SUMURI

RECON IMAGER

MANUAL

1.Introduction

RECON IMAGER was developed by SUMURI to provide the digital forensic practitioner with a bootable imaging utility that supports all modern Macintosh computers with Intel processors. This is accomplished via three macOS based boot environments that have been modified to ensure that there are no writes to internal or externally attached media.

Additionally, RECON IMAGER helps the practitioner to easily identify Apple File System (APFS) container disks and volumes, FileVault, Fusion and other Core Storage volumes.

RECON IMAGER has been designed to get as much data as possible to include the Apple Extended Attributes and Local Time Machine Snapshots (APFS Snapshots).

In addition to creating forensic images of physical disks and/or volumes, RECON IMAGER can also image Mac RAM without the need for an administrator password within RECON IMAGER's boot environment.

RECON IMAGER also supports imaging Macs with T2 Security Chipsets via Target Disk Mode or disabling Secure Boot via the Mac's Recovery Mode.

2. Version Comparisons

There are two versions of RECON IMAGER – Standard and PRO.

RECON IMAGER PRO is now included in RECON ITR.

RECON IMAGER (Standard)

RECON IMAGER (standard) is based on macOS. Since it is based on macOS it natively boots Intel Macs. It also supports Apple proprietary technology such as Apple File System (APFS) container disks and volumes, FileVault, Fusion and other Core Storage volumes. RECON IMAGER includes the option to image logically which allows an examiner to import Apple data into forensic tools that do not natively support proprietary Apple file systems. This allows you to use any forensic tool to process the data.

RECON IMAGER PRO

In addition to all the features of RECON IMAGER (standard), RECON IMAGER PRO includes a new Enhanced Logical Imager and the ability to image to a network server. The Enhanced Logical Imager allows the user to capture and preserve a variety of Mac artifacts automatically. The collected artifacts can be processed manually or automatically using RECON LAB.

The Enhanced Logical Imager also allows the user to create an image or logical copy of individual files and/or directories selected by the collection agent. For example, if you are limited to accessing data from a single user it is possible to only select that user's directory for imaging.

RECON IMAGER PRO also includes the ability to image across a network via SMB. This allows collections agents to image directly to an evidence server within a lab or to a NAS out in the field.

3. Supported Hardware

RECON IMAGER works with Intel-based Macs and has three boot options installed to support the largest numbers of Macs.

Always start with the highest Mode ("A" being the lowest, "C" being the highest) for your supported hardware. For example, if a Mac is supported by Mode-B and Mode-C, try Mode-C first.

For specific models supported please see below.

3.1 MODE A - SUPPORTED HARDWARE (Version 4.0.0)

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

3.2 MODE B - BOOT SUPPORTED HARDWARE (Version 5.0.0)

- MacBook (Late 2009 or newer)
- MacBook Pro (Mid 2010 or newer)
- MacBook Air (Late 2010 or newer)
- Mac mini (Mid 2010 or newer)
- iMac (Late 2009 or newer)
- Mac Pro (Mid 2010 or newer)

3.3 MODE C - SUPPORTED HARDWARE (Version 5.0.7 A2)

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

4. Before You Start

Imaging a Mac disk or volume is not as straightforward as imaging other file systems. We highly recommend that you read the following sections before you begin as it will save you from creating an unusable image.

4.1 How Will You Process The Image?

Before using RECON IMAGER you must ask what tool will be used to process the image that is created with RECON IMAGER?

Other than RECON LAB, there are no forensic tools that fully support all of Apple's proprietary file systems, technologies, and artifacts.

RECON LAB is the only forensic suite designed completely on a Mac to natively support Mac images and its data.

If you are going to process your image with any other tool other than RECON LAB you will miss case-solving data.

4.2 What To Image?

Once you have decided on the forensic tool that will be used to process the collected data the image format can now be chosen.

RECON IMAGER utilizes macOS so it will automatically detect and present traditional physical disks, logical volumes, Core Storage disks, FileVault volumes, synthesized and virtualized disks and volumes. Collection agents must be careful to select the correct volume or disk in addition to the correct image format to get usable forensic images or data.

This manual will include best practices on what to image based on what forensic tool of your choice.

It is recommended that all information in this manual is reviewed. As always, if unsure, verify before imaging.

4.3 What Image Format Should I Use?

Selecting the correct image format is crucial to get an image or data that will work with a specific forensic tool. RECON IMAGER has multiple imaging options to support as many forensic tools as possible.

It is important to understand that not all forensic tools can interpret proprietary Apple file systems and/or volumes. SUMURI's RECON LAB is one of the only tools that can mount all Apple file systems and interpret its data properly as it is developed on and for macOS.

In order to obtain data that can be used with other tools that do not support proprietary Apple file systems or volumes, one of RECON IMAGER's logical imaging options must be selected.

5. Key Concepts To Understand

Before using RECON IMAGER it is important to understand key concepts about imaging Mac computers.

5.1 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.

RECON IMAGER can create forensic images that can be processed and analyzed with RECON LAB natively.

RECON IMAGER can also create "logical" copies of an APFS drive. RECON IMAGER's "logical" image can be imported by any forensic tool that supports adding directories or files (including Windows forensic tools).

5.2 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 RECON IMAGER and processed by RECON LAB provide the most extensive views of Apple Extended Metadata.

Understanding Apple Extended Metadata is critical to investigations.

For example, macOS utilizes Apple Extended Attributes for timestamps in favor of POSIX timestamps.

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

5.3 Fusion Drives

Some Mac computers utilize Fusion Drives which are a "marriage" of two or more physical disks which are then seen as a single drive. Originally, the smaller disk was an SSD (for speed) and the larger disk was typically a traditional spinning platter drive (for low-cost long term storage). Keep in mind that both disks in a Fusion Drive can be SSDs.

Forensic examiners are traditionally taught to image the physical disks. This would be true if using most other imaging utilities (such as PALADIN). In order to properly see the directory structure of a Fusion "disk" when utilizing other imaging solutions to process in traditional forensic tools, you would have to manually mount both images on a Mac and then re-image. However, this is not necessary when using RECON IMAGER.

In RECON IMAGER, a process known as Core Storage "marries" the two disks of the Fusion drive into a "single" disk. Imaging the "single" disk created by Core Storage will allow you to obtain a forensic image where the files and its directories can easily be seen by most forensic tools.

5.4 Core Storage

Core Storage is the macOS version of Logical Volume Management (LVM). Core Storage (or LVM) is used by the Mac as a way of allowing one or more physical disks to be seen as a single new disk. This was first utilized by Apple to support

Fusion drives. However, Core Storage is used by the macOS even if there is only a single disk in the system for macOS Extended file systems (HFS+).

RECON IMAGER will allow you to see traditional physical disks and Core Storage "virtualized" disks. In most situations, the Core Storage "virtualized" disk "derived from" a Core Storage volume or volumes will be imaged.

5.5 FileVault

FileVault (version 2) is 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 IMAGER can create a decrypted forensic image of a FileVault volume by providing the user's login password or the Recovery Key. If the password or the Recovery Key is not known the disk or volume can still be imaged in its encrypted state (this applies to non-T2 Chipset Macs).

The created image can be processed with RECON LAB if the password or Recovery Key is obtained later.

5.6 T2 Security Chipset

In newer Macs, Apple has added the T2 Security Chipset. The T2 Security Chipset serves several purposes, however, a couple of them require extra steps in order to collect data or an image.

By default, Macs with T2 Security Chipsets have Secure Boot enabled along with a setting to disable booting to external media. Both of these settings must be turned off to allow the Mac to boot to RECON IMAGER. To turn off these settings an admin password must be known.

If the admin password is unknown, the Mac with the T2 Security Chipset can be placed in Target Disk Mode and can be connected to another Mac booted with

RECON IMAGER to obtain data. This is true of Macs with macOS 10.14.4 or below.

Please note, Macs with macOS 10.14.5 or above, will require an admin password to connect to another Mac.

5.7 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). When 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 referred to as APFS Snapshots by some.

RECON IMAGER is the only solution that can display, image and hash Local Time Machine Snapshots in Macs with T2 Security Chipsets and without.

5.8 Apple Boot Camp

Apple Boot Camp is a technology that assists a Mac user with installing a Windows operating system on a Mac. Forensic images of the Boot Camp volumes can be created with RECON IMAGER.

6. Booting RECON IMAGER

As with any new forensic tool, please test and validate RECON IMAGER before using on real evidence.

Additionally, please read all the instructions and information included in this manual. If you should have any questions or concerns please contact us.

6.1 Instant On - Portable Macs

Be aware that newer MacBooks have an "instant-on" feature.

Newer MacBooks will automatically boot when the lid is opened. Additionally, if the lid is already opened and power is connected, or the trackpad or keys are touched the MacBook may also start.

Make sure that you are prepared to interrupt the boot process by holding down the ALT/OPTION key in any of these situations.

6.2 Firmware Password

Mac has the ability to set a boot level password to prevent booting to any source other than the installed macOS. This is known as a Firmware Password which can be enabled or disabled by the user in the macOS Recovery Mode.

Before booting a Mac please familiarize yourself with the macOS Firmware Password option.

