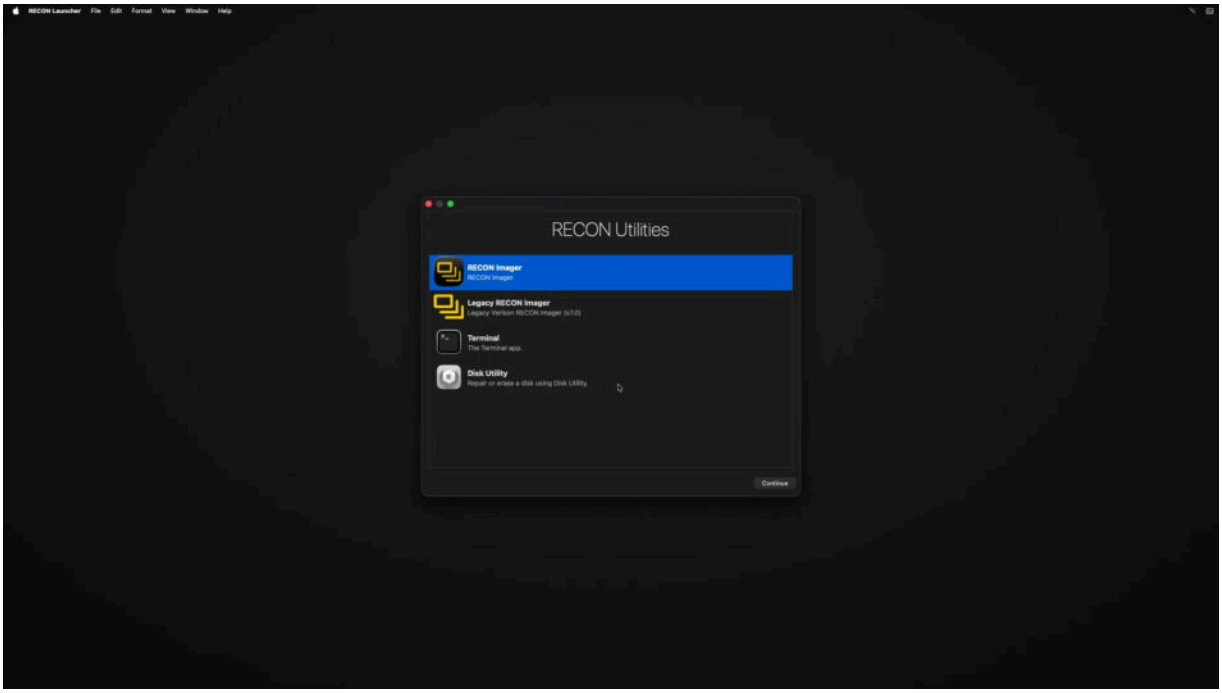
current Imager version is not supported. Select the option that corresponds to the processor architecture of the target device.

6.3 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 **RECON Imager**, to boot from. Once in Startup Disk Mode, you can choose and boot into the RECON Bootable Imager. 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 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.

6.4 RECON Utilities - (Boot Only)

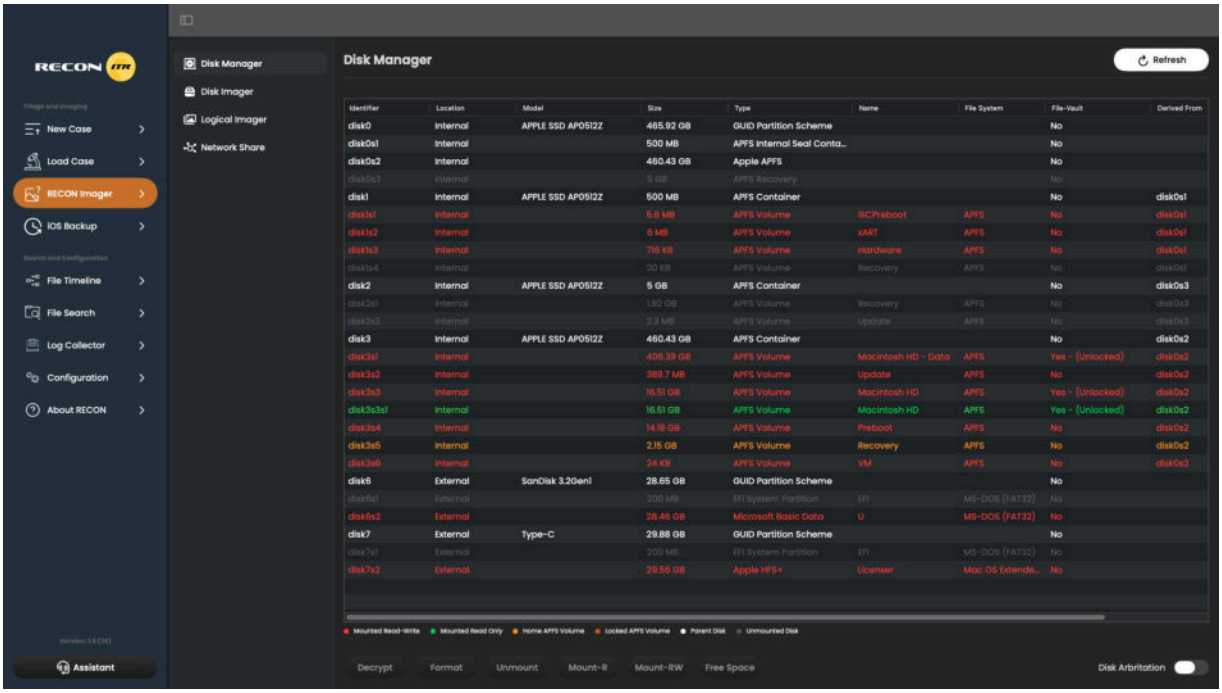


After selecting a Bootable Imager, you may be presented with the **RECON Utilities** screen if the device being booted is an Intel device. This screen displays a list of applications available on the bootable imager. Below are the applications currently included: - **RECON Imager** Launches the **RECON Imager** application, which allows you to capture images of the booted device. Supports both physical disk imaging and logical user data imaging. - **Legacy RECON**

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Imager Launches the v7 RECON Imager Application. This Application can be useful when the device does not support the latest version of RECON Imager. If the device does not support the latest version, a popup notification will appear notifying you that the Legacy RECON Imager nee - **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.

6.5 Disk Manager



The Disk Manager provides access to all disks currently detected by the system. From this tab, you can perform various actions to view and manage the selected disk. **Decrypt** - Unlocks a locked - FileVault encrypted APFS volume provided either: - Administrator password - FileVault Recovery Key

Format - Formats a drive using one of the following file systems: - APFS (Apple File System) - HFS+ (MacOS Extended Journaled) - ExFat - FAT32 (MS-DOS) - Commonly used to prepare a destination drive for collection

Unmount - Unmounts the currently selected mounted partition or APFS volume

Mount-R - Mounts the selected volume or partition as read-only

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Mount-RW - Mounts the selected volume or partition as read-write

Free Space - Displays the free space available on the selected partition or APFS volume

Refresh - Updates the disk information displayed in the Disk Manager table

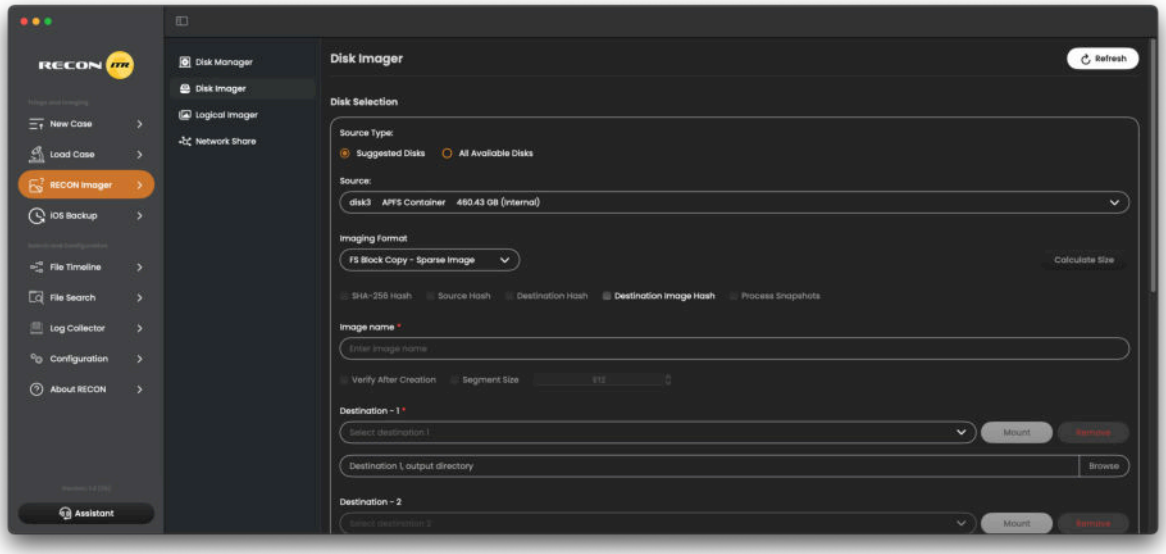
** Disk Arbitration **- Function available in the live environment to prevent macOS from automatically mounting drives. - When** enabled**, macOS** will not auto-mount disks**. Disks will need to be manually mounted through the Disk manager - When** disabled**, macOS** will auto-mount disks**

Notice:

Disk capacities within RECON ITR are displayed using binary units (base-1024) rather than decimal units (base-1000)

RECON ITR incorporates a color-coded system within the Disk Manager to assist examiners in quickly distinguishing between disk types and status conditions. A legend is provided at the bottom of the Disk Manager screen. The color indicators in the table correspond to the following classifications: - **Red** - Mounted as Read/Write - **Green** - Mounted Read-Only - **Orange** - Home APFS Volume - **Dark** Orange - Locked File Vault volume - **White** - Parent disk - **Grey** - Unmounted partition or volume

6.6 Disk Imager



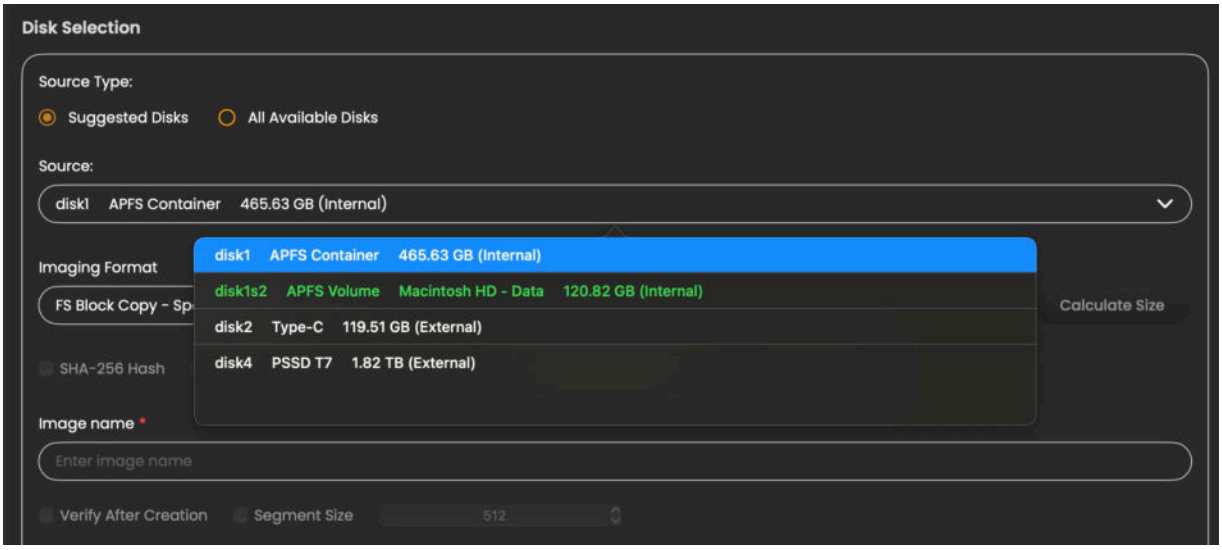
The **Disk Imager** tab allows investigators to create forensic images of both internal and

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

external disks. The ability to acquire a physical image is dependent on the devices hardware: - **Pre-T2 Intel Macs**: Full physical imaging is possible. - **External drives:** 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 (when provided with admin credentials)

6.6.1 Supported Disk Sources



The Source dropdown menu by default will display a list of suggested source disks. The list of suggested disks that appear in the dropdown may vary by device. For example, on T2 Intel Macs and Apple Silicon Macs, the internal physical drives and partitions will be hidden as they are physically encrypted. Should a disk that needs to be imaged not appear in the dropdown, you may press on the **All Available Disks** option. This will display a full list of every disk detected on the system. To see all currently connected devices: - Click the **Refresh** button. - The disk list will update based on devices and disks currently detected.

To visually aid in selecting the source disk, the APFS data volume should be highlighted in Green. Should an APFS volume be locked, the source will be listed in red and marked as “LOCKED”. The selected source will determine the available hashing options and supported image types. This behavior is intentional and ensures compatibility with both Apple Silicon systems and pre-T2 Intel Macs, where physical acquisition is supported.

Notice:

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

Before choosing a source, 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.

6.6.2 Metadata Preservation

Metadata plays an important role in macOS forensic analysis. On APFS volumes, much of this metadata is managed through Spotlight, the macOS indexing system responsible for enabling fast file searches and organizing system metadata. Spotlight stores a large portion of macOS metadata as Apple Extended Attributes. These attributes are maintained within the Spotlight database rather than being stored directly in the file header. As a result, preserving Spotlight metadata is important during forensic acquisition to ensure that investigators retain the most accurate representation of file activity and system information. When performing an acquisition of an APFS volume, **RECON ITR** makes a best effort to preserve Apple Extended Attributes associated with files on the system.

6.6.2.1 Live Environment Metadata Collection

When operating in a live environment, **RECON ITR** creates a database ("**Recon_metadata.sqlite**") that stores the original Apple Extended Attributes associated with each file on the system. This database captures the metadata directly from macOS, preserving the extended attribute information as it exists on the device. This database will reside inside the case folder but outside of the forensic image. Storing this information separately allows **RECON LAB** to interpret Apple Extended Attributes without relying on reverse engineering of the Spotlight database. This approach helps reduce the risk of misinterpreting Spotlight metadata during forensic analysis. The metadata database created during acquisition is later processed by **RECON LAB**, allowing investigators to view and analyze the preserved Apple Extended Attributes. This metadata preservation process is performed only during live acquisitions and is not able to performed when operating in the bootable environment.

6.6.3 Supported Source Options by Mac Type

The available acquisition targets in **RECON ITR** vary based on the selected device. This is due to hardware-level security protections present in certain Mac systems. Apple Silicon Macs (M-series) and Intel Macs equipped with the T2 Security Chip use Secure Enclave technology, which prevents physical imaging of the internal storage. As a result, physical disk acquisition is not possible on these systems. Instead, logical acquisition targets, such as

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Synthesized APFS Containers or APFS Data Volumes, must be selected. On Intel Macs without T2 protection, physical imaging of the internal drive remains possible and is the preferred acquisition method. Because of these architectural differences, the supported sources and recommended acquisition targets will change depending on the device type detected. Always select the highest-level available target in the order listed below for the most complete acquisition possible. **Apple Silicon Macs (M1, M2, M3, 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")

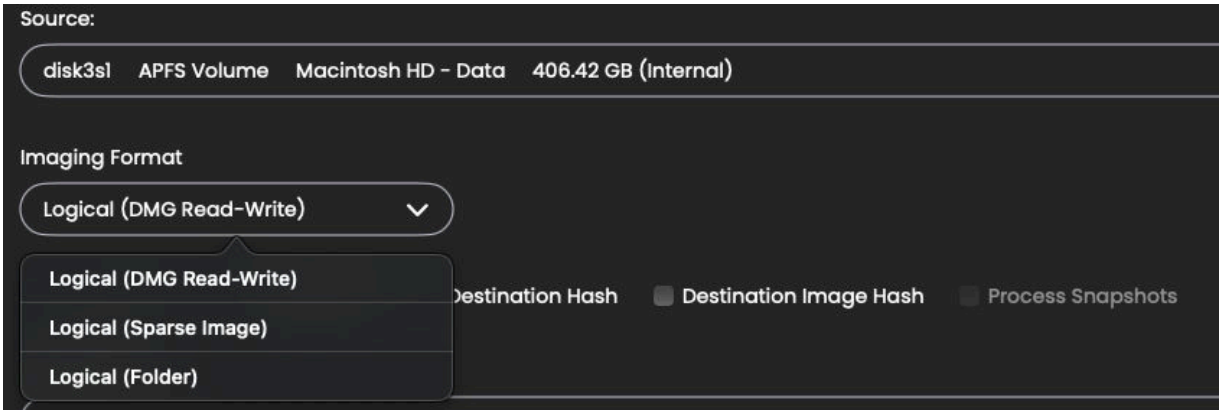
T2 Intel Macs Physical imaging is not possible on T2-protected devices. Preferred targets (in order): 1. Synthesized APFS Container (commonly disk1) 2. APFS Data Volume (commonly disk1s1 — "Macintosh HD - Data")

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) 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 Preferred targets (in order): 1. Physical external drive 2. Partition 3. Synthesized APFS Container 4. APFS Data Volume

6.6.4 Image Type Options



Use the Image Type dropdown menu to select the desired forensic image format. The available image formats will vary depending on the selected acquisition source.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

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.
ASIF	Apple's proprietary dynamic sparse file that is designed to support near native read/write speeds	Only available on devices running macOS26 and later
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.	Mountable on macOS.
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.

6.6.4.1 Image Type Options 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

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

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.

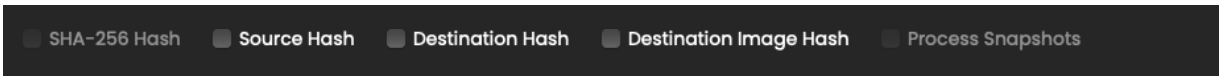
Physical Imaging Limitations: - Due to Secure Enclave protections (T2 and Apple Silicon), physical imaging is no longer possible on most modern Macs.

Formats like E01, DD, and SMART are primarily used only on older Intel-based Macs without Secure Enclave protection.

Notice:

Always consult your agency's policies and case requirements before selecting an image type. Verify that the chosen image format is compatible with your intended forensic tools. Additionally, ensure you have selected the correct source disk, as choosing an incorrect source could result in an unreadable image.

6.6.5 Hashing Options and Source Options



- **Destination Image Hash**
  - Creates a MD5 / SHA1 Hash of the resulting image file
  - Available with the following image formats:
    - FS Block Copy - DMG
    - FS Block Copy - Sparse Image
    - Logical (DMG Read-Write)
    - Logical (Sparse Image)
    - ASIF (Apple System Image)
- **Source Hash**
  - Creates a MD5 / SHA1 Hash of every individual file to be copied on the selected source volume
  - Available with the following image formats:
    - Logical (DMG Read-Write)
    - Logical (Sparse Image)
    - Logical (Folder)
    - ASIF (Apple System Image)

- **Destination Hash**
  - Creates a MD5 / SHA1 Hash of every individual file that is in the forensic image, after it has been imaged over
  - Available with the following image formats:
    - Logical (DMG Read-Write)
    - Logical (Sparse Image)
    - Logical (Folder)
    - ASIF (Apple System Image)
- **SHA256 Hash**
  - The SHA256 hash of the resulting image file will be calculated *(This is In addition to the already provided SHA1 and MD5 hash by default)*.
  - Available with the following image formats:
    - DD (Raw Disk Image)
    - DMG (Disk Image)
- **Process Snapshots**
  - This will compare the selected source volume against selected APFS snapshots to identify files that have been modified or deleted. The files that have been modified and deleted, will be extracted into the snapshot folder and stored inside the case folder for review. The comparisons for each Snapshot will be stored in their respective folder and the data will be broken into two separate files:
    - **Modified:** These entries identify files present in both the Snapshot and the active File System where the file data or metadata has changed.
    - **Deleted:** These entries identify files present within the Snapshot that are no longer present in the active File System.
  - This option is only available when an APFS Volume is selected as the source, and Time Machine must have been set up and running for snapshots to have been created.
  - Available with the following image formats:
    - Logical (Folder)
    - Logical (Sparse Image)

6.6.5.1 Additional Imaging Options

- **Compression Level**
  - This will attempt to compress the forensic image to make the resulting image file smaller. The compression levels available are:
    - **None**: No compression. Fastest imaging.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

        - **Fast**: Minimal compression. Good balance between speed and size.
        - **Best**: Maximum compression. Slower imaging process.
    - Available with the following image formats:
        - EWF (.E01)
        - EWF Extended (.Ex01)
        - EWF Smart (.s01)
- **Segment Size**
    - This allows an image to be broken up into smaller individual files.
    - The segment size may be configured to the desired size (in MB).
    - Available with the following image formats:
        - DD (Raw Disk Image)
        - EWF (.E01)
        - EWF Extended (.EX01)
        - EWF Smart (.s01)
- **Verify After Creation**
    - Performs a verification hash (MD5 and SHA-1) on the output image after acquisition.
    - Available with the following image formats:
        - EWF (.E01)
        - EWF Extended (.Ex01)
        - EWF Smart (.s01)

6.6.6 Destination Drives

Before creating a forensic image, you must select a destination drive where the image will be saved. This ensures sufficient storage space and allows for optional duplication to multiple drives if required. To select a destination drive 1. Click the **Select Destination** dropdown 2. Choose the disk where you want the forensic image to be written - The **RECON Imager Data** partition on the **RECON ITR** drive - A separate external drive.

The dropdown displays the total size of the destination partition and, if mounted, may also show available free space. Up to two destination drives can be selected simultaneously to write the forensic image to multiple drives at once.

6.6.6.1 Mounting the destination drive

- 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 ITR** saves images inside a new case folder at the root of the destination drive.

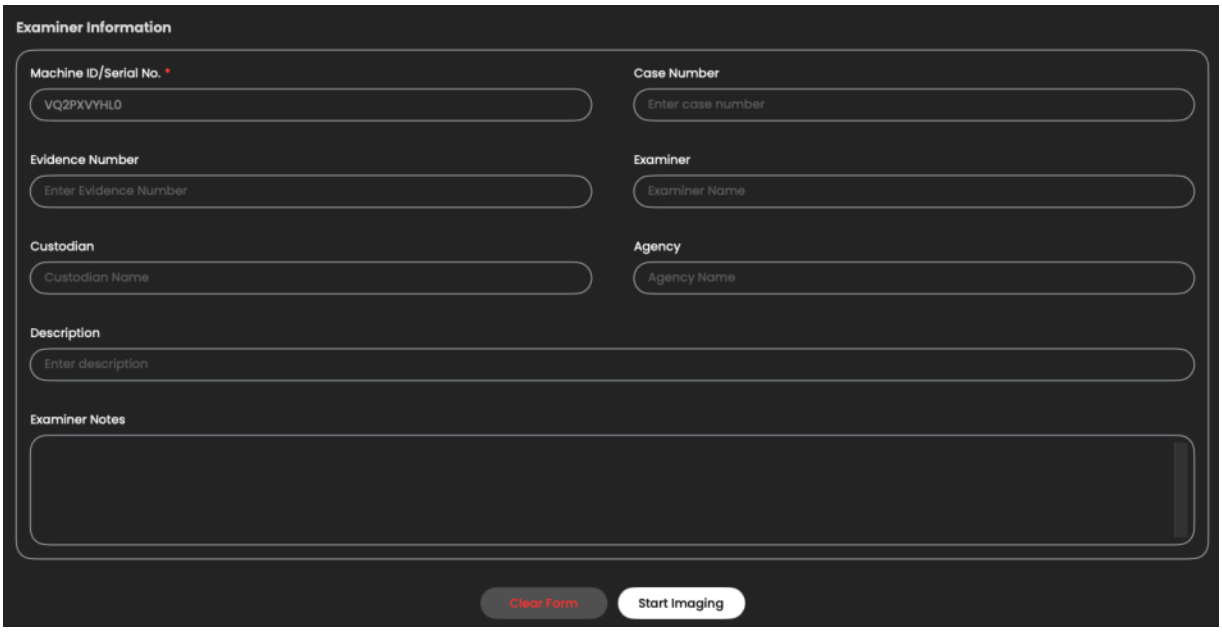
To change the default case folder location: 1. Click **Mount**. 2. Click **Browse**. 3. Navigate to the desired folder where you want the case folder to be created.

6.6.6.2 Writing to multiple destinations

To simultaneously create two copies of the image: 1. Select the **Select Destination 2** dropdown 2. Choose a second destination drive. 3. **RECON ITR** will write the image to both locations during acquisition.

> **Notice:**
>
> When selecting an external destination drive, it is recommended to use a drive that is at least 25% larger than the source. It is also recommended to format the destination drive as HFS+ or APFS.

