RECON LAB Manual

1. Introduction

RECON LAB is a full Forensic Suite that supports numerous file systems such as Windows, macOS, Linux, iOS, Android and more. RECON LAB was created to solve multiple problems inherent in other forensic tools and to expedite processing and analysis without sacrificing the quality of the exam.

RECON LAB was designed, developed and runs on macOS. MacOS was the only logical choice for developing a modern forensic tool to support the most common and largest number of file systems and artifacts without losing data.

The most difficult file system and operating system (OS) for most forensic tools to support is macOS. Mac understands itself and can interpret its own artifacts. This is not true of other file

systems, operating systems, and other forensic tools as they do not natively support macOS and its artifacts.

In addition to supporting its own file system and artifacts, macOS supports a multitude of other file systems and the artifacts of Windows, Linux, Unix and many more.

RECON LAB is the only full Forensic Suite designed natively on macOS to take full advantage of the power within macOS. Other forensic tools that run on a Mac were ported from other non-Mac operating systems and experience limitations. Instead of utilizing native macOS libraries they rely on reverse engineering and third-party applications which can lead to missed data, improper interpretation of data and slower processing times.

RECON LAB primarily relies on native macOS libraries so support for new macOS file systems and/or artifacts is quick or instantaneous.

RECON LAB comes with one full year of free updates and support.

1.1 Why Use a Mac for Forensic Analysis?

Until the release of RECON LAB, no other forensic tool properly processed or utilized the correct timestamps for macOS.

This is only one example of an extremely important artifact that is improperly interpreted or missed completely by other forensic tools.

It is imperative to understand the importance of macOS in forensic exams and what may be missed by other forensic tools.

1.1.1 Apple Extended Attributes

Apple Extended Attributes are special metadata created only within macOS to allow searches via the macOS search utility - Spotlight.

Apple Extended Attributes contain extremely valuable information for investigations. This special metadata cannot be seen in Windows. Most Windows forensic tools ignore or have a limited ability to display Apple Extended Attributes as they are not natively supported.

Images and data collected by SUMURI's RECON ITR and processed by RECON LAB provide the most extensive views of Apple Extended Metadata.

Understanding Apple Extended Metadata is critical to investigations.

1.1.2 Viewing Proper Timestamps

Apple's macOS utilizes Apple Extended Attributes for timestamps in favor of POSIX (Unix) timestamps.

RECON IMAGER, when used with RECON LAB, is the only solution to properly view and utilize the correct macOS timestamps.

1.1.3 Viewing Files Natively

There are many file types and artifacts proprietary to macOS. As RECON LAB is designed on macOS it supports all macOS files and artifacts natively.

For example, Applications in macOS are actually "bundle" files. Everything needed for the application to run is found within the bundle file. What looks and appears to a single file to the Mac user is actually thousands of innocuous files and folders. In traditional forensic tools, these bundle files are expanded adding unnecessary artifacts to your case.

RECON LAB also is integrated with macOS's Quick Look which natively supports viewing hundreds of file types without needing or using the original application. Unlike other forensic tools, the files do not have to be exported first to view saving time.

1.1.4 Apple File System (APFS)

Apple File System (APFS) is a proprietary file system from Apple and utilized for macOS, iOS, watchOS, and tvOS. APFS is natively and fully supported on macOS High Sierra (10.13) and above. APFS has limited support in macOS Sierra (10.12). APFS has no support within Windows operating systems. Any support for APFS on Windows and/or Windows forensic tools are using reversed engineered non-native technologies.

SUMURI's RECON ITR can create forensic images that can be processed and analyzed with RECON LAB natively.

RECON ITR and RECON LAB also automatically supports the imaging and processing macOS 10.15 System and user DATA partitions.

1.1.5 Local Time Machine Snapshots (APFS)

Time Machine is a utility in macOS that is used for creating backups. Time Machine must be activated by the user and requires a local or remote disk to store the backups (Time Machine disk). If the Time Machine disk is not available the backups are stored locally. These backups are known as "Local Time Machine Snapshots" in APFS. They are also sometimes referred to as APFS Snapshots.

RECON IMAGER (included with RECON ITR) along with RECON LAB are the only solutions that can display, image, hash and analyze Local Time Machine Snapshots in Macs with T2 Security Chipsets and without.

Note: An examiner should not expect to find Local Time Machine Snapshots in every case. They will only exist when the conditions above have been met.

1.1.6 FileVault

FileVault (version 2) is the macOS full *volume* encryption of which there are no backdoors. FileVault is mounted and decrypted with the user's login password or Recovery Key which is created when FileVault was originally enabled.

RECON LAB allows the examiner to decrypt the forensic image of a Mac encrypted with FileVault natively using either the password or Recovery Key.

1.1.7 Support for Other File Systems

RECON LAB was designed to harness the power of macOS. Whatever the Mac can mount, RECON LAB can process.

MacOS natively supports APFS, macOS Extended (HFS+), MS-DOS FAT, ExFAT and NTFS (as read-only).

Using freely available open-source FUSE solutions and Paragon Software drivers (included) just about any file system can be mounted and processed with RECON LAB such as Linux ext2, ext3, and ext4.

1.2 Hybrid Processing Engine

Unlike any other forensic solution, RECON LAB utilizes a Hybrid Processing Engine.

The Hybrid Processing Engine processes a forensic image both inside RECON LAB and mounted outside RECON LAB using macOS.

The Hybrid Process Engine maximizes the recovery of artifacts and simultaneously increases the speed of processing.

Additionally, this approach uniquely allows RECON LAB to utilize the power of macOS natively.

1.3 Three Stage Analysis

RECON LAB offers three-stages of analysis.

Stage One – Parse and recovery thousands of artifacts with **Automated Analysis** of Windows, macOS, iOS, AndroidOS, and Google Takeout.

Stage Two – Four **Advanced Forensic Viewers** assist in parsing and examining macOS Property Lists (.plist), SQLite Databases, Hex, and the Window's Registry.

Stage Three – Utilize hundreds of features built into RECON LAB make **manual analysis** easier.

1.4 Support for Hundreds of Timestamps

RECON LAB currently supports several hundred individual timestamps. These include file systems, Apple Extended Metadata and application-specific timestamps.

These timestamps are integrated throughout RECON LAB to provide "one of a kind" analysis along with exponential reporting options.

Additionally, RECON LAB provides “second to none” chronological analysis and reporting.

1.5 Advanced Timelines

With such large support for hundreds of timestamps, RECON LAB can generate both textual and graphical views of events to make analysis easier.

Placing these events in chronological order allows an examiner to see events unfold minute by minute or even second by second.

Having the ability to see events in order based on time allows an examiner to solve cases and render opinions faster and more accurately.

1.6 Advanced Data Correlation

In a single day, a person of interest will probably use several devices capable of storing electronic data. For example, they may use a laptop or tablet at home, a mobile phone on their way to work and a desktop computer when they arrive. On each of these devices, our person of interest could use multiple web browsers and messaging apps. To add even more complexity, our person of interest is moving to different locations throughout the day and generating different location artifacts.

To get a clear picture of what our person of interest has done in a day RECON LAB has developed Advanced Data Correlation to collate all of this information into single views regardless of device or application.

Advanced Data Correlation (as **Redefined Results**) along with support for hundreds of timestamps provides an examiner with amazing investigative insight.

1.7 Advanced Reporting With Full Control

RECON LAB provides you with exponential reporting options from the granular level (single artifact) to the global level (all artifacts included).

Additionally, RECON LAB includes the first of its kind WYSIWYG (What You See Is What You Get) reporting mode called Story Board.

Story Board allows the user to have full control over the reporting process and is as easy to use as a word processor.

The examiner has the ability to add, remove or annotate bookmarks anywhere in the report at any time.

Story Board also allows you to add your bookmarks and tags in chronological order to make it easier to understand the timeline of events.

2. Recommended Minimum Requirements

Macs are unique in doing more with less. That being said, RECON LAB will work on most Macs.

Keep in mind the simple formula: **Processor + RAM = Speed**

The faster the processor and the more RAM that is installed will determine how fast you can process data.

2.1 Minimum Recommended Specifications for Running RECON LAB

Any Mac with an i7 Quad-core Processor or Apple Silicon (M1, M2, M3, or M4) equivalent with 16GB of RAM capable of running macOS 12.7.6 or above.

An Admin user required.

To get faster speeds, even with slower Macs, consider using a Thunderbolt 3 External RAID. Putting both the evidence and case files on the external Thunderbolt 3 RAID will provide an extra boost in the speed of processing.

SUMURI has tested and offers the ARECA 8-Bay Thunderbolt 3 RAID Storage with various storage options.

3. Helpful Hints

Before starting a new case with RECON LAB please refer to these helpful tips.

Use macOS Extended for Evidence Drives

The macOS can support a variety of file systems, however, in testing, we have the best results with macOS Extended (HFS+).

If you want to mount your macOS Extended evidence drive on Windows use the HFS+ for Windows drivers from Paragon Software that are provided to you with your purchase of RECON LAB.

Additionally, if you are creating logical images of Mac data to any non-Mac file system you will lose the Apple Extended Metadata.

Use Apple Disk Image Format (.dmg) for Imaging Evidence

The Apple Disk Image that is created with RECON ITR or PALADIN is a RAW image format that can be loaded into any forensic tool that supports RAW images. The .dmg image is natively supported by the Mac.

Although RECON LAB supports Expert Witness Formats (.E01, .Ex01) it is not native to the Mac and requires the use of FUSE. FUSE acts as an interpreter to mount non-native file systems. Using FUSE adds an additional unnecessary layer between the forensic image and RECON LAB and is not recommended.

Avoid Segmentation of Forensic Image Files

RECON LAB supports segmented image files. However, with extremely large disk sizes found in modern devices, thousands of segments can be created which may cause issues. If possible, avoid segmenting forensic images and use a single file.

4. Getting Support

Support for RECON LAB is available via our Online Support site and submitting a ticket here:
https://helpdesk.sumuri.com

During regular business hours, we strive to respond in less than one hour but no longer than 24 hours.

SUMURI is based in the state of Delaware, USA (Eastern Time Zone – EST/EDT).

Our office hours are 0900-1700 (9 a.m. – 5 p.m.). SUMURI is closed for US Federal Holidays.

Law Enforcement Emergency Support

If you are law enforcement, and are in need of immediate emergency assistance with any of our products, please contact us anytime at +1 302.570.0015.

5. Renewing RECON LAB

RECON LAB comes with one full year of support and updates. Once RECON LAB expires, its license will need to be renewed in order to continue to receive updates and support.

RECON LAB can be renewed online via our website here:
https://sumuri.com/product/recon-lab-renewal/

Additionally, RECON LAB can be renewed by contacting our office to be assisted by a team member

6. Training

SUMURI offers vendor-neutral training on Mac Forensics. SUMURI's courses teach the concepts and knowledge to use RECON ITR (or other tools) to process Mac artifacts and Mac file systems.

- Best Practices In Mac Forensics (MFSC-101)
- Advanced Practices In Mac Forensics (MFSC-201)

If interested in hosting a training course at your location and receiving up to two free seats please contact us via the link below.

- Hosting SUMURI Training

7. Installation

RECON LAB includes and relies on native libraries, some third-party applications and utilities to ensure that largest amount of data can be processed and analyzed.

Please install all the recommended applications, in order, and one at a time, using the instructions below.

Due to Mac's strict adherence to security, you may be asked to provide your password various times during the installation.

Periodically check to make sure that all dependent applications are updated:

Updates for RECON LAB can be downloaded at: https://sumuri.com/updates/

7.1 Installing Xcode and Command Line Tools

Xcode is a free development environment provided by Apple. Xcode and Xcode Command Line Tools include additional binaries and applications which are used in RECON LAB.

Installing Xcode

1.) Apple Xcode is available for free using Apple's App Store

2.) Click the "Get" button to install Xcode on your Mac via the Apple App Store.

3.) Be sure to open and fully install the application before going forward.

Installing Xcode Command Line Tools

To install or check to see if Xcode Command Line Tools are installed follow the instructions below:

1.) Open the Terminal Application – /Applications/Utilities/Terminal

2.) Type the following command and hit return: xcode-select --install

3.) Follow the instructions provided by the application.

7.2 Installing FUSE for macOS

FUSE for macOS is a free open-source application that acts as an interpreter for non-native file systems. FUSE for macOS assists in loading Expert Witness Format (EWF) forensic images such as .E01 and .Ex01. FUSE for macOS must be installed to mount and process EWF images.

Installing FUSE for macOS

1.) Navigate to the FUSE for macOS website and download the version that matches your macOS from here: https://osxfuse.github.io/

2.) Double-click on the .dmg file downloaded.

3.) Double-click on the “FUSE for macOS” icon to install.

4.) Follow the application instructions for completing the installation.

7.3 Installing Paragon Drivers

SUMURI has partnered with Paragon Software to include helpful file system drivers for both Mac and Windows. You will receive a license code for downloading and activating Paragon Software applications when you purchase a full version of RECON LAB.

To download and install Paragon Software applications follow the instructions below.

Accessing Paragon Software Applications

1.) Navigate to Paragon Software’s website and create an account if you do not already have one here: https://my.paragon-software.com/#/login

2.) Navigate to “Register New Product” and enter the code provided to you when you purchased RECON LAB.

3.) Navigate to “My Products” after entering the code to access and download your applications.

Installing extFS for Mac by Paragon Software

1.) Download extFS for Mac following the instructions above.

2.) Double-click on the .dmg downloaded from Paragon.

3.) Double-click on “Install extFS for Mac” to install drivers for Linux file systems.

4.) Complete the installation by following the instructions provided.

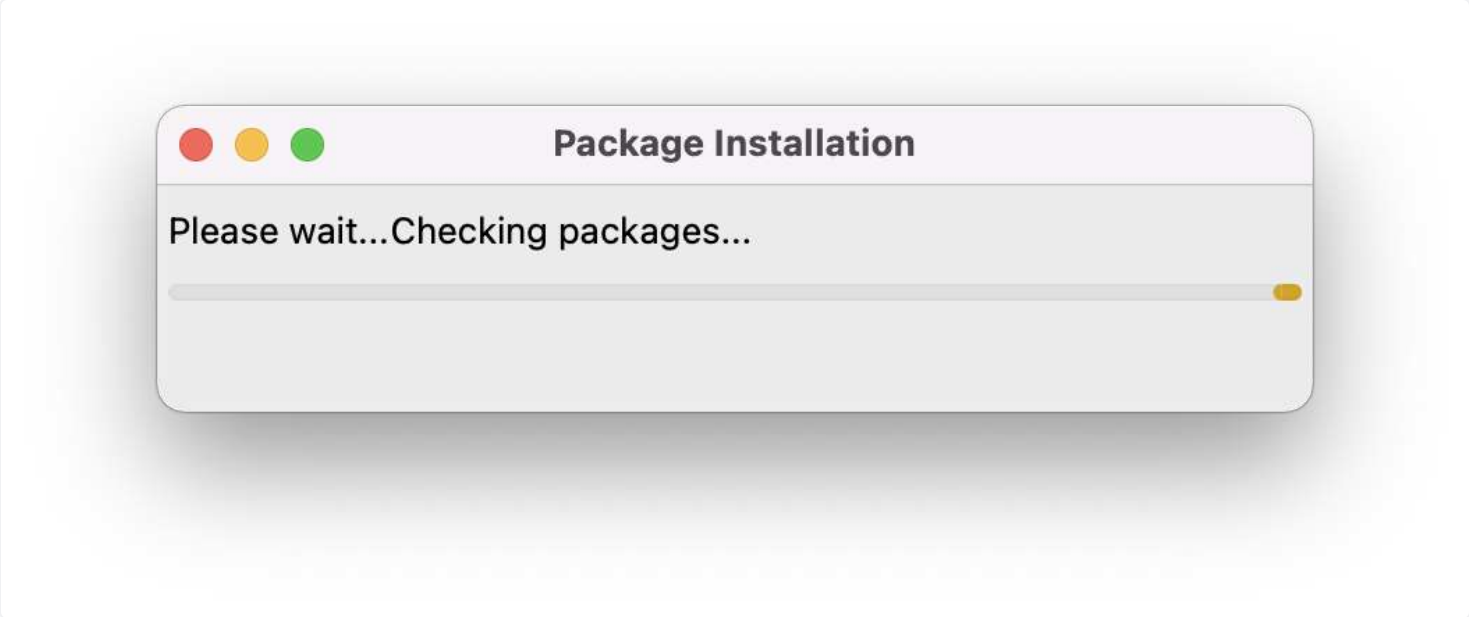
7.4 Installing RECON LAB

Make sure that you have downloaded the most current version of RECON LAB and follow the instructions below to install. Go to Section 7.7 for more information.

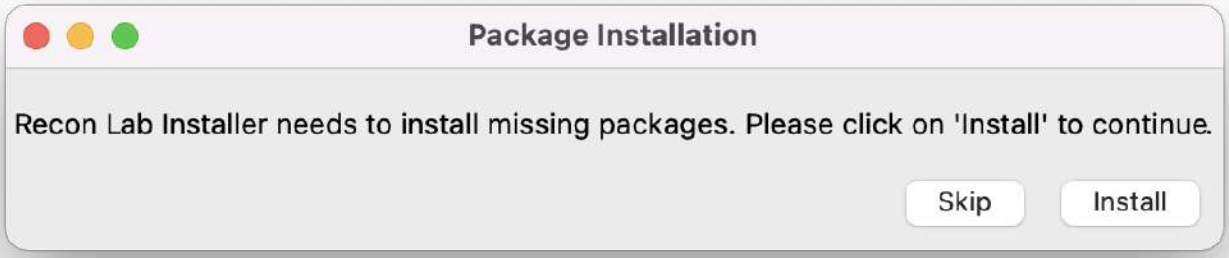
Move the RECON LAB installer .dmg to your Desktop and double-click to mount the installer.

A notification window will appear to ask if you want to open the application. Choose “Open”.

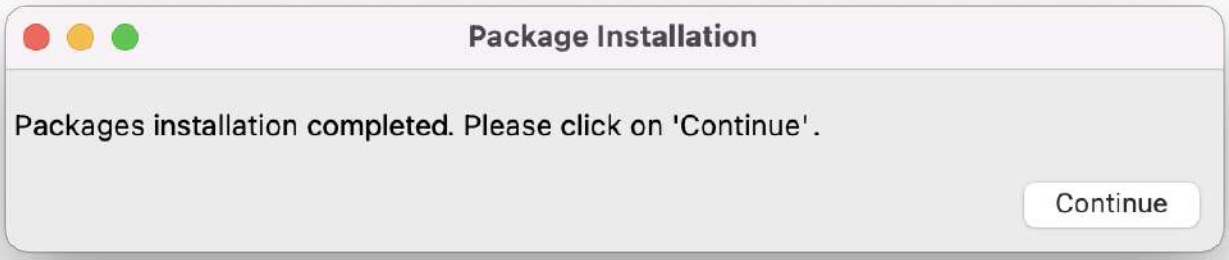
RECON LAB will then begin scanning to see if additional packages need to be installed and may prompt you to install extra components.



If prompted, select install to install the extra packages.



Once that has been completed, the installer will ask you to continue. Select Continue to launch the RECON LAB Installer.



The RECON LAB Installer window will now appear.

Choose one of the following options:

Install – Updates existing RECON LAB installations preserving your settings, examiner and agency information.

Clean Install – Use this for first time installs or to reset RECON LAB to its original settings.

Uninstall – Use this option to remove RECON LAB from your Mac.

When the installation reports **Done**, quit the installer and eject the RECON LAB Installer disk image (right-click “Eject”).

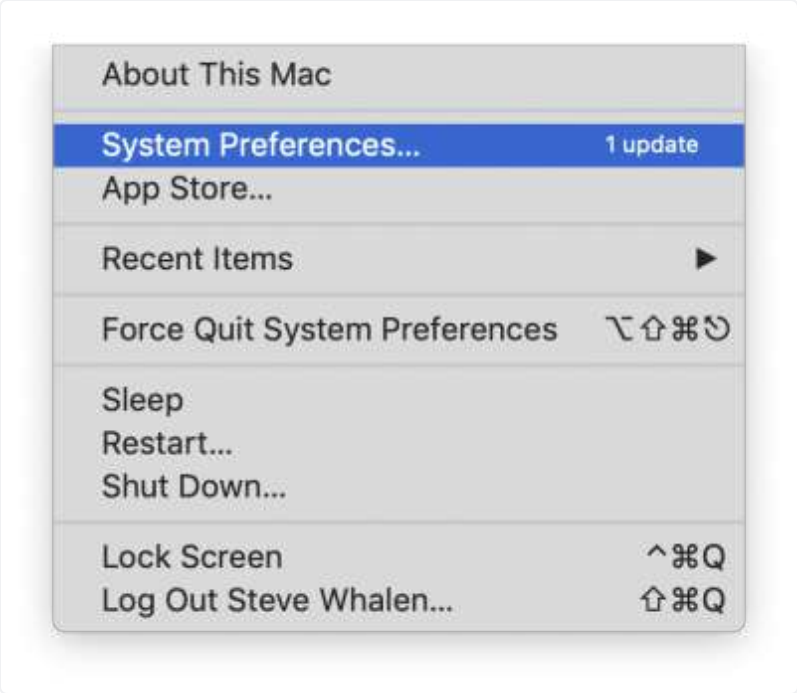
7.5 Granting Privileges

Before launching RECON LAB for the first time, RECON LAB will need to be given Full Disk Access. This allows RECON LAB to gain access to areas and files restricted by standard permissions.

7.5.1 Full Disk Access

The following describes how to change the Full Disk Access permissions according to the version of macOS your examiner machine is running.

7.5.1.1 macOS 12 and Below



To give RECON LAB Full Disk Access on macOS 12 and below, navigate to **System Preferences** using the **Apple Menu** found in the top left corner (Apple Menu – System Preferences).

From **System Preferences** select the **Security & Privacy** icon.

Follow the steps below to add RECON LAB to the **Full Disk Access** column.

1.) Click on the lock icon in the bottom left corner and enter the admin password to unlock.

2.) Select the **Privacy** tab and then **Full Disk Access** in the sidebar.

3.) Click the **“+”** symbol and navigate to the RECON LAB application.

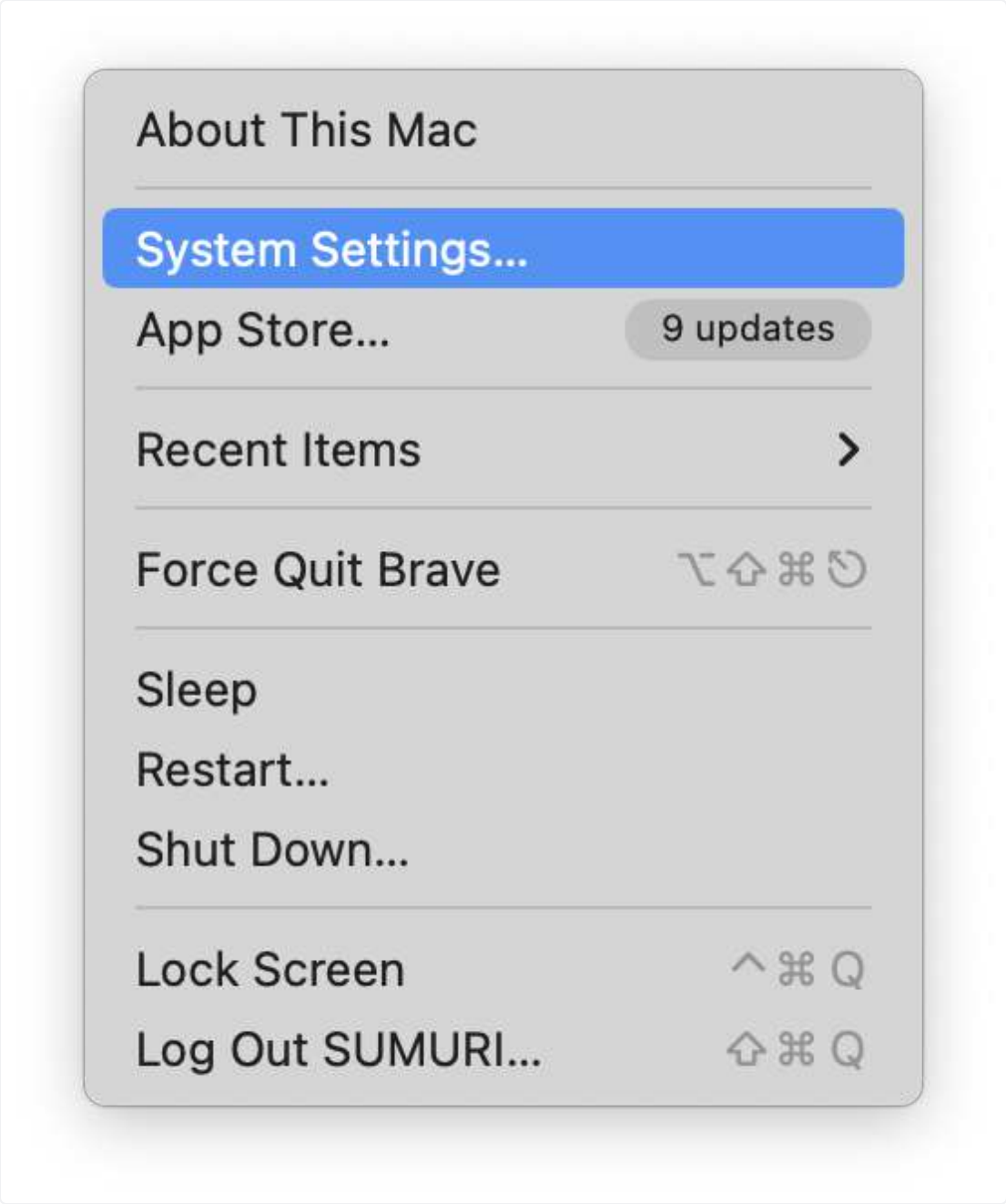
4.) Select the **RECON LAB** application to give Full Disk Access permissions.

7.5.1.2 macOS 13 and above

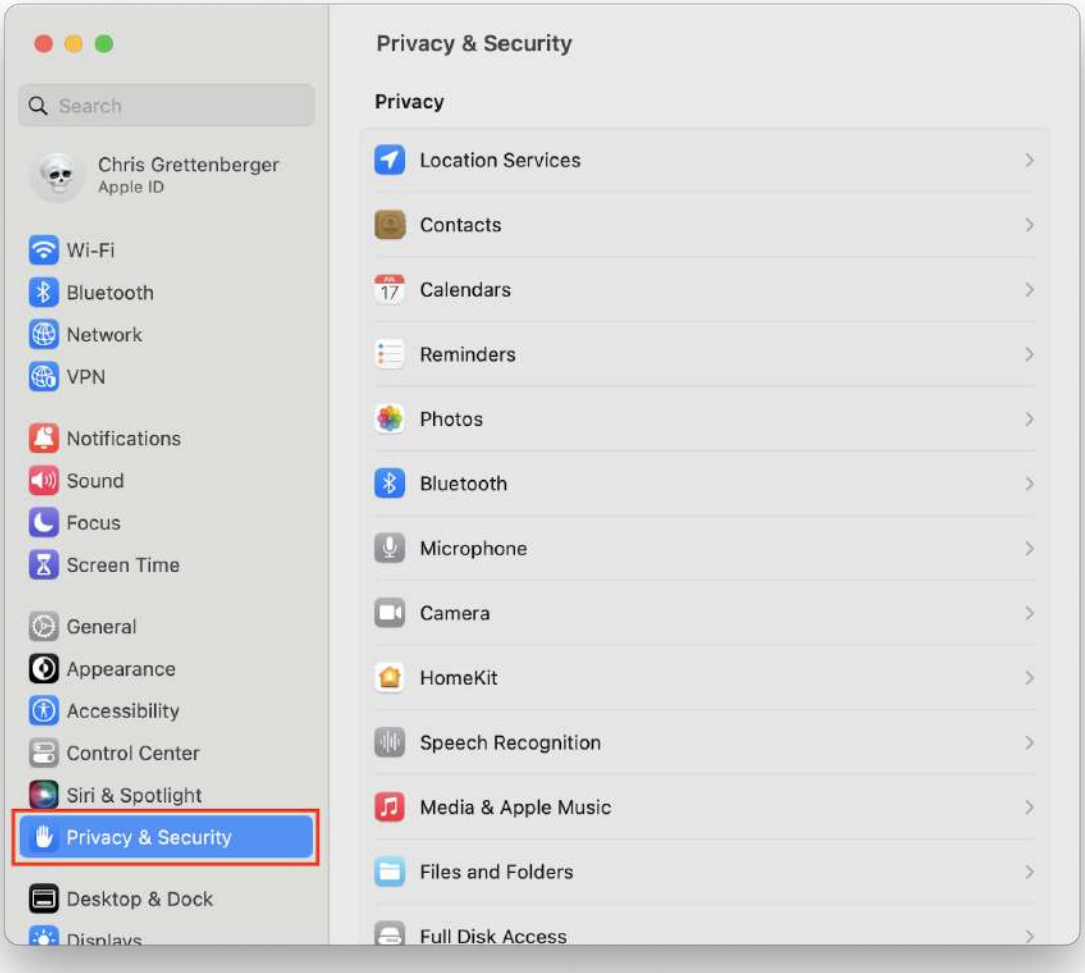
Alongside the release of macOS 13, Apple introduced a change to the tried and true System Preferences to make it more akin to iOS. System Preferences has now been changed to System

Settings and includes a new interface.

To give RECON LAB Full Disk Access on macOS 12 and below, navigate to **System Settings** using the **Apple Menu** found in the top left corner (Apple Menu – System Settings).



From **System Settings** select the **Security & Privacy** icon.



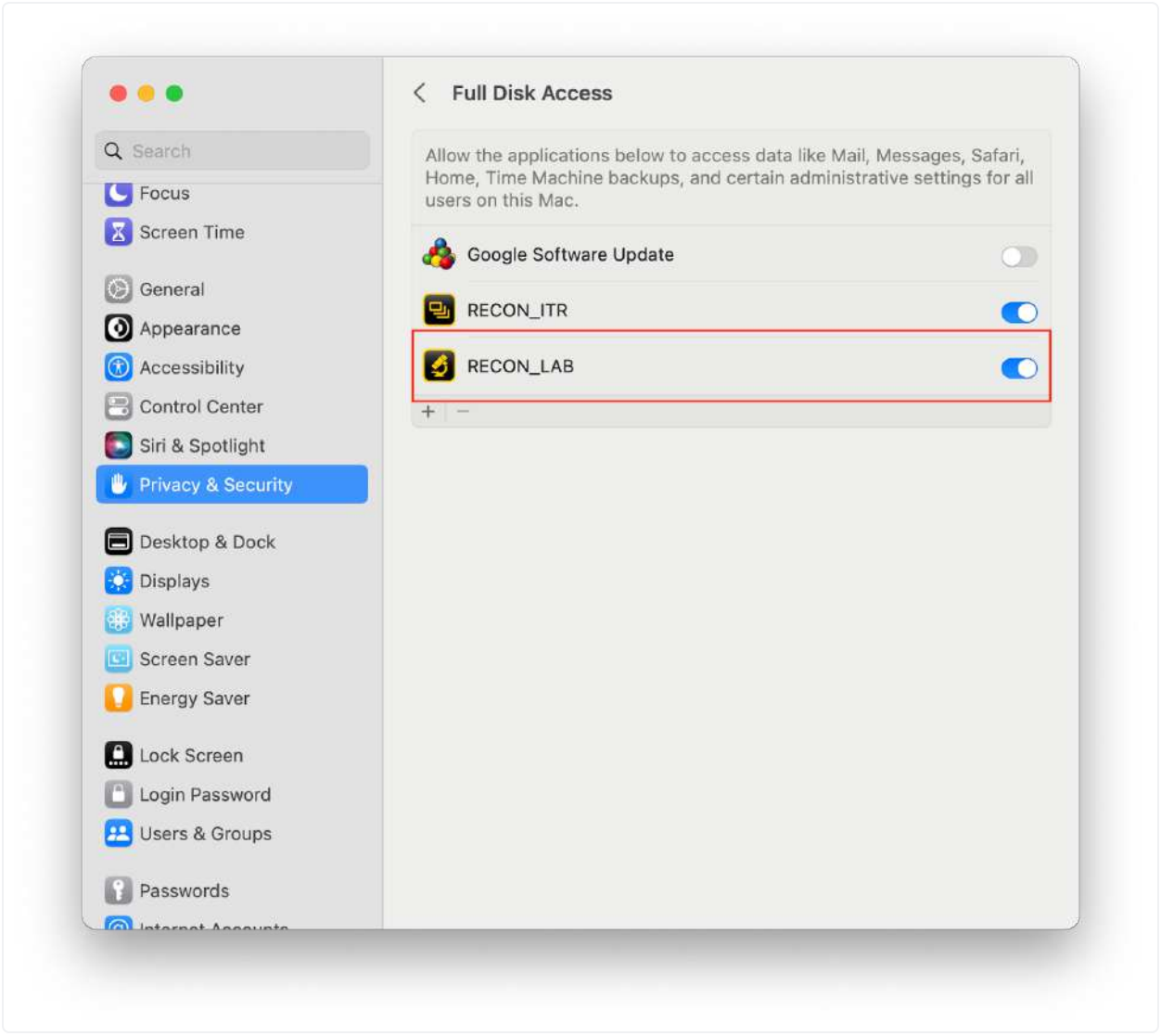
1.) Navigate to **Full Disk Access**

2.) Scroll to the bottom of the window to locate the **"+"** symbol.

3.) Click the **“+”** symbol and enter the **administrator password**.

4.) Navigate to the **RECON LAB** application.

5.) Select the **RECON LAB** application and enable the switch to give Full Disk Access permissions.

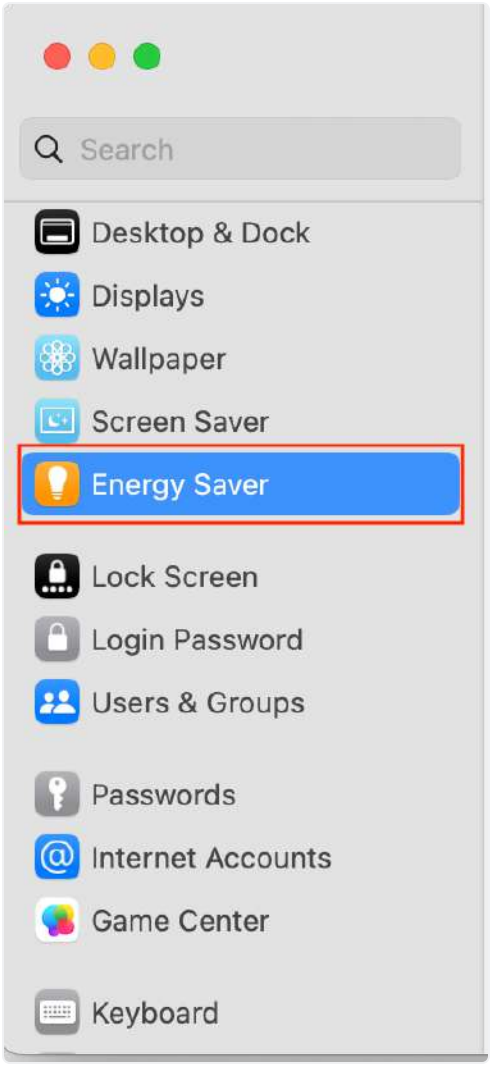


7.6 Energy and Sleep Settings

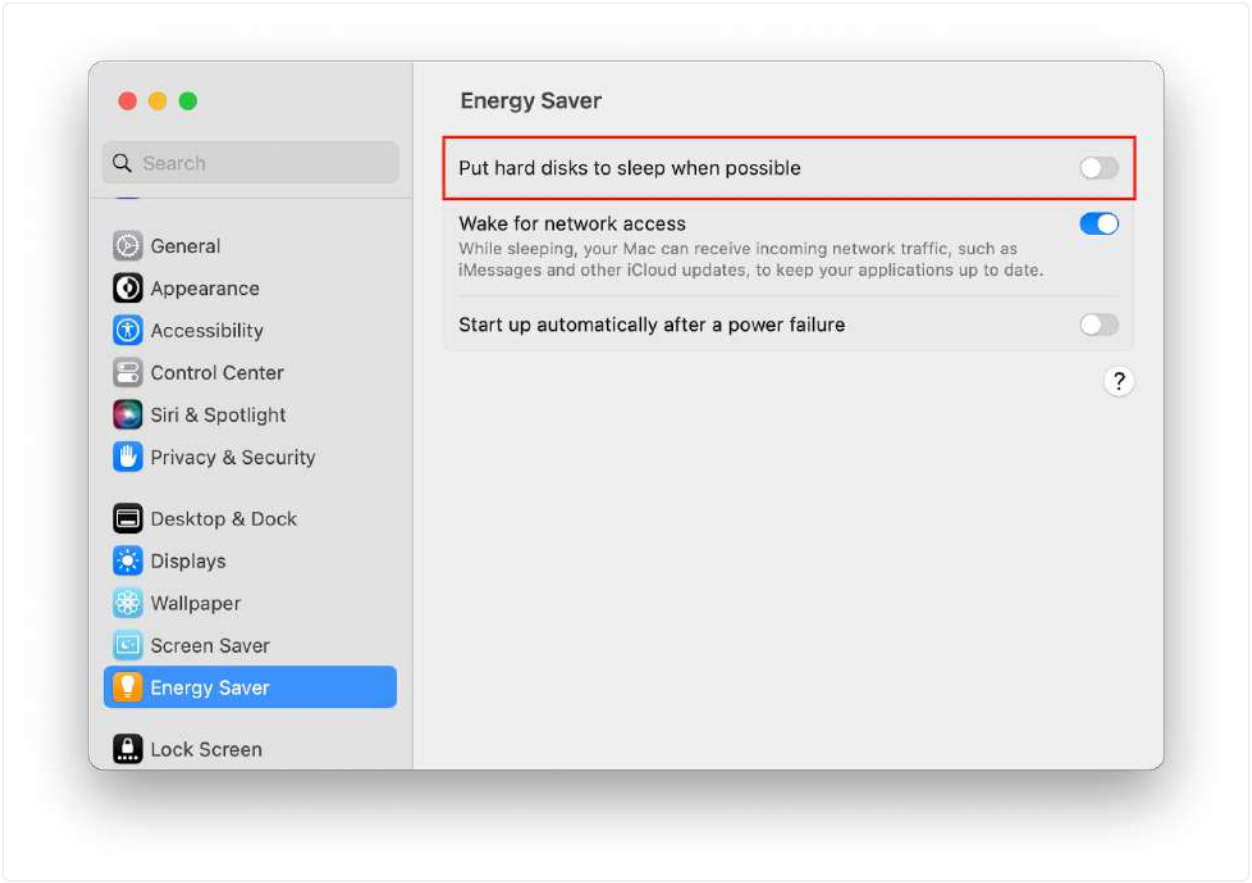
Allowing your Mac to go to sleep in the middle of processing a case will most likely cause issues. Make sure that you disable any settings which “Put hard disks to sleep when possible” or that allows the computer to sleep when working with RECON LAB.

These settings can be changed in System Preferences (Apple Menu – System Preferences) in macOS 12 or in System Settings (Apple Menu – System Settings) in macOS 13.

7.6.1 macOS 13 (Ventura) and below

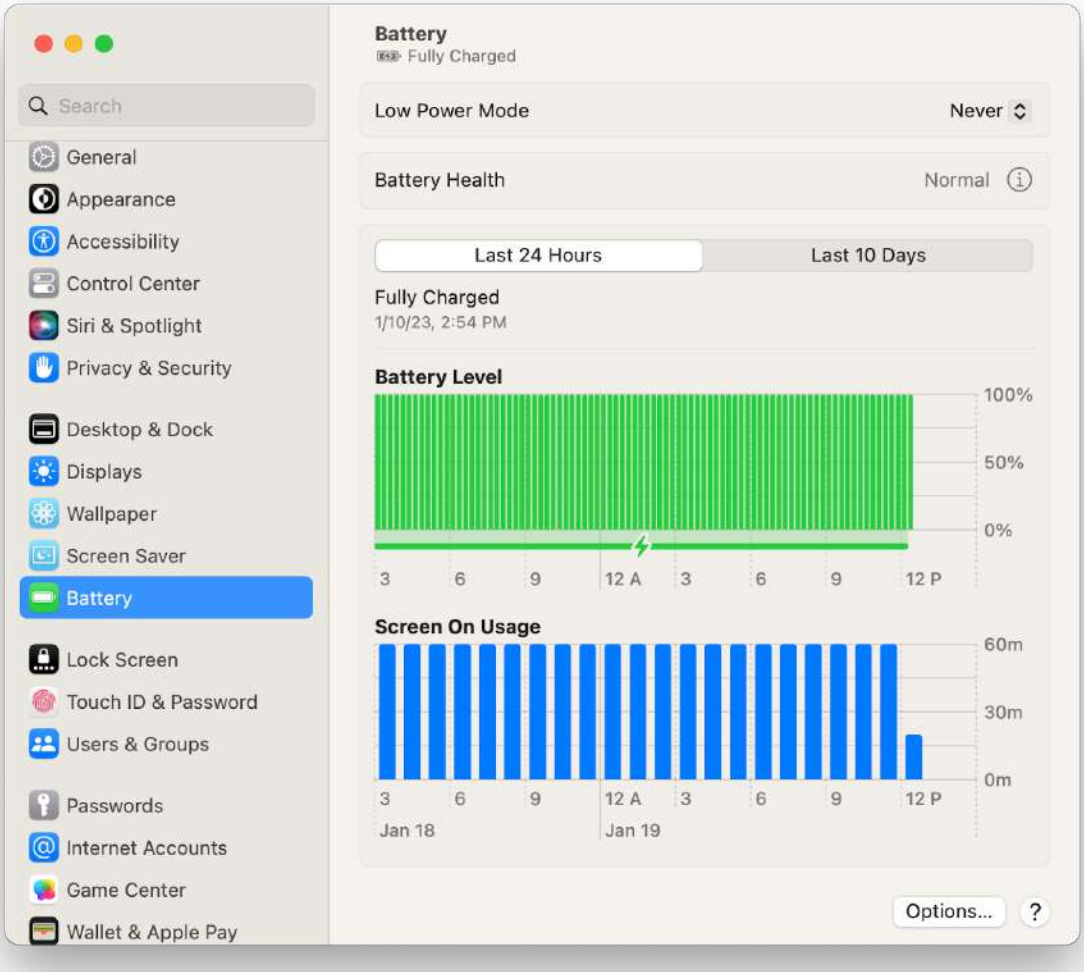


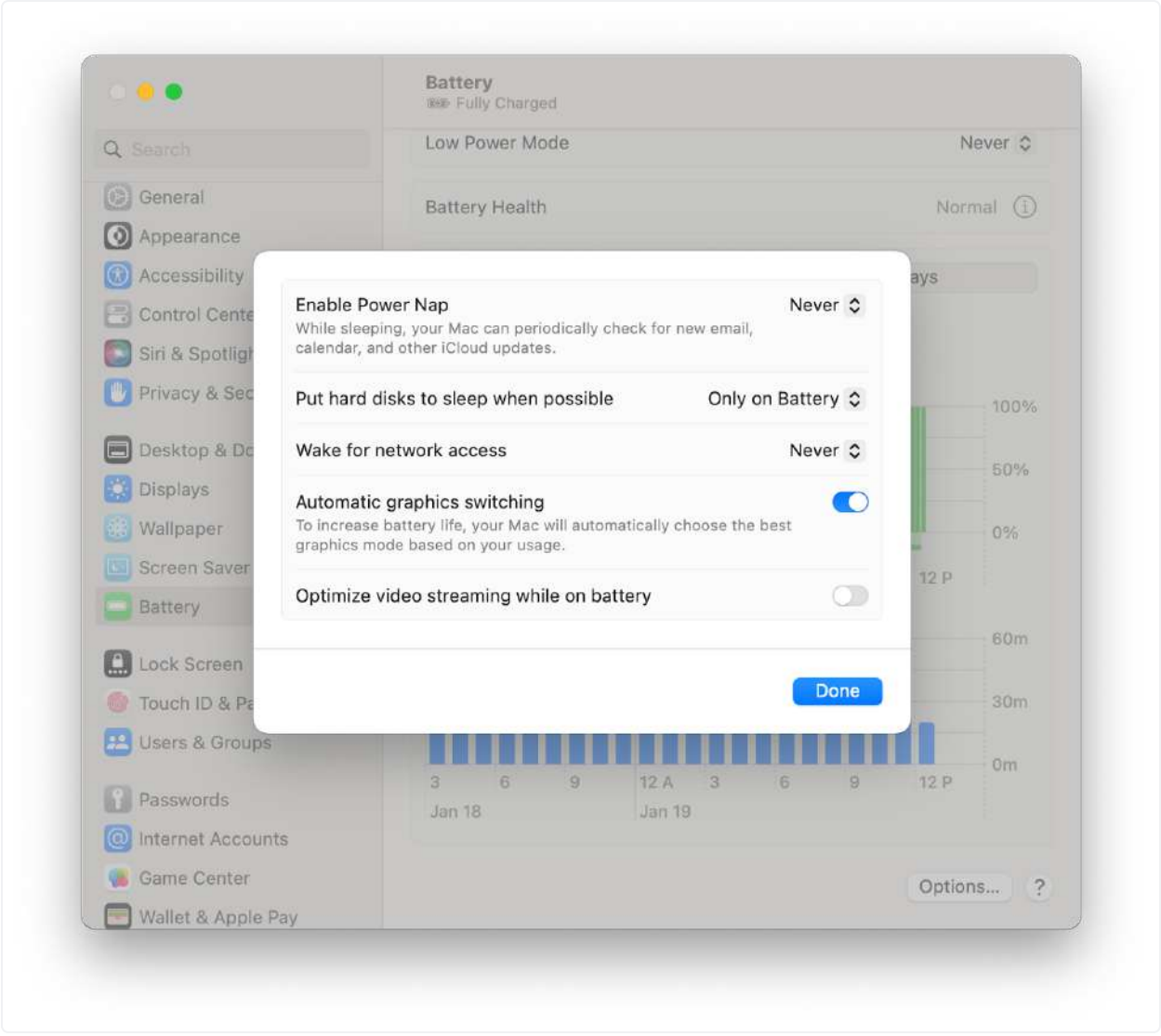
Look for the **Energy Saver** icon.



Set the “Put hard disks to sleep when possible” setting to “Never.” This should ensure that RECON LAB’s processes will run uninterrupted.

On M1, M2, M3, and M4 laptops (such as the MacBook Pro) this setting may appear as “Battery” instead.

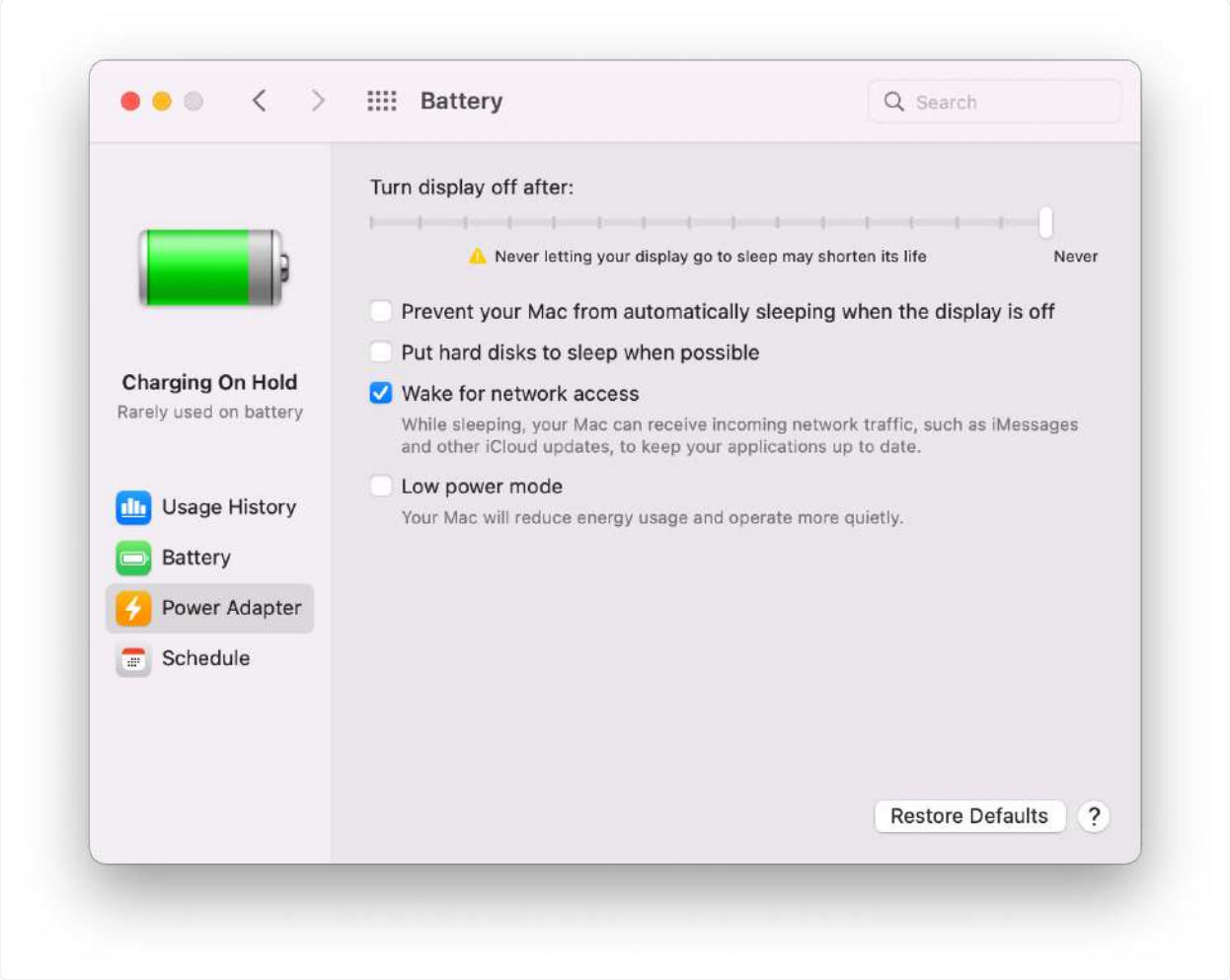

Search
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Security
Desktop & Dock
Displays
Wallpaper
Screen Saver
Battery
Lock Screen
Touch ID & Password
Users & Groups
Passwords
Internet Accounts
Game Center
Wallet & Apple Pay
Battery
Fully Charged
Low Power Mode
Never
Battery Health
Normal
Last 24 Hours
Last 10 Days
Fully Charged
1/10/23, 2:54 PM
Battery Level
100%
50%
0%
3
6
9
12 A
3
6
9
12 P
Screen On Usage
60m
30m
0m
3
6
9
12 A
3
6
9
12 P
Jan 18
Jan 19
Options...
?



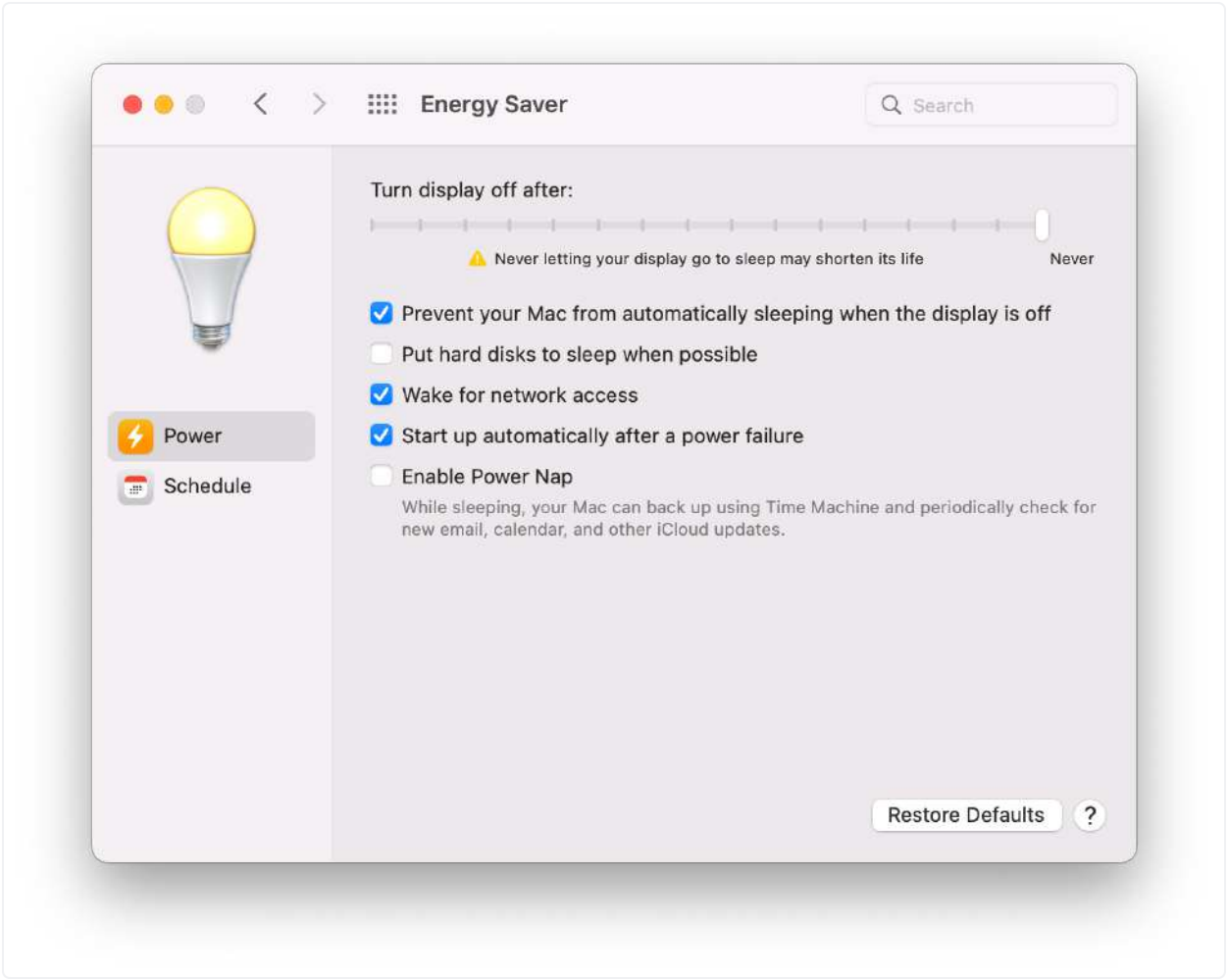
Once “Battery” is selected, set the “Put hard disks to sleep when possible” setting to “Never.”

7.6.2 macOS 12 (Monterey) and below

Look for the **Energy Saver** icon. Then check both of the settings for **Battery** and **Power Adapter**.



Under the **Battery** section, ensure the “Put hard disks to sleep when possible” and the “Enable Power Nap while on battery power” options are disabled in the **Power Adapter** tab. Additionally, be sure that the “Prevent computer from sleeping automatically when the display is off” option is enabled. Finally, make sure that “Turn Display off after:” is also set to “Never”.



Energy Saver will bring you to the window shown above when working with an Apple machine that does not rely on battery power.

Under the **Power** tab, ensure the “Put hard disks to sleep when possible” and the “Enable Power Nap while on battery power” options are disabled. Also, be sure that the “Prevent computer from sleeping automatically when the display is off” option is enabled and that “Turn Display off after:” is also set to “Never”.

After following these steps, RECON LAB should have all the permissions it needs run uninterrupted.

7.7 Updating RECON LAB

Before using RECON LAB, please make sure that you have the latest update.

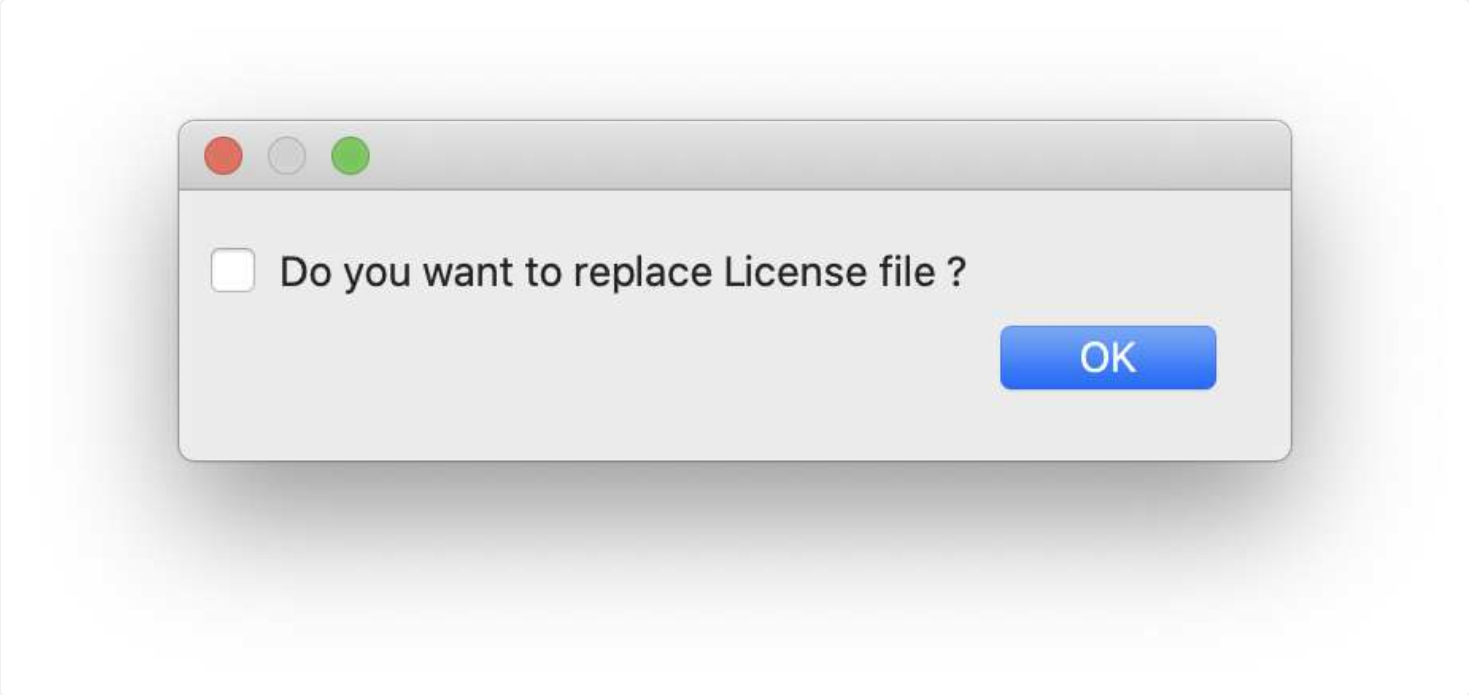
RECON LAB updates can be found here: https://goo.gl/wWm2qi

Download the latest version (highest-numbered) and move the .dmg to your Desktop.

Notifications for new updates will be sent out to the email address that we have on file. If you are not sure if you are on the RECON LAB update list and would like to be notified when updates are released please let us know at hello@sumuri.com.

Updating with a Renewed License

When updating RECON LAB, you have the option to point to a new license file. Click “Clean Install” in the Installer window, and you will see the option to replace your License file. Check the box and you can change your license file without losing configuration settings in RECON LAB.



Click “Install” in the Installer window, and you will see the option to replace your License file. Make sure it is unchecked, and RECON LAB will update without the need to point to the license file.

8. Starting RECON LAB

Once installed, RECON LAB can be found in your **Applications** directory.

For quick access, you can grab the RECON LAB icon and drag it to your dock to create a shortcut.

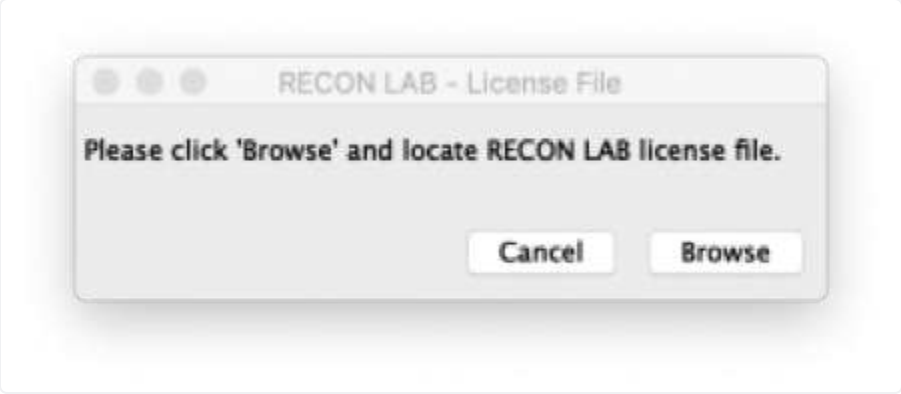
To start RECON LAB, double-click the icon in the Applications folder or single-click if you created a shortcut within the dock.

8.1 Adding Your License

When you run RECON LAB for the first time after installation you will be prompted to add your license.

Your license can be found on the RECON LAB USB which also acts as your security dongle. The RECON LAB USB will need to be attached to your Mac in order to run.

If a demo was requested or if RECON LAB was recently renewed the license will be sent by email. Please keep your license some place safe.



If you are prompted to add your license choose “Browse” and navigate to your license file.

Select your license file and choose “Open”.

RECON LAB will add your license and restart.

8.2 Installing Python

Python, which is a common scripting language used in forensics, is utilized for some features in RECON LAB and should be installed. Make sure that Xcode and its Command Line Tools have been previously installed.

Installing Python

1. Download and install Python version 3.9.6 for macOS from this link: https://www.python.org/downloads/

2. Open Finder then go to the Applications folder, find the Python application, on the left side of the Python app you will see a dropdown arrow, expand it and double click on "Install Certificates.command”.

3. After installing the certificates open your terminal and run the following command to install additional required libraries: python3 -m pip install lz4 enum34

4. Messages regarding updating “pip” can be ignored.

8.3 Admin Password

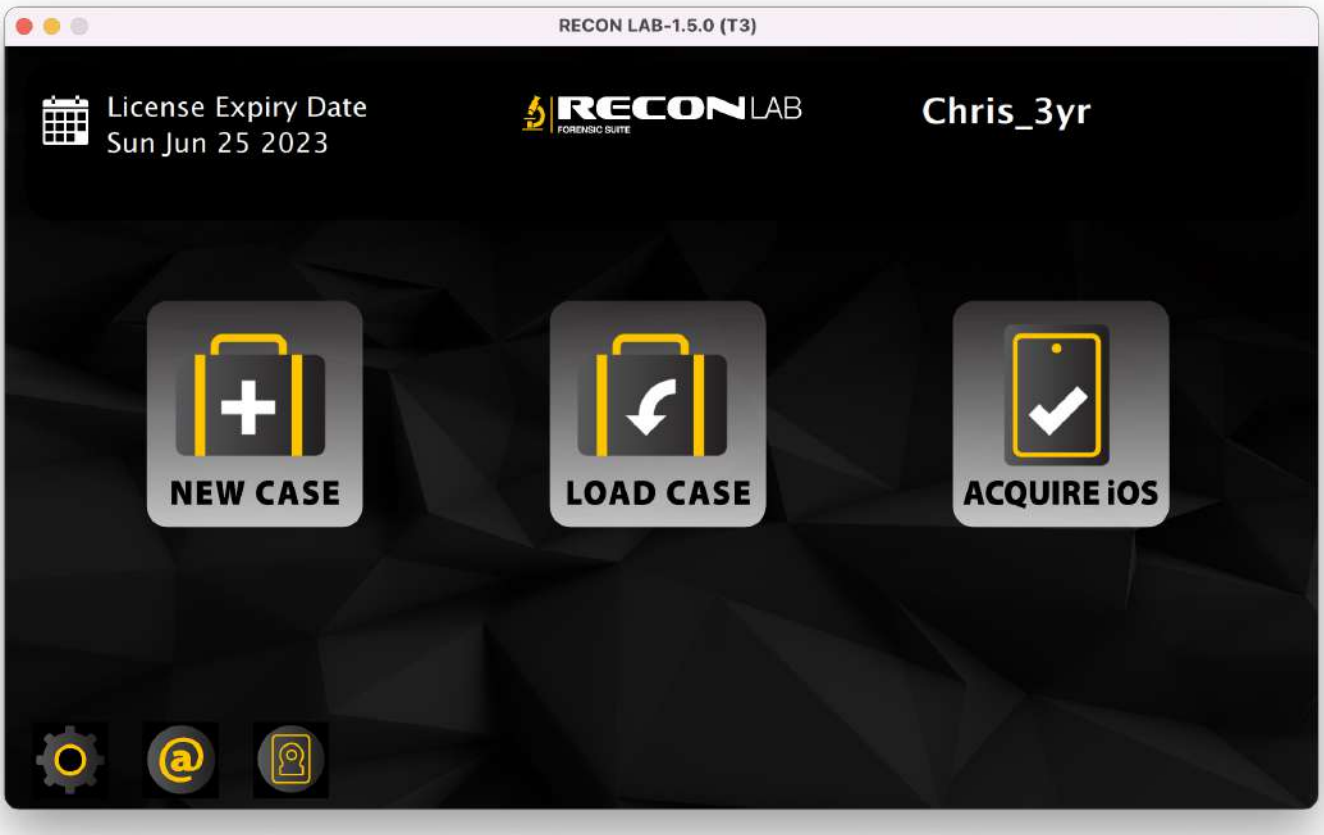
Upon the first run of RECON LAB you will be prompted to enter your admin password one time. Enter your admin password and click “OK”.

8.4 Access Warning Messages

When starting RECON LAB a message window will appear with some important information. This information may change so please review from time to time.

If you do not want the message to appear when you start RECON LAB select “Don’t show this message again”.

8.5 RECON LAB Welcome Screen



Upon starting RECON LAB you will be presented with the **Welcome Screen**.

The Version of RECON LAB will be found in the title bar.

In the bottom right corner, the Licensee, Purchase Date and Expiration Date are displayed for your reference.

The buttons along the bottom of the Welcome Screen are:

About RECON – Access to RECON LAB's EULA, change logs, exceptions and/or known issues, special requirements, support and updates information.

RECON Config – Allows the examiner to create persistent settings.

Acquire iOS Device – Opens the RECON LAB iOS Imager interface.

New Case – Starts the New Case Wizard.

Load Case – Allow an examiner to select a RECON LAB Case Folder.

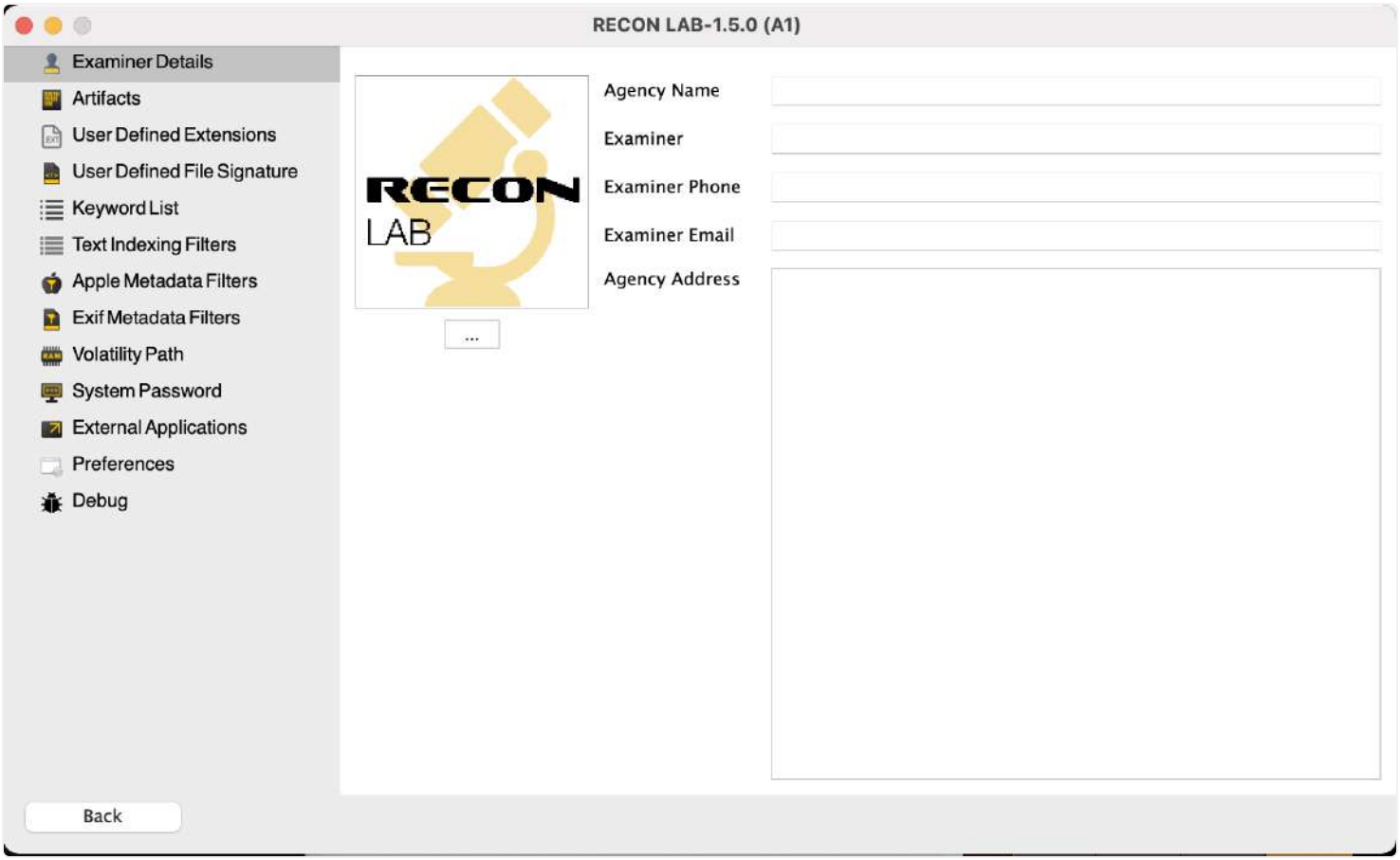
9. Configuration

Every examiner will have a unique approach to an examination.

RECON LAB allows an examiner to configure a variety of settings prior to starting a case. Configuration settings are persistent and will automatically be set for each new case.

This approach saves a lot of time. Configuration settings can be overridden at any time if required.

9.1 Examiner Details



The **Examiner Details** settings allow entry of the following information:

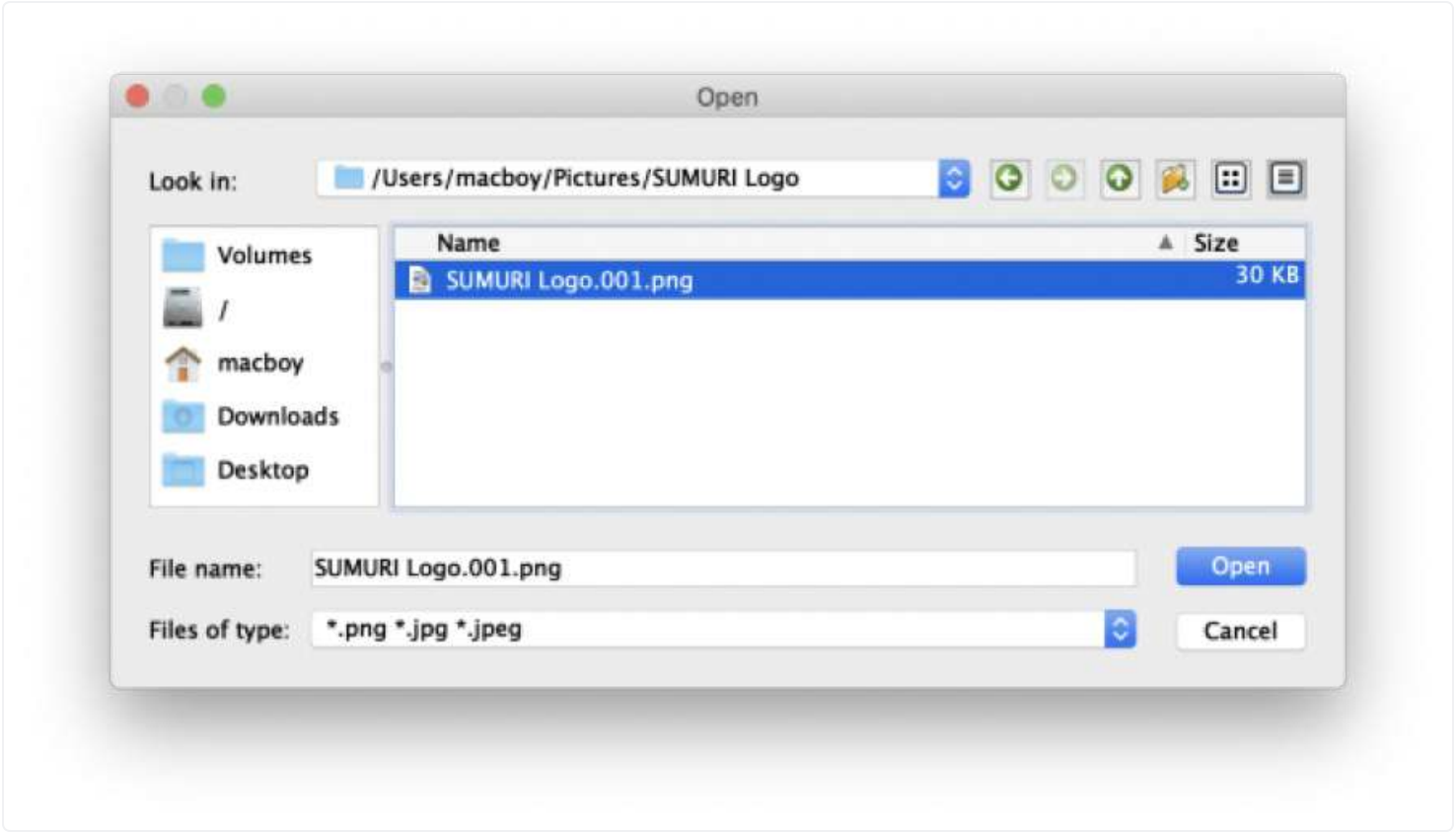
Agency Name – Name of the examination agency.

Examiner – Name of the examiner.

Examiner Phone – Phone number for the examiner.

Agency Address – Agency address.

The agency logo can be changed by selecting the three dots under the current logo.



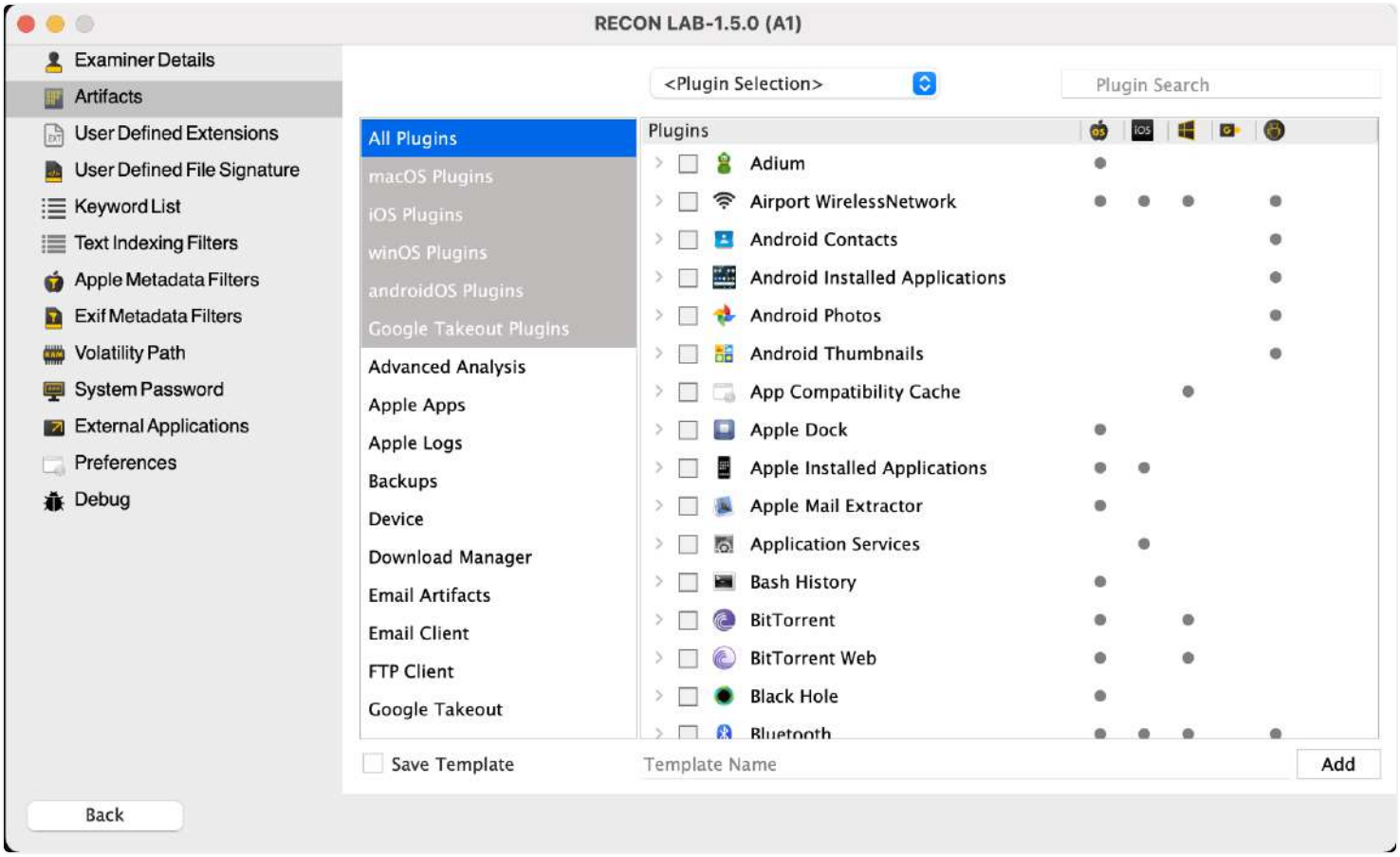
Any graphic can be selected for the agency logo. RECON LAB supports adding PNG or JPEG image formats.

All information entered in the Examiner Details will automatically be added to any reports generated by RECON LAB.

9.2 Artifacts and Plugins

RECON LAB includes hundreds of plugins that recover thousands of artifacts automatically from Windows, macOS, iOS, Android and Google Takeout.

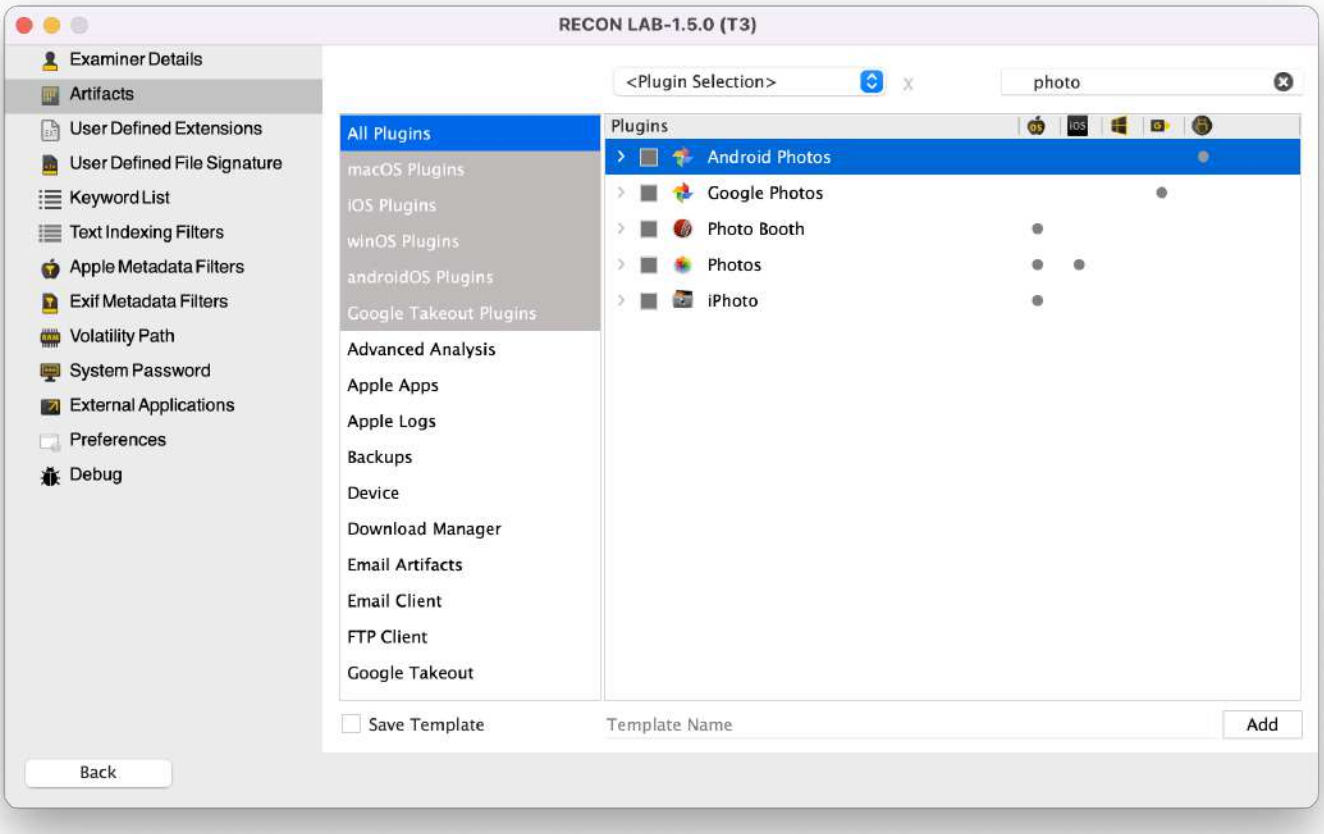
RECON LAB allows an examiner to enable plugins to run on every case and/or create templates for specific investigations.



Above is the interface for RECON LAB's Plugin and Artifact selection. Columns and dots were added to the interface to help you quickly see if a plugin is supported within a specific platform.

Each plugin can have multiple artifacts. Activating a checkbox will enable the plugin.

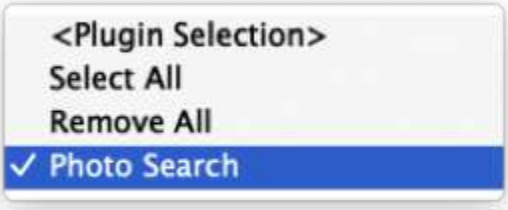
On the left side, there are filters at the top for "All Plugins" and specific operating systems (i.e. "winOS") and platforms (i.e. "Google Takeout"). Selecting any filter on the left-side removes all plugins from the Plugin Window on the right-side except for what is relevant to the operating system or platform selected. For example, if you select the "iOS Plugins" filter on the left you will only see plugins relating to iOS on the right.



Similarly, there is a Plugin Search box in the upper right corner that can be used to quickly filter all plugins. In the example above, the keyword “photo” was used to show all plugins that contained the word “photo” (i.e. Android Photos, Photo Booth).

At the bottom of the window, there is a “Save Template” button. Checking this box and providing a name will make a permanent template that can be used again.

Saving a Template for Plugins and Artifacts

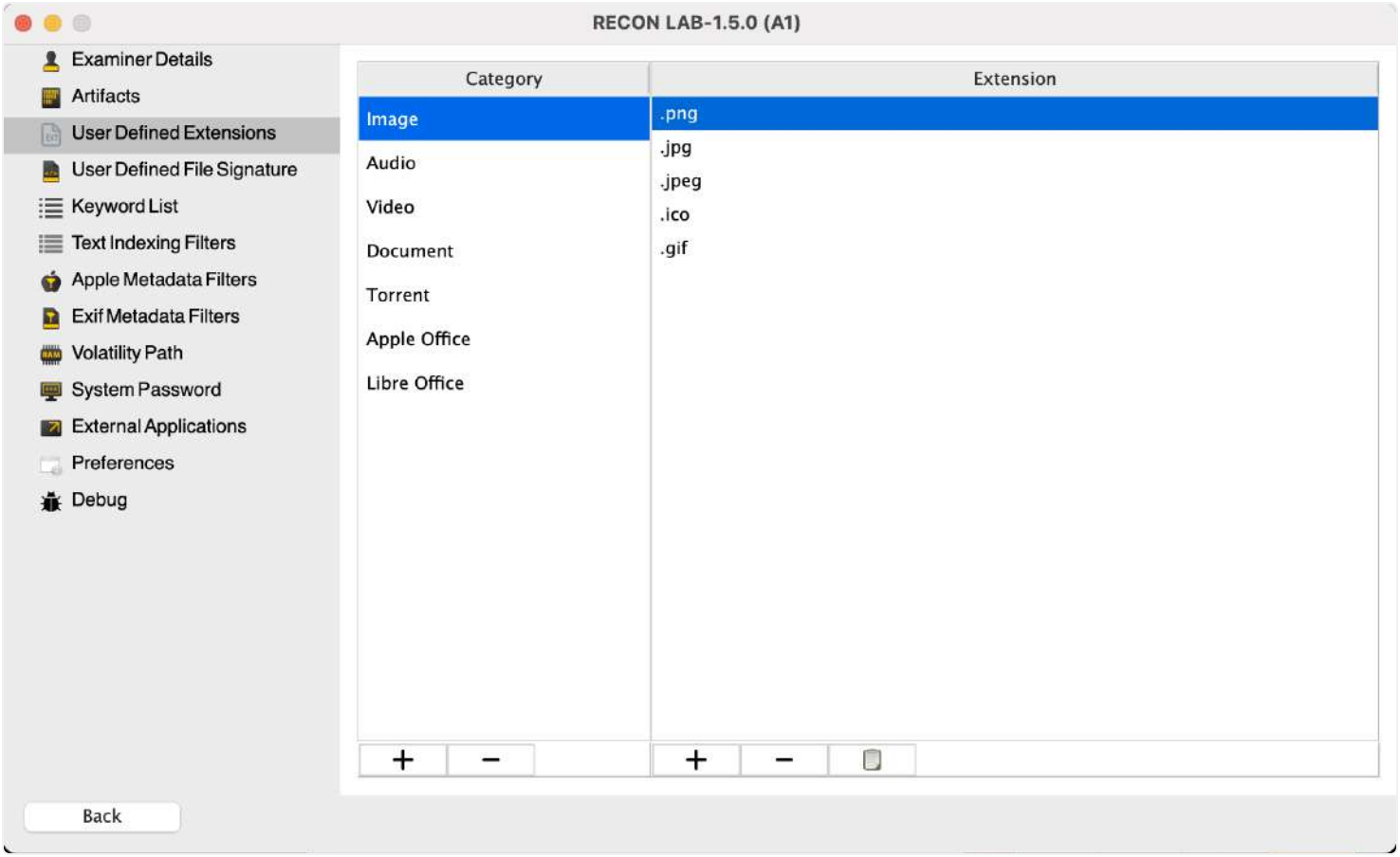


1. Using the example above, the Plugin Search was used to find all plugins with the word “photo”.
2. Each of these plugins was selected using the checkboxes.
3. The “Save Template” box was checked and the name “Photo Search” was given to the template.
4. To save the new template the “Add” button was clicked.
5. The new template can now be selected and applied in the dropdown box at the top of the window.

Remember, settings can always be changed at any time within the case.

9.3 User Defined Extensions

User Defined Extension settings allow the examiner to create “buckets” (categories) for various file extensions. These categories will appear in the RECON LAB Sidebar. Any files with a matching file extension included in a Category will automatically be filtered and appear in the “bucket” in RECON LAB’s Sidebar.



In the example above, the category Image contains the file extensions .png, .jpg, .jpeg, .ico and .gif. When a new case is started, any files matching these extensions will automatically be found in the Sidebar in a “bucket” named “Image”.

Adding or Removing Categories and Extensions

To create a new Category or to add an Extension simply click the “+” button. Enter the text and hit return.

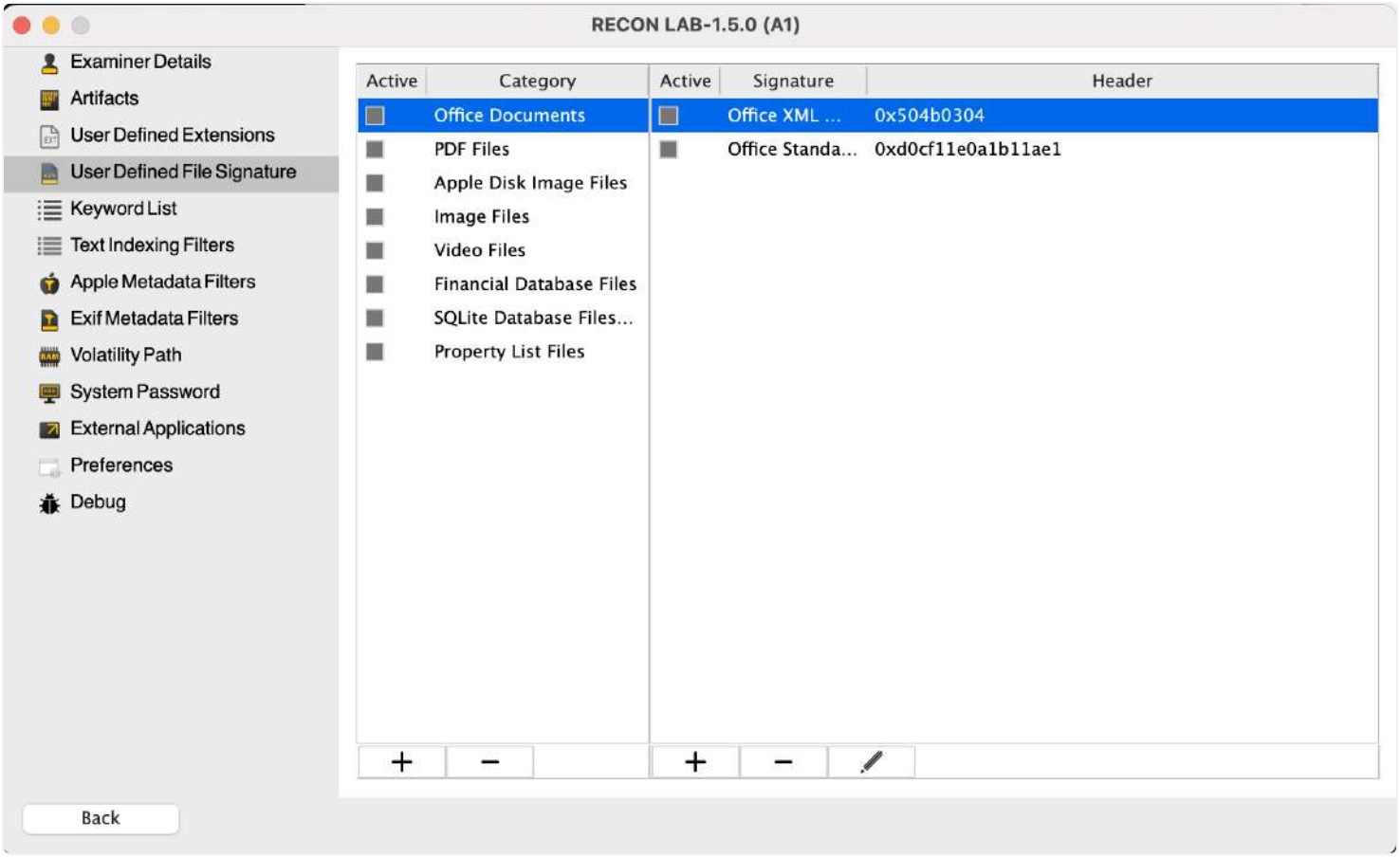
To remove a Category or Extension select the item and click the “-” button.

To add multiple extensions at the same time use the “paste” or clipboard button. Make sure that your text is entered as on item per line with a single carriage return. Copy all the text to your Clipboard and then use the “paste” (clipboard) button to add multiple items at the same time.

9.4 User Defined File Signatures

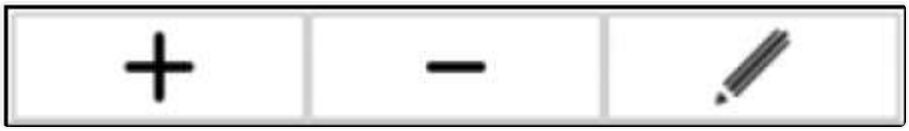
User Defined File Signature settings allow the examiner to create “buckets” (categories) using a file’s signature. File signatures help identify files in the absence of extensions or if the file extension is incorrect.

The categories created will appear in the RECON LAB Sidebar. Any files with a matching a file’s signature included in a Category will automatically be filtered and appear in the “bucket” in RECON LAB’s sidebar



In the example above, the category “Financial Database Files” contains the file signatures for Quicken backup and database files. When a new case is started, any files matching these signatures will automatically be found in the Sidebar in a “bucket” named “Financial Database Files”.

Adding or Removing File Signatures



To create a new Category or to add a new File Signature simply click the “+” button.

1. Use the “Label” field to provide a name.

2. Add the signature as HEX or ASCII and select the appropriate button.

3. If the file signature begins at a specific offset add the value in the “Offset” field.

4. Click “Add”.

To remove a Category or File Signature select the time and then click the “-” button.

Editing a File Signature

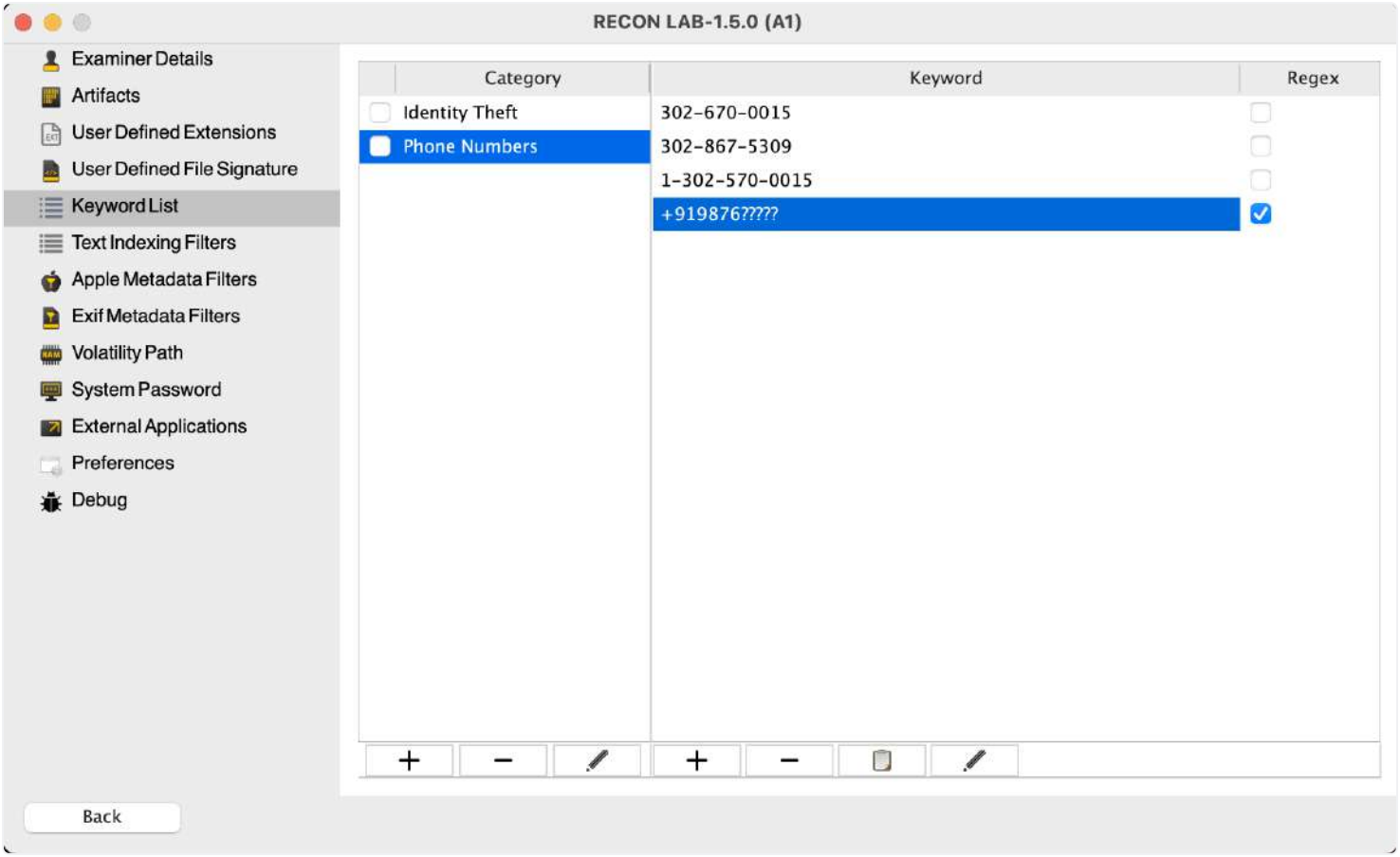
To edit a previously stored File Signature click the “Edit” (pencil icon) button. Make the required changes and click “Add” to save.

9.5 Keyword Lists

The Keyword List settings allow the examiner to create lists ahead of time for content-based searches. Various search options will be explained later in this manual.

Keywords can be grouped into categories. Content keywords can be plain text or regular expressions (REGEX) that conform to dtSearch rules.

dtSearch’s Quick Reference Guide can be found here: http://support.dtsearch.com/Support/forms/iframes_advanced/default.html



In the example above a category was created for “Phone Numbers”. Four phone numbers were entered as keywords. The first three are standard text. The last one (“+919876?????”) is an example of a regular expression to find an Indian phone number where we know the first six numbers but we do not know the last five. We checked the “Regex” checkbox to let RECON LAB know that the text entered should be treated as a regular expression.

Adding or Removing Categories or Keywords

To create a new Category or Keyword simply click the “+” button. Enter the text and hit return.

If the Keyword is to be treated as a regular expression click the “Regex” box.

To remove a Category or Keyword select the entry and click the “-” button.

To add multiple keywords at the same time use the “paste” or clipboard button. Make sure that your text is entered as on item per line with a single carriage return. Copy all the text to your Clipboard and then use the “paste” (clipboard) button to add multiple items at the same time.

Editing a Keyword

To edit a previously entered keyword click the “Edit” (pencil icon) button. Make the required changes and click “Add” to save.

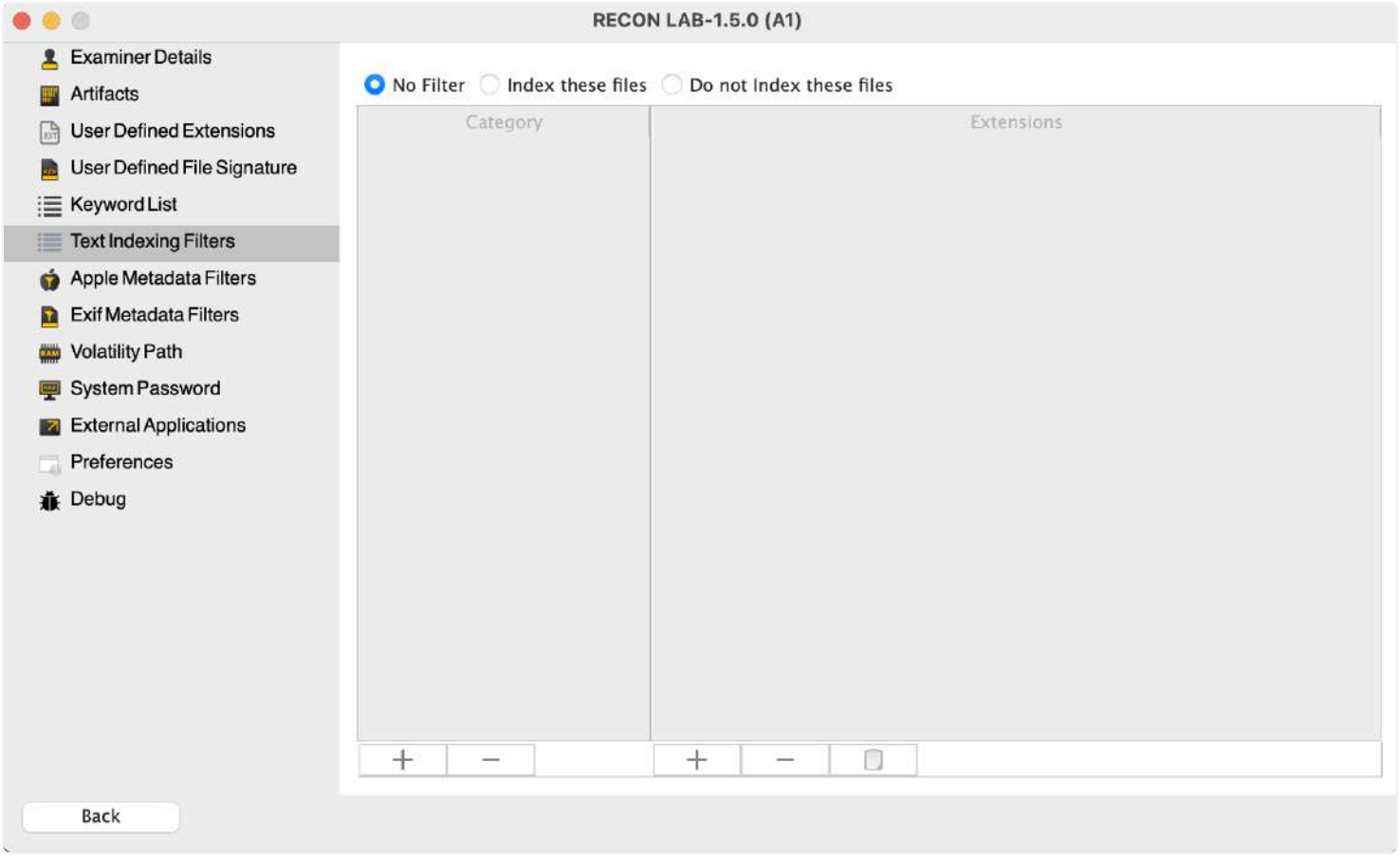
9.6 Text Indexing Filters

RECON LAB has included features to speed up your examination.

Text Indexing Filter settings allow you to set files to index or not index during a case ahead of time.

Default Index – No Filter

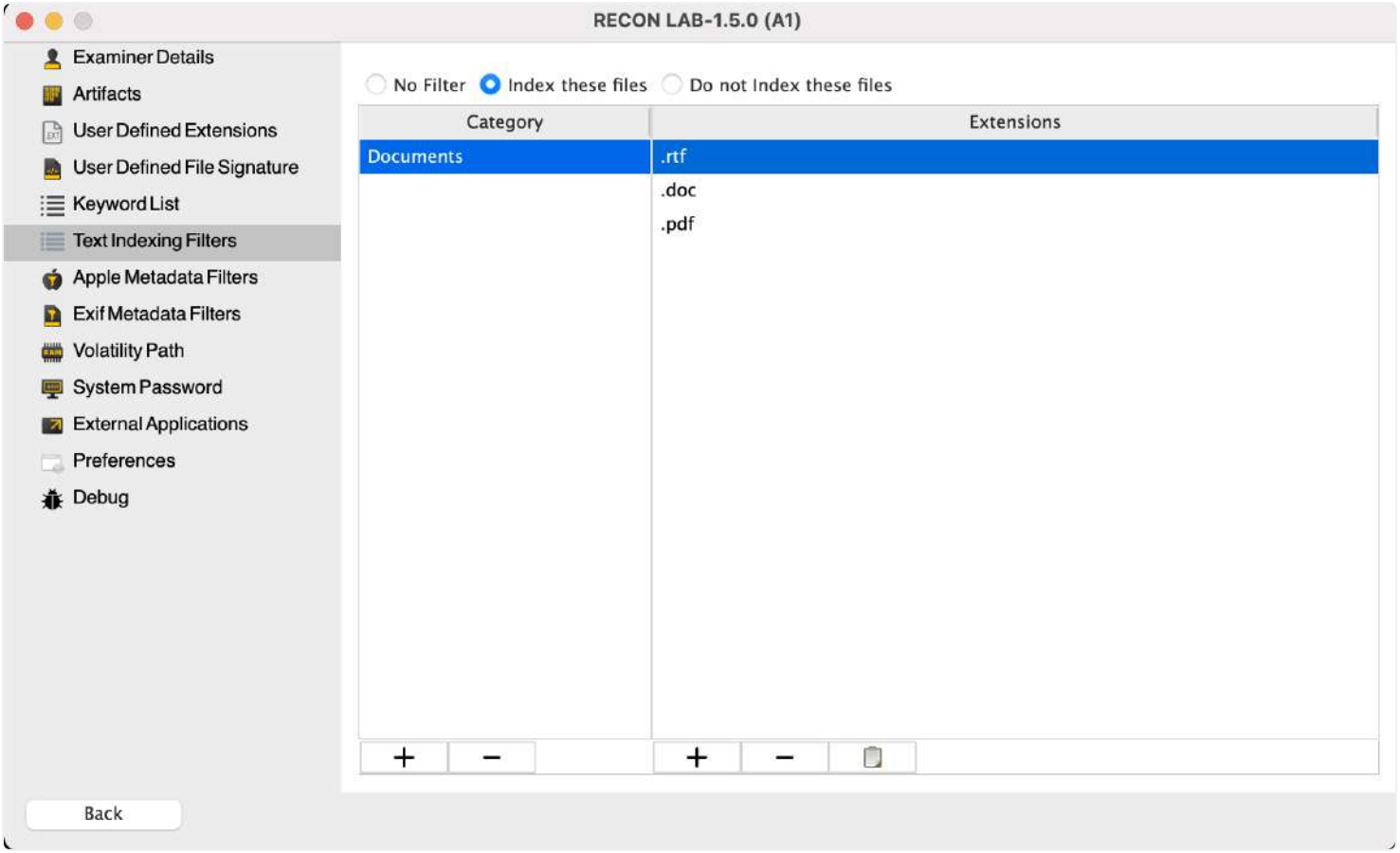
The default setting for indexing is “No Filter”. Leave this setting if you want to index all files.



Indexing Specific Files Only

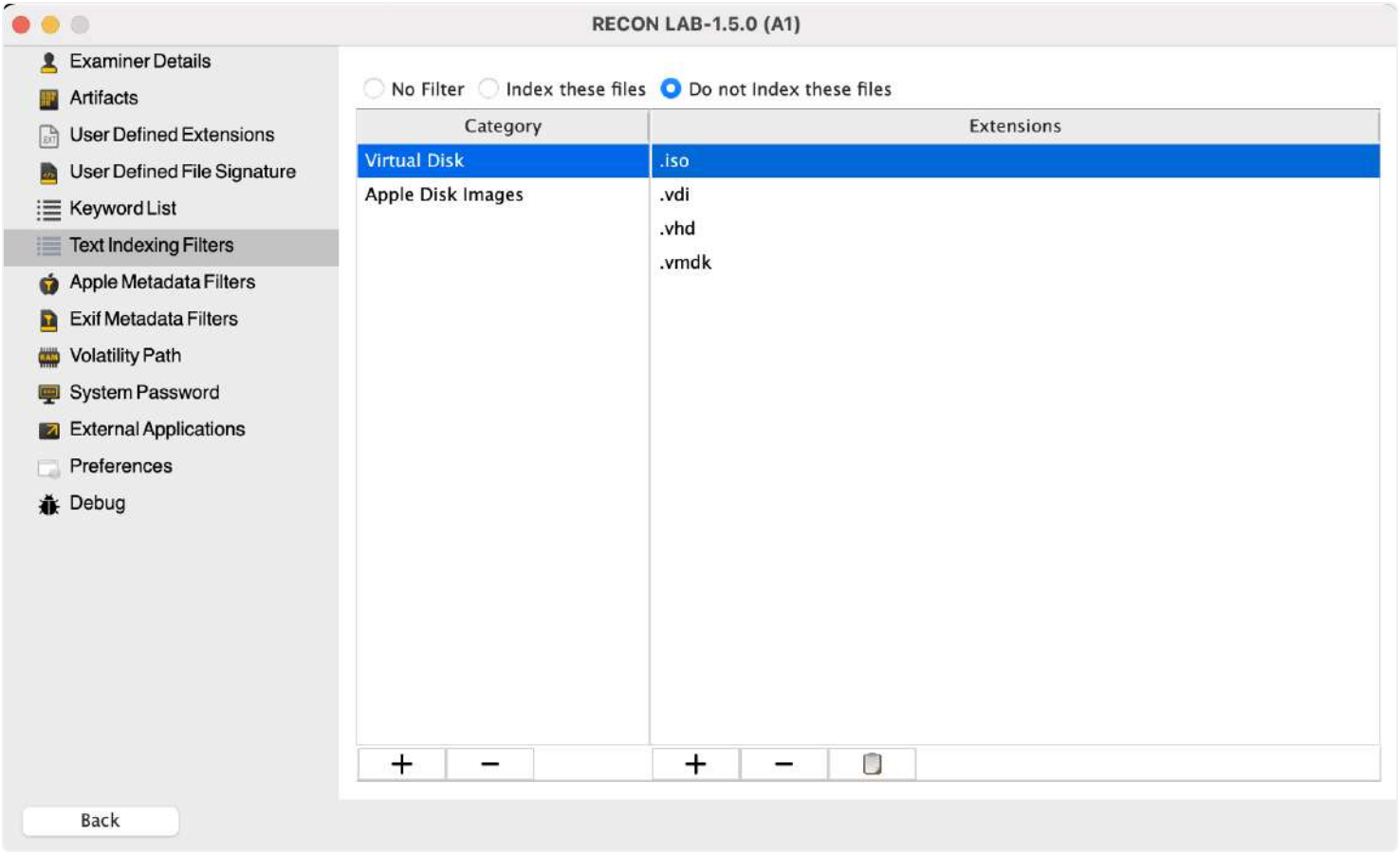
To speed up processing you can have RECON LAB index only certain file types (based on extension) by selecting “Index these files”.

In the example below, a category was created for “Documents”. In the “Documents” category three file types were added (.rtf, .doc, .pdf). With these settings, RECON LAB will only index RTF, Word Document and PDF files and ignore all other file types.



Eliminating Files From Indexing

Also, to speed up processing, RECON LAB can ignore indexing specific file types (based on extension) by selecting “Do not index these files”.



In the example above, a category for “Virtual Disk” was created. Within the category the extensions of .iso, .vdi, .vhd, and .vmdk were added. This category will reduce our processing time dramatically as RECON LAB will index all files except for those added to the lists below.

Adding or Removing Categories and Extensions

To create a new Category or to add an Extension simply click the “+” button. Enter the text and hit return.

To remove a Category or Extension select the item and click the “-” button.

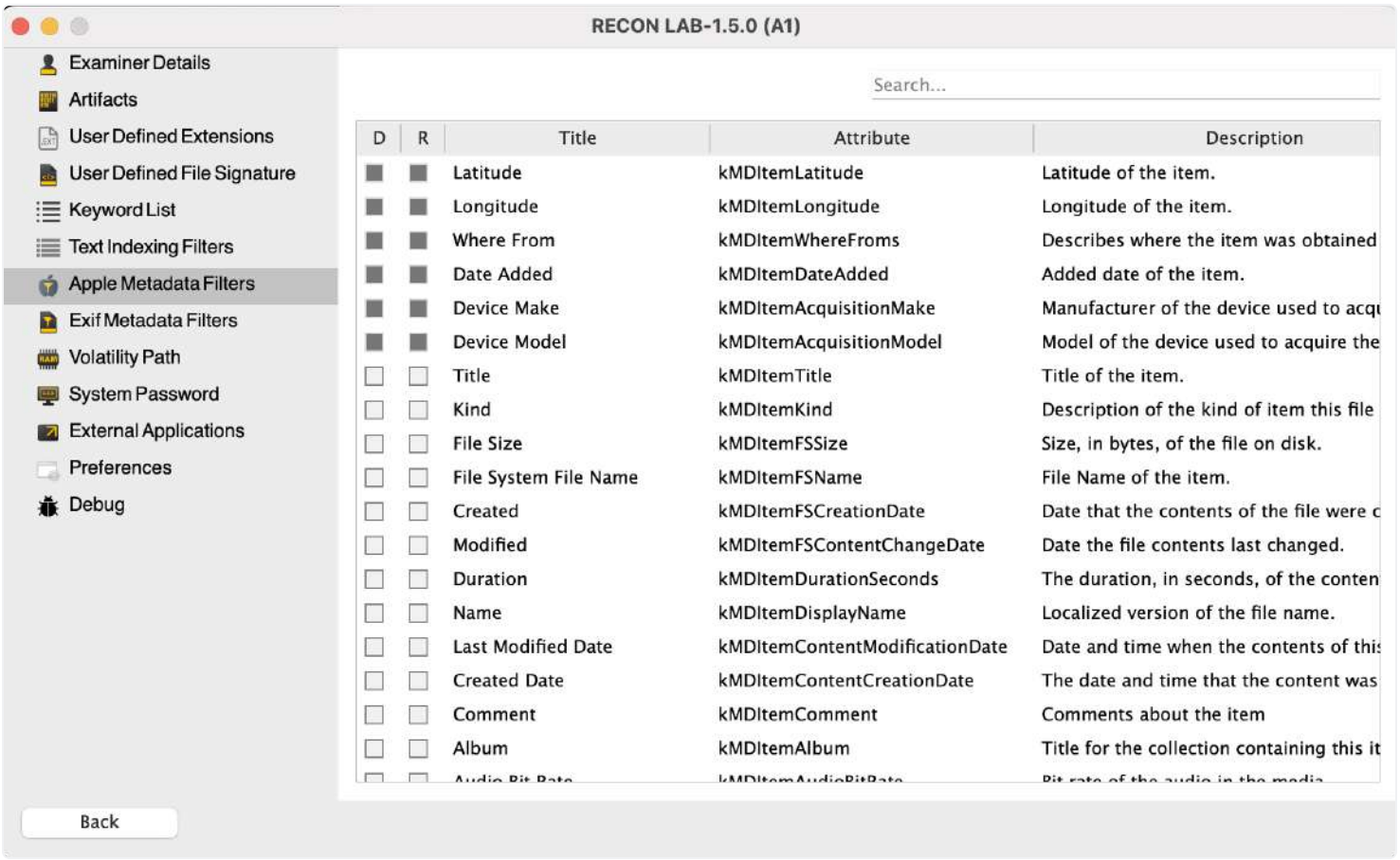
To add multiple extensions at the same time use the “paste” or clipboard button. Make sure that your text is entered as on item per line with a single carriage return. Copy all the text to your Clipboard and then use the “paste” (clipboard) button to add multiple items at the same time.

9.7 Apple Metadata Filters

RECON LAB is the only forensic suite that is developed on a Mac to utilize macOS libraries natively. This allows RECON LAB to see and fully utilize Apple Extended Metadata. Other solutions do not natively support Apple Extended Metadata and rely on third-party and reversed engineered solutions that may not see or support all the metadata that exists which can lead to missed evidence.

Within the main RECON LAB interface, all Apple Extended Metadata is visible.

For the Apple Metadata Filter settings, we have selected some of the most common and important Apple Extended Metadata attributes which can be set to always show in the RECON LAB sidebar or within reports.



Apple Metadata Filter Column Descriptions

D – Check this box to add this Apple Extended Attribute to the RECON LAB Sidebar. Any files matching selected attributes will automatically be filtered and placed in the Sidebar.

R – Checking this box will include the selected attribute's metadata automatically to reports.

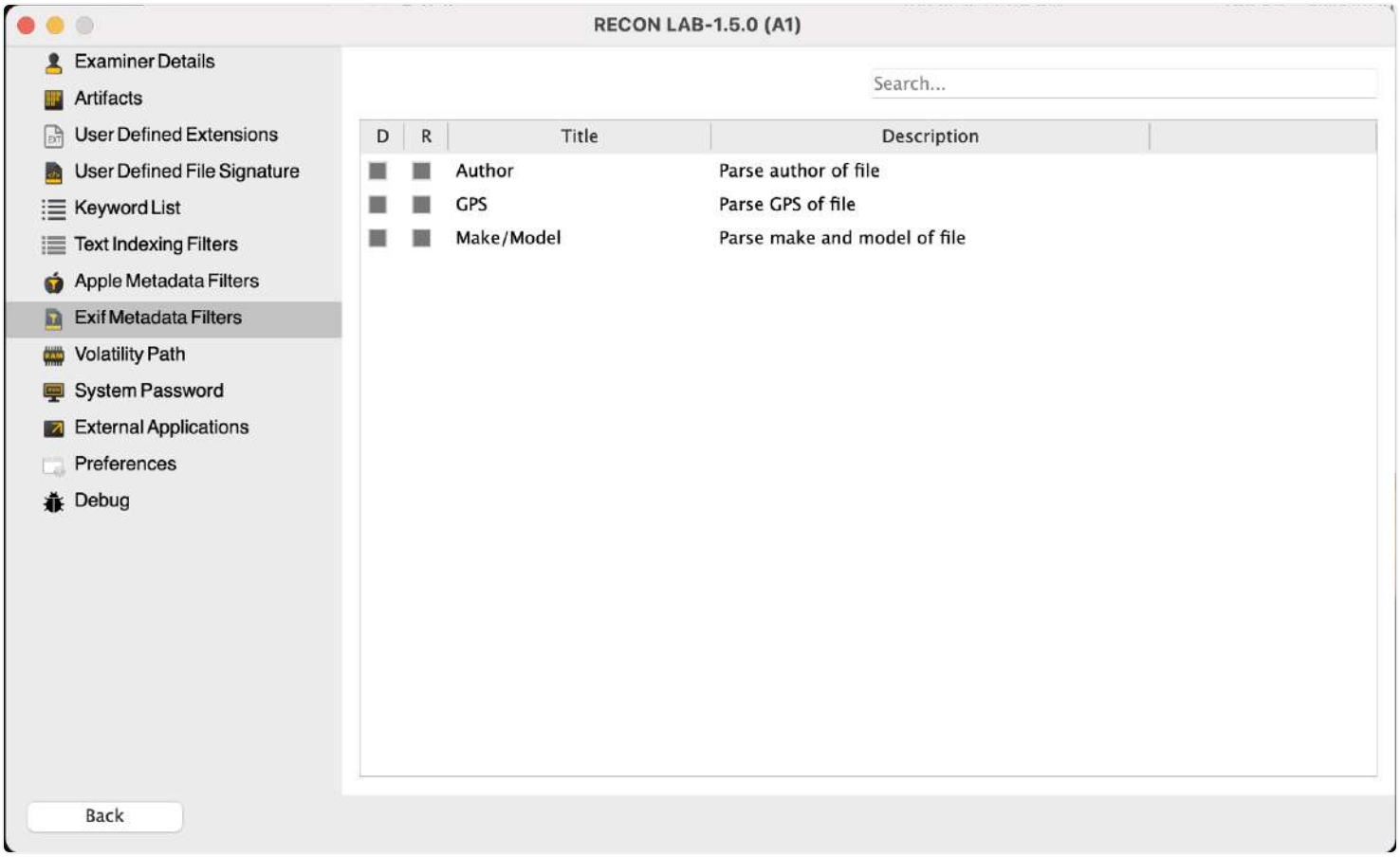
Title – The common name of the Apple Extended Attribute.

Attribute – The specific name of the Apple Extended Attribute.

Description – The official description of the Apple Extended Attribute.

9.8 EXIF Metadata Filters

RECON LAB also parses EXIF metadata. The EXIF Metadata Filters allows an examiner to automatically filter out files with specific EXIF attributes to the RECON LAB Sidebar and/or always include select attributes in reports.



EXIF Metadata Filter Column Descriptions

D – Check this box to add the EXIF Metadata to the RECON LAB Sidebar. Any files matching selected metadata will automatically be filtered and placed in the Sidebar.

R – Checking this box will include the selected EXIF metadata automatically to reports.

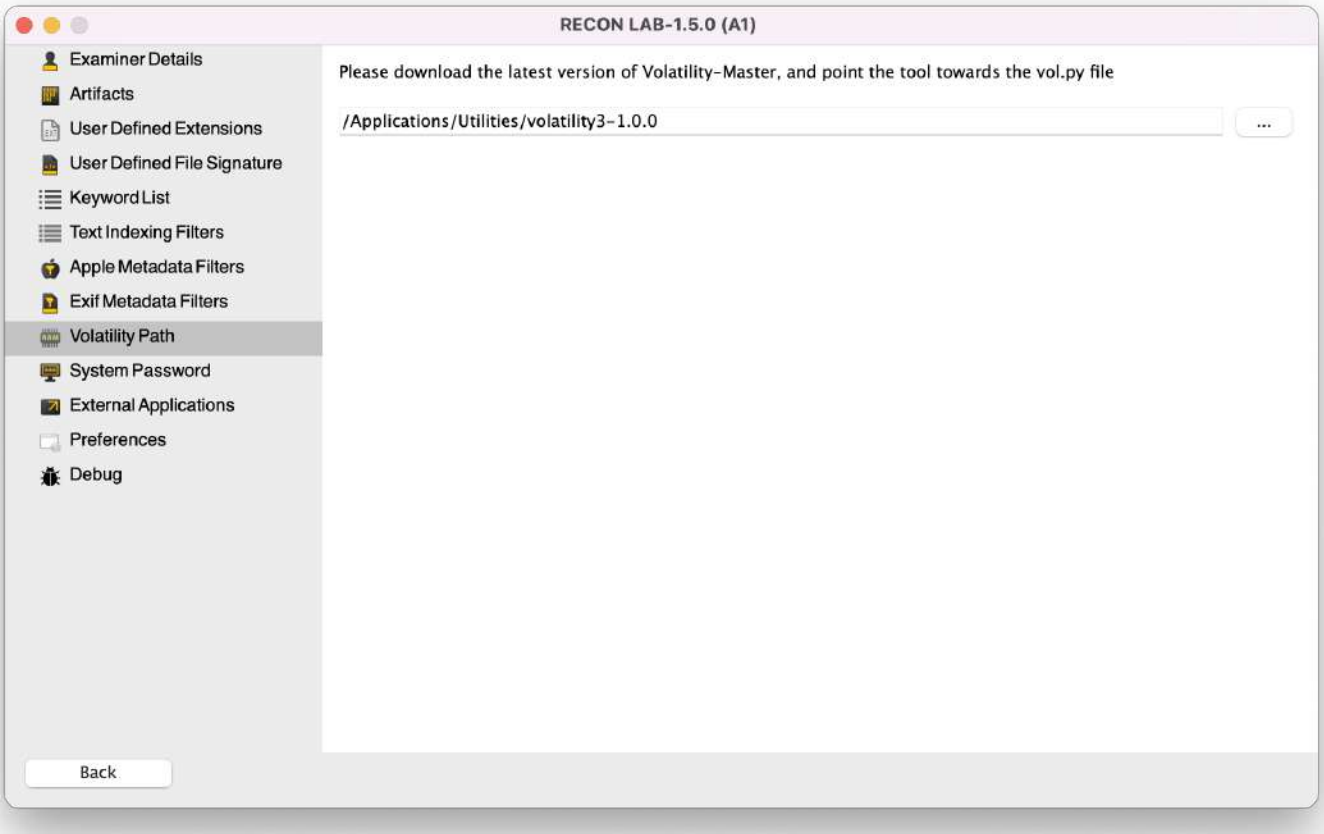
Title – The common name of the EXIF Metadata.

Description – The official description of the Apple Extended Attribute.

9.9 Volatility Path

RECON LAB supports Volatility for RAM analysis. Volatility can be downloaded from https://www.volatilityfoundation.org/

Once downloaded, Volatility can be configured to work with RECON LAB.

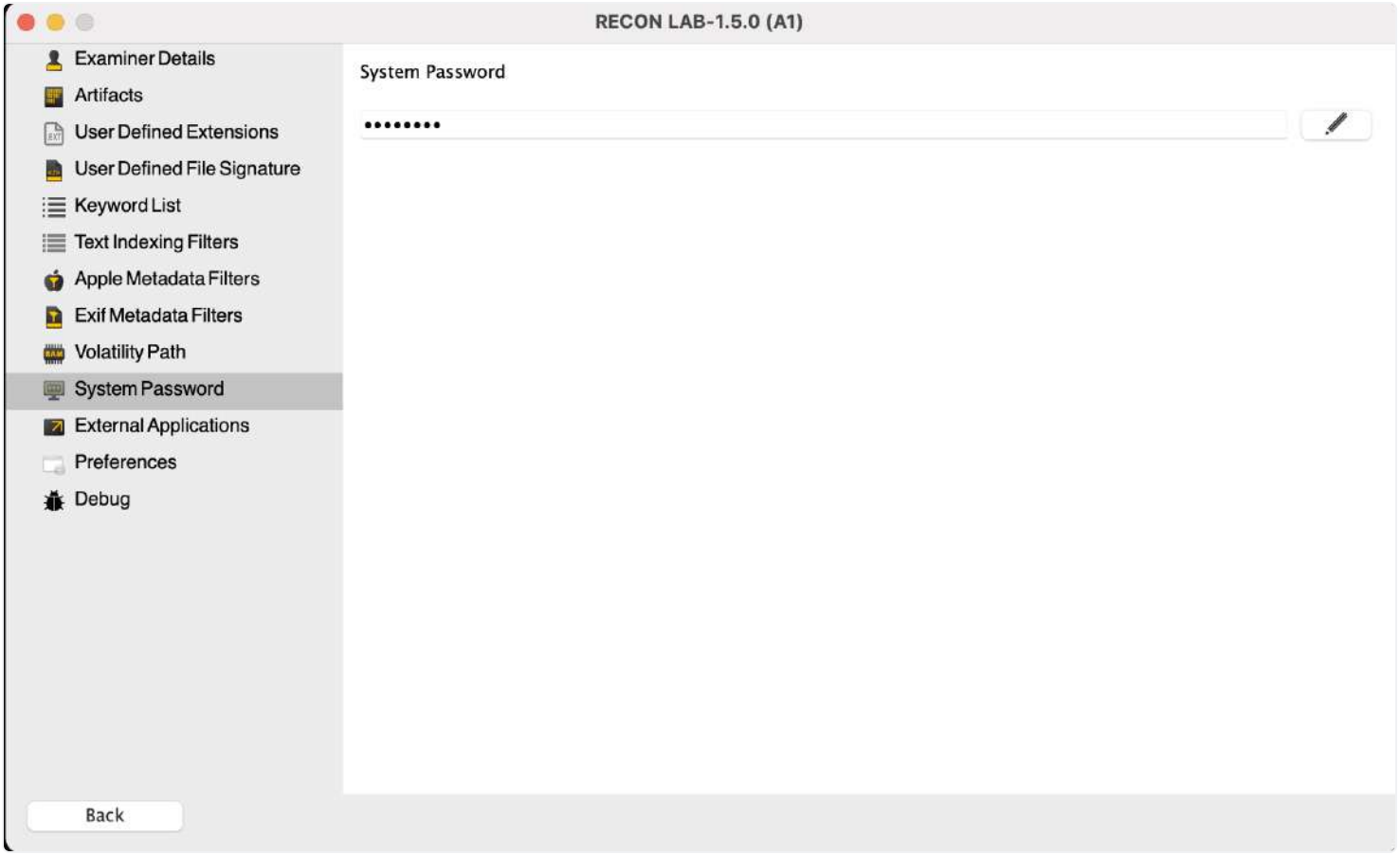


To use Volatility within RECON LAB select the three dots in the Volatility Path settings. Navigate to and select the "vol.py" file to save the path.

