UNIVERSITY OF HERTFORDSHIRE (UH)

SCHOOL OF PHYSICS, ENGINEERING AND COMPUTER SCIENCE

COURSE: MSc COMPUTER SCIENCE WITH CYBER SECURITY

MODULE: DIGITAL FORENSIC 7COM1067-0206-2023

ACADEMIC YEAR: 2023-2024

ASSIGNMENT TITLE: DIGITAL FORENSICS IN PRACTICE

NAME: OLUWATOBI ELIJAH AKANNI

STUDENT NUMBER: 22060310

Table of Contents

Table of Figures

ABSTARCT

This report outlines the activities conducted in the investigation of a case involving a forensic image of a computer's hard disk. The case management section discusses the setup of the new case and addresses continuity and integrity issues. The evidence analysis section covers various aspects of the forensic image, including partitions, operating system installations, time zone settings, software program installations, hardware devices, user profiles, and other significant findings. The findings and conclusions are presented in a factual manner following best practices, Contemporaneous notes are included in appendix iv to demonstrate the chain of custody maintenance.

1.0 INTRODUCTION

Digital investigations contribute to today's investigations by giving insights into electronic devices and associated data. This paper presents the results of analysing a computer's hard drive image using case management, evidence evaluation, and result interpretation. The comprehensive technique guarantees that relevant information is retrieved from sources while maintaining integrity and continuity. By providing an outline of the examination technique and its consequences for the specific case under consideration, this investigation emphasises the importance of digital forensics in discovering critical evidence and resolving complicated legal issues.

1.1 Objective

The purpose of this paper is to highlight the critical significance of digital investigations in modern investigations by giving findings from a study of a computer's hard drive image. The paper aims to demonstrate how relevant information is collected from digital sources while preserving criteria of integrity and continuity. This study emphasises the relevance of digital forensics in discovering critical evidence and addressing complex legal issues by offering an outline of the examination technique and its ramifications for the specific case under consideration.

2.0 CASE MANAGEMENT

The digital investigation in Case E001 involved analyzing a computer's hard drive image to extract pertinent information for the specific legal matter under review. The investigation followed a meticulous process of case management, evidence evaluation, and result interpretation to uphold integrity and continuity standards.

2.1 Case Establishment

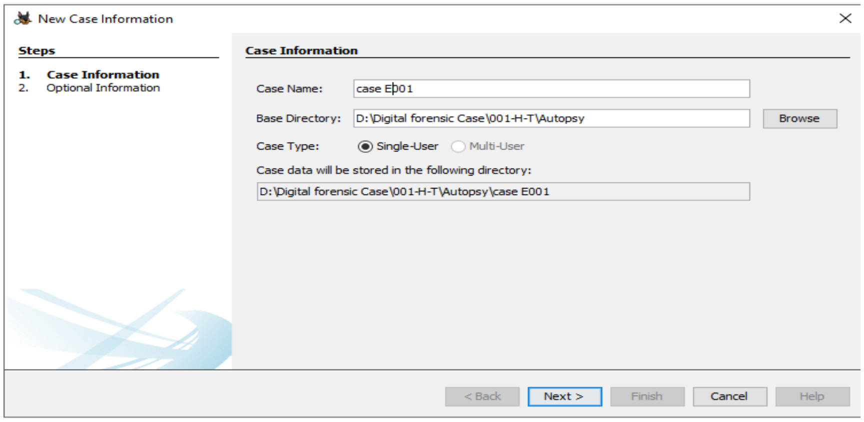
The case was established with care and precision making sure to gather all required data and materials. Consistency and trustworthiness concerns were handled with caution during the handling and transfer of items to preserve the integrity of the evidence.

2.1.1 Case Information

The case was assigned the name " Case E001" by the organization's file naming conventions. It was then saved on an external hard drive to prevent any corruption of the original data and avoid potential data loss. ***(see figure 1)***

2.1.2 Optional Information

The investigator's information, including their name, phone number, and email, was documented. Additionally, a case number "001" was assigned to the file. The organization details, specifying the University of Hertfordshire, were also included in this section. ***(see figure2)***


New Case Information

Steps
1. Case Information
2. Optional Information

Case Information

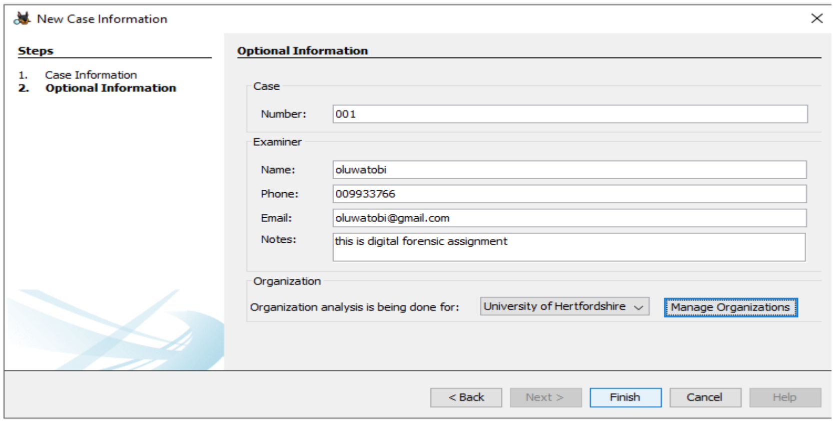
Case Name: case E001

Base Directory: D:\Digital forensic Case\001-H-T\Autopsy

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:
D:\Digital forensic Case\001-H-T\Autopsy\case E001

Figure 1: case Information


New Case Information

Steps
1. Case Information
2. Optional Information

Optional Information

Case
Number: 001

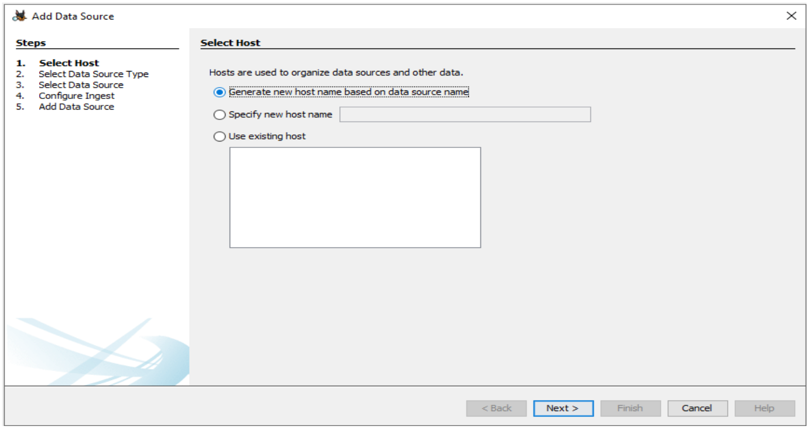
Examiner
Name: oluwatobi
Phone: 009933766
Email: oluwatobi@gmail.com
Notes: this is digital forensic assignment

Organization
Organization analysis is being done for: University of Hertfordshire

Figure 2: Optional Information

2.1.3 Selecting of Host

A hostname was selected to automatically generate a new hostname using the data source name. ***(see figure 3)***


Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

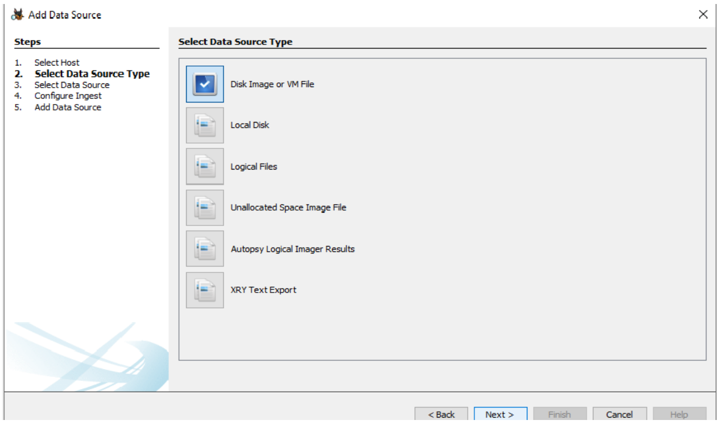
○ Specify new host name

○ Use existing host

Figure 3: select Host

2.1.4 Selecting Data Source Type

Selecting a disk image in Autopsy for analysis ensures a complete copy of the original storage device, preserving evidence integrity. Disk images contain all relevant data for thorough forensic examination, enabling investigators to uncover valuable information and build strong cases. This approach is essential for effective forensic analysis of image files. ***(see figure 4)***



Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

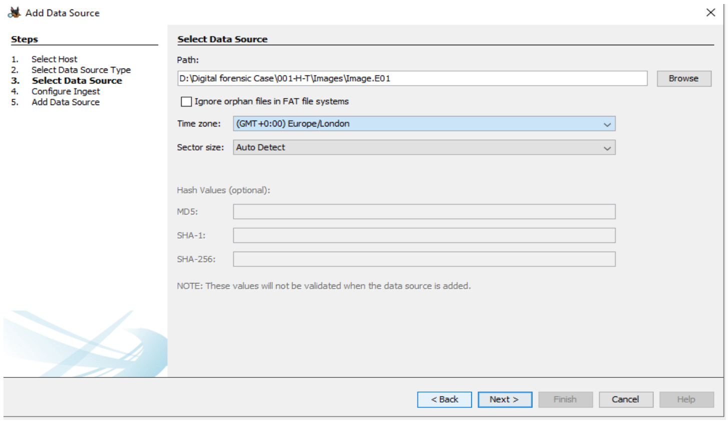
Select Data Source Type

- ☑ Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Figure 4: select Data Source Type

2.1.5 Selecting Data Source

The image file "image.E01" was selected from a specific path on the hard drive (refer to the figure). The Time zone was configured to (GMT+00) Europe/London to match the geographical location of the forensic investigation site. ***(see figure 6)***



Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: D:\Digital forensic Case\001-H-T\Images\Image.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/London

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

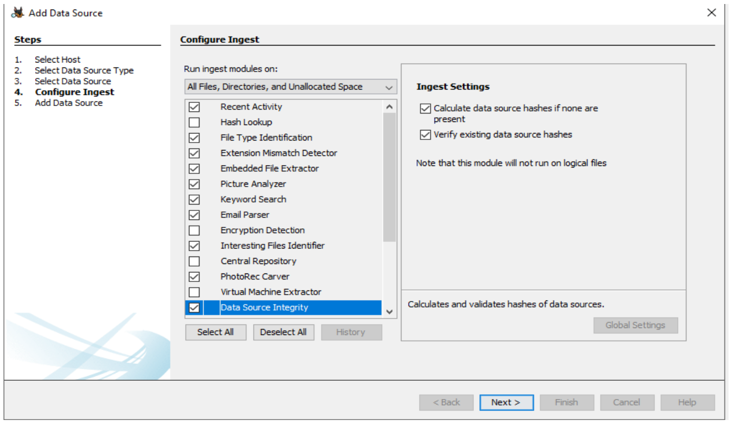
SHA-256:

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

Figure 5: Select Data Source

2.1.6 Configure Ingest

Configuring Autopsy digital forensic tool involves selecting modules like Recent Activity, File Type Identification, Extension Mismatch Detector, Embedded File Extractor, Picture Analyzer, Keyword Search, Email Parser, Interesting Files Identifier, PhotoRec Carver, and Data Source Integrity to efficiently analyse data and extract insights during investigations *(see figure 5)*. These modules help forensic analysts identify important information, detect anomalies, and recover valuable evidence from the digital sources. Autopsy's comprehensive suite of tools enables thorough examination of digital evidence, aiding in the investigation process and providing crucial support in solving cases.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

☑ Recent Activity
☐ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Picture Analyzer
☑ Keyword Search
☑ Email Parser
☐ Encryption Detection
☑ Interesting Files Identifier
☐ Central Repository
☑ PhotoRec Carver
☐ Virtual Machine Extractor
☑ Data Source Integrity

Ingest Settings

☑ Calculate data source hashes if none are present
☑ Verify existing data source hashes

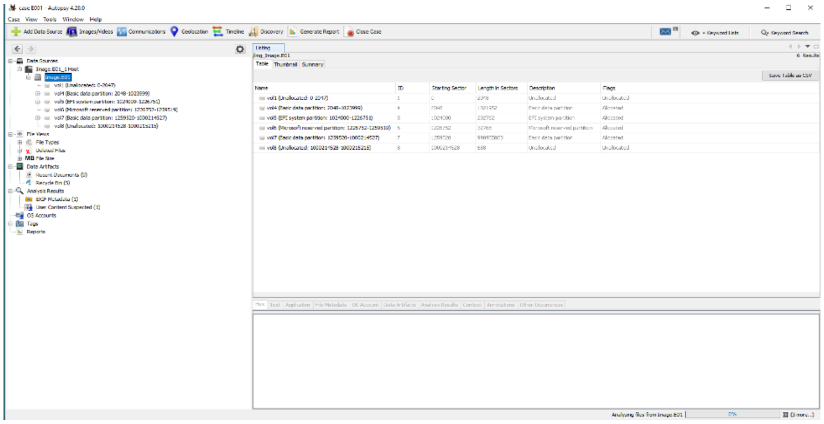
Note that this module will not run on logical files

Calculates and validates hashes of data sources.

Figure 6: Configure Ingest

3.0 EVIDENCE ANALYSIS

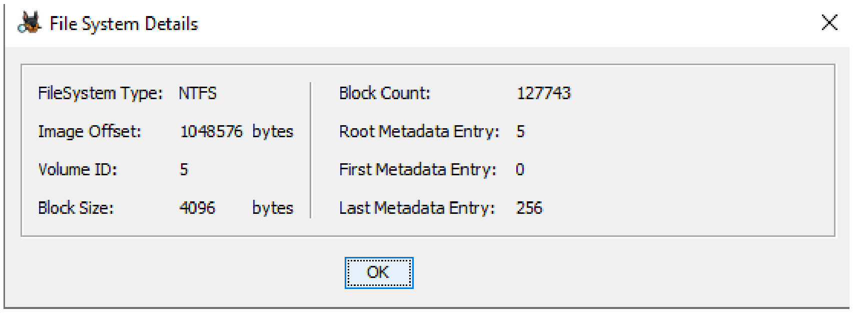
3.1 Partitions and system File Types: The examination of the forensic image uncovered multiple partitions on the hard disk, revealing the file system structure. Upon further analysis of the partitions, it was observed that volume 1 is currently unallocated, *(as depicted in Figure 7)*. Unallocated space on a hard drive is the area available for users to store new files. This unallocated space, also known as free space, can be utilized to store various types of data without any restrictions. Conversely, the portion of the hard drive that already contains files is referred to as "allocated space" (threat.media, 2023).



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

Figure 7: shows the system partitions

Volumes 4, and 7 contain NTFS, *(as shown in Figure 7,8, and 10)*. The NT file system (NTFS), sometimes referred to as the New Technology File System, is a method used by the Windows NT operating system to efficiently store, organize, and locate files on a hard disk. NTFS was initially introduced in 1993. (Weiss, 2022).

