

**PES1UG20CS581**

**ROHITH H**

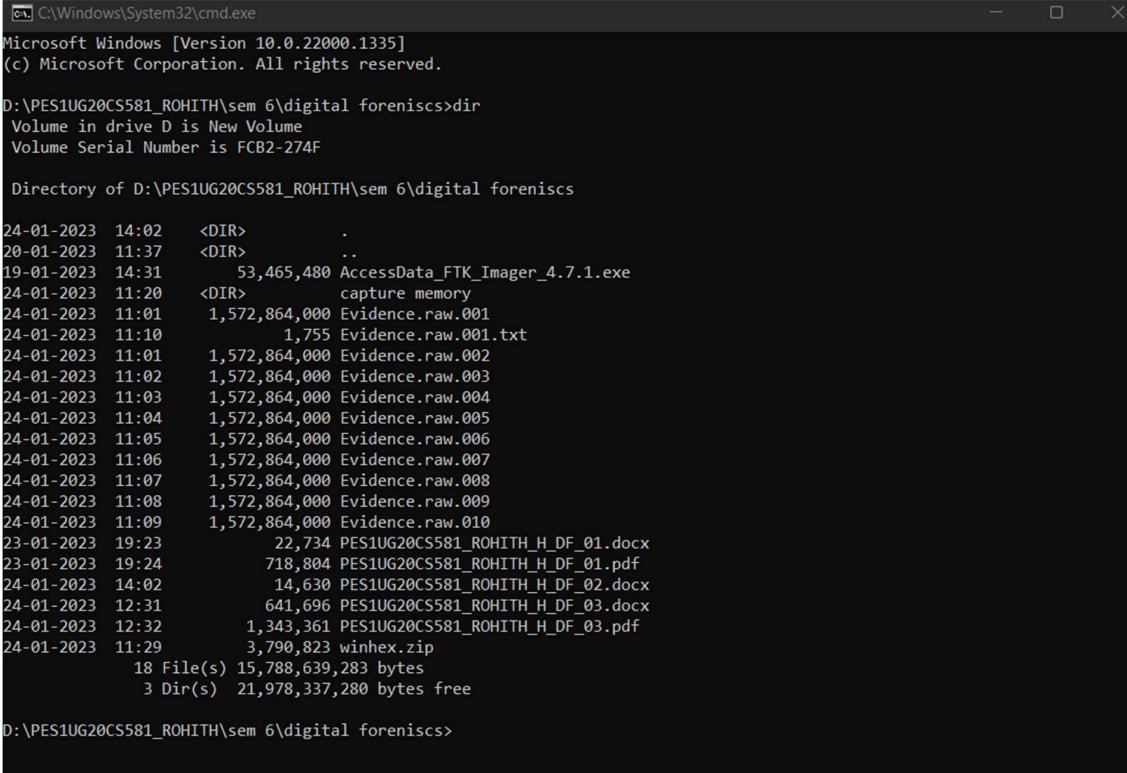
**J SEC**

## ***DIGITAL FORENSICS ASSIGNMENT -02***

### ***TASK -01***

#### ***USB Drive Acquisition from FTK imager***

***The DIR command to list all the items inside the directory***



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.1335]
(c) Microsoft Corporation. All rights reserved.

D:\PES1UG20CS581_ROHITH\sem 6\digital forensics>dir
Volume in drive D is New Volume
Volume Serial Number is FCB2-274F

Directory of D:\PES1UG20CS581_ROHITH\sem 6\digital forensics

24-01-2023  14:02    <DIR>          .
20-01-2023  11:37    <DIR>          ..
19-01-2023  14:31             53,465,480  AccessData_FTK_Imager_4.7.1.exe
24-01-2023  11:20    <DIR>          capture memory
24-01-2023  11:01      1,572,864,000 Evidence.raw.001
24-01-2023  11:10             1,755 Evidence.raw.001.txt
24-01-2023  11:01      1,572,864,000 Evidence.raw.002
24-01-2023  11:02      1,572,864,000 Evidence.raw.003
24-01-2023  11:03      1,572,864,000 Evidence.raw.004
24-01-2023  11:04      1,572,864,000 Evidence.raw.005
24-01-2023  11:05      1,572,864,000 Evidence.raw.006
24-01-2023  11:06      1,572,864,000 Evidence.raw.007
24-01-2023  11:07      1,572,864,000 Evidence.raw.008
24-01-2023  11:08      1,572,864,000 Evidence.raw.009
24-01-2023  11:09      1,572,864,000 Evidence.raw.010
23-01-2023  19:23             22,734 PES1UG20CS581_ROHITH_H_DF_01.docx
23-01-2023  19:24             718,804 PES1UG20CS581_ROHITH_H_DF_01.pdf
24-01-2023  14:02             14,630 PES1UG20CS581_ROHITH_H_DF_02.docx
24-01-2023  12:31             641,696 PES1UG20CS581_ROHITH_H_DF_03.docx
24-01-2023  12:32             1,343,361 PES1UG20CS581_ROHITH_H_DF_03.pdf
24-01-2023  11:29             3,790,823 winhex.zip
                18 File(s) 15,788,639,283 bytes
                3 Dir(s)  21,978,337,280 bytes free

