BIRZEIT UNIVERSITY

Computer Science Department
Dr. Mohammad Alkhanafseh
DIGITAL FORENSICS ANALYSIS COMP438
Section: 1 S, W.

A Digital Forensics Investigation

using FTK-Imager and Active Disk Editor

This report was written for the Digital Forensics Analysis coursework, specifically the first assignment. In which, steps and screenshots for each investigation process are recorded.

Summary

Throughout this investigation, the process was divided mainly into 4 sections. The first section is where the programs FTK and Active are introduced and the investigation is overviewed. The second section is concerned with building evidence which is A virtual Hard disk drive image and justifying why it was chosen. The third section presents the creation of a Virtual Hardisk Drive, and its partitions (primary and extended), then deleting two of them. The fourth section is about Evidence and file recovery.

Table of contents

Section 1: Introduction

In this section, the programs used in the investigation process are introduced, and the versions used in this investigation. An overview of the investigation process is also discussed.

1.1 Overview of the report

This investigation process involves four sections shown in the contents. Including evidence creation, virtual disk partition, analysis, and conclusions.

1.2 About FTK-imager

"FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Forensic Toolkit (FTK®) is warranted. Create forensic images of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media" (Exterro)

Figure (1): FTK logo

The version used: 4.7.1.2

1.3 About Active Disk Editor

"Active@ Disk Editor uses a simple, low-level disk viewer which displays information in binary and text modes at the same time. You can use this view to analyze the contents of data storage structure elements such as Hard disk drives, SSD & USB Disks, Partitions & Volumes, Files, and other projects." (Active @ Disk editor)

The version used: 23.0.1

Figure (2): Active @ Disk Editor

Section 2: Building evidence

In this section, the creation of the image evidence is presented in detail. This represents the first requirement of the assignment.

2.1 Storage space specification

For storage space used to build an image in this investigation, the Virtual Hard disk drive created in section 2 is specified.

2.2 Storage space justification

The Virtual Hard disk drive is specified as storage space for this investigation because the scope of the process is expected to deal with a virtual hard disk drive after reading the requirements. So the justification is the relevancy.

2.3 Image building

For building an image of the hard disk drive, the FTK imager is used. After opening the FTK imager, the file and Add Evidence item are clicked as shown below in Figure (3).

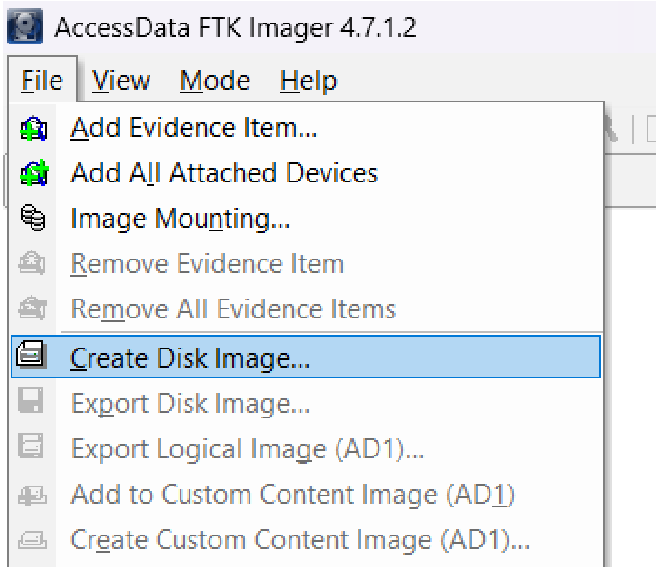
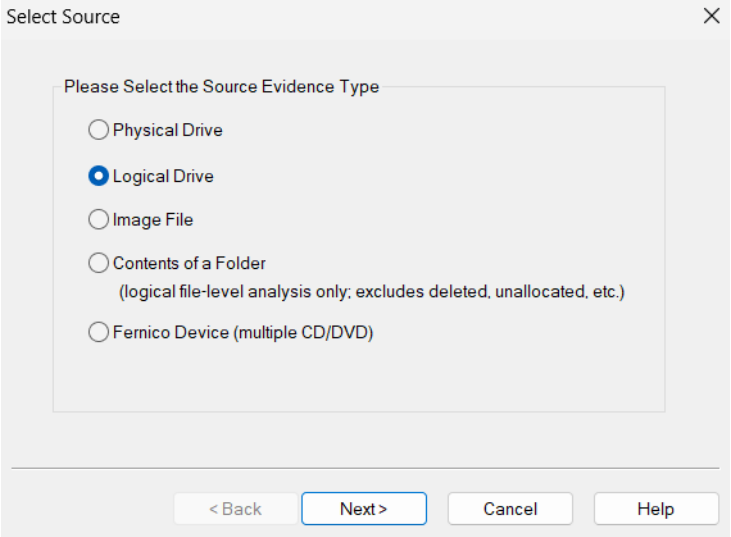

AccessData FTK Imager 4.7.1.2
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...

Figure (3): Create Disk Image

The Virtual Disk drive (logical drive) is selected as the source of the evidence as mentioned earlier. This step is shown in Figure (4).



Select Source

Please Select the Source Evidence Type

○ Physical Drive

● Logical Drive

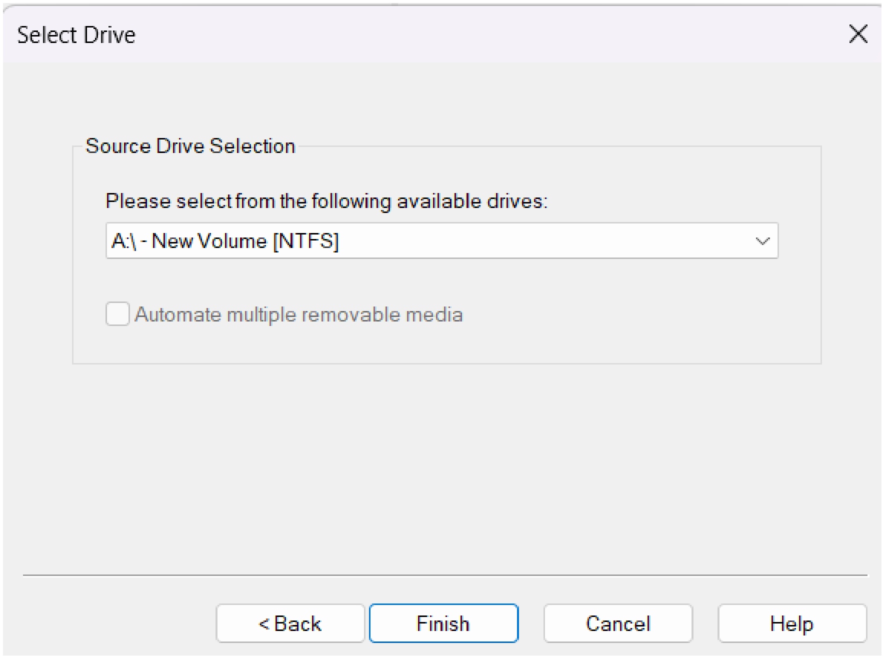
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

Figure (4): source selection

Clicking next shows a dialog that asks for the source drive, Virtual Hardisk Drive created in the next section is specified, below in Figure (5)



Select Drive

Source Drive Selection

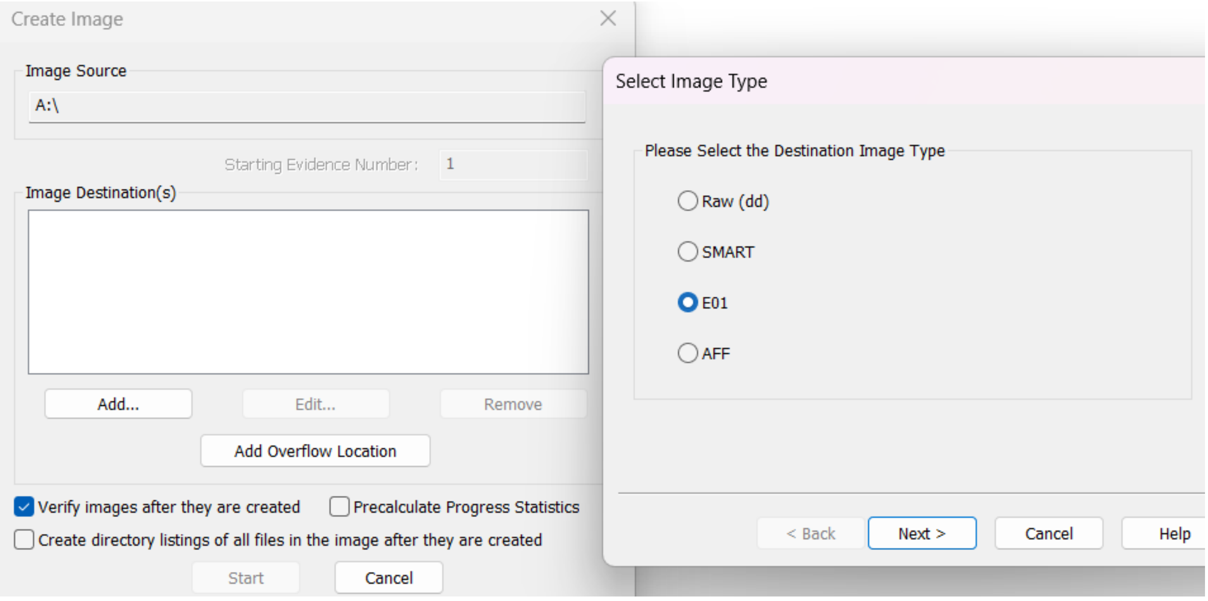
Please select from the following available drives:

A:\ - New Volume [NTFS]

□ Automate multiple removable media

Figure (5): Hard disk drive image FTK dashboard

In Figure (6), an image destination is added, but first, the image type E01 is selected for the reason of saving the image segmented and compressed:



Create Image

Image Source: A:\

Starting Evidence Number: 1

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

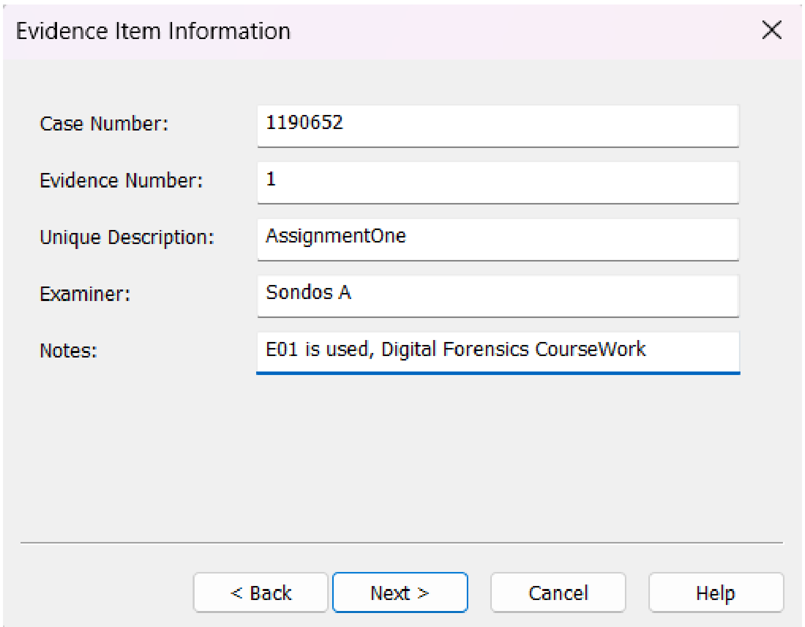
Select Image Type

Please Select the Destination Image Type

○ Raw (dd)
○ SMART
● E01
○ AFF

Figure (6): Select image type

For documentation purposes, the evidence item information is added as shown in Figure (7) below:

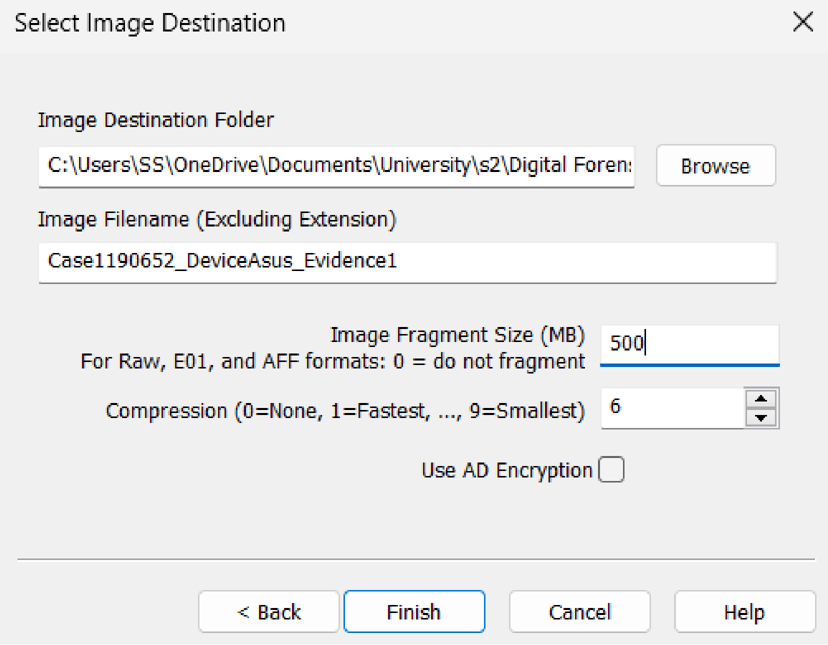


Evidence Item Information

Case Number:	1190652
Evidence Number:	1
Unique Description:	AssignmentOne
Examiner:	Sondos A
Notes:	E01 is used, Digital Forensics CourseWork

