LL*IMAGER* *version 3.8*

User Manual

Contents

Preface

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 all synthesized APFS volumes and targeted folders for logical images.

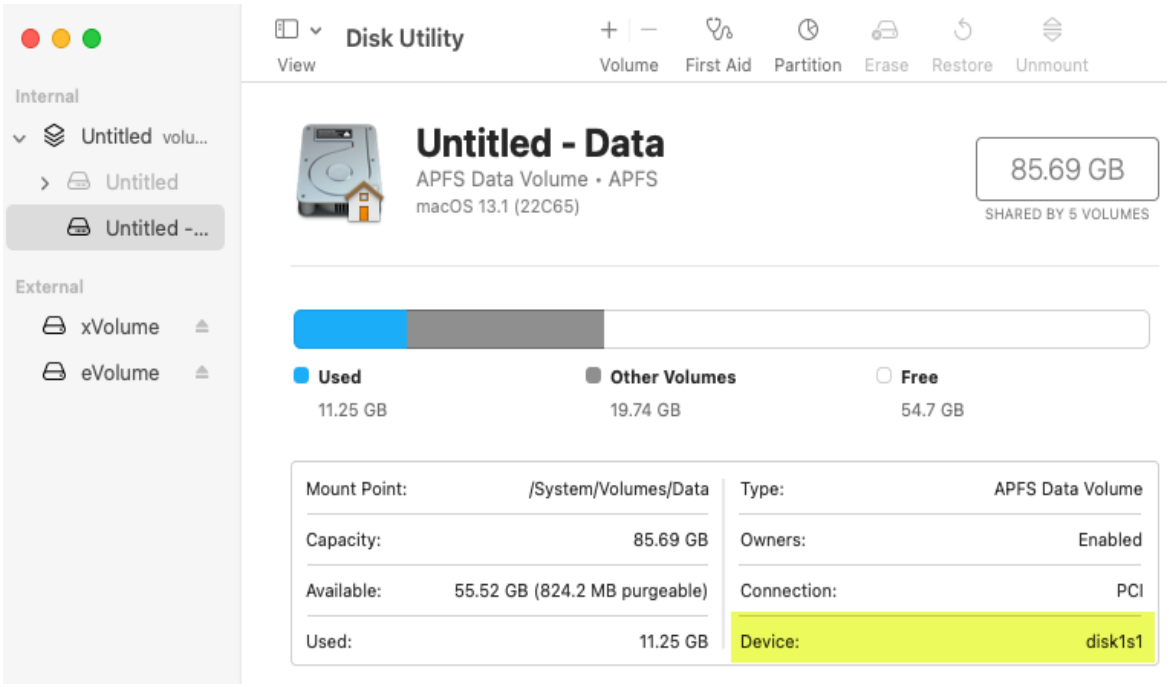
LL*IMAGER* is user-friendly and easy enough for entry level digital forensics examiners. The application leverages built-in Mac utilities, providing a versatile solution compatible with a wide range of macOS versions, both past and present. This ensures the tool remains functional across diverse system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

Terminology

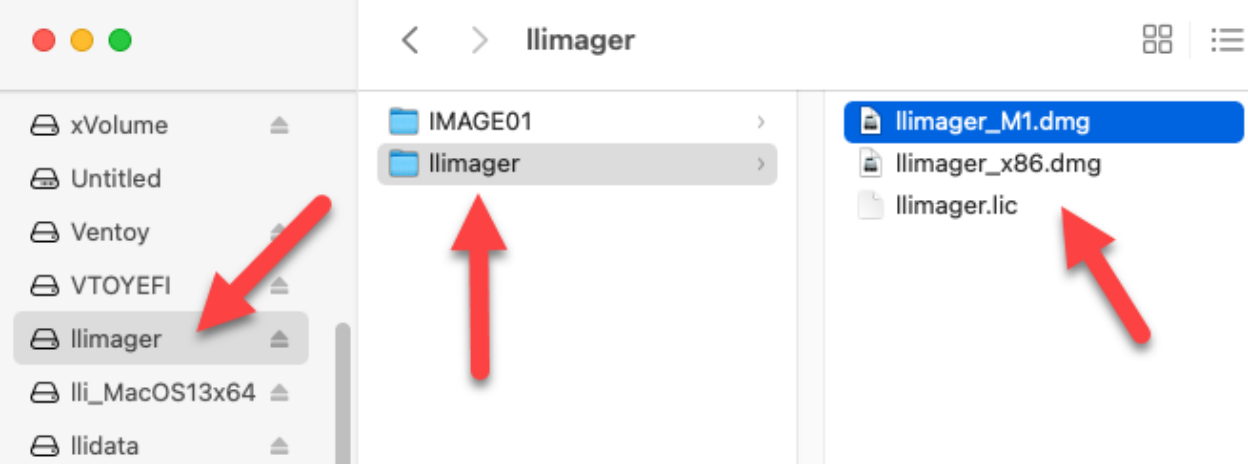
Sparse image file: a native macOS image format that is dynamic and used within the Mac environment. The file grows as data is added to the image, taking up only as much disk space as stored in it.

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.



USB Label / Name: This is the name of a mounted partition, physical or virtual. It can be located using Finder, on the left side of the window, as illustrated in the following picture. 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 Intel executable is "LLimager_x86" and the M1/M2/M3 is "LLimager_m1".

Supported Mac Hardware

Live Image (booted from internal disk)

LL*IMAGER* works with Intel-based Macs and new hardware M1/M2/M3.

