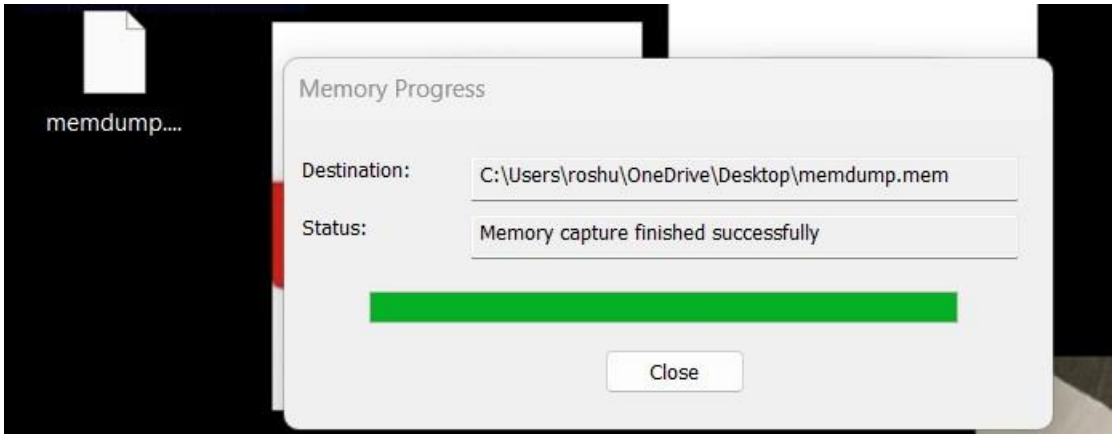



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sha256sum memory_dump1.mem
b894b81becbf09c616aaf8f597a5f29a69e2857a9f0d46aa2618c3bbee470ce2  memory_dump1.mem

┌──(kali㉿kali)-[~/Desktop]
└─$
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sha256sum memory_dump2.mem
581dc5e493b7653ba8d1465eb7efb6aacff900e1f4551a106dadde9dbd0fd4ec  memory_dump2.mem
```

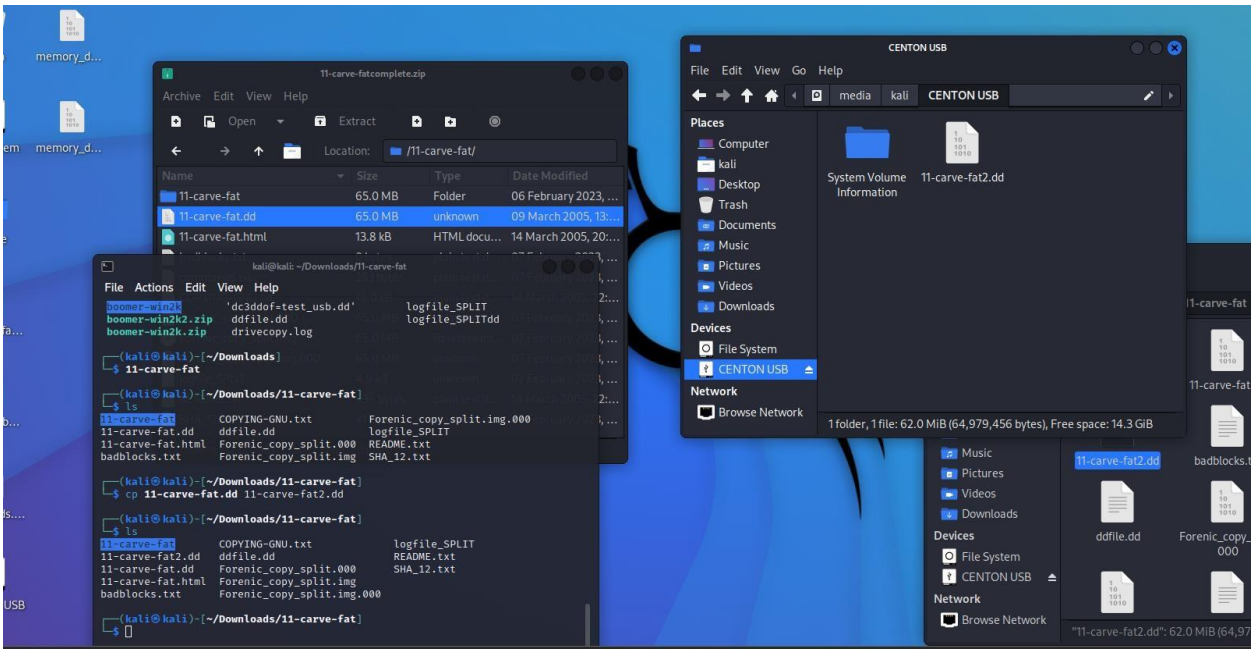
```
C:\Users\roshu\Desktop>certutil -hashfile "memory_dump1.mem" SHA256
SHA256 hash of memory_dump1.mem:
b894b81becbf09c616aaf8f597a5f29a69e2857a9f0d46aa2618c3bbee470ce2
CertUtil: -hashfile command completed successfully.