6.6.7 Case Details



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. This file will be found in the root of the case folder. The **Complete.txt** file records: - The entered Case Details - Imaging start and

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

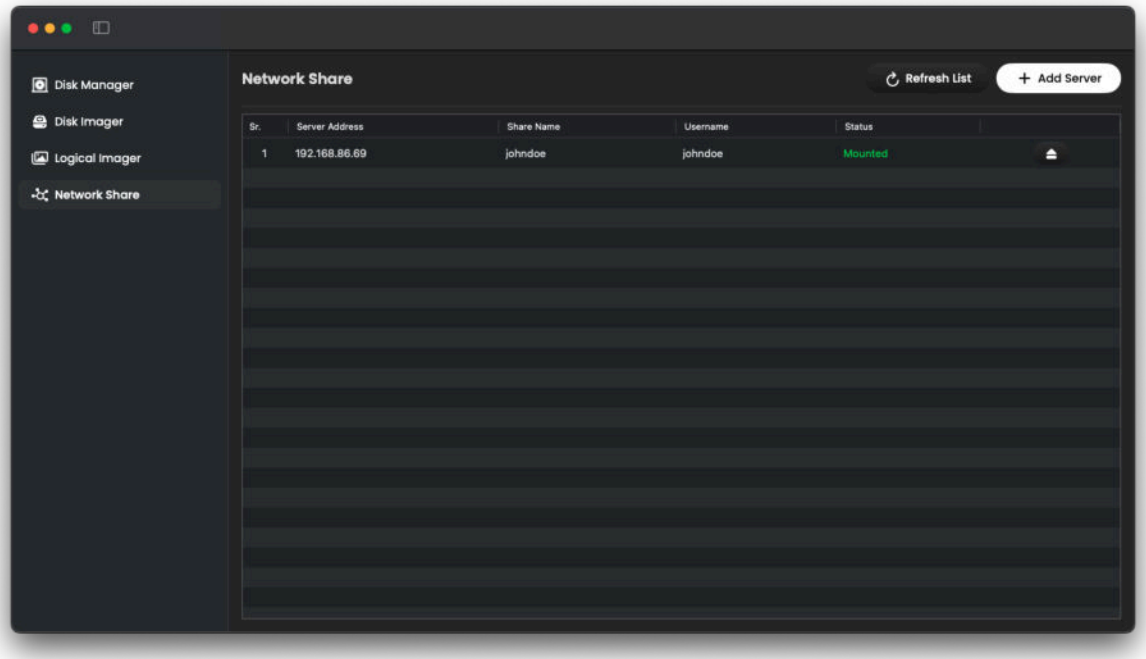
end times - Imaging settings and summary details - The resulting hashes, if enabled

6.6.7.1 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 ID / Serial No (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 (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.

6.6.8 Network Share

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com



The Network Share feature allows you to add a SAMBA (SMB) network drive. Once added, this drive can be used to store your forensic images directly to the network location. - **Refresh List** – Updates the currently connected Network Shares. Use this if a share has been added or removed outside of **RECON ITR**. - **Add Server** – Opens a dialog to connect to a new network share.

6.6.8.1 Add SMB Options

When adding a server, you will need to provide: - **Server Address** – The IP address of the SMB server. - **Share Name** – The exact name of the shared directory on the server. - **Username** – The account name used to log into the SMB share. - **Password** – The password associated with the username.

Add Options: - **Add** – Adds the SMB share for one-time use. The share will not be remembered after closing **RECON ITR**. - **Add and Save** – Adds the SMB share and saves it for future sessions. The share will remain available even after closing and reopening **RECON ITR**.

The Status column in the Network Share table indicates the current state of the SMB share: - **Mounted** – The SMB share is successfully connected and ready for use. - **Connecting…** – The Mac is currently attempting to connect to the SMB share. - **Failed** – The Mac was unable to connect to the SMB share. Check the share name, username, password, and network

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

connectivity.

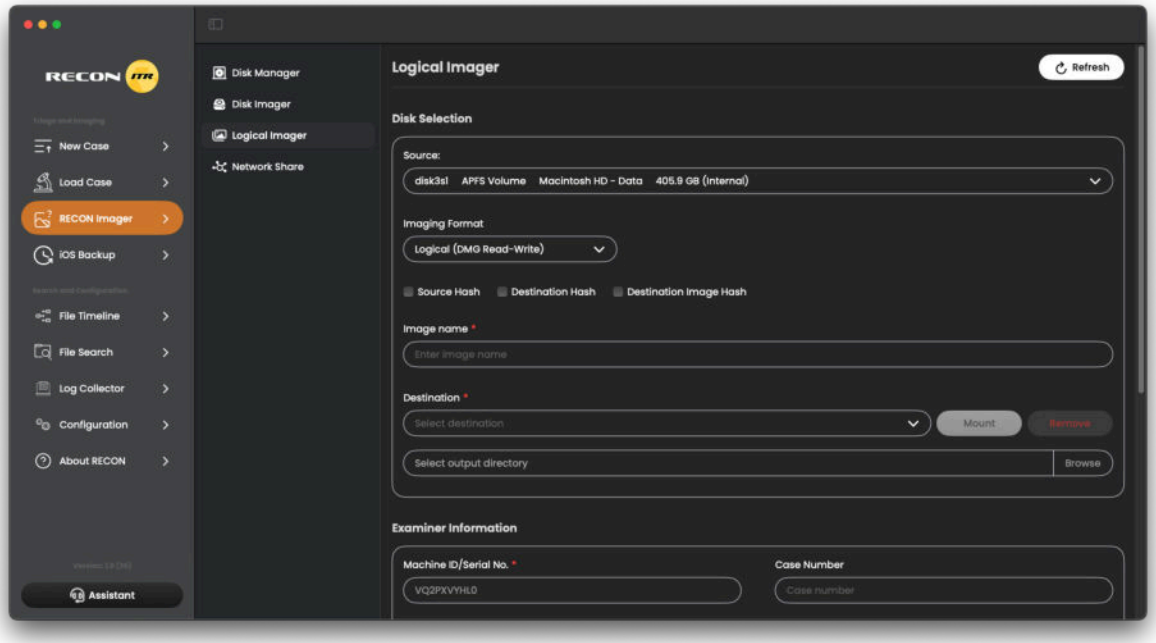
6.6.8.2 Using an SMB Share

Once an SMB share has been added, it can be accessed from the **Destination dropdown** menus in **RECON ITR**. The SMB share will typically appear in the following format: //@/ Example: *//johndoe@192.168.86.69/Documents*

6.7 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

6.7.1 Creating a Logical Imager Case



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

Field	Description
Source Dropdown	Select the disk that the logical acquisition will be of
Imaging Format	This is the forensic image file format the source will be imaged as
Destination Dropdown	Select the disk that the image will be written to.
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.
Evidence Number (Optional)	Enter the evidence tag or number for the device, if applicable.
Custodian (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.

6.7.1.1 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 the volume is locked - If FileVault encryption remains active, a warning will appear notifying you that FileVault is still enabled.

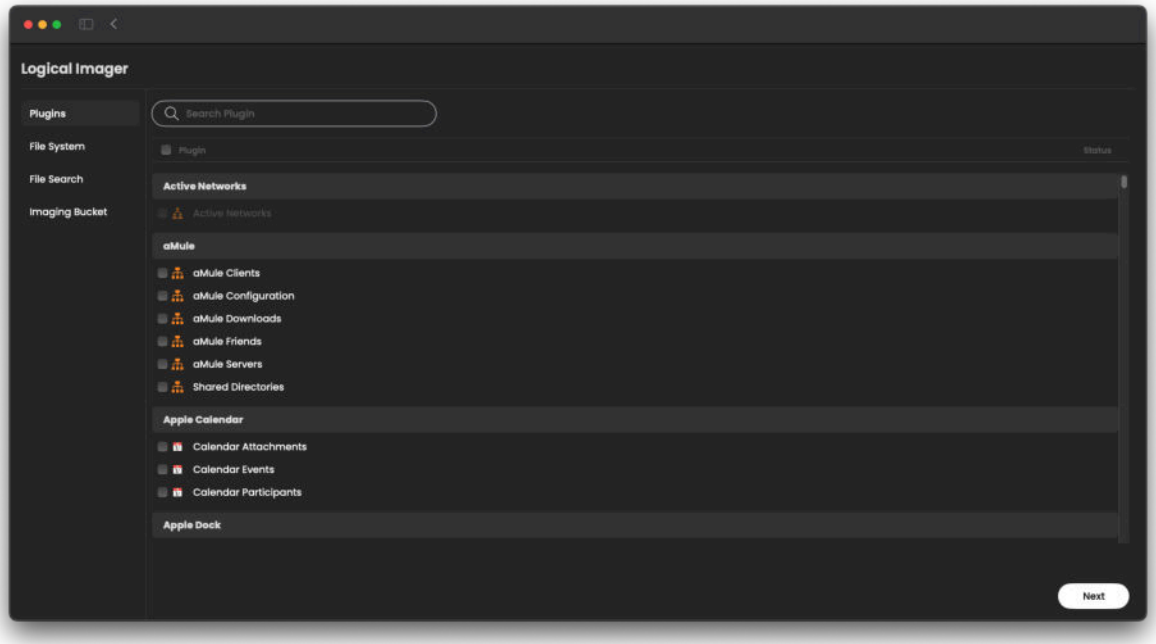
Decrypting FileVault ensures that all targeted files and metadata can be properly accessed and imaged.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Notice:

The Logical Imager is ideal for live environments when imaging only specific user data (e.g., Documents, Downloads, Desktop).

6.7.2 Plugins



The Artifacts Panel is the first tab that you will be started in. It will display a list of artifacts available for logical imaging. When an artifact is selected: - **RECON ITR** attempts to locate 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.

To **Select All Plugins**, press the checkbox at the top located next to Plugin.

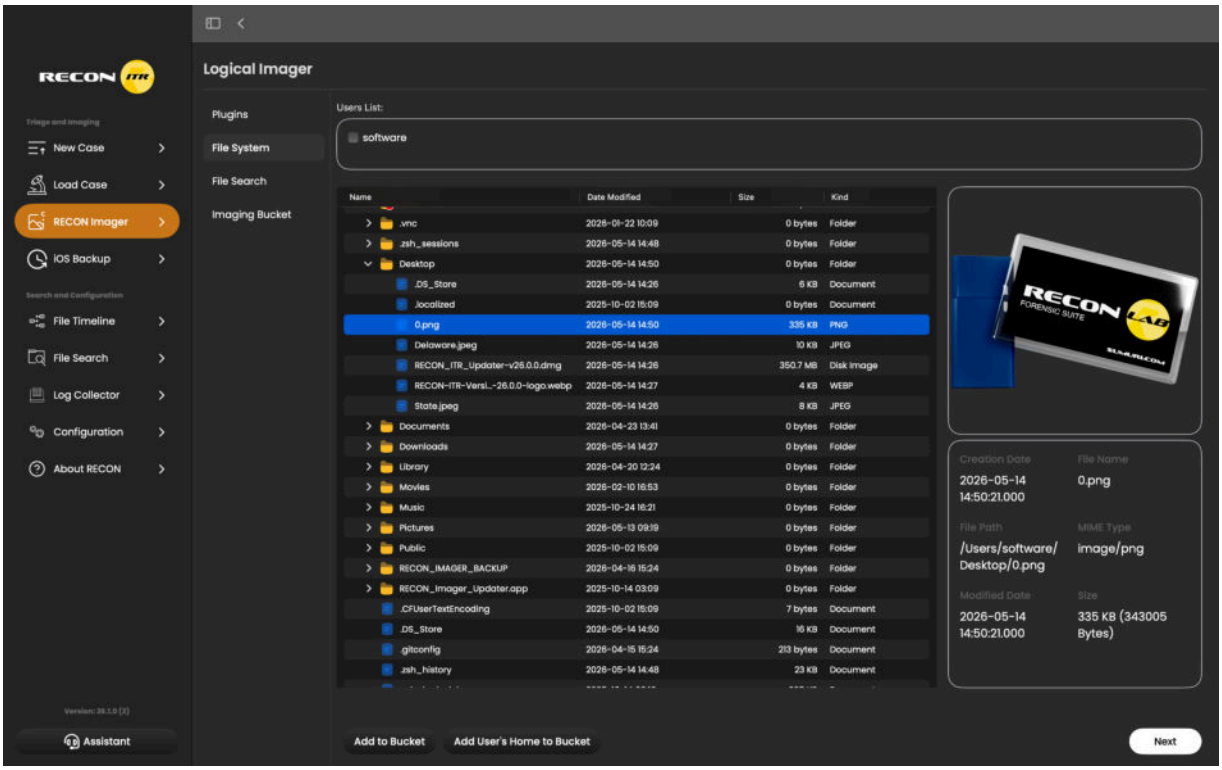
P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Notice:

When the case is run, the selected plugins will only be run against the selected users profile. Users may be selected through the Imaging Bucket.

This allows you to dynamically expand and limit the scope of your investigation

6.7.3 File System View



The File System view will allow you to view the selected source volume or partition. Through this window you are able to add individual files and directories to the imaging bucket. Files added to the imaging bucket will be captured when the acquisition process is started. **To add a file or folder to the imaging bucket**: 1. Select the desired directory or file 2. Press on "**Add to Bucket**" 3. The item will now appear in the Imaging Bucket

To add the users home directory: 1. Select the checkbox next to the users name in the **Users List** 2. Press on "**Add User's Home to Bucket**" 3. This will now add the users profile to the Imaging Bucket

Once the desired files and folders have been added to the bucket, the Next button may be pressed to proceed to the next step.

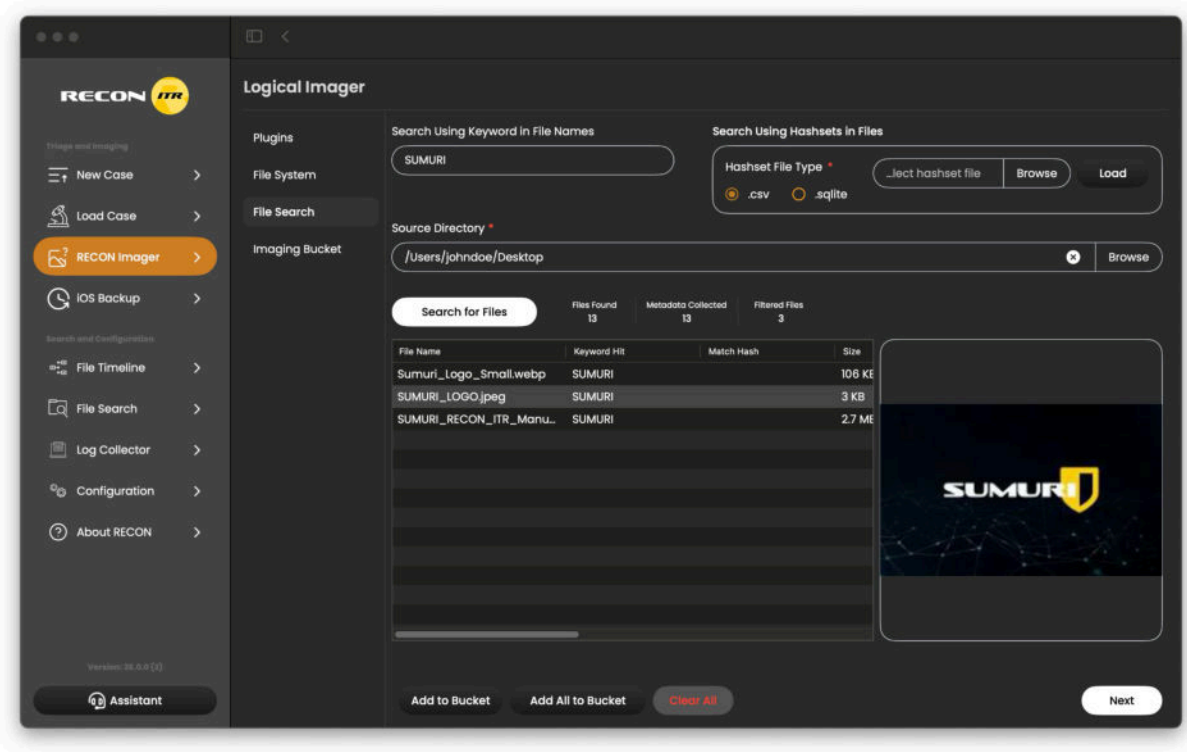
P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Notice:

When executing RECON ITR within a live environment as a Standard User with the Data Volume selected as the source, the File System view will default to the root of the User's Home Directory rather than the Data Volume root. This behavior is due to macOS permission structures preventing non-administrative accounts from accessing protected system and cross-user directories.

Files or directories labeled with a red "-" symbol indicate an "Access Denied" state, signifying that the current user context lacks the necessary privileges to read or traverse that specific path.

6.7.4 File Search



- File Name (filename or extension)
- Hash Value (MD5 or SHA1 hash using a loaded hashset)

Files found through File Search can be added to the Imaging Bucket, which contains the list of

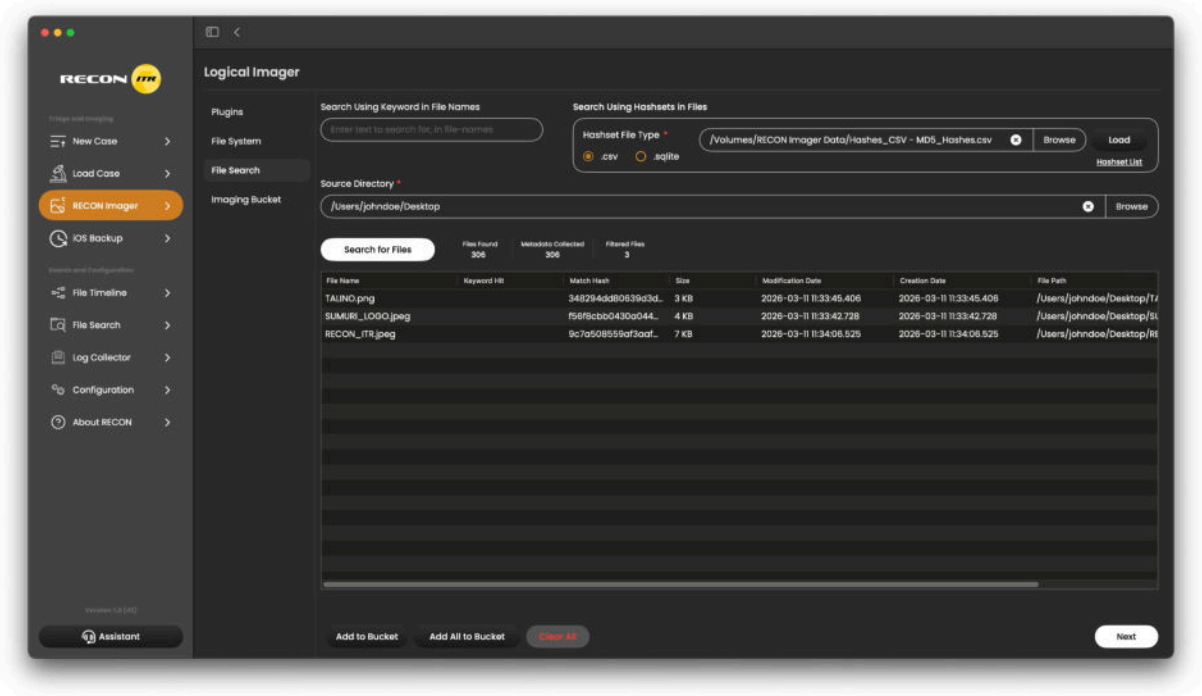
P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

all files and paths that will be imaged.

6.7.4.1 The key areas of the File Search Tab

Button	Description
“Add to Bucket”	Adds the currently 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.
“Clear All”	Clears all of the selected filters and directories Please note, this option does does not remove added items from the bucket

6.7.4.2 To search with Hashset



The Hash Set Search feature allows examiners to identify files on a system by comparing file hashes against a provided list of known hash values. This feature supports searching for files based on **MD5** or **SHA1** hashes. Hash lists can be provided in either CSV or SQLite file formats. Once a hash set is loaded, **RECON ITR** will calculate the hashes of files within the selected directory and compare them against the hashes contained in the provided file. **RECON ITR** performs this comparison as a whitelist search, meaning it attempts to locate

files whose hashes match those contained in the provided hash set.

Supported Hash Set Formats

The Hash Set Search feature supports the following formats: - **CSV** – A comma-separated file containing **MD5** or **SHA1** hashes. - **SQLite** – A database file containing stored hash values.

For the hash set to be recognized correctly, the column name containing the hashes must match the selected hash type: - **MD5** hashes must be stored in a column named “**MD5**”. - **SHA1** hashes must be stored in a column named “**SHA1**”.

Loading and Managing Hash Sets

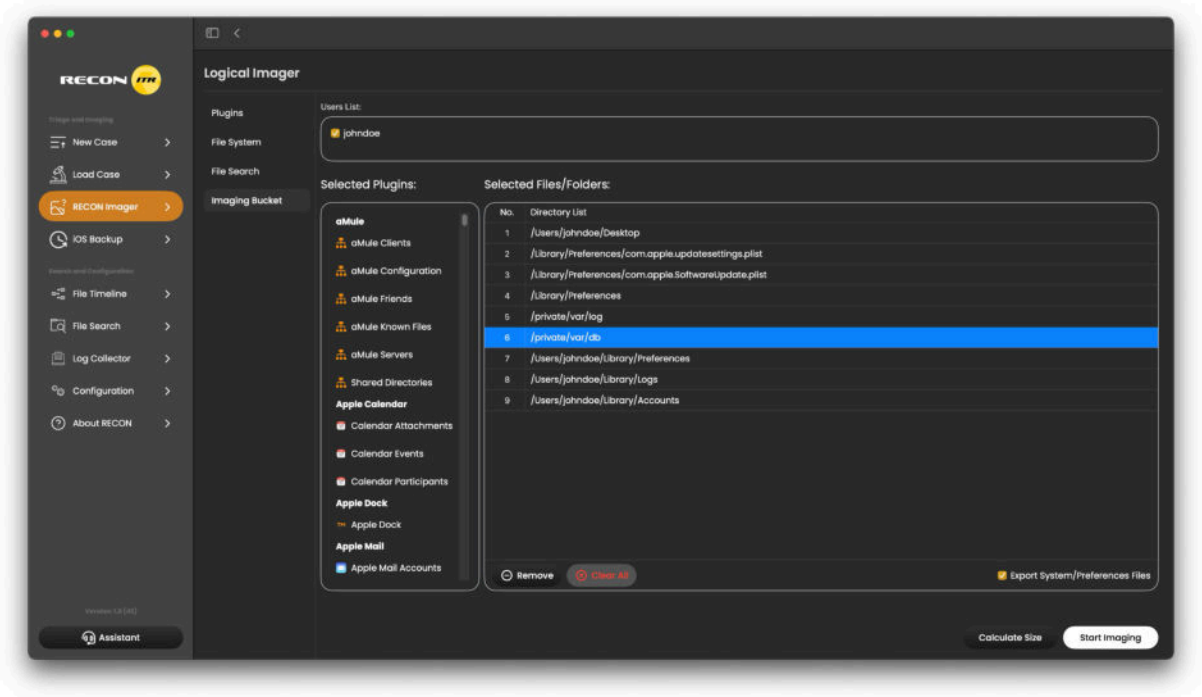
To begin using the feature, a hash set must first be loaded into **RECON ITR**. After selecting the hash set format and browsing to the desired file, press Load. Once loaded, the hash set will be added to the Hash Set List, and a Hash Set List button will appear in the interface. The Hash Set List allows examiners to manage loaded hash sets. From this menu, hash sets can be added or removed as needed. **RECON ITR** supports loading multiple hash sets simultaneously, allowing files to be compared against several hash lists during a single search.

Performing a Hash Set Search

To perform a hash set search: 1. Navigate to the File Search tab within the Logical Imager. 2. Select the hash set format (CSV or SQLite). 3. Click Browse and navigate to the file containing the hash list. 4. Click Load to import the hash set into **RECON ITR**. 5. Set the Source Directory that you want to search. 6. Click Search for Files to begin the hash comparison process. 7. Any files whose hashes match entries in the provided hash set will

appear in the search results and can be added to the Imaging Bucket if desired.

6.7.5 Imaging Bucket



The **Imaging Bucket** within the **Logical Imager** provides an overview of the items that have been selected for acquisition. It allows examiners to review users, plugins, and specific files or folders that will be included in the forensic image before the imaging process begins. Several tabs and controls are available within the **Imaging Bucket** to help manage the acquisition scope.

6.7.5.1 User List

The User List displays all user accounts detected on the selected volume. These users may be referenced by various plugins or artifact collections during the imaging process.

6.7.5.2 Selected Plugins

The Selected Plugins tab displays a list of all plugins that are currently active for the acquisition. These plugins represent artifact collections that **RECON ITR** will attempt to acquire from the system. Plugins cannot be deselected from within the **Imaging Bucket**. To modify plugin selections, examiners must navigate to the Plugins tab, where plugins can be enabled or disabled.

6.7.5.3 Selected Files / Folders

The Selected Files / Folders tab displays files and directories that have been manually added

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

to the **Imaging Bucket**. Items may be added from either the File System View or the File Search View. The following controls are available within this section: - **Remove** – Removes the currently selected file or folder from the Imaging Bucket. - **Clear All** – Removes all files and folders currently listed in the bucket. - **Export System** / **Preference Files** – Automatically adds common system log paths and user preference paths to the Imaging Bucket for any users currently selected in the User List.

6.7.5.4 Imaging Controls

Two primary controls are available to prepare and begin the acquisition process: - **Calculate Size** – Calculates the estimated size of the selected data and provides an approximation of how much space will be required on the destination drive. - **Start Imaging** – Begins the forensic acquisition process using the selected plugins, files, and folders currently listed in the **Imaging Bucket**.

6.8 Shutdown - (Boot Only)

When using the bootable 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.

