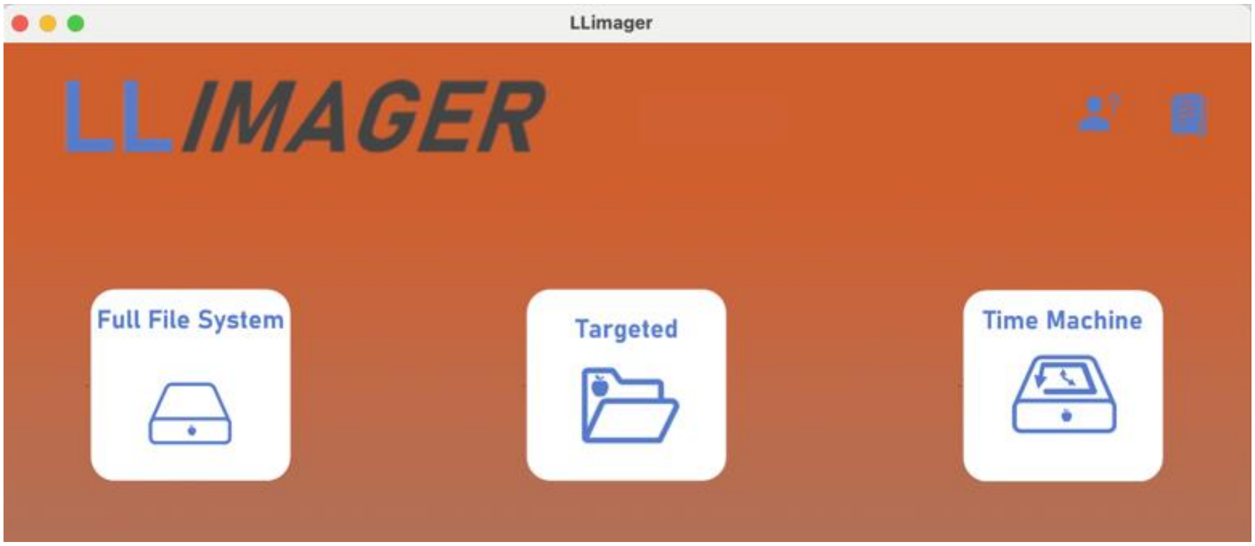


Version 5.1

User Manual

Contents

Release Notes

Welcome to LL*IMAGER* 5.1 released on March 2025, with the following updates:

- Added imaging option via Time Machine backup

- Performance enhancements

- Acquisition log updates

Preface

LL*IMAGER* is a cutting-edge solution for mac forensic imaging. As a complete rewrite in version 4.x. , LL*IMAGER* has been meticulously crafted to meet the demanding needs of digital investigators, e-discovery services providers, law enforcement professionals, and cybersecurity experts. Powered by Apple's Swift language, it combines robust functionality with an intuitive user interface, making it the go-to tool for acquiring and preserving digital evidence. Whether you're conducting criminal investigations, e-discovery, or incident response, LL*IMAGER* empowers you to extract critical data from Mac systems with precision and efficiency.

LL*IMAGER* was created in response to emerging trends in macOS forensic imaging such as limited "dead box" options, and Apple's macOS security enhancements that tend to restrict access.

It was designed to meet the need for robust and comprehensive forensic imaging of Mac computers, capable of capturing targeted folders (logical images) and active space from all APFS synthesized volumes and HFS+ volumes.

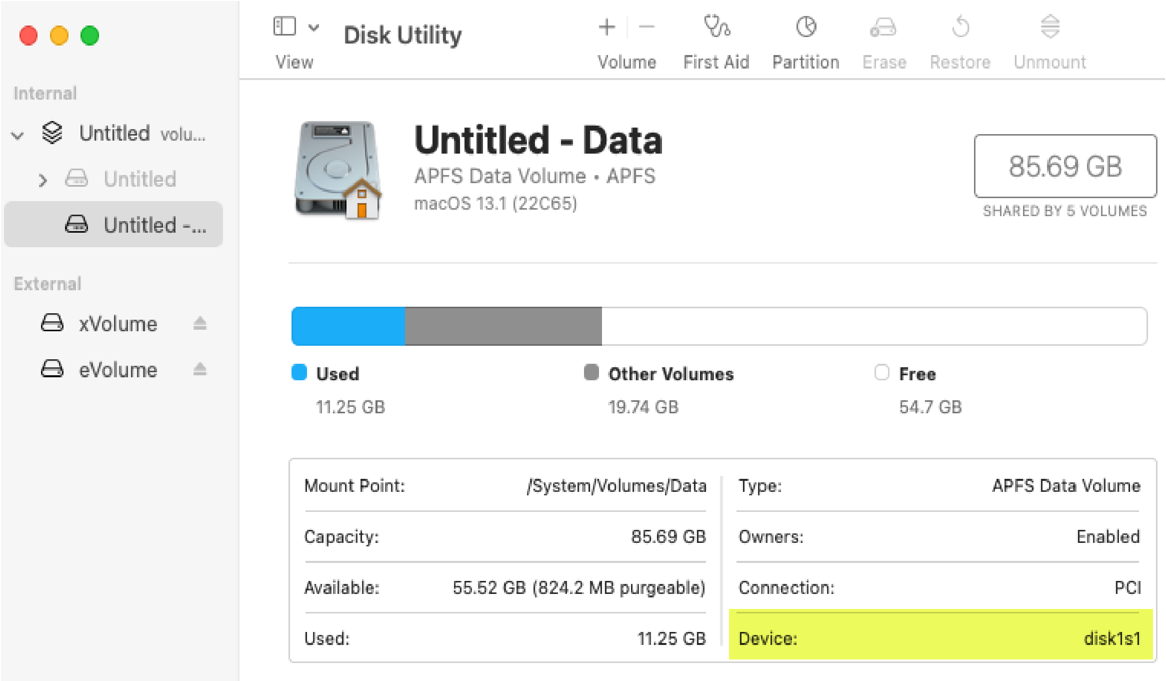
LL*IMAGER* is user-friendly and easy enough for entry level digital forensics examiners. The application leverages built-in Mac utilities, providing a versatile solution compatible with a wide range of macOS versions, both past and present. This ensures the tool remains functional across diverse system configurations.

Terminology

Sparse image file: a native macOS image format that is dynamic and used within the Mac environment. The file grows as data is added to the image, taking up only as much disk space as stored in it.

DMG file: a native macOS disk image format like the sparse image but less versatile. It is used primarily to distribute software to Mac users. It is more compatible with other commercial software and can be imported into any modern forensic applications.

Device Identifier (ID): the term used herein refers to the unique identifier used by the operating system to identify a mounted storage device with a disk number (disk1, disk1s1, etc.). This can be located using the Disk Utility as seen highlighted in the following picture.



Untitled - Data

APFS Data Volume • APFS

macOS 13.1 (22C65)

85.69 GB

SHARED BY 5 VOLUMES

Used	Other Volumes	Free
11.25 GB	19.74 GB	54.7 GB

Mount Point:	/System/Volumes/Data	Type:	APFS Data Volume
Capacity:	85.69 GB	Owners:	Enabled
Available:	55.52 GB (824.2 MB purgeable)	Connection:	PCI
Used:	11.25 GB	Device:	disk1s1

USB Label / Name: This is the name of a mounted partition, physical or virtual. It can be found using Finder, on the left side of the window. Note that a disk can have more than one partition, hence, each partition will be mounted with its own name.

LL*IMAGER* USB Drive: This is a USB drive with the two DMG files containing the executable file of the same name, and the license key file. The executable is “llimager.app”.

Supported Mac Hardware

Live Image (booted from internal disk)

LL*IMAGER* works with Intel-based Macs and new Silicon processors including M4s.

Before You Start

The Mac native Apple Software Restore (ASR) utility is used for the imaging process, thus basically any Mac can be imaged from an admin authenticated session on the Mac computer, and there should be no issues with Apple data encryption, be it FileVault of T2 chipset, or Apple new hardware M1/M2/M3/M4.

The imaging process will first create a sparse image container and use it as the destination of the disk’s image. Once the imaging of the disk has completed, the sparse image will be used to create a compressed read-only DMG file that can be processed with popular forensic and e-discovery pre-processing applications[1].

The application does not provide an option to encrypt the DMG, as encrypted DMGs are not currently supported by many forensics' applications.

In the event a DMG image must be securely encrypted, the following options are recommended:

1. Usage of a hardware-encrypted external USB disk to save the unencrypted image.
2. Encrypt the DMG and place it on a normal unencrypted disk.
3. Copy the unencrypted image to a compatible encrypted container on a normal USB disk.

The image format is limited to those used by Apple, in our case, DMG. Other applications can be used to convert the DMG to other formats (e01, …).

Requirements

- **A local admin password** for the Mac computer to be imaged.
- **LL*IMAGER* must have "Full Disk Access" permission** (set this in: Settings > Privacy & Security > Full Disk Access)
- **LL*IMAGER* USB disk**: Containing a copy of the imager executable "llimager.app" and the required license file (llimager.lic).
- **Temporary Image USB disk (if used)**: Since LL*IMAGER* creates a temporary sparse Image, the optimal method of acquisition is to have a holding disk for it. The disk can either be the LL*IMAGER* USB or another dedicated USB drive. In both cases, enough free space is required, which should be equivalent *to the total used space plus 10% or larger*.
- **Destination USB disk**: external disks formatted with exFAT are recommended to be used as the destination of the disk image (for compatibility between Operating Systems). Of course, any Mac writeable partition format will work.
  - *The USB disk should have free space equal to or greater than twice the size of the source device's used space plus 10%.* If a separate Temporary Image USB disk is used, each should have free space equal to at least the size of the used space plus 10% of the source device. Use these guides as a rule:

Source Size	**Source Space Used**	**Minimum Disk Size (when using One Destination Disk for Temp & DMG)**	**Minimum Disk Size (when using two Destination Disks for Temp & DMG)**
500GB	50GB	110GB	55GB, 55GB
500GB	400GB	880GB	440GB, 440GB
2TB	120GB	264GB	132GB, 132GB

[1] Forensic applications change over time, and support for image types may vary. Test the image produced by LL*IMAGER* during the trial period to ensure compatibility with your application(s).

  - **The best practice with respect to optimal performance is to use two USB disks, one for the sparse image, and one for the final converted DMG. This will significantly reduce the time to convert the sparse image to the DMG file**.
  - When using two USB disks, each must have a unique name.

Live System Boot

Boot the computer normally and login using an account with admin privileges. This is the most straight-forward option. An admin password is needed however to run the application.

Getting Started with LL*IMAGER*

Refer to the pertinent scenario below.

USB SSD/HDD Version

- Login as an admin into the target Mac computer and connect the LL*IMAGER* USB SSD drive that contains the copy of the imager (llimager.app, manual and license key file).

- Connect the destination disk(s) – refer to Requirements section for details on options and best practices.

- Open Finder to identify the destination USB volume names for the sparse image, and for the DMG by opening Finder.

- On the LL*IMAGER* USB SSD, navigate to /llimager and double click on "llimager.app" .

- Proceed to image.

User-Supplied USB SSD/HDD Version

- Login to any Windows computer.

- Prepare the USB SSD/HDD by:
  - Inserting an SSD into a Windows computer and create an exFAT partition named "llimager" (case sensitive). This can be a relatively small partition, e.g., 35GB.
  - Create a folder named "llimager", which when mounted on a mac, should result in "/Volumes/llimager/llimager" and on Windows "\llimager".
  - Download the most current version of LL*IMAGER* from "www.llimager.com/download" and unzip into "/llimager"
  - Optional: If you plan to use the "Send To Cloud" feature to copy images to AWS, Google Cloud or Azure, you will need the Cloud Library, and must download the most current version from "www.llimager.com/download" and unzip into the "/llimager" folder which should appear as "/llimager/llimagerCloudServices/" (**case sensitive**).

  - Copy the purchased license file (llimager.lic) into “\llimager”.
  - Your disk is now properly loaded, and you can open the manual or download it from “llimager.com/resources/llimager-manual”

- Login as an admin into the target Mac computer.

- Connect the user-supplied USB SSD drive that contains the copy of the imager (llimager.app, manual and license key file).

- Connect the destination disk(s) – refer to Requirements section for details on options and best practices.

- Open Finder to identify the destination USB volume names for the sparse image, and for the DMG by opening Finder.

- On your USB SSD, navigate to /llimager and double-click on “llimager.app”.

  WARNING: if you receive an error message, “llimager.app is damaged and can't be opened” or “The application “LLIMAGER” can’t be opened” you have run into a mac quarantine issue and you need to reload the software from a Windows computer; see FAQ #1 on our website.

- Proceed to image.

Trial Versions

- Login to a Windows computer.

- Download the trial from “llimager.com/trial-1” on to the internal disk and after receiving the license file (llimager.lic) from e-Forensics, you are ready to proceed.

- Prepare your USB Flash or SSD by:
  - Insert Flash/SSD into a Windows and create a small (~35GB) exFAT partition named “llimager” (case sensitive)
  - Create a folder named “llimager”, which should result in “\llimager”
  - While in Windows, download the most current version of LL*IMAGER* from “llimager.com/download” and unzip into “\llimager”
  - Copy the trial license file (llimager.lic) into “\llimager”.
  - Your trial version disk is now properly loaded, and you can open the manual or download it from “llimager.com/resources/llimager-manual”

- Login as an admin into the target Mac computer.

- Connect your USB Flash/SSD drive that contains the trial copy of the imager (llimager.app, manual and license key file).

- Connect the destination disk(s) – refer to Requirements section for details on options and best practices.

- Open Finder to identify the destination USB volume names for the sparse image, and for the DMG by opening Finder.

- On your USB Flash/SSD, navigate to /llimager and double-click on “llimager.app”.

- WARNING: if you receive an error message, “llimager.app is damaged and can't be opened” or “The application “LLIMAGER” can’t be opened” you have run into a mac quarantine issue and you need to reload the software from a Windows computer; see FAQ #1 on our website.

- Proceed to image.

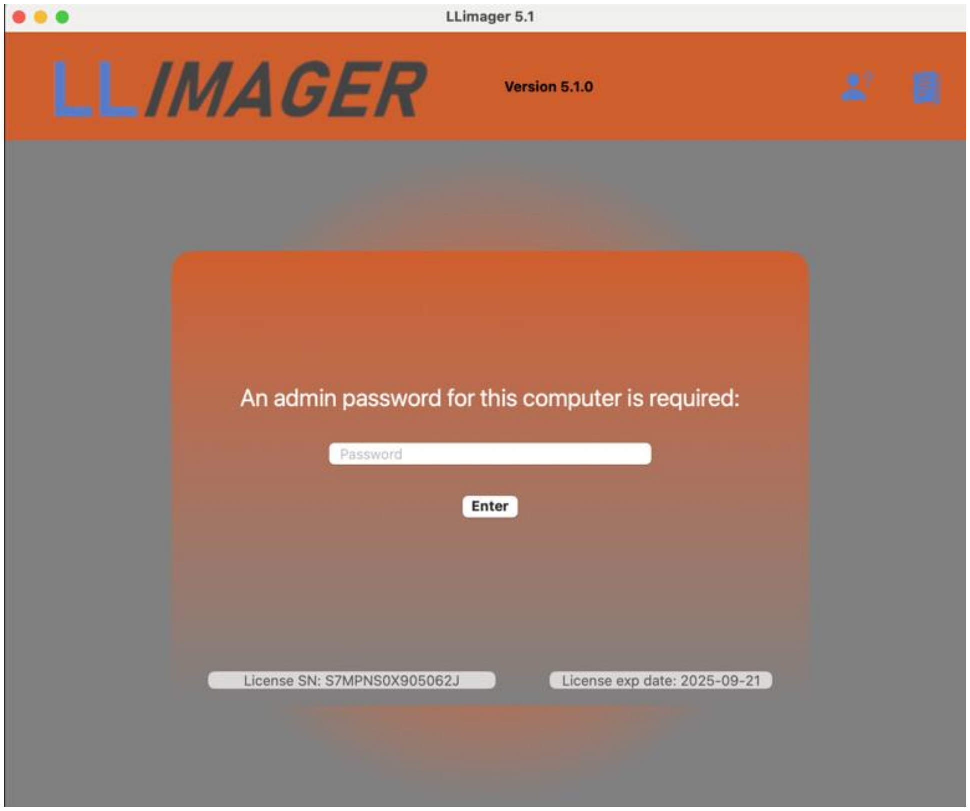
NOTE: What to do if a window pops up with the message “llimager cannot be opened because it is from an unidentified developer” or any other message related to security restrictions.

Temporarily disable Gatekeeper and try running the app again. Once the imaging is completed, exit the application, and re-enable Gatekeeper. To disable, or re-enable Gatekeeper, open a Terminal window, and use one of the following commands accordingly to disable/enable, an admin password is required:

```
sudo spctl --master-disable

sudo spctl --master-enable
```

LL*IMAGER* Menu

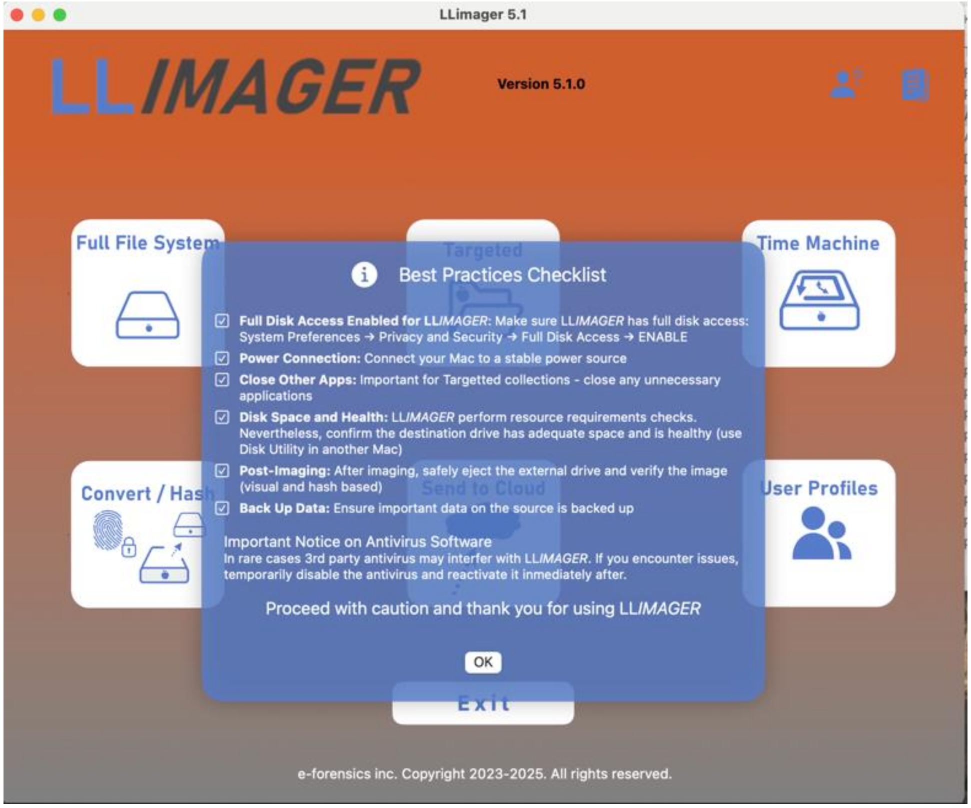
The application starts by requesting a password from a user with admin rights, followed by a best practices checklist. The password will be used throughout the usage of the app in any of the task’s selection where it is required.



An admin password for this computer is required:

License SN: S7MPNS0X905062J

License exp date: 2025-09-21



Best Practices Checklist

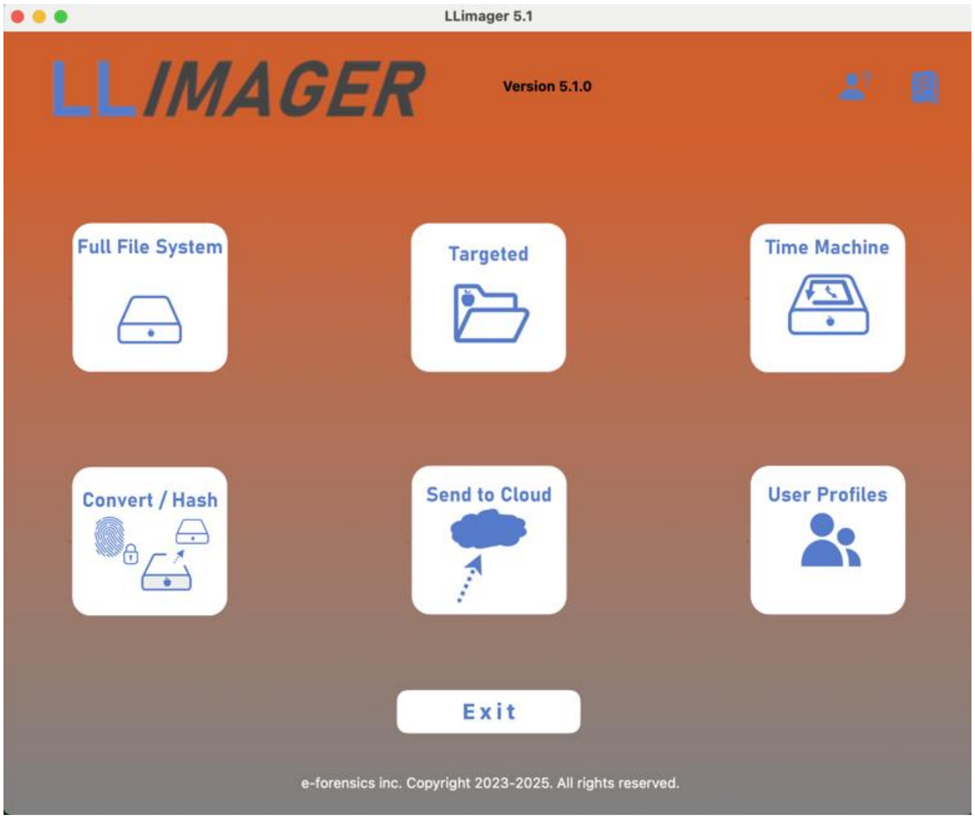
- ☑ **Full Disk Access Enabled for LL*IMAGER*:** Make sure LL*IMAGER* has full disk access: System Preferences → Privacy and Security → Full Disk Access → ENABLE
- ☑ **Power Connection:** Connect your Mac to a stable power source
- ☑ **Close Other Apps:** Important for Targetted collections - close any unnecessary applications
- ☑ **Disk Space and Health:** LL*IMAGER* perform resource requirements checks. Nevertheless, confirm the destination drive has adequate space and is healthy (use Disk Utility in another Mac)
- ☑ **Post-Imaging:** After imaging, safely eject the external drive and verify the image (visual and hash based)
- ☑ **Back Up Data:** Ensure important data on the source is backed up

Important Notice on Antivirus Software
In rare cases 3rd party antivirus may interfer with LL*IMAGER*. If you encounter issues, temporarily disable the antivirus and reactivate it inmediately after.

Proceed with caution and thank you for using LL*IMAGER*

e-forensics inc. Copyright 2023-2025. All rights reserved.

The Main Menu:



Full File System - This option is equivalent to a full file system and allows the entire process of imaging the computer's hard disk volumes' active space, saving the image to a Mac sparse image container and then conversion of the image to a compressed DMG file, and calculating the hash value of the DMG file. During the process, there will be an option to fully automate the process by creating the final DMG or to just generate the sparse file.

Targeted - This option allows the imaging of targeted files/folders on the computer's hard disk, saving the image to a compressed read-only DMG file, and calculating the hash value of the DMG file. It includes granular selection of documents and folders based on custom file types (extensions) and file system dates such as the birth time (creation), modified, accessed and the change time (inode delta). Moreover, profiles are available to save selections for future jobs.

Time Machine - A Time Machine-based disk image of the near-full data volume, including Trash folders, can be created using this feature. Unlike standard Time Machine backups, LL*IMAGER* includes all Trash folders, which are typically excluded, and packages the image into a single DMG file. Note, Time Machine omits specific system, log, and cache files, thus this option is better suited for e-discovery rather than digital forensics workflows.

Convert/ Hash - This option allows the process of converting a sparse image file to a compressed DMG file, and to calculate the hash value of the DMG file.

