

NOTTINGHAM TRENT UNIVERSITY

SCHOOL OF SCIENCE AND TECHNOLOGY

COMP40572: Computer Forensics Report

By

Harihara Krishna

N1261158

I hereby declare that I am the sole author of this report, and associated work. I confirm that all third-party items including code have been adequately acknowledge and referenced.

Signature,

Harihara Krishna

Contents

1. Introduction	4
1.1. Scene Assessment: Search & Seize	5
2. Acquisition: Forensic Image Creation	8
2.1. Creating memory image	8
2.2 Creating a case	9
3. Forensic Image Analysis.....	10
3.1. File analysis	14
3.1.1. Hex and extension analysis	14
3.1.2 Deleted, Hidden and other suspicious file analysis	14
4. Reporting	16
4.1 Evidence Reporting	16
4.2 Record of Actions taken during Search and Seize	17
4.3 Chain of Custody	17
4.4 General Case Documentation	20
4.5 Process Documentation	20
5. Conclusion	21
6. References	21

1. Introduction

The following report and investigation was conducted by Harihara Krishna. My role is to analyse the evidence provided and present facts that appear pertinent to the case.

Today is Thursday 1st July 2004, and an organisation has invited me to investigate the scene wherein the organisation has suspected one of its staff members to have breached organisational policy. The suspect has been accused as a member of a religious group which considers geometric shapes important. In May 2004, the suspect was explicitly cautioned against using organizational resources to create, store, search for on the internet, or share images of such shapes. The investigation must conclude whether there are relevant evidences pertinent to the accusations.

The upcoming sections of the report are detailed according to the Kruse Model and will detail about the investigations set to be conducted on the scene and the device of an organisation used by a staff member who is suspected of breaking organisational policy.

The list of equipment which are required for the investigation are listed below:

- Video recording device for photographic evidence
- Write blocker software/hardware to prevent unintentional modifications on HDD
- USB stick to capture volatile memory.
- Screwdriver set to take the hard drive out
- Faraday/non-static bags to seize electronic devices and prevent any signal interference
- chain of custody labels for Faraday bags to identify evidence
- Emergency battery for mobile based devices.
- Some cables for mobile phones.
- Paper clip to open CD drives

1.1. Scene Assessment: Search & Seize

On arriving at the investigation site on the 1st of July 2004, a desktop computer (unlocked and ON), monitor, keyboard, mouse is present at the scene and taken note of. Adding to these are USB stick(s), a flash memory card specialised for recording images of capacity 32 Mb, a SIM card, a mobile phone and a pair of batteries. A book named "Catch me if you can" by Frank W. Abagnale is taken note along with a set of printed sheets lying under the book. Since the system appears to be unlocked, the IT team need not be contacted for password assistance.

The above mentioned scene must be documented before coming in contact with any tangible evidence. The scene has been photographed in order to create a detailed record for legal and investigative purposes. Figure 1 depicts the scene which was left untouched before any further analysis.

