Experiment No .8

6.1 Aim: Static Acquisition: Using a Write Blocker, Creating a Forensic Image

Example Scenario:
You are working as an intern in a digital forensics lab. The lab receives a suspect's hard drive for investigation. Before you can analyze it, you must make sure the data on the drive is not changed in any way. To do this, you connect the drive through a **write blocker** so it can only be read, not written to.
Next, you create a **forensic image** — a complete copy of the drive — using a forensic tool. This image will be used for examination while keeping the original drive safe and untouched.

Tasks:

1. Connect the suspect's hard drive to your computer using a **write blocker**.
2. Check that the drive is detected as **read-only** on your system.
3. Open a forensic imaging tool such as **FTK Imager, Autopsy, or EnCase Imager**.
4. Create a **bit-by-bit copy** (forensic image) of the drive.
5. Generate **hash values (MD5/SHA1)** for both the original drive and the image.
6. Compare the hash values to confirm that the image is an exact copy.
7. Take screenshots or write short notes for each step as part of your lab record.

6.2 Lab Outcome :

- To learn how to safely collect digital evidence by using a write blocker and creating a verified forensic image without changing the original data.

6.3Learning Objectives:

- To understand what **static acquisition** means in digital forensics.
- To learn how to create and verify a **forensic image**.
- To know how a **write blocker** protects evidence from being changed.
- To use **hash values** to confirm that a forensic image is identical to the original media.

6.4 Requirement:

Hardware:

- A computer or laptop (forensic workstation)
- Suspect's hard drive or USB drive
- Write blocker device or software
- External storage drive to save the image

Software:

- FTK Imager / Autopsy / EnCase Imager / dc3dd
- Hash calculator (MD5/SHA1)
- Windows or Linux operating system

6.5 Related Theory :

Static Acquisition:

In static acquisition, data is collected from a device that is turned off. The storage device is connected to the forensic computer using a write blocker to avoid any accidental changes.

Write Blocker:

A write blocker lets you read data from a storage device but stops any writing or editing. It protects the original evidence so it can be accepted in court.

Forensic Image:

A forensic image is a complete copy of a drive — including deleted files and hidden areas. It is used for analysis so that the original drive remains unchanged.

Hash Verification:

Hashing is a method of generating a unique digital fingerprint for data. If the hash values of the original drive and the forensic image are the same, it means the image is an exact copy with no alterations.