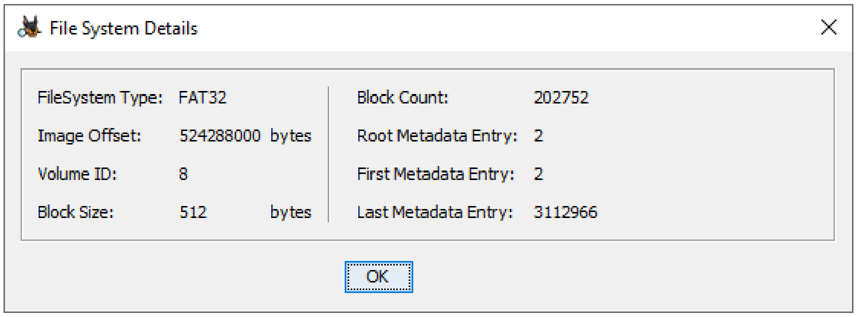


File System Details

FileSystem Type:	NTFS	Block Count:	127743
Image Offset:	1048576 bytes	Root Metadata Entry:	5
Volume ID:	5	First Metadata Entry:	0
Block Size:	4096 bytes	Last Metadata Entry:	256

Figure 8: File System Volume 4

Volume 5 contains FAT32 (as seen in Figures 7 and 9). FAT32 is an outdated file system that is less efficient than NTFS and lacks support for a variety of functions. However, it is more compatible with other operating systems. FAT32 is the oldest of the three file systems accessible to Windows, having been introduced in Windows 95 to replace the previous FAT16 file system used in MS-DOS and early versions of Windows (Hoffman & Lewis, 2023).

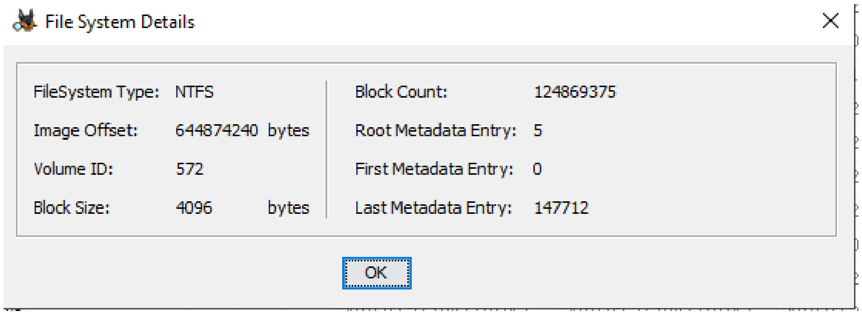


File System Details

FileSystem Type:	FAT32	Block Count:	202752
Image Offset:	524288000 bytes	Root Metadata Entry:	2
Volume ID:	8	First Metadata Entry:	2
Block Size:	512 bytes	Last Metadata Entry:	3112966

Figure 9: File System Volume 5

Volume 6 is a Microsoft reserved partition *(see figure 7)*, When you clean install Windows 7/8/10, the System Reserved partition appears before the system partition (usually the C: disc). Because Windows seldom assigns a drive letter to the System Reserved partition, you'll only see it when you use Disc Management or a similar application. (Linda, 2023)



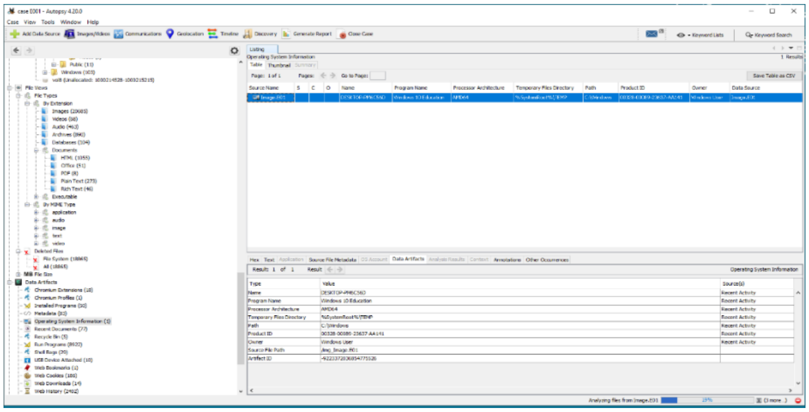
File System Details

FileSystem Type:	NTFS	Block Count:	124869375
Image Offset:	644874240 bytes	Root Metadata Entry:	5
Volume ID:	572	First Metadata Entry:	0
Block Size:	4096 bytes	Last Metadata Entry:	147712

Figure 10: File System volume 7

Volume 8 is labeled unallocated *(see figure 7)*, unallocated space does not necessarily mean empty. When people delete files on their computer it is not really erased from the hard drive. Instead, the space is merely labeled unallocated and available for other files (See figure 7). The deleted file’s data is still there, although it can be overwritten by new data when the space is reused. (threat.media, 2023)

3.2 Operating System Installations: The image contained evidence of Windows operating system installation**.** The system is running Windows 10 Education on an AMD64 processor architecture. The operating system files are in the c:directory. The product ID for this installation is 00328-00089-23637-AA141. The owner of the system is identified as a Windows User. The source file path for the system is /img_Image.E01, and the artifact ID is -9223372036854775527. *(see figure 11)*



Operating System Information

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Data Source
Image.E01				DESKTOP-PM6C56D	Windows 10 Education	AMD64	%SystemRoot%\TEMP	C:\Windows	00328-00089-23637-AA141	Windows User	Image.E01

Result: 1 of 1 — Operating System Information

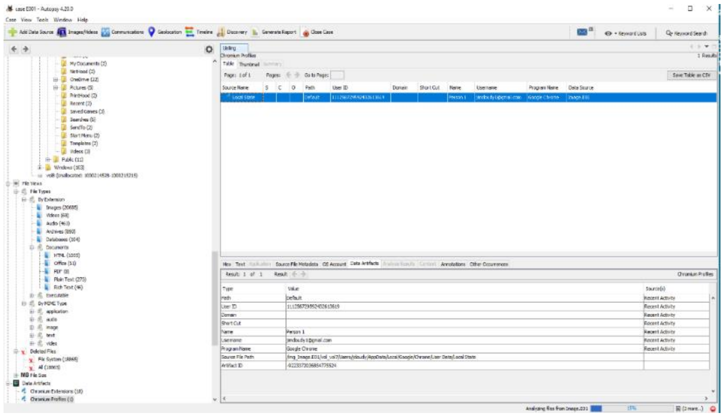
Type	Value	Source(s)
Name	DESKTOP-PM6C56D	Recent Activity
Program Name	Windows 10 Education	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00328-00089-23637-AA141	Recent Activity
Owner	Windows User	Recent Activity
Source File Path	/img_Image.E01	
Artifact ID	-9223372036854775526	

Figure 11: Operating system(OS) installation information

3.3 Time Zone Settings: In the digital forensic case, images were found in path F:forensic case01-H-T.E01. The time zone is (GMT+0:00) Europe/London, with sector size set to auto-detect for analysis. *(see figure 6)*

3.4 User Profiles: Person 1 is a user with a default profile in Google Chrome (Profile ID: 111256729592432613619) who uses the email jimcloudy1@gmail.com. Their profile image path is located at /img_Image.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Local State, and they have bookmarks saved in their browser *(see Figure 11)*.

Person 1 appears to be an individual who utilizes Google Chrome for browsing activities*(see Figure 12)*, potentially with a personalized profile for their online interactions. The presence of bookmarks suggests that they may frequently access specific websites or pages for convenience or reference. The use of a distinct email address and profile image path indicates a level of customization and organization in their online presence.



