RECON LAB Manual

SUMURI LLC
RECON LAB 1.6.6

Jul 28, 2025

---

1 RECON LAB Introduction

RECON LAB is a full forensic analysis 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.

The purchase of 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 save 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 just about any file system can be mounted and processed with RECON LAB.

1.2 Three Stage Analysis

RECON LAB offers three-stages of analysis.

Stage One – Parse and recover 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 to make manual analysis easier.

1.3 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.

1.4 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.

1.5 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.

1.6 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

RECON LAB requires a Mac with at least a quad-core Intel i7 processor or an Apple Silicon chip (M1, M2, M3, or M4) and a minimum of 16GB RAM. The system must be capable of running macOS 12.7.6 or later.

An administrator user account is required.

For improved performance—even on older or slower Macs—we recommend using an external Thunderbolt 3 RAID. Storing both the evidence and case files on the external RAID can significantly boost processing speed.

SUMURI has tested and offers the ARECA 8-Bay Thunderbolt 3 RAID Storage, available in various storage configurations.

---

3 Before Starting a New Case in RECON LAB: Helpful Tips

3.0.0.1 Use macOS Extended (HFS+) for Evidence Drives

While macOS supports multiple file systems, our testing has shown that macOS Extended (HFS+) provides the most reliable results when used with RECON LAB.

Important: When creating logical images of Mac data, avoid using non-Mac file systems. Doing so will result in the loss of Apple Extended Metadata.

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

Disk images created with RECON ITR or PALADIN use the Apple Disk Image (.dmg) format, which is a RAW image compatible with most forensic tools that support RAW. Additionally, .dmg files are natively supported by macOS.

RECON LAB also supports Expert Witness formats (.E01, .Ex01), but these are not native to macOS and require FUSE to mount. FUSE introduces an extra translation layer between the forensic image and RECON LAB, which can negatively impact performance and reliability. We recommend using .dmg whenever possible.

3.0.0.3 Avoid Segmenting Forensic Image Files

Although RECON LAB supports segmented image files, modern storage capacities can result in thousands of segments, potentially causing stability or performance issues. Whenever feasible, use a single image file instead of segmented formats.

---

4 Getting Support

Support for RECON LAB is available via our Online Support site and submitting a ticket here:

https://sumuri.zohodesk.com/portal/en/signin

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 all 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/

---

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 the largest amount of data can be processed and analyzed. Due to Mac's strict adherence to security, you may be asked to provide your password various times during the installation.

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

7.1 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.

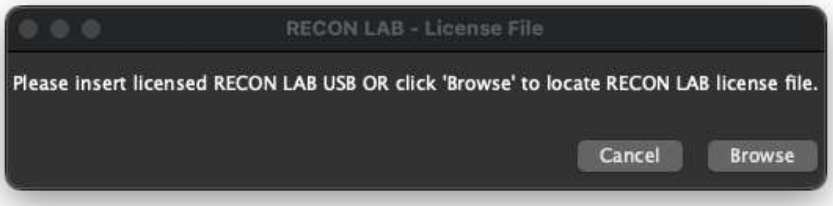
7.1.0.1 Installing FUSE for macOS

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 Updating and Installing RECON LAB

Please ensure you have downloaded the latest version of RECON LAB from our website: https://sumuri.com/updates/

1. Plug the RECON LAB USB into the Mac.
2. Download the DMG from the software update page.
3. Double-click on the DMG to mount the DMG.
4. Drag and drop the “**RECON_LAB.app**” from the DMG to your Applications folder.
5. Open “**System Settings**” and navigate to the “**Privacy and Security Tab**”. Press on “**Full Disk Access**” and add the “**RECON_LAB.app**” to the list of Applications that have full disk access.
6. Double click on **RECON LAB** to launch the application.
7. A notification window will appear to ask if you want to open an application downloaded from the internet. Choose “**Open**”.



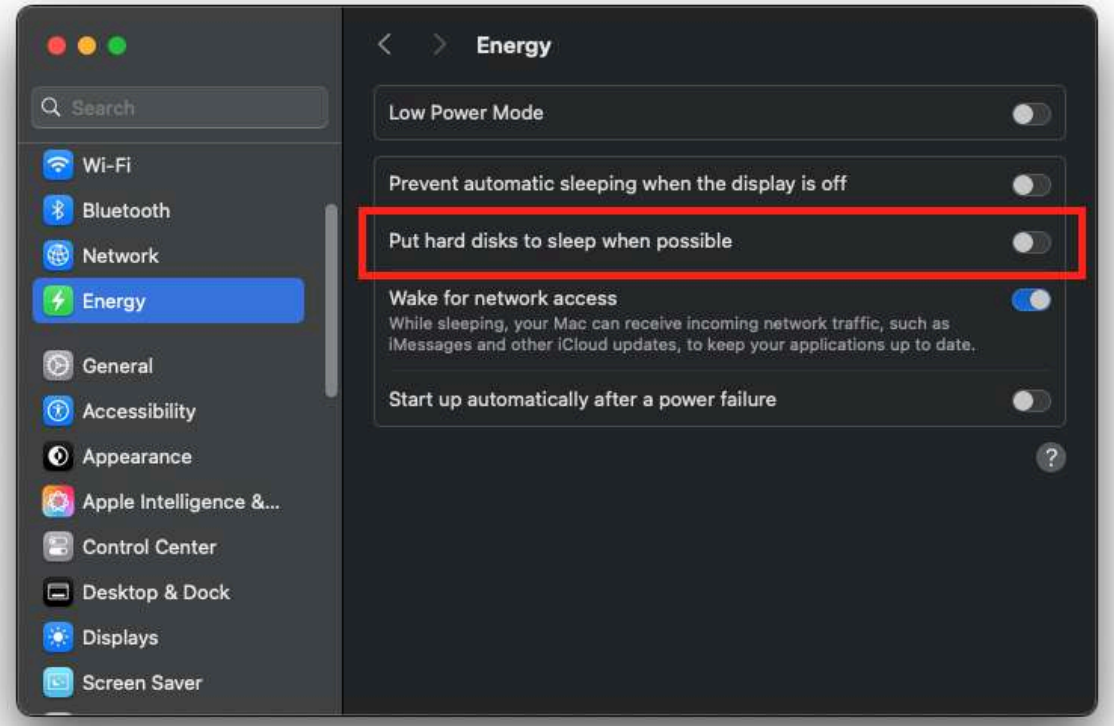
8. After the application has launched it may prompt you for the license file. Press on “Browse” and navigate to the “License” file on the RECON LAB USB.

7.4 Energy and Sleep Settings

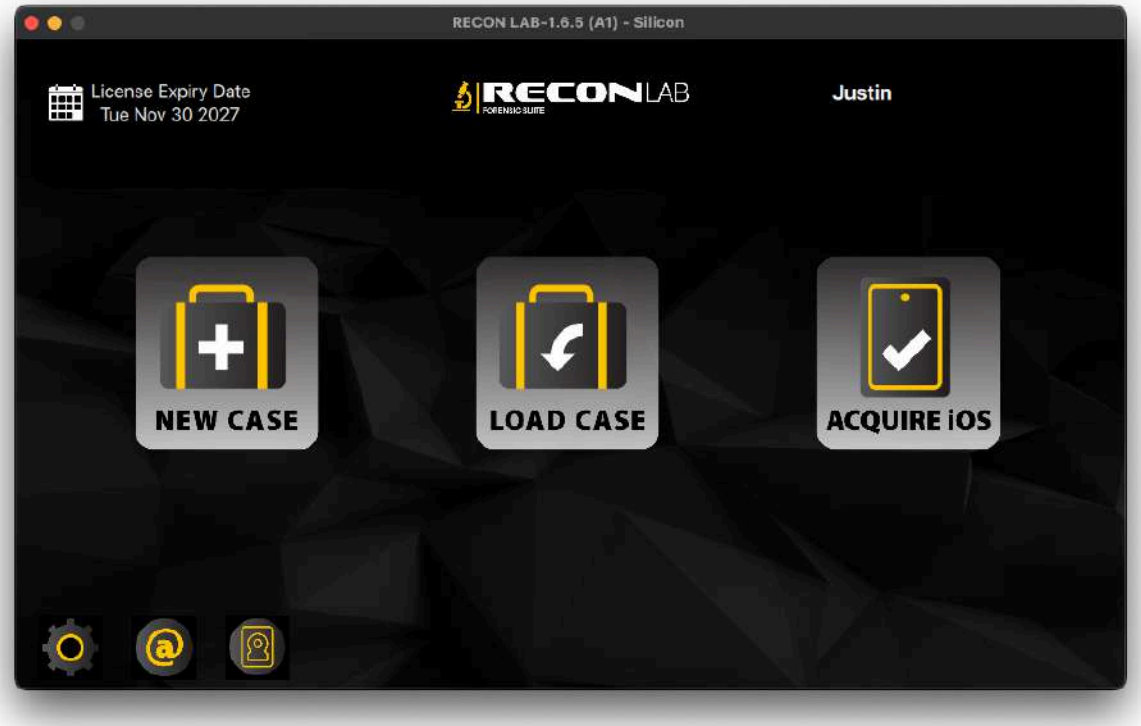
Allowing your Mac to go to sleep in the middle of processing a case will most likely cause issues. Make sure that you disable any settings which “Put hard disks to sleep when possible” or that allows the computer to sleep when working with RECON LAB.

These settings can be changed in System Settings in macOS 13 and above:

1. Open “System Settings”.
2. Press on the “Energy” tab.
3. Turn off “Put hard disks to sleep when possible”.


Energy
Search
Wi-Fi
Bluetooth
Network
Energy
General
Accessibility
Appearance
Apple Intelligence &...
Control Center
Desktop & Dock
Displays
Screen Saver
Low Power Mode
Prevent automatic sleeping when the display is off
Put hard disks to sleep when possible
Wake for network access
While sleeping, your Mac can receive incoming network traffic, such as iMessages and other iCloud updates, to keep your applications up to date.
Start up automatically after a power failure

8 RECON LAB Splash Screen



The Main Menu is the first window that you will be greeted with upon launching the RECON LAB software. From here the examiner can:

- Start a new RECON LAB case
- Load an existing RECON LAB case
- Set RECON LAB Configurations
- View Change Logs
- Manage connected disks

8.1 Splash Screen Options

8.1.1 New Case

- Will open a window where the examiner can create a new RECON LAB Case.
- Where the examiner can add evidence and start case creation.

8.1.2 Load Case

- This is where an examiner can load an existing RECON LAB Case
- Will open a prompt where the examiner can navigate to an existing RECON LAB Case folder, and select it to be open.

- RECON LAB can load other RECON LAB cases created in different or older versions of RECON LAB.

8.1.3 Acquire iOS

- This will open the iOS acquisition prompt.
- Examiner will be able to acquire an unencrypted backup of a connected iOS device

8.1.4 Configuration

- Allows the examiner to add their examiner details, these will be the examiners details that are included in their reports and the initial case creation.
- Examiner can set up configuration settings for RECON LAB for data processing

8.1.5 About RECON

- Will open a Window where the examiner can view information about the license and current EULA agreements.

8.1.6 Disk Manager

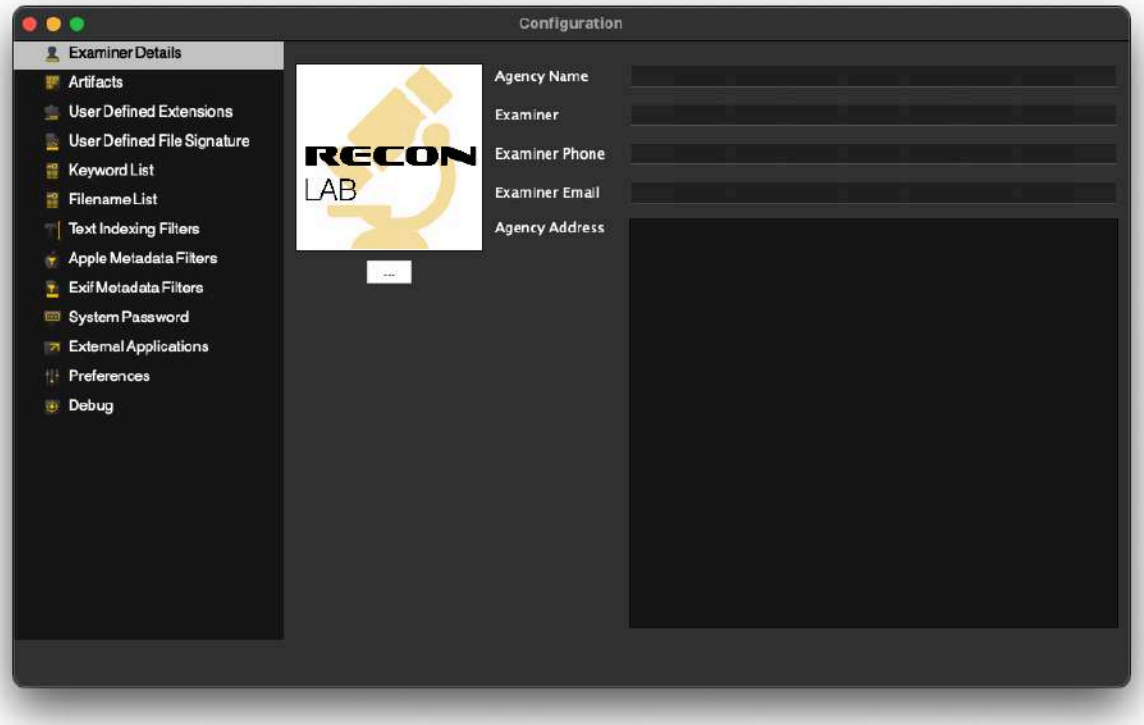
- The Disk manager will open a screen where the examiner can control the connected disks.

---

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

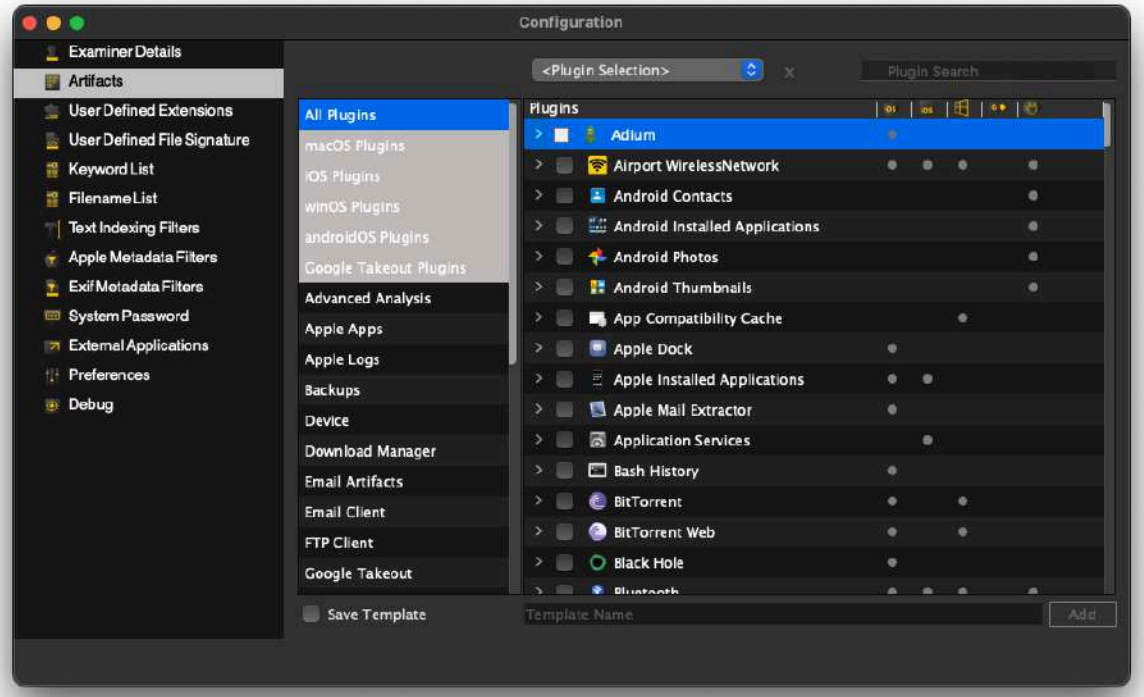


The Examiner Details settings allow entry of the following information:

- 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



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. In this Window an examiner can:

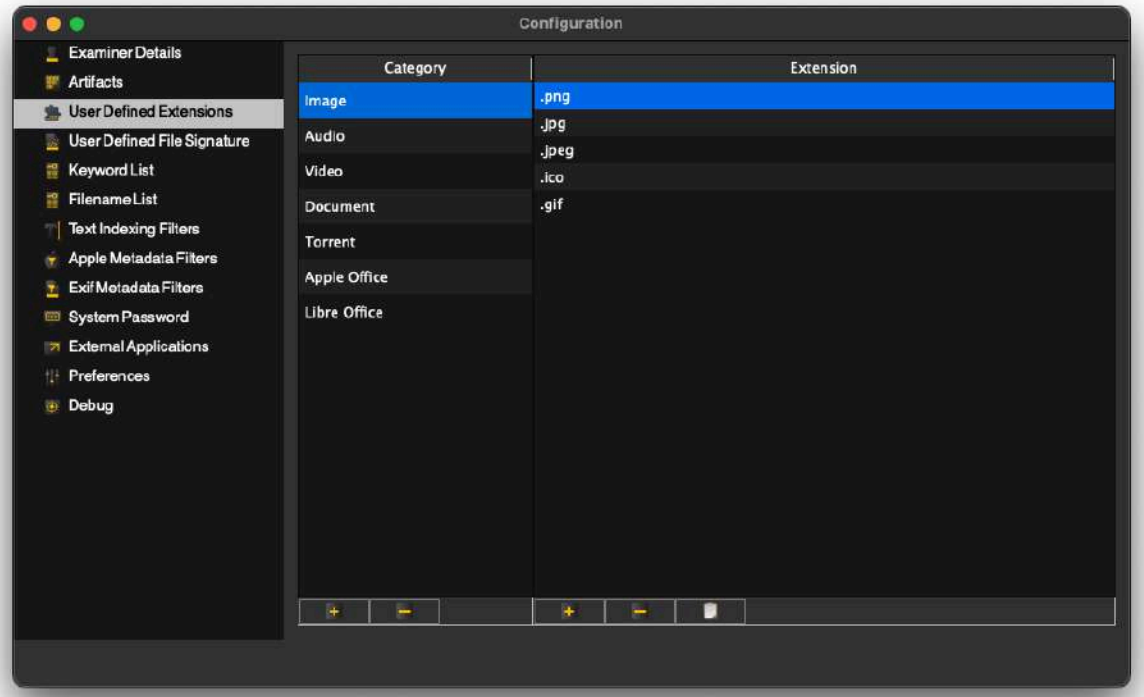
- View what plugins RECON LAB supports
- View the data that each plugin will parse. To view a full list of parsed artifacts, press the > button in each of the plugin records.
- Create and manage plugin templates, which are saved sets of plugins you can easily reuse whenever you need them
- View what artifacts are supported based on what source is being ingested. Plugins will have a dot beneath the source, if that plugin is supported for that source. The different sources are:
    - macOS: This will be symbolized with the Apple Symbol.
    - iOS: This will be symbolized with the iOS text
    - Windows: This will have the windows icon
    - Google Takeout: This will be symboled with the G
    - Android: This will be symbolized with the android.
- Search for plugins by name. To search a plugin by name, type the keyword in the **Plugin Search** textbox.

9.2.0.1 To create a plugin template:

1. Press the Checkbox next to the plugins name
2. Press the checkbox next to the **Save Template** button
3. In the **Template Name** text field, enter the name that would like to call this template

4. Press on the **Add** button
5. To view the list currently created templates, press on the **Plugin Selection** dropdown

9.3 User Defined Extensions

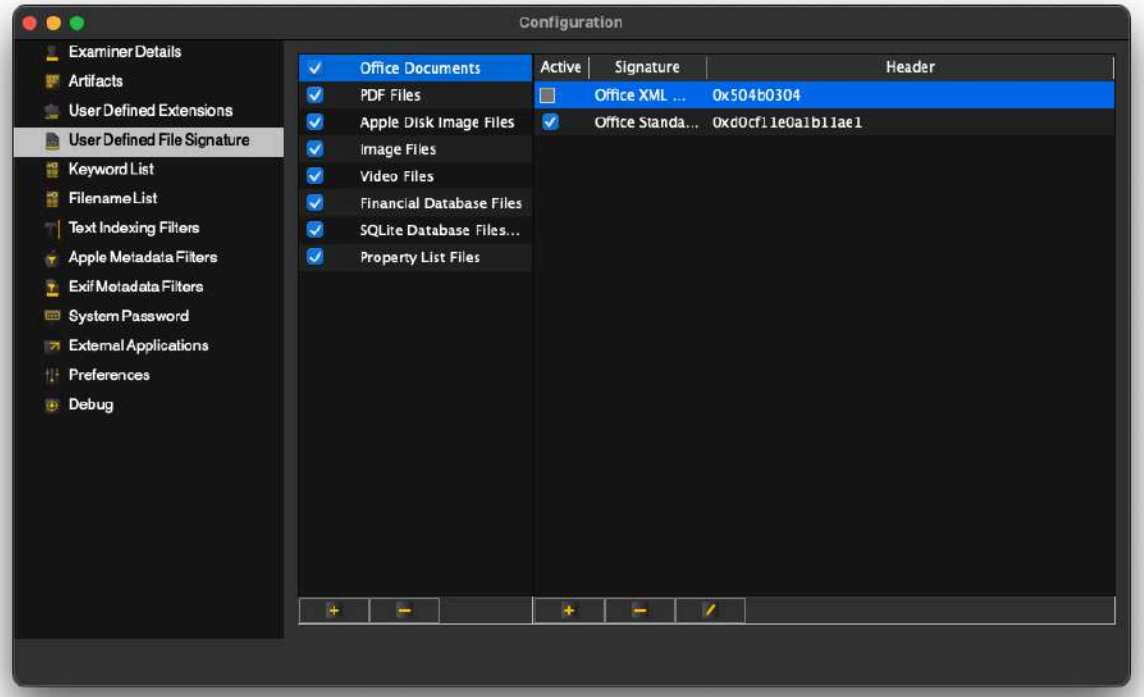


User Defined Extension settings allow examiners to create custom “buckets” (categories) for specific file extensions. These buckets appear in the RECON LAB Sidebar, and any file with a matching extension is automatically filtered into the appropriate category.

Each bucket is shown under the Category column, and its associated file extensions are listed under Extension.

- To add a new category or extension, click the + button.
- To remove a selected category or extension, click the − button.
- To add multiple extensions at once, use the clipboard (paste) button. Your list must be formatted as one extension per line, with each item separated by a single carriage return. Copy the entire list to your clipboard before pasting.

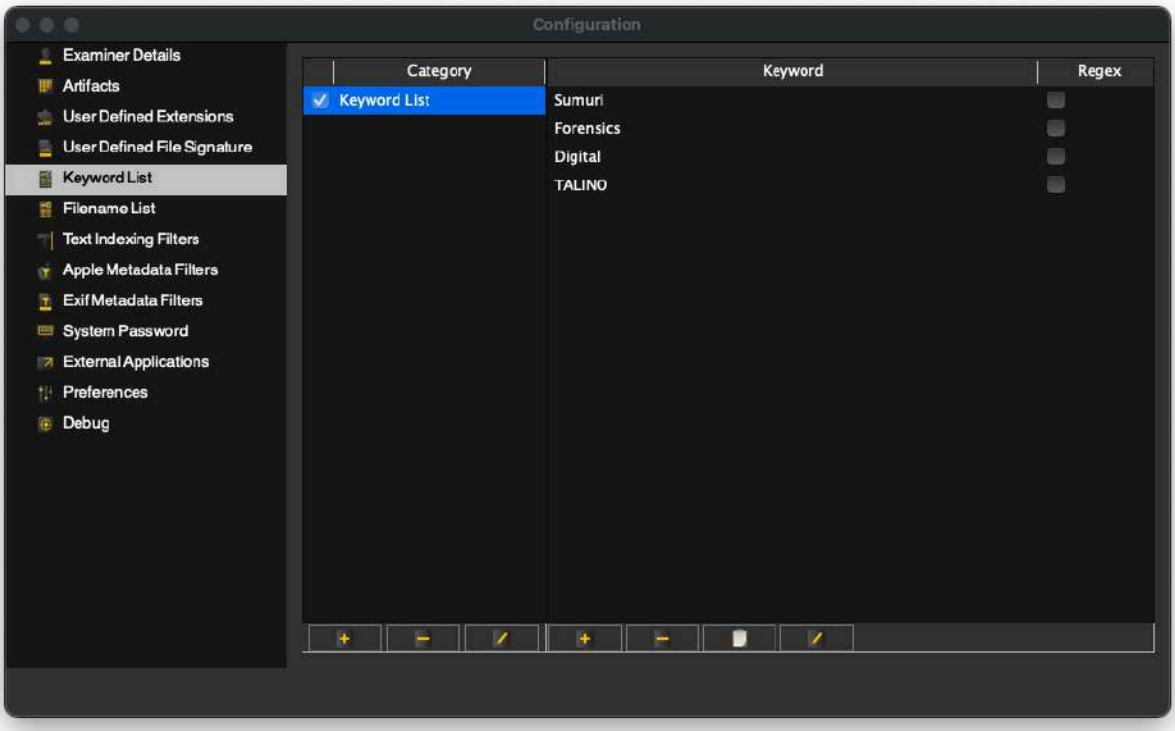
9.4 User File Signatures



User Defined File Signature settings allow examiners to create custom “buckets” (categories) based on file signatures. File signatures are used to identify files even when extensions are missing or incorrect. These categories will appear in the RECON LAB Sidebar, and any file with a matching signature will automatically be filtered into the appropriate bucket.

- To create a new category or add a file signature, click the + button.
    - Use the Label field to name the category.
    - Enter the file signature in HEX or ASCII, and select the appropriate option.
    - If the signature starts at a specific offset, enter the value in the Offset field.
    - Click Add to save.
- To remove a category or file signature, select it and click the − button.
- To edit an existing file signature, click the Edit (pencil) icon, make the necessary changes, and click Add to save the updates.

9.5 Keyword Lists



The Keyword List settings allow examiners to create keyword lists in advance for use during content-based searches. Various search options will be detailed later in this manual.

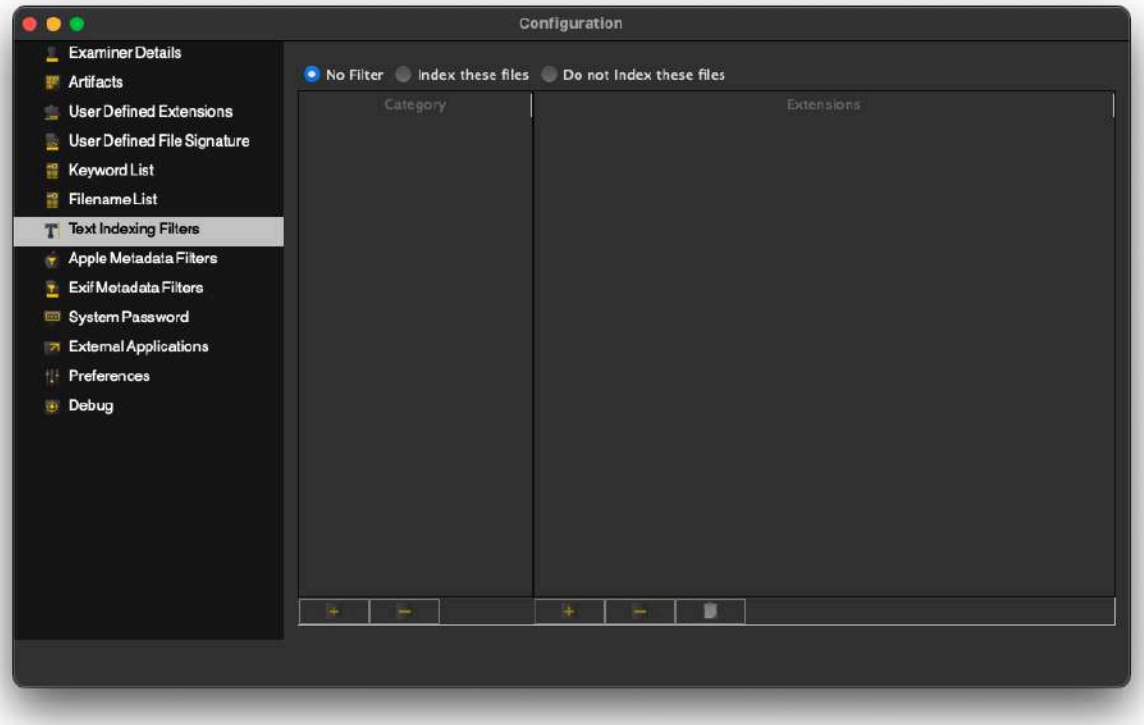
Keywords can be organized into categories and may include plain text or regular expressions (REGEX) formatted according to dtSearch rules.

For reference, dtSearch's Quick Reference Guide is available here:
http://support.dtsearch.com/Support/forms/iframes_advanced/default.html

9.5.0.1 Adding or Removing Categories and Keywords

- To create a new category or keyword, click the + button, enter the desired text, and press Return.
- If the keyword should be treated as a regular expression, check the Regex box before adding it.
- To remove a category or keyword, select the entry and click the − button.
- To add multiple keywords at once, use the clipboard (paste) button. Ensure each keyword is on its own line, separated by a single carriage return. Copy the list to your clipboard and then paste it into RECON LAB.
- To edit an existing keyword, click the Edit (pencil icon), make the necessary changes, and click Add to save.

9.6 Text Indexing Filters

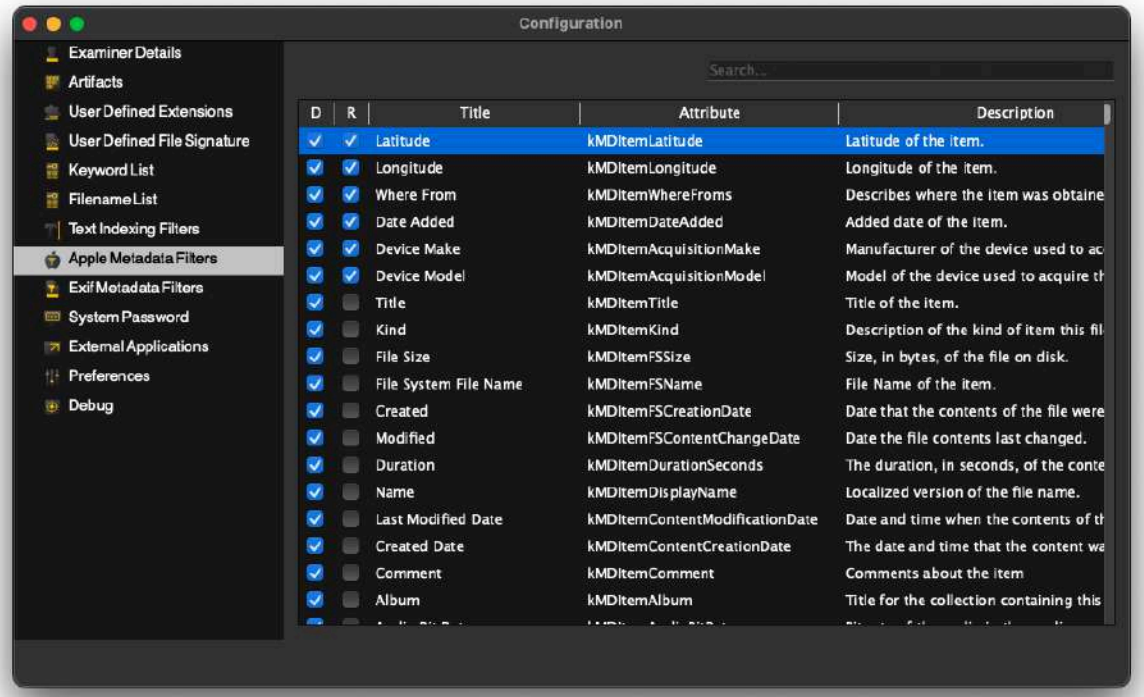


RECON LAB provides Text Indexing Filter settings to help streamline your examination process. These settings allow you to define which files should be indexed—or excluded from indexing—before starting your case. This can significantly improve processing speed by limiting the scope of text indexing.

9.6.0.1 Text Indexing Options:

- **No Filter**
  - Default setting.
  - All files will be indexed without restriction.
- **Index These Files**
  - Only the specified file types (by extension) will be indexed.
  - Click the + button to add extensions.
  - Click the − button to remove extensions.
- **Do Not Index These Files**
  - All files will be indexed except those specified by extension.
  - Click the + button to add extensions to exclude.
  - Click the − button to remove extensions from the exclusion list.

9.7 Apple Metadata Filters



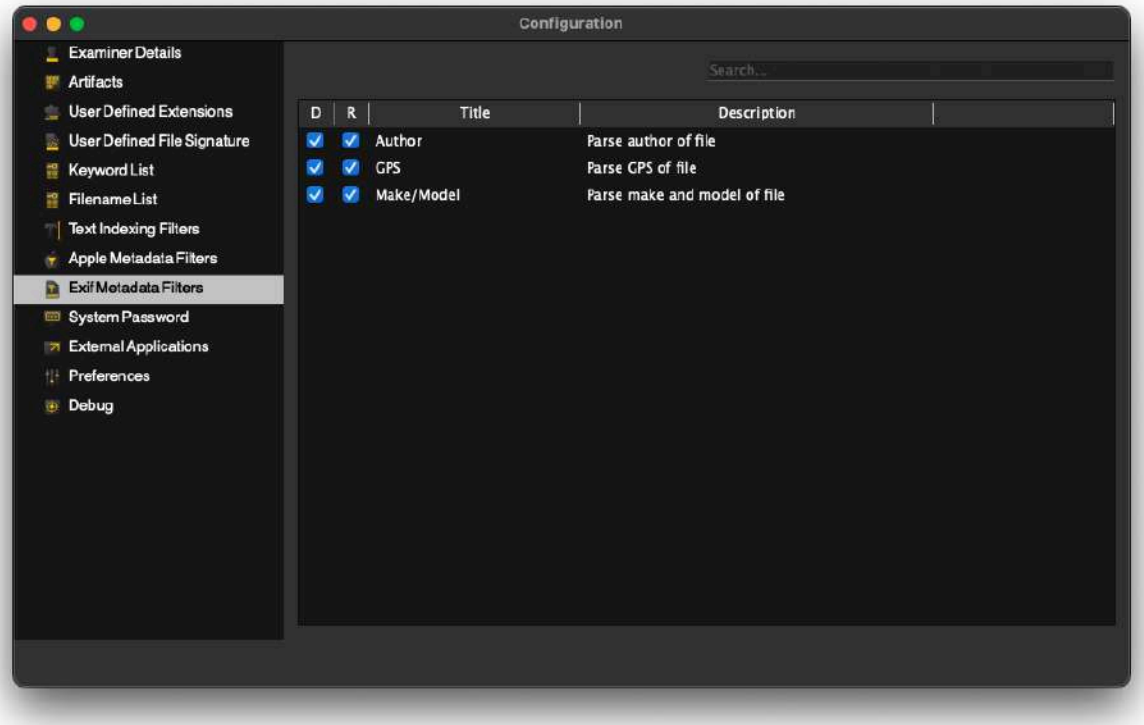
RECON LAB is the only forensic suite developed natively on macOS, allowing it to fully access and utilize Apple Extended Metadata without relying on third-party or reverse-engineered solutions. This ensures more accurate and complete metadata analysis, reducing the risk of missed evidence.

In the main RECON LAB interface, all Apple Extended Metadata is fully visible. The Apple Metadata Filter settings allow you to select key metadata attributes to display in the Sidebar or include in reports.

9.7.0.1 Apple Metadata Filter Column Descriptions:

- **D** – Check this box to display the Apple Extended Attribute in the RECON LAB Sidebar. Files with matching attributes will be automatically filtered into the Sidebar.
- **R** – Check this box to automatically include the selected attribute's metadata in generated reports.
- **Title** – The common name of the Apple Extended Attribute.
- **Attribute** – The exact name of the Apple Extended Attribute.
- **Description** – The official description of the Apple Extended Attribute.

9.8 EXIF Metadata Filters

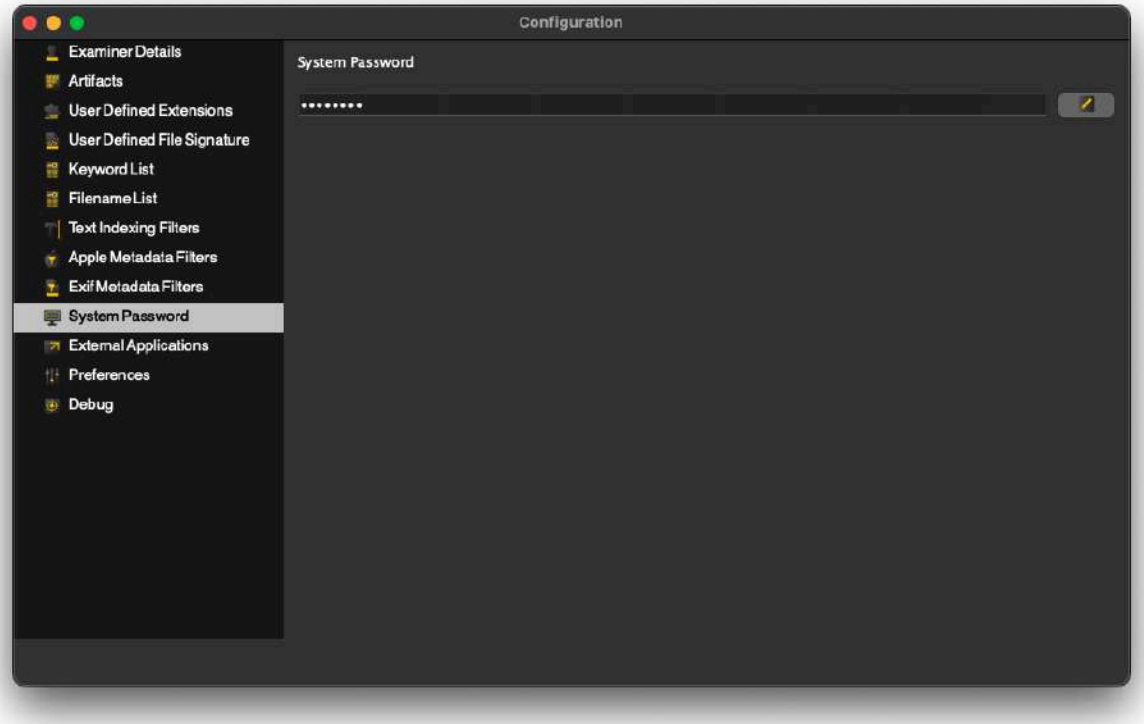


RECON LAB parses EXIF metadata and provides EXIF Metadata Filter settings to help examiners automatically filter files based on specific EXIF attributes. These filtered files can be displayed in the RECON LAB Sidebar, and selected metadata attributes can be included in reports.

9.8.0.1 EXIF Metadata Filter Column Descriptions:

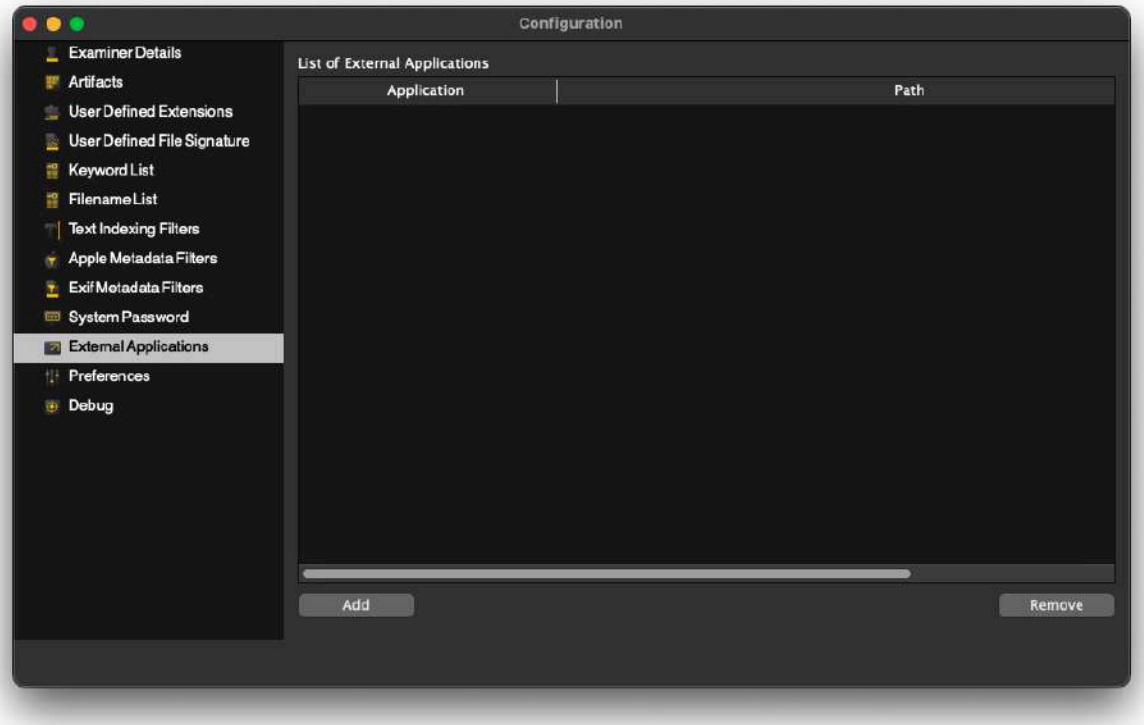
- **D** – Check this box to add the EXIF metadata attribute to the RECON LAB Sidebar. Files with matching metadata will be automatically filtered into the Sidebar.
- **R** – Check this box to include the selected EXIF metadata attribute automatically in reports.
- **Title** – The common name of the EXIF metadata attribute.
- **Description** – The official description of the EXIF metadata attribute.

9.9 System Password



When RECON LAB is launched for the first time—or after a reset—you will be prompted to enter the system Admin password. If the Admin password is changed after installation, it must be updated within the System Password settings to ensure continued access and functionality.

9.10 External Applications

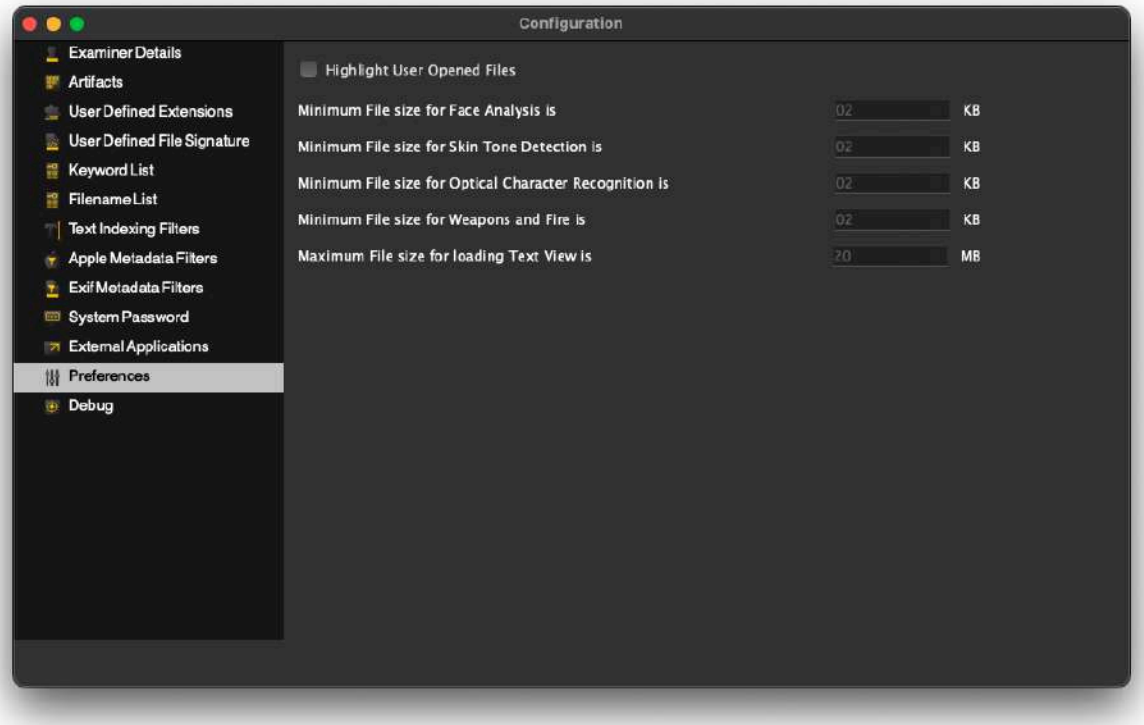


RECON LAB allows you to open files in external applications for further analysis or review. Applications can be added or removed from this list as needed.

9.10.0.1 Available Options:

- **Add** – Click this button to browse for and select an external application to add to RECON LAB.
- **Remove** – Highlight the application you wish to remove and click this button to delete it from the list.

9.11 Preferences

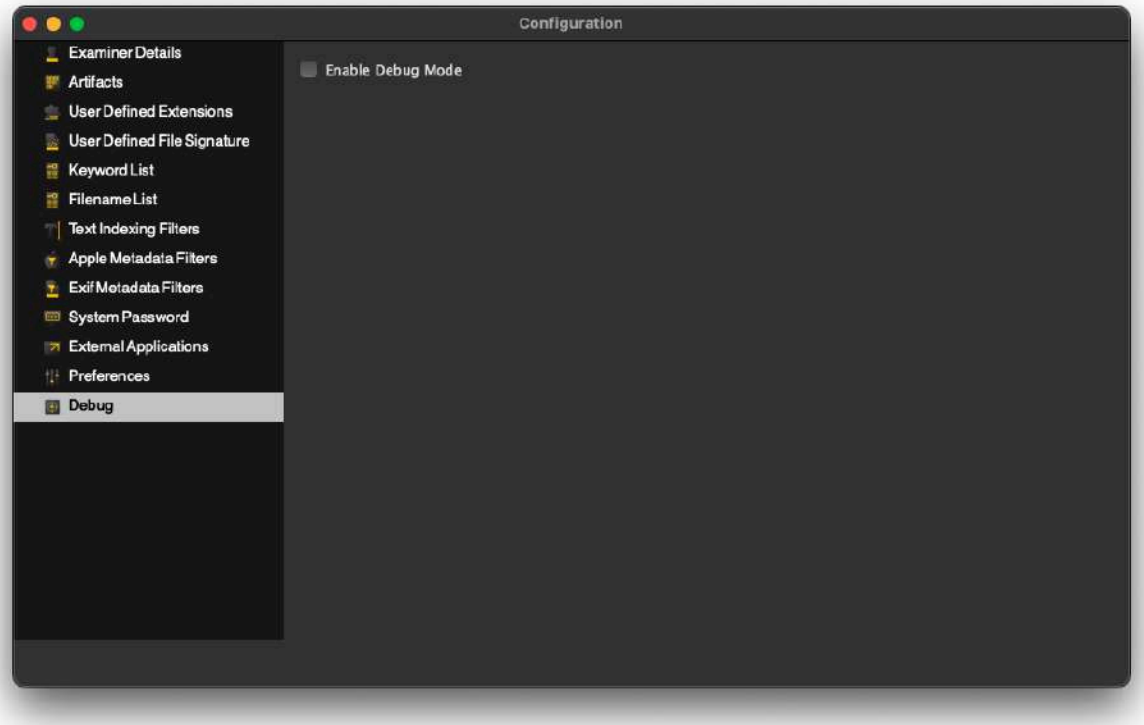


The Preferences view allows the examiner to configure the default behavior of RECON LAB. These settings help tailor the examination environment and can improve overall performance.

9.11.0.1 Available Options:

- **Highlight User Opened Files** – Enables visual highlighting (yellow) for files that have a recorded use count in their Apple Extended Attributes metadata.
  Note: The Apple Metadata Process must be run for this highlight to appear.
- **Minimum File Sizes** – Allows the examiner to set minimum file size thresholds for various AI functions. Adjusting these values can help reduce processing time.

9.12 Debug Mode



RECON LAB includes the ability to log errors that may cause the application to fail. Enabling Debug Mode helps the development team identify, diagnose, and address issues more effectively.

9.12.0.1 To Enable Debug Mode:

- Check the box next to Enable Debug Mode.
- When the box is checked, Debug Mode is active and RECON LAB will begin logging error information.

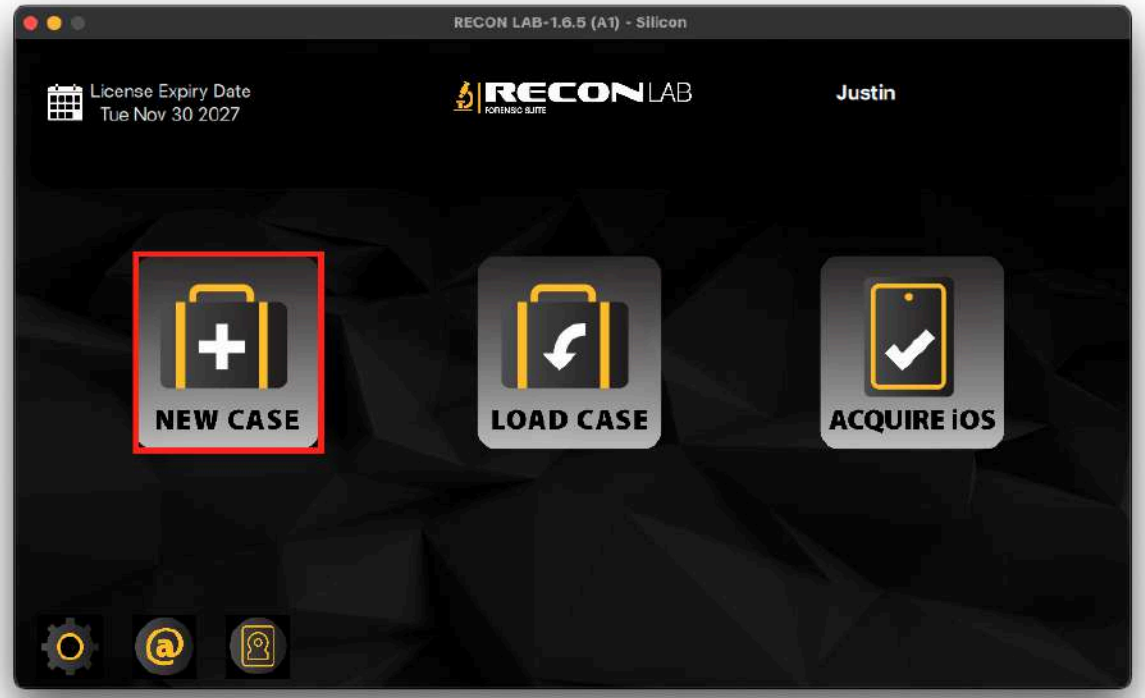
9.12.0.2 Log File Location:

- Debug logs are saved to a folder named RECON_LOGS, which is automatically created on the active user's Desktop.

---

10 New Case

Case Info

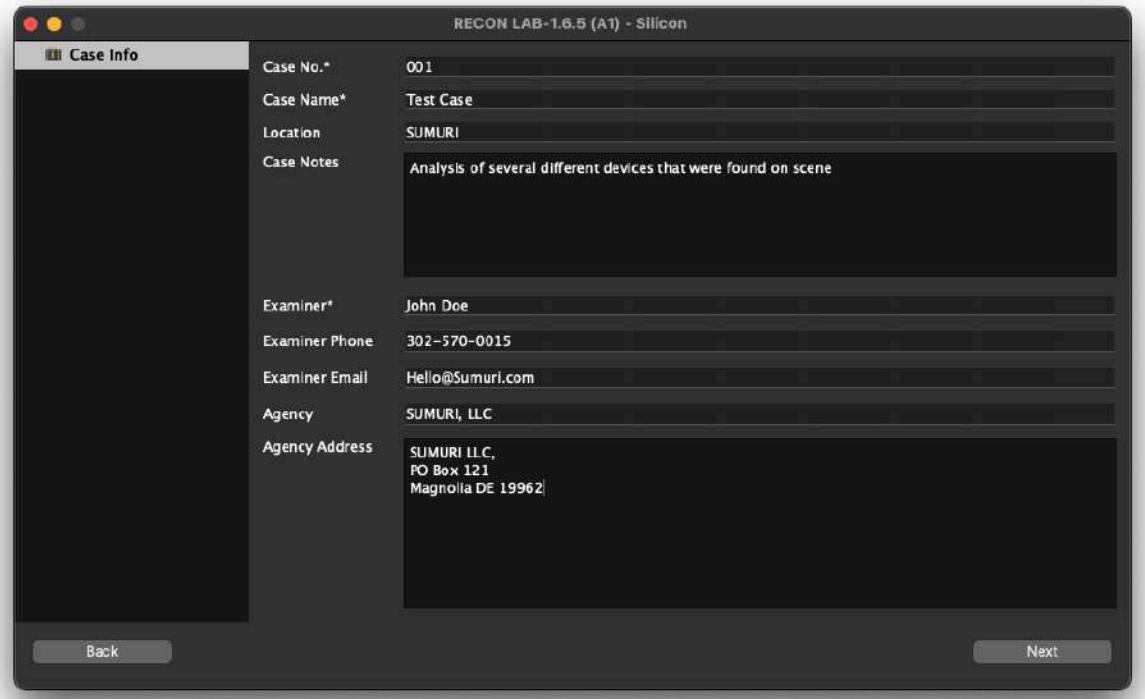


To begin a case in RECON LAB, select New Case from the Welcome Screen. This will launch the Case Wizard, starting with the Case Info screen.

If any case-related information was previously entered in the RECON Configuration settings, it will automatically populate the relevant fields.

Important Notes:

- The information entered in the Case Info screen will be included in RECON LAB reports.
- Mandatory fields are marked with an asterisk (*) and must be completed to proceed to the next screen.



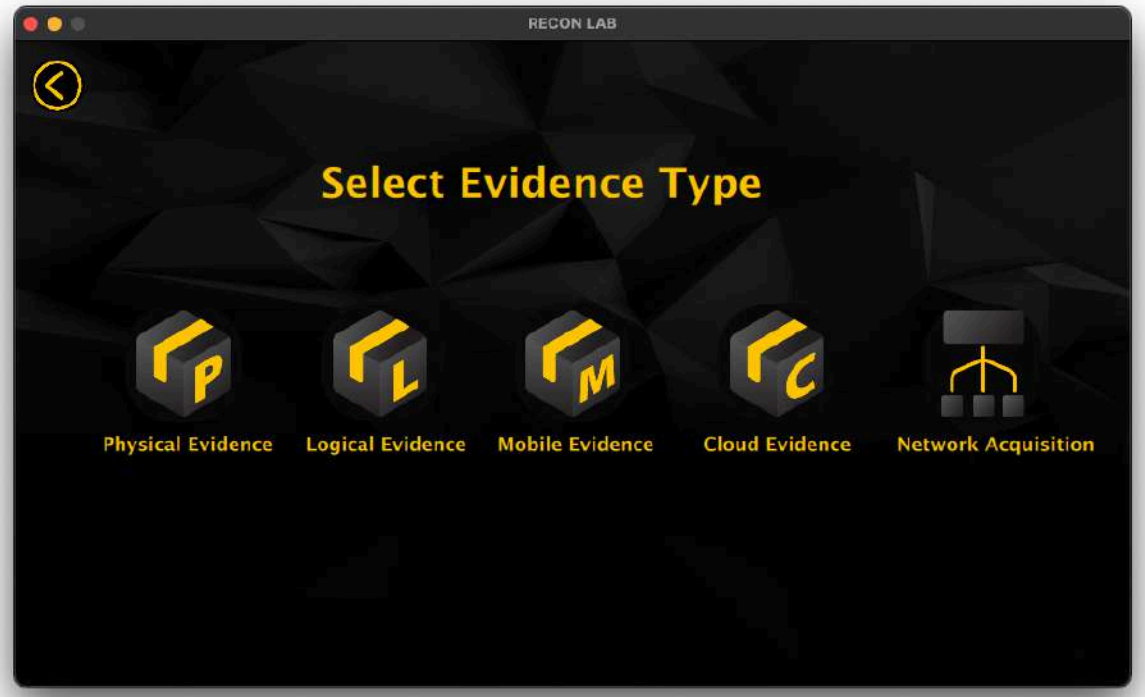
The Case Info window allows the examiner to enter case-specific details that will appear in RECON LAB reports. Some fields will be automatically populated with data from the RECON Configuration settings if previously entered.

10.1.0.1 Available Case Info fields

- Case No. (mandatory) – A unique case number.
- Case Name (mandatory) – The name of the case.
- Location – The location of the incident or examination.
- Case Notes – A free-form text field for any relevant notes.
- Examiner (mandatory) – The examiner's name. Auto-filled from Configuration settings if available.
- Examiner Phone – The examiner's phone number. Auto-filled from Configuration settings if available.
- Examiner Email – The examiner's email address. Auto-filled from Configuration settings if available.
- Agency – The name of the agency. Auto-filled from Configuration settings if available.
- Agency Address – The agency's address.

Once all mandatory fields and any desired additional information are entered, click Next to proceed.

10.2 Source



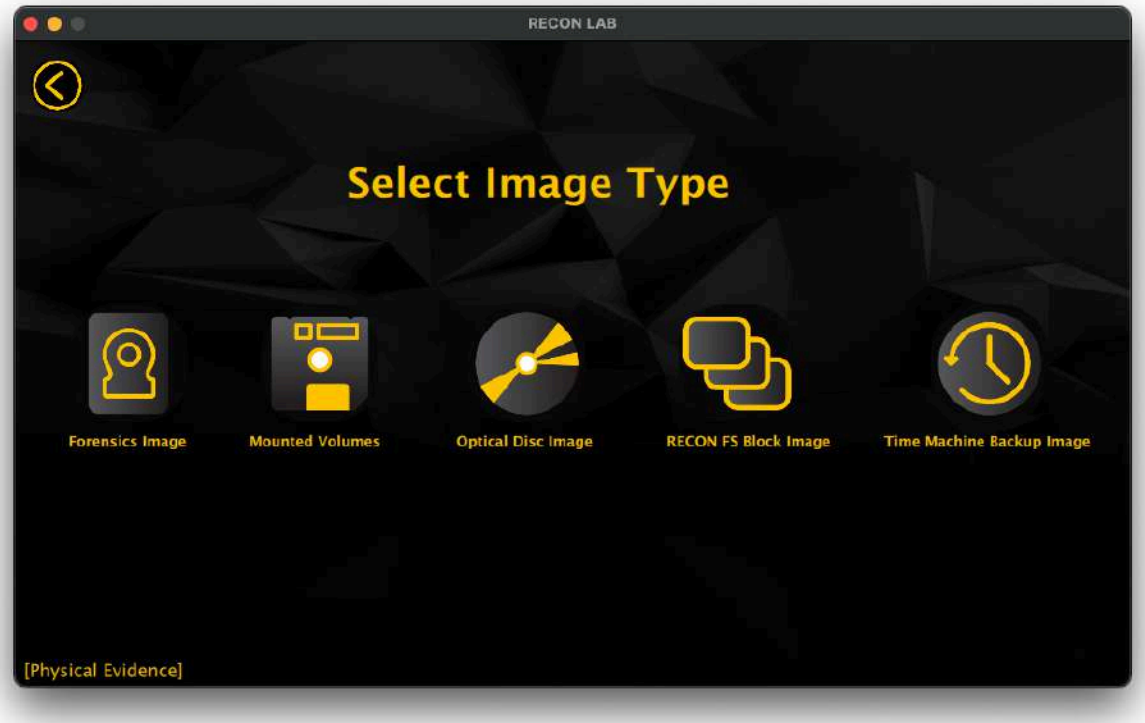
The Source tab allows the examiner to add a new source for processing. Sources must be correctly identified to ensure proper analysis within RECON LAB.

To add a source, use the Add Source menu and select the appropriate source type. Source types are divided into five categories, each with specific image format options. Choosing the correct category is essential, as it can affect how the data is interpreted and processed.

To add a source:

1. Click the Add Source button.
2. Select the appropriate source type from the available categories.
3. Follow the prompts based on the selected category to complete the source addition.

Physical Evidence



10.2.1.1 Forensics Image

- Use this option to add physical images. **This option refers specifically to full physical disk** acquisitions
- Select the operating system that the image pertains to.
- Additional fields for macOS physical images:
    - Image Path – File path of the image to be ingested.
    - Is FileVaulted – If the image was acquired while FileVault was locked, enter the admin or recovery key to decrypt the image.
    - Is Fusion – For Fusion Drives, add the SSD image first, then select the Is Fusion Drive option to pair it with the larger HDD image.
- Supported formats: .dd, .000, .00001, .raw, .dmg, .sparsebundle, .E01, .EX01, .LO1, .SO1, .AFF4.

10.2.1.2 Mounted Volumes

- Select from currently mounted volumes on the system.
- Useful for processing volumes directly connected to the examiner's machine.

10.2.1.3 Optical Disk Image

- Used to ingest optical disk images.
- Supported formats: .iso, .cdr.

10.2.1.4 RECON FS Block Image

- Add APFS container images created with RECON ITR.
- Supported formats: .dmg, .sparseimage.

10.2.1.5 Time Machine Backup Images

- Add physical images taken of a Time Machine backup drive.
- Supported formats: .dmg, .sparseimage.

Logical Evidence

- **10.2.2.1 Time Machine Backup Folder**
  - Used to add an image of the user's home directory for analysis.
- **10.2.2.2 macOS Home Directory**
  - Used to add an image of the user's home directory for analysis.
- **10.2.2.3 RECON Logical Image**
  - Used to add logical images acquired by RECON ITR.
  - Use this option when:
    - The image was taken with the **logical imager** in RECON ITR
    - The image was of an **APFS volume taken through Disk Imager in RECON ITR**
  - Supported formats: .dmg, .sparseimage, folder.
- **10.2.2.4 Encase Logical Image**
  - This option allows the examiner to add an Encase Logical Image
  - Supported format: .LO1.
- **10.2.2.5 Folder**
  - Use this option to add a directory from the system as a source.
- **10.2.2.6 File**
  - Select this option to add a single file as a source for processing.

