Lab Requirements

1. Microsoft Windows virtual machine
2. Kali Linux virtual machine
3. [Optional] A machine running macOS

Content

Part I: Hash Functions on Windows, macOS, and Linux [Revisited]

STEP 1: To obtain the hash value of a file in *Windows command prompt*, use the following command.

```
# Compute the hash value of a file
# Supported hash functions: MD2, MD4, MD5, SHA1, SHA256, SHA384, and SHA512
C:\tools\images> certutil -hashfile img1.jpg sha384
    SHA384 hash of img1.jpg:
    5059877992c2799cb22bc478f10d52b1875ba3a2568ef681423a6ab3a914cb1a813cd5d16a56
    f648288701d0ba06fa73
    CertUtil: -hashfile command completed successfully.

# Compute the hash values of a list of files
C:\tools\images> FORFILES /M *.jpg /C "cmd /C certutil -hashfile @FILE"
   SHA1 hash of img.jpg:
   48e1934cedd901c1422c97788651aa6399af7b28
   CertUtil: -hashfile command completed successfully.
   SHA1 hash of img1.jpg:
   7513b0fa2282c4864c62735b8e9a66881608f3fa
   CertUtil: -hashfile command completed successfully.
```

STEP 2: To obtain the hash value of a file in *Windows PowerShell*, use the following command.

```
# Compute the hash value of a file or a group of files
# Supported hash functions: MACTRIPLEDES, MD5, RIPEMD160, SHA1, SHA256, SHA384,  #
SHA512
PS C:\tools\images> Get-FileHash -A SHA1 *.jpg

   Algorithm       Hash                                   Path
   ---------       ----                                   ----
   SHA1     48E1934CEDD901C1422C97788651AA6399AF7B28   C:\tools\images\img.jpg
   SHA1     7513B0FA2282C4864C62735B8E9A66881608F3FA   C:\tools\images\img1.jpg
   SHA1     B1BFB5AF1488C3779635F8ECEEEF0737BEC79875   C:\tools\images\img3.jpg
   SHA1     7433C01CC1CFD1E8C163D45A5DFE101983A93C32   C:\tools\images\img4.jpg
```

STEP 3: To obtain the hash value of a file in *macOS*, use the following command.

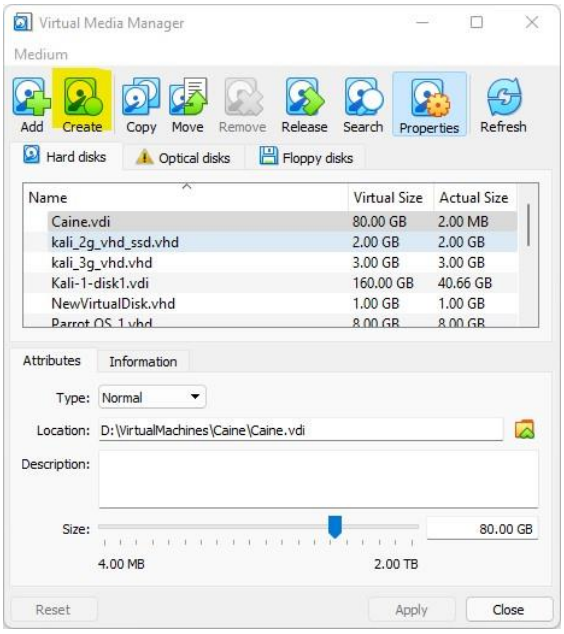
```
# Compute the hash value of a string, file or a list of files using shasum
(base)     Adam:tools     adam     $          printf     hello     |     shasum
   aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d  -

# shasum hash functions -a 224, 256, 384, 512
(base) Adam:tools adam $  shasum -a 224 *.txt
   150113ac08fffedb561cde7708ee30beb059a59a1f057ad29fb0b8a7  forensics.txt

(base) Adam:tools adam $  md5 *.txt
   MD5 (forensics.txt) = b5a6a1c1876747056863492c651305b7

# Compute hash values using the openssl library
(base) Adam:tools adam $  openssl dgst -list
   Supported digests:
   -blake2b512               -blake2s256               -md4
   -md5                      -md5-sha1                 -mdc2
   -ripemd                   -ripemd160                -rmd160
   -sha1                      -sha224                    -sha256
   -sha3-224                 -sha3-256                 -sha3-384
   -sha3-512                 -sha384                   -sha512
   -sha512-224               -sha512-256               -shake128
   -shake256                 -sm3                      -ssl3-md5
   -ssl3-sha1                -whirlpool

(base) Adam:tools adam $  openssl dgst -sha3-224 *.txt

   SHA3-224(forensics.txt)=
   b535386b7b787a0579a1d3f1fa8b4649df062655ec97ced5ba65c197
```

STEP 4: To obtain the hash value of a file in *Linux*, use the following command.

