Digital Forensics and Investigation:

Digital Corpora 2018 Lone Wolf Scenario

Solved By:

Khubab Ahmed and Muhammad Saim

Table of Contents

1. Introduction

The 2018 Lone Wolf scenario presents a fictional case involving the seizure of a laptop from an individual suspected of planning a mass shooting. The case was initiated when the suspect's brother alerted the police about his increasingly concerning behavior. Following this alert, the police seized the suspect's laptop, which was subsequently imaged using the FTK Imager program.

For this project, we were provided with a single image from the laptop. Our task is to conduct a forensic examination and produce an expert witness report. Throughout this process, we must document any suspicious findings, detail the methodology employed, and list all the tools utilized. The documentation must also adhere to the guidelines provided in the Expert Evidence, along with any supplementary documents provided for the scenario.

2. Case Managment

2.1 Chain of Custody

The first people in this chain of custody are the people who collected the machine/system from the crime scene. Which would be Tom Moore. Those investigators created an image so that the original machine doesn't go through any irreversible change. This image is further used by different investigators.

After that the person to receive the image would be us Khubab Ahmed & Muhammad Saim making me the second person to interact with this image/machine. The examination/work performed by me on the image is present down below but firstly we confirm that the image wasn't tampered during its movement from Tom Moore to me.

Acquisition details and current examiner details are given below:

	Acquisition Details	Current Examiner Details
Description	Lone Wolf Scenario	Lone Wolf Scenario
Examiner Name	Tom Moore	Khubab Ahmed & Muhammad Saim

Acquired Date	Fri Apr 6 12:50:44 2018	Mon June 3 0:00 2024
System Date	Fri Apr 6 12:50:44 2018	Fri Apr 6 12:50:44 2018
Acquiry Operating System	Win 201x	Win 201x
Acquiry Software Version	ADI3.1.1.8	ADI3.1.1.8

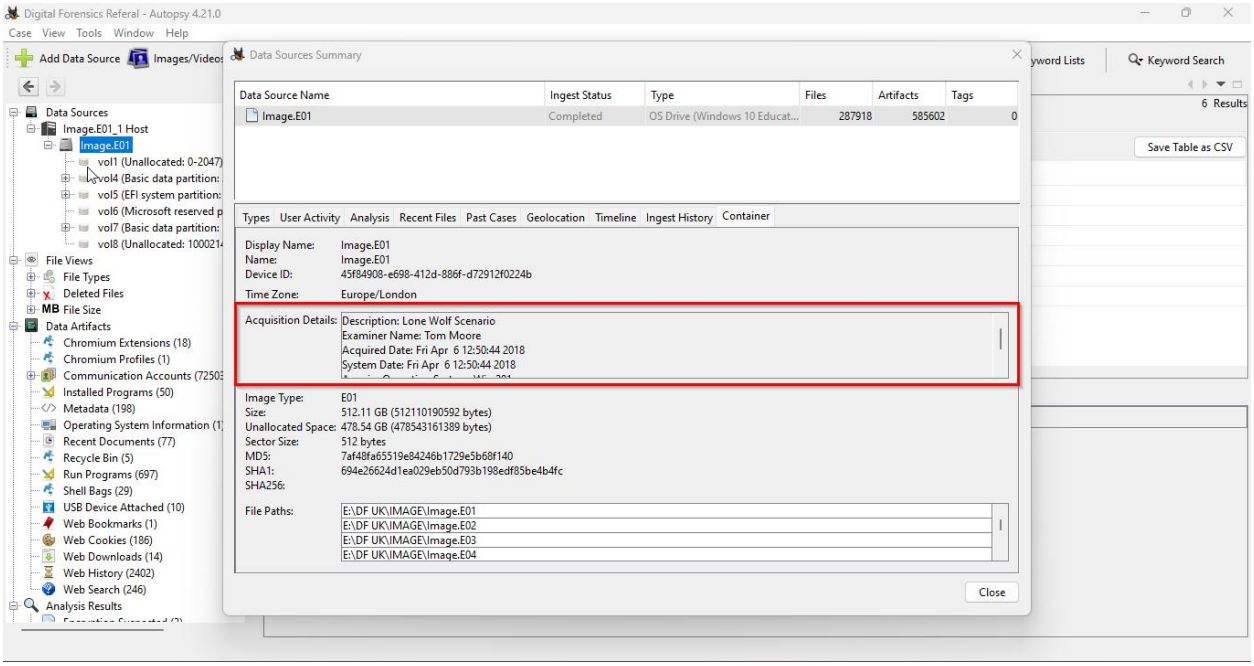

Figure 1 Acquisition Details

[SPACE INTENTIONALLYLEFTBLANK]

2.2 Verifying an Evidence

Verifying Evidence is important as the image received by us must be the same as the image formed by the investigator. This is an integrity check to ensure we don't work with an altered image.

To verify the images, we compared both hashes of original image hash and copy image hash. Both images are the same.

	MD5	SHA1
Original Image Hash	7af48fa65519e84246b1729e5b68f140	694e26624d1ea029eb50d793b198edf85be4b4fc
Copying Image hash	7af48fa65519e84246b1729e5b68f140	694e26624d1ea029eb50d793b198edf85be4b4fc

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Right Click to View Summary Information --> Select Container tab

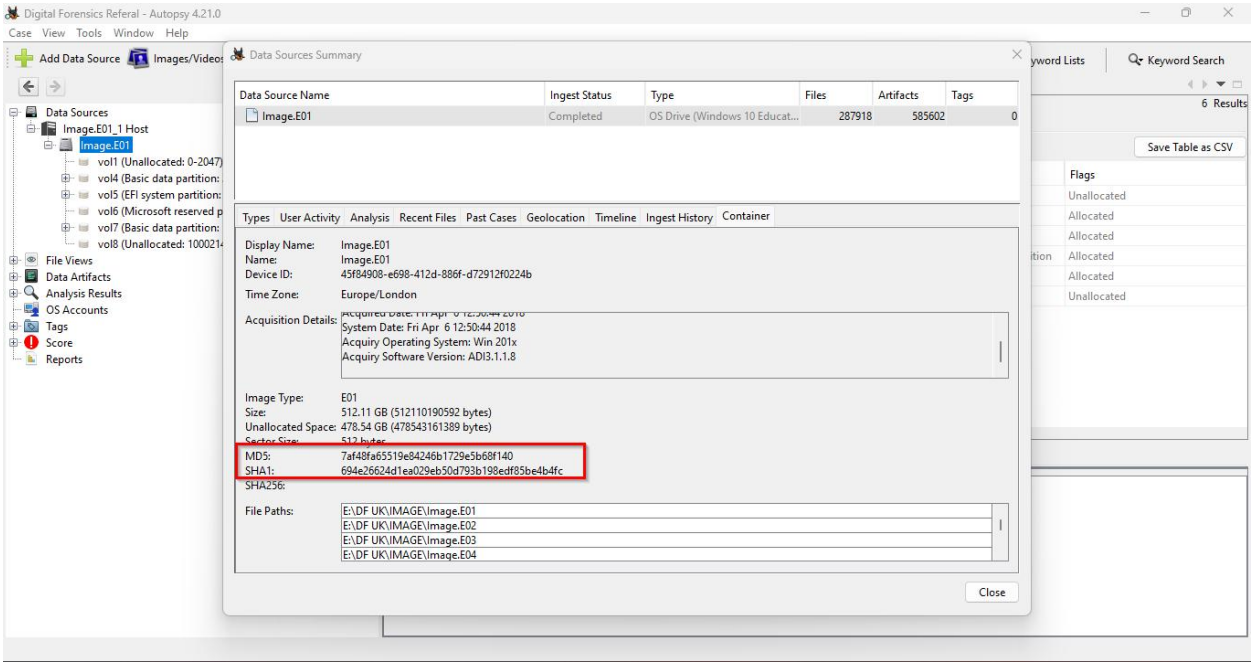

Figure 2 Hashes of Image

2.3 Tools Used

The tools used are autopsy and registry viewer.

2.3.1 Autopsy

Autopsy is a comprehensive digital forensic tool that offers a wide range of features for acquiring, analyzing, and reporting on digital evidence. Its user-friendly interface and extensibility make it a popular choice among forensic examiners and investigators worldwide.

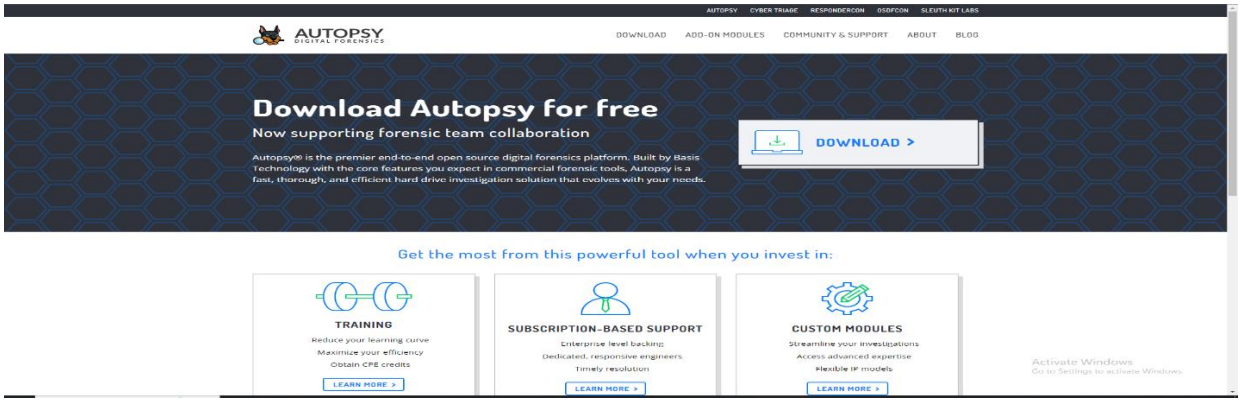

Figure 3 Autopsy

2.3.2 Registry Viewer

A registry viewer is a versatile tool that provides insights into the configuration and behavior of Windows systems, making it invaluable for system administrators, digital forensic analysts, and security professionals.

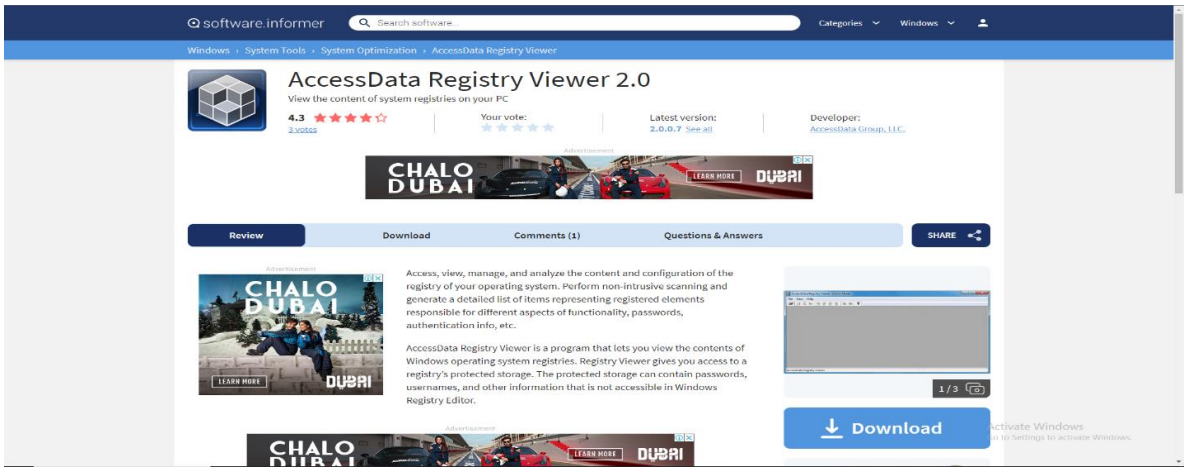

Figure 4 Registry Viewer

3. Basic Image Analysis

3.1 Partition Information:

Partition contains a lot of information which is needed in the analysis. It can tell us about any hidden or deleted partitions. Users can hide or delete malicious stuff from the partitions or keep a separate partition for malicious activity. This is the analysis of the partitions provided.

