

Lab - Digital Forensics Using Autopsy Part I

In this lab, students are introduced to two digital forensic tools built into Kali Linux, Autopsy and Sleuth Kit. Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. Law enforcement, military, and corporate examiners can use it to investigate what happened on a computer. Autopsy can also be used to recover lost or deleted files and images.

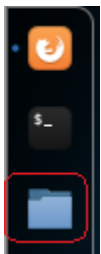
Autopsy was built to sit on top of the Sleuth Kit to offer an intuitive, GUI-based forensic suite that utilizes the strength of Sleuth Kit, while at the same time offering the basics of a case management tool.

The student should read the entire lab before beginning. Again, read the entire lab carefully before beginning!

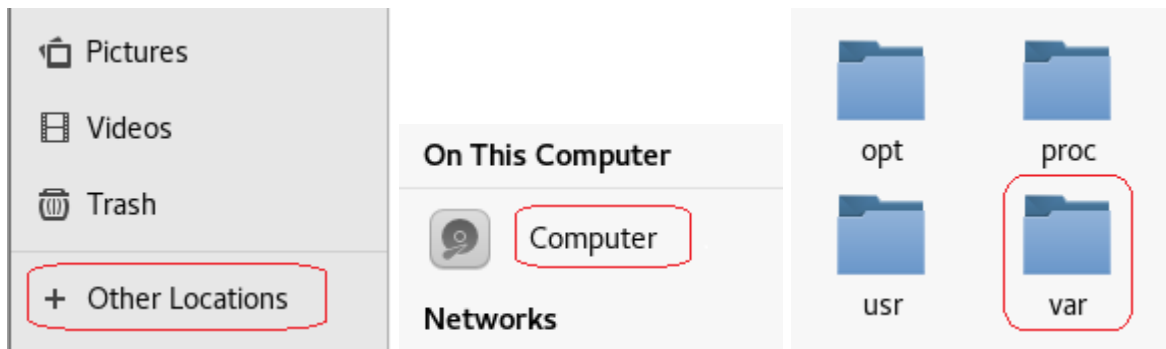
Lab Prep:

Create a folder called **forensics** inside of the VAR directory.

Click on **Folder icon from the quick launch menu**

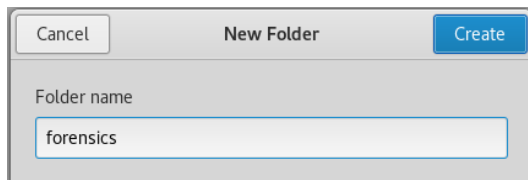


At the bottom of the files directory, click on Other Location and the top of the next windows pane, click Computer, open the VAR folder

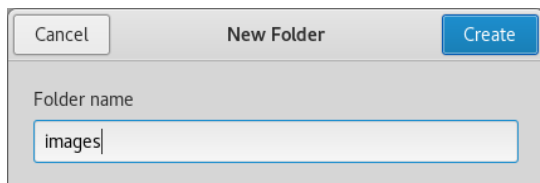


Inside the **var** directory, right-click on any white area and select **New folder**

Name the folder **forensics**



Open the **forensics** folder and create a second folder called **images**



Important! Upper and lower-case lettering do matter in Linux. When naming directories, folders, and files in Linux, use only lower-case lettering. For blank spaces, use the underscore_.

Remember this location!

Go to the "Digital Forensics Tool Testing Images" Website.