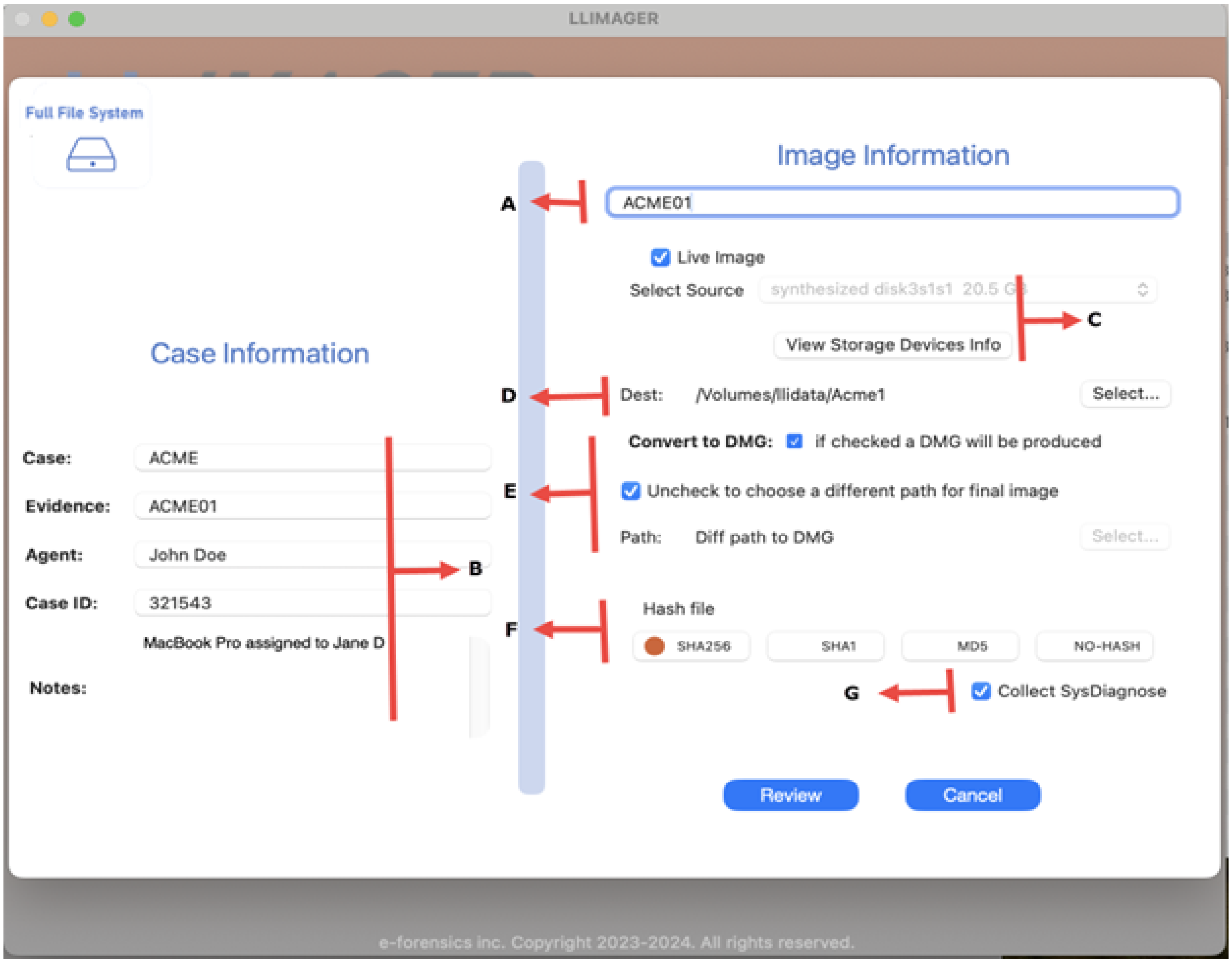
Send to Cloud – Allows uploading of images to AWS, Google Cloud or Microsoft Azure using authentication keys and giving option to securely saving credentials for future uploads. Note, you can preview the upload speed on the environment where the upload process will be occurring.

User Profiles - This option allows the imaging of targeted user profile(s), saving the image to a ZIP or DMG file, and calculating the hash value.

Exit - This option will exit the application.

Menu Option (Full File System)

Identify and input information about the device to be imaged, and the destination USBs where the image will be saved (see figure below). Additionally, provide information related to the case, name of the image and folders to use to save the file, select to convert or not to DMG, and choose to hash, and type of hash. The following picture shows the requested information.



LLIMAGER

Full File System

Case Information

Case: ACME

Evidence: ACME01

Agent: John Doe

Case ID: 321543

Notes: MacBook Pro assigned to Jane D

Image Information

ACME01

☑ Live Image

Select Source synthesized disk3s1s1 20.5 G

Dest: /Volumes/llidata/Acme1

Convert to DMG: ☑ if checked a DMG will be produced

☑ Uncheck to choose a different path for final image

Path: Diff path to DMG

Hash file ● SHA256 ○ SHA1 ○ MD5 ○ NO-HASH

☑ Collect SysDiagnose

e-forensics inc. Copyright 2023-2024. All rights reserved.

See the below description of each section.

A – Related to the image. Name assigned to the image files (sparse and DMG)

B- Related to the case. Case name, evidence number, agent, case ID and notes.

C – Related to the *device to be imaged*. Requires the selection of the device ID to be imaged. The app will verify the device and display the volume name, and the GB size of the device.

D – Related to the *destination of the sparse image and DMG file*. Requires the selection of the USB label (partition) to be used to save the files. The app will verify the device and display the device ID.

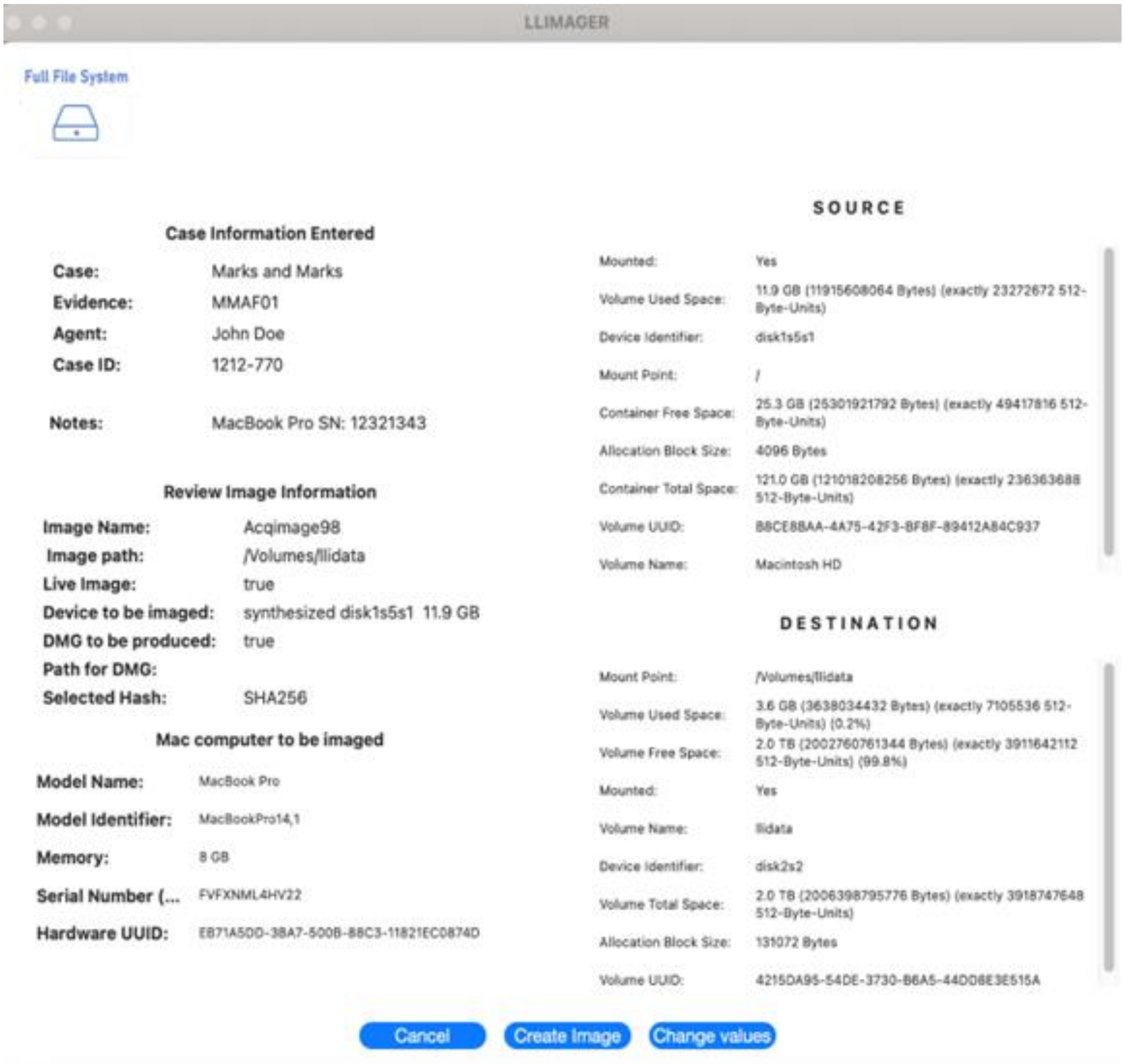
E – Select to convert or not to DMG, and to save to the same disk as the sparse or to a different disk.

F – Related to *hashing of the DMG* file. Specify if hashing should be done and type.

G – Option to collect macOS sysdiagnose.

Note, there are power saving settings on the computer that may interfere and break the imaging process, these settings are temporarily disabled during the image.

After completing the selections, click on Review and a summary of the information provided will be displayed. See the following picture:



Case Information Entered

Case:	Marks and Marks
Evidence:	MMAF01
Agent:	John Doe
Case ID:	1212-770
Notes:	MacBook Pro SN: 12321343

Review Image Information

Image Name:	Acqimage98
Image path:	/Volumes/llidata
Live Image:	true
Device to be imaged:	synthesized disk1s5s1 11.9 GB
DMG to be produced:	true
Path for DMG:	
Selected Hash:	SHA256

Mac computer to be imaged

Model Name:	MacBook Pro
Model Identifier:	MacBookPro14,1
Memory:	8 GB
Serial Number (...	FVFXNML4HV22
Hardware UUID:	EB71A5DD-38A7-500B-88C3-11821EC0874D

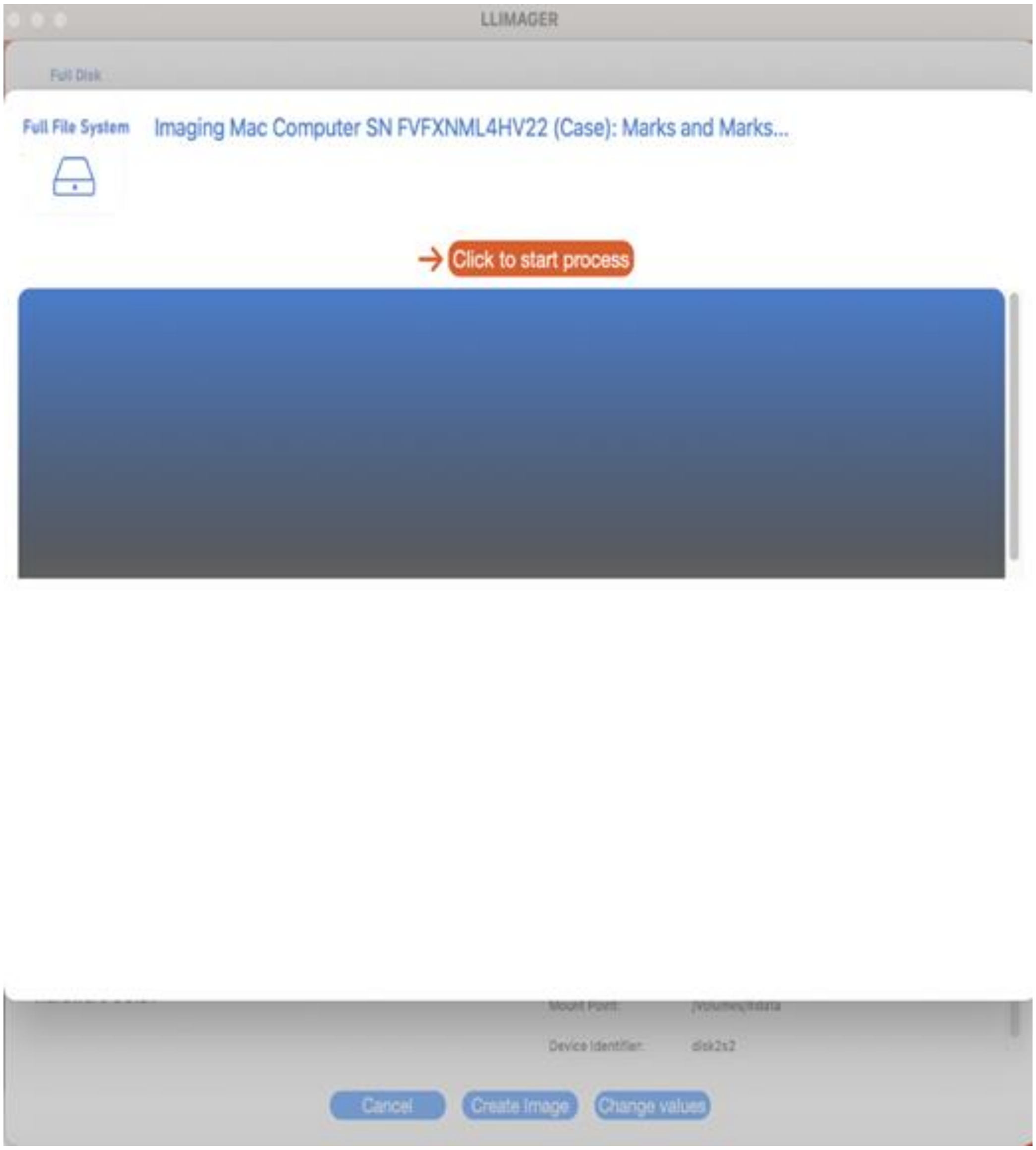
SOURCE

Mounted:	Yes
Volume Used Space:	11.9 GB (11915608064 Bytes) (exactly 23272672 512-Byte-Units)
Device Identifier:	disk1s5s1
Mount Point:	/
Container Free Space:	25.3 GB (25301921792 Bytes) (exactly 49417816 512-Byte-Units)
Allocation Block Size:	4096 Bytes
Container Total Space:	121.0 GB (121018208256 Bytes) (exactly 236363688 512-Byte-Units)
Volume UUID:	B8CE8BAA-4A75-42F3-BF8F-89412A84C937
Volume Name:	Macintosh HD

DESTINATION

Mount Point:	/Volumes/llidata
Volume Used Space:	3.6 GB (3638034432 Bytes) (exactly 7105536 512-Byte-Units) (0.2%)
Volume Free Space:	2.0 TB (2002760761344 Bytes) (exactly 3911642112 512-Byte-Units) (99.8%)
Mounted:	Yes
Volume Name:	llidata
Device Identifier:	disk2s2
Volume Total Space:	2.0 TB (2006398795776 Bytes) (exactly 3918747648 512-Byte-Units)
Allocation Block Size:	131072 Bytes
Volume UUID:	4215DA95-54DE-3730-B6A5-44DD8E3E515A

After validating and accepting the information, click on “Create Image” and the following will appear:

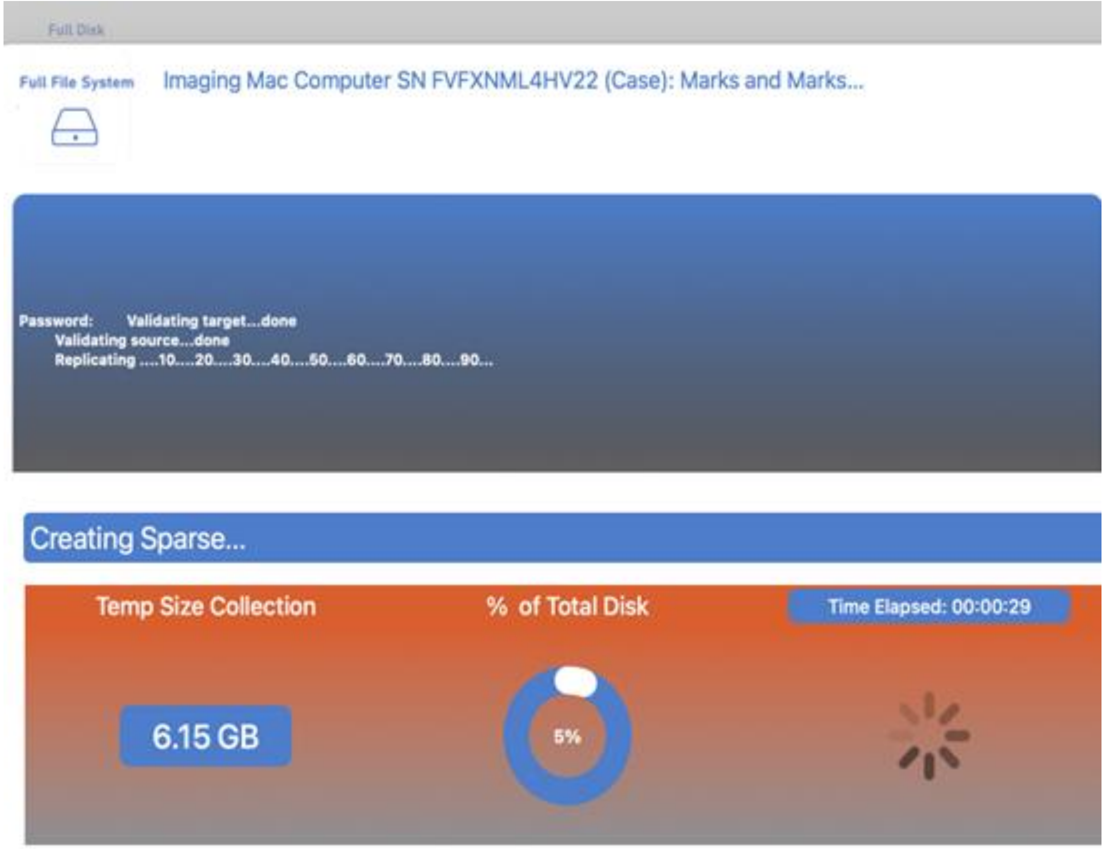


Imaging Mac Computer SN FVFXNML4HV22 (Case): Marks and Marks...

Mount Point: [illegible]

Device Identifier: disk2s2

Click on “Click to start process” and as the process commences, a progress screen indicating that the sparse image is being generated will appear -- see below:



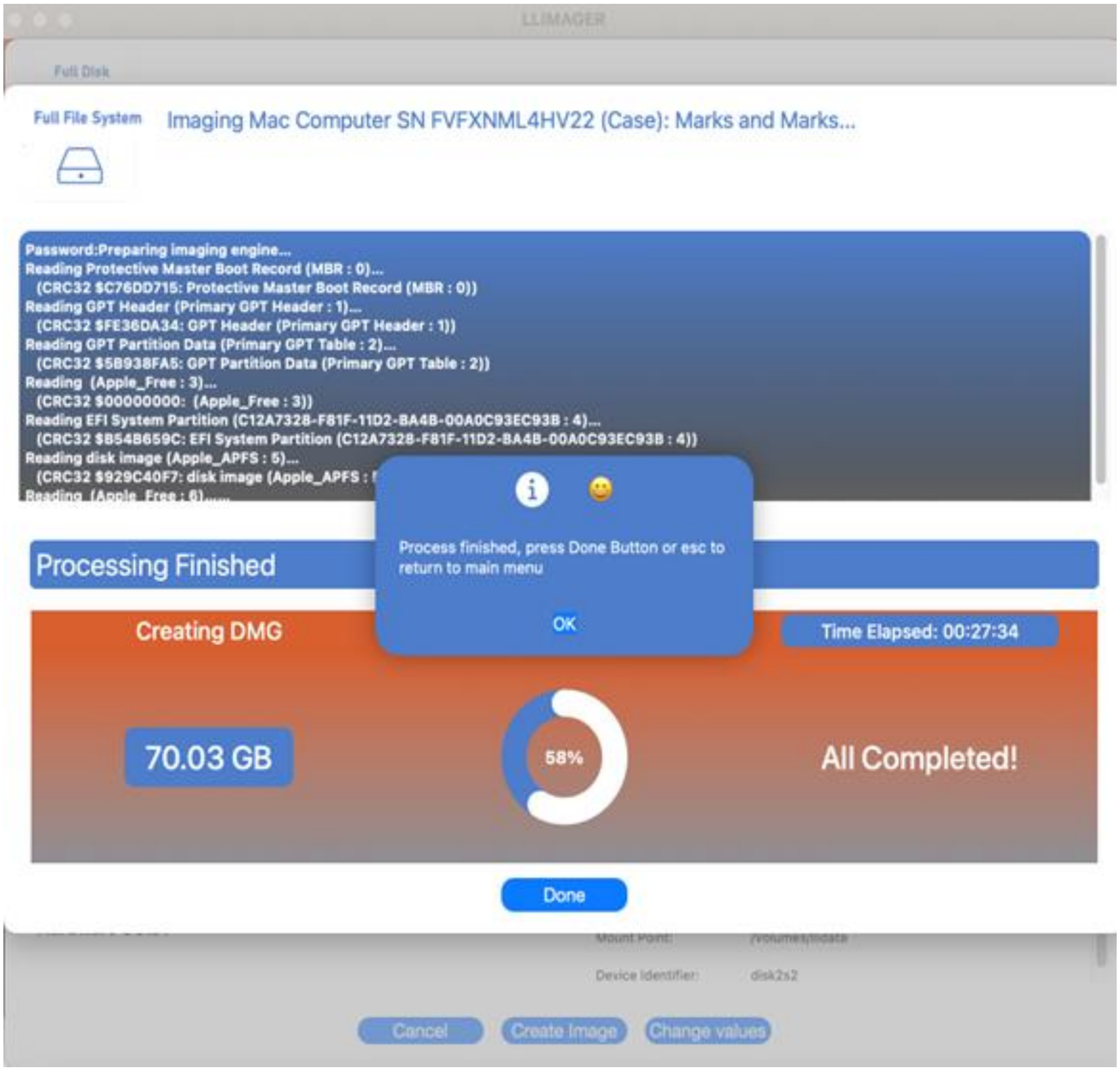
Full Disk
Full File System
Imaging Mac Computer SN FVFXNML4HV22 (Case): Marks and Marks...

```
Password:      Validating target...done
       Validating source...done
       Replicating ....10....20....30....40....50....60....70....80....90...
```

Creating Sparse...

Once the sparse image is completed, if “Convert to DMG” was selected, LL*IMAGER* will proceed to create the DMG.

After the DMG conversion is completed, LL*IMAGER* will proceed to hash the DMG if “Hash file” was selected -- see below:



Imaging Mac Computer SN FVFXNML4HV22 (Case): Marks and Marks...

```
Password:Preparing imaging engine...
Reading Protective Master Boot Record (MBR : 0)...
  (CRC32 $C76DD715: Protective Master Boot Record (MBR : 0))
Reading GPT Header (Primary GPT Header : 1)...
  (CRC32 $FE36DA34: GPT Header (Primary GPT Header : 1))
Reading GPT Partition Data (Primary GPT Table : 2)...
  (CRC32 $5B938FA5: GPT Partition Data (Primary GPT Table : 2))
Reading  (Apple_Free : 3)...
  (CRC32 $00000000:  (Apple_Free : 3))
Reading EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4)...
  (CRC32 $B54B659C: EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4))
Reading disk image (Apple_APFS : 5)...
  (CRC32 $929C40F7: disk image (Apple_APFS :
Reading  (Apple_Free : 6)......
```

Processing Finished

Process finished, press Done Button or esc to return to main menu

Creating DMG

Time Elapsed: 00:27:34

70.03 GB

58%

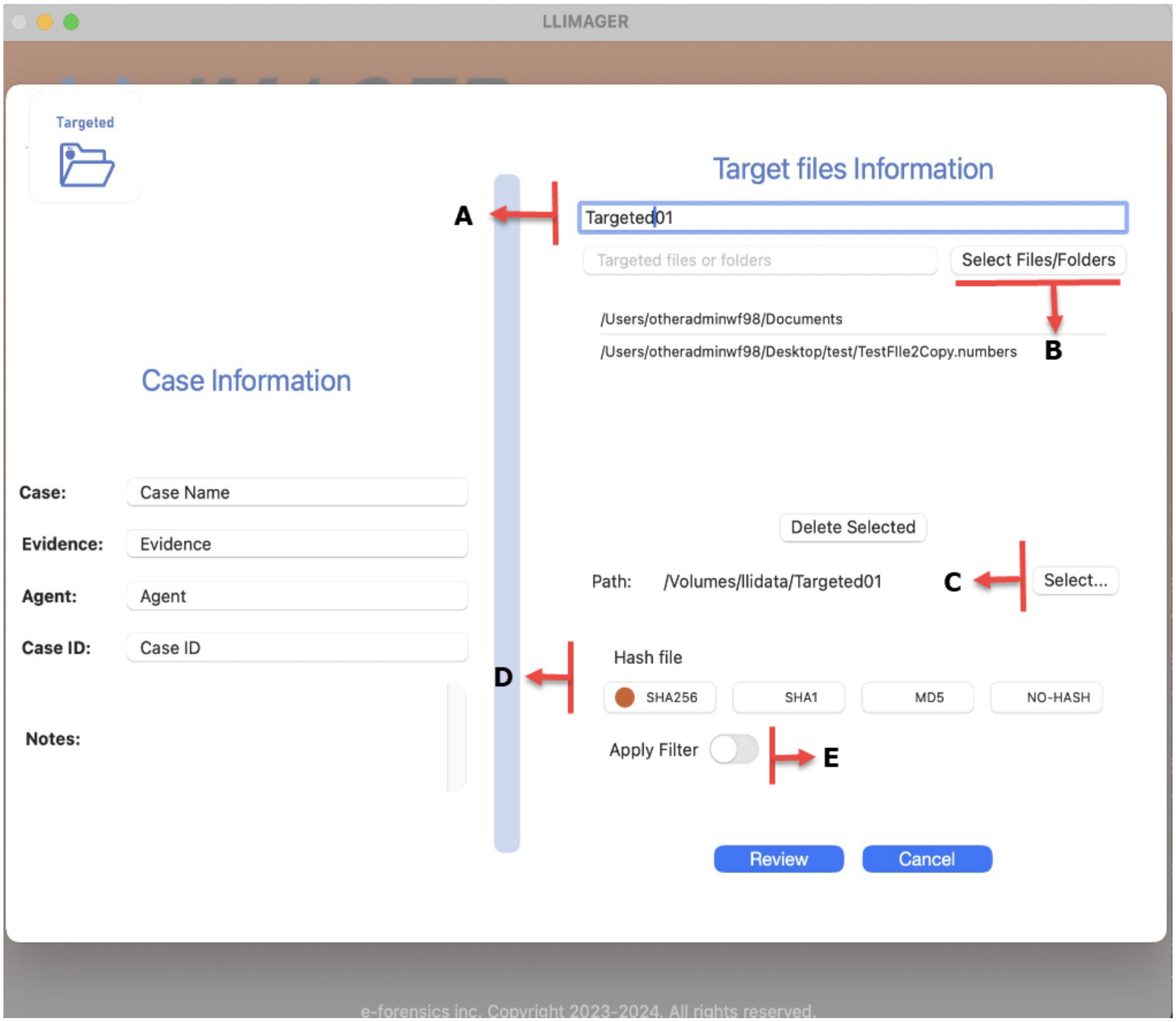
All Completed!