Mobile Evidence

- **10.2.3.1 iTunes iOS Backup**
  - Used to add an iOS backup as a source.
  - Browse to and select the manifest.db database file to add the iTunes backup.
- **10.2.3.2 Cellebrite iOS Backup**
  - Supports ingesting Cellebrite UFED extractions in unencrypted .tar and .ufdr formats.
  - Supported formats: .tar, .ufdr.
- **10.2.3.3 GrayKey Backup**
  - Supports ingesting GrayKey backup images provided as .zip files.
- **10.2.3.4 ADB Android Backup**
  - Supports processing Android Debug Bridge (ADB) backups and files.
  - Supported formats: .ab backup file or folder.

Cloud Evidence

- **10.2.4.1 Google Takeout**
  - Used to add data downloaded from Google Takeout as a source.
  - Navigate to the directory containing the Google Takeout data to add it to the case.

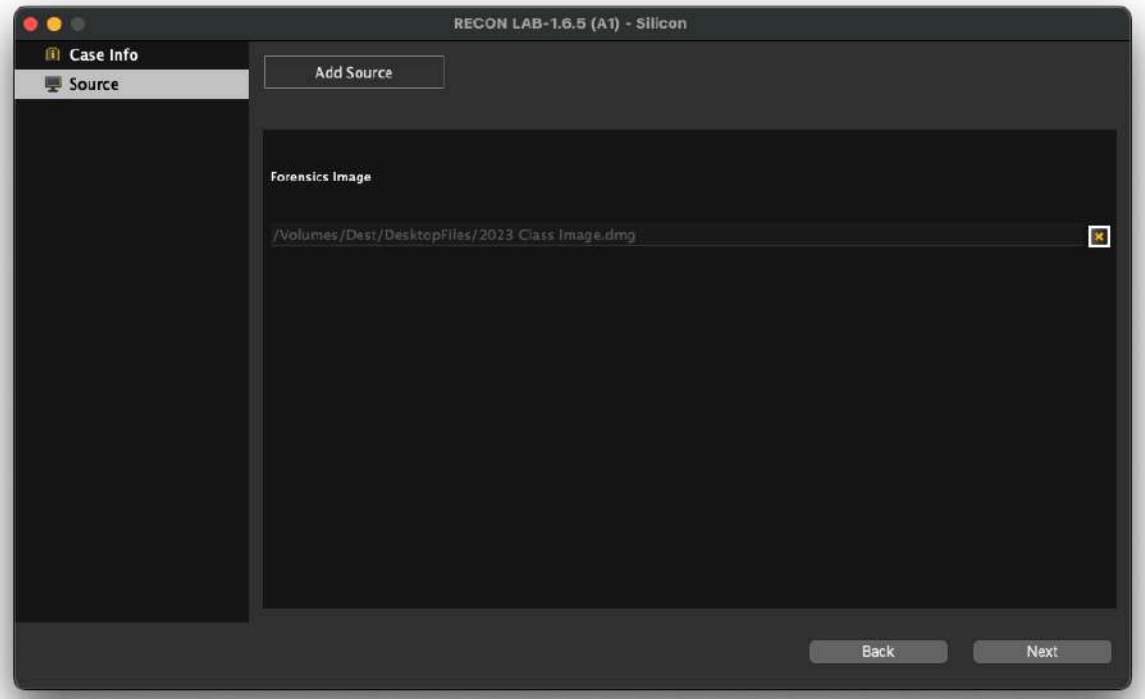
Network Acquisition

- **10.2.5.1 RECON MAC Sharing Mode**
  - Network Acquisition refers to acquisitions performed over a connection like SMB. RECON LAB currently supports one type of Network Acquisition, RECON MAC Sharing Mode.
  - Images that were taken in Target Share Mode on Silicon Macs, M1, M2, M3, etc.
  - Supported formats: DMG, Sparse Image, Folder

10.2.6 Adding Source Information

When adding a source, you can enter identifying details for the evidence to ensure proper documentation and processing. Some sources may also require a password to access specific artifacts within the image.

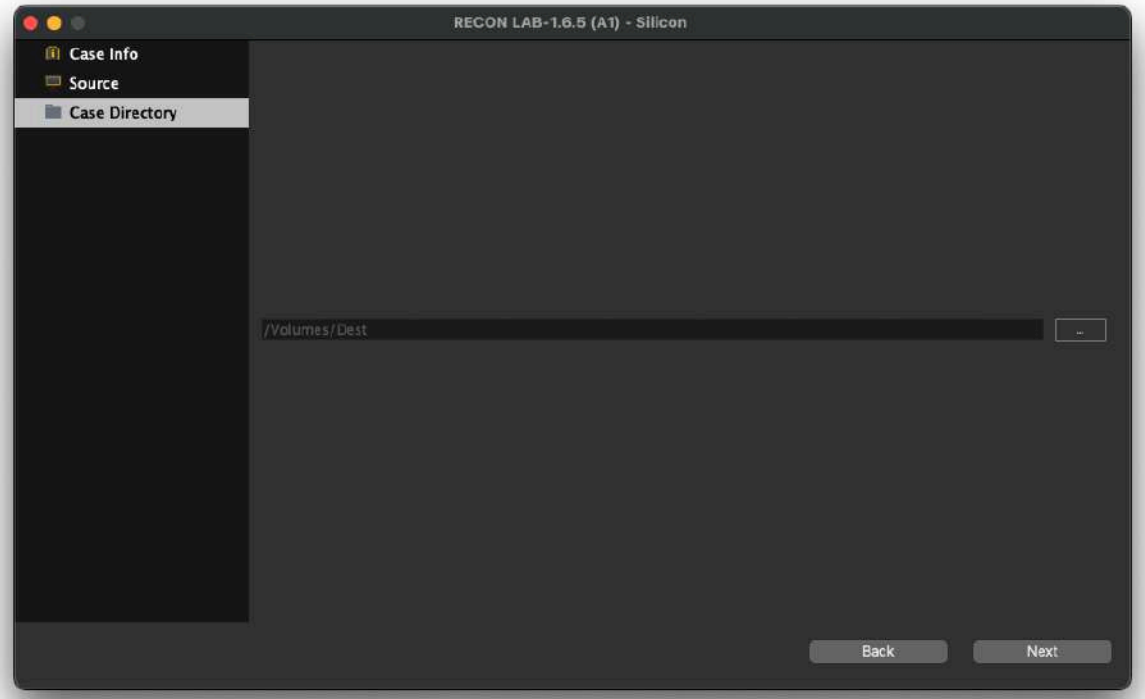
- Evidence No. – Enter a unique identifier for the piece of evidence.
- Description – Optional field to provide a brief description of the evidence.
- Source Password – If required, enter the admin password from the forensic image. This allows RECON LAB to access certain protected artifacts.



After selecting OK, additional sources can be added or removed as needed.

- **Add Source** – Click to add another source to the case.
- **X** Button – Click the X icon next to a listed source to remove it from the case.

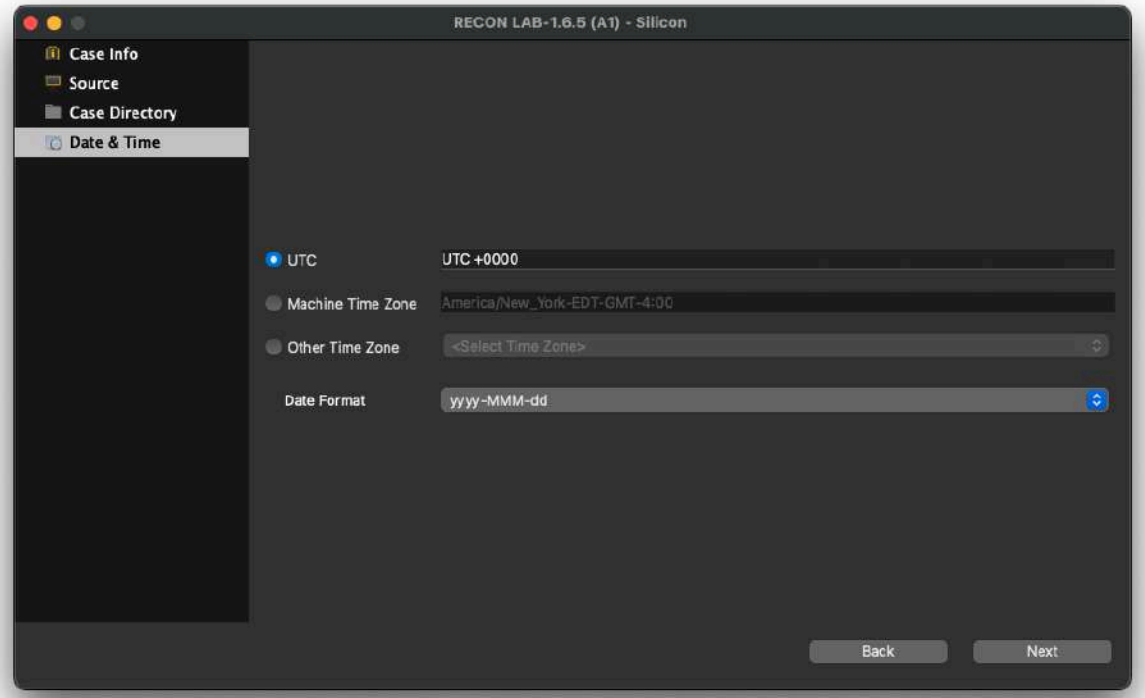
10.3 Case Directory



After adding your sources, you must choose a location for the RECON LAB Case Directory. This directory will store all case-related data and can grow significantly in size depending on the amount of processed data.

- Ensure there is sufficient available space on the selected drive.
- It is recommended to use a macOS Extended (HFS+) formatted drive for best compatibility and performance.

10.4 Date & Time



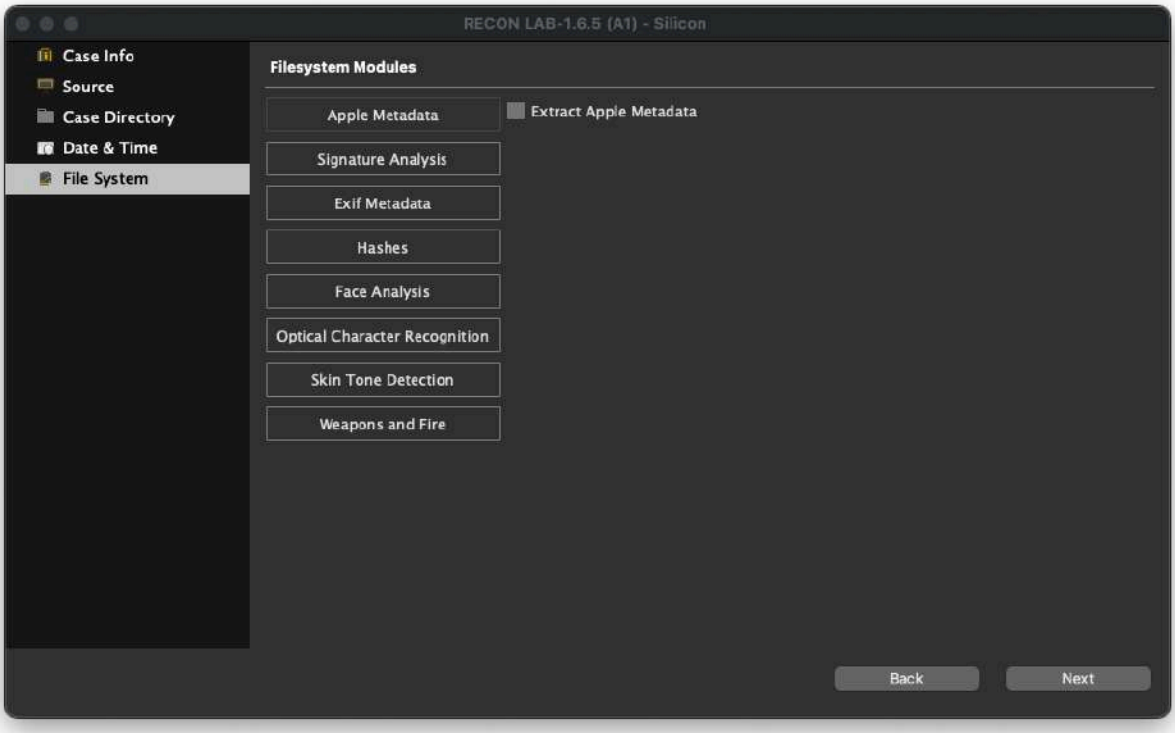
RECON LAB provides several options to configure how time and date information is displayed. These settings apply globally in the RECON LAB case.

- UTC – Sets the time zone to Coordinated Universal Time (+00:00).
- Machine Time Zone – Uses the time zone of the examiner's system, if detected.
- Other Time Zone – Allows manual selection of any global time zone from a dropdown menu.
- Date Format – Allows selection of a preferred date format to be used throughout RECON LAB.

10.5 File System

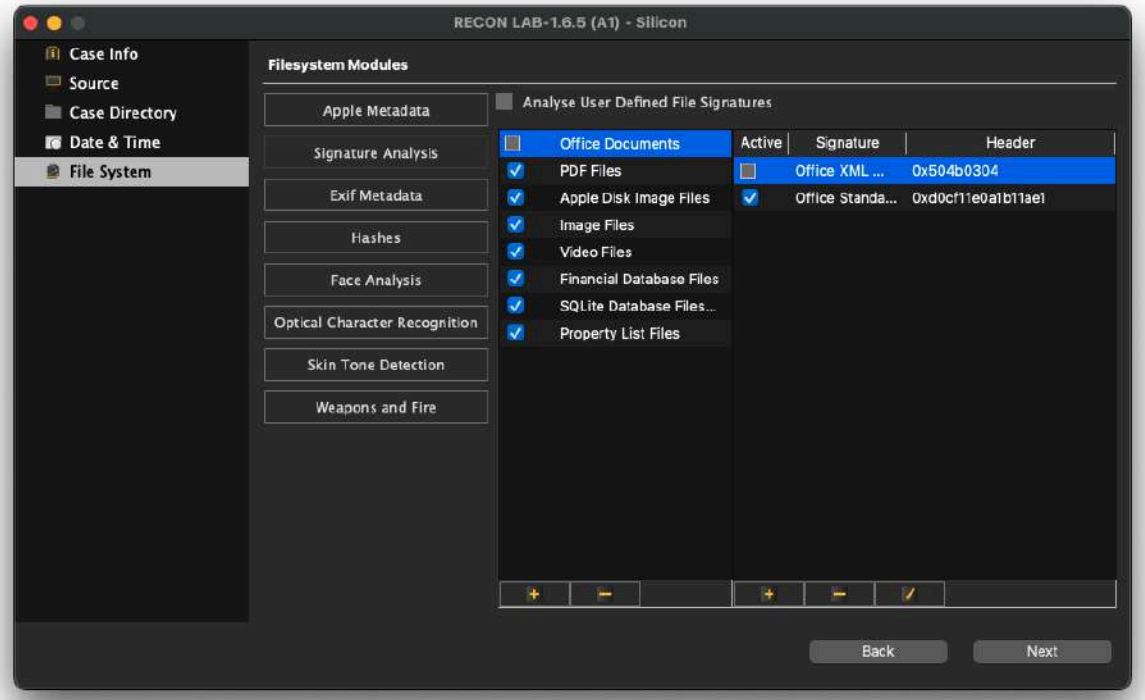
RECON LAB is designed to provide examiners with granular control over the processing of each case. Examiners can enable or disable individual File System Modules based on the specific needs of their investigation. By running only the necessary modules, processing time can be significantly reduced, improving overall efficiency.

10.5.1 Apple Metadata



To activate the Apple Metadata module for macOS sources, check the box next to Extract Apple Metadata. This enables the parsing of Apple Extended Metadata from the spotlight database within the source.

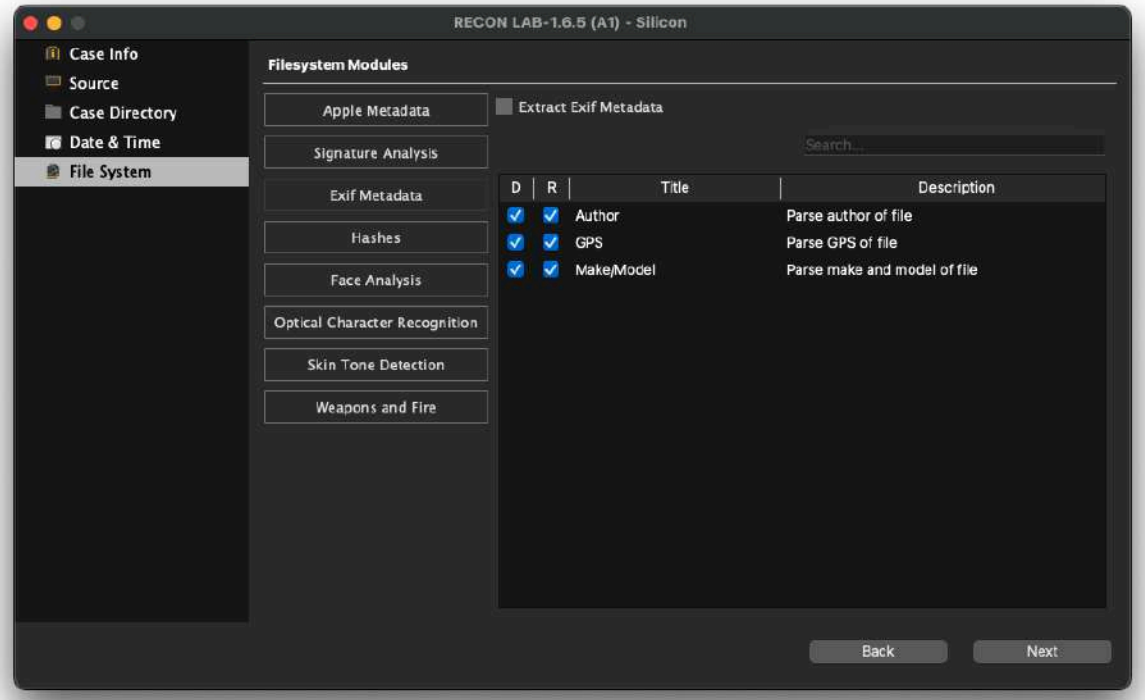
10.5.2 Signature Analysis



Selecting Analyse User Defined File Signatures runs a module that identifies files based on their headers (file signatures). These signatures can be added during the Case Wizard or previously in the RECON LAB Configuration.

For instructions on how to add or remove file signatures, please refer to the Configuration section of this manual.

10.5.3 Exif Metadata

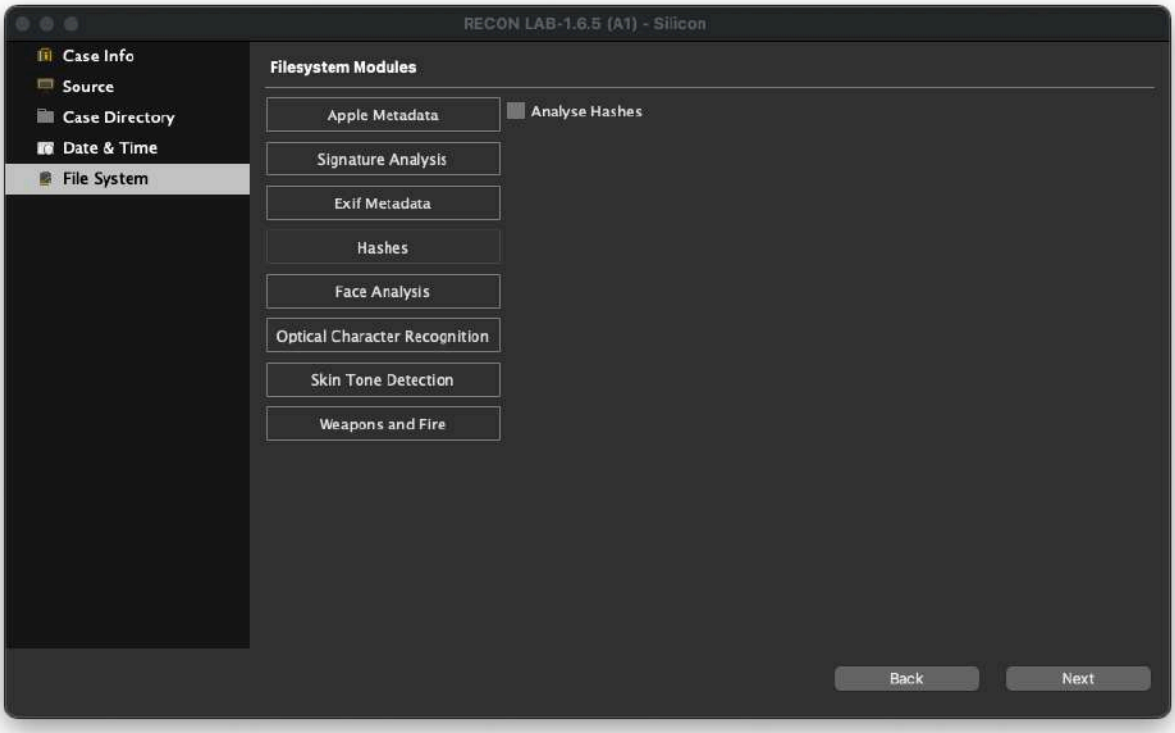


Selecting Extract Exif Metadata instructs RECON LAB to recover any EXIF metadata selected within this module. RECON LAB will also attempt to recover additional metadata not listed in the table above.

- **D** – Check this box to add the EXIF metadata to the RECON LAB Sidebar. Files matching the selected metadata will be automatically filtered and placed in the Sidebar.
- **R** – Check this box to include the selected EXIF metadata automatically in reports.
- **Title** – The common name of the EXIF metadata.
- **Description** – The official description of the EXIF metadata.

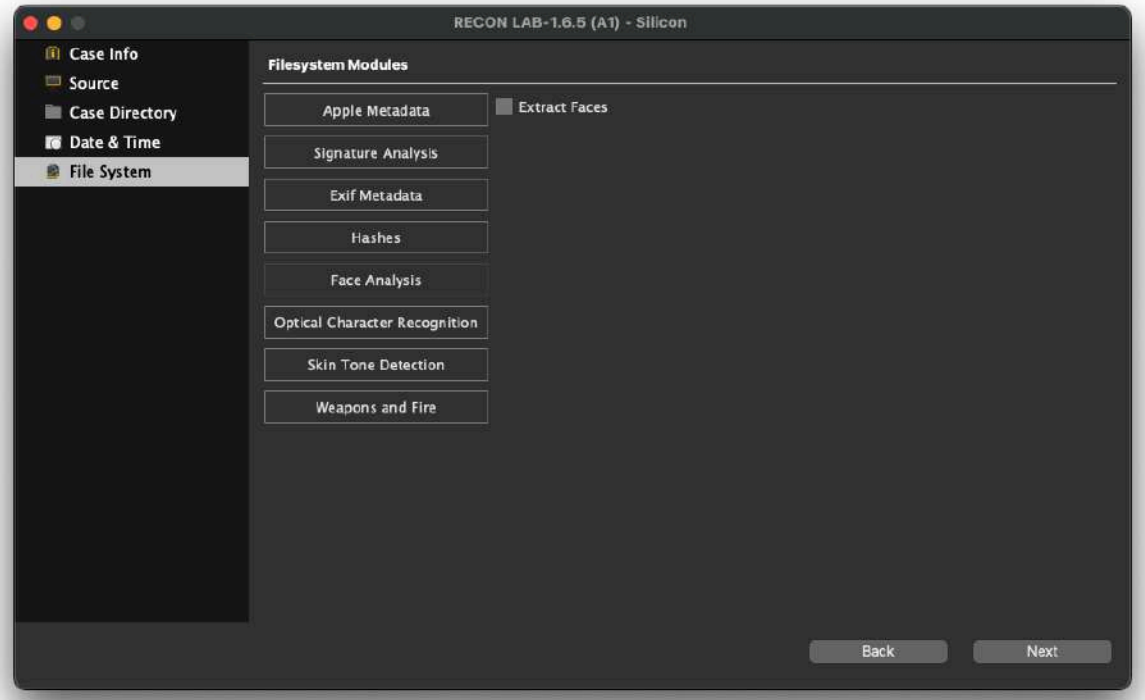
For instructions on configuring EXIF Metadata, please refer to the Configuration section of this manual.

10.5.4 Hashes



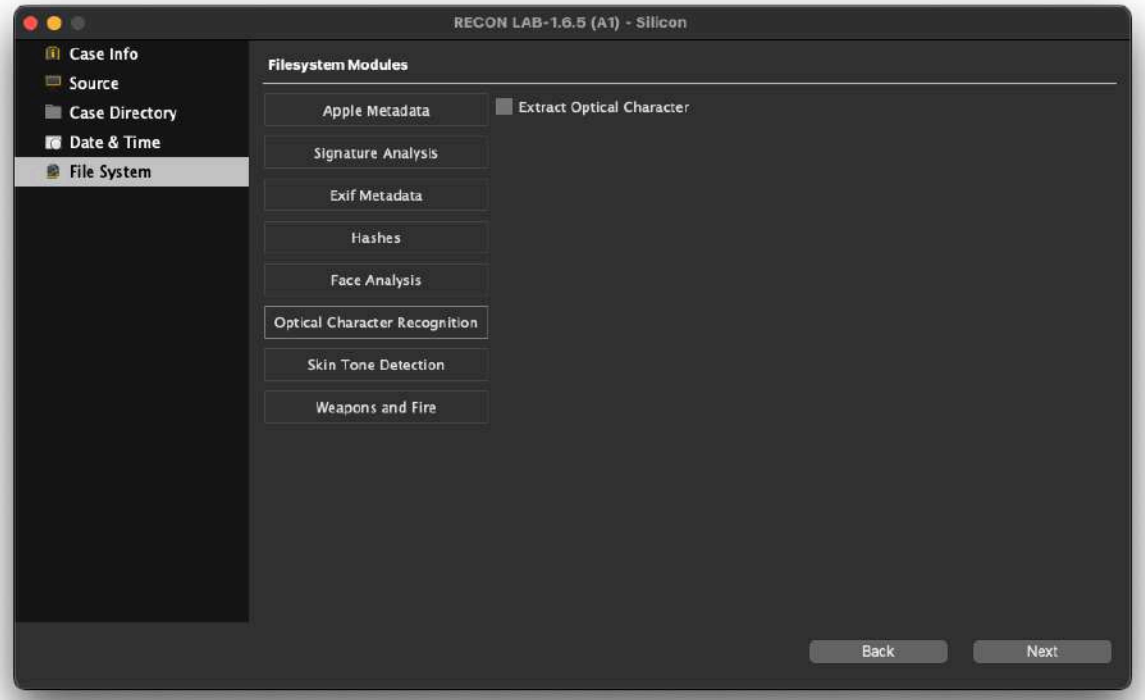
Check **Analyze Hashes** if you plan to use pre-configured hash sets during your investigation or analysis. RECON LAB will generate both SHA1 and MD5 hashes for all files within the selected sources.

10.5.5 Face Analysis



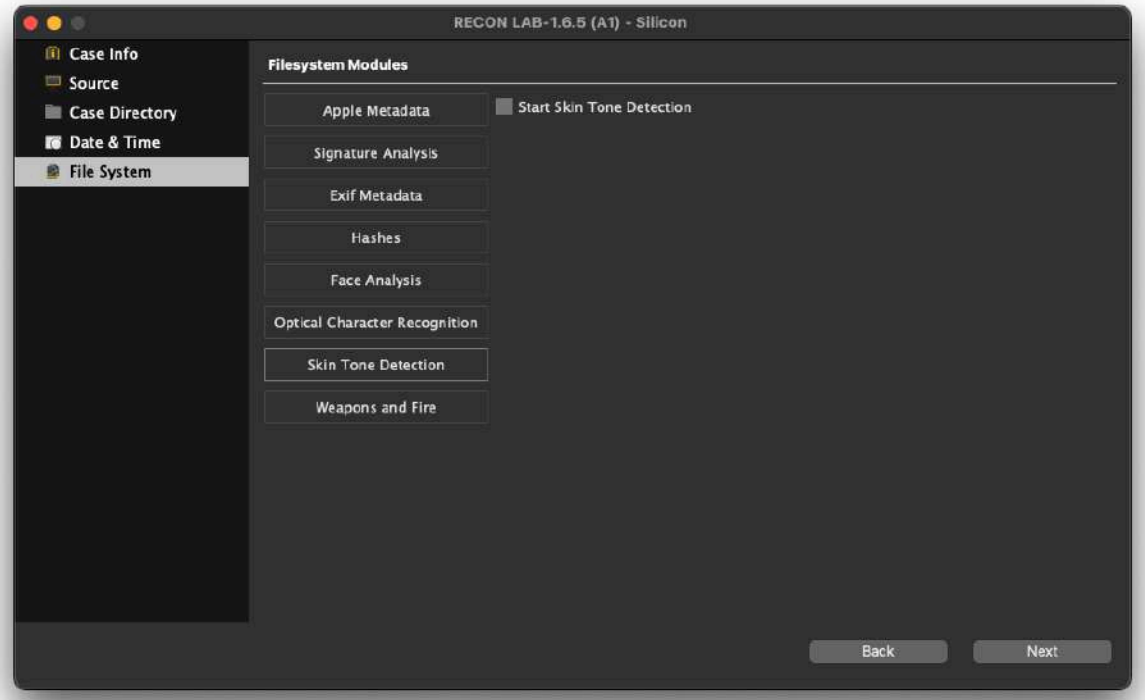
Face Analysis scans all image files on the selected source devices to identify and categorize faces by individual. This process can be time-consuming depending on the size of the source data.

10.5.6 Optical Character Recognition



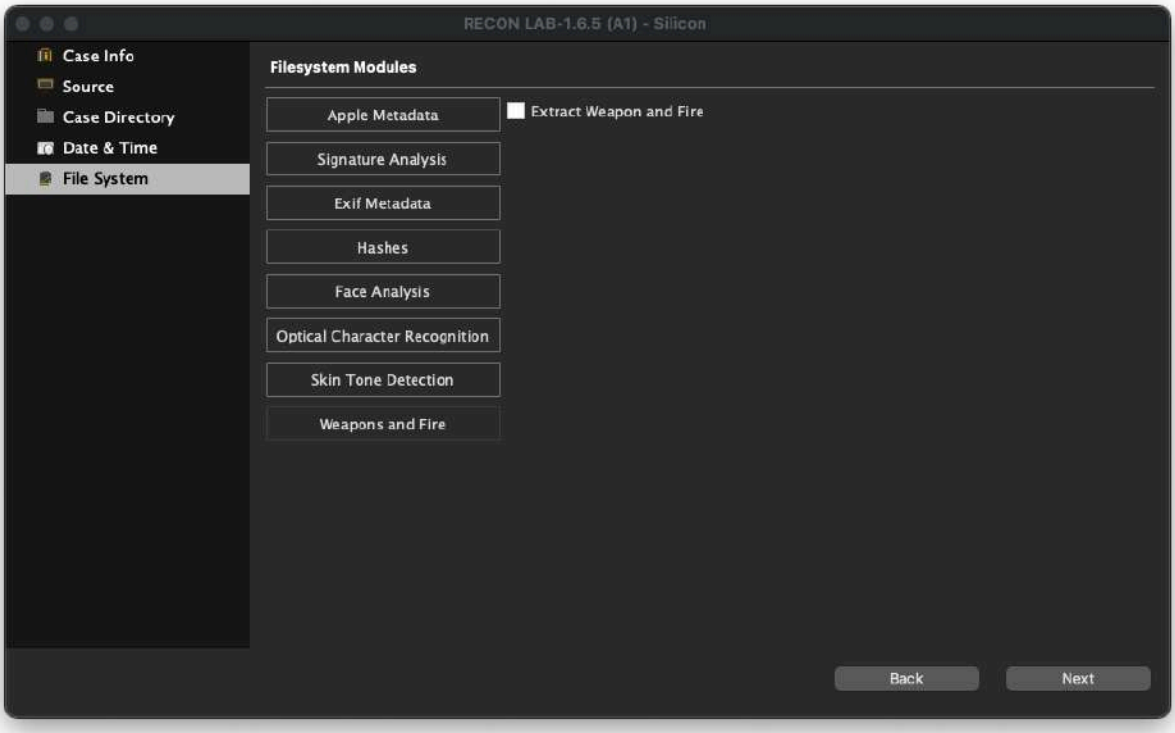
This feature scans source media files and attempts to extract text characters contained within those files using Optical Character Recognition (OCR) technology. Be aware that processing time may be lengthy depending on the size of the source data.

10.5.7 Skin Tone Detection



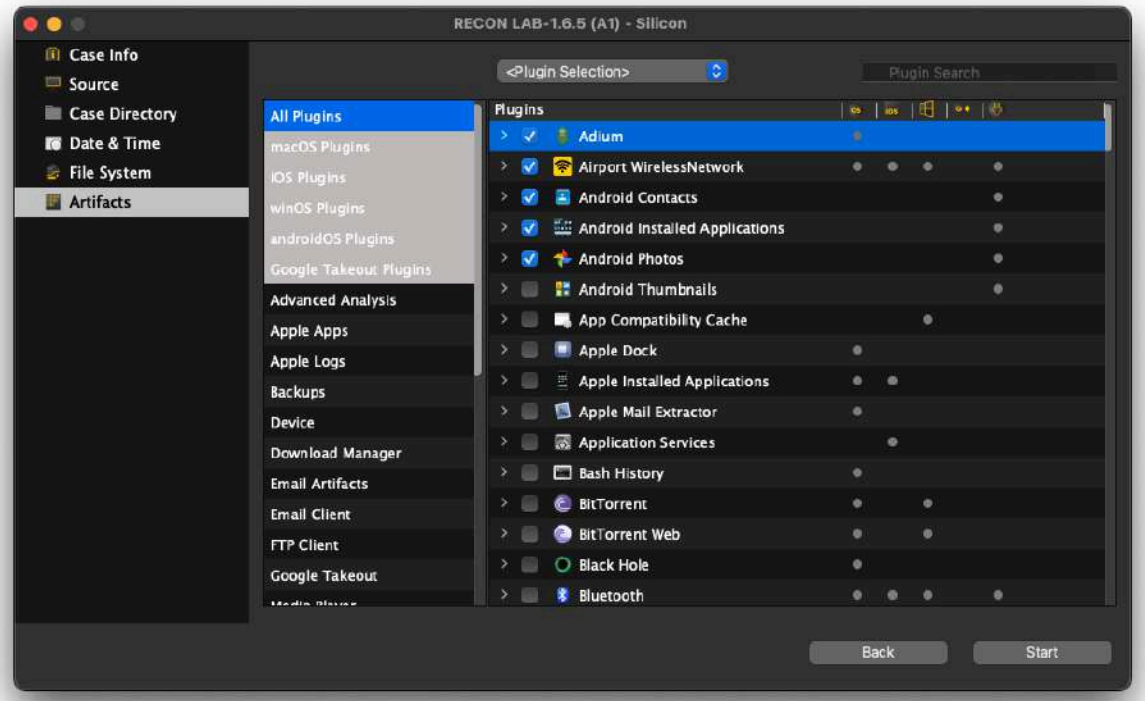
This module analyzes all image files on the selected source devices to identify media containing skin tones. Be aware that processing time may be lengthy depending on the size of the source data.

10.5.8 Weapons and Fire



This module analyzes all image files on the selected source devices to identify media containing weapons and fire. Please note that processing time may be lengthy depending on the size of the source data.

10.6 Artifacts



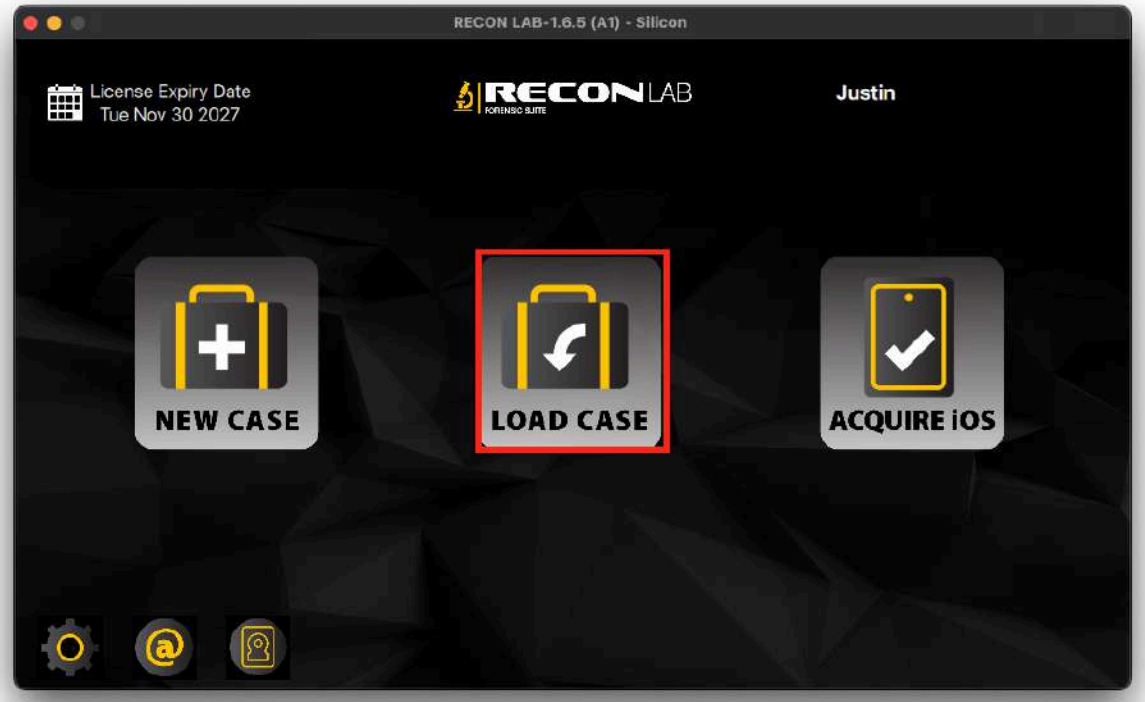
RECON LAB automatically processes and analyzes thousands of artifacts using hundreds of plugins for Windows, macOS, iOS, Android, and Google, as described in the Configuration section of this manual.

- Select individual artifacts to process by checking the box next to the plugin's name.
- Alternatively, choose a preset template from the Plugin Selection dropdown menu.

To begin processing all sources with the selected File System Modules and selected Artifact Analysis, click Start.

---

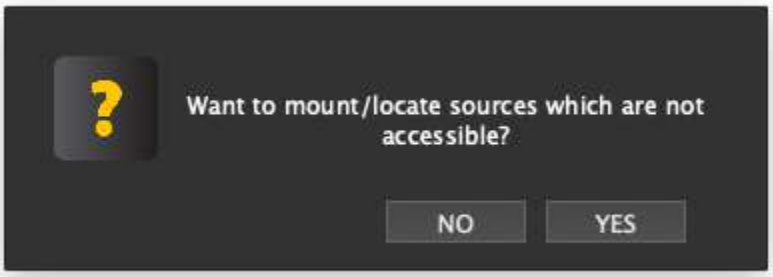
11 Loading a case



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

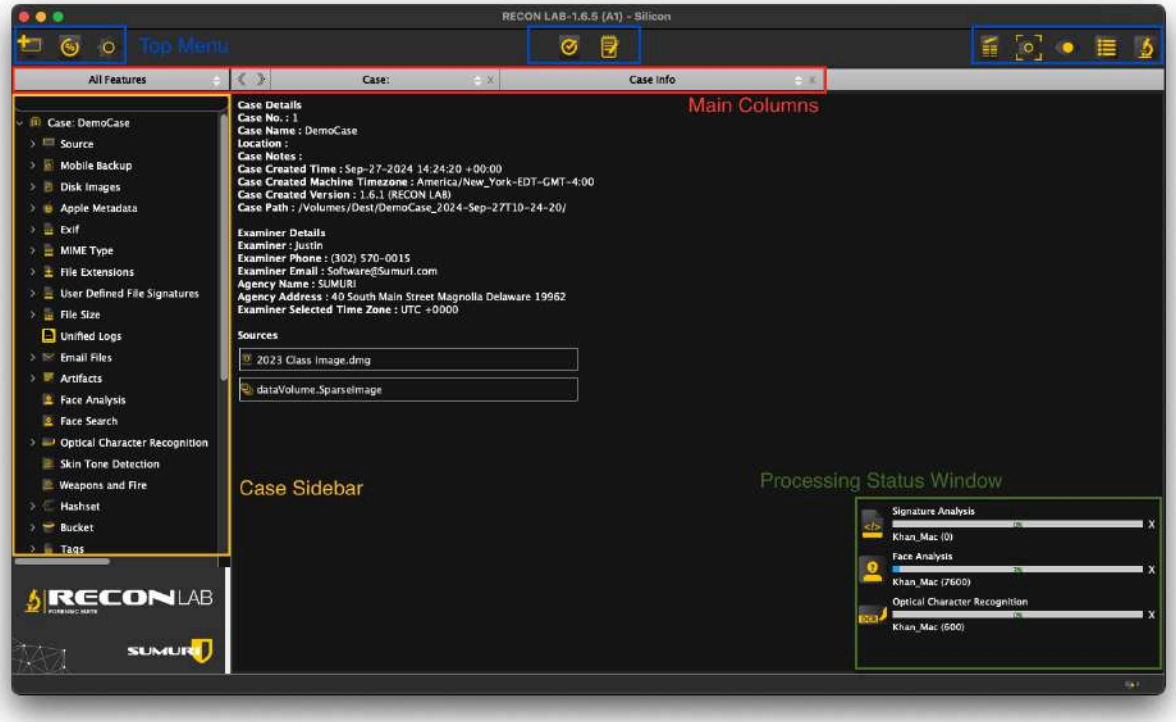
- A popup window will prompt you to navigate to the desired case folder and click Open.
- The case folder name follows the structure:
  Case Name-YYYY-MTH-DYTHH-MM-SC
  (e.g., Fraud_Investigation_2018-SEP-19T13-25-44)

Next, you will be asked whether to re-mount the original sources for the case.



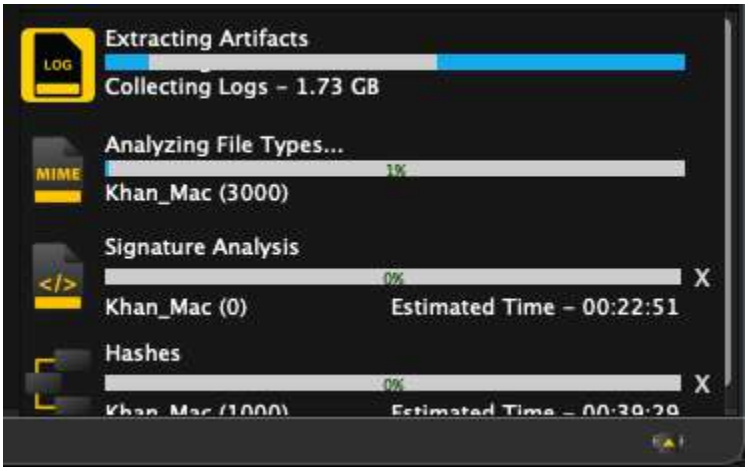
The sources must be re-mounted for RECON LAB to function properly. If the sources have been moved since the case was last opened, RECON LAB will prompt you to locate and reattach them.

12 RECON LAB Interface



The RECON LAB Main Interface is designed to be intuitive and simple to use, with the main window views dynamically changing based on the selected option.

12.1 Processing Status Window

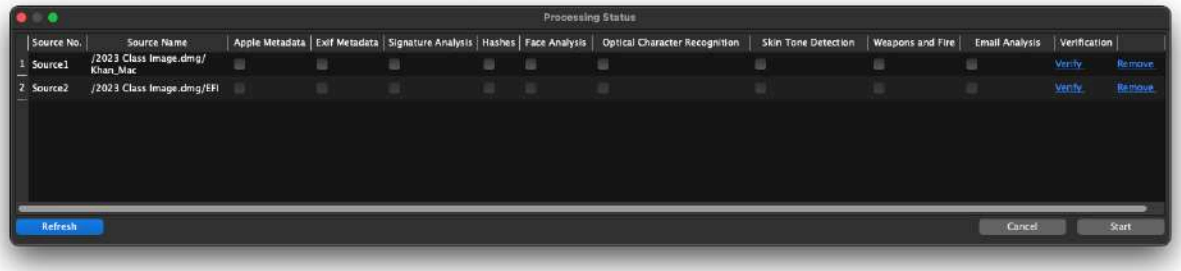


RECON LAB lets you start working within minutes by automatically running multiple tasks simultaneously, adjusting their workload based on available system resources to maximize efficiency. The first step is to add a source to the case, which is required before manual evidence review can begin. Almost immediately, automated artifact analysis starts extracting data and populating the Sidebar, allowing you to review results as soon as each plugin completes.

At the same time, RECON LAB begins parsing MIME Types. If selected, Apple Extended Timestamps are extracted for macOS file systems—these timestamps, unique to macOS, provide crucial forensic information that traditional POSIX (Unix) timestamps do not capture. RECON LAB, together with RECON IMAGER, is the only solution that properly captures and utilizes Apple Extended Metadata timestamps in a forensic context.

After the Apple Extended Timestamp extraction starts, RECON LAB proceeds with identifying and categorizing files by MIME type, followed by running the Apple Metadata, Signature Analysis, and EXIF Metadata modules. Finally, the Hashes module runs to create file hashes.

Each module's output becomes available immediately upon completion and can be reviewed right away. Modules can be canceled by clicking the "X" button, though it may take some time for them to fully stop. The Processing Status Window can be minimized by clicking the triangle icon in the bottom right corner.



To view the status of current or completed processes, click the % icon in the top menu bar. This opens the Processing Status Window.In this window, the examiner can:

- View the sources currently loaded in the case
- Review which processes have been run

- Run new processes on selected sources

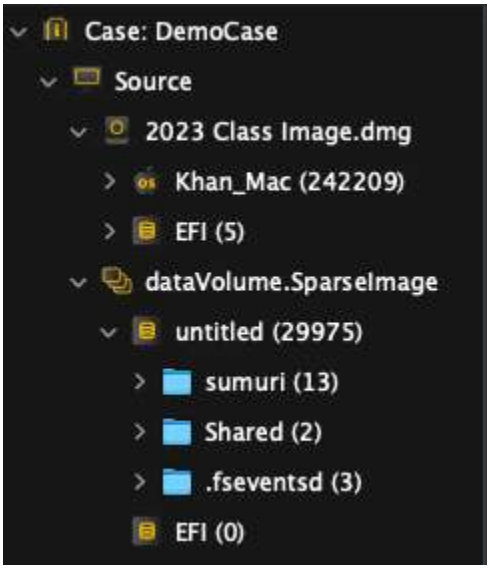
Running a Process

1. Check the box beneath the desired task.
2. Click Start to begin processing.

Available Actions

- Verify – Hashes the selected source to ensure data integrity.
- Remove – Removes the selected source from the case.

12.2 Case View



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

The Main Window displays key information about the case, including:

- Case Details
- Examiner Details
- Source Information

If a source contains multiple partitions, you can view them by clicking the main source item (e.g., “2023 Class Image.dmg”). Selecting an individual partition will display additional details, such as the operating system version.

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

The interface top menu comprises 10 icons, providing examiners with quick access to key case management functions:

1. Add Source – Add additional sources after the case has begun.
2. Processing Status – Displays all added sources and the status of modules run against them; sources can also be removed.
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 – Enables examiners to take notes relevant to their case, which can be added to reports.
7. Screenshot – Allows capturing screenshots to include in reports.
8. Quick Look – Activates the native macOS file viewer supporting hundreds of file types.
9. Show/Hide Sidebar – Toggles the Sidebar visibility.
10. Show Detailed Information – Toggles the Detailed Information Window visibility.

12.3.2 macOS Menu Bar

RECON LAB uses the macOS Menu Bar to organize the interface into five main categories, making navigation user-friendly and efficient. These categories provide quick access to various features related to processing, searching, timelines, exporting, and reporting:

12.3.2.1 Process

1. Run Artifacts – Launches the Artifacts and Plugins module for automated analysis.
2. Text Indexing – Enables indexing of files and directories.
3. Hash Sets – Allows creation or importing of hash sets.

12.3.2.2 Search

1. File Search – Locate files using criteria like timestamps, names, extensions, and sizes.
2. Content Search – Opens a configuration window for keyword searches.
3. EXIF Metadata Search – Search files based on EXIF metadata.
4. Apple Metadata Search – Search files using Apple Extended Metadata.
5. Artifacts Keyword Search – Quickly search all parsed artifacts by keyword.
6. Recognize Face – Search the indexed faces, for a selected face.

12.3.2.3 Timeline

1. Artifacts Timeline – Generate timelines and graphs from artifact timestamps.
2. Super Timeline – Create enhanced timelines using all available timestamps from files and artifacts.

12.3.2.4 Export

1. Tagged File Export – Export files that have been tagged or bookmarked.
2. Export Case – Export a portable case version compatible with Windows systems

12.3.2.5 Report

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.

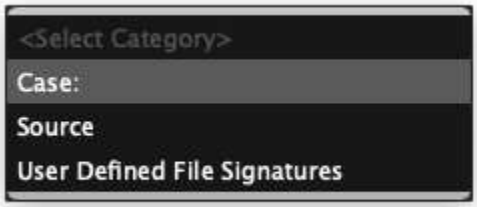
When you navigate to different modules or views these columns will keep a history of these. Clicking on the columns will allow you to return to a previous module or view.

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

12.4.0.1 Sidebar Column

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

12.4.0.2 Select Category Column

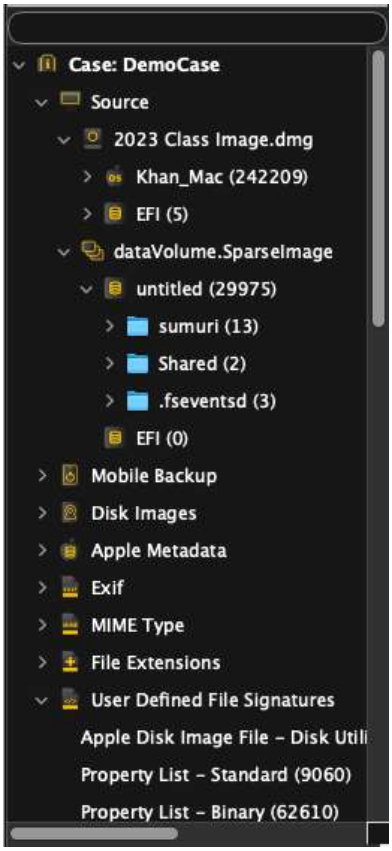


The Select Category Column keeps a history of modules and sources previously viewed. Clicking the title of the column will show previous items. Select any item to return to the module or source.

12.4.0.3 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.

12.5.1 Case Sidebar Options

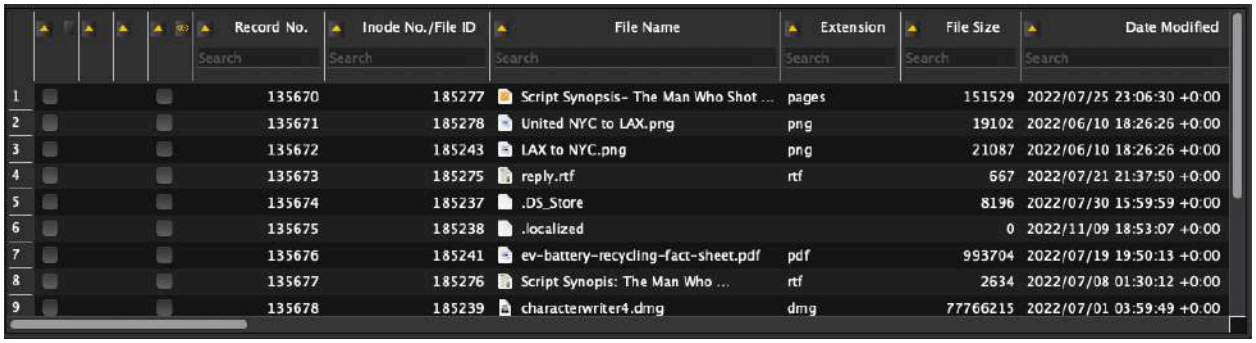
The RECON LAB interface is organized into several key tabs, each designed to provide you with focused access to different aspects of your digital investigation. This section outlines the purpose and functionality of these tabs.

- **Source**: This tab displays a comprehensive list of all data sources currently added to the active case.
- **Mobile Backup**: Here, you will find a list of all mobile backups identified within any macOS source images. This tab allows you to add these identified backups as individual sources for analysis.
- **Disk Images**: This tab lists all disk images detected within your added sources. From here, you can select and add these disk images as new sources to your case.
- **Apple Metadata**: This tab displays the parsed results from the Apple Metadata Process. The specific categories of Apple Metadata shown here are configurable within the application's settings.

- **Exif**: This tab presents the parsed Exif Metadata extracted from relevant files. The display format and specific Exif fields shown can be customized in the Configuration settings.
- **MIME Type**: Upon adding a source, this tab automatically populates, categorizing files based on their detected MIME type.
- **File Extensions**: Similar to MIME Type, this tab automatically organizes files by their file extension as soon as a source is added. The specific file extensions displayed can be configured within the application settings.
- **User Defined File Signatures**: After running the Signature Analysis process, this tab will list files categorized according to user-defined file signatures. You can manage and configure these signatures within the application.
- **File Size**: This tab automatically categorizes files based on their size.
- **Unified Logs**: Following the execution of the Unified Logs process, this tab will display a detailed list of the extracted logs.
- **Email Files**: This tab opens the integrated email viewer, displaying all identified email files from the analyzed sources. This process runs automatically.
- **Artifacts**: This tab provides a list of all artifacts that have been processed. Only artifacts containing identified records will be displayed here.
- **Face Analysis**: When the Face Analysis feature is utilized, this tab will display all parsed and identified faces within the analyzed data.
- **Face Search**: This tab lists all face searches that have been performed using the Face Search functionality.
- **Optical Character Recognition**: After running the OCR module, this tab will contain any files where text was successfully identified and extracted.
- **Skin Tone Detection**: If the Skin Tone Detection module is run, this tab will display files identified as containing skin tones.
- **Weapons and Fire**: Following the execution of the Weapons and Fire module, this tab will list any files identified as potentially containing images of weapons or fire.
- **Hashset**: This tab displays the currently configured hashsets. You can manage and configure hashsets through this interface.
- **Bucket**: This dropdown menu lists any files that have been manually sent to user-defined buckets for organization or further review.
- **Tags**: This tab provides a list of all files and records that have been bookmarked or tagged for specific attention.
- **Notes**: This tab keeps track of all notes that have been added to individual files and records within the case.
- **File Search**: This tab maintains a history of all file searches performed using the File Search feature.
- **Artifacts Keyword Search**: This tab displays the results of each Artifact Keyword Search that has been conducted.
- **Content Search**: This tab lists all Content Searches that have been performed on the data.
- **Exif Metadata Search**: This tab provides a record of all searches conducted on Exif metadata.
- **Artifacts Timeline**: This tab displays any timeline artifacts that have been generated from the processed data.
- **Redefined Results**: This tab displays various categories of parsed artifacts that have been reprocessed or refined for more specific analysis.
- **Saved Redefined Result**: This tab lists any redefined analysis results that have been saved within the application.
- **Screenshots**: This tab contains a list of any screenshots that have been captured and saved within the application during the analysis process.

- **Story Board**: This tab displays a list of any storyboard reports that have been generated.
- **Saved Graph Results**: This tab lists any data visualizations or graphs that have been created and saved within the application.
- **Saved Maps**: This tab displays any geographical maps that have been generated and saved.

12.6 Main Viewer Window



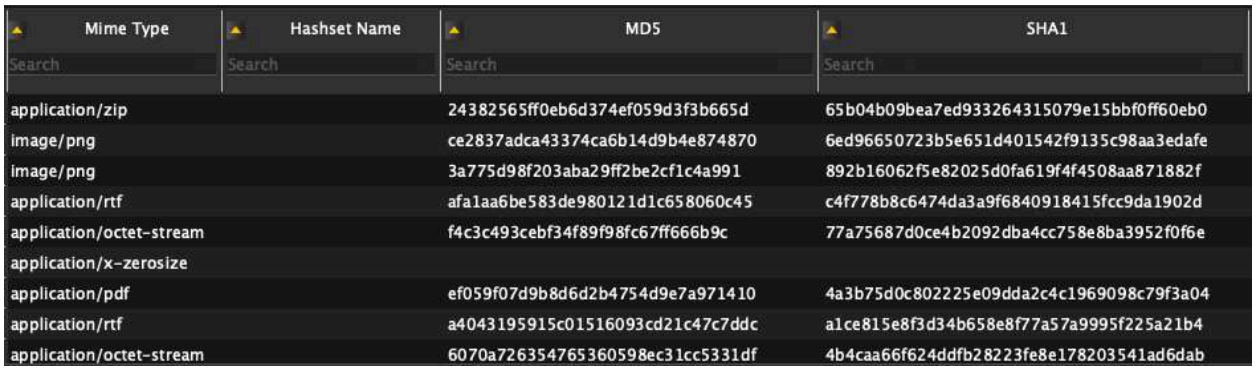
	Record No.	Inode No./File ID	File Name	Extension	File Size	Date Modified
1	135670	185277	Script Synopsis- The Man Who Shot ...	pages	151529	2022/07/25 23:06:30 +0:00
2	135671	185278	United NYC to LAX.png	png	19102	2022/06/10 18:26:26 +0:00
3	135672	185243	LAX to NYC.png	png	21087	2022/06/10 18:26:26 +0:00
4	135673	185275	reply.rtf	rtf	667	2022/07/21 21:37:50 +0:00
5	135674	185237	.DS_Store		8196	2022/07/30 15:59:59 +0:00
6	135675	185238	.localized		0	2022/11/09 18:53:07 +0:00
7	135676	185241	ev-battery-recycling-fact-sheet.pdf	pdf	993704	2022/07/19 19:50:13 +0:00
8	135677	185276	Script Synopis: The Man Who ...	rtf	2634	2022/07/08 01:30:12 +0:00
9	135678	185239	characterwriter4.dmg	dmg	77766215	2022/07/01 03:59:49 +0:00

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.

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.

In the table, the different columns are:

- 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
application/zip		24382565ff0eb6d374ef059d3f3b665d	65b04b09bea7ed933264315079e15bbf0ff60eb0
image/png		ce2837adca43374ca6b14d9b4e874870	6ed96650723b5e651d401542f9135c98aa3edafe
image/png		3a775d98f203aba29ff2be2cf1c4a991	892b16062f5e82025d0fa619f4f4508aa871882f
application/rtf		afa1aa6be583de980121d1c658060c45	c4f778b8c6474da3a9f6840918415fcc9da1902d
application/octet-stream		f4c3c493cebf34f89f98fc67ff666b9c	77a75687d0ce4b2092dba4cc758e8ba3952f0f6e
application/x-zerosize			
application/pdf		ef059f07d9b8d6d2b4754d9e7a971410	4a3b75d0c802225e09dda2c4c1969098c79f3a04
application/rtf		a4043195915c01516093cd21c47c7ddc	a1ce815e8f3d34b658e8f77a57a9995f225a21b4
application/octet-stream		6070a726354765360598ec31cc5331df	4b4caa66f624ddfb28223fe8e178203541ad6dab

- 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

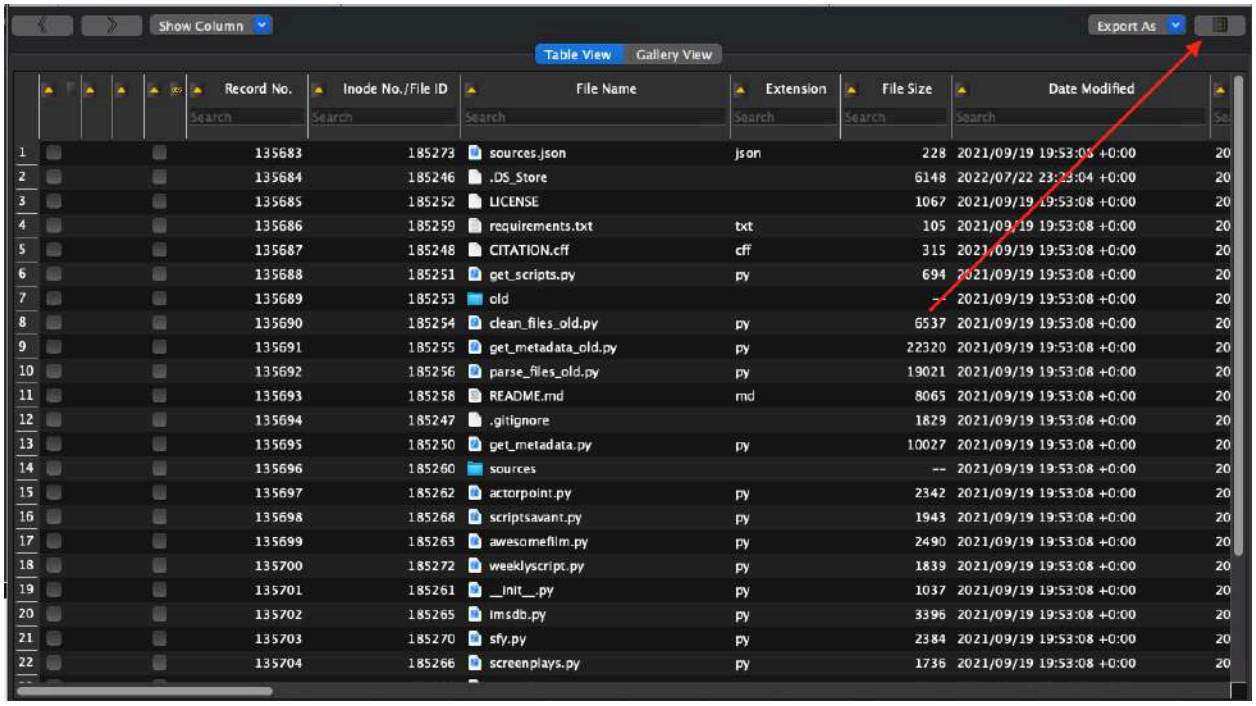
- Date Modified – Standard timestamp for Date Modified.
- Date Change – Standard timestamp for Date Changed.
- Date Accessed – Standard timestamp for Date Accessed.