6.9 About RECON - (Boot Only)

When using the bootable Imager, you may also see an **About RECON** 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 - View acknowledgements

Note: It is important to review the EULA to understand the usage rights, restrictions, and

responsibilities associated with using **RECON ITR**.

6.10 Disk Arbitration - (Boot Only)

The bootable Imager includes a built-in Disk Arbitrator tool. This may be accessed through the top right system bar. This Disk Arbitrator service will only be available for Intel Macs. The Disk Arbitrator controls how volumes are mounted, overriding the macOS system's default disk handling behavior to help maintain evidence integrity.

6.10.0.1 Key Details

- **Supported Macs**:
  - Supported when imaging Intel-based Macs.
  - Not supported when imaging Apple Silicon (M1, M2, M3, etc.) Macs.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

- **Default Behavior:**
  - Disk Arbitrator is enabled by default when the bootable imager loads.
- **Accessing Disk Arbitrator:**
  - Click the green or blue disk icon located in the top-right corner of the system bar.
  - From here, you can enable or disable Disk Arbitrator as needed.

6.10.0.2 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)

Notice:

This chapter about Disk Arbitration is only for the Disk Arbitration running as a background service in the bootable imager for when imaging Intel Macs.

Please see the Disk Manager Chapter for assistance using the Disk Arbitrator in the Disk Manager window for Live acquisition.

6.11 Files and Directories Created in an Imager Case

When a case is created, **RECON ITR** may create metadata files outside of the forensic image to help document the provided case details and hashes. A few files that may be found inside of a **RECON** Case folder are:

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

File / Directory Name	Description
_Complete.txt	Documents 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. Documents SHA256 hash if “SHA-256” was selected
Hash CSVs (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. The 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.
Recon_metadata.sqlite	An SQLite database created during logical acquisitions to preserve and document the original Apple Extended Attributes directly from the Mac.

Notice:

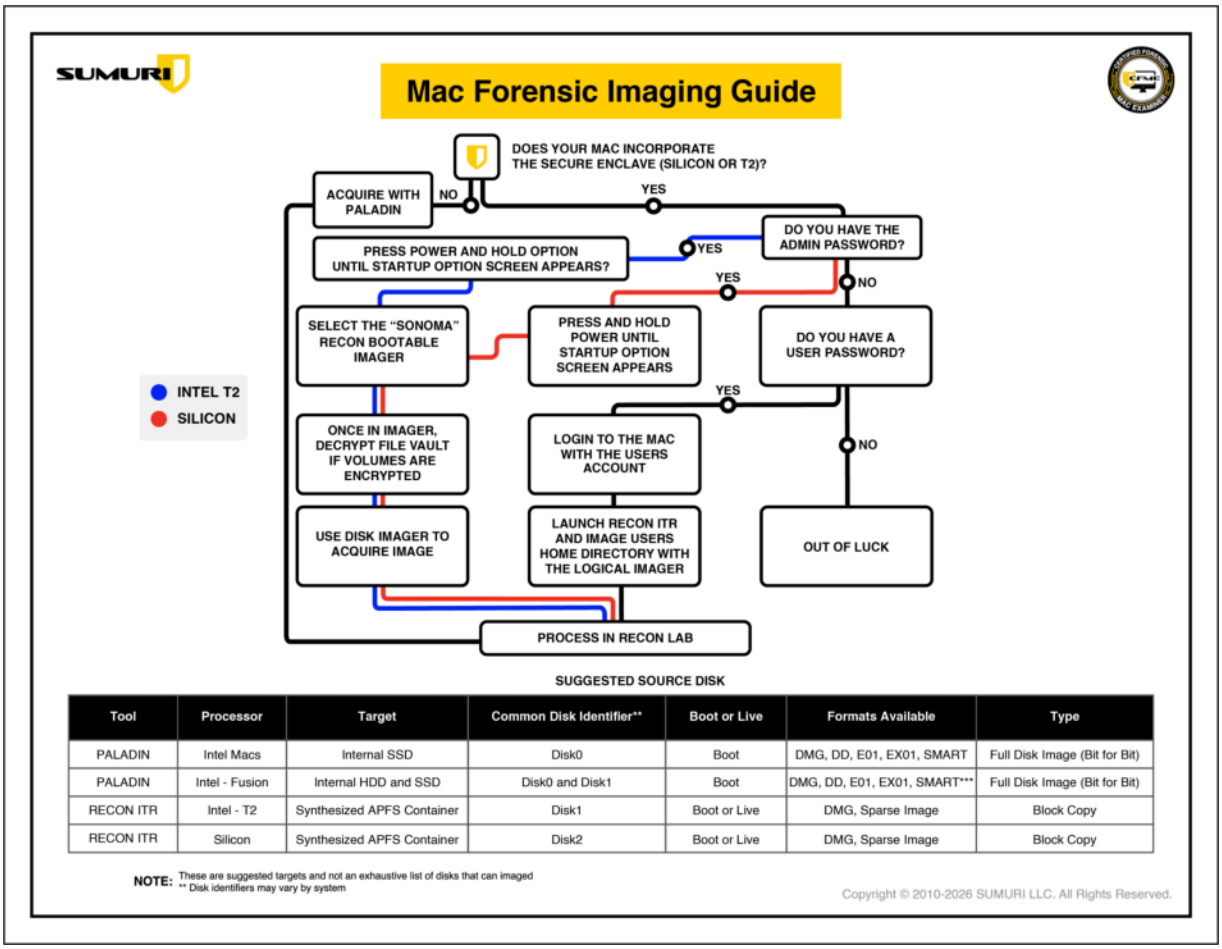
After RECON ITR has completed the forensic image, the forensic image file will be locked. Locking the image protects the integrity of the forensic evidence while preserving chain of custody by preventing accidental access or deletion.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

7 Imaging Guidelines

The following instructions are intended to serve as a general baseline for using the Imager built into **RECON ITR**. 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.

7.0.0.1 Mac Forensic Imaging Guide



Tool	Processor	Target	Common Disk Identifier**	Boot or Live	Formats Available	Type
PALADIN	Intel Macs	Internal SSD	Disk0	Boot	DMG, DD, E01, EX01, SMART	Full Disk Image (Bit for Bit)
PALADIN	Intel - Fusion	Internal HDD and SSD	Disk0 and Disk1	Boot	DMG, DD, E01, EX01, SMART***	Full Disk Image (Bit for Bit)
RECON ITR	Intel - T2	Synthesized APFS Container	Disk1	Boot or Live	DMG, Sparse Image	Block Copy
RECON ITR	Silicon	Synthesized APFS Container	Disk2	Boot or Live	DMG, Sparse Image	Block Copy

7.0.0.2 Pre-Imaging Preparation:

Prior to initiating the imaging process, take a few moments to verify that both your software and hardware are properly prepared. Completing these preliminary checks helps ensure a smooth acquisition process and reduces the risk of errors or incomplete images. - **Confirm Software Version:** Ensure that **RECON ITR** is updated to the latest version. Running the most current release ensures compatibility with supported macOS versions and hardware and

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

provides the latest fixes and improvements. - **Test System Verification:** Verify functionality on a non-evidence test system before deploying in the field. This confirms that the startup disk, external drives, and imaging workflow are operating as expected. - **Tool Familiarization:** Review the **RECON ITR** manual and ensure you have a clear understanding of the imaging workflow before use. Examiners should be familiar with the available source disk options and understand how source selection may impact the scope and results of the acquisition.

7.1 Bootable Imaging

Bootable imaging involves shutting down the Mac, powering it on, and selecting a bootable **RECON ITR** startup disk as the Startup Disk. This allows a forensic image to be acquired outside of the live operating system environment. When booted from a **RECON ITR** startup disk, the device operates offline and is not connected to a network by default. If FileVault is enabled and the device is shut down, the disk will be in a FileVault-locked state. An administrator password or the FileVault recovery key must be provided to acquire a decrypted image.

7.1.1 Pre-Imaging Preparation

Power State Verification: Confirm that the target Mac (the device to be imaged) is completely powered off before beginning the bootable imaging process. Ensure the system is fully shut down and not merely logged out, asleep, or with the display turned off.

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 .*
        - After adjusting settings, shut down the Mac.

3. **Boot into Startup Options**
    - **Apple Silicon Macs**: Press and hold the power button until you see "Loading startup options…".

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

- **Intel Macs**: Press the power button, then immediately hold the Option key while the device starts up.

4. **Select RECON Bootable Imager**
   - When the Startup Disks appear choose the **RECON 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**
   - **Intel Macs:** From the , select the **RECON Imager** application and click "**Continue**".
   - **Apple Silicon Macs:** Login to one of the listed Admin accounts

7. **Start RECON Imager**
   - When the **RECON Imager** Splash Screen appears press on "**Start**"

8. **Check FileVault Status**
   - When the screen loads:
     - Check if the target volume shows active FileVault encryption (look under the Encrypted column).
     - If FileVault is enabled:
       - Select the encrypted volume.
       - Click "**Decrypt**".
       - Enter an Admin password or the FileVault Recovery Key. For full instructions, see .

9. **Start Imaging**
   - Click the tab.

10. **Select Source Disk**
    - When the **Disk Imager** screen loads:
      - Click the Source dropdown.
      - Select the source drive, container, or volume to image. For guidance, see .

11. **Select Image Format**
    - In the Image Type dropdown, choose your preferred forensic image format. For options, see .

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

12. **Configure Hashing (*Optional*)**
    - Select any desired hashing options (e.g., Destination Image Hash, Source Hash). For more details, see .

13. **Enter Image Name**
    - Enter the required “**Image Name**” for the forensic image file.

14. **Select Destination Drive**
    - Use the Destination-1 dropdown to select the destination drive. For instructions, see .

15. **Enter Case Details**
    - Optionally, fill out the Case Number, Examiner, Evidence Number, Custodian Name, Description, and Notes fields.

16. **Start Imaging Process**
    - After verifying all selections, click “**Start Imaging**”.
    - A confirmation window will appear — click “**Continue**” to begin the imaging process.

7.2 Live Imaging with Admin Credentials

Live imaging as an admin is performed while the Mac remains powered on and logged in to an admin account. **RECON ITR** runs within the active macOS environment to acquire the forensic image without shutting down or rebooting the system. Because acquisition occurs within the live operating system, certain files and directories may be protected by macOS privacy controls. When administrator credentials are available, it is strongly recommended to grant **RECON ITR Full Disk Access**. This allows the application to access protected system locations and user data that would otherwise be restricted. If FileVault is enabled and the user is logged in, the disk is already in an unlocked state.

7.2.1 Pre-Imaging Preparation

Live Environment Preparation: When performing imaging in a live environment, confirm that the currently logged-in user has administrative privileges. This ensures that **RECON ITR** has the necessary permissions to access all relevant files and system areas. Attempting to image from a non-admin account may result in incomplete data acquisition or restricted access to protected directories. **Full Disk Access**: Ensure that **RECON ITR** has been granted Full Disk Access in the macOS Security & Privacy settings. Without this permission, certain protected files and system directories may be inaccessible during live imaging, potentially resulting in an incomplete acquisition. Verifying Full Disk Access before starting the imaging process helps

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

guarantee comprehensive data collection.

7.2.2 Live Imaging with Admin Credentials 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 .

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 .

4. **Launch RECON ITR**
    - Launch the **RECON ITR** application.
    - When prompted to "**Grant Administrative Privileges**", enter your Admin credentials.

5. **Open RECON Imager**
    - On the **RECON ITR** splash screen, click the **RECON Imager** button.
    - Press on "**Start**" to launch **RECON Imager**

6. **Select Source Disk**
    - When the **Disk Imager** screen loads:
        - Click the Source dropdown.
        - Select the source drive, container, or volume to image. For guidance, see .

7. **Select Image Format**
    - In the Image Type dropdown, choose your preferred forensic image format. For options, see .

8. **Configure Hashing (*Optional*)**
    - Select any desired hashing options (e.g., Destination Image Hash, Source Hash). For more details, see .

9. **Select Destination Drive**
    - Use the Destination-1 dropdown to select the destination drive. For

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

instructions, see .

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**
    - After verifying all selections, click “**Start Imaging**”.
    - A confirmation window will appear — click “**Continue**” to begin the imaging process.

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

If the target Mac is already powered on and a user is logged in, but administrator credentials are unavailable, you can still acquire a forensic image of that user’s home directory. Because this method does not use an admin account, access is limited to files and directories that the logged-in user can read. Protected system locations and other users’ data will remain inaccessible, and a full disk acquisition is not possible. This approach is suitable for capturing the logged-in user’s accessible data only. It does not provide a complete forensic image of the entire system or all users’ data.

7.3.1 Pre-Imaging Preparation

Credentials: When performing imaging in a live environment **without administrator credentials**, confirm that no known administrative account credentials are available for the system. **RECON ITR** will operate with the privileges of the currently logged-in user, which may restrict access to certain protected files, system areas, and user directories.

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. **Launch RECON ITR**
    - Open the **RECON ITR** application.
    - When prompted to “**Enable Full Disk Access**”, click “**Skip**”
    - When prompted to “**Grant Administrative Privileges**”, click “**Skip**”

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

3. **Access RECON Imager**
    - On the **RECON ITR** splash screen, click the “**RECON Imager”** button.
    - When the “**RECON Imager**” splash screen appears, click on “**Start**”
4. **Switch to Logical Imager**
    - Click the “**Logical Imager**” tab.
5. **Select Source Volume**
    - From the “**Source”** dropdown, select the APFS Data Volume.
6. **Select Image Format**
    - In the “**Imaging Format**” dropdown, choose your preferred forensic image format. For options, see .
7. **Configure Hashing (*Optional*)**
    - Select any desired hashing options (e.g., Destination Image Hash, Source Hash). For more details, see .
8. **Enter Image Name**
    - Enter the required “**Image Name**” for the logical image file.
9. **Select Destination Drive**
    - From the “**Destination**” dropdown, choose the drive where you want to save the logical image. For drive preparation details, see .
10. **Enter Case Details (Optional)**
    - Optionally fill out Case Number, Examiner, Evidence Number, Custodian Name, Description, and Notes.
    - Once completed, press on “**Next**”
11. **Access the File System Tab**
    - Once the “**Logical Imager**” has loaded, press on the “**File System**” tab
12. **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.
13. **Configure Imaging Bucket**
    - Click the “**Imaging Bucket**” tab.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

- Confirm that the user's home directory path has been added.

14. **Start Imaging Process**
    - Review all selections carefully.
    - Click “**Start Imaging**”.
    - Confirm your choices by clicking “**Continue**” when prompted to begin the imaging process.

7.4 Imaging in Target Disk Mode

Target Disk Mode allows an Intel-based Mac to be mounted as an external disk on another Mac, enabling direct access to its storage for forensic imaging. This method works for Intel Macs with or without a T2 Security Chip and provides a straightforward way to acquire a full disk image without booting the target system into a separate environment.

7.4.1 Pre-Imaging Preparation

Verify macOS Version: Ensure that the examiner Mac is running a newer version of macOS than the target Mac. Using a newer OS on the examiner system provides the best compatibility and reduces the risk of errors when mounting and imaging the target disk. **Grant Full Disk Access:** Confirm that the **RECON ITR** application on the examiner Mac has Full Disk Access in the Security & Privacy settings. This is necessary to ensure the application can read all areas of the target disk once it is mounted. **Confirm FileVault or Admin Credentials:** If FileVault is enabled on the target Mac, make sure that either the FileVault password or an administrator password is known. Without these credentials, it will not be possible to acquire a decrypted, full disk image of the target system.

7.4.2 Target Disk Mode Imaging Procedure

7.4.2.1 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.

7.4.2.2 Examiner Mac Setup (Mac Running RECON ITR)

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

7.4.2.3 Imaging Process

1. **Check FileVault Status**
    - When the screen loads:
        a. Check if the target volume shows active FileVault encryption (look under the Encrypted column).
        b. If FileVault is enabled:
            i. Select the encrypted volume.
            ii. Click "**Decrypt**".
            iii. Enter an Admin password or the FileVault Recovery Key. For full instructions, see .
2. **Start Imaging**
    - Click the tab.
3. **Select Source Disk**
    - When the **Disk Imager** screen loads:
        a. Click the Source dropdown.
        b. Select the source drive, container, or volume to image. For guidance, see .

4. **Select Image Format**
    - In the Image Type dropdown, choose your preferred forensic image format. For options, see .

5. **Configure Hashing (*Optional*)**
    - Select any desired hashing options (e.g., Destination Image Hash, Source Hash). For more details, see .

6. **Enter Image Name**
    - Enter the required “**Image Name**” for the forensic image file.

7. **Select Destination Drive**
    - Use the Destination-1 dropdown to select the destination drive. For instructions, see .

8. **Enter Case Details**
    - Optionally, fill out the Case Number, Examiner, Evidence Number, Custodian Name, Description, and Notes fields.

9. **Start Imaging Process**
    - After verifying all selections, click “**Start Imaging**”.
    - A confirmation window will appear — click “**Continue**” to begin the imaging process.

7.5 Imaging in Share Disk Mode

Share Disk Mode is a feature available on Apple Silicon Macs that allows the internal storage of one Mac to be accessed by another Mac over a direct USB-C or Thunderbolt connection. This feature can provide access to a target system’s data without booting into its operating system. However, it is primarily intended as a recovery or troubleshooting tool, not a standard forensic acquisition method.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Notice:

Share Disk Mode should be used only as a last resort. It is not recommended for routine forensic imaging because it was not designed for transferring large amounts of data and is significantly slower than other methods, such as bootable or live imaging. Always use direct imaging methods when available, and reserve Share Disk Mode for situations where no other acquisition method is possible.

7.5.1 Pre-Imaging Preparation

Apple Silicon Requirement: Both the target and host Macs must be Apple Silicon models (M1, M2, M3, etc.). Share Disk Mode is not supported on Intel-based Macs, and attempting to use it on incompatible hardware will prevent access to the target Mac's internal storage.
Connection Type: A direct USB-C or Thunderbolt connection must be used between the two Macs. Other connection types are not supported and may result in the target Mac's storage not being recognized.

7.5.2 Target Disk Mode Imaging Procedure

7.5.2.1 Initial Setup

1. **Connect the Devices**
    - Connect the Examiner Mac and the Target Mac (Both Devices must be 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.

7.5.2.2 Setup on the Examiner Mac

1. **Connect RECON Devices**
    - Connect the **RECON ITR** drive to the Examiner Mac.
    - Connect a destination drive if needed for saving the forensic image.

2. **Adjust Power Settings**
    - Configure the Examiner Mac's Energy and Power Settings to prevent sleep

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

or shutdown. ➔ See for instructions.

3. **Grant Full Disk Access**
    - Give the RECON_ITR.app Full Disk Access through: System Settings ➔ Privacy & Security ➔ Full Disk Access. ➔ See for detailed setup.

4. **Launch RECON ITR**
    - Open the **RECON ITR** application.
    - When prompted to "**Grant Administrative Privileges**", enter your admin password

5. **Access RECON Imager**
    - On the **RECON ITR** splash screen, click the "**RECON Imager**" button and then press on "**Start**"

7.5.2.3 Imaging Process

1. **Start Imaging**
    - Click the tab.

2. **Select Source Disk**
    - When the **Disk Imager** screen loads:
        a. Click the Source dropdown.
        b. Select the source drive, container, or volume to image. For guidance, see .

3. **Select Image Format**
    - In the Image Type dropdown, choose your preferred forensic image format. For options, see .

4. **Configure Hashing (*Optional*)**
    - Select any desired hashing options (e.g., Destination Image Hash, Source Hash). For more details, see .

5. **Enter Image Name**
    - Enter the required "**Image Name**" for the forensic image file.

6. **Select Destination Drive**
    - Use the Destination-1 dropdown to select the destination drive. For instructions, see .

7. **Enter Case Details**
    - Enter the required Image Name.

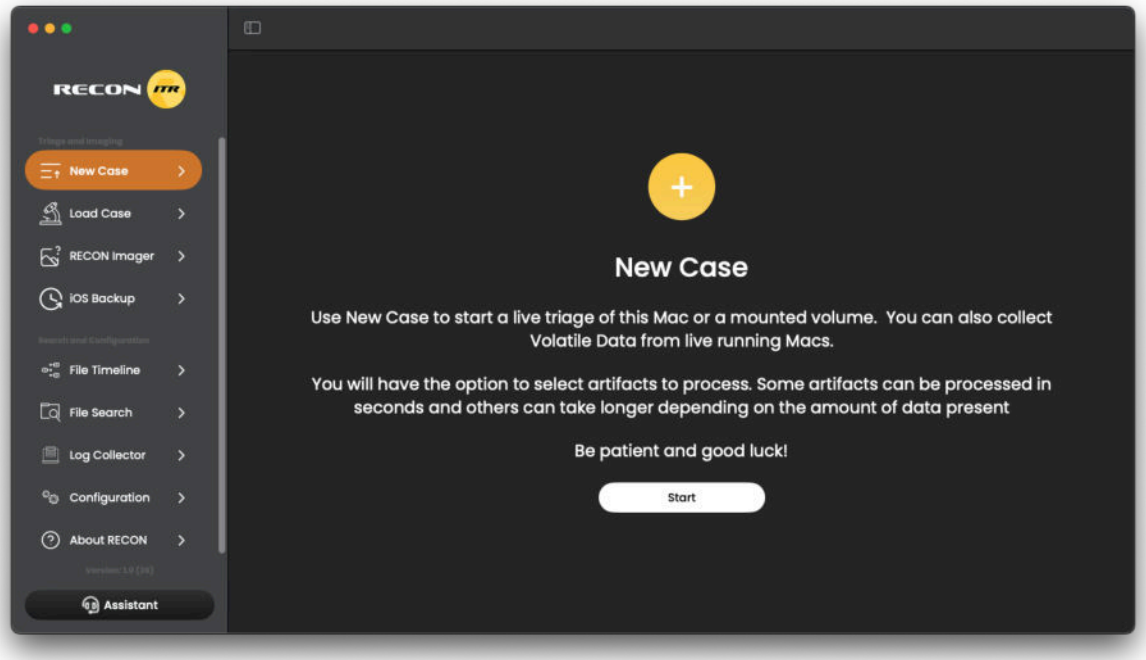
P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

- Optionally, complete the fields for Case Number, Examiner, Evidence Number, Custodian Name, Description, and Notes.

8. **Start Imaging Process**
   - After verifying all selections, click “**Start Imaging**”.
   - A confirmation window will appear — click “**Continue**” to begin the imaging process.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Live Triage



The Live Triage feature allows **RECON ITR** to quickly examine a running macOS system and identify relevant artifacts. It is primarily used to scan and parse commonly used applications and system data, giving examiners a rapid overview of potential evidence without creating a full forensic image. Live Triage is designed for on-site triage, enabling investigators to assess a system's state and collect key artifacts quickly. This approach allows examiners to make informed decisions about further acquisition steps or prioritize evidence collection while minimizing disruption to the live system. In addition to standard application and system artifacts, Live Triage includes volatile plugins that capture data existing only in memory or other temporary locations. These artifacts cannot be recovered from a traditional forensic image, making Live Triage essential for capturing time-sensitive information. A new Live Triage case can be started by selecting **New Case**, which launches the Case Creation Wizard for live analysis. Previously created triage cases can be reopened for review or reporting using **Load Case**.

8.1 Triage Case Creation

The Triage Case Creation Wizard guides examiners through creating a new Live Triage case in RECON ITR . The wizard consists of three pages that help define case details,

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

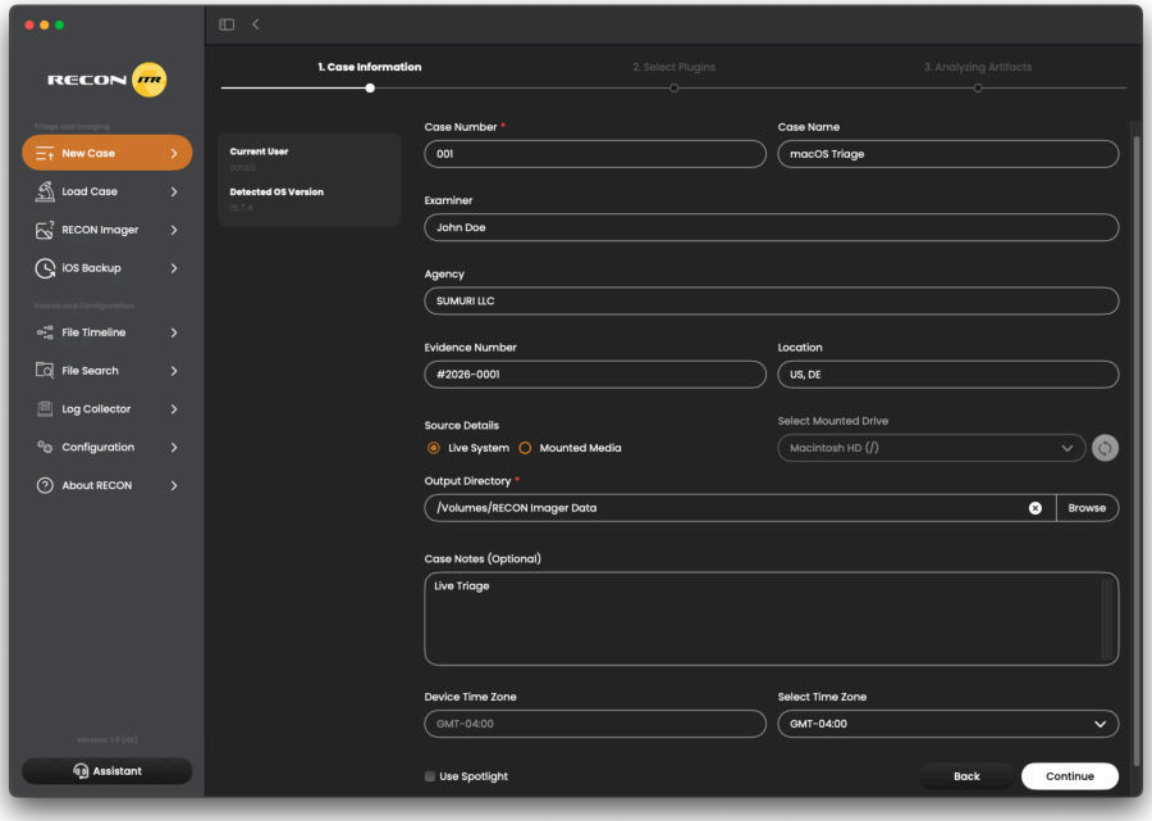
configure plugins, and start processing. These pages include Case Information , Select Plugins and Analyzing Artifacts .