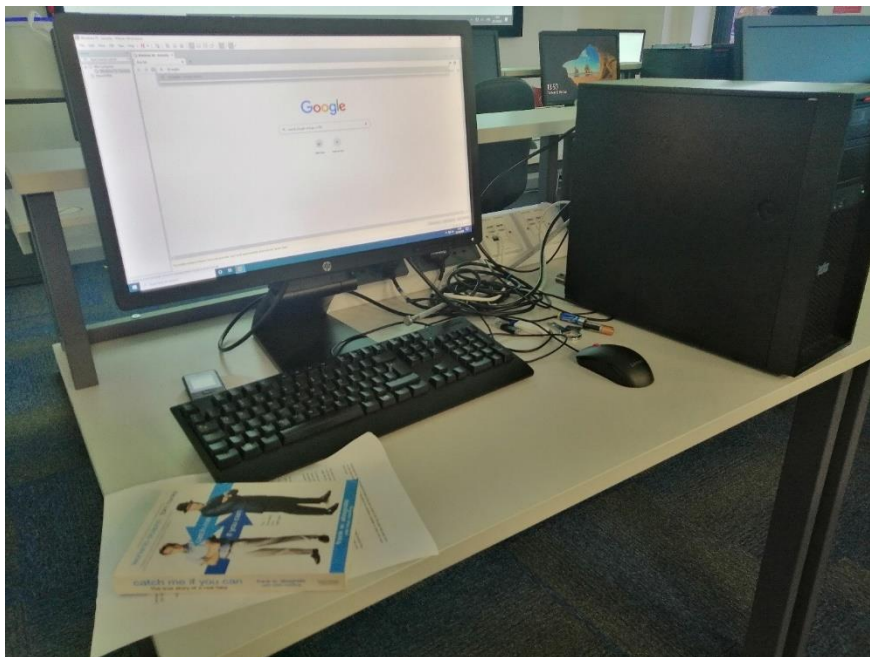


Figure 1 Investigation Site

The foremost step is to secure the scene. Since the device must be investigated for evidence, our actions must be recorded as video recordings.

Visual Inspection

- At first the hard disk light is checked in Figure 1, wherein if found flashing red rapidly it indicates that there must be a destructive program running in the background.
- The serial number/label along with the model of PC was documented for inventory and identification purposes.
- Carefully observe the screen for any visual on-screen content. Screenshots of all open windows and minimised tabs must be taken.
- The word on the google search bar was taken note of for any future relevance.
- Check the book and the sheets below for any written notes or handwritings.
- Running applications must be checked if they use any actively used software.
- Suspicious files and folders which may seem irrelevant given the environment, must be dealt with by locating the paths of these files and noting their names and owners.
- Inspect the pair of batteries for additional components or relatable devices in the surroundings which can use them.
- Trace and document the connections of the mouse, keyboard and other peripheral devices to check if they lead to any external storage devices.
- Search for cables associated with the E-cigarette. E-cigarettes can be means of tracking usage or transferring malicious files through the cables coming along with them.
- **Items Seized:** USB sticks, SIM card attached to/beneath a USB stick shaped like a tin opener, batteries, flash memory card specialised for recording images of capacity 32 Mb (Fujifilm XD picture card), cables associated with E-Cigarette and the E-cigarette, DVD/CD Drive. All non-static and faraday bags must be labelled.



Figure 2 Back of PC

Surrounding Accessories:

The scene must be searched for any possible documents which might contain direct or indirect leads to password(s) or any associated leads which might help identify any laws violated. The book can only be seized if it contains any handwriting or handwritten notes in them. The sheets of paper lying under the book must be inspected for its content and its relevance towards the religious organisation. Prior to this, irrespective of the password obtained, a USB stick must be used to capture volatile memory.

As depicted in figure 2,

- The PC happens to have wireless antennas which should be seized and inspected to analyze wireless communication or unauthorized remote access.

- The paper sheets under the book have been seized due to its content having the word praying more than once in several sentences.
- The book named "Catch me if you can" by Frank W. Abagnale can only be seized if and only if they contain handwritings or extra notes.
- Figure 1 depicts a keypad mobile phone, which should be checked whether it's ON and must be imaged shortly after receiving if ON and seized using faraday bag.
- **Items Seized:** wireless antennas, paper sheets indicating some prayer technique, keypad phone.

It is important to document and remove the connected power cable to safely power down the system (if not already off) in order to avoid accidental data changes in volatile memory and protect the hardware for analysis. Uncover the system case after adequate documentation for inspection and seize:

- Hard drives, whether they are HDD or SSD, are primary storage devices that hold the majority of the data.
- RAM modules are used for analyzing volatile memory when the system is turned on.
- Graphics card or other components that are concerning due to potential data storage or involvement in criminal activities.

The PC was unscrewed and the hard drive was safely ejected as it had to be seized for inspection. The hard drive was labelled and seized in a faraday bag. All seized electronic items were labelled and seized in faraday bags.

