

Introduction	2
Case Management	2
Preparation	2
Collection and Preservation	2
Examination and Analysis	2
Disseminating the Case	3
Presentation and Reporting	3
Evidence Analysis	3
Partitions in Forensics Image	3
Operating System in Forensics Image	4
Time Zone Settings in Forensics Image	4
Software Program Installations in Forensics Image	5
Hardware Devices Attached	5
User Email Activity	6
User Internet Activity	6
Personal Data Analysis	8
Findings and Conclusion	9
Operating System and User Access:	9
Time Zone Settings:	9
Suspicious Software Installations:	9
Attached Hardware Devices:	10
Email Activity:	10
Internet Activity:	10
Personal Document Analysis:	11
Conclusion:	11
Appendix	12
Preparation	12
Collection and Preservation	12
Examination and Analysis	12
Disseminating the Case	13
Contemporary Notes	13

Introduction

Digital Forensics is an essential part of cybersecurity. It refers to the collecting, analyzing the digital evidence in a way that maintains its integrity. Digital forensics is used to investigate cybercrimes but it can also help in criminal and civil investigations. With the increase in the usage of mobile phones, computers, and the use of mobile phones, computers in crime, the importance of digital forensics is growing rapidly.

Case Management

Case management is crucial in a digital forensics investigation to ensure that all evidence is properly handled, documented, and preserved. This case involves the analysis of a hard drive retrieved from a crime scene. The drive was divided into nine images, and each image was analyzed for forensic evidence to provide insights into the activities conducted on the system. Case management is divided into 5 steps:

Preparation

The investigator initiated the case by establishing a structured plan of action. This included assigning a distinct case name and setting up a secure environment for handling the digital evidence. The investigator also identified and validated the tools and methodologies to be used throughout the investigation, ensuring they were ready for deployment.

Collection and Preservation

In the collection phase, the investigator acquired the original digital evidence from the crime scene, taking measures to ensure its integrity. Forensic images of the data were then created to allow for detailed analysis while preserving the original evidence. These images were securely stored in a restricted-access location to protect them from unauthorized access or tampering. The investigator documented every step in the chain of custody, maintaining a clear and unbroken record of how the evidence was managed, even as the sole handler.

Examination and Analysis

During the examination and analysis phase, the investigator conducted a thorough review of the forensic images, utilizing specialized tools to extract relevant information and uncover any hidden or deleted data. Each analysis step was carefully documented, to ensure that the findings were both reproducible and transparent. The investigator approached the evidence with a strong focus on maintaining the integrity of the evidence, ensuring that the analysis was comprehensive, accurate, and defensible.

Disseminating the Case

As the investigation progressed, the investigator compiled interim findings and prepared to disseminate this information as needed. Although operating alone, the investigator organized all notes and ensured that the relevant information was clearly documented, facilitating any necessary sharing with legal counsel or law enforcement. The investigator aimed to ensure that all findings were comprehensible and could be effectively communicated, despite being the sole handler of the case.

Presentation and Reporting

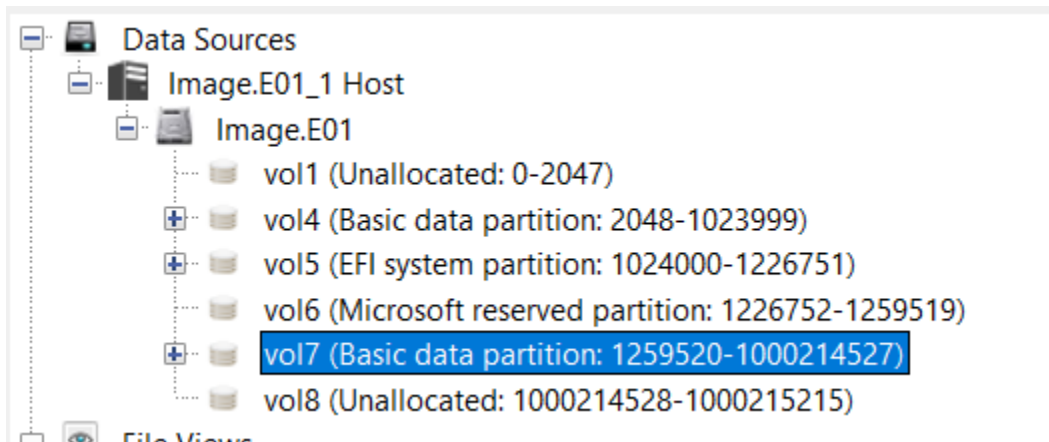
In the final phase, the investigator compiled a detailed report of the investigation, summarizing the methods, findings, and conclusions. The report provided a comprehensive account of the entire process, from preparation through to the final analysis, with a focus on clarity and accuracy. The investigator prepared to present these findings in a formal setting, such as a courtroom, ensuring that all documentation and evidence were ready to withstand scrutiny. The report was designed to be thorough and accessible, offering a clear narrative of the investigation from start to finish.