Notice:

Triage can be run as a standard user. However, for the most complete acquisition, it is recommended to: Grant Full Disk Access to RECON ITR Enter your admin password when prompted to “Grant Administrative Privileges”

Doing so allows the tool to access and acquire the maximum amount of data from the system.

8.1.2 Case Information

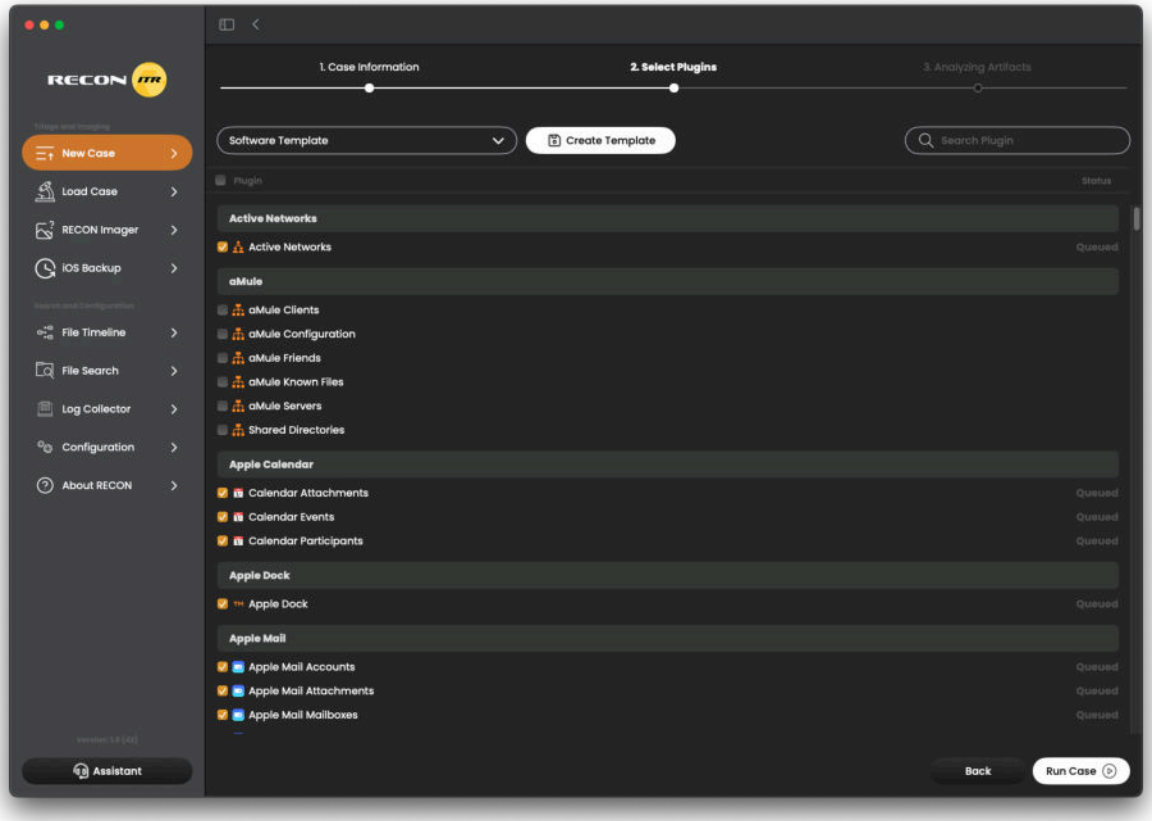


The Case Information screen is the first step in the Triage Case creation process. This screen allows the examiner to enter case metadata and configure settings before initiating the triage process. Within this screen, the examiner must also select a Target Source, which is the device against which the plugins will be executed. The selected source may be either the system currently running **RECON ITR** or a connected external device. A **Time Zone** may also be selected within the Case Information screen. The chosen time zone determines how

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

timestamps are displayed within the tool and ensures that artifact times are interpreted correctly during analysis. By default, the timestamps will be displayed in the live devices Timezone. The **Use Spotlight** configuration option controls how file searches are performed by certain plugins. When enabled, plugins that search for specific file types (such as the Documents plugin) will query the macOS Spotlight index rather than iterating through the entire file system. Using Spotlight often results in faster searches; however, results are limited to files that have already been indexed in the Spotlight database. The **Output Directory** specifies the location where all parsed data generated during the triage process will be stored. When a case is created, **RECON ITR** will automatically generate a case folder within the selected output directory. This case folder contains all collected and parsed artifacts associated with the triage session. The case can later be reopened by selecting **Load Case** from the splash screen interface and choosing the previously created case folder.

8.1.3 Select Plugins



The **Select Plugins** screen allows the examiner to choose which artifacts and data sources **RECON ITR** will analyze during the triage process. Each plugin is designed to identify and parse specific types of forensic artifacts from the selected source device. If an external device is selected as the source, volatile plugins will be automatically disabled. Volatile plugins

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

collect artifacts that are only available from a live system and therefore cannot be executed against offline or external sources.

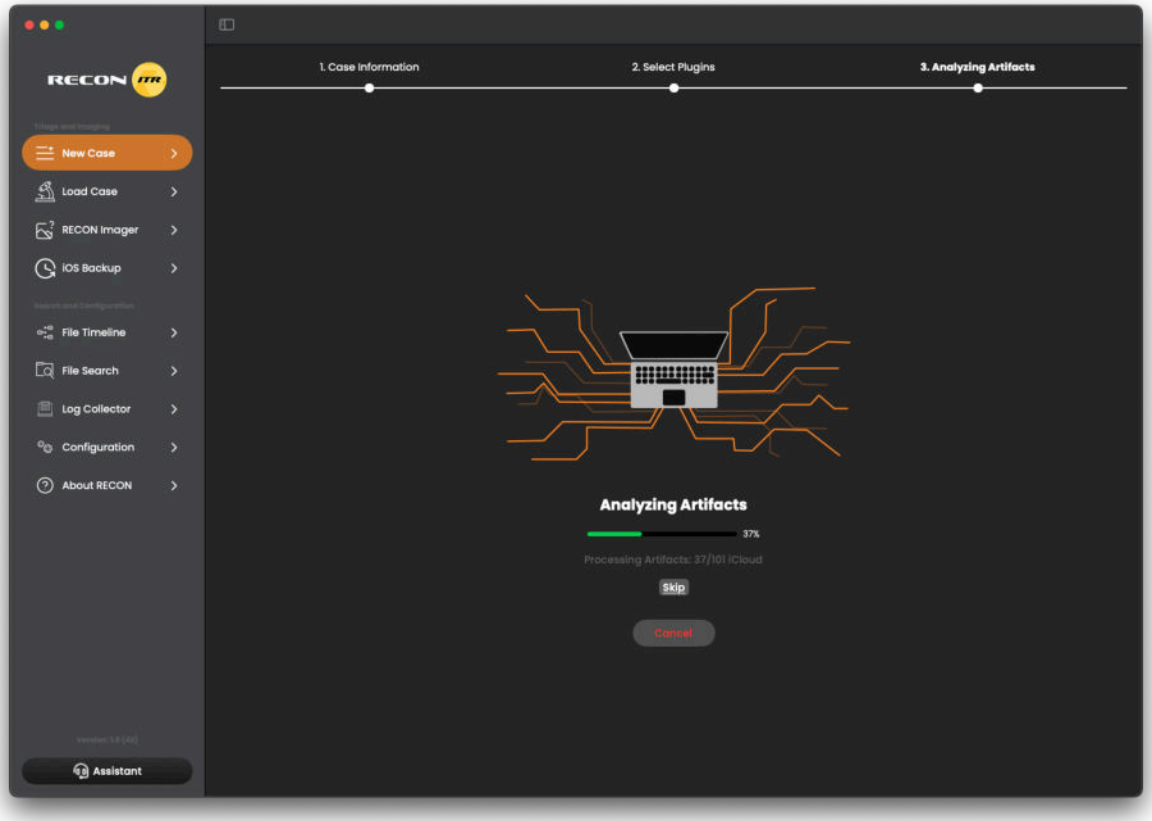
8.1.2.1 Templates

Templates provide a convenient way to quickly select a predefined set of plugins. Once created, templates can be reused across multiple cases, allowing examiners to standardize triage workflows. **To create a template:** 1. Select the desired plugins using the checkbox next to the plugins name. 2. Click “**Create Template”**.

To update an existing template: 1. Select the template from the Template dropdown menu. 2. Modify the selected plugins as needed. 3. Click “**Update Template**”.

Saved templates can be accessed or removed through the Template dropdown menu. Once all desired plugins have been selected, click “**Run Case**” to begin the triage process.

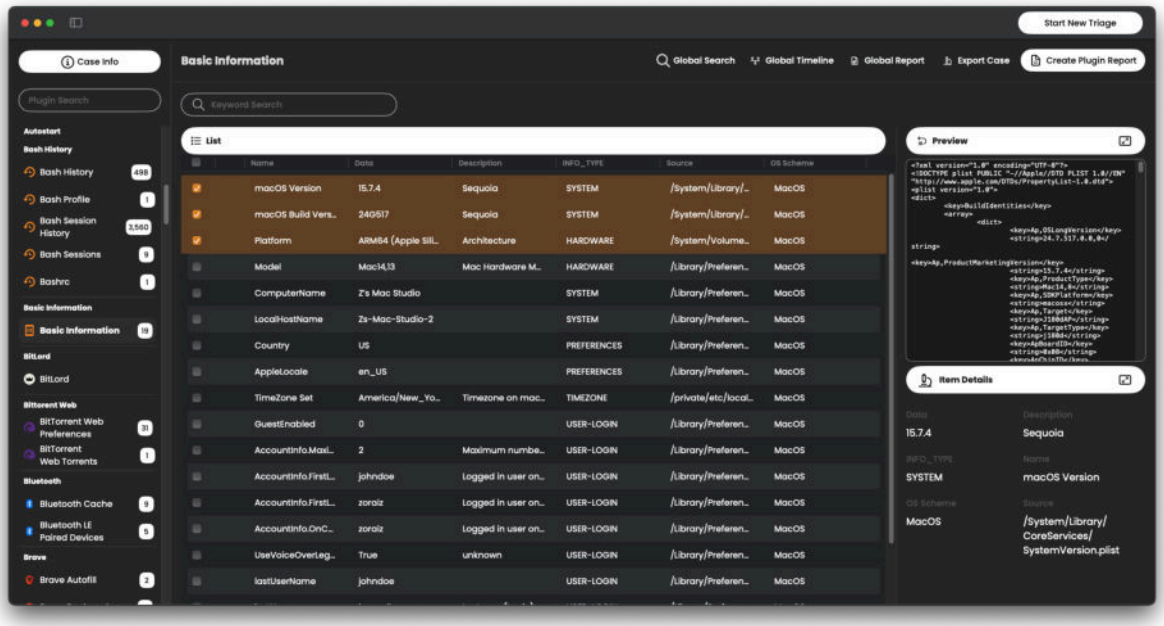
8.1.4 Analyzing Artifacts



The Analyzing Artifacts screen appears after the case has started and plugins are being executed. This window displays the current plugin being processed and provides a live view of the analysis progress. Examiners can monitor the status of each plugin in real time. If

necessary, a plugin can be skipped during processing by selecting the “**Skip**” option, allowing the examiner to continue with the remaining plugins without interruption.

8.2 Triage Result Viewer



The Triage Result Viewer appears once all selected plugins have completed parsing during the Analyzing Artifacts stage. This screen provides a comprehensive overview of the artifacts collected, allowing examiners to review, search, and export data efficiently.

8.2.0.1 Left-Hand Panel – Plugin List

The left-hand panel lists all plugins executed during the triage session. Numbers next to each plugin indicate the total number of records parsed for that artifact. A blank number indicates that no artifacts were recovered for that plugin. Selecting a plugin from this panel populates the central table with all records retrieved by that plugin. This allows the examiner to focus on specific artifact types, such as documents, system logs, or browser history. The panel also allows for quick navigation between plugins without losing the current view or search context.

8.2.0.2 Central Table – Plugin Results

The central table displays detailed records for the selected plugin, including parsed artifact metadata (e.g., timestamps, file paths, user information, and other relevant details depending on the plugin). Examiners can: - Sort and filter records to prioritize relevant artifacts. - Bookmark records to flag important items for reporting or further analysis. - Preview content where available, such as text, file names, or paths.

This table is the primary workspace for reviewing collected artifacts and determining next steps in an investigation.

8.2.0.3 Case Information

Click “**Case Info**” to view metadata entered during case creation. Certain examiner-entered fields (like notes or case tags) can be modified after the case has started. However, critical settings such as Source Device and Output Directory are read-only once parsing begins, ensuring data integrity and consistency.

8.2.0.4 Top Tabs – Global Triage Case Functionality

The tabs at the top of the Result Viewer provide powerful cross-plugin functionality: - **Global Search** – Execute keyword searches across all plugins or a selected subset. Results are displayed in a dedicated table, allowing examiners to quickly identify artifacts related to specific terms. - **Global Timeline** – Construct a chronological timeline of events from one or multiple plugins. This provides context across artifact types and helps identify correlations between system activity, file creation, and user actions. - **Global Report** – Generate a consolidated report of all bookmarked records, either from a single plugin or multiple sources. This is ideal for documentation, evidence sharing, or preparing findings for a case file. - **Export Case** – Export source files for selected plugins while maintaining the folder structure and metadata. This is useful for sharing raw artifacts or providing evidence to other tools.

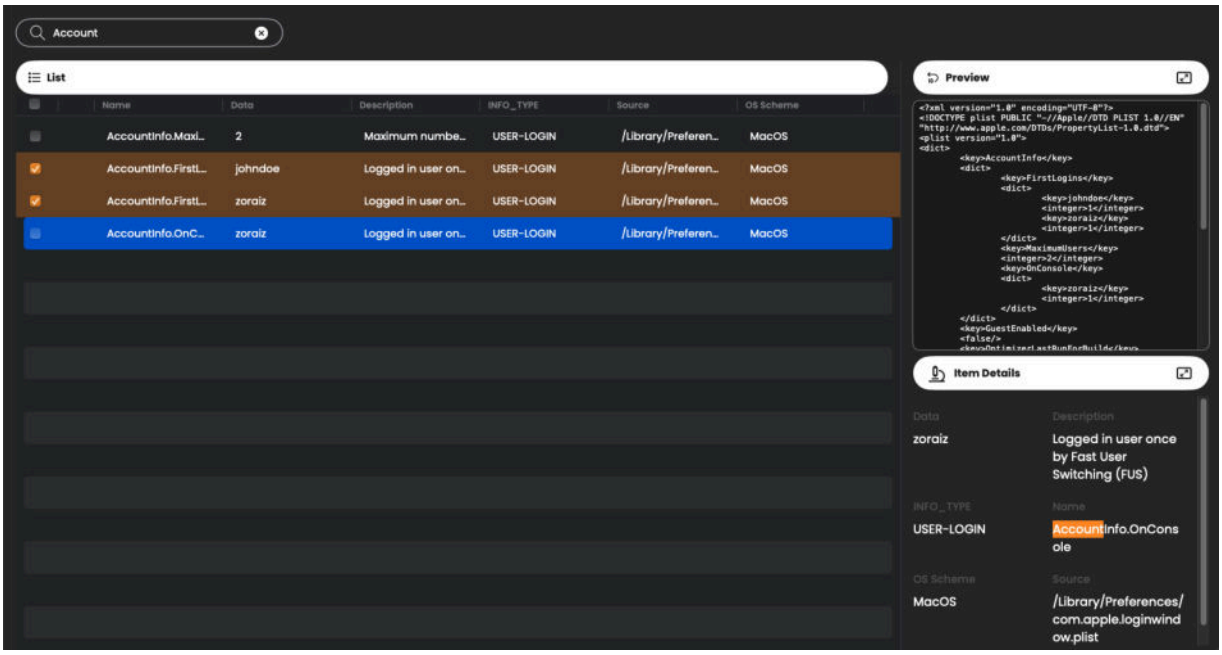
8.2.0.5 Additional Features

- **Start New Triage** – Opens the Case Creation window while a case is still loaded, enabling the examiner to initiate another case without closing **RECON ITR**.
- **Load Case** – Previously created cases can be reopened at any time, allowing examiners to continue analysis, review bookmarked items, or generate reports from

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

prior sessions. The **Load Case** option will appear on the main Splash screen.

8.3 Plugin Results Table



The Plugin Results Table displays all records for the selected plugin. A plugin may be selected from the Plugin List on the left-hand panel of the Triage Result Viewer. This table serves as the primary workspace for reviewing, bookmarking, annotating, and exporting artifacts collected during triage.

8.3.1 Key Components

8.3.1.1 List of Records

The table lists every record retrieved by the selected plugin. Examiners can bookmark records or add notes directly from the table. A horizontal scroll bar is available at the bottom of the table to access all columns and details.

8.3.1.2 Item Details

The Item Details panel displays all metadata and information for the currently selected record in the table. Clicking the expand icon opens the item in a separate window, which dynamically updates as different records are selected.

8.3.1.3 Search

The Search function allows examiners to perform a keyword search within the selected plugin.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Hits are highlighted in the Item Details panel, making it easy to locate relevant artifacts quickly.

8.3.1.4 Preview

The Preview functionality leverages macOS native preview capabilities, allowing examiners to view the contents of selected files directly without exporting them.

8.3.1.5 Right-Click Options

Right-clicking an item in the Plugin Results Table provides several options, along with their associated keyboard shortcuts: - **Quick Look** – Opens the selected item in macOS Quick Look for a fast preview. - **Bookmark** – Marks the currently selected record for reporting or further review. - **Bookmark All** – Bookmarks all records currently displayed in the table. - **Remove All** – Removes bookmarks from all records currently displayed. - **Add Note** – Adds a note to the selected record. Notes are editable, viewable, and included in any generated report. - **Add Note to Bookmarks** – Adds a note to all bookmarked records. - **Remove Note** – Deletes the note associated with the selected artifact.

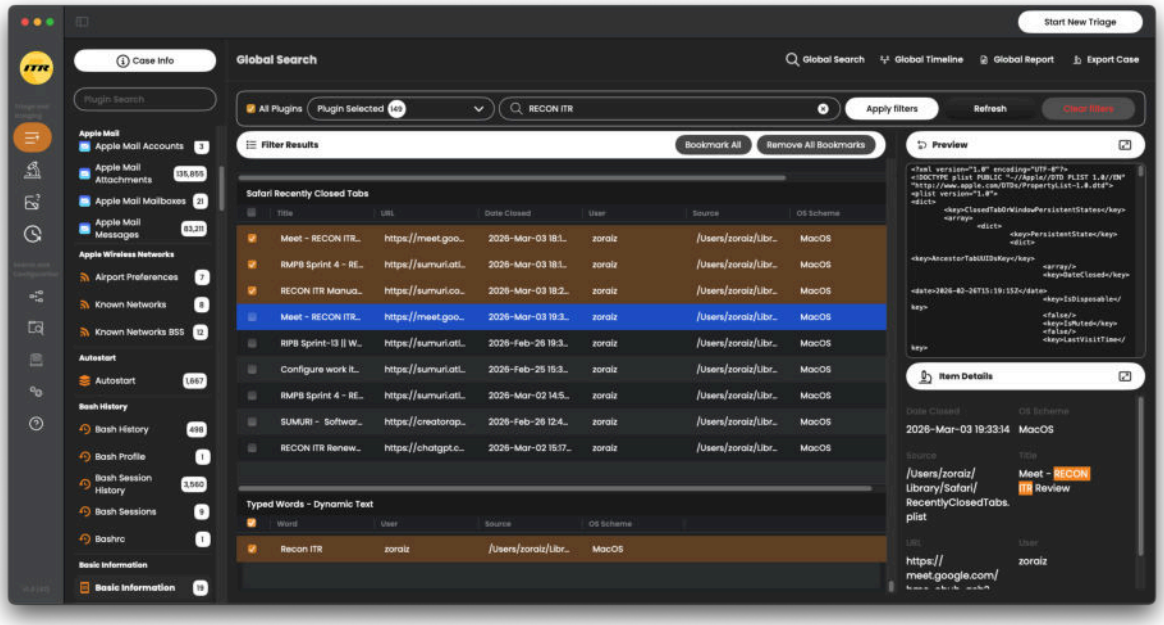
8.3.2 Create Plugin Report

The “**Create Plugin Report**” feature allows examiners to quickly generate reports for the selected plugin. Notes that have been added to plugins will appear in the reports. Reports can be customized based on the following options: - **Bookmarked Items** – Includes only bookmarked records. - **All Items** – Includes every record in the Plugin Results Table. - **Screen Items** – Includes only records currently filtered or displayed in the table.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Available Report Formats: - HTML - PDF - CSV - KML

8.4 Global Search



The “**Global Search**” feature allows examiners to perform a keyword search across multiple plugins at once, providing a centralized view of all artifacts that match the search criteria. This functionality is useful for quickly identifying related artifacts across different plugins and sources.

8.4.0.1 Search Scope

Examiners can choose to search either all plugins or a selected subset of plugins. Searching all plugins ensures a comprehensive review, while limiting the search to specific plugins can focus the query on relevant artifact types. This can be configured through the “**Select Plugins**” dropdown.

8.4.0.2 Keyword Search

Enter a single keyword to locate artifacts containing the specified term. The keyword is matched against artifact metadata and, where applicable, plugin-extracted content.

8.4.0.3 Search Results

Matching records are displayed in the **Global Search** Results Table, which follows a layout similar to the **Plugin Results** Table. Each record shows the plugin name, relevant metadata, and highlights the matched keyword. Selecting a record updates the Item Details panel to

display full metadata and content, with keyword hits highlighted for easy reference.

8.4.0.4 Bookmarks and Notes

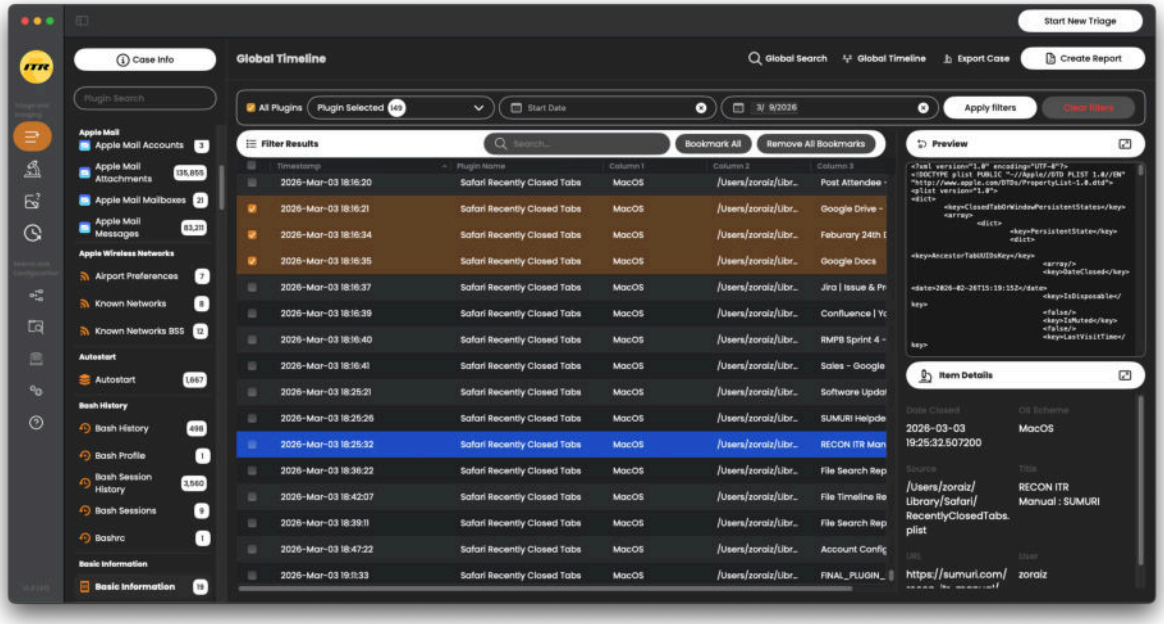
Records found through **Global Search** can be bookmarked or annotated with notes. Bookmarks and notes are synchronized between the **Global Search** view and the **Plugin Results** Table, ensuring that bookmarks added in one view are immediately reflected in the other. This provides a consistent workflow for tracking significant artifacts across different views.

