## **RECON LAB Manual**

## 1. Introduction



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

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

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

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

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

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

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

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

## 1.1 Why Use a Mac for Forensic Analysis?

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

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

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

#### **1.1.1 Apple Extended Attributes**

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

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

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

Understanding Apple Extended Metadata is critical to investigations.

#### 1.1.2 Viewing Proper Timestamps

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

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

#### 1.1.3 Viewing Files Natively

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

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

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

### 1.1.4 Apple File System (APFS)

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

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

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

### 1.1.5 Local Time Machine Snapshots (APFS)

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

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

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

#### 1.1.6 FileVault

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

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

#### 1.1.7 Support for Other File Systems

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

MacOS natively supports APFS, macOS Extended (HFS+), MS-DOS FAT, ExFAT and NTFS (as readonly). Using freely available open-source FUSE solutions and Paragon Software drivers (included) just about any file system can be mounted and processed with RECON LAB such as Linux ext2, ext3, and ext4.

## **1.2 Hybrid Processing Engine**

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

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

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

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

### 1.3 Three Stage Analysis

RECON LAB offers three-stages of analysis.

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

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

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

## 1.4 Support for Hundreds of Timestamps

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

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

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

### **1.5 Advanced Timelines**

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

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

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

### **1.6 Advanced Data Correlation**

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

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

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

## **1.7 Advanced Reporting With Full Control**

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

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

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

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

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

## 2. Recommended Minimum Requirements

Macs are unique in doing more with less. That being said, RECON LAB will work on most Macs. Keep in mind the simple formula: **Processor + RAM = Speed** 

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

# 2.1 Minimum Recommended Specifications for Running RECON LAB

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

An Admin user required.

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

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

## 3. Helpful Hints

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

#### Use macOS Extended for Evidence Drives

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

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

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

#### <u>Use Apple Disk Image Format (.dmg) for Imaging Evidence</u>

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

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

#### Avoid Segmentation of Forensic Image Files

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

## 4. Getting Support

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

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

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

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

#### 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: <u>https://sumuri.com/product/recon-lab-renewal/</u>

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

## 6. Training

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

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

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

• Hosting SUMURI Training

## 7. Installation

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

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

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

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

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

## 7.1 Installing Xcode and Command Line Tools

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

#### Installing Xcode

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

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

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

#### Installing Xcode Command Line Tools

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

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

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

3.) Follow the instructions provided by the application.

## 7.2 Installing FUSE for macOS

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

#### **Installing FUSE for macOS**

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

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

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

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

## 7.3 Installing Paragon Drivers

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

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

#### **Accessing Paragon Software Applications**

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

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

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

#### Installing extFS for Mac by Paragon Software

- 1.) Download extFS for Mac following the instructions above.
- 2.) Double-click on the .dmg downloaded from Paragon.
- 3.) Double-click on "Install extFS for Mac" to install drivers for Linux file systems.
- 4.) Complete the installation by following the instructions provided.

## 7.4 Installing RECON LAB

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



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

-	"RECON_LAB_INS" Internet. Are you	TALLER" is an app downloade sure you want to open it?	ed from the
4	"RECON_LAB_INSTAL "RECON_LAB_1,2,2,7dr October 4, 2019.	LER* is on the disk image ng*. Safari downloaded this disk ima	ege on
	Don't warn me v	when opening applications on t	his disk imag
?	Cancel	Show Disk Image	Open

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

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

	Package Installation	
Please waitC	hecking packages	
		-

If prompted, select install to install the extra packages.

•••	Package Installation
Recon Lab Installer n	eeds to install missing packages. Please click on 'Install' to continue.
	Skip Install

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

Packages installation completed. Please click on 'Continue'.	
	Continue

The RECON LAB Installer window will now appear.



Choose one of the following options:

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

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

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

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

## 7.5 Granting Privileges

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

#### 7.5.1 Full Disk Access

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

#### 7.5.1.1 macOS 12 and Below

About This Mac	
System Preferences	1 update
App Store	
Recent Items	►
Force Quit System Preferences	70#0
Sleep	
Restart	
Shut Down	
Lock Screen	^#Q
Log Out Steve Whalen	企業Q

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



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



- 1.) Click on the lock icon in the bottom left corner and enter the admin password to unlock.
- 2.) Select the **Privacy** tab and then **Full Disk Access** in the sidebar.
- 3.) Click the **"+"** symbol and navigate to the RECON LAB application.
- 4.) Select the **RECON LAB** application to give Full Disk Access permissions.

#### 7.5.1.2 macOS 13 and above

Alongside the release of macOS 13, Apple introduced a change to the tried and true System Preferences to make it more akin to iOS. System Preferences has now been changed to System To give RECON LAB Full Disk Access on macOS 12 and below, navigate to **System Settings** using the **Apple Menu** found in the top left corner (Apple Menu – System Settings).

About This Mac	
System Settings	
App Store	9 updates
Recent Items	>
Force Quit Brave	℃&#©</td></tr><tr><td>Sleep</td><td></td></tr><tr><td>Restart</td><td></td></tr><tr><td>Shut Down</td><td></td></tr><tr><td>Lock Screen</td><td><b>~</b> 米 Q</td></tr><tr><td>Log Out SUMURI</td><td><b>ት ដ</b> Q</td></tr></tbody></table>

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

•••	Privacy & Security	
Q Search	Privacy	
Chris Grettenberger Apple ID	Location Services	>
🛜 Wi-Fi	Contacts	>
8 Bluetooth	77 Calendars	>
Network     VPN	E Reminders	×
Notifications	🌸 Photos	>
Sound	8 Bluetooth	>
Focus	Microphone	>
General	Camera	>
Appearance	🙆 HomeKit	>
Accessibility     Control Center	III Speech Recognition	>
Siri & Spotlight	10 Media & Apple Music	>
Privacy & Security	Files and Folders	>
Desktop & Dock	Full Disk Access	>

- 1.) Navigate to Full Disk Access
- 2.) Scroll to the bottom of the window to locate the "+" symbol.
- 3.) Click the **"+"** symbol and enter the **administrator password**.
- 4.) Navigate to the **RECON LAB** application.
- 5.) Select the **RECON LAB** application and enable the switch to give Full Disk Access permissions.

C Search	Allow the applications below to access data like Mail, Messages, Safari,
S Focus	users on this Mac.
🔀 Screen Time	A Google Software Lindate
6 General	
	RECON_ITR
Accessibility	👩 RECON_LAB
Control Center	+ -
🔄 Siri & Spotlight	
Privacy & Security	
Dealstern & Deals	
Desktop & Dock	
Displays	
Wallpaper	
Screen Saver	
Energy Saver	
Lock Screen	
🔟 Login Password	
Users & Groups	
Passwords	
Internet Accounts	

## 7.6 Energy and Sleep Settings

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

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

#### 7.6.1 macOS 13 (Ventura) and below



Look for the **Energy Saver** icon.



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

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



Coursels	Low Power Mode	Never 0
a Search		
General	Battery Health	Normal (1)
Appearance		
Accessibility		ays
Control Cente	Enable Power Nap Never While sleeping, your Mac can periodically check for new email.	
💽 Siri & Spotligi	calendar, and other iCloud updates.	
🕑 Privacy & Sec	Put hard disks to sleep when possible Only on Battery <	100%
Desktop & Do	Wake for network access Never 🗘	50%
🔅 Displays	Automatic graphics switching	
Wallpaper	To increase battery life, your Mac will automatically choose the best graphics mode based on your usage	0%
Screen Saver	graphies mode based on your asage.	12 P
Battery	Optimize video streaming while on battery	
		60m
Lock Screen	Done	20-
Touch ID & Pa		SUM
Users & Groups		Om
Passwords	3 6 9 12 A 3 6 9	12 P
Internet Account	ts	
🐻 Game Center		Options
Wallet & Apple F	Pay	Colorising 1

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

#### 7.6.2 macOS 12 (Monterey) and below



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

	Turn display off after:		
			U
9	Never letting your display go	o to sleep may shorten its life	Never
	Prevent your Mac from automatic	cally sleeping when the displa	y is off
	Put hard disks to sleep when post	ssible	
Charging On Hold Rarely used on battery	🗹 Wake for network access		
	While sleeping, your Mac can receive and other iCloud updates, to keep you	incoming network traffic, such as ur applications up to date.	iMessages
	Low power mode		
Usage History	Your Mac will reduce energy usage an	nd operate more quietly.	
Battery			
🗲 Power Adapter			
Schedule			
		Restore De	faults ?

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



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

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

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

## 7.7 Updating RECON LAB

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

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

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

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

#### Updating with a Renewed License

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

Do you want to replace License	file ?
	ОК

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

## 8. Starting RECON LAB

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

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



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

## 8.1 Adding Your License

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

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

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

Please click '	Browse' and loca	ate RECON LAB	license file.
		Cancel	Browse

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

Select your license file and choose "Open".

RECON LAB will add your license and restart.

## 8.2 Installing Python

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

#### Installing Python

- 1. Download and install Python version 3.9.6 for macOS from this link: <u>https://www.python.or</u> <u>g/downloads/</u>
- 2. Open Finder then go to the Applications folder, find the Python application, on the left side of the Python app you will see a dropdown arrow, expand it and double click on "Install Certificates.command".
- 3. After installing the certificates open your terminal and run the following command to install additional required libraries: python3 -m pip install lz4 enum34
- 4. Messages regarding updating "pip" can be ignored.

### 8.3 Admin Password

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

## 8.4 Access Warning Messages

0 0	RECON LAB
When adding a source that RECON LAB to access "your	contains Apple Calendar, Reminder or Contact files your system will ask you to allow " Calendar, Reminders or Contact files.
You must give permission	for RECON LAB to continue.
RECON LAB is accessing the occurs when macOS detect	e source files only and not your Calendar, Reminder or Contact files. This prompt s any Calendar, Reminder or Contact files.
If you are using macOS 10. Preferences->Security & Pr	14 or above, make sure you give full disk access to RECON LAB. (Apple Menu->System ivacy->Privacy->Full Disk Access).
Please check 'About RECON	'-> 'Requirement' section for installation of open source libraries required.
Don't show this message	again

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

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

## 8.5 RECON LAB Welcome Screen



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

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

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

The buttons along the bottom of the Welcome Screen are:

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

**RECON Config** – Allows the examiner to create persistent settings.

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

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

## 9. Configuration

Every examiner will have a unique approach to an examination.

RECON LAB allows an examiner to configure a variety of settings prior to starting a case. Configuration settings are persistent and will automatically be set for each new case. This approach saves a lot of time. Configuration settings can be overridden at any time if required.

### 9.1 Examiner Details

			RECON LAB-1.5.0 (	A1)
2	Examiner Details			
	Artifacts		Agency Name	
	User Defined Extensions		Examiner	
	User Defined File Signature	BECON	Examiner Phone	
	Keyword List		Examiler Phone	
:=	Text Indexing Filters	LAB	Examiner Email	
Ó	Apple Metadata Filters		Agency Address	
	Exif Metadata Filters			
	Volatility Path			
(m)	System Password			
7	External Applications			
	Preferences			
Ť	Debug			
	Back			

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.

Look in:	Users/macboy/Pictures/SUMURI Logo	o o o 🛤 🗉 🗉
Volume / macboy Downlo	s Name SUMURI Logo.001.png ads	▲ Size 30 KB
File name:	SUMURI Logo.001.png	Open
Files of type:	*.png *.jpg *.jpeg	Cancel

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

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

## 9.2 Artifacts and Plugins

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

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



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

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

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

Artifacte		<plugin selection=""> 📀 🗴 photo</plugin>	
<ul> <li>Artifacts</li> <li>User Defined Extensions</li> <li>User Defined File Signature</li> <li>Keyword List</li> <li>Text Indexing Filters</li> <li>Apple Metadata Filters</li> <li>Exif Metadata Filters</li> <li>Volatility Path</li> <li>System Password</li> </ul>	All Plugins macOS Plugins IOS Plugins winOS Plugins androidOS Plugins Google Takeout Plugins Advanced Analysis Apple Apps	Plugins         Plugins         Image: Selection Photos         Image: Selection	
<ul> <li>External Applications</li> <li>Preferences</li> <li>Debug</li> </ul>	Apple Apps Apple Logs Backups Device Download Manager Email Artifacts Email Client FTP Client Google Takeout		
Back	Save Template	Template Name	Add

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

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

#### Saving a Template for Plugins and Artifacts



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

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

### 9.3 User Defined Extensions

User Defined Extension settings allow the examiner to create "buckets" (categories) for various file extensions. These categories will appear in the RECON LAB Sidebar. Any files with a matching file extension included in a Category will automatically be filtered and appear in the "bucket" in RECON LAB's Sidebar.
		RECO	N LAB-1.5.0 (A1)
-	Examiner Details Artifacts	Category	Extension
	User Defined Extensions User Defined File Signature Keyword List Text Indexing Filters Apple Metadata Filters Exif Metadata Filters Volatility Path System Password External Applications Preferences Debug	Image         Audio         Video         Document         Torrent         Apple Office         Libre Office         Libre Office	.jpg .jpeg .ico .gif
	Back		

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

#### Adding or Removing Categories and Extensions



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

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

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

# 9.4 User Defined File Signatures

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

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



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

#### Adding or Removing File Signatures



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

- 1. Use the "Label" field to provide a name.
- 2. Add the signature as HEX or ASCII and select the appropriate button.
- 3. If the file signature begins at a specific offset add the value in the "Offset" field.
- 4. Click "Add".

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

#### Editing a File Signature

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

# 9.5 Keyword Lists

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

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

dtSearch's Quick Reference Guide can be found here: <u>http://support.dtsearch.com/Support/form</u> <u>s/iframes\_advanced/default.html</u>



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

#### Adding or Removing Categories or Keywords



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

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

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

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

#### Editing a Keyword

919876////		
	Cancel	Add

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

### 9.6 Text Indexing Filters

RECON LAB has included features to speed up your examination.

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

#### <u> Default Index – No Filter</u>

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

	RECOM	N LAB-1.5.0 (A1)
Examiner Details Artifacts	• No Filter 🔿 Index these files	O Do not Index these files
User Defined Extension User Defined File Signa	s Category ture	Extensions
Fext Indexing Filters     Apple Metadata Filters     Evif Metadata Filters		
Volatility Path		
<ul> <li>External Applications</li> <li>Preferences</li> </ul>		
∦ik Debug		
	+ -	+ -
Back		

#### Indexing Specific Files Only

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

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

		RECO	ON LAB-1.5.0 (A1)	
2	Examiner Details Artifacts	🔿 No Filter 🧿 Index these file	s 🔿 Do not Index these files	
	User Defined Extensions	Category	1	Extensions
	User Defined File Signature	Documents	.rtf	
	Keyword List		.doc	
10	Text Indexing Filters		.pdf	
Ó	Apple Metadata Filters			
	Exif Metadata Filters			
	Volatility Path			
	System Password			
7	External Applications			
	Preferences			
Ť	Debug			
		+ -	+ - 0	
	Back			
( <u> </u>				

### Eliminating Files From Indexing

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

	D		RECO	N LAB-1.5.0 (A1)	
2	5	Examiner Details Artifacts	○ No Filter ○ Index these files	O Do not Index these files	
	4	User Defined Extensions	Category	Extensions	
	9 1	User Defined File Signature	Virtual Disk	.iso	
		Keyword List	Apple Disk Images	.vdi	
1	1111	Text Indexing Filters		.vnd	
ú	5	Apple Metadata Filters		windk	
		Exif Metadata Filters			
(1)		Volatility Path			
-		System Password			
	7	External Applications			
	1	Preferences			
ð	k	Debug			
			+ -	+ - 0	
		Back			

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

#### Adding or Removing Categories and Extensions



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

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

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

# 9.7 Apple Metadata Filters

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

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

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

		RECON L	AB-1.5.0 (A1)	
Examiner Details Artifacts			Search	
User Defined Extensions	DR	Title	Attribute	Description
💩 User Defined File Signature		Latitude	kMDItemLatitude	Latitude of the item.
E Keyword List		Longitude	kMDItemLongitude	Longitude of the item.
Text Indexing Filters		Where From	kMDItemWhereFroms	Describes where the item was obtained
🍙 Apple Metadata Filters		Date Added	kMDItemDateAdded	Added date of the item.
Exif Metadata Filters		Device Make	kMDItemAcquisitionMake	Manufacturer of the device used to acqu
Wolatility Path		Device Model	kMDItemAcquisitionModel	Model of the device used to acquire the
System Password		Title	kMDItemTitle	Title of the item.
		Kind	kMDItemKind	Description of the kind of item this file
		File Size	kMDItemFSSize	Size, in bytes, of the file on disk.
Preferences		File System File Name	kMDItemFSName	File Name of the item.
🐞 Debug		Created	kMDItemFSCreationDate	Date that the contents of the file were c
		Modified	kMDItemFSContentChangeDate	Date the file contents last changed.
		Duration	kMDItemDurationSeconds	The duration, in seconds, of the conten
		Name	kMDItemDisplayName	Localized version of the file name.
		Last Modified Date	kMDItemContentModificationDate	Date and time when the contents of this
		Created Date	kMDItemContentCreationDate	The date and time that the content was
		Comment	kMDItemComment	Comments about the item
		Album	kMDItemAlbum	Title for the collection containing this it
		Audio Dit Data	kMDItom Audio Dit Data	Dit rate of the audie in the modia
Back				

Apple Metadata Filter Column Descriptions

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

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

Title – The common name of the Apple Extended Attribute.

Attribute – The specific name of the Apple Extended Attribute.

**Description** – The official description of the Apple Extended Attribute.

### 9.8 EXIF Metadata Filters

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



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

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

**Title** – The common name of the EXIF Metadata.

**Description** – The official description of the Apple Extended Attribute.

### 9.9 Volatility Path

RECON LAB supports Volatility for RAM analysis. Volatility can be downloaded from <u>https://www.v</u> <u>olatilityfoundation.org/</u>

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

	RECON LAB-1.5.0 (AI)	
Examiner Details Artifacts	Please download the latest version of Volatility-Master, and point the tool towards the vol.py file	
User Defined Extensions	/Applications/Utilities/volatility3-1.0.0	
🛯 📠 User Defined File Signature		
i≣ Keyword List		
Text Indexing Filters		
Apple Metadata Filters		
Exif Metadata Filters		
www.VolatilityPath		
System Password		
External Applications		
Preferences		
₩ik Debug		
Back		

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

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

# 9.10 System Password

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

		RECON LAB-1.5.0 (A1)	
	Examiner Details	System Password	
	Artifacts		
EXT	User Defined Extensions		
	User Defined File Signature		
1	Keyword List		
1	Text Indexing Filters		
Ó	Apple Metadata Filters		
	Exif Metadata Filters		
-	Volatility Path		
	System Password		
	External Applications		
13	Preferences		
Ť	Debug		
-	Daale		
	васк		

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

# 9.11 External Applications

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

	-17		RECON L	AB-1.5.0 (A1)		
Examiner Details	Lis	t of Ex	xternal Applications			
Artifacts			Application		Path	
User Defined Extensions	1	🌒 F	ile Juicer.app	/Applications/File Juicer.app		
User Defined File Signature	2		OB Browser for SQLite.app	/Applications/DB Browser for SQLite.app		
i≣ Keyword List	3	🛃 P	Preview.app	/System/Applications/Preview.app		
Text Indexing Filters	4	⊿т	FextEdit.app	/System/Applications/TextEdit.app		
🍿 Apple Metadata Filters						
Exif Metadata Filters						
🗰 Volatility Path						
System Password						
External Applications						
Preferences						
🐞 Debug						
		Ac	dd			Remove
Back						

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

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

### 9.12 Highlight User Opened Files

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

	0	RECON LAB-1.5.0 (A1)	
2	Examiner Details Artifacts	✓ Highlight User Opened Files	
	User Defined Extensions User Defined File Signature Keyword List Text Indexing Filters Apple Metadata Filters Exif Metadata Filters Volatility Path	Minimum File size for Face Analysis is Minimum File size for Skin Tone Detection is Minimum File size for Optical Character Recognition is Minimum File size for Weapons is Minimum File size for Fire Analysis is Maximum File size for Ioading Text View is	КВ КВ КВ КВ КВ КВ КВ
	System Password External Applications Preferences		
Ð	: Debug		
	Back		

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

	*	Source	An_Mac (2023 Class Image.dmg) [Source	¢ ×		
3	() > ()	Show Column 🕑				Export As 😒
			Table View Gallery	View		
	Record No.	Inode No./File ID	File Name	Extension	🔼 File Size	Date Modified
	rch	Search	Search	Search	Search	Search
	82562	185102	Screen Shot 2022-06-26 at 9.59.21	png	40373	2022/06/26 11:59:26 -5:00
	82563	185097	IMG_0081.jpeg	jpeg	2546906	2022/06/21 10:30:12 -5:00
	82564	185095	.DS_Store		8196	2022/08/01 12:37:00 -5:00
	82565	185103	Screen Shot 2022-07-21 at 2.32.33	png	46854	2022/07/21 16:32:39 -5:00
	82566	185096	localized		0	2022/11/09 13:53:07 -5:00
	82567	185099	🔋 Its going to be mine.jpeg	jpeg	135704	2022/07/16 12:57:04 -5:00
2	82568	185104	Screen Shot 2022-07-21 at 6.51.40	png	46522	2022/07/21 20:51:46 -5:00
i.	82569	185100	Production Presentation alias		960	2022/07/02 18:36:24 -5:00
Ŕ,	82570	185098	IMG_0144.jpeg	jpeg	4160010	2022/07/19 11:41:13 -5:00
0	87571	185101	s progit pdf	ndf	18672492	2022/06/30 10:00:26 -5:00

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

# 9.13 Text View Settings

		RECON LAB-1.5.0 (A1)	
-	Examiner Details Artifacts	✓ Highlight User Opened Files	
	User Defined Extensions User Defined File Signature Keyword List Text Indexing Filters Apple Metadata Filters Exif Metadata Filters	Minimum File size for Face Analysis is         Minimum File size for Skin Tone Detection is         Minimum File size for Optical Character Recognition is         Minimum File size for Weapons is         Minimum File size for Fire Analysis is	КВ КВ КВ КВ КВ
	Volatility Path System Password External Applications Preferences	Maximum File size for loading Text View is	МВ
*	Debug		
	Back		

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

# 9.14 Debug Mode

	Configuration	
<ul> <li>User Defined Extensions</li> <li>User Defined File Signature</li> <li>Keyword List</li> <li>Text Indexing Filters</li> <li>Apple Metadata Filters</li> <li>Exif Metadata Filters</li> <li>Volatility Path</li> <li>System Password</li> <li>External Applications</li> <li>Time Zone</li> <li>Preferences</li> <li>Debug</li> </ul>	Configuration  Configuration	
		Apply

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

# **10. Starting A New Case**



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

### 10.1 Case Info

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



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

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

**Case Name** (mandatory) – Name for your case.

**Location** – Location of the incident or the exam.

Case Notes – free form to add any notes required.

Examiner (mandatory) – Examiner name.

**Examiner Phone** – Phone number for the examiner.

Examiner Email – Email for the examiner.

Agency – Agency name.

Agency Address – Address for the agency.

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

### **10.2 Adding Source Data to Process**

RECON LAB can accept a variety of sources to process.



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

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



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

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

Mobile Evidence- includes options for different mobile backups and extractions

Cloud Evidence- includes options for cloud production data

**Network Acquisition**- includes options for acquisitions done over a network

### **10.2.1 Physical Evidence**



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

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



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



10.2.1.1 Forensics Images

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

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



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

#### 10.2.1.1.1 Physical Images of macOS

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



From here, you can configure the image as needed.

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

Currently accepted formats are: **RAW Images** – .dd, .000, .00001, .raw **Apple Disk Images** – .dmg, .sparsebundle, .sparseimage **Expert Witness Format** (EWF) – .E01, .Ex01, .L01, .S01 **Advanced Forensic File Format** - AFF4

\*.dd \*.DD \*.E01 \*.e01 \*.dmg \*.DMG \*.sparsebundle \*.sparseimage \*.Ex01 \*.ex01 \*.501 \*.501 \*.000 \*.00001 \*.raw \*.RAW \*.vmdk \*101 \*L01 \*vhd \*VHD

Select your image and hit 'Open' to continue.

	Open			
Look in:	📘 /Users/chrisgrettenbersktop/Willia	m Campbell	0	0 0 🙉 🗉 🛙
Volum	Name ~	Size	Kind	Date Modified
	📄 William_Campbell_MacBook.dmg	113GiB	dmg File	4/15/2:02 AM
· ·	William_Campbell_MacBook_source.txt	957tes	txt File	4/15/2:57 AM
chrisg	William_Campbellook_complete.txt	1.85 KIB	txt File	12/17/:57 AM
o Down	Willam_Campbel_Wacsbor_case.txt	140165	CALTINE	4/13/237 AM
Deskt				
Docur				
_				
File name:	William_Campbell_MacBook.dmg			Open
Files of type:	*.dd *.DD *.E01 *.e01 *.dmg *.DMG *.spa	rsebundle *	.sparseima	ige *. 📀 🛛 Cancel

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

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

#### 10.2.1.1.2 Physical Images of Windows Machines

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



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

Select your image and hit 'Open' to continue.

	Open			
Look in:	📄 /Users/chrisgrettenbersktop/Willia	m Campbell	0	0 🖗 🗉 🗉
Volum	_ Name ~	Size	Kind	Date Modified
<b>—</b> ,	William_Campbell_MacBook.dmg	113GiB	dmg File	4/15/2:02 AM
	William_Campbell_MacBook_source.txt	957tes	txt File	4/15/2:57 AM
chrisg	William Campbell MacBook case tyt	1.65 KIB	txt File	4/15/2 ·57 AM
💽 Down	in whitehing composition action of the	140	CALLING	4/10/2
Deskt				
Docur				
File name:	William_Campbell_MacBook.dmg			Open
Files of type:	*.dd *.DD *.E01 *.e01 *.dmg *.DMG *.spa	rsebundle *	.sparseima	ige *.
_		_	_	

### <u>10.2.1.1.3 Physical Images of Other OS Machines</u>

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



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

Select your image and hit 'Open' to continue.

Look in:	📘 /Users/chrisgrettenbersktop/Willia	m Campbell	0	0 🖗 🗉
Volum	Name ~	Size	Kind	Date Modified
<b></b> ,	William_Campbell_MacBook.dmg	113GiB	dmg File	4/15/2:02 AM
	William_Campbell_MacBook_source.txt	1.95 Vip	txt File	4/15/2:57 AM
chrisg	William Campbell MacBook case.txt	143tes	txt File	4/15/2:57 AM
Down				
Deskt				
Docur				
File name:	William_Campbell_MacBook.dmg			Open
Files of turner	* dd * DD * F01 * a01 * dma * DMC * ana	rechundle *		
rifes of type.	".dd ".DD ".E01 ".e01 ".dmg ".DMG ".spa	rsebundle	.sparseima	
		-		

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

#### 10.2.1.2 Mounted Volumes

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

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

	Select	Image Typ	be	
୭		A A	RAM	Q
Forensics Image	Mounted Volumes	Optical Disc Image	RAM Image	RECON FS Block Image

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

/Volumes/BOOTCAMP		
/Volumes/DEST		
/Volumes/RECON LAB		
	Cancel	Add

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

### 10.2.1.3 Optical Disc Image

RECON LAB can support Optical Disc image formats as a source. RECON LAB currently supports .ISO and .cdr Optical Disc formats.



Select the 'Optical Disk Image' Icon under 'Select Image Type'.

	Select	Image Typ	De	
୭			RAM	Ð
Forensics Image	Mounted Volumes	Optical Disc Image	RAM Image	RECON FS Block Image

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

Select your image and click 'Open' to continue.

	open			
Look in:	Users/chrisgrettenbere/carbon-p	oaladin v8.05	0	0 闷 📰 🗉
Volum	Name	Size	Kind	Date Modified
	🚞 PALADIN Pro Update Guide	<u></u>	Folder	7/19/21 3:14 PM
	a carbon-paladin.iso	3.59 GiB	iso File	6/21/2:37 AM
🛅 chrisg	6-17-2021-HowALADIN-USB.pdf	649KiB	pdf File	7/27/21 3:09 PM
Down	DS_Store	6.00 KiB	DSile	12/21/:24 PM
Deskt				
Docur				
File name:	carbon-paladin.iso			Open
Files of type:	*.iso *.ISO *.cdr *.CDR			Cancel

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

### <u>10.2.1.4 RAM Image</u>

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

To load a RAM image, select the 'RAM Image' icon in the Physical Evidence 'Select Image Type'

	Select	Image Ty	pe	8
Forensics Image	Mounted Volumes	Optical Disc Image	RAM Image	RECON FS Block Imag

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



	Open			
Look in:	📄 /Users/chrisgrettenbersktop/Willia	m Campbell	0	0 闷 🔛 🛙
Volum	Name ~	Size	Kind	Date Modified
	William_Campbell_MacBook.dmg	113GiB	dmg File	4/15/2:02 AM
chrise	William Campbell_ook_complete_txt	1.85 KiB	txt File	4/15/257 AM
	William_Campbell_MacBook_case.txt	143tes	txt File	4/15/2:57 AM
Down				
Deskt				
Docur				
File name:	William_Campbell_MacBook.dmg			Open
Files of type	* dd * DD * F01 * e01 * dmg * DMC * sna	rsebundle *	snarseima	Ide * 🙆 Cancel
thes of type.		a seburiale	ispuiseinia	Cancer
		-	-	

Select your image and click 'Open' to continue.

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

### 10.2.1.5 RECON FS Block Image



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

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

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


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

Select your image and click 'Open' to continue.

	open			
Look in:	📄 /Users/chrisgrettenbersktop/Willia	m Campbell	0	0 闷 🗉 🗉
Volum	Name ~	Size	Kind	Date Modified
	William_Campbell_MacBook.dmg	113GiB	dmg File	4/15/2:02 AM
	William_Campbell_MacBook_source.txt	957tes	txt File	4/15/2:57 AM
chrisg	William Campbell MacBook case.txt	143tes	txt File	4/15/2:57 AM
Down				
Deskt				
Docur				
File name:	William_Campbell_MacBook.dmg			Open
Files of type:	*.dmg *DMG			Cancel

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

### 10.2.2 Logical Evidence

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

is not loaded properly.

	Select E	vidence T	Гуре	
6		C.	1	$\overline{\mathbf{+}}$
Physical Evidence	Logical Evidence	Mobile Evidence	Cloud Evidence	Network Acquisition

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



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

#### 10.2.2.1 Time Machine Backup



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

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



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

Look in:	/Volumes/Macbook 2012 Backup/Bacb	ackupdb/Steve's MacBook Pro (2) 📀	000 🖬 🗉 🗉
Volu	Name	A Size Kin	d Date Modified
-	2018-04-22-223306	Fol	der 4/22/1:33 PM
/ 🔤	2018-04-29-130655	Fol	der 4/29/1:06 PM
The macl	o 🖿 2018-06-25-160201	Fol	der 6/25/1:02 PM
Down	2018-06-25-162329	Fol	der 6/25/1:23 PM
Dow	2018-06-26-220733	Fol	der 6/26/1:07 PM
- Deal	Eatest	Fol	der 6/26/1:07 PM
Directory:	2018-06-25-160201		Choose
Files of type:	Directories		Cancel

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

#### 10.2.2.2 macOS Home Directory

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



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

0 0		RECON LAB	
$\bigotimes$			
Source Path	Select macOS Home Directory		()
Username	Type Username		
		Add	
Logical Evidence	> macOS Home Directory]		
and a matched	in the billectory i		

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

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

#### 10.2.2.3 RECON Logical Image

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



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

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

Selec	t Image Typ	be	
	Q		
Sparseimage	DMG	Folder	

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

Look in:	/Volumes/T7 2TBDest/William Camp	bell		0 0 🙉 🖬 🛙
Volum 🔁	Name ~	Size	Kind	Date Modified
	William_Campbell_MacBook.dmg	057 toc	amg File	4/15/2:02 AM
chrise	William Campbell ook complete txt	1.85 KiB	txt File	12/17/ 57 AM
Chrisg	William Campbell MacBook case.txt	143tes	txt File	4/15/2:57 AM
O Down				
Deskt				
Docur				
_				
File name:	William_Campbell_MacBook.dmg			Open
Files of turns	t dmg tDMC			Ganal
riles of type:				Cancel
		_	_	

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

### 10.2.2.4 Encase Logical Image

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

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



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

Selec	t Image Ty	/pe	
	LUI		

Select the L01 Icon.

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



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

#### 10.2.2.5 Logical Folder

Individual folders can be added as a source to process.



