Title:

Week 1 Digital Forensics Disk Image Task

Name	Saad Naveed
Email	saadnaveed524@gmail.com
Date	3rd July 2025
Position	Digital Forensics Interne
Company	Cyborts

Table of Contents

Objective

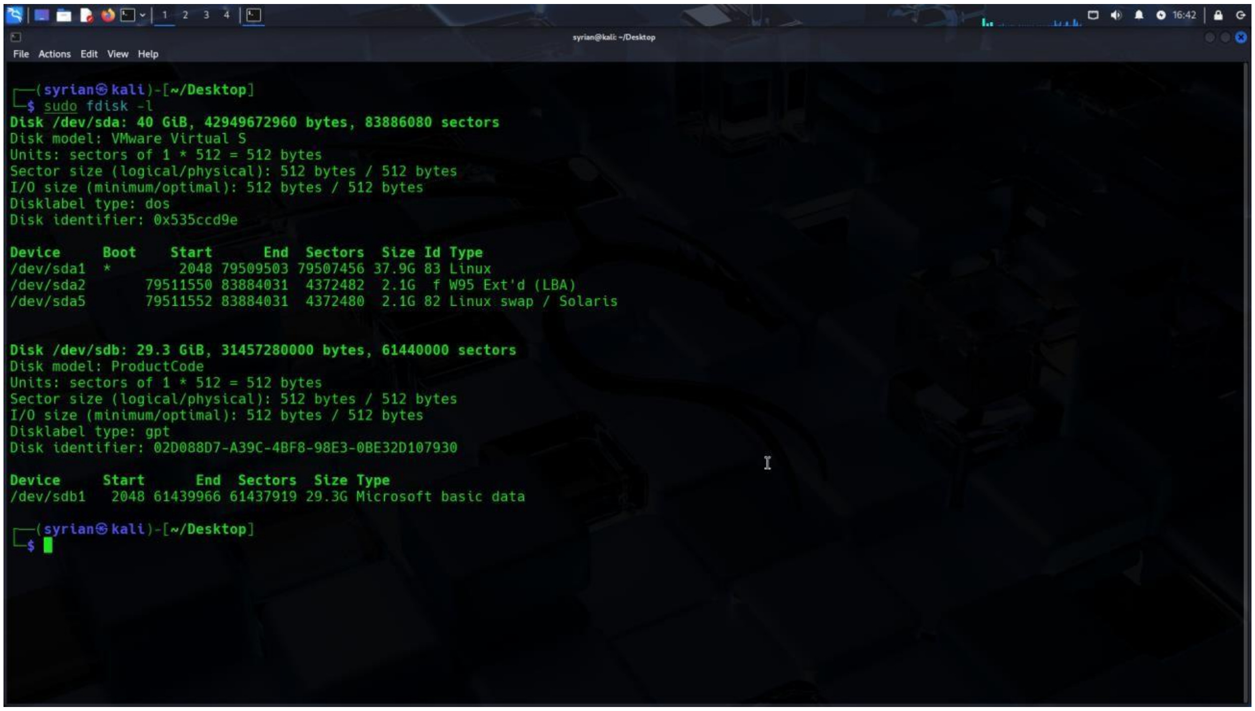
The objective of this task is to perform a complete forensic acquisition of a removable USB storage device in a manner that ensures the integrity and admissibility of the evidence. This involves creating a bit-by-bit image of the USB drive using a reliable forensic tool (FTK Imager), generating cryptographic hash values (MD5 and SHA1/SHA256) before and after the imaging process, and verifying that these hashes match. Matching hashes confirm that the image is an exact copy of the original device and has not been altered during the acquisition process. This task demonstrates the foundational principles of digital evidence handling and chain of custody documentation.