Evidence Analysis

The analysis involved examining the nine forensic images of the hard drive. Each image was analyzed for various elements, including partition structures, operating systems, software installations, connected hardware, user profiles, email activity, internet history, and personal data. The following sections detail the findings from this analysis.

Partitions in Forensics Image

The **partitions found** after the analysis of the image are **4**.



The **four partitions** are:

- Vol 4: Basic data partition
- Vol 5: EFI system Partition
- Vol 6: Microsoft reserved partition
- Vol 7: Basic data partition

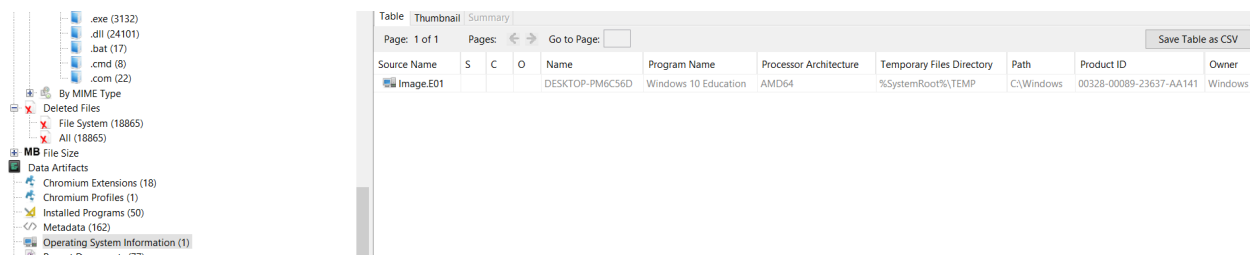
The list of partitions can be found at **Data Sources -> Image.E01_1 Host -> Image.E01**

These partitions are standard partitions. Vol 4 and Vol 7 partitions contain user files and applications stored. Vol 5 contains the bootloader and other files used at the time of system boot. Vol 6 is a unique partition. It is not present in the file explorer menu. It is used by windows to manage disk operations and it is usually of size 16 MB 128 MB.

Operating System in Forensics Image

The operating system installed is **Windows 10 Education**. The information about the operating system can be found at: **Data Artifacts -> Operating system Information**.

The OS Account can be logged in by only typing the username and does not require any password. The username is jcloudy