2. Acquisition: Forensic Image Creation

2.1. Creating memory image

Given the volatile nature of information stored in computer memory, live forensic imaging will be performed with the FTK Imager tool to gather history and log files of the activities in the volatile memory.

- The original evidence of the memory was left untouched and was duplicated using cyber forensic tools.
- The system clock was checked and found it accurate
- The disk was physically examined and nothing unusual was noted.
- A physical chain of custody was maintained
- The disk was write protected, so that the exact copy of the memory is created without disrupting its integrity.
- The memory stick/computer memory was imaged using FTK Imager. The output location and the file format of the forensic image was specified.
- The memory image was ensured of its integrity by creating hashes of the image created using MD5 and SHA256 algorithm and was cross checked. The hash value is then checked for subsequent analysis.
- Live memory capture occurs while the computer is up and running. Consequently, the bit stream copy technique will be utilized to duplicate and generate backup clones of the memory dump.
- The memory image is then stored on a secure external drive to preserve evidence and maintain chain of custody.

2.2 Creating a case

The forensic analysis of the USB drive image was carried out in the Autopsy Tool. The memory images of both the computer and one of the USB sticks were captured using the Autopsy imaging tool. Since the computer memory image hasn't been efficient enough in identifying relevant leads, the image of one of the seized USB sticks have been utilised to proceed further with this investigation

A new case was created in Autopsy named cwk1 as depicted in Figure 3.

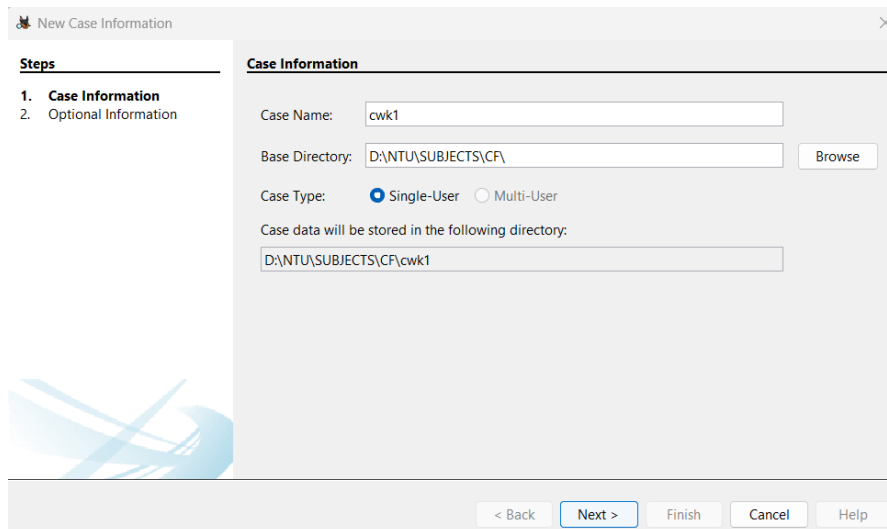


Figure 3 Autopsy Imager

The Autopsy imager requires a data source for the image wherein the seized and write blocked hard drive was imaged as a local disk. This is depicted in Figure 4. Since the time zone of the disk and my device were similar, there was no need to set the time zone.