Please refer to Volatility documentation for downloading and setting up Volatility profiles and plugins here: https://github.com/volatilityfoundation/volatility/wiki

9.10 System Password

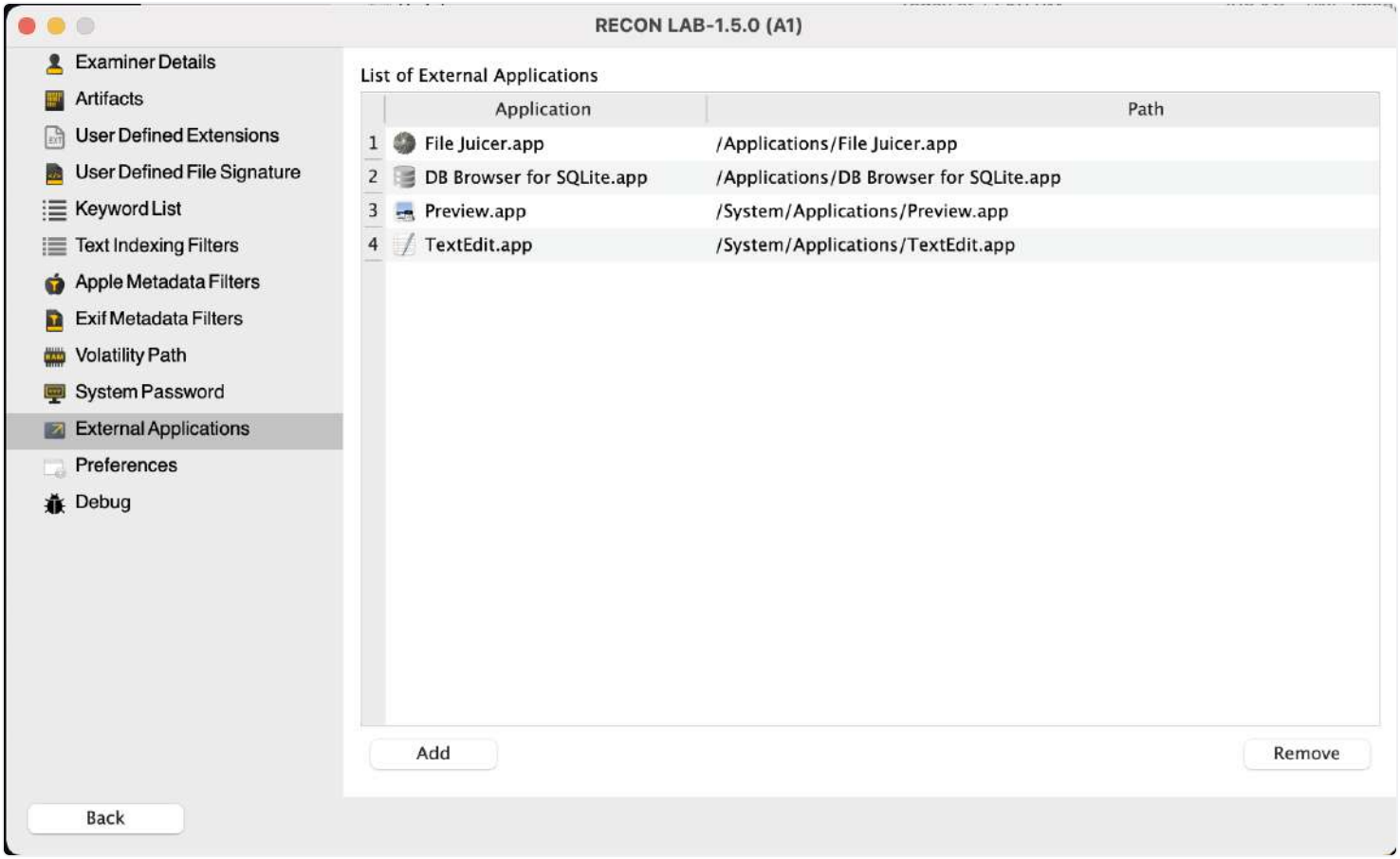
When you start RECON LAB for the first time or if you reset RECON LAB you will be prompted to enter your Admin password. If you change your password after installing RECON LAB you will have to update it using the System Password settings.



To update, click the pencil icon and enter your new password.

9.11 External Applications

RECON LAB allows files to be sent to and opened in external applications.

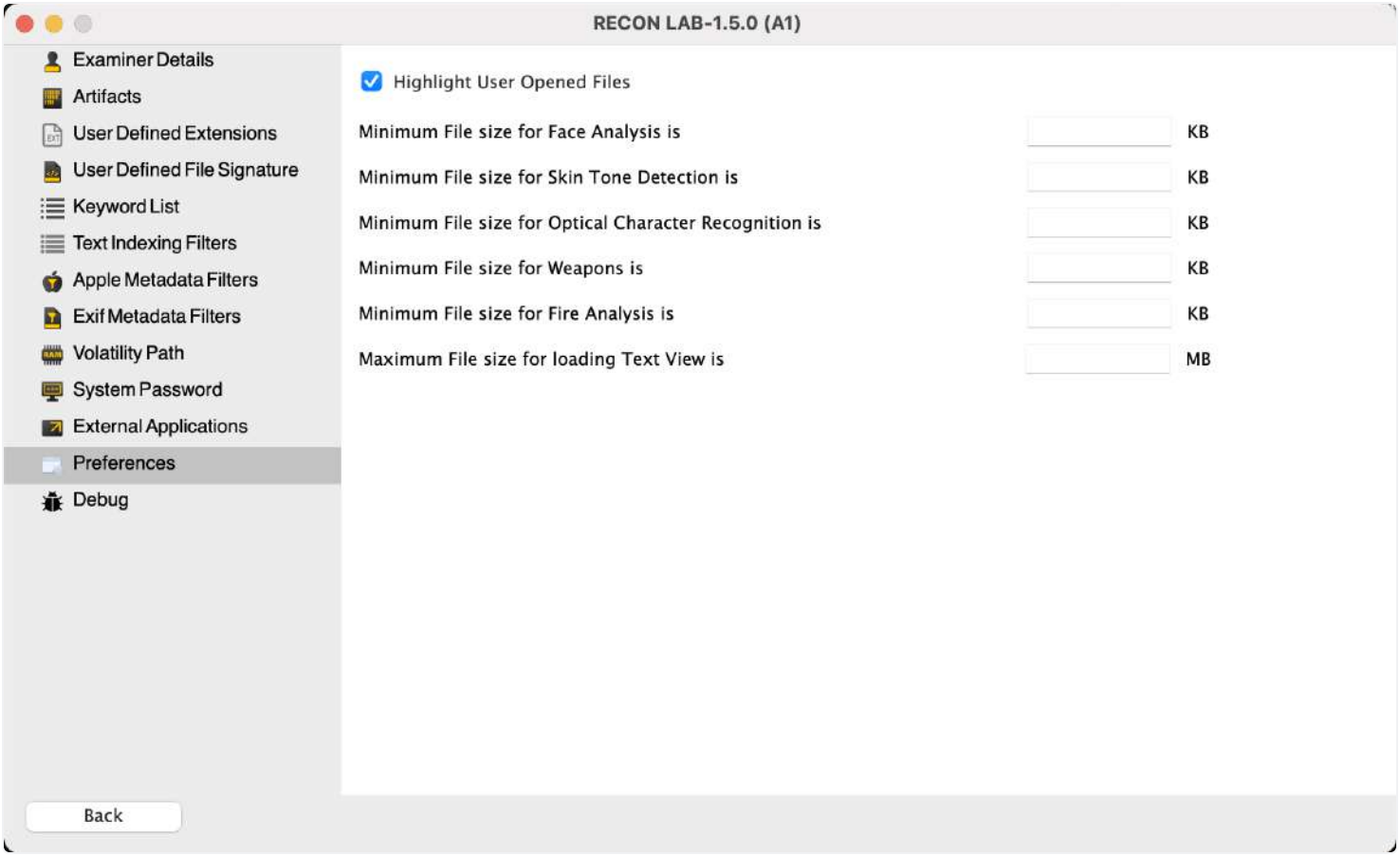


To add an application select the “Add” button. Navigate to and select the application that you would like to add.

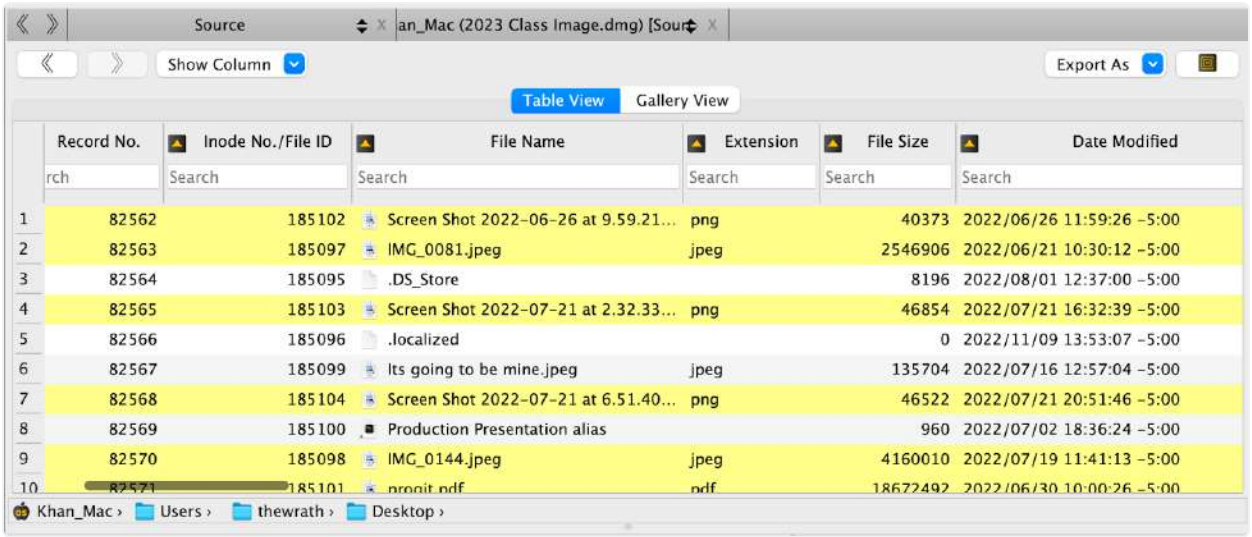
To remove an application, highlight the application to remove and select the “Remove” button.

9.12 Highlight User Opened Files

RECON LAB gives examiners the option to highlight files that were opened by a user on the source device. In the configuration menu navigate to Preferences and select “Highlight User Opened Files.” This can be done in the configuration menu before you start a case or after a case has already been started.

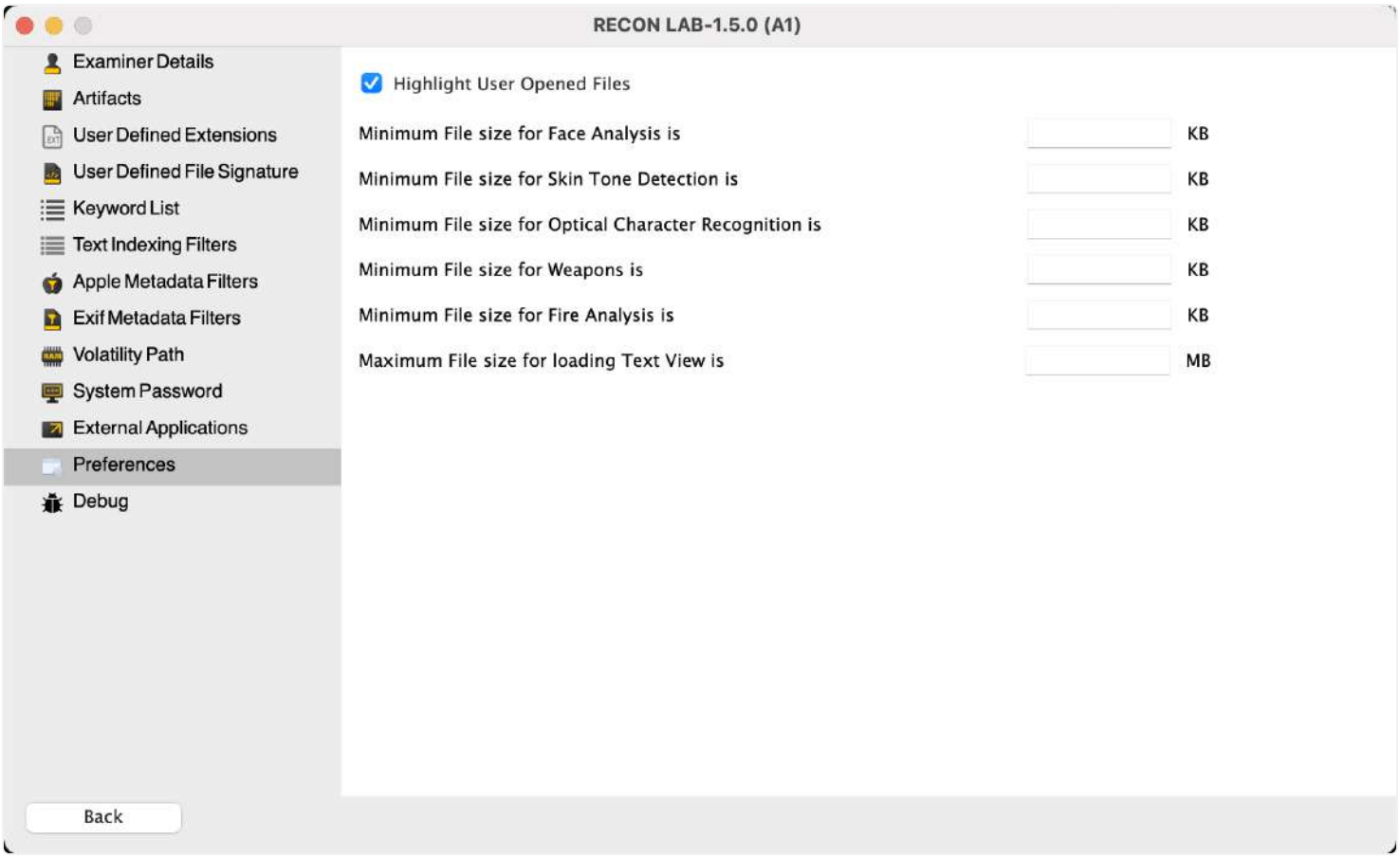


Files will be highlighted yellow if they have an entry in the use count in their Apple Extended Attributes metadata.



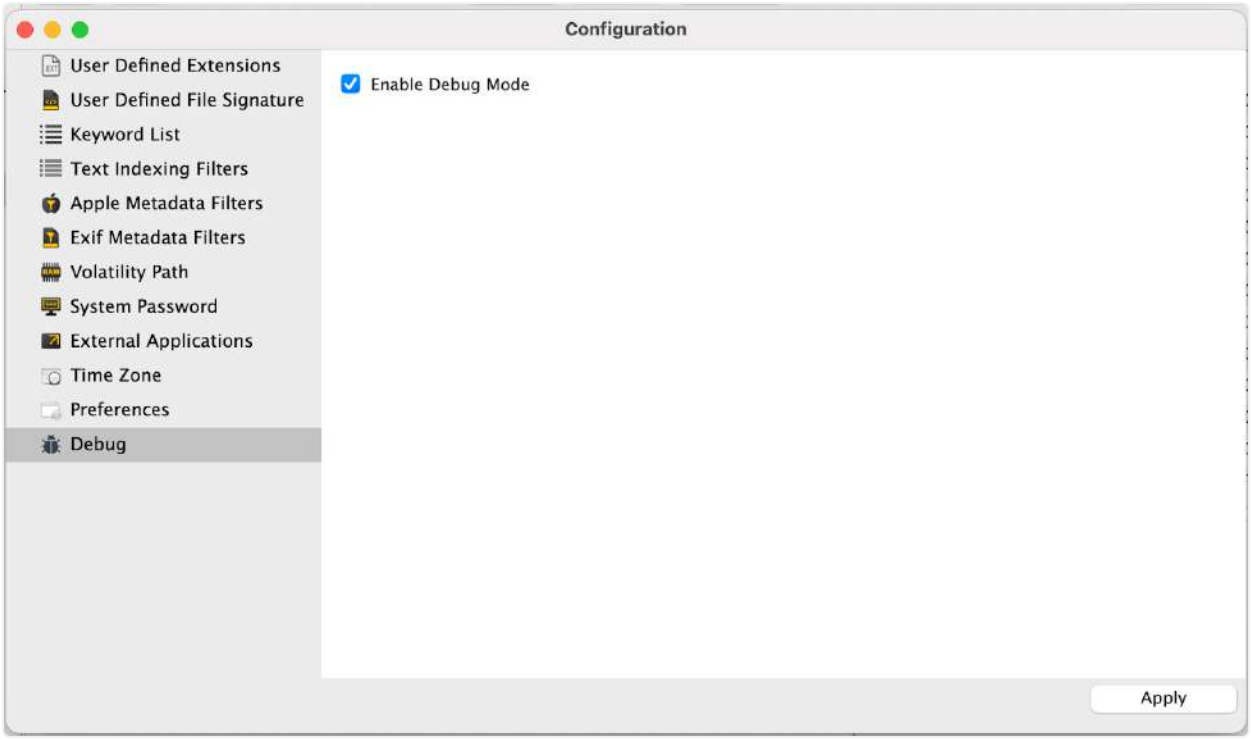
To remove the highlights open RECON Config from the menu bar and deselect “Highlight User Opened Files” then click “Apply.”

9.13 Text View Settings



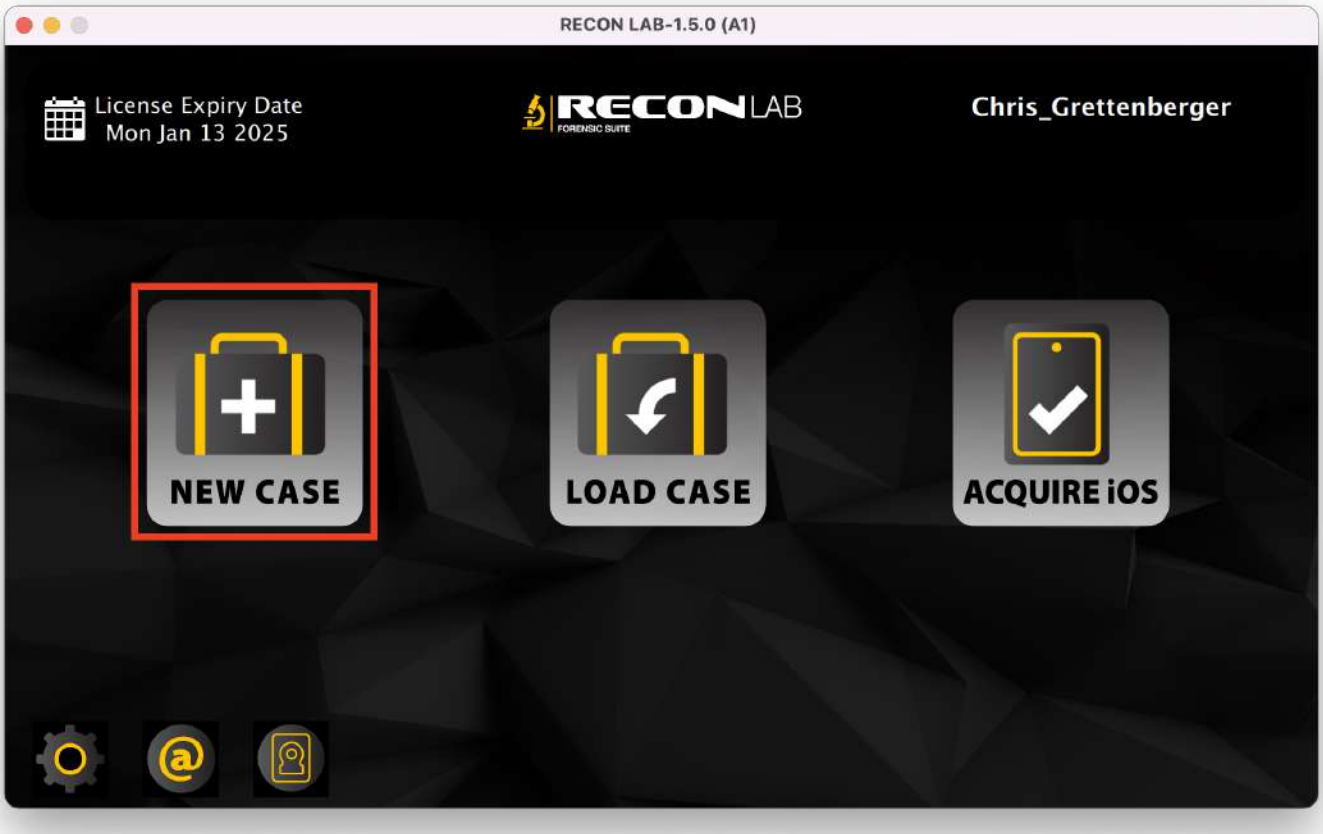
To speed up processing RECON LAB allows you to set the Maximum File Size for the Text View. The default setting is 20 MB. To increase or decrease the size, enter any value. Keep in mind the value will be interpreted as megabytes.

9.14 Debug Mode



RECON LAB has the ability to log any errors that cause the application to fail. Using this feature will make our development team aware of the error, and allow them to diagnose and fix the error. This is accomplished by turning on debug mode (as shown above). To turn on debug mode, select “Debug” from the side bar menu on the left side of the screen. After that click the check box next to “Enable Debug Mode.” When the box is checked, “Debug mode” is active

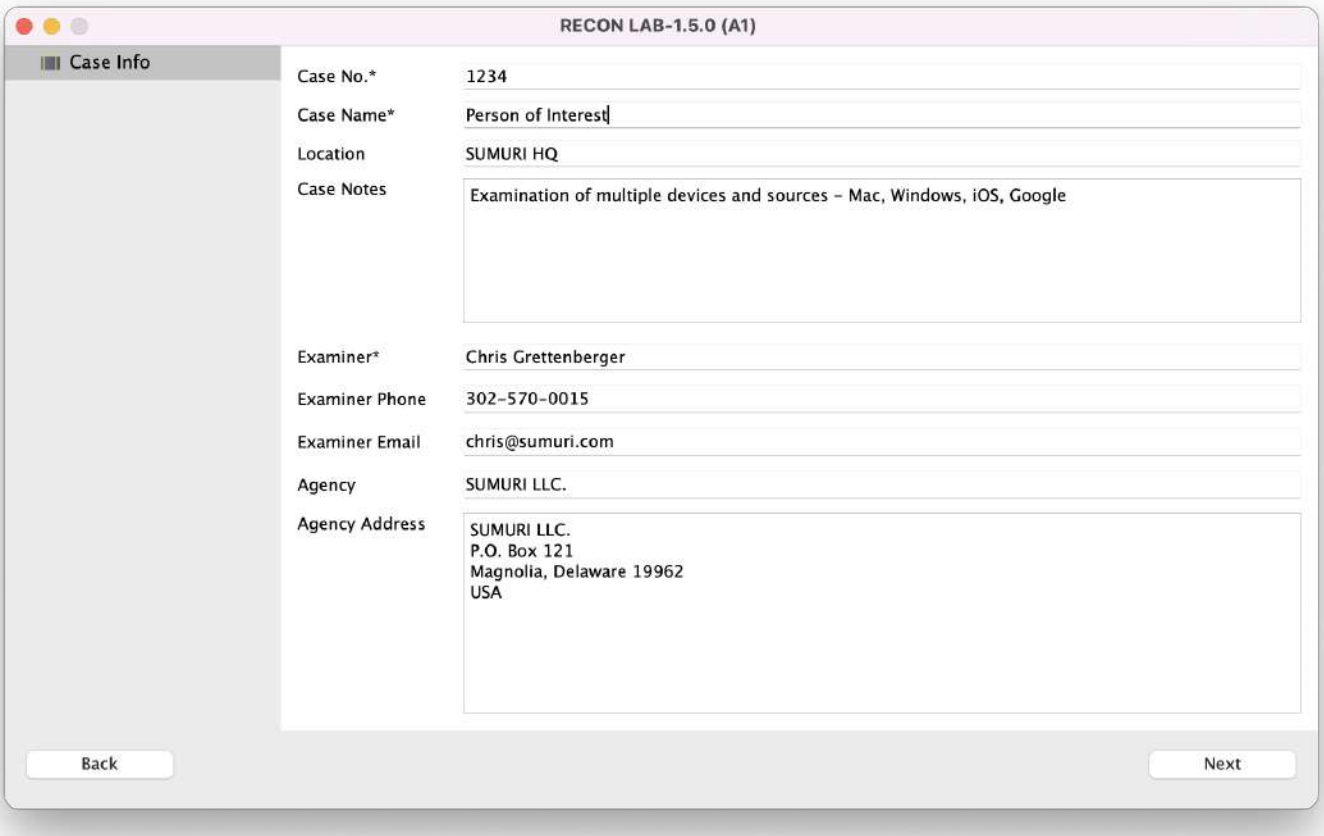
10. Starting A New Case



To start a case with RECON LAB select “New Case” from the Welcome Screen.

10.1 Case Info

When you start a new case with RECON LAB the Case Wizard starts with the Case Info screen. If any information was added previously in the RECON Configuration settings that info will automatically be included. The information entered here will be included in RECON LAB reports. Certain fields are mandatory and must be entered to proceed to the next screen. These fields are marked with an asterisk.



The following information can be entered into the Case Info window.

Case No. (mandatory) – A unique case number.

Case Name (mandatory) – Name for your case.

Location – Location of the incident or the exam.

Case Notes – free form to add any notes required.

Examiner (mandatory) – Examiner name.

Examiner Phone – Phone number for the examiner.

Examiner Email – Email for the examiner.

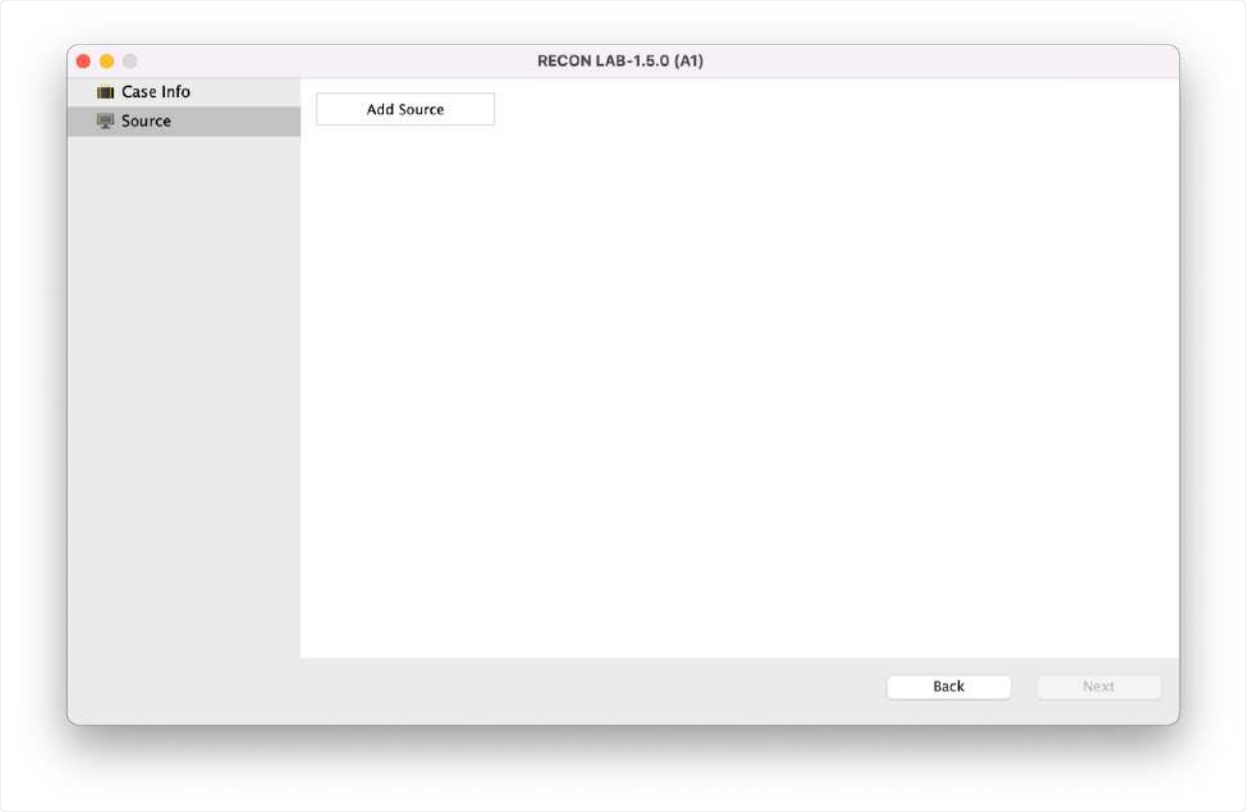
Agency – Agency name.

Agency Address – Address for the agency.

After you have entered the mandatory information and any additional information that you want then click “Next”.

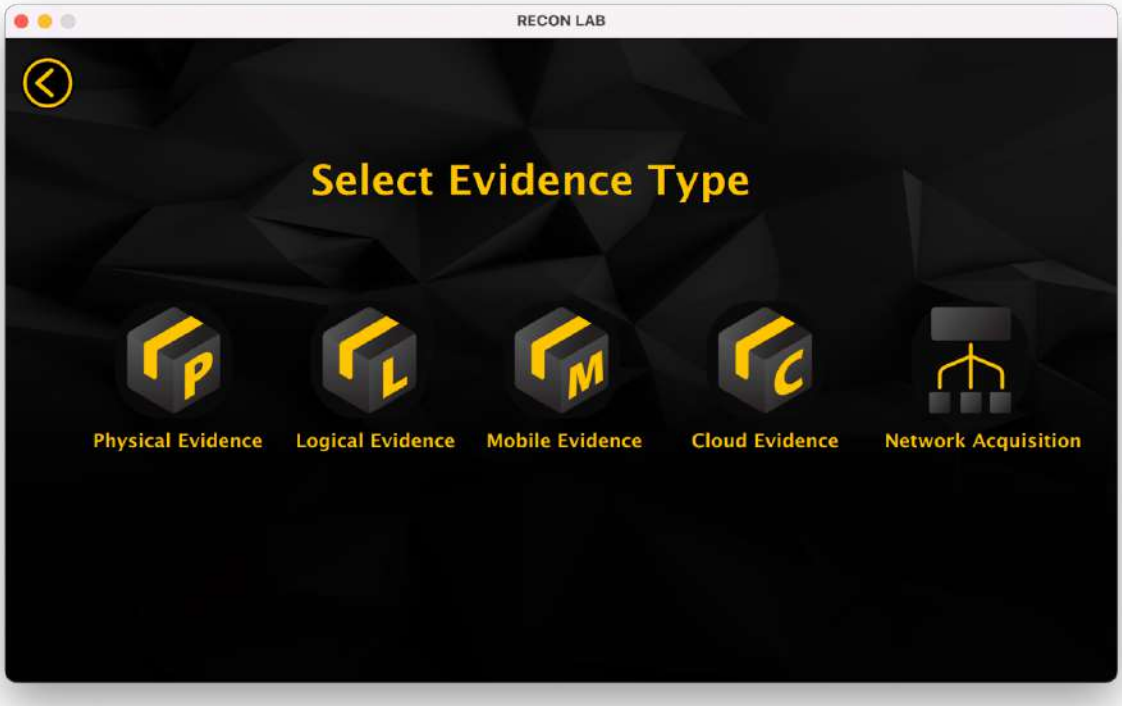
10.2 Adding Source Data to Process

RECON LAB can accept a variety of sources to process.



To select a source to process use the “Add Source” dropdown and select a source to process.

Options for adding sources are broken down into five categories. Each category has specific image type options, some of which will change the way your image is processed. It is imperative that the correct source type is selected for your image.



Physical Evidence- includes options for physically attached media and physically acquired forensic images

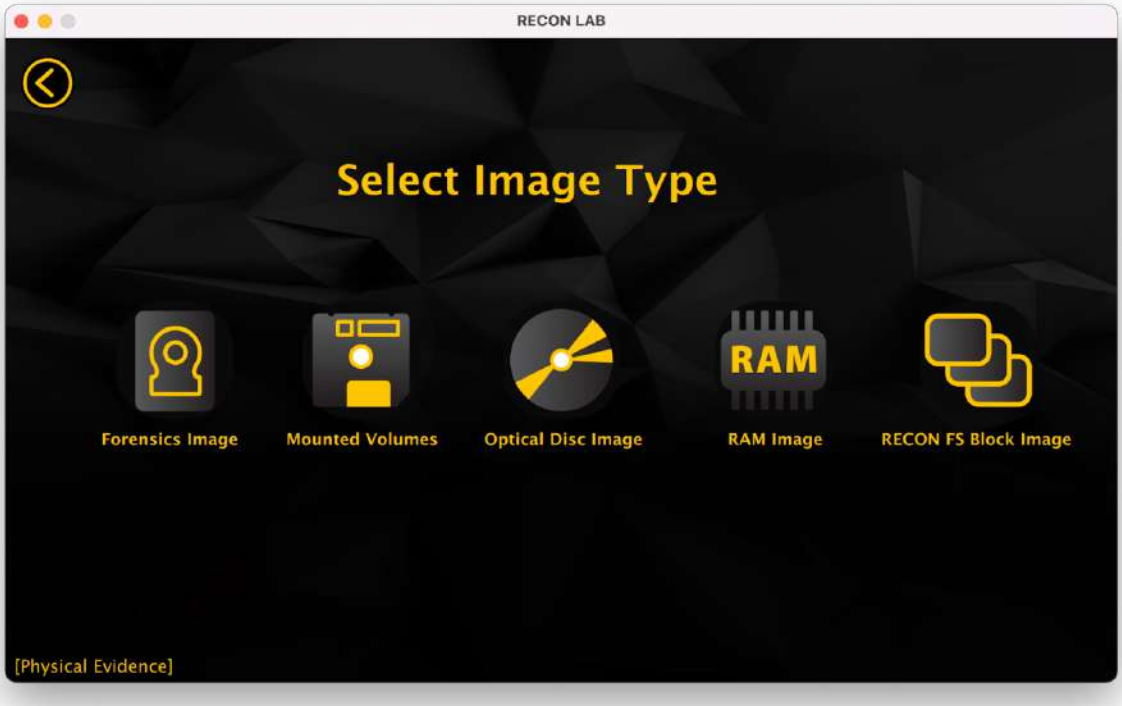
Logical Evidence- includes options for logically acquired forensic images, including ones specifically captured with RECON ITR

Mobile Evidence- includes options for different mobile backups and extractions

Cloud Evidence- includes options for cloud production data

Network Acquisition- includes options for acquisitions done over a network

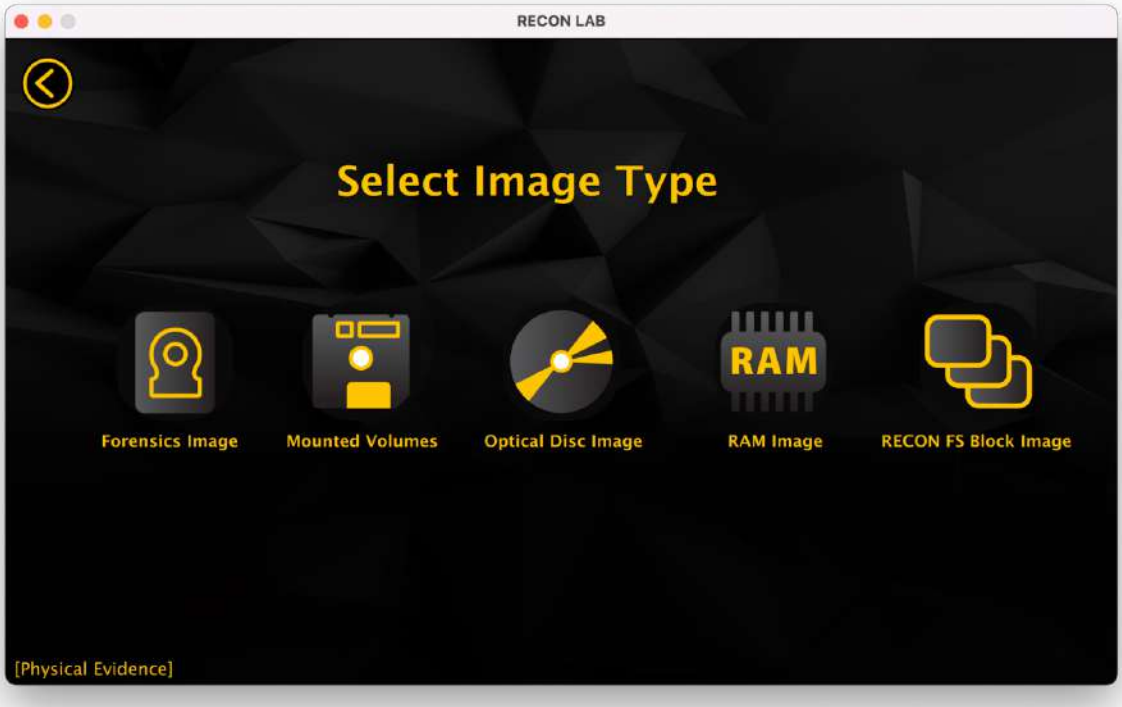
10.2.1 Physical Evidence



RECON LAB supports ingesting multiple different types of Physical Evidence from multiple types of sources. From forensic images of macOS, Windows, and Linux, to RAM images and Optical Disc images.

To begin loading physical evidence into your case, select the Physical Evidence icon from the ‘Evidence Type’ menu.

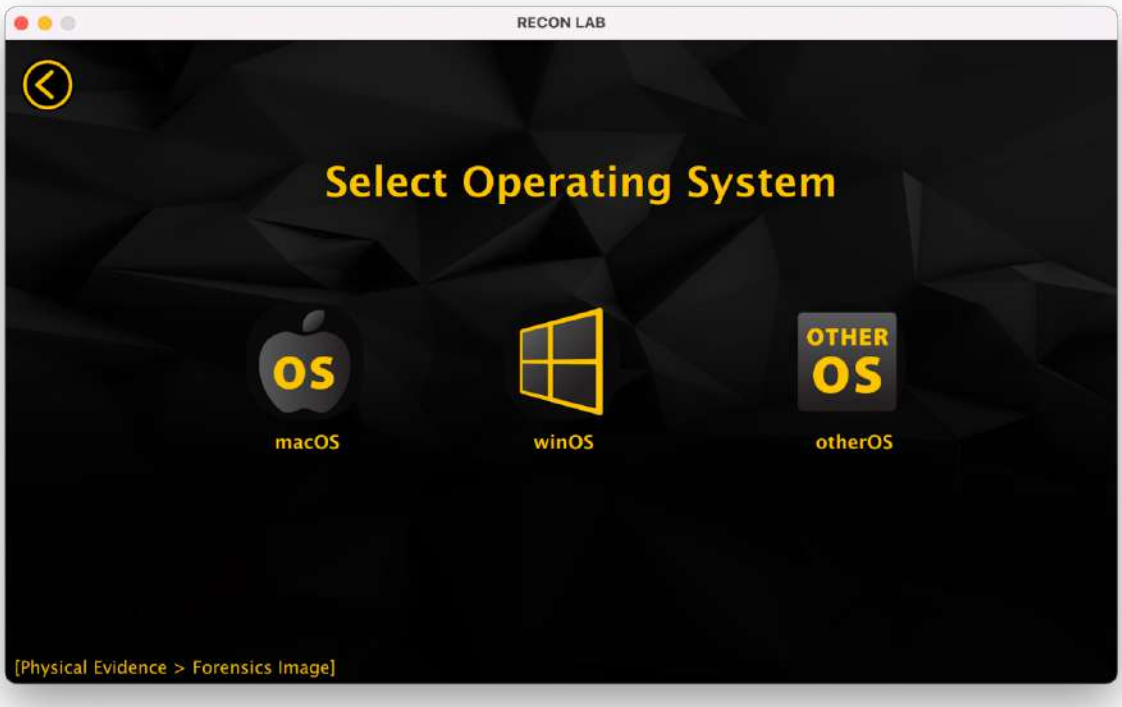
The ‘Select Image Type’ screen will then load and allow you to choose the type of image you’d like to load.



10.2.1.1 Forensics Images

RECON LAB supports just about any forensic image format. This option refers specifically to full physical disk acquisitions.

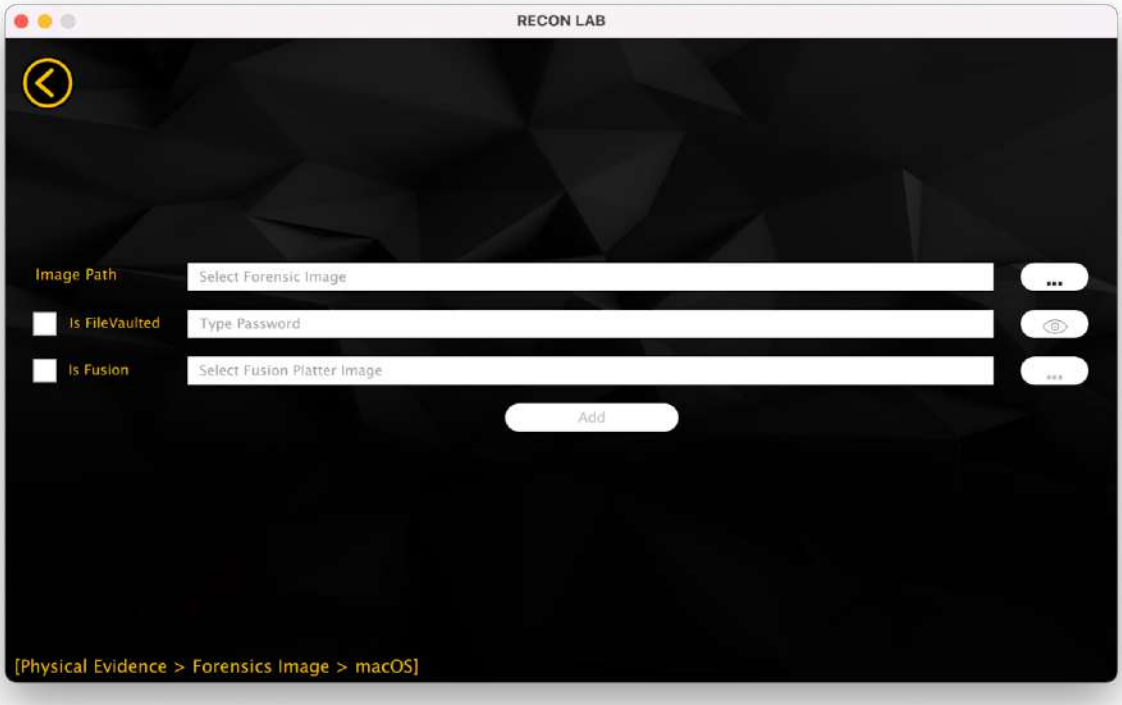
To begin, select the Forensics Image at the Image Type screen.



Next, select the Operating System that your image is of.

10.2.1.1.1 Physical Images of macOS

If the image is of a Mac, select the macOS icon to be greeted with the following screen.



From here, you can configure the image as needed.

Select the '...' icon on the right side to open a file browser window, allowing you to navigate to your stored image file.

Currently accepted formats are:

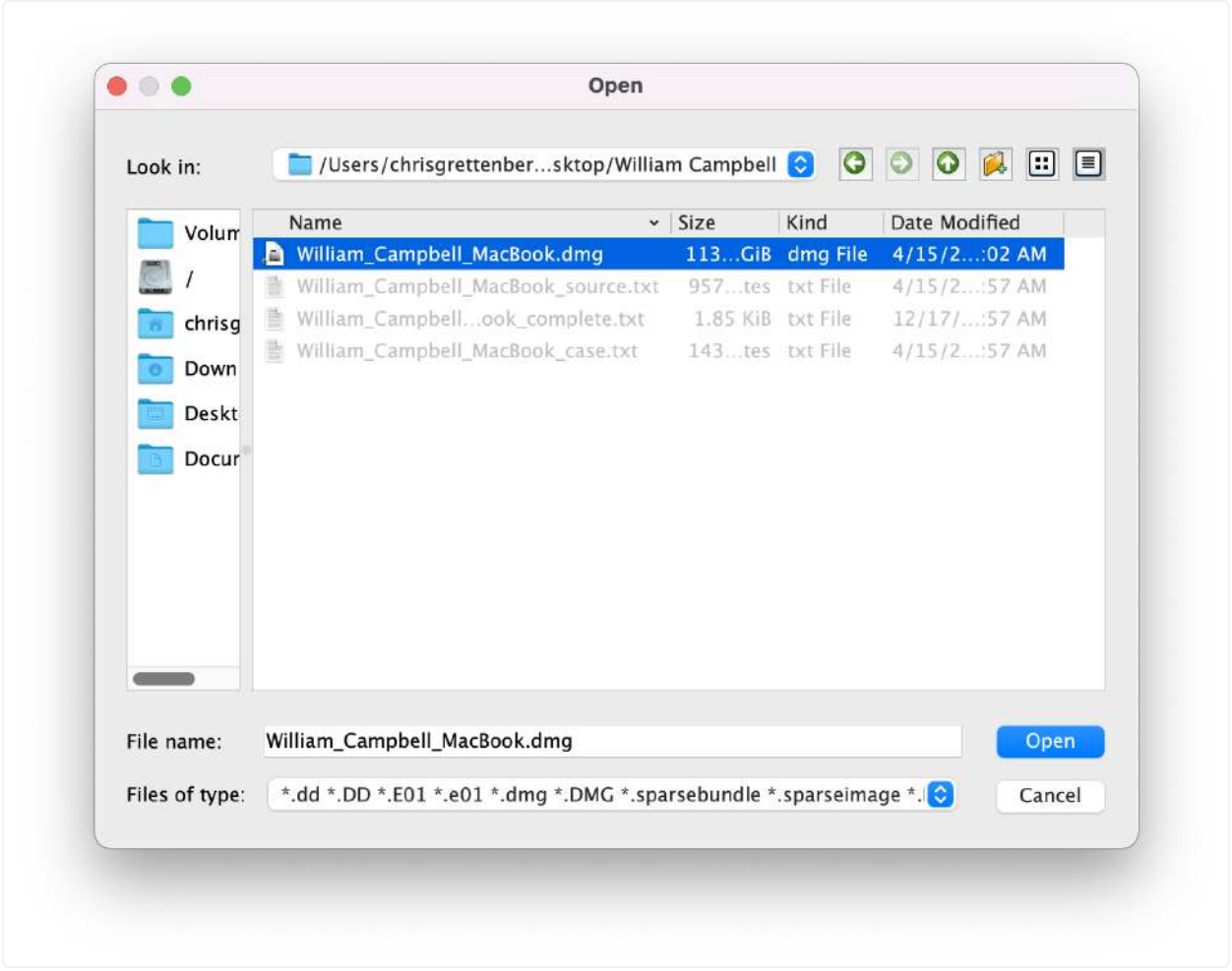
RAW Images – .dd, .000, .00001, .raw

Apple Disk Images – .dmg, .sparsebundle, .sparseimage

Expert Witness Format (EWF) – .E01, .Ex01, .L01, .S01

Advanced Forensic File Format - AFF4

Select your image and hit 'Open' to continue.

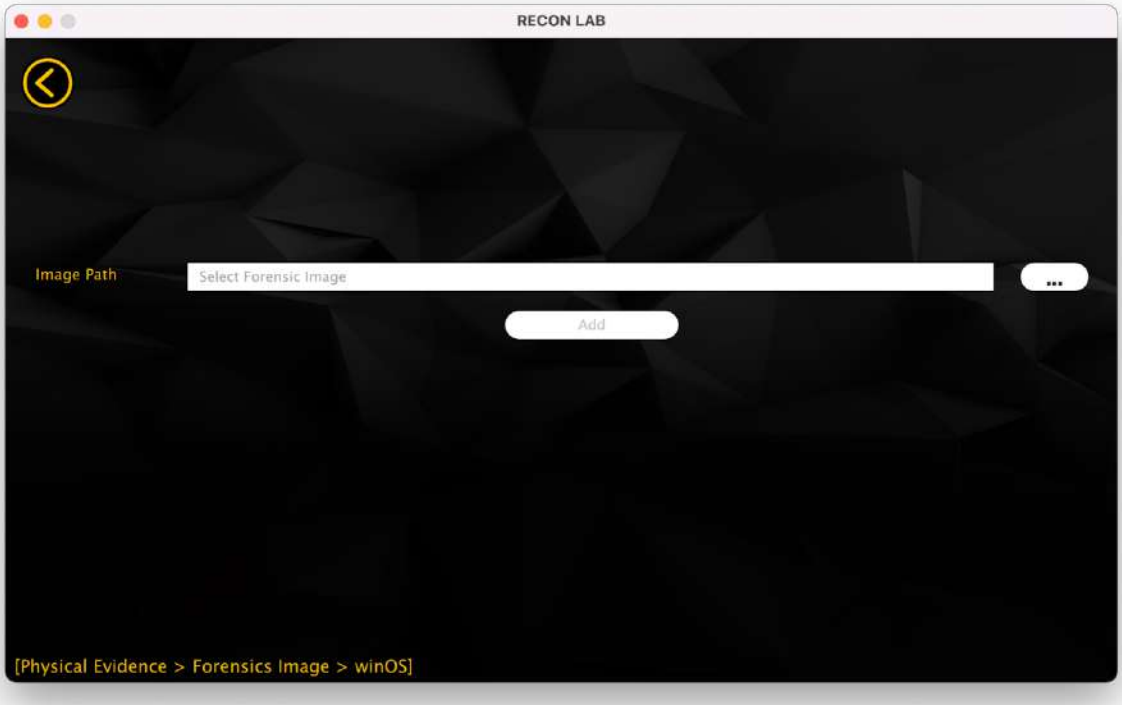


If the image is of a FileVaulted Mac, select the 'Is FileVaulted' option, then enter the administrator password of the image to automatically decrypt it during processing.

If the image is of a Fusion Drive Mac, ensure that the first image added is of the smaller SSD drive before continuing to the next step. Then, select the 'Is Fusion Drive' option, and navigate to the location of the larger HDD image to automatically pair the images together during processing.

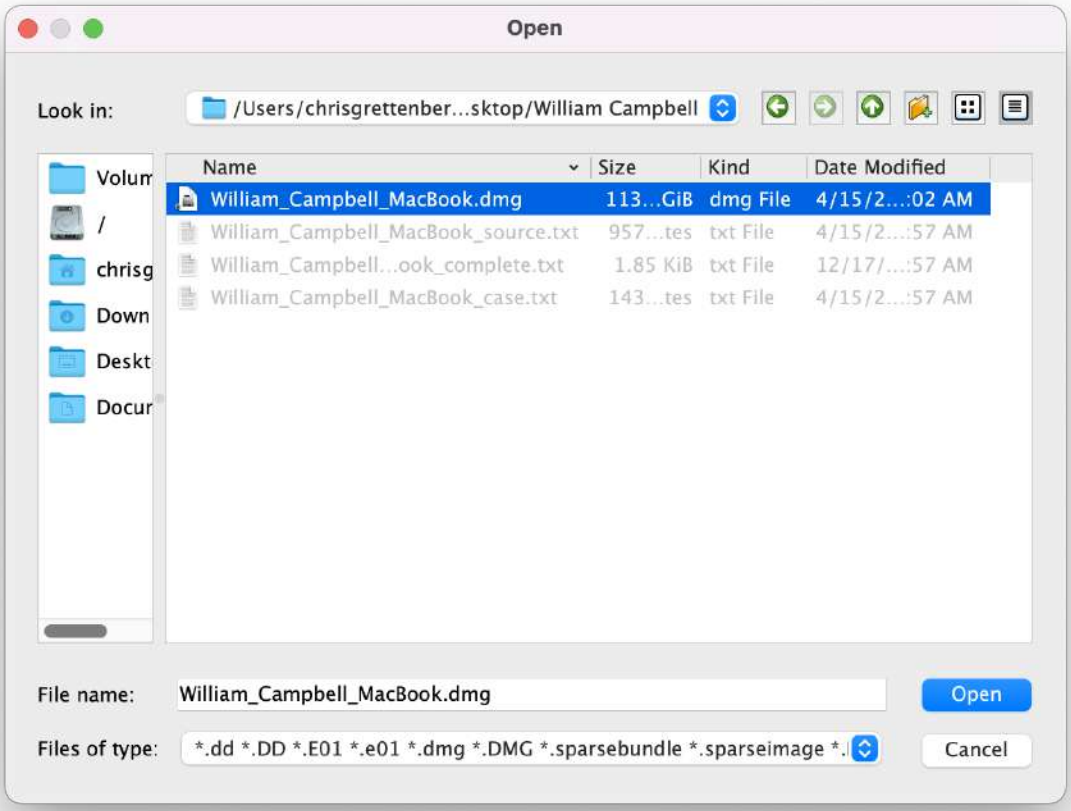
10.2.1.1.2 Physical Images of Windows Machines

If you're loading images of a Windows machine, select the Windows Icon to be greeted with the following screen.



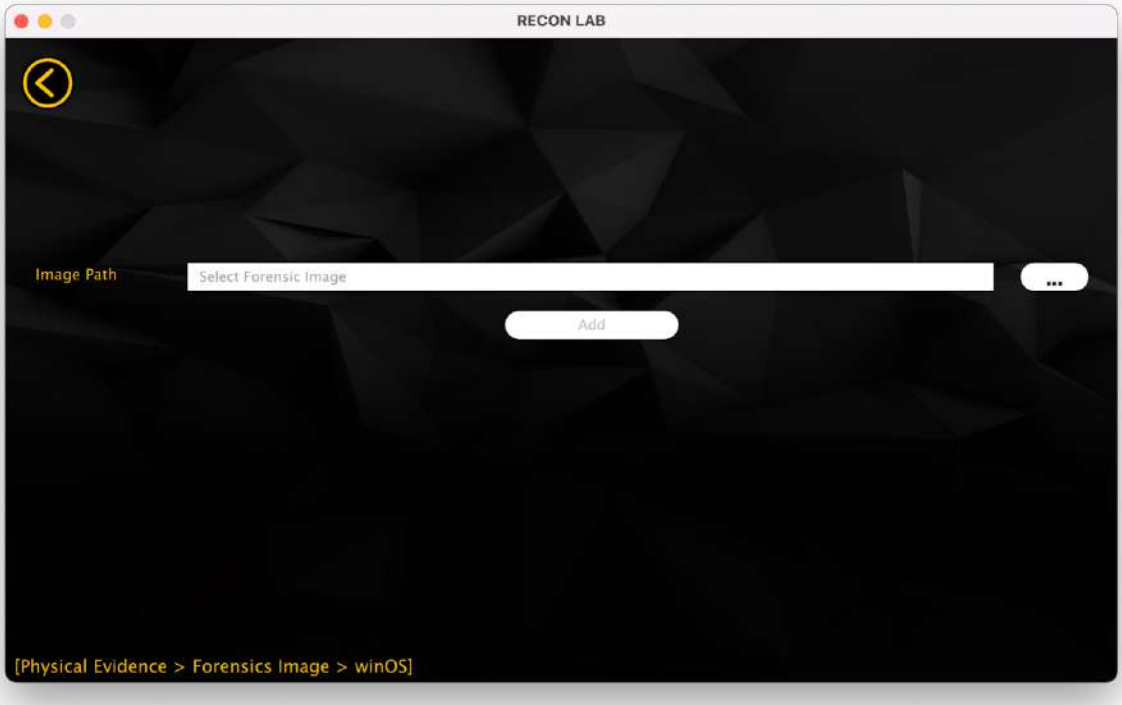
From here, select the '...' icon on the right side to open a File Browser window. This will allow you to navigate to your stored image file.

Select your image and hit 'Open' to continue.



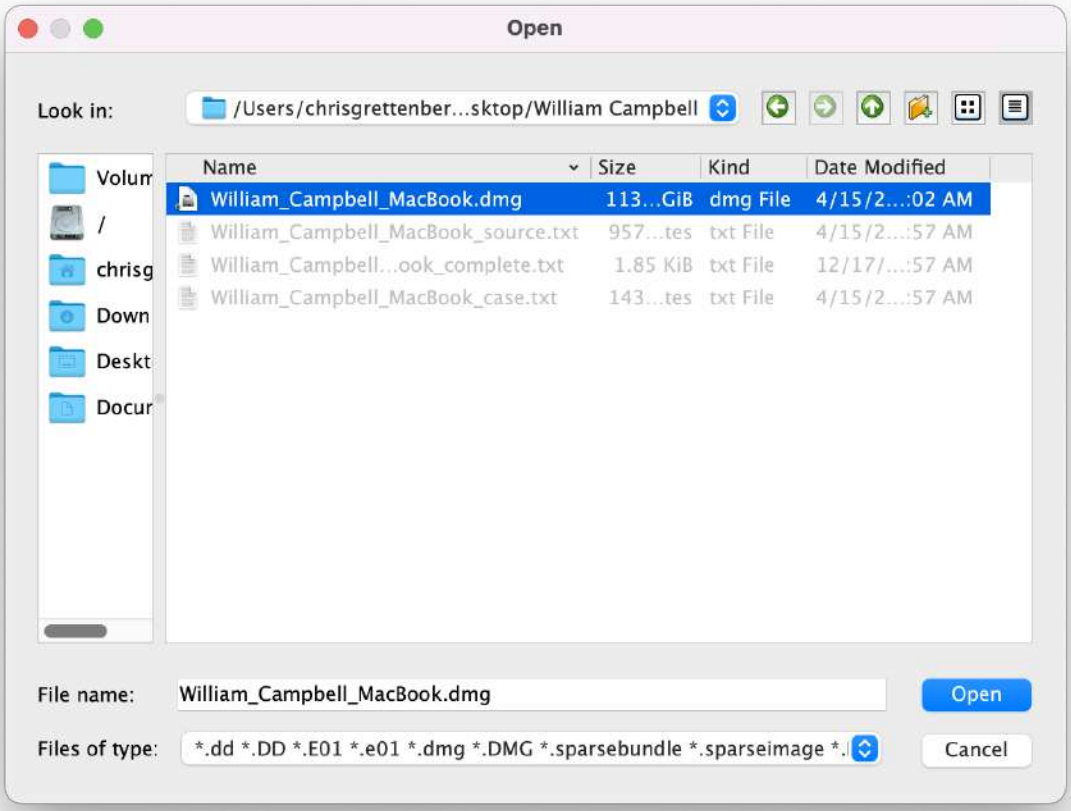
10.2.1.1.3 Physical Images of Other OS Machines

If you're loading images of a Windows machine, select the Windows Icon to be greeted with the following screen.



From here, select the '...' icon on the right side to open a File Browser window. This will allow you to navigate to your stored image file.

Select your image and hit 'Open' to continue.

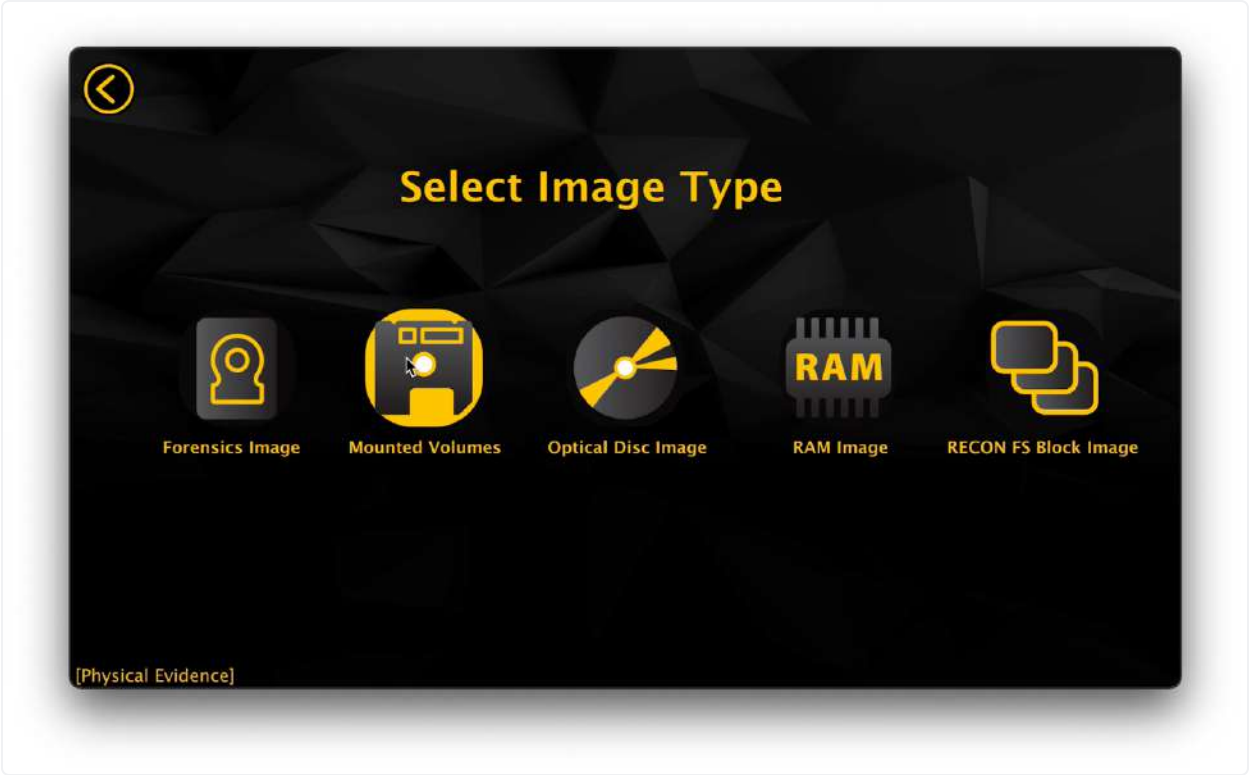


Select ‘Add’ to add the Image to your case for processing.

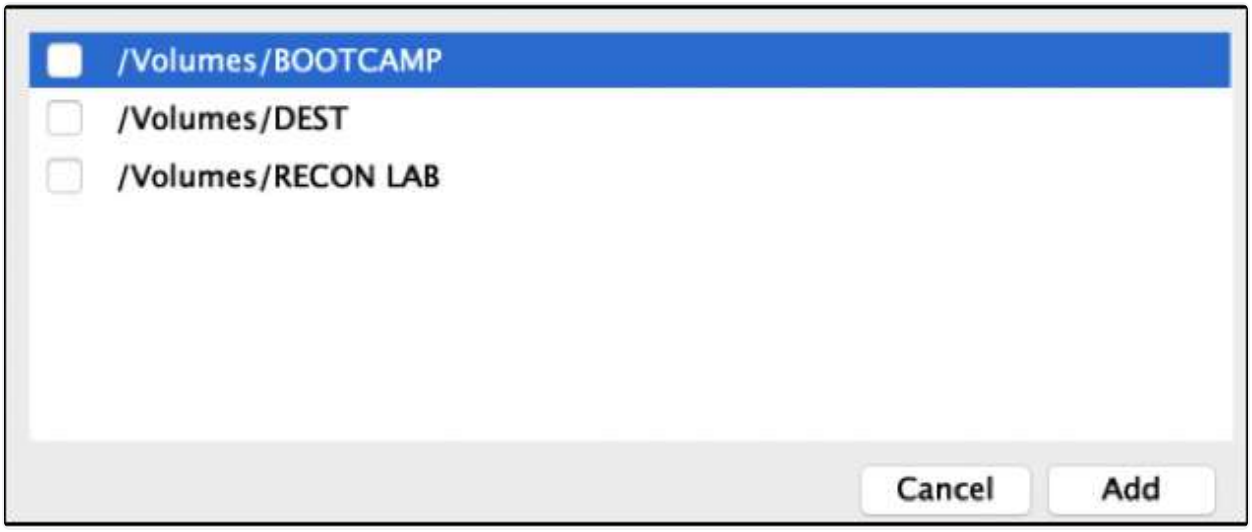
10.2.1.2 Mounted Volumes

RECON LAB can add mounted volumes as a source as well.

To add a mounted volume as a source, select the ‘Mounted Volumes’ Icon from the Physical Evidence ‘Select Image Type Menu’.



Selecting Mounted Volumes presents you with a selection box. Any currently mounted volumes with be displayed.

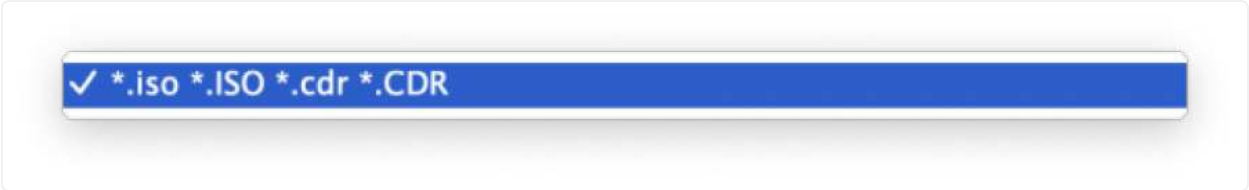


To add, check the box next to the volume path and then click “Add”.

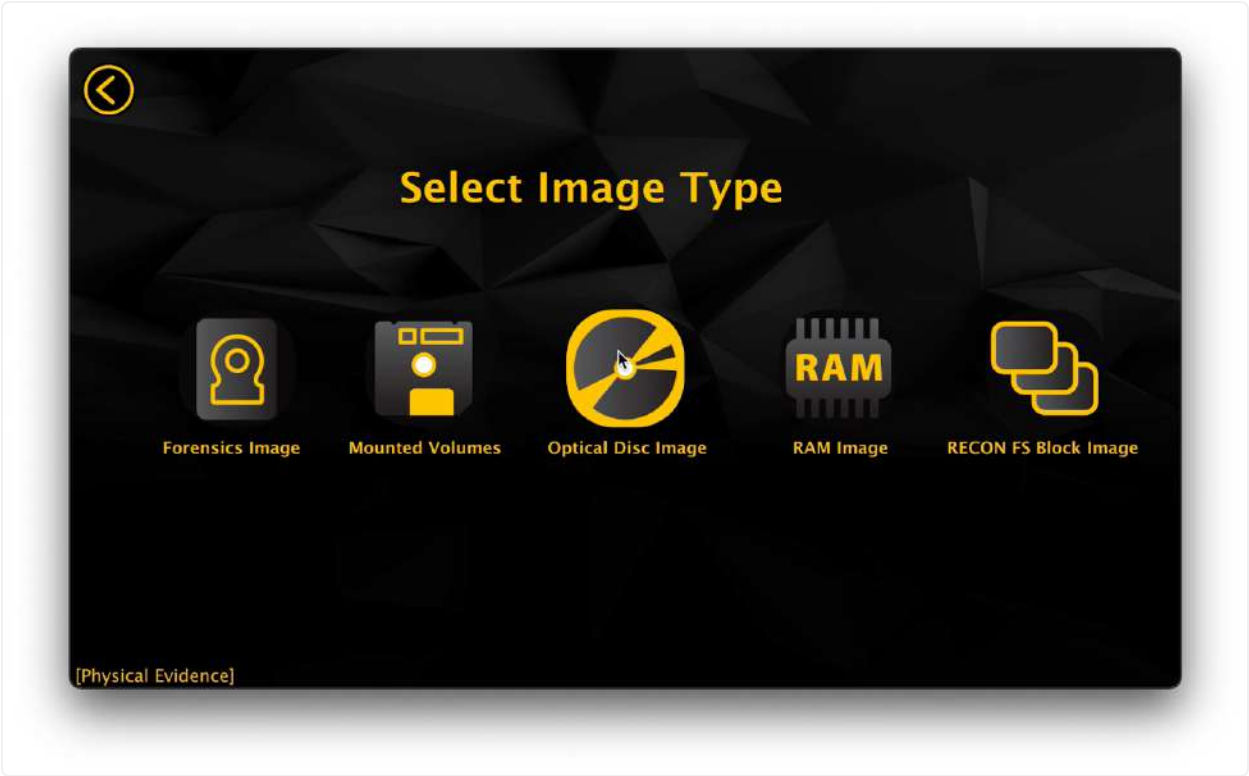
10.2.1.3 Optical Disc Image

RECON LAB can support Optical Disc image formats as a source.

RECON LAB currently supports .ISO and .cdr Optical Disc formats.

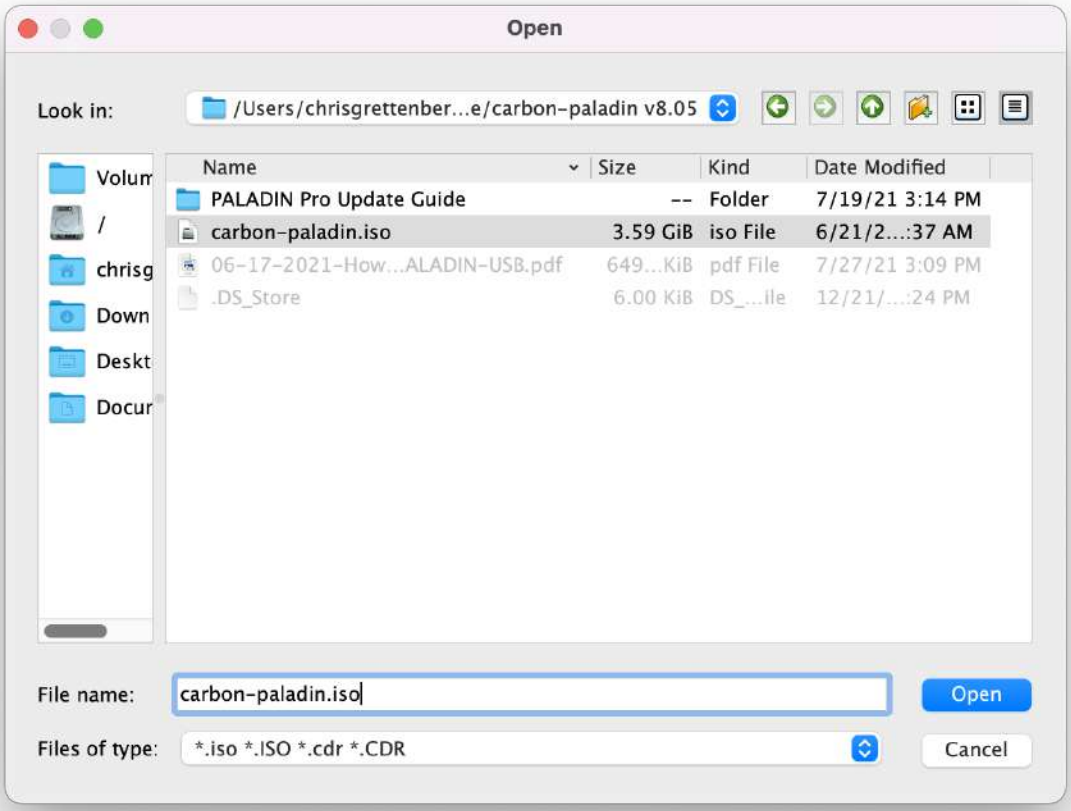


Select the ‘Optical Disk Image’ Icon under ‘Select Image Type’.



From here, select the ‘...’ icon on the right side to open a File Browser window. This will allow you to navigate to your stored image file.

Select your image and click ‘Open’ to continue.

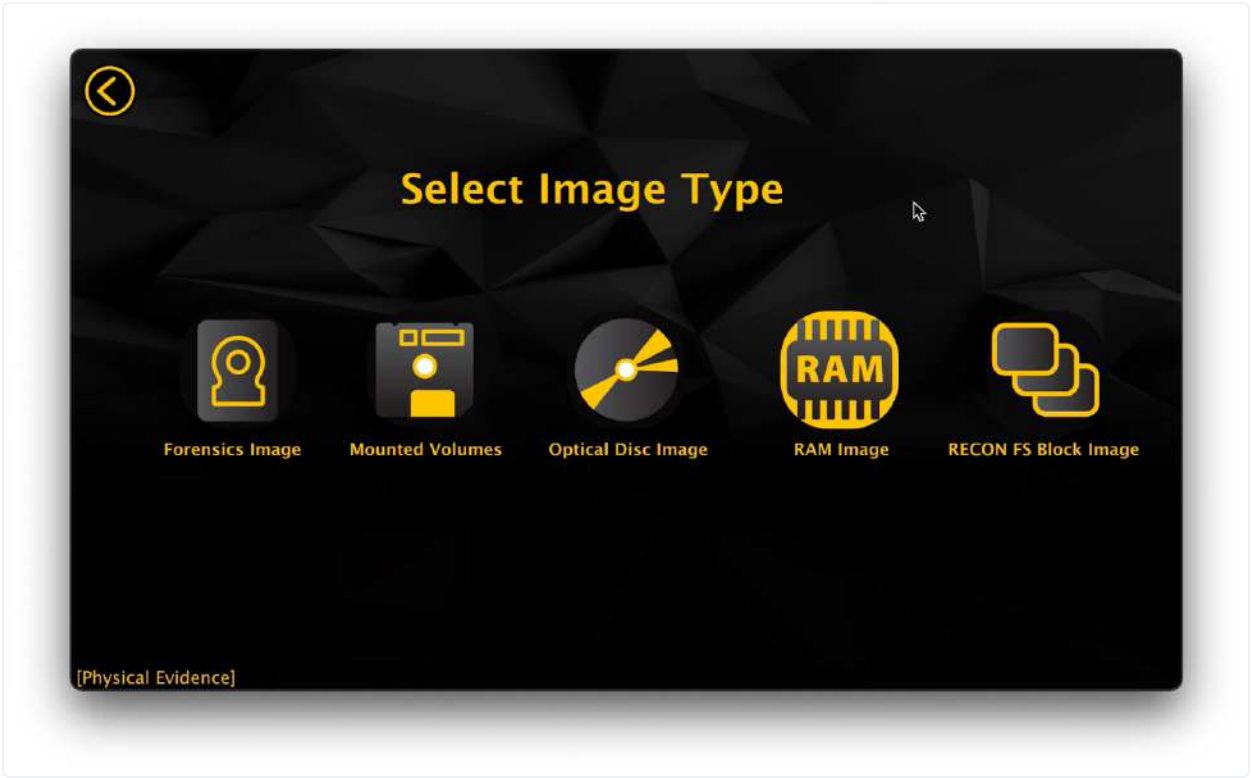


Select ‘Add’ to add the Optical Disc Image to your case for processing.

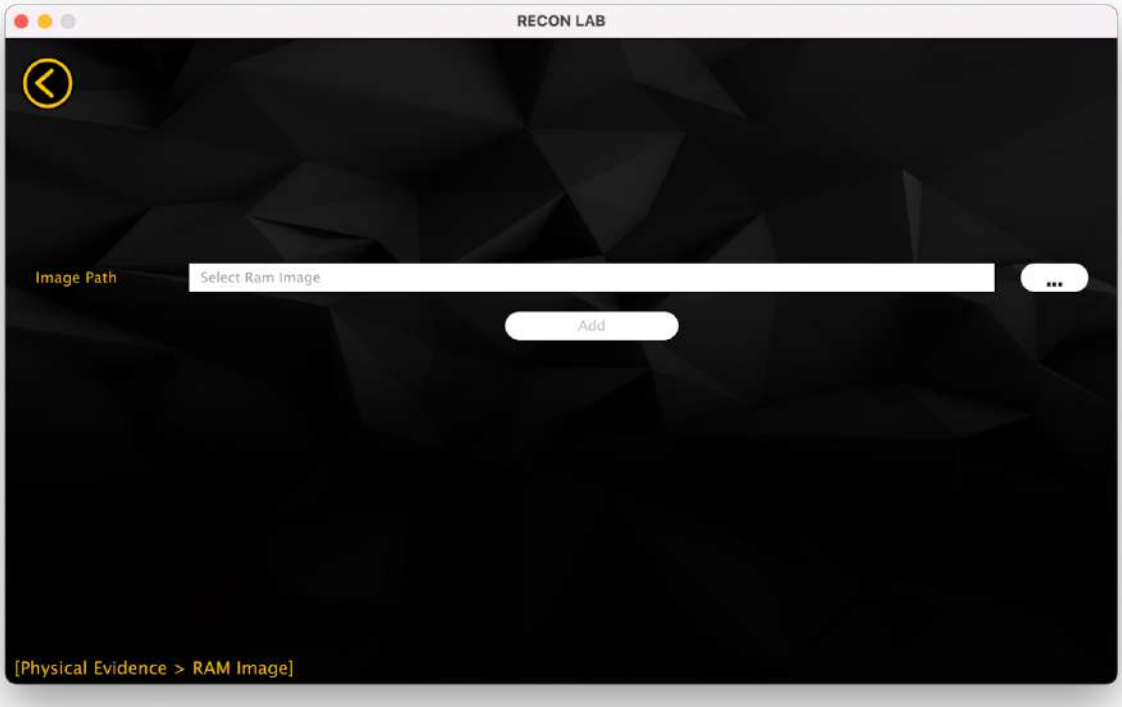
10.2.1.4 RAM Image

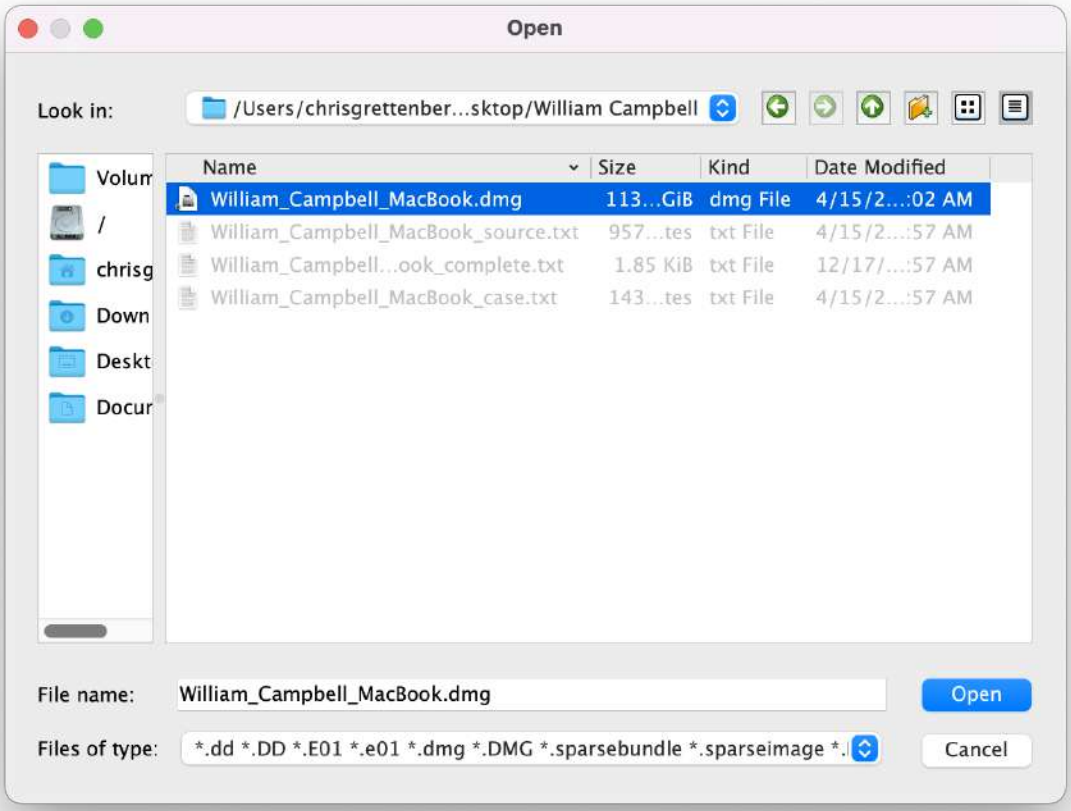
RECON LAB supports loading RAM images which are usually in raw format.

To load a RAM image, select the ‘RAM Image’ icon in the Physical Evidence ‘Select Image Type’ menu.



From there, select the ‘...’ icon on the right side to open a File Browser window. This will allow you to navigate to your stored image file.

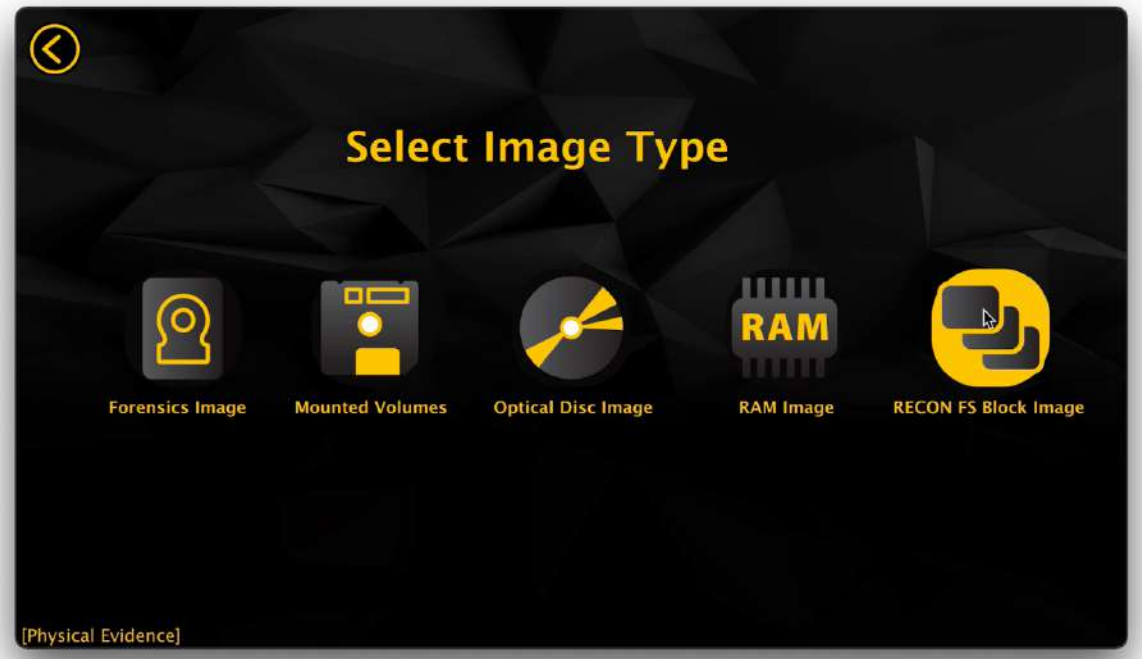




Select your image and click ‘Open’ to continue.

Select ‘Add’ to add the RAM Image to your case for processing.

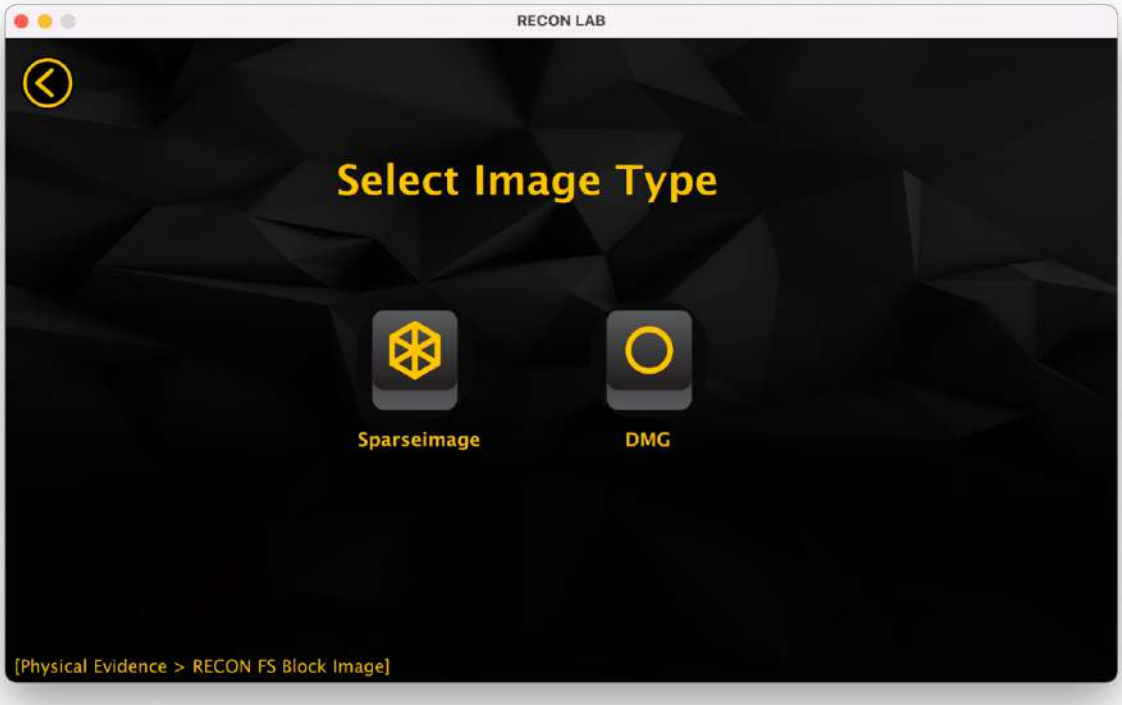
10.2.1.5 RECON FS Block Image



FS Block Copy is the primary output format of T2 Macs imaged with RECON ITR.

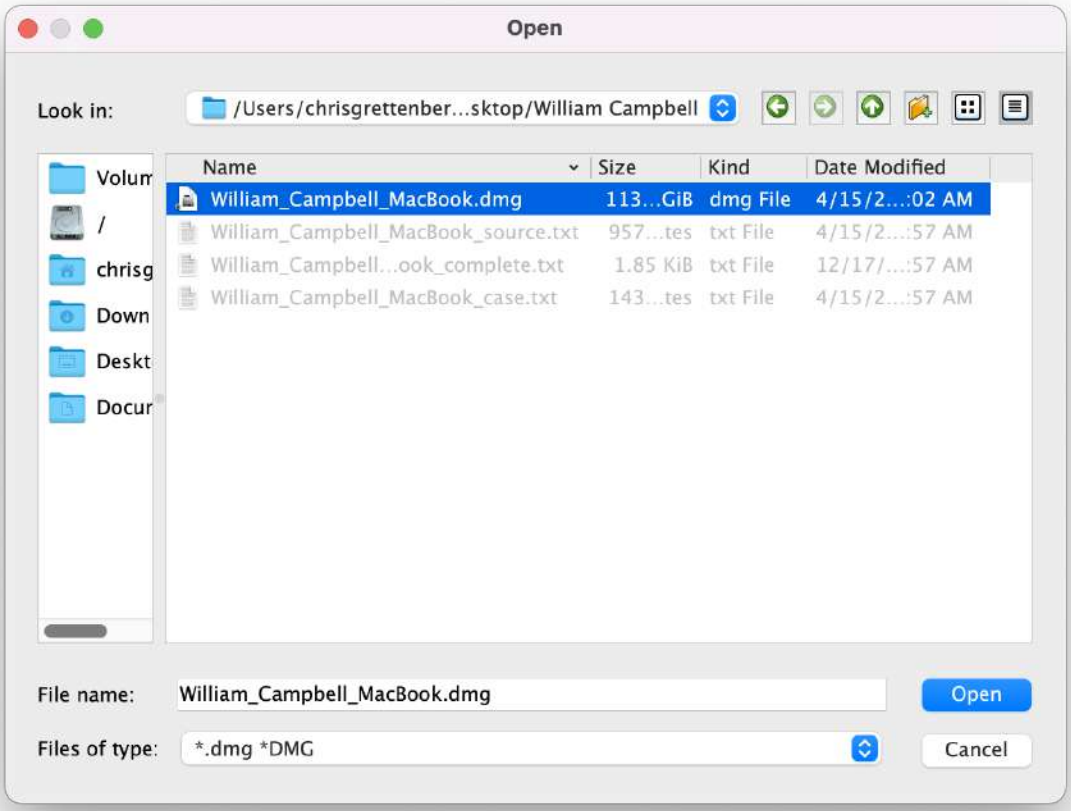
To select an FS Block Copy image created with RECON ITR, select the RECON FS Block Image icon in the Physical Evidence ‘Select Image Type’ menu.

Once selected, RECON LAB will display the available image formats for a RECON FS Block Image. Choose either sparseimage or DMG depending on what format your image is in.



From here, select the '...' icon on the right side to open a File Browser window. This will allow you to navigate to your stored image file.

Select your image and click 'Open' to continue.



Select ‘Add’ to add the RECON FS Block Image to your case for processing.

10.2.2 Logical Evidence

RECON LAB supports multiple kinds of logical acquisitions. It is particularly important to select the correct option when dealing with logical acquisitions. Some features present features that are important when using RECON LAB and RECON ITR together may not function properly if a source

is not loaded properly.

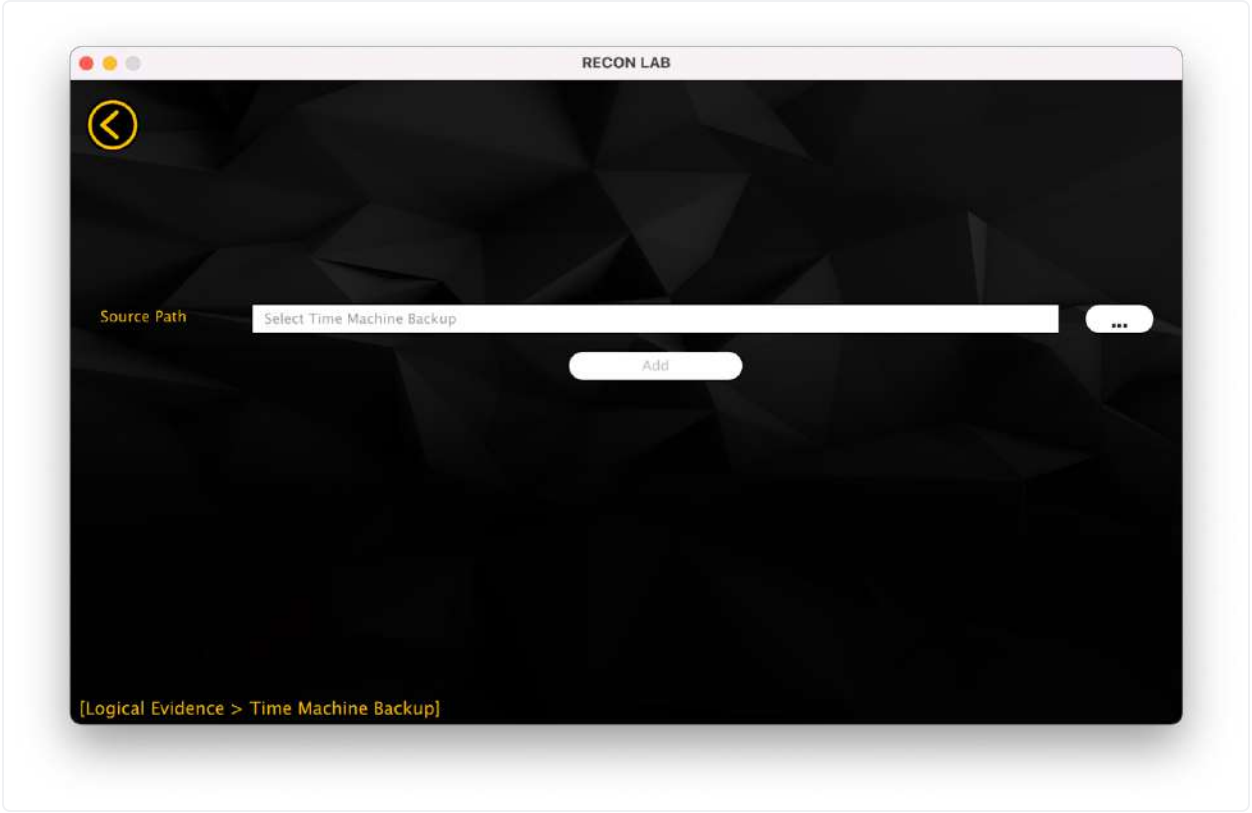
To begin loading logical evidence into your case, select the Logical Evidence icon from the Evidence Type selection.

From the ‘Select Image Type’ menu, you can select the type of logical evidence you’d like to ingest.

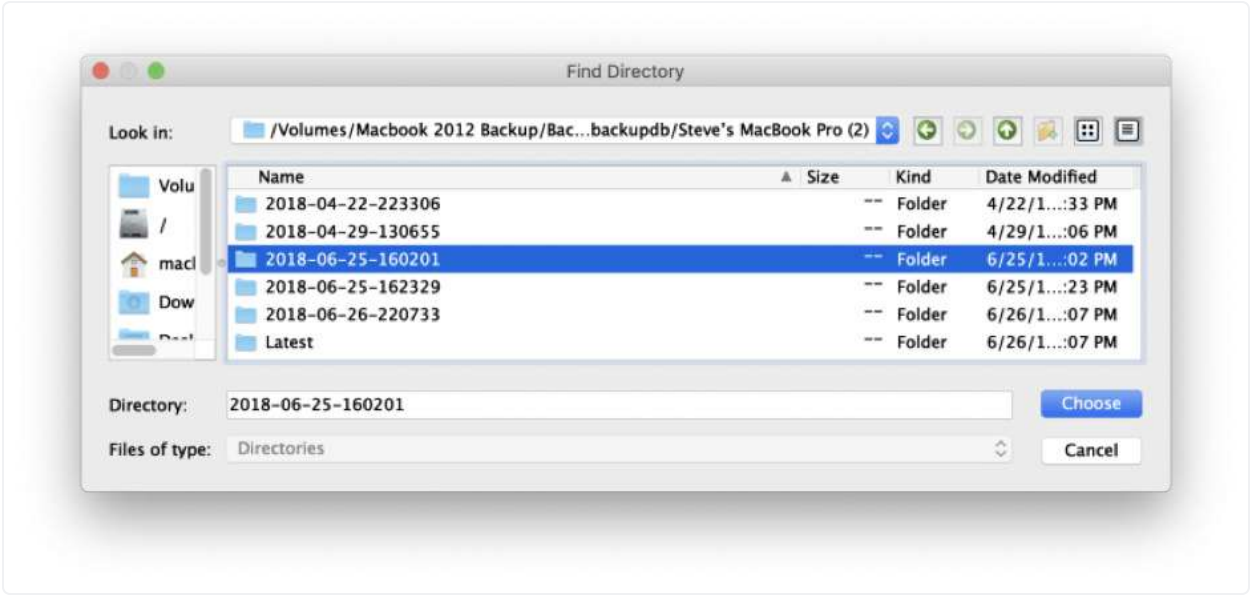
10.2.2.1 Time Machine Backup

RECON LAB supports the processing and automated analysis of individual macOS Time Machine Backups.

To begin adding your Time Machine Backups to your case, select the Time Machine Backup icon from the Logical Evidence ‘Image Type’ Menu.



Select the '...' icon and navigate to the directory of the backup in which you would like to process. Select "Choose" to add the backup directory.

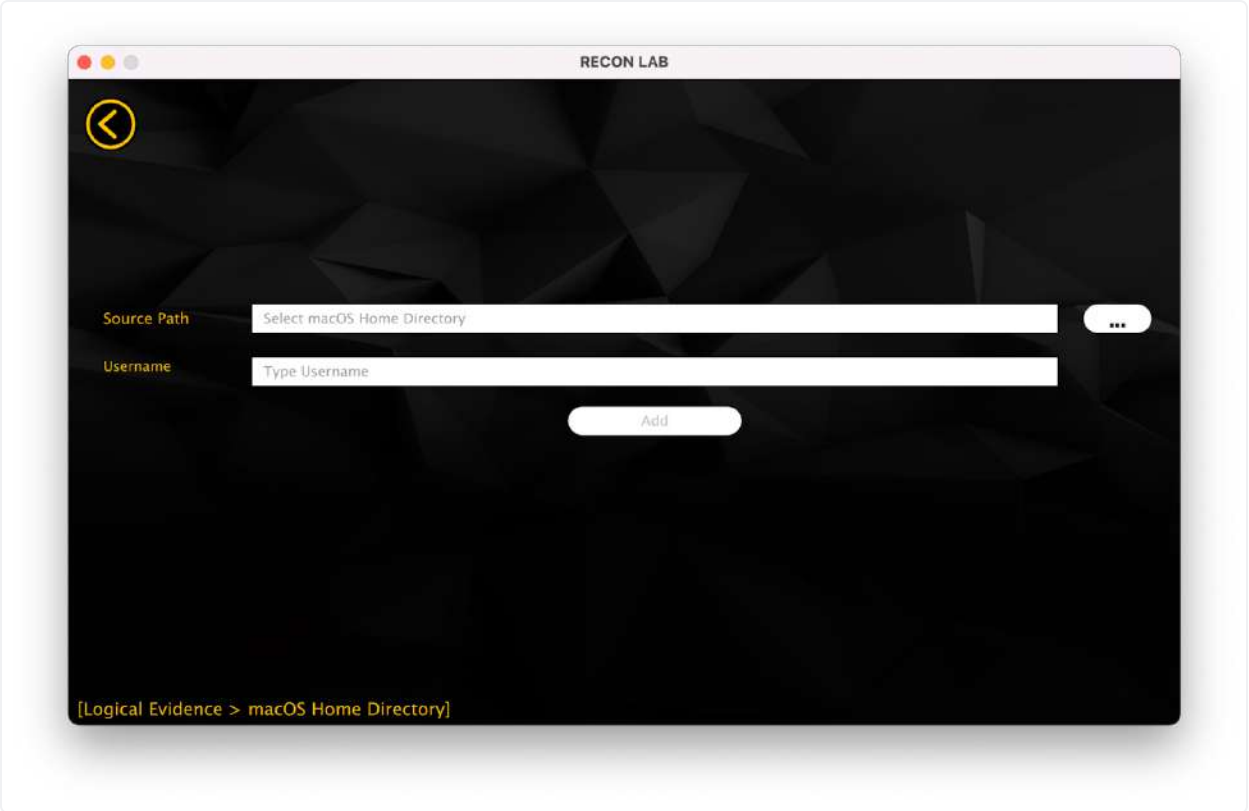


Select 'Add' to add the Time Machine Backup to your case for processing.

10.2.2.2 macOS Home Directory

There are many situations in Mac investigations where only a single user's home directory can be acquired. RECON LAB supports adding and automatically processing a macOS Home Directory.

To begin loading a macOS Home Directory to your case, select the ‘macOS Home Directory’ icon from the Logical Evidence ‘Select Image Type Menu’.



Next, select the ‘...’ icon and navigate to the home directory you’d like to add. Select Choose to continue.

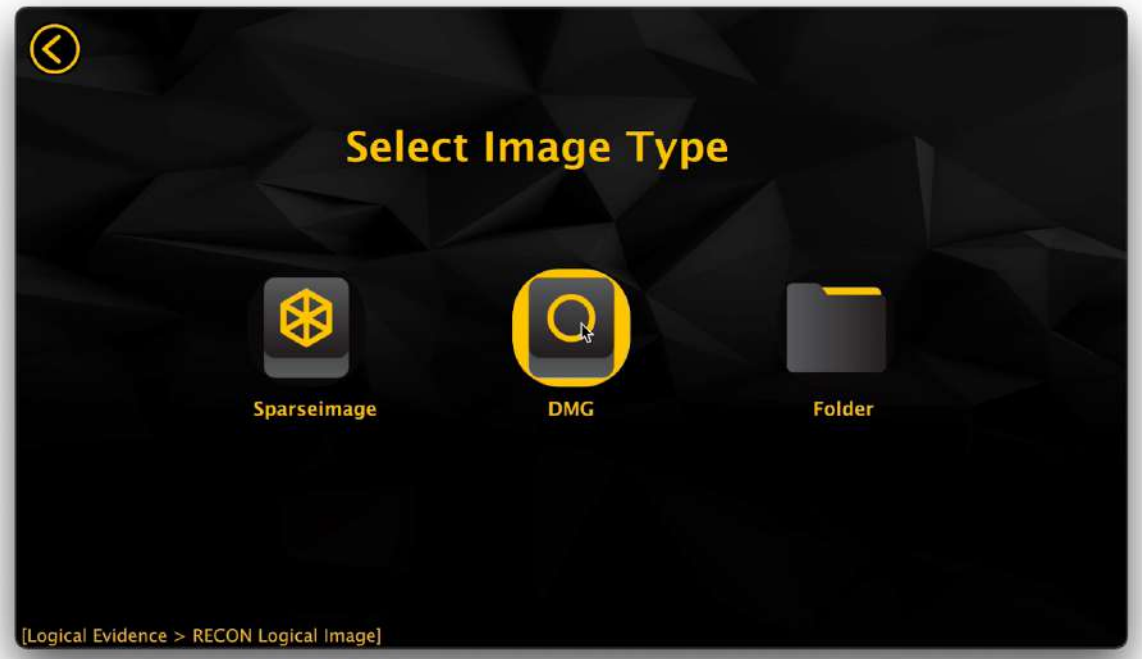
Enter the username of the home directory and select ‘Add’ to the home directory for processing.

10.2.2.3 RECON Logical Image

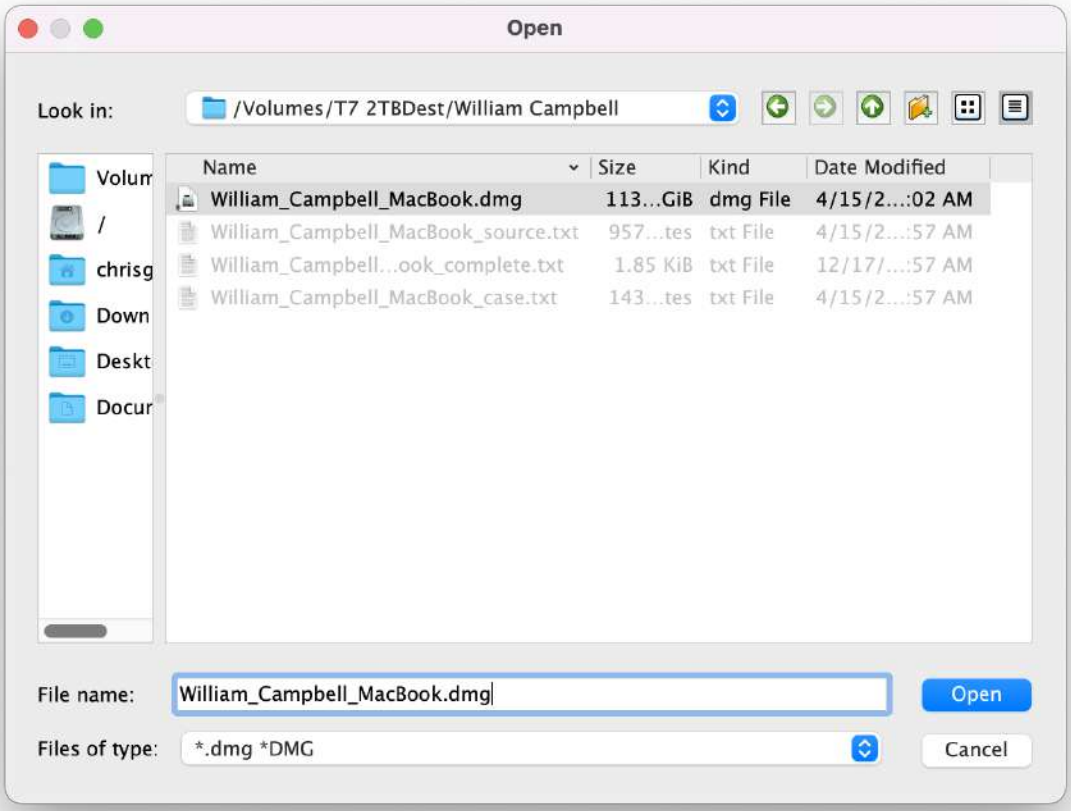
A RECON Logical image is any logical image that was taken with RECON ITR. There are three supported file formats for RECON Logical images, Sparseimage, DMG, and Folder. A RECON Logical image will utilize a database made at the time of imaging to display the correct Modify, Access and Create Date and Time stamps of a logical image. This database is create any time RECON ITR makes a logical image.

To load a RECON Logical image, navigate to the RECON Logical Image icon in the Logical Evidence 'Select Image Type' Menu.

Next, choose the type of RECON Logical Image you'd like to load. Select the icon that matches the format of the image you have.



Select the '...' icon to browse to your image location and select 'Open'.



Select ‘Add’ to add the RECON Logical Image to your case for processing.

10.2.2.4 Encase Logical Image

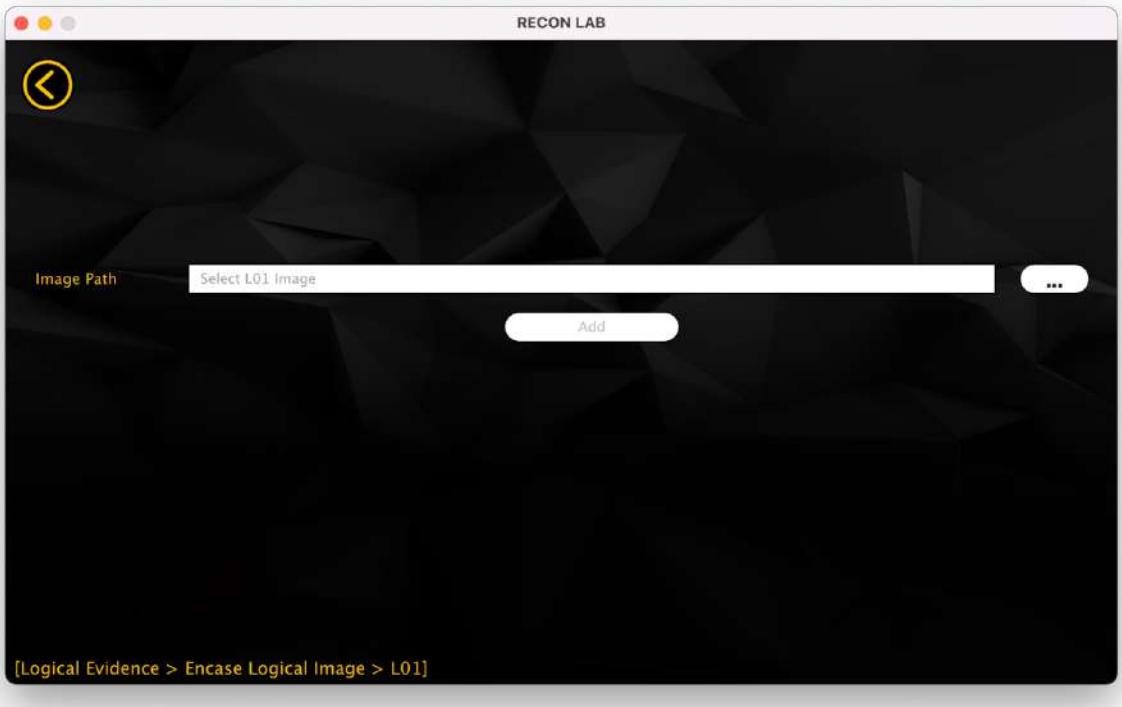
Access Data has its own proprietary logical container format, popularly known as L01.

RECON LAB has support for ingesting these containers using the Logical Evidence section.

To load your L01 in RECON LAB, navigate to the ‘Encase Logical Image’ icon in the Logical Evidence ‘Select Image Type’ Menu.

Select the L01 Icon.

Select the '...' icon to browse to your image file and click 'Open' to continue.

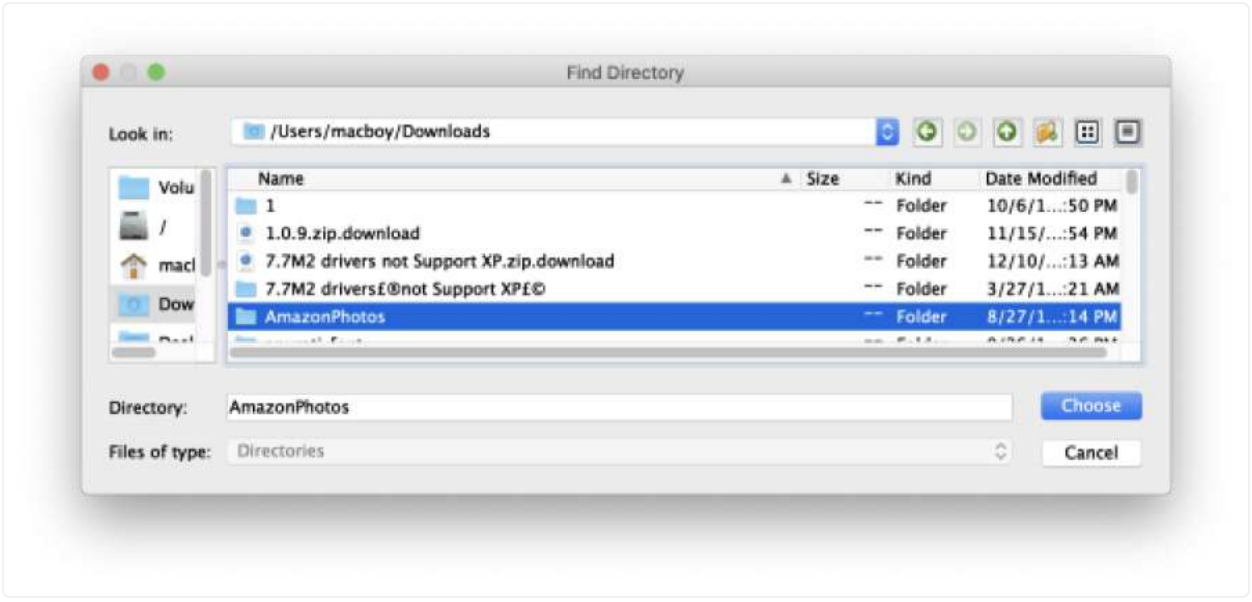


Select 'Add' to add the L01 to your case for processing.

10.2.2.5 Logical Folder

Individual folders can be added as a source to process.

To add a folder as a source, navigate to the Folder icon in the Logical Evidence ‘Select Image Type’ menu.



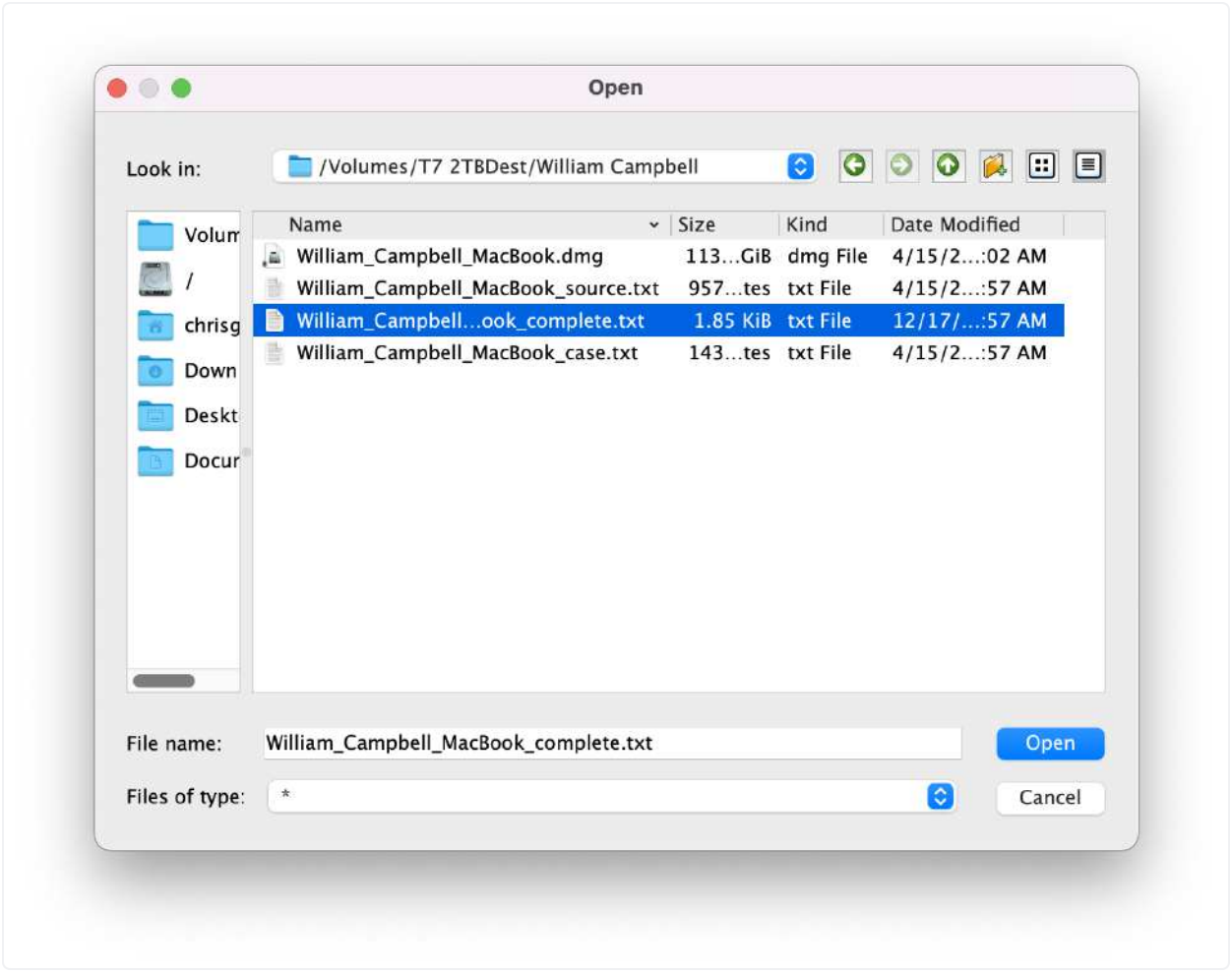
Click the ‘...’ icon to browse to the folder you’d like to add and select ‘Open’.

Select ‘Add’ to add the Folder to your case for processing.

10.2.2.6 Logical File

Individual files can be added as a source to process.

To add a file as a source, navigate to the File icon in the Logical Evidence ‘Select Image Type’ menu.

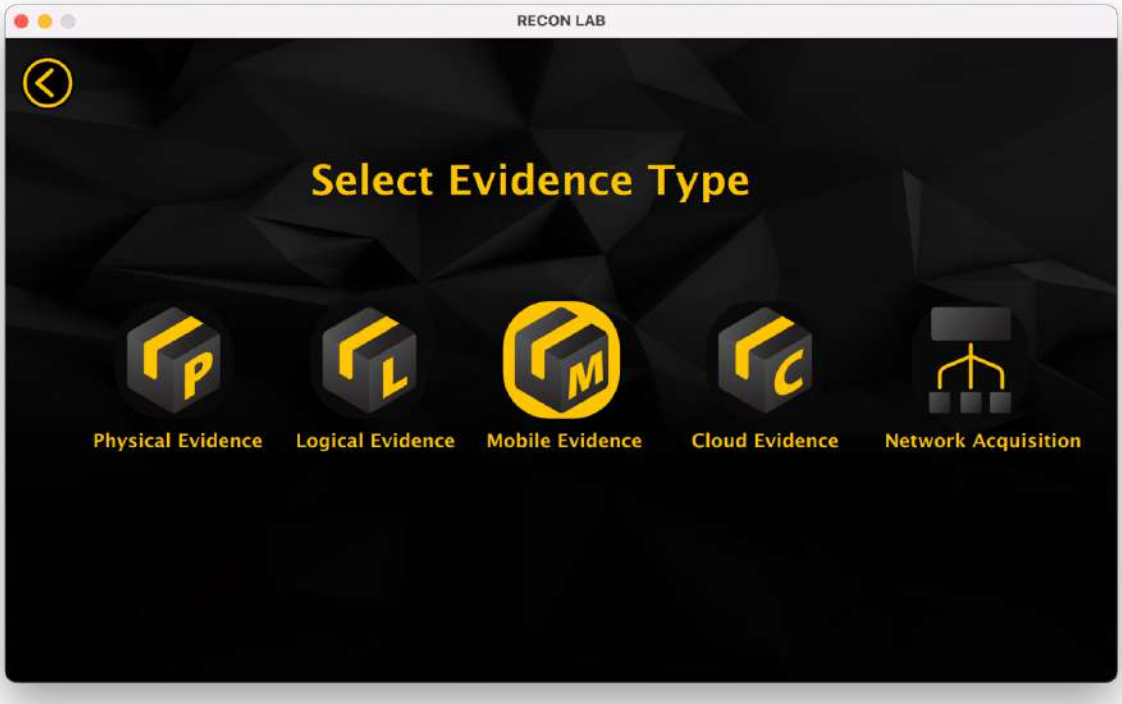


Click the '...' icon to browse to the folder you'd like to add and select 'Open'.

Select 'Add' to add the File to your case for processing.

10.2.3 Mobile Evidence

RECON LAB has support for processing multiple forms of iOS and Android sources, that can all be accessed through the Mobile Evidence section, including support for both Cellebrite iOS backups and ADB Backups.



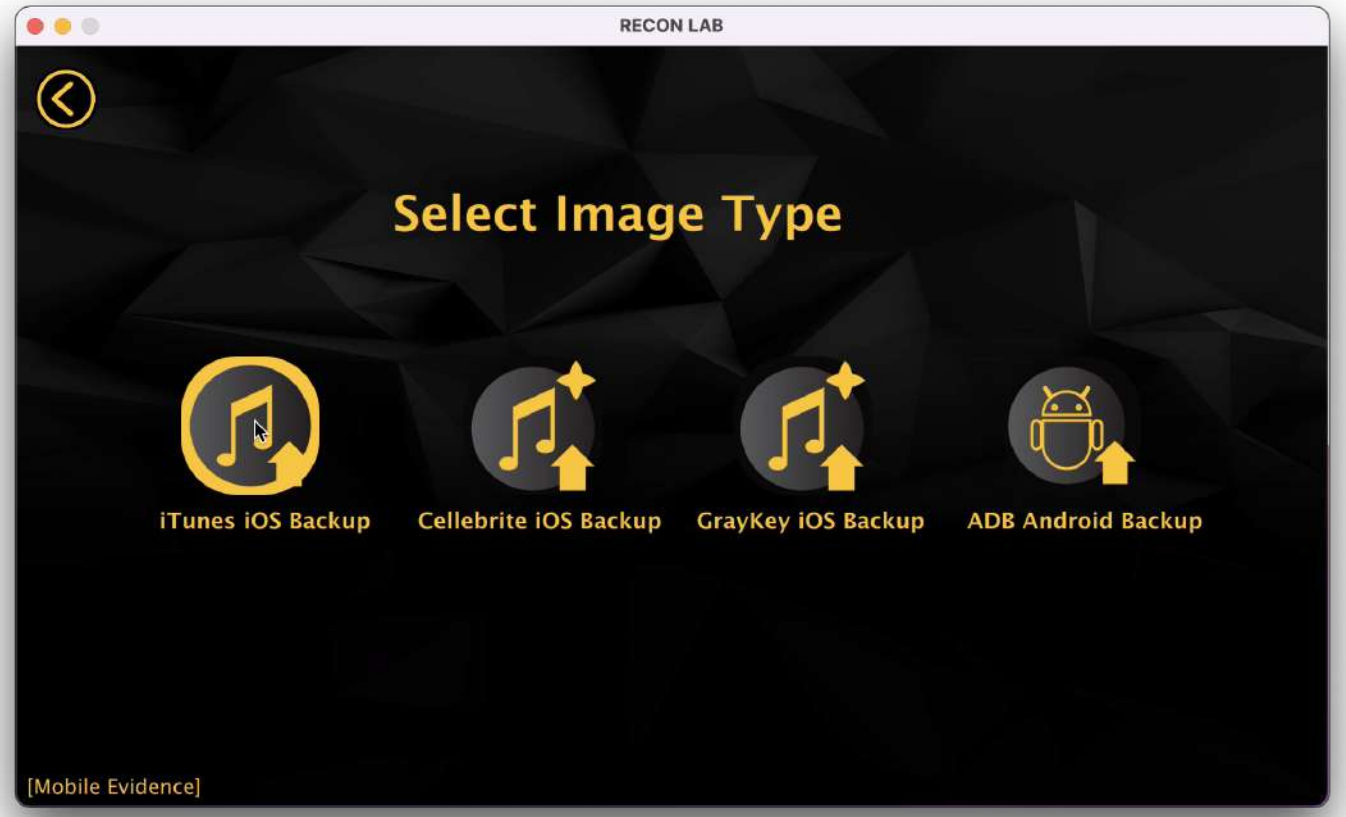
To begin loading Mobile Evidence into RECON LAB, select the Mobile Evidence icon from the 'Select Evidence Type' Window.

10.2.3.1 iTunes iOS Backup

RECON LAB supports the analysis of Apple iOS backups.

Most forensic tools that image iOS devices utilize the iTunes engine to create an iTunes backup to process.

RECON LAB also has the ability to image and iOS device and create an iOS backup which is discussed later in this manual.



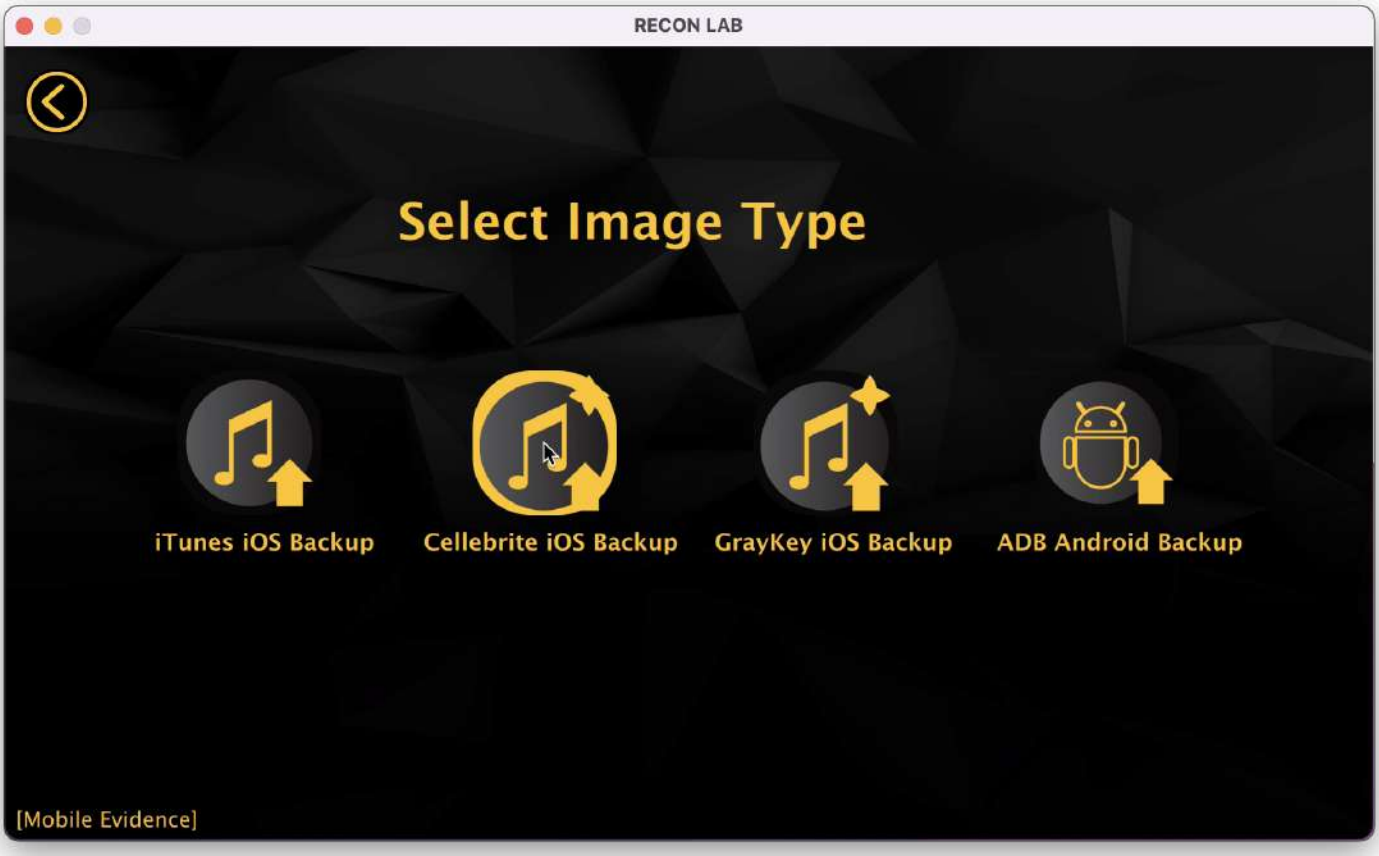
To add an iOS backup as a source navigate to the ‘iTunes iOS Backup’ icon from the Mobile Evidence ‘Select Image Type’ Menu.

Select the ‘...’ icon to browse to the manifest.db file inside the iTunes iOS Backup and select ‘Open’.

Select ‘Add’ to add the backup to your case for processing.