Mount Point: /Volumes/lldata

Device Identifier: disk2s2

Menu Option (Targeted)

Input the image destination name and location of the destination logical DMG file. Additionally, choose to hash and type of hash. The following picture shows the requested information.



Target files Information

Targeted01

Targeted files or folders

/Users/otheradminwf98/Documents

/Users/otheradminwf98/Desktop/test/TestFIle2Copy.numbers

Case Information

Case: Case Name

Evidence: Evidence

Agent: Agent

Case ID: Case ID

Notes:

Path: /Volumes/llidata/Targeted01

Hash file

● SHA256 ○ SHA1 ○ MD5 ○ NO-HASH

Apply Filter ○

e-forensics inc. Copyright 2023-2024. All rights reserved.

See below for a description of each section.

A – Specify the name of the image.

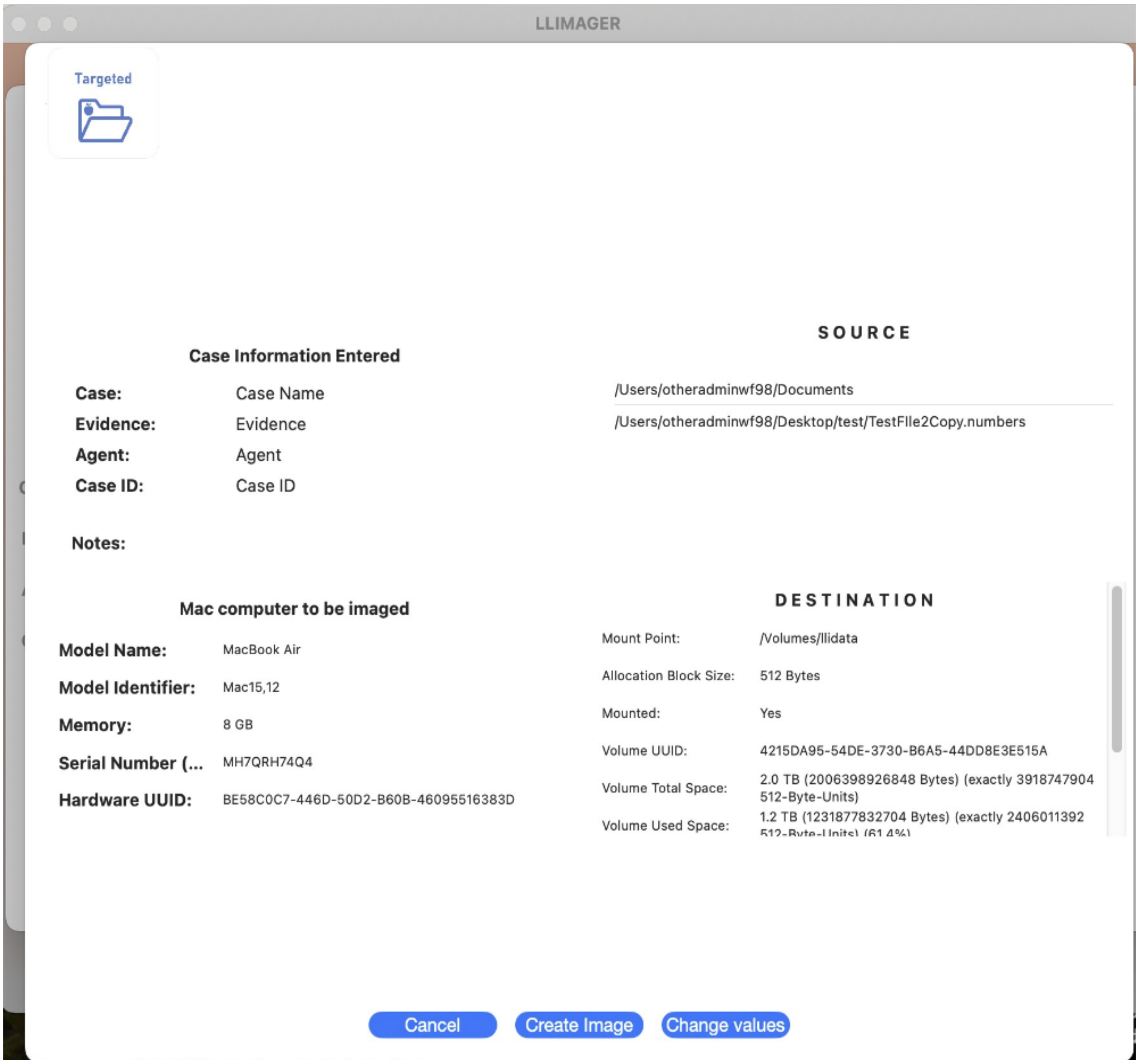
B – Related to the *source files/folders*. Requires selection of the source files/folders to acquire.

C – Related to the *destination of the DMG* file. Requires selection of path where the DMG will be saved.

D – Related to *hashing of the DMG* file. Specify if the DMG will be hashed then specify the type of hash.

E – For granular selections and saving to profile.

After completing the selections, a summary of the information provided; see below.



Case Information Entered

Case:	Case Name
Evidence:	Evidence
Agent:	Agent
Case ID:	Case ID

Notes:

SOURCE

/Users/otheradminwf98/Documents

/Users/otheradminwf98/Desktop/test/TestFIle2Copy.numbers

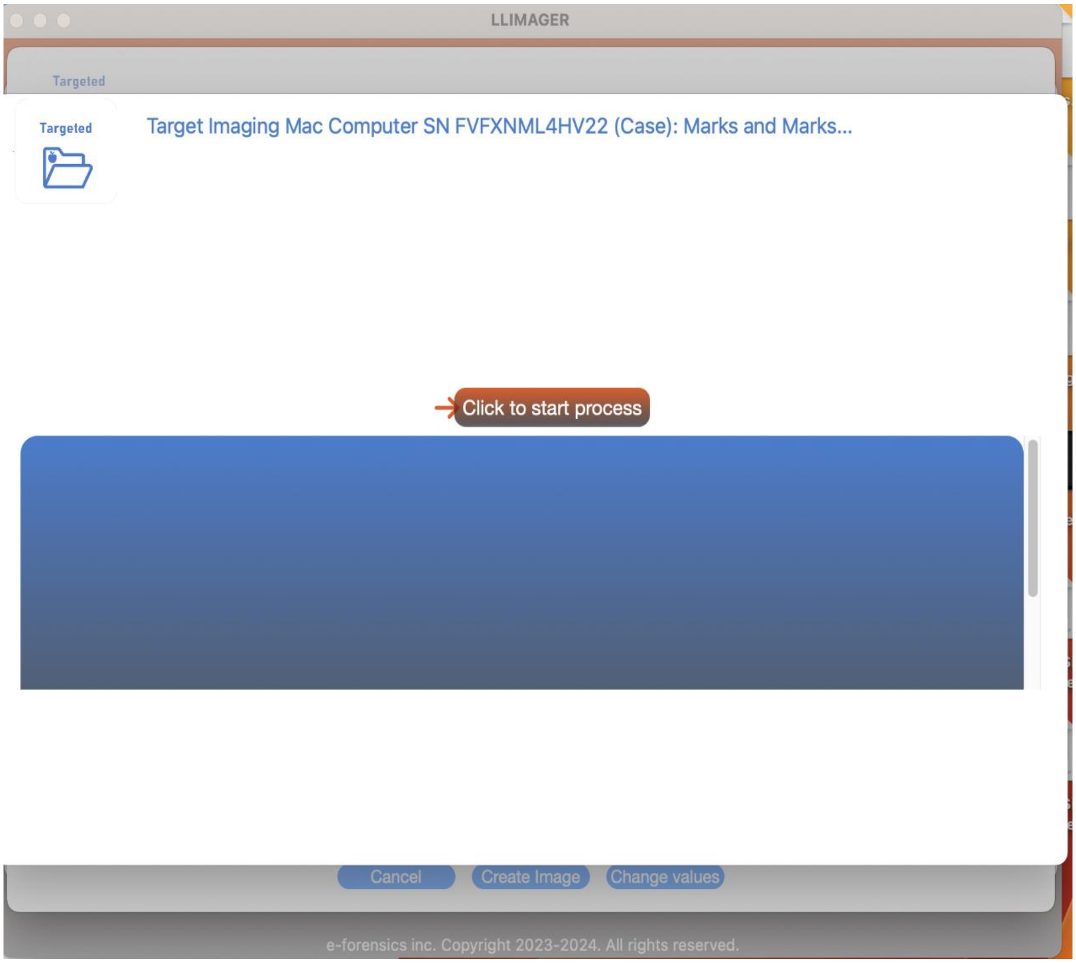
Mac computer to be imaged

Model Name:	MacBook Air
Model Identifier:	Mac15,12
Memory:	8 GB
Serial Number (...	MH7QRH74Q4
Hardware UUID:	BE58C0C7-446D-50D2-B60B-46095516383D

DESTINATION

Mount Point:	/Volumes/llidata
Allocation Block Size:	512 Bytes
Mounted:	Yes
Volume UUID:	4215DA95-54DE-3730-B6A5-44DD8E3E515A
Volume Total Space:	2.0 TB (2006398926848 Bytes) (exactly 3918747904 512-Byte-Units)
Volume Used Space:	1.2 TB (1231877832704 Bytes) (exactly 2406011392 512-Byte-Units) (61.4%)

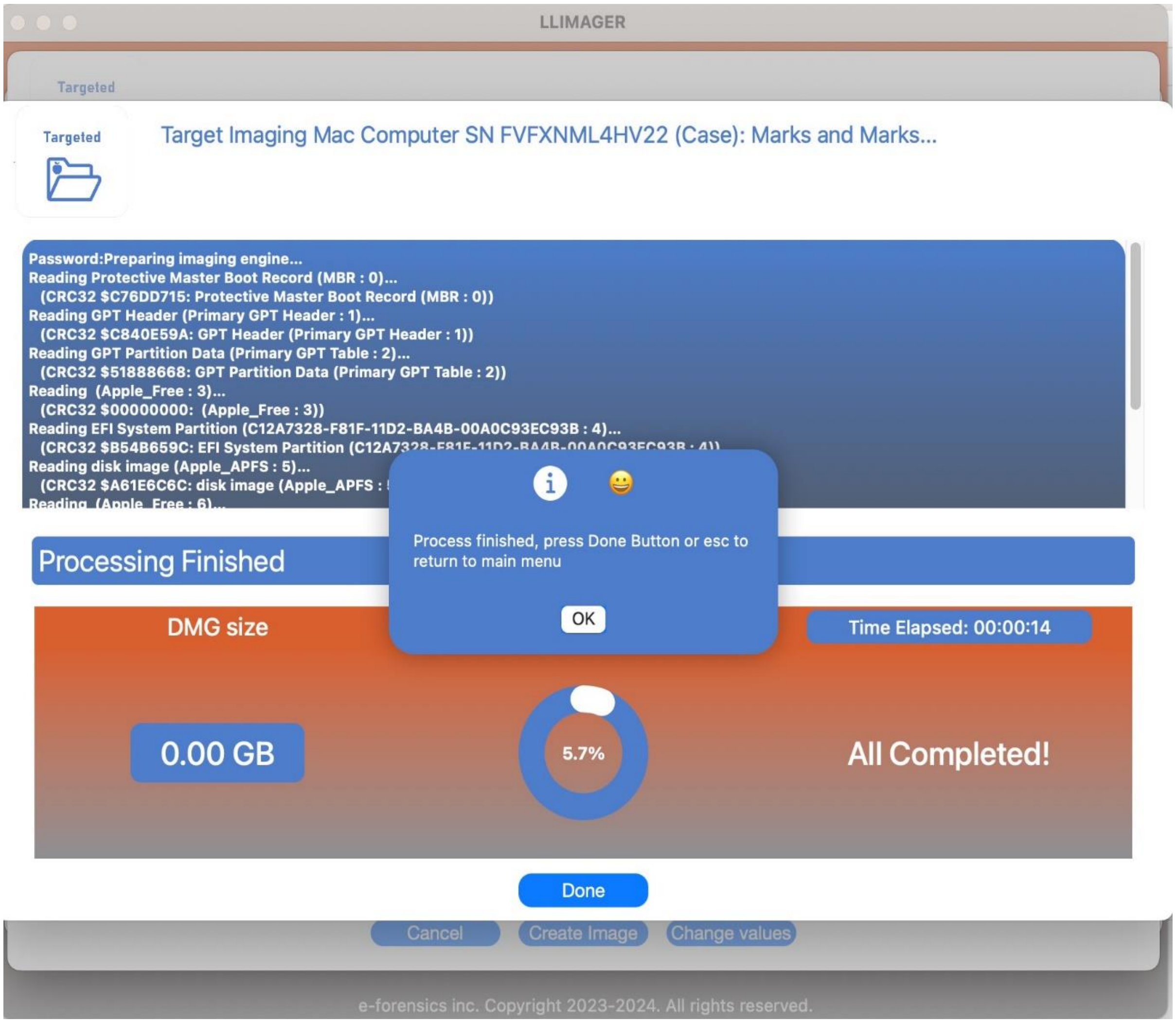
After validating and accepting the information, click on “Create Image” and the following will appear:



Target Imaging Mac Computer SN FVFXNML4HV22 (Case): Marks and Marks...

e-forensics inc. Copyright 2023-2024. All rights reserved.

Click on “Click to start process” and as the process commences, a progress screen indicating that the DMG logical image is being generated will appear -- see below:



Target Imaging Mac Computer SN FVFXNML4HV22 (Case): Marks and Marks...

```
Password:Preparing imaging engine...
Reading Protective Master Boot Record (MBR : 0)...
  (CRC32 $C76DD715: Protective Master Boot Record (MBR : 0))
Reading GPT Header (Primary GPT Header : 1)...
  (CRC32 $C840E59A: GPT Header (Primary GPT Header : 1))
Reading GPT Partition Data (Primary GPT Table : 2)...
  (CRC32 $51888668: GPT Partition Data (Primary GPT Table : 2))
Reading  (Apple_Free : 3)...
  (CRC32 $00000000:  (Apple_Free : 3))
Reading EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4)...
  (CRC32 $B54B659C: EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4))
Reading disk image (Apple_APFS : 5)...
  (CRC32 $A61E6C6C: disk image (Apple_APFS :
Reading  (Apple_Free : 6)...
```

Process finished, press Done Button or esc to return to main menu

Processing Finished

DMG size

0.00 GB

5.7%

Time Elapsed: 00:00:14

All Completed!

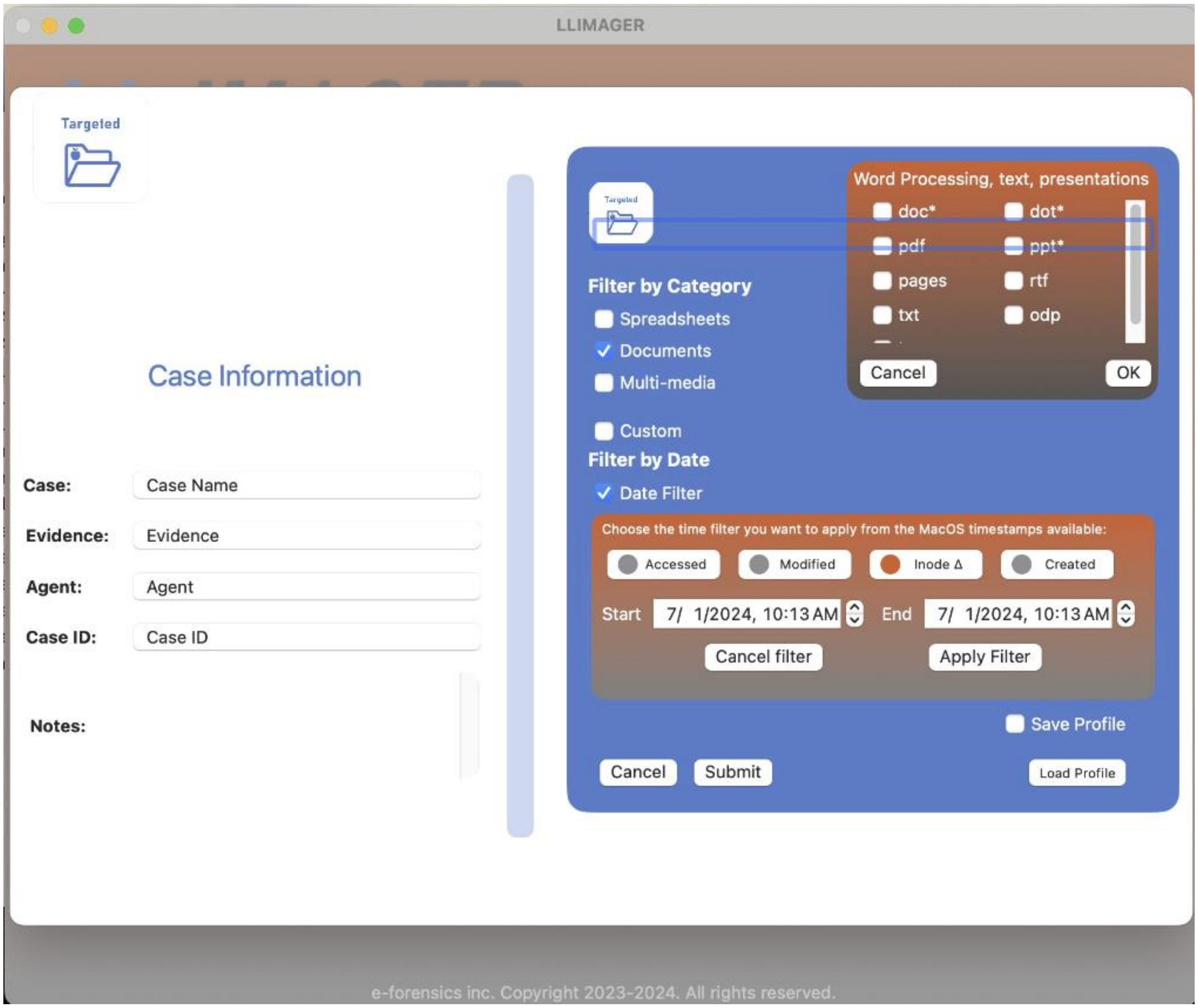
e-forensics inc. Copyright 2023-2024. All rights reserved.

Menu Option (Targeted – Using Filtering)

As of release 4.1.04, LLIMAGER includes enhanced filtering for improved digital forensics and e-discovery collection workflows. The filtering includes:

- File System dates:
    - Access Time (st_atime): This represents the last time the file's data was read or accessed.
    - Modification Time (st_mtime): This indicates the last time the file's content was modified.
    - Change Time (st_ctime): This reflects the last time the file's metadata was changed. This includes permission modifications, ownership changes, or any other alterations to the file's properties outside the content itself.
    - Birth Time (st_birthtime also referred to as st_ctime on some systems). This can be a bit confusing because depending on the file system implementation, st_ctime might sometimes refer to the birth time (creation time) on some systems.
- File Types:
    - File Categories:
        - Spreadsheets: common spreadsheet file extension names
        - Documents: common word processing, presentation, and text file extensions
        - Multi-Media: common audio, video and images file extensions
        - Custom: add custom file extensions.
- Profiles: Option to save filtered selections to a customer profile name.