Before the Image

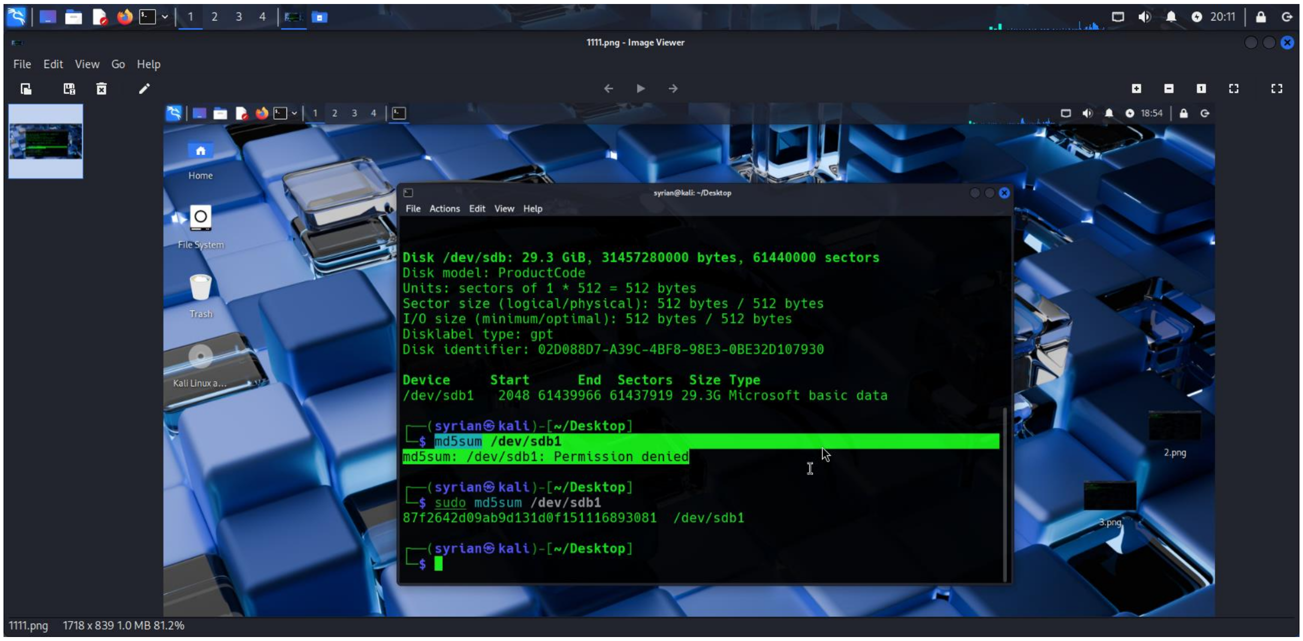
Before creating the image, I generated the hash value using Kali Linux.

Using command:

- sudo fdisk –l
- Select Usb



```
┌──(syrian㉿kali)-[~/Desktop]
└─$ sudo fdisk -l
Disk /dev/sda: 40 GiB, 42949672960 bytes, 83886080 sectors
Disk model: VMware Virtual S
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: 0x535ccd9e

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 79509503 79507456 37.9G 83 Linux
/dev/sda2       79511550 83884031  4372482  2.1G  f W95 Ext'd (LBA)
/dev/sda5       79511552 83884031  4372480  2.1G 82 Linux swap / Solaris


Disk /dev/sdb: 29.3 GiB, 31457280000 bytes, 61440000 sectors
Disk model: ProductCode
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: gpt
Disk identifier: 02D088D7-A39C-4BF8-98E3-0BE32D107930

Device     Start      End  Sectors  Size Type
/dev/sdb1   2048 61439966 61437919 29.3G Microsoft basic data

┌──(syrian㉿kali)-[~/Desktop]
└─$ 
```