Volume	ID	Bootable	Starting Sector	Length in Sector	Size	Description	Flag
vol1	1	No	0	2048		Unallocated	Unallocated
vol4	4	No	2048	1021952		Basic Data Partition	Allocated
vol5	5	No	1024000	202752		EFI system Partition	Allocated
vol6	6	No	1556752	32768		Microsoft reserved Partition	Allocated
vol7	7	Yes	1259520	998955008		Basic data partition	Allocated
vol8	8	No	1000214528	688		Unallocated	Unallocated

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the volume --> Right Click on Properties to View Information

Note: The remaining information like Size is calculated and Bootable information is view by the volume contents.

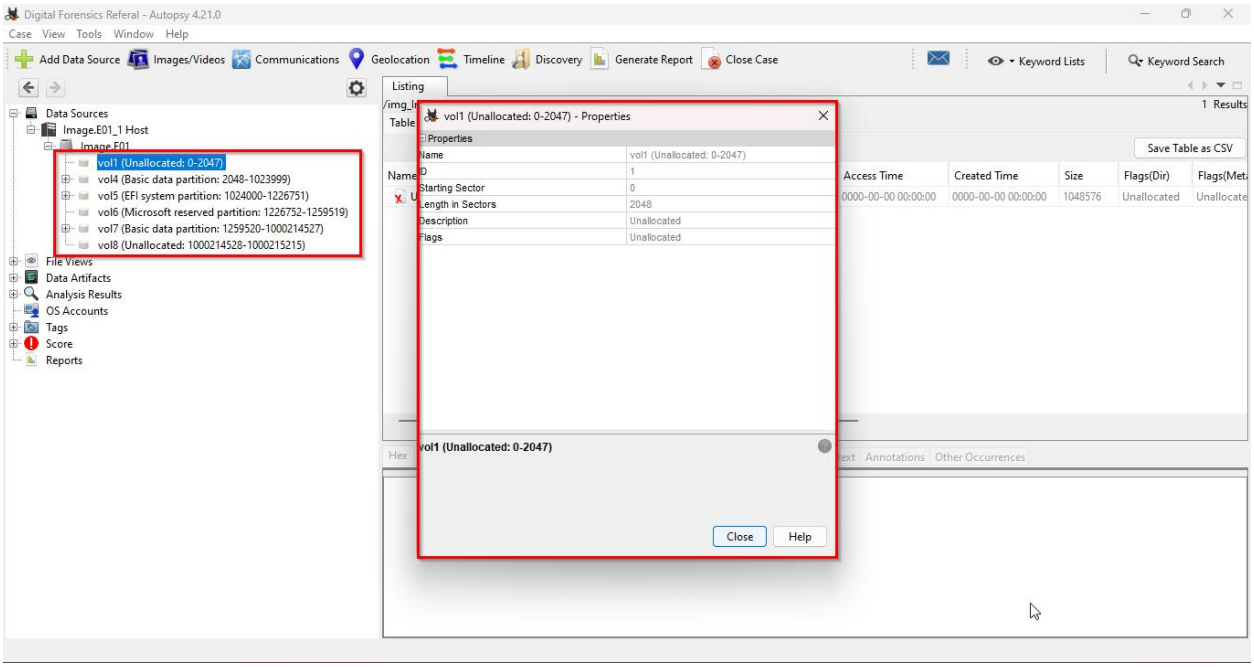

Figure 5 Partition Information

[SPACE INTENTIONALLY LEFT BLANK]

3.2 Filing System:

Below are the partitions which were allocated by the users. The rest of the partitions were unallocated by the user. Basic Data Partition is the standard partition for storing system and user data while EFI system Partition is used by systems with Unified Extensible Firmware Interface.

vol4	NTFS
vol5	FAT32
vol7	NTFS

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the volume --> Right Click and Select File System Details

Note: The remaining partitions are unallocated.

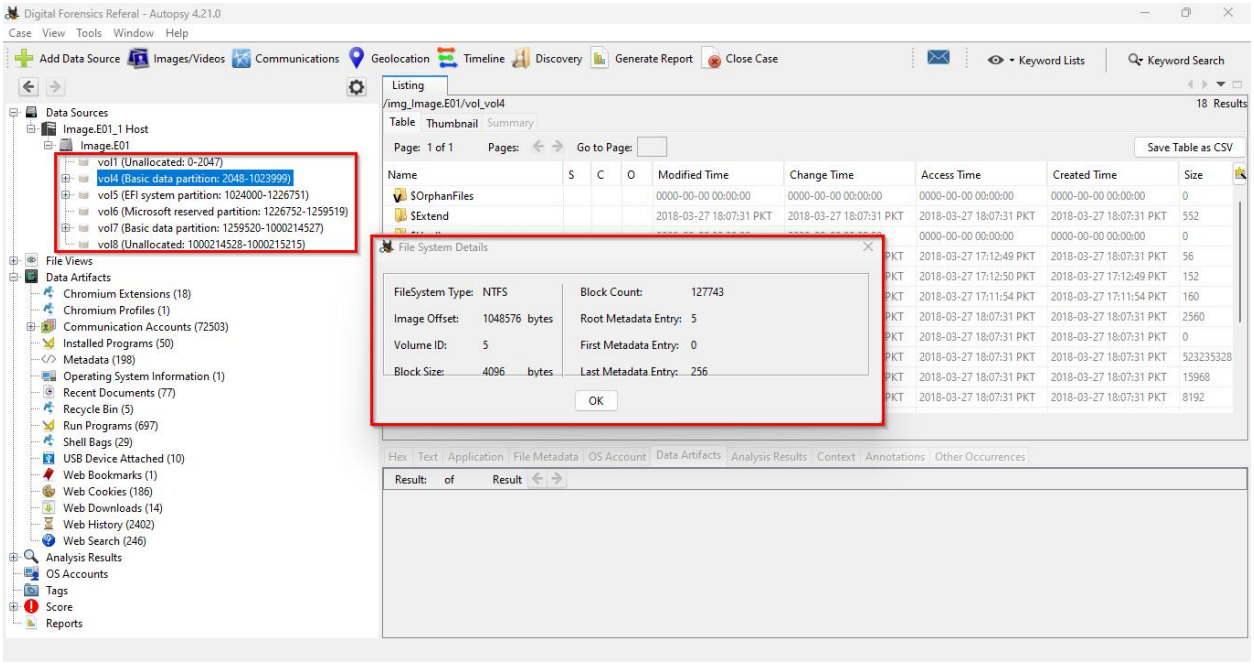

Figure 6 Filing System

3.3 Mounted Devices:

Mounted devices refer to hardware devices connected and recognized by the system. It tells us about the device usage of the user. We can identify what devices the user used. Here we can see that a device assigned device letter C, D and E was connected and Volume without name suggest no name was assigned to these devices

Devices Connected	Letters
DosDevices - C:	C
DosDevices - D:	D
DosDevices - E:	E
?? - Volume{5c3108bb-31c0-11e8-9b10-806e6f6e6963}	Not Assigned
?? - Volume{3869c27a-31b8-11e8-9b12-ecf4bb487fed	Not Assigned

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SOFTWARE registry file.

Open it on Registry Viewer tool --> SOFTWARE --> MountedDevices

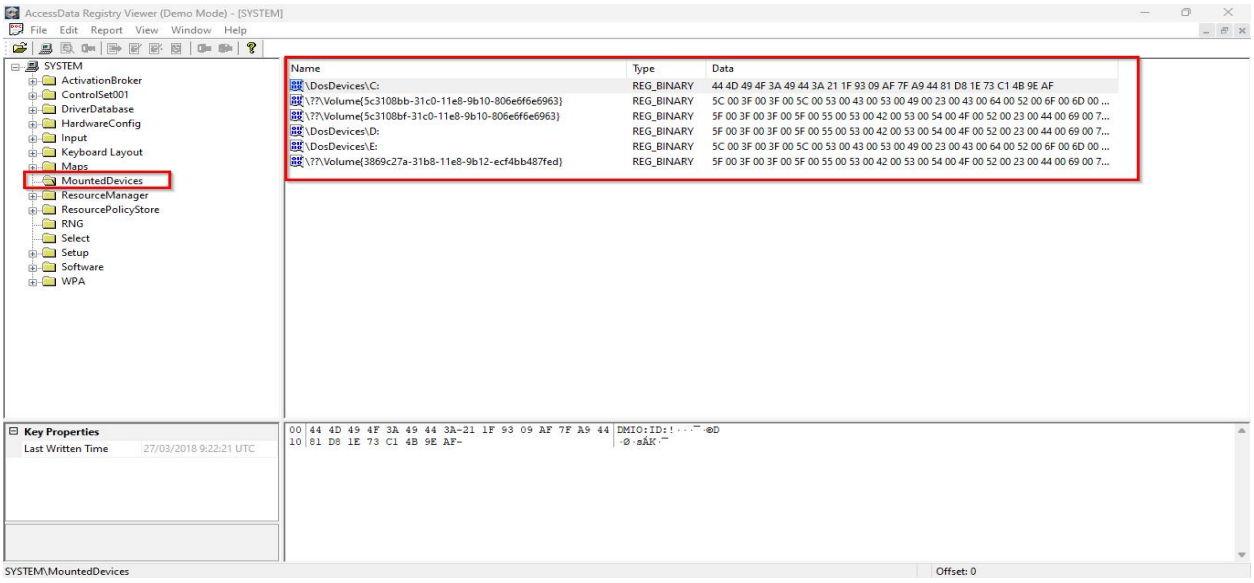

Figure 7 Mounted Devices

3.4 Operating System Information:

OS information is one of the most crucial pieces of information we can find. It tells us about the registration time and registration user of the OS. Assuming it isn't pirated and is licensed.

Product Name	Windows 10 Education
Version	6.3
Edition ID	Education
Current Build	16299
Current Type	Multiprocessor Free
Release ID	1709
Product ID	00328-00089-23637-AA141
Registered Owner	Windows User
System Path	C:¥Windows
OS Install Date (UTC)	Tue Mar 27 12:13:27 2018
Installation Type	Client

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SOFTWARE registry file.

Open it on Registry Viewer tool --> SOFTWARE --> Microsoft --> Select Windows NT --> Current Version

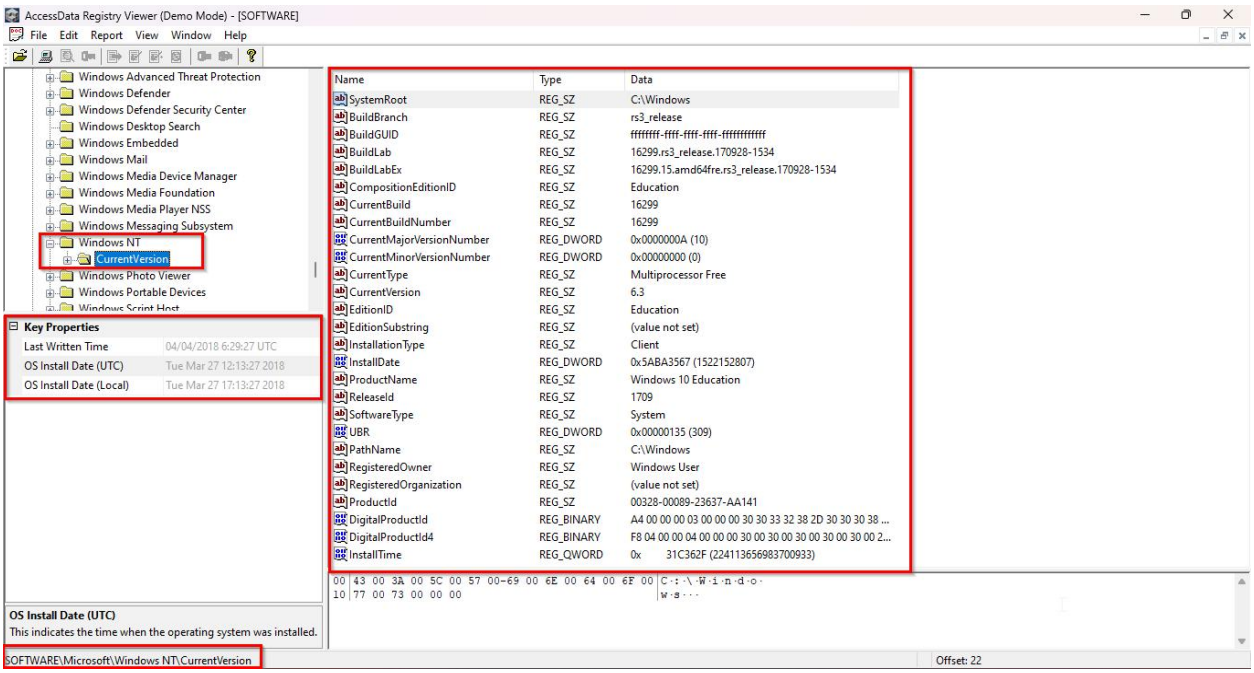

Figure 8 Operating System Information

[SPACE INTENTIONALLY LEFT BLANK]

3.5 System Time Zone:

Time zones information can be used to geolocate the system and can be further used in timeline reconstruction later in documentation.

