



Course Work

ST4060CEM

Digital Forensic Fundamental



Submitted by
Suvani Basnet

Submitted to
Prof.Ganesh Bhusal



Acknowledgement

The success and final outcome of the assignment required a lot of guidance and assistance from plethora of websites and my module teacher. I am extremely fortunate to have got this all along the completion of my final course work. Whatever I have done I only due to such guidance and assistance and I won't forget to thank them. I respect and thank Mr Ganesh Bhushal for giving me an opportunity to do this assignment work and providing all support and guidance.



EXECUTIVE SUMMARY



In the realm of digital forensics, understanding and addressing the complexities of cybercrimes and mobile device-related criminal activities are paramount. This executive summary delves into two distinct scenarios: deliberate email server shutdown and the role of mobile devices in criminal investigations. Through comprehensive examination and recommendations, this summary underscores the significance of proactive prevention and meticulous investigative procedures. This assignment underscores the necessity of proactive prevention and robust investigation techniques in addressing cybercrimes and mobile device-related criminal activities. By adhering to best practices, leveraging specialized tools, and fostering awareness, digital forensics can effectively combat modern challenges and contribute to a secure digital landscape.

Contents

Case Study of Dr Smith	7
Causes of Email Server Shutdown	7
1. Hardware problems	7
2. Malicious Code Exploitation	7
3. Denial-of-Service (DoS) Attack.....	9
4. Zero-Day Vulnerability	10
5. Malware Infection.....	10
6. System Misconfiguration	11
7. Insider Threat	11
Sources of evidence.....	12
Incident Response for email server being shut down.....	12
Preliminary Assessment	12
Securing the Crime Scene	12
Obtaining Legal Authorization.....	13
Collection of Physical Evidence	13
Preservation of Digital Evidence.....	13
Analysis of Digital Evidence.....	14
Documentation and Reporting	16
Prevention of such scenarios in future	16
ACPO principle in Dr.Smith's Case.....	18
Chain of custody	19
Unveiling the dark side: Mobile phone as tools for modern criminal activities	21
Unmasking Common (Mobile) Cyber Crimes	21
Importance of Call Logs, History, and Network Data in Investigations	22
Protecting digital assets: defending against online crimes.....	23
Hypothetical Scenario: Theft of Sensitive Data from Mobile Devices.....	23
Source of evidence	24
.....	24
The guidelines to be followed while investigating.....	24

Crime Scene Investigation	25
ACPO principle 3	26
Records to maintain.....	26
Device Identification and seizure	27
Forensic Imaging.....	27
Data extraction/analysis	28
Data Recovery	28
Damaged Phone	29
State	29
Difficulties.....	30
Investigation process	30
Burnt down phone.....	31
Difficulties.....	31
Investigation-methods	32
Water Damaged Phone.....	33
Difficulties.....	33
Investigation-methods	34
References	35

Table of figures

Figure 1:mail	
Figure 2 antivirus activation in windows.....	8
Figure 3: using snort for intrusion detection.....	8
Figure 4: using wire shark to monitor network.....	9
Figure 5: using tor's hammer to look out for ddos attack.....	9
Figure 6:using Nmap for scanning.....	10
Figure 7:using Malwarebytes to scan the potential malware.....	10
Figure 8creating a virtualized environment in sandbox to examine malware information	11
Figure 9: sources of evidence	12
Figure 10:using encase tool to perform the system's further analysis	14
Figure 11:wire shark to find the evidence of a network traffic.....	15
Figure 12:configuring autopsy for comprehensive analysis	15
Figure 13:using volatility for memory forensic of the employee's computer	15
Figure 14:sources of evidence	24
Figure 15:faraday's bag.....	27
Figure 16:ftk imager for data extraction	28
Figure 17:celebrite UFED tool for extraction and analysis of mobile data.....	28
Figure 18:encase tool for data recovery.....	29
Figure 19:condition of damaged phone	29
Figure 20:condition of a burnt phone.....	31
Figure 21:condition of a water damaged phone.....	33

Case Study of Dr Smith

D. Smith, a contract employee, intentionally sent a file named 'ZIP-78' to the organization's email server, resulting in a complete shutdown and substantial financial losses. This incident emphasizes the significance of recognizing the risks associated with file downloads and underscores the importance of robust security measures and employee awareness. Our forensic investigation aims to determine the cause, collect evidence, and offer preventive recommendations against similar attacks.

