Digital Forensics Hands on Lab

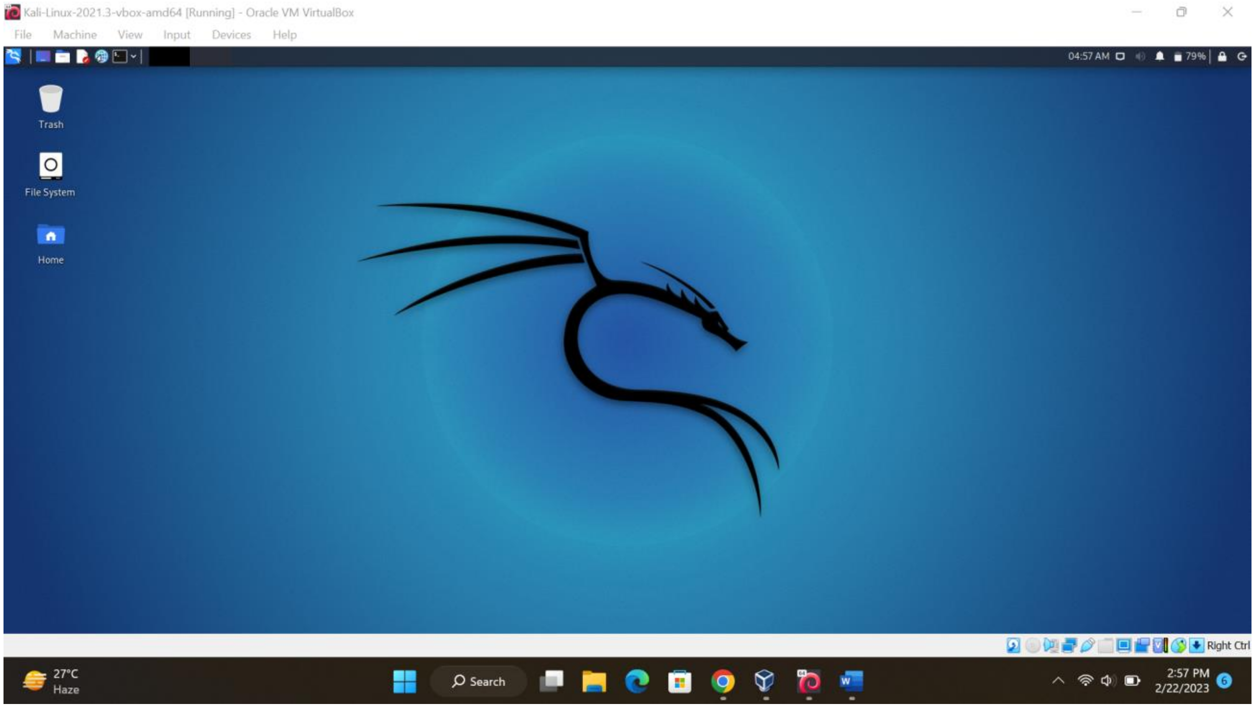
Contents

Digital Forensics Using Autopsy

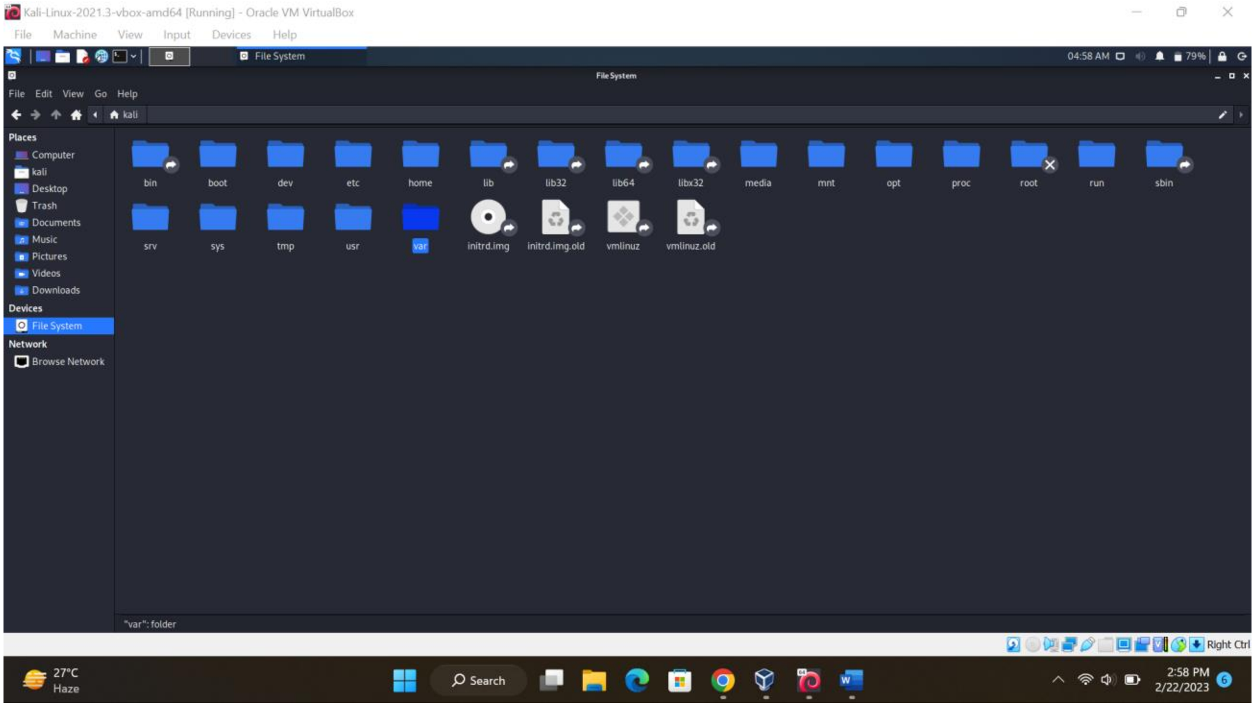
In this lab, we are introduced digital forensic tools built into Kali Linux, Autopsy. Autopsy is a digital forensics platform and graphical interface. Law enforcement, military, and corporate examiners can use it to investigate what happened on a computer. Autopsy can also be used to recover lost or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

Lab Prep:

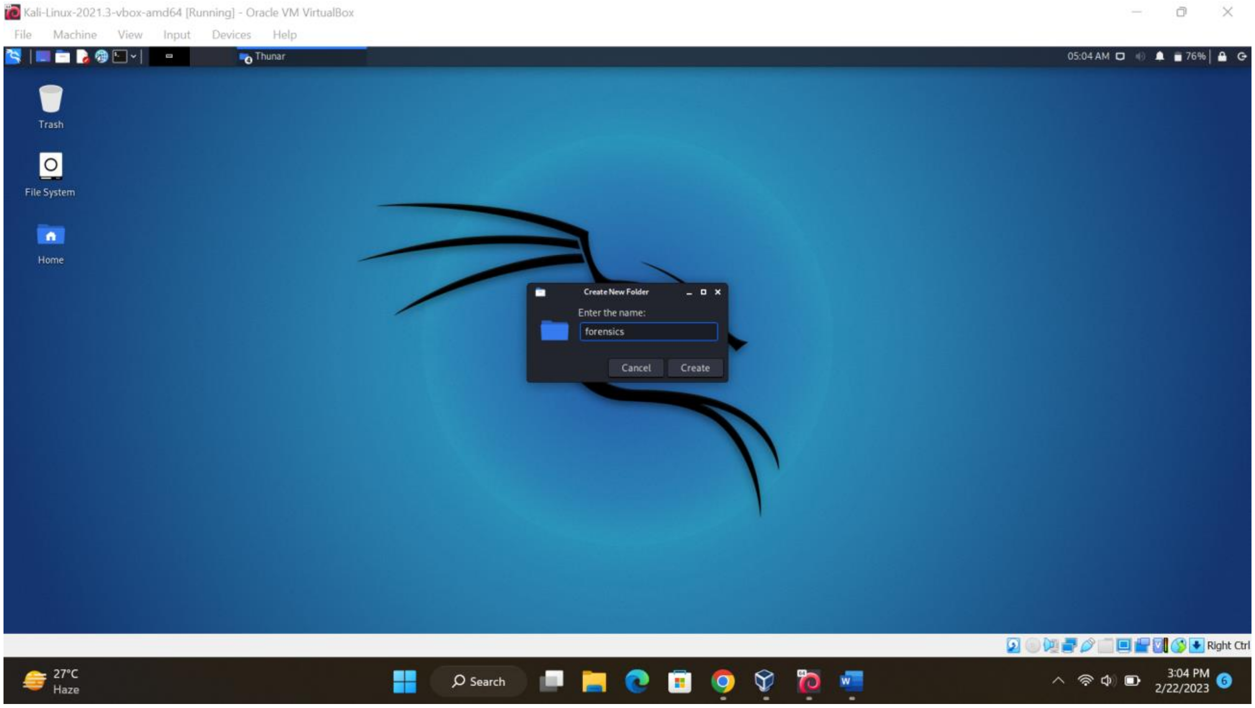
- First of fall install Kali Linux using any virtualization tool like ***VMware, vSphere, VirtualBox*** etc.



- Open ***Home*** and click on file location option.

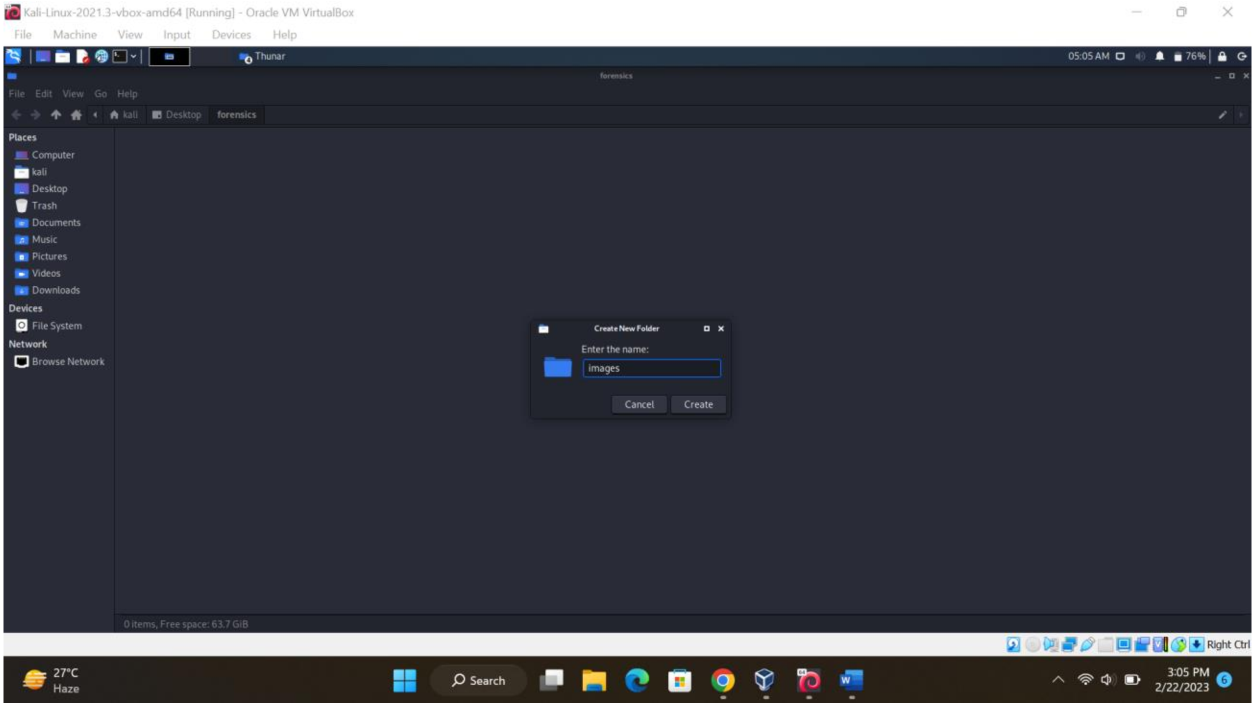


- Create a folder called **forensics** inside of VAR directory.
- Inside the **var** directory, right click on any white area and select **new folder.**
- Open the **forensics** folder and create a second folder called **images.**