Last Used Date	Use Count	Date Added	Content Creation Date	Content Modification Date
2022/07/28 01:30:01 +0:00	1	2022/12/06 22:58:31 +0:00	2022/07/25 23:06:30 +0:00	2022/07/25 23:06:30 +0:00
		2022/12/06 22:58:31 +0:00	2022/06/10 18:26:26 +0:00	2022/06/10 18:26:26 +0:00
		2022/12/06 22:58:31 +0:00	2022/06/10 18:26:26 +0:00	2022/06/10 18:26:26 +0:00
2022/07/27 14:21:02 +0:00	1	2022/12/06 22:58:31 +0:00	2022/07/21 21:37:50 +0:00	2022/07/21 21:37:50 +0:00
		2022/12/06 22:58:31 +0:00	2022/07/19 19:50:13 +0:00	2022/07/19 19:50:13 +0:00
2022/07/20 02:03:26 +0:00	1	2022/12/06 22:58:31 +0:00	2022/07/08 01:30:12 +0:00	2022/07/08 01:30:12 +0:00
		2022/12/06 22:58:30 +0:00	2022/07/01 03:59:49 +0:00	2022/07/01 03:59:49 +0:00

- 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

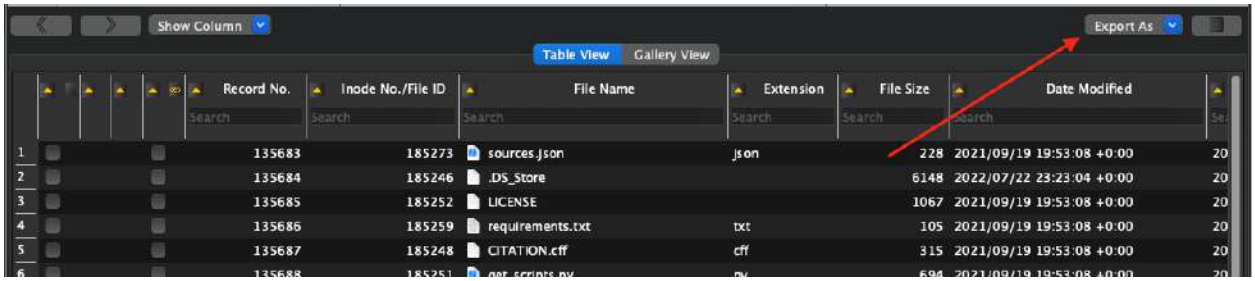
12.6.1.1 Recursive View



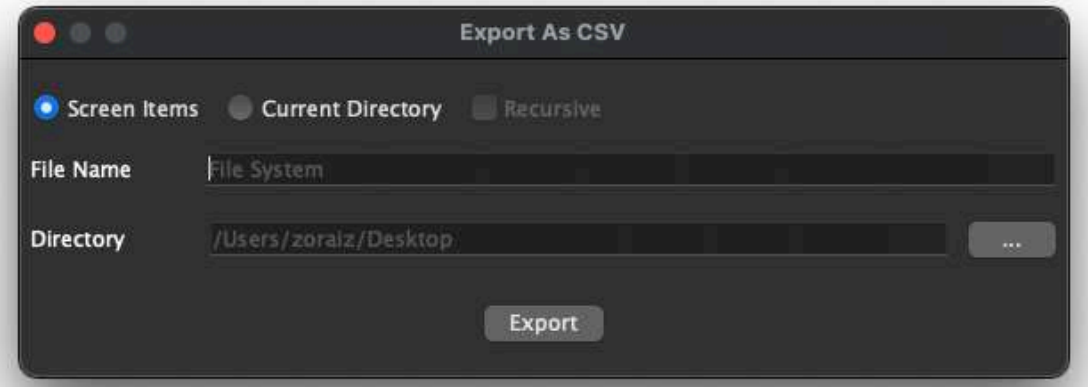
	Record No.	Inode No./File ID	File Name	Extension	File Size	Date Modified
1	135683	185273	sources.json	json	228	2021/09/19 19:53:08 +0:00
2	135684	185246	.DS_Store		6148	2022/07/22 23:23:04 +0:00
3	135685	185252	LICENSE		1067	2021/09/19 19:53:08 +0:00
4	135686	185259	requirements.txt	txt	105	2021/09/19 19:53:08 +0:00
5	135687	185248	CITATION.cff	cff	315	2021/09/19 19:53:08 +0:00
6	135688	185251	get_scripts.py	py	694	2021/09/19 19:53:08 +0:00
7	135689	185253	old		--	2021/09/19 19:53:08 +0:00
8	135690	185254	clean_files_old.py	py	6537	2021/09/19 19:53:08 +0:00
9	135691	185255	get_metadata_old.py	py	22320	2021/09/19 19:53:08 +0:00
10	135692	185256	parse_files_old.py	py	19021	2021/09/19 19:53:08 +0:00
11	135693	185258	README.md	md	8065	2021/09/19 19:53:08 +0:00
12	135694	185247	.gitignore		1829	2021/09/19 19:53:08 +0:00
13	135695	185250	get_metadata.py	py	10027	2021/09/19 19:53:08 +0:00
14	135696	185260	sources		--	2021/09/19 19:53:08 +0:00
15	135697	185262	actorpoint.py	py	2342	2021/09/19 19:53:08 +0:00
16	135698	185268	scriptsavant.py	py	1943	2021/09/19 19:53:08 +0:00
17	135699	185263	awesomefilm.py	py	2490	2021/09/19 19:53:08 +0:00
18	135700	185272	weeklyscript.py	py	1839	2021/09/19 19:53:08 +0:00
19	135701	185261	__init__.py	py	1037	2021/09/19 19:53:08 +0:00
20	135702	185265	imsdb.py	py	3396	2021/09/19 19:53:08 +0:00
21	135703	185270	sfy.py	py	2384	2021/09/19 19:53:08 +0:00
22	135704	185266	screenplays.py	py	1736	2021/09/19 19:53:08 +0:00

The Recursive View feature will recursively expand any subdirectories in the current view. This is frequently done prior to creating a full file listing. To expand all directories recursively, click the Recursive View button.

12.6.1.2 Export to CSV



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”.

Download_Files.csv — Open with Numbers

Sr. No	Inode No./File ID	File Name	Extension	File Path	File Size (Bytes)	File Size (Units)
1	185273	sources.json	json	/Users/thewrath/Downloads/Movie-Script-Database-master/sources.json	228	228 B
2	185246	.DS_Store		/Users/thewrath/Downloads/Movie-Script-Database-master/.DS_Store	6148	6.00 KB
3	185252	LICENSE		/Users/thewrath/Downloads/Movie-Script-Database-master/LICENSE	1067	1.04 KB
4	185259	requirements.txt	txt	/Users/thewrath/Downloads/Movie-Script-Database-master/requirements.txt	105	105 B
5	185248	CITATION.cff	cff	/Users/thewrath/Downloads/Movie-Script-Database-master/CITATION.cff	315	315 B
6	185251	get_scripts.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/get_scripts.py	694	694 B
7	185253	old		/Users/thewrath/Downloads/Movie-Script-Database-master/old	--	0 B
8	185254	clean_files_old.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/old/clean_files_old.py	6537	6.38 KB
9	185255	get_metadata_old.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/old/get_metadata_old.py	22320	21.80 KB
10	185256	parse_files_old.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/old/parse_files_old.py	19021	18.58 KB
11	185258	README.md	md	/Users/thewrath/Downloads/Movie-Script-Database-master/README.md	8065	7.88 KB
12	185247	.gitignore		/Users/thewrath/Downloads/Movie-Script-Database-master/.gitignore	1829	1.79 KB
13	185250	get_metadata.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/get_metadata.py	10027	9.79 KB
14	185260	sources		/Users/thewrath/Downloads/Movie-Script-Database-master/sources	--	0 B
15	185262	actorpoint.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/actorpoint.py	2342	2.29 KB
16	185268	scriptsavant.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/scriptsavant.py	1943	1.90 KB
17	185263	awesomefilm.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/awesomefilm.py	2490	2.43 KB
18	185272	weeklyscript.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/weeklyscript.py	1839	1.80 KB
19	185261	__init__.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/__init__.py	1037	1.01 KB
20	185265	imsdb.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/imsdb.py	3396	3.32 KB
21	185270	sfy.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/sfy.py	2384	2.33 KB
22	185266	screenplays.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/screenplays.py	1736	1.70 KB
23	185269	scriptslug.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/scriptslug.py	2184	2.13 KB
24	185267	scriptpdf.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/scriptpdf.py	2032	1.98 KB
25	185271	utilities.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/utilities.py	2077	2.03 KB
26	185264	dailyscript.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/sources/dailyscript.py	2523	2.46 KB
27	185257	parse_files.py	py	/Users/thewrath/Downloads/Movie-Script-Database-master/parse_files.py	25396	24.80 KB

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. 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.

Table View Filter and Search

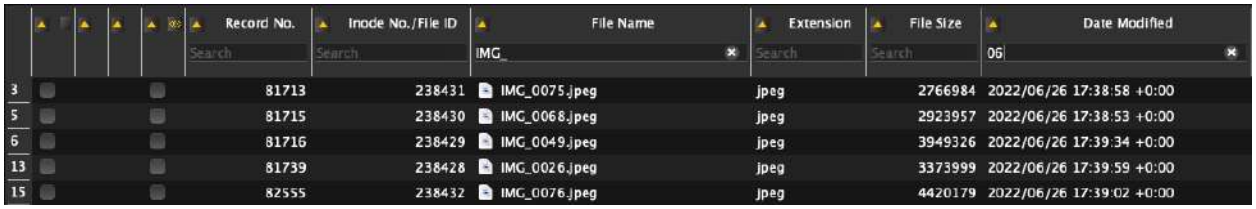
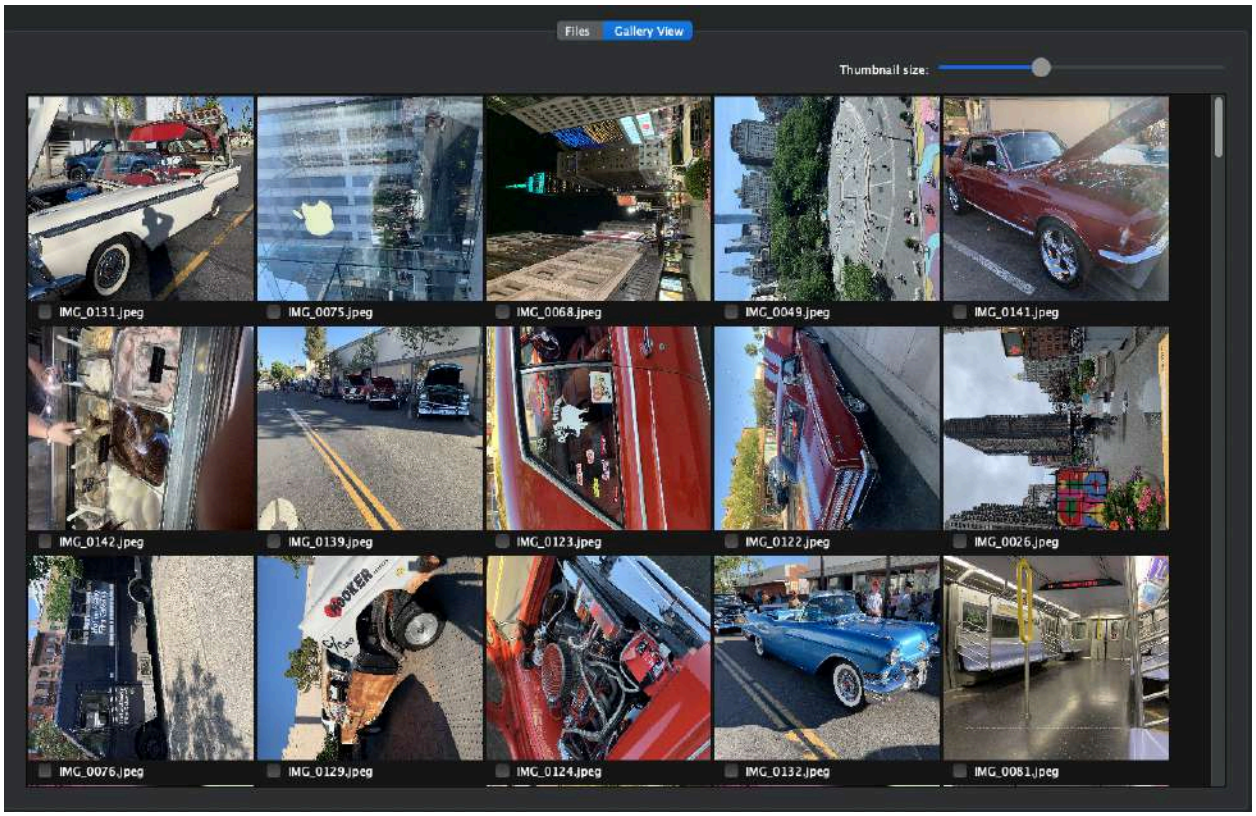


Table View includes a search feature with filters. These filters will be located above the search table column.

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.

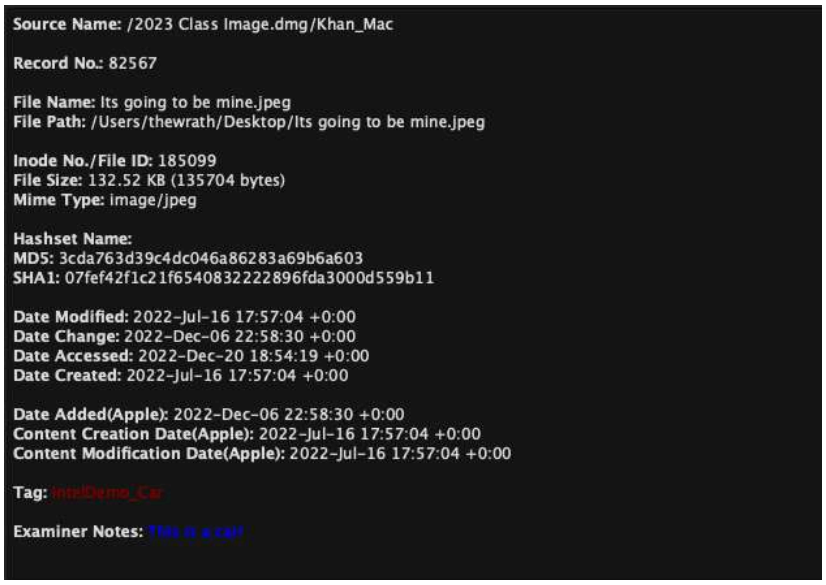
Pictures will be displayed as a thumbnail. Selecting the checkbox next to the image name will bookmark the file. Right-clicking on the picture file will present additional options (discussed later in this manual).

12.7 Viewer Panes

RECON LAB has multiple viewer panes to assist with presenting additional information or views of files. The following views available are:

- Detailed Information – Shows the location of a file within the source, dates and times, examiner's notes and more.
- Optical Character Recognition – Shows the extracted OCR text
- 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.
- Preview – Shows a preview of a media file

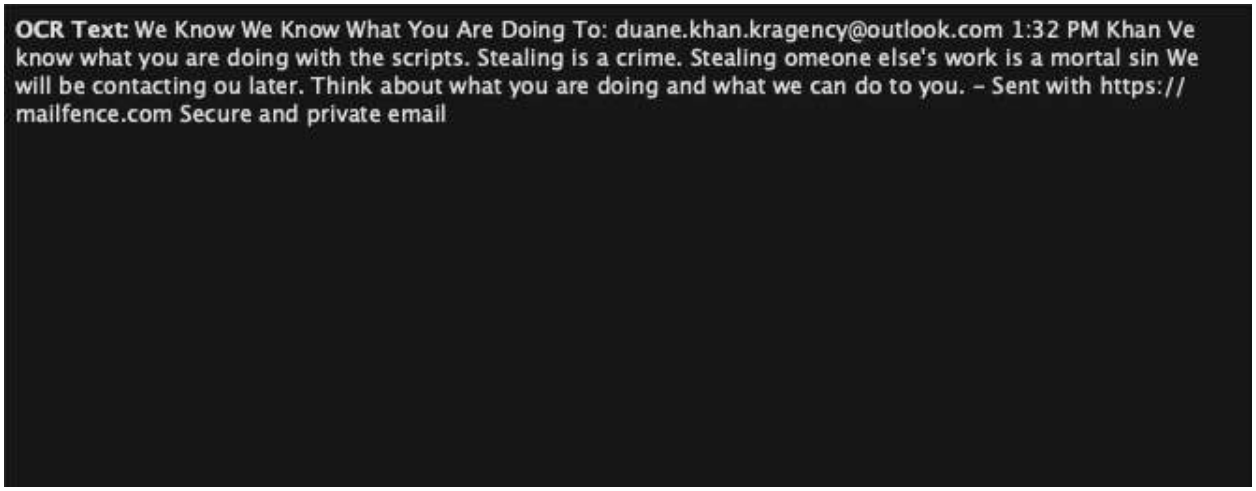
12.7.1 Detailed Information



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.

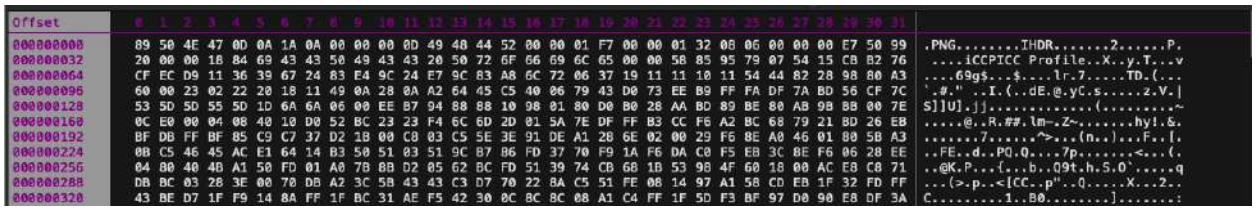
In the example above, a picture from the Desktop was selected. The file's name, path, dates and times, tags and examiner notes are displayed. Additionally, some useful Apple Extended Attributes are shown (Date Added, Content Creation Date).

12.7.2 Optical Character Recognition

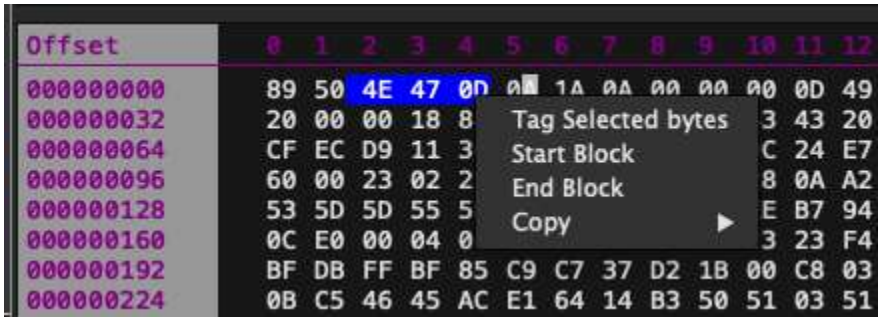


When the OCR module is run, it analyzes the selected file and attempts to extract English characters from any text found within images.

12.7.3 Hex View

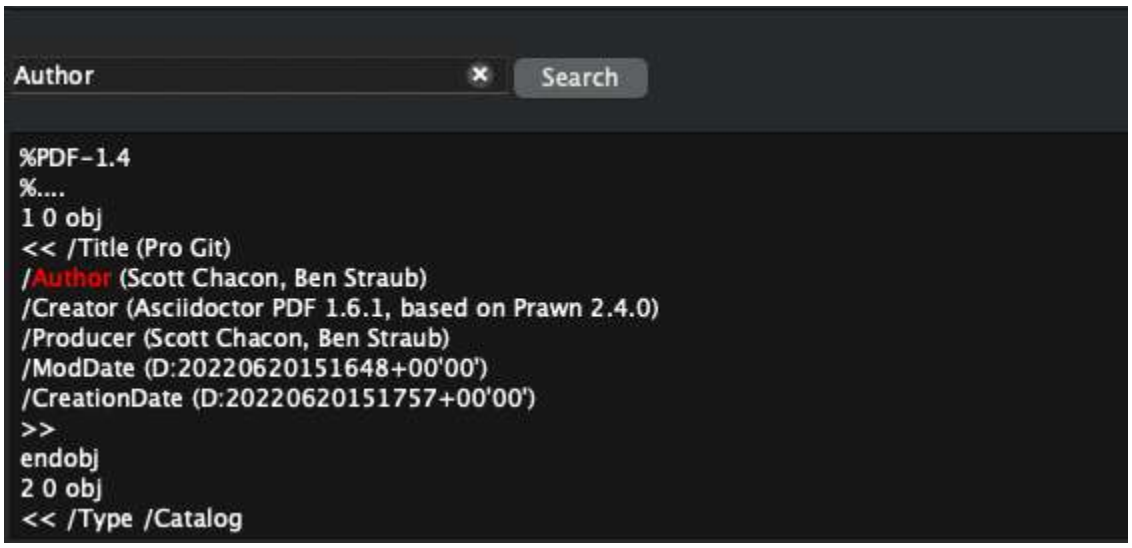


When a file is highlighted in the Main Viewer the Hex View pane will show its hex view. Both hex and ASCII will be shown. In the example above an image file was selected.



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

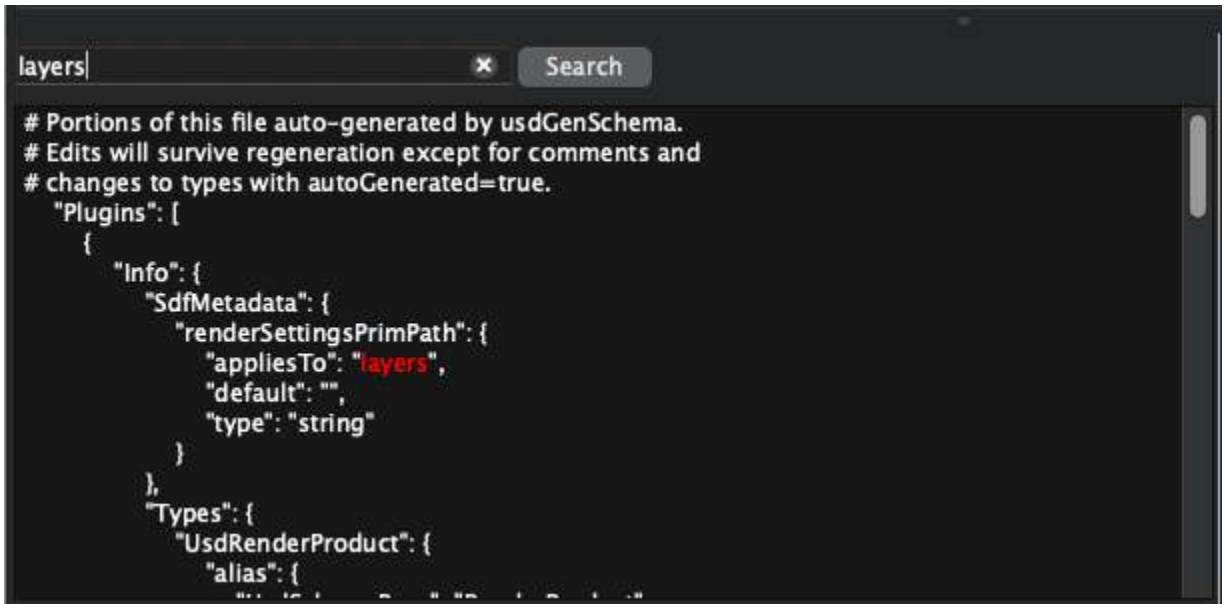
12.7.4 Text View Pane



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. Any matching keywords will be highlighted in red.

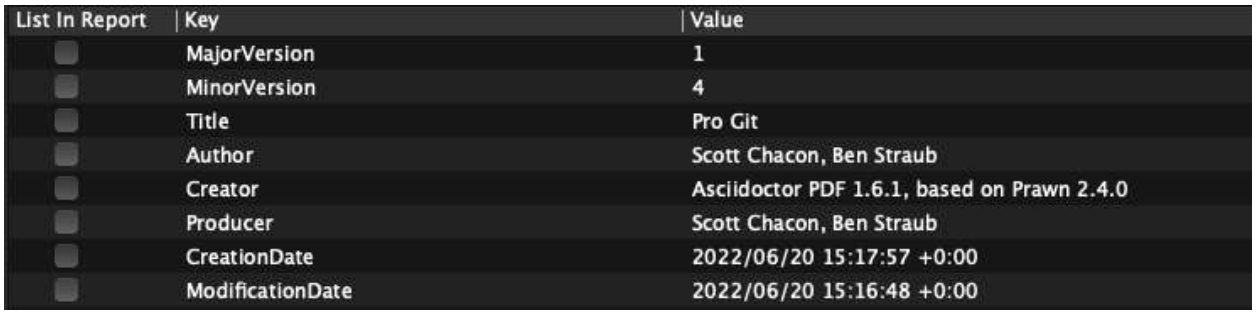
12.7.5 Strings View Pane



When a file is selected from the main viewer, the String View pane displays the contents of the file as a string of readable characters.

Once the String View is open, the examiner can perform keyword searches within the displayed data to locate relevant text quickly.

12.7.6 EXIF Metadata View Pane



List In Report	Key	Value
☐	MajorVersion	1
☐	MinorVersion	4
☐	Title	Pro Git
☐	Author	Scott Chacon, Ben Straub
☐	Creator	Asciidoctor PDF 1.6.1, based on Prawn 2.4.0
☐	Producer	Scott Chacon, Ben Straub
☐	CreationDate	2022/06/20 15:17:57 +0:00
☐	ModificationDate	2022/06/20 15:16:48 +0:00

When a file or item is highlighted in the Main Viewer, the Exif View pane displays any parsed Exif metadata associated with the file.

To include specific metadata in the final report, check the “List in Report” box next to the desired key. This will mark that metadata for inclusion when generating the report.

12.7.7 Apple Metadata View Pane

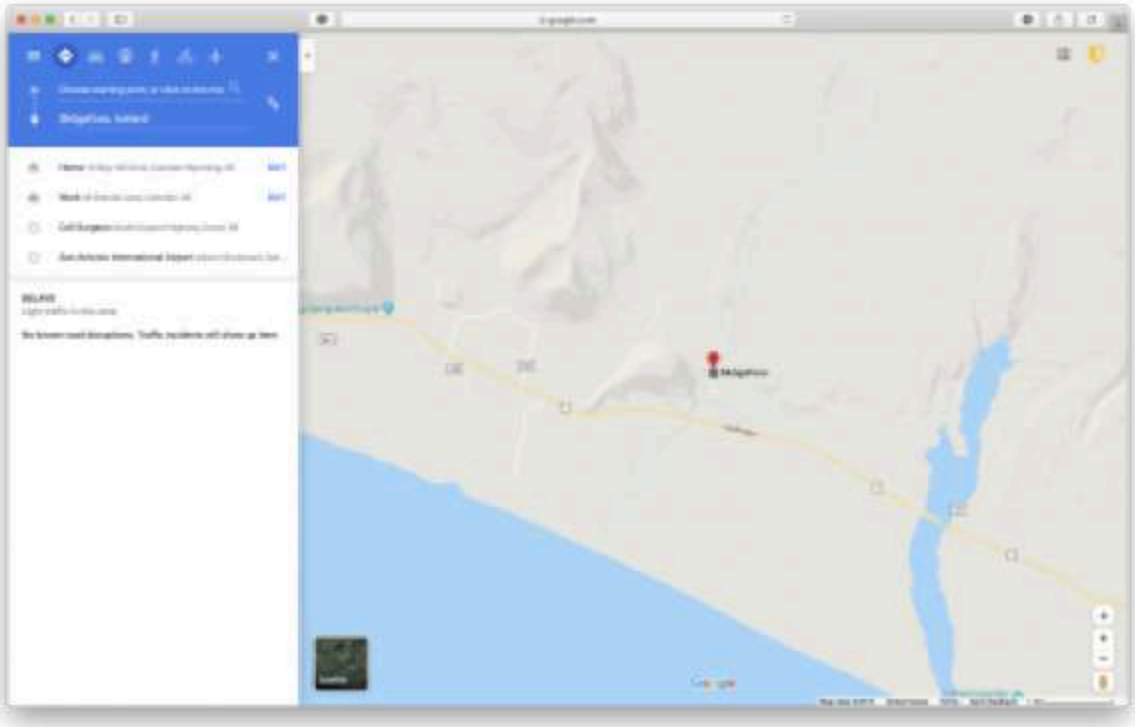
List In Report	Attribute	Value
☐	kMDItemDateAdded	2022-Dec-06 22:58:30 +0:00
☐	kMDItemKind	PNG image
☐	kMDItemDisplayName	Screen Shot 2022-07-21 at 2.32.33 PM
☐	kMDItemContentModificationDate	2022-Jul-21 21:32:39 +0:00
☐	kMDItemContentCreationDate	2022-Jul-21 21:32:39 +0:00
☐	kMDItemComment	Screenshot
☐	kMDItemLastUsedDate	2022-Jul-21 21:32:39 +0:00
☐	kMDItemBitsPerSample	32
☐	kMDItemColorSpace	RGB
☐	kMDItemContentType	public.png
⌄ ☐	kMDItemContentTypeTree	public.png
		public.image
		public.data
		public.item
		public.content

When a file or item highlighted in the Main Viewer contains Apple Extended Metadata, the Apple Metadata pane will display the available attributes.

To include a specific extended attribute in the final report, check the “List in Report” box next to the corresponding item.

12.7.8 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.

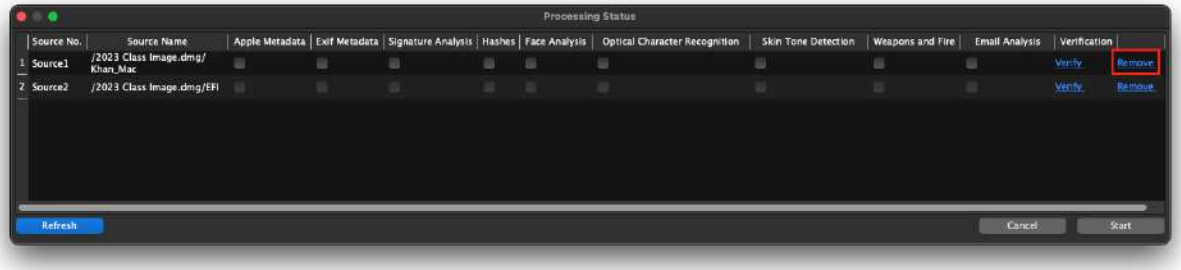


If the examination system is connected to the Internet there is the option to “Open with Google”.

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

---

13 Removing a Source

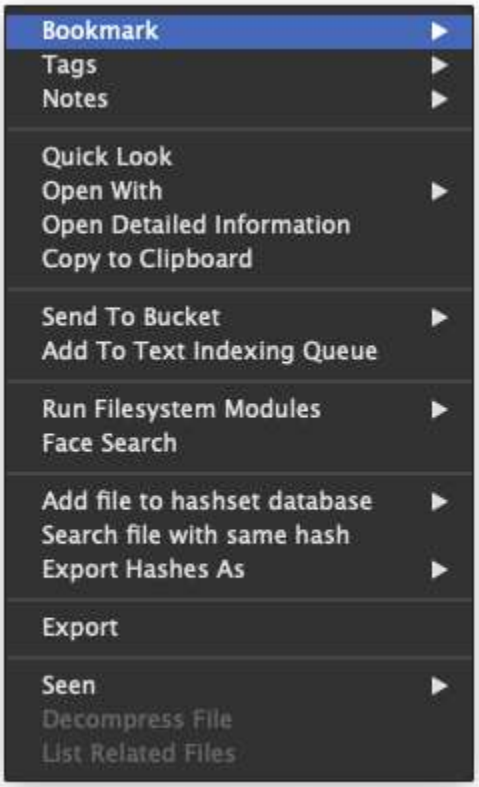


If necessary, it is possible to remove a source after the case has been processed. Pressing the Remove button will remove the selected source from the RECON LAB case.

---

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.

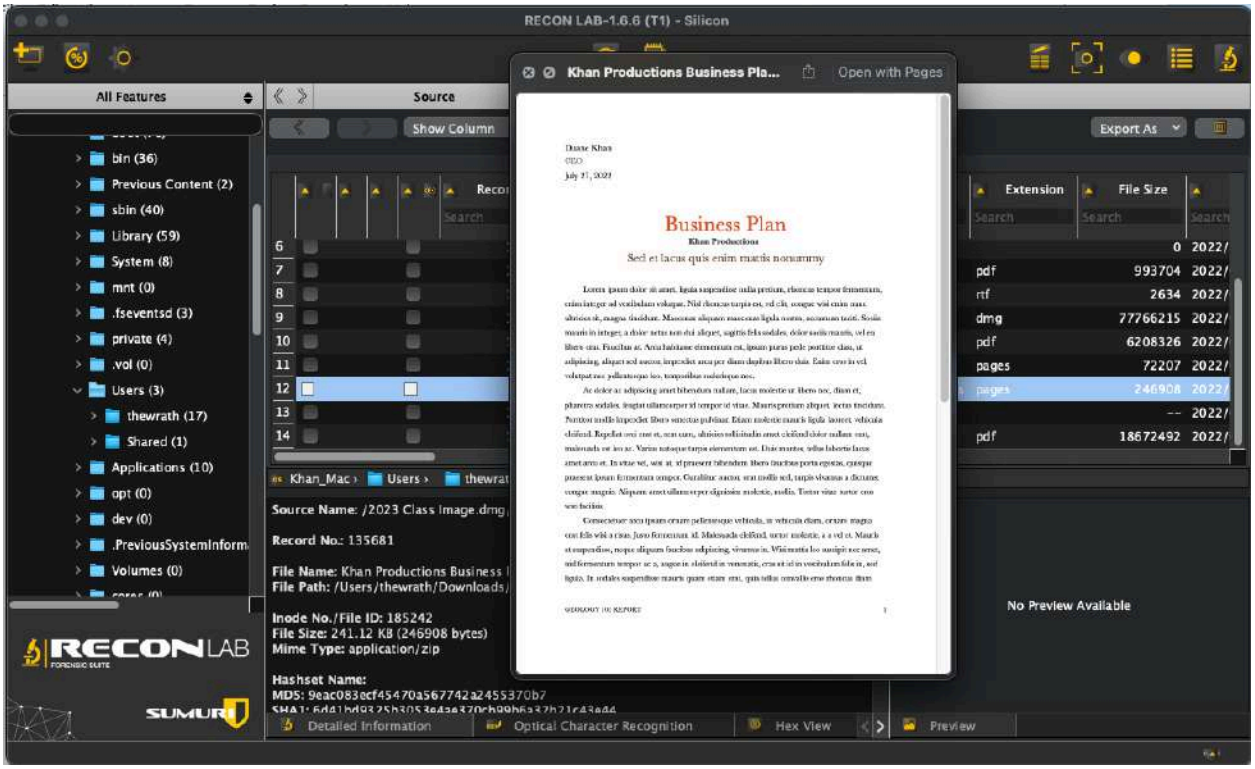


- Bookmark – Adds or removes a basic bookmark to a file or item.
- Tags – Allows the examiner to “tag” a file with a color or custom name.
- Notes – Allows the examiner to enter or remove notes for a file or item.
- Quick Look – Activates the macOS file viewer to preview a file or show additional information.
- Open With – Opens the file in RECON LAB’s built-in Plist, Hex, SQLite or Registry Viewer.
- Open Detailed Information – Opens a floating window with the file or artifact’s detailed information.
- Copy to Clipboard – Copies the detailed information about the file to the clipboard.
- 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.
- Add to Text Indexing Queue – Adds selected files or folders to the queue as an item to be indexed.
- Run Filesystem Modules – Run file system modules against individual files or directories.
- Face Search – Search the faces that have been indexed for a selected face
- Add file to hash set database – Add selected file to a pre-configured hash set database.
- Search file with the same hash – Finds any files with the same hash in pre-configured hash sets.
- Export as Hashes As – Exports selected hashes and a selected files
- Export – Allows the examiner to export the selected file or directory
- Seen – Allows the examiner to mark, and show / hide files that have been marked as seen

- Decompress File – Opens a preview of the zipped file

---

15 Previewing Files



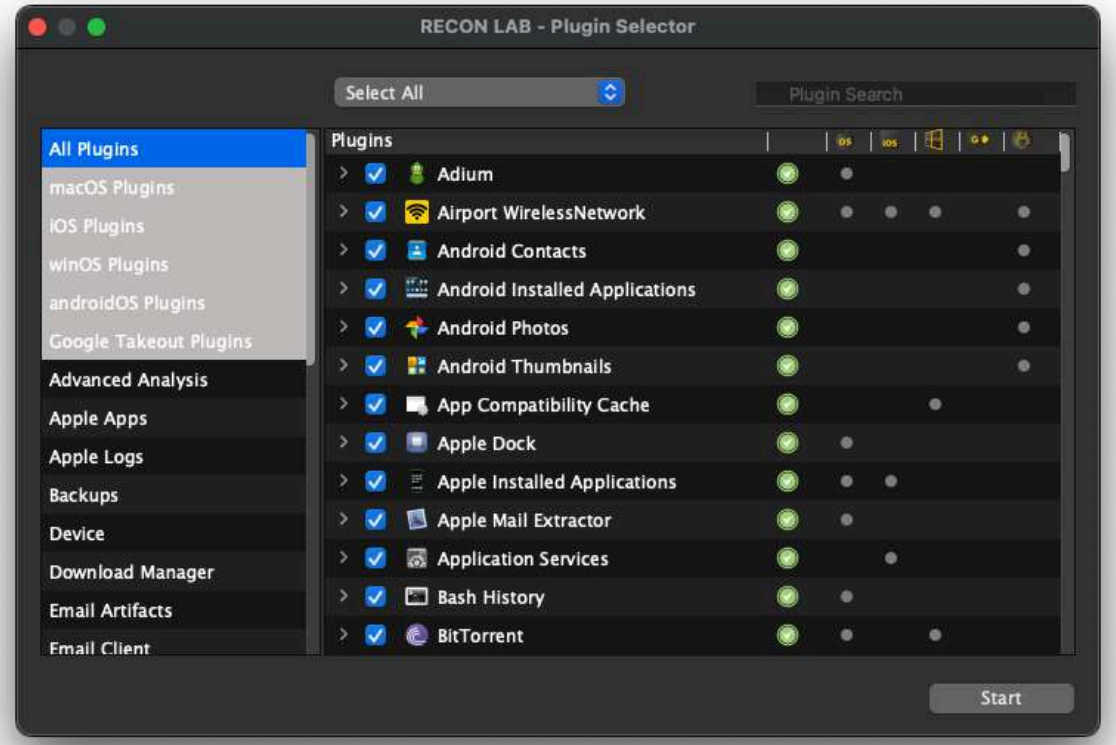
RECON LAB supports previewing hundreds of file types even if the parent applications are not installed. For example, if MS Word is not installed, RECON LAB can still preview the MS Word document file. As RECON LAB is designed on a Mac it takes advantage of macOS's Quick Look. To activate Quick Look to 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.

---

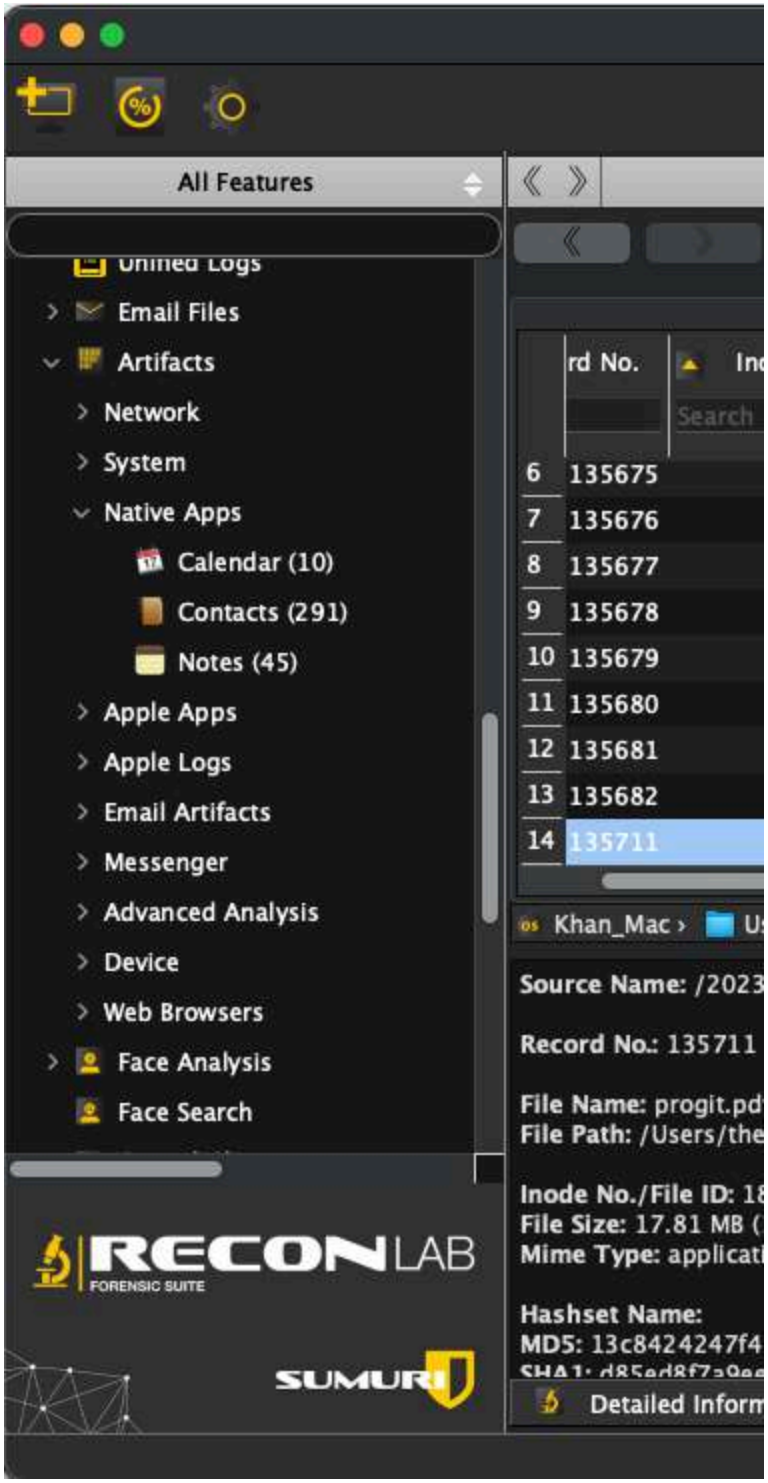
16 Plugin Selector

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. For more information, please see Artifacts.

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.

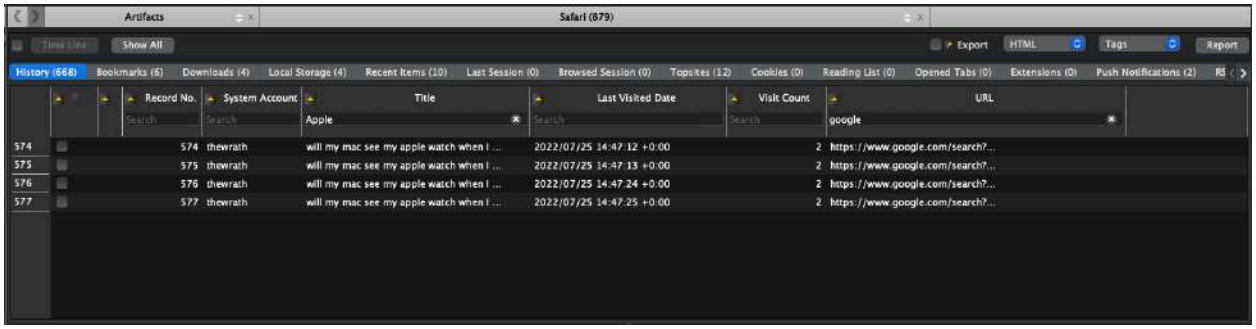


The number listed next to the plugin is the number of artifacts recovered. Double-clicking on the plugin opens the data in the Main Viewer window.

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.

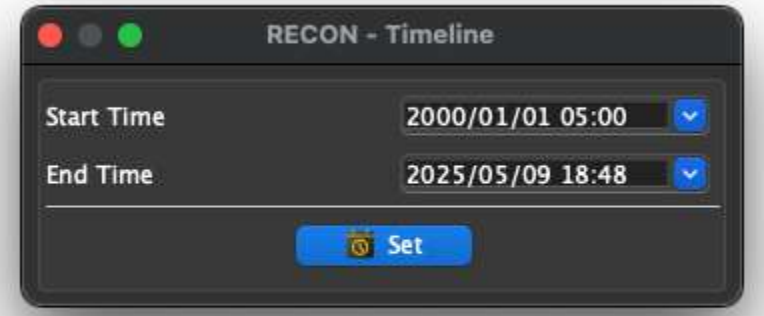
16.0.0.1 Filtering Data with Keyword Searches

There is the ability to search within plugins to filter the data using the Keyword Search box. These Search Boxes will be located below each column. If more than one Keyword is entered, it will be treated as an AND search.



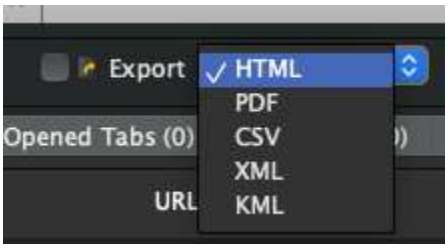
16.0.0.2 Setting a Timeline to Filter Data

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

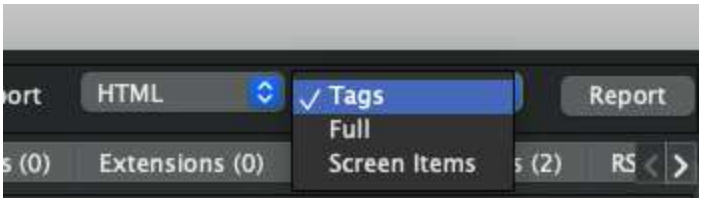


Data can be filtered by setting a Start Time and an End Time and clicking the Set button. Activate the set timeline by checking the box next to the “Time Line” button and click Search.

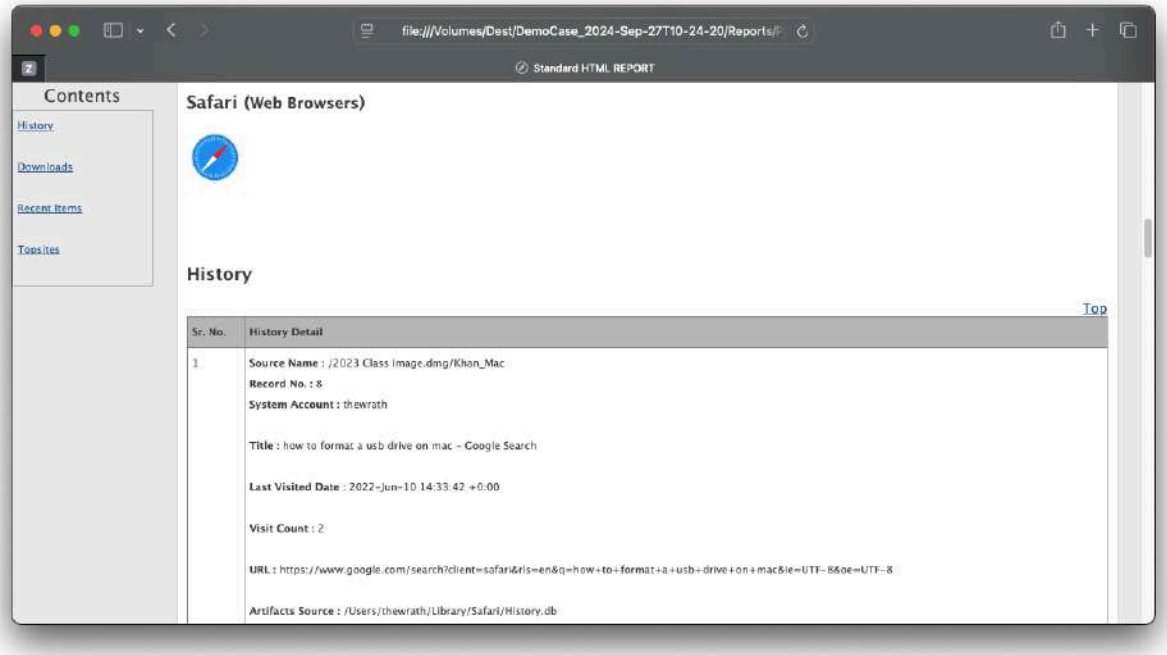
16.0.0.3 Generating Reports from Plugin Window



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

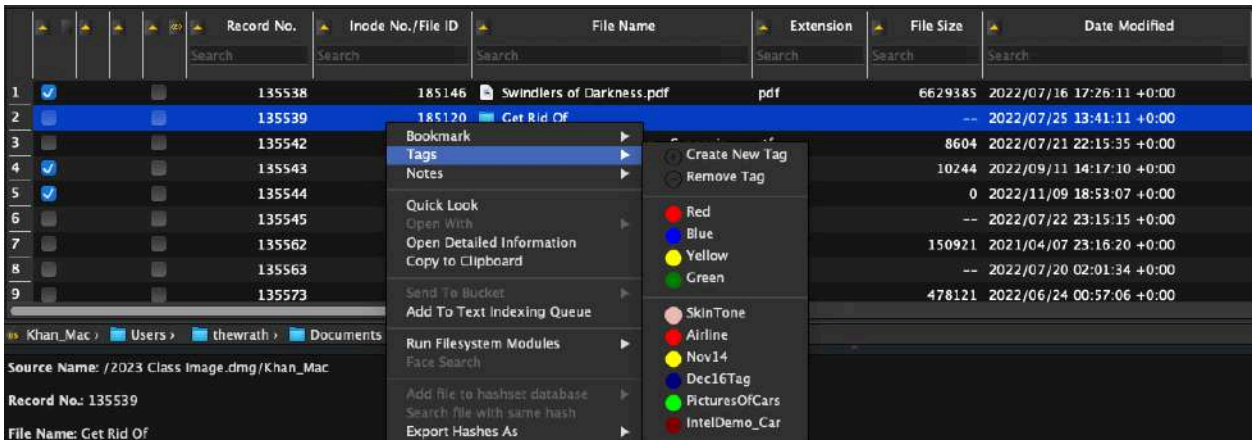
Bookmarks are the simplest way to mark items of interest in RECON LAB. In almost every area of RECON LAB there will be a checkbox next to any item that can be bookmarked. To bookmark a file just check the box with the “bookmark” icon in the column.

		Record No.	Inode No./File ID	File Name	Extension	File Size	Date Modified
1	☑	135538	185146	Swindlers of Darkness.pdf	pdf	6629385	2022/07/16 17:26:11 +0:00
2	☐	135539	185120	Get Rid Of		--	2022/07/25 13:41:11 +0:00
3	☐	135542	185145	Script Writers Workshop - Synopsis ...	rtf	8604	2022/07/21 22:15:35 +0:00
4	☑	135543	185106	.DS_Store		10244	2022/09/11 14:17:10 +0:00
5	☑	135544	185107	.localized		0	2022/11/09 18:53:07 +0:00
6	☐	135545	185127	Pics		--	2022/07/22 23:15:15 +0:00
7	☐	135562	185108	D Khan - Actor to Screenwriter ...	pdf	150921	2021/04/07 23:16:20 +0:00

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

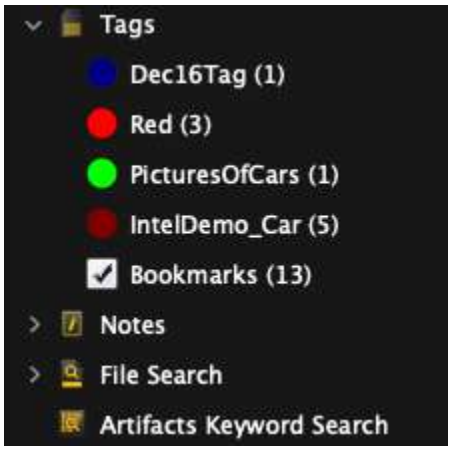
17.2 Tags

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).

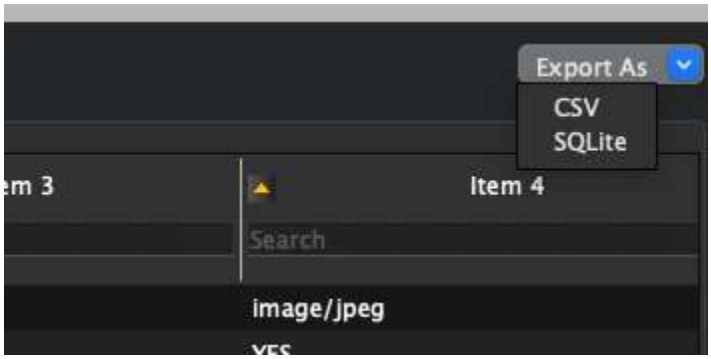
17.3 Finding Tags and Bookmarks in Sidebar



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.



17.4 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. The 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.

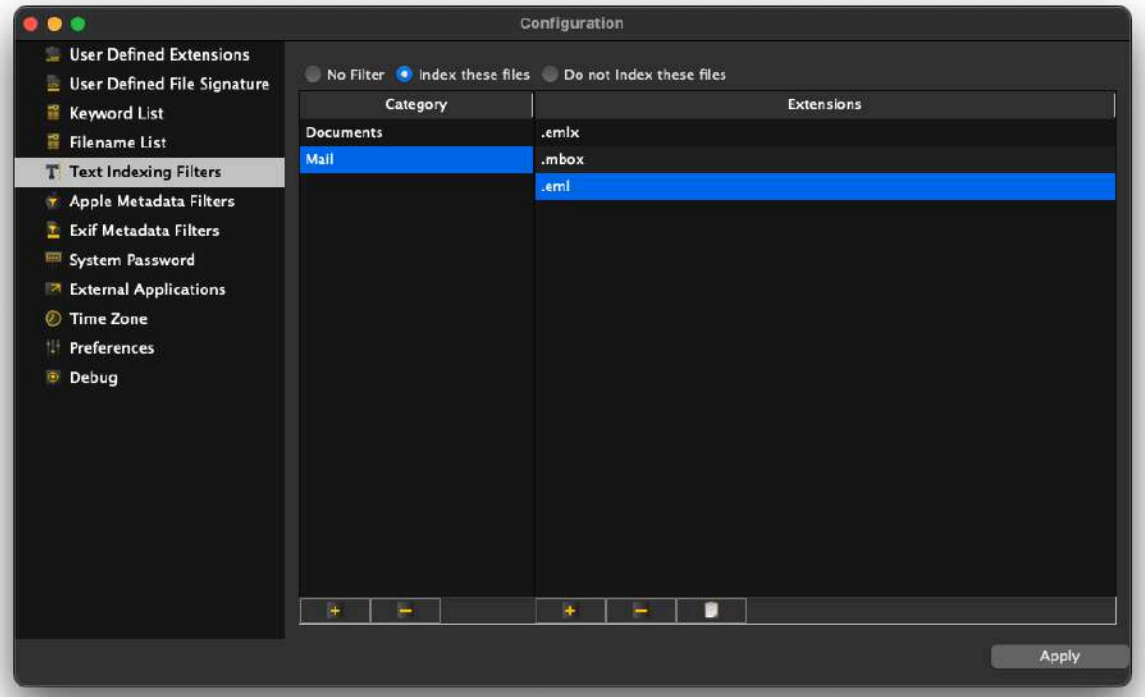
The goal is to perform surgical indexing and searches to find the information needed in less time.

18.0.1 Indexing Example with RECON LAB

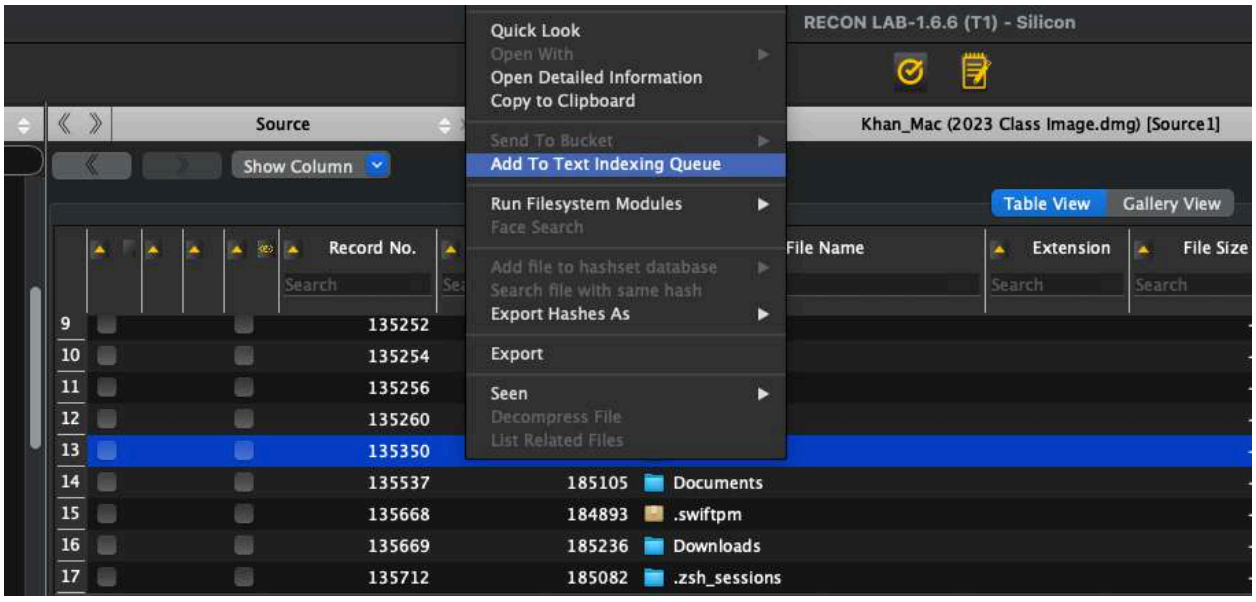
Let’s use this as an example. You are tasked with finding any emails containing information about a company named “SUMURI” and we know the person of interest uses the Apple Mail client. You had the ability to image his company MacBook and are now performing the analysis.

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

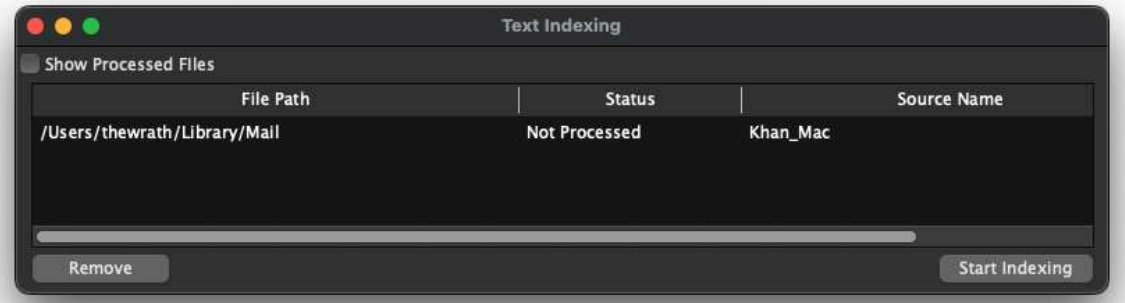
Or, we can use RECON LAB’s indexing in a more intelligent way.



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”.

After indexing is complete we can now perform a Content Search for the keyword “production” 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.