If a user has set the Firmware Password no startup commands other than the ALT/OPTION key will prevent booting to the login screen. If you encounter anything that looks like a "lock" when starting with the ALT/OPTION key then the Firmware Password is set.
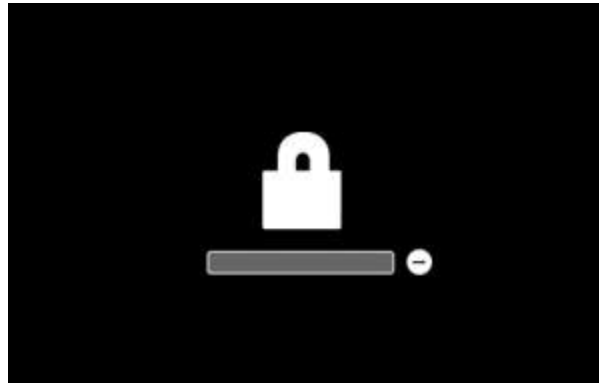
You must enter the Firmware Password PIN or passcode in order to see the boot options (this includes RECON IMAGER if it is attached).

Apple Certified Technicians have the ability to disable a Firmware Password.

6.3 Connecting RECON IMAGER

- Make sure that you start with the Mac powered off.
- Identify how many ports and what type of ports which are available on the Mac before you start.
- If there is only one port make sure you use a high-quality hub to add additional ports. Keep in mind that using low quality or non-Apple certified adapters can damage the Mac.
- If using traditional spinning platters make sure that the hub used has power connected or that your drive has its own power supply.
- RECON IMAGER can be inserted into any open port on the Mac itself or via a hub using the Type-A or Type-C connector.

6.4 Connecting Your Destination Drive

See the notes listing in "Connecting RECON IMAGER" regarding adapters, hubs, and power.

It is recommended that the formatting or initialization of the destination drive be done using RECON IMAGER, if possible.

Once the destination drive is prepared using RECON IMAGER it should be removed and tested to see if it mounts on the examination system. This step is recommended as formatting with one tool or environment may be different from another. Some operating systems may not recognize or work well with the partitioning scheme created with a different operating system.

After verifying that the destination drive can be seen by the examination system reconnect it to the Mac to be imaged.

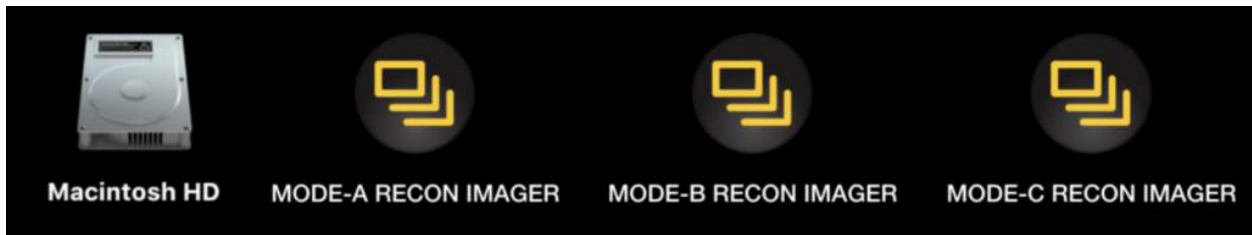## 6.5 Starting RECON IMAGER

With the Mac off, connect RECON IMAGER to an open port, press the power key, and then immediately hold down the OPTION/ALT key.

All boot options, including three from RECON IMAGER, should be displayed. Please review the supported hardware documented in this manual for assisting in choosing the correct version of RECON IMAGER.

Select the boot option that best supports the Mac being booted:

- MODE-A RECON IMAGER
- MODE-B RECON IMAGER
- MODE-C RECON IMAGER

MODE-C is for newer Macs, MODE-A is for the oldest Macs and MODE-B is for everything in-between.

The Mac will start to boot after the selection. Be patient as this may take a couple of minutes to boot. You will see the Apple Boot Logo or the SUMURI logo while RECON IMAGER boots the Mac.

Selecting MODE-C RECON IMAGER will prompt a language selector for English or Chinese.

After RECON IMAGER has completed booting you will see the window below. Select the RECON IMAGER application and click the "Continue" button.
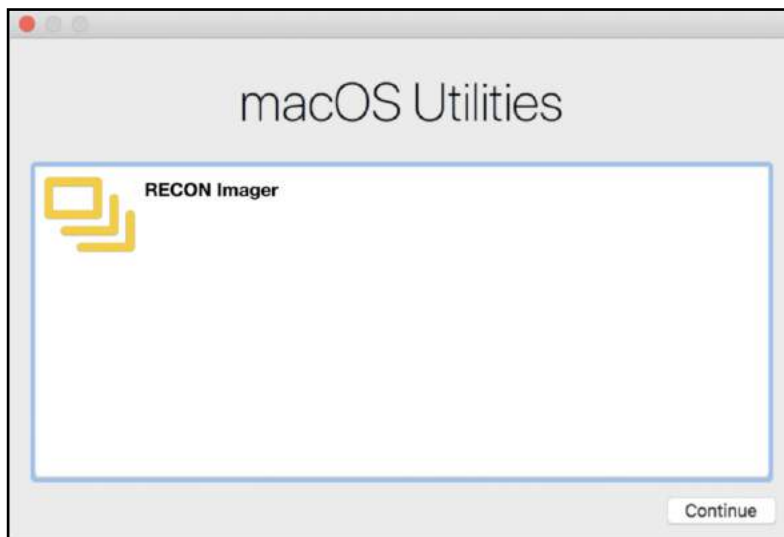
7. Using RECON Imager

When RECON IMAGER loads there will be five options presented for the standard version and seven for RECON IMAGER PRO.

- Disk Manager – Displays traditional, virtual and synthesized disks and volumes.
- Disk Imager – The disk imaging interface.
- RAM Imager – The RAM imaging interface.
- Network Share (PRO) – The interface for configuring SMB network connections to send forensic images to a destination over the network.
- Logical Imager (PRO) – The interface for automated imaging of macOS artifacts or selective imaging of files and folders.
- Shut Down – Safely powers down the Mac.
- License Agreement – Displays SUMURI's License Agreement and Change Logs.

7.1 Disk Manager

The Disk Manager allows you to see all connected devices to the Mac in a software write-blocked environment. Each system can vary, however, the Disk Manager will show all traditional, virtual or synthesized physical disks and logical volumes.

Below are descriptions of the column names used in the Disk Manager:

- Device – the disk and partition (slice) identifier
- Location – if the drive is internal or external
- Model – hardware model

- Size – the size of the disk/partition
- Type – disk or volume type
- Name – volume name
- File System – the file system of the partition
- Derived From – list of the parent volumes for virtualized or synthesized disks
- Encrypted – YES, if encryption (ex. FileVault) is on – NO, if encryption is off
- Mode – displays the read-write status

The RECON IMAGER Disk Manager uses the following color scheme for quick identification:

- Parent disk (i.e. "disk0") – grey
- Mounted and Read-Only (i.e. "disk0s3") – green
- Mounted and Read-Write – red
- Apple Core Storage Logical Volume Family (i.e. "disk2s2" and "disk3s2") – orange
- Mounted Fusion Disk (i.e. "disk4")- yellow
- APFS Partitions – light brown
- APFS FileVault Decrypted – olive green

7.1.1 Refresh To Detect Changes

If a drive is attached or disconnected anytime after RECON IMAGER has been started the "Refresh" button must be clicked to search for new drives or remove drives that were previously detected.
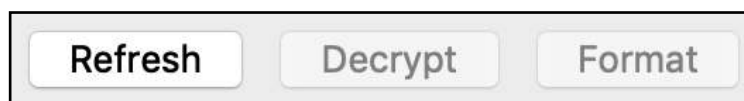
7.1.2 Formatting a Collection Drive

RECON IMAGER can format a collection drive within Disk Manager. BE
CAREFUL to select the correct disk to format.

From the Disk Manager tab select the disk to format and choose "Format".
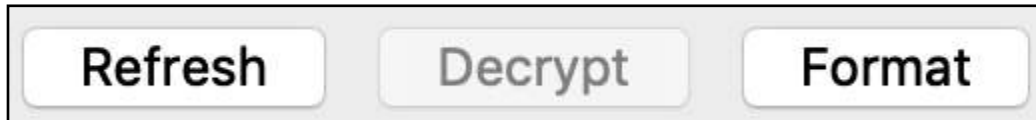
A confirmation message will appear.

The collection drive can be formatted with an APFS, macOS Extended (HFS+) or exFAT file system.
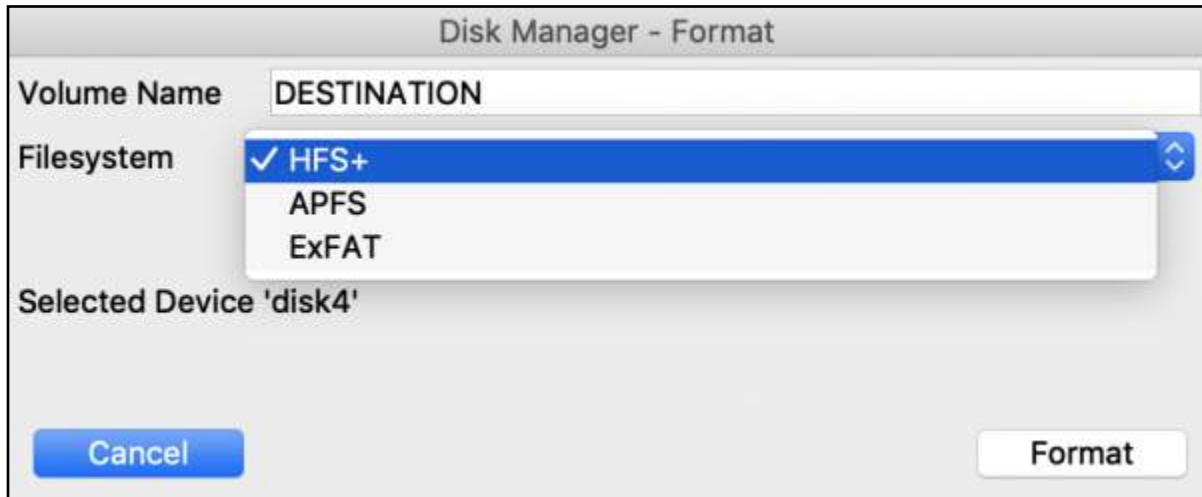
Once the collection drive has been formatted it is always good practice to attach the destination drive to the examination system to see if it will be detected properly. Although, the file system is correct the examination system may not recognize the partition scheme used in formatting. This is especially true of older operating systems.