Create New Folder

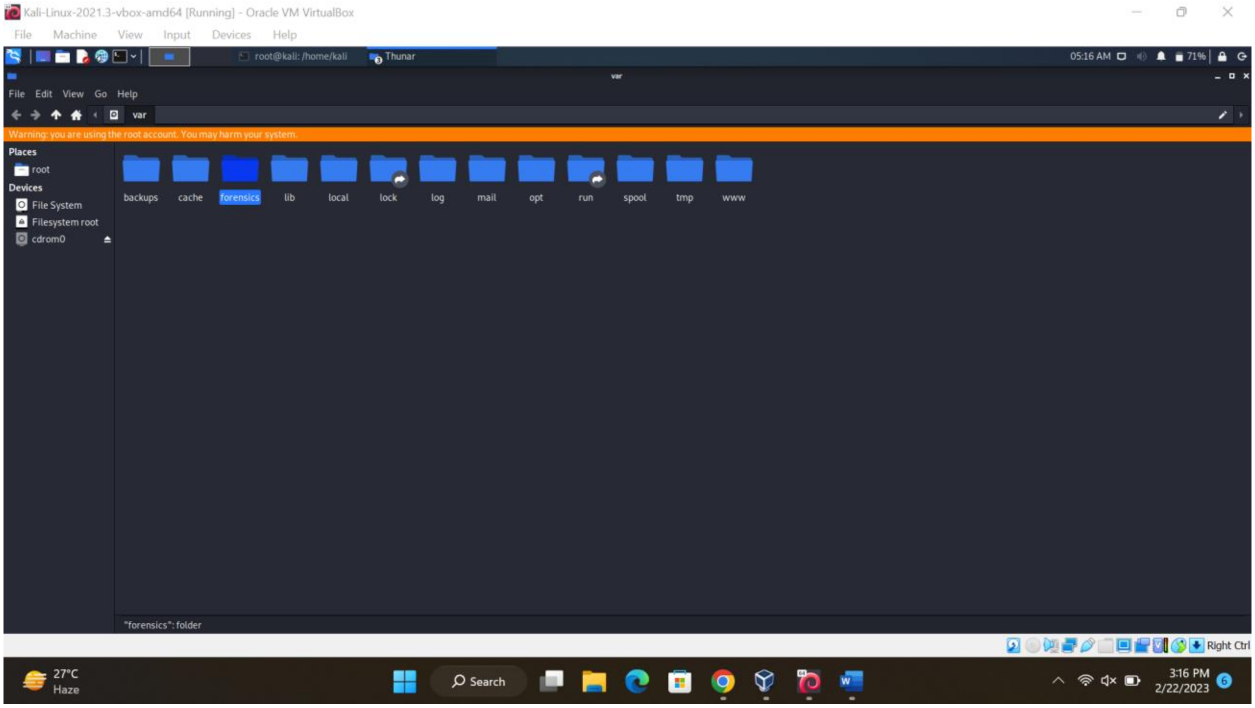
Enter the name: forensics

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Thunar
05:04 AM 76%
Trash
File System
Home
Cancel
Create
Right Ctrl
27°C
Haze
Search
3:04 PM
2/22/2023



Enter the name: images

0 items, Free space: 63.7 GiB

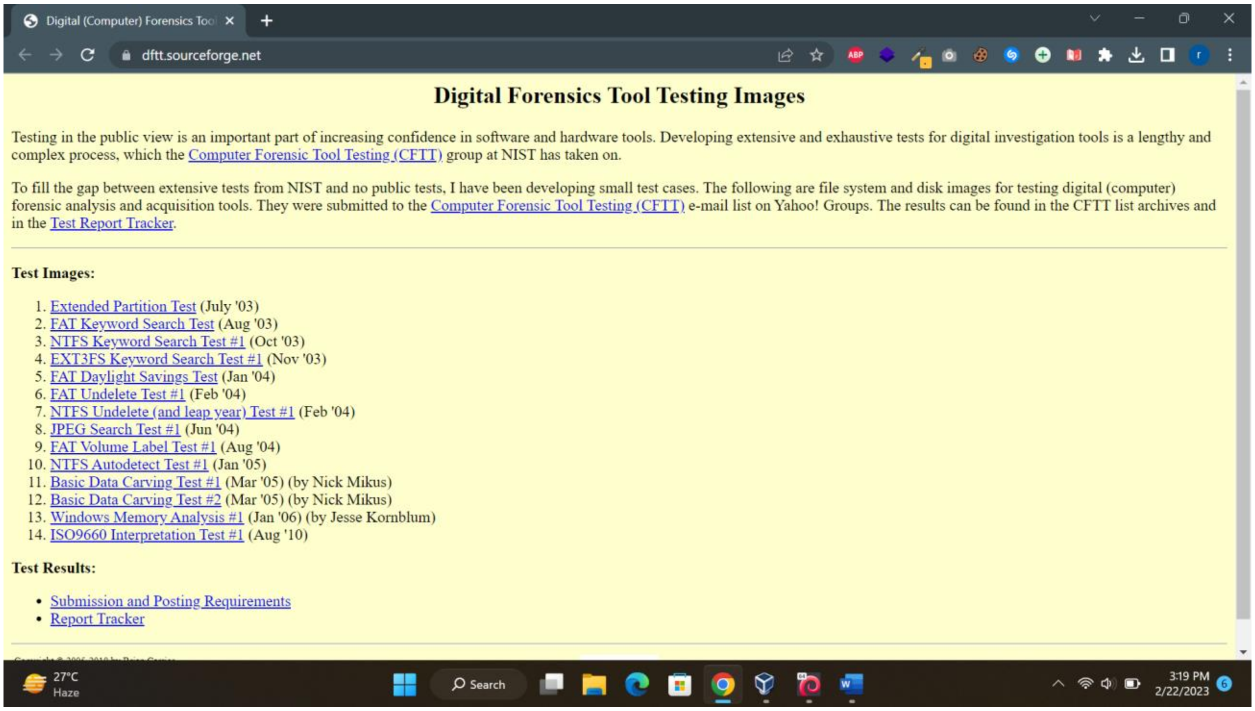


Warning: you are using the root account. You may harm your system.

"forensics": folder

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

  a. Go To **http://dftt.sourceforge.net/**
  b. Click on "8. JPEG Search Test #1"



Digital Forensics Tool Testing Images

Testing in the public view is an important part of increasing confidence in software and hardware tools. Developing extensive and exhaustive tests for digital investigation tools is a lengthy and complex process, which the Computer Forensic Tool Testing (CFTT) group at NIST has taken on.

To fill the gap between extensive tests from NIST and no public tests, I have been developing small test cases. The following are file system and disk images for testing digital (computer) forensic analysis and acquisition tools. They were submitted to the Computer Forensic Tool Testing (CFTT) e-mail list on Yahoo! Groups. The results can be found in the CFTT list archives and in the Test Report Tracker.

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)

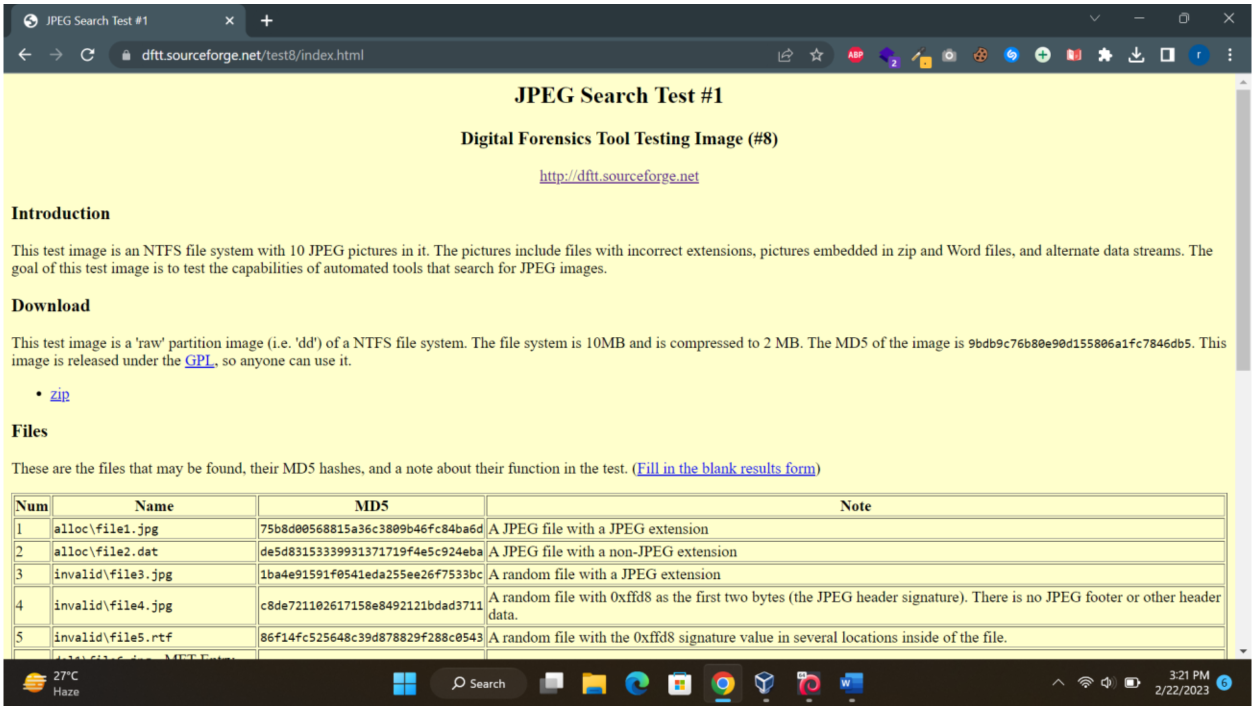
Test Results:

- Submission and Posting Requirements
- Report Tracker

- 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.**

- Save the download as a zip.



