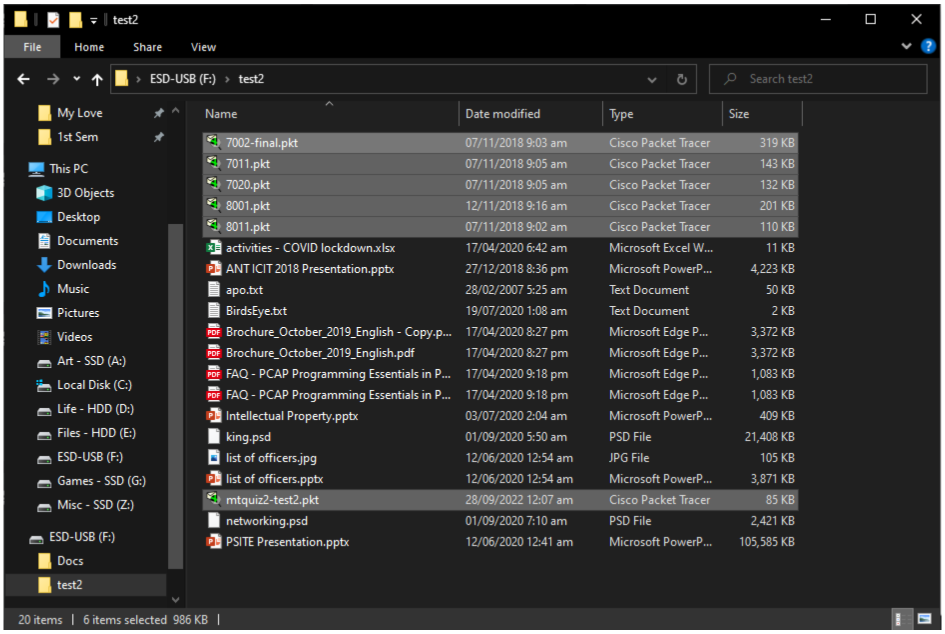
1. Prepare your flash drive.