Chromium Profiles

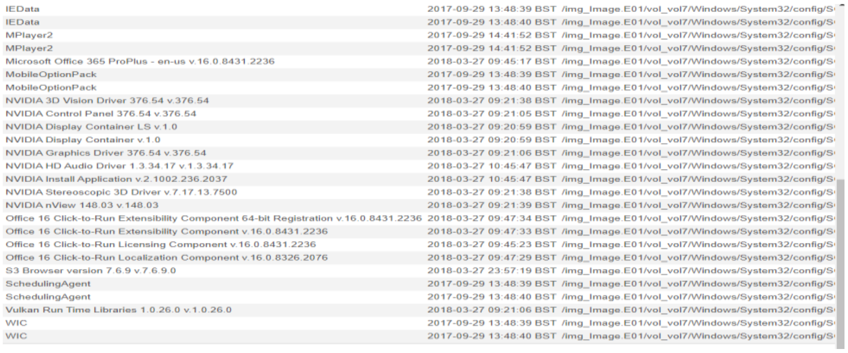
Source Name	S	C	O	Path	User ID	Domain	Short Cut	Name	Username	Program Name	Data Source
Local State				Default	111256729592432613619			Person 1	jimcloudy1@gmail.com	Google Chrome	Image.E01

Result: 1 of 1 — Chromium Profiles

Type	Value	Source(s)
Path	Default	Recent Activity
User ID	111256729592432613619	Recent Activity
Domain		Recent Activity
Short Cut		Recent Activity
Name	Person 1	Recent Activity
Username	jimcloudy1@gmail.com	Recent Activity
Program Name	Google Chrome	Recent Activity
Source File Path	/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Local State	
Artifact ID	-9223372036854775524	

Figure 12: User Profile base on Internet

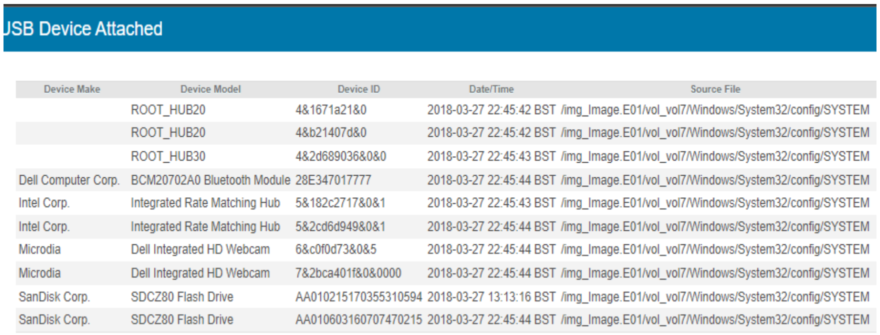
3.5. Software Program Installations: The presence of "Schedulingagent," "MobileOptionPack," "IEData," "DirectDrawEX," and "DXM_Runtime" *(see Figure 13).* in the installed programs on the hard drive indicates potential hacking tools used for executing a Trojan attack*(see figure III)*. These programs may be utilized to compromise system security and infiltrate sensitive data, posing a significant threat to the system's integrity *(see figure II)*.



IEData	2017-09-29 13:48:39 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
IEData	2017-09-29 13:48:40 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
MPlayer2	2017-09-29 14:41:52 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
MPlayer2	2017-09-29 14:41:52 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
Microsoft Office 365 ProPlus - en-us v.16.0.8431.2236	2018-03-27 09:45:17 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
MobileOptionPack	2017-09-29 13:48:39 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
MobileOptionPack	2017-09-29 13:48:40 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA 3D Vision Driver 376.54 v.376.54	2018-03-27 09:21:38 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA Control Panel 376.54 v.376.54	2018-03-27 09:21:05 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA Display Container LS v.1.0	2018-03-27 09:20:59 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA Display Container v.1.0	2018-03-27 09:20:59 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA Graphics Driver 376.54 v.376.54	2018-03-27 09:21:06 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA HD Audio Driver 1.3.34.17 v.1.3.34.17	2018-03-27 10:45:47 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA Install Application v.2.1002.236.2037	2018-03-27 10:45:47 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA Stereoscopic 3D Driver v.7.17.13.7500	2018-03-27 09:21:38 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
NVIDIA nView 148.03 v.148.03	2018-03-27 09:21:39 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
Office 16 Click-to-Run Extensibility Component 64-bit Registration v.16.0.8431.2236	2018-03-27 09:47:34 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
Office 16 Click-to-Run Extensibility Component v.16.0.8431.2236	2018-03-27 09:47:33 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
Office 16 Click-to-Run Licensing Component v.16.0.8431.2236	2018-03-27 09:45:23 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
Office 16 Click-to-Run Localization Component v.16.0.8326.2076	2018-03-27 09:47:29 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
S3 Browser version 7.6.9 v.7.6.9.0	2018-03-27 23:57:19 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
SchedulingAgent	2017-09-29 13:48:39 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
SchedulingAgent	2017-09-29 13:48:40 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
Vulkan Run Time Libraries 1.0.26.0 v.1.0.26.0	2018-03-27 09:21:06 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
WIC	2017-09-29 13:48:39 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S
WIC	2017-09-29 13:48:40 BST	/img_Image.E01/vol_vol7/Windows/System32/config/S

Figure 13: Software Installed relevant to the investigation

3.6 Hardware Devices: On March 27, 2018, at the specified time and date, various hardware devices were connected to the system, including ROOT_HUB20 and ROOT_HUB30, Dell Bluetooth Module, Intel Integrated Rate Matching Hub, Microdia Dell Integrated HD Webcam, and SanDisk Flash Drives. The device information was recorded in the system configuration file located at /img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM. This data can provide insights into the connected peripherals and their configurations during the forensic investigation of the system at that moment *(see figure 14)*.



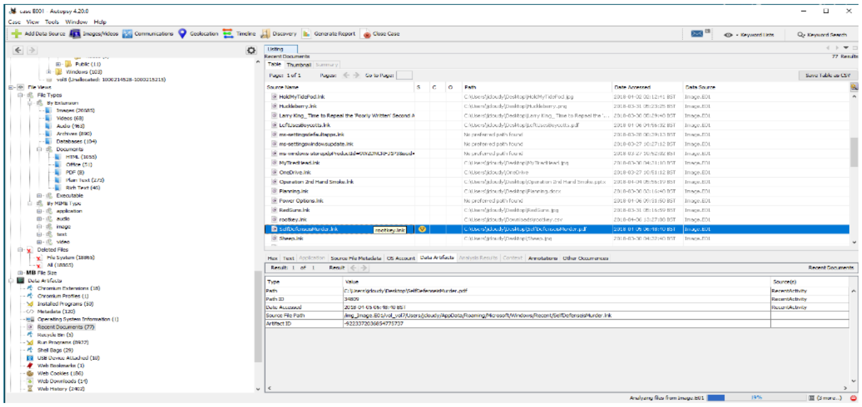
JSB Device Attached

Device Make	Device Model	Device ID	Date/Time	Source File
	ROOT_HUB20	4&1671a21&0	2018-03-27 22:45:42 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
	ROOT_HUB20	4&b21407d&0	2018-03-27 22:45:42 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
	ROOT_HUB30	4&2d689036&0&0	2018-03-27 22:45:43 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
Dell Computer Corp.	BCM20702A0 Bluetooth Module	28E347017777	2018-03-27 22:45:44 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
Intel Corp.	Integrated Rate Matching Hub	5&182c2717&0&1	2018-03-27 22:45:43 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
Intel Corp.	Integrated Rate Matching Hub	5&2cd6d949&0&1	2018-03-27 22:45:44 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
Microdia	Dell Integrated HD Webcam	6&c0f0d73&0&5	2018-03-27 22:45:44 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
Microdia	Dell Integrated HD Webcam	7&2bca401f&0&0000	2018-03-27 22:45:44 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
SanDisk Corp.	SDCZ80 Flash Drive	AA010215170355310594	2018-03-27 13:13:16 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM
SanDisk Corp.	SDCZ80 Flash Drive	AA010603160707470215	2018-03-27 22:45:44 BST	/img_Image.E01/vol_vol7/Windows/System32/config/SYSTEM

Figure 14: Hardware Devices connected to the investigated system

3.7 Other Findings: Additional findings such as deleted files, recent documents, and web search were noted.

3.7.1 Recent documents: there are seventy-seven (77) files in the recent file, including additions related to the investigation such as "Cloudy Thoughts," "Planning," "Airport Information," "Amen," "Operation 2nd Hand Smoke," "Cloudy Manifesto," and "UKBanKnife." *(see figure 15)*