19.0.0.1 Local Search Options

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

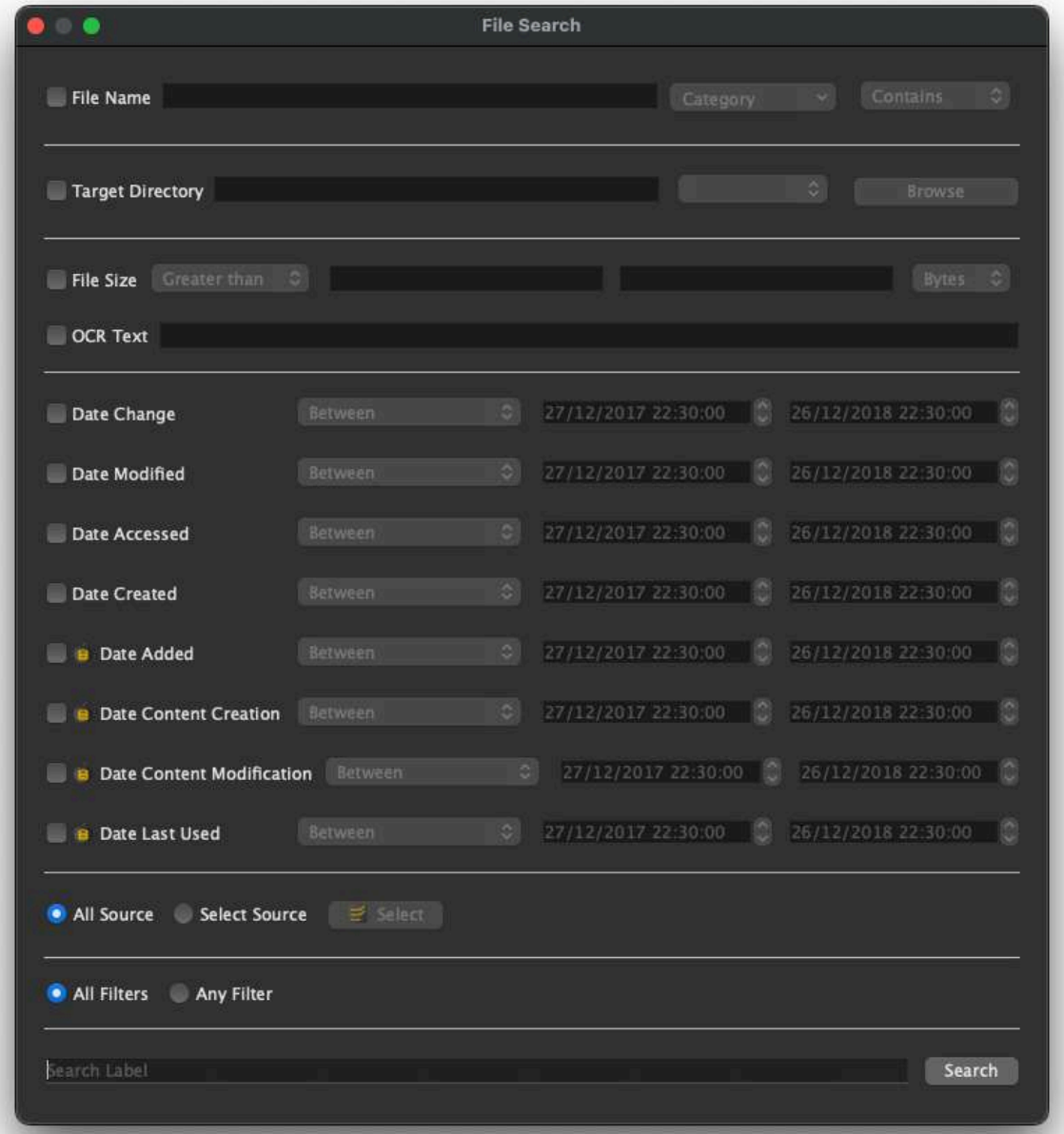
19.0.0.2 Global Search Options

- File Search
- Content Search
- EXIF Metadata Search
- Apple Metadata Search
- Artifact Keyword Search
- Recognize Face

19.1 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.



A search can be performed with the following criteria:

- File Name – The examiner can search for a file name of interest. To select a File name list entered in the configuration window press on the Category dropdown. Searches of the names can be performed with the following criteria:

    - Contains
    - Matches
    - Starts With
    - Ends With
- Target Directory – This allows the examiner to set the scope of their investigation. If selected, the examiner can select the source they would like to search for the file in. By pressing Browse the examiner can choose what directory within that source they would like to analyze
- File Size
- OCR Text
- Date Searches – The examiner can perform a date search of any of the following timestamps:
    - Date Change
    - Date Modified
    - Date Accessed
    - Date Created
    - Date Added
    - Date Content Creation
    - Date Content Modification
    - Date Last Used

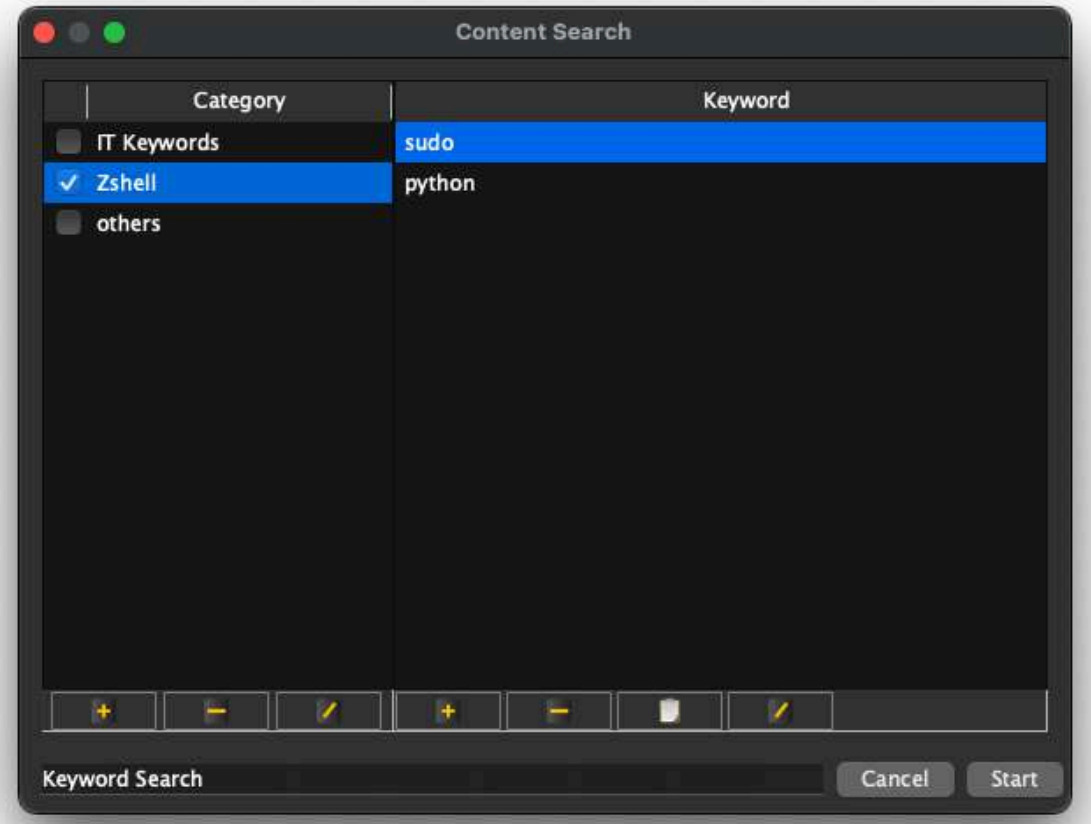
19.2 Content Search

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.

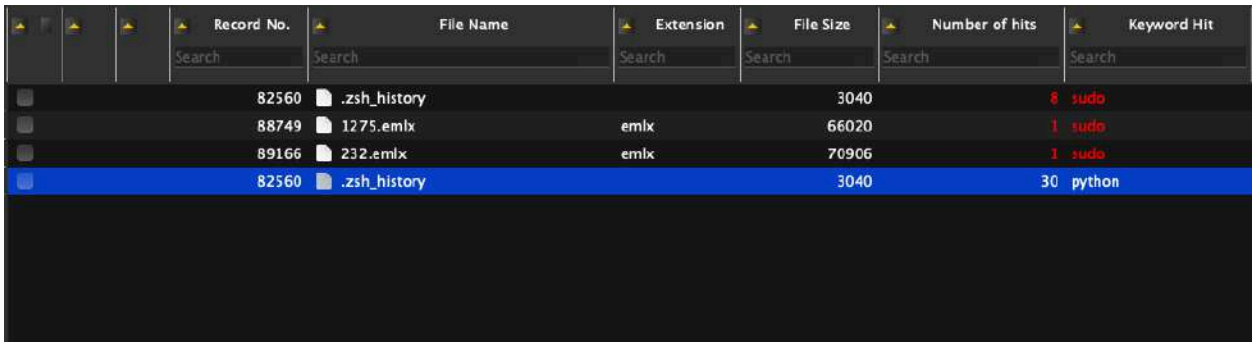
1. Create your list of keywords (Top Menu – Configuration – Keyword Lists).
2. Create and apply any Text Indexing Filters (Top Menu – Configuration – Text Indexing Filters).
3. Selected data from the source (Right-click on a source and “Add to Text Indexing Queue”).
4. Indexed selected data (Menu Bar - Process – Text Indexing).
5. 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.



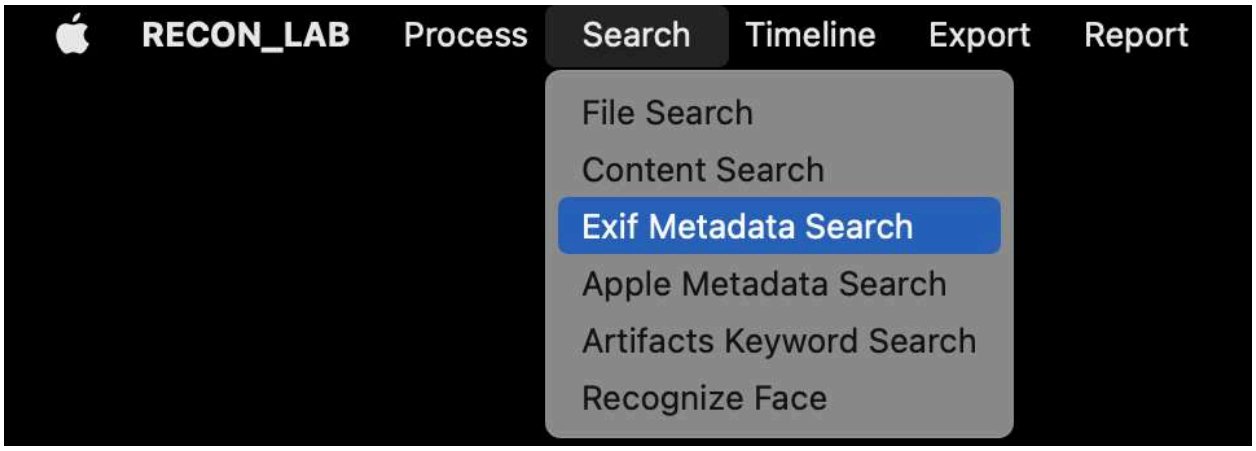
The Content Search selection window will appear allowing the examiner to select pre-configured categories and/or edit keywords prior to the content search. To begin the search enter a label for the search than click “Start”.



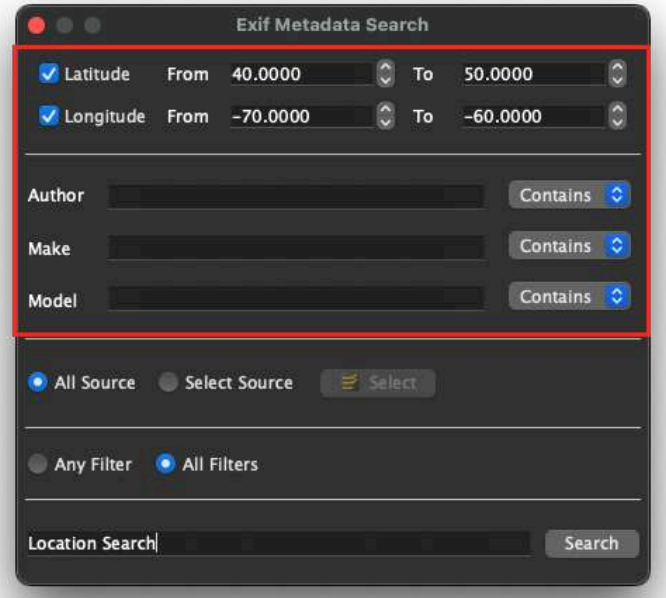
After the Content Search is complete the results will be available in the Main Viewer window and the search will be added to the Sidebar.

19.3 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

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.

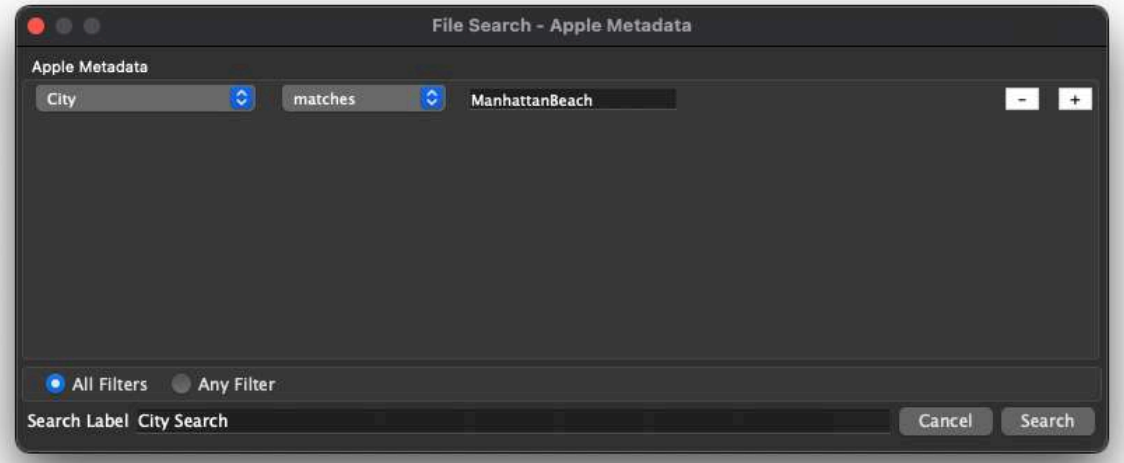
Note: Using both Latitude and Longitude filters will allow filtering data to a known geographical area.

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.



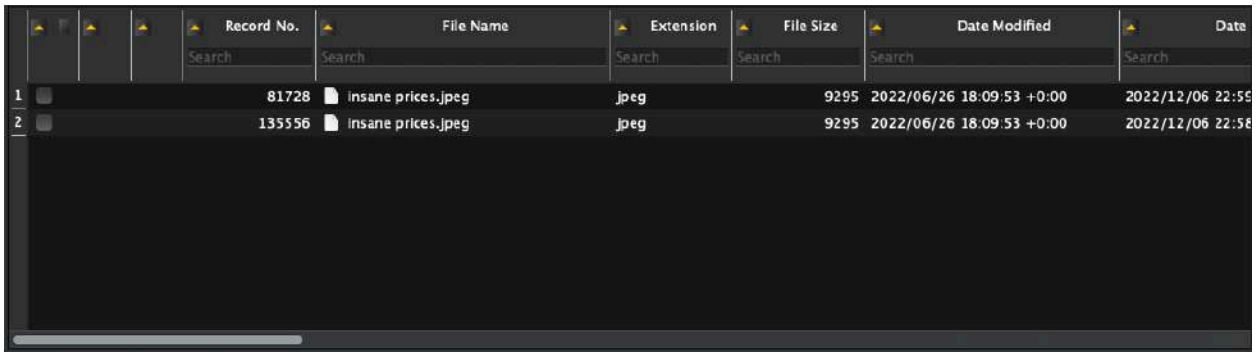
The Apple Metadata File Search window will appear with the ability to select, add, remove or configure filters for Apple Extended Metadata.

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 “City” extended attribute with the keyword “ManhattanBeach”.

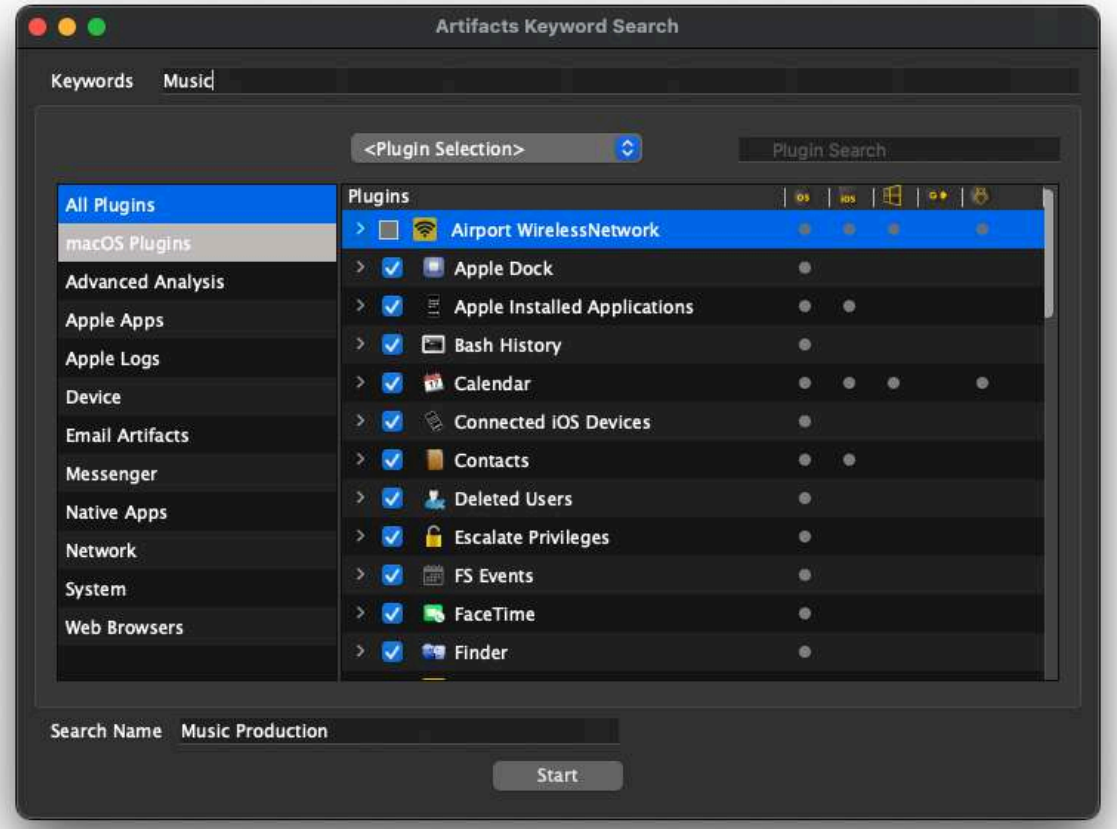


Once the search is completed you will have the option to review the results which will appear in the Main Viewer window.

19.5 Artifacts Keyword Search

As mentioned earlier, RECON LAB can automatically parse and recover 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.

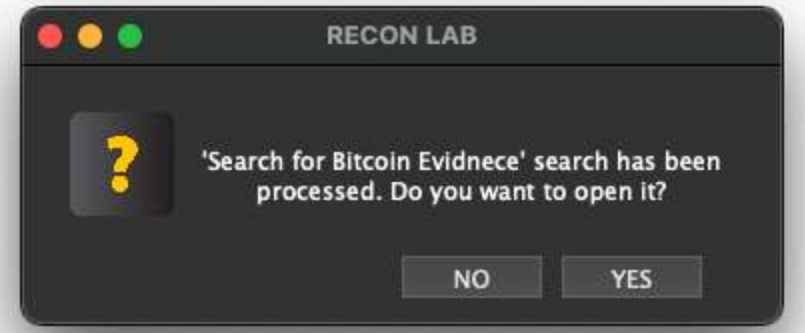


Enter a keyword and select the plugins of interest for the search. If you would like to enter more than one keyword at a time, separate the keywords with a comma and no space. For example, if you want to search for the keywords “apples, oranges and bananas” enter the keywords as:

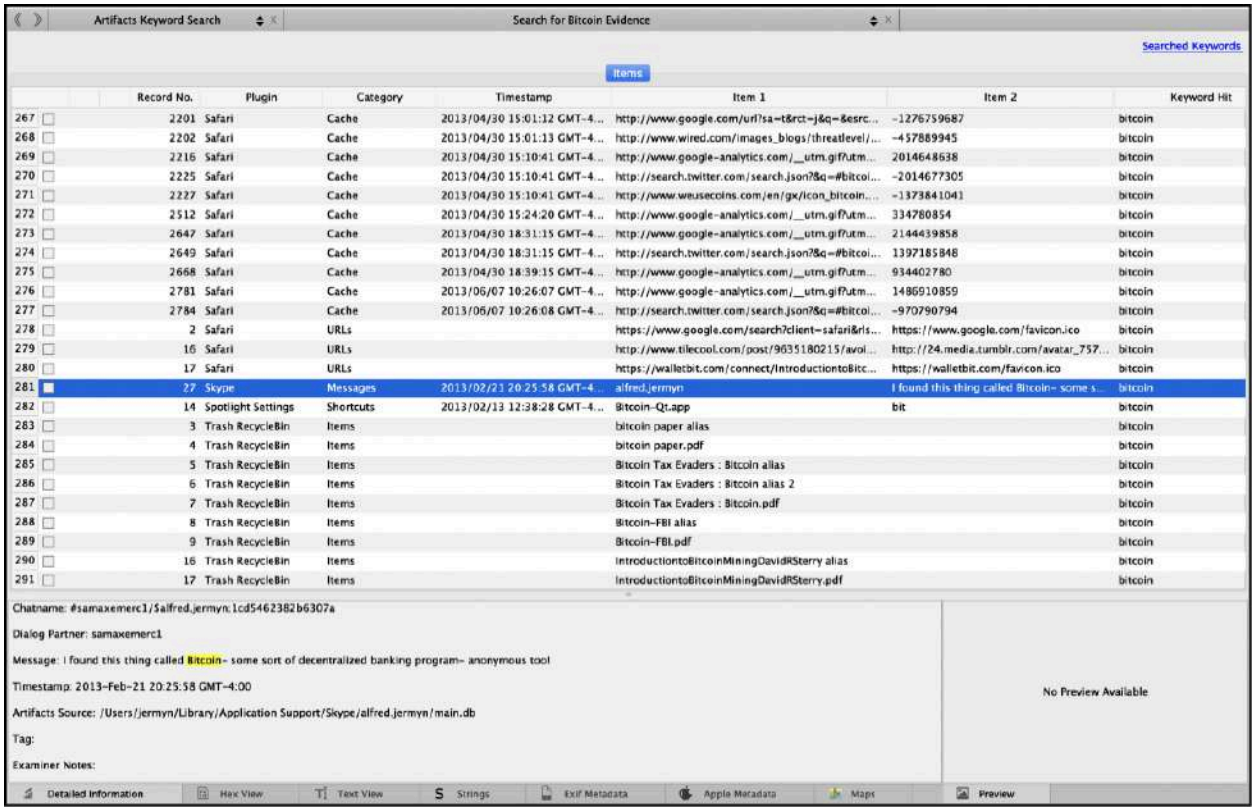
apples,oranges,bananas

After entering your keywords, provide a name for the search then click “Start”.

In the example above the examiner is searching for the keyword “Music”. All Plugins were selected using the dropdown box and the name for the search was “Music Production”.



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 detail or bookmarked.

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

19.6 Recognize Face

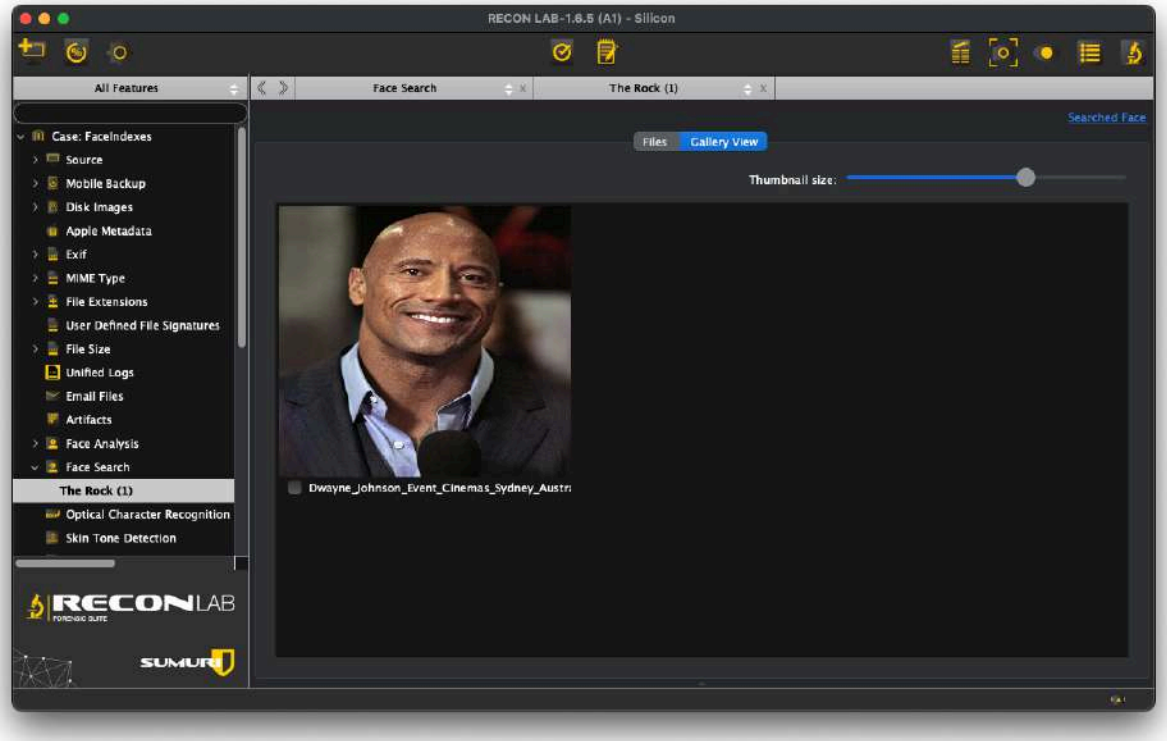
The Recognize Face search option allows the examiner to search for an individual, based on a picture, through the list of the indexed faces in that case. This can be accessed through Search > Recognize Face.

The Recognize Face menu provides tools to search for matching faces within your face indexed files. Before using this search functionality please ensure the Face Analysis function has been run. Use the following steps to perform a face recognition search:

1. Click the three dots "..." to navigate to and select a photo of the person you want to search for.
2. After opening the photo, press Extract Faces to isolate the face within the image.

3. To save your search, enter a name in the Save Result As text box.
4. Press Start to initiate the search process.

19.6.1 Reviewing Results



After performing a face search, the results can be reviewed in the Face Search tab. This tab contains two viewing options for examining the results:

- Files – Displays a list of files that contain matching faces.
- Gallery View – Shows thumbnails of the matching faces for visual comparison.

To view the original image used in the search, click Searched Face.

---

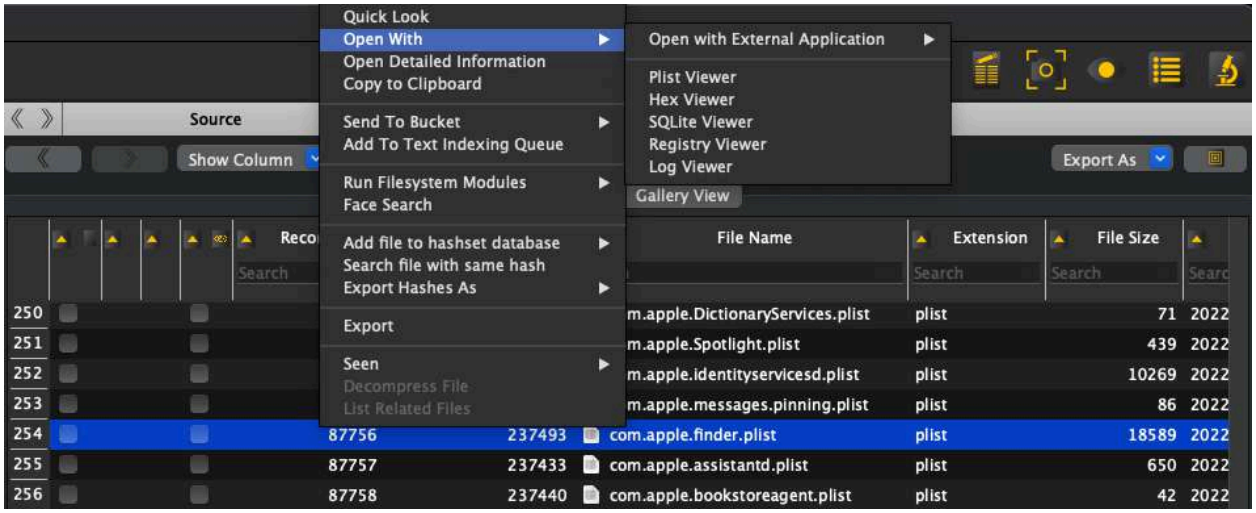
20 Advanced Viewers

Integrated into RECON LAB are five advanced viewers.

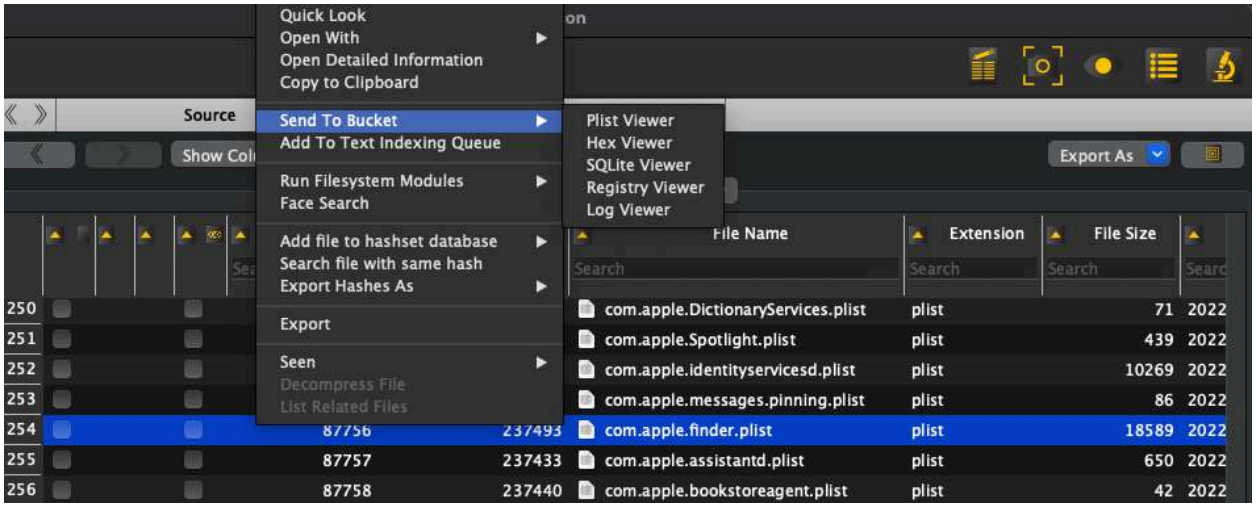
- **Property List Viewer** – for Apple binary and standard plist files.
- **HEX Viewer** – a full Hex viewer with advanced functions for forensic investigations.
- **SQLite Viewer** – a forensic SQLite viewer with the ability to create custom SQLite queries.
- **Registry Viewer** – for analysis and documentation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

20.1 Plist Viewer

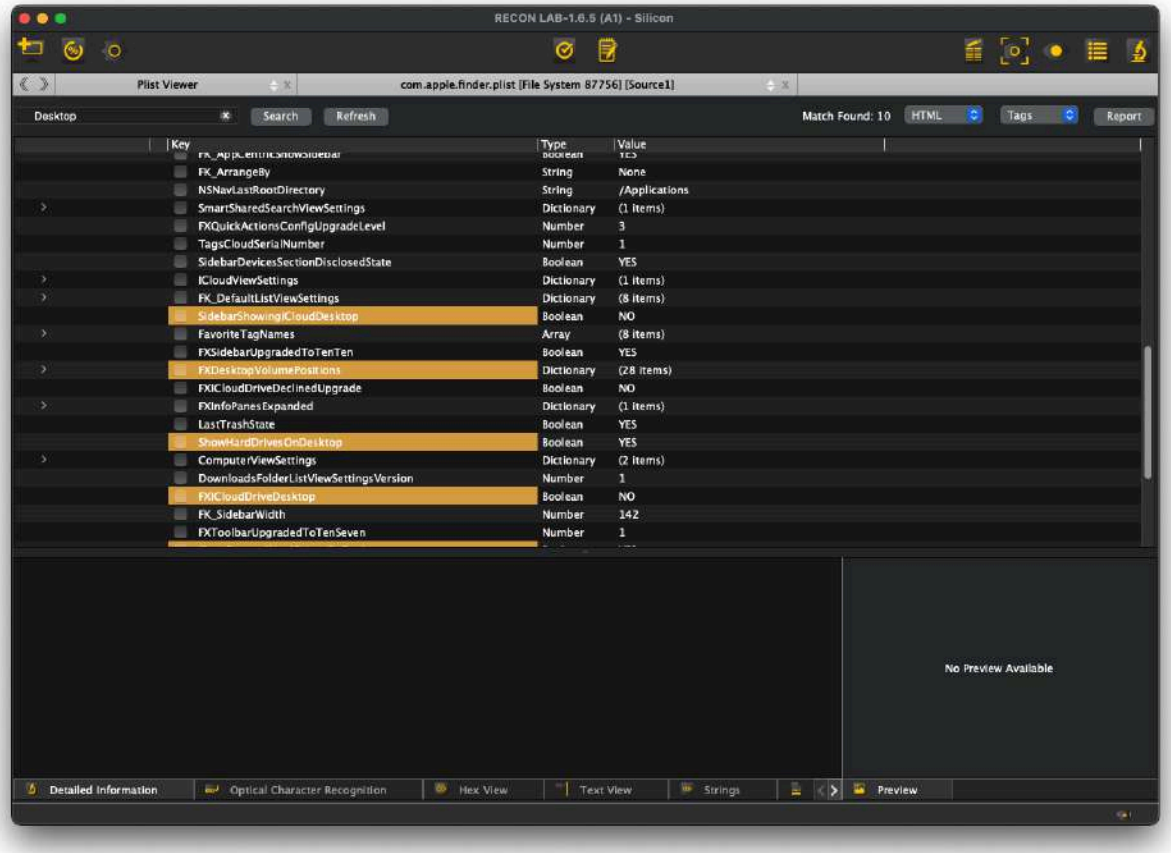
The Property List Viewer (Plist Viewer) works with both standard and binary macOS Property Lists (.plist files). Property List files are one of two common storage formats for Mac data.



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”.

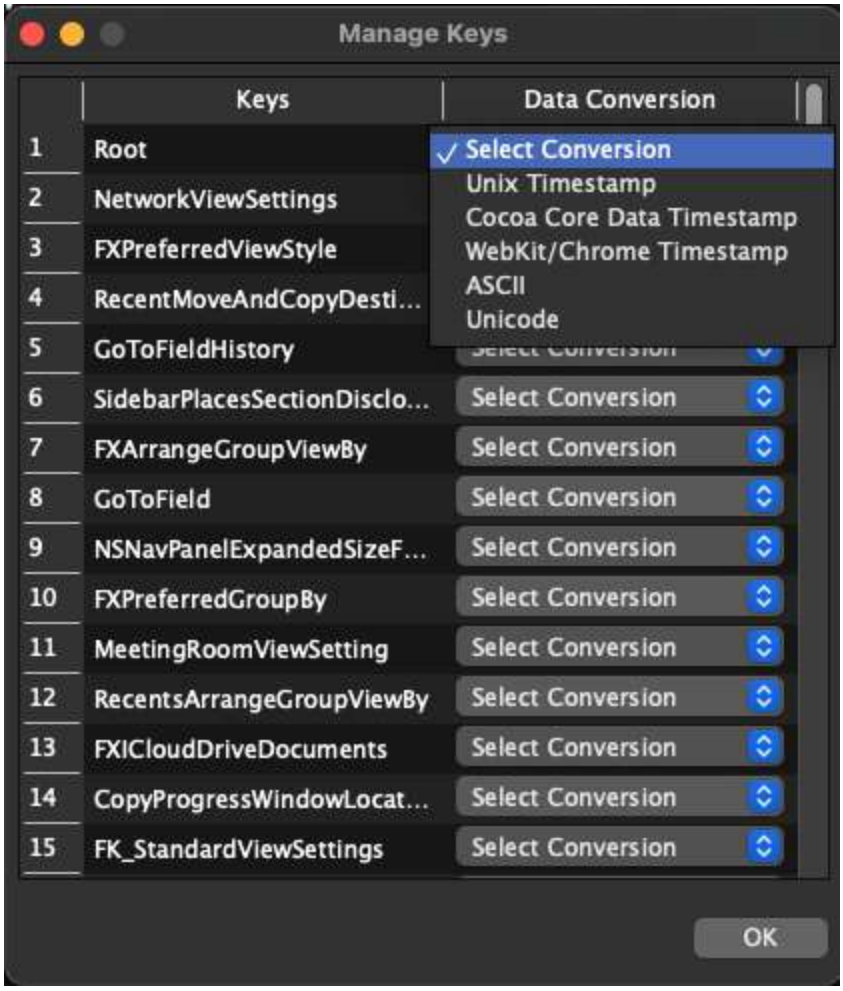


The Property List Viewer opens the plist in the Main Viewer window. Search options and reporting options are available.

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.

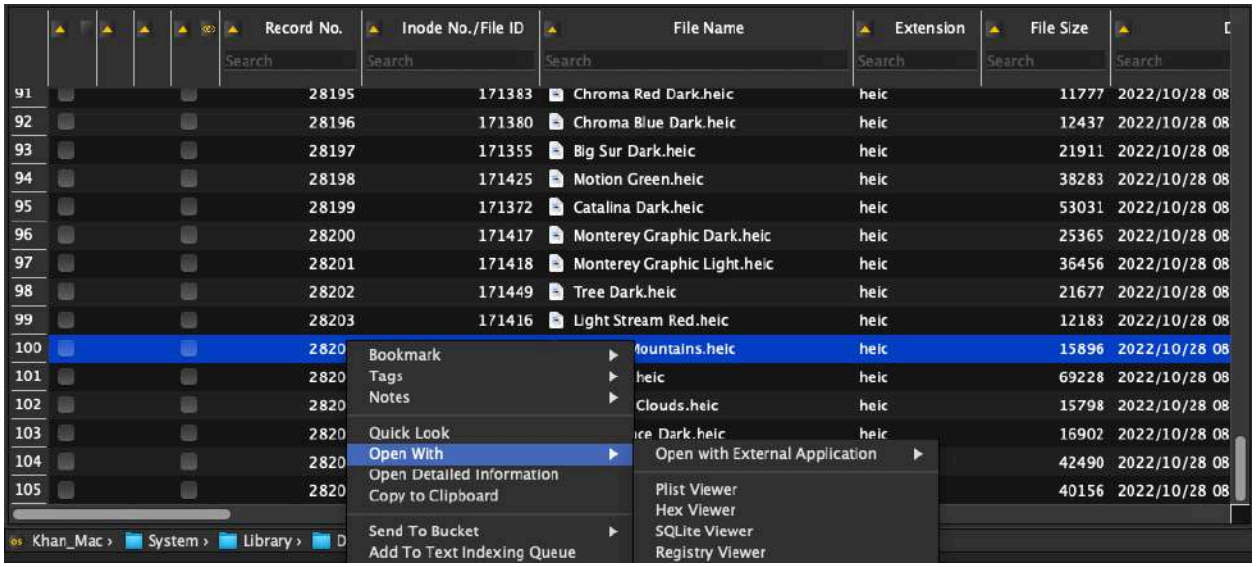


After selecting the conversion type, select the data key to see the conversion in the main window of the Property List Viewer.

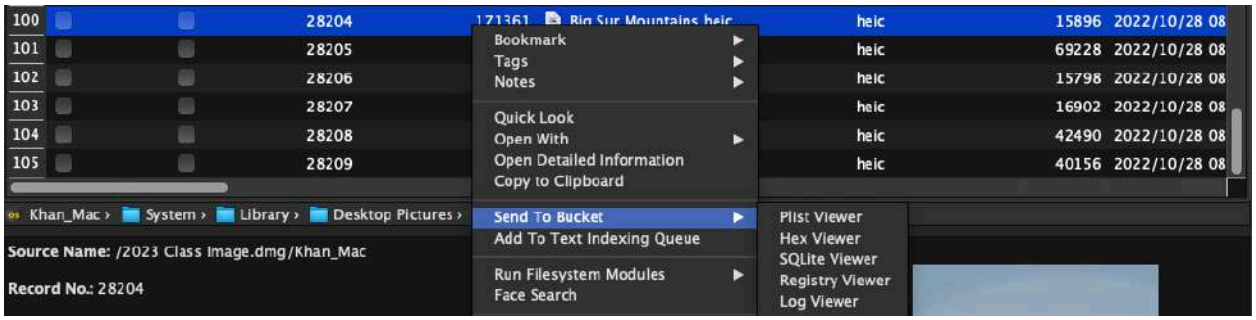
20.2 Hex Viewer

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

20.2.0.1 Open File in Hex Viewer



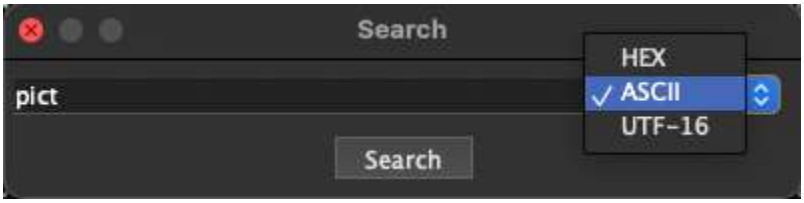
To open a file in the Hex Viewer, right-click and select “Open With – Hex Viewer”.



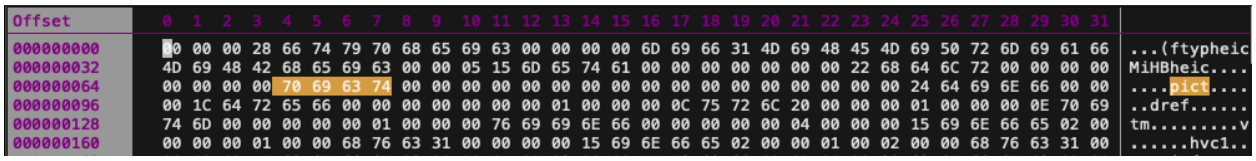
If you would like to add the file to review later in the Sidebar Bucket select “Send to Bucket – Hex Viewer”. The Hex Viewer will open in the Main Viewer window. The number of “Bytes per line” can be adjusted using the dropdown box with values between 2 and 32.

20.2.0.2 Search in Hex Viewer

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

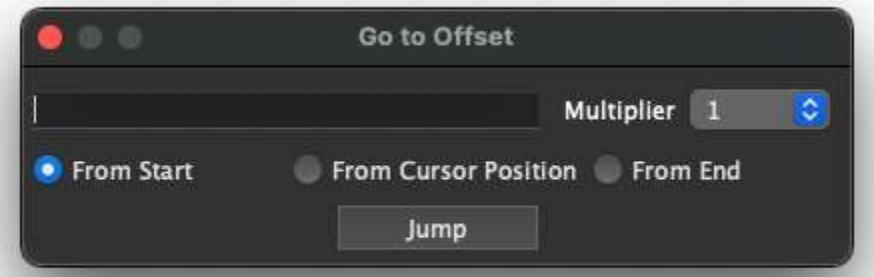


After entering the search term click “Search”.



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

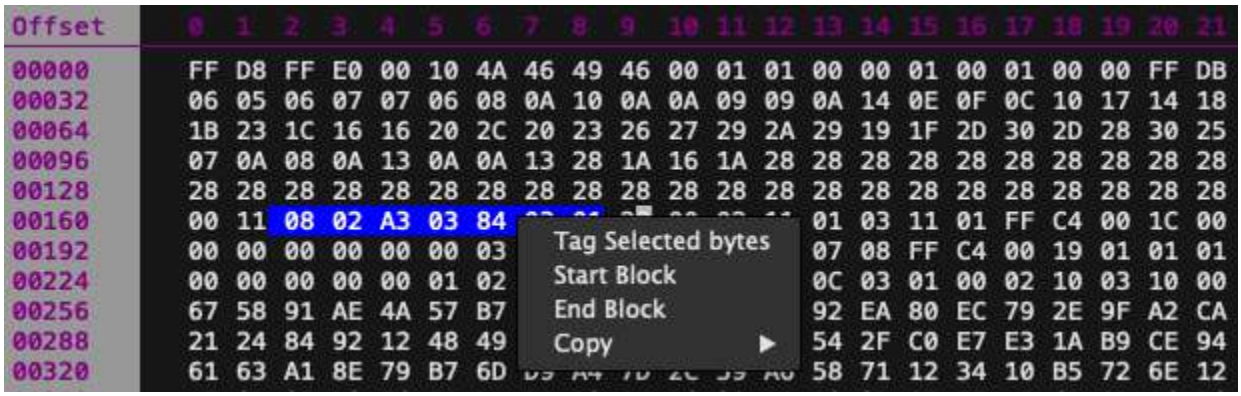
20.2.0.3 Jump to an Offset



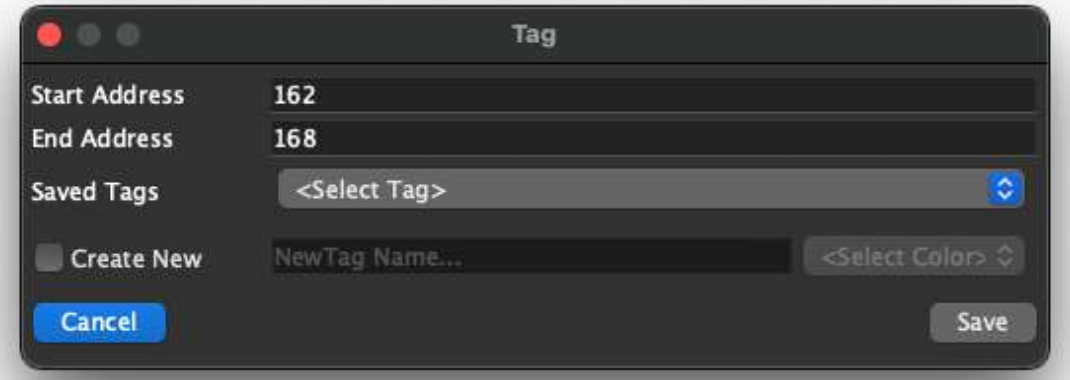
To jump to a specific offset click the “Go to Offset” button at the top of the Hex Viewer. Enter a value and select a multiplier (between 1 and 8192). Select where to begin:

- **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.

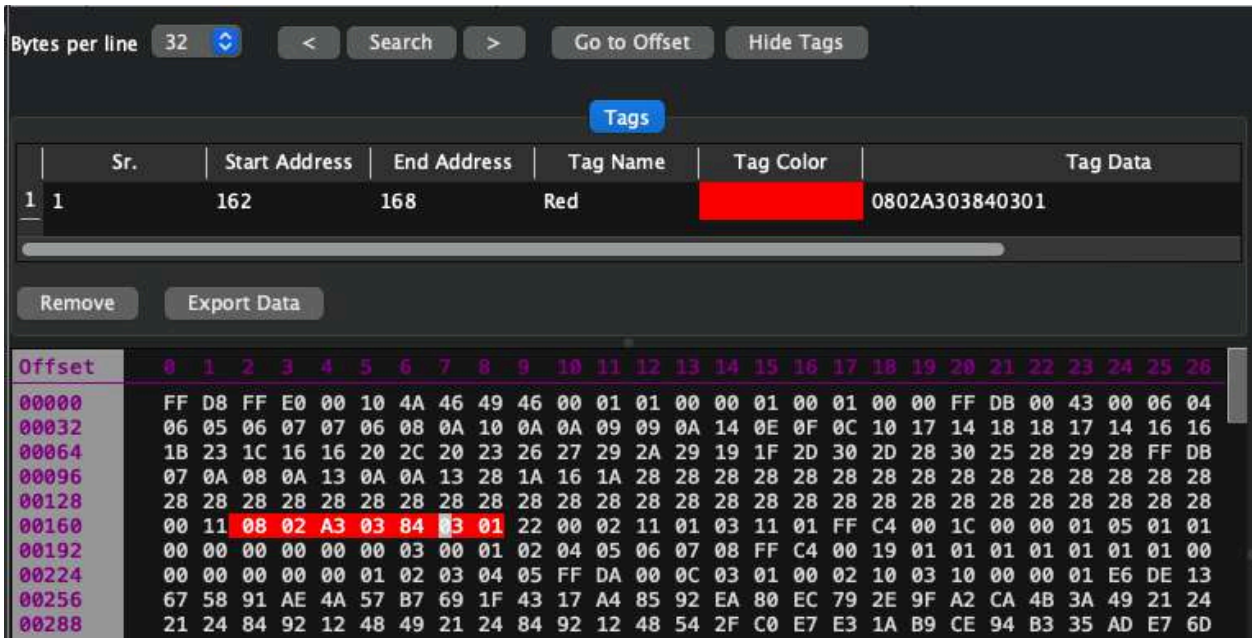
20.2.0.4 Tag Selected Bytes



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.

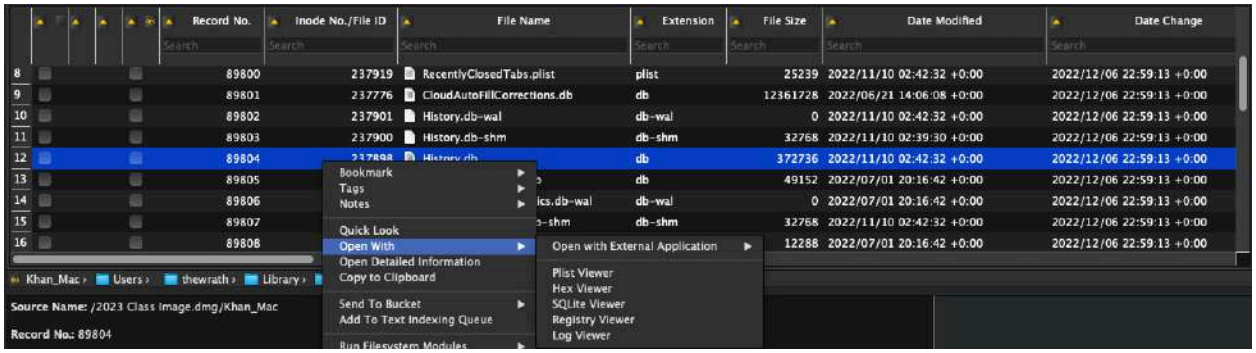
20.2.0.5 Hex Viewer Information Pane

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.

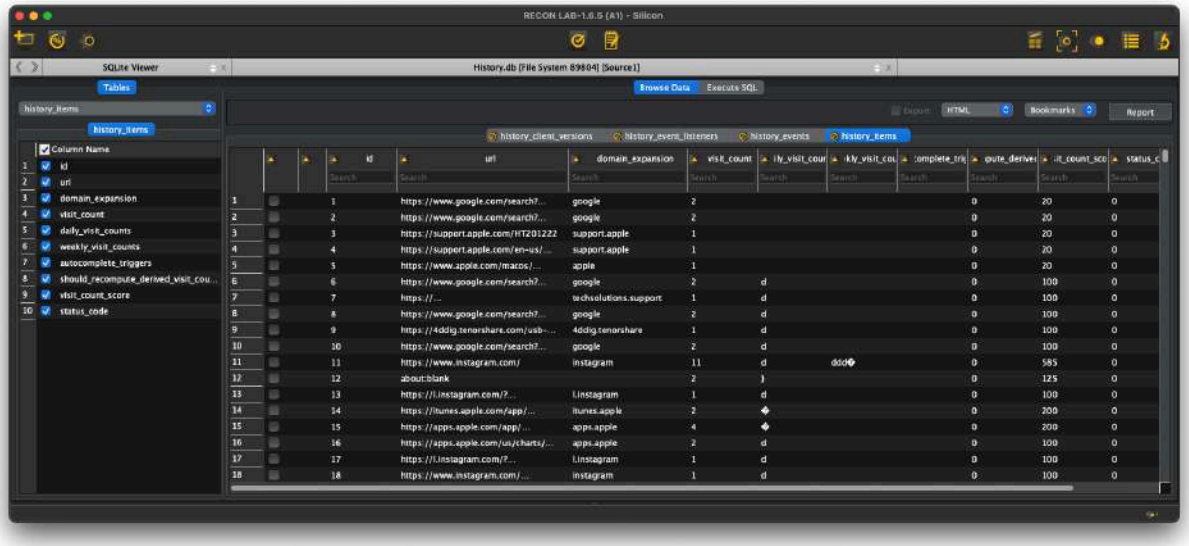
20.3 SQLite Viewer

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.

20.3.0.1 Open File in SQLite Viewer

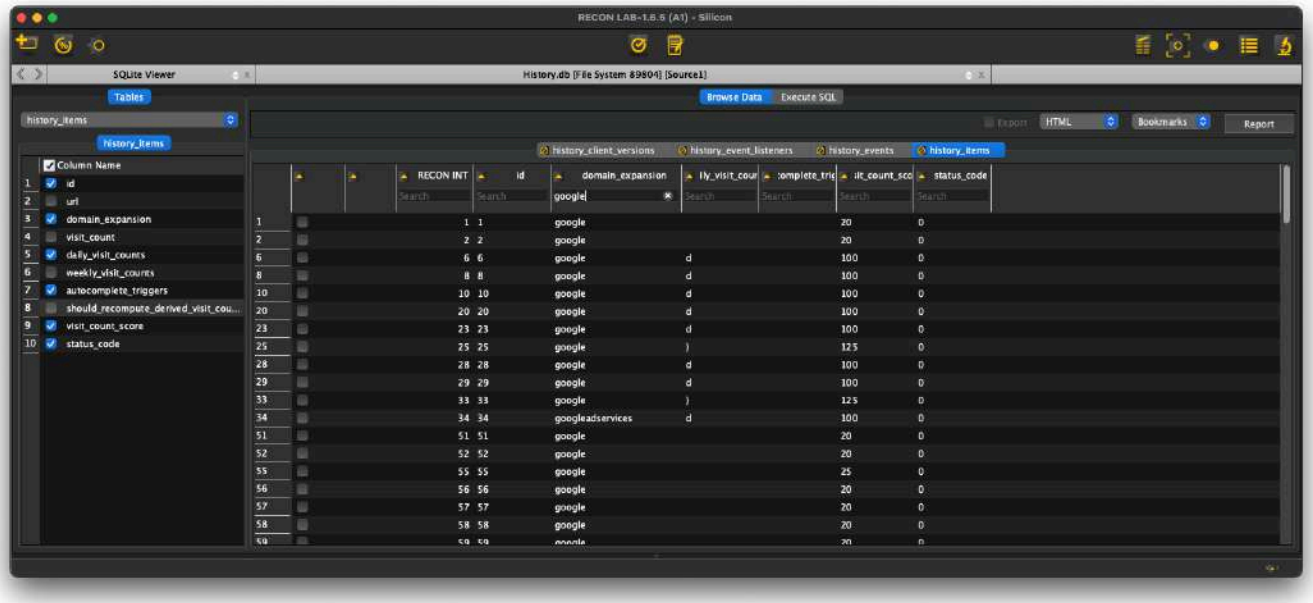


To open a file in the SQLite Viewer, right-click and select “Open With – SQLite Viewer”. If you would like to add the file to review later in the Sidebar Bucket select “Send to Bucket – SQLite Viewer”.



The SQLite Viewer will open in the Main Viewer window.

20.3.0.2 Filtering Table Data



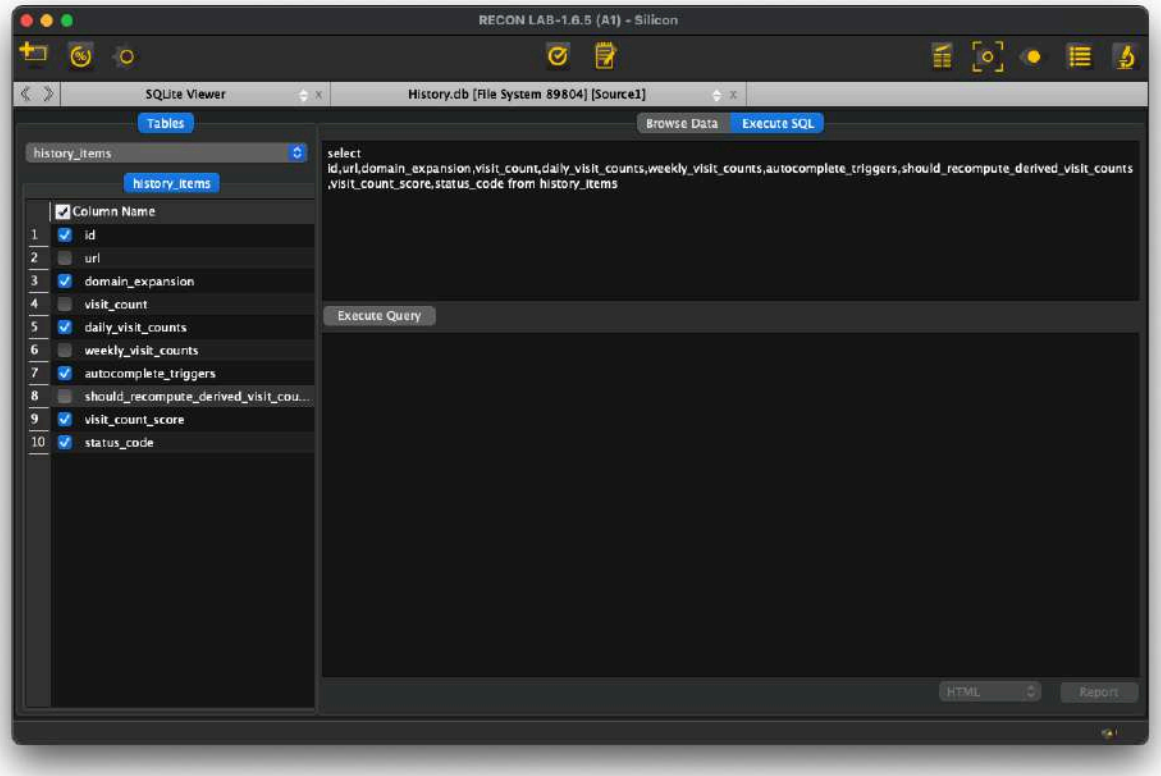
Individual SQLite tables can be selected by using the Tables dropdown box.

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

Keyword searches can be performed by entering a keyword in the Searchbox underneath the individual columns.

20.3.0.3 Executing a SQLite Query

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



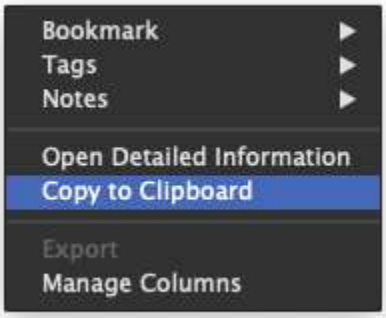
To execute an SQLite query first select a table then click the “Execute SQL” tab.

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

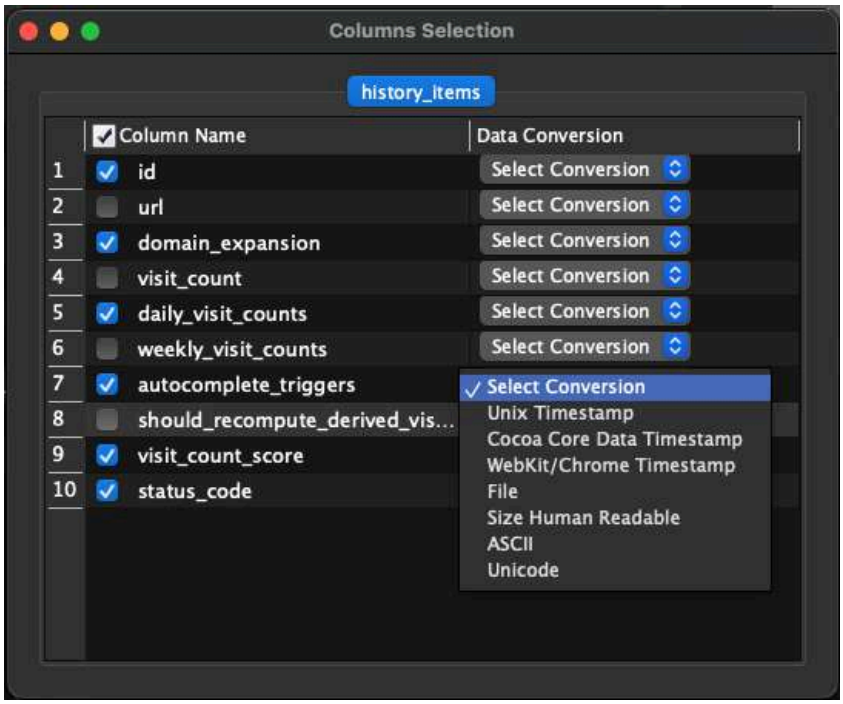
Once the query has been entered click the “Execute Query” button to view the results.

20.3.0.4 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”.

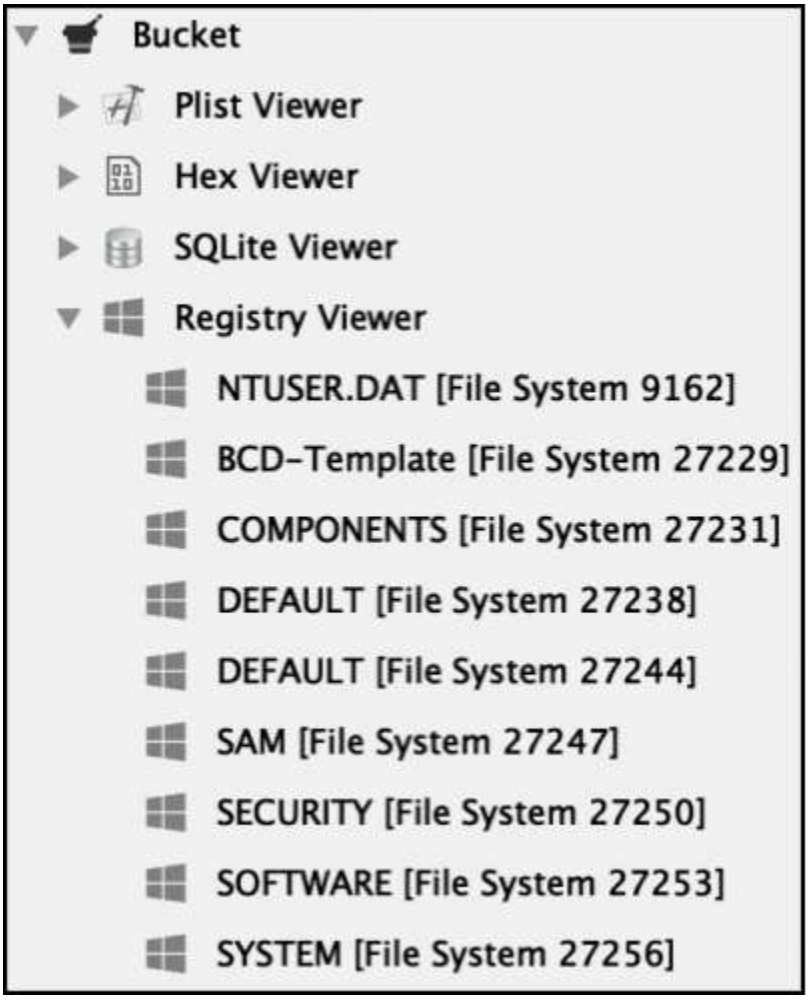


From the “Manage Column” window, you can select which of the columns you would like converted to a different display method. Select your desired format from the dropdown menu.