2. Go to google drive, under digital forensic software, copy the test 2 folder on your clean flash drive.

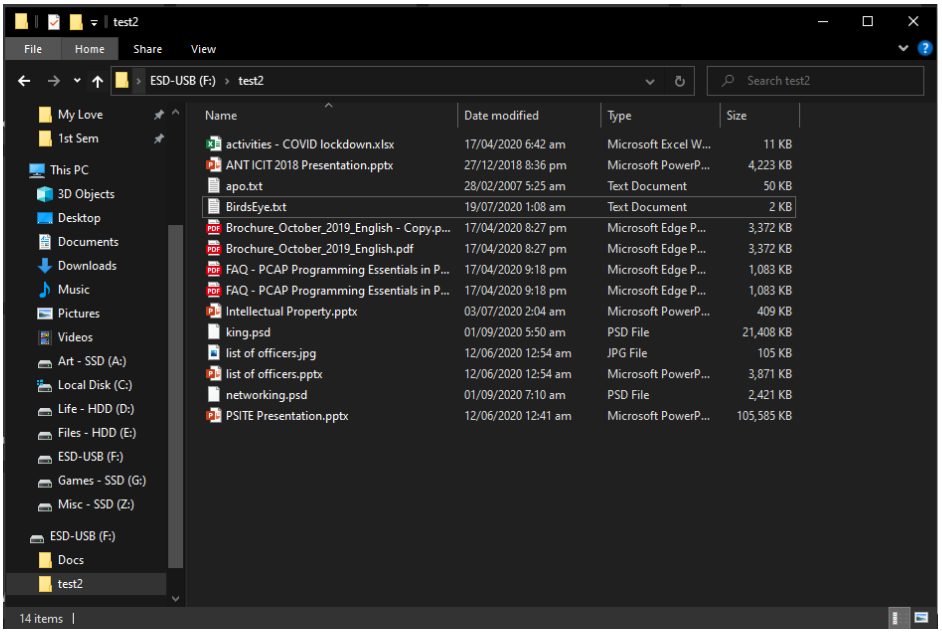


Name	Date modified	Type	Size
7002-final.pkt	07/11/2018 9:03 am	Cisco Packet Tracer	319 KB
7011.pkt	07/11/2018 9:05 am	Cisco Packet Tracer	143 KB
7020.pkt	07/11/2018 9:05 am	Cisco Packet Tracer	132 KB
8001.pkt	12/11/2018 9:16 am	Cisco Packet Tracer	201 KB
8011.pkt	07/11/2018 9:02 am	Cisco Packet Tracer	110 KB
activities - COVID lockdown.xlsx	17/04/2020 6:42 am	Microsoft Excel W...	11 KB
ANT ICIT 2018 Presentation.pptx	27/12/2018 8:36 pm	Microsoft PowerP...	4,223 KB
apo.txt	28/02/2007 5:25 am	Text Document	50 KB
BirdsEye.txt	19/07/2020 1:08 am	Text Document	2 KB
Brochure_October_2019_English - Copy.p...	17/04/2020 8:27 pm	Microsoft Edge P...	3,372 KB
Brochure_October_2019_English.pdf	17/04/2020 8:27 pm	Microsoft Edge P...	3,372 KB
FAQ - PCAP Programming Essentials in P...	17/04/2020 9:18 pm	Microsoft Edge P...	1,083 KB
FAQ - PCAP Programming Essentials in P...	17/04/2020 9:18 pm	Microsoft Edge P...	1,083 KB
Intellectual Property.pptx	03/07/2020 2:04 am	Microsoft PowerP...	409 KB
king.psd	01/09/2020 5:50 am	PSD File	21,408 KB
list of officers.jpg	12/06/2020 12:54 am	JPG File	105 KB
list of officers.pptx	12/06/2020 12:54 am	Microsoft PowerP...	3,871 KB
mtquiz2-test2.pkt	28/09/2022 12:07 am	Cisco Packet Tracer	85 KB
networking.psd	01/09/2020 7:10 am	PSD File	2,421 KB
PSITE Presentation.pptx	12/06/2020 12:41 am	Microsoft PowerP...	105,585 KB

20 items | 6 items selected 986 KB |

3. Go to your flash drive and erase all packet tracer files. Take a screenshot of the files deleted

Proof that Files have been deleted

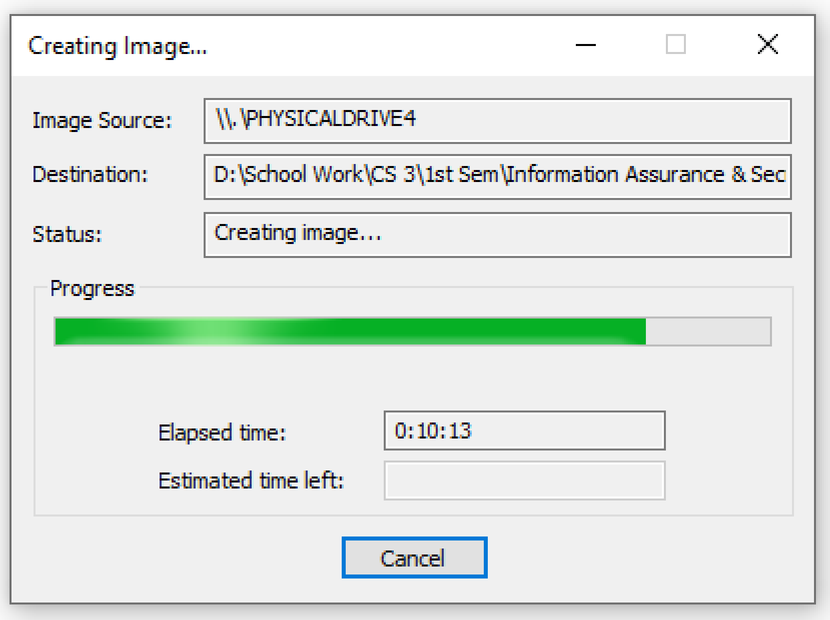


Name	Date modified	Type	Size
activities - COVID lockdown.xlsx	17/04/2020 6:42 am	Microsoft Excel W...	11 KB
ANT ICIT 2018 Presentation.pptx	27/12/2018 8:36 pm	Microsoft PowerP...	4,223 KB
apo.txt	28/02/2007 5:25 am	Text Document	50 KB
BirdsEye.txt	19/07/2020 1:08 am	Text Document	2 KB
Brochure_October_2019_English - Copy.p...	17/04/2020 8:27 pm	Microsoft Edge P...	3,372 KB
Brochure_October_2019_English.pdf	17/04/2020 8:27 pm	Microsoft Edge P...	3,372 KB
FAQ - PCAP Programming Essentials in P...	17/04/2020 9:18 pm	Microsoft Edge P...	1,083 KB
FAQ - PCAP Programming Essentials in P...	17/04/2020 9:18 pm	Microsoft Edge P...	1,083 KB
Intellectual Property.pptx	03/07/2020 2:04 am	Microsoft PowerP...	409 KB
king.psd	01/09/2020 5:50 am	PSD File	21,408 KB
list of officers.jpg	12/06/2020 12:54 am	JPG File	105 KB
list of officers.pptx	12/06/2020 12:54 am	Microsoft PowerP...	3,871 KB
networking.psd	01/09/2020 7:10 am	PSD File	2,421 KB
PSITE Presentation.pptx	12/06/2020 12:41 am	Microsoft PowerP...	105,585 KB

14 items |

4. Using your pro-Discover or Access Data FTK, recover the mtquiz2-test2. Take a screenshot of the steps in recovering the file.

Creating an image of the USB drive



Creating Image...