Time Zone	Eastern Standard Time
Standard Start Date	First Sun in Nov at 2:00:00 am Local
Daylight Start Date	Second Sun in Mar at 2:00:00 am Local
Standard Bias	0
Daylight Bias	-60

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SYSTEM registry file.

Open it on Registry Viewer tool --> SYSTEM --> ControlSet001 --> Control --> TimeZoneInformation

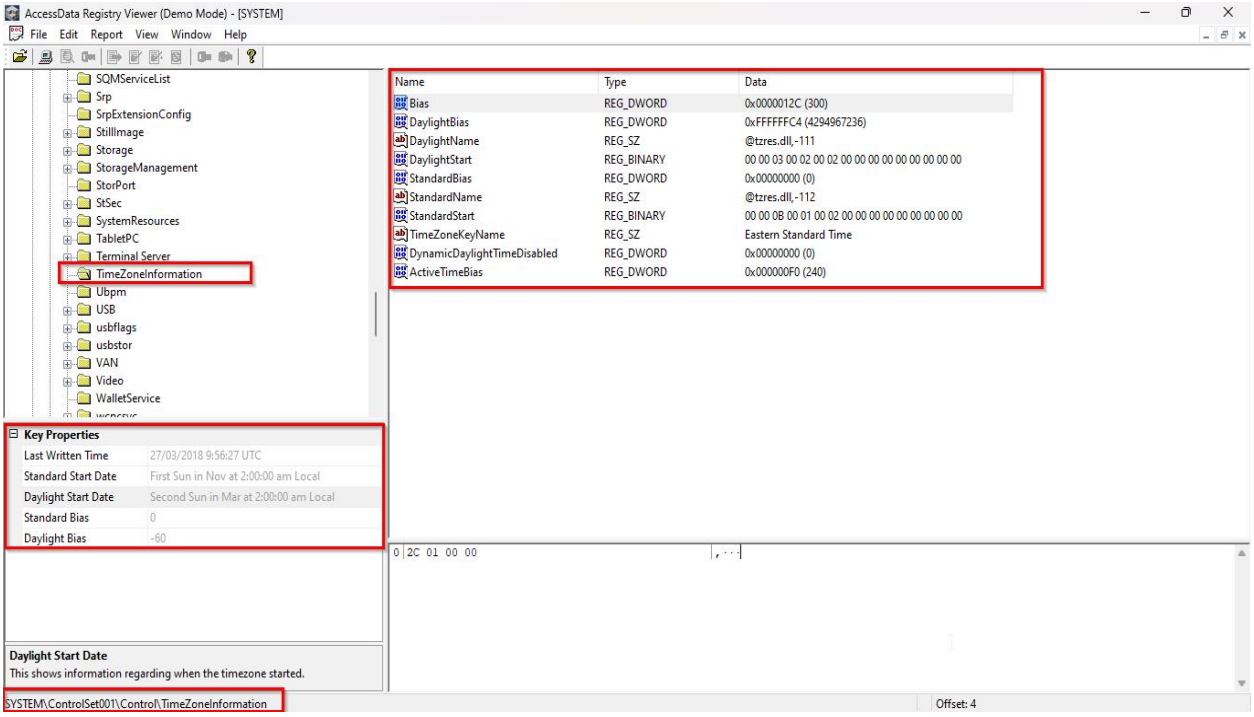

Figure 9 System Time Zone

3.6 Computer's Name:

Unique identifier of a user. It is also customizable by the user, or it is also present by default.

Computer Name	DESKTOP-PM6C56D

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SYSTEM registry file.

Open it on Registry Viewer tool --> SYSTEM --> ControlSet001 --> Control --> ComputerName --> ComputerName

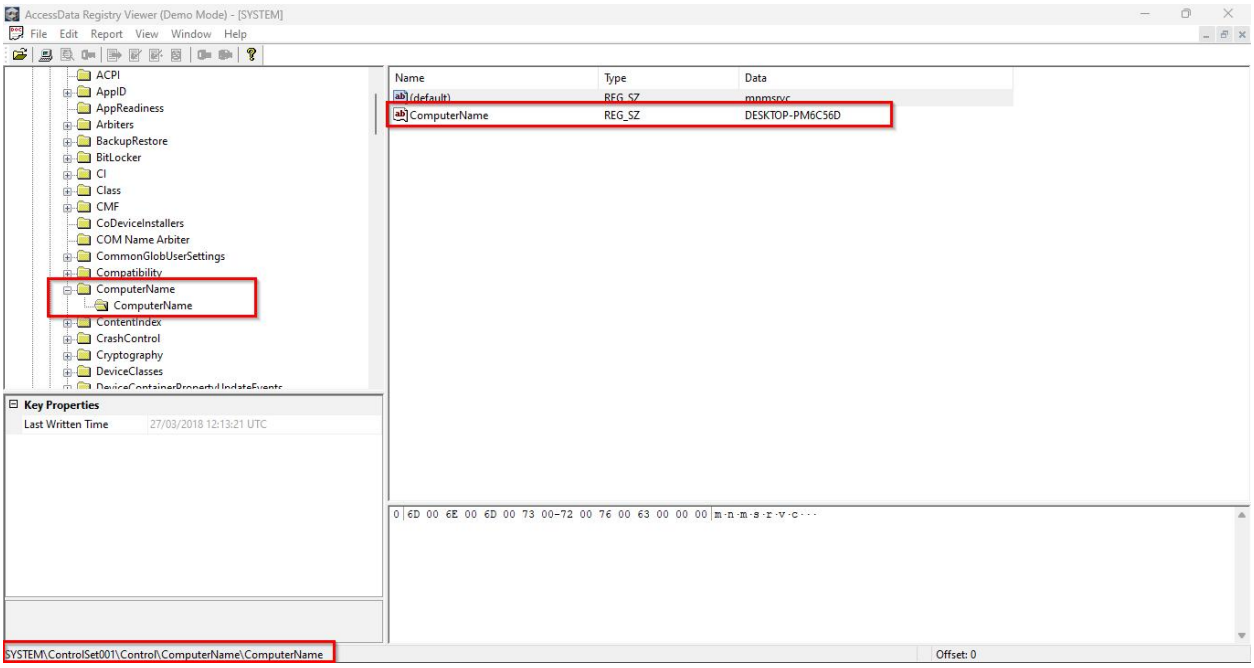

Figure 10 Computer Name

3.7 OS Accounts:

Refers to the users present on the system. This is also a crucial piece of information as it tells us about the users present on the machine and with login information, we can single out from which user a malicious action was performed if there are multiple users on a single machine. Here we can see that only jcloudy was the user who logged on to the system.

Username	RID	Logon Count	Last Logon Time	Last Password Change	Invalid Logon Count	Last Failed Login
Administrator	500	0	Never	Never	0	Never
Guest	501	0	Never	Never	0	Never
DefaultAccount	503	0	Never	Never	0	Never
WDAGUtilityAccount	504	0	Never	27/03/2018 12:11:45 UTC	0	Never
jcloudy	1001	23	06/04/2018 12:26:27 UTC	27/03/2018 9:18:58 UTC	0	06/04/2018 3:30:52 UTC

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SAM registry file.

Open it on Registry Viewer tool --> SAM --> SAM --> Domains --> Account --> Users

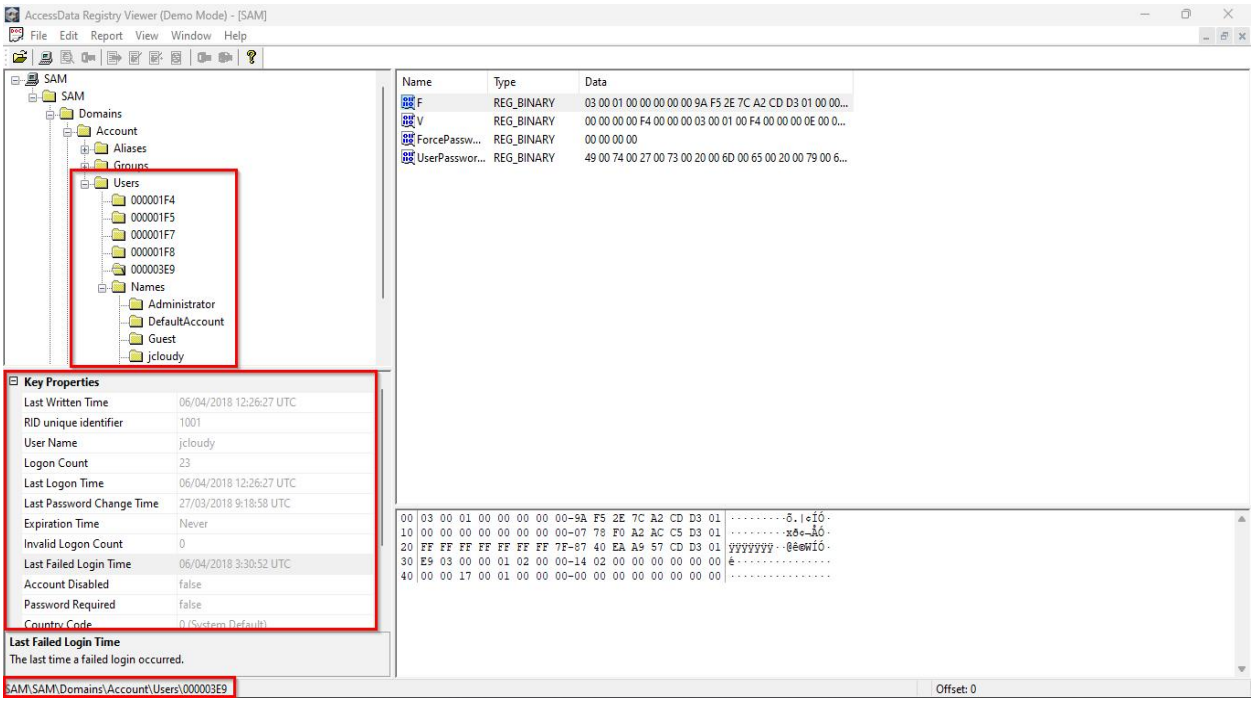

Figure 11 OS Accounts

[SPACE INTENTIONALLY LEFT BLANK]

3.8 Last System Logon

The last system logon tells us about the user who was last present on the machine. Which would be assumed to have performed that malicious action. This information also helps in timeline construction. We can see that jcloudy was the last person logon on the system.

User Name	jcloudy
SID	S-1-5-21-2734969515-1644526556-1039763013-1001

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SOFTWARE registry file.

