Report 5

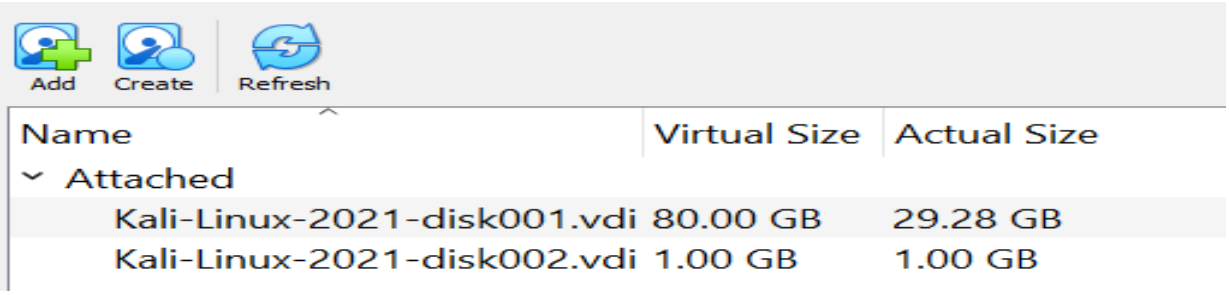
For this week's lab, the focus was on Data Acquisition and Analysis using Kali Linux. Part 1 of the lab involved an overview of creating hash functions on Linux and Windows. The second part involved creating a Virtual Hard Drive for the VM to use for the lab. Part 3 then involved sanitizing the media. Part 4 was the section where we used Linux Carving to recover images using the recoverjpeg tool. Part 5 used the foremost tool for data recovery. Part 6 used the scalpel tool for data recovery. The last part involved using the bulk_extractor for data recovery and information retrieval.

Part 1 was an overview of creating hashing functions on Linux. I used **printf hello | sha1sum** and **openssl dgst -sha3-224 *.txt** commands to verify my hash function were working properly.

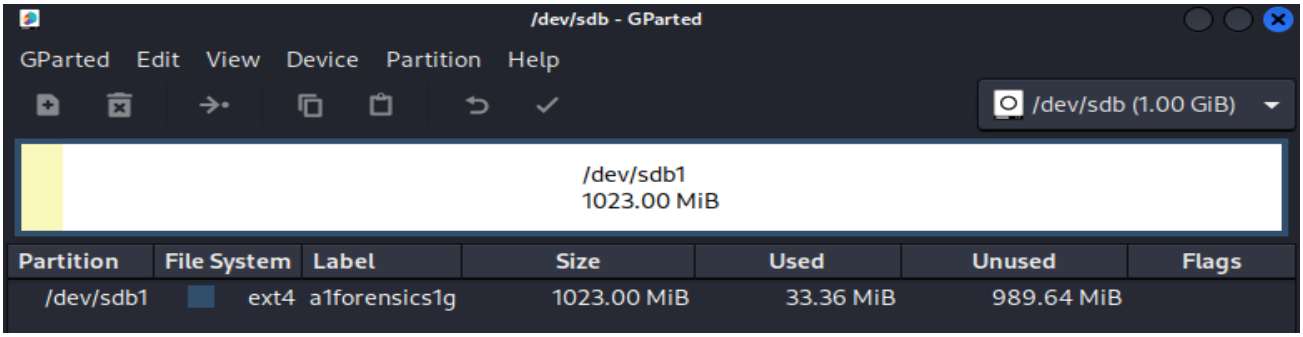
```
┌──(kali㉿kali)-[~]
└─$ print hello world | sha1sum
22596363b3de40b06f981fb85d82312e8c0ed511  -

┌──(kali㉿kali)-[~]
└─$ openssl dgst -sha3-224 *.txt
SHA3-224(10-million-password-list-top-1000000.txt)= 1b7b4ba76fb8fbb4d99c18a8266f0b84b7e2620b83d4dbf64411b89f
SHA3-224(file1.txt)= c26ffff22d5f4adc95a446d4eb95ea0d7081a53b0ca51acdeb6fa874
SHA3-224(hash.txt)= 719555611332720ed39fef9ce0307bc064a55b4ab62adfe0eb2888fb
SHA3-224(Test.txt)= c68dc338df1b3ede5f269b77600316458c0275d73acc8ec7df09477b
```

Part 2, I needed to create the VHD for this lab. In the VM setting, I made a 1 GB virtual drive that I will be using for the rest of the parts for this lab.