Below is the screenshot representing the filtering options and saving to a profile:



Case:	Case Name
Evidence:	Evidence
Agent:	Agent
Case ID:	Case ID

Word Processing, text, presentations

□ doc*	□ dot*
□ pdf	□ ppt*
□ pages	□ rtf
□ txt	□ odp

Filter by Category

□ Spreadsheets
☑ Documents
□ Multi-media

□ Custom

Filter by Date

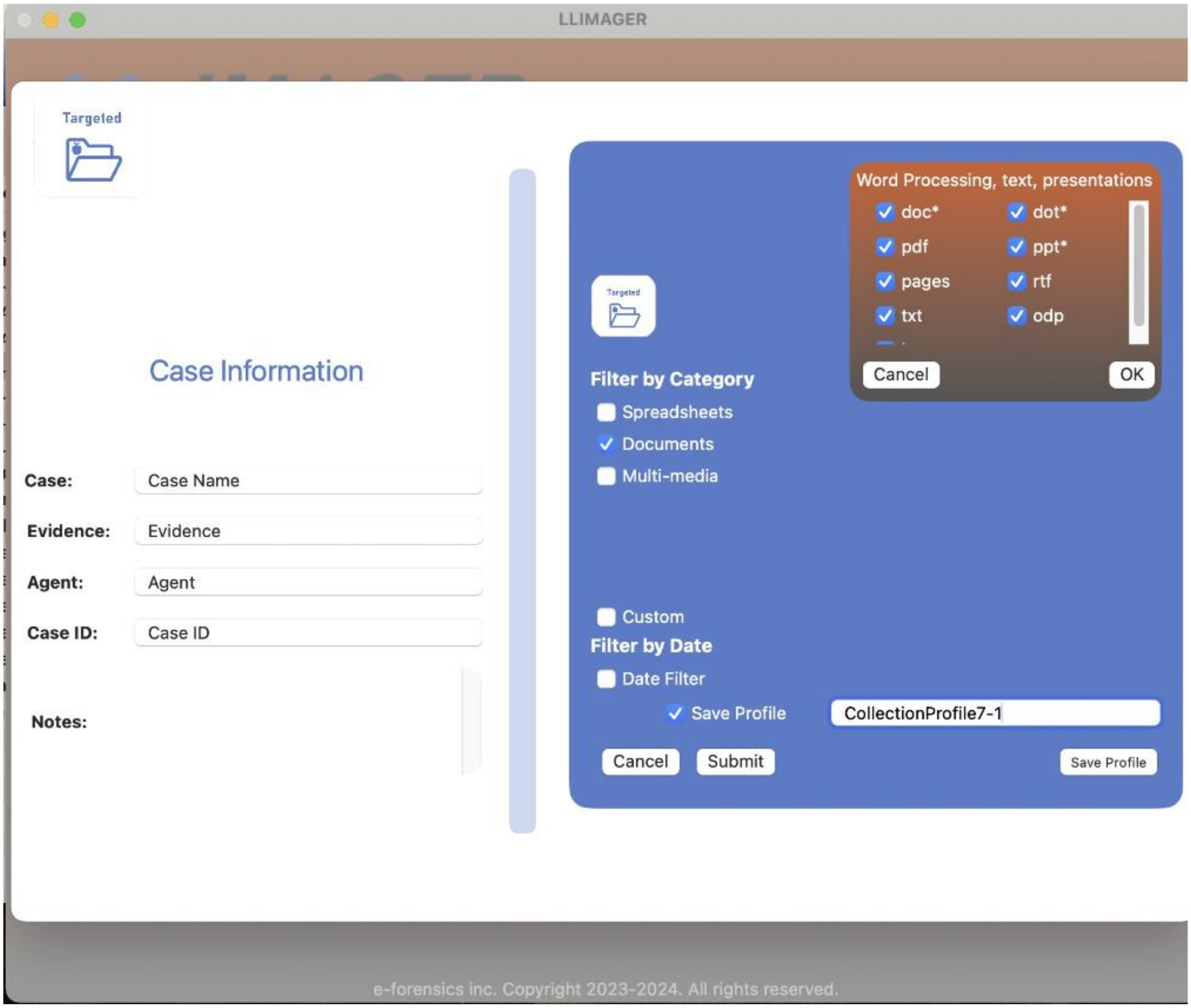
☑ Date Filter

Choose the time filter you want to apply from the MacOS timestamps available:

○ Accessed ○ Modified ● Inode Δ ○ Created

Start 7/ 1/2024, 10:13 AM End 7/ 1/2024, 10:13 AM

□ Save Profile



Case Information

Case: Case Name

Evidence: Evidence

Agent: Agent

Case ID: Case ID

Notes:

Word Processing, text, presentations

☑ doc* ☑ dot*
☑ pdf ☑ ppt*
☑ pages ☑ rtf
☑ txt ☑ odp

Filter by Category

□ Spreadsheets
☑ Documents
□ Multi-media

□ Custom

Filter by Date

□ Date Filter

☑ Save Profile CollectionProfile7-1

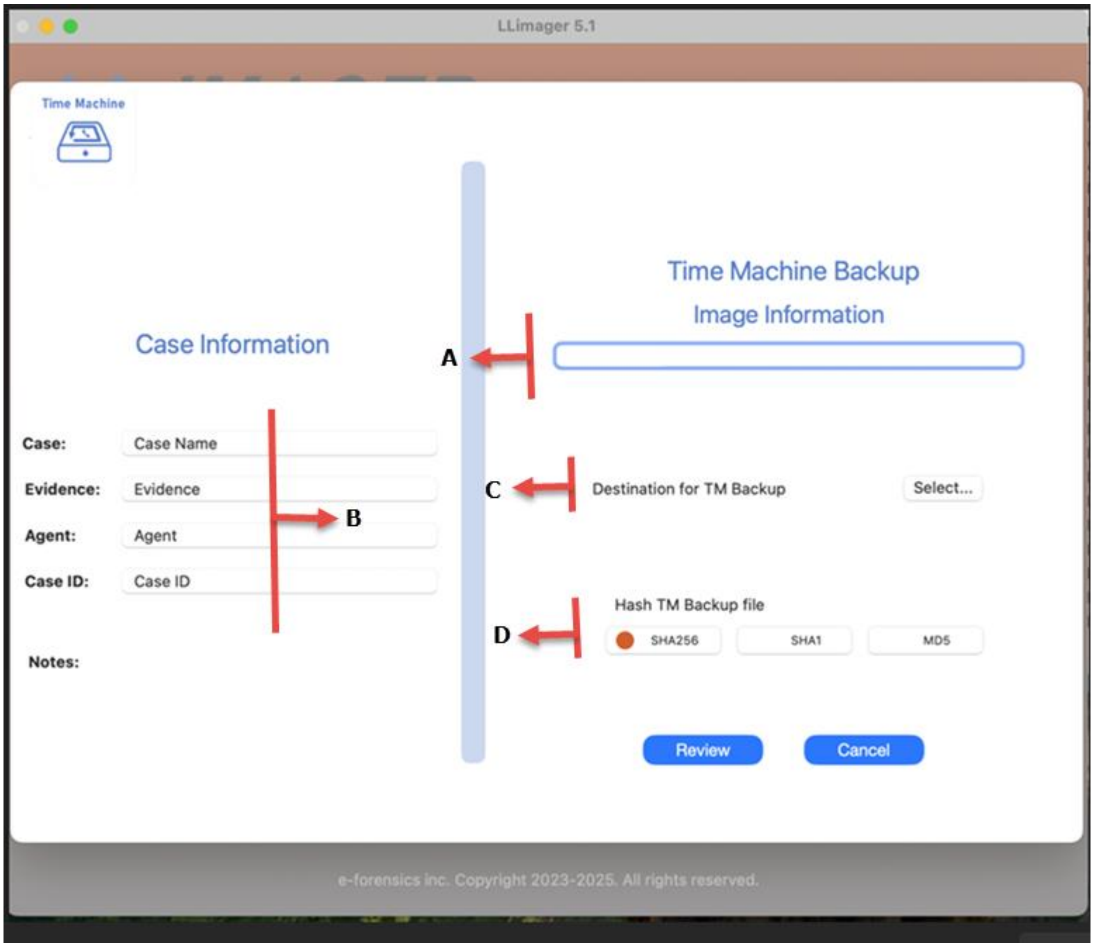
Menu Option (Time Machine)

Note, Time Machine backups, while valuable for general data recovery, intentionally exclude certain system folders and files to optimize backup size and performance.

Specifically, Time Machine omits volatile data within /private/var/folders/, temporary files from /private/var/tmp/ and /private/tmp/, cache files from /Library/Caches/ and /Users/*/Library/Caches/, and all user and system trash folders (~/.Trash, /Volumes/*/.Trashes/, and /.Trashes/). This exclusion of temporary and system-generated data is designed to focus on backing up essential user documents and settings.

However, LL*IMAGER* Time Machine backups do collect the Trash folders and bundles into the final DMG. Thus, making it a suitable image for e-discovery and depending on the scope, some digital forensics workflows.

To proceed with the Time Machine imaging, Input the image destination name and location of the destination logical DMG file. Additionally, choose to hash and type of hash. The following picture shows the requested information.



LLimager 5.1

Time Machine

Case Information

Case: Case Name

Evidence: Evidence

Agent: Agent

Case ID: Case ID

Notes:

Time Machine Backup

Image Information

Destination for TM Backup

Hash TM Backup file

● SHA256 ○ SHA1 ○ MD5

e-forensics inc. Copyright 2023-2025. All rights reserved.

See below for a description of each section.

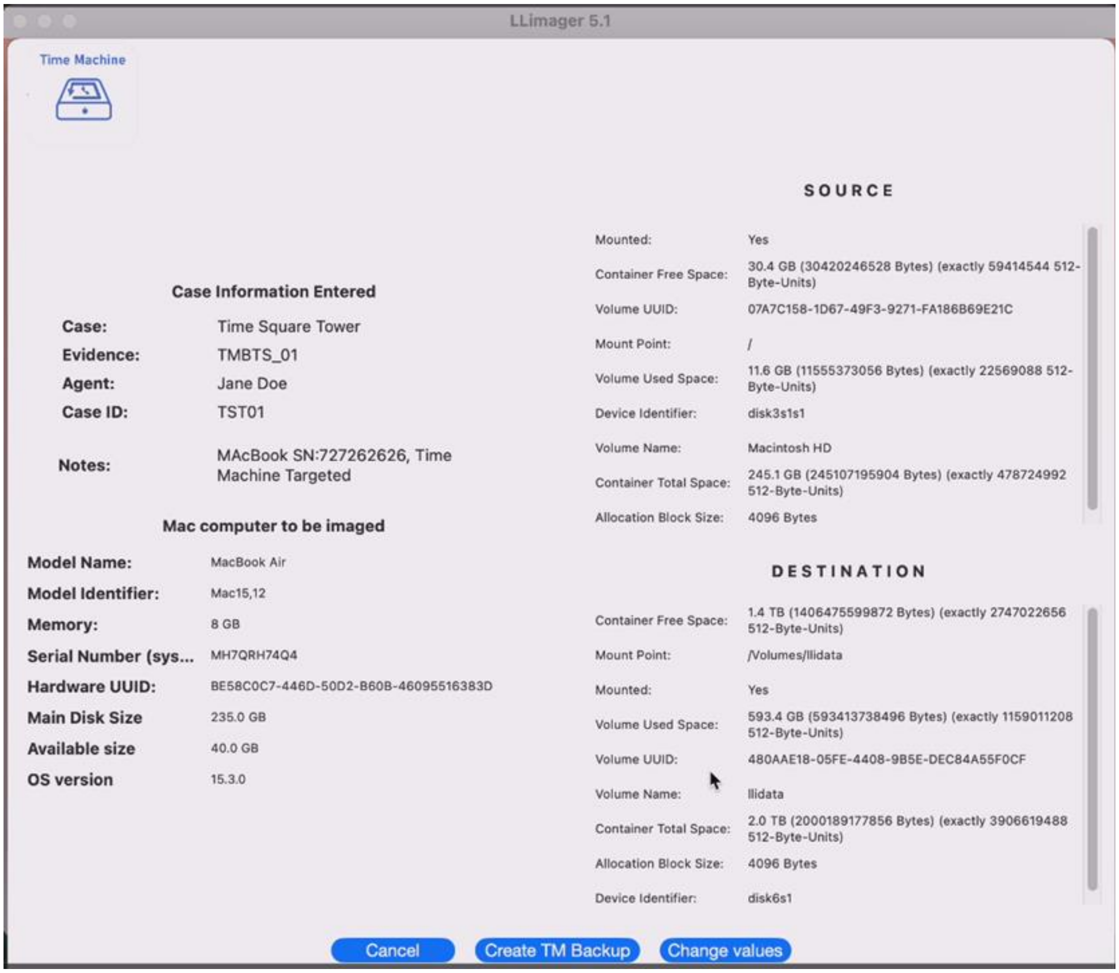
A – Specify the name of the image.

B -- Related to the case. Case name, evidence number, agent, case ID and notes.

C – Related to the *destination of the Time Machine DMG* file. Requires selection of path where the DMG will be saved.

D – Related to *hashing of the DMG* file. Specify if the DMG will be hashed then specify the type of hash.

After completing the selections, a summary of the information provided; see below.



Case Information Entered

Case:	Time Square Tower
Evidence:	TMBTS_01
Agent:	Jane Doe
Case ID:	TST01
Notes:	MAcBook SN:727262626, Time Machine Targeted

Mac computer to be imaged

Model Name:	MacBook Air
Model Identifier:	Mac15,12
Memory:	8 GB
Serial Number (sys...	MH7QRH74Q4
Hardware UUID:	BE58C0C7-446D-50D2-B60B-46095516383D
Main Disk Size	235.0 GB
Available size	40.0 GB
OS version	15.3.0

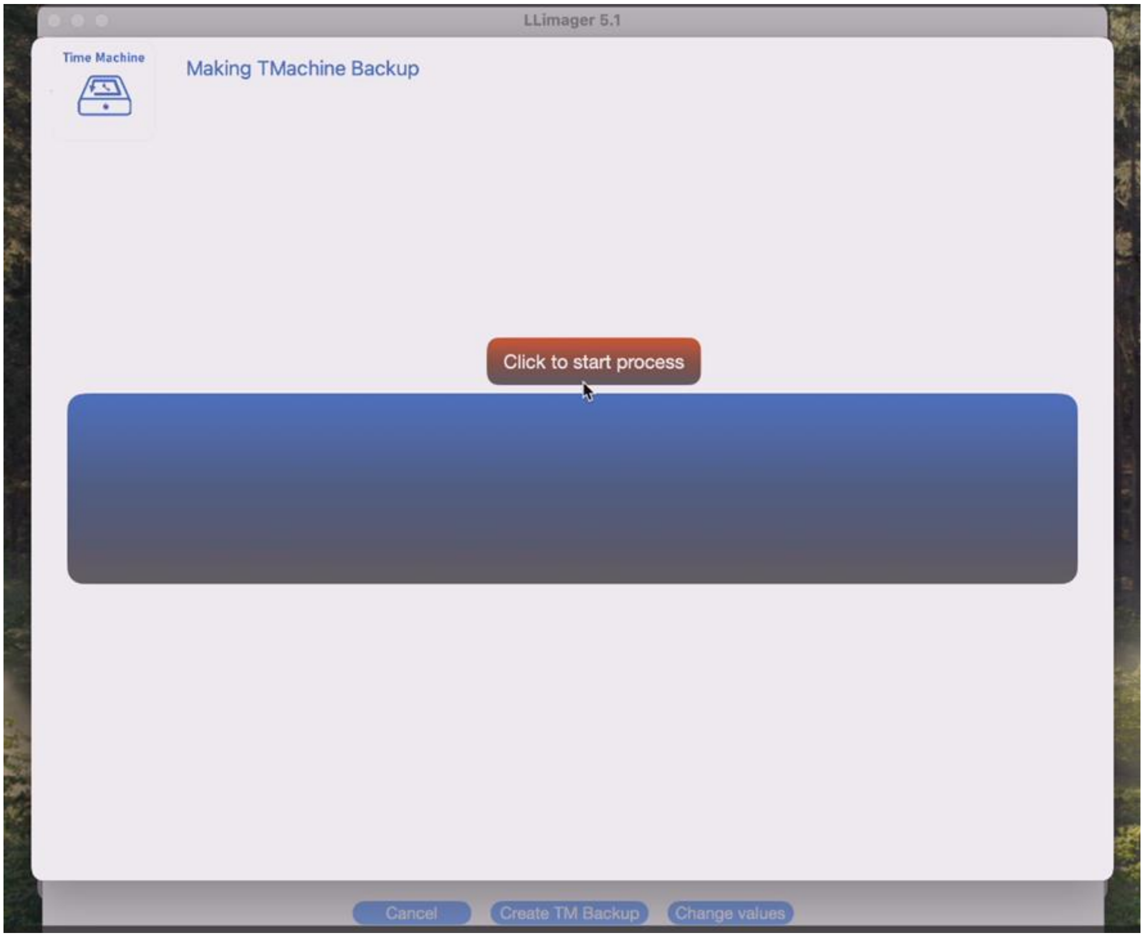
SOURCE

Mounted:	Yes
Container Free Space:	30.4 GB (30420246528 Bytes) (exactly 59414544 512-Byte-Units)
Volume UUID:	07A7C158-1D67-49F3-9271-FA186B69E21C
Mount Point:	/
Volume Used Space:	11.6 GB (11555373056 Bytes) (exactly 22569088 512-Byte-Units)
Device Identifier:	disk3s1s1
Volume Name:	Macintosh HD
Container Total Space:	245.1 GB (245107195904 Bytes) (exactly 478724992 512-Byte-Units)
Allocation Block Size:	4096 Bytes

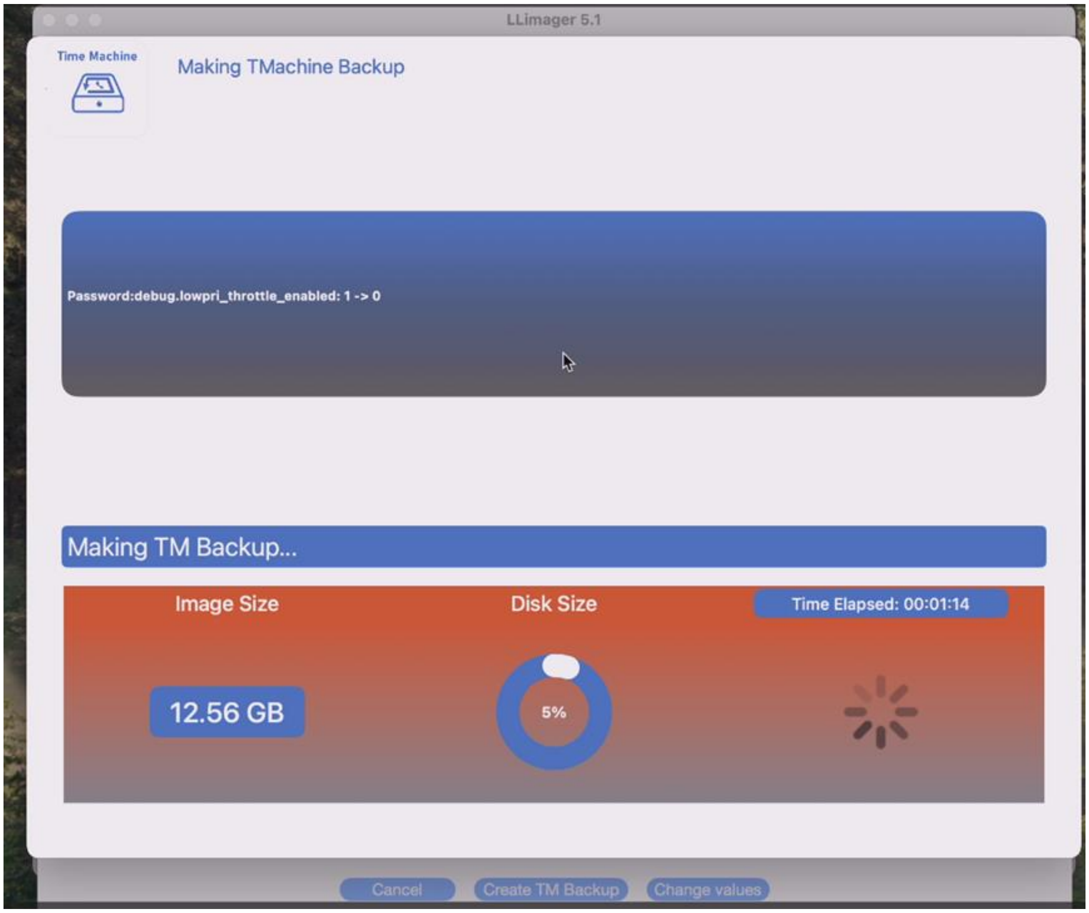
DESTINATION

Container Free Space:	1.4 TB (1406475599872 Bytes) (exactly 2747022656 512-Byte-Units)
Mount Point:	/Volumes/llidata
Mounted:	Yes
Volume Used Space:	593.4 GB (593413738496 Bytes) (exactly 1159011208 512-Byte-Units)
Volume UUID:	480AAE18-05FE-4408-9B5E-DEC84A55F0CF
Volume Name:	llidata
Container Total Space:	2.0 TB (2000189177856 Bytes) (exactly 3906619488 512-Byte-Units)
Allocation Block Size:	4096 Bytes
Device Identifier:	disk6s1

After validating and accepting the information, click on “Create TM Backup” and the following will appear:



Click on “Click to start process” and as the process commences, a progress screen indicating that the DMG logical image is being generated will appear -- see below:



Making TMachine Backup

```
Password:debug.lowpri_throttle_enabled: 1 -> 0
```

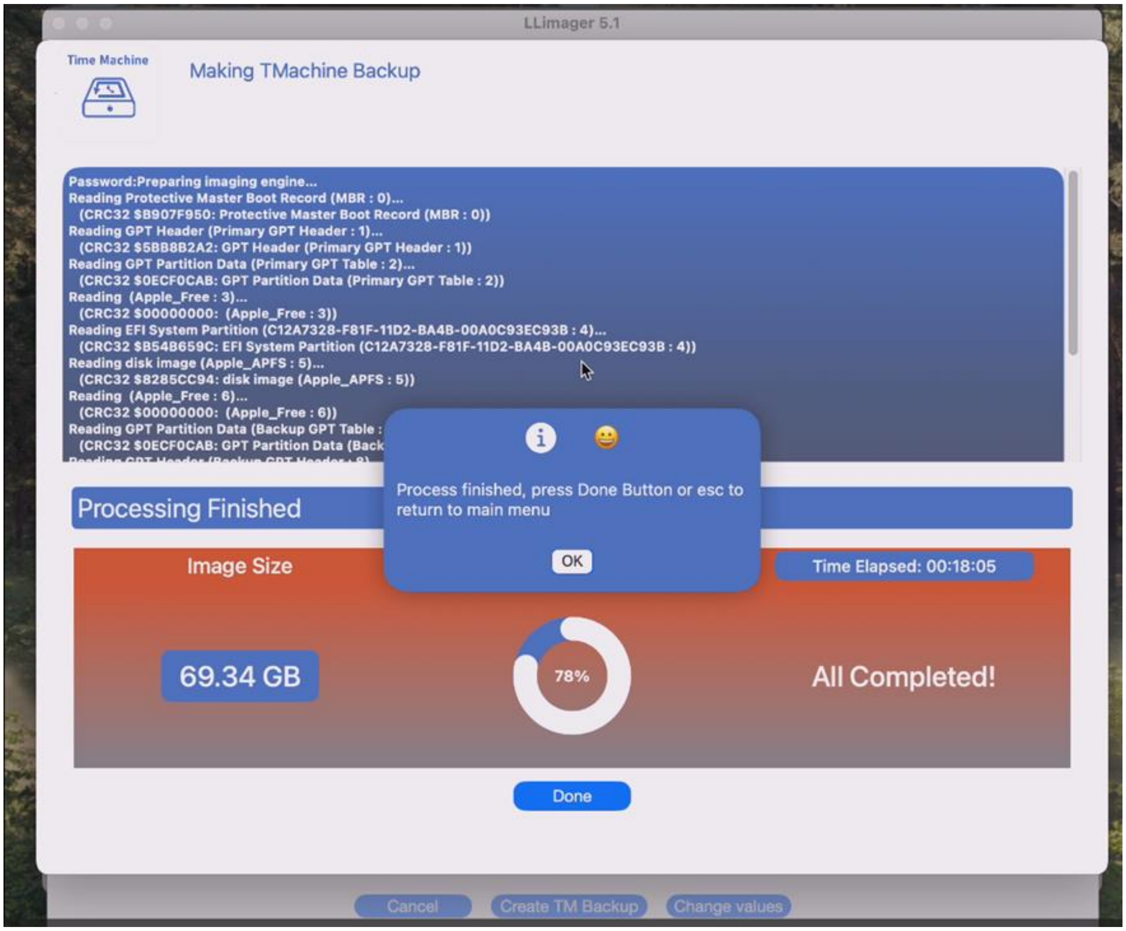
Making TM Backup...