- a. Go To <http://dfft.sourceforge.net/>
- b. Click on "8. JPEG Search Test #1"

Test Images:

1. [Extended Partition Test](#) (July '03)
2. [FAT Keyword Search Test](#) (Aug '03)
3. [NTFS Keyword Search Test #1](#) (Oct '03)
4. [EXT3FS Keyword Search Test #1](#) (Nov '03)
5. [FAT Daylight Savings Test](#) (Jan '04)
6. [FAT Undelete Test #1](#) (Feb '04)
7. [NTFS Undelete \(and leap year\) Test #1](#) (Feb '04)
8. [JPEG Search Test #1](#) (Jun '04)
9. [FAT Volume Label Test #1](#) (Aug '04)
10. [NTFS Autodetect Test #1](#) (Jan '05)
11. [Basic Data Carving Test #1](#) (Mar '05) (by Nick Mikus)
12. [Basic Data Carving Test #2](#) (Mar '05) (by Nick Mikus)
13. [Windows Memory Analysis #1](#) (Jan '06) (by Jesse Kornblum)
14. [ISO9660 Interpretation Test #1](#) (Aug '10)

2. Download the Image File
 - a. Under Download, click on the "zip" link.
 - b. If the dftt website or zip link is down, click on the alternative link provided --> [here](#).
3. Save the download as a zip.
4. Right-click at the top of the **Firefox** browser grey taskbar.
5. Place a check next to **Menu Bar**
6. From the new menu bar, go to **Tools>Downloads>** find the **8-jpeg-search. zip** file (the file you just downloaded.)
7. To the right of the file name, click on the folder icon (to the right) to open the containing folder
8. Right-click on the **8-jpeg-search. zip** download and select **copy**
9. In the left Windowpane, click on **File System**, find the **var** directory, find the **forensics** folder, and open the **forensics** folder. Next, open the **Images** folder. Right-click in anywhere inside the **images** folder and select paste.
10. **Remember the path!**
11. Unzipping the Image

Open a terminal Run the following commands

- `cd /var/forensics/images`
- `ls -lta`
- `unzip 8-jpeg-search.zip`

```
root@kali: /var/forensics/images
File Edit View Search Terminal Help
root@kali:~# cd /var/forensics/images <=> Change directory
root@kali:/var/forensics/images# ls -lrta <=> List contents and folder
total 1908
drwxr-xr-x 3 root root 4096 Jun 1 18:45 ..
-rw-r--r-- 1 root root 1944066 Jun 1 18:51 8-jpeg-search.zip
drwxr-xr-x 2 root root 4096 Jun 1 18:56 .
root@kali:/var/forensics/images# unzip 8-jpeg-search.zip <=> Extract contents
Archive: 8-jpeg-search.zip
  inflating: 8-jpeg-search/8-jpeg-search.dd <=> This is our image
  inflating: 8-jpeg-search/COPYING-GNU.txt
  inflating: 8-jpeg-search/README.txt
  inflating: 8-jpeg-search/index.html
  inflating: 8-jpeg-search/results.txt
root@kali:/var/forensics/images#
```

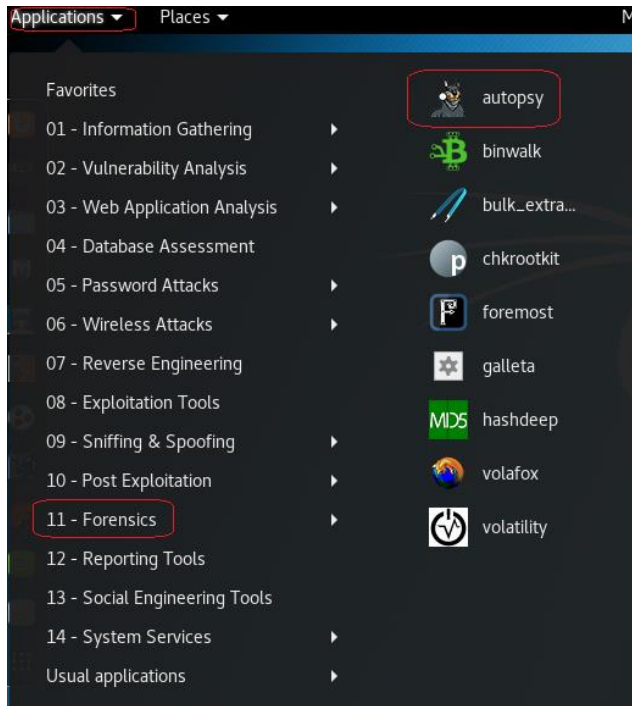
If you are having issues with the (file not found or no such file or directory, browse to the images folder that you created: **computer > file system > forensics > images**