Image Source: \\.\PHYSICALDRIVE4

Destination: D:\School Work\CS 3\1st Sem\Information Assurance & Sec

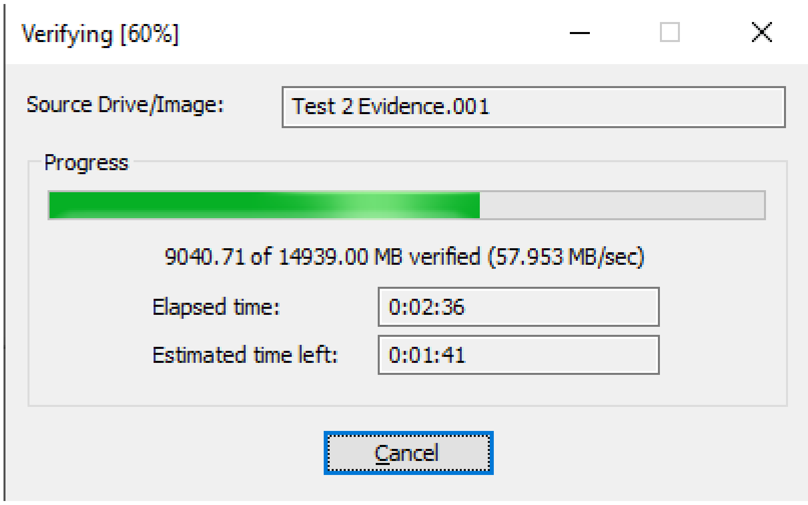
Status: Creating image...

Progress

Elapsed time: 0:10:13

Estimated time left:

Verifying that evidence is unchanged



Verifying [60%]

Source Drive/Image: Test 2 Evidence.001

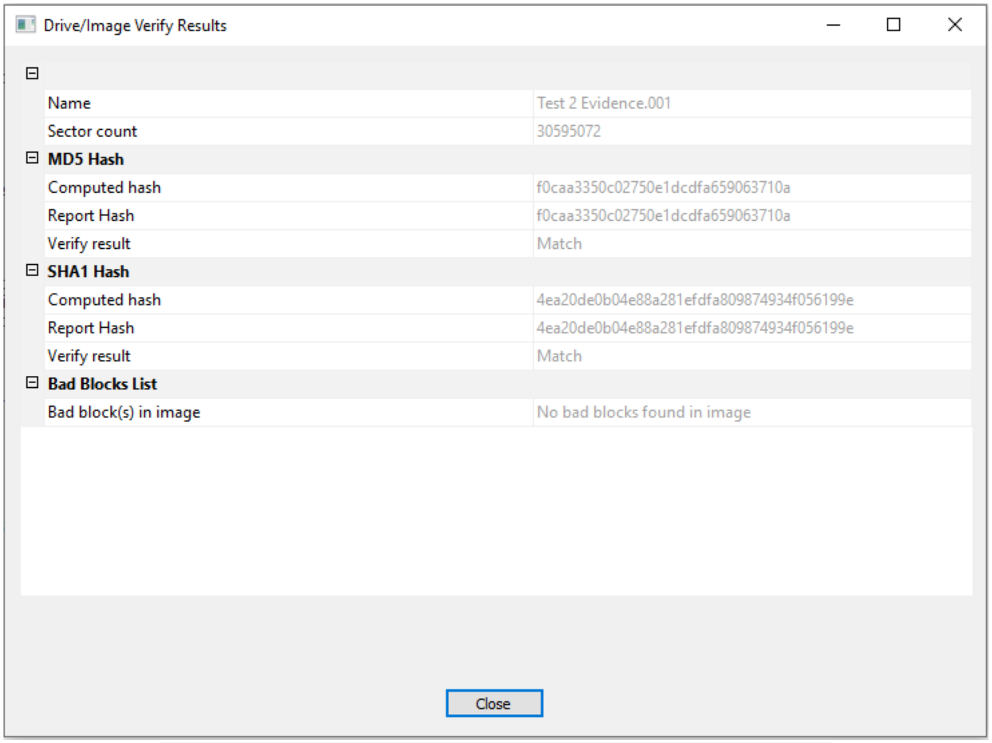
Progress

9040.71 of 14939.00 MB verified (57.953 MB/sec)