I then created the partition table using the **sudo gparted** command and used the ext4 file system. This drive is sdb1.



I verified to see if I created the drive using the **sudo lshw -class volume -short** command.

```
┌──(kali㉿kali)-[~]
└─$ sudo lshw -class volume -short
H/W path          Device      Class       Description
==================================================
/0/100/d/0/1      /dev/sda1   volume      79GiB EXT4 volume
/0/100/d/0/2      /dev/sda2   volume      975MiB Extended partition
/0/100/d/0/2/5    /dev/sda5   volume      975MiB Linux swap volume
/0/100/d/1/1      /dev/sdb1   volume      1023MiB EXT4 volume
```

Then I changed the name of that drive to *a1forensics1g using* the **sudo tune2fs -L a1forensics1g /dev/sdb1** command

```
┌──(kali㉿kali)-[~]
└─$ sudo tune2fs -L a1forensics1g /dev/sdb1
[sudo] password for kali:
tune2fs 1.46.5 (30-Dec-2021)
```

In part 3, we need to sanitize the media so the first task was to wipe the partition. This is done by using the **sudo dd if=/dev/random of=/dev/sdb1 bs=1M status=progress** command. Doing so will delete the file system. Here below I will be using the sdb1 drive I created for this lab's data recovery.

```
┌──(kali㉿kali)-[~]
└─$ sudo dd if=/dev/random of=/dev/sdb1 bs=1M status=progress
954204160 bytes (954 MB, 910 MiB) copied, 3 s, 318 MB/s
dd: error writing '/dev/sdb1': No space left on device
1024+0 records in
1023+0 records out
1072693248 bytes (1.1 GB, 1023 MiB) copied, 3.50042 s, 306 MB/s
```

I also used the **sudo dcfldd pattern=AAAA of=/dev/sdb1 bs=1M** command to wipe the drives again using an 'AAAA' pattern. Doing this will wipe the partition table. I used sudo gparted again to create the partition table for sdb1 using the ext4 file system.

```
┌──(kali㉿kali)-[~]
└─$ sudo dcfldd pattern=AAAA of=/dev/sdb1 bs=1M
768 blocks (768Mb) written.dcfldd:: No space left on device
```

Now we can begin on part 4. The next task was to download the files that will be used for the data recovery. I used the command **wget**

https://digitalcorpora.s3.amazonaws.com/corpora/files/govdocs1/zipfiles/101.zip to download the zip file. Here below is the file saved in my Downloads directory.

```
┌──(kali㉿kali)-[~]
└─$ wget https://digitalcorpora.s3.amazonaws.com/corpora/files/govdocs1/zipfiles/101.zip                    1
--2022-09-26 23:22:56--  https://digitalcorpora.s3.amazonaws.com/corpora/files/govdocs1/zipfiles/101.zip
Resolving digitalcorpora.s3.amazonaws.com (digitalcorpora.s3.amazonaws.com)... 52.92.192.33
Connecting to digitalcorpora.s3.amazonaws.com (digitalcorpora.s3.amazonaws.com)|52.92.192.33|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 178312230 (170M) [application/zip]
Saving to: '101.zip'

101.zip                     100%[===================================================>] 170.05M  2.07MB/s    in 1m 43s

2022-09-26 23:24:39 (1.66 MB/s) - '101.zip' saved [178312230/178312230]
```

Now I go to the Downloads directory using **cd Downloads** to unzip the folder using **unzip 101.zip** command to begin the data recovery. I moved the files that were contained in the 101.zip to the a1forensics1g drive. This is the sdb1 virtual drive I created earlier.

```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
101.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ unzip 101.zip
Archive:  101.zip
   creating: 101/
  inflating: 101/101000.txt
  inflating: 101/101001.txt
  inflating: 101/101002.txt
  inflating: 101/101003.txt
  inflating: 101/101004.txt
  inflating: 101/101005.txt
  inflating: 101/101006.txt
  inflating: 101/101007.txt
  inflating: 101/101008.pdf
  inflating: 101/101009.txt
  inflating: 101/101010.doc
  inflating: 101/101011.doc
```

```
┌──(kali㉿kali)-[~]
└─$ cd /media/kali/a1forensics1g

┌──(kali㉿kali)-[/media/kali/a1forensics1g]
└─$ ls
101  lost+found

┌──(kali㉿kali)-[/media/kali/a1forensics1g]
└─$ cd 101

┌──(kali㉿kali)-[/media/kali/a1forensics1g/101]
└─$ ls -L | grep .jpg | wc -L
10

┌──(kali㉿kali)-[/media/kali/a1forensics1g/101]
└─$ sudo rm *.jpg | wc -L
[sudo] password for kali:
0
```

