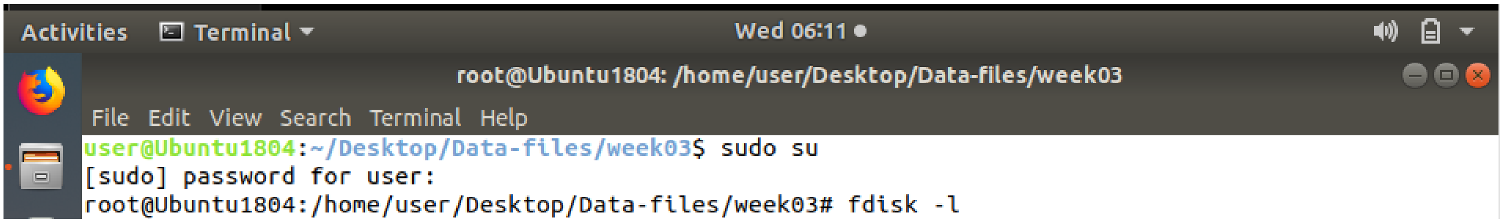
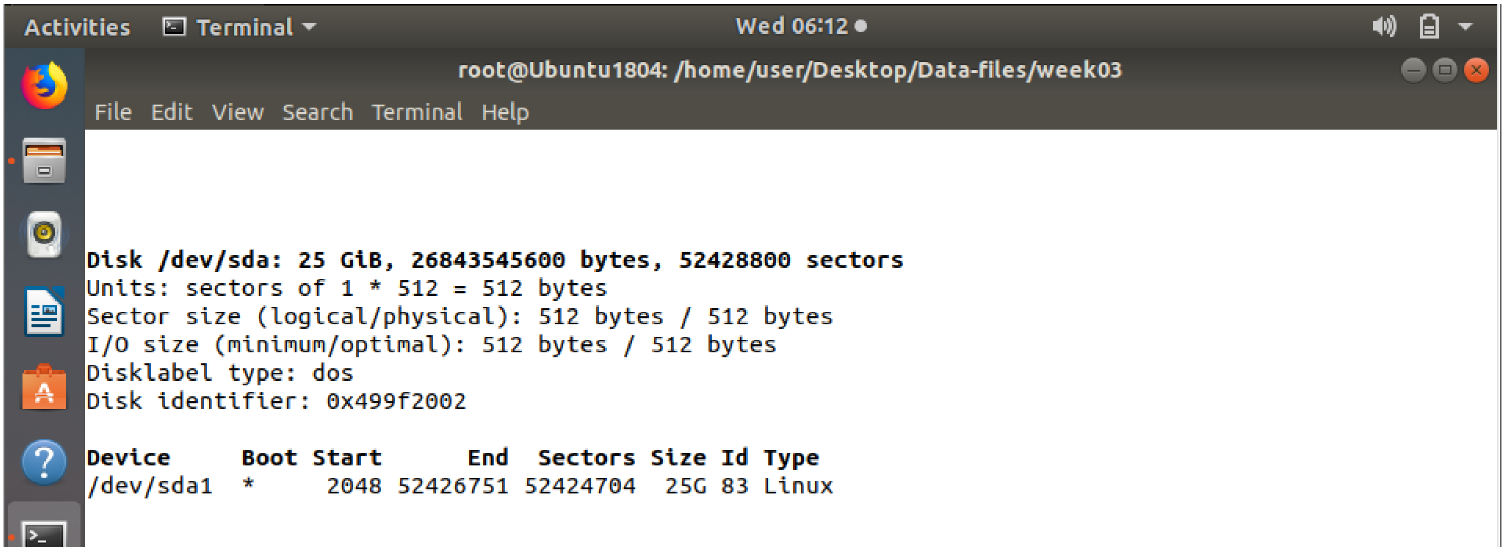
Introducing dd and dcfldd

First, I confirmed the available disks and found that /dev/sda was available

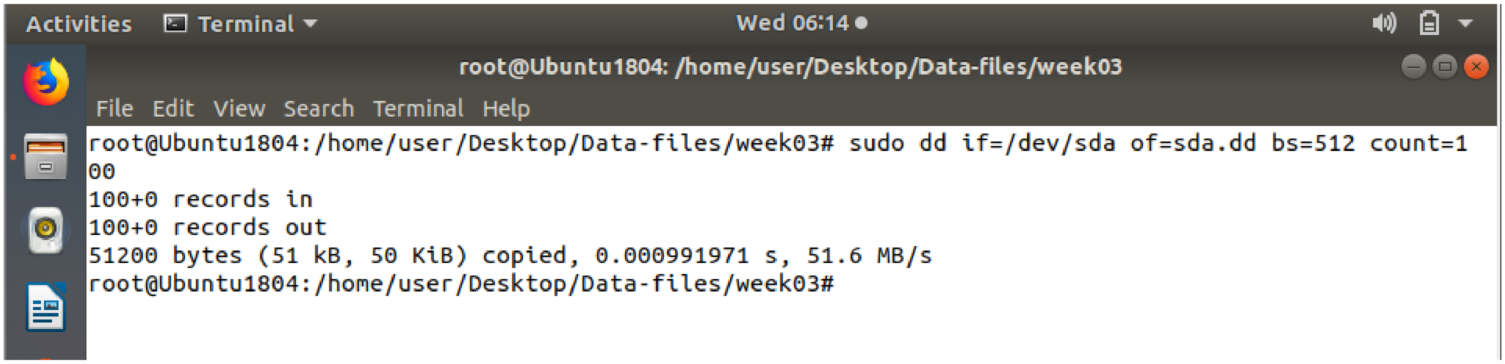

Activities
Terminal
Wed 06:11
root@Ubuntu1804: /home/user/Desktop/Data-files/week03
File Edit View Search Terminal Help

```
user@Ubuntu1804:~/Desktop/Data-files/week03$ sudo su
[sudo] password for user:
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# fdisk -l
```