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

Look in:	/Users/macboy/Downloads		1	0	0	S 🗉 🗉
Volu	Name	.▲ Size		Kind	Date M	odified
-	1			Folder	10/6/1	:50 PM
<u> </u>	1.0.9.zip.download			Folder	11/15/	:54 PM
The maci	7.7M2 drivers not Support XP.zip.download			Folder	12/10/	:13 AM
	7.7M2 drivers£@not Support XP£©			Folder	3/27/1	:21 AM
Dow	📷 AmazonPhotos			Folder	8/27/1	14 PM
	and the second second second			F.14	A 194 1	20.000
Directory:	AmazonPhotos					Choose
Files of type:	Directories				0	Cancel

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

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

#### 10.2.2.6 Logical File

Individual files can be added as a source to process.



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

	Open				
Look in:	🚞 /Volumes/T7 2TBDest/William Camp	bell	0	0	:: =
Volum	Name ~	Size	Kind	Date Modified	d T
1	William_Campbell_MacBook.dmg	957tes	dmg File txt File	4/15/2:02	AM
chrisg	William_Campbellook_complete.txt	1.85 KiB	txt File	12/17/:57	AM
Down	William_Campbell_MacBook_case.txt	143tes	txt File	4/15/2:57	AM
🔲 Deskt					
Docur					
File name:	William_Campbell_MacBook_complete.txt				Open
Files of type:	*			٢	Cancel

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

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

#### **10.2.3 Mobile Evidence**

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



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

#### 10.2.3.1 iTunes iOS Backup

RECON LAB supports the analysis of Apple iOS backups.

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

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



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

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

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

#### 10.2.3.2 Cellebrite iOS Backup

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



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

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



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

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

#### 10.2.3.3 GrayKey Backup

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



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



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

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

#### 10.2.3.4 ADB Android Backup

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



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



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



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

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

### 10.2.4 Cloud Evidence

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



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

#### 10.2.4.1 Google Takeout

RECON LAB supports data downloaded from Google Takeout:<u>https://takeout.google.com</u> RECON LAB has numerous plugins to automate the analysis of Google Takeout data.



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



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

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

### 10.2.5 Network Acquisition

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



#### 10.2.5.1 RECON Mac Sharing Mode

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

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



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



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

### **10.3 Adding Source Information**

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

Evidence No.	001
Description :	RECON Logical image using RECON IMAGER to preserve original timestamps from a Mac with T2 Chipset running macOS 10.15.
	ОК

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

After entering the information click "Ok".

# **10.4 Adding Multiple Sources**

RECON LAB can process multiple sources at the same time.

	RECON LAB-1.5.0 (A1)
I Case Info	Add Source
	Forensics Image
	/Users/chrisgrettenberger/Desktop/William Campbell/William_Campbell_MacBook.dmg
	RECON FS Block Image
	/Volumes/T7 2T8Dest/POI iMac Sparseimage/POI_IMac_Sparseimage_Test.sparseimage
	Back Next

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

# 10.5 Case Directory

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

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



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

# 10.6 Date and Time Settings

RECON LAB has several options for setting time zones.

		RECON LAB-1.5.0 (A1)	
<ul> <li>Case Info</li> <li>Source</li> <li>Case Directory</li> </ul>			
O Date & Time			
	О итс	UTC +0000	
	Machine Time Zone	America/New_York-EST-GMT-5:00	
	Other Time Zone	<select time="" zone=""></select>	٥
	Date Format	yyyy-MMM-dd	0
_			Back Next

UTC – Coordinated Universal Time or +00:00

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

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

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

# **10.7 File System Modules Selection**

S Extract Apple Metadata	
Extract Apple Metadata	
Back	Next
	Back

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

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

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

### 10.7.1 Apple Metadata Module

Case Info	Filesystem Modules	d.														
Case Directory	Apple Metadata	Apple Metadata Extract Apple Metadata														
🔯 Date & Time	Signature Analysis		Search													
III File System		D	D	Title	Attribute											
	Exif Metadata			Latitude	kMDItem atitude	Latitude of the iter										
	Hashes	15		Longitude	kMDItemLongitude											
		12	Ξ.	Where From	kMDitemWhereFroms	Describes where t										
		12	Ξ.	Date Added	kMDItemDateAdded	Added date of the										
			-	Device Make	kMDItemAcquisitionMake	Manufacturer of th										
				Device Model	kMDItemAcquisitionModel	Model of the devic										
				Title	kMDItemTitle	Title of the item.										
				Kind	kMDItemKind	Description of the										
				File Size	kMDItemFSSize	Size, in bytes, of t										
				File System File Name	kMDItemFSName	File Name of the it										
				Created	kMDItemFSCreationDate	Date that the cont										
				Modified	kMDItemFSContentChangeDate	Date the file conte										
				Duration	kMDItemDurationSeconds	The duration, in se										
				Name	kMDItemDisplayName	Localized version										
				Last Modified Date	kMDItemContentModificationDate	Date and time whe										
					Back	Next										
			_		Juck											

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

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

#### **Apple Metadata Filter Column Descriptions**

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

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

**Title** – The common name of the Apple Extended Attribute.

Attribute – The specific name of the Apple Extended Attribute.

**Description** – The official description of the Apple Extended Attribute.



### 10.7.2 Signature Analysis Module

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

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

### 10.7.3 EXIF Metadata Module



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

#### **EXIF Metadata Filter Column Descriptions**

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

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

Title – The common name of the EXIF Metadata.

**Description** – The official description of the Apple Extended Attribute.

10.7.4 Hashes Module

Filesystem Modules																		
٩p	ole N	etad	ata	<b>A</b>	nalyse	Hashes												
gna	ature	Ana	lysi	5														
Exi	if Me	tada	ta															
	Has	hes																
				-														
													Back			1	Next	
											_			Back	Back	Back	Back	Back Next

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

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

# **10.8 Artifact Plugin Selection Module**

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

Select any plugins or artifacts that you want to run.



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

# 11. Reloading a Case

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



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

The naming structure of the folder will consist of the:

#### Case Name-YYYY-MTH-DYTHH-MM-SC

(i.e. Fraud\_Investigation\_2018-SEP-19T13-25-44)

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


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

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

# **12. RECON LAB Interface**



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

## **12.1 Processing Status Window**

RECON LAB will let you begin working in minutes.

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

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

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

reviewing the results.



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

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

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

-	Extracting Apple Timestamps					
0	0% Initializing APPLE SSD	×				

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

this is a sentence.

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



Finally, the Hashes module is run.

-	Hashes	
	60%	×
	APPLE SSD - Data (122000)	

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

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



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

## 12.2 Case View



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

Case Details	
Case No.: 1234	
Case Name : Person of Interest	
Location : SUMURI HQ	
Case Notes :	
Case Created Time : Jan-13-2022 14:26:42 +	00:00
Case Created Machine Timezone : America/N	ew_York-EST-GMT-5:00
Case Created Version : 1.5.0 (RECON LAB)	
Case Path : /Users/chrisgrettenberger/Deskto	p/Person_of_Interest_2022-Jan-13T09-26-42/
Examiner Details	
Examiner : Chris Grettenberger	
Examiner Phone: 302-570-0015	
Examiner Email : chris@sumuri.com	
Agency Name : SUMURI LLC.	
Agency Address : SUMURI LLC. P.O. Box 121 M	lagnolia, Delaware 19962 USA
Examiner Selected Time Zone : America/New	York-EST-GMT-5:00
Sources	
William_Campbell_MacBook.dmg	Source Details
MAPPLE SSD	Source Name : /William_Campbell_MacBook.dmg/APPLE SSD - Data Evidence No. : 001
	OS Type : macOS
Preboot	File System : aprs
	Product Type : MacBookAir7,2
Recovery	User(s) : williamcampbell
	OS Version : 11.0.1
E VM	OS Version : 11.0.1
	Country .
	City :
MAPPLE SSD - Data	
	System Time Zone :
Update	Description :
	Installer Date : Mar-19-2021 10:22:36 ±00:00
EFI	mstanet Date . Mai-13-2021 10.22.30 +00.00

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

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

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

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

## 12.3 Menu Options

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

## 12.3.1 Interface Top Menu

-	6	0	Ø	E	my		0	:=	-
1	2	3	4	5	6	7	8	9	10

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

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

## 12.3.2 macOS Menu Bar

## **É RECON\_LAB** Process Search Timeline Export Report

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

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

## 12.3.2.1 Process

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

- 1. **Run Artifacts** Calls the Artifacts and Plugins module for automated analysis.
- 2. **RAM Analysis** Opens the RAM Analysis module which is a GUI for Volatility and may include a "Carve Password" feature (vetted agencies only).

- 3. **Text Indexing** Allows the indexing of files and directories.
- 4. Hash Sets Allows creation or importing of hash sets.

## 12.3.2.2 Search

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

1. **File Search** – Allows for locating files based on a combination of timestamps, file names, extensions, file sizes and more.

- 2. **Content Search** Calls the Content Search configuration window to allow searching with keywords.
- 3. **EXIF Metadata Search** Allows the examiner to conduct a search using EXIF Metadata.
- 4. **Apple Metadata Search** Allows for locating files based on Apple Extended Metadata.
- 5. **Artifacts Keyword Search** Allows the examiner to conduct a single keyword search quickly within all recovered artifacts.
- 6. **Recognize Face** Allows the examiner to extract faces from a picture.

## 12.3.2.3 Timeline



The Timeline tab allows the following features to be accessed.

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

## 12.3.2.4 Export

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

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

## 12.3.2.5 Report

## 

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

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

## 12.4 Main Columns

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

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

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

#### <u>Sidebar Column</u>

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

## Select Category Column

<select category=""></select>	
Case:	
Artifacts	
Email Files	
Source	
Mobile Backup	
MIME Type	

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

## Select Feature Column

<select feature=""></select>	
Device Model (3)	

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

## 12.5 Case Sidebar



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

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

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

## 12.6 Main Viewer Window

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

Į.	0	Record No.	Inode No./File ID	File Name	Extension	File Path	File Size
1		1208592		.DS_Store		/Users/macboy/Downloads/.DS_Store	6148
2	22	1208593		localized		/Users/macboy/Downloads/.localized	0
3		1208594		DB.Browser.for.SQLite-3.11.2.dmg	dmg	/Users/macboy/Downloads/DB.Browser.for.SQLite-3.11.2.dmg	16857319
4		1208595		googlechrome.dmg	dmg	/Users/macboy/Downloads/googlechrome.dmg	80845370
5 🗌		1208596		iOS_iPadOS_13_Beta_Profile.mobileconfig	mobileco	/Users/macboy/Downloads/iOS_iPadOS_13_Beta_Profile.mobilec	7348
6		1208597		macOSDeveloperBetaAccessUtility.dmg	dmg	/Users/macboy/Downloads/macOSDeveloperBetaAccessUtility.d	92222

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

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

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

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

File Name – The name of the file.

**Extension** – The extension of the file.

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

File Size – Size of the file in bytes.

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

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

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

**MD5** – The calculated MD5 hash of a file.

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

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

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

**Date Modified** – Standard timestamp for Date Modified.

**Date Change** – Standard timestamp for Date Changed.

**Date Accessed** – Standard timestamp for Date Accessed.

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

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

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

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

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

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

## 12.6.1 Table View

#### 12.6.1.1 Recursive View

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

«	>			Source	\$×	CATALIN/	(CATALINA.sp	arseimage) 💠 🛛			
	«	$\sim$				Search	Filters	Show All		Export as CSV	
							Table View	Gallery View	()		
17		1 1	•	Record No.	Inode No./	/File ID	File	e Name	Extension	File Path	
1				1241500			Google Chro	me Brand.plist	plist	/Users/macboy/Library/Google/Goog	le Chrome
2				1241501			GoogleSoftw	areUpdate		/Users/macboy/Library/Google/Goog	leSoftware

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

<	🔇 📎 Source 😂 🗶 CATALINA (CATALINA.spars		seimage) 🗢 🛛							
					Search		Filters 🔽	Show All		Export as CSV
						I	Table View	Gallery View		
		0	Record No.	Inode No	o./File ID		File	e Name	Extension	File Path
1			1241500			9	Google Chro	me Brand.plist	plist	/Users/macboy/Library/Google/Google Chrom
2			1241501				GoogleSoftw	vareUpdate		/Users/macboy/Library/Google/GoogleSoftwa
3			1241502				Actives			/Users/macboy/Library/Google/GoogleSoftwa
4			1241503			9	CountingMe	trics.plist	plist	/Users/macboy/Library/Google/GoogleSoftwa
5			1241504				Crashes			/Users/macboy/Library/Google/GoogleSoftwa
6			1241505			6	completed			/Users/macboy/Library/Google/GoogleSoftwa
7			1241506				new			/Users/macboy/Library/Google/GoogleSoftwa
8		255	1241507				pending			/Users/macboy/Library/Google/GoogleSoftwa
9			1241508				settings.dat		dat	/Users/macboy/Library/Google/GoogleSoftwa
10			1241509				GoogleSoftw	vareUpdate.bundle	bundle	/Users/macboy/Library/Google/GoogleSoftwa
11			1241510				Contents			/Users/macboy/Library/Google/GoogleSoftwa
12			1241511				_CodeSignat	ture		/Users/macboy/Library/Google/GoogleSoftwa
13			1241512				CodeResour	ces		/Users/macboy/Library/Google/GoogleSoftwa

## <u>12.6.1.2 Export to CSV</u>

« »	1.	Source	\$ X			CAT	ALINA (CATALIN	Asparseimage) 🗢 🗴			
~ «			Se	arch	Filters	Show All				Export	as CSV
							Table V	ew Gallery View			
	•	Record No.	Inode No./File ID	>	Fi	ile Name	Extension	File Path	File Size	Mime Type	Hashset Name
1		1208592			.DS_Store			/Users/macboy/Downloads/.DS_Store	6148	application/octet-st	1
z 🗆		1208593			.localized			/Users/macboy/Downloads/.localized	0	application/x-zeros	
3		1208594			DB.Browser	r.for.SQLite-3.11.2.	dmg	/Users/macboy/Downloads/DB.Browser.for.SQLite-3.11.2.dmg	16857319	application/octet-st	
4 🗆		1208595			googlechro	ome.dmg	dmg	/Users/macboy/Downloads/googlechrome.dmg	80845370	application/x-bzip	3
5 🗌		1208596		0	iOS_iPadOS	_13_Beta_Profile.m.	mobileco	/Users/macboy/Downloads/iOS_IPadOS_13_Beta_Profile.mobilec	7348	application/octet-st	
6 🗌		1208597			macOSDeve	eloperBetaAccessUti	dmg	/Users/macboy/Downloads/macOSDeveloperBetaAccessUtility.d	92222	application/octet-st	

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

00		Export AS CSV	
O Screen Items	O Current Directory	Recursive	
File Name	Downloads File Listing		
/Users/macboy/	/Desktop		
		Export	

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

00			(COR)	enkowdos, Fille, Lb	stang.cov			Open with Number	•
Sr. No	Fie Name	File Path	File Size (Bytes)	File Size (Units)	Nime Tape	Histoire Name	ROS	SHAD	Date Hode
+	D6,Store	/Users/mackey/Downloods/ 2/6_Store	4148	6.03 KB	application/indet-stream		194577a7e30bdcc?after7s8502cs34c	d??fteb1400scmd909s33c1cf8040071121e07	2019/08/2
3	Socialized	/Users/mackey/Downloads/ Jacalized	4	0.8	application/s-terosize				3019/08/3
3	OB. Browser for SQLite-3.11.2 drug	/Users/macbay/Downloads/08.Browsector.SQ.Is+3.11.2.dvg	16857210	16.03 HG	application/octat-stream		+1x606660c46e8c10752070c7x964	\$127121a00x000x7b3acc4c6346h196h8a3a4ccb	2019/66/2
+	googlechrone.itrig	/Gean/mackey/Downloads/geoglectrome.strg	80845370	77.18.HB	application/s-bolp		7c11c1n8558bc8x1877bo401435b435	ecs2x117%dx25dca699416355c6061ae05c845	2019/08/2
5	105_Fad05_13_8eta_Profile.reals?ecor/lig	/Users/macboy/Downloads/305_PadD5_13_Beta_Profile.mobileconfig	7348	2.18 HB	application/adult-stream		3x80c27%2x929395391118345x0461f	d#74/3613x866x45x46618054293xd8x810/05175	2019/06/2
6	mac05DeveloperSetaAccessU6Ry.dmg	/Usam/mackey/Downloads/marOSDeveloperSetaAccessURIN, dmg	92222	90.05.68	application/locket obviant		c5x3#0225x1/0/731x94025x40488475	01284b0279:0685194e00147401:1:59850602a6	2019/08/0

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

#### 12.6.1.3 Table View Filter and Search

Table View includes a search feature with filters.

IMG_			Search Filters 💙 Show All		
					Files
	H	Record No.	File Name	File Size	Mime Type
86		261973	1MG_0001.JPG	1896240	image/jpeg
87		261974	MG_0002.JPG	2604768	image/jpeg
88		261975	MG_0003.JPG	2505426	image/jpeg
89		261976	MG_0004.JPG	1268382	image/jpeg
90		261977	MG_0005.JPG	1852262	image/jpeg
219		686545	MG_0001.JPG	1896240	image/jpeg
220		686546	MG_0002.JPG	2604768	image/jpeg

In the example above the keyword, "IMG\_" was entered. Clicking the "Search" button showed all files with "IMG\_" in the File Name.

To reset the view click the "Show All" button.

Record No. ✓ File Name File Size Mime Type Signature Name Signature Value Hashset Name MD5 SHA1 Date Modified Date Change Date Accessed Date Added **Content Creation Date** Content Modification Date Last Used Date Use Count Source Name File Path Decompression Status

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

#### 12.6.1.4 Navigation Buttons



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

## 12.6.2 Gallery View



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

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

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

## 12.7 Multimedia Preview Pane



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

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

## **12.8 Viewer Panes**

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

1	Detailed Information	B Hex View	T] Text View	S Strings	Exif Metadata	🐇 Apple Metadata	🏄 Maps

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

Hex View – Shows the file in Hex View.

Text View – Shows the file text view.

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

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

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

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

## 12.8.1 Detailed Information Pane

Source Name: /CATALINA.spar	seimage/CATALINA					
Record No.: 1353						
File Name: Google Chrome.app File Path: /Applications/Google	Chrome.app					
Inode No./File ID: File Size: Mime Type:						
Date Modified: 2019-Sep-17 1 Date Change: 2019-Sep-27 11 Date Accessed: 2019-Sep-27 1	8:21:54 GMT-4:00 :08:55 GMT-4:00 1:08:53 GMT-4:00					
Date Added(Apple): 2019-Sep- Content Creation Date(Apple): Content Modification Date(App Last Used Date(Apple): 2019-A	24 14:06:08 GMT-4:00 2019-Aug-06 00:29:55 le): 2019-Sep-17 22:21 ug-26 21:31:19 GMT-4	GMT-4:00 :54 GMT-4:00 :00				
Used Dates(Apple): 2019-Aug-23 04:00:00 GMT-4 2019-Aug-26 04:00:00 GMT-4	4:00 4:00					
Use Count: 3						
Tag: Red						
Examiner Notes: Browser used	by person of interest.					
Detailed Information	III Hex View	T] Text View	S Strings	Exif Metadata	🚯 Apple Metadata	🛓 Maps

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

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

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

## 12.8.2 Hex View Pane

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
000000000	ff	d8	ff	e0	00	10	4a	46	49	46	00	01	01	01	00	48	00	48	00	00	ff	e1	26	a7	45	78	69	66	00	00	4d	4d	
00000032	00	2a	00	00	00	08	00	0d	01	Of	00	02	00	00	00	12	00	00	00	aa	01	10	00	02	00	00	00	0c	00	00	00	bc	
00000064	01	12	00	03	00	00	00	01	00	01	00	00	01	1a	00	05	00	00	00	01	00	00	00	c8	01	1b	00	05	00	00	00	01	
00000096	00	00	00	d0	01	28	00	03	00	00	00	01	00	02	00	00	01	31	00	02	00	00	00	Of	00	00	00	d8	01	32	00	02	
000000128	00	00	00	14	00	00	00	e8	01	3b	00	02	00	00	00	0f	00	00	00	fc	02	13	00	03	00	00	00	01	00	01	00	00	
000000160	82	98	00	02	00	00	00	Of	00	00	01	0c	87	69	00	04	00	00	00	01	00	00	01	1c	88	25	00	04	00	00	00	01	·····
000000192	00	00	03	62	00	00	04	3c	4e	49	4b	4f	4e	20	43	41	52	50	4f	52	41	54	49	4f	4e	00	4e	49	4b	4f	4e	20	b <ni corporati="" kon="" kon<="" ni="" on.="" td=""></ni>
000000224	44	38	30	30	45	00	00	00	00	48	00	00	00	01	00	00	00	-48	00	00	00	01	41	70	65	72	74	75	72	65	20	33	D800E H H Aperture 3
000000256	2e	34	2e	35	00	00	32	30	31	32	3a	30	38	3a	30	38	20	31	34	3a	35	35	3a	33	30	00	4e	69	63	6f	6c	61	. 4. 5 2012: 08: 08 14: 55: 30. Ni col a
000000288	73	20	43	6f	72	6e	65	74	00	00	4e	69	63	6f	60	61	73	20	43	6f	72	6e	65	74	00	00	00	26	82	9a	00	05	s CornetNi collas Cornet&
000000320	00	00	00	01	00	00	02	ea	82	9d	00	05	00	00	00	01	00	00	02	f2	88	22	00	03	00	00	00	01	00	01	00	00	
00000352	88	27	00	03	00	00	00	01	00	c8	00	00	90	00	00	07	00	00	00	04	30	32	33	30	90	03	00	02	00	00	00	14	.*
000000384	00	00	02	fa	90	04	00	02	00	00	00	14	00	00	03	0e	91	01	00	07	00	00	00	04	01	02	03	00	92	01	00	0a	
000000416	00	00	00	01	00	00	03	22	92	02	00	05	00	00	00	01	00	00	03	2a	92	04	00	0a	00	00	00	01	00	00	03	32	
000000448	92	05	00	05	00	00	00	01	00	00	03	3a	92	07	00	03	00	00	00	01	00	05	00	00	92	08	00	03	00	00	00	01	******
000000480	00	00	00	00	92	09	00	03	00	00	00	01	00	10	00	00	92	0a	00	05	00	00	00	01	00	00	03	42	92	91	00	02	B
000000512	00	00	00	02	34	00	00	00	92	92	00	02	00	00	00	02	34	00	00	00	a0	00	00	07	00	00	00	04	30	31	30	30	4
000000544	aO	01	00	03	00	00	00	01	00	01	00	00	a0	02	00	04	00	00	00	01	00	00	0b	<b>b</b> 8	<b>06</b>	03	00	04	00	00	00	01	

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.

6	7	8	9	10	11	12	13	14	15	16	17	18	19
4a	46	49	-					-7	48	00	48	00	00
00	0d	01	1	ag Si	elect	eat	oytes	• •	12	00	00	00	aa
00	01	00	St	art I	Block	<		)	05	00	00	00	01
00	03	00	Er	nd B	lock			)	00	01	31	00	02
00	e8	01	C	ору				>	Se	lecte	ed By	vtes	1
00	Of	00	UU	UI	UC	8/	69	UC	Se	lecte	Abe	SCII	1
04	3c	4e	49	4b	4f	4e	20	43					_2

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

## 12.8.3 Text View Pane



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

The Text View pane also includes a quick search feature.

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

All instances of "adobe" are now highlighted in red.

## 12.8.4 Strings View Pane



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

The Strings View pane also includes a quick search feature.

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

All instances of "adobe" are now highlighted in red.

## 12.8.5 EXIF Metadata View Pane

Key			Value				
1	Model		iPhone X				
10	Make		Apple				
	DateTimeOriginal		2018:03:30 12:14:19				
10	MeteringMode		5				
6	BrightnessValue		8.45529				
10	FocalLenIn35mmFilm		52				
	LensMake		Apple				
15	FNumber		2.4				
E.	FocalLength		6				
i C	ShutterSpeedValue		7.70425				
	ApertureValue		2.52607				
15	SceneType		1				
i C	SceneCaptureType		0				
1 II	ColorSpace		65535				
	LensModel		iPhone X back dual came	ra 6mm f/2.4			
\$	Detailed Information	Hex View	T] Text View	S Strings	Exif Metadata	🚯 Apple Metadata	🍰 Maps

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

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

## 12.8.6 Apple Metadata View Pane

Attrib	bute			Value								
v iC	DS_IP	adO5_13_Beta_Profile.mobile	config									
	۲ (C	kMDItemWhereFroms		https://download.develope	r.appl	e.com/WWD0	_2019/10	OS_iPadOS_13_beta	Config	uration_Profile/iOS_iP	adOS_13_Beta_Prof	ile.mobileconfig
				https://developer.apple.co	m/do	wnload/						
		kMDItemDateAdded	1	2019-Aug-23 01:50:26 GM	IT-4:0	00						
		kMDItemKind		Configuration Profile								
		kMDItemDisplayName		OS_IPadOS_13_Beta_Profile	.mobi	leconfig						
		kMDltemContentModificati	ionDate	2019-Aug-23 01:50:25 G	IT-4:0	00						
		kMDItemContentCreationD	Date	2019-Aug-23 01:50:25 GM	T-4:0	00						
		kMDltemLastUsedDate	1	2019-Aug-23 18:22:02 G	IT-4:0	00						
		kMDItemContentType		com.apple.mobileconfig								
V	6E	kMDltemContentTypeTree		com.apple.mobileconfig								
				public.xml								
				public.text								
				public.data								
				public.item								
				public.content								
		kMDItemUseCount		6								
٧	• E	kMDItemUsedDates		2019-Aug-22 04:00:00 GM	AT-4:0	00						
				2019-Aug-23 04:00:00 G	IT-4:0	00						
.6		tailed information	Alana Manur	T Tout Man	c	Partners	0	Polf Manufactor	air.	Angle Metadata	A Marca	

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

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

## 12.8.7 Maps Preview Pane



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



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



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

# 13. Removing a Source

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

	Source No.	Source Name	Apple Metadata	Exif Metadata	Mime Type	Signature Analysi	Hashes	Verification	
1	Source1	/CATALINA.sparseimage/EFI	Not Supported						Remove
z	Source2	/CATALINA.sparseimage/CATALINA	Completed	Completed	Completed	Completed			Remove
3	Source3	/Takeout	Not Supported	Completed	Completed	Completed	. 🗆		Remove
4	Source4	/Jermyn_Image.dmg/Jermyn_01	Completed	Completed	Completed	Completed		<u>Verify</u>	Remove
	Refresh							Cancel	Start

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

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

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

# 14. Right-Click Options

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



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

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

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

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

**Remove Bookmarks** – Removes a file's bookmark.

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

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

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

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

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

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

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

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

Hide Seen Files – Hide files from the case marked as "Seen".

Mark as Seen – Mark files seen by the examiner.

Mark as Unseen – Remove the "Seen" tag.

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

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

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

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

**Remove Bookmarks** – Remove the bookmark tag.

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

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

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

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

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

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

#### RECON LAB-1.5.0 (A1) 🕎 🙆 🚫 💷 🔬 📮 🐻 🔆 Den with Preview @ Ø 5D1A4316-9DCF-4E93-88E8-F6120A4F7E1E.ipeg All Features 🔹 🔍 🐊 Artifacts . \* X G-Export HTML Keyword Search Time Lin 0 Tags 0 Report Face Analysis All Photos (7) Faces (0) E Face Search Projects (0) Slid Moments (4) Shared Albums (0) Memories (0) Search Suggestion Keyword (1) Record No. System Aco Cotical Character Recognition WhereFrom File Path Skin Tone Detection 1 11 1 williamcampa /Users/williamcampbell/Pictures/. 2 williamcampt /Users/williamcampbell/Pictures/ Weapons а. Fire Analysis 4 williamcampb /Users/williamcampbell/Pictures/... 📴 File Extensions 5 williamcampt /Users/williamcampbell/Pictures/... User Defined Extension 6 williamcamp /Users/williamcampbell/Pictures/ Image (44173) 7 7 williamcampa /Users/williamcampbell/Pictures/... Audio (7415) Video (13) Document (419) Torrent (29660) Apple Office (0) Libre Office (0) Quicken (88980) Plugin: Photos Category: All Photos User Defined File Signatures File Size Source Name: /William\_Campbell\_MacBook.dmg// 😨 Snapshots Record No.: 3 System Account: williamcampbell 🐔 Hashset File Name: 5D1A4316-9DCF-4E93-B8E8-F6120A4 File Complete Name: File Path: /Users/williamcampbell/Pictures/Photos File Size: 235.91 KB (241575 bytes) Email Files Artifacts Messenger Height: 1190 Width: 800 Messages (197) Apple Apps Favourite: NO Hidden: O Photo Sooth (1) Photos (43) Creator Bundle ID: com.apple.Photos Artifacts Keyword Search UID File Name: UID File Path: File Search Creation Date: 2021-Mar-31 18:39:45 - 5:00 Modification Date: 2021-Mar-31 18:39:45 - 5:00 Original File Creation Date: Exit Timestamp: Last Shared Date: Scene Analysis Timestamp: 2021-Mar-31 18:39 In Trash Date: Exif Metadata Search Content Search Artifacts Timeline Bucket File MIME Type: public.jpeg Import Complete: Is In Trash: RECON LAB IRISH WOLFHOUND SUMURI Orininal File Name: Irish wolfbound inc

# **15. Previewing Files**

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



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

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

# **16. Automated Analysis**

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

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



Select the artifacts of interest and click "Start".

#### 

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

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

l 🙆 🗘					Ø						M 🔟 🤇	• ≔
All Features 🖨	< >	Artifacts	\$×		G	oogle Chrome (1	69)		<b>‡</b> X			
	Keyword Sean	ch I [	Time Line	Search	Show All				🗌 🔂 Export	HTML 0	Tags	C Rep
Artifacts	History (80)	Downloads (2) To	opsites (0) Bo	ookmarks (0)	Search Items (19)	Logins (0)	Shortcuts (10)	Autofill (5)	Autofill Profiles (0)	Credit Cards (0)	Favicons (4	6) Search E
> Network		Respect Ma	Curtam Array	1	Tale		Maria Course		Last Mailand Data			1184
> System		Necora No.	system Account	nadeae colored	inte ula 2021 - Casala i	an art	visit couri	3 303	Last visited Date	here a file		UNL
> Apple Apps	2	1	williamcamp	San Diago Pa	dres Schedule   San	Diena Padrer		1 202	1/03/31 17:20:13 -5:00	https://ww	w.googe.com	ly searchir
<ul> <li>Web Browsers</li> </ul>	2 -	2	williamcamp	San Diego Pa	ures Schedule   San	Diego Padres		1 202	1/03/31 17:14:38 -3:00	https://ww	/w.mib.com/p	adres/schedu
Brave Browser (170)	s	3	williamcamp	San Diego Pa	ores scriedule   san	Diego Padres		3 202	1/04/01 10:02:59 -5:00	nups://ww	/w.mib.com/p	adres/scriedu
Google Chrome (169)	4 <b>-</b>	1	williamcamp	Tickets   San	Diego Padres vs. An	izona		2 202	1/03/31 17:17:46 -5:00	https://ww	/w.ticketmaste	er.com/event/
5 Safari (909)	· ·	3	williamcamp	lickets   san	Diego Padres vs. An	izona		2 202	1/04/01 10:02:45 -5:00	https://ww	w.ticketmaste	er.com/event/
> Native Apps	b	6	williamcamp	world series .	2021 - Google Searc	in		3 202.	1/04/01 10:02:27 -5:00	https://ww	w.google.com	n/search?
> FTP Client	-	/	williamcamp	world series .	2021 dates - Googie	e Search		3 202	1/03/31 17:27:45 -5:00	https://ww	w.google.com	n/search?
Apple Long		8	williamcamp	world series .	2021 dates - Googie	Search		1 202	1/03/31 17:27:17 -5:00	https://ww	/w.google.com	n/search/
Apple Logs	9	9	williamcamp	Official San D	iego Padres Website	MLB.com		2 202.	L/04/01 10:17:02 -5:00	https://ww	w.mlb.com/p	adres/
Email Artifacts	10	10	williamcamp	Padres Email	Newsletters   San Di	iego Padres		1 202	L/04/01 10:17:24 -5:00	https://ww	w.mlb.com/p	adres/fans/r
Messenger	11	11	williamcamp	Register for P	adres Newsletters	San Diego		2 202	1/04/01 10:23:59 -5:00	https://ww	vw.mlb.com/p	adres/fans/r
Advanced Analysis	12	12	williamcamp	Login   MLB.c	om			1 202	1/04/01 10:20:09 -5:00	https://ww	vw.mlb.com/lo	ogin?redirecti
> Microsoft Office	13	13	williamcamp	Registration	MLB.com			1 202.	L/04/01 10:20:13 -5:00	https://ww	vw.mlb.com/re	egistration?re
> Media Player	14	14	williamcamp	Profile   MLB.	com			1 202	L/04/01 10:24:34 -5:00	https://ww	vw.mib.com/a	ccount/favor
Artifacts Keyword Search	15	15	williamcamp	Profile   MLB.	com			1 202	1/04/01 10:28:22 -5:00	https://ww	vw.mib.com/a	ccount/secu
Eile Search	16	16	williamcamp	Profile   MLB.	com			1 202	1/04/01 10:28:22 -5:00	https://ww	vw.mlb.com/a	ccount/subs
Evif Metadata Search	17	17	williamcamp	MLB.TV Welco	ome Center   MLB.co	m		1 2021	L/04/01 10:28:30 -5:00	http://mlt	).tv/	
Content Search	18	18	williamcamp	MLB.TV Welco	ome Center   MLB.co	m		1 202	1/04/01 10:28:30 -5:00	https://ww	vw.mlb.com/tv	v?affiliateId=
- Content Search	19 🔳	19	williamcamp	Follow D-bac	ks at Padres game F	REE with MLB		1 202	1/04/01 10:28:37 -5:00	https://ww	ww.mlb.com/g	ameday/634
Artifacts Timeline	20	20	williamcamp	Follow D-bac	ks at Padres game F	REE with MLB		1 202	L/04/01 10:28:37 -5:00	https://ww	vw.mlb.com/g	ameday/d-b
Bucket	21 🔳	21	williamcamp	Follow D-bac	ks at Padres game F	REE with MLB		2 202	L/04/01 10:28:38 -5:00	https://ww	vw.mlb.com/g	ameday/d-b
🚔 Tags	22 🔳	22	williamcamp	Follow D-bac	ks at Padres game F	REE with MLB		4 202	L/04/01 10:28:39 -5:00	https://ww	ww.mlb.com/g	ameday/d-b
Notes	23 🔳	23	williamcamp	Follow D-bac	ks at Padres game F	REE with MLB		62 202	1/04/01 13:20:33 -5:00	https://ww	ww.mlb.com/g	ameday/d-b
Redefined Result	24	24	williamcamp	Yu Darvish St	ats, Fantasy & News	MLB.com		1 202	L/04/01 10:29:13 -5:00	https://ww	ww.mlb.com/p	layer/50643
Saved Redefined Result	25 🗆	25	williamcamp	Yu Darvish St	ats, Fantasy & News	MLB.com		1 202	L/04/01 10:29:13 -5:00	https://ww	vw.mib.com/p	layer/yu-dar
	26	26	williamcamp	Yu Darvish na	amed Opening Day s	starter		1 202	L/04/01 10:32:45 -5:00	https://ww	vw.mlb.com/n	ews/yu-darv
	27 🗌	27	williamcamp	google drive	for macos - Google	Search		2 202	1/04/02 15:09:38 -5:00	https://ww	vw.google.com	n/search?
RECON	28	28	williamcamp	Download - 0	Google Drive			1 202	L/04/02 15:09:39 -5:00	https://ww	vw.google.com	n/intl/en_mu
LAB	29	29	williamcamp	Google Drive	on the App Store			2 202	L/04/02 15:10:11 -5:00	https://ap	ps.apple.com/	/app/google-
	30	30	williamcamp	majors 2021	schedule – Google S	search		2 202	1/04/05 17:35:00 -5:00	https://ww	vw.google.com	n/search7
SUMURI	31	31	williamcamp	washington n	ationals games 202	1 - Google		3 202	L/04/05 17:40:33 -5:00	https://ww	vw.aooale.com	n/search?