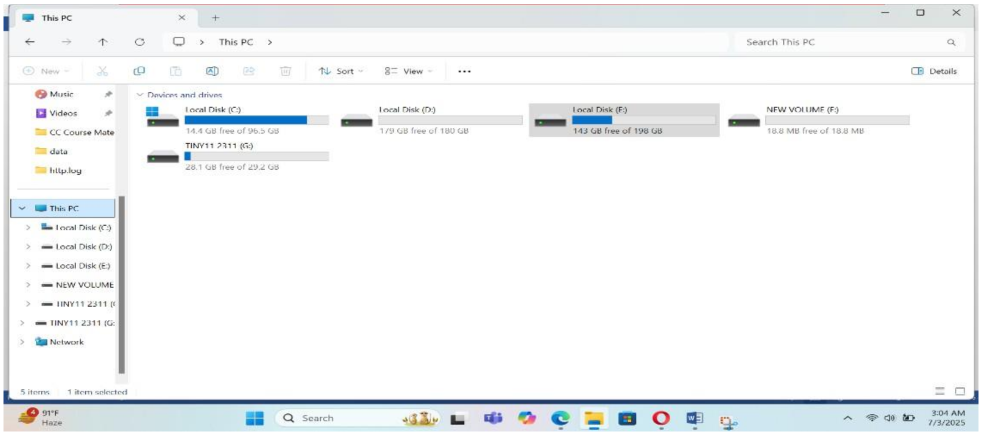
```
Disk /dev/sdb: 29.3 GiB, 31457280000 bytes, 61440000 sectors
Disk model: ProductCode
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 02D088D7-A39C-4BF8-98E3-0BE32D107930

Device      Start      End  Sectors  Size Type
/dev/sdb1    2048 61439966 61437919 29.3G Microsoft basic data

┌──(syrian㉿kali)-[~/Desktop]
└─$ md5sum /dev/sdb1
md5sum: /dev/sdb1: Permission denied

┌──(syrian㉿kali)-[~/Desktop]
└─$ sudo md5sum /dev/sdb1
87f2642d09ab9d131d0f151116893081  /dev/sdb1

┌──(syrian㉿kali)-[~/Desktop]
└─$ 
```

Tools Used

FTK imager

I have already install FTK in my machine.

Now Launch FTK Imager and add USB.