Open it on Registry Viewer tool --> SOFTWARE --> Microsoft --> Windows NT --> CurrentVersion --> Winlogon

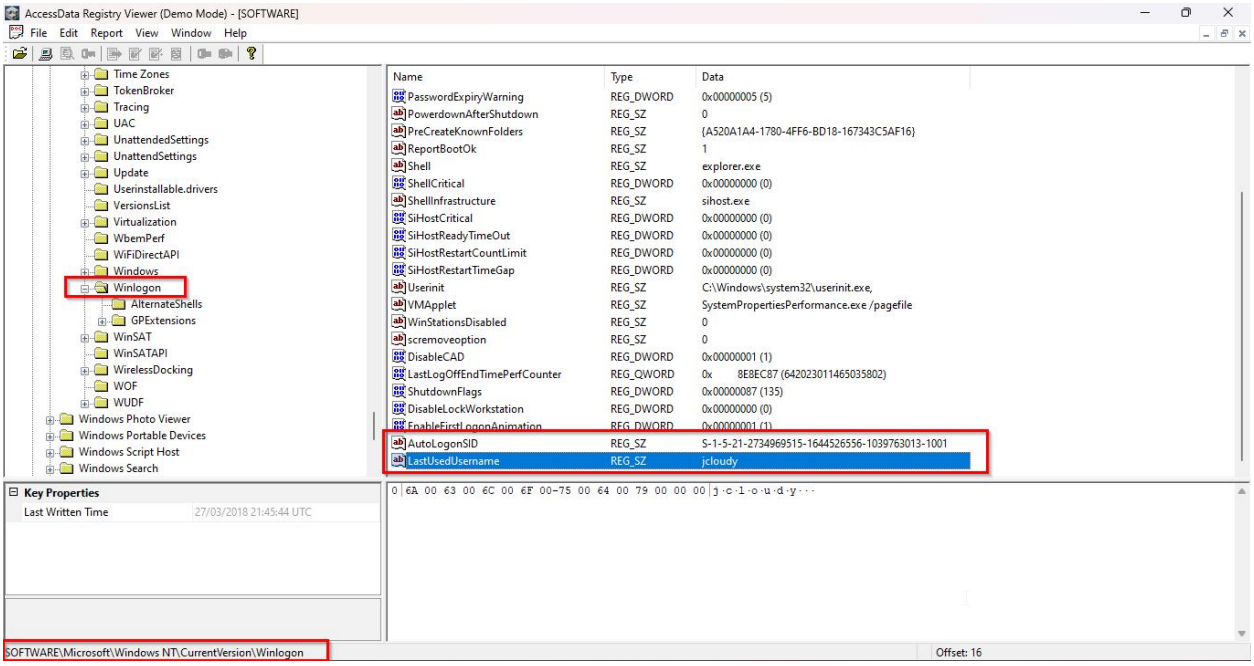

Figure 12 Last System Logon

3.9 Last recorded Shutdown Date/Time:

This tells us about the last time a user had intentionally or unintentionally shut down the system. It helps with timeline reconstruction in documentation.

LastDiskLayoutTimeString	2018/03/27-20:22:39

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SOFTWARE registry file.

Open it on Registry Viewer tool --> SOFTWARE --> Microsoft --> Windows NT --> CurrentVersion --> Prefetcher

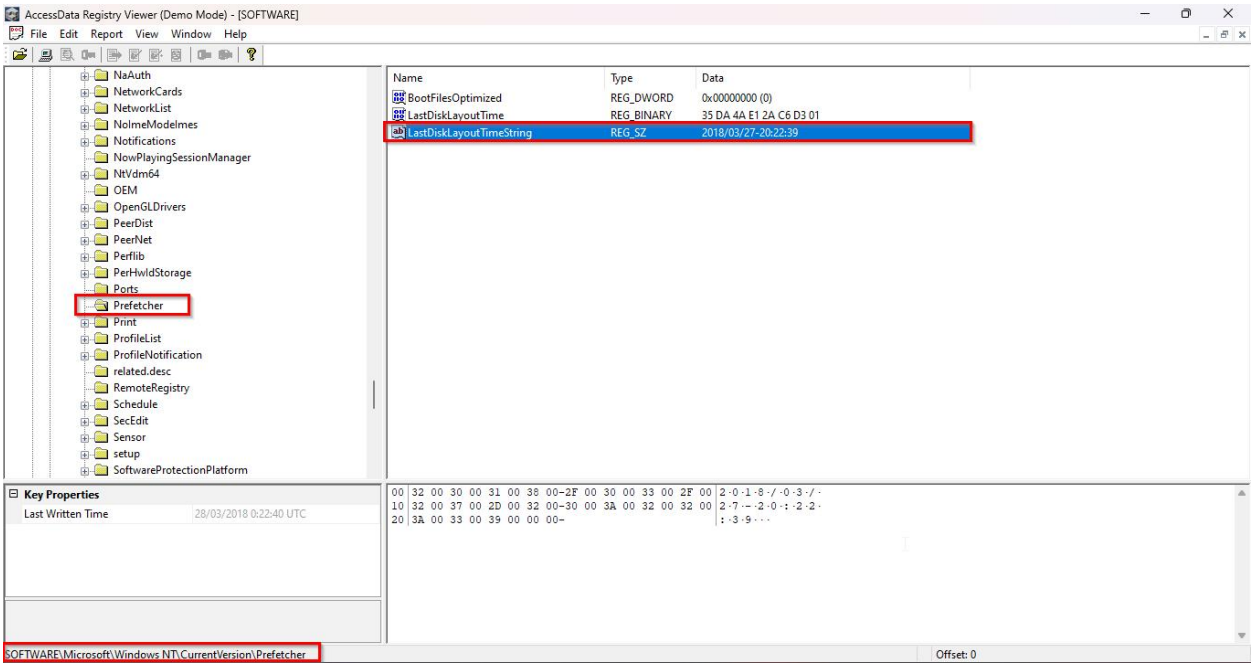

Figure 13 Last Recorded Shutdown Date/Time

3.10 Network Cards:

Network Cards tells us about the network capabilities of the user. Network configuration and connection status. Below are the network cards used by the user.

1	Intel(R) 82579LM Gigabit Network Connection
2	Broadcom 802.11n Network Adapter

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SOFTWARE registry file.

Open it on Registry Viewer tool --> SOFTWARE --> Microsoft --> Windows NT --> CurrentVersion --> NetworkCards

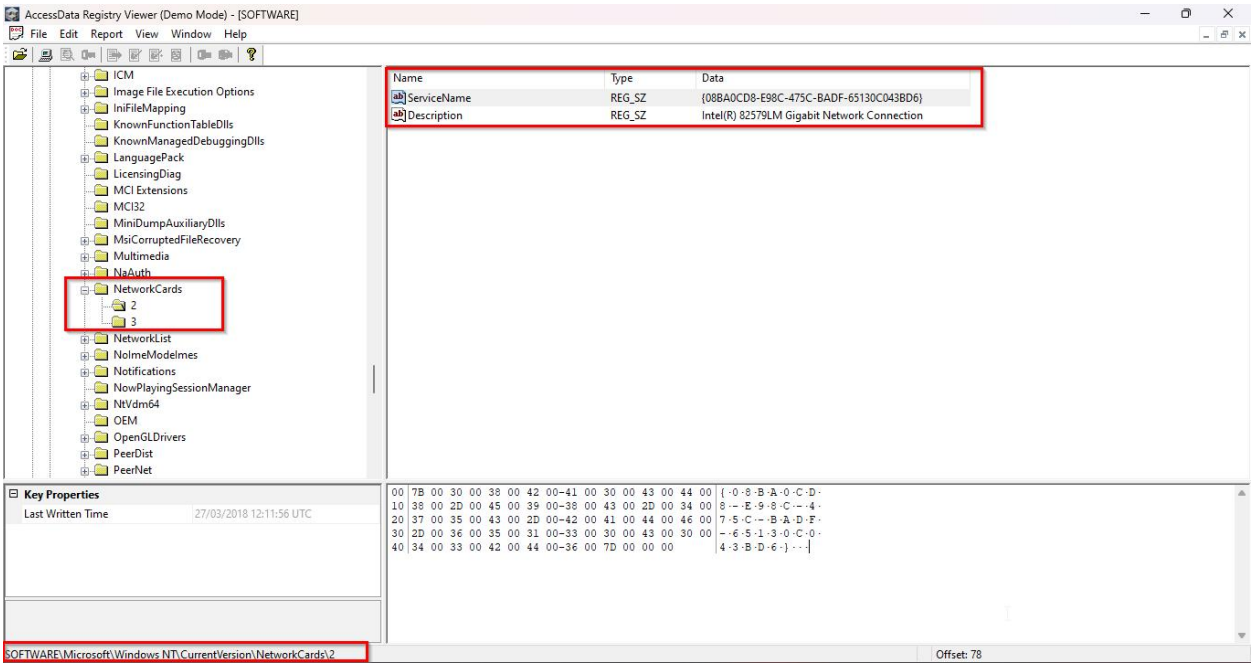

Figure 14 Network Cards

3.11 Network Interfaces:

Below are the servers with their IPS. Below is DHCP server the user was connected to, and the IP address provided by the DHCP server. With the DNS server the user was using. This information can be used to identify the router Ip /system Ip of the user. Which can help in identifying the network activities of the user.

DHCP IP Address	192.168.0.7
DHCP Subnet Mask	255.255.255.0
DHCP Server	192.168.0.1
DHCP Name Servers	'68.105.28.11' '68.105.29.11' '68.105.28.12'
DHCP Default Gateway	192.168.0.1

Method:

Click on Data source --> Select the Image.E01_1 Host --> Select the Image.E01 --> Select the vol7 --> Go to Windows Folder --> system32 folder ---> config folder ---> Extract the SYSTEM registry file.

Open it on Registry Viewer tool --> SYSTEM --> ControlSet001 --> Services --> Tcpip --> Parameters --> Interfaces

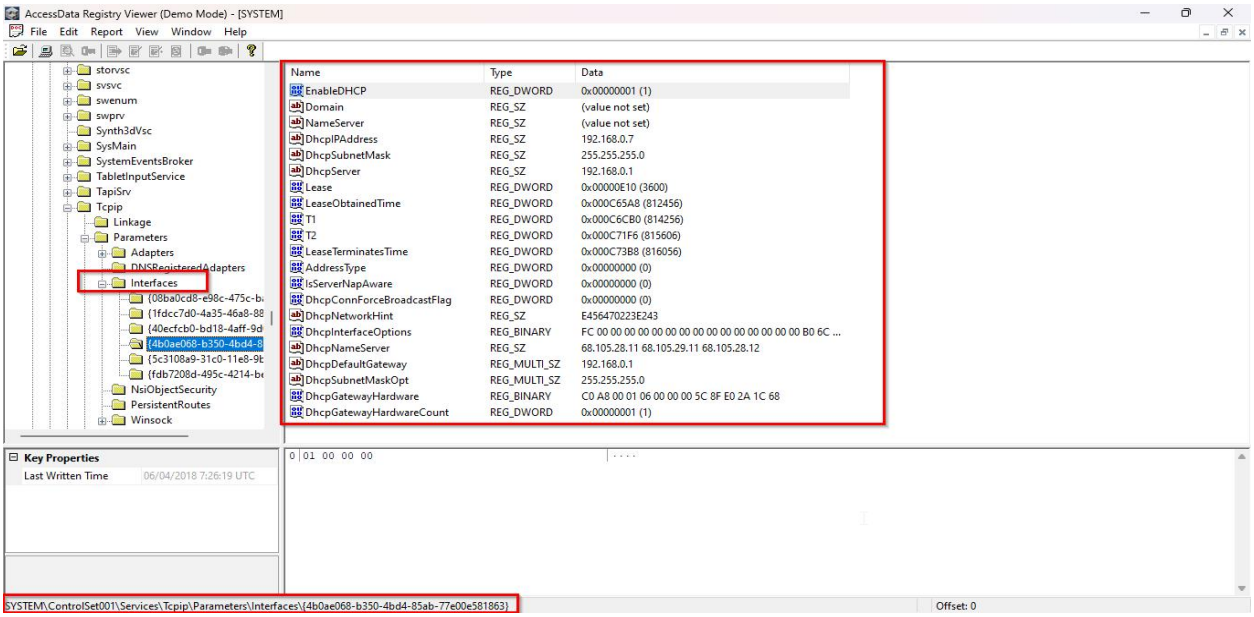

Figure 15 Network Interfaces

4. Specific Image Analysis

4.1 Jcloudy

We are starting specific analysis on the only active user jcloudy.

Below is the only user which was found to be active on the system and our primary suspect of any malicious activity. We can see that jcloudy has logon on the system 23 times as the only user on the system.