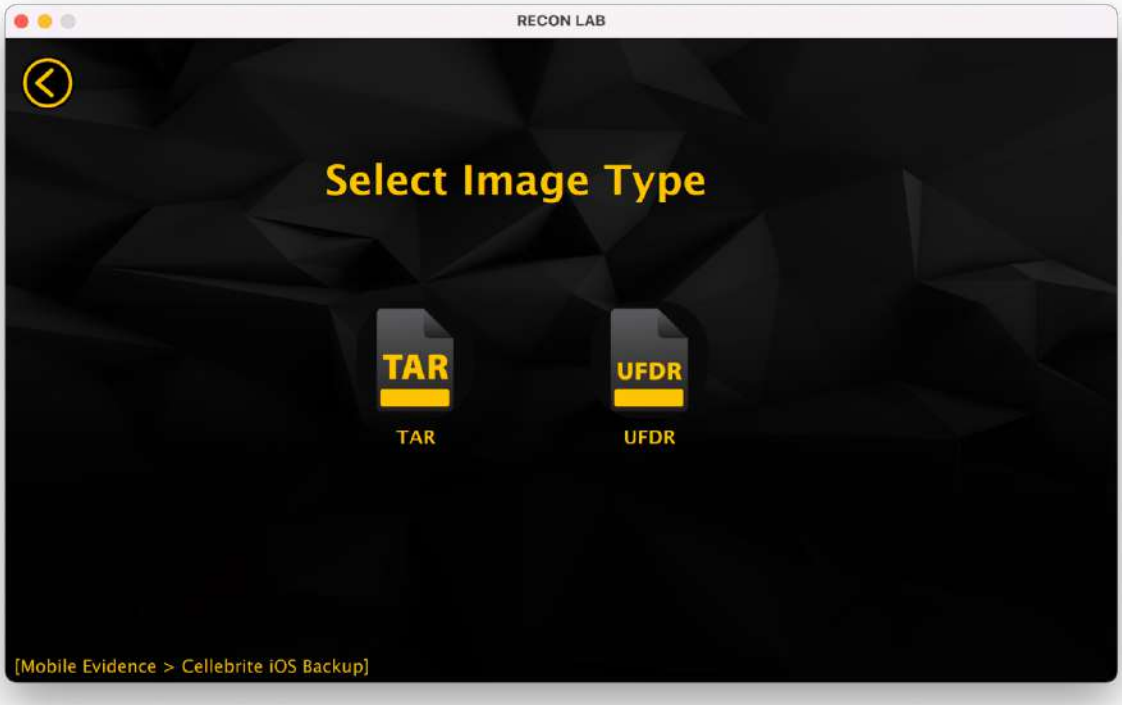
10.2.3.2 Cellebrite iOS Backup

RECON LAB supports ingesting of Cellebrite UFED extractions in the form of unencrypted .tar and UFDR.



To add an iOS backup as a source navigate to the ‘Cellebrite iOS Backup’ icon from the Mobile Evidence ‘Select Image Type’ Menu.

Select the evidence type that you’d like to ingest, either an unencrypted .tar backup or a UFDR folder.

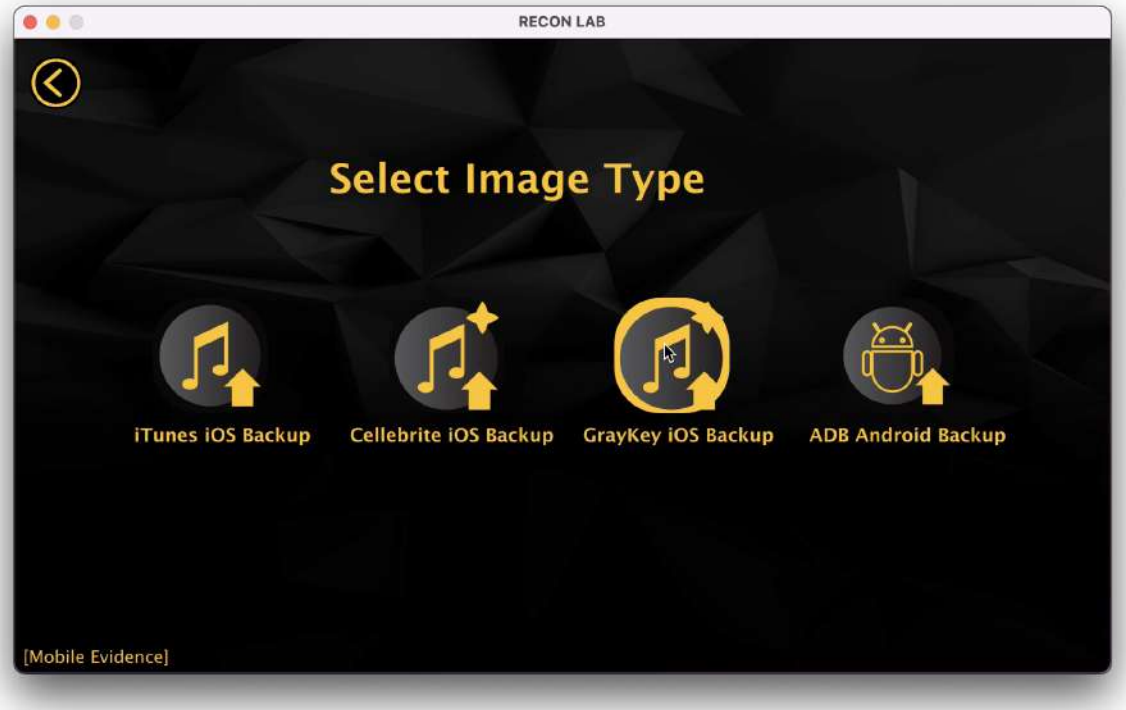


Select the '...' icon to browse to the image file and select 'Open'.

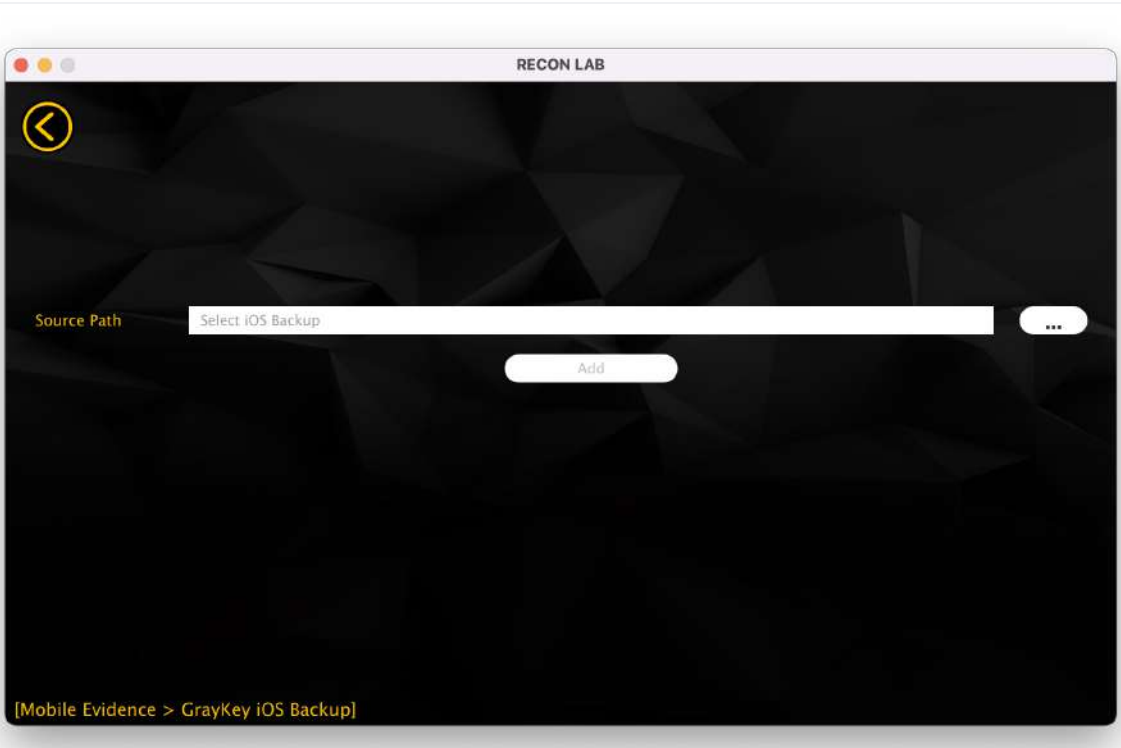
Select 'Add' to add the backup to your case for processing.

10.2.3.3 GrayKey Backup

RECON LAB supports ingesting of GrayKey images in the form of .zip files.



To add an iOS backup as a source navigate to the ‘GrayKey iOS Backup’ icon from the Mobile Evidence ‘Select Image Type’ Menu.

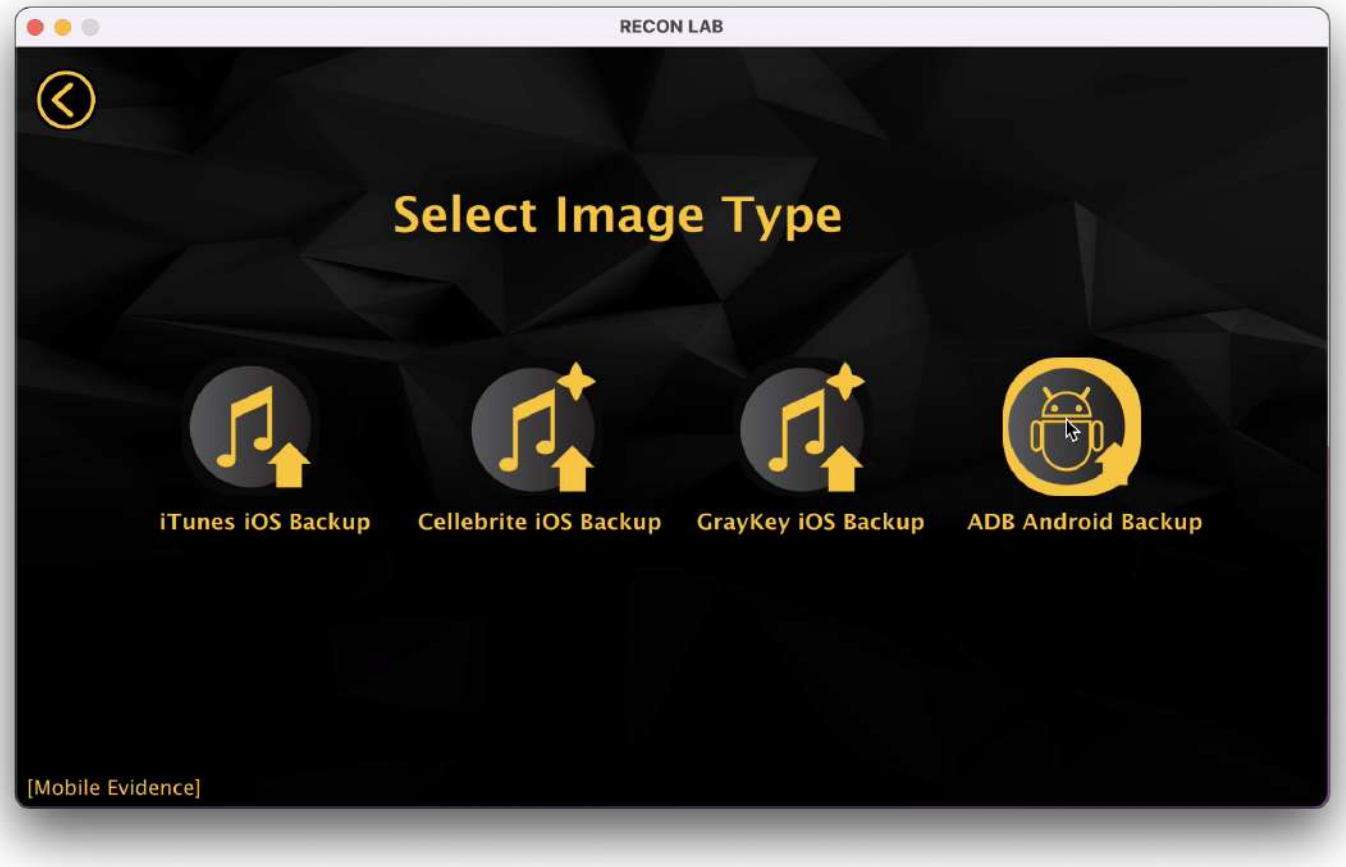


Select the ‘...’ icon to browse to the file and select ‘Open’.

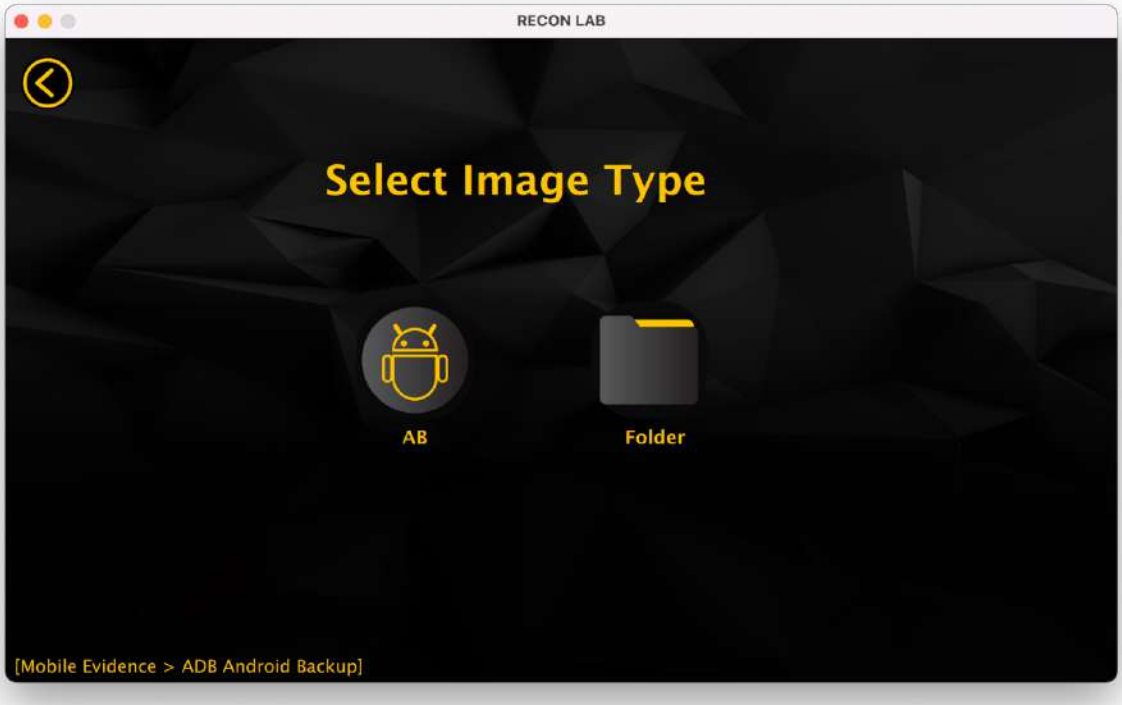
Select ‘Add’ to add the backup to your case for processing.

10.2.3.4 ADB Android Backup

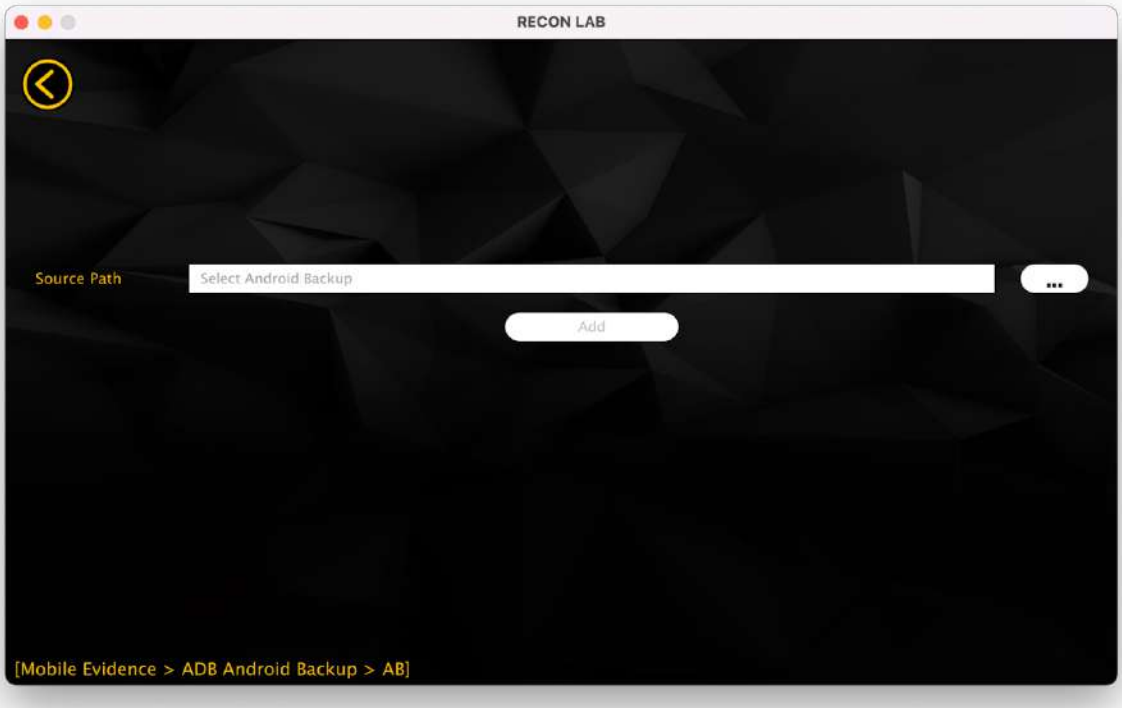
RECON LAB supports processing Android Debug Bridge (ADB) files and backups of Android Devices.



To add an ADB Backup as a source navigate to the ‘ADB Android Backup’ icon from the Mobile Evidence ‘Select Image Type’ Menu.



Select the type of backup you have, either an AB backup or a folder.



Select the '...' icon to browse to the file and select 'Open'.

Select ‘Add’ to add the backup to your case for processing.

10.2.4 Cloud Evidence

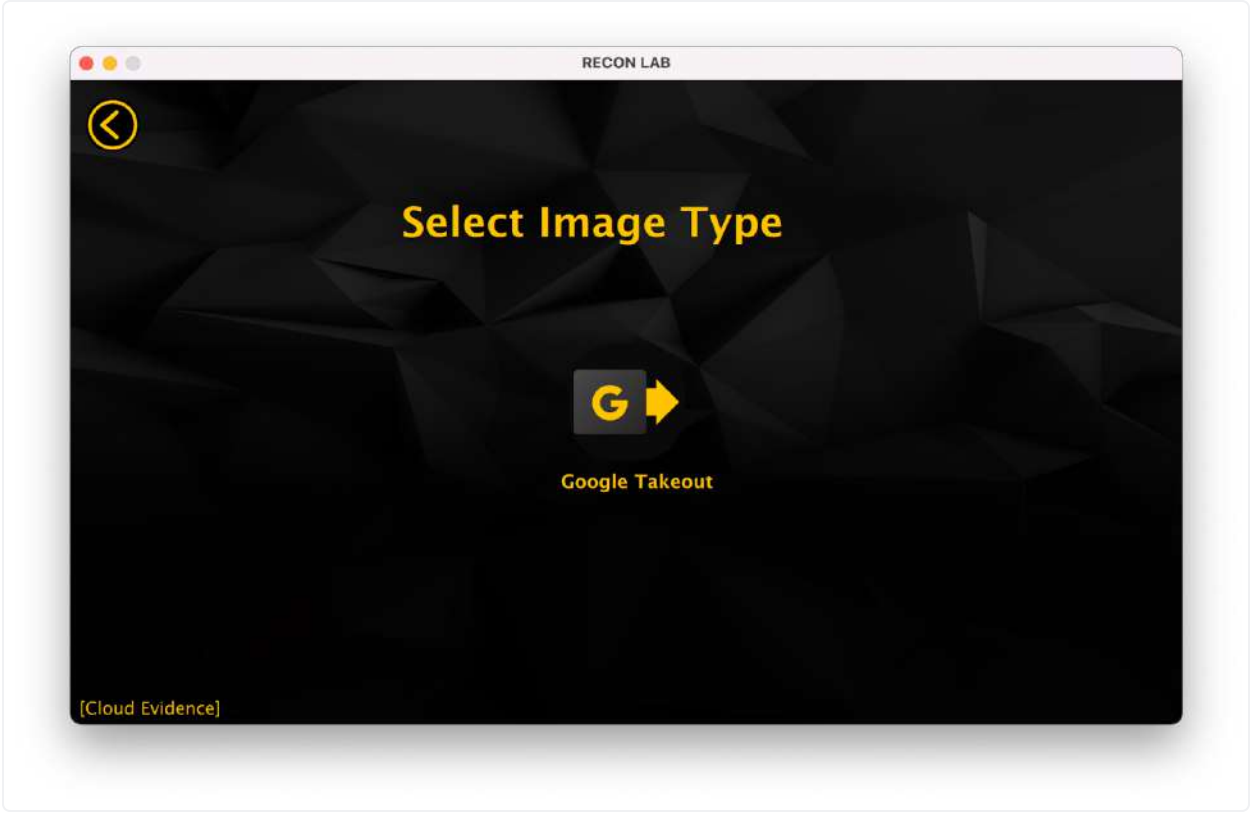
RECON LAB supports ingesting evidence related to cloud storage as well. The currently supported format is Google Takeout downloads. These can be added and parsed with RECON LAB by following the section below.

To begin processing Cloud Evidence, select the ‘Cloud Evidence’ Icon from the ‘Select Evidence Type’ Menu.

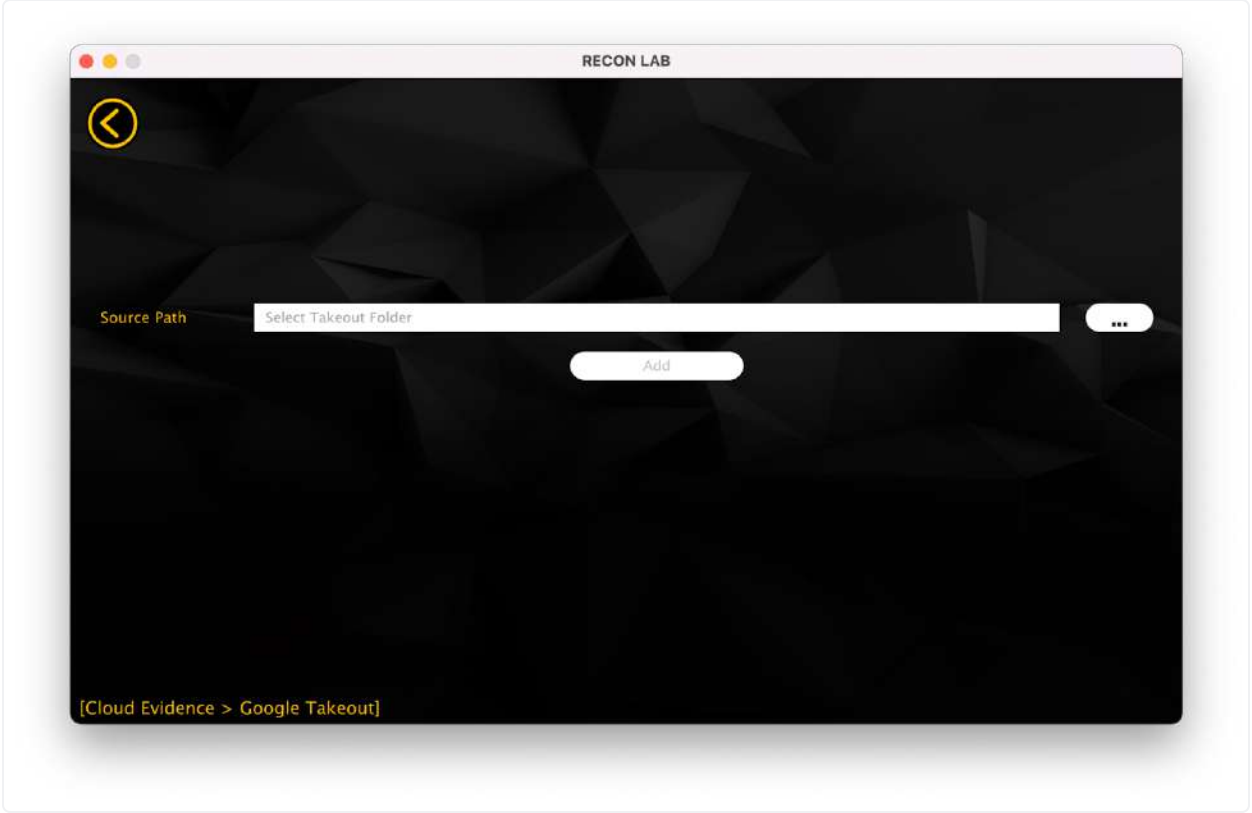
10.2.4.1 Google Takeout

RECON LAB supports data downloaded from Google Takeout: https://takeout.google.com

RECON LAB has numerous plugins to automate the analysis of Google Takeout data.



To load data from Google Takeout select the Google Takeout option from the ‘Select Image Type’ Menu.

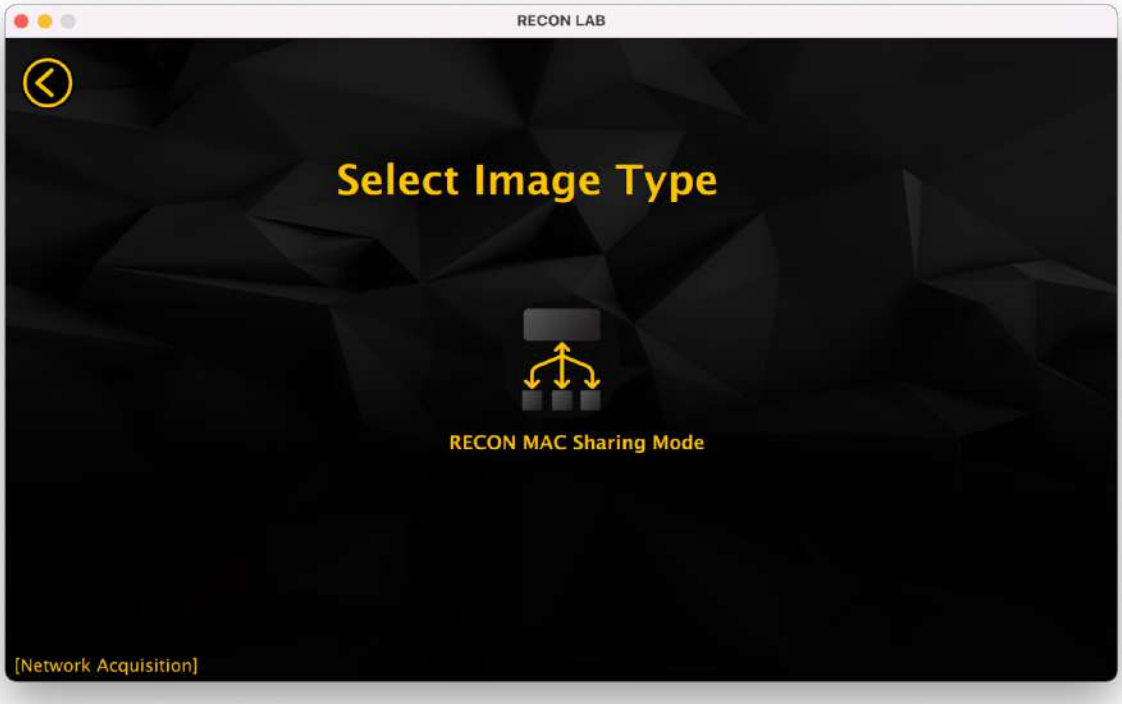


Then, select the '...' option and navigate to the directory with the Google Takeout data. Then, select 'Open' to continue.

Select 'Add' to add the Google Takeout to your case for processing.

10.2.5 Network Acquisition

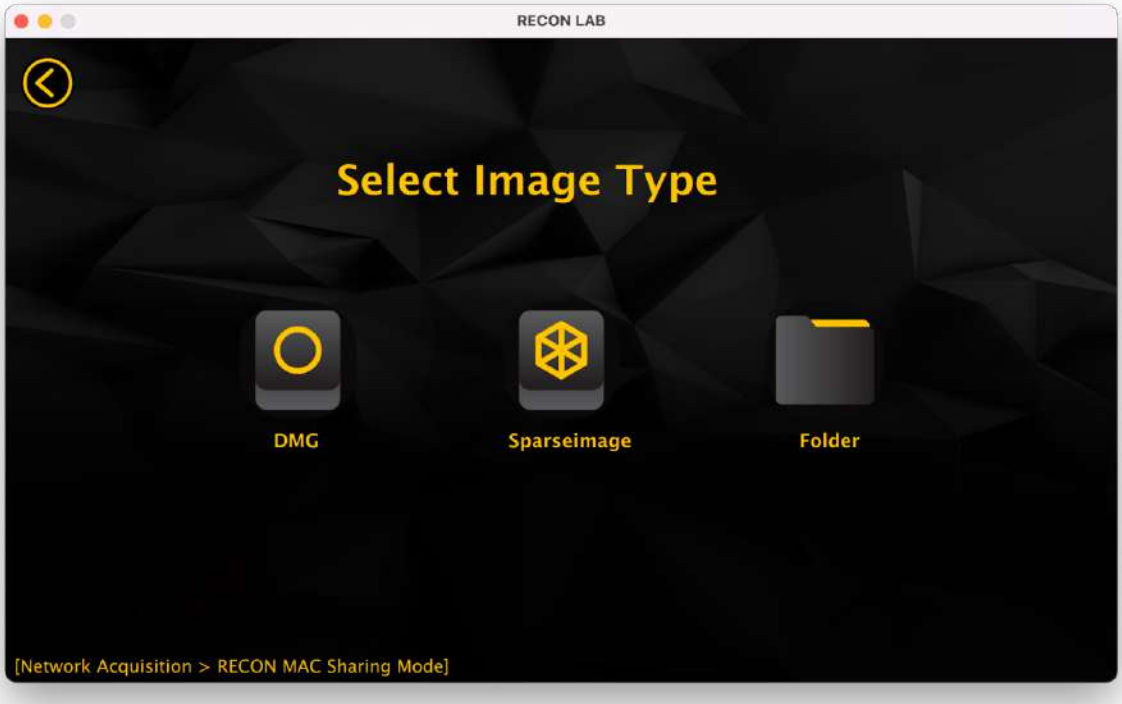
Network Acquisition refers to acquisitions performed over a connection like SMB. RECON LAB currently supports one type of Network Acquisition, RECON MAC Sharing Mode.



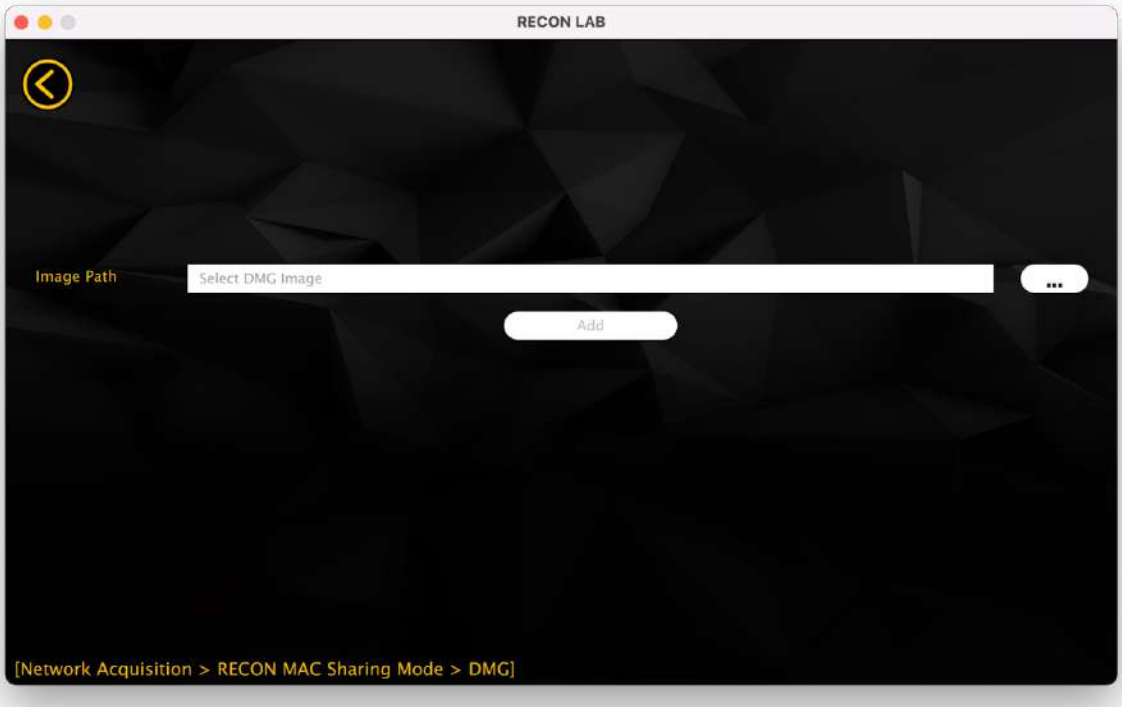
10.2.5.1 RECON Mac Sharing Mode

RECON ITR supports imaging the new M1 , M2, M3, and M4 Macs using Apple's new Sharing Mode. This method of imaging is run over an SMB connection, so the image is created differently than your conventional synthesized disk image.

To begin adding your Sharing Mode image, select the RECON Mac Sharing Mode icon and select the format of your image.



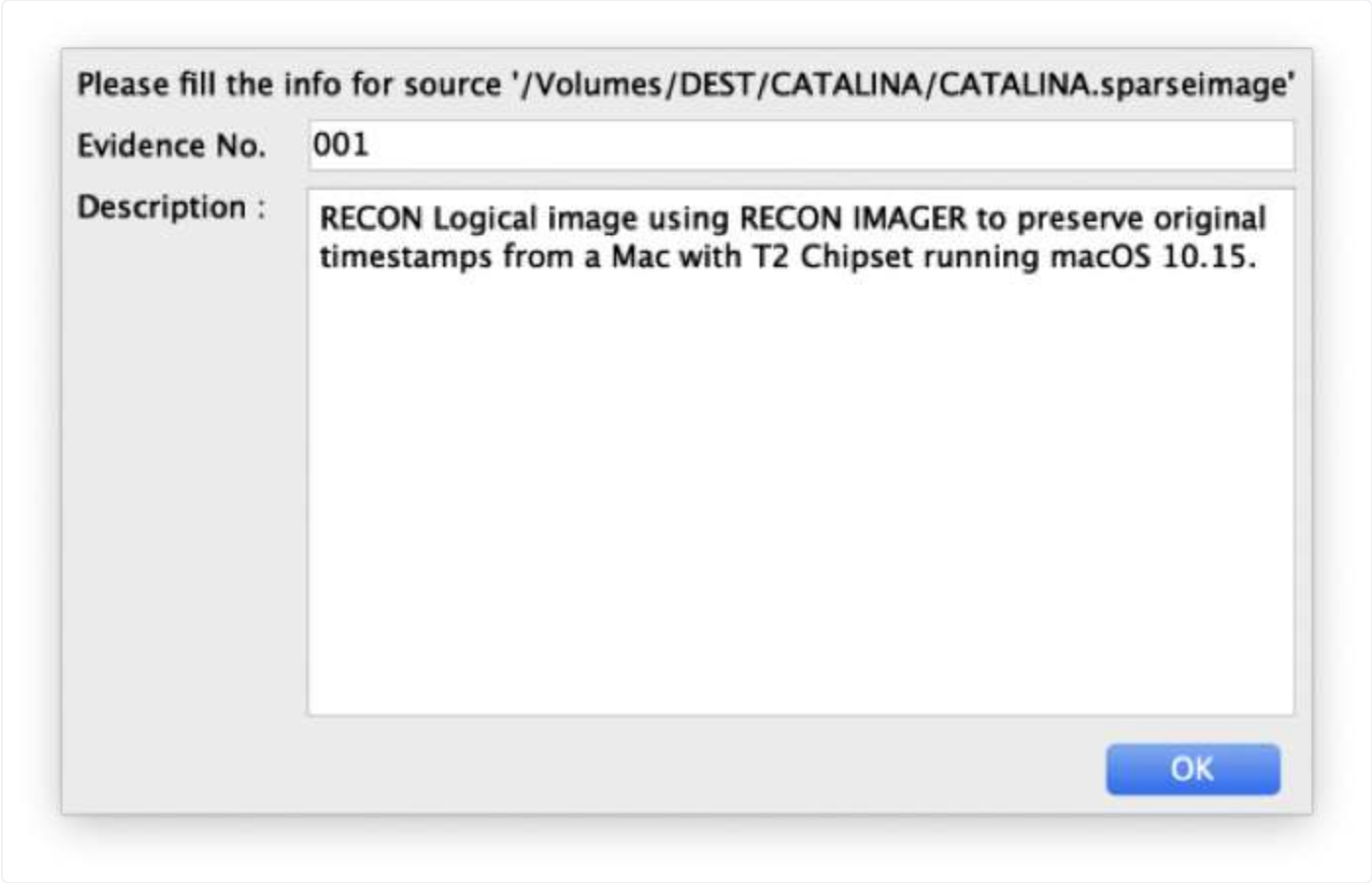
Next, select the '...' option and navigate to the image. Then, select 'Open' to continue.



Select 'Add' to add the Sharing Mode image to your case for processing.

10.3 Adding Source Information

Once a Source has been selected the Source Information window will appear.

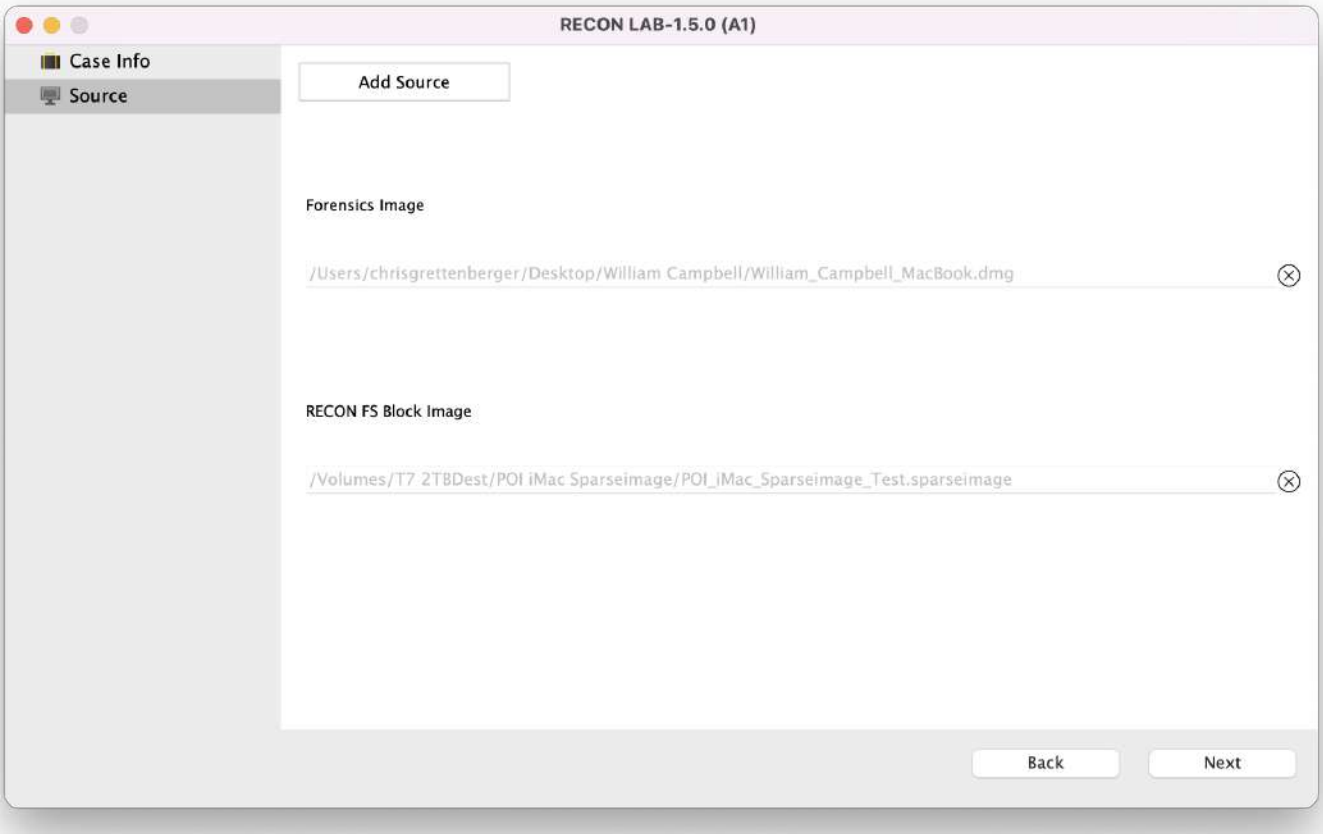


Here you can add a unique evidence number (“Evidence No.”) and a description of the evidence.

After entering the information click “Ok”.

10.4 Adding Multiple Sources

RECON LAB can process multiple sources at the same time.

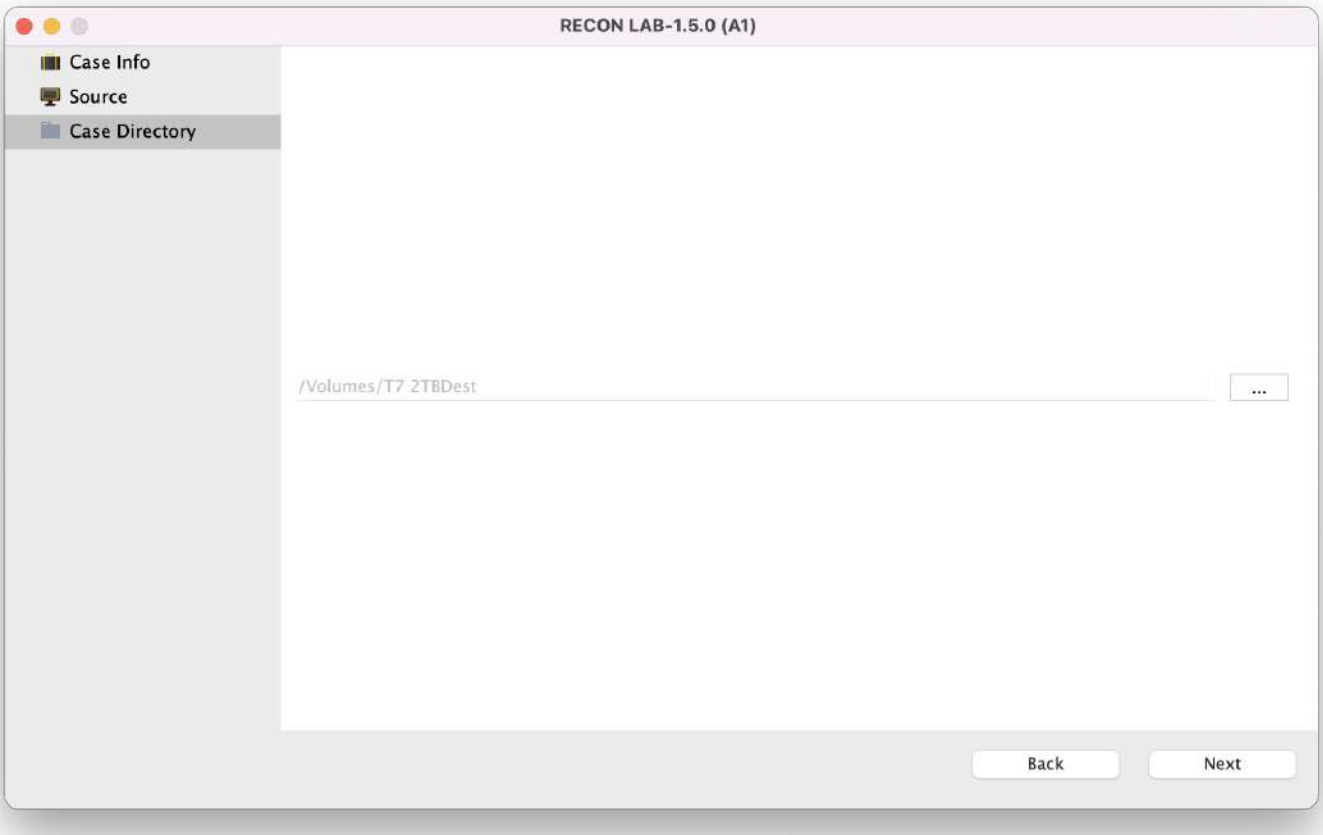


To add more than one source use the “Add Source” button. Additional sources will be listed once added. To remove a source before processing begins click the “X” button.

10.5 Case Directory

After adding your sources to process you have to select the location for your RECON LAB Case Directory. This directory is used to store everything and can become quite large in size depending on the amount of data to be processed. Make sure that there is enough space on the media where the Case Directory is placed.

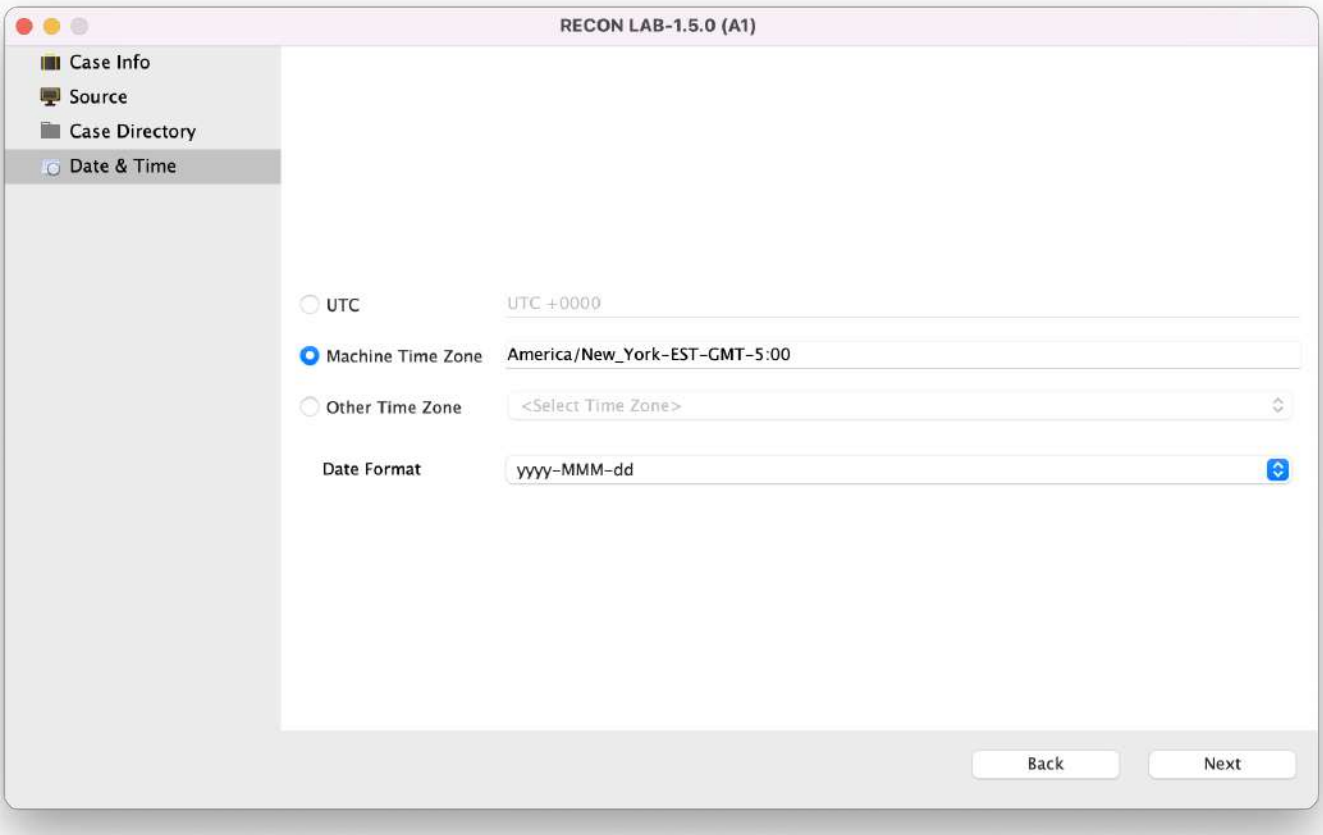
It is recommended to use a macOS Extended (HFS+) formatted drive for the location of the Case Directory.



To select the location for the Case Directory click the three dots. Navigate to the desired location and click “Choose”.

10.6 Date and Time Settings

RECON LAB has several options for setting time zones.



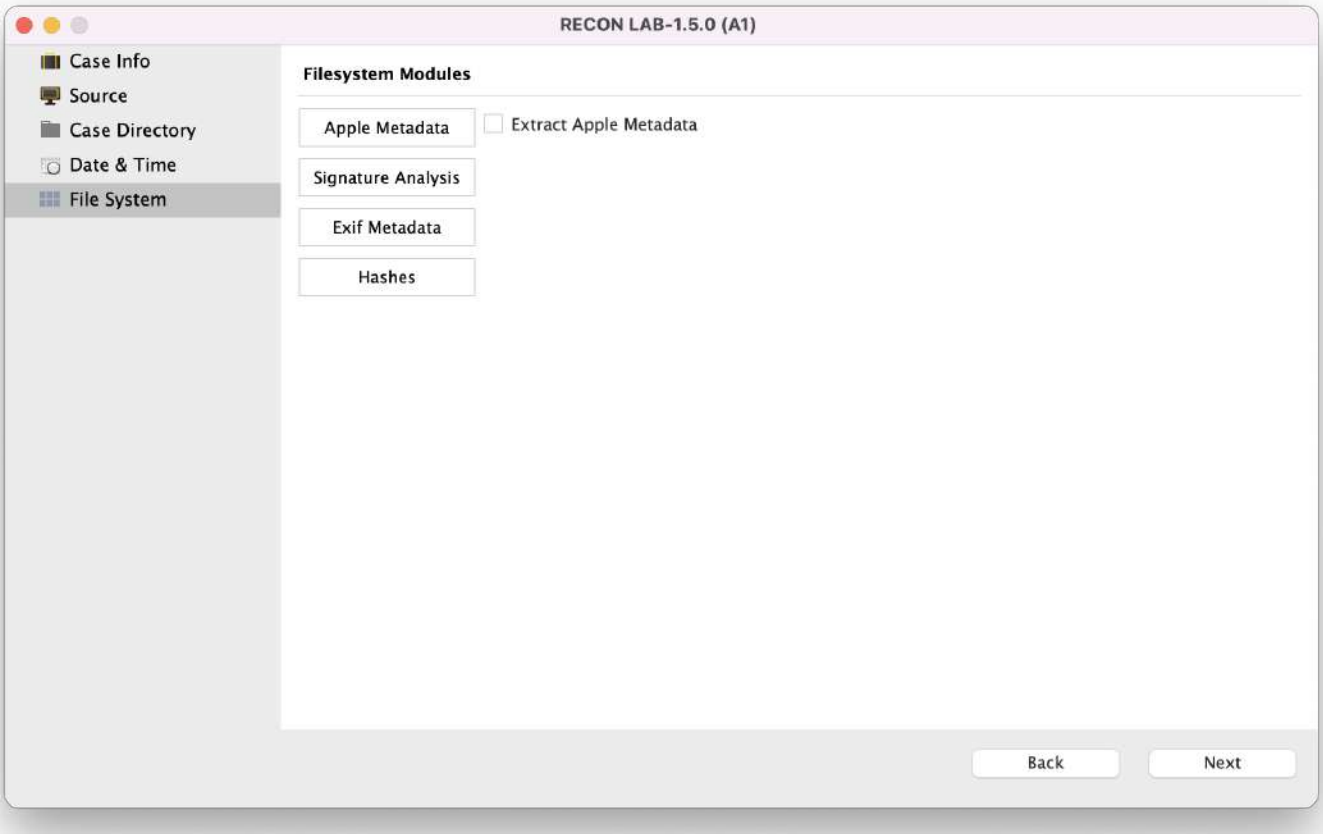
UTC – Coordinated Universal Time or +00:00

Machine Time Zone – This is the time zone of your examination system if detected.

Other Time Zone – This dropdown menu will allow you to pick any time zone in the world.

RECON LAB also has several options for the Date Format. Whatever Date Format is chosen here will take effect globally in RECON LAB.

10.7 File System Modules Selection

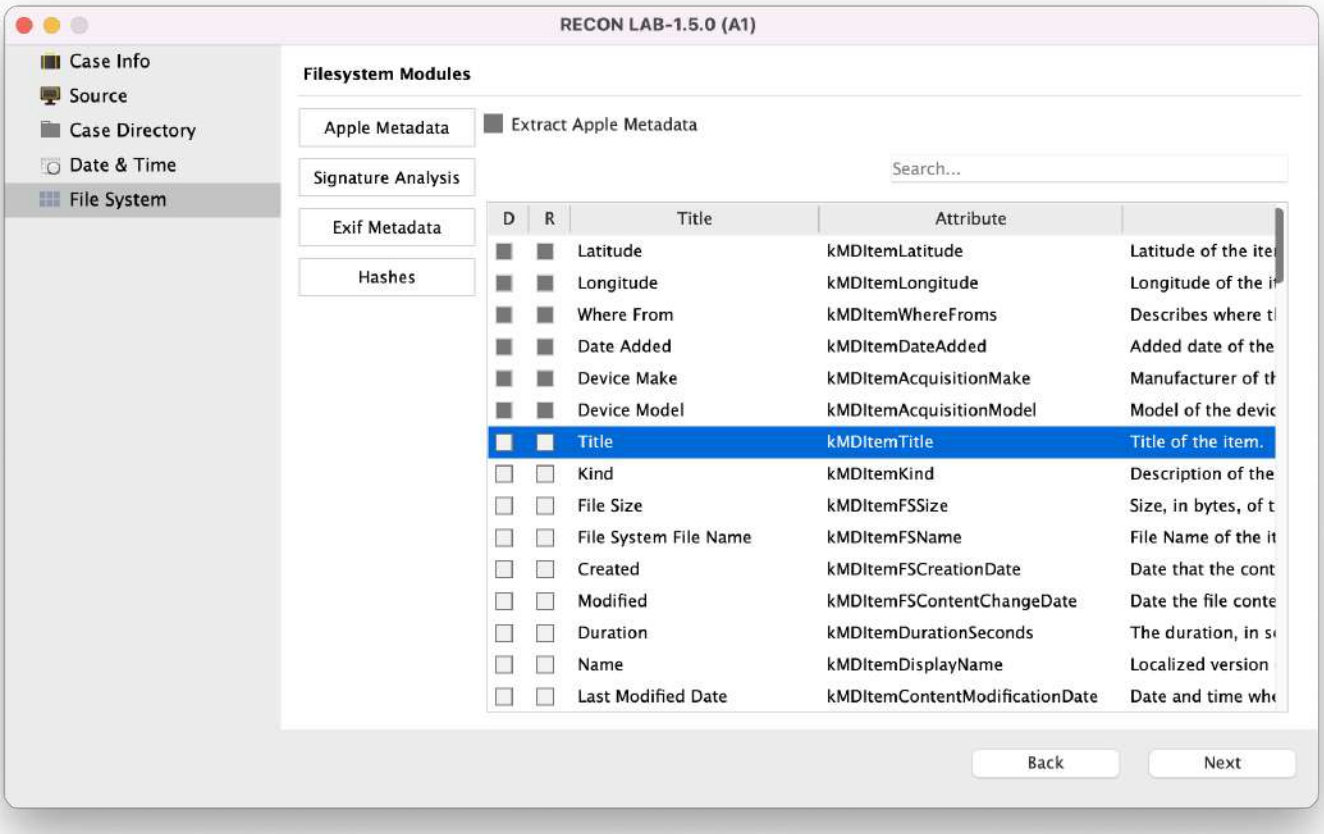


RECON LAB was designed to give an examiner as much control as possible. This control can help an examiner complete investigations and analysis faster.

The examiner has the option of enabling or disabling individual File System Modules.

For example, if your case does not require the need for signature analysis then you do not have to activate this module which will save processing time.

10.7.1 Apple Metadata Module



To activate the Apple Metadata module for macOS sources, check the box next to “Extract Apple Metadata”.

If you have previously configured this module your selections will be present. At this time you can add or remove attributes.

Apple Metadata Filter Column Descriptions

D – Check this box to add this Apple Extended Attribute to the RECON LAB Sidebar. Any files matching selected attributes will automatically be filtered and placed in the Sidebar.

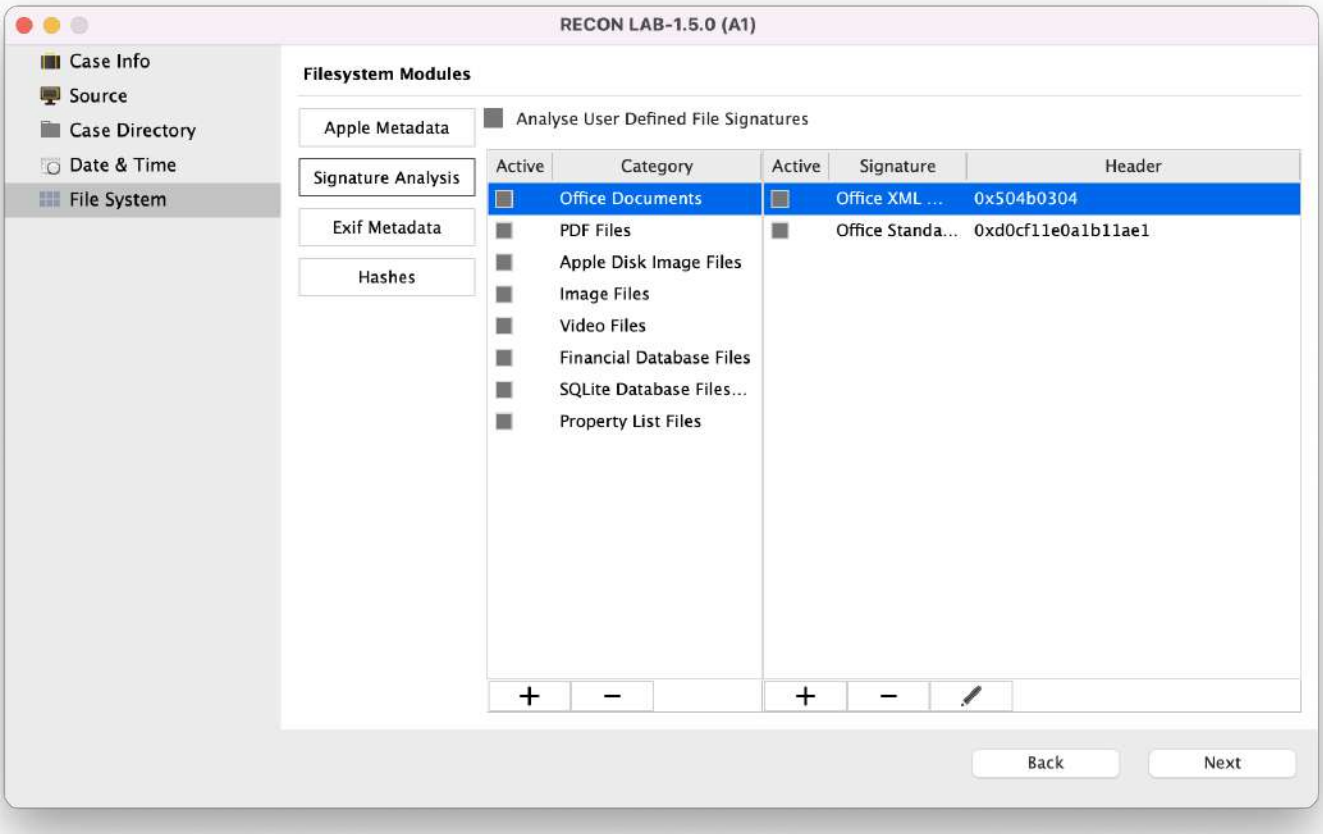
R – Checking this box will include the selected attribute’s metadata automatically to reports.

Title – The common name of the Apple Extended Attribute.

Attribute – The specific name of the Apple Extended Attribute.

Description – The official description of the Apple Extended Attribute.

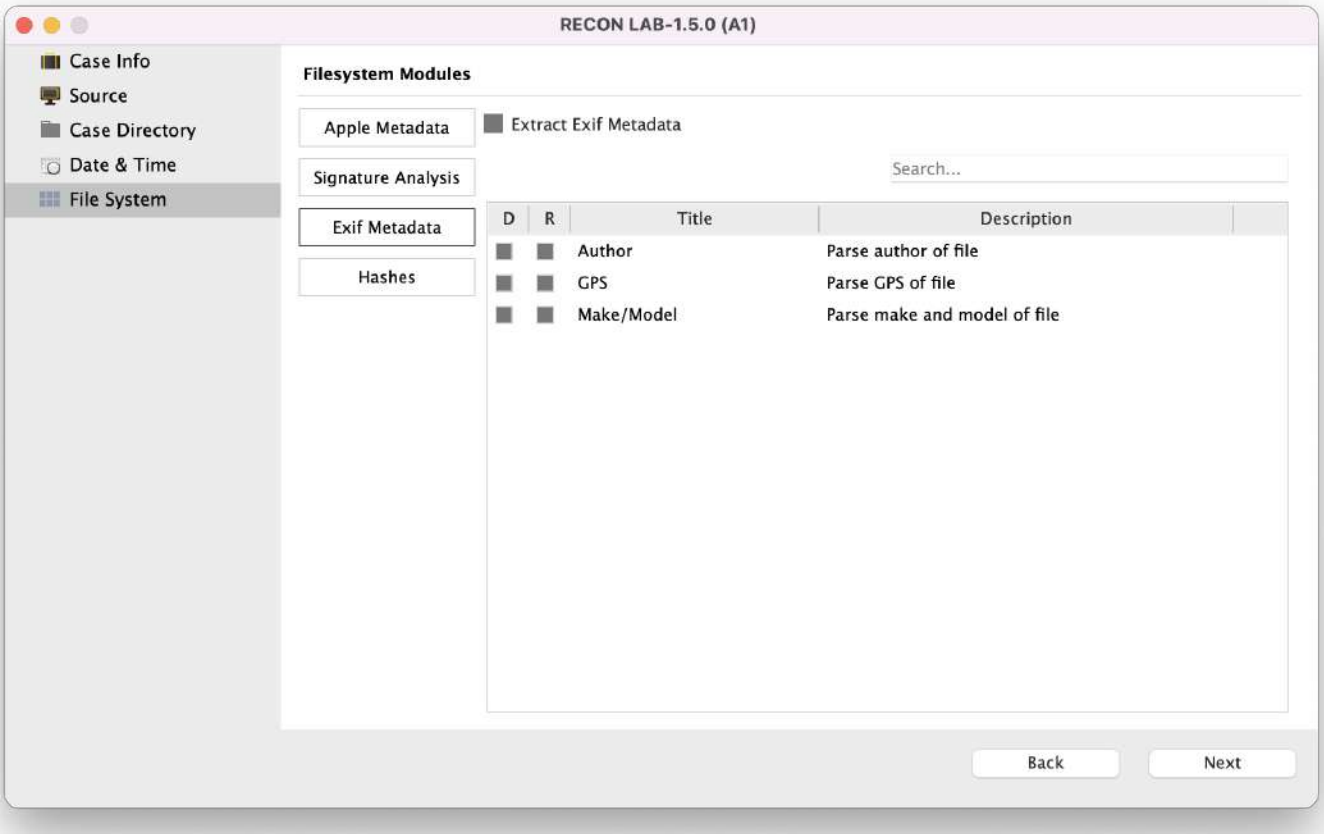
10.7.2 Signature Analysis Module



Selecting “Analyse User Defined File Signatures” run a module to identify files based on the file’s headers (or signature). The file signatures can be added in the Case Wizard or previously in RECON LAB Configuration.

To learn how to enter or remove a file signature please refer to the previous instruction in the “Configuration” section of this manual.

10.7.3 EXIF Metadata Module



Selecting “Extract Exif Metadata” tells RECON LAB to recover any EXIF metadata selected in this module.

EXIF Metadata Filter Column Descriptions

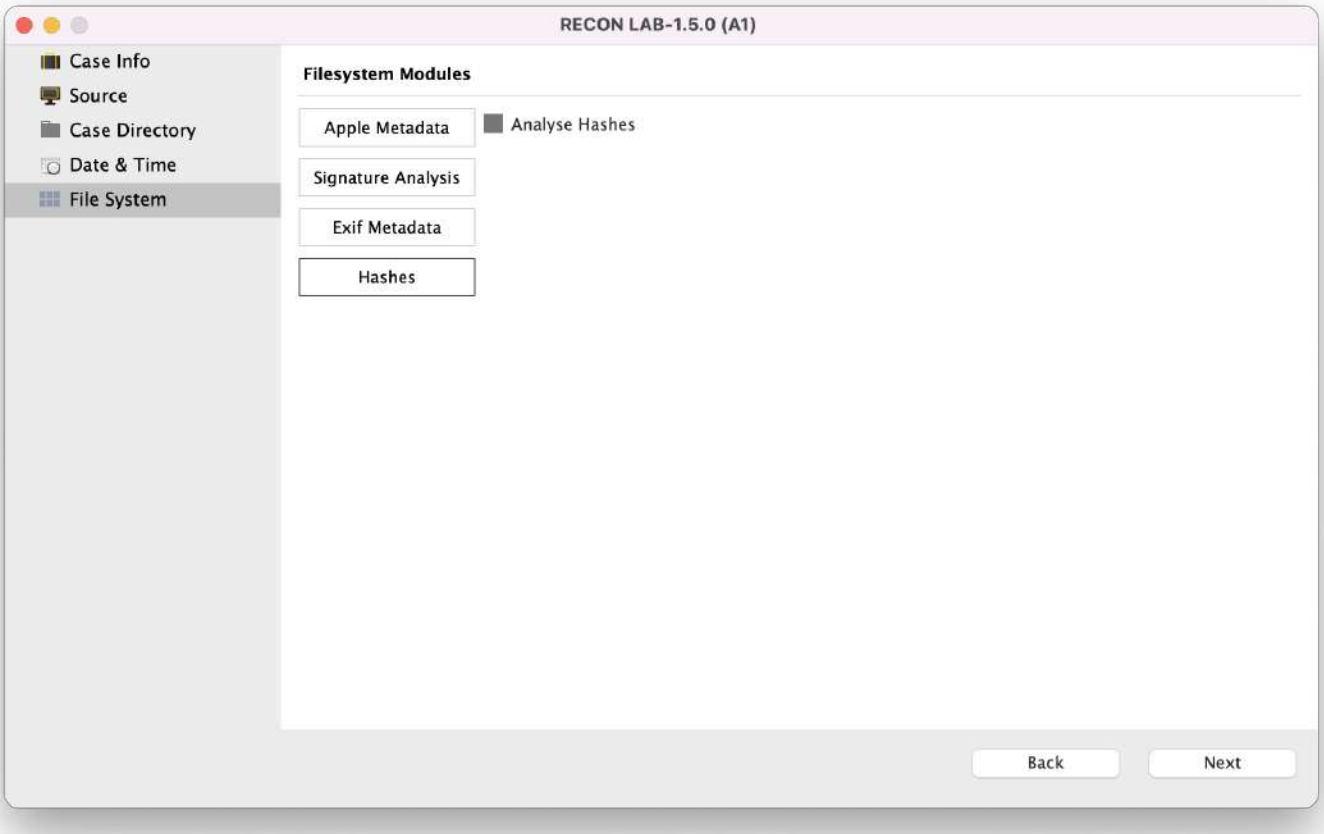
D – Check this box to add the EXIF Metadata to the RECON LAB Sidebar. Any files matching selected metadata will automatically be filtered and placed in the Sidebar.

R – Checking this box will include the selected EXIF metadata automatically to reports.

Title – The common name of the EXIF Metadata.

Description – The official description of the Apple Extended Attribute.

10.7.4 Hashes Module



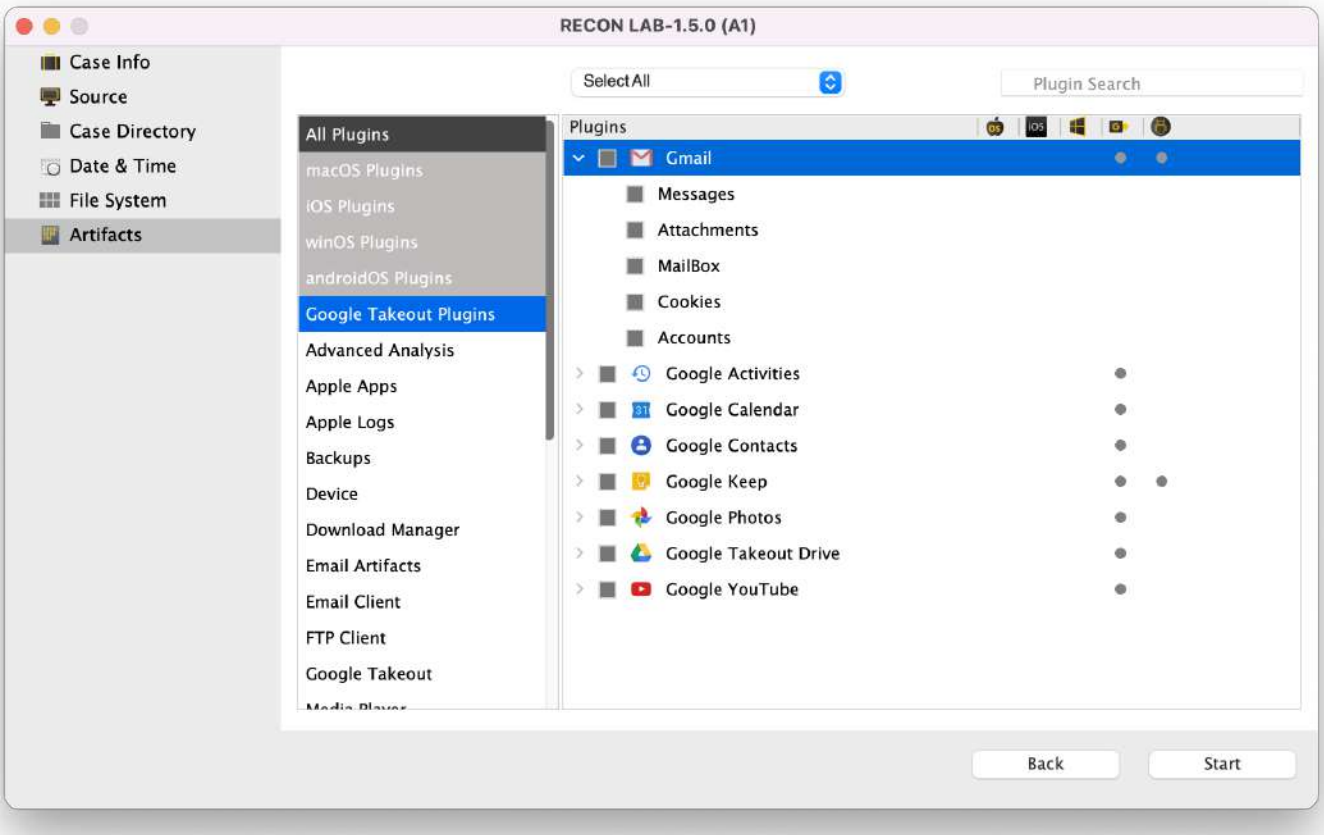
If you will be utilizing pre-configured hash sets in your investigation or analysis choose “Analyze Hashes”.

RECON LAB will create hashes of all files within the case.

10.8 Artifact Plugin Selection Module

As described previously in the “Configuration” part of this manual, RECON LAB automatically processes and analyzes thousands of artifacts using hundreds of plugins for Windows, macOS, iOS, Android and Google.

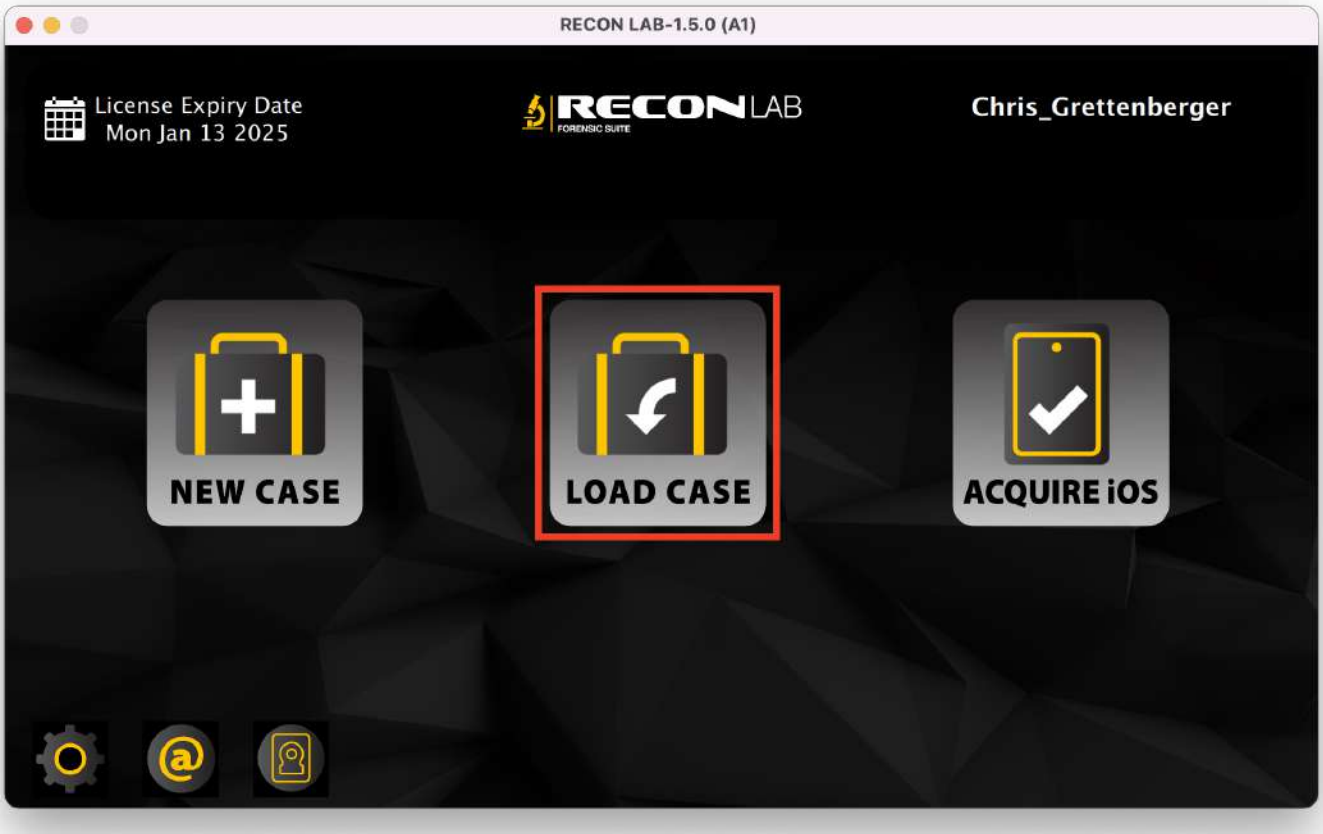
Select any plugins or artifacts that you want to run.



To begin processing of all sources with the selected Filesystem Modules and Automatic Artifact Analysis, click “Start”.

11. Reloading a Case

To open a previously created case, select Load Case from the initial splash screen.

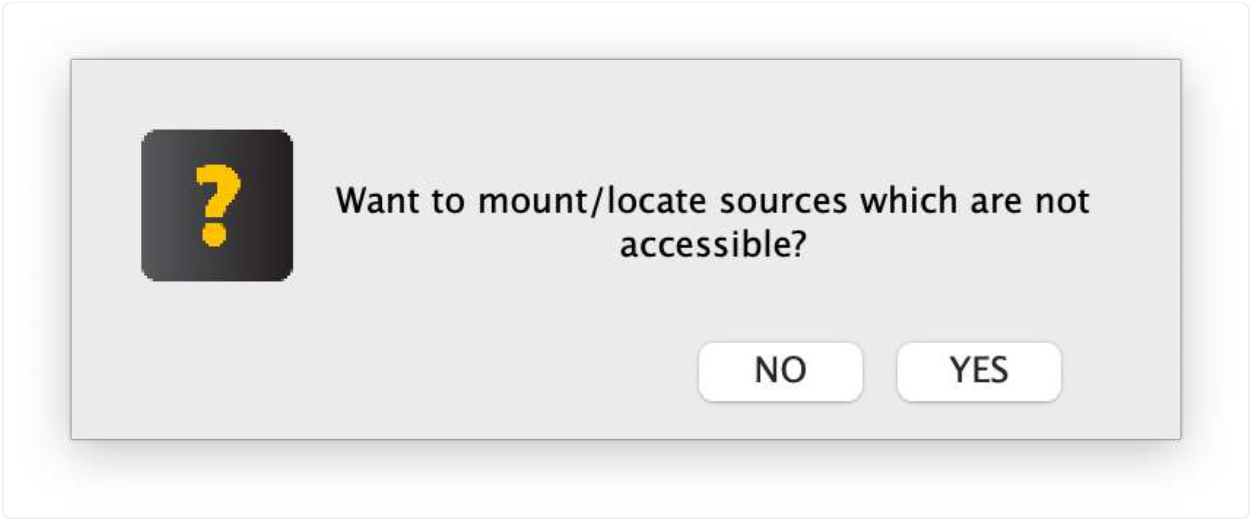


The popup window instructs the examiner to navigate to the desired case folder and click Open.

The naming structure of the folder will consist of the:

Case Name-YYYY-MTH-DYTHH-MM-SC
(i.e. Fraud_Investigation_2018-SEP-19T13-25-44)

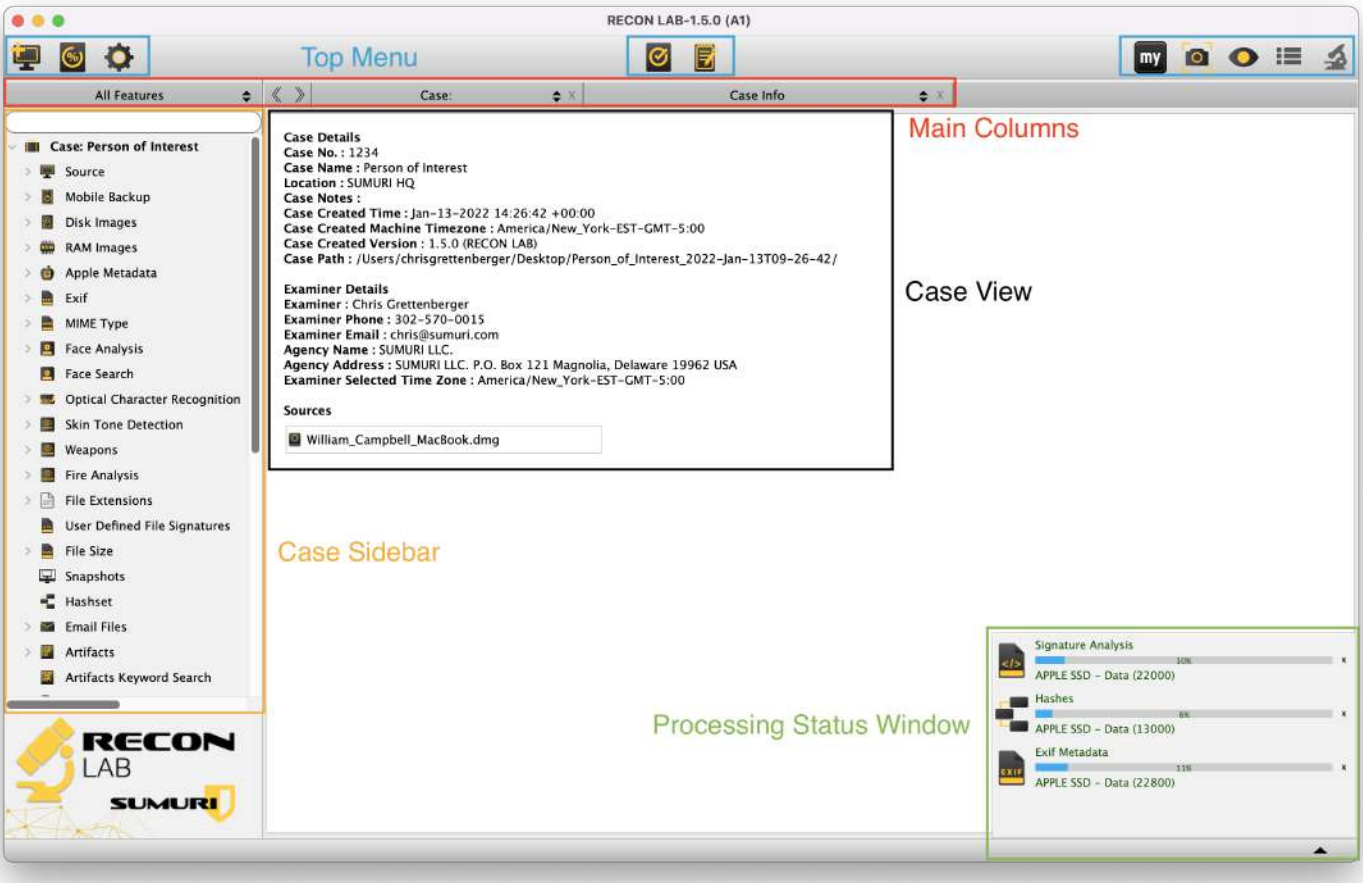
The following screen will ask the examiner if they want the original sources re-mounted.



The sources must be re-mounted in order for RECON LAB to function properly.

If the sources have moved RECON LAB will prompt you to locate them.

12. RECON LAB Interface



The RECON LAB Main Interface is designed to be intuitive and simple to use. The views in the main window will change depending on what is selected.

12.1 Processing Status Window

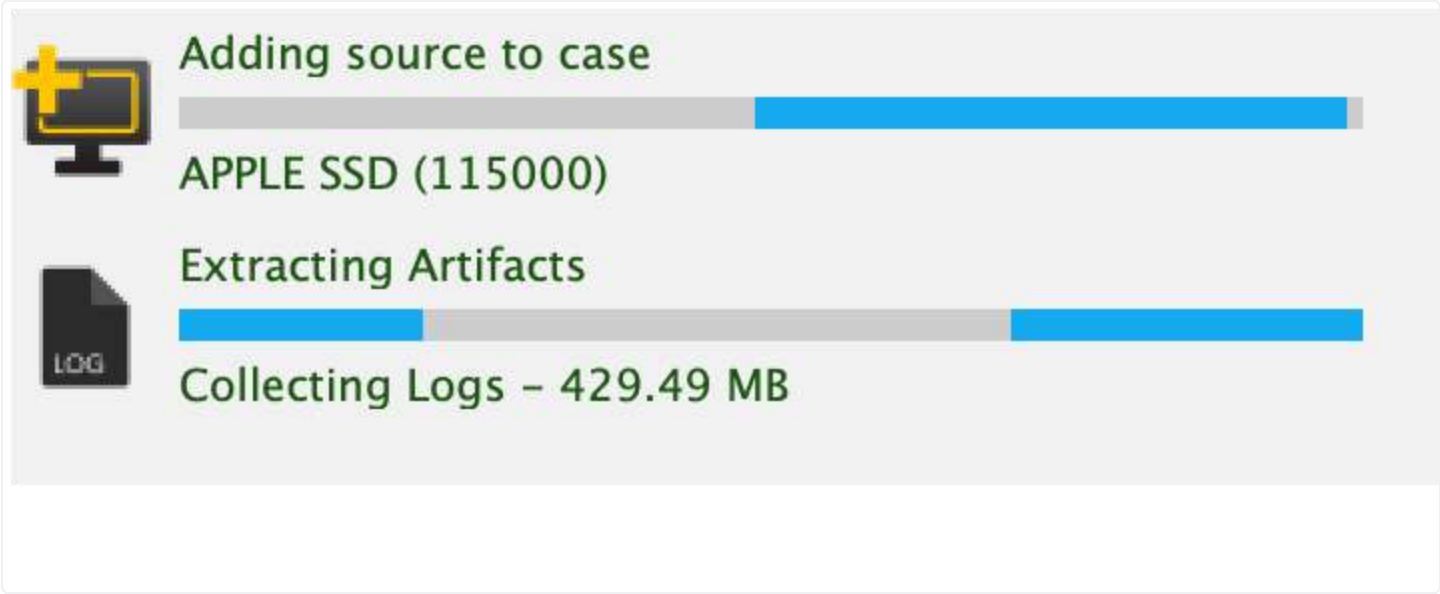
RECON LAB will let you begin working in minutes.

RECON LAB automatically and intelligently runs multiple tasks and processes at the same time. RECON LAB adjusts the different tasks based on the available resources to complete processing as quickly as possible.

RECON LAB first process is to “Add source to case”. This must be completed before you can manually review the evidence.

However, almost simultaneously, the automated analysis of artifacts begins (“Extracting Artifacts) and starts populating the Sidebar. As soon as a plugin is complete you can immediately begin

reviewing the results.



At this stage, RECON LAB will also begin automatically parsing MIME Types.

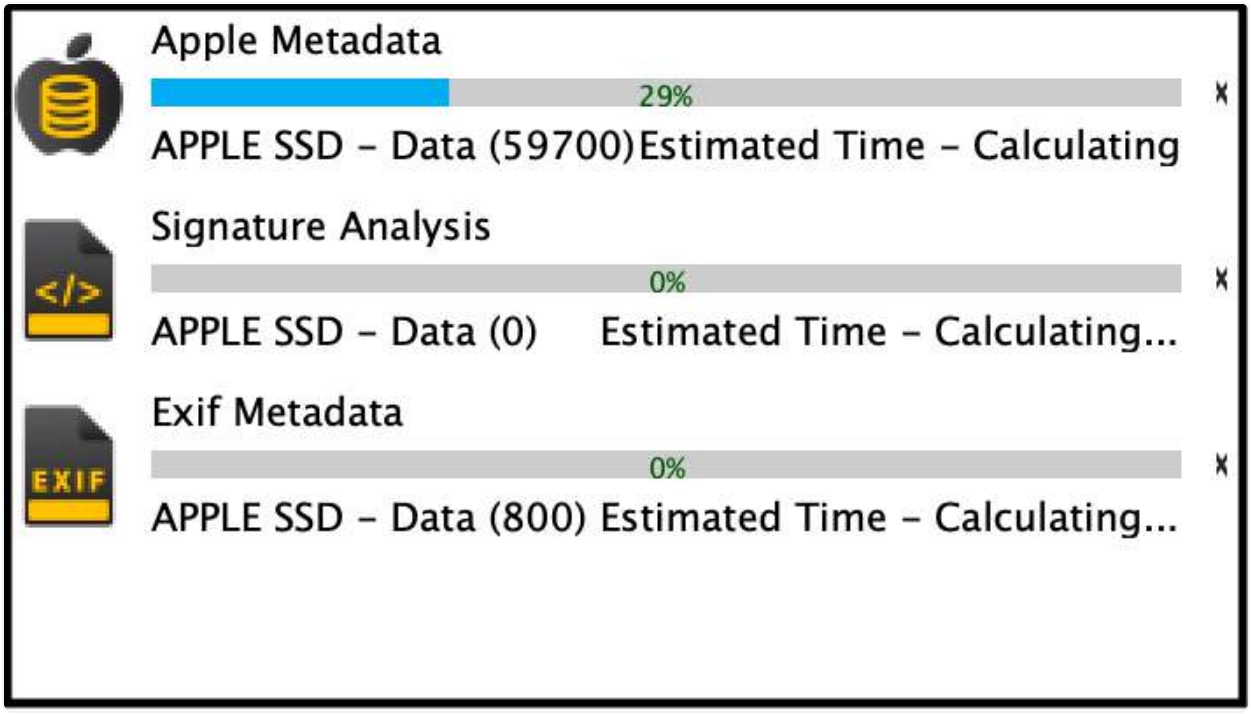
Next, if selected Apple Extended Timestamps are extracted for macOS file systems. Apple Extended Attributes are the timestamps utilized by macOS.

Other forensic tools extract and display macOS POSIX (Unix) timestamps. Favoring POSIX timestamps over Apple Extended Attribute timestamps will cause you to miss important evidentiary information and can lead to incorrect conclusions. RECON LAB along with RECON IMAGER is the only solution that allows you to properly capture, analyze and utilize Apple Extended Metadata timestamps within a forensic tool.

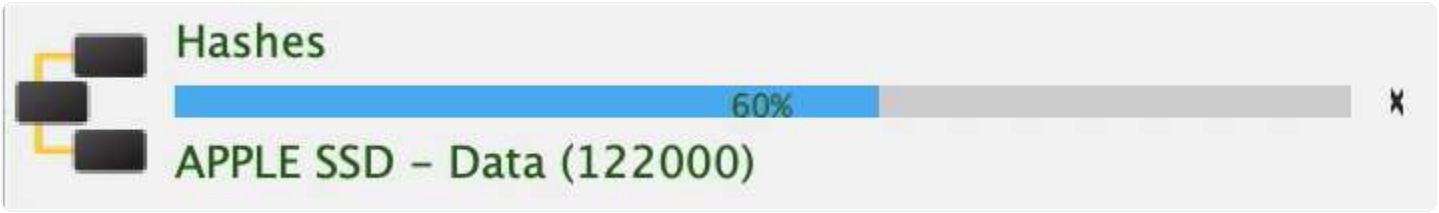
After the Apple Extended Attribute Timestamps module has started the identification and categorization of files based on MIME types begins.

this is a sentence.

This is followed by the Apple Metadata, Signature Analysis, and EXIF Metadata modules.

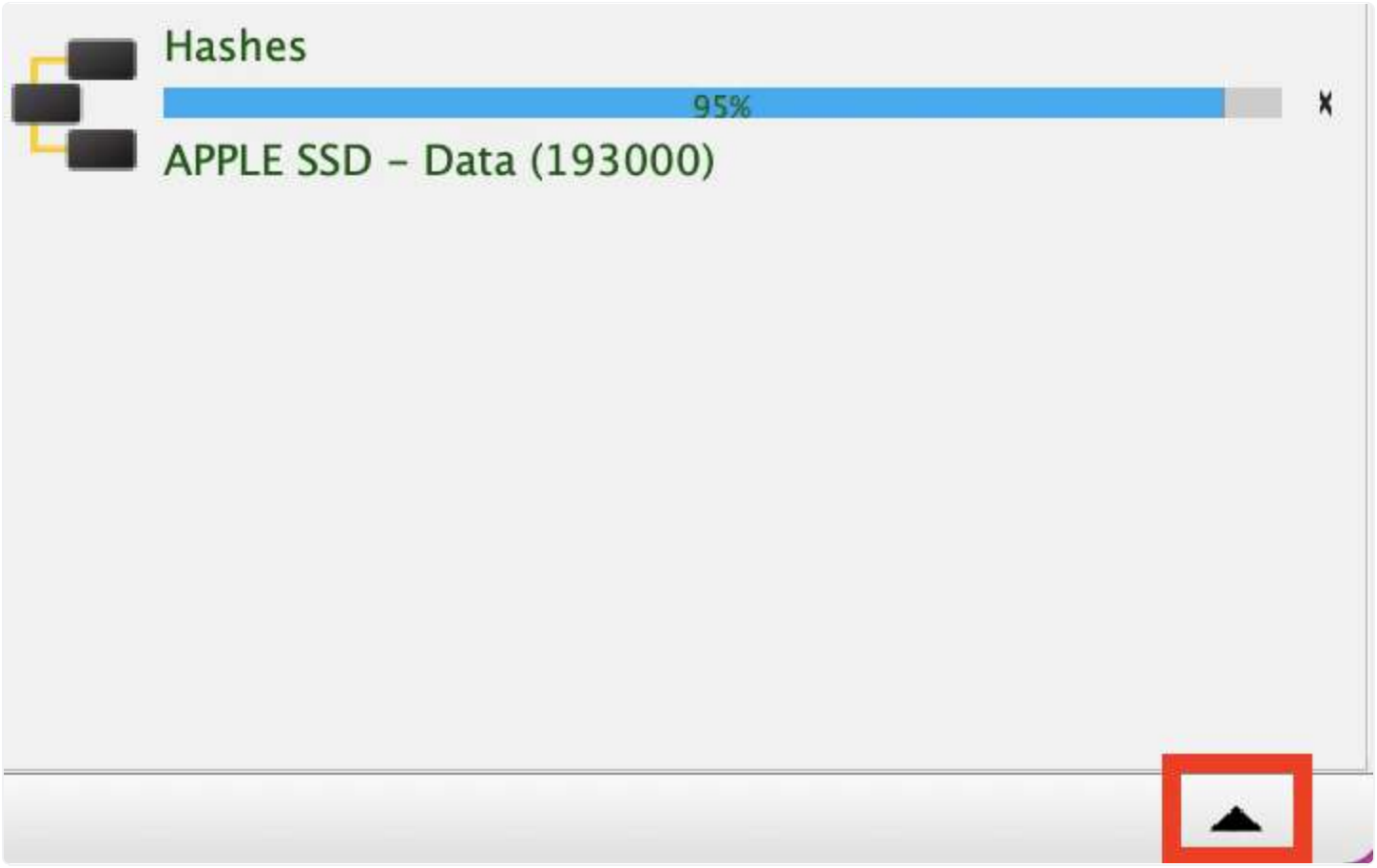


Finally, the Hashes module is run.



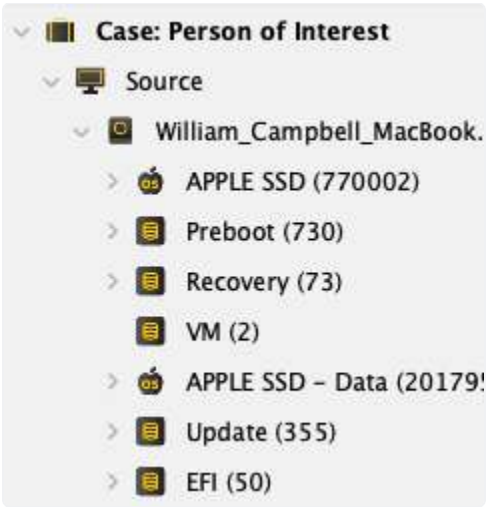
The information generated by each module is available as soon as it completes and can be reviewed immediately.

Modules can be canceled by clicking the “X” button. Keep in mind it may take some time before the module quits completely after the “X” button is pressed.

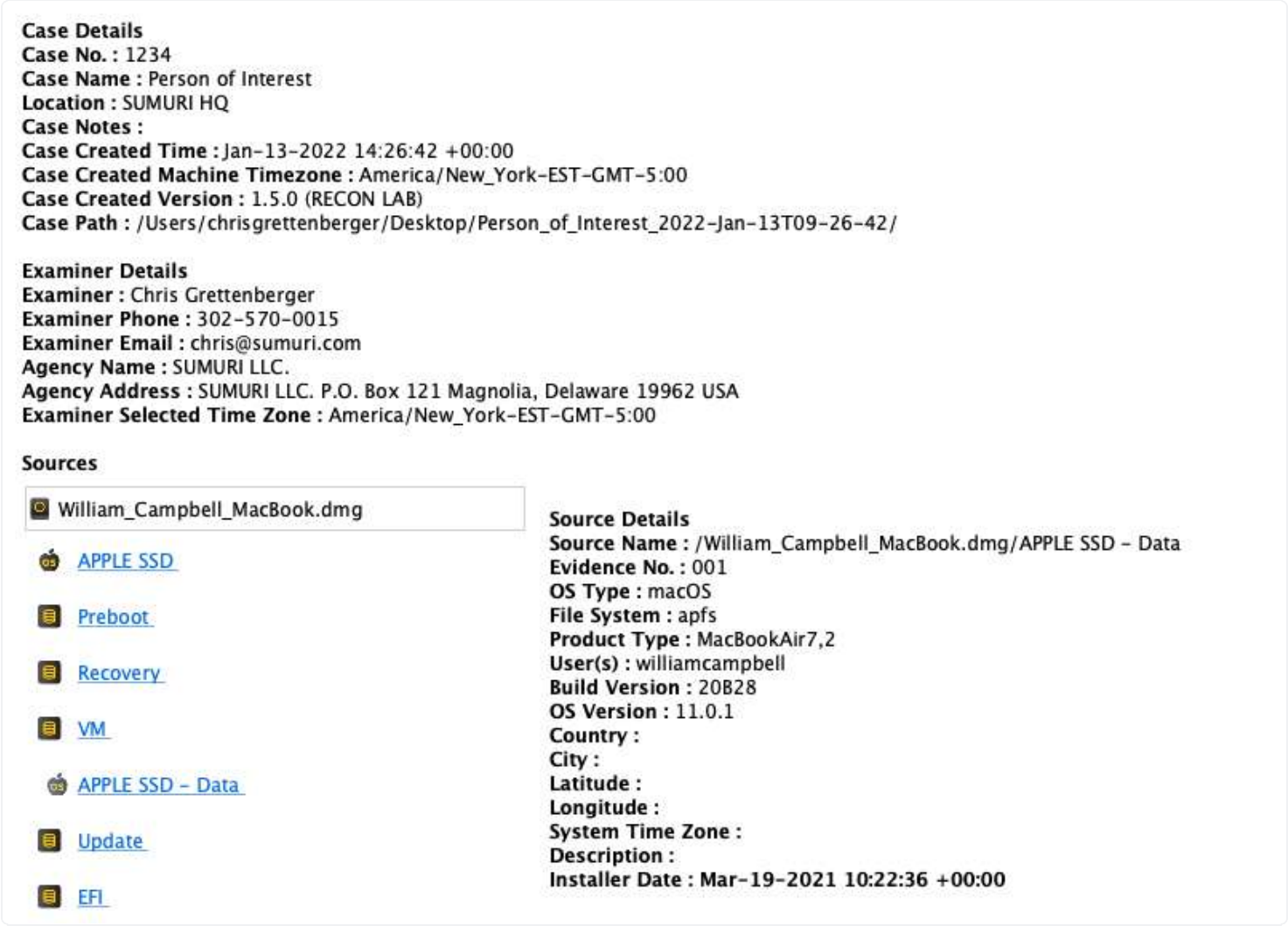


The Processing Status Window can be minimized by clicking the triangle icon in the bottom right corner.

12.2 Case View



The Case View can be activated by selecting the “briefcase” icon at the top of the Sidebar.



In Main Window you will find the Case Details, Examiner Details and Source information.

If multiple partitions exist they can be seen by clicking on the main source item (i.e. “Catalina.sparseimage”).

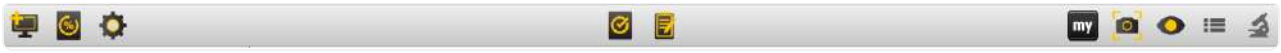
Clicking any of the partitions will display additional information for the source (i.e. “OS Version”).

The information found in the Case Details is almost always added automatically to any generated reports.

12.3 Menu Options

RECON LAB’s Top Menu is broken up into two parts, those accessible as icons on the top of the tool, and those that are accessible through macOS’s Menu Bar.

12.3.1 Interface Top Menu



1 2 3 4 5 6 7 8 9 10

The interface top menu is comprised of 10 total icons, allowing examiners quick access to some of the most important aspects of case management.

1. **Add Source** – Used to add additional sources after the case has begun.
2. **Processing Status** – Displays all added sources and the status of modules run against the sources. Sources can be removed as well.
3. **Configuration** – Allows changes to configuration settings.
4. **Global Report** – Automatic Report generation.
5. **Story Board** – Creates a new report in a WYSIWYG report editor.
6. **Examiner Space** - Allows examiners to take down notes relevant to their case which can be added to their reports.
7. **Screenshot** – Allows the user to create a screenshot that can be added to reports.
8. **Quick Look** – Activates the native macOS file viewer supporting hundreds of file types.
9. **Show/Hide Sidebar** – Pressing this button will show or hide the Sidebar.
10. **Show Detailed Information** – Pressing this button will show or hide the Detailed Information Window

12.3.2 macOS Menu Bar

RECON LAB also uses the macOS Menu Bar to organize the interface in a more user-friendly way.

The Menu Bar is accessible from the top of your screen and is broken into 5 categories. Process, Search, Timeline, Export, and Report.

12.3.2.1 Process

The Process tab allows for the following features to be accessed.

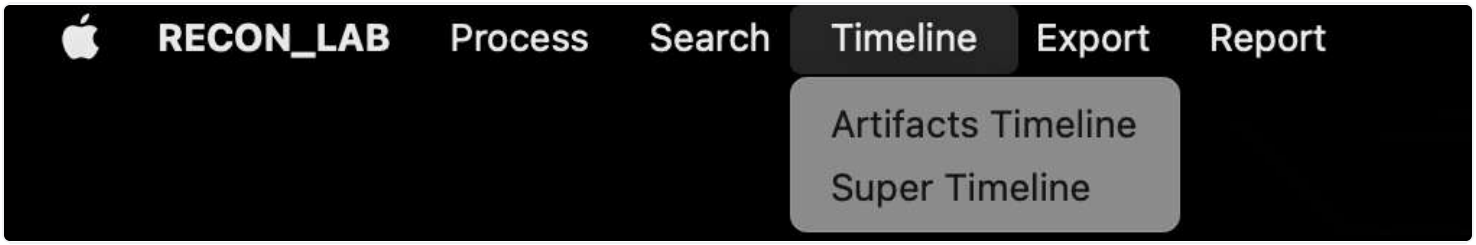
1. **Run Artifacts** – Calls the Artifacts and Plugins module for automated analysis.
2. **RAM Analysis** – Opens the RAM Analysis module which is a GUI for Volatility and may include a “Carve Password” feature (vetted agencies only).
3. **Text Indexing** – Allows the indexing of files and directories.
4. **Hash Sets** – Allows creation or importing of hash sets.

12.3.2.2 Search

The Search tab allows for the following features to be accessed.

1. **File Search** – Allows for locating files based on a combination of timestamps, file names, extensions, file sizes and more.
2. **Content Search** – Calls the Content Search configuration window to allow searching with keywords.
3. **EXIF Metadata Search** - Allows the examiner to conduct a search using EXIF Metadata.
4. **Apple Metadata Search** – Allows for locating files based on Apple Extended Metadata.
5. **Artifacts Keyword Search** – Allows the examiner to conduct a single keyword search quickly within all recovered artifacts.
6. **Recognize Face** - Allows the examiner to extract faces from a picture.

12.3.2.3 Timeline



The Timeline tab allows the following features to be accessed.

1. **Artifacts Timeline** – Opens the Artifacts Timeline module used for generating timelines and graphs for timestamps recovered from the Artifacts and Plugin module.
2. **Super Timeline** – Creates an enhanced timeline using all timestamps available from file and file artifacts.

12.3.2.4 Export

The Export tab allows for the following features to be accessed.

1. **Tagged File Export** – Allows the export of files that have been tagged or bookmarked.
2. **Export Case** - Allows the user to export a portable version of their case that be loaded on a Windows machine. See Section 34 for more details.

12.3.2.5 Report

The Report tab allows for the following features to be accessed.

1. **Global Report** – Automatic Report generation.
2. **Story Board** – Creates a new report in a WYSIWYG report editor.

12.4 Main Columns

There are three main columns at the top of the Main Window for RECON LAB. These columns can be used for quick navigation.

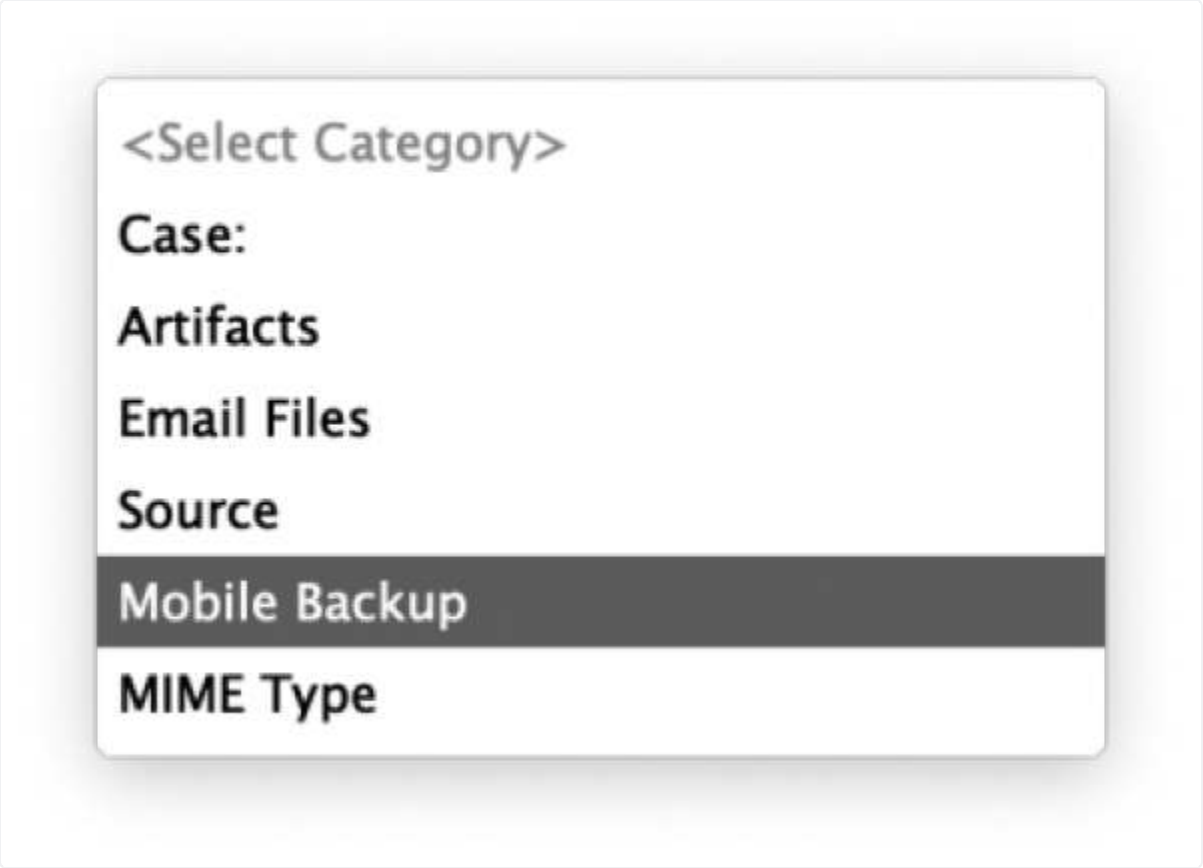
When you navigate to different modules or views these columns will keep a history of these. Clicking on the columns will allow you to return to a previous module or view.

Views or modules can be removed by selecting the “X” button.

Sidebar Column

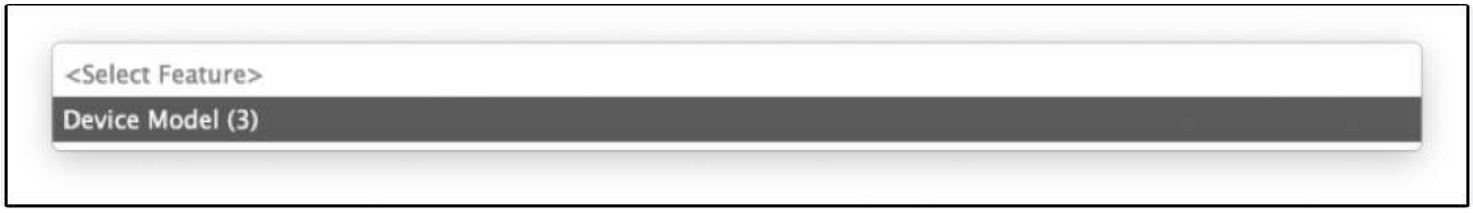
The Sidebar Column allows quick access to the modules and views located in the Sidebar.

Select Category Column



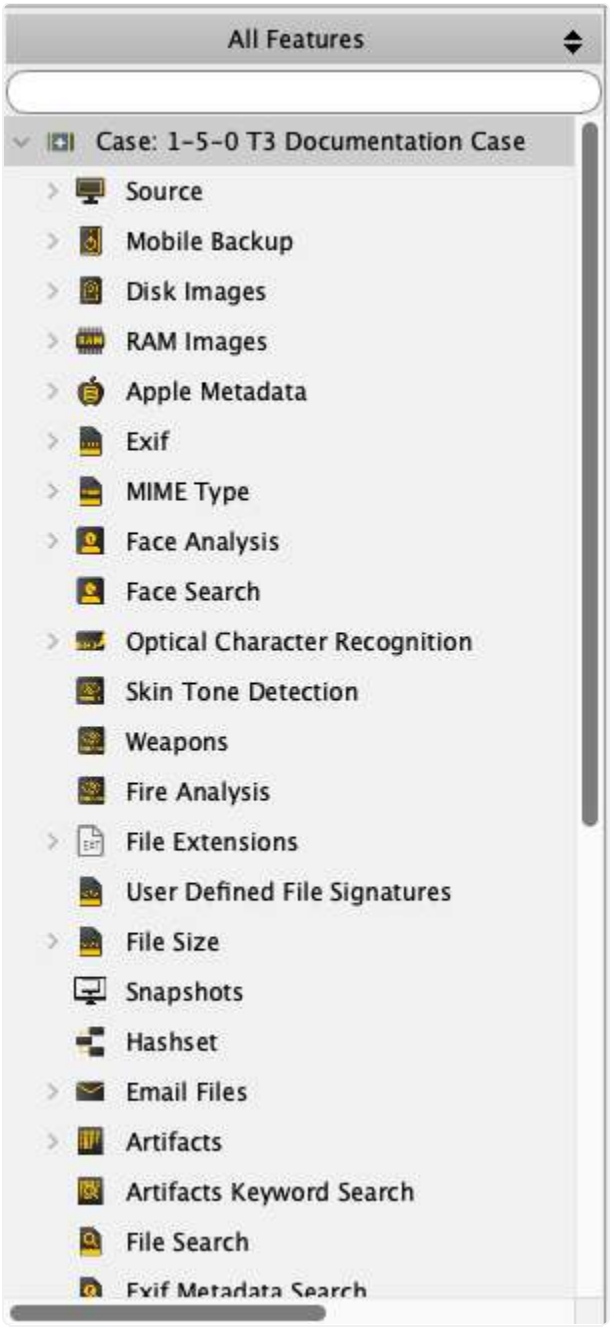
The Select Category Column keeps a history of modules and sources previously viewed. Clicking the title of the column will show previous items. Select any item to return to the module or source.

Select Feature Column



The Select Feature Column keeps a history of different windows viewed. Clicking the title of the column will show previous items. Select any item to return to a previous window.

12.5 Case Sidebar



The Sidebar is used to quickly access data recovered from processing, analysis, and reporting. It is also used for manually navigating through the source data.

Clicking the triangle next to a category or feature will expand the category.

The Quick Search field can be used to quickly find a plugin or module.

12.6 Main Viewer Window

The Main Viewer window has a Table View and a Gallery View. The following is an example of the Table View when a source is selected in the Sidebar. Specifically, this is a user's Download folder.

			Record No.	Inode No./File ID	File Name	Extension	File Path	File Size
1	☐	☐	1208592		.DS_Store		/Users/macboy/Downloads/.DS_Store	6148
2	☐	☐	1208593		.localized		/Users/macboy/Downloads/.localized	0
3	☐	☐	1208594		DB.Browser.for.SQLite-3.11.2.dmg	dmg	/Users/macboy/Downloads/DB.Browser.for.SQLite-3.11.2.dmg	16857319
4	☐	☐	1208595		googlechrome.dmg	dmg	/Users/macboy/Downloads/googlechrome.dmg	80845370
5	☐	☐	1208596		iOS_iPadOS_13_Beta_Profile.mobileconfig	mobileco...	/Users/macboy/Downloads/iOS_iPadOS_13_Beta_Profile.mobilec...	7348
6	☐	☐	1208597		macOSDeveloperBetaAccessUtility.dmg	dmg	/Users/macboy/Downloads/macOSDeveloperBetaAccessUtility.d...	92222

The first column with the checkbox is to bookmark the file.

The second column with the checkbox is for marking a file as "seen" by the examiner. Call it the "been there, done that" tag.

Record No. – This is a unique number assigned to a record by RECON LAB.

Inode No./File ID – Shows the Inode, FileID or CNID number of a file.

File Name – The name of the file.

Extension – The extension of the file.

File Path – The path of the file in relation to the source.

File Size – Size of the file in bytes.

Mime Type	Hashset Name	MD5	SHA1	Decompression Status
application/octet-stream		194577a7e20bdcc7afbb718f502c134c	df2fbeb1400acda0909a32c1cf6bf492f1121e07	
application/x-zerosize				
application/octet-stream		e1a6b6b80cc4be9c16f526fffbc7ef64	512f321a50d268c7b3acc9c6246b196b5a2a4cde	
application/x-bzip		7c11c1fd6958bc6b1877be401426b435	ece2e107fb8e25dca689416056c6961ab05dbff5	
application/octet-stream		2e60c27fa3d936fb3f1b182f63e04b1f	dd74f361be8da45a46016094292ad8ddf1f05173	
application/octet-stream		c0a3d022ba1f2f731a94029e404f847b	0126db627fc6685194e001d74f2c1c54b0a662a6	

Mime Type – Shows the type of file as identified by MIME Types.

HashSet Name – If the file hash matches a hash found within a HashSet the name of the HashSet is shown.

MD5 – The calculated MD5 hash of a file.

SHA1 – The calculated SHA-1 hash of a file.

Decompression Status – Shows if a file (i.e. zip file) has been expanded. If expanded, the word "Decompressed" will show.

Date Modified	Date Change	Date Accessed
2019/08/22 22:25:15 GMT-4:00	2019/08/22 22:25:15 GMT-4:00	2019/08/23 09:27:24 GMT-4:00
2019/08/22 10:07:53 GMT-4:00	2019/08/22 10:07:53 GMT-4:00	2019/08/22 10:07:53 GMT-4:00
2019/08/22 20:57:42 GMT-4:00	2019/08/22 20:59:22 GMT-4:00	2019/08/22 20:57:42 GMT-4:00
2019/08/23 09:27:13 GMT-4:00	2019/08/23 09:27:35 GMT-4:00	2019/08/23 09:27:15 GMT-4:00
2019/08/22 21:50:25 GMT-4:00	2019/08/23 14:22:02 GMT-4:00	2019/08/23 14:22:01 GMT-4:00
2019/08/22 10:13:15 GMT-4:00	2019/08/22 10:13:23 GMT-4:00	2019/08/22 10:13:20 GMT-4:00

Date Modified – Standard timestamp for Date Modified.

Date Change – Standard timestamp for Date Changed.

Date Accessed – Standard timestamp for Date Accessed.

Date Added	Content Creation Date	Content Modification Date	Last Used Date	Use Count
2019/08/23 00:57:42 GMT-4:00	2019/08/23 00:57:26 GMT-4:00	2019/08/23 00:57:42 GMT-4:00	2019/08/23 00:57:42 GMT-4:00	5
			2019/08/23 13:27:15 GMT-4:00	1
2019/08/23 01:50:26 GMT-4:00	2019/08/23 01:50:25 GMT-4:00	2019/08/23 01:50:25 GMT-4:00	2019/08/23 18:22:02 GMT-4:00	6
			2019/08/22 14:13:16 GMT-4:00	1

Date Added – macOS Apple Extended Attribute for when a file was added to the volume.

Content Creation Date – macOS Apple Extended Attribute for when the content of the file was created.

Content Modification Date – macOS Apple Extended Attribute for when the content of the file was modified.

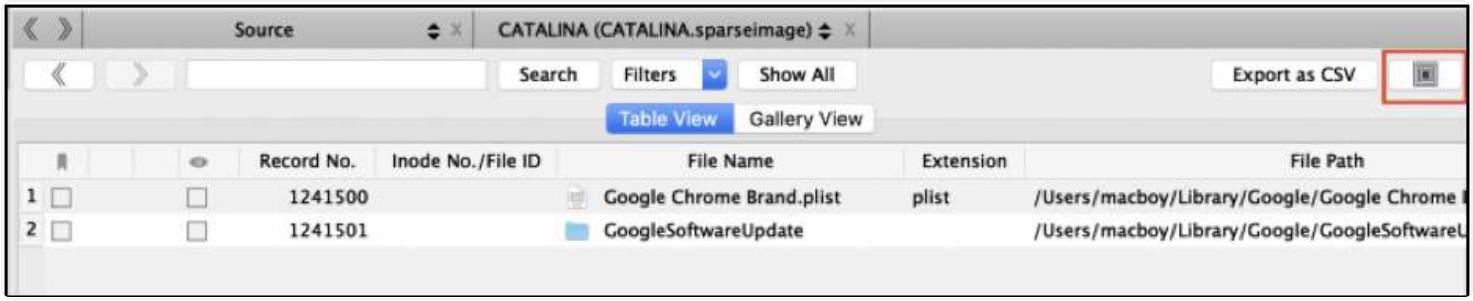
Last Used Date – macOS Apple Extended Attribute for when the file was last opened by a human (double-click to open).

Use Count – macOS Apple Extended Attribute that approximates how many times a file was opened by a human (double-click to open).

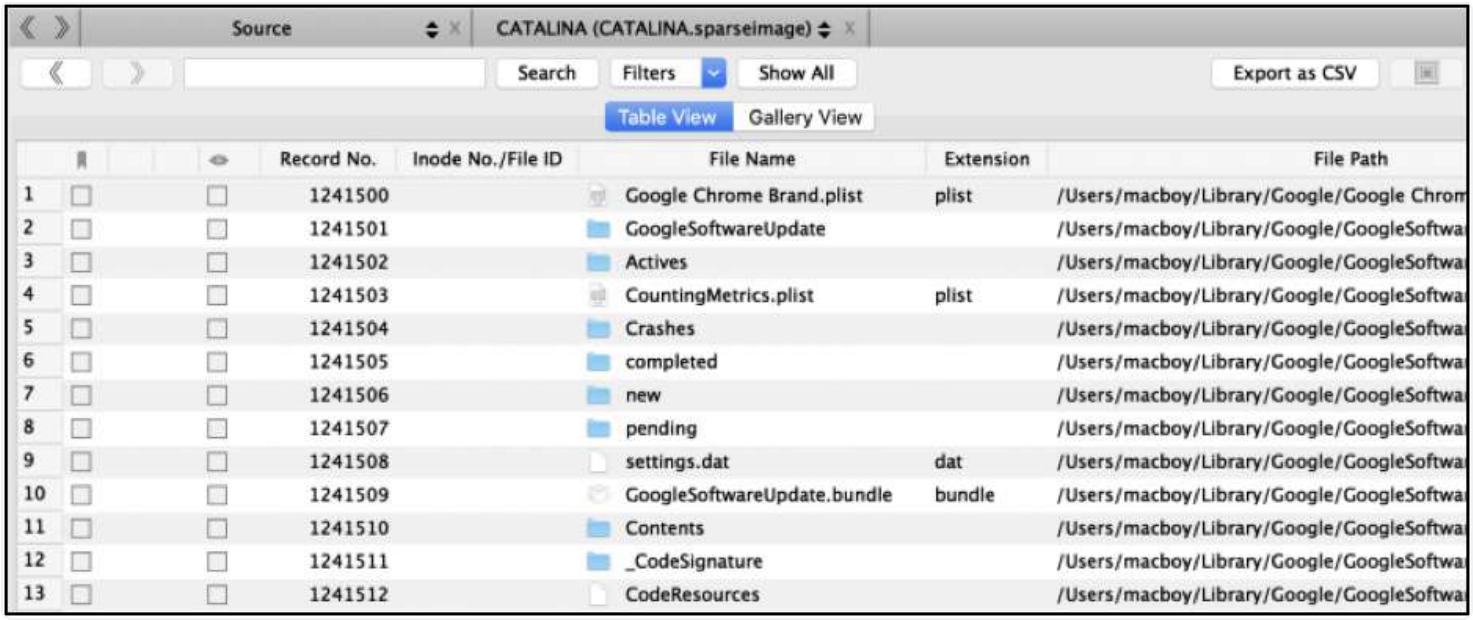
12.6.1 Table View

12.6.1.1 Recursive View

The Recursive View feature will recursively expand any subdirectories in the current view. This is frequently done prior do creating a full file listing.

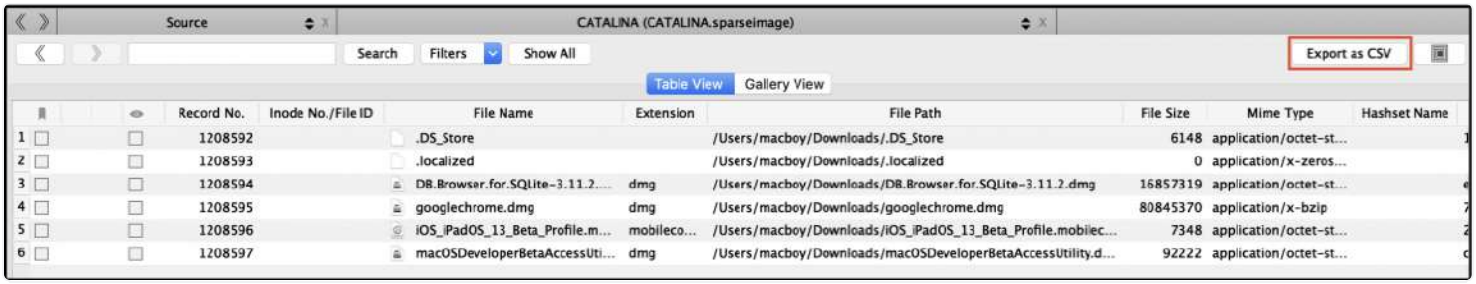


To expand all directories recursively, click the Recursive View button.



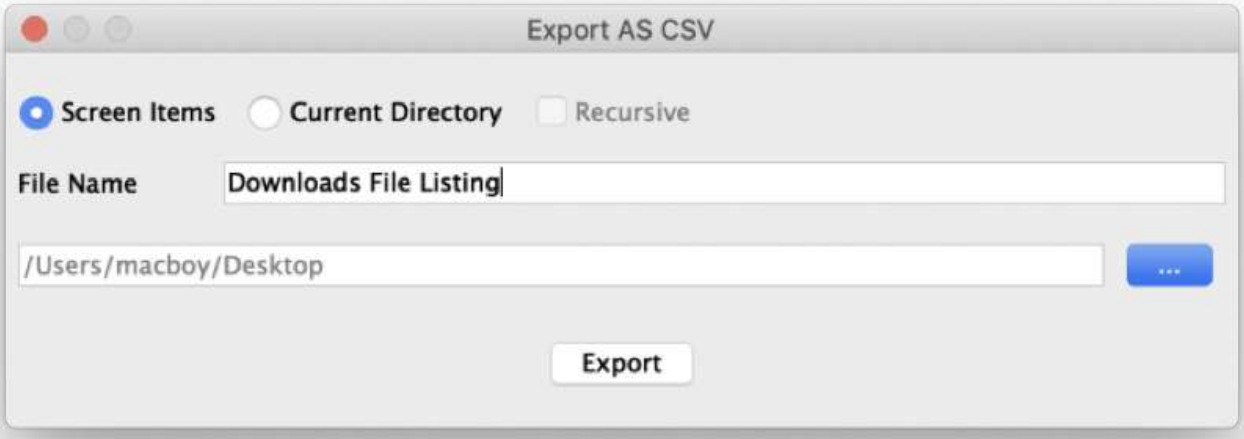
	Record No.	Inode No./File ID	File Name	Extension	File Path
1	1241500		Google Chrome Brand.plist	plist	/Users/macboy/Library/Google/Google Chrom
2	1241501		GoogleSoftwareUpdate		/Users/macboy/Library/Google/GoogleSoftwa
3	1241502		Actives		/Users/macboy/Library/Google/GoogleSoftwa
4	1241503		CountingMetrics.plist	plist	/Users/macboy/Library/Google/GoogleSoftwa
5	1241504		Crashes		/Users/macboy/Library/Google/GoogleSoftwa
6	1241505		completed		/Users/macboy/Library/Google/GoogleSoftwa
7	1241506		new		/Users/macboy/Library/Google/GoogleSoftwa
8	1241507		pending		/Users/macboy/Library/Google/GoogleSoftwa
9	1241508		settings.dat	dat	/Users/macboy/Library/Google/GoogleSoftwa
10	1241509		GoogleSoftwareUpdate.bundle	bundle	/Users/macboy/Library/Google/GoogleSoftwa
11	1241510		Contents		/Users/macboy/Library/Google/GoogleSoftwa
12	1241511		_CodeSignature		/Users/macboy/Library/Google/GoogleSoftwa
13	1241512		CodeResources		/Users/macboy/Library/Google/GoogleSoftwa

12.6.1.2 Export to CSV

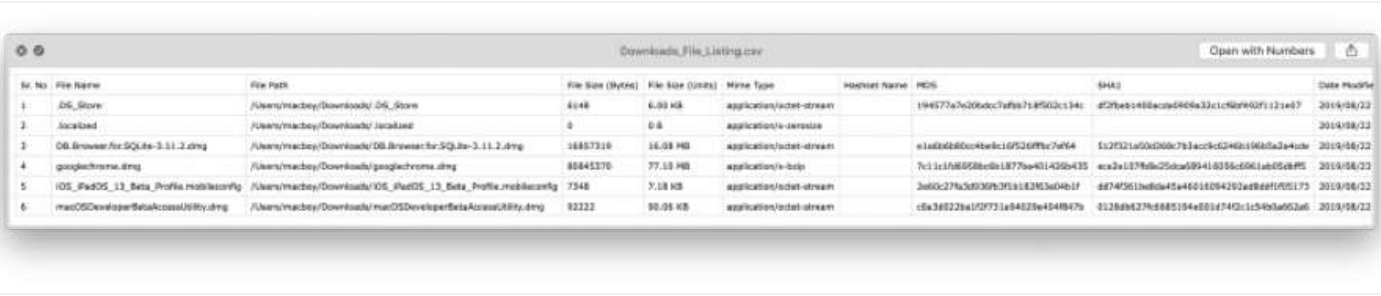


	Record No.	Inode No./File ID	File Name	Extension	File Path	File Size	Mime Type	Hashset Name
1	1208592		.DS_Store		/Users/macboy/Downloads/.DS_Store	6148	application/octet-st...	
2	1208593		.localized		/Users/macboy/Downloads/.localized	0	application/x-zeros...	
3	1208594		DB.Browser.for.SQLite-3.11.2....	dmg	/Users/macboy/Downloads/DB.Browser.for.SQLite-3.11.2.dmg	16857319	application/octet-st...	
4	1208595		googlechrome.dmg	dmg	/Users/macboy/Downloads/googlechrome.dmg	80845370	application/x-bzip	
5	1208596		iOS_iPadOS_13_Beta_Profile.m...	mobileco...	/Users/macboy/Downloads/iOS_iPadOS_13_Beta_Profile.mobilec...	7348	application/octet-st...	
6	1208597		macOSDeveloperBetaAccessUti...	dmg	/Users/macboy/Downloads/macOSDeveloperBetaAccessUtility.d...	92222	application/octet-st...	