Local Disk (C:)
14.4 GB free of 96.5 GB

Local Disk (D:)
179 GB free of 180 GB

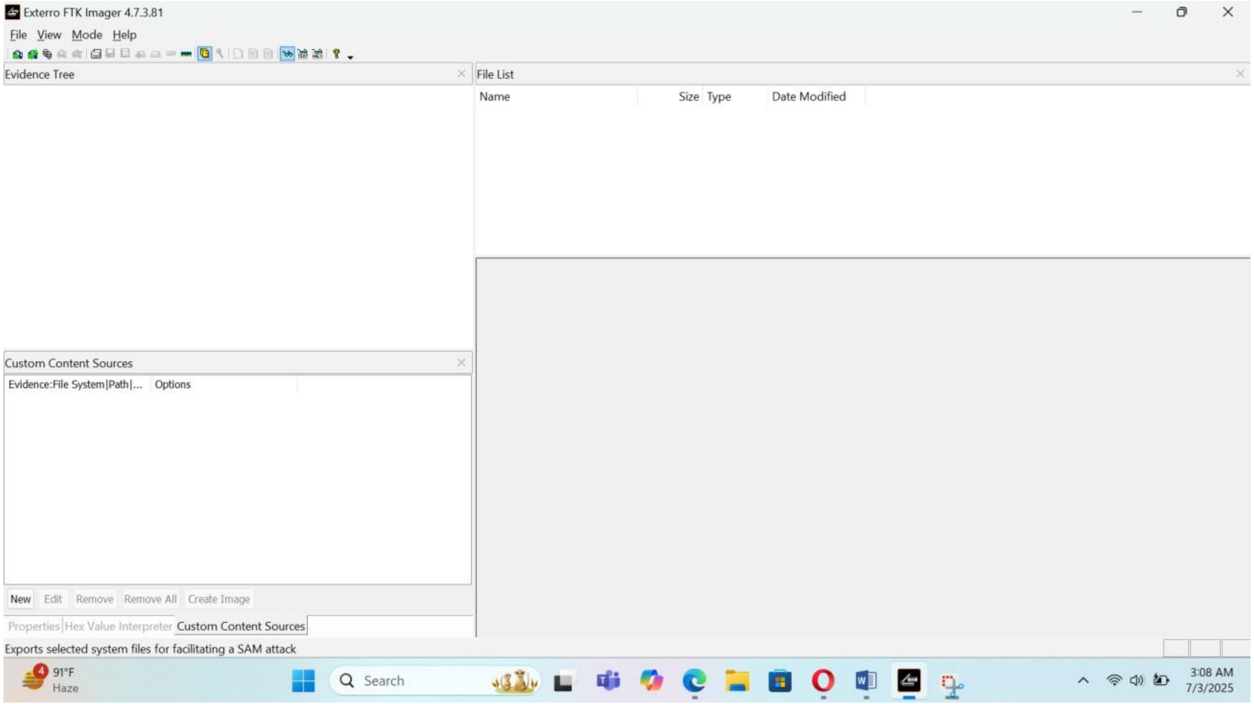
Local Disk (E:)
143 GB free of 198 GB

NEW VOLUME (F:)
18.8 MB free of 18.8 MB

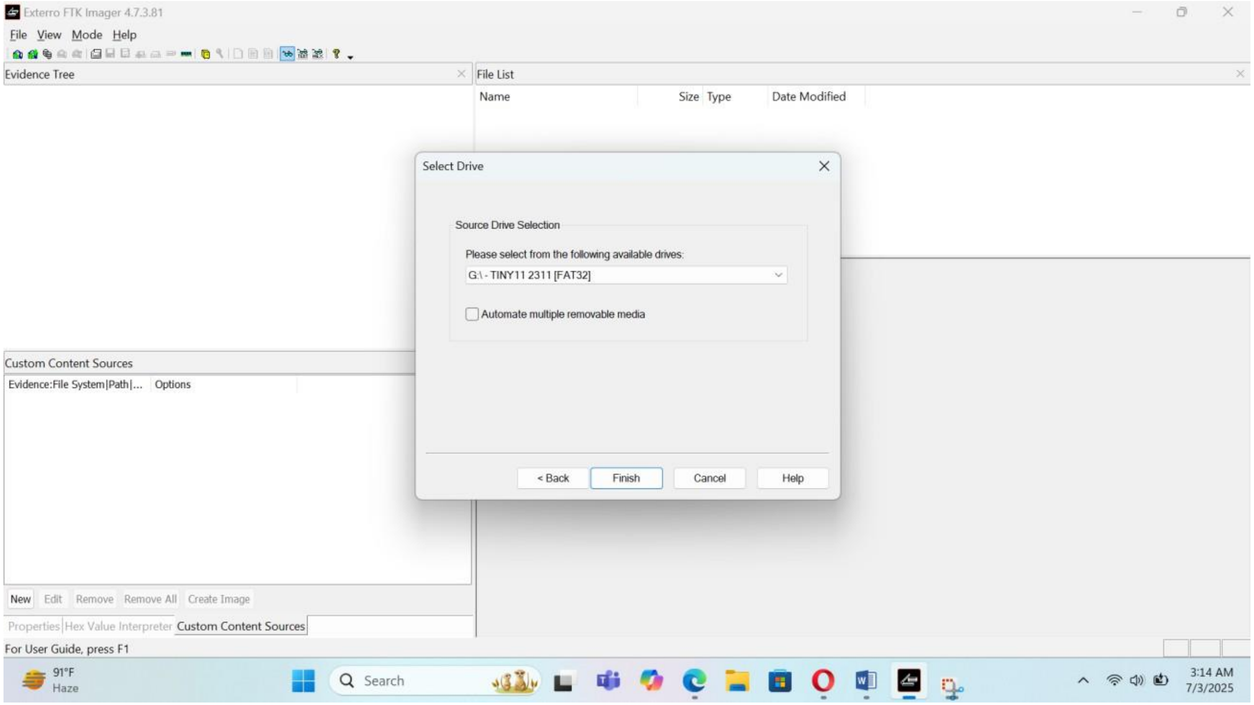
TINY11 2311 (G:)
28.1 GB free of 29.2 GB

In this screenshot showing USB (TINY11 2311(G)) device which I used in this task.

Launch FTK Imager.



