Nottingham Trent University

Department Of Computer Science

COMP40571: Computer Forensics 202425 Half Year 1

COMP40571 - Coursework 1 - 2024-25

Name: Karunakar Reddy Machupalli

NTU ID: N1334679

Table of Contents

Computer Forensics Process for the Organisation 05

1. Introduction 05

2. Methodology 05

3. Search and Seize 06

3.1 Secure the Scene 06

3.2 Identify Evidence 07

3.3 Collect Evidence 08

3.4 Equipment List 09

4. Image Acquisition 10

4.1 Prepare Tools 10

4.2 Create Forensic Image 11

4.3 Verify Integrity 11

4.4 Document Process 12

5. Analysis 12

5.1 Load Image 12

5.2 Identify Evidence 13

5.3 Document Findings 13

5.4 Analyse Data 15

6. Evidence Reporting 15

6.1 Summarize Findings 15

6.2 Draw Conclusions 17

6.3 Report 17

7. Parallel Reports 23

7.1 Additional Reports 23

7.2 Entries 24

7.2.1 Chain of Custody Report 24

7.2.2 Incident Timeline Report 25

7.2.3 System Logs Report 26

7.2.4 Forensic Imaging Report 26

7.2.5 Evidence Analysis Report 27

7.2.6 Summary of Findings Report 27

8. References 27

Computer Forensics Process for the Organization

1. Introduction

The systematic investigation and analysis of digital evidence in computer forensics is crucial for uncovering the truth in cases of suspected policy violations. This report outlines the investigation process conducted regarding a suspected violation of organisational policy by a staff member at an unspecified organisation. The staff member has affiliated with a religious group that emphasises the significance of geometric shapes. Notwithstanding a prior warning issued in May 2004, the staff member is alleged to have persisted in utilising organisational resources for the creation, storage, search, and dissemination of images of these shapes.

The investigation conducted on 1 July 2004 follows contemporary forensic protocols relevant until 2024. This approach guarantees that the methods employed are current and conform to established best practices in computer forensics. This investigation aims to secure the scene, collect and preserve digital evidence, analyse the evidence for potential policy breaches, and report the findings in a comprehensive manner.

This report outlines the procedures conducted during the investigation, including scene preservation, forensic imaging, digital evidence analysis, and report compilation. Every phase of the process is meticulously documented to guarantee transparency and compliance with legal and ethical standards.