The “Export as CSV” feature allows an examiner to create a file listing of the current Screen Items or Current Directory. If you select a directory you have the option of including all files recursively by checking the “Recursive” button.



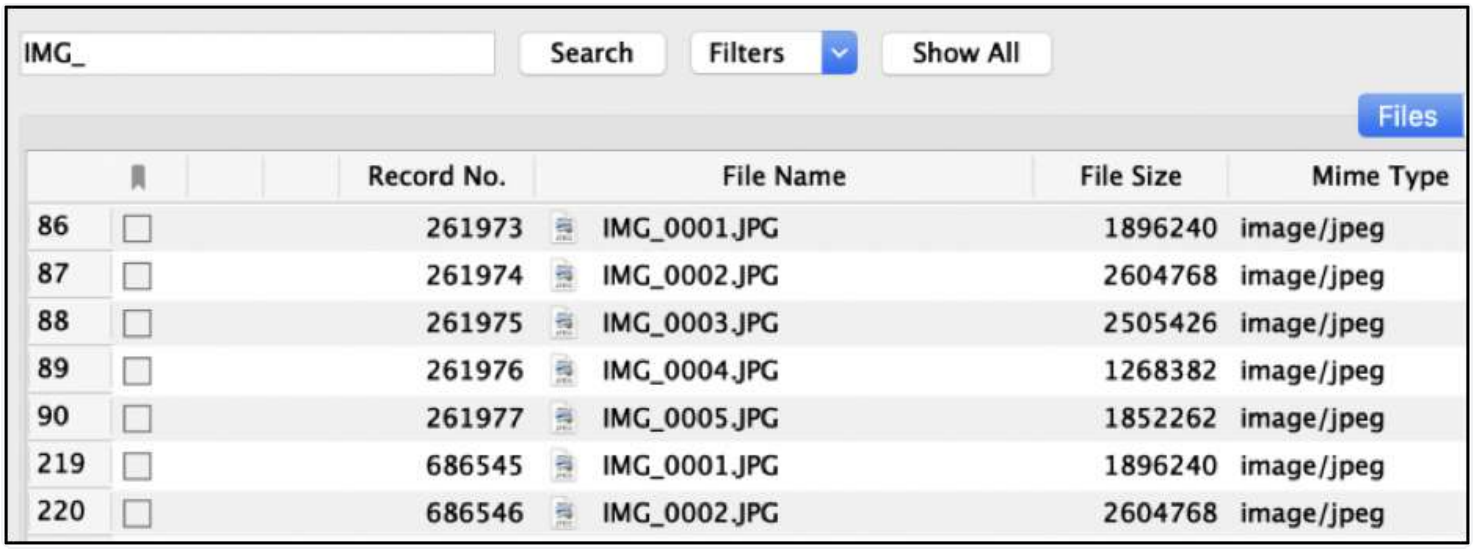
Provide a File Name for the report and choose the location for the report. When done, click “Export”.



A folder will be created in the location you chose and RECON LAB will ask you if you would like to open the CSV file created.

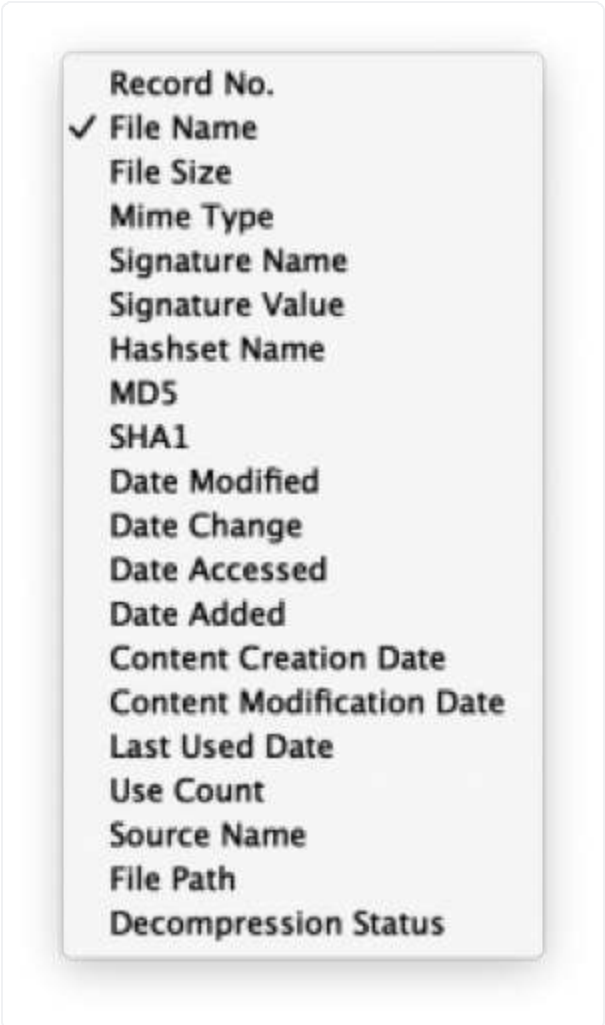
12.6.1.3 Table View Filter and Search

Table View includes a search feature with filters.



In the example above the keyword, “IMG_” was entered. Clicking the “Search” button showed all files with “IMG_” in the File Name.

To reset the view click the “Show All” button.

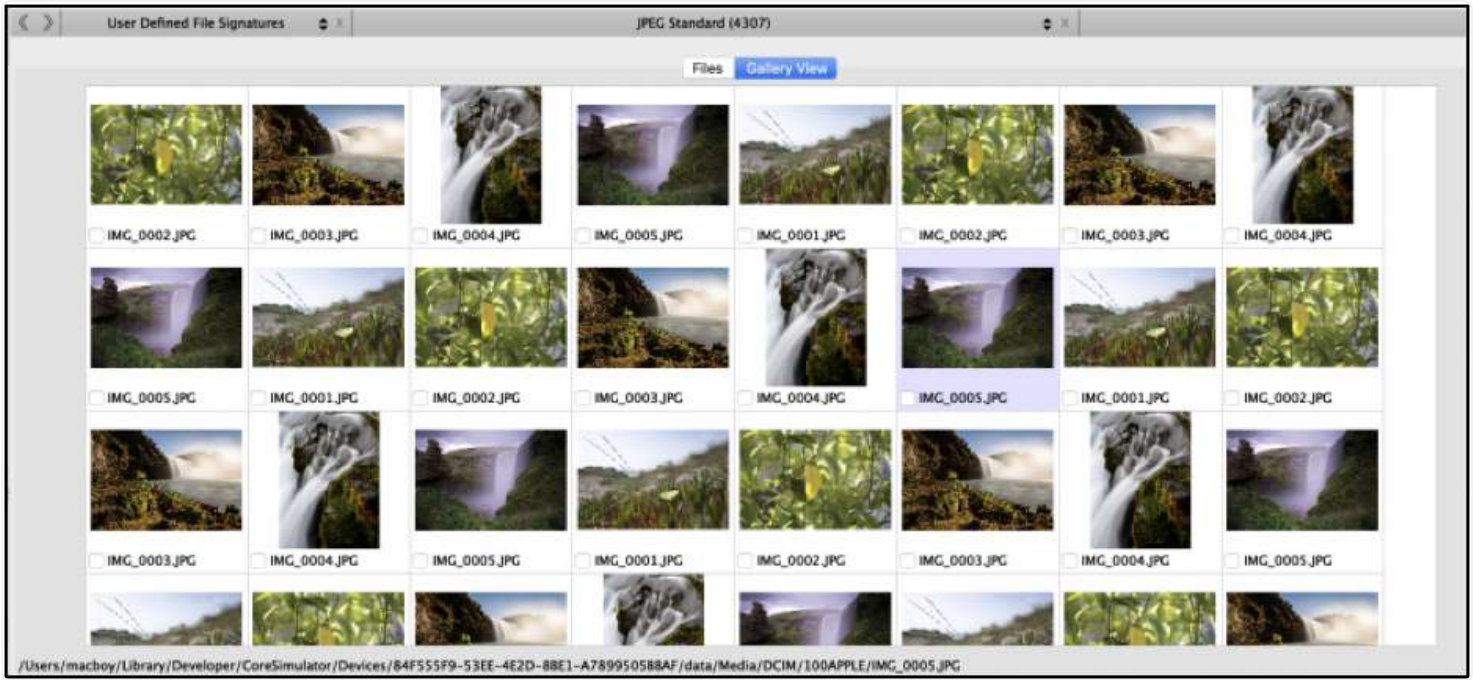


Additional filters can be selected and used in the “Filters” dropdown box.

12.6.1.4 Navigation Buttons

The Main Viewer window includes backward and forward navigation buttons that work similarly to web browser navigation buttons.

12.6.2 Gallery View

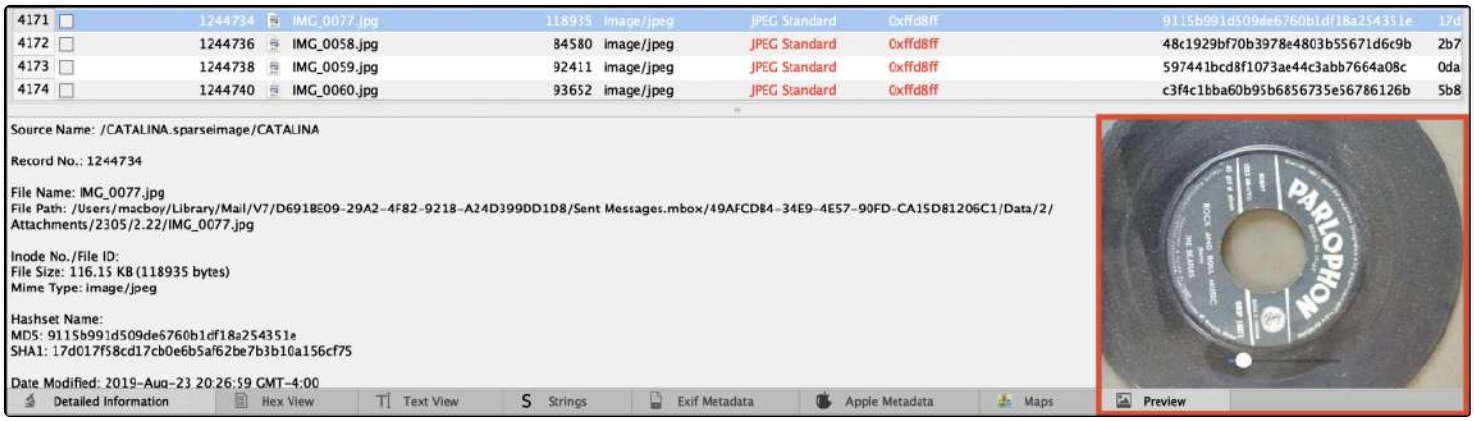


If any pictures exist within the items listed in the Main Viewer the Gallery View tab can be selected.

Pictures will be displayed as a thumbnail. Selecting the checkbox next to the image name will bookmark the file.

Right-clicking on the picture file will present additional options (discussed later in this manual).

12.7 Multimedia Preview Pane



The bottom right corner of the RECON LAB interface contains the Multimedia Preview Pane. The Preview Pane supports a variety of images, audio and video files.

Any file selected in the Main Viewer window that is supported by the Preview Pane will be displayed.

12.8 Viewer Panes

RECON LAB has multiple viewer panes to assist with presenting additional information or views of files.

Detailed Information – Shows the location of a file within the source, dates and times, examiner's notes and more.

Hex View – Shows the file in Hex View.

Text View – Shows the file text view.

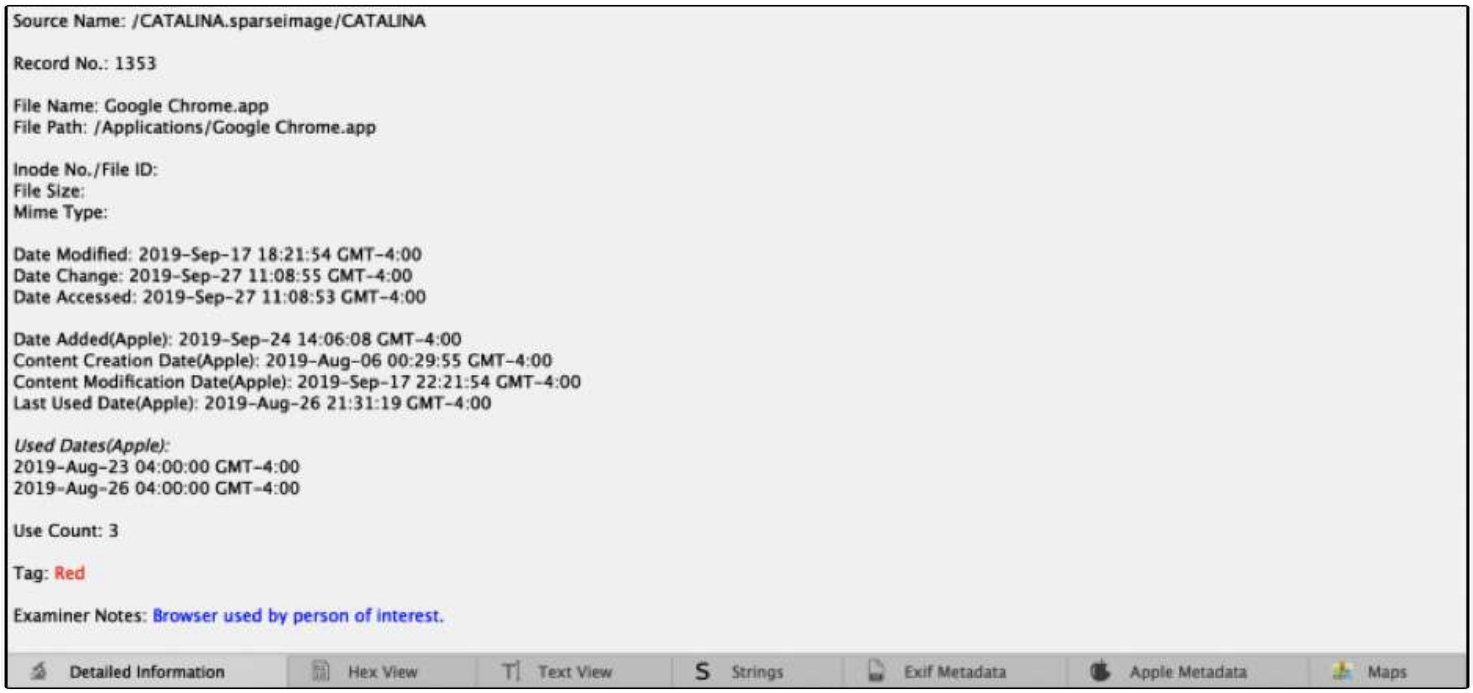
Strings View – Shows the text view of a file with binary data removed.

Exif Metadata – Interprets and shows special metadata contained in specific files.

Apple Metadata – Shows all of the Apple Extended Metadata of a macOS file.

Maps – Shows both online and offline maps for files that contain location data.

12.8.1 Detailed Information Pane

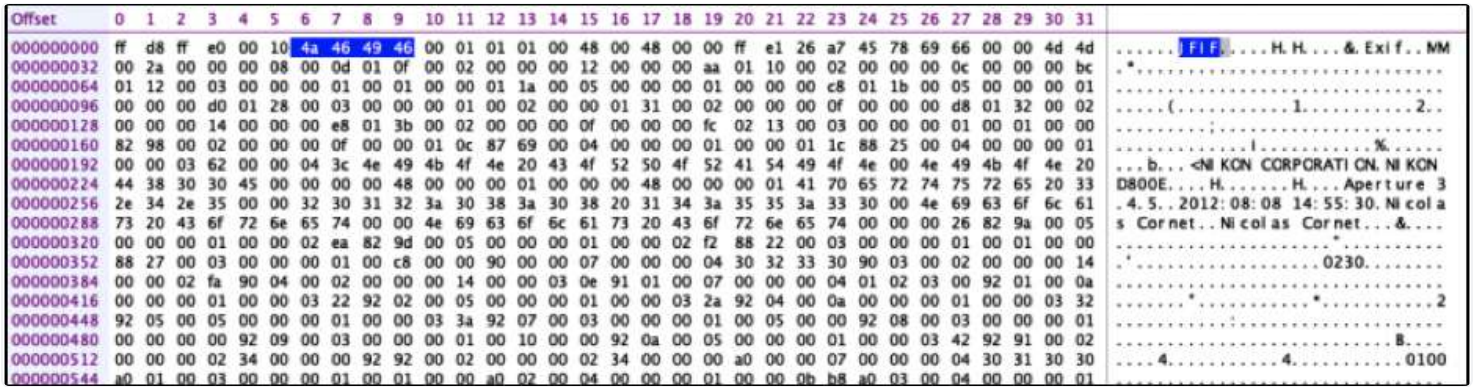


When a file or item is highlighted in the Main Viewer the Detailed Information pane will show as much information as possible. The content will change depending on what is selected in the Main Viewer.

In the example above, the Google Chrome application was selected.

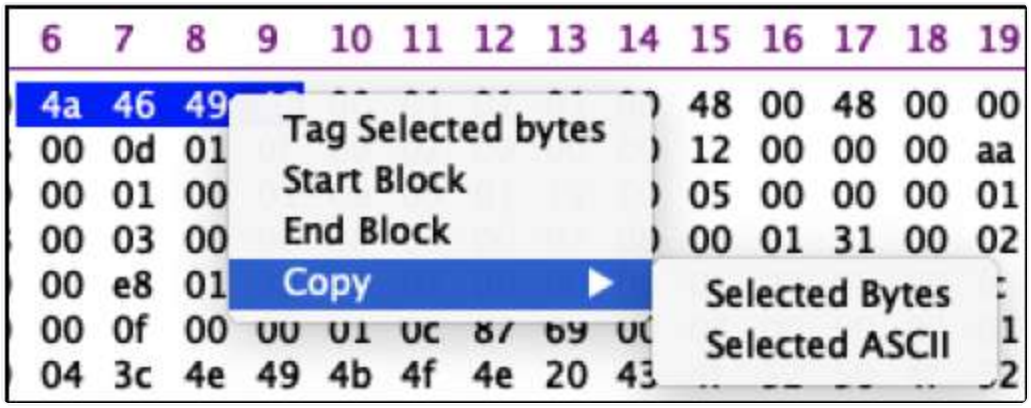
The application's name, path, dates and times, tags and examiner notes are displayed. Additionally, some useful Apple Extended Attributes are shown (Use Count and Used Dates).

12.8.2 Hex View Pane



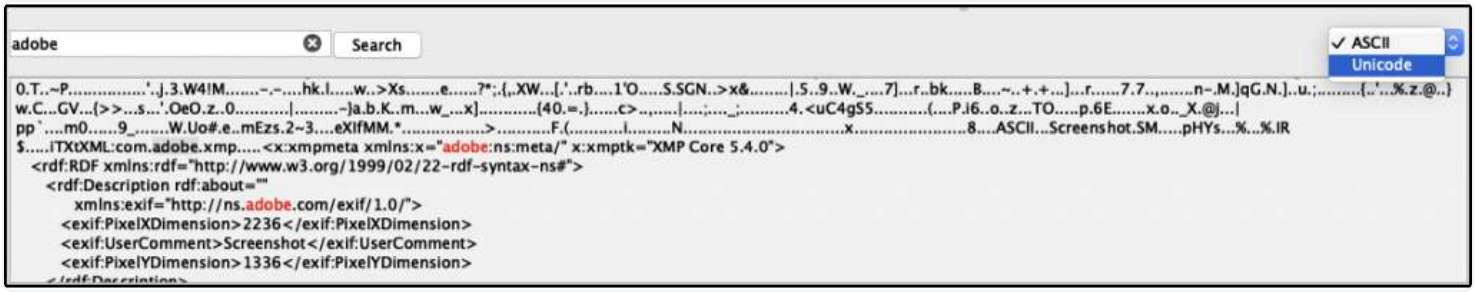
When a file is highlighted in the Main Viewer the Hex View pane will show its hex view. Both hex and ASCII will be shown.

In the example above an image file was selected.



Hex or text can be highlighted and additional options for tagging, bookmarking or copying data can be applied with a right-click.

12.8.3 Text View Pane



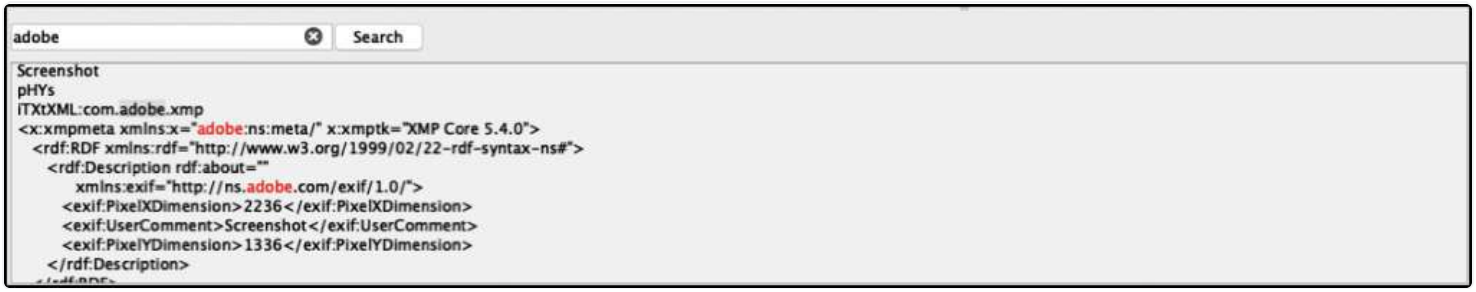
When a file or item is highlighted in the Main Viewer the Text View pane will show the file as text (ASCII) or Unicode. This can be changed with the dropdown box in the upper right corner.

The Text View pane also includes a quick search feature.

In the example above the keyword, “adobe” was entered and the “Search” button was clicked.

All instances of “adobe” are now highlighted in red.

12.8.4 Strings View Pane



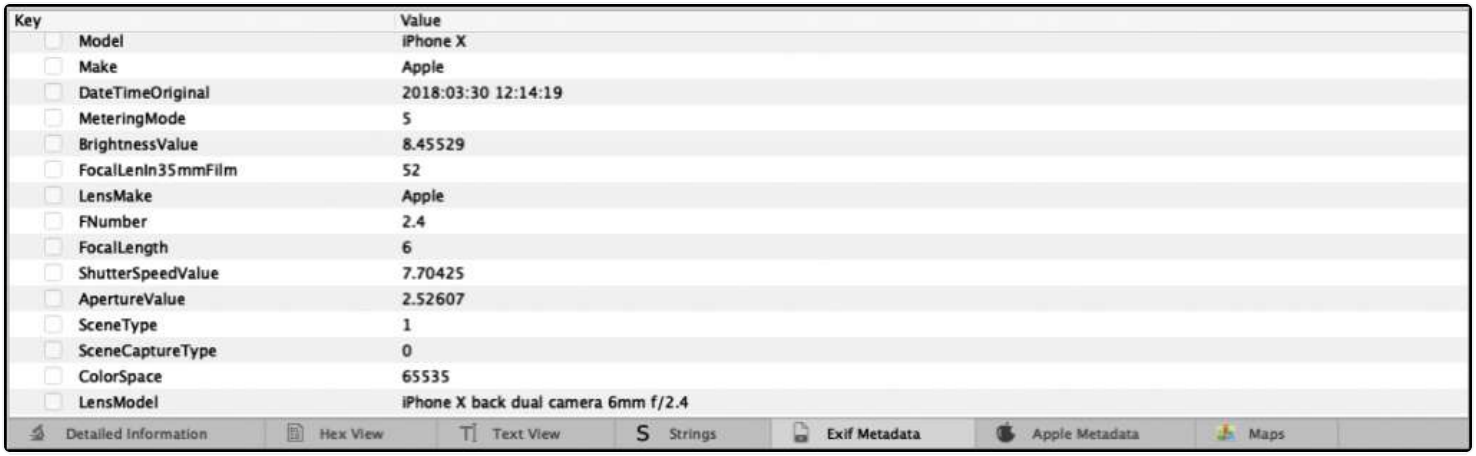
When a file or item is highlighted in the Main Viewer the Strings View pane will show the file with binary data removed (non-human readable characters).

The Strings View pane also includes a quick search feature.

In the example above the keyword, “adobe” was entered and the “Search” button was clicked.

All instances of “adobe” are now highlighted in red.

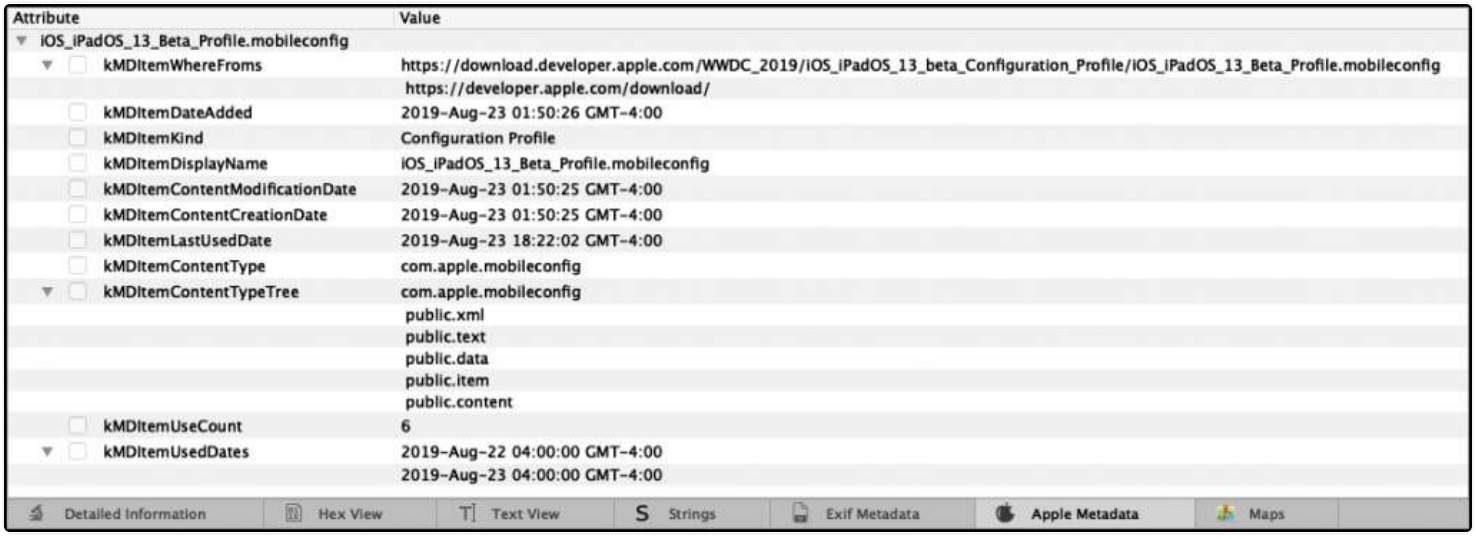
12.8.5 EXIF Metadata View Pane



When a file or item is highlighted in the Main Viewer the Exif View pane will show any Exif metadata of the file.

Clicking the checkbox next to the Exif metadata will add that information to reports.

12.8.6 Apple Metadata View Pane

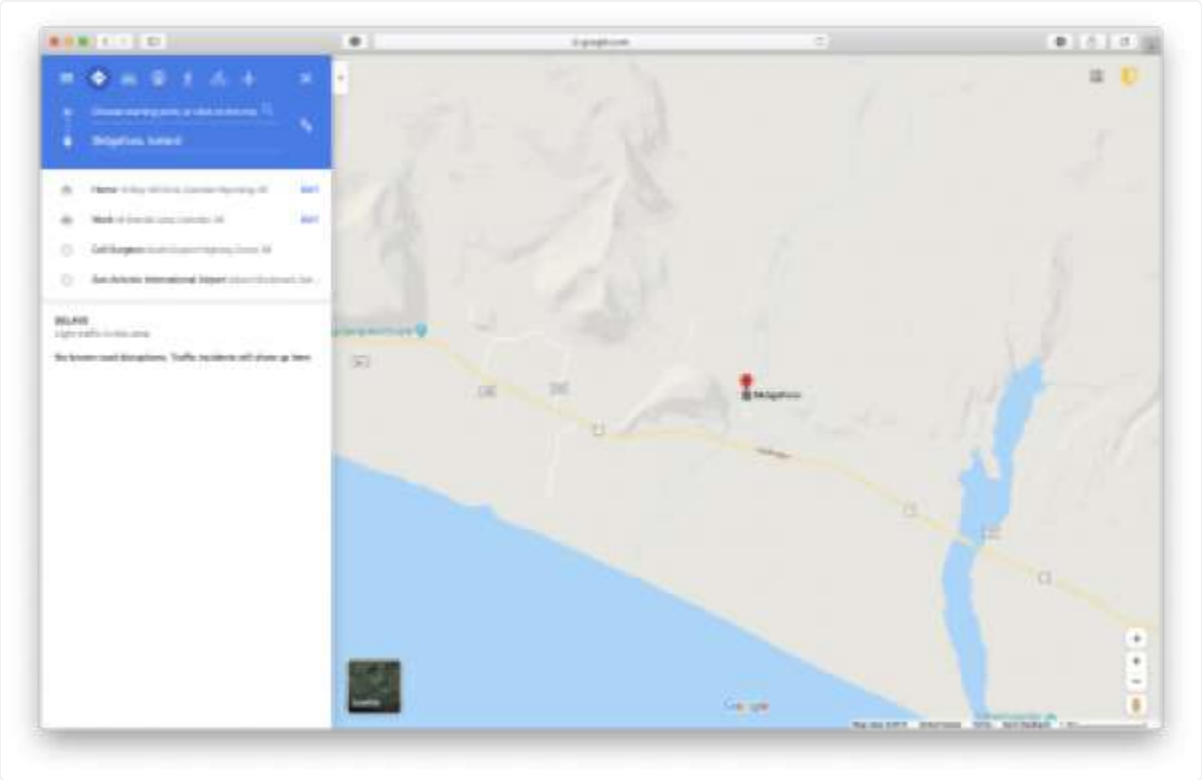


When a file or item is highlighted in the Main Viewer has Apple Extended Metadata the Apple Metadata pane will show the attributes.

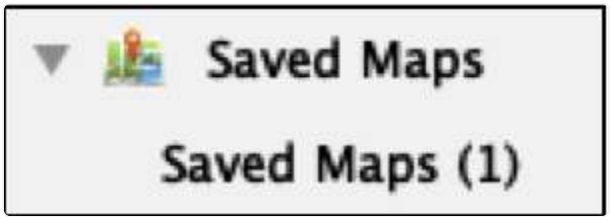
Clicking the checkbox next to an Extended Attribute will add that information to reports.

12.8.7 Maps Preview Pane

When a file or item is highlighted in the Main Viewer contains the location information the Maps Preview Pane will show the location in offline maps.



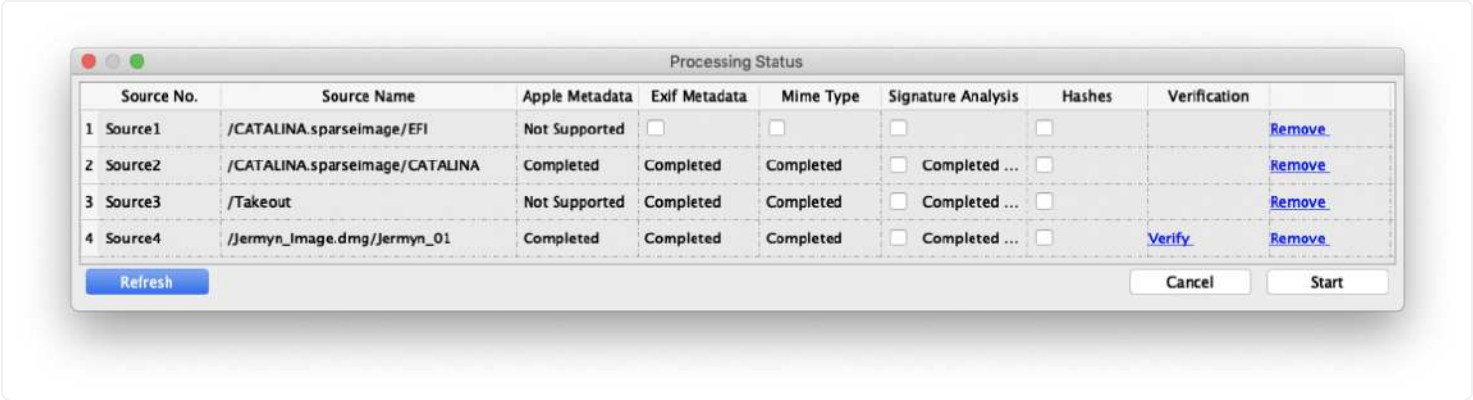
If the examination system is connected to the Internet there is the option to “Open with Google”.



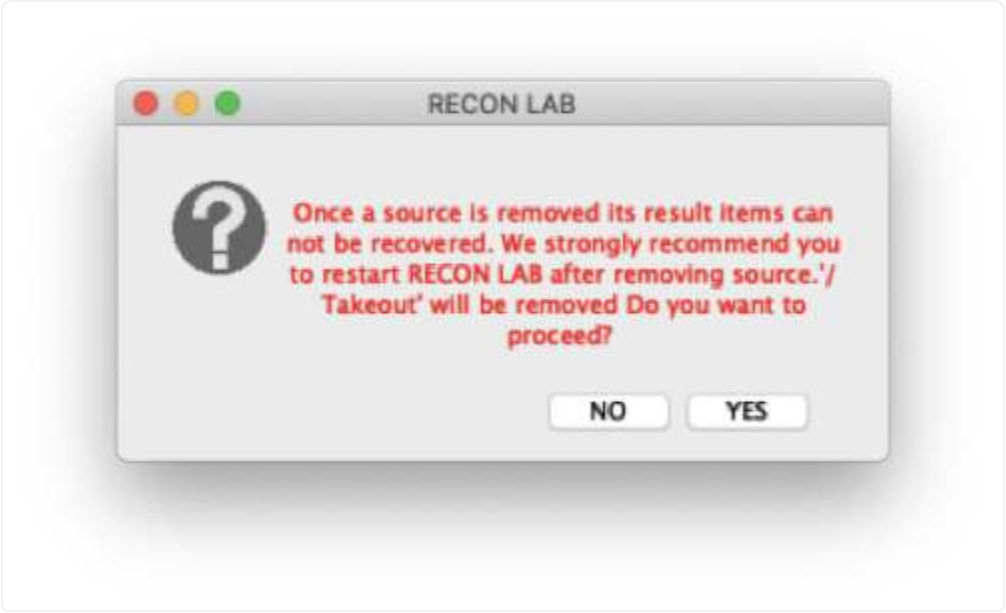
Clicking the “Save” button will bookmark the location and add the information to “Saved Maps” in the Sidebar.

13. Removing a Source

If necessary, it is possible to remove a source after the case has been processed.



To remove a source, open the Processing Status window. Identify the source to remove from the case and then click the “Remove” button.

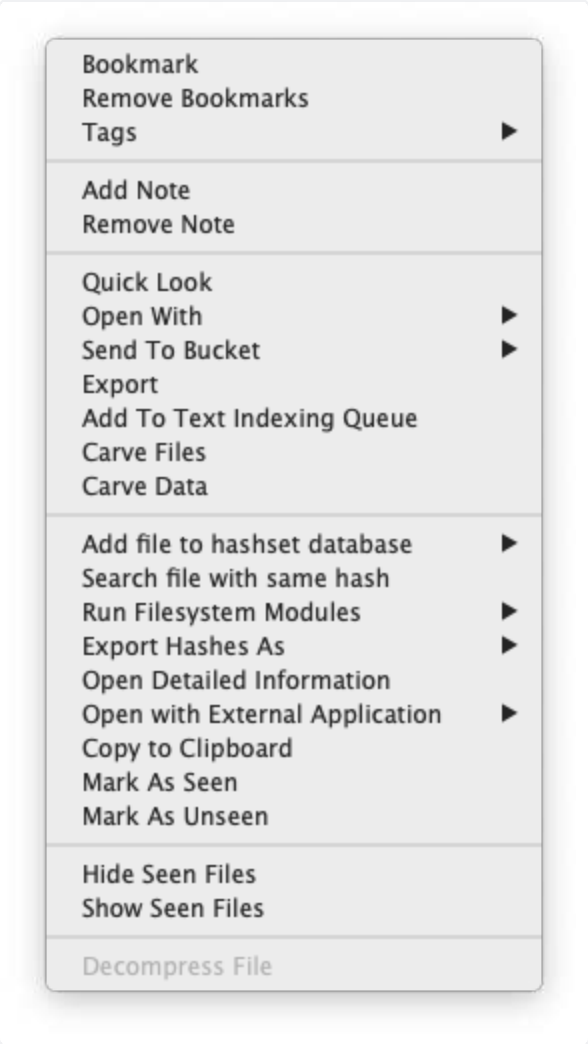


Once you choose to “Remove” a source a warning message will appear.

Make sure you quit and restart RECON LAB if you choose to remove a source.

14. Right-Click Options

Right-clicking on a file in the Main Viewer provides a host of options and features. The menus will change depending on the current window or item selected.



Add file to hash set database – Add selected file to a pre-configured hash set database.

Add Note – Allows the examiner to enter notes for a file or item.

Add to Text Indexing Queue – Adds selected files or folders to the queue as an item to be indexed.

Bookmark – Adds a basic bookmark to a file or item.

Remove Bookmarks – Removes a file's bookmark.

Carve Data – Files are searched for data such as URLs, credit card numbers, phone numbers and more.

Carve Files – Activates the built-in data carver to recover files.

Copy to Clipboard – Copies the detailed information about the file to the clipboard.

Decompress File – Expands compressed files and adds them to the case.

Export – Provides options for exporting files or directories to a .zip file or folder.

Export as KML – Creates a file in KML (Keyhole Markup Language) is supported.

Export Hashes As Vic – Option to create Project Vic hashes from selected files.

Go to Source – Opens the location where the selected file or artifact exists in the source.

Hide Seen Files – Hide files from the case marked as “Seen”.

Mark as Seen – Mark files seen by the examiner.

Mark as Unseen – Remove the “Seen” tag.

Open Detailed Information – Opens a floating window with the file or artifact’s detailed information.

Open with External Application – Open file in an external application (does not require exporting).

Open With – Opens the file in RECON LAB’s built-in Plist, Hex, SQLite or Registry Viewer.

Quick Look – Activates the macOS file viewer to preview a file or show additional information.

Remove Bookmarks – Remove the bookmark tag.

Remove Note – Removes examiner's notes for a file or item.

Run Filesystem Modules – Run file system modules against individual files or directories.

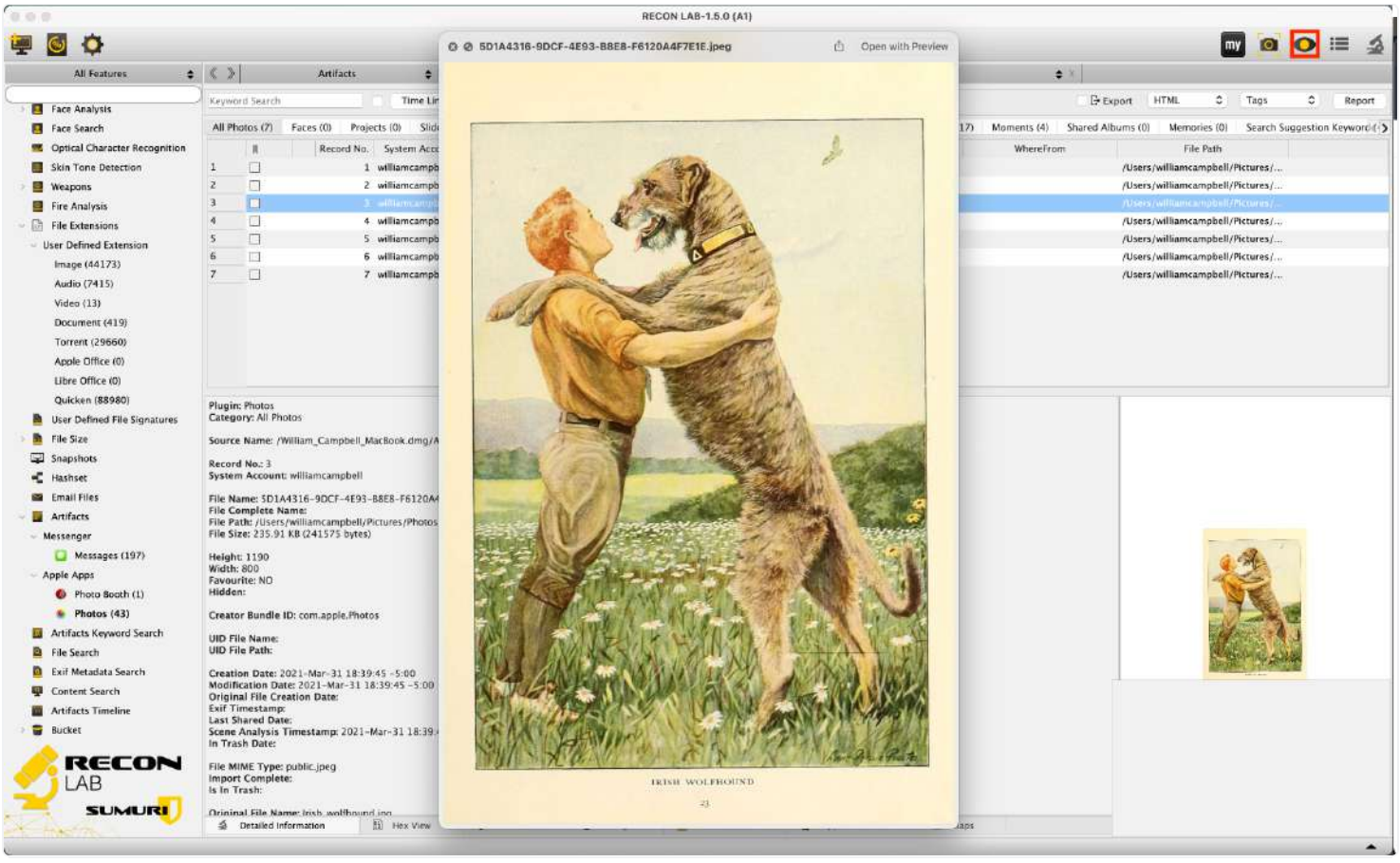
Search file with the same hash – Finds any files with the same hash in pre-configured hash sets.

Send to Bucket – Sends the file to RECON LAB's built-in Plist, Hex, SQLite or Registry Viewer in the Sidebar in the "Bucket" category.

Show Seen Files – Unhide files marked as "Seen" and hidden.

Tags – Allows the examiner to "tag" a file with a color or custom name.

15. Previewing Files



RECON LAB supports previewing hundreds of file types even if the parent applications are not installed. For example, if MS Word is not installed, RECON LAB can still preview the MS Word document file.

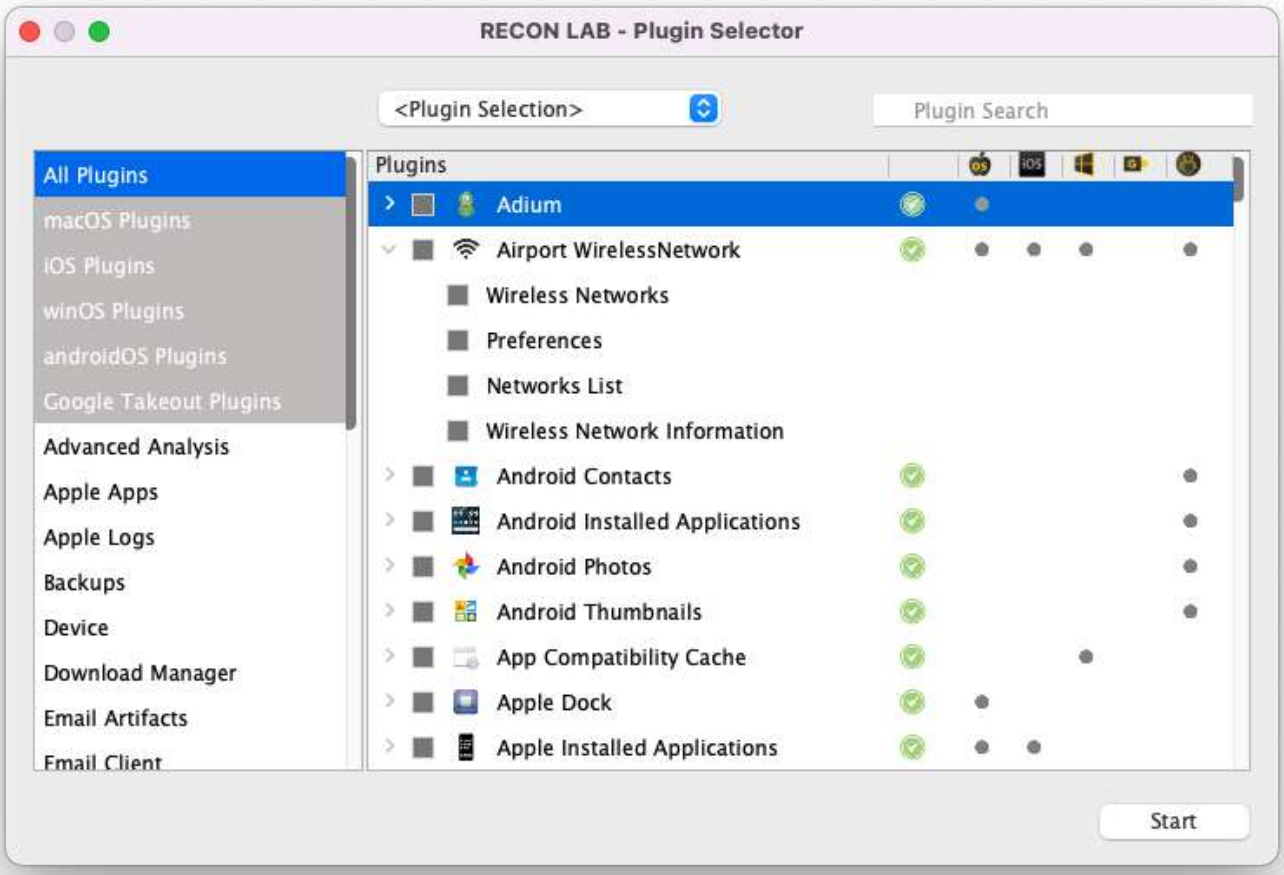
As RECON LAB is designed on a Mac it takes advantage of macOS's Quick Look. To activate Quick Look to preview a file right-click and select "Quick Look" or tap your spacebar.

Additionally, you can highlight a file and click the Quick Look in the Top Menu.

16. Automated Analysis

RECON LAB includes hundreds of plugins that recover thousands of artifacts automatically from Windows, macOS, iOS, Android and Google Takeout.

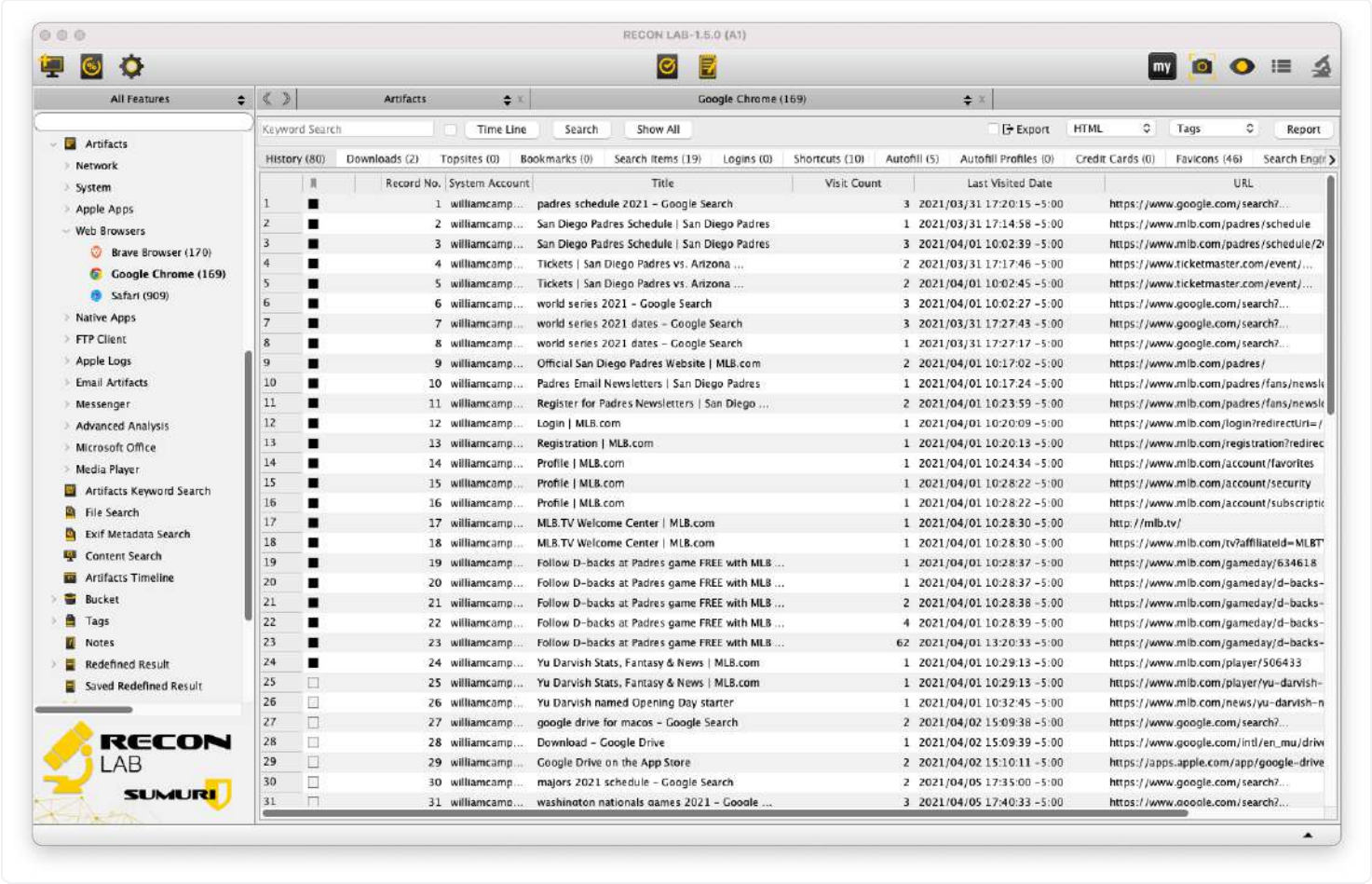
To have RECON LAB automatically recover artifacts click the "Run Artifacts" button to bring up the configuration window. Refer to the "Artifact and Plugin" section of this manual found under "Configuration" for information on using this module.



Select the artifacts of interest and click “Start”.

Once completed the recovered artifacts will populate in the sidebar under the “Artifacts” category.

Each artifact group can be expanded by clicking its triangle icon.

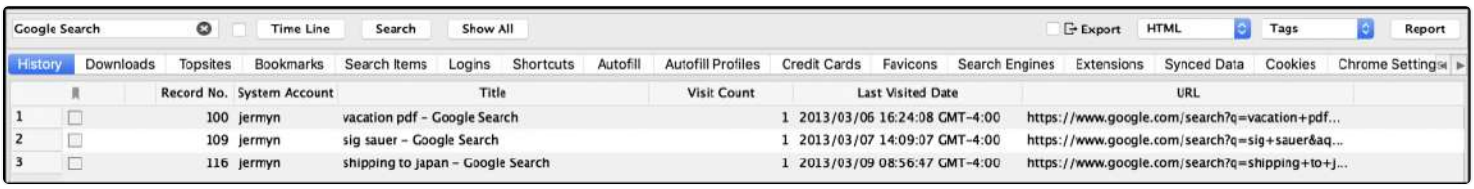


The number listed next to the plugin is the number of artifacts recovered. Double-clicking on the plugin opens the data in the Main Viewer window.

Plugins can have multiple artifacts that are usually separated into tabs. In the previous example, the Google Chrome plugin is selected and the “History” tab is highlighted. The “History” tab is showing all of the Google Chrome history recovered from the sources.

Filtering Data with Keyword Searches

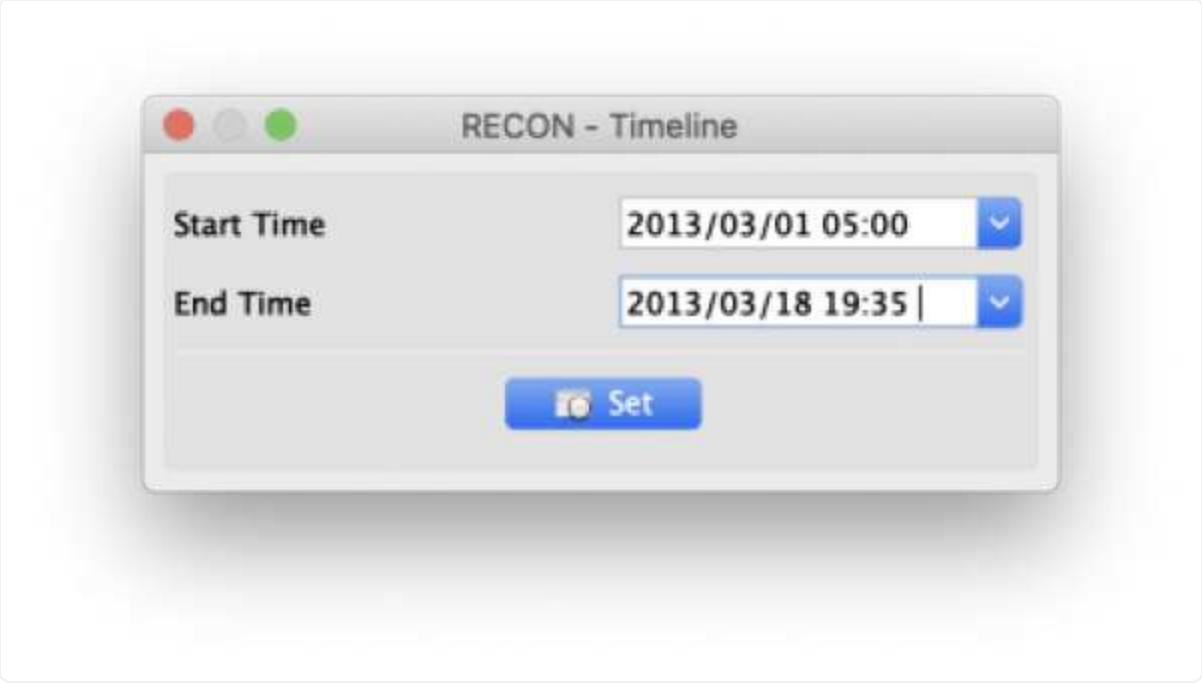
There is the ability to search within this plugin to filter the data using the Keyword Search box.



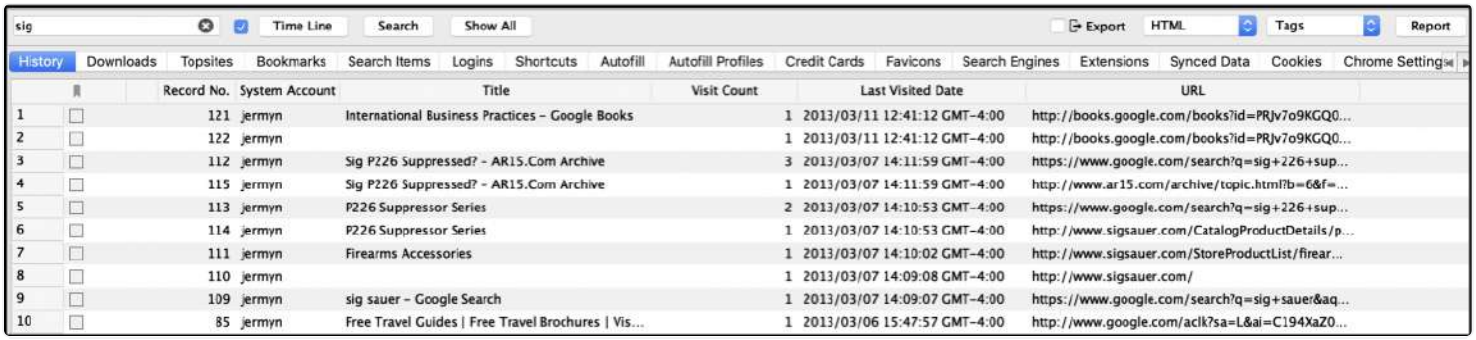
Using the Keyword Search box the keyword “Google Search” was entered. RECON LAB quickly filters the data to show any Google Chrome history with the keyword “Google Search”.

Setting a Timeline to Filter Data

An examiner can refine the results of a data query to a specific date range by clicking the “TimeLine” button.



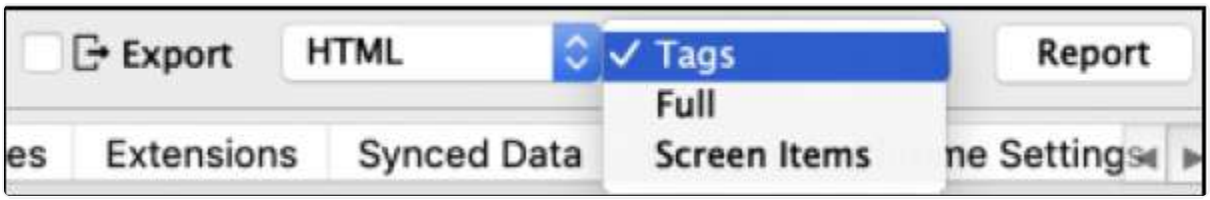
Data can be filtered by setting a **Start Time** and an **End Time** and clicking the **Set** button.



Activate the set timeline by checking the box next to the “Time Line” button and click **Search**.

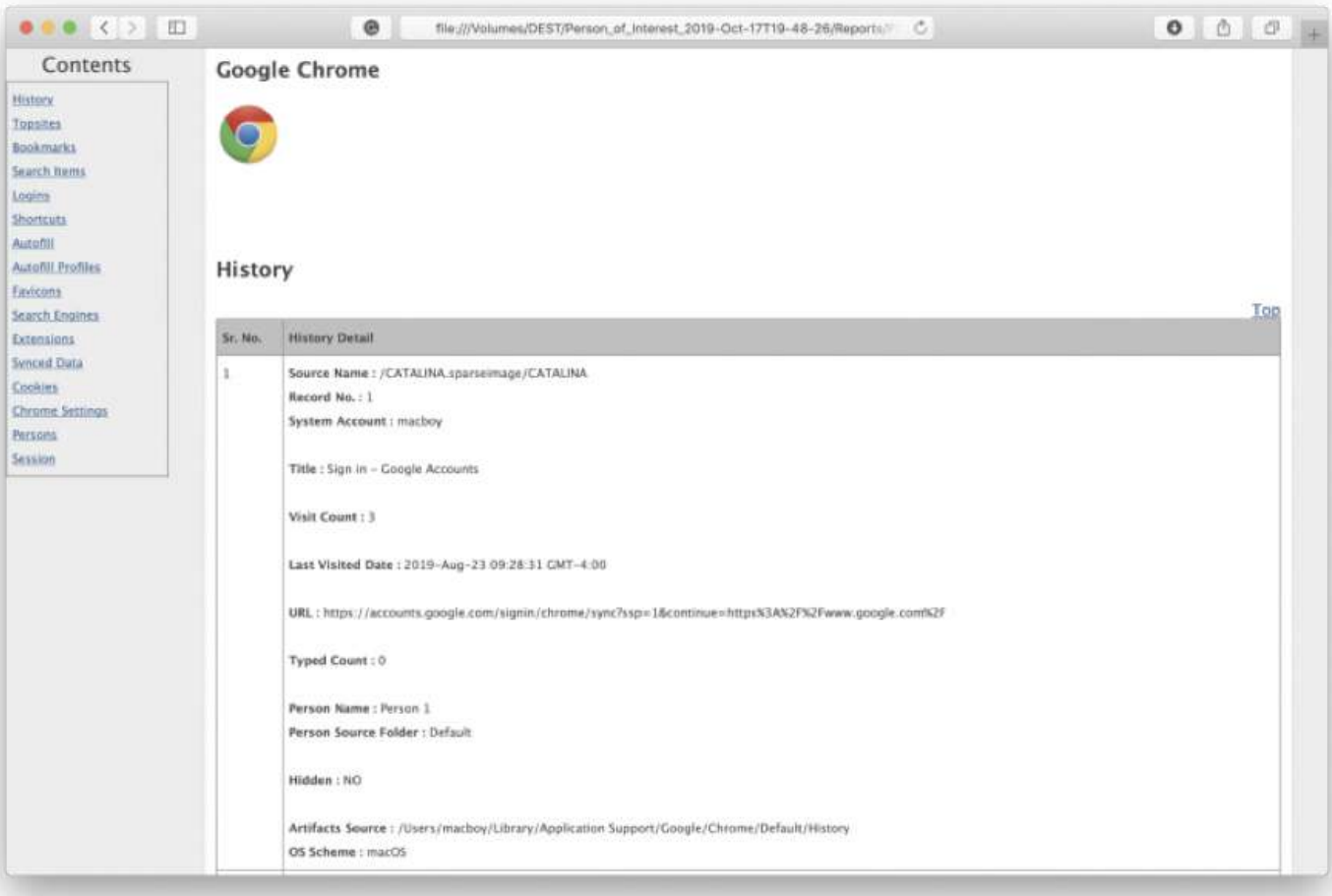
Generating Reports from Plugin Window

Reports in various formats can easily be generated from the plugin window. Reports can be in HTML, PDF, CSV, XML or KML formats. (Note: KML formatting is only supported for plugins with location data)



Reporting options include Tags (bookmarks), the Full module or just the items on the screen.

If interested in exporting associated files the examiner can click the “Export” button.

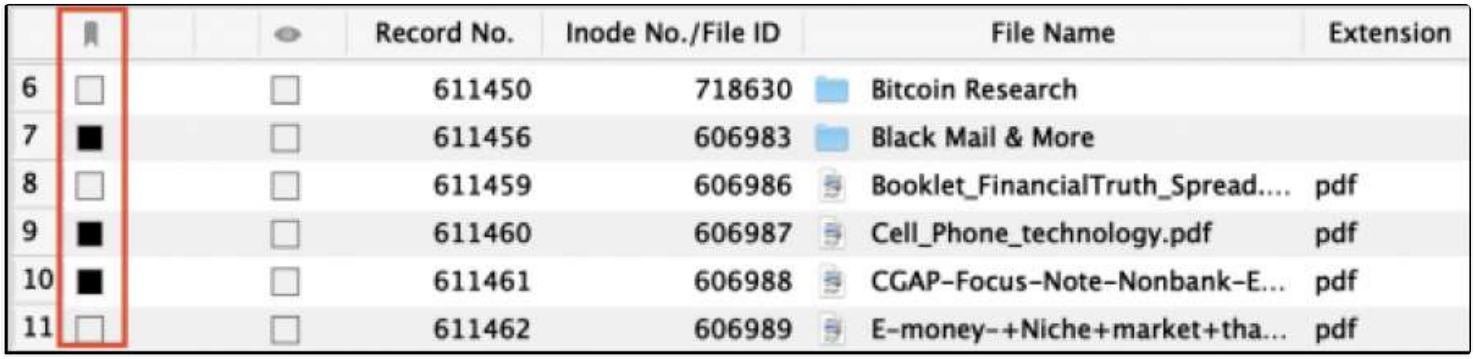


Once you have bookmarked items of interest and you have chosen your reporting settings click “Report”. RECON LAB will ask if you want to open the report once it is generated.

17. Bookmarks and Tagging Evidence

17.1 Bookmarks

Bookmarks are the simplest way to mark items of interest in RECON LAB. In almost every area of RECON LAB there will be a checkbox next to any item that can be bookmarked. To bookmark a file just check the box with the “bookmark” icon in the column.

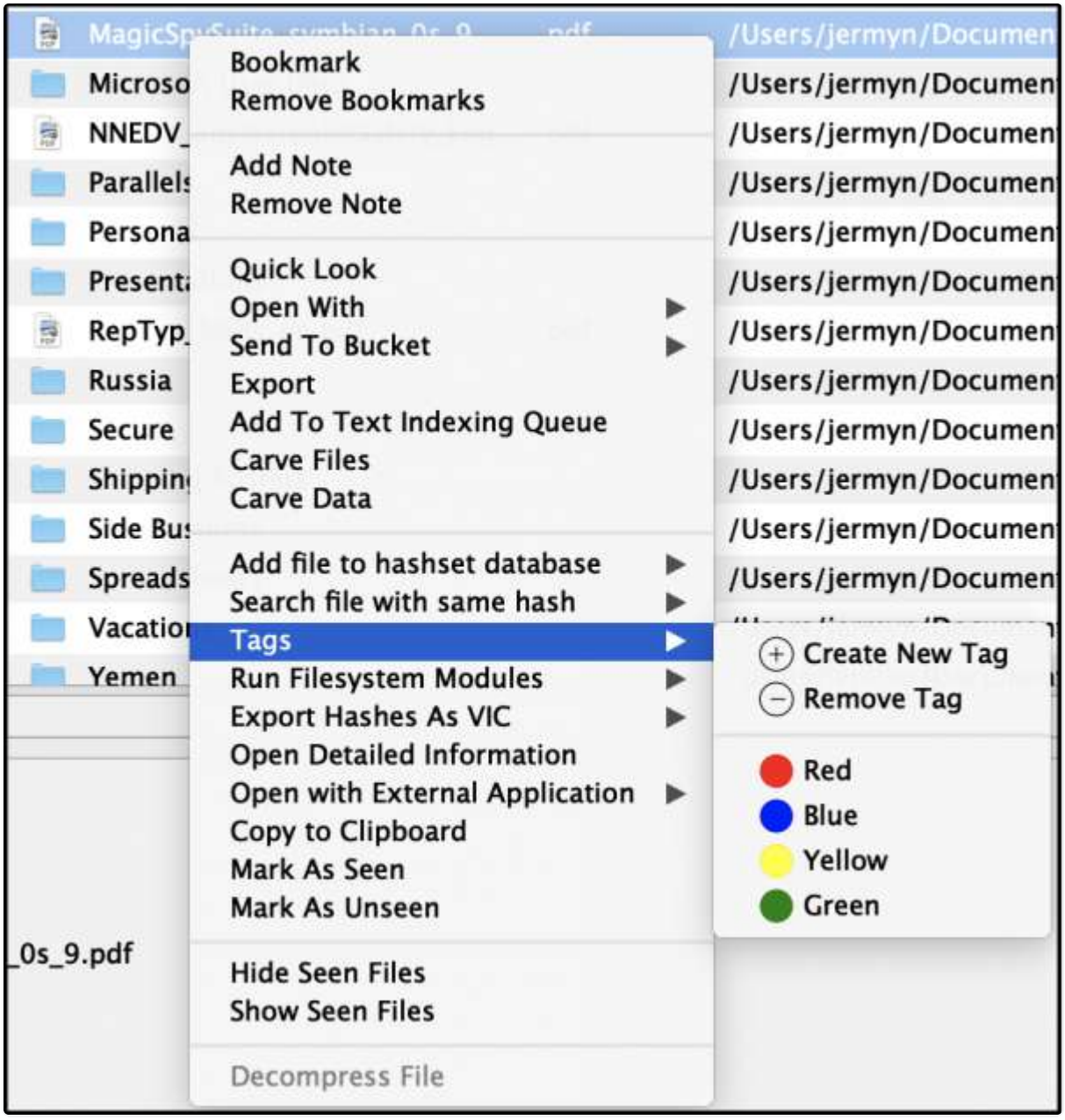


			Record No.	Inode No./File ID	File Name	Extension
6	☐	☐	611450	718630	Bitcoin Research	
7	■	☐	611456	606983	Black Mail & More	
8	☐	☐	611459	606986	Booklet_FinancialTruth_Spread....	pdf
9	■	☐	611460	606987	Cell_Phone_technology.pdf	pdf
10	■	☐	611461	606988	CGAP-Focus-Note-Nonbank-E...	pdf
11	☐	☐	611462	606989	E-money-+Niche+market+tha...	pdf

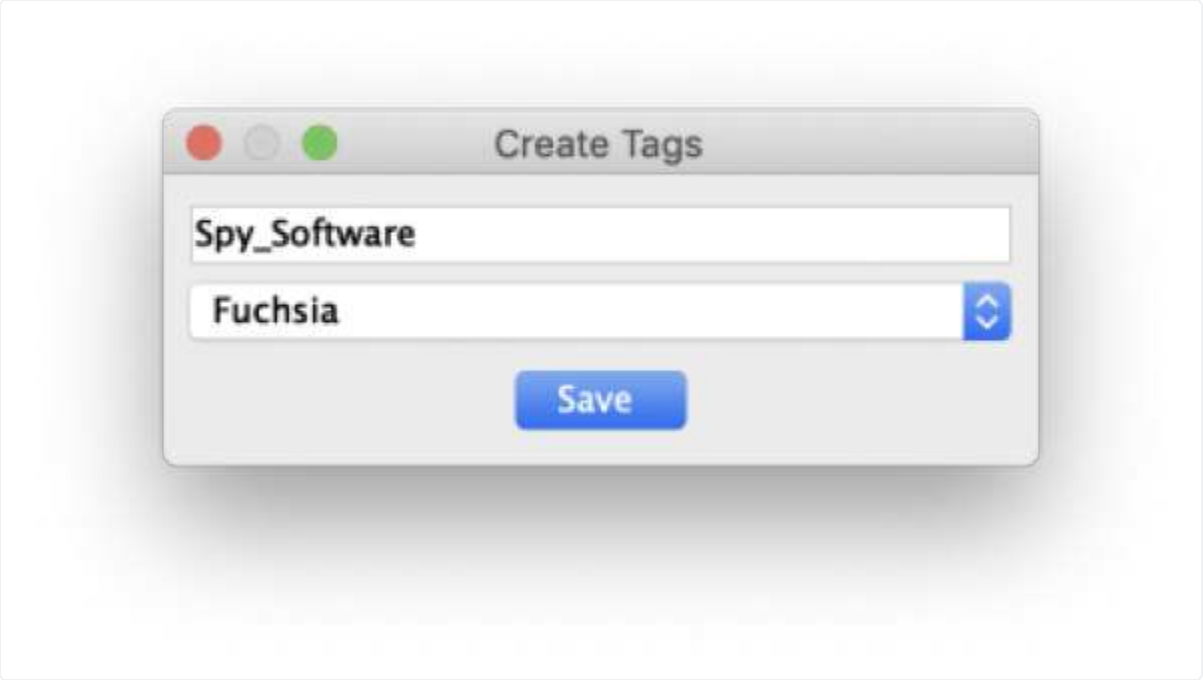
Files can also be bookmarked via the right-click options or by using the “B” key.

17.2 Tags

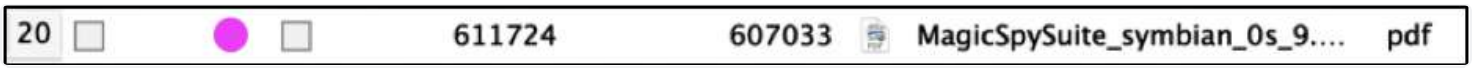
Tags are custom bookmarks. Tags can be colored markers, custom names or both.

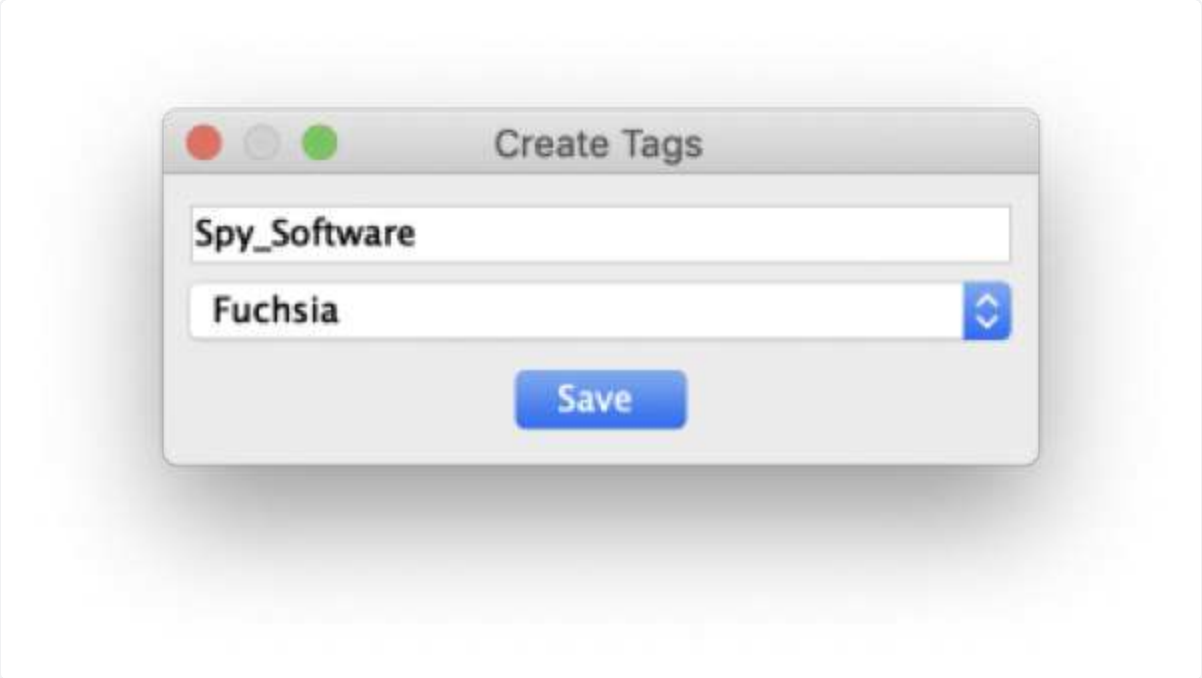


Tags are created by right-clicking on the item of interest and selecting “Tags”. An examiner can select one of the four colors to tag the file or “Create New Tag”.



Selecting “Create New Tag” allows the examiner to create a new Tag Category and assign a color (optional).





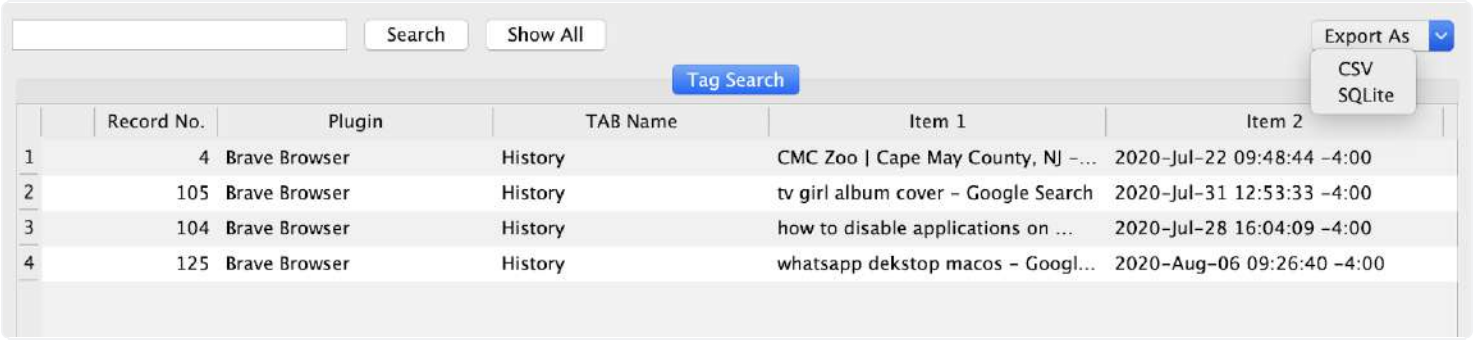
Clicking “Save” will tag the file with the new tag name and color in the Table View and in the Detailed Information.

17.3 Finding Tags and Bookmarks in Sidebar

Tags and bookmarks can always be located, accessed and sorted in the Sidebar.

17.3.1 Exporting Tags

Tags can be exported as CSV or SQLite files when opened in the Sidebar pane.



	Record No.	Plugin	TAB Name	Item 1	Item 2
1	4	Brave Browser	History	CMC Zoo | Cape May County, NJ -...	2020-Jul-22 09:48:44 -4:00
2	105	Brave Browser	History	tv girl album cover - Google Search	2020-Jul-31 12:53:33 -4:00
3	104	Brave Browser	History	how to disable applications on ...	2020-Jul-28 16:04:09 -4:00
4	125	Brave Browser	History	whatsapp dekstop macos - Googl...	2020-Aug-06 09:26:40 -4:00

17.5 Removing Tags and Bookmarks

To remove a Tag or Bookmark from any item of interest simply right-click and select “Remove Bookmark” or “Tags -> Remove Tag”.

18. Indexing

With the increased size of media and the number of sources seized RECON LAB takes a different approach to indexing.

Traditionally, forensic tools gave the examiner the option of indexing everything or not at all. Examiner dreaded the thought of a full index due to long processing times.

RECON LAB handles index at a granular level using the leading indexing and search solution – dtSearch.

With RECON LAB an examiner has the ability to index a single file, the entire source or any combination in-between. Additionally, with the ability to white-list or black-list files RECON LAB's indexing is intelligent and useful.

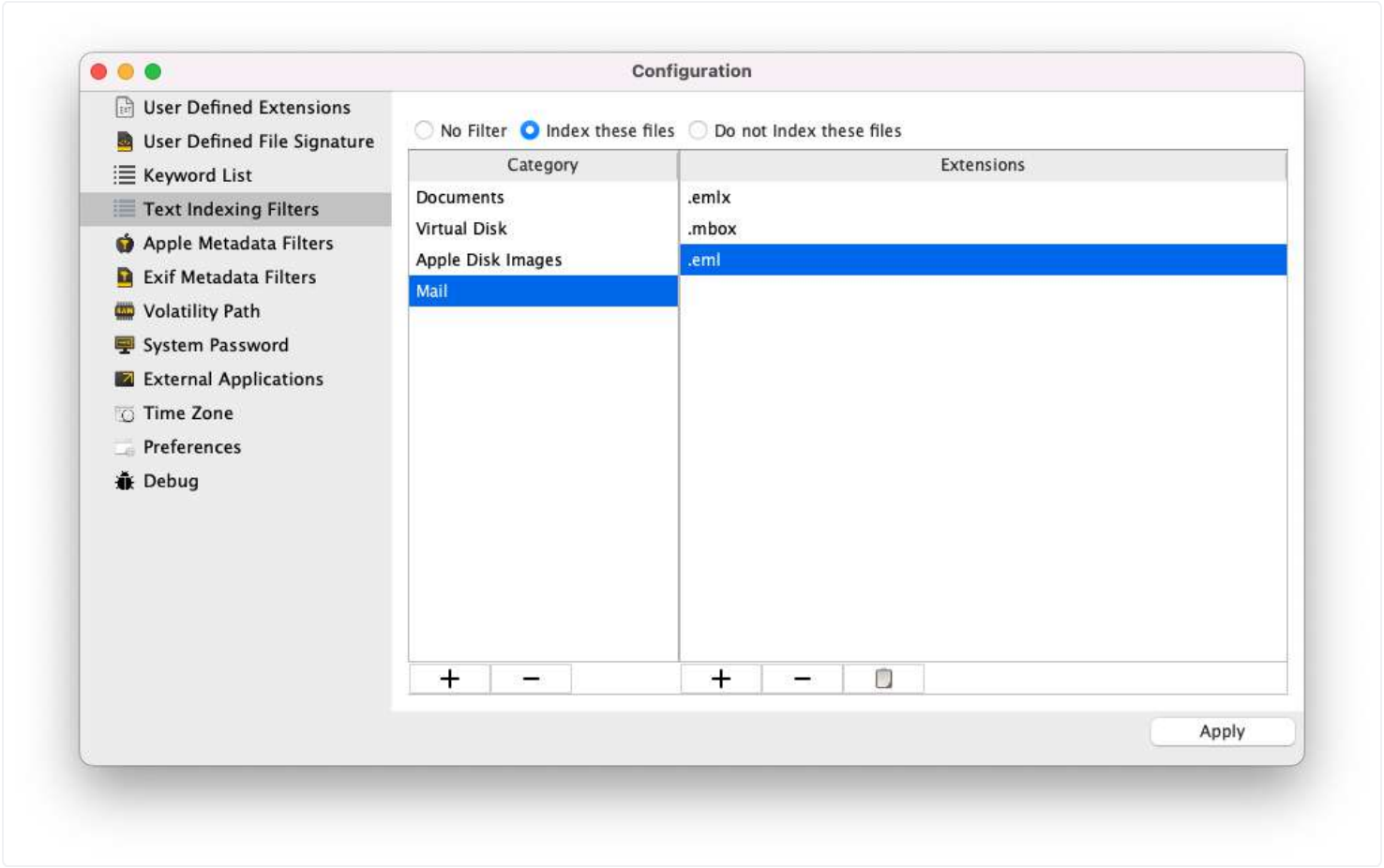
The goal is to perform surgical indexing and searches to find the information needed in less time.

Indexing Example with RECON LAB

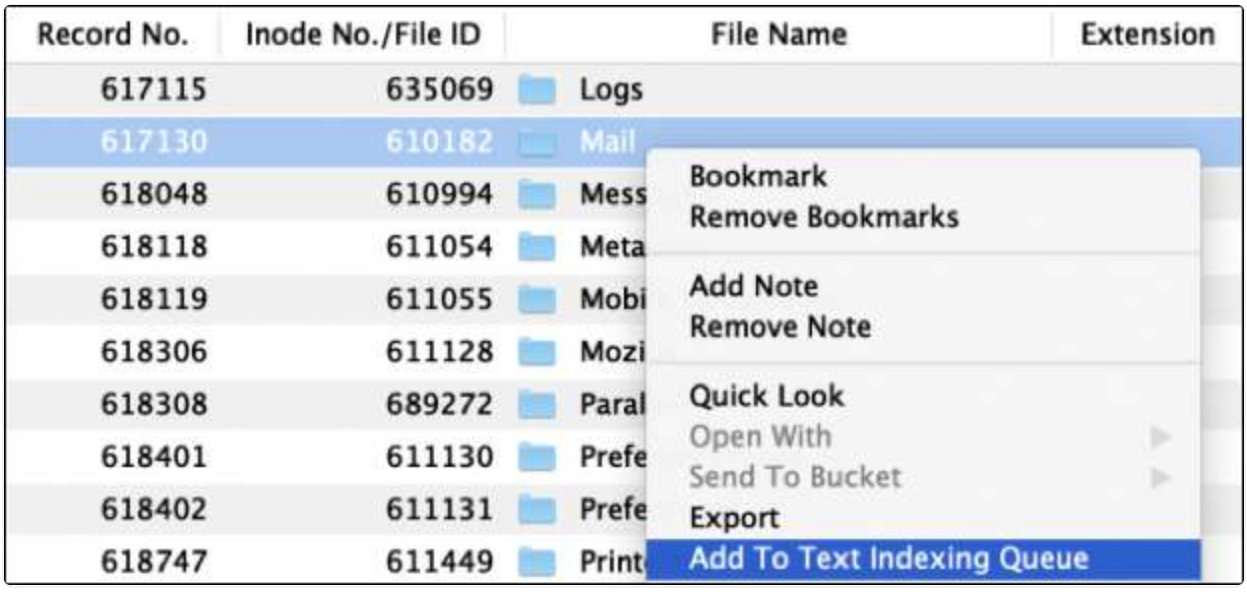
Let's use this as an example. You are tasked with finding any emails containing information about a company named "SUMURI" and we know the person of interest uses the Apple Mail client. You had the ability to image his company MacBook and are now performing the analysis.

The caveman approach is to index everything and wait days for the indexing to finish.

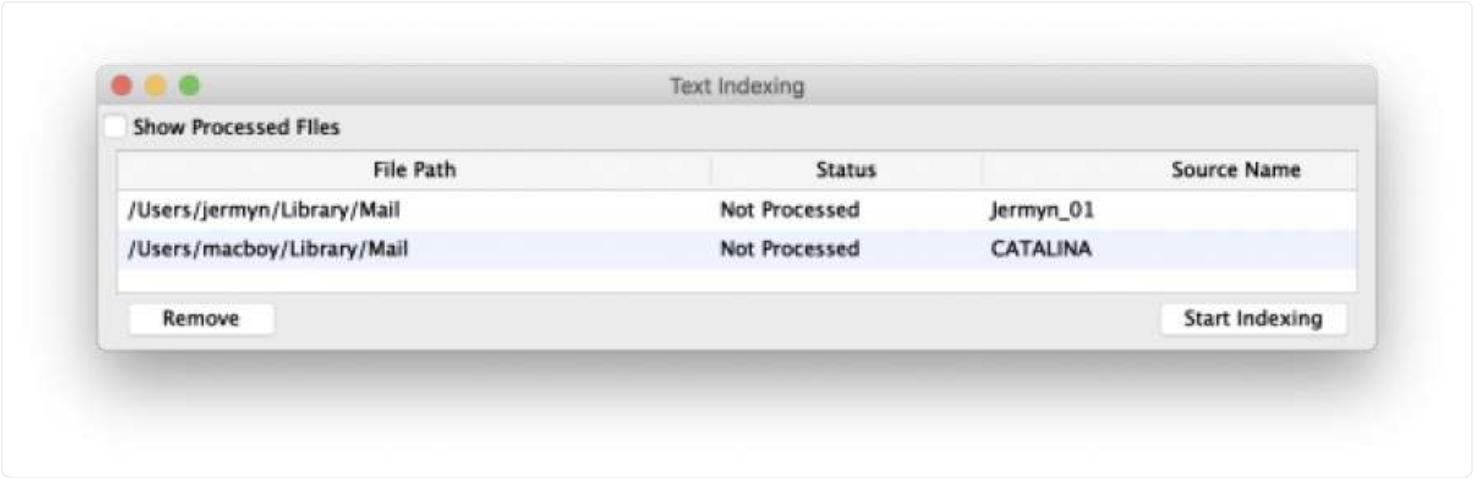
Or, we can use RECON LAB's indexing in a more intelligent way.



We start by setting up a white-list in the Configuration Text Indexing Filters. Here we create a category for “Mail” and add Apple Mail file formats (.eml, .emlx. .mbox), select “Index these files”, then “Apply”.



We now navigate to the folders where the Apple Mail client stores emails and “Add to Text Indexing Queue” using the right-click option.



We now select Text Indexing from the Top Menu and confirm that the files or directories that we want to parse are there. We now click “Start Indexing”.

	Record No.	File Name	File Size	Mime Type	Extension	Number of hits	Keyword Hit
120	1244917	2150.partial.emlx	3424	text/plain	emlx	5	SUMURI
121	1244919	2152.emlx	2122	text/plain	emlx	5	SUMURI
122	1244921	2154.emlx	1112	text/plain	emlx	5	SUMURI
123	1244938	2171.emlx	869	text/plain	emlx	5	SUMURI
124	1244941	2174.partial.emlx	1334	text/plain	emlx	5	SUMURI
125	1244960	2193.partial.emlx	1282	text/plain	emlx	5	SUMURI
126	1244963	2196.partial.emlx	7717	text/plain	emlx	5	SUMURI
127	1245271	402.emlx	1910	text/plain	emlx	5	SUMURI
128	1245272	403.emlx	1910	text/plain	emlx	5	SUMURI

After indexing is complete we can now perform a Content Search for the keyword “SUMURI” and review the results.

We can preview the email hits using Quick Look or any of RECON LAB's other viewers.

19. Search Options

RECON LAB has many different ways to search for files and data. They can be broken into two categories. The first are "local" searches that relate to individual Plugin results and Viewers. The second are "global" searches that search across all sources and their data.

Local Search Options

- Keyword search and filters within the Plugin results view.
- Keyword search and filters within viewers (Hex, Text, Strings, etc.)

Global Search Options

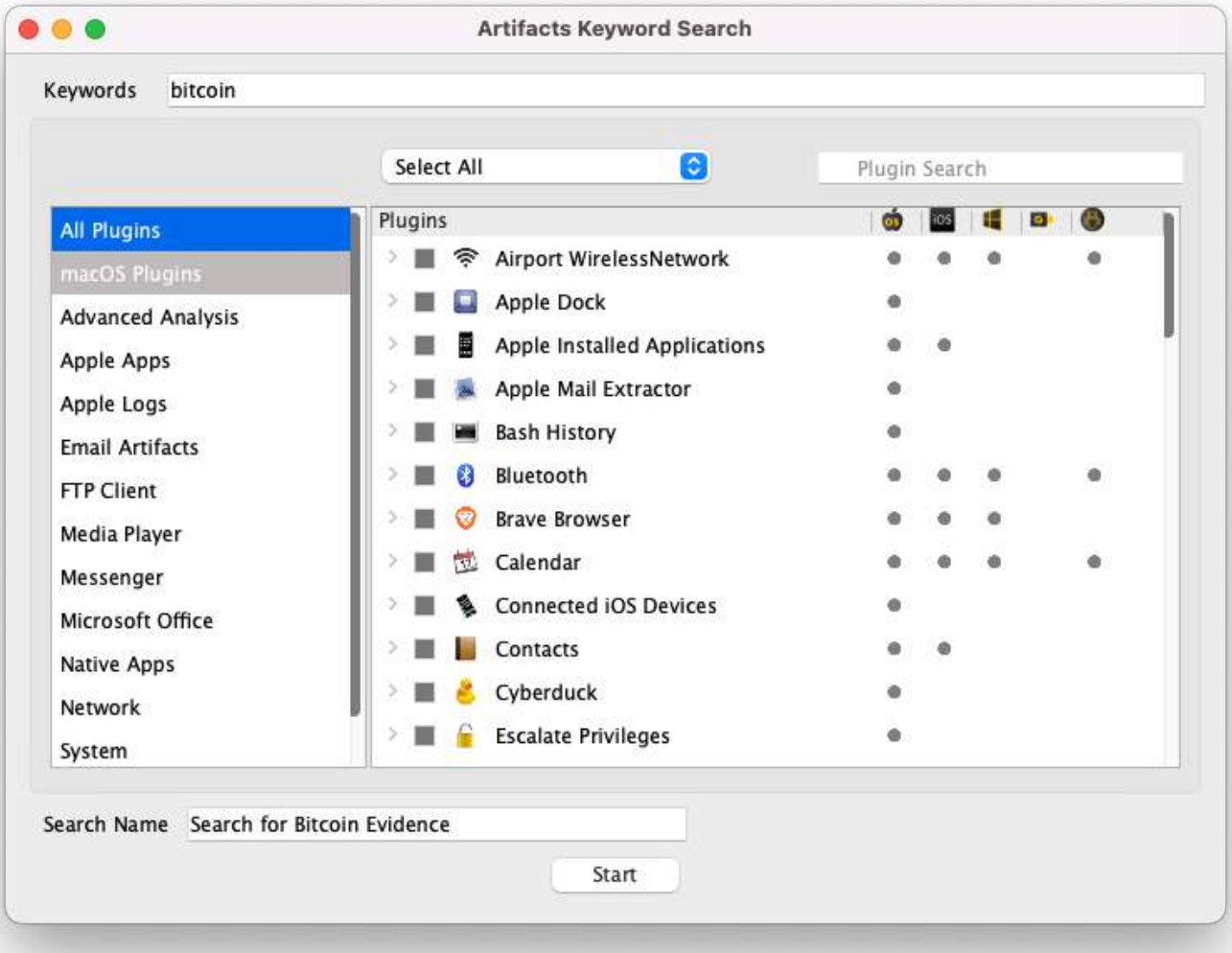
- Artifact Keyword Search
- File Search
- Content Search
- Apple Extended Metadata Search
- EXIF Metadata Search

19.1 Artifacts Keyword Search

As mentioned earlier, RECON LAB can automatically parse and recovery thousands of artifacts from Windows, macOS, iOS, Android and Google Takeout. An examiner can quickly search through these results using the Artifacts Keyword Search.

The Artifacts Keyword Search can be used to create custom searches by selecting any combination of artifacts.

To start a search of the recovered artifacts select Search > Artifact Keyword Search from the Menu Bar.

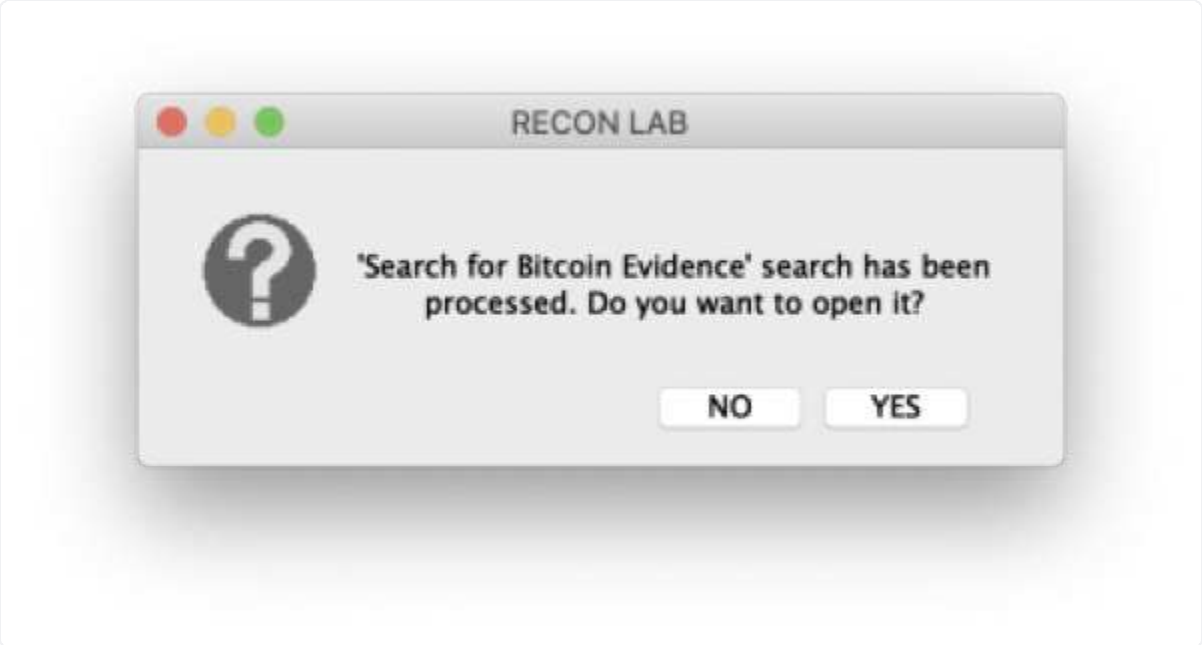


Enter a keyword and select the plugins of interest for the search. If you would like to enter more than one keyword at a time separate the keywords with a comma and no space. For example, if you want to search for the keywords “apples, oranges and bananas” enter the keywords as:

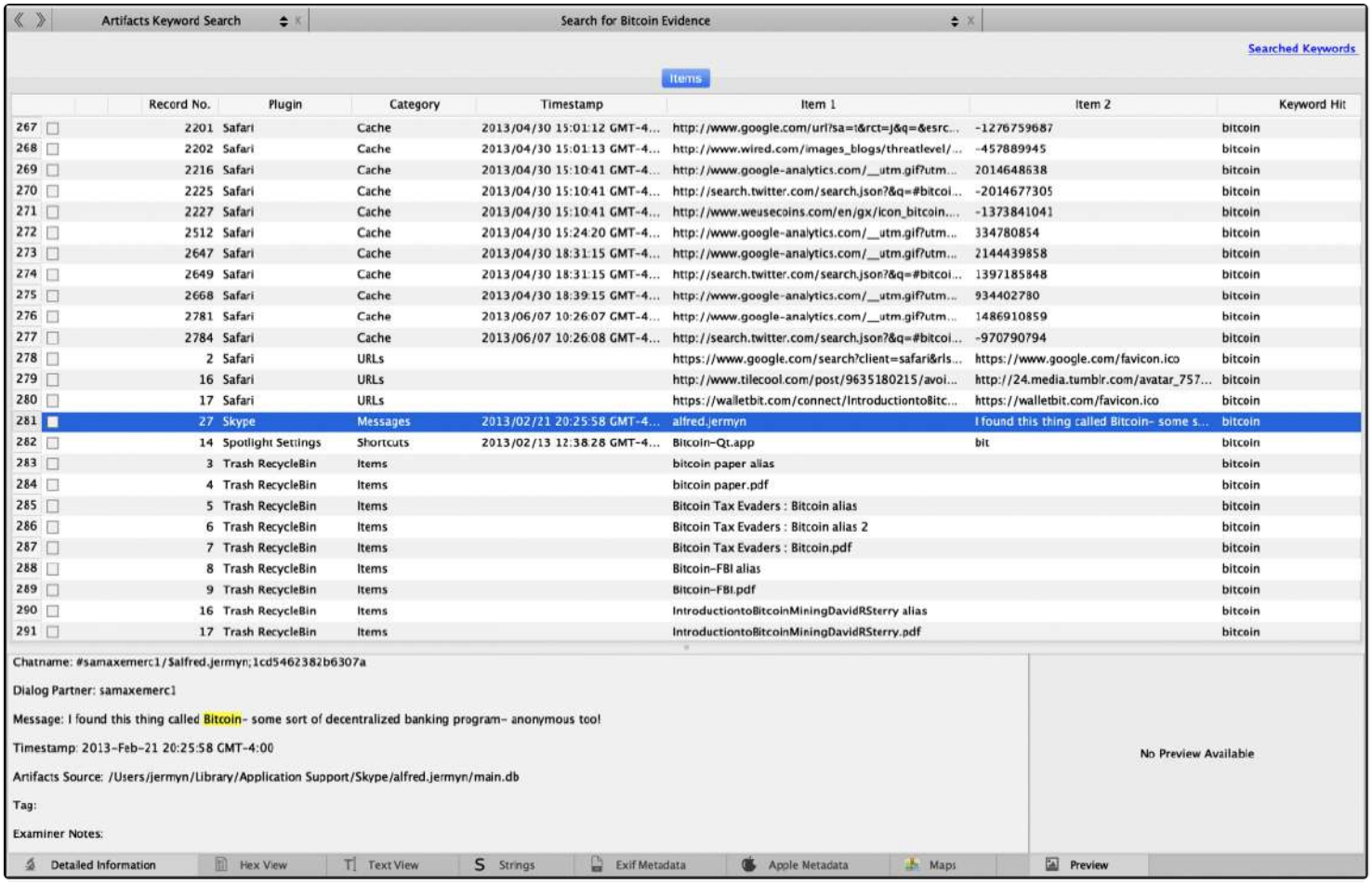
apples,oranges,bananas

After entering your keywords, provided a name for the search than click “Start”.

In the example above the examiner is searching for the keyword “bitcoin”. All Plugins were selected using the dropdown box and the name for the search was “Search for Bitcoin Evidence”.



Once the search is complete you will have the option of reviewing the results.



If you select “Yes” the results will appear in the Main Viewer.

Any plugin with a keyword hit will be displayed in a table view for review. As you can see above the keyword “bitcoin” was found in many plugins (i.e. Safari, Skype, Spotlight, Trash).

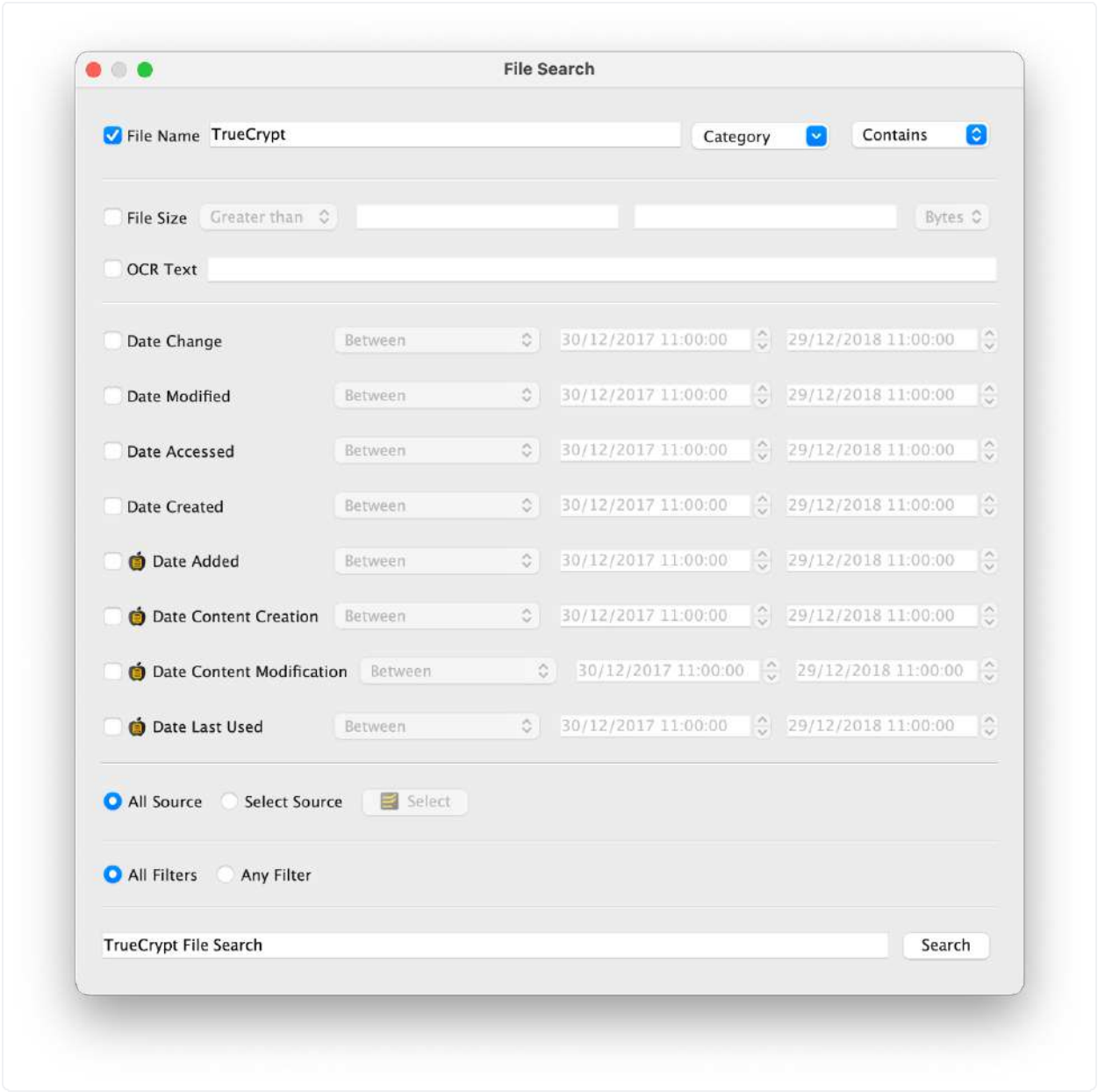
The results can now be reviewed, examined in more detailed or bookmarked.

All Artifacts Keyword Searches are saved to the Sidebar for review at any time.

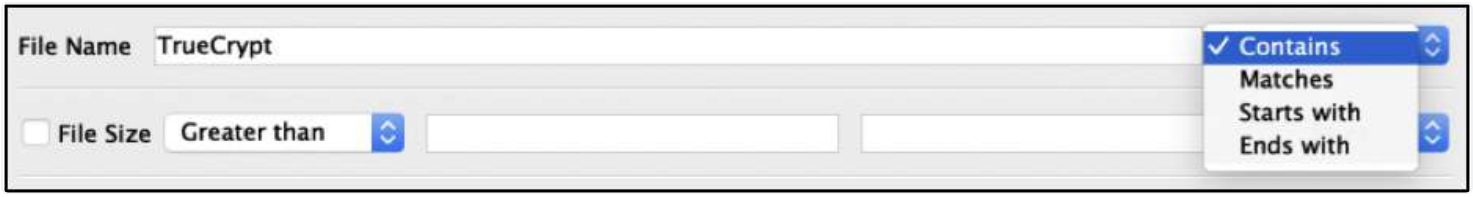
19.2 File Search

RECON LAB's File Search can be used to search by file and folder names along with file size and their dates and times. This is not a content search.

To start a File Search, select Search > File Search from the Menu Bar.

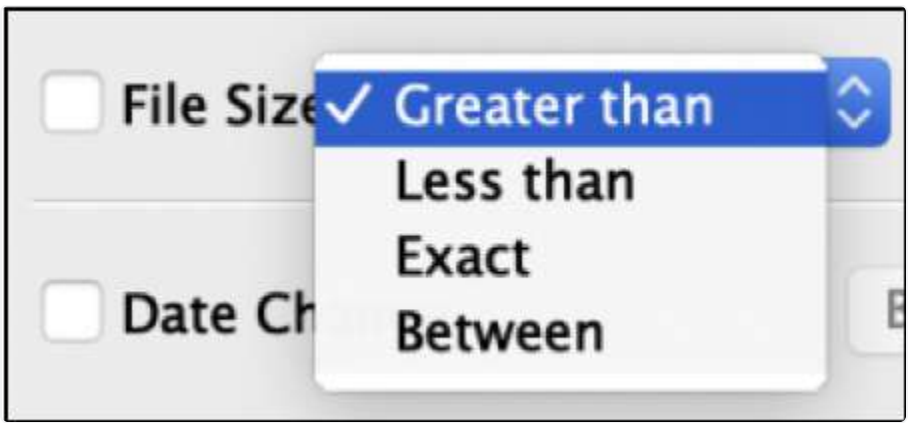


The File Search configuration window will appear.

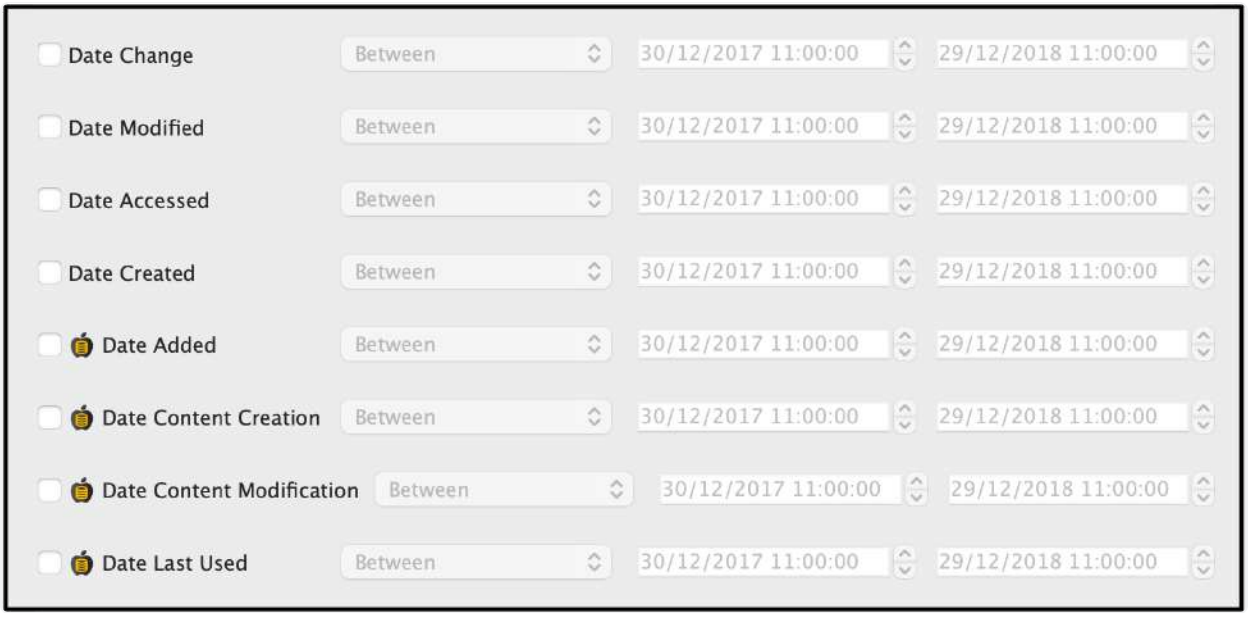


Use the File Name field to enter the keyword to be searched. Options for the file name can be “Contains, Matches, Starts with, Ends with”.

File Size can be used as a parameter for the search.



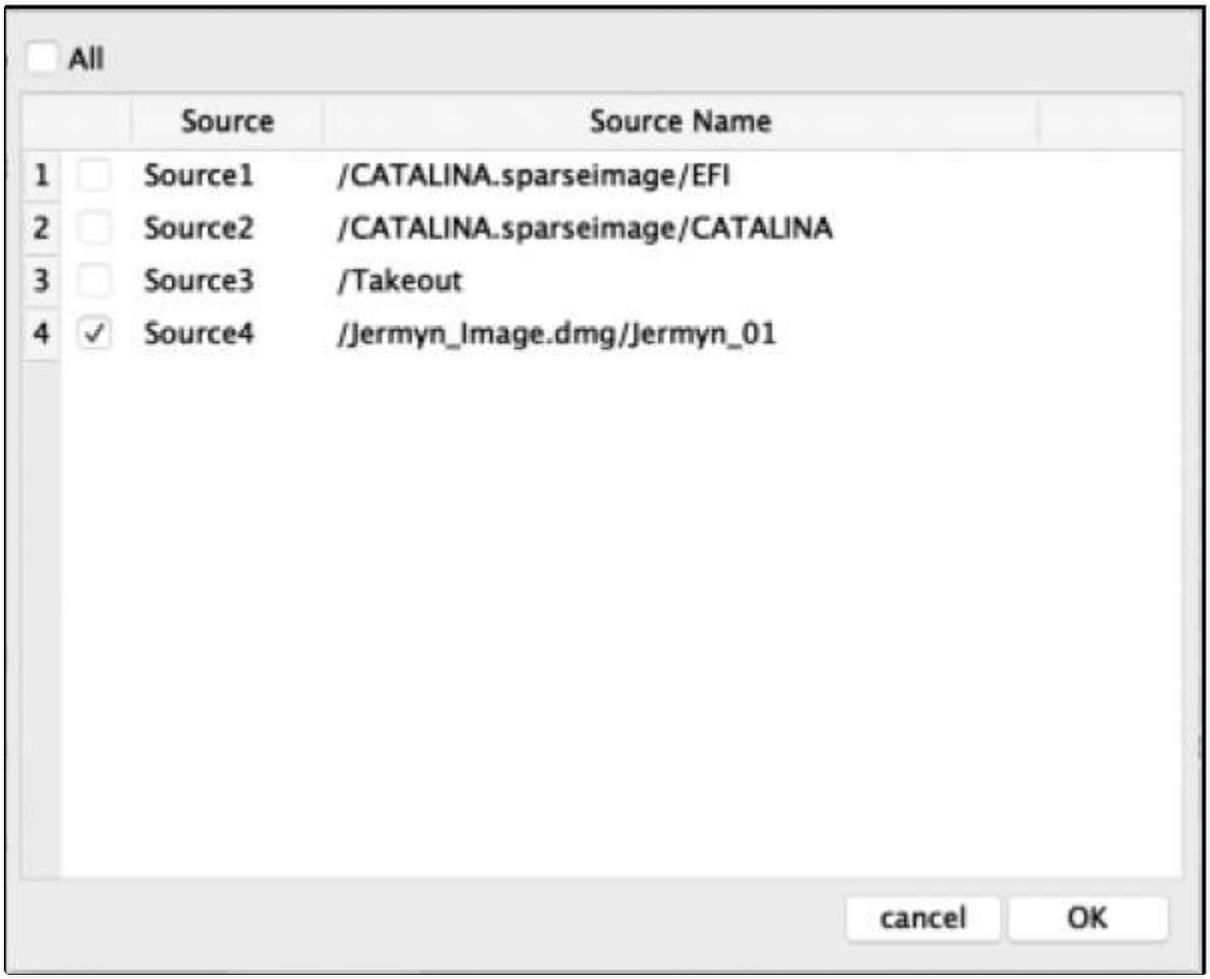
To activate File Size filters, check the box next to File Size. Options for the File Size filter can be “Greater than, Less than, Exact, Between”. Also, as seen above, the unit of measure for the file size can also be adjusted.



Both standard date attributes and Apple Extended Attributes can be used as filters for a File Search as well.

To activate any Date filter just check the box next to the date attribute to be used. Additional options for the date filter are “Between, Before, After”.

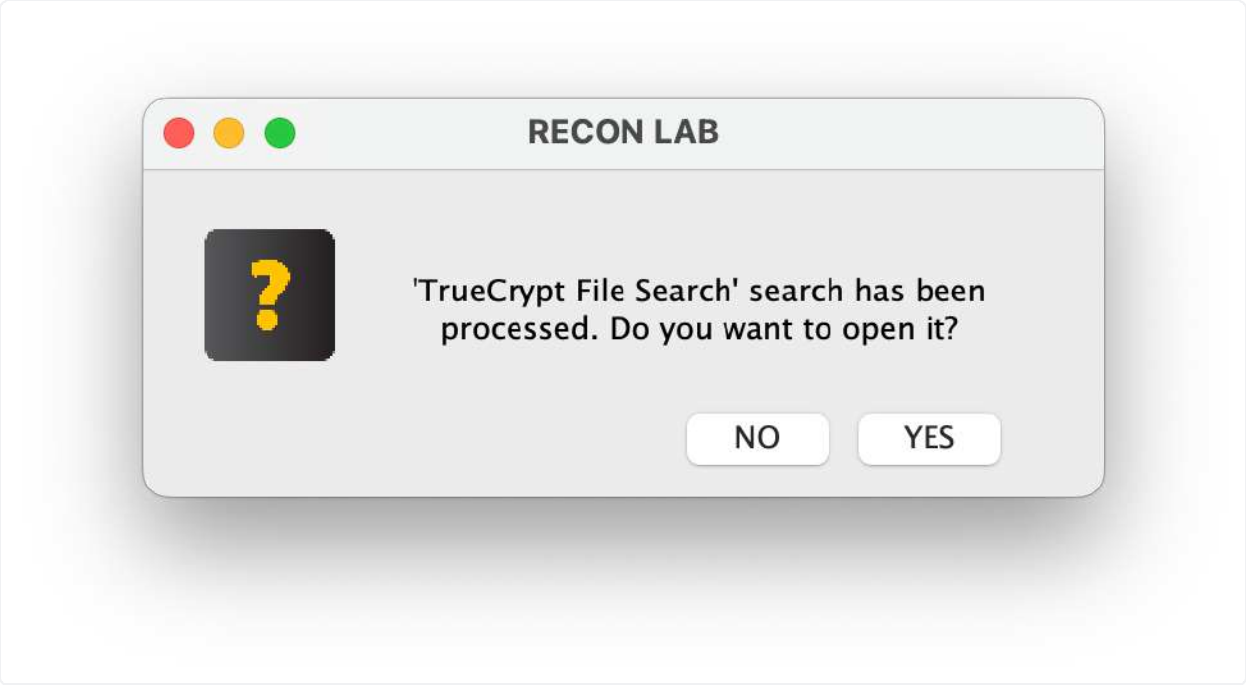
A File Search can be conducted using all sources or a combination of sources. Additionally, there is the option for using All Filters or Any Filter.



To select more than one source check “Select Source” then the “Select Source” button.

Select any source by checking the box next to the Source of interest then click “OK”.

When ready, provide the search for a unique name and click “Search”.



Once the search is complete you will be provided the option of reviewing the search.

		Record No.	File Name	File Size	Mime Type	Extension
1		261203	TrueCrypt.app	--		app
2		261207	TrueCrypt	10941620	application/x-java	
3		261213	TrueCrypt User Guide.pdf	923969	application/pdf	pdf
4		261214	TrueCrypt.icns	60982	image/x-icns	icns
5		384653	org.TrueCryptFoundation.TrueCrypt.bom	35763	application/octet-st...	bom
6		384654	org.TrueCryptFoundation.TrueCrypt.plist	260	application/octet-st...	plist
7		612364	TrueCrypt 7.1a Mac OS X.dmg	9526318	application/x-bzip	dmg
8		614283	TrueCrypt	--		
9		615545	http:%2F%2Fwww.google.com%2Fsearch?client=safari&rls=en&...	169	application/octet-st...	webhistory
10		615685	http:%2F%2Fwww.truecrypt.org%2F.webhistory	197	application/octet-st...	webhistory
11		615686	http:%2F%2Fwww.truecrypt.org%2Fdownloads.webhistory	218	application/octet-st...	webhistory
12		618734	org.TrueCryptFoundation.TrueCrypt.plist	353	application/octet-st...	plist
13		618975	org.TrueCryptFoundation.TrueCrypt.savedState	--		savedState

If you click “YES," any search results will appear in the Main Viewer window for additional analysis and bookmarking.

19.3 Content Search

There are several steps required before conducting a search by content in RECON LAB. Some of these steps have been explained in the previous sections of this manual.

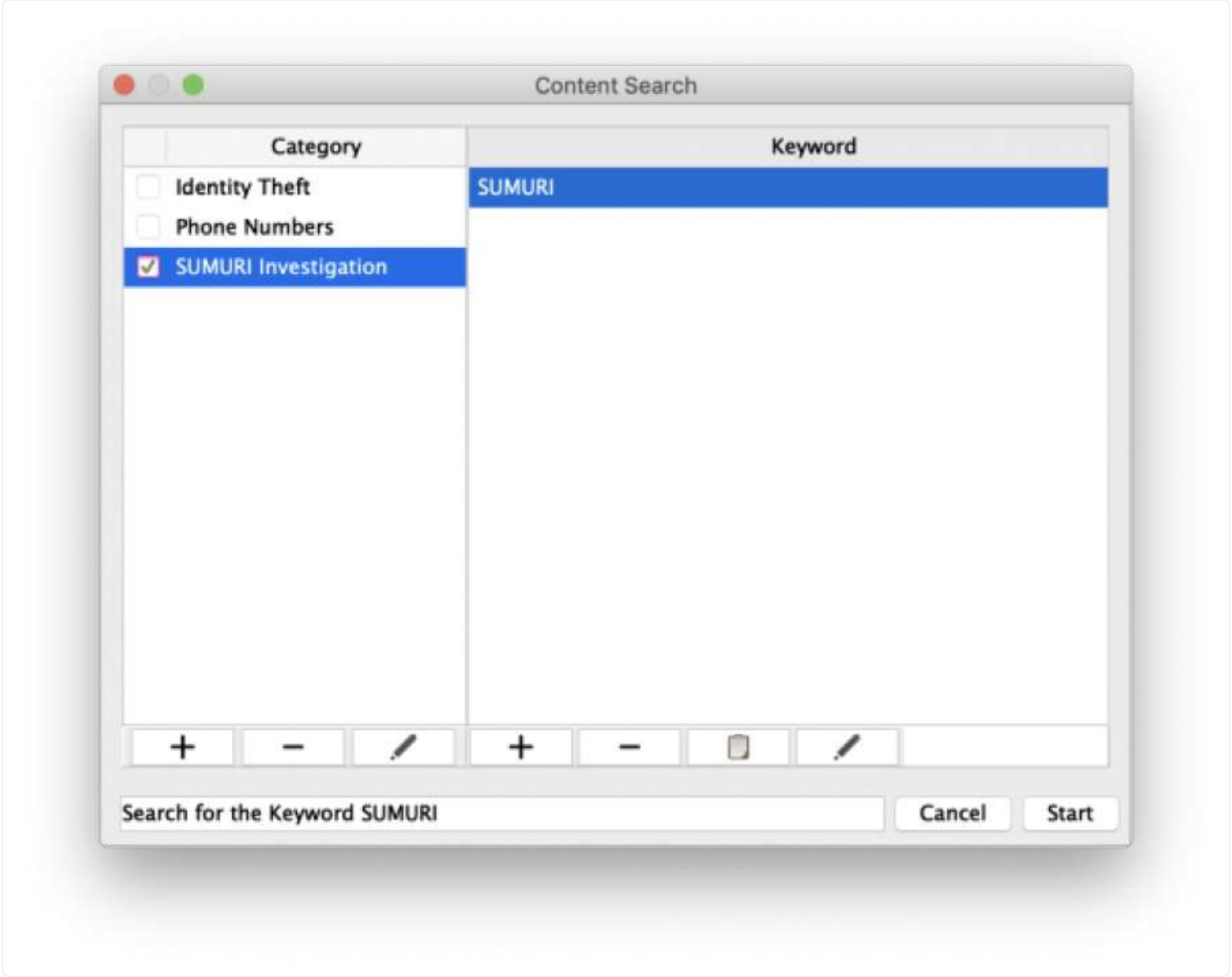
1. Create your list of keywords (Top Menu – Configuration – Keyword Lists).

2. Create and apply any Text Indexing Filters (Top Menu – Configuration – Text Indexing Filters).
3. Selected data from the source (Right-click on a source and “Add to Text Indexing Queue”).
4. Indexed selected data (Menu Bar - Process – Text Indexing).

Reminder: RECON LAB utilizes dtSearch for indexing and content searches.

dtSearch’s Quick Reference Guide can be found here: http://support.dtsearch.com/Support/forms/iframes_advanced/default.html

Once you have prepared and configured RECON LAB with the steps above start a Content Search by selecting Search > Content Search from the Menu Bar.



The Content Search selection window will appear allowing the examiner to select pre-configured categories and/or edit keywords prior to the content search. To begin the search enter a label for the search than click “Start”.

	Record No.	File Name	File Size	Mime Type	Extension	Number of hits	Keyword Hit
1	1241966	1009.emlx	84855	text/plain	emlx	21	SUMURI
2	1241983	1026.emlx	114343	text/plain	emlx	1	SUMURI
3	1243271	1087.partial.emlx	1396	text/plain	emlx	3	SUMURI
4	1243273	1089.emlx	2976	text/plain	emlx	6	SUMURI
5	1243274	1090.emlx	1069	text/plain	emlx	6	SUMURI

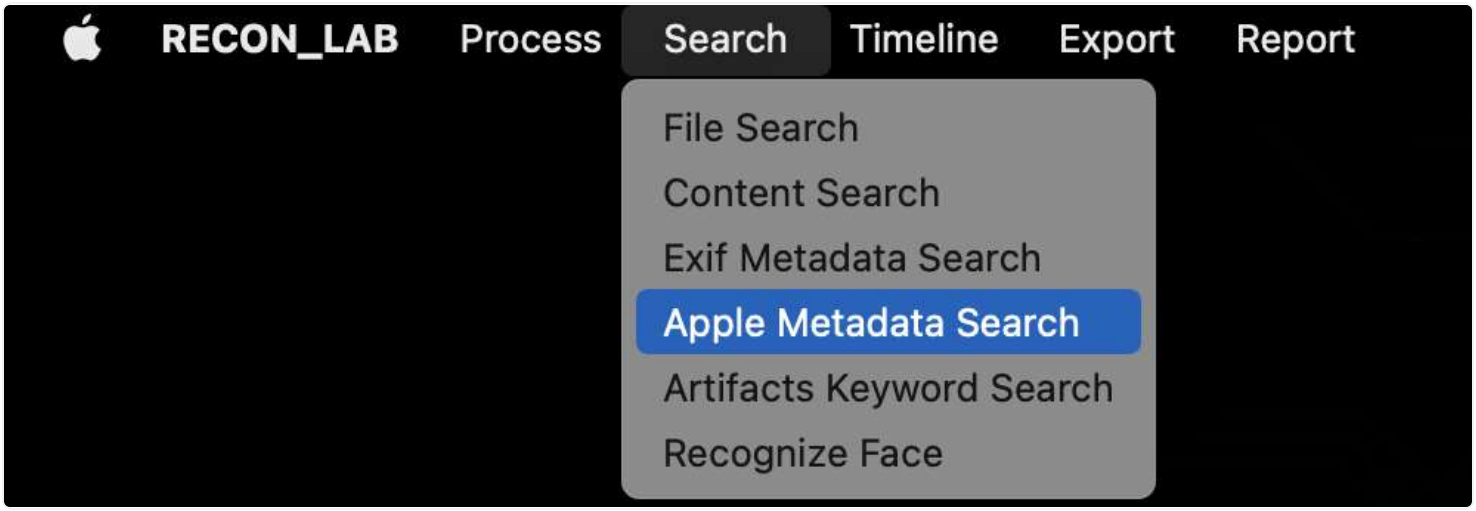
After the Content Search is complete the results will be available in the Main Viewer window and the search will be added to the Sidebar.

19.4 Apple Metadata Search

If a source in RECON LAB is macOS, it is possible to search for files using Apple Extended Metadata.

Before using this feature make sure that you have:

1. Selected Apple Extended Metadata using the “D” or “Display” option (Top Menu – Configuration – Apple Metadata Filters).
2. Processed the Apple Extended Metadata in the Source (Top Menu – Processing Status).



To begin a search for files using Apple Extended Metadata, select Search > Apple Metadata Search from the Menu Bar.