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

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

#### Filtering Data with Keyword Searches

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

Google S	earch	0	Time Line	Search	Show	All						Export	HTML	Tags	0	Report
History	Downloads	Topsites	Bookmarks	Search Items	Logins	Shortcuts	Autofill	Autofill Profiles	Credit Cards	Favicons	Search Engin	es Extensions	Synced Data	Cookies	Chrome	Settings
	R	Record No.	System Account		Titl	e		Visit Count	L	st Visited Da	ite		URL			
1		100	jermyn	vacation pdf - 0	Google Sea	rch			1 2013/03/0	6 16:24:08 0	MT-4:00 ht	tps://www.googl	e.com/search?q=v	acation+pd	t	
2		109	jermyn	sig sauer - Goo	gle Search				1 2013/03/0	7 14:09:07 0	MT-4:00 ht	tps://www.googl	e.com/search?q=s	ig+sauer&a	q	
3		116	jermyn	shipping to japa	an – Googl	e Search			1 2013/03/0	9 08:56:47 0	MT-4:00 ht	tps://www.googl	e.com/search?q=s	hipping+to-	H	

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

#### <u>Setting a Timeline to Filter Data</u>

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

Start Time	2013/03/01 05:00
End Time	2013/03/18 19:35
Lind Time	2013/03/10 13:331
	📷 Set

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

sig		0	Time Line	Search	Show	All					(	G• Export	HTML [	Tags	0	Report
History	Downloads	Topsites	Bookmarks	Search Items	Logins	Shortcuts	Autofill	Autofill Profiles	Credit Cards	Favicons	Search Engine	s Extensions	Synced Data	Cookies	Chrome	Settings 🕨
	R	Record No.	System Account		Tit	e		Visit Count	La	st Visited Da	ate		URL			
1		121	jermyn	International Bu	siness Pra	ctices - Goog	e Books		1 2013/03/1	1 12:41:12 0	MT-4:00 http	://books.googl	e.com/books?id=P	Rjv7o9KGQ	0	
2		122	jermyn						1 2013/03/1	1 12:41:12 0	MT-4:00 http	://books.googl	e.com/books?id=F	RJv7o9KGQ	0	
3		112	jermyn	Sig P226 Suppr	essed? - A	R15.Com Arch	ive		3 2013/03/0	7 14:11:59 0	MT-4:00 http	s://www.google	e.com/search?q=s	g+226+su	D	
4		115	jermyn	Sig P226 Suppr	essed? - A	R15.Com Arch	ive		1 2013/03/0	7 14:11:59 0	MT-4:00 http	.//www.ar15.co	m/archive/topic.h	tml?b=6&f		
5		113	jermyn	P226 Suppress	or Series				2 2013/03/03	7 14:10:53 0	MT-4:00 http	s://www.google	.com/search?q-s	g+226+su	<b>.</b>	
6		114	jermyn	P226 Suppress	or Series				1 2013/03/0	7 14:10:53 0	MT-4:00 http	://www.sigsaue	r.com/CatalogPro	ductDetails	p	
7		111	jermyn	Firearms Acces	sories				1 2013/03/0	7 14:10:02 0	MT-4:00 http	://www.sigsaue	r.com/StoreProdu	tList/firear		
8		110	jermyn						1 2013/03/0	7 14:09:08 0	MT-4:00 http	://www.sigsaue	r.com/			
9		109	jermyn	sig sauer - Goo	gle Search				1 2013/03/03	7 14:09:07 0	MT-4:00 http	s://www.google	e.com/search?q=s	g+sauer&a	<b>q</b>	
10		85	jermyn	Free Travel Gui	des   Free	Travel Brochu	res   Vis		1 2013/03/0	6 15:47:57 0	GMT-4:00 http	://www.google	.com/aclk?sa=L&a	=C194XaZ	)	

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

#### <u>Generating Reports from Plugin Window</u>

0	G• Export	V HTML	0	Tags	\$	Report	
es	Extensio	CSV	:a	Cookies	Chrome	Settingse	•
		KML					

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)

	🗗 Export	HTML 📀	✓ Tags	Report	
			Full		
es	Extension	s Synced Data	Screen Items	ne Settingse	

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.

Contents	Goog	le Chrome							
History	-								
Topoites									
Bookmarks									
Search Items									
Logina .									
Autofili Autofili Profiles									
	Histo	rv							
Envicona	111300								
Search Engines	The second second		Top						
Extensions	Sr. No.	History Detail							
Synced Data	1	Source Name : /CATALINA.sparseimage/CATALINA							
Chrome Settings		Record No. : 1							
Persona		System Account : macboy							
Session		Wildow Flow Inc. Workshold Associate							
	8	Finde 1 sign in - Google Accounts							
		Visit Count : 3							
		Last Visited Date : 2019-Aug-23-09:28:31 CMT-4:00							
		URL: https://accounts.google.com/signin/chrome/sync?ssp=1&continue=https%3AN2F%2Fwww.google.com%2F							
		Typed Count : 0							
		Person Name : Person 1							
		Person Source Folder : Default							
		Hidden : NO							
		Artifacts Source : /Users/macboy/Library/Application Support/Google/Chrome/Default/History							
		OS Scheme : macOS							

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.

	Д.	<ul> <li>Record No.</li> </ul>	Inode No./File ID	File Name	Extension
6		61145	718630	📄 Bitcoin Research	
7		61145	606983	🔲 Black Mail & More	
8		61145	606986	Booklet_FinancialTruth_Spread	pdf
9		☐ 61146	606987	Gell_Phone_technology.pdf	pdf
10		61146	606988	GGAP-Focus-Note-Nonbank-E	pdf
11		61146	606989	B E-money-+Niche+market+tha	pdf

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

## 17.2 Tags

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

MagicSp+	Suita cumbian Ac O		/Users/jermyn/Documen		
Microso	Bookmark Remove Bookmarks		/Users/jermyn/Documen		
NNEDV_			/Users/jermyn/Documen		
Parallels	Add Note Remove Note		/Users/jermyn/Documen /Users/jermyn/Documen /Users/jermyn/Documen /Users/jermyn/Documen		
📄 Persona	Remove Note				
Present:	Quick Look				
🗟 RepTyp	Send To Bucket				
📄 Russia	Export	-	/Users/jermyn/Documen		
Secure Secure	Add To Text Indexing Queue		/Users/jermyn/Documen		
E Shippin	Carve Files Carve Data		/Users/jermyn/Documen		
📄 Side Bu	Carve Data		/Users/jermyn/Documen		
📄 Spreads	Add file to hashset database	•	/Users/jermyn/Documen		
📄 Vacation	Tags	5	······································		
Yemen	Run Filesystem Modules Export Hashes As VIC	A A	Create New Tag     O     Remove Tag		
	Open Detailed Information Open with External Application Copy to Clipboard Mark As Seen Mark As Unseen		<ul> <li>Red</li> <li>Blue</li> <li>Yellow</li> <li>Green</li> </ul>		
_0s_9.pdf	Hide Seen Files Show Seen Files				
	Decompress File				

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".
Spy_Software		
Fuchsia		٢
	Save	
_	Save	_

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

	Create Tags	
Spy_Software		
Fuchsia		
	Save	

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

### 17.3 Finding Tags and Bookmarks in Sidebar



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

### 17.3.1 Exporting Tags

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

		Search	Show All			Export As	
Tag Search							
	Record No.	Plugin	TAB Name	Item 1	Item 2		
	4	Brave Browser	History	CMC Zoo   Cape May County, NJ	2020-Jul-22 09:48:44	-4:00	
	105	Brave Browser	History	tv girl album cover – Google Search	2020-Jul-31 12:53:33	-4:00	
	104	Brave Browser	History	how to disable applications on	2020-Jul-28 16:04:09	-4:00	
	125	Brave Browser	History	whatsapp dekstop macos - Googl	2020-Aug-06 09:26:4	0 -4:00	

## **17.5 Removing Tags and Bookmarks**

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

# 18. Indexing

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

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

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

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

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

#### **Indexing Example with RECON LAB**

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

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

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

<b>•</b> •		Configuration	
User Defined Extensions	🔿 No Filter 🧿 Index these	e files 🔘 Do not Index these files	
E Keyword List	Category		Extensions
Text Indexing Filters	Documents	.emix	
🍿 Apple Metadata Filters	Virtual Disk	.mbox	
Exif Metadata Filters	Apple Disk Images	.emi	
w Volatility Path	Mail		
🖳 System Password			
External Applications			
🔞 Time Zone			
🗔 Preferences			
🐞 Debug			
	+	+ - 0	
			Apply

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".

Record No.	Inode No./File ID		File Name	Extension
617115	635069	Logs		
617130	610182	Mail		
618048	610994	Mess	Bookmark Bomovo Bookmarks	
618118	611054	Meta	Kemove bookmarks	
618119	611055	Mobi	Add Note	
618306	611128	Mozi	Kemove Note	
618308	689272	Paral	Quick Look	
618401	611130	Prefe	Open With	
618402	611131	Prefe	Export	
618747	611449	Print	Add To Text Indexing Que	ue

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

Show Processed Eller			
File Path	Status		Source Name
/Users/jermyn/Library/Mail	Not Processed	Jermyn_01	
/Users/macboy/Library/Mail	Not Processed	CATALINA	
Remove			Start Indexing

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".

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

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

Steve Whalen April 18, 2011 at 5:07:00 AM EDT To: Timothy Craig

No sleep again! Give me a call if you get this before 0600.

Steve Whalen, CFCE Managing Director, SUMURI www.sumuri.com

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

# **19. Search Options**

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

#### Local Search Options

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

#### **Global Search Options**

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

### **19.1 Artifacts Keyword Search**

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

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

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

Keywords bitcoin							
	Select All	٢	Plugin	Sear	ch		
All Plugins	Plugins		<b>(</b>	105	4	•	
macOS Plugins		Airport WirelessNetwork			0		
Advanced Analysis	>∎ ₽	Apple Dock					
Apple Apps	2	Apple Installed Applications		0			
Apple Logs	> 🔳 🏨	Apple Mail Extractor					
Email Artifacts	> 🔳 🔳	Bash History					
ETP Client	> 🔳 😮	Bluetooth			0		
Media Plaver	> 🔳 😳	Brave Browser					
Messenger	> 🔳 📩	Calendar			0		
Microsoft Office	2 🔳 🔌	Connected iOS Devices					
Native Anns	> 🖬 📕	Contacts					
Network	> 🔳 🕹	Cyberduck					
System	i > 🔳 🔒	Escalate Privileges					
An and an							
Search Name Search for B	itcoin Evidence						
		Start					
				-	_		

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

#### apples,oranges,bananas

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

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



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

« »	Artifacts Keyword Search 😩 🕅		Search for Bitcoin	Evidence 🗘	×	
						Searched Keywords
				Items		
	Record No. Plugin	Category	Timestamp	Item 1	Item 2	Keyword Hit
267	2201 Safari	Cache	2013/04/30 15:01:12 GMT-4	http://www.google.com/uri?sa=t&rct=j&q=&esrc	-1276759687	bitcoin
268	2202 Safari	Cache	2013/04/30 15:01 13 GMT-4	http://www.wired.com/images_blogs/threatlevel/	-457889945	bitcoin
269	2216 Safari	Cache	2013/04/30 15:10:41 GMT-4	http://www.google-analytics.com/utm.gif?utm	2014648638	bitcoin
270	2225 Safari	Cache	2013/04/30 15:10:41 GMT-4	http://search.twitter.com/search.json?&q=#bitcoi	-2014677305	bitcoin
271	2227 Safari	Cache	2013/04/30 15:10:41 GMT-4	http://www.weusecoins.com/en/gx/icon_bitcoin	-1373841041	bitcoin
272	2512 Safari	Cache	2013/04/30 15:24:20 GMT-4	http://www.google-analytics.com/_utm.gif?utm	334780854	bitcoin
273	2647 Safari	Cache	2013/04/30 18:31:15 GMT-4	http://www.google-analytics.com/_utm.gif?utm	2144439858	bitcoin
274	2649 Safari	Cache	2013/04/30 18:31:15 GMT-4	http://search.twitter.com/search.json?&q=#bitcoi	1397185848	bitcoin
275	2668 Safari	Cache	2013/04/30 18:39:15 GMT-4	http://www.google-analytics.com/_utm.gif?utm	934402780	bitcoin
276	2781 Safari	Cache	2013/06/07 10:26:07 GMT-4	http://www.google-analytics.com/_utm.gif?utm	1486910859	bitcoin
277 🗌	2784 Safari	Cache	2013/06/07 10:26:08 GMT-4	http://search.twitter.com/search.json?&q=#bitcoi	-970790794	bitcoin
278	2 Safari	URLs		https://www.google.com/search?client=safari&rls	https://www.google.com/favicon.ico	bitcoin
279	16 Safari	URLs		http://www.tilecool.com/post/9635180215/avoi	http://24.media.tumblr.com/avatar_757	bitcoin
280	17 Safari	URLs		https://walletbit.com/connect/IntroductiontoBitc	https://walletbit.com/favicon.ico	bitcoin
281	27 Skype	Messages	2013/02/21 20:25:58 GMT-4	alfred.jermyn	I found this thing called Bitcoin- some s	bitcoin
282	14 Spotlight Settings	Shortcuts	2013/02/13 12:38 28 GMT-4	Bitcoin-Qt.app	bit	bitcoin
283	3 Trash RecycleBin	ltems		bitcoin paper alias		bitcoin
284	4 Trash RecycleBin	ltems		bitcoin paper.pdf		bitcoin
285	5 Trash RecycleBin	ltems		Bitcoin Tax Evaders : Bitcoin alias		bitcoin
286	6 Trash RecycleBin	ltems		Bitcoin Tax Evaders : Bitcoin alias 2		bitcoin
287	7 Trash RecycleBin	ltems		Bitcoin Tax Evaders : Bitcoin.pdf		bitcoin
288	8 Trash RecycleBin	Items		Bitcoin-FBI alias		bitcoin
289	9 Trash RecycleBin	Items		Bitcoin–FBI.pdf		bitcoin
290	16 Trash RecycleBin	ltems		IntroductiontoBitcoinMiningDavidRSterry alias		bitcein
291	17 Trash RecycleBin	ltems		IntroductiontoBitcoinMiningDavidRSterry.pdf		bitcoin
Chatname: #s	amaxemerc1/Salfred.jermyn;1cd5462382b6	307a				
Dialog Partne	r: samaxemerc1					
Message: I for	und this thing called <mark>Bitcoin</mark> - some sort of de	centralized banking p	program- anonymous too!			
Timestamp: 2	013-Feb-21 20:25:58 GMT-4:00				No Preview A	vailable
Artifacts Sour	ce: /Users/jermyn/Library/Application Suppo	ort/Skype/alfred.jermy	vn/main.db			
Tag:						
Examiner Not	es:					
Detailer	d Information 👔 Hex View	T] Text View	S Strings 🔛 Exif Meta	idata 🔹 Apple Metadata 🛛 👗 Maps	Preview	

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

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

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



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

### 19.2 File Search

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

. . . **File Search** File Name TrueCrypt Contains 0 Category File Size Greater than 0 Bytes C OCR Text 29/12/2018 11:00:00 ~ Date Change Between < > Date Modified \$ 30/12/2017 11:00:00 0 29/12/2018 11:00:00 Between \$ 29/12/2018 11:00:00 30/12/2017 11:00:00 Date Accessed Between 29/12/2018 11:00:00 Date Created Between. 30/12/2017 11:00:00 \$ \$ 29/12/2018 11:00:00 Date Added Between 30/12/2017 11:00:00 C 30/12/2017 11:00:00 C 29/12/2018 11:00:00 ( Date Content Creation Between ♀ 30/12/2017 11:00:00 ♀ 29/12/2018 11:00:00 ♀ (i) Date Content Modification Between 30/12/2017 11:00:00 29/12/2018 11:00:00 0 🇯 Date Last Used Between O All Source Select Source 🛃 Select O All Filters Any Filter TrueCrypt File Search Search

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

The File Search configuration window will appear.

File Name	TrueCrypt	✓ Contains
File Size	Greater than	Matches Starts with Ends with

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

File Size Greater than	1 🗘					✓ Bytes	0
-						KB MB	
Date Change	Between	0	01/01/2018 1:30:00	0	31/12/2018	GB	\$

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



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

Date Change	Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
Date Modified	Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
Date Accessed	Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
Date Created	Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
🗌 🍎 Date Added	Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
🗌 🍎 Date Content Creation	Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
🗌 🍎 Date Content Modificati	on Between	0	30/12/2017 11:00:00	0	29/12/2018 11:00:00	0
🗌 🍵 Date Last Used	Between	0	30/12/2017 11:00:00	< >	29/12/2018 11:00:00	0

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

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

• All Source • Select Source	≣ Select	
• All Filters • Any Filter		
TrueCrypt File Search		Search

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

D	All				
		Source	Source Name		
1		Source1	/CATALINA.sparseimage/EFI		
2		Source2	/CATALINA.sparseimage/CATALINA		
3		Source3	/Takeout		
4	$\checkmark$	Source4	/Jermyn_Image.dmg/Jermyn_01		
				cancel	OK

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

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



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



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

	 Record No.		File Name	File Size	Mime Type	Extension
1	261203	9	TrueCrypt.app			app
2	261207		TrueCrypt	10941620	application/x-java	
3	261213		TrueCrypt User Guide.pdf	923969	application/pdf	pdf
4	261214	19	TrueCrypt.icns	60982	image/x-icns	icns
5	384653		org.TrueCryptFoundation.TrueCrypt.bom	35763	application/octet-st	bom
6	384654	康	org.TrueCryptFoundation.TrueCrypt.plist	260	application/octet-st	plist
7	612364		TrueCrypt 7.1a Mac OS X.dmg	9526318	application/x-bzip	dmg
8	614283		TrueCrypt			
9	615545		http:%2F%2Fwww.google.com%2Fsearch?client=safari&rls=en&	169	application/octet-st	webhistory
10	615685		http:%2F%2Fwww.truecrypt.org%2F.webhistory	197	application/octet-st	webhistory
11	615686		http:%2F%2Fwww.truecrypt.org%2Fdownloads.webhistory	218	application/octet-st	webhistory
12	618734		org.TrueCryptFoundation.TrueCrypt.plist	353	application/octet-st	plist
13	618975		org.TrueCryptFoundation.TrueCrypt.savedState			savedState

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

### **19.3 Content Search**

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

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

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

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

dtSearch's Quick Reference Guide can be found here: <u>http://support.dtsearch.com/Support/form</u> <u>s/iframes\_advanced/default.html</u>

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.

	Category		_	Keyword					
Identity	Theft		SUMURI						
Phone N	umbers								
SUMURI	Investigatio	m							
						1			
+	-	/	+	-					
Search for the	Keyword S	IMURI					Cancel	Start	
search for the	Keyword 3	OMORI					Cancer	Juli	

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

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

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

## 19.4 Apple Metadata Search

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

Before using this feature make sure that you have:

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

Ś	RECON_LAB	Process	Search	Timeline	Export	Report
			File Searc	ch		
			Content S	Search		
			Exif Meta	data Search	n	
			Apple Me	etadata Seai	rch	
			Artifacts	Keyword Se	earch	
			Recogniz	e Face		

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

Device Make Contain C LG - + Device Model Ratches C VM670 - +	Apple Metadata					
Device Model  matches VM670 +  All Filters Any Filter iearch Label Photo Search Cancel Search	Device Make	😋 contain	0	LG		- +
All Filters Any Filter iearch Label Photo Search Cancel Search	Device Model	matches	0	VM670		- +
Search Label Photo Search Cancel Search		ny Filter			Const.	<b>C (</b> 1)
	All Filters A				Cancel	Search

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

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

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

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

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

		Files	Gallery View			
	Record No.	File Name	File Size	Mime Type	Extension	Hashset Name
1	612378 🚊	2012-08-26 12.02.24.jpg	726622	image/jpeg	jpg	
2	612379 🚊	2012-08-26 12.09.03.jpg	788715	image/jpeg	jpg	
3	612380 😤	2012-08-26 12.34.38.jpg	964273	image/jpeg	jpg	
4	612381 🚊	2012-08-26 12.34.45.jpg	867309	image/jpeg	jpg	
5	612382	2012-08-26 12.52.44.jpg	1040153	image/jpeg	jpg	
6	612383	2012-08-26 12.57.12.jpg	980533	image/jpeg	ipg	
7	612384 🔮	2012-08-26 12.57.34.jpg	999564	image/jpeg	jpg	
8	612385	2012-08-26 14.44.38.jpg	897284	image/jpeg	jpg	
9	612386 👼	2012-08-26 14.52.01.jpg	880673	image/jpeg	jpg	
10	612387 🖷	2012-08-26 14.54.33.jpg	874261	image/jpeg	jpg	
11	612388 🖷	2012-08-26 14.58.58.jpg	954659	image/jpeg	jpg	
12	612389	2012-08-26 14.59.05.jpg	930774	image/jpeg	jpg	
13	612390 🖷	2012-08-26 14.59.13.jpg	879356	image/jpeg	jpg	
				0.000 TO 000 TO 100		
Attribute		Value		1		
	kMDItemPixelCount	3.14573e+6		3. 3	Sec. Sec.	
	kMDItemOrientation	1		1000	New Sector	
	kMDItemResolutionWidthDPI	72		4 6 2	AND IN COLUMN	
	kMDItemBitsPerSample	32		3199		
E.	kMDItemResolutionHeightDPI	72		Post- Part		
	kMDItemHasAlphaChannel	0				The second second
1	kMDItemColorSpace	RGB			And	1
	kMDItemPixelWidth	1536		and.		
	kMDltemPixelHeight	2048			ALC: NO	
	kMDItemLogicalSize	980533		1991.0	2 A A	
	kMDItemProfileName	sRGB IEC61966-2.1		1	-	
	kMDItemEXIFVersion	2.2				
	kMDitemAcquisitionMake	LG Electronics				
	kMDitemLatitude	43.6428		200		ters later
	kMDItemLongitude	-70.2465		100	2	
	kMDitemAltitude	0.05			A CONTRACTOR	21
	KMDItemTimestamp	16:56:57				A
-	KMDRemAcquisitionModel	VM670				
. E	KMDitemGPSDateStamp	2012:08:26		A 1995		0

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

## 19.5 EXIF Metadata Search

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

Ć	RECON_LAB	Process	Search	Timeline	Export	Report				
			File Searc	ch						
			Content S	Search						
			Exif Meta	Exif Metadata Search						
			Apple Me	tadata Sea	rch					
			Artifacts	Keyword Se	earch					
			Recogniz	e Face						

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

🔽 Latit	ude	From	40.0000		То	50.0000	
🗸 Long	itude	From	-70.2450		То	-70.0000	
Author						Contains	
Make	[]					Contains	<b>•</b>
Model		<u> </u>		0		Contains	
Model All So	urce lter	O Sele	ct Source ilters	ŝ≣ Selec	t	Contains	

Enter information for any of the following filters:

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

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



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

Location Search	Search

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

« )	» [	xif Metadata Searc	h	\$ X			ocation Search (14)		\$	x		
			Sear	ch Filters	Show A	11						
							Files Ga	llery View				
	1.1.1	Record No.		File Nar	ne	File Size	Author	Ma	ake Mor	del Latitud	le Longitude	Da
1	П	612879	= 20	12-08-26 12.	34.38.ipg	964273		LG Electronic	s VM670	4	3.6709 -70.157	2012/08/26 1
2		612884	₩ 20	12-08-26 14.4	44.38.ing	897284		LG Electronic	S VM670	4	-70,2420	2012/08/26 1
3		612885	· 20	12-08-26 14	52.01 ing	880673		LG Electronic	s VM670	4	-70 228	2012/08/26 1
4		612886	= 20	12-08-26 14	54.33 ing	874261		LG Electronic	× VM670	4	3 6542 -70 2230	2012/08/26 1
5		612887	20	12-08-26 14	58 58 ing	954659		LG Electronic	× VM670	43	3 6522 -70 214	2012/08/26 1
6		612888	= 20	12-08-26 14	59.05 ing	930774		LG Electronic	× VM670	4	3 6521 -70 2140	2012/08/26 1
7		612880	20	12-08-26 14	59.13 ing	879356		LG Electronic	S VM670		43 652 -70 214	2012/08/26 1
8		612300	E 20	12-00-20 14.	55.15.jpg	013330		Lochestronic	- VM670	0.0	26519 -70.214	2012/00/201
9		612801	20	12.09.26.15	01.28 inc	964206		LC Electronic	× VM670		26518 -70.210	2012/08/26 1
10		612891	20	12-08-20 15.	01.28.jpg	904200		LG Electronic			70.2190	2012/08/201
10		612892	20	12-08-26 15.	06.21.jpg	924163		LG Electronic	S VM670		-70.215	2012/08/26 1
11		612893	9 20	12-08-26 15.	07.45.jpg	975282		LG Electronic	S VM670	4	3.6497 -70.2174	2012/08/26 1
12		612894	20	12-08-26 15.	56.24.jpg	1092847		LG Electronic	s VM670	4:	1.6506 -70.2037	2012/08/26 1
13		612895	<u>⊒</u> 20.	12-08-26 16.	10.01.jpg	953250		LG Electronic	s VM670	4:	3.6576 -70.2171	2012/08/26 1
14		612896	<u>⇒</u> 20	12-08-26 16.	10.07.jpg	957537		LG Electronic	s VM670	4	3.6577 -70.2174	2012/08/26 1
Key				Value						1	//	
100	Pixerruim	ension		2040						1		
	AltitudePo	f		43.0518								
4	DateStam			2012-08	26						11 5	
1	Altitude			0.019								
1	Longitude			70.2194								
Ē	Longitude	Ref		w								
	TimeStam	2		19:01:06	i .							
	LatitudeRe	f		N								
1	PixelWidth			1536								
2	Detailed Info	mation	HexV	iew 7	Text View	S Strings	🔓 Exif Me	tadata 🛛 🐻	Apple Metadata	📥 < 🗲 🖼 Pr	eview	

# 20. Advanced Viewers

Integrated into RECON LAB are four advanced viewers.

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

### 20.1 Plist Viewer

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

	0	Record No.	Inode No./File ID	File Name	Exter	sion	Fil	e Path
26		618457	874079	com.apple.finder.plist	plist	Altere (Jorean (Liberov) Bookmark Remove Bookmarks	Declaras	ces/com.apple.finder.plist
						Add Note Remove Note		
						Quick Look		
						Open With		Plist Viewer
						Send To Bucket Export Add To Text Indexing Queue Carve Files	*	Hex Viewer SQLite Viewer Registry Viewer

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

Open With	*	
Send To Bucket		Plist Viewer
Export Add To Text Indexing Queue		Hex Viewer SOLite Viewer
Carve Files Carve Data		Registry Viewer

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

« »	Plist Viewer 😂 🛠	com.apple.finder.plist [File System	618457] <b>\$</b> ×			
Q. Desktop	Search	Refresh	Match	Found: 7 HTML	Tags	C Report
	Key		Туре	Value		
w	Root		Dictionary	(52 items)		
	NSNavBrowserPrefe	eredColumnContentWidth	Number	186		
) F	SearchViewSettings		Dictionary	(1 items)		
•	FXDesktopVolume	Positions	Dictionary	(69 items)		
>	FK_StandardViewSe	ettings	Dictionary	(4 items)		
F	NSToolbar Configu	ration Browser	Dictionary	(6 items)		
	NSNavLastRootDire	ctory	String	~/Dropbox		
	FXArrangeGroupVie	ewBy	String	Name		
	SidebarPlacesSection	onDisclosedState	Boolean	YES		
	FXLastSearchScope	k	String	SCcf		
	NSNavPanelExpand	ledSizeForOpenMode	String	(765, 448)		
	ShowPathbar		Boolean	YES		
	FXSavePBFAfterTra	sh	Boolean	YES		
	FlowViewHeight		Number	505		
Þ	FXInfoPanesExpand	ied	Dictionary	(4 items)		
	FK_SavedViewStyle		String	clmv		
Þ	TrashViewSettings		Dictionary	(4 items)		
	SidebarSharedSecti	onDisclosedState	Boolean	YES		
•	ComputerViewSett	ings	Dictionary	(2 items)		
	ShowMountedServe	rsOnDesktop	Boolean	YES		
	BackupProgressWir	ndowLocation	String	{1023, 36}		
	ShowHardDrivesOr	Desktop	Boolean	YES		
<b>F</b>	FXRecentFolders		Array	(7 items)		
	SidebarDevicesSect	tionDisclosedState	Boolean	YES		
	ShowRemovableMe	diaOnDesktop	Boolean	YES		

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.

