A digital crime scene investigation of a hard drive image using Autopsy and FTK imager

By Hazrat Umer

4/5/2024

In this report I have completed a forensics analysis of a hard drive image found during a during a crime scene.

Contents

Introduction:

The following report outlines the case management procedures undertaken during the digital forensic investigation conducted in collaboration with an international agency. As a digital forensic analyst at a UK law enforcement agency, the investigation involved the analysis of a forensic image obtained from a computer seized as evidence from the scene of a crime.

Setting up the New Case:

Upon receiving the assignment, the case was initiated within the agency's case management system. A unique case number was assigned, and a case folder was created to organize all relevant documentation and evidence associated with the investigation.

Team Assignments and Resource Allocation:

Roles and responsibilities were assigned to members of the investigation team, including forensic analysts, case managers, and technical specialists. Resources such as forensic workstations, software tools, and storage facilities were allocated to support the investigation.

Evidence Collection and Preservation:

A member of the investigation team was responsible for collecting forensic artifacts from the crime scene. Stringent procedures were followed to ensure the integrity and continuity of the evidence during collection, transportation, and storage. Special care was taken to preserve the chain of custody for each item seized. A forensic image technician created a forensic image of seized hard disk and calculated a hash value for it, and stored it securely.

Chain of Custody Management:

The chain of custody was properly documented to track the movement and handling of the forensic artifacts throughout the investigation. Each transfer of custody was recorded, including the date, time, location, and individuals involved. Measures were implemented to safeguard the integrity of the evidence at all times.

Quality Assurance and Documentation:

Quality assurance measures were implemented to verify the accuracy and reliability of the forensic analysis. Forensic tools and methodologies were properly tested to ensure their effectiveness and validity. Comprehensive documentation, including contemporaneous notes, case logs, and investigative reports, was maintained throughout the investigation.

Coordination with External Agencies:

Effective communication and collaboration were established with the international agency involved in the investigation. Information sharing mechanisms were put in place to facilitate collaboration across jurisdictions and organizations. Regular updates and progress reports were exchanged to ensure alignment and coordination between all parties involved.

Conclusion and Summary:

In conclusion, the successful management of the case relied on proper planning, coordination, and execution of forensic procedures. By following best practices in evidence handling, chain of custody management, and quality assurance, the investigation was conducted with integrity and professionalism.

Evidence analysis:

As a Forensic Analyst, I created a copy of the forensics image, compared that hash present with image file. Started analysis on the digital evidence and analyzed the following.

Partition Analysis:

Partitions:

During investigation of the provided disk image. I found 4 partitions and 2 unallocated spaces.

- Vol4 which is Basic data partition
- Vol5 (EFI, which is system partition)
- Vol6 which is Microsoft Reserved partition.
- Vol7 which is basic data partition

Unallocated Spaces:

- Vol1 which is unallocated
- Vol8 It is an unallocated space.

File System:

During an investigation I found that the File System is NTFS.

Operating System Installations:

By analyzing the provided image in Autopsy, I come into a conclusion that the user was using Windows 10 Education version as an operating system.

Programs installed:

There were total 50 programs installed in the target disk. Following are some of them.

- Some were Graphic drivers, such as NVIDIA Stereoscopic 3d Driver v7.17.13.7500. Google Chrome v.65.0.3325.181,Mplayer2,AddressBook,Office 16 and Drop box etc. but the interesting ones that are One drive and Amazon S3 and Drop box and Microsoft Office because the user was using these all the times.

Analyzing Internet Activity:

There are various things to analyze internet activity of the target but I analyzed the following.

Browser Used:

The target user was using Google Chrome browser. I found he was using one Google account on it.

User Accounts:

One User Profile found on Google Chrome. The profile was created on 2018-03-27 09:33:01 GMT and last accessed and modified on 2018-04-06 12:49:35 GMT.

User Profiles:

There were several users present, i.e Jcloudy, Administrator, Guest, and while some were default accounts, some of them were service accounts. I ignored all those because there were no login activities from those accounts. During an investigation I found a User named Jcloudy, his account was created on 2018-03-27. He logged in into his account 23 times. His last login was on 2018-03-27 09:18:58 GMT time. It is normal user account.

Personal data Analysis:

During my analysis different type of MS word, Excel, Power Point and .rtf files were present there. I found total 36 Files.

Analyzing the Metadata of Files:

I analyzed the metadata of some word and Excel files.

Analyzing the word documents for the Jcloudy User:

Found a MS Word file named ***f_0016a6*** own by user Jcloudy found at location ***/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/UserData/Default/Cache/f_0016a6.*** This document was created on 2018-03-29 21:29:00 GMT. The information I found on this document is discussed in Findings and Conclusion section. I found another an interesting MS Word file located at the following location. */img_Image.E01/vol_vol7/Users/jcloudy/Desktop/Planning.docx* named planning.docx. Having size of 4060 containing 588 characters. I am calling this is an interesting file because the user was planning some criminal activity. I have shared the mentioned file screenshots in the appendix section and explained my findings in detail in the findings and conclusion section.

Analyzing the MS Excel file of the Jcloudy User:

Found a Microsoft Excel File named was rootkey((Autosaved-306579222169168469)).xlsb and the original file name was ROOTKE~1.XLS at location

/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Roaming/Microsoft/Excel/rootkey306579560141686273/rootkey((Autosaved-306579222169168469)).xlsb

owned by User Jcloudy. This Excel sheet was created on Created on 2018-04-06 12:37:32 GMT The last modification date and time was 2018-04-06 12:37:32 GMT. The last access data was 2018-04-06 12:37:32 GMT. All three dates and time were the same and the file size was 8966.

Findings and Conclusions:

Found an MS Word document named f_0016a6 owned by user Jcloudy containing Airport Information, and the location information. The Snapshot is attached at Appendix section. Found another file named AIRPORT INORMATION.docx/Image1.png located at JCloudy Desktop where the user was searching for the round trip cost from Washington DC to Denpasar Bali Indonesia.

An Excel file named rootkey((Autosaved-306579222169168469)).xlsb at location

/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Roaming/Microsoft/Excel/rootkey3065795601416 86273/rootkey((Autosaved-306579222169168469)).xlsb.

Owned by User Jcloudy containing AWS Secret key and AWS Key Id, snapshot is attached at appendix Section. The another thing that I found is the user was using Google Chrome browser, there was only single Google account found with associated Gmail address and the user email was jimcloudy1@gmail.com.

By analyzing Jcloudy's Desktop file named Planning.docx. The person is criminal and he is planning to kill someone. He is planning that he should have a good escape route and a zone where he is targeting someone must be a gun free zone. He is planning to purchase gun from black market market and mentioned location as well and he has also a plan B for it.

He want to purchase 9mm and mentioned the price which is $360 in the planning document. His other option is to purchase Kel-Tec Sub 2000 9mm for $400.

His plan C is to purchase gloves, plan D is to purchase Velcro tear away clothing and he is planning a cash for it. He is also want to create a plan for escape after doing his criminal activity, He is planning not to go to extradition countries. His one choice is Indonesia but this is expensive for him. The 2nd option for him is Vietnam and he is choosing a country that he can live easily by sending 100 USD a day for 9 years. His other option is to book a ticket for same day, the day he conclude his mission, he prefers direct flight. He also want a suitcase with him in the car.

He want to write his ideas and thoughts and saving it in a separate locations for redundancy and placing it in a cloud so that he can access it remotely. He is releasing it in a press once he go back home.

According to Operation 2nd Hand Smoke.pptx document. He named his activity an Operation 2nd Hand Smoke. From sheep.jpg located at his desktop it can be concluded from " I would be a lone wolf rather than part of a pair of sheep. It means that he is committing this alone.

At the end according to my investigation the person is committing a crime, for this purpose he is collecting information and creating a proper plan that how he will be doing all the necessary steps like from purchasing guns to escaping and releasing it in a press.

References:

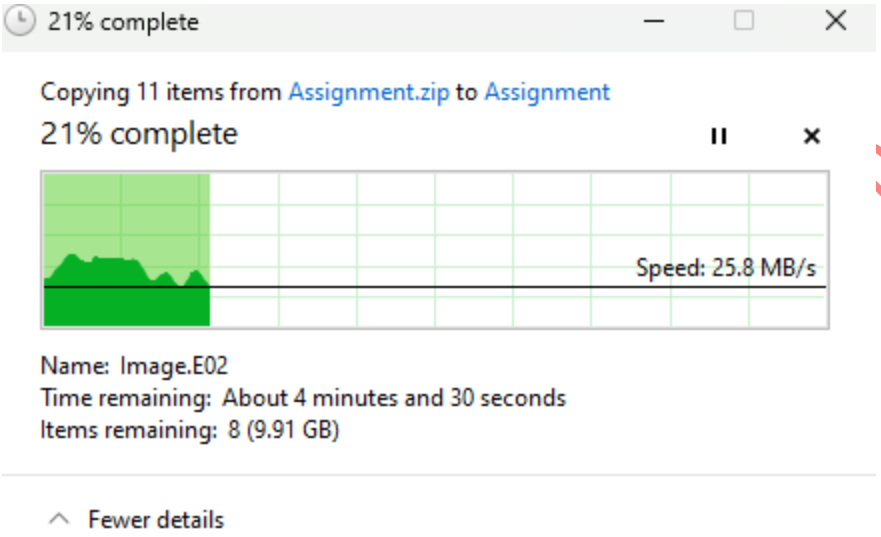
James, (2022). Data Artifacts, Analysis Results, and Reporting in Autopsy. Retrieved from URL https://dfir.science/2022/02/data-artifacts-analysis-results-and-reporting-in-autopsy.

Rose, (2023). How to Forensically Analyze a Disk Using Autopsy?. Retrieved from URL https://thesecmaster.com/blog/how-to-forensically-analyze-a-disk-using-autopsy.

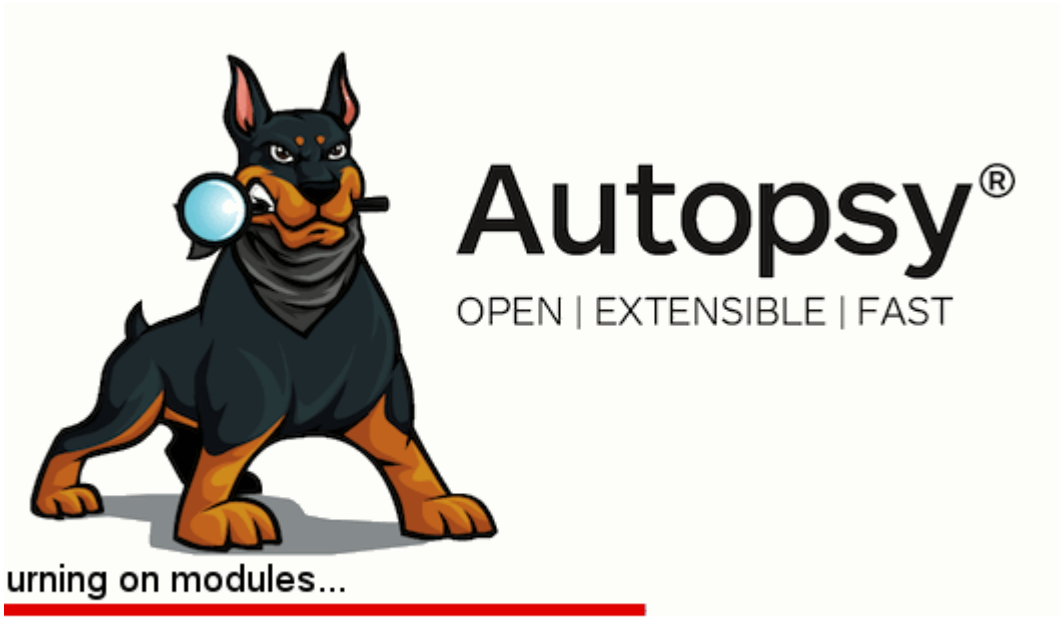
Dixon, (2023). TryHackMe: Disk Analysis & Autopsy. Retrieved from URL https://terguttac.medium.com/tryhackme-disk-analysis-autopsy-d4883eb7ab51.