C:\Users\roshu\Desktop>certutil -hashfile "memory_dump2.mem" SHA256
SHA256 hash of memory_dump2.mem:
60da0d0bf9ac3b110c4de0fbd20a4134cf47d10a2d01f44faec0606bfa22f7e0
CertUtil: -hashfile command completed successfully.
```

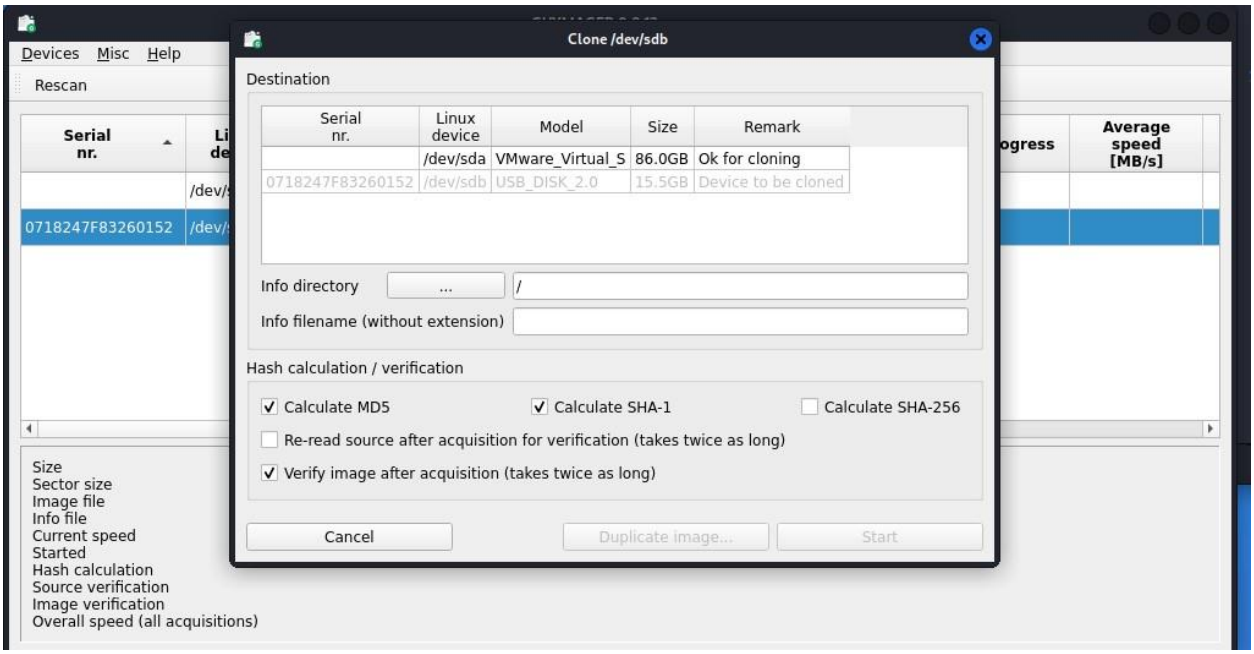
```
C:\Users\roshu\Desktop>certutil -hashfile "memory_dump2.mem" SHA256 > memory_dump2.txt

C:\Users\roshu\Desktop>certutil -hashfile "memory_dump1.mem" SHA256 > memory_dump1.txt
```

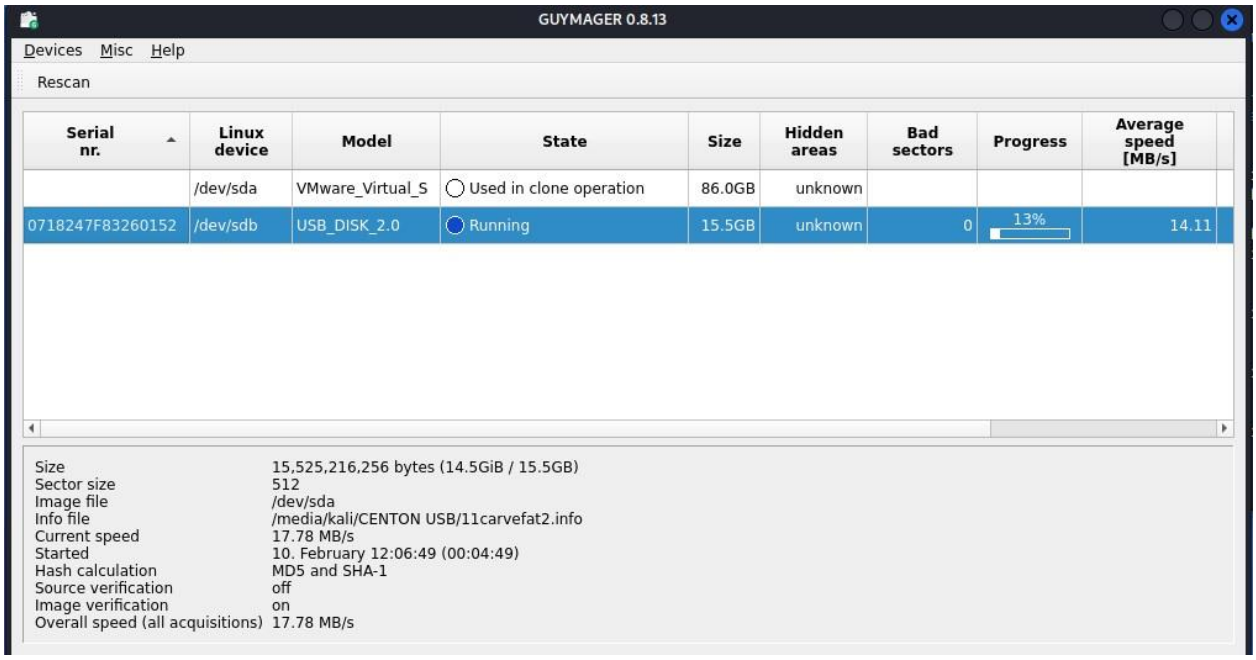
The files do not have the same checksums due to not be duplicates. One file is the original of the device before having an mem file versus the second has an mem already on the device creating a different checksum for the second file.

For live systems if the device is to be turned off a saturated system, running multiple applications can impact the data acquisition process.

Task 2


11-carve-fatcomplete.zip
Archive Edit View Help
Open Extract
Location: /11-carve-fat/
Name Size Type Date Modified
11-carve-fat 65.0 MB Folder 06 February 2023, ...
11-carve-fat.dd 65.0 MB unknown 09 March 2005, 13:...
11-carve-fat.html 13.8 kB HTML docu... 14 March 2005, 20:...
kali@kali: ~/Downloads/11-carve-fat
File Actions Edit View Help
boomer-win2k 'dc3ddof-test_usb.dd' logfile_SPLIT
boomer-win2k2.zip ddfile.dd logfile_SPLITdd
boomer-win2k.zip drivecopy.log
(kali㉿kali)-[~/Downloads]
$ 11-carve-fat
(kali㉿kali)-[~/Downloads/11-carve-fat]
$ ls
11-carve-fat COPYING-GNU.txt Forenic_copy_split.img.000
11-carve-fat.dd ddfile.dd logfile_SPLIT