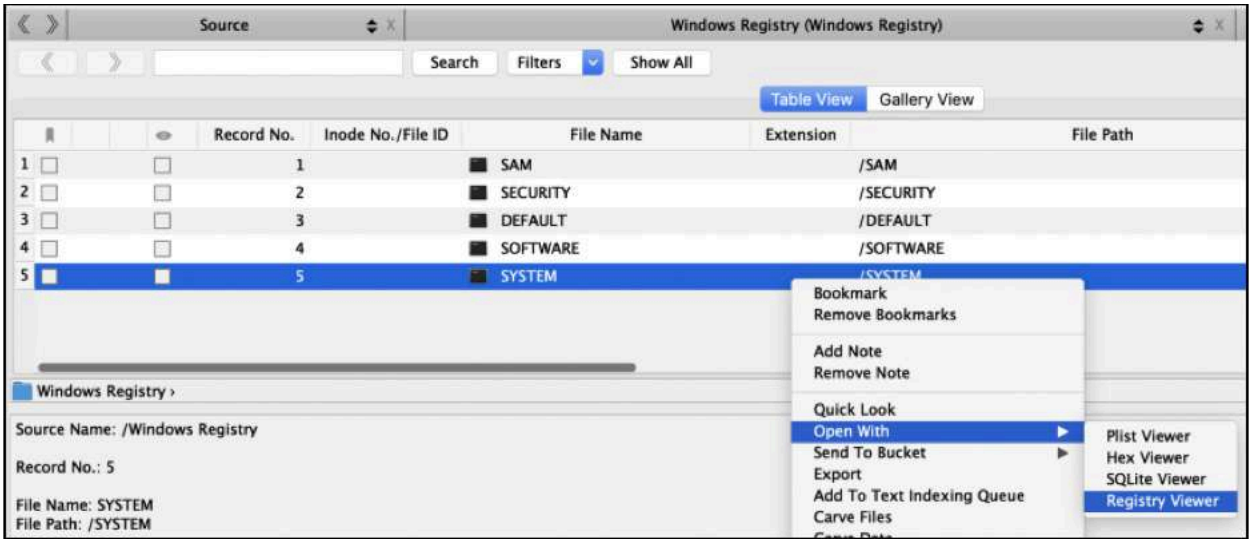


After selecting the conversion type, select the desired entry to see the conversion in the main window of the SQLite viewer.

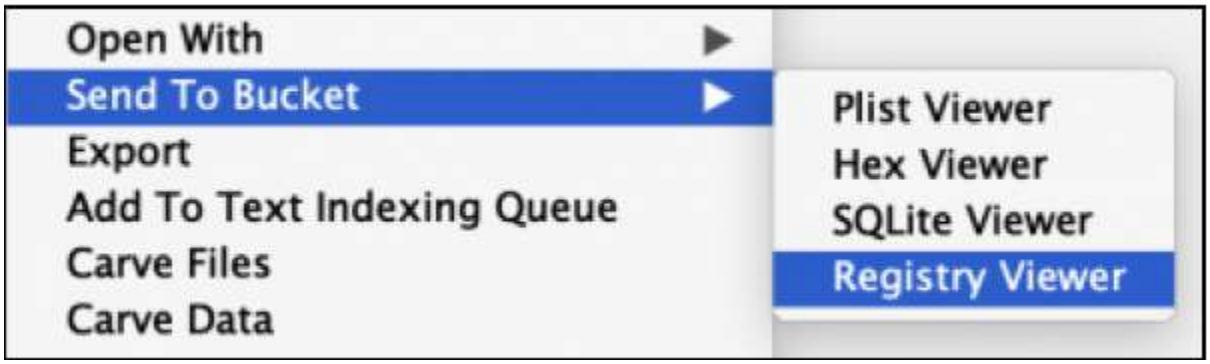
20.4 Registry Viewer



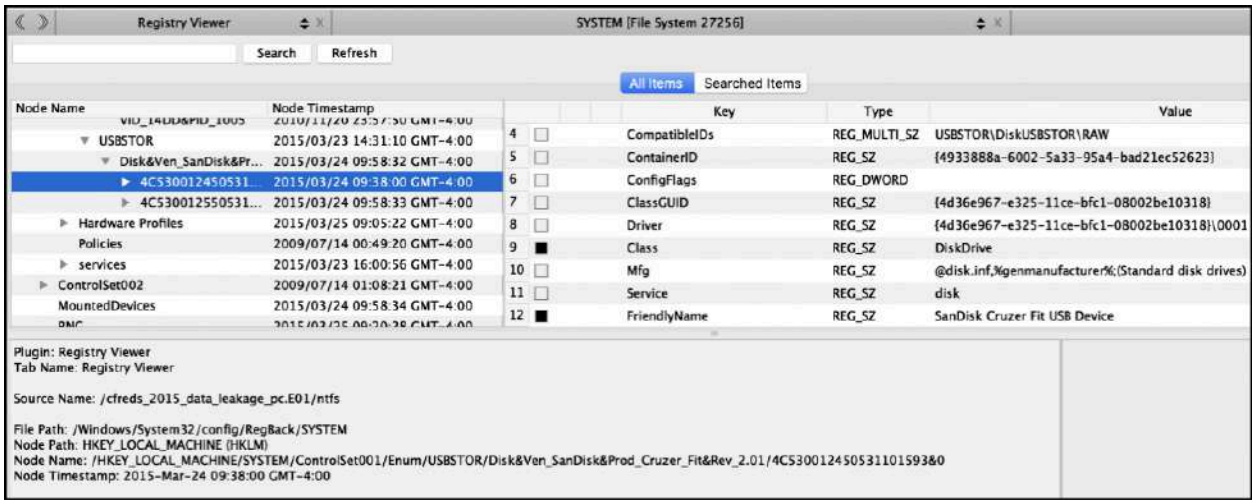
When a source is added to RECON LAB that contains Windows registry information it is automatically parsed and added to the Sidebar Bucket under Registry Viewer.



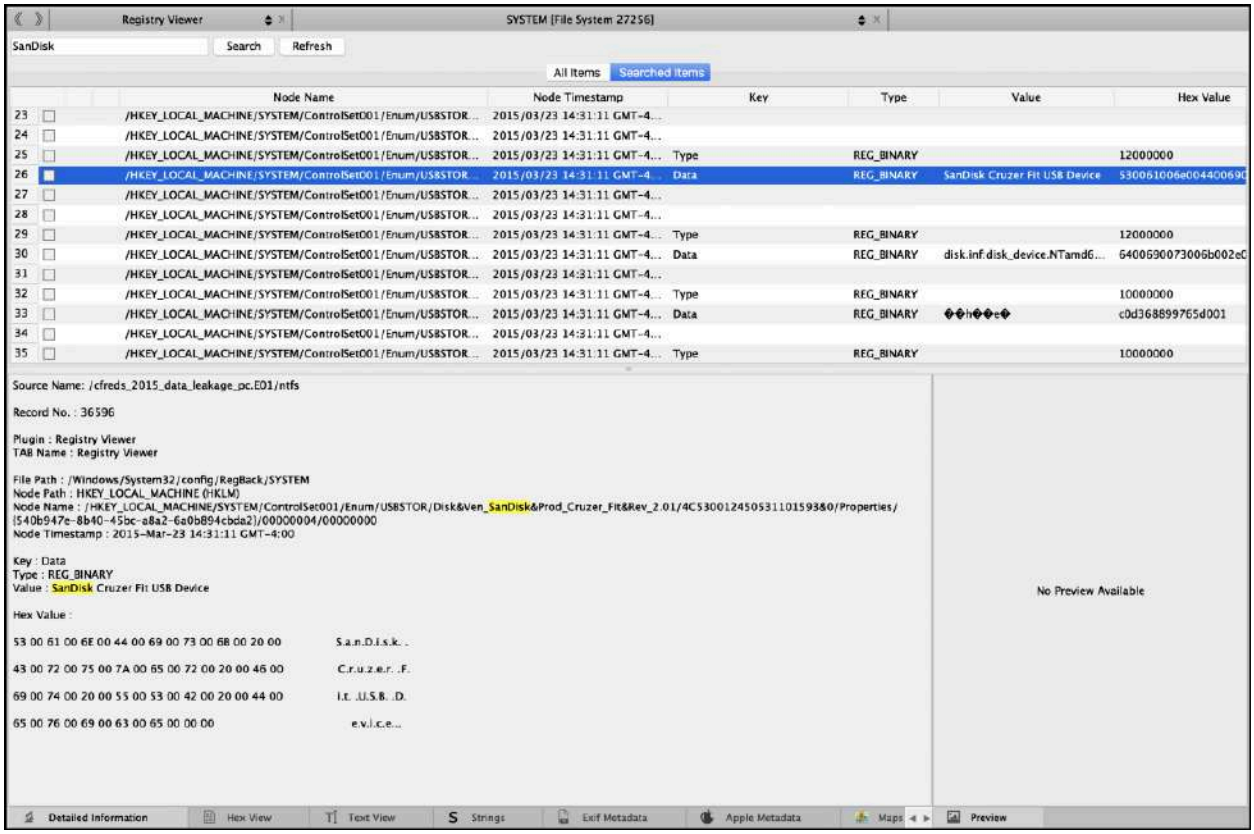
If you need to manually load a Windows registry artifact right-click on the file and select “Open With – Registry Viewer”.



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.

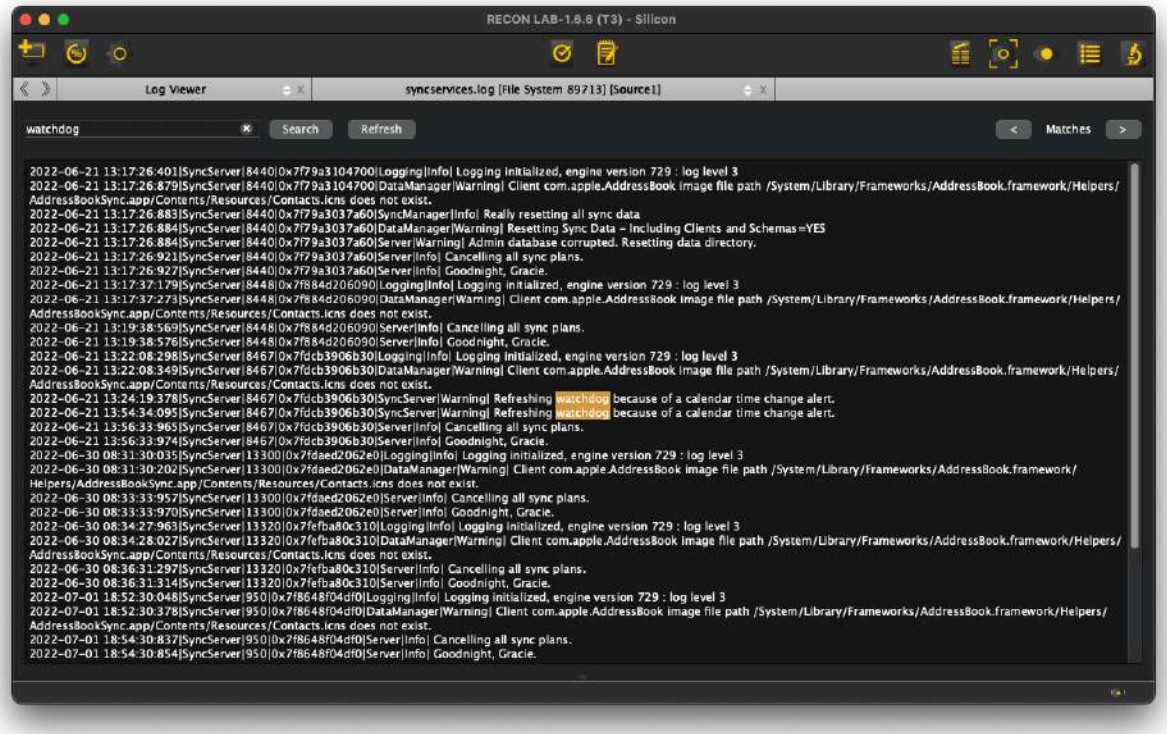


To search inside a hive enter a keyword in the search field and click “Search”.

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

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

20.5 Log Viewer



When a “.log” file from macOS is opened in the Log Viewer, RECON LAB displays the file’s contents in a readable format. Once the log file is loaded, the examiner can:

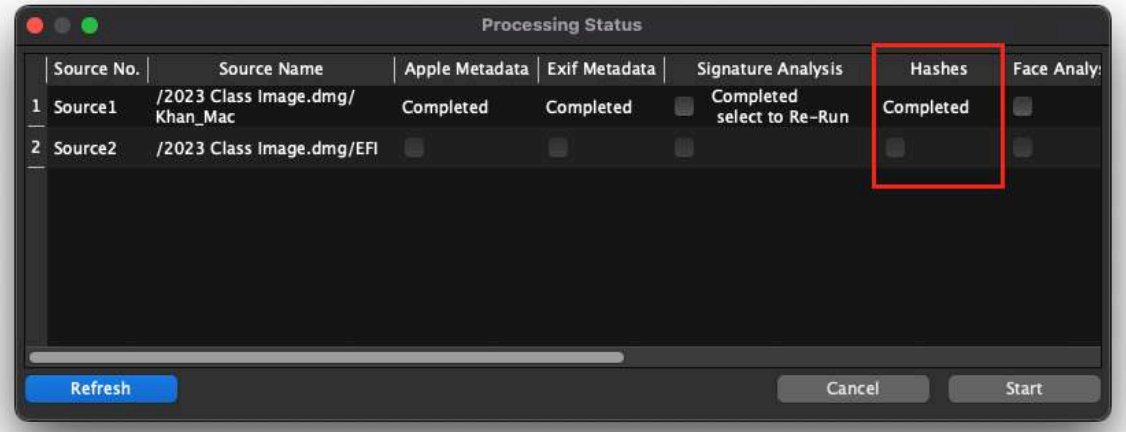
- Perform a keyword search using the Keyword Search text box
- Navigate through each match using the < and > buttons

This functionality helps examiners quickly locate relevant entries within large log files.

---

21 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.



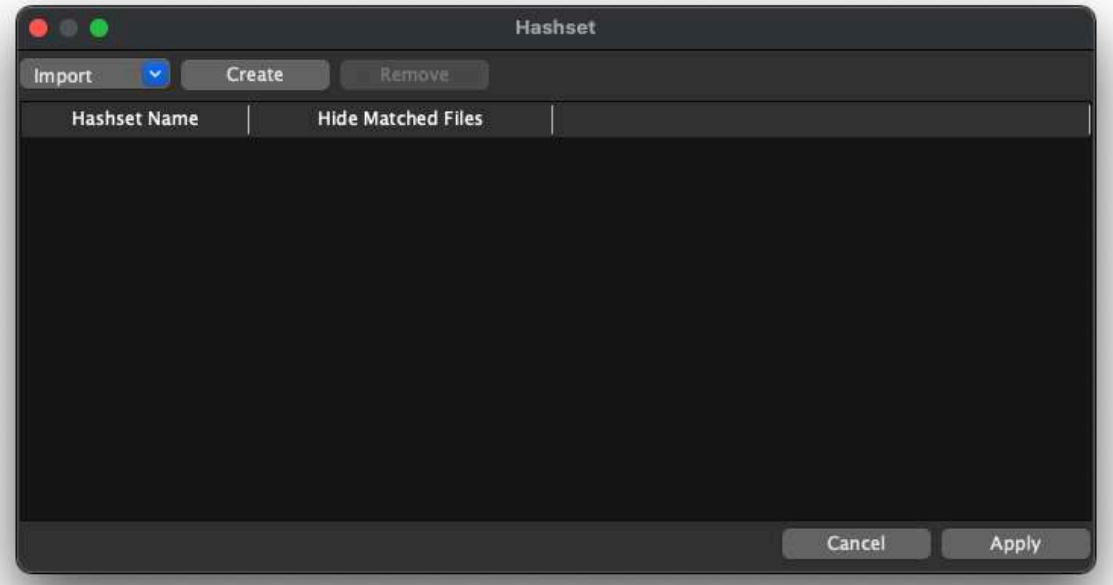
Before using hash set databases RECON LAB will need to hash the files in the source first. To find out if hashing is completed for a source click the Processing Status icon in the Top Menu.

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

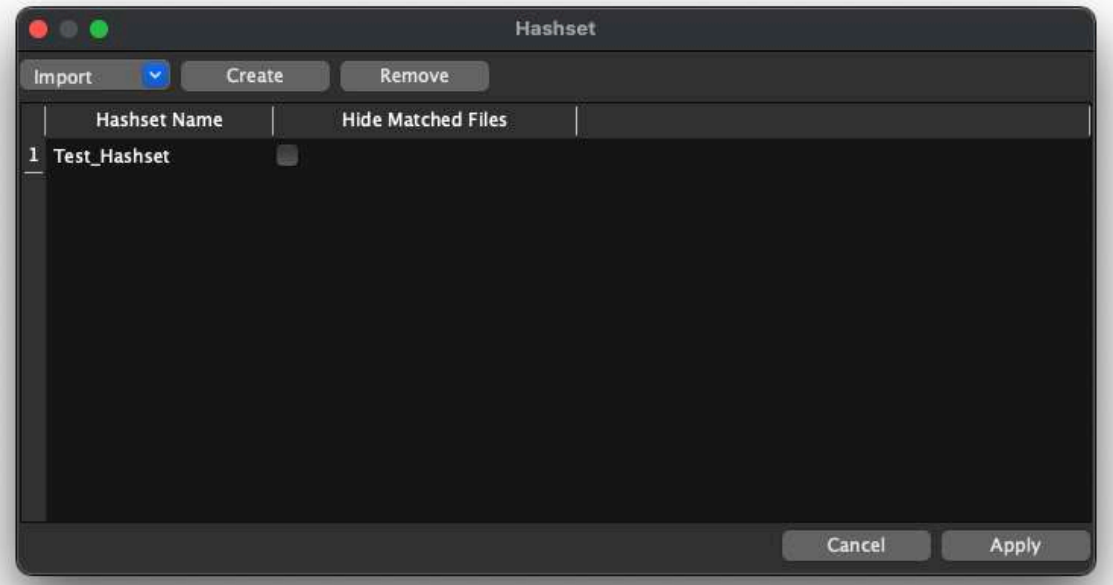
21.1 Creating Hash Sets

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.

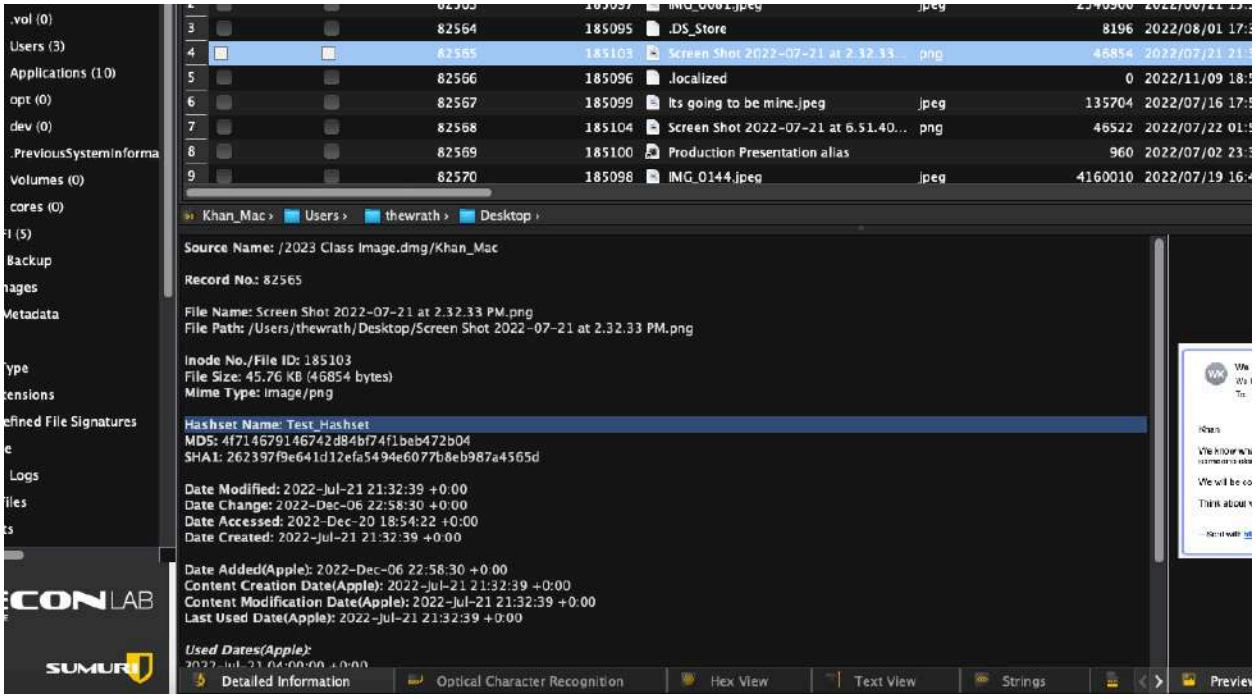


The Hash Set main window will appear.



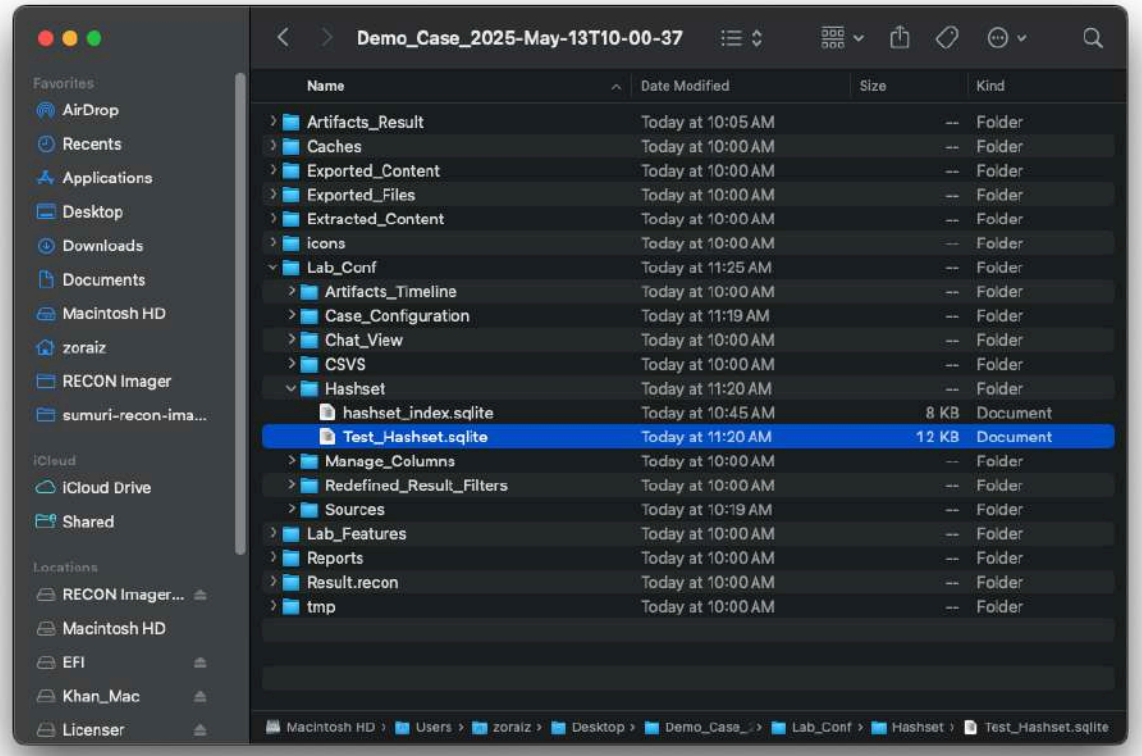
Click “Create” and enter a name for your new hash set and click “Create” again. The new hash set category is now created.

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.

21.1.0.1 Archiving the Hash Set Database

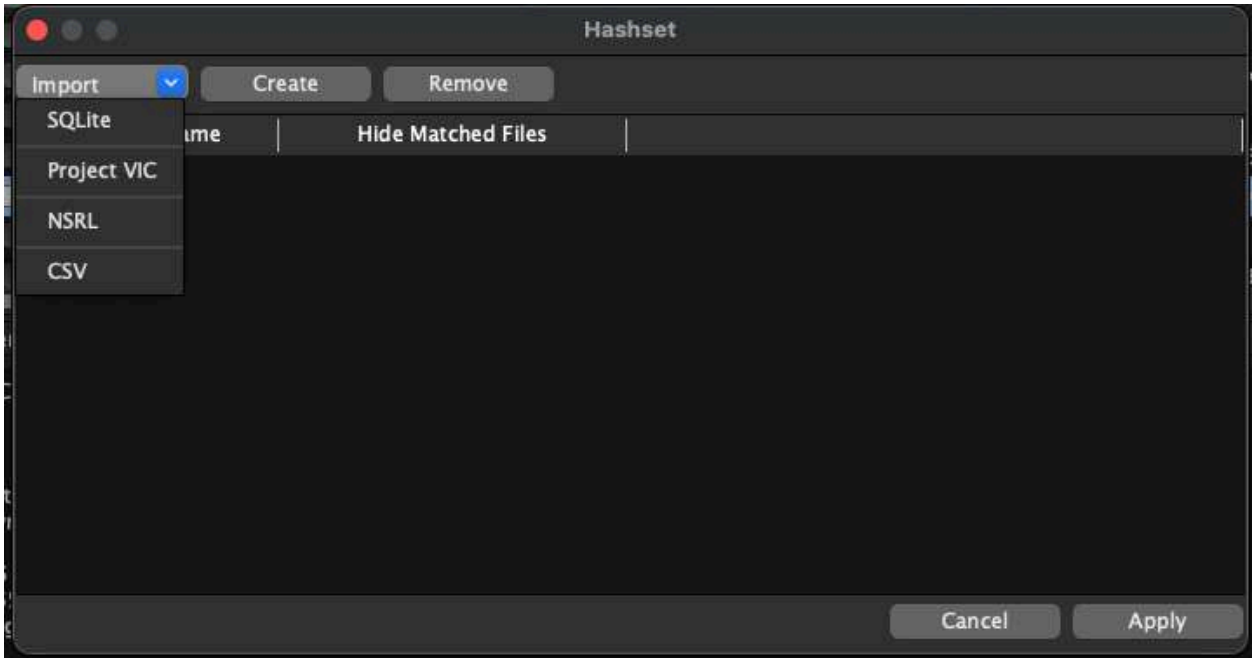


If you want to archive your newly created hash set database so it can be imported into other cases navigate the “Lab_Conf – Hashset” directory in your RECON LAB Case Folder. Here you will find the hash set databases to archive.

21.2 Importing Hash Sets

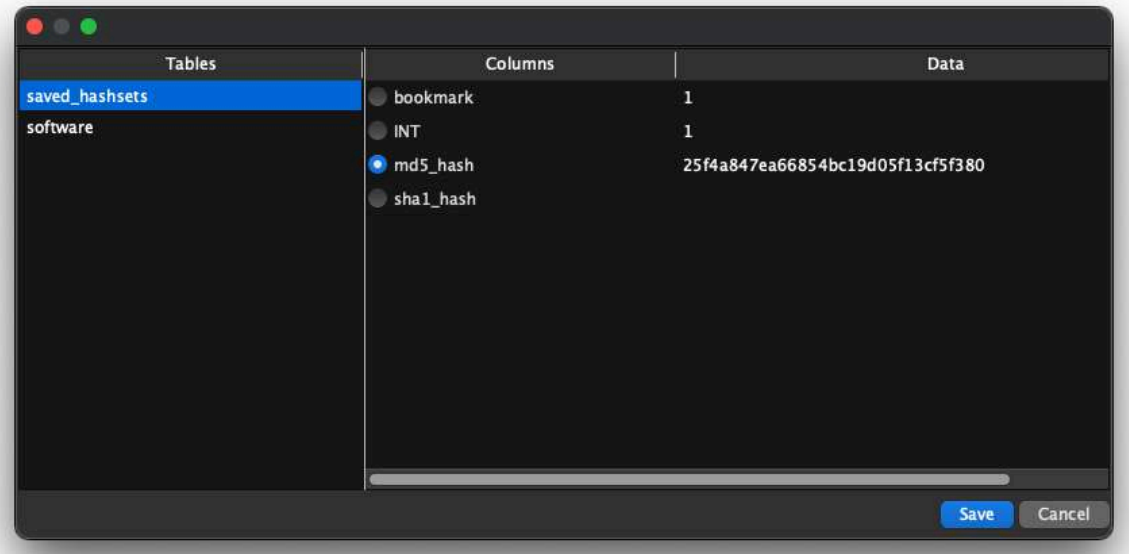
RECON LAB can import the following hash set database formats:

- 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”.

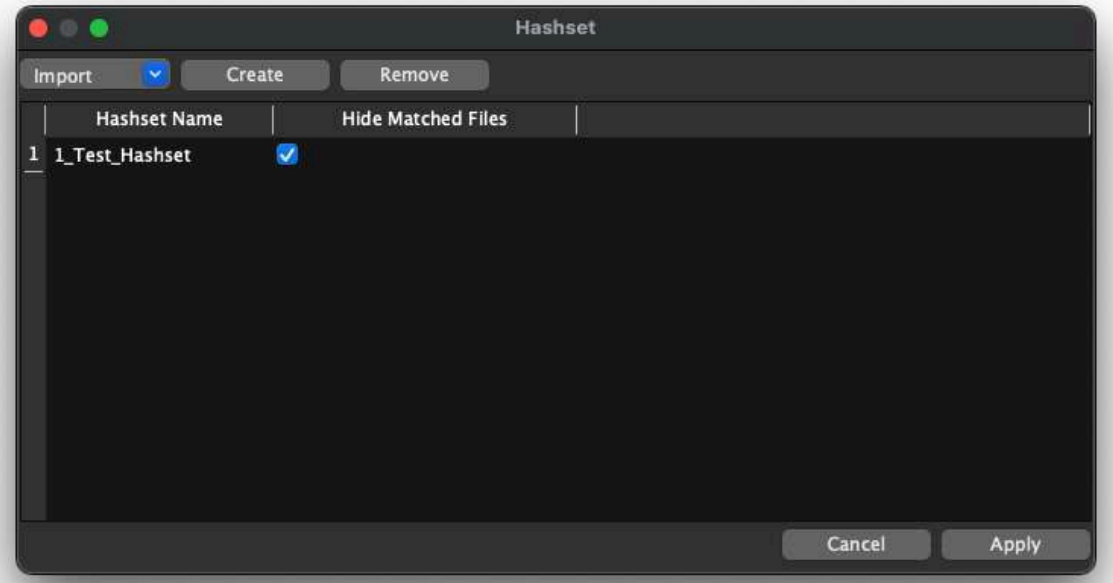


You may be prompted to select a specific table in order to import. For RECON LAB SQLite databases select the “saved_hashsets” table and the “md5_hash” column. After clicking “Save” the new hash set will be available for use.

21.3 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”.

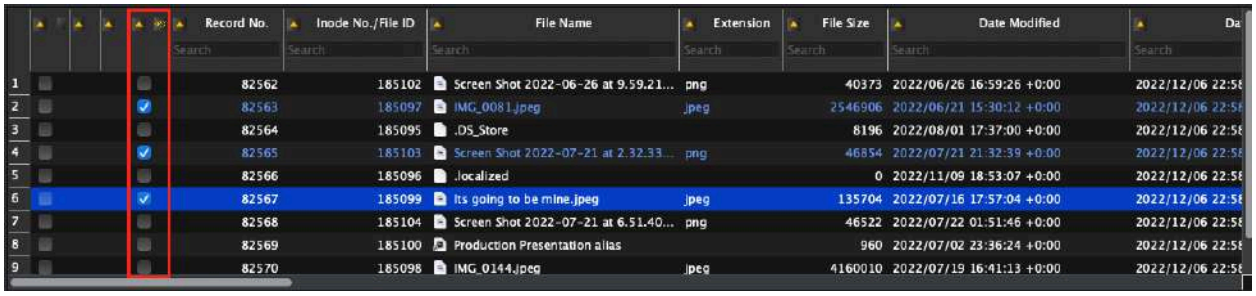
Files matching the hashes in the hash set database will be hidden.

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

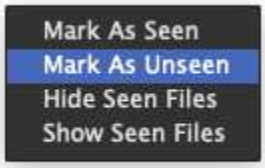
---

22 Hide or Show Files

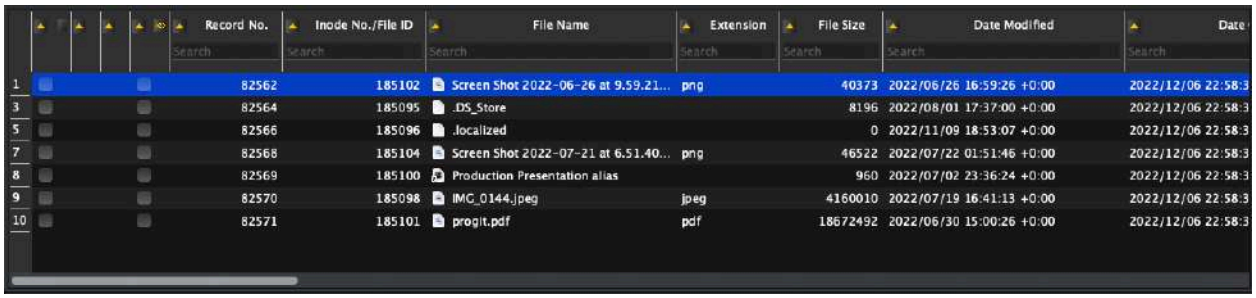
RECON LAB includes a feature to “Mark files as Seen”. This is a way of tracking files that you have already reviewed. To mark a file as seen click the checkbox in the “Seen” column.



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.

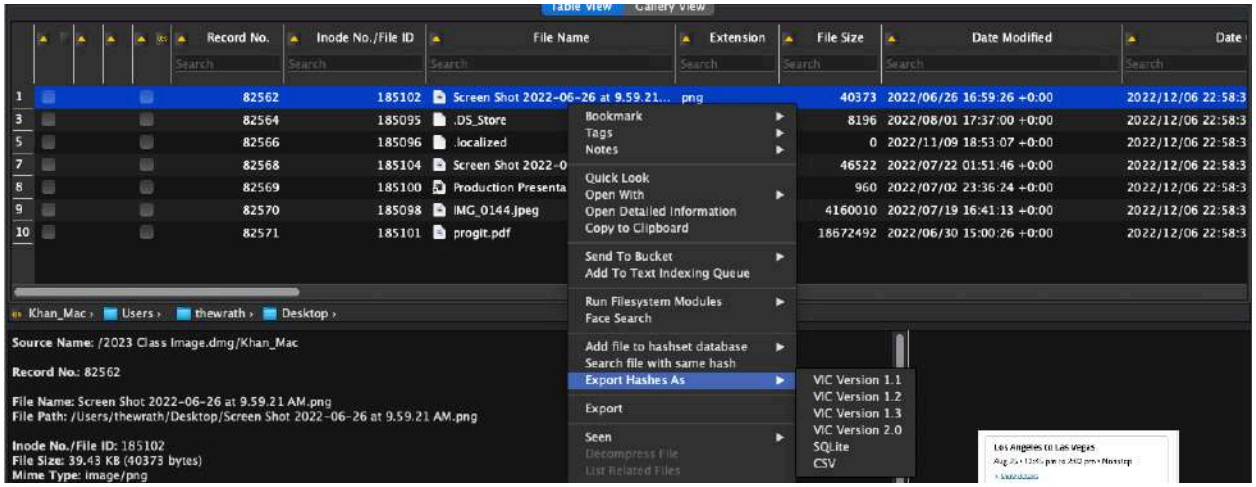


---

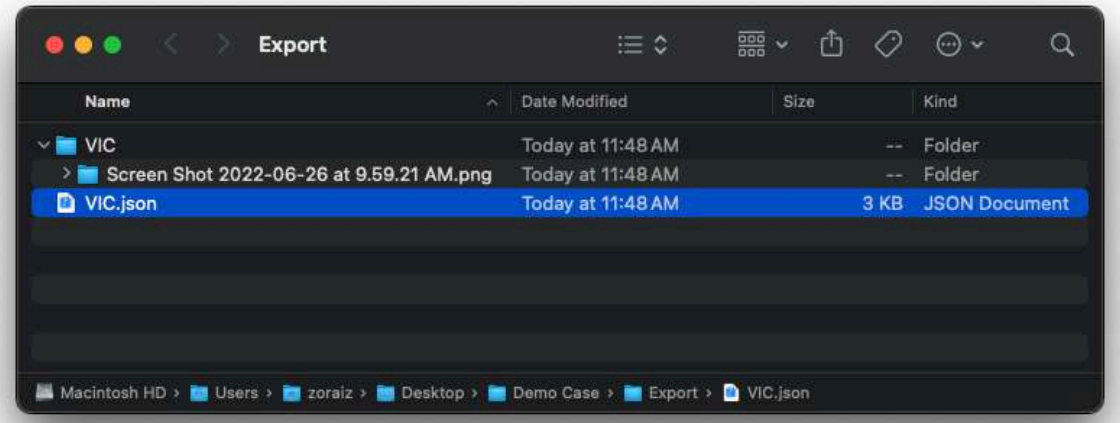
23 Project Vic

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

23.0.0.1 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.



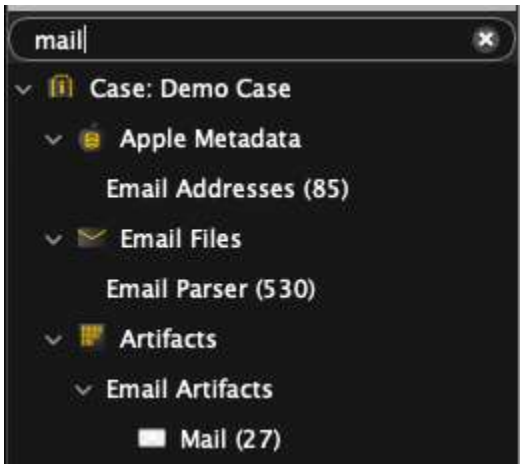
The above picture is an example of a Project VIC export using RECON LAB.

---

24 Email Analysis

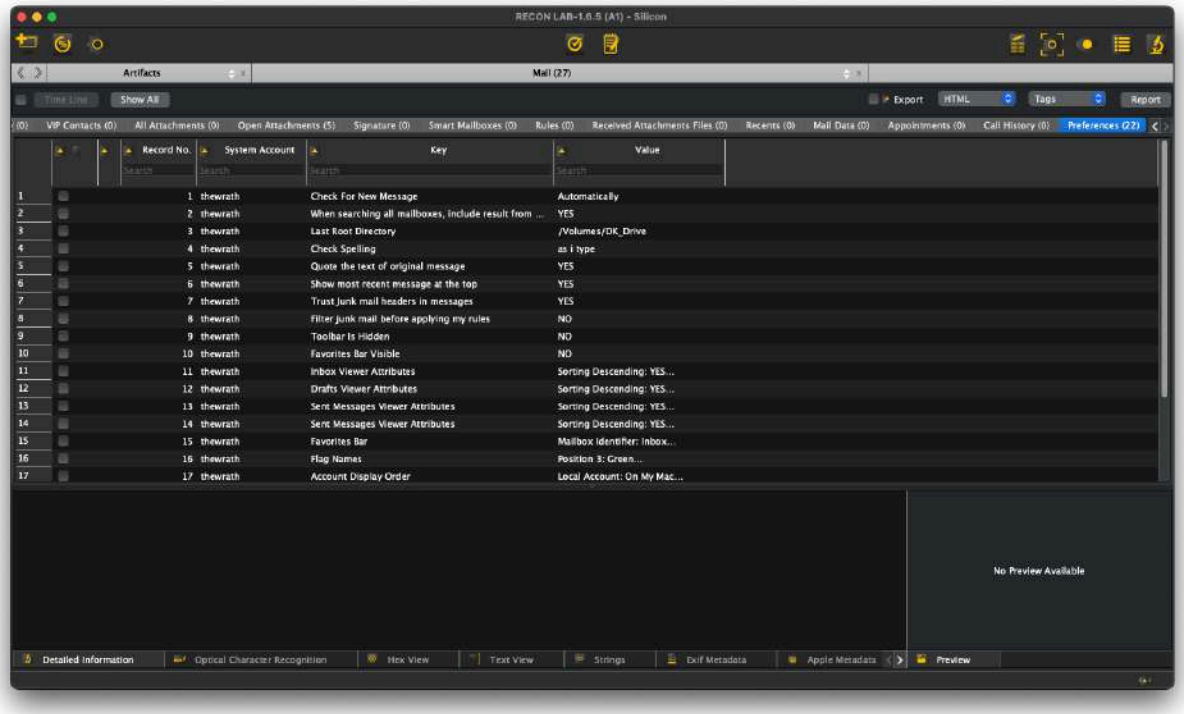
There are two ways to conduct email analysis in RECON LAB.

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



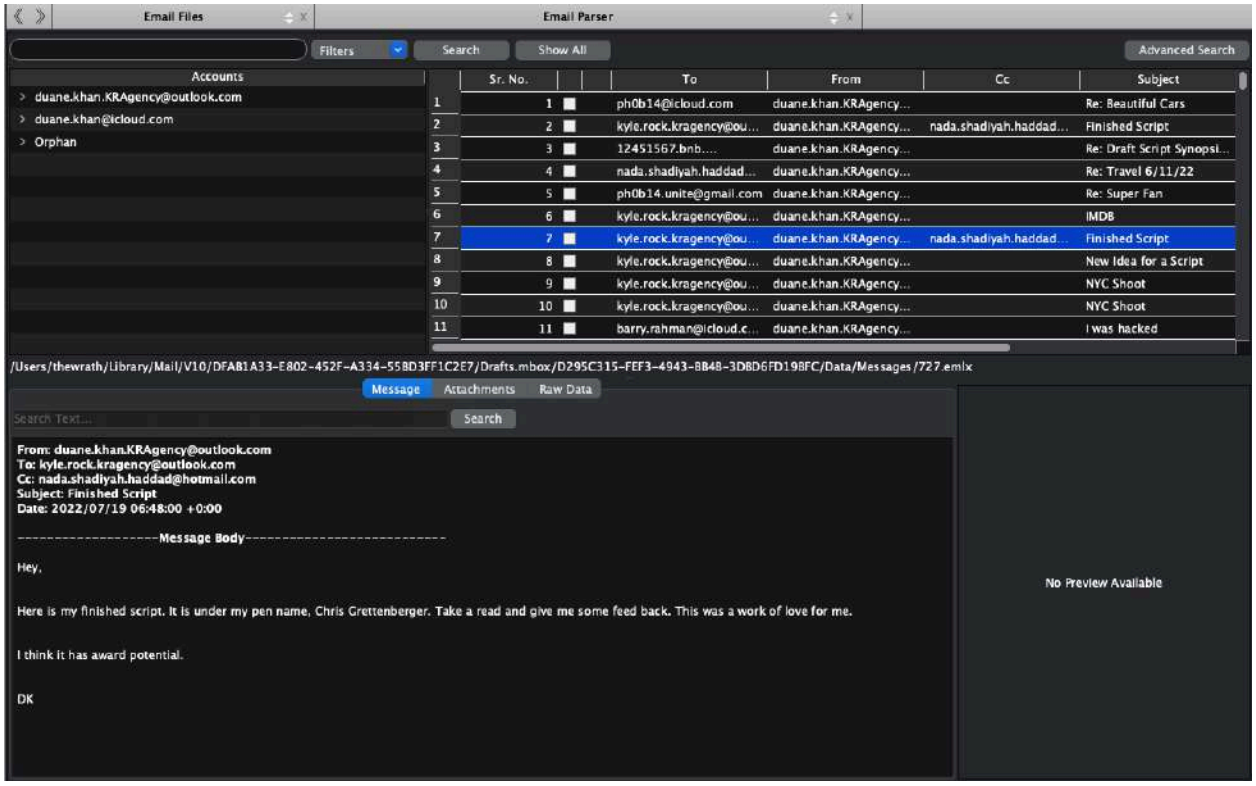
24.0.0.1 Automated Artifacts Analysis

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.



24.0.0.2 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.



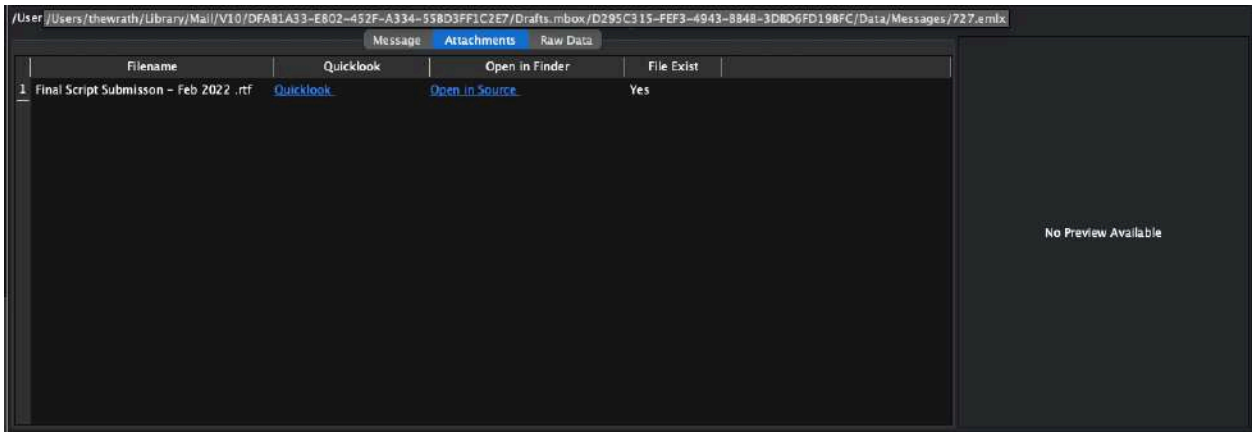
The upper left panel is the “Accounts” pane. All supported mail accounts will be found here along with their mailboxes.

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

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

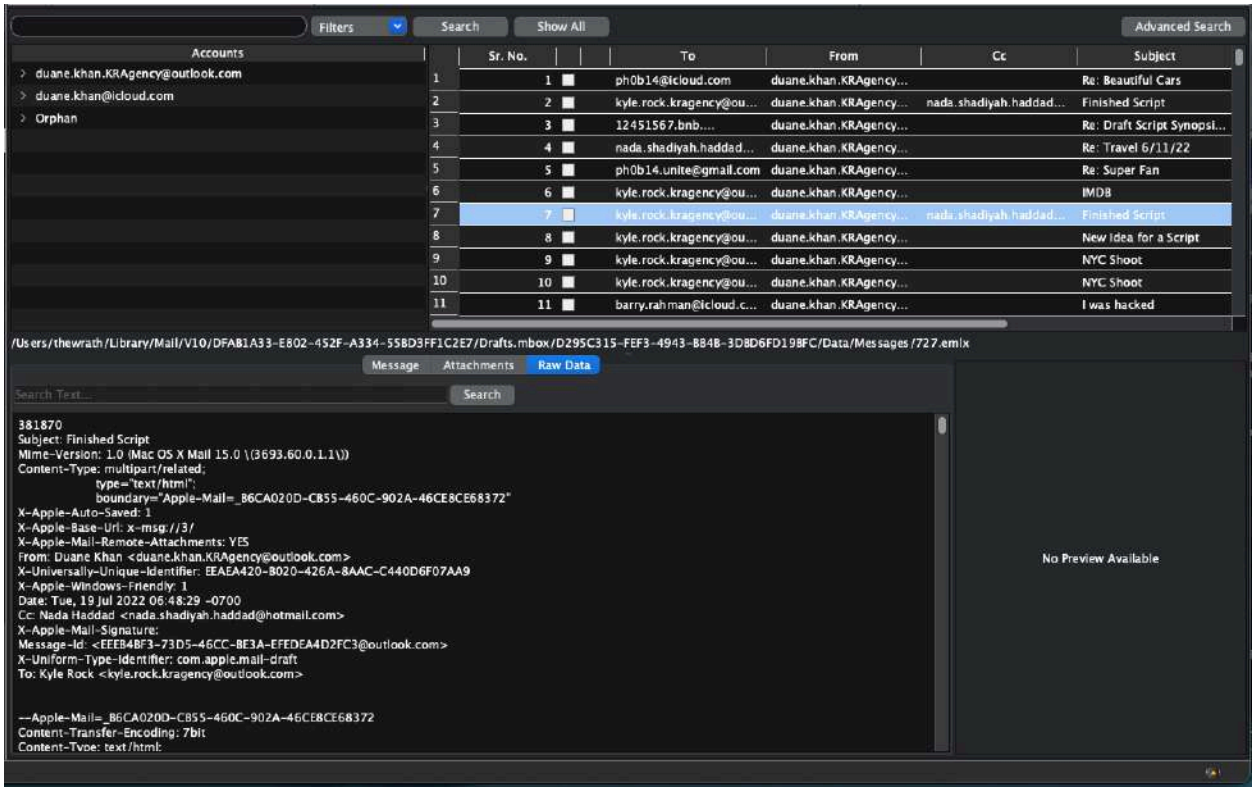
The “Message” tab seen above shows the message in HTML view.

24.0.0.3 Attachments



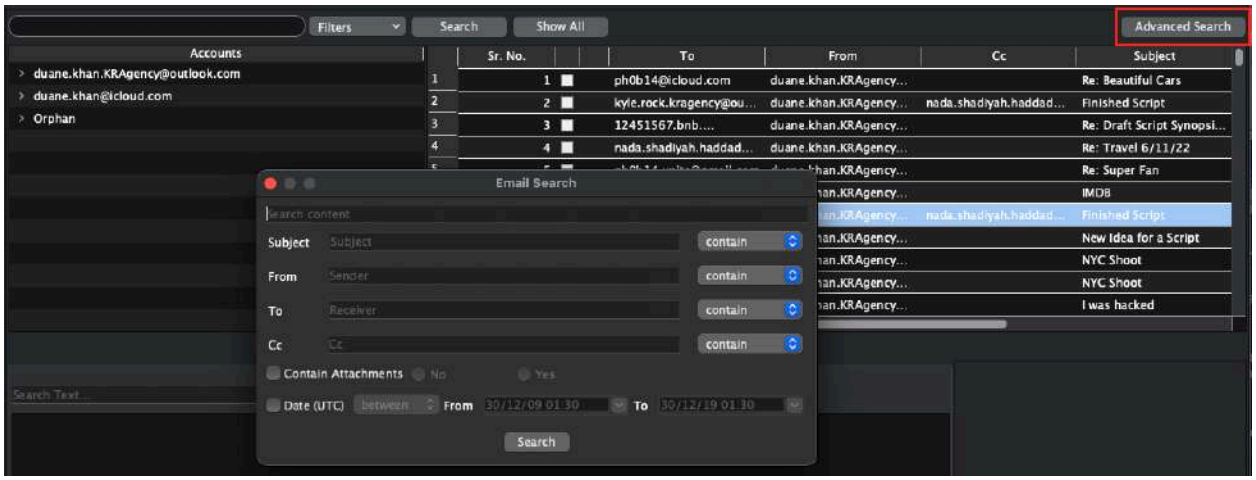
If an attachment exists they will be listed in the “Attachments” tab. Two links are provided for opening the file in the source (“Open in Source”) and to preview the file with “Quick Look”.

24.0.0.4 Viewing Message As Raw Data



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

24.0.0.5 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.

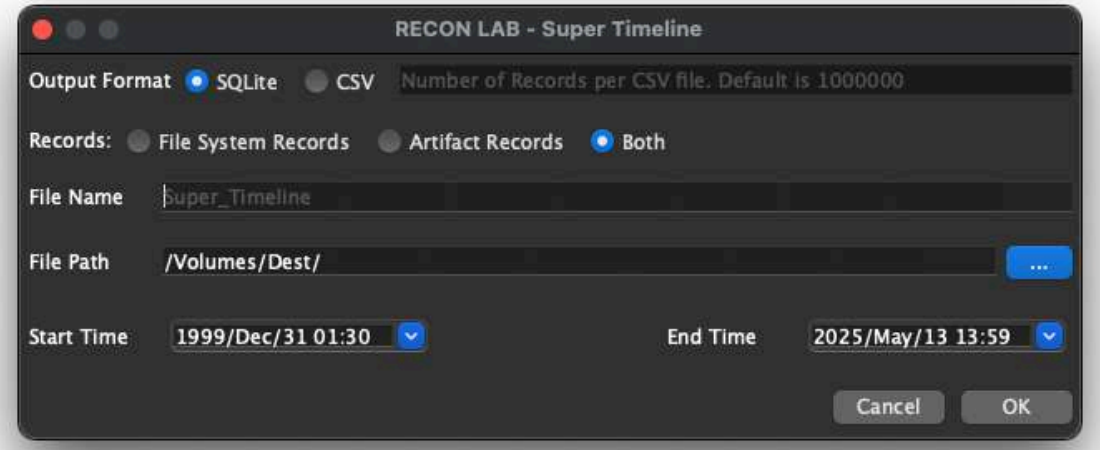
25 Timeline Analysis

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.

25.1 Super Timeline

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



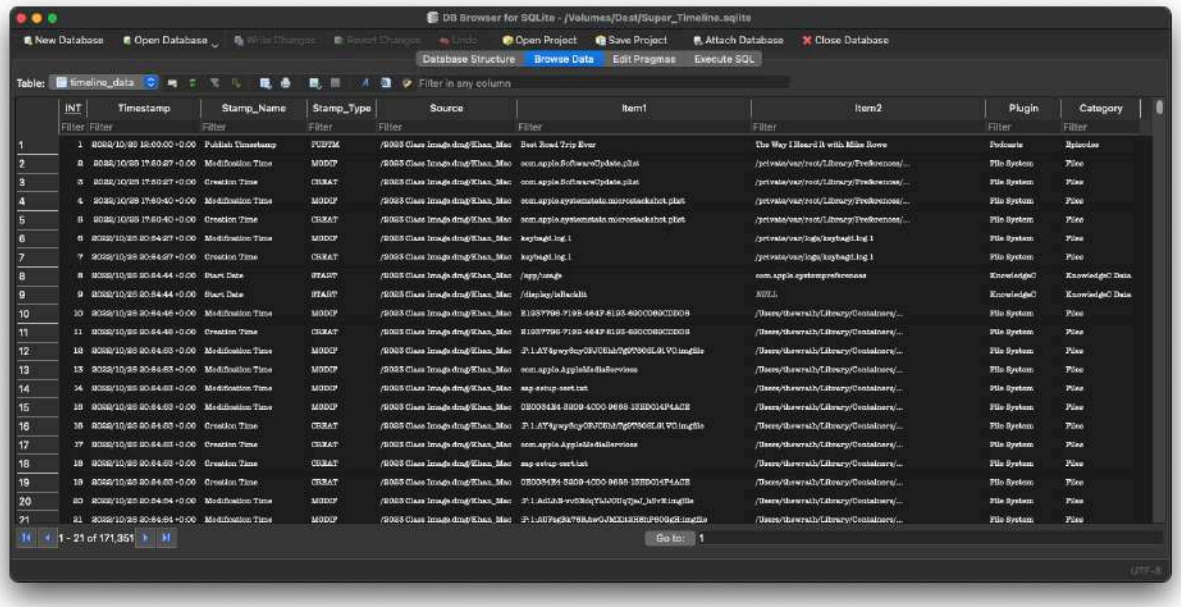
Once selected the Super Timeline configuration window will appear.

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.

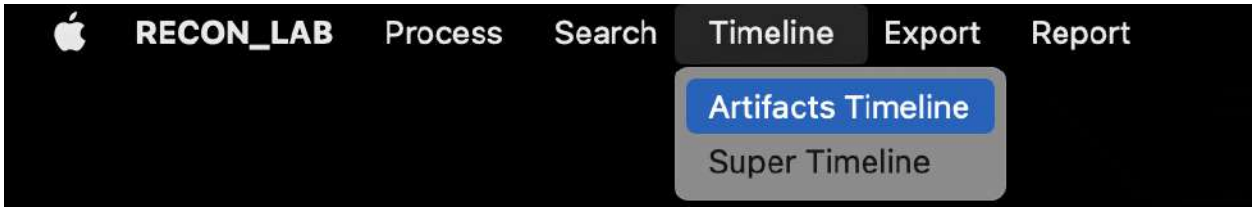
To create the Super Timeline provide a File Name, File Path and click OK.



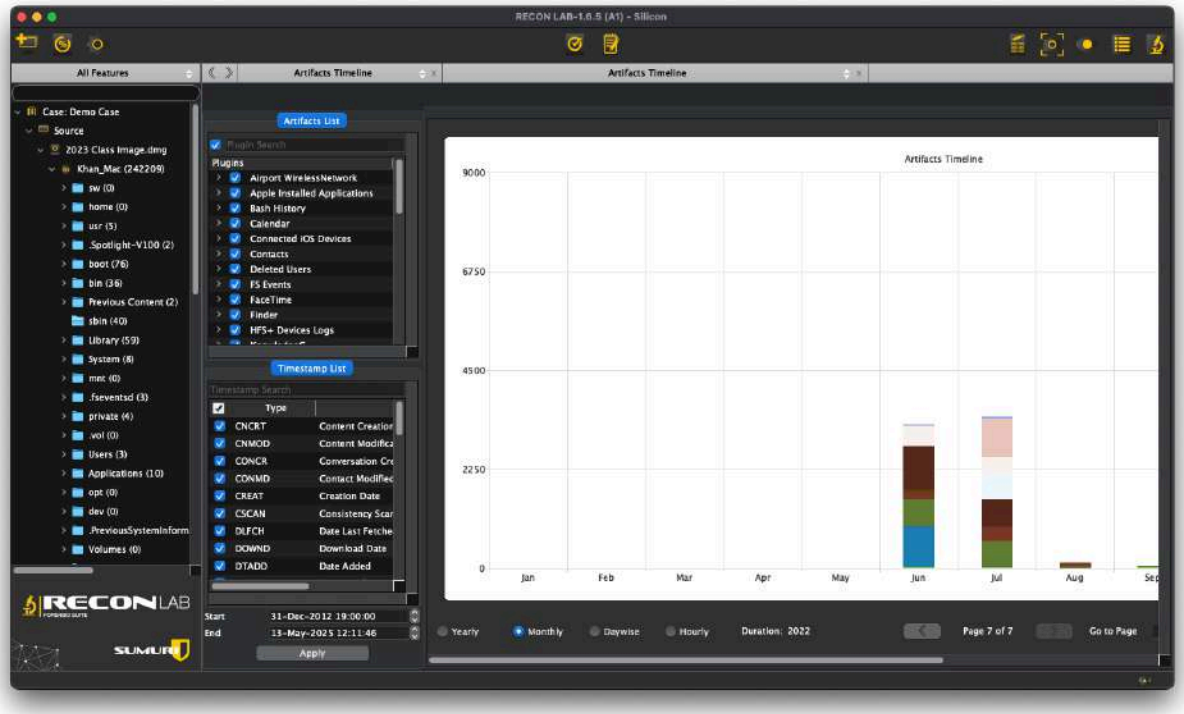
Once the Super Timeline is created you will be prompted to review the results.

25.2 Artifacts Timeline

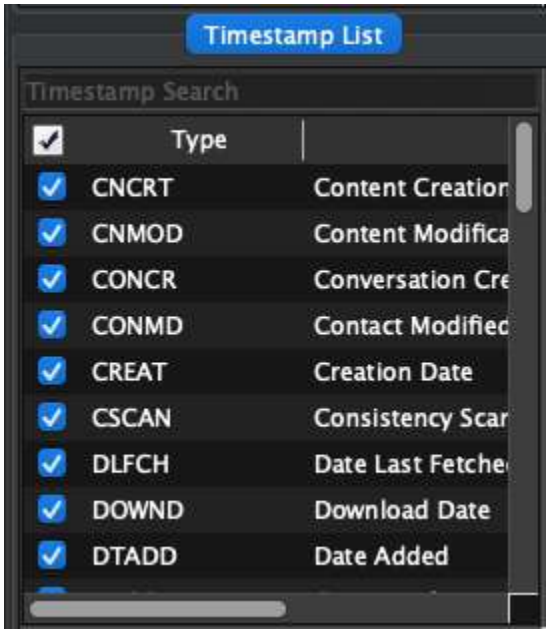
In order for the Artifacts Timeline to create a timeline make sure that you have run some or all of the Artifacts and Plugin modules for automatic analysis.



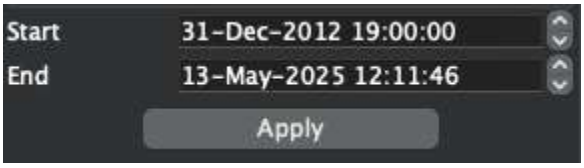
An Artifact Timeline can be created by selecting Timeline > Artifact Timeline from the Menu Bar.