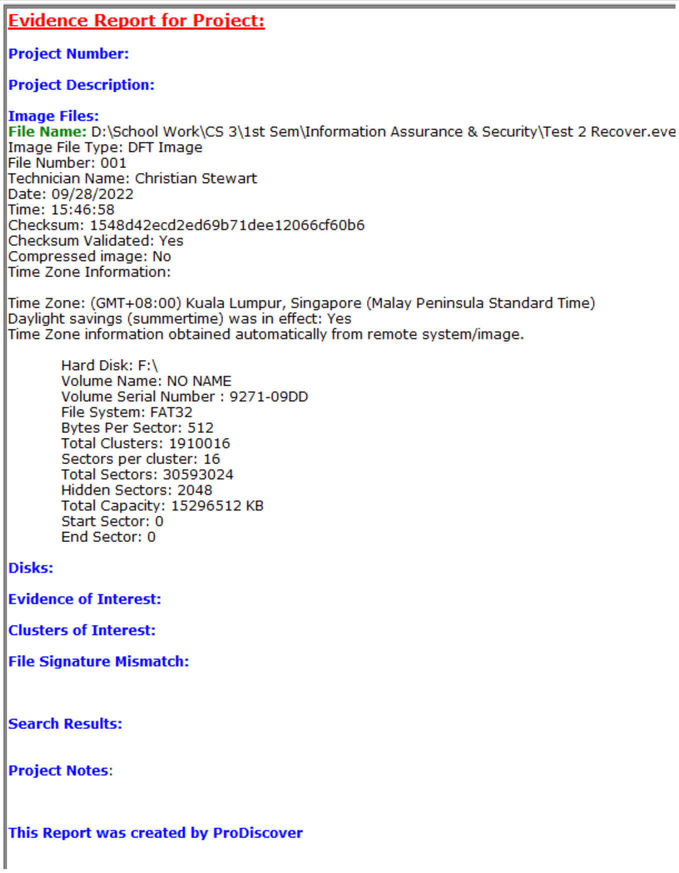
Elapsed time: 0:02:36

Estimated time left: 0:01:41

Proof that evidence is unchanged



Name	Test 2 Evidence.001
Sector count	30595072
MD5 Hash	
Computed hash	f0caa3350c02750e1dcdfa659063710a
Report Hash	f0caa3350c02750e1dcdfa659063710a
Verify result	Match
SHA1 Hash	
Computed hash	4ea20de0b04e88a281efdfa809874934f056199e
Report Hash	4ea20de0b04e88a281efdfa809874934f056199e
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image



Evidence Report for Project:

Project Number:

Project Description:

Image Files:
File Name: D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Recover.eve
Image File Type: DFT Image
File Number: 001
Technician Name: Christian Stewart
Date: 09/28/2022
Time: 15:46:58
Checksum: 1548d42ecd2ed69b71dee12066cf60b6
Checksum Validated: Yes
Compressed image: No
Time Zone Information:

Time Zone: (GMT+08:00) Kuala Lumpur, Singapore (Malay Peninsula Standard Time)
Daylight savings (summertime) was in effect: Yes
Time Zone information obtained automatically from remote system/image.

```
        Hard Disk: F:\
        Volume Name: NO NAME
        Volume Serial Number : 9271-09DD
        File System: FAT32
        Bytes Per Sector: 512
        Total Clusters: 1910016
        Sectors per cluster: 16
        Total Sectors: 30593024
        Hidden Sectors: 2048
        Total Capacity: 15296512 KB
        Start Sector: 0
        End Sector: 0
```

Disks:

Evidence of Interest:

Clusters of Interest:

File Signature Mismatch:

Search Results:

Project Notes:

This Report was created by ProDiscover

Summary of Findings

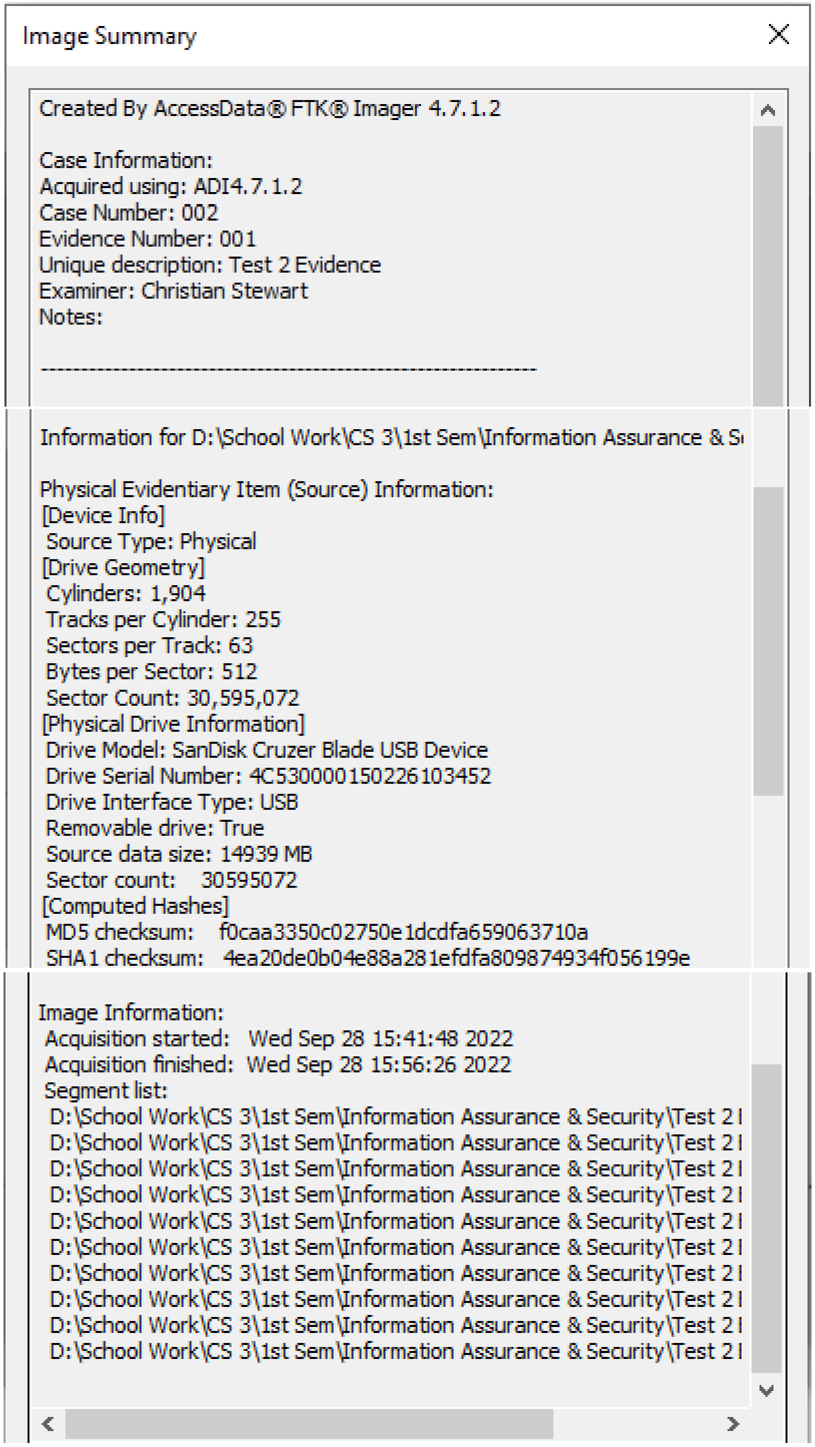
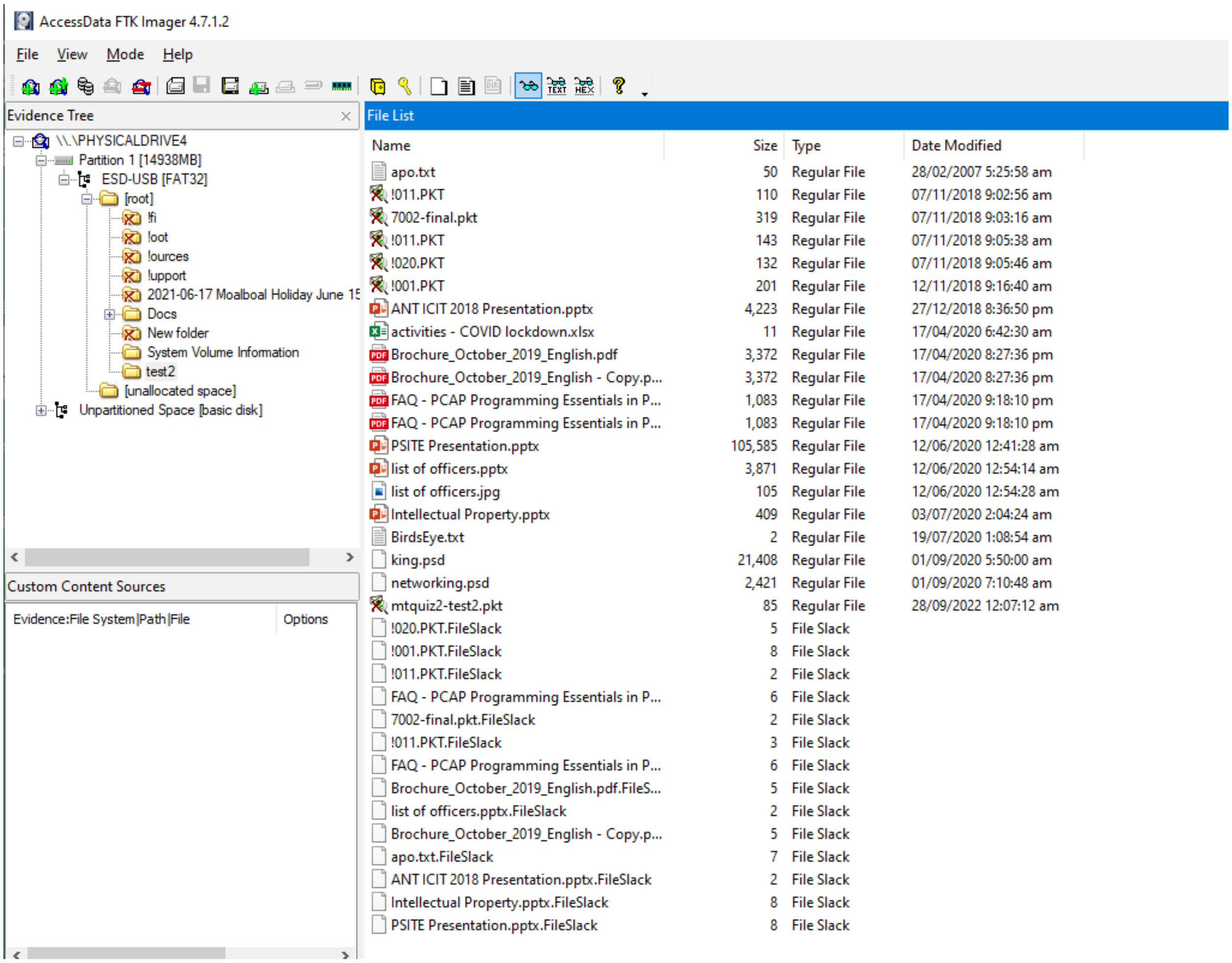