	Keys	Data Conversion
1	Root	✓ Select Conversion
2	MCMMetadataldentifier	Unix Timestamp
3	MCMMetadataInfo	WebKit/Chrome Timestamp
4	MCMMetadataVersion	ASCII
5	MCMMetadataUserIdentity	
6	MCMMetadataContentClass	Select Conversion
7	MCMMetadataUUID	Select Conversion
8	MCMMetadataSchemaVersi	Select Conversion
9	MCMMetadataActiveDPClass	Select Conversion
10	com.apple.MobileInstallati	Select Conversion
11	posixUID	Select Conversion
12	posixGID	Select Conversion
13	personaUniqueString	ASCII 😒
14	type	Select Conversion
15	version	Select Conversion

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

« :	Plist Viewer	¢ X S	SampleList (File Syster	n 1] [Source2]	\$ X			
ĸ	eyword Search	Search Refresh				HTML	🔁 Tags	😌 Report
	Key		Type	Value				
~	Root		Dictionary	(4 items)				
	TestHex		String	54 68 69 73 20 69 7	73 20 74 65 73 74 20	74 6		
	TestInt		Number	2319				
	TestData		Data	d31e78d31ebcd31e	bdd31ef7d31db4d31e	sbdd		
	TestHexCombined		String	5468697320697320	74657374207465787	74		
Sour	ce Name: /SampleList							
View	er Display Name: SampleList [File	System 1] [Source2]						
Key:	TestHexCombined							
Type	<u>e String</u>							
Valu	e: 5468697320697320746573747	2074657874						
Value	acconverteu). This is test text						No Preview Availat	ale
Key	Path: Root/TestHexCombined							
File	Name: Samplel ist							
File	Path: /SampleList							
-								
13/	Detailed Information	Optical Character Recognition	Itex Vie	w T Text Vi	ew S	Preview	1	
-		aprivat unanative trangetting					h-	

### 20.2 Hex Viewer

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

### Open File in Hex Viewer

5	612382	120	2012-08-26 12.52.44.jpg	1040153	image/jp	eg	43.65	08	-7
6	612383		2012-08-26 12.57.12.jpg	980533	image/j	Peelsmark	12.54	28	-7
7	612384	-	2012-08-26 12.57.34.jpg	999564	image/j	Remove Bookmarks		8	-7
8	612385		2012-08-26 14.44.38.jpg	897284	image/j			9	-7
9	612386	101	2012-08-26 14.52.01.jpg	880673	image/j	Add Note Remove Note		7	-7
10	612387		2012-08-26 14.54.33.jpg	874261	image/j	Go to Source		2	-7
11	612388	-	2012-08-26 14.58.58.jpg	954659	image/j	Export as KML		2	-7
12	612389		2012-08-26 14.59.05.jpg	930774	image/j	Quick Look		1	-7
13	612390	-	2012-08-26 14.59.13.jpg	879356	image/j	Open With	►	E	Plist Viewer
14	612391		2012-08-26 15.01.22.jpg	943964	image/j	Open with External Applicatio	n 🕨		Hex Viewer
15	612392	199	2012-08-26 15.01.28.jpg	964206	image/j	Send To Bucket Run Filesystem Modules	-		SQLite Viewer
16	612393		2012-08-26 15.06.21 ing	924163	image/ii	Export		L.	Registry 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".

« »	Hex Viewer	\$ X	2012-08-26 12.57.12.jpg [File System 612383] 🗘 🕏 K	
Bytes per line 32	<u></u> < s	earch >	Go to Offset Show Tags	
Offset 0 1 2	34567	8 9 10 11 12	2 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Use Little Endian format for Integers
00000 ff d8 ff 00032 00 6e 01	e1 a4 8c 45 78	69 66 00 00 4c	d 4d 00 2a 00 00 00 08 00 08 01 0f 00 02 00 00 00 0f 00 00Exif. MV.*	Data Type Value
00064 00 01 00	00 00 8e 01 28	00 03 00 00 00	0 01 00 02 00 00 02 13 00 03 00 00 00 01 00 01 00 087 69	1 8 bit binary
00128 63 74 72	6f 6e 69 63 73	00 00 56 4d 36	5 37 30 00 00 00 00 00 00 48 00 00 01 00 00 04 800 00 ctronics. VM670HH	2 8 bit signed
00192 00 00 00	14 00 00 01 1c	91 01 00 07 00	0 00 04 01 02 03 00 a0 00 00 07 00 00 04 30 31 30 30	3 8 bit unsigned
00256 00 00 08	00 a0 05 00 04	00 00 00 00 01 00	0 00 01 30 00 00 00 03 20 31 32 3a 30 38 3a 32 36 20 31 	4 16 bit signed
00320 00 02 00	00 00 04 52 39	38 00 00 02 00	0 07 00 00 00 04 30 31 30 30 00 00 00 00 09 00 11 00 02 0 07 00 00 00 04 30 31 30 30 00 00 00 00 09 00 10 00 2	5 16 bit unsig
00332 00 00 00 00	02 40 00 00 00 00	00 02 00 03 00 00 00 01 d8 00	0 05 00 01 00 00 01 00 00 00 00 00 00 00 00	6 32 bit signed
00418 00 00 01	00 00 07 00 05 0b 00 00 02 1c		0 00 02 b 00 00 01 00 00 00 00 00 00 00 00 00 00	7 32 bit unsig
00480 00 00 03	e8 00 00 00 45 e8 00 00 00 10	00 00 00 01 00	0 00 00 80 00 00 01 00 00 00 98 00 00 03 88 00 00 03 22	8 64 bit signed
00576 00 00 01	1a 00 05 00 00	00 01 00 00 02	2 76 01 1b 00 05 00 00 00 01 00 00 02 7e 01 28 00 03 00 00 01 00 00vvv	9 64 bit unsig
00508 00 01 00 00 00 00 00 00 00 00 00 00 00	00 00 48 00 00 00 00 48 00 00	00 04 00 00 00	0 48 00 00 00 02 86 02 02 00 04 00 00 00 01 00 00 11 fe 00 00 0 48 00 00 00 01 ff d8 ff db 00 84 00 03 02 02 03 02 02 03 	10 DOS Time
00572 03 03 03 00704 0e 11 0e	04 03 03 04 05 0b 0b 10 16 10	11 13 14 15 15	4 05 0a 07 07 05 08 0C 0a 06 0C 00 0a 06 06 06 12 10 0a	Selection -
00736 09 05 05 00768 14 14 14	09 14 0d 0b 0d 14 14 14 14 14	14 14 14 14 14 14 14 14 14 14 14	4 14 14 14 14 14 14 14 14 14 14 14 14 14	Selection Count :
00800 c0 01 50 00832 00 00 00	03 01 22 00 02 01 02 03 04 05	11 01 03 11 01 06 07 08 09 0a	l ff c4 01 a2 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 .P."	© Cursor Position : 0 (0x0)
00864 02 03 00 00896 33 62 72	04 11 05 12 21 82 09 0a 16 17	31 41 06 13 51 18 19 1a 25 26	l 61 07 22 71 14 32 81 91 a1 08 23 42 b1 c1 15 52 d1 f0 24l1ACa."q.2#BR.S 6 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 3br%&'()*456789: CDEFGHIJ	File Name 2012-08-26 12 57 12 inc
00928 53 54 55 00960 92 93 94	56 57 58 59 5a 95 96 97 98 99	63 64 65 66 67 9a a2 a3 a4 a5	7 68 69 6a 73 74 75 76 77 78 79 7a 83 84 85 86 87 88 89 8a 5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6	File Path: //Jsers/jermyn/Dropbox/Camei
00992 c7 c8 c9 01024 fa 01 00	ca d2 d3 c4 d5 03 01 01 01 01	d6 d7 d8 d9 da 01 01 01 01 01	a el e2 e3 e4 e5 e6 e7 e8 e9 ea fl f2 f3 f4 f5 f6 f7 f8 f9 1 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 11 00	File 3/2e . 937.33 KB
01056 02 01 02 01088 22 32 81	04 04 03 04 07 08 14 42 91 al	05 04 04 00 01 b1 c1 09 23 33	1 02 77 00 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13	
01120 28 29 2a 01152 6a 73 74	35 36 37 38 39 75 76 77 78 79	3a 43 44 45 46 7a 82 83 84 85	5 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 ()*56789: CDEFGHIJSTUVWXYZcdefghi 5 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a az a3 a4 a5 a6 istuvwxyz.	
01184 a7 a8 a9	a b2 b3 b4 b5	b6 b7 b8 b9 ba	a c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2	

The Hex Viewer will open in the Main Viewer window.

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

### Search in Hex Viewer

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

0.0	Search		
VM670		V HEX	0
	Search	ASCII UTF-16	

After entering the search term click "Search".

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
00096	00	04	00	00	00	01	00	00	00	96	88	25	00	04	00	00	00	01	00	00	01	4e	00	00	02	28	4c	47	20	45	6c	65	N(LG Ele
00128	63	74	72	6f	6e	69	63	73	00	00	56	4d	36	37	30	00	00	00	00	00	00	48	00	00	00	01	00	00	00	48	00	00	ctronics VM670 H H
00160	00	01	00	09	90	00	00	07	00	00	00	04	30	32	32	30	90	03	00	02	00	00	00	14	00	00	01	08	90	04	00	02	
00192	00	00	00	14	00	00	01	10	91	01	00	07	00	00	00	04	01	02	03	00	aO	00	00	07	00	00	00	04	30	31	30	30	
00224	a0	01	00	03	00	00	00	01	00	01	00	00	a0	02	00	04	00	00	00	01	00	00	06	00	a0	03	00	04	00	00	00	01	
00256	00	00	08	00	aO	05	00	04	00	00	00	01	00	00	01	30	00	00	00	00	32	30	31	32	3a	30	38	3a	32	36	20	31	
00288	32	3a	35	37	3a	31	32	00	32	30	31	32	3a	30	38	3a	32	36	20	31	32	3a	35	37	3a	31	32	00	00	02	00	01	2: 57: 12. 2012: 08: 26 12: 57: 12

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

#### Jump to an Offset

	Go to Offset
	Multiplier 1
O From Start	From Cursor Position     From End
	Jump

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

Select where to begin:

**From Start** – from the beginning of the file.

From Cursor Position – from where the cursor currently sits.

**From End** – From the end of the file.

#### Tag Selected Bytes

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1
00000	ff	d8	ff	<b>e</b> 1	a4	8c	45	78	69	66	00	00	4d	4d	00	2a	00	00	00	08	00	08	01	Of	00	02	00	00	00	Of	00	00	Exi f NN. *
00032	00	6e	01	10	00	02	00	00	00	08	00	00	00	7e	01	1a	00	05	00	00	00	01	00	00	00	86	01	1b	00	05	00	00	. n ~
00064	00	01	00	00	00	8e	01	28	00	03	00	00	00	01	00	02	00	00	02	13	00	03	00	00	00	01	00	01	00	00	87	69	·····(····i
00096	00	04	00	00	00	01	00	00	00	96	88	25	00	04	00	00	00	01	00	00	01	4e	00	00	02	28	4c	47	20	45	6c	65	N
00128	63	74	72	<b>6</b> f	6e	69	63	73	00	00	56	4d	36	37	30	00	~~	-			20	48	00	00	00	01	00	00	00	48	00	00	ctronics VN670 H H H
00160	00	01	00	09	90	00	00	07	00	00	00	04	30	32	32	Ta	g Se	lecte	ed b	ytes	0	00	00	14	00	00	01	08	90	04	00	02	
00192	00	00	00	14	00	00	01	1c	91	01	00	07	00	00	00	Sta	rt Bl	ock			D	00	00	07	00	00	00	04	30	31	30	30	
00224	a0	01	00	03	00	00	00	01	00	01	00	00	a0	02	00	En	d Blo	ock			0	00	06	00	a0	03	00	04	00	00	00	01	
00256	00	00	08	00	aO	05	00	04	00	00	00	01	00	00	01	Co	nv				. 2	30	31	32	3a	30	38	3a	32	36	20	31	
00288	22	32	35	37	32	31	32	00	32	30	31	32	22	30	35	~~~	P7			5	.2	22	35	37	30	31	32	00	00	02	00	01	2.57.12 2012.08.26 12.57.12

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".

Start Address	122	
End Address	142	
Saved Tags	<select tag=""></select>	0
🗹 Create New	Camera_Name	Yellow
Cancel		Save

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".

																				1	Та	gs											
1	s	r.		St	art A	ddr	ess	E	nd A	ddre	255		Tag	Nar	ne		Та	g Ca	olor						1	Гag	Data						
1 1				122	2			14	2			Ca	mer	a_N	ame					ł	4c47	7204	56c	656	3747	726f	6e6	9637	7300	0005	64d	3	
Re	move		E	хро	rt Da	ata																											
Offse	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0000	) ff	d8	ff	e1	a4	8c	45	78	69	66	00	00	4d	4d	00	2a	00	00	00	08	00	08	01	Of	00	02	00	00	00	Of	00	00	Exi f NN. *
0003	2 00	6e	01	10	00	02	00	00	00	08	00	00	00	7e	01	1a	00	05	00	00	00	01	00	00	00	86	01	1b	00	05	00	00	. n ~
0006	00	01	00	00	00	8e	01	28	00	03	00	00	00	01	00	02	00	00	02	13	00	03	00	00	00	01	00	01	00	00	87	69	
0009	5 00	04	00	00	00	01	00	00	00	96	88	25	00	04	00	00	00	01	00	00	01	4e	00	00	02	28	4c	47	20	45	60	65	N(LG Ele
0012	63	74	72	6f	6e	69	63	73	00	00	56	4d	36	37	30	00	00	00	00	00	00	48	00	00	00	01	00	00	00	48	00	00	ct roni cs VN670 H H
0016	00 (	01	00	09	90	00	00	07	00	00	00	04	30	32	32	30	90	03	00	02	00	00	00	14	00	00	01	08	90	04	00	02	

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

### Hex Viewer Information Pane

	Data Type	Value
1	8 bit binary	01100011
2	8 bit signed	99
3	8 bit unsigned	99
4	16 bit signed	25459
5	16 bit unsig	25459
6	32 bit signed	1668481024
7	32 bit unsig	1668481024
8	64 bit signed	7166071433524491831
9	64 bit unsig	7166071433524491831
10	DOS Time	14:27:24
iele iele Curs	ction : 134–134 ction Count : 1 (( sor Position : 135	0x1) ; (0x87)

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

### 20.3 SQLite Viewer

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

#### **Open File in SQLite Viewer**

							Files	Galler
	R	Record No.	File Name		File Size	м	ime Type	Sig
16		1211660	2041457d5fe04d39	applicat	pplication/x-sqlite3			
17		1216130	Manifest.db		10743808	applicat	tion/x-sqlite3	SQLit
18		612859	places.sqlite	Berthmark	10495760	applicat	ion/x-sqlite3	SQLit
19		619058	places.sqlite	BOOKMARK Remove Bookr	narks		on/x-sqlite3	SQLit
20		256560	valid.sqlite3				on/x-sqlite3	SQLit
21		386572	valid.sqlite3	Add Note Remove Note			on/x-sqlite3	SQLit
22		681132	valid.sqlite3	Go to Source			on/x-sqlite3	SQLit
23		1211346	12b144c0bd44f2b	Export as KML			on/x-sqlite3	SQLit
24		63186	valid.sqlite3	Quick Look			on/x-sqlite3	SQLit
25		487758	valid.sqlite3	Open With			Plist Viewe	r
26		1172625	valid.sqlite3	Open with Ext	ernal Applicat	tion 🕨	Hex Viewe	r
27		735077	gk.db	Send To Bucke	t Modules		SQLite Vie	wer
28	735488		ak dh	Eurost	imodules	Registry V	iewer	

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".

《 》 SQLite V	/lewer 🗘	X.			places.sq	ite (File System 6	12859]		¢ X				
Tables							Browse Da	Execute SQL					
moz_places	D	Keyw	ord Search		Searc	h Show All			Export	HTML	Bookmarks		Report
moz. p/ac	ies					O moz an	attributes O	moz historovisits	mor places				
Column Name	Search			12	7252	1 - Conversion - Inter							
1 🔳 id			1999	10	un			title		rev_nost	VISIT_COUNT	nidden	tÀI
2 🔳 url		257		258	https://ww	w.google.com/se	earch?q=gun+clean	gun cleaner lut	ricant – Google Search	moc.elgoog	1	0	0
3 🔳 title		258		259	http://ww	w.googleadservic	es.com/pagead/aclk.	•		moc.secivres	1	1	0
4 my host		259		260	http://ww	w.cheaperthandin	.net/product/5739	Break-Free CLF	Cleaner Lubricant an	ten.tridnahtr	1	0	0
5 Digit count		260		261	https://ww	w.google.com/se	arch?q=CLP+gun+	. clp gun cleane	- Google Search	moc.elgoog	1	0	0
6 hidden		261		262	https://ww	w.google.com/si	arch?q=how+to+u	how to use clp	gun cleaner - Google	moc.eigoog	1	0	0
o niuden		262		263	http://ww	w.google.com/url	7sa=t&rct=j&q=&es.			moc.elgoog	1	0	0
/ Typed		263	1	264	http://ww	w.youtube.com/w	atch?v=teHpfPSgRfk	CLP breakfree	what to use to clean yo	moc.ebutuoy	1	0	0
8 favicon_id		264	n.	265	http://ww	w.poogle.com/url	7sa=t&rct=i&g=&es.			moc.elapop	1	0	0
9 frecency		265	171	266	http://ww	w.voutube.com/m	sults?search query	. dp cleaner - Y	ouTube	moc.ebutuov	1	0	0
10 Inst_visit_date		266	-	267	http://www	www.ube.com/w	atch?v=H6ClOhaPow	a Basic Introduct	ion to rieaning any aut	mor ehuture	1	0	0
11 🔳 guid		267	and a second	269	https://ww	er occale com/o	arch?a-hours to su	how to use clo	Coools Search	mor alanan			
		200	1.1	200	https://ww	m.google.com/si	aschig-now-to-u.	. now to use up	- Google Search	moclegoog			
		200		209	ndp://ww	w.googie.com/un	sa=tarct=j&q=&es.			muc.ergoog	1	0	0
		269		270	http://ww	w.thehighroad.org	archive/index.php.	How do you us	e CLP? - THR	gro.daorhgih	1	0	0

The SQLite Viewer will open in the Main Viewer window.

### Filtering Table Data

«	» sql	.ite Viewer 🔶	×		pla	ces.sqlite [File Sys	item 612859]		¢ X
	Tab	les						Browse Data	Execute SQL
m	z_places	0	Keyw	ord Search		Search S	now All		
	moz	places						moz pla	ices
	Coloum Name	Search	-			10247	1.00.0		
1	🗌 id	П			RECON INT	url	title	visit_count	last_visit_date
2	url		1		1	http://www		0	
3	E title		2		2	http://www	201	0	
-		-	3		3	http://www	**	0	
-	rev_nost		4		4	http://www		0	
2	visit_count	-	5		5	http://www.		0	
6	hidden		6		6	place sort=8		0	
7	typed		7		7	place:Solt=0		0	
8	favicon_id		-		,	place:roider	•	0	
9	frecency		8		8	place:type=6		0	
10	last visit date	-	9		9	http://www		1	1356533519
11		-	10		10	http://www	Welcome to F	1	1356533520
	gene.		11		11	https://www	dropbox - G.	1	1356533726

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

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

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

#### Searching in the SQLite Viewer

SQLite Vie	ewer 🗘	X			pl	aces.sqlite [F	ile System 61285	거	\$ X				
Tables								Browse Data	Execute SQL				
moz_places	0	gun			Ø	Search	Show All		Exp	ort HTML	Bookmarks	C Rep	port
_moz_place		_					O moz anno att	ributes Om	oz historwisits				
Column Name	Search								alat.	-	indefe annual	bidden.	
1 🔳 id		2	1000	10	ur	annan ann an			uue	rev_nost	VISIT_COUNT	nicden	
2 🔳 url		1		183	ht	tp://www.go	ogle.com/url?sa=	t&rct=j&q=&es		moc.elgoog	. 1	0	
3 🔳 title		2		184	h	tp://www.tes	wksburyrodandgu	n.org/documen	SIGARMS Classic Owners Manual I	22 gro.nugdnad.	_ 0	0	_
4 🔳 rev_host		3		203	ht	tp://us.gloci	ccom/		GLOCK "Safe Action"® Pistols   He	ndg moc.kcolg.su	- 1	0	
5 visit_count		4		241	ht	tps://www.g	oogle.com/search	7q=cdl+gun+cl	cdl gun cleaner - Google Search	moc.elgoog	. 1	0	
6 🔳 hidden		5		242	ht	tps://www.g	oogle.com/search	?q=cdl+gun+cl	. top gun cleaners - Google Search	moc.elgoog	. 1	0	
7 Etyped		6		243	ht	tp://www.go	ogle.com/url7sa=	t&rct=J&q=&es		moc.elgoog	. 1	0	
8 g favicon_id		7		244	ht	tp://www.us	acarry.com/forum	s/handgun-ma	What is the best gun cleaning pro	duc moc.yrracasu	1	0	
9 frecency	-	8		245	ht	tps://www.g	oogle.com/search	7q-gun+cleani	gun cleaning products - Google S	earch moc.elgoog	. 1	0	
10 Iast visit date		9		246	ht	tp://www.go	ogle.com/url?sa=	t&rct=j&q=&es		moc.elgoog	. 1	0	
		10	in .	747	in	tn-//www.he	nunalis com/aun.	rlassing_cham	Cun Cleaning Sunnlies & Chemica	ls n mor clianume	1	0	
able: moz_places d: 203													
arl: http://us.glock.com/													
itle: GLOCK "Safe Action"® Pist	tols   Handguns   Fit	rearms (	GLOCK USA									10.2.1	
ev_host: moc.kcolg.su.											No Preview Availa	able	
isit_count: 1													
idden: 0													
vined: 0	_	_		_	_								_
Detailed Information	The Piex View		T Text View	S	Strings	1	xil Metadata	Apole Me	tadata Maps	in Preview			

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

### Executing a SQLite Query

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

« >	SQLite V	lewer 🗢	x		places.sqlite [File Sys	tem 612859]		• ×
	Tables					Browse Data	Execute SQL	
mo	z_places	٢	select id,url,tit	le,visit_count,	last_visit_date,guid from moz_place	es		
	moz_plac	es						
	Coloum Name	Search						
1	📕 id							
2	🔳 url							
3	📕 title							
4	rev_host							
5	visit_count		Execute Qu	ery		Query Successful	l.	
6	hidden			id	url	title	visit_count	last_visit_date
7	typed		251	252	https://www.google.com/	gun cleaning crl - Google Se	1	1362425164269666
8	favicon_id	•	252	253	https://www.google.com/	gun cleaning product cdl	1	1362425197892446
9	frecency	-	253	254	http://www.google.com/u		1	1362425202561107
10	Iast_visit_date		254	255	http://www.remington.co	Rem Oil - Gun Care - Gun C	1	1362425216454530
11	guid	-	255	256	https://www.google.com/	gun cleaner lunricant - Goo	1	1362425254306520

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

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

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

#### Data Conversion

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



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



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

(Tétére)									Erowse Date	Execute SQL					
chat 🗧													Tapion HTML	8 Bookmark	Beport
(THE								W SolwDa	utabaseProperties	Se menager	(9) (M/)				
Column Name				1	_	-	_				-		-		
1 🖸 ROWD		s_archived	addressed_h	a display_name	a diant in	is filtered	CCCESSINI da	e 🖾 engraming	Ber dunge t	o CK_Sync_state	a diam diona	a isst, read, message_timestamp		clou	en trocora id
2 🛃 guid		1271	Saarch	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search		
3 🖸 style			cuare khan		ACADAFSE		1		z	1	SC39A9FC-	67899281512044236	stbd506adececc7bf	8153622104229:35	ac101138956d101122
4 👩 sizza	2		duine khan		COENCEA0-	1	<u> </u>	6	10		#8542100-4	68013310608076379	56cf5+6+3d11168	20758041340226401	d227c193f5059102b
5 🛃 account_id	3		Guare, khan		59048150-0		1	v	×	1	59048F5D-0	67958435710985396	ecb11da01bb594fr	dex05271847550044	4444acl0fa425b3681
# 🛃 properties	74		Chane, khan		0986AF58-6		1		16	1	098EAF58-0	68108629050163174	1 d2310c996fd895bd	bde9c01ef15c994d5	4861db1211c30/589a
7 🛃 chat, identifier	5		coune, khan		20609AFF		1		12	1	INFORME	6783324330000000	d486ececd5865a15	0540200012992553	84512438196807500
8 Service_name															
9 👩 noom_name															
10 🛃 account Jopin															
11 👩 is archived															
12 🛃 last_addressed_handle															
🖬 🛃 display_name															
14 📶 group_id															
1 10 1 18582 100 - 8427 - 41510 - 9144 - 7161 99467 084 19163 - 1916 - 8427 - 41510 - 91467 09467 094 1916 - 914 -														No Preview Ava	lative

### 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.
« »	> Source \$ X			Windows Registry (Windows Registry)					¢ ×
	>		Se	arch	Filters 🔽	Show All	Table View Gallery View		
	•	Record No.	Inode No./File ID	i l	File f	Name	Extension	Fi	le Path
1		1			SAM		/SAM		
2		2			SECURITY		/SECURITY		
3 🗌		3			DEFAULT		/DEFAULT		
4		4			SOFTWARE		/SOFTWARE		
5	-	5		-	SYSTEM		Bookmark Remove Bookmarks		
Window	vs Registry >			_		-	Add Note Remove Note Ouick Look		
Source Name: /Windows Registry Record No.: 5 File Name: SYSTEM File Path: /SYSTEM							Open With Send To Bucket Export Add To Text Indexing Carve Files	Deve	Plist Viewer Hex Viewer SQLite Viewer Registry Viewer

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

Open With	*	
Send To Bucket		Plist Viewer
Export		Hex Viewer
Add To Text Indexing Queue		SOLite Viewer
Carve Files		Registry Viewer
Carve Data		incgioni f incinci

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

« »	Registry Viewer	\$×			S	YSTEM [File System 27256]		e x
		Search	Refresh					
						All Items Searched Items		
Node Name		Node Tim	nestamp	1		Key	Туре	Value
v	USBSTOR	2015/03	/23 14:31:10 GMT-4:00	4		CompatibleIDs	REG_MULTI_SZ	USBSTOR\DiskUSBSTOR\RAW
	Disk&Ven SanDisk&Pr.	2015/03	/24 09:58:32 GMT-4:00	5		ContainerID	REG_SZ	{4933888a-6002-5a33-95a4-bad21ec52623}
1	4C530012450531.	. 2015/03	/24 09:38:00 GMT-4:00	6		ConfigFlags	REG_DWORD	
	▶ 4C530012550531	. 2015/03	/24 09:58:33 GMT-4:00	7		ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
► Ha	ardware Profiles	2015/03	/25 09:05:22 GMT-4:00	8		Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
Po	olicies	2009/07	/14 00:49:20 GMT-4:00	9		Class	REG SZ	DiskDrive
⊧ se	ervices	2015/03	/23 16:00:56 GMT-4:00	10	Ē	Mfg	REG SZ	@disk.inf.%genmanufacturer%:(Standard disk drives)
▶ Contr	rolSet002	2009/07	/14 01:08:21 GMT-4:00	11	<u> </u>	Service	REG SZ	disk
Moun	ntedDevices	2015/03	/24 09:58:34 GMT-4:00	12		FriendlyName	REC SZ	SanDick Cruzer Ett USB Device
PNC		2015/02	125 00.20.28 CMT_4.00		-		KEG_JE	Sandisk Cluzer nit 036 Device
Plugin: Regis Tab Name: R Source Name File Path: /W Node Path: H Node Name: Node Timest	itry Viewer legistry Viewer 2: /cfreds_2015_data_leakag indows/System32/config/Rk IKEY_LOCAL_MACHINE (HKLI /HKEY_LOCAL_MACHINE/SY amp: 2015-Mar-24 09:38:0	je_pc.E01/nt egBack/SYST M) 'STEM/Contr 0 GMT-4:00	rfs TEM rolSet001/Enum/USBSTOR/I	Disk&	Ven_SanD	sk&Prod_Cruzer_Fit&Rev_2.01/4C530	01245053110159	3&0

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.

« »	>	Registry Viewer	\$ X		SYSTEM [File System 27256	1		\$ ×		
SanD	isk	Sea	arch Refresh							
					All Items Searc	hed Items				
			Node Name		Node Timestamp		Key	Туре	Value	Hex Value
23		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4					
24		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4					
25		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Туре		REC_BINARY		12000000
26		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Data		REC_BINARY	SanDisk Cruzer Fit USB Device	530061006e004400690
27		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4					
28		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4					
29		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Туре		REG_BINARY		12000000
30		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Data		REC_BINARY	disk.inf:disk_device.NTamd6	6400690073006b002e0
31		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4					
32		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Туре		REG_BINARY		1000000
33		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Data		REC_BINARY	<b>O</b> OhOOeO	c0d368899765d001
34		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4					
35		/HKEY_LOCAL_MACHIN	NE/SYSTEM/ControlSet	001/Enum/USBSTOR	2015/03/23 14:31:11 GMT-4	Туре		REC_BINARY		1000000
File P Node Node {5401 Node Key : Type Value	ath : /Window Path : HKEY_L Name : /HKEY 9947e-8b40-4 Timestamp : Data : REG_BINARY : SanDisk Cru	s/System32/config/Regi ocCAL_MACHINE (HKLM) y_LOCAL_MACHINE(SYST 15bc-a8a2-6a0b894cbd; 2015-Mar-23 14:31:11 izer Fit USB Device	Back/SYSTEM TEM/ControlSe:001/En a2}/0000004/000006 GMT-4:00	um/USBSTOR/Disk&Ven 100	<mark>SanDisk</mark> &Prod_Cruzer_Fit&Rev.	2.01/4C53	001245053110155	3&0/Properties/	No Preview Av	ailable
Hex \	/alue :									
53 00	0 61 00 6E 00	44 00 69 00 73 00 68 0	0 20 00 S.a.r	.D.i.s.k						
43 00	0 72 00 75 00	7A 00 65 00 72 00 20 0	0 46 00 C.r.	ı.z.e.rF.						
69 00	0 74 00 20 00	55 00 53 00 42 00 20 0	0 44 00 i.t	U.S.BD.						
65 00	0 76 00 69 00	63 00 65 00 00 00	e.	v.i.ce						
2	Detailed infor	mation He	x View T[ Te	xt View S Str	ings 🛛 🗋 Exif Metadata	6	Apple Metadata	🎩 Maps 🚽 🕨	Preview	

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

Select the "Searched Items" tab to review the results.

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

## 21. Carving

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

File Carving – recover files from any source.