Figure (7): Add evidence item information

The Image destination is chosen to be the Case Folder, naming it with the case number and device name, and the date acquired, as shown in Figure(9):



Select Image Destination

Image Destination Folder

C:\Users\SS\OneDrive\Documents\University\s2\Digital Foren:

Image Filename (Excluding Extension)

Case1190652_DeviceAsus_Evidence1

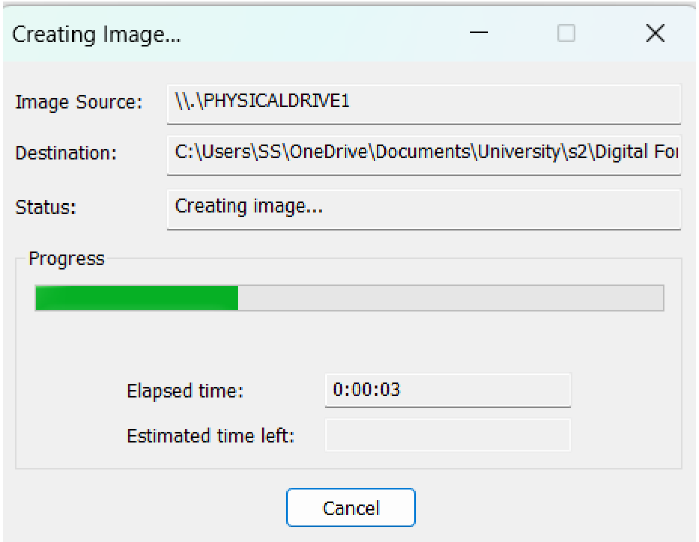
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption □

Figure (8): Image destination

In Figure (9), the creation process of the image in the early specified goal is in progress:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\SS\OneDrive\Documents\University\s2\Digital Fo

Status: Creating image...

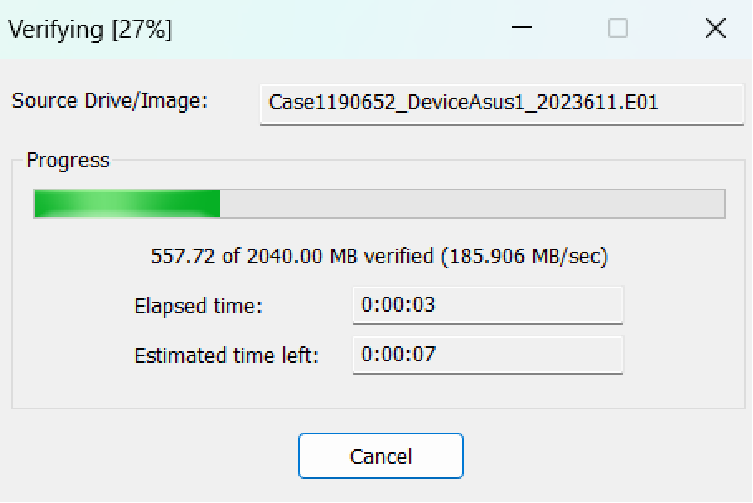
Progress

Elapsed time: 0:00:03

Estimated time left:

Figure (9): Creating Image, elapsed time

Figure (10), shows the progress of the verification process below:



Verifying [27%]

Source Drive/Image: Case1190652_DeviceAsus1_2023611.E01

Progress

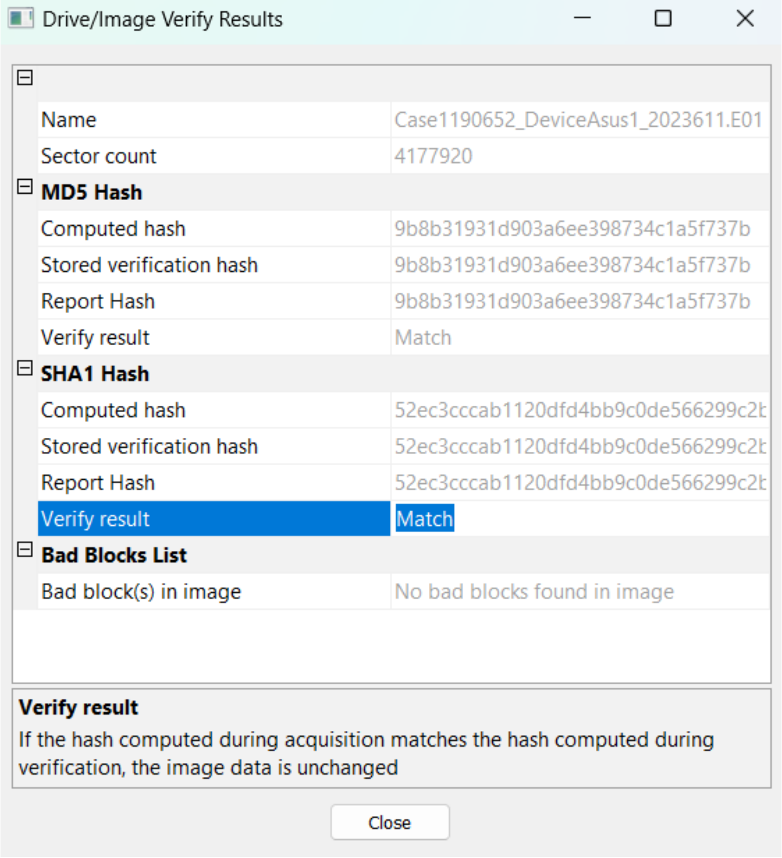
557.72 of 2040.00 MB verified (185.906 MB/sec)

Elapsed time: 0:00:03

Estimated time left: 0:00:07

Figure(10): verification process

The verification results of the virtual disk image are shown In Figure (11). Where the verify results are Match:



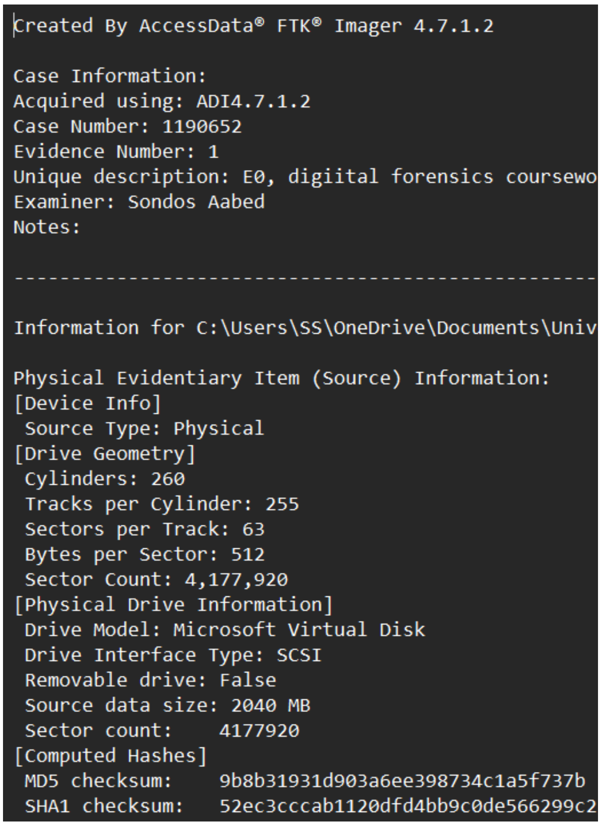
Drive/Image Verify Results

Name	Case1190652_DeviceAsus1_2023611.E01
Sector count	4177920
MD5 Hash	
Computed hash	9b8b31931d903a6ee398734c1a5f737b
Stored verification hash	9b8b31931d903a6ee398734c1a5f737b
Report Hash	9b8b31931d903a6ee398734c1a5f737b
Verify result	Match
SHA1 Hash	
Computed hash	52ec3cccab1120dfd4bb9c0de566299c2b
Stored verification hash	52ec3cccab1120dfd4bb9c0de566299c2b
Report Hash	52ec3cccab1120dfd4bb9c0de566299c2b
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Verify result
If the hash computed during acquisition matches the hash computed during verification, the image data is unchanged

Figure(11): Image verify results

Following in Figure (12) are the created image and the about image summary text file of the investigated virtual disk drive saved in the case folder:



```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 1190652
Evidence Number: 1
Unique description: E0, digiital forensics coursewo
Examiner: Sondos Aabed
Notes:

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

Information for C:\Users\SS\OneDrive\Documents\Univ

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 260
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 4,177,920
[Physical Drive Information]
 Drive Model: Microsoft Virtual Disk
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 2040 MB
 Sector count:    4177920
[Computed Hashes]
 MD5 checksum:    9b8b31931d903a6ee398734c1a5f737b
 SHA1 checksum:   52ec3cccab1120dfd4bb9c0de566299c2
```

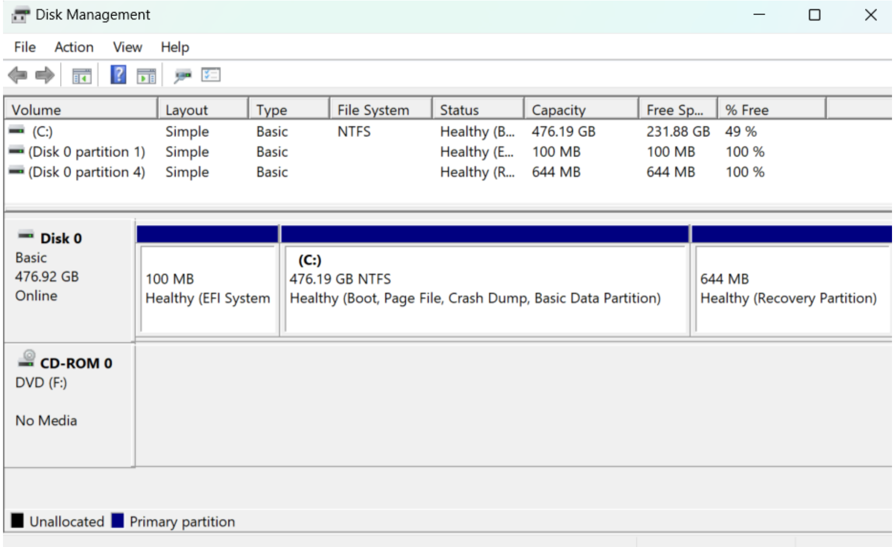
Figure (12): The created image of the virtual disk drive

Section 3: Virtual partition

In this section, the creation, and each partition properties are discussed in detail. Some partitions are deleted and detected afterward. This is the second set of requirements in the Assignment.

3.1 Partitions Creation

To build the virtual hard disk drive, the Disk manager in Windows 11 is opened, as shown in Figure (13):



Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	476.19 GB	231.88 GB	49 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	644 MB	644 MB	100 %

Disk 0
Basic
476.92 GB
Online

100 MB
Healthy (EFI System

(C:)
476.19 GB NTFS
Healthy (Boot, Page File, Crash Dump, Basic Data Partition)

644 MB
Healthy (Recovery Partition)

CD-ROM 0
DVD (F:)

No Media

■ Unallocated ■ Primary partition

Figure (13): Active @ Disk Editor dashboard

In this step, the virtual hard disk drive (VHDD) is built by clicking on create VHD as shown below:

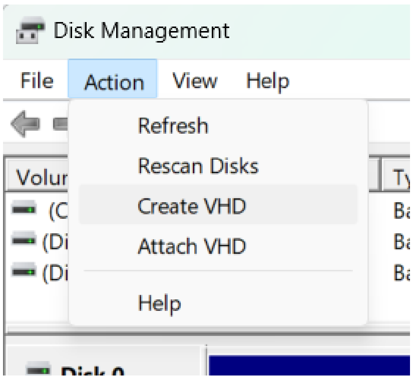
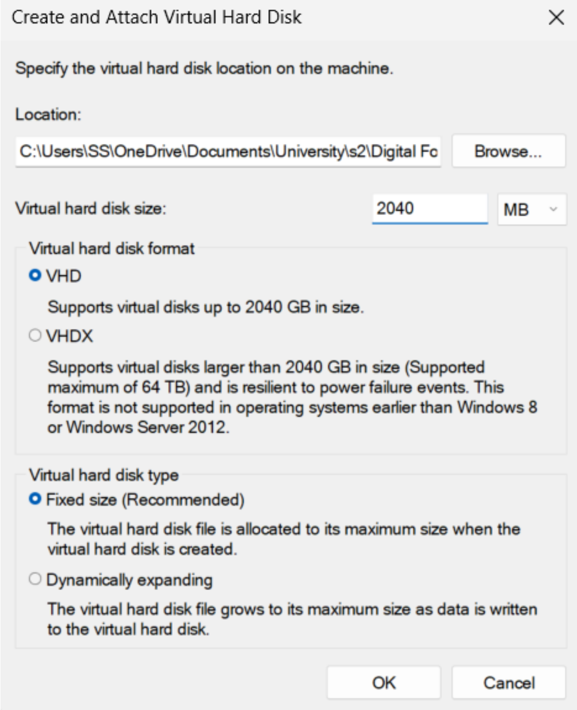


Figure (14): Specify the Physical Drive

In the next step, the Virtual Hard Disk drive is created and attached:



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location: C:\Users\SS\OneDrive\Documents\University\s2\Digital Fo

Virtual hard disk size: 2040 MB

Virtual hard disk format

● VHD

Supports virtual disks up to 2040 GB in size.