Image Summary

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 002
Evidence Number: 001
Unique description: Test 2 Evidence
Examiner: Christian Stewart
Notes:

--------------------------------------------------------------

Information for D:\School Work\CS 3\1st Sem\Information Assurance & S

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,904
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30,595,072
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530000150226103452
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 14939 MB
 Sector count:    30595072
[Computed Hashes]
 MD5 checksum:    f0caa3350c02750e1dcdfa659063710a
 SHA1 checksum:   4ea20de0b04e88a281efdfa809874934f056199e

Image Information:
 Acquisition started:   Wed Sep 28 15:41:48 2022
 Acquisition finished:  Wed Sep 28 15:56:26 2022
 Segment list:
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 I
```

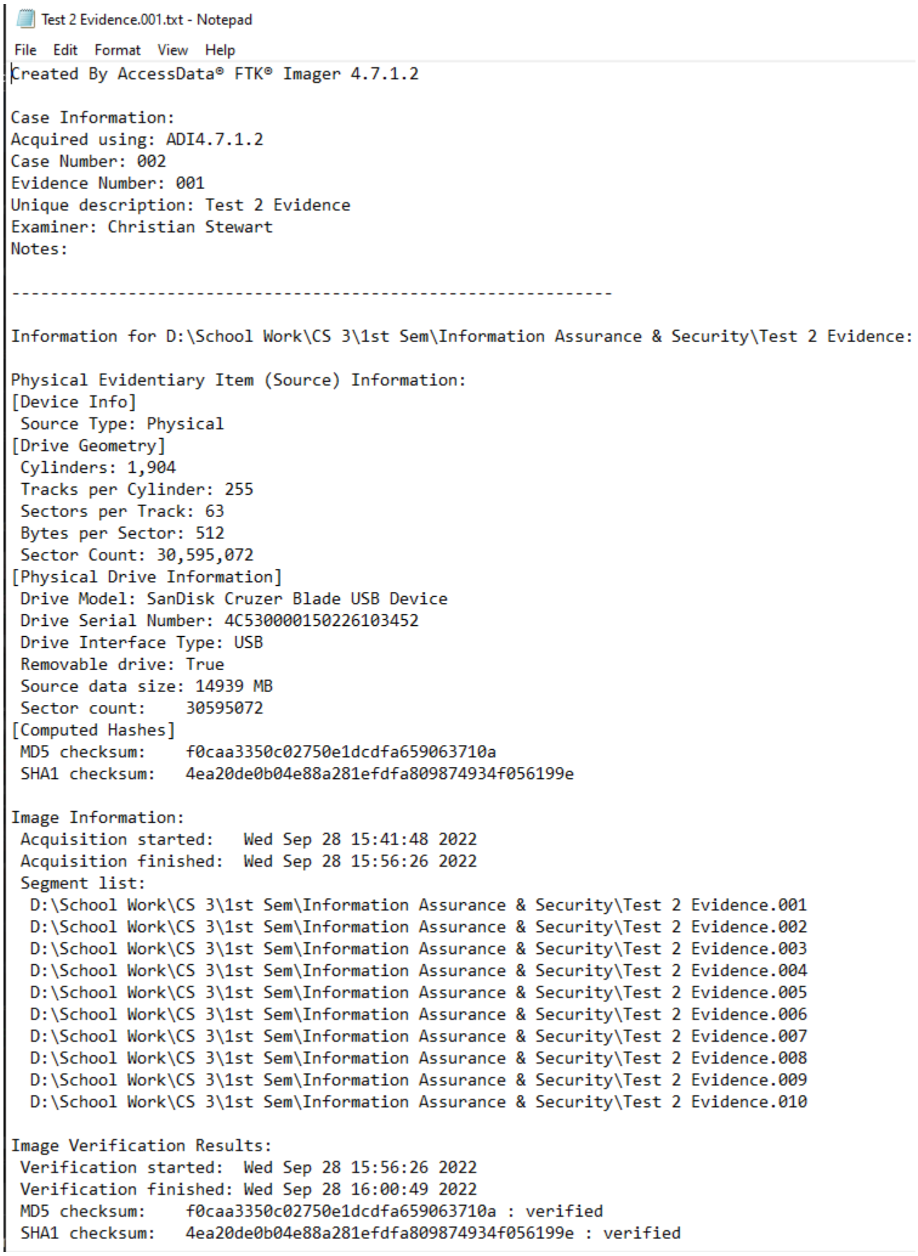
Viewing of Evidence and Deleted Files