 It is highly recommended that you use HFS+ (macOS Extended) for native support in Mac environments and to preserve Apple Extended Metadata during logical imaging.

To mount Apple native file systems within Windows consider using applications such as HFS+ for Windows by Paragon.

7.1.3 Decrypting A FileVault Volume

If an encrypted volume is found, RECON IMAGER will display a pop-up window with the disk and volume number of the encrypted disks or volumes.
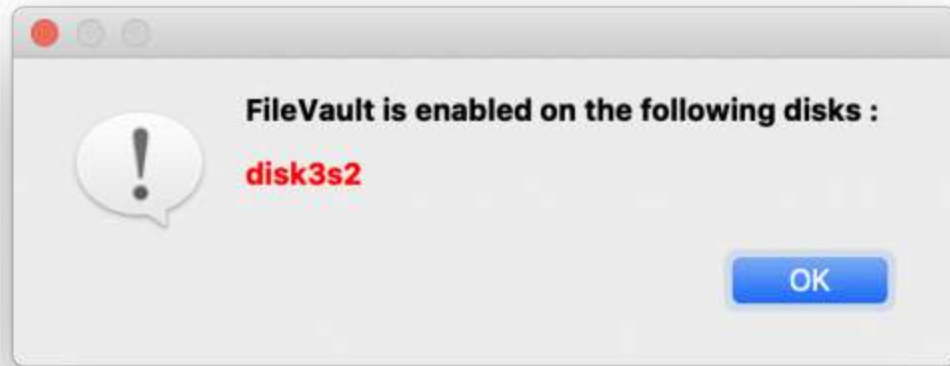
In the Device Manager you will also see "YES" in the "Encrypted" column to identify any encrypted disks or volumes.

RECON IMAGER can decrypt FileVault 2 encrypted volumes if the passcode or the Recovery Key is known. To decrypt, highlight the FileVault volume within Disk Manager and select "Decrypt".

A window will appear allowing the entry of the user's password or the Recovery Key. Once the password or key is entered select "Decrypt."

After a few moments, a status message will appear and the decrypted FileVault volume will display within the Disk Manager window.

If the FileVault volume was on a macOS Extended file system (HFS+) a new decrypted volume will mount with a new disk number.

If the FileVault volume was on an APFS file system no new volumes will mount.

7.1.4 System Date and Time

System Clock: 2019-Oct-09 14:56:56 PDT

For convenience, the system's detected date and time will appear at the bottom of the RECON IMAGER window. This can be used to check to see if the reported system clock is accurate.

7.2 Disk Imager
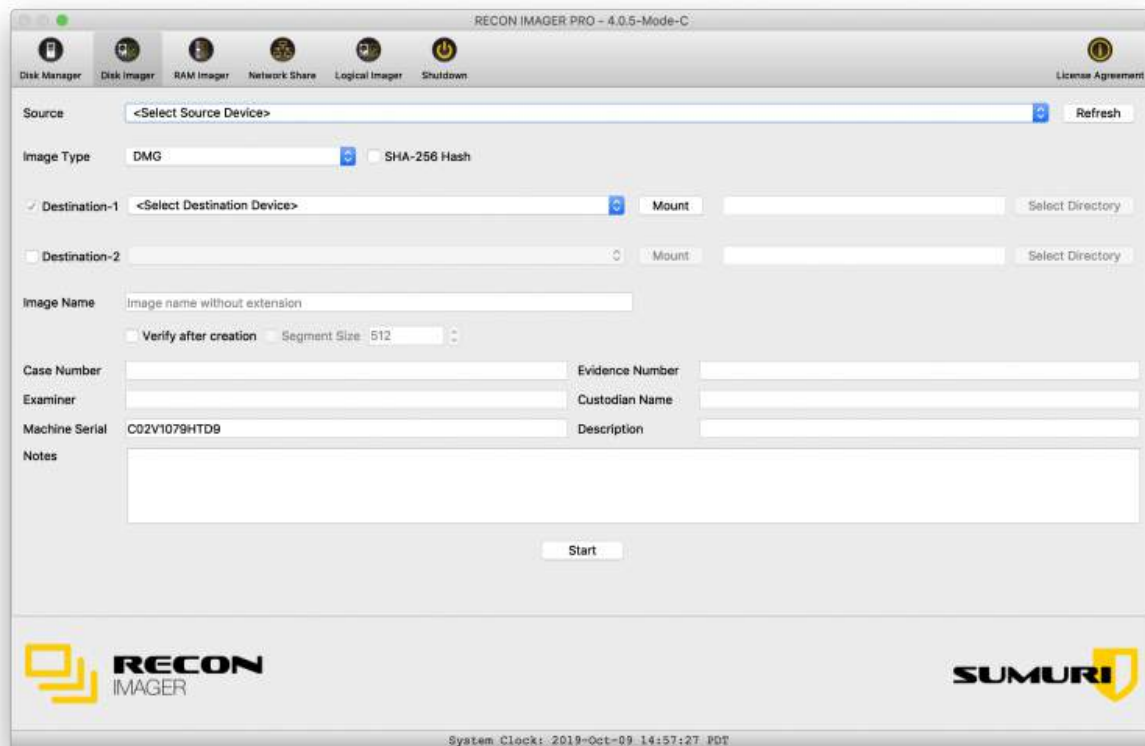
The RECON IMAGER Disk Imager allows for the acquisition of any internal disk(s) or volumes or any attached storage media including other Macs in Target Disk Mode. The options presented in the Disk Imager will change depending on what Image Type (output format) is selected.

7.2.1 Source

The Source field allows you to select the source device (e.g., the suspect's hard drive) to be imaged.

If the drive was recently attached, select Refresh to identify any newly connected disks.

WARNING – Please be familiar with imaging Apple file systems. There are many factors that will affect your selection for the source and the choice of an output format.

An incorrect choice will lead to an unusable image. Please follow the best practices suggested in this manual for different imaging scenarios.

7.2.2 Image Type

RECON IMAGER supports a variety of image output formats in order to allow the data to be imported into any modern forensic tool. Before selecting the Image Type be sure to check that forensic tool to be used for processing can support the output that you are generating. Many forensic tools do not natively support Apple's proprietary file systems. SUMURI's RECON LAB can process all Apple file systems without conversion and without losing important artifacts such as Apple Extended Metadata.

RECON IMAGER can produce output in the following formats:
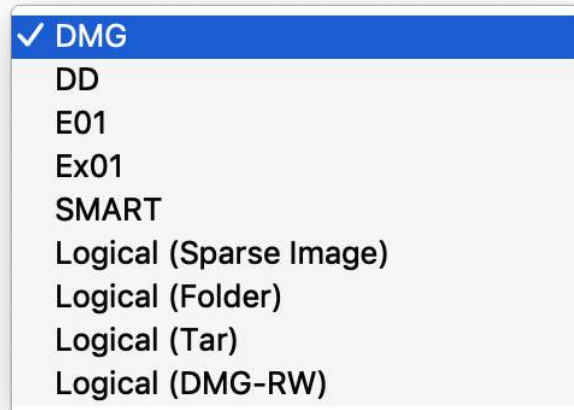
- DMG (dmg): The native disk image format for macOS and what is highly recommended for image output. This image output is also a raw image that can be imported into any modern forensic tool.
- DD (RAW): Bit-for-bit forensic copy of the source medium which is also a raw image.
- EWF (E01): Expert Witness Format – Version 1.
- EWF2 (Ex01): Expert Witness Format Version 2.
- SMART (S01): ASR Data's version of EWF bitstream image.
- Logical (Sparseimage): A native macOS image format that is dynamic and can only be used within the Mac environment.
- Logical (Folder): A logical data extraction of the file system which is able to be used in both Mac and Windows forensic tools.
- Logical (Tar): A logical archive of the file system that can be used in most forensic tools.
- Logical (DMG-RW): A native macOS image format that is static and can only be used within the Mac environment.
- ASR (Sparseimage): ASR imaging uses Apple's native system restore feature to logically acquire a sparseimage of a machines Synthesized Disk

7.2.3 Compression Options

Compression options are available for the Expert Witness formats (.E01, .Ex01) and ASR Data's SMART image format (.S01).
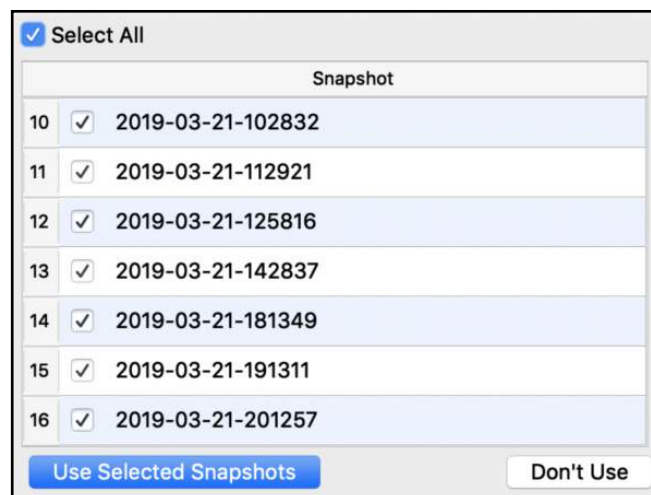
- none: No compression (fastest)
- fast: Compression is minimal while imaging speed is maximized (fast).
- best: Compression is the most efficient, however, the imaging process will be prolonged (slowest).