8.4.0.5 Reporting

To generate a report of search results, the examiner must press **Global Report** in the Triage Result Viewer.

> **Notice:**
>
> Bookmarks and notes will be synced between the Plugin View and the Global Search view. A refresh of the search may need to be performed to see the synced changes.

8.5 Global Timeline



The **Global Timeline** feature allows examiners to perform timeline analysis across multiple plugins simultaneously. The timeline is generated using records from a selected list of plugins, allowing artifacts from different sources to be viewed in chronological order. For each record

parsed by a plugin, a Global Timeline entry is created for every column that contains a timestamp. This allows artifacts with multiple timestamps (such as creation, modification, or access times) to appear multiple times in the timeline, providing a more complete chronological view of activity. Examiners may define a start date and end date to filter the timeline. Records that fall outside of the selected date range will be excluded from the results. All timestamps displayed in the Global Timeline are adjusted based on the timezone selected when the case was initially created.

8.5.0.1 Filter Results

The **Filter Results** panel allows examiners to refine the timeline data that is currently displayed. Through this panel, examiners can: - Enter a single keyword to search through the timeline records. The search will return records that contain the specified keyword within the artifact data. Specific keyword hits will be highlighted in the Item Details tab. - Define a start date and end date to limit results to a specific time range. - Bookmark all currently displayed records. - Remove bookmarks from all currently displayed records.

8.5.0.2 Preview Panel

The **Preview Panel** displays a preview of the source file associated with the selected record when available. The preview uses macOS native preview functionality. - The preview allows examiners to quickly view the contents of supported files without opening them in an external application. - The **expand icon** allows the preview to be opened in a larger window for easier examination.

8.5.0.3 Item Details

The Item Details panel displays the full metadata and artifact information for the selected timeline record. - All available record information is displayed within this panel. - Pressing the expand icon will open the item details in a separate window, allowing the record information to be viewed outside of the main Global Timeline interface.

8.5.0.4 Create Report

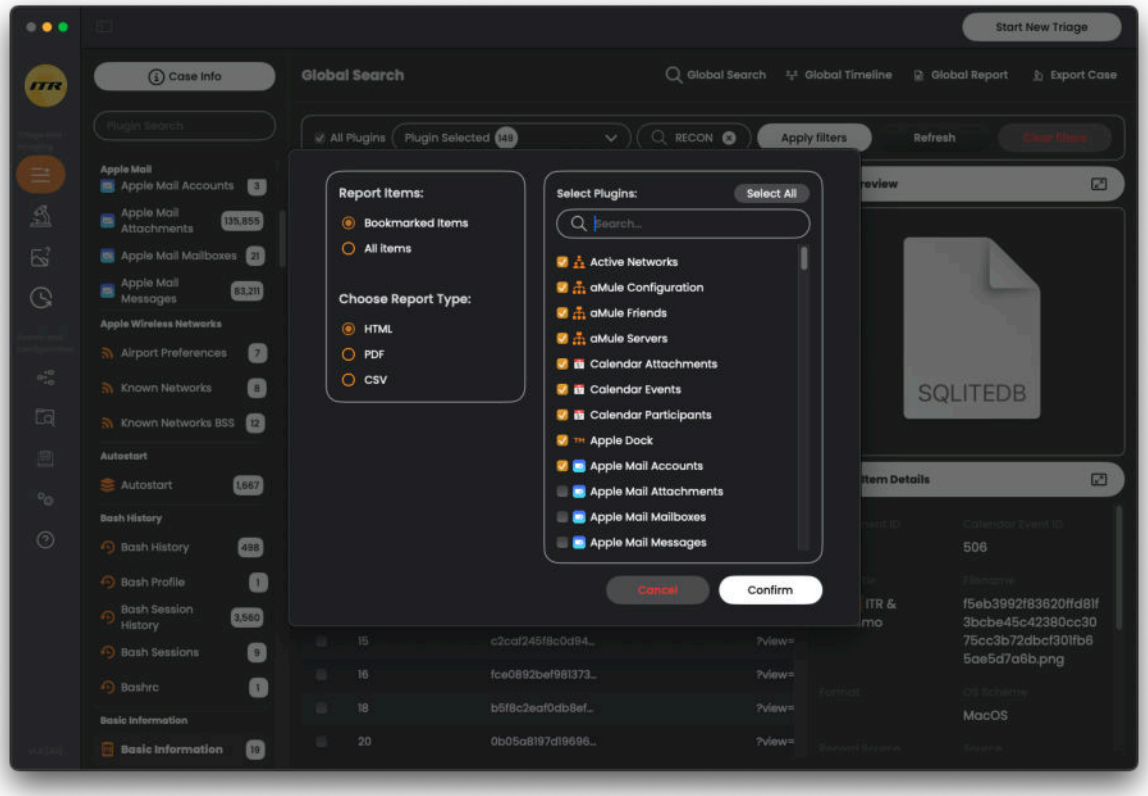
The Create Report function allows examiners to generate a report containing records from the Global Timeline. Reports generated through this feature include only records present in the Global Timeline view. **Available report options include:** - **Bookmarked Items** – Includes only bookmarked records. - **All Items** – Includes every record currently present in the Global Timeline. - **Screen Items** – Includes only records currently filtered or displayed in the table.

Available report formats: - HTML - PDF - CSV

Notice:

Bookmarks in the Global Timeline are not synchronized with bookmarks in the Plugin Results Table or Global Search. This is because a single plugin record may generate multiple timeline entries if it contains multiple date fields.

8.6 Global Report



The **Global Report** feature allows examiners to generate reports from records that have been bookmarked through either the **Plugin Results** Table or **Global Search**. This feature provides a centralized way to document significant artifacts across multiple plugins, streamlining the reporting process for investigations. When the examiner presses the **Global Report** button, a window opens that allows for the selection of which plugins to include in the report. Reports can be generated for all plugins or a selected subset, depending on the scope of the investigation.

Items that are checked in the Select Plugins view are the plugins that will be included in the report. **Available report options include:** - **Bookmarked Items** – Includes only bookmarked records. - **All Items** – Includes every record currently present in the Global Timeline. - **Screen**

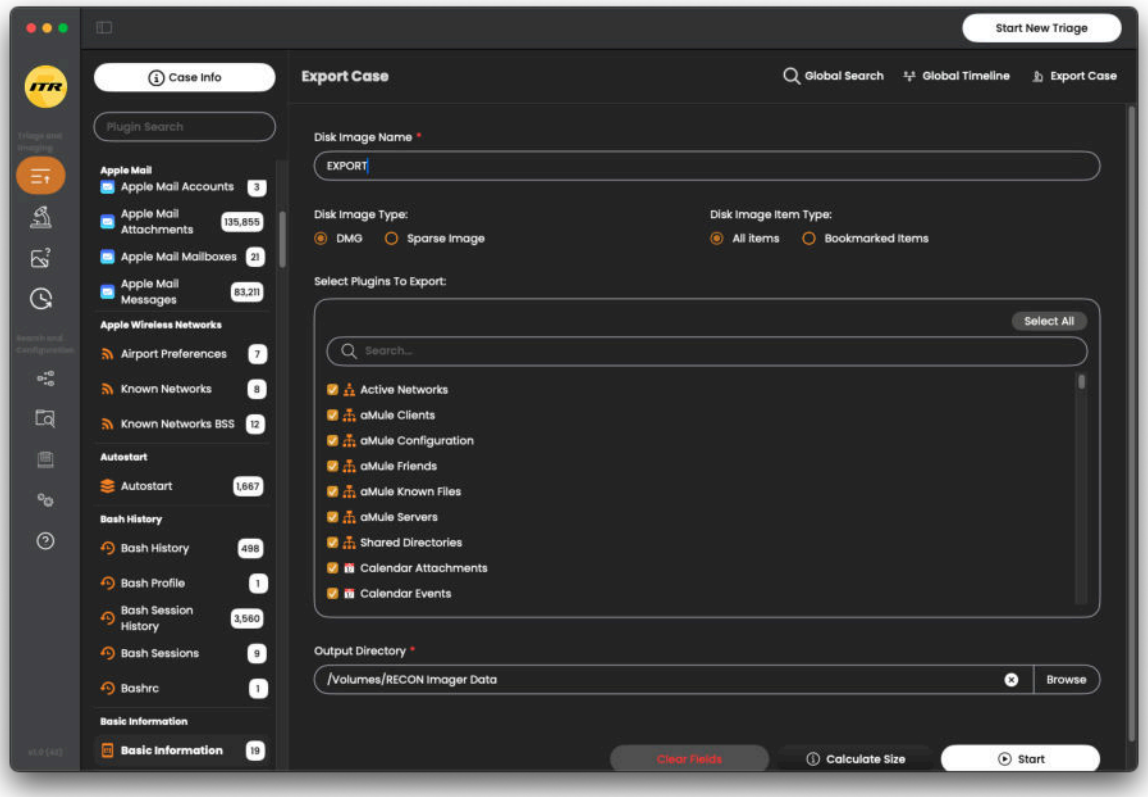
Items – Includes only records currently filtered or displayed in the table.

Available report formats: - HTML - PDF - CSV

Notice:

Items bookmarked in the Global Timeline will not be included in the Global Report. The Global Report is a report of all items that have been bookmarked through the Plugin table view or the Global Search table.

8.7 Export Case



The **Export Case** feature allows examiners to export source files from selected plugins to a DMG or Sparse Image. This functionality provides a convenient way to preserve and share original source files associated with a case. Examiners can choose to export either All Items or Bookmarked Items: - **All Items** – Exports every source file for all records in the selected plugins. - **Bookmarked Items** – Exports only the source files associated with records that have been bookmarked.

The file path listed in the "**Source**" column in the Plugin Results Table identifies the exact file that will be exported.

8.7.0.1 Selecting Plugins

The **Select Plugins** to Export table displays only the plugins that were executed in the current case. Examiners can select one or multiple plugins to include in the export.

8.7.0.2 Output Directory

The **Output Directory** specifies where the export case folder will be created. All exported source files will be organized within this folder.

8.7.0.3 Calculate Size

The **Calculate Size** button provides an estimate of the storage space required on the destination drive to write the forensic image. The required space depends on: - The number of source files being exported - The number of plugins selected for export

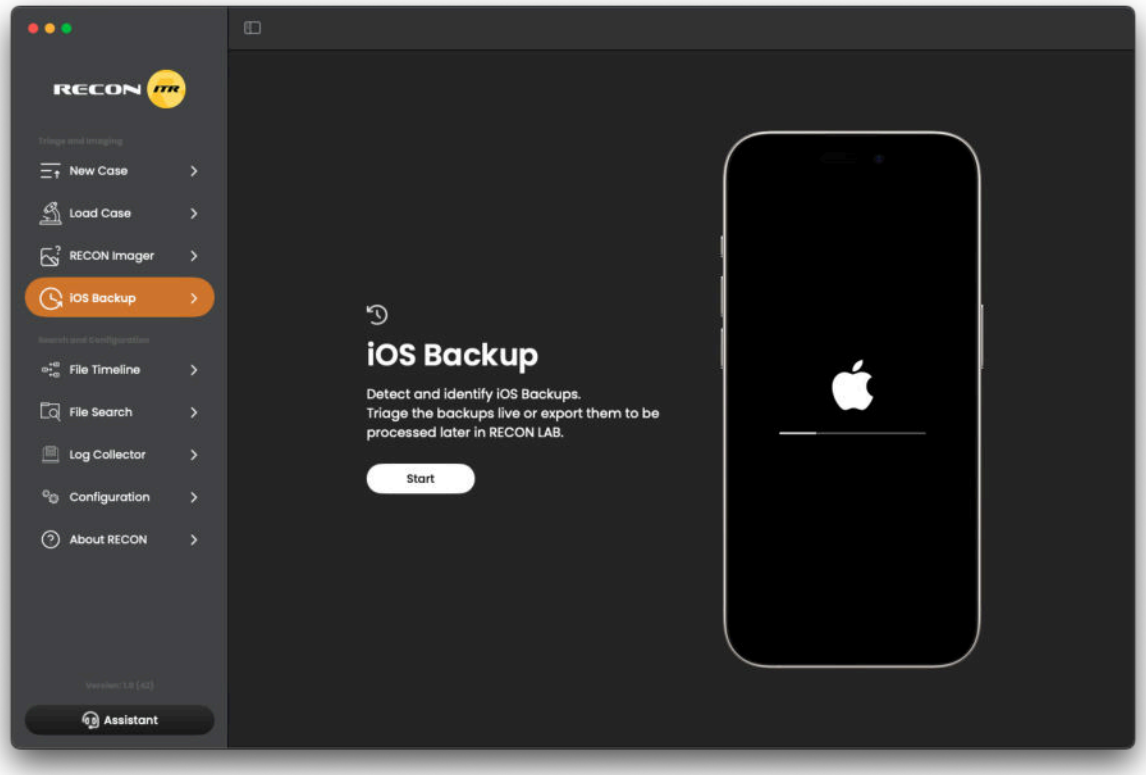
This allows examiners to ensure there is sufficient free space before starting the export process.

Notice:

The Export Case option is not meant for forensic imaging. The export case will not capture a full forensic image and is intended only for exporting plugin source files. For full forensic imaging, please use the Disk Imager or Logical Imager.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

9 iOS Backup



The **iOS Backup** tool is accessible from the **RECON ITR** splash screen and provides examiners with the ability to export or analyze iOS device backups stored on a macOS system. This feature enables investigators to quickly locate iOS backups present on the examiner machine and perform triage analysis using integrated **iLEAPP plugins**.

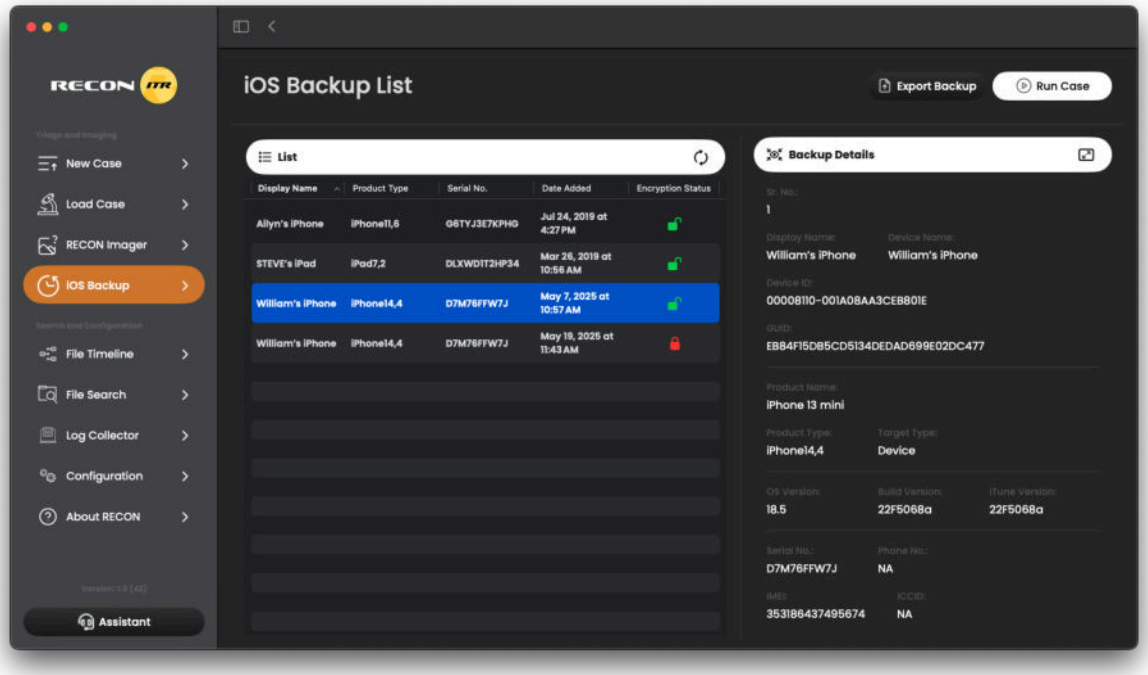
RECON ITR currently utilizes **iLEAPP Version 2.3.0** for the parsing and analysis of iOS backup artifacts. The iOS Backups workflow allows the examiner to: - Detect iOS backups present on the system - Review metadata associated with each backup - Export a backup for external analysis - Perform triage analysis of a backup using iLEAPP plugins

9.0.0.1 Locating iOS Backups

When the **iOS Backups** tool is opened, **RECON ITR** automatically scans the default macOS backup location: ~/Library/Application Support/MobileSync/Backup/ This directory is used by **Finder and iTunes** to store iOS device backups created when an iPhone or iPad is backed up to the computer. Any backups detected within this directory will be displayed within the **iOS**

Backup List.

9.1 iOS Backup List



The **iOS Backup List** displays all detected backups located within the MobileSync directory. Each entry represents a backup associated with an iOS device. When a backup is selected from the list, detailed metadata about the backup is displayed within the Backup Details panel. This information allows examiners to quickly identify the device associated with the backup before performing further analysis. Available information may include: - Backup Name - Device Name - Device Model / Product Name - Phone Number associated with the device - Backup Encryption Status

If additional space is required to review this information, the Expand icon can be used to open the backup details in a separate window. This allows the examiner to review the device metadata in greater detail while preparing for export or analysis.

9.1.0.1 Encrypted Backups

Some iOS backups may be encrypted. Encryption protects sensitive data contained within the backup and requires the backup password to access the data. If an encrypted backup is selected, **RECON ITR** will prompt the examiner to enter the backup password before the backup can be exported or analyzed. The correct password must be provided in order to

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

continue processing the backup.

9.2 Export Backup

The **Export Backup** option allows the examiner to extract the contents of an iOS backup and write the unpacked data to a selected output directory. During the export process, **RECON ITR** will: 1. Read the selected backup from the MobileSync directory 2. Unpack the backup contents 3. Write the extracted files to the selected output location

This feature is useful when the examiner needs to collect an iOS backup from a system without immediately performing analysis or the need to capture a full forensic image. The exported backup can later be processed using other forensic tools, including **RECON LAB**.

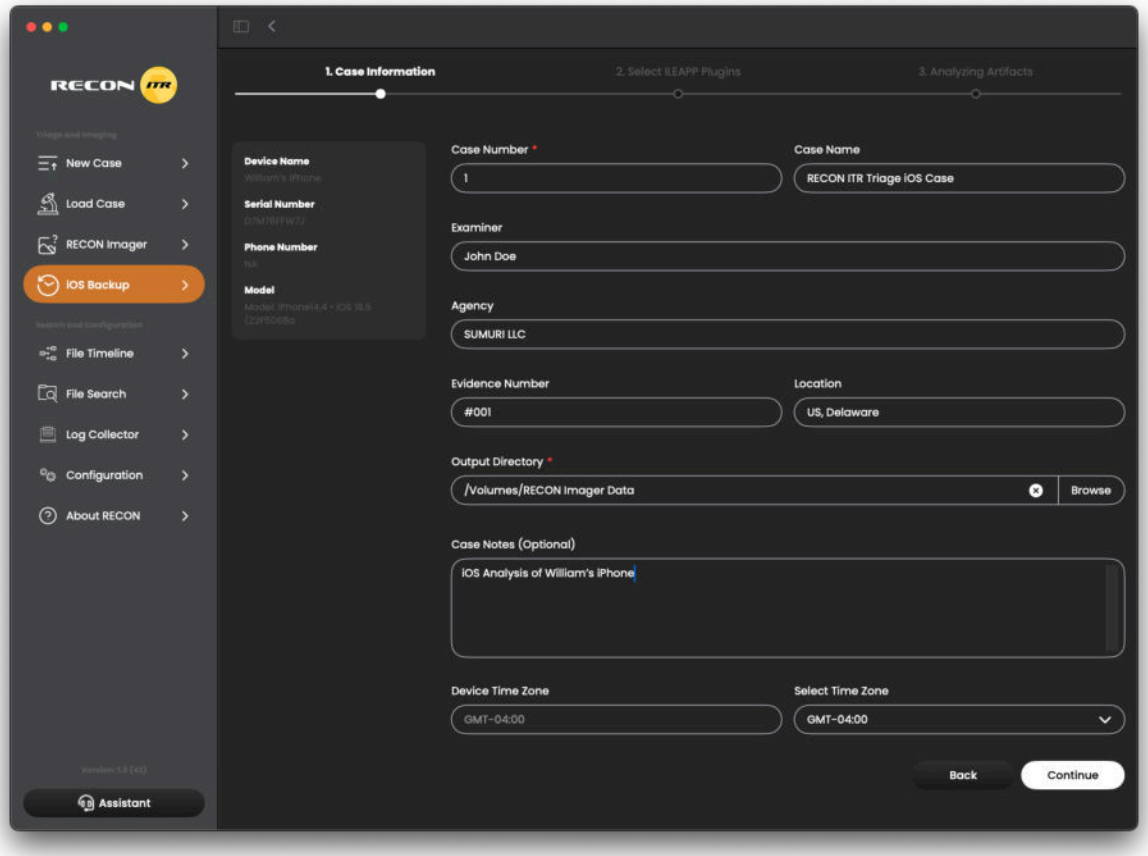
9.3 Run Case (iOS Triage)

The **Run Case** option allows examiners to perform a forensic triage analysis of a selected iOS backup. This process uses integrated **iLEAPP plugins** to identify and parse artifacts

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

contained within the backup.

9.3.1 Case Information



The **Case Information** screen is the first step in the triage case creation process. This screen allows the examiner to configure basic case settings before initiating artifact analysis. Examiners can enter case-related metadata and configure important processing options prior to starting the analysis.

9.3.1.1 Time Zone

A **Time Zone** can be selected to control how timestamps are displayed during analysis. This ensures that artifact timestamps are interpreted correctly throughout the case. By default, timestamps are displayed using the time zone of the live device running **RECON ITR**.

9.3.1.2 Output Directory

The **Output Directory** specifies where all parsed data generated during the triage process will be stored. When the triage case begins, **RECON ITR** automatically creates a case folder within the selected output directory. This case folder contains all artifacts and parsed data

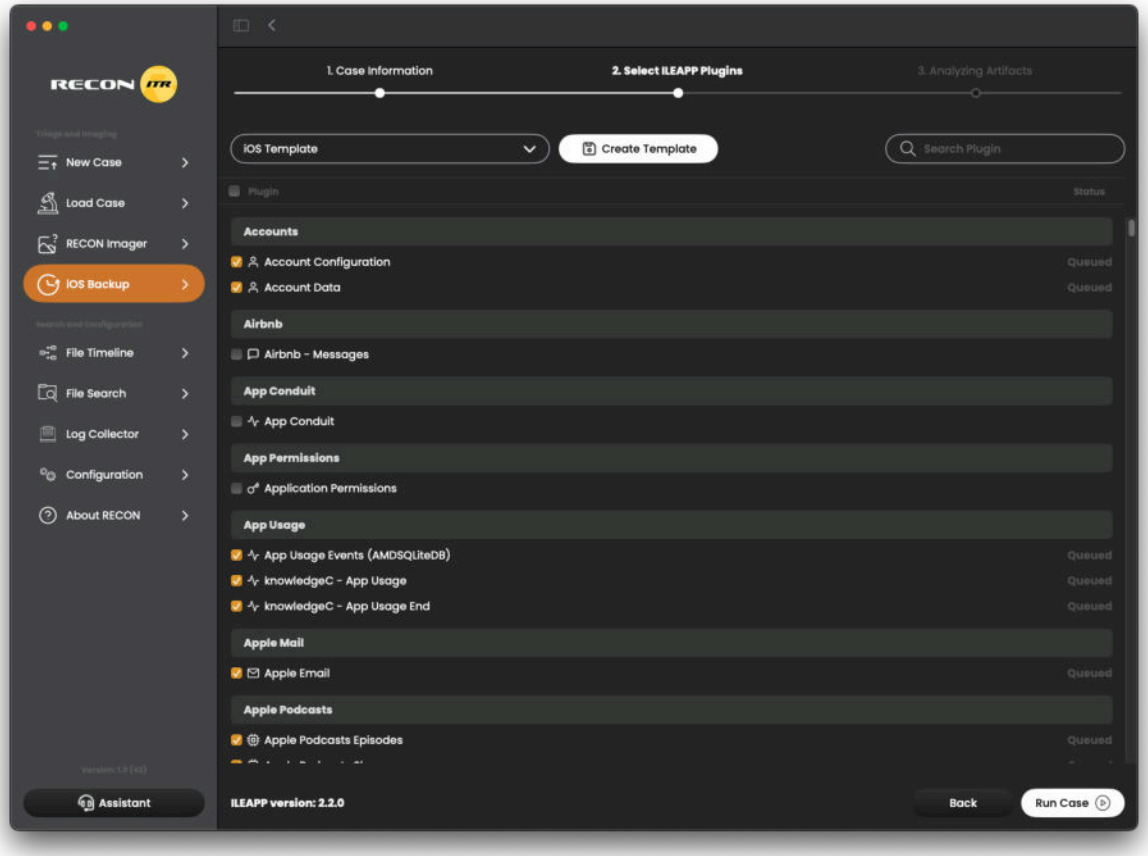
P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

generated during analysis.