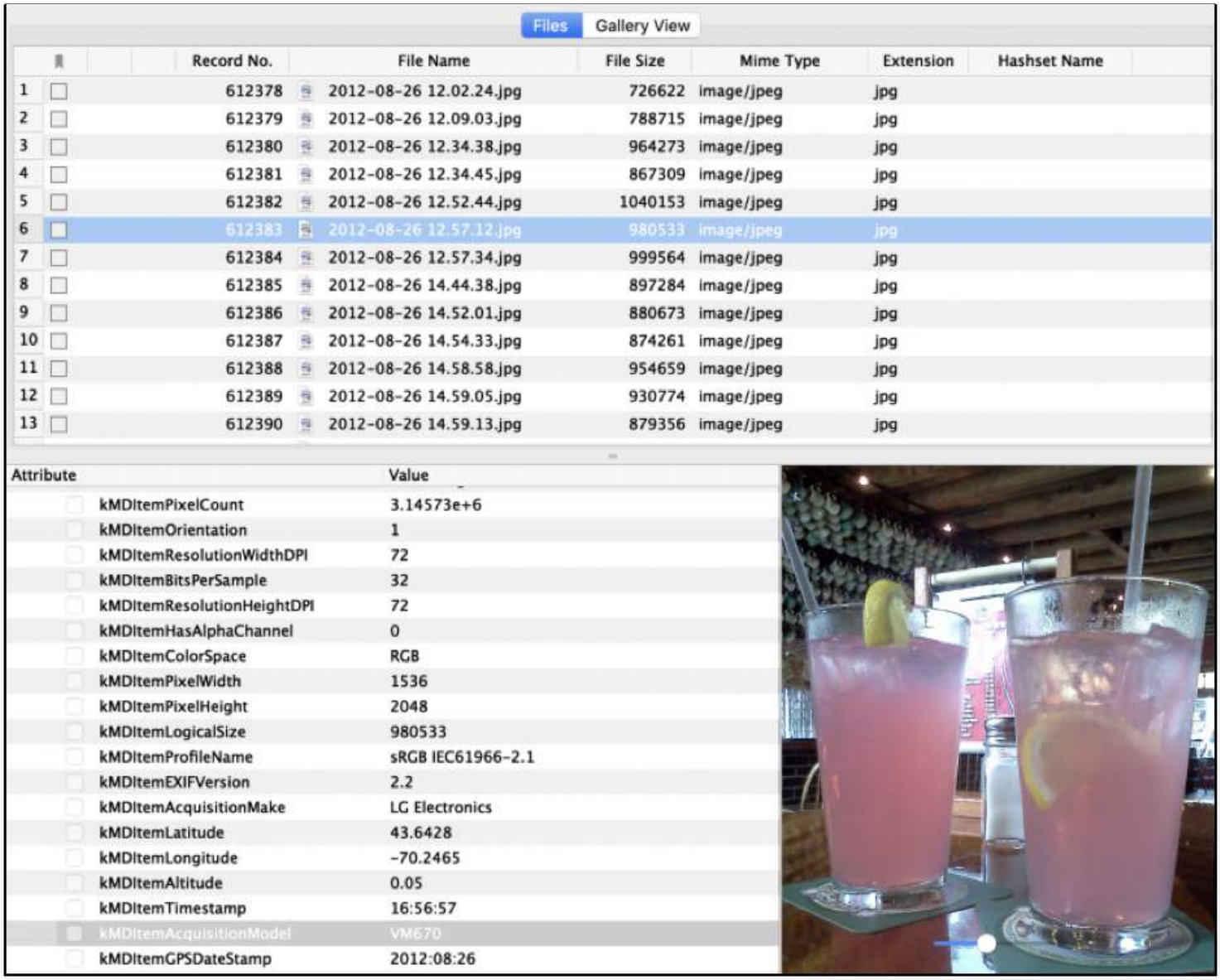
The Apple Metadata File Search window will appear with the ability to select, add, remove or configure filters for Apple Extended Metadata.

Use the dropdown boxes to select available Apple Extended Attributes and conditions and then enter a keyword.

Use the “+” and “-” buttons to add or remove filters.

Next, choose “All Filters” or “Any Filters”. Provide a Search Label and click “Search” to find files.

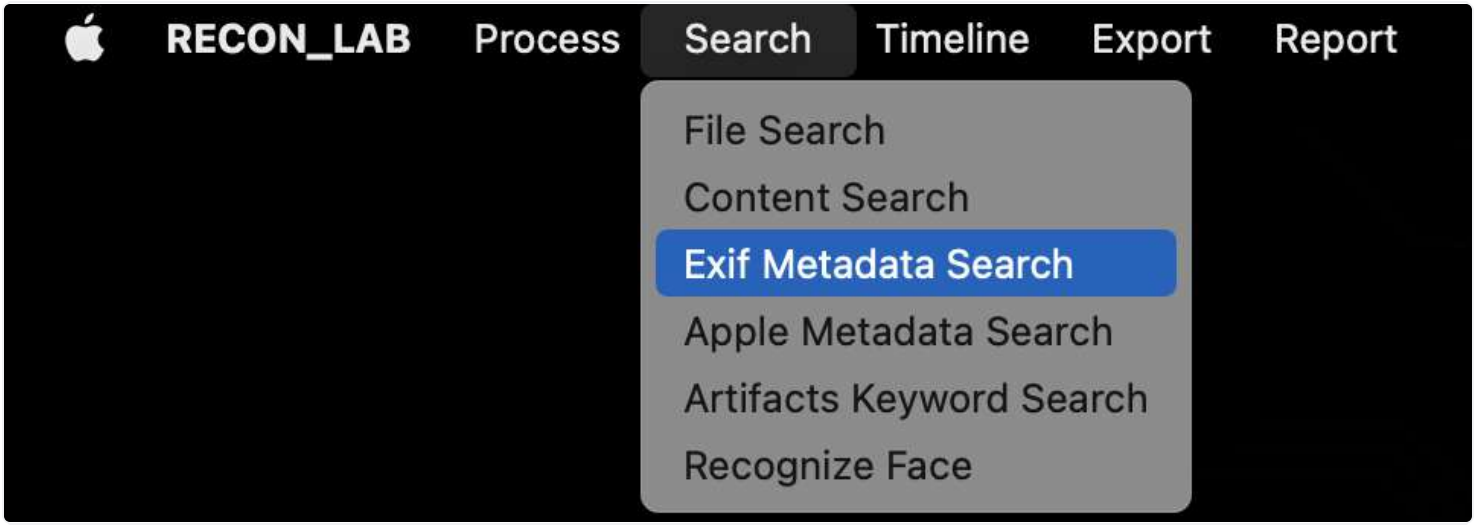
In the previous example, we used the “Device Make” extended attribute with the keyword “LG” and the “Device Model” extended attribute using the keyword “VM670” for the filters.



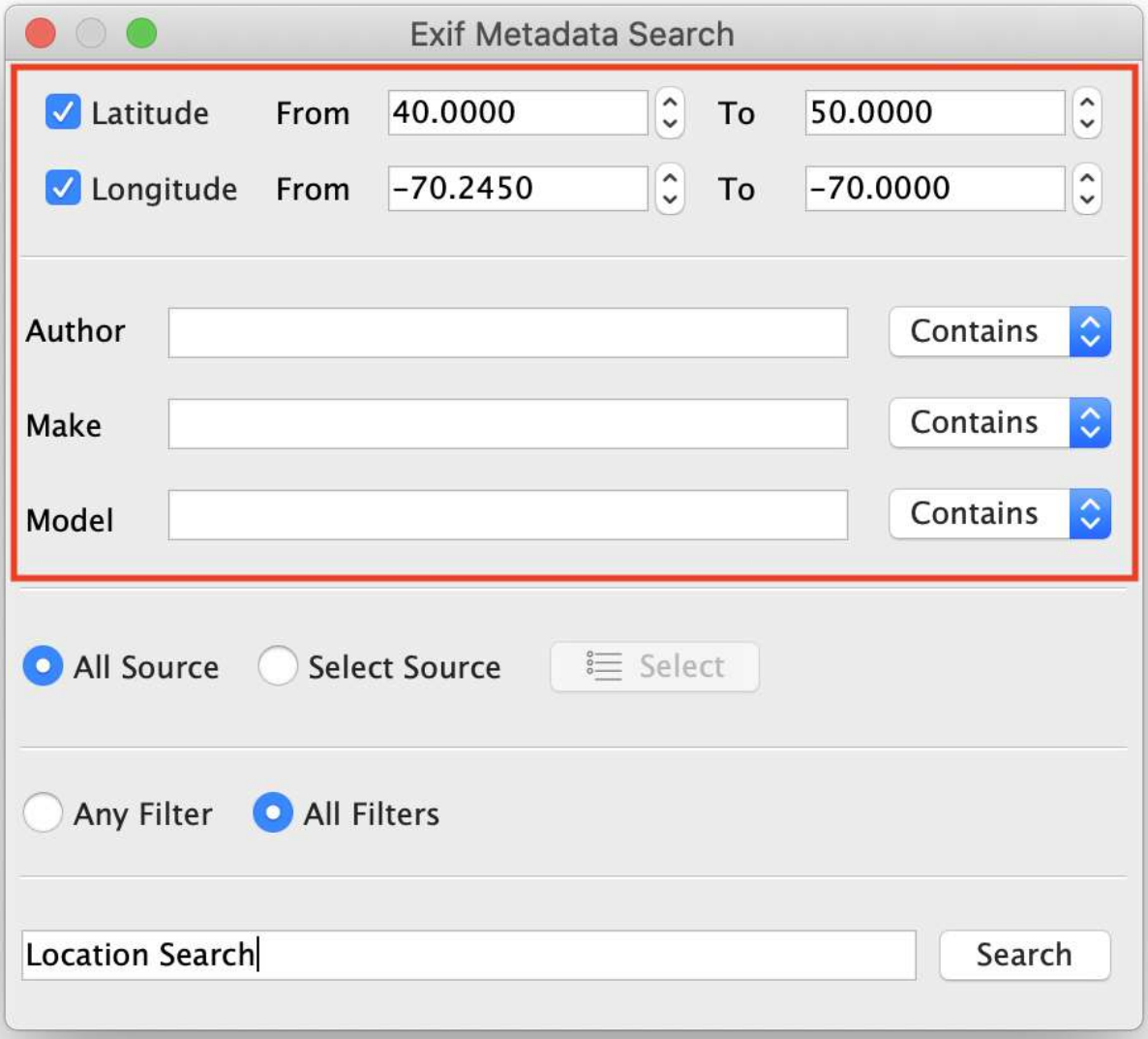
Once the search is completed you will have the option to review the results which will appear in the Main Viewer window.

19.5 EXIF Metadata Search

EXIF metadata is contained in many file types. RECON LAB includes the ability to find or filter files by Latitude, Longitude, Author, Make and Model EXIF metadata.



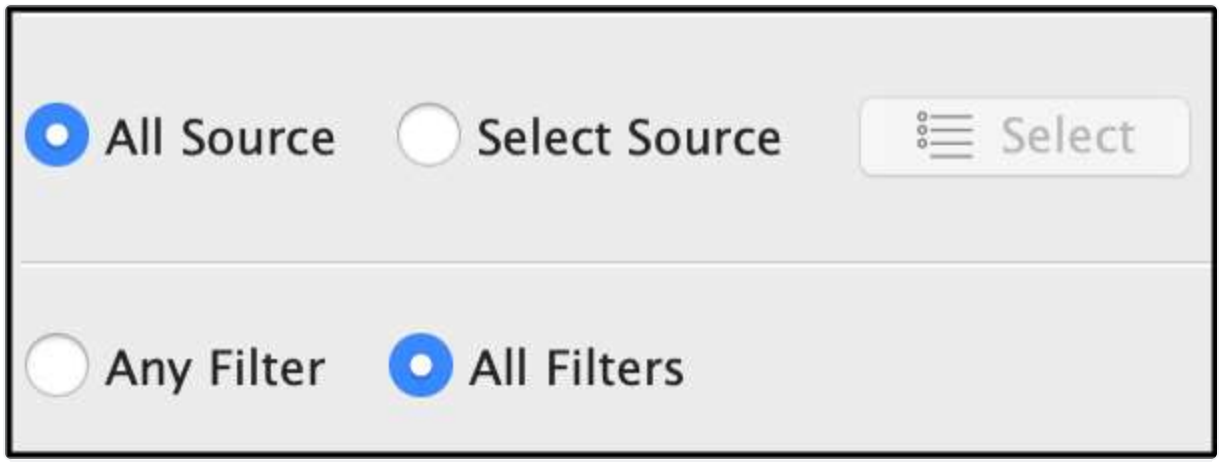
To start a search for EXIF Metadata, select Search > EXIF Metadata Search from the Menu Bar.



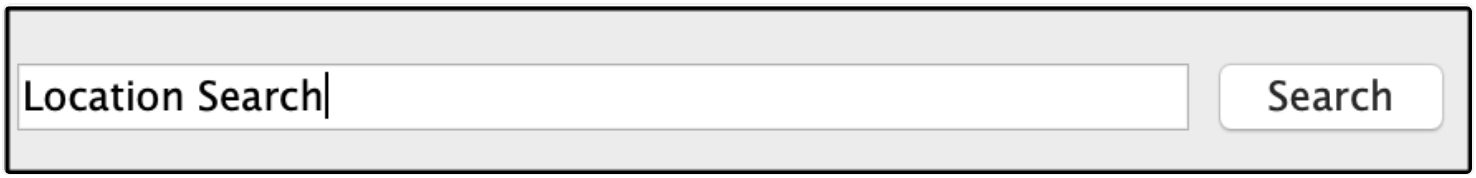
Enter information for any of the following filters:

- **Latitude** - In Decimal Degrees (DD) notation from lowest to highest
- **Longitude** - In Decimal Degrees (DD) notation from lowest to the highest
- **Author** - Author of a file
- **Make** - Make of the device creating the file
- **Model** - Model of the device creating the file

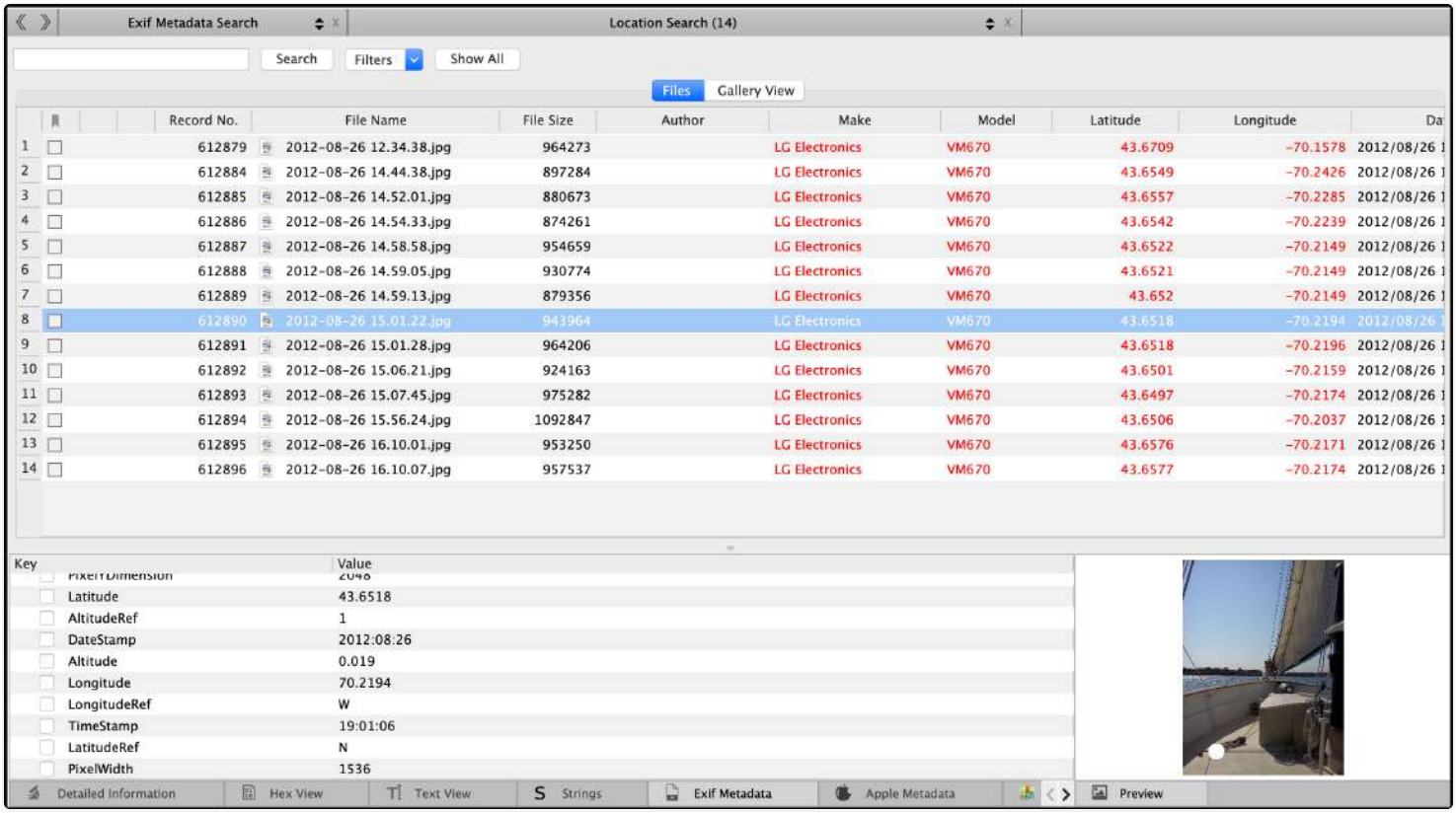
Note: Using both Latitude and Longitude filters will allow filtering data to a known geographical area.



The examiner has the option to search all sources or select individual sources as well as applying all filters or any filter.



Click Search after entering a name for the query to complete the search and to see the results.



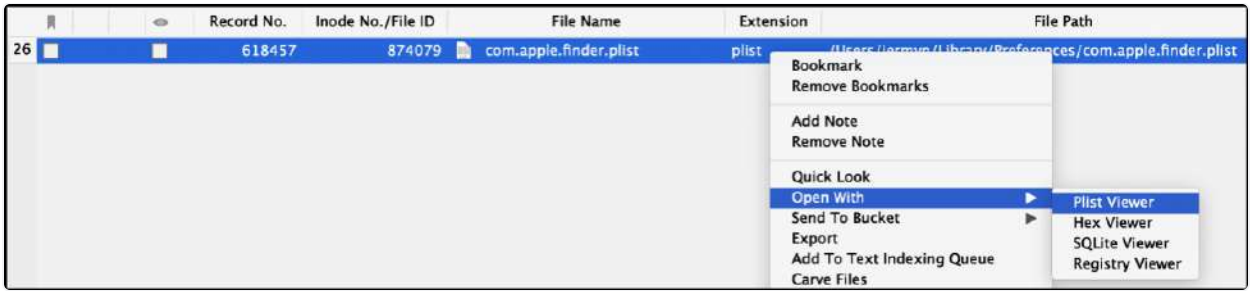
20. Advanced Viewers

Integrated into RECON LAB are four advanced viewers.

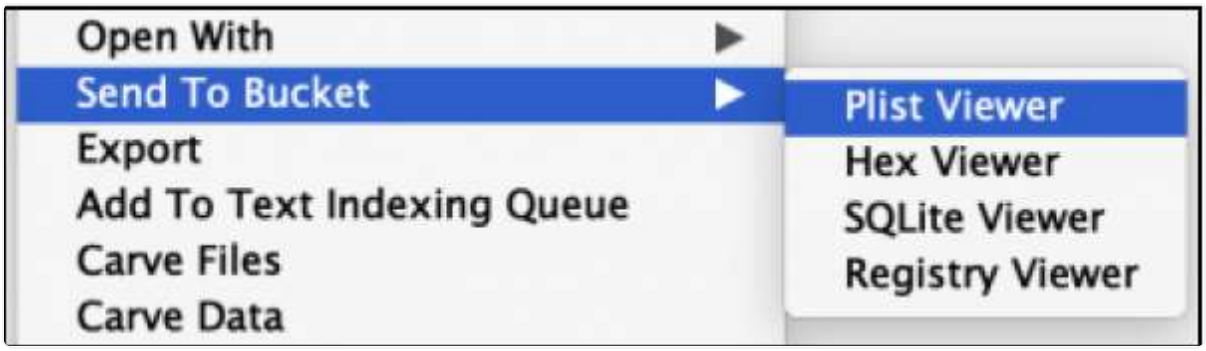
- **Property List Viewer** – for Apple binary and standard plist files.
- **HEX Viewer** – a full Hex viewer with advanced functions for forensic investigations.
- **SQLite Viewer** – a forensic SQLite viewer with the ability to create custom SQLite queries.
- **Registry Viewer** – for analysis and documentation of Windows Registry files.

20.1 Plist Viewer

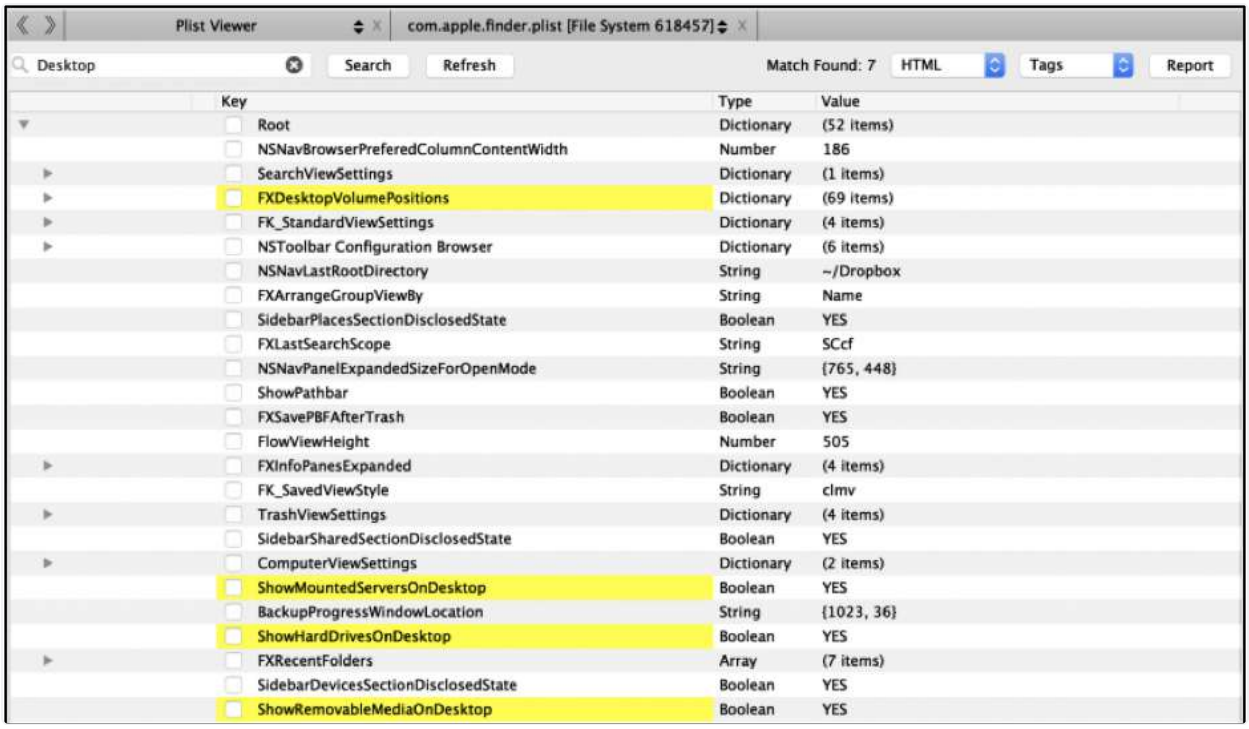
The Property List Viewer (Plist Viewer) works with both standard and binary macOS Property Lists (.plist files). Property List files are one of two common storage formats for Mac data.



To examine a file using the Property List Viewer, right-click on a property list file and select “Open With – Plist Viewer”.



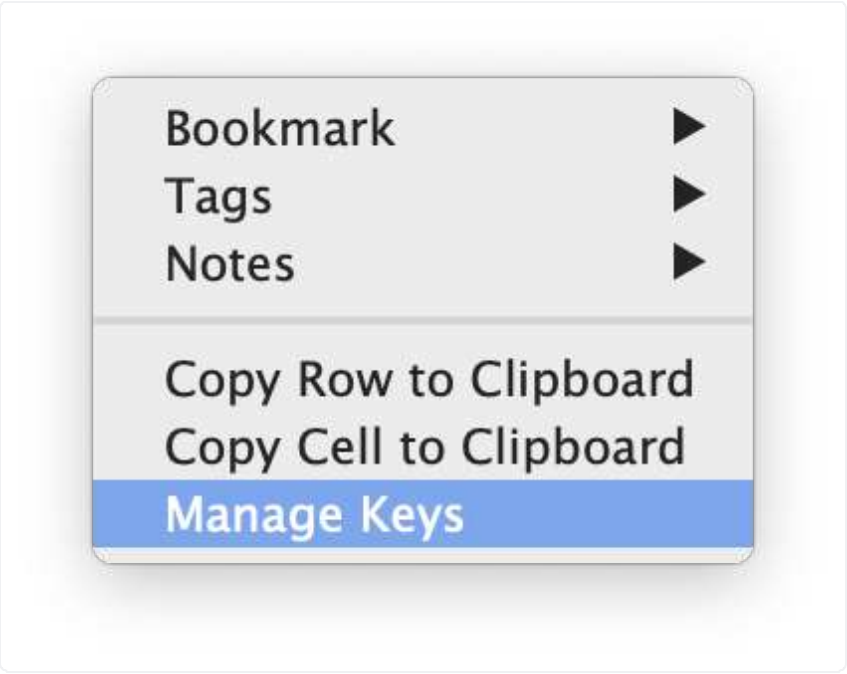
If you would like to add the file to review later in the Sidebar Bucket select “Send to Bucket – Plist Viewer”.



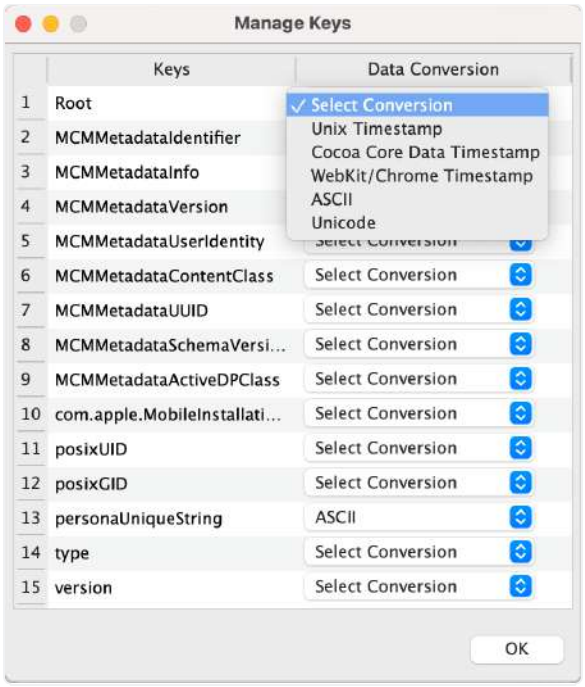
The Property List Viewer opens the plist in the Main Viewer window. Search options and reporting options are available.

In the example above, the “com.apple.finder.plist” was opened in the Property List Viewer. The keyword “Desktop” was entered for a search term. All hits are highlighted in yellow.

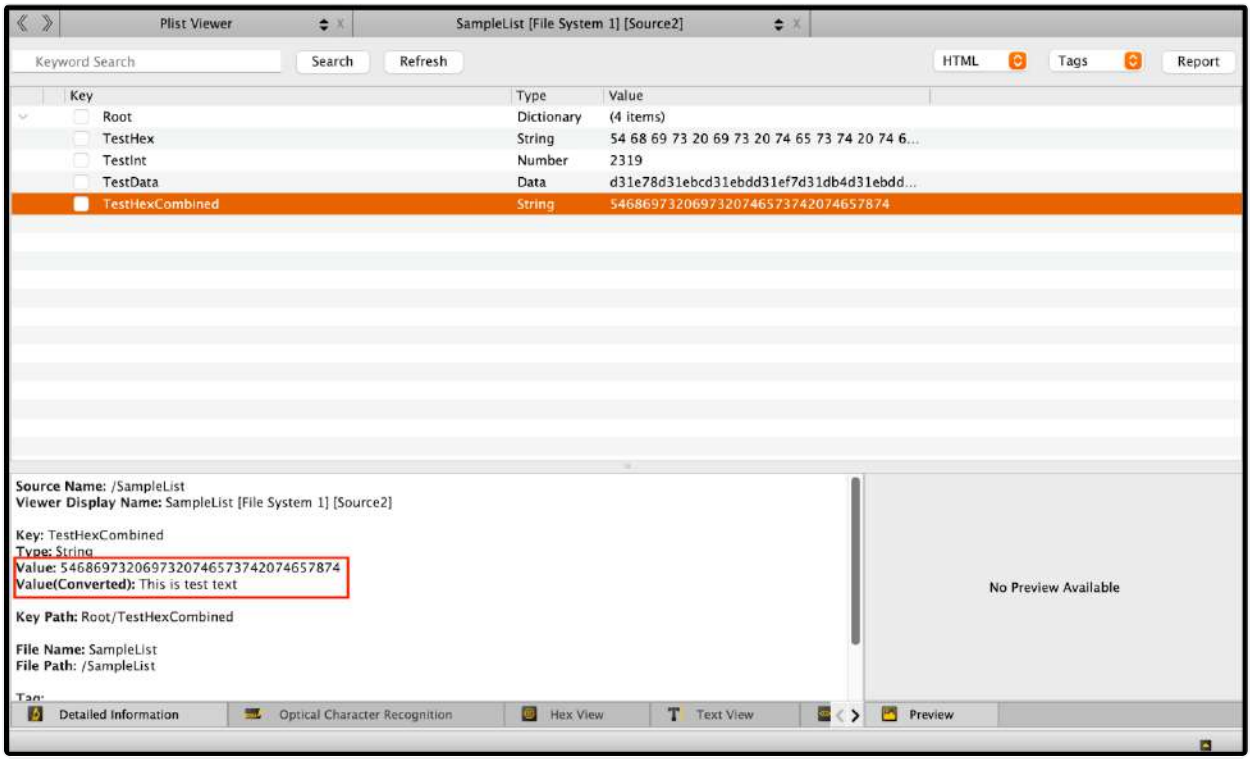
The Property List Viewer also allows you to see the raw data of any plist that has already been sent to the viewer. To see the different display methods, right click on the column name section and select “Manage Key”.



From the “Manage Keys” window, you can select which of the data keys you would like converted to a different display method. Select your desired format from the dropdown menu.



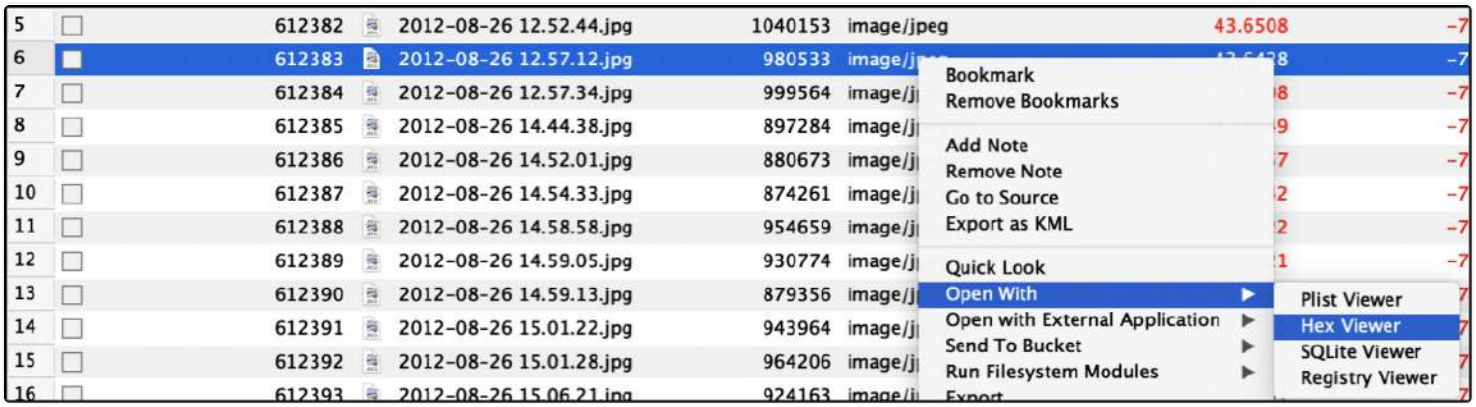
After selecting the conversion type, select the data key to see the conversion in the main window of the Property List Viewer.



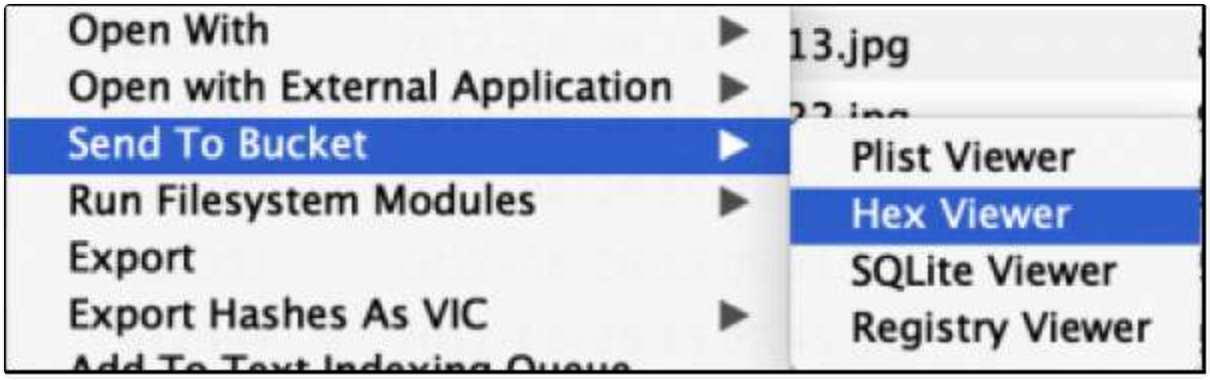
20.2 Hex Viewer

The Advanced Hex Viewer within RECON LAB is extremely powerful and full of helpful features.

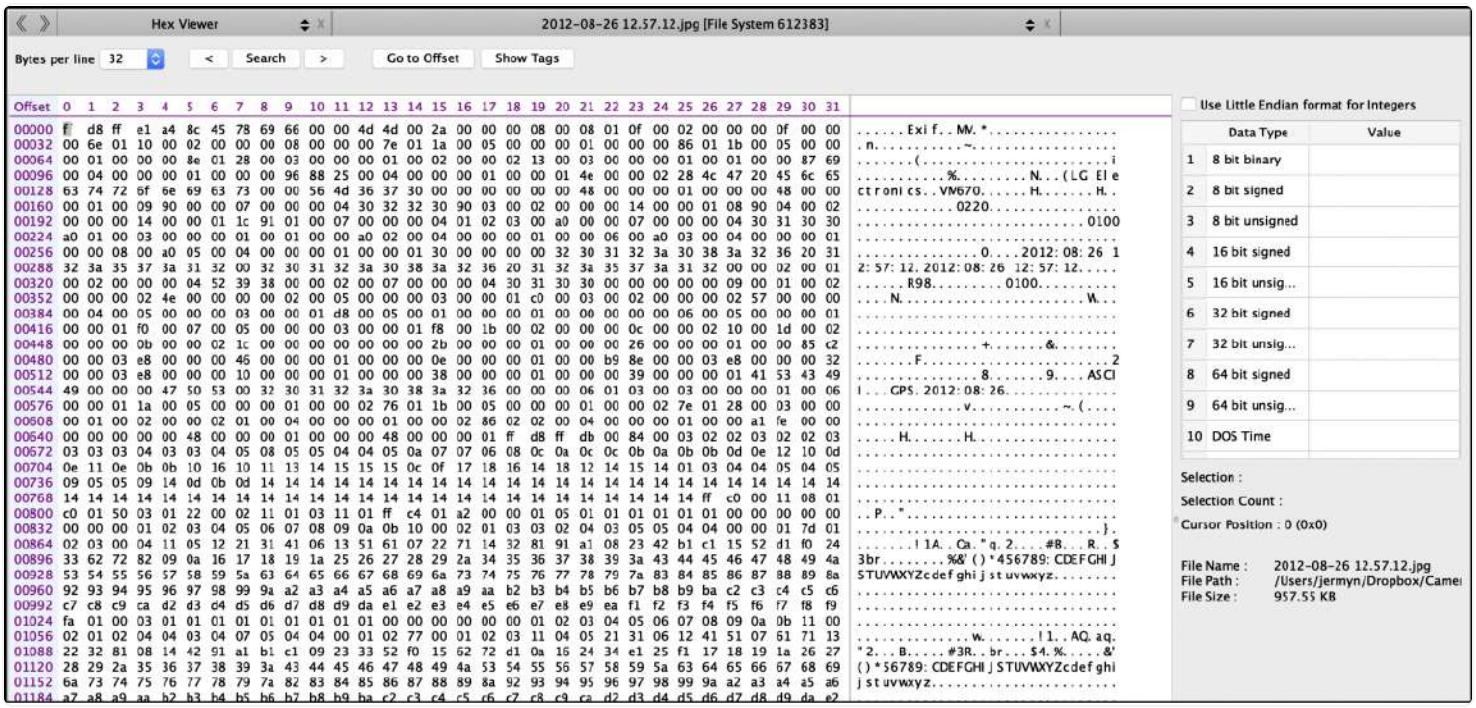
Open File in Hex Viewer



To open a file in the Hex Viewer, right-click and select “Open With – Hex Viewer”.



If you would like to add the file to review later in the Sidebar Bucket select “Send to Bucket – Hex Viewer”.

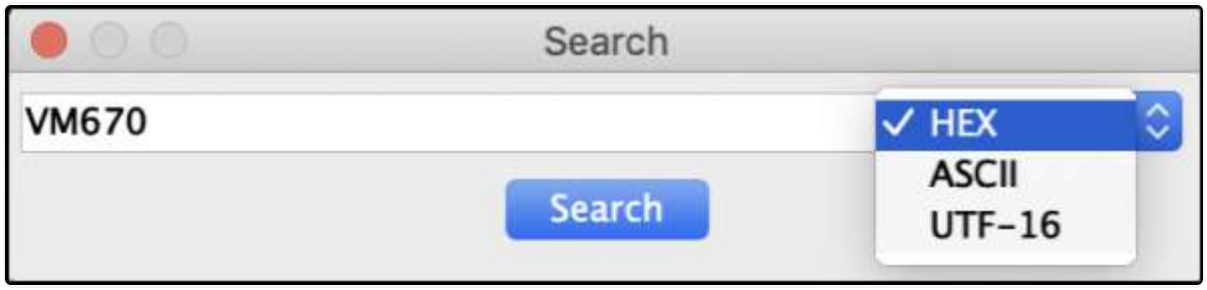


The Hex Viewer will open in the Main Viewer window.

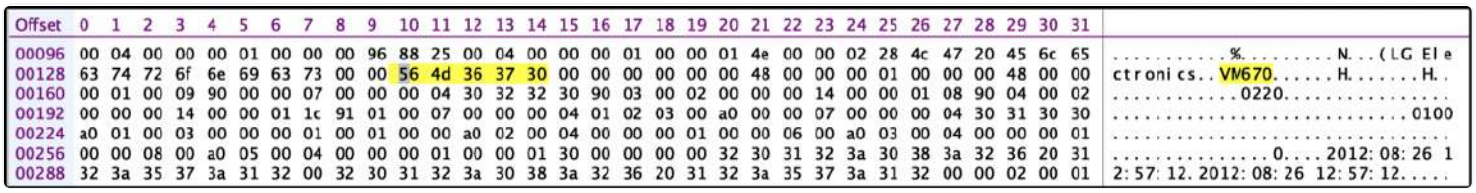
The number of “Bytes per line” can be adjusted using the dropdown box with values between 2 and 32.

Search in Hex Viewer

To search within the hex select the “Search” button to presented with the Search options box. Options allow for the search term to be entered as hex, ASCII, or UTF-16 (Unicode).

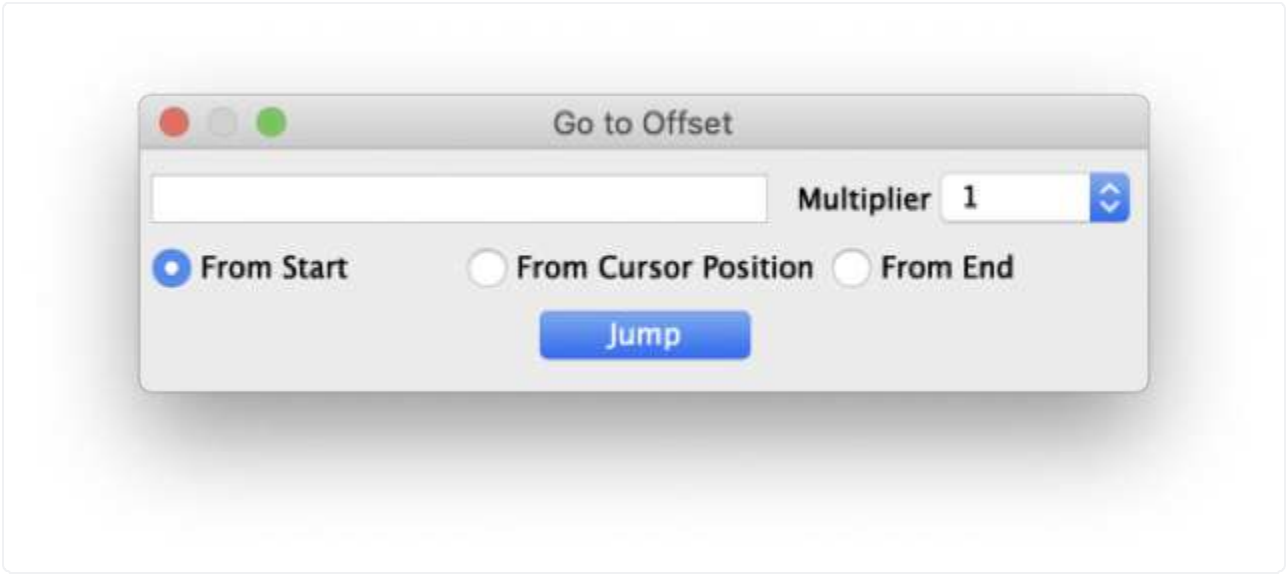


After entering the search term click “Search”.



Hits will be highlighted in yellow. Use the backward and forward buttons (next to the Search button) to move between hits.

Jump to an Offset



To jump to a specific offset click the “Go to Offset” button at the top of the Hex Viewer. Enter a value and select a multiplier (between 1 and 8192).

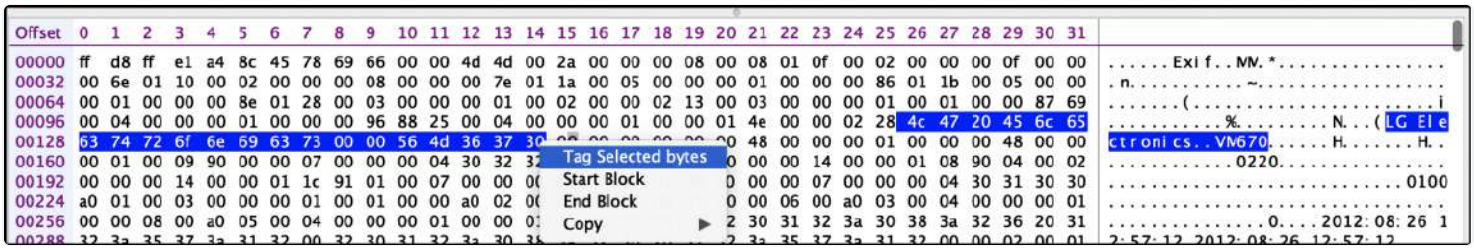
Select where to begin:

From Start – from the beginning of the file.

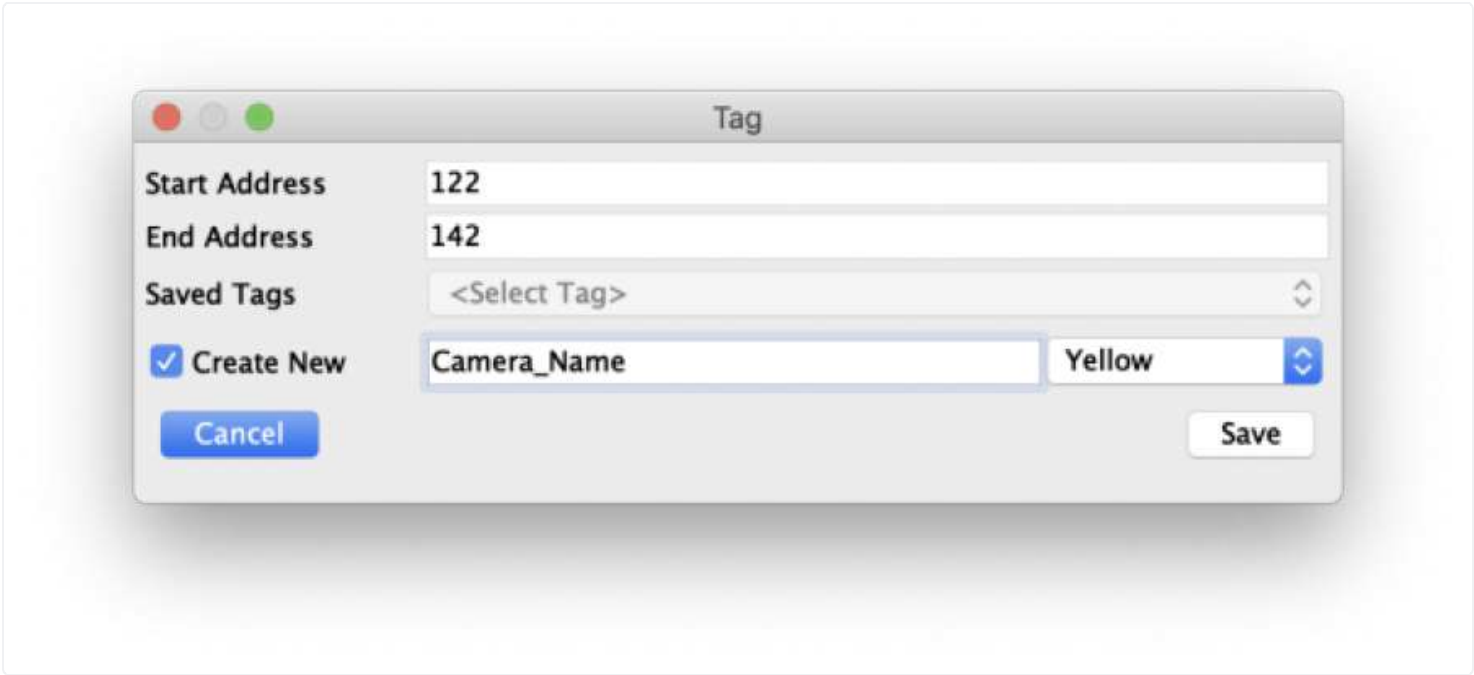
From Cursor Position – from where the cursor currently sits.

From End – From the end of the file.

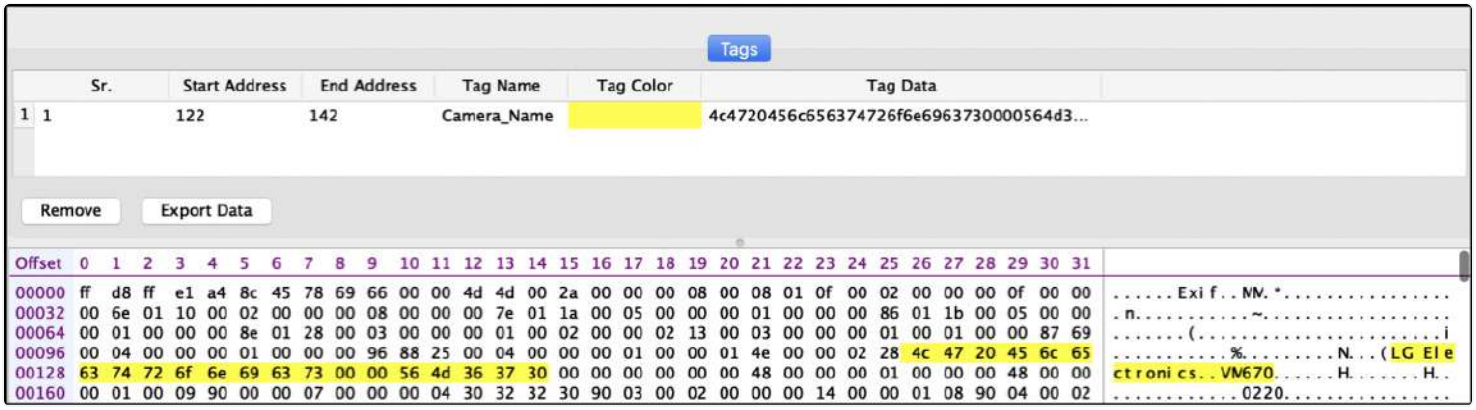
Tag Selected Bytes



Data can be tagged within the Hex Viewer by “swiping” over or highlighting the data. Right-click on the data to be tagged and select “Tag Selected bytes”.

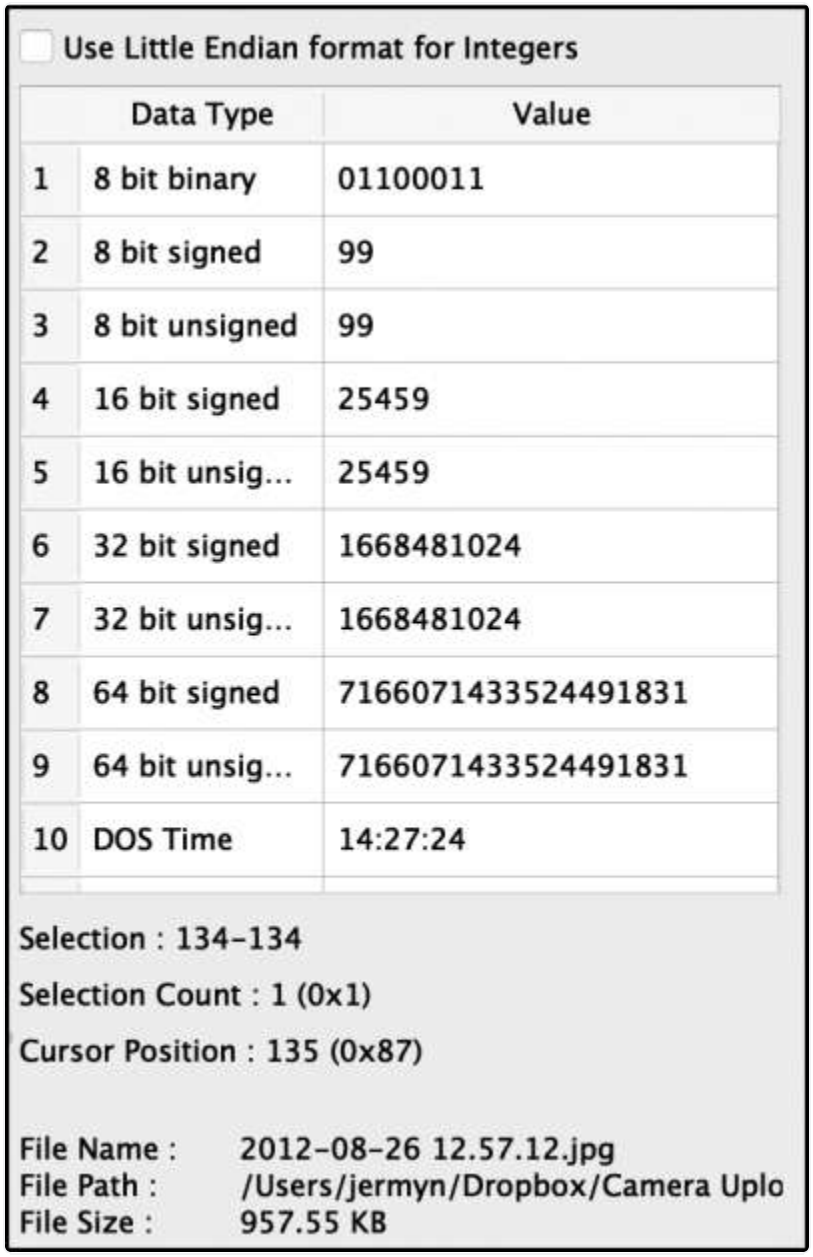


Assign the data to an existing “Saved Tags” or create a new tag by checking the “Create New” box, entering a name and selecting a color. The tagged data will appear in the Sidebar under “Tags”.



Tags can also be recalled by selecting the “Show Tags” button at the top of the Hex Viewer.

Hex Viewer Information Pane

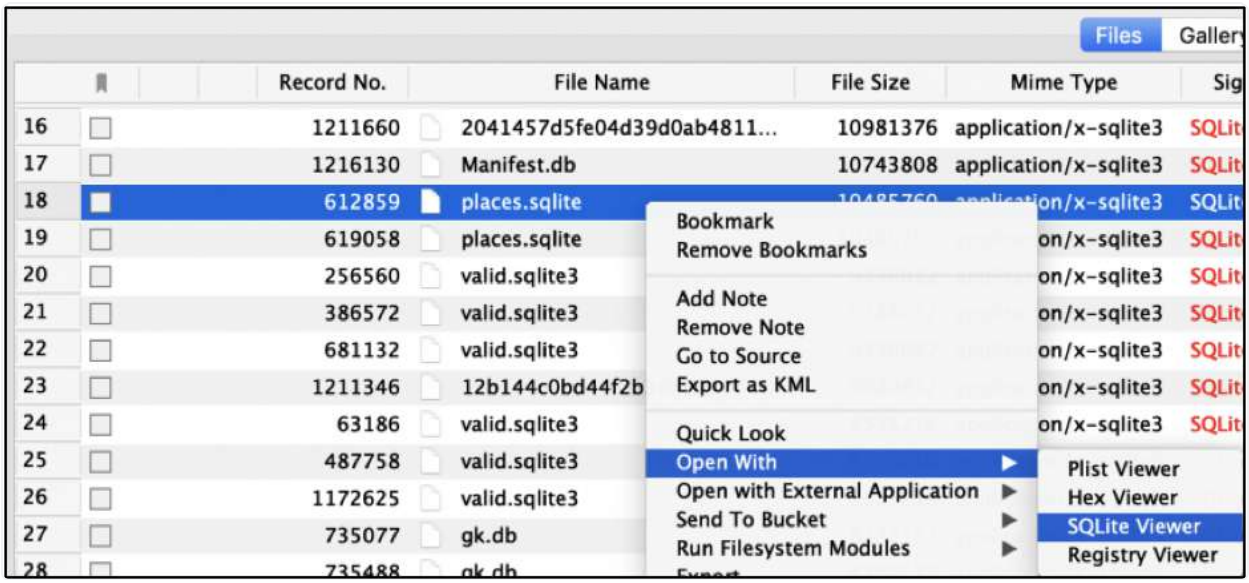


The Information Pane on the right side of the Hex Viewer will display the values of swiped or highlighted data. It can also be used to toggle Little Endian/Big Endian interpretation on and off using the checkbox.

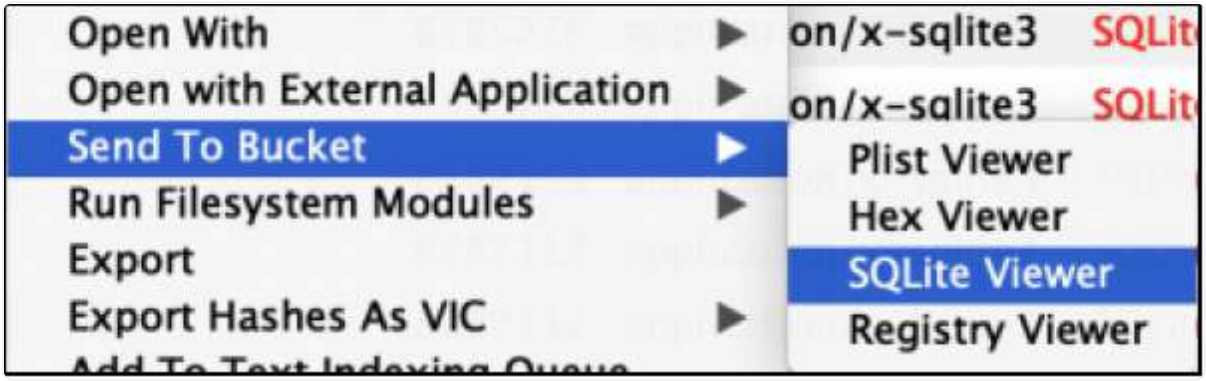
20.3 SQLite Viewer

The Advanced SQLite Viewer within RECON LAB has the ability to search, filter and execute SQLite queries to make it easier to document evidence found in SQLite files.

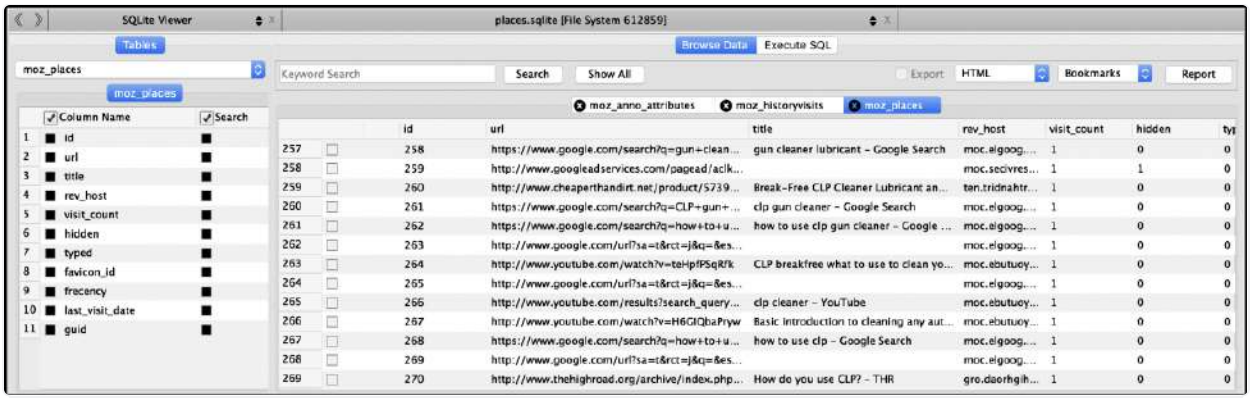
Open File in SQLite Viewer



To open a file in the SQLite Viewer, right-click and select “Open With – SQLite Viewer”.

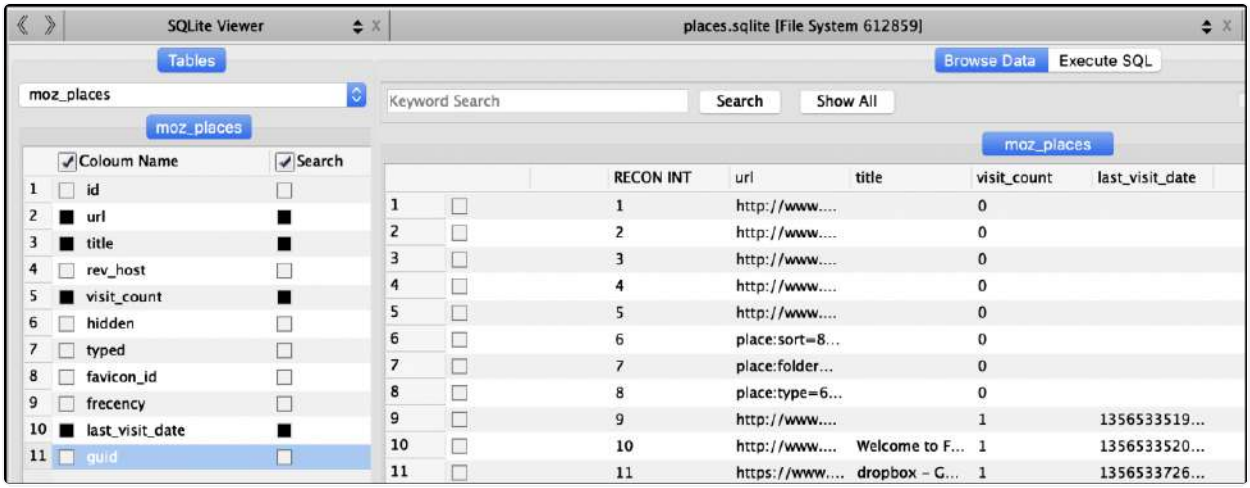


If you would like to add the file to review later in the Sidebar Bucket select “Send to Bucket – SQLite Viewer”.



The SQLite Viewer will open in the Main Viewer window.

Filtering Table Data

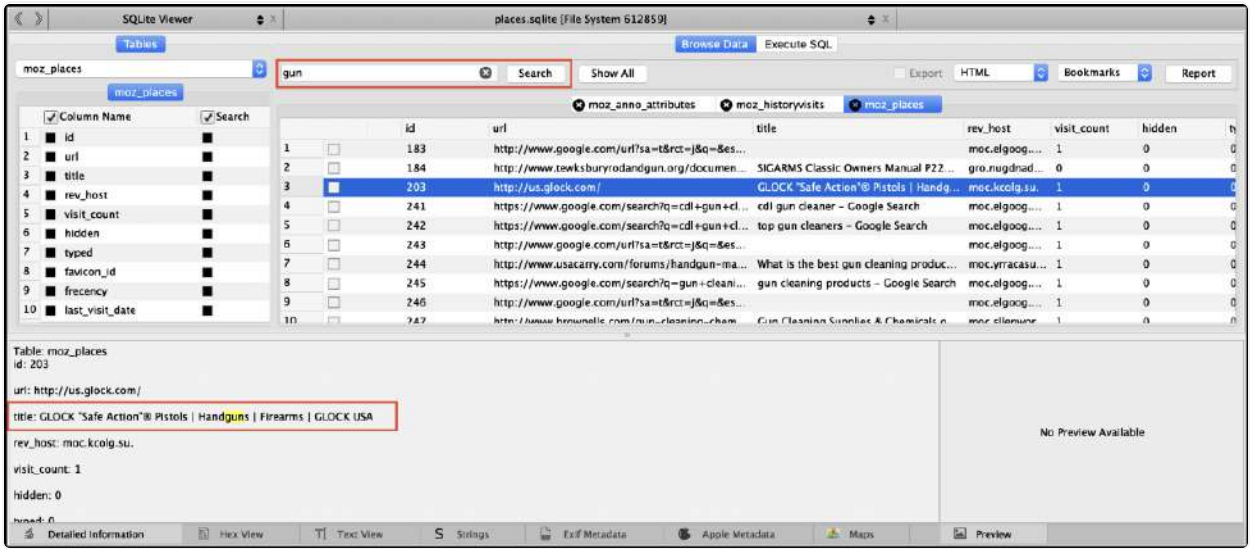


Individual SQLite tables can be selected by using the Tables dropdown box.

Columns can be turned on and off by checking or unchecking the box underneath “Column Name”.

Likewise, the ability to search through individual columns can be turned on and off by checking or unchecking the box underneath “Search”.

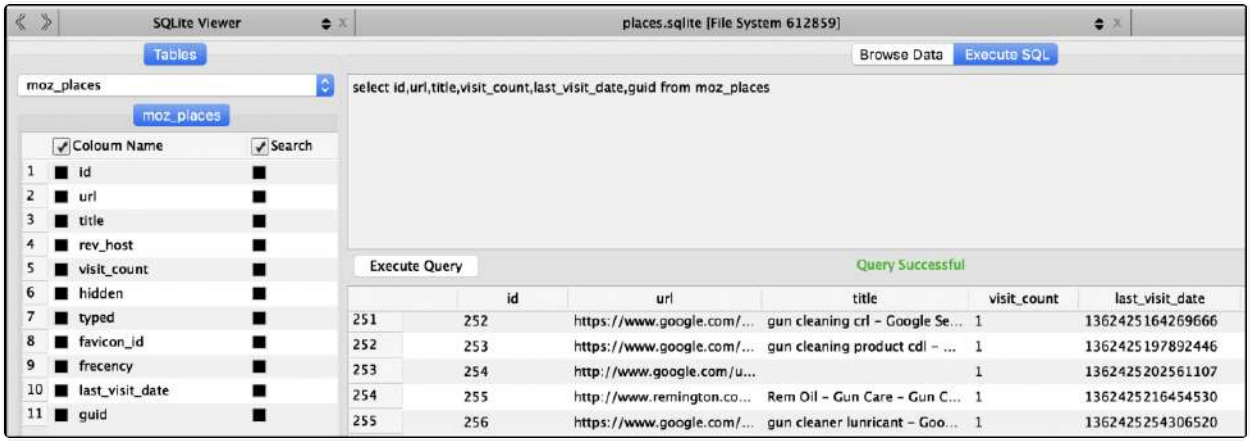
Searching in the SQLite Viewer



After selecting a table of interest enter a keyword in the search field and click “Search”. Items in the table matching the keyword will remain and can be reviewed and/or bookmarked.

Executing a SQLite Query

Instruction for SQLite queries is beyond the scope of this manual. However, there are many great resources available online.



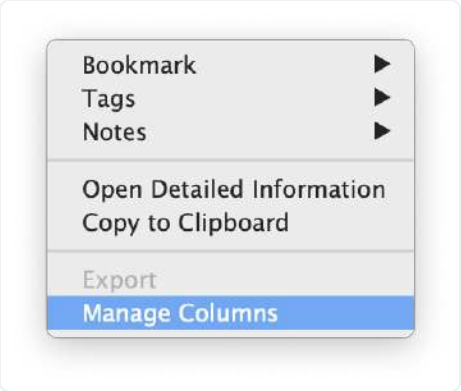
To execute an SQLite query first select a table then click the “Execute SQL” tab.

RECON LAB will pre-populate the work area with existing column names from the table. This can be modified to using common SQLite syntax.

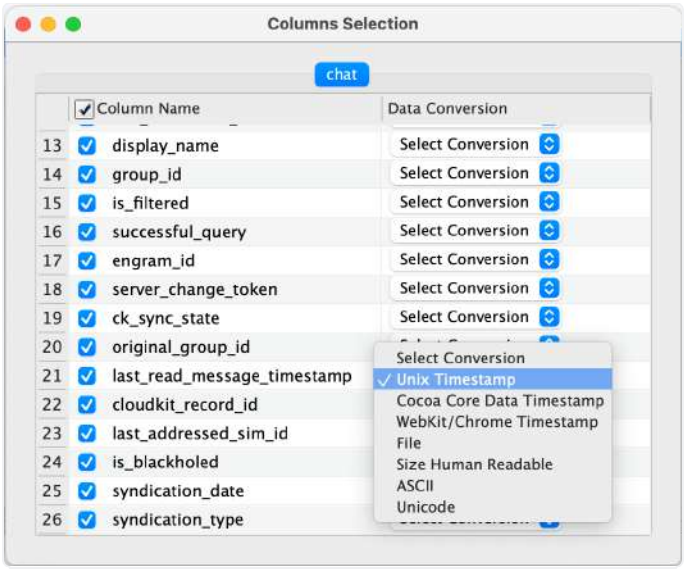
Once the query has been entered click the “Execute Query” button to view the results.

Data Conversion

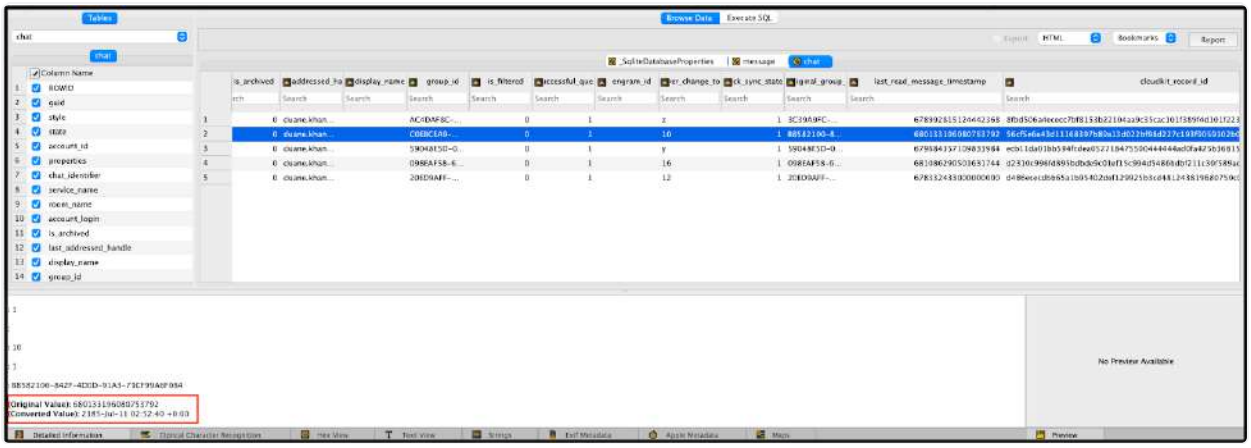
The SQLite Viewer also allows you to see the raw data of any SQL table that has already been sent to the viewer. To see the different display methods, right click on the column name section and select “Manage Column”.



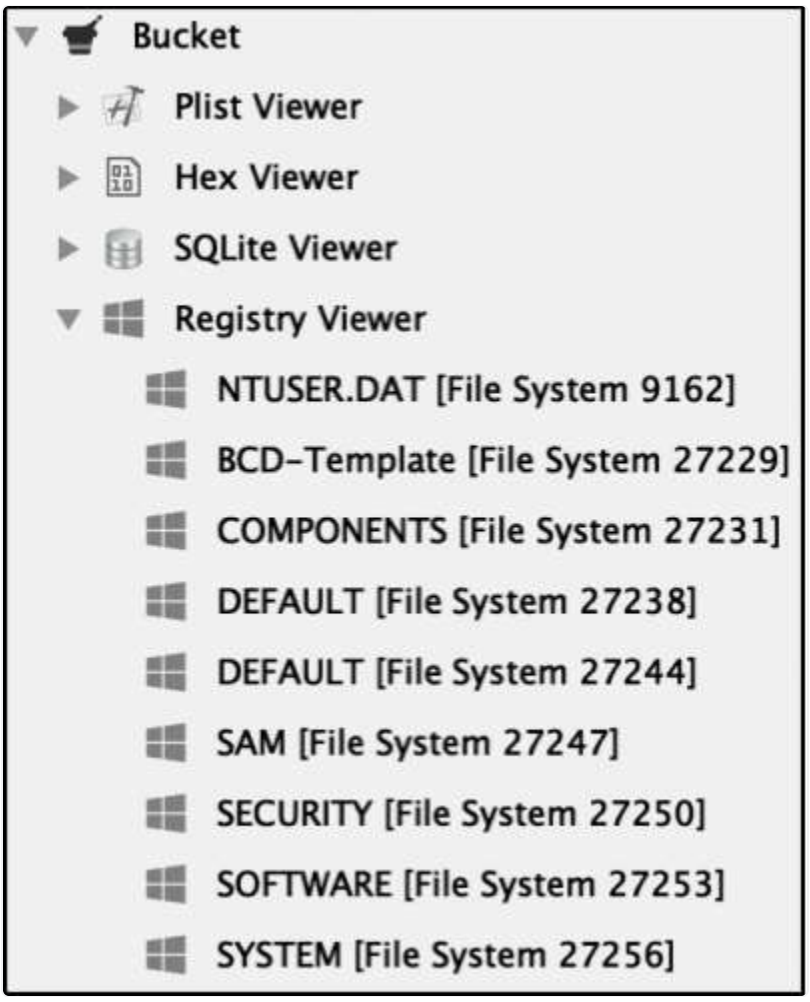
From the “Manage Column” window, you can select which of the columns you would like converted to a different display method. Select your desired format from the dropdown menu.



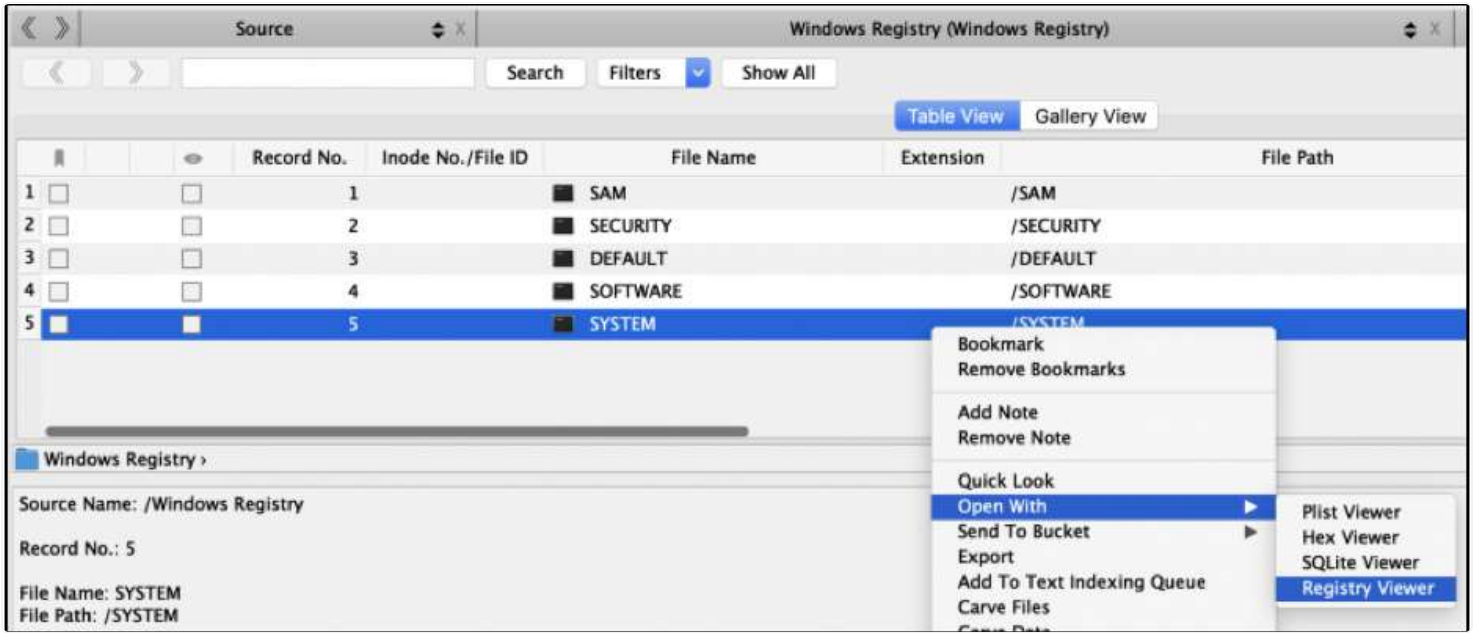
After selecting the conversion type, select the desired entry to see the conversion in the main window of the SQLite viewer.



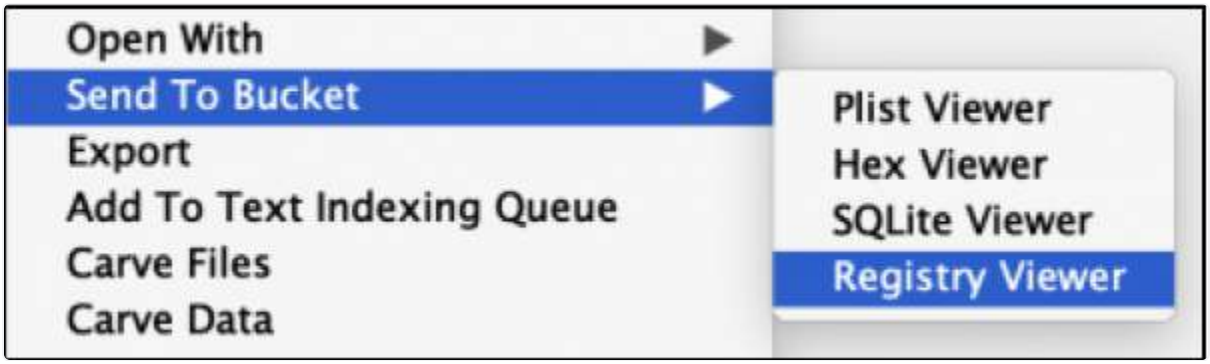
20.4 Registry Viewer



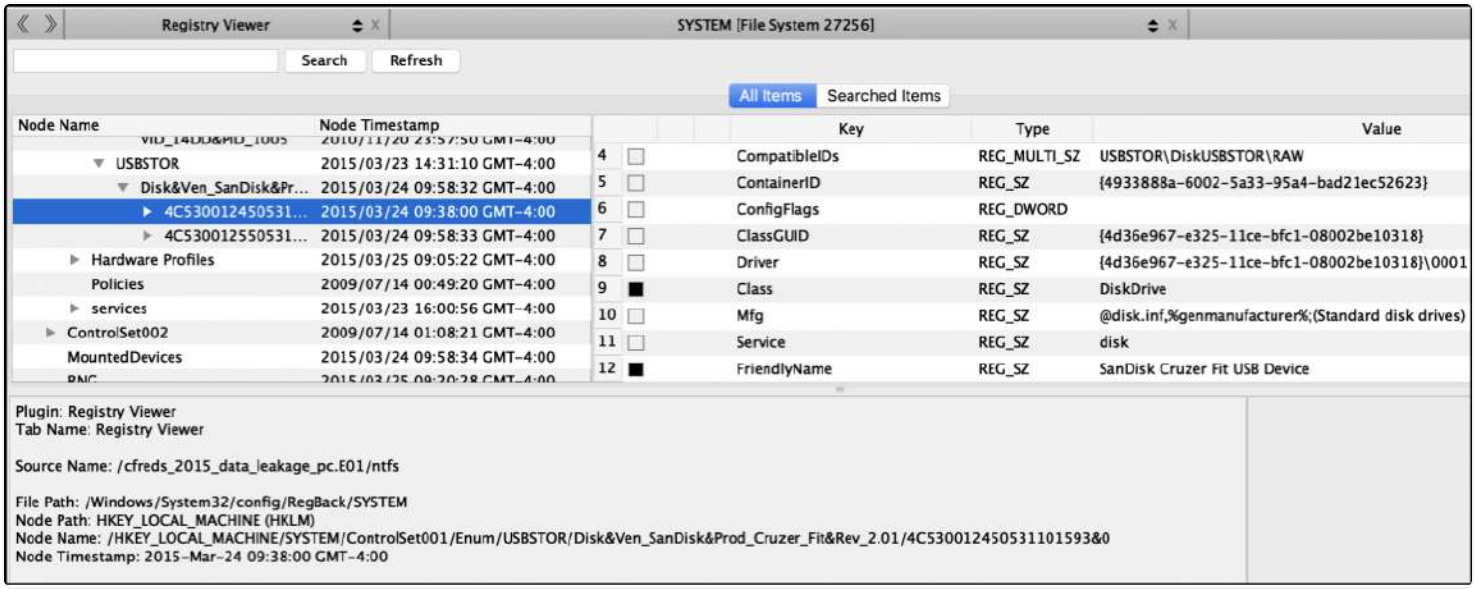
When a source is added to RECON LAB that contains Windows registry information it is automatically parsed and added to the Sidebar Bucket under Registry Viewer.



If you need to manually load a Windows registry artifact right-click on the file and select “Open With – Registry Viewer”.

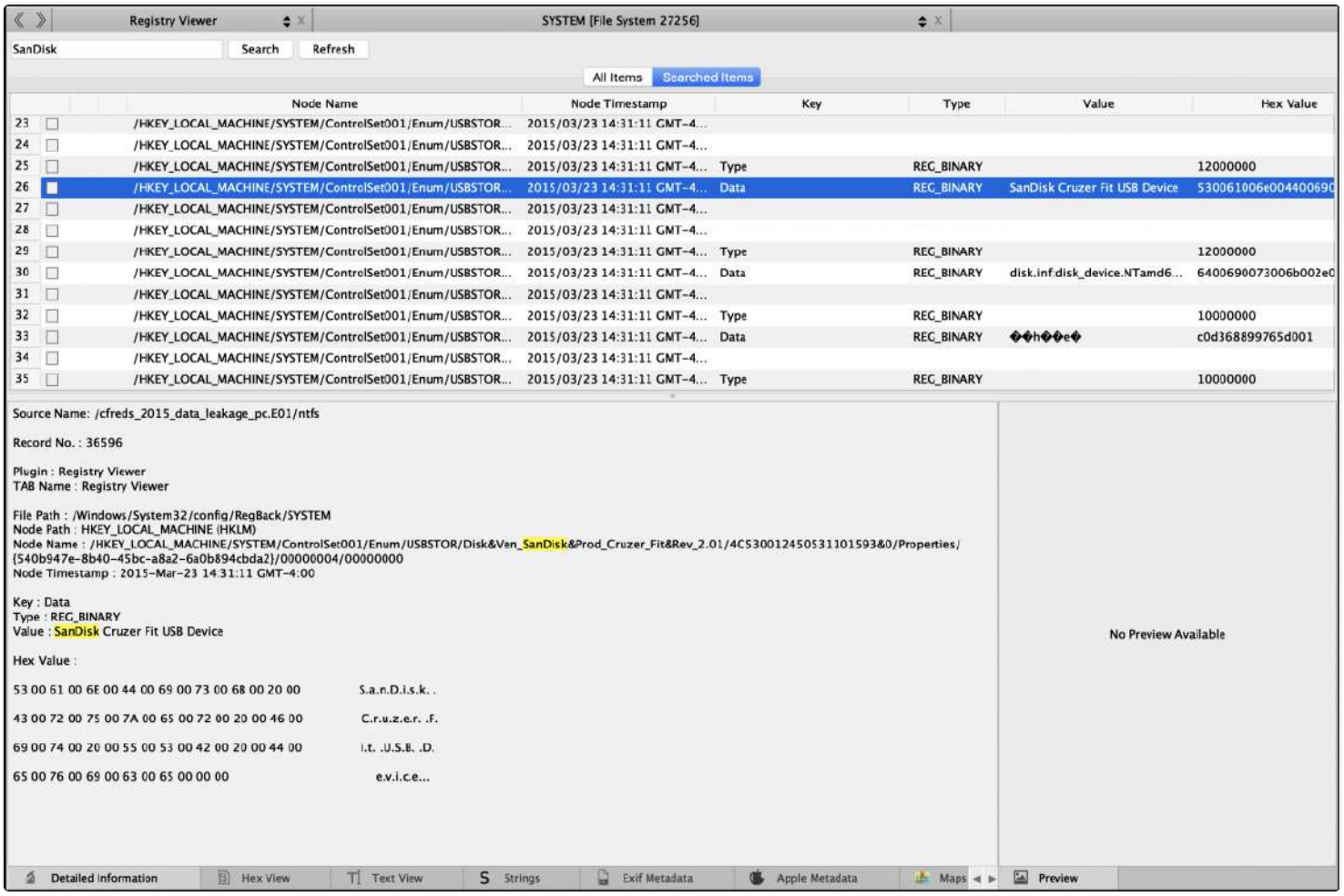


To add the registry artifact to the Sidebar choose “Send to Bucket – Registry Viewer”.



To examine Windows registry artifacts select a registry hive to open in the Sidebar. The registry hive will open in the Registry Viewer in the Main Window.

The registry hives and keys can now be explored and bookmarked.



To search inside a hive enter a keyword in the search field and click “Search”.

Select the “Searched Items” tab to review the results.

In the example above the keyword, “SanDisk” was used as the search term.

21. Carving

Both data and files can be carved in RECON LAB. There are three options available for carving.

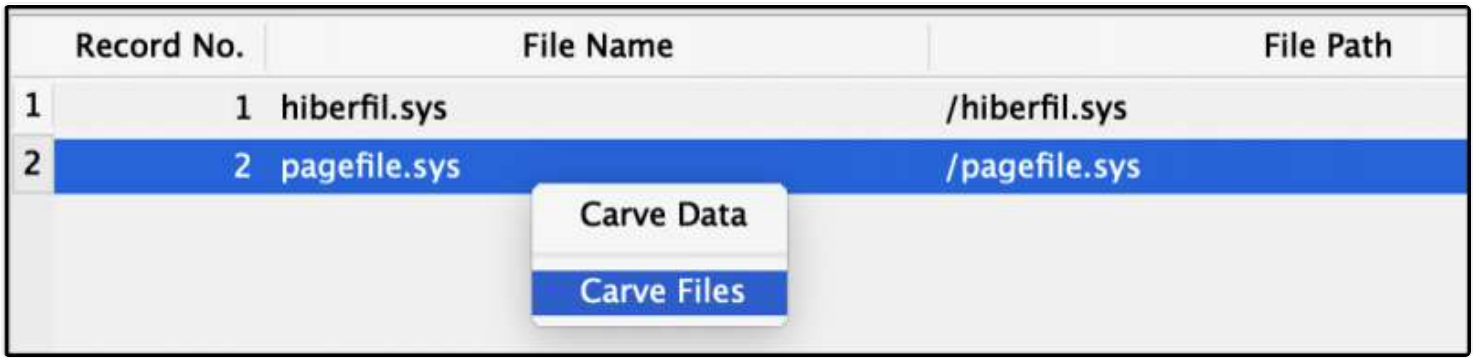
File Carving – recover files from any source.

Data Carving – recovery of information such as email addresses, social security numbers, URLs, etc.

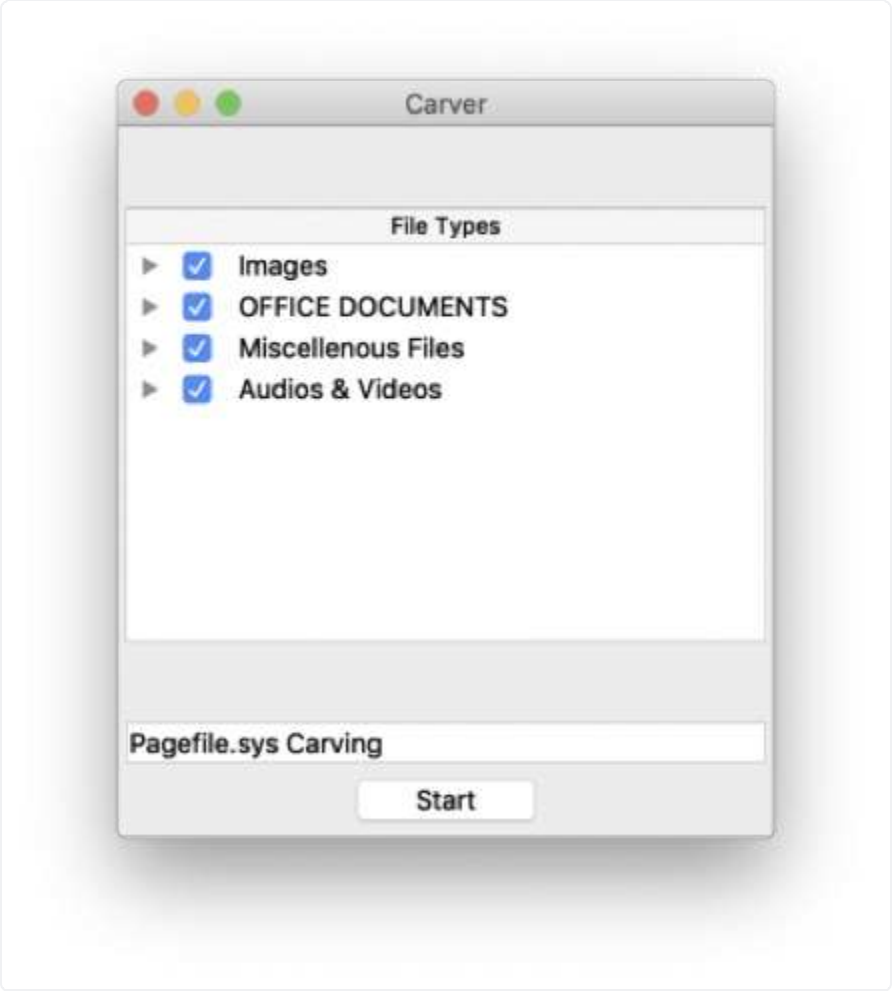
Carving Unallocated Space – a search of files from the unallocated space of supported file systems.

21.1 File Carving

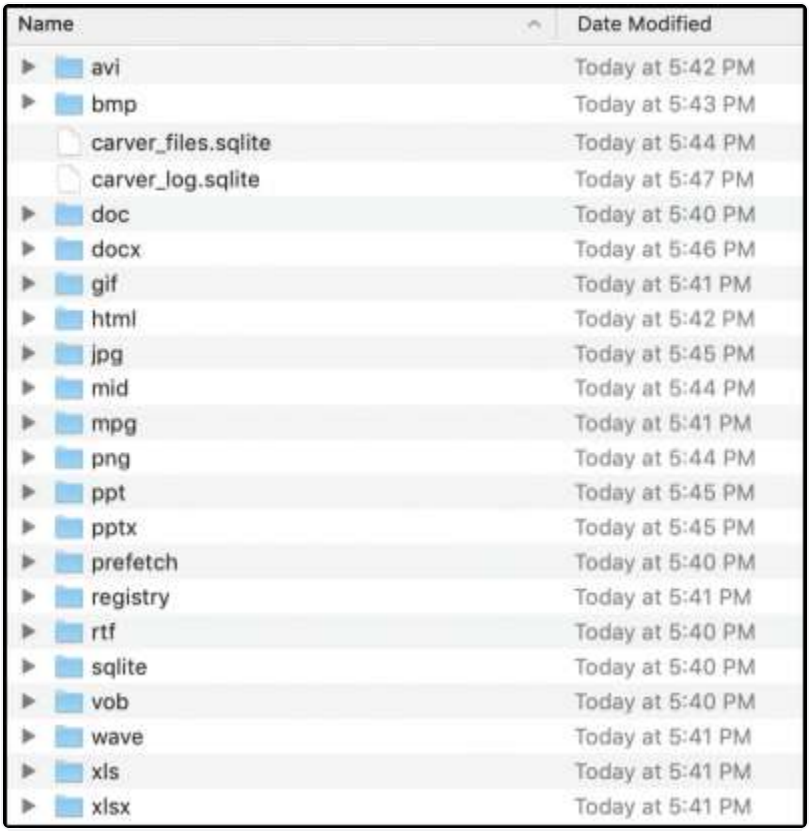
To carve files from within the Table View right-click on an item to process and select “Carve Files”.



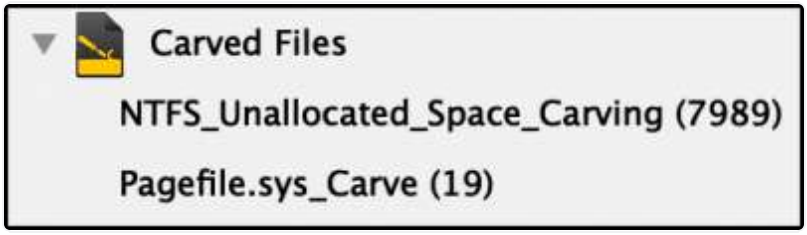
In the example above we are asking RECON LAB to carve files from the pagefile.sys file. A window will appear allowing the selection of files to carve.



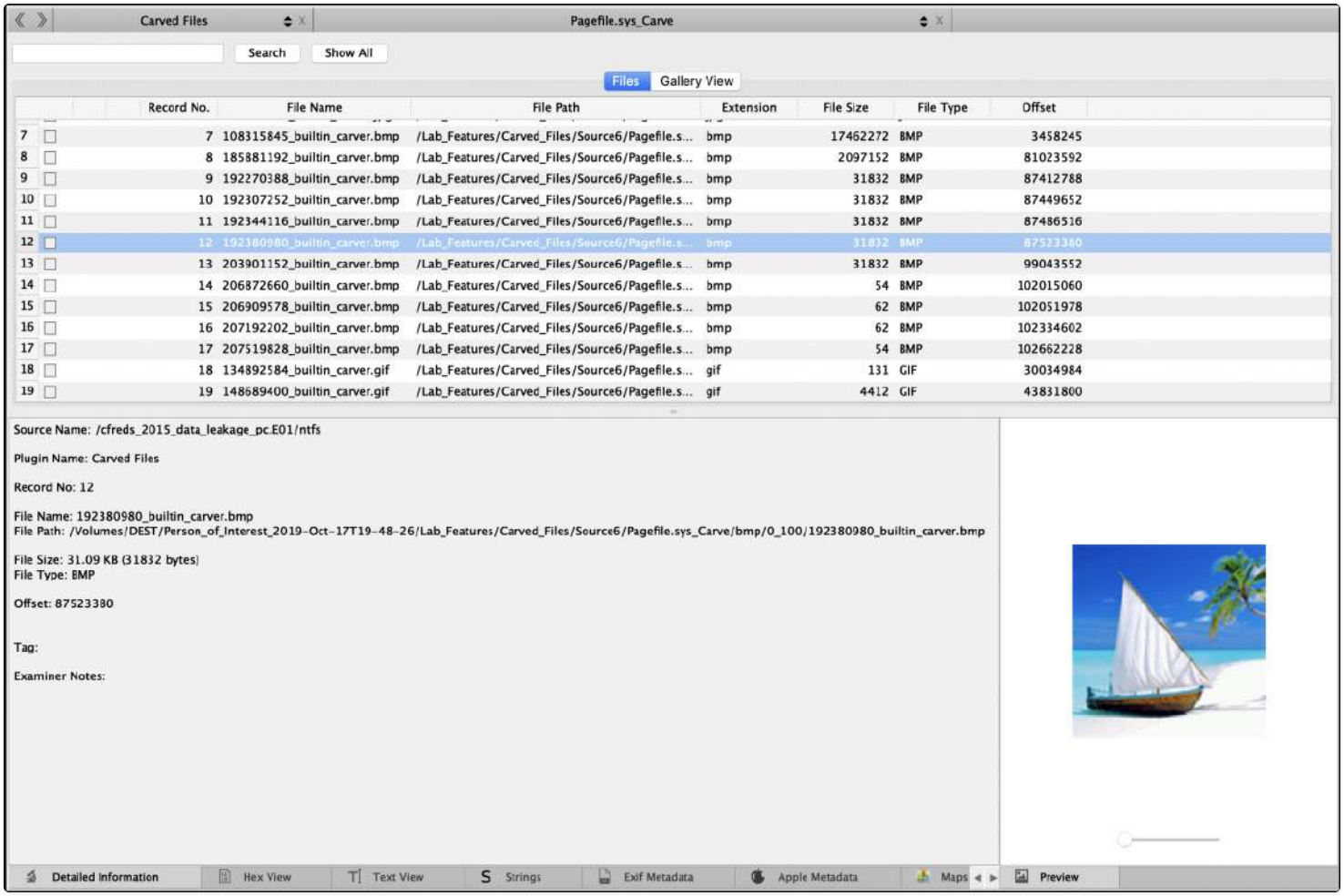
During the carving, a Finder window will appear with live results. These carved files will be added back to RECON LAB for review and documentation when the carving is complete.



When the carving is complete, the results can be found under “Carved Files” in the Sidebar.

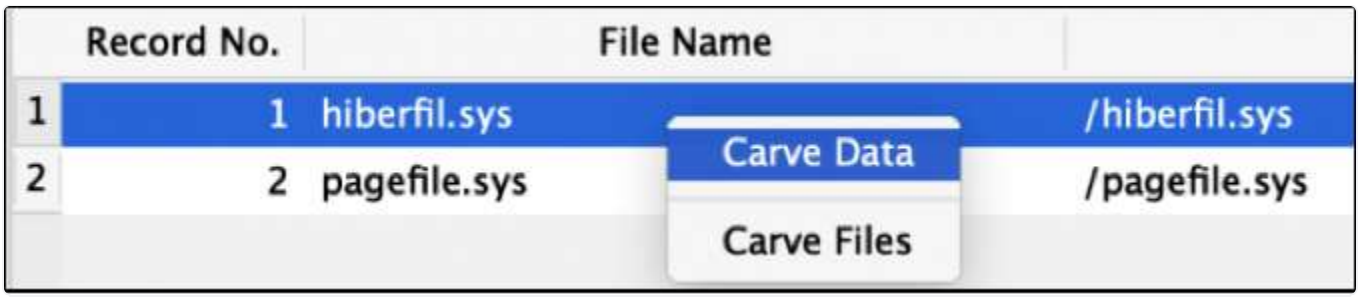


Selecting the item in the Sidebar will load the results of the carving in the Main Viewer window.

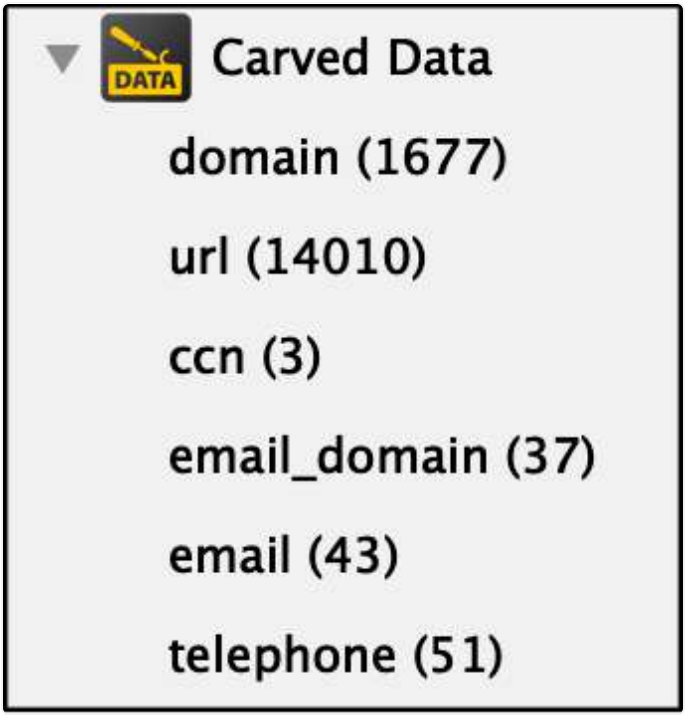


21.2 Data Carving

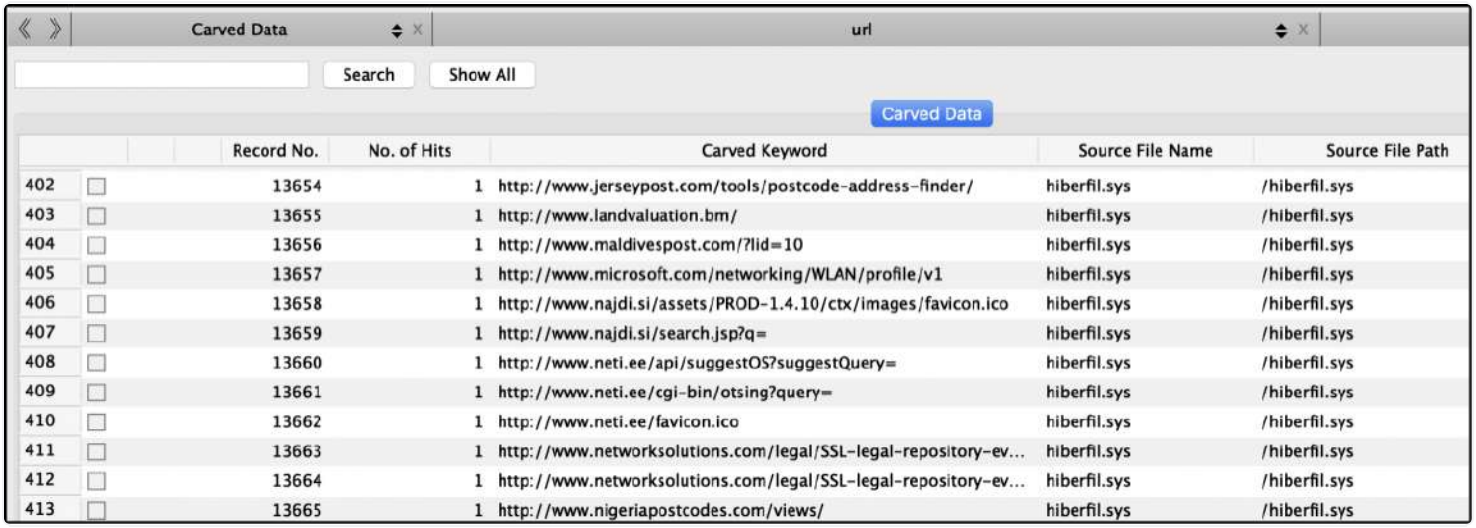
To carve data from within the Table View right-click on an item to process and select “Carve Data”.



In the example above we are asking RECON LAB to carve data from the hiberfil.sys file. A window will appear allowing the selection of files to carve.



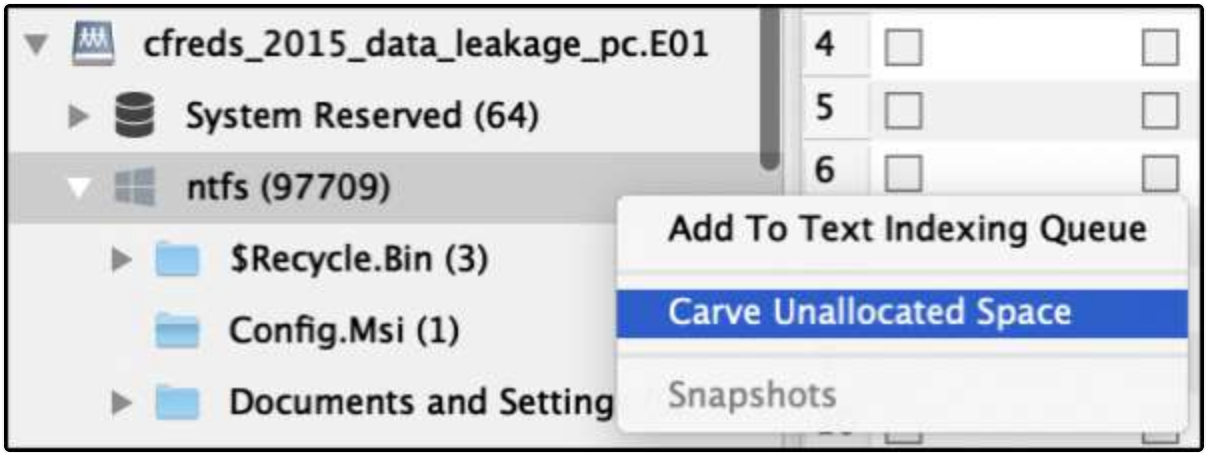
When the carving is complete, the results can be found under “Carved Files” in the Sidebar.



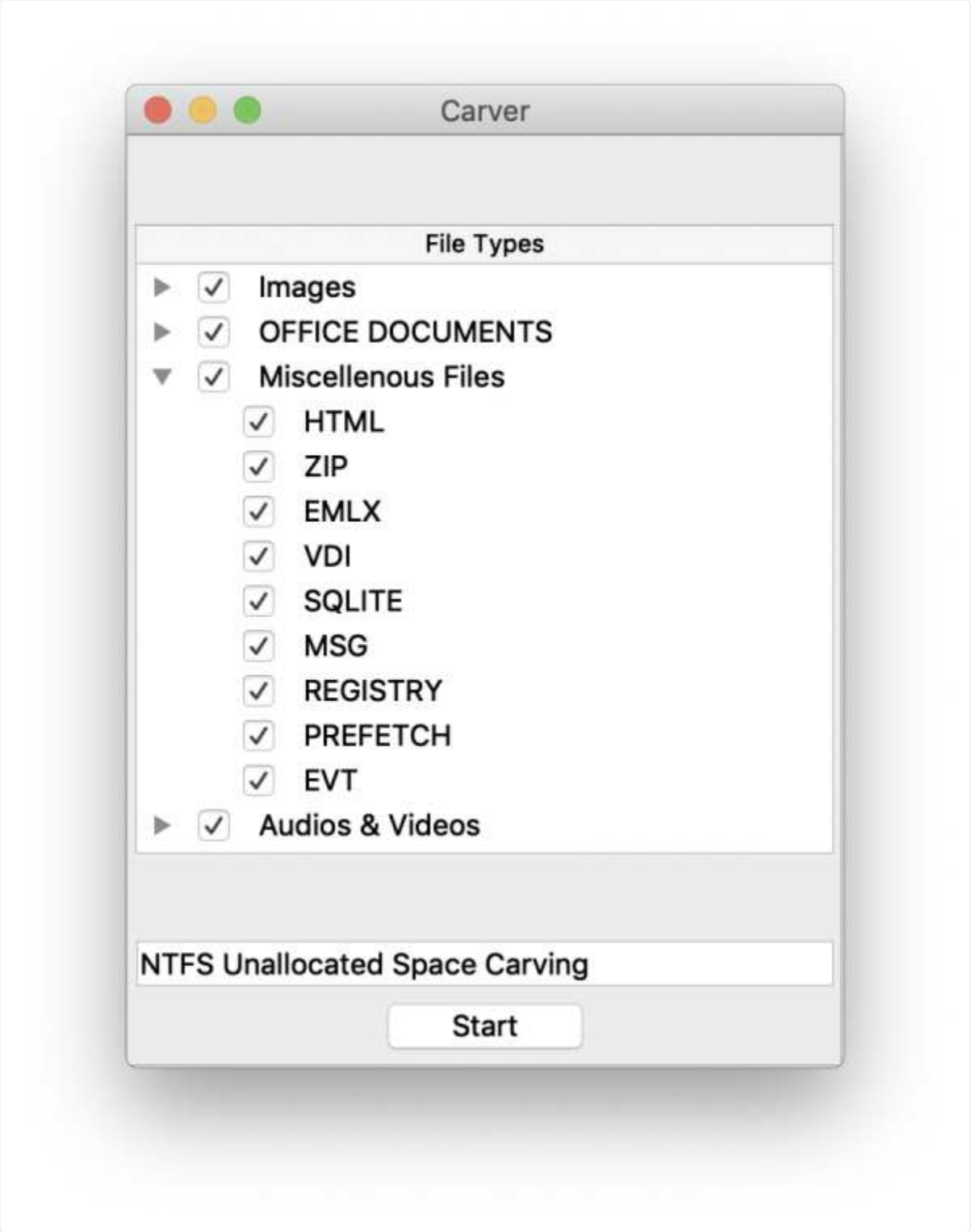
		Record No.	No. of Hits	Carved Keyword	Source File Name	Source File Path
402		13654	1	http://www.jerseypost.com/tools/postcode-address-finder/	hiberfil.sys	/hiberfil.sys
403		13655	1	http://www.landvaluation.bm/	hiberfil.sys	/hiberfil.sys
404		13656	1	http://www.maldivespost.com/?lid=10	hiberfil.sys	/hiberfil.sys
405		13657	1	http://www.microsoft.com/networking/WLAN/profile/v1	hiberfil.sys	/hiberfil.sys
406		13658	1	http://www.najdi.si/assets/PROD-1.4.10/ctx/images/favicon.ico	hiberfil.sys	/hiberfil.sys
407		13659	1	http://www.najdi.si/search.jsp?q=	hiberfil.sys	/hiberfil.sys
408		13660	1	http://www.neti.ee/api/suggestOS?suggestQuery=	hiberfil.sys	/hiberfil.sys
409		13661	1	http://www.neti.ee/cgi-bin/otsing?query=	hiberfil.sys	/hiberfil.sys
410		13662	1	http://www.neti.ee/favicon.ico	hiberfil.sys	/hiberfil.sys
411		13663	1	http://www.networksolutions.com/legal/SSL-legal-repository-ev...	hiberfil.sys	/hiberfil.sys
412		13664	1	http://www.networksolutions.com/legal/SSL-legal-repository-ev...	hiberfil.sys	/hiberfil.sys
413		13665	1	http://www.nigeriapostcodes.com/views/	hiberfil.sys	/hiberfil.sys

Selecting the item in the Sidebar will load the results of the data carving in the Main Viewer window.

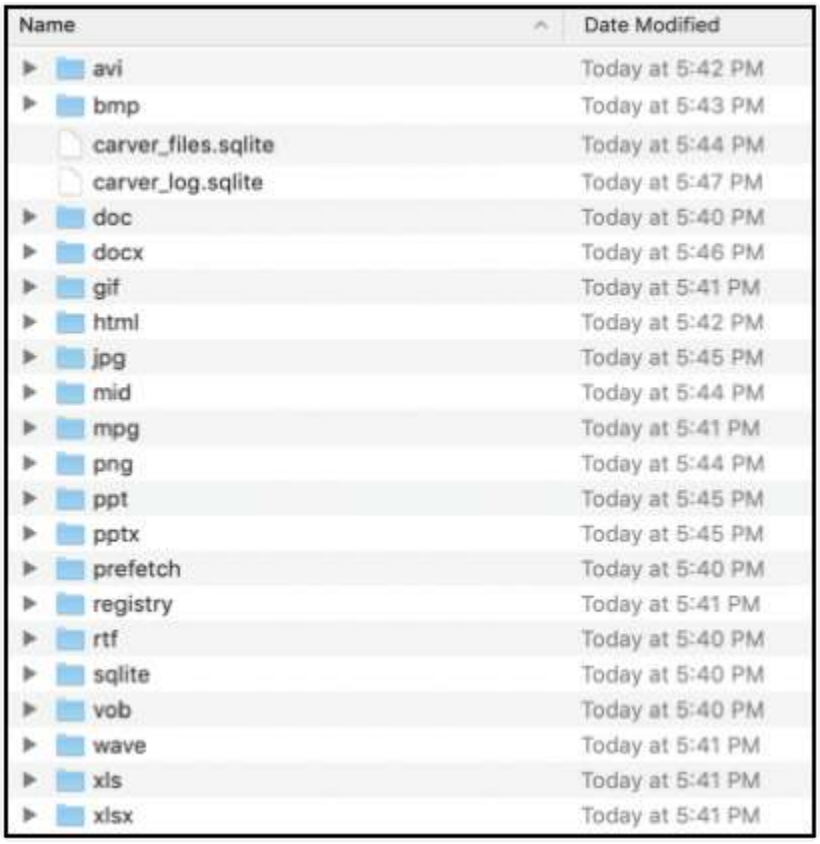
21.3 Carving Unallocated Space



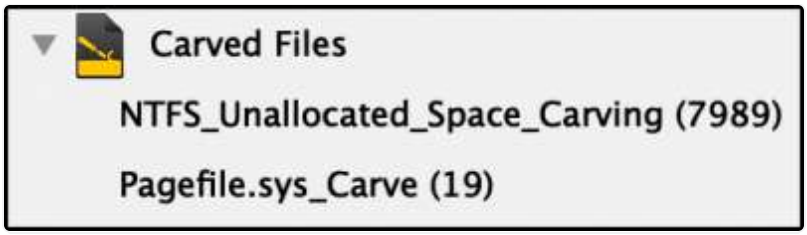
To carve files from the unallocated space of a supported file system right-click on the volume under the Source in the Sidebar and select “Carve Unallocated Space”.



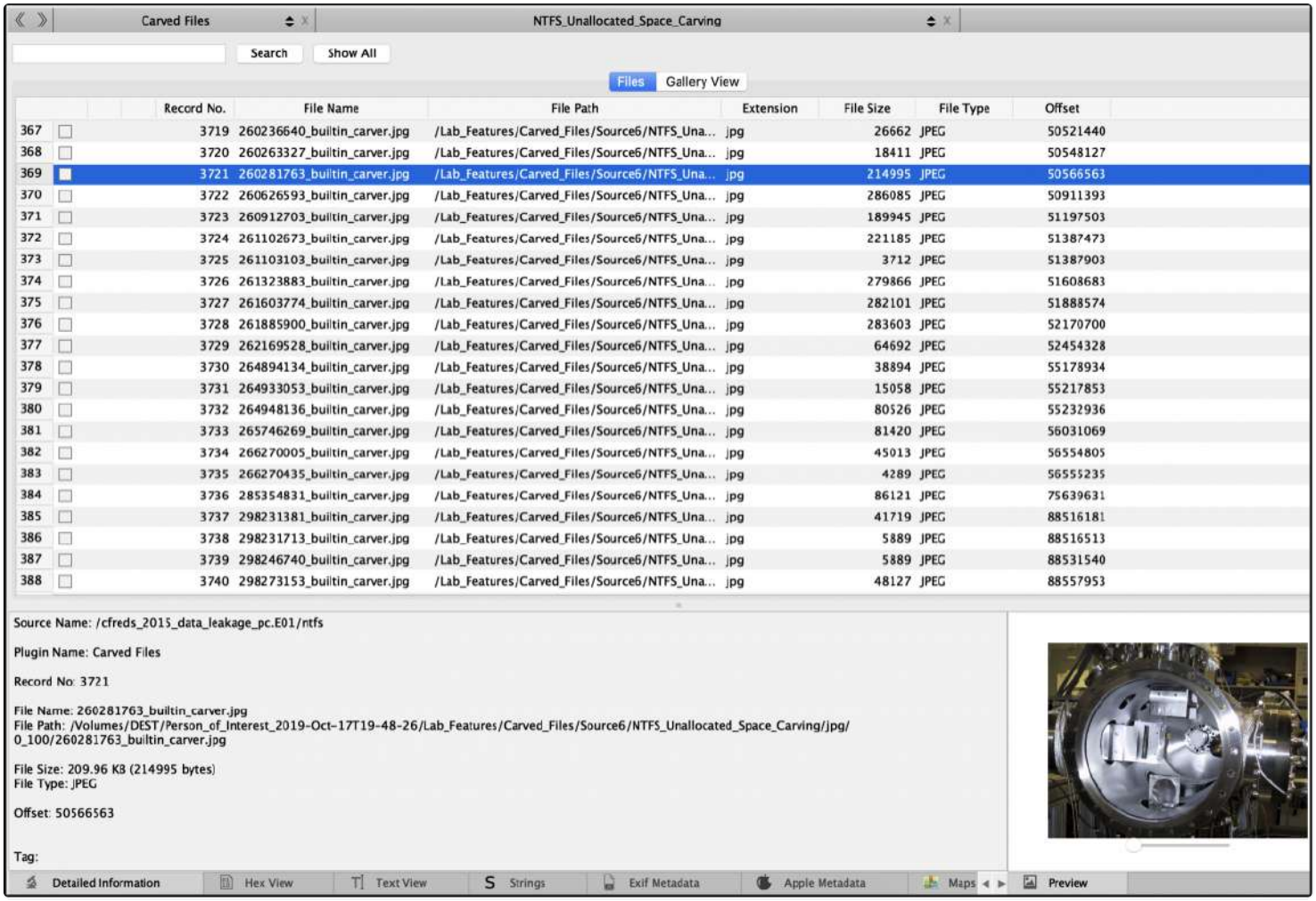
In the example above we are asking RECON LAB to carve files from the unallocated space of an NTFS volume. A window will appear allowing the selection of files to carve.



During the carving, a Finder window will appear with live results. These carved files will be added back to RECON LAB for review and documentation when the carving is complete.



When the carving is complete, the results can be found under “Carved Files” in the Sidebar.

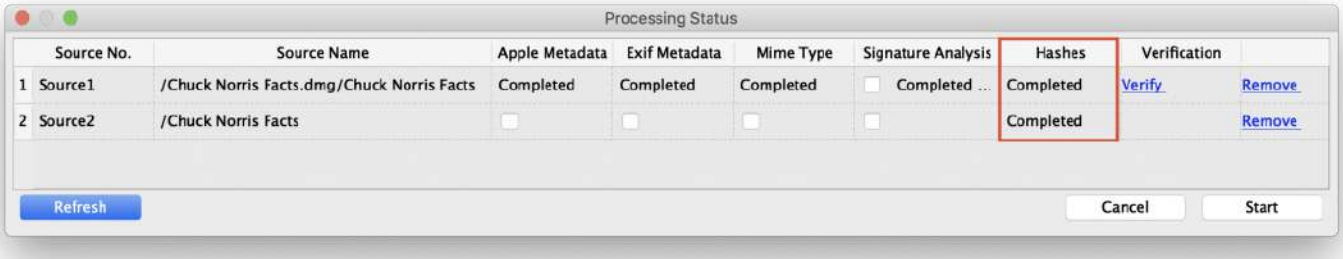


Selecting the item in the Sidebar will load the results of the carving in the Main Viewer window.

22. Hash Sets

RECON LAB has the ability to create and import commonly used forensic hash set databases.

The hash sets can help an examiner identify files and/or remove files from a case.

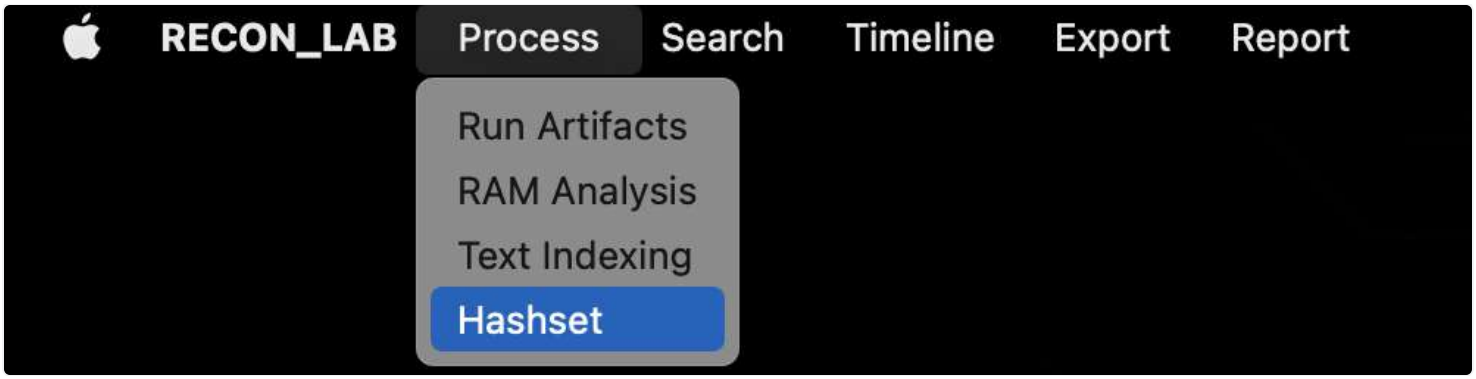


Before using hash set databases RECON LAB will need to hash the files in the source first. To find out if hashing is completed for a source click the Processing Status icon in the Top Menu.

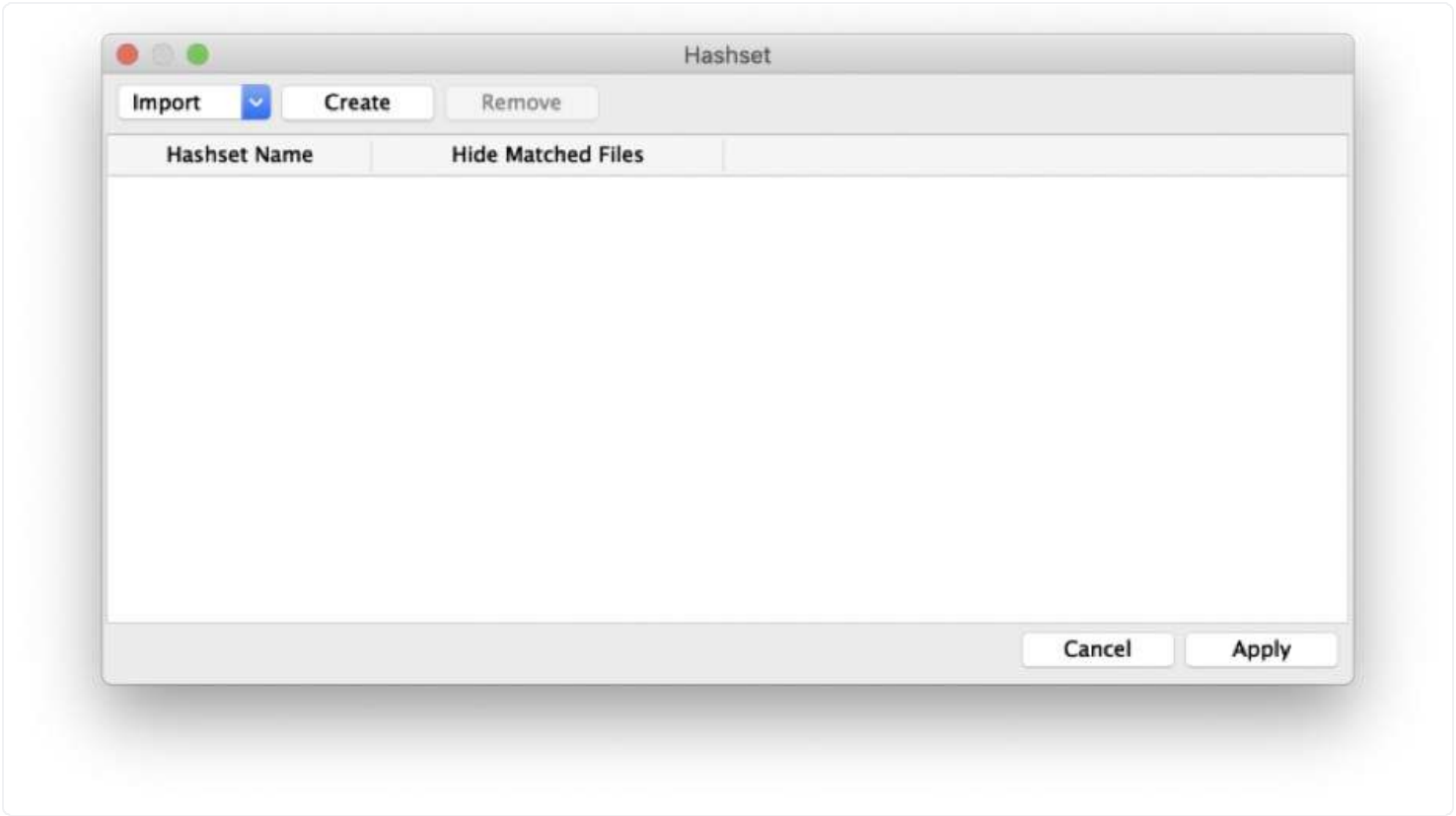
If the hashes have not been calculated for a Source click the checkbox and “Start”.

22.1 Creating Hash Sets

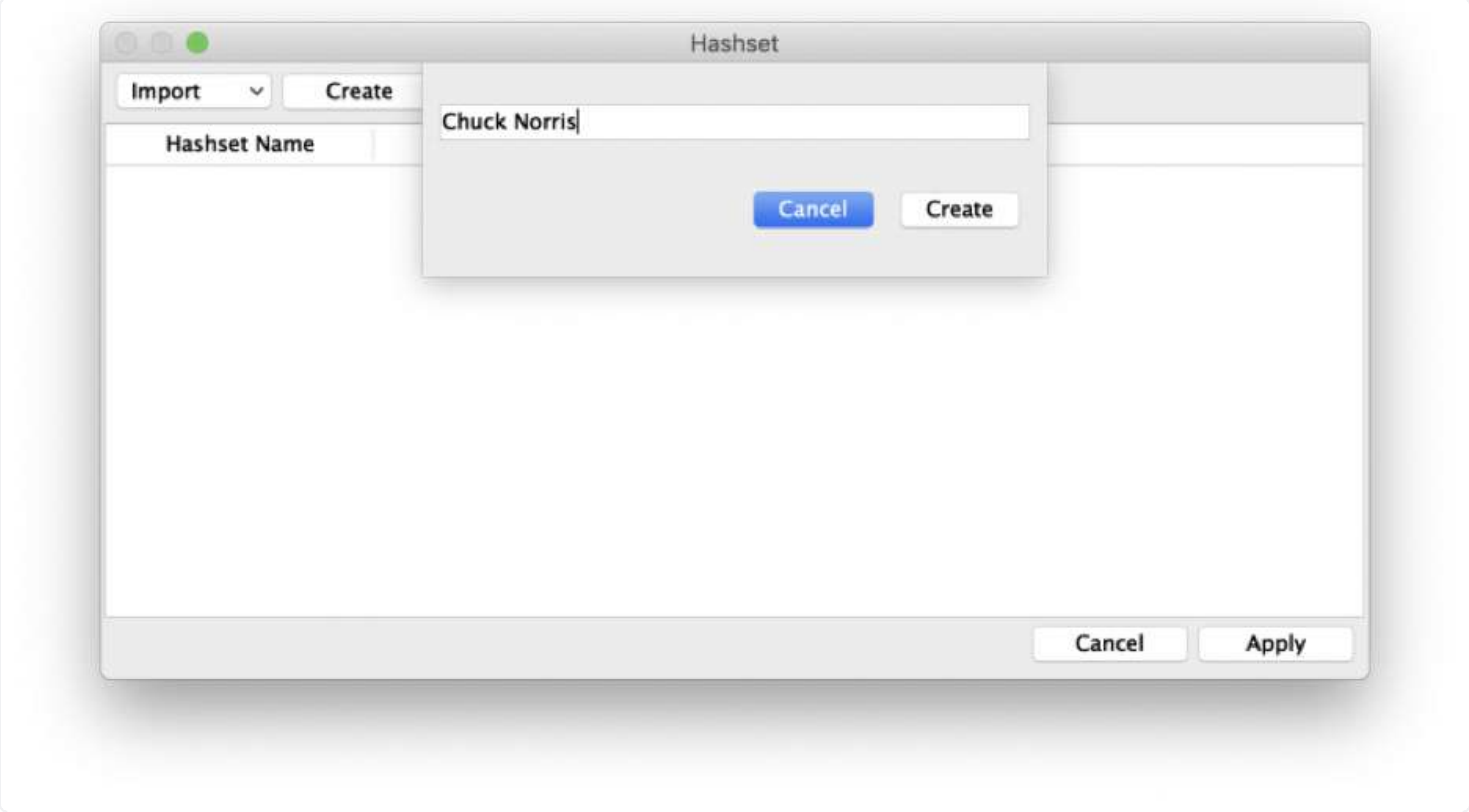
Before working with hash set features, a hash set category must be created and file hashes must be added.



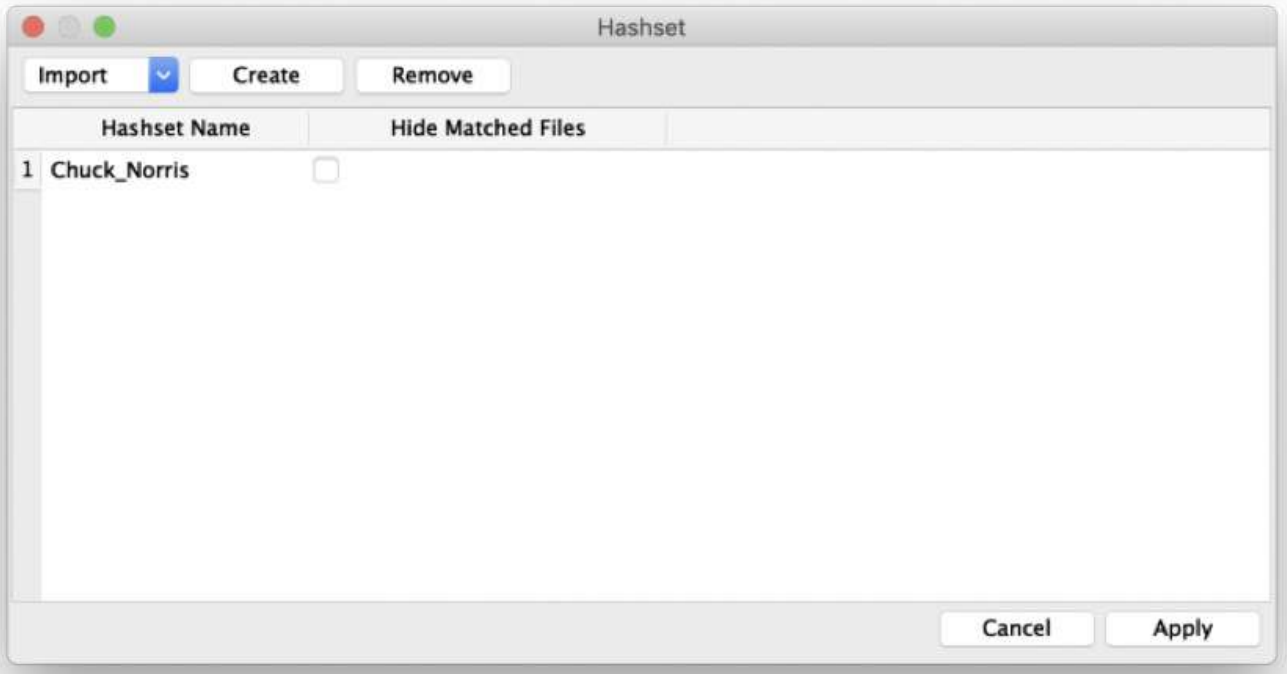
To create a new hash set, select Process > Hashset from the Menu Bar.