7.2.4 Processing Local Time Machine Snapshots (APFS)

RECON IMAGER is an intelligent imager and the only solution to identify Local Time Machine Snapshots (APFS Snapshots) prior to imaging

If Local Time Machine Snapshots exist a window will appear allowing the user to select all or individual snapshots for imaging.

Once selected, RECON IMAGER will process the Local Time Machine Snapshots at the time of imaging to dramatically reduce the size of the collection as compared to physical imaging.

RECON IMAGER's Advanced Snapshot Processing finds all files modified or previously deleted by the user within the snapshots selected.

7.2.5 Destination
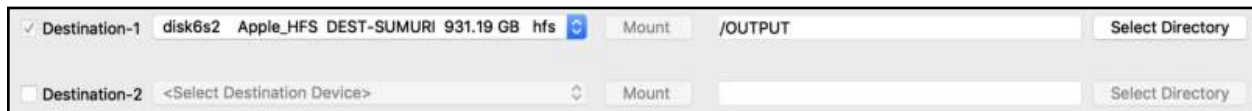
RECON IMAGER has the ability to image to two destinations at the same time. If a second destination is required just select the checkbox to activate the dropdown.

RECON IMAGER also allows you to choose and/or create directories to send the images to by clicking "Select Directory."

7.2.6 Image Name

Use the "Image Name" field to provide a unique name for your image output. The label provided will be the name for the parent folder containing the image output and any logs.

Other than the Logical Image (Folder) option the name provided in the "Image Name" field will also be used for the image output files.

7.2.7 Segment Size

RECON IMAGER allows for certain image outputs to be segmented if required. If the image output selected supports segmenting within RECON IMAGER the "Segment Size" checkbox will be active.

To set the segment size check the box next to "Segment Size" and enter the size in MBs.

Segmenting is not available for the .dmg image output or any of the logical imaging formats.

7.2.8 Evidence Descriptor Fields

Before imaging, optional identifying information about your source may be entered.

- Case Number – Relevant case number.
- Evidence Number – Unique evidence/log number.
- Examiner – Individual creating the image.
- Custodian Name – Custodian of the evidence.
- Machine Serial – Serial Number of the booted device which is automatically populated when possible

○ MODE-C RECON IMAGER - Unchecking the machine serial box will allow the examiner to manually input a serial number

- Description – Description of the media being imaged.
- Notes – Any additional information relevant to the investigation.

7.2.9 Hashing and Verification

Traditional Image Types

An MD5 and SHA-1 hash of the SOURCE will be calculated for the following image types:

- dd (RAW)
- EWF (E01)
- EWF2 (Ex01)
- SMART (S01)
- DMG (dmg)

For DD and DMG images there is also the option to select SHA-256.

For the traditional image types listed above, there is an option of selecting "Verify after creation" within Disk Imager.

If "Verify after creation" is selected an MD5 and SHA-1 will be calculated for the OUTPUT.

A summary of the hashing will be displayed in a pop-up window at the completion of the imaging and can also be found in the logs within the image output folder.

Logical Image (Folder)

For the Logical Image – Folder option a hash can be calculated for both the "Source" files and the files copied to the "Destination".

Logical Image (Tar)

For the Logical Image – Tar option a hash can be calculated for both the "Source" files and of the .tar image created on the "Destination".

Logical Image (Sparseimage and DMG-RW)

For the Logical Image – Sparseimage and DMG-RW option a hash can be calculated for both the "Source" files and the files copied to the "Destination".

Note: Be advised that the hashing of every individual file during a "Logical" image WILL TAKE TIME.

8. APFS Imaging

Many forensic tools do not natively support APFS. By creating a "traditional" image your forensic tool may not see the data.

Traditional forensic tools that can mount APFS volumes may still have limitations such as:

- no access to Apple Extended Metadata
- limited access to Apple Extended Metadata

- limited parsing of Apple Extended Metadata
- inability to utilize proper timestamps

RECON LAB from SUMURI is the first and only tool that can identify and properly parse Apple Extended Metadata and its timestamps.

Apple Extended Metadata is extremely important in macOS investigations. Ignoring Apple Extended Metadata is equivalent to a doctor performing surgery after only seeing a small portion of an entire battery of test results and scans.

There are two ways to image APFS. The first is for processing with RECON LAB in order to see all the Apple Extended Attributes and timestamps. The second is for importing into traditional forensic tools.

8.1 APFS Imaging to Process with RECON LAB

APFS – PROCESS IN RECON LAB

Non-T2 Chipset Mac as Source – Select the physical disk containing the APFS Container and volumes. On a single internal drive, this is usually "disk0". Be careful not to select the APFS synthesized container disk.

Image Type – DMG

Another benefit of processing with RECON LAB is that you do not have to decrypt before imaging.

—

T2 Chipset Mac as Source – Select the user volume within the APFS synthesized disk. On a single internal drive, this is usually "disk1s1".

Image Type – Logical (.sparseimage or DMG-RW)

—

Note: RECON IMAGER is the only solution to preserve original source timestamps when selecting logical imaging and processing in RECON LAB.

8.1.1 APFS Imaging Using ASR in RECON ITR Live

On a live machine the APFS Container Disk can be imaged using ASR Imaging. After you launch RECON IMAGER included in the Live Version of RECON ITR select disk1. The only image type available will be ASR, this will output a logical .sparseimage of the entire APFS drive. This .sparseimage can be loaded into RECON LAB as a RECON Logical image in order to preserve the original source timestamps.

8.1.2 ASR Imaging with FileVault using RECON ITR Bootable

When imaging a APFS container with FileVault enabled, be sure to **Decrypt** the the partition before adding it as a source in the Disk Manager. If not, you will be prompted with a message in Disk Imager to decrypt the volume before imaging.
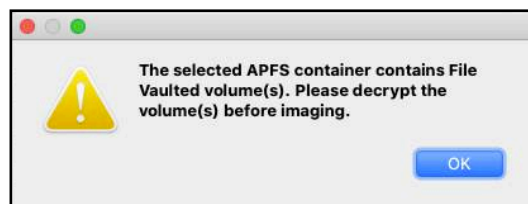
Once the partition is decrypted using the password, select the FileVault encrypted volume as a source in Disk Imager and click **Refresh**.
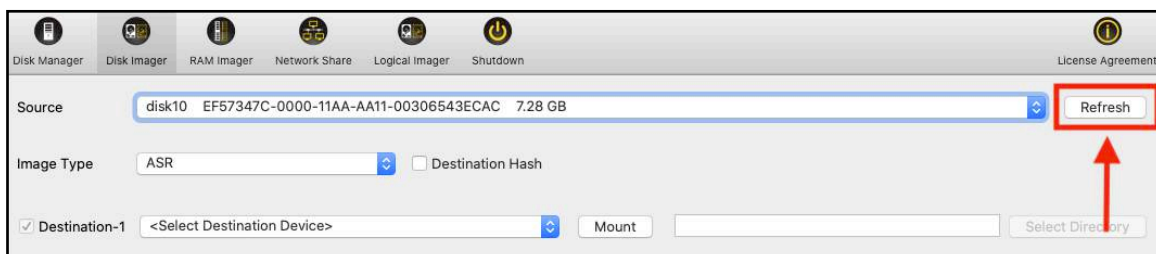
Then, you can input the necessary information and click **Start** to begin the imaging process.

8.2 APFS Imaging to Process in Other Tools

Note: If you are not using RECON LAB test and validate that your forensic tool supports APFS encrypted and/or decrypted images. All other solutions, other than RECON LAB, support APFS in various degrees as their APFS support has to be reversed engineered. RECON LAB is the only solution that supports APFS natively.

If your tools do not support physical images of non-T2 Chipset Macs then follow the best practices below.

APFS – NO FILEVAULT – PROCESS IN OTHER TOOLS

Source: Select the volume containing the user data within the APFS synthesized container disk.

Typically, there are four or five volumes (the user DATA volume, Preboot, Recovery, VM). There is an extra "system" volume for macOS 10.15 and above which has the label "DATA" appended to the volume name. Select the DATA volume and be aware the name can vary. The default volume name is usually "Macintosh HD".

Image Type – You have two options.

Option-1: Logical Image (Folder) – this is a logical copy of the files from the source to the destination.

Option-2: Logical Image (Tar) – this is a logical copy of the files from the source placed into a .tar archive. This option will take longer then Option-1. Make sure your forensic tool supports unpacking a .tar archive file properly to preserve the directory structure.

Note: RECON IMAGER used along with RECON LAB is the only solution to maintain the source timestamps during logical imaging.

APFS – WITH FILEVAULT – PROCESS IN OTHER TOOLS

Use the Disk Manager to select the APFS container volume with the user data as described above and select the "Decrypt" button. Use the password or Recovery Key option to decrypt the FileVault volume. If you are collecting information from macOS 10.15 or above also decrypt the System volume.

Once decrypted follow the steps listed above for imaging.

9. Core Storage Imaging - Single Disk

CORE STORAGE – SINGLE DISK – NO FILEVAULT

Source – Select the physical disk which is usually "disk0". This can be identified in the Disk Manager.