JPEG Search Test #1

Digital Forensics Tool Testing Image (#8)

http://dftt.sourceforge.net

Introduction

This test image is an NTFS file system with 10 JPEG pictures in it. The pictures include files with incorrect extensions, pictures embedded in zip and Word files, and alternate data streams. The goal of this test image is to test the capabilities of automated tools that search for JPEG images.

Download

This test image is a 'raw' partition image (i.e. 'dd') of a NTFS file system. The file system is 10MB and is compressed to 2 MB. The MD5 of the image is `9bdb9c76b80e90d155806a1fc7846db5`. This image is released under the GPL, so anyone can use it.

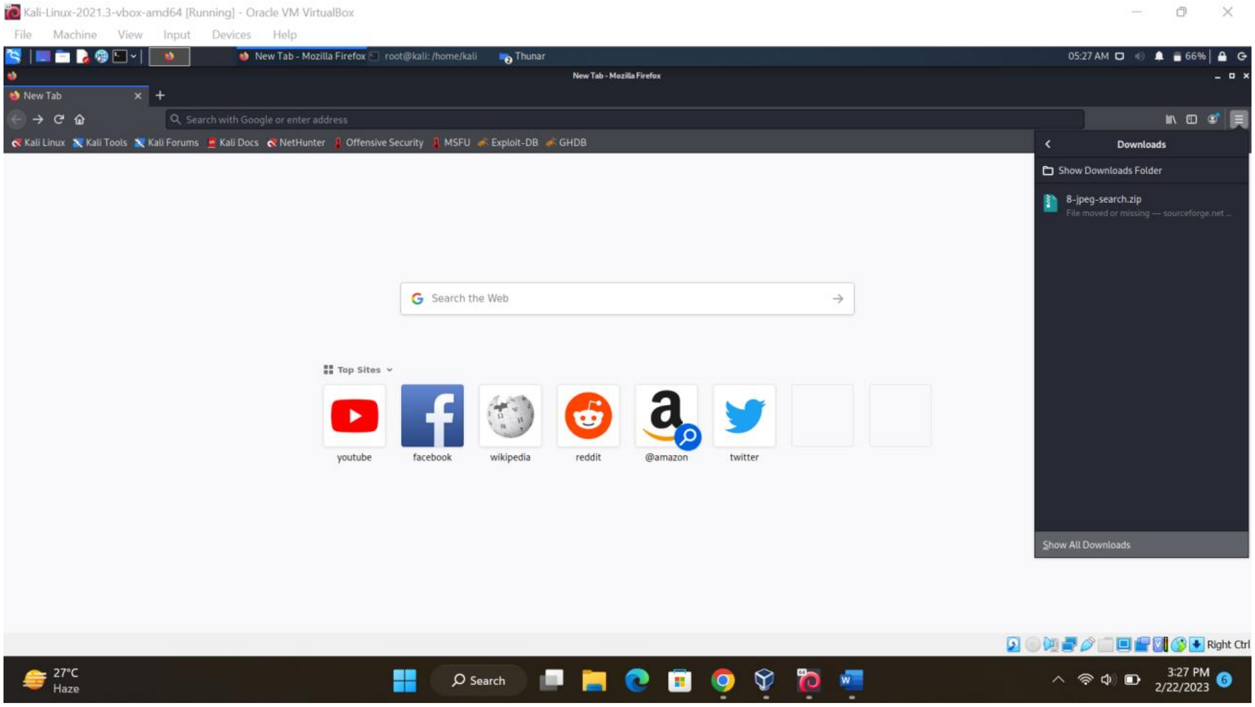
- zip

Files

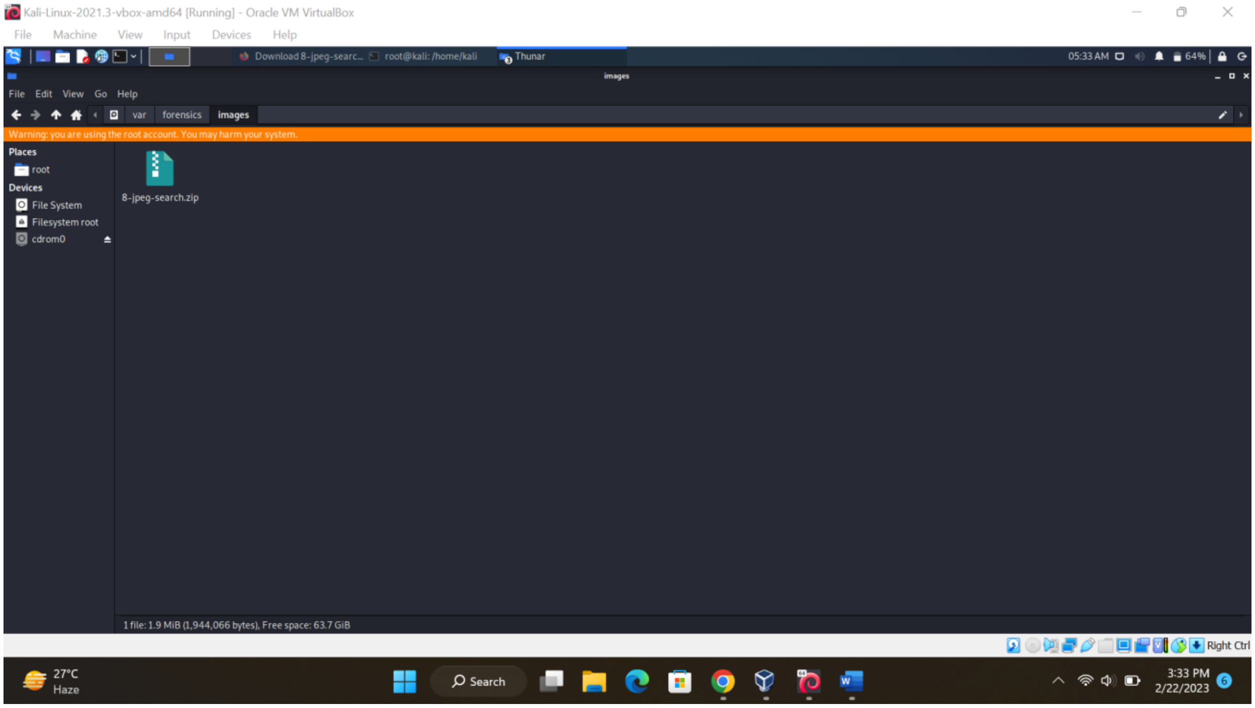
These are the files that may be found, their MD5 hashes, and a note about their function in the test. (Fill in the blank results form)

Num	Name	MD5	Note
1	`alloc\file1.jpg`	`75b8d00568815a36c3809b46fc84ba6d`	A JPEG file with a JPEG extension
2	`alloc\file2.dat`	`de5d83153339931371719f4e5c924eba`	A JPEG file with a non-JPEG extension
3	`invalid\file3.jpg`	`1ba4e91591f0541eda255ee26f7533bc`	A random file with a JPEG extension
4	`invalid\file4.jpg`	`c8de721102617158e8492121bdad3711`	A random file with 0xffd8 as the first two bytes (the JPEG header signature). There is no JPEG footer or other header data.
5	`invalid\file5.rtf`	`86f14fc525648c39d878829f288c0543`	A random file with the 0xffd8 signature value in several locations inside of the file.

- From the new menu bar, go to **Tools**>**Downloads>** find the **8-jpeg-search. zip** file (the file you just downloaded.)
- To the right of the file name, click on the folder icon (to the right) to open the containing folder.
- Right click on the **8-jpeg-search. zip** download and select **copy.**
- 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.
- **Remember the path!**
- Unzipping the Image



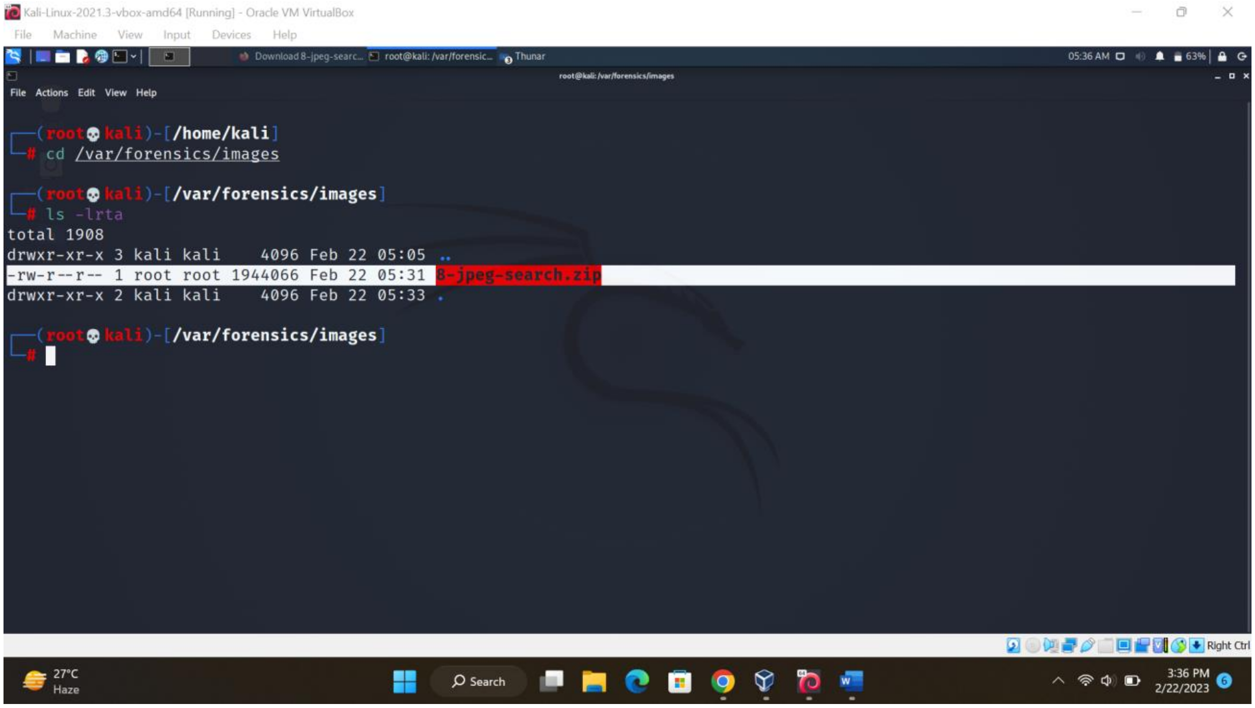
8-jpeg-search.zip
File moved or missing — sourceforge.net ...