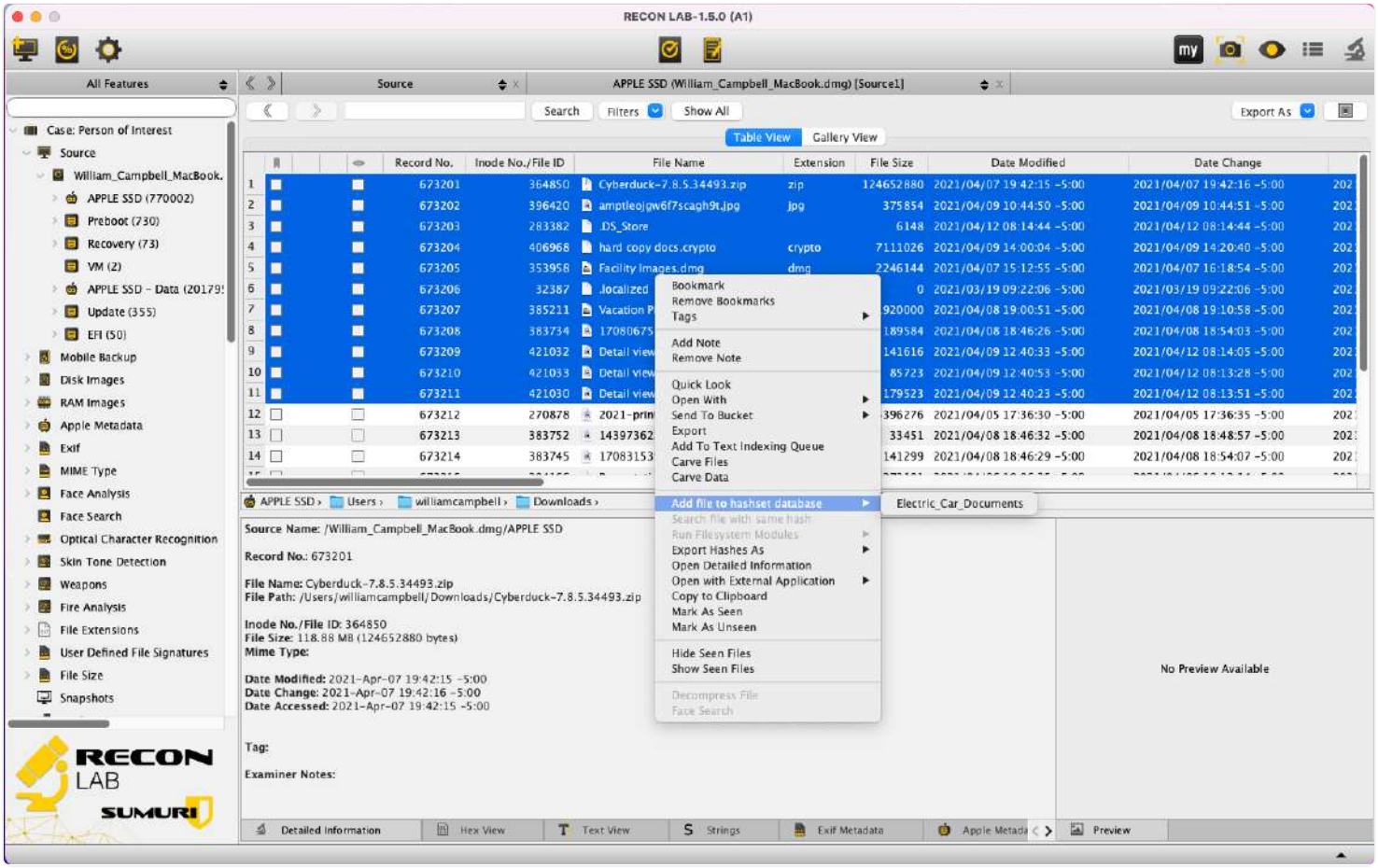
The Hash Set main window will appear.



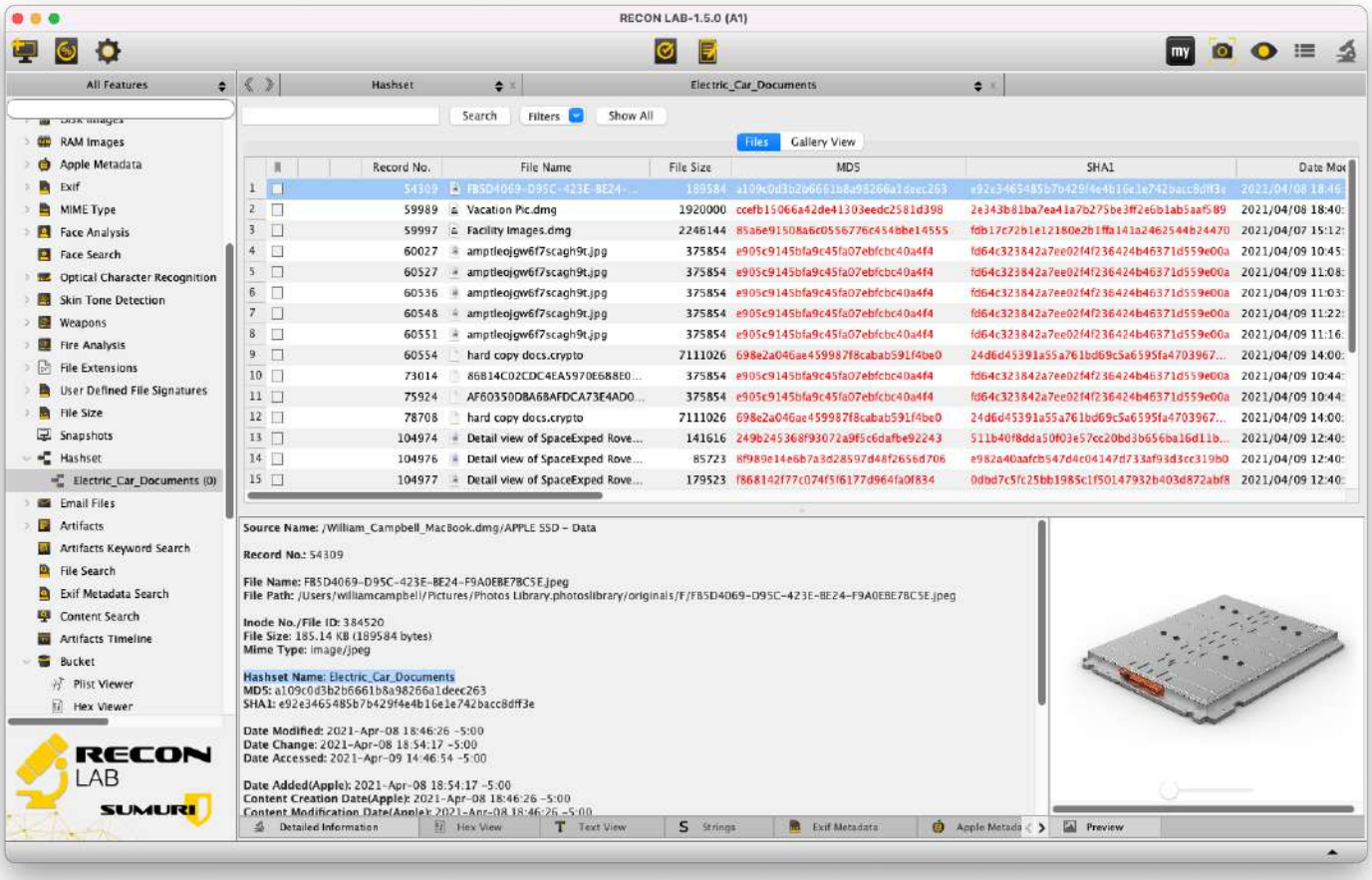
Click “Create” and enter a name for your new hash set and click “Create” again.



The new hash set category is now created.

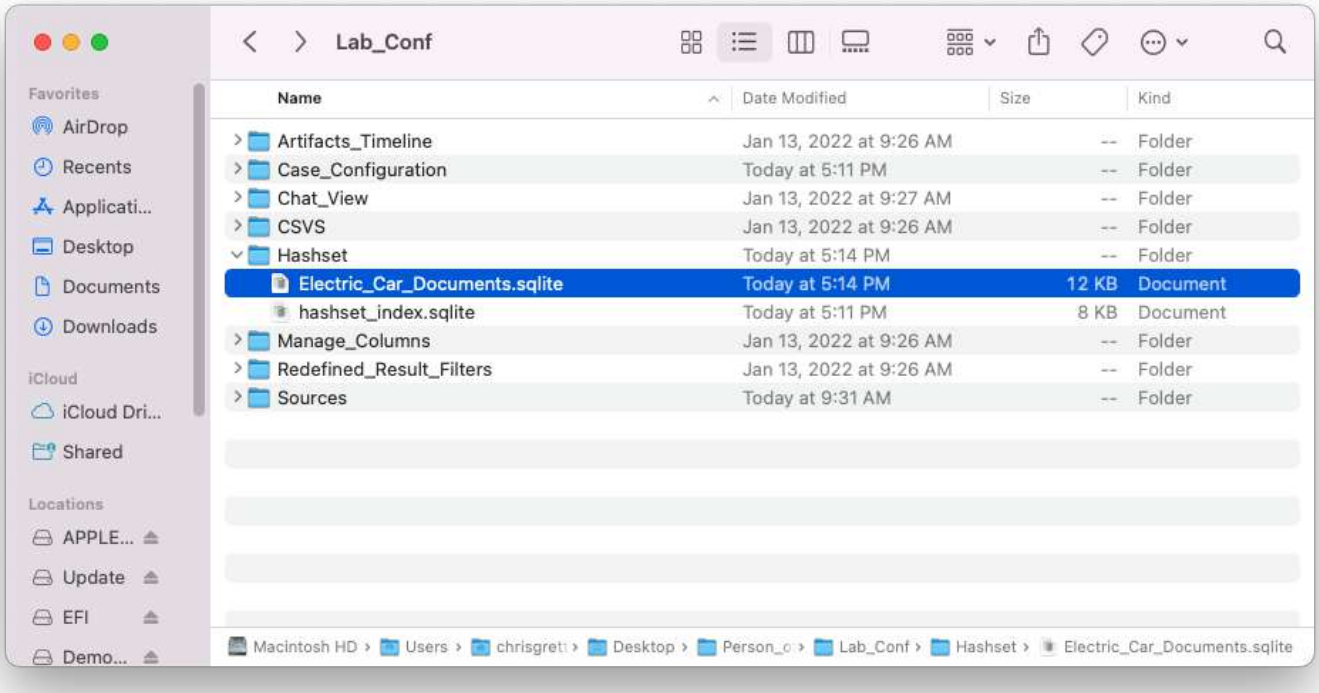


To add files to the new category right-click on any files that have previously been hashed and select “Add file to hashset database”.



Any files matching the hashes within the hash set database will be identified in the Table View Column “Hashset Name” and in the Detailed Information pane.

Archiving the Hash Set Database

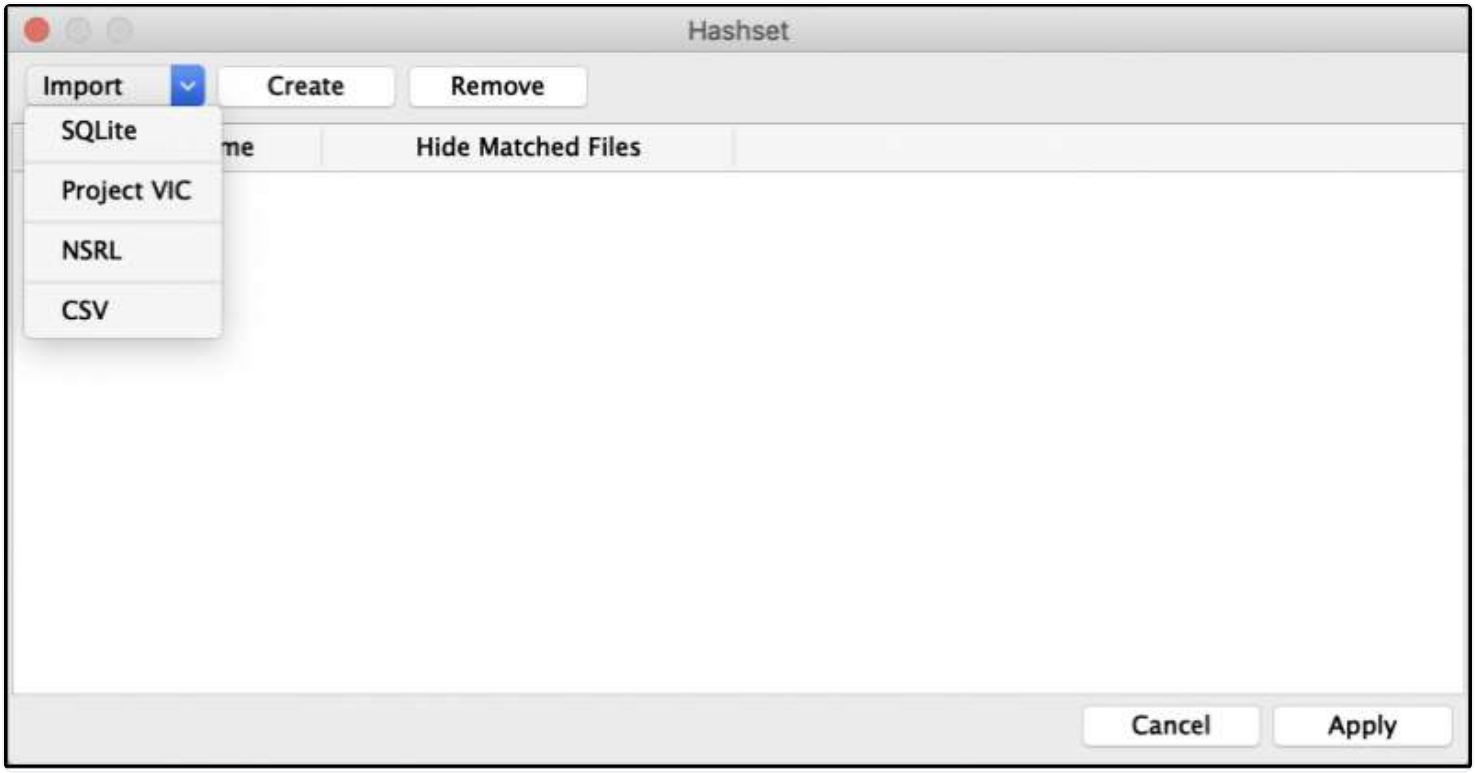


If you want to archive your newly created hash set database so it can be imported into other cases navigate the “Lab_Conf – Hashset” directory in your RECON LAB Case Folder. Here you will find the hash set databases to archive.

22.2 Importing Hash Sets

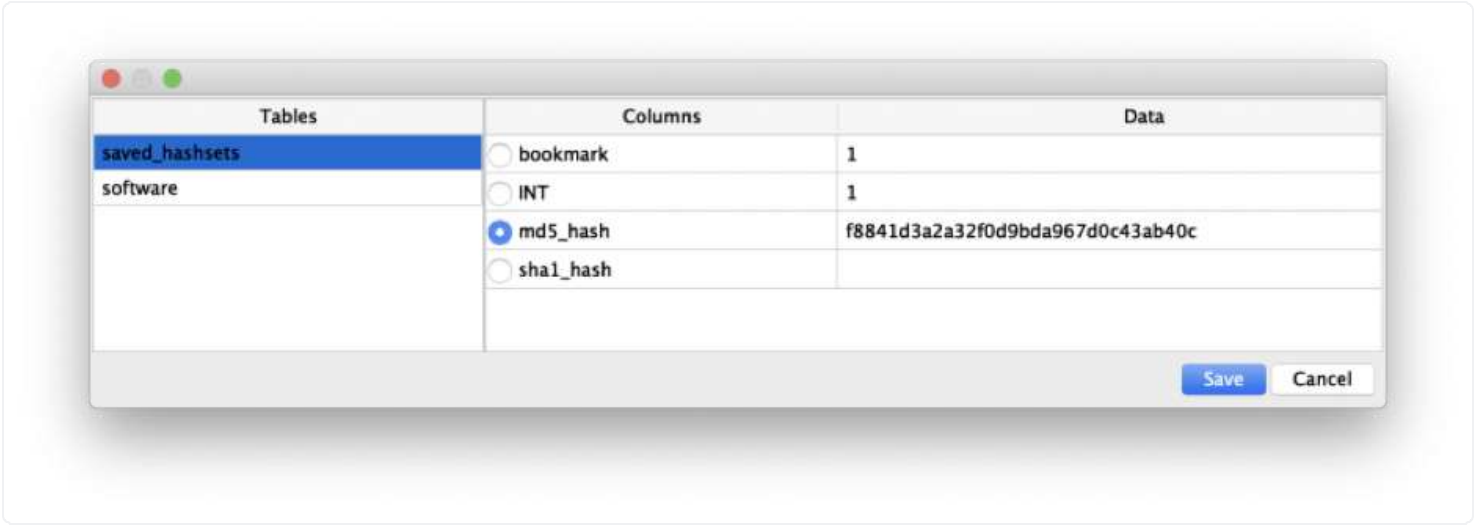
RECON LAB can import the following hash set database formats:

- RECON LAB SQLite
- Project VIC
- NSRL
- CSV

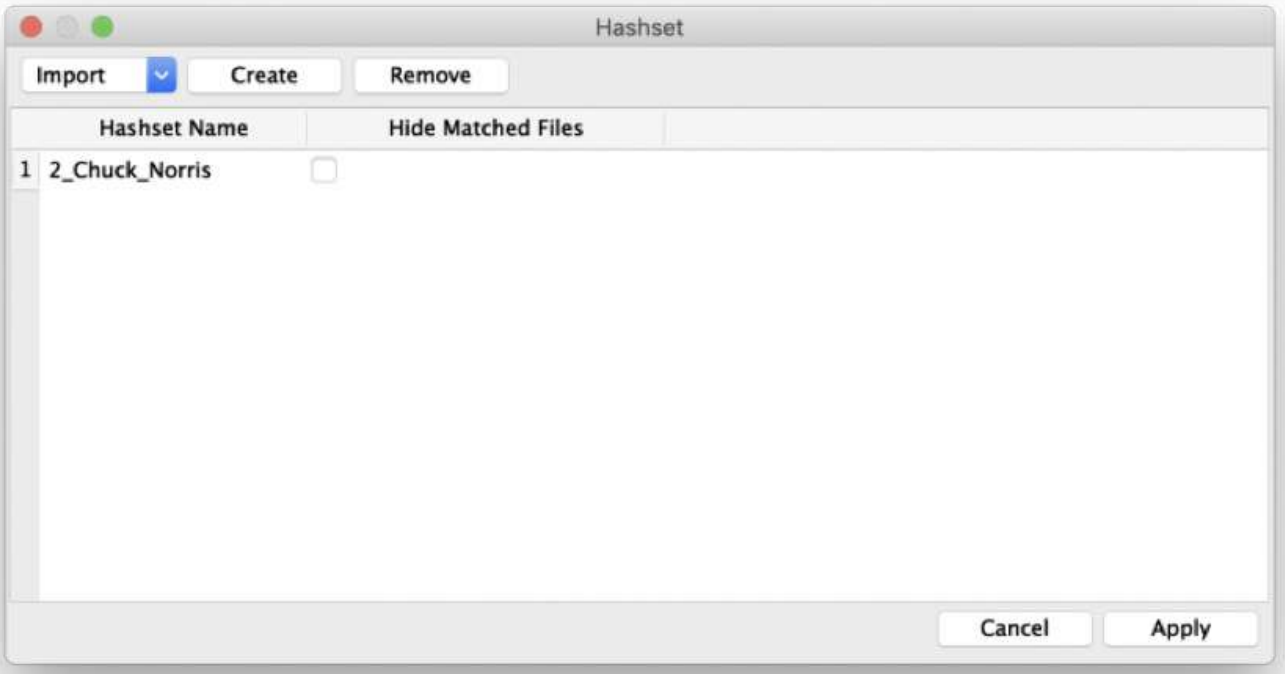


To import a hash set database click on the “Hashset” icon in the Top Menu. Use the dropdown box to select a hash set database format.

Navigate to the location of the database and click “Open”.



You may be prompted to select a specific table in order to import. For RECON LAB SQLite databases select the “saved_hashsets” table and the “md5_hash” column.

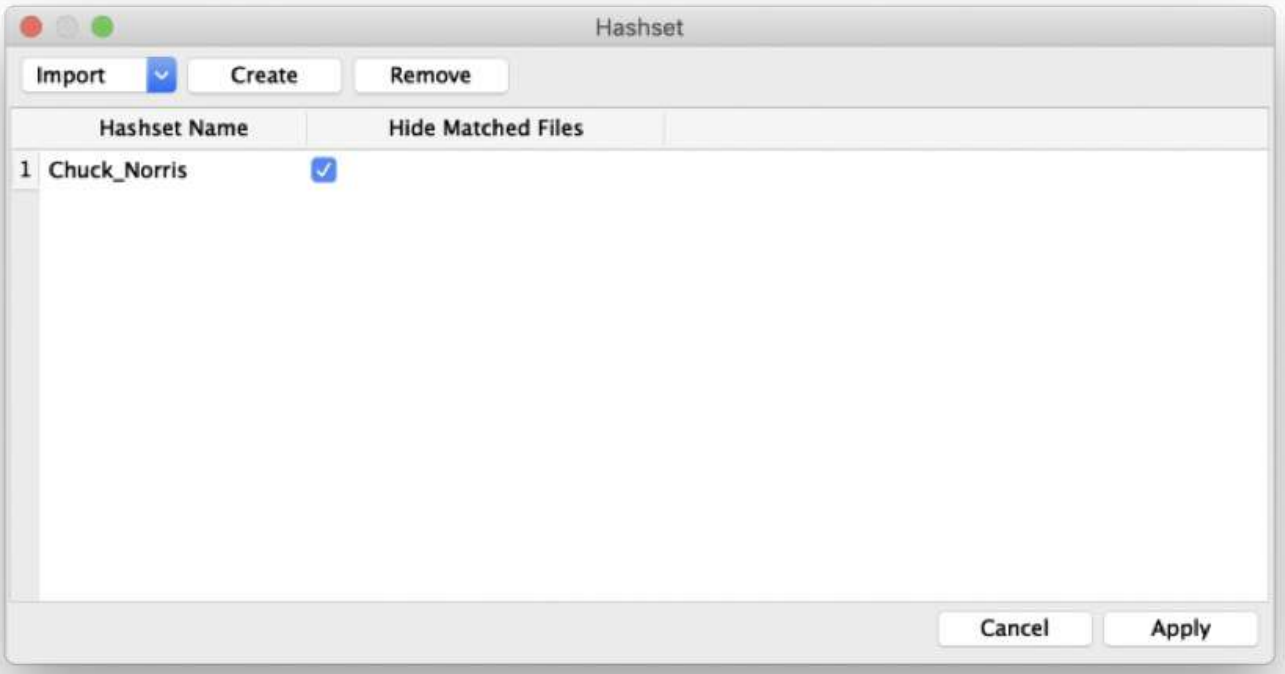


After clicking “Save” the new hash set will be available for use.

22.3 Removing Files From Case Using Hash Sets

RECON LAB provides the option of removing (hiding) files in a case that match hashes found in a hash set database. This is useful for hiding benign system files that are irrelevant to your investigation.

To remove files from a case with hashes click on the “Hashset” icon in the Top Menu.



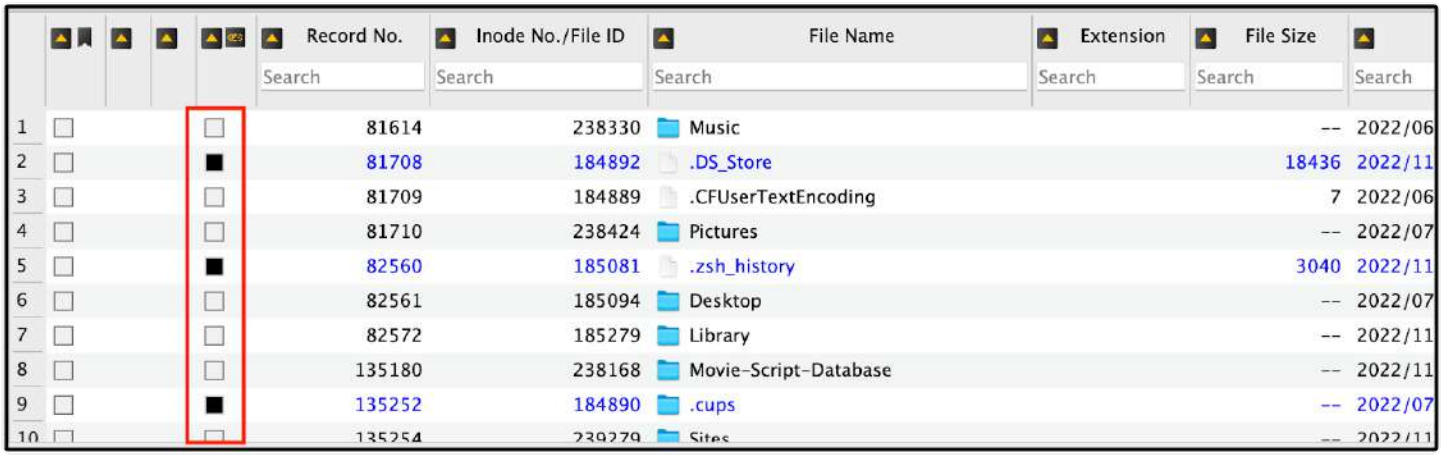
Click the checkbox next to the hash set under the column “Hide Matched Files” and then “Apply”.

Files matching the hashes in the hash set database will be hidden.

To unhide the files uncheck the checkbox and hit “Apply” again.

23. Hide or Show Files

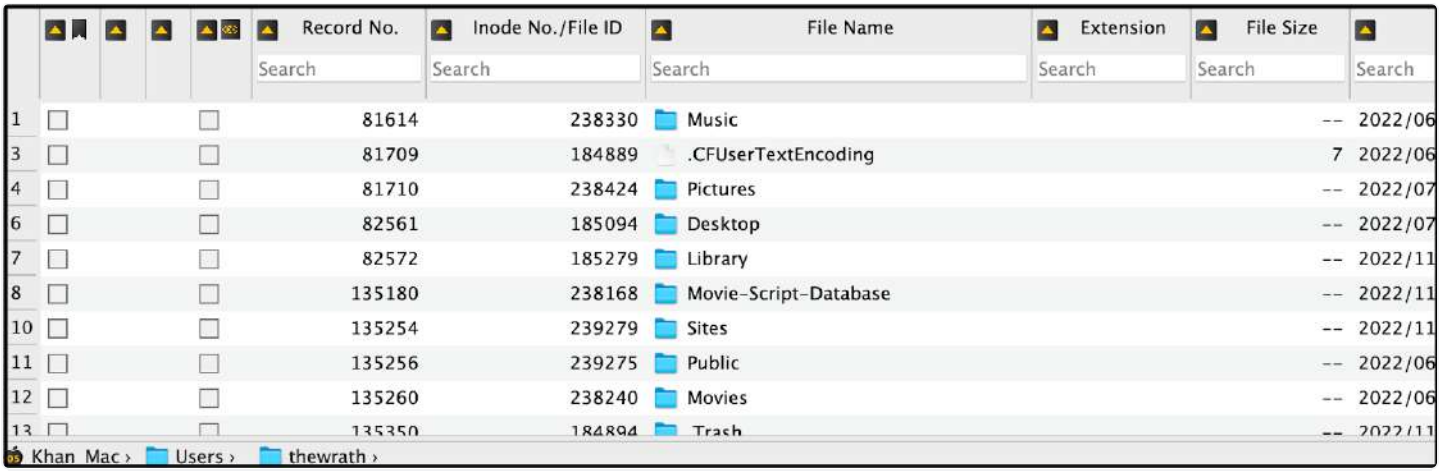
RECON LAB includes a feature to “Mark files as Seen”. This is a way of tracking files that you have already reviewed. To mark a file as seen click the checkbox in the “Seen” column.



				Record No.	Inode No./File ID	File Name	Extension	File Size	
				Search	Search	Search	Search	Search	Search
1	☐		☐	81614	238330	Music		--	2022/06
2	☐		■	81708	184892	.DS_Store		18436	2022/11
3	☐		☐	81709	184889	.CFUserTextEncoding		7	2022/06
4	☐		☐	81710	238424	Pictures		--	2022/07
5	☐		■	82560	185081	.zsh_history		3040	2022/11
6	☐		☐	82561	185094	Desktop		--	2022/07
7	☐		☐	82572	185279	Library		--	2022/11
8	☐		☐	135180	238168	Movie-Script-Database		--	2022/11
9	☐		■	135252	184890	.cups		--	2022/07
10	☐		☐	135254	239279	Sites		--	2022/11

Files marked as seen can also be “hidden” from the case view. To “Hide Seen Files” or “Show Seen Files” right-click on any file and make a selection.

In the below image “Hide Seen Files” was activated. Only the files that were left unchecked above are still visible.



				Record No.	Inode No./File ID	File Name	Extension	File Size	
				Search	Search	Search	Search	Search	Search
1	☐		☐	81614	238330	Music		--	2022/06
3	☐		☐	81709	184889	.CFUserTextEncoding		7	2022/06
4	☐		☐	81710	238424	Pictures		--	2022/07
6	☐		☐	82561	185094	Desktop		--	2022/07
7	☐		☐	82572	185279	Library		--	2022/11
8	☐		☐	135180	238168	Movie-Script-Database		--	2022/11
10	☐		☐	135254	239279	Sites		--	2022/11
11	☐		☐	135256	239275	Public		--	2022/06
12	☐		☐	135260	238240	Movies		--	2022/06
13	☐		☐	135350	184894	Trash		--	2022/11

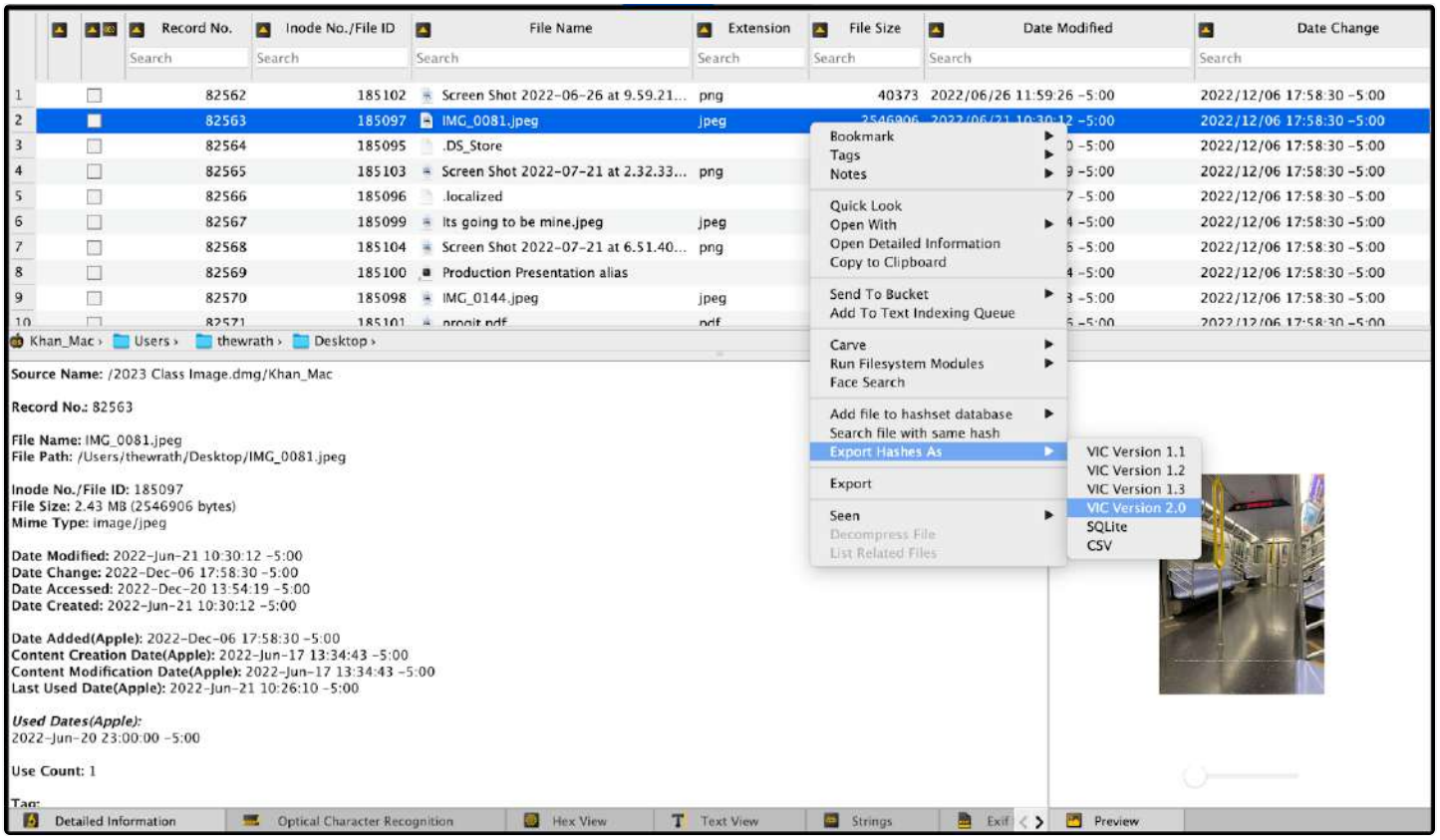
Khan Mac › Users › thewrath ›

24. Project Vic

RECON LAB supports Project VIC database formats Versions 1.1, 1.2 and 1.3.

For more information about Project VIC please visit their website here: https://www.projectvic.org

Exporting as Project VIC Format



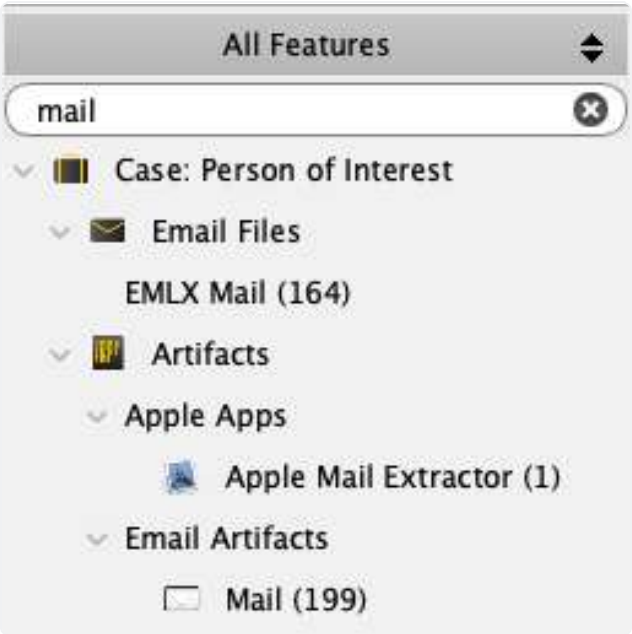
To export files in one of Project VIC formats select the files of interest and right-click. Select “Export Hashes as VIC” and select the version of choice.

The above picture is an example of a Project VIC export using RECON LAB.

25. Email Analysis

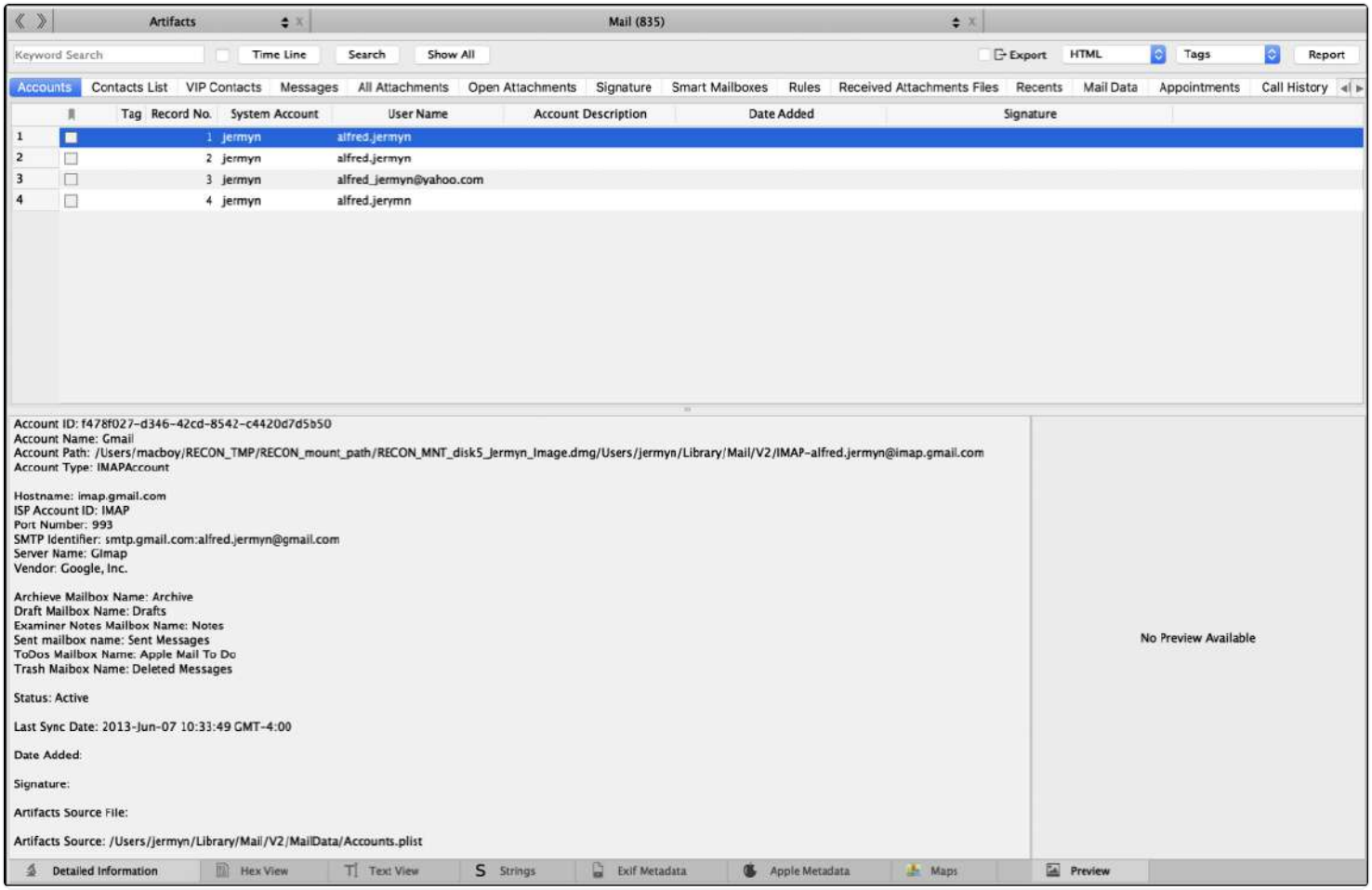
There are two ways to conduct email analysis in RECON LAB.

1. Automated Artifact Analysis using plugins.
2. Email Files Module



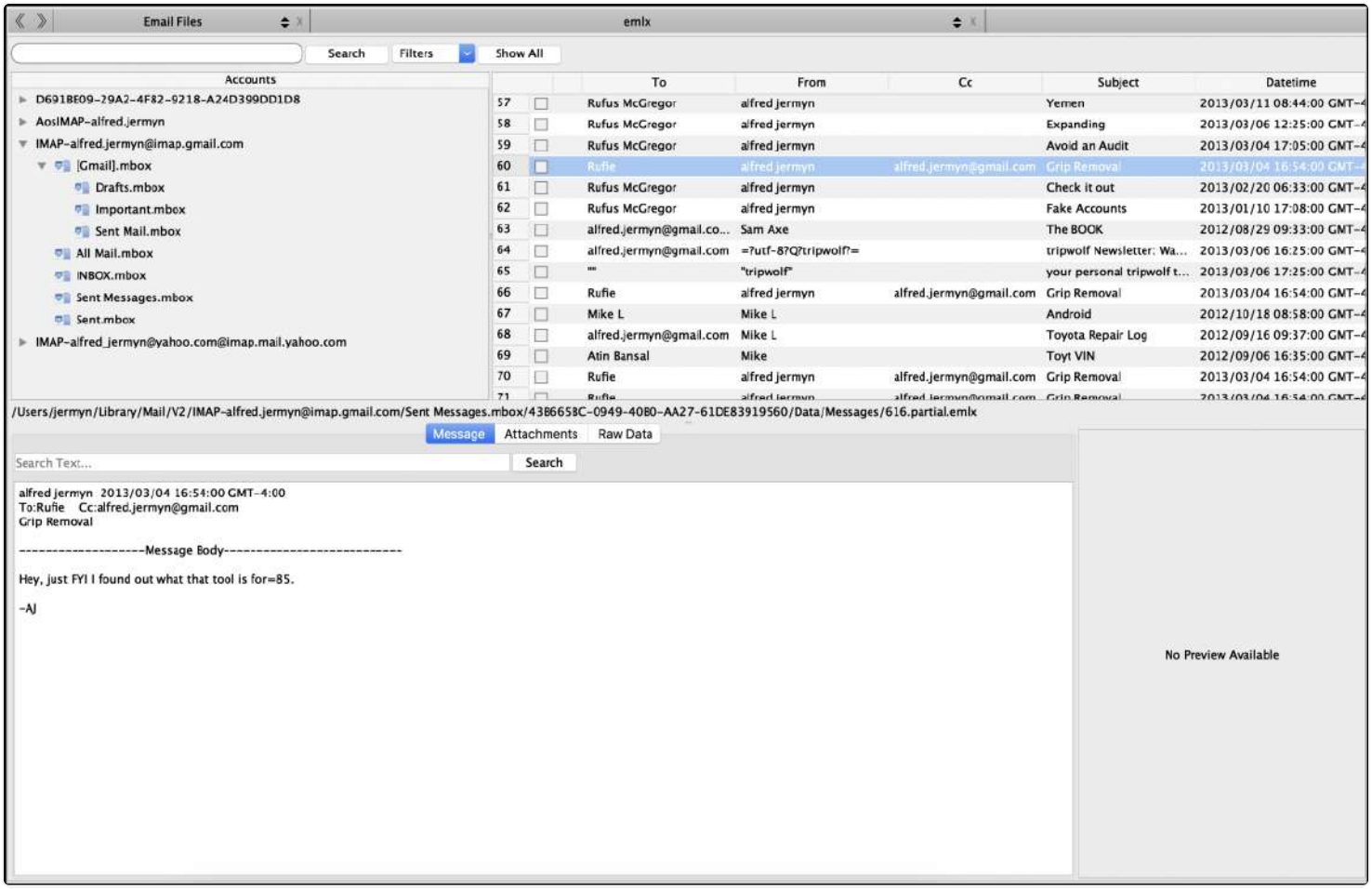
Automated Artifacts Analysis

There are a variety of automated plugins for various email clients. If an automated analysis is run and artifacts are found for a specific email client the results will be loaded in the Sidebar for access. To view the results in the Main Viewer window select the plugin in the Sidebar.



Email Files Module

A separate “Email Files Module” can be found in the Sidebar. This module attempts to unify as many mail accounts as possible into one review platform.



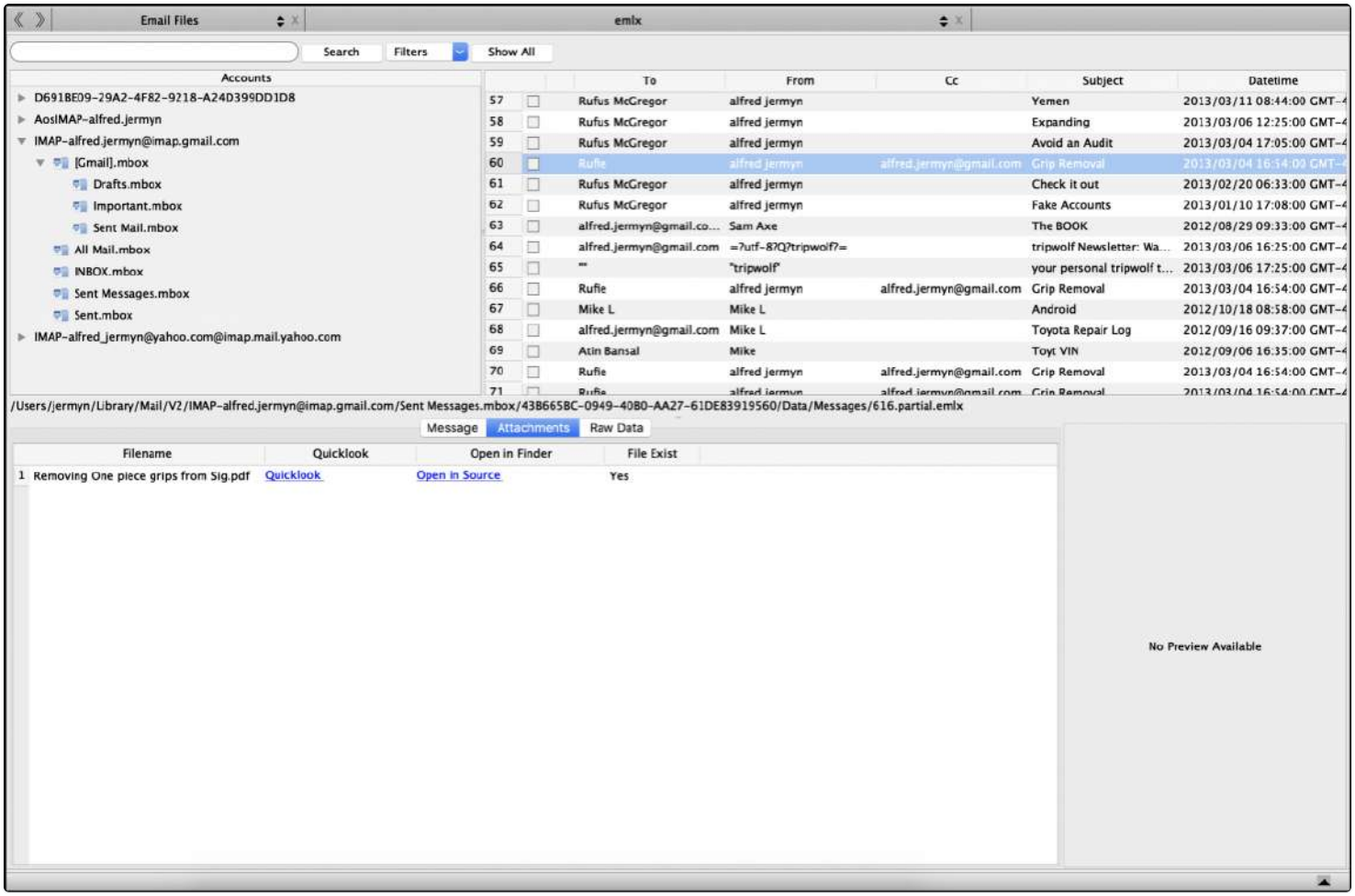
The upper left panel is the “Accounts” pane. All supported mail accounts will be found here along with their mailboxes.

The right panel contains a table view of supported mail messages.

Additional information is provided below when a mail message is selected.

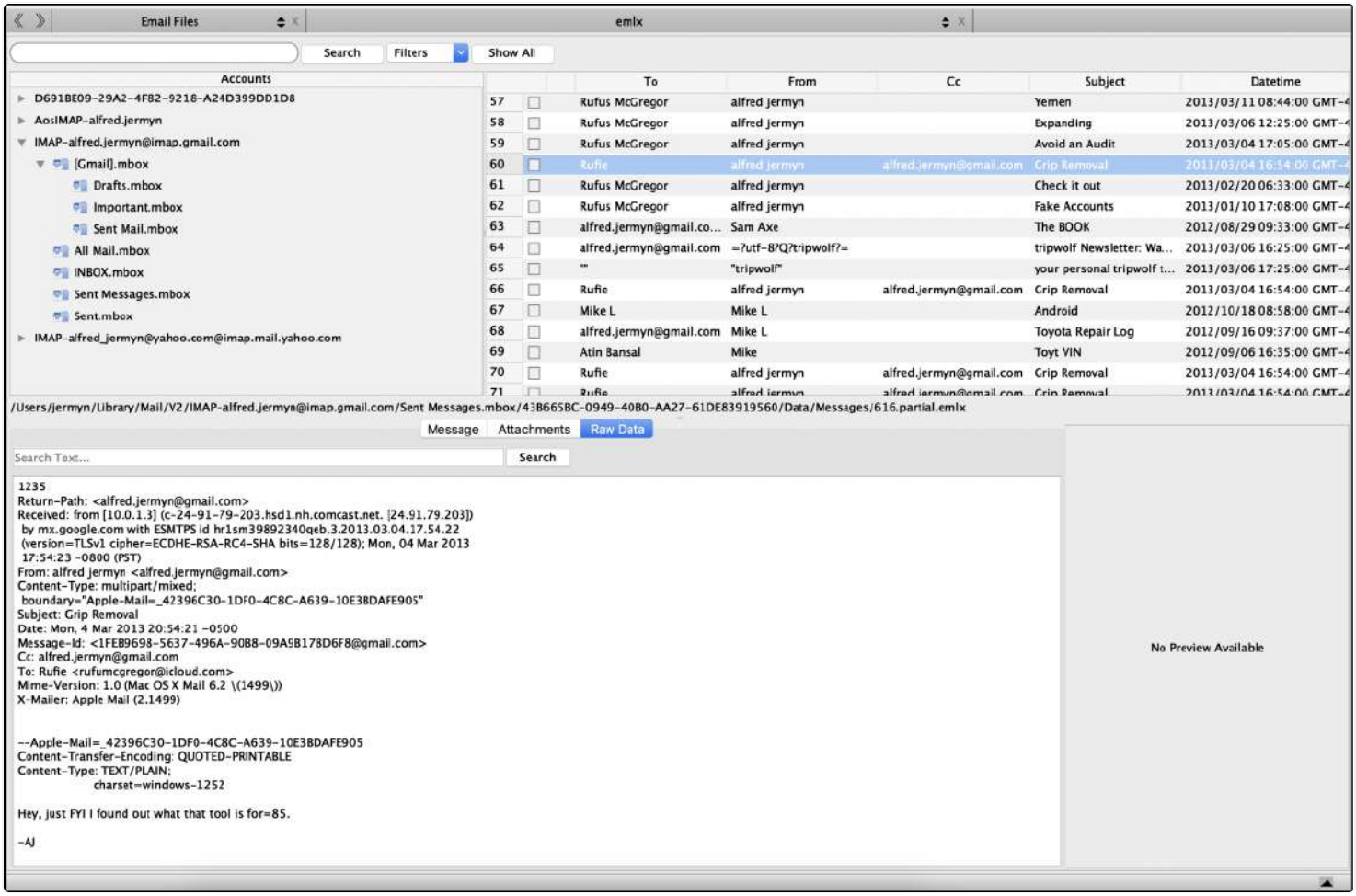
The “Message” tab seen above shows the message in HTML view.

Attachments



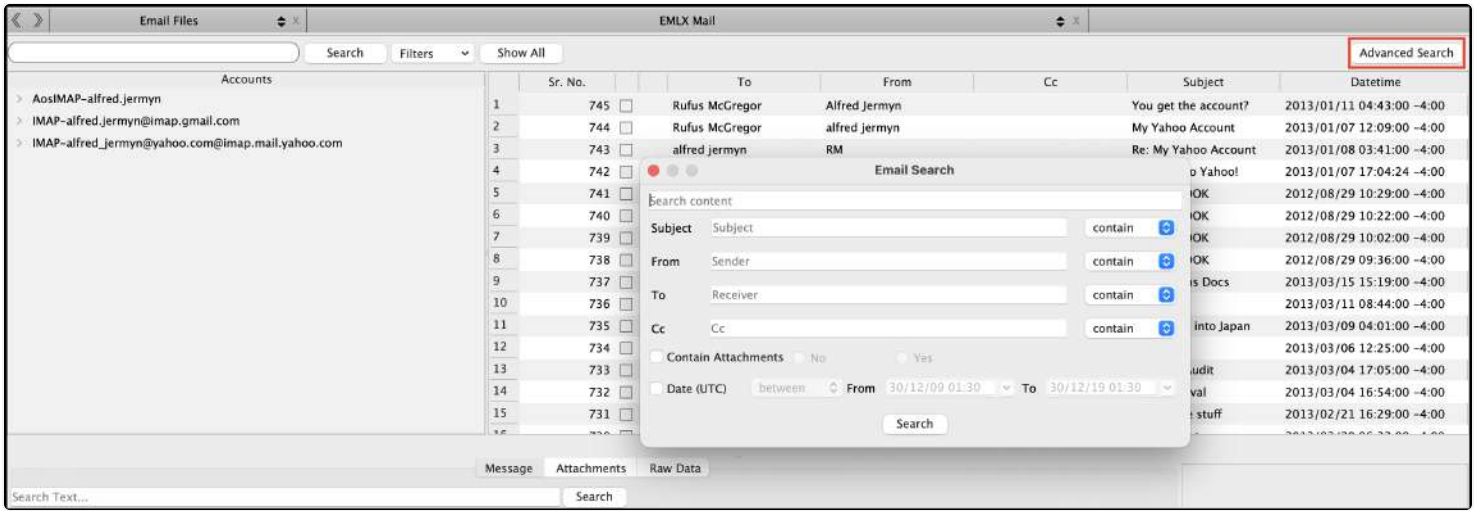
If an attachment exists they will be listed in the “Attachments” tab. Two links are provided for opening the file in the source (“Open in Source”) and to preview the file with “Quick Look”.

Viewing Message As Raw Data



The last tab interprets the message as text. This view is commonly used to see email header information.

Advanced Searching



Advanced Search can be found at the top right of the Email Files interface and helps examiners to narrow down email files, allowing them to search specific fields, and date range of extracted email data.

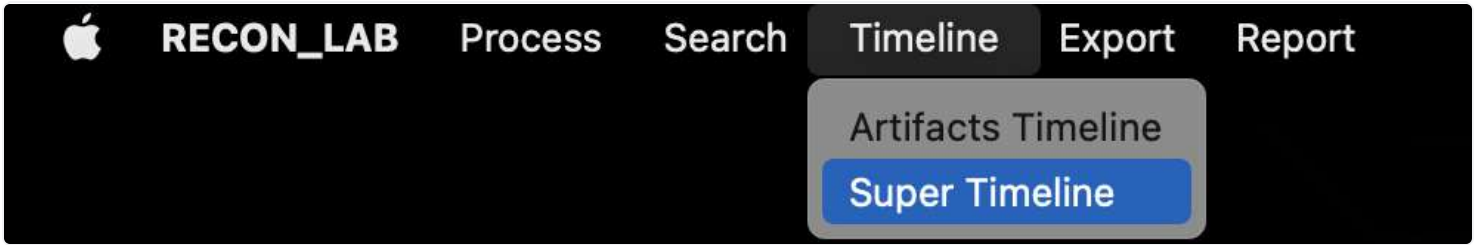
26. Timeline Analysis

The ability to sort data by timestamps is found throughout RECON LAB.

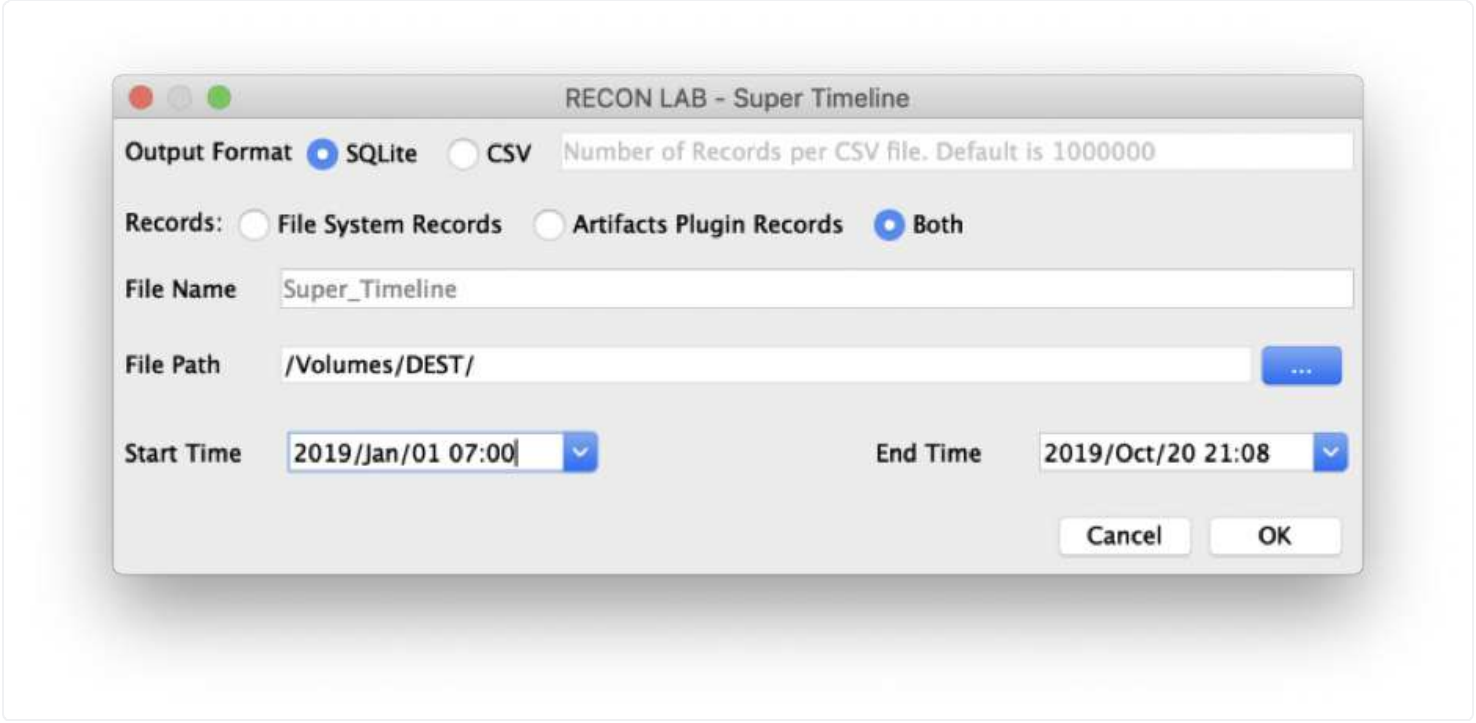
RECON LAB includes two special ways to create amazing timelines with support for hundreds of unique timestamps.

1. **Super Timeline** – creates a CSV or SQLite database of standard system timestamps and/or Artifact Plugin timestamps.
2. **Artifacts Timeline** – visual view of events based on timestamps from automated analysis.

26.1 Super Timeline



The Super Timeline can be activated by selecting Timeline > Super Timeline from the Menu Bar.



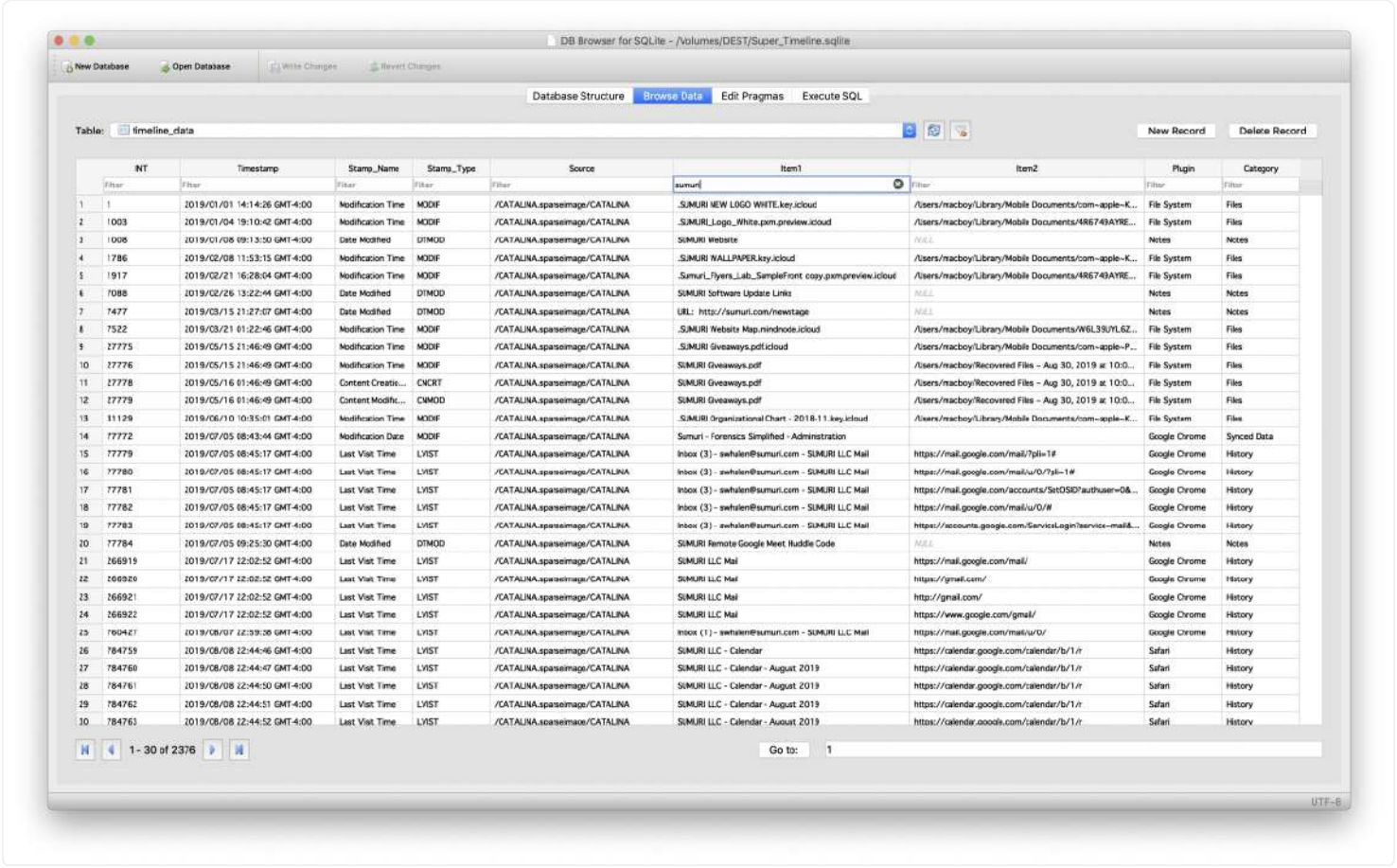
Once selected the Super Timeline configuration window will appear.

The Output Format can either be SQLite (recommended) or CSV. If you choose CSV the number of records is limited to 1,000,000.

An examiner can choose to include the standard timestamps of File System Records, timestamps of Artifacts Plugin Records or both.

A **Start Time** and an **End Time** can also be provided.

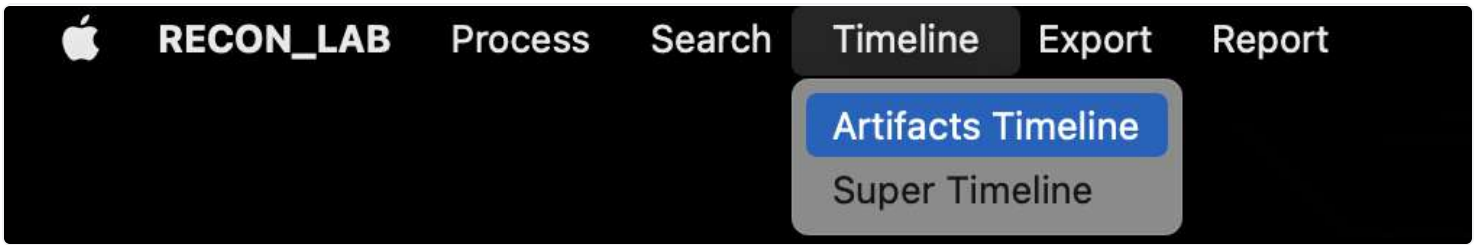
To create the Super Timeline provide a File Name, File Path and click OK.



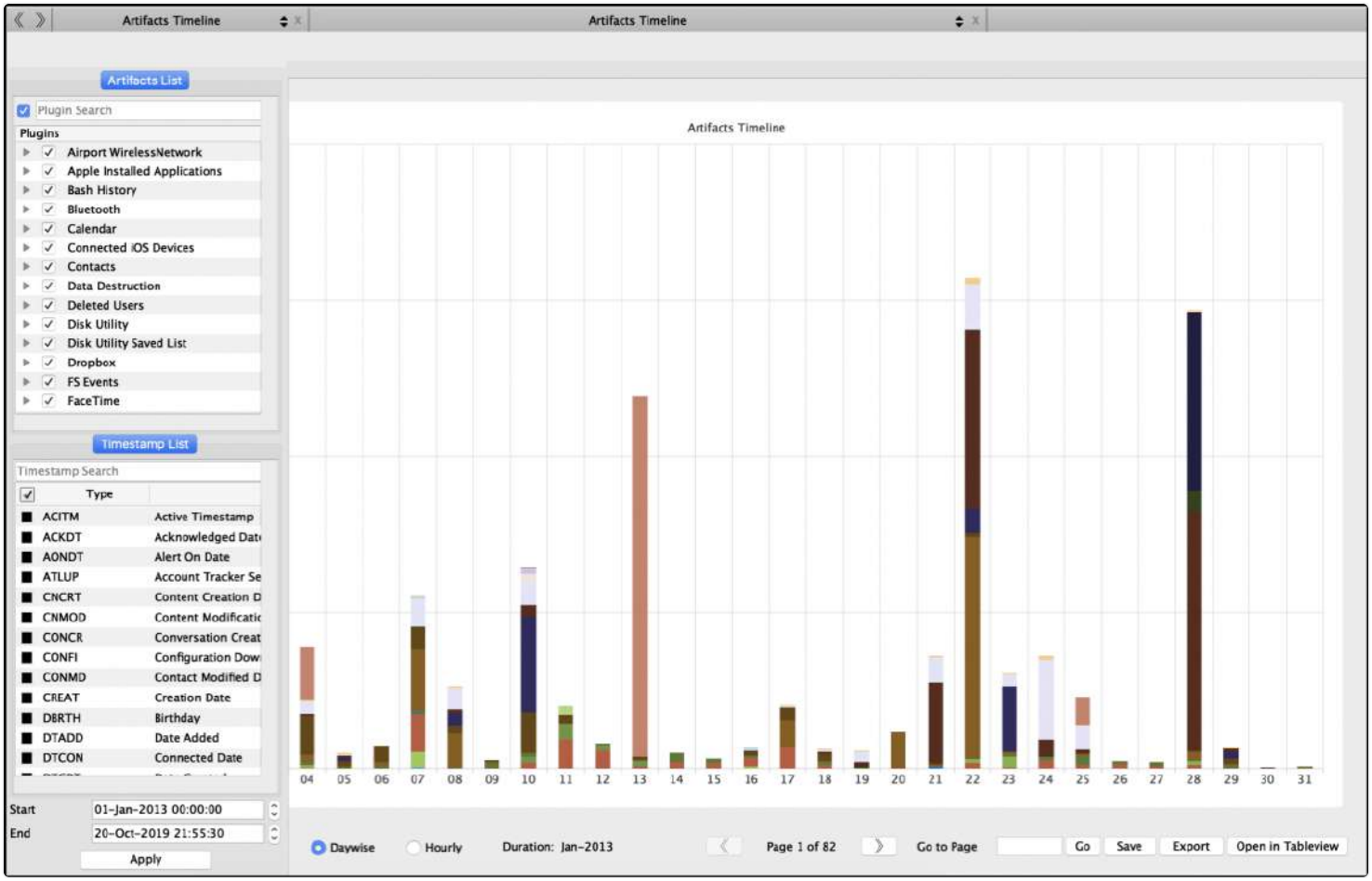
Once the Super Timeline is created you will be prompted to review the results.

26.2 Artifacts Timeline

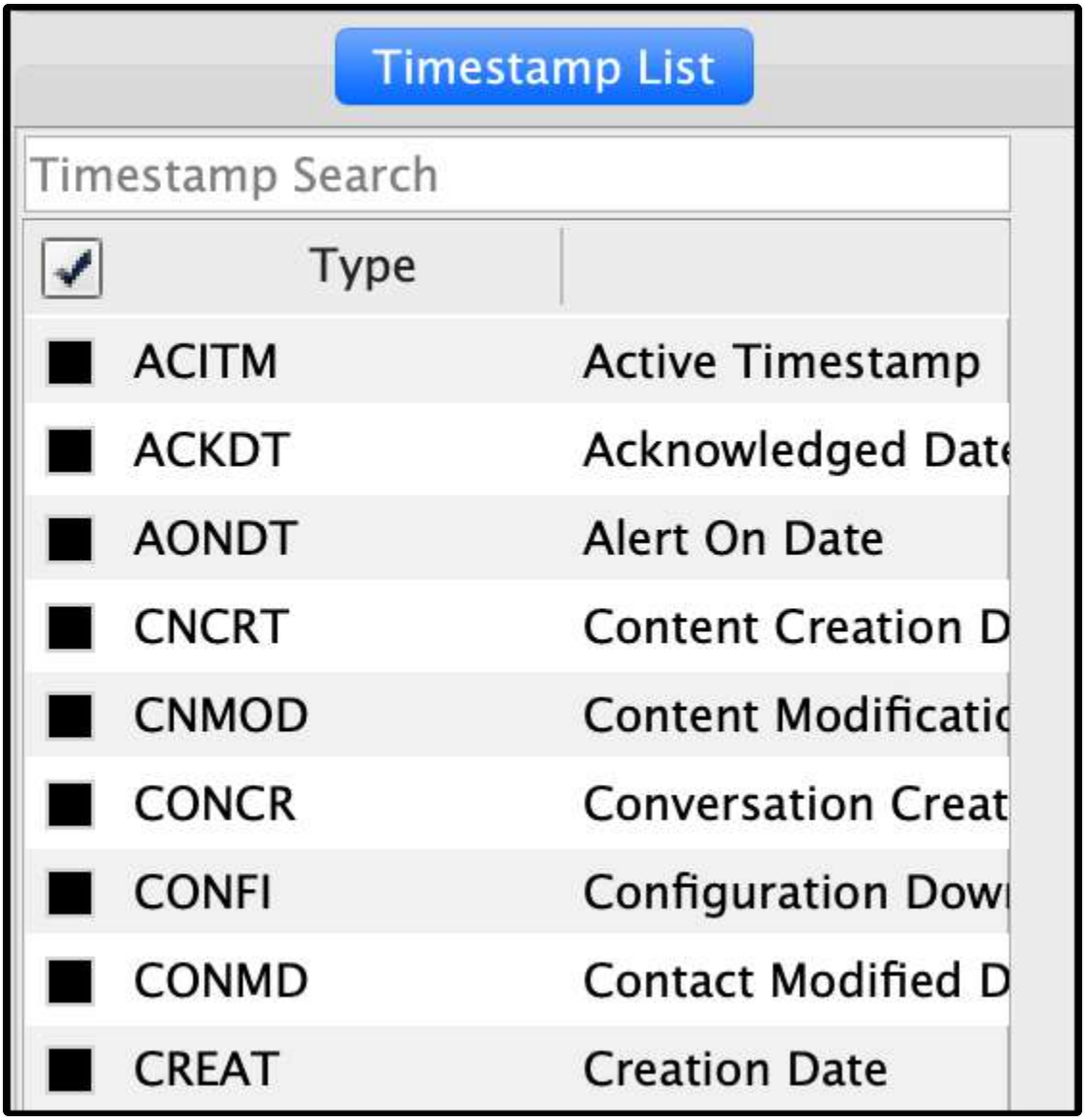
In order for the Artifacts Timeline to create a timeline make sure that you have run some or all of the Artifacts and Plugin modules for automatic analysis.



An Artifact Timeline can be created by selecting Timeline > Artifact Timeline from the Menu Bar.



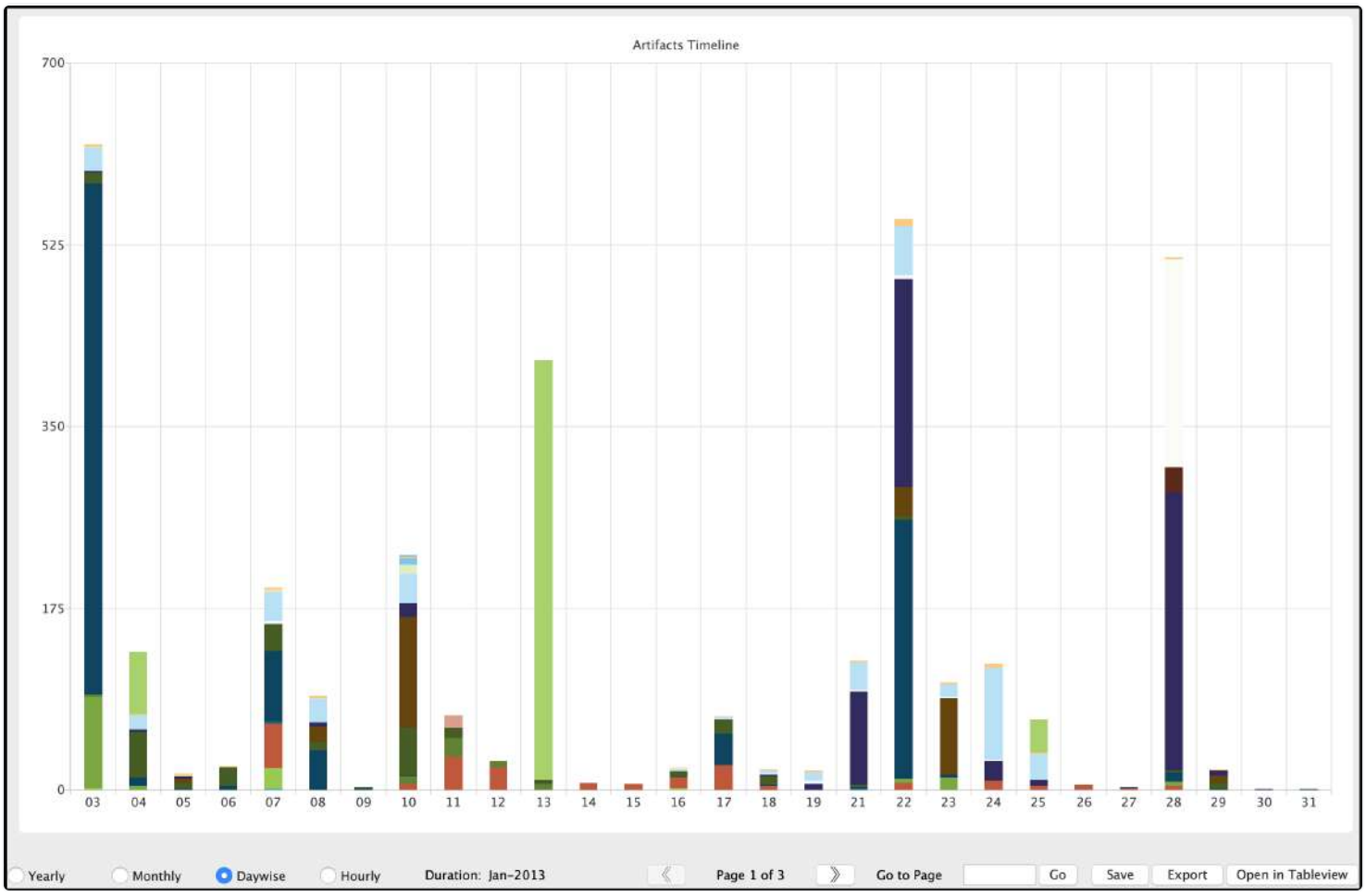
Start by selecting the artifacts of interest in the Artifacts List and timestamps of interest in the Timestamp List.



Note: FS Events artifacts can contain millions of records. Be aware that this will take time to load.

Next, select your Start and End dates and click Apply to create the Timeline.

Once complete you will have a graphical view of all the parsed and selected artifacts along a graphical timeline.



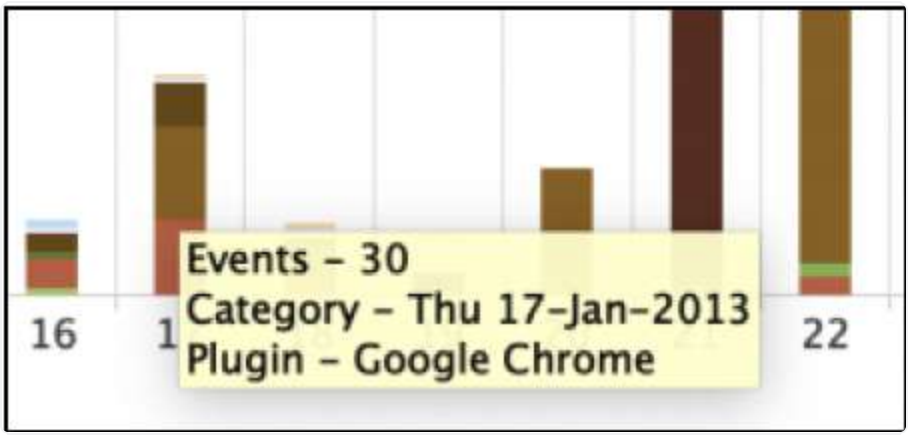
The timeline can be viewed by Year, Month, Day wise and Hourly.

To move backward and forward through the timeline pages use the navigation buttons or go directly to a page by using the “Go to Page” option.

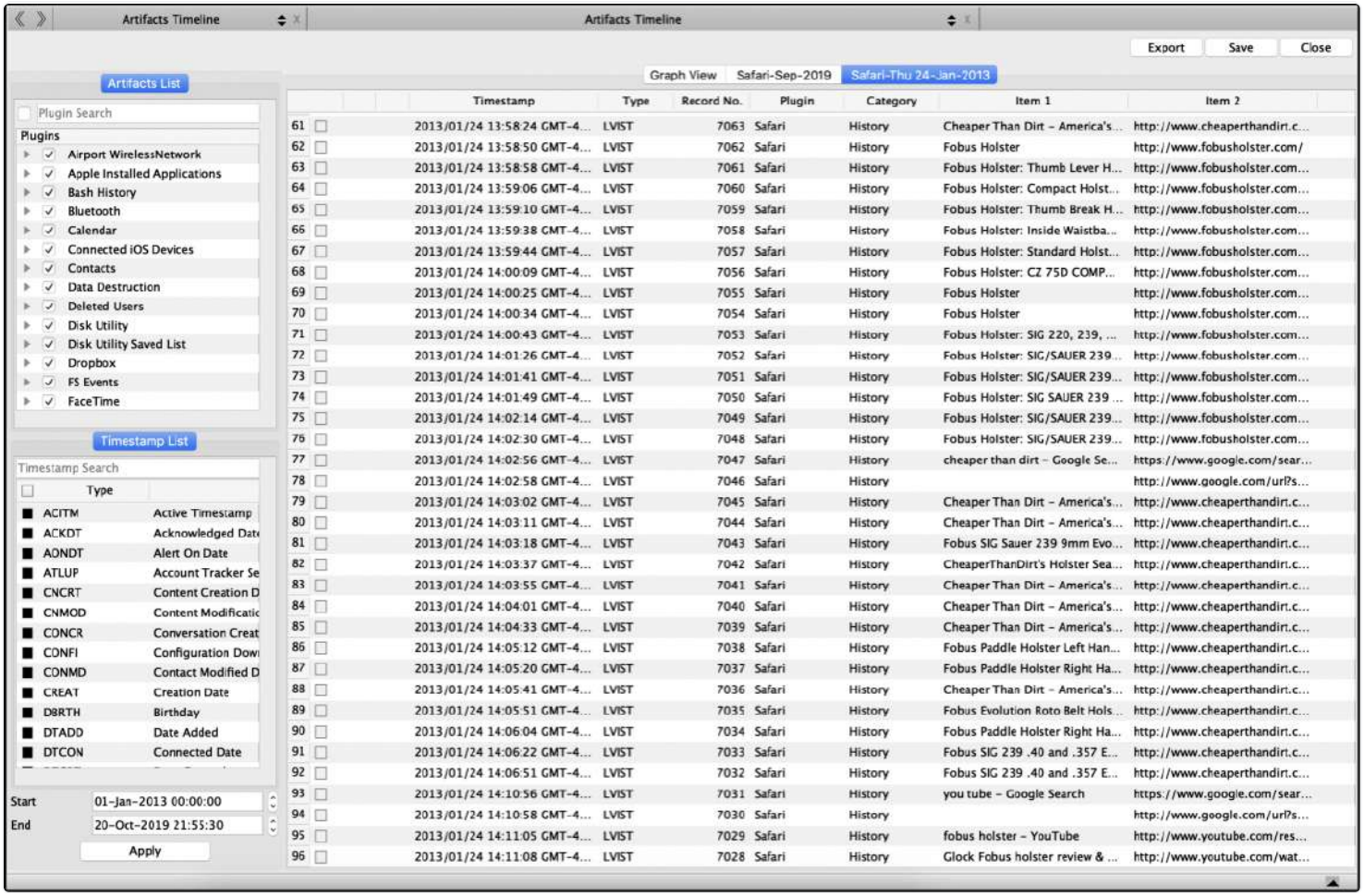
In the graphical view, you can save a picture of the current graph by clicking the “Save” button.

To export the data into a CSV file click the Export button.

To review the results in a table view click the “Tableview” button.



Each color in the graph represents a different artifact. Hovering over the color will display a popup window with additional information about the plugin.



Double-clicking on a plugin in the graph will open its results in a table view.

The results can be exported to a CSV file using the “Export” button.

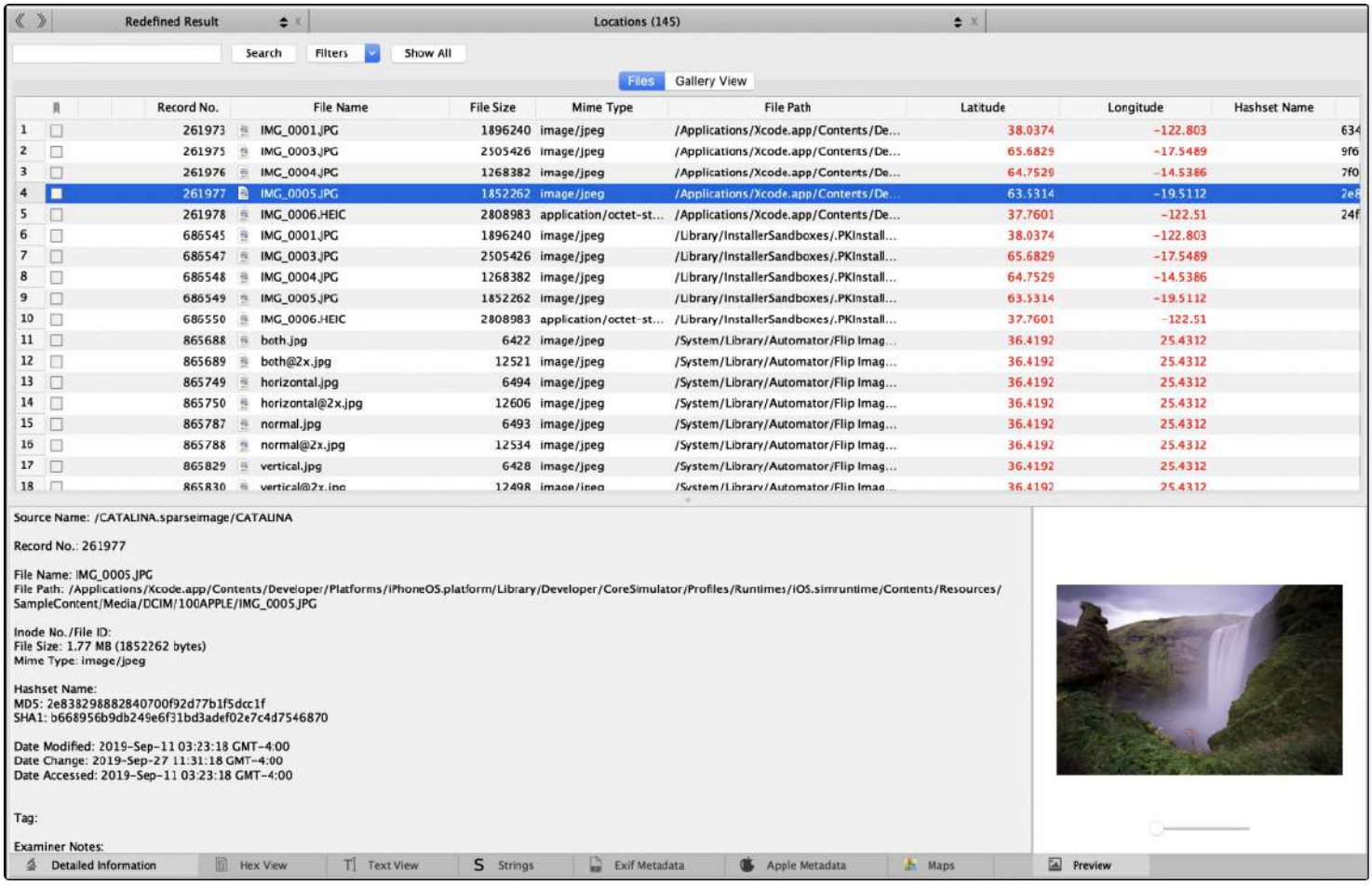
Selecting the “Save” button will save this table to the Sidebar and can be found under “Artifacts Timeline”.

Clicking the “Close” button will close the graph.

27. Redefined Results

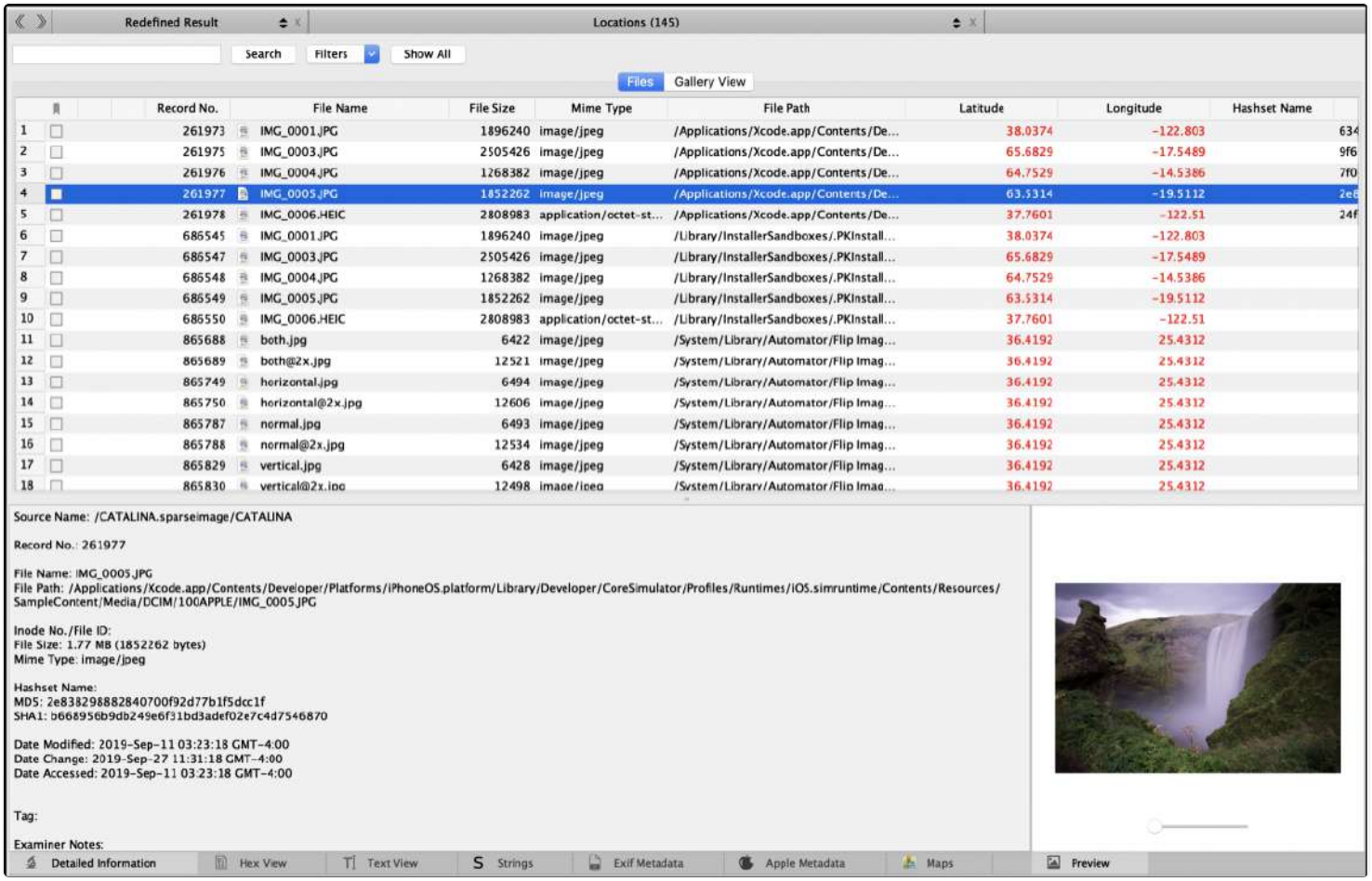
Redefined Results are a way to collate data across different devices that use different applications. It allows a complete picture of events even when a person is using a mobile device, laptop, and a computer in a single day.

Redefined Results are available for **Web History**, **Messaging** and **Location Data**.



Redefined Results can be found in the Sidebar and viewed by double-clicking on the result of your choice.

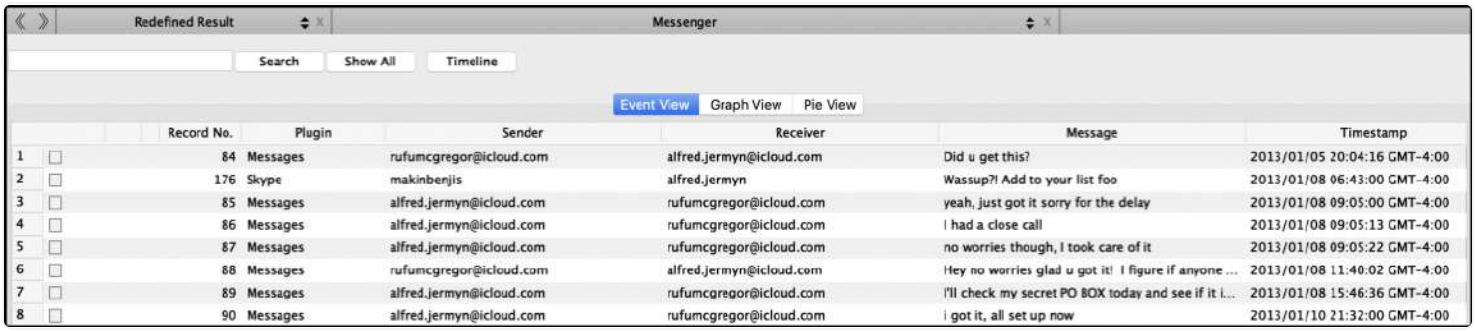
27.1 Collated Location History



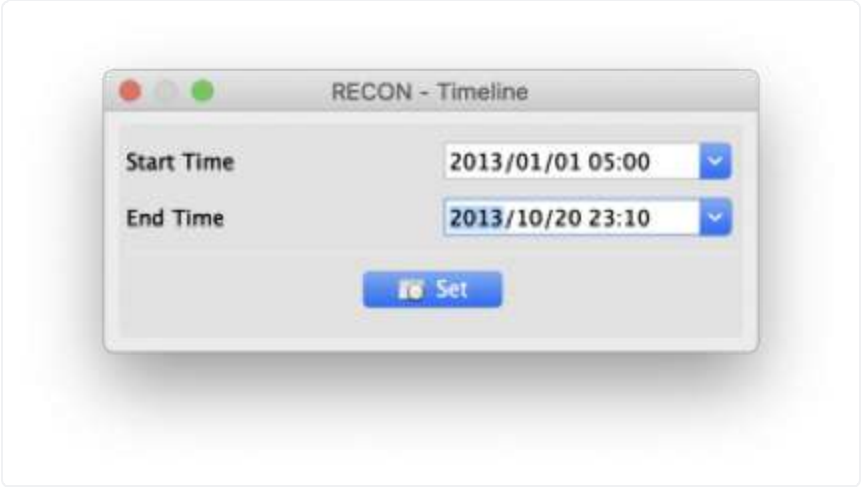
Any data containing location data will be collated in the Redefined Results for Location History.

27.2 Collated Messaging

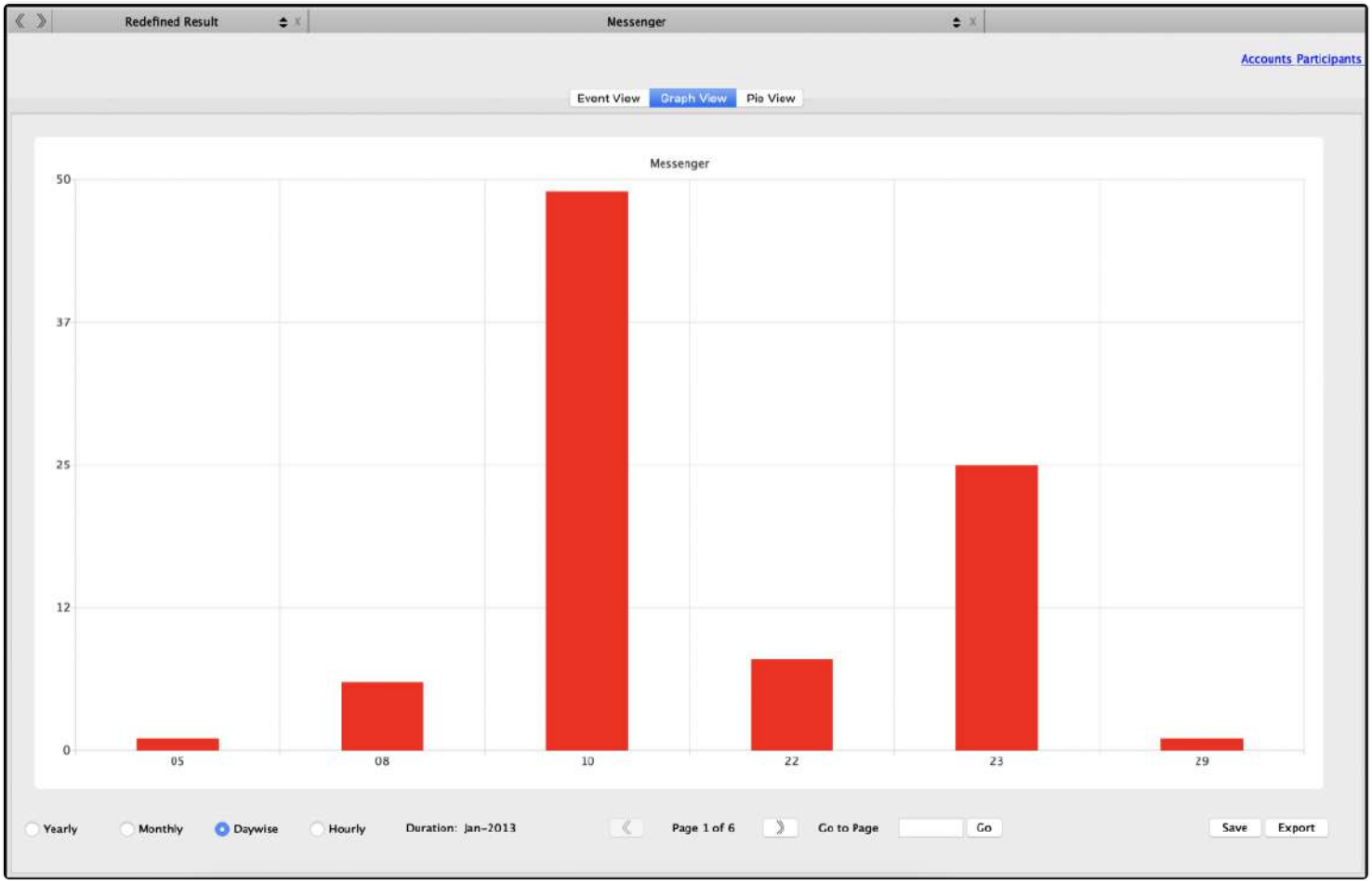
Messenger Redefined Results collate different messenger applications from different sources into one.



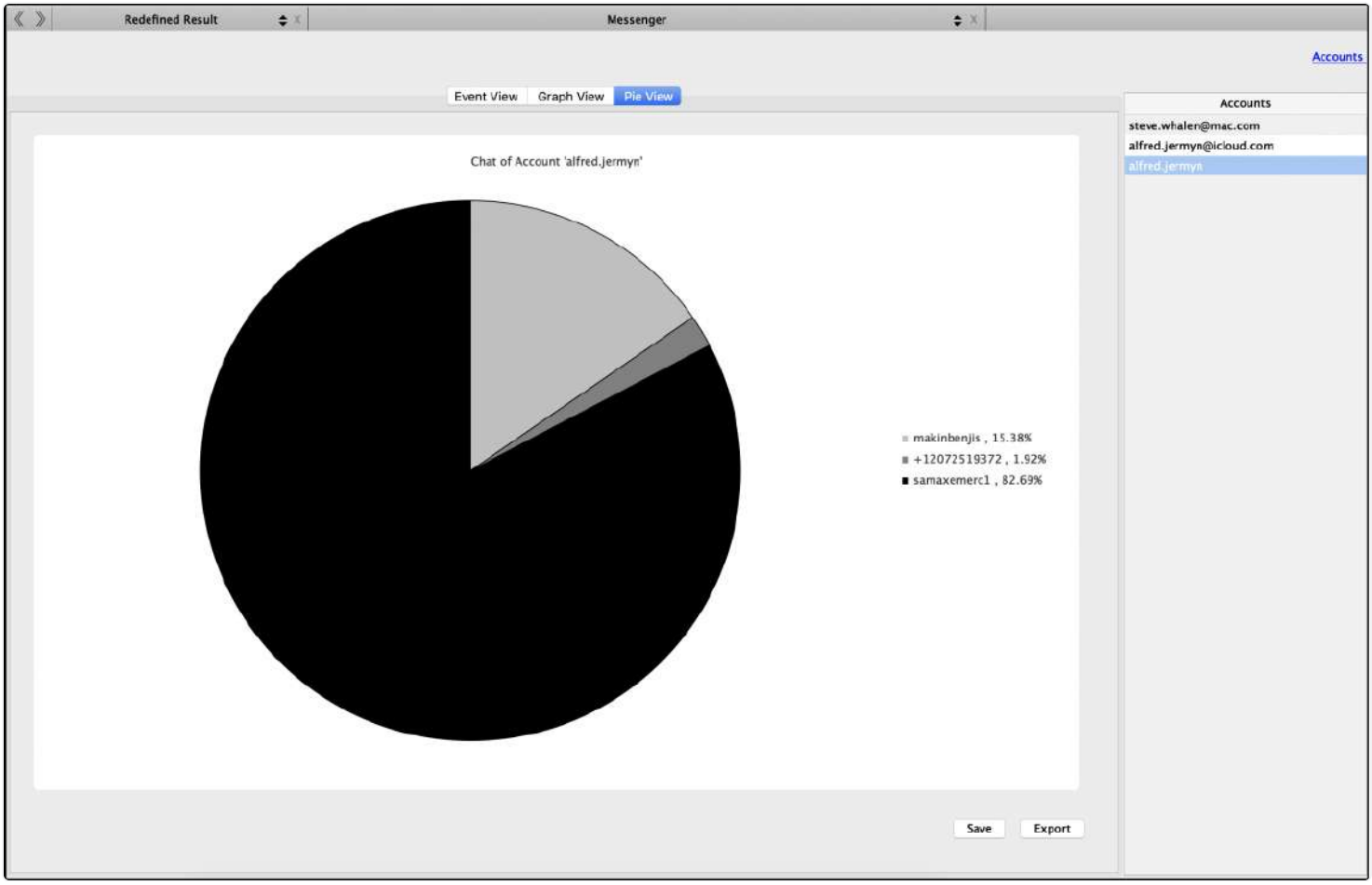
The Event View tab provides a table view of all the data. The results can be filtered using the Search box.



A **Start Time** and **End Time** can be applied to the results by clicking the Timeline button.

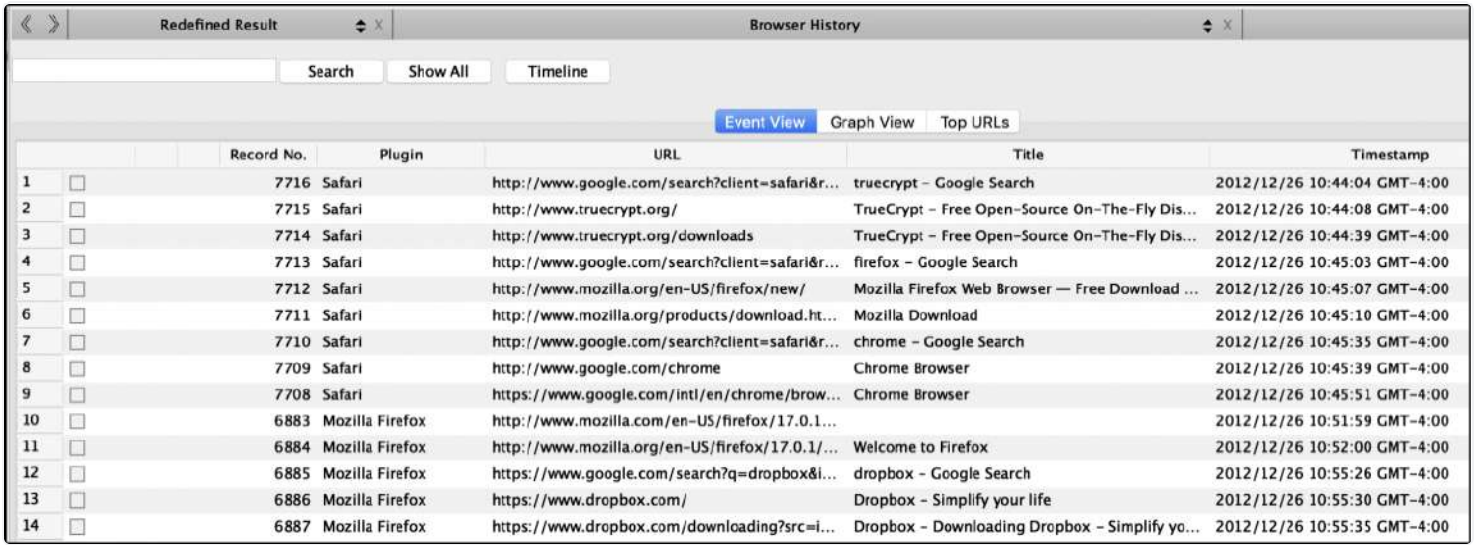


The **Graph View** provides a visual view of the messaging data in a timeline.



The Pie View tab provides another visual analysis of the data based on percentages.

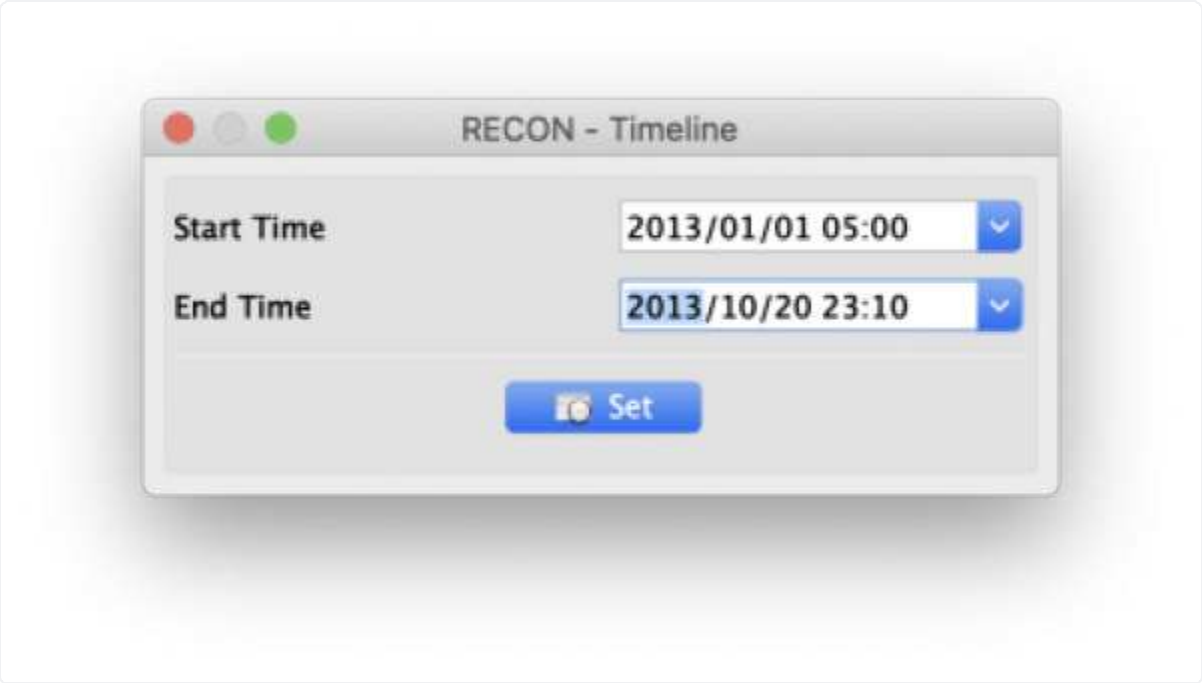
27.3 Collated Web History



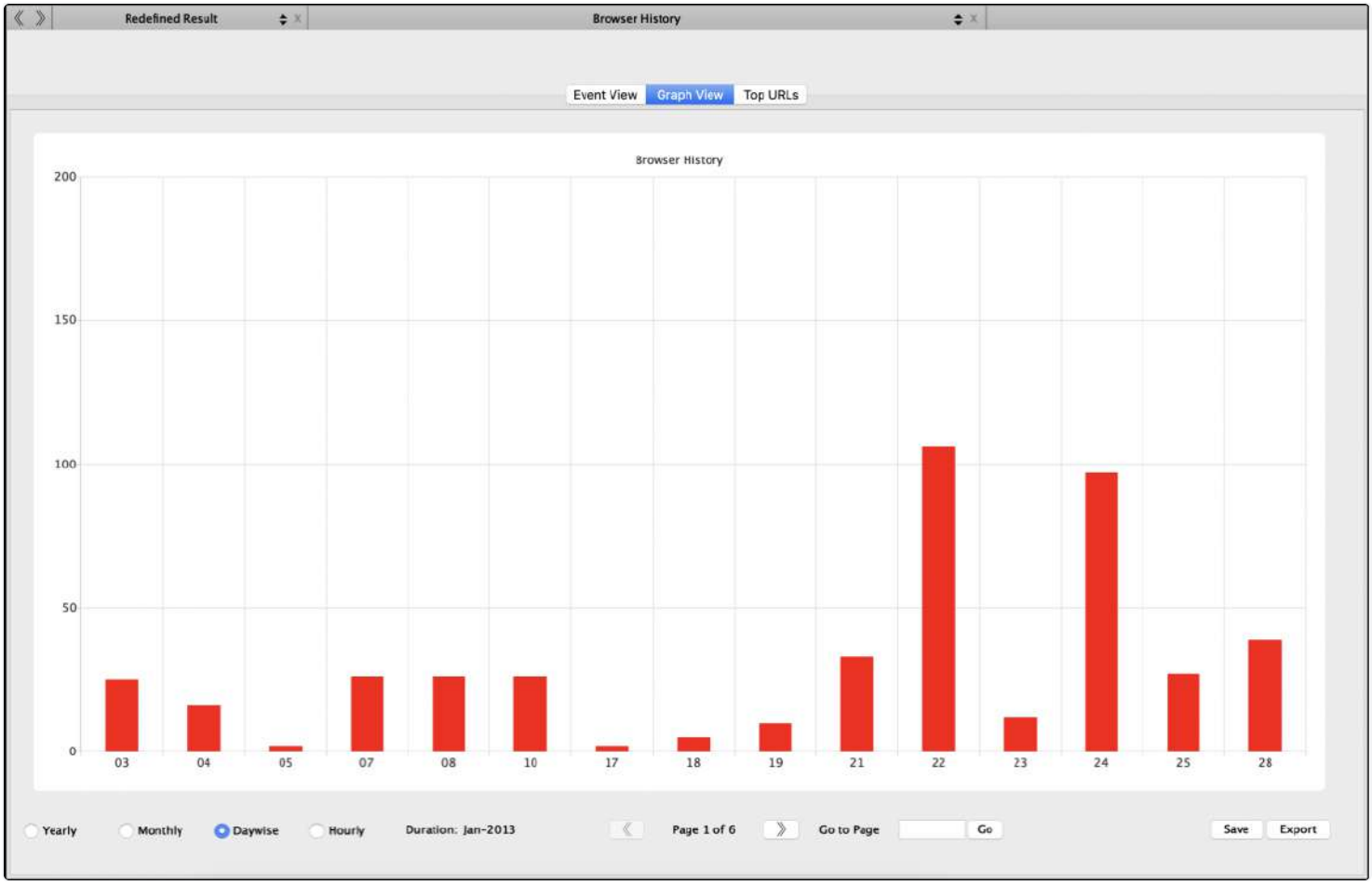
		Record No.	Plugin	URL	Title	Timestamp
1	☐	7716	Safari	http://www.google.com/search?client=safari&r...	truecrypt - Google Search	2012/12/26 10:44:04 GMT-4:00
2	☐	7715	Safari	http://www.truecrypt.org/	TrueCrypt - Free Open-Source On-The-Fly Dis...	2012/12/26 10:44:08 GMT-4:00
3	☐	7714	Safari	http://www.truecrypt.org/downloads	TrueCrypt - Free Open-Source On-The-Fly Dis...	2012/12/26 10:44:39 GMT-4:00
4	☐	7713	Safari	http://www.google.com/search?client=safari&r...	firefox - Google Search	2012/12/26 10:45:03 GMT-4:00
5	☐	7712	Safari	http://www.mozilla.org/en-US/firefox/new/	Mozilla Firefox Web Browser — Free Download ...	2012/12/26 10:45:07 GMT-4:00
6	☐	7711	Safari	http://www.mozilla.org/products/download.ht...	Mozilla Download	2012/12/26 10:45:10 GMT-4:00
7	☐	7710	Safari	http://www.google.com/search?client=safari&r...	chrome - Google Search	2012/12/26 10:45:35 GMT-4:00
8	☐	7709	Safari	http://www.google.com/chrome	Chrome Browser	2012/12/26 10:45:39 GMT-4:00
9	☐	7708	Safari	https://www.google.com/intl/en/chrome/brow...	Chrome Browser	2012/12/26 10:45:51 GMT-4:00
10	☐	6883	Mozilla Firefox	http://www.mozilla.com/en-US/firefox/17.0.1...		2012/12/26 10:51:59 GMT-4:00
11	☐	6884	Mozilla Firefox	http://www.mozilla.org/en-US/firefox/17.0.1/...	Welcome to Firefox	2012/12/26 10:52:00 GMT-4:00
12	☐	6885	Mozilla Firefox	https://www.google.com/search?q=dropbox&i...	dropbox - Google Search	2012/12/26 10:55:26 GMT-4:00
13	☐	6886	Mozilla Firefox	https://www.dropbox.com/	Dropbox - Simplify your life	2012/12/26 10:55:30 GMT-4:00
14	☐	6887	Mozilla Firefox	https://www.dropbox.com/downloading?src=i...	Dropbox - Downloading Dropbox - Simplify yo...	2012/12/26 10:55:35 GMT-4:00

Browser History Redefined Results collate different web browsing applications from different sources into one.

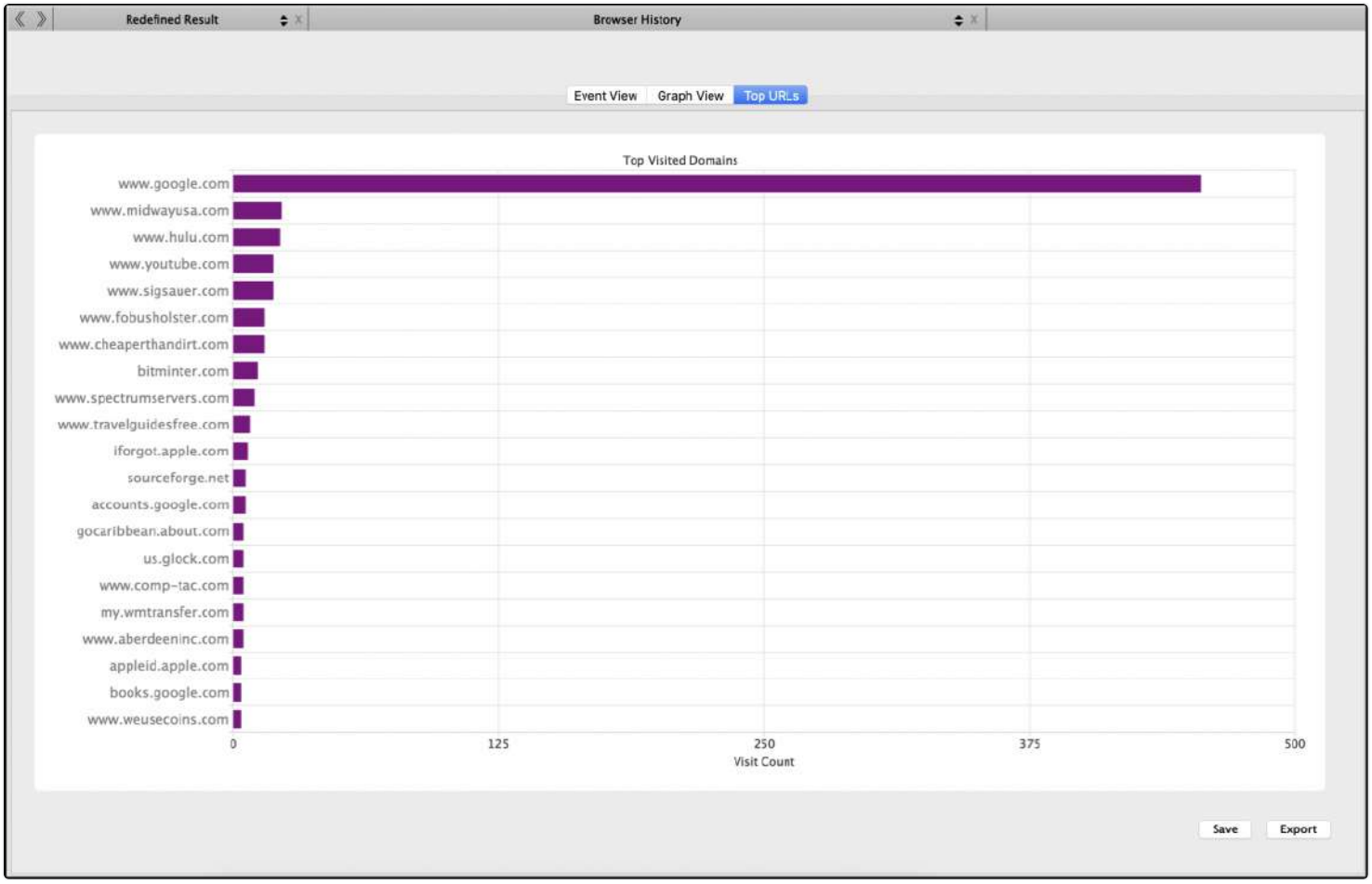
The **Event View** tab provides a table view of all the data. The results can be filtered using the Search box.



A **Start Time** and **End Time** can be applied to the results by clicking the Timeline button.



The **Graph View** provides a visual view of web browser data in a timeline.



The **Top URLs** tab is a graphical view that shows the most visited websites based on frequency.

28. RAM Analysis

The RAM Analysis module in RECON LAB contains a Graphical User Interface (GUI) for the Volatility Framework. The output from Volatility can be bookmarked and used for documentation within RECON LAB. Currently, RECON LAB supports Volatility (Version 2).

RECON LAB's RAM Analysis module also includes the ability to carve user and Keychain passwords from RAM images.

The RAM Analysis module supports processing both Windows and macOS RAM images. Supported operating system profiles can be found here:

https://github.com/volatilityfoundation/volatility/blob/master/README.txt

28.1 Setting Up Volatility Framework

Before continuing, please ensure that you have configured the bvolatility framework by following the steps in Section 9.9 Volatility Path.

28.2 Selecting a RAM Image to Process

Make sure that RAM images have been added to RECON LAB in raw format as a Source. A raw RAM image can be created using RECON *ITR*.

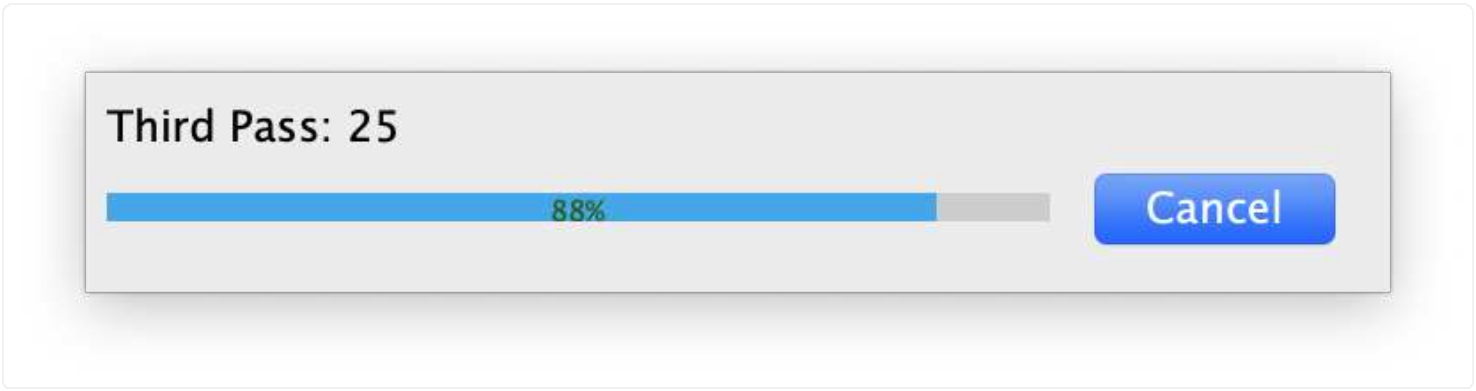
Start the **RAM Analysis** module by selecting Process > Super Timeline from the Menu Bar.

If a RAM image has been added as a source then it can be selected in the **Source** dropdown list.

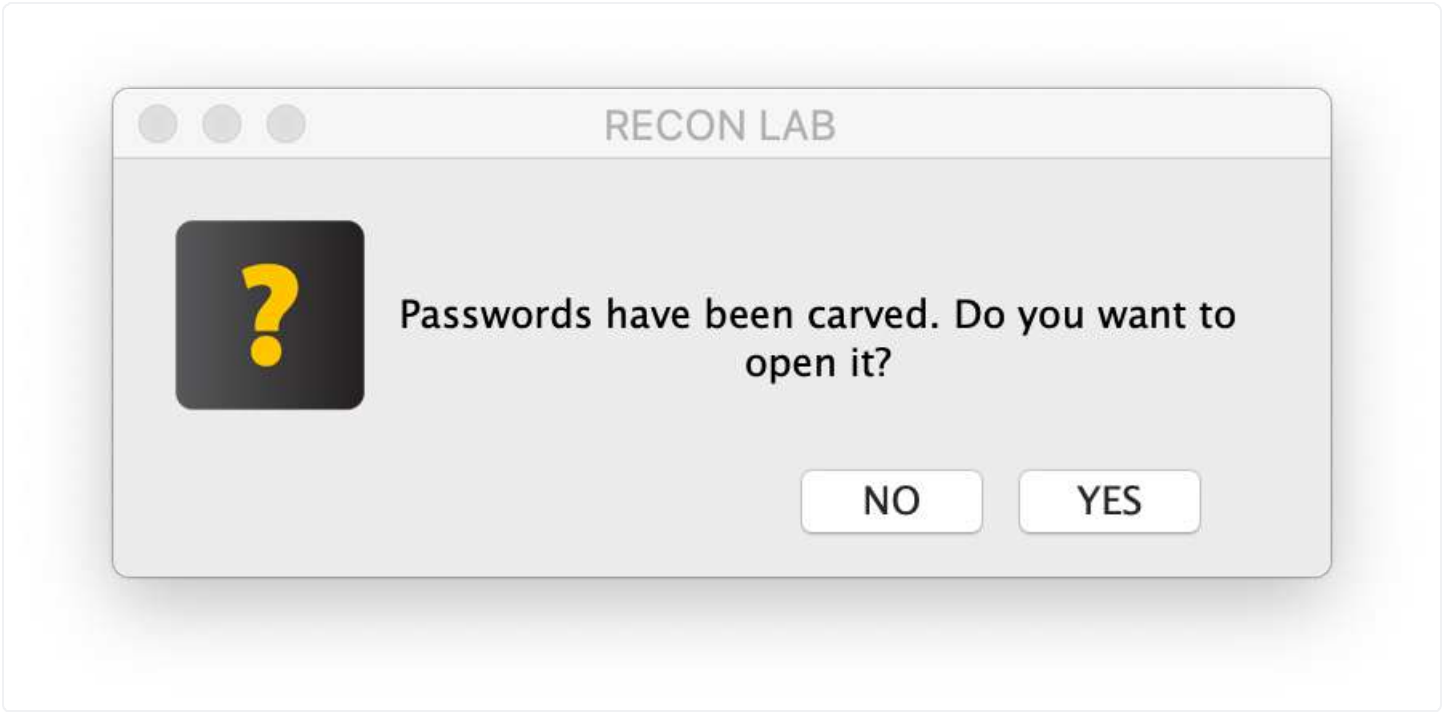
28.3 Carving Passwords from RAM

Note: Carving passwords from volatile memory is not guaranteed to work. Many factors can influence successfully carving passwords.