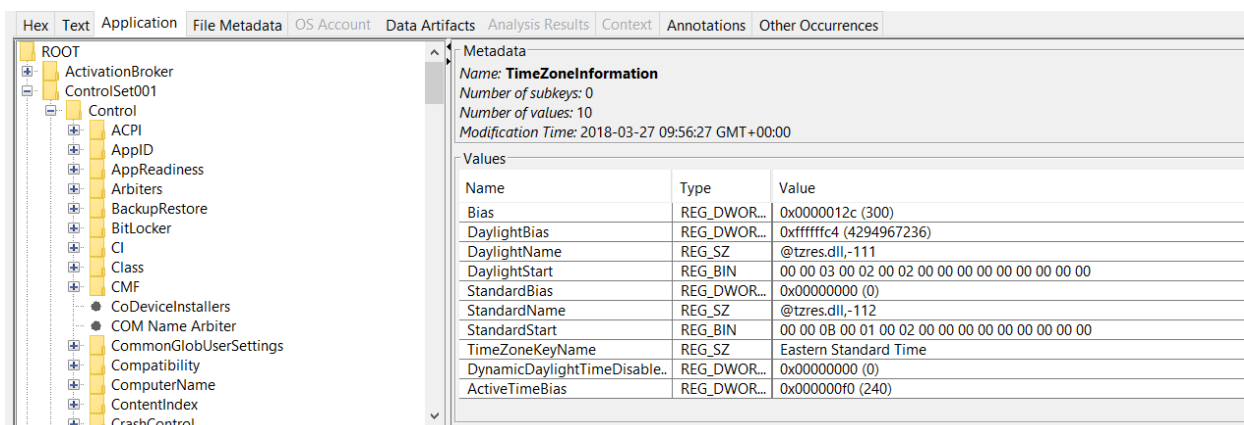
The image shows a file explorer interface on the left with a list of file types: .exe (3132), .dll (24101), .bat (17), .cmd (8), .com (22), Deleted Files, File System (18865), All (18865), MB File Size, Data Artifacts, Chromium Extensions (18), Chromium Profiles (1), Installed Programs (50), Metadata (162), Operating System Information (1), and Recent Documents (77). On the right, there is a table titled 'Table' with tabs for 'Thumbnail' and 'Summary'. The 'Summary' tab is active, showing a table with columns: Source Name, S, C, O, Name, Program Name, Processor Architecture, Temporary Files Directory, Path, Product ID, and Owner. The table contains one row for 'Image.E01'.

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

Time Zone Settings in Forensics Image

The time zone settings in the forensics image is set to the Eastern Time Zone. The bias is set to 300.

The Eastern Time zone is typically UTC-5 hours and the bias value of 300 minutes corresponds to UTC-5 hours, verifying that the time zone information is correct and is not manipulated.



Software Program Installations in Forensics Image

Many programs are installed in the forensics image. Some of the programs that raise suspicion are:

- **Microsoft Office Pro Plus:** This could indicate that the documentation of the planning of criminal activity is done using Microsoft Office suite.
- **Google Chrome:** This could indicate that the research of the criminal activity is done using Google Chrome.
- **Box and sync from Google:** This could indicate that the criminal has an account on google drive and is also storing planning documents on google drive for remote access.
- **Dropbox:** This could indicate that the criminal has also an account of dropbox. Documents related to criminal activity might also be on dropbox.

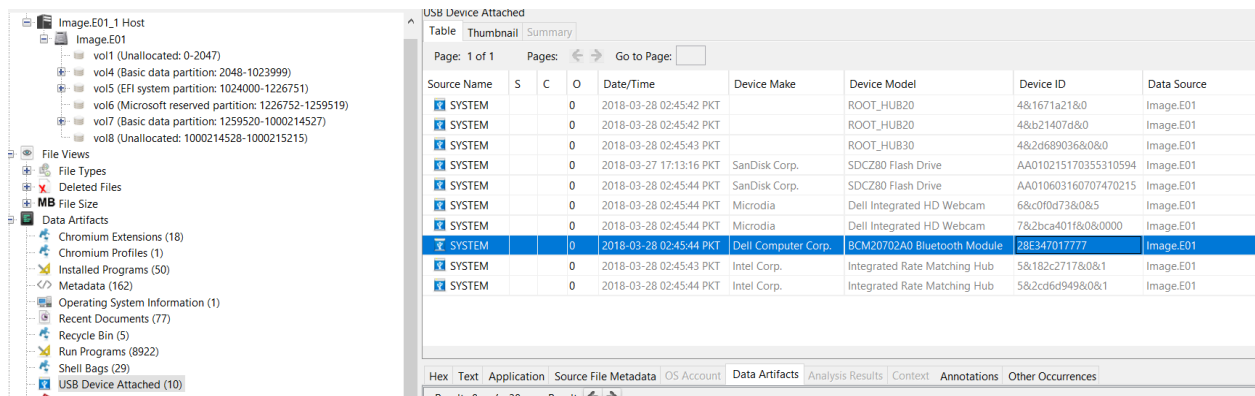
Installed programs can be found at: **Data Artifacts -> Installed Programs.**

Hardware Devices Attached

There are many Hardware Devices attached. The hardware devices attached that raised suspicion are:

- **SanDiskCorp Flash Drive:** Flash Drive attached could indicate that the criminal is moving the data related to the criminal activity to the flash drive. And according to the analysis there are 2 different Flash Drives attached because of two different device IDs.
- **Microdia Dell Webcam:** Microdia Dell webcam is also attached. It is an integrated webcam. But it can also indicate that the criminal is talking to someone live.

