Part 1. Disk imaging using FTK Imager

Task 1:
(Note: Answers are in RED)

1. **After the imaging process was complete, what files did FTK Imager create? (Select all that apply.)**

    - **The image file with an extension of .001**
    - **A text file for image summary**
    - **An image file with an extension of .Ex01**
    - **No files**

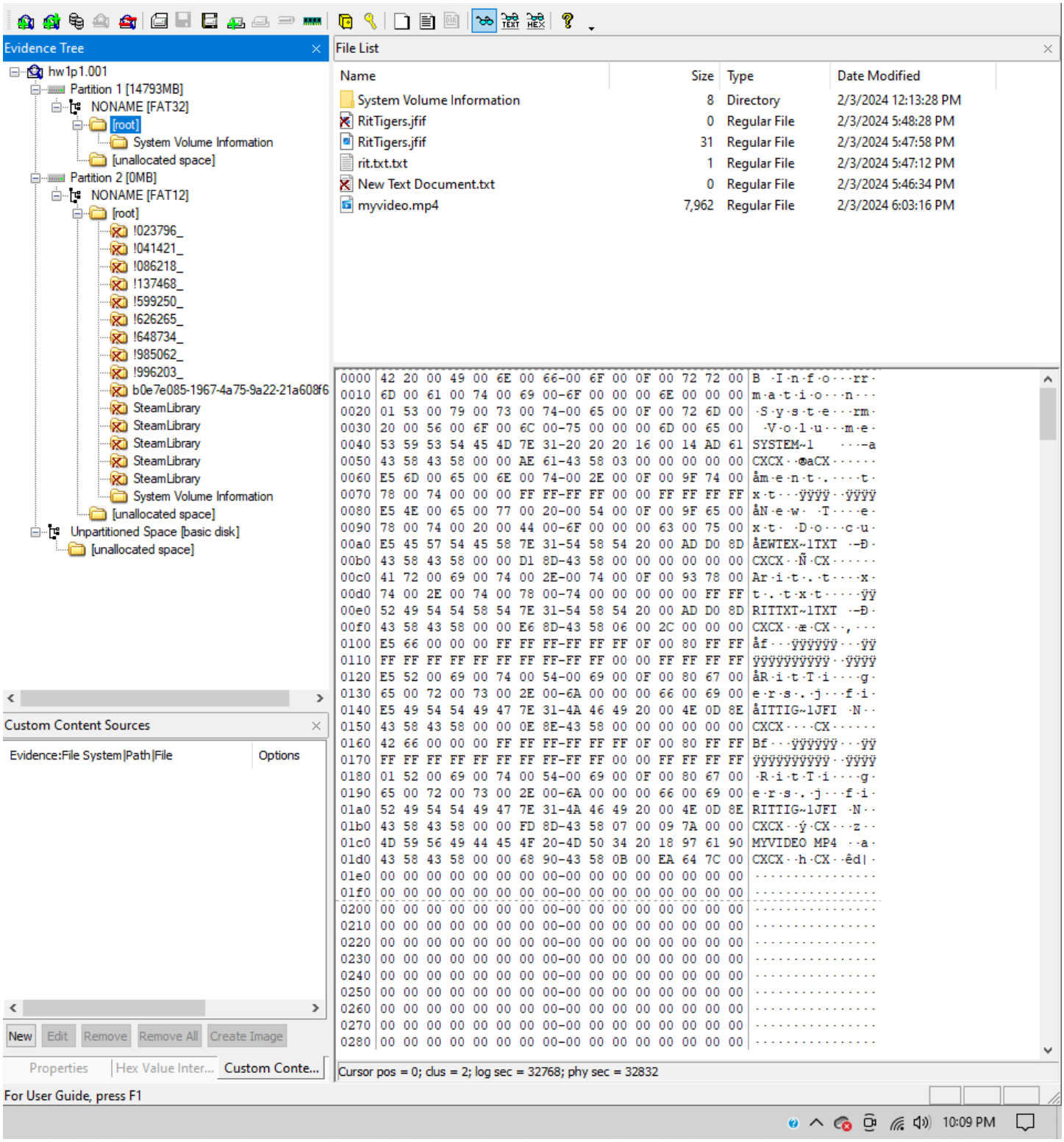
2. **During the imaging process, you should have noticed that "Verify images after they are created" is checked by default. What is the result of having this option checked? (choose a single best answer)**