○ VHDX

Supports virtual disks larger than 2040 GB in size (Supported maximum of 64 TB) and is resilient to power failure events. This format is not supported in operating systems earlier than Windows 8 or Windows Server 2012.

Virtual hard disk type

● Fixed size (Recommended)

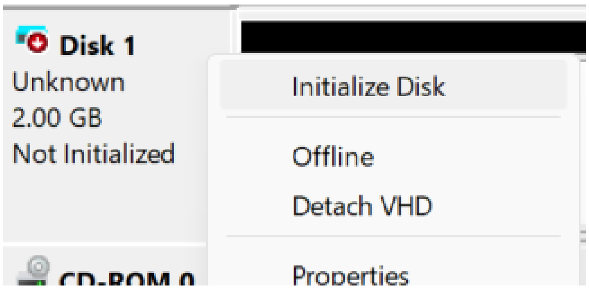
The virtual hard disk file is allocated to its maximum size when the virtual hard disk is created.

○ Dynamically expanding

The virtual hard disk file grows to its maximum size as data is written to the virtual hard disk.

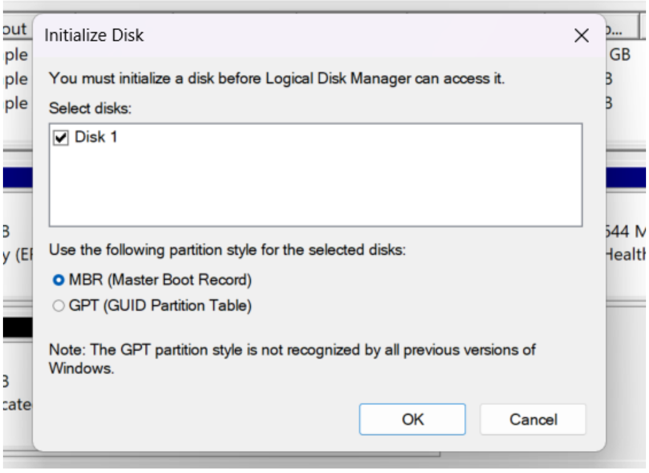
Figure (15): Create and attach virtual hard disk drive

This disk needs to be initialized. The initialization process is shown in both Figure (16) and Figure (17):



Disk 1
Unknown
2.00 GB
Not Initialized

Figure (16): initialize disk



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

Use the following partition style for the selected disks:

● MBR (Master Boot Record)

○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

Figure (17): chose for partition style

Now that the VHDD is created, it is divided into 8 different partitions. The First three partitions are the main partition, and the next 5 are extended partitions of the 4th partition:

The names of each partition are the following:

- **Main partitions**: A, B, E
- **Extended partitions of E**

Shows Figure(18) A new simple volume is created.

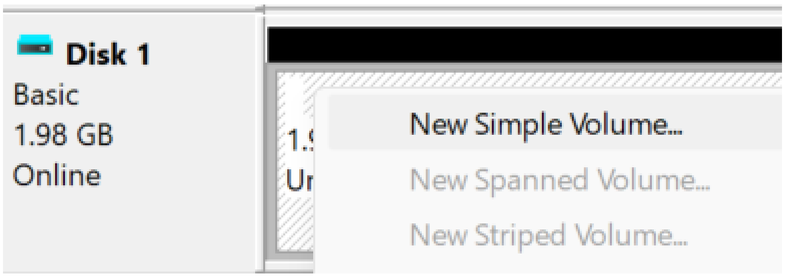
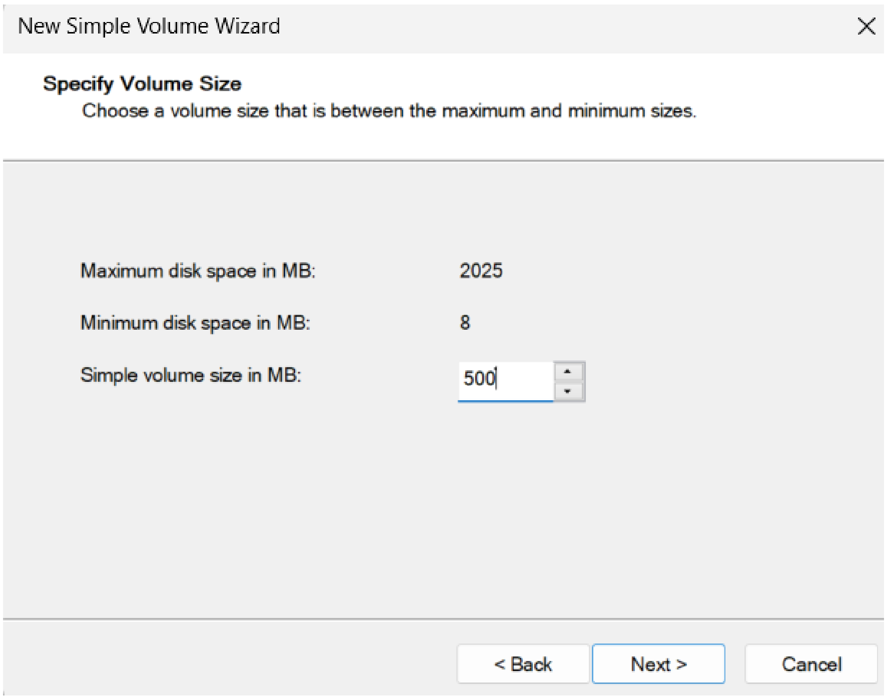


Figure (18): New Simple Volume

Then the volume size is specified as 500 MB shown in Figure (19):

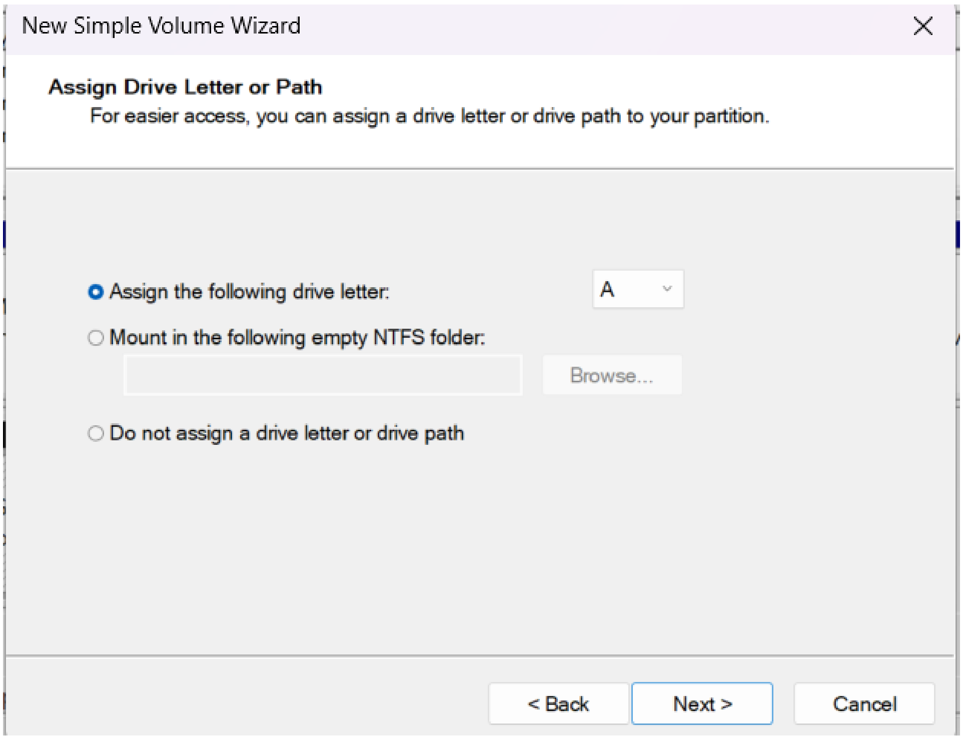

New Simple Volume Wizard

Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 2025
Minimum disk space in MB: 8
Simple volume size in MB: 500

Figure (19): Specify Volume Size

Now the path and the Drive letter are assigned Figure (20) and then it is Formated to NFT file system Figure (21):



Assign Drive Letter or Path

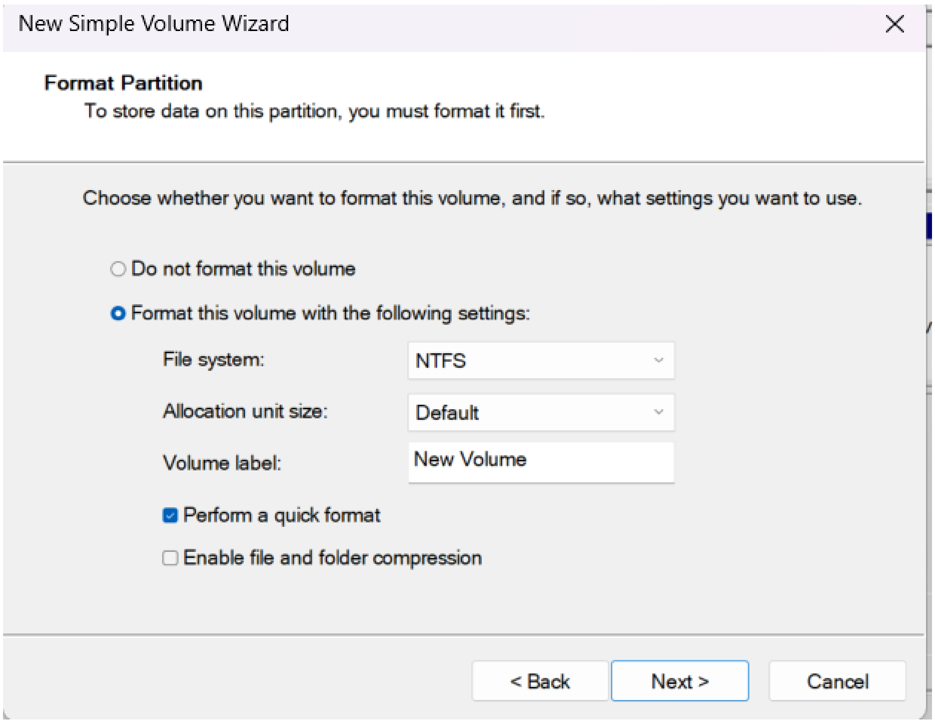
For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: A

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

Figure (20): Assign Drive Letter



Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

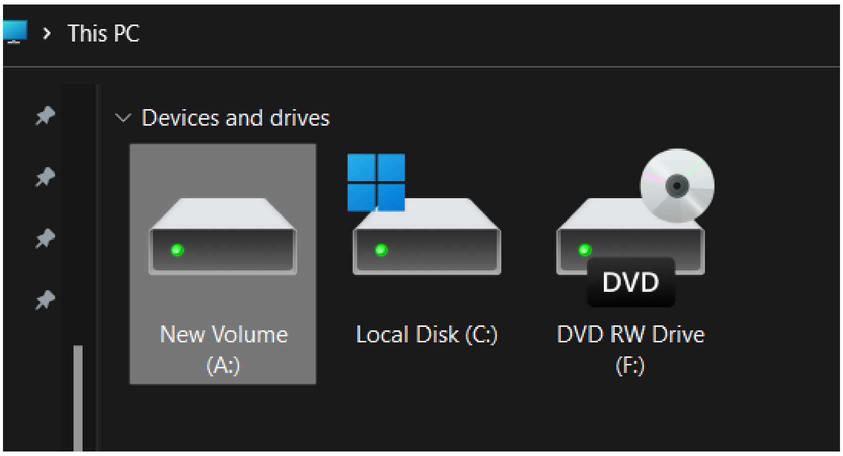
Volume label: New Volume

☑ Perform a quick format

□ Enable file and folder compression

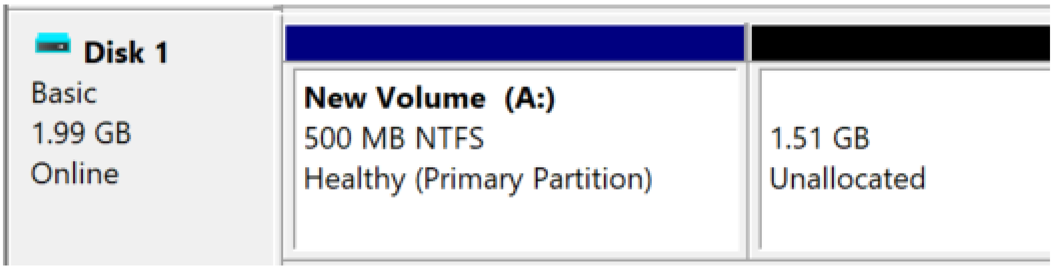
Figure (21): Format Partition

The following figure shows the final step which is finishing the new simple volume wizard after clicking the Finish button. After that, if the PC is checked out, the New volume is found as shown in Figure (22):