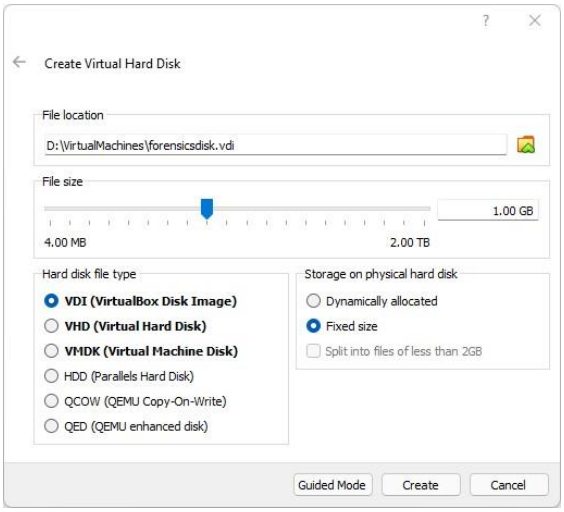
```
# Available hash functions: md5sum, sha1sum, sha224sum, sha256sum, sha384sum,
# sha526sum
kali@kali)-[~] printf hello | sha1sum aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d
   -

kali@kali)-[~] openssl dgst -sha3-224 *.txt SHA3-224(file1.txt)=
   e2562f9498a4968fca5eaaae689bcda379a9fb8150e92261db57b339
   SHA3-224(file2.txt)=
   29f028dcc24927071ab152284f034338b8f249cb2c2b7ef7d82ec276
```

Part II: Creating a Virtual Hard Drive and Attaching it to a VM using Oracle VirtualBox

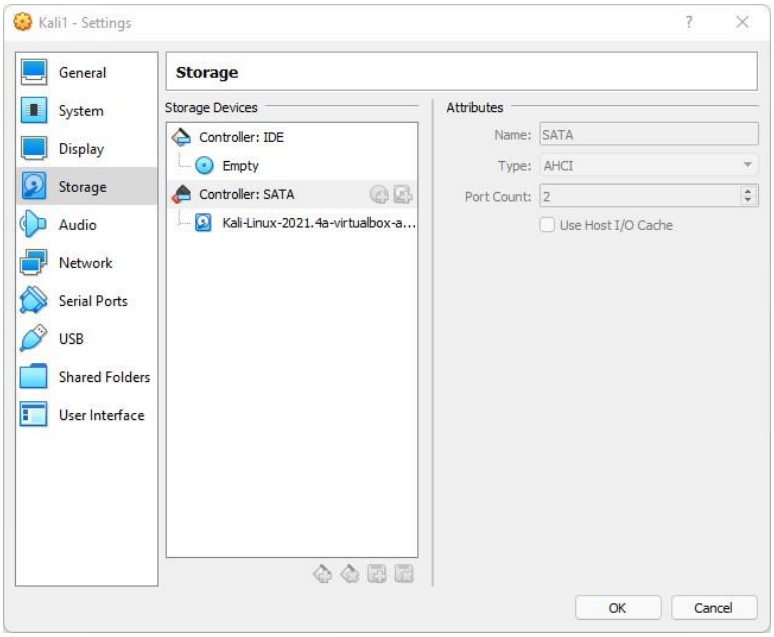
STEP 5: On the main interface on VirtualBox, go to FILE and select VIRTUAL MEDIA MANAGER. Instead, the VIRTUAL MEDIA MANAGER can be opened by clicking [CTRL + D].



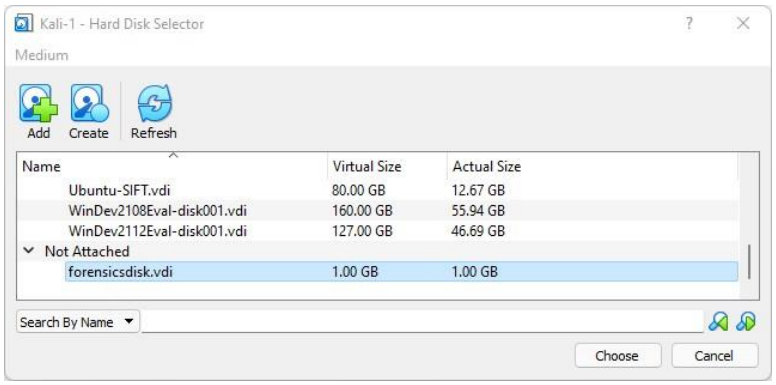
STEP 6: Click on CREATE to create a new virtual media. In the next interface, click on the EXPERT MODE button. Select the NAME of the drive, file TYPE, file SIZE (1 GB), and set the drive to be of FIXED SIZE. Click on the CREATE button to create the new disk. Close the VIRTUAL MEDIA MANAGER.