6.6 Output:

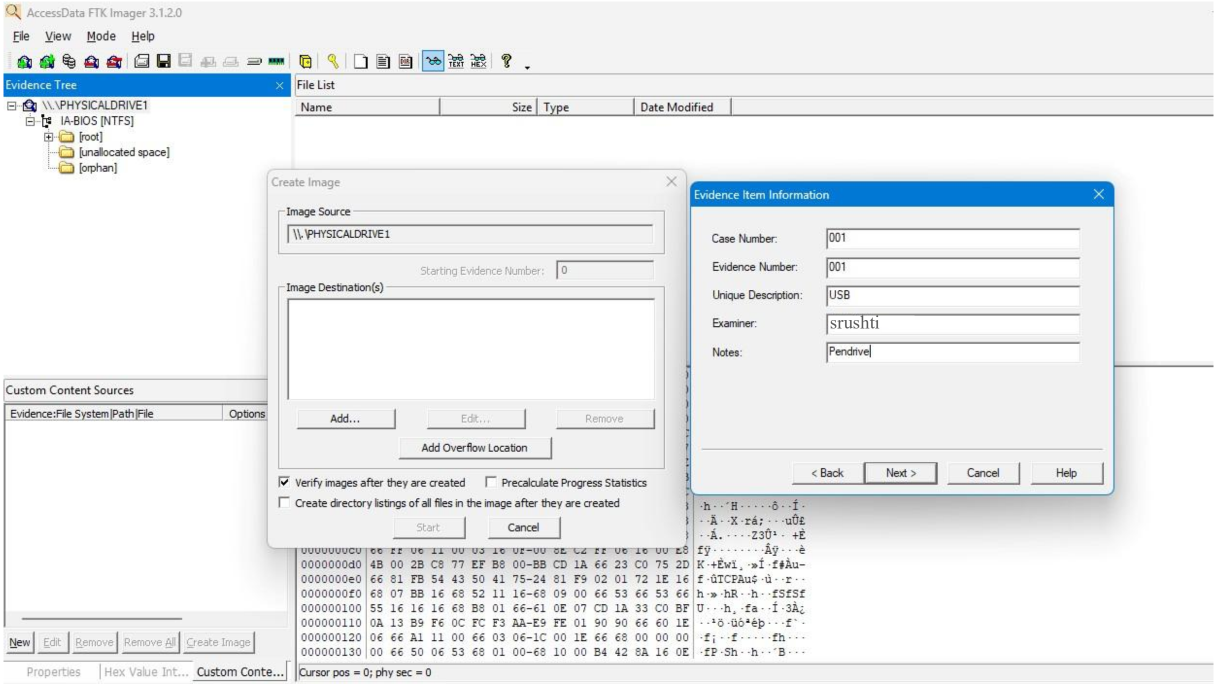


Image Source: \\.\PHYSICALDRIVE1

Starting Evidence Number: 0

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Case Number: 001

Evidence Number: 001

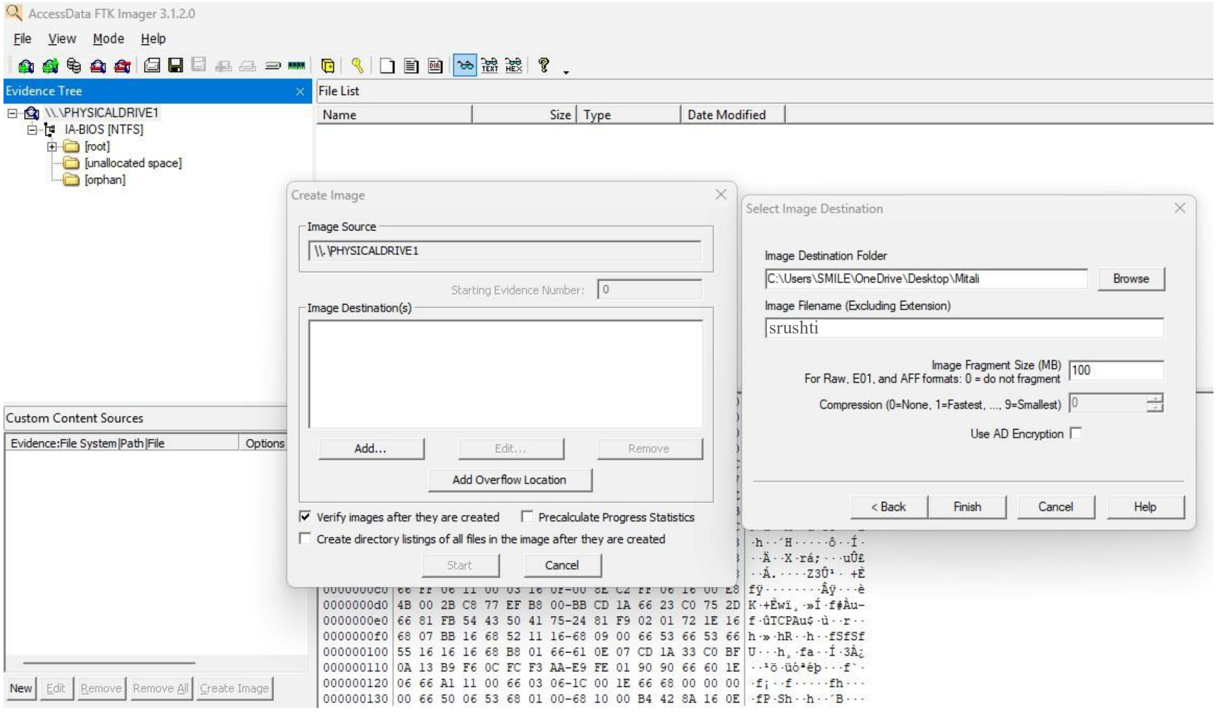
Unique Description: USB

Examiner: srushti

Notes: Pendrive

```
000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ········Âÿ···è
000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
00000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
00000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
00000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f·····fh···
00000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh··h··´B···
```