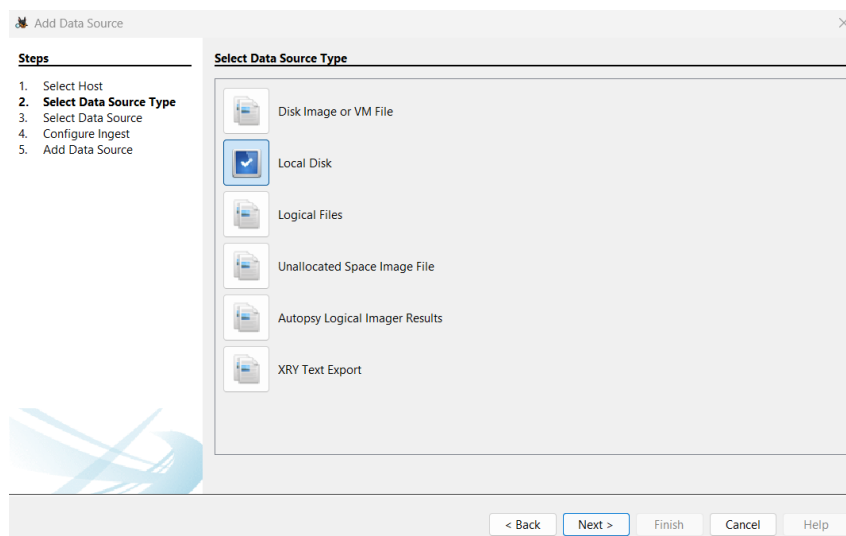


Figure 4 Autopsy Data Source

Since the computer memory imaging proved futile during analysis, the image of the USB stick was imaged similarly.

3. Forensic Image Analysis

The replica of the USB drive was analysed and is detailed about all throughout Section 3.

The information about the USB stick which was imaged is as follows:


Listing					
cwk1.dd_1 Host					
Table Thumbnail Summary					
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
 cwk1.dd	Image	10289152	512	Europe/London	0aeb72e-81c7-4cb3-9673-56914ed07db5
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences					
Metadata					
Name:	/img_cwk1.dd				
Type:	Raw Single				
Size:	10289152				
MD5:	9bdb9c76b80e90d155806a1fc7846db5				
SHA1:	7e9a3852fc53f3871d2f89a0a72c939405febbae				
SHA-256:	9c43d6a2dd5132cf6afc29e5c644cde0cb747c64998a68e73f2efb787887b126				
Sector Size:	512				
Time Zone:	Europe/London				
Acquisition Details:	Unknown				
Device ID:	0aeb72e-81c7-4cb3-9673-56914ed07db5				
Internal ID:	1				
Local Path:	D:\NTU\SUBJECTS\CF\cwk1.dd				

Figure 5 cwk1.dd metadata

As depicted in Figure 5, the metadata of the captured memory is checked for its integrity using trusted hash algorithms such as MD5, SHA1 and SHA256. The time zone of the device is noted Europe/London. Multiple ingest modules facilitated by the Autopsy tool were run on the case file containing the image "cwk1.dd" as a data source. The next step was to analyse user activity in order to know if the user had any malicious intent to destroy, hide or manipulate directories and files belonging to the USB drive.

The below table shows the timestamps of every file that consists of geometric images wherein all the files have a timestamp defined after the warning issued on May 2004. The table throws light on the evidences for violation of the organizational policy and has been sorted according to modification time.

Table 1 Geometric image file paths and timestamps

Image File path	Time Created(BST)	Time Modified(BST)
/img_cwk1.dd/archive/file9.bo0/file9.jpg	-	2004-06-09 20:53:32
/img_cwk1.dd/archive/file8.zip/file8.jpg	-	2004-06-09 21:52:20

/img_cwk1.dd/archive/file10.tar.gz/file10.tar/file10.jpg	-	2004-06-10 02:54:53
/img_cwk1.dd/misc/file13.dll:here (ADS)	2004-06-10 04:29:18	2004-06-10 04:29:45
/img_cwk1.dd/alloc/file2.dat	2004-06-10 04:27:36	2004-06-10 07:46:52
/img_cwk1.dd/del1/file6.jpg	2004-06-10 04:28:00	2004-06-10 07:48:08
/img_cwk1.dd/del2/file7.hmm	2004-06-10 04:28:00	2004-06-10 07:49:18
/img_cwk1.dd/alloc/file1.jpg	2004-06-10 04:27:36	2004-06-10 07:59:40
/img_cwk1.dd/misc/file12.doc	2004-06-10 04:29:17	2004-06-10 08:20:58
/img_cwk1.dd/invalid/file3.jpg	2004-06-10 04:28:20	2004-06-10 08:27:02
/img_cwk1.dd/invalid/file4.jpg	2004-06-10 04:28:20	2004-06-10 08:38:06
/img_cwk1.dd/invalid/file5.rtf	2004-06-10 04:28:20	2004-06-10 08:41:54
/img_cwk1.dd/misc/file11.dat	2004-06-10 04:29:17	2004-06-10 08:44:46