Attached hardware devices can be found at: **Data Artifacts -> USB Devices Attached.**



The screenshot shows a forensic tool interface. On the left, a 'File Views' pane lists various system artifacts including partitions (vol1-vol8), file types, deleted files, file sizes, data artifacts (Chromium Extensions, Profiles, Installed Programs, Metadata, OS Information, Recent Documents, Recycle Bin, Run Programs, Shell Bags), and USB devices. The 'USB Device Attached' table is selected and displays the following data:

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM	0		0	2018-03-28 02:45:42 PKT		ROOT_HUB20	481671a21&0	Image.E01
SYSTEM	0		0	2018-03-28 02:45:42 PKT		ROOT_HUB20	48b21407d&0	Image.E01
SYSTEM	0		0	2018-03-28 02:45:43 PKT		ROOT_HUB30	482d689036&0&0	Image.E01
SYSTEM	0		0	2018-03-27 17:13:16 PKT	SanDisk Corp.	SDCZ80 Flash Drive	AA010215170355310594	Image.E01
SYSTEM	0		0	2018-03-28 02:45:44 PKT	SanDisk Corp.	SDCZ80 Flash Drive	AA010603160707470215	Image.E01
SYSTEM	0		0	2018-03-28 02:45:44 PKT	Microdia	Dell Integrated HD Webcam	68c0f0d73&0&5	Image.E01
SYSTEM	0		0	2018-03-28 02:45:44 PKT	Microdia	Dell Integrated HD Webcam	782bca401f8&0&0000	Image.E01
SYSTEM	0		0	2018-03-28 02:45:44 PKT	Dell Computer Corp.	BCM20702A0 Bluetooth Module	28E347017777	Image.E01
SYSTEM	0		0	2018-03-28 02:45:43 PKT	Intel Corp.	Integrated Rate Matching Hub	58182c2717&0&1	Image.E01
SYSTEM	0		0	2018-03-28 02:45:44 PKT	Intel Corp.	Integrated Rate Matching Hub	582cd6d949&0&1	Image.E01

User Email Activity

Email activity was analyzed, revealing that the criminal actually have 2 email addresses, jimcloudy@outlook.com and jimcloudy1@gmail.com. The emails were primarily sent and received through an encrypted email service i.e. Gmail and Outlook.

Two gmail accounts were found by using keyword searches.

Source Name	S	C	O	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time	Access Ti
NTUSER.DAT			0	jimcloudy	jimcloudy	unattendloadednk 9=jimcloudy@outlook.com5wbnapf	2018-03-28 02:45:21 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	title : inbox (7) - «jimcloudy1@gmail.com - gmail	2018-04-06 17:49:35 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	title : inbox (7) - «jimcloudy1@gmail.com - gmail	2018-04-06 17:49:35 PKT	2018-03-;
NTUSER.DAT			0	jimcloudy1	jimcloudy	me.exe(7computer - «jimcloudy1@gmail.com - gmail	2018-03-28 02:45:21 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	e your box signup - «jimcloudy1@gmail.com - gmail	2018-04-06 17:49:35 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	. add some files! - «jimcloudy1@gmail.com - gmail	2018-04-06 17:49:35 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	?confirmemail.php&e=«jimcloudy1@gmail.com&c=	2018-04-06 17:49:35 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	title : inbox (7) - «jimcloudy1@gmail.com - gmail	2018-04-06 17:49:35 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	/confirmemail.php?e=«jimcloudy1@gmail.com&c=.	2018-04-06 17:49:35 PKT	2018-03-;
WebCacheV01.dat			0	jimcloudy	jimcloudy	tname : value : «jimcloudy@outlook.com b5e4e06	2018-04-04 09:33:09 PKT	2018-03-;
History			0	jimcloudy1	jimcloudy	ljhs5yj2oo9oa&email=«jimcloudy1@gmail.com&ore	2018-04-06 17:49:35 PKT	2018-03-;

User Internet Activity

The user browser history was analyzed and it revealed that the user searches were related to:

- Researching about which cloud storage is best and comparing them.