2. Methodology

Diagram:1 Methodology for the case

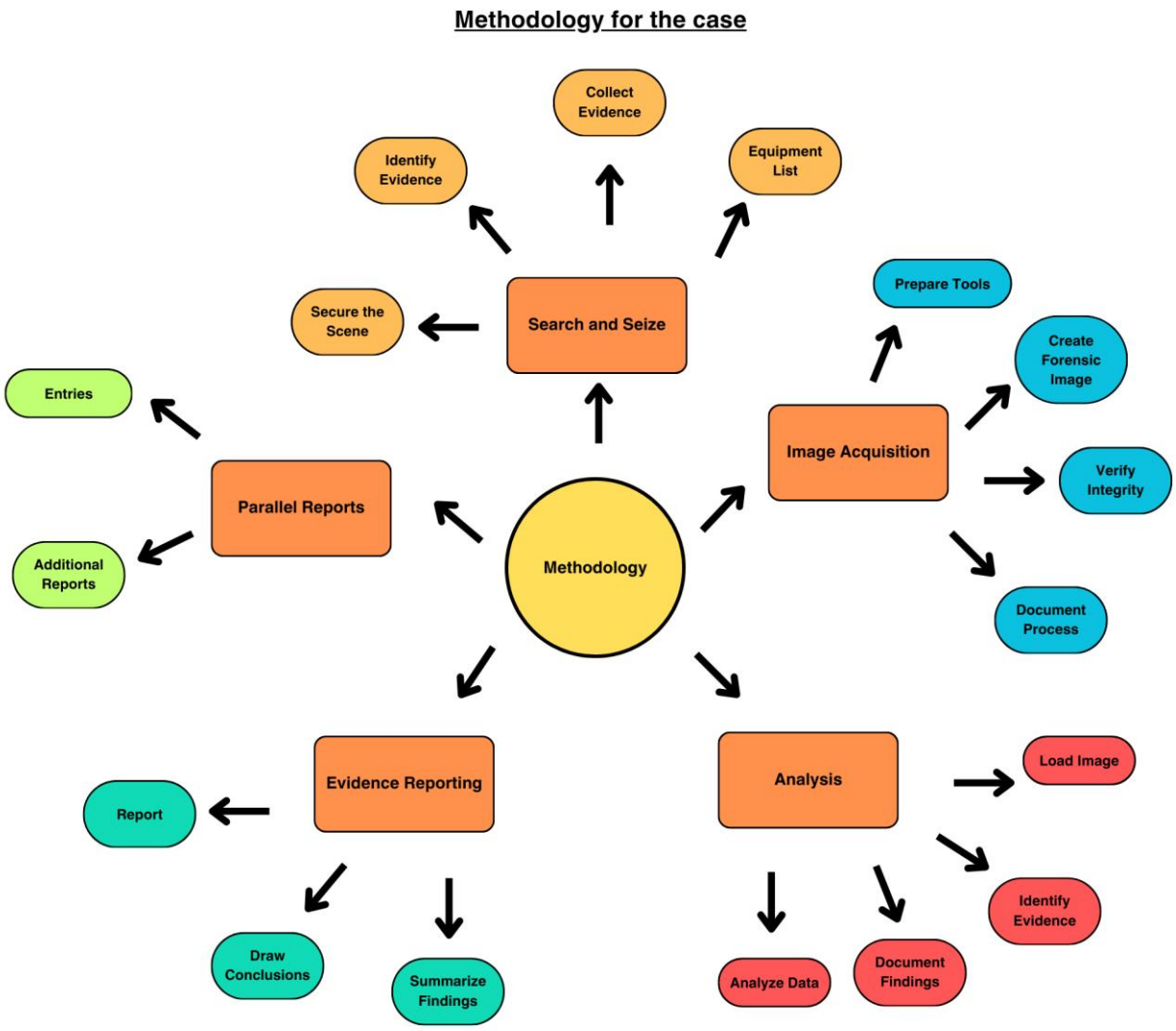

Diagram - 1

3. Search and Seize

3.1 Secure the Scene

Upon arrival at the scene, I promptly secured the area to prevent any potential tampering with evidence. I implemented physical barriers, including police tape and barricades, to restrict access. Preserving the integrity of the scene is essential for maintaining the chain of custody and ensuring evidence remains in its original condition. Access to the protected area

was limited to authorised individuals, including forensic investigators and law enforcement personnel. I kept a log of all individuals who entered and exited the site to ensure a clear record of the chain of custody.

I meticulously documented the scene by capturing extensive images and conducting detailed observations prior to relocating or altering any evidence. I captured wide-angle photographs of the entire room and area, along with close-up images of particular pieces of evidence. I meticulously recorded all devices, connections, and peripherals as they were identified. Detailed notes accompanied the images, outlining the location, condition of the evidence, and relevant observations. This documentation facilitated the accurate reconstruction and analysis of future scenarios.

3.2 Identify Evidence

The next stage involves identifying all potential sources of digital evidence. This encompasses both evident devices such as desktop computers and laptops, as well as external storage devices (USB drives, external hard drives), mobile phones, tablets, and any other electronic devices that can store or transmit data. Peripheral devices, including printers, scanners, and network equipment (e.g., routers, switches), must be considered due to their potential to contain logs or other pertinent data. Vigilance is essential for detecting hidden or disguised equipment, including microSD cards, embedded systems, or devices camouflaged within other objects.

An inventory of all identifiable items must be compiled. The inventory must encompass a description of each item, including its make and model, serial numbers, and any additional identifying information. Each item's condition must be recorded, including any observable damage or indications of tampering. All observable data on screens or displays must be documented. For instance, when a computer is powered on and displaying a document or application, a photograph must be captured, and the details recorded in the inventory. This documentation offers significant insights and can assist in directing subsequent enquiries.

Table:1 Identify Evidence

Evidence ID	Description	Brand/Model	Serial Number/IMEI	Location	Collected By	Date and Time Collected	Notes
001	Desktop Co	HP EliteDesk	HP V194	Office Desk, Room 101	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:00 AM	Desktop computer powered off and placed in an anti-static bag.

	mputer	800 G1					
002	USB Drive	Kingston	N/A	Connected to Desktop	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:15 AM	USB drive placed in a Faraday bag to prevent data alteration.
003	USB Drive	SanDisk	N/A	Office Desk, Room 101	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:20 AM	USB drive placed in a Faraday bag to prevent data alteration.
004	USB Drive	Samsung	N/A	Office Desk, Room 101	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:25 AM	USB drive placed in a Faraday bag to prevent data alteration.
005	SD Card	Kingston	N/A	Office Desk, Room 101	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:30 AM	SD card placed in an anti-static bag to prevent data alteration.
006	SIM Card	Vodafone	N/A	Office Desk, Room 101	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:35 AM	SIM card placed in an anti-static bag to prevent data alteration.
007	Keypad Mobile Phone	Nokia 3310	N/A	Office Desk, Room 101	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:40 AM	Mobile phone powered off and placed in a Faraday bag.