Right-click on the **images** folder and select “**Open in Terminal.**”

If the 8-jpeg-search folder returns the same error, repeat the process only this time select **8-jpeg-search** folder to “**Open in Terminal.**”

Open Autopsy

In Kali, go to **Applications -> Kali Linux -> Forensic** and select **autopsy** from the list.



When you do so, you will open a screen that looks like that below. Notice that it asks you to open up a browser at <http://localhost:9999/autopsy>. **Remember not to close the terminal session.**

```
Terminal
File Edit View Search Terminal Help

=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====

Evidence Locker: /var/lib/autopsy
Start Time: Mon Jan  8 18:40:16 2018
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Step 2: Open a Web Browser

Open any browser and navigate to the address above. This takes us to the local web server on our system (localhost) and accesses port 9999 where Autopsy is running. (Try copying the address inside the terminal. Then paste the address into the address bar of the browser) for this demonstration, we are using the default browser in Kali, Firefox.

When we navigate to the address, we get a webpage like below.





As mentioned earlier, Autopsy is just a GUI overlay on top of Brian Carrier's excellent suite of forensic tools, Sleuth Kit. Since Sleuth Kit only uses command-line instructions, Autopsy makes working with it much simpler and more intuitive.

Create a New Case

As in any real forensic investigation, you will need to create a case and organize all of your evidence and information. In this regard, autopsy requires that you start a case to get started.

Here, we have given this case a numerical case name (101) and a description of "image recovery," and I have provided my name as the investigator (clk). Please note that I can provide up to six (6) investigator names. In a real forensic investigation, you will seldom be working alone. **You will use your name, not mine.**

CREATE A NEW CASE

1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.

101

2. Description: An optional, one line description of this case.