    - **FTK imager will compute the hash value of the image**
    - **FTK imager will compute the hash value of the USB drive**
    - **FTK imager will compute the MD5 and SHA1 hashes of the USB drive and the MD5 and SHA1 hashes of the image, and verify the hashes match.**
    - **FTK imager will compute the MD5 hash of the USB drive and the MD5 hash of the image, and verify the hashes match**

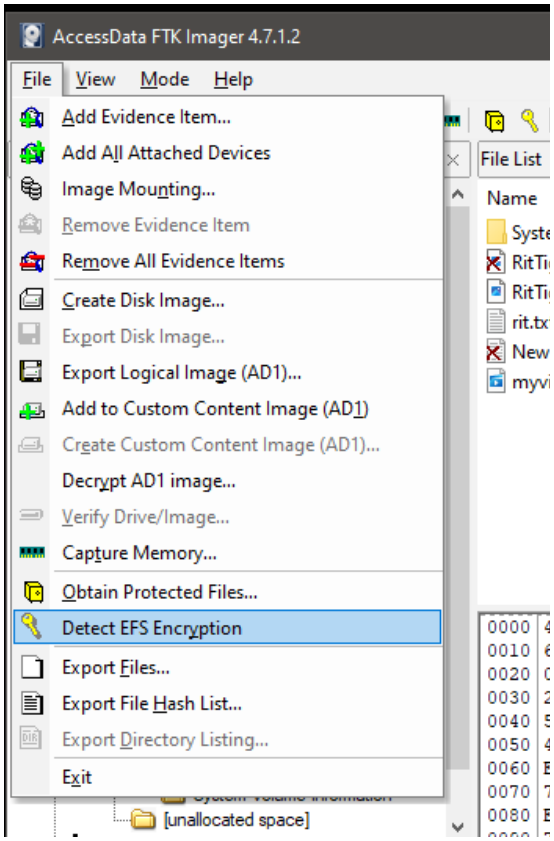
3. **How many hash algorithms did the FTK imager use to verify the image has not been altered? (choose a single best answer)**

    - **One hash algorithm**
    - **Two hash algorithms**
    - **Three hash algorithms**
    - **Four hash algorithms**