Activities
Terminal
Wed 06:12
root@Ubuntu1804: /home/user/Desktop/Data-files/week03
File Edit View Search Terminal Help

```
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x499f2002

Device     Boot Start      End  Sectors Size Id Type
/dev/sda1  *     2048 52426751 52424704  25G 83 Linux
```

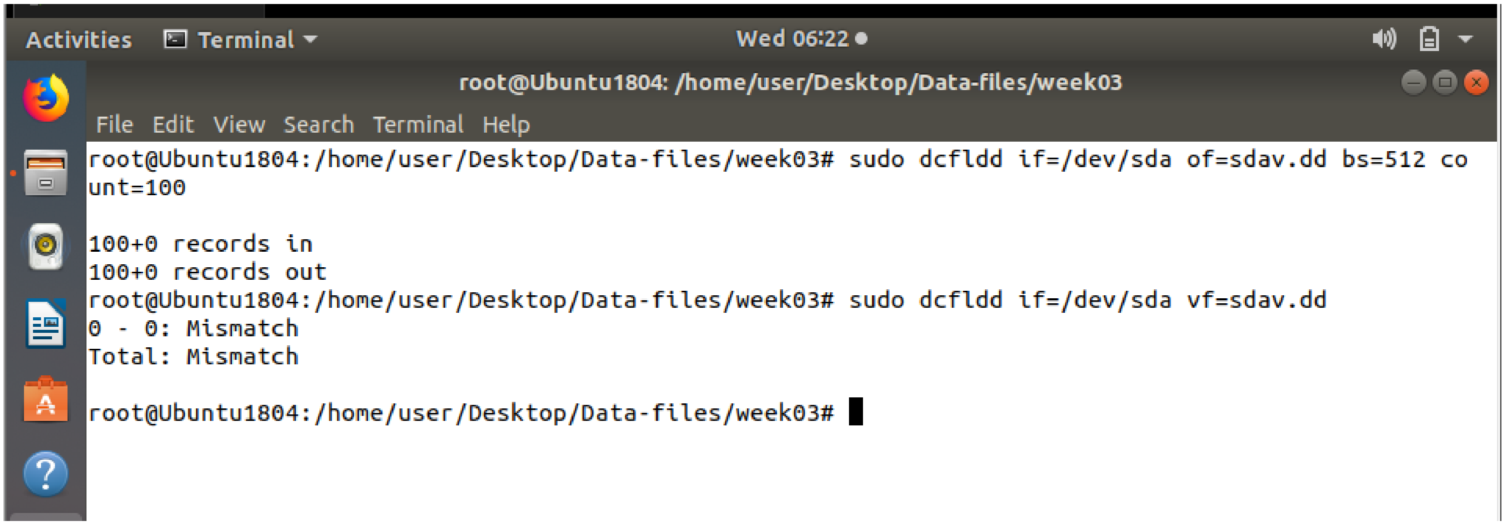
Then I entered the command **"sudo dd if=/dev/sda of=sda.dd bs=512 count=100"** to analyze the /dev/sda disk to acquire the first 100 sectors of the disk drive of the virtual machine.


Activities
Terminal
Wed 06:14
root@Ubuntu1804: /home/user/Desktop/Data-files/week03
File Edit View Search Terminal Help

```
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# sudo dd if=/dev/sda of=sda.dd bs=512 count=1
00
100+0 records in
100+0 records out
51200 bytes (51 kB, 50 KiB) copied, 0.000991971 s, 51.6 MB/s
root@Ubuntu1804:/home/user/Desktop/Data-files/week03#
```

The input file is the /dev/sda and the output file will be sda.dd we will introduce its sister tool dcfldd. It is almost used in the same manner as dd. When we acquire an image, dcfldd uses the same set of parameters as dd. But when we need to verify the image, we will use the option “vf” instead of “of”. In the following screenshot, you can observe that the image “sdav.dd” has been verified with the source.

Then I used the command “**sudo dcfldd if=/dev/sda of=sdav.dd bs=512 count=100”** which is to analyze the disk and then used the command **“sudo dcfldd if=/dev/sda vf=sdav.dd bs=512 count=100”** which will now dump the disk to verify it with the source