UserName	jcloudy
RID	1001
Creation Date	2018−03−2709:18:58 UTC
Last Login	06/04/2018 12:26:27 UTC
Login Count	23
Password Hint	It's me you idiot!
Password Fail Date	06/04/2018 3:30:52 UTC

Method:

Select Data Artifacts--> OS Accounts

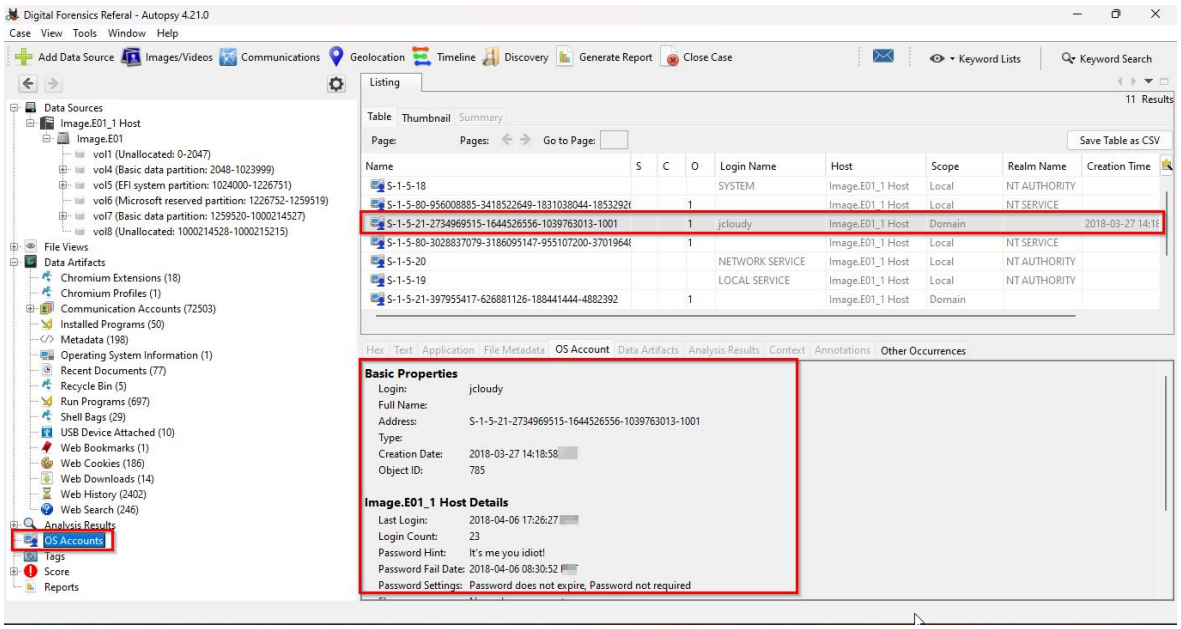

Figure 16 OS Account Details

4.2 Data Artifacts:

Data Artifacts refers to pieces of information or traces which have been left in the system. In our case this is the information which was left. This is once again a crucial piece of information as it talks about all the software and web information present with all the metadata. Below is the information left on the system.

Artifact Type	Child Count
Chromium Extensions	18
Chromium Profiles	1
Installed Programs	50
Metadata	198
Operating System Information	1
Recent Documents	77
Recycle Bin	5
Run Programs	697
Shell Bags	29
USB Device Attached	10
Web Bookmarks	1
Web Cookies	186
Web Downloads	14
Web History	2402
Web Search	246

Artifact Type	Child Count
Chromium Extensions (18)	18
Chromium Profiles (1)	1
Communication Accounts (72503)	
Installed Programs (50)	50
Metadata (198)	198
Operating System Information (1)	1
Recent Documents (77)	77
Recycle Bin (5)	5
Run Programs (697)	697
Shell Bags (29)	29
USB Device Attached (10)	10
Web Bookmarks (1)	1
Web Cookies (186)	186
Web Downloads (14)	14
Web History (2402)	2402
Web Search (246)	246

Figure 17 Data Artifacts

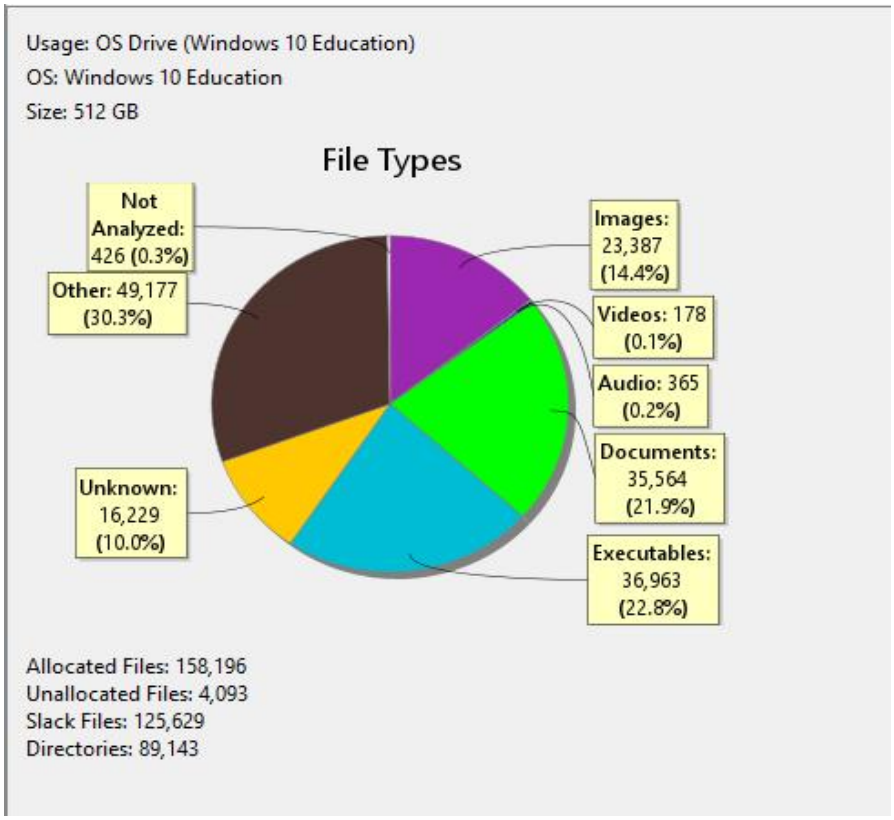

Figure 18 Data Artifacts Graph

Method:

Select Data Artifacts

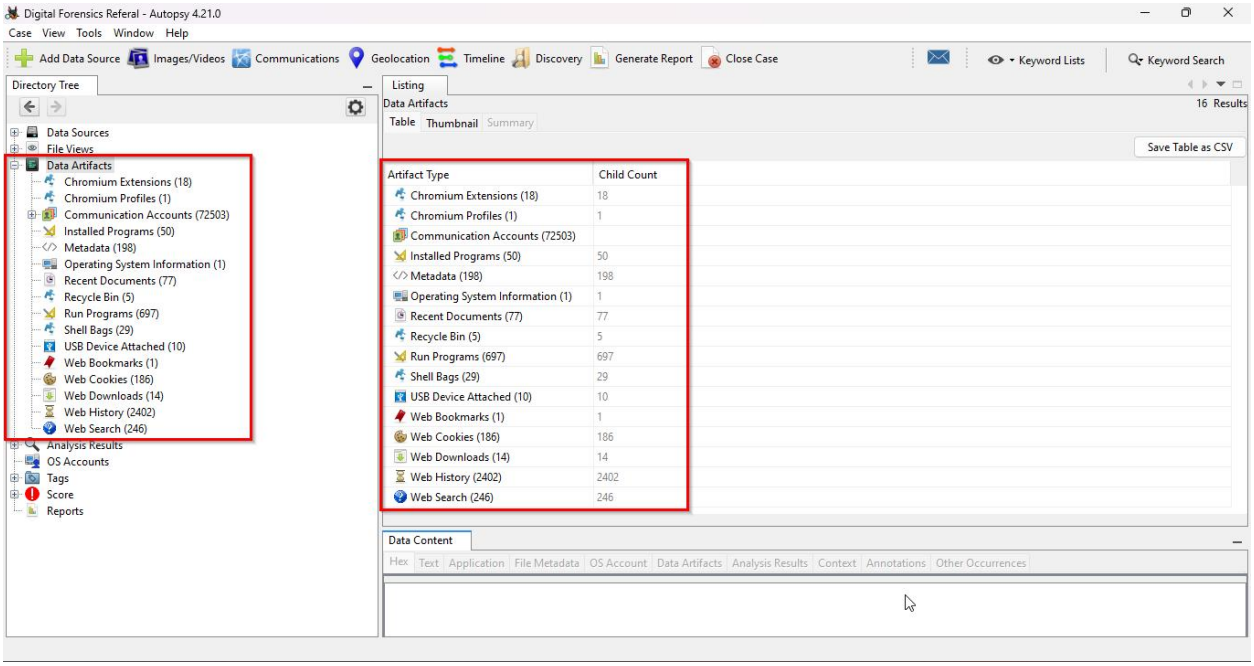

Figure 19 Data Artifacts

[SPACE INTENTIONALLYLEFTBLANK]

4.3 Software Inventory

Below is the software present on the system. We can dictate the type of activities the user was involved in e.g. Microsoft Office 365 tells us the user was involved in documentation. We can identify any malicious tool or software used. Below are the tools installed on the system by jcloudy.

No.	Program Names	Uses
1.	Box Sync v.4.0.7900.0	Synchronizes files between Box cloud storage and your local computer.
2.	S3 Browser version 7.6.9 v.7.6.9.0	Manages files on Amazon S3 storage.
3.	Backup and Sync from Google v.3.40.8921.5350	Synchronizes files between Google Drive and your local computer.
4.	NVIDIA HD Audio Driver 1.3.34.17 v.1.3.34.17	Supports NVIDIA HD audio output.
5.	NVIDIA Install Application v.2.1002.236.2037	Manages the installation of NVIDIA drivers and software.
6.	Office 16 Click-to-Run Extensibility Component 64-bit Registration v.16.0.8431.2236	Provides extensibility components for Office 2016 Click-to-Run installations.
7.	Office 16 Click-to-Run Licensing Component v.16.0.8431.2236	Manages licensing for Office 2016 Click-to-Run installations.
8.	Microsoft Office 365 ProPlus - en-us v.16.0.8431.2236	Provides Office 365 ProPlus applications like Word, Excel, PowerPoint, and Outlook.
9.	NVIDIA nView 148.03 v.148.03	Manages multi-display settings and desktop organization.
10.	NVIDIA 3D Vision Driver 376.54 v.376.54	Supports NVIDIA 3D Vision hardware.
11.	Vulkan Run Time Libraries 1.0.26.0 v.1.0.26.0	Provides Vulkan graphics API runtime libraries.
12.	NVIDIA Graphics Driver 376.54 v.376.54	Supports NVIDIA GPU graphics.
13.	NVIDIA Control Panel 376.54 v.376.54	Provides a graphical interface for configuring NVIDIA GPU settings.

14.	NVIDIA Display Container v.1.0	Manages display-related settings for NVIDIA GPUs.
15.	NVIDIA Display Container LS v.1.0	Runs services for NVIDIA Display Container.
16.	Dell Touchpad v.10.1207.101.103	Manages settings for Dell touchpad devices.
17.	DXM_Runtime	Related to DirectX runtime, used for running applications that use DirectX.
18.	MPlayer2	A media player for video and audio files.
19.	AddressBook	Contact management application.
20.	Connection Manager	Manages network and internet connections.
21.	DirectDrawEx	Part of the DirectX API, used for rendering graphics.
22.	Fontcore	Manages font rendering.
23.	IE40, IE4Data, IE5BAKEX, IEData	Components of Internet Explorer, managing data and settings.
24.	MobileOptionPack	Provides additional options for mobile device support.
25.	SchedulingAgent	Manages scheduled tasks and applications.
26.	WIC	Windows Imaging Component, used for image processing.
27.	Dropbox v.46.4.65	Synchronizes files between Dropbox cloud storage and your local computer.
28.	Dropbox Update Helper v.1.3.65.1	Manages updates for Dropbox.
29.	Google Update Helper v.1.3.33.7	Manages updates for Google applications.
30.	Google Chrome v.65.0.3325.181	Web browser developed by Google.