Source Name	S	C	O	Path	Date Accessed	Data Source
HoldMyTidePod.lnk				C:\Users\jcloudy\Desktop\HoldMyTidePod.jpg	2018-04-02 02:12:41 BST	Image.E01
Huckleberry.lnk				C:\Users\jcloudy\Desktop\Huckleberry.png	2018-03-31 05:23:25 BST	Image.E01
Larry King_ Time to Repeal the 'Poorly Written' Second A				C:\Users\jcloudy\Desktop\Larry King_ Time to Repeal the '...	2018-03-30 05:29:40 BST	Image.E01
LeftUsesBoycotts.lnk				C:\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf	2018-04-06 04:56:32 BST	Image.E01
ms-settingsdefaultapps.lnk				No preferred path found	2018-03-28 00:39:13 BST	Image.E01
ms-settingswindowsupdate.lnk				No preferred path found	2018-03-27 10:27:12 BST	Image.E01
ms-windows-store:pdp?productId=9WZDNCRFJ3PS&ocid=				No preferred path found	2018-03-27 10:52:02 BST	Image.E01
MyTiredHead.lnk				C:\Users\jcloudy\Desktop\MyTiredHead.jpg	2018-03-30 04:31:10 BST	Image.E01
OneDrive.lnk				C:\Users\jcloudy\OneDrive	2018-03-27 10:51:12 BST	Image.E01
Operation 2nd Hand Smoke.lnk				C:\Users\jcloudy\Desktop\Operation 2nd Hand Smoke.pptx	2018-04-04 05:56:19 BST	Image.E01
Planning.lnk				C:\Users\jcloudy\Desktop\Planning.docx	2018-03-30 03:16:40 BST	Image.E01
Power Options.lnk				No preferred path found	2018-04-06 09:31:50 BST	Image.E01
RedGuns.lnk				C:\Users\jcloudy\Desktop\RedGuns.jpg	2018-03-31 05:16:59 BST	Image.E01
rootkey.lnk				C:\Users\jcloudy\Downloads\rootkey.csv	2018-04-06 13:27:08 BST	Image.E01
SelfDefenseisMurder.lnk				C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	2018-04-05 06:48:40 BST	Image.E01
Sheep.lnk				C:\Users\jcloudy\Desktop\Sheep.jpg	2018-03-30 04:32:40 BST	Image.E01

Type	Value	Source(s)
Path	C:\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf	RecentActivity
Path ID	34809	RecentActivity
Date Accessed	2018-04-05 06:48:40 BST	RecentActivity
Source File Path	/img_Image.E01/vol_vol7/Users/jcloudy/AppData/Roaming/Microsoft/Windows/Recent/SelfDefenseisMurder.lnk	
Artifact ID	-9223372036854775737	

Figure 15: Recent document added on the hard drive image

3.7.2 Deleted file: Several files, including articles on gun control by Anthony Rizzo and Larry King, along with an image named DemGun.jpg, were deleted on April 5th and 6th, 2018, with their original locations in the Recycle Bin *(see figure 16 and 17)*. These deletions suggest a potential cleanup or reorganization of digital content.

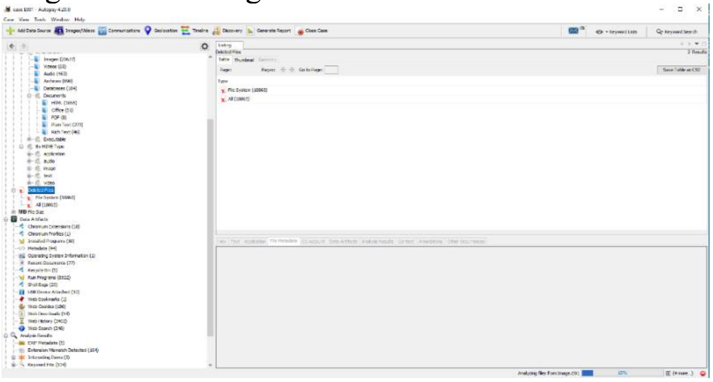
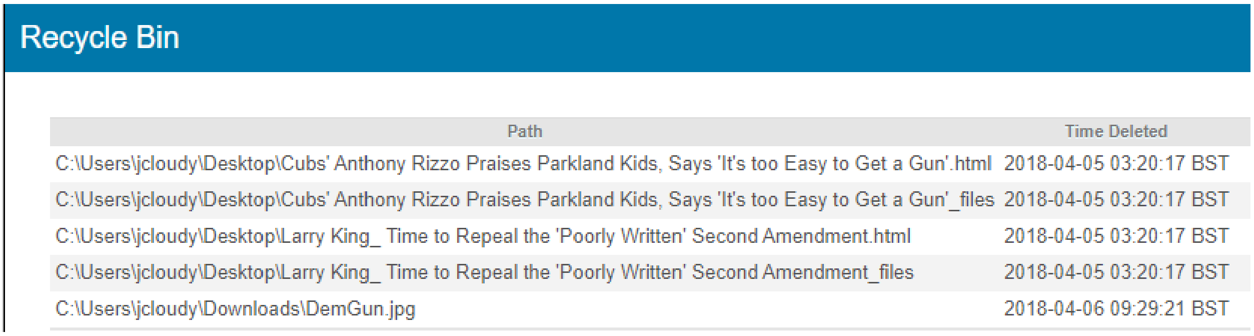


Figure 16: Deleted files

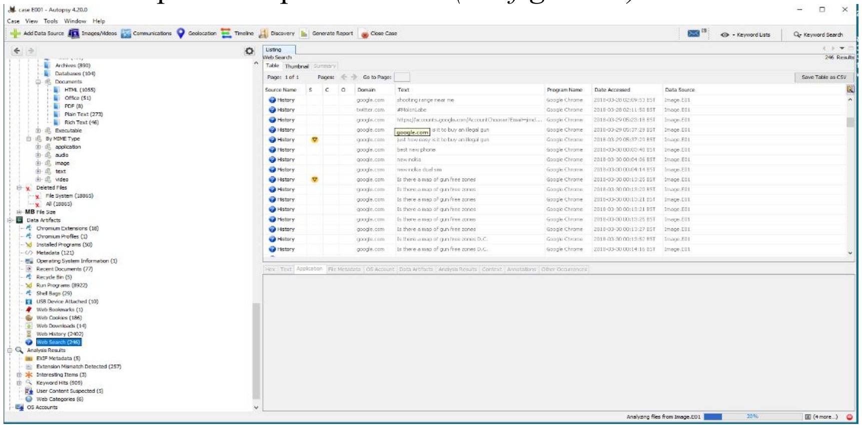


Recycle Bin

Path	Time Deleted
C:\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html	2018-04-05 03:20:17 BST
C:\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'_files	2018-04-05 03:20:17 BST
C:\Users\jcloudy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html	2018-04-05 03:20:17 BST
C:\Users\jcloudy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment_files	2018-04-05 03:20:17 BST
C:\Users\jcloudy\Downloads\DemGun.jpg	2018-04-06 09:29:21 BST

Figure 17: content inside the deleted file related to the investigation

3.7.3 **Web search:** There are two hundred and forty-six (246) files within the web search results stored on the hard drive, with some related to the investigation, such as "430 South Capital Street, DC," "9mm rifles," "Can you defend yourself from burglars in London," "Is there a map of gun-free zones," "Northern Virginia Gun Works," "There would be a rifle behind every blade of grass," "Airports near DC," "anti-gun rally near me," "Can I strap cash to myself and walk through TSA," "Can I tape cash to myself and walk through TSA," "Gun control in Indonesia," "Gun store near me," "Just how easy is it to buy an illegal gun," "Which DC airport has the fewest delays," and "Which state has the worst police response times."*(see figure 18)*