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 within an open 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.

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 will provide the option to encrypt the DMG, however, you should be aware that the encrypted DMG is not currently supported by many forensics' applications, and therefore require conversion to unencrypted DMG before processing in the unsupported forensics apps.

[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).

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, …).

Be aware of messages starting with "ATTENTION", these are messages that need intervention to correct data provided, or a decision you need to make before continuing.

Requirements

- **A local admin password** for the Mac computer to be imaged.
- **Terminal 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 executables (M1: LLimger_M1 and Intel: LLimager_x86) and the required license file (llimager.lic).
- **Temporary Image USB disk**: 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 the size of the source disk 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, if the separate Temporary Image USB disk is used, each should have free space equal to at least the size of the source device.
    - **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

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

Getting Started with LL*IMAGER*

Refer to the pertinent scenario below.

From LL*IMAGER* USB SSD

- Login as an admin into the source Mac computer and connect the LL*IMAGER* USB SSD drive that contains the copy of the imager (LLimager_M1.dmg and LLimager_x86.dmg, 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 Terminal, and Disk Utility. (Finder: Applications > Utilities > Terminal | Disk Utility)

- On the LL*IMAGER* USB SSD, navigate to /llimager and double click on "LLimager_M1.dmg" (for Silicon macs), and then double click on the executable, "LLimager_M1". For Intel macs, use "LLimager_x86".

- Proceed to image.

From User-Supplied USB SSD/HDD

- Login as an admin into any Mac computer other than the source.

- Prepare your USB SSD by:
    - Insert SSD into the mac and create a volume named "llimager" (case sensitive)
    - Create a folder named "llimager", which should result in /Volumes/llimager/llimager
    - Download the most current version of LL*IMAGER* from "llimager.com/download" and unzip into "/Volumes/llimager/llimager"
    - Copy the purchased license file (llimager.lic) into "/Volumes/llimager/llimager".
    - **To clean the extended attributes created for the downloaded file, run the command: xattr -cr /Volumes/llimager/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 source Mac computer.

- Connect the user-supplied USB SSD drive that contains the copy of the imager (LLimager_M1.dmg and LLimager_x86.dmg, 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 Terminal, and Disk Utility. (Finder: Applications > Utilities > Terminal | Disk Utility)

- On your USB SSD, navigate to /llimager and doubleclick on “LLimager_M1.dmg” (for Silicon macs), and then double click on the executable, “LLimager_M1”. For Intel macs, use “LLimager_x86”.

  WARNING: if you receive an error message, “"LLimager_M1" is damaged and can't be opened.”:

  This is an erroneous and misleading error that generally occurs when the application is downloaded from the web on a Mac computer using certain browser (Safari, Firefox, Edge), Chrome works fine; the issue is generated by an attribute (quarantine) that is assigned to the downloaded file and propagated to its children. This will occur even when updating to the new versions. Downloading on the Mac with Chrome or updating using a Windows computer will not produce the issue.

  To resolve, go to Terminal and enter the following command to clear out the extended attributes on the files within "/Volumes/llimager/llimager":

  ```
  xattr -cr /Volumes/llimager/llimager
  ```

- Proceed to image.

From Trial Versions

- Login as an admin into any Mac computer other than the source.

- 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 the mac and create a volume named “llimager” (case sensitive)
  - Create a folder named “llimager”, which should result in /Volumes/llimager/llimager
  - Download the most current version of LL*IMAGER* from “llimager.com/download” and unzip into “/Volumes/llimager/llimager”
  - Copy the trial license file (llimager.lic) into “/Volumes/llimager/llimager”.
  - **To clean the extended attributes created for the downloaded file, run the command: xattr -cr /Volumes/llimager/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 source Mac computer.

- Connect your USB Flash/SSD drive that contains the trial copy of the imager (LLimager_M1.dmg and LLimager_x86.dmg, 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 Terminal, and Disk Utility. (Finder: Applications > Utilities > Terminal | Disk Utility)

- On your USB Flash/SSD, navigate to /llimager and double click on “LLimager_M1.dmg” (for Silicon macs), and then double click on the executable, “LLimager_M1”. For Intel macs, use “LLimager_x86”.

- WARNING: if you receive an error message, “"LLimager_M1" is damaged and can't be opened.”:

  This is an erroneous and misleading error that generally occurs when the application is downloaded from the web on a Mac computer using certain browser (Safari, Firefox, Edge), Chrome works fine; the issue is generated by an attribute (quarantine) that is assigned to the downloaded file and propagated to its children. This will occur even when updating to the new versions. Downloading on the Mac with Chrome or updating using a Windows computer will not produce the issue.

  To resolve, go to Terminal and enter the following command to clear out the extended attributes on the files within "/Volumes/llimager/llimager":

  ```
  xattr -cr /Volumes/llimager/llimager
  ```

- 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.