Figure(22): the new partition

Figure (23) shows the partition in disk management after the partition is done:



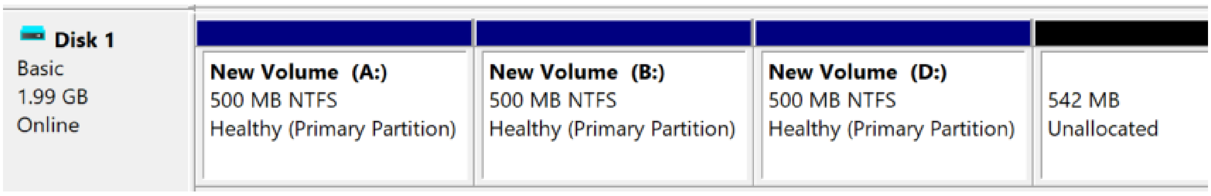
Disk 1
Basic
1.99 GB
Online

New Volume (A:)
500 MB NTFS
Healthy (Primary Partition)

1.51 GB
Unallocated

Figure(23): Disk management new partition

Selecting again new Simple volume on the unallocated space will create another main partition as shown in Figure (24):



Disk 1
Basic
1.99 GB
Online

New Volume (A:)
500 MB NTFS
Healthy (Primary Partition)

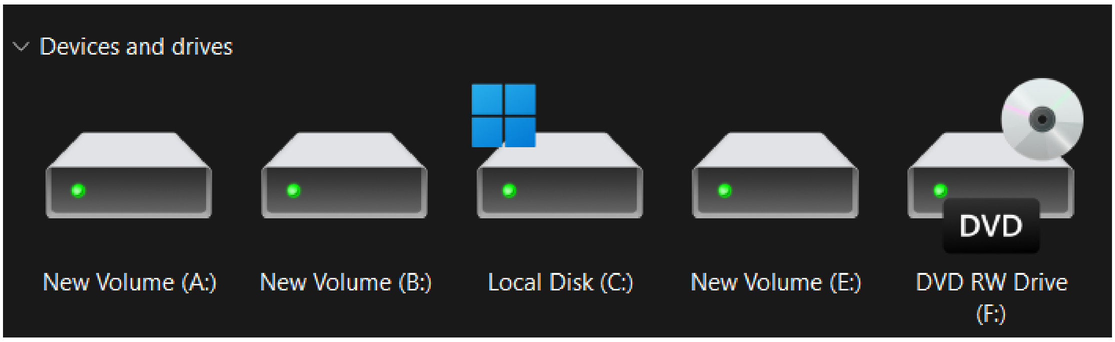
New Volume (B:)
500 MB NTFS
Healthy (Primary Partition)

New Volume (D:)
500 MB NTFS
Healthy (Primary Partition)

542 MB
Unallocated

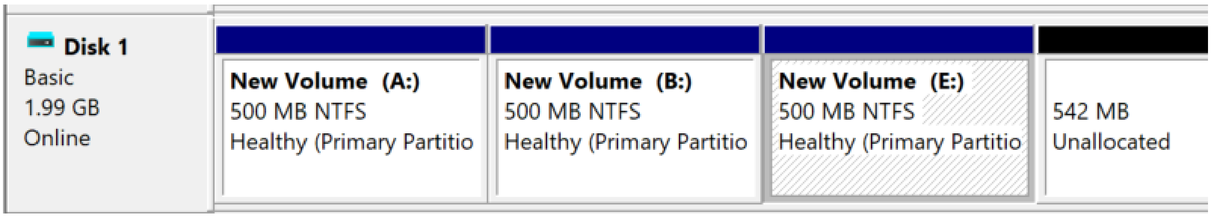
Figure(24): New Volume

Now repeating that until the result gives 3 main partitions: A, B, and E as shown in Figure (25):



Figure(25): PC after partition

Figure (26) shows the Disk in disk management after the three main partitions are done:

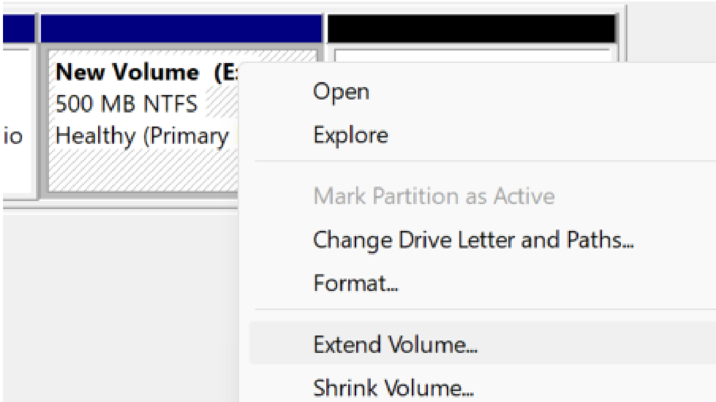


Disk 1
Basic
1.99 GB
Online

New Volume (A:)	New Volume (B:)	New Volume (E:)	
500 MB NTFS	500 MB NTFS	500 MB NTFS	542 MB
Healthy (Primary Partitio	Healthy (Primary Partitio	Healthy (Primary Partitio	Unallocated

Figure(26): disk manager after partition

The following steps will result in 5 extended partitions. The new volume E is extended using Extend Volume as shown in Figure (27):

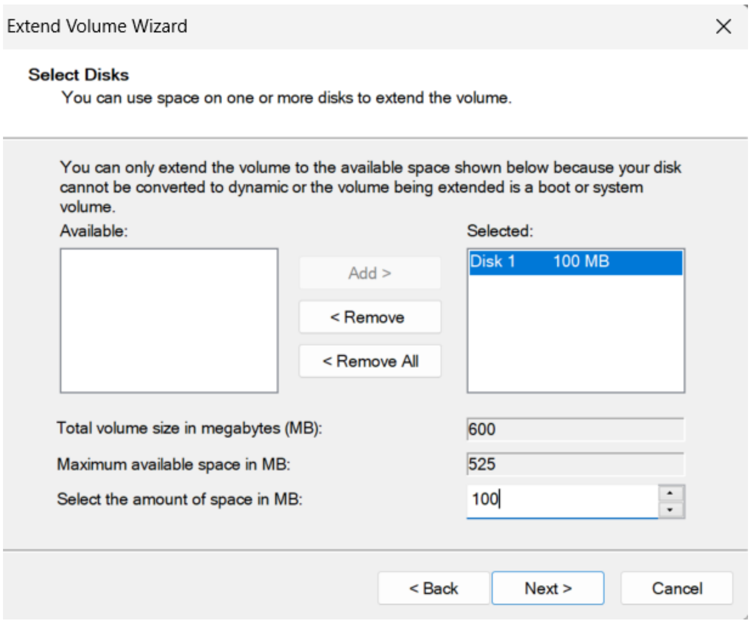


io

New Volume (E:
500 MB NTFS
Healthy (Primary

Figure(27): Extended Volume

The below Figure(28), shows selecting the space that will be used to extend the Volume space:



Extend Volume Wizard

Select Disks
You can use space on one or more disks to extend the volume.

You can only extend the volume to the available space shown below because your disk cannot be converted to dynamic or the volume being extended is a boot or system volume.

Available:

Selected:
Disk 1 100 MB

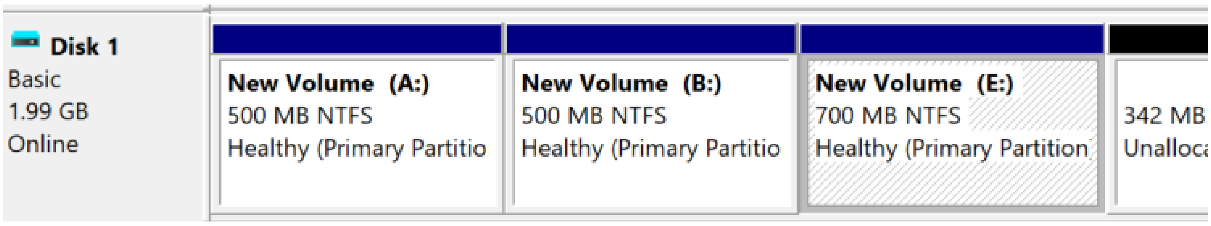
Total volume size in megabytes (MB): 600

Maximum available space in MB: 525

Select the amount of space in MB: 100

Figure(28): Select Disks

After applying that, notice the size of the new Volume E: is now extended to 700 MB in Figure (29):

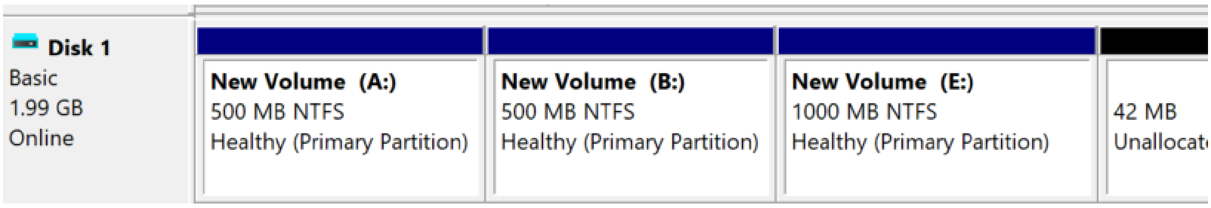


Disk 1
Basic
1.99 GB
Online

New Volume (A:)	New Volume (B:)	New Volume (E:)	
500 MB NTFS	500 MB NTFS	700 MB NTFS	342 MB
Healthy (Primary Partitio	Healthy (Primary Partitio	Healthy (Primary Partition	Unalloca

Figure(29): Extended size

Repeating that five times will result in the following partitions shown in Figure (30):



Disk 1
Basic
1.99 GB
Online

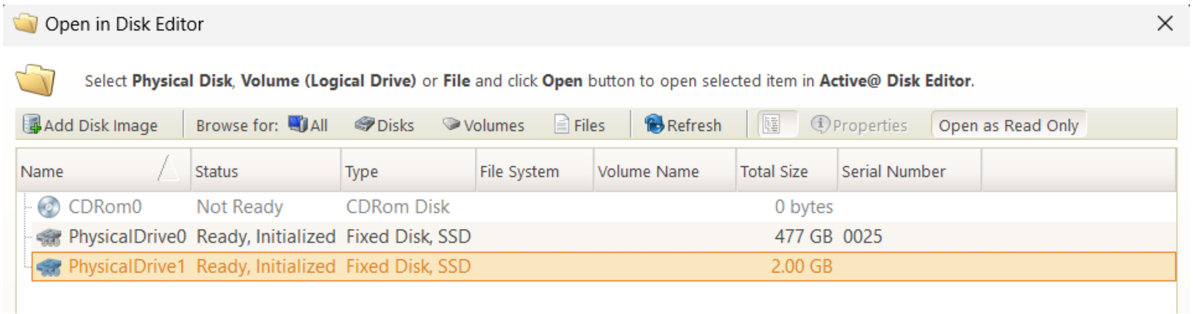
New Volume (A:)	New Volume (B:)	New Volume (E:)	
500 MB NTFS	500 MB NTFS	1000 MB NTFS	42 MB
Healthy (Primary Partition)	Healthy (Primary Partition)	Healthy (Primary Partition)	Unallocat

Figure(30): Final extended size

3.2 About the partitions

In this section following information about the VHDD is presented. This is done using Active @ Disk Editor.

After launching the application, the open disk drive is selected and the previously created disk is opened as shown in Figure(31):


Open in Disk Editor
Select Physical Disk, Volume (Logical Drive) or File and click Open button to open selected item in Active@ Disk Editor.
Add Disk Image
Browse for:
All
Disks
Volumes
Files
Refresh
Properties
Open as Read Only

Name	Status	Type	File System	Volume Name	Total Size	Serial Number
CDRom0	Not Ready	CDRom Disk			0 bytes	
PhysicalDrive0	Ready, Initialized	Fixed Disk, SSD			477 GB	0025
PhysicalDrive1	Ready, Initialized	Fixed Disk, SSD			2.00 GB	

Figure(31): opening disk editor

As shown in the next page Figure (32), each partition’s file system is highlighted by the color green. Size is by color brown, and Starting in LBA with the color grey.