Image Type – DMG (remember, this is also a raw image and can be imported into other tools).

CORE STORAGE – SINGLE DISK – WITH FILEVAULT

Use the Disk Manager to select the physical disk as described above and select the "Decrypt" button. Use the password or Recovery Key option to decrypt the FileVault volume.

Once decrypted a new disk will mount. In Disk Imager select the newly mounted decrypted disk to image.

Source – Select the newly decrypted mounted disk.

Image Type – DMG (remember, this is also a raw image and can be imported into other tools).

10. Fusion Drive Imaging

FUSION DRIVE – NO FILEVAULT

Source – Select the virtualized physical disk which is usually derived from disk0s2 and disk1s2. This can be identified in the Disk Manager.

Image Type – DMG (remember, this is also a raw image and can be imported into other tools).

FUSION DRIVE – WITH FILEVAULT

Use the Disk Manager to select the virtualized physical disk with the user data as described above and select the "Decrypt" button. Use the password or Recovery Key option to decrypt the FileVault volume.

Once decrypted a new disk will mount. In Disk Imager select the newly mounted decrypted disk to image.

Source – Select the newly decrypted mounted disk.

Image Type – DMG (remember, this is also a raw image and can be imported into other tools).

FUSION DRIVE – APFS macOS 10.14

Use the Disk Manager to identify the user data partition of the synthesized APFS Fusion drive. The logical volume will be displayed underneath the APFS Synthesized Volume (usually named "Macintosh HD"). The examiner will have to decrypt the volume if FileVault is enabled. Once decrypted, a logical image can be made.

Source – Select the decrypted user DATA partition (usually named "Macintosh HD").

Image Type – Any Logical Option. The sparse image or DMG-RW format is best with Mac-based Forensic tools such as RECON Lab while the Folder or .tar format is best for usage in Windows-based Forensic tools.

FUSION DRIVE – APFS macOS 10.15 and Above

Use the Disk Manager to identify both the user DATA partition and the System partition of the synthesized APFS Fusion drive. The user DATA partition will be displayed under the APFS Synthesized Volume (usually named "Macintosh HD - DATA"). The System partition will be displayed underneath the APFS Synthesized Volume (usually named "Macintosh HD"). The examiner will have to decrypt both volumes if FileVault is enabled. Once decrypted, a logical image can be made by selecting the user DATA partition.

Source – Select the decrypted user DATA partition (usually named "Macintosh HD - DATA").

Image Type – Any Logical Option. The sparse image or DMG-RW format is best with Mac-based Forensic tools such as RECON Lab while the Folder or .tar format is best for usage in Windows-based Forensic tools.

11. Imaging A Mac With A T2 Chipset

Newer Macs have been shipping with proprietary T2 Security Chipsets which add extra layers of security. One of these new security features prevents booting from external media. This "Secure Boot" is enabled by default and can only be turned off in Recovery Mode and with an admin password.

We strongly recommend that you take your own Mac with you to incident response scenes.

In the event that the examiner has attempted to boot a T2 Chipset Mac with RECON IMAGER without disabling Secure Boot and booting from external media you may see the following message:

"A Software Update is required to use this startup disk."

There are currently two methods for imaging a Mac with a T2 Chipset disabling Secure Boot and Startup Utilities or through Target Disk Mode.

11.1 Disable Secure Boot and Booting to External Media from Recovery Mode

1. Ensure your RECON IMAGER USB is updated to the latest version.
2. Boot the source Mac into Recovery Mode by pressing and holding the Command + R keys on startup.
3. From the top menu, select "Utilities" then click on "Startup Security Utility."
4. You'll be prompted to enter an administrator password.
5. In the Startup Security Utility set "Secure Boot" to No Security and "External Boot" to Allow booting from external media.
6. Shutdown the Mac after changing the settings.
7. Insert the RECON IMAGER USB to the source Mac.
8. Power up the source Mac while holding down the ALT/Option key.
9. Use MODE-C.
10. Follow the instructions in this manual to create a logical image of a T2 Security Chipset Mac.
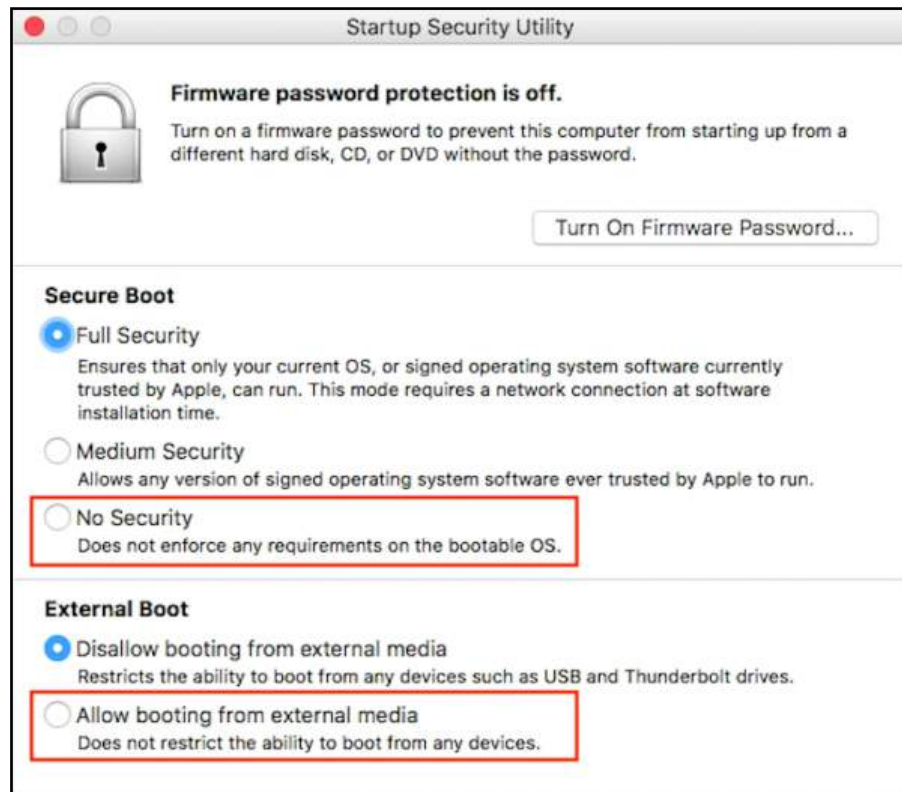
11.2 Target Disk Mode (TDM)

1. Place the Mac with the T2 chipset into Target Disk Mode (TDM) by holding down the "T" key when starting the computer. You will see symbols displayed on the screen. These symbols represent supported methods for connecting the Mac to another computer (i.e., Thunderbolt, USB 3.1).
2. Boot a second Mac with RECON IMAGER and a collection drive.
3. Start RECON IMAGER on the second Mac which is capable of supporting APFS.
4. Using a proper cable, connect the Mac in TDM to the second Mac booted with RECON IMAGER.
5. Use the "Refresh" button to view the disks and volumes of the Mac in TDM. If the Mac in TDM is using 10.14.5 or above you will need to know an admin password to complete the connection.

6. Follow the instructions in this manual to create a logical image of a Mac with a T2 Security Chipset.

12. Imaging Mac RAM

RECON IMAGER allows you to image Mac RAM without the need for an admin password (required in a live environment) within the RECON IMAGER boot environment.

To image Mac RAM on a live running system please use RECON ITR Live Mode.

Note: Imaging Mac RAM is not a 100% guarantee. Mac RAM is protected and it is not intended to be imaged. Many factors such as hardware, kernel version, and other processes running in RAM can affect a successful image.

To increase your chances of obtaining a successful RAM image, the following suggestions are recommended.

1. If a Mac is up and running do not shut it down. Connect RECON IMAGER and attempt a soft restart and immediately boot to RECON IMAGER.
2. If a Mac desktop is powered off but still plugged in do not unplug. Connect RECON IMAGER and follow the steps below to image RAM.

Mac is on and you have access to the Desktop

1. Plug in the RECON IMAGER USB and your destination drive.
2. Use the Apple Menu (upper left) to select "Restart".
3. Hold down the Alt/Option key during the restart to display boot options.
4. Select the RECON IMAGER Mode that supports the Mac that you are booting.
5. Use the RAM Imager to immediately image the RAM.

The RAM image that is created can be processed using RECON LAB or another tool of your choice.

Mac is on and you do not have access to the Desktop

Some older Macs can be restarted by force. This does not work with Macs that have a Touch Bar.

- Command + Control + Power Button – Forces restart your Mac.
- Command Control + Media Eject button – Quits all apps and restarts the Mac.