Cursor pos = 0; phy sec = 0



Create Image

Image Source: \\.\PHYSICALDRIVE1

Starting Evidence Number: 0

Image Destination(s)

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created

Select Image Destination

Image Destination Folder: C:\Users\SMILE\OneDrive\Desktop\Mitali

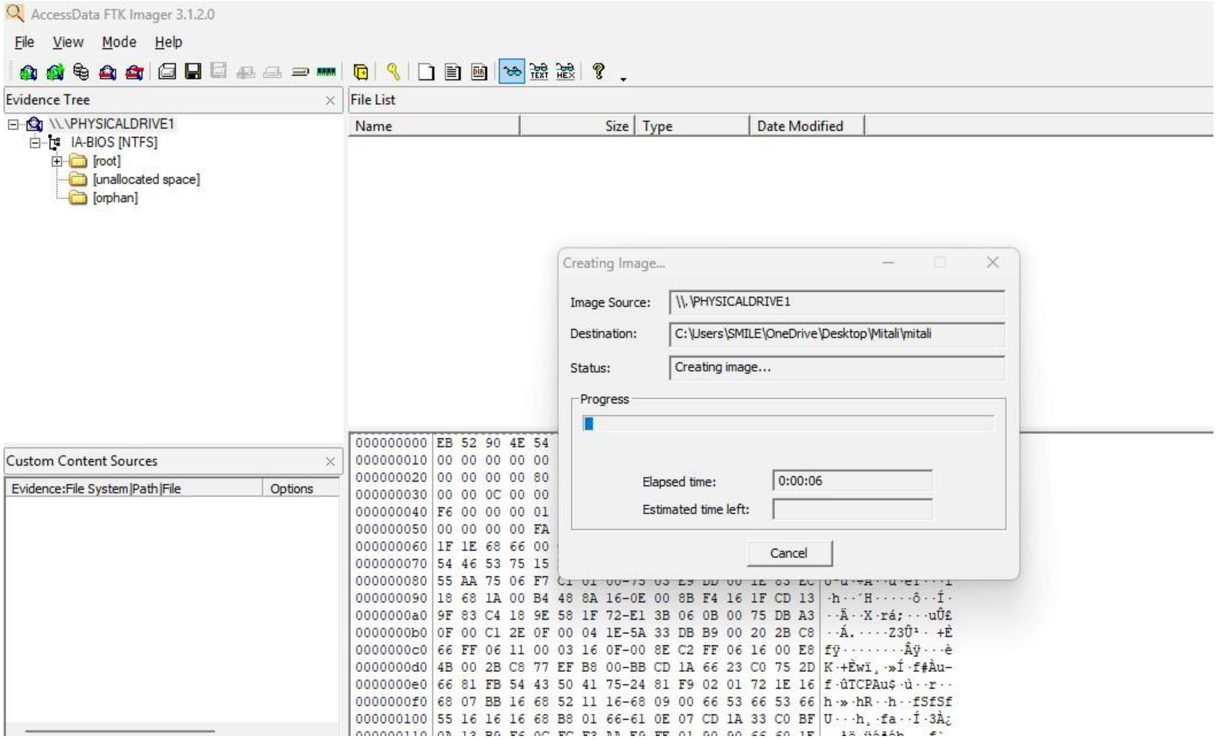
Image Filename (Excluding Extension): srushti

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 100

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

```
                                                        ·h··´H·····ô··Í·
                                                        ··Ä··X·rá;···uÛ£
                                                        ··Á.····Z3Û¹· +È
0000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ········Âÿ···è
0000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
0000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
0000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
000000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
000000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
000000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f·····fh···
000000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh··h··´B···
```



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\SMILE\OneDrive\Desktop\Mitali\mitali