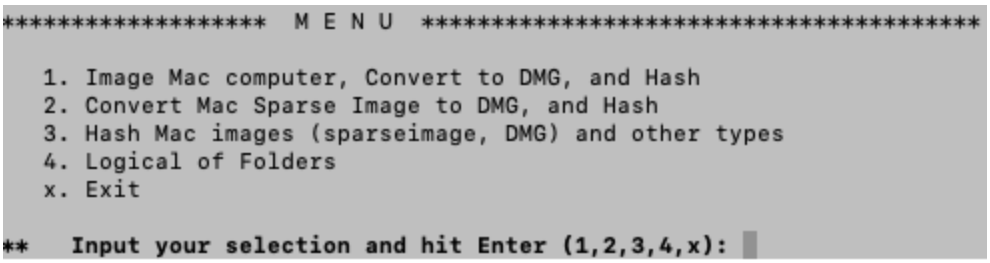
Temporarily disable Gatekeeper and try running the app again. Once the imaging is completed, exit the application, and re-enable Gatekeeper. To disable, or re-enable Gatekeeper, open a Terminal window, and use one of the following commands accordingly to disable/enable, an admin password is required:

```
sudo spctl --master-disable

sudo spctl --master-enable
```

LL*IMAGER* Menu

The application starts by displaying a summary of the usage and recommendations, and by requesting the password for an account with admin privilege. The password will be used throughout the usage of the app in any of the task’s selection where it is required. The app will exit if the password is empty or incorrect.

The Main Menu:



Option 1. This option allows the entire process of imaging the computer's hard disk, saving the image to a Mac sparse image container; conversion of the image to a compress DMG file, and calculating the hash value of the DMG file. During the process, it will prompt to select whether a fully automatic process is desired, or to confirm the execution of each of the processes.

Option 2. This option allows the process of converting a sparse image file to a compress DMG file, and to calculate the hash value of the DMG file.

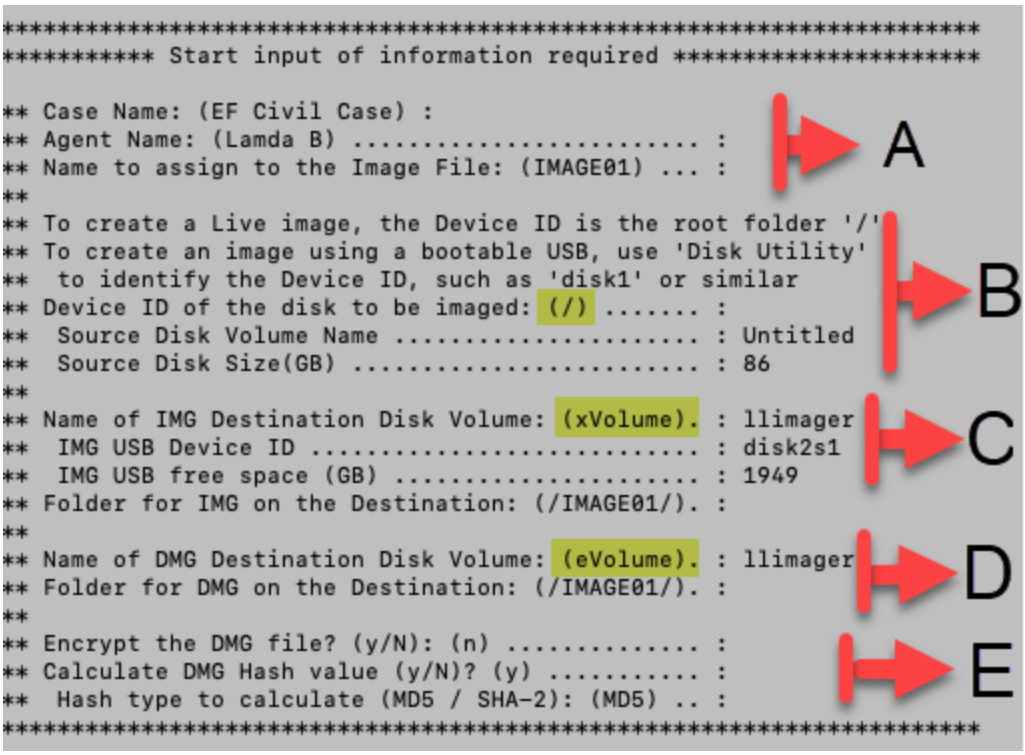
Option 3. This option allows you to calculate the hash value of the sparse image or the DMG file.

Option 4. This option allows the imaging of targeted 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.

Option x. This option will exit the application.

Menu Option 1 (imaging full process)

Here you are required to identify and input information about the device to be imaged, and the destination USBs where the image will be saved (highlighted in yellow in the picture below). Additionally, you need to provide information related to the case, name of the image and folders to use to save the file, choose to encrypt the image or not, to hash, type of hash. The following picture shows the texts requesting information, line by line.



There is a blank line between the sections related to each device and other information requested. See the below description of each section.

A – Related to the case. Name of case, agent, and image.

B – Related to the *device to be imaged*. Requires the input 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.

C – Related to the *destination of the sparse image* file. Requires the input of the USB label (partition) to be used to save the sparse image file, and the name of a folder/path to save the files. The app will verify the device and display the device ID and the free space.

D – Related to the *destination of the DMG* file. Requires the input of the USB label to be used to save the DMG file, and the name of a folder/path to save the files. The app will verify the device and display the device ID and the free space, if the disk is different from the sparse image's disk.

E – Related to *encrypting and hashing of the DMG* file. You need to specify if the DMG will be encrypted, and, if it should be hashed then specify the type of hash.

Note that by leaving the input empty and hitting Enter will accept the default value shown within the parenthesis ().