STEP 7: Got the settings of the VM to which you intend to attach the created virtual disk. Under STORAGE, click on "CONTROLLER: SATA" and click on "ADDS HAD DISK."



STEP 8: Scroll down to display the list of "NOT ATTACHED" disks, where the disk created in previous steps will be listed. Select on the unattached drive and click on CHOOSE.

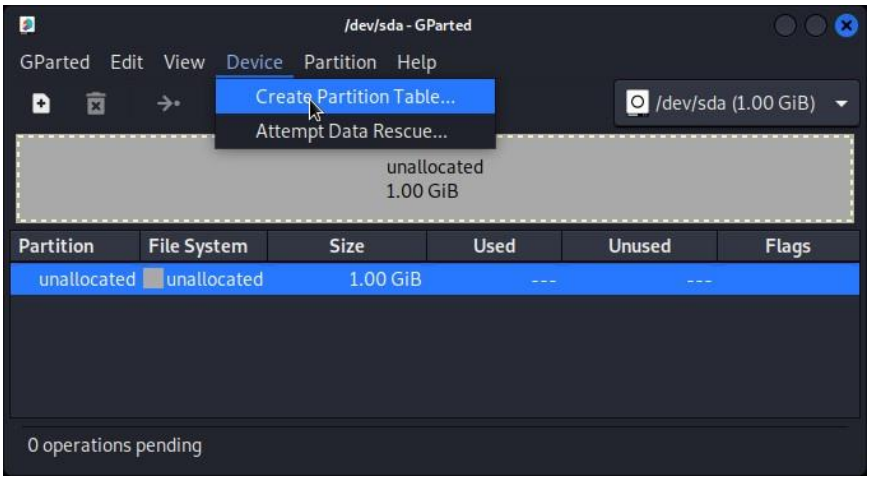


STEP 9: Assume that you only have two hard disks; the bootable hard disk and the one created in the previous steps. Power on the Kali VM and type the following commands. Note that the disk **/DEV/SDA** is not formatted yet (does not have a defined file system) nor it has any partitions.

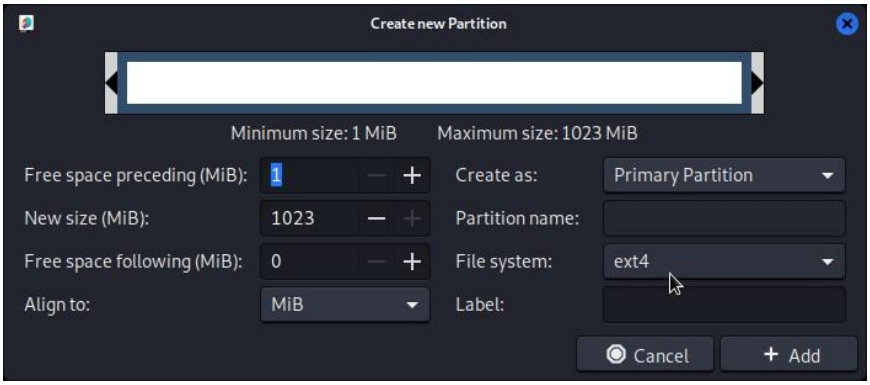
```
# list the recognized disks
kali@kali)-[~] sudo lshw -class disk -short
   H/W path          Device      Class       Description
   ====================================================
   /0/100/1.1/0.0.0  /dev/cdrom  disk        CD-ROM
   /0/100/d/0        /dev/sdb    disk        85GB VBOX HARDDISK
   /0/100/d/1        /dev/sda    disk        1073MB VBOX HARDDISK

kali@kali)-[~] sudo lshw -class volume -short
   H/W path          Device      Class       Description
   ====================================================
   /0/100/d/0/1      /dev/sdb1   volume      79GiB EXT4 volume
   /0/100/d/0/2      /dev/sdb2   volume      975MiB Extended partition
   /0/100/d/0/2/5    /dev/sdb5   volume      975MiB Linux swap volume
```