Source Name	S	C	V	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	can i sync a file to multiple cloud storage locations	Google Chrome	2018-03-28 04:34:08 PKT	Image.E01
History				google.com	cloud storage solutions	Google Chrome	2018-03-28 04:42:35 PKT	Image.E01
History				google.com	amazon cloud storage	Google Chrome	2018-03-28 04:46:32 PKT	Image.E01
History				google.com	can i use amazon s3 for free	Google Chrome	2018-03-28 04:47:13 PKT	Image.E01
History				google.com	sync amazon s3 from desktop?	Google Chrome	2018-03-28 04:47:57 PKT	Image.E01
History				google.com	tntdrive	Google Chrome	2018-03-28 04:48:18 PKT	Image.E01
History				google.com	tntdrive vs	Google Chrome	2018-03-28 04:49:10 PKT	Image.E01
History				google.com	s3 desktop client	Google Chrome	2018-03-28 04:50:07 PKT	Image.E01
History				google.com	dropbox	Google Chrome	2018-03-28 05:01:35 PKT	Image.E01
History				google.com	box storage	Google Chrome	2018-03-28 05:03:56 PKT	Image.E01
History				google.com	box storage	Google Chrome	2018-03-28 05:04:10 PKT	Image.E01
History				google.com	stream futarama	Google Chrome	2018-03-28 05:04:45 PKT	Image.E01

- Researching about which gun is the best and how a gun can be bought illegally.

History			google.com	apm5giwu	Google Chrome	2018-03-28 05:49:29 PKT	Image.E01
History			youtube.com	best tactical rifle	Google Chrome	2018-03-28 05:53:01 PKT	Image.E01
History			google.com	mega cloud storage	Google Chrome	2018-03-28 05:55:24 PKT	Image.E01
History			google.com	ruger 10-22	Google Chrome	2018-03-28 05:56:42 PKT	Image.E01
History			google.com	keltec sub 2000	Google Chrome	2018-03-28 05:57:22 PKT	Image.E01
History			youtube.com	fn p90	Google Chrome	2018-03-28 06:00:56 PKT	Image.E01
History			google.com	fnp90	Google Chrome	2018-03-28 06:01:11 PKT	Image.E01
History			google.com	twitter	Google Chrome	2018-03-28 06:06:33 PKT	Image.E01
History			google.com	shooting range near me	Google Chrome	2018-03-28 06:09:53 PKT	Image.E01
History			twitter.com	#MolonLabe	Google Chrome	2018-03-28 06:11:50 PKT	Image.E01
History			google.com	https://accounts.google.com/AccountChooser?Email=ji...	Google Chrome	2018-03-29 09:23:18 PKT	Image.E01
History			google.com	just how easy is it to buy an illegal gun	Google Chrome	2018-03-29 09:37:29 PKT	Image.E01
History			google.com	just how easy is it to buy an illegal gun	Google Chrome	2018-03-29 09:37:29 PKT	Image.E01

- Researching about where can gun shooting be practiced and researched about what is the cops average response time
- Researching about which airport has the shortest delays
- The user also searched about How to smuggle cash out of United States and also researched about the idea of strapping cash to oneself and walk through TSA

All of these searches indicate that the user was trying to buy a gun and rob a place, possibly Democratic National Committee. And then leave the country via airplane. The user is trying to filter the airports by less delay time.

The information about User Internet Activity can be found at:

Data Artifacts -> Web History and Data Artifacts -> Web Search

Personal Data Analysis

Personal documents in the forensics documents were analyzed. Documents analyzed included: Planning.docx, AIRPORT INFORMATION.docx, Cloudy thoughts.docx.