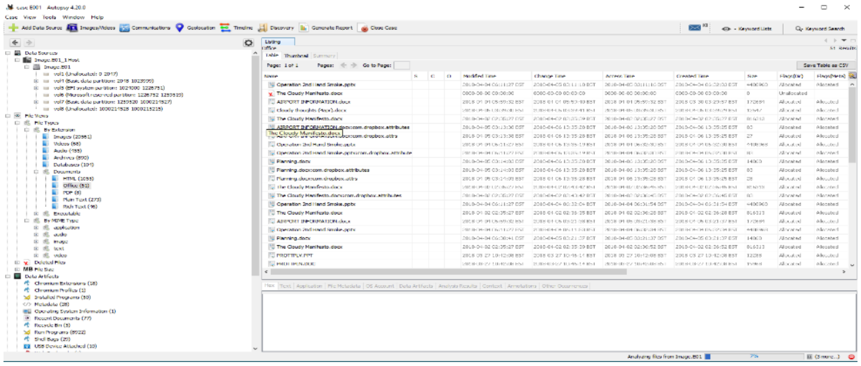
Web Search — 246 Results

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	shooting range near me	Google Chrome	2018-03-28 02:09:53 BST	Image.E01
History				twitter.com	#MolonLabe	Google Chrome	2018-03-28 02:11:50 BST	Image.E01
History				google.com	https://accounts.google.com/AccountChooser?Email=jmd...	Google Chrome	2018-03-29 05:23:18 BST	Image.E01
History				google.com	google.com is it to buy an illegal gun	Google Chrome	2018-03-29 05:37:29 BST	Image.E01
History	▽			google.com	just how easy is it to buy an illegal gun	Google Chrome	2018-03-29 05:37:20 BST	Image.E01
History				google.com	best new phone	Google Chrome	2018-03-30 00:03:40 BST	Image.E01
History				google.com	new nokia	Google Chrome	2018-03-30 00:04:06 BST	Image.E01
History				google.com	new nokia dual sim	Google Chrome	2018-03-30 00:04:14 BST	Image.E01
History	▽			google.com	Is there a map of gun free zones	Google Chrome	2018-03-30 00:13:25 BST	Image.E01
History				google.com	Is there a map of gun free zones	Google Chrome	2018-03-30 00:13:20 BST	Image.E01
History				google.com	Is there a map of gun free zones	Google Chrome	2018-03-30 00:13:21 BST	Image.E01
History				google.com	Is there a map of gun free zones	Google Chrome	2018-03-30 00:13:21 BST	Image.E01
History				google.com	Is there a map of gun free zones	Google Chrome	2018-03-30 00:13:25 BST	Image.E01
History				google.com	Is there a map of gun free zones	Google Chrome	2018-03-30 00:13:27 BST	Image.E01
History				google.com	Is there a map of gun free zones D.C.	Google Chrome	2018-03-30 00:13:52 BST	Image.E01
History				google.com	Is there a map of gun free zones D.C.	Google Chrome	2018-03-30 00:14:16 BST	Image.E01

Figure 18: Web Search

4.0 FINDINGS

Upon investigation of the digital evidence retrieved from the suspect's system on 10/04/2024, several alarming discoveries were made. The digital evidence retrieved from the suspect's system paints a chilling picture of a meticulously planned and potentially imminent threat against the government. The attacker's attempt to access an illegal site, "pshingsiteedge,"*(see appendix IV)* triggering a threat warning, indicates a willingness to engage in illicit activities to further their nefarious intentions. Within the office files, the presence of Airport Information containing details relevant to the planned attack suggests a strategic focus on logistical aspects to ensure the success of the operation *(see figure 19)*.



Office

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
Operation 2nd Hand Smoke.pptx				2018-04-04 06:11:27 BST	2018-04-05 03:11:10 BST	2018-04-05 03:11:10 BST	2018-04-04 06:32:03 BST	4400960	Allocated	Allocated
The Cloudy Manifesto.docx				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	Unallocated	
AIRPORT INFORMATION.docx				2018-04-01 05:59:32 BST	2018-04-01 05:59:10 BST	2018-04-01 05:59:32 BST	2018-03-30 03:29:57 BST	172691	Allocated	Allocated
Cloudy thoughts (4age).docx				[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Allocated	Allocated
The Cloudy Manifesto.docx				2018-04-02 02:35:27 BST	2018-04-02 02:35:29 BST	2018-04-02 02:35:27 BST	2018-04-02 02:35:27 BST	816313	Allocated	Allocated
AIRPORT INFORMATION.docx:com.dropbox.attributes				2018-04-05 03:13:38 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated	Allocated
The Cloudy Manifesto.docx ...docx:com.dropbox.attrs				2018-04-05 03:13:38 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	27	Allocated	Allocated
Operation 2nd Hand Smoke.pptx				2018-04-04 06:11:27 BST	2018-04-06 13:35:19 BST	2018-04-04 06:32:30 BST	2018-04-04 06:32:30 BST	4400960	Allocated	Allocated
Operation 2nd Hand Smoke.pptx:com.dropbox.attribute				[illegible]	[illegible]	[illegible]	[illegible]	83	Allocated	Allocated
Planning.docx				2018-04-05 03:14:03 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	14063	Allocated	Allocated
Planning.docx:com.dropbox.attributes				2018-04-05 03:14:03 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated	Allocated
Planning.docx:com.dropbox.attrs				2018-04-05 03:14:03 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated	Allocated
The Cloudy Manifesto.docx				[illegible]	[illegible]	[illegible]	[illegible]	816313	Allocated	Allocated
The Cloudy Manifesto.docx:com.dropbox.attributes				2018-04-02 02:35:27 BST	2018-04-02 02:43:42 BST	2018-04-02 02:36:45 BST	2018-04-02 02:36:45 BST	83	Allocated	Allocated
Operation 2nd Hand Smoke.pptx				2018-04-04 06:11:27 BST	2018-04-04 06:32:04 BST	2018-04-04 06:31:54 BST	2018-04-04 06:31:54 BST	4400960	Allocated	Allocated
The Cloudy Manifesto.docx				2018-04-02 02:35:27 BST	2018-04-02 02:36:35 BST	2018-04-02 02:36:28 BST	2018-04-02 02:36:28 BST	816313	Allocated	Allocated
AIRPORT INFORMATION.docx				2018-04-01 05:59:32 BST	2018-04-05 03:21:38 BST	2018-04-05 03:21:38 BST	2018-04-05 03:21:37 BST	172691	Allocated	Allocated
Operation 2nd Hand Smoke.pptx				[illegible]	[illegible]	[illegible]	[illegible]	4400960	Allocated	Allocated
Planning.docx				2018-04-04 06:30:41 BST	2018-04-05 03:21:37 BST	2018-04-05 03:21:37 BST	2018-04-05 03:21:37 BST	14063	Allocated	Allocated
The Cloudy Manifesto.docx				2018-04-02 02:35:27 BST	2018-04-02 02:35:39 BST	2018-04-02 02:36:52 BST	2018-04-02 02:36:52 BST	816313	Allocated	Allocated
PROTTPLV.PPT				2018-03-27 10:12:08 BST	2018-03-27 10:16:14 BST	2018-03-27 10:12:08 BST	2018-03-27 10:12:08 BST	12288	Allocated	Allocated
PROTTPLN.DOC				[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Allocated	Allocated

Figure 19: Evidence present in the office file

Furthermore, the communication within the office files revealing discussions about the weather being favorable for the attack and mentioning a key individual named "PAUL" *(see figure 18)* hints at a coordinated effort involving multiple parties. A file named cloudy manifesto and cloudy thought outlining plans to launch an attack on the government and escape using the fastest airline underscores the attacker's determination and calculated approach to carrying out their sinister agenda.