12.1 RAM Imager Interface
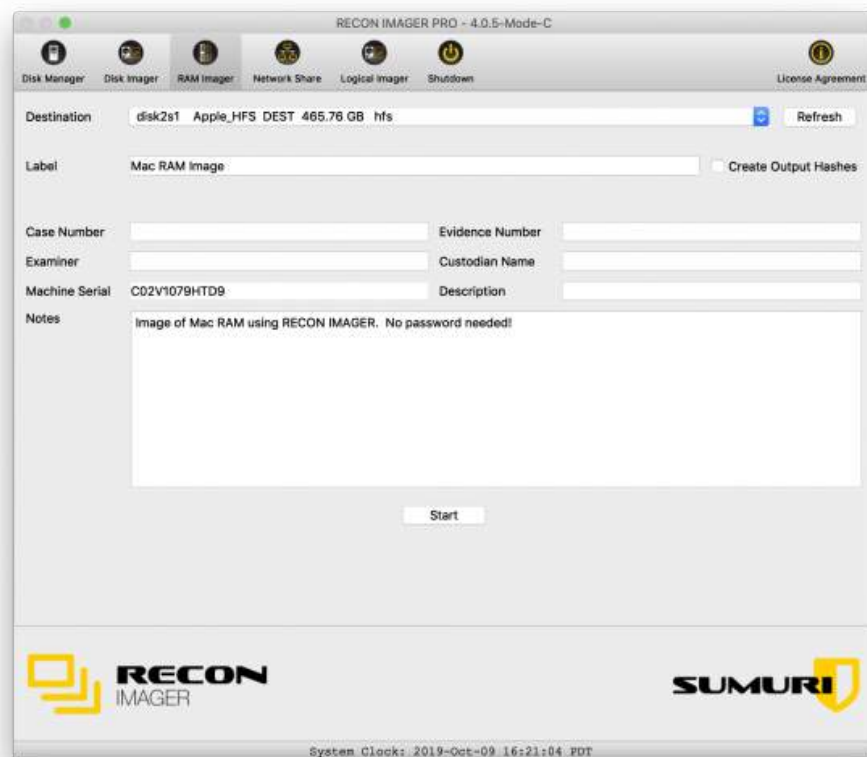
1. To image RAM after booting to RECON IMAGER select the RAM IMAGER tab.

2. Click "Refresh" to poll any attached devices.
3. Choose your "Destination" drive.
4. Provide your image with a name in the "Label" field.
5. Optional – Fill out the case information.
6. Click "Start".

Keep in mind that Mac RAM is protected by design which can sometimes lead to unsuccessful imaging.

13.RECON IMAGER PRO

RECON IMAGER PRO is an enhanced version of RECON IMAGER which provides the following extra features:

Selective Logical Imaging – Ability to select and image specific user accounts, folders and/or files. This is useful if the scope of your data collection has been limited or to save time by grabbing only the data that you need.

Automatic Artifact Extraction – RECON IMAGER PRO will automatically recover files and data related to a variety of macOS artifacts.

For example, if you want to extract Safari artifacts, RECON IMAGER PRO will automatically find files containing Safari artifacts and place them into the image to be processed later.

Network Imaging – RECON IMAGER PRO has the ability to image to a destination on a network configured via SMB.
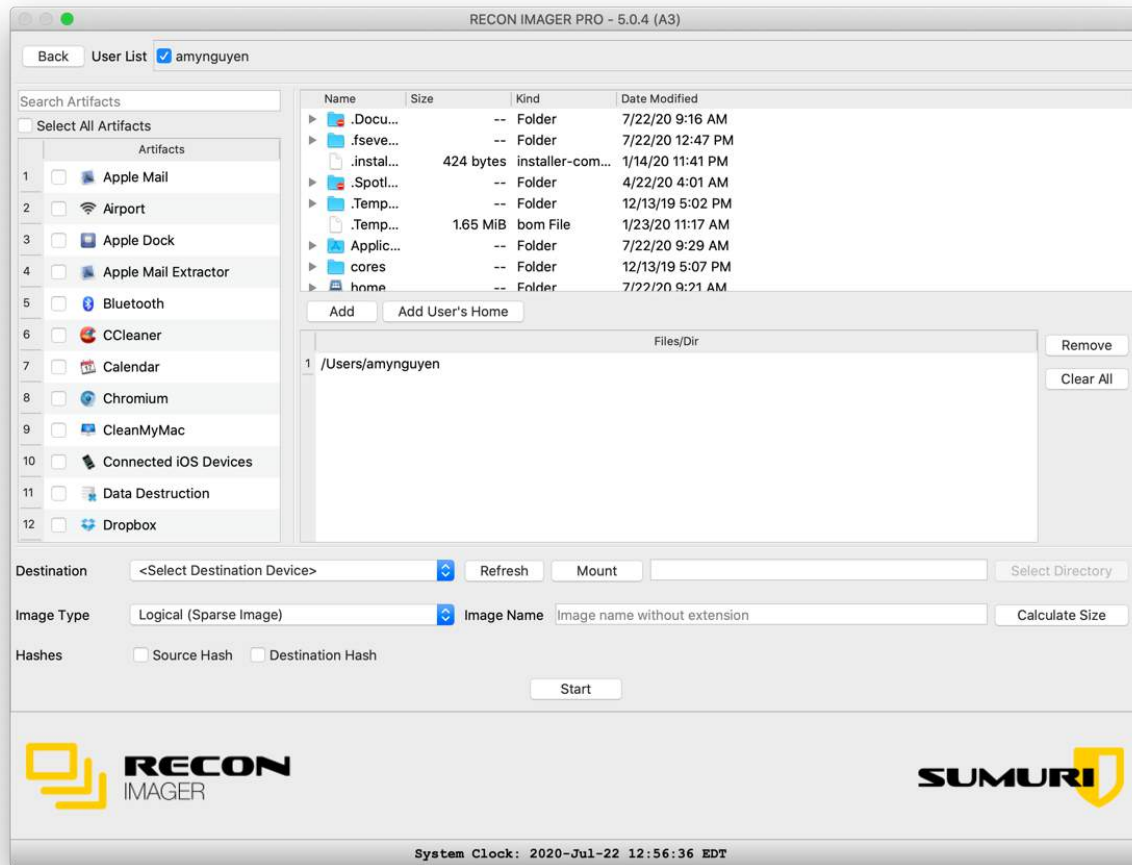
13.1.RECON IMAGER PRO - Logical Imager

To use the Logical Imager select the volume where the files of interest are stored in the "Source" dropdown. Fill in any of the optional case information and click "Select" to open the full Logical Imager interface.

—

RECON IMAGER PRO – Logical Imager Interface

- **User List** – Allows for the selection of individual users or all users on the volume selected. Selected artifacts will be captured for the users selected.
- **Artifact Selection** – Selecting any or all of these artifacts will automatically recover the files containing information related to the selected artifact during the logical imaging. Once created, the resulting image can be added to RECON LAB for automated processing or you can process manually.
- **File System Tree** – Use this interface to select any files and/or directories to be included in the logical image. Once a file or directory is selected click "Add" to include it in the logical image. Use "Remove" to remove a file or directory from the list.

- Add User's Home — Add any user's home directory selected in the User List
- Destination – Use this dropdown box to select your destination drive. If you are using the "Logical" image type you should use a destination drive formatted as macOS Extended or APFS to preserve the Apple Extended Metadata which is important for your investigation.
- Logical Image Type – This is the format you would like to use to create your logical image.
  - Sparse Image will put your selected files into a .sparseimage file. This file can be natively mounted on a Mac and can be processed by RECON LAB depending on what was selected for imaging.
  - DMG-RW will put your selected files into a .dmg file. This file can be natively mounted on a Mac and can be processed by RECON LAB depending on what was selected for imaging.
  - Folder copies selected plugins artifacts, directories, and files to the destination logically. If you want to preserve Apple Extended Attributes make sure the destination drive is formatted APFS or macOS Extended. Choosing the "Logical (Folder)" image type will allow you to import the data collected into most forensic tools.
  - TAR is a compressed logical data image that maintains native timestamps; able to be used in Mac or Windows forensic tools.
- Image Name – Name for your forensic image.
- Calculate Size – Used to provide an estimate of the size of the logical data to be imaged.
- Source Hash – This option will conduct a "pre-hash" of the files selected before the imaging.
- Destination Hash – This option will hash the image output.
- Mount – used for mounting a destination volume to select or create a directory
- Start – begins the imaging process.

Note: The number and size of the files will affect the time it takes to hash and create the image.

13.2.RECON IMAGER PRO - Network Share

RECON IMAGER PRO allows you to enable networking and configure a SAMBA share allowing you to image to a network destination such as a NAS or Evidence Server.

Select the Network Share Tab in RECON IMAGER PRO to begin.
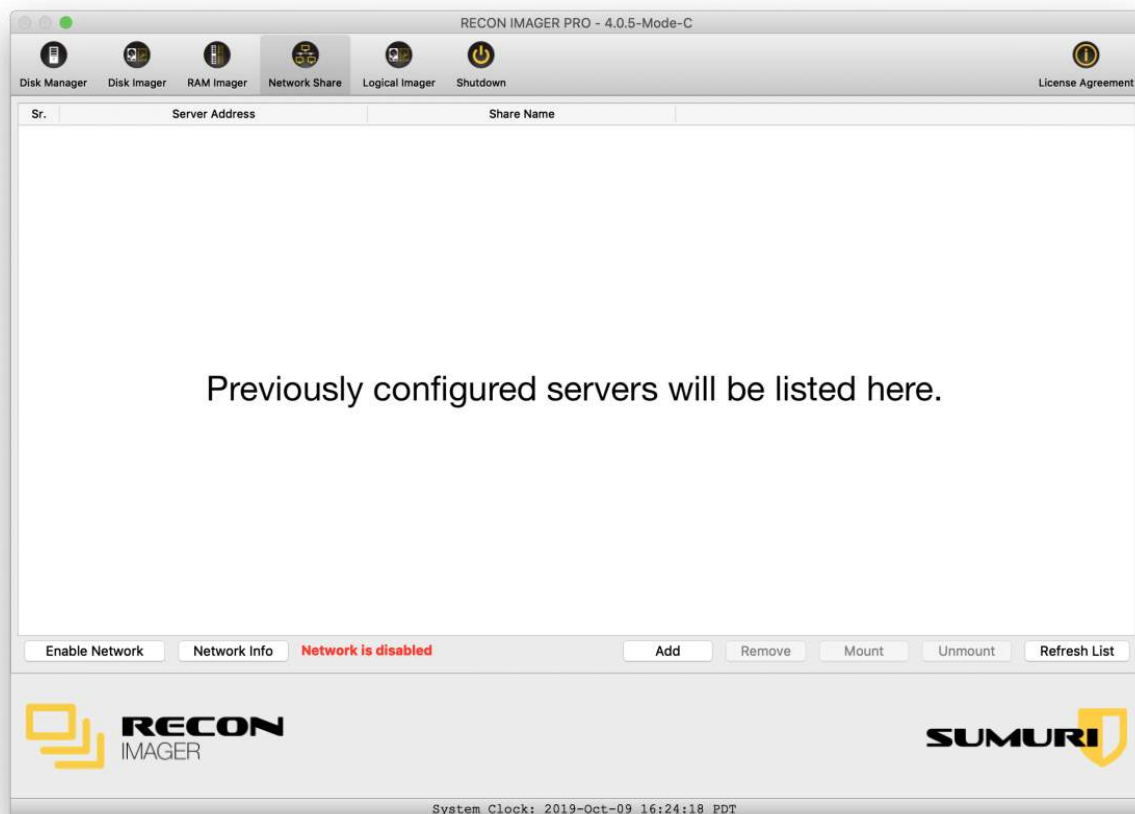
RECON IMAGER PRO has the ability to save and store previously configured networked settings. These will be shown in the main window above.