- Now click File option.
- Select Create Disk Image.
- Select Logical Drive and then Select USB.
- Then Finish


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|... Options
New Edit Remove Remove All Create Image
Properties Hex Value Interpreter Custom Content Sources
For User Guide, press F1
91°F
Haze
Search
3:14 AM
7/3/2025

Select Drive

Source Drive Selection

Please select from the following available drives:

G:\ - TINY11 2311 [FAT32]

□ Automate multiple removable media

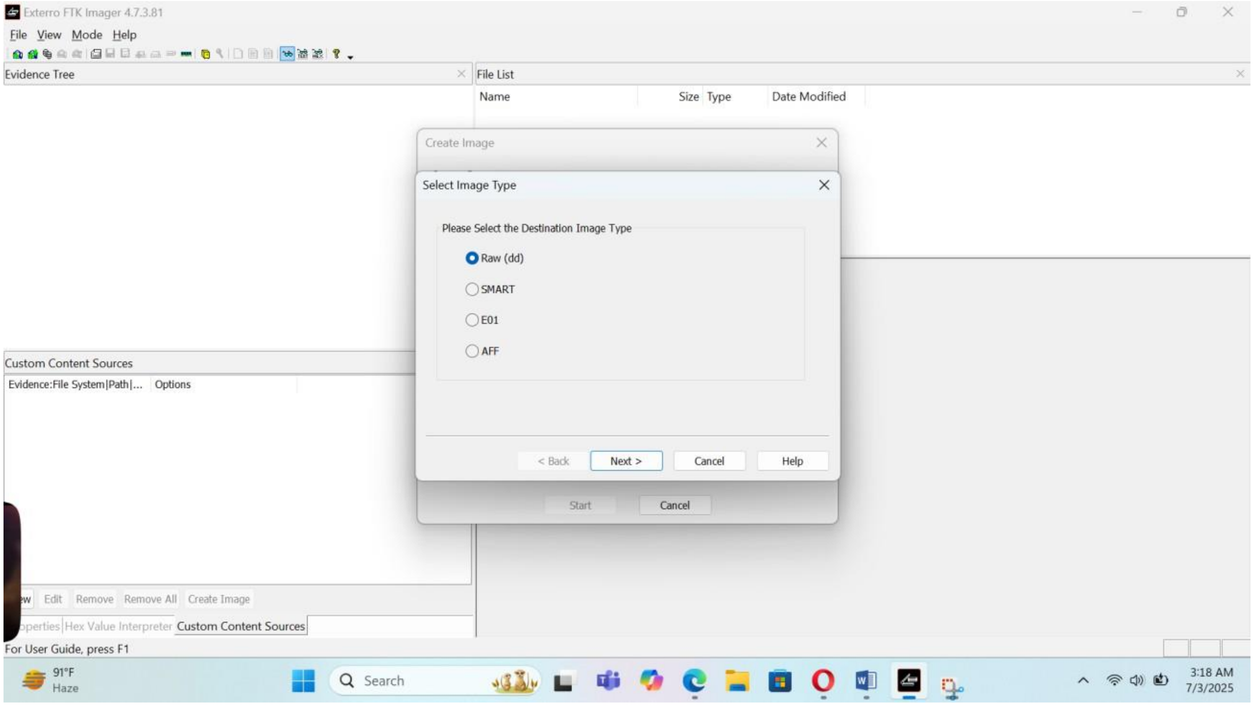
< Back | Finish | Cancel | Help

Image Destination

Click Add...

Choose format: **Raw (dd)** → Click Next.

Enter these details:


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Custom Content Sources
Evidence:File System|Path|... Options
< Back Next > Cancel Help
Start Cancel
Edit Remove Remove All Create Image
Hex Value Interpreter Custom Content Sources
For User Guide, press F1
91°F Haze
Search
3:18 AM 7/3/2025