After completing the inputs, a summary of the information provided, by typing or by selecting the default, will be displayed. See the following picture:

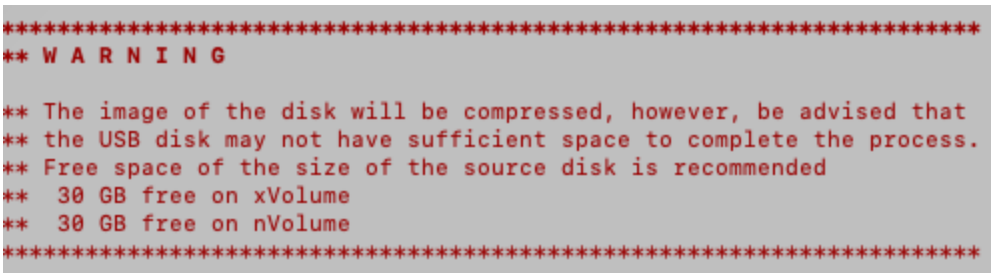
```
****************** Data that was provided *******************************

** Case Name ............... : EF Civil Case
** Agent Name .............. : Lamda B
** Image File Name ........ : IMAGE01
**
** Source Device ID ....... : /
**  Source Volume Name .... : [ Untitled ]
**  Source Disk Size (GB) . : [ 86 ]
**
** IMG USB Disk Volume Name : xVolume
**  IMG USB Device ID ..... : [   ]
**  IMG USB Free Space (GB) : [   ]
** IMG folder on USB Disk . : /IMAGE01/
**
** DMG USB Disk Volume Name : eVolume
**  DMG USB Device ID ..... : [   ]
**  DMG USB Free Space (GB) : [   ]
** DMG folder on USB Disk . : /IMAGE01/
**
** Encrypt DMG image ...... : n
** Calculate Hash ......... : y
**  Hash Type .............. : MD5

*************************************************************************
```

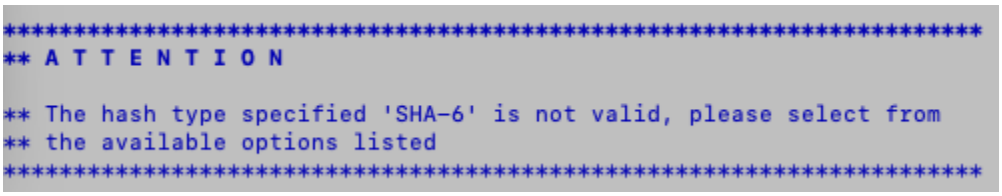
There will be a validation of all the information, and you will be notified of any error, missing devices specified, warning of low disk space, or if the image already exists. The following are examples of the messages.

```
*************************************************************************
** A T T E N T I O N

** The Image Destination volume "xVolume" is not available, please
** make sure the spelling is correct, and that the disk is connected
*************************************************************************
```

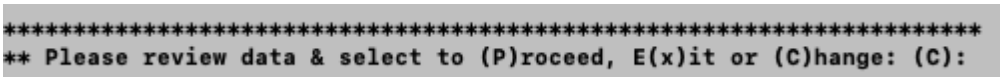
```
*************************************************************************
** A T T E N T I O N

** Image files with the name IMAGE01 already exist, please
**  - Delete the existing files from the USB and try again
**     /Volumes/llimager/IMAGE01/IMAGE01.sparseimage
**     /Volumes/llimager/IMAGE01/IMAGE01.dmg
**  - or enter a different name for the image
*************************************************************************
```

```
*************************************************************************
** W A R N I N G

** The image of the disk will be compressed, however, be advised that
** the USB disk may not have sufficient space to complete the process.
** Free space twice the size of the source disk is recommended
*************************************************************************
```



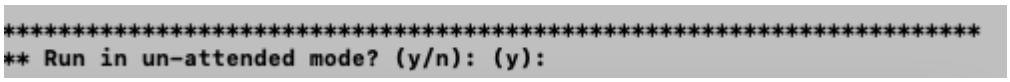


After validating and accepting the information, the app presents the options to proceed, change any of the information provided or to exit.



Selecting “P” will continue to collect data from the computer.

Next, select to run in attended or un-attended mode.



- By selecting “y”, un-attended mode, all processes will be executed automatically one after the other.
- By selecting “n”, attended mode, you will be prompted to decide on running each process, a) create image, b) convert to DMG, and c) hash the DMG.

After confirming this mode, the imaging process will start.

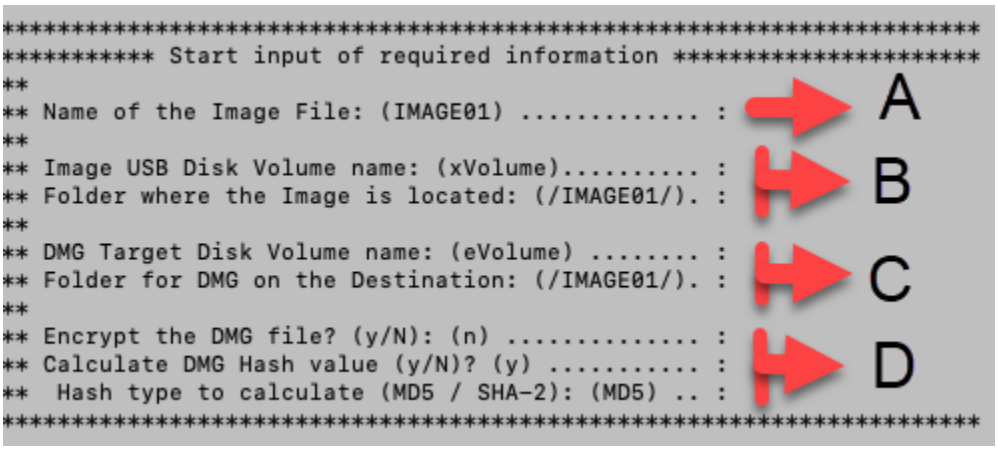
There are power saving settings on the computer that may interfere and break the imaging process, these settings are temporarily disabled during the image.