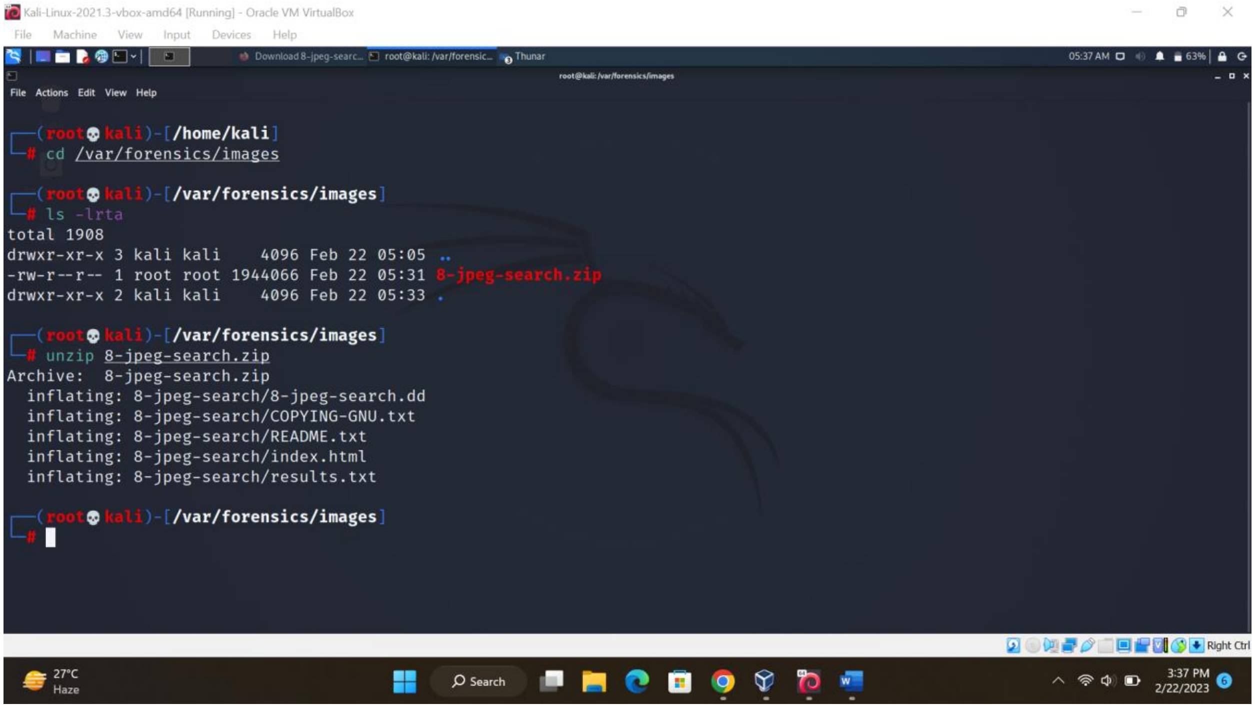
Warning: you are using the root account. You may harm your system.

1 file: 1.9 MiB (1,944,066 bytes), Free space: 63.7 GiB

- **Open a terminal Run the following commands.**
  - cd /var/forensics/images
  - ls -lrta
  - unzip 8-jpeg-search.zip


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Download 8-jpeg-searc... root@kali: /var/forensic... Thunar
05:36 AM 63%
root@kali: /var/forensics/images
File Actions Edit View Help
Right Ctrl
27°C Haze
Search
3:36 PM 2/22/2023

```
┌──(root💀kali)-[/home/kali]
└─# cd /var/forensics/images

┌──(root💀kali)-[/var/forensics/images]
└─# ls -lrta
total 1908
drwxr-xr-x 3 kali kali    4096 Feb 22 05:05 ..
-rw-r--r-- 1 root root 1944066 Feb 22 05:31 8-jpeg-search.zip
drwxr-xr-x 2 kali kali    4096 Feb 22 05:33 .

┌──(root💀kali)-[/var/forensics/images]
└─# 
```


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Download 8-jpeg-searc... root@kali: /var/forensic... Thunar
05:37 AM 63%
root@kali: /var/forensics/images
File Actions Edit View Help
Right Ctrl
27°C Haze
Search
3:37 PM 2/22/2023

```
┌──(root💀kali)-[/home/kali]
└─# cd /var/forensics/images

┌──(root💀kali)-[/var/forensics/images]
└─# ls -lrta
total 1908
drwxr-xr-x 3 kali kali    4096 Feb 22 05:05 ..
-rw-r--r-- 1 root root 1944066 Feb 22 05:31 8-jpeg-search.zip
drwxr-xr-x 2 kali kali    4096 Feb 22 05:33 .

┌──(root💀kali)-[/var/forensics/images]
└─# unzip 8-jpeg-search.zip
Archive:  8-jpeg-search.zip
  inflating: 8-jpeg-search/8-jpeg-search.dd
  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]
└─# 
```

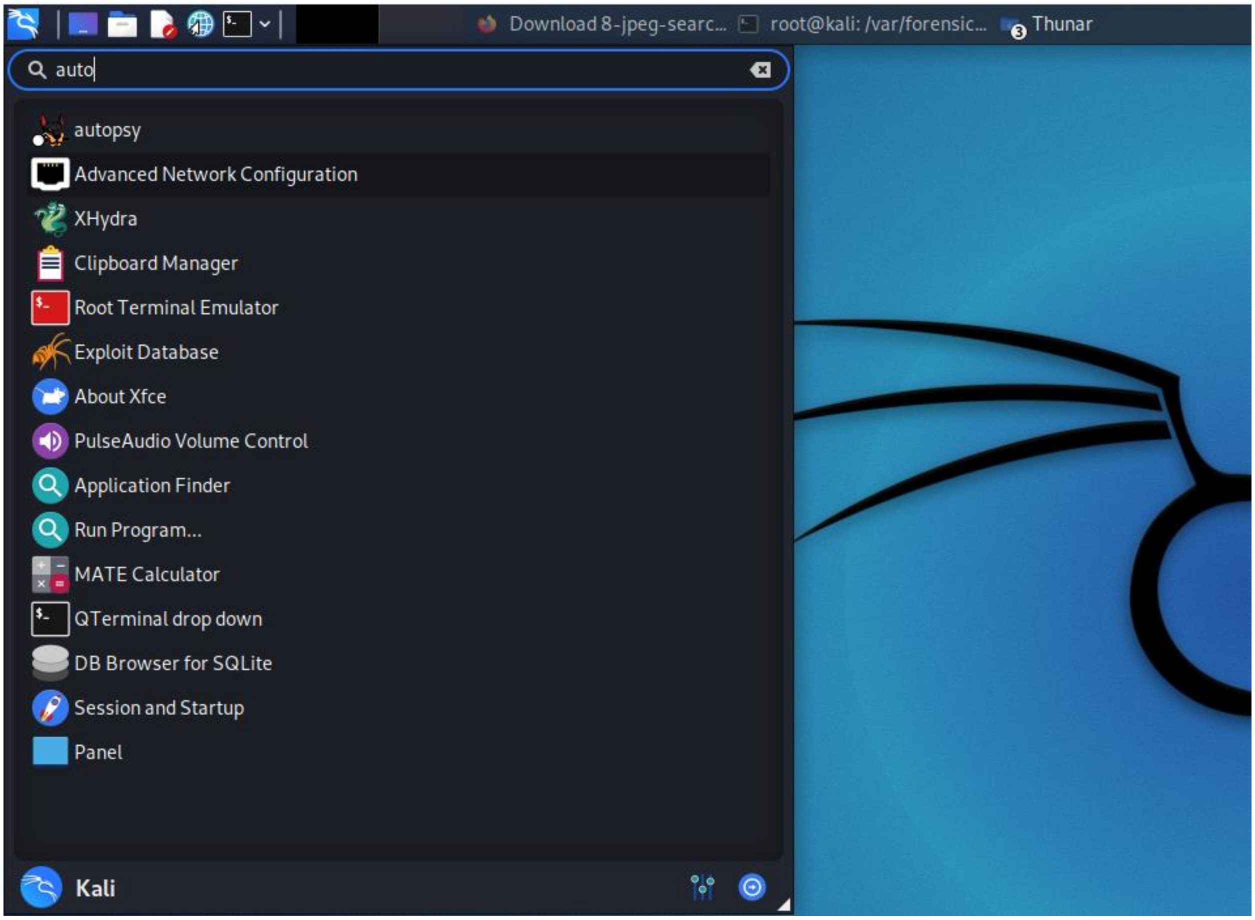
If you are having issues with the (file not found or no such file or directory, browse to the images folder that you created: computer > file system > forensics > images

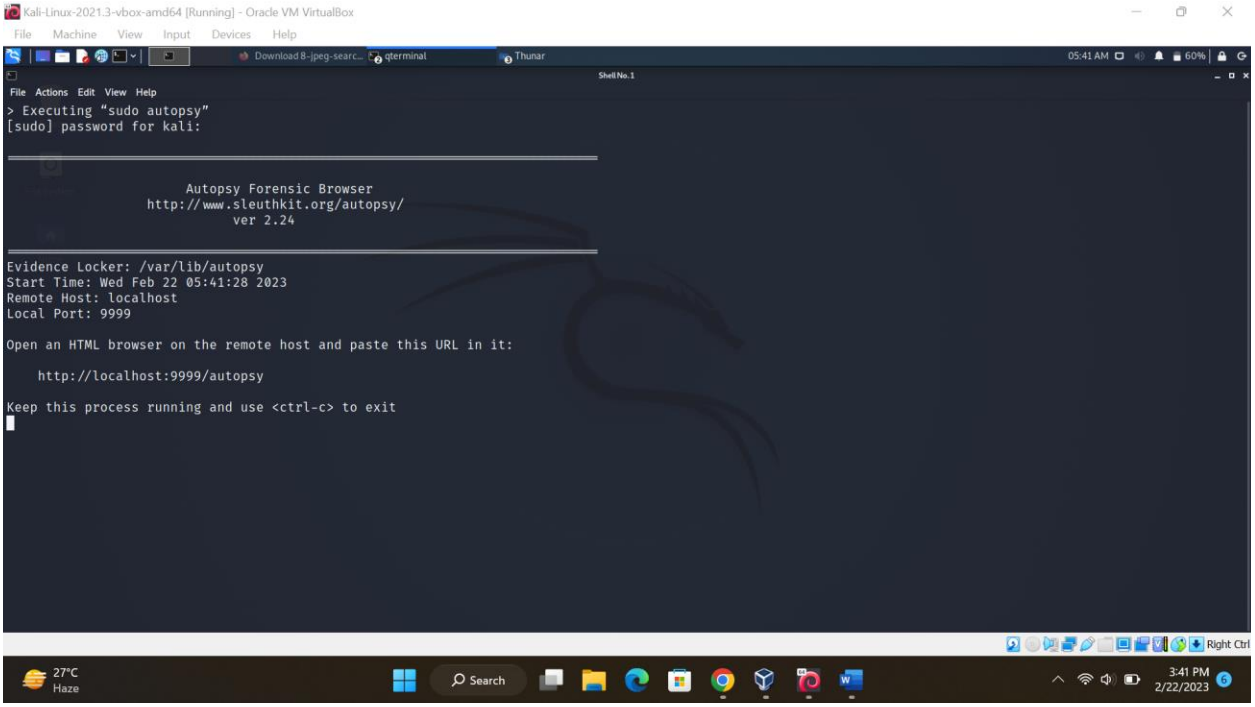
Right click on the images folder and select “Open in Terminal.”