```
\\.\PHYSICALDRIVE4
  Partition 1 [14938MB]
    ESD-USB [FAT32]
      [root]
        !fi
        !oot
        !ources
        !upport
        2021-06-17 Moalboal Holiday June 15
        Docs
        New folder
        System Volume Information
        test2
      [unallocated space]
  Unpartitioned Space [basic disk]
```

Name	Size	Type	Date Modified
apo.txt	50	Regular File	28/02/2007 5:25:58 am
!011.PKT	110	Regular File	07/11/2018 9:02:56 am
7002-final.pkt	319	Regular File	07/11/2018 9:03:16 am
!011.PKT	143	Regular File	07/11/2018 9:05:38 am
!020.PKT	132	Regular File	07/11/2018 9:05:46 am
!001.PKT	201	Regular File	12/11/2018 9:16:40 am
ANT ICIT 2018 Presentation.pptx	4,223	Regular File	27/12/2018 8:36:50 pm
activities - COVID lockdown.xlsx	11	Regular File	17/04/2020 6:42:30 am
Brochure_October_2019_English.pdf	3,372	Regular File	17/04/2020 8:27:36 pm
Brochure_October_2019_English - Copy.p...	3,372	Regular File	17/04/2020 8:27:36 pm
FAQ - PCAP Programming Essentials in P...	1,083	Regular File	17/04/2020 9:18:10 pm
FAQ - PCAP Programming Essentials in P...	1,083	Regular File	17/04/2020 9:18:10 pm
PSITE Presentation.pptx	105,585	Regular File	12/06/2020 12:41:28 am
list of officers.pptx	3,871	Regular File	12/06/2020 12:54:14 am
list of officers.jpg	105	Regular File	12/06/2020 12:54:28 am
Intellectual Property.pptx	409	Regular File	03/07/2020 2:04:24 am
BirdsEye.txt	2	Regular File	19/07/2020 1:08:54 am
king.psd	21,408	Regular File	01/09/2020 5:50:00 am
networking.psd	2,421	Regular File	01/09/2020 7:10:48 am
mtquiz2-test2.pkt	85	Regular File	28/09/2022 12:07:12 am
!020.PKT.FileSlack	5	File Slack	
!001.PKT.FileSlack	8	File Slack	
!011.PKT.FileSlack	2	File Slack	
FAQ - PCAP Programming Essentials in P...	6	File Slack	
7002-final.pkt.FileSlack	2	File Slack	
!011.PKT.FileSlack	3	File Slack	
FAQ - PCAP Programming Essentials in P...	6	File Slack	
Brochure_October_2019_English.pdf.FileS...	5	File Slack	
list of officers.pptx.FileSlack	2	File Slack	
Brochure_October_2019_English - Copy.p...	5	File Slack	
apo.txt.FileSlack	7	File Slack	
ANT ICIT 2018 Presentation.pptx.FileSlack	2	File Slack	
Intellectual Property.pptx.FileSlack	8	File Slack	
PSITE Presentation.pptx.FileSlack	8	File Slack	

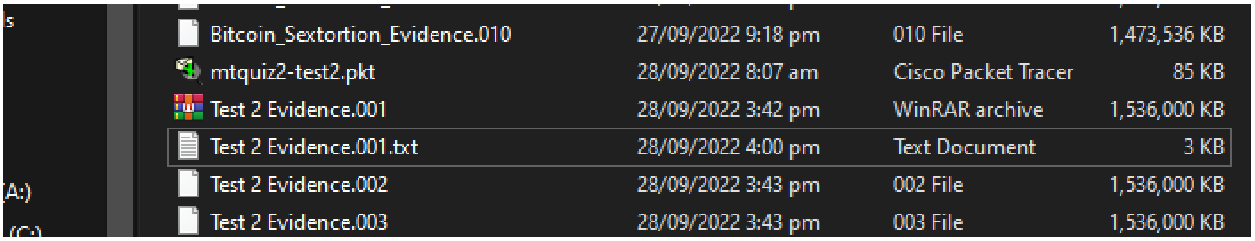
Text File as Proof



```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 002
Evidence Number: 001
Unique description: Test 2 Evidence
Examiner: Christian Stewart
Notes:

--------------------------------------------------------------

Information for D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,904
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30,595,072
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530000150226103452
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 14939 MB
 Sector count:    30595072
[Computed Hashes]
 MD5 checksum:    f0caa3350c02750e1dcdfa659063710a
 SHA1 checksum:   4ea20de0b04e88a281efdfa809874934f056199e