To configure a network destination start by selecting the "Enable Network" button to turn on networking.

Next, click the Add button to activate the Network Share Configuration window.
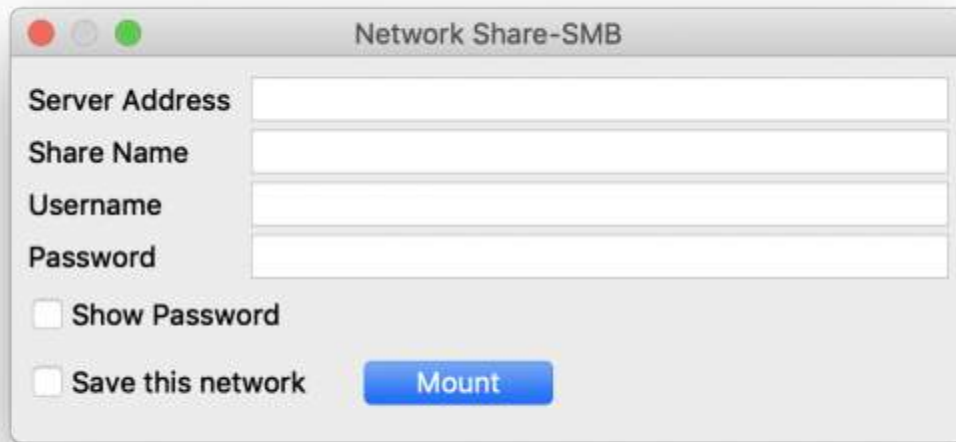
RECON IMAGER PRO supports SAMBA. Enter your SAMBA network settings and credentials. If you would like to save the network configuration check "Save this network".

After the network settings have been entered click "Mount".

Once added, your network destination will be added and visible as a Destination option for imaging.

13.2.1.RECON IMAGER PRO - Network Info

Selecting the "Network Info" button within the Network Share tab brings up a Network Information window with three additional features.

Network Interface

The "Network Interface" tab provides information about active networks.
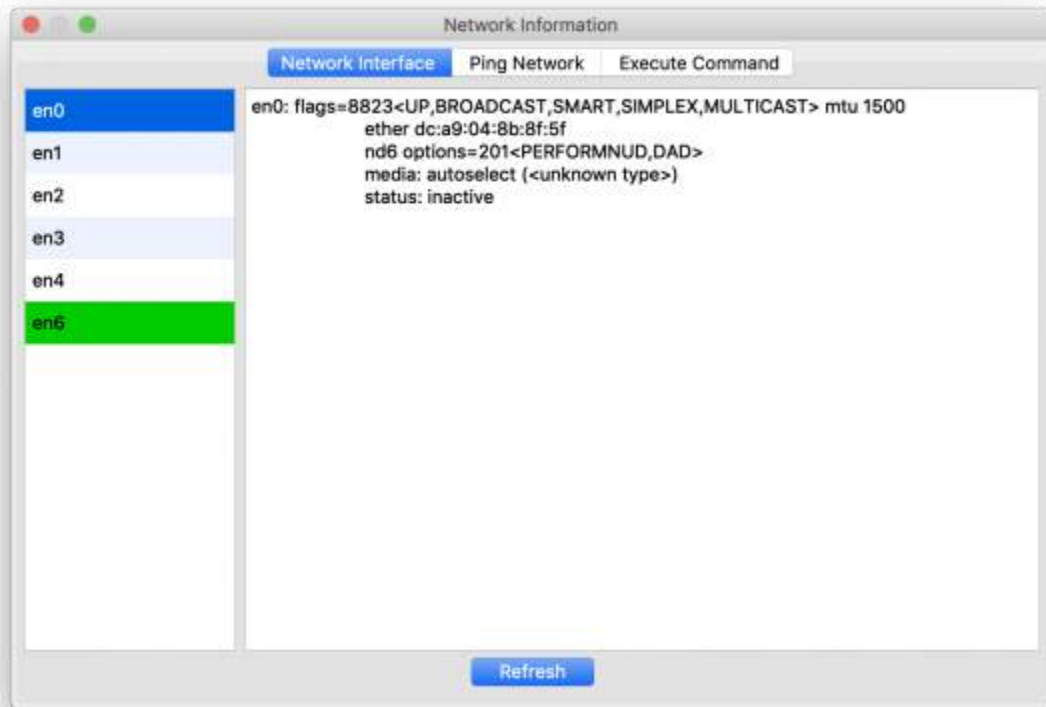
Ping Network

The "Ping Network" tab allows you to test if a network is active by entering a network address and selecting the "Ping" button.
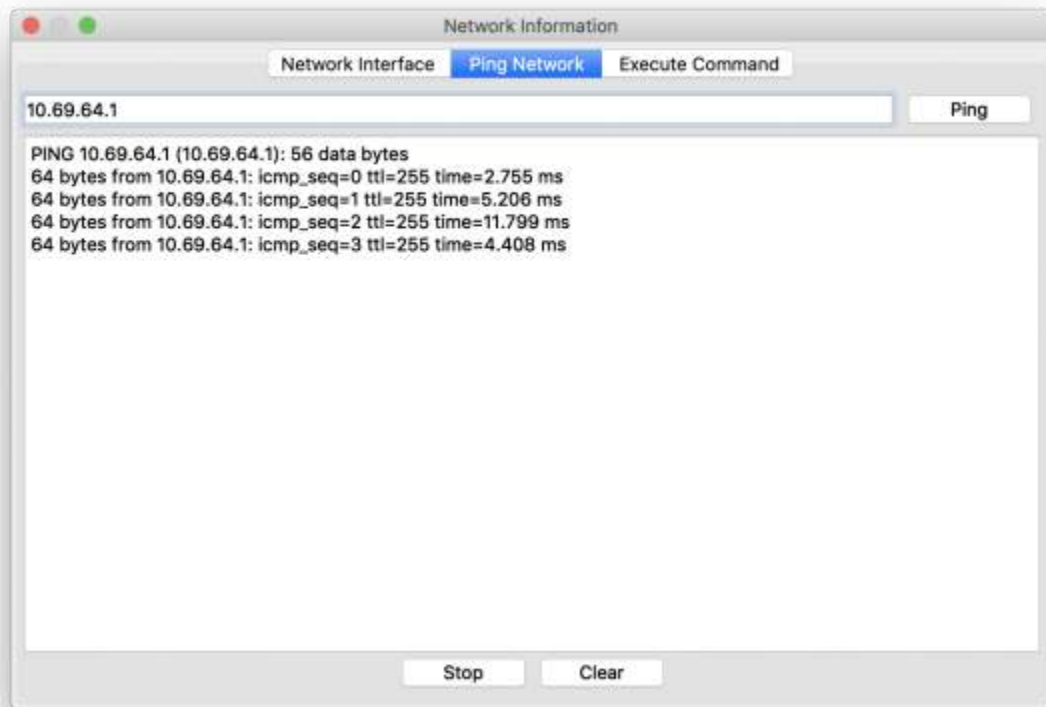
Execute Command