STEP 10: To partition the disk **/DEV/SDA**, use **GPARTED** visual program. To do that, type the following command. The following interface is displayed. Select the **/DEV/SDA** drive and select **CREATE PARTITION TABLE…** from the **DEVICE** menu.

```
kali@kali)-[~] sudo gparted
```

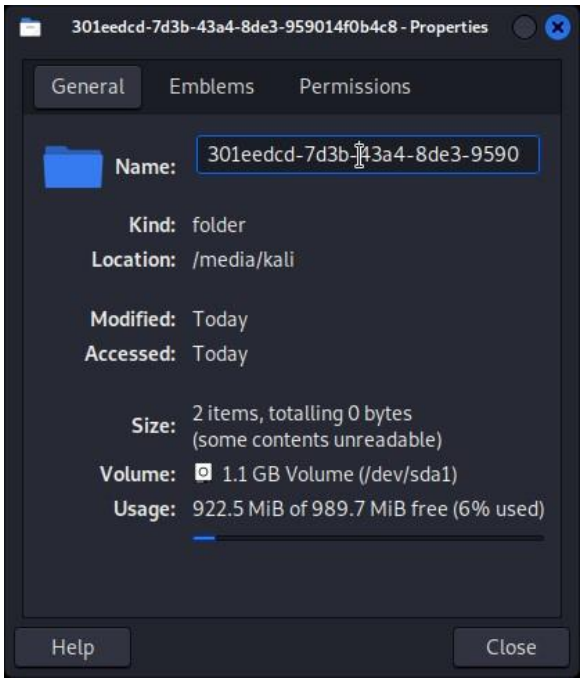


STEP 11: After the previous step is complete, right-click on unallocated partition and select **NEW**. From the **FILE SYSTEM** list, select ext4 (Linux file system), and click on **+ ADD**. Click on "**APPLY ALL OPERATIONS**" and close the **GPARTED** utility.



STEP 12: After the previous step is complete, type the following command and remark the difference with the results obtained in **STEP 9**.

```
# list the recognized disks
kali@kali)-[~] sudo lshw -class volume -short
   H/W path          Device      Class       Description
   ========================================================
   /0/100/d/0/1      /dev/sdb1   volume      79GiB EXT4 volume
   /0/100/d/0/2      /dev/sdb2   volume      975MiB Extended partition
   /0/100/d/0/2/5    /dev/sdb5   volume      975MiB Linux swap volume
/0/100/d/1/1      /dev/sda1   volume      1023MiB EXT4 volume
```



STEP 13: To display **/DEV/SDA1** volume's name, type the following command. Remark that the volume does not have a name and its UUID will be displayed as its name, and the UUID will be the name of the folder created under **/MEDIA/KALI**, where the volume is mounted. Use the commands **FINDMNT**, **MOUNT** or **DF** to display the mounting locations of volumes.

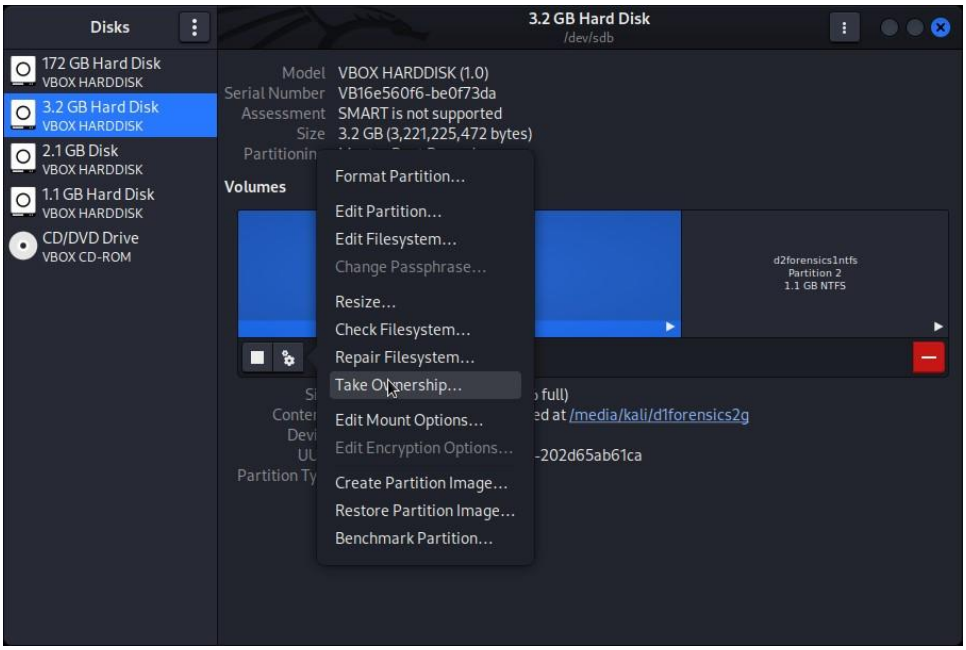
```
# The following is a selected list of the displayed results
kali@kali)-[~] sudo tune2fs -l /dev/sda1  tune2fs 1.46.4
(18-Aug-2021)
   Filesystem volume name:   <none>
   Last mounted on:          <not available>
   Filesystem UUID:          301eedcd-7d3b-43a4-8de3-959014f0b4c8
   Filesystem OS type:       Linux
   Filesystem created:       Tue Feb  8 00:27:26 2022
   Last mount time:          Tue Feb  8 00:38:10 2022
   Last write time:          Tue Feb  8 00:38:10 2022

# a shortened output is displayed below kali@kali)-[~]
df
   Filesystem     1K-blocks    Used Available Use% Mounted on
   /dev/sdb1       81000912 9935188  66905112  13% /
   /dev/sda1        1013420      24    944636   1% /media/kali/301eedcd-7d3b-
   43a4-8de3-959014f0b4c8
```