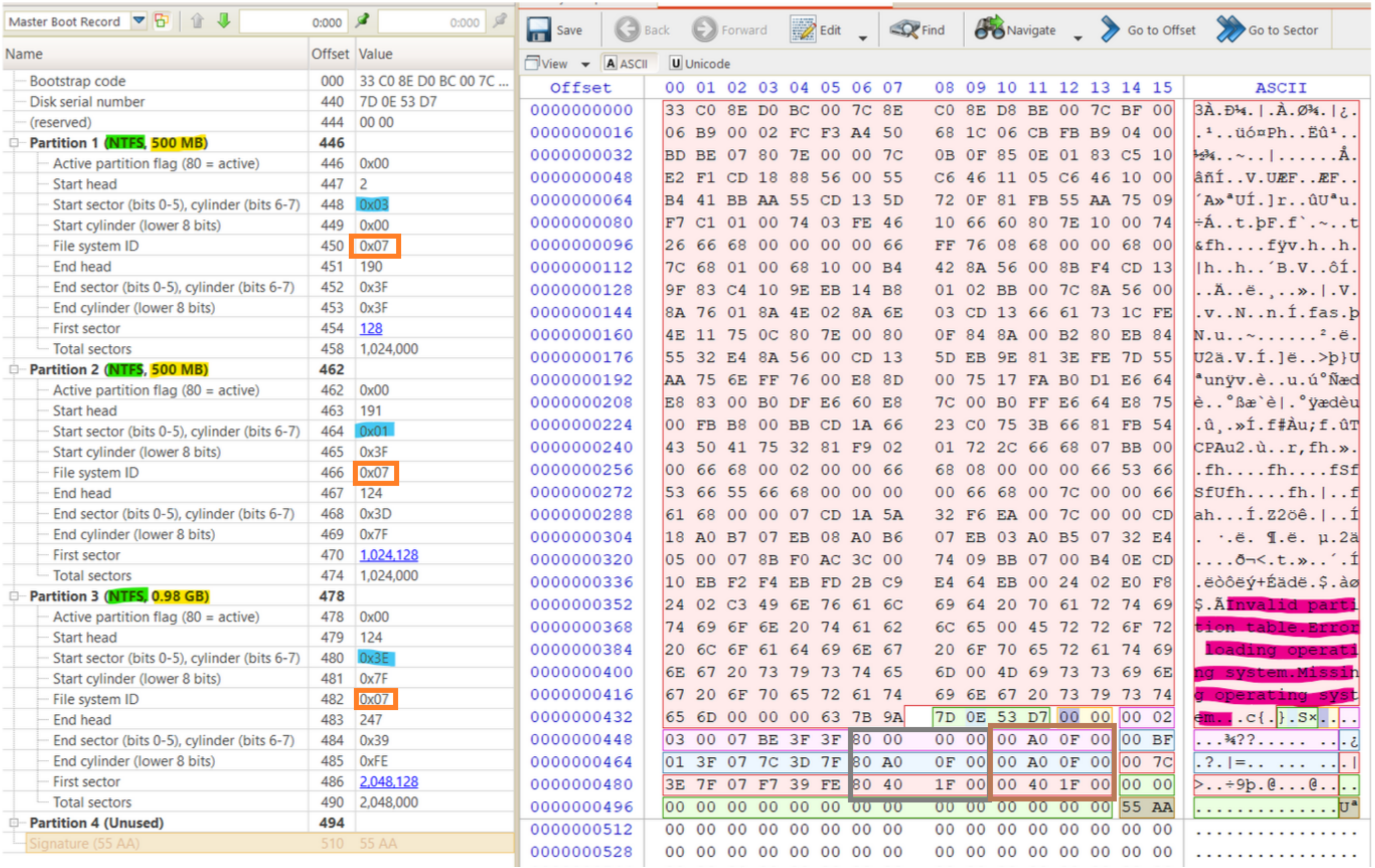
Also highlighted in yellow, is each partition’s size which is as follows:

- Partition 1: 500 MG
- Partition 2: 500 MG
- Partitions 3: 0.98 GB

The start sector of each partition is highlighted in light blue. Shows as follows:

- Partition 1: 0x03
- Partition 2: 0x01
- Partition 3: 0x3E

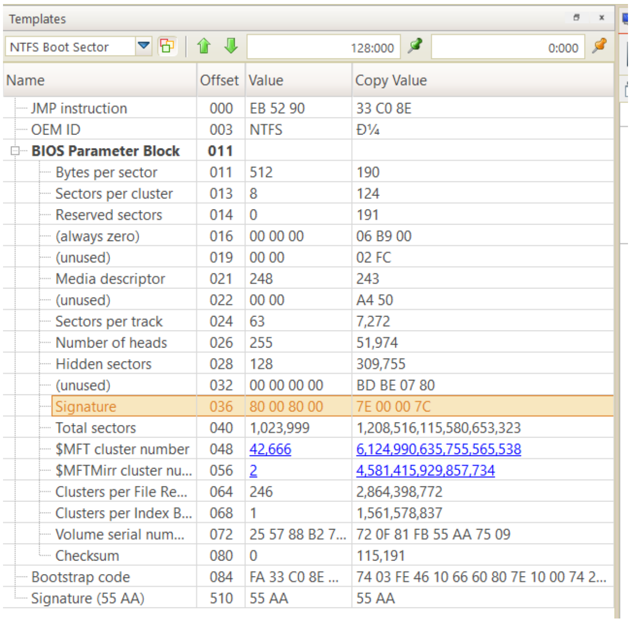
In the below figure, an error is highlighted is observed, which states that “Invalid partition table Error operating system missing operating system” in the observations section