Appendix:

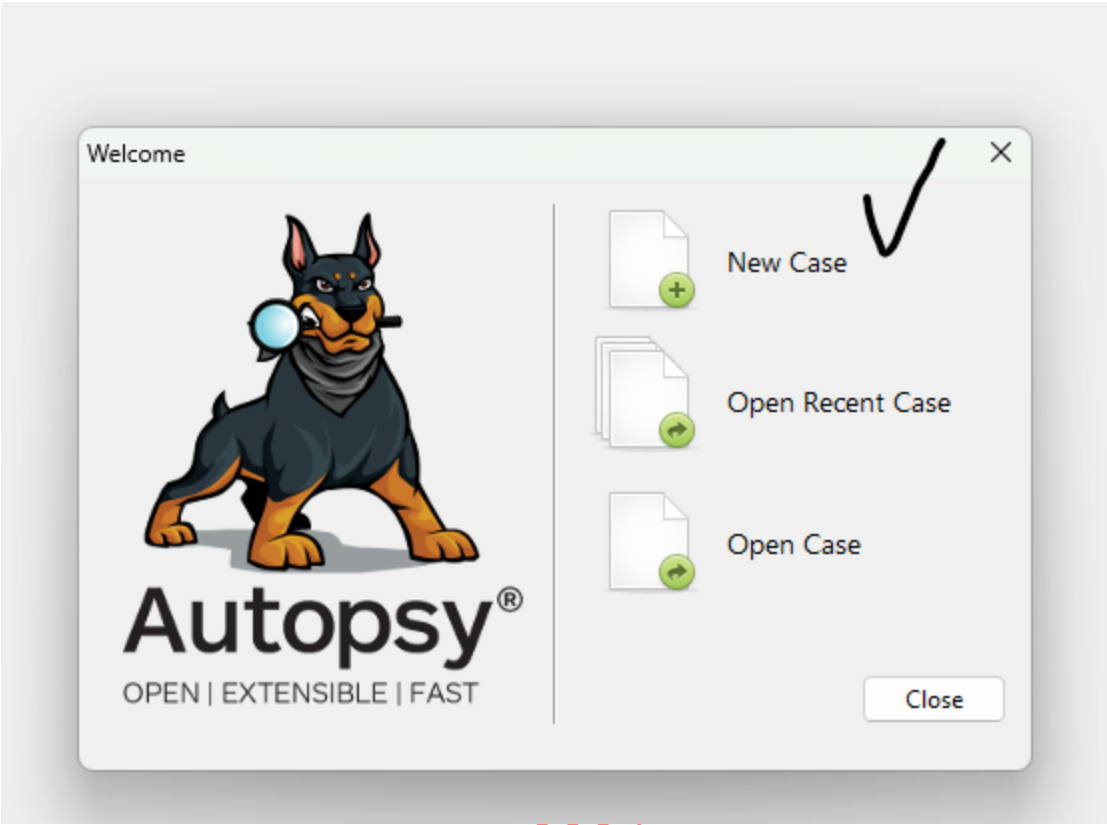
First I have downloaded the image provided and extracted it. Installed the Autopsy and FTK imager to analyze this image. But I have only inserted the Autopsy screenshots here.



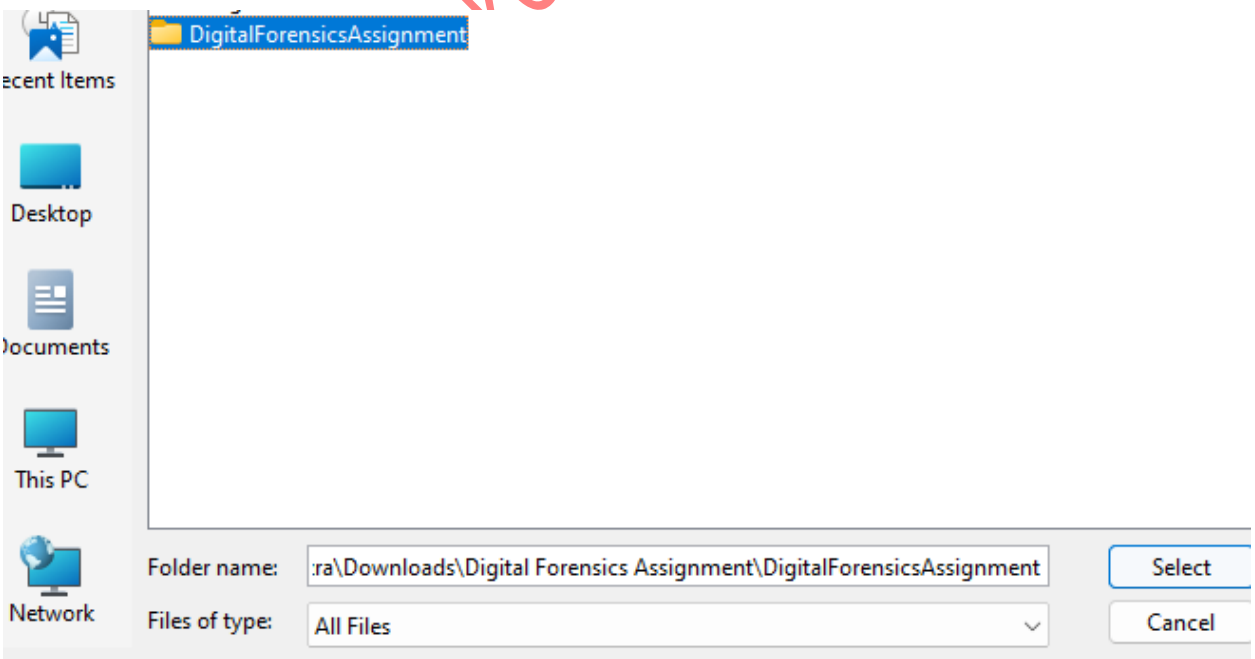
Opened Autopsy 4.21.0

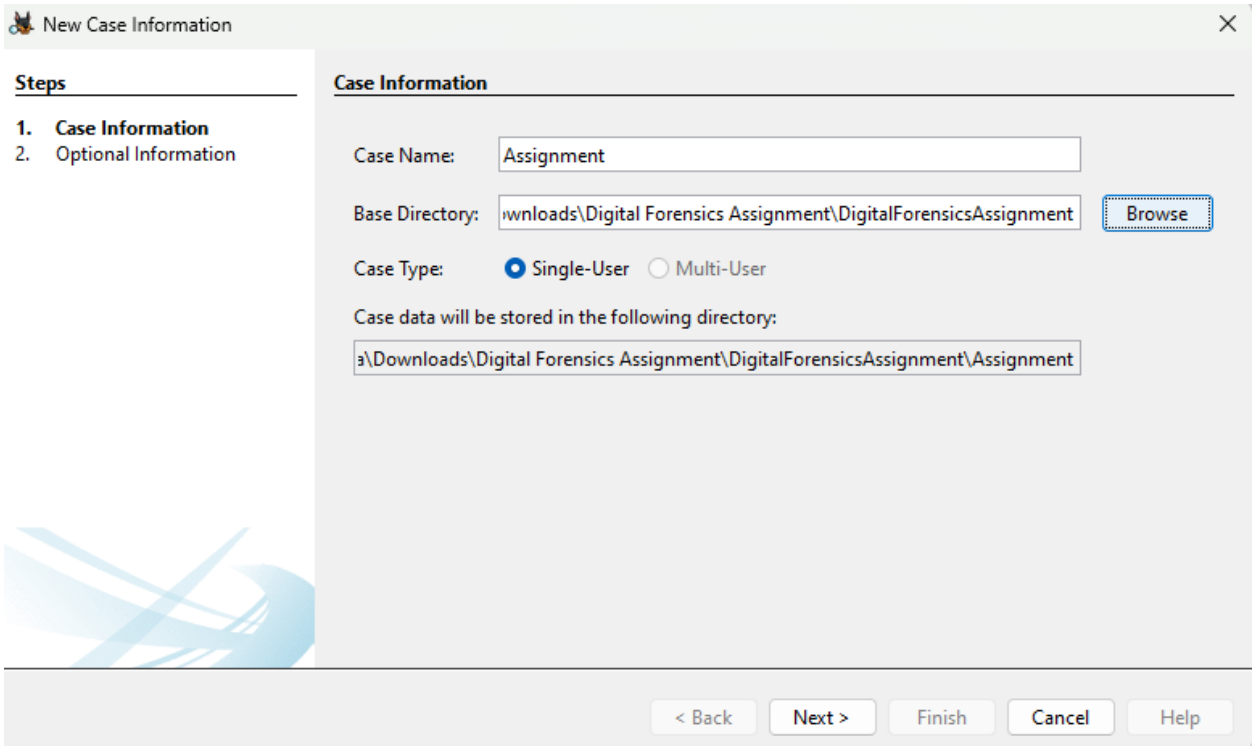


Created New Case:

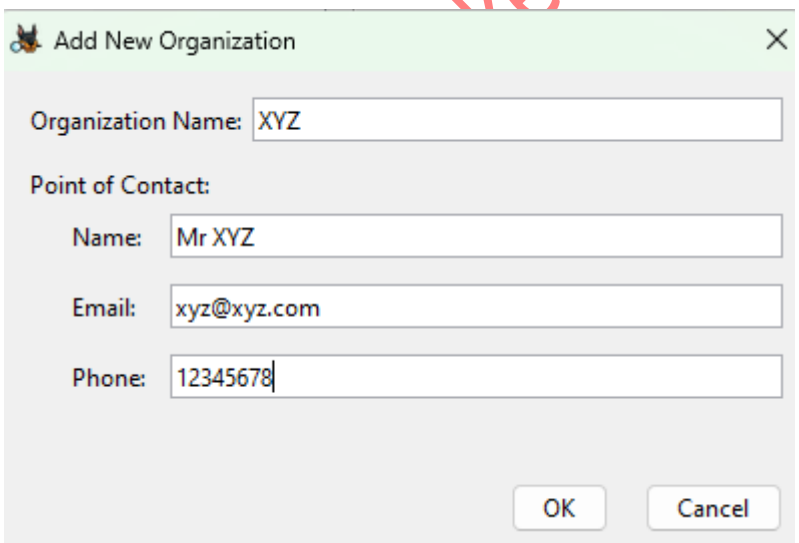


Case our Case Name is DigitalForensicAssignment

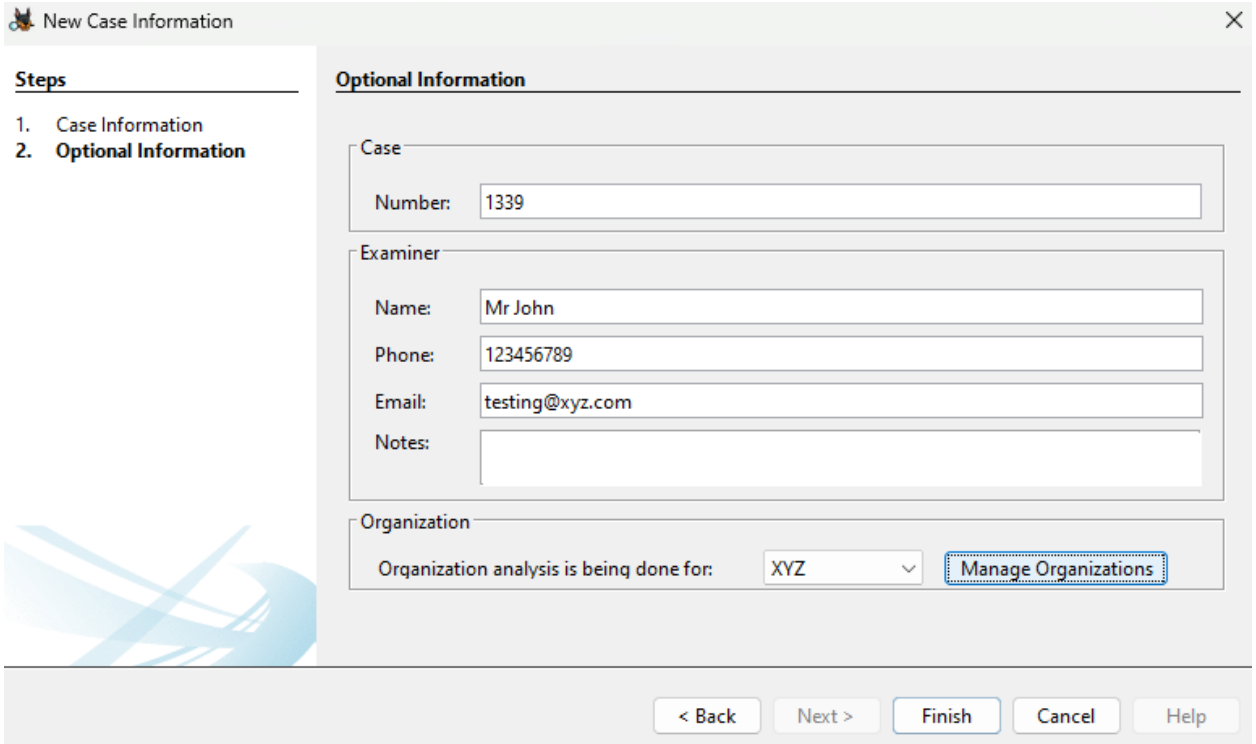




Added Organizational Information:



Assigned a case Number and examiner details.

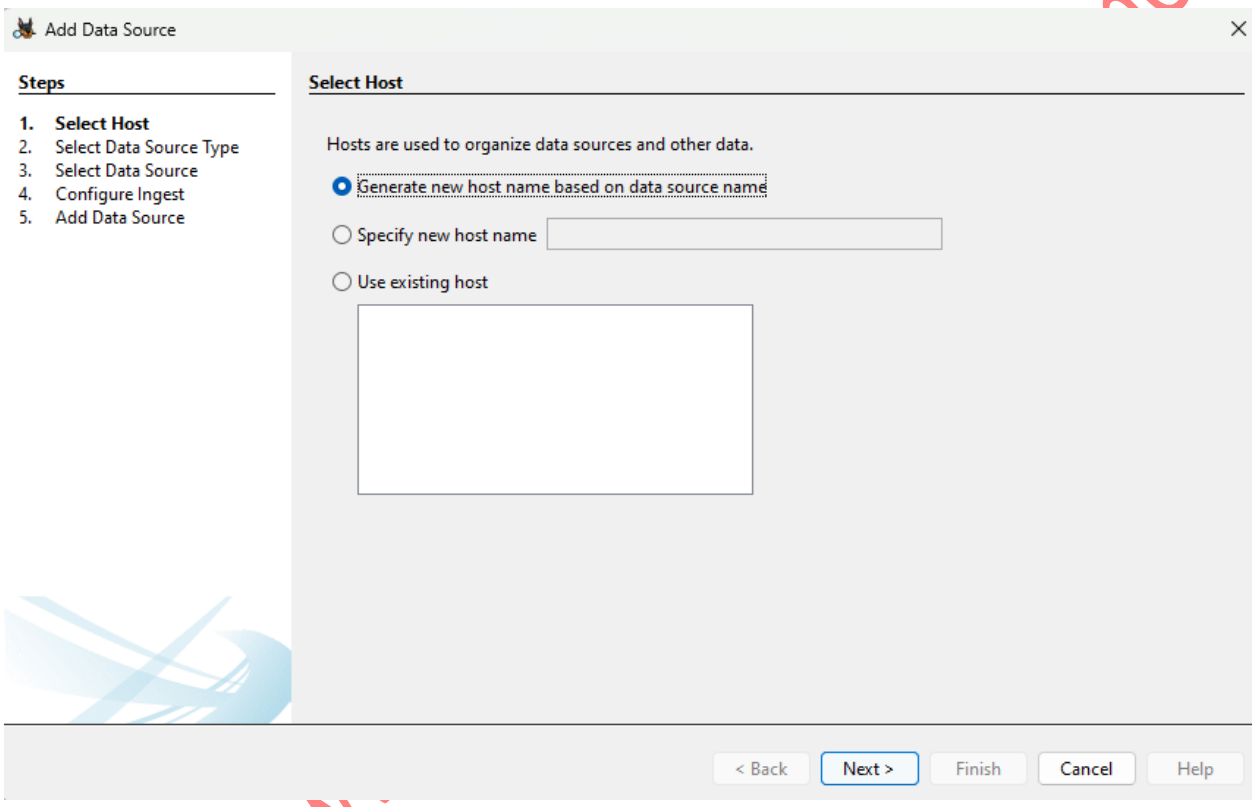


Adding Data source:

Now I am adding the data source.

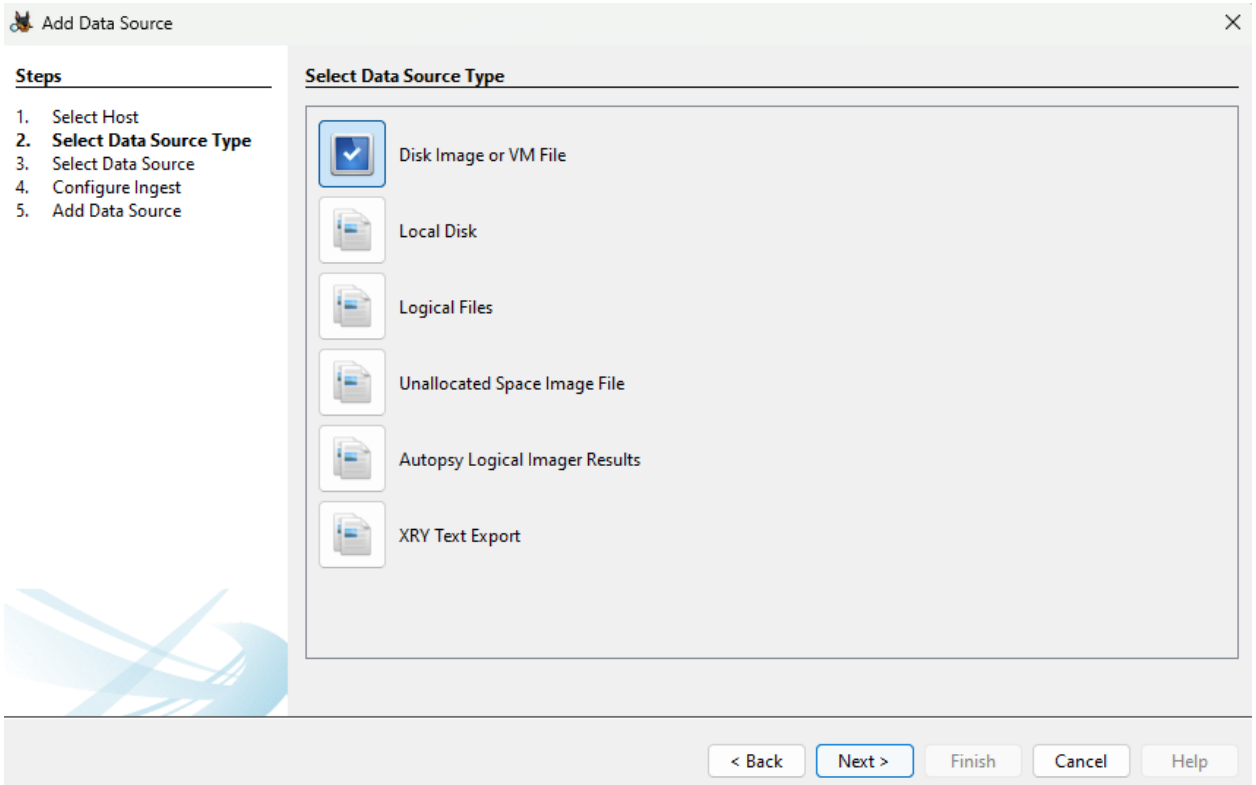
Selecting Host.

I am selecting the Generate new host name based on data source name. Through this option the Autopsy will auto generate new host name based on the data source name.