9.3.1.3 Device Information

Information about the iOS device associated with the selected backup is displayed on the left-hand side of the Case Information screen. This allows the examiner to confirm the device being analyzed before starting the triage process. Displayed information may include: - Device Name - Phone Number - Device Model - Serial Number

9.3.2 Select Plugins

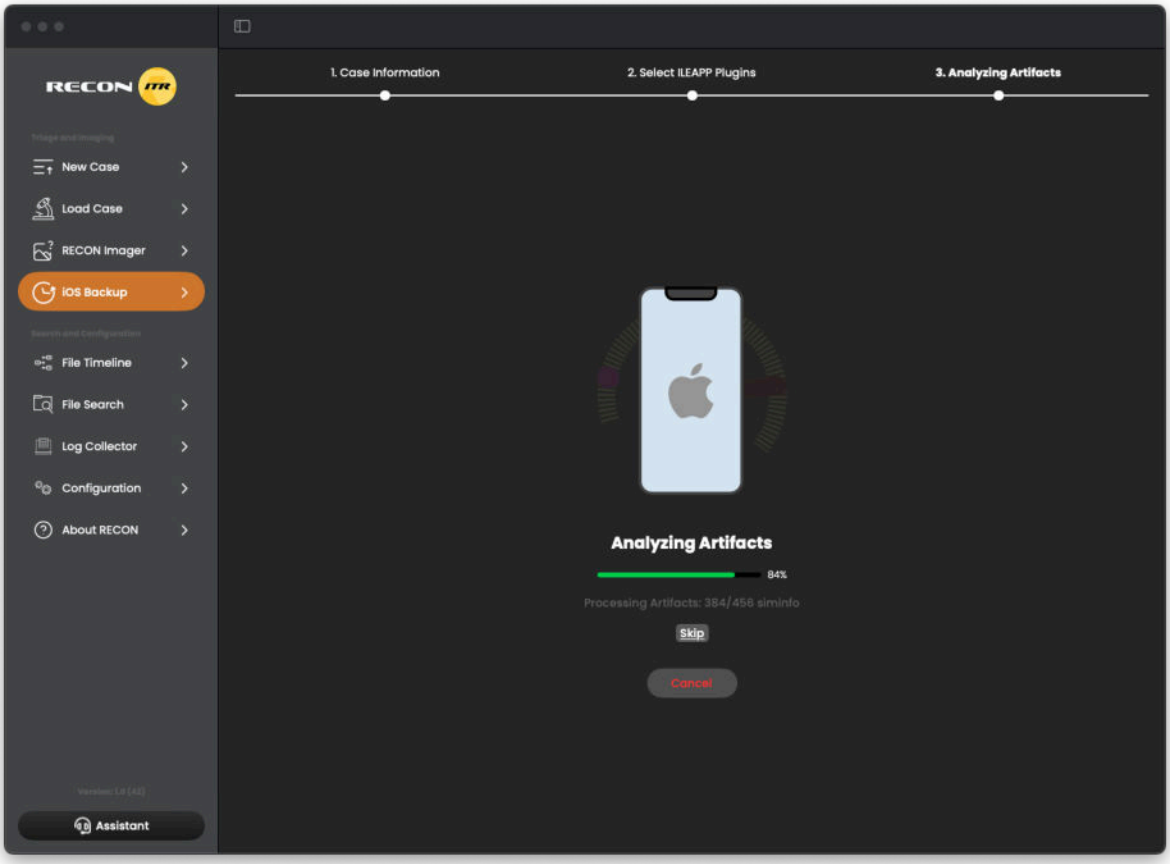


The Select Plugins screen allows the examiner to determine which artifacts **RECON ITR** will analyze during the triage process. Each plugin is designed to identify and parse specific types of forensic artifacts from the iOS backup. **RECON ITR** utilizes **iLEAPP plugins** for the parsing of iOS artifacts. Selecting only the necessary plugins can help streamline analysis and reduce processing time. Templates allow examiners to quickly apply a predefined set of plugins to future triage cases. This can help standardize analysis workflows across investigations. **To create a new template:** 1. Select the desired plugins. 2. Click “**Create Template**”. 3. The selected plugins will be saved as a reusable template.

Updating an Existing Template 1. Select the template from the Template dropdown menu. 2. Adjust the plugin selections as needed. 3. Click “**Update Template**”.

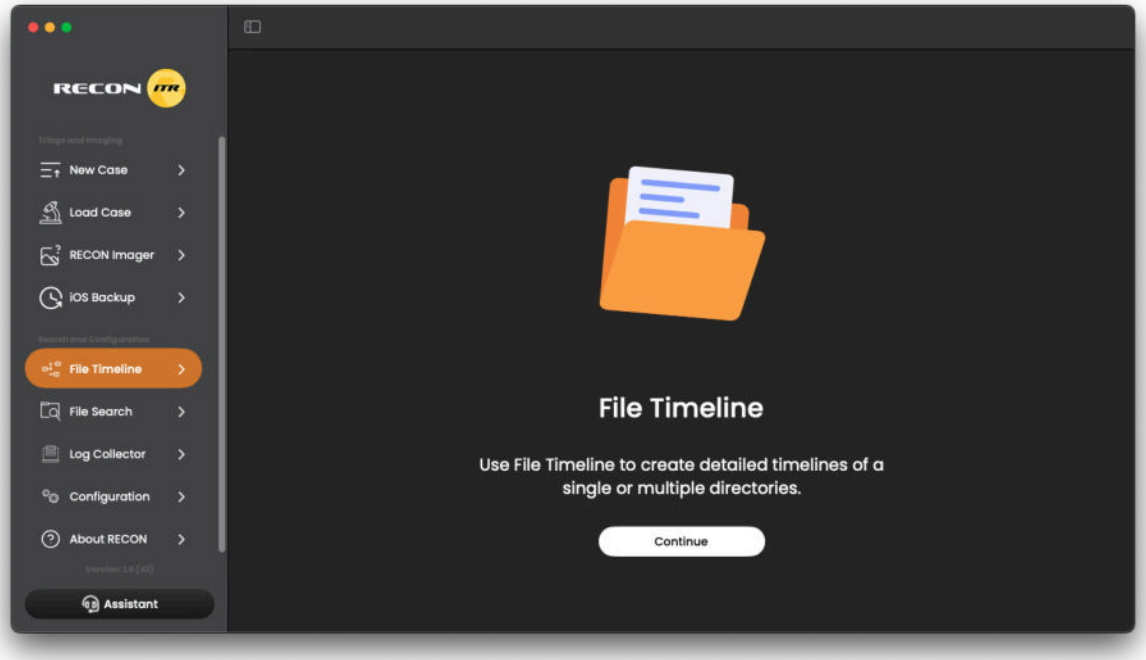
Templates can be selected or removed through the Template dropdown menu. Once the desired plugins have been selected, click “**Run Case**” to begin artifact analysis.

9.4 Analyzing Artifacts



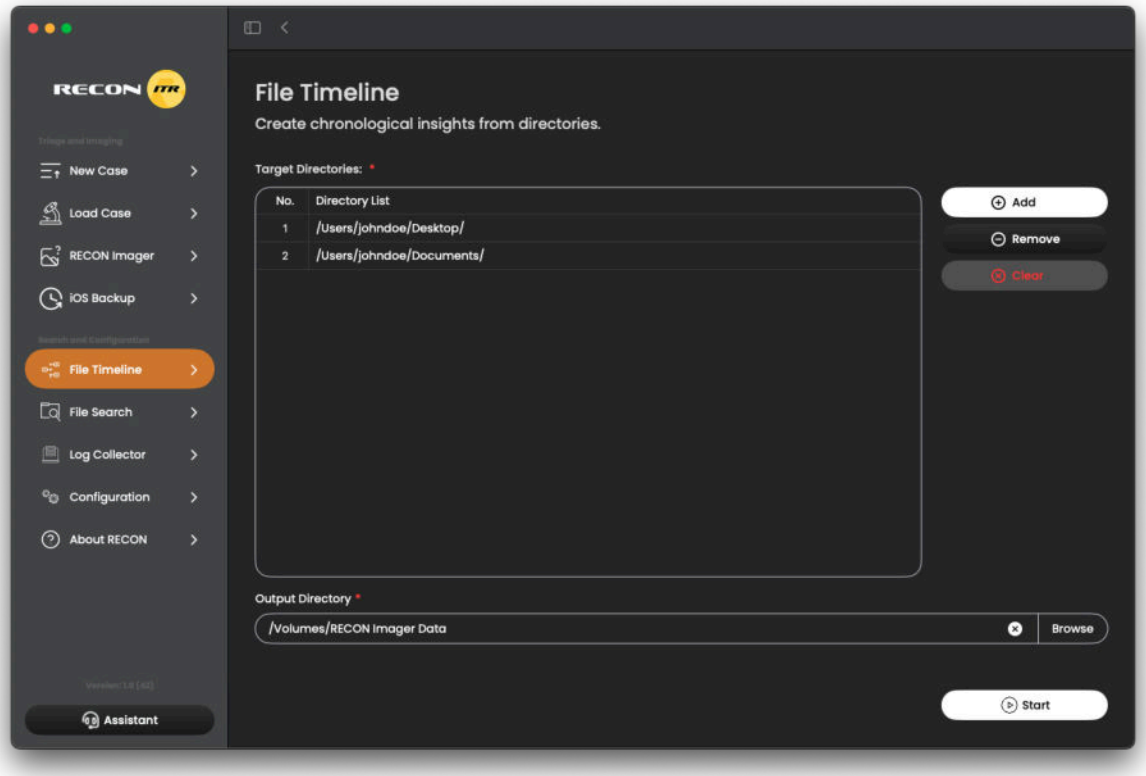
After the triage process begins, the **Analyzing Artifacts** screen displays the progress of the analysis. This window provides a real-time view of the plugins currently being executed and shows the progress of artifact processing. Examiners can monitor the status of each plugin as it runs. If necessary, a plugin can be skipped during processing by selecting the Skip option. This allows the examiner to bypass a plugin while allowing the remaining plugins to continue running without interruption. Once the process completes the will appear.

10 File Timeline



The **File Timeline** feature allows examiners to analyze file activity within selected directories by extracting Apple extended attributes and associated timestamps from files. These attributes often contain valuable metadata that can assist in reconstructing user activity, such as when files were created, modified, added to the file system, or last used. By targeting specific directories, the File Timeline focuses analysis on relevant areas of the system rather than scanning the entire file system.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com



10.0.0.1 Target Directories

The **Target Directories** list defines which folders will be analyzed during the timeline creation process. The following controls are available: - **Add** – Opens a Finder window where a new directory can be selected and added to the target directory list. - **Remove** – Removes the currently selected directory from the target directories list. - **Clear** – Removes all directories from the target directories list.

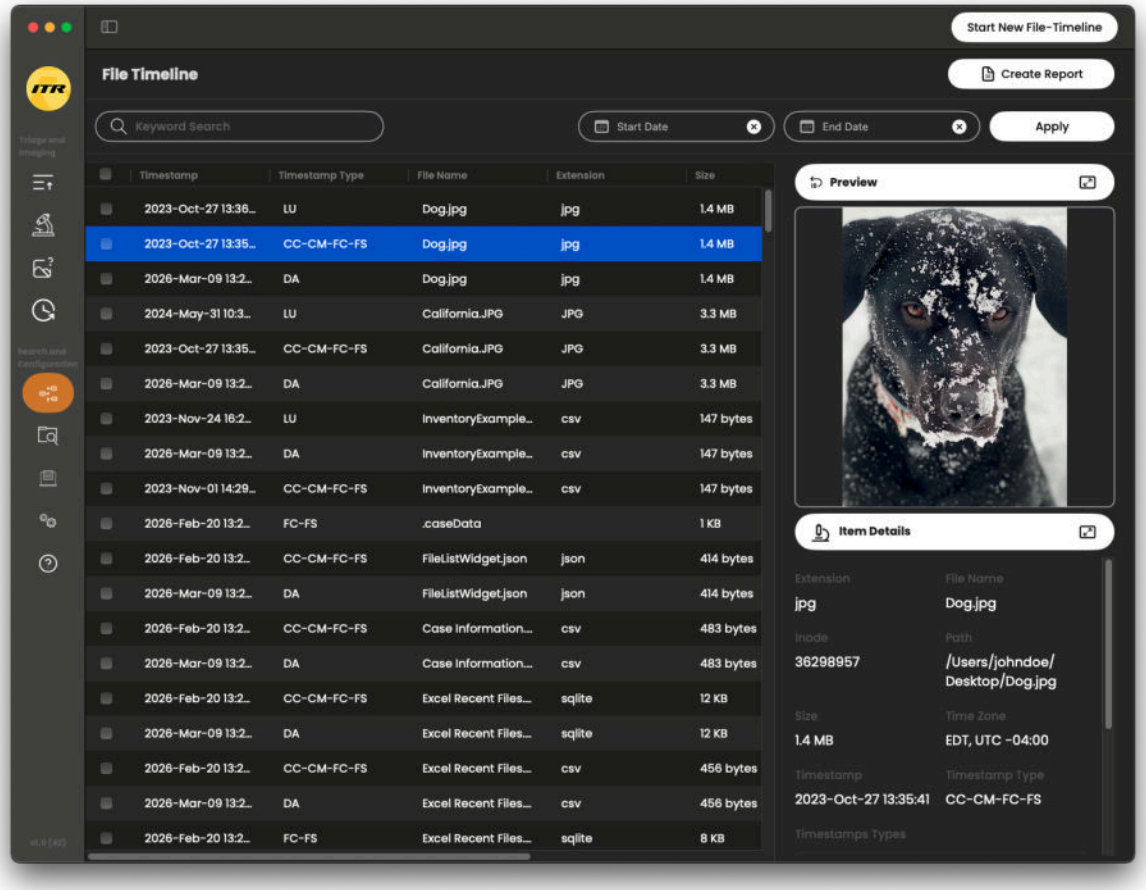
10.0.0.2 Additional Options

- **Output Directory** – Specifies where the File Timeline case data will be written.
- **Start** – Begins the timeline creation process using the selected directories.

Once processing has completed, the File Timeline Table will appear and display the timeline

records extracted from the analyzed files.

10.1 File Timeline Table



The **File Timeline** table contains records representing timestamp events associated with files. Each record corresponds to a specific time when an event occurred. If a file contains multiple timestamps that occurred at the same time, they will be grouped into a single record. As a result, the timeline will contain one record per file per event time, even if multiple timestamp types share that same time value. The following timestamp types may appear in the File Timeline: - **CC** — Content Creation - **FC** — File System Creation - **CM** — Content Modification - **FS** — File System Change - **DA** — Date Added - **LU** — Last Used

10.1.1 Filtering and Searching

The **File Timeline** includes tools that allow examiners to quickly narrow results and locate relevant activity. - **Start Date** / **End Date** – Allows the examiner to filter events to a specific time range. Only records occurring within the selected date range will be displayed. -

Keyword Search – Allows the examiner to search File Timeline records for matching keywords.

10.1.2 Artifact Review

When a record is selected, additional information is available through the preview and item details panels. - **Preview Panel** – Allows the examiner to open the source file for the selected artifact using Apple's native preview functionality. - **Item Details** – Displays detailed information about the selected record, including the timestamps associated with the event and general file information.

10.1.3 Table Right-Click Options

The **File Timeline** table includes several context menu options that assist with reviewing and organizing artifacts. - **QuickLook** – Opens the selected record's source file using Apple's native preview. - **Bookmark** – Bookmarks the selected item. - **Remove Bookmark** – Removes the bookmark from the selected item. - **Bookmark All** – Bookmarks all records currently displayed in the table. - **Remove All Bookmarks** – Removes bookmarks from all displayed records.

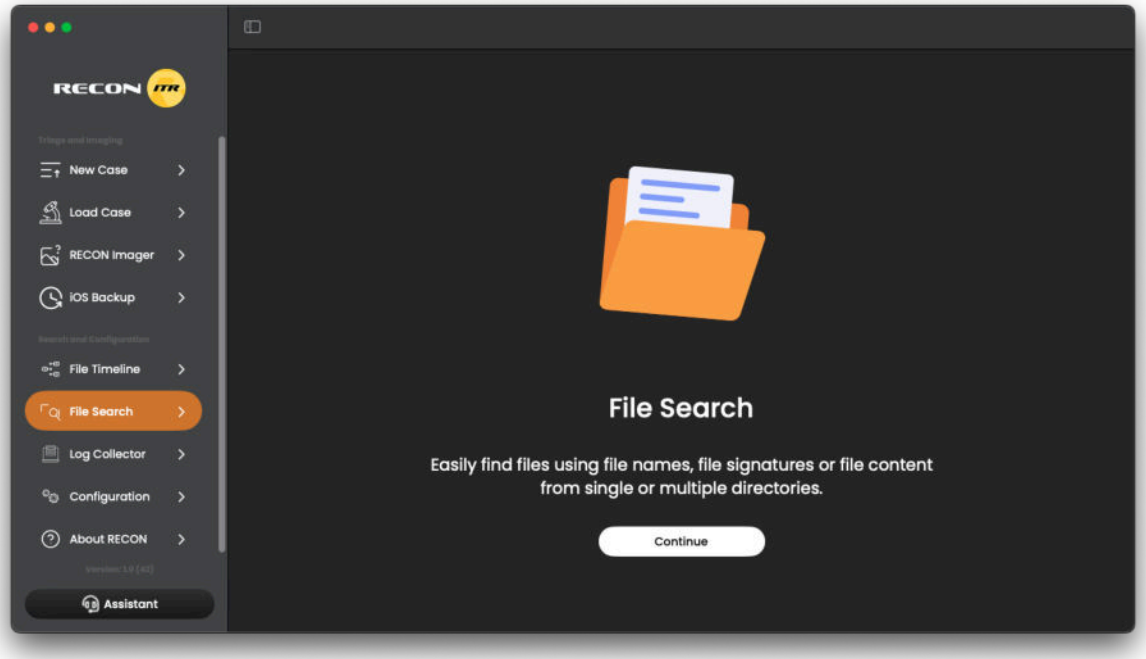
10.1.4 Creating Reports

Reports can be generated directly from the **File Timeline** to export the analyzed records. Report scope options include: - **Bookmarked Items** – Includes only bookmarked records. - **All Items** – Includes every record currently present in the File Timeline table. - **Screen Items** – Includes only records currently displayed after filtering or searching.

Available report formats: - HTML - PDF - CSV

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

11 File Search



The **File Search** feature allows examiners to locate files within selected directories based on user-defined criteria. Searches can be performed using file signatures, file names, or keywords, allowing investigators to identify files of interest during triage or analysis. The **File Search** workflow consists of two primary stages: - **Configuration** – Defining the search criteria to be used during the scan. - **Analysis** – Reviewing the results of files identified during the search.

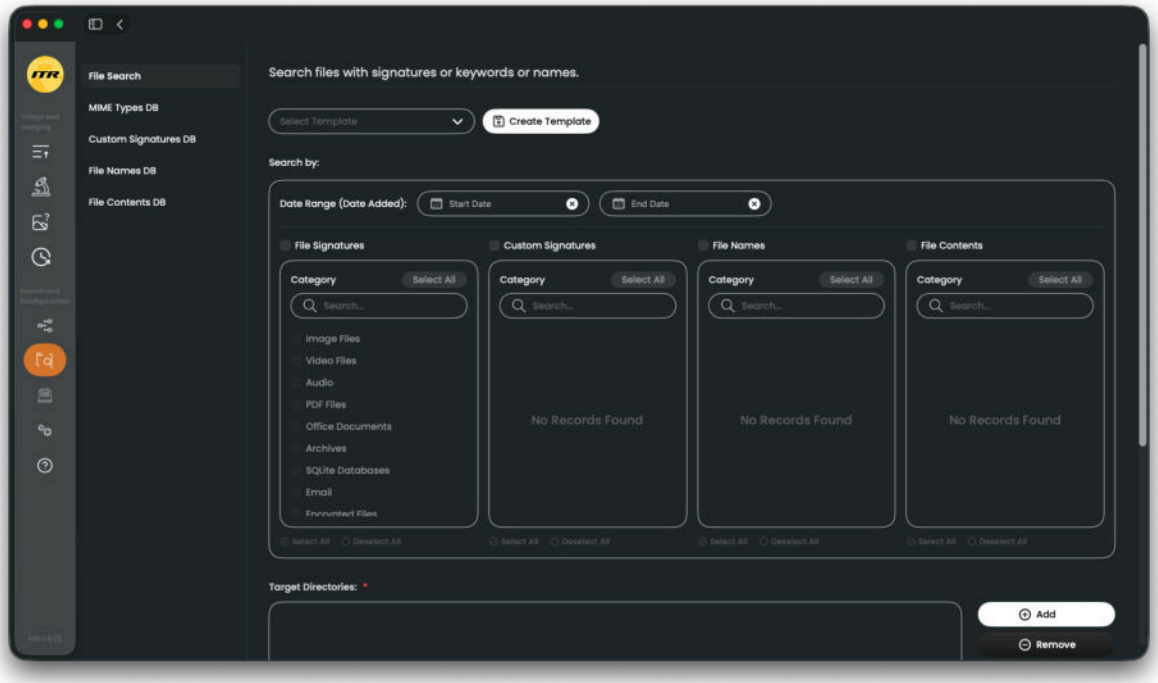
11.1 Configuration

The configuration interface allows examiners to define and manage the search criteria before running a search. The configuration section contains four tabs: - **File Search** - **MIME Types**

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

DB - **Custom Signatures DB** - **File Names DB** - **File Contents DB**

11.1.1 File Search



The **File Search** tab allows examiners to configure which search categories will be used during the File Search process. From this interface, examiners can enable or disable the available search options and select the specific categories that should be included in the analysis. File Search can be configured to run the following search types: - **File Signatures** - **Custom Signatures** - **File Name** - **File Contents**

Within each enabled search type, the examiner can select one or more categories that contain the items to be searched.

11.1.1.1 Date Added Filter

The **File Search** tab also allows examiners to define a date range for the Date Added attribute (kMDItemDateAdded). When this filter is enabled, files whose Date Added value falls outside of the specified range will be excluded from the search results. This allows examiners to narrow searches to files that were added to the system during a specific timeframe.

11.1.1.2 Templates

Templates allow examiners to save commonly used **File Search** configurations. This is useful when the same set of categories is used across multiple cases. A template stores the following selections: - Enabled File Search Options (File Names, File Signatures, File

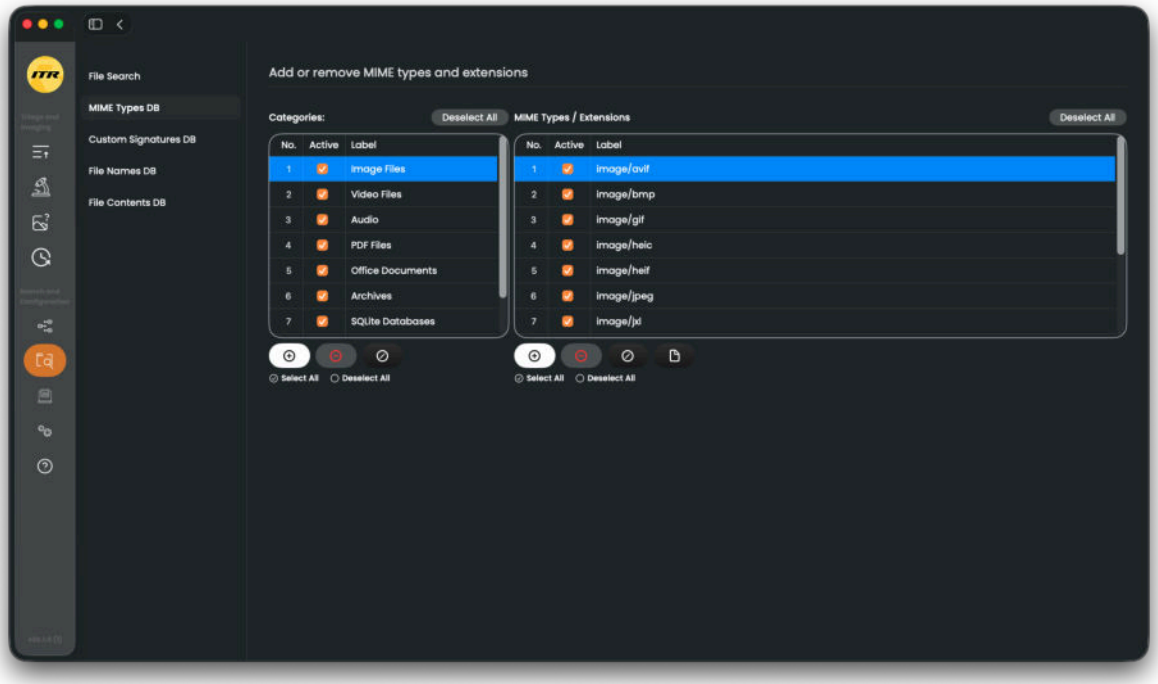
Keywords) - The enabled categories selected within each option

When a template is applied, **RECON ITR** will automatically enable the saved options and category selections. **Creating a Template** 1. Enable the desired File Search Options (File Names, File Signatures, File Keywords). 2. Select the categories you want included in the template. 3. Click “**Create Template**”. 4. Enter a name for the template.

The template will then be available in the Template dropdown menu. Selecting a template from the dropdown will automatically apply the saved configuration. **Updating a Template** 1. Select the template from the Template dropdown. 2. Modify the enabled categories or search options. 3. Click “**Update Template**”.

The template will be updated to reflect the new configuration. **Removing a Template** 1. Click the Template dropdown. 2. Press the Delete button next to the template name. 3. Confirm by selecting “**Yes, Delete**”.