image recovery

3. Investigator Names: The optional names (with no spaces) of the investigators for this case.

a. clk b.

c. d.

e. f.

g. h.

i. j.

NEW CASE **CANCEL** **HELP**



After hitting the "New Case" button, you are greeted with the following screen.

Creating Case: 101

Case directory (/var/lib/autopsy/101/) created
Configuration file (/var/lib/autopsy/101/case.aut) created

We must now create a host for this case.

Please select your name from the list:

Add Host

This screen simply gives us the name of the case, where the case will be stored (/var/lib/autopsy/101), and where its configuration file will be stored (/var/lib/autopsy/101/case.aut). Our next step is to add a host.

The host is the machine we are investigating.

Step 4: Add a New Host

Click on the "Add Host" button on the line where you can select your name. When we click on that, it takes us to another screen where we can add information about our host like that below.

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Here we can add the hostname (host1), a description (image recovery), and the time zone (GMT) we are working in. For this lab, you can add your own host (machine name) name, description, and time zone, as appropriate.

Step 5: Add an Image File

Next, we need to import an image file. An image file is a bit-by-bit copy of the storage device that we captured for evidence when we arrived at the crime scene (Lab 1). This was completed at the beginning of the lab.

Adding host: host1 to case 101

Host Directory (/var/lib/autopsy/101/host1/) created

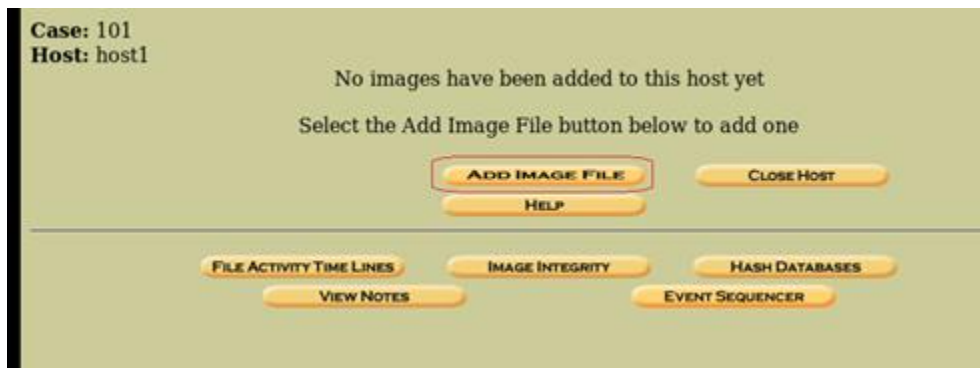
Configuration file (/var/lib/autopsy/101/host1/host.aut) created

We must now import an image file for this host

ADD IMAGE

We have a test image called **8-jpeg-search.dd** that we downloaded and extracted at the beginning of the lab.

Click Add Image




We can now import that image to Autopsy by giving it the location where I saved the image:

/var/forensics/images/8-jpeg-search/8-jpeg-search.dd


Tell autopsy the type of image (**partition**), and the import method (**symlink**).

ADD A NEW IMAGE