Select Image Type

Please Select the Destination Image Type

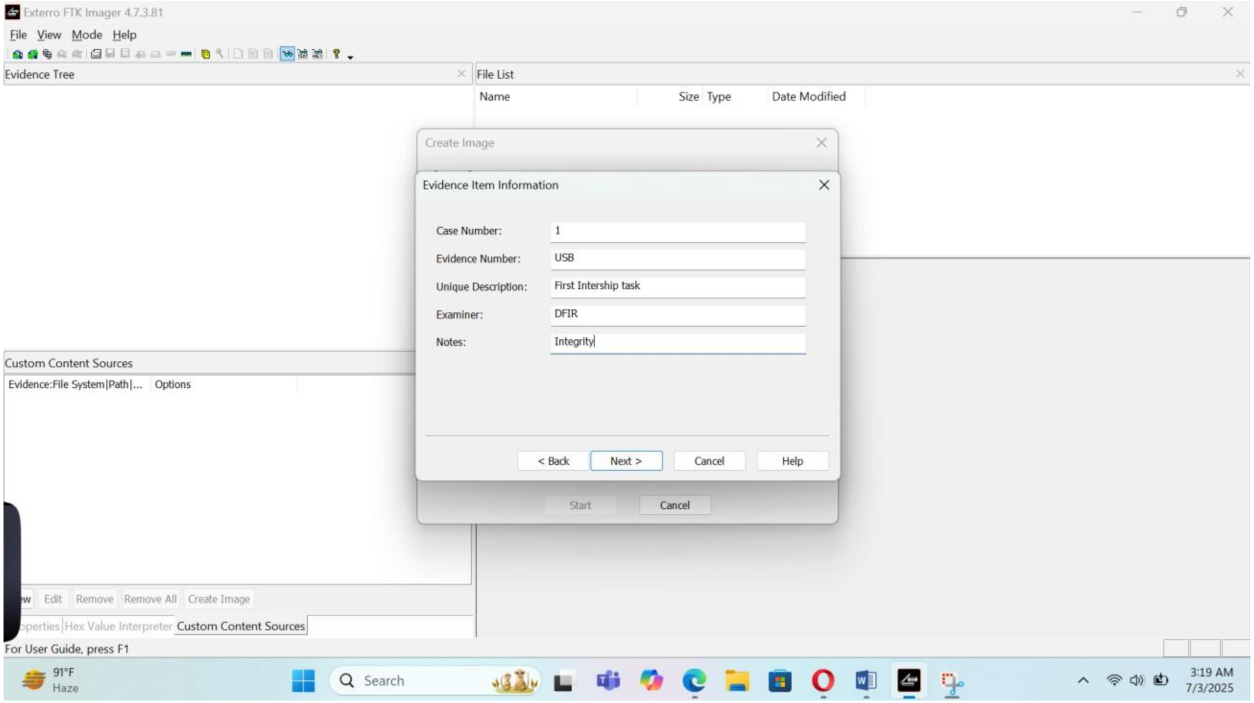
● Raw (dd)

○ SMART

○ E01

○ AFF

Now I add Case Info.


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Custom Content Sources
Evidence:File System|Path|... Options
< Back Next > Cancel Help
Start Cancel
Edit Remove Remove All Create Image
Hex Value Interpreter Custom Content Sources
For User Guide, press F1
91°F Haze
Search
3:19 AM 7/3/2025

Evidence Item Information

Case Number:	1
Evidence Number:	USB
Unique Description:	First Intership task
Examiner:	DFIR
Notes:	Integrity

Now select destination path and file name and then press start.