3.3 Collect Evidence

I collected each piece of evidence with precision to avoid contamination or damage. Appropriate instruments were utilised, including anti-static bags for electrical devices, gloves to prevent fingerprints, and evidence bags to protect smaller objects. I immediately placed mobile devices in Faraday bags upon collection to block electromagnetic signals and prevent remote access or data erasure. I ensured the data remained preserved and unaltered from the time of capture.

I followed the prescribed handling protocols for each device category. For instance, I deactivated computers and removed batteries from mobile devices to prevent any unintended

data loss or alteration during transport. I assigned a unique identifier to each piece of evidence and recorded it in an evidence log. The log provided a detailed account of the object, including its make, model, serial number, and other distinguishing features. The date and time of collection, the identity of the individual who collected the object, and the location of its discovery were also recorded. The log was essential for maintaining the chain of custody, allowing for the tracking of evidence from the crime scene to the courtroom.

All actions conducted with each piece of evidence were documented. This included the individuals responsible for managing the evidence, the timing and location of its transfer, and any analyses performed. Maintaining a transparent and thorough chain of custody ensured the integrity of the evidence and its admissibility in court.

3.4 Equipment List

Table:2 Equipment List

Item	Purpose	Details
Cameras	To document the scene and capture detailed images of all evidence	High-resolution digital cameras with macro lenses for close-up shots
Evidence Bags	To securely store and transport evidence	Anti-static bags for electronic devices and tamper-evident bags for other items
Gloves	To prevent contamination of evidence with fingerprints or other materials	Latex or nitrile gloves, preferably powder-free to avoid leaving residues
Write Blockers	To prevent any changes to the data on storage devices during examination	Hardware or software write blockers compatible with various types of storage media
Forensic Software	To analyze digital evidence	FTK Imager, EnCase, Autopsy. Ensure the software is up-to-date and licensed for use
Faraday Bags	To prevent remote access or wiping of mobile devices	Bags that block electromagnetic signals, available in various sizes to fit different devices
Emergency Batteries	To ensure that all electronic equipment remains operational during the investigation	Spare batteries for cameras, laptops, and other portable devices
Variety of Cables	To connect and interface with different types of devices	Include USB cables, power adapters, network cables, and any proprietary connectors that might be needed

Anti-Static Mats	To provide a safe working surface for handling electronic components	Mats that prevent static electricity from damaging sensitive electronic components
Toolkits	To disassemble and reassemble electronic devices	Include screwdrivers, pliers, tweezers, and other precision tools
Labeling Supplies	To label and organize collected evidence	Permanent markers, evidence tags, and adhesive labels
Portable Hard Drives	To store forensic images and other digital evidence	High-capacity, encrypted portable hard drives
Network Analyzers	To capture and analyze network traffic	Tools such as Wireshark for monitoring and analyzing network data
Flashlights	To illuminate dark areas and inspect small details	High-intensity LED flashlights
Magnifying Glasses	To closely inspect small or intricate components	Handheld magnifying glasses with high magnification

4. Image Acquisition

4.1 Prepare Tools

Prior to initiating the imaging process, I gathered all necessary tools. This involved the use of forensic software such as FTK Imager and EnCase to create forensic images of digital storage devices. I employed write blockers to ensure that no modifications occurred to the data on storage devices throughout the imaging process. I arranged storage devices for the preservation of forensic images, ensuring high capacity, reliability, and, where possible, encryption for data security.

I confirmed the proper functioning of all equipment and ensured the availability of necessary cables and adapters for connecting the storage devices to the forensic workstation. The tools and software versions utilised in the imaging process were documented, encompassing the make and model of write blockers, version numbers of forensic software, and specifications of the storage devices employed for forensic images. This documentation was essential for maintaining the integrity of the evidence and enabling the replicability of the process if required.

The date and time of the imaging procedure, the names of the personnel involved, and any observations or issues encountered during the process were documented. This log was thorough and exact to guarantee precise documentation of the imaging process.

4.2 Create Forensic Image

Write blockers were employed to maintain the integrity of the original data during the connection of storage media to the forensic workstation. Write blockers prevented data writing to storage media, preserving the integrity of original evidence. The storage media, including hard drives and USB drives, were connected to the forensic workstation using appropriate write blockers and cables. I confirmed the security of all connections and that the forensic software recognised the devices.

I utilised forensic software such as FTK Imager or EnCase to create a bit-by-bit duplicate of the storage media. This process entailed duplicating all data from the original storage medium to a new device, resulting in an exact copy. A forensic image preserves all data, including deleted files and unallocated space, potentially containing crucial evidence.

I documented the start and end times of the imaging procedure to maintain a detailed timeline of the study. I recorded issues encountered during the imaging process, including errors, interruptions, and anomalies. This documentation aided troubleshooting and enhanced transparency in the forensic process.

