

Lab - Examining a Forensic Disk Image Using Autopsy

Overview

Overview

In our last lab, we attached an acquired disk image to the same SATA controller being used by our Kali Forensic Mode virtual disk. The VDI disk used for analysis was created by Dr. Mike Murphy, Costal Carolina University. This three-part lab series was created using the recorded lecture posted by Dr. Murphy on [YouTube](#). Use of the video content and the VDI image are granted by Dr. Murphy under the [Creative Commons Attribution license \(reuse allowed\)](#).



In this lab, we will use the Autopsy Forensic Browser. Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. Autopsy is built into Kali Linux and the SANS Investigative Forensic Toolkit Workstation (SIFT Workstation) that you can download from forensics.sans.org.

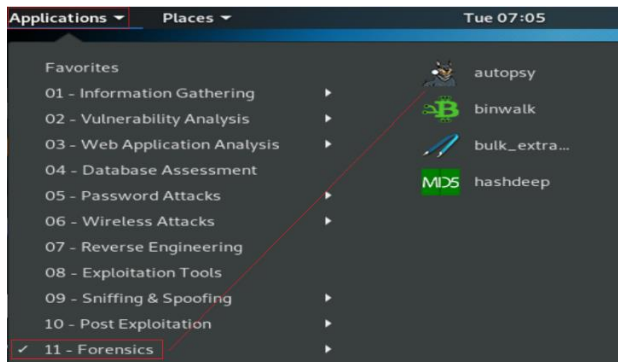
So far, we have created a virtual machine using VirtualBox for running Kali in forensic mode and we have captured a forensic image using the DD command. In this lab, you will learn how to build a forensic case using Autopsy.

Ensure you have your image created from the last lab. If you powered down or restarted your instance of Kali Forensic Mode, you will need to recreate the image again using the following command.

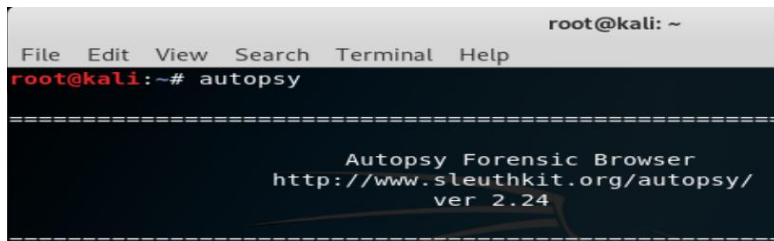
```
dd if=/dev/sdb of=forensic.img
```

Start the Autopsy Forensic Browser

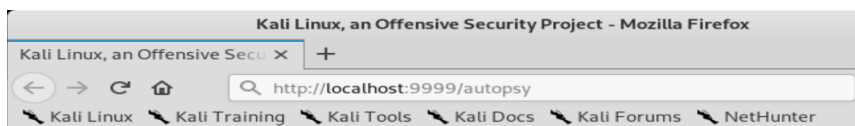
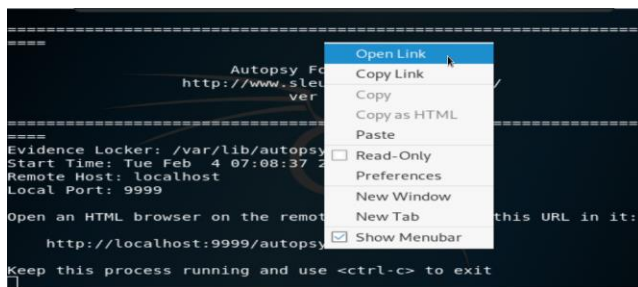
Autopsy is launched by expanding Applications menu, selecting Forensics, and from the results, clicking on Autopsy.



Tip: You can also type 'autopsy' at the terminal prompt to open the program.



Once you launch Autopsy, be sure to leave your terminal session open. Right click on the URL and from the context menu, select 'Open Link.'



This launches Firefox and starts the Autopsy Forensic Browser. Click on the button labeled 'New Case.'