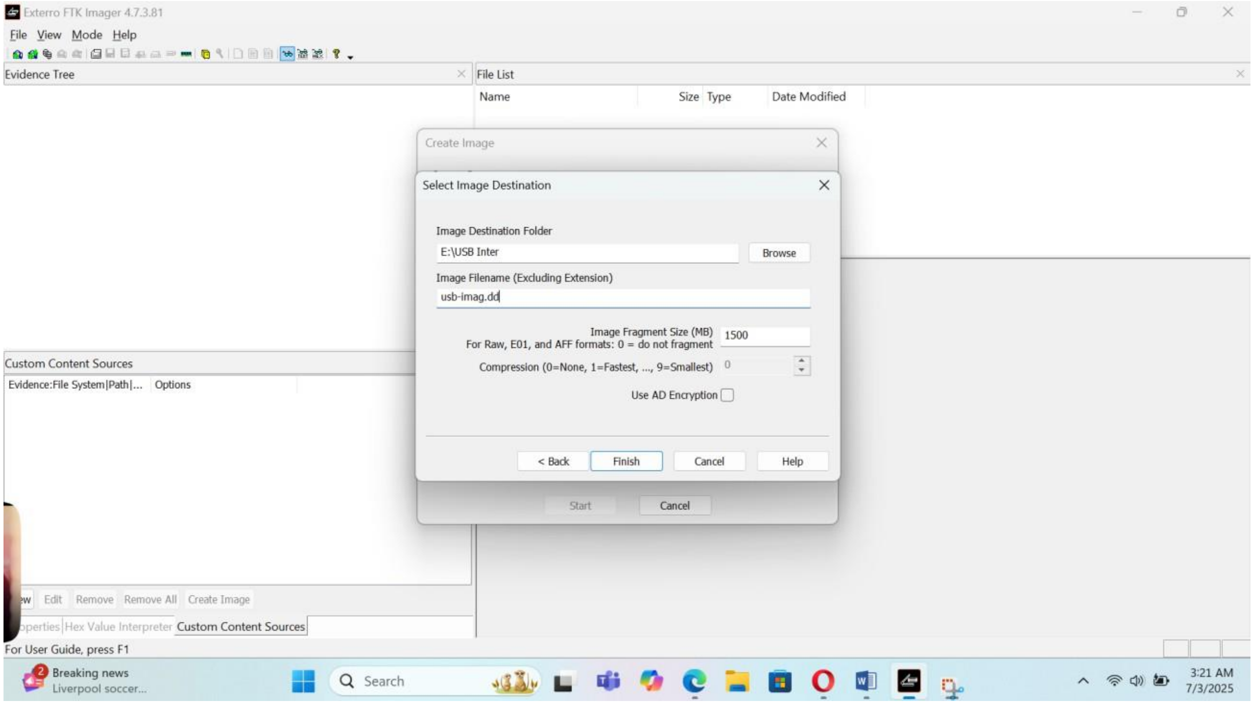


Image Destination Folder: E:\USB Inter

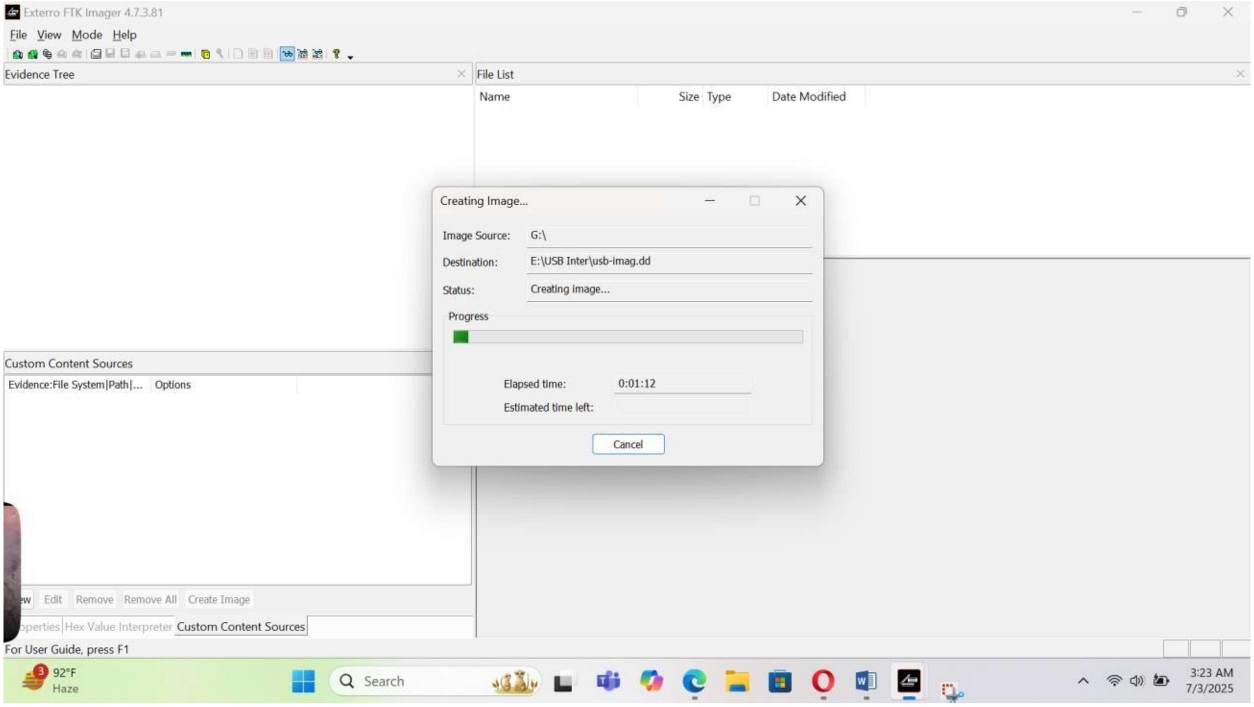
Image Filename (Excluding Extension): usb-imag.dd