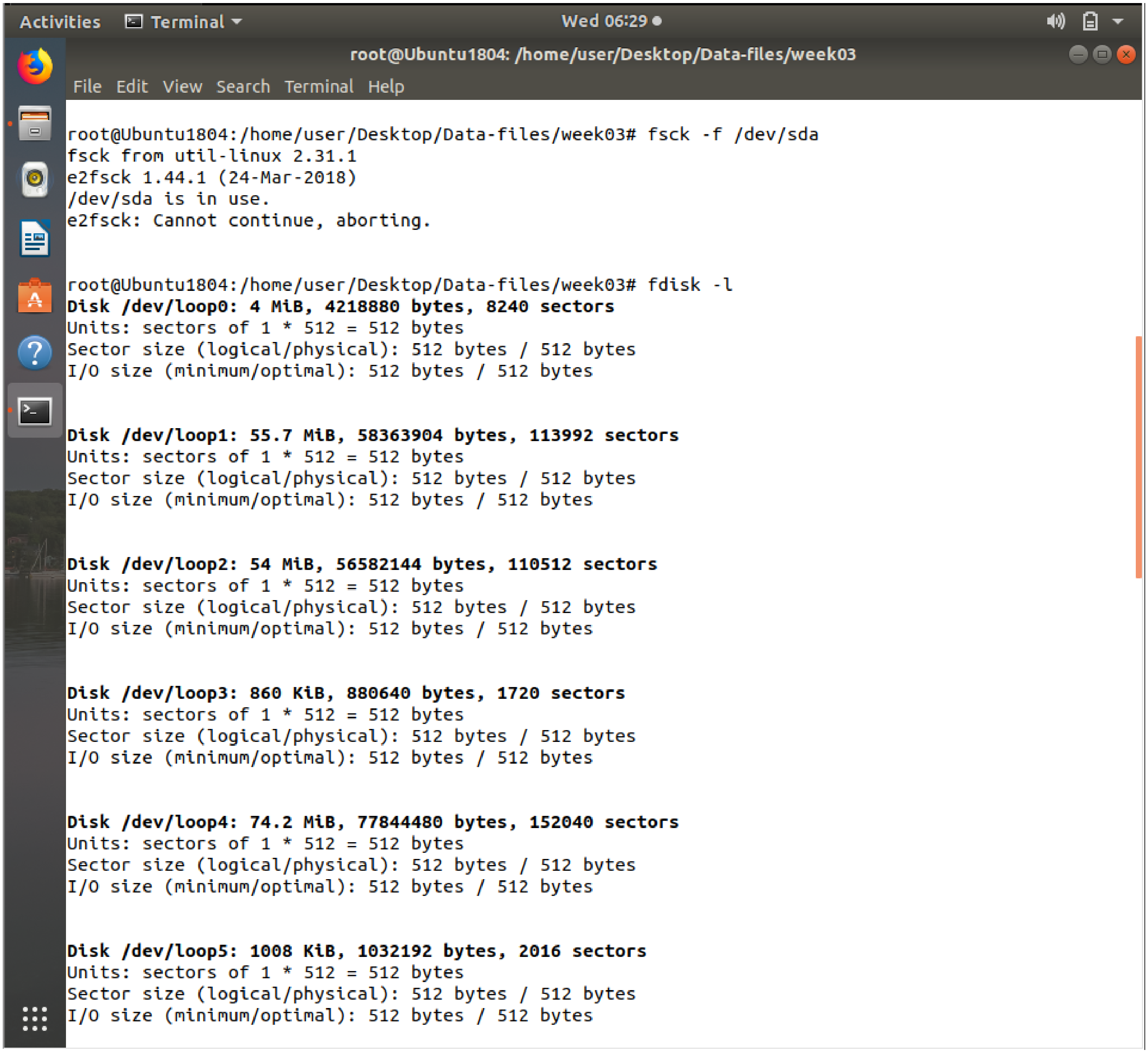
```
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# sudo dcfldd if=/dev/sda of=sdav.dd bs=512 co
unt=100

100+0 records in
100+0 records out
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# sudo dcfldd if=/dev/sda vf=sdav.dd
0 - 0: Mismatch
Total: Mismatch

root@Ubuntu1804:/home/user/Desktop/Data-files/week03# 
```

We got a “Mismatch” because /dev/sda is currently in use. We should not dump a disk that is in use. Running “dcfldd” on a mounted disk or in-use disk could cause data loss or corruption, as it may modify the contents of the disk.

We can scan the disk and check the status of disks by running the following command:

sudo fsck –f /dev/sda (You will see /dev/sda is in use)

sudo fdisk –l



Activities
Terminal
Wed 06:29
root@Ubuntu1804: /home/user/Desktop/Data-files/week03
File Edit View Search Terminal Help