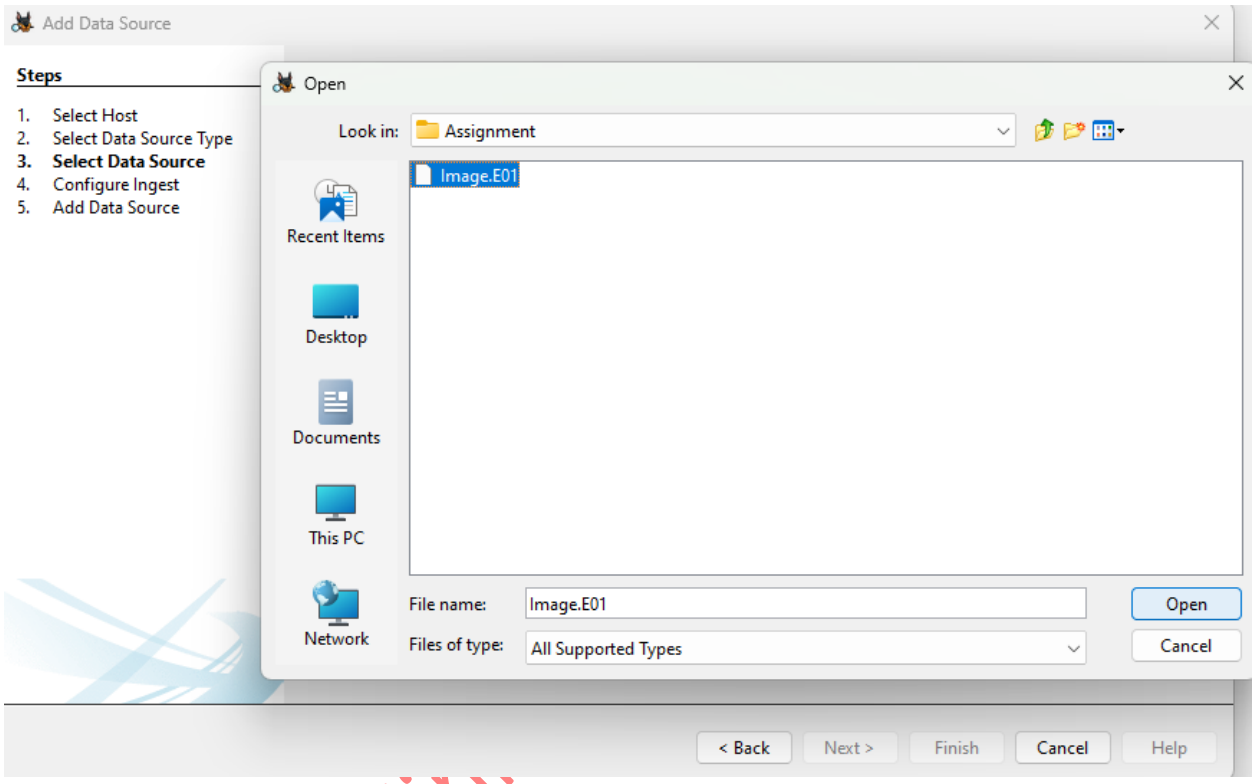
Choosing Data Source Type:

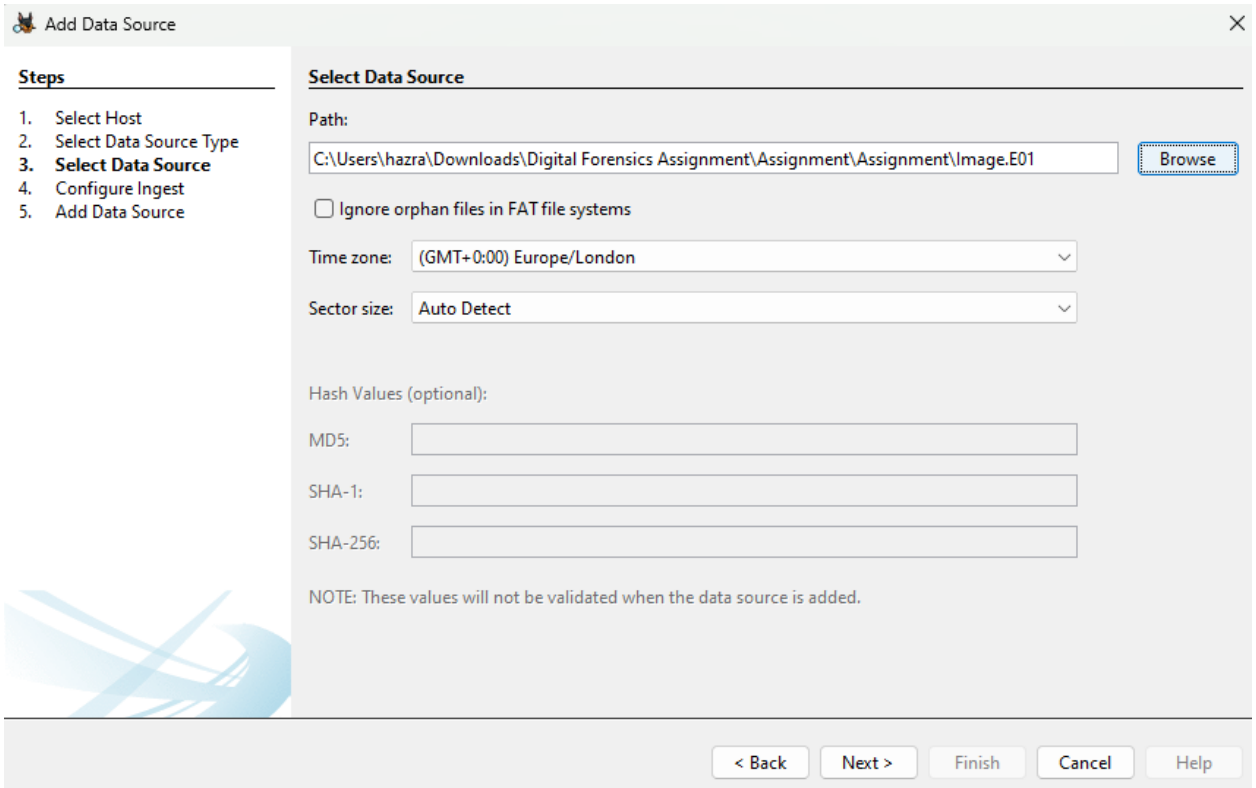
Since I am doing it on a disk image. I am selecting Disk Image option here.



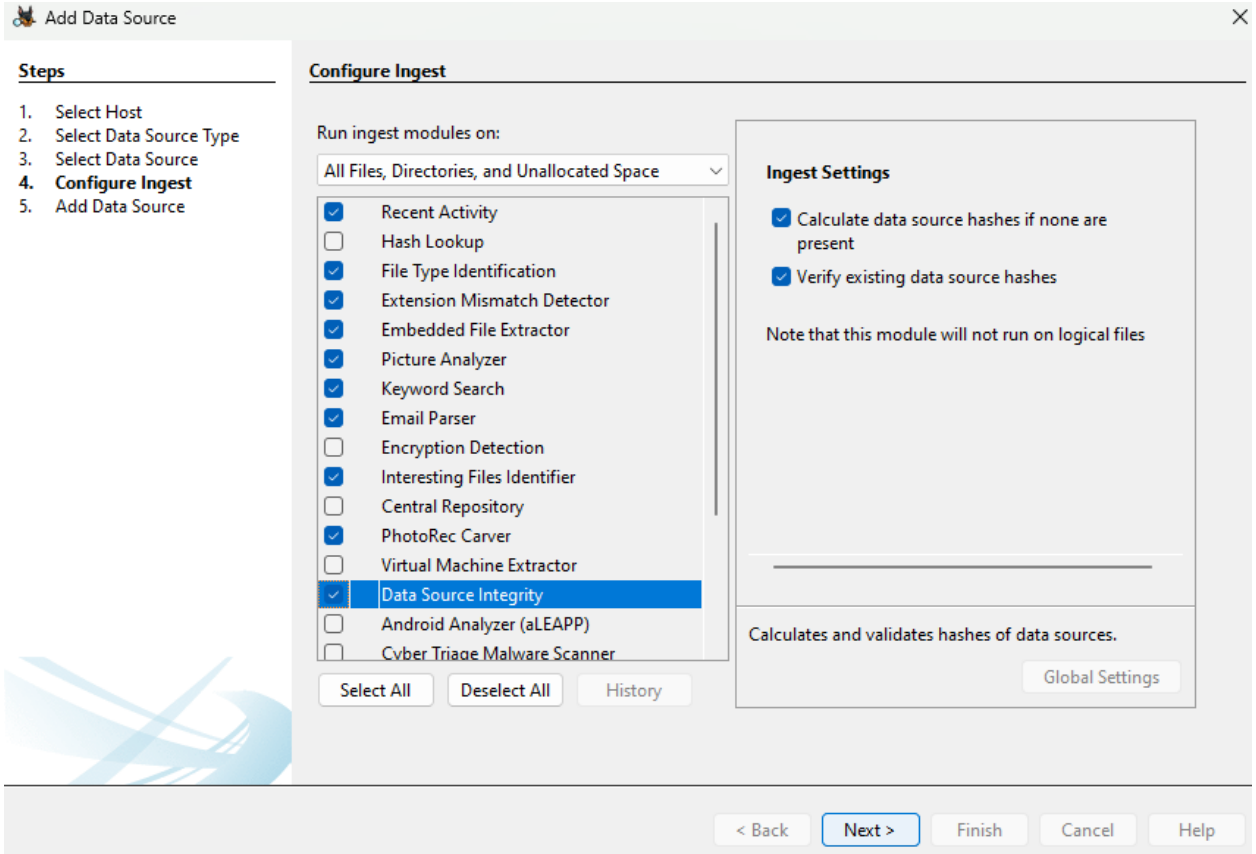
Selecting a Data Source:

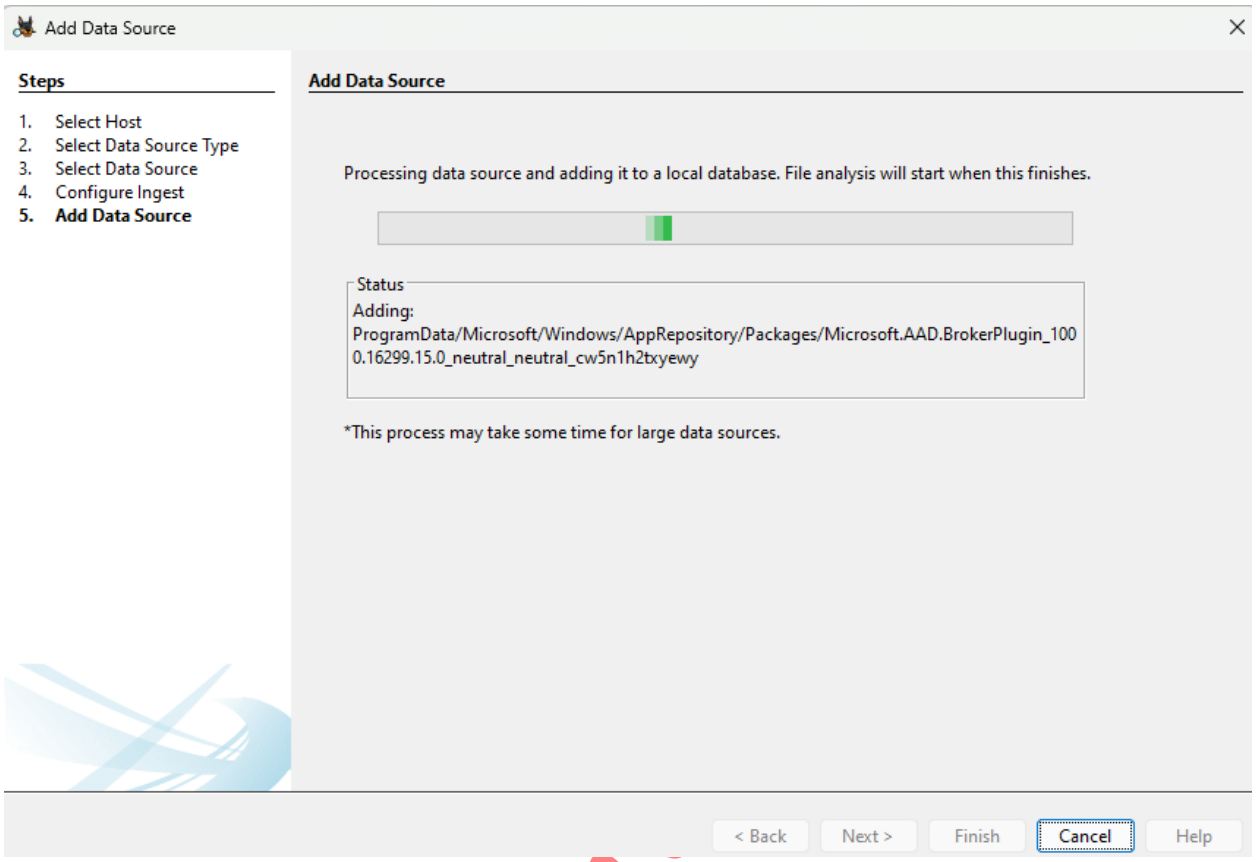
Providing a location where, Forensics Image resides