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.




Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Download 8-jpeg-searc...
qterminal
Thunar
05:41 AM
60%
Shell No. 1
File Actions Edit View Help
Right Ctrl
27°C
Haze
Search
3:41 PM
2/22/2023

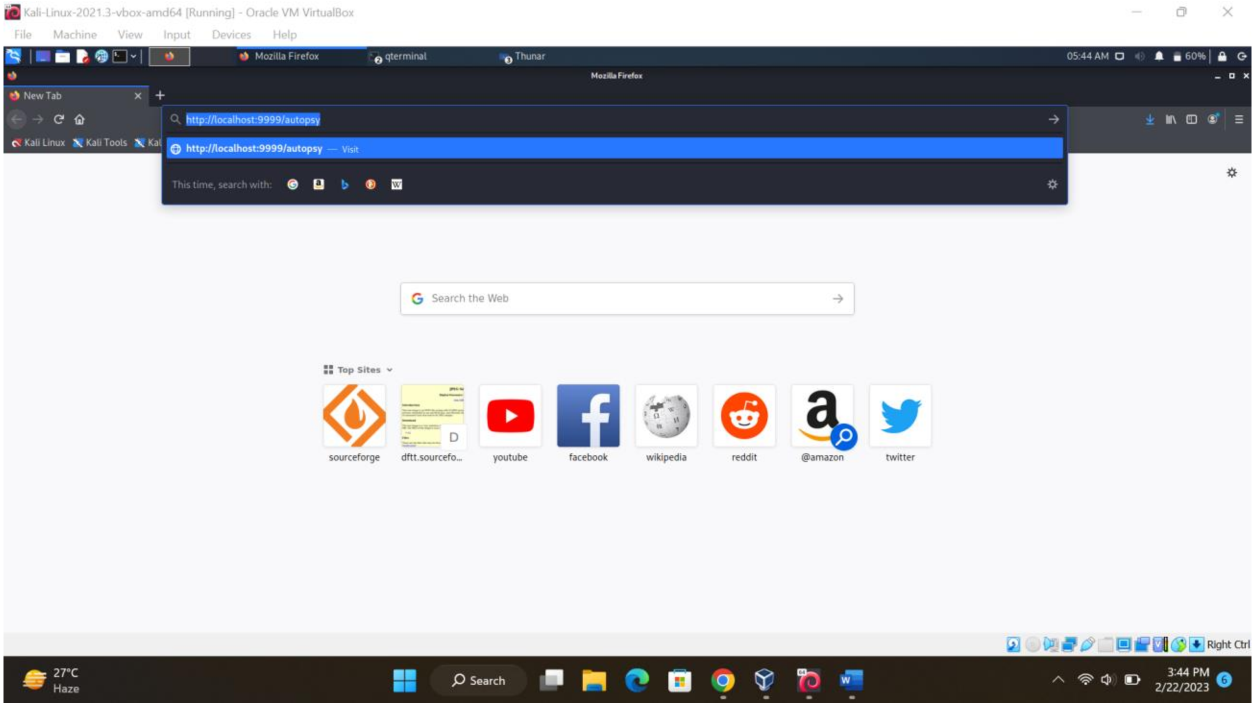
```
> Executing “sudo autopsy”
[sudo] password for kali:

============================================================================

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

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Wed Feb 22 05:41:28 2023
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
```

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

Open a Web Browser

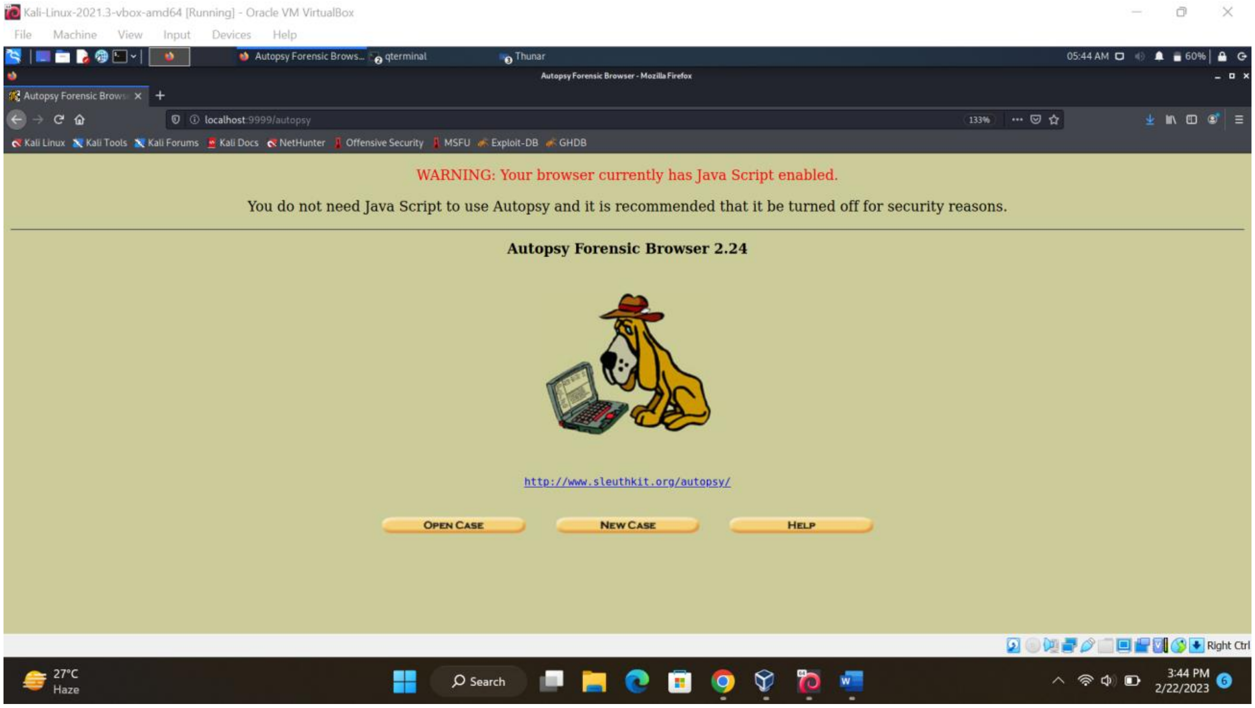
Open any browser and navigate to the address above. This takes us to the local web server on our system (localhost) and accesses port ***9999*** where Autopsy is running. (Try copying the address inside the terminal. Then paste the address into the address bar of the browser) for this demonstration,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

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



Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

http://localhost:9999/autopsy



Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox

Autopsy Forensic Browser - Mozilla Firefox

localhost:9999/autopsy

WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

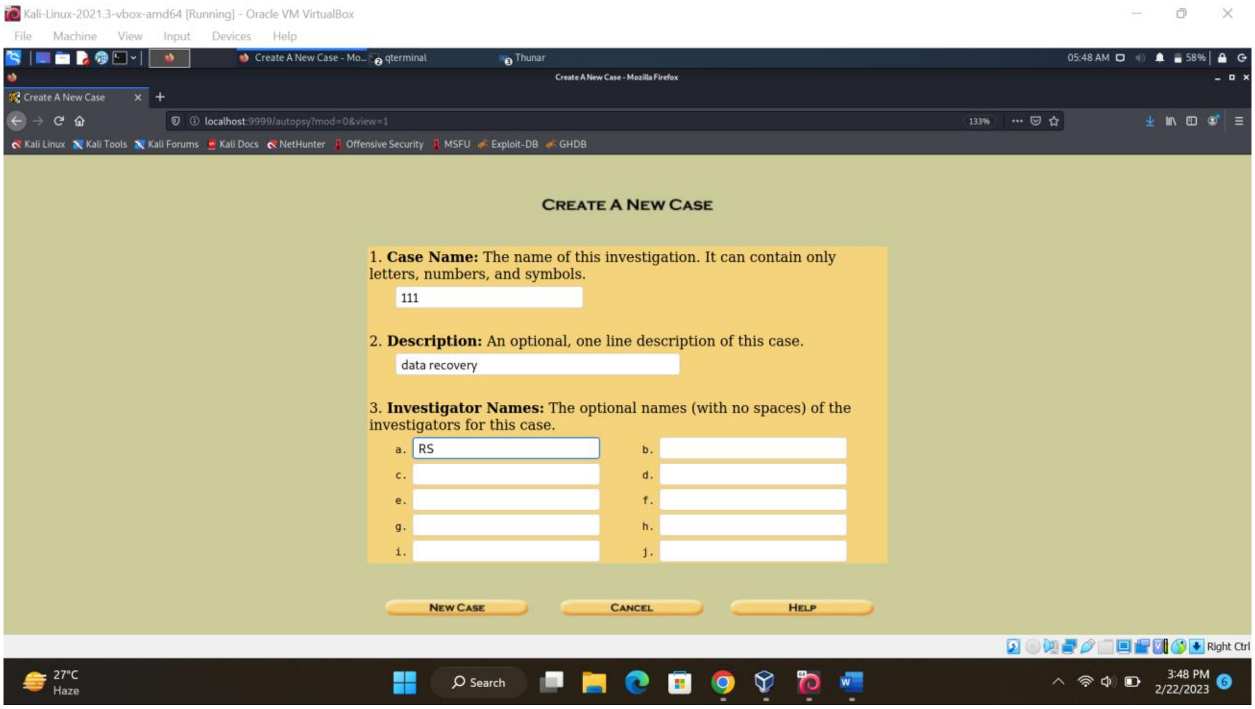
http://www.sleuthkit.org/autopsy/

As mentioned earlier, Autopsy is just a GUI overlay on top of Brian Carrier's excellent suite of forensic tools, 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 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 ***(111)*** and a description of "***data recovery***," and I have provided my name as the investigator ***(RS).*** Please note that I can provide up to six (6) investigator names. In a real forensic investigation, you will seldom be working alone.