The USB stick consists of an NTFS file architecture, which consists of an MFT table which in turn stores the file names and metadata. The key point which was notable in this investigation was that alternate data streams (ADS) were present within the file system. Alternate Data Streams are often used to hide information by spreading the data across the file architecture (Alexander, S.,2018). This is confirmed by the files file13.dll and file13.dll:here. Below shown is the metadata of the file "file13.dll".

```

$LogFile Sequence Number: 1094029
Allocated File
Links: 1

$STANDARD INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 259 ()
Created: 2004-06-10 04:29:18.103897600 (GMT Daylight Time)
File Modified: 2004-06-10 04:29:45.673540800 (GMT Daylight Time)
MFT Modified: 2004-06-10 04:29:45.673540800 (GMT Daylight Time)
Accessed: 2004-06-10 04:29:45.673540800 (GMT Daylight Time)

$FILE NAME Attribute Values:
Flags: Archive
Name: file13.dll
Parent MFT Entry: 41 Sequence: 1
Allocated Size: 0 Actual Size: 0
Created: 2004-06-10 04:29:18.103897600 (GMT Daylight Time)
File Modified: 2004-06-10 04:29:18.103897600 (GMT Daylight Time)
MFT Modified: 2004-06-10 04:29:18.103897600 (GMT Daylight Time)
Accessed: 2004-06-10 04:29:18.103897600 (GMT Daylight Time)

Attributes:
Type: $STANDARD INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE NAME (48-2) Name: N/A Resident size: 86
Type: $DATA (128-3) Name: N/A Non-Resident size: 58391 init size: 58391
Starting address: 2339, length: 115
Type: $DATA (128-5) Name: here Non-Resident size: 124038 init size: 124038
Starting address: 6688, length: 10
Starting address: 10107, length: 20
Starting address: 10005, length: 43
Starting address: 2454, length: 133
Starting address: 12831, length: 37

```

Figure 6 Metadata of suspicious file13.dll

From the above image it is inferred that:

\$DATA (128-3) happens to be the main data stream which has 58,391 bytes stored outside the MFT, starting at address 2339 with a length of 115 clusters. It is allocated and usable.

However, \$DATA(128-5) is an alternate data stream named "here", with a non-resident size of 124,038 bytes, starting at multiple addresses ranging from 6688,10107,10005,2454 and 12381 with different lengths. This is confirmed by the FTK Imager tool as well.

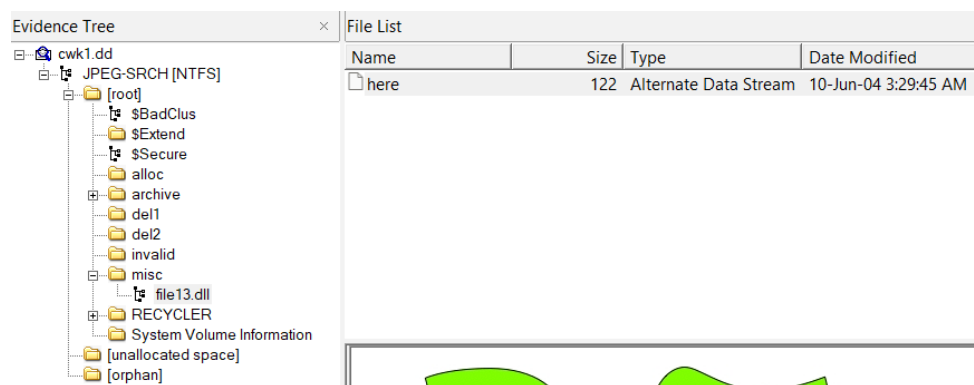


Figure 7 Alternate Data Streams

From the above mentioned evidence, a deeper investigation is carried out to identify any other suspicious activities in the upcoming sections. The upcoming files which belong to NTFS file architecture will be analysed using HxD hex editor.