Causes of Email Server Shutdown

1. Hardware problems

Hardware issues can cause email server shutdowns. Faulty components like servers, storage devices, network equipment, or power supply units can lead to crashes or failures, disrupting server functionality. Timely troubleshooting, diagnostics, and maintenance are vital to address hardware problems and ensure server stability.

2. Malicious Code Exploitation

The 'ZIP-78' file could have contained harmful instructions that were specifically designed to take advantage of weaknesses in the email server. These instructions could have caused the server to crash or malfunction, similar to a computer virus.

Tools



Figure 1 antivirus activation in windows

```
(kali@kali)~/Downloads/snort/Snort_RegisteredUser_rules
$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

--= Initializing Snort ==
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702
4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 818
0:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
```

Figure 2: using snort for intrusion detection

4. Zero-Day Vulnerability

The 'ZIP-78' file could have taken advantage of a security flaw in the email server software that the organization didn't know about yet. Attackers could have discovered a secret weakness using it to harm the server, causing it to shut down. This is why it's important to regularly update software to fix known vulnerabilities.

```
(suvani@suvani)-[~]
$ nmap 192.168.1.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-07 13:53 BST
Nmap scan report for 192.168.1.100
Host is up (0.00010s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

Figure 5:using Nmap for scanning

5. Malware Infection

The 'ZIP-78' file could have contained harmful software, similar to a computer virus. When the file was opened or its contents were extracted, the harmful software infected the email server spreading through the server's files, causing disruptions and making it difficult to restore normal operations.

Tools

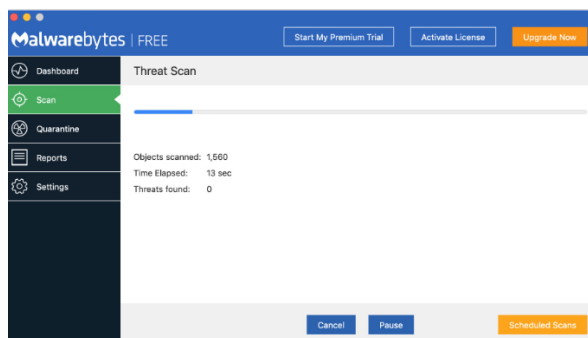


Figure 6:using Malwarebytes to scan the potential malware

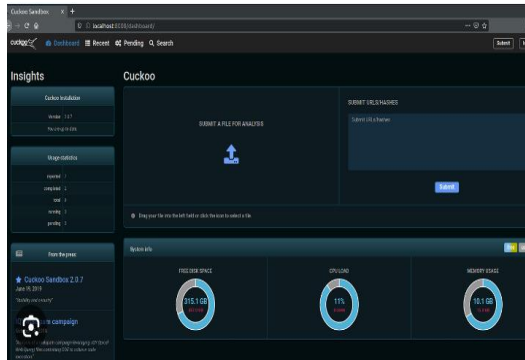


Figure 7 creating a virtualized environment in sandbox to examine malware informatio

6. System Misconfiguration

The email server might not have been set up properly or had weak security settings, of which the attackers took advantage of these weaknesses to harm the server. To prevent this, it's important to configure servers correctly and follow security best practices, such as using strong passwords and limiting access to sensitive systems.

7. Insider Threat

Smith, the contract employee, could have intentionally modified the 'ZIP-78' file to harm the organization's email server. It's like a person working from inside a company who purposely does something harmful. This highlights the importance of monitoring employees' activities and providing security awareness training to prevent insider threats.

In this scenario, a contract employee intentionally caused a complete email server shutdown. As a forensic investigator, our goal is to gather evidence, determine the extent of the damage, and identify the responsible party. By following proper procedures and utilizing forensic tools, we aim to uncover the truth behind the incident.

Sources of evidence

- Email Server Logs
- Network Traffic Logs
- System Logs
- Email Metadata
- Email Content

Figure 8: sources of evidence

Incident Response for email server being shut down

Preliminary Assessment