There will be messages informing you of what is being processed.

- Imaging of the disk
- Converting to DMG
- Calculating hash of the DMG
- Saving of the acquisition log
- Completion

Menu Option 2 (DMG converter)

Here you are required to input the image name to identify and input information about the image location, identify and input information about the DMG file destination. Additionally, you need to choose to encrypt the DMG file or not, and hash type if hash is selected. The following picture shows the texts requesting information, line by line.



There is a blank line between the sections related to each device and other information requested. See the below description of each section.

A – Specify the name of the image.

B – Related to the *location of the sparse image* file. Requires the input of the USB label (partition) and the folder/path where the sparse image file is located. The app will verify the information and display the free space of the USB disk, and the size of the sparse image file.

C – Related to the *destination of the DMG* file. Requires the input of the USB label and the folder/path to use to save the files. The app will verify the USB disk and display the free space if the disk is different from the sparse image's disk.

D – Related to *encrypting and hashing of the DMG* file. You need to specify if the DMG will be encrypted, and, if it should be hashed then specify the type of hash.

Note that by leaving the input empty and hitting Enter will accept the default value shown within the parenthesis ().

After completing the inputs, a summary of the information provided, by typing or by selecting the default, will be displayed. See below:

```
***************** Data that was provided ****************************

** Image File Name ........ : IMAGE01
** IMG USB Disk Volume Name : xVolume
**  IMG USB Free Space (GB) : [  ]
** IMG folder on USB Disk . : /IMAGE01/
**
** DMG USB Disk Volume Name : eVolume
**  DMG USB Free Space (GB) : [  ]
** DMG folder on USB Disk . : /IMAGE01/
**
** Encrypt DMG image ...... : n
** Calculate Hash ......... : y
**  Hash Type .............. : MD5

*********************************************************************
```

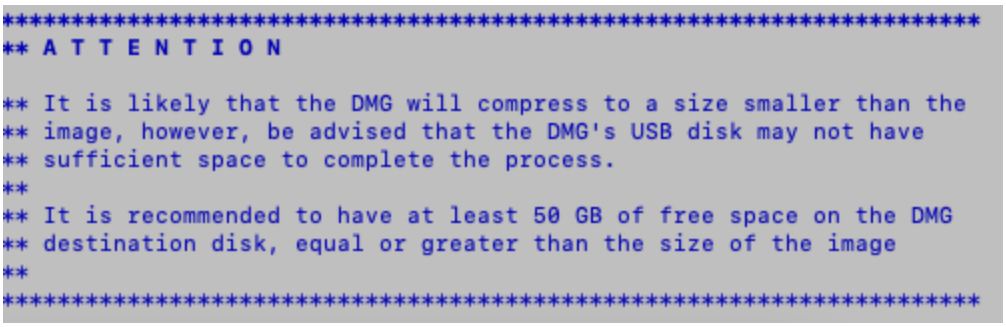
There will be a validation of all the information, and you will be notified of any error, missing devices specified, warning of low disk space, or if the image already exists. The following are examples of the messages.

```
*********************************************************************
** A T T E N T I O N

** Image file IMAGE01.sparseimage was not located, please
**  Try again after updating the following:
**   The image USB Volume name: xVolume
**   The image USB folder: /IMAGE01/
**   The Image name IMAGE01
*********************************************************************
```

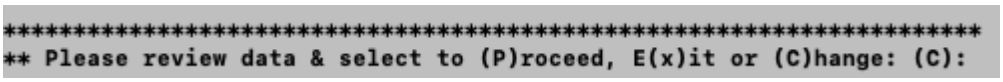
```
*********************************************************************
** A T T E N T I O N

** DMG file IMAGE01.dmg already exist, please
**  - Delete the existing files from the USB and try again
**  - or select a different folder to save the DMG
*********************************************************************
```

```
*********************************************************************
** A T T E N T I O N

** DMG's USB Volume "eVolume" does not exist, please verify that
** the volume is mounted and is spelled correctly
*********************************************************************
```

```
*********************************************************************
** A T T E N T I O N

** The hash selected "SHA6" is not valid, please select from
** the available options listed
*********************************************************************
```

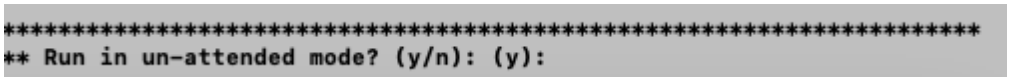


After validating and accepting the information, the app presents the options to proceed, change any of the information provided or to exit.



Selecting “P” will move forward with the process.

Next, select to run in attended or un-attended mode.



- By selecting “y”, un-attended mode, all processes will be executed automatically one after the other.
- By selecting “n”, attended mode, you will be prompted to decide on running each process, a) convert to DMG, and b) hash the DMG.

After confirming this mode, conversion of the sparse image to DMG will start.

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

There will be messages informing you of what is being processed.

- Converting to DMG
- Calculating hash of the DMG
- Saving of the image log and DMG conversion
- Completion

Menu Option 3 (Hashing)

This option is used to calculate the hash of a file, be it sparse image, DMG or any other type.