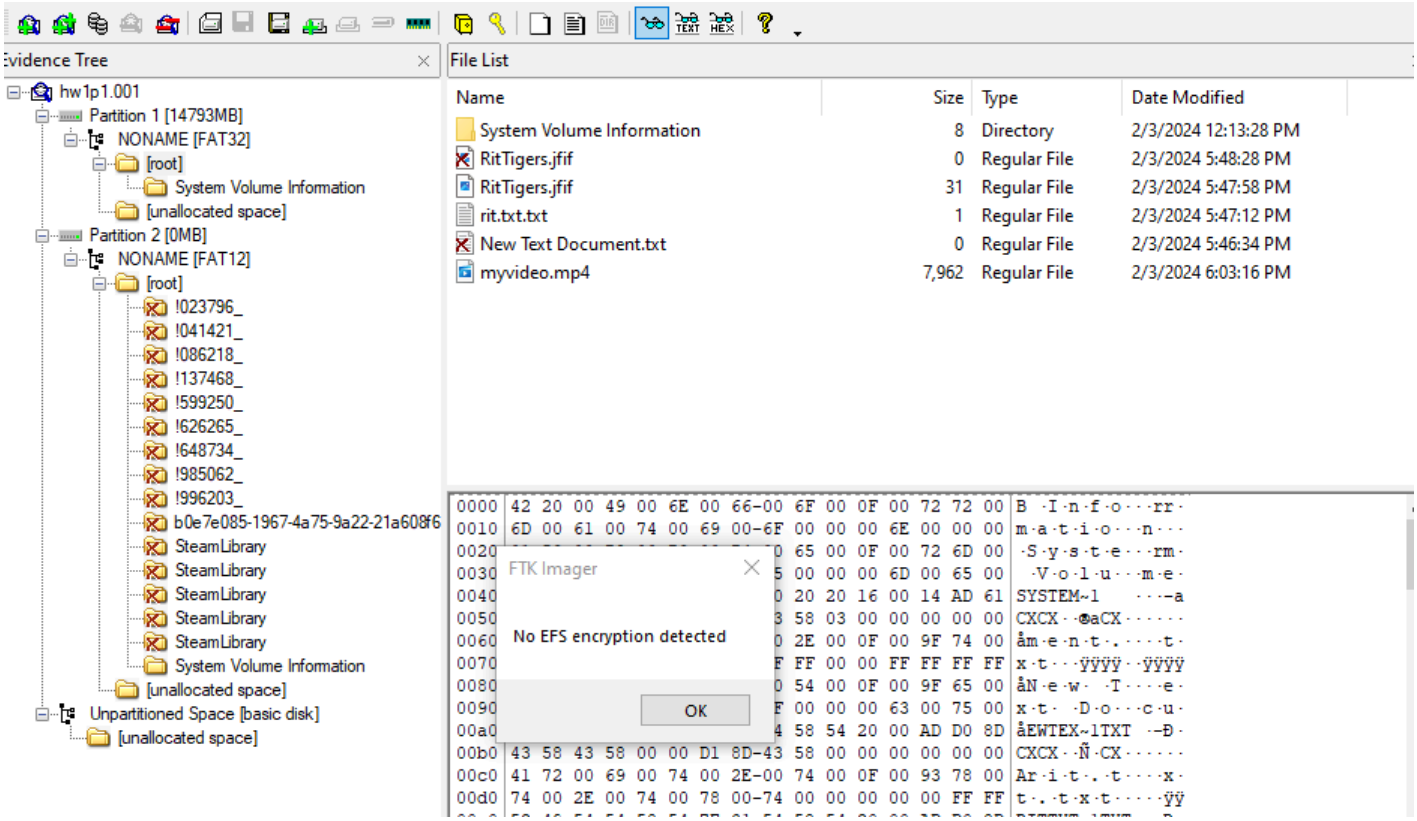
Task 2: Screenshot of FTK imager after you have loaded the USB image was loaded into the FTK imager.



Task 3: One of the FTK Imager features is Detecting EFS Encryption. Basically, you can check for encrypted data on a physical drive or an image with the FTK Imager. When using this feature, the program scans the evidence and notifies if encrypted files are located.