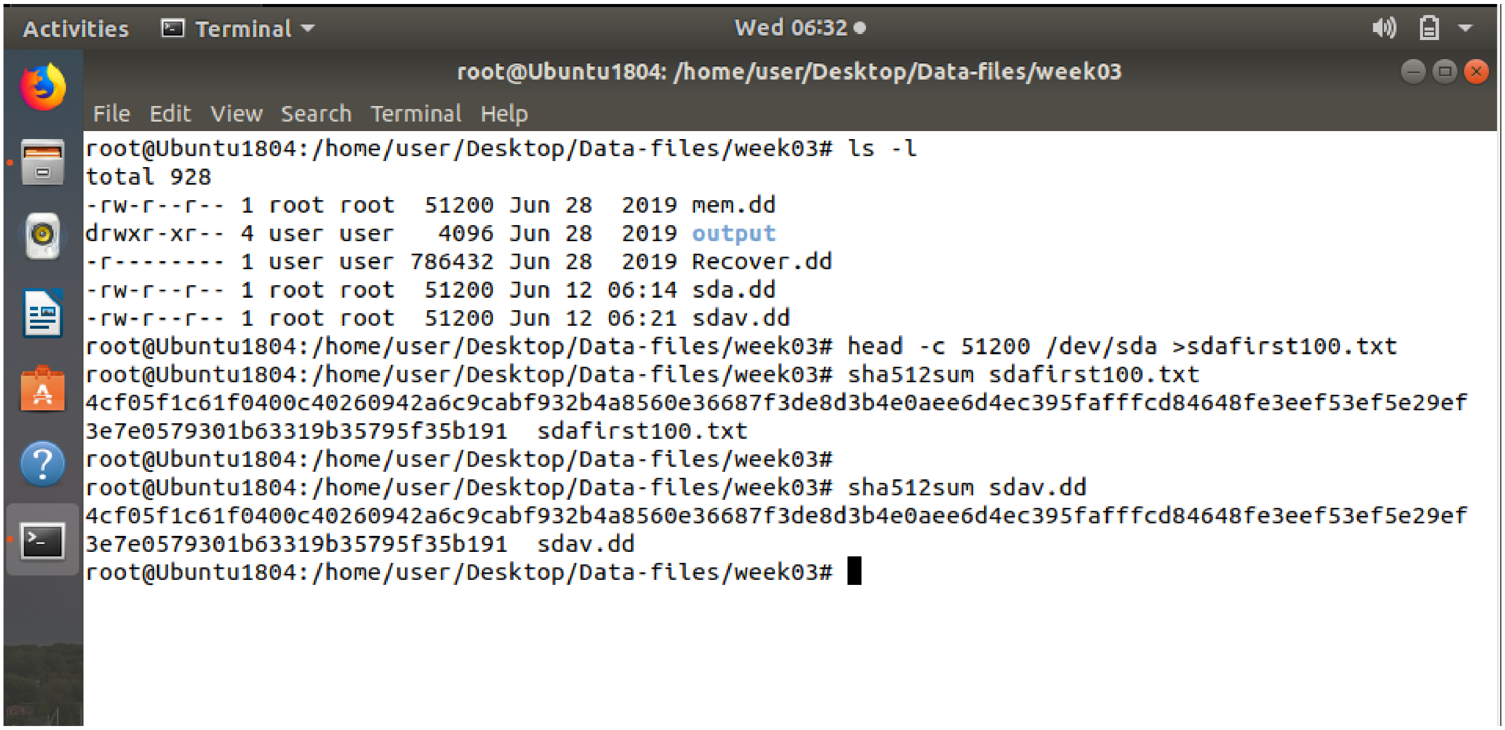
```
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# fsck -f /dev/sda
fsck from util-linux 2.31.1
e2fsck 1.44.1 (24-Mar-2018)
/dev/sda is in use.
e2fsck: Cannot continue, aborting.


root@Ubuntu1804:/home/user/Desktop/Data-files/week03# fdisk -l
Disk /dev/loop0: 4 MiB, 4218880 bytes, 8240 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop1: 55.7 MiB, 58363904 bytes, 113992 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop2: 54 MiB, 56582144 bytes, 110512 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop3: 860 KiB, 880640 bytes, 1720 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop4: 74.2 MiB, 77844480 bytes, 152040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop5: 1008 KiB, 1032192 bytes, 2016 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

In this case, we can compare the hash value (e.g. sha512) of the first 512*100 bytes of **/dev/sda** and that of the **sdav.dd**. We cannot directly sha512sum the first 512*100 bytes of **/dev/sda**, so we first extract that part to a file, then hash. So, for that I used the following commands below:

sudo head –c 51200 /dev/sda > sdafirst100.txt – this one will create a file called sdafirst100.txt file as the output.

sha512sum sdafirst100.txt – here we find the hash value of that image **/dev/sda** using the text file.

sha512sum sdav.dd – then we check the hash value of sdav.dd image

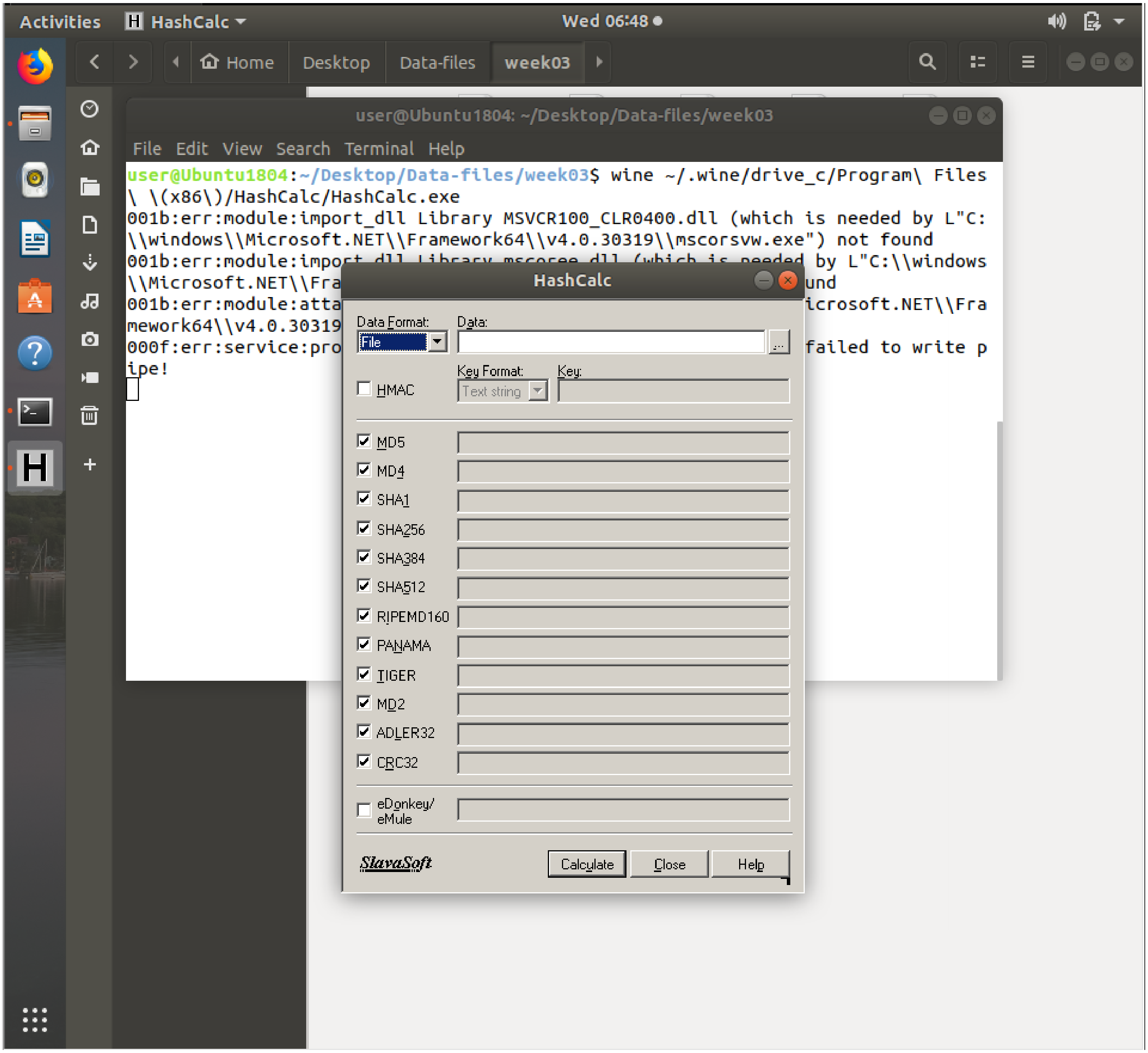

Activities
Terminal
Wed 06:32
root@Ubuntu1804: /home/user/Desktop/Data-files/week03
File Edit View Search Terminal Help