D:\PES1UG20CS581_ROHITH\sem 6\digital forensics>
```

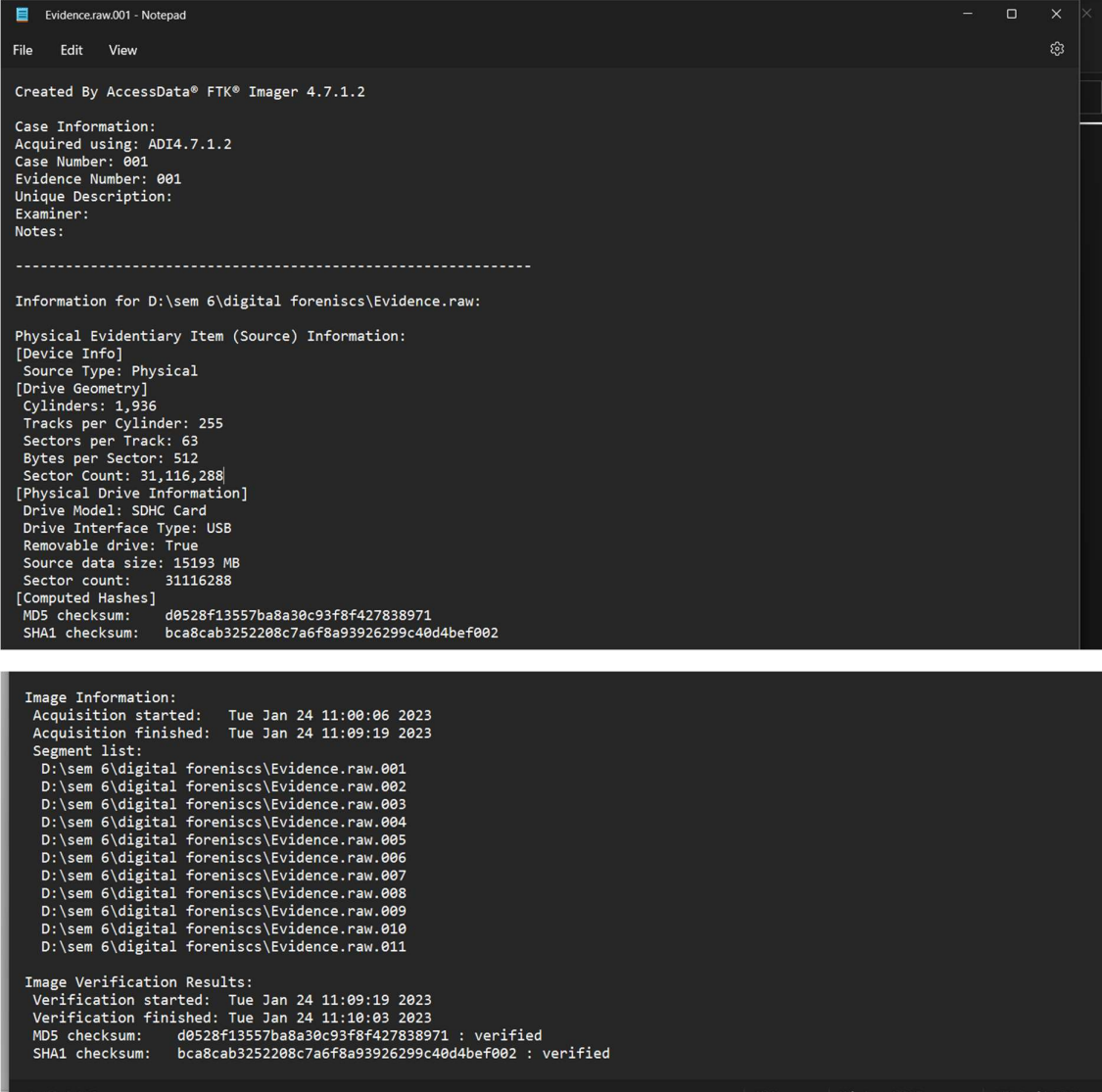
***The file obtained after capturing the USB drive by using the FTK Image Capture***

**PES1UG20CS581**

**ROHITH H**

**J SEC**

## ***DIGITAL FORENSICS ASSIGNMENT -02***