During this stage, I would interview potential suspects, witnesses, and the people involved in order to learn as much as I could. I would also talk with relevant staff members from the IT department, supervisors, and the people involved. Setting the incident's backdrop and attempting to map the occurrence according to other people's perspectives are the two main goals of this interview.

Securing the Crime Scene

Once on-site, it is very crucial to secure the crime scene. This may involve installing -do-not-cross-bars to isolate the crime scene in order to avoid further damage or unnecessary fingerprints, among other things. In this specific scenario, isolating the server or required devices allows me to do a full examination later to determine if needed.

Obtaining Legal Authorization

As a forensic investigator, it is vital to follow principles and norms by obtaining a legal licence and approval before moving further with the inquiry. This might take the form of a court-issued search order or the management of the organization's signed authorization. This step guarantees that I have the right to access and inspect the devices I need as an investigator.

Collection of Physical Evidence

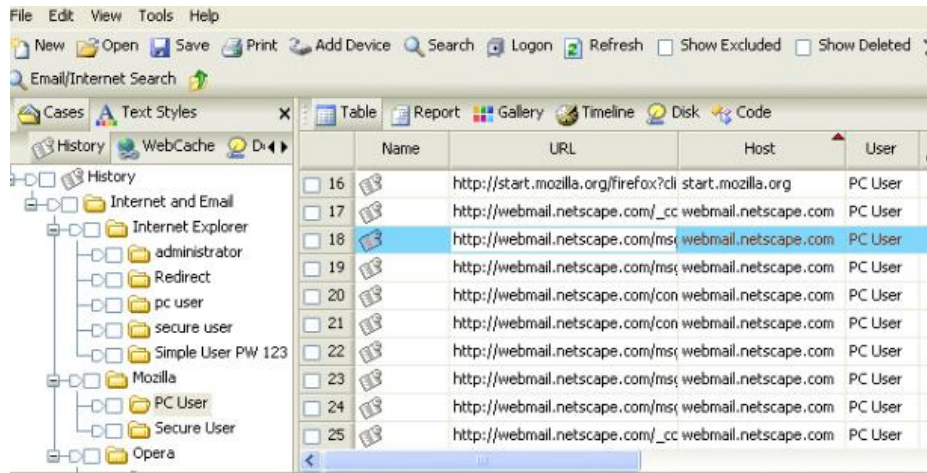
The server's physical configuration, including location connection and external storage options, would be documented during this step, and any removable media that could contain evidence would be marked and securely packed away. It is necessary to keep track of the possession and transfer of physical evidence in order to ensure its integrity for legal purposes.

Preservation of Digital Evidence

I would use specialised programmes like encase and ftk imager to produce a forensic copy of the email storage medium. I would use these copies as the foundation for my study while preserving the original data. hash values can be saved for integrity of data.

Tactics:

- Preservation of email server logs
- Using encase tool



The screenshot shows the Encase software interface. On the left is a file system tree with folders like 'Internet and Email', 'Internet Explorer', 'administrator', 'Redirect', 'pc user', 'secure user', 'Simple User PW 123', 'Mozilla', 'PC User', 'Secure User', and 'Opera'. On the right is a table with columns: Name, URL, Host, and User. The table contains 10 rows of data, with row 18 highlighted.

	Name	URL	Host	User
16		http://start.mozilla.org/firefox?cl	start.mozilla.org	PC User
17		http://webmail.netscape.com/_cc	webmail.netscape.com	PC User
18		http://webmail.netscape.com/ms	webmail.netscape.com	PC User
19		http://webmail.netscape.com/ms	webmail.netscape.com	PC User
20		http://webmail.netscape.com/con	webmail.netscape.com	PC User
21		http://webmail.netscape.com/con	webmail.netscape.com	PC User
22		http://webmail.netscape.com/ms	webmail.netscape.com	PC User
23		http://webmail.netscape.com/ms	webmail.netscape.com	PC User
24		http://webmail.netscape.com/ms	webmail.netscape.com	PC User
25		http://webmail.netscape.com/_cc	webmail.netscape.com	PC User

Figure 9: using encase tool to perform the system's further analyses

- Checking employees' email and history or browsers and email server logs.

Analysis of Digital Evidence

During the analysis phase, forensic software tools like Autopsy, Volatility, or file analysis tools are used to examine the forensic copies of the server's storage media. System logs, email metadata, and memory forensics techniques are utilized to identify suspicious activities, establish a timeline, and detect any malicious content or unauthorized activities.

Tools

[illegible]

Figure 10: wire shark to find the evidence of a network traffic

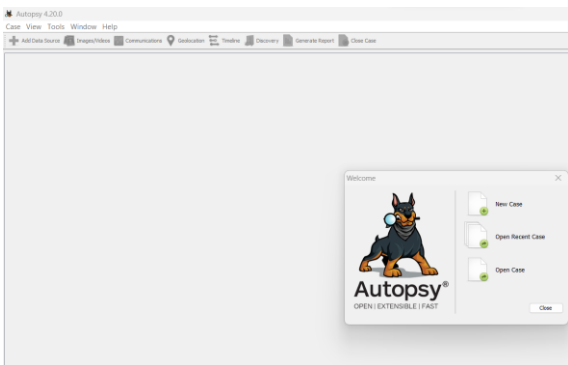


Figure 11: configuring autopsy for comprehensive analysis