Name	Offset	Value
Bootstrap code	000	33 C0 8E D0 BC 00 7C ...
Disk serial number	440	7D 0E 53 D7
(reserved)	444	00 00
Partition 1 (NTFS, 500 MB)	**446**	
Active partition flag (80 = active)	446	0x00
Start head	447	2
Start sector (bits 0-5), cylinder (bits 6-7)	448	0x03
Start cylinder (lower 8 bits)	449	0x00
File system ID	450	0x07
End head	451	190
End sector (bits 0-5), cylinder (bits 6-7)	452	0x3F
End cylinder (lower 8 bits)	453	0x3F
First sector	454	128
Total sectors	458	1,024,000
Partition 2 (NTFS, 500 MB)	**462**	
Active partition flag (80 = active)	462	0x00
Start head	463	191
Start sector (bits 0-5), cylinder (bits 6-7)	464	0x01
Start cylinder (lower 8 bits)	465	0x3F
File system ID	466	0x07
End head	467	124
End sector (bits 0-5), cylinder (bits 6-7)	468	0x3D
End cylinder (lower 8 bits)	469	0x7F
First sector	470	1,024,128
Total sectors	474	1,024,000
Partition 3 (NTFS, 0.98 GB)	**478**	
Active partition flag (80 = active)	478	0x00
Start head	479	124
Start sector (bits 0-5), cylinder (bits 6-7)	480	0x3E
Start cylinder (lower 8 bits)	481	0x7F
File system ID	482	0x07
End head	483	247
End sector (bits 0-5), cylinder (bits 6-7)	484	0x39
End cylinder (lower 8 bits)	485	0xFE
First sector	486	2,048,128
Total sectors	490	2,048,000
Partition 4 (Unused)	**494**	
Signature (55 AA)	510	55 AA

```
   Offset     00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15        ASCII
0000000000    33 C0 8E D0 BC 00 7C 8E  C0 8E D8 BE 00 7C BF 00   3À.Ð¼.|.À.Ø¾.|¿.
0000000016    06 B9 00 02 FC F3 A4 50  68 1C 06 CB FB B9 04 00   .¹..üó¤Ph..Ëû¹..
0000000032    BD BE 07 80 7E 00 00 7C  0B 0F 85 0E 01 83 C5 10   ½¾..~..|......Å.
0000000048    E2 F1 CD 18 88 56 00 55  C6 46 11 05 C6 46 10 00   âñÍ..V.UÆF..ÆF..
0000000064    B4 41 BB AA 55 CD 13 5D  72 0F 81 FB 55 AA 75 09   ´A»ªUÍ.]r..ûUªu.
0000000080    F7 C1 01 00 74 03 FE 46  10 66 60 80 7E 10 00 74   ÷Á..t.þF.f`.~..t
0000000096    26 66 68 00 00 00 00 66  FF 76 08 68 00 00 68 00   &fh....fÿv.h..h.
0000000112    7C 68 01 00 68 10 00 B4  42 8A 56 00 8B F4 CD 13   |h..h..´B.V..ôÍ.
0000000128    9F 83 C4 10 9E EB 14 B8  01 02 BB 00 7C 8A 56 00   ..Ä..ë.¸..».|.V.
0000000144    8A 76 01 8A 4E 02 8A 6E  03 CD 13 66 61 73 1C FE   .v..N..n.Í.fas.þ
0000000160    4E 11 75 0C 80 7E 00 80  0F 84 8A 00 B2 80 EB 84   N.u..~......².ë.
0000000176    55 32 E4 8A 56 00 CD 13  5D EB 9E 81 3E FE 7D 55   U2ä.V.Í.]ë..>þ}U
0000000192    AA 75 6E FF 76 00 E8 8D  00 75 17 FA B0 D1 E6 64   ªunÿv.è..u.ú°Ñæd
0000000208    E8 83 00 B0 DF E6 60 E8  7C 00 B0 FF E6 64 E8 75   è..°ßæ`è|.°ÿædèu
0000000224    00 FB B8 00 BB CD 1A 66  23 C0 75 3B 66 81 FB 54   .û¸.»Í.f#Àu;f.ûT
0000000240    43 50 41 75 32 81 F9 02  01 72 2C 66 68 07 BB 00   CPAu2.ù..r,fh.».
0000000256    00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66   .fh....fh....fSf
0000000272    53 66 55 66 68 00 00 00  00 66 68 00 7C 00 00 66   SfUfh....fh.|..f
0000000288    61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD   ah...Í.Z2öê.|..Í
0000000304    18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4   . ·.ë. ¶.ë. µ.2ä
0000000320    05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD   ....ð¬<.t.»..´.Í
0000000336    10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8   .ëòôëý+Éädë.$.àø
0000000352    24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69   $.ÃInvalid parti
0000000368    74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72   tion table.Error
0000000384    20 6C 6F 61 64 69 6E 67  20 6F 70 65 72 61 74 69    loading operati
0000000400    6E 67 20 73 79 73 74 65  6D 00 4D 69 73 73 69 6E   ng system.Missin
0000000416    67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74   g operating syst
0000000432    65 6D 00 00 00 63 7B 9A  7D 0E 53 D7 00 00 00 02   em...c{.}.S×....
0000000448    03 00 07 BE 3F 3F 80 00  00 00 00 A0 0F 00 00 BF   ...¾??.........¿
0000000464    01 3F 07 7C 3D 7F 80 A0  0F 00 00 A0 0F 00 00 7C   .?.|=..........|
0000000480    3E 7F 07 F7 39 FE 80 40  1F 00 00 40 1F 00 00 00   >..÷9þ.@...@....
0000000496    00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA   ..............Uª
0000000512    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0000000528    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

Figure(32): Virtual Disk Image



Name	Offset	Value	Copy Value
JMP instruction	000	EB 52 90	33 C0 8E
OEM ID	003	NTFS	Đ¼
BIOS Parameter Block	**011**		
Bytes per sector	011	512	190
Sectors per cluster	013	8	124
Reserved sectors	014	0	191
(always zero)	016	00 00 00	06 B9 00
(unused)	019	00 00	02 FC
Media descriptor	021	248	243
(unused)	022	00 00	A4 50
Sectors per track	024	63	7,272
Number of heads	026	255	51,974
Hidden sectors	028	128	309,755
(unused)	032	00 00 00 00	BD BE 07 80
Signature	036	80 00 80 00	7E 00 00 7C
Total sectors	040	1,023,999	1,208,516,115,580,653,323
$MFT cluster number	048	42,666	6,124,990,635,755,565,538
$MFTMirr cluster nu...	056	2	4,581,415,929,857,734
Clusters per File Re...	064	246	2,864,398,772
Clusters per Index B...	068	1	1,561,578,837
Volume serial num...	072	25 57 88 B2 7...	72 0F 81 FB 55 AA 75 09
Checksum	080	0	115,191
Bootstrap code	084	FA 33 C0 8E ...	74 03 FE 46 10 66 60 80 7E 10 00 74 2...
Signature (55 AA)	510	55 AA	55 AA

Figure(33): Signature for Partitions 1, 2, and 3

By clicking the start sector of each partition, The signature of partition one is shown in the table it is 7E 00 00 7C. It is highlighted in orange in Figure (33).

(Wikipedia, 2023)

In the following table for each partition, the following information is presented:

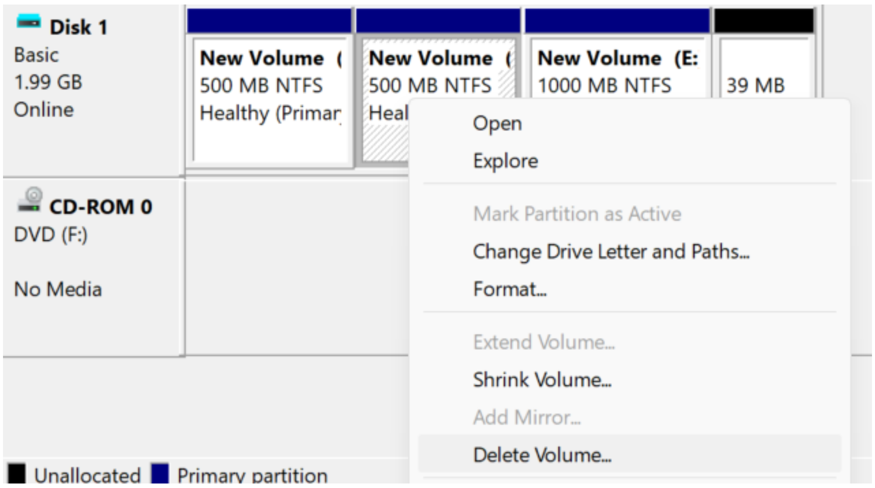
- If it's bootable or not. In this case **0x00** they are all non-bootable.
- The type of each partition. All of the type NFTs **0x07**
- The starting LBA address.
- The Size in Little-Endian.

Partition #	Flag (Boot ind)	Type (Sys ID)	Starting LBA Address	In Decimal	Size (In little endian)	In Decimal * 512 (In Bytes)
1	0x00	0x07	0x80	8	0xFA000	1,329,152,000
2	0x00	0x07	0xFA080	1,024,128	0xFA000	524,288,000
3	0x00	0x07	0xAF4080	11,485,312	0x1F4000	1,048,576,000

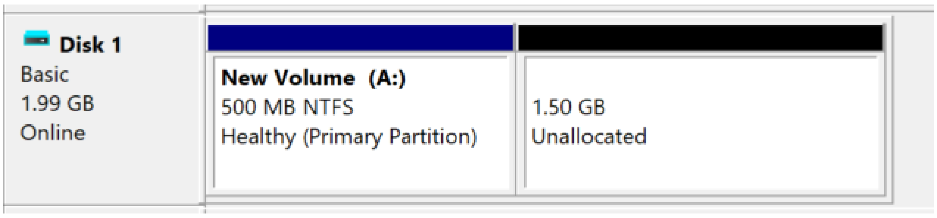
Table (1): Information about the partitions

3.3 Partitions Deletion

As the title shows, two partitions of the main three (A, B, E) will be deleted (B and E will be deleted). As shown in Figure(38) below:

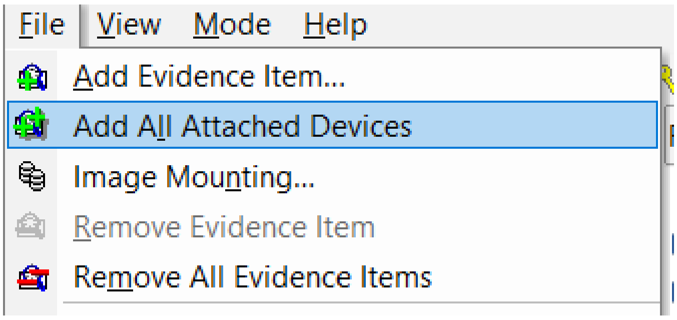


Figure(38): the partitions are deleted



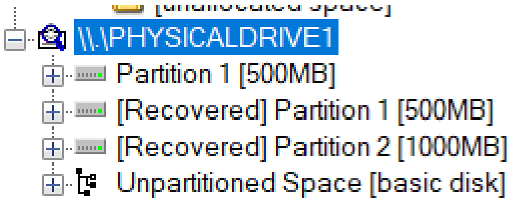
Figure(39): the virtual disk after deletion

Now that the partitions are deleted, the attached devices are added so that the virtual disk is shown with the evidence.



Figure(40): add the attached devices

Now adding the virtual disk has shown the following content in the following Figure(41) that is there found the deleted two partitions 1 and 2 with their sizes:



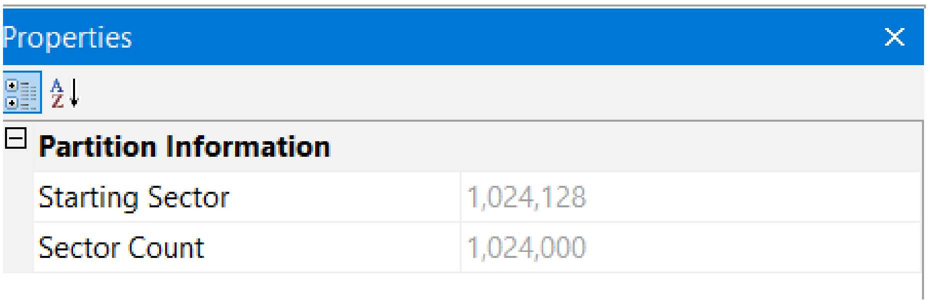
[unallocated space]
\\.\PHYSICALDRIVE1
- Partition 1 [500MB]
- [Recovered] Partition 1 [500MB]
- [Recovered] Partition 2 [1000MB]
- Unpartitioned Space [basic disk]

Figure(41): Content of the virtual disk

The information about each deleted partition including the size of the deleted partitions is shown below in Figure(40)below

Deleted Partition 1:

Size is 500 MB:



Properties

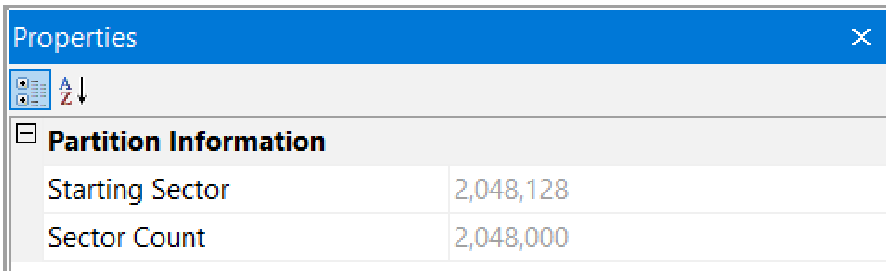
Partition Information

Starting Sector	1,024,128
Sector Count	1,024,000

Figure(42): Partition 1

Deleted Partition 2:

Size is 1000 MB:



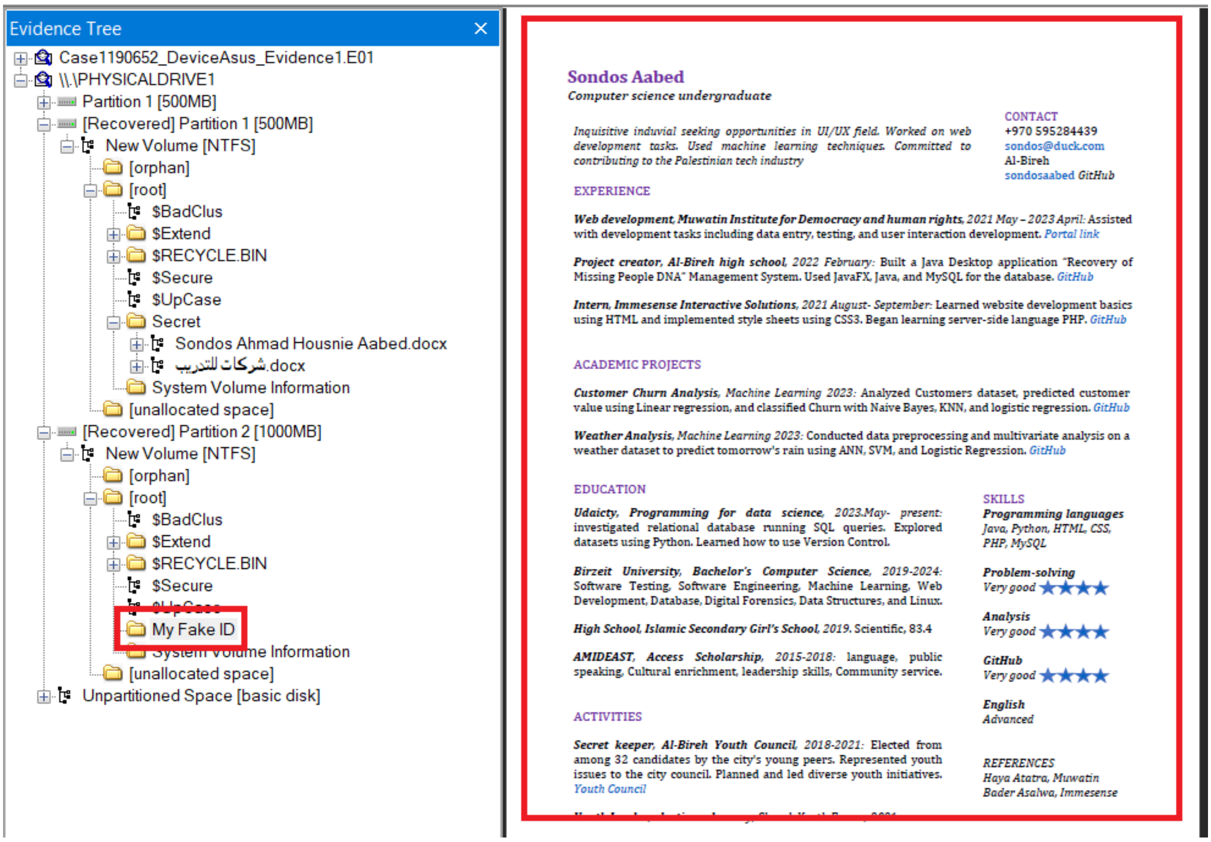
Properties

Partition Information

Starting Sector	2,048,128
Sector Count	2,048,000

Figure(43): Partition 2

In the following figure, one of the deleted files are also recovered from partition 2 and shown. The file name indicated that it is a fake ID:



Sondos Aabed
Computer science undergraduate

Inquisitive induvial seeking opportunities in UI/UX field. Worked on web development tasks. Used machine learning techniques. Committed to contributing to the Palestinian tech industry

CONTACT
+970 595284439
sondos@duck.com
Al-Bireh
sondosaabed *GitHub*

EXPERIENCE

***Web development, Muwatin Institute for Democracy and human rights**, 2021 May – 2023 April:* Assisted with development tasks including data entry, testing, and user interaction development. *Portal link*

***Project creator, Al-Bireh high school**, 2022 February:* Built a Java Desktop application "Recovery of Missing People DNA" Management System. Used JavaFX, Java, and MySQL for the database. *GitHub*

***Intern, Immesense Interactive Solutions**, 2021 August- September:* Learned website development basics using HTML and implemented style sheets using CSS3. Began learning server-side language PHP. *GitHub*

ACADEMIC PROJECTS

***Customer Churn Analysis**, Machine Learning 2023:* Analyzed Customers dataset, predicted customer value using Linear regression, and classified Churn with Naive Bayes, KNN, and logistic regression. *GitHub*

***Weather Analysis**, Machine Learning 2023:* Conducted data preprocessing and multivariate analysis on a weather dataset to predict tomorrow's rain using ANN, SVM, and Logistic Regression. *GitHub*

EDUCATION

***Udaicty, Programming for data science**, 2023.May- present:* investigated relational database running SQL queries. Explored datasets using Python. Learned how to use Version Control.

***Birzeit University, Bachelor's Computer Science**, 2019-2024:* Software Testing, Software Engineering, Machine Learning, Web Development, Database, Digital Forensics, Data Structures, and Linux.

***High School, Islamic Secondary Girl's School**, 2019.* Scientific, 83.4

***AMIDEAST, Access Scholarship**, 2015-2018:* language, public speaking, Cultural enrichment, leadership skills, Community service.

ACTIVITIES

***Secret keeper, Al-Bireh Youth Council**, 2018-2021:* Elected from among 32 candidates by the city's young peers. Represented youth issues to the city council. Planned and led diverse youth initiatives. *Youth Council*

SKILLS
Programming languages
Java, Python, HTML, CSS, PHP, MySQL

Problem-solving
Very good ★★★★

Analysis
Very good ★★★★

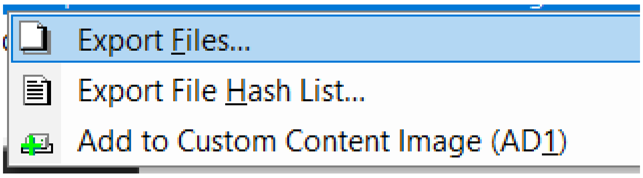
GitHub
Very good ★★★★

English
Advanced

REFERENCES
Haya Atatra, Muwatin
Bader Asalwa, Immesense

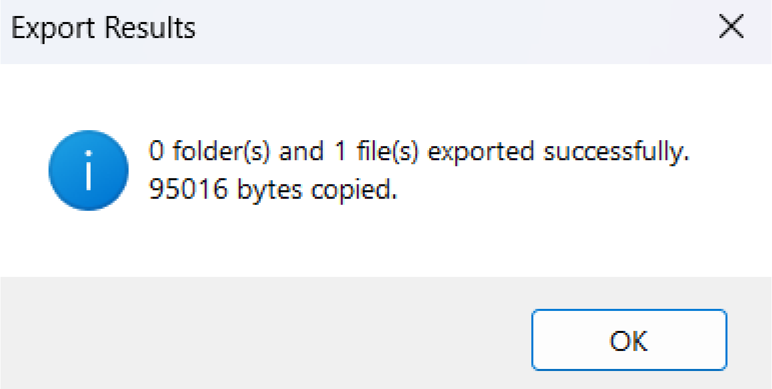
Figure(44): Recover Deleted File

To get the recovered file, the option to export it was selected as shown in figue 45:



Figure(45): Export Deleted File

After exporting it the following message was shown, indicating that the file was successfully recovered:

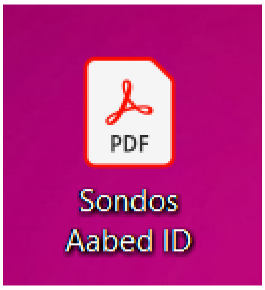


Export Results

0 folder(s) and 1 file(s) exported successfully.
95016 bytes copied.

Figure(46): Export Deleted File

After that, the file was found in the chosen saving directory as it was never deleted as shown in the below figure:



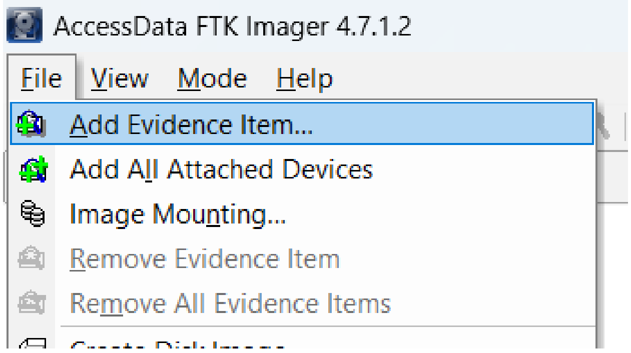
Figure(47): File recovered

Section 4: Evidence

In this section, the evidence built in Section One is opened and the file recovery process is worked on.

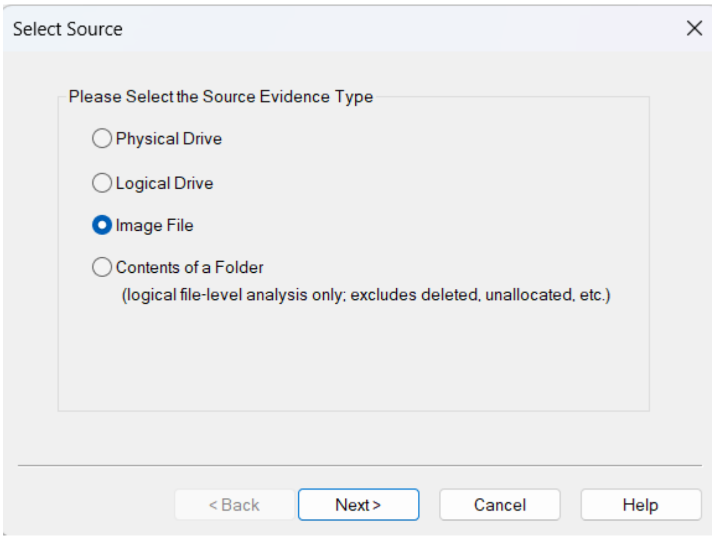
4.1 Using Backup

The FTK Imager is launched and the Add evidence File option is selected as shown in Figure(48):



Figure(48): Add evidence Item

The evidence created through section number 1 is now selected because it is a virtual hard disk drive image. Hence, the source is an image file as shown in Figure(49):


Select Source

Please Select the Source Evidence Type

○ Physical Drive

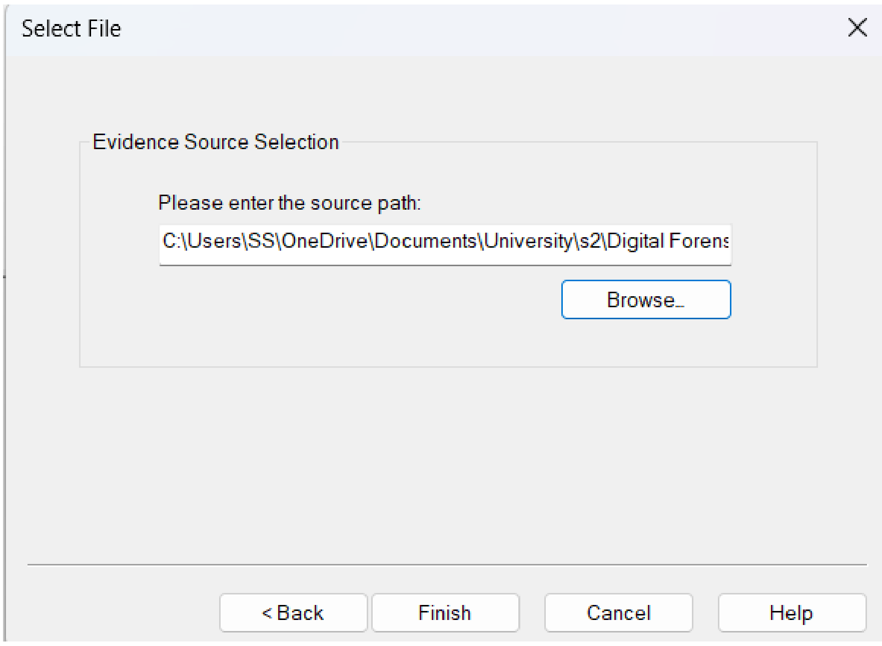
○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Figure(49): Image file

Now that the image file is selected, the source of the image path is defined in Figure(50):



Select File

Evidence Source Selection

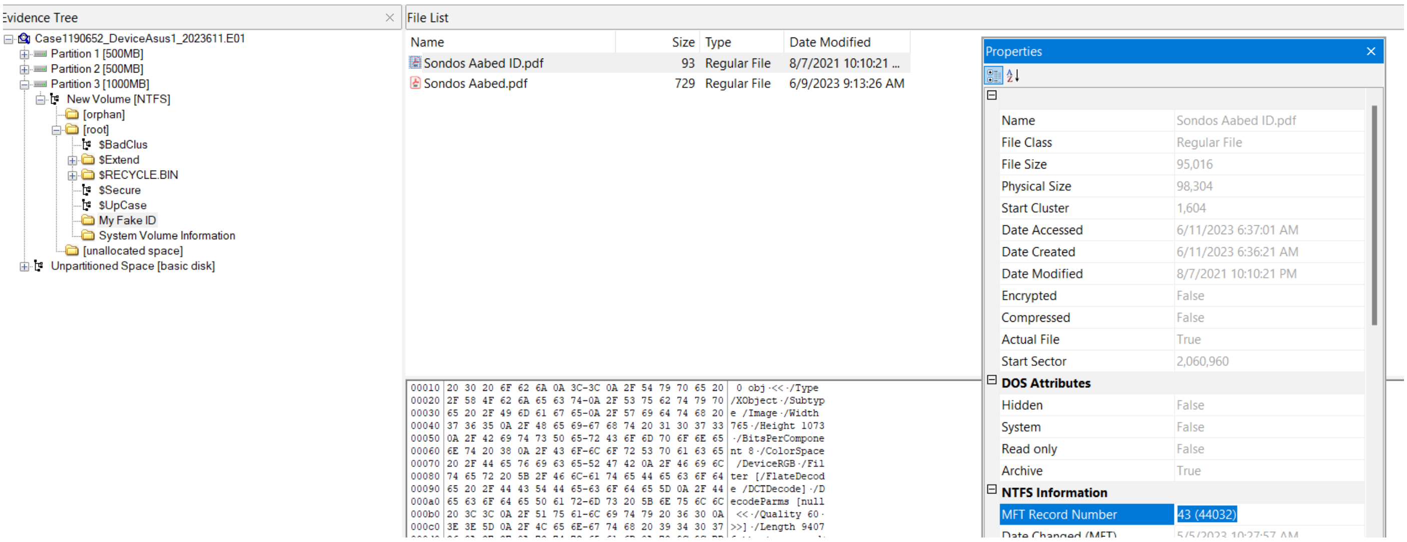
Please enter the source path:

C:\Users\SS\OneDrive\Documents\University\s2\Digital Forens

Figure(50): define the source path

4.2 File recovery

The search will be conducted on the Fake ID in partition 2. The MFT record number is 43 using the properties of the file. Shown in Figure (51)