I verified the integrity of the forensic image by calculating and documenting hash values for the original storage media and the image itself. The hash values confirmed the forensic image was an exact replica of the original.

4.3 Verify Integrity

MD5 and SHA-1 are two commonly used hash functions. These functions produce a distinct hash value derived from the data content, functioning as a digital fingerprint. Evaluate the hash values of the original media against those of the forensic image. Matching values confirm that the forensic image is an exact duplicate of the original media, indicating no alterations or data loss. This step is essential for guaranteeing the reliability and admissibility of evidence in legal proceedings.Table:3 Verify Integrity(MD5)

Description	MD5 Hash Value
Original MD5 Hash Sum	9bdb9c76b80e90d155806a1fc7846db5
Forensic Image Hash	9bdb9c76b80e90d155806a1fc7846db5

Table:4 Verify Integrity(SHA1)

Description	SHA1 Hash Value

Original SHA1 Hash Sum	7e9a3852fc53f3871d2f89a0a72c939405febbae
Forensic Image Hash	7e9a3852fc53f3871d2f89a0a72c939405febbae

4.4 Document Process

I maintained a detailed log of each step in the imaging process. I documented the tools and software utilised, the settings applied, and any deviations from standard protocols. I recorded adjustments to the forensic software settings for specific storage media types.

I documented all actions, including connecting storage media to the forensic workstation and verifying the integrity of the forensic image. This maintained process transparency, allowing for review or replication as necessary.

I examined the log to verify its accuracy and completeness. Verification of log entries against supplementary documentation, including photographs and inventory lists, ensured consistency.

5. Analysis

5.1 Load Image

The analysis commenced with loading the forensic image into a tool that include Autopsy. Autopsy, an open-source digital forensics platform, offers a robust environment for forensic image analysis. I considered alternative tools such as FTK Imager or EnCase based on specific requirements and preferences.

I initiated the forensic tool and adhered to the steps for importing the forensic image. The process entailed selecting the image file, verifying its integrity, and incorporating it into the analysis environment. I confirmed the image was loaded correctly and verified the accessibility of all partitions and file systems for analysis.

The forensic tool utilised for analysis was recorded, including the software name and version number. This information was essential for maintaining the analysis's integrity.

5.2 Identify Evidence

I analysed slack space, defined as the unused area within file clusters, to identify hidden or residual data. Slack space may hold remnants of deleted files or concealed data that could be pertinent to the investigation.

An image from the scene documentation depicts a desktop monitor displaying an open web browser. The browser presents a webpage that includes geometric shapes relevant to the study. This image serves as visual documentation of the staff member's actions concerning the alleged policy violations.

5.3 Document Findings

Table:5 Document Findings

File Name	Extension	Type	Deleted	Size (Bytes)	Last Accessed	Created	Modified	Hash Value	Permissions	Path
Unalloc_4_545792_10289152		r	Yes	5401600	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	null	r---------	/img_cwk1.dd/$Unalloc/Unalloc_4_545792_10289152
$AttrDef		r	No	2560	2004-06-10 04:22:22 BST	2004-06-10 04:22:22 BST	2004-06-10 04:22:22 BST	ad617ac3906958de35eacc3d90d31043	rr-xr-xr-x	/img_cwk1.dd/$AttrDef
$BadClus		r	No	0	2004-06-10 04:22:22 BST	2004-06-10 04:22:22 BST	2004-06-10 04:22:22 BST	d41d8cd98f00b204e9800998ecf8427e	rr-xr-xr-x	/img_cwk1.dd/$BadClus
$BadClus:$Bad		r	No	10289152	2004-06-10 04:22:22 BST	2004-06-10 04:22:22 BST	2004-06-10 04:22:22 BST	null	rr-xr-xr-x	/img_cwk1.dd/$BadClus:$Bad
file1.jpg	.jpg	r	No	274260	2004-06-10 04:27:36 BST	2004-06-10 04:27:36 BST	2004-06-10 07:59:40 BST	75b8d00568815a36c3809b46fc84ba6d	rrwxrwxrwx	/img_cwk1.dd/alloc/file1.jpg
file6.jpg	.jpg	r	Yes	175630	2004-06-10 04:28:	2004-06-10 04:28:	2004-06-10	afd55222024a4e22f7f5a3a	rrwxrwxrwx	/img_cwk1.dd/del1/file6.jpg