```
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# ls -l
total 928
-rw-r--r-- 1 root root  51200 Jun 28  2019 mem.dd
drwxr-xr-- 4 user user   4096 Jun 28  2019 output
-r-------- 1 user user 786432 Jun 28  2019 Recover.dd
-rw-r--r-- 1 root root  51200 Jun 12 06:14 sda.dd
-rw-r--r-- 1 root root  51200 Jun 12 06:21 sdav.dd
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# head -c 51200 /dev/sda >sdafirst100.txt
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# sha512sum sdafirst100.txt
4cf05f1c61f0400c40260942a6c9cabf932b4a8560e36687f3de8d3b4e0aee6d4ec395fafffcd84648fe3eef53ef5e29ef
3e7e0579301b63319b35795f35b191  sdafirst100.txt
root@Ubuntu1804:/home/user/Desktop/Data-files/week03#
root@Ubuntu1804:/home/user/Desktop/Data-files/week03# sha512sum sdav.dd
4cf05f1c61f0400c40260942a6c9cabf932b4a8560e36687f3de8d3b4e0aee6d4ec395fafffcd84648fe3eef53ef5e29ef
3e7e0579301b63319b35795f35b191  sdav.dd
root@Ubuntu1804:/home/user/Desktop/Data-files/week03#
```

We can come to a conclusion that the hash values match.

Using HashCalc to Get Hash Values

First I started HashCalc using the command **“wine ~/.wine/drive_c/Program\ Files\ \(x86\)/HashCalc/HashCalc.exe”**



Activities
HashCalc
Wed 06:48
Home
Desktop
Data-files
week03
user@Ubuntu1804: ~/Desktop/Data-files/week03
File Edit View Search Terminal Help