I changed the directory to that drive using the **cd /media/kali/a1forensics1g.** I then used **ls** to view the contents of the drive. Next, I went to the 101 directories using **cd 101.** To start the image recovery, I first counted all the number of jpg files that were in the folder using the **ls -l | grep .jpg | wc -l.** I then erased the jpg images and counted the number of files in the folder using the **ls -l | grep.jpg | wc -l** command. In this case, it is 0.

Here below is the number of files that remained in the 101 directories using the **ls -l | wc -l** command.

```
┌──(kali㉿kali)-[/media/kali/a1forensics1g/101]
└─$ ls -l | wc -l
974
```

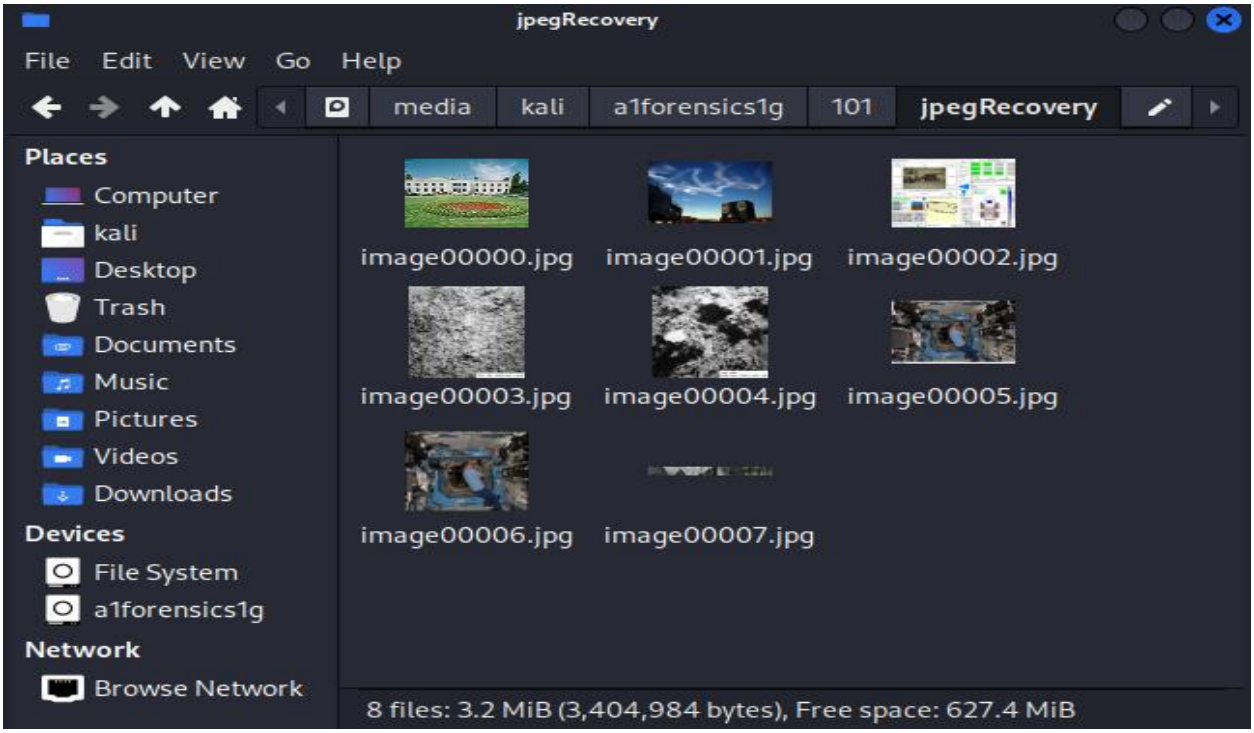
Next, I created a new folder to store carved .jpg media files using **mkdir jpegrecovery && cd ../jpegrecovery** commands below.

```
┌──(kali㉿kali)-[/media/kali/a1forensics1g/101]
└─$ sudo mkdir jpegRecovery && cd jpegRecovery
```