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

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

Use AD Encryption ☐

Now creating image start.



Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Creating Image...
Progress
Cancel
Custom Content Sources
Evidence:File System|Path|... Options
Edit Remove Remove All Create Image
Hex Value Interpreter Custom Content Sources
For User Guide, press F1
92°F
Haze
Search
3:23 AM
7/3/2025

Image Source: G:\

Destination: E:\USB Inter\usb-imag.dd

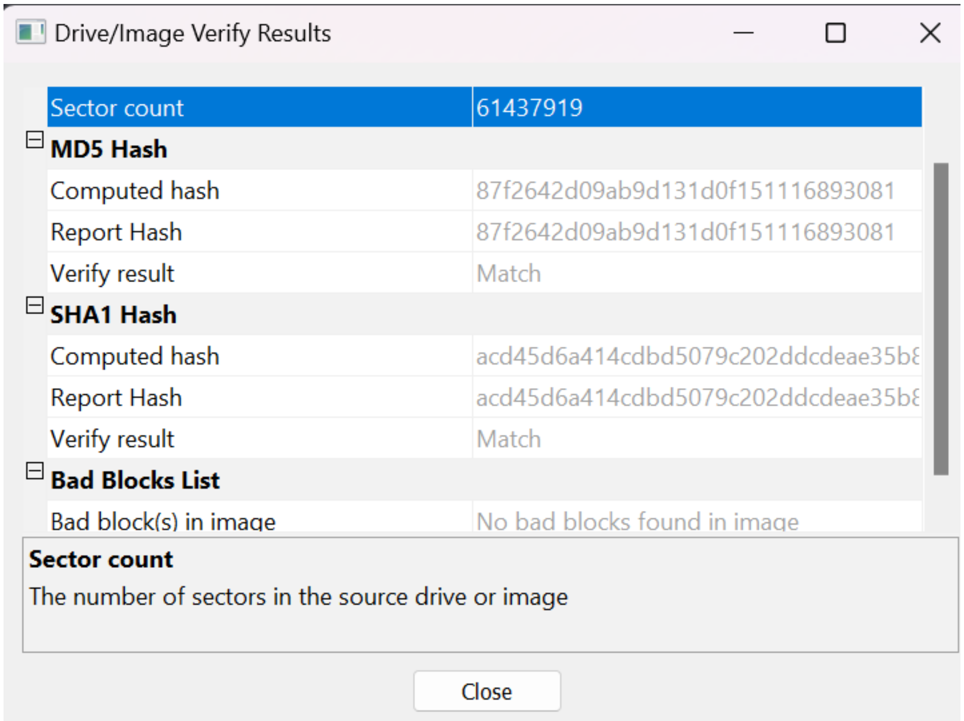
Status: Creating image...

Elapsed time: 0:01:12

Estimated time left:

After the Image.

After some time, the image creation is completed and a hash value is generated.



Drive/Image Verify Results

Sector count	61437919
MD5 Hash	
Computed hash	87f2642d09ab9d131d0f151116893081
Report Hash	87f2642d09ab9d131d0f151116893081
Verify result	Match
SHA1 Hash	
Computed hash	acd45d6a414cdbd5079c202ddcdeae35b8
Report Hash	acd45d6a414cdbd5079c202ddcdeae35b8
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Sector count

The number of sectors in the source drive or image

Conclusion

In this digital forensics task, I was assigned to verify the integrity of a USB drive by calculating its hash value before and after imaging. I successfully calculated both MD5 and SHA256 hashes using standard tools, and the values remained exactly the same before and after creating the forensic image.