Following is the menu of hashing options.

```
*************************************************************************
*********** Start input of required information **********************
**
**   1. Mac Sparse Image file
**   2. Mac DMG Image file
**   3. Other file type (full name required)
**
**  Select the file type to hash and hit Enter (1,2,3): (1) . : 1
```

The hashing option allows you to select from three different types of files to hash, sparse image, DMG or any other type. Hashing options 1 and 2 are tied to the image management procedure from the main Menu Options 1 and 2. The name of the image is required, but the file extension is assigned based on the option selected. The input information required for both options is the same.

The hashing option 3 was included as an addition to be able to hash any one file; the input information required is like those of options 1 and 2, with the difference that the full file name, including the file extension, needs to be provided.

The following picture shows the texts requesting information, line by line.

```
**
*************************************************************************
**  Name of the Image File: (IMAGE01) ......... :
**  File's Disk Volume name: (xVolume)......... :
**  File's Folder name: (/IMAGE01/)............ :
**  Hash type to calculate (MD5 / SHA-2): (MD5) :
```

Information requested:

- Name of the image file to be hashed.
- Name of the volume where the file is located.
- The folder / path of the file.
- Type of hash needed.

Note that by leaving the input empty and hitting Enter will accept the default value shown within the parenthesis ().

After completing the inputs, a summary of the information provided, by typing or by selecting the default, will be displayed. See the following picture:

Hashing option 1 and 2 (file extension omission)

```
***************** Data that was provided ****************************

**  File Type (1,2,3) ..... :  1
**  Image file name ........ :  IMAGE01
**  File's Disk Volume Name. :  xVolume
**  File's Folder name ..... :  /IMAGE01/
**  Hash Type to calculate.. :  MD5

*********************************************************************
```

Hashing option 3 (file extension required)

```
***************** Data that was provided ****************************

**  File Type (1,2,3) ..... :  3
**  File to hash name ..... :  IMAGE01.img
**  File's Disk Volume Name. :  xVolume
**  File's Folder name ..... :  /IMAGE01/
**  Hash Type to calculate.. :  MD5

*********************************************************************
```

There will be a validation of the information, and you will be notified of any error, missing devices specified, or if the image file does not exist. The following are examples of the messages.

```
*********************************************************************
** A T T E N T I O N

** File to hash IMAGE01.sparseimage was not located, please
** Try again after updating the following:
**   The File's disk Volume name: xVolume
**   The File's folder name: /IMAGE01/
**   The file to hash name IMAGE01.sparseimage
*********************************************************************
```

```
*********************************************************************
** A T T E N T I O N

** The hash selected "SHA6" is not valid, please select from
** the available options listed
*********************************************************************
```

After validating and accepting the information, the app presents the options to proceed, change any of the information provided or to exit.

```
*********************************************************************
** Please review data & select to (P)roceed, E(x)it or (C)hange: (C):
```

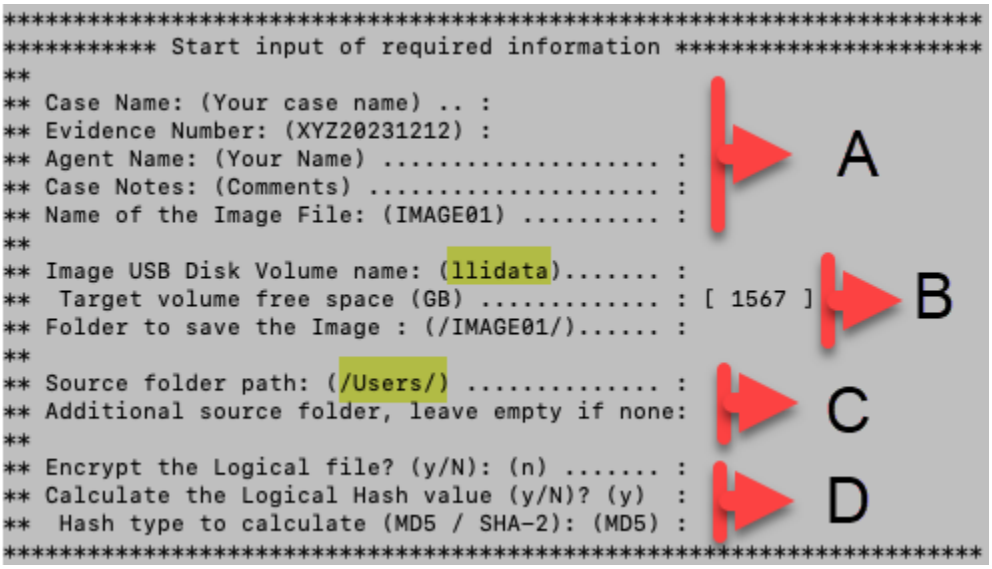
Selecting “P” will move forward and start calculating the hash.

There will be messages informing you of what is being processed.

- Calculating hash of the DMG
- Saving log of the image name and hash
- Completion

Menu Option 4 (Logical of Folders)

Here you are required to identify and input the path of the targeted folders to be imaged, and the destination volume where the image will be saved (highlighted in yellow in the picture below). Additionally, you need to provide information related to the case, name of the image and folder to use to save the logical image, choose to encrypt the image or not, to hash, type of hash. The following picture shows the texts requesting information, line by line.



See the below description of each section of the information input shown above.