On the next page, give your case a user-friendly name. I've chosen to call this new case, suspect_case_001. You are free to name your new case as you see fit. You are free to add additional information.

CREATE A NEW CASE

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

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

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

a. <input type="text" value="Prof. K"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>

Scroll to the bottom of the window and click the 'New Case button.'

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

a. <input type="text" value="Prof. K"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

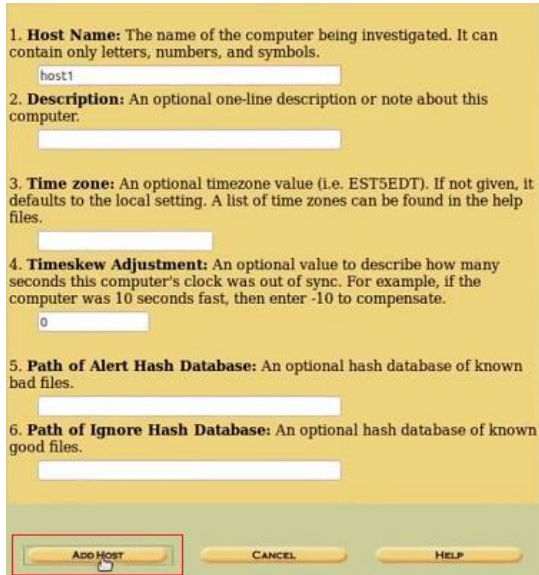
On the next screen you are prompted to add a host. Click the Add Host button and on the next screen, accept the defaults.

Creating Case: suspect_case_001

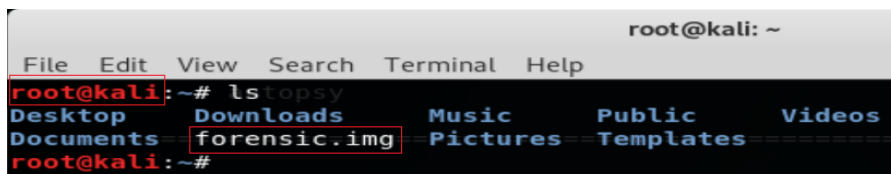
Case directory (/var/lib/autopsy/suspect_case_001/) created
 Configuration file (/var/lib/autopsy/suspect_case_001/case.aut) created

We must now create a host for this case.

Scroll to the bottom and click the button that says, 'Add Host.'



On the next screen, we must import the image of the suspect's hard drive that we created. For this lab, we created and saved the image directly to the root of our Kali Forensic Mode Live CD.



The path for the image would be /root/forensic.img

Click on the 'Add Image' button.



On the next screen, click the 'Add Image File' button. In the Location field type, /root/forensic.img. Since we copied the entire disk, leave the type as Disk and keep the default import method as symlink. Click the Next button.

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.

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

NEXT

On this next screen, we need to calculate a hash value for the image. The hash value we generate will be used to validate the integrity of the image. Accept the rest of the defaults. Click the 'Add' button.

Image File Details

Local Name: images/lecture.img

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: Microsoft basic data)
Sector Range: 2048 to 8158

Mount Point: File System Type:

ADD **CANCEL** **HELP**

Since this is a small image, Autopsy can calculate the hash very quickly. With a larger image, it would take more time depending on how large the image file was. We have fingered printed the image. If the image file is modified in any way, the hash values will differ giving us notice that a change to the image has occurred we did not anticipate. Click 'OK.'

Calculating MD5 (this could take a while)