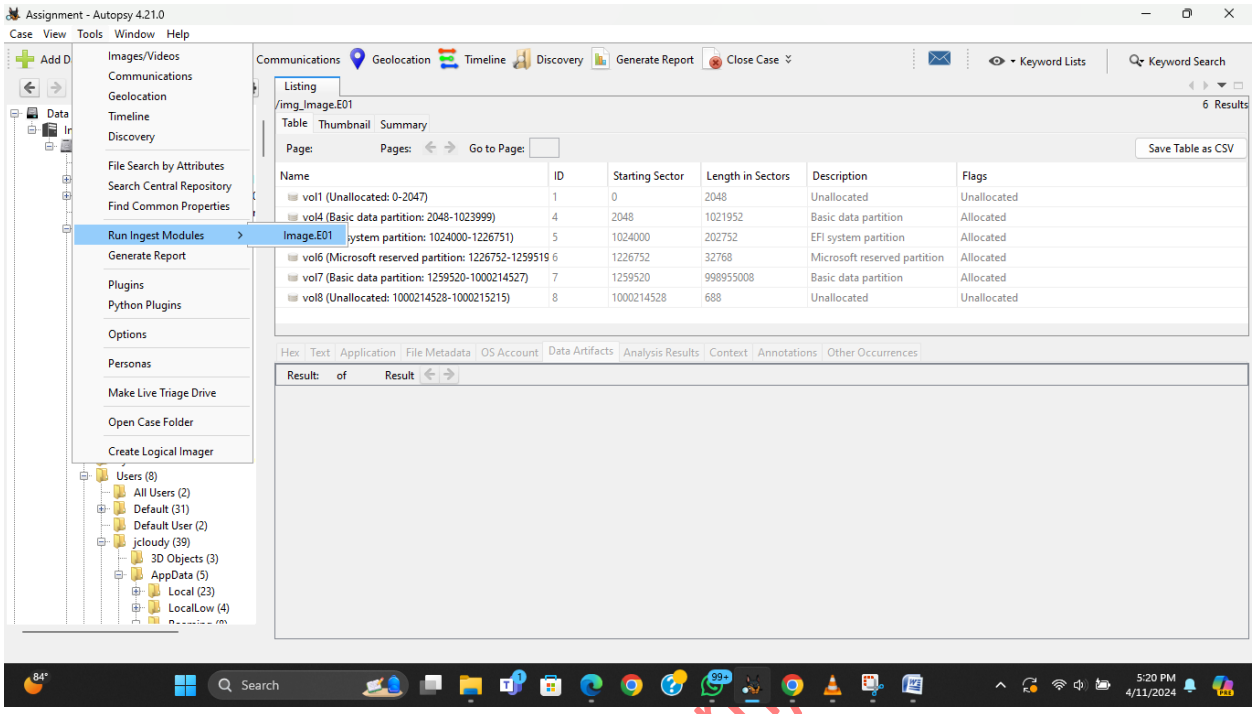


Configuring Ingest:



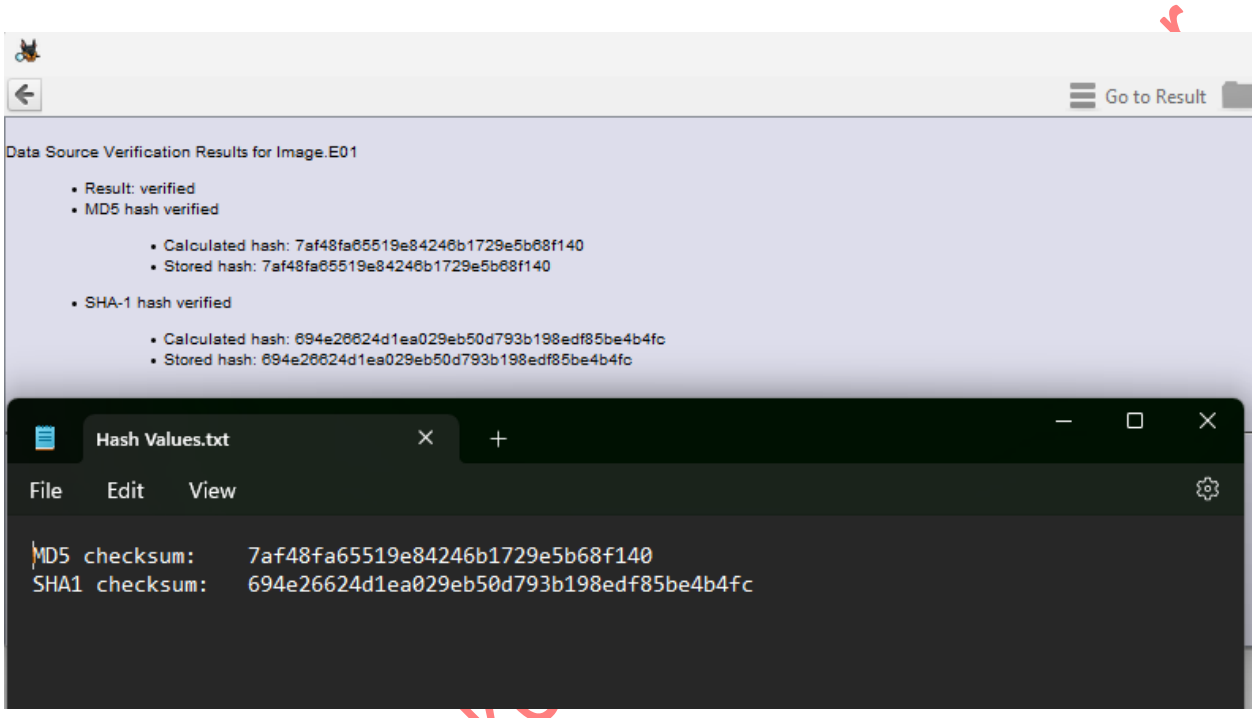


Checking the Data Source Integrity:



Comparing Hash Values:

By cross checking the hash value we want to know about the integrity of a file. If there is any changes in the original Image then integrity of a file will be compromised. Since both the provided and calculated hash is same in our case. So there is no issue with the integrity of the provided image that I am investigating.



Doing Partition Analysis:

Found 6 partitions, 2 are unallocated.

/img_Image.E01

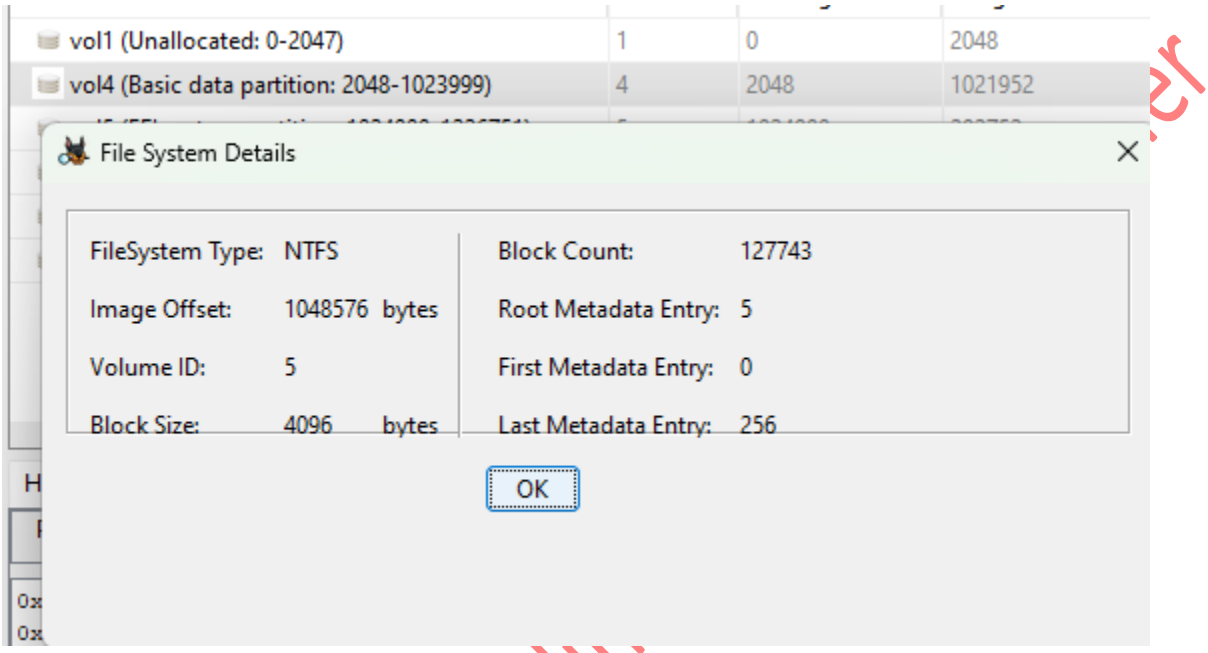
Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page:

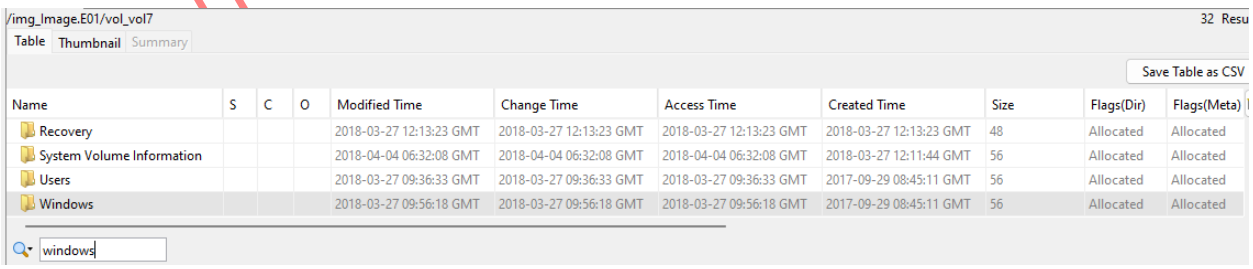
Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol4 (Basic data partition: 2048-1023999)	4	2048	1021952	Basic data partition	Allocated
vol5 (EFI system partition: 1024000-1226751)	5	1024000	202752	EFI system partition	Allocated
vol6 (Microsoft reserved partition: 1226752-1259519	6	1226752	32768	Microsoft reserved partition	Allocated
vol7 (Basic data partition: 1259520-1000214527)	7	1259520	998955008	Basic data partition	Allocated
vol8 (Unallocated: 1000214528-1000215215)	8	1000214528	688	Unallocated	Unallocated