```
root@kali:~# volatility -f ram.mem --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 2840
```

Figure 12:using volatility for memory forensic of the employee's computer

Documentation and Reporting

Preparing comprehensive investigation report, summarizing findings, timestamps, file paths, and supporting information. Accuracy and clarity are prioritized to provide a clear overview of the incident and the investigator's conclusions. Evidence custody forms are completed to maintain the chain of custody, ensuring evidence integrity and admissibility in legal proceedings.

- Chain of custody form

Prevention of such scenarios in future

- i. Employee Education and Awareness: Prioritize comprehensive cybersecurity training programs to educate employees about the risks of downloading files from untrusted sources, emphasize adherence to security policies, and encourage reporting of suspicious activities. Email headers are always necessary to analyse just in case for phishing attacks, tools like: mx tool email header analyser could be used
- ii. Robust Email Filtering and Security Measures: Implement advanced spam filters, antivirus software, and email security protocols (DMARC, SPF, DKIM) to detect and
- iii. block suspicious attachments, enhance email authentication, and prevent email spoofing.
- iv. Regular Software Updates and Patch Management: Establish a robust patch management process to regularly update and patch all systems, including email servers, operating systems, and applications, to address known vulnerabilities and reduce the risk of exploitation.

- v. Strong Access Controls and User Privileges: Enforce strong access controls and user privileges based on the principle of least privilege, ensuring employees have access only to the resources necessary for their job functions. Regularly review and revoke unnecessary privileges to mitigate insider threat risks.

- vi. Effective incident response plans and continuous monitoring, utilizing intrusion detection, log monitoring, and SIEM solutions, enable timely threat detection, proactive identification of suspicious activities, and swift mitigation of security incidents.

ACPO principle in Dr.Smith's Case



ASSOCIATION OF
CHIEF POLICE OFFICERS

ACPO Principle 1

Preserve digital evidence without altering or compromising its integrity during the investigation involving Dr Smith's case.

ACPO Principle 2

Demonstrate competence when accessing and analysing the 'ZIP-78' file to maintain the credibility of the evidence.

ACPO Principle 3

Create and maintain a detailed audit trail of all investigation processes to establish the validity and integrity of the procedures followed.

ACPO Principle 4

The investigator leading the case holds the overall responsibility to ensure compliance with the law and ACPO principles, ensuring an ethical and legally sound investigation.

Chain of custody

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Client Name: ABC organization

Project Manager(s): Suvani Basnet

Related Evidence ID Numbers: C0001052965

Description of Evidence	
BOX 1	
C0001052965	
Location: ABC cooperation	
General Description: Malicious file transmission	
Item #	Description of Item (Binder, Notebook, etc.)
1	Memory Dump, server logs.
2	Email logs/documents with email log details, with no any faults.
3	PCs, model (Dell Inspiron Desktop 5000 Series) Laptop model (lenovo thinkpad)x1, carbon. all the devices were in good condition

Chain of Custody				
Item #	Date/Time	Released by (Name & Organization)	Received by (Name & Organization)	Comments/Location (office number, cabinet number)
1	15/08/2023	D.Smith (contract employee)	Suvani Basnet Forensic investigator	Incident involving zip 78 file from email server (main office of dr smith)
2	18/08/2023	Forensic Investigator Suvani Basnet	IT Department Supervisor	Secure Evidence Storage (Cabinet 2) Initial evidence collection
3	19/08/2023	It department supervisor	Forensic Investigator Suvani Basnet	Secure Evidence Storage (Cabinet 3) Additional evidence handover
4	22/08/2023	Sugam karki	Court Clerk (1123)	Evidence submitted to court
5	23/08/2023	Court clerk	Sugam Karki	Evidence returned back from court

Final Disposal Authority	
Authorization for Disposal	
Item(s) #: <u>2</u> on this document is(are) no longer needed as evidence and is/are authorized for disposal by:	
<input type="checkbox"/> Return to Owner	
Name of Authorizing Agent: <u>Suvani Basnet</u>	Signature: <u>Suvani Basnet</u> Date: <u>2023-08-29</u>