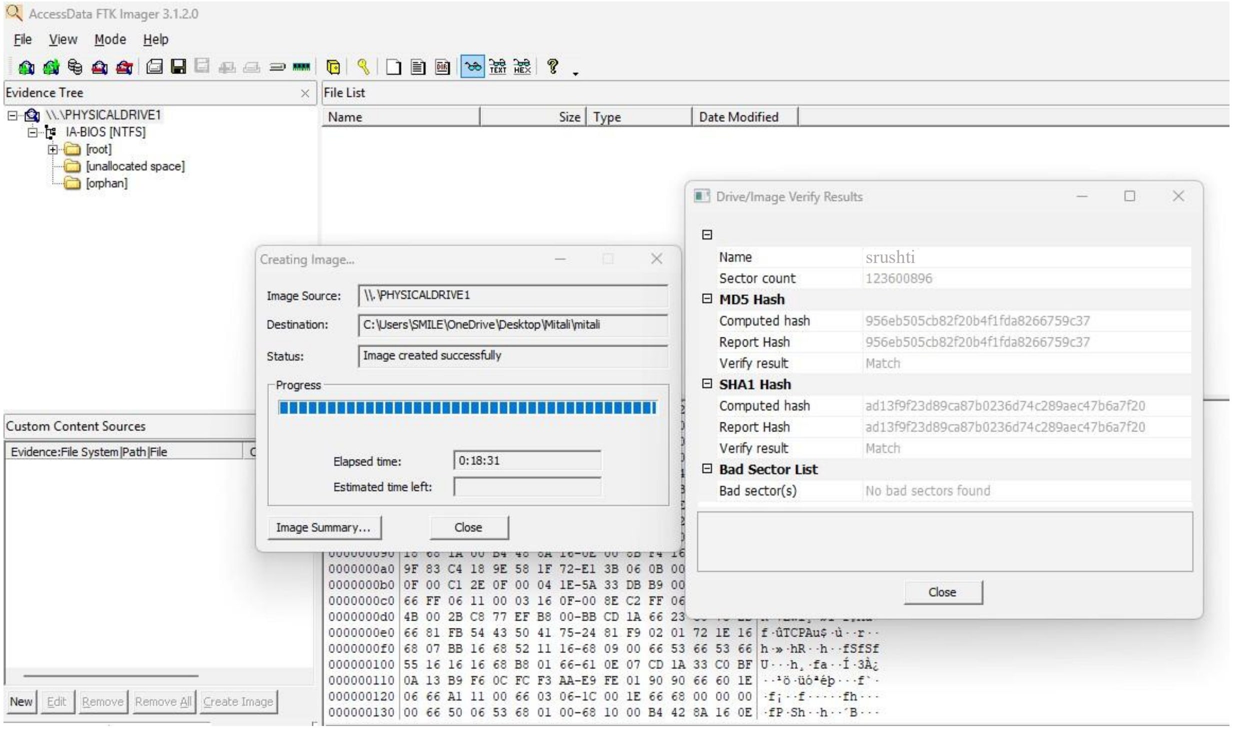
Status: Creating image...

Progress

Elapsed time: 0:00:06

Estimated time left:

```
000000000 EB 52 90 4E 54
000000010 00 00 00 00 00
000000020 00 00 00 00 80
000000030 00 00 0C 00 00
000000040 F6 00 00 00 01
000000050 00 00 00 00 FA
000000060 1F 1E 68 66 00
000000070 54 46 53 75 15
000000080 55 AA 75 06 F7
000000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··´H·····ô··Í·
0000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä··X·rá;···uÛ£
0000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8 ··Á.····Z3Û¹· +È
0000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ········Âÿ···è
0000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
0000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
0000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
000000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
```



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\SMILE\OneDrive\Desktop\Mitali\mitali