- ❖ Planning.docx: This document is related to the planning of criminal activity. Upon analyzing, it was revealed that the document is divided into multiple sections.
 - First section is related to Target. What is the target and what is the criminal trying to achieve?
 - Criminal is trying to pick up a target that has an easy escape route and is near the airport.
 - Second section is related to Supplies.
 - In this section, the criminal has listed the address from where the guns will be bought.
 - **Northern VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153**
 - **NOVA 412 W Broad Street Falls Church, VA 22046**
 - These are the addresses from where the guns are bought.
 - Prices of Ammo is also listed in the second section
 - **9mm is 1000 for \$360**
 - **Kel-Tec Sub 2000 9mm \$400.**
 - These are the prices of ammo.
 - Moreover, the criminal also has planned on wearing latex gloves and Velcro strap clothes. Most probably to quickly change clothes after a shootout.
 - The third section of the document is related to Escape route.
 - The criminal has two places in mind to escape: Vietnam or Indonesia.
 - The criminal planned to have same day tickets for the destination and preferably a direct flight to the destination
 - The criminal planned on having the suitcase in the car.
- ❖ The second file analyzed is AIRPORT INFORMATION.docx
 - After analyzing the AIRPORT INFORMATION.docx file, it became clear that the criminal's target is a shootout at **Fairfax County Democratic Committee.**
 - The criminal will use Dulles airport because it has best record of on time flights
 - The criminal will go to Indonesia with a layover at Qatar.
 - The criminal will go to Indonesia because it has nice living.
- ❖ The third file analyzed is Cloudy thoughts.docx
 - In this file, the criminal discusses how stressed he is and that writing calms him down.

- Moreover he discusses the plan whether it will work or not. He said **"It's 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."**
- Moreover, he said that he is leaving alot behind and its a great responsibility and wants his family to understand that what he is doing is just and right. If he is killed in the act then so be it. Freedom requires sacrifice.
- He said that he won't delete any of the records and he wants the world to know. He said that all of his records are in the cloud and Paul will have only other keys.

Findings and Conclusion

Based on the forensic analysis of the evidence obtained from the digital image, several critical findings have been uncovered that suggest a well-planned criminal activity.

Operating System and User Access:

The forensic analysis revealed that the operating system installed on the suspect's computer was Windows 10 Education. The OS account associated with the username "jcloudy" was configured in such a way that it did not require a password for login. This lax security setting could indicate that the suspect either operated in a low-security environment or had confidence in physical security, potentially minimizing digital footprints.

Time Zone Settings:

The time zone settings on the system were set to the Eastern Time Zone with a bias of 300 minutes, corresponding to UTC-5 hours. This time zone setting is consistent with the physical location where the device was used, suggesting that there was no manipulation of time zone data, which could have been used to obscure timelines of activities.

Suspicious Software Installations:

Several software programs installed on the system raised red flags:

Microsoft Office Pro Plus: Indicates potential use for documenting plans related to criminal activities.

Google Chrome: Likely used for researching methods or opportunities to commit crimes.

Box and Sync from Google, Dropbox: The presence of these cloud storage services suggests that the suspect stored or shared documents and files related to the criminal activities, possibly to facilitate access from different locations or devices.

Attached Hardware Devices:

The analysis revealed that two different SanDisk flash drives were connected to the system, as indicated by different device IDs. This suggests the potential use of external drives to store or transfer incriminating data. Additionally, a Microdia Dell integrated webcam was identified, which might have been used to communicate with accomplices or monitor surroundings during criminal planning.

Email Activity:

The suspect, using the aliases "jimcloudy" and "jimcloudy1," primarily communicated through encrypted services like Gmail and Outlook. This use of multiple email accounts is consistent with efforts to compartmentalize communications and avoid detection. However, keyword searches indicate that the suspect might have used these accounts to coordinate the criminal activities or communicate with collaborators.

Internet Activity:

The suspect's browsing history included searches related to:
Cloud storage options, likely for storing or sharing documents related to the criminal plans.
Methods for illegally purchasing a firearm and practicing shooting, which strongly suggests preparation for a violent act.
Information on airport delays and smuggling tactics, indicative of planning an escape from the country after committing the crime.

Personal Document Analysis:

Several documents found on the system provided clear evidence of criminal intent:

Planning.docx: Detailed the target (Fairfax County Democratic Committee), supplies needed (guns and ammunition), and escape routes (with specific focus on Vietnam or Indonesia).

AIRPORT INFORMATION.docx: Confirmed the suspect's plan to escape via Dulles Airport, with a flight itinerary prepared for immediate departure after the crime.

Cloudy thoughts.docx: Contained reflections on the upcoming crime, indicating psychological stress and a belief in the righteousness of the planned act. This document also revealed the suspect's intention to leave records intact as a testament to their actions.