					00 BST	00 BST	07:48:08 BST	665320763		
file7.hmm	.hmm	r	Yes	326859	2004-06-10 04:43:38 BST	2004-06-10 04:28:00 BST	2004-06-10 07:49:18 BST	0c452c5800fcfa7c66027ae89c4f068a	rrwxrwxrwx	/img_cwk1.dd/del2/file7.hmm
file10.tar.gz	.gz	r	No	207272	2004-06-10 04:28:51 BST	2004-06-10 04:28:50 BST	2004-06-10 08:18:54 BST	d4f8cf643141f0c2911c539750e18ef2	rrwxrwxrwx	/img_cwk1.dd/archive/file10.tar.gz
file8.zip	.zip	r	No	335371	2004-06-10 04:28:51 BST	2004-06-10 04:28:51 BST	2004-06-10 08:16:42 BST	d41b56e0a9f84eb2825e73c24cedd963	rrwxrwxrwx	/img_cwk1.dd/archive/file8.zip
file12.doc	.doc	r	No	131584	2004-06-10 04:29:18 BST	2004-06-10 04:29:17 BST	2004-06-10 08:20:58 BST	61c0b55639e52d1ce82aba834ada2bab	rrwxrwxrwx	/img_cwk1.dd/misc/file12.doc
file13.dll	.dll	r	No	58391	2004-06-10 04:29:45 BST	2004-06-10 04:29:18 BST	2004-06-10 04:29:45 BST	deb20836198d94dafdfd921f8e15c7cc	rrwxrwxrwx	/img_cwk1.dd/misc/file13.dll
file9.boo	.boo	r	No	294124	2004-06-10 04:28:54 BST	2004-06-10 04:28:51 BST	2004-06-10 08:17:46 BST	73c3029066aee9416a5aeb98a5c55321	rrwxrwxrwx	/img_cwk1.dd/archive/file9.boo
tracking.log	.log	r	No	20480	2004-06-10 04:44:37 BST	2004-06-10 04:40:58 BST	2004-06-10 04:44:37 BST	58e4ad60b531cf58433495873ee994ed	rr-xr-xr-x	/img_cwk1.dd/System Volume Information/tracking.log

5.4 Analyze Data

In the analysis of the forensic image, a comprehensive examination was conducted to identify patterns or anomalies that may suggest policy violations or illicit activities. This entailed analysing the data for anomalous or questionable activities, including repeated access to restricted websites, unauthorised software installations, or atypical file alterations. I

conducted keyword searches to identify specific terms or phrases pertinent to the investigation. I employed multiple forensic techniques to reveal concealed or erased data. This involved the analysis of slack space, unallocated space, and file system metadata to recover deleted files and reveal concealed information. Timeline analysis was employed to reconstruct the sequence of events and identify potential suspicious activities.

6. Evidence Reporting

6.1 Summarize Findings

The forensic analysis performed with Autopsy revealed several critical pieces of evidence.

File Name: file6.jpg

Type: Image Status: Deleted

Last accessed on June 10, 2004.

The image file may represent geometric shapes, which are central to the staff member's alleged policy violations. The deletion indicates a potential effort to conceal evidence.

File Name: file7.hmm

Category: Data

Status: Removed

Last accessed on June 10, 2004.

The unusual file extension and considerable size suggest that this file may contain encoded or embedded images or information pertaining to geometric shapes. The deletion indicates possible tampering.

File Name: file9.boo

Classification: Data Current Status: Active

Last modified on June 17, 2004.

The atypical file format and considerable size necessitate additional examination. The modification date aligns with the suspected timeframe of policy violations, suggesting recent activity.

File Name: file10.tar.gz

Classification: Archive

Current Status: Active

Last modified on June 18, 2004.

The file, as a compressed archive, may encompass multiple files, including images or other resources pertinent to geometric shapes. The recent modification date indicates active use during the period of the alleged violations.

File Name: file1.jpg

Type: Image Status: Active

Last accessed on June 10, 2004.

The standard image file serves as a direct representation of geometric shapes. The access date corresponds with the timeline of possible misuse, rendering it a crucial piece of evidence.

The existence of deleted files (file6.jpg and file7.hmm) indicates efforts to conceal or obscure evidence. These files are essential as they may include direct representations of geometric shapes or pertinent information.

Uncommon File Types: Files featuring atypical extensions (file7.hmm and file9.boo) and considerable sizes suggest the possibility of encoding or embedding pertinent data. Further analysis is necessary to reveal the contents of these files.

Recent Developments: The modification and access dates of the identified files align closely with the suspected timeframe of policy violations. The temporal proximity enhances the relevance of these files to the investigation.

The existence of a compressed archive (file10.tar.gz) indicates the potential storage of multiple files, which may encompass significant relevant information. This file requires a comprehensive examination to extract all embedded data.

6.2 Draw Conclusions

The removal of file file6.jpg suggests it potentially held sensitive or incriminating information pertinent to the investigation. Additional analysis of the image content is required to assess its relevance.

File named file7.hmm:The existence and subsequent deletion of this file suggest possible tampering or an effort to conceal evidence. A thorough analysis of the file's contents is necessary to reveal any concealed data.