3.1. File analysis

3.1.1. Hex and extension analysis

The below table summarises the findings of the analysis conducted on the case:

Path	Material Evidence	Description
/img_cwk1.dd/misc/file12.doc	Word document metadata	A Microsoft word document whose metadata consists of a name "Brian Carrier" as its author whose content contains an image of a triangle named "image_0.jpg"
/img_cwk1.dd/alloc/file1.jpg /img_cwk1.dd/misc/file12.doc/image_0.jpg /img_cwk1.dd/archive/file9.boo/file9.jpg /img_cwk1.dd/archive/file10.tar.gz/file10.tar/file10.jpg /img_cwk1.dd/archive/file8.zip/file8.jpg	Image files	The mentioned images consisted of geometric shapes wherein file9.boo was a zip file containing file9.jpg with contradicting timestamps.
/img_cwk1.dd/alloc/file2.dat	Extension mismatch (Originally jpg file)	The extension of the file has been manipulated and identified by Autopsy. Consists of image #2
/img_cwk1.dd/misc/file11.dat	Manipulated hex header (Originally jpg file)	The initial 1572 bytes of random bytes of the file have been edited such that the JPG header is unidentified. Consists of image #8
/img_cwk1.dd/invalid/file3.jpg	Extension mismatch (Originally text file)	The file extension was manipulated and the file size was increased which was known through the text file contents and the hex code.
/img_cwk1.dd/misc/file13.dll:here & /img_cwk1.dd/misc/file13.dll	Extension mismatch (Originally JPG file with ADS)	Traces of alternate data streams found along with image #10
/img_cwk1.dd/invalid/file4.jpg	Damaged/Corrupted hex	Incomplete hex header having bytes 0xffd8 (JPEG signature header) and no trailer bytes. Can be a partial image (Wikipedia contributors 2024)

Table 2 Hex and extension mismatches

/img_cwk1.dd/invalid/file5.rtf	Doesn't contain hex header for RTF 7B 5C 72 74 66	A file with the 0xffd8 hex signature in several locations inside the file. (Wikipedia contributors, 2024)
--------------------------------	---	---

3.1.2 Deleted, Hidden and other suspicious file analysis

The files analysed in this section were either marked unallocated or deleted.

Path	Material Evidence	Description
/img_cwk1.dd/\$CarvedFiles/1/f0003372.db	FlashPix file whose extension has been mismatched/manipulated	The carved file was extracted and analysed for its metadata using EXIF/metadata tool which conveys that the file is a FlashPix file which is primarily linked to digital image software or cameras that accommodate this format.(2004)
/img_cwk1.dd/del2/file7.hmm	Extension mismatch (Originally jpg file)	The image was found to be deleted along with its extension manipulated. Consists of image #4 with numerous mentions
/img_cwk1.dd/del1/file6.jpg	Geometric Image	The image was deleted and is mentioned multiple times in the hex of many files.
/img_cwk1.dd/\$Unalloc/Unalloc_4_545792_10289152	Multiple JPEG headers and trailers found	The JPEG headers of file7.jpg, file6.jpg & the flashpix file.
/img_cwk1(1).dd/RECYCLER/ S-1-5-21-1757981266-484763869-1060284298-1003	Hiding malicious files in windows using a recycle bin folder attribute	A hidden file used to store information about the arrangement of a windows folder done by user with SID= S-1-5-21-1757981266-484763869-1060284298-1003.
/img_cwk1.dd/System Volume Information/tracking.log	Suspicious word "thorntons" found	The word "thorntons" was logged by an application tracking the user activity.