The files labeled "Operation 2nd hand smoke" and "Planning" *(see figure 18)* provide specific details of the attack plan, including targets and supplies, indicating a well-thought-out strategy. The use of IRM protection to secure certain files demonstrates a level of sophistication in maintaining secrecy and avoiding detection. Additionally, the PDF files titled "AMEN," "SelfDefenseisMurder," and "UKknifeBan" *(see figure 19)* offer further insight into the attacker's mindset and strategies, shedding light on potential motivations and ideologies driving their actions.

Moreover, the identification of installed programs on the hard drive as hacking tools for executing a Trojan attack *(see Appendix II*) raises concerns about the attacker's capabilities and intent to cause harm through malicious means. Considering these alarming findings, swift and decisive action is imperative to prevent potential harm and ensure the safety and security of the public.

5.0 CONCLUSIONS

In conclusion, based on the findings of the investigation, it is evident that the attacker poses a significant threat to national security. Law enforcement agencies must act swiftly to apprehend the suspect and prevent any planned attacks from being carried out. The detailed planning and intent displayed in the digital evidence highlight the urgency of the situation and the need for proactive measures to safeguard against potential harm.

REFERENCES

Adrien, D., Tanguy, G., Emmanuel, G. & Christophe, R., 2023. File type identification tools for digital investigations. *Forensic Science International: Digital Investigation,* 46(dubettier2023file), p. 301574.

Baroto, W. A. & Prasetyo, A. H., 2020. Digital forensic process in fraud investigation: A case study on email analysis. *International Journal of Scientific Engineering and Science,* 2(baroto2020digital), pp. 36--40.

Hoffman, C. & Lewis, N., 2023. *howtogeek.* [Online]
Available at: https://www.howtogeek.com/
[Accessed 30 march 2024].

Linda, 2023. *What Is System Reserved Partition and Can You Delete It?.* [Online]
Available at: https://www.minitool.com
[Accessed 9 April 2024].

Mahmoud, K., Youssef, I. & Jones, A., 2013. Phishing detection: a literature survey. *IEEE Communications Surveys \& Tutorials,* 15(IEEE), pp. 2091--2121.

threat.media, 2023. *threat.media.* [Online]
Available at: https://threat.media/definition/what-is-unallocated-space/#:~:text=Unallocated%20space%20refers%20to%20the,is%20called%20%E2%80%9Callocated%20space.%E2%80%9D
[Accessed 30 March 2024].

Weiss, D., 2022. *datto.* [Online]
Available at: https://www.datto.com/
[Accessed 30 march 2024].

ZHU, Z., 2015. Study on computer trojan horse virus and its prevention. *International Journal of Engineering and Applied Sciences,* 2(Engineering Research Publication), p. 257840.

APPENDIX I

Forensic Analysis Contemporaneous Notes

Case Reference:22060310 (Oluwatobi Elijha Akanni)
Case Type: Image Disk
Analyst Name: Oluwatobi Elijah Akanni
Analyst Agency: Digital Forensic
Client Name: Case 01
Client Agency: University of Hertfordshire
Client Contact:
Case Started: 10/04/2024 - 17:45
Last Modified: 10/04/2024 - 19:02
Case Status: Initiated

10/04/2024 19:02:08

CASE NOTE

FORENSIC TOOL USED

Autopsy 4.21.0

CASE INFORMATION

17:45 10/04/2024: Case Name case E01
17:45 10/04/2024: Base Directory: F:\Digital forensic case\001-H-T\Autopsy
17:45 10/04/2024: Case Type: Single user

OPTIONAL INFORMATION

17:46 10/04/2024 Case Number: 001
17:46 10/04/2024 Examiner Information: Oluwatobi Akanni, +447760990746, akannioluwatobi@gmail.com
17:46 10/04/2024: organisation: University of Hertfordshire

SELECTING OF HOST

17:47 10/04/2024: Generate new hostname based on data source and data source name

SELECTING DATA SOURCE TYPE

12:47 10/04/2024: Disk Image or VM File

SELECTING DATA SOURCE

17:47 10/04/2024: Path: F:\Digital forensic case\001-H-T\Images\Images.E01
17:48 10/04/2024: Time Zone: (GMT+0:00) Europe/London
17:48 10/04/2024: Sector Size: Auto Detect

CONFIGURE INGEST

17:48 10/04/2024: All the Ingest was selected

ADDING DATA SOURCE

17:49 10/04/2024: Data source was added

ANALYSING OF THE IMAGE

17:50 10/04/2024: the analysis of data started

PARTITIONS PRESENT IN THE IMAGE / FILE TYPES

17:52 10/04/2024:
There are six (6) partitions present in the image disk and two different file types they are:

PARTITIONS	**FILE TYPE**
VOL1	unallocated

VOL4	NTFS
VOL5	FAT32
VOL6	NTFS
VOL7	NTFS
VOL8	unallocated

OPERATING SYSTEM (OS) INSTALLED

17:54 10/04/2024:
WINDOWS 10 EDUCATION is the OS running on the disk image, this was seen under the Data Artifacts in the operating system information

KEYWORD SEARCH

cloudy
murder
kill
bomb

FILE TYPE BY EXTENSION

17:56 10/04/2024: File types were also check, narrowing it down to by Extension(in the extension, Images (20455), Video (68), Audio (455), Archives (889), database(104)
was found in the Extension.

DOCUMENTS

17:57 10/04/2024: Documents, under the document there are five (5) files under the document named, HTML(994), office(51), PDF (8), Plain text (273), Rich Text (46).

17: 58 10/04/2024: on the HTML file the user tries to enter some illegal site e.g. pshingsiteedge which came out as a warning that it contains a threat.

17:59 10/04/2024: on the office which contains 51 files, the user has an office file containing Airport records named "AIRPORT INFORMATION"

18:04 10/04/2024: on the office file, the user was communicating with a person, and he got a message that the weather was bad, and it was good for the attack, which means they were planning to conduct an attack. Also, the attacker made mention of a particular name "PAUL"(who is Paul: Paul is holding the other key to the attacker plan)

18:08 10/04/2024: The attacker created a cloudy manifesto and cloudy thought; the attacker talks about governments not being able to protect the country, which means he is launching an attack on the government. and after finishing his attack, the attacker plans to escape by a faster airline, that has low delay time, which is why he got airport information.

18:11 10/04/2024: The attacker save another file as Operation 2nd hand smoke: which state the Event (attack) time: 1230 - 1400.

18:15 10/04/2024: The attacker has another file save as Planning, the attacker listed what he intends to do. e.g., the Target, supplies, Ammo, and Release.

18:17 10/04/2024: The attacker uses IRM protection to protect some files.

18:17 10/04/2024: Under the PDF folder on the attacker system, there is a PDF file saved as AMEN in the PDF, the title was theblaze which stated, "You can't fight the government'? It's time to debunk this popular anti-gun talking point".

18:19 10/04/2024: A PDF file titled SelfDefenseisMurder was saved, discussing strategies for defending oneself from a potential murder. The attacker seeks a guide on post-attack defense tactics, using it as a case study for planning future attacks if caught.

18:22 10/04/2024: Also there was another file named as UKknifeBan.

NOTE: Folders that were not referenced do not have any relevant information about the investigation.

DELETED FILE

18:24 10/04/2024: When focusing on the deleted file within the file system, there are (18445) instances where all files have been deleted from the system, totaling 18445 deletions.

MB FILE SIZE

18:26 10/04/2024: the MB file size MB 50-200(mb) (34)
18:26 10/04/2024: MB 200(mb) - 1(GB)(10)
18:26 10/04/2024: MB 1GB+ (6)

DATA ARTIFACTS

18:29 10/04/2024:
INSTALLED PROGRAMS

- Schedulingagent
- MobileOptionPack
- IEData
- DirectDrawEX
- DXM_Runtime

Note: these are part of the installed programs on the hard drive, the installed programs listed are on the hard drive and they are hacking tools used for executing a Trojan attack on a system.