Status: Image created successfully

Progress

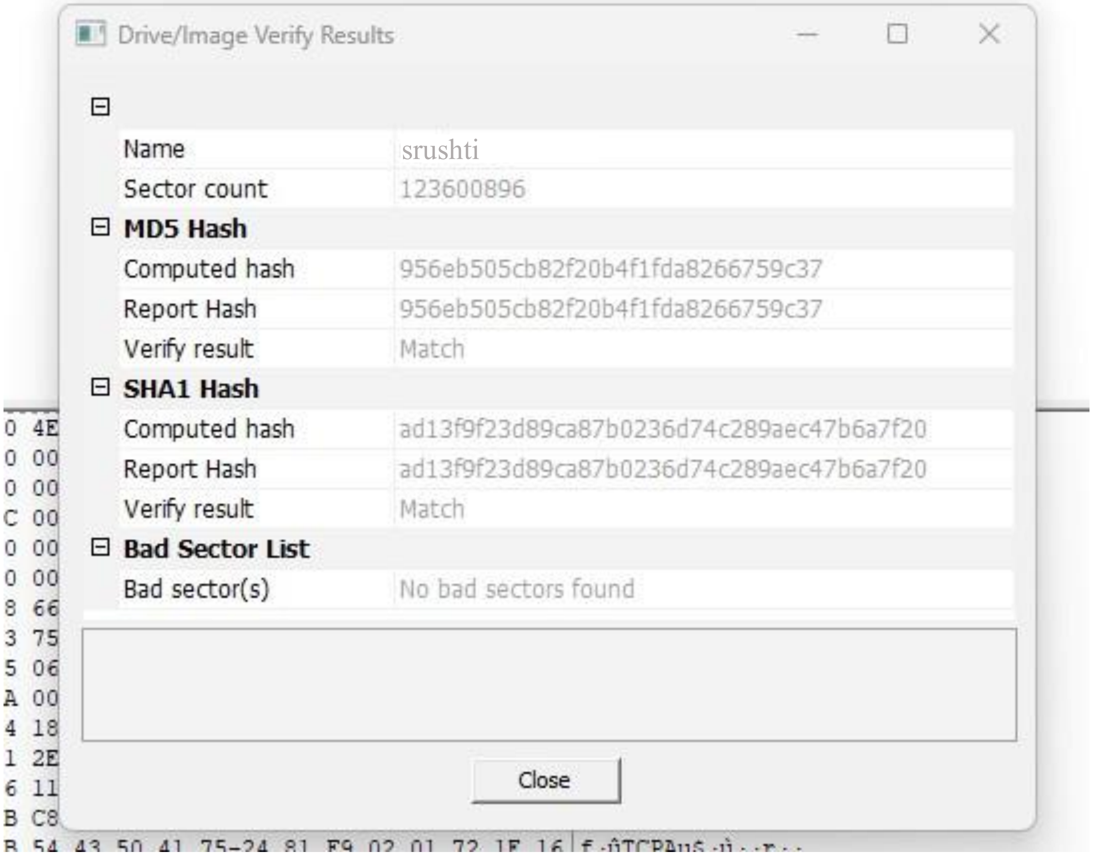
Elapsed time: 0:18:31

Estimated time left:

```
0000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00
0000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00
0000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06
0000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23
0000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
0000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
000000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
000000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
000000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f·····fh···
000000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh··h··´B···
```

Drive/Image Verify Results

Name	srushti
Sector count	123600896
MD5 Hash	
Computed hash	956eb505cb82f20b4f1fda8266759c37
Report Hash	956eb505cb82f20b4f1fda8266759c37
Verify result	Match
SHA1 Hash	
Computed hash	ad13f9f23d89ca87b0236d74c289aec47b6a7f20
Report Hash	ad13f9f23d89ca87b0236d74c289aec47b6a7f20
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found



Drive/Image Verify Results

Name	srushti
Sector count	123600896
MD5 Hash	
Computed hash	956eb505cb82f20b4f1fda8266759c37
Report Hash	956eb505cb82f20b4f1fda8266759c37
Verify result	Match
SHA1 Hash	
Computed hash	ad13f9f23d89ca87b0236d74c289aec47b6a7f20
Report Hash	ad13f9f23d89ca87b0236d74c289aec47b6a7f20
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

6.7 Conclusion:

A bit-by-bit static acquisition of the USB drive was successfully performed using FTK Imager Lite. The integrity of the image was verified through MD5 and SHA1 hash comparison, ensuring the forensic image is an exact replica of the original drive