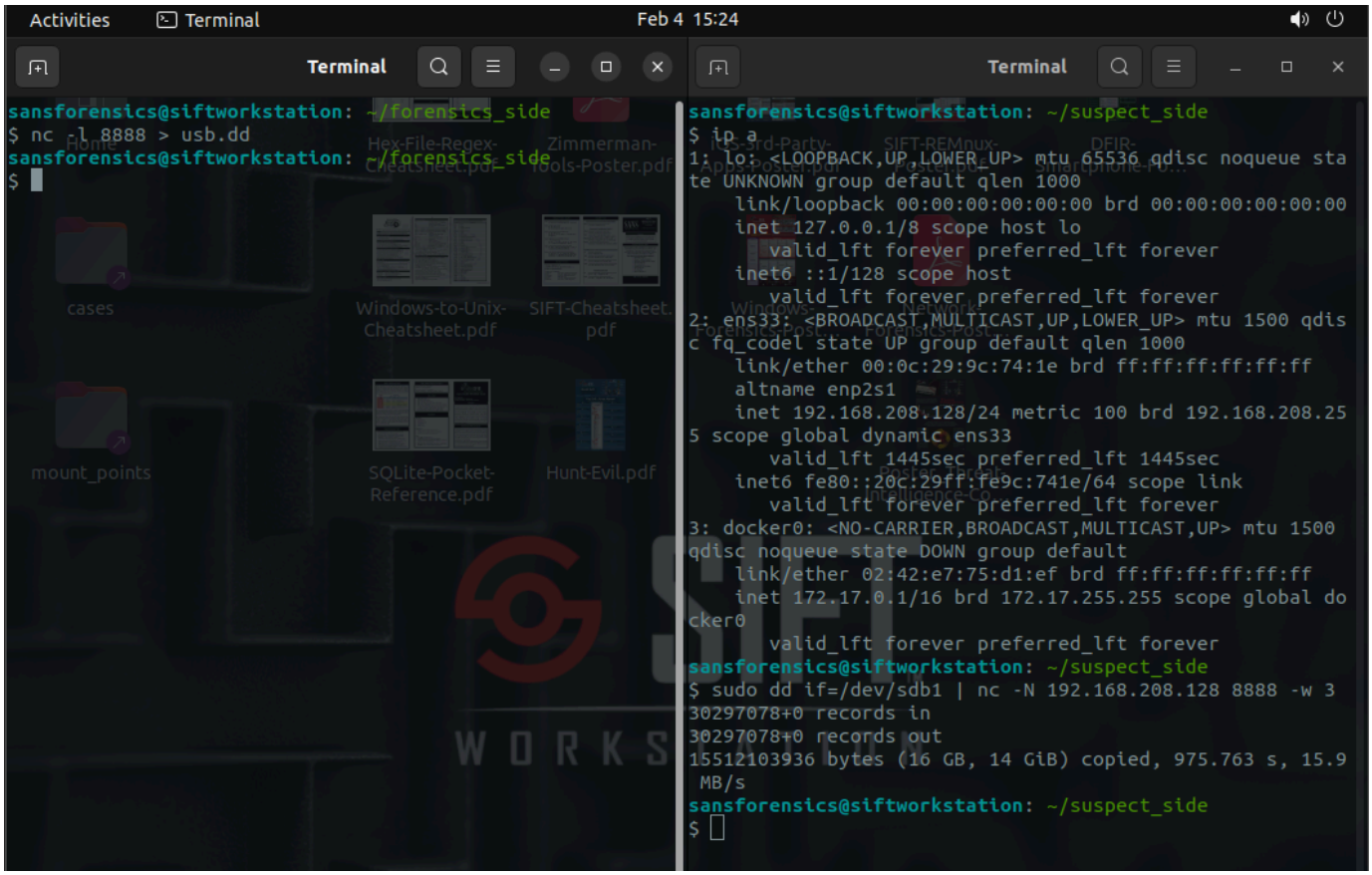
However, for me there was no EFS encryption detected.



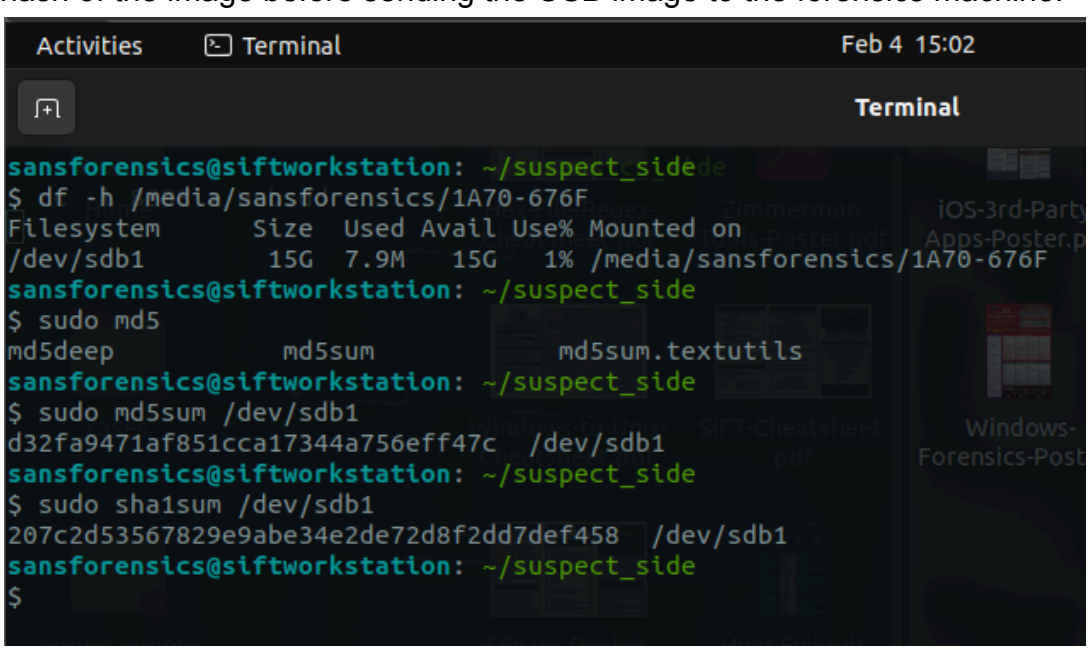
Part 2. Imaging with dd and netcat (nc)