Image Information:
 Acquisition started:   Wed Sep 28 15:41:48 2022
 Acquisition finished:  Wed Sep 28 15:56:26 2022
 Segment list:
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.001
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.002
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.003
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.004
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.005
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.006
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.007
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.008
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.009
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Test 2 Evidence.010

Image Verification Results:
 Verification started:  Wed Sep 28 15:56:26 2022
 Verification finished: Wed Sep 28 16:00:49 2022
 MD5 checksum:    f0caa3350c02750e1dcdfa659063710a : verified
 SHA1 checksum:   4ea20de0b04e88a281efdfa809874934f056199e : verified
```

Test 2
Evidence.001.txt

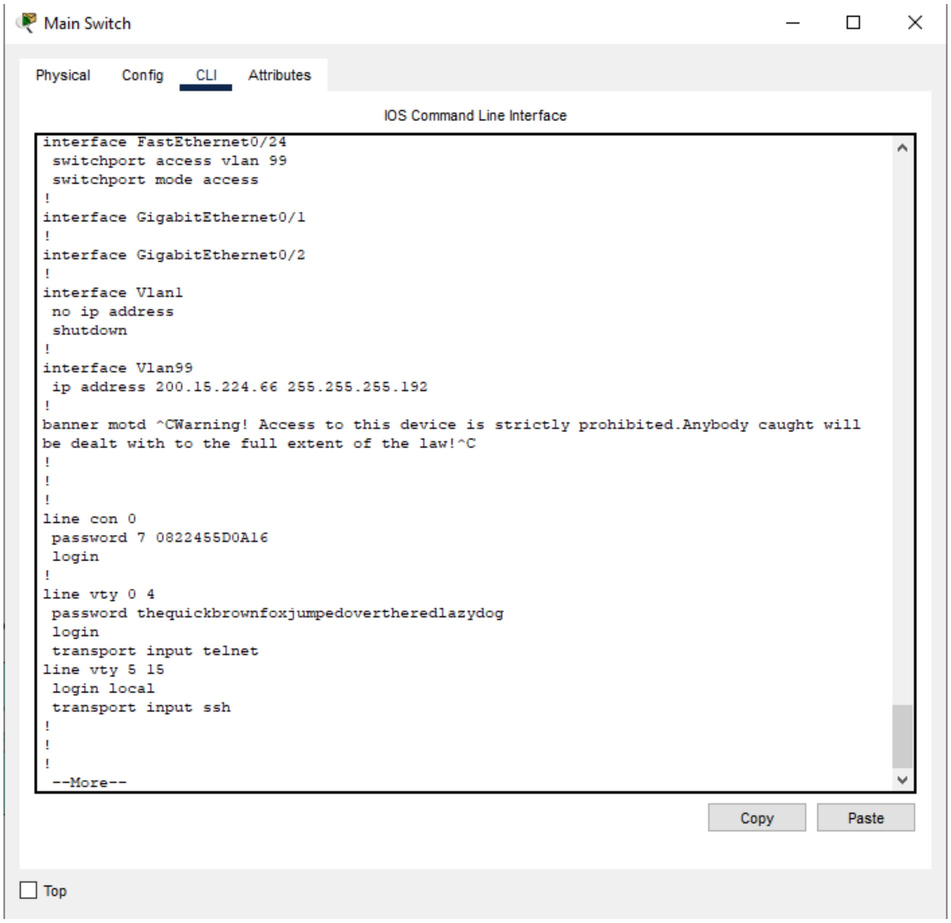
Proof that File has been recovered



Bitcoin_Sextortion_Evidence.010	27/09/2022 9:18 pm	010 File	1,473,536 KB
mtquiz2-test2.pkt	28/09/2022 8:07 am	Cisco Packet Tracer	85 KB
Test 2 Evidence.001	28/09/2022 3:42 pm	WinRAR archive	1,536,000 KB
Test 2 Evidence.001.txt	28/09/2022 4:00 pm	Text Document	3 KB
Test 2 Evidence.002	28/09/2022 3:43 pm	002 File	1,536,000 KB
Test 2 Evidence.003	28/09/2022 3:43 pm	003 File	1,536,000 KB

5. Once recovered, use the password for your Test 3 Exam, it is the password in the line vty 0 4.

Proof that password has been found



```
interface FastEthernet0/24
 switchport access vlan 99
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 200.15.224.66 255.255.255.192
!
banner motd ^CWarning! Access to this device is strictly prohibited.Anybody caught will
be dealt with to the full extent of the law!^C
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password thequickbrownfoxjumpedovertheredlazydog
 login
 transport input telnet
line vty 5 15
 login local
 transport input ssh
!
!
!
 --More--
```

thequickbrownfoxjumpedovertheredlazydog is the password

6. Start taking the MT Quiz2: Test 3