The "Execute Command" button allows you to enter single Terminal command and shows the results of those commands.
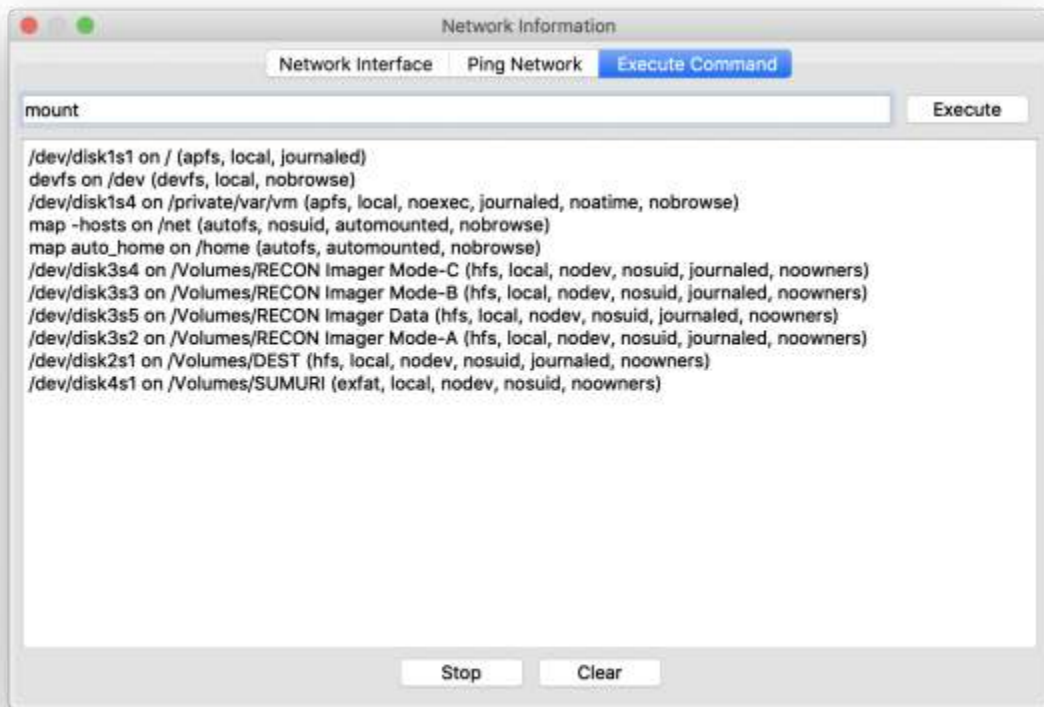
14.Shutdown

To shutdown RECON IMAGER just select the "Shutdown" button from the menu. You will be presented with a confirmation before the shutdown begins.

15.Updating RECON IMAGER

Finding Your Expiration Date

RECON IMAGER comes with one full year of updates. After your license has expired you will be required to purchase an additional year in order to continue to receive updates. RECON IMAGER will not "lock" if your license expires.

You can find your expiration date by clicking on the "License Agreement" button.

Where to Find RECON IMAGER Updates

RECON IMAGER updates can be found here:

https://sumuri.awsapps.com/workdocs/index.html#/share/document/30d21cb9833c47d418e68315913ce44f72062b218745d619db5b2f30c5a503a3

To ensure that our customers are always able to access updates we have alternative links for all downloads. If you experience any trouble with the main link hosted on Google Drive try downloading from this alternative: http://gofile.me/5dMCE/K17N0ALq2

RECON IMAGER Update Instructions

Please follow the instructions below EXACTLY in order to properly update RECON IMAGER. Please make sure that you have an adequate Internet connection with sufficient speed and no interruption while updating. Make sure that your Mac does not hibernate during the update process.
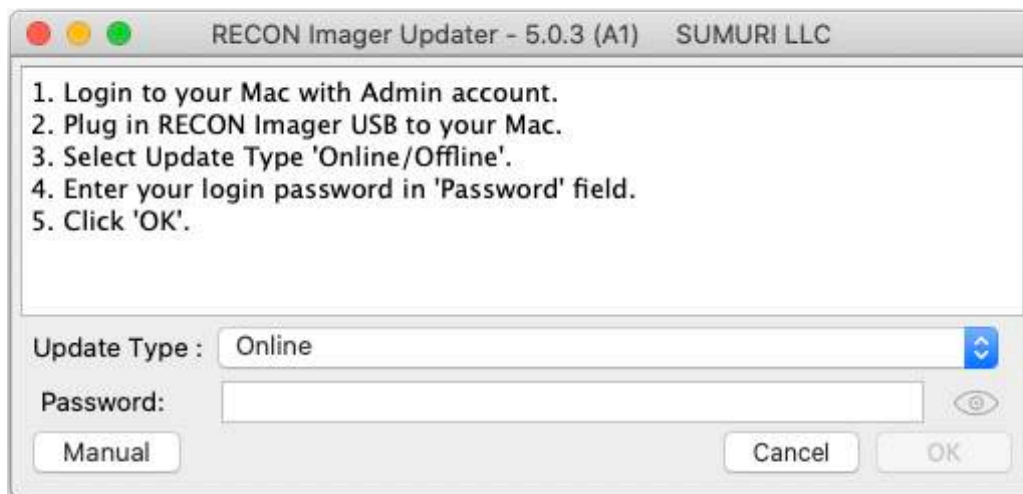
RECON IMAGER has two options for updating Offline and Online

Online

1. You must have a Mac running macOS 10.15 or higher in order to perform the update.
2. You also must be an Admin user and know your login password to perform the update. If you are a single user on a Mac you are an Admin. When RECON IMAGER prompts you for the password please enter your Mac login password to give the updater permission to run.
3. To update RECON IMAGER download the latest updater dmg file from the below link – https://goo.gl/7pcy25
4. Double-click on the Imager Updater dmg file to mount the volume and connect the desired RECON IMAGER USB to your Mac.
5. Double-click on the RECON_Imager_Updater.app and follow the instructions provided by the application.

Offline

1. You must have a Mac running macOS 10.15 or higher in order to perform the update.
2. You also must be an Admin user and know your login password to perform the update. If you are a single user on a Mac you are an Admin. When RECON IMAGER prompts you for the password please enter your Mac login password to give the updater permission to run.
3. To update RECON IMAGER download the latest Imager Updater and Offline Updater Mode dmg file from the link – https://goo.gl/7pcy25
4. Double-click on the Imager Updater dmg file to mount the volume and connect the desired RECON IMAGER USB to your Mac.
5. Double-click on the RECON_Imager_Updater.app, select Offline as the update type, and click OK.
6. The updater will then prompt you to navigate to the Offline_Updater_Mode dmg file.

7. After selecting dmg file, wait until it finishes installing.

Adding a Renewal License

After renewing your license a SUMURI representative will send you an updated license file.

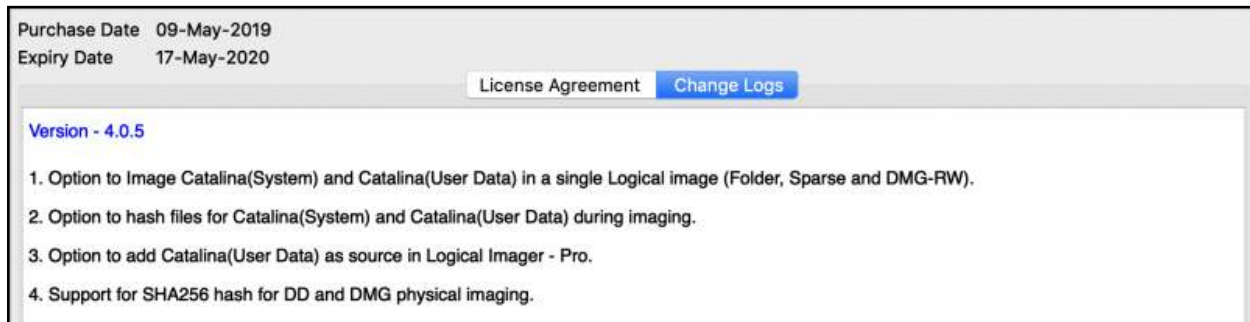1. To update your license connect your RECON IMAGER USB to a Mac.
2. Delete the old license file(s) from each of the RECON IMAGER partitions (Mode A, B, C or RECON IMAGER Newer Macs & RECON IMAGER Default). The license file(s) are located at the root of the partitions.
3. Copy the new license file to the root of the RECON IMAGER partitions.

Note: If you do not have a Samsung Duo USB please contact us for a free replacement.

16.Change Logs

Change Logs for RECON IMAGER can be found by selecting the License Agreement icon in the Main Menu then selecting the "Change Logs" tab.

Purchase Date 09-May-2019
Expiry Date 17-May-2020

License Agreement **Change Logs**

Version - 4.0.5

1. Option to Image Catalina(System) and Catalina(User Data) in a single Logical image (Folder, Sparse and DMG-RW).

2. Option to hash files for Catalina(System) and Catalina(User Data) during imaging.

3. Option to add Catalina(User Data) as source in Logical Imager - Pro.

4. Support for SHA256 hash for DD and DMG physical imaging.

17.Support - Getting Help

For support and troubleshooting please fill out a support ticket at SUMURI's Help Desk:

https://helpdesk.sumuri.com

SUMURI is located in Delaware, USA and our offices are open 0900 – 1700 EST (9AM – 5 PM). SUMURI offices are closed during US Federal Holidays.

Help Tickets are typically handled during regularly scheduled business hours as soon as possible.

For comments or feature requests please email us at:

hello@sumuri.com

18.Terms and Conditions

RECON IMAGER

Copyright 2021 – SUMURI LLC

www.sumuri.com

IMPORTANT, PLEASE READ CAREFULLY. THIS IS A LICENSE AGREEMENT

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

End User License Agreement

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

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

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

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

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

Disclaimer of Warranty – The software is provided 'AS IS' without warranty of any kind. **SUMURI LLC** and its suppliers disclaim and make no express or implied warranties and specifically disclaim the warranties of merchantability,

fitness for a particular purpose and non-infringement of third-party rights. The entire risk as to the quality and performance of the software is with you. Neither **SUMURI LLC** nor its suppliers warrant that the functions contained in the software will meet your requirements or that the operation of the software will be uninterrupted or error-free. **SUMURI LLC** is not obligated to provide any updates to the software for any user who does not have a software maintenance subscription.

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

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

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

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

OEM Product Support – Product support for the **RECON IMAGER** is provided by **SUMURI LLC**. For product support, please call **SUMURI LLC**.

Should you have any questions concerning this, please refer to the address provided in the documentation.

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

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

Jurisdiction – 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.