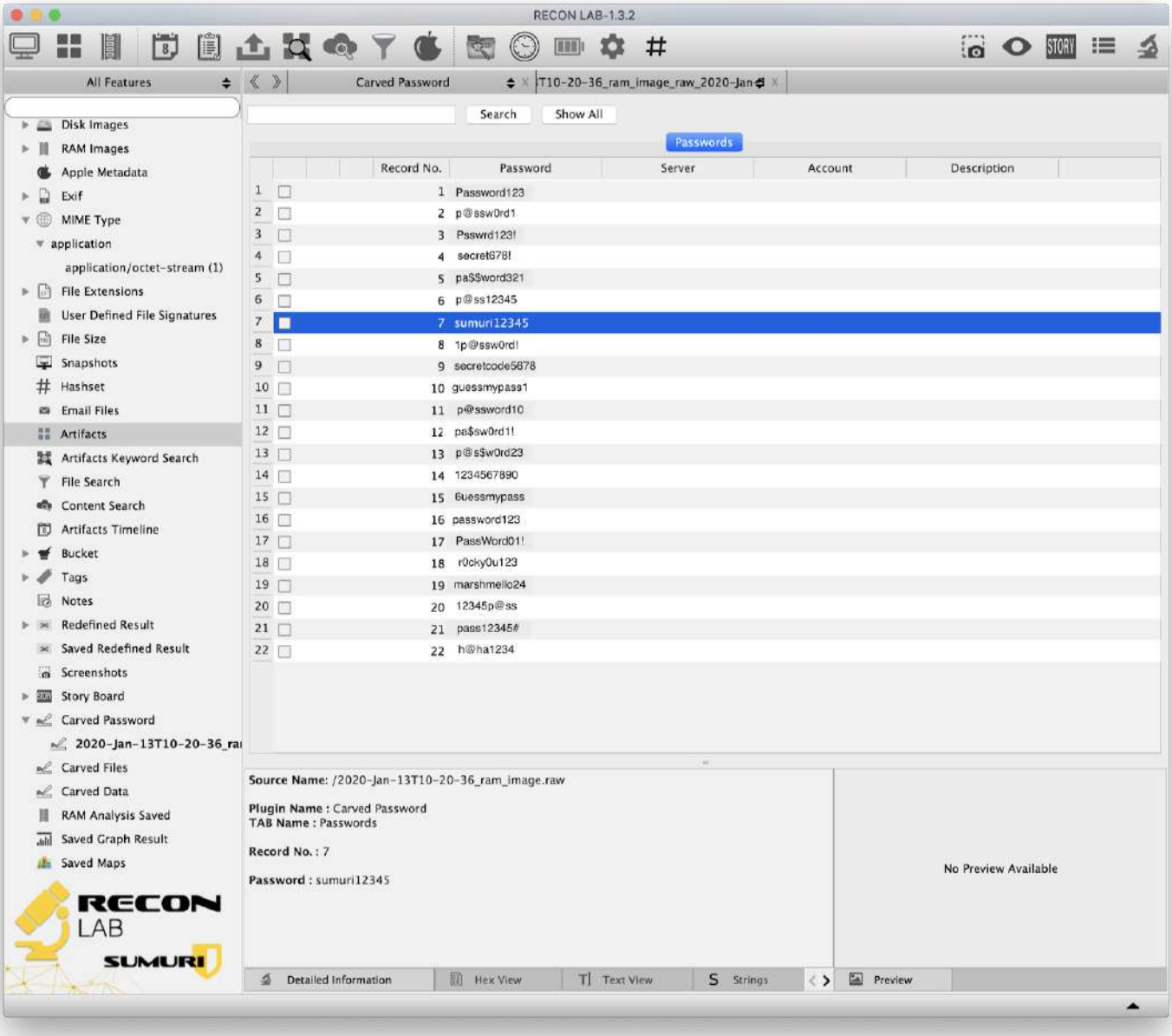
To run the Carve Password module select a RAM image from the Source dropdown list and click **Carve Password.**



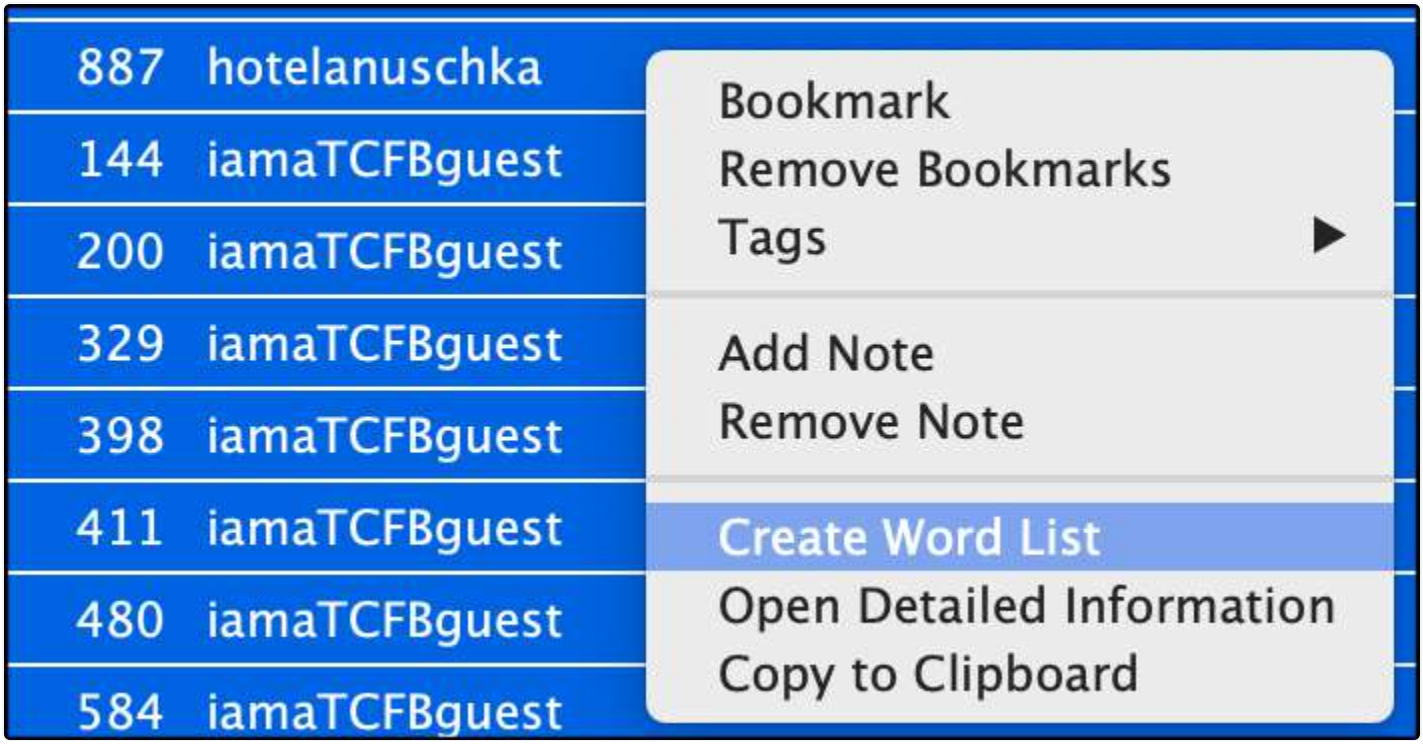
RECON LAB will utilize three algorithms in an attempt to collect as many passwords as possible. A counter will increase for each password found.



When the Carving Passwords module has completed a prompt will appear asking if you would like to open the list of passwords.



The Main Viewer window will display any passwords carved which can be bookmarked and added to reports.



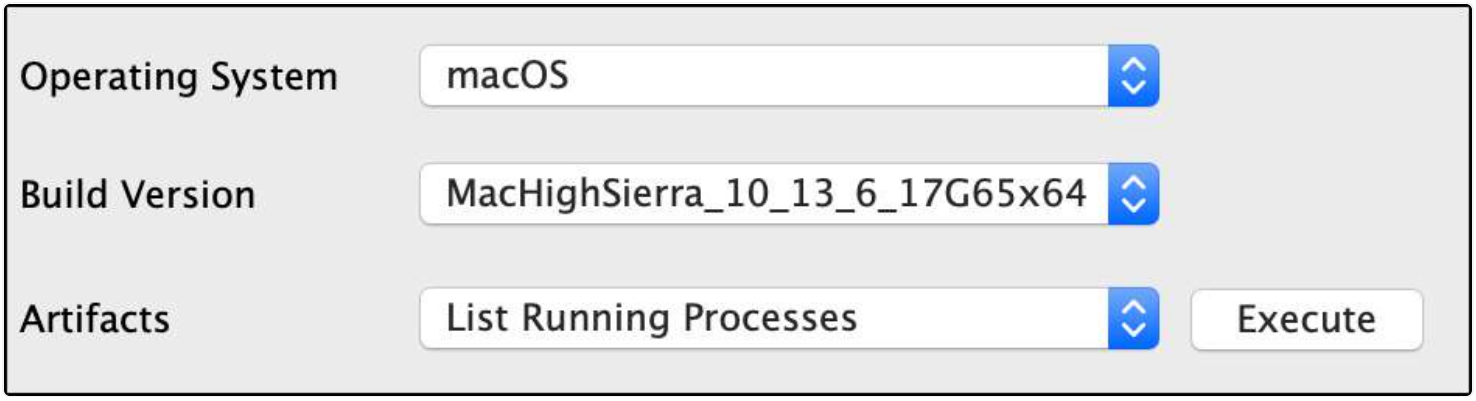
Additionally, a dictionary can be created from the recovered passwords by right-clicking on any highlighted password and selecting **Create Word List**.

28.4 Using Volatility Framework in RECON LAB

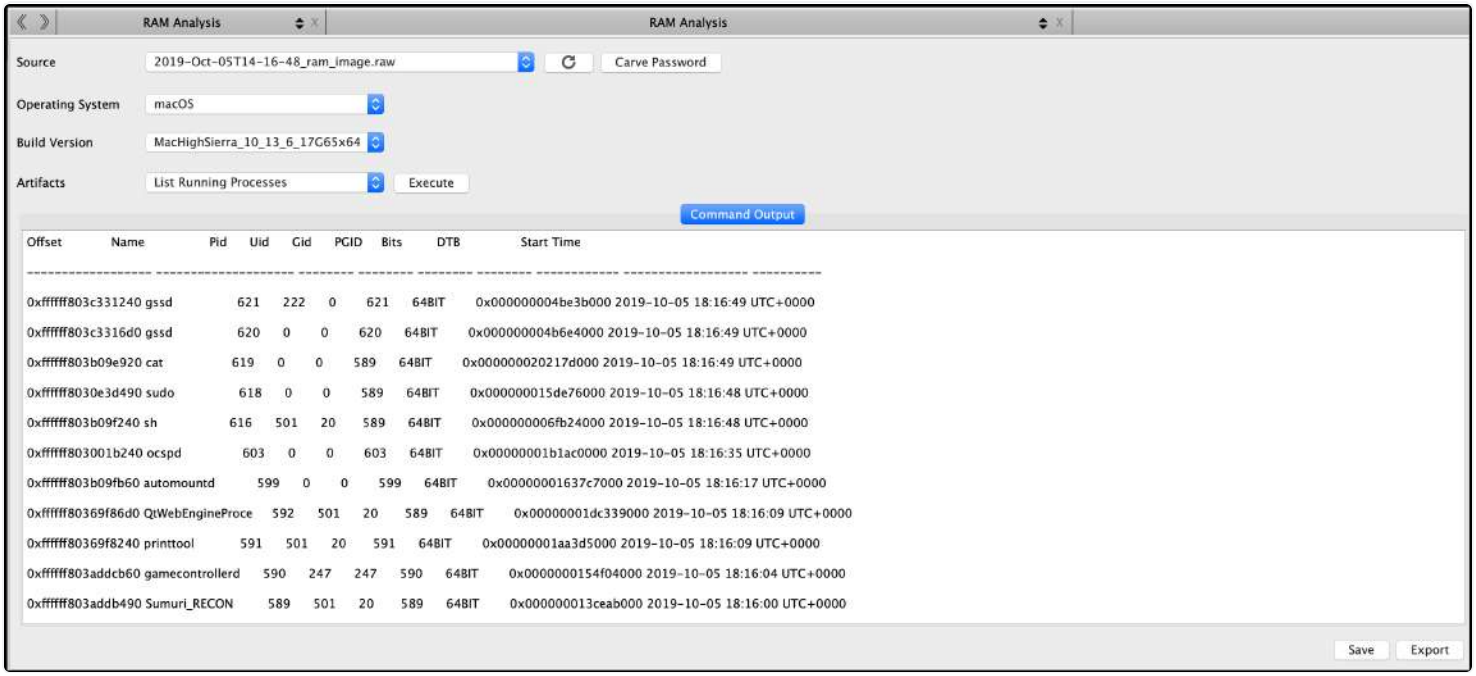
Make sure that the steps have been followed in **Section 29.1** to properly download and install Volatility Framework. Also, be sure to properly install any profiles that are to be used for analysis.

Start the **RAM Analysis** module by selecting Process > Super Timeline from the Menu Bar.

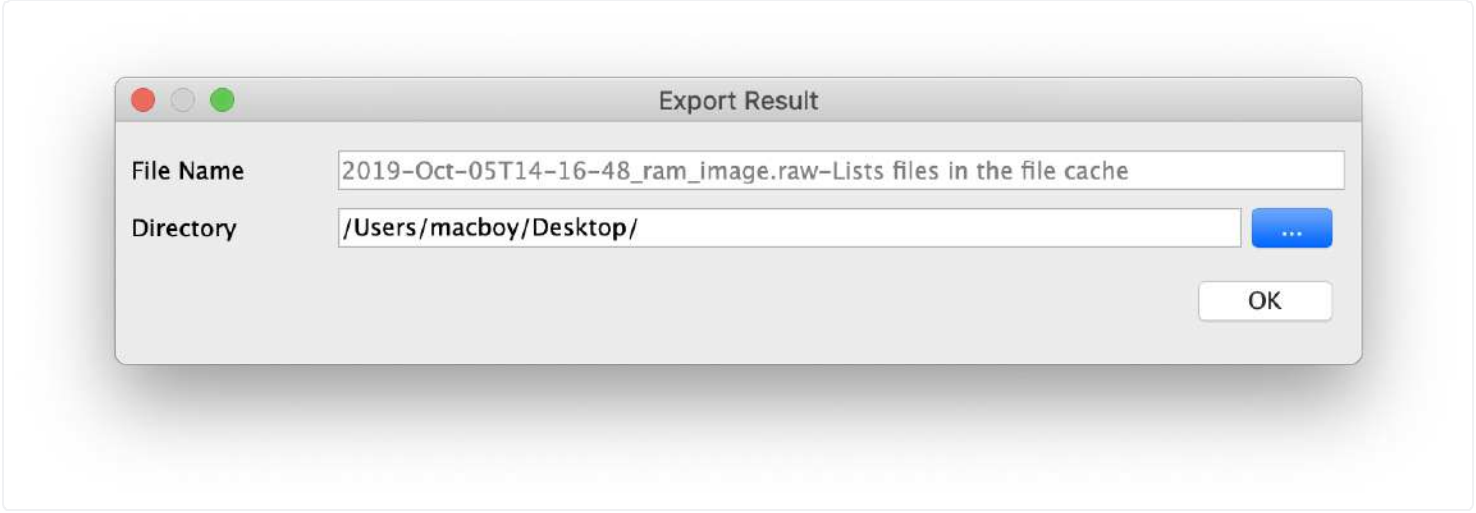
Next, select the RAM image to be analyzed from the **Source** dropdown list.



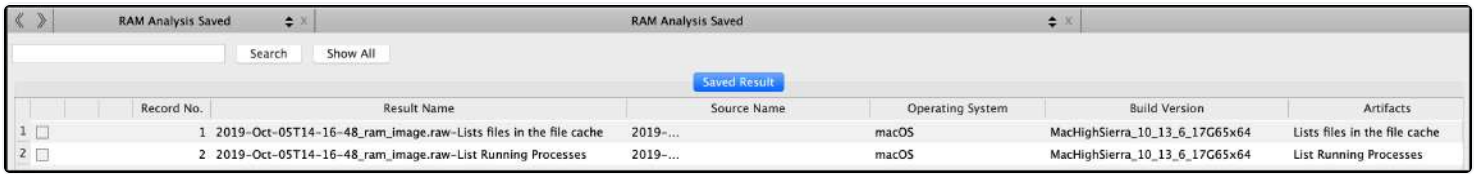
Finally, select the correct **Operating System**, **Build Version and Artifacts** to be analyzed from the remaining dropdown lists and press **Execute**.



If successful, the output will be displayed in the **Command Output** window



The output can be exported as a text file by clicking the **Export** button.



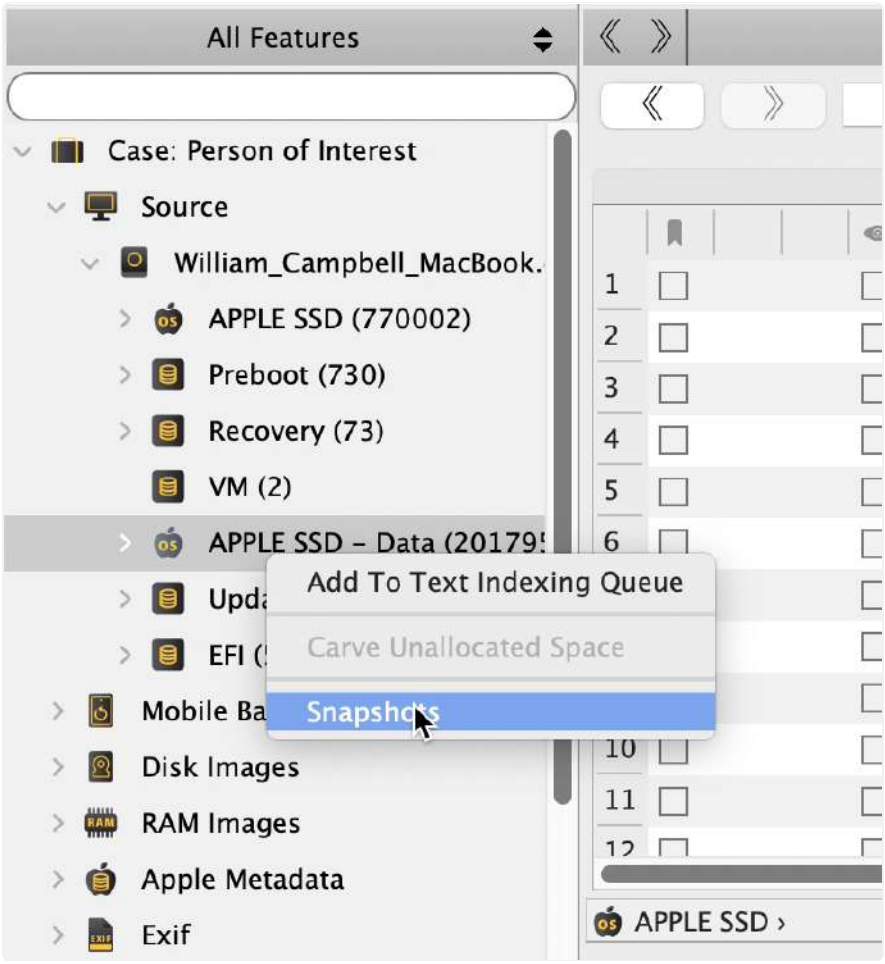
Additionally, the output can be saved to the Sidebar under **RAM Analysis Saved** by clicking the **Save** button.

From the RAM Analysis Saved window the output of the RAM Analysis can be bookmarked for reporting.

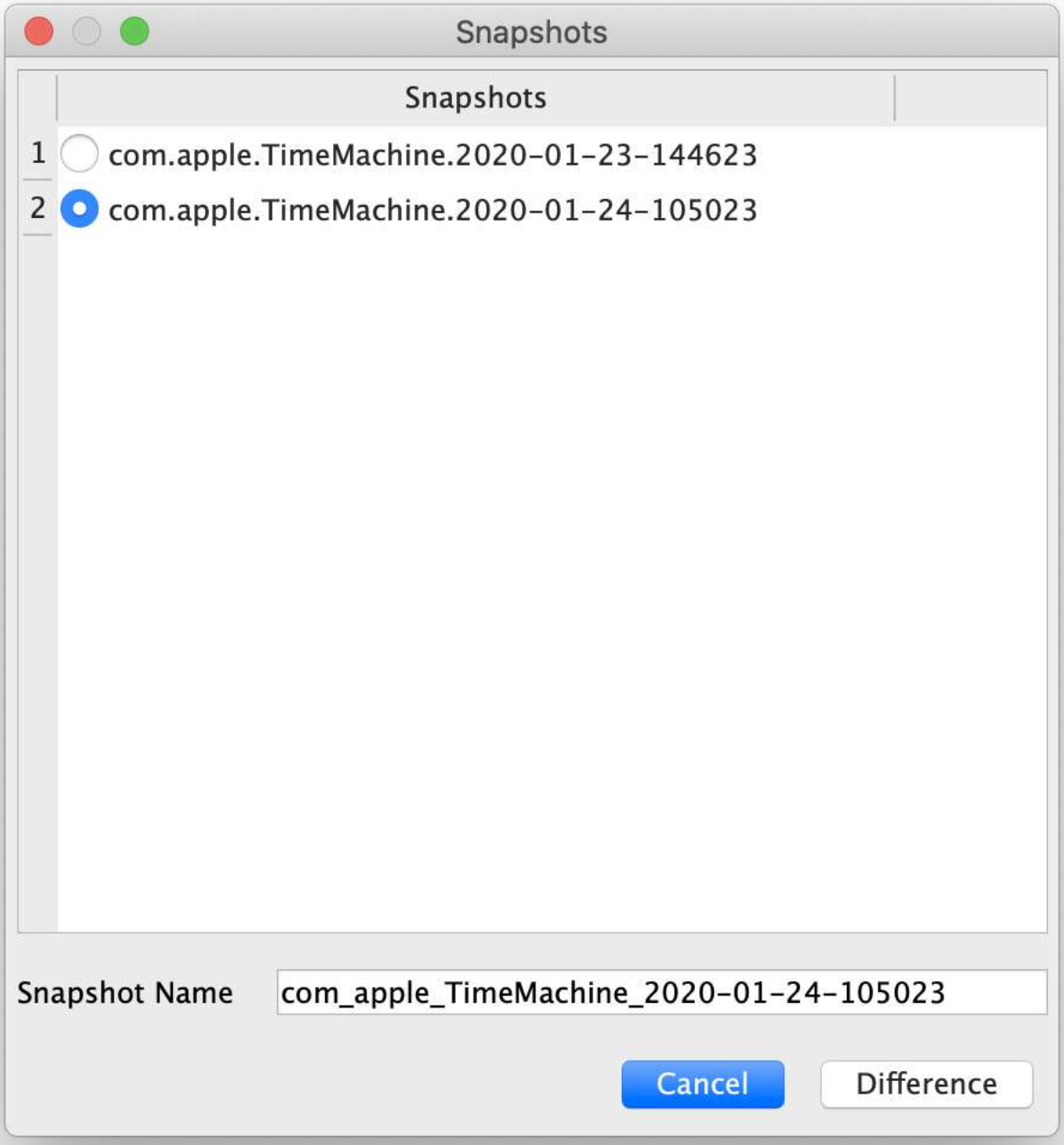
29. Local Time Machine Snapshots (APFS Snapshots)

RECON LAB can identify and perform differential analysis of Local Time Machine Snapshots contain within a forensic image of an APFS if they exist. Local Time Machine Snapshots are sometimes referred to as APFS Snapshots. Refer to **Section 1.1.5** of this manual for additional information.

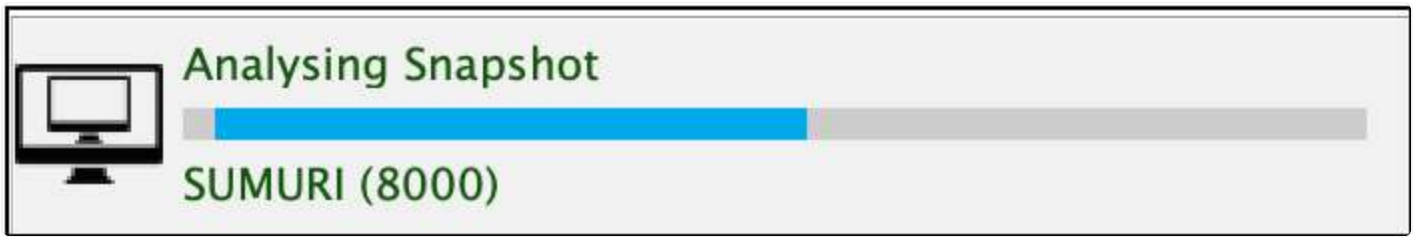
29.1 Processing Local Time Machine Snapshots



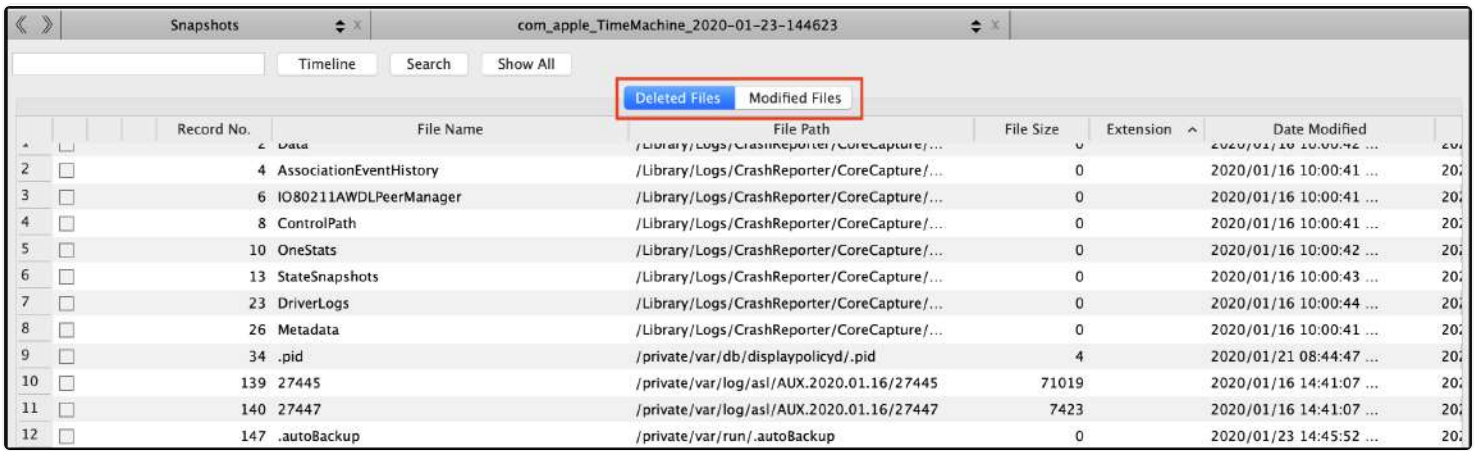
Local Time Machine Snapshots only exist in APFS. To identify if Local Time Machine Snapshots exist in the case right-click on the AFPS volume containing the user data and select **Snapshots**.



If any Local Time Machine Snapshots exist a window will appear listing all of the snapshots.



Select the snapshot to be processed and added to the case.



	Record No.	File Name	File Path	File Size	Extension	Date Modified
2	4	AssociationEventHistory	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:41 ...
3	6	IO80211AWDLPeerManager	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:41 ...
4	8	ControlPath	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:41 ...
5	10	OneStats	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:42 ...
6	13	StateSnapshots	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:43 ...
7	23	DriverLogs	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:44 ...
8	26	Metadata	/Library/Logs/CrashReporter/CoreCapture/...	0		2020/01/16 10:00:41 ...
9	34	.pid	/private/var/db/displaypolicyd/.pid	4		2020/01/21 08:44:47 ...
10	139	27445	/private/var/log/asl/AUX.2020.01.16/27445	71019		2020/01/16 14:41:07 ...
11	140	27447	/private/var/log/asl/AUX.2020.01.16/27447	7423		2020/01/16 14:41:07 ...
12	147	.autoBackup	/private/var/run/.autoBackup	0		2020/01/23 14:45:52 ...

RECON LAB performs a differential analysis of the Local Time Machine Snapshot by comparing with the current state of the image and identifying modified and deleted files.

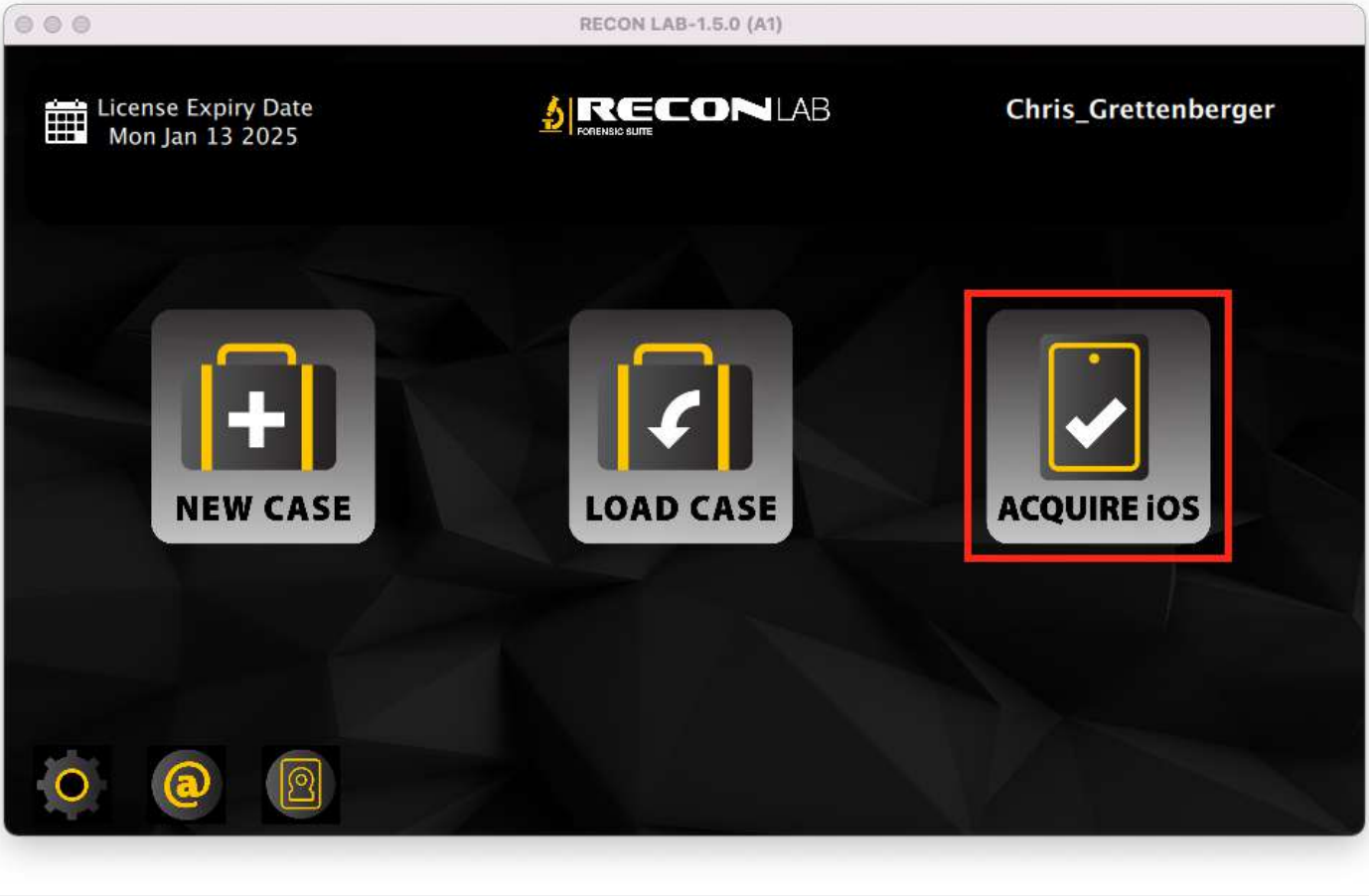
Analysis of Local Time Machine Snapshots can be repeated for any additional snapshots that exist.

Processed Local Time Machine Snapshots can be found in **Sidebar** under **Snapshots**.

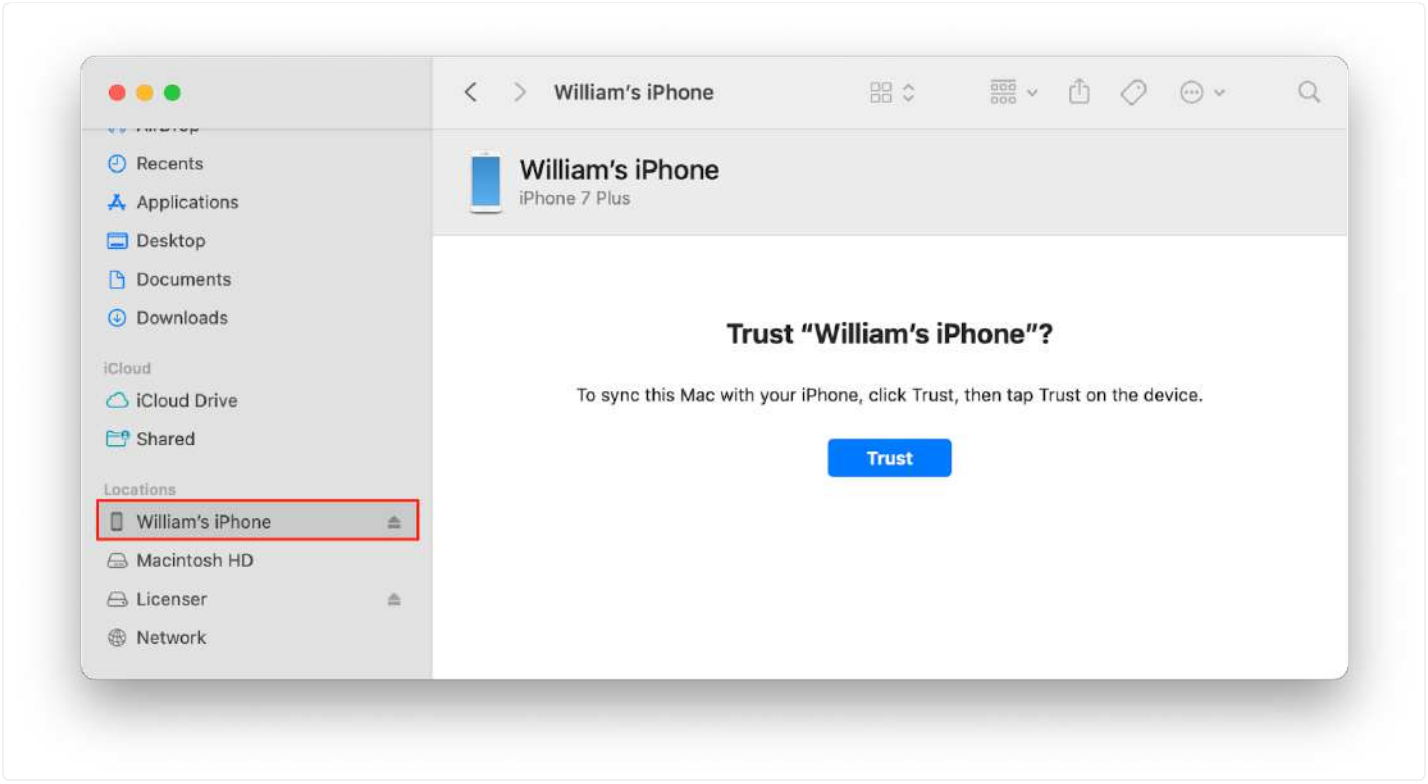
30. Acquiring and Processing iOS Devices

In the initial Splash screen, examiners have the ability to acquire an iOS image from an iPhone, iPod, or iPad that is connected to their forensic Mac. The examiner will need the authentication credentials for the iOS device and the ability to interact with the iOS display (i.e. a functioning screen). iTunes must be installed on the Mac and it must to be up to date. In macOS 10.15 iTunes has been removed and the functionality of iTunes has been divided into three different applications and integrated into macOS.

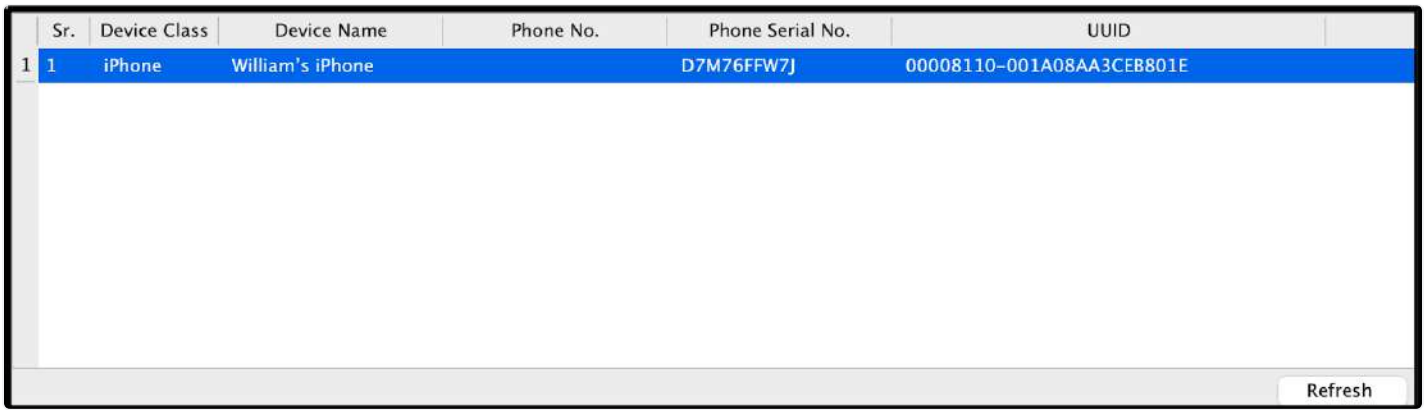
30.1 Acquiring an iOS Device



Unlock the iOS device to be acquired. Start RECON LAB and select the **Acquire iOS Device** button. The iOS Device window will appear.



Connect the **unlocked** iOS device to the Mac and make sure that the iOS device as been authorized to connect to the Mac by clicking the **Trust** button. If the Trust button does not appear automatically select the iOS device from the Finder Sidebar. A prompt to **Trust** may also appear on the iOS device as well.



Once the device has been authorized click the **Refresh** button to see any connected iOS devices.

Select the iOS device to acquire from the list and click the **Acquire** button.

Select the **Destination** for the output to begin the acquisition. Once completed a prompt will appear asking if you would like to open the output.

See section 10.2.3.1 iTunes iOS Backup to add the iOS backup as a source to your case.

31. Reporting

RECON LAB includes a variety of reporting options from the granular level (single artifacts or plugins) to the global level (all artifacts or plugins included) and anything in-between.

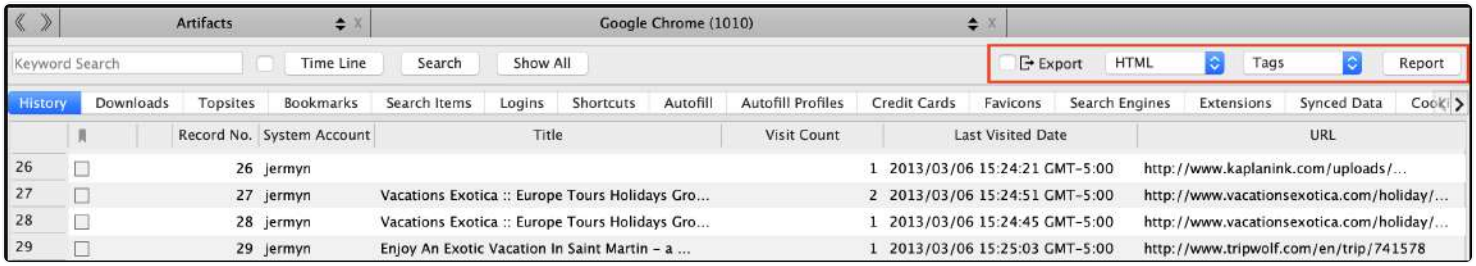
Additionally, RECON LAB includes the first of its kind WYSIWYG (What You See Is What You Get) reporting mode called StoryBoard. Story Board allows the examiner to have full control over the reporting process and is as easy to use as a word processor. The examiner has the ability to add, remove or annotate bookmarks anywhere in the report at any time.

Story Board also allows the examiner to add his/her bookmarks and tags in chronological order to make it easier to understand the timeline of events.

31.1 Plugin Reports

RECON LAB supports automatically processing thousands of artifacts using hundreds of plugins. Processed artifacts can be found by expanding **Artifacts** in the Sidebar.

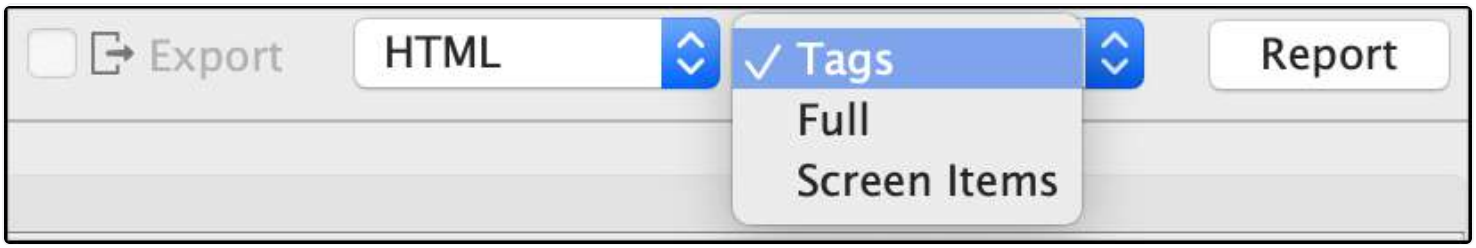
Selecting any **Plugin** category will open a results window. Every Plugin has the ability to create a variety of reports depending on the type of artifacts recovered.



Plugin reports can be generated by selecting a few options found in the upper right-hand corner of the plugin results window.

The **type of report** can be selected from the first dropdown list. The options are the following:

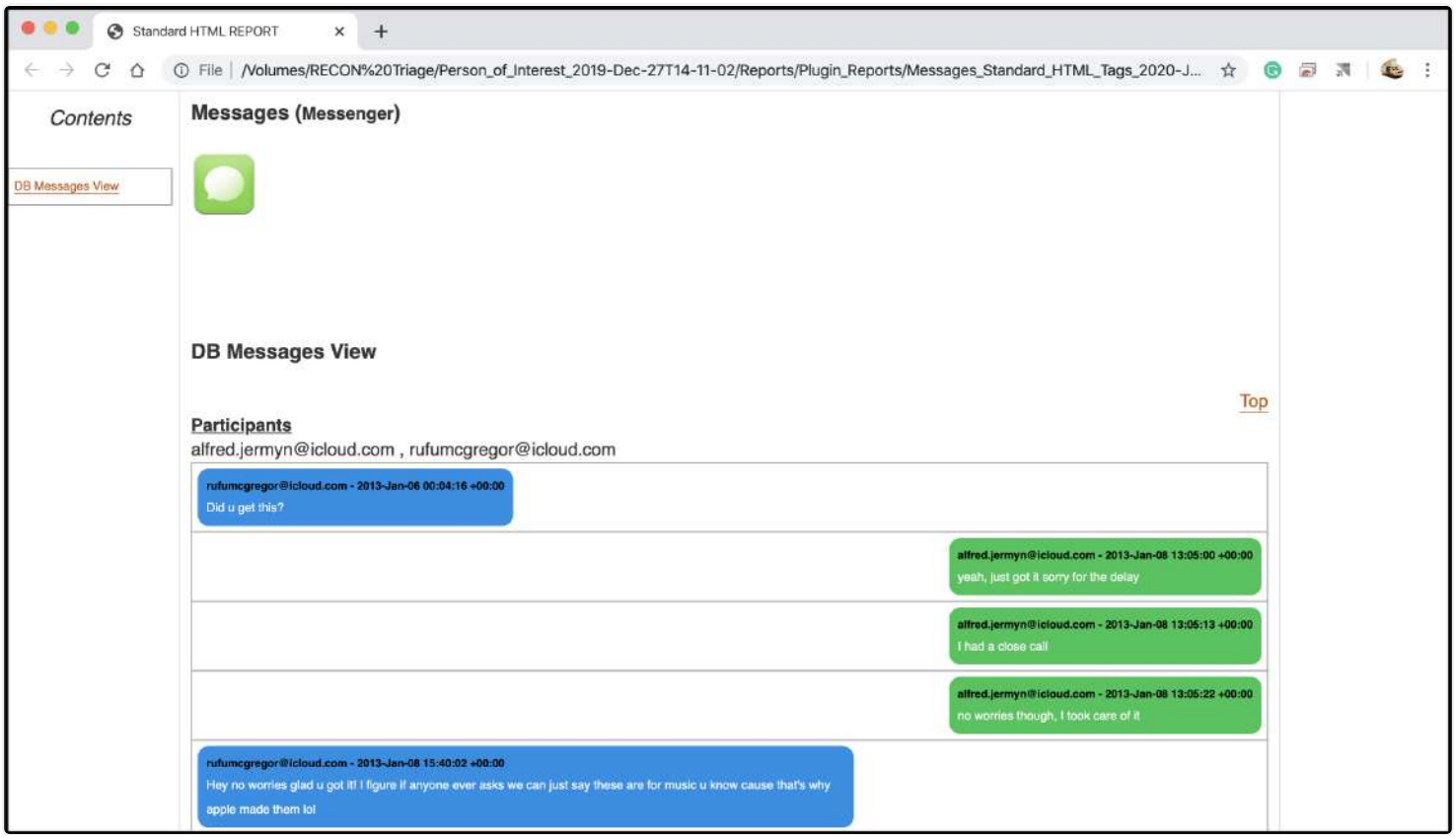
- **HTML** - Report which can be easily opened with a web browser
- **PDF** - Portable Document Format
- **CSV** - Comma Separated Value (spreadsheet)
- **XML** - Extensible Markup Language
- **KML** - Keyhole Markup Language file used for files that contain geotags



The second dropdown list allows the examiner to select **what will be included** in the report. The options are the following:

- **Tags** - a report with only the items that have been bookmarked in the current plugin and its tabs
- **Full** - a report of all artifacts from all tabs of the current plugin
- **Screen Items** - includes what is currently displayed in the list of results including the results of any filters

Any items selected with the previous settings that include exportable data can be included with the report by checking the **Export** checkbox.



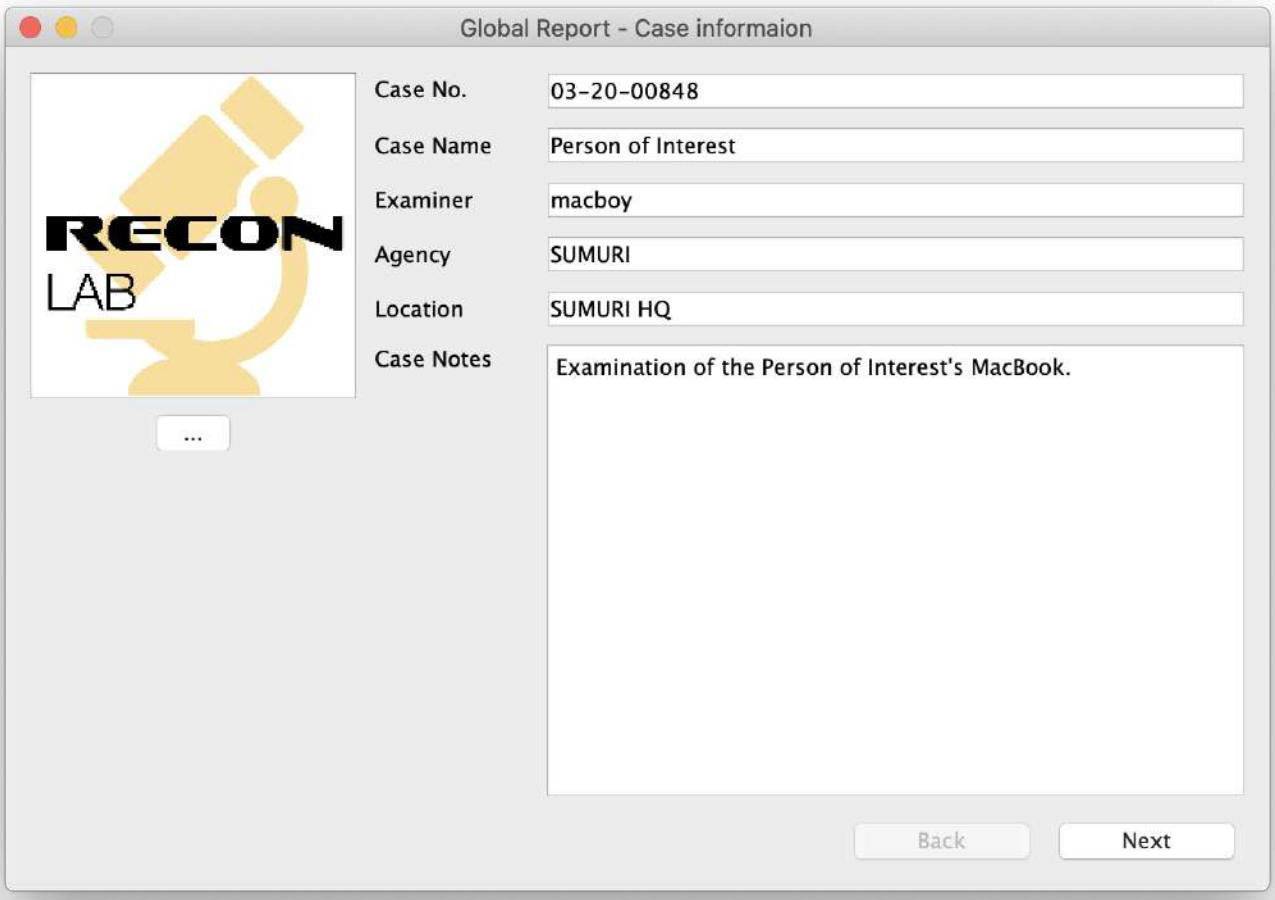
Once all the settings have been selected the report can be generated by clicking the **Report** button.

31.2 Global Artifacts Report

The Global Artifacts Report automatically creates reports from bookmarks and tags.

To begin creating a Global Artifacts Report and to open the Global Report Case Information window click on the **Global Report icon** from the Top Menu.

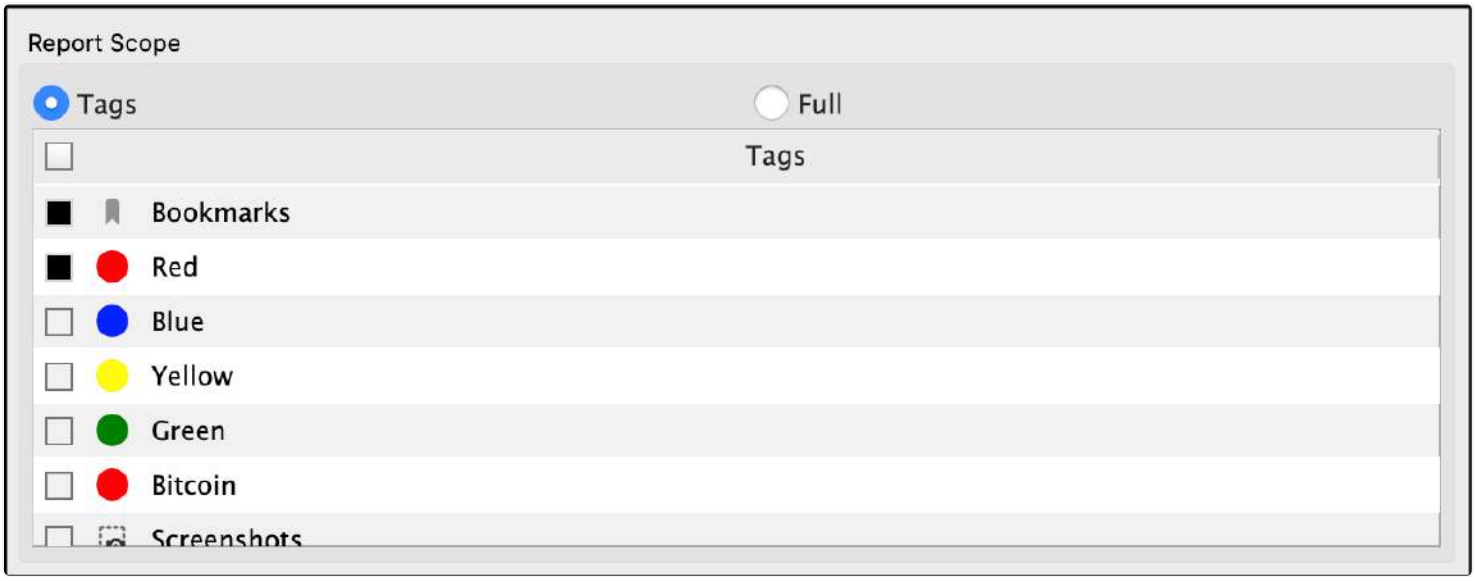
31.2.1 Case Information Window



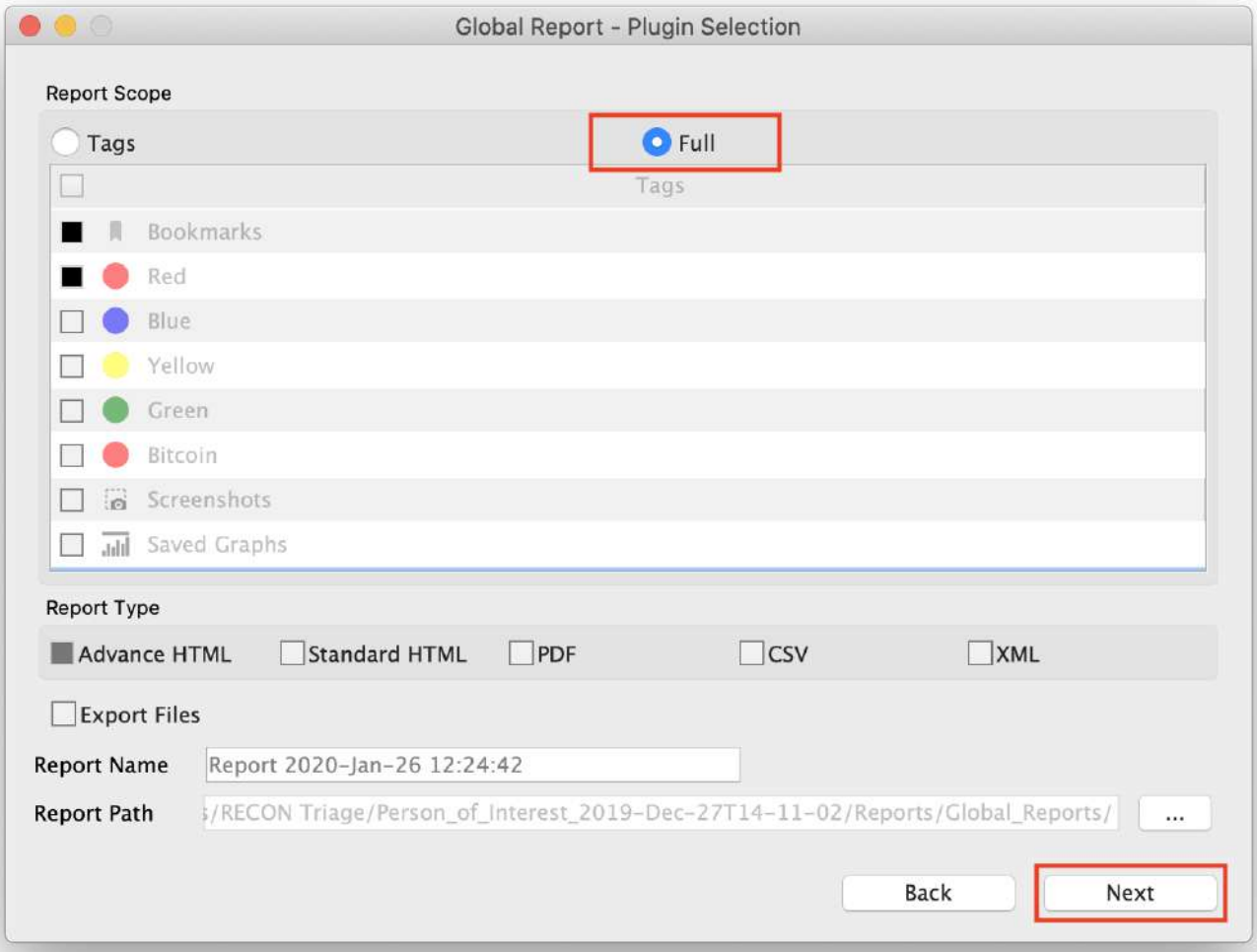
The **Global Report Case Information** window allows the examiner to adjust and enter additional information to be included in the report. To proceed to the **Global Report - Report Category** selection click the **Next** button.

31.2.2 Customizing Global Reports

The Global Report can be customized using the **Report Scope** and **Report Type** options in the Global Report - Report Category window.

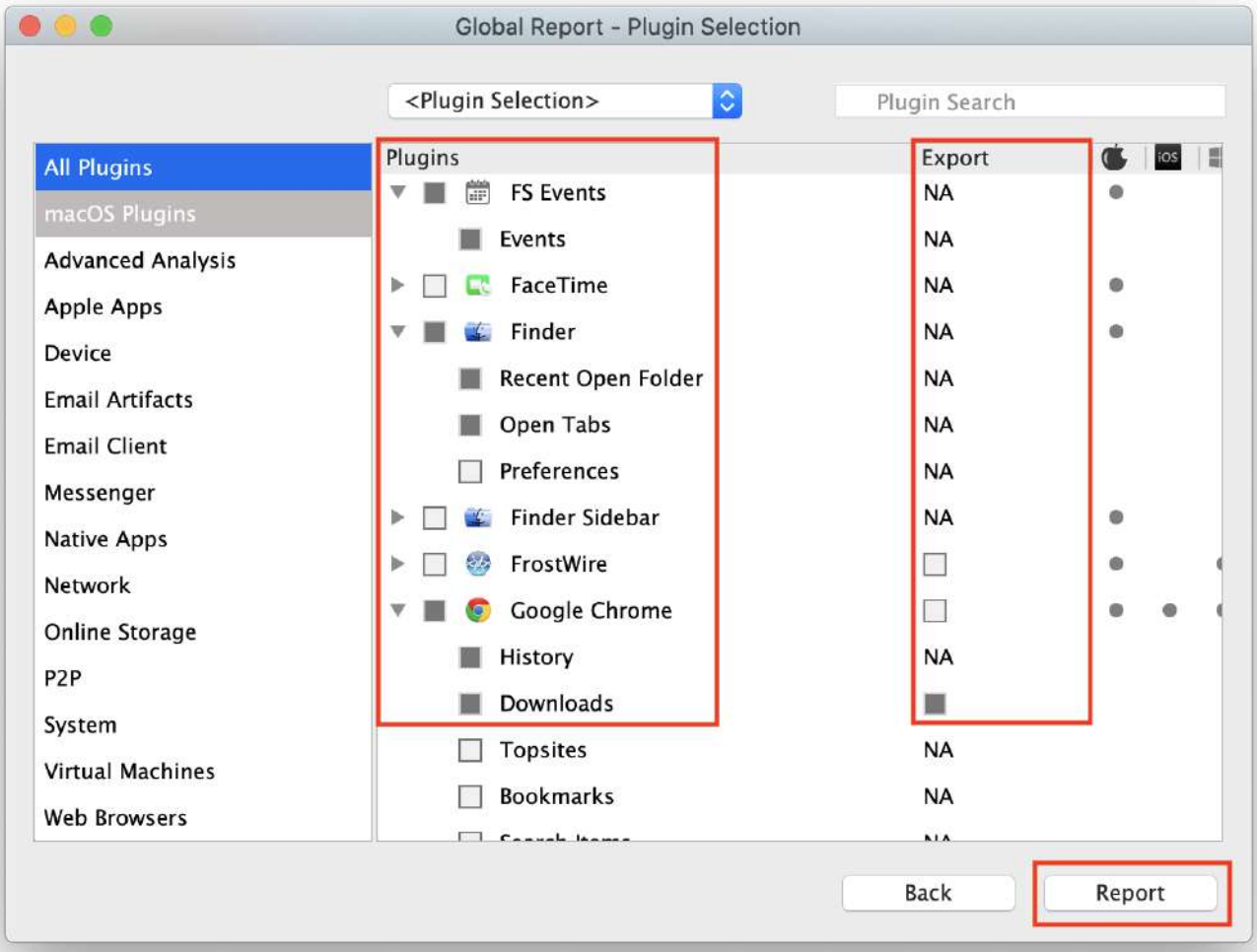


If **Tags** is selected under **Report Scope** the examiner can then choose any category of bookmarks or tags to include in the report.



If **Full** is selected under **Report Scope** then the Report button will change to **Next** to allow the examiner to select individual Plugins to be included in the report.

Note: Make sure to set the Report Type, Report Name and Report Path options before proceeding. These options will be discussed later.

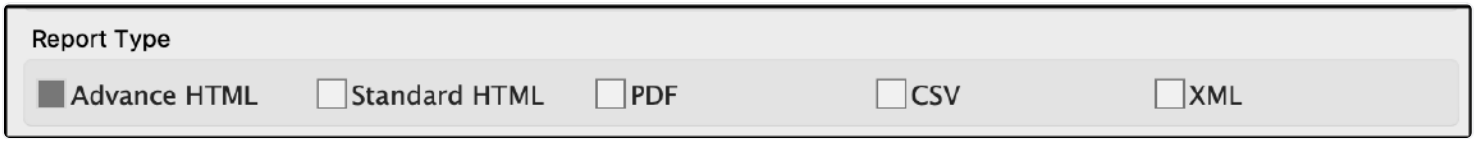


From the Global Report - Plugin Selection window individual plugins and their artifacts can be selected for inclusion in the report by checking the boxes.

If there are any files that can be exported during report creation the examiner can activate the checkbox under the Export column.

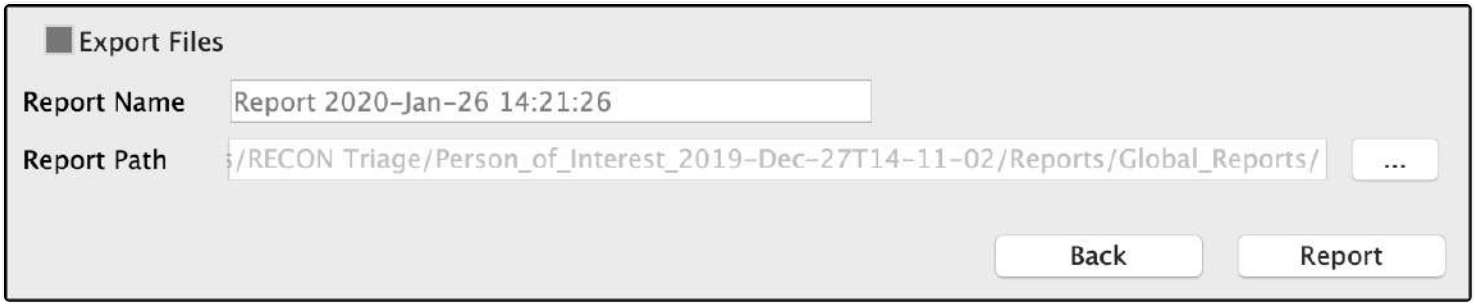
To create a Global Report from the Plugin Selection window just click Report.

31.2.3 Global Report Type



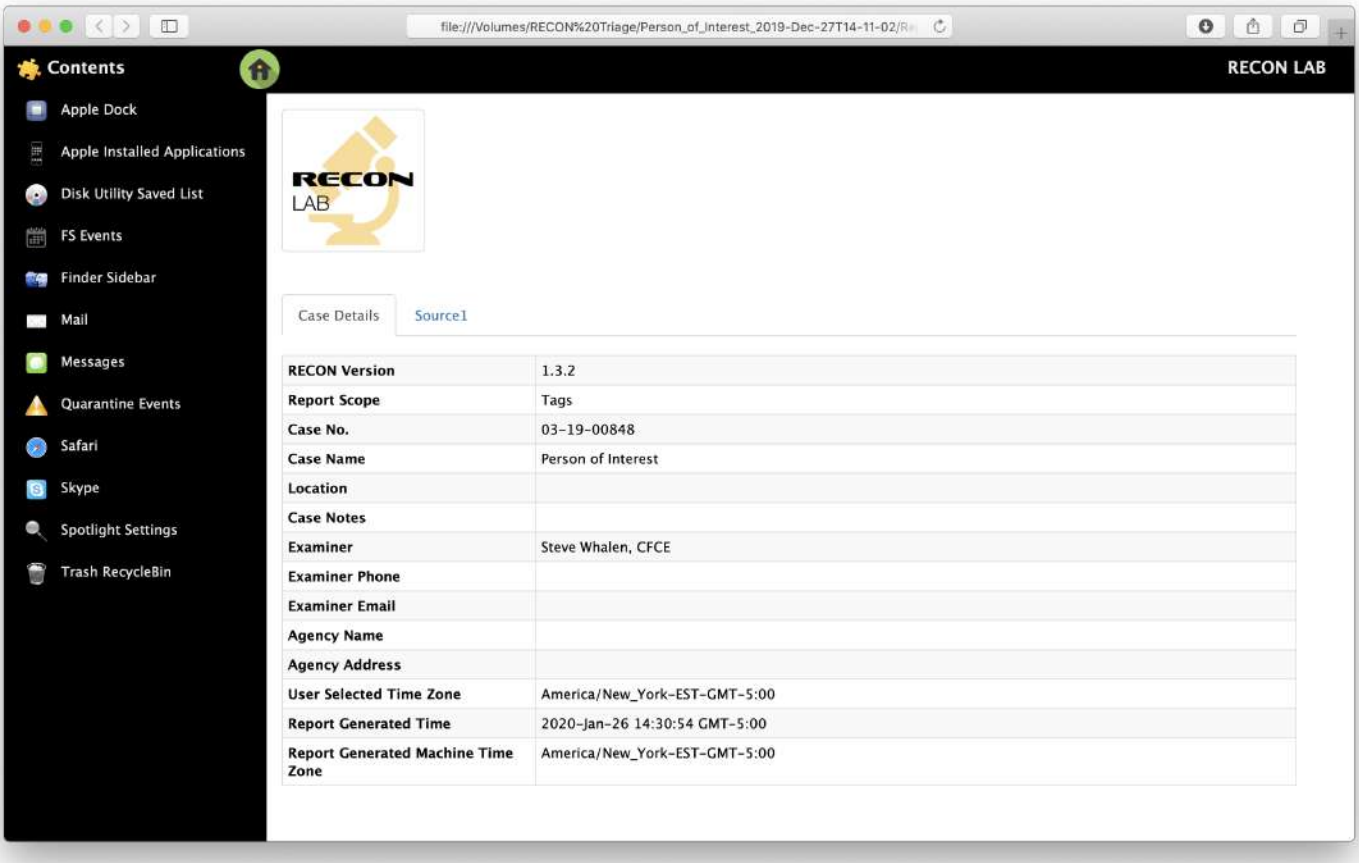
The **Report Type** can be selected in the Global Report - Report Category window. The following report types are available:

- **Advanced HTML** - Report which can be easily opened with a web browser and have advanced navigation
- **Standard HTML** - Report which can be easily opened with a web browser in a linear format
- **PDF** - Portable Document Format
- **CSV** - Comma Separated Value (spreadsheet)
- **XML** - Extensible Markup Language



To create the Global Report from the Report Category window select whether or not to **Export Files** by activating the checkbox.

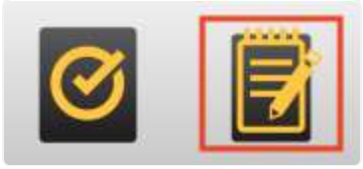
Optionally, the **Report Name** and **Report Path** can be changed.



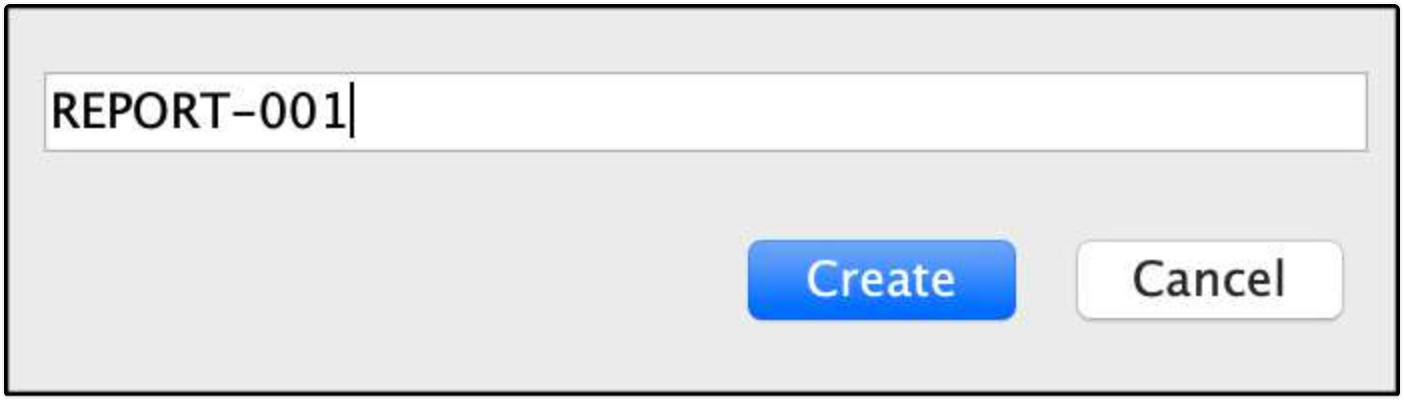
Once all options have been selected click **Report** to generate the report.

31.3 Story Board Reports - WYSIWYG Reports

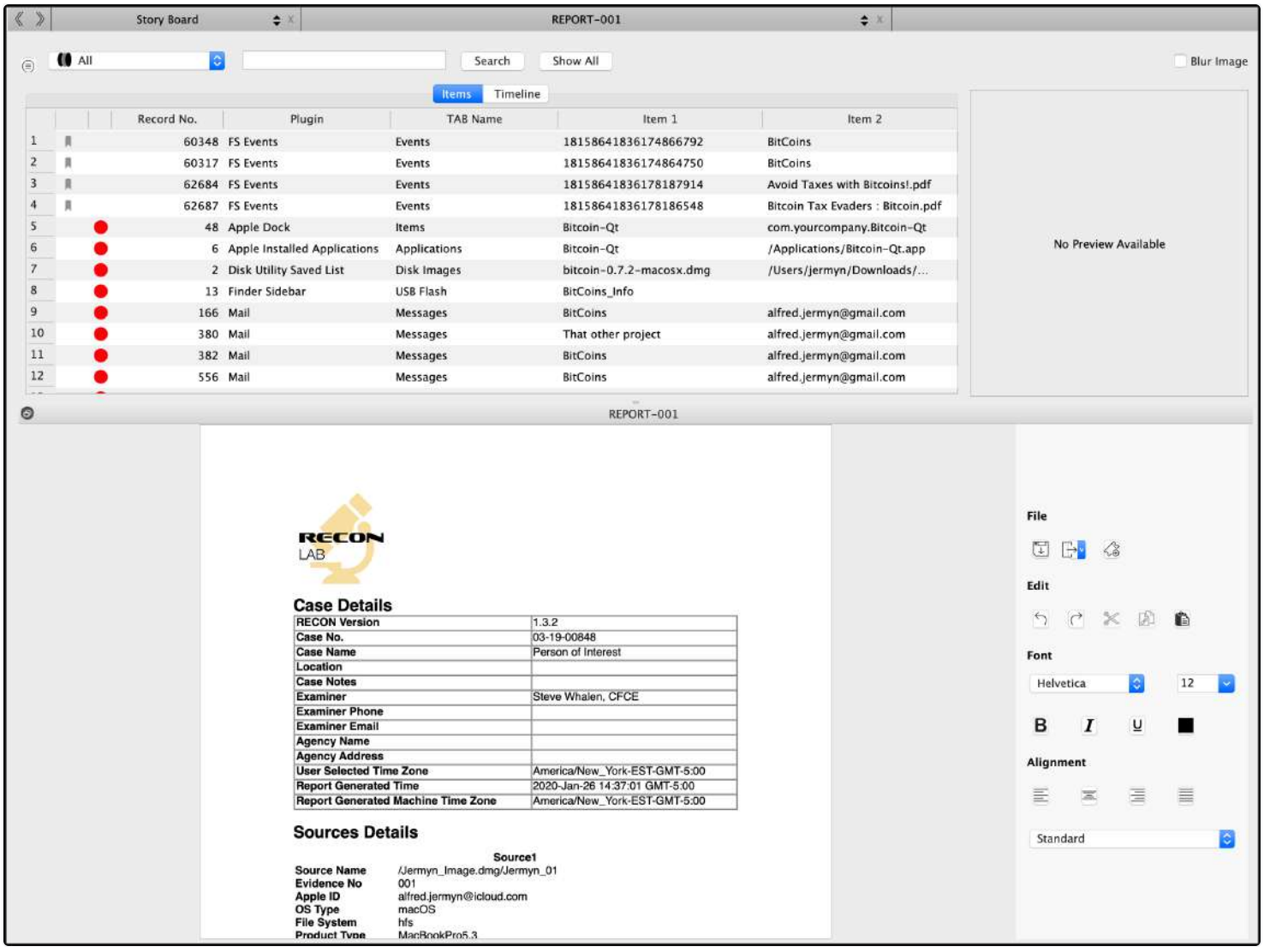
RECON LAB includes the first ever “What you see is what you get” (WYSIWYG) reporting option in a forensic suite called Story Board. With **Story Board**, the examiner has full control over reporting allowing a user to add text, tags, bookmarks at will. Additionally, Story Board includes the ability to sort and add bookmarks and tags chronologically. Chronological reporting is proven to increase understand of factual events.



To create a report using the Story Board reporting mode click the **Story Board** icon in the Top Menu.

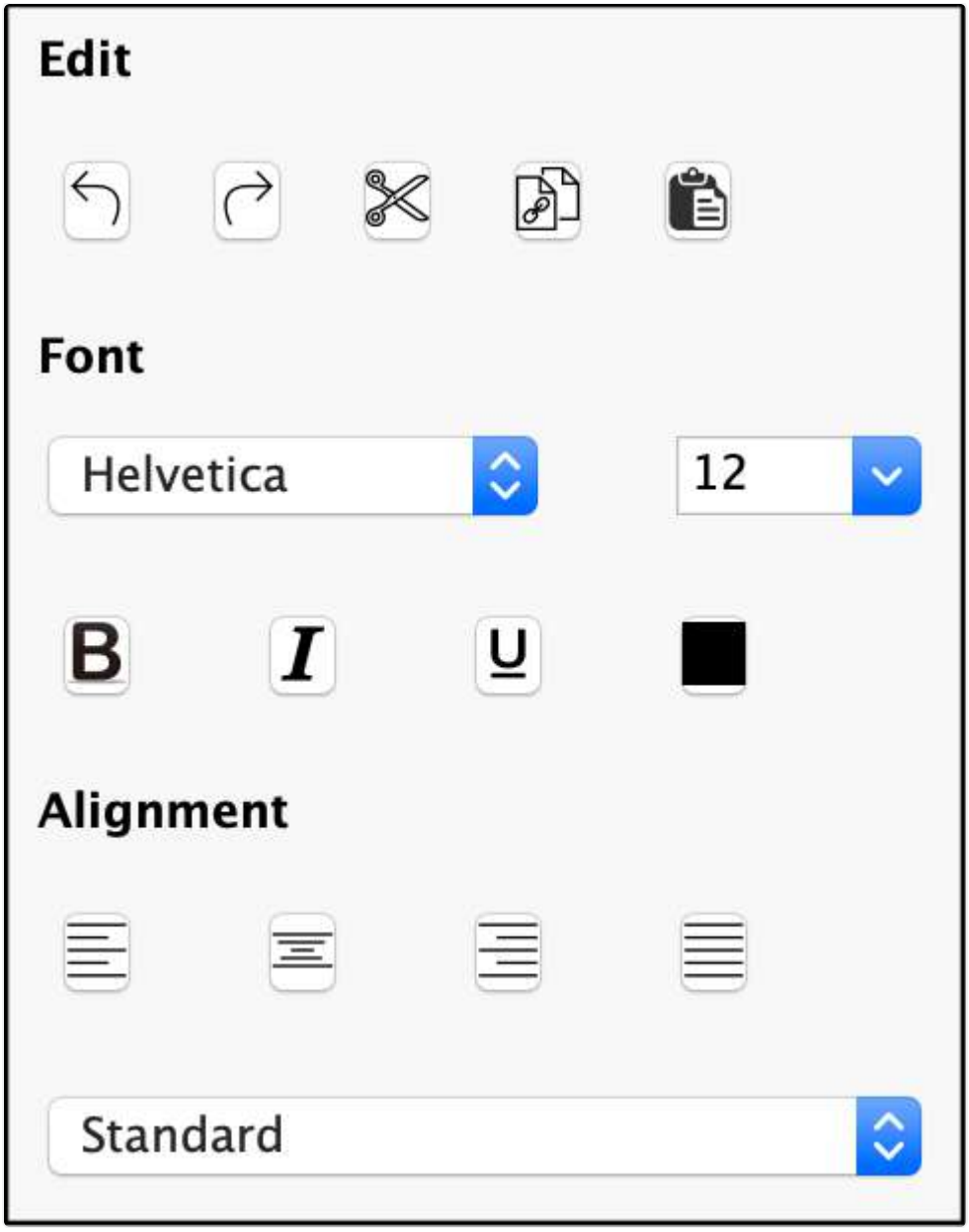


Enter a name for the report and click **Create** and the Story Board main interface will open.



The Story Board interface is divided into two sections. All tags and bookmarks from the case are accessible and found at the top. The report is found in the bottom section.

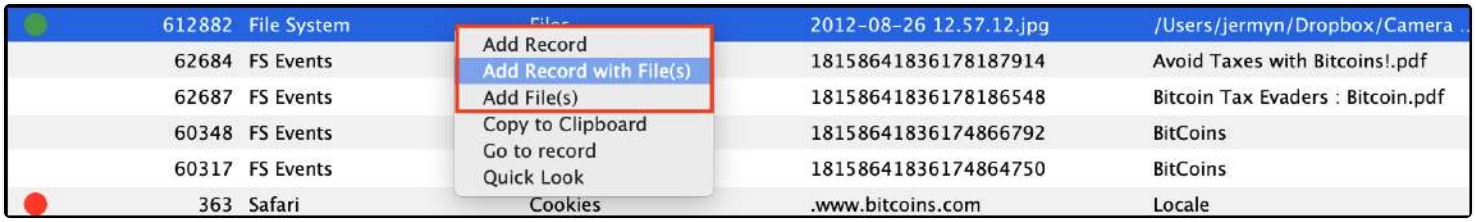
31.3.1 Editing a Report



The Story Board interface includes a word processor with common formatting options which can be found to the right of the report.

- **Edit** - Undo, Redo, Cut, Copy, Paste
- **Font** - Installed Fonts, Font Size, Bold, Italic, Underline, Font Color
- **Alignment** - Left-centered, Centered, Right-centered, Justified, List Options

32.3.2 Adding Tags and Bookmarks to a Report



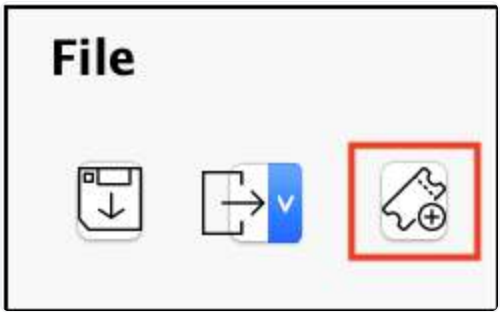
To add an item (record) to the Story Board report place the cursor at the location where the item is to be placed. Right-click on an item from the bookmarks and tags list and select from one of the three options:

- **Add Record** - adds details about the record (bookmark, tag) to the report without the file
- **Add Record with File(s)** - adds both the details of the record to the report with the file (export)
- **Add File(s)** - adds the file only to the report (export)

Detailed Information	File Preview
Source Name: /Jermyn_Image.dmg/Jermyn_01 **Record No.:** 612882 **File Name:** 2012-08-26 12.57.12.jpg **File Path:** /Users/jermyn/Dropbox/Camera Uploads/2012-08-26 12.57.12.jpg **Inode No./File ID:** 607635 **File Size:** 957.55 KB (980533 bytes) **Mime Type:** image/jpeg **Date Modified:** 2012-Aug-26 11:57:12 GMT-5:00 **Date Change:** 2013-Apr-30 12:43:25 GMT-5:00 **Date Accessed:** 2013-Apr-30 12:43:25 GMT-5:00 **Date Added(Apple):** 2013-Mar-06 14:04:30 GMT-5:00 **Content Creation Date(Apple):** 2012-Aug-26 11:57:12 GMT-5:00 **Content Modification Date(Apple):** 2012-Aug-26 11:57:12 GMT-5:00 **Tag:** Green **Examiner Notes:**	

The above is an example of a record added to the report with the file.

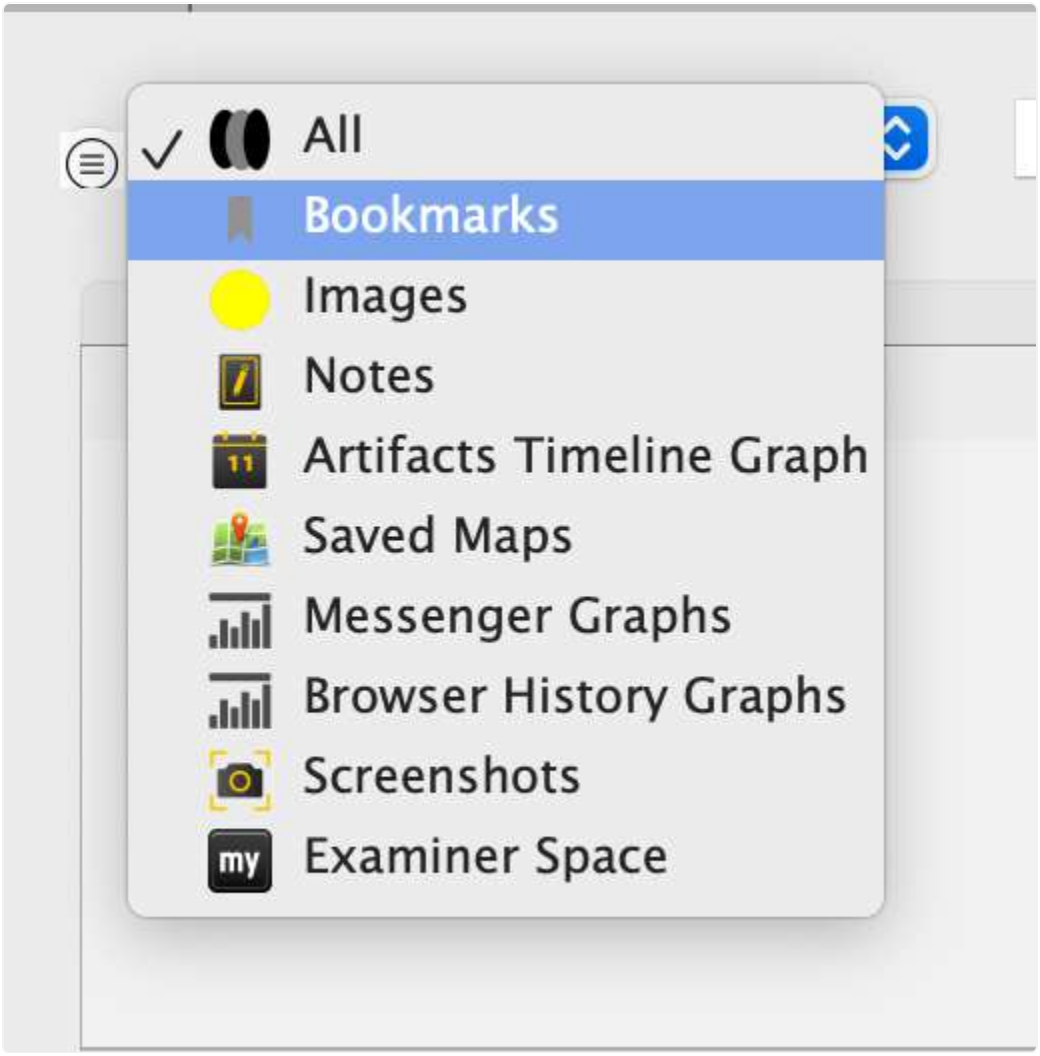
31.3.3 Adding External Files to a Report



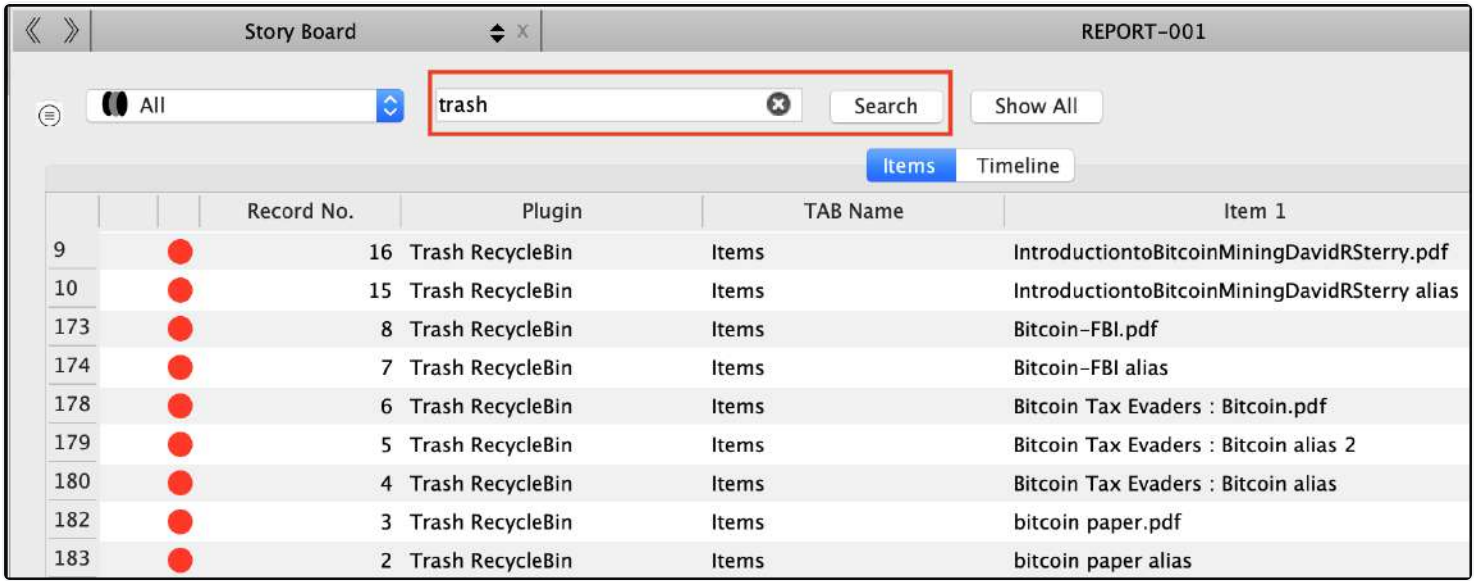
To add external files to the Story Board report click the **Add File** button found above the formatting options to the right of the report.

Navigate to the file to add and click Open to add the file to the report.

31.3.4 Filtering Records In Story Board



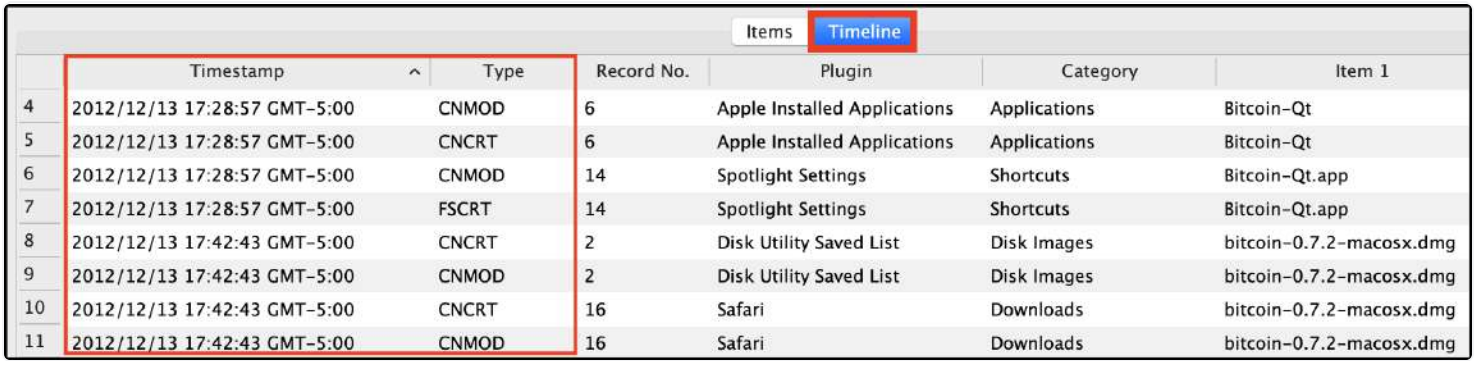
Categories of records can be selected and filtered by using the dropdown list.



		Record No.	Plugin	TAB Name	Item 1
9		16	Trash RecycleBin	Items	IntroductiontoBitcoinMiningDavidRSterry.pdf
10		15	Trash RecycleBin	Items	IntroductiontoBitcoinMiningDavidRSterry alias
173		8	Trash RecycleBin	Items	Bitcoin-FBI.pdf
174		7	Trash RecycleBin	Items	Bitcoin-FBI alias
178		6	Trash RecycleBin	Items	Bitcoin Tax Evaders : Bitcoin.pdf
179		5	Trash RecycleBin	Items	Bitcoin Tax Evaders : Bitcoin alias 2
180		4	Trash RecycleBin	Items	Bitcoin Tax Evaders : Bitcoin alias
182		3	Trash RecycleBin	Items	bitcoin paper.pdf
183		2	Trash RecycleBin	Items	bitcoin paper alias

Additionally, records can be filtered by entering a keyword in the **Search** box.

31.3.5 Adding Records in Chronological Order



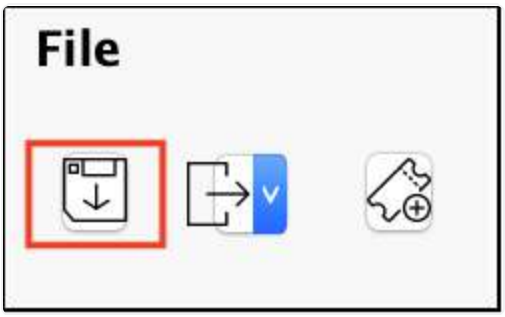
	Timestamp	Type	Record No.	Plugin	Category	Item 1
4	2012/12/13 17:28:57 GMT-5:00	CNMOD	6	Apple Installed Applications	Applications	Bitcoin-Qt
5	2012/12/13 17:28:57 GMT-5:00	CNCRT	6	Apple Installed Applications	Applications	Bitcoin-Qt
6	2012/12/13 17:28:57 GMT-5:00	CNMOD	14	Spotlight Settings	Shortcuts	Bitcoin-Qt.app
7	2012/12/13 17:28:57 GMT-5:00	FSCRT	14	Spotlight Settings	Shortcuts	Bitcoin-Qt.app
8	2012/12/13 17:42:43 GMT-5:00	CNCRT	2	Disk Utility Saved List	Disk Images	bitcoin-0.7.2-macosx.dmg
9	2012/12/13 17:42:43 GMT-5:00	CNMOD	2	Disk Utility Saved List	Disk Images	bitcoin-0.7.2-macosx.dmg
10	2012/12/13 17:42:43 GMT-5:00	CNCRT	16	Safari	Downloads	bitcoin-0.7.2-macosx.dmg
11	2012/12/13 17:42:43 GMT-5:00	CNMOD	16	Safari	Downloads	bitcoin-0.7.2-macosx.dmg

Selecting the Timeline tab allows records to be sorted chronologically. Records can then be added to the report in sequence of occurrence.

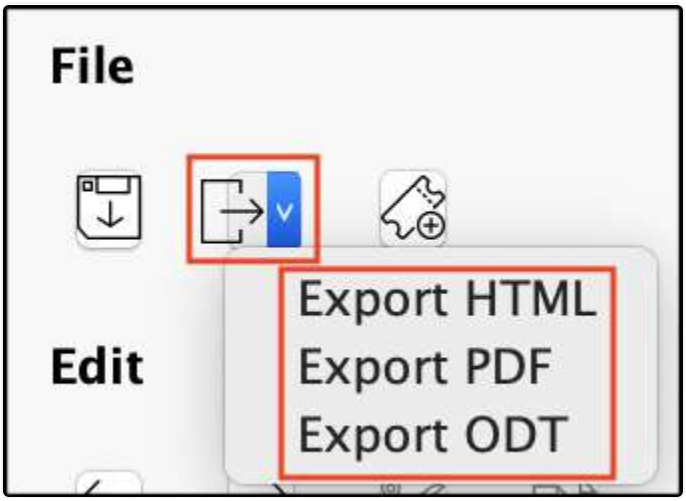
31.3.6 Blur Image in Report

To blur and image that is to be added to a Story Board report check the **Blur Image** button before adding an image to the report.

31.3.7 Saving and Exporting a Story Board Report



Use the **Save** button to save the current state of the Story Board report.



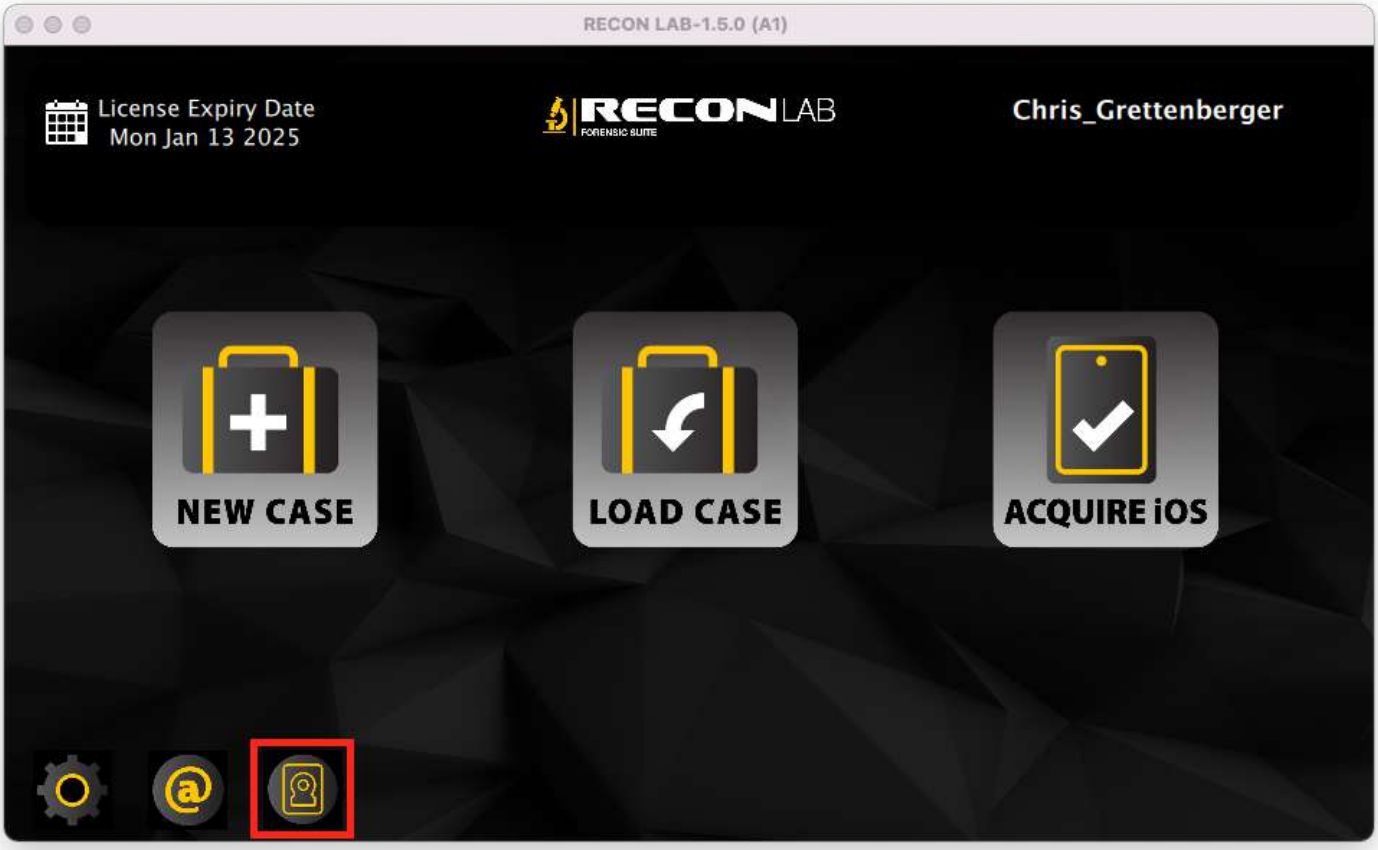
To export the report in a HTML, PDF or ODT format click the **Export** button and select one of the options from the dropdown list.

32. Shutdown RECON LAB

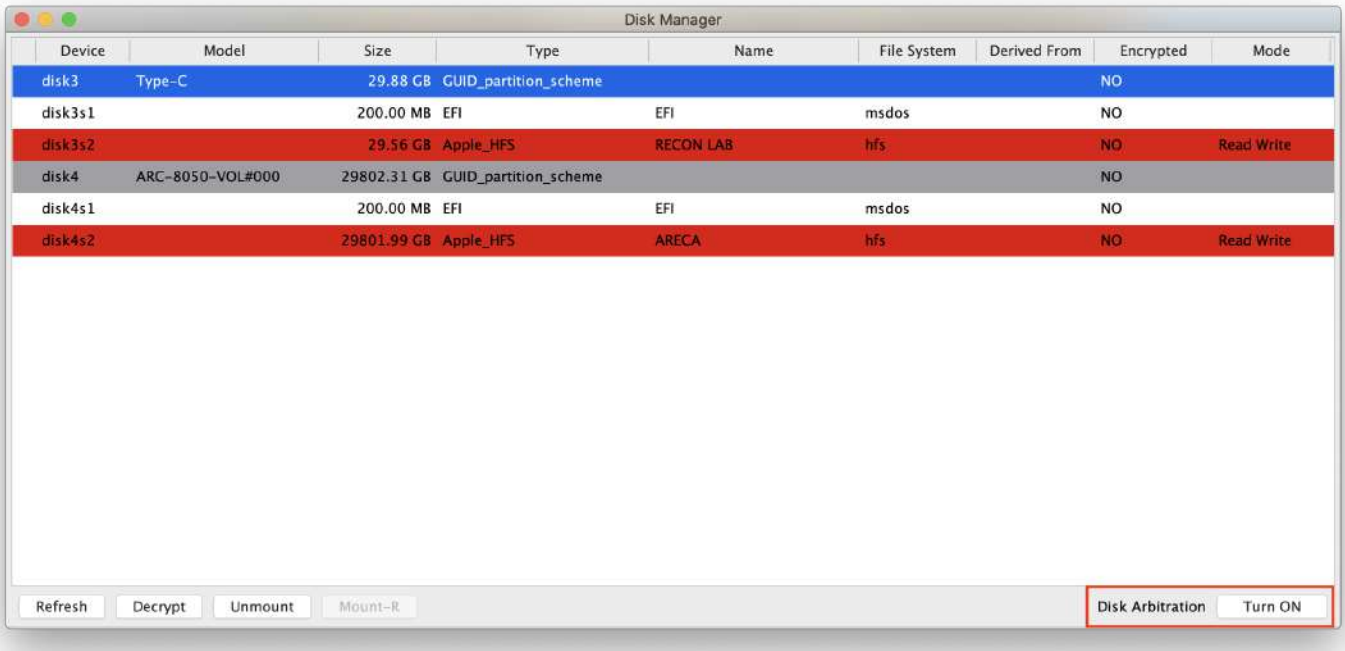
To quit RECON LAB select “Quit RECON_LAB” from the top menu

33. Disk Manager with Write-Block

Disk Manager allows the processing and analysis of connected devices and their volumes by using RECON LAB’s Disk Manager and software write-blocking features.



Disk Manager can be accessed from the RECON LAB Welcome Screen by clicking the **Disk Manager** button.

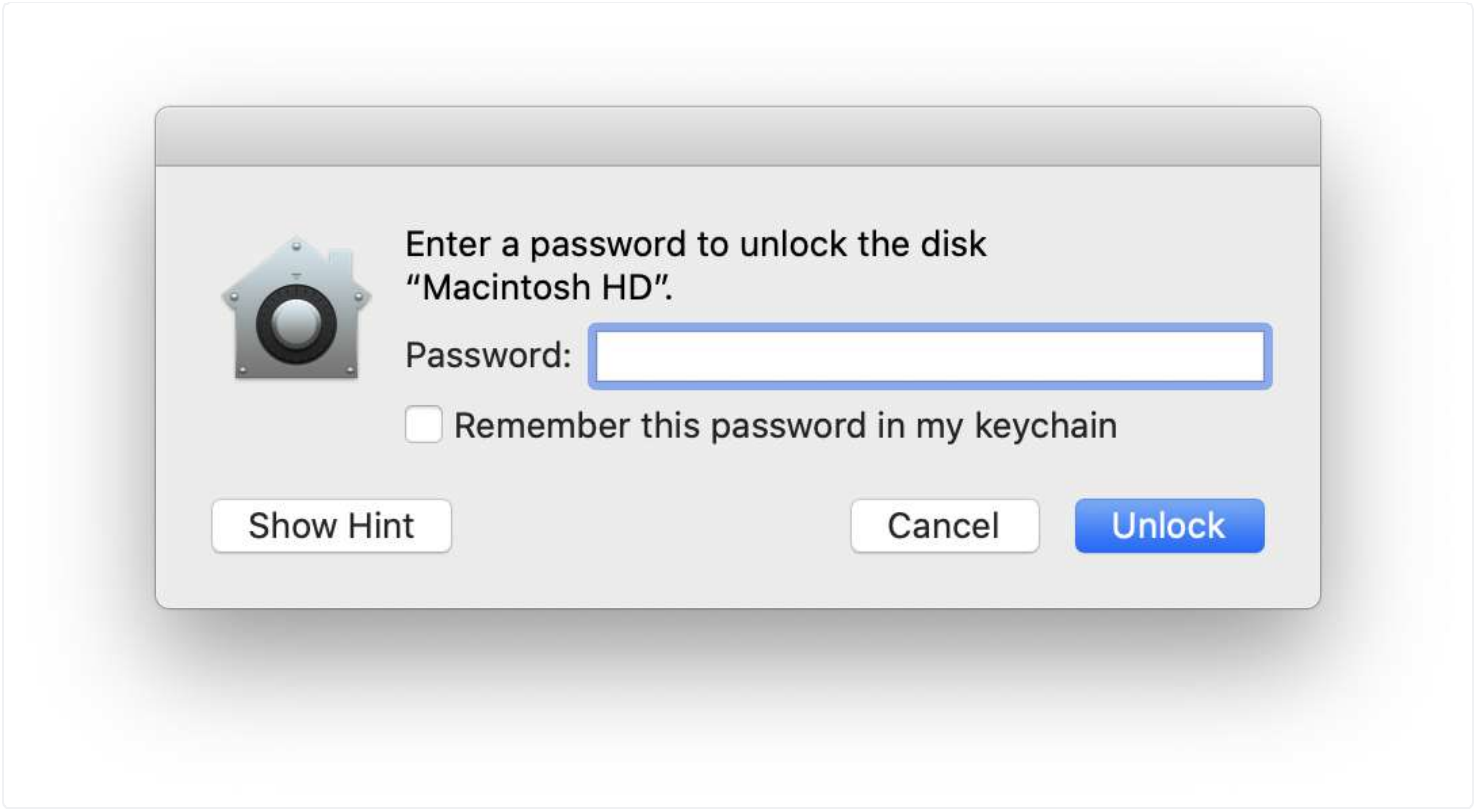


The Disk Manger window will open showing all connected disks and volumes that can be accessed by RECON LAB.

33.1 Write-Blocking

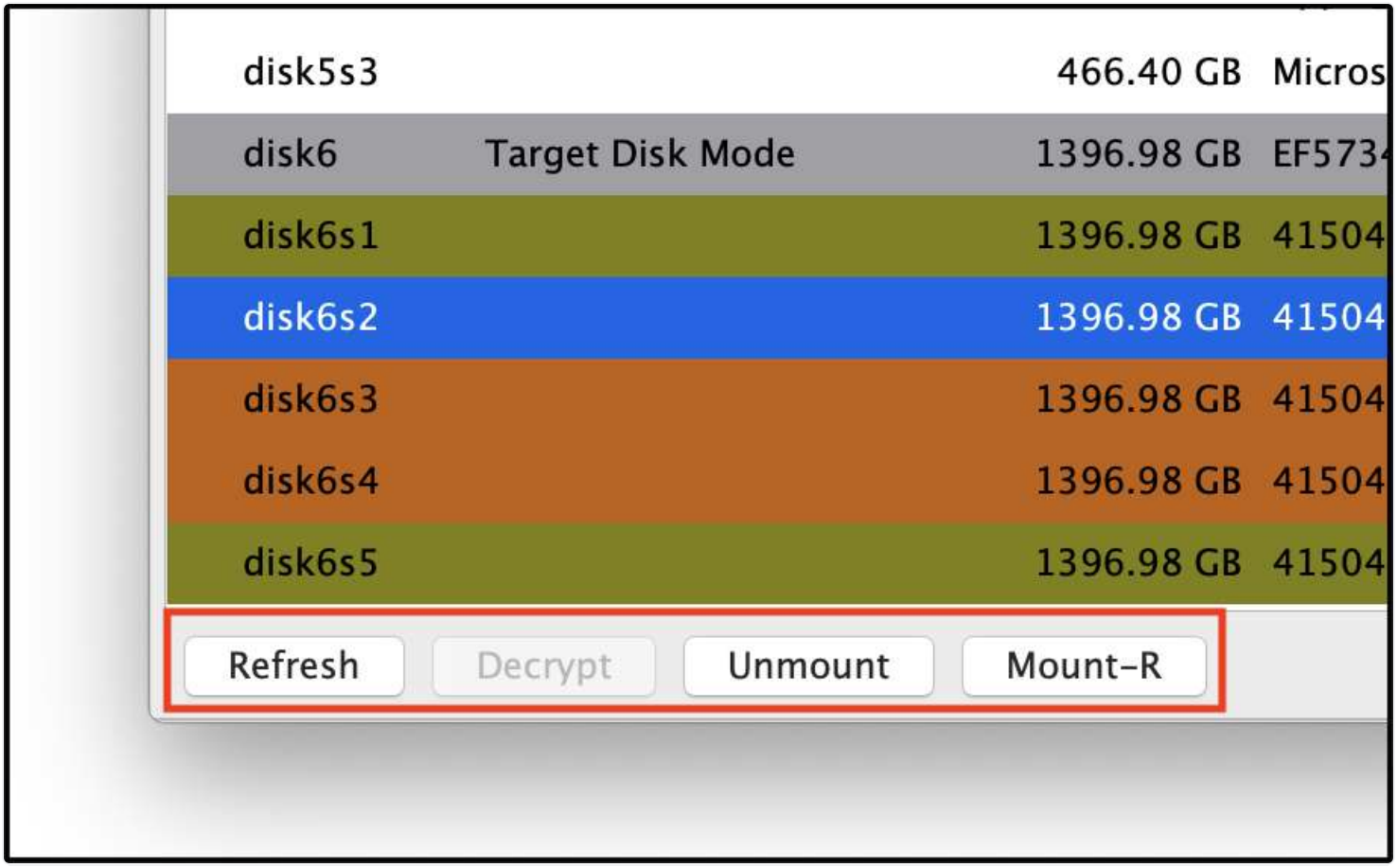
Mac computers in Target Disk Mode and other disks can be connected safely (write-block) to RECON LAB by disabling the Disk Arbitration daemon. To turn off Disk Arbitration click the **Turn Off** button at the bottom right of the Disk Manager.

Once disabled hard disks and Mac computers placed in Target Disk Mode can be connected safely to your examination Mac.



If the Mac being connected contains a T2 Security Chipset there will be prompt to enter a password for an active account on the Mac being connected in Target Disk Mode.

After connecting the device click the Refresh button to show the new devices.

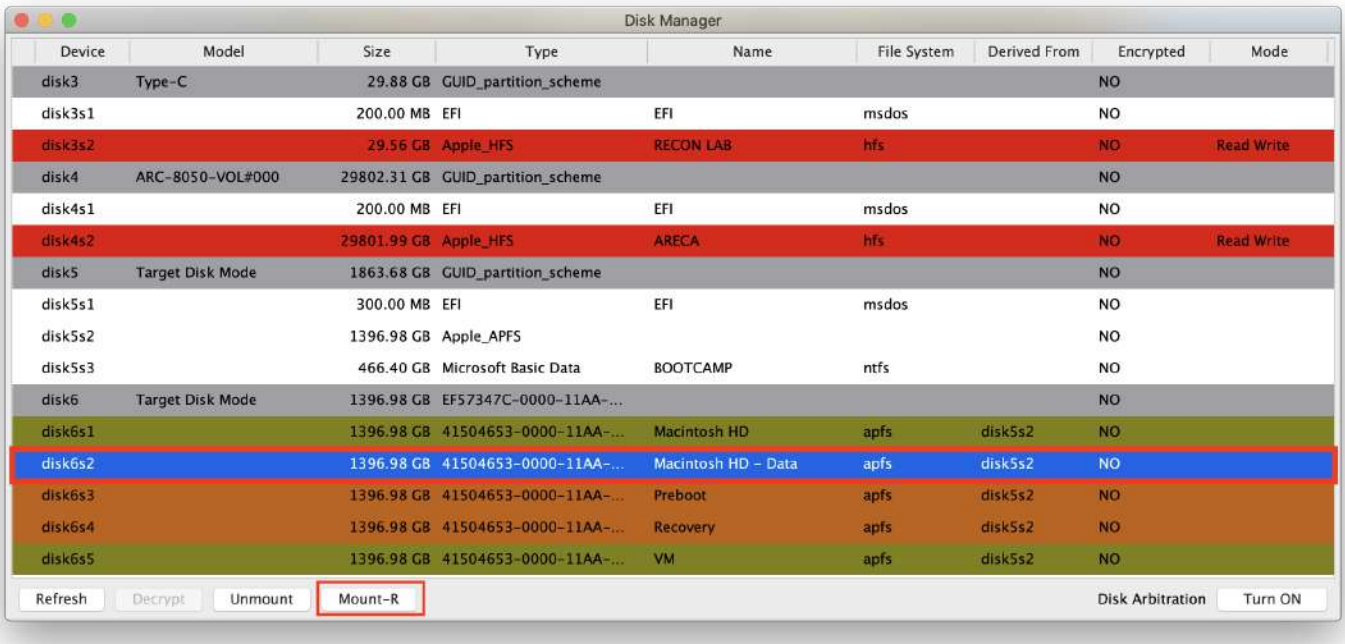


With the new devices displayed, the following options exist:

- **Refresh** - re-poll for changes to connected devices
- **Decrypt** - allows an examiner to decrypt FileVault volumes with a password or Recovery Key
- **Unmount** - unmount any previously mounted volume
- **Mount-R** - mounts a volume or disk read-only

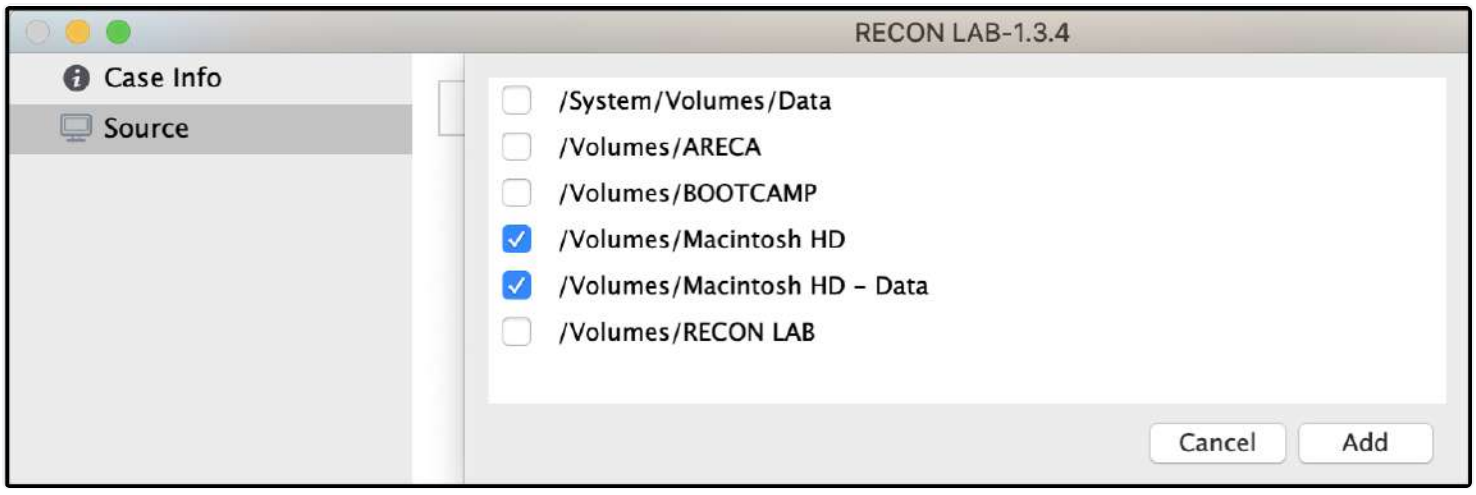
33.2 Mounting a Device Read-Only

The Disk Manager can be used to mount volumes as read only to ensure that there are no changes to data.



Select the volume in the Disk Manager to mount as read-only and click Mount-R.

Note: If you are mounting a Mac in Target Disk Mode with macOS 10.15 or higher you will need to mount both the System and Data partitions as read-only.



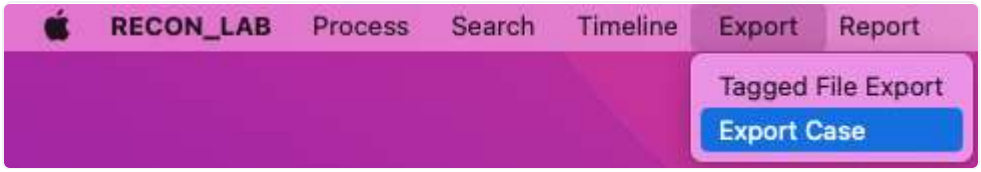
Once mounted read-only, the volumes can be added to RECON LAB for processing.

34. RECON LAB Case Exporter

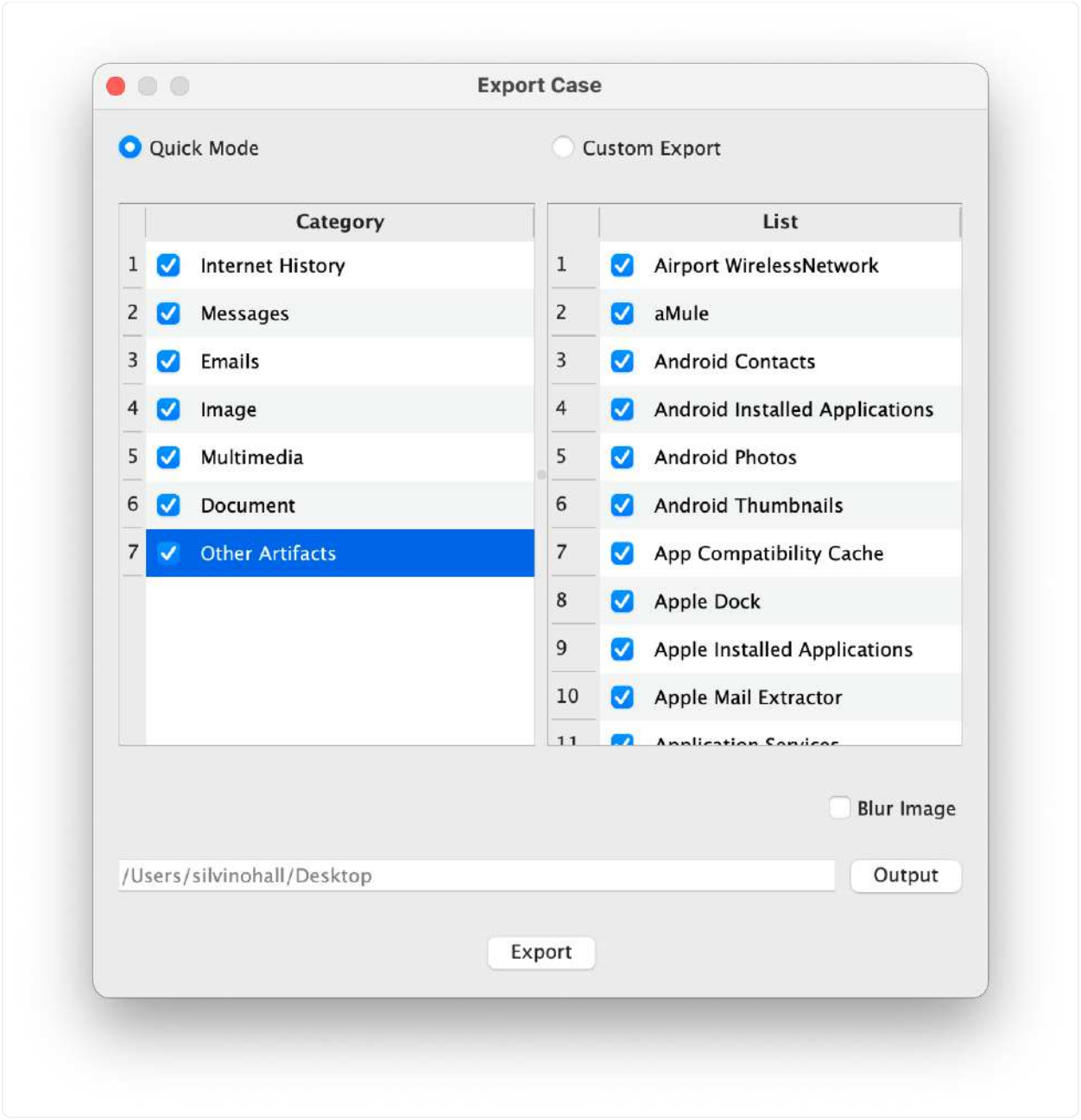
RECON LAB's Case Exporter feature allows examiners to collaborate with one another by using a portable case. This feature gives teams the ability to export all of the important information to a standalone application that can be reviewed by a Windows computer.

34.1 Exporting a Case

Exporting a case is a simple process that allows examiners to export findings in a way that can be further analyzed without the need for a RECON LAB license.



Select Export > **Export Case** in the Menu Bar, and the Export Case window will appear.



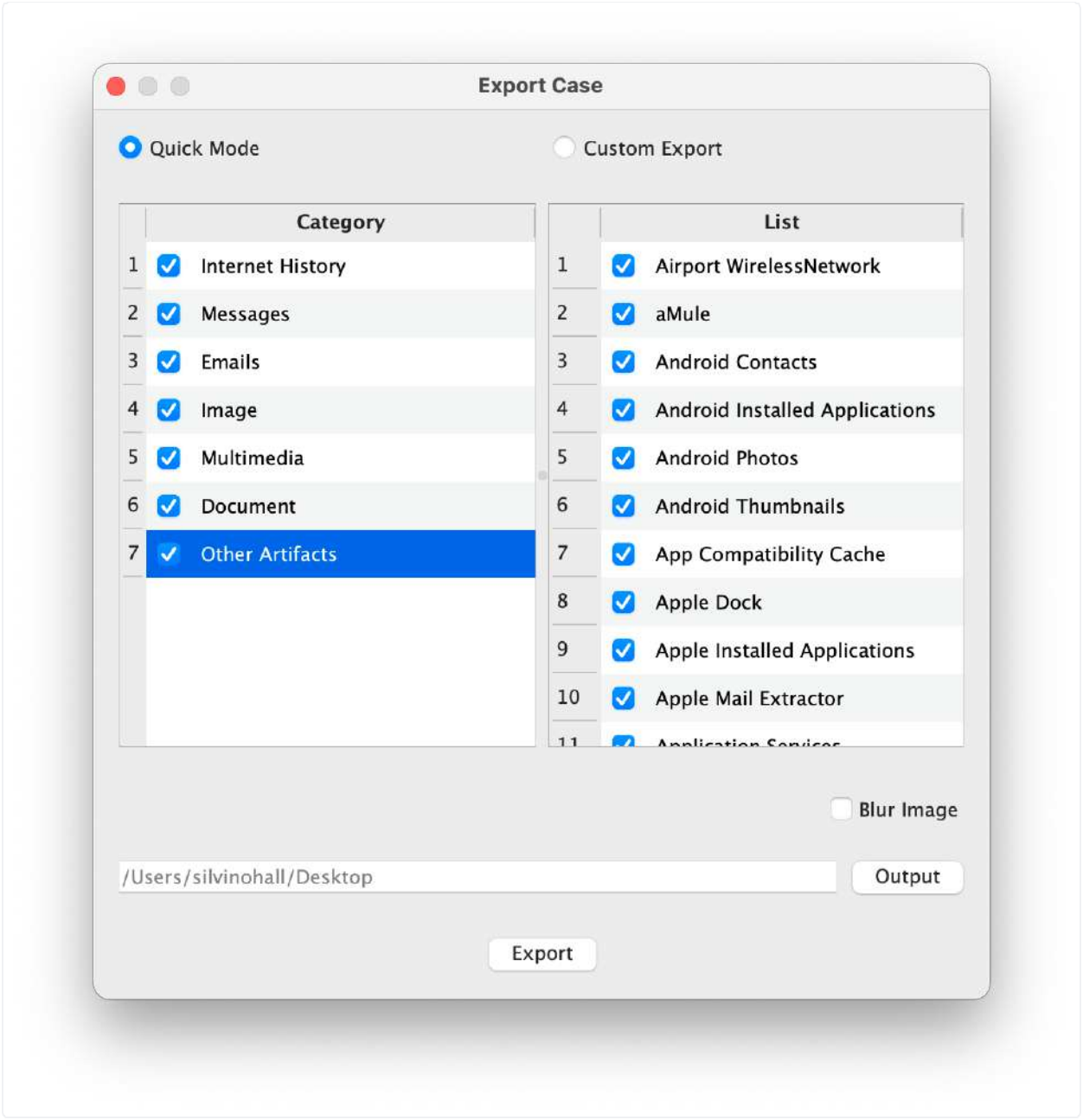
RECON LAB has two options when exporting a case:

Quick Mode - Allows examiners to quickly export data from the case using RECON LAB's preset configurations from automated plugins

Custom Export - Allows examiners to selectively include data for their case from bookmarks and tags

34.1.2 Quick Mode

In **Quick Mode**, select the **Category** options with their corresponding automated plugins under **List** to export and analyze in RECON CASE READER.

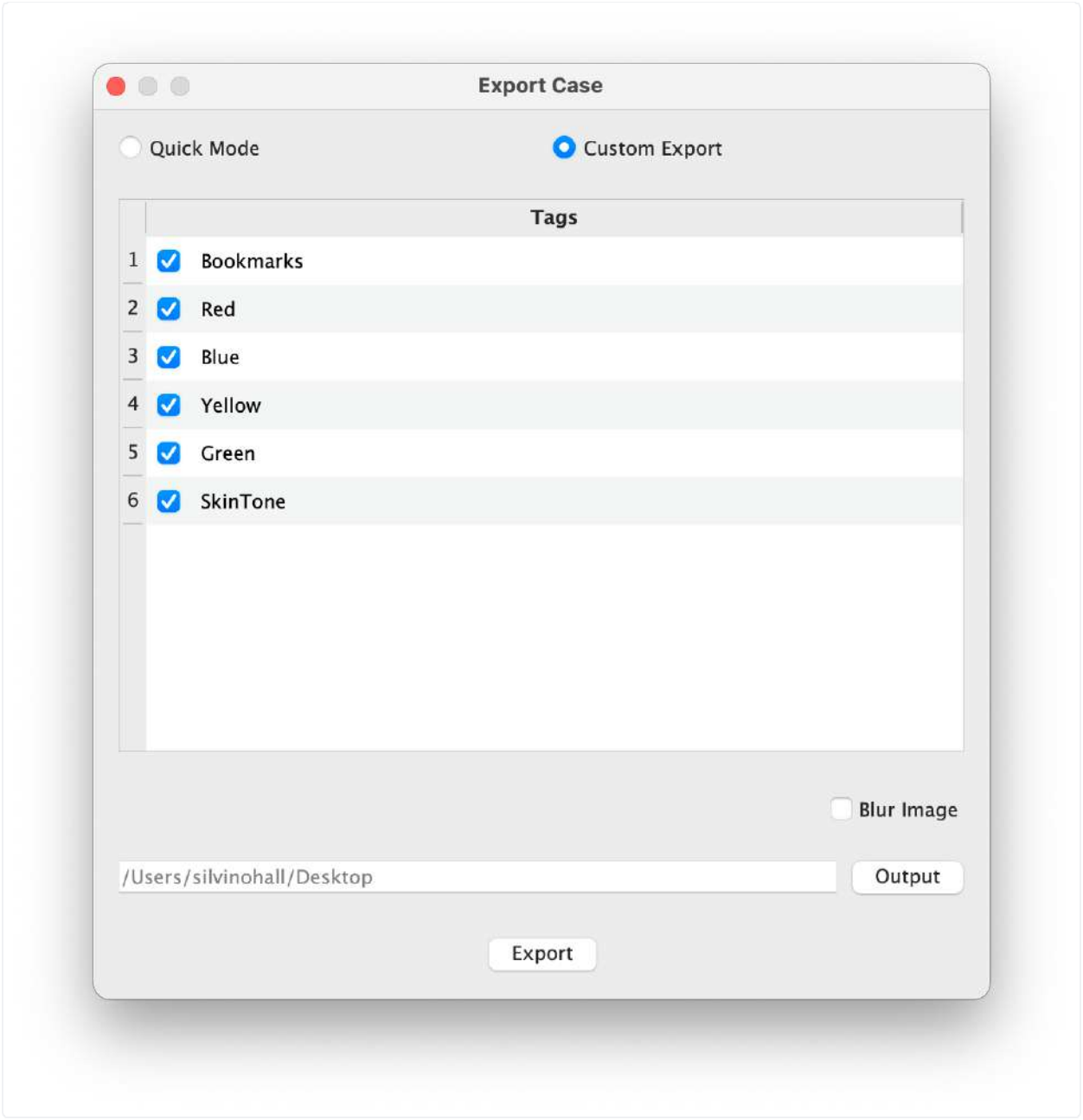


Note: Automated plugins need to be processed before exporting a case in Quick Mode. For more information about RECON LAB's automated plugins, see Section 9.2.

34.1.3 Custom Mode

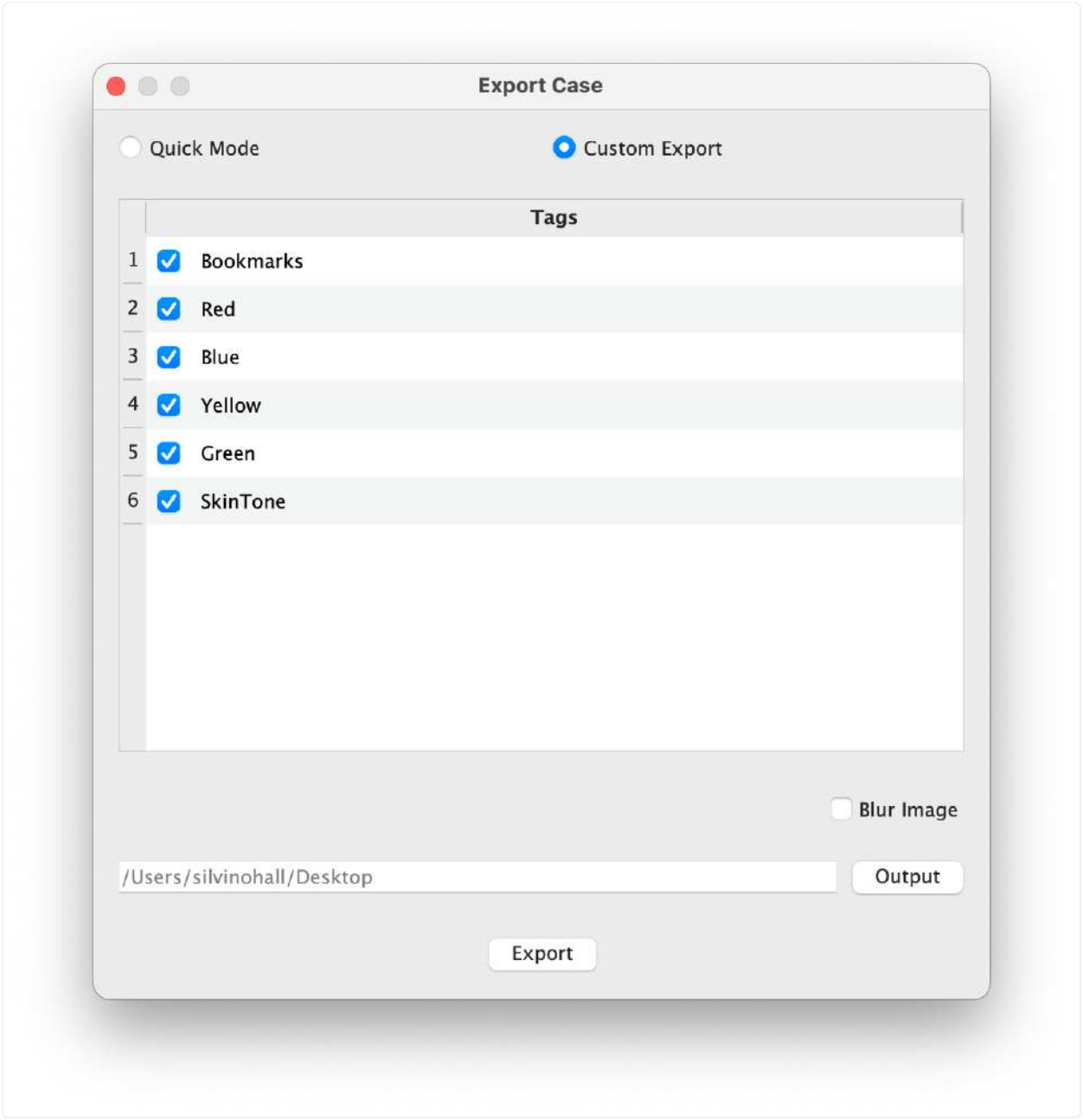
In **Custom Mode**, select the specific data marked by tags and bookmarks to export and analyze in RECON CASE READER.