```
Evidence Tree
Case1190652_DeviceAsus1_2023611.E01
  Partition 1 [500MB]
  Partition 2 [500MB]
  Partition 3 [1000MB]
    New Volume [NTFS]
      [orphan]
      [root]
        $BadClus
        $Extend
        $RECYCLE.BIN
        $Secure
        $UpCase
        My Fake ID
        System Volume Information
      [unallocated space]
  Unpartitioned Space [basic disk]
```

File List

Name	Size	Type	Date Modified
Sondos Aabed ID.pdf	93	Regular File	8/7/2021 10:10:21 ...
Sondos Aabed.pdf	729	Regular File	6/9/2023 9:13:26 AM

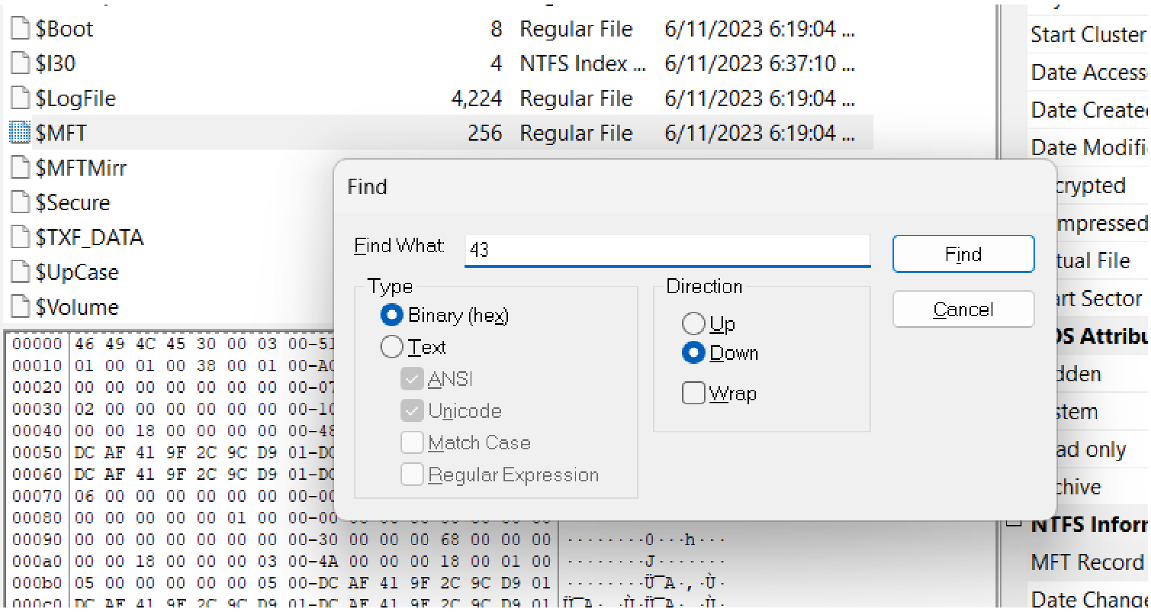
```
00010 20 30 20 6F 62 6A 0A 3C-3C 0A 2F 54 79 70 65 20  0 obj·<<·/Type
00020 2F 58 4F 62 6A 65 63 74-0A 2F 53 75 62 74 79 70 /XObject·/Subtyp
00030 65 20 2F 49 6D 61 67 65-0A 2F 57 69 64 74 68 20 e /Image·/Width
00040 37 36 35 0A 2F 48 65 69-67 68 74 20 31 30 37 33 765·/Height 1073
00050 0A 2F 42 69 74 73 50 65-72 43 6F 6D 70 6F 6E 65 ·/BitsPerCompone
00060 6E 74 20 38 0A 2F 43 6F-6C 6F 72 53 70 61 63 65 nt 8·/ColorSpace
00070 20 2F 44 65 76 69 63 65-52 47 42 0A 2F 46 69 6C  /DeviceRGB·/Fil
00080 74 65 72 20 5B 2F 46 6C-61 74 65 44 65 63 6F 64 ter [/FlateDecod
00090 65 20 2F 44 43 54 44 65-63 6F 64 65 5D 0A 2F 44 e /DCTDecode]·/D
000a0 65 63 6F 64 65 50 61 72-6D 73 20 5B 6E 75 6C 6C ecodeParms [null
000b0 20 3C 3C 0A 2F 51 75 61-6C 69 74 79 20 36 30 0A  <<·/Quality 60·
000c0 3E 3E 5D 0A 2F 4C 65 6E-67 74 68 20 39 34 30 37 >>]·/Length 9407
```

Properties

Name	Sondos Aabed ID.pdf
File Class	Regular File
File Size	95,016
Physical Size	98,304
Start Cluster	1,604
Date Accessed	6/11/2023 6:37:01 AM
Date Created	6/11/2023 6:36:21 AM
Date Modified	8/7/2021 10:10:21 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	2,060,960
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	43 (44032)
Date Changed (MFT)	5/5/2023 10:27:57 AM

Figure(51): properties of file ID

Now the number is used to search for a specific file in the storage space using MFT as shown in the Figure (52):



$Boot	8	Regular File	6/11/2023 6:19:04 ...
$I30	4	NTFS Index ...	6/11/2023 6:37:10 ...
$LogFile	4,224	Regular File	6/11/2023 6:19:04 ...
$MFT	256	Regular File	6/11/2023 6:19:04 ...
$MFTMirr			
$Secure			
$TXF_DATA			
$UpCase			
$Volume			