Task 4:

1. I used the command *nc -l 8888 > usb.dd* to save receive data over the network to usb.dd
2. I used the command *sudo dd if=/dev/sdb1 | nc -N 192.168.208.128 8888 -w 3* to send the USB image to the forensics machine terminal.

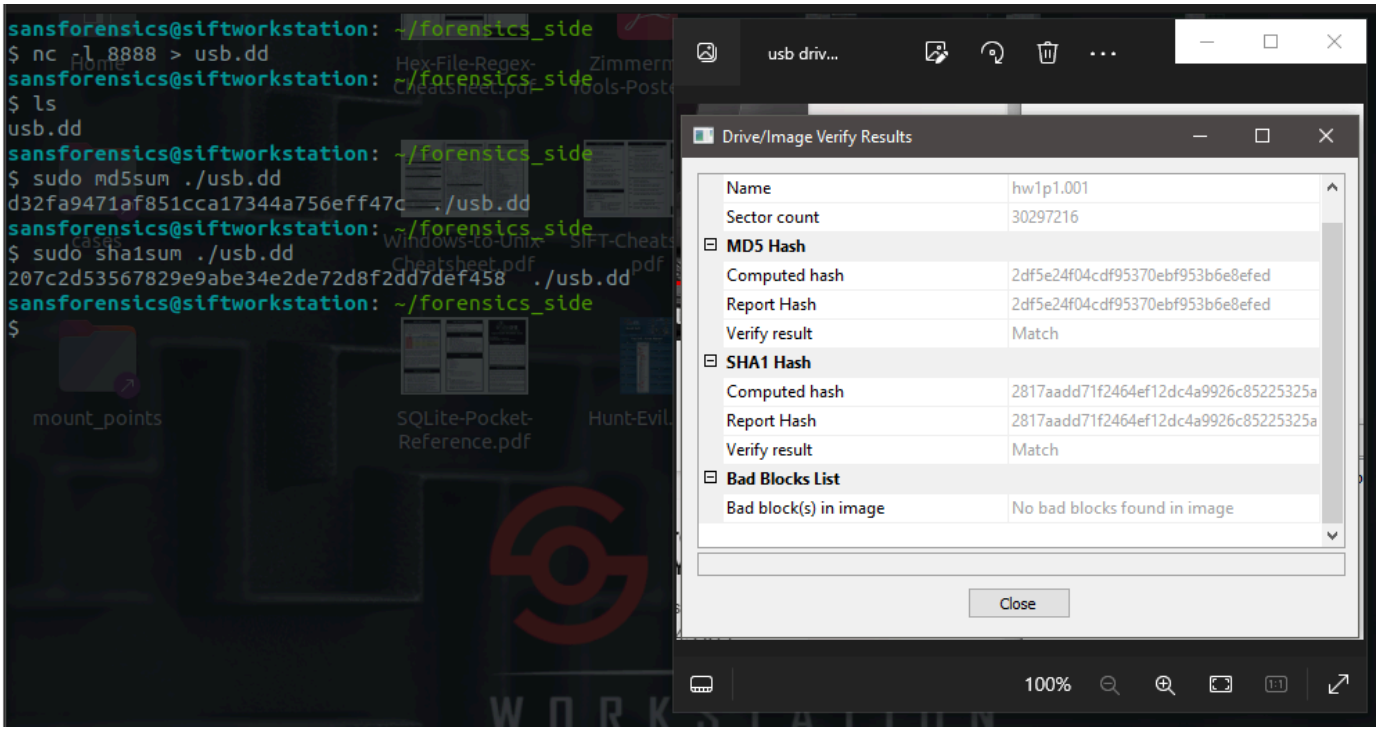


3. I used *sudo md5sum /dev/sdb1*, and *sudo sha1sum /dev/sdb1* to calculate the md5 and sha1 hash of the image before sending the USB image to the forensics machine.