Image Size: 12.56 GB

Disk Size: 5%

Time Elapsed: 00:01:14

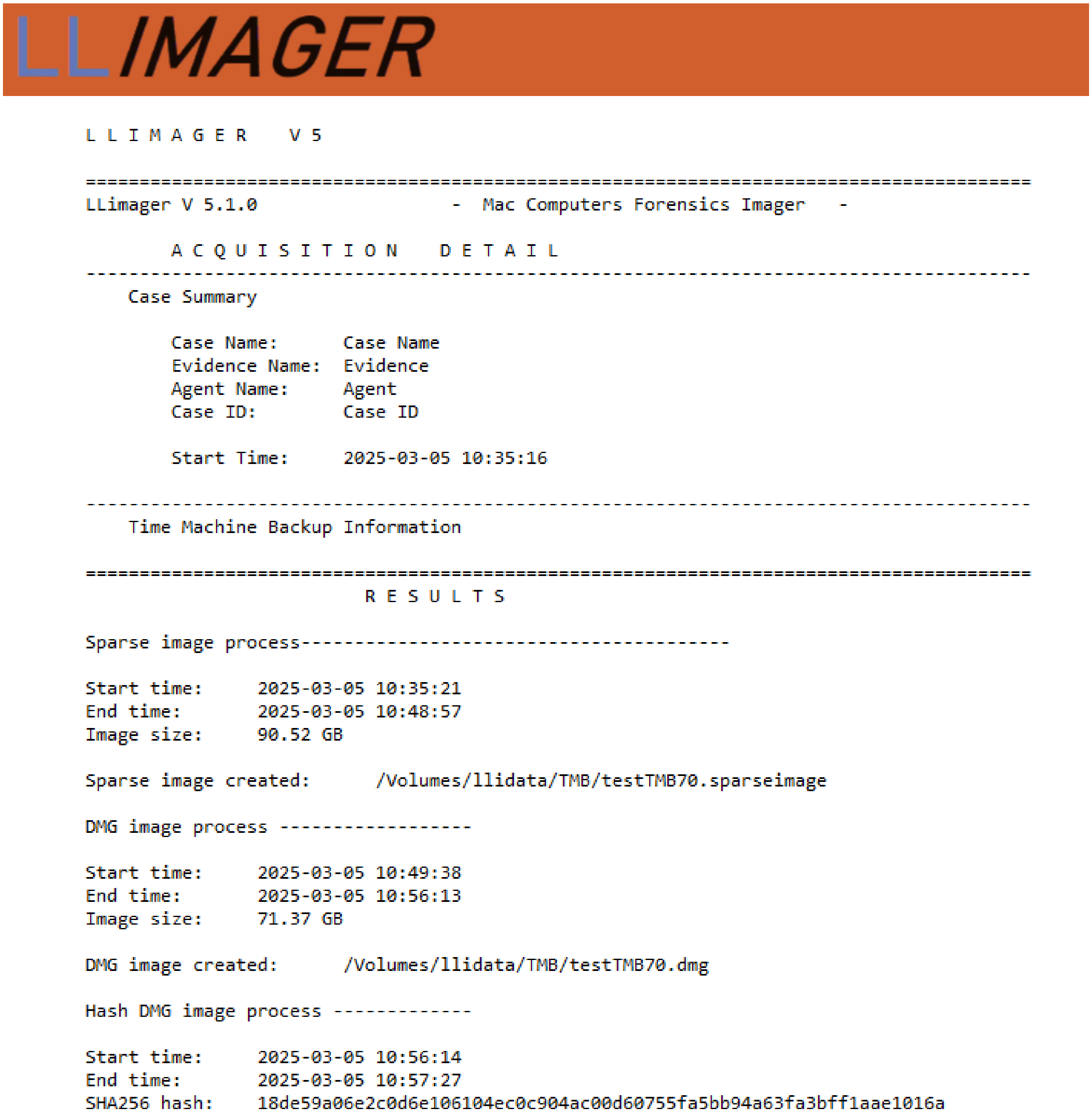
When complete, the following will appear:



```
Password:Preparing imaging engine...
Reading Protective Master Boot Record (MBR : 0)...
  (CRC32 $B907F950: Protective Master Boot Record (MBR : 0))
Reading GPT Header (Primary GPT Header : 1)...
  (CRC32 $5BB8B2A2: GPT Header (Primary GPT Header : 1))
Reading GPT Partition Data (Primary GPT Table : 2)...
  (CRC32 $0ECF0CAB: GPT Partition Data (Primary GPT Table : 2))
Reading  (Apple_Free : 3)...
  (CRC32 $00000000:  (Apple_Free : 3))
Reading EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4)...
  (CRC32 $B54B659C: EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4))
Reading disk image (Apple_APFS : 5)...
  (CRC32 $8285CC94: disk image (Apple_APFS : 5))
Reading  (Apple_Free : 6)...
  (CRC32 $00000000:  (Apple_Free : 6))
Reading GPT Partition Data (Backup GPT Table :
  (CRC32 $0ECF0CAB: GPT Partition Data (Back
```

Process finished, press Done Button or esc to return to main menu

The produced acquisition log will appear as below:

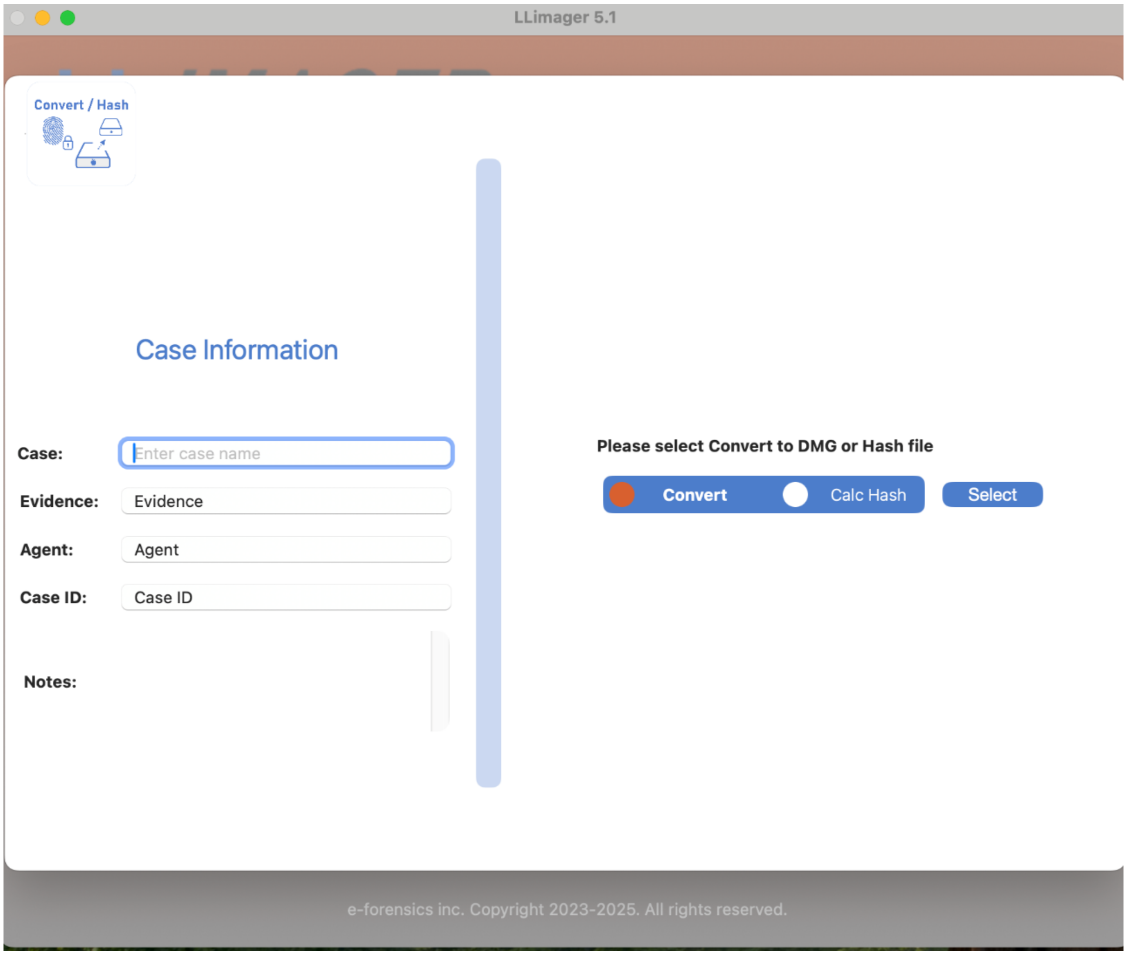


LLIMAGER

```
L L I M A G E R   V 5

=========================================================================================
LLimager V 5.1.0                  -  Mac Computers Forensics Imager   -

        A C Q U I S I T I O N   D E T A I L
-----------------------------------------------------------------------------------------
    Case Summary

        Case Name:       Case Name
        Evidence Name:   Evidence
        Agent Name:      Agent
        Case ID:         Case ID

        Start Time:      2025-03-05 10:35:16

-----------------------------------------------------------------------------------------
    Time Machine Backup Information

=========================================================================================
                          R E S U L T S

Sparse image process----------------------------------------

Start time:     2025-03-05 10:35:21
End time:       2025-03-05 10:48:57
Image size:     90.52 GB

Sparse image created:      /Volumes/llidata/TMB/testTMB70.sparseimage

DMG image process ------------------

Start time:     2025-03-05 10:49:38
End time:       2025-03-05 10:56:13
Image size:     71.37 GB

DMG image created:      /Volumes/llidata/TMB/testTMB70.dmg

Hash DMG image process -------------

Start time:     2025-03-05 10:56:14
End time:       2025-03-05 10:57:27
SHA256 hash:    18de59a06e2c0d6e106104ec0c904ac00d60755fa5bb94a63fa3bff1aae1016a
```

Menu Option (**Convert**/Hash)

This feature is available to convert the temp file (spare image) to a DMG.



Case Information

Case: Enter case name

Evidence: Evidence

Agent: Agent

Case ID: Case ID

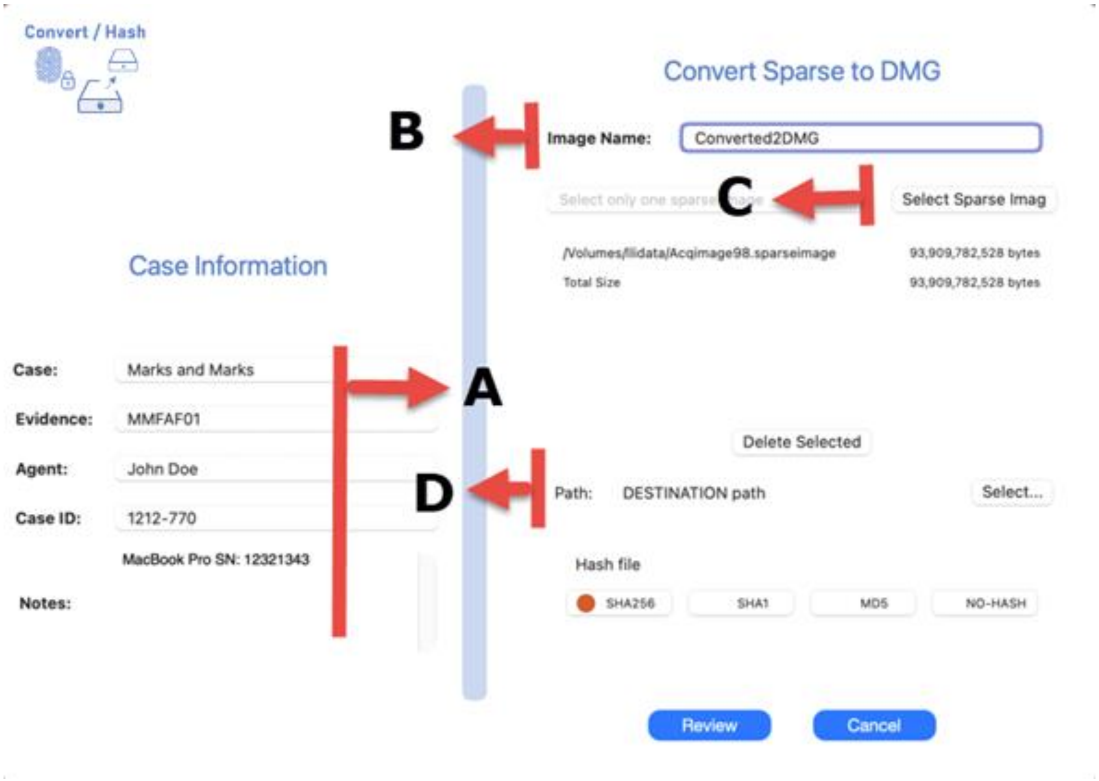
Notes:

Please select Convert to DMG or Hash file

● Convert ○ Calc Hash

e-forensics inc. Copyright 2023-2025. All rights reserved.

Input the DMG file name and location of the destination logical DMG file. The following picture shows the requested information.



Convert Sparse to DMG

Image Name: Converted2DMG

Select only one sparse image — Select Sparse Imag

/Volumes/llidata/Acqimage98.sparseimage	93,909,782,528 bytes
Total Size	93,909,782,528 bytes

Delete Selected

Path: DESTINATION path — Select...

Hash file

● SHA256 ○ SHA1 ○ MD5 ○ NO-HASH

Case Information

Case: Marks and Marks

Evidence: MMFAF01

Agent: John Doe

Case ID: 1212-770

Notes: MacBook Pro SN: 12321343

See below for a description of each section.

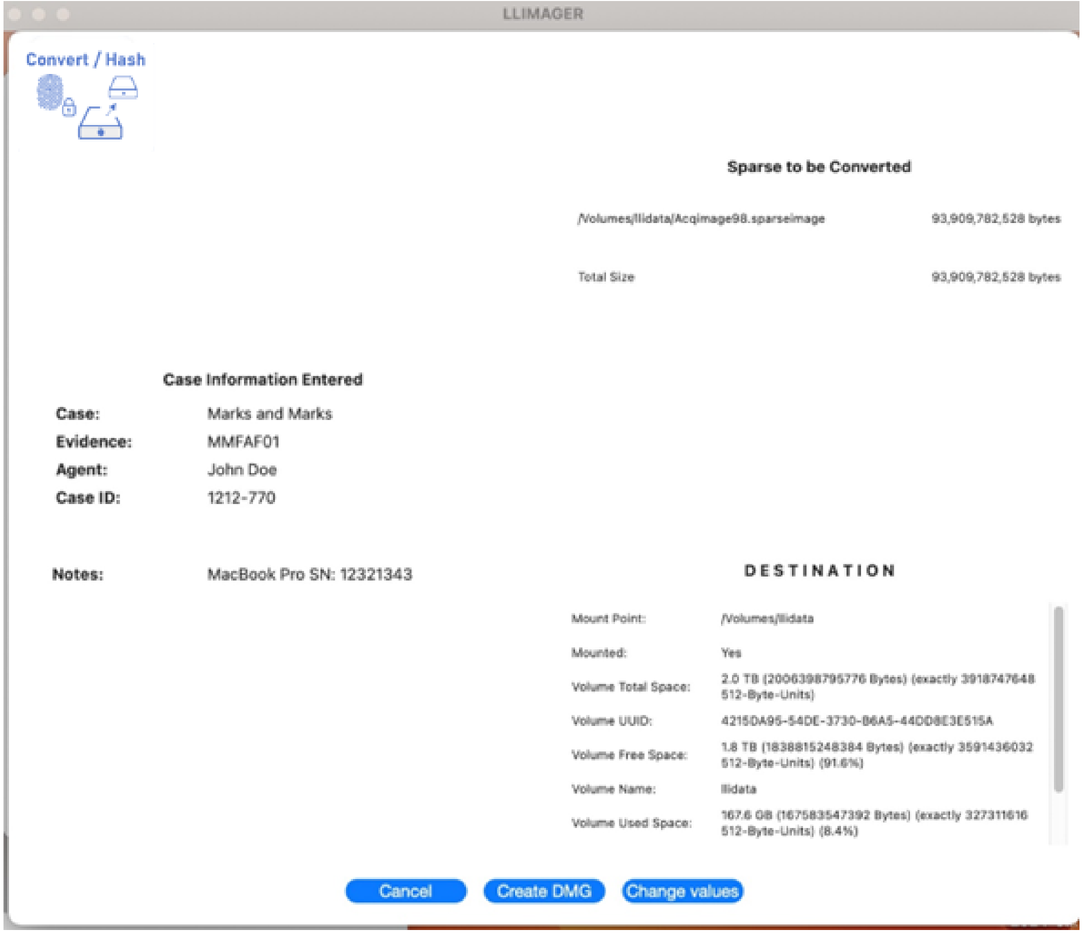
A – Specify case related information

B – Related to the name to give the DMG file.

C – Related to the source sparse image to be converted.

D – The path where the destination DMG will be stored.

After completing the selections, clock on Review for summary of the information provided; see below.



Sparse to be Converted

/Volumes/llidata/Acqimage98.sparseimage	93,909,782,528 bytes
Total Size	93,909,782,528 bytes

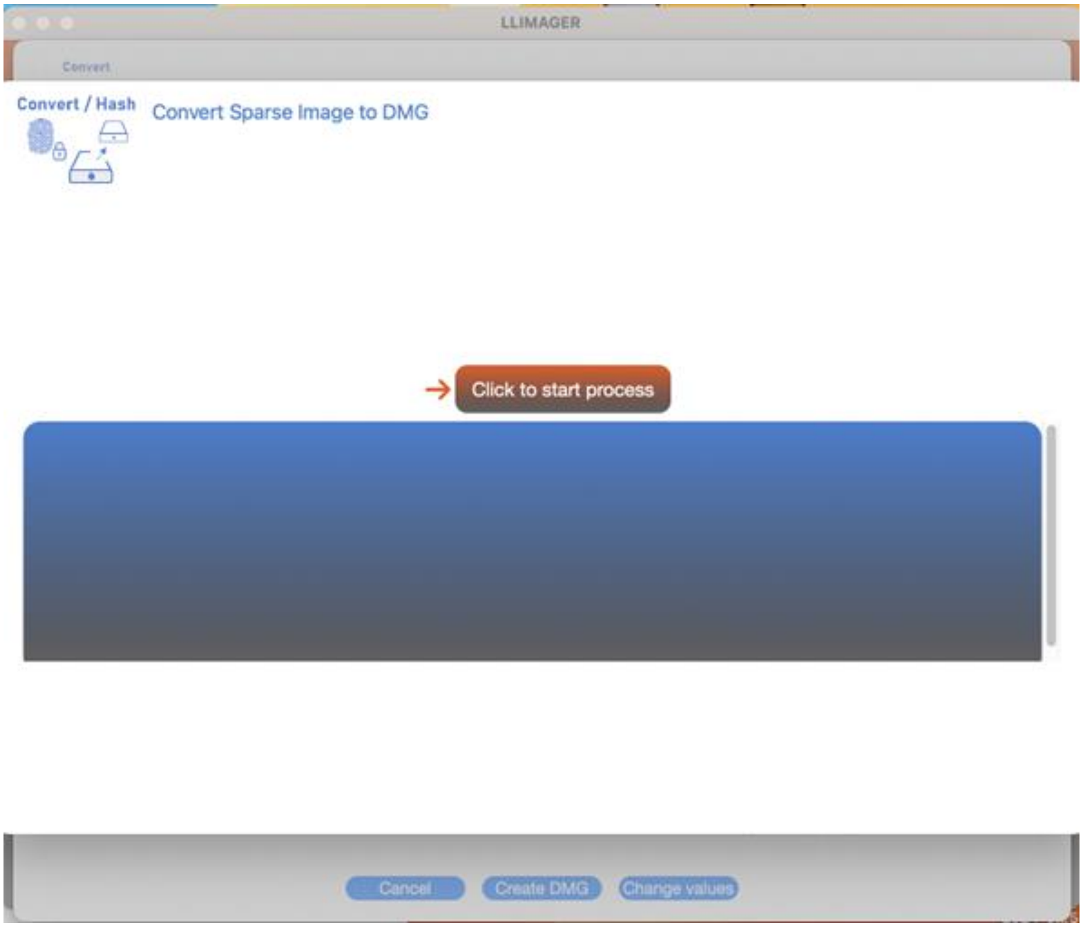
Case Information Entered

Case:	Marks and Marks
Evidence:	MMFAF01
Agent:	John Doe
Case ID:	1212-770
Notes:	MacBook Pro SN: 12321343

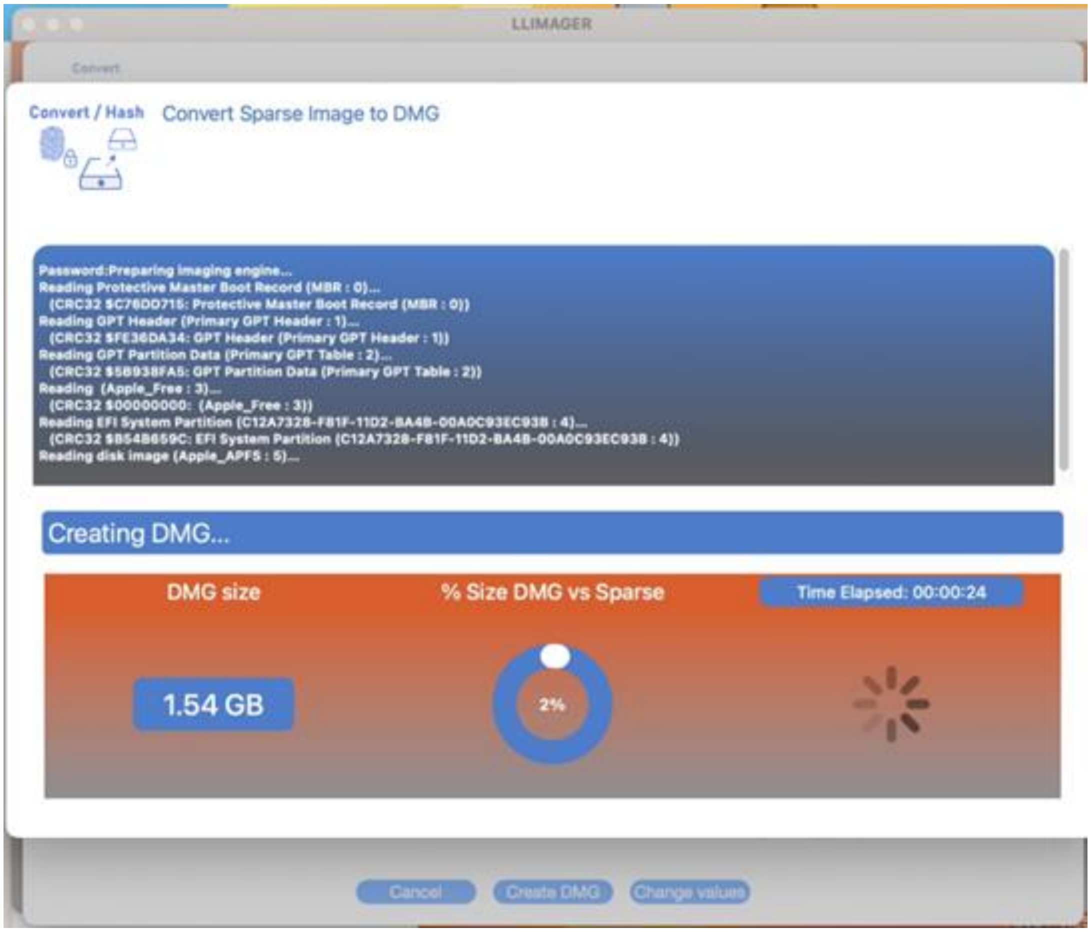
DESTINATION

Mount Point:	/Volumes/llidata
Mounted:	Yes
Volume Total Space:	2.0 TB (2006398795776 Bytes) (exactly 3918747648 512-Byte-Units)
Volume UUID:	4215DA95-54DE-3730-86A5-44DD8E3E515A
Volume Free Space:	1.8 TB (1838815248384 Bytes) (exactly 3591436032 512-Byte-Units) (91.6%)
Volume Name:	llidata
Volume Used Space:	167.6 GB (167583547392 Bytes) (exactly 327311616 512-Byte-Units) (8.4%)

Upon completing the review, click “Create DMG” and the following screen will appear, and click on “Click to start process”):



Upon completion, the following will appear:



```
Password:Preparing imaging engine...
Reading Protective Master Boot Record (MBR : 0)...
  (CRC32 $C76DD715: Protective Master Boot Record (MBR : 0))
Reading GPT Header (Primary GPT Header : 1)...
  (CRC32 $FE36DA34: GPT Header (Primary GPT Header : 1))
Reading GPT Partition Data (Primary GPT Table : 2)...
  (CRC32 $5B938FA5: GPT Partition Data (Primary GPT Table : 2))
Reading  (Apple_Free : 3)...
  (CRC32 $00000000:  (Apple_Free : 3))
Reading EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4)...
  (CRC32 $B54B659C: EFI System Partition (C12A7328-F81F-11D2-BA4B-00A0C93EC93B : 4))
Reading disk image (Apple_APFS : 5)...
```

Creating DMG...