A – Related to the case. Name of case, notes, agent, and image name.

B – Related to the *destination of the logical image* file. Requires the input of the volume label (partition) to be used to save the logical image file, and the name of a folder/path to save the files. The app will verify the device and display the free space.

C – Related to the *folders to be imaged*. Requires the input of the folder/path to be imaged. By default, the "/Users" folder is selected, hit Enter to accept, or input a different path. The app will prompt for additional folder, input another path to be imaged, or leave empty and hit Enter to complete the input of folders to be imaged.

D – Related to *encrypting and hashing of the DMG* file. You need to specify if the Logical image will be encrypted, and, if it should be hashed, then specify the type of hash.

Note that by leaving the input empty and hitting Enter will accept the default value shown within the parenthesis (). Very important also, path and name are case sensitive so be careful to enter all correctly.

After completing the inputs, a summary of the information provided, by typing or by selecting the default, will be displayed. See the following picture:

```
***************** Data that was provided ******************************

** Case Name ................. : Your case name
** Evidence Number .......... : XYZ20231212
** Agent Name ................ : Your Name
** Case Notes ................ : Comments
** Logical File Name ........ : IMAGE01

** Logical target Volume Name : llidata
**  Target Free Space (GB) .. : [ 1567 ]
** Logical target folder .... : /IMAGE01/
**
** Source folders for Logical : /Users/
**
** Encrypt Logical image? ... : n
** Calculate Hash value? .... : y
**  Hash Type ................ : MD5

***********************************************************************
```

There will be a validation of all the information, and you will be notified of any error, missing devices specified, or if the image already exists. The following are examples of the messages.

```
***********************************************************************
** A T T E N T I O N

** File IMAGE01_0.dmg already exist, please
**  - Delete the existing files from the Volume and try again
**  - or select a different folder to save the DMG
***********************************************************************
```

```
***********************************************************************
** A T T E N T I O N

** The following source folder does not exist, please verify
** /application
***********************************************************************
```

After validating and accepting the information, the app presents the options to proceed, change any of the information provided or to exit.

```
***********************************************************************
** Please review data & select to (P)roceed, E(x)it or (C)hange: (C): p
```

Selecting “P” will continue to collect data from the computer.

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

There will be messages informing you of what is being processed.

- Creating the Logical image
- Calculating hash of the DMG
- Saving of the acquisition log
- Completion

Acquisition Log Sample

The following is a sample of the disk acquisition log.

```
************************************************************************
LLIMAGER v3.8
  Mac Computers Forensic Imager
  Acquisition log details
************************************************************************
Case Summary:

  Case_Name:     EF Civil Case
  Agent_Name:    Lamda B
  OSversion:     macOS 14.1.1
  Serial_Number: 47RHKGYWRJ
  Model_Number:  Mac14,2
  Start_time:    Tue Dec  5 11:17:04 EST 2023

************************************************************************
Hardware:

    Hardware Overview:

      Model Name: MacBook Air
      Model Identifier: Mac14,2
      Model Number: MLY33LL/A
      Chip: Apple M2
      Total Number of Cores: 8 (4 performance and 4 efficiency)
      Memory: 8 GB
      System Firmware Version: 10151.41.12
      OS Loader Version: 10151.41.12
      Serial Number (system): 47RHKGYWRJ
      Hardware UUID: 130E90CB-E98C-56F4-A251-C55BBEC24E3D
      Provisioning UDID: 00008112-000471DA21DBC01E
      Activation Lock Status: Disabled


************************************************************************
Source Disk Information

   Device Identifier:        disk7s1
   Device Node:              /dev/disk7s1
   Whole:                    No
   Part of Whole:            disk7

   Volume Name:              Macintosh HD
   Mounted:                  No

   Partition Type:           41504653-0000-11AA-AA11-00306543ECAC
   File System Personality:  APFS
   Type (Bundle):            apfs
   Name (User Visible):      APFS
   Owners:                   Disabled

   OS Can Be Installed:      No
   Booter Disk:              disk7s3
   Recovery Disk:            disk7s4
   Media Type:               Generic
   Protocol:                 Disk Image
```

```
   SMART Status:              Not Supported
   Volume UUID:               8ED3C213-E76F-4003-BE27-D4EEC5CF17F0
   Disk / Partition UUID:     8ED3C213-E76F-4003-BE27-D4EEC5CF17F0

   Disk Size:                  263.9 GB (263930732544 Bytes) (exactly 515489712 512-Byte-
Units)
   Device Block Size:         4096 Bytes

   Volume Used Space:         9.9 GB (9896615936 Bytes) (exactly 19329328 512-Byte-Units)
   Container Total Space:      263.9 GB (263930732544 Bytes) (exactly 515489712 512-Byte-
Units)
   Container Free Space:       241.1 GB (241116286976 Bytes) (exactly 470930248 512-Byte-
Units)

   Media OS Use Only:         No
   Media Read-Only:           No
   Volume Read-Only:          Not applicable (not mounted)

   Device Location:           External
   Removable Media:           Removable
   Media Removal:             Software-Activated

   Solid State:               Info not available

   This disk is an APFS Volume.  APFS Information:
   APFS Container:            disk7
   APFS Physical Store:       disk6s2
   Fusion Drive:              No
   APFS Volume Group:         E53044FB-BEE1-439A-9720-377826409FEB
   Encrypted:                 No
   FileVault:                 No
   Sealed:                    Broken
   Locked:                    No


**********************************************************************
Image information:

Sparse Image Name: EFI01_FULL.sparseimage
Sparse Image Start Time: Tue Dec  5 11:17:09 EST 2023
Sparse Image End Time..: Tue Dec  5 11:24:15 EST 2023

DMG Image Name: EFI01_FULL.dmg
DMG Image Start Time: Tue Dec  5 11:24:17 EST 2023
DMG Image End Time..: Tue Dec  5 11:31:28 EST 2023

EFI01_FULL.dmg MD5 Hash: b6acf349e75bd1eff59b1af14abc7aea
Hashing Start Time..: Tue Dec  5 11:31:28 EST 2023
Hashing End Time....: Tue Dec  5 11:33:42 EST 2023


**********************************************************************
Completion Information:

Process completed on: Tue Dec  5 11:33:42 EST 2023

**********************************************************************
```