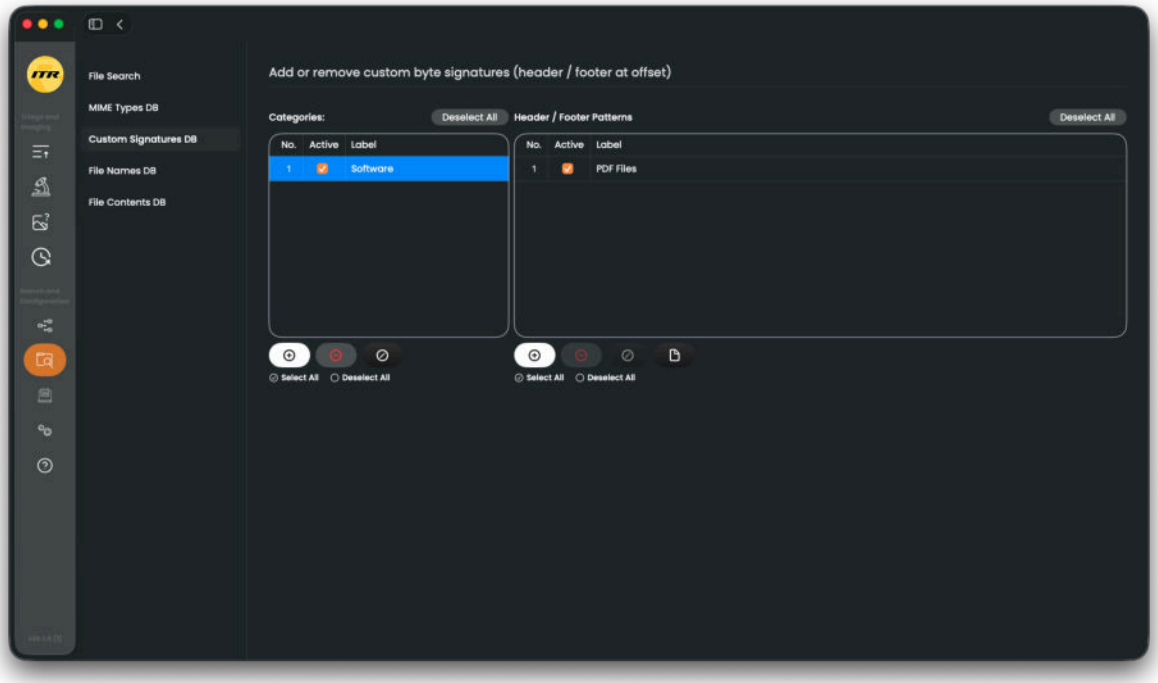
11.1.2 MIME Types DB



The MIME Types DB allows you to search for Files based on their MIME Type. These MIME Types are determined by macOS. By default, the most common MIME Types will be added for

immediate use.

11.1.3 Custom Signatures DB

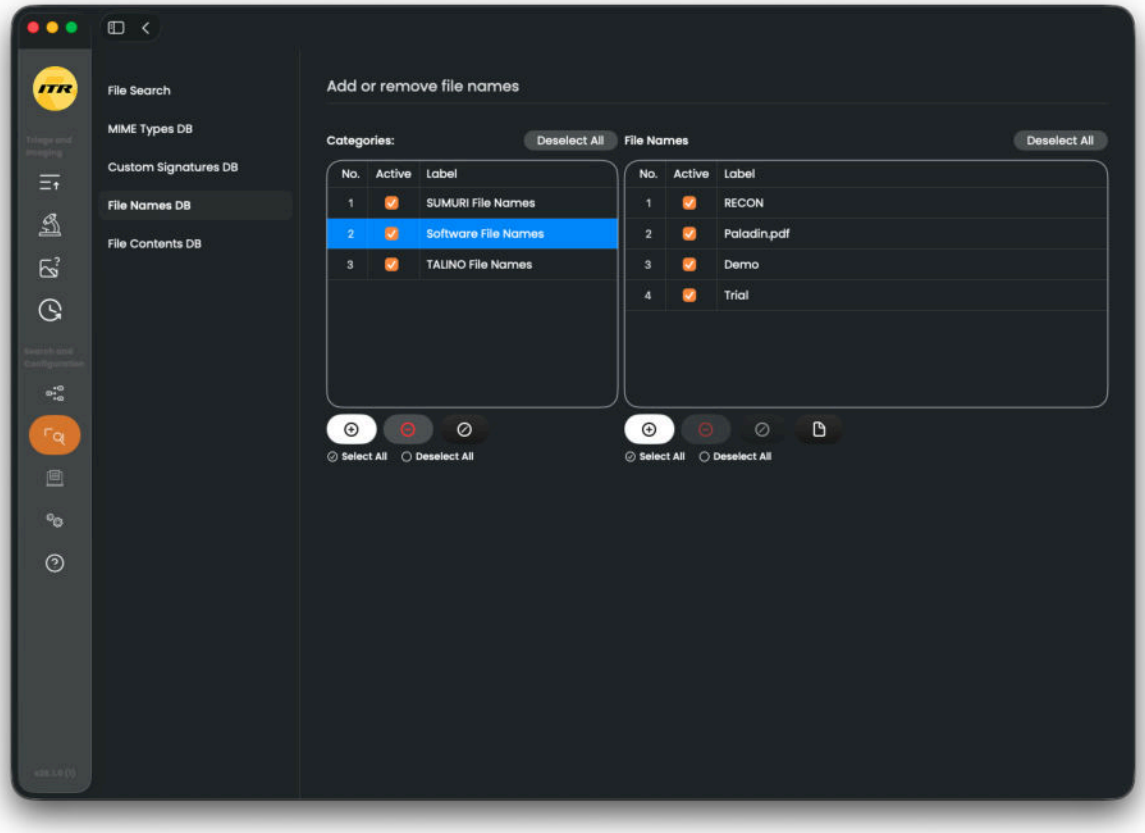


The **Custom Signatures DB** tab allows examiners to define custom file signatures that **RECON ITR** will search for during analysis. Signatures can be identified by either the header

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

or the footer of the file. Signatures may be defined using either: - ASCII - Hexadecimal

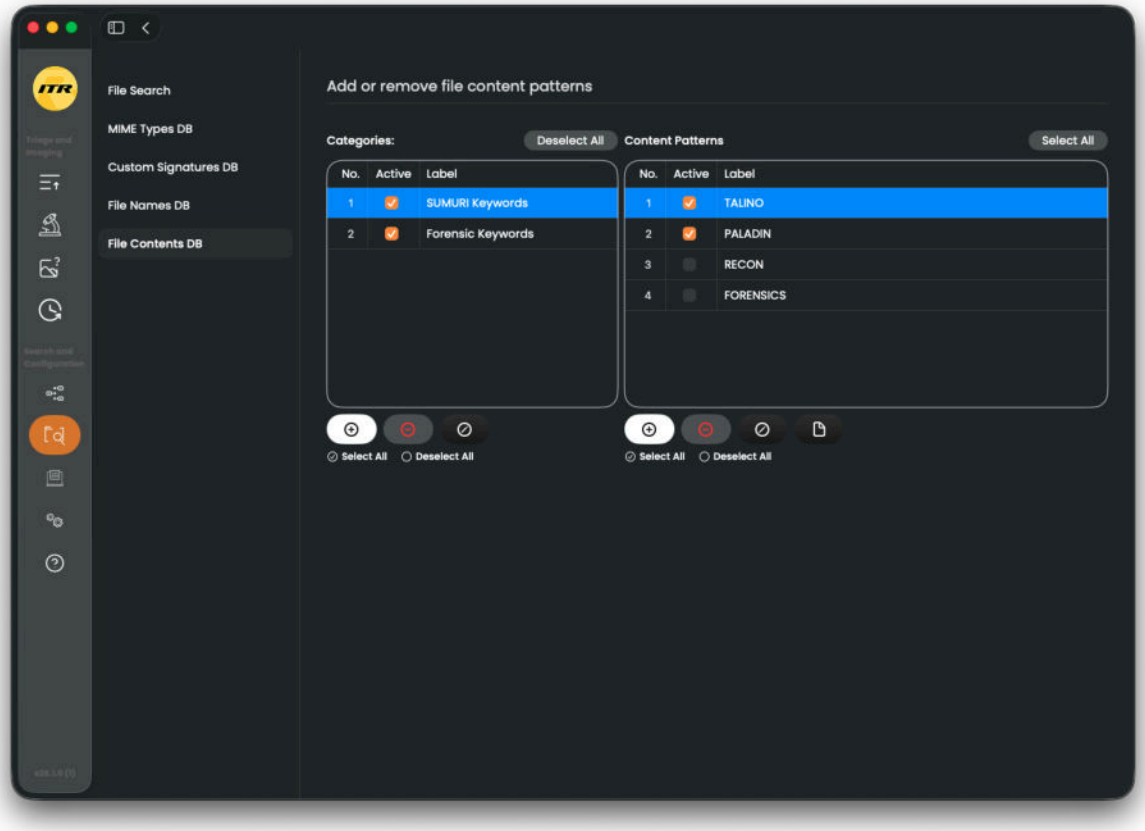
11.1.4 File Names DB



The **File Names DB** tab allows examiners to define a list of file names that **RECON ITR** will

search for within the selected directories.

11.1.5 File Contents DB



The **File Keywords DB** tab allows examiners to define keywords that will be used to perform a raw keyword search against files located within the selected directories.

11.1.6 Database Organization

The **MIME Types DB, Custom Signatures DB, File Names DB,**, and **File Contents DB** tabs use a similar interface for organizing search criteria.

11.1.6.1 Categories

Categories are used to organize search items into logical groups. The following controls are available: - **+ (Add)** – Creates a new category. - **– (Remove)** – Removes the currently selected category. - **Pencil Icon** – Allows the name of the selected category to be edited. -

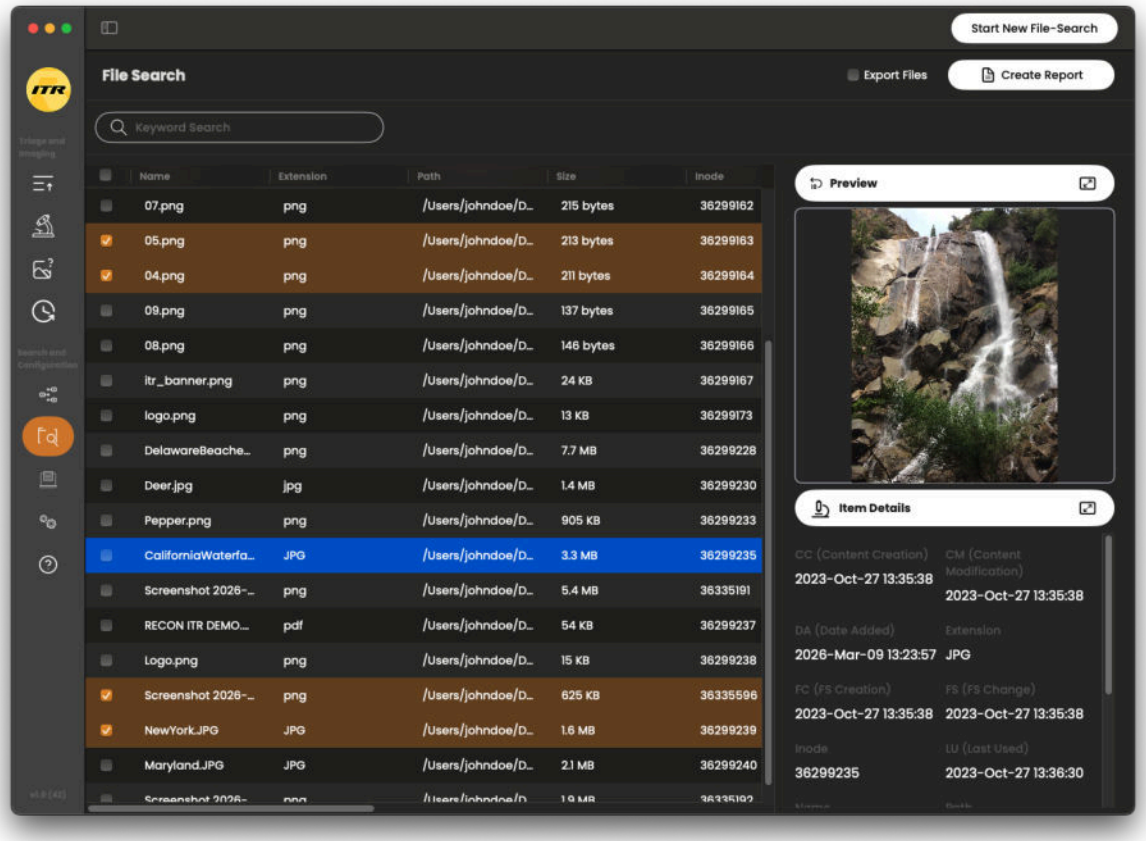
Active – If an item is marked as active it will appear in File Search as a runnable category

11.1.6.2 Items

Each category contains individual search items such as file signatures, file names, or keywords. The following controls are available for managing items: - **+ (Add)** – Creates a new search item within the selected category. - **– (Remove)** – Removes the selected item. - **Pencil Icon** – Allows the selected item to be renamed or edited. - **File Icon** – Pastes the contents of the clipboard and separates entries using newline characters, allowing multiple items to be added at once. - **Active** – If an item is marked as active it will be run when its category is selected. If it is not marked as active, the item will not be run, even if its category is selected

Once the search criteria have been configured, the examiner can return to the **File Search tab** to select the categories to run during the search. The results can then be reviewed through the File Search results interface.

11.2 Analysis



The analysis of **File Search** can be conducted after the FIle Search process has finished

running.

11.2.1 Filtering and Searching

The **File Search** includes tools that allow examiners to quickly narrow results and locate relevant activity. - **Keyword Search** – Allows the examiner to search **File Search** records for matching keywords.

11.2.2 Artifact Review

When a record is selected, additional information is available through the preview and item details panels. - **Preview Panel** – Allows the examiner to open the source file for the selected artifact using Apple's native preview functionality. - **Item Details** – Displays detailed information about the selected record, including the timestamps associated with the event and general file information.

11.2.3 Table Right-Click Options

The **File Search** results table includes several context menu options that assist with reviewing and organizing artifacts. - **QuickLook** – Opens the selected record’s source file using Apple's native preview. - **Bookmark** – Bookmarks the selected item. - **Remove Bookmark** – Removes the bookmark from the selected item. - **Bookmark All** – Bookmarks all records currently displayed in the table. - **Remove All Bookmarks** – Removes bookmarks from all displayed records.

11.2.4 Creating Reports

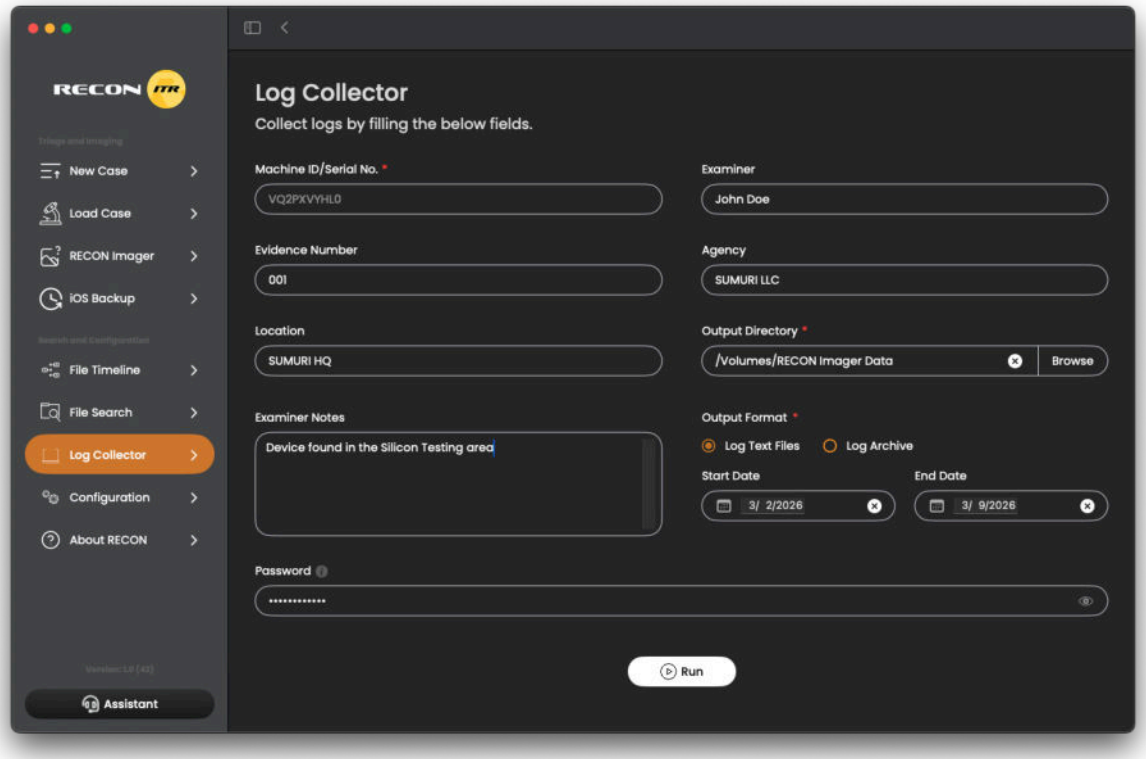
Reports can be generated directly from the **File Search** analysis view to export the analyzed records. Report scope options include: - **Bookmarked Items** – Includes only bookmarked records. - **All Items** – Includes every record currently present in the File Timeline table. - **Screen Items** – Includes only records currently displayed after filtering or searching.

Available report formats: - **HTML** - **PDF** - **CSV**

Additional Options - **Export Files** - This will export the selected files alongside the report. When files are exported, they will keep the same relative file path. These files will be exported to a directory.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

12 Log Collector



The **Log Collector** in **RECON ITR** is used to acquire Apple Unified Logs (AUL) from the system. Apple Unified Logs contain detailed records of system and application activity and can be useful for reconstructing system events, identifying user actions, and troubleshooting system behavior. The **Log Collector** allows the examiner to configure how logs are collected, define a time range for the acquisition, and select the format in which the logs will be exported.

12.1 Log Collector Configuration

Before starting a collection, the examiner can configure several options that determine how the Apple Unified Logs will be acquired and exported.

12.1.0.1 Output Format

The examiner can select the format in which the logs will be exported. - **Log Archive** – This option collects logs in Apple's native log archive format, which preserves the structure of Apple Unified Logs and is intended for use with Apple's log viewing tools and other

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

compatible analysis utilities. - **Log Text Files** – This option exports the logs as raw text files, allowing them to be easily reviewed using standard text editors or log analysis tools.

12.1.0.2 Date Range

The examiner can define a starting date for log collection, which limits the logs to entries occurring on or after the selected date. An ending date can also be specified when the Log Text Files format is selected. When using the Log Archive format, the ending date option is not available.

12.1.0.3 Output Directory

The **Output Directory** specifies where the **Log Collector** case folder will be written. Once the acquisition process has completed, the collected logs and associated metadata will be stored in this directory.

12.1.0.4 Administrator Password (Optional)

The examiner may provide the administrator password to allow **RECON ITR** to access additional logs that require elevated privileges. This field is optional, but providing the administrator password is strongly recommended, as it may allow the collection of a more complete set of Apple Unified Logs.

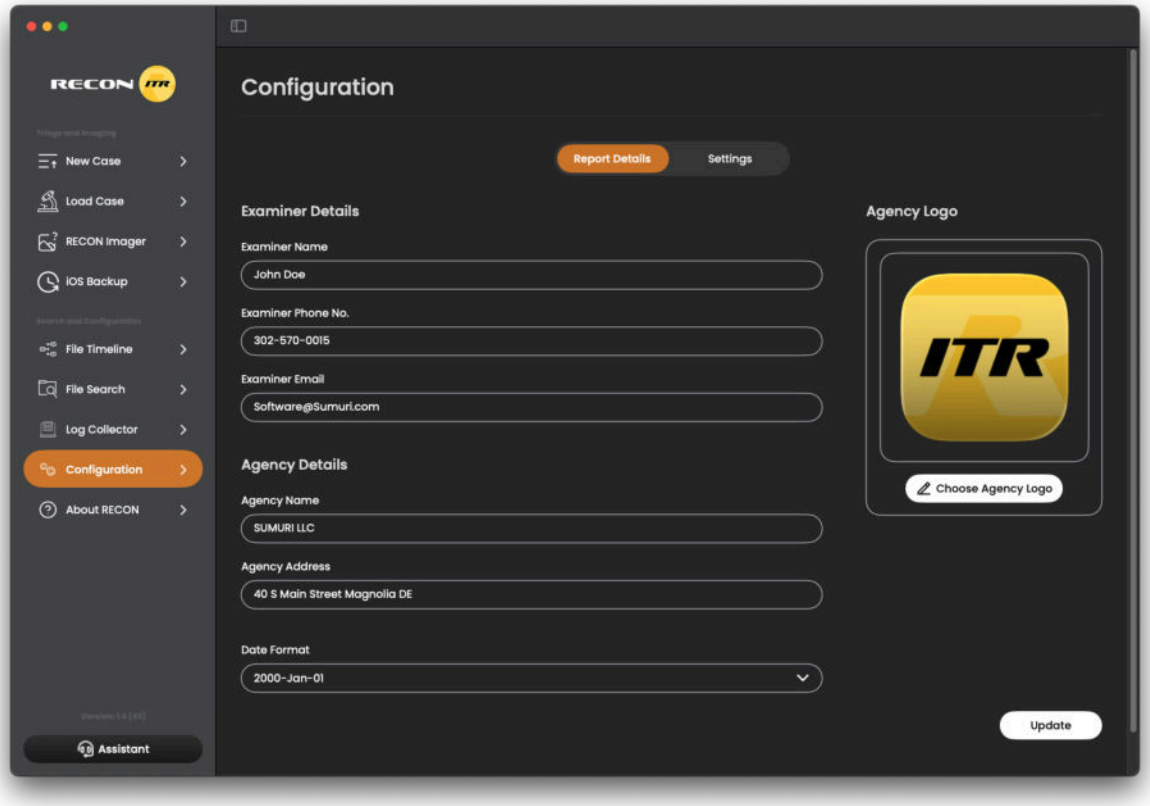
12.2 Acquisition Process

When the examiner presses “**Run”**, **RECON ITR** begins collecting Apple Unified Logs using the selected configuration options. After the acquisition has completed, a case folder will be created in the selected output directory containing the collected logs and metadata describing the acquisition.

12.2.0.1 Case Metadata Files

Each Log Collector case includes two metadata files that document the acquisition process. - **_case_report.txt** – A text report containing case information such as: - Acquisition start time - Acquisition completion time - Case metadata entered when the case was started - **_case_report.html** – An HTML version of the same report contained in _case_report.txt, formatted for easier viewing in a web browser.

13 Configuration



The Configuration tab allows examiners to define application settings and examiner details used throughout **RECON ITR**. Information entered in this section is automatically applied to case creation dialogs and reports generated by the tool. This helps ensure consistent case metadata and reporting information across multiple cases and examinations. The Configuration section contains two tabs: - Report Details - Settings

13.1 Report Details Tab

The Report Details tab allows the examiner to define metadata that will automatically populate various case creation fields and appear in generated reports. Metadata fields that can be selected and entered: - **Examiner Name** – The Examiner name will be included in the reports and will autofill during Case Creation of different triage cases. - **Agency Name** – The Agency name will be included in the reports and will autofill during Case Creation of different triage cases. - **Date Format** – The Date Format setting determines how dates are displayed within the **RECON ITR** triage and analysis windows. - **Agency Logo** – The Agency Logo setting

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

allows the examiner to replace the default report logo with their own agency logo. The selected logo will appear in reports generated by **RECON ITR**. Supported formats include - JPG - PNG - **Additional Report Metadata** – Other metadata fields available in this section will appear in generated reports and provide additional case documentation details.

13.2 Settings Tab

The Settings tab contains additional configuration options related to application behavior and configuration management.

13.2.0.1 Configuration Sync

Configuration Sync allows an examiner to import configuration settings from another **RECON ITR** instance. This is useful when an examiner maintains multiple **RECON ITR** drives and wants their configuration and report settings to remain consistent across them. To synchronize configuration settings: 1. Locate the **RECON ITR** instance that already contains the desired configuration settings. 2. Navigate to the location where the **RECON ITR** application is launched from (commonly the LIVE partition). 3. Copy the “**Configuration”** folder located inside the “**ReconITR Resources”** directory. 4. Launch the **RECON ITR** instance you want to update. 5. Use **Configuration Sync** to point to the copied “**Configuration”** folder. 6. Once selected, the settings from that configuration will be applied.