```
Evidence.raw.001 - Notepad
File Edit View

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: 001
Unique Description:
Examiner:
Notes:

-----

Information for D:\sem 6\digital forensics\Evidence.raw:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 1,936
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 31,116,288
[Physical Drive Information]
Drive Model: SDHC Card
Drive Interface Type: USB
Removable drive: True
Source data size: 15193 MB
Sector count: 31116288
[Computed Hashes]
MD5 checksum: d0528f13557ba8a30c93f8f427838971
SHA1 checksum: bca8cab3252208c7a6f8a93926299c40d4bef002


Image Information:
Acquisition started: Tue Jan 24 11:00:06 2023
Acquisition finished: Tue Jan 24 11:09:19 2023
Segment list:
D:\sem 6\digital forensics\Evidence.raw.001
D:\sem 6\digital forensics\Evidence.raw.002
D:\sem 6\digital forensics\Evidence.raw.003
D:\sem 6\digital forensics\Evidence.raw.004
D:\sem 6\digital forensics\Evidence.raw.005
D:\sem 6\digital forensics\Evidence.raw.006
D:\sem 6\digital forensics\Evidence.raw.007
D:\sem 6\digital forensics\Evidence.raw.008
D:\sem 6\digital forensics\Evidence.raw.009
D:\sem 6\digital forensics\Evidence.raw.010
D:\sem 6\digital forensics\Evidence.raw.011

Image Verification Results:
Verification started: Tue Jan 24 11:09:19 2023
Verification finished: Tue Jan 24 11:10:03 2023
MD5 checksum: d0528f13557ba8a30c93f8f427838971 : verified
SHA1 checksum: bca8cab3252208c7a6f8a93926299c40d4bef002 : verified
```

### ***TASK -02***

#### ***Memory Acquisition Using FTK imager***

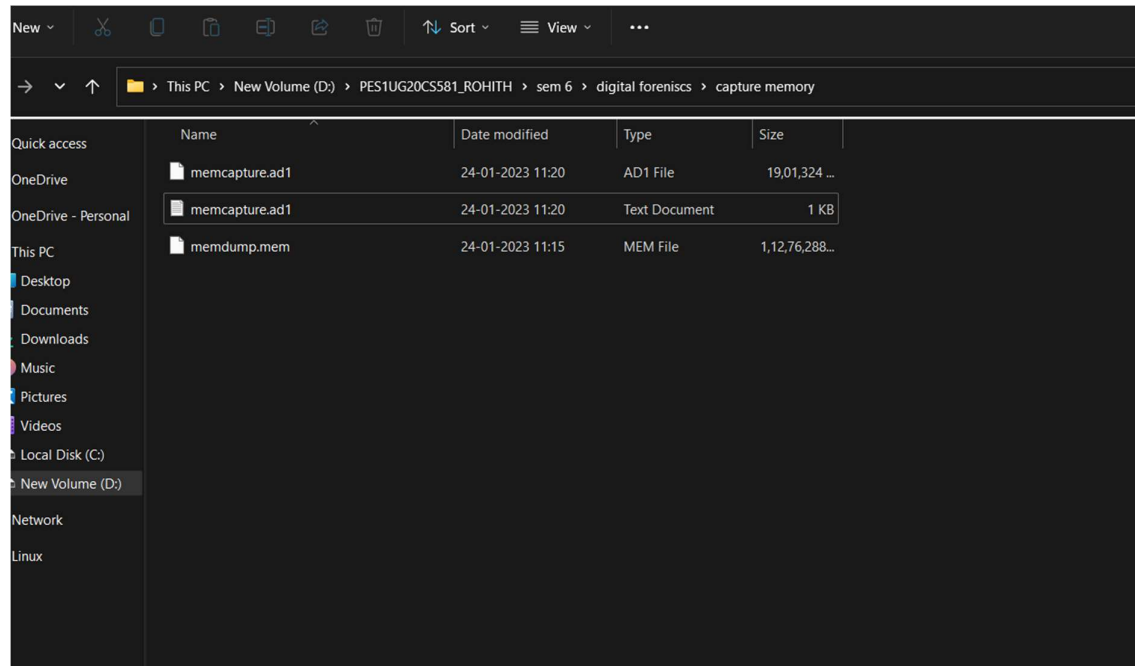
*The list of items obtained after capturing the memory by using the FTK imager the macro editor file that is the mem file is been shown in the below screenshot*

**PES1UG20CS581**

**ROHITH H**

**J SEC**

### ***DIGITAL FORENSICS ASSIGNMENT -02***



*The text file which was obtained when we did the memory capture is given below*