Current MD5: 9711B60E9C4FFA6142B72069E3B0D7CA

Testing partitions

Linking image(s) into evidence locker

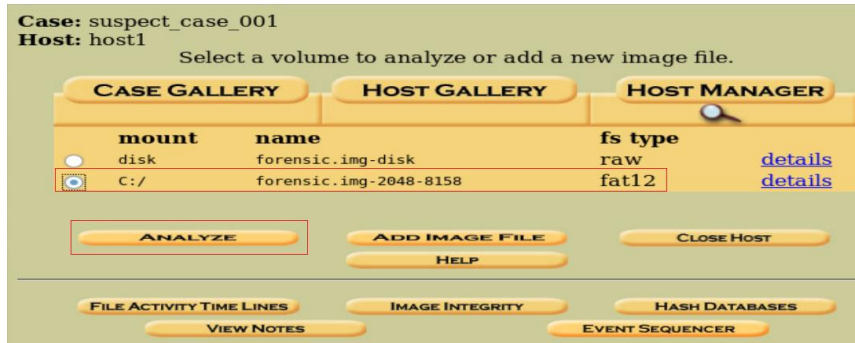
Image file added with ID img1

Disk image (type gpt) added with ID vol1

Volume image (2048 to 8158 - fat12 - C:) added with ID vol2

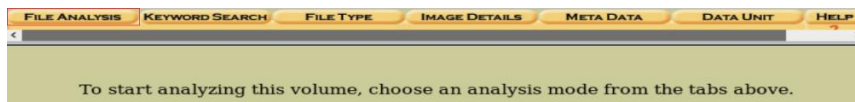
OK **ADD IMAGE**

On the next page, we can see the list of volumes we can analyze. Select the second option, C:/ as this is the image we imported.

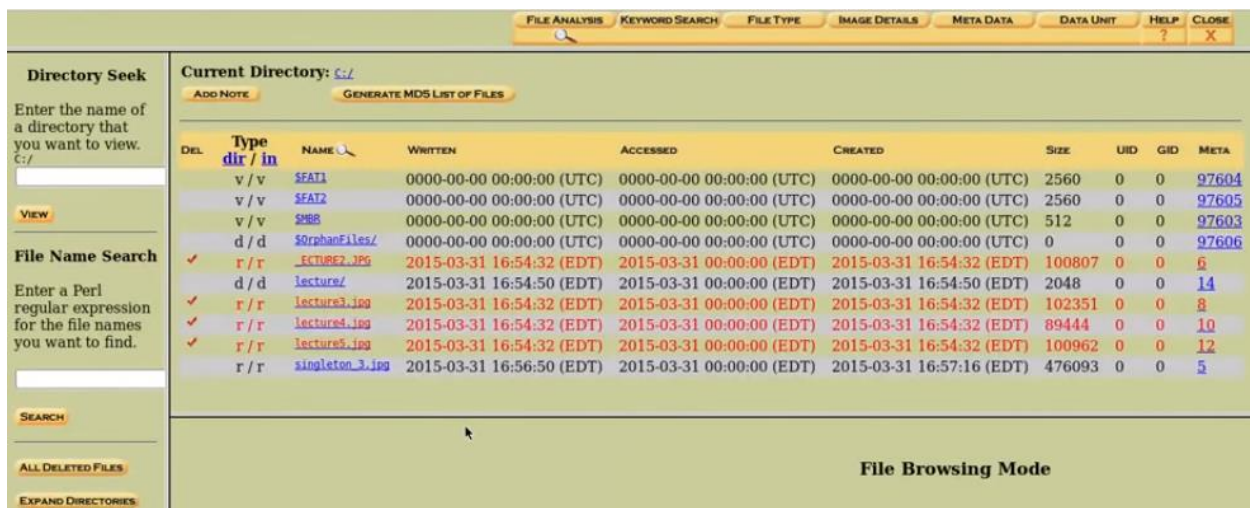
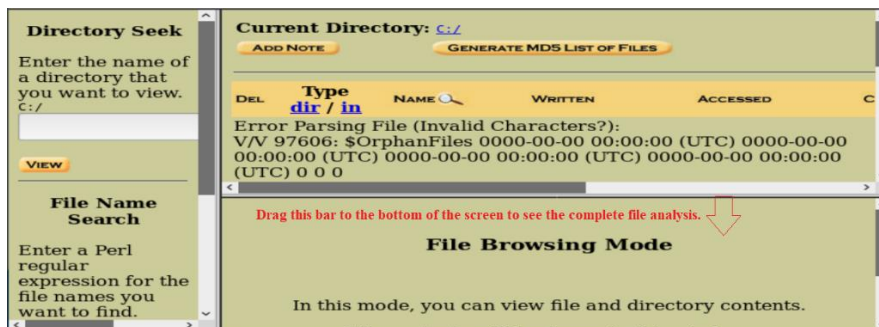


Click the button, 'Analyze.'