STEP 13: Type the following commands to change the volume's name to **A1FORENSIC1G**. After rebooting the system in **LINE 6**, click on the **A1FORENSIC1G** drive located on the desktop to mount it.

```
# The following is a selected list of the displayed results
kali@kali)-[~] sudo tune2fs -L a1forensics1g /dev/sda1 tune2fs
1.46.4 (18-Aug-2021)

# reboot the system kali@kali)-[~]
reboot

# a shortened output is displayed below
kali@kali)-[~] df
Filesystem     1K-blocks    Used Available Use% Mounted on
/dev/sdb1       81000912 9935188  66905112  13% /
/dev/sda1        1013420      24    944636   1% /media/kali/a1forensics1g
```

STEP 14: You can the above and more functionalities using the gnome-disk-utility. An interesting functionality of this utility is to Take Ownership of the partition to avoid writing errors.

```

kali@kali)-[~] sudo apt-get upgrade

kali@kali)-[~] sudo apt-get install gnome-disk-utility
# Run the utility kali@kali)-[~]
gnome-disks

```



Part III: Sanitizing the Target Media

STEP 15: Use the command dd to sanitize the media volume before copying content to it. In the following command, random values are generated using the **/DEV/RANDOM** device and copied to the /**DEV/SDA1** volume. You might wish to use **/DEV/ZERO** to overwrite the partition with zeros.

NOTE 15-1: Wiping the partition deletes the file system.

```
# status=progress shows the progress of the wiping operation
kali@kali)-[~] sudo dd if=/dev/random of=/dev/sda1 bs=1M status=progress
   939524096 bytes (940 MB, 896 MiB) copied, 3 s, 313 MB/s dd:
   error writing '/dev/sda1': No space left on device
   1024+0 records in
   1023+0 records out
   1072693248 bytes (1.1 GB, 1023 MiB) copied, 3.87043 s, 277 MB/s

# Copy 0 values to the target volume/disk kali@kali)-[~]
sudo dd if=/dev/zero of=/dev/sda1 bs=1M
```

STEP 16: Use the command dcfldd to wipe the content of a drive/partition with a given a pattern.

```
# status=progress shows the progress of the wiping operation  kali@kali)-[~]
sudo dcfldd pattern=AAAA of=/dev/sda1 bs=1M
```

NOTE 15-1: Create a new partition after wiping the content of the partition. Use gparted.

Part IV: Linux Image Carving using recoverjpeg Tool

STEP 17: Download the following two folders, unzip their contents, and copy their content to the partition /dev/sda1. These are sample files which we will be working with. You can copy any other files of your choice. The first folder contains 980 files of different formats and the second folder contains 221 .jpg files.