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

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

### 21.1 File Carving

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

Re	cord No.		File Name	File Path
1	1	hiberfil.sys		/hiberfil.sys
2	2	pagefile.sys		/pagefile.sys
			Carve Data	
			Carve Files	

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

	Carver
	File Types
+ 1	🖉 Images
-	OFFICE DOCUMENTS
> (	Miscellenous Files
> 8	Audios & Videos
Page	file svs Carving
rage	nie.sys Calving
	Start

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

Nam	e	 Date Modified
>	avi 📃	Today at 5:42 PM
>	mp bmp	Today at 5:43 PM
	carver_files.sqlite	Today at 5:44 PM
	carver_log.sqlite	Today at 5:47 PM
>	doc 🗧	Today at 5:40 PM
▶	docx	Today at 5:46 PM
>	gif	Today at 5:41 PM
►	html	Today at 5:42 PM
*	gqi 📰	Today at 5:45 PM
-	💼 mid	Today at 5:44 PM
-	mpg	Today at 5:41 PM
* 1	png	Today at 5:44 PM
>	ppt	Today at 5:45 PM
+	pptx	Today at 5:45 PM
*	prefetch	Today at 5:40 PM
+	registry	Today at 5:41 PM
>	rtf	Today at 5:40 PM
>	sqlite	Today at 5:40 PM
*	vob	Today at 5:40 PM
*	wave	Today at 5:41 PM
*	📰 xls	Today at 5:41 PM
>	xlsx	Today at 5:41 PM

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



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

≪ ≫	Carved Files	¢ X		Pagefile.sys_Carve			\$ ×		
		Search	Show All						
				Files Galler	y View				
	Record No.	File	Name	File Path	Extension	File Size	File Type	Offset	
7 🗆	7	108315845 bui	Itin carver hmn	/Lab Features/Carved Files/Source6/Pagefile s	hmn	17452272	RMP	3458245	
8	. 8	185881192 bui	Itin carver.bmp	/Lab Features/Carved Files/Source6/Pagefile.s	bmp	2097152	BMP	81023592	
9 🗆	9	192270388 bui	Itin carver.bmp	/Lab Features/Carved Files/Source6/Pagefile.s	bmp	31832	BMP	87412788	
10	10	192307252 bui	Itin carver.bmp	/Lab Features/Carved Files/Source6/Pagefile.s	bmp	31832	BMP	87449652	
11	11	192344116_bui	ltin_carver.bmp	/Lab_Features/Carved_Files/Source6/Pagefile.s	bmp	31832	BMP	87486516	
12	12	192380980_50	ltin_carver.bmp	/Lab_Pestures/Carved_Files/Source6/Pagefile.s	bmp	31832	BMP	67523380	
13	13	203901152_bui	ltin_carver.bmp	/Lab_Features/Carved_Files/Source6/Pagefile.s	bmp	31832	8MP	99043552	1
14	14	206872660_bui	ltin_carver.bmp	/Lab_Features/Carved_Files/Source6/Pagefile.s	bmp	54	BMP	102015060	
15	15	206909578_bui	ltin_carver.bmp	/Lab_Features/Carved_Files/Source6/Pagefile.s	bmp	62	BMP	102051978	
16	16	207192202_bui	ltin_carver.bmp	/Lab_Features/Carved_Files/Source6/Pagefile.s	bmp	62	BMP	102334602	
17	17	207519828_bui	ltin_carver.bmp	/Lab_Features/Carved_Files/Source6/Pagefile.s	bmp	54	BMP	102662228	
18	18	134892584_bui	ltin_carver.gif	/Lab_Features/Carved_Files/Source6/Pagefile.s	gif	131	GIF	30034984	
19	19	148589400_bui	ltin_carver.gif	/Lab_Features/Carved_Files/Source6/Pagefile.s	gif	4412	GIF	43831800	
Plugin Name: C: Record No: 12 File Name: 192; File Path: /Volue File Size: 31.09 File Type: BMP Offset: 8752331 Tag: Examiner Notes	arved Files 380980_builtin_carve mes/DEST/Person_of KB (31832 bytes) 30	r.bmp f_Interest_2019-4	Oct-17T19-48-2	6/Lab_Features/Carved_Files/Source6/Pagefile.sys_	Carve/bmp/0_10	0,192380980_bu	iltin_carver.bmp		
Detailed I	information	Hex View	T] Text V	iew S Strings 🔛 Exif Metadata	🕼 Ap	pie Metadata	🏦 Maps ୶ I	Preview	

### 21.2 Data Carving

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

	Record No.	F	ile Name	
1	1	hiberfil.sys	-	/hiberfil.sys
2	2	pagefile.sys	Carve Data	/pagefile.sys
			Carve Files	

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



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

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

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

## 21.3 Carving Unallocated Space



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

	File Types
•	Images
• •	OFFICE DOCUMENTS
•	Miscellenous Files
	✓ HTML
	✓ ZIP
	EMLX
	VDI
	SQLITE
	MSG
• •	Audios & Videos
NTFS	Unallocated Space Carving
	Start

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

Nam	ie	<ul> <li>Date Modified</li> </ul>	Ĩ
*	avi 🔤	Today at 5:42 PM	
•	bmp:	Today at 5:43 PM	
	carver_files.sqlite	Today at 5:44 PM	
	carver_log.sqlite	Today at 5:47 PM	
*	doc	Today at 5:40 PM	
>	docx	Today at 5:46 PM	
>	gif	Today at 5:41 PM	
*	html	Today at 5:42 PM	
>	eqi 📑	Today at 5:45 PM	
•	i mid	Today at 5:44 PM	
•	mpg	Today at 5:41 PM	
•	in png	Today at 5:44 PM	
>	ppt	Today at 5:45 PM	
>	pptx 📃	Today at 5:45 PM	
*	prefetch	Today at 5:40 PM	
▶.	registry	Today at 5:41 PM	
*	💼 rtf	Today at 5:40 PM	
+	sqlite	Today at 5:40 PM	
*	vob	Today at 5:40 PM	
*	wave	Today at 5:41 PM	
•	xis	Today at 5:41 PM	
*	xlsx	Today at 5:41 PM	

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



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

« »	Carved Files	÷×.	NTFS_Unallocated_Space_Carving	1		¢×	
		Search Show All					
			Files Gallery V	/iew			
	Record No.	File Name	File Path	Extension	File Size	File Type	Offset
367	3719	260236640 builtin carver.ing	/Lab Features/Carved Files/Source6/NTFS Una	ipa	26662	IPEG	50521440
368	3720	260263327 builtin carver.jpg	/Lab Features/Carved Files/Source6/NTFS Una	ipg	18411	JPEG	50548127
369	3721	260281763_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	ipg	214995	JPEG	50566563
370	3722	260626593_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	286085	JPEG	50911393
371	3723	260912703_builtin_carver.jpg	/Lab_Features/Carved_Files/Source5/NTFS_Una	jpg	189945	JPEG	51197503
372	3724	261102673_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	pg	221185	JPEG	51387473
373 🗌	3725	261103103_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	3712	JPEG	51387903
374	3726	261323883_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	279866	JPEG	51608683
375	3727	261603774_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	282101	JPEG	51888574
376	3728	261885900_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	283603	JPEG	52170700
377	3729	262169528_builtin_carver.jpg	/Lab_Features/Carved_Files/Source5/NTFS_Una	jpg	64692	JPEG	52454328
378	3730	264894134_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	38894	JPEG	55178934
379	3731	264933053_builtin_carver.jpg	/Lab_Features/Carved_Files/Source5/NTFS_Una	jpg	15058	JPEG	55217853
380	3732	264948136_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	80526	JPEG	55232936
381	3733	265746269_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	81420	JPEG	56031069
382	3734	266270005_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	45013	JPEG	56554805
383	3735	266270435_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	4289	JPEG	56555235
384	3736	285354831_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	86121	JPEG	75639631
385	3737	298231381_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	41719	JPEG	88516181
386	3738	298231713_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	pg	5889	JPEG	88516513
387	3739	298246740_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	5889	JPEG	88531540
388	3740	298273153_builtin_carver.jpg	/Lab_Features/Carved_Files/Source6/NTFS_Una	jpg	48127	JPEG	88557953
source Name: /c	freds_2015_data_leak	age_pc.E01/ntfs	8				
Plugin Name: Ca	rved Files						
. againtaine. ea							Just -
Record No: 3721	Ļ.						
File Name: 2602	81763_builtin_carver.j	ipg					
File Path: /Volun	nes/DEST/Person_of_li	nterest_2019-Oct-17T19-48-26,	Lab_Features/Carved_Files/Source6/NTFS_Unallocat	ed_Space_Carving	/jpg/		
0_100/200201/	os_buildin_carren.jpg						
File Size: 209.96 File Type: JPEG	KB (214995 bytes)						
Offset: 5056656	3						
Fag:							0
	H ///	WINT TOTAL AND AN AND AND AND AND AND AND AND AND	NUMBER OF THE OF THE OWNERS TO THE	The state of the second state	Marcal Marca	Contraction of the local division of the loc	IN THE REPORT OF T

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

## 22. Hash Sets

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

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

Sou									
500	rce No.	Source Name	Apple Metadata	Exif Metadata	Mime Type	Signature Analysis	Hashes	Verification	
Sourc	e1	/Chuck Norris Facts.dmg/Chuck Norris Facts	Completed	Completed	Completed	Completed	Completed	<u>Verify</u>	Remove
Sourc	e2	/Chuck Norris Facts					Completed		Remove
Ref	esh							Cancel	Start
-			_						

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

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

### 22.1 Creating Hash Sets

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



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

Hashset Name	Hide Matched Files	
		Cancel Apply
		Calicei

The Hash Set main window will appear.

Import v Create					
Hashset Name	Chuck Norris			-	
Hashset Hame	-			-	
		Cancel	Create		
				Cancel	Apply

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

	Hashset	
Import 🔽 Create	Remove	
Hashset Name	Hide Matched Files	
Chuck_Norris		
		Cancel Apply

The new hash set category is now created.

					RECO	N LAB-1.5.0 (A1)					
🐖 🙆 🔅						Ø 🛃				🔤 🔟 💿	i 🗐
All Features 🗢 🖨	< >	Source		\$×	APPLE S	D (William_Campbe	II_MacBook.dmg)	)[Sourcel]	\$ X		
				Search	Filters	Show All				Export	As 🖸 🔳
Case: Person of Interest	0					Table	View Gallery	View			
Source	R	Recor	rd No. Inc	ode No./File ID	F	ile Name	Extension	File Siz	e Date Modified	Date Change	1.11
William_Campbell_MacBook.	1		573201	364850	Cyberduck-	-7.8.5.34493.zip	zip	1246528	80 2021/04/07 19:42:15 -5:00	2021/04/07 19:42:16 -5:0	0 202
APPLE SSD (770002)	2		573202	396420	amptleojgv	of7scagh9t.jpg	ipg	3758	54 2021/04/09 10:44:50 -5:00	2021/04/09 10:44:51 -5:0	0 2021
> 📴 Preboot (730)	3	1     1	573203	283382	DS_Store			61	48 2021/04/12 08:14:44 -5:00	2021/04/12 08:14:44 -5:0	0 202
🗧 📴 Recovery (73)	4	. 6	573204	406968	hard copy i	docs.crypto	crypto	71110	26 2021/04/09 14:00:04 -5:00	2021/04/09 14:20:40 -5:0	0 2021
🗐 VM (2)	5		573205	353958	Facility Ima	gesiding	dmg	22461	44 2021/04/07 15:12:55 -5:00	2021/04/07 16:18:54 -5:0	0 2021
APPLE SSD - Data (20179)	6		573206	32387	localized	Bookmark Remove Bookmay	due .		0 2021/03/19 09:22:06 -5:00	2021/03/19 09:22:06 -5:0	0 202.
> 🧾 Update (355)	7		573207	385211	Vacation P	Tags	NS	9200	00 2021/04/08 19:00:51 -5:00	2021/04/08 19:10:58 -5:0	0 2021
> 📴 EFI (50)	8		573208	383734	17080675	Add Note		1895	84 2021/04/08 18:46:26 -5:00	2021/04/08 18:54:03 -5:0	0 202
Mobile Backup	9		573209	421032	Detail view	Remove Note		1416	16 2021/04/09 12:40:33 -5:00	2021/04/12 08:14:05 -5:0	0 2021
Disk Images	10		573210	421033	Detail view	Ouick Look		857	23 2021/04/09 12:40:53 -5:00	2021/04/12 08:13:28 -5:0	0 202
> 🇱 RAM Images	11		573211	421030	Detail view	Open With		1795	23 2021/04/09 12:40:23 -5:00	2021/04/12 08:13:51 -5:0	0 202.
🗧 🏟 Apple Metadata			573212	270878	2021-prin	Send To Bucket		▶ 3962	76 2021/04/05 17:36:30 -5:00	2021/04/05 17:36:35 -5:0	3 202
Exif			573213	383752	• 14397362	Add To Text Inde	xing Queue	334	51 2021/04/08 18:46:32 -5:00	2021/04/08 18:48:57 -5:0	202:
MIME Type	14		073214	383745	× 17083153	Carve Files		1412	99 2021/04/08 18:46:29 -5:00	2021/04/08 18:54:07 -5:0	3 202
Face Analysis	Ginnen					Carve Data					
Face Search	APPLE SSD >	Users > 🔽 w	illiamcampb	ell > Downloa	is)	Add file to hashs	et database	Ele	ectric_Car_Documents		
Contical Character Recognition	Source Name: /	William_Campbell	_MacBook.dr	mg/APPLE SSD		Run Filesystem M	lodules				
Skin Tone Detection	Record No.: 673	201				Export Hashes As Onen Detailed In	i formation	*			
> 🕎 Weapons	File Name: Cybe	rduck-7.8.5.3449	93.zip			Open with Extern	al Application				
Fire Analysis	File Path: /Users	/williamcampbell	I/Downloads	/Cyberduck-7.8.5	i.34493.zip	Copy to Clipboar	d				
Elle Extensions	Inode No./File I	D: 364850				Mark As Unseen					
User Defined File Signatures	File Size: 118.80 Mime Type:	3 MB (124652880	bytes)			Hide Seen Files		_			
Elle Size	Date Medifieds	2021 Apr 07.10	43-15 5-00			Show Seen Files				No Preview Available	
Snapshots	Date Change: 2 Date Accessed:	021-Apr-07 19:4 2021-Apr-07 19:4	2:16 -5:00 :42:15 -5:00	) )		Decompress File					
	Tag: Examiner Notes	ć.									
K-freen -	Detailed in	formation	Hex V	/iew T	Text View	S Strings	Exif Me	etadata	🍎 Apple Metada < > 🔛 P	review	

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

	-	-		324-01					194				
	All Features 🗢 🗘	$\langle \rangle$	Hashset	¢×		Electric	Car_Documents		• ×				
. 104	ызк шадез			Search Filt	ers 😇 🛛 Show All								
- 00	RAM Images						Files Gallery Vie	w					
0	Apple Metadata		Record No.	File	Name	File Size	М	D5		SHA1		1 ()	Date Mo
	Exif	1	54309	B msp4009 b9	10-428E-8824+	169584	a109c0d3b2b6661b8	140826641 decc2l	3 192x346548	1670429/4e4016e3e742	waseBdHBr	2023/04/0	8 18/46
-	MIME Type	2	59989	Vacation Pic.dn	ng	1920000	ccefb15066a42de413	303eedc2581d39	8 2e343b81ba	/ea41a7b275be3ff2e6b	lab5aaf589	2021/04/0	8 18:40
	Face Analysis	3	59997	a Facility Images	dmg	2246144	85a5e91508a6c0556	776c454bbe145	5 fdb17c72b1e	12180e2b1ffa141a2462	544b24470	2021/04/0	7 15:12
-	Face Search	4	60027	amptleojgw6f7	scagh9t.jpg	375854	e905c9145bfa9c45fa	07ebfcbc40a4f4	fd64c323842	a7ee02141236424b4633	71d559e00a	2021/04/0	9 10:45
	Optical Character Recognition	5	60527	amptleojgw6f7	scagh9t.jpg	375854	e905c9145bfa9c45fa	07ebfcbc40a4f4	fd64c323842	a7ee02f4f236424b4633	71d559e00a	2021/04/0	9 11:08
	Skin Tone Detection	6	60536	amptleojgw6f7	scagh9t.jpg	375854	e905c9145bfa9c45fa	07ebfcbc40a4f4	fd64c323842	a7ee02f4f236424b4633	71d559e00a	2021/04/0	9 11:03
	Weapons	7	60548	amptleojgw6f7	scagh9t.jpg	375854	e905c9145bfa9c45fa	07ebfcbc40a4f4	fd64c323842	a7ee0214f236424b4633	71d559e00a	2021/04/0	9 11:22
-	Fire Analysis	8	60551	amptleojgw6f7	scagh9t.jpg	375854	e905c9145bfa9c45fa	07ebfcbc40a4f4	fd64c323842	a7ee02f4f236424b4631	71d559e00a	2021/04/0	9 11:16
6	File Extensions	9	60554	hard copy docs	.crypto	7111026	698e2a046ae459987	f8cabab591f4be	24d6d45391	a55a761bd69c5a6595fa	4703967	2021/04/0	9 14:00
	The Extensions	10	73014	86B14C02CDC	4EA5970E688E0	375854	e905c9145bfa9c45fa	07ebfcbc40a4f4	fd64c323842	a7ee02f4f236424b4633	71d559e00a	2021/04/0	9 10:44
2	User Defined File Signatures	11	75924	AF60350DBA6	BAFDCA73E4AD0	375854	e905c9145bfa9c45fa	i07ebfcbc40a4f4	fd64c323842	a7ee02141236424b4633	71d559e00a	2021/04/0	9 10:44
	File Size	12	78708	hard copy docs	crypto	7111026	698e2a046ae459987	7f8cabab591f4be	24d6d45391	a55a761bd69c5a6595fa	4703967	2021/04/0	9 14:00
	Snapshots	13	104974	Detail view of S	paceExped Rove	141616	249b245368f93072a	a9f5c6dafbe9224	3 511b40f8dda	50f03e57cc20bd3b656	ba16d11b	2021/04/0	9 12:40
- 5	Hashset	14	104976	Detail view of S	paceExped Rove	85723	8f989e14e6b7a3d28	1597d48f2656d70	6 e982a40aafd	547d4c04147d733af9	3d3cc319b0	2021/04/0	9 12:40
1	Electric_Car_Documents (0)	15 📋	104977	Detail view of S	paceExped Rove	179523	1868142177c0741516	177d964fa0f834	Odbd7c5fc25	bb1985c1f50147932b4	03d872abf8	2021/04/0	9 12:40
-	Email Files						1.87			200			
P	Artifacts	Source Name: /Wil	liam_Campbell_Ma	Book.dmg/APPLE 5	SD – Data				1				
<b>8</b> 1	Artifacts Keyword Search	Record No.: 54309											
	File Search	File Mamou FRI D 40	50 D050 4335 B		Inne								
	Exif Metadata Search	File Path: /Users/w	illiamcampbell/Pic	tures/Photos Libran	y.photoslibrary/origi	inals/F/F85D40	69-D95C-423E-8E24	-F9A0EBE7BC5E.j	peg				
щ	Content Search	Inode No /File ID:	384520								10 . V.	1.30	1.1
	Artifacts Timeline	File Size: 185.14 K	B (189584 bytes)							-	· 250	1	and.
-	Bucket	Mime Type: image	/jpeg							the second		. 2	-
10	Plist Viewer	Hashset Name: Ele	ctric_Car_Documer	its							2	1	-
ä	Hex Viewer	SHA1: e92e346548	35b7b429f4e4b16e	le742bacc8dff3e							and a second	-	
	RECON	Date Modified: 202 Date Change: 202 Date Accessed: 20 Date Added(Apple Content Creation	21-Apr-08 18:46:2 1-Apr-08 18:54:17 21-Apr-09 14:46 ): 2021-Apr-08 18 Date(Apple): 2021	6 -5:00 -5:00 54 -5:00 :54:17 -5:00 -Apr-08 18:46:26 -	5:00								
	SOMON	Detailed Infor	mation	Hex View	T Text View	S String	s 🖹 Exif Me	stadata (	Apple Metada <	Preview			
					A. 00000000								

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

#### Archiving the Hash Set Database

Favorites	Name	Date Modified     Size		Kind
AirDrop				1 March 199
	> Artifacts_Timeline	Jan 13, 2022 at 9:26 AM		Folder
(e) Recents	Case_Configuration	Today at 5:11 PM		Folder
🙏 Applicati	> Chat_View	Jan 13, 2022 at 9:27 AM		Folder
Desides	> CSVS	Jan 13, 2022 at 9:26 AM		Folder
Desktop	V Hashset	Today at 5:14 PM		Folder
Documents	Electric_Car_Documents.sqlite	Today at 5:14 PM	12 KB	Document
Downloads	hashset_index.sqlite	Today at 5:11 PM	8 KB	Document
O Dominoudo	> Columns > Columns	Jan 13, 2022 at 9:26 AM		Folder
iCloud	Redefined_Result_Filters	Jan 13, 2022 at 9:26 AM		Folder
O iCloud Dri	> Cources	Today at 9:31 AM		Folder
Charad				
Shared				
Locations				
⊖ APPLE ≜				
🖂 Update 🔺				
🖂 EFI 🔺				
⊖ Demo ≜	🖾 Macintosh HD > 🤖 Users > 🔄 chrisgret: > 🚞 D	Desktop > 🛅 Person_c > 🛅 Lab_Conf > 🛅 Hashset >	Electric	_Car_Documents.sq

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

## 22.2 Importing Hash Sets

RECON LAB can import the following hash set database formats:

- RECON LAB SQLite
- Project VIC
- NSRL
- CSV

000				Hashset			
Import 🔽	Crea	te Remove					
SQLite	me	Hide Matc	ned Files				
Project VIC							
NSRL							
CSV							
						Cancel	Apply

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".

Tables	Columns	Data
saved_hashsets	🔵 bookmark	1
software		1
	🔿 md5_hash	f8841d3a2a32f0d9bda967d0c43ab40c
	sha1_hash	
		Save Cancel

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.

Import Create	Remove	
Hashset Name	Hide Matched Files	
1 2_Chuck_Norris		
		Cancel Apply
		Cancel Apply

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

## 22.3 Removing Files From Case Using Hash Sets

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

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

🕘 🔘 🕘	1	ashset		
Import 🔽 Create	Remove			
Hashset Name	Hide Matched Files			
1 Chuck_Norris				
			Const.	
			Cancel	Apply

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

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

To unhide the files uncheck the checkbox and hit "Apply" again.

## 23. Hide or Show Files

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

		<b>A</b>	Record No.	Inode No./File ID	File Name	Extension	File Size	
			Search	Search	Search	Search	Search	Search
1			81614	238330	🚞 Music	1		2022/06
2			81708	184892	.DS_Store		18436	2022/11
3			81709	184889	.CFUserTextEncoding		7	2022/06
4			81710	238424	🚞 Pictures			2022/07
5			82560	185081	.zsh_history		3040	2022/11
6			82561	185094	🚞 Desktop			2022/07
7			82572	185279	🚞 Library			2022/11
8			135180	238168	🚞 Movie-Script-Database			2022/11
9			135252	184890	Cups			2022/07
10			135254	220270	Cites			2022/11

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

Mark As Seen Mark As Unseen Hide Seen Files

Show Seen Files

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

				Record No.	Inode No./File ID	File Name	Extension	File Size	
				Search	Search	Search	Search	Search	Search
1				81614	238330	🚞 Music			2022/06
3				81709	184889	.CFUserTextEncoding		7	2022/06
4				81710	238424	Pictures			2022/07
6				82561	185094	🔁 Desktop			2022/07
7				82572	185279	🛅 Library			2022/11
8				135180	238168	📄 Movie-Script-Database			2022/11
10				135254	239279	Sites		122	2022/11
11				135256	239275	Public 📃			2022/06
12				135260	238240	Movies			2022/06
13			<b>F</b>	135350	184894	Trach			2022/11
55	Khan M	lac >	Users >	thewrath >					

# 24. Project Vic

RECON LAB supports Project VIC database formats Versions 1.1, 1.2 and 1.3. For more information about Project VIC please visit their website here: <u>https://www.projectvic.org</u>

#### **Exporting as Project VIC Format**

		Record No.	Inode No./File ID	File Name	Extension	File Size		Date M	odified		Date Change
		Search	Search	Search	Search	Search	Search			Search	
1		82562	185102	Screen Shot 2022-06-26 at 9.59.21	png	40373	2022/06/26	11:59:20	5 -5:00	2022/12/0	06 17:58:30 -5:00
2		82563	185097	B IMC_0081.jpeg	jpeg	2545906	2022/06/21	10:30-1	2 -5:00	2022/12/0	06 17:58:30 -5:00
3		82564	185095	.DS_Store		Bookmark		E.	0 -5:00	2022/12/0	6 17:58:30 -5:00
4		82565	185103	- Screen Shot 2022-07-21 at 2.32.33	png	Notes			9 -5:00	2022/12/0	06 17:58:30 -5:00
5		82566	185096	localized		Oulek Look			7 -5:00	2022/12/0	06 17:58:30 -5:00
6		82567	185099	Its going to be mine.jpeg	jpeg	Open With			4 -5:00	2022/12/0	06 17:58:30 -5:00
7		82568	185104	Screen Shot 2022-07-21 at 6.51.40	png	Open Detailed	Information		5 -5:00	2022/12/0	06 17:58:30 -5:00
8		82569	185100	Production Presentation alias		Copy to Clipbe	pard		4 -5:00	2022/12/0	06 17:58:30 -5:00
9		82570	185098	IMG_0144.jpeg	jpeg	Send To Bucke	et	•	8 -5:00	2022/12/0	06 17:58:30 -5:00
10	1	82571	185101	🛓 nroait ndf	ndf	Add To Text I	ndexing Queue		5 -5.00	2022/12/0	06 17:58:30 -5:00
ᡠ Khan_N	lac > 🗋	Users > 🔚 thew	rath > 🛅 Desktop >			Carve		•			
Source Na	me: /20	023 Class Image.dr	ng/Khan_Mac			Face Search	n Modules				
Record No	.: 8256	3 081 iper				Add file to has Search file wit	shset database h same hash	•			
File Path:	/Users/	thewrath/Desktop/	IMG_0081.jpeg			Export Hashes	As		VIC Version 1.1		
Inode No.	/File ID	: 185097				Export			VIC Version 1.2 VIC Version 1.3	MA -	
File Size: Mime Typ	2.43 MB e: imag	(2546906 bytes) e/jpeg )22-lun-21 10:30:1	2 -5:00			Seen Decompress F Ust Related Fl	ile. Ies	•	VIC Version 2.0 SQLite CSV		
Date Char Date Acce Date Crea	nge: 202 ssed: 2 ted: 20	22-Dec-06 17:58:3 022-Dec-20 13:54 22-Jun-21 10:30:1	0 -5:00 :19 -5:00 2 -5:00								
Date Adde Content C Content N Last Used	ed(Appl reation lodifica Date(A	le): 2022-Dec-06 1 Date(Apple): 2022 tion Date(Apple): 2 tion Date(Apple): 2	7:58:30 -5:00 !-Jun-17 13:34:43 -5:00 2022-Jun-17 13:34:43 -! 1 10:26:10 -5:00	5:00						1/	
<b>Used Date</b> 2022-Jun-	es(Appl 20 23:0	'e): 00:00 -5:00									
Use Coun	t: 1										
Tan						-					
Det Det	ailed Inte	ormation	<ul> <li>Optical Character Reco</li> </ul>	ignition 🔛 Hex View T	lext View	Strings	Exif	<>>	Preview		

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



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

# 25. Email Analysis

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

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



#### **Automated Artifacts Analysis**

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

« »		Artif	acts		\$ X				Mail (83	5)		+	x							
Keywo	rd Sea	rch		Tim	e Line	Search	Show	All					Exp	ert H	TML	0	Tags	0	Repo	rt
Acco	unts	Contacts List	VIP C	ontacts	Messages	All Attack	hments	Open Attachmer	nts Signature	Smart Mailboxes	Rules	Received Attachments	Files Re	ents	Mail Data	Ap	pointments	Call H	story	4( Þ
-		Tag Rec	ord No.	System	Account	Use	r Name	Acco	unt Description	Date	e Added		Signa	ture						
1			1	jermyn		alfred.jermyn	i i													
2			2	jermyn		alfred.jermyn	1													
3			3	jermyn		alfred_jermyr	n@yahoo.e	com												
4			4	jermyn		alfred.jerymn	1													
Accou Accou Accou Hostn ISP Ac Port N SMTP Server Vendo Archie Draft I Exami Sent n ToDos Trash Status Last S Date A Signat	nt ID: f nt Nam nt Path nt Type ame: in count I umber: count I umber: r: Goog ve Mail Mailbox Mailbox Mailbox Mailbox : Active vnc Dat	478f027-d346 e: Cmail : /Users/macbo e: IMAPAccount nap.gmail.com D: IMAP 0: IMAP : 993 er: smtp.gmail. Gimap gle, Inc. Ibox Name: Arrol c Name: Drafts tes Mailbox Nan name: Sent Me c Name: Deleted e te: 2013-Jun-07	42cd-8 y/RECO com:alfr nive ne: Note ssages Mail To Messag	S42-c442 N_TMP/RE ed.jermyn s Do jes 49 GMT-4	0d7d5b50 (CON_moun @gmail.com	t_path/RECO	N_MNT_di	iskS_Jermyn_Imag	e.dmg/Users/jen	myn/Library/Mail/V2	/IMAP-alf	red.jermyn@imap.gmail.cr	m		N	lo Pre	view Availabl	le		
Artifad	ure: Its Soul	rce File:																		
Artifa	ts Sou	rce: /Users/jern	ıyn/Libr	ary/Maii/\	/2/MailData	/Accounts.pl	list													
2	Detaile	d Information		Hex V	iew	T] Text Vie	tw	S Strings	Exif Me	tadata 🛛 🕵	Apple Meta	data 🛛 🏄 Maps		Pr	review					

#### 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.

) Search	Filters	Shov	N All					
ı				-			5.11.4	P. e. d
		57		10	From	u	Subject	Datetime
		57		Rufus McGregor	afred jerniyn		Temen	2013/03/11 08:44:00 GMT-
		50		Rufus McCregor	alfred Jermyn		Avoid an Audit	2013/03/06 12:25:00 GMT-
		60		Kulus mediegoi	arreujerniyn	alfred ierminitemail.com	Colo Romano	2013/03/04 17:03:00 GMT-
		61	-	Rufus McCreaor	alfred lermyn	an i Eu Jei in ynigeg nam e un	Check it out	2013/02/20 06:33:00 CNT-
		62		Rufus McGregor	alfred jermyn		Fake Accounts	2013/01/10 17:08:00 CNT-
		63		alfred iermyn@amail.co	Sam Aye		The BOOK	2012/08/29 09:33:00 CNT-
		64		alfred.iermyn@gmail.com	=?utf-8?O?tripwoif?=		tripwolf Newsletter: Wa	2013/03/06 16:25:00 GNT-
		65			"tripwolf"		your personal tripyolf t	2013/03/06 17:25:00 CMT-
		66		Rufie	alfred iermyn	alfred iermyn@omail.com	Crin Removal	2013/03/04 16:54:00 CNT-
		67	-	Mike I	Mike	and an general regenetit.com	Android	2012/10/18 08:58:00 CNT-
2		68	H	alfred iermyn@amail.com	Mike		Toyota Repair Los	2012/09/16 09:37:00 CMT-
hoo.com		69	ä	Atin Bansal	Nike		Toyt VIN	2012/09/06 16:35:00 GNT-
		70	ä	Rufie	alfred iermyn	alfred.iermvn@omail.com	Grin Removal	2013/03/04 16:54:00 GMT-
		71		Rufia	alfred Jermin	alfred jermyn@gmail.com	Crip Removal	2012/02/04 16:54:00 CNT
							No P	review Available
	ıhoo.com n⊛imap.gmail.c	ıhoo.com n@imap.gmail.com/Sent Message Message	ihoo.com 64 65 66 70 70 70 70 70 70 Message .mbo	ihoo.com	64 alfred.jermyn@gmail.com 65	64       alfred.jermyn@gmal.com       =7utf-87Q?tripwolf?=         65       """"""""""""""""""""""""""""""""""""	64       alfred.jermyn@gmail.com       =?utf-87Q?tripwolf?=         65       **       *tripwolf?         66       Rufie       alfred.jermyn@gmail.com         67       Mike L       Nike L         68       alfred.jermyn@gmail.com       Nike L         69       Atin Bansal       Nike L         70       Rufie       alfred.jermyn@gmail.com         70       Rufie       alfred.jermyn         alfred.jermyn@gmail.com       #ifred.jermyn@gmail.com         70       Rufie       alfred.jermyn         alfred.jermyn@gmail.com       #ifred.jermyn@gmail.com         m@imap.gmail.com/Sent Messages.mbox/4386658C-0494-0480-AA27-61DE83919560/Data/Messages/616.partial.emk         Message       Attachments         Search       Search	64       alfred.jermyn@gmal.com       =?utf-&?Q?tripwolf?=       tripwolf Newsitetter: WL         65       Rufie       alfred.jermyn@gmal.com       Grip Removal         66       Rufie       alfred.jermyn@gmal.com       Grip Removal         67       Mike L       Android       Android         68       alfred.jermyn@gmal.com       Nike L       Android         69       Atin Bansal       Nike       Toyota Repair Log         69       Atin Bansal       Nike       Toyota Repair Log         71       Rufie       alfred.jermyn@gmal.com       Grip Removal         71       Rufie       alfred.jermyn@gmal.com       Grip Removal         71       Rufie       alfred.jermyn@gmal.com       Grip Removal         71       Rufie       alfred.jermyn       alfred.jermyn@gmal.com       Grip Removal         10       Rufie       alfred.jermyn       alfred.jermyn@gmal.com       Grip Removal         11       Rufie       alfred.jermyn@gmal.com       Grip Removal         12       Rufie       Search       Search       No P