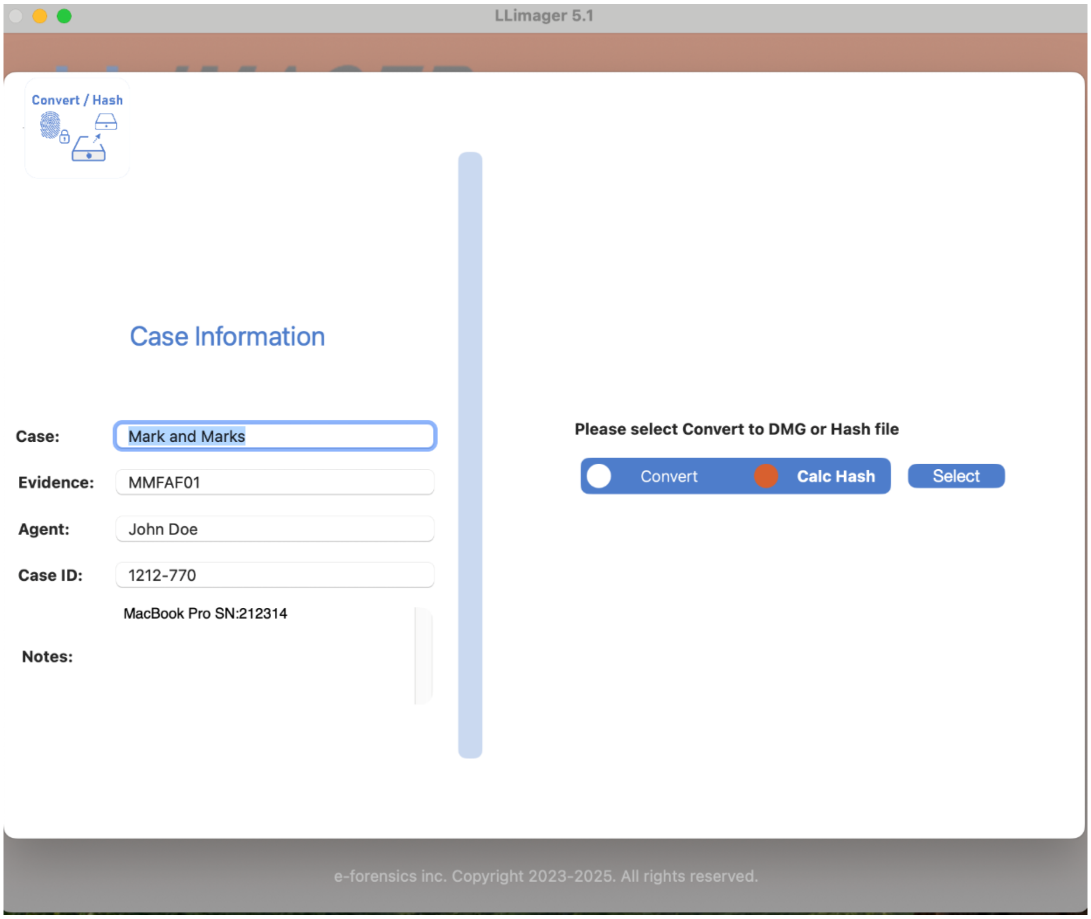
DMG size: 1.54 GB

% Size DMG vs Sparse: 2%

Time Elapsed: 00:00:24

Menu Option (Convert/Hash)

The hash option is used to calculate the hash of a file, be it sparse image, DMG or any other type, and the following picture shows the fields and selection options:



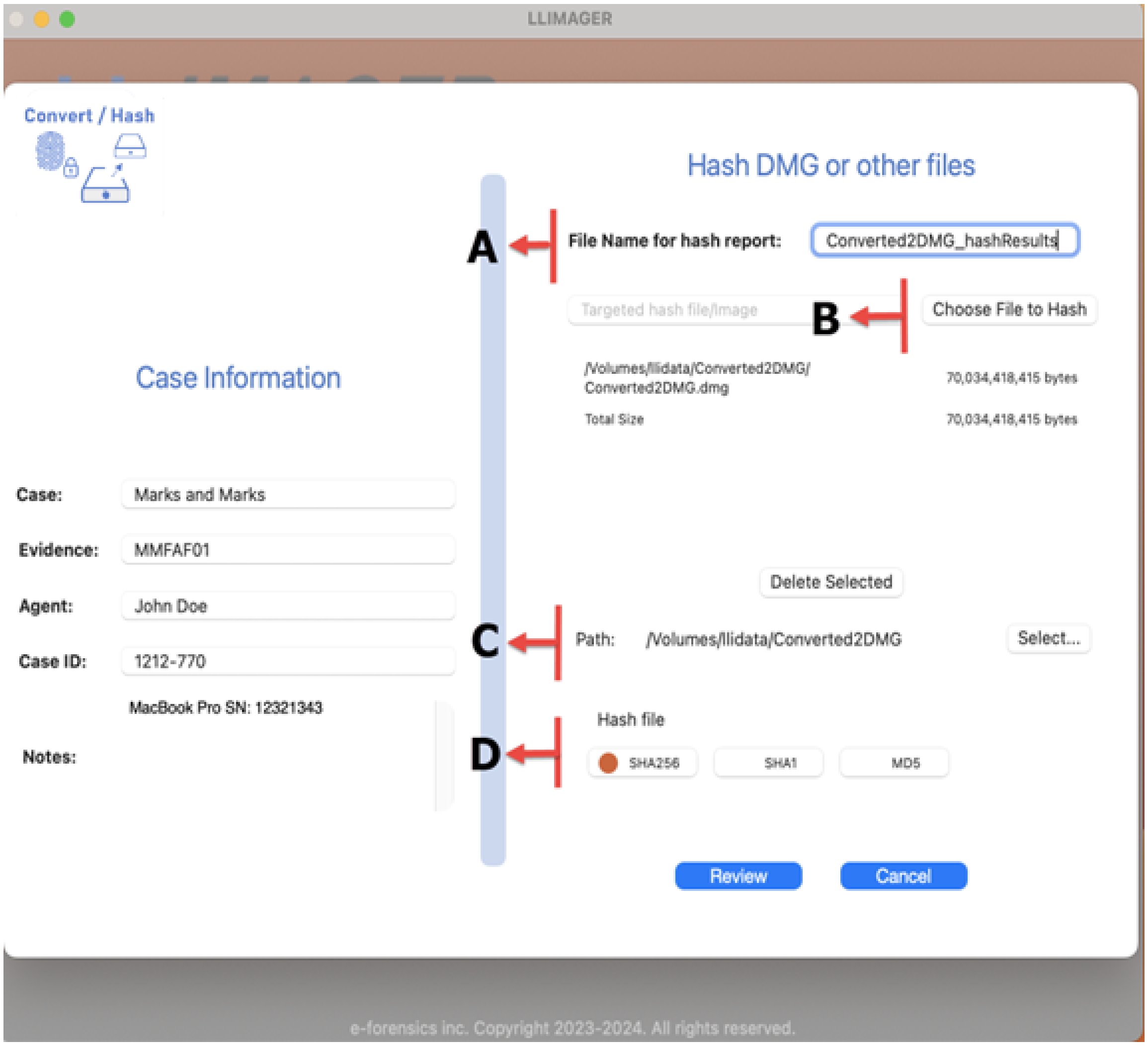
Case Information

Case:	Mark and Marks
Evidence:	MMFAF01
Agent:	John Doe
Case ID:	1212-770
Notes:	MacBook Pro SN:212314

Please select Convert to DMG or Hash file

○ Convert ● Calc Hash

e-forensics inc. Copyright 2023-2025. All rights reserved.



LLIMAGER

Convert / Hash

Hash DMG or other files

File Name for hash report: Converted2DMG_hashResults

Targeted hash file/image — Choose File to Hash

/Volumes/llidata/Converted2DMG/ Converted2DMG.dmg	70,034,418,415 bytes
Total Size	70,034,418,415 bytes

Case Information

Case:	Marks and Marks
Evidence:	MMFAF01
Agent:	John Doe
Case ID:	1212-770
	MacBook Pro SN: 12321343
Notes:	

Delete Selected

Path: /Volumes/llidata/Converted2DMG — Select...

Hash file

● SHA256 ○ SHA1 ○ MD5

Review — Cancel

e-forensics inc. Copyright 2023-2024. All rights reserved.

See below for a description of each section.

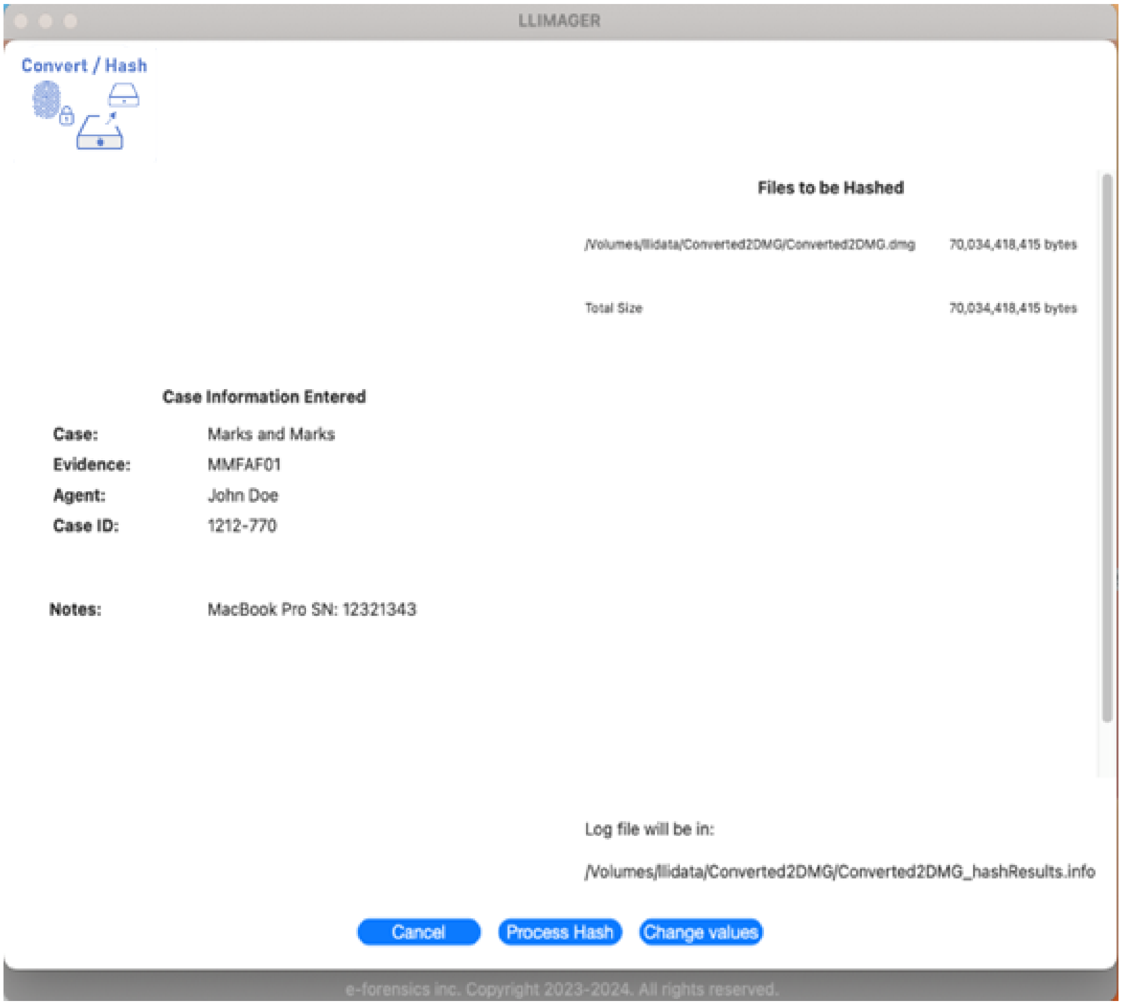
A – Specify the name of the hash report file.

B – Related to the *source files/folders*. Requires selection of the source files to hash.

C – Related to the *destination of the hash report* file. Requires selection of path hash report destination folder.

D – Related to *hashing type.* Specify the type of hash.

After completing the selections, a summary of the information is provided; see below.



Files to be Hashed

/Volumes/llidata/Converted2DMG/Converted2DMG.dmg	70,034,418,415 bytes
Total Size	70,034,418,415 bytes

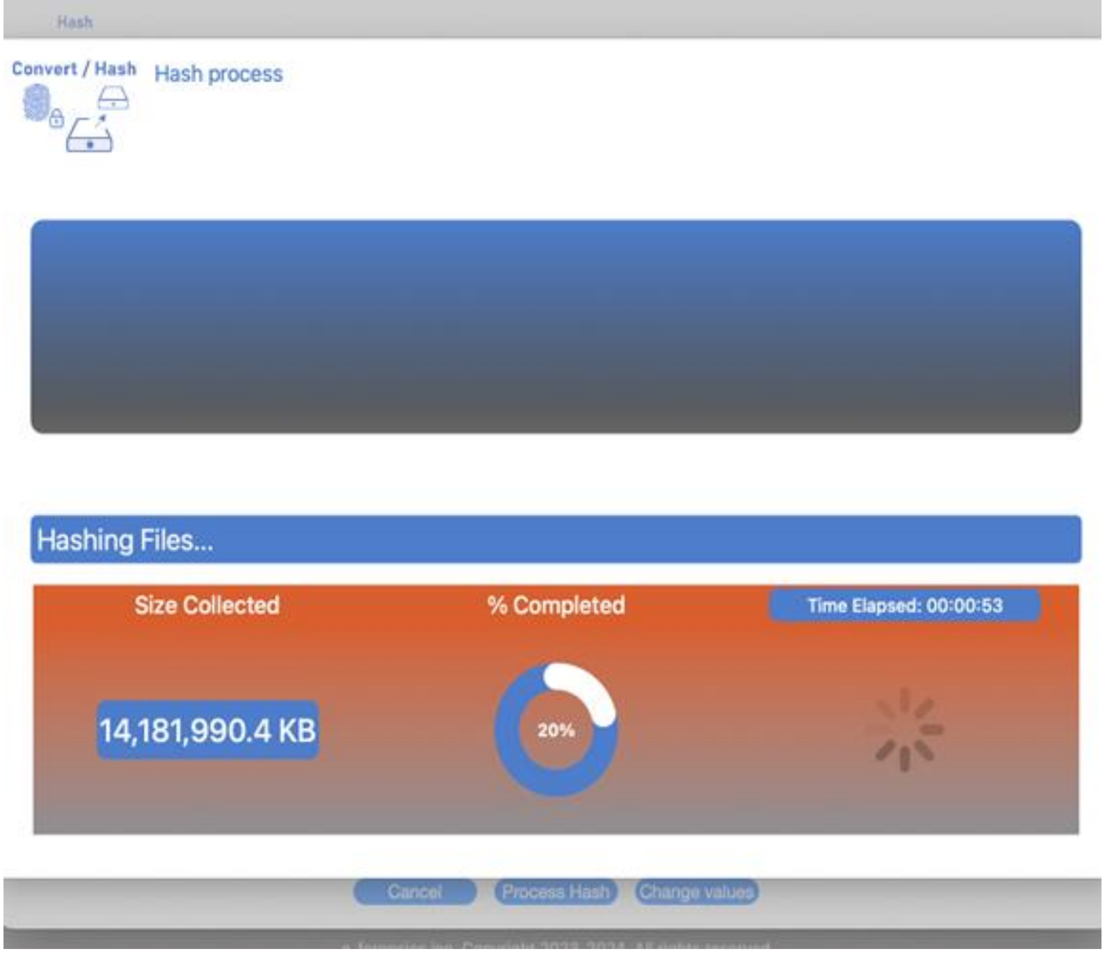
Case Information Entered

Case:	Marks and Marks
Evidence:	MMFAF01
Agent:	John Doe
Case ID:	1212-770
Notes:	MacBook Pro SN: 12321343

Log file will be in:

/Volumes/llidata/Converted2DMG/Converted2DMG_hashResults.info

Proceed to click on "Process Hash" and the following will appear:

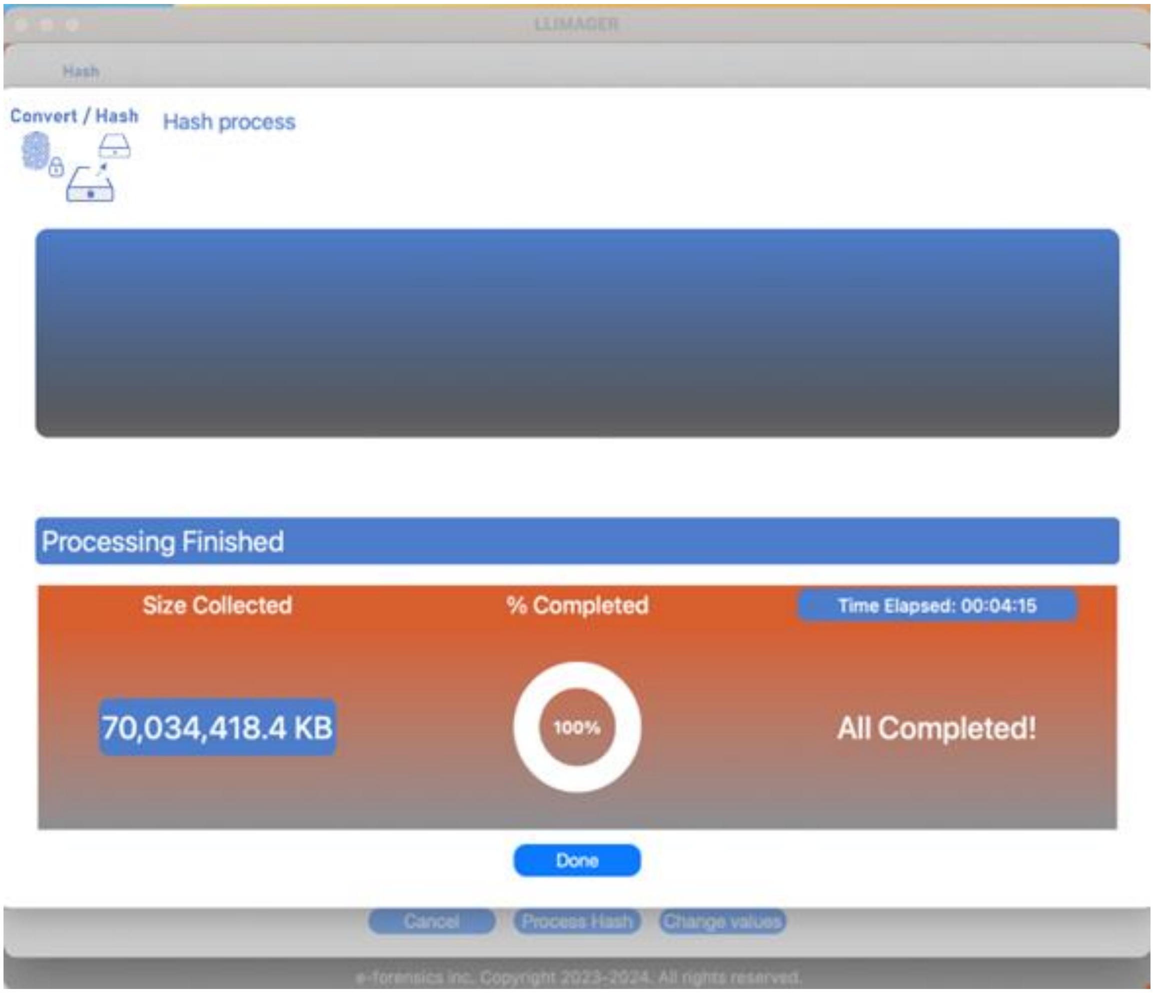


Hashing Files...

Size Collected: 14,181,990.4 KB

% Completed: 20%

Time Elapsed: 00:00:53



Hash process

Processing Finished

Size Collected: 70,034,418.4 KB

% Completed: 100%

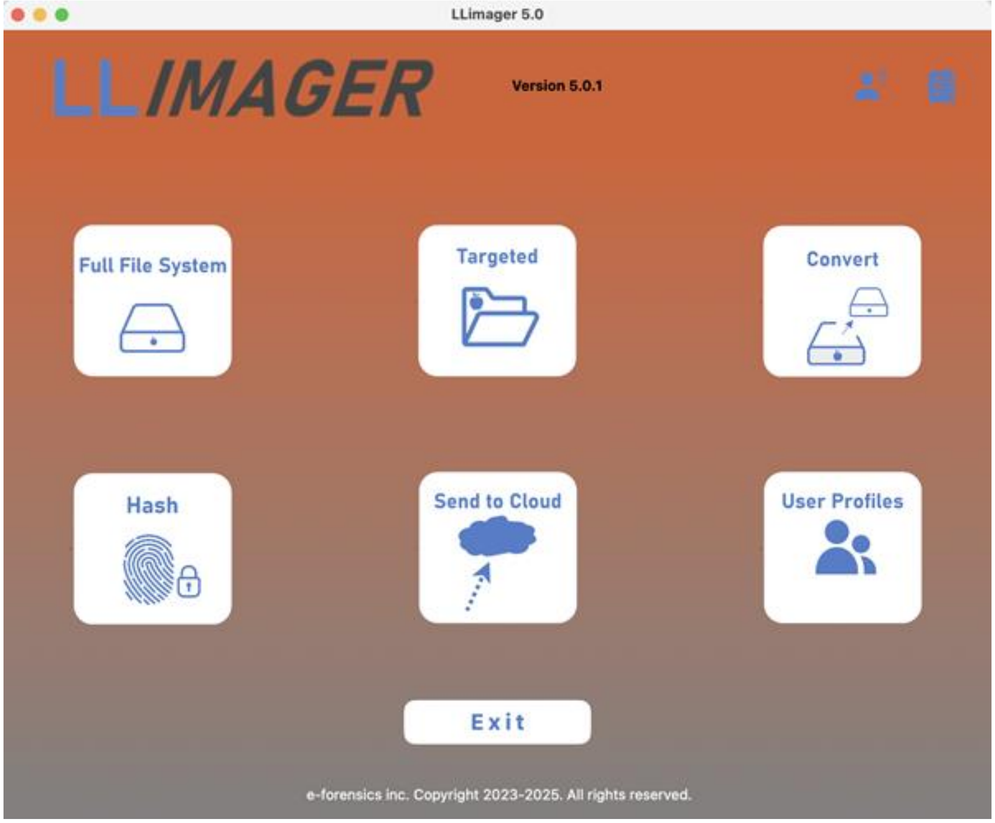
Time Elapsed: 00:04:15

All Completed!

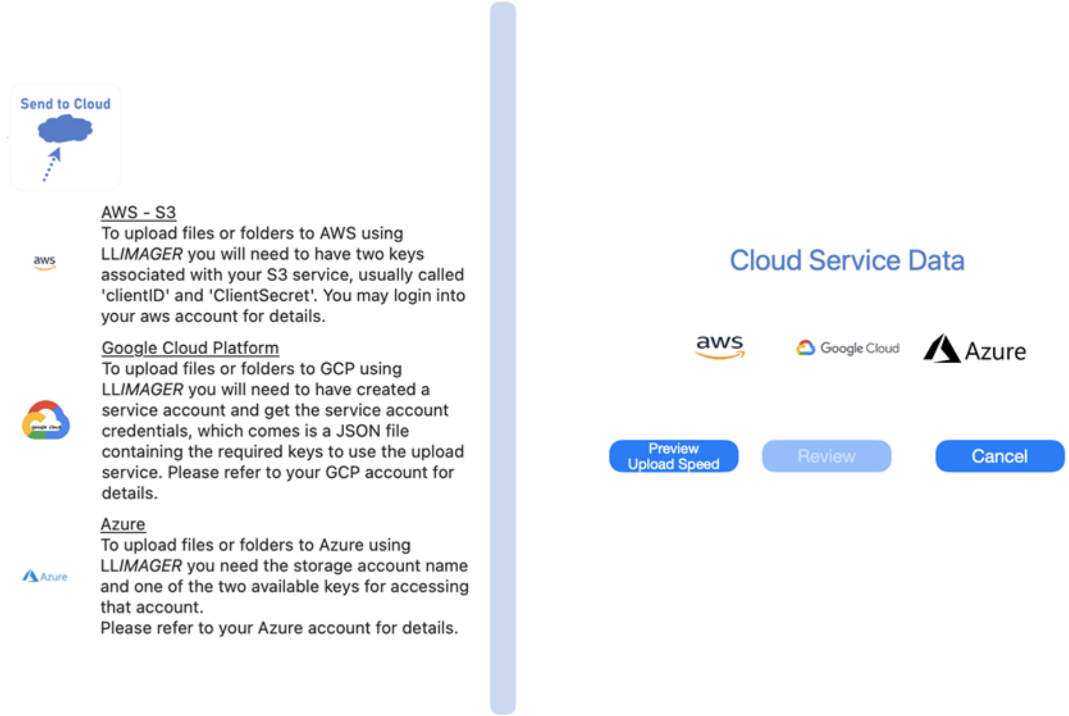
e-forensics inc. Copyright 2023-2024. All rights reserved.

Menu Option (Send To Cloud)

For examiners and e-discovery services providers with cloud storage availability, LL*IMAGER* has added a feature to copy images to AWS, Google Cloud or Azure.



Upon clicking the "Send to Cloud" button, the main interface displays two primary sections. The left pane provides general information regarding the prerequisites for utilizing each supported cloud service, while the right pane presents the service selection interface.



AWS - S3
To upload files or folders to AWS using LL*IMAGER* you will need to have two keys associated with your S3 service, usually called 'clientID' and 'ClientSecret'. You may login into your aws account for details.

Google Cloud Platform
To upload files or folders to GCP using LL*IMAGER* you will need to have created a service account and get the service account credentials, which comes is a JSON file containing the required keys to use the upload service. Please refer to your GCP account for details.

Azure
To upload files or folders to Azure using LL*IMAGER* you need the storage account name and one of the two available keys for accessing that account.
Please refer to your Azure account for details.

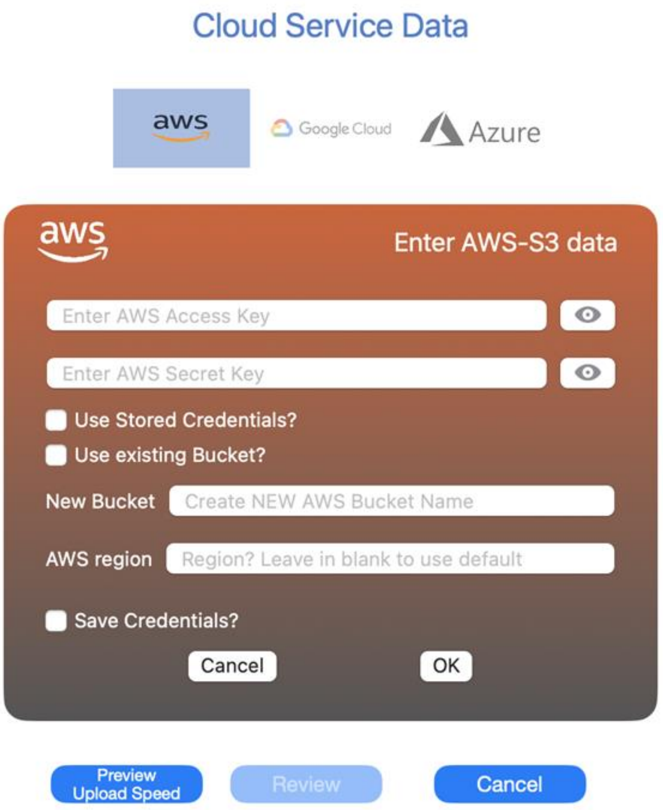
Specific authentication requirements for each service are as follows:

- **Amazon Web Services (AWS):** Uploads to AWS require two credentials: a Client ID and a Secret ID. These credentials can be readily obtained by the user through the AWS Management Console.
- **Google Cloud Platform (GCP):** Uploads to GCP require a credential JSON file, accessible through the user's Google Cloud account.
- **Azure Storage:** Uploads to Azure Storage necessitate two credentials: the Account Name and one of the two Secret Keys associated with that account. These keys are provided by Azure.