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

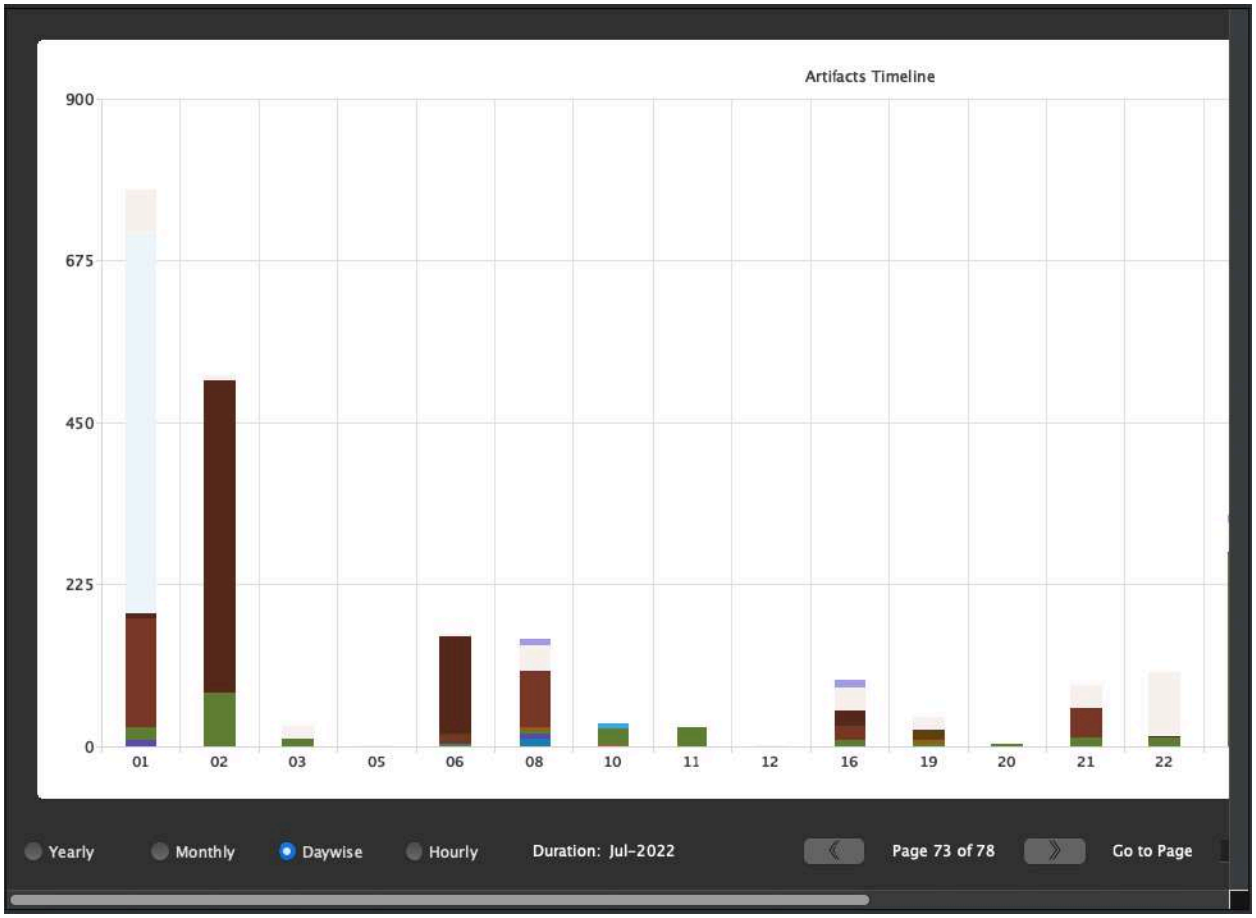


Note: FS Events artifacts can contain millions of records. Be aware that this will take time to load.



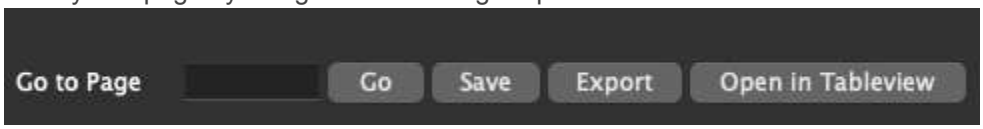
Next, select your Start and End dates and click Apply to create the Timeline.

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.

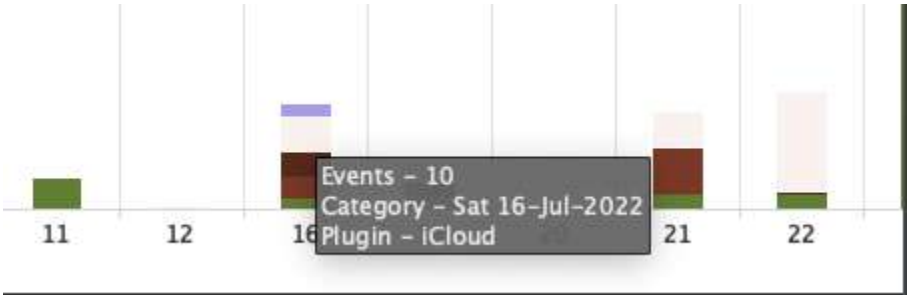
To move backward and forward through the timeline pages use the navigation buttons or go directly to a page by using the “Go to Page” option.



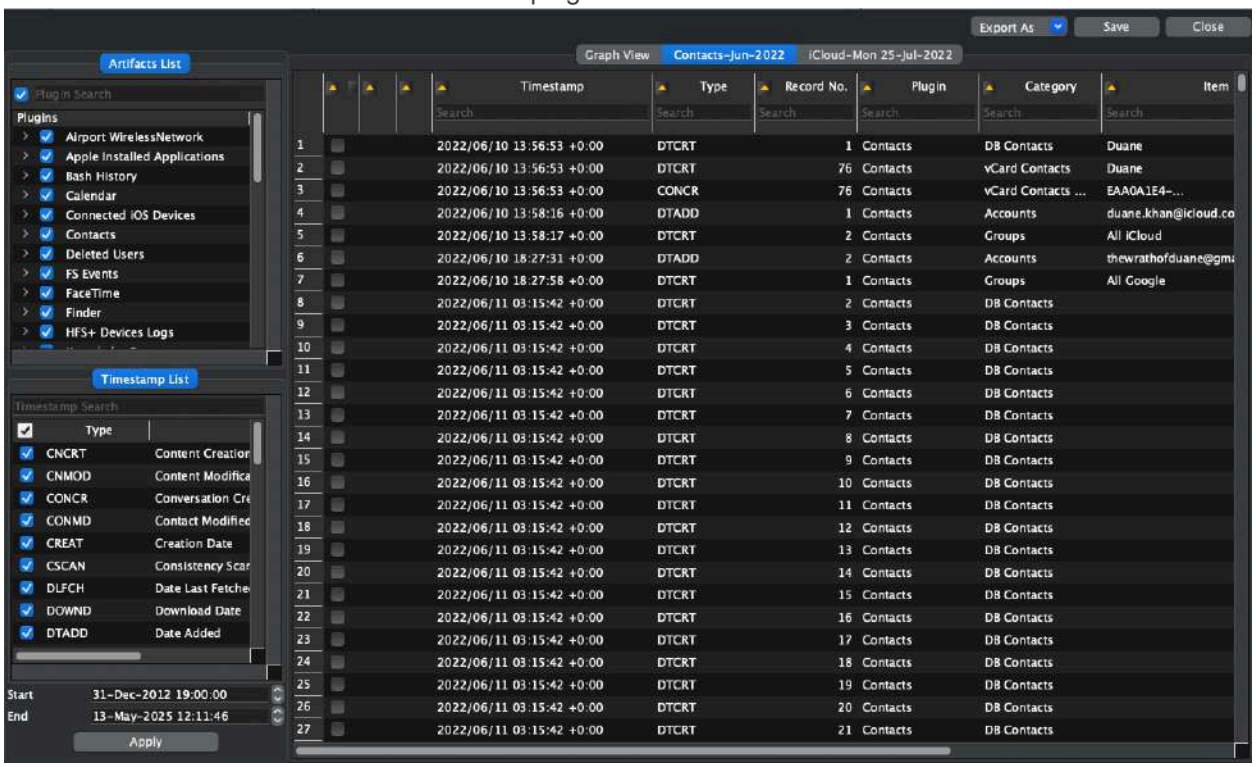
In the graphical view, you can save a picture of the current graph by clicking the “Save” button.

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”.

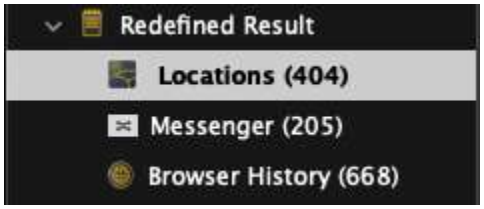
Clicking the “Close” button will close the graph.

---

26 Redefined Results

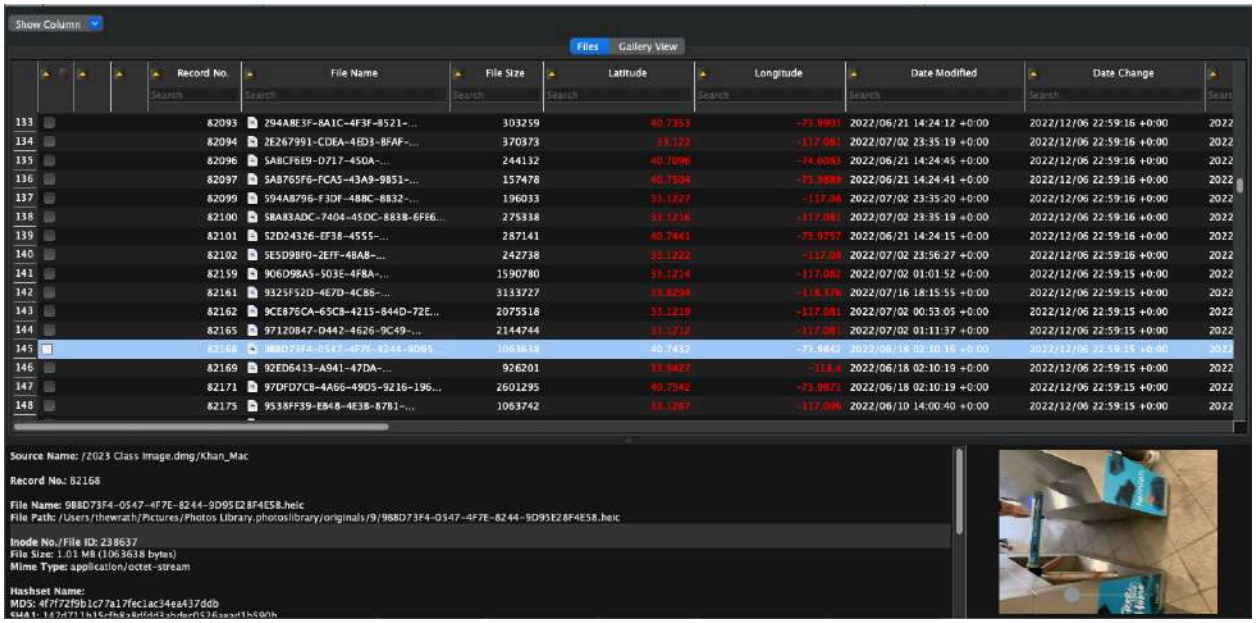
Redefined Results are a way to collate data across different devices that use different applications. It allows a complete picture of events even when a person is using a mobile device, laptop, and a computer in a single day.

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.

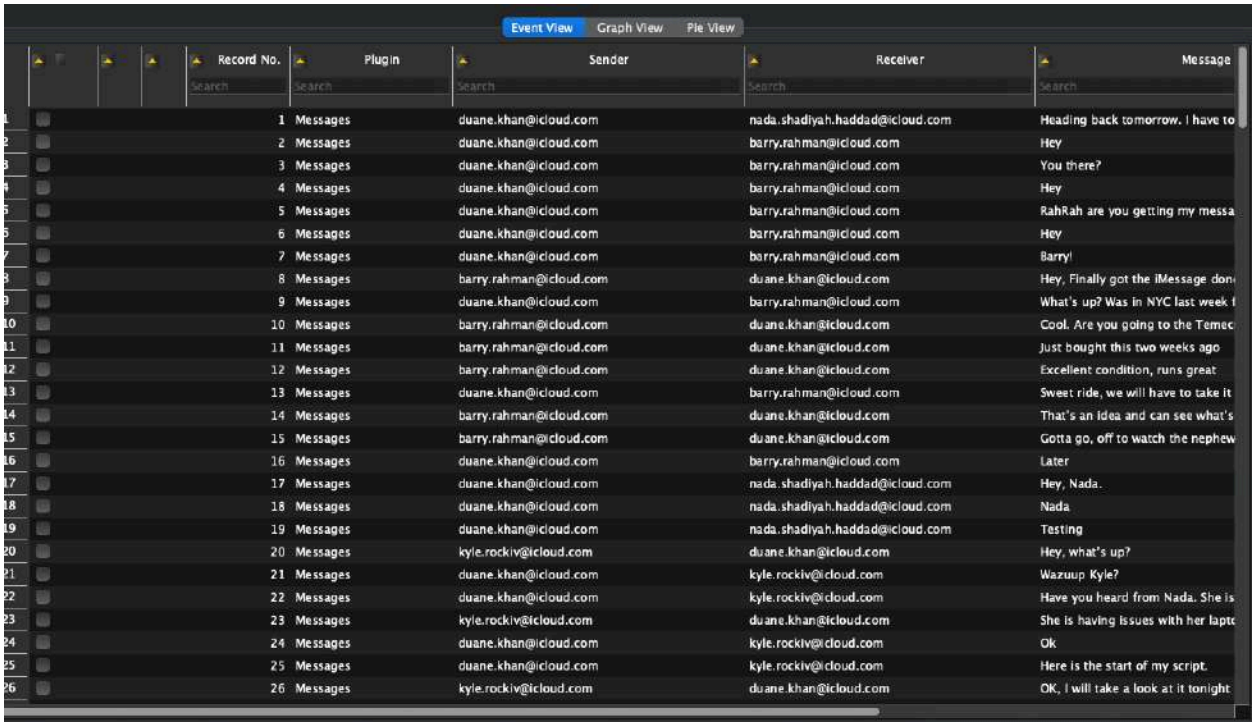
26.1 Collated Location History



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

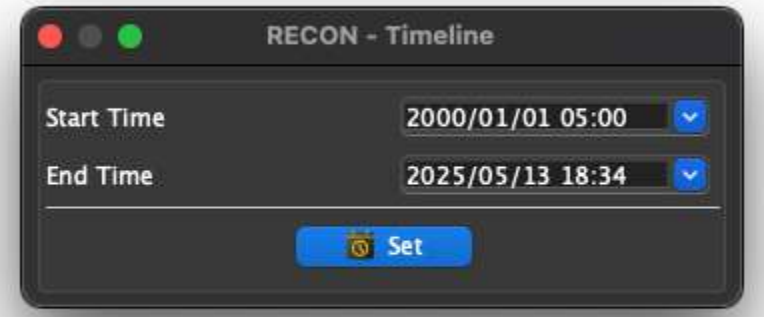
26.2 Collated Messaging

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

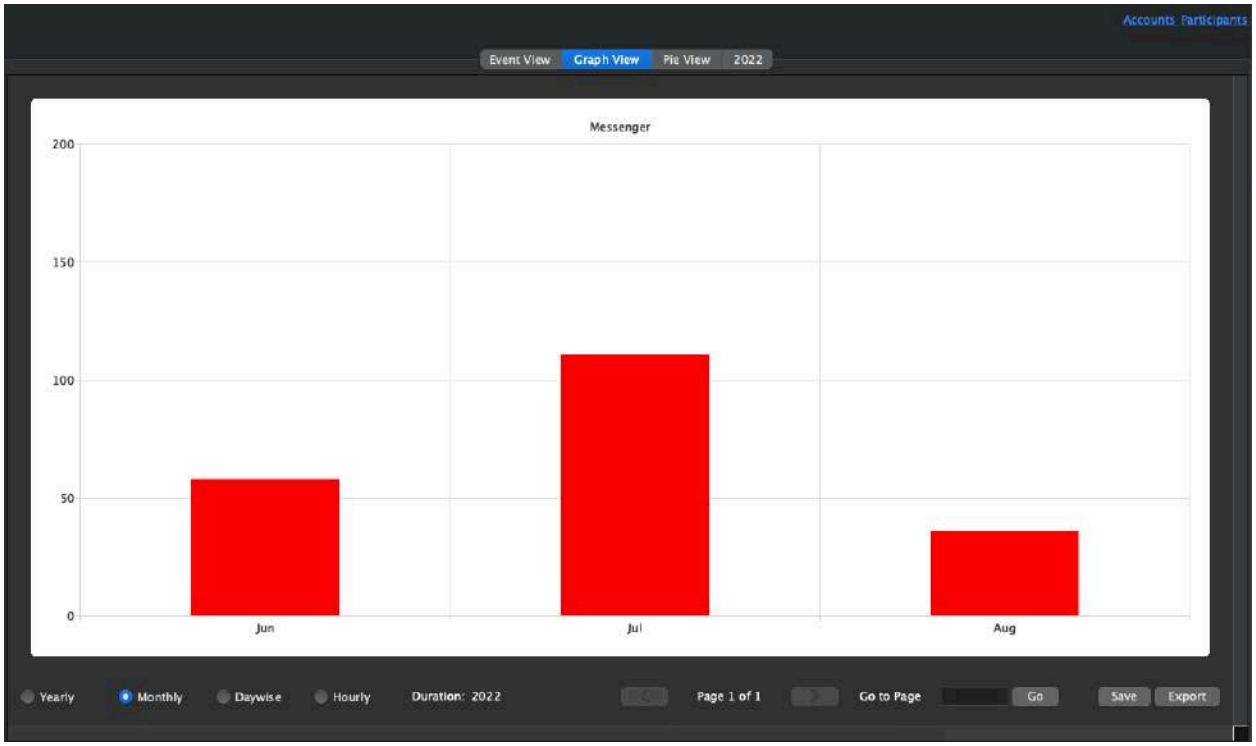


	Record No.	Plugin	Sender	Receiver	Message
1	1	Messages	duane.khan@icloud.com	nada.shadiyah.haddad@icloud.com	Heading back tomorrow. I have to
2	2	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	Hey
3	3	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	You there?
4	4	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	Hey
5	5	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	RahRah are you getting my messa
6	6	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	Hey
7	7	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	Barry!
8	8	Messages	barry.rahman@icloud.com	duane.khan@icloud.com	Hey, Finally got the iMessage don
9	9	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	What's up? Was in NYC last week
10	10	Messages	barry.rahman@icloud.com	duane.khan@icloud.com	Cool. Are you going to the Temec
11	11	Messages	barry.rahman@icloud.com	duane.khan@icloud.com	Just bought this two weeks ago
12	12	Messages	barry.rahman@icloud.com	duane.khan@icloud.com	Excellent condition, runs great
13	13	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	Sweet ride, we will have to take it
14	14	Messages	barry.rahman@icloud.com	duane.khan@icloud.com	That's an idea and can see what's
15	15	Messages	barry.rahman@icloud.com	duane.khan@icloud.com	Gotta go, off to watch the nephew
16	16	Messages	duane.khan@icloud.com	barry.rahman@icloud.com	Later
17	17	Messages	duane.khan@icloud.com	nada.shadiyah.haddad@icloud.com	Hey, Nada.
18	18	Messages	duane.khan@icloud.com	nada.shadiyah.haddad@icloud.com	Nada
19	19	Messages	duane.khan@icloud.com	nada.shadiyah.haddad@icloud.com	Testing
20	20	Messages	kyle.rockiv@icloud.com	duane.khan@icloud.com	Hey, what's up?
21	21	Messages	duane.khan@icloud.com	kyle.rockiv@icloud.com	Wazuup Kyle?
22	22	Messages	duane.khan@icloud.com	kyle.rockiv@icloud.com	Have you heard from Nada. She is
23	23	Messages	kyle.rockiv@icloud.com	duane.khan@icloud.com	She is having issues with her lapt
24	24	Messages	duane.khan@icloud.com	kyle.rockiv@icloud.com	Ok
25	25	Messages	duane.khan@icloud.com	kyle.rockiv@icloud.com	Here is the start of my script.
26	26	Messages	kyle.rockiv@icloud.com	duane.khan@icloud.com	OK, I will take a look at it tonight

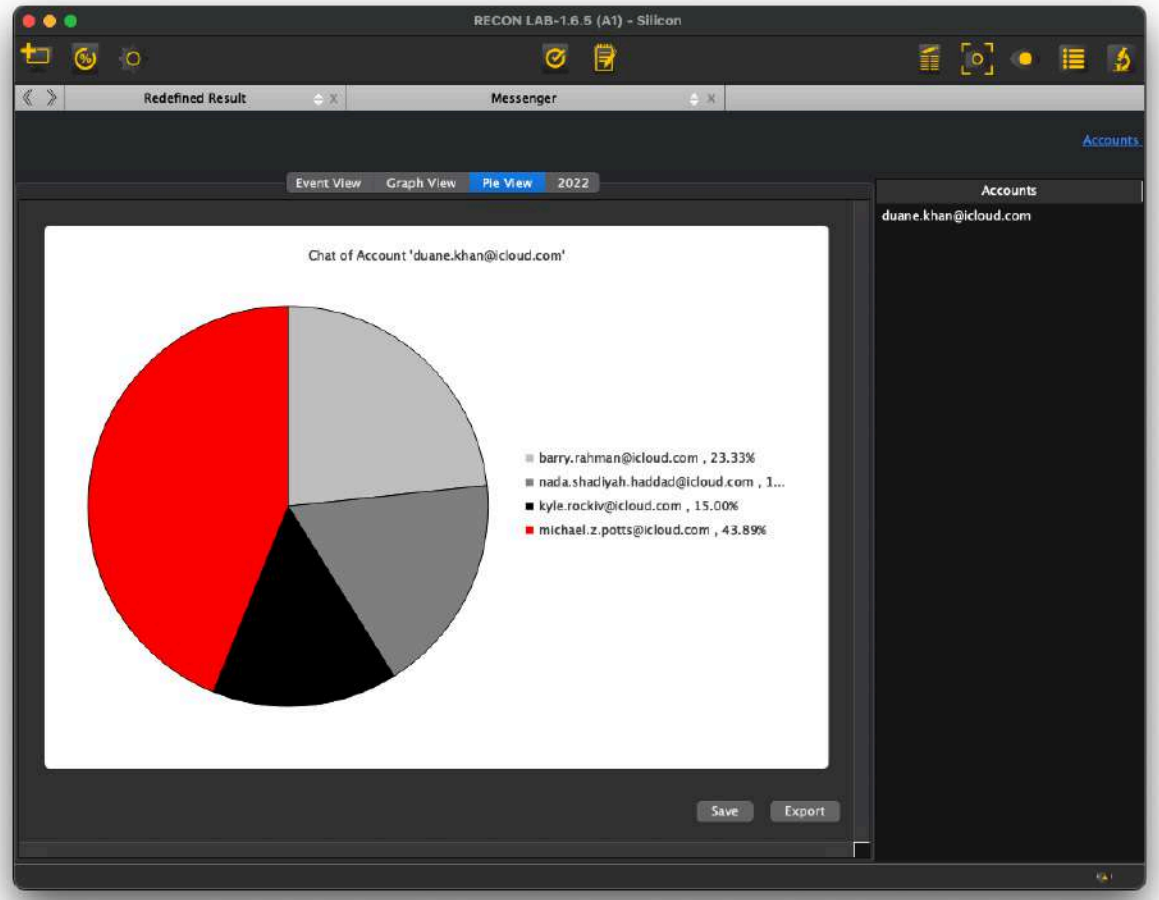
The Event View tab provides a table view of all the data. The results can be filtered using the Search box.



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

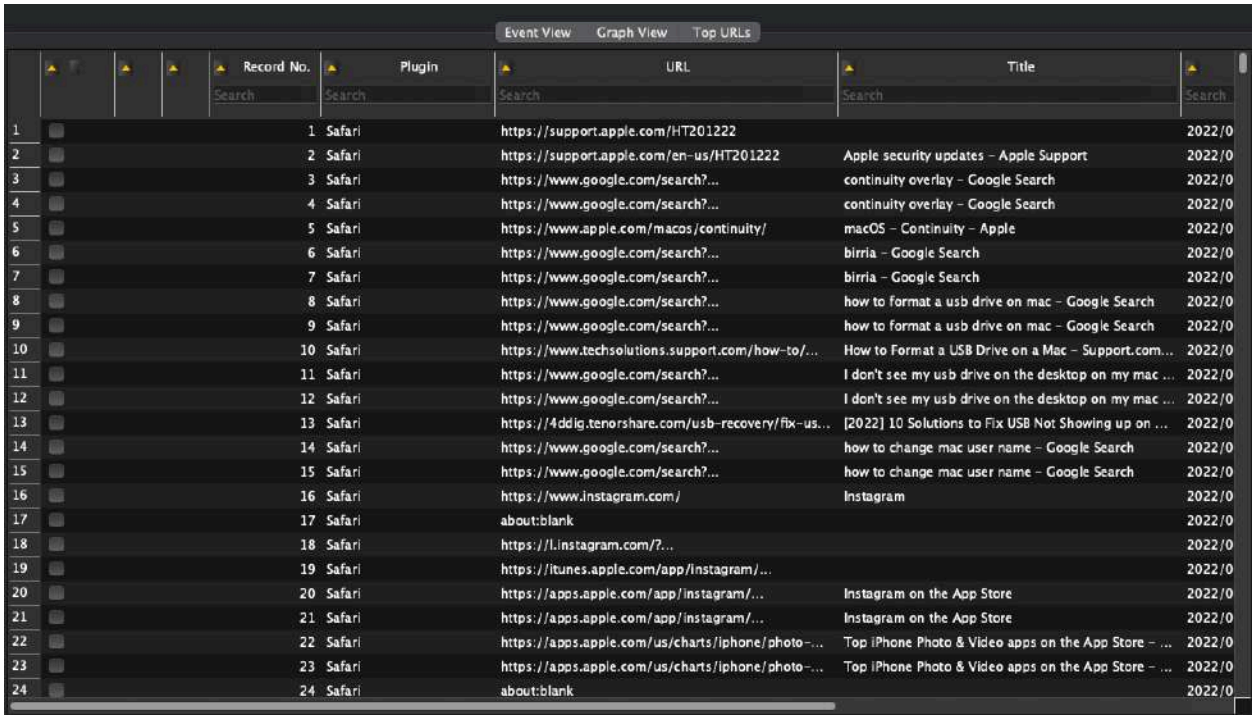


The Graph View provides a visual view of the messaging data in a timeline.



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

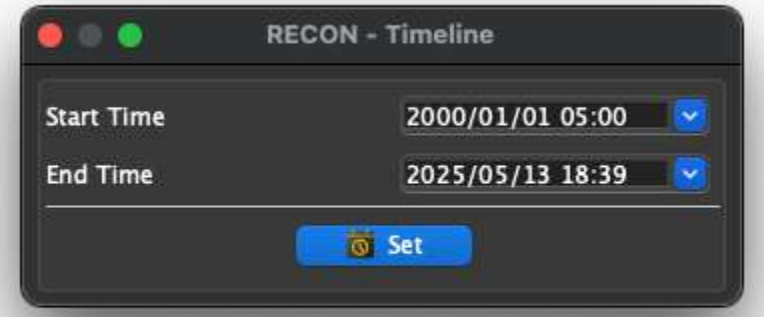
26.3 Collated Web History



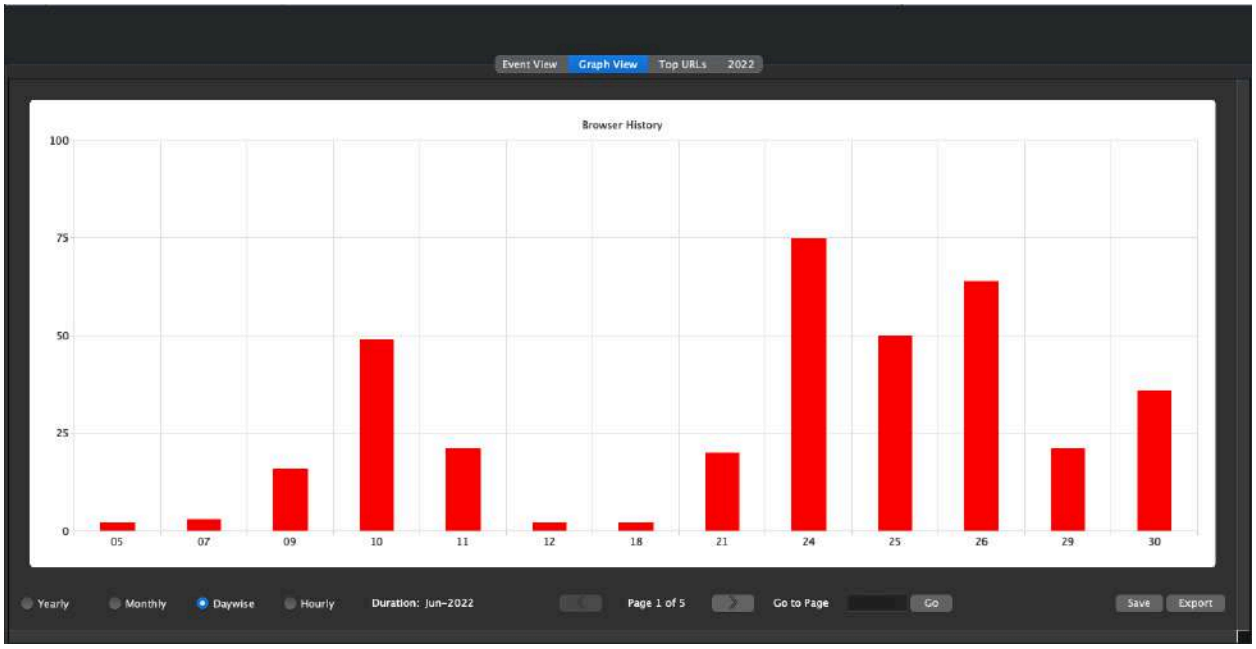
	Record No.	Plugin	URL	Title	
	Search	Search	Search	Search	Search
1	1	Safari	https://support.apple.com/HT201222		2022/0
2	2	Safari	https://support.apple.com/en-us/HT201222	Apple security updates – Apple Support	2022/0
3	3	Safari	https://www.google.com/search?...	continuity overlay – Google Search	2022/0
4	4	Safari	https://www.google.com/search?...	continuity overlay – Google Search	2022/0
5	5	Safari	https://www.apple.com/macos/continuity/	macOS – Continuity – Apple	2022/0
6	6	Safari	https://www.google.com/search?...	birria – Google Search	2022/0
7	7	Safari	https://www.google.com/search?...	birria – Google Search	2022/0
8	8	Safari	https://www.google.com/search?...	how to format a usb drive on mac – Google Search	2022/0
9	9	Safari	https://www.google.com/search?...	how to format a usb drive on mac – Google Search	2022/0
10	10	Safari	https://www.techsolutions.support.com/how-to/...	How to Format a USB Drive on a Mac – Support.com...	2022/0
11	11	Safari	https://www.google.com/search?...	I don't see my usb drive on the desktop on my mac ...	2022/0
12	12	Safari	https://www.google.com/search?...	I don't see my usb drive on the desktop on my mac ...	2022/0
13	13	Safari	https://4ddig.tenorshare.com/usb-recovery/fix-us...	[2022] 10 Solutions to Fix USB Not Showing up on ...	2022/0
14	14	Safari	https://www.google.com/search?...	how to change mac user name – Google Search	2022/0
15	15	Safari	https://www.google.com/search?...	how to change mac user name – Google Search	2022/0
16	16	Safari	https://www.instagram.com/	Instagram	2022/0
17	17	Safari	about:blank		2022/0
18	18	Safari	https://l.instagram.com/?...		2022/0
19	19	Safari	https://itunes.apple.com/app/instagram/...		2022/0
20	20	Safari	https://apps.apple.com/app/instagram/...	Instagram on the App Store	2022/0
21	21	Safari	https://apps.apple.com/app/instagram/...	Instagram on the App Store	2022/0
22	22	Safari	https://apps.apple.com/us/charts/iphone/photo-...	Top iPhone Photo & Video apps on the App Store – ...	2022/0
23	23	Safari	https://apps.apple.com/us/charts/iphone/photo-...	Top iPhone Photo & Video apps on the App Store – ...	2022/0
24	24	Safari	about:blank		2022/0

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

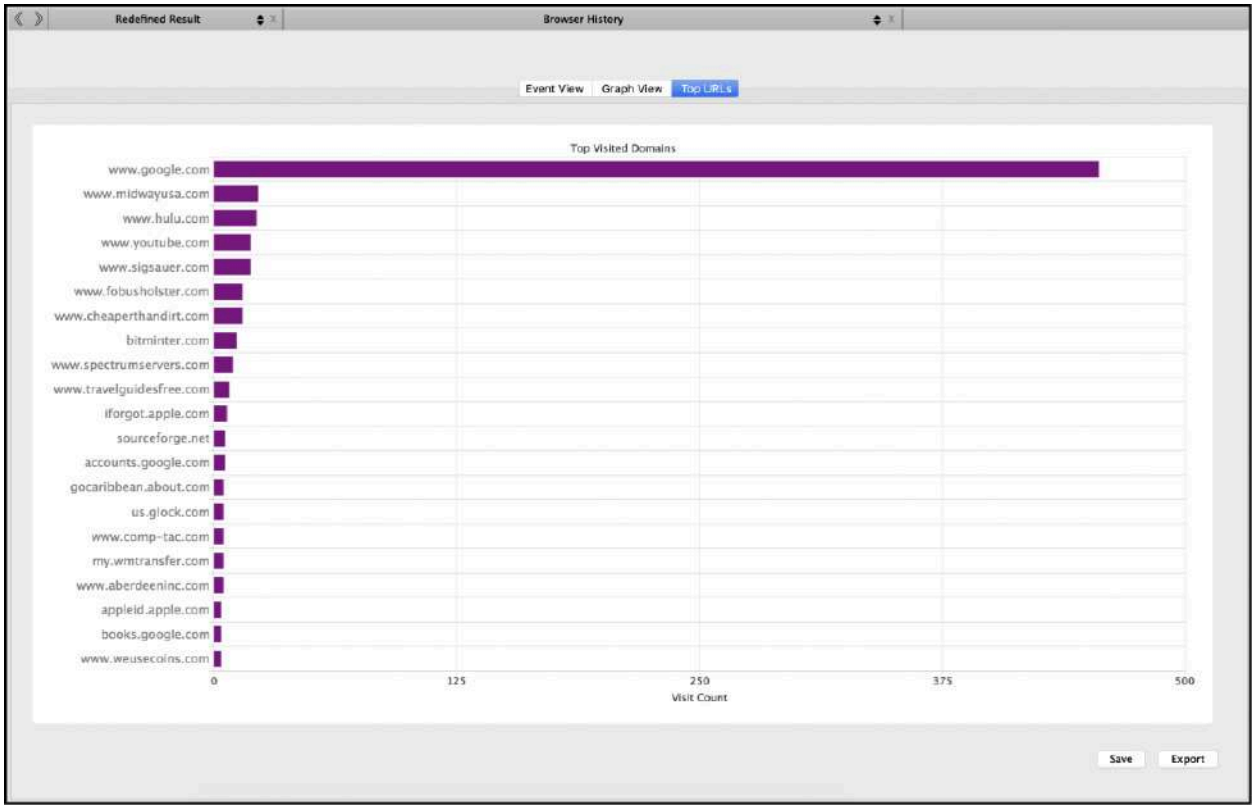
The Event View tab provides a table view of all the data. The results can be filtered using the Search box.



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



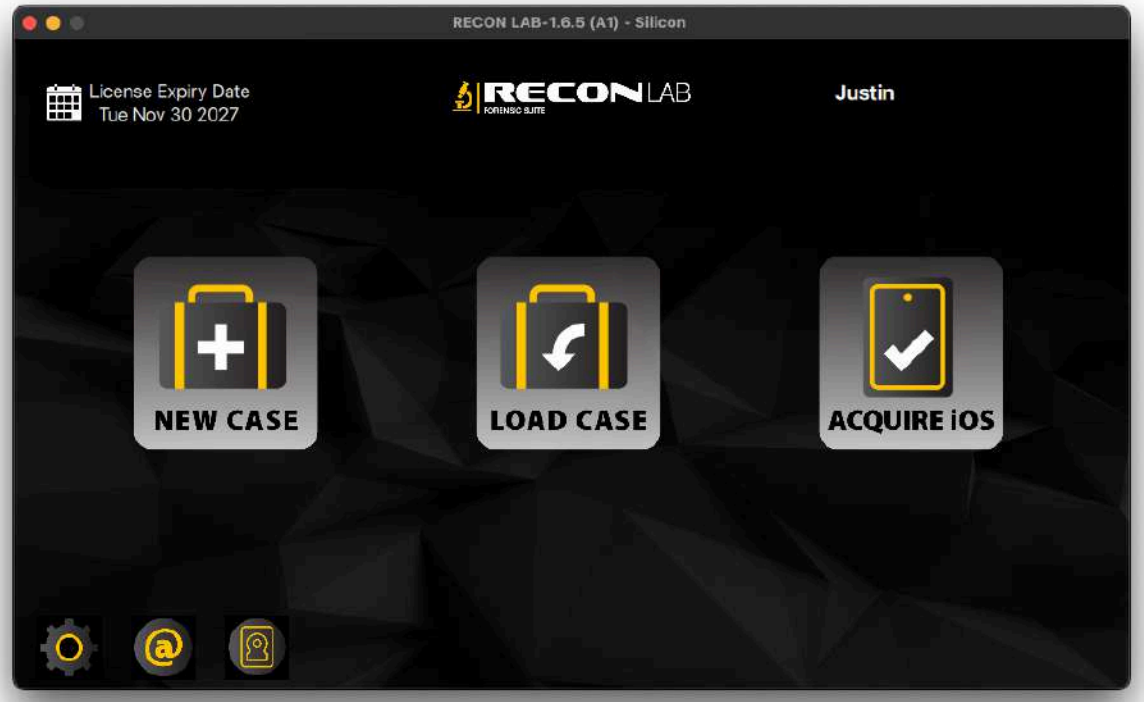
The Graph View provides a visual view of web browser data in a timeline.



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

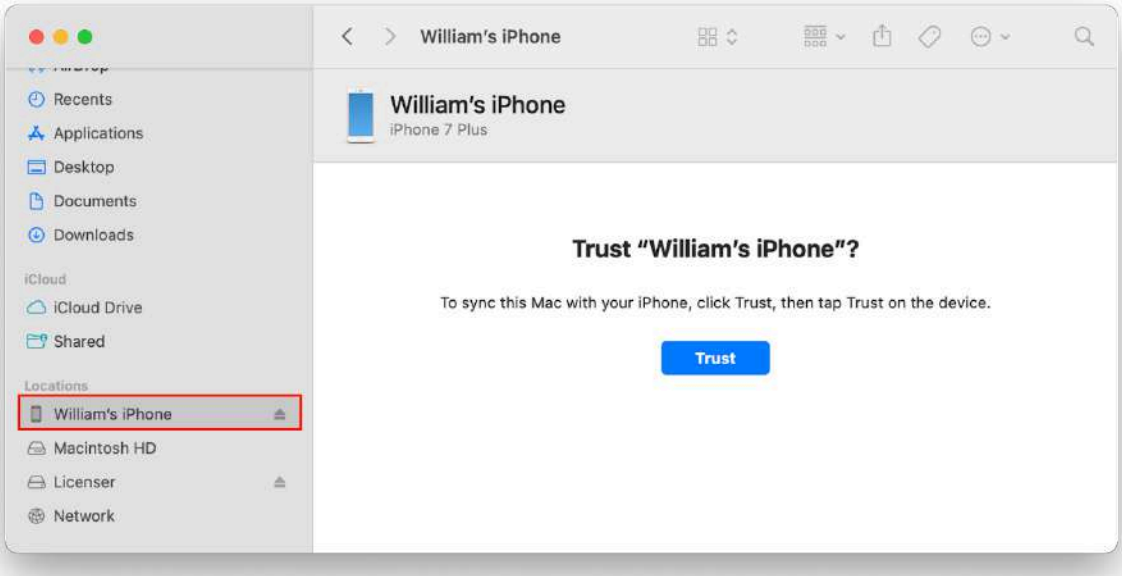
27 Acquiring and Processing iOS Devices

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).

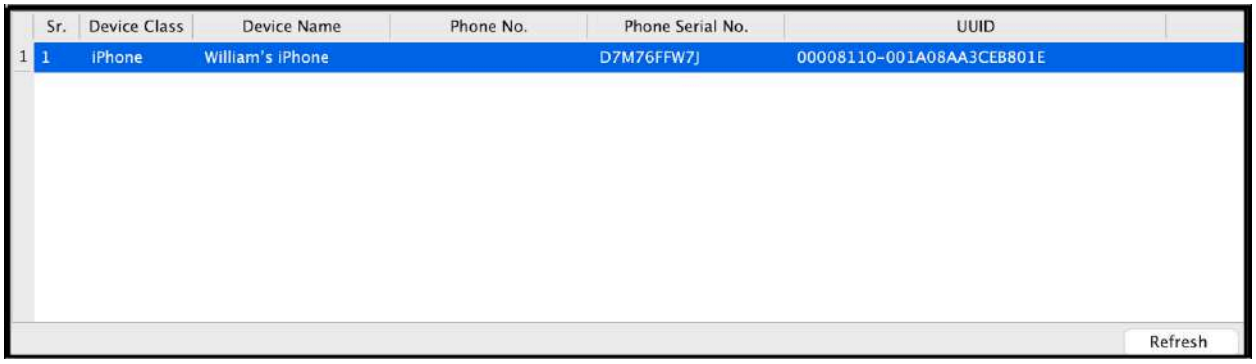


27.1 Acquiring an iOS Device

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. This iOS Backup may be analyzed as a source when you generate a new RECON LAB case.

---

28 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.

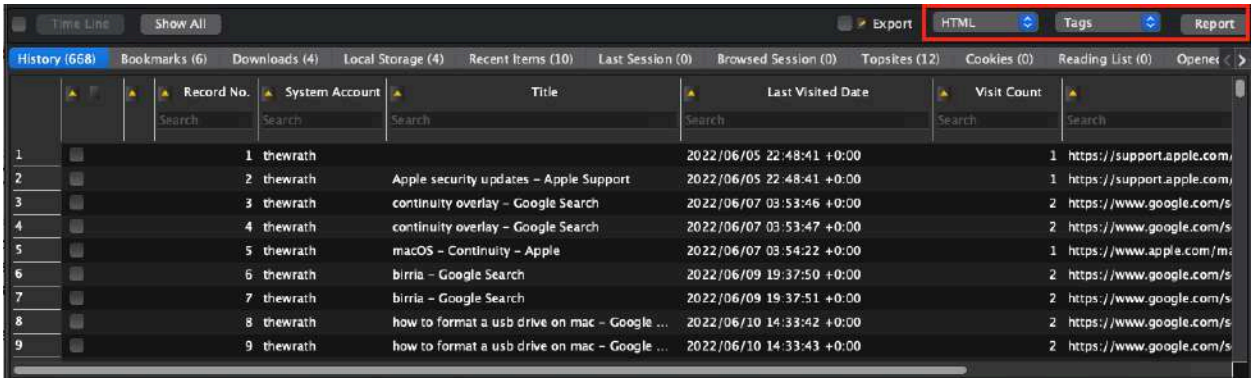
Additionally, RECON LAB includes the first of its kind WYSIWYG (What You See Is What You Get) reporting mode called StoryBoard. Story Board allows the examiner to have full control over the reporting process and is as easy to use as a word processor. The examiner has the ability to add, remove or annotate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

28.1 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.

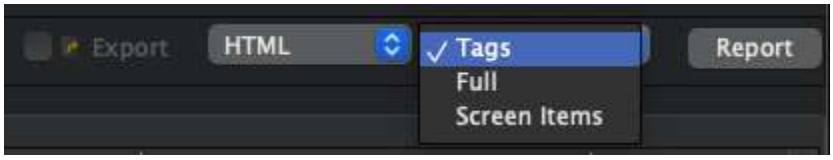
Selecting any Plugin category will open a results window. Every Plugin has the ability to create a variety of reports depending on the type of artifacts recovered.



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

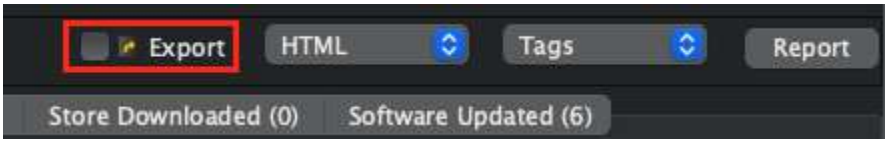
The type of report can be selected from the first dropdown list. The options are the following:

- 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

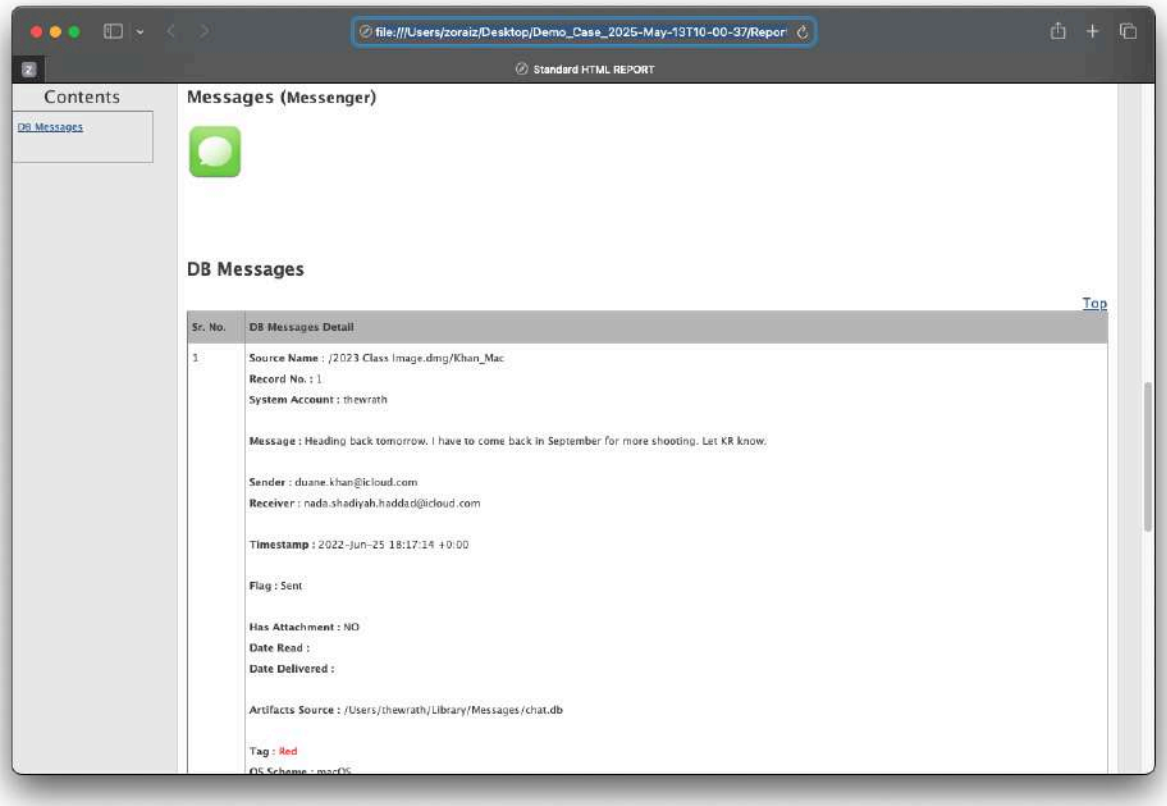


The second dropdown list allows the examiner to select what will be included in the report. The options are the following:

- 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.



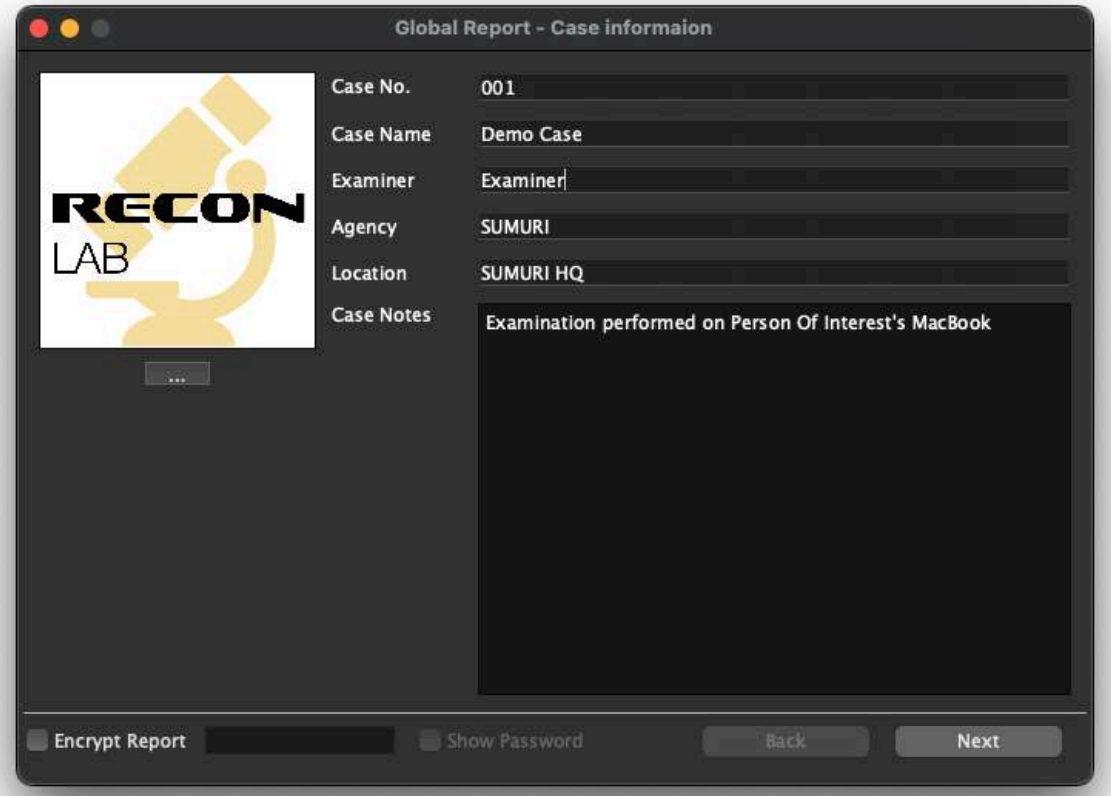
Once all the settings have been selected the report can be generated by clicking the Report button.

28.2 Global 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.

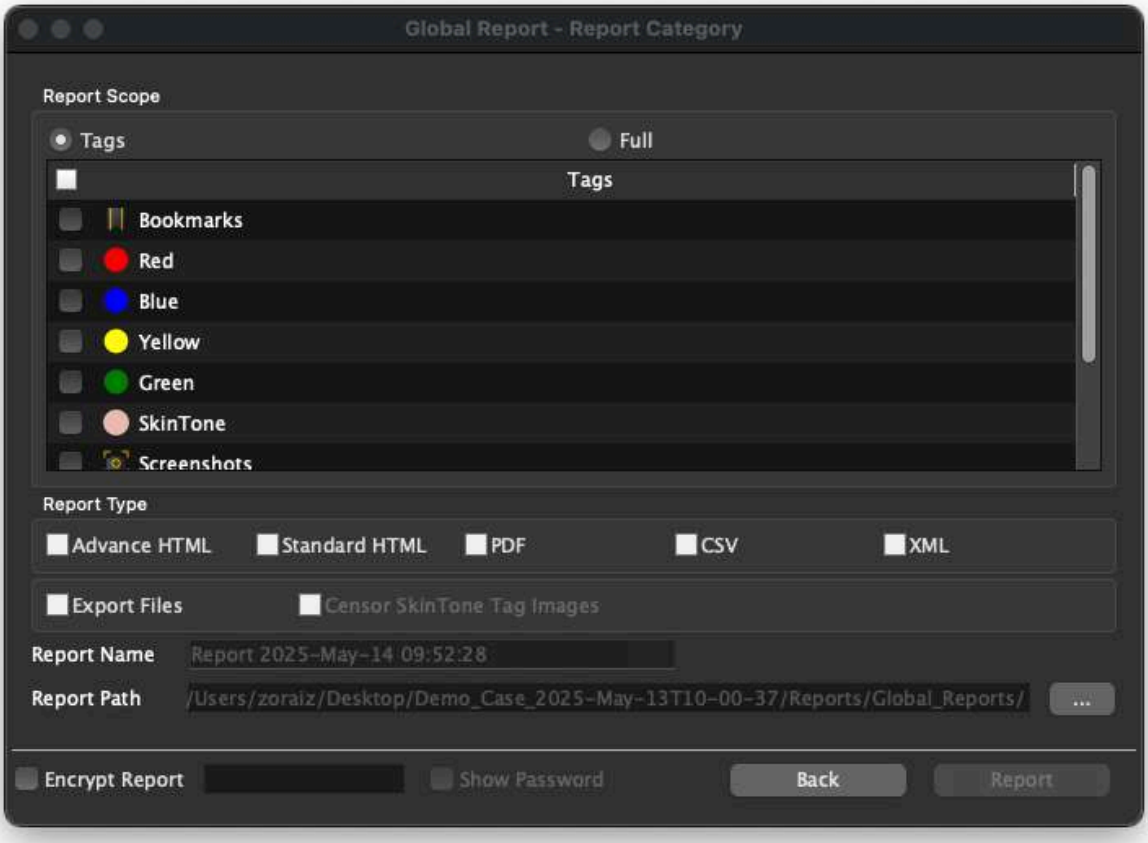
28.2.1 Case Information Window



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.

28.2.2 Customizing Global Reports

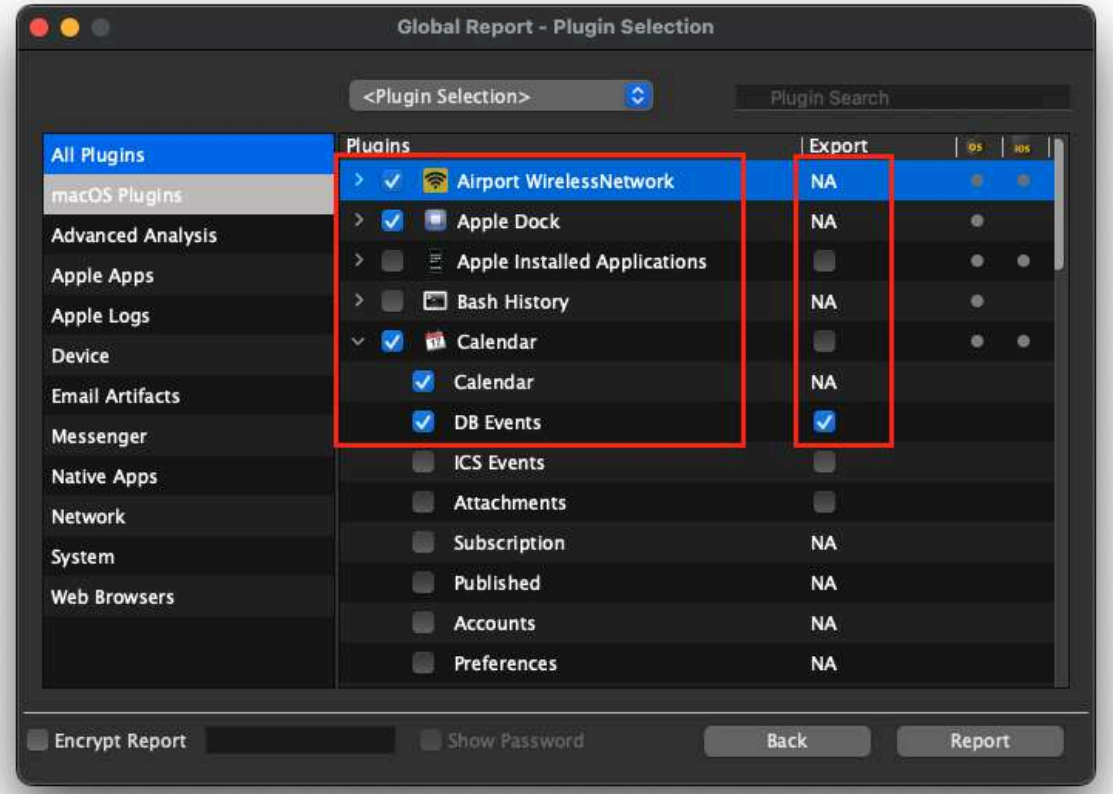
The Global Report can be customized using the Report Scope and Report Type options in the Global Report - Report Category window.



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.

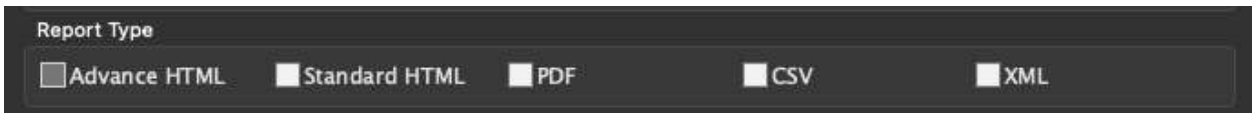


From the Global Report - Plugin Selection window individual plugins and their artifacts can be selected for inclusion in the report by checking the boxes.

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

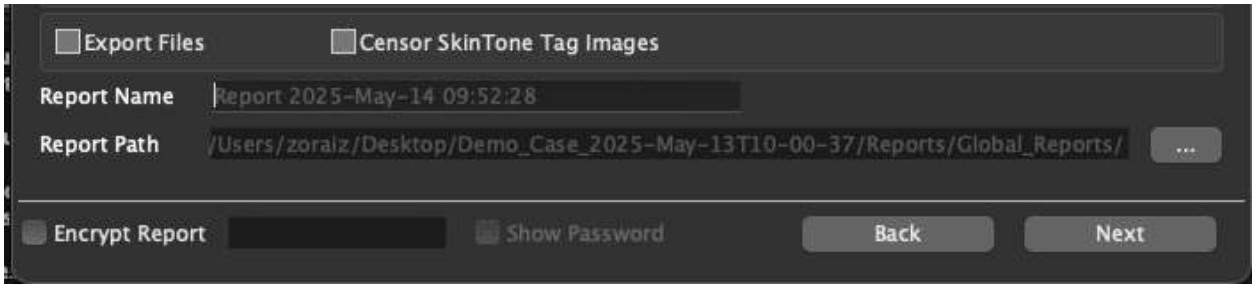
To create a Global Report from the Plugin Selection window just click Report.

28.2.3 Global Report Type



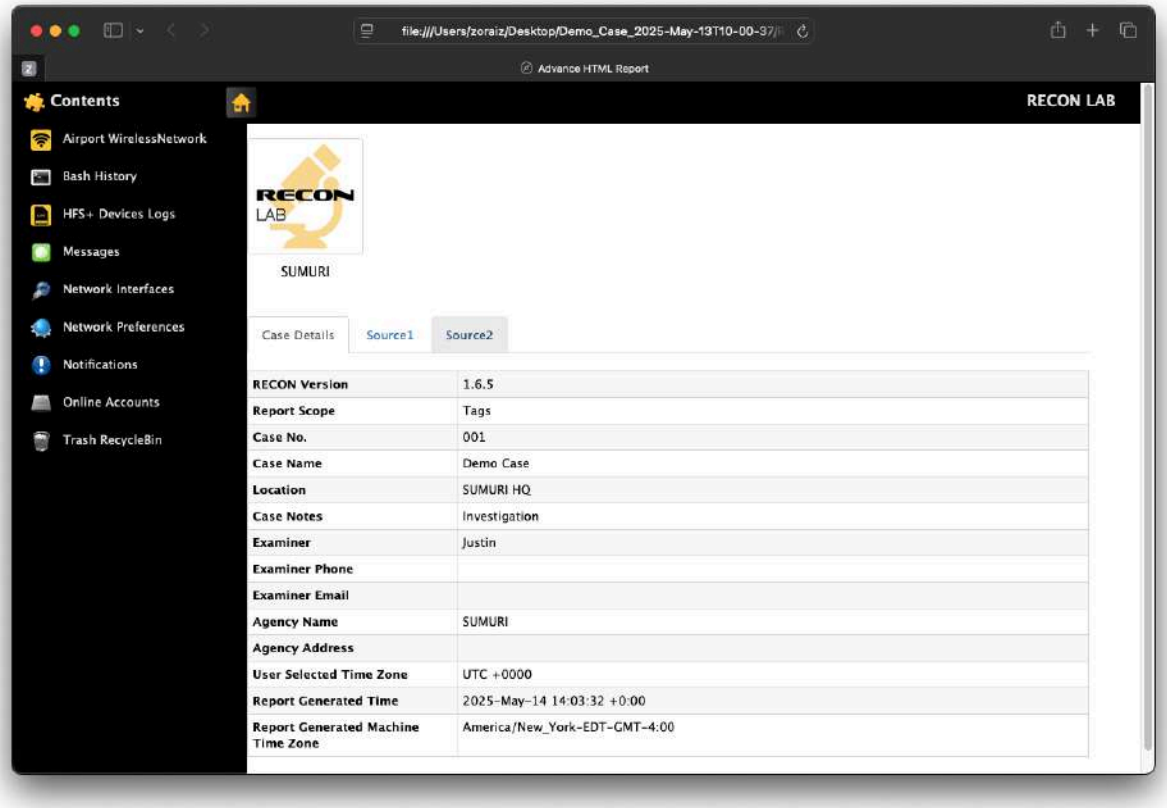
The Report Type can be selected in the Global Report - Report Category window. The following report types are available:

- 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.