13.2.0.2 Debug Logging

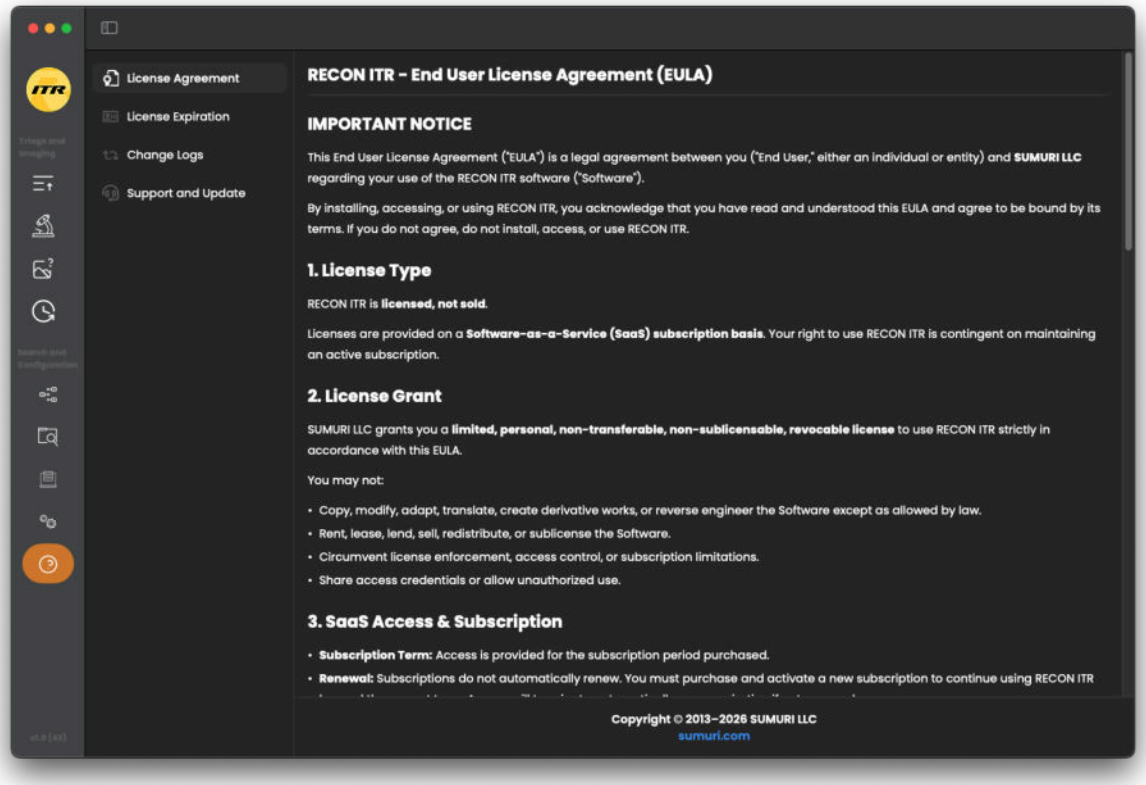
The Enable option allows **RECON ITR** to generate debug logs. These logs can be useful for troubleshooting and may be shared with the **SUMURI** development team if an issue occurs while using the tool. Debug logs are stored in the ReconDebugLogs directory located in the same location where **RECON ITR** was launched. This will commonly be the LIVE partition.

Notice:

Debug logs are not encrypted, and examiners should review them before sharing with SUMURI because they may contain potentially sensitive or private information.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

14 About RECON



The **About RECON** section provides examiners with important information about the software, licensing, updates, and support resources. This section is organized into four tabs, each focusing on a specific aspect of the application.

14.0.0.1 License Agreement

The **License Agreement** tab displays the current **End User License Agreement** (EULA) for **RECON ITR**. Examiners can review the terms and conditions governing the use of the software in this tab.

14.0.0.2 License Expiration

The License Expiration tab shows the date on which the current license will expire. Examiners can also use this tab to point to a new license file if they need to update or renew their

license.

14.0.0.3 Change Logs

The Change Logs tab displays a list of recent changes, updates, and fixes that have been made to the software. This provides examiners with a historical record of software updates and improvements.

14.0.0.4 Support and Update

The Support and Update tab provides web links to commonly accessed resources, including support documentation, tutorials, and update information. This tab allows examiners to quickly access resources that may assist with troubleshooting, learning new features, or keeping the software up to date

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

15 Appendix

15.1 Apple Extended Attributes

Apple Extended Attributes are specialized metadata in macOS that store additional file information, such as creation, user access times, system access times, and modification times. This metadata may not be visible in Windows-based forensic tools. Why it matters: - Preserves accurate timestamps and file metadata. - Ensures reliable timeline reconstruction. - Allows **RECON ITR** to provide a complete view of file activity.

RECON ITR Advantage: RECON ITR and **RECON IMAGER** automatically recognize and preserve Extended Attributes, ensuring investigators see correct macOS timestamps and full metadata.

15.2 APFS

Apple File System (APFS) is Apple's proprietary file system used across macOS, iOS, watchOS, and tvOS. APFS introduces advanced features such as snapshots, space sharing, and improved metadata handling, which are important in forensic investigations.

15.2.0.1 Key Points About APFS

- **Native Support** – Fully supported in macOS High Sierra (10.13) and later.
- **Partial Support** – Limited support in macOS Sierra (10.12).
- **Windows Support** – No native APFS support in Windows. Windows-based forensic tools rely on reverse-engineered implementations, which can be incomplete or unreliable.

Important: Analysts should exercise caution when using Windows tools to process APFS volumes, as these may not fully preserve APFS structures or metadata.

15.2.1 RECON ITR and APFS

RECON ITR is built natively for macOS and fully supports APFS and other Mac file systems. APFS volumes and containers are processed accurately without relying on reverse-engineered methods.

15.2.1.1 Supported Imaging Options

- **Logical Copies of APFS Volumes** – Creates logical forensic images of individual

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

APFS volumes. These images can be imported into forensic tools that support directories or files, including some Windows tools.

- **Block Copies of Synthesized APFS Containers** – Captures block-level forensic images of entire APFS containers, commonly used in macOS installations.

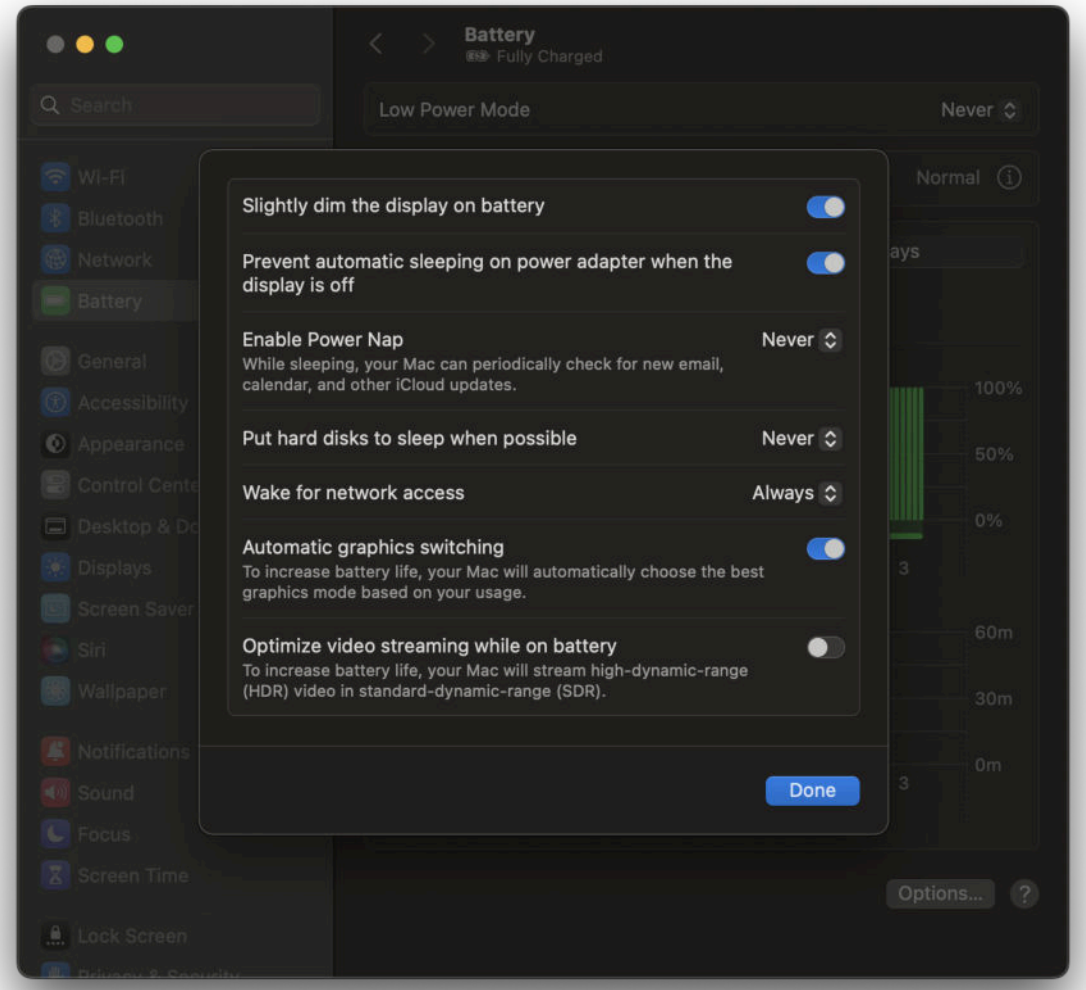
15.2.1.2 Data Volume vs System Volume (Macintosh HD)

Modern versions of macOS separate the operating system and user data into two distinct volumes within the same APFS container. On most systems, these volumes appear as **Macintosh HD** and **Macintosh HD – Data**. The **Macintosh HD** volume is the system volume. This volume contains the macOS operating system files and is mounted as a read-only volume during normal operation. Its contents generally only change when macOS is updated. The **Macintosh HD – Data** volume is the data volume. This volume contains the system's read/write data, including user home directories, application data, and other files created or modified during normal system use. For forensic acquisitions, it is typically recommended to image the APFS Data Volume (Macintosh HD – Data), as this volume contains the majority of

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

user-generated and application-related data relevant to an investigation.

15.3 Energy and Power Settings



The Energy and Power Settings on a Mac control: - How long the device stays logged in while idle - When the screen turns off - When hard disks go to sleep

Proper configuration of these settings is critical when using **RECON ITR** for imaging or triage. If the Mac goes to sleep during an acquisition, the process can be interrupted, potentially

impacting evidence collection.

15.3.0.1 Why Adjust Energy Settings?

Before starting any imaging or triage process, adjust the **Energy and Power Settings** to prevent the Mac from sleeping. When performing imaging or triage in the live environment: - Ensure the device remains active and awake throughout the process. - Preventing sleep avoids interruptions in imaging, triage, or evidence collection.

Disabling Sleep Settings on Macs Without a Battery 1. Click the Apple icon in the top-left system toolbar. 2. Select System Settings. 3. Navigate to Energy. 4. Disable Put hard disks to sleep when possible.

Disabling Sleep Settings on MacBooks (Laptops with Batteries) 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 Options (bottom right corner). 5. Set Put hard disks to sleep when possible to Never.

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 to ensure uninterrupted imaging or triage.

Notice:

Energy settings only ever need to be adjusted if using the live RECON ITR application.

15.4 Firmware Password

Firmware Passwords are a security feature on Intel-based Macs that prevent unauthorized booting from external devices or alternate startup volumes. Apple Silicon Macs (M1, M2, M3, M4) do not use traditional **Firmware Passwords**. Startup security is managed through the Secure Enclave and Activation Lock, so you will not encounter a **Firmware Password** lock screen on these devices. **When enabled on Intel Macs, a Firmware Password:** - Blocks access to Startup Options without the password. - Prevents booting from anything other than the internal macOS installation. - Displays a **lock icon** when pressing **ALT/OPTION** during startup.

15.4.0.1 Removal of Firmware Passwords

- Only Apple Certified Technicians can remove Firmware Passwords with proper authorization.
- Law enforcement may contact Apple Legal if required under applicable laws.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

- Firmware Passwords are hardware-level protections and are different from standard macOS login passwords.

15.5 FileVault

FileVault is Apple's full-disk encryption feature used to protect data on macOS systems. It encrypts both the System and Data APFS volumes on a Mac.

15.5.0.1 FileVault Behavior

- If a user is logged in, the APFS Data Volume is unlocked and imaging can proceed normally.
- If the device is powered off or the user is logged out, FileVault locks the volume and the data remains encrypted.
- To unlock a FileVault-protected volume, one of the following is required:
    - The administrator account password, or
    - The FileVault recovery key.

15.5.0.2 Imaging Considerations

- When the device is logged in, the volume is already decrypted and imaging can proceed.
- When the device is powered off or logged out, FileVault must be unlocked before imaging.

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

15.5.0.3 Non-T2 Intel Macs

On non-T2 Intel Macs, if neither the password nor recovery key is available, and file vault is enabled, the physical disk can still be imaged in its encrypted state. If the password or recovery key becomes available later, the encrypted image can be processed and decrypted using **RECON LAB**. Imaging an encrypted disk without credentials captures the encrypted data exactly as stored, not the decrypted contents.

15.6 Full Disk Access

Full Disk Access is a macOS security feature that allows applications to access files and directories that are normally restricted, including system files, user data, and other protected areas. Granting Full Disk Access to **RECON ITR** is highly recommended when using Live

Imaging or Live Triage.

15.6.0.1 Why Full Disk Access is Important

Without Full Disk Access, the **RECON ITR** live application may not be able to access all system artifacts, user files, or application data. This can result in incomplete triage results or missing evidence. Granting Full Disk Access helps ensure a complete and thorough acquisition during live imaging and triage.

15.6.0.2 Granting Full Disk Access to RECON ITR

1. Open System Settings.
2. Select Privacy & Security from the sidebar.
3. Scroll down and select Full Disk Access.
4. Click the + (Add) button.
5. Locate and select the **RECON ITR** application.
6. Enter the administrator username and password if prompted.

> **Notice:**
>
> Full Disk Access is not required when using a bootable imaging environment, since those environments operate outside of macOS user permissions.

15.7 Local Time Machine Snapshots

Time Machine is the built-in backup utility in macOS. It normally creates backups of files and system data to an external or network disk known as the Time Machine disk.

15.7.0.1 How Local Time Machine Snapshots Work

If the Time Machine backup disk is not connected, macOS may still create temporary backups on the internal drive. On APFS-formatted systems, these temporary backups are stored as Local Time Machine Snapshots, often referred to simply as APFS Snapshots.

15.7.0.2 Key Points

- Local snapshots are stored within the APFS file system on the internal drive.
- They allow macOS to maintain backup points even when the external Time Machine disk is unavailable.
- macOS automatically manages these snapshots, deleting older ones when disk space becomes limited.
- These snapshots may contain previous versions of files that have since been

modified or deleted

15.8 Secure Enclave

The Secure Enclave is a dedicated security component in modern Macs that protects sensitive data and manages encryption keys. It ensures that data stored on the device remains secure and enforces system integrity, including the boot process and disk encryption. Examiners should understand that the Secure Enclave affects how data can be accessed and imaged, particularly on systems with T2 Intel chips and Apple Silicon Macs.

15.8.1 History and Function

The Secure Enclave was first introduced with the Apple T2 Security Chip in Intel Macs, beginning with the iMac Pro in December 2017. On these systems, the Secure Enclave operates as a separate co-processor alongside the main Intel CPU. It performs critical security functions, including: - Managing disk encryption keys - Protecting Touch ID and other sensitive data - Securing the boot process and enforcing system integrity

Each Secure Enclave contains a unique hardware identifier (UUID) that is permanently embedded during manufacturing. This UUID is used to derive encryption keys for the device's storage and is inaccessible to the operating system, applications, or users, providing a hardware-level security foundation for macOS.

15.8.1.1 Apple Silicon Integration

With the introduction of Apple Silicon (M1 and later) in 2020, the Secure Enclave was integrated directly into the system-on-chip (SoC). While the hardware design changed, the Secure Enclave continues to handle: - Encryption key management - Data protection - System security enforcement

15.8.2 Imaging Considerations

On Macs with a Secure Enclave—T2 Intel Macs and Apple Silicon—physical imaging of the internal storage is not possible. Examiners can instead capture: - The APFS Data Volume, or - The Synthesized APFS Container

Authentication is commonly** required to access these volumes: - Administrator password, or - FileVault recovery key

15.9 Startup Security Utility

Startup Security settings control whether a Mac can boot from external devices and enforce operating system trust. Examiners need to understand these settings when preparing a Mac

for bootable imaging with **RECON ITR**. On Apple Silicon Macs, no changes are typically required to boot **RECON ITR**, while Intel Macs with a T2 chip may require adjusting Startup Security settings. Intel Macs with a T2 chip manage Startup Security through the Startup Security Utility in Recovery Mode, which may require lowering security settings to allow external booting. Apple Silicon Macs use Security Policy settings in RecoveryOS and generally allow external booting by default, so no changes are needed.

15.9.0.1 Lowering Startup Security on Intel T2 Macs

Intel Macs with a T2 chip may require adjustments to allow booting from an external drive. To lower security settings: 1. Power down the Mac. 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 menu bar, select Utilities ➔ Startup Security Utility. 5. Authenticate if required. 6. Under Secure Boot, select No Security. 7. Under Allowed Boot Media, select Allow booting from external or removable media. 8. Close the window and shut down from the Apple menu. 9. Boot again and select the **RECON ITR** drive.

15.9.0.2 Overview

Apple Silicon Macs can boot from **RECON ITR** without modifying security settings. Intel T2 Macs require lowering security settings via the Startup Security Utility (No Security + Allow External Boot). Examiners should also verify whether a Firmware Password or Activation Lock is present, as these can restrict access even when Startup Security is adjusted.

15.10 Target Disk Mode (TDM) & Share Mode

Target Disk Mode (TDM) and Share Mode are macOS features that allow a Mac to behave like an external drive, making it accessible from another Mac. These modes are useful for transferring large amounts of data or performing forensic imaging with **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. Examiners can then target the disk for imaging as if it were an attached external drive.

15.10.0.1 Platform Support

- Target Disk Mode (TDM) – Available on Intel Macs only. The Mac's internal storage is mounted directly as an external drive over Thunderbolt or USB-C.
- Share Mode – Available on Apple Silicon Macs only. The Mac shares its internal volume over the network as an SMB server.

15.10.0.2 Connecting Intel Macs via Target Disk Mode (TDM)

1. Connect the examiner Mac and the target Mac using a Thunderbolt or USB-C cable.
2. Power off the target Mac.

3. Press and hold the T key, then press the power button.
4. Continue holding T until the Target Disk Mode symbol appears (Thunderbolt or USB).
5. On the examiner Mac, the target Mac's internal drive will mount as an external disk.
6. Use **RECON ITR** to image the mounted drive as normal.

15.10.0.3 Connecting Apple Silicon Macs via Share Mode

1. Connect the examiner Mac and the target Mac using a Thunderbolt or USB-C cable.
2. Shut down the target Mac.
3. Press and hold the power button until the Startup Options appear.
4. Click Options, then Continue to enter RecoveryOS.
5. In the Mac Utilities window, click Utilities in the menu bar and select Share Disk.
6. Choose the volume to share and click Start.
7. On the examiner Mac, open Finder and navigate to the Network section. The target Mac's shared disk will appear.
8. **RECON ITR** can then target the shared volume for imaging.

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

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

16 Glossary

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

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.
Secure Enclave	A dedicated security processor that manages encryption keys, authentication data, and sensitive operations on Macs with T2 Intel 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.

17 Third-Party Software & License Notices

RECON ITR includes the following open-source software components. This notice is provided in compliance with the applicable license terms.

17.0.1 Third-Party Components

Component	Copyright	License
GRDB.swift	Gwendal Roué	MIT
TPPDF	Philip Niedertscheider / techprimate GmbH	MIT
ZIPFoundation	Thomas Zoechling	MIT
CSV.swift	Yasuhiro Hatta	MIT
Lottie for iOS	Airbnb, Inc.	Apache 2.0
OpenSSL	The OpenSSL Project Authors	Apache 2.0
dc3dd	Department of Defense Cyber Crime Center	GPL v3
rsync	Andrew Tridgell, Paul Mackerras, et al.	GPL v3
libewf	Joachim Metz	LGPL v3

17.0.2 Source Code Availability

Certain components included with RECON ITR are licensed under the GNU General Public License (GPL) or the GNU Lesser General Public License (LGPL). In accordance with these licenses, the complete corresponding source code for these components is available upon request. To obtain source code, please contact: **SUMURI, LLC** Email: sumuri.com">support@sumuri.com Web: sumuri.com This offer is valid for three (3) years from the date of distribution of the corresponding version of RECON ITR.

17.0.3 License Texts

17.1 MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software

and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

17.1.0.1 Apache License, Version 2.0

Licensed under the Apache License, Version 2.0 (the "License"); you may not use these components except in compliance with the License. You may obtain a copy of the License at: https://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

17.1.0.2 GNU General Public License, Version 3

Certain components are licensed under the GNU General Public License, Version 3 (GPL v3). You may obtain a copy of the license at: https://www.gnu.org/licenses/gpl-3.0.html These components are free software: you can redistribute them and/or modify them under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version. They are distributed in the hope that they will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

17.1.0.3 GNU Lesser General Public License, Version 3

Certain components are licensed under the GNU Lesser General Public License, Version 3 (LGPL v3). You may obtain a copy of the license at: https://www.gnu.org/licenses/lgpl-3.0.html These components are free software: you can redistribute them and/or modify them under the terms of the GNU Lesser General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

18 Terms and Conditions

Copyright © 2013–2025 SUMURI LLC ** IMPORTANT NOTICE **This End User License Agreement ("EULA") is a legal agreement between you ("End User," either an individual or entity) and** SUMURI LLC **regarding your use of the RECON ITR software ("Software"). By installing, accessing, or using RECON ITR, you acknowledge that you have read and understood this EULA and agree to be bound by its terms. If you do not agree, do not install, access, or use RECON ITR.** 1. License Type **RECON ITR is** licensed, not sold**. Licenses are provided on a** Software-as-a-Service (SaaS) subscription basis**. Your right to use RECON ITR is contingent on maintaining an active subscription.** 2. License Grant **SUMURI LLC grants you a** limited, personal, non-transferable, non-sublicensable, revocable license** to use RECON ITR strictly in accordance with this EULA. You may not: - Copy, modify, adapt, translate, create derivative works, or reverse engineer the Software except as allowed by law. - Rent, lease, lend, sell, redistribute, or sublicense the Software. - Circumvent license enforcement, access control, or subscription limitations. - Share access credentials or allow unauthorized use.

3. SaaS Access & Subscription - **Subscription Term**: Access is provided for the subscription period purchased. - **Renewal**: Subscriptions do **not** automatically renew. You must purchase and activate a new subscription to continue using RECON ITR beyond the current term. Access will terminate automatically upon expiration if not renewed. - **Termination**: SUMURI LLC may suspend or terminate your access for breach of this Agreement or non-payment. Upon termination or expiration, all rights to use RECON ITR immediately cease. - **Notifications**: SUMURI LLC may send courtesy reminders before expiration, but you remain solely responsible for timely renewal.

4. Ownership & Intellectual Property - RECON ITR is the exclusive property of SUMURI LLC and its licensors. - This license does not transfer any ownership rights. - All rights not expressly granted to you are reserved by SUMURI LLC.

5. Restrictions You may not: - Use RECON ITR for unlawful purposes. - Remove or alter proprietary notices or trademarks. - Interfere with, bypass, or attempt to gain unauthorized access to any licensing, activation, or security mechanism within the Software.

6. Updates & Support - Updates and upgrades are available only during an active subscription. - Debug logs, updates, and support files are generated and submitted manually at the discretion of the user. - SUMURI LLC provides support according to its then-current support policies but does not guarantee resolution of all issues.

7. Data & Privacy - **Offline Use**: RECON ITR is designed to operate fully offline. Internet connectivity is required only for manual license activation, renewal, or optional updates. - **No**

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com

Data Collection: SUMURI LLC does not collect, access, or transmit any user data, forensic evidence, case files, or related information processed with RECON ITR. - **User Control**: All updates, debug logs, and support files are created and shared solely at the discretion of the user. Nothing is transmitted automatically. - **Responsibility**: You remain solely responsible for maintaining the confidentiality, legality, and integrity of any data you process with RECON ITR.

8. Disclaimer of Warranties THE SOFTWARE IS PROVIDED **"AS IS" AND "AS AVAILABLE"** WITHOUT WARRANTIES OF ANY KIND. SUMURI LLC DISCLAIMS ALL EXPRESS, IMPLIED, AND STATUTORY WARRANTIES, INCLUDING BUT NOT LIMITED TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. **9. Limitation of Liability** To the fullest extent permitted by law: - SUMURI LLC's total liability shall not exceed the fees paid by you for the subscription during the twelve (12) months preceding the claim. - SUMURI LLC shall not be liable for indirect, incidental, consequential, or special damages (including lost profits, business interruption, or data loss), even if advised of the possibility of such damages.

10. Indemnification You agree to indemnify and hold harmless SUMURI LLC, its officers, employees, and affiliates from any claims, damages, or expenses arising from: - Your breach of this EULA, - Your misuse of the Software, or - Any violation of applicable laws or third-party rights.

11. Termination This Agreement is effective until terminated. It may be terminated: - By you, upon expiration of your subscription; - Automatically, if you fail to comply with this EULA; - By SUMURI LLC, for cause or non-payment.

Upon termination or expiration, you must immediately cease all use of RECON ITR. **12. Jurisdiction** This Agreement shall be governed by and construed under the laws of the State of Delaware, USA, without regard to conflict of law provisions. You consent to the **exclusive jurisdiction of the federal and state courts of Delaware**. **13. Entire Agreement** This EULA, together with your purchase or subscription order, constitutes the **entire agreement** between you and SUMURI LLC with respect to RECON ITR. No prior or contemporaneous agreements override these terms.

P.O. BOX 121 Magnolia, Delaware 19962 USA • +1 302 570 0015 • hello@sumuri.com • www.sumuri.com