FOLDER 1: https://digitalcorpora.s3.amazonaws.com/corpora/files/govdocs1/zipfiles/101.zip

FOLDER 2: http://lci.micc.unifi.it/labd/cmfd/MICC-F220.zip

STEP 18: Assume that you have downloaded the above two folders to the Downloads folder on your home directory (/home/kali/Downloads/). After unzipping the files, copy the unzipped folders to the destination volume /dev/sda1 (or any name it the 1GB partition is given on your system).

```
# status=progress shows the progress of the wiping operation
kali@kali)-[~] cd Downloads kali@kali)-[~/Downloads] unzip
101.zip kali@kali)-[~/Downloads] unzip MICC-F220.zip
```

NOTE 17-1: You can use the command MV to move the folders, using the graphical user interface where you can copy the folders manually to the destination media.

STEP 19: Change the working folder to the mounting folder of the created disk. Delete all the .jpg files located in in both folders. After running these commands, the partition will not contain any .jpg files.

```
# Change the woring directory to the mounting point of the extra disk we
# defined in early steps.
kali@kali)-[~] cd /media/kali/a1forensics1g

#  list  the  content  of  the  partition
kali@kali)-[/media/kali/a1forensics1g] ls
101  lost+found  MICC-F220


kali@kali)-[/media/kali/a1forensics1g] cd MICC-F220

# Count the number of .jpg files in the folder kali@kali)-
[/media/kali/a1forensics1g/MICC-F220] ls -l | grep .jpg | wc -l 221

# Delete all .jpg files from this folder kali@kali)-
[/media/kali/a1forensics1g/MICC-F220] sudo rm *.jpg
# Count the number of .jpg files in the folder (after deleting them)
kali@kali)-[/media/kali/a1forensics1g/MICC-F220] ls -l | grep .jpg | wc -l
0

# Do the same for the second folder kali@kali)-
[/media/kali/a1forensics1g/MICC-F220] cd ../101
# Count the number of .jpg files in the folder kali@kali)-
[/media/kali/a1forensics1g/101] ls -l | grep .jpg | wc -l 7

# Delete all .jpg files from this folder kali@kali)-
[/media/kali/a1forensics1g/101] sudo rm *.jpg
# Count the number of .jpg files in the folder (after deleting them)
kali@kali)-[/media/kali/a1forensics1g/101] ls -l | grep .jpg | wc -l 0
```

```
36
37 # Display the number of files in the 101 folder (non-jpeg files)
38 kali@kali)-[/media/kali/a1forensics1g/101] ls -l | wc -l 974
```

STEP 20: Create a new folder to store carved .jpg media files.

```
1 # Run the two commands in order from left to right using the && operator
2 kali@kali)-[ /media/kali/a1forensics1g/101] mkdir jpegrecovery && cd
3 ../jpegrecovery kali@kali)-[ /media/kali/a1forensics1g/jpegrecovery] ls
4 -l
```

STEP 21: Update the system and install recoverjpeg.

```
1 # Update the Linux system  kali@kali)-[ /media/kali/a1forensics1g] sudo
2 apt-get upgrade -y kali@kali)-[ /media/kali/a1forensics1g] sudo apt-get
3 install recoverjpeg -y
```

STEP 22: Use recoverjpeg to recover deleted .jpg files.

```
1
2 # Run recoverjpeg: -o option is used to provide the destination folder
3 kali@kali)-[ /media/kali/a1forensics1g] sudo recoverjpeg /dev/sdb1 o
4 ./jpegrecovery
5 Restored 228 pictures
6
7 # count the number of recovered image files kali@kali)-[
8 /media/kali/a1forensics1g] ls -l ./jpegrecovery/*.jpg | wc -l 228
```

Part V: Data Recovery using foremost Tool

STEP 22: Unlike recoverjpeg which can be sued to recover .jpg files, foremost is sued to recovered a long list of file formats, including jpg, gif, png, avi, mov, exe, pdf, doc, and zip. Use the -t option to specify the desired file extensions of the files to be recovered. The tool foremost was created by special agents Kris Kendall and Jesse Kornblum of the U.S. Air Force Office of Special Investigations. Type the following commands to install foremost.

```
1 # Update the Linux system & install foremost kali@kali)-[
2 /media/kali/a1forensics1g] sudo apt-get upgrade -y kali@kali)-[
3 /media/kali/a1forensics1g] sudo apt-get install foremost -y
```