Conclusion:

The forensic evidence strongly suggests that the suspect was in the advanced stages of planning a criminal act, likely involving the use of firearms in a targeted attack. The thorough preparation, as seen in the detailed plans and escape routes, combined with the suspect's efforts to maintain encrypted communication and secure storage of documents, point to a high level of premeditation. The suspect's use of multiple email accounts, external storage devices, and meticulous internet research further reinforce the conclusion that this was not a spontaneous act but rather a carefully orchestrated plan.

These findings provide substantial grounds for further legal action and serve as critical evidence in building a case against the suspect. The evidence collected and analyzed will be pivotal in determining the suspect's intent and capability, as well as in establishing the timeline and scope of the planned criminal activities.

Appendix

Preparation

- **Case Name:** Assigned a unique case Name **Digital Forensics** for identification and tracking throughout the investigation.
- **Evidence Collection:** Retrieved the hard drive from the crime scene and secured it in a tamper-evident container for transport to the forensic lab.
- **Forensic Imaging:** Created forensic images of the hard drive using [Imaging Tool]. Hash values (MD5 and SHA-1) were generated before and after imaging to ensure the integrity of the forensic copies.

Collection and Preservation

- **Original Evidence:** The original hard drive was stored in a locked evidence room with restricted access to prevent any tampering. Only the investigator has access to this storage.
- **Forensic Images:** Forensic images were saved on an encrypted and secured drive. All access to the forensic images was logged, ensuring no unauthorized access.

Examination and Analysis

- **Partition Analysis:**
 - **Partitions Identified:** The hard drive contained multiple partitions: Vol 4 (Basic Data Partition), Vol 5 (EFI System Partition), Vol 6 (Microsoft Reserved Partition), Vol 7 (Basic Data Partition). These partitions were analyzed for file system structure and content.
- **Operating System:**
 - **Installed OS:** Windows 10 Education was identified as the installed operating system. The OS account "jcloudy" was found to require no password for login, indicating a potential security vulnerability.
- **Time Zone Settings:**
 - **Time Zone:** The system's time zone was set to Eastern Time (UTC-5) with a bias of 300 minutes, consistent with the Eastern Time Zone, confirming that there was no manipulation of time settings.
- **Installed Software:**
 - **Suspicious Programs:** Several programs that could be related to criminal activities were identified, including Microsoft Office Pro Plus (potentially used for documentation), Google Chrome (used for research), Box and Sync from Google (indicating cloud storage usage), and Dropbox. These installations suggest the user might have been planning or executing criminal activities and storing related documents both locally and in the cloud.

- **Hardware Devices:**
 - **Attached Devices:** Two distinct SanDiskCorp flash drives were connected to the system at different times, as indicated by unique device IDs. Additionally, a Microdia Dell webcam was also attached, which could imply the user was engaged in live communication or recording.
- **User Email Activity:**
 - **Emails Identified:** The user, associated with the accounts "jimcloudy@outlook.com" and "jimcloudy1@gmail.com," primarily used encrypted services (Gmail and Outlook) for communication. Two email addresses were identified through keyword searches, indicating possible multiple accounts used for different aspects of the criminal activity.
- **Internet Activity:**
 - **Search History:** The user's browser history revealed searches related to purchasing guns illegally, choosing the best cloud storage, planning an escape, and smuggling cash out of the United States. These searches suggest detailed planning of a potential criminal activity involving robbery and a planned escape from the country.
- **Personal Documents:**
 - **Documents Analyzed:** Several documents, including "Planning.docx," "AIRPORT INFORMATION.docx," and "Cloudy thoughts.docx," were analyzed. These documents contained detailed plans for a potential crime, including target selection, acquisition of weapons, escape routes, and personal reflections on the planned criminal activity.

Disseminating the Case

- **Document Review:** After completing the analysis, all findings were reviewed for accuracy, consistency, and completeness. A comprehensive report was drafted to detail the investigation's results.
- **Chain of Custody:** Updated the chain of custody to reflect all actions taken, ensuring the integrity and authenticity of the evidence throughout the investigation.

Contemporary Notes

The case involved the retrieval, imaging, and secure storage of a hard drive, followed by a detailed analysis of the partitions, installed software, and user activity. Suspicious programs, email accounts, internet searches, and personal documents indicated potential criminal planning, with findings documented and the chain of custody maintained throughout.