Table 3 Carved and Deleted file analysis

```
D:\NTU\SUBJECTS\CF\forensi x + v
ExifTool Version Number      : 13.04
File Name                    : f0003372.db
Directory                    : D:\NTU\SUBJECTS\CF\forensic tools\exiftool-13.04_64\exiftool-13.04_64
File Size                    : 4.6 kB
File Modification Date/Time   : 2024:11:28 16:53:34+00:00
File Access Date/Time        : 2024:11:28 18:08:28+00:00
File Creation Date/Time      : 2024:11:28 16:53:34+00:00
File Permissions              : -rw-rw-rw-
File Type                    : FPX
File Type Extension          : fpx
MIME Type                    : image/vnd.fpx
-- press ENTER --
```

Figure 8 EXIF tool results for one of the carved files

4. Reporting

4.1 Evidence Reporting

From Table 3 it is evident that the user having SID "S-1-5-21-1757981266-484763869-1060284298-1003" has used file hiding techniques by mishandling the .ini file settings by changing the attributes (Parvez 2010) to a recycle bin folder. Additionally, Alternate data streams were present in the disk which also conveys that the user has tried to hide files prior to inspection.

As shown in Figure 8, the .fpx file (Aleksey 2024) obtained from the "carved" folder is not as widely supported by softwares as other image formats. However, Flashpix is (Anon n.d.) closely associated with its creator Kodak, which was developed for its capability to retain various resolutions of an image in a single file, allowing users to see and interact with images at different dimensions and degrees of detail. The file can have strong relevance with the flash memory card (FujiFilm XD picture card) as the card can be used with a digital camera.

Similarly, Table 1 conveys the obvious violation of organizational policy by user "Brian Carrier" in using a geometric image in his own document "file12.doc". The file "file3.jpg" with an extension mismatch conveys the malicious intent of the user in trying to tamper

file hex signatures along with filling the text file with a taunting intention. Files "file11.dat" & "file2.dat" supports the above statement by having hex tampering and extension tampering evidences.

4.2 Record of Actions taken during Search and Seize

- The organization suspects a staff member of breaching policies by engaging in activities related to a religious group that assigns significance to geometric shapes.
- In May 2004, this individual received a formal warning against using organizational resources to create, store, search for, or disseminate images of geometric shapes.
- Cranjis McBasketball who is a witness has overseen a recent internet search prior to the investigation for the word "angles" at the investigated site but seems unsure.
- The autopsy keyword search results do not show valid emails or credit card numbers (Gehl, Plecas 2017b).
- 11 images from the USB stick image have proved to be geometric shapes along with a suspicious name "Brian Carrier".

4.3 Chain of Custody

To maintain the chain of custody, every step was carefully documented to ensure accountability and transparency. This process began with collecting evidence at the crime scene, where each device was assigned a unique identifier to prevent mix-ups or loss.

Detailed descriptions of the devices were recorded, noting their condition and the reasons for their seizure. The initial state of the evidence was documented thoroughly, including hashing to verify the integrity of the devices and data collected.

Objective	To assess if a staff member has used organizational resources for unauthorized tasks such as creating, sharing, or searching for data online.
Type of device	USB stick drive
Device ID	0aeb72e-81c7-4cb3-9673-56914ed07db5
Description	<ul style="list-style-type: none"> The USB drive was confiscated as it satisfies the suspicions that it might have been used to store or process data which was against organisational policy.
Unique Identifier	CWK-6x70
MD5 hash	9bdb9c76b80e90d155806a1fc7846db5
Tools used	FTK imager, EXIFTool, Autopsy, HxD hex editor
Date/time	July 1st 2004 11:00 AM
Received by	Harihara Krishna (Lead Cyber Forensic Investigator)
Comments	The device was successfully seized with consent of the staff member prior to acquisition. The USB drive was removed from storage and signed for at 11:50 AM and returned back to storage by Harihara Krishna at 4:20 PM on Thu 1 st July 2004.