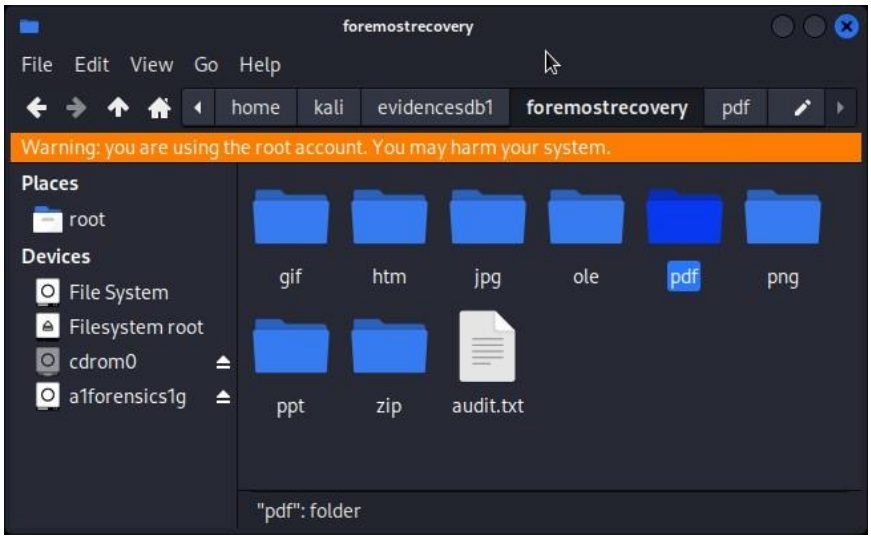
STEP 23: Delete all the files and folders on the partition /dev/sdb1/. You should open the mounting folder as a Root to be able to delete all files and directories.

STEP 24: Create a raw image of the /dev/sdb1 partition to be used in the following data recovery steps. You can use either dd or dcfldd (DCFL: Department of Defense Computer Forensics Lab).

```
# Create an image and store the image on the main partition kali@kali)-
[/media/kali/a1forensics1g] cd ~ && mkdir evidencesdb1 kali@kali)-[~] sudo
dcfldd if=/dev/sdb1 of=./evidencesdb1/sdb1image.dd hash=sha1
hashlog=./evidencesdb1/hashlog.log
   [sudo] password for kali:
   32512 blocks (1016Mb) written.
   32736+0 records in
   32736+0 records out
    kali@kali)-[~] ls
evidencesdb1 hashlog.log
sdb1image.dd
    kali@kali)-[~] cat
./evidencesdb1/hashlog.log
   Total (sha1): 53458640106f3e2b595dbbe5d243534187dbcc6d
```

STEP 25: Get familiar with the capabilities and usage of foremost by typing `man foremost`. Use foremost to recover the content of the partition. After the following command is completed, navigate to the output folder and check its contents. The audit.txt file contains information about the number of recovered files of each file format. The Microsoft documents are recovered as OLE files. The names of the recovered files are assigned sequentially and don't match the names of the original files on the investigated media.

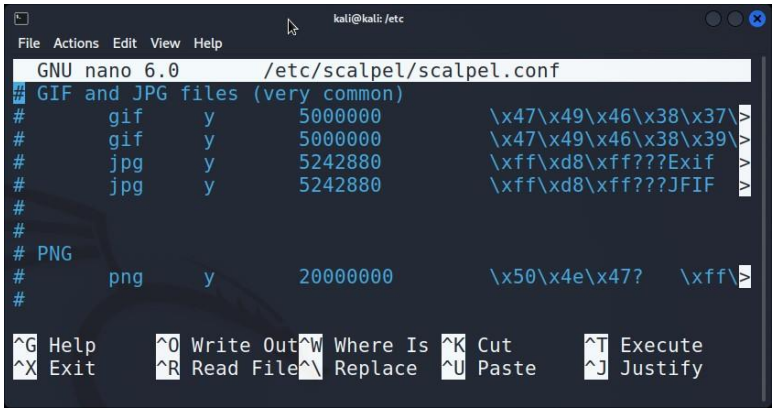
```
kali@kali)-[~] sudo foremost -t all -i ./evidencesdb1/sdb1image.dd o
./evidencesdb1/foremostrecovery
```



Part VI: Data Recovery using scalpel Tool

STEP 26: Scalpel is an efficient tool that performs similar tasks to those of foremost. Type the following commands to download scalpel. You should specify the file formats to be carved by scalpel in the configuration file whose path is /etc/scalpel/scalpel.conf (shown below). To recover a certain file type, uncomment the corresponding line – lines contains file format, header and footer.