4. I used *sudo md5sum ./usb.dd*, and *sudo sha1sum ./usb.dd* commands to compute the md5 and sha1 hash of the usb.dd image.

5. The hash value of usb.dd in linux by dd command is different from the hash values of the raw image created by FTK imager in part 1. The reasons could be the the metadata, FTK Imager includes metadata about the image in its output, which is not included in a raw dd image. This additional data can cause a difference in the hash values. Also, FTK Imager and dd might acquire the data differently. For example, FTK Imager might be doing a physical drive capture, while dd might be capturing only the logical drive. This difference in acquisition methods can lead to different hash values.



Part 3. Linux memory acquisition using LiME

Task 5: Screenshot of lsmod | grep lime

```
sansforensics@siftworkstation: ~/lime/src
$ lsmod | grep lime
lime                   16384  0
sansforensics@siftworkstation: ~/lime/src
$
```

Task 6: Two strings commands that was used

This is commands has been used to get the hashed version of the password for sansforensics.
sudo strings -f -d ../Desktop/mh8872_memory_dump.bin > strings_output_1
and
cat strings_output_1 | grep password

```
../Desktop/mh8872_memory_dump.bin: hc_DES_read_password
../Desktop/mh8872_memory_dump.bin:  password prompts for encrypted file systems.
../Desktop/mh8872_memory_dump.bin:  password prompts for encrypted file systems.
../Desktop/mh8872_memory_dump.bin: Description: run common desktop actions without password
../Desktop/mh8872_memory_dump.bin:  to run common actions without being asked for their password:
../Desktop/mh8872_memory_dump.bin:  /etc/java-8-openjdk/management/jmxremote.password 7b46c291e7073c31d3ce0adae2f755
4f
```

```
../Desktop/mh8872_memory_dump.bin:  password-manager-service:
../Desktop/mh8872_memory_dump.bin: dialog-password-symbolic
../Desktop/mh8872_memory_dump.bin: Description: runtime support for password checker library cracklib2
../Desktop/mh8872_memory_dump.bin: including programs to build the password dictionary databases used by
../Desktop/mh8872_memory_dump.bin: {"userName":"sansforensics","uid":1000,"gid":1000,"homeDirectory":"/home/sansfore
nsics","shell":"/bin/bash","privileged":{"hashedPassword":["$2a$10$xeAdkxMLN5dzg4l55bGKfuRy0TegEBPBzxglWq4edAWgl7rxO
znxi"]},"passwordChangeNow":false,"lastPasswordChangeUSec":1681862400000000,"passwordChangeMaxUSec":8639913600000000
,"passwordChangeWarnUSec":604800000000}
../Desktop/mh8872_memory_dump.bin: mount-op-ask-password
```

This commands was used to see and find what media was attached to the machine which is my USB.
sudo strings -n 8 ../Desktop/mh8872_memory_dump.bin > strings_output_2
and
Cat strings_output_2 | grep GET

```
'RGET=/media/sansforensics/1A70-676F ROOT=/ OPTS=uhelper=udisks2
NAUTILUS_VIEW_GET_IFACE (view)->get_view_id
NAUTILUS_VIEW_GET_IFACE (view)->set_templates_menu
```

Task 7:

Command used: foremost -d -i ../Desktop/mh8872_memory_dump.bin -o ./foremost_output/

```
133:    06769348.exe          781 KB      3465906304
134:    06807300.exe          781 KB      3485337728
135:    06837364.exe          781 KB      3500730496
136:    06927724.exe          781 KB      3546994816
137:    07787316.doc           11 MB      3987106064
138:    07824340.doc           11 MB      4006062240
Finish: Sun Feb  4 21:13:09 2024

139 FILES EXTRACTED

doc:= 9
exe:= 130
----------------------------------------------------------------

Foremost finished at Sun Feb  4 21:13:09 2024
sansforensics@siftworkstation: ~/Documents/foremost_output
$ ls
audit.txt  doc  exe
sansforensics@siftworkstation: ~/Documents/foremost_output
$
```

With the command I found a lot of doc files and exe files. Some of the exe files seems to be system related files, and some of the docs files seems to be related to some of forensics pdf files in the linux.