CREATE A NEW CASE

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

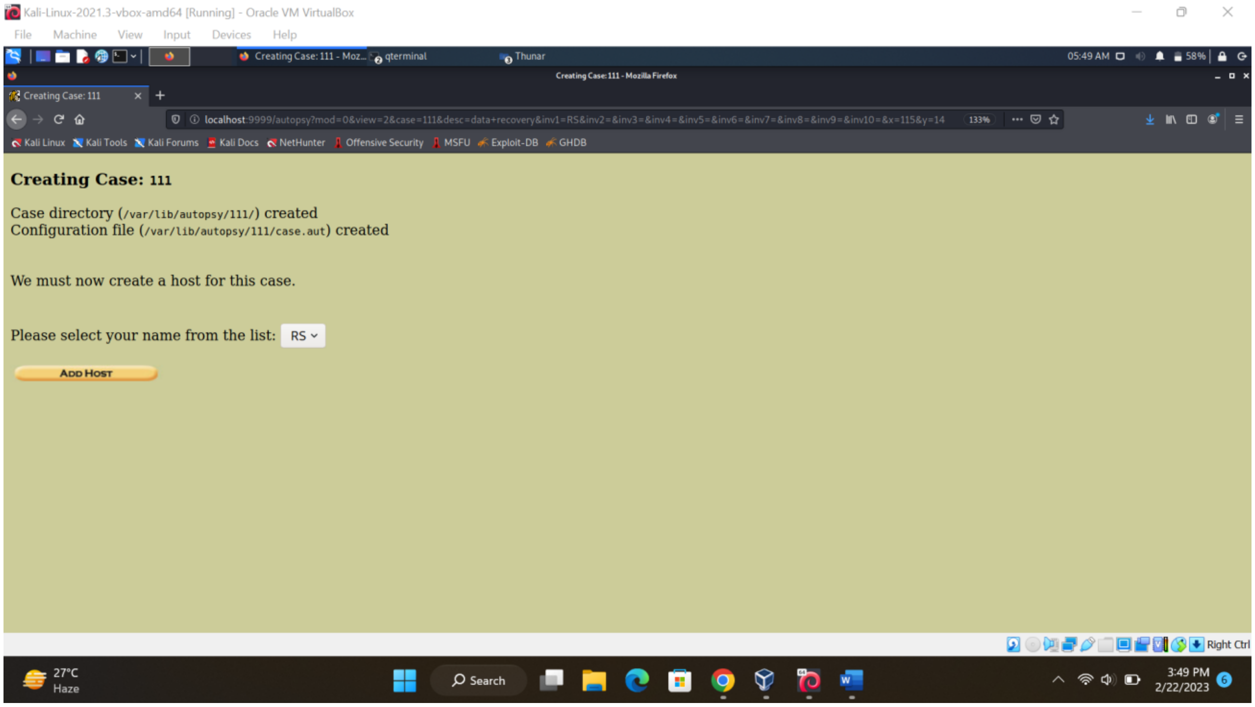
111

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

data recovery

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

a. RS
b.
c.
d.
e.
f.
g.
h.
i.
j.


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Creating Case: 111 - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=2&case=111&desc=data+recovery&inv1=RS&inv2=&inv3=&inv4=&inv5=&inv6=&inv7=&inv8=&inv9=&inv10=&x=115&y=14
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
27°C Haze
Search
3:49 PM 2/22/2023

Creating Case: 111

Case directory (`/var/lib/autopsy/111/`) created
Configuration file (`/var/lib/autopsy/111/case.aut`) created

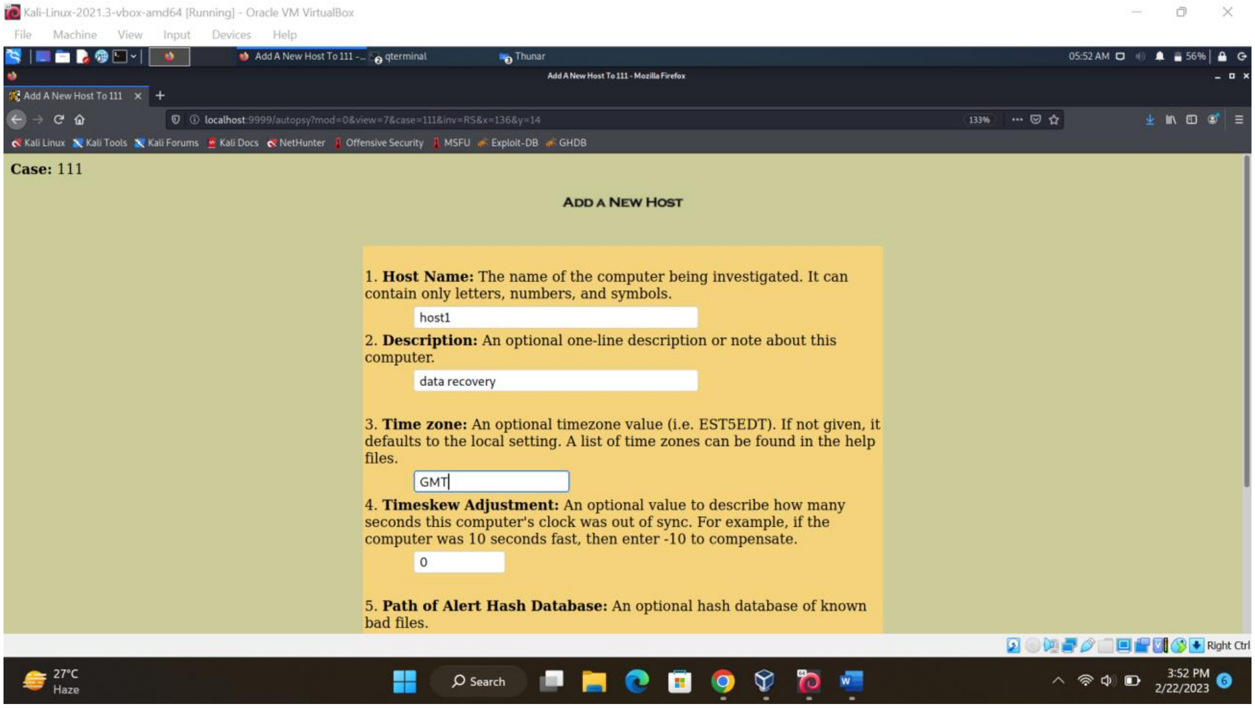
We must now create a host for this case.

Please select your name from the list: RS

ADD HOST

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.


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Add A New Host To 111 - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=7&case=111&inv=RS&x=136&y=14
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
27°C Haze
Search
3:52 PM 2/22/2023

Case: 111

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
host1

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

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.
GMT

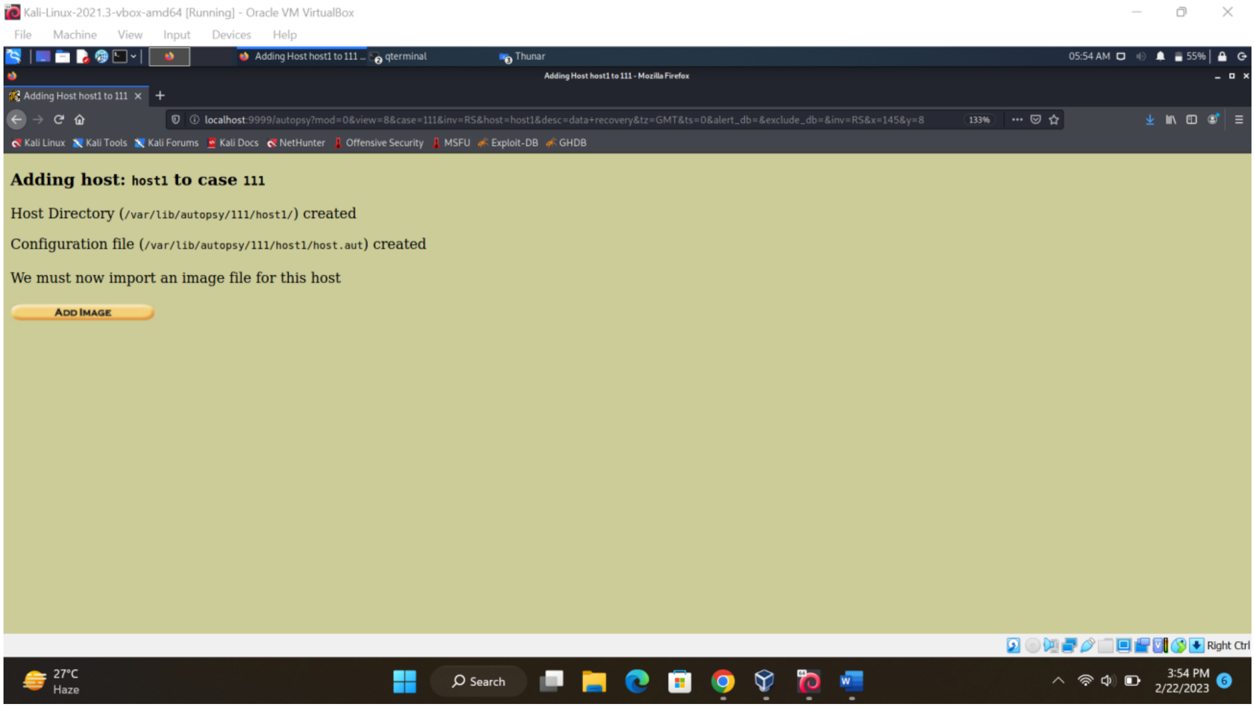
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0

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

Here we can add the hostname ***(host1),*** a description ***(data 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.

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.***



Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Adding Host host1 to 111 ...
qterminal
Thunar
05:54 AM
Adding Host host1 to 111 - Mozilla Firefox
Adding Host host1 to 111
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
133%
Right Ctrl
27°C
Haze
Search
3:54 PM
2/22/2023

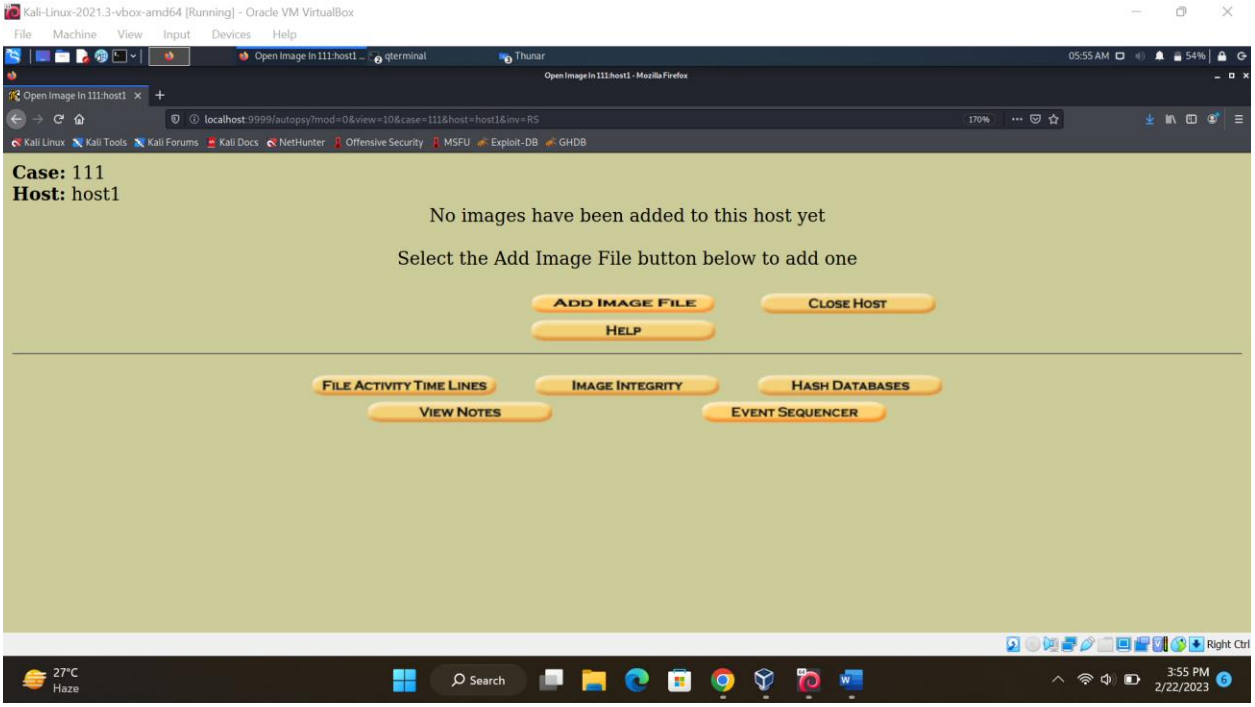
localhost:9999/autopsy?mod=0&view=8&case=111&inv=RS&host=host1&desc=data+recovery&tz=GMT&ts=0&alert_db=&exclude_db=&inv=RS&x=145&y=8