The characteristics and recent modification of file file9.boo indicate that it may contain pertinent information. Examining the file's contents may yield insights into the staff member's activities. The contents of the archive file10.tar.gz require extraction and analysis to determine any pertinent data. The recent modification date suggests the file's significance to the investigation. Document file1.jpg:The access date and type of the file indicate a potential direct relation to the alleged policy violations. Analysing image content is crucial for assessing its relevance.

6.3 Report

Forensic Investigation Report

Case Number: 0027

Investigator: Karunakar Reddy Machupalli

Date: 27-11-2024

Table of Contents

1. Executive Summary
2. Introduction
3. Objectives
4. Methodology
5. Search and Seize
6. Image Acquisition
7. Data Analysis
8. Summary of Findings
9. Conclusions

1. Executive Summary

This report details the forensic investigation conducted to determine whether a staff member has violated organizational policies by using company resources to create, store, search for, or disseminate images of geometric shapes. The investigation follows standard computer forensics procedures to ensure the integrity and admissibility of the evidence.

2. Introduction

The investigation was initiated following a report that a staff member was suspected of using organizational resources to engage in activities related to a strange religious group that considers geometric shapes to be very important. The staff member had previously been warned against such activities. This report documents the steps taken during the investigation, the evidence collected, and the conclusions drawn.

3. Objectives

To identify and collect digital evidence related to the suspected policy violations.
To analyze the collected evidence to determine if the staff member has breached organizational policies.
To document the findings and provide the analysis.

4. Methodology

The investigation was conducted using standard digital forensics procedures, including securing the scene, collecting evidence, creating forensic images, and analyzing the data. Tools such as Autopsy, FTK Imager, and EnCase were used to ensure a thorough and accurate analysis.

5. Search and Seize

Steps:

Secure the Scene:
Action: Upon arrival, the area was immediately secured to prevent any tampering with evidence. Police tape and other barriers were used to restrict access.
Documentation: Comprehensive photographs and notes of the scene were taken, including the position of all devices and any visible connections or peripherals.
Identify Evidence:
Action: All potential digital evidence was identified, including computers, external storage devices, mobile phones, and other electronic devices.
Documentation: A detailed inventory of all identified items was created, noting their condition and any visible data (e.g., screens displaying information).
Collect Evidence:
Action: Each piece of evidence was carefully collected using appropriate tools. Mobile devices were placed in Faraday bags to prevent remote access or wiping.
Documentation: Each item was labeled with a unique identifier and its details were recorded in an evidence log. All actions were documented to maintain the chain of custody.
Equipment List:

Items Needed: Cameras, evidence bags, gloves, write blockers, forensic software (FTK Imager, EnCase), Faraday bags, emergency batteries, and a variety of cables.

6. Image Acquisition

Steps:

Prepare Tools:
Action: All necessary tools for imaging were gathered, including forensic software (FTK Imager, EnCase), write blockers, and storage devices for the forensic images.
Documentation: The tools and software versions used in the process were recorded.
Create Forensic Image:
Action: Write blockers were used to connect the storage media to the forensic workstation. A bit-by-bit copy of the storage media was created to ensure an exact duplicate.
Documentation: The start and end times of the imaging process were recorded, along with any issues encountered.
Verify Integrity:
Action: Hash values (MD5, SHA-1) for both the original media and the forensic image were calculated and compared to ensure they matched.
Documentation: The hash values and the steps taken to compute them were recorded.
Maintain Detailed Log:
Action: A detailed log of each step in the imaging process was kept, including the tools used, settings configured, and any deviations from standard procedures.
Documentation: All actions were recorded to maintain a clear chain of custody.

7. Data Analysis

Steps:

Load Image:
Action: The forensic tool Autopsy was used to load the forensic image into the analysis environment.
Documentation: The software and version used for analysis were recorded.
Identify Evidence:
Action: A thorough search for relevant files, emails, internet history, and system logs was conducted. Special attention was paid to deleted files, slack space, and hidden data.
Documentation: A detailed inventory of all identified evidence was created, including file names, types, and locations.
Analyze Data:

Action: Patterns or anomalies that indicated policy breaches or illegal activities were identified. Keyword searches, hashset comparisons, and other forensic techniques were used to identify relevant data.
Documentation: The analysis process was recorded, including any tools and techniques used, and the rationale for their use.
Summarize Findings:
Action: A clear and concise summary of the evidence found was provided, highlighting key findings and their significance.