File System Analysis:

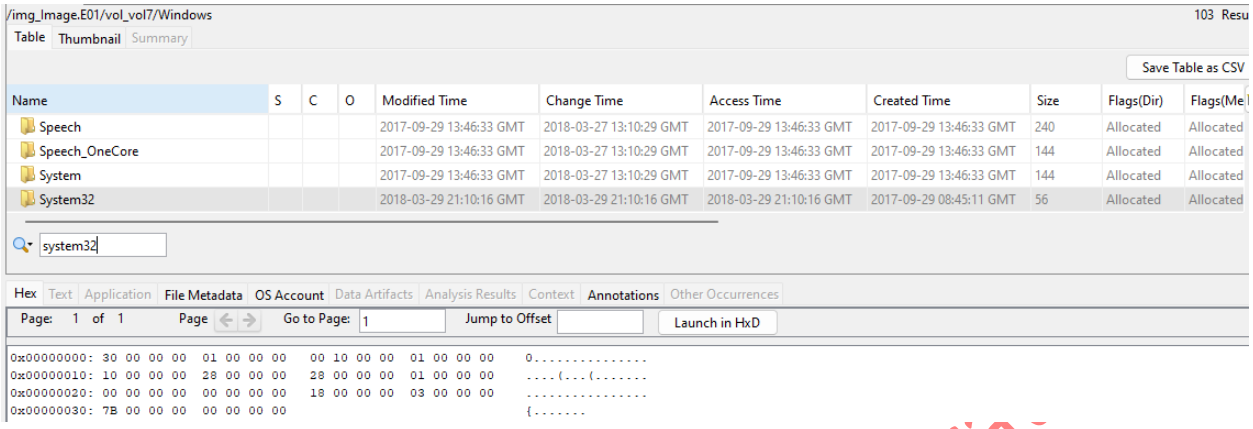
The partition type is NTFS here.



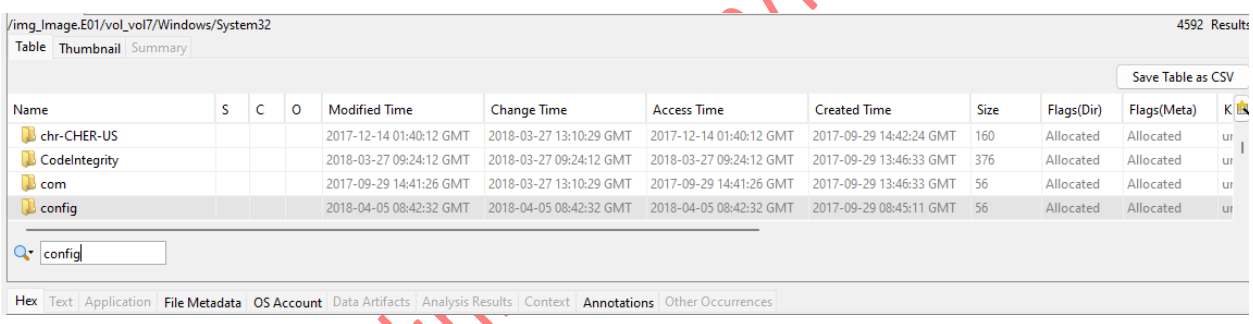
Searching for Windows folder



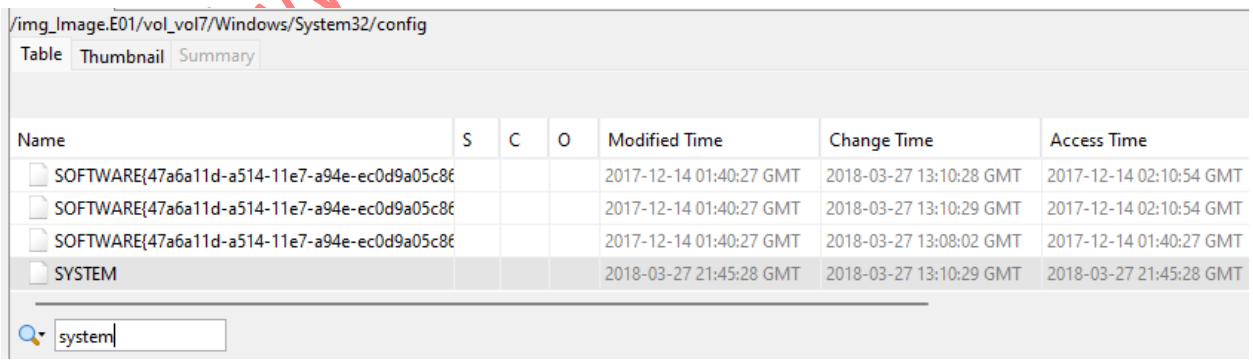
System32

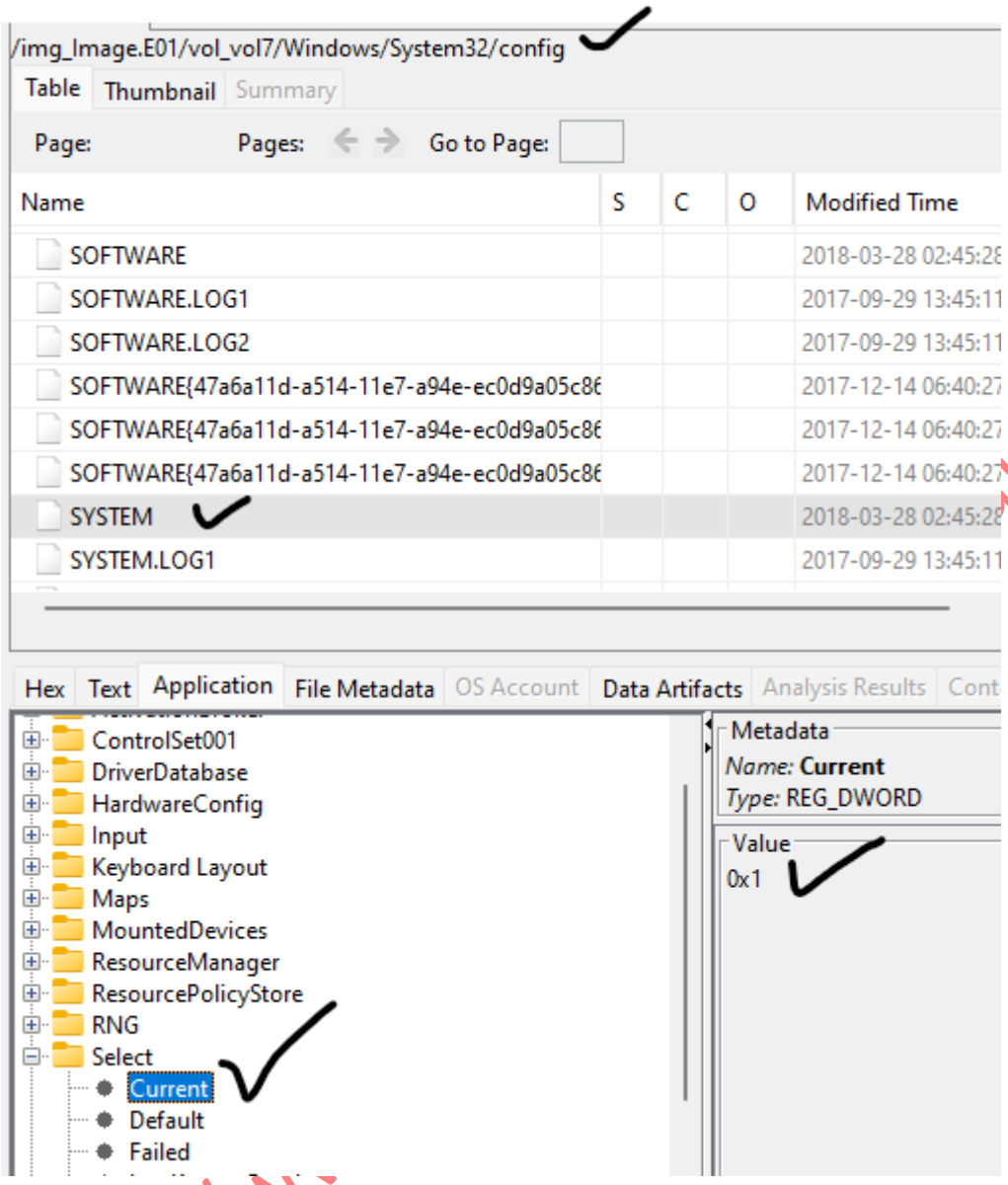


Searched for config folder



Inside Config searched for System File

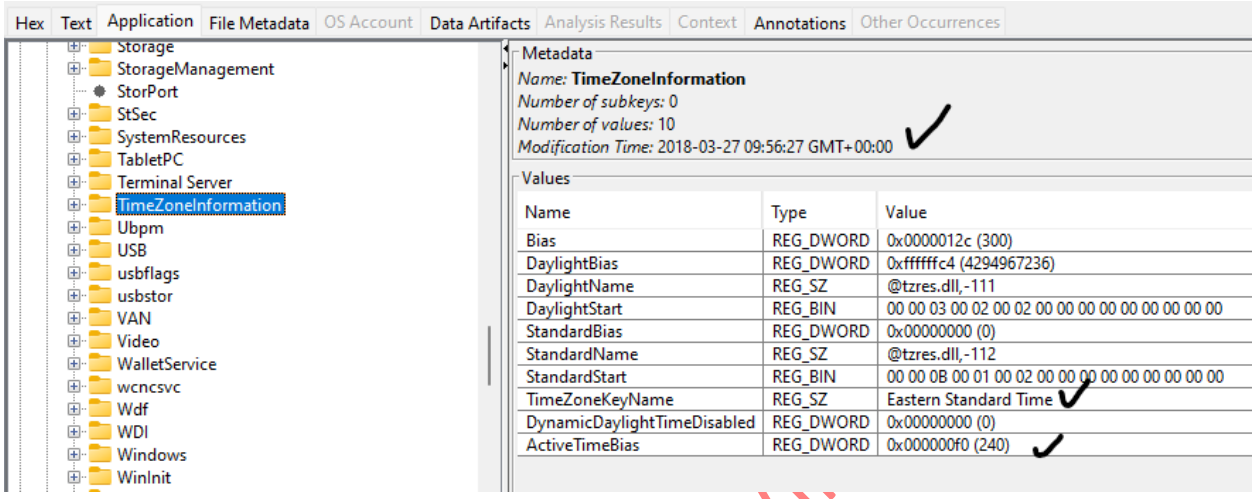




Got value 1 which means we are using control set 1.