```
user@Ubuntu1804:~/Desktop/Data-files/week03$ wine ~/.wine/drive_c/Program\ Files
\ \(x86\)/HashCalc/HashCalc.exe
001b:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:
\\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001b:err:module:import_dll Library mscoree.dll (which is needed by L"C:\\windows
\\Microsoft.NET\\Fra                                            und
001b:err:module:atta                                            icrosoft.NET\\Fra
mework64\\v4.0.30319
000f:err:service:pro                                            failed to write p
ipe!
```

HashCalc

Data Format: File
Data:

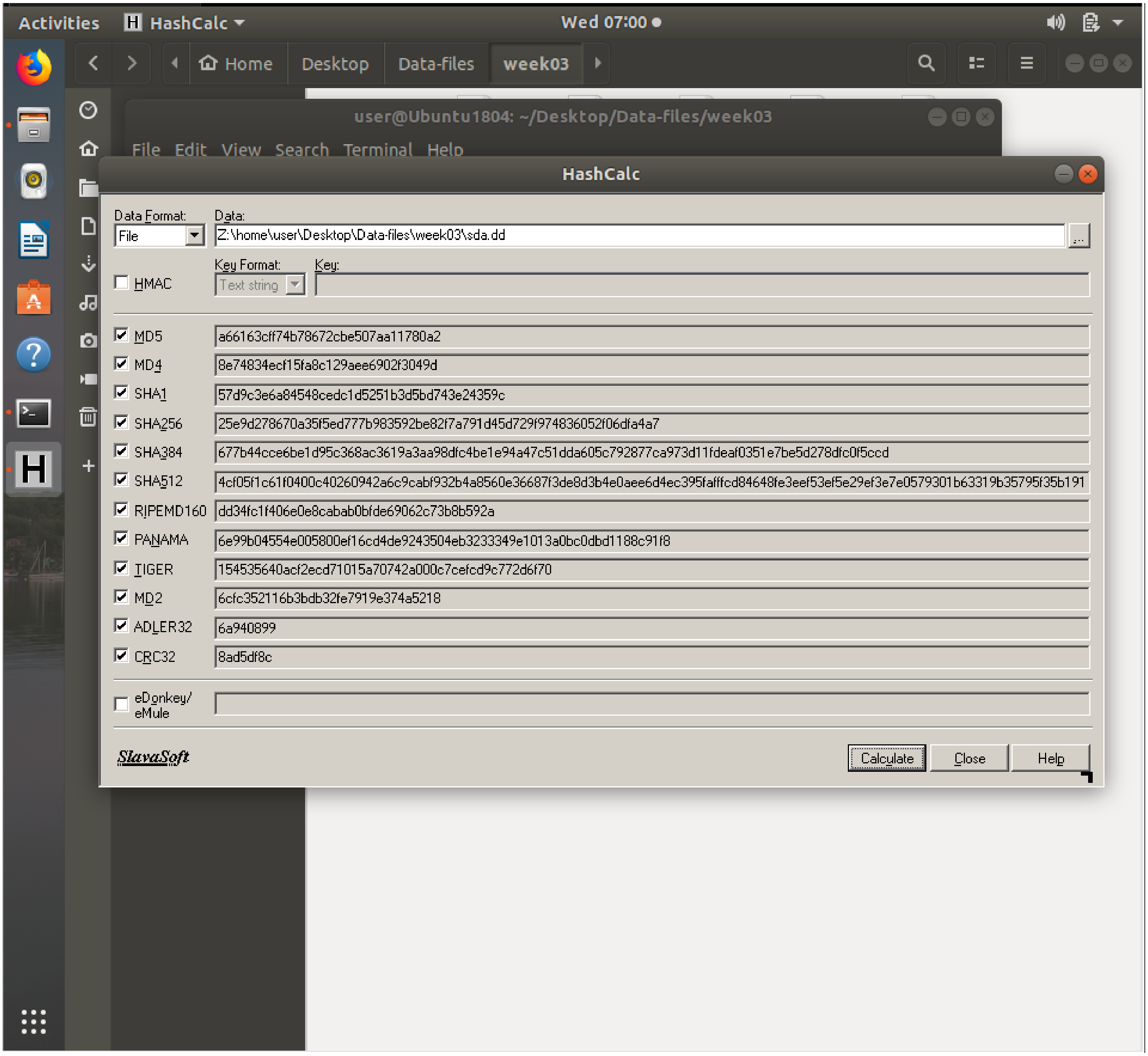
□ HMAC
Key Format: Text string
Key:

☑ MD5
☑ MD4
☑ SHA1
☑ SHA256
☑ SHA384
☑ SHA512
☑ RIPEMD160
☑ PANAMA
☑ TIGER
☑ MD2
☑ ADLER32
☑ CRC32

□ eDonkey/ eMule

After I started the application, I calculated all the types of hash algorithms for both sda.dd image file and sdav.dd file and found out their hash values match

Sda.dd



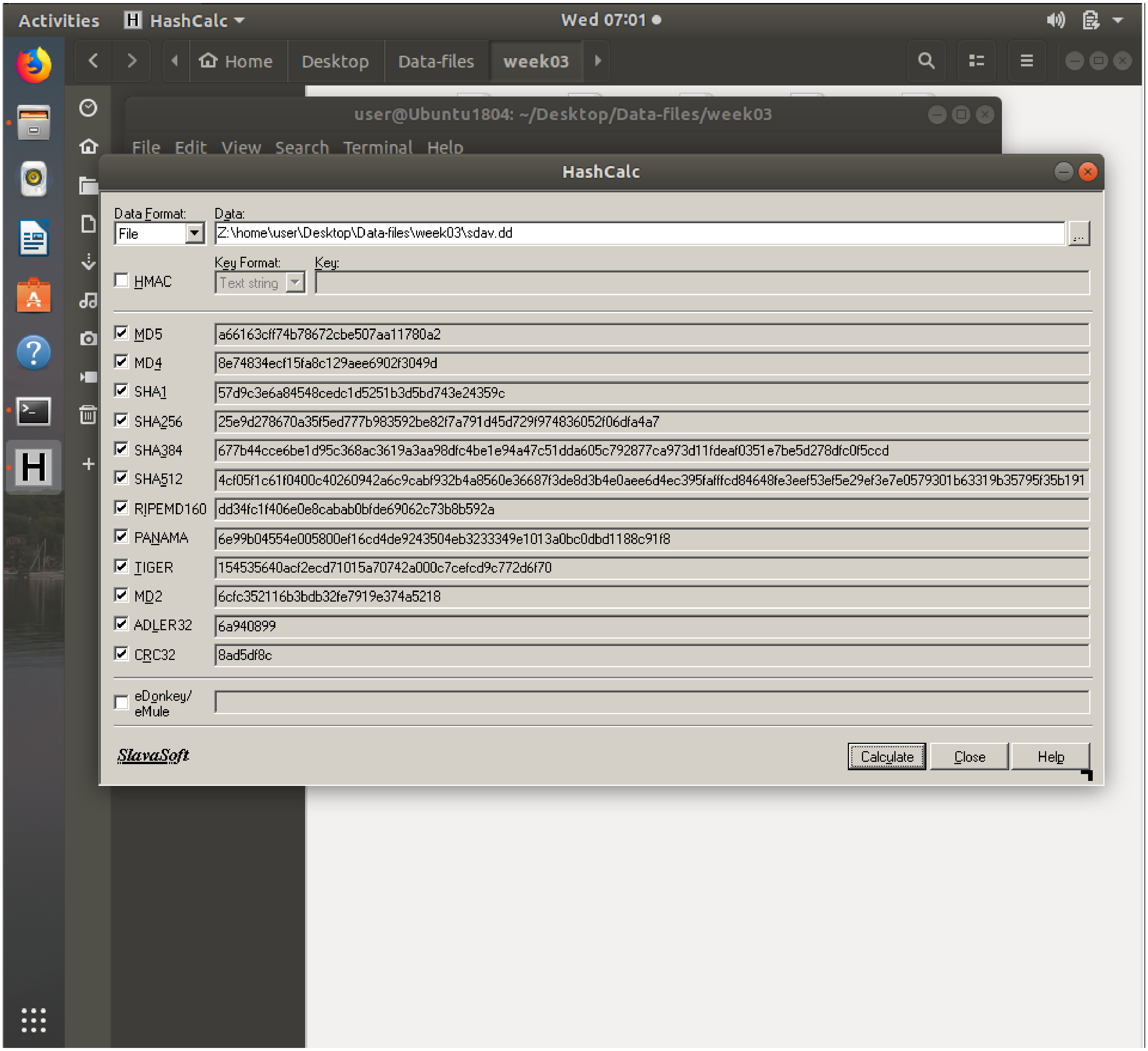
Data Format: File

Data: Z:\home\user\Desktop\Data-files\week03\sda.dd

□ HMAC Key Format: Text string Key:

☑ MD5	a66163cff74b78672cbe507aa11780a2
☑ MD4	8e74834ecf15fa8c129aee6902f3049d
☑ SHA1	57d9c3e6a84548cedc1d5251b3d5bd743e24359c
☑ SHA256	25e9d278670a35f5ed777b983592be82f7a791d45d729f974836052f06dfa4a7
☑ SHA384	677b44cce6be1d95c368ac3619a3aa98dfc4be1e94a47c51dda605c792877ca973d11fdeaf0351e7be5d278dfc0f5ccd
☑ SHA512	4cf05f1c61f0400c40260942a6c9cabf932b4a8560e36687f3de8d3b4e0aee6d4ec395fafffcd84648fe3eef53ef5e29ef3e7e0579301b63319b35795f35b191
☑ RIPEMD160	dd34fc1f406e0e8cabab0bfde69062c73b8b592a