Objective	To assess if a staff member has used organizational resources for unauthorized tasks such as creating, sharing, or searching for data online.
Type of device	Hard Disk Drive
Device ID	02e-81c7-4cb3-963-56914b5
Description	<ul style="list-style-type: none"> The HDD was seized to analyse whether its contents have relevant geometric shapes dated on or after May 2004.
Unique Identifier	CWK-4x20
MD5 hash	5bd6487cf1a608551d09e08b67c9bdb9
Tools used	FTK imager, EXIFTool, Autopsy
Date/time	July 1st 2004 10:00 AM
Received by	Harihara Krishna (Lead Cyber Forensic Investigator)
Comments	The device was successfully seized with consent of the staff member prior to acquisition. The USB drive was removed from storage and signed for at 11:50 AM and returned to Harihara Krishna at 4:20 PM on Thu 1 st July 2004 by the associate forensic investigator Candice Gefuhrst Klaus.

4.4 General Case Documentation

The organizational head Mr. Immaneid aajob has suspected one of his staff members of violating company policy after a strict warning for which I was authorized by the head of the organization to conduct an investigation on site. The court granted a search warrant, thereby allowing us to proceed to collect, investigate and seize evidence from the staff member's legally.

Contact Details:

Name	Designation	Contact
Immaneid aajob	Organisational Head	gimeajob@gmail.com

4.5 Process Documentation

- FTK Imager Version 3.3.0 User Guide user manual link
<https://support.accessdata.com/hc/en-us/articles/204275735-FTK-Imager-version-3-3-0-User-Guide>
- Autopsy installation manual https://sleuthkit.org/autopsy/docs/userdocs/4.0/installation_page.html
- Tableau Write blocker tool user guide
<https://h11dfs.com/wpcontent/uploads/2017/07/Tableau-Forensic-Universal-Bridge-Integration-Guide.pdf>
- HxD hex editor documentation and licensing <https://mh-nexus.de/en/hxd/license.php>
- EXIFTool v13.04 documentation <https://exiftool.org/ExifTool.html>

5. Conclusion

From the evidence report (Section 4.1) submitted it is evident that the user has violated the policy even after awarding a warning on May 2004 for such activities. The investigation carried out in this report also presents the intention of the suspect to hide evidences across the file stream and tampering files. The influence of the book "*Catch Me If You Can*" on the employee's behavior opens intriguing possibilities and might have acted as a catalyst for the unusual actions. Alongside other findings and legal factors, the detailed cyber forensic analysis provides a solid foundation for the organization to take steps to address and resolve the policy violation.

6. References

- Gehl, R., Plecas, D., 2017b. Chapter 8: Crime Scene Management [online]. *Pressbooks*. Available at: <https://pressbooks.bccampus.ca/criminalinvestigation/chapter/chapter-8-crime-scene-management/>.
- Alexander, S., 2018. Understanding Deleted Files and What They Mean [online]. hgexperts.com. Available at: <https://www.hgexperts.com/expert-witness-articles/understanding-deleted-files-and-what-they-mean-44950> [Accessed 1 December 2024].
- Wikipedia contributors, 2024. List of file signatures [online]. Wikipedia. Available at: https://en.wikipedia.org/wiki/List_of_file_signatures.
- Anon, FPX File: How to open FPX file (and what it is) [online]. file.org. Available at: <https://file.org/extension/fpx>.
- Parvez, 2010. Hiding malicious files in Windows folders – GreyHatHacker.NET [online]. Available at: <https://www.greyhathacker.net/?p=216>.
- Aleksey, 2024. TryHackMe writeup: Digital Forensics Case B4DM755 - InfoSec Write-ups [online]. Medium. Available at: <https://infosecwriteups.com/tryhackme-writeup-digital-forensics-case-b4dm755-e196e00eae9a>.

- Anon, 2008. ..Jpg pictures received as .dat files [online]. Tech Support Guy. Available at: <https://www.techguy.org/threads/jpg-pictures-received-as-dat-files.677321/>.