For enhanced security and streamlined access, all credentials can be securely stored (password-protected) on the LL*IMAGER* device.

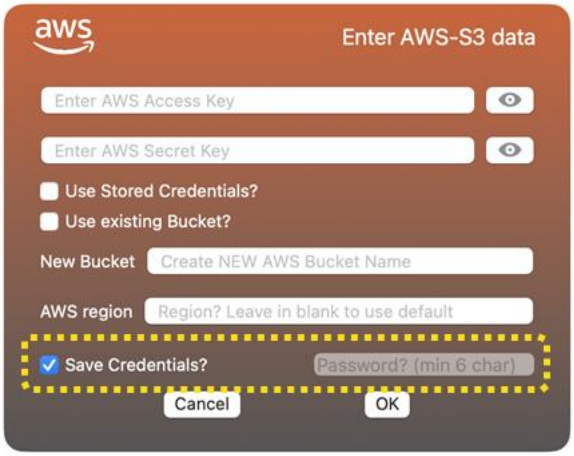
Furthermore, the interface provides a preview of the anticipated upload speeds within the target environment.

For example, to use AWS:

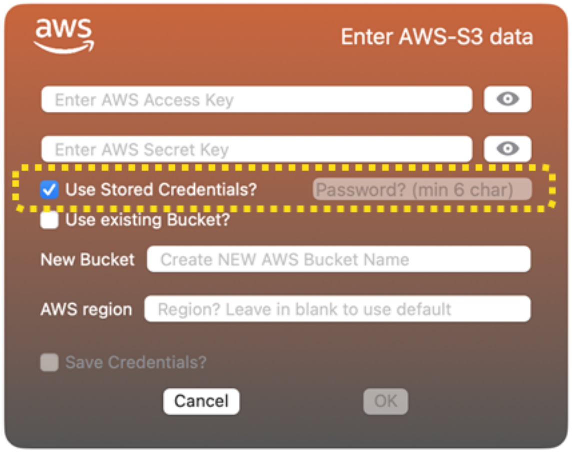


The two required AWS credentials, Client ID and Secret ID, should be entered in the designated fields. Users have the option to select an existing bucket or create a new one.

For most users, utilizing the default AWS region is recommended. This can be achieved by leaving the AWS Region field blank.



To save the AWS credentials for future use, click "Save Credentials?" and a password prompt will appear to add a password.



Enter AWS Access Key

Enter AWS Secret Key

☑ Use Stored Credentials? Password? (min 6 char)

□ Use existing Bucket?

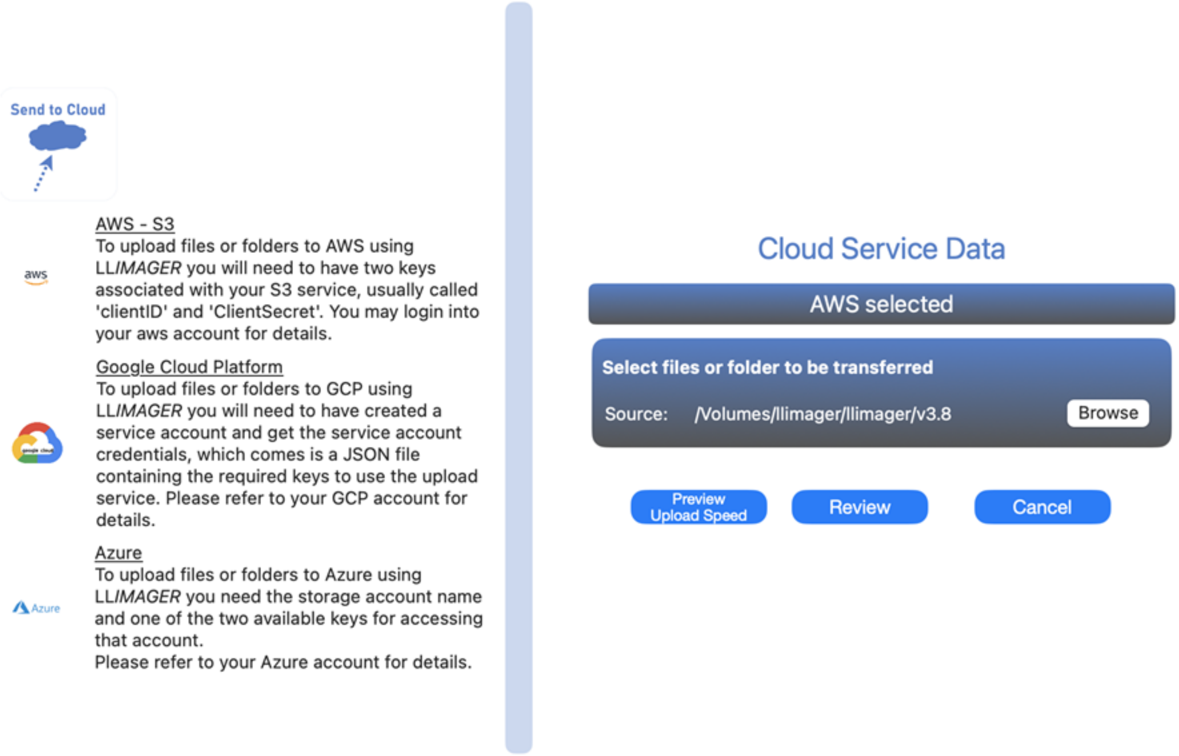
New Bucket: Create NEW AWS Bucket Name

AWS region: Region? Leave in blank to use default

□ Save Credentials?

Previously saved credentials can be retrieved by clicking "Use Stored Credentials?" Note, selecting "Use Stored Credentials" disables "Save Credentials".

Upon pressing the OK button, the next step is to select the image or folder to be uploaded; see below:



AWS - S3
To upload files or folders to AWS using LL*IMAGER* you will need to have two keys associated with your S3 service, usually called 'clientID' and 'ClientSecret'. You may login into your aws account for details.

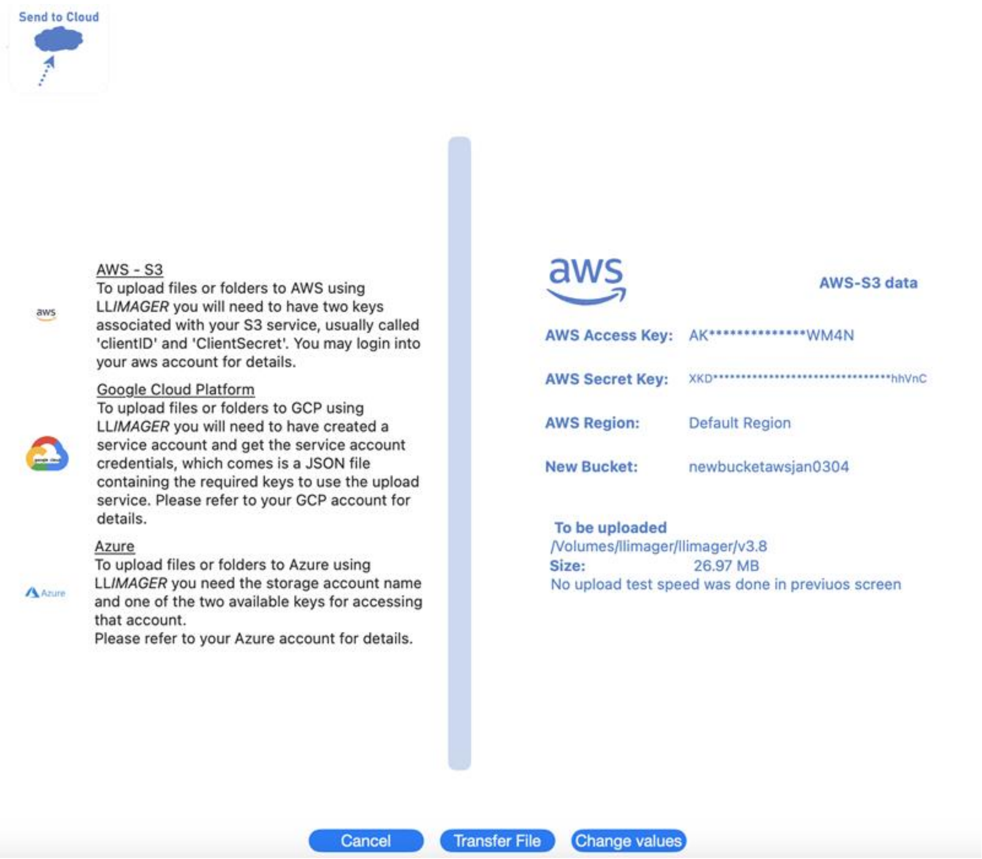
Google Cloud Platform
To upload files or folders to GCP using LL*IMAGER* you will need to have created a service account and get the service account credentials, which comes is a JSON file containing the required keys to use the upload service. Please refer to your GCP account for details.

Azure
To upload files or folders to Azure using LL*IMAGER* you need the storage account name and one of the two available keys for accessing that account.
Please refer to your Azure account for details.

Select files or folder to be transferred

Source: /Volumes/llimager/llimager/v3.8

Once the credentials have been entered, and the file or folder to upload has been selected, the review screen is presented showing all fields entered (credential masked) for review. Once satisfied click the Transfer File button; see below:



AWS - S3
To upload files or folders to AWS using LL*IMAGER* you will need to have two keys associated with your S3 service, usually called 'clientID' and 'ClientSecret'. You may login into your aws account for details.

Google Cloud Platform
To upload files or folders to GCP using LL*IMAGER* you will need to have created a service account and get the service account credentials, which comes is a JSON file containing the required keys to use the upload service. Please refer to your GCP account for details.

Azure
To upload files or folders to Azure using LL*IMAGER* you need the storage account name and one of the two available keys for accessing that account.
Please refer to your Azure account for details.

AWS-S3 data

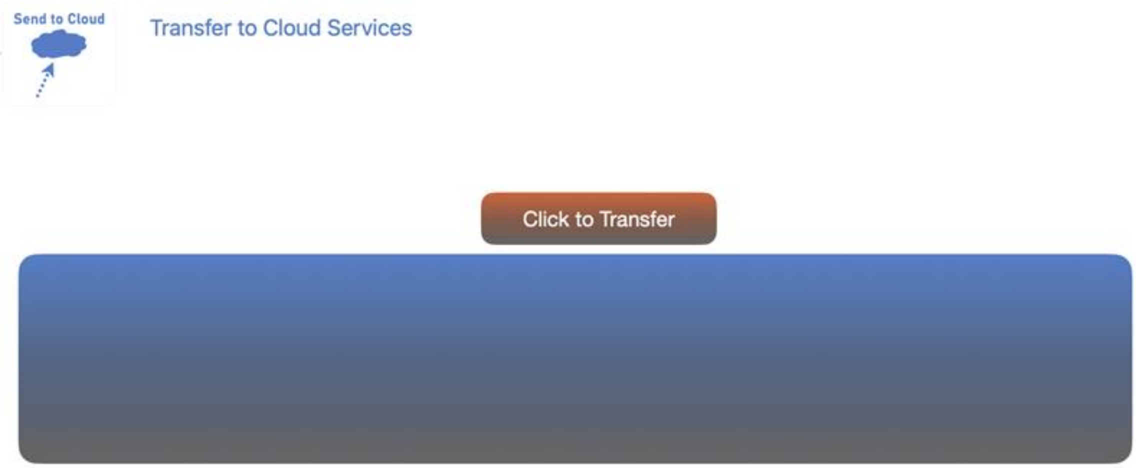
AWS Access Key: AK****************WM4N

AWS Secret Key: XKD********************************hhVnC

AWS Region: Default Region

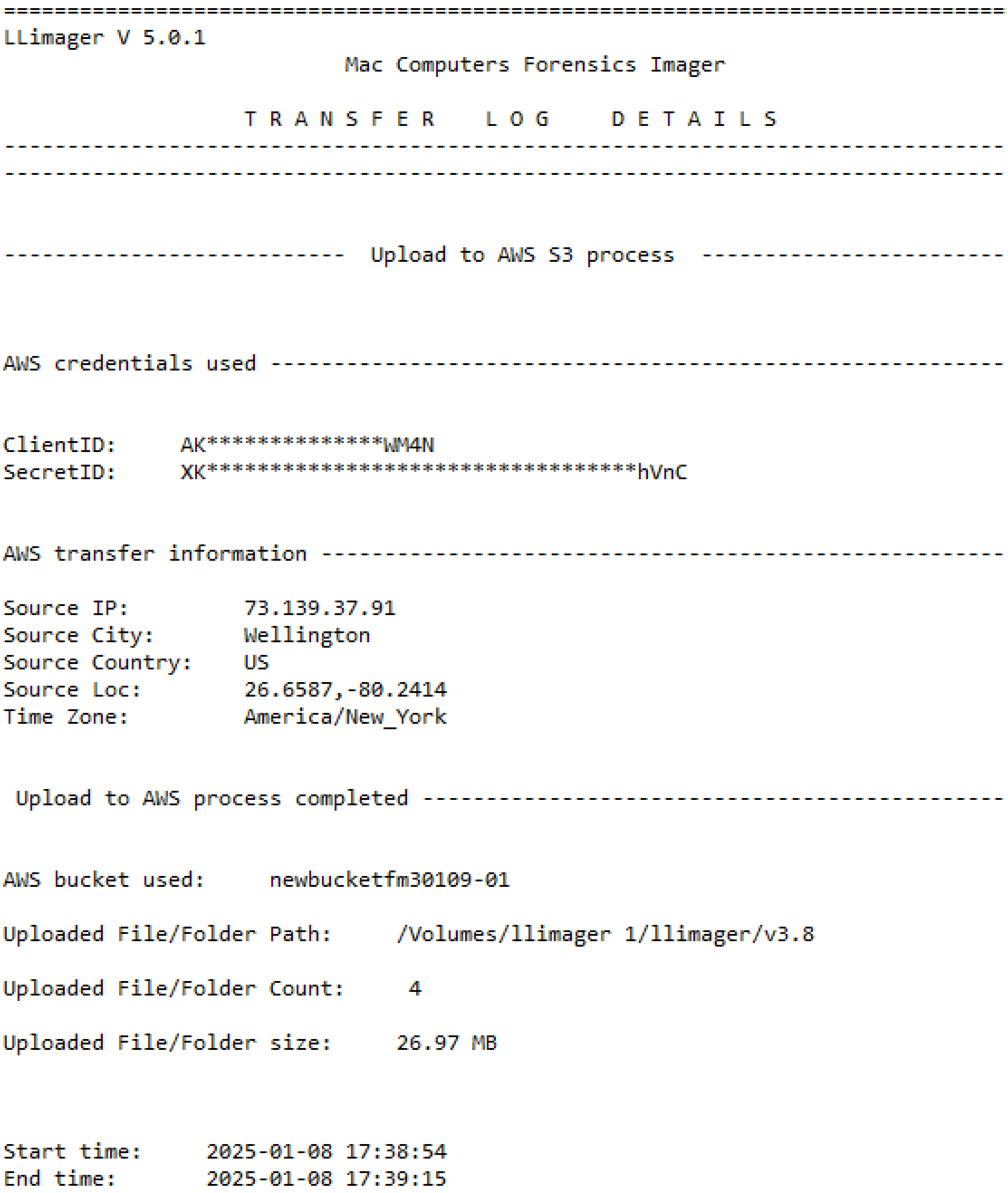
New Bucket: newbucketawsjan0304

To be uploaded
/Volumes/llimager/llimager/v3.8
Size: 26.97 MB
No upload test speed was done in previuos screen

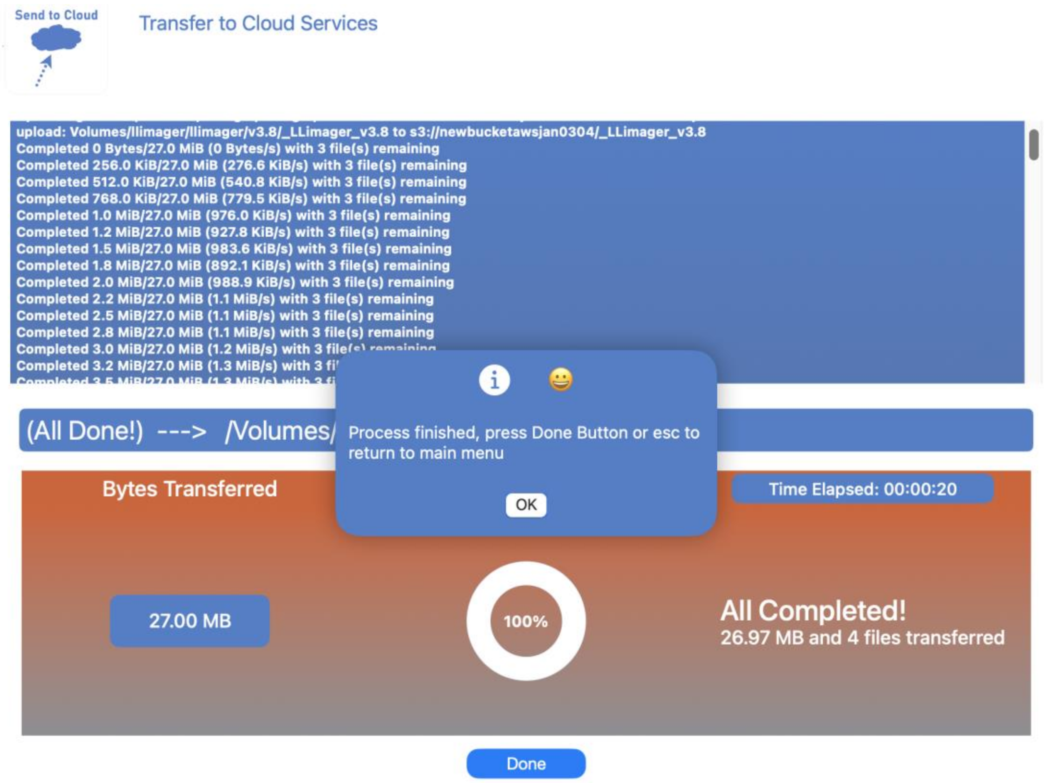


Transfer to Cloud Services

Below is a sample of the transfer log:



```
===============================================================================
LLimager V 5.0.1
                           Mac Computers Forensics Imager

                   T R A N S F E R    L O G    D E T A I L S
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------


---------------------------  Upload to AWS S3 process  ------------------------



AWS credentials used ----------------------------------------------------------


ClientID:     AK**************WM4N
SecretID:     XK**********************************hVnC


AWS transfer information ------------------------------------------------------

Source IP:         73.139.37.91
Source City:       Wellington
Source Country:    US
Source Loc:        26.6587,-80.2414
Time Zone:         America/New_York


 Upload to AWS process completed ----------------------------------------------


AWS bucket used:     newbucketfm30109-01

Uploaded File/Folder Path:     /Volumes/llimager 1/llimager/v3.8

Uploaded File/Folder Count:     4

Uploaded File/Folder size:     26.97 MB



Start time:     2025-01-08 17:38:54
End time:       2025-01-08 17:39:15
```



Transfer to Cloud Services

```
upload: Volumes/llimager/llimager/v3.8/_LLimager_v3.8 to s3://newbucketawsjan0304/_LLimager_v3.8
Completed 0 Bytes/27.0 MiB (0 Bytes/s) with 3 file(s) remaining
Completed 256.0 KiB/27.0 MiB (276.6 KiB/s) with 3 file(s) remaining
Completed 512.0 KiB/27.0 MiB (540.8 KiB/s) with 3 file(s) remaining
Completed 768.0 KiB/27.0 MiB (779.5 KiB/s) with 3 file(s) remaining
Completed 1.0 MiB/27.0 MiB (976.0 KiB/s) with 3 file(s) remaining
Completed 1.2 MiB/27.0 MiB (927.8 KiB/s) with 3 file(s) remaining
Completed 1.5 MiB/27.0 MiB (983.6 KiB/s) with 3 file(s) remaining
Completed 1.8 MiB/27.0 MiB (892.1 KiB/s) with 3 file(s) remaining
Completed 2.0 MiB/27.0 MiB (988.9 KiB/s) with 3 file(s) remaining
Completed 2.2 MiB/27.0 MiB (1.1 MiB/s) with 3 file(s) remaining
Completed 2.5 MiB/27.0 MiB (1.1 MiB/s) with 3 file(s) remaining
Completed 2.8 MiB/27.0 MiB (1.1 MiB/s) with 3 file(s) remaining
Completed 3.0 MiB/27.0 MiB (1.2 MiB/s) with 3 file(s) remaining
Completed 3.2 MiB/27.0 MiB (1.3 MiB/s) with 3 fi
Completed 3.5 MiB/27.0 MiB (1.3 MiB/s) with 3 fi
```

(All Done!) ---> /Volumes/

Process finished, press Done Button or esc to return to main menu

Bytes Transferred: 27.00 MB

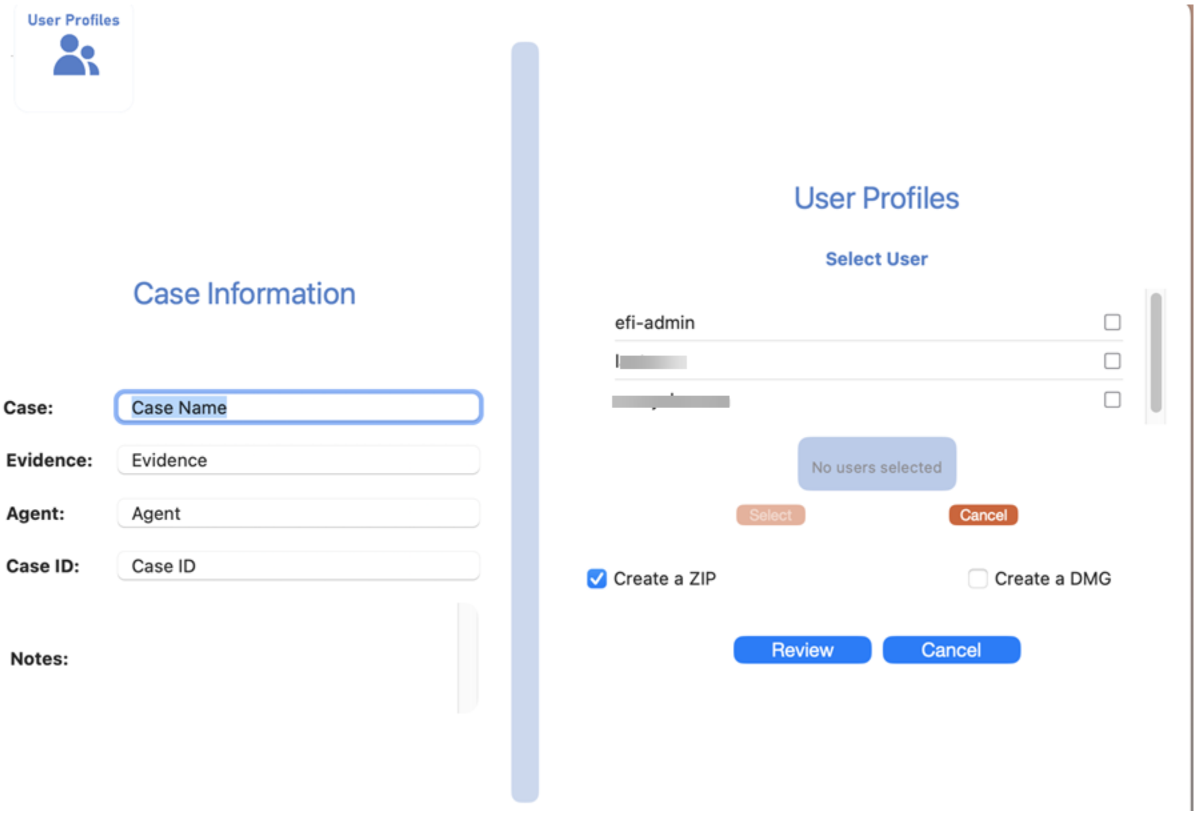
Time Elapsed: 00:00:20

All Completed!
26.97 MB and 4 files transferred

Menu Option (Profiles)

Aside from Targeted collections, LL*IMAGER* offers a forensic collection of user profiles from macOS systems.