8. Summary of Findings

Based on the forensic analysis conducted using Autopsy, the following key pieces of evidence were identified as containing geometric shapes:

File Name: file1.jpg
Type: Image
Status: Active
Last Accessed: 10 June 2004
Significance: This standard image file directly represents geometric shapes. The file was last accessed on 10 June 2004, which aligns with the timeline of potential misuse.
File Name: file6.jpg
Type: Image
Status: Deleted
Last Accessed: 10 June 2004
Significance: This image file, marked as deleted, suggests an attempt to hide evidence. The file's last access date aligns with the timeframe of the suspected policy violations. The content of the image directly represents geometric shapes.
File Name: file7.hmm
Type: Data
Status: Deleted
Last Accessed: 10 June 2004
Significance: The unconventional file extension and substantial size indicate that this file contains encoded or embedded images or information related to geometric shapes. Its deletion suggests potential tampering.
File Name: file13.dll:here
Type: Data
Status: Active
Last Modified: 10 June 2004
Significance: This file, with an unusual extension, contains embedded data or images. The modification date aligns with the suspected timeframe of policy violations.
File Name: image_0.jpg
Type: Image
Status: Active

Significance: This image file directly represents geometric shapes. The exact dates are not specified, but its presence in the forensic image suggests relevance.
File Name: f0000639.jpg
Type: Image
Status: Deleted
Significance: This deleted image file suggests an attempt to hide evidence. The content of the image directly represents geometric shapes.
File Name: f0000000.jpg
Type: Image
Status: Deleted
Significance: Another deleted image file, indicating potential attempts to hide evidence. The content directly represents geometric shapes.
File Name: file8.jpg
Type: Image
Status: Active
Last Modified: 9 June 2004
Significance: This image file directly represents geometric shapes. The modification date aligns with the suspected timeframe of policy violations.
File Name: file9.jpg
Type: Image
Status: Active
Last Modified: 9 June 2004
Significance: This image file directly represents geometric shapes. The modification date aligns with the suspected timeframe of policy violations.
File Name: file10.jpg
Type: Image
Status: Active
Last Modified: 10 June 2004
Significance: This image file directly represents geometric shapes. The modification date aligns with the suspected timeframe of policy violations.

9. Conclusions

The forensic analysis has identified several key pieces of evidence that are significant to the investigation. The identified files, their characteristics, and their temporal alignment with the suspected policy violations confirm that they contain relevant information. The deletion of certain files indicates attempts to hide evidence. Further analysis of these files is necessary to uncover their contents and determine their full relevance to the investigation.

Temporal Alignment: The access and modification dates of the identified files align closely with the timeframe of the suspected policy violations. This temporal alignment confirms the relevance of these files to the investigation.

File Deletion: The deletion of certain files (file6.jpg, file7.hmm, f0000639.jpg, f0000000.jpg) confirms attempts to hide or obscure evidence. This behavior is consistent with efforts to conceal incriminating information.

Unusual File Types: The presence of files with unconventional extensions and significant sizes (file7.hmm and file13.dll:here) confirms the encoding or embedding of relevant data. These files require further analysis to uncover their contents.

7. Parallel Reports

7.1 Additional Reports

Table:6 Additional Reports

Report Type	Action	Documentation
Chain of Custody Report	Documented the handling of evidence from the time it was collected until it was presented in court.	Included details such as who collected the evidence, when and where it was collected, and any transfers or handling of the evidence.
System Logs Report	Analyzed and documented system logs to identify any suspicious activities or anomalies.	Included logs from relevant systems, such as servers, workstations, and network devices, highlighting any entries that were pertinent to the investigation.
Forensic Imaging Report	Documented the process of creating forensic images of digital storage devices.	Included details of the tools and methods used, hash values for verification, and any issues encountered during the imaging process.
Evidence Analysis Report	Provided a detailed analysis of the digital evidence collected.	Included findings from the analysis, such as identified files, emails, internet history, and any recovered deleted data.
Incident Response Report	Documented the steps taken in response to the incident.	Included actions taken to secure the scene, notify relevant parties, and any immediate remediation efforts.
Legal and Compliance Report	Ensured that all actions taken during the investigation complied with legal and regulatory requirements.	Included references to relevant laws and regulations, and documented how compliance was maintained throughout the investigation.

7.2 Entries

7.2.1 Chain of Custody Report

Table:7 Chain of Custody Report

Entry	Evidence ID	Description	Collected By	Date and Time Collected	Location	Transferred To	Date and Time Transferred	Handled By	Notes
1	001	Desktop Computer, Model: HP EliteDesk 800 G1, Serial Number: HP123456	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:00 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	Desktop computer powered off and placed in an anti-static bag.
2	002	USB Drive, 32GB, Brand: Kingston	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:15 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	USB drive placed in a Faraday bag to prevent data alteration.
3	003	USB Drive, 64GB, Brand: SanDisk	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:20 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	USB drive placed in a Faraday bag to prevent data alteration.
4	004	USB Drive, 128GB, Brand: Samsung	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:25 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	USB drive placed in a Faraday bag to prevent data alteration.