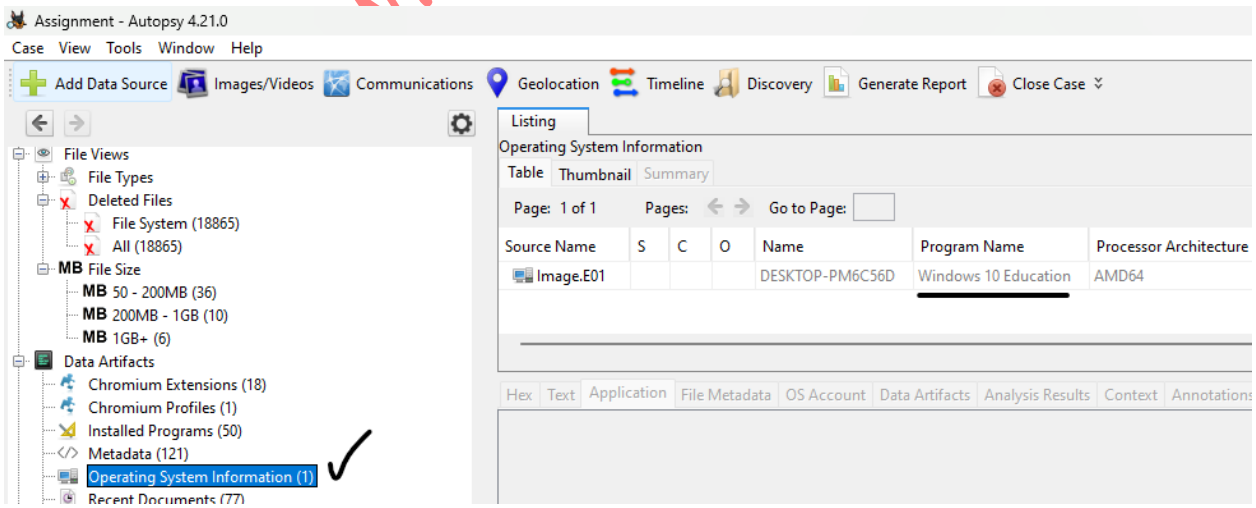
Now Clicking on ConrolSet001 to go to the Control and then clicking on TimeZoneInformation.

Now we can see the time zone information.



Operating System Information:

The user is using Windows 10 Education Version.



User information:

Under the OS Accounts found a user named Jcloudy

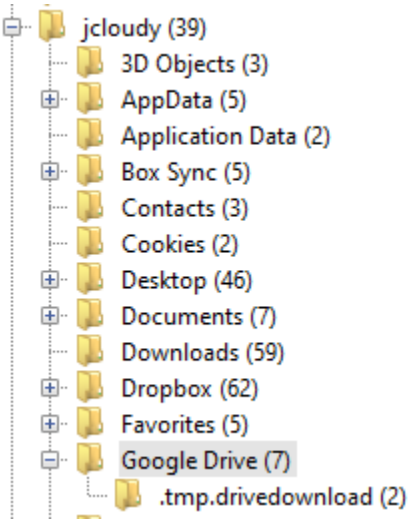
Listing

Table | Thumbnail | Summary

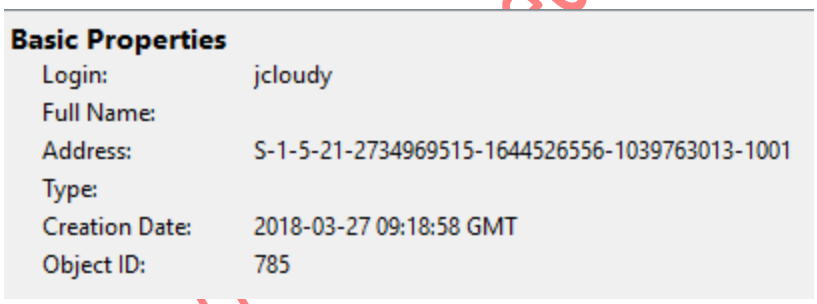
Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	Image.E0...	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-18532			0		Image.E0...	Local	NT SERVICE	
S-1-5-21-2734969515-1644526556-1039763013-1001			0	jcloudy	Image.E0...	Domain		2018-03-27 09:18:58 GMT
S-1-5-80-3028837079-3186095147-955107200-37019			0		Image.E0...	Local	NT SERVICE	
S-1-5-20				NETWORK SERVICE	Image.E0...	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	Image.E0...	Local	NT AUTHORITY	
S-1-5-21-397955417-626881126-188441444-4882392			0		Image.E0...	Domain		
S-1-5-21-2734969515-1644526556-1039763013-503			0	DefaultAccount	Image.E0...	Domain		2018-03-27 12:13:26 GMT
S-1-5-21-2734969515-1644526556-1039763013-500			0	Administrator	Image.E0...	Domain		2018-03-27 12:13:26 GMT
S-1-5-21-2734969515-1644526556-1039763013-501			0	Guest	Image.E0...	Domain		2018-03-27 12:13:26 GMT
S-1-5-21-2734969515-1644526556-1039763013-504			0	WDAGUtilityAccount	Image.E0...	Domain		2018-03-27 12:13:26 GMT

There are many users, e.g Jcloudy Local account, Administrator and Guest User. But there were no logins from these users. Some of the users that I found were Service Accounts having privileged access. Here I found an interesting user that have performed several logins and have utilized data and different programs. My main aim is to investigate the Jcloudy User because some of the accounts were disabled while other accounts don't have performed any activity.

Found A user named: Jcloudy



The account was normal user account, The account creation date and time is 2018-03-27 09:18:58 GMT.



Basic Properties

Login:	jcloudy
Full Name:	
Address:	S-1-5-21-2734969515-1644526556-1039763013-1001
Type:	
Creation Date:	2018-03-27 09:18:58 GMT
Object ID:	785

The password settings were set to Password does not expire and the This was normal User account.

Password Settings:	Password does not expire, Password not required
Flag:	Normal user account
Home Directory:	C:/Users/jcloudy

The user last logged in to his account on 2018-04-06 and the user home directory is under C:/Users/jcloudy.

Findings:

Analyzing f_0016a6 word document:

Found 136 results in Metadata. Containing different MS Word documents and Excel sheets.

Metadata 136 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Date Modified	Program Name	Date Created	User ID	Owner
f_0016a6				2018-04-03 23:59:00 GMT	Microsoft Office Word	2018-03-29 21:29:00 GMT	jcloudy	jcloudy
rootkey((Autosaved-306579222169168469)).xlsb				2018-04-06 07:37:32 GMT	Microsoft Excel		jcloudy	
~ar2499.xar				2018-04-06 07:37:32 GMT	Microsoft Excel		jcloudy	
TM01840907[[fn=Equations]].dotx				2011-03-17 14:58:00 GMT	Microsoft Office Word			
TM02835233[[fn=Text Sidebar (Annual Report Red a				2012-03-05 15:27:00 GMT	Microsoft Office Word			
TM03998158[[fn=Element]].dotx				2013-01-11 17:17:00 GMT				
TM03998159[[fn=Insight]].dotx				2013-01-11 17:14:00 GMT				
Normal.dotm				2018-04-04 00:30:00 GMT	Microsoft Office Word	2018-03-29 21:15:00 GMT	jcloudy	jcloudy

Analyzing the first one named f_0016a6 and extracting text.

Listing

Metadata 136 Result

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Date Modified	Program Name	Date Created	User ID	Owner
f_0016a6				2018-04-03 23:59:00 GMT	Microsoft Office Word	2018-03-29 21:29:00 GMT	jcloudy	jcloudy
rootkey((Autosaved-306579222169168469)).xlsb				2018-04-06 07:37:32 GMT	Microsoft Excel		jcloudy	
~ar2499.xar				2018-04-06 07:37:32 GMT	Microsoft Excel		jcloudy	
TM01840907[[fn=Equations]].dotx				2011-03-17 14:58:00 GMT	Microsoft Office Word			
TM02835233[[fn=Text Sidebar (Annual Report Red a				2012-03-05 15:27:00 GMT	Microsoft Office Word			
TM03998158[[fn=Element]].dotx				2013-01-11 17:17:00 GMT				
TM03998159[[fn=Insight]].dotx				2013-01-11 17:14:00 GMT				
Normal.dotm				2018-04-04 00:30:00 GMT	Microsoft Office Word	2018-03-29 21:15:00 GMT	jcloudy	jcloudy

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

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

AIRPORT INFORMATION
Ronald Reagan has best record of on-time departures.
Dulles has flights to Indonesia. With Layover in Qatar.

22 min from Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 to Dulles Airport.

Aw we can see that, this information is found from by analyzing the mentioned document.

AIRPORT INFORMATION
Ronald Reagan has best record of on-time departures.
Dulles has flights to Indonesia. With Layover in Qatar.

22 min from Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 to Dulles Airport.

Analyzing word File found at Jcloudy User Desktop:

An interesting File Found named Planning.docx

Listing

/img_Image.E01/vol_vol7/Users/jcloudy/Desktop 46 Resu

Table Thumbnail Summary

Page: Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
LeftUsesBoycotts.pdf				2018-04-06 03:56:37 GMT	2018-04-06 03:56:43 GMT	2018-04-06 03:56:33 GMT	2018-04-06 03:56:31
MyTiredHead.jpg				2018-03-30 03:31:11 GMT	2018-04-02 01:12:46 GMT	2018-03-30 03:30:58 GMT	2018-03-30 03:31:10
MyTiredHead.jpg:Zone.Identifier				2018-03-30 03:31:11 GMT	2018-04-02 01:12:46 GMT	2018-03-30 03:30:58 GMT	2018-03-30 03:31:10
Operation 2nd Hand Smoke.pptx				2018-04-04 05:11:27 GMT	2018-04-04 05:11:53 GMT	2018-04-04 05:11:27 GMT	2018-04-04 04:56:19
Planning.docx				2018-04-04 05:30:41 GMT	2018-04-04 05:30:49 GMT	2018-04-04 05:30:41 GMT	2018-03-30 02:16:48
RedGuns.jpg				2018-03-31 04:16:59 GMT	2018-04-02 01:12:46 GMT	2018-03-31 04:16:48 GMT	2018-03-31 04:16:59
RedGuns.jpg:Zone.Identifier				2018-03-31 04:16:59 GMT	2018-04-02 01:12:46 GMT	2018-03-31 04:16:48 GMT	2018-03-31 04:16:59
SelfDefenseisMurder.pdf				2018-04-05 05:48:42 GMT	2018-04-05 05:48:52 GMT	2018-04-05 05:48:41 GMT	2018-04-05 05:48:40

Analyzing Jcloudy's Desktop Data:

Found some interesting Files at Jcloudy's Desktop.