The application presents a list of all available user profiles on the target system, allowing the examiner to select one or more profiles for extraction. Upon selection, the chosen profiles are collected and packaged into a single archive. Users can choose between two archive formats: ZIP or DMG (Apple Disk Image). This functionality enables efficient and comprehensive collection of user data for forensic analysis; see below:



Case Information

Case:	Case Name
Evidence:	Evidence
Agent:	Agent
Case ID:	Case ID
Notes:	

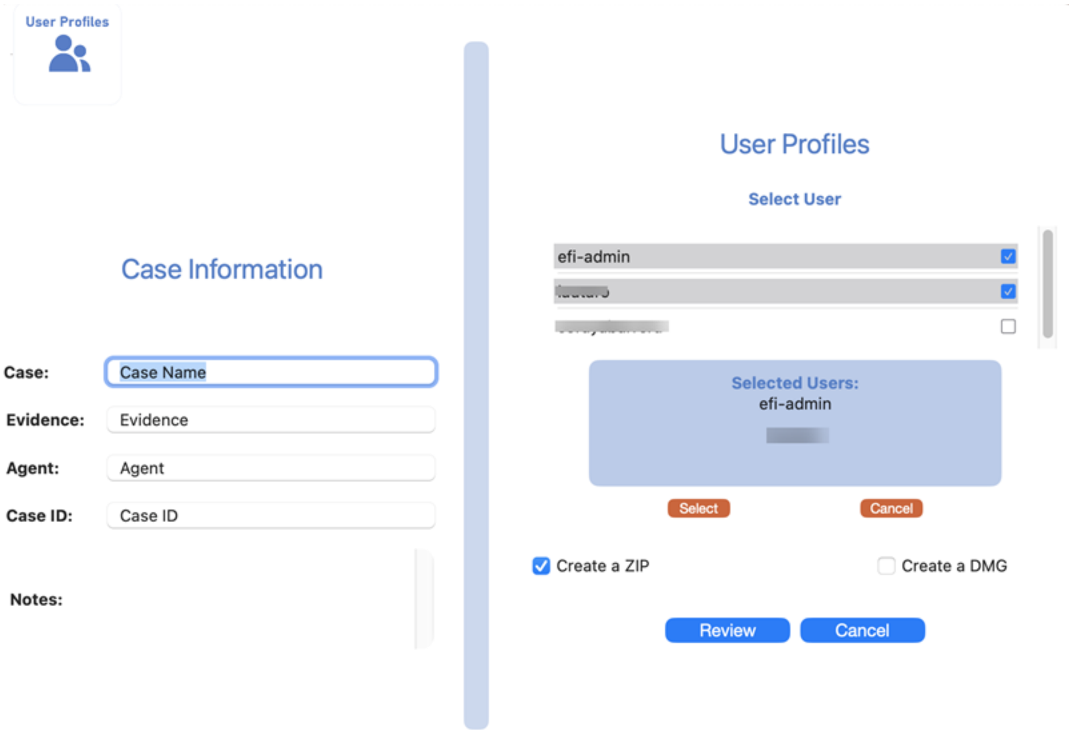
User Profiles

Select User

efi-admin	☐
[redacted]	☐
[redacted]	☐

No users selected

☑ Create a ZIP ☐ Create a DMG



Case Information

Case:	Case Name
Evidence:	Evidence
Agent:	Agent
Case ID:	Case ID
Notes:	

User Profiles

Select User

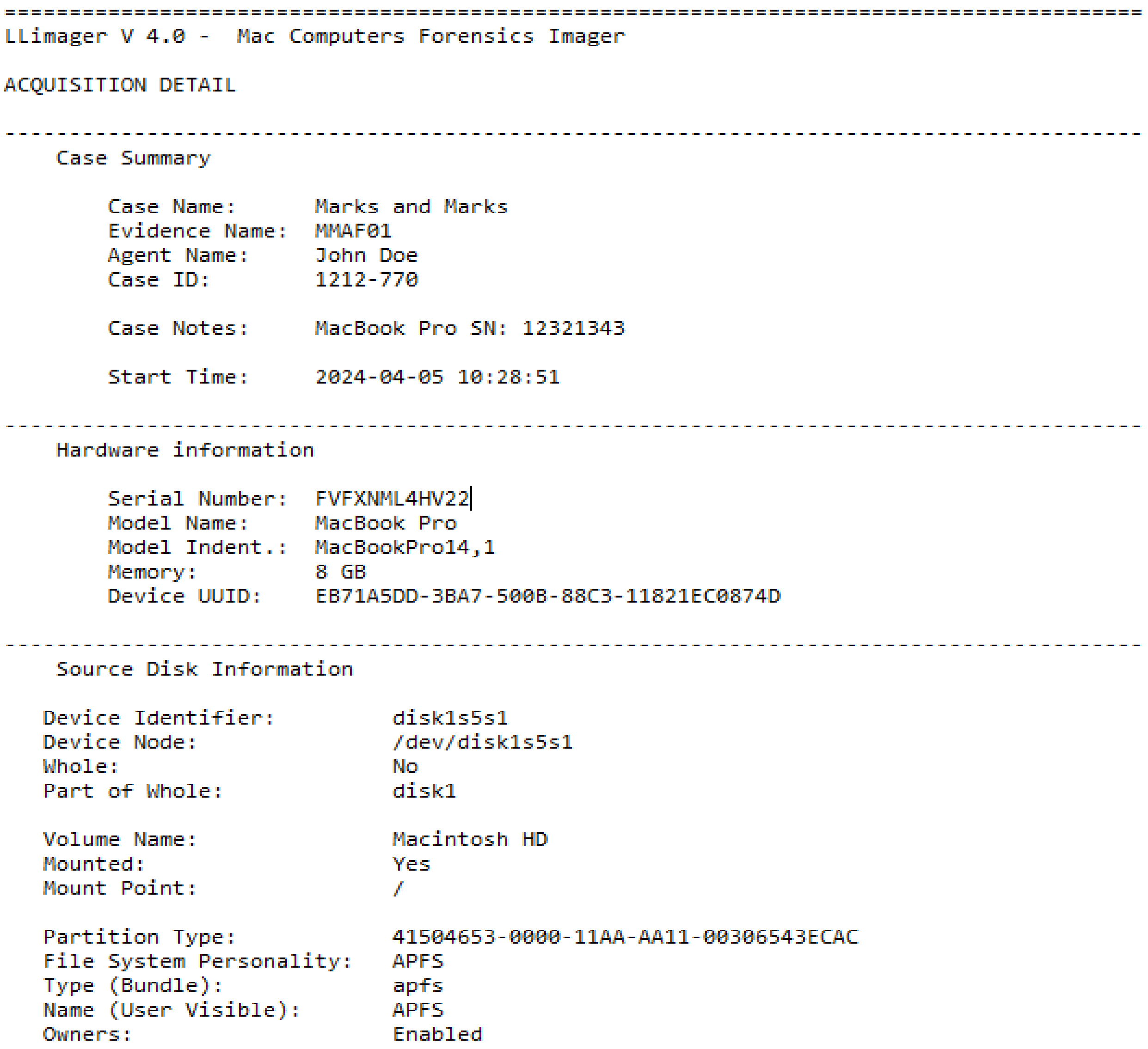
- efi-admin ☑
- [redacted] ☑
- [redacted] □

Selected Users:
efi-admin
[redacted]

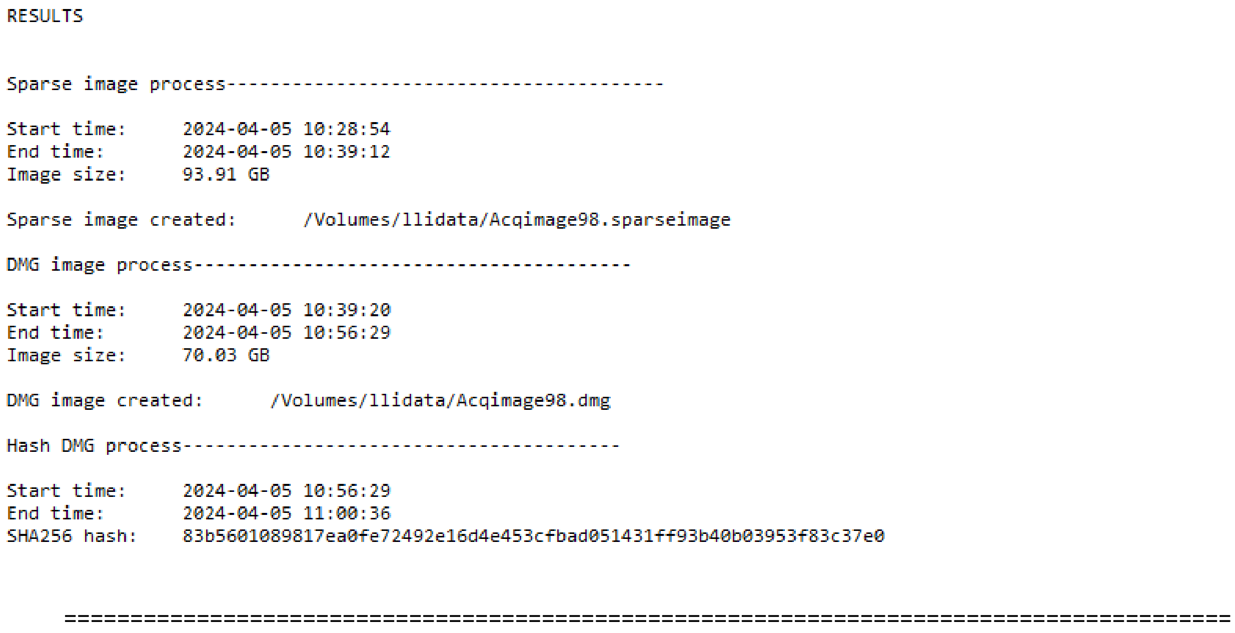
☑ Create a ZIP □ Create a DMG

Disk Acquisition Log Sample

The following is a sample of the disk acquisition log.



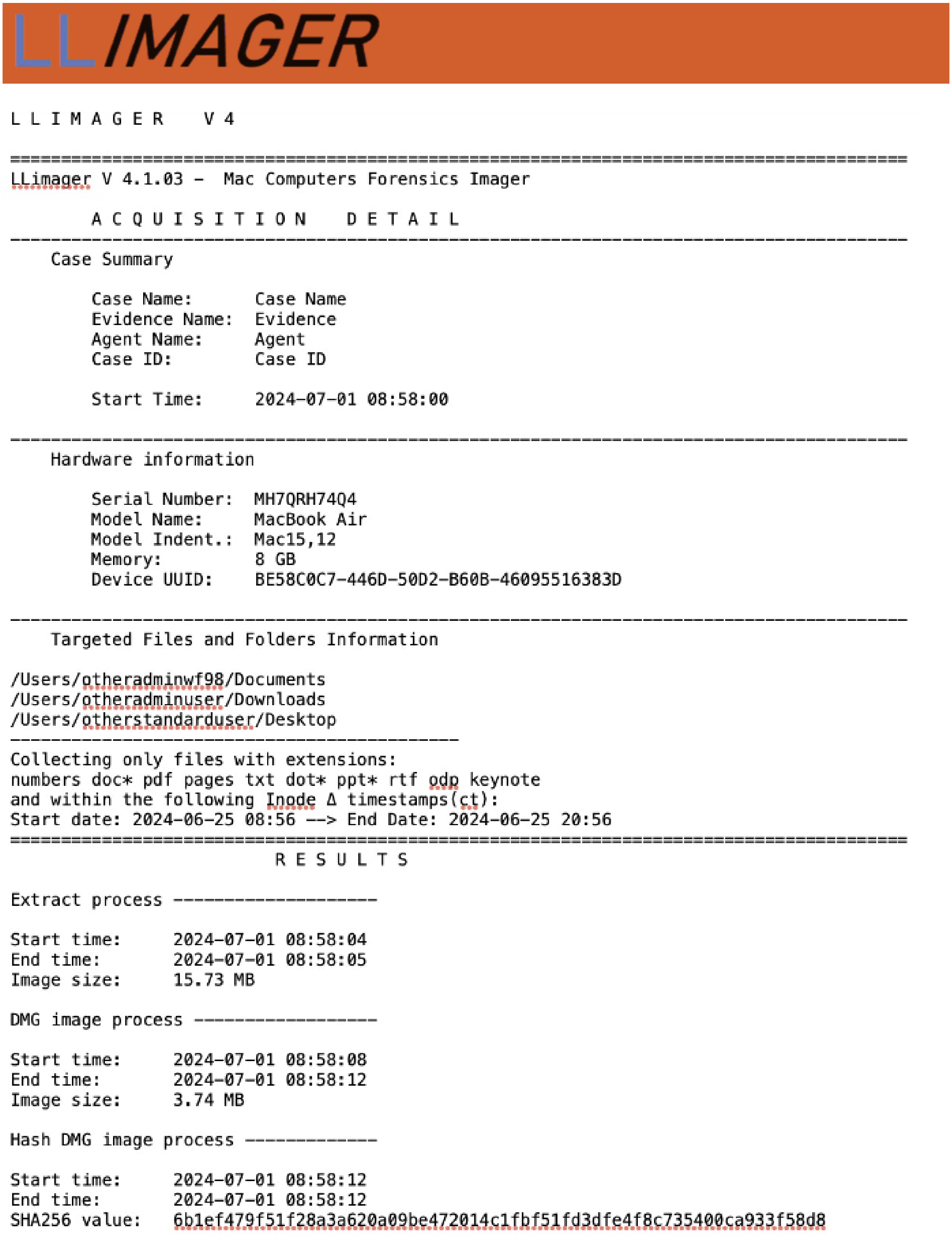
```
=========================================================================================
LLimager V 4.0 -  Mac Computers Forensics Imager

ACQUISITION DETAIL

-----------------------------------------------------------------------------------------
    Case Summary

        Case Name:       Marks and Marks
        Evidence Name:   MMAF01
        Agent Name:      John Doe
        Case ID:         1212-770

        Case Notes:      MacBook Pro SN: 12321343

        Start Time:      2024-04-05 10:28:51

-----------------------------------------------------------------------------------------
    Hardware information

        Serial Number:   FVFXNML4HV22
        Model Name:      MacBook Pro
        Model Indent.:   MacBookPro14,1
        Memory:          8 GB
        Device UUID:     EB71A5DD-3BA7-500B-88C3-11821EC0874D

-----------------------------------------------------------------------------------------
    Source Disk Information

   Device Identifier:          disk1s5s1
   Device Node:                /dev/disk1s5s1
   Whole:                      No
   Part of Whole:              disk1

   Volume Name:                Macintosh HD
   Mounted:                    Yes
   Mount Point:                /

   Partition Type:             41504653-0000-11AA-AA11-00306543ECAC
   File System Personality:    APFS
   Type (Bundle):              apfs
   Name (User Visible):        APFS
   Owners:                     Enabled
   OS Can Be Installed:      No
   Booter Disk:              disk1s2
   Recovery Disk:            disk1s3
   Media Type:               Generic
   Protocol:                 PCI-Express
   SMART Status:             Verified
   Volume UUID:              B8CE8BAA-4A75-42F3-BF8F-89412A84C937
   Disk / Partition UUID:    B8CE8BAA-4A75-42F3-BF8F-89412A84C937

   Disk Size:                121.0 GB (121018208256 Bytes) (exactly 236363688 512-Byte-Units)
   Device Block Size:        4096 Bytes

   Volume Used Space:        11.9 GB (11915608064 Bytes) (exactly 23272672 512-Byte-Units)
   Container Total Space:    121.0 GB (121018208256 Bytes) (exactly 236363688 512-Byte-Units)
   Container Free Space:     25.3 GB (25298644992 Bytes) (exactly 49411416 512-Byte-Units)
   Allocation Block Size:    4096 Bytes

   Media OS Use Only:        No
   Media Read-Only:          Yes
   Volume Read-Only:         Yes (read-only mount flag set)

   Device Location:          Internal
   Removable Media:          Fixed

   Solid State:              Yes
   Hardware AES Support:     No

   This disk is an APFS Volume Snapshot.  APFS Information:
   APFS Snapshot Name:       com.apple.os.update-A17B27811581529D33626973A757590AE0168469175C377BE4B1C7BDFDED1E84
   APFS Snapshot UUID:       B8CE8BAA-4A75-42F3-BF8F-89412A84C937
   APFS Container:           disk1
   APFS Physical Store:      disk0s2
   Fusion Drive:             No
   APFS Volume Group:        890F1145-BA72-4388-B74E-D0E7C79835AB
   EFI Driver In macOS:      2142140009000000
   Encrypted:                No
   FileVault:                Yes
   Sealed:                   Broken
   Locked:                   No

   APFS Snapshots are defined upon this APFS Volume.  Snapshot list:
   Snapshot UUID:            B8CE8BAA-4A75-42F3-BF8F-89412A84C937
   Name:                     com.apple.os.update-A17B27811581529D33626973A757590AE0168469175C377BE4B1C7BDFDED1E84
   XID:                      58627287
   Snapshot UUID:            D56BC470-A1BF-436F-8F17-D82DA8C35346
   Name:                     com.apple.os.update-MSUPrepareUpdate
   XID:                      59597868

========================================================================================
```



```
RESULTS


Sparse image process----------------------------------------

Start time:     2024-04-05 10:28:54
End time:       2024-04-05 10:39:12
Image size:     93.91 GB

Sparse image created:      /Volumes/llidata/Acqimage98.sparseimage

DMG image process----------------------------------------

Start time:     2024-04-05 10:39:20
End time:       2024-04-05 10:56:29
Image size:     70.03 GB

DMG image created:      /Volumes/llidata/Acqimage98.dmg

Hash DMG process----------------------------------------

Start time:     2024-04-05 10:56:29
End time:       2024-04-05 11:00:36
SHA256 hash:    83b5601089817ea0fe72492e16d4e453cfbad051431ff93b40b03953f83c37e0


     ===========================================================================================================
```

Targeted Acquisition Log Sample

The following is a sample of the targeted folders acquisition log.



LLIMAGER

```
L L I M A G E R   V 4

========================================================================================
LLimager V 4.1.03 -  Mac Computers Forensics Imager

        A C Q U I S I T I O N   D E T A I L
----------------------------------------------------------------------------------------
    Case Summary

        Case Name:      Case Name
        Evidence Name:  Evidence
        Agent Name:     Agent
        Case ID:        Case ID

        Start Time:     2024-07-01 08:58:00

----------------------------------------------------------------------------------------
    Hardware information

        Serial Number:  MH7QRH74Q4
        Model Name:     MacBook Air
        Model Indent.:  Mac15,12
        Memory:         8 GB
        Device UUID:    BE58C0C7-446D-50D2-B60B-46095516383D

----------------------------------------------------------------------------------------
    Targeted Files and Folders Information

/Users/otheradminwf98/Documents
/Users/otheradminuser/Downloads
/Users/otherstandarduser/Desktop
--------------------------------------------
Collecting only files with extensions:
numbers doc* pdf pages txt dot* ppt* rtf odp keynote
and within the following Inode Δ timestamps(ct):
Start date: 2024-06-25 08:56 --> End Date: 2024-06-25 20:56
========================================================================================
                          R E S U L T S

Extract process --------------------

Start time:     2024-07-01 08:58:04
End time:       2024-07-01 08:58:05
Image size:     15.73 MB

DMG image process ------------------

Start time:     2024-07-01 08:58:08
End time:       2024-07-01 08:58:12
Image size:     3.74 MB

Hash DMG image process -------------

Start time:     2024-07-01 08:58:12
End time:       2024-07-01 08:58:12
SHA256 value:   6b1ef479f51f28a3a620a09be472014c1fbf51fd3dfe4f8c735400ca933f58d8
```

Changelog

July 20, 2023: Commercial Version 3.5 (beta core)

September 8, 2023: Commercial Version 3.7: Major cosmetic

September 15, 2023: Commercial Version 3.7.1: Minor updates to license key processing, and packaging executables into DMGs

October 2, 2023: Commercial Version 3.7.2: Added new feature to create logical image of targeted folders.

November 14, 2023: Manual documentation update regarding resolution of LLimager being damaged and can't open.

November 17, 2023: Update to EULA

December 8, 2023: Commercial Version 3.8: Major update

- Transparent management of System sleeping time.
- Removed the required input requesting confirmation to erase the sparse after selecting to run in Unattended mode.
- Updated messages during the process to make warning messages more notable.
- Updated the imaging of targeted folders.
- Changed the process to save all targeted folders into one DMG.
- Enhanced error trapping.
- Updates to the acquisition log file.
- Other minor changes to enhance performance.
- Manual documentation update regarding resolution of LLimager_M1 being damaged and can't open.

April 8, 2024: Complete rewrite to GUI using in Swift.

July 1, 2024: 4.1.03: Major update

- Granular targeted imaging
- Enhanced performance
- Improved error trapping and reporting
- Updated acquisition log

July 10, 2024: Bug fix to correct failed acquisitions due to copying to destination folders created by the user with a space in the name.

September 3, 2024: Updates to the trial version which includes watermarking of image. Added option to collect sysdiagnose.

January 10, 2025: 5.01: Major update

- Copy images to Cloud storage

- Collect User Profiles
- Improved error trapping and reporting
- Updated acquisition log

March 13, 2025: 5.1: Minor update

- Added Time Machine-based Imaging
- Improved error trapping and reporting
- Updated acquisition log

End User License Agreement

LL*IMAGER*

2023-2025, e-Forensics Inc.

This End User License Agreement (EULA) is a legal agreement between you (either an individual or an entity) and e-Forensics for the software product named LL*IMAGER* (the "Software"). By installing, copying, or using the Software, you agree to be bound by the terms of this EULA.

1**. Grant of License**

e-Forensics grants you a non-exclusive, non-transferable, limited license to use the Software for your own internal business purposes. You may not modify, adapt, or translate the Software. You may not reverse engineer, decompile, or disassemble the Software.

2. Subscription

The Software is licensed on an annual subscription basis. Your subscription will automatically expire at the end of the term, and it must be renewed for continued use.

3. Fees

Contact e-Forensics for the annual subscription fee.

4. **Term and Termination**

This EULA will remain in effect until terminated by either party. You may terminate this EULA at any time by uninstalling the Software and destroying all copies of the Software. e-Forensics may terminate this EULA if you fail to comply with any of the terms of this EULA.

5**. Ownership**

The Software is owned by e-Forensics and is protected by copyright law. You do not acquire any ownership rights to the Software under this EULA.

6. **Restrictions**

You may not:

- Rent, lease, or sub-license the Software;

- Sell, distribute, or transfer the Software to any third party;
- Use the Software for commercial purposes other than digital forensics;
- Use the Software in a way that violates any applicable law or regulation.

7. Disclaimer of Warranties

The Software is provided "as is" and e-Forensics makes no warranties, express or implied, about the Software. e-Forensics does not guarantee that the Software will be error-free or that it will meet your requirements.

We are committed to providing high-quality hardware products to our customers. However, we do not offer refunds or returns on hardware/software purchases. All hardware products are covered by a 1-year warranty. This warranty covers replacement and ground shipping. If you experience any problems with your hardware, please contact us for a warranty service.

8. Limitation of Liability

In no event will e-Forensics be liable to you for any damages, including direct, indirect, incidental, consequential, or special damages, arising out of or in connection with this EULA or the use of the Software, even if e-Forensics has been advised of the possibility of such damages.

9. Governing Law

This EULA will be governed by and construed in accordance with the laws of the State of Florida, without regard to its conflict of laws provisions.

10. Entire Agreement

This EULA constitutes the entire agreement between you and e-Forensics regarding the Software and supersedes all prior or contemporaneous communications, representations, or agreements, whether oral or written.

11. Severability

If any provision of this EULA is held to be invalid or unenforceable, such provision will be struck from this EULA and the remaining provisions will remain in full force and effect.

12. Waiver

No waiver of any provision of this EULA will be effective unless in writing and signed by both parties.

13. Headings

The headings in this EULA are for convenience only and will not affect its interpretation.

14. Counterparts

This EULA may be executed in one or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

15. Language

This EULA is in the English language and will not be translated into any other language.

Contact Information

For questions or further information about LL*IMAGER* or this License, please contact e-Forensics Inc. at:

e-Forensics Inc.

support@e-forensicsinc.com

sales@e-forensicsinc.com

Support & Feedback

For commercial licensed users, please send all support inquiries and feedback to support@e-forensicsinc.com, and include registration e-mail address and product serial number.

Acknowledgements

A special thanks to the key contributors: Larry Britton, Lautaro Barrera, Jesus F. Pena and Jannette Perez