Method:

Select Data Artifacts--> Installed Programs

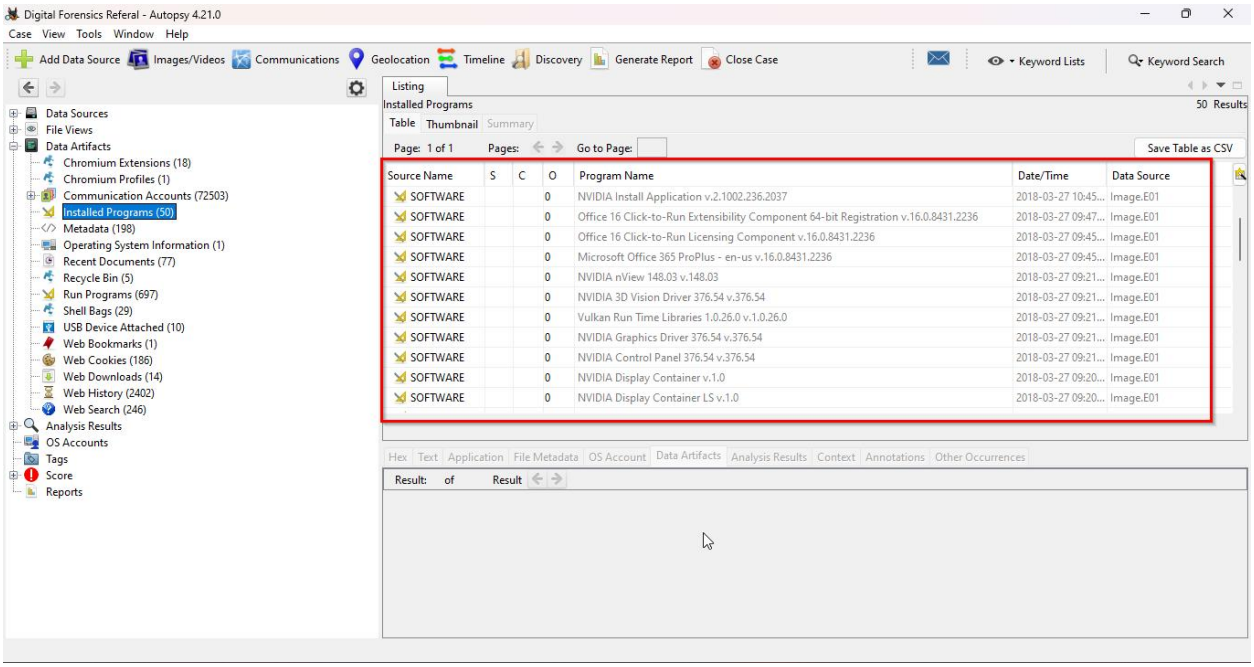

Figure 20 Installed Programs

[SPACE INTENTIONALLYLEFTBLANK]

4.4 USB Device Attached:

All the devices connected to the system are given with their device model name device company make with device id. We can use this information to identify the device if it were to be found. E.g. the Flash Drive, if it were to be found by the investigator, they can use this information to 100% identify as the Flash Drive connected to this system.

Device Model	Device Make	Device ID	Date/Time
ROOT_HUB20		4&1671a21&0	2018-03-27 21:45:42 UTC
ROOT_HUB20		4&b21407d&0	2018-03-27 21:45:42 UTC
ROOT_HUB30		4&2d689036&0&0	2018-03-27 21:45:43 UTC
SDCZ80 Flash Drive	SanDisk Corp.	AA010215170355310594	2018-03-27 12:13:16 UTC
SDCZ80 Flash Drive	SanDisk Corp.	AA010603160707470215	2018-03-27 21:45:44 UTC
Dell Integrated HD Webcam	Microdia	6&c0f0d73&0&5	2018-03-27 21:45:44 UTC
Dell Integrated HD Webcam	Microdia	7&2bca401f&0&0000	2018-03-27 21:45:44 UTC
BCM20702A0 Bluetooth Module	Dell Computer Corp.	28E347017777	2018-03-27 21:45:44 UTC
Integrated Rate Matching Hub	Intel Corp.	5&182c2717&0&1	2018-03-27 21:45:43 UTC
Integrated Rate Matching Hub	Intel Corp.	5&2cd6d949&0&1	2018-03-27 21:45:44 UTC

Method:

Select Data Artifacts --> USB Device Attached

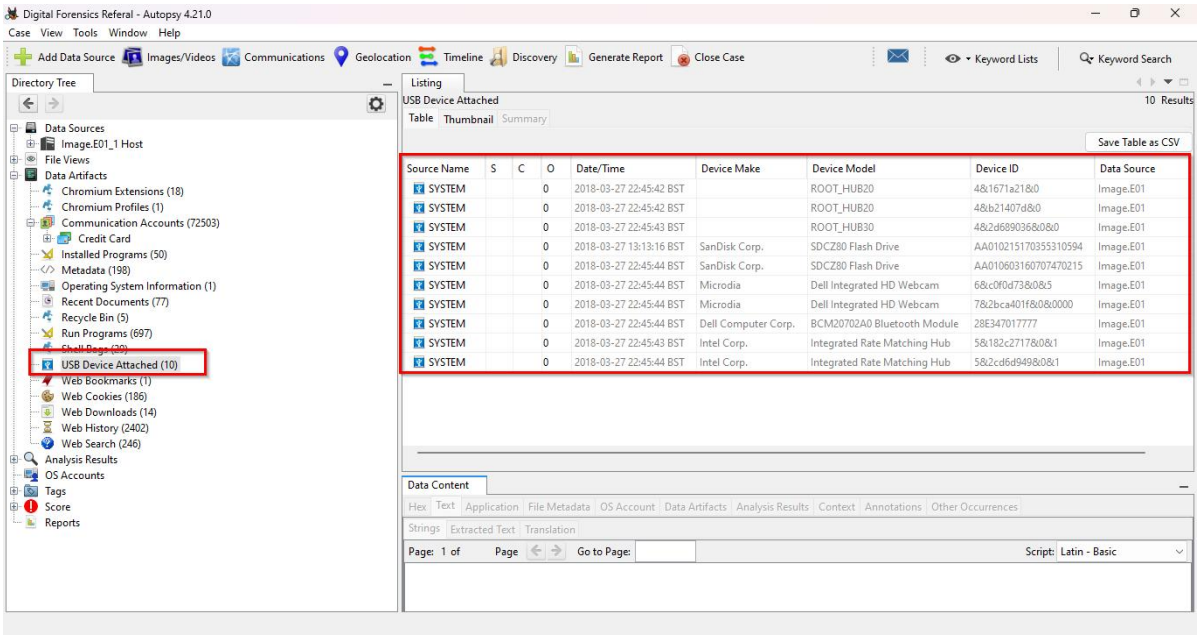

Figure 21 USB Device Attached

[SPACE INTENTIONALLY LEFT BLANK]

4.5 Browser Profile:

Every browser has a profiling option. E.g. Firefox allows you to create and save a profile. This profile can then be imported into another browser. This saves a lot of time changing the theme and many other options to a user's preference again and again. Below is jcloudy's Browser Profile.

Path	Default
User ID	111256729592432613619
Name	Person 1
Username	jimcloudy1@gmail.com
Program Name	Google Chrome
OS Account	jcloudy

Method:

Select Data Artifacts--> Chromium Profiles

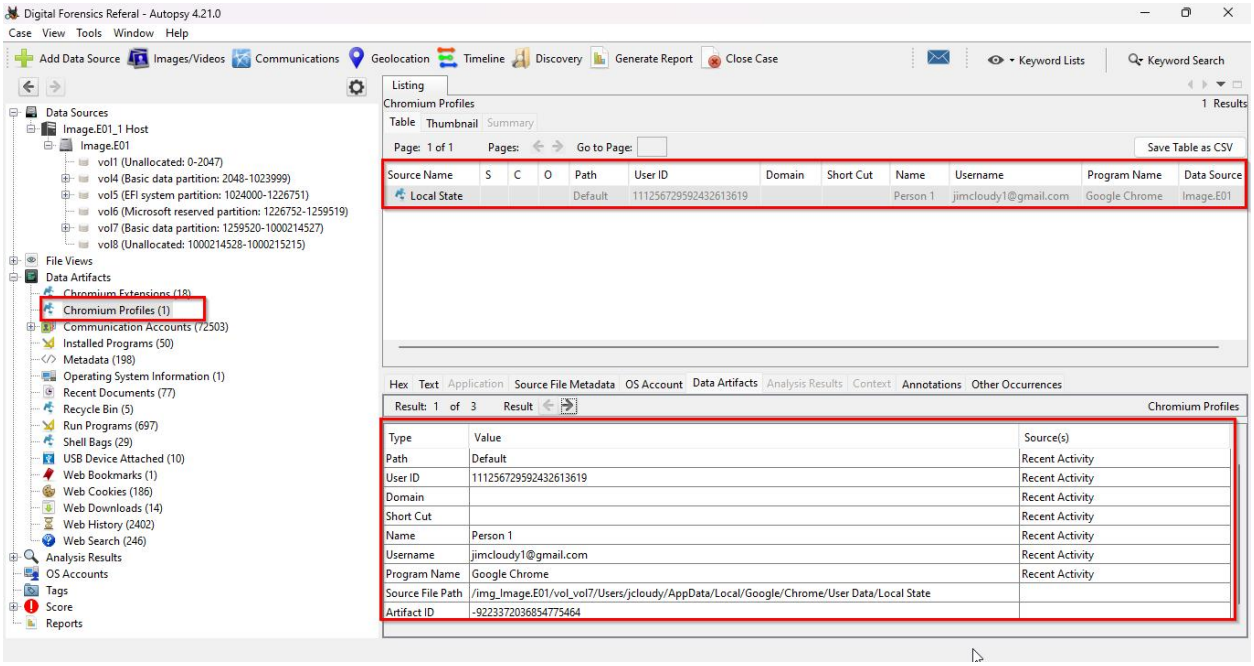

Figure 22 Browser Profile

4.6 Documents:

Documents present on the system. Below are the 77 Documents found on the jcloudy system.

Recent Documents	77

4.7 Suspicious Documents:

There are few suspicious and notable documents which would be considered from the 77 documents present on the system.

4.7.1 Document 1

This Document named Planning.docx was found on jcloudy's documents. This document lists a plan of selecting a target, finding a good escape route. With supplies such as guns, ammo, gloves, clothing and cash. For escape Vietnam and Indonesia were considered. This is an extreme planning for mass shoutout at a location and then flying to Indonesia or Vietnam. This is primary evidence against jcloudy.

File name	Planning.docx
Type	docx
File Path	/img_Image.E01/vol_vol7/Users/jcloudy/Desktop/Planning.docx
Created	2018-03-30 02:16:48 UTC
Modified	2018-04-04 05:30:41 UTC
Accessed	2018-04-04 05:30:41 UTC
MD5	4ef414e469b7830faa2db429fe1321ee
SHA256	Od87fa0cb21fd3cd3e2eab41149e611593f0c6a5224ed264cd5632692c126e1

Metadata	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 588 Character-Count-With-Spaces: 690 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-03-30T02:16:00Z Last-Author: jcloudy Last-Modified: 2018-04-04T05:30:00Z Last-Save-Date: 2018-04-04T05:30:00Z Line-Count: 4 Page-Count: 1 Paragraph-Count: 1 Revision-Number: 9 Template: Normal Total-Time: 2635 Word-Count: 103 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 9 creator: jcloudy date: 2018-04-04T05:30:00Z dc:creator: jcloudy dc:publisher:

Planning

1. Target
a. Must have good escape route
b. Preferably near Airport
c. Must be Gun Free zone.

2. Supplies
a. Gun (black market)
i. Norther VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153
ii. NOVA 412 W Broad Street Falls Church, VA 22046
iii.
b. Ammo.
i. 9mm is 1000 for $360
ii. Kel-Tec Sub 2000 9mm $400.
c. Latex gloves
d. Velcro tear away clothing?
e. Cash

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.