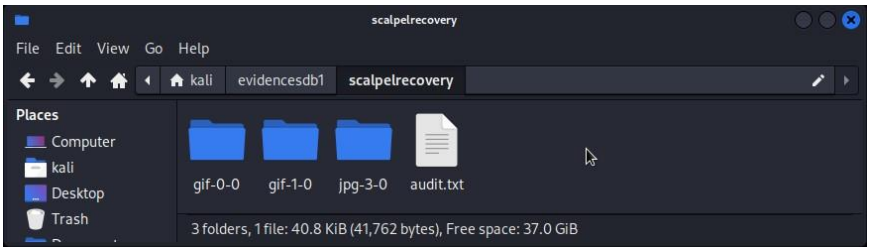
```
kali@kali)-[~] sudo apt-get upgrade -y kali@kali)-[~]
sudo apt-get install scalpel -y
```



STEP 27: Type the following command to retrieve the selected file formats. Note that scalpel might carve more files than foremost. Some of these files might be incomplete. Verify the carved data by navigating to the output directory.

```
kali@kali)-[~] sudo scalpel -
o  ./evidencesdb1/scalpelrecovery/ ./evidencesdb1/sdb1image.dd

    Opening target "/home/kali/evidencesdb1/sdb1image.dd"
    Image file pass 1/2.
    ./evidencesdb1/sdb1image.dd: 100.0%
    |************************************************************| 1023.0
    MB    00:00 ETAAllocating work queues...
    Work queues allocation complete. Building carve lists...
    Carve lists built.  Workload:
    gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 4
    files gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b"
    --> 4 files jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66"
    and footer "\xff\xd9" --> 0 files
```

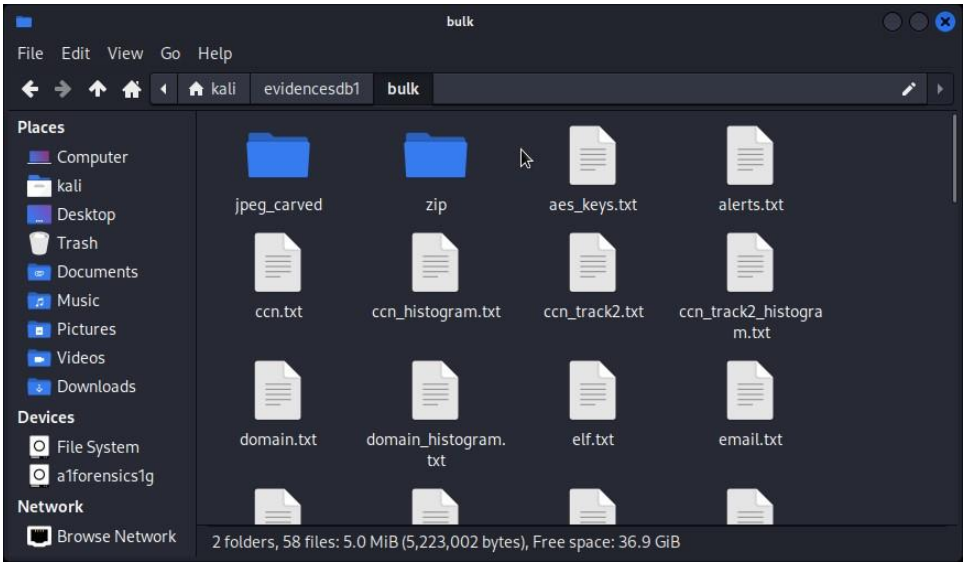
```
    jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer
    "\xff\xd9" --> 670 files Carving
    files from image.
    Image file pass 2/2.
    ./evidencesdb1/sdb1image.dd: 100.0%
    |*************************************************************| 1023.0
    MB    00:00 ETAProcessing of image file complete. Cleaning up...
    Done.
    Scalpel is done, files carved = 678, elapsed = 43 seconds.
```



Part VII: Data Recovery and Information Retrieval using bulk_extractor

STEP 28: Scalpel and foremost are great tools to retrieve files stored on suspect drives and volumes. In addition to files, more information, including email addresses, encryption keys, domain names, credit card numbers, among others can also be stored on suspect media. Such information can be recovered using bulk_extractor. Type the following command to extract more information from the suspect sdb1image.dd image.

```
kali@kali)-[~] sudo bulk_extractor -
o ./evidencesdb1/bulk ./evidencesdb1/sdb1image.dd
```


bulk
File Edit View Go Help
kali
evidencesdb1
bulk
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
a1forensics1g
Network
Browse Network
jpeg_carved
zip
aes_keys.txt
alerts.txt
ccn.txt
ccn_histogram.txt
ccn_track2.txt
ccn_track2_histogram.txt
domain.txt
domain_histogram.txt
elf.txt
email.txt
2 folders, 58 files: 5.0 MiB (5,223,002 bytes), Free space: 36.9 GiB