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

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

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

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

#### **Attachments**

Starch       Filter       Stow All         Accounts       C       Subject         AdMAA-alled_pirmyn       Vinen       CC       Subject         AdMAA-alled_pirmyn       Vinen       Staranting       2013/00/1         MAM-alled_pirmyn       Staranting       2013/00/1         Sig (fmail_motox       Sig (fmail_motox       Sig (fmail_motox       Sig (fmail_motox       Sig (fmail_motox         Sig (fmail_motox	K Email Files	÷×					emix		\$ X		
Accounts     To     From     Cc     Subject       > D051889-29A2-4828-2918-A24803990D108     52     Rufus Micregor     alfred jermyn     Expanding     2013/03/0       Y     Consulted jermyn     Expanding     2013/03/0     Axold Ax-Jalifed jermyn     Axold Ax Jalifed 2013/03/0       Y     Consulted jermyn     Anold Ax-Jalifed jermyn     Axold Ax Jalifed 2013/03/0     Axold Ax Jalifed 2013/03/0       Y     Consult index     61     Rufus Micregor     alfred jermyn     Axold Ax Jalifed 2013/03/0       Y     Consult index     61     Rufus Micregor     alfred jermyn     Check Hout     2013/03/0       Y     Consult index     61     Rufus Micregor     alfred jermyn     Check Hout     2013/03/0       Y     Consult index     61     Rufus Micregor     alfred jermyn     alfred jermyn     File Accounts     2013/03/0       Y     Consult index     61     Rufus Micregor     alfred jermyn     alfred jermyn     general 2013/03/0       Y     Sent Missages:mbox     66     Rufus     alfred jermyn     alfred jermyn gigmal.com     Crie Revolut     2013/03/0       Y     Sent Missages:mbox     66     Rufu     alfred jermyn gigmal.com     Crie Revolut     2013/03/0       Y     Mide Internal     Mike I     Micregor <th>(</th> <th></th> <th>Search</th> <th>Filters 🔽</th> <th>Shov</th> <th>N All</th> <th></th> <th></th> <th></th> <th></th> <th></th>	(		Search	Filters 🔽	Shov	N All					
D 05 1820 - 2592 - 4582 - 2518 - 32 03 950D 108       2 0       Rufus Mick-regor       alfred jermyn       Yean       2013/02/14         A 041MAP-alfred jermyn@mang mull.com       58       Rufus Mick-regor       alfred jermyn       Acada Audit       2013/02/14         Y 0       [Cmail].mox       60       Bufus Mick-regor       alfred jermyn       alfred jermyn       Acada Audit       2013/02/14         Y 0       [Cmail].mox       60       Bufus Mick-regor       alfred jermyn       Check to Q4       2013/02/12         Y 0       [Instructure]       61       Rufus Mick-regor       alfred jermyn       Check to Q4       2013/02/12         Y 1       [Instructure]       62       Rufus Mick-regor       alfred jermyn       Check to Q4       2013/02/12         Y 1       [Instructure]       Rufus Mick-regor       alfred jermyn       Check to Q4       2013/02/12         Y 1       [Instructure]       Rufus Mick-regor       alfred jermyn       Check to Q4       2013/02/12         Y 1       [Instructure]       Rufus Mick-regor       alfred jermyn@gmail.com for Back to Q11/02/16       2012/02/12         Y 1       [Instructure]       Rufus Mick-regor       alfred jermyn@gmail.com for Back to Q12/02/12       2013/02/02         Y 2       [Instructure]       R	Accourt	nts					To	From	CC	Subject	Datetime
<ul> <li>AndMA-aifred.jermyn@imag.gmail.com</li> <li>MAMP-aifred.jermyn@imag.gmail.com</li> <li>MAMP-aifred.jermyn@imag.gmail.com</li> <li>Rufus MGCregor</li> <li>Rufus MGCregor</li></ul>	D691BE09-29A2-4F82-9218-A24D3990	DD1D8			57		Rufus McGregor	alfred jermyn		Yemen	2013/03/11 08:44:00 GMT
MM-alfred_jermyn@mag.pmal.com       59       Bufts MGCregor       alfred_jermyn       Acoda a. Adat       2013/03/0         * 91       Goralls.mbox       60       Kufts MGCregor       alfred_jermyn       Acoda a. Adat       2013/03/0         61       Kufts MGCregor       alfred_jermyn       Check it out       2013/03/0         62       Rufts MGCregor       alfred_jermyn@mal.com       Check it out       2013/03/0         63       Rufts MGCregor       alfred_jermyn@mal.com       Check it out       2013/03/0         63       Rufts MGCregor       alfred_jermyn@mal.com       Check it out       2013/03/0         64       alfred_jermyn@mal.com       Sam Ake       The BOOK       2013/03/0         64       alfred_jermyn@mal.com       alfred_jermyn@gmal.com       Check it out       2013/03/0         65       Rufts       alfred_jermyn@gmal.com       Check it out       2013/03/0         70       Nake Kanget mbox       66       Rufts       alfred_jermyn@gmal.com       Check it out       2013/03/0         70       Make L       Antridigermyn@gmal.com       Antridigermyn@gmal.com       Check it out       2013/03/0         70       Make L       Antridigermyn@gmal.com       Antridigermyn@gmal.com       Check it out       2013/03/0<	AosIMAP-alfred.jermyn				58		Rufus McGregor	alfred jermyn		Expanding	2013/03/06 12:25:00 GMT
	IMAP-alfred.jermyn@imap.gmail.com				59		Rufus McGregor	alfred jermyn		Avoid an Audit	2013/03/04 17:05:00 GMT
<ul> <li></li></ul>	🔻 📬 [Gmail].mbox				60		Rufe	alfred Jermyn	alfred.jermyn@gmail.com	Grip Renoval	2013/03/04 16:54:02 GMT
9         Inportant.mbox         62         affred.jemmy@gmail.co.         affred.jemmy@gmail.co.         The BOOK         2012/01/2           9         Mikal.mbox         63         affred.jemmy@gmail.co.         m/aff-d.RQPtrpwof7#         tripwol7         tripwol7         2013/01/0           9         Mikal.mbox         65         *         tripwol7         your personal tripwol7.         2013/01/0           9         Mikot.mbox         65         *         tripwol7         your personal tripwol7.         2013/01/0           9         Mikot.mbox         65         *         tripwol7         your personal tripwol7.         2013/01/0           9         Mikot.mbox         65         Rufe         affred.jemmy@gmail.co.         fifred.jemmy@gmail.co.	📲 Drafts.mbox				61		Rufus McGregor	alfred jermyn		Check it out	2013/02/20 06:33:00 GM
9         Snit Mall.nibox         63         affed.jermyn@gmall.com         Snit Ake         The BOOK         2012/05/1           9         Mi Mali.nibox         64         affed.jermyn@gmall.com         Snit Akg.Zprtpwol7/2         tripwol7/100/100/100/100/100/100/100/100/100/10	The Important.mbox				62		Rufus McGregor	alfred jermyn		Fake Accounts	2013/01/10 17:08:00 GM
************************************	Sent Mail.mbox				63		alfred.jermyn@gmail.co	Sam Axe		The BOOK	2012/08/29 09:33:00 GM
************************************	T All Mail.mbox				64		alfred.jermyn@gmail.com	=?utf-8?Q?tripwolf?=		tripwolf Newsletter: Wa	2013/03/06 16:25:00 GM
Sent Messages.mbox       66       Rufie       alfred jermyn@gmail.com       Grip Renoval       2013/03/0         Sent.mbox       Mike L       Mike L       Android       2012/09/1         F       Mike L       Mike L       Android       2012/09/1         68       Atin Bansal       Mike       Toyota Repair Log       2013/03/0         71       Bute       alfred jermyn@gmail.com       Grip Renoval       2013/03/0         71       Bute       Renoving One piece grips from Sig pdf       Quicklook       Open in Source       Yes         1       Removing One piece grips from Sig pdf       Quicklook       Open in Source       Yes         No Preview Availa       No	INBOX mbox				65		-	"tripwolf"		your personal tripwolf t	2013/03/06 17:25:00 GM
Ger in the second	Sent Messages mbox				66		Rufie	alfred jermyn	alfred.jermyn@gmail.com	Grip Removal	2013/03/04 16:54:00 GM
IMAP-afred_jermyn@yahoo.com@imap.mail.yahoo.com       68       alfred.jermyn@yahoo.com@imap.mail.yahoo.com       70       Catina Banisal       Mike       Toyota Repair Log       2012/09/0         07       Catina Banisal       Mike       alfred.jermyn@yahio.com       Toyota Repair Log       2012/09/0         07       Catina Banisal       Mike       alfred.jermyn@yahio.com       For Renoval       2013/03/0         1       Refine       Quicklook       Open in Finder       File baist       Toyota Repair Log       2013/03/0         1       Removing One piece grips from Sig pdf       Quicklook.       Open in Source       Yes       No Preview Availa	The sent messages.mov				67		Mike L	Mike L		Android	2012/10/18 08:58:00 GM
Impervanted entry flegratio.Colling integration of the same	<ul> <li>MAR alfred instrum@uabox com@iman n</li> </ul>	milunhar			68	101	alfred.jermyn@gmail.com	Mike L		Toyota Repair Log	2012/09/16 09:37:00 GM
70         Rufie         aifred jermyn         aifred jermyn@gmail.com         Grip Removal         2013/03/0           71         Brike         aifred jermyn         aifred jermyn@gmail.com         Grip Removal         2013/03/0           Users/jermyn/Ubrary/Mail/V2/IMAP-alfred.jermyn@gmail.com         Grip Removal         2013/03/0           Message         Attachments         Raw Data           I         Removing One piece grips from Sig.pdf         Quicklook         Open in Source         Yes	<ul> <li>MAC-anteo_ennyn@yanoo.com@inap.n</li> </ul>	nan.yanou	o.com		69		Atin Bansal	Mike		Toyt VIN	2012/09/06 16:35:00 GM
Users/jermyn/Library/Mail/V2/IMAP-alfred.jermym@imap.gmail.com/Sent Message         New Subsection         Stend iarmum@innail.com         Crin Ramoual         2013/03/0           Users/jermyn/Library/Mail/V2/IMAP-alfred.jermym@imap.gmail.com/Sent Message         Message         Matematic         Raw Data         2013/03/0           I Removing One piece grips from Sig.pdf         Quicklook         Open in Finder         File Exist         Image: Communic					70		Rufie	alfred jermyn	alfred.jermyn@gmail.com	Grip Removal	2013/03/04 16:54:00 GM
Users/jermyn/Library/Mail/V2/IMAP-alfred.jermyn@imap.gmail.com/Sent Messages.mbox/4386658C-0949-4080-AA27-61DE83919560/Data/Messages/616.partial.emtx  Message Attachments Raw Data  Filename Quicklook Open in Finder File Exist  Removing One piece grips from Sig.pdf Quicklook Open in Source Yes  No Preview Availa					71	m	Rufie	alfred iermvn	alfred iermvn@amail.com	Grin Removal	2013/03/04 16-54-00 CM
	1 Removing One piece grips from Sig.pdf	Quickloo	<u>ok</u>	Open in Sc	uurce.		Yes			No P	review Available

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".

#### <u>Viewing Message As Raw Data</u>

				emix		• ×		
Search Fil	ters	Show	All					
Accounts				То	From	Cr.	Subject	Datetime
D6918E09-29A2-4F82-9218-A24D399DD1D8		57	-	Rufus McGregor	alfred lermyn	cc	Yemen	2013/03/11 08:44:00 GMT-
AosIMAP-alfred.jermyn		58	n	Rufus McGregor	alfred jermyn		Expanding	2013/03/06 12:25:00 GMT-
IMAP-alfred.jermyn@imap.gmail.com		59	m	Rufus McGreoor	alfred jermyn		Avoid an Audit	2013/03/04 17:05:00 GMT-
🔻 📲 [Gmail].mbox		60	ā	Rufie	alfred iermyn	alfred.iermvn@omail.com	Crip Removal	2013/03/04 16:54:00 GMT
📲 Drafts.mbox		61	Π	Rufus McGregor	alfred jermyn		Check it out	2013/02/20 06:33:00 GMT
7 Important.mbox		62		Rufus McGregor	alfred jermyn		Fake Accounts	2013/01/10 17:08:00 GMT-
🧐 Sent Mail.mbox		63		alfred.jermyn@gmail.co	Sam Axe		The BOOK	2012/08/29 09:33:00 GMT
All Mail.mbox		64	0	alfred.jermyn@gmail.com	=?utf-8?Q?tripwolf?=		tripwolf Newsletter: Wa	2013/03/06 16:25:00 GMT-
C INBOX mbox		65			"tripwolf"		your personal tripwolf t	2013/03/06 17:25:00 GMT
Sent Messages mbox		66		Rufie	alfred jermyn	alfred.jermyn@gmail.com	Crip Removal	2013/03/04 16:54:00 GMT
Sent mbox		67		Mike L	Mike L		Android	2012/10/18 08:58:00 GMT-
<ul> <li>IMAD alfred iarmun@uaboa com@imaa mail uaboa com</li> </ul>		68		alfred.jermyn@gmail.com	Mike L		Toyota Repair Log	2012/09/16 09:37:00 GMT-
MAX-arred_lermyn@yanoo.com@imap.mar.yanoo.com		69		Atin Bansal	Mike		Toyt VIN	2012/09/06 16:35:00 GMT-
		70		Rufie	alfred jermyn	alfred.jermyn@gmail.com	Grip Removal	2013/03/04 16:54:00 GMT-
		71	.n	Rufie	alfred iermun	alfred iermun@amail.com	Crin Removal	2013/03/04 16-54-00 CMT.
Statut Later		18	Search					
1235 Return-Path: <alfred.jermyn@gmail.com> Return-Qath: <alfred.jermyn@gmail.com> Received: from [10.0.13] (c-24-91-79-203.hsd1.nh.comcast.net. [24, by mz.google.com with ESNTP5 id hritm39802340qeb.3.2013.03.04, (version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128); Mon, 0- 17:34-23 -0800 (PST) Fom: alfred.jermyn</alfred.jermyn@gmail.com> Content-Type: multipart/mixed; boundary="Apple-Mail_24396C30-1DF0-4C8C-A639-10E38DAFE90 Subject: Grip Removal Date: Mon, 4 Mar 2013 20:54:21 -0500 Message-Id: &lt;1FEB9698-5637-496A-9088-09A9B178D6F8@gmail.com Cc: alfred.jermyn@gmail.com To: Rufle <rurnyn@gmail.com> Mime-Version: 1.0 (Mar OS X Mail 6.2 \(1499\))) X-Mailer: Apple Mail (2.1499) Apple-Mail= 42396C30-1DF0-4C8C-A639-10E38DAFE905 Content-Transfer-Encoding: QUOTED-PRINTABLE Content-Type: TEXT/PLNH; charset=windows-1252 Hey, just FY1 I found out what that tool is for=85.</rurnyn@gmail.com></alfred.jermyn@gmail.com>	.91.79.203]) .17.54.22 4 Mar 2013 05"		Search				No P	review Available
1235 1235 Received: from [10.0.1.3] (-24-9]-79-203.hsd1.nh.comcast.net. [24, by mc_google.com with ESNTP5 id h-Inm39892340qeb.3.2013.03.04, (version=TLSV1 cipher=ECDHE-RSA-RC4-SHA bits=128/128); Mon, 0- 17:54:23 - 0800 (PST) Fom: alfred jermyn <alifred.jermyn@gmail.com> Content=Type: multipart/mixed; boundary="Apple-Mail=24396C30-1DF0-4C8C-A639-10E38DAFE9( Subject: Grip Removal Date: Mon, A Mar 2013 20:54:21 - 0500 Message-Id: <ifeb9698-5637-496a-9088-09a9b178d6f8@gmail.co Cc: alfred.jermyn@gmail.com&gt; Mime-Version: 1.0 (Mac OS X Mail 6.2 \(1499\)) X-Mailer: Apple Mail (2.1499) Apple-Mail= 42396C30-1DF0-4C8C-A639-10E38DAFE905 Content-Type: TEXT/PLAIN; charset=windows-1252 Hey, just PY1 I found out what that tool is for=85. -AJ</ifeb9698-5637-496a-9088-09a9b178d6f8@gmail.co </alifred.jermyn@gmail.com>	.91.79.203]) 17.54.22 4 Mar 2013 05°		Search				No P	review Available

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

#### Advanced Searching

🔊 Email Files 🗢 🌣			EMLX Mail		\$ X			
) Search Filters	- Show	All						Advanced Search
Accounts		Sr. No.	То	From	Cc		Subject	Datetime
AosIMAP-alfred.jermyn	1	745 🗔	Rufus McGregor	Alfred Jermyn	,	'ou get	the account?	2013/01/11 04:43:00 -4:00
IMAP-alfred.jermyn@imap.gmail.com	2	744 🖂	Rufus McGregor	alfred jermyn	,	dy Yaho	o Account	2013/01/07 12:09:00 -4:00
IMAP-alfred_jermyn@yahoo.com@imap.mail.yahoo.com	3	743 🖂	alfred jermyn	RM	1	te: My 1	ahoo Account	2013/01/08 03:41:00 -4:00
	4	742 🔲		Email Search			o Yahoo!	2013/01/07 17:04:24 -4:00
	5	741 🗌	Easth contant				IOK	2012/08/29 10:29:00 -4:00
	6	740 🗌	pearen concent				IOK	2012/08/29 10:22:00 -4:00
	7	739 🗔	Subject Subject		contain	e	IOK	2012/08/29 10:02:00 -4:00
	8	738 🔲	From Sender		contain	0	IOK	2012/08/29 09:36:00 -4:00
	9	737 🗔					is Docs	2013/03/15 15:19:00 -4:00
	10	736 🗔	To Receiver		contain			2013/03/11 08:44:00 -4:00
	11	735 🗔	Cc Cc		contain		into Japan	2013/03/09 04:01:00 -4:00
	12	734 🔲	Court in America					2013/03/06 12:25:00 -4:00
	13	733 🔲	Contain Attachments	NO YES			udit	2013/03/04 17:05:00 -4:00
	14	732 🔲	Date (UTC) Detwee	n © From 30/12/09.01	30 Y To 30/12/19/01/3	9 👻	val	2013/03/04 16:54:00 -4:00
	15	731 🖂					stuff	2013/02/21 16:29:00 -4:00
	16	**** FTL:		Search				2012102120.00.22.00.1.00
	Message	Attachments	Raw Data					
earch Text		Search						

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

## 26. Timeline Analysis

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

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

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

### 26.1 Super Timeline



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

Output Format 🧿 SQLite 🛛 CSV	Number of Records per C	5V file. Defaul	t is 1000000
ecords: File System Records	Artifacts Plugin Records	O Both	
ile Name Super_Timeline			
ile Path /Volumes/DEST/			
tart Time 2019/Jan/01 07:00	<b>~</b>	End Time	2019/Oct/20 21:08
			Cancel OK

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.

					Database Structure	owse Data Edit Pragmas Execute SQL			
able	e 🔲 timeline	data				1	a 😰 😼	New Record	Delete Record
	NT	Timestamp	Stamp_Name	Stama_Type	Source	item1	iten2	Plugin	Category
	Fiter	Ther	Fitar	Fiter	fibur	aumuni	Filter	Filter	Filter
	3	2019/01/01 14:14:26 GMT-4:00	Modification Time	MODIF	/CATALINA.spasseimage/CATALINA	.SUMURI NEW LOGO WHITE.key.icloud	/Users/macboy/Library/Mobile Documents/com~apple~K	File System	Files
	1003	2019/01/04 19:10:42 GMT-4:00	Modification Time	MODIF	/CATALINA.spaseimage/CATALINA	_SUMURI_Logo_White.pxm.preview.idoud	/Users/macboy/Ubrary/Mobile Documents/4R6749AYRE	File System	Files
	1008	2019/01/08 09:13:50 GMT-4:00	Date Modified	DTMOD	/CATALINA.spatseimage/CATALINA	SUMURI Website	NOL2.	Notes	Notes
	1786	2019/02/08 11:53:15 GMT-4:00	Modification Time	MODIF	/CATALINA.spaseimage/CATALINA	.SUMURI WALLPAPER.kzy.icloud	/Users/macboy/Library/Mobile Documents/com~apple~K	File System	Files
	1917	2019/02/21 16:28:04 GMT-4:00	Modification Time	MODIF	/CATALINA.sparseimage/CATALINA	.Samuri_Flyers_Lab_SampleFront copy.pxm.preview.icloud	/Users/macboy/Library/Mobile Documents/4R6749AYRE	File System	Files
	7088	2019/02/26 13:22:44 GMT-4:00	Date Modified	DTMOD	/CATALINA.sparseimage/CATALINA	SUMURI Software Update Links	NUL	Notes	Notes
	7477	2019/03/15 21:27:07 GMT-4:00	Date Modified	DTMOD	/CATALINA.spaseimage/CATALINA	URL: http://sunuri.com/newstage	NAL	Notes	Notes
	7522	2019/03/21 01:22:46 GMT-4:00	Modification Time	MODIF	/CATALINA.spatieimage/CATALINA	.SUMURI Website Map.mindnode.icloud	Alsers/macboy/Ubrary/Mobile Documents/W6L39UYL6Z	File System	Files
	27775	2019/05/15 21:46:49 GMT-4:00	Modification Time	MODIF	/CATALINA.sparseimage/CATALINA	.SUMURI Giveaways.pdf.icloud	/Users/macboy/Library/Mobile Documents/com~apple~P	File System	Files
)	27776	2019/05/15 21:46:49 GMT-4:00	Modification Time	MODIF	/CATALINA spaseimage/CATALINA	SUMURI Gweaways.pdf	/Users/macboy/Recovered Files - Aug 30, 2019 at 10:0	File System	Files
1	27778	2019/05/16 01:46:49 GMT-4:00	Content Creatie	CNCRT	/CATAUNA.sparseimage/CATALINA	SUMURI Greaways.pdf	/Users/macboy/Recovered Files - Aug 30, 2019 at 10:0	File System	Files
£	27779	2019/05/16 01:46:49 GMT-4:00	Content Modific	CNMOD	/CATALINA.spaseimage/CATALINA	SUMURI Greaways.pdf	/Users/macboy/Recovered Files - Aug 30, 2019 at 10:0	File System	Files
	11129	2019/06/10 10:35:01 GMT-4:00	Modification Time	MODIF	/CATALINA spasseimage/CATALINA	SUMURI Organizational Chart - 2018-11.key.icloud	Alsers/macboy/Library/Mobile Documents/com-spple-K	File System	Files
۴	17772	2019/07/05 08:43:44 GMT-4:00	Modification Date	MODIF	/CATALINA.spatseimage/CATALINA	Sumuri - Forensics Simplified - Administration		Google Chrome	Synced Data
5	77779	2019/07/05 08:45:17 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spatseimage/CATALINA	Inbox (3) - swhalen@sumuri.com - SUMURI LLC Mail	https://mail.google.com/mail/?pli=1#	Google Chrome	History
5	77780	2019/07/05 (8:45:17 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spessimage/CATALINA	Intex (3) - swhalen@sumuri.cem - SUMURI LLC Mail	https://mail.google.com/mail/u/0/?sli-1#	Google Chrome	History
7	77781	2019/07/05 (8:45:17 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spasseimage/CATALINA	Inbox (3) - swhalen@sumuri.com - SUMURI LLC Mail	https://mail.google.com/accounts/SetOSiD?authuser=0&	Google Cyrome	History
8	17782	2019/07/05 08:45:17 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spaseimage/CATALINA	Inbox (3) - swhalen@sumuri.com - SUMURI LLC Mail	https://mail.google.com/mail/u/0/W	Google Chrome	History
2	77783	2019/07/05 68:45:17 GMT-4:00	Last Vist Time	LVIST	/CATALINA.spetielimage/CATALINA	Intex (3) - swhalen@sumuri.csm - SUMURI LLC Mail	https://sccounts.google.com/ServiceLogin?service-mail&	Google Chrome	History
)	77784	2019/07/05 09:25:30 GMT-4:00	Date Modified	DTMOD	/CATALINA.sparseimage/CATALINA	SUMURI Remote Google Neet, Huddle Code	MAL	Notes	Notes
£	266919	2019/07/17 22:02:52 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spaseimage/CATALINA	SUMURI LLC Mail	https://mail.google.com/mail/	Google Chrome	History
2	200920	2019/07/17 22:02:52 OMT-4:00	Last Vialt Time	LVIST	/CATAUNA.apatasimaga/CATAUNA	SUMURI LLC Mail	https://gmail.com/	Google Chrome	History
3	266921	2019/07/17 22:02:52 GMT-4:00	Last Visit Time	LVIST	/CATALINA.sparseimage/CATALINA	SUMURI LLC Mai	http://gnail.com/	Google Chrome	History
\$	266922	2019/07/17 22:02:52 GMT-4:00	Last Visit Time	LVIST	/CATALINA.sparseimage/CATALINA	SUMURI LLC Mail	https://www.google.com/gmail/	Google Chrome	History
•	760427	2019/08/07 22:59:38 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spasemage/CATALINA	Intex (1) - swhalen@sumun.com - SUMURI LLC Mail	https://mail.goxgte.com/mail/u/0/	Google Chrome	History
	784759	2019/08/08 22:44:46 GMT-4:00	Last Vist Time	LVIST	/CATALINA.sparseimage/CATALINA	SUMURI LLC - Calendar	https://calendar.google.com/calendar/b/1/r	Safari	History
	784760	2019/08/08 22:44:47 GMT-4:00	Last Visit Time	LVIST	/CATALINA.spasseimage/CATALINA	SUMURI LLC - Calendar - August 2019	https://calendar.google.com/calendar/b/1/r	Səfari	History
5	784761	2019/08/08 22:44:50 GMT-4:00	Last Visit Time	LVIST	/CATALINA.sparseimage/CATALINA	SUMURI LLC - Calendar - August 2019	https://calendar.google.com/calendar/b/1/r	Safan	History
•	784762	2019/08/08 22:44:51 GMT-4:00	Last Visit Time	L'AST	/CATALINA.sparseimage/CATALINA	SUMURI LLC - Calendar - August 2019	https://calendar.google.com/calendar/b/1/r	Safari	History
2	784763	2019/08/08 22:44:52 GMT-4:00	Last Visit Time	LVIST	/CATALINA.sparseimage/CATALINA	SUMURI LLC - Calendar - Auouat 2019	https://calendar.google.com/calendar/b/1/r	Sefari	History
(	4 1- 30 of	2376				Go to: 1			

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

## 26.2 Artifacts Timeline

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



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



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



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



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

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



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

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



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

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

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



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

··· //								and design	
									Export Save Ci
-	Artifacts List			G	raph View Sa	fari-Sep-2019	Safari-Thu 24	-Jan-2013	
Munin Coore	ab a second s		Timestamp	Type	Record No.	Plugin	Category	item 1	Item 2
Plugin searc		61 🗌	2013/01/24 13:58:24 GMT-4	LVIST	7063	Safari	History	Cheaper Than Dirt - America's	http://www.cheaperthandirt.c
lugins		62 🖂	2013/01/24 13:58:50 GMT-4	LVIST	7062	Safari	History	Fobus Holster	http://www.fobusholster.com/
Arpor	t WirelessNetwork	63 🗌	2013/01/24 13:58:58 GMT-4	LVIST	7061	Safari	History	Fobus Holster: Thumb Lever H	http://www.fobusholster.com
Rash H	listory	64	2013/01/24 13:59:06 GMT-4	LVIST	7060	Safari	History	Fobus Holster: Compact Holst	http://www.fobusholster.com
✓ Blueto	oth	65 🗌	2013/01/24 13:59:10 GMT-4	LVIST	7059	Safari	History	Fobus Holster: Thumb Break H	http://www.fobusholster.com
Calend	dar	66 🗆	2013/01/24 13:59:38 CMT-4	LVIST	7058	Safari	History	Fobus Holster: Inside Waistba	http://www.fobusholster.com
✓ Conne	cted iOS Devices	67 🗆	2013/01/24 13:59:44 GMT-4	LVIST	7057	Safari	History	Fobus Holster: Standard Holst	http://www.fobusholster.com
Conta	cts	68	2013/01/24 14:00:09 GMT-4	LVIST	7056	Safari	History	Fobus Holster: CZ 75D COMP	http://www.fobusholster.com
🖌 🖌 Data D	Destruction	69	2013/01/24 14:00:25 GMT-4	LVIST	7055	Safari	History	Fobus Holster	http://www.fobushoister.com
🕗 Delete	d Users	70	2013/01/24 14:00:34 GMT-4	LVIST	7054	Safari	History	Fobus Holster	http://www.fobusholster.com
<ul> <li>Disk U</li> </ul>	Itility	71 □	2013/01/24 14:00:43 GMT-4	LVIST	7053	Safari	History	Fobus Holster, SIG 220, 219	http://www.fobusholster.com
✓ Disk U	Itility Saved List	72 □	2013/01/24 14:01:26 CMT-4	LVIST	7052	Safari	History	Fobus Holster: SIC/SAUER 239	http://www.fobusholster.com
✓ Dropb	ox	73 🗆	2013/01/24 14:01:41 CMT-4	LVIST	7051	Safari	History	Fobus Holster: SIG/SALIER 239	http://www.fobusholster.com
J FS Eve	nts	74	2013/01/24 14-01:49 CMT-4	LVIST	7050	Safari	History	Fobus Holster: SIC SAUER 239	http://www.fobusholstar.com
V Face II	me	75	2013/01/24 14:02:14 CMT-4	LVIST	7049	Safari	History	Fobus Holster: SIC /SALIER 239	http://www.fobusholster.com
	Timestamp Links	75	2013/01/24 14:02:30 GMT-4	LVIST	7045	Safari	History	Fobus Holster: SIG/SAUER 239	http://www.fobusholster.com
		77	2013/01/24 14-02-56 CMT-4	IVIST	7047	Safari	History	cheaper than dirt - Google Se	https://www.coogle.com/sear
mestamp Sea	rch	78	2013/01/24 14:02:58 CMT-4	IVIST	7046	Safari	History	cheiper instrant avogre sem	http://www.google.com/urPs
Ty	pe	79	2013/01/24 14:02:02 CMT_4	LVIST	7040	Safari	History	Chapper Than Dirt - America's	http://www.google.com/unes
ACITM	Active Timestamp	80 □	2013/01/24 14:03:02 CMT-4	LVIST	7043	Safari	History	Cheaper Than Dirt - America's	http://www.cheaperthandirt.c
ACKDT	Acknowledged Date	81	2012/01/24 14:02:19 CMT 4	LVIST	7043	Salari	History	Endure SIC Source 220 Amm Euro	http://www.cheaperthandirt.c
AONDT	Alert On Date	82 🗆	2013/01/24 14:03:18 041-4	LVIST	7043	Salari	History	Chapper Than Dirt's Veleter Sea	http://www.cheapertnandirt.c
ATLUP	Account Tracker Se	02	2013/01/24 14:03:57 GMT-4	LVIDT	7042	Selari	HISTORY	Cheaper manDirt's Hoister Sea	http://www.cheapertnandiri.c
CNCRT	Content Creation D	83	2013/01/24 14:03:55 GM1-4	LVIST	7041	Sarari	History	Cheaper I han Dirt - America's	http://www.cneapertnandiri.c
CNMOD	Content Modificatic	04	2013/01/24 14:04:01 GMT-4	LVIST	7040	Safari	History	Cheaper I han Dirt - America's	http://www.cheaperthandirt.c
CONCR	Conversation Creat	0)	2013/01/24 14:04:33 GMT-4	LVIST	7039	Sarari	History	Cheaper I han Dift - America S	http://www.cheaperthandiri.c
CONFI	Configuration Dow	00	2013/01/24 14:05:12 GMT-4	LVIST	7038	Sarari	History	Fobus Paddle Holster Left Han	http://www.cheaperthandirt.c
CONMD	Contact Modified D	8/	2013/01/24 14:05:20 GMT-4	LVIST	/03/	Sarari	History	Fobus Paddle Hoister Kight Ha	http://www.cheaperthandirt.c
CREAT	Creation Date	88	2013/01/24 14:05:41 GMT-4	LVIST	7036	Safari	History	Cheaper Than Dirt - America's	http://www.cheaperthandirt.c
DBRTH	Birthday	89	2013/01/24 14:05:51 GMT-4	LVIST	7035	Safari	History	Fobus Evolution Roto Belt Hols	http://www.cheaperthandirt.c
DTADD	Date Added	90	2013/01/24 14:06:04 GMT-4	LVIST	7034	Safari	History	Fobus Paddle Holster Right Ha	http://www.cheaperthandirt.c
DICON	Connected Date	91	2013/01/24 14:06:22 GMT-4	LVIST	7033	Salari	History	Fobus SIG 239 .40 and .357 E	http://www.cheaperthandirt.c
		92	2013/01/24 14:06:51 GMT-4	LVIST	7032	Safari	History	Fobus SIG 239 .40 and .357 E	http://www.cheaperthandirt.c
irt 0	1-Jan-2013 00:00:00	93	2013/01/24 14:10:56 GMT-4	LVIST	7031	Safari	History	you tube - Google Search	https://www.google.com/sear
d 2	0-Oct-2019 21:55:30	94	2013/01/24 14:10:58 GMT-4	LVIST	7030	Safari	History		http://www.google.com/url?s
	Analy	95	2013/01/24 14:11:05 GMT-4	LVIST	7029	Safari	History	fobus holster – YouTube	http://www.youtube.com/res
	Арріу	96	2013/01/24 14:11:08 GMT-4	LVIST	7028	Safari	History	Glock Fobus holster review &	http://www.youtube.com/wat

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

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

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

Clicking the "Close" button will close the graph.