11-carve-fat.html Forenic_copy_split.000 README.txt
badblocks.txt Forenic_copy_split.img SHA_12.txt
(kali㉿kali)-[~/Downloads/11-carve-fat]
$ cp 11-carve-fat.dd 11-carve-fat2.dd
(kali㉿kali)-[~/Downloads/11-carve-fat]
$ ls
11-carve-fat COPYING-GNU.txt logfile_SPLIT
11-carve-fat2.dd ddfile.dd README.txt
11-carve-fat.dd Forenic_copy_split.000 SHA_12.txt
11-carve-fat.html Forenic_copy_split.img
badblocks.txt Forenic_copy_split.img.000
(kali㉿kali)-[~/Downloads/11-carve-fat]
$
CENTON USB
File Edit View Go Help
media kali CENTON USB
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
CENTON USB
Network
Browse Network
System Volume Information
11-carve-fat2.dd
1 folder, 1 file: 62.0 MiB (64,979,456 bytes), Free space: 14.3 GiB
11-carve-fat2.dd
ddfile.dd
badblocks.t
Forenic_copy_000


Devices Misc Help
Rescan
Clone /dev/sdb
Destination
Serial nr. Linux device Model Size Remark
/dev/sda VMware_Virtual_S 86.0GB Ok for cloning
0718247F83260152 /dev/sdb USB_DISK_2.0 15.5GB Device to be cloned
Info directory ... /
Info filename (without extension)
Hash calculation / verification
Calculate MD5
Calculate SHA-1
Calculate SHA-256
Re-read source after acquisition for verification (takes twice as long)
Verify image after acquisition (takes twice as long)
Cancel
Duplicate image...
Start
Serial nr.
Average speed [MB/s]
0718247F83260152
Size
Sector size
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
Overall speed (all acquisitions)



After the deleting the file, the checksums on the usb did change minor but not as much compared to task 1.