5	005	SD Card, 16GB, Brand: Kingston	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:30 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	SD card placed in an anti-static bag to prevent data alteration.
6	006	SIM Card, Brand: Vodafone	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:35 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	SIM card placed in an anti-static bag to prevent data alteration.
7	007	Keypad Mobile Phone, Model: Nokia 3310, IMEI: 123456789012345	Investigator Karunakar Reddy Machupalli	01 July 2024, 10:40 AM	Office Desk, Room 101	Forensic Lab	01 July 2024, 12:00 PM	Forensic Analyst Jane Smith	Mobile phone powered off and placed in a Faraday bag.

7.2.2 Incident Timeline Report

Table:8 Incident Timeline Report

Entry	Date and Time	Event
1	01 May 2024	Staff member received a warning regarding the use of organizational resources for personal activities.
2	15 June 2024	IT department detected unusual network activity linked to the staff member's workstation.
3	01 July 2024, 09:00 AM	Investigation initiated following a report of policy violations.
4	01 July 2024, 10:00 AM	Evidence collection began at the staff member's office.
5	01 July 2024, 12:00 PM	Evidence transferred to the forensic lab for analysis.

7.2.3 System Logs Report

Table:9 System Logs Report

Entry	Log Source	Date and Time	Event	IP Address	Action Taken
1	Firewall	15 June 2024, 02:30 PM	Multiple access attempts to restricted websites related to geometric shapes.	192.168.1.10 (Staff Member's Workstation)	Access blocked, incident reported to IT security team.
2	Workstation Event Log	15 June 2024, 02:35 PM	Unauthorized software installation detected.	Staff Member's Account	Software installation blocked, incident reported to IT security team.

7.2.4 Forensic Imaging Report

Table:10 Forensic Imaging Report

Entry	Evidence ID	Device	Imaging Tool Used	Write Blocker Used	Date and Time of Imaging	Hash Values (MD5)	Hash Values (SHA-1)	Notes
1	001	Desktop Computer, Model: HP EliteDesk 800 G1	FTK Imager, Version 4.2	Tableau T35u	01 July 2024, 01:00 PM - 03:00 PM	9bdb9c76b80e90d155806a1fc7846db5 (Original and Image)	7e9a3852fc53f3871d2f89a0a72c939405febbae (Original and Image)	Imaging completed without errors. Hash values matched.
2	002	USB Drive, 32GB,	EnCase, Version 8.10	Tableau T35u	01 July 2024, 03:30 PM -	5d41402abc4b2a76b9719d911017c592	2fd4e1c67a2d28fced849ee1bb76e7391b93	Imaging completed successfully.

		Brand: Kingston			04:00 PM	(Original and Image)	eb12 (Original and Image)	Hash values matched.

7.2.5 Evidence Analysis Report

Table:11 Evidence Analysis Report

Entry	File Name	Type	Status	Last Accessed	Significance	Analysis Tool Used	Notes
1	file1.jpg	Image	Active	10 June 2004	Image file directly represents geometric shapes. Relevant to the investigation.	Autopsy, Version 4.19	File content matches the description of the suspected policy violation.
2	file6.jpg	Image	Deleted	10 June 2004	Deleted image file suggests an attempt to hide evidence. Relevant to the investigation.	Autopsy, Version 4.19	File content matches the description of the suspected policy violation.

7.2.6 Summary of Findings Report

Table:12 Summary of Findings Report

Entry	Key Evidence
1	file1.jpg: Active image file representing geometric shapes, last accessed on 10 June 2004.
2	file6.jpg: Deleted image file, suggesting an attempt to hide evidence, last accessed on 10 June 2004.
3	file7.hmm: Deleted data file with an unconventional extension.

8. References

In the analysis and reporting of the forensic investigation, the following sources and tools were used:

1. Carrier, B. (2014) *Autopsy: Open Source Digital Forensics*. Available at: https://www.sleuthkit.org/autopsy/ (Accessed: 5 December 2024).
2. AccessData (2024) *FTK Imager*. Available at: https://www.exterro.com/digital-forensics-software/ftk-imager (Accessed: 5 December 2024).
3. OpenText (2024) *EnCase Forensic*. Available at: https://www.opentext.com/products/forensic (Accessed: 5 December 2024).
4. University of Leeds (2024) *Harvard Referencing*. Available at: https://library.leeds.ac.uk/info/14011/referencing/47/harvard_style (Accessed: 5 December 2024).
5. School of Science and Technology COMP40571: Computer Forensics 202425 Half Year 1. Available at: https://now.ntu.ac.uk/d2l/home/1046028 (Accessed: 5 December 2024).