☑ PANAMA	6e99b04554e005800ef16cd4de9243504eb3233349e1013a0bc0dbd1188c91f8
☑ TIGER	154535640acf2ecd71015a70742a000c7cefcd9c772d6f70
☑ MD2	6cfc352116b3bdb32fe7919e374a5218
☑ ADLER32	6a940899
☑ CRC32	8ad5df8c
□ eDonkey/ eMule	

Sdav.dd



Activities
HashCalc
Wed 07:01
Home
Desktop
Data-files
week03
user@Ubuntu1804: ~/Desktop/Data-files/week03
File Edit View Search Terminal Help
HashCalc

Data Format: File

Data: Z:\home\user\Desktop\Data-files\week03\sdav.dd

□ HMAC Key Format: Text string Key:

☑ MD5 a66163cff74b78672cbe507aa11780a2

☑ MD4 8e74834ecf15fa8c129aee6902f3049d

☑ SHA1 57d9c3e6a84548cedc1d5251b3d5bd743e24359c

☑ SHA256 25e9d278670a35f5ed777b983592be82f7a791d45d729f974836052f06dfa4a7

☑ SHA384 677b44cce6be1d95c368ac3619a3aa98dfc4be1e94a47c51dda605c792877ca973d11fdeaf0351e7be5d278dfc0f5ccd

☑ SHA512 4cf05f1c61f0400c40260942a6c9cabf932b4a8560e36687f3de8d3b4e0aee6d4ec395fafffcd84648fe3eef53ef5e29ef3e7e0579301b63319b35795f35b191

☑ RIPEMD160 dd34fc1f406e0e8cabab0bfde69062c73b8b592a

☑ PANAMA 6e99b04554e005800ef16cd4de9243504eb3233349e1013a0bc0dbd1188c91f8

☑ TIGER 154535640acf2ecd71015a70742a000c7cefcd9c772d6f70

☑ MD2 6cfc352116b3bdb32fe7919e374a5218

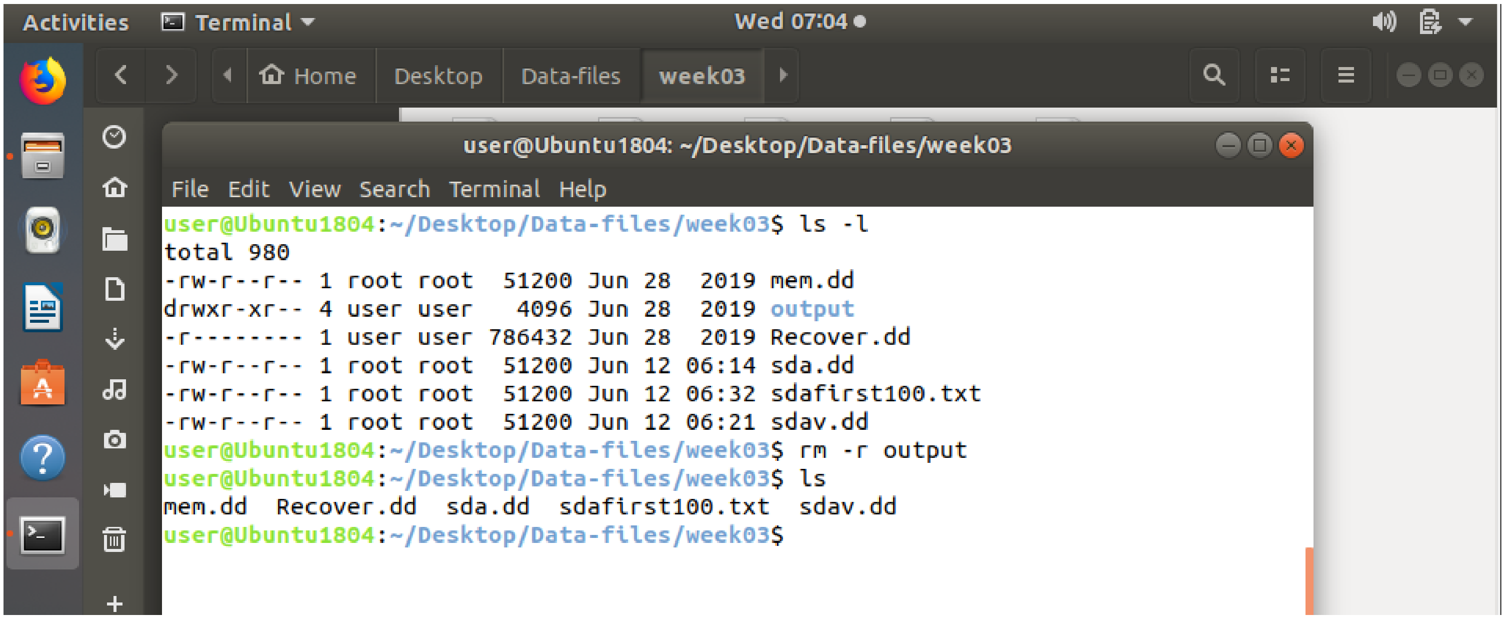
☑ ADLER32 6a940899

☑ CRC32 8ad5df8c

□ eDonkey/ eMule

Recovering Files Using Foremost

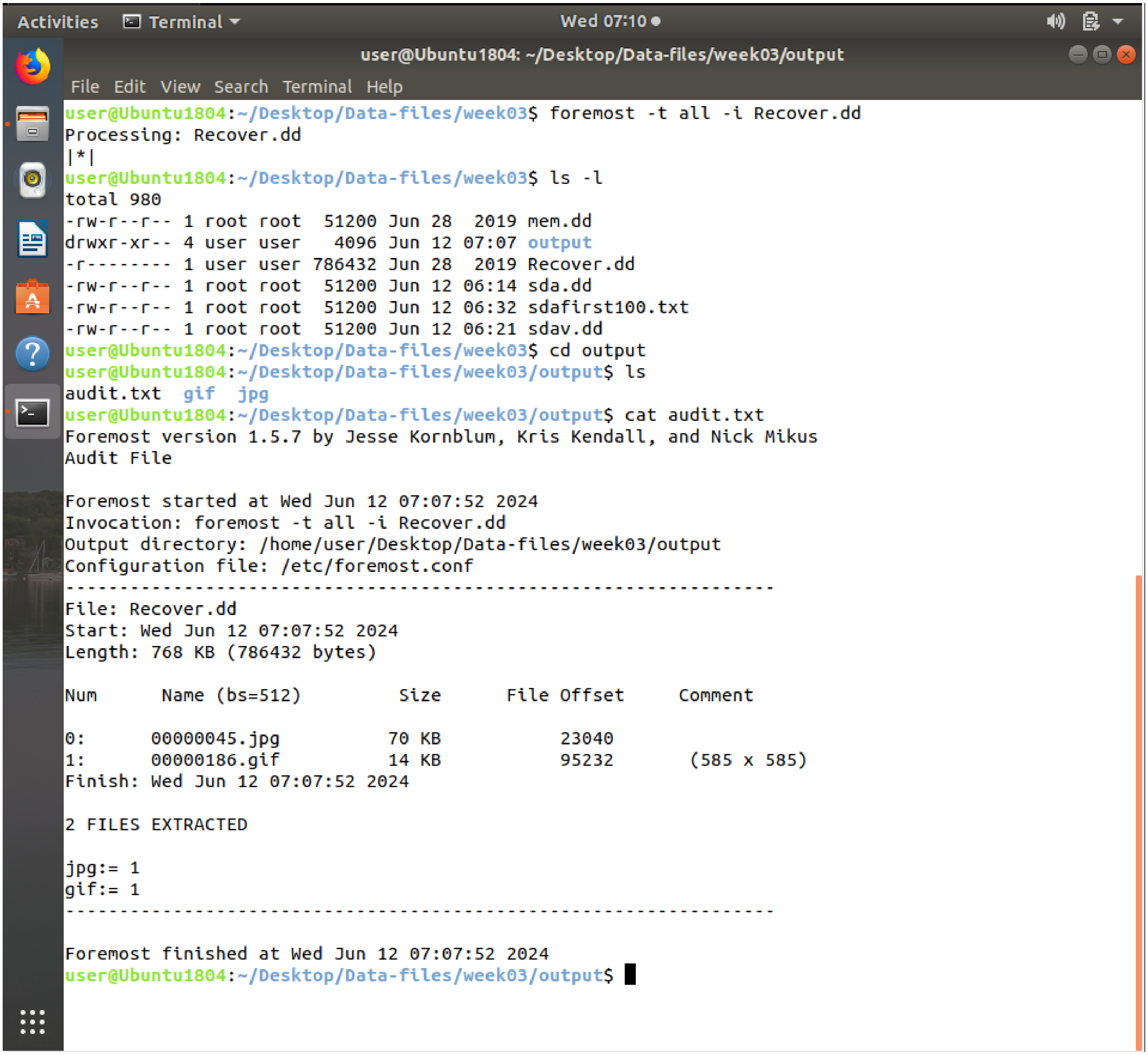
First, I made sure that there are no any other folders called output, so I deleted a directory which there already using the command “**rm -r output”**



Activities
Terminal
Wed 07:04
Home
Desktop
Data-files
week03
user@Ubuntu1804: ~/Desktop/Data-files/week03
File Edit View Search Terminal Help