This Evidence Chain-of-Custody form is to be retained as a permanent record by ERS.	

Mobile Forensics



Unveiling the dark side: Mobile phone as tools for modern criminal activities

Mobile phone has been both boon and a curse to human society. In this age there might be handful percentile of people who are disconnected from these social media and mobile phones. In this era of social media influencers where online platforms have been an integral part of our lives, yet it is important for us to exclude this digital space from our life. This very assignment delves into the various ways in which mobile phones has been exploited for criminal usage.

Unmasking Common (Mobile) Cyber Crimes

- Phishing and Scams: Tricking users into clicking malicious links or downloading harmful software through social engineering.
- Theft of Identity: Illegally using someone's personal info (e.g., credit cards, photos) for fraud or illegal activities.
- Online Bullying: Sharing embarrassing content triggering shame and psychological issues, especially among teens.
- Online Harassment: Cyberstalking with persistent, unwelcome content to control and intimidate like unwanted calls.

Importance of Call Logs, History, and Network Data in Investigations

- To identify the mobile network provider associated with the phone number(s) used in the crime through victim information, witness accounts, or surveillance footage.
- For contacting the relevant mobile network operator to obtain Call Detail Records (CDRs) containing call details like date, time, duration, and phone numbers involved.
- Analysing the acquired CDRs to uncover valuable insights by comparing phone numbers and timestamps to identify connections.
- Cell tower information provided by mobile network providers to locate mobile devices and narrow down the investigation by examining tower IDs, coverage zones, and subscriber details.
- Forensic investigation tools like Oxygen Forensic Detective, Cellebrite, etc to analyse mobile devices, call logs, text messages, social media, etc.
- Recover relevant data using techniques such as timestamps and GPS coordinates.

Protecting digital assets: defending against online crimes.

- Keep your software updated and use trusted anti-virus software to shield your computer from cyber threats.
- Protect your accounts with robust passwords and avoid clicking on suspicious links in emails or unfamiliar websites.
- Only share sensitive data in secure environments and independently contact companies to verify requests for personal information.
- Be cautious of website URLs and enable security features for online transactions. Regularly monitor bank statements for any suspicious activity.
- Remain cautious with spam emails, never open attachments from unknown senders, and exercise caution with email communications. Check email headers to find out faulty mails.

Hypothetical Scenario: Theft of Sensitive Data from Mobile Devices

Let us consider a hypothetical scenario, considering Mrs Basnet got her sensitive data compromised. Now, this report would demonstrate how forensic compromised, using the report.

Source of evidence

- Call Logs
- Text Messages
- Contacts
- Emails
- Photos and Videos
- Internet Browsing History
- Social Media Activity
- GPS Location Data

Figure 13:sources of evidence

The guidelines to be followed while investigating

- To guarantee thorough investigations, digital forensic specialists should conduct hypothesis testing, data collecting, relationship identification, hidden data analysis, significance evaluation, event data reconstruction, and concluding results.
- Professionals should provide unbiased, in-depth reports that are organised chronologically, comprehensible to non-technical audiences, and contain facts that can be defended. Validation may involve working with trained forensic interviewers.

- It is imperative to adhere to regulatory standards and rules, such as ISO/IEC 27037:2012 and ISO/IEC DIS 27042, to ensure that digital evidence is identified, collected, preserved, analysed, and interpreted correctly.
- Experts in forensics must follow moral principles, ethics, act impartially, and take into account other possibilities for the existence of data, such as the existence of harmful software.

Crime Scene Investigation

Upon receiving the crime scene, we interviewed with Mrs Basnet by asking plethora of questions like

1. Can you provide us the exact time you noticed something suspicious on your accounts & what was it(was it a scam mail, transaction, messages) also what was the very account .