# 27. Redefined Results

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

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

«	>		Redefined Result		te x		Locations (14	15)	\$ X		
				3	iearch Filters 🗹 Sh	ow All	Files	Gallery View			
F	-		Record No.		File Name	File Size	Mime Type	File Path	Latitude	Lorgitude	Hashset Name
	1		261073	1	INC 0001 IPC	1896740	image/ineg	(Applications /)code app/Contents /De	38 0374	-172 803	634
2			261975		IMG_0003.IPG	2505426	image/jpeg	Applications/xcode.app/contents/De	65 6829	-17 5489	916
3		-	261975		IMC 0004 IPC	1268382	image/jpeg	/Applications/Xcode app/Contents/De	64 7520	-14 5386	760
4			261977	B	IMC 0005 IPC	1852252	image/jpeg	/Applications/Xcode app/Contents/De	63 5314	-19 5112	265
5	5	1	261978		IMG 0006.HEIC	2808983	application/octet-st	/Applications/Xcode.app/Contents/De	37,7601	-122.51	24f
6	5 1	1	686545	1	IMG 0001.IPG	1896240	image/ipeg	/Library/InstallerSandboxes/.PKInstall	38.0374	-122.803	
7	7	-	686547	1	IMG 0003.IPG	2505426	image/jpeg	/Library/InstallerSandboxes/.PKInstall.	65.6829	-17.5489	
8	3	7	686548	- 8	IMG 0004.IPG	1268382	image/ipeg	/Library/InstallerSandboxes/.PKInstall	64,7529	-14.5386	
9		7	686549		IMG 0005JPG	1852262	image/ipeg	/Library/InstallerSandboxes/.PKInstall	63.5314	-19.5112	
1	10	-	686550		IMG 0006.HEIC	2808983	application/octet-st	/Library/InstallerSandboxes/.PKInstall	37.7601	-122.51	
1	11	1	865688	6	both.jpg	6422	image/jpeg	/System/Library/Automator/Flip Imag	36,4192	25.4312	
1	12	1	865689	-	both@2x.jpg	12521	image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
1	13	7	865749		horizontal.jpg	6494	image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
3	14		865750	-	horizontal@2x.jpg	12606	image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
1	15	1	865787	-	normal.jpg	6493	image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
1	16		865788	15	normal@2x.jpg	12534	image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
1	17	-	865829	1	vertical.jpg	6428	image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
1	18 1	٦	865830	1	vertical@2x.inc	12498	imace/inec	/System/Library/Automator/Flip Imag	36.4192	25.4312	
Re Fil Fil Sa In Fil M Hi M Sł Di Di Di Di	ecord le Nar le Patl amplei ode N le Size ime T ashsei DS: 2 HA1: t ate M ate Cr ate Ac	No.: 2619 me: IMG_0 h: /Applic Content/N lo./File ID e: 1.77 ME ype: Imag t Name: e8382988 5668956b oddified: 20 nange: 20 ccessed: 2	005.JPG atlons/Xcode.app/Co fedia/DCIM/100APPL (1852262 bytes) e/jpeg 82840700f92d77b11 9db249e6f31bd3ade 019-Sep-1103:23:1{ 19-Sep-27.11:31:18 019-Sep-1103:23:1	5do f02e GMT 8 GM	ts/Developer/Platforms/iPhon IG_0005 JPG 21f 7c4d7546870 T=4:00 -4:00 IT=4:00	:OS.platform/Library	y/Developer/CoreSimula	tor/Profiles/Runtimes/IO5.simruntime/Conten	ts/Resources/		
Та	ag:									0	
Đ	amin ⊴ [	er Notes: Detailed Inf	formation	H	x View T] Text View	S Strings	Exif Metac	iata 🔹 Apple Metadata 🐁	Maps 🛃	Preview	

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

## 27.1 Collated Location History
«	>	Redefined Result		e x		Locations (14	45)	s x		
				Search Filters 🔽	Show All	Files	Gallery View			
	8	Record No.		File Name	File Size	Mime Type	File Path	Latitude	Longitude	Hashset Name
1	Π	261973	i a	IMG 0001.IPG	189624	0 image/ineg	/Applications/Xcode.app/Contents/De	38.0374	-122,803	634
2	i i i	261975		IMG 0003.IPG	250542	6 image/ipeg	/Applications/Xcode.app/Contents/De	65,6829	-17.5489	9f6
3	- n	261976	1	IMG 0004 JPG	126838	2 image/jpeg	/Applications/Xcode.app/Contents/De	64.7529	-14.5386	7f0
4		261977		IMG_0005_PG	185226	2 image/jpeg	/Applications/Xcode.app/Contents/De	63.5314	-19.5112	200
5		261978	1	IMG_0006.HEIC	280898	3 application/octet-st	/Applications/Xcode.app/Contents/De	37.7601	-122.51	24f
6		686545		IMG_0001JPG	189624	0 image/jpeg	/Ubrary/InstallerSandboxes/.PKInstall	38.0374	-122.803	
7		686547	1.18	IMG_0003JPG	250542	6 image/jpeg	/Library/InstallerSandboxes/.PKInstall	65.6829	-17.5489	
8		685548	1.3	IMG_0004 JPG	126838	2 image/jpeg	/Ubrary/InstallerSandboxes/.PKInstall	64.7529	-14.5386	
9		686549		IMG_0005.JPG	185226	2 image/jpeg	/Library/InstallerSandboxes/.PKinstall	63.5314	-19.5112	
10		685550	-	IMG_0006.HEIC	280898	3 application/octet-st	/Library/InstallerSandboxes/.PKInstall	37.7601	-122.51	
11		865688	15	both.jpg	642	2 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
12		865689	1	both@2x.jpg	1252	1 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
13		865749	1	herizontal.jpg	649	4 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
14		865750	. (8	horizontal@2x.jpg	1260	6 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
15		865787	19	normal.jpg	649	3 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
16		865788		normal@2x.jpg	1253	4 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
17		865829	1	vertical.jpg	642	8 image/jpeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
18		865830	11.68	vertical@2x.inc	1249	8 image/ipeg	/System/Library/Automator/Flip Imag	36.4192	25.4312	
Rec File File San File Min Has MD SH/P Dat Dat	ord No.: 263 Name: IMG_ Path: /Appl pleContent; de No./File I Size: 1.77 M to No./File I Size: 1.77 M to No. S: 2e838294 L: b668956 e Modified: e Modified: e Accessed:	1977 	fodc fodc GMI 8 GM	nts/Developer/Platforms/ MG_0005 JPG c1f e7c4d7546870 AT-4:00 MT-4:00 MT-4:00	/iPhoneOS.platform/Libra	ry/Developer/CoreSimula	tor/Profiles/Runtimes/IOS.simruntime/Conter	tts/Resources/		
Tag	;								<u> </u>	
Exa	miner Notes	S.	1	ing View Ti Tau	e Viana C Cardan	The sufference	fata 🧖 Anala Matadata 🧍	Hand Fal	Draulau	
- 34	verailed I	monnation	1	iex view [] Tex	String	is is Exit Metao	Jata Sppie Metadata	maps	rreview	

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

### 27.2 Collated Messaging

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

«	>	Redefined Result	\$ X		Messenger	<b>♦</b> X	
			Search	Show All Timeline			
-					Event View Graph View Pie View		
		Record No.	Plugin	Sender	Receiver	Message	Timestamp
1		84	Messages	rufumcgregor@icloud.com	alfred.jermyn@icloud.com	Did u get this?	2013/01/05 20:04:16 GMT-4:00
2		176	Skype	makinbenjis	alfred.jermyn	Wassup?! Add to your list foo	2013/01/08 06:43:00 GMT-4:00
3		85	Messages	alfred.jermyn@icloud.com	rufumcgregor@icloud.com	yeah, just got it sorry for the delay	2013/01/08 09:05:00 GMT-4:00
4		86	Messages	alfred.jermyn@icloud.com	rufumcgregor@icloud.com	had a close call	2013/01/08 09:05:13 GMT-4:00
5		87	Messages	alfred.jermyn@icloud.com	rufumcgregor@icloud.com	no worries though, I took care of it	2013/01/08 09:05:22 GMT-4:00
6		88	Messages	rufumcgregor@icloud.com	alfred.jermyn@icloud.com	Hey no worries glad u got it! I figure if anyone	2013/01/08 11:40:02 GMT-4:00
7		89	Messages	alfred.jermyn@icloud.com	rufumcgregor@icloud.com	I'll check my secret PO BOX today and see if it i	2013/01/08 15:46:36 GMT-4:00
8		90	Messages	alfred.jermyn@icloud.com	rufumcgregor@icloud.com	i got it, all set up now	2013/01/10 21:32:00 GMT-4:00

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



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



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



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

## 27.3 Collated Web History

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

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

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

End Time	2013/10/20 23:10
	2013/10/20 23:10
	To Set

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



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



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

## 28. RAM Analysis

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

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

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

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

### 28.1 Setting Up Volatility Framework

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

#### 28.2 Selecting a RAM Image to Process

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

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



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

#### 28.3 Carving Passwords from RAM

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

Source	2020-Jan-14T12-48-14_ram_image.raw	۵	C	Carve Password

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



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



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

2		-	A	Q,	T		R	O		4	#							0	0	STURY	:=	3
	All Features 🔶	«	»		Carved	Passwor	1	¢× ∣⊺	10-20-3	6_ram_	image_raw	_2020	)-Jan 🖨 👌	¥.								
25	Disk Images						Sea	rch	Show A	ll.												
	RAM Images										Pas	sword	5									
	Aonia Matadata				Re	cord No.		Passwor	d		Server		-		Account			Descri	otion			
6	Evif	1				1	Passwo	d123														
1 1 1 1 1	LXII	2				2	p@ssw0	rd1														
0	MIME Type	3				3	Psswrd1	23!														
	ipplication	4				4	secret6	781														
	application/octet-stream (1)	5				5	pa\$\$wor	d321														
0	File Extensions	6				6	p@ss12	345														
M	User Defined File Signatures	7				7	sumuri	2345														
1	File Size	8				8	1p@ssw	Ord!														
Ŧ	Snapshots	9				9	secretco	de5678														
#	Hashset	10				10	guessmy	pass1														
8	Email Files	11				11	p@sswc	ord10														
**	Artifacts	12				12	pa\$sw0r	d1!														
試	Artifacts Keyword Search	13				13	p@s\$w0	ord23														
Ŧ	File Search	14				14	1234567	890														
ŝ	Content Search	15				15	buessmy	pass														
D	Artifacts Timeline	10				16	Descille	123														
Ħ	Bucket	18	10			1/	r0ckv0u	123														
1	Tags	19				10	marshme	1024														
12	Notes	20				20	12345p	ess														
*	Redefined Result	21				21	pass123	45#														
×	Saved Redefined Result	22	n			22	h@ha12	234														
0	Screenshots																					
201	Story Board																					
2	Carved Password																					
,	2020-Jan-13T10-20-36 rai																					
~	Carved Files											0.00										
S.	Carved Data	Sou	rce Nan	ne: /202	20-Jan-	13T10-2	0-36_ran	_image.	raw													
	RAM Analysis Saved	Plug	in Nam	e : Can	ed Pass	sword																
	Saved Craph Result	TAB	Name	Passwo	ords																	
400	Saved Mans	Rec	ord No.	: 7																		
-	Saveu maps	Pase	word :	sumuri	12345													No Previ	ew Avail	able		
	RECON																					
2	LAB																					
	SUMURI																					
	A A	3	Detai	led Infor	mation		間 Hex	View	[T]	Text V	ew	S	Strings		$\sim$	Previ	iew					
																						•

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

887 hotelanuschka	Bookmark
144 iamaTCFBguest	Remove Bookmarks
200 iamaTCFBguest	Tags 🕨
329 iamaTCFBguest	Add Note
398 iamaTCFBguest	Remove Note
411 iamaTCFBguest	Create Word List
480 iamaTCFBguest	Open Detailed Information
584 iamaTCFBguest	Copy to Clipboard

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

## 28.4 Using Volatility Framework in RECON LAB

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

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



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

Operating System	macOS	\$	
Build Version	MacHighSierra_10_13_6_17G65x64	٢	
Artifacts	List Running Processes	\$	Execute

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

< >	RAM Analysis	į.	\$	×.			RAM Analysis	e x	
Source	2019-Oct-0	5T14-1	16-48_r	am_ima	ige.raw		C Carve Password		
Operating System	macOS				0				
Build Version	MacHighSier	ra_10_1	13_6_17	G65×6	4 💽				
Artifacts	List Running	Proces	ses			Execute			
-							Command Output		
Offset Nam	e Pid	Uid	Gid	PGI	D Bit	s DTB	Start Time		
0xffffff803c331240	) gssd	621	222	0	621	64BIT	0x00000004be3b000 2019-10-05 18:16:49 UTC+0000		
0xffffff803c3316d0	) gssd	620	0	0	620	64BIT	0x00000004b6e4000 2019-10-05 18:16:49 UTC+0000		
0xffffff803b09e920	) cat	619	0	0	589	64BIT	)x000000020217d000 2019-10-05 18:16:49 UTC+0000		
0xffffff8030e3d490	) sudo	618	0	0	589	64BIT	0x000000015de76000 2019-10-05 18:16:48 UTC+0000		
0xffffff803b09f240	sh	616	501	20	589	64BIT	0x00000006fb24000 2019-10-05 18:16:48 UTC+0000		
0xfffff803001b240	0 ocspd	603	0	0	603	64BIT	0x0000001b1ac0000 2019-10-05 18:16:35 UTC+0000		
0xffffff803b09fb60	automountd	59	99 0	0	59	9 64BIT	0x00000001637c7000 2019-10-05 18:16:17 UTC+0000		
0xffffff80369f86d0	QtWebEngine	roce	592	501	20	589 64	BIT 0x0000001dc339000 2019-10-05 18:16:09 UTC+0000		
0xffffff80369f8240	printtool	591	501	20	591	64BIT	0x0000001aa3d5000 2019-10-05 18:16:09 UTC+0000		
0xffffff803addcb60	) gamecontrolle	rd 5	i90 i	247	247	590 64	IT 0x000000154f04000 2019-10-05 18:16:04 UTC+0000		
0xffffff803addb490	) Sumuri_RECO	N	589	501	20	589 64	UT 0x000000013ceab000 2019-10-05 18:16:00 UTC+0000		
									Save Export

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

00	Export Result
File Name	2019-Oct-05T14-16-48_ram_image.raw-Lists files in the file cache
Directory	/Users/macboy/Desktop/
	OK
	OK .

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

< >	RAM Analysis Saved	\$ ×	RAM Analysis Saved		\$ X	
	Searc	ch Show All				
			Saved Result			
	Record No.	Result Name	Source Name	Operating System	Build Version	Artifacts
1	1 2019-Oct-	05T14-16-48_ram_image.raw-Lists files in the file cache	2019	macOS	MacHighSierra_10_13_6_17G65x64	Lists files in the file cache
2	2 2019-Oct-	05T14-16-48_ram_image.raw-List Running Processes	2019	macOS	MacHighSierra_10_13_6_17G65x64	List Running Processes

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

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

# 29. Local Time Machine Snapshots (APFS Snapshots)

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

## 29.1 Processing Local Time Machine Snapshots



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

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



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

«	»	Snapshots	\$×	com	_apple_TimeMachine_2020-01-23-144623	\$ X		
			Timeline	Search Show A	II Deleted Files Modified Files			
		Record No.	Data	File Name	File Path / Library/Logs/Crashkeponer/CoreCapture/	File Size	Extension A Date Modified	20.
2		4	AssociationEve	ntHistory	/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:41	20;
3		6	IO80211AWDL	PeerManager	/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:41	20
4		8	ControlPath		/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:41	202
5		10	OneStats		/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:42	20;
6		13	StateSnapshots	i i	/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:43	20;
7		23	DriverLogs		/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:44	20
8		26	Metadata		/Library/Logs/CrashReporter/CoreCapture/	0	2020/01/16 10:00:41	202
9		34	.pid		/private/var/db/displaypolicyd/.pid	4	2020/01/21 08:44:47	202
10		139	27445		/private/var/log/asl/AUX.2020.01.16/27445	71019	2020/01/16 14:41:07	20;
11		140	27447		/private/var/log/asl/AUX.2020.01.16/27447	7423	2020/01/16 14:41:07	20;
12		147	.autoBackup		/private/var/run/.autoBackup	0	2020/01/23 14:45:52	20;

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

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

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

# **30. Acquiring and Processing iOS Devices**

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

### 30.1 Acquiring an iOS Device



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



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

Sr.	Device Class	Device Name	Phone No.	Phone Serial No.	UUID	1
1 1	iPhone	William's iPhone		D7M76FFW7J	00008110-001A08AA3CEB801E	ii ii
						Refresh

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

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

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

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

# 31. Reporting

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

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

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

#### **31.1 Plugin Reports**

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

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

« »		2	Artifacts	<b>\$</b> X			Google	Chrome (1	010)		\$X						
Keywor	d Se	earch		Time Line	Search	Show	All				C	G• Ex	port HTM	1L 📀	Tags	0	Report
Histor	/	Downloads	Topsites	Bookmarks	Search Items	Logins	Shortcuts	Autofill	Autofill Profiles	Credit Car	ds Fav	icons	Search Eng	ines Exte	nsions	Synced Data	Cook >
			Record No.	System Account		Titl	e		Visit Count		Last Vis	ited Dat	te			URL	
26		]	26	jermyn						1 2013/0	3/06 15:2	4:21 G	MT-5:00	http://www.	kaplanin	k.com/uploads	<i>I</i>
27		]	27	jermyn	Vacations Exoti	ica :: Europ	e Tours Holid	ays Gro		2 2013/0	3/06 15:2	4:51 G	MT-5:00	http://www.	vacation	sexotica.com/h	oliday/
28		]	28	jermyn	Vacations Exoti	ca :: Europ	e Tours Holid	ays Gro		1 2013/0	3/06 15:2	4:45 GI	MT-5:00	http://www.	vacation	sexotica.com/h	oliday/
29		]	29	jermyn	Enjoy An Exotic	Vacation I	n Saint Martin	ı – a		1 2013/0	3/06 15:2	25:03 GI	MT-5:00	http://www.	tripwolf.	com/en/trip/74	1578

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

Export	✓ HTML	\$ Tags	<b>\$</b>	Report
	PDF CSV XML KML			

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

Export	HTML	\$ √ Tags	\$ Report
		Full Screen Items	

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.

🖲 🥌 💿 🔗 Standard	HTML REPORT × +					
$\leftrightarrow$ $\rightarrow$ $G$ $\triangle$ $G$	File / Volumes/RECON%20Triage/Person_of_Interest_2019-Dec-27T14-11-02/Reports/Plugin_Reports/Mes	sages_Standard_HTML_Tags_2020-J	☆	0	75	:
Contents	Messages (Messenger)					
DB Messages View						
	DB Messages View		To			
	Participants		10			
	rutumegregor@icloud.com - 2013-Jan-06 00:04:16 +00:00 Did u get this?					
		alfred.jermyn@icloud.com - 2013-Jan-08 13:05:00 yeah, just got it sony for the delay	+00:00			
		attred.jermyn@icloud.com - 2013-Jan-08 13:05:13 I had a close call	+00:00			
		alfred.jermyn@icloud.com - 2013-Jan-08 13:05:22 no worries though, I took care of it	+00:00			
	rufumogregor @Icloud.com - 2013-Jan-08 15:40:02 +08:00 Hey no worries glad u got it! I figure if anyone ever asks we can just say these are for music u know cause that's why apple made them lo!					

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

#### **31.2 Global Artifacts Report**

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



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

#### 31.2.1 Case Information Window

)	Globa	al Report - Case informaion
	Case No.	03-20-00848
	Case Name	Person of Interest
	Examiner	macboy
RECO	Agency	SUMURI
LAB	Location	SUMURI HQ
	Case Notes	Examination of the Person of Interest's MacBook.
		Back Next

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

#### **31.2.2 Customizing Global Reports**

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

Report Scope	
<b>O</b> Tags	🔘 Full
	Tags
Bookmarks	
🔳 🛑 Red	
🗌 🛑 Blue	
🗌 😑 Yellow	
🗌 🕒 Green	
🔲 🛑 Bitcoin	
Screenshots	

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

Report Scope				
Tags		O Full		
		Tags		
Bookmarks				
🔳 🥚 Red				
Blue				
Yellow				
Green				
🔲 🔴 Bitcoin				
Screenshots				
Saved Graphs				
Report Type				
Advance HTML	Standard HTML PDF	CSV	XML	
Export Files				
	2020 1 2012-24-42			
Report Name Report 2	2020-Jan-26 12:24:42			
Report Path //RECON	I Triage/Person_of_Interest_2	019-Dec-27114-11-02/	Reports/Global_Reports/	
			Back	Next
			Back	NCAL

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.* 

	<plugin selection=""></plugin>	Plugin Search	
All Plugins macOS Plugins Advanced Analysis Apple Apps Device Email Artifacts Email Client Messenger Native Apps Network Online Storage P2P System Virtual Machines Web Browsers	Plugins   FS Events   Events   FaceTime   FaceTime   Finder   Recent Open Folder   Open Tabs   Preferences   Finder Sidebar   FrostWire   Soogle Chrome   History   Downloads   Topsites   Bookmarks	Export         NA         NA     <	
		Back Report	

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

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

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

#### 31.2.3 Global Report Type

Report Type					
Advance HTML	Standard HTML	PDF	CSV	XML	

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

port 2020–Jan–26 14:21:26		
ECON Triage/Person_of_Interest_2019-Dec-27T	14-11-02/Reports/Globa	I_Reports/
	Back	Report
p	ort 2020-Jan-26 14:21:26 CON Triage/Person_of_Interest_2019-Dec-27T	ort 2020-Jan-26 14:21:26 CON Triage/Person_of_Interest_2019-Dec-27T14-11-02/Reports/Globa Back

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.

- Contents			RECONLAR
	/		
Apple Dock			
Apple Installed Applications			
Disk Utility Saved List	RECON		
ES Evente	LAD		
🥡 Finder Sidebar			
Mail	Case Details Source1		
Messages	RECON Version	122	
	Report Scope	1.3.Z Tans	
	Case No.	03-19-00848	
📀 Safari	Case Name	Person of Interest	
🛐 Skype	Location		
Contlight Settings	Case Notes		
Spourgine Sectings	Examiner	Steve Whalen, CFCE	
👕 Trash RecycleBin	Examiner Phone		
	Examiner Email		
	Agency Name		
	Agency Address	America New York FCT CHT 5:00	
	User Selected Time Zone	America/New_York-ES1-GM1-5:00	
	Report Generated Machine Time	America/New York-EST-GMT-5:00	
	Zone		

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

#### 31.3 Story Board Reports - WYSIWYG Reports

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



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

REPORT-001		
	Create	Cancel

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

« »		Story Board	¢ ×		REPORT-001	\$ X	
۲	() All	•		Search	Show All		Blur Image
1 2 3 4 5 6 7 8 9 10 11 11	R R R	Record No. 60348 60317 62684 62687 48 6 2 13 166 380 380 382 556	Plugin FS Events FS Events FS Events FS Events Apple Dock Apple Installed Applications Disk Utility Saved List Finder Sidebar Mail Mail Mail	TAB Name Events Events Events Events Items Applications Disk Images USB Flash Messages Messages Messages	Item 1           18158641836174866792           18158641836174866750           18158641836178187914           18158641836178187914           18158641836178186548           Bitcoin-Qt           Bitcoin-Qt           Bitcoins_Info           BitCoins           That other project           BitCoins           BitCoins	Item 2 BitCoins BitCoins Avoid Taxes with Bitcoins!.pdf Bitcoin Tax Evaders : Bitcoin.pdf com.yourcompany.Bitcoin-Qt /Applications/Bitcoin-Qt.app /Users/jermyn/Downloads/ alfred.jermyn@gmail.com alfred.jermyn@gmail.com alfred.jermyn@gmail.com	No Preview Available
0			RECON		REPORT-001		File
			Case Details RECON Version Case No. Case Name Location Case Notes Examiner Examiner Email Agency Address User Selected Til Report Generate Beport Generate	S ne Zone Time Machine Time Zone	1.3.2 03-19-00848 Person of Interest Steve Whalen, CFCE America/New_York-EST-GMT-5:00 2020-Jan-26 14.37.01 GMT-5:00 America/New_York-EST-GMT-5:00		Edit S C & D D Font Helvetica O 12 V B I U D Alignment E E E E
			Sources De Evidence No Apple ID OS Type File System Product Type	tails Sourc /Jermyn_Image.dmg/Jerr 001 alfred.jermyn@icloud.con macDS hfs MacBookPro5.3	re1 nyn_01 n		Standard 📀

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.



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

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

32.3.2 Adding Tags and Bookmarks to a Report

612882	File System	Files	2012-08-26 12.57.12.jpg	/Users/jermyn/Dropbox/Camera
62684	FS Events	Add Record with File(s)	18158641836178187914	Avoid Taxes with Bitcoins!.pdf
62687	FS Events	Add File(s)	18158641836178186548	Bitcoin Tax Evaders : Bitcoin.pdf
60348	FS Events	Copy to Clipboard	18158641836174866792	BitCoins
60317	FS Events	Go to record Ouick Look	18158641836174864750	BitCoins
363	Safari	Cookies	.www.bitcoins.com	Locale

To add an item (record) to the Story Board report place the cursor at the location where the item is to be placed. Right-click on an item from the bookmarks and tags list and select from one of the three options:

- Add Record adds details about the record (bookmark, tag) to the report without the file
- Add Record with File(s) adds both the details of the record to the report with the file (export)
- Add File(s) adds the file only to the report (export)

Detailed Information	File Preview
Source Name: /Jermyn_Image.dmg/Jermyn_01	
Record No.: 612882	
File Name: 2012-08-26 12.57.12.jpg File Path: /Users/jermyn/Dropbox/Camera Uploads/2012-08-26 12.57.12.jpg	
Inode No./File ID: 607635	
File Size: 957.55 KB (980533 bytes)	
Mime Type: image/jpeg	
Date Modified: 2012-Aug-26 11:57:12 GMT-5:00 Date Change: 2013-Apr-30 12:43:25 GMT-5:00 Date Accessed: 2013-Apr-30 12:43:25 GMT-5:00 Date Added(Apple): 2013-Mar-06 14:04:30 GMT-5:00 Content Creation Date(Apple): 2012-Aug-26 11:57:12 GMT-5:00 Content Modification Date(Apple): 2012-Aug-26 11:57:12 GMT-5:00	
Tag: Green	
Examiner Notes:	

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

#### 31.3.3 Adding External Files to a Report



To add external files to the Story Board report click the **Add File** button found above the formatting options to the right of the report.



Navigate to the file to add and click Open to add the file to the report.

#### 31.3.4 Filtering Records In Story Board



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

« »	Story Board	\$ X		REPORT-001
	All	trash	Search	Show All
			ltems	Timeline
	Record No.	Plugin	TAB Name	Item 1
9	6 16	Trash RecycleBin	ltems	IntroductiontoBitcoinMiningDavidRSterry.pdf
10	6 15	Trash RecycleBin	ltems	IntroductiontoBitcoinMiningDavidRSterry alias
173		Trash RecycleBin	ltems	Bitcoin-FBI.pdf
174	9 7	Trash RecycleBin	Items	Bitcoin-FBI alias
178	6	Trash RecycleBin	Items	Bitcoin Tax Evaders : Bitcoin.pdf
179	6 5	Trash RecycleBin	ltems	Bitcoin Tax Evaders : Bitcoin alias 2
180	6 4	Trash RecycleBin	ltems	Bitcoin Tax Evaders : Bitcoin alias
182	9 3	Trash RecycleBin	ltems	bitcoin paper.pdf
183	2	Trash RecycleBin	Items	bitcoin paper alias

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

S1.5.5 Adding Records in enronological order	31	.3.5	Adding	<b>Records</b> ir	n Chrono	logical (	Order
--	----	------	--------	-------------------	----------	-----------	-------

1	Items Timeline						
	Timestamp	∧ Туре	Record No.	Plugin	Category	ltem 1	
4	2012/12/13 17:28:57 GMT-5:00	CNMOD	6	Apple Installed Applications	Applications	Bitcoin-Qt	
5	2012/12/13 17:28:57 GMT-5:00	CNCRT	6	Apple Installed Applications	Applications	Bitcoin-Qt	
6	2012/12/13 17:28:57 GMT-5:00	CNMOD	14	Spotlight Settings	Shortcuts	Bitcoin-Qt.app	
7	2012/12/13 17:28:57 GMT-5:00	FSCRT	14	Spotlight Settings	Shortcuts	Bitcoin-Qt.app	
8	2012/12/13 17:42:43 GMT-5:00	CNCRT	2	Disk Utility Saved List	Disk Images	bitcoin-0.7.2-macosx.dmg	
9	2012/12/13 17:42:43 GMT-5:00	CNMOD	2	Disk Utility Saved List	Disk Images	bitcoin-0.7.2-macosx.dmg	
10	2012/12/13 17:42:43 GMT-5:00	CNCRT	16	Safari	Downloads	bitcoin-0.7.2-macosx.dmg	
11	2012/12/13 17:42:43 GMT-5:00	CNMOD	16	Safari	Downloads	bitcoin-0.7.2-macosx.dmg	

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

#### 31.3.6 Blur Image in Report



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

#### 31.3.7 Saving and Exporting a Story Board Report



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



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

## 32. Shutdown RECON LAB



To quit RECON LAB select "Quit RECON\_LAB" from the top menu

## 33. Disk Manager with Write-Block

Disk Manager allows the processing and analysis of connected devices and their volumes by using RECON LAB's Disk Manager and software write-blocking features.


Disk Manager can be accessed from the RECON LAB Welcome Screen by clicking the **Disk Manager** button.

				Disk Wallage			72
Device	Model	Size	Туре	Name	File System Derived From	Encrypted	Mode
disk3	Түре-С	29.88 GB	GUID_partition_scheme			NO	
disk3s1		200.00 MB	EFI	EFI	msdos	NO	
disk3s2		29.56 GB	Apple_HFS	RECON LAB	his	NO	Read Write
disk4	ARC-8050-VOL#000	29802.31 GB	GUID_partition_scheme			NO	
disk4s1		200.00 MB	EFI	EFI	msdos	NO	
disk4s2		29801.99 GB	Apple_HFS	ARECA	hfs	NO	Read Write
Dofrach	Decrypt Unmount	Mount-R				Disk Arbitration	Turn ON

The Disk Manger window will open showing all connected disks and volumes that can be accessed by RECON LAB.

## 33.1 Write-Blocking



Mac computers in Target Disk Mode and other disks can be connected safely (write-block) to RECON LAB by disabling the Disk Arbitration daemon. To turn off Disk Arbitration click the **Turn Off** button at the bottom right of the Disk Manager.

Once disabled hard disks and Mac computers placed in Target Disk Mode can be connected safely to your examination Mac.

	Enter a password to unlock the disk "Macintosh HD".
U.	Password:
	Remember this password in my keychain
Show H	int Cancel Unlock

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.

disk5s3		466.40 GB	Micros
disk6	Target Disk Mode	1396.98 GB	EF5734
disk6s1		1396.98 GB	41504
disk6s2		1396.98 GB	41504
disk6s3		1396.98 GB	41504
disk6s4		1396.98 GB	41504
disk6s5		1396.98 GB	41504
Refresh	Decrypt Unmount	Mount-R	

With the new devices displayed, the following options exist:

- **Refresh** re-poll for changes to connected devices
- **Decrypt** allows an examiner to decrypt FileVault volumes with a password or Recovery Key
- Unmount unmount any previously mounted volume
- **Mount-R** mounts a volume or disk read-only

# 33.2 Mounting a Device Read-Only

The Disk Manager can be used to mount volumes as read only to ensure that there are no changes to data.

Device	Model	Size	Туре	Name	File System	Derived From	Encrypted	Mode
disk3	Type-C	29.88 GB	GUID_partition_scheme				NO	
disk3s1		200.00 MB	EFI	EFI	msdos		NO	
disk3s2		29.56 GB	Apple_HFS	RECON LAB	hfs		NO	Read Write
disk4	ARC-8050-VOL#000	29802.31 GB	GUID_partition_scheme				NO	
disk4s1		200.00 MB	EFI	EFI	msdos		NO	
disk4s2		29801.99 GB	Apple_HFS	ARECA	hfs		NO	Read Write
disk5	Target Disk Mode	1863.68 GB	GUID_partition_scheme				NO	
disk5s1		300.00 MB	EFI	EFI	msdos		NO	
disk5s2		1396.98 GB	Apple_APFS				NO	
disk5s3		466.40 GB	Microsoft Basic Data	BOOTCAMP	ntfs		NO	
disk6	Target Disk Mode	1396.98 GB	EF57347C-0000-11AA				NO	
disk6s1		1396.98 GB	41504653-0000-11AA	Macintosh HD	apfs	disk5s2	NO	
disk6s2		1396.98 GB	41504653-0000-11AA	Macintosh HD – Data	apfs	disk5s2	NO	
disk6s3		1396.98 GB	41504653-0000-11AA	Preboot	apfs	disk5s2	NO	
disk6s4		1396.98 GB	41504653-0000-11AA	Recovery	apfs	disk5s2	NO	
disk6s5		1396.98 GB	41504653-0000-11AA	VM	apfs	disk5s2	NO	
Refresh	Decrypt Unmount	Mount-R					Disk Arbitration	Turn ON

Select the volume in the Disk Manager to mount as read-only and click Mount-R.

disk6s1	1396.98 GB 41504653-0000-11AA	Macintosh HD	apfs	disk5s2	NO	Read Only
disk6s2	1396.98 GB 41504653-0000-11AA	Macintosh HD - Data	apfs	disk5s2	NO	Read Only

Note: If you are mounting a Mac in Target Disk Mode with macOS 10.15 or higher you will need to mount both the System and Data partitions as read-only.