1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

 Path to the image

2. Type
Please select if this image file is for a disk or a single partition.

☐ Disk ☒ Partition 

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☒ Symlink  ☐ Copy ☐ Move

Data Integrity

Whenever we are creating an image or saving an image that might be used in any legal proceeding, it is critical we maintain the integrity of the image. This means we can prove that the image has not been tampered with from the time the image was captured until the time of the trial.

We can do this by creating a hash of the image.

Image File Details

Local Name: images/8-jpeg-search.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☐ Ignore the hash value for this image.

☒ Calculate the hash value for this image.

☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ntfs)

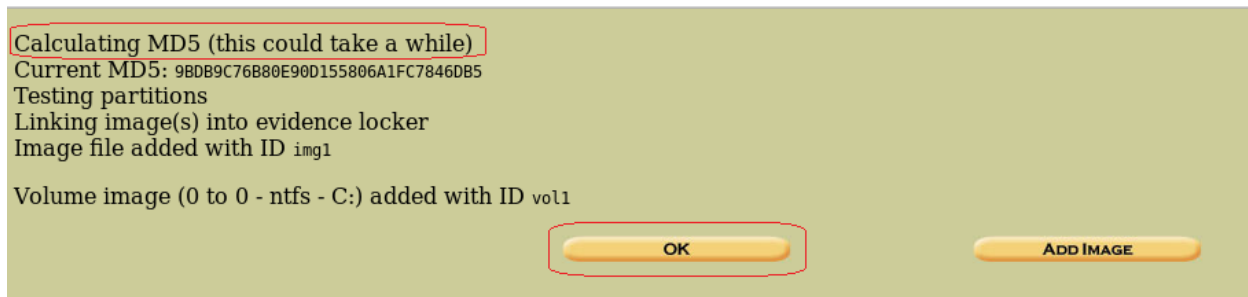
Mount Point: File System Type:

In this screen, Autopsy asks us whether we want to:

- **Ignore** the hash value for this image,
- **Calculate** the hash value for this image, or
- **Add** the following MD5 hash value for this image.

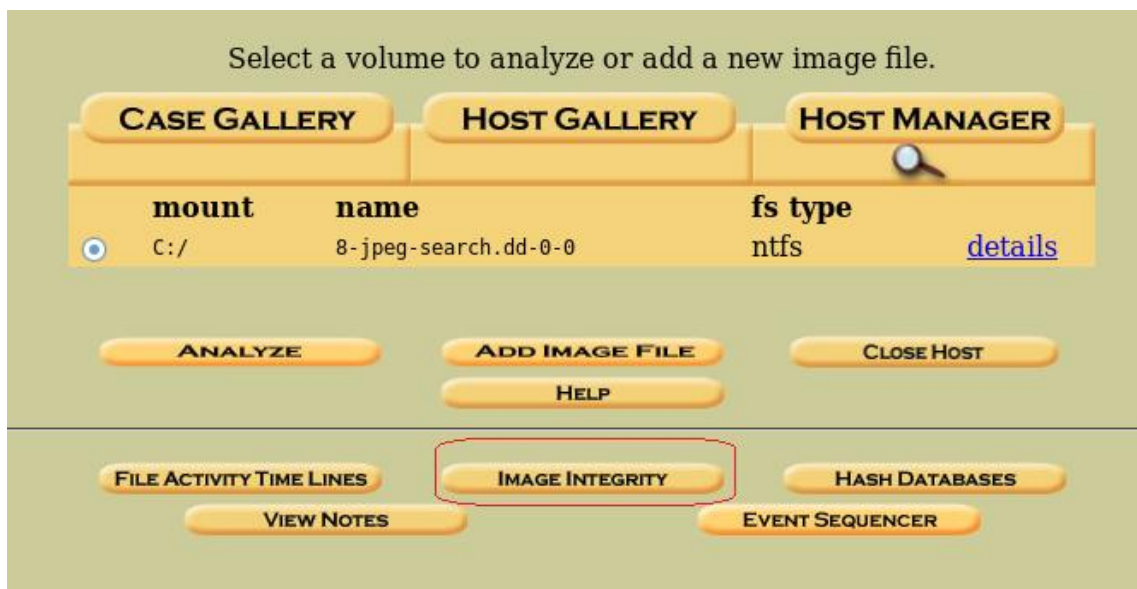
If you did not calculate the hash value when you captured the image (best practice), now is the time to do that. The results of the investigation must be above reproach! You need a hash of the image!

Do your hash calculation.



Select the OK button.

Click the Image Integrity Button



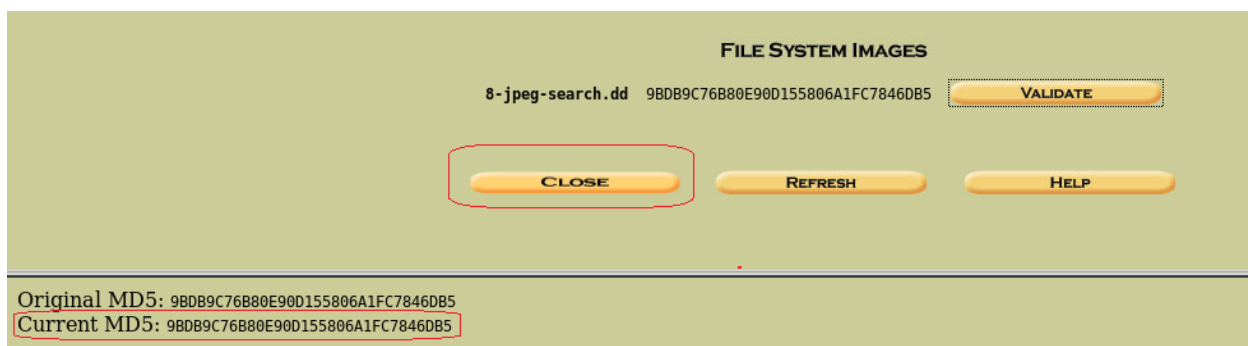
Click on the validate button.



Viewing the MD5 CheckSum.

Notice the MD5 Checksum of the 8-jpeg-search.dd image is displayed below.

- Verify the below checksum is the same as being correct
- Click the Close Button



Summary

In our first lab, we saw how we create a forensic image. This is a crucial step and it is important that we ensure the integrity of the image contents by hashing the image.

The steps of creating a forensic case are as follows:

- Create the image
- Create the case
- Analyze the data



In our next forensics lab, students pick up where this lab leaves off and begin the analysis of the forensic image.

End of the lab!