2. Can you reminisce if you have shared your digital information to any person.
3. Can you reminisce if you have surfed through vulnerable websites or logged to any suspicious website with your credentials. What is the method you choose to save your credentials, is it paper books, or digital notebook?
4. Have you ever within few days or months have connected to public, free WIFI's or using the vpn?

ACPO principle 3

Principle 3 of the ACPO Guidelines stresses the importance of retaining specific papers during the seizure of mobile devices to ensure the highest level of evidence integrity. These papers document important details such as the date, time, location, and condition of the device, supporting the credibility of the investigation and maintaining a reliable chain of custody.

Records to maintain

- The Seizure Log, which serves as the investigation's primary record of the date, time, place, and circumstances of the mobile device seizure, is an essential document. (The Seizure Log)
- Documentation of the mobile device's chain of custody is essential for the integrity of the evidence and its admissibility in court. (Chain of custody log)
- For conclusively identifying the mobile device in issue, accurate documentation of device characteristics, including model number, serial number, IMEI, and unique identifiers, is essential. (Device Characteristics Documentation)
- Documenting actions taken to preserve the integrity of the seized mobile device, such as switching it off, using a Faraday bag, and disconnecting from the network, are crucial. (Preservation action documentation)
- To avoid unauthorised access and manipulation, it's crucial to keep meticulous records of mobile device storage or any seals, and site security. (storage & site security records)



Device Identification and seizure

Using the information collected we proceed to now view the victims' phones for further investigation. It's considered a better practise to use hand gloves and faradays bag so that the device remains disconnected from any wifis and Bluetooth connections. Then we calmly proceeded to take the evidences(devices) i.e the phone on our forensic lab.



Figure 14:faraday's bag

Forensic Imaging

In the forensic lab, then we began forensic imaging using the tools like ftk imager and Encase tool to make the bit-by-bit image in order to protect the actual evidence from any damages.

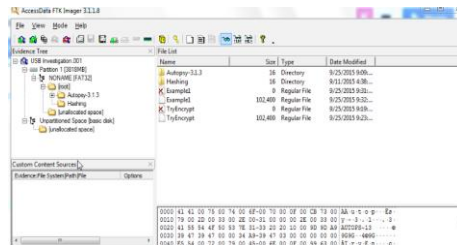


Figure 15: ftk imager for data extraction

Data extraction/analysis

During the extraction process uncovering evidences like call logs, text messages, social media logs take place. It would be beneficial to uncover communication patterns of all suspicious acts to trace it into the possible results.

Tools:



Figure 16:celebrite UFED tool for extraction and analysis of mobile data

Data Recovery

After the recovery of deleted data's/ evidences we can trace the clues into certain evidences where the data was compromised. Deleted files, hidden content can be seen using various tools after this we can create a timeline of event that has happened using the notes, we gather

. Documents like chain of custody can be prepared which aids on providing credibility and reliability of the crime..

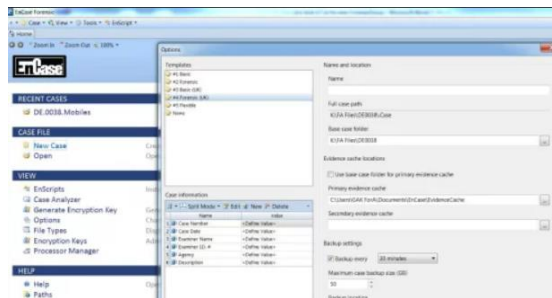


Figure 17:encase tool for data recovery

Damaged Phone



Figure 18:condition of damaged phone

State

- Except for the motherboard, every component of the gadget was broken.
- It has damaged screen, back panel, and many screen components.

Difficulties

- Several components of the gadget have extensive damage that has to be repaired or replaced.
- Potential short-circuiting of the PCB, which might impair operation and data extraction.

Investigation process

- Device repair involved opening the silicon sandwich structure, covering touching parts with insulating material, and transplanting the motherboard and other parts into a new screen combo
- The Universal Forensic Extraction Device Touch-2 (UFED-2, Version-7.42) from Cellebrite was used for data extraction.
- The extracted data included contacts, call logs, messages, multimedia artifacts (images, videos, documents), internet browsing history, and application data from social media accounts (WhatsApp, Facebook, Telegram, etc.)
- Data analysis was conducted using the software Physical Analyzer, Version-7.42.



Burnt down phone



Figure 19:condition of a burnt phone