Adding host: `host1` to case `111`

Host Directory (`/var/lib/autopsy/111/host1/`) created

Configuration file (`/var/lib/autopsy/111/host1/host.aut`) created

We must now import an image file for this host

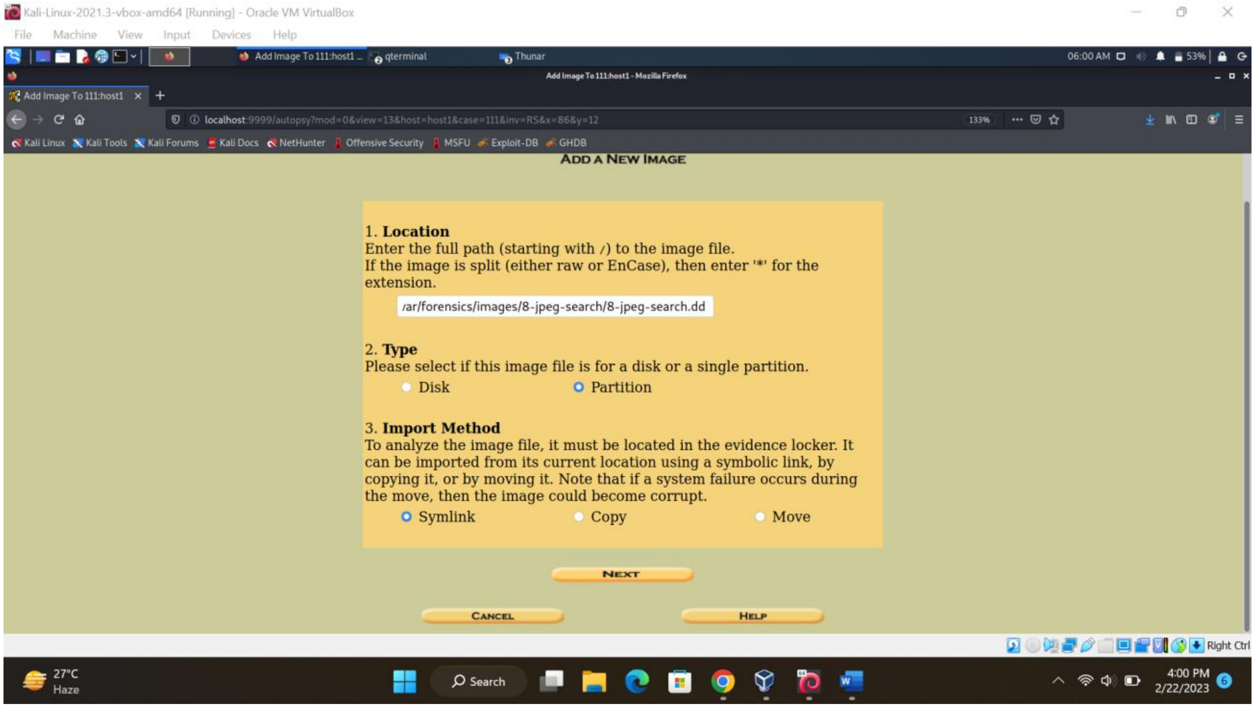


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Open Image In 111:host1 - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=10&case=111&host=host1&inv=RS
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
27°C Haze
Search
3:55 PM 2/22/2023

Case: 111
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one



Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Add Image To 111:host1 - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=13&host=host1&case=111&inv=RS&x=86&y=12
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
NEXT
CANCEL
HELP
27°C Haze
Search
4:00 PM 2/22/2023

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.

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

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

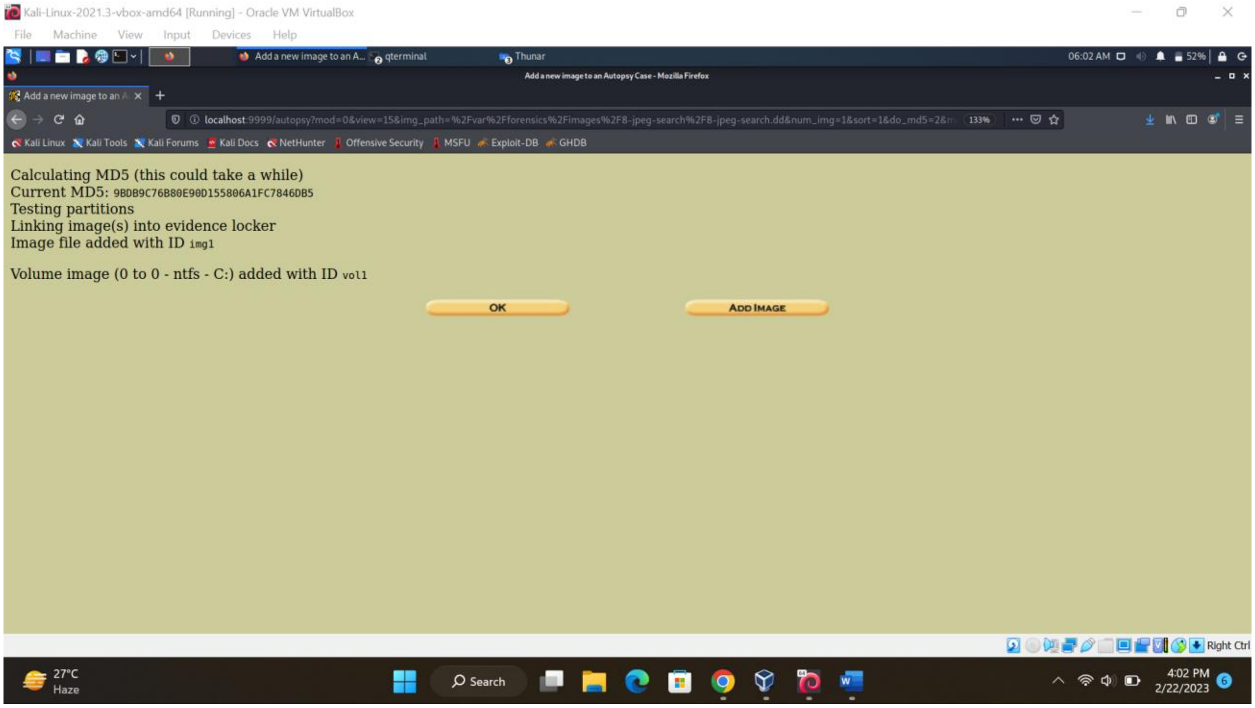
Whenever we are creating an image or saving an image that might be used in any legal proceeding, it is critical we maintain the integrity of the image. This means we can prove that the image has not been tampered with from the time the image was captured until the time of the trial.

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

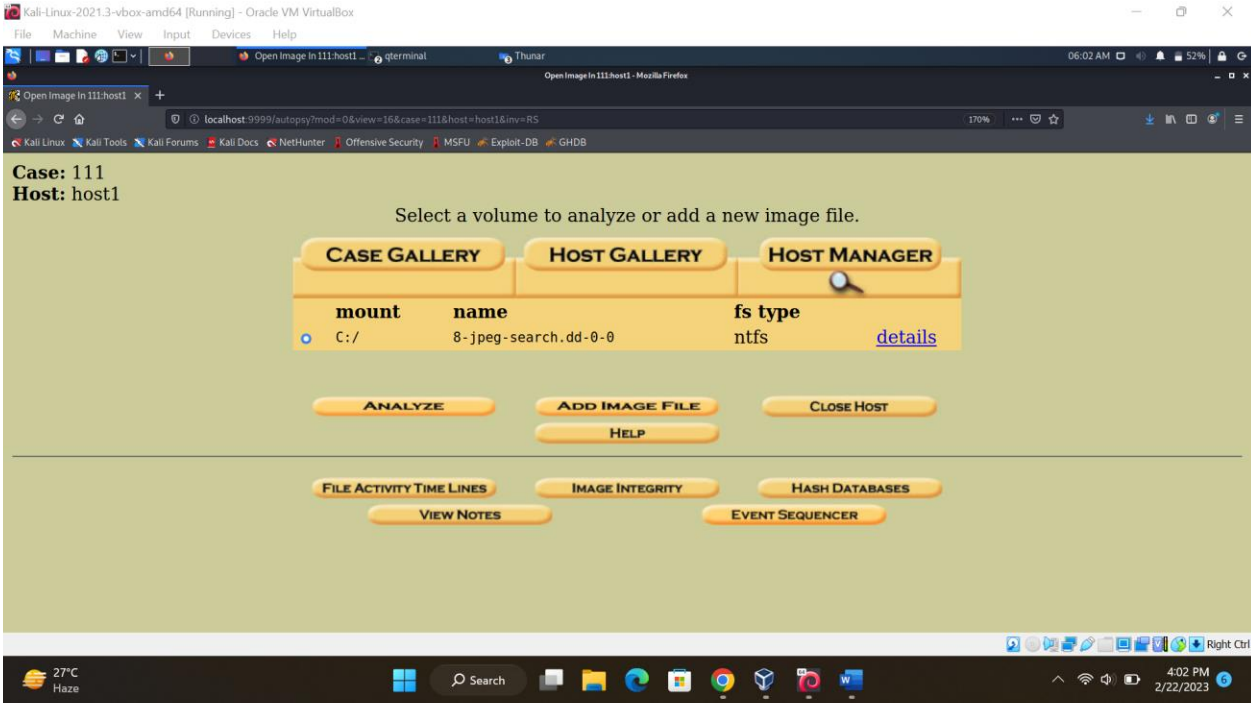
In this screen, Autopsy asks us whether we want to:

- **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.



```
Calculating MD5 (this could take a while)
Current MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Volume image (0 to 0 - ntfs - C:) added with ID vol1
```


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Open Image In 111:host1 - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=16&case=111&host=host1&inv=RS
Case Gallery
Host Gallery
Host Manager
Analyze
Add Image File
Close Host
Help
File Activity Time Lines
Image Integrity
Hash Databases
View Notes
Event Sequencer
27°C Haze
4:02 PM 2/22/2023

Case: 111
Host: host1

Select a volume to analyze or add a new image file.