```
user@Ubuntu1804:~/Desktop/Data-files/week03$ ls -l
total 980
-rw-r--r-- 1 root root  51200 Jun 28  2019 mem.dd
drwxr-xr-- 4 user user   4096 Jun 28  2019 output
-r-------- 1 user user 786432 Jun 28  2019 Recover.dd
-rw-r--r-- 1 root root  51200 Jun 12 06:14 sda.dd
-rw-r--r-- 1 root root  51200 Jun 12 06:32 sdafirst100.txt
-rw-r--r-- 1 root root  51200 Jun 12 06:21 sdav.dd
user@Ubuntu1804:~/Desktop/Data-files/week03$ rm -r output
user@Ubuntu1804:~/Desktop/Data-files/week03$ ls
mem.dd  Recover.dd  sda.dd  sdafirst100.txt  sdav.dd
user@Ubuntu1804:~/Desktop/Data-files/week03$
```

Then I typed in the command **“foremost -t all -i Recover.dd”** to recover the files from the Recover.dd image and create a directory called output which will have the recovered files.



Activities
Terminal
Wed 07:10
user@Ubuntu1804: ~/Desktop/Data-files/week03/output
File Edit View Search Terminal Help

```
user@Ubuntu1804:~/Desktop/Data-files/week03$ foremost -t all -i Recover.dd
Processing: Recover.dd
|*|
user@Ubuntu1804:~/Desktop/Data-files/week03$ ls -l
total 980
-rw-r--r-- 1 root root  51200 Jun 28  2019 mem.dd
drwxr-xr-- 4 user user   4096 Jun 12 07:07 output
-r-------- 1 user user 786432 Jun 28  2019 Recover.dd
-rw-r--r-- 1 root root  51200 Jun 12 06:14 sda.dd
-rw-r--r-- 1 root root  51200 Jun 12 06:32 sdafirst100.txt
-rw-r--r-- 1 root root  51200 Jun 12 06:21 sdav.dd
user@Ubuntu1804:~/Desktop/Data-files/week03$ cd output
user@Ubuntu1804:~/Desktop/Data-files/week03/output$ ls
audit.txt  gif  jpg
user@Ubuntu1804:~/Desktop/Data-files/week03/output$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Jun 12 07:07:52 2024
Invocation: foremost -t all -i Recover.dd
Output directory: /home/user/Desktop/Data-files/week03/output
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: Recover.dd
Start: Wed Jun 12 07:07:52 2024
Length: 768 KB (786432 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000045.jpg          70 KB           23040
1:      00000186.gif          14 KB           95232       (585 x 585)
Finish: Wed Jun 12 07:07:52 2024

2 FILES EXTRACTED

jpg:= 1
gif:= 1
------------------------------------------------------------------

Foremost finished at Wed Jun 12 07:07:52 2024
user@Ubuntu1804:~/Desktop/Data-files/week03/output$ 
```