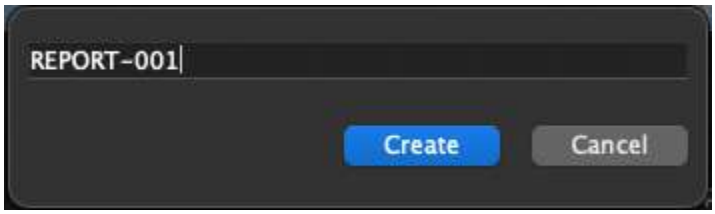


Once all options have been selected click Report to generate the report.

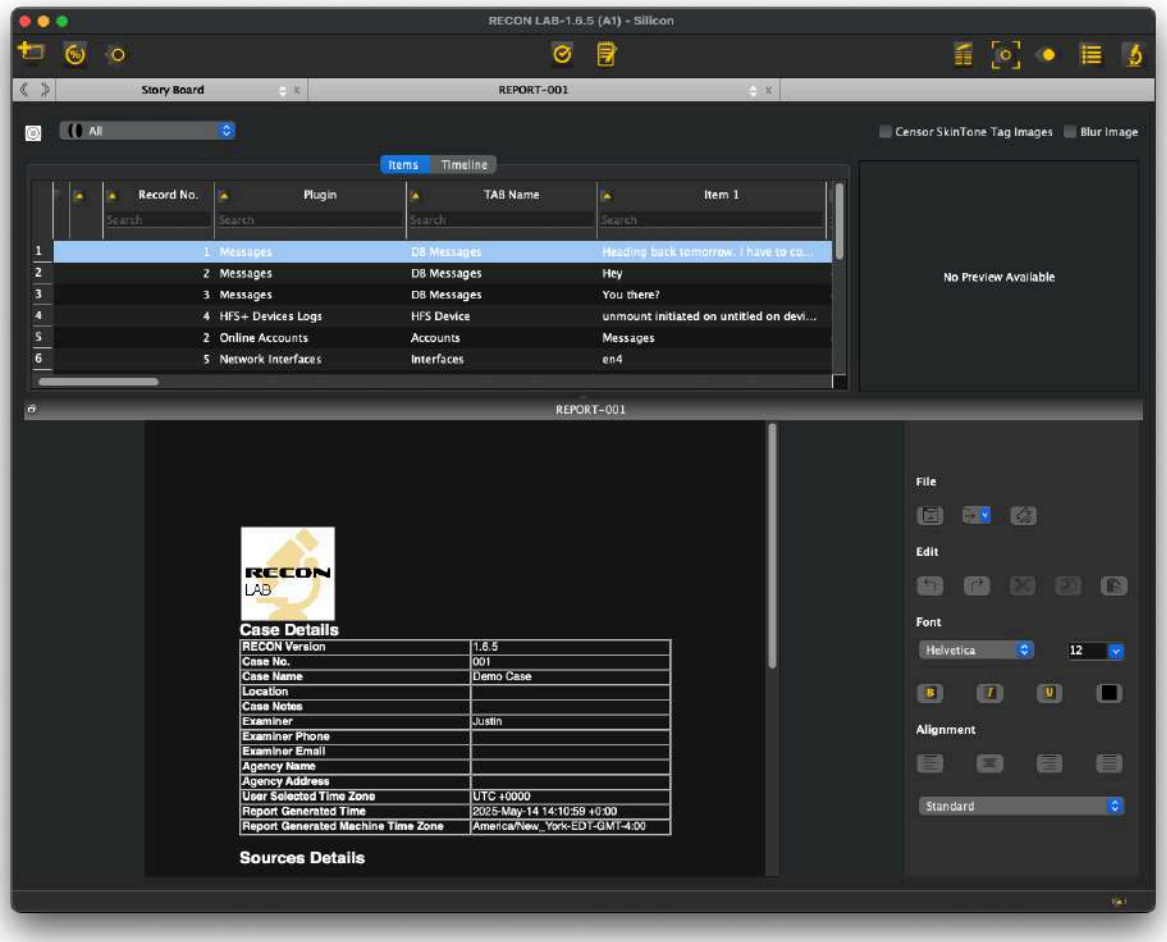
28.3 Story Board - WYSIWYG Reports

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 understanding 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.



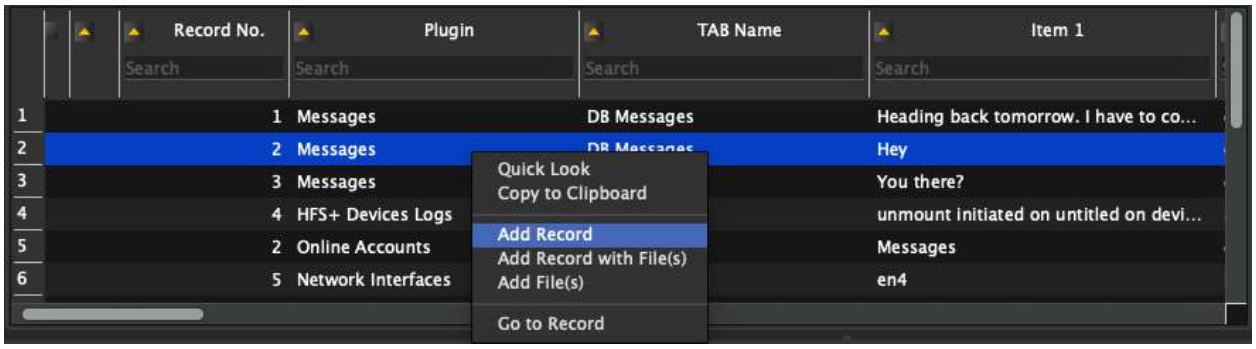
The Story Board interface is divided into two sections. All tags and bookmarks from the case are accessible and found at the top. The report is found in the bottom section.

28.3.1 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

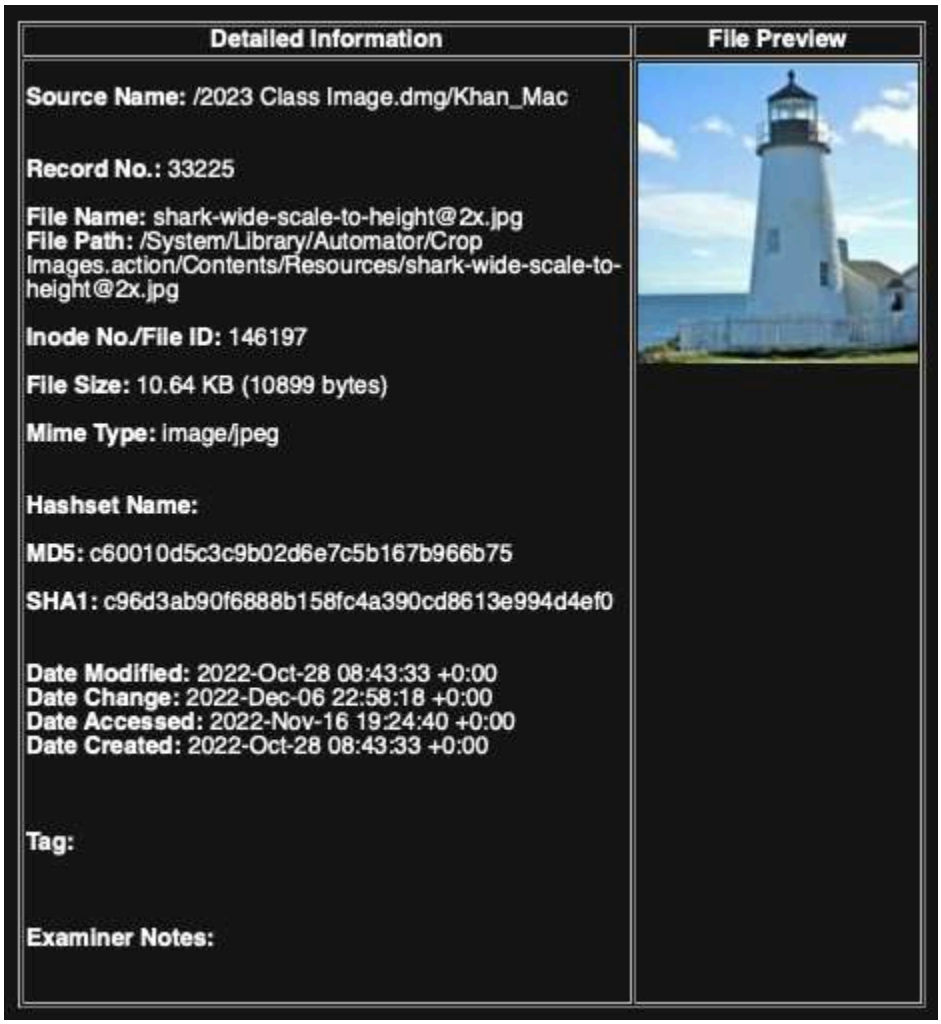
28.3.2 Adding Tags and Bookmarks to a Report



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)



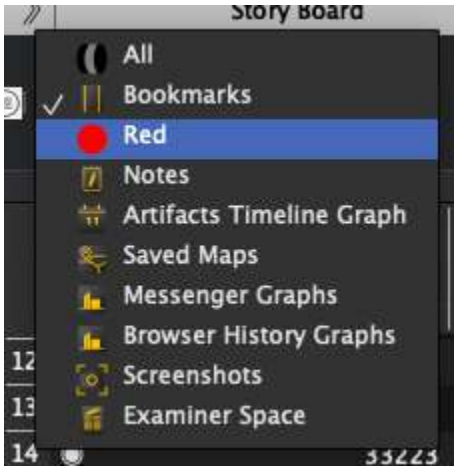
Detailed Information	File Preview
Source Name: /2023 Class Image.dmg/Khan_Mac **Record No.:** 33225 **File Name:** shark-wide-scale-to-height@2x.jpg **File Path:** /System/Library/Automator/Crop Images.action/Contents/Resources/shark-wide-scale-to-height@2x.jpg **Inode No./File ID:** 146197 **File Size:** 10.64 KB (10899 bytes) **Mime Type:** image/jpeg **Hashset Name:** **MD5:** c60010d5c3c9b02d6e7c5b167b966b75 **SHA1:** c96d3ab90f6888b158fc4a390cd8613e994d4ef0 **Date Modified:** 2022-Oct-28 08:43:33 +0:00 **Date Change:** 2022-Dec-06 22:58:18 +0:00 **Date Accessed:** 2022-Nov-16 19:24:40 +0:00 **Date Created:** 2022-Oct-28 08:43:33 +0:00 **Tag:** **Examiner Notes:**	

The above is an example of a record added to the report with the file.

28.3.3 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.

28.3.4 Filtering Records In Story Board

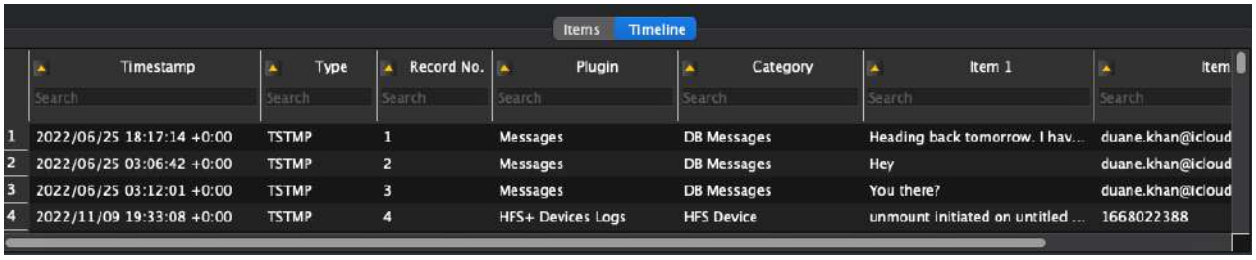


Categories of records can be selected and filtered by using the dropdown list.

		Record No.	Plugin	TAB Name	Item 1	Item 2
		Search	trash	Search	Search	Search
11		4	Trash RecycleBin	Items	Swindlers of Darkness.pdf	YES
12		3	Trash RecycleBin	Items	Systems	YES

Additionally, records can be filtered by entering a keyword in the Search box.

28.3.5 Adding Records in Chronological Order

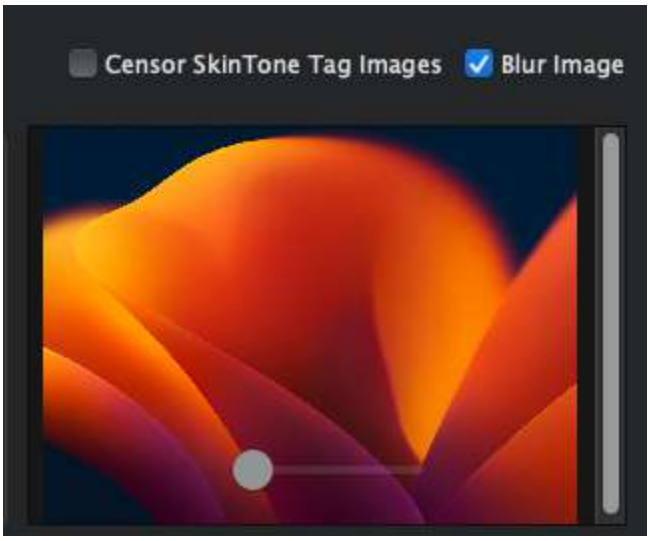


Items | Timeline

	Timestamp	Type	Record No.	Plugin	Category	Item 1	Item
	Search	Search	Search	Search	Search	Search	Search
1	2022/06/25 18:17:14 +0:00	TSTMP	1	Messages	DB Messages	Heading back tomorrow. I hav...	duane.khan@icloud
2	2022/06/25 03:06:42 +0:00	TSTMP	2	Messages	DB Messages	Hey	duane.khan@icloud
3	2022/06/25 03:12:01 +0:00	TSTMP	3	Messages	DB Messages	You there?	duane.khan@icloud
4	2022/11/09 19:33:08 +0:00	TSTMP	4	HFS+ Devices Logs	HFS Device	unmount initiated on untitled ...	1668022388

Selecting the Timeline tab allows records to be sorted chronologically. Records can then be added to the report in sequence of occurrence.

28.3.6 Blur / Censor Image in Report

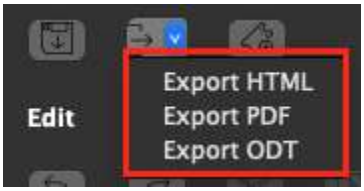


To blur and image that is to be added to a Story Board report check the Blur Image button before adding an image to the report.

If the image contains skin tones that should be censored, press the “Censor Skinetone Tag Images” item. This will blur all files that had been tagged with SkinTone.

28.3.7 Saving and Exporting a Story Board Report

Use the Save button to save the current state of the Story Board report.



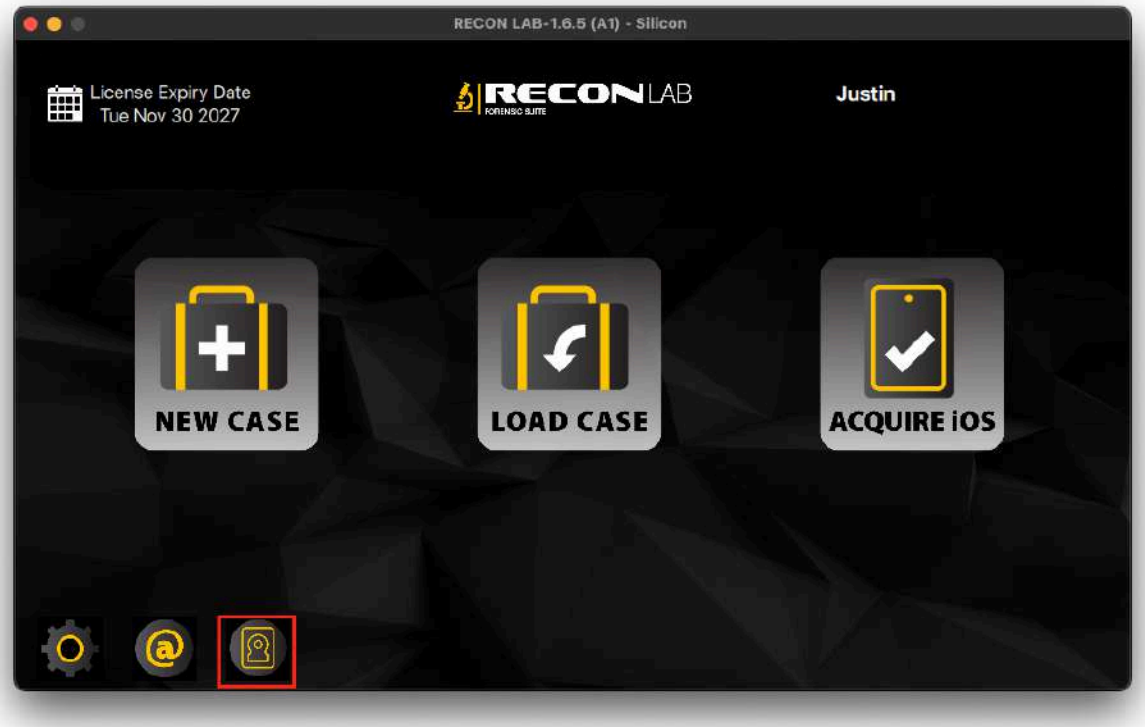
To export the report in a HTML, PDF or ODT format click the Export button and select one of the options from the dropdown list.

29 Exit RECON LAB

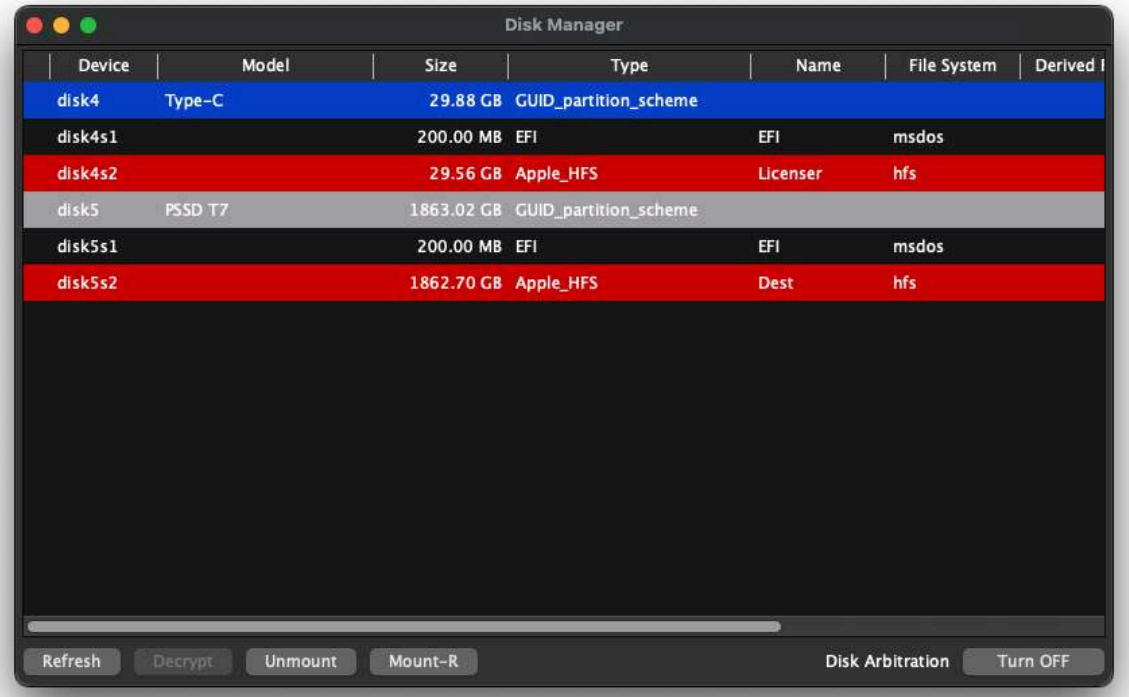
To quit RECON LAB select “Quit RECON_LAB” from the top menu

30 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.

30.1 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.

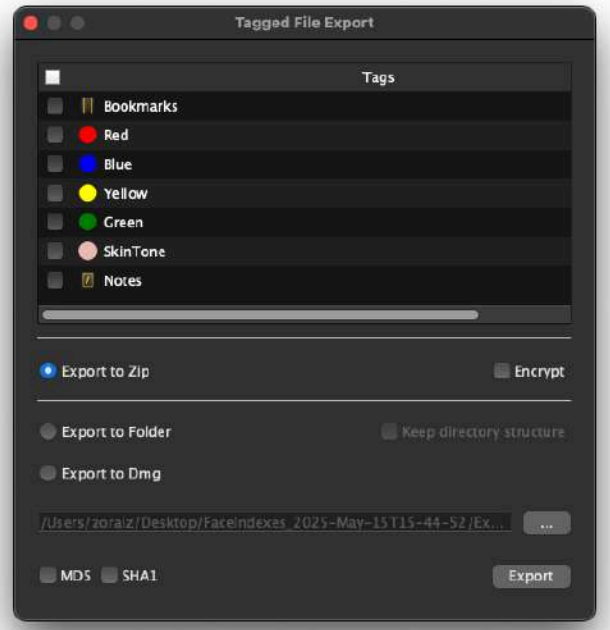
After connecting the device click the Refresh button to show the new devices. With the new devices displayed, the following options exist:

- 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

---

31 Tagged File Export

The Tagged File Export feature allows the examiner to export selected files from the source to a new location. Examiners can define export criteria and choose the desired destination file format. This feature can be accessed from the top menu via Export > Tagged File Export.



In the Tagged File Export interface, the examiner can customize what types of tagged content to export, the format to export it in, and whether to include hash values.

Types of files available for export:

- Files that have been bookmarked
- Files that have been tagged
- Files where notes have been added

Available export formats:

- Zip – Optionally encrypted with a password.
- Folder – Allows preservation of the original directory structure.
- DMG – Also supports saving the original directory structure.

Additional options:

- MD5 and SHA1 hashes can be generated for all export types. These will be included in the exported package.

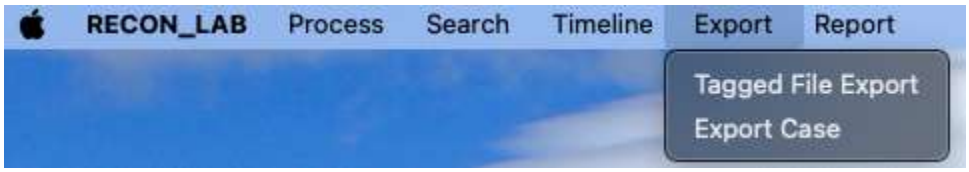
---

32 RECON LAB Case Exporter

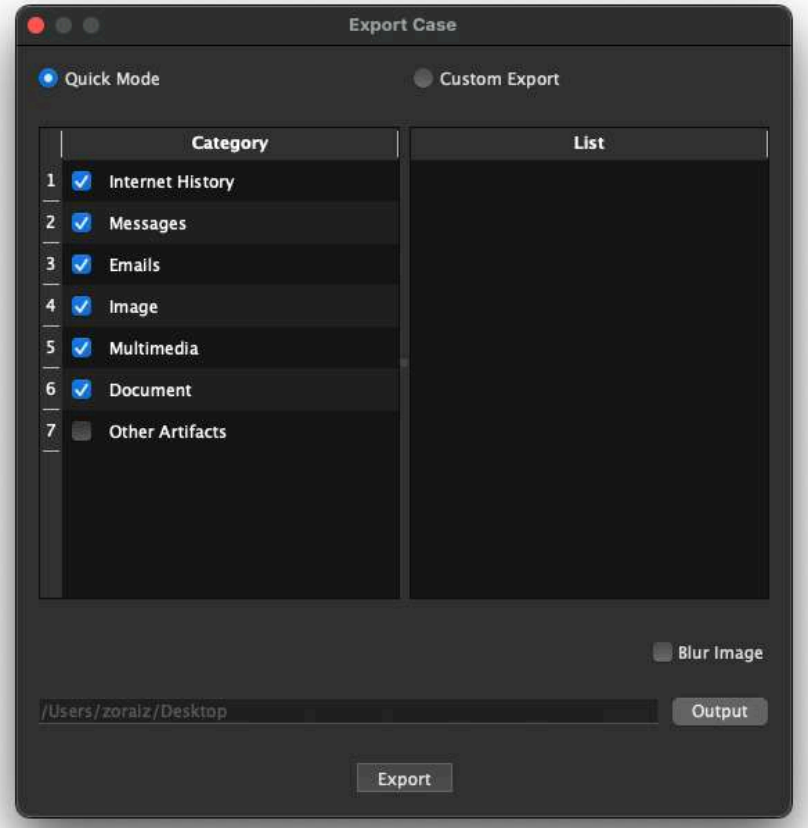
RECON LAB's Case Exporter feature allows examiners to collaborate with one another by using a portable case. This feature gives teams the ability to export all of the important information to a standalone application that can be reviewed by a Windows computer.

32.1 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.

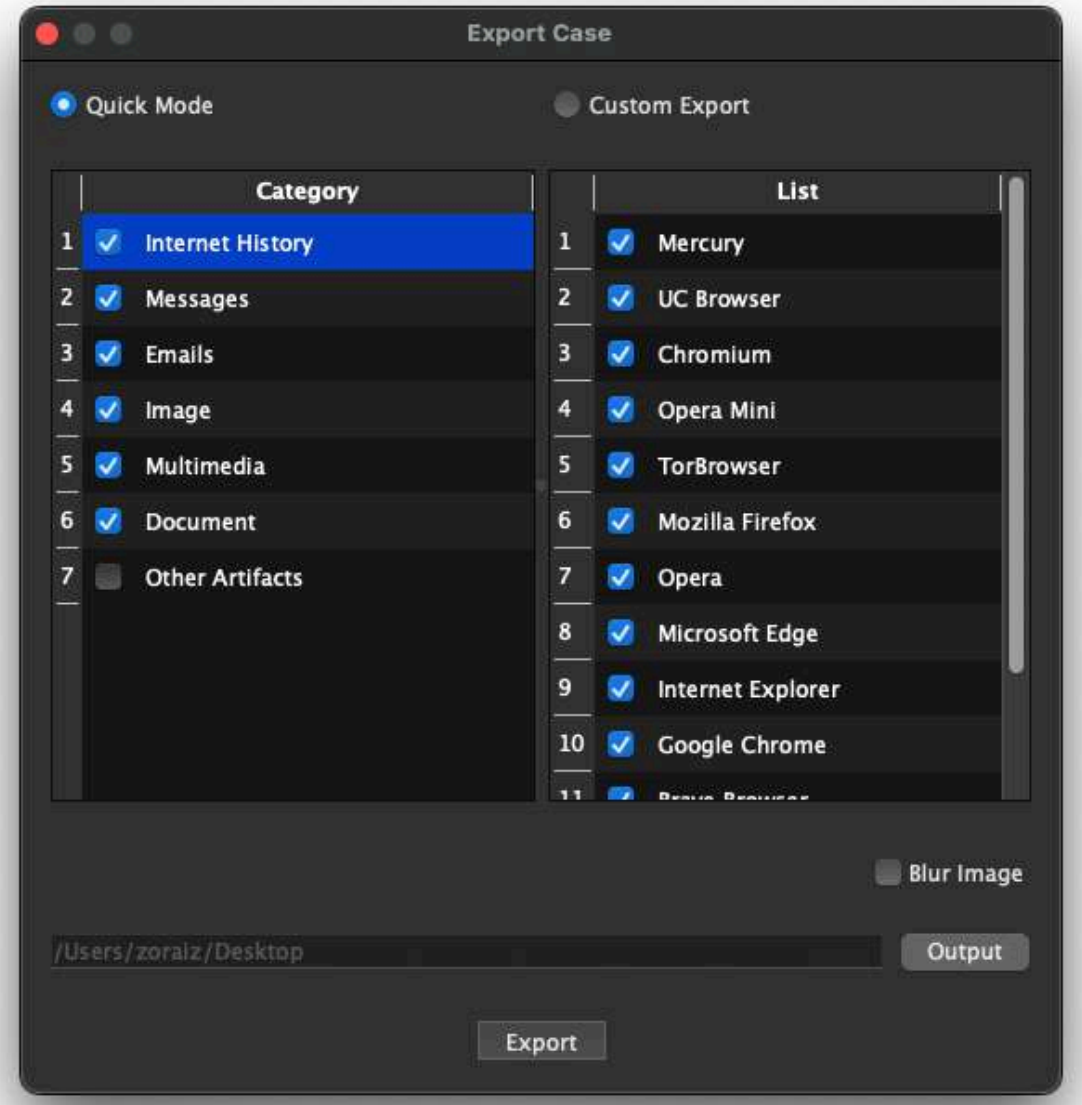


RECON LAB has two options when exporting a case:

- 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

32.1.1 Quick Mode

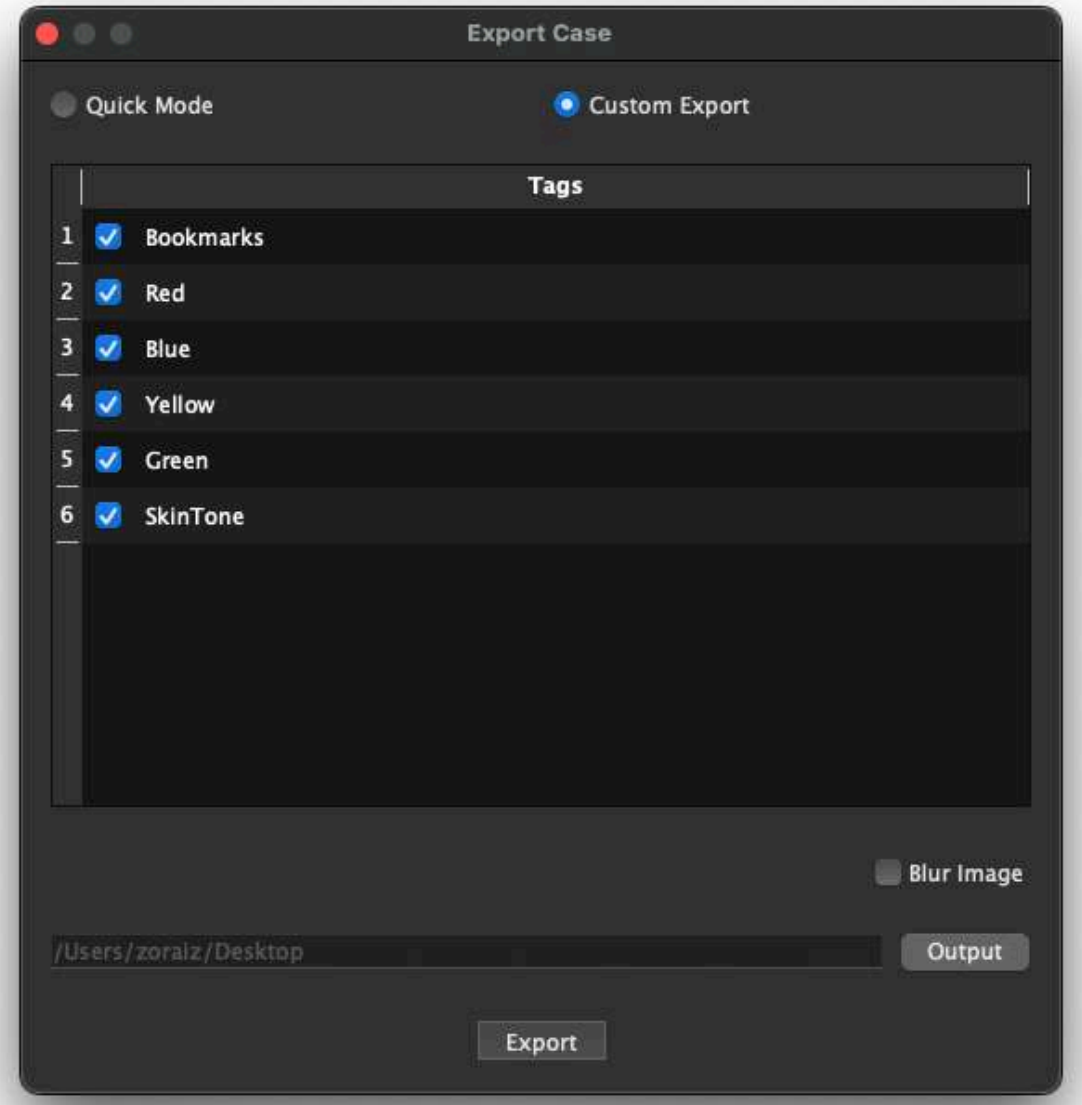
In Quick Mode, select the Category options with their corresponding automated plugins under List to export and analyze in RECON CASE READER.



Note: Automated plugins need to be processed before exporting a case in Quick Mode. For more information about RECON LAB's automated plugins, see [Artifacts]

32.1.2 Custom Mode

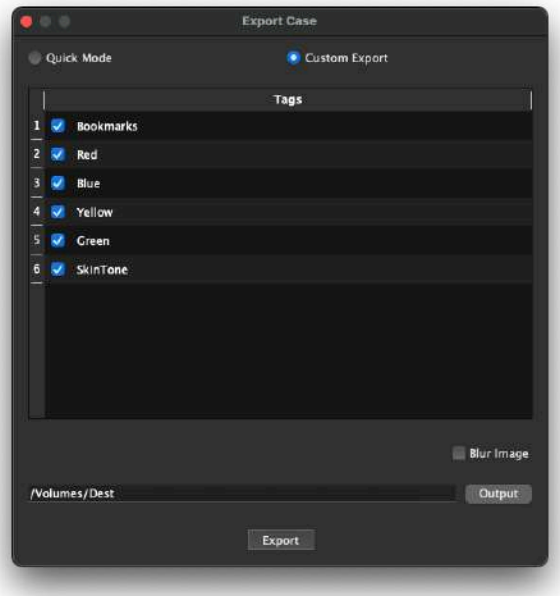
In Custom Mode, select the specific data marked by tags and bookmarks to export and analyze in RECON CASE READER.



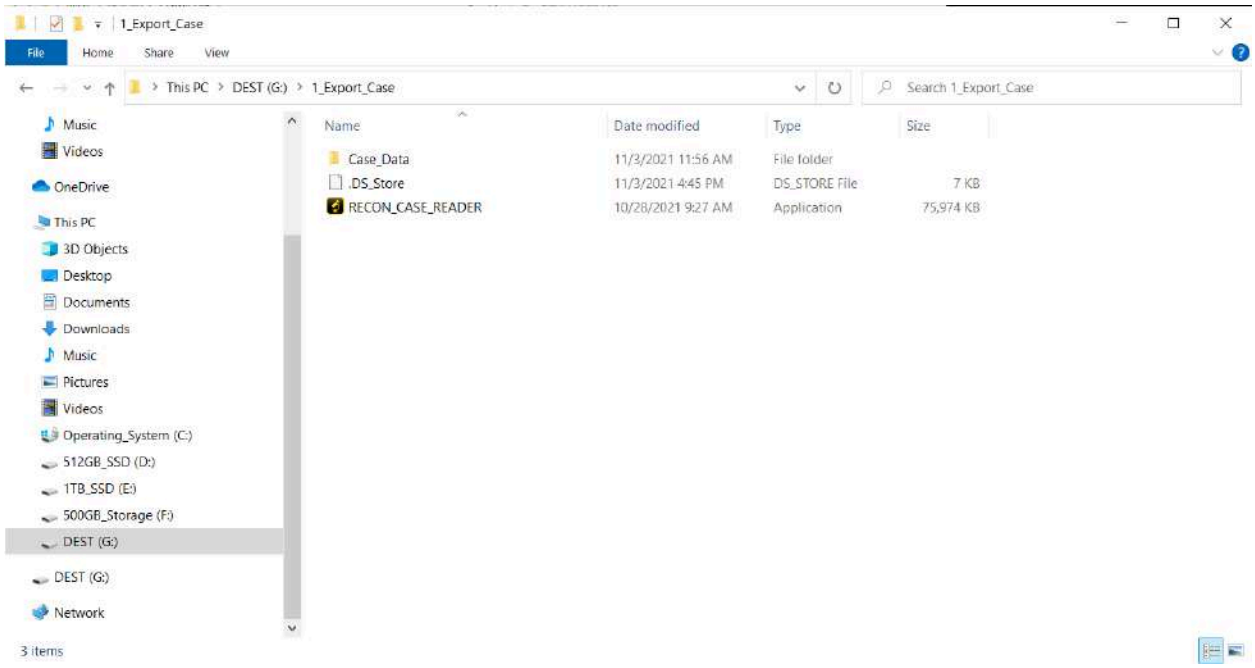
For more information on bookmarking and tagging, see Section 17

32.1.3 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.



33 CASE Reader

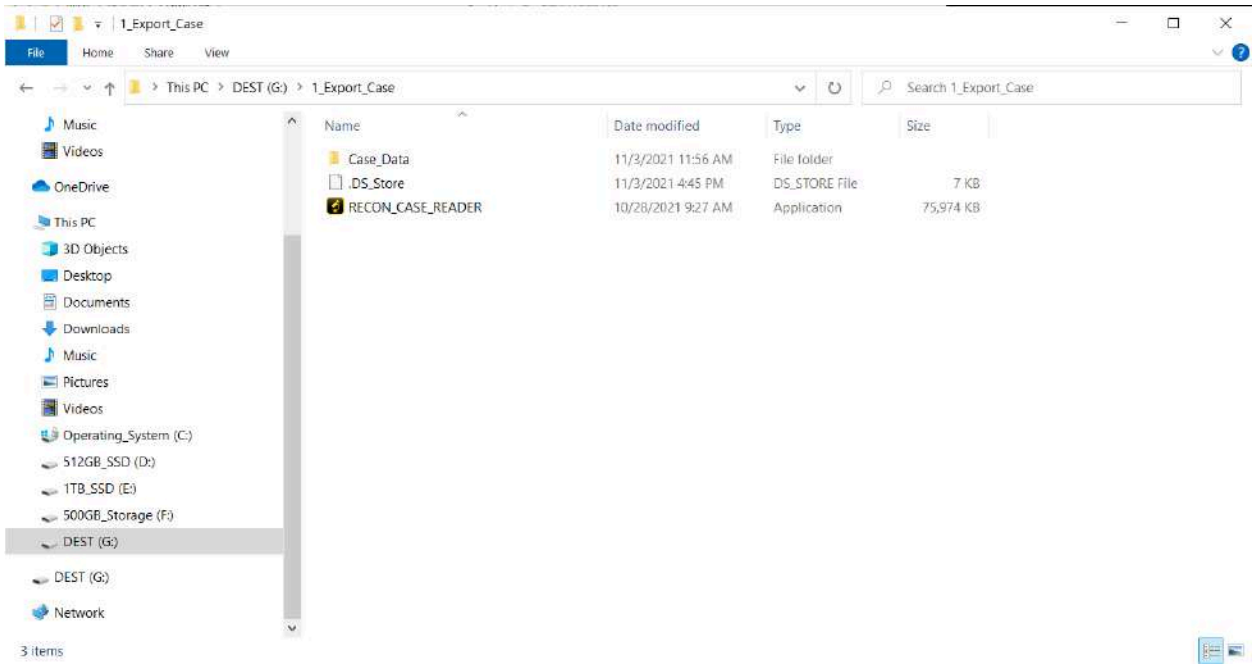
The RECON_CASE_READER.exe is included every time a case is exported. The executable is used to install the RECON LAB Case Reader application onto a Windows machine. The application only needs to be installed one time. After installation, any exported case can be loaded into the RECON LAB Case Reader.

33.1 Minimum System Requirements

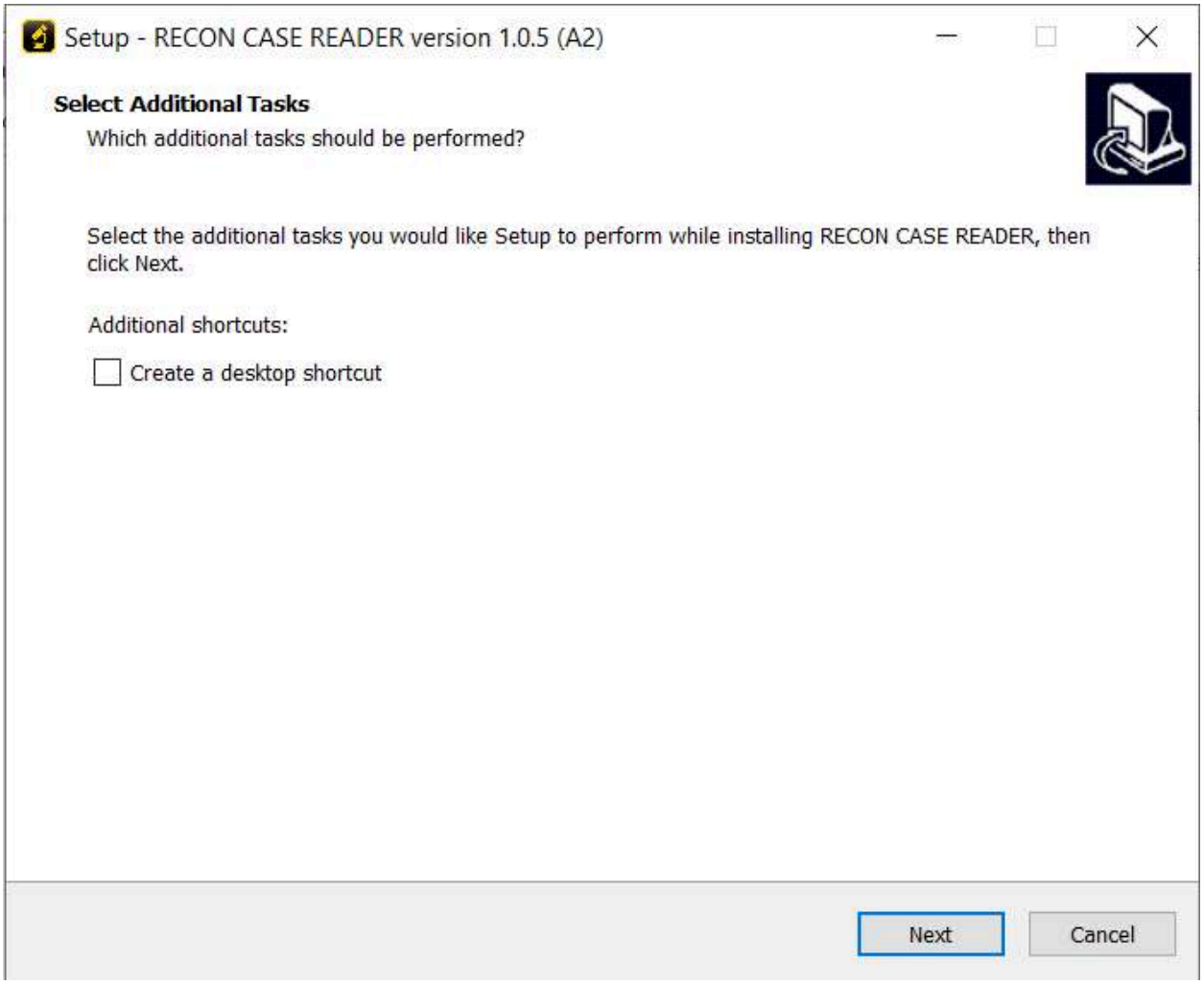
Windows 10 with Intel i5 processor with 8GB of RAM.

33.2 Installation

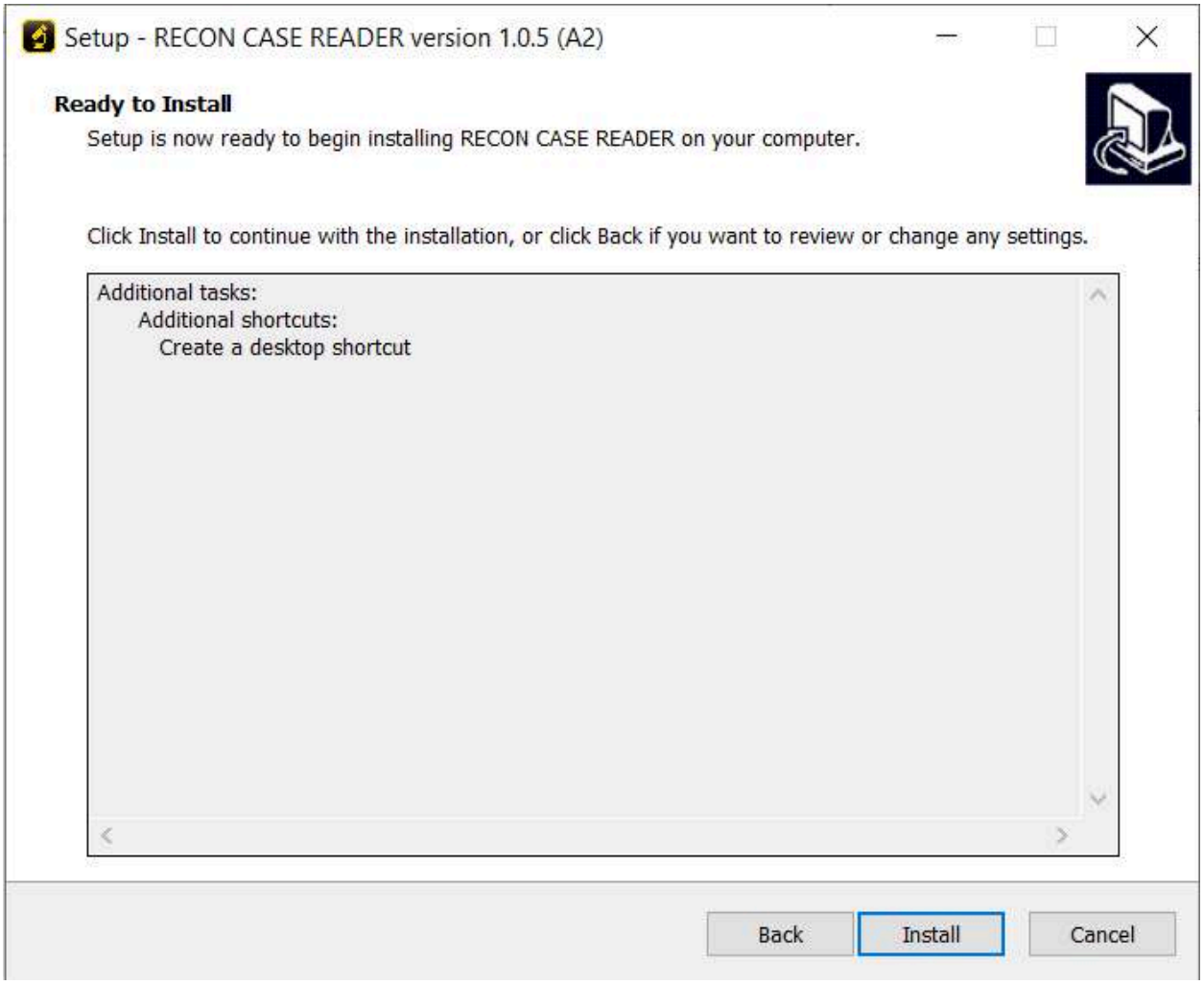
To install the RECON CASE Reader double click on the RECON_CASE_READER.exe. Windows may ask to allow the application to make changes to your device. If so, select yes.



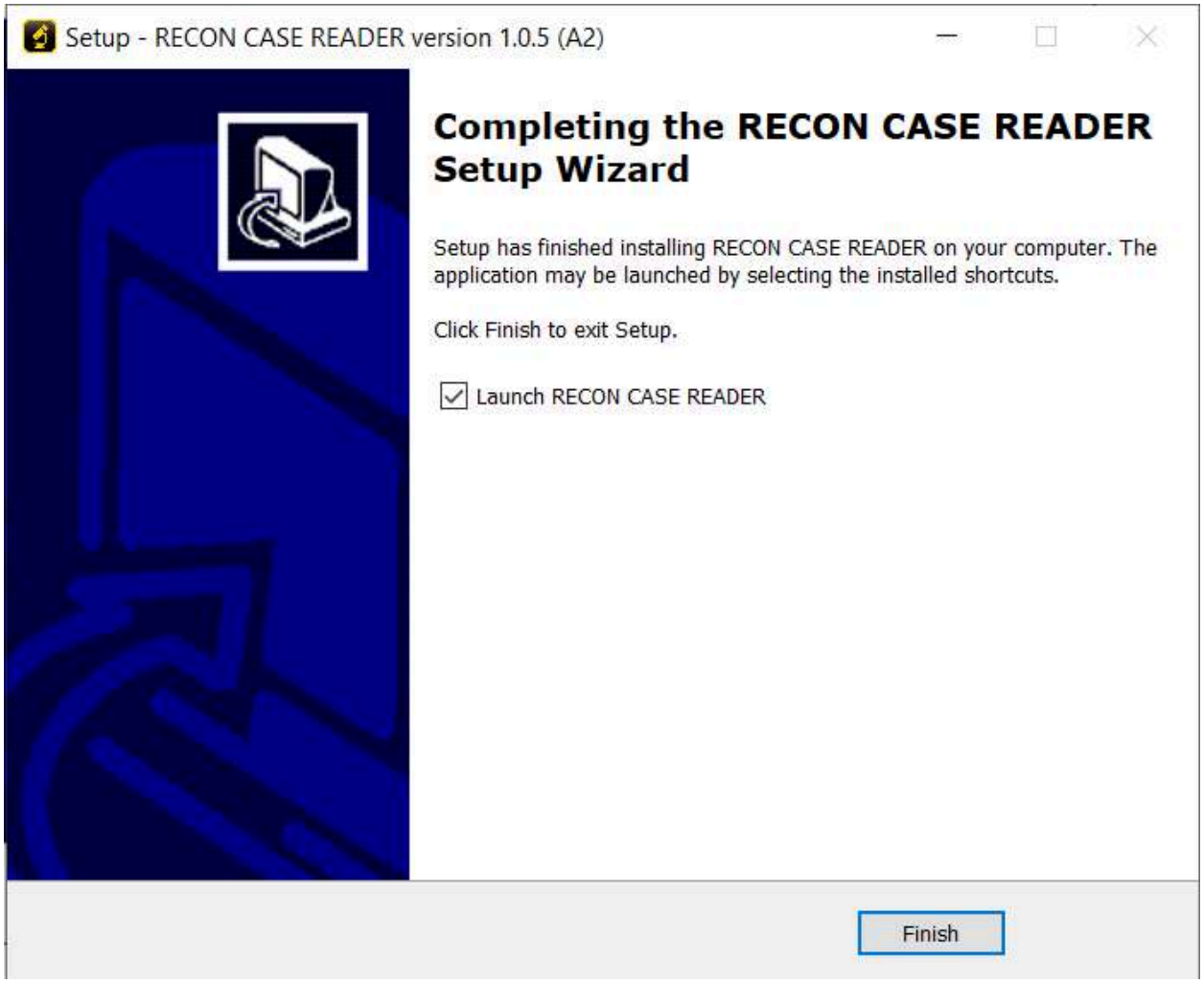
The next step in the installation will ask if the examiner wants to create an additional desktop shortcut on the user's desktop. Check the box to add a desktop shortcut or uncheck it to not add one.

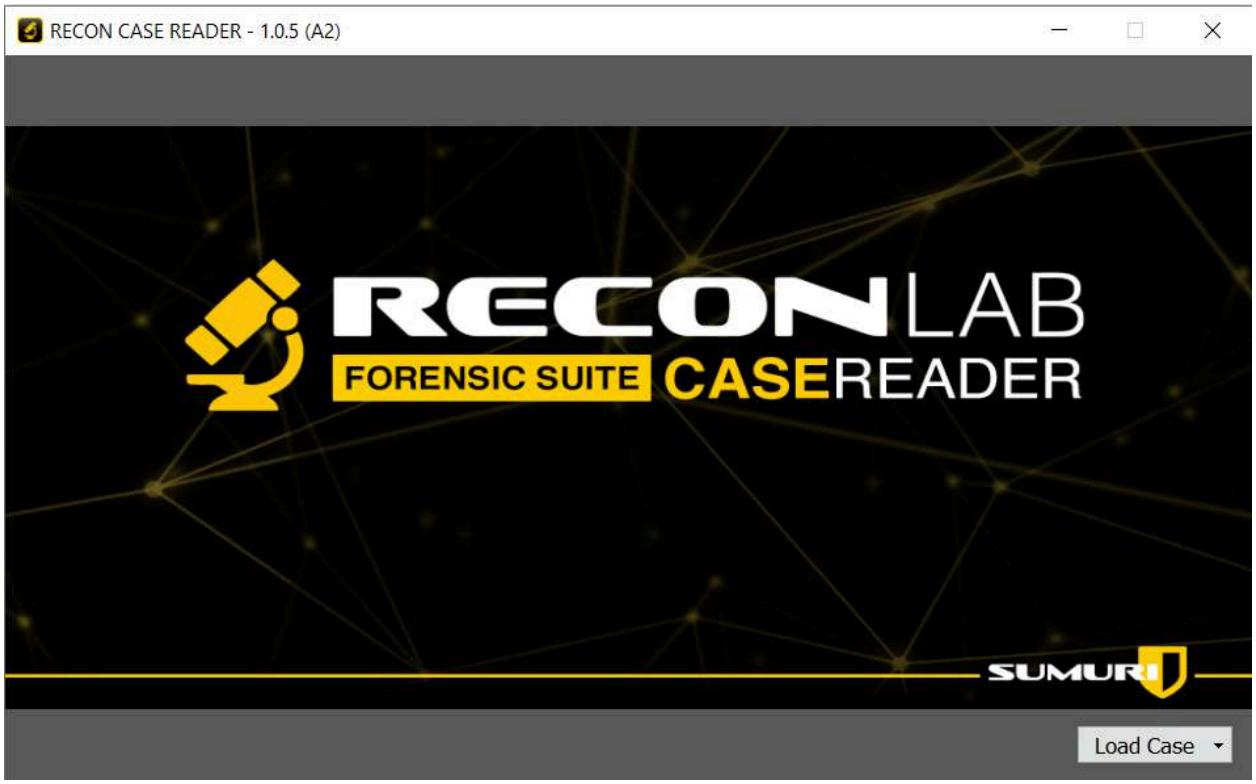


Click Install to begin installing RECON CASE. The default installation path is C:\Program Files (x86)> RECON CASE READER

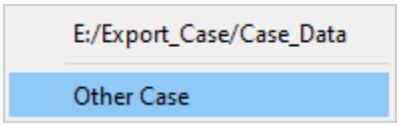


Click Finish to complete the installation. Keeping the Launch RECON CASE READER box checked will automatically launch the RECON CASE READER once the installation is complete.

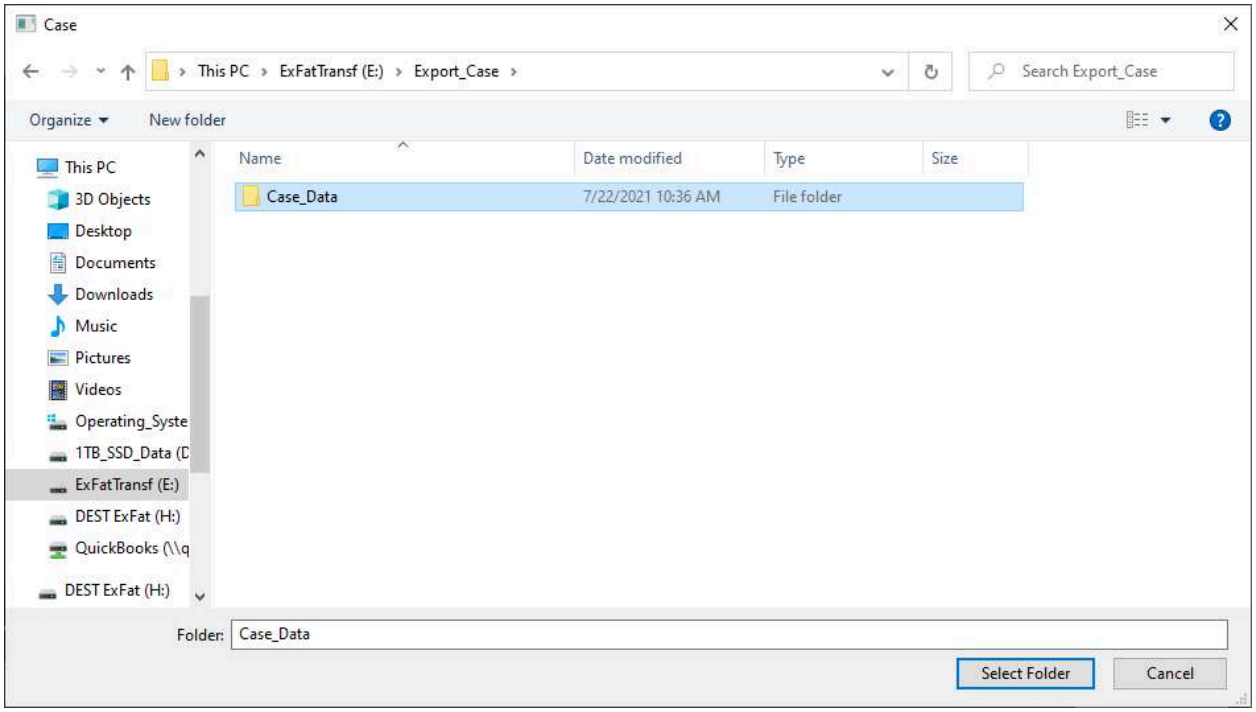

Setup - RECON CASE READER version 1.0.5 (A2)
Completing the RECON CASE READER Setup Wizard
Setup has finished installing RECON CASE READER on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch RECON CASE READER
Finish



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.



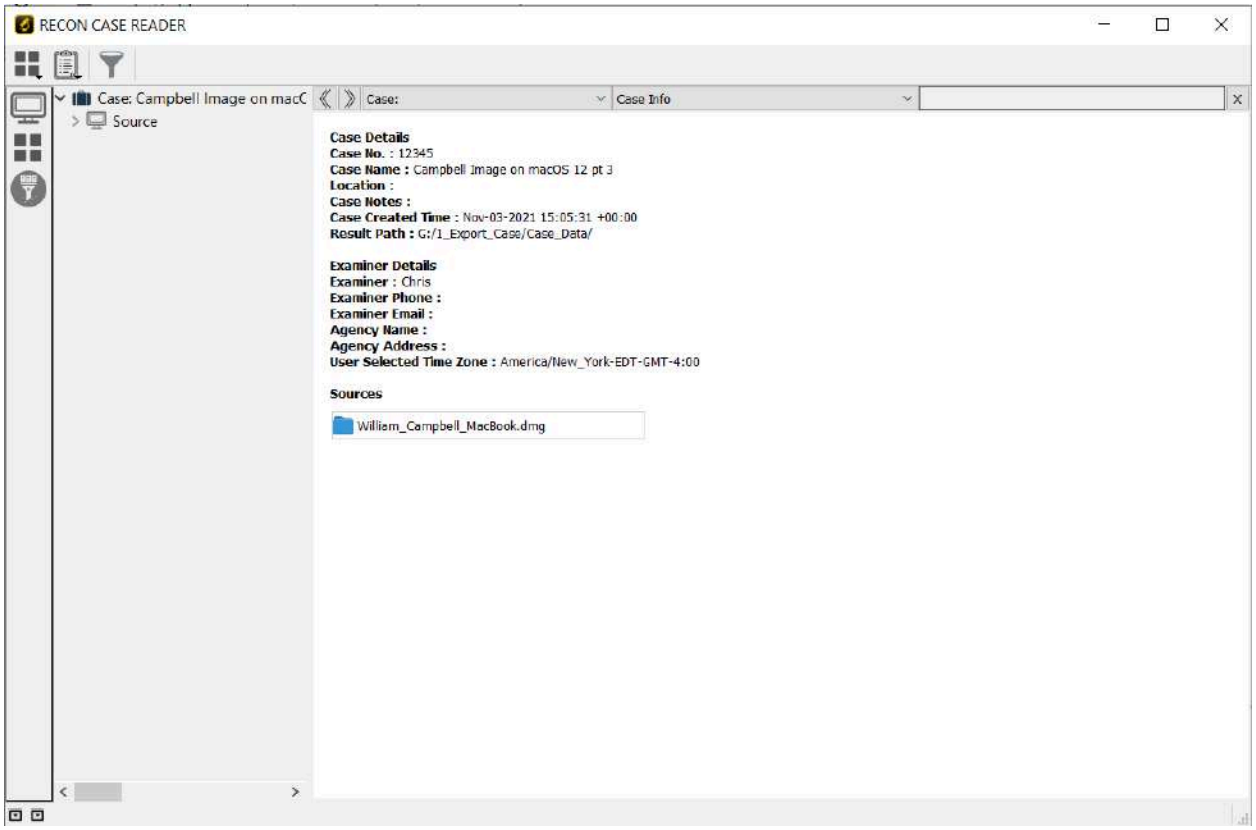
Other Case will open a File Explorer window where examiners can navigate to exported RECON LAB case folders. Exported case folders are named Case_Data by default.



Once a case folder or previously loaded case is selected RECON CASE READER will begin to load results.