Listing

img_Image.E01/vol_vol7/Users/jcloudy/Desktop 46 Result

Table Thumbnail Summary

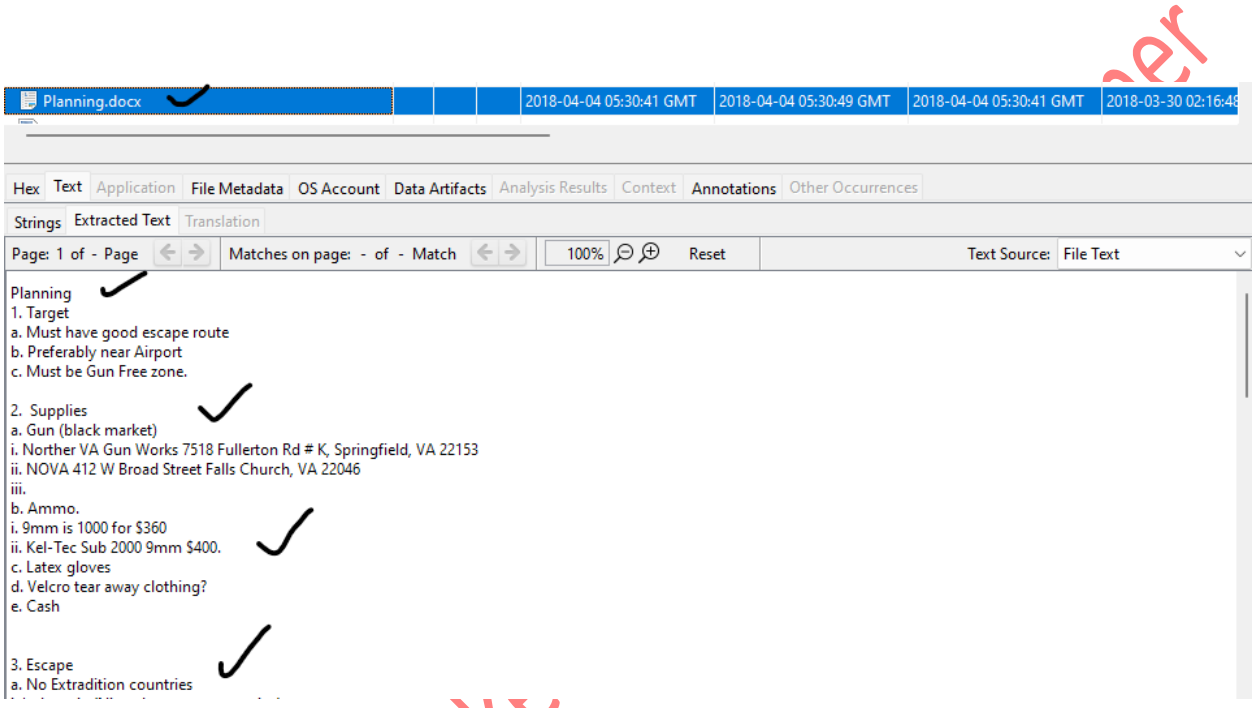
Page: Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Operation 2nd Hand Smoke.pptx				2018-04-04 05:11:27 GMT	2018-04-04 05:11:53 GMT	2018-04-04 05:11:27 GMT	2018-04-04 04:56:19
Planning.docx				2018-04-04 05:30:41 GMT	2018-04-04 05:30:49 GMT	2018-04-04 05:30:41 GMT	2018-03-30 02:16:48
RedGuns.jpg				2018-03-31 04:16:59 GMT	2018-04-02 01:12:46 GMT	2018-03-31 04:16:48 GMT	2018-03-31 04:16:59
RedGuns.jpg:Zone.Identifier				2018-03-31 04:16:59 GMT	2018-04-02 01:12:46 GMT	2018-03-31 04:16:48 GMT	2018-03-31 04:16:59
SelfDefenseisMurder.pdf				2018-04-05 05:48:42 GMT	2018-04-05 05:48:52 GMT	2018-04-05 05:48:41 GMT	2018-04-05 05:48:40
Sheep.jpg				2018-03-30 03:32:40 GMT	2018-04-02 01:12:46 GMT	2018-03-30 03:32:34 GMT	2018-03-30 03:32:40
Sheep.jpg:Zone.Identifier				2018-03-30 03:32:40 GMT	2018-04-02 01:12:46 GMT	2018-03-30 03:32:34 GMT	2018-03-30 03:32:40
The Cloudy Manifesto.docx				2018-04-02 01:35:27 GMT	2018-04-02 01:35:39 GMT	2018-04-02 01:35:27 GMT	2018-04-02 01:35:27
UKknifeBan.pdf				2018-04-05 05:51:45 GMT	2018-04-05 05:51:54 GMT	2018-04-05 05:51:42 GMT	2018-04-05 05:51:41

Planning.docx, RedGuns.jpg, SelfDefenseMurder.pdf etc Lets Analyze it.

Analyzing Planning.docx

He is planning some a murder. During analysis of this document I came into conclusion that he is planning to do some type of murder.

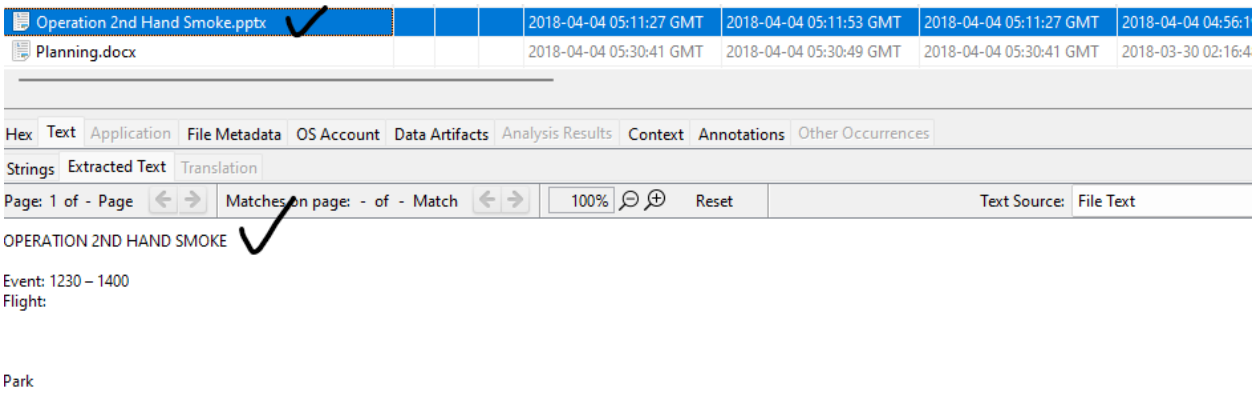


3. Escape
a. No Extradition countries
i. Indonesia (Nicer, but more expensive)
ii. Vietnam
iii. Can live very well on 100 a day, for 9 years.
b. Buy tickets for same day
c. Preferable direct flight
d. Have suitcase in car.

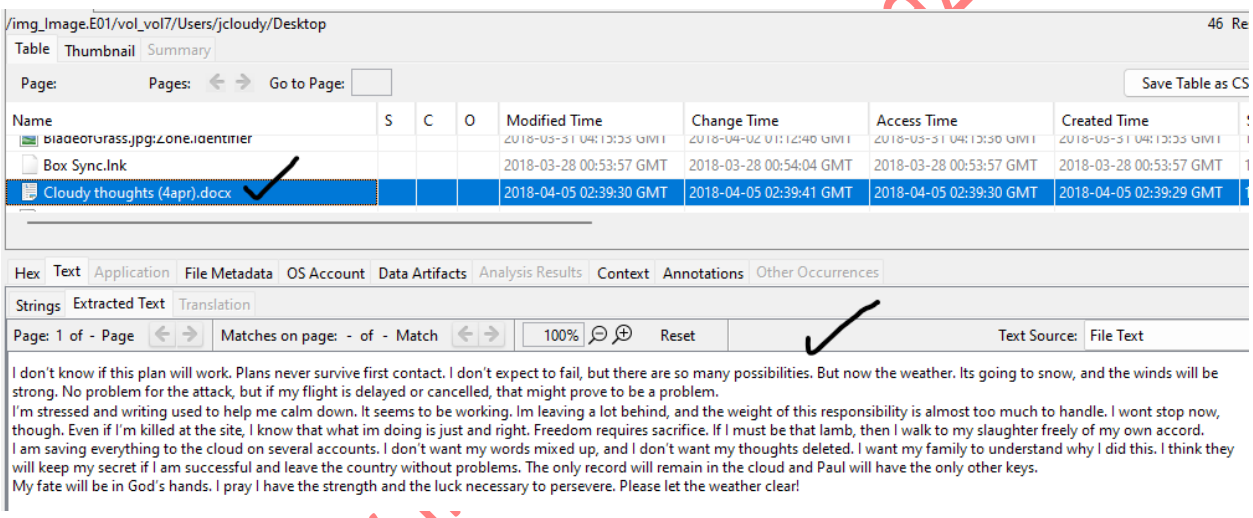
4. Release
a. Start writing ideas and thoughts
b. Save to separate locations for redundancy
c. Place it in the cloud for remote access
d. "Press Release" once home free.

Yes I got it that's why he was searching for the Airport and roundtrip.

He have given a name to his operation 2nd Hand SMOKE



Analyzing Cloudy thoughts.docx file



Analyzing The 1st Excel File:

Metadata 136 Resu

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Date Modified	Program Name	Date Created	User ID	Owner
f_0016a6				2018-04-03 23:59:00 GMT	Microsoft Office Word	2018-03-29 21:29:00 GMT	jcloudy	jcloudy
rootkey((Autosaved-306579222169168469)).xlsb				2018-04-06 07:37:32 GMT	Microsoft Excel		jcloudy	
~ar2499.xar				2018-04-06 07:37:32 GMT	Microsoft Excel		jcloudy	
TM01840907[[fn=Equations]].dotx				2011-03-17 14:58:00 GMT	Microsoft Office Word			
TM02835233[[fn=Text Sidebar (Annual Report Red a				2012-03-05 15:27:00 GMT	Microsoft Office Word			

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 1 Result Metadata

Type	Value	Source(s)
User ID	jcloudy	org.sleuthkit.autopsy.key
Date Modified	2018-04-06 07:37:32 GMT	org.sleuthkit.autopsy.key
Program Name	Microsoft Excel	org.sleuthkit.autopsy.key
Source File Path	/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Roaming/Microsoft/Excel/rootkey306579560141686273/rootkey((Autosaved-306579222169168469)).xlsb	
Artifact ID	-9223372036854755318	

During Analysis of Excel File I found

/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Roaming/Microsoft/Excel/rootkey306579560141686273 4 Resu

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	560	Allocated
[parent folder]				2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:27:07 GMT	392	Allocated
rootkey((Autosaved-306579222169168469)).xlsb				2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	8966	Allocated
rootkey.csv.lnk				2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	2018-04-06 12:37:32 GMT	618	Allocated

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

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

```
rootkey
        AWSAccessKeyId=AKIAJQCL74OG6U6JRXKQ
        AWSSecretKey=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



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

Application-Name: Microsoft Excel
Application-Version: 16.0300
Content-Type: application/vnd.ms-excel.sheet.binary.macroenabled.12
Last-Author: jcloudy
Last-Modified: 2018-04-06T12:37:32Z
Last-Save-Date: 2018-04-06T12:37:32Z
```

AWS Secret key and AWS Key Id Found:

```
rootkey
        AWSAccessKeyId=AKIAJQCL74OG6U6JRXKQ
        AWSSecretKey=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
```

Analyzing Internet Activity:

One Chrome User Account found

Listing

Chromium Profiles

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Source Name	S	C	O	Path	User ID	Domain	Short Cut	Name	Username	Program Name	Data Source
Local State				Default	111256729592432613619			Person 1	jimcloudy1@gmail.com	Google Chrome	Image.E01

Airport Information .docx found image1.png file. I have discussed about this in the finding section of this document.