	mount	name	fs type	
○	C:/	8-jpeg-search.dd-0-0	ntfs	details

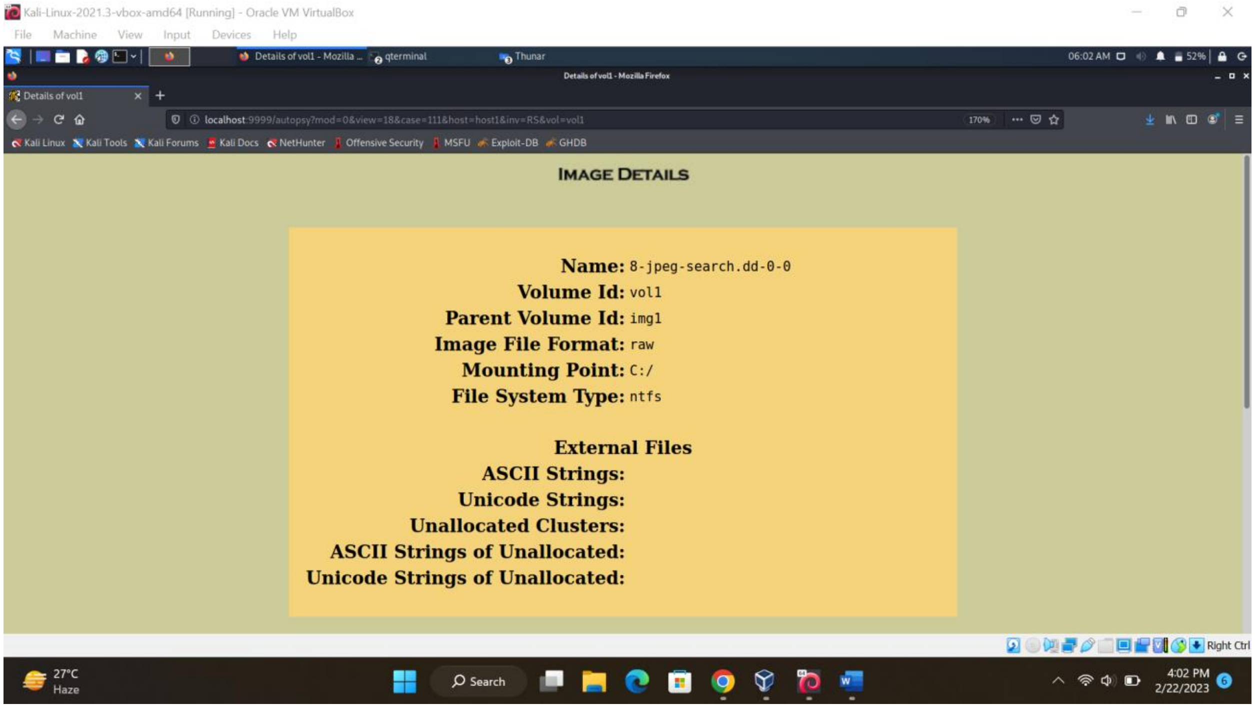
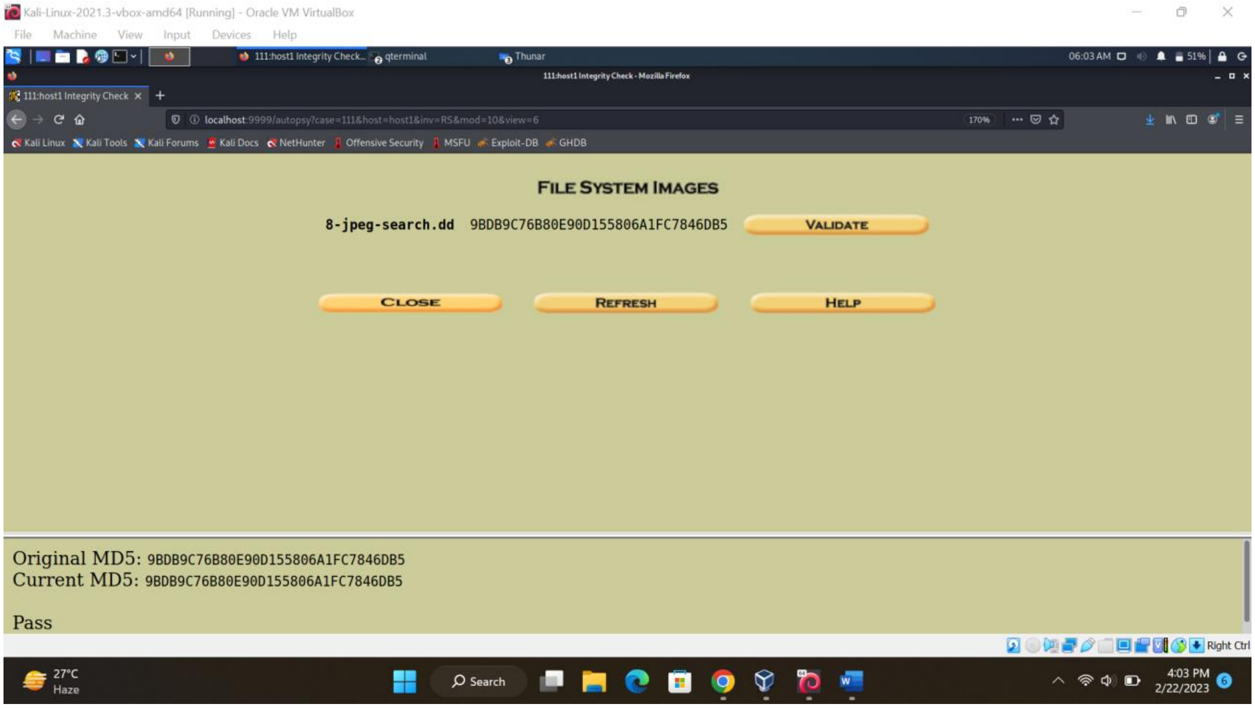

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Details of vol1 - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=18&case=111&host=host1&inv=RS&vol=vol1
27°C Haze
4:02 PM 2/22/2023

IMAGE DETAILS

Name: 8-jpeg-search.dd-0-0
Volume Id: vol1
Parent Volume Id: img1
Image File Format: raw
Mounting Point: C:/
File System Type: ntfs

External Files
ASCII Strings:
Unicode Strings:
Unallocated Clusters:
ASCII Strings of Unallocated:
Unicode Strings of Unallocated:

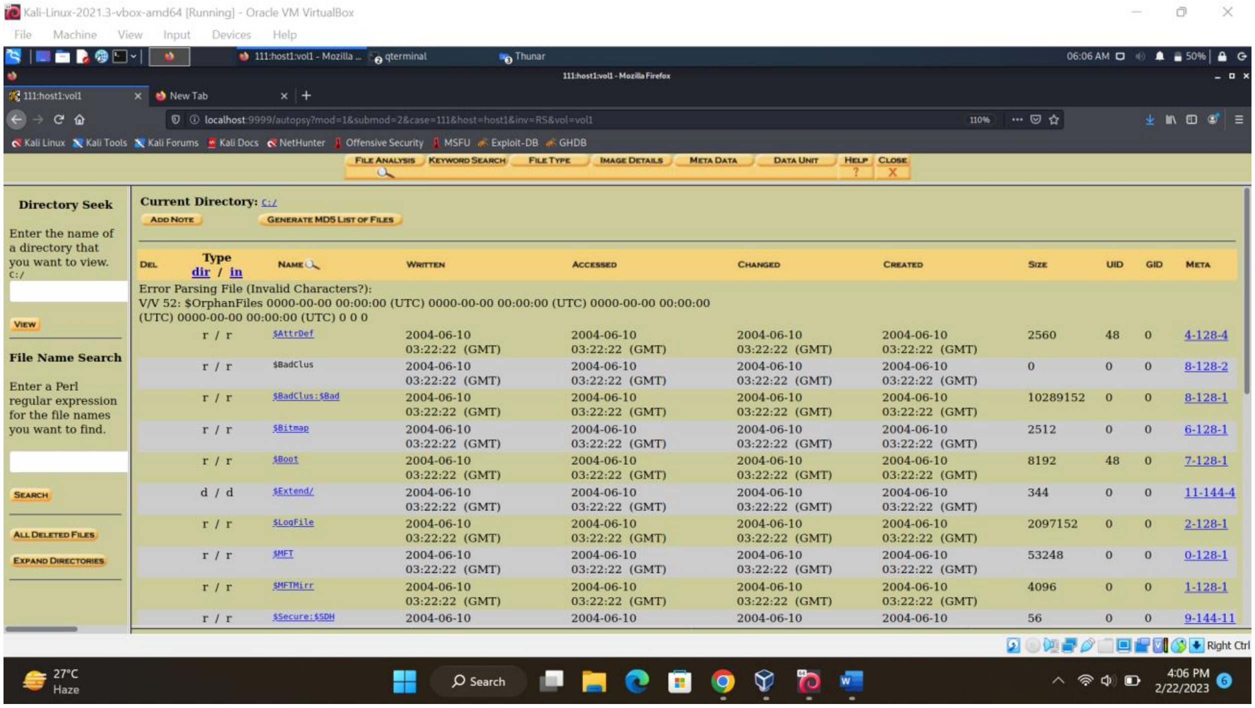
Now validate the integrity.


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
111:host1 Integrity Check - Mozilla Firefox
localhost:9999/autopsy?case=111&host=host1&inv=RS&mod=10&view=6
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
CLOSE
REFRESH
HELP
VALIDATE
27°C Haze
Search
4:03 PM 2/22/2023

FILE SYSTEM IMAGES

8-jpeg-search.dd 9BDB9C76B80E90D155806A1FC7846DB5

```
Original MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Current MD5: 9BDB9C76B80E90D155806A1FC7846DB5

Pass
```


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
111:host1:vol1 - Mozilla Firefox
New Tab
localhost:9999/autopsy?mod=1&submod=2&case=111&host=host1&inv=RS&vol=vol1
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
ADD NOTE
GENERATE MD5 LIST OF FILES
VIEW
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
27°C Haze
Search
4:06 PM 2/22/2023

Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

Current Directory: C:/

Error Parsing File (Invalid Characters?):
V/V 52: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	$AttrDef	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2560	48	0	4-128-4
	r / r	$BadClus	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	0	0	0	8-128-2
	r / r	$BadClus:$Bad	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	10289152	0	0	8-128-1
	r / r	$Bitmap	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2512	0	0	6-128-1
	r / r	$Boot	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	8192	48	0	7-128-1
	d / d	$Extend/	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	344	0	0	11-144-4
	r / r	$LogFile	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2097152	0	0	2-128-1
	r / r	$MFT	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	53248	0	0	0-128-1
	r / r	$MFTMirr	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	2004-06-10 03:22:22 (GMT)	4096	0	0	1-128-1
	r / r	$Secure:$SDH	2004-06-10	2004-06-10	2004-06-10	2004-06-10	56	0	0	9-144-11

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!