```
00000 46 49 4C 45 30 00 03 00-51
00010 01 00 01 00 38 00 01 00-AC
00020 00 00 00 00 00 00 00 00-07
00030 02 00 00 00 00 00 00 00-10
00040 00 00 18 00 00 00 00 00-48
00050 DC AF 41 9F 2C 9C D9 01-DC
00060 DC AF 41 9F 2C 9C D9 01-DC
00070 06 00 00 00 00 00 00 00-00
00080 00 00 00 00 00 01 00 00-00
00090 00 00 00 00 00 00 00 00-30 00 00 00 68 00 00 00  ········0···h···
000a0 00 00 18 00 00 00 03 00-4A 00 00 00 18 00 01 00  ········J·······
000b0 05 00 00 00 00 00 05 00-DC AF 41 9F 2C 9C D9 01  ········Ü¯A·,·Ù·
000c0 DC AF 41 9F 2C 9C D9 01-DC AF 41 9F 2C 9C D9 01  Ü¯A·,·Ù·Ü¯A·,·Ù·
```

Find

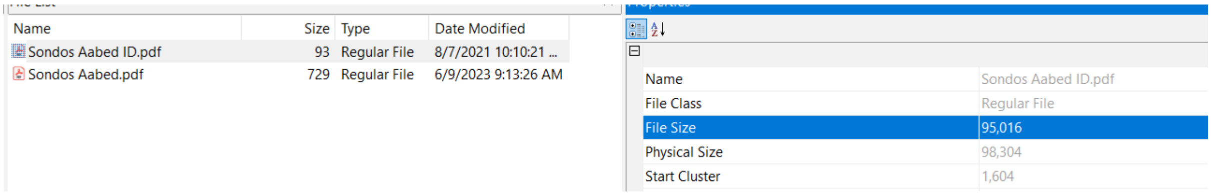
Find What: 43

Type
● Binary (hex)
○ Text
☑ ANSI
☑ Unicode
□ Match Case
□ Regular Expression

Direction
○ Up
● Down
□ Wrap

Figure(52): Search for a specific file in the storage space using MFT

The file size is defined in KB 95016. Shown in the below figure.

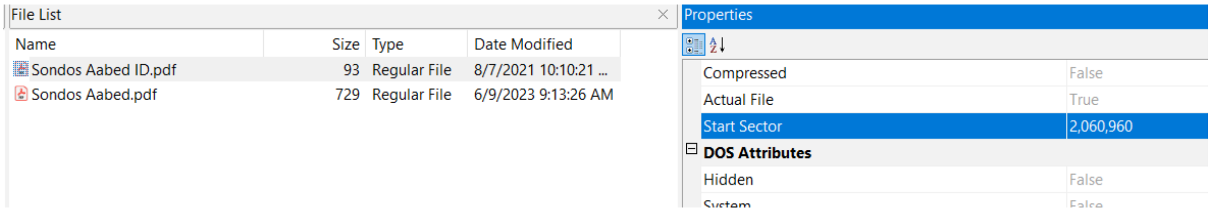


Name	Size	Type	Date Modified
Sondos Aabed ID.pdf	93	Regular File	8/7/2021 10:10:21 ...
Sondos Aabed.pdf	729	Regular File	6/9/2023 9:13:26 AM

Name	Sondos Aabed ID.pdf
File Class	Regular File
File Size	95,016
Physical Size	98,304
Start Cluster	1,604

Figure(53): file size

As for the start sector of the defined file it is specified in the properties of the file in the following figure:



File List

Name	Size	Type	Date Modified
Sondos Aabed ID.pdf	93	Regular File	8/7/2021 10:10:21 ...
Sondos Aabed.pdf	729	Regular File	6/9/2023 9:13:26 AM

Properties

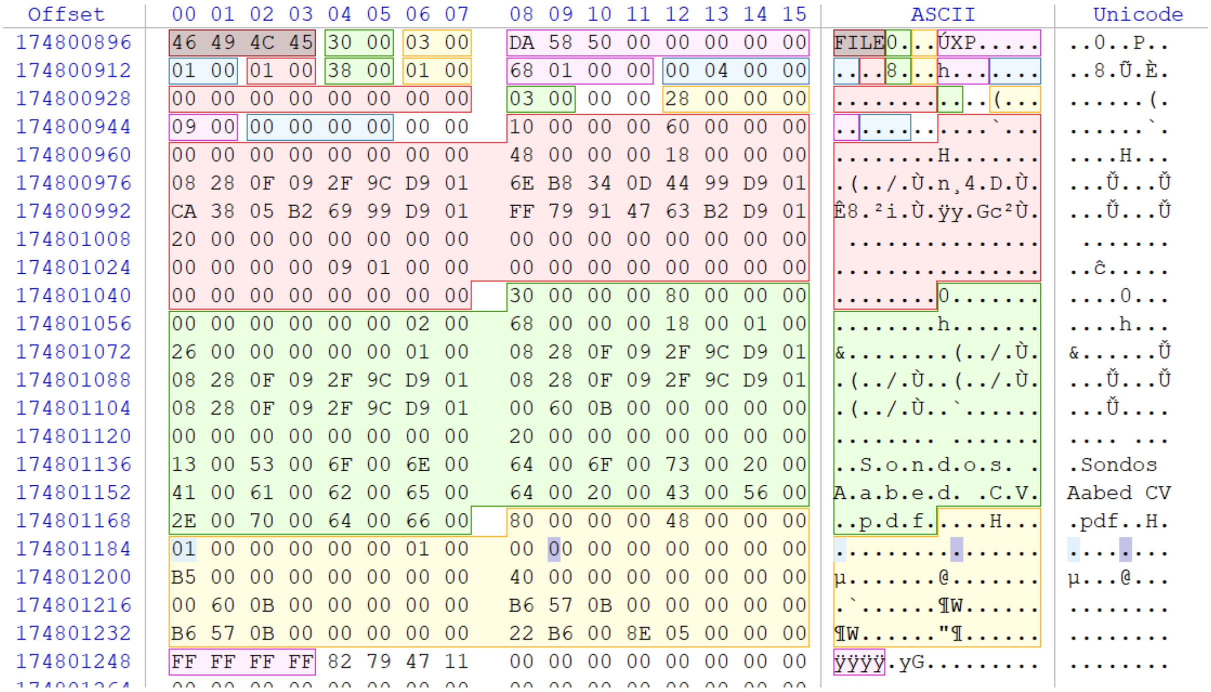
Compressed	False
Actual File	True
Start Sector	2,060,960
DOS Attributes	
Hidden	False
System	False

Figure(55): first sector

4.3 File Storage in MFT

In this section the Active @ disk Editor is used to determine wether the file is stored in sequence or not. And then if so the fragments of the file is recovered.

The file name is Sondos Aabed CV and the type of the file is pdf. First the file is opened using the tool:



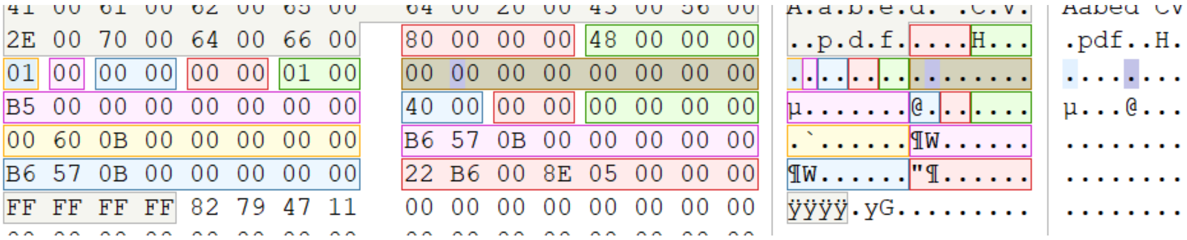
```
  Offset     00 01 02 03 04 05 06 07  08 09 10 11 12 13 14 15       ASCII          Unicode
174800896    46 49 4C 45 30 00 03 00  DA 58 50 00 00 00 00 00  FILE0...ÚXP.....   ..0..P..
174800912    01 00 01 00 38 00 01 00  68 01 00 00 00 04 00 00  ....8...h.......   ..8.Ǔ.È.
174800928    00 00 00 00 00 00 00 00  03 00 00 00 28 00 00 00  ............(...   ......(.
174800944    09 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ............`...   ......`.
174800960    00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......   ....H...
174800976    08 28 0F 09 2F 9C D9 01  6E B8 34 0D 44 99 D9 01  .(../.Ù.n¸4.D.Ù.   ...Ǔ...Ǔ
174800992    CA 38 05 B2 69 99 D9 01  FF 79 91 47 63 B2 D9 01  Ê8.²i.Ù.ÿy.Gc²Ù.   ...Ǔ...Ǔ
174801008    20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............    .......
174801024    00 00 00 00 09 01 00 00  00 00 00 00 00 00 00 00  ................   ..ĉ.....
174801040    00 00 00 00 00 00 00 00  30 00 00 00 80 00 00 00  ........0.......   ....0...
174801056    00 00 00 00 00 00 02 00  68 00 00 00 18 00 01 00  ........h.......   ....h...
174801072    26 00 00 00 00 00 01 00  08 28 0F 09 2F 9C D9 01  &........(../.Ù.   &......Ǔ
174801088    08 28 0F 09 2F 9C D9 01  08 28 0F 09 2F 9C D9 01  .(../.Ù..(../.Ù.   ...Ǔ...Ǔ
174801104    08 28 0F 09 2F 9C D9 01  00 60 0B 00 00 00 00 00  .(../.Ù..`......   ...Ǔ....
174801120    00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ........ .......   .... ...
174801136    13 00 53 00 6F 00 6E 00  64 00 6F 00 73 00 20 00  ..S.o.n.d.o.s. .   .Sondos
174801152    41 00 61 00 62 00 65 00  64 00 20 00 43 00 56 00  A.a.b.e.d. .C.V.   Aabed CV
174801168    2E 00 70 00 64 00 66 00  80 00 00 00 48 00 00 00  ..p.d.f.....H...   .pdf..H.
174801184    01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00  ................   ........
174801200    B5 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  µ.......@.......   µ...@...
174801216    00 60 0B 00 00 00 00 00  B6 57 0B 00 00 00 00 00  .`......¶W......   ........
174801232    B6 57 0B 00 00 00 00 00  22 B6 00 8E 05 00 00 00  ¶W......"¶......   ........
174801248    FF FF FF FF 82 79 47 11  00 00 00 00 00 00 00 00  ÿÿÿÿ.yG.........   ........
```

Figure(56): File opened by active @ disk editor

As shown if the above figure this file has 3 partitions (Attributes of the file). The definition of each is as follow:

- The partition that starts with (FILE) is The header partition.
- The partition in red is Information about the file that begins with (10 00..)
- The partition in green is the File name begins with (30 00 …)
- The partition in Yellow is the Data attribute which begins with (80 00 …)

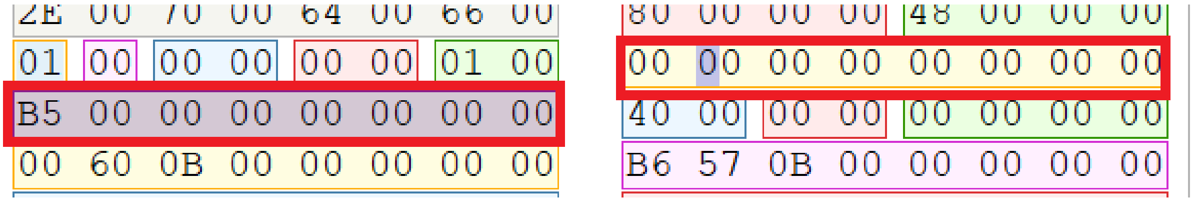
In this part the Data attribute section is the one that will be looked into which is shown in the following figure, which is the one that is in color yellow:



```
41 00 61 00 62 00 65 00  64 00 20 00 43 00 56 00  A.a.b.e.d. .C.V.  Aabed CV
2E 00 70 00 64 00 66 00  80 00 00 00 48 00 00 00  ..p.d.f.....H...  .pdf..H.
01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00  ................  ........
B5 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  µ.......@.......  µ...@...
00 60 0B 00 00 00 00 00  B6 57 0B 00 00 00 00 00  .`......¶W......  ........
B6 57 0B 00 00 00 00 00  22 B6 00 8E 05 00 00 00  ¶W......"¶......  ........
FF FF FF FF 82 79 47 11  00 00 00 00 00 00 00 00  ÿÿÿÿ.yG.........  ........
```

Figure(57): Data Attribute of the file

To define if the file was sequence stored or not, these two numbers are interpreted the first one defined in red is the First Virtual Cluster Number (VCN) which is 0, the second one is the Last (VCN) which is 181.



```
2E 00 70 00 64 00 66 00      80 00 00 00 48 00 00 00
01 00 00 00 00 00 01 00      00 00 00 00 00 00 00 00
B5 00 00 00 00 00 00 00      40 00 00 00 00 00 00 00
00 60 0B 00 00 00 00 00      B6 57 0B 00 00 00 00 00
```

Figure(58): First and Last VCN

Because the Last and the first VCN are not the same that indicates that the file is not stored in sequence instead it was fragmented.

Section 5: Conclusion

In this section, the observations of the investigation process are presented. Some recommendations for the process were shown too.

5.1 Findings and Observations

During the investigation, when the Active access tool was used on the virtual hard disk drive. An error message was shown that the operating system was not found and the partition table was not valid. That is thought to be due to the virtual disk created not being considered bootable.

5.2 Recommendations

Some suggestions are made in this section, regarding the techniques and methods used throughout the steps of the investigation. Generally, to have a higher accuracy of the investigation results.

For example, The devices are so vital in such investigation, the suggestion is to use proper investigation devices, due to the constant stopping of the current used.

References

Exterro. "Features & Capabilities." *Exterro software*, 2023, FTK Imager - Exterro. Accessed 5 6 2023.

Active Disk editor. "Overview." *Active@ Disk Editor*, 2023, Active@ Disk Editor. Accessed 5 6 2023.

Partition type. (2023, June 22). In *Wikipedia*. https://en.wikipedia.org/wiki/Partition_type