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

```
************************************************************************
LLIMAGER v3.8
  Mac Computers Forensic Imager
  Logical Image of Folders
  Acquisition log details
************************************************************************
Case Summary:

  Case_Name:     Your case name
  Agent_Name:    Your Name
  OSversion:     macOS 14.1.1
  Serial_Number: 47RHKGYWRJ
  Model_Number:  Mac14,2
  Start_time:    Tue Dec  5 12:25:44 EST 2023

************************************************************************
Hardware:

    Hardware Overview:

      Model Name: MacBook Air
      Model Identifier: Mac14,2
      Model Number: MLY33LL/A
      Chip: Apple M2
      Total Number of Cores: 8 (4 performance and 4 efficiency)
      Memory: 8 GB
      System Firmware Version: 10151.41.12
      OS Loader Version: 10151.41.12
      Serial Number (system): 47RHKGYWRJ
      Hardware UUID: 130E90CB-E98C-56F4-A251-C55BBEC24E3D
      Provisioning UDID: 00008112-000471DA21DBC01E
      Activation Lock Status: Disabled


************************************************************************
Source Disk Information

   Device Identifier:         disk3s1s1
   Device Node:               /dev/disk3s1s1
   Whole:                     No
   Part of Whole:             disk3

   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:               disk3s2
   Recovery Disk:             disk3s3
   Media Type:                Generic
   Protocol:                  Apple Fabric
   SMART Status:              Verified
```

```
   Volume UUID:               B7AD18B0-AA32-47E8-BDE7-D735A0E76542
   Disk / Partition UUID:     B7AD18B0-AA32-47E8-BDE7-D735A0E76542

   Disk Size:                  245.1 GB (245107195904 Bytes) (exactly 478724992 512-Byte-
Units)
   Device Block Size:         4096 Bytes

   Volume Used Space:        10.3 GB (10254770176 Bytes) (exactly 20028848 512-Byte-Units)
   Container Total Space:      245.1 GB (245107195904 Bytes) (exactly 478724992 512-Byte-
Units)
   Container Free Space:       148.1 GB (148076089344 Bytes) (exactly 289211112 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:      Yes

   This disk is an APFS Volume Snapshot.  APFS Information:
   APFS     Snapshot     Name:                                          com.apple.os.update-
B9BEB63D27BD183CAF94E819C5D4F29F726EDA51D3672F1D3EC69FC59C9FC2D5
   APFS Snapshot UUID:        B7AD18B0-AA32-47E8-BDE7-D735A0E76542
   APFS Container:            disk3
   APFS Physical Store:       disk0s2
   Fusion Drive:              No
   APFS Volume Group:         754EE304-95FD-486E-A314-1512AFD8874B
   EFI Driver In macOS:       2235041001000000
   Encrypted:                 No
   FileVault:                 No
   Sealed:                    Broken
   Locked:                    No

   APFS Snapshots are defined upon this APFS Volume.  Snapshot list:
   Snapshot UUID:             B7AD18B0-AA32-47E8-BDE7-D735A0E76542
   Name:                                                         com.apple.os.update-
B9BEB63D27BD183CAF94E819C5D4F29F726EDA51D3672F1D3EC69FC59C9FC2D5
   XID:                       76412
   Snapshot UUID:             9287B2C0-5E50-467A-AA9A-9AC28BD77E8A
   Name:                                                         com.apple.os.update-
4AB291B82A6F7AF00ABF2EB483404181363A0F0165B9560DE354E11ADC2D1BBF4BADA49469B2D7A403305EFD4A
3E8D53
   XID:                       253343
   Snapshot UUID:             1E33D436-909A-442B-BD80-2301039B2738
   Name:                      com.apple.os.update-MSUPrepareUpdate
   XID:                       253354


**********************************************************************
Acquisition Information:

Logical Image Name: EFI01_FOLDERS.dmg
Logical Image Start Time: Tue Dec  5 12:25:45 EST 2023
Logical Image End Time..: Tue Dec  5 12:53:29 EST 2023

Targeted Folders: /Users
```

```
                    /Applications
                    /bin
                    /cores
                    /opt
                    /sbin
                    /usr

***************************************************************
Hash Information:

Logical Image Name: EFI01_FOLDERS.dmg
Logical Image Hash: 763cf4f4f7cbc7a2766d34abae952ded
Logical Hash Start Time: Fri Dec  5 12:53:30 EST 2023
Logical Hash End Time..: Fri Dec  5 13:56:11 EST 2023

***************************************************************
```

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_M1 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.

End User License Agreement

LL*IMAGER*

2023, 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

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 and Jesus F. Pena