Figure 23 Planning.docx

4.7.2 Document 2

This document named AIRPORT INFORMATION.docx was found on jcloudy's system. This document lists the on-time departure to Denpasar Bali, Indonesia from Washington DC

File name	AIRPORT INFORMATION.docx
Type	docx
File Path	/img_Image.E01/vol_vol7/Users/jcloudy/Desktop/AIRPORT INFORMATION.docx
Created	2018-03-30 2:29:57 UTC
Modified	2018-04-04 04:59:32 UTC
Accessed	2018-04-04 04:59:32 UTC
MD5	297eec248647f33f887d72328ab56f3c
SHA256	1fb5577d8559562d97ac3023e0ca91cc6b8b55d2e5fabaa81160c109f0abf9b6
Metadata	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 215 Character-Count-With-Spaces: 251 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-03-30T02:29:00Z Last-Author: jcloudy Last-Modified: 2018-04-04T04:59:00Z Last-Save-Date: 2018-04-04T04:59:00Z Line-Count: 1 Page-Count: 1 Paragraph-Count: 1 Revision-Number: 9 Template: Normal Total-Time: 4701 Word-Count: 37 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 9 creator: jcloudy date: 2018-04-04T04:59:00Z dc:creator: jcloudy dc:publisher:

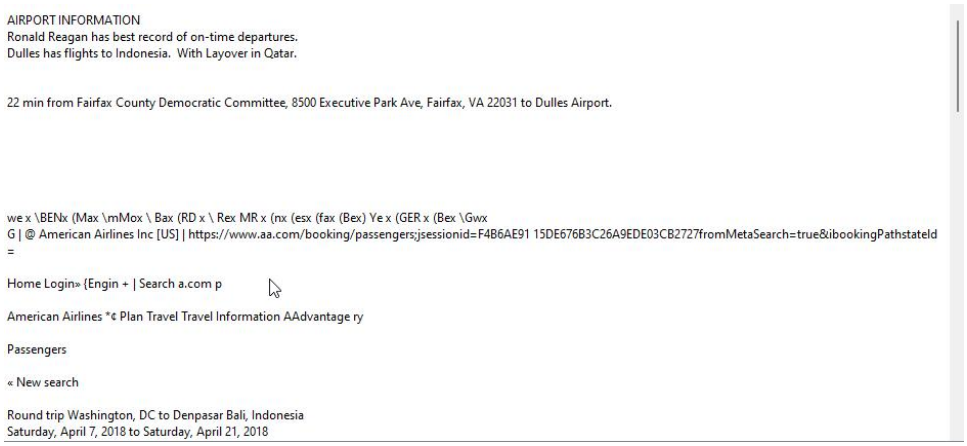

Figure 24 AIRPORT INFORMATION.docx

[SPACE INTENTIONALLYLEFTBLANK]

4.7.3 Document 3

This file documents the thoughts of jcloudy related to his intended attack. He mentions he doesn't expect to succeed but even if he fails it's much better to live as a lamb and that freedom can only come with sacrifice. He said he saved all the records on cloud on several accounts He also mentioned that the cloud keys are with Paul.

File name	Cloudy thoughts (4apr).docx
Type	docx
File Path	/img_Image.E01/vol_vol7/Users/jcloudy/Desktop/Cloudy thoughts (4apr).docx
Created	2018-04-05 02:39:29 UTC
Modified	2018-04-05 02:39:30 UTC
Accessed	2018-04-05 02:39:30 UTC
MD5	f8c2bc733c109a88405dfd13b47d0690
SHA256	37cd60bccb8cf01fd36be13d89e5df64749bcc072133d3bad1ed0c430e436dfd
Metadata	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 986 Character-Count-With-Spaces: 1156 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-04-05T02:32:00Z Last-Author: jcloudy Last-Modified: 2018-04-05T02:39:00Z Last-Save-Date: 2018-04-05T02:39:00Z Line-Count: 8 Page-Count: 1 Paragraph-Count: 2 Revision-Number: 1 Template: Normal Total-Time: 7 Word-Count: 172 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 1 creator: jcloudy date: 2018-04-05T02:39:00Z dc:creator: jcloudy dc:publisher:

I don't know if this plan will work. Plans never survive first contact. I don't expect to fail, but there are so many possibilities. But now the weather. Its going to snow, and the winds will be strong. No problem for the attack, but if my flight is delayed or cancelled, that might prove to be a problem.

I'm stressed and writing used to help me calm down. It seems to be working. Im leaving a lot behind, and the weight of this responsibility is almost too much to handle. I wont stop now, though. Even if I'm killed at the site, I know that what im doing is just and right. Freedom requires sacrifice. If I must be that lamb, then I walk to my slaughter freely of my own accord.

I am saving everything to the cloud on several accounts. I don't want my words mixed up, and I don't want my thoughts deleted. I want my family to understand why I did this. I think they will keep my secret if I am successful and leave the country without problems. The only record will remain in the cloud and Paul will have the only other keys.

My fate will be in God's hands. I pray I have the strength and the luck necessary to persevere. Please let the weather clear!

Figure 25 Cloudy thoughts (4apr).docx

[SPACE INTENTIONALLYLEFTBLANK]

4.7.4 Document 4

In this document jcloudy compiles PowerPoint presentations, he captured a series of screenshots along with the corresponding website URLs and taskbar date and time, storing them on his Microsoft OneDrive account. 1st slide names the operation as Operation 2nd Hand Smoke. 2nd slide shows the Town Hall Project (gun safety) event date, Saturday April 7th, 2018, and time 1230hrs to 1400hrs. Location: Cascades Library, 21030 Whitfield Place Sterling, VA 20165. 3rd slide is the street view of the location from 2nd slide. 4th and 5th slide jcloudy has color coded the routes he intended to take to the Cascades Library and exit out towards the Dulles International airport. 6th slide show jcloudy's flight with Seoul airs from Washington to Seoul and from Seoul to Denpasar (Bali). 7th slide shows the hotel booking in sea breeze Candidasa.

File name	Operation 2nd Hand Smoke.pptx
Type	pptx
File Path	/img_Image.E01/vol_vol7/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx
Created	2018-04-04 04:56:19 UTC
Modified	2018-04-04 05:11:27 UTC
Accessed	2018-04-04 05:11:27 UTC
MD5	b301fbf4104fb64b566b076c12a5d113
SHA256	7b08d680f342f3d28a79c2a324bfd0576586958992cd738319aec3ccd5d1e129
Metadata	Application-Name: Microsoft Office PowerPoint Application-Version: 16.0000 Author: jcloudy Content-Type: application/vnd.openxmlformats-officedocument.presentationml.presentation Creation-Date: 2018-04-04T04:32:32Z Last-Author: jcloudy Last-Modified: 2018-04-04T05:11:27Z Last-Save-Date: 2018-04-04T05:11:27Z Paragraph-Count: 4 Presentation-Format: Widescreen Revision-Number: 7 Slide-Count: 7 Total-Time: 33 Word-Count: 12 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 7 creator: jcloudy date: 2018-04-04T05:11:27Z dc:creator: jcloudy

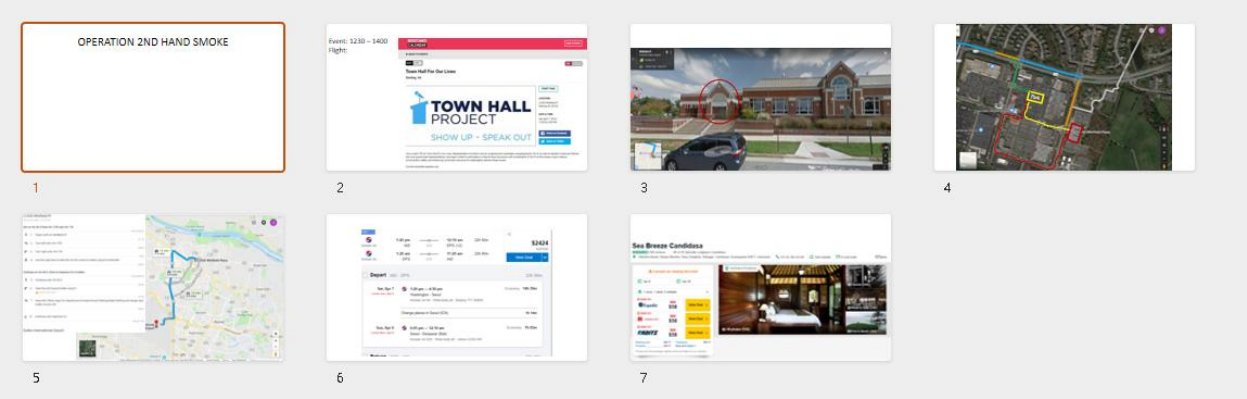

Figure 26 Operation 2nd Hand Smoke.pptx

[SPACE INTENTIONALLYLEFTBLANK]

4.7.5 Document 5

These contain some of the things that jcloudy was following. Different articles and different statistics.

File name	The Cloudy Manifesto.docx
Type	docx
File Path	/img_Image.E01/vol_vol7/Users/jcloudy/Desktop/The Cloudy Manifesto.docx
Created	2018-04-02 01:35:27 UTC
Modified	2018-04-02 01:35:27 UTC
Accessed	2018-04-02 01:35:27 UTC
MD5	14c07920ddc81fbd489e61d60e5c9f28
SHA256	fee91c8bafb9fb51574b11bfeed5a08b89e7bb90e874c07d95562c76380f2c65
Metadata	Application-Name: Microsoft Office Word Application-Version: 16.0000 Author: jcloudy Character Count: 4087 Character-Count-With-Spaces: 4795 Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Creation-Date: 2018-04-02T01:00:00Z Last-Author: jcloudy Last-Modified: 2018-04-02T01:35:00Z Last-Save-Date: 2018-04-02T01:35:00Z Line-Count: 34 Page-Count: 7 Paragraph-Count: 9 Revision-Number: 1 Template: Normal Total-Time: 35 Word-Count: 717 X-Parsed-By: org.apache.tika.parser.DefaultParser cp:revision: 1 creator: jcloudy date: 2018-04-02T01:35:00Z dc:creator: jcloudy dc:publisher:

Figure 27 The Cloudy Manifesto.docx

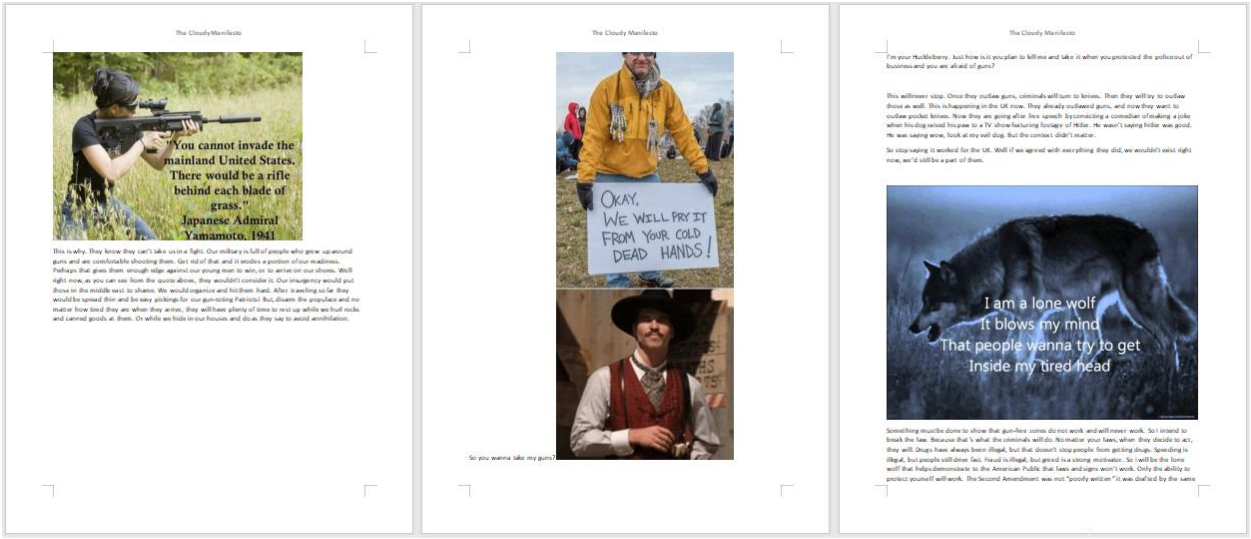

Figure 28 The Cloudy Manifesto.docx

men who drafted the rest of the Constitution. And no one is complaining about he protections and freedom it gives you. Especially the 1st amendment which allows you to spew your crazy gun-control thoughts.