On the next screen, click the first option, 'File Analysis.'



On the next screen, to see the complete file analysis. You will need to drag the bottom window down to the bottom of the screen.



The first three entries, \$FAT1, \$FAT2, and \$SMBR, are files related to the disk itself. These files contain information about the disk file, most of which is information for the file allocation table written in binary. The \$SMBR is the master boot record which is also mostly written in binary.

The \$Orphanfiles/ are any files not completely deleted.

The next results show four files that have been deleted (_ECTURE.JPG, lecture3.jpg, Lecture4.jpg and lecture5.jpg.) and these are marked with a check mark under the column labeled, DEL. For fat32 file system, any file that has been deleted, will have the first letter of the name replaced with an underscore.

Down at the bottom of the list is file, marked, singleton_3.jpg. If we click on this entry, we can see the thumbnail view of the image. If you want to view the full size image, click the option next to the image.



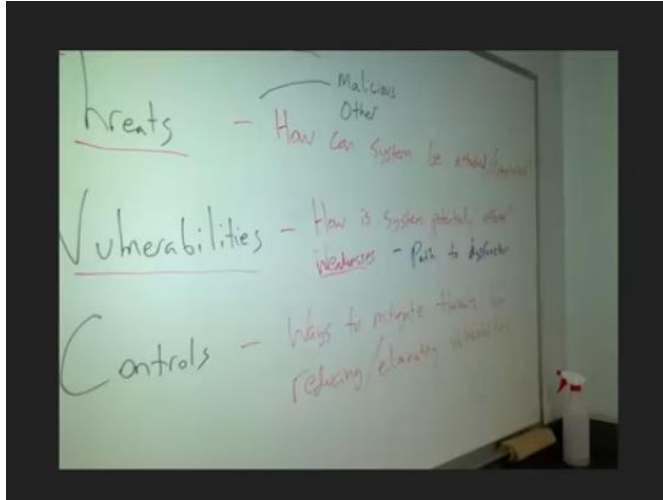
The next entry is marked as a directory, lecture. You can click this entry to view the contents of the directory.

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	Size	UID	GID	Meta
	dir / in								
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2560	0	0	97604
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2560	0	0	97605
	v / v	\$MFT	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	97603
	d / d	\$Orphanfiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	97606
✓	r / r	_ECTURE.JPG	2015-03-31 16:54:32 (EDT)	2015-03-31 00:00:00 (EDT)	2015-03-31 16:54:32 (EDT)	100807	0	0	6
✓	d / d	lecture/	2015-03-31 16:54:50 (EDT)	2015-03-31 00:00:00 (EDT)	2015-03-31 16:54:50 (EDT)	2048	0	0	14
✓	r / r	lecture3.jpg	2015-03-31 16:54:32 (EDT)	2015-03-31 00:00:00 (EDT)	2015-03-31 16:54:32 (EDT)	102351	0	0	8
✓	r / r	lecture4.jpg	2015-03-31 16:54:32 (EDT)	2015-03-31 00:00:00 (EDT)	2015-03-31 16:54:32 (EDT)	89444	0	0	10
✓	r / r	lecture5.jpg	2015-03-31 16:54:32 (EDT)	2015-03-31 00:00:00 (EDT)	2015-03-31 16:54:32 (EDT)	100962	0	0	12
	r / r	singleton_3.jpg	2015-03-31 16:56:50 (EDT)	2015-03-31 00:00:00 (EDT)	2015-03-31 16:57:16 (EDT)	476093	0	0	5

You are shown the contents of the folder.



You can click, through each of images to see the contents.



Summary –

In this lab, we took an image we created using the dd command and using Autopsy, we created a hash value for the image and examined the contents of the suspect's disk. This entire process from start to finish used the Kali forensic Mode Live CD.