For more information on bookmarking and tagging, see Section 17

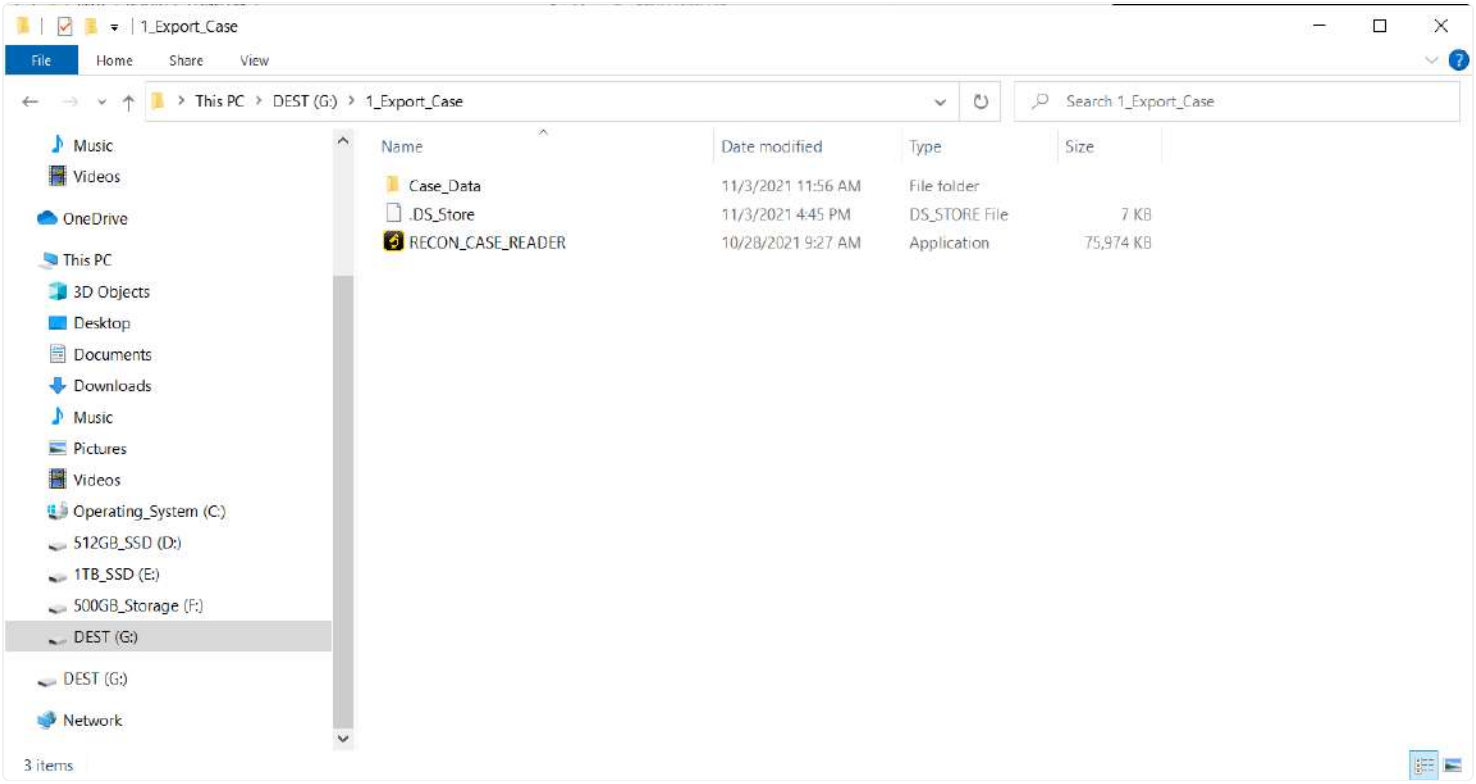


34.1.4 Exported Case Output

Select the desired **Output** directory to export the case, and click **Export**.



The case will output to a folder named **Export_Case** in the selected directory and will include a **RECON_CASE_READER.exe** and a **Case_Data** Folder.



35. CASE Reader

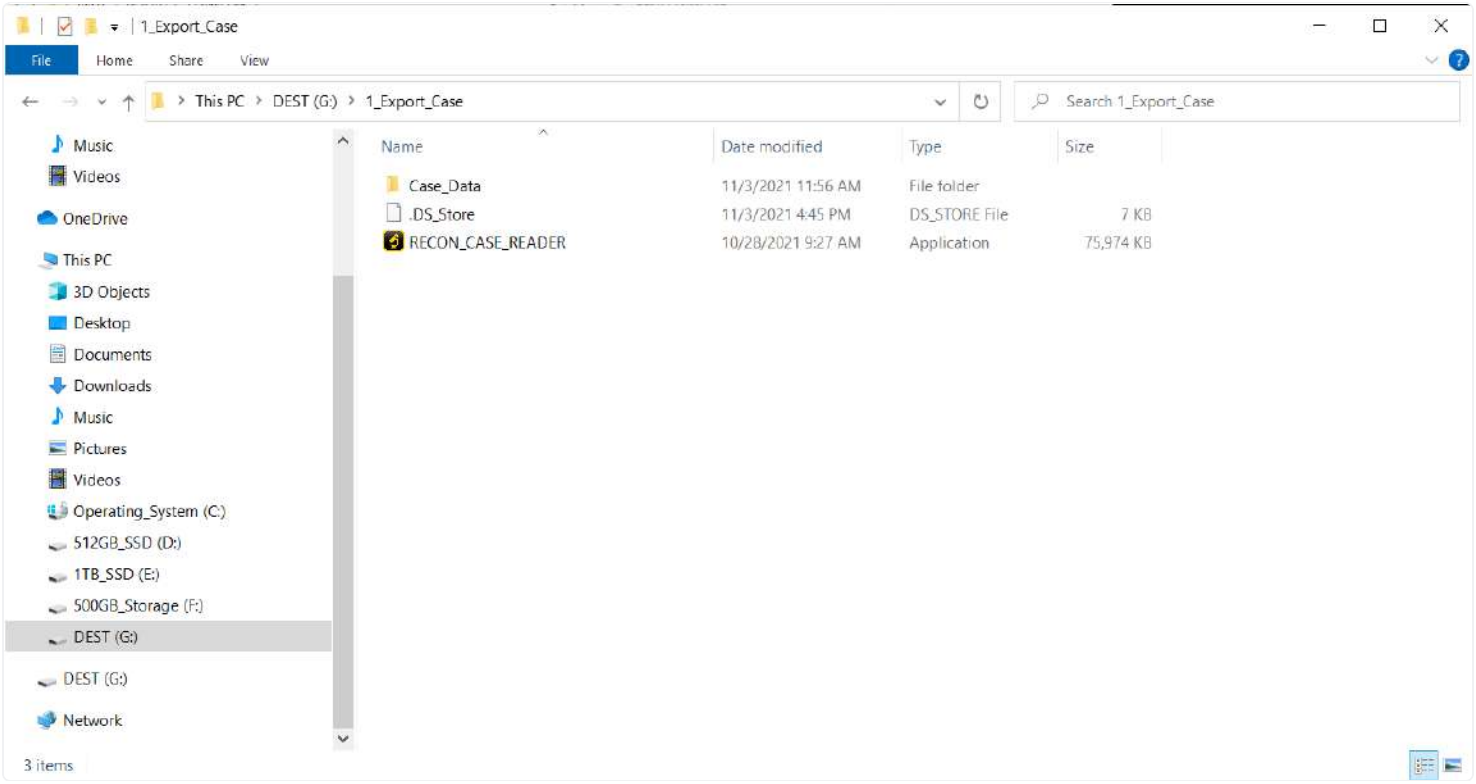
The RECON_CASE_READER.exe is included every time a case is exported. The executable is used to install the RECON LAB Case Reader application onto a Windows machine. The application only needs to be installed one time. After installation, any exported case can be loaded into the RECON LAB Case Reader.

35.1 Minimum System Requirements

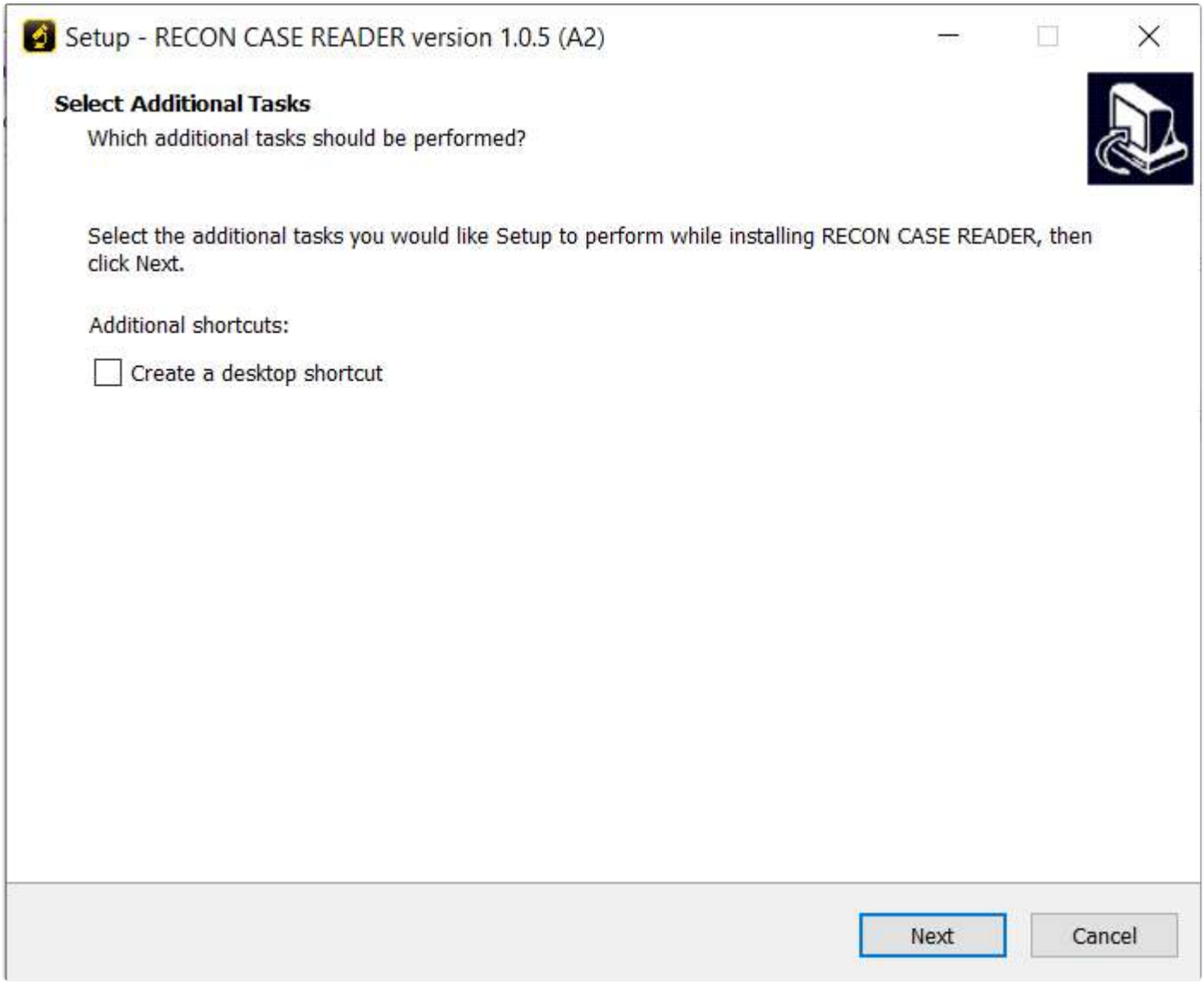
Windows 10 with Intel i5 processor with 8GB of RAM.

35.2 Installation

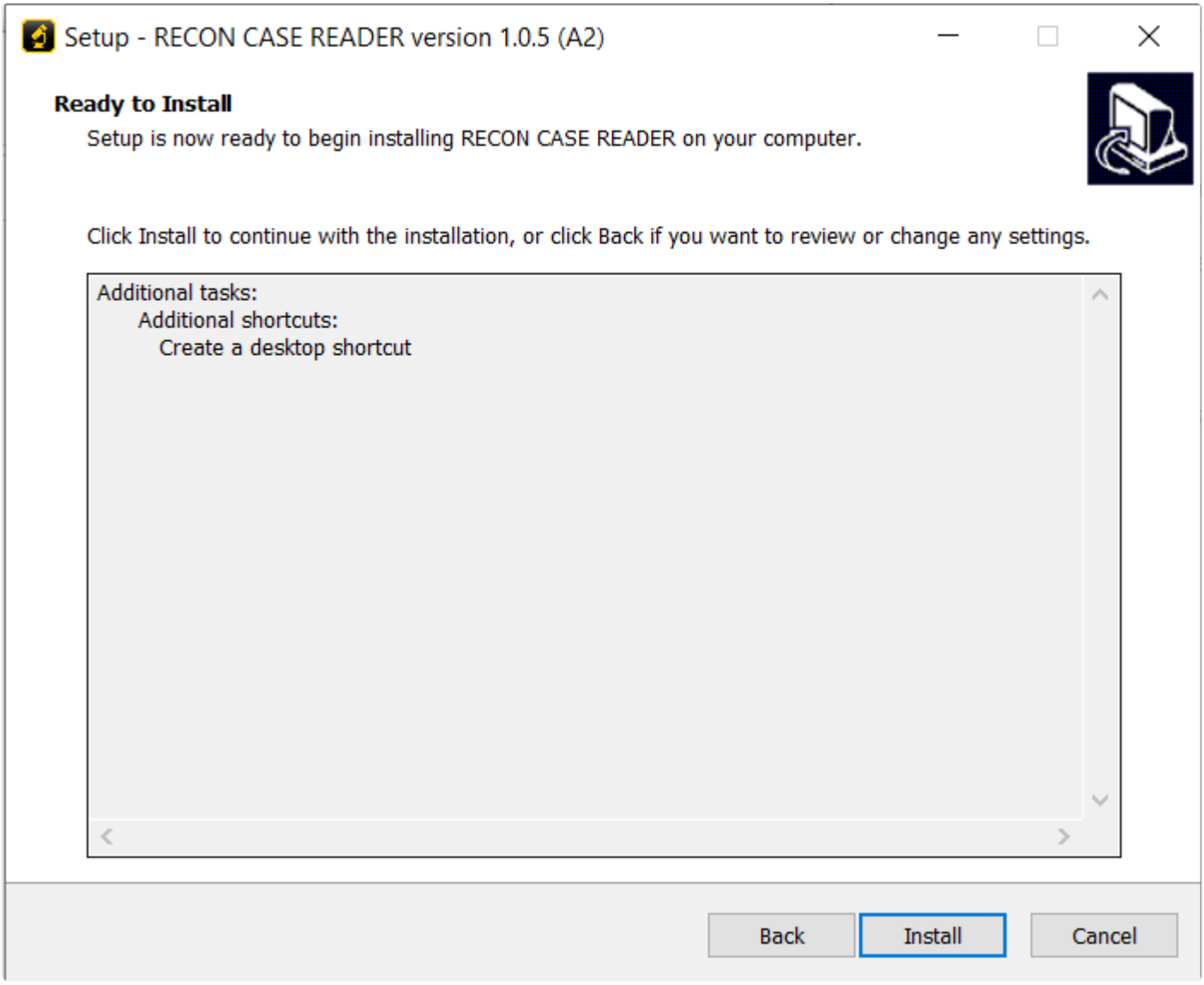
To install the RECON CASE Reader double click on the RECON_CASE_READER.exe. Windows may ask to allow the application to make changes to your device. If so, select yes.



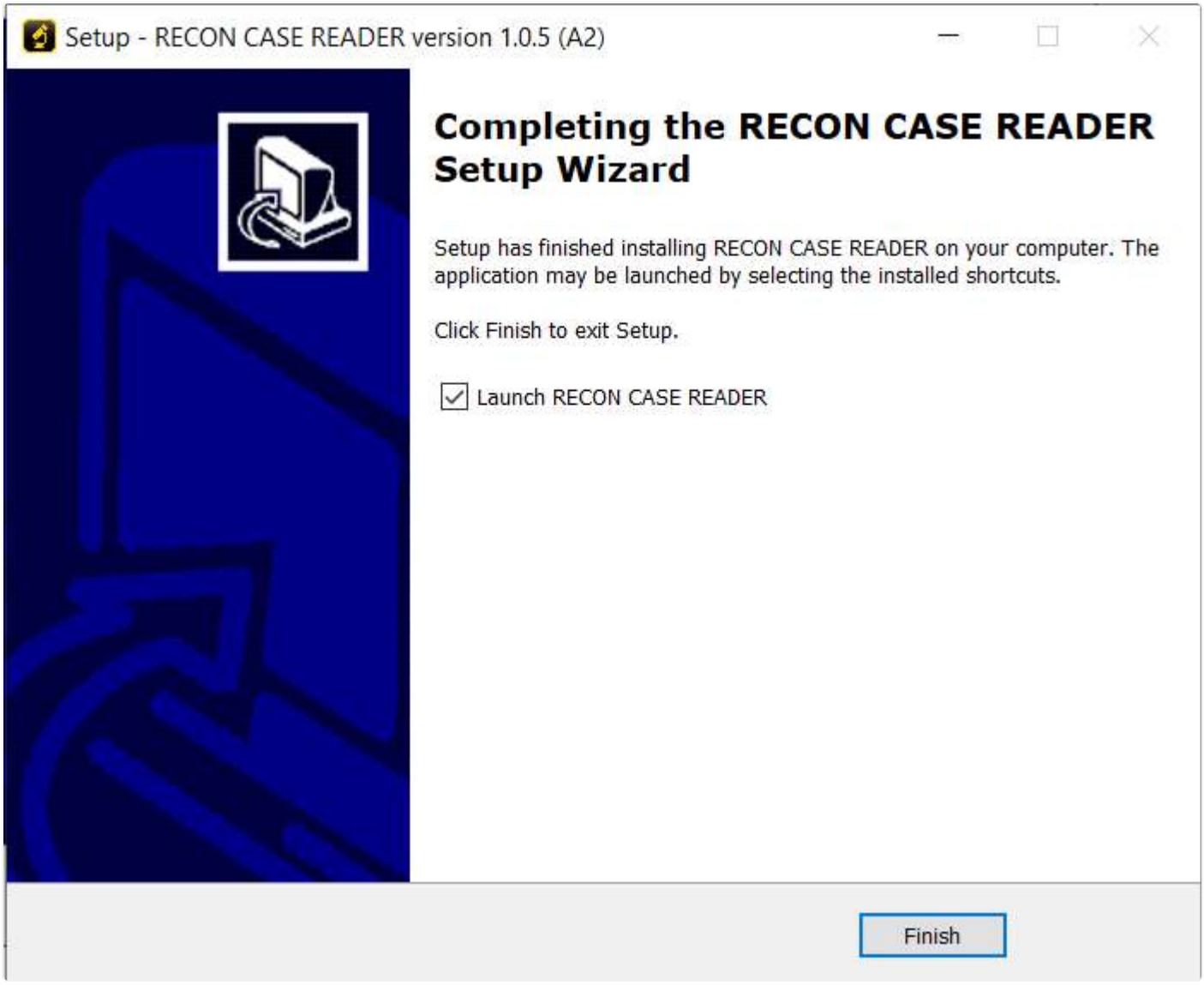
The next step in the installation will ask if the examiner wants to create an additional desktop shortcut on the user's desktop. Check the box to add a desktop shortcut or uncheck it to not add one.



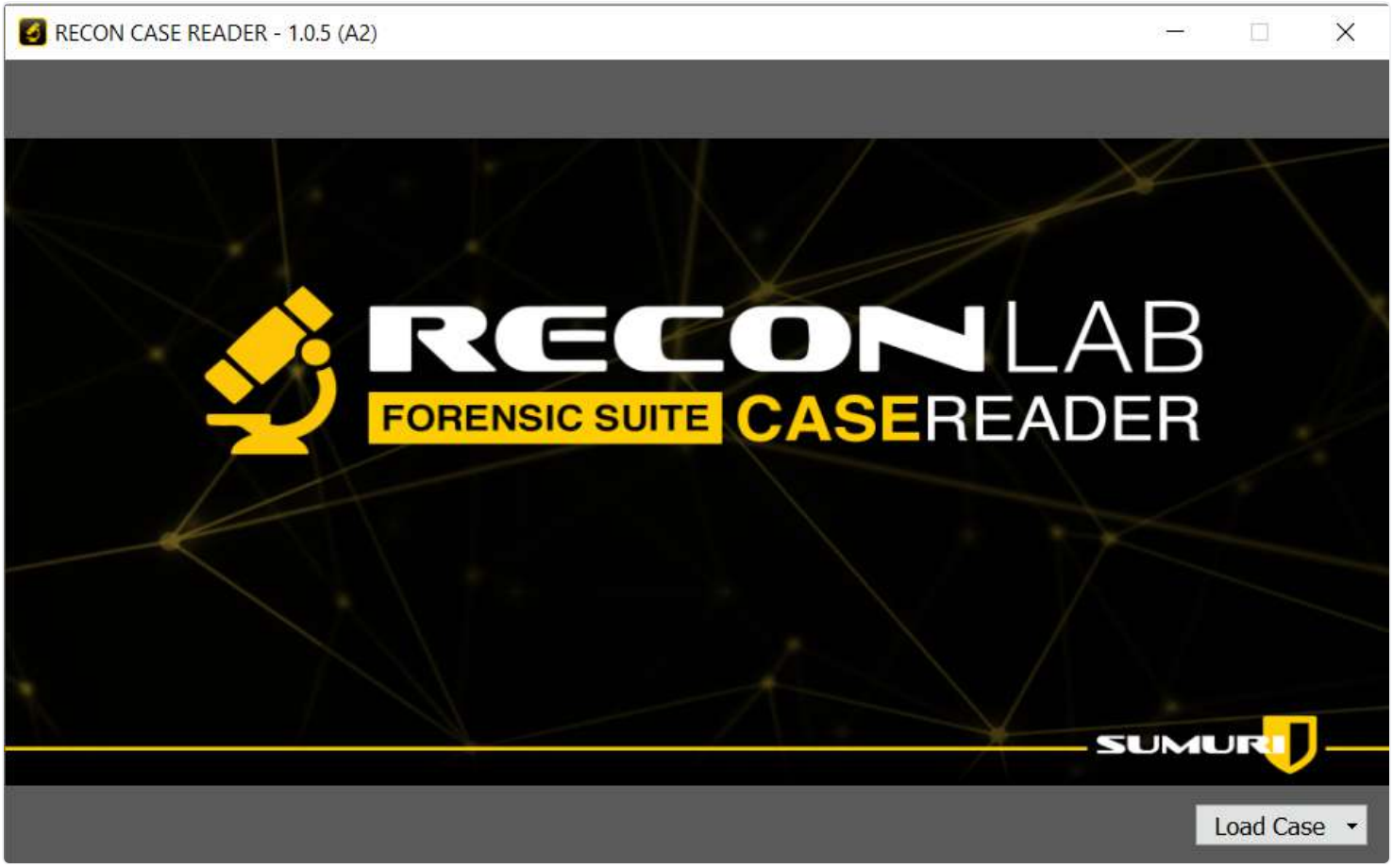
Click Install to begin installing RECON CASE. The default installation path is C:\Program Files (x86)> RECON CASE READER



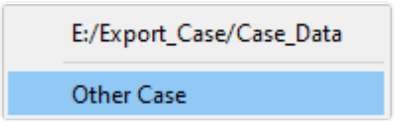
Click Finish to complete the installation. Keeping the Launch RECON CASE READER box checked will automatically launch the RECON CASE READER once the installation is complete.



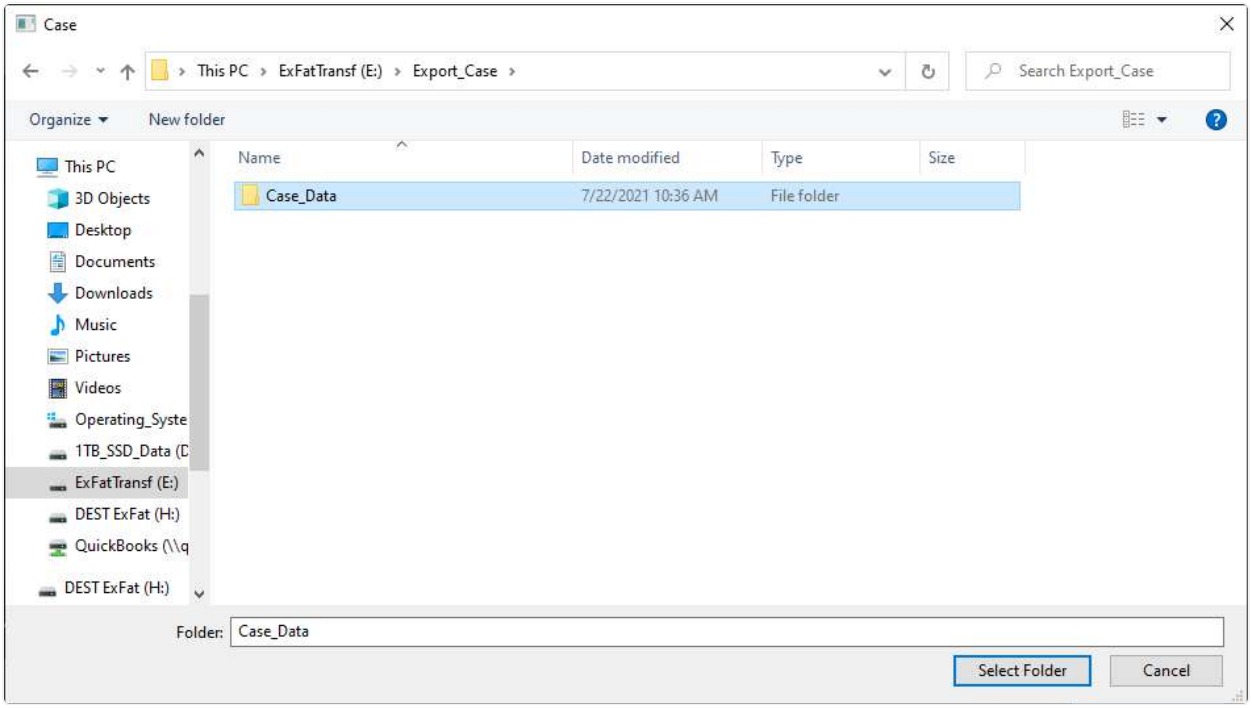
35.3 Loading a case



The RECON CASE READER splash screen gives the examiner the option to load any case that is exported from RECON LAB. Clicking **Load Case** will give the option to select previously loaded cases or **Other Case**.



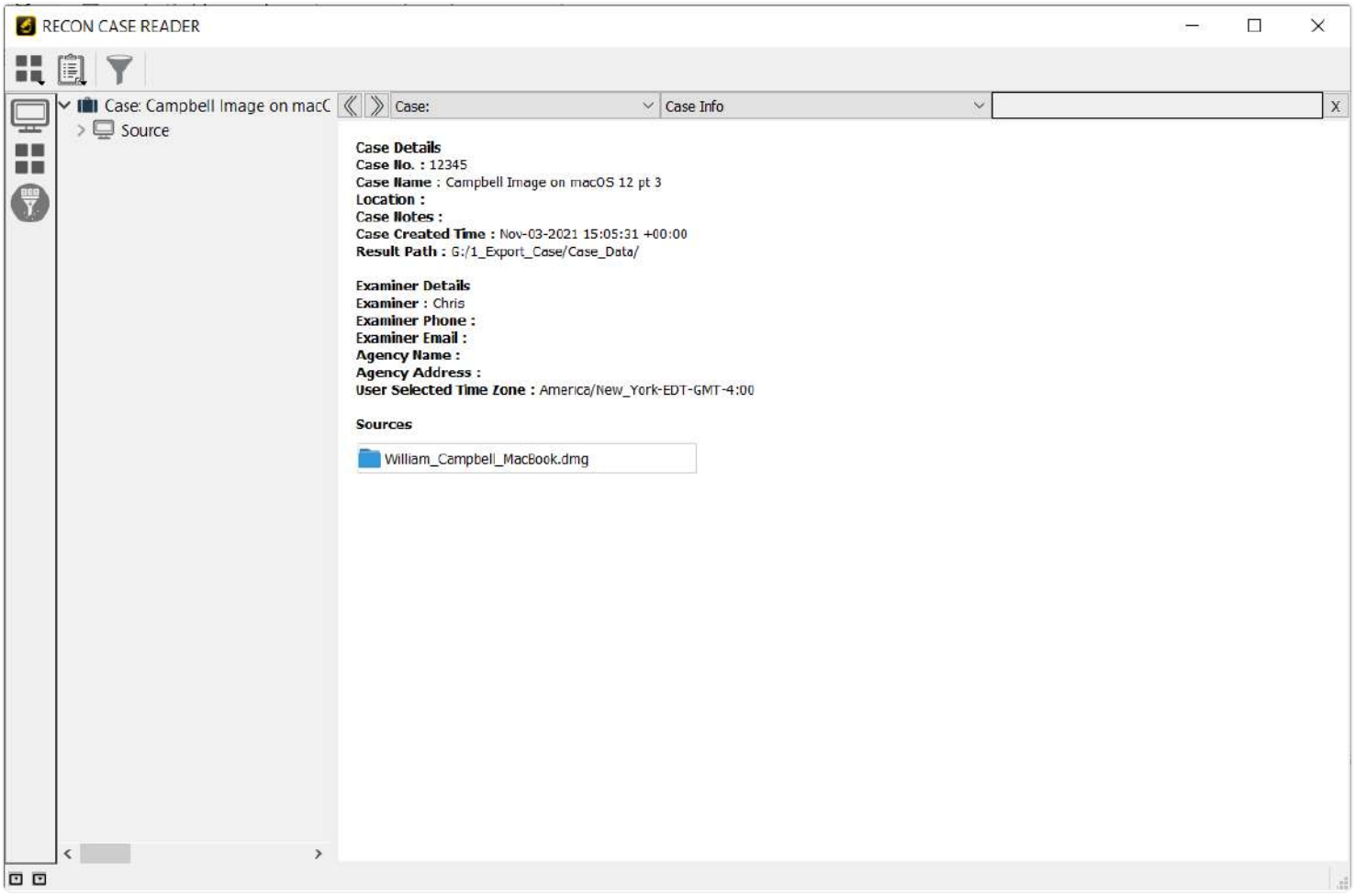
Other Case will open a File Explorer window where examiners can navigate to exported RECON LAB case folders. Exported case folders are named Case_Data by default.



Once a case folder or previously loaded case is selected RECON CASE READER will begin to load results.

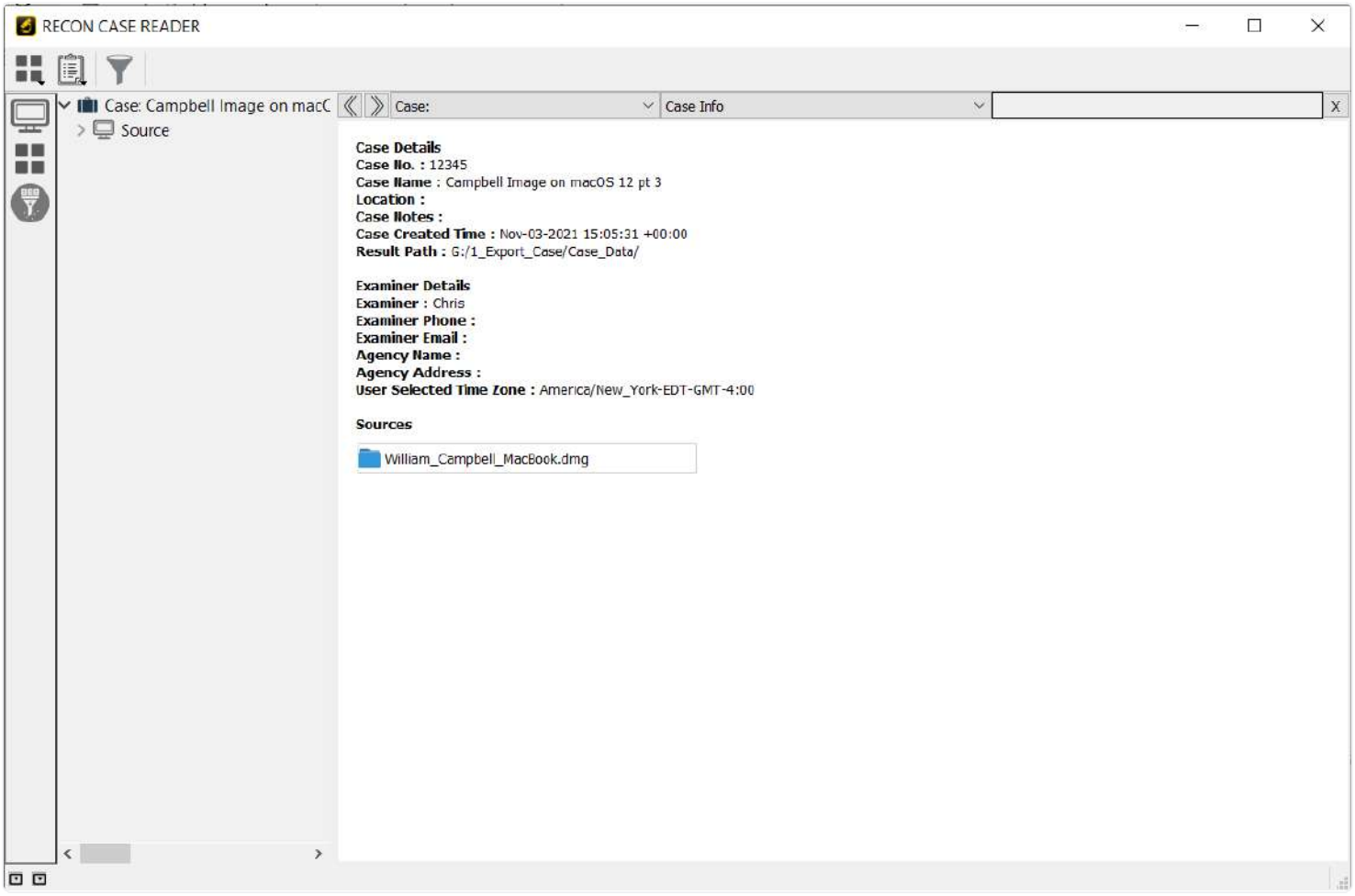
35.4 RECON CASE Reader Interface

The RECON CASE Reader interface is designed to mirror RECON LAB's simple and intuitive design. Many features in the RECON CASE READER function the same way as they do in RECON LAB.



35.5 Case View

Once a case is loaded examiners will be greeted with the Case View Screen. The Case View screen can also be accessed by clicking the “briefcase” icon at the top of the sidebar



Case View displays information about the case including information about the case and the examiner. ***Note* This information is taken from RECON LAB at the time of the export and can not be changed.**

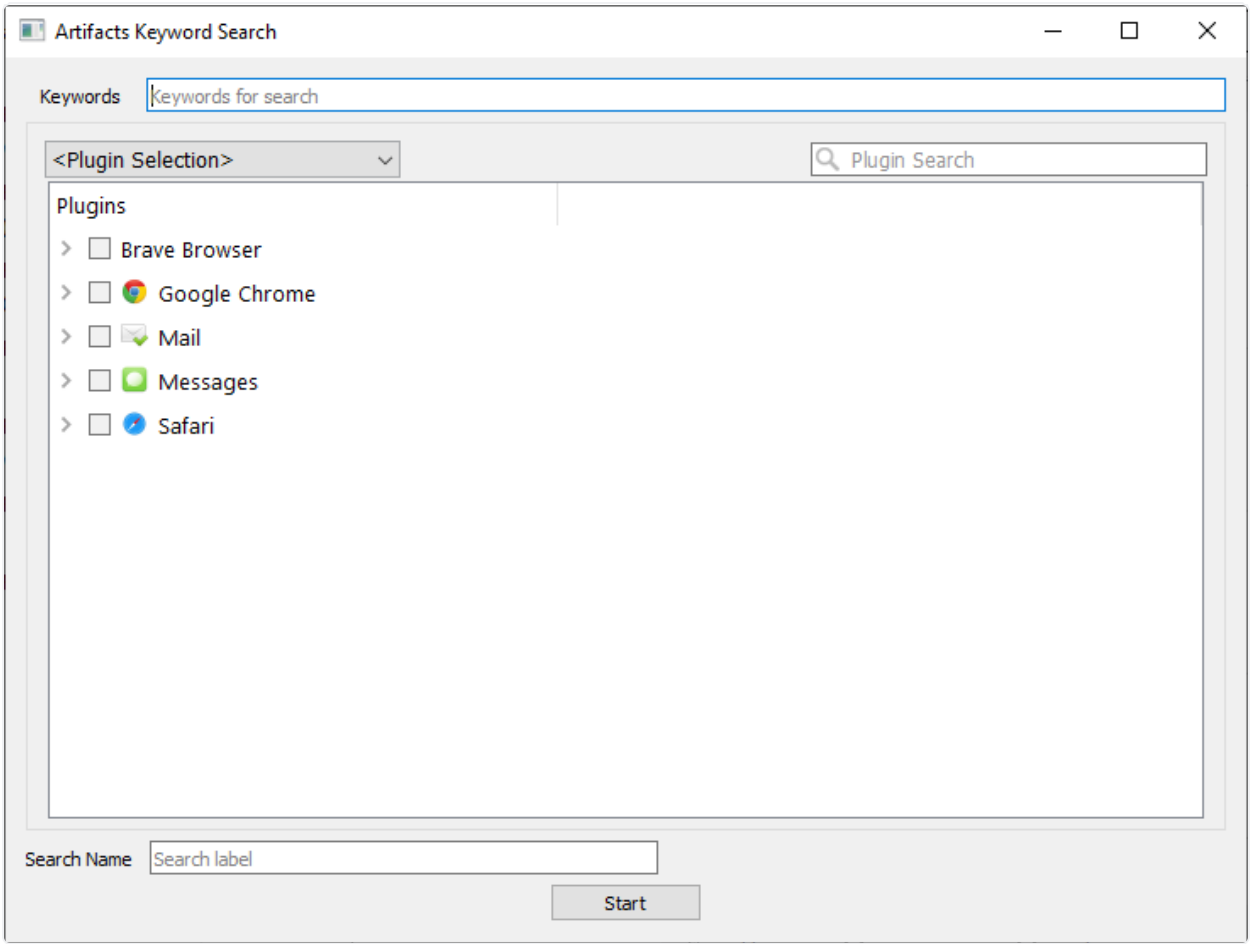
The Case Info screen displays the sources used when exporting the case. More information about each source can be found by clicking on the name of the source.

35.6 Top Menu

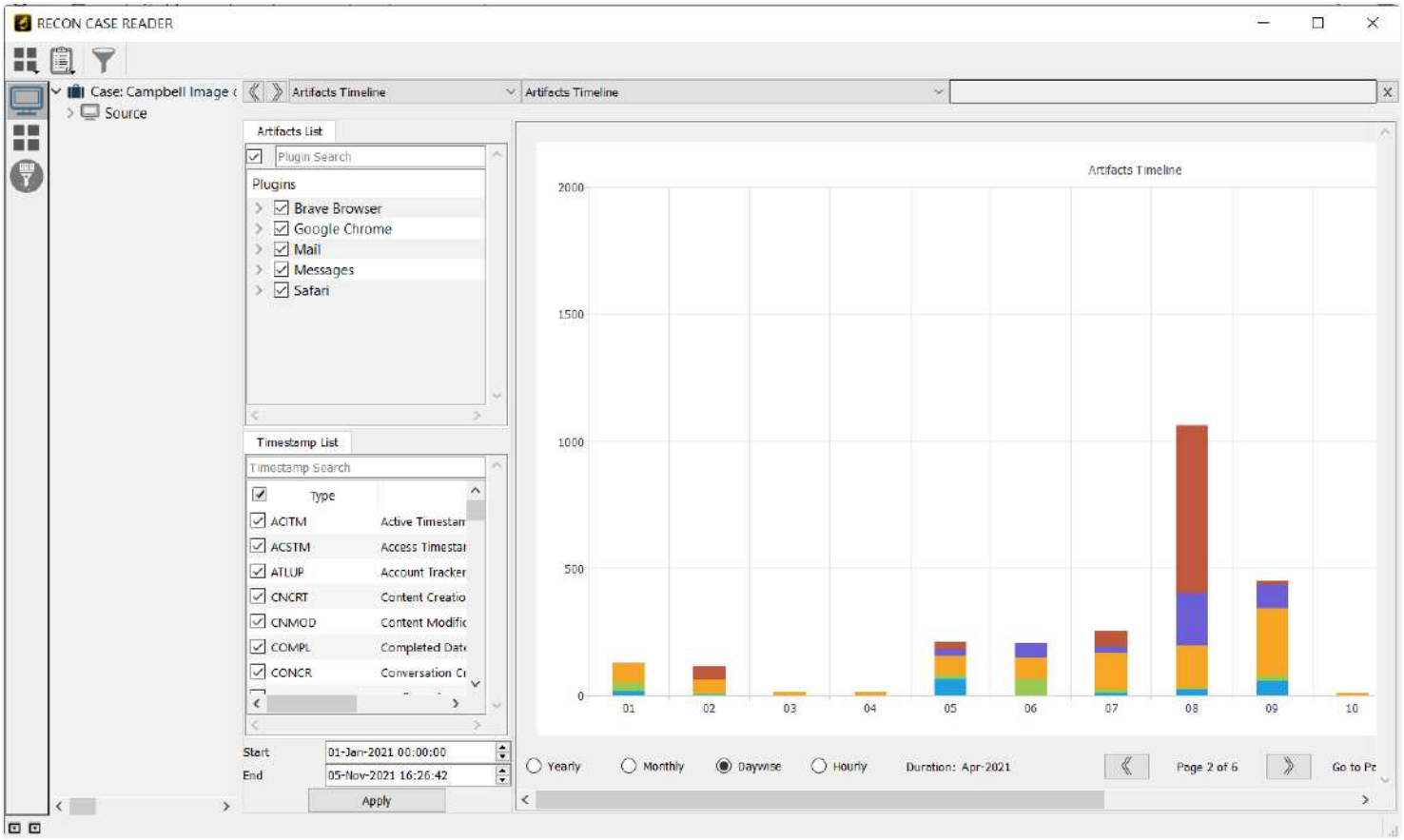
RECON CASE Readers Top Menu has 3 buttons two of which have sub-menus.

Artifacts - contains the “Search Artifacts” and “Artifact Timeline” sub-menus

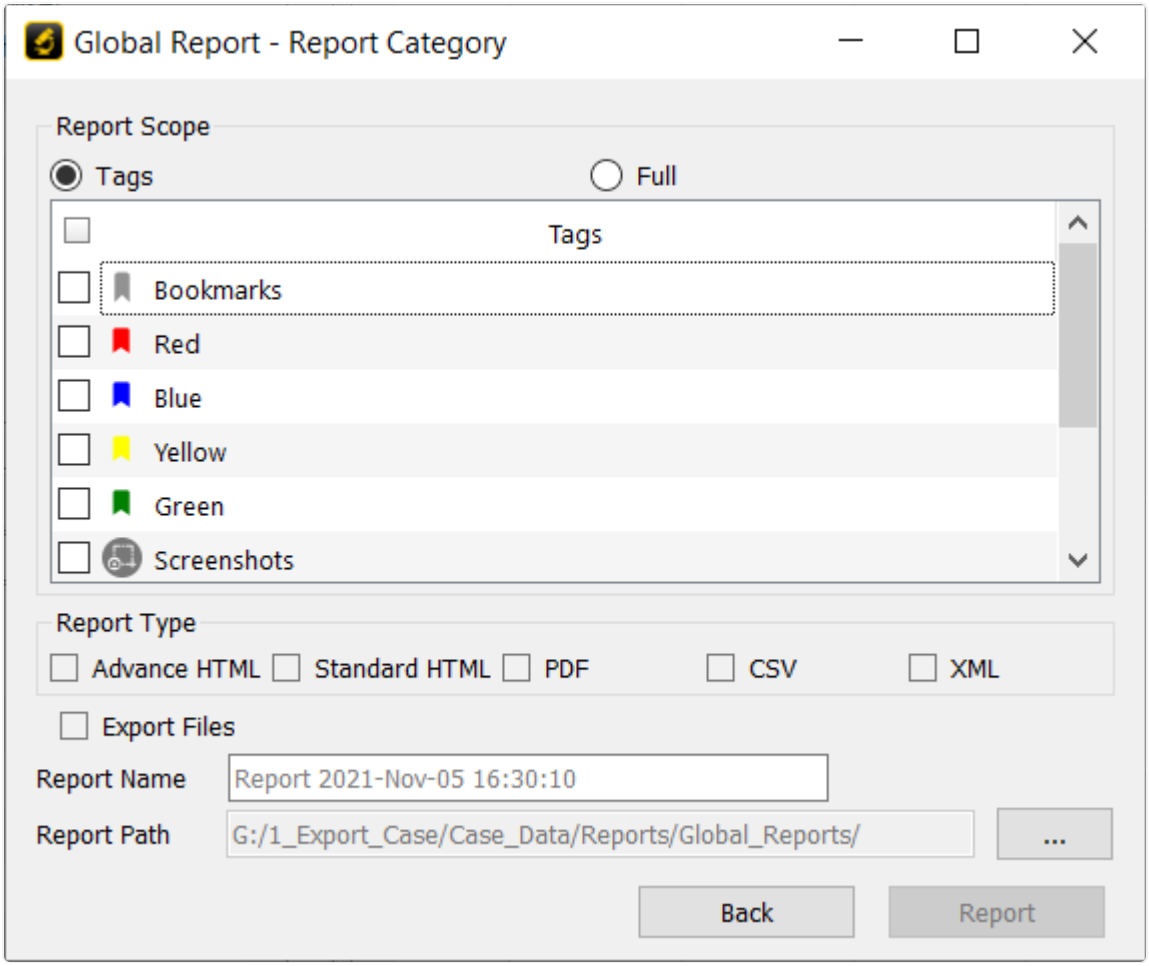
Search Artifacts - allows the examiner to conduct a single keyword search quickly within all exported artifacts. Section 19.1 has more information about Artifact Keyword searching.



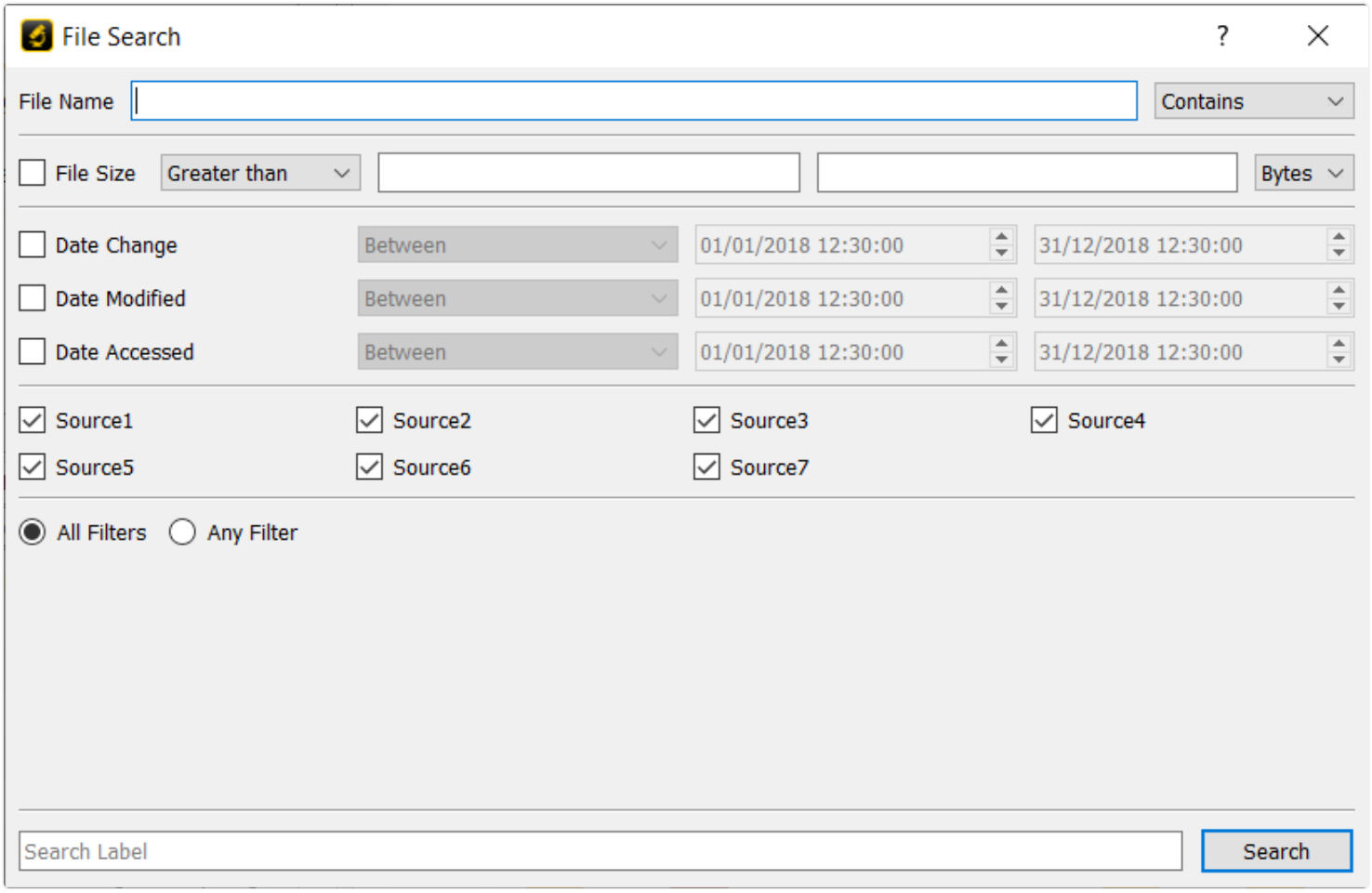
Artifacts Timeline - Opens the Artifacts Timeline module used for generating timelines and graphs for timestamps recovered from the exported Artifacts and Plugins module. Section 27.2 has more information on Artifacts Timeline.



1. **Generate Report - contains the “Automated Report” menu**
    a. **Automated Report - automatically generates reports from bookmarks or plugins. Section 32.2 has more information about Global Reports**



a. **File Search - Allows for locating files based on a combination of timestamps, file names, extensions, file sizes, and more. Section 19.2 has detailed information about File Search.**

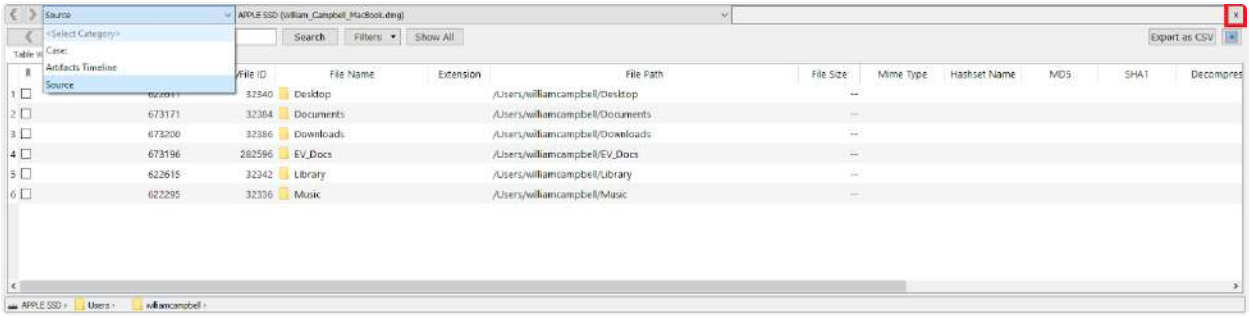


35.6 Main Columns

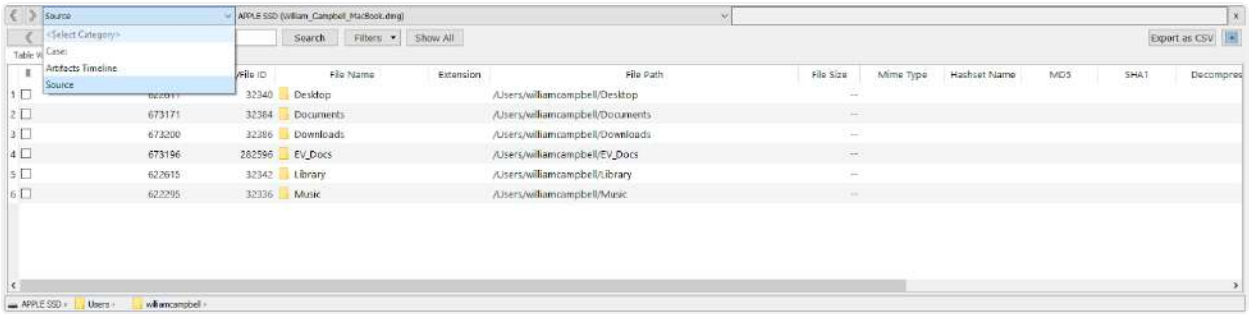
There are two main columns at the top of the Main Window for the RECON CASE READER. These columns can be used for quick navigation.

When you navigate to different modules or views these columns will keep a history of these. Clicking on the columns will allow you to return to a previous module or view.

Views or modules can be removed by selecting the “X” button.

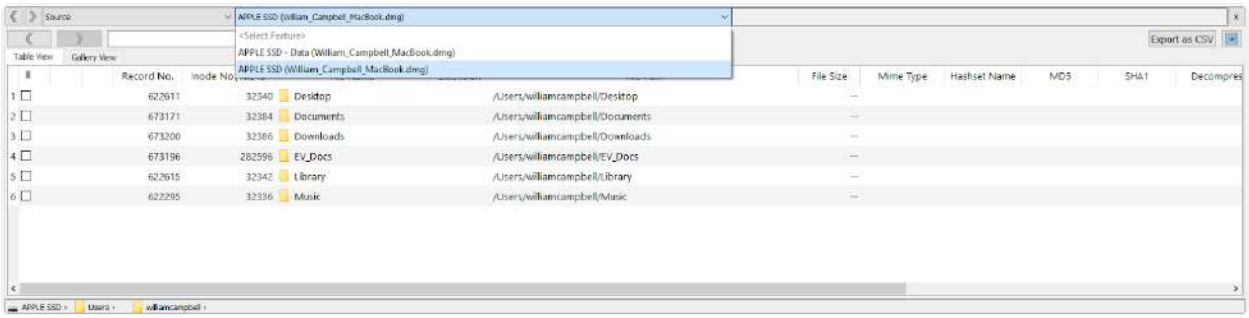


Select Category Column



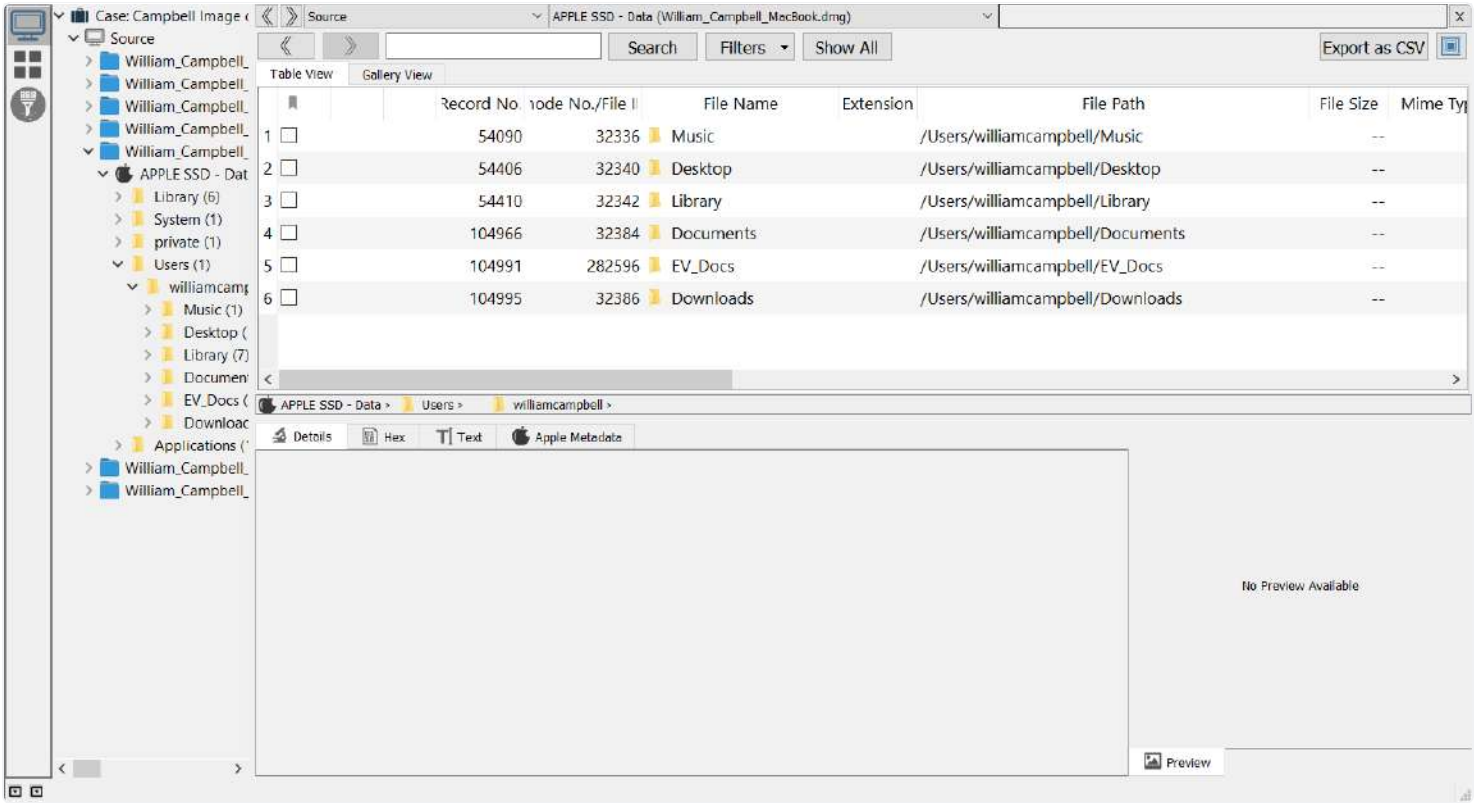
The Select Category Column keeps a history of modules and sources previously viewed. Clicking the title of the column will show previous items. Select any item to return to the module or source.

Select Feature Column



The Select Feature Column keeps a history of different windows viewed. Clicking the title of the column will show previous items. Select any item to return to a previous window.

35.7 Case Sidebar



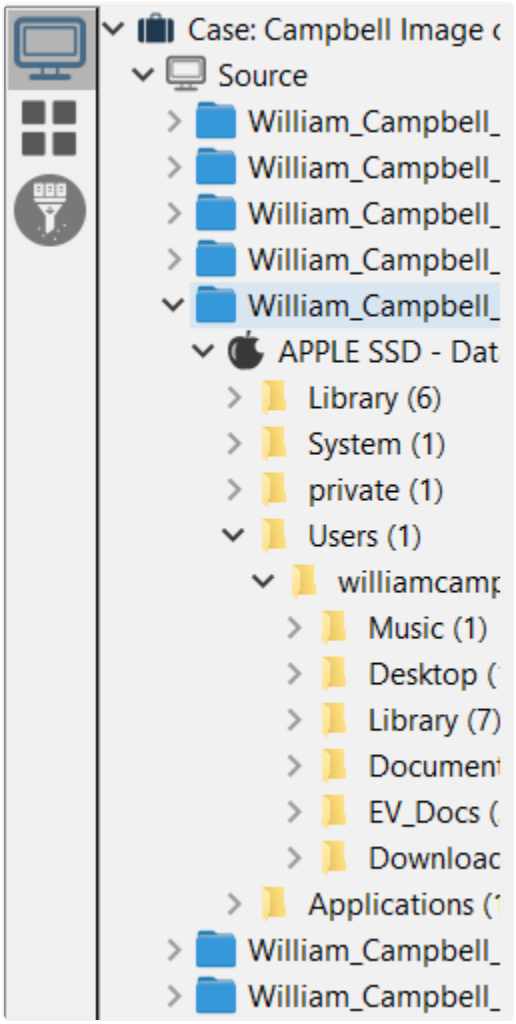
The sidebar is used to quickly access data found from processing and analysis. It can also be used to manually navigate through the exported source data.

Clicking the dropdown arrow next to a category or directory will expand it.

The case sidebar is broken up into three sections.

1. **Source - Displays the exported data allowing for manual review and analysis.**
2. **Artifacts - Displays data parsed from artifacts at the time of export as well as artifact keyword search results and artifact timeline results**
3. **File Filters - Displays information about file types and File Search results**

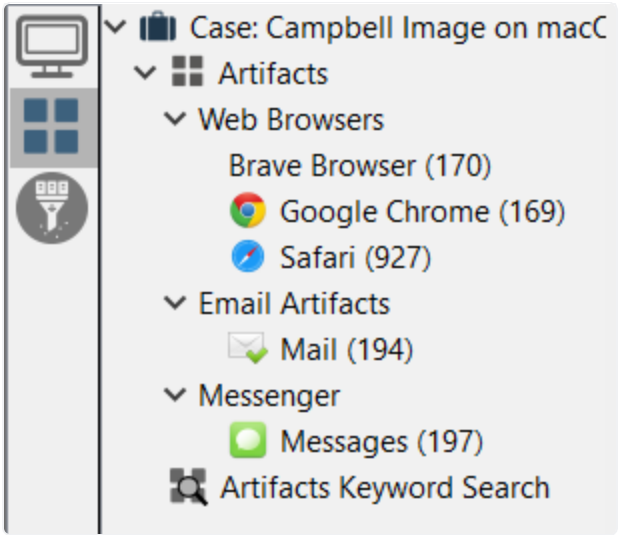
35.7.1 Source Tab

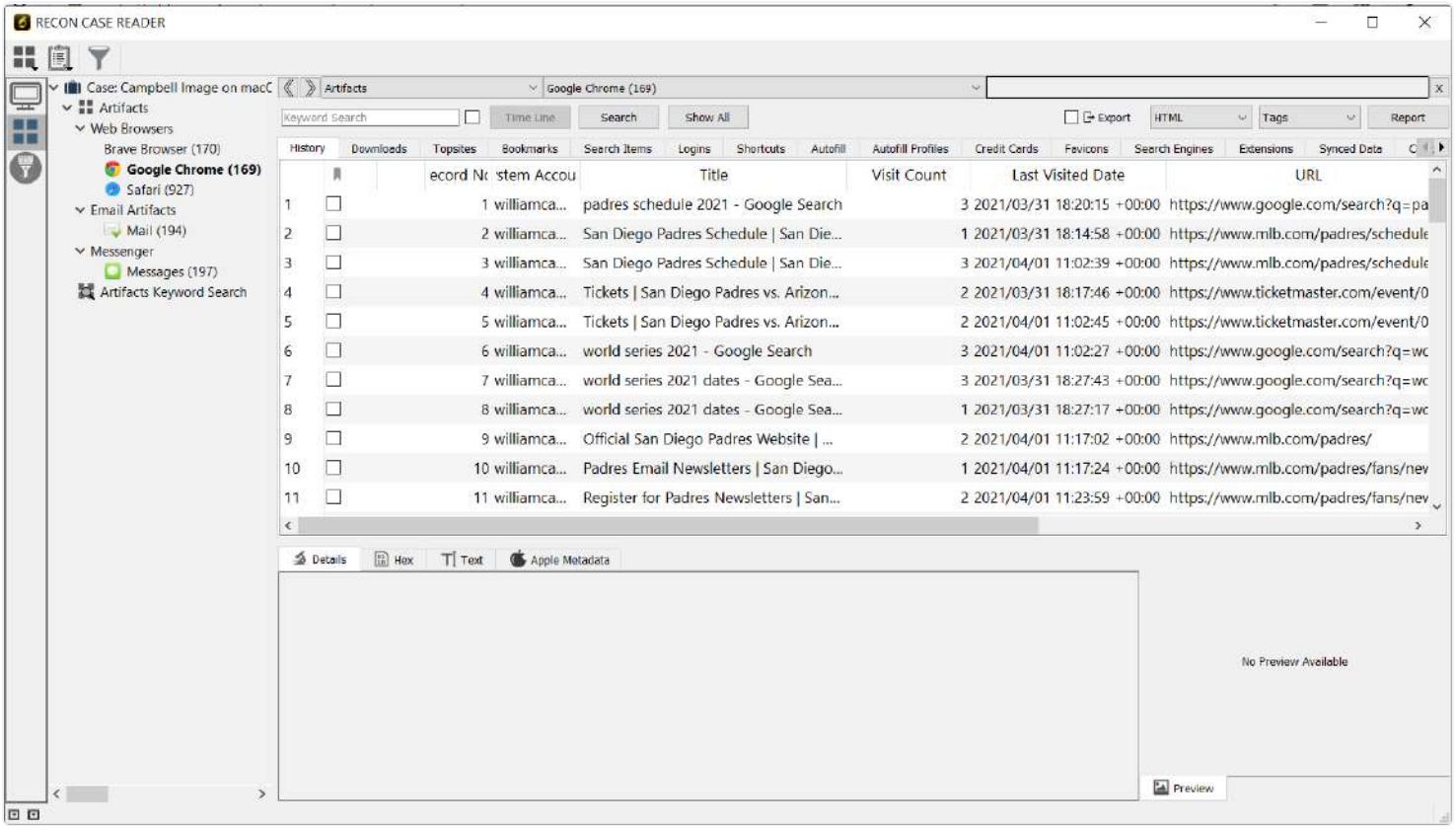


The source tab shows the exported files in a directory structure. Examiners can easily manually navigate through the directories of the exported data.

35.7.2 Artifacts Tab

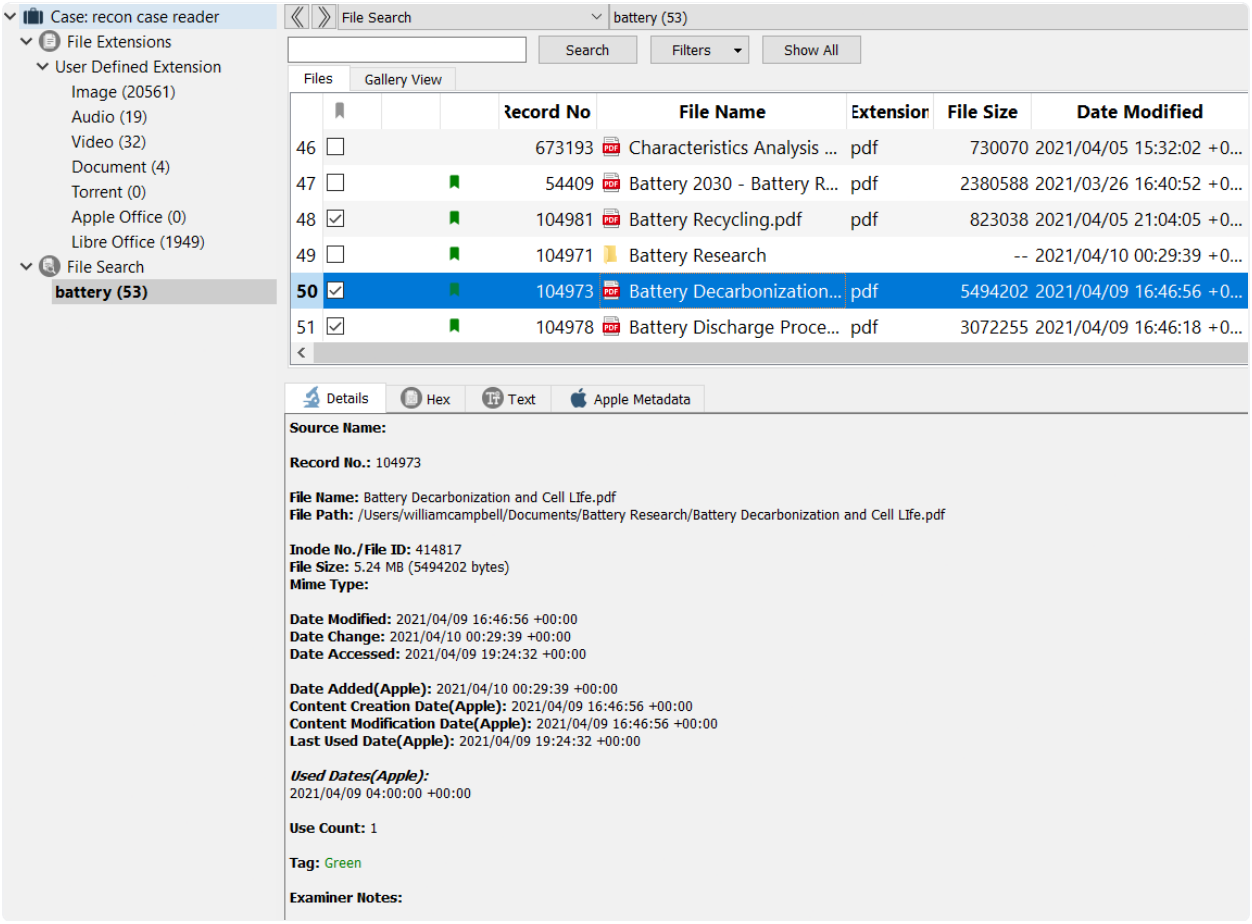
The artifacts tab displays information from exported artifacts along with the results from Artifact Keyword searches and Artifact Timelines.





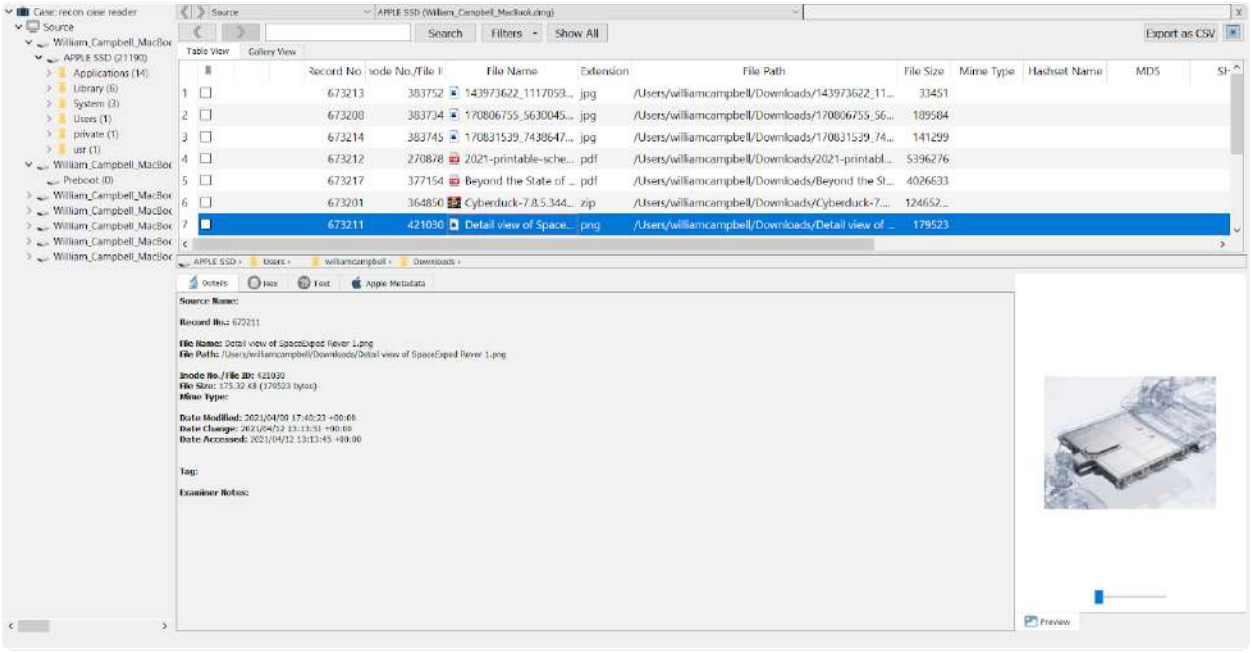
35.7.3 File Filters

The File Filters tab contains data relating to file extensions and results from file searches. Files will be sorted by extensions or categorized by searched keywords.



35.8 Main Viewer Window

The RECON CASE Reader main view is designed to mirror the interface of RECON LAB. See section 12.6-12.8 for more information about the main view, covering the Details, Hex Viewer, Text Viewer, Apple Metadata, and more.



36. Importing your Case into RECON LAB

Case folders exported and analyzed in RECON CASE READER can be loaded back into RECON LAB for further analysis or more robust report generation.

Simply select to Load Case when starting RECON LAB and point to the case folder used in the RECON CASE READER.

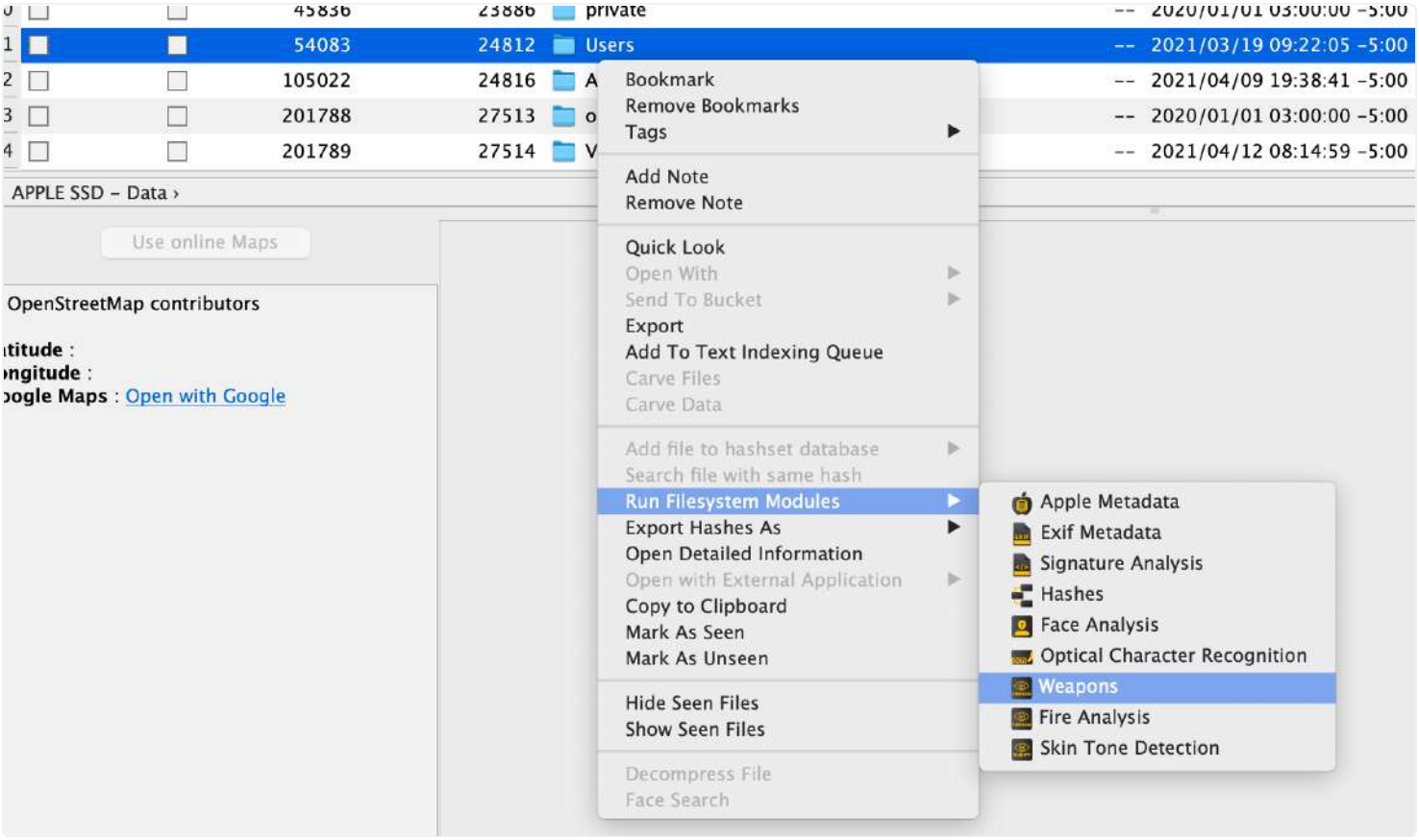
37. Weapon Analysis

The weapon analysis file system module allows RECON LAB to automatically identify and categorize pictures that have firearms in them. Pictures will be categorized as either Guns or Rifles and put into their own category.

37.1 Processing for Weapon Analysis

Weapon Analysis is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing

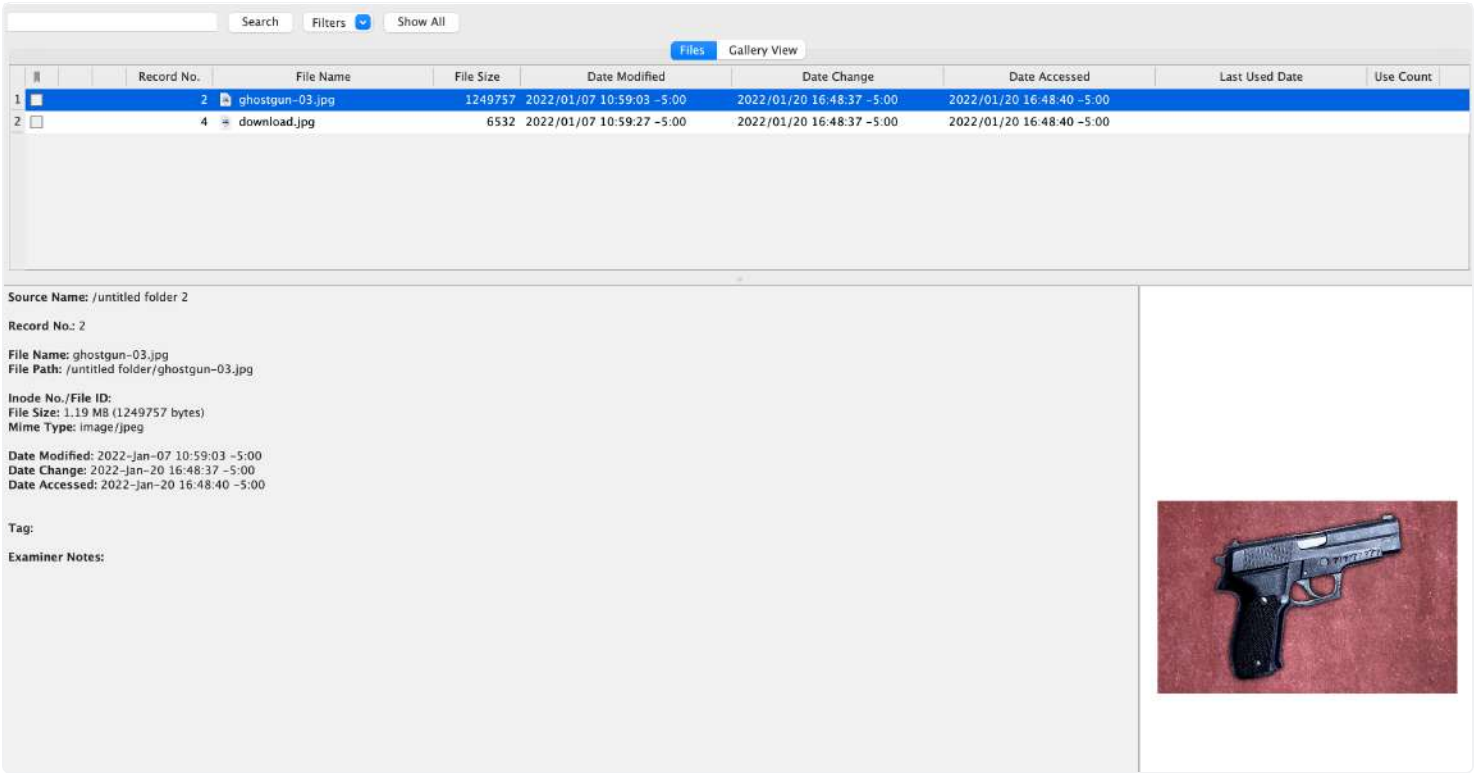
options including Weapon Analysis.



37.2 Weapon Analysis Results

Results for weapon analysis are put into their own category on the left menu. The results are broken into two subcategories of Guns or Rifles.

After selecting a category results are displayed in the main pane. Results can be viewed as either a list of files or in a gallery view.



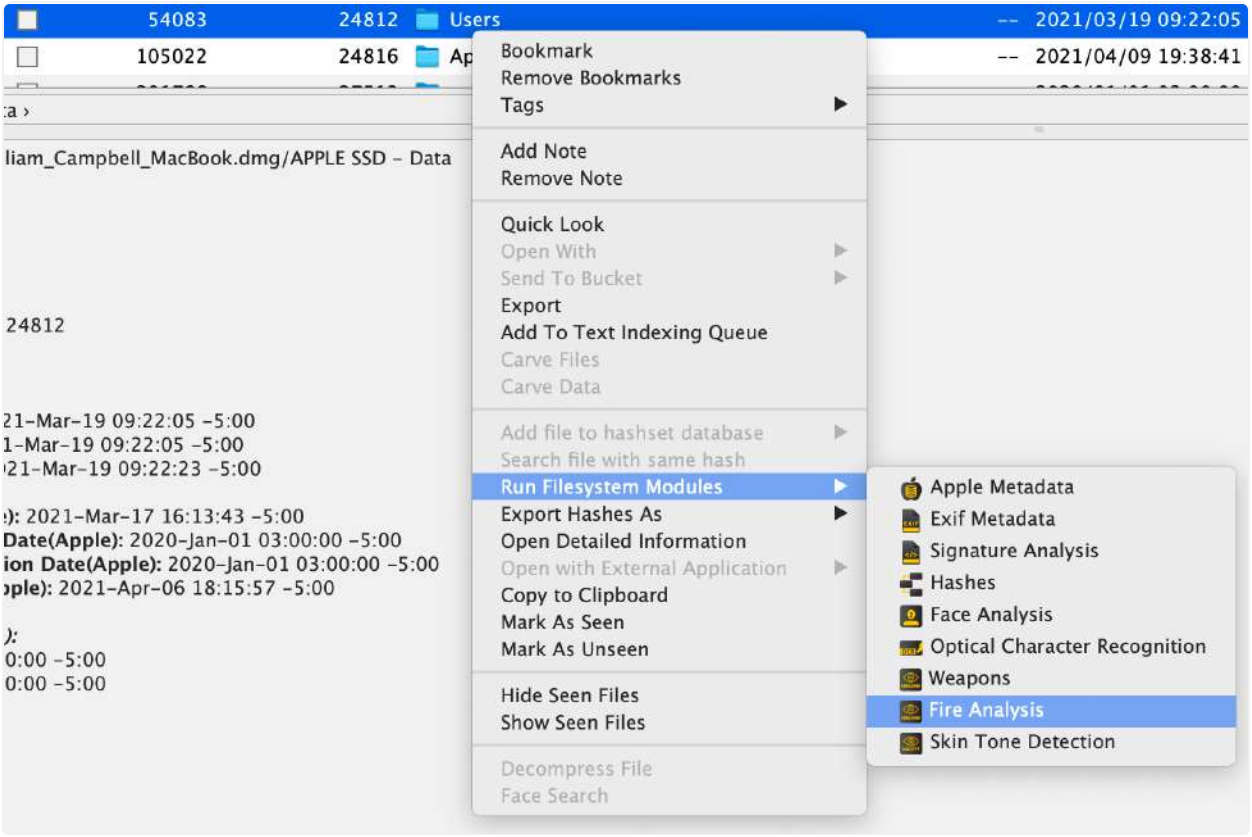
38. Fire Analysis

The Fire Analysis File System Module allows RECON LAB to automatically identify and categorize pictures that have fire in them. Detected pictures will be put into their own category for easy analysis.

38.1 Processing for Fire Analysis

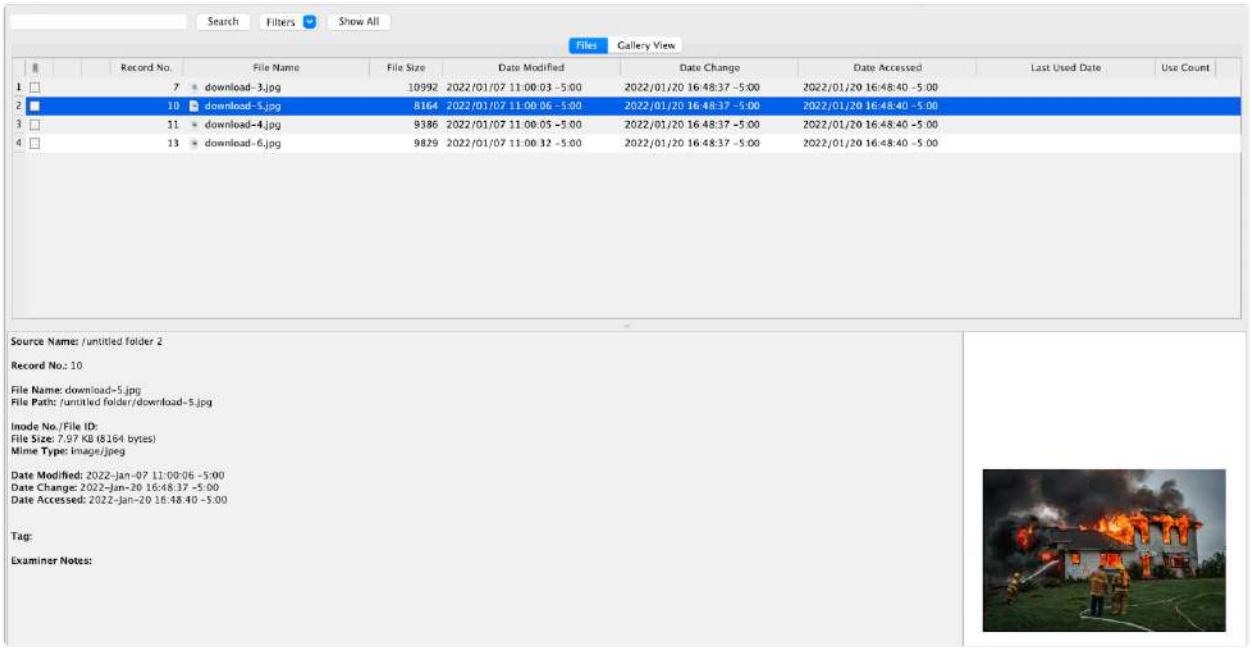
Fire Analysis is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing

options including Fire Analysis.



38.2 Fire Analysis Results

Results from Fire Analysis are displayed in their own category in the left menu. After selecting Fire Analysis results are displayed in the main pane and can be viewed in a file list or a gallery view



39. Skin Tone Detection

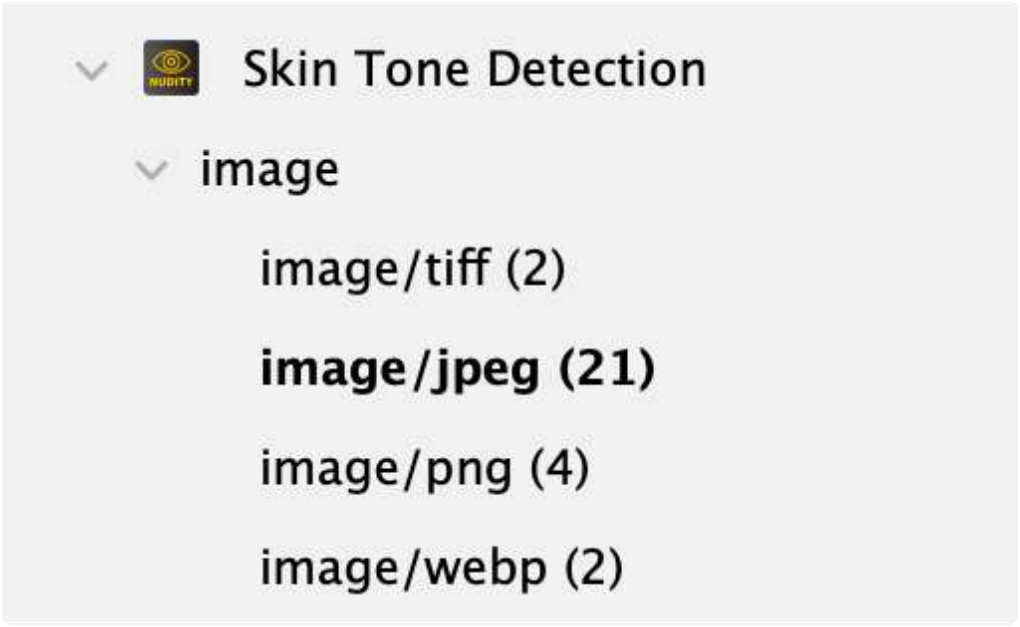
The Skin Tone Analysis File System Module allows RECON LAB to automatically identify and categorize pictures that have a detected skin tone in them. Detected pictures will be put into their own category for easy analysis.

39.1 Processing Skin Tone Detection

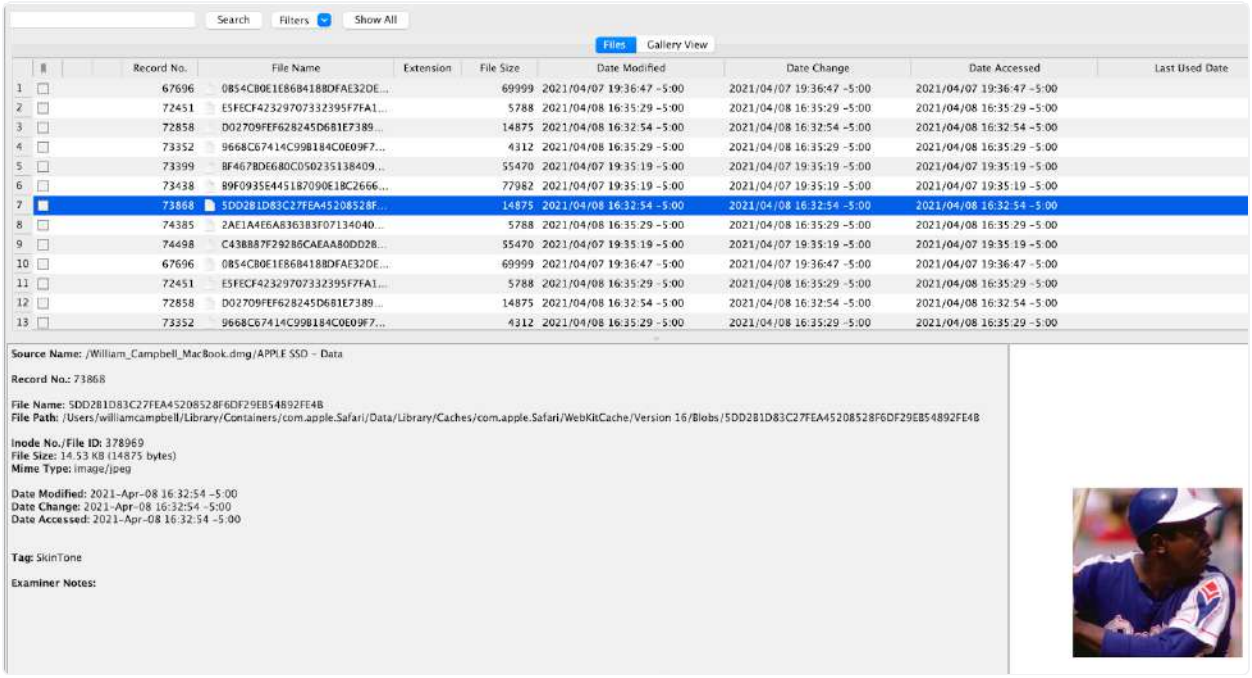
Skin Tone Analysis is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing options including Skin Tone Detection.

39.2 Skin Tone Detection Results

Results from Skin Tone Detection results are displayed in their own category in the left menu. After selecting Skin Tone Detection results are split into different file types.



After selecting a file type results are displayed in the main pane and can be viewed in a file list or a gallery view.



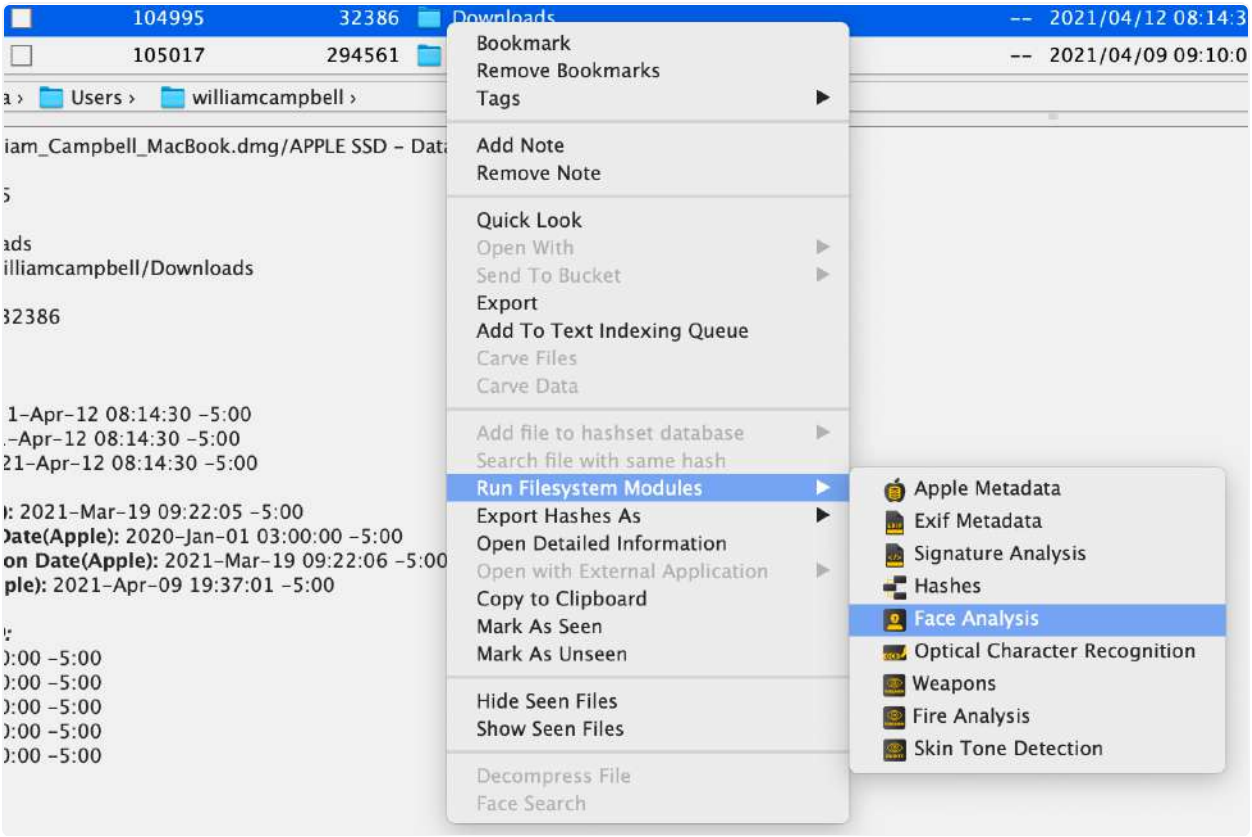
40. Face Analysis

The Face Analysis File System Module allows RECON LAB to automatically identify and categorize pictures that have a detected face in them. Detected pictures will be put into their own category

for easy analysis. After faces are identified examiners can then search for faces using the Face Search Feature.

40.1 Processing for Face Analysis

Face Analysis is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing options including Face Analysis.

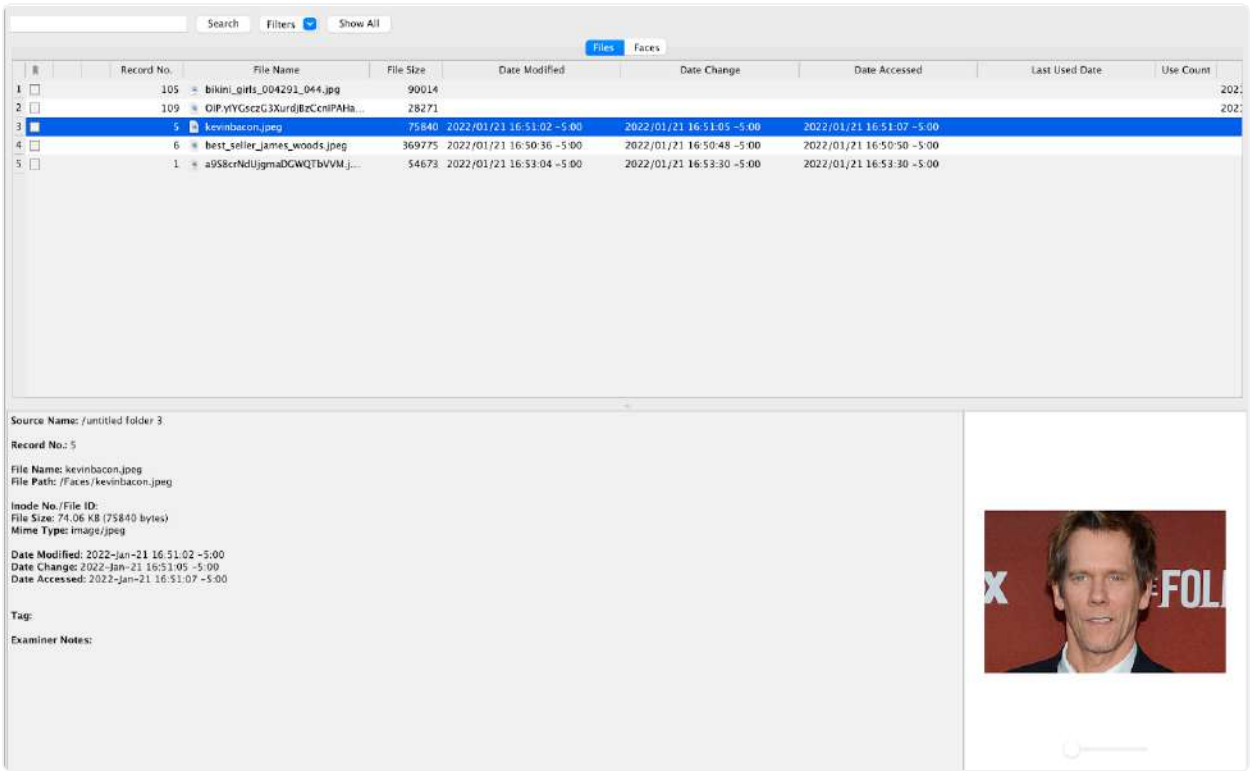


Note Faces must be indexed using the Face Analysis Feature before the Face Search Feature can be used.

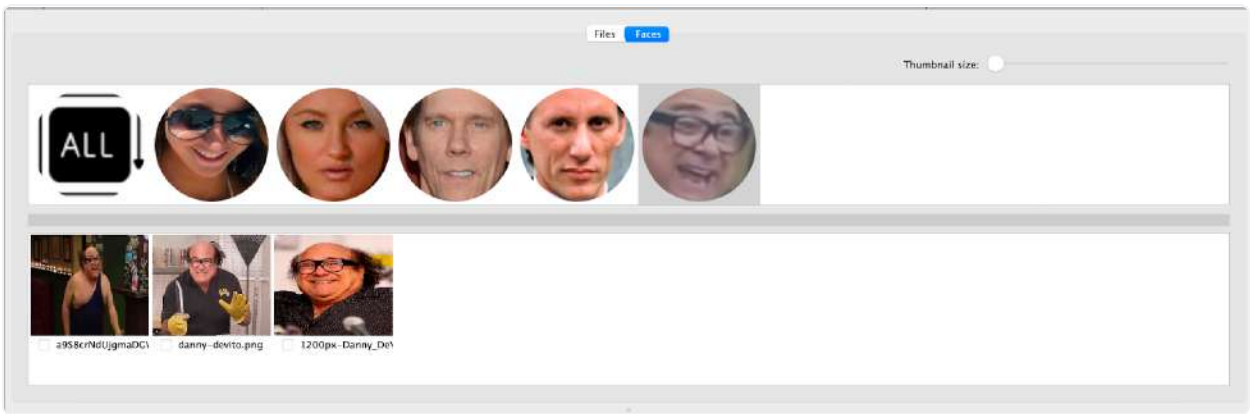
40.2 Face Analysis Results

Results from Face Search are displayed in their own category in the left menu. After selecting Faces all of the detected faces will be displayed in one section. Files can be displayed as either a

list of files or a list of faces.



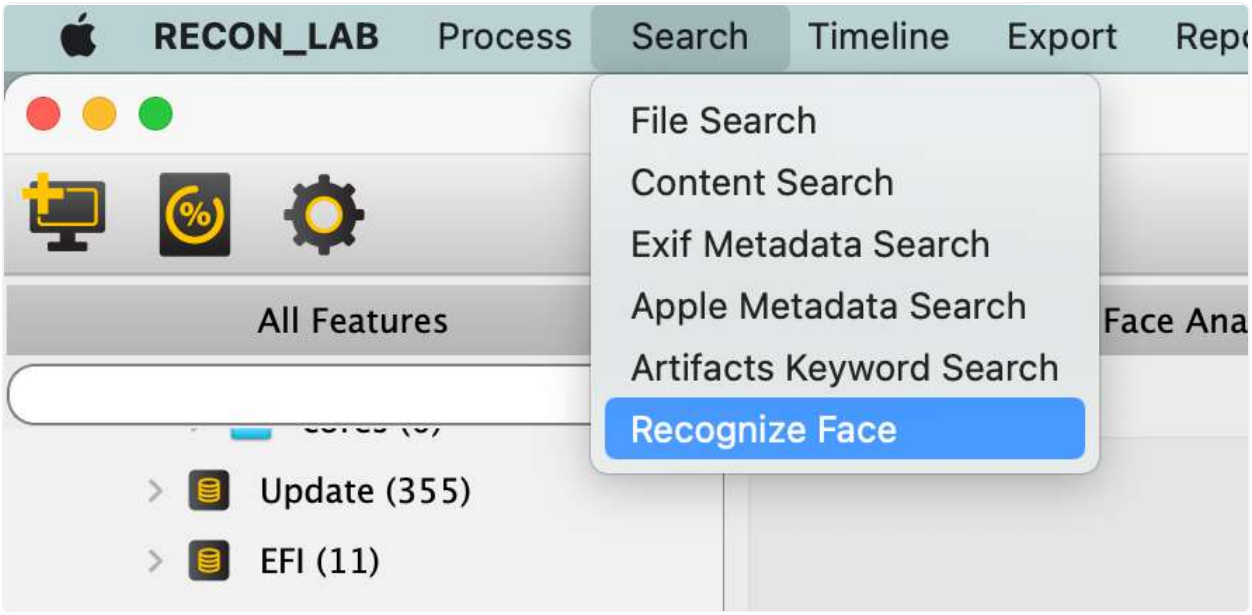
The Faces option for displaying results will show a list of faces and all images associated with each face. Simply click on each face to show a gallery of all images associated with the detected face.



40.3 Face Search

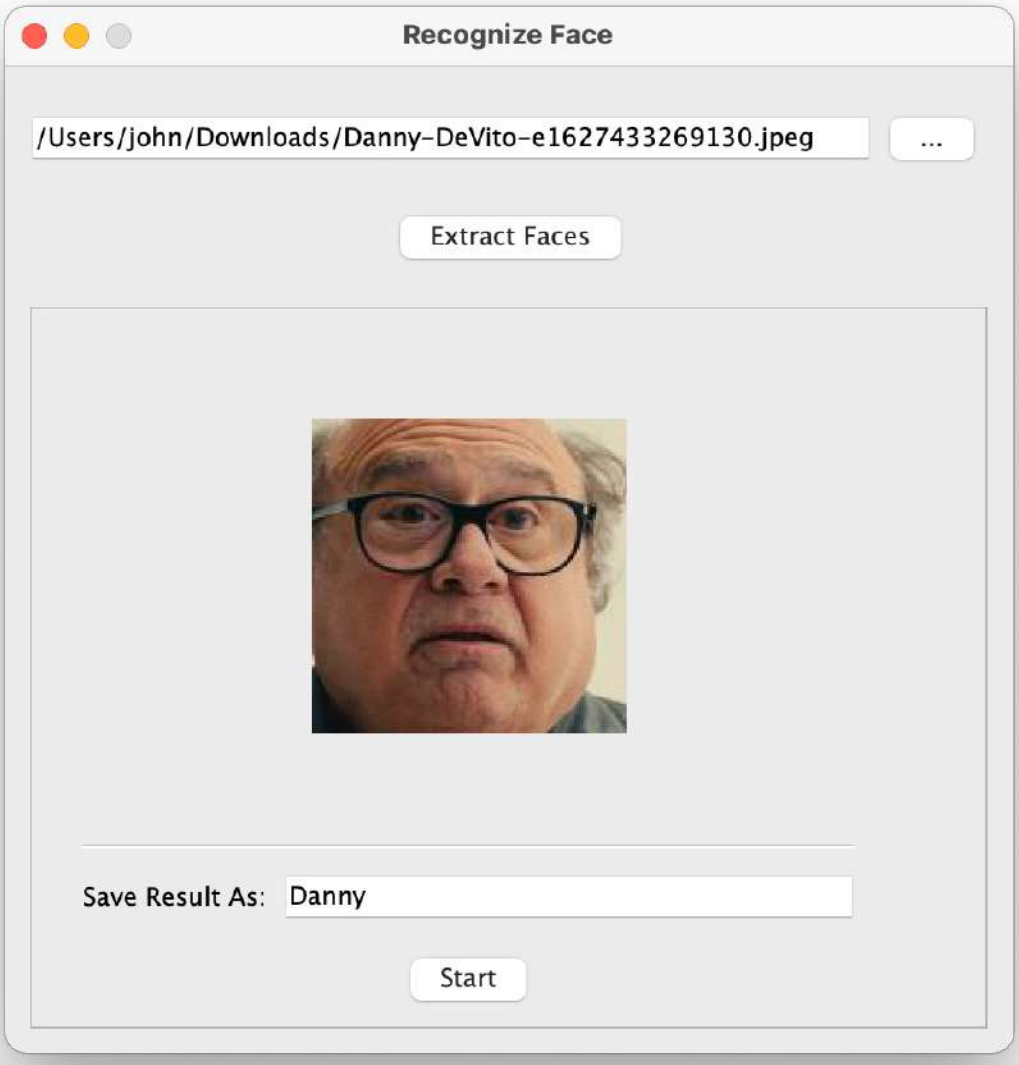
After indexing faces with the Face Analysis file system module examiners can import an image and search for any pictures with that face in them.

In the Menu Bar select Search>Recognize Face.

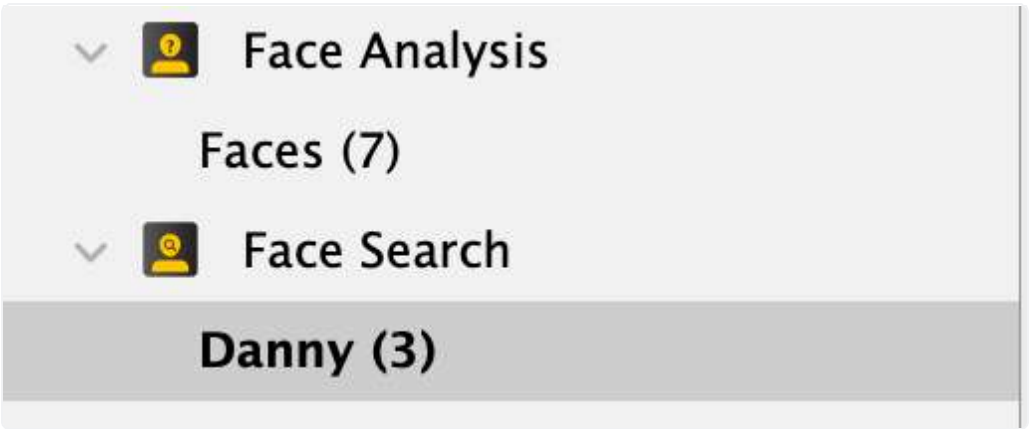


A window will pop up that allows examiners to load a file of their choosing. Click the three dots at the top of the window to open a Finder window and navigate to your desired picture. After the picture is selected click the Extract Faces button to detect the face in the picture.

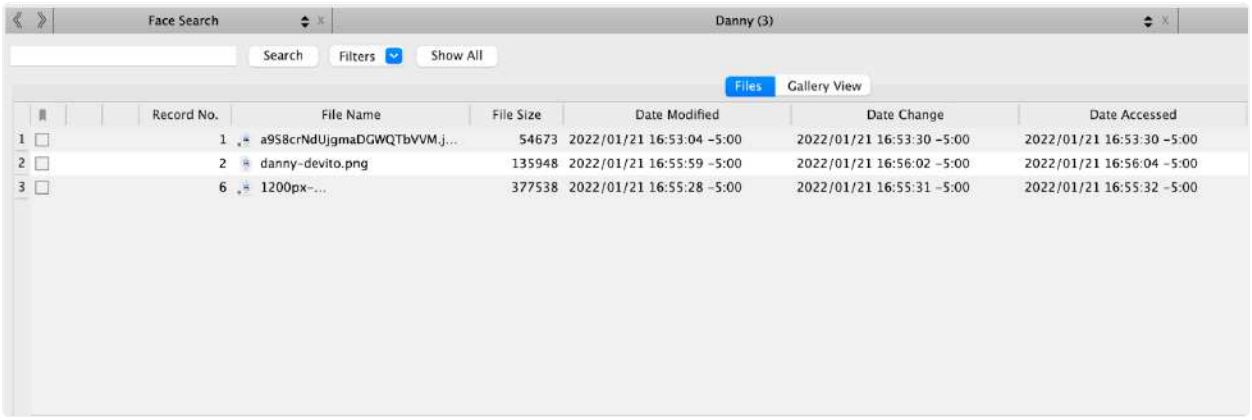
After the face is detected add a name to save the results as and click Start.

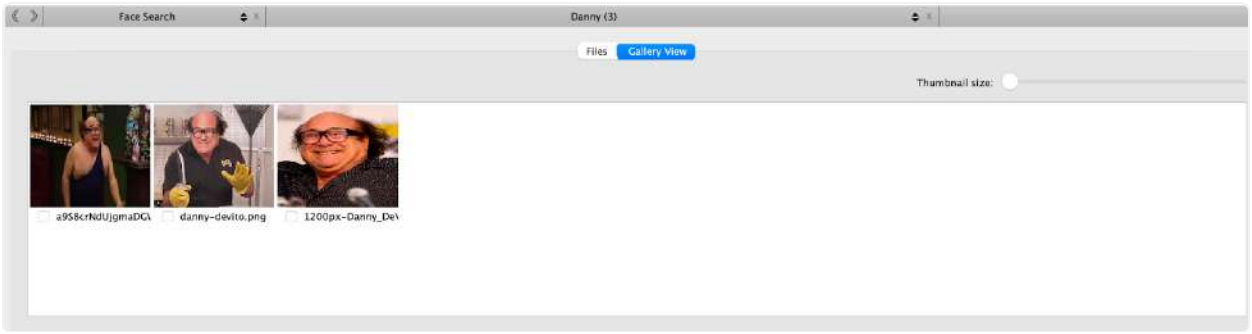


Face Search results will be displayed in the left menu under Face Search.



Results will be displayed as a file list view and can be changed to a gallery view for easy analysis.





41. Optical Character Recognition (OCR)

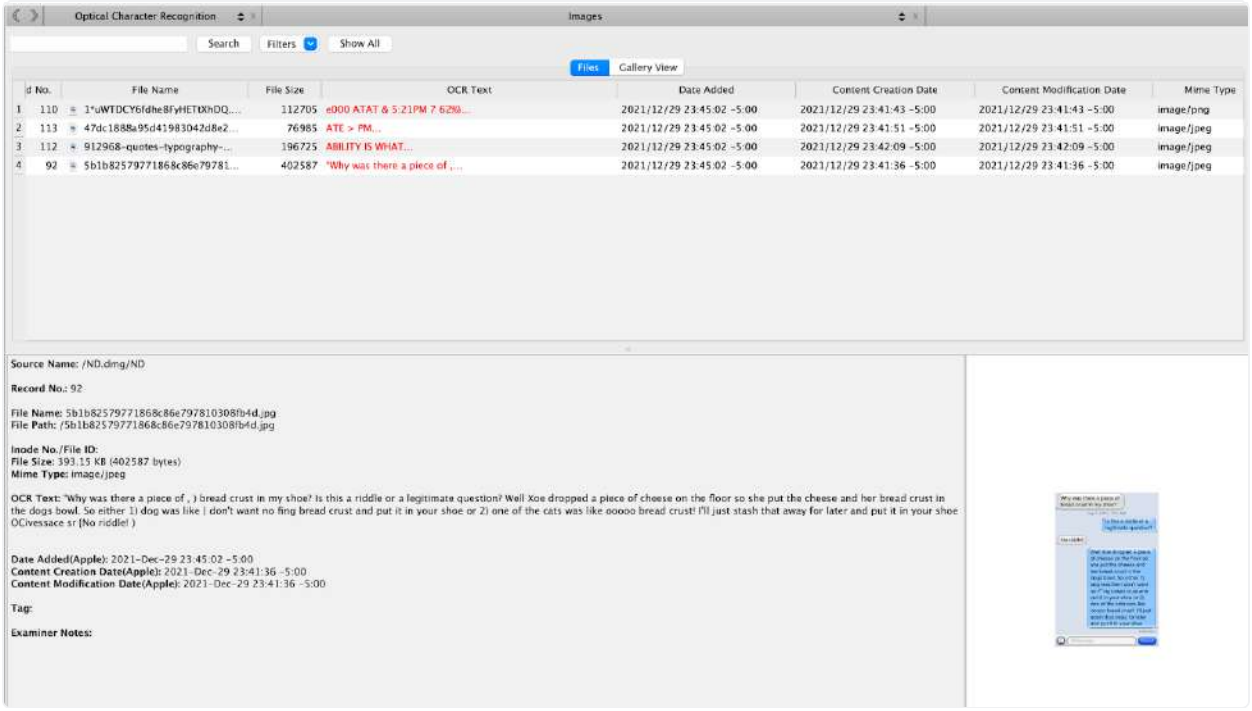
The Optical Character Recognition File System Module allows RECON LAB to automatically identify and index pictures that have text in them. Detected pictures will be put into their own category for easy analysis.

41.1 Processing Optical Character Recognition (OCR)

Optical Character Recognition is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing options including Optical Character Recognition.

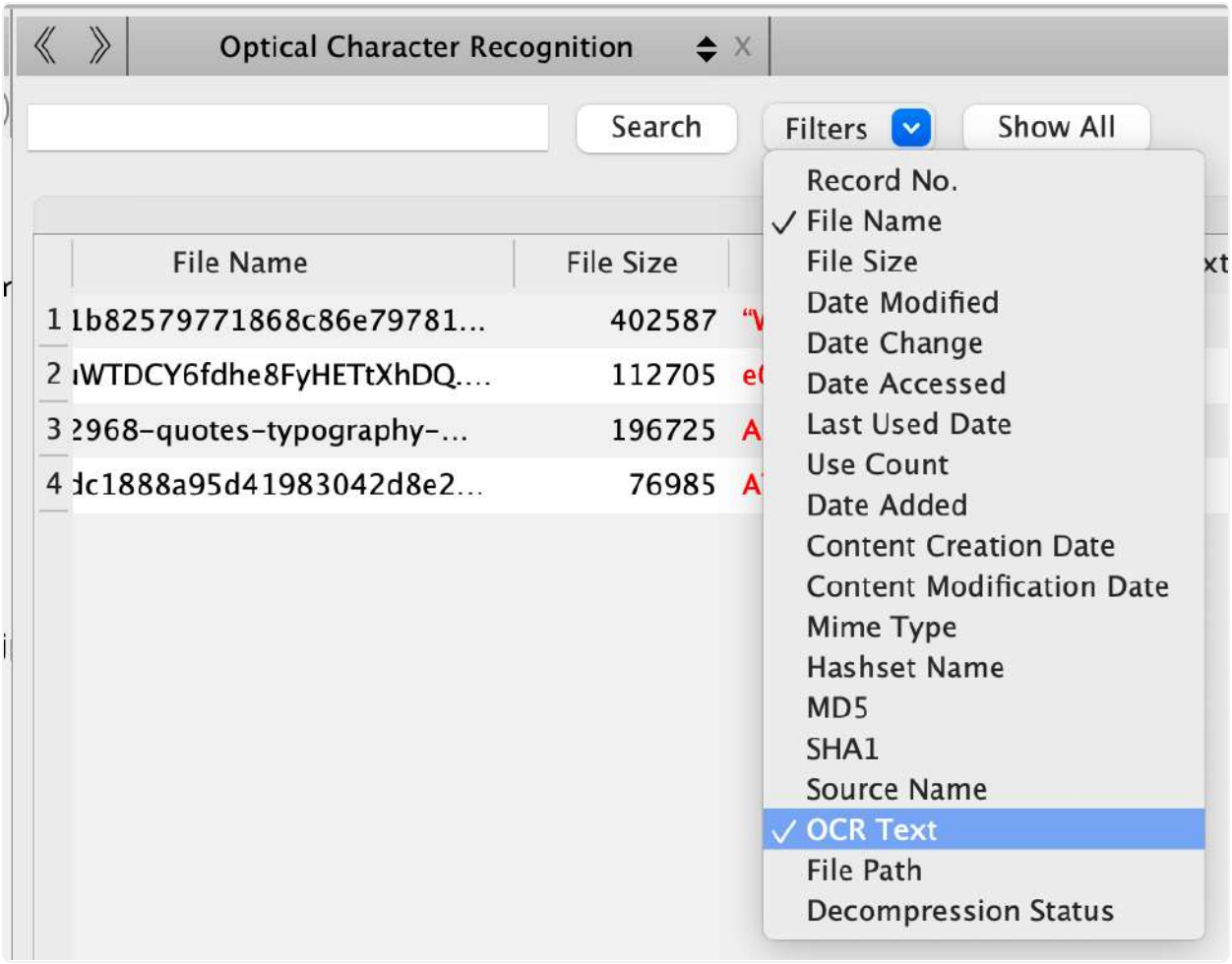
41.2 Optical Character Recognition (OCR) Analysis

Results from Optical Character Recognition are displayed in their own category in the left menu. After selecting Images all of the pictures with extracted text will be displayed in the main pane. Files can be displayed as either a list of files or a gallery view.



A preview of the extracted text is shown in red under the OCR Text column.

Searching the extracted OCR text is done using the Search box at the top left corner of the Optical Character Recognition Pane. To search OCR indexed text click the Filter dropdown menu and check the OCR Text option.



The Show All button will remove the search filter and show all indexed files again.

After selecting the file the full OCR indexed will be displayed in the Detailed Information pane under OCR Text:

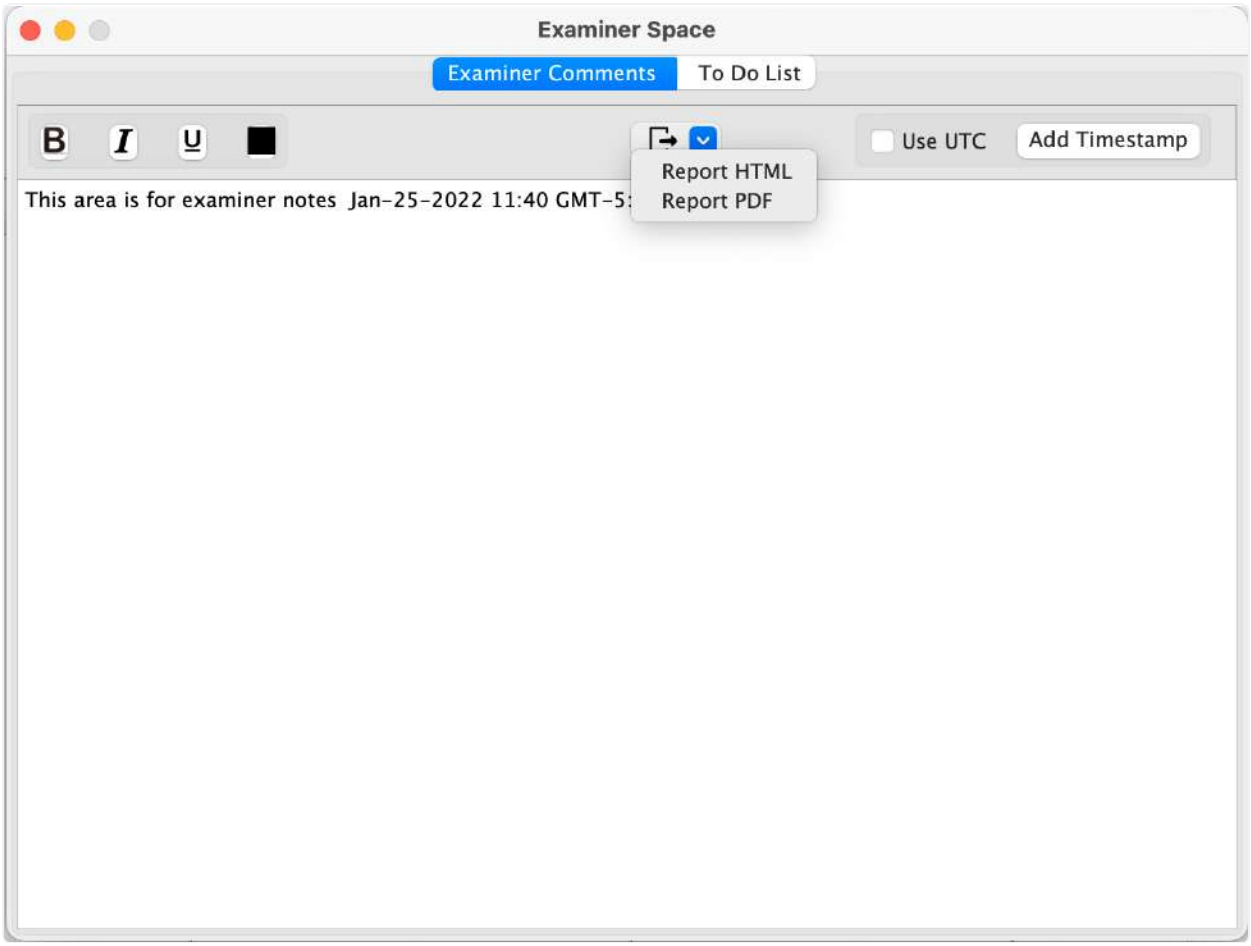
43. Examiner Space

RECON LAB's examiner space is a feature that allows examiners to easily take notes about their case and add those notes to their final reports. The Examiner space has an Examiner comments note-taking area and a to-do list.

43.1 Examiner Comments

The Examiner comments tab acts as a general note-taking option where examiners can add notes about their current case. Examiners can edit their text using the options in the top left for **bold**, *italic*, underline, and font color.

The export button in the center of the window allows examiners to export their report in either a PDF or HTML format.



The Add Timestamp button will inset a timestamp of the current machine time as either UTC (by checking the Use UTC box) or the current timezone offset of the examination machine.

43.2 Adding Examiner Notes to a Report

Examiner Notes can be added to a storyboard report as their own item. Once examiners create a storyboard report (see section 31.3 for how to generate a storyboard report) the same way any other bookmark is added.

Simply choose the Examiner Space option from the dropdown menu and add the record by right-clicking and selecting Add Record.

44. Terms and Conditions

RECON LAB

www.sumuri.com

IMPORTANT, PLEASE READ CAREFULLY. THIS IS A LICENSE AGREEMENT

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

End-User License Agreement

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

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

License Grant – SUMURI LLC grants to you a personal, non-transferable and non-exclusive right to use the copy of the software provided with this EULA. You agree you will not copy or duplicate the

software. You agree that you may not copy the written materials accompanying the software. Modifying, translating, renting, copying, transferring or assigning all or part of the software, or any rights granted hereunder, to any other persons and removing any proprietary notices, labels or marks from the software is strictly prohibited. Furthermore, you hereby agree not to create derivative works based on the software. You may not transfer this software.

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

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

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

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

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

Transfer – You may not transfer the software to a third party, without written consent from SUMURI LLC and written acceptance of the terms of this Agreement by the transferee. Your license is automatically terminated if you transfer the software without the written consent of SUMURI LLC. You are to ensure that the software is not made available in any form to anyone not subject to this Agreement.

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

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

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

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

Jurisdiction – The parties consent to the exclusive jurisdiction and venue of the federal and state courts located in the State of Delaware, USA, in any action arising out of or relating to this Agreement. The parties waive any other venue to which either party might be entitled by domicile or otherwise.