Difficulties

- Burned-down phones frequently sustain physical damage, which can make it challenging to reach the phone's internal parts.
- Data Corruption: Because of the heat and flames from the fire, some types of data may be difficult or impossible to retrieve.
- Specialised Tools: Extraction of data from a burnt down phone may require specialised tools and methods that are not easily accessible to the common user 1.
- Limited Access: In certain circumstances, the phone may be so severely damaged that it is impossible to access the internal storage at all .

Investigation-methods

- Mobile device forensic tools (MDFTs) allow investigators to retrieve complete phone data, surpassing security measures.
- Hardware and software tools aid forensic professionals in accessing a phone's memory chips when the device is non-functional or data ports are faulty.
- The JTAG (Joint Test Action Group) approach is utilized by digital forensic experts to retrieve data from broken phones using circuit board taps.
- Forensic evidence repair specialists thoroughly examine internal parts and connectors to recover any lost data when the device has extensive damage.
- Digital forensics is employed to restore lost data from mobile phones, with specialists using tools like Cellebrite to extract content from the pho



Water Damaged Phone



Figure 20: condition of a water damaged phone

Difficulties

- Water damage to phones can affect functionality, integrity, and data stored on the device.
- Preserving evidence and preventing further water exposure is crucial when recovering a drowned phone.
- Care must be taken to avoid unintended power-on events that could alter the data.
- Placing the device in a Faraday bag can isolate it from external signals and prevent automatic power-on.
- Extracting data from a drowned phone requires appropriate techniques and tools to minimize further damage.

Investigation-methods

- The detective examines the phone for water damage, records its condition, and carefully dries it to remove moisture.
- They visually inspect the phone for indications of water damage, focusing on the logic board and memory chips, and record their observations.
- Using forensic software like Cellebrite UFED, Oxygen Forensic Detective, EnCase Forensic, or XRY, they attempt to extract data from the memory chips.
- If necessary, they remove the memory chip to access the data with specialized tools.

References

- (n.d.). Retrieved from https://answers.microsoft.com/en-us/outlook_com/forum/all/email-shutdown-in-progress/4c56b673-df04-4e1e-968e-06eabc5b35dc
- (n.d.). Retrieved from <https://www.flashbackdata.com/forensic-options-locked-broken-mobile-devices/>
- (n.d.). Retrieved from <https://www.atmail.com/blog/email-services-shut-down/>
- (n.d.). Retrieved from <https://info-savvy.com/list-of-mobile-forensic-tools/>
- *ACPO Guidelines & Principles Explained*. (202, 11 6). Retrieved from ForensicControl: <https://forensiccontrol.com/guides/acpo-guidelines-and-principles-explained/>
- Akhlesh Kumar, B. D. (n.d.). *Forensic Analysis of Broken and Damaged Mobile Phone - A Crime Case Study*. Retrieved from https://www.researchgate.net/publication/353109381_Forensic_Analysis_of_Broken_and_Damaged_Mobile_Phone_-_A_Crime_Case_Study
- Bryce.s. (n.d.). *Digital Forensic Imaging: Types & Examples*. Retrieved from study.com: <https://study.com/academy/lesson/digital-forensic-imaging-types-examples.html>
- Cooley, W. (2022, December 21). *How to Preserve Digital Evidence: The Importance of Data Collection*. Retrieved from ADFnews: <https://www.adfsolutions.com/news/how-to-preserve-digital-evidence-the-importance-of-data-collection>
- *Extracting Evidence From Damaged Devices*. (2021, August 20). Retrieved from ForensicFocus: <https://www.forensicfocus.com/webinars/extracting-evidence-from-damaged-devices/>
- Filipkowski, B. (2023, April 20). *FieldEffect*. Retrieved from What is digital forensics and incident response (DFIR)?: <https://fieldeffect.com/blog/digital-forensics-incident-response>
- Mcsweeny, k. (2020, January 31). *ZDNET*. Retrieved from Burn, drown, or smash your phone: Forensics can extract data anyway: <https://www.zdnet.com/article/burn-drown-or-smash-your-phone-forensics-can-extract-data-anyway/>

- silvas, J. (2016, september 27). *WHAT ARE THE STEPS TO PRESERVING DIGITAL DATA AND EVIDENCE?* Retrieved from cornerstone discovery: <https://cornerstonediscovery.com/what-are-the-steps-to-preserving-digital-data-and-evidence/>