You will soon see when the blood has been shed and the defenseless bodies stacked high. I will do what I must. No matter who is hurt, the collateral damage will be worth it.

I will be the change. I will be the revolutionary. I will be the history maker. I will fight. I will be the Lone Wolf.

Figure 29 The Cloudy Manifesto.docx

[SPACE INTENTIONALLYLEFTBLANK]

4.8 Web History:

Below is the web history left of the user jcloudy. 2402 was left.

Total Web History	2402

Web History Analysis:

1. Cloud Storage

Web History Analysis shows that jcloudy wants to sync data on cloud. Basically, as mentioned in Document 3 he wants to save all the reasons behind the attack into cloud storage. So, his thoughts are not mixed up behind his sacrifice. In cloud storage there are mostly searches related to cloud belonging to OneDrive, Amazon S3 Services, Box Storage and Mega Backup.

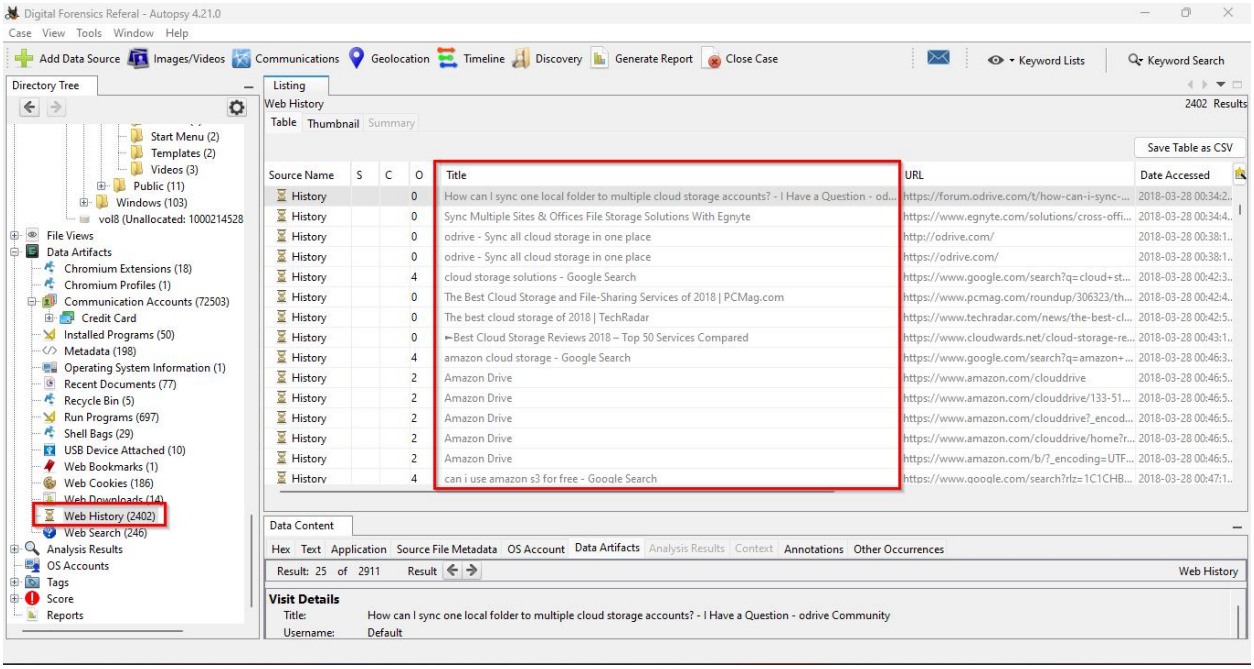

Figure 30 Web History Cloud Storage

2. *Guns*

His most searches belong to the Guns. As mentioned in Planning.docx he wants to buy a gun for the attack. His searches further cement his intentions.

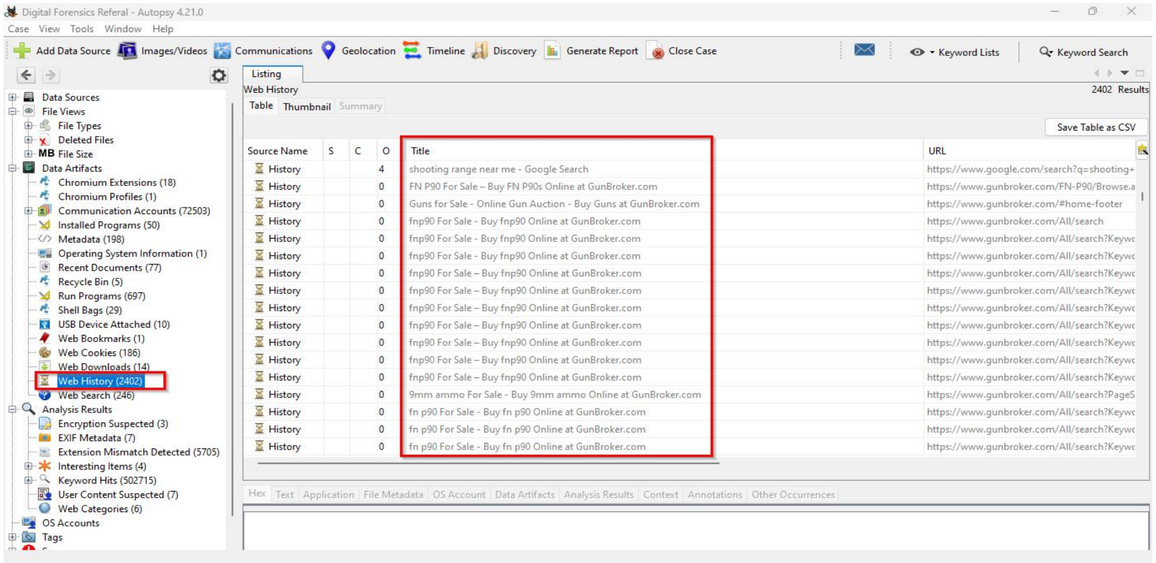

Figure 31 Web History Guns

3. *Escape*

After the attack, he wants to take an escape route, as mentioned in Planning.docx. His searches further cement this point. His priorities escape seems to between Indonesia and Vietnam.

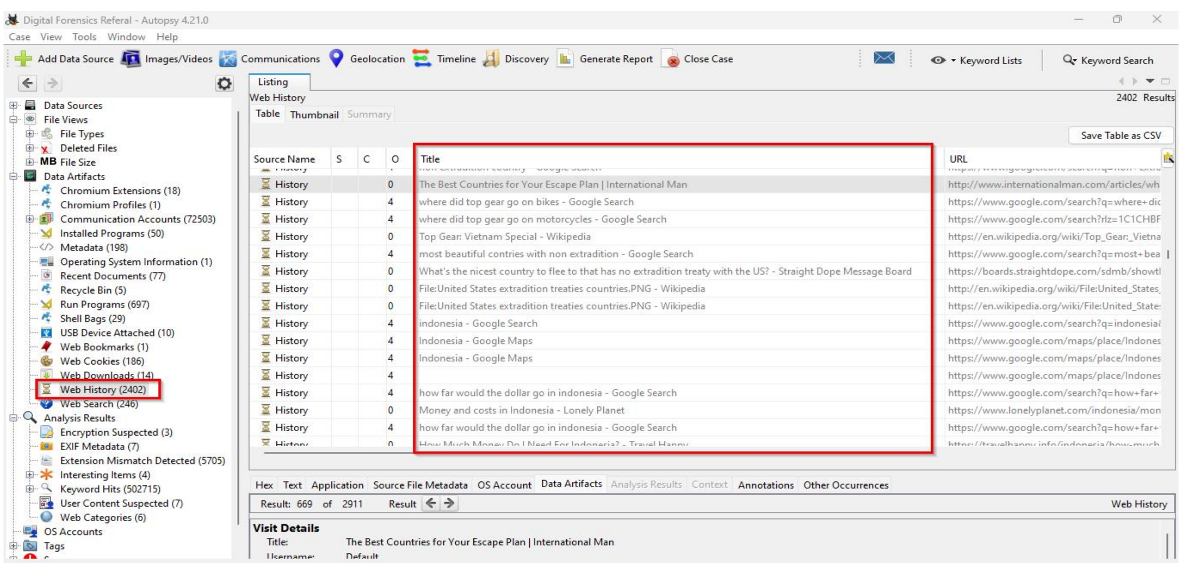

Figure 32 Web History Escape

5. Finding/Conclusion

After completing the analysis, the following notable things were discovered about this case.

Firstly, following the documents that were discovered on the system.

Malicious Document: ‘The Cloudy Manifesto.docx’

In this document ‘The Cloudy Manifesto.docx’, ‘jcloudy’ seems to be following some fake data and some fake quotes with questionable statistics. In the document he talks how it’s our own right to protect ourselves as the government has failed us, not only that if the government can’t protect us at least we need to protect ourselves.

Lone Wolf

Now following this theme, he talks about implementing gun control laws would only lead to the criminal changing to other weapons and this way the government could control us like a herd of sheep. He beliefs this way we would be throwing stones at them while they can use their guns to get rid of us.

Following this theme, he beliefs that he should rather live as a ‘lone wolf’ the live as a helpless sheep. Which leads him further down this path.

Notable Document: ‘Planning.docx’

In this document ‘Planning.docx’ following his ‘sheep and wolf’ terminology, he starts working on a mass shoot out plan. Firstly, he selects a target namely a place with gun control law and an airport nearby. Next, he wants to buy a gun with its ammo type and then get an escape route. Namely fleeing the country.

Notable Document: ‘AIRPORT INFORMATION.docx’

In this document ‘AIRPORT INFORMATION.docx’ he narrows down on countries which would be harder to find him for his escape. He narrows it down to Indonesia. He makes a document with flight details to Denpasar, Indonesia.

Notable Document: ‘Cloudy thoughts (4apr).docx’

In this document ‘Cloudy thoughts (4apr).docx’, he talks about saving his plan on cloud storage as he wants his family to understand his reasoning and the responsibility he had to shoulder. He also mentions how even if his plan fails, he is alright with it as through this sacrifice he can get his freedom.

Notable Document: ‘Operation 2nd Hand Smoke.pptx’

In this PowerPoint slide ‘Operation 2nd Hand Smoke.pptx’ discovered in the system he details his plan to attack Cascades Library, 21030 Whitfield Place Sterling, VA 20165 on the Town Hall Project (gun safety) event. Which is true to his ideology as mentioned previously. He color coded his attack route and escape route to airport for there he will get one flight from Washington DC to Seoul and second from Seoul to Indonesia. He also shows his hotel details in this PowerPoint slide.

Notable Internet History

Next from his internet search history we can see that he was searching for cloud storage platforms. To store his plan as mentioned previously. He is discovered to be searching for guns and ammo with also for flights details for other countries.

Conclusion

In conclusion, it is clear that ‘jcloudy’ was an ill mind. He had been following the wrong ideology, this whole time possibly stemming from some trauma. His intentions of a mass shootout are also clear with all the documents and all the web history. Which makes it clear of the crime he is to get on him.

6. References

- Sleuth Kit. (n.d.). *Autopsy User Documentation 4.12.0*. Retrieved from https://sleuthkit.org/autopsy/docs/user-docs/4.12.0/index.html
- Williams, O. W. (n.d.). *Internet Browser Forensics with Autopsy*. LinkedIn. Retrieved from https://www.linkedin.com/pulse/internet-browser-forensics-autopsy-octavious-w--rq7be#:~:text=To%20view%20the%20data%20in,visits%2C%20keyword_search_terms%2C%20downloads
- Cyberspace Security. (2019, February 12). *Autopsy Internet History Analysis - Open-Source Digital Forensics*. [Video]. YouTube. https://www.youtube.com/watch?v=wU5hHPuf1Lo
- AccessData. (2012). *Registry Viewer User Guide*. Scribd. Retrieved from https://www.scribd.com/document/144984450/Registry-Viewer-User-Guide