METADATA

18:30 10/04/2024:
There are one hundred and twenty-one (121) files in the metadata.

OPERATING SYSTEM (OS) INFORMATION

18:33 10/04/2024:

TYPE	**VALUE**
Name	DESKTOP-PM6c56D
Program Name	Windows 10 Education
Processor Architecture	AMD64
Path	c:\Windows
Product ID	00328-00089-23637-AA141
Owner	Windows User
Source File Path	/img_Image.E01
Artifact ID	-9223372036854775527

RECENT DOCUMENTS

18:35 10/04/2024:
There are a total of seventy-seven (77) files in the recent file. Among the recent additions linked to the investigation are files named "Cloudy Thoughts," "Planning," "Airport Information," "Amen," "Operation 2nd Hand Smoke," "Cloudy Manifesto," and "UKBanKnife."
NOTE: the recent file displays documents that have been recently added to the hard drive.

RECYCLE BIN

18:37 10/04/2024:
There are five (5) files in the recycle bin, which are: “Cubs' Anthony Rizzo Praises Parkland Kids, says 'It's too Easy to Get a Gun'”, “Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html”, “DemGun” this are the file that is connected to the investigation.

WEB COOKIES

18:39 10/04/2024:
There are one hundred and eighty-six (186) web cookies found on the hard drive which none are related to the investigation.

WEB HISTORY

18:42 10/04/2024:
These are a few of the web history that is connected to the investigation, found on the hard drive.

- file:///C:/Users/jcloudy/Desktop/AIRPORT%20INFORMATION.docx
- file:///C:/Users/jcloudy/Desktop/AMEN.pdf
- file:///C:/Users/jcloudy/Desktop/Cloudy%20thoughts%20(4apr).docx
- file:///C:/Users/jcloudy/Desktop/Planning.docx
file:///C:/Users/jcloudy/Desktop/Operation%202nd%20Hand%20Smoke.pptx,
- file:///C:/Users/jcloudy/Desktop/RedGuns.jpg
- file:///C:/Users/jcloudy/Desktop/SelfDefenseisMurder.pdf
- ile:///C:/Users/jcloudy/Desktop/UKknifeBan.pdf
- file:///C:/Users/jcloudy/Downloads/DemGun.jpg
- http://www.dailykos.com/stories/2017/4/17/1653154/-DNC-DCCC-DSCC-How-to-decipher-the-alphabet-soup-of-Democratic-Party-organizations
- http://traveltips.usatoday.com/travel-airline-cash-9937.html
- http://washington.cbslocal.com/2014/11/12/d-c-area-claims-some-of-best-and-worst-airports-for-delays/
- http://www.internationalman.com/articles/which-countries-can-the-nsa-whistleblower-escape-to
- http://www.politifact.com/florida/statements/2017/feb/21/richard-corcoran/do-most-mass-shootings-happen-gun-free-zones/

WEB DOWNLOAD
18:45 10/04/2024:
Among the fourteen downloads on the hard drive, only two files related to the investigation are image files named "RedGuns" and "DemGun."
WEB SEARCH
18:50 10/04/2024:
Within the web search results stored on the hard drive, there are two hundred and forty-six (246) files, some of which pertain to the investigation are listed below.

- 430 South Capital Street, DC
- 9mm rifles
- Can you defend yourself from burglars in london
- Is there a map of gun free zones
- Northern Virginia Gun Works
- There would be a rifle behind every blade of grass
- Airports near dc
- anti-gun rally near me
- Can I strap cash to myself and walk through tsa
- Can I tape cash to myself and walk through tsa
- Gun control in indonesia
- Gun store near me
- Just how easy is it to buy an illegal gun
- Which dc airport has fewest delays
- Which state has the worst police response times
- Why is there a timespan on my flight departure

REPORT GENERATED

18:52 10/04/2024: I generated Report after the file Analysis

· file:///F:/Digital%20forensic%20Case/001-H-T/Autopsy/case%20E001/Reports/case%20E001%20HTML%20Report%2004-09-2024-12-55-49/report.html

· file:///F:/Digital%20forensic%20Case/001-H-T/Autopsy/case%20E001/Reports/case%20E001%20HTML%20Report%2004-09-2024-12-56-34/report.html

FINDINGS NARRATION

The investigation has uncovered various pieces of digital evidence related to the recent activities on the hard drive, including recent documents, items in the recycle bin, web cookies, web history, web downloads, and web searches. Some notable findings include:

- The investigation commenced on April 10, 2024, at 17:45 with the selection of the data source type.
- The forensic image (E01) was successfully loaded into Autopsy at 17:47, with the time and location set to Europe/London.
- Ingest configuration was completed by selecting all data at 17:48, followed by the successful addition of the data source at 17:49.
- Image analysis began at 17:50, revealing 18,445 deleted files within the file system.
- File types were analyzed by extension, identifying 20,455 images, 68 videos, 455 audio files, 889 archives, and 104 databases.
- Specific images such as "Death.jpg" were identified with associations to Americans and timestamped actions in 2018.
- Document analysis unveiled HTML (994), office (51), PDF (8), plain text (273), and rich text (46) files.
- Noteworthy findings include attempts to access illegal sites in HTML files and communication regarding a planned airport attack in office documents.
- Detailed planning for attacks, including event times and target information, was discovered in various files (office file and PDF file).
- The use of IRM protection to safeguard specific files was noted during the investigation.
- Executable files were categorized by type and size, with varying distributions observed.
- These digital artifacts provide valuable insights into the user's online activities and interests that may be relevant to the investigation at hand.
- Recent documents with titles such as "Cloudy Thoughts," "Planning," "Airport Information," "Amen," "Operation 2nd Hand Smoke," "Cloudy Manifesto," and "UKBanKnife."
- Files in the recycle bin titled “Cubs' Anthony Rizzo Praises Parkland Kids, says 'It's too Easy to Get a Gun',” “Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html,” and “DemGun” are connected to the investigation.
- Web history entries related to documents like "AIRPORT INFORMATION.docx," "AMEN.pdf," "Cloudy thoughts (4apr).docx," "Planning.docx," "Operation 2nd Hand Smoke.pptx," "RedGuns.jpg," "SelfDefenseisMurder.pdf," and "UKknifeBan.pdf."
- Web searches for topics such as gun control, gun stores, anti-gun rallies, airport delays, and more.
- A comprehensive report was generated post-analysis, accessible at the provided URL.

APPENDIX II

Software Program Installations

To enhance the forensic investigation process, various tools and techniques can be implemented. Firstly, file type identification tools like TrID or DROID can be used to identify file types based on their signatures and headers. This helps in determining the format of ingested files (Adrien, et al., 2023). Secondly, an extension mismatch detector tool can be employed to check for inconsistencies between file extensions and actual file types, flagging potential issues with malicious files (Baroto & Prasetyo, 2020). Embedded file extractors like ExifTool or foremost can be utilized to extract hidden data from documents or images. Image analysis tools such as Tesseract OCR can be used for text extraction and steganography detection. Keyword search tools like grep or Autopsy's functionality can help in quickly identifying specific terms within data. Email parsing tools like Emailchemy can extract and analyze email content. Custom scripts or tools like Bulk Extractor can identify interesting files based on predefined criteria. PhotoRec can recover deleted files, and checksum verification tools like md5sum ensure data integrity during the ingest process.

APPENDIX III

Trojan Horse

A Trojan Horse Virus is a sort of malware that hides on a computer as a genuine program. The distribution technique often involves an attacker using social engineering to conceal harmful code into genuine applications to acquire system access through their product (ZHU, 2015).

APPENDIX IV

Phishing

A digital kind of social engineering in which individuals are sent authentic looking but phony e-mails requesting information or directed to a fake Web site that demands information. Using social engineering tactics to deceive consumers into visiting a bogus website and providing personal information (Mahmoud, et al., 2013)