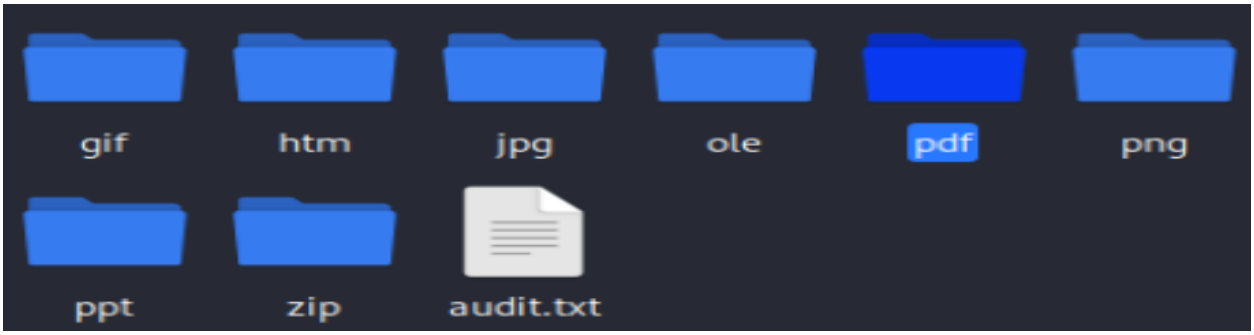
After that I updated the system and installed recoverjpeg by using **sudo apt-get upgrade -y** and **sudo apt-get install recoverjpeg -y.** Now that I stalled the package, I can use the command **sudo recoverjpeg /dev/sdb1 – o ./jpegrecovery.** Here below is the number of images **8.**

```
┌──(kali㉿kali)-[/media/kali/a1forensics1g/101]
└─$ sudo recoverjpeg /dev/sdb1 -o ./jpegRecovery
Restored 8 pictures
```

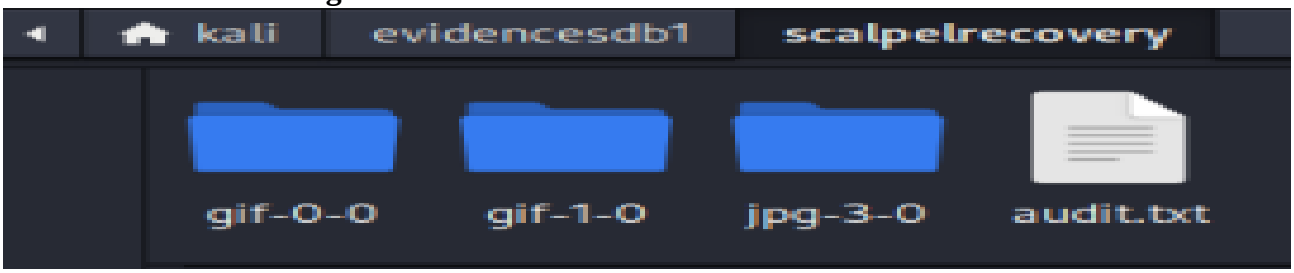
Here below are the images that I recovered.



Part 5 of the lab involed using the foremost tool. First I had to upgrade the tool and install foremost by using the **sudo apt-get upgrade -y** and **sudo apt-get install foremost -y** commands. I then created an image and stored it on the main partition. After that I recovered the files using the **sudo foremost -t all -I ./evidencesdb1/sdb1image.dd -o ./evidencesdb1/foremost recovery command.** Here are the files I recovered below.



Part 6 involved using the scalpel tool to receive the data. First, we need to upgrade the package and install it by using the commands **sudo apt-get upgrade -y** and **sudo apt-get install scalpel -y.** After that, you can use the **sudo scalpel -o ./evidencesdb1/scalpelrecovery/ ./evidencesdb1/sdb1image.dd** to recover the files. These are the files I recovered below.



The last part of the lab involved using the bulk_extractor for data recovery and information retrieval. You can use the **sudo bulk_extractor - o ./evidencesdb1/bulk ./evidencesdb1/sdb1image.dd** command to do this. This will allow you to recover email addresses, encryption keys, domain names, and credit card numbers, among other information.