0 🔵 🔵	RECON LAB-1.3.4
Case Info	<ul> <li>/System/Volumes/Data</li> <li>/Volumes/ARECA</li> <li>/Volumes/BOOTCAMP</li> <li>/Volumes/Macintosh HD</li> <li>/Volumes/Macintosh HD - Data</li> <li>/Volumes/RECON LAB</li> </ul>
	Cancel Add

Once mounted read-only, the volumes can be added to RECON LAB for processing.

# 34. RECON LAB Case Exporter

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

### 34.1 Exporting a Case

Exporting a case is a simple process that allows examiners to export findings in a way that can be further analyzed without the need for a RECON LAB license.



Select Export > **Export Case** in the Menu Bar, and the Export Case window will appear.

Quick Mode	0 c	ustor	n Export
Category	<b>y</b>	1	List
Internet History	1		Airport WirelessNetwork
Messages	2		aMule
Emails	3		Android Contacts
🗹 Image	4		Android Installed Applications
🗹 Multimedia	5		Android Photos
🖸 🗹 Document	6		Android Thumbnails
Other Artifacts	7	☑	App Compatibility Cache
	8		Apple Dock
	9		Apple Installed Applications
	10		Apple Mail Extractor
	11		Application Convices
			🗌 Blur Image
Jsers/silvinohall/Desktop			Output
	Export		

RECON LAB has two options when exporting a case:

**Quick Mode -** Allows examiners to quickly export data from the case using RECON LAB's preset configurations from automated plugins

**Custom Export -** Allows examiners to selectively include data for their case from bookmarks and tags

### 34.1.2 Quick Mode

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

0	Quio	k Mode	0	Cust	tor	n Export
	1	Category		[		List
1		Internet History	1	6	2	Airport WirelessNetwork
2		Messages	2		/	aMule
3		Emails	3		/	Android Contacts
4		Image	4		/	Android Installed Applications
5		Multimedia	5			Android Photos
6		Document	6	6	/	Android Thumbnails
7	~	Other Artifacts	7		/	App Compatibility Cache
			8		2	Apple Dock
			9		/	Apple Installed Applications
			1(	0	2	Apple Mail Extractor
_			1	1	N	Application Convices
						Blur Image
/Us	sers/	/silvinohall/Desktop				Output
			Export	:		

Note: Automated plugins need to be processed before exporting a case in Quick Mode. For more information about RECON LAB's automated plugins, see Section 9.2.

### 34.1.3 Custom Mode

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

For more information on bookmarking and tagging, see Section 17

			Export Case	
0 (	Quic	k Mode	O Custom Export	
			Tags	
1		Bookmarks		
2		Red		
3		Blue		
4		Yellow		
5	<	Green		
6		SkinTone		
				Blur Image
/Us	ers/	silvinohall/Desktop		Output
			Export	

## 34.1.4 Exported Case Output

Select the desired **Output** directory to export the case, and click **Export**.

Quick Mode Custom Export     Tags     1   2   8   2   7   Red   3   2   8   4   2   7   8   8   4   2   7   8   8   9   7   7   9   7   7   7   8   8   7   9   7   8   8   9   7   9   9   7   9			Export Case	
Tags         Sookmarks         Red         Blue         Felow         Green         SkinTone	Qu	iick Mode	O Custom Export	
1 Image: Second s			Tags	
2 ? Red   3 ? Blue   4 ? Yellow   5 ? Green   6 ? SkinTone     6 ? SkinTone     Blur Image        7Users/silvinohall/Desktop Output	1	Bookmarks		
<ul> <li>Blue</li> <li>Yellow</li> <li>Green</li> <li>SkinTone</li> </ul> Blur Image Users/silvinohall/Desktop Output	2 🗸	Red Red		
4 ♀ Yellow 5 ♀ Green 6 ♀ SkinTone Blur Image /Users/silvinohall/Desktop Output	3 🔽	] Blue		
5 SkinTone 6 SkinTone Blur Image Users/silvinohall/Desktop Output Export	4 🔽	Yellow		
6 SkinTone Blur Image /Users/silvinohall/Desktop Output Export	5 🔽	Green		
/Users/silvinohall/Desktop Output Export	6 🗸	SkinTone		
/Users/silvinohall/Desktop Output Export				
/Users/silvinohall/Desktop Output				Blur Image
Export	/User	s/silvinohall/Desktop		Output
			Export	

The case will output to a folder named **Export\_Case** in the selected directory and will include a **RECON\_CASE\_READER.exe** and a **Case\_Data** Folder.



# 35. CASE Reader

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

# 35.1 Minimum System Requirements

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

## **35.2 Installation**

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



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

Setup - RECON CASE READER version 1.0.5 (A2)			×
Select Additional Tasks			
Which additional tasks should be performed?			
Select the additional tasks you would like Setup to perform while installing RECON C/ click Next.	ASE READ	ER, then	
Additional shortcuts:			
Create a desktop shortcut			
	Vext	Ca	ncel

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

Setup - RECON CASE READER version 1.0.5 (A2)	_		×
Ready to Install			
Setup is now ready to begin installing RECON CASE READER on your computer.			
Click Install to continue with the installation, or click Back if you want to review or	r change any	settings.	
			_
Additional tasks:		/	N
Additional shortcuts:			
Create a desktop shortcut			
		· · · · · · · · · · · · · · · · · · ·	/
<		>	
		-	
Pack	Install	6	ncel
Back	Instan	Ca	licer

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



35.3 Loading a case



X

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**.

E:/Export_Case/Case_Data
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.

Case						þ
🔶 -> -* 🕇 🛄 > Thi	is PC → ExFatTrar	nsf (E:) > Export_Case	>	~	ر الم	ch Export_Case
Organize 👻 New folde	er					== - (3
This PC	Name	^	Date modified	Туре	Size	
3D Objects	📙 Case_Data		7/22/2021 10:36 AM	File folder		
🛄 Desktop						
Documents						
Downloads						
Music						
Pictures						
Videos						
TR SSD Data (F						
ExFatTransf (E:)						
DEST ExFat (H:)						
👳 QuickBooks (\\q						
DEST ExFat (H:)						
Folde	r: Case_Data					
					Select Fold	ler Cancel

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

# 35.4 RECON CASE Reader Interface

The RECON CASE Reader interface is designed to mirror RECON LAB's simple and intuitive design. Many features in the RECON CASE READER function the same way as they do in RECON LAB.



## 35.5 Case View

Once a case is loaded examiners will be greeted with the Case View Screen. The Case View screen can also be accessed by clicking the "briefcase" icon at the top of the sidebar



**Case View** displays information about the case including information about the case and the examiner. **\*Note\* This information is taken from RECON LAB at the time of the export and can not be changed.** 

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

## 35.6 Top Menu



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

#### Artifacts - contains the "Search Artifacts" and "Artifact Timeline" sub-menus

Search Artifacts - allows the examiner to conduct a single keyword search quickly within all exported artifacts. Section 19.1 has more information about Artifact Keyword searching.

Artifacts Keyword Search	-	×
Keywords Keywords for search		
<plugin selection=""></plugin>		
Plugins		
>  Brave Browser		
> 🗌 💿 Google Chrome		
> 🗆 🖂 Mail		
> 🗌 🚨 Messages		
> 🗌 🧭 Safari		
Search Name Search label		
Start		

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



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

Global Report - Report Category -	- 🗆 X
Report Scope	
● Tags O Full	
Tags	^
Bookmarks	
Red	
🔲 📕 Blue	
Yellow	
Green	
Screenshots	~
Report Type	
Advance HTML Standard HTML PDF CSV	XML
Export Files	
Report Name Report 2021-Nov-05 16:30:10	
Report Path G:/1_Export_Case/Case_Data/Reports/Global_Reports/	/
Back	Report

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

🛃 File Search			? ×
File Name			Contains ~
File Size Greater than V			Bytes ~
Date Change	Between $\vee$	01/01/2018 12:30:00	31/12/2018 12:30:00
Date Modified	Between $\vee$	01/01/2018 12:30:00	31/12/2018 12:30:00
Date Accessed	Between $\vee$	01/01/2018 12:30:00	31/12/2018 12:30:00
Source1	Source2	Source3	Source4
Source5	Source6	Source7	
All Filters Any Filter			
Search Label			Search

## 35.6 Main Columns

There are two main columns at the top of the Main Window for the RECON CASE READER. These columns can be used for quick navigation.

\left > Case: ~	Case Info	$\sim$

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.

{ }	Source		ARALE SSD	(William_Campbell_MacBook.dt	gi	*						×
Table V	<select category=""> Case:</select>		P	Search Filters	Show All						Đợ	ort as CSV 📧
1	Artifacts Timeline		File ID	File Name	Extension	File Path	File Size	Mime Type	Hashset Name	MD5	SHAT	Decompres
1 🗆	Source	022011	32340	Desktop		/Users/williamcampbell/Desktop	2					1 h (5236/0454333
20		673171	32384	Documents		AUsers/williamcampbell/Documents						
з 🗆		673200	32386	Downloads		/Users/wilfiamcampbell/Downloads						
4 🗆		673196	282596	EV_Docs		/Users/williamcompbell/EV_Docs	-					
5 🗌		622615	32342	Library		/Users/williamcampbeil/Library	- 24					
6 🗋		622295	32336	Music		Alsers,/williamcampbell/Music						
¢												3
APPL	SSD + 📙 Usern + 🗧	willamcampbel -										

#### Select Category Column

< >	Source	APPLE SSD	(William_Campbell_MacBook.ding)		~						×
Table V	«Select Category» Case:		Search Filters •	Show All						Đợi	nt as CSV 📳
1	Artifacts Timeline	/File ID	Fão Name	Extension	File Path	File Size	Mime Type	Hashset Name	MDS	SHAT	Decompres
10	Source 022011	32340	Desktop	/Users/will	iamcampbell/Desktop						
20	673171	32384	Documents	/Users/will	iamcampbell/Documents						
3 🗌	673200	32386	Downloads	/Users/will	amcampbell/Downloads	(÷					
4 🗆	673196	282596	EV_Docs	/Users/will	amcampbell/EV_Docs						
5 🗌	622615	32342	Library	/Users/will	iamcampbell/Library	-					
6 🗌	622295	32336	Music	AUsers/with	amcampbell/Music						
¢											,
- APPL	: SSD + 🛄 Users + 🛄 williamcampbel +										

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

#### Select Feature Column

< > so	rce.	MPLE SSD	(William_Campbell_MacBook.drsg)		~					×
C Table View	Gallery Vew	<select.fe APPLE SSE</select.fe 	nture> •- Data (William_Campbell,MacB	cok.dmg)					Equ	ort as CSV
1	Record No.	Inode No	(William_Lampbell_MacBook.d	ng)	File Size	Mime Type	Hashset Name	MD5	SHA1	Decompres
1 🗆	622611	32340	Desktop	/Users/williamcampbell/Desktop						
2 []	673171	32384	Documents	/Users/williamcampbell/Documents						
3 🗆	673200	32386	Downloads	/Users/williamcampbell/Downloads	14					
4 🗆	673196	282596	EV_Docs	/Users/williamcampbell/EV_Docs	-					
5 🗆	622615	32342	Library	/Users/williamcampbell/Library						
6 🖸	622295	32336	Music	/Users/wilkamcampbell/Music	10					
¢										ž
APPLE SS	🕞 📙 Usaro 🛌 wiliamtang	pbell (								

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

### 35.7 Case Sidebar

🛩 💼 Case: Campbell Image 🤆	« » Sou	ince		~ APPLE SSD - Data	(William_Campbell_MacBe	ook.dmg)	~				x
 V Q Source	«	>		Sea	rch Filters -	Show All				Export as	CSV 🔳
William_Campbell_	Table View	W Gall	ery View			1					
> William_Campbell_	. <b>П</b> .		Record No.	10de No./File I	File Name	Extension	i	File Path	i.	File Size	Mime Ty
> Nilliam_Campbell_	1 🗆		54090	32336	Music		/Users/willia	mcampbell/Music			
Villiam_Campbell_	2 🗌		54406	32340	Desktop		/Users/willia	mcam <mark>pbell/Deskt</mark> e	ор		
> 📙 Library (6)	3		54410	32342	Library		/Users/willia	mcampbell/Librar	у	2 <del>48</del>	
> System (1)	4 🗆		104966	32384	Documents		/Users/willia	mcam <mark>pbell/D</mark> ocur	m <mark>ents</mark>		
✓ 📙 Users (1)	5 🗆		104991	282596	EV_Docs		/Users/willia	mcam <mark>pbell/EV_D</mark> o	ocs	122	
<ul> <li>williamcamp</li> <li>Music (1)</li> </ul>	6 🗌		104995	32386	Downloads		/Users/willia	mcam <mark>pbell/D</mark> own	loads		
> Desktop (											
> Library (7)											
> EV_Docs (		SD - Data	Ulgers a live	illiamcamphell >							1
> 📒 Download	Anico	50 5010		indirican poen >							
Applications ('	🔮 Detai	5 🔛	Hex T] Text 🕻	Apple Metadata							
> William_Campbell_											
										No Preview Available	
									Provident	2	
								0	and rievew		104

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

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

The case sidebar is broken up into three sections.

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

35.7.1 Source Tab



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

### 35.7.2 Artifacts Tab

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



	Image on macC	« »	Artifacts	5		∀ Googl	le Chrome (169)	ř.			~					x
-	V III Artifacts	Keywo	d Search	1		Time Line	Search	Show A	8			🗌 🗗 Export	HTML		5	Report
	Brave Browser (170)	Histor	y Do	wnioads	Topsites	Bookmarks	Search Items	Logins	Shortcuts Autofill	Autofill Profiles	Credit Cards	Favicons	Search Engines	Extensions	Synced Data	- c ()
0	Google Chrome (169) Safari (037)				ecord N	stem Accou		Title		Visit Count	Last V	<b>√isited</b> Date		U	IRL	^
	✓ Email Artifacts	1			1	williamca	padres sch	e <mark>dule 2021</mark>	- Google Search		3 2021/03/31	1 18:20:15 +00	0:00 https://	www.google	.com/search	n?q=pa
	Mail (194)	2			2	! williamca	San Diego	Padres Sch	nedule   San Die		1 2021/03/31	1 18:14:58 +00	):00 https://	www.mlb.co	m/padres/s <mark>o</mark>	chedule
	Messenger	3			3	williamca	San Diego	Padres Sch	iedule   San Die		3 2021/04/01	1 11:02:39 +00	0:00 https://	www.mlb.co	m/padres/s <mark>o</mark>	chedule
	Artifacts Keyword Search	4			4	williamca	Tickets   Sa	in Diego Pa	adres vs. A <mark>riz</mark> on		2 2021/03/31	1 18:17:46 +00	0:00 https://	www.ticketm	aster.com/e	avent/0
		5			5	williamca	Tickets   Sa	in Diego Pa	adres vs. Arizon		2 2021/04/01	1 11:02:45 +00	0:00 https://	www.ticketm	aster.com/e	avent/0
		6			6	williamca	world serie	s 2021 - G	oogle Search		3 2021/04/01	1 11:02:27 +00	):00 https://	www.google	.com/search	n?q=wc
		7			7	' williamca	world serie	s 2021 dat	es - Google Sea		3 2021/03/31	1 18:27:43 +00	0:00 https://	www.google	.com/search	n?q=wc
		8			E	8 williamca	world serie	s 2021 dat	es - Google Sea		1 2021/03/31	1 18:27:17 +00	0:00 https://	www.google	.com/search	n?q=wc
		9			9	) williamca	Official San	n Diego Pa	dres Website		2 2021/04/01	1 11:17:02 +00	0:00 https://	www.mlb.co	m/padres/	
		10			10	) williamca	Padres Ema	ail Newslet	ters   San Diego		1 2021/04/01	1 11:17:24 +00	0:00 https://	www.mlb.com	m/padres/fa	ans/nev
		11			11	williamca	Register for	r Padres N	ewsletters   San		2 2021/04/01	1 11:23:59 +00	):00 https://	www.mlb.co	m/padres/fa	ans/nev 🗸
		<														>
		20	etails	Hex	T[ ⊤ext	💰 Apple Me	atadata									
														1. P. i.u.		
														NO PREMEW	Available	

#### 35.7.3 File Filters

The File Filters tab contains data relating to file extensions and results from file searches. Files will be sorted by extensions or categorized by searched keywords.



#### 35.8 Main Viewer Window

The RECON CASE Reader main view is designed to mirror the interface of RECON LAB. See section 12.6-12.8 for more information about the main view, covering the Details, Hex Viewer, Text Viewer, Apple Metadata, and more.

✓ IIII Case: recon case reader	< > Source		~ APPL	E SSD (William,	Campbell_MacBaok.cimg)		ت ان					X
V Source	<	2		Searc	h Filters - S	how All					Export	as CSV 🔝
Case: recon cose reader     Source     Source	Table View	Gollery View										
> Applications (14)			Record No. tode	No./File I	File Name	Extension	File Path	File Size	Mime Type	Hashset Name	MD5	SF-^
> Library (6) System (3)	1		673213	383752 🖹	143973622_1117059	ł., jpg	/Users/williamcampbell/Downloads/143973622_11	33451				
Usors (1)	2 🗆		673208	383734 🖬	170806755_5630045	i,₊ jpg	/Users/williamcampbell/Dovmloads/170806755_56	189584				
> private (1)	3 🗆		673214	383745 🖹	170831539_7438647	/ jpg	/Users/williamcampbell/Downloads/170831539_74	141299				
<ul> <li>usr (1)</li> <li>William Campbell MacRov</li> </ul>	4 🗆		673212	270878	2021-printable-sch	e pdf	/Users/williamcampbell/Downloads/2021-printabl	5396276				
Preboot (0)	5 🗀		673217	377154	Beyond the State of	fpdf	/Users/williamcampbell/Downloads/Beyond the St	4026633				
William_Campbell_MacBot	6 🔲		673201	364850	Cyberduck-7.8.5.34	4 zip	/Users/williamcampbell/Downloads/Cyberduck-7	124652				
<ul> <li>William Campbell MacBoc</li> <li>William Campbell MacBoc</li> </ul>	7		673211	421030	Detail view of Space	a png	/Users/williamcampbell/Downloads/Detail view of	179523				
🗦 🧫 William_Campbell_MacBox	<											, ×
) 🥪 William_Campbell_MacBoc	APPLE SSD	> Users +	willancampboll +	Oswatioads	9							
	🔬 Octars	O 1412	💮 Test 🛛 📹 Apple M	eindata								
	Source Name	4										
	Record No.: 6	573211										
	File Name: De File Path: /Us	tail view of Spac ecs/williamcomp	eExped Rever Long bell/Downloads/Detail very	of SpaceExped	Rever 1.png							
	Incide He./His ID: (2103)										1000	1000
	File Size: 175.20 K8 (17652) bytes) bine Type:										AR	
	Date Modilie	d: 2021/04/02 13	7:40:23 +00:00								Server.	Same and
	Date Change Date Access	: 2021/04/12 13 ed: 2021/04/12	:13:51 ±00:00 13:13:45 ±00:00							-	1	1
										-		and a
	Tag:									3	at the lot of the lot	
	Examiner Not	8552										
										ALC: NO		
c >										Preview		

# 36. Importing your Case into RECON LAB

Case folders exported and analyzed in RECON CASE READER can be loaded back into RECON LAB for further analysis or more robust report generation.

Simply select to Load Case when starting RECON LAB and point to the case folder used in the RECON CASE READER.

# 37. Weapon Analysis

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

## **37.1 Processing for Weapon Analysis**

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



# **37.2 Weapon Analysis Results**

Results for weapon analysis are put into their own category on the left menu. The results are broken into two subcategories of Guns or Rifles.

After selecting a category results are displayed in the main pane. Results can be viewed as either a list of files or in a gallery view.



# 38. Fire Analysis

The Fire Analysis File System Module allows RECON LAB to automatically identify and categorize pictures that have fire in them. Detected pictures will be put into their own category for easy analysis.

## **38.1 Processing for Fire Analysis**

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

#### options including Fire Analysis.

🔲 54083 24812 💼 Us	ers	2021/03/19 09:22:0
□ 105022 24816 <b>□</b> Ag □	Bookmark Remove Bookmarks Tags Þ	2021/04/09 19:38:4
iam_Campbell_MacBook.dmg/APPLE SSD - Data	Add Note Remove Note	
24812	Quick Look Open With Send To Bucket Export Add To Text Indexing Queue Carve Files Carve Data	
1-Mar-19 09:22:05 -5:00 -Mar-19 09:22:05 -5:00 21-Mar-19 09:22:23 -5:00	Add file to hashset database Search file with same hash Run Filesystem Modules	n Apple Metadata
: 2021-Mar-17 16:13:43 -5:00 bate(Apple): 2020-Jan-01 03:00:00 -5:00 on Date(Apple): 2020-Jan-01 03:00:00 -5:00 ple): 2021-Apr-06 18:15:57 -5:00 :	Export Hashes As Open Detailed Information Open with External Application Copy to Clipboard Mark As Seen Mark As Unseen	<ul> <li>Exif Metadata</li> <li>Signature Analysis</li> <li>Hashes</li> <li>Face Analysis</li> <li>Optical Character Recognition</li> </ul>
0:00 -5:00	Hide Seen Files Show Seen Files	Weapons     Fire Analysis     Silin Taxa Datation
	Decompress File Face Search	Skin Tone Detection

### **38.2 Fire Analysis Results**

Results from Fire Analysis are displayed in their own category in the left menu. After selecting Fire Analysis results are displayed in the main pane and can be viewed in a file list or a gallery view



	Search Filters 💟	Show All					
			Files	Gallery View			
Record No.	File Name	File Size	Date Modified	Date Change	Date Accessed	Last Used Date	Use Count
1 🖂 7	download-3.jpg	10992	2022/01/07 11:00:03 -5:00	2022/01/20 16:48:37 -5:00	2022/01/20 16:48:40 -5:00		
2 🔲 10	download-5.jpg	8164	2022/01/07 11:00:06 - 5:00	2022/01/20 16:48:37 -5:00	2022/01/20 16:48:40 -5:00		
3 🛄 11	download-4.jpg	9386	2022/01/07 11:00:05 -5:00	2022/01/20 16 48:37 -5:00	2022/01/20 16:48:40 -5:00		
4 🗌 13	# download-6.jpg	9829	2022/01/07 11:00:32 -5:00	2022/01/20 16:48:37 -5:00	2022/01/20 16:48:40 -5:00		
Source Name: /untitled folder 2							
Record No.: 10 File Name: download-5.jpg File Path: /untitled folder/download Inode No./File ID: File Size: 7.97 KB (8164 bytes)	I-Sjpg						
Mime Type: image/jpeg Date Modified: 2022-jan-07 11:00 Date Change: 2022-jan-08 16:48 Date Accessed: 2022-jan-20 16:48 Tag: Examiner Notes:	06 - 5:00 7 - 5:00 1:40 - 5:00						

# **39. Skin Tone Detection**

The Skin Tone Analysis File System Module allows RECON LAB to automatically identify and categorize pictures that have a detected skin tone in them. Detected pictures will be put into their own category for easy analysis.

# **39.1 Processing Skin Tone Detection**

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

## **39.2 Skin Tone Detection Results**

Results from Skin Tone Detection results are displayed in their own category in the left menu. After selecting Skin Tone Detection results are split into different file types.

Skin Tone Detection								
✓ image								
image/tiff (2)								
image/jpeg (21)								
image/png (4)								
image/webp (2)								

After selecting a file type results are displayed in the main pane and can be viewed in a file list or a gallery view.

			Search	Filters 🖸	Show All						
								Files Gallery Vi	ew		
1		Record No.	F	ile Name		Extension	File Size	Date Modified	Date Change	Date Accessed	Last Used Date
1 🗆		67696	0B54CB0E1	E8684188DF	AE32DE		69999	2021/04/07 19:36:47 -5:00	2021/04/07 19:36:47 -5:00	2021/04/07 19:36:47 -5:00	
2		72451	ESFECF423	2970733239	SF7FA1		5788	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	
3 🖂		72858	D02709FEF	628245D681	E7389		14875	2021/04/08 16:32:54 -5:00	2021/04/08 16:32:54 -5:00	2021/04/08 16:32:54 -5:00	
4		73352	9668C674	4C99B184C0	DE09F7		4312	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	
5 🗋		73399	BF467BDE6	80C0502351	38409		55470	2021/04/07 19:35:19 -5:00	2021/04/07 19:35:19 -5:00	2021/04/07 19:35:19 -5:00	
6		73438	B9F0935E4	45187090E1	BC2666		77982	2021/04/07 19:35:19 -5:00	2021/04/07 19:35:19 -5:00	2021/04/07 19:35:19 -5:00	
7	t	73868	500281D8	3C27FEA452	08528F		14875	2021/04/08 16:32:54 -5:00	2021/04/08 16:32:54 -5:00	2021/04/08 16:32:54 -5:00	
8		74385	2AE1A4E6/	836383F071	34040		5788	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	
9		74498	C438887F2	9286CAEAA8	0DD28		\$5470	2021/04/07 19:35:19 -5:00	2021/04/07 19:35:19 -5:00	2021/04/07 19:35 19 -5:00	
10		67696	0B54CB0E1	E8684188DF	AE32DE		69999	2021/04/07 19:36:47 -5:00	2021/04/07 19:36:47 -5:00	2021/04/07 19:36:47 -5:00	
11		72451	ESFECF423	2970733239	SF7FA1		5788	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 - 5:00	
12		72858	D02709FEF	6282450681	E7389		14875	2021/04/08 16:32:54 -5:00	2021/04/08 16:32:54 -5:00	2021/04/08 16:32:54 -5:00	
13 🖂		73352	9668C6741	4C998184C0	DE09F7		4312	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	2021/04/08 16:35:29 -5:00	
Record / File Nam File Path Inode Ni File Size Mime Ty Date Mo Date Chi Date Act	No.: 73868 se: SDD281D83 s: /Users/williar o./File ID: 3785 : 14.53 KB (148 rpe: image/ipes dified: 2021-A ange: 2021-A ange: 2021-A	C27FEA452085 ncampbell/Libri 175 bytes) 1 pr-08 16:32:54 spr-08 16:32:54	528F6DF29EB5/ ary/Containers 1 -5:00 -5:00 4 -5:00	1892FE4B /com.apple.S	afari/Data/	Library/Cacl	nes/com.apple.S	afari/WebKRCache/Version 16/8	ilobs/5DD281D83C27FEA45208528F6	DF29E854892FE48	
Tag: Skir Examine	nTone r Notes:										

# 40. Face Analysis

The Face Analysis File System Module allows RECON LAB to automatically identify and categorize pictures that have a detected face in them. Detected pictures will be put into their own category

for easy analysis. After faces are identified examiners can then search for faces using the Face Search Feature.

# 40.1 Processing for Face Analysis

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



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

## 40.2 Face Analysis Results

Results from Face Search are displayed in their own category in the left menu. After selecting Faces all of the detected faces will be displayed in one section. Files can be displayed as either a

list of files or a list of faces.



The Faces option for displaying results will show a list of faces and all images associated with each face. Simply click on each face to show a gallery of all images associated with the detected face.



### 40.3 Face Search

After indexing faces with the Face Analysis file system module examiners can import an image and search for any pictures with that face in them.
In the Menu Bar select Search>Recognize Face.

ć	RECON_LAB	Process	Search	Timeline	Export	t Rep
<ul> <li>All Features</li> <li>Update (355)</li> <li>EFI (11)</li> </ul>			File Search Content Search Exif Metadata Search Apple Metadata Search Artifacts Keyword Search			Face Ana
			Recogniz	e Face		

A window will pop up that allows examiners to load a file of their choosing. Click the three dots at the top of the window to open a Finder window and navigate to your desired picture. After the picture is selected click the Extract Faces button to detect the face in the picture.

After the face is detected add a name to save the results as and click Start.

•	Recognize Face	
Users/john/Dov	wnloads/Danny-DeVito-e1627433269130.jpeg	
	Extract Faces	
Save Result A	As: Danny	
	Start	

Face Search results will be displayed in the left menu under Face Search.

🗸 🙎 Face Analysis				
Faces (7)				
🗸 🧧 Face Search				
Danny (3)				
	1			

Results will be displayed as a file list view and can be changed to a gallery view for easy analysis.



## 41. Optical Character Recognition (OCR)

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

### 41.1 Processing Optical Character Recognition (OCR)

Optical Character Recognition is processed as a file system module and is accessed by rightclicking a file or directory in the file system. The screenshot below shows the file system module processing options including Optical Character Recognition.

### 

### 41.2 Optical Character Recognition (OCR) Analysis

Results from Optical Character Recognition are displayed in their own category in the left menu. After selecting Images all of the pictures with extracted text will be displayed in the main pane. Files can be displayed as either a list of files or a gallery view.

(>)	Optical Character Recognition 😄	8.		Images		6 X		
	Search	Filters 🕑	Show All					
				Files	Gallery View			
d No.	File Name	File Size	OCR Text		Date Added	Content Creation Date	Content Modification Date	Mirne Typ
110	= 1*uWTDCY6fdhe8fyHETtXhDQ	112705	e000 ATAT & 5:21PM 7 62%		2021/12/29 23:45:02 -5:00	2021/12/29 23:41:43 -5:00	2021/12/29 23:41:43 -5:00	image/png
113	47dc1888a95d41983042d8e2	76985	ATE > PM		2021/12/29 23:45:02 -5:00	2021/12/29 23:41:51 -5:00	2021/12/29 23:41:51 -5:00	image/jpeg
112	<ul> <li>912968-guotes-typography</li> </ul>	196725	ABILITY IS WHAT		2021/12/29 23:45:02 -5:00	2021/12/29 23:42:09 -5:00	2021/12/29 23:42:09 -5:00	image/ipeg
92	= 5b1b82579771868c86e79781	402587	"Why was there a piece of		2021/12/29 23:45:02 -5:00	2021/12/29 23:41:36 -5:00	2021/12/29 23:41:36 - 5:00	image/jpeg
urce Nan	e: /ND.dmg/ND						1	
cord No. e Name: e Path: /! ode No./!	92 5b1b82579771868c86e797810308fb4 b1b82579771868c86e797810308fb4 (le ID: 1 5 CF (402587 hyrac)	d.jpg d.jpg						
me Type	image/jpeg							
CR Text: " te dogs bo Civessace	Why was there a piece of , ) bread crust wl. So either 1) dog was like   don't war sr (No riddle! )	t in my shoe? Is nt no fing brea	this a riddle or a legitimate question? Well Xo d crust and put it in your shoe or Z) one of the	e dropped a pie cats was like o	ice of cheese on the floor so she pu loood bread crust! I'll just stash that	It the cheese and her bread crust in away for later and put it in your shoe	(Mary Mill (Mary A) Sandar Annar Mary	224L
ate Addec ontent Cri ontent Mo	(Apple): 2021-Dec-29 23:45:02 -5:00 sation Date(Apple): 2021-Dec-29 23:4 dification Date(Apple): 2021-Dec-29	) 11:36 -5:00 23:41:36 -5:0	0				Construction of the second sec	2000 A. 1920 - 19 19 19 19
lg:							den de l'expensione de la constante de la constant	Lawyer
kaminer N	otes:							

A preview of the extracted text is shown in red under the OCR Text column.

Searching the extracted OCR text is done using the Search box at the top left corner of the Optical Character Recognition Pane. To search OCR indexed text click the Filter dropdown menu and check the OCR Text option.



The Show All button will remove the search filter and show all indexed files again.

After selecting the file the full OCR indexed will be displayed in the Detailed Information pane under OCR Text:

# 43. Examiner Space

RECON LAB's examiner space is a feature that allows examiners to easily take notes about their case and add those notes to their final reports. The Examiner space has an Examiner comments note-taking area and a to-do list.

### 43.1 Examiner Comments

The Examiner comments tab acts as a general note-taking option where examiners can add notes about their current case. Examiners can edit their text using the options in the top left for **bold**, *italic*, <u>underline</u>, and font color.

The export button in the center of the window allows examiners to export their report in either a PDF or HTML format.



The Add Timestamp button will inset a timestamp of the current machine time as either UTC (by checking the Use UTC box) or the current timezone offset of the examination machine.

### 43.2 Adding Examiner Notes to a Report

Examiner Notes can be added to a storyboard report as their own item. Once examiners create a storyboard report (see section 31.3 for how to generate a storyboard report) the same way any other bookmark is added.

Simply choose the Examiner Space option from the dropdown menu and add the record by rightclicking and selecting Add Record.

# 44. Terms and Conditions

#### **RECON LAB**

Copyright 2013-2024 – SUMURI LLC

#### 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.