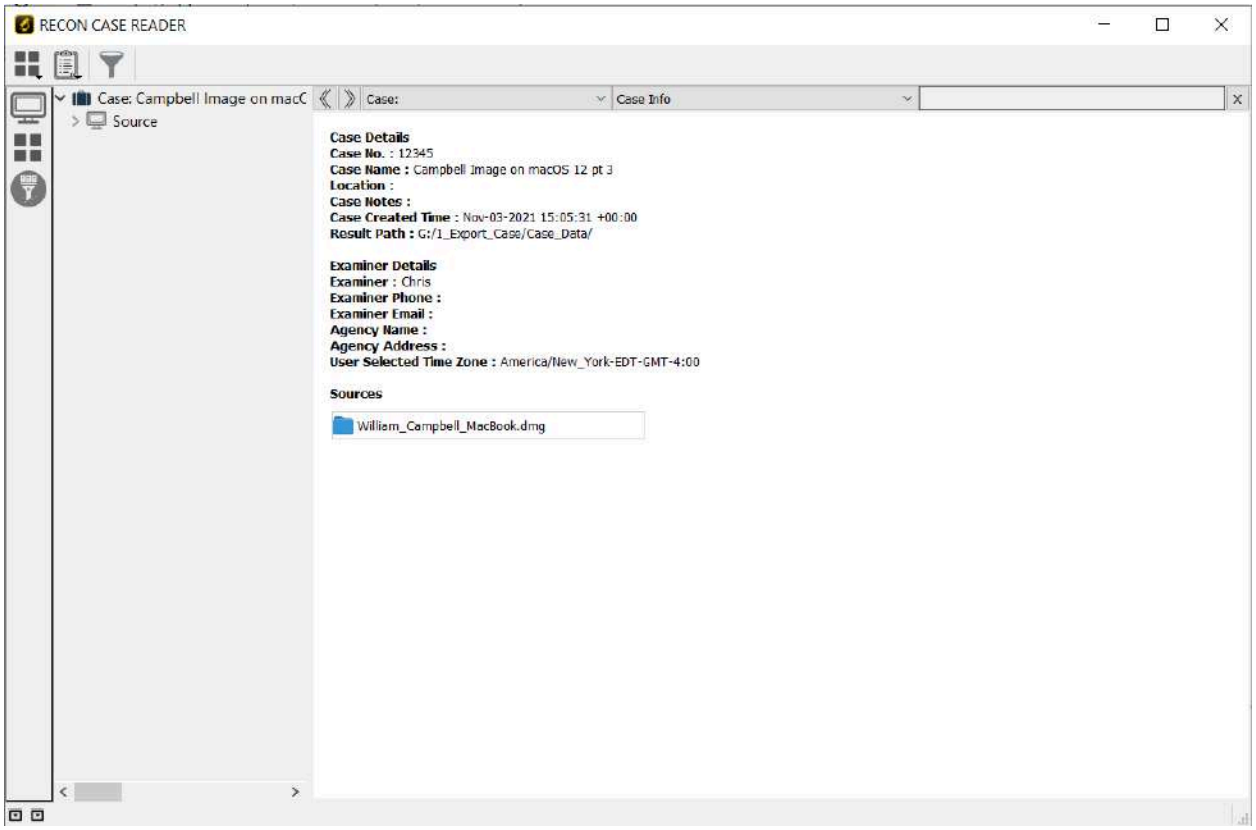
33.3 RECON CASE Reader Interface

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.



33.4 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.

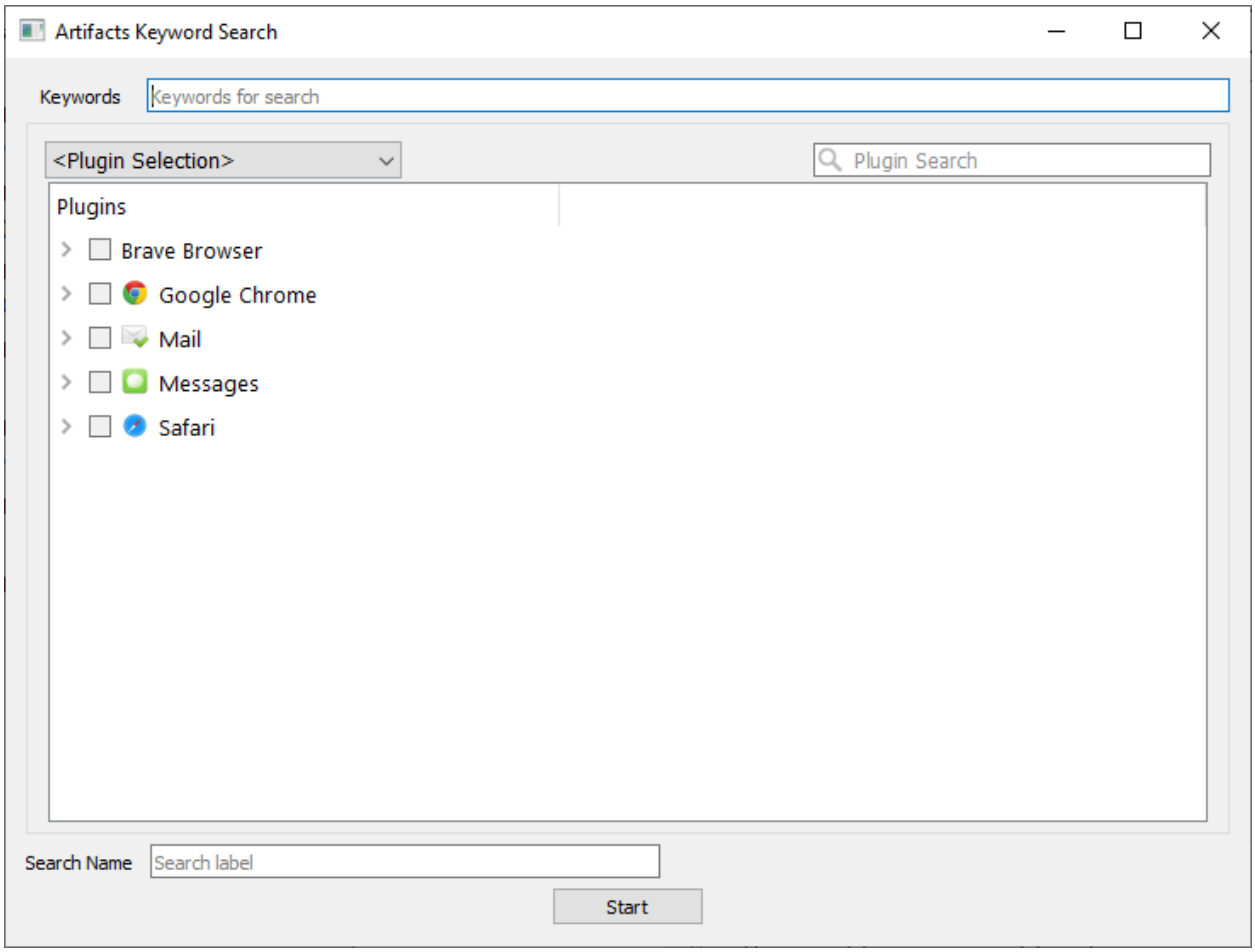
The Case Info screen displays the sources used when exporting the case. More information about each source can be found by clicking on the name of the source.

33.5 Top Menu

RECON CASE Readers Top Menu has 3 buttons two of which have sub-menus.

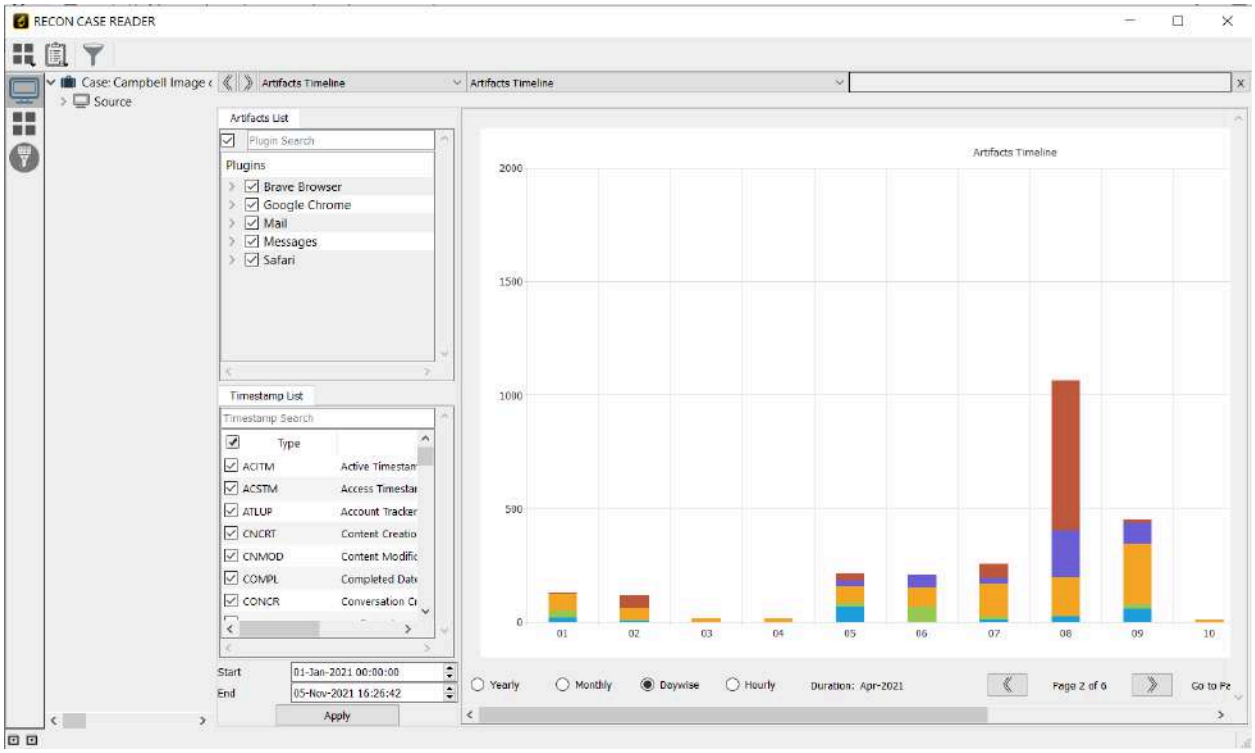
- Artifacts - contains the “Search Artifacts” and “Artifact Timeline” sub-menus

- 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.

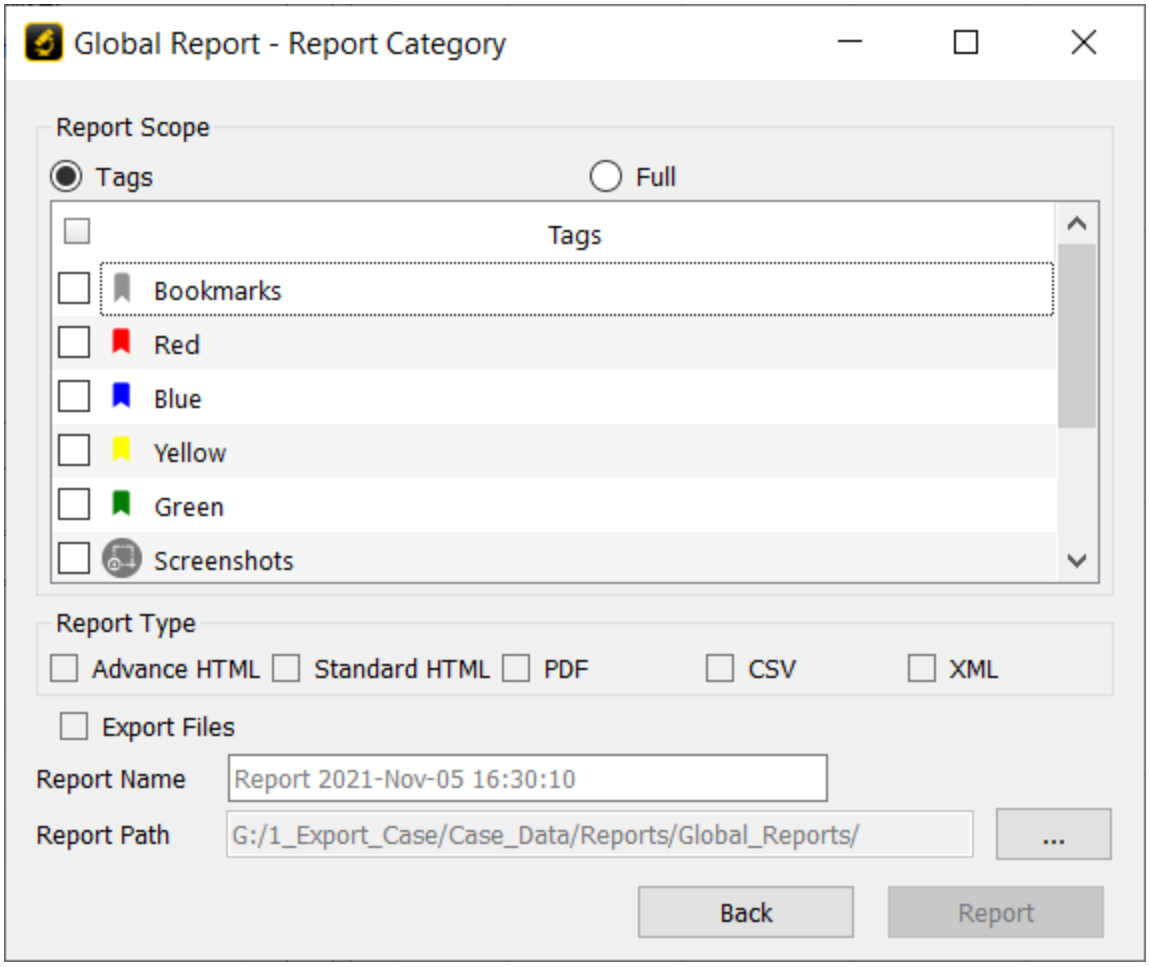


- Artifacts Timeline - Opens the Artifacts Timeline module used for generating timelines and graphs for timestamps recovered from the exported Artifacts and Plugins module. Section 27.2

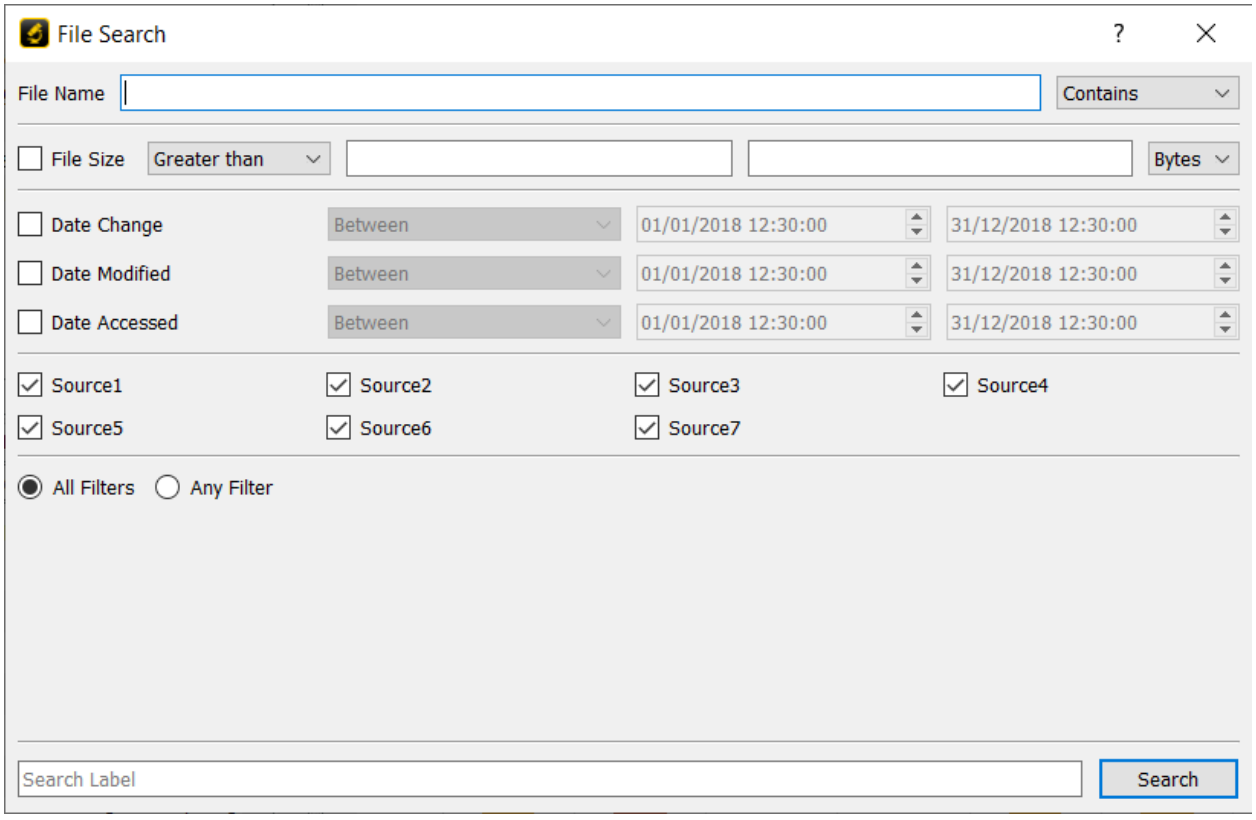
has more information on Artifacts Timeline.



- Generate Report - contains the “Automated Report” menu
- Automated Report - automatically generates reports from bookmarks or plugins. Section 32.2 has more information about Global Reports



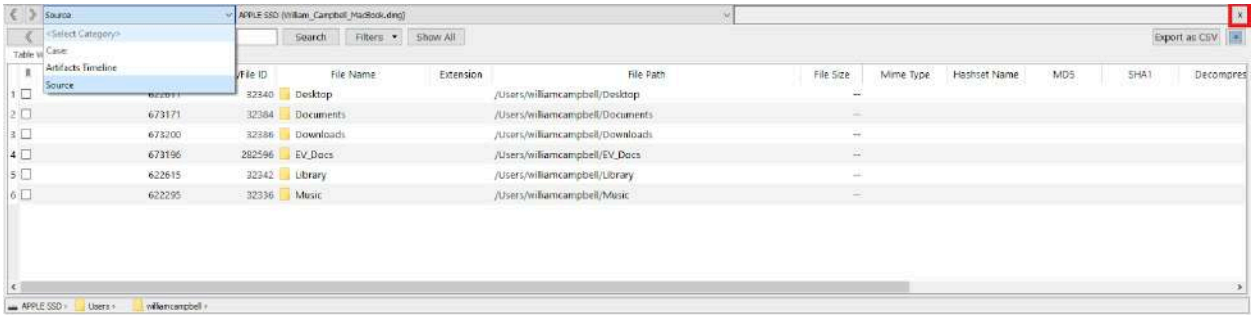
File Search - Allows for locating files based on a combination of timestamps, file names, extensions, file sizes, and more. Section 19.2 has detailed information about File Search.



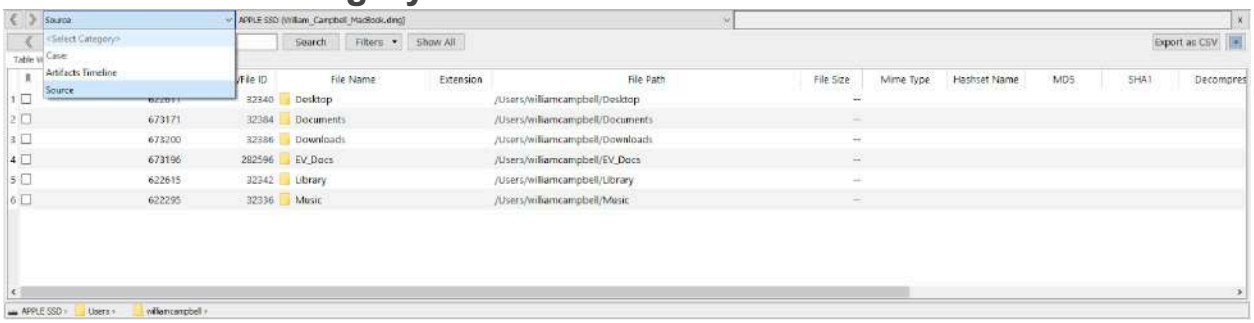
33.6 Main Columns

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.

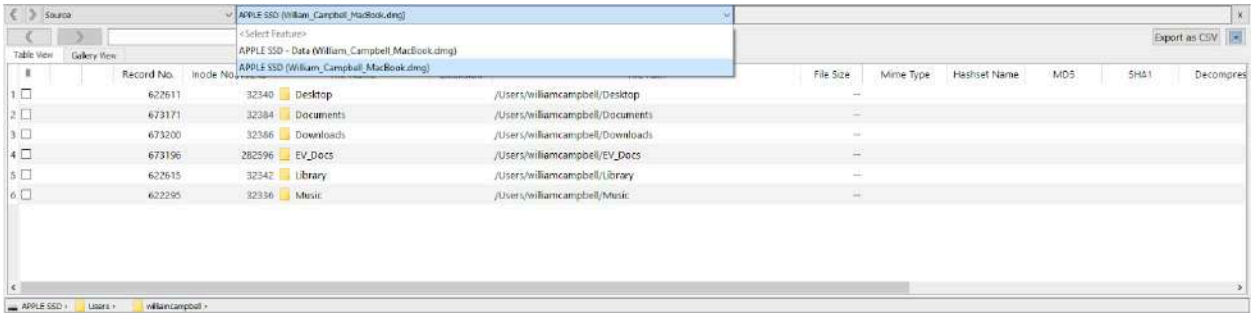


33.6.0.1 Select Category Column



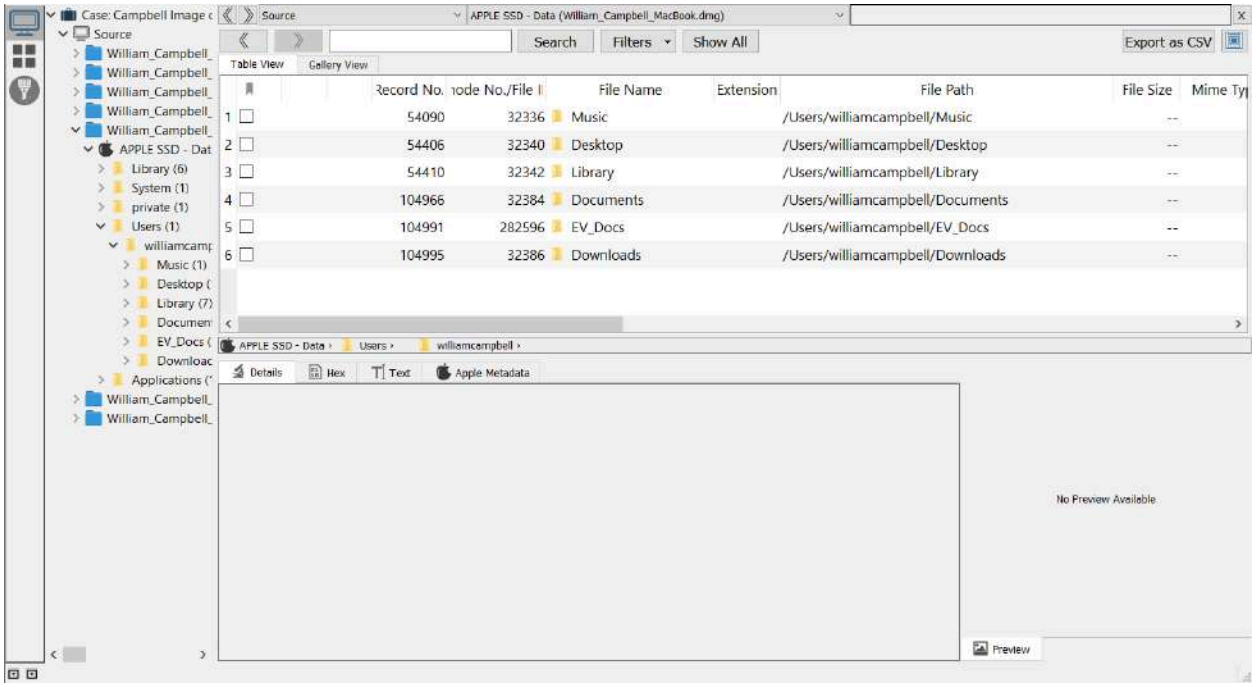
The Select Category Column keeps a history of modules and sources previously viewed. Clicking the title of the column will show previous items. Select any item to return to the module or source.

33.6.0.2 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.

33.7 Case Sidebar



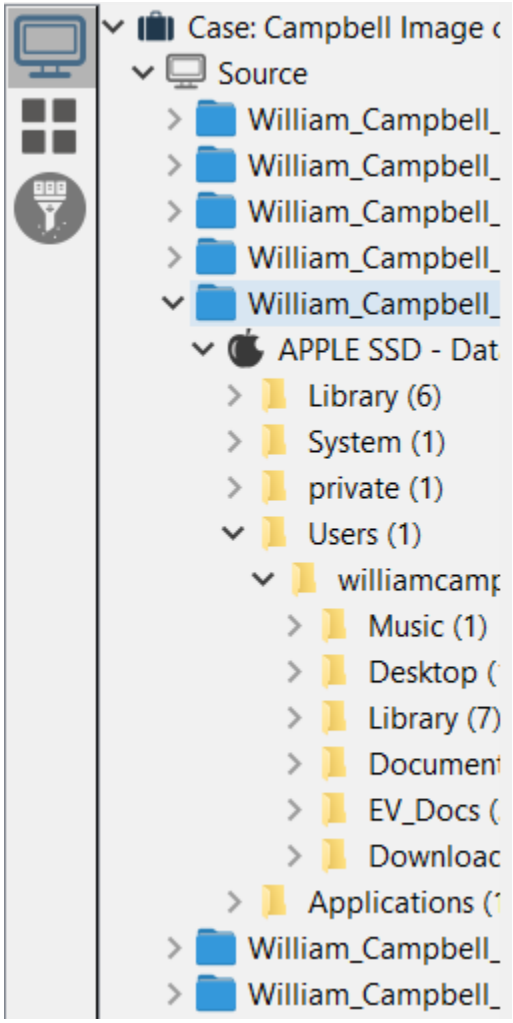
The sidebar is used to quickly access data found from processing and analysis. It can also be used to manually navigate through the exported source data.

Clicking the dropdown arrow next to a category or directory will expand it.

The case sidebar is broken up into three sections.

- Source - Displays the exported data allowing for manual review and analysis.
- Artifacts - Displays data parsed from artifacts at the time of export as well as artifact keyword search results and artifact timeline results
- File Filters - Displays information about file types and File Search results

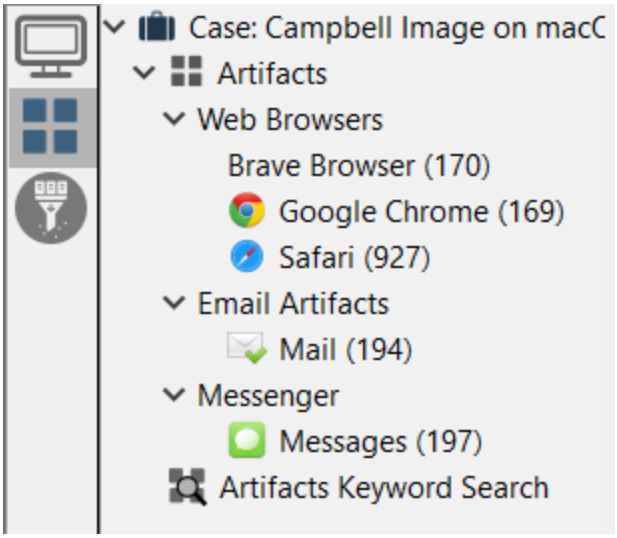
33.7.1 Source

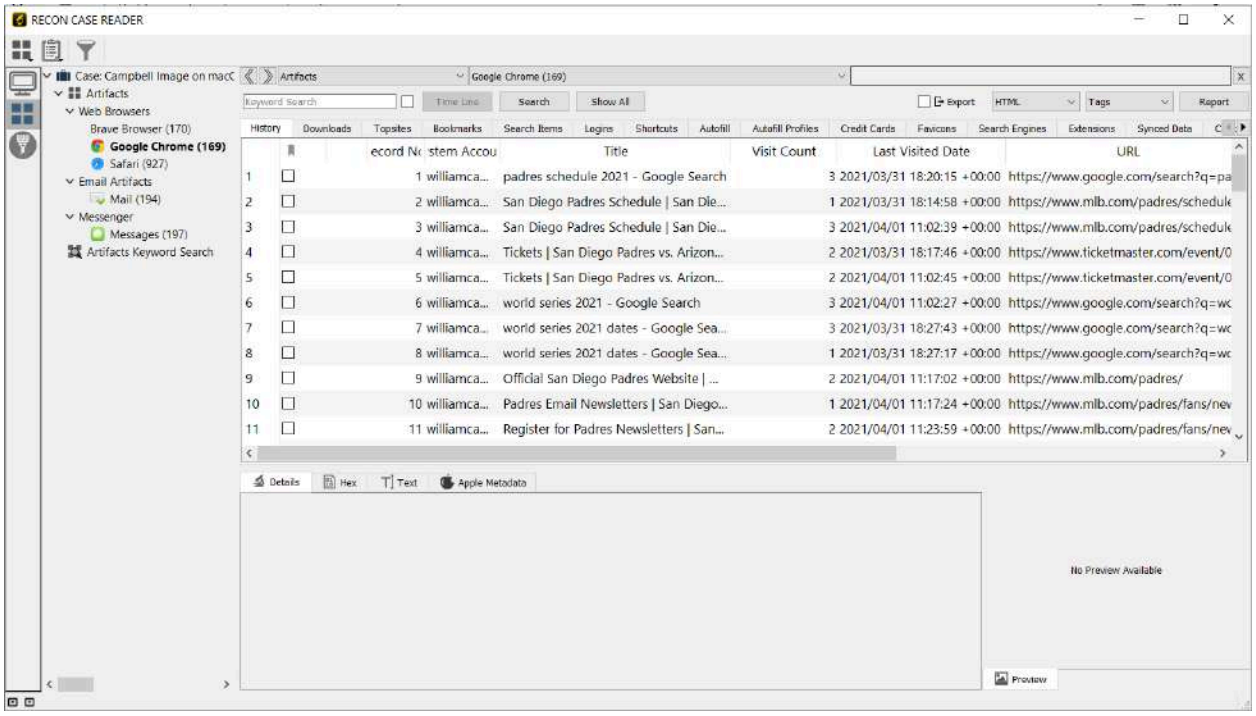


The source tab shows the exported files in a directory structure. Examiners can easily manually navigate through the directories of the exported data.

33.7.2 Artifacts

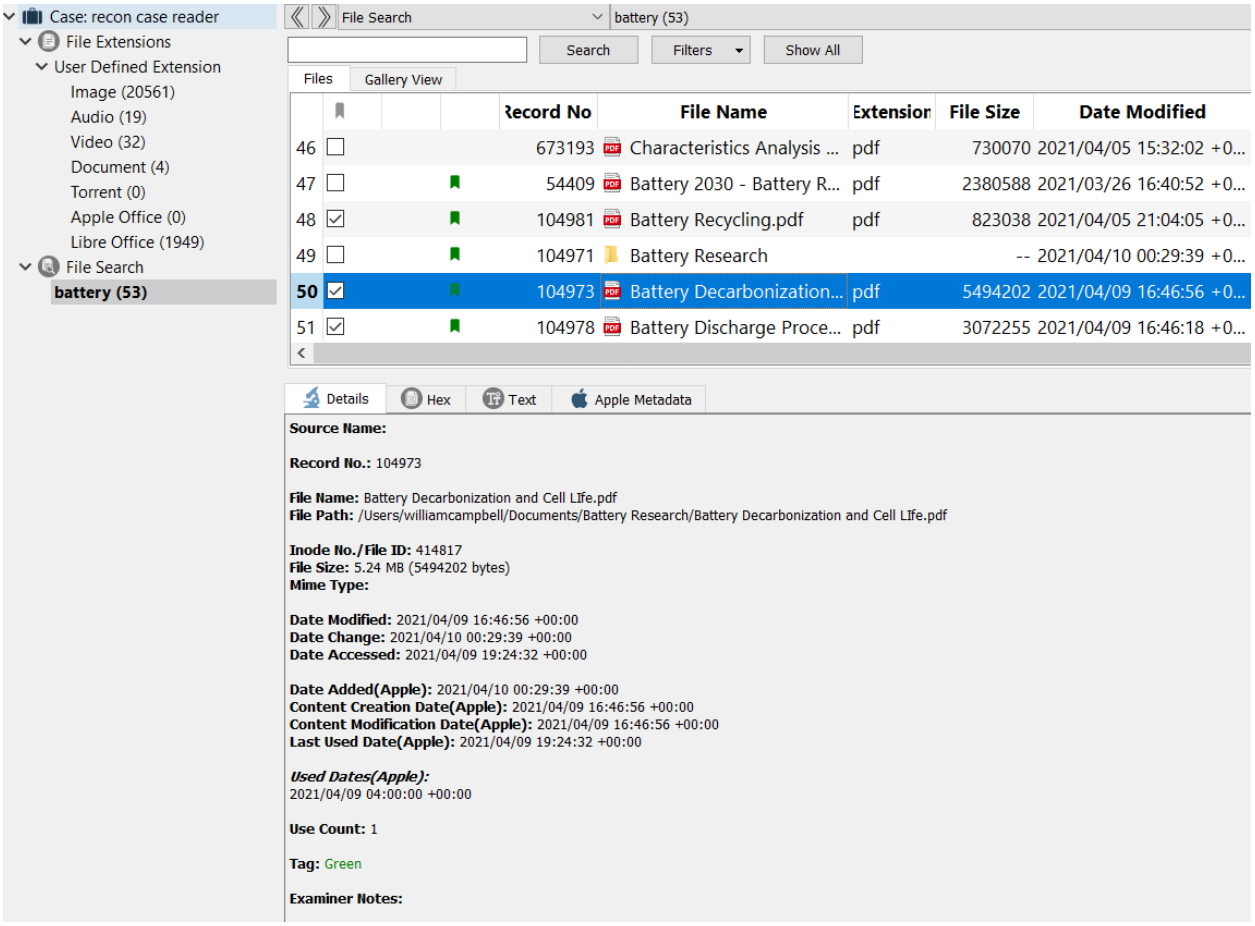
The artifacts tab displays information from exported artifacts along with the results from Artifact Keyword searches and Artifact Timelines.





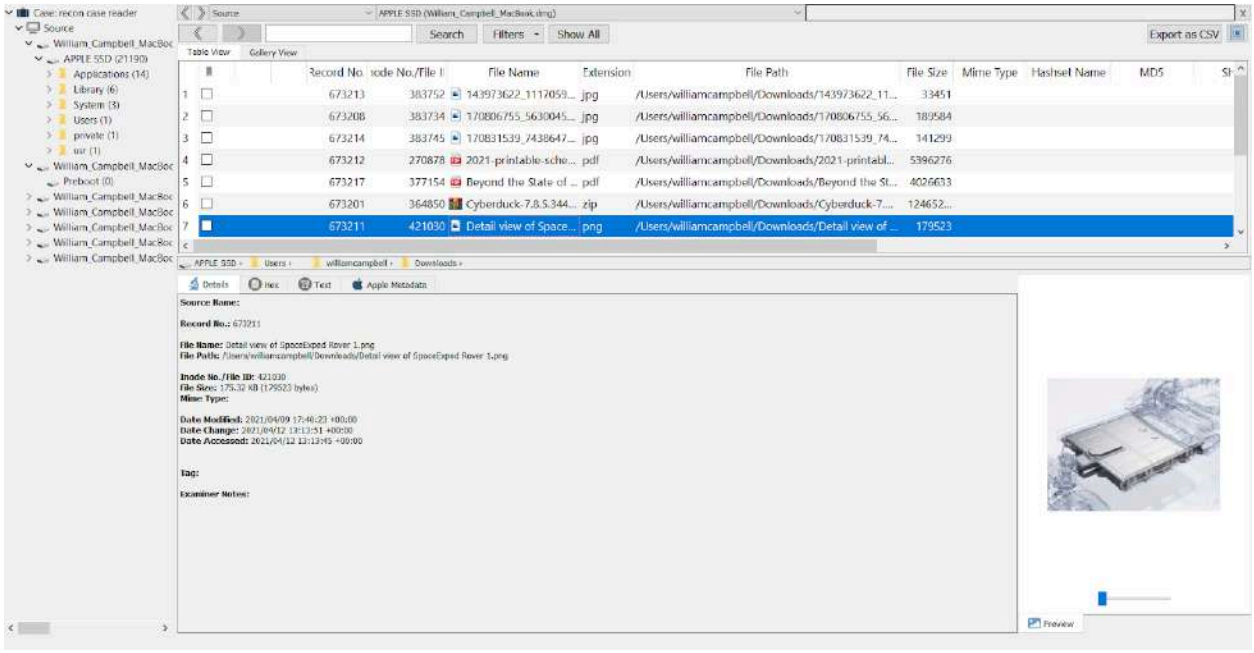
33.7.3 File

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.



33.8 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.



---

34 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.

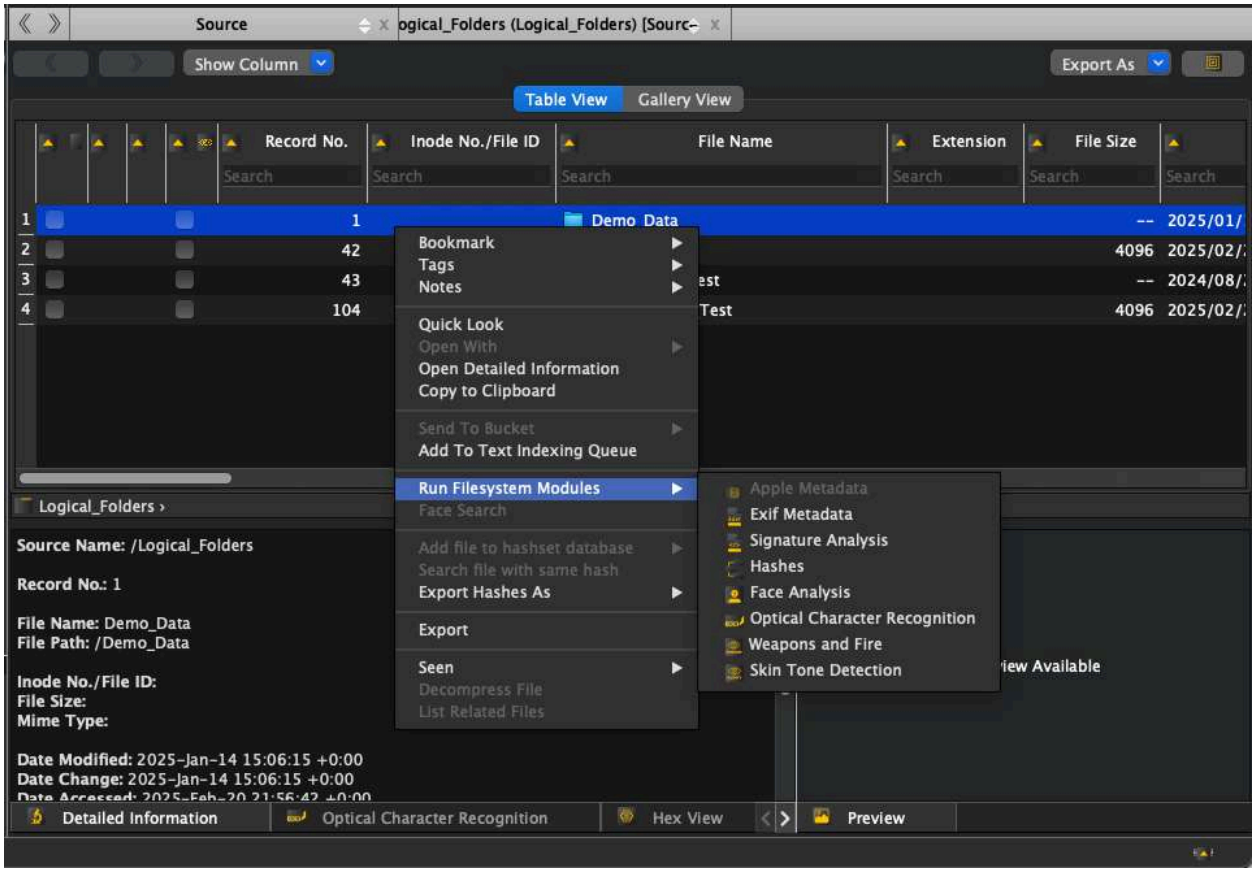
---

35 Weapon and Fire Analysis

The Weapon and Fire analysis file system module allows RECON LAB to automatically identify and categorize pictures that have firearms and fire in them. Pictures will be categorized as either Guns or Rifles, or Fire and put into their own category.

35.1 Processing for Weapon and Fire Analysis

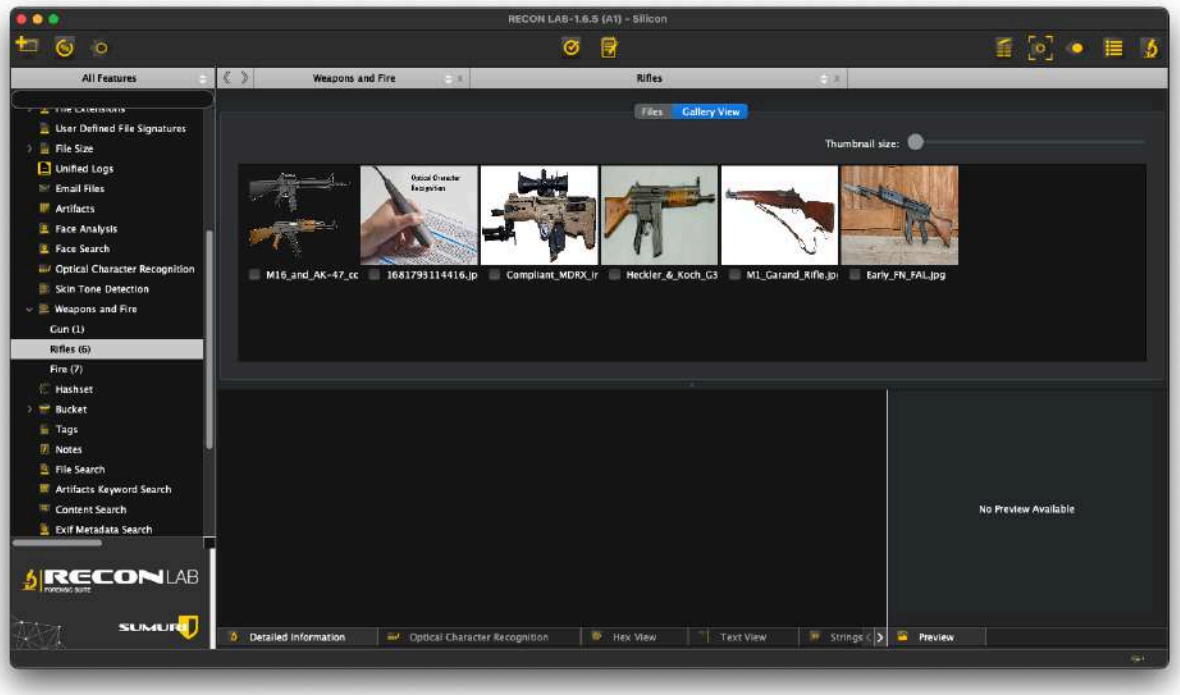
Weapon and Fire is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing options including Weapons and Fire Analysis. This can also be accessed through the Process tab.



35.2 Analysis Results

Results are put into their own category on the left menu. The results are broken into three subcategories of Guns, Rifles, Fire.

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.



---

36 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.

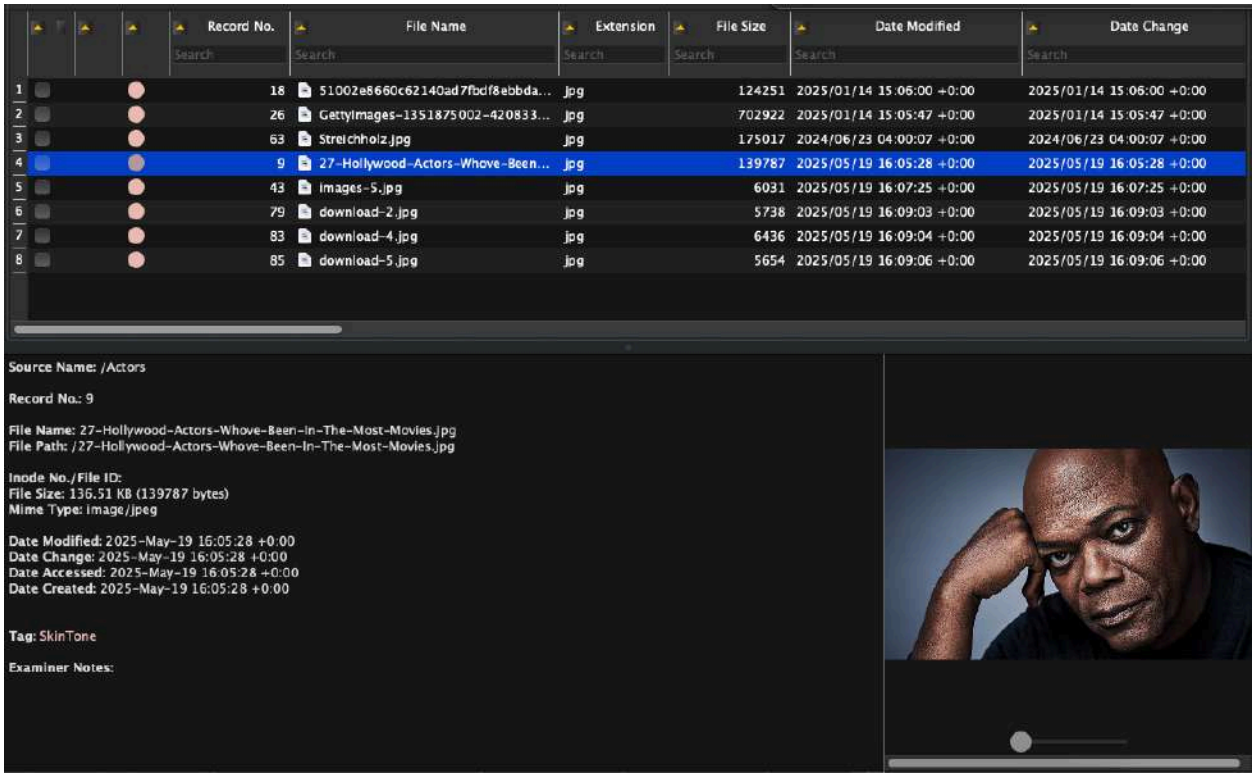
36.1 Processing Skin Tone Detection

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.

36.2 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.



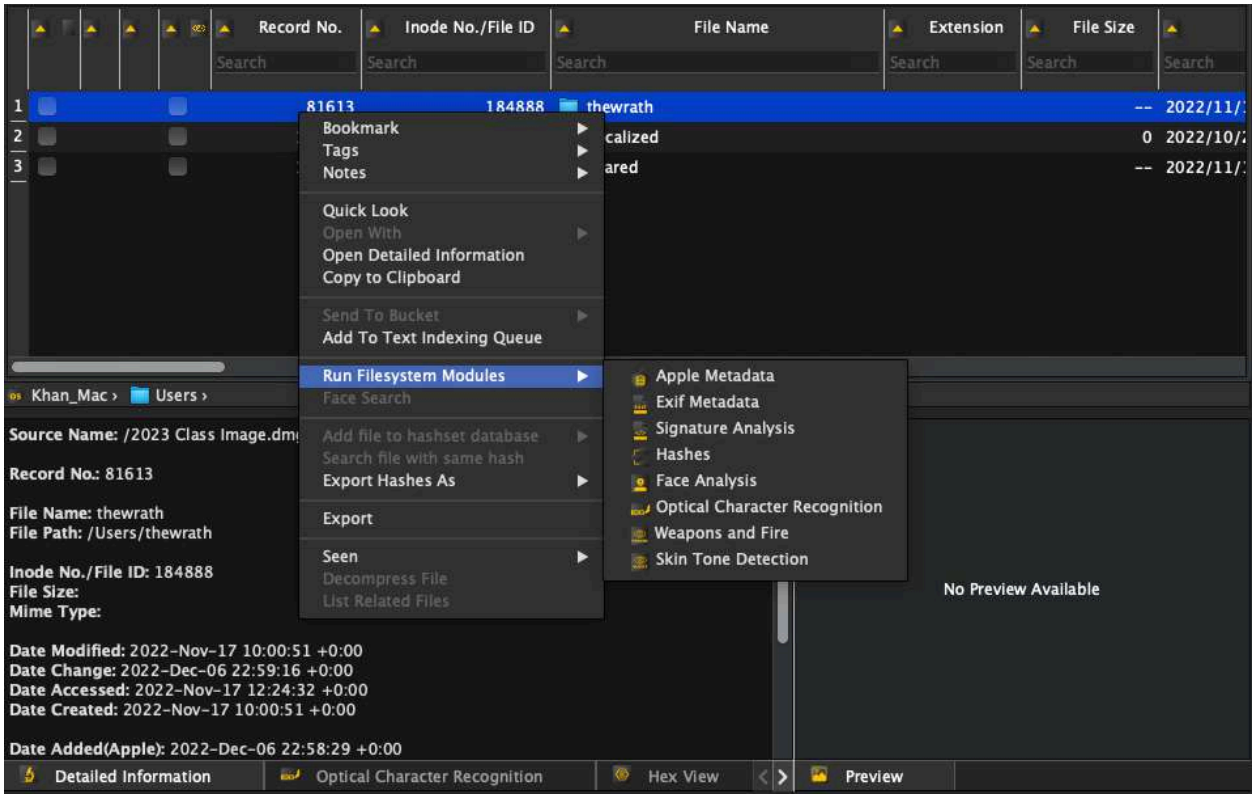
---

37 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.

37.1 Processing for Face Analysis

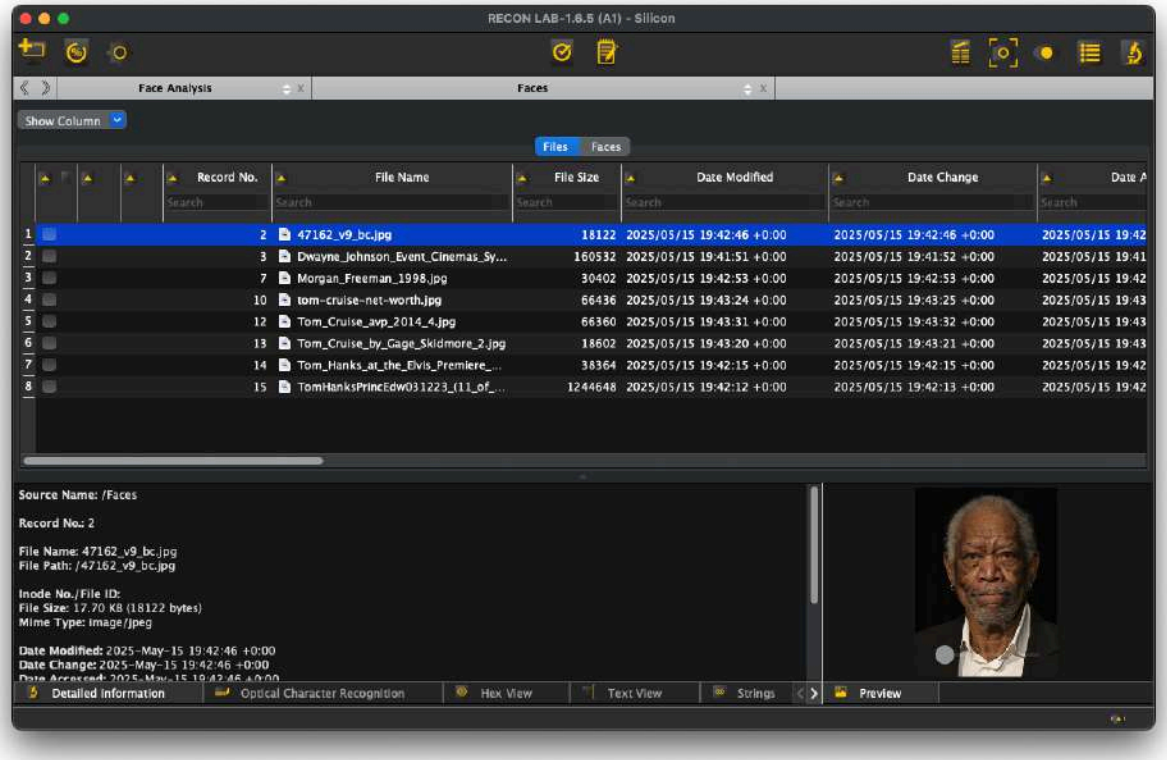
Face Analysis is processed as a file system module and is accessed by right-clicking a file or directory in the file system. The screenshot below shows the file system module processing options including Face Analysis.



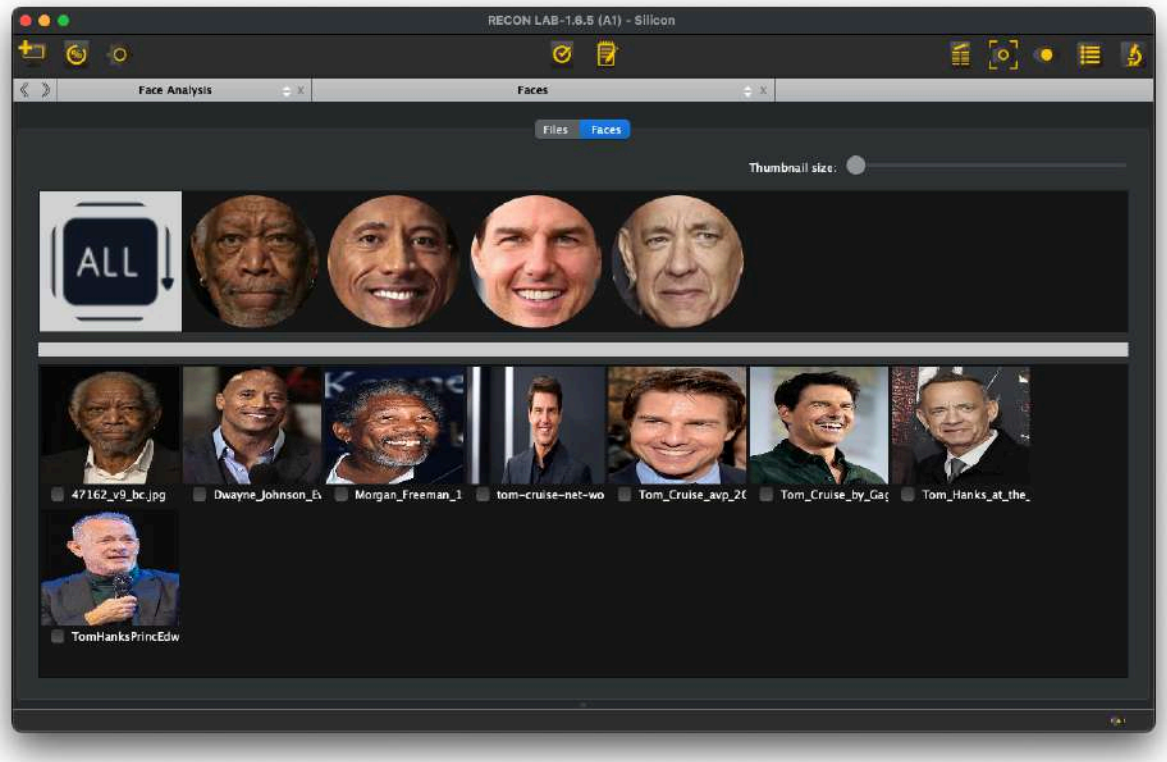
**Note* Faces must be indexed using the Face Analysis Feature before the Face Search Feature can be used.*

37.2 Face Analysis Results

Results from Face Analysis are displayed in their own category in the left menu. After selecting Faces all of the detected faces will be displayed in one section. The identified faces 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.



---

38 Optical Character Recognition (OCR)

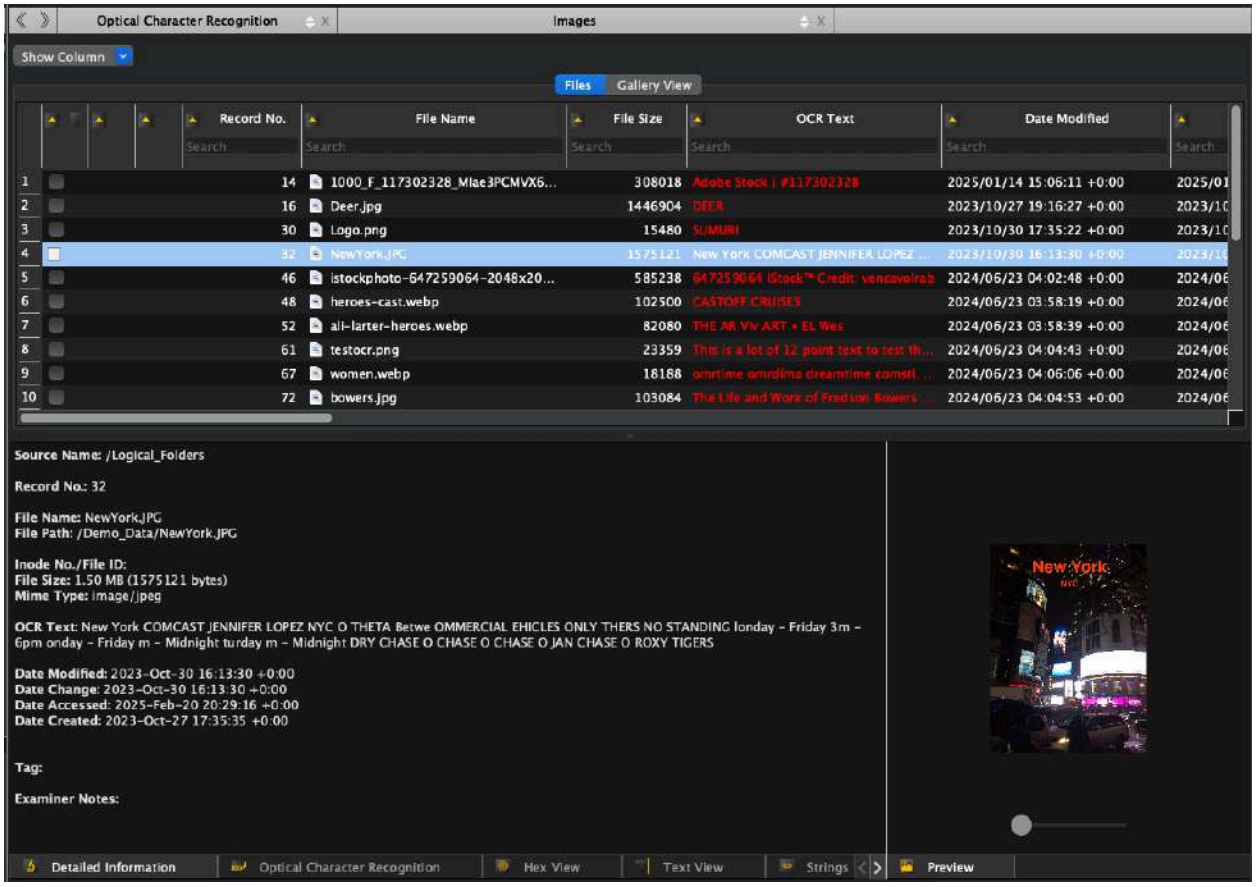
The Optical Character Recognition File System Module allows RECON LAB to automatically identify and index pictures that have text in them. Detected pictures will be put into their own category for easy analysis.

38.1 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.

38.2 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. Running OCR on a file or directory, allows those files to be searched via the OCR search in the File Search window.

---

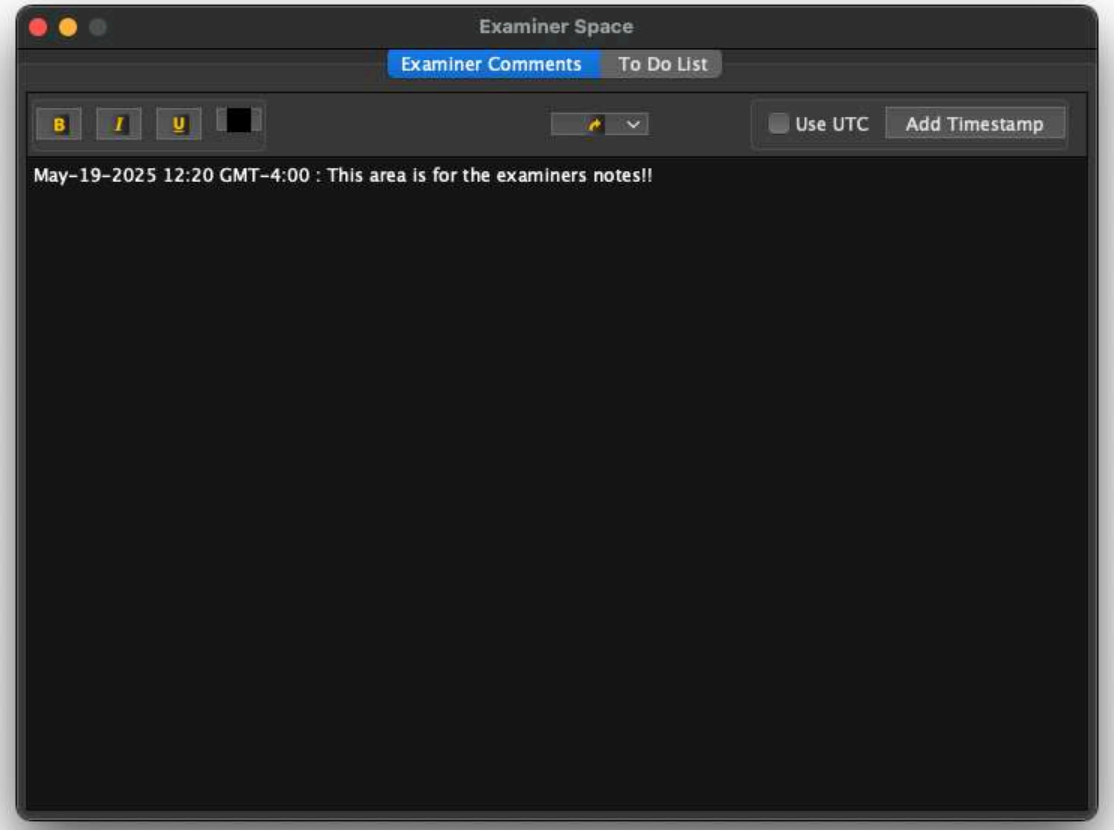
39 Examiner Space

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.

39.1 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.

39.2 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.

40 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.