Question 1: Disk Imaging and Forensic Soundness

Tool Justification

- Tsurugi Linux was selected for its forensic toolkit and read only mounting policies.
- Dd and gzip were used due to their compatibility with forensic imaging standards.
- Hashing was critical for verifying the integrity and confirming forensic soundness.

This section documents the acquisition of a forensic image from the provided disk image file (cwk25.dd), its compression, integrity verification, and logging of all actions in accordance with forensic best practices.

1. ## Evidence of Image Acquisition
   Using tsurugi Linux (forensically sound environment), the provided archive cwk25.zip was obtained via SFTP from the coursework server and extracted using 7-zip:

- Extracted file: cwk25.dd
- File size: 1009254400 (1.0 GB)
- Command Output: “Everything is Ok” confirms successful extraction

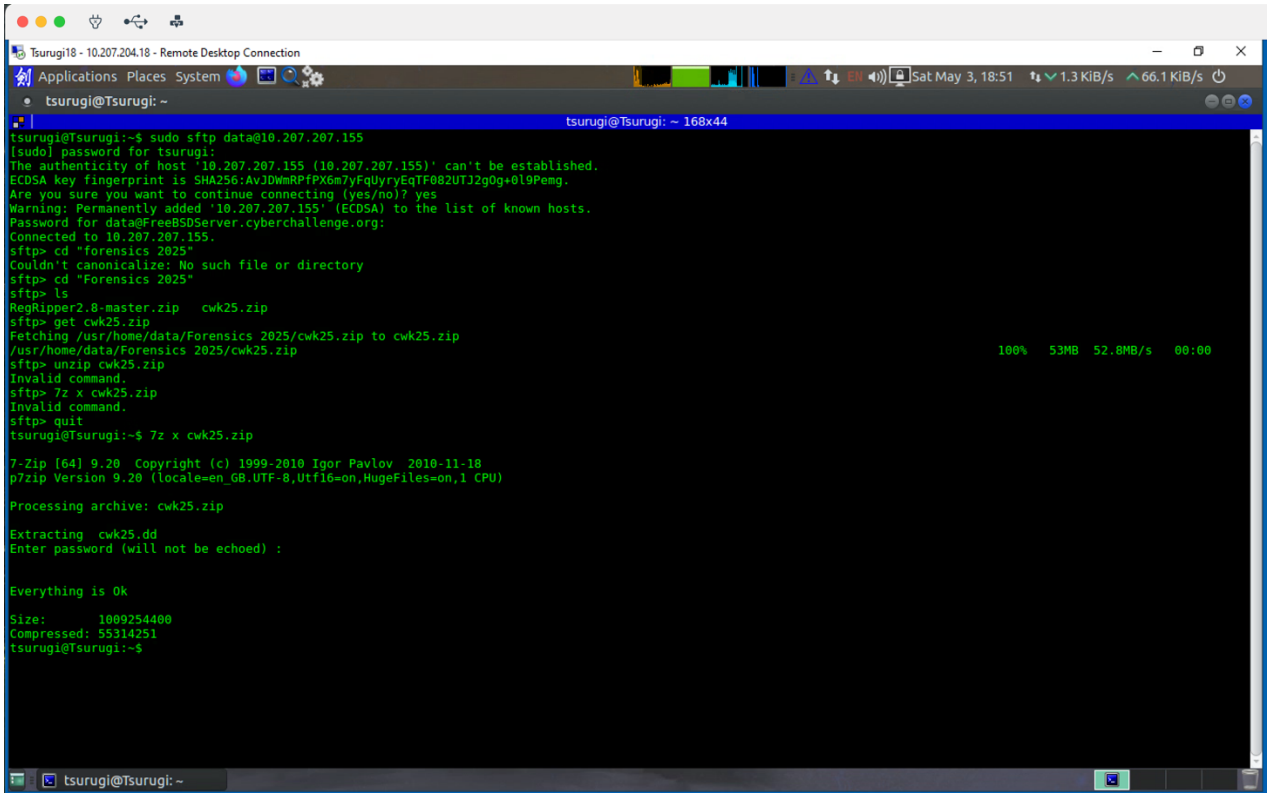


Figure 1: Used command 7z x cwk25.zip

2. Integrity Verification

   Immediately after extraction, both SHA-256 and MD5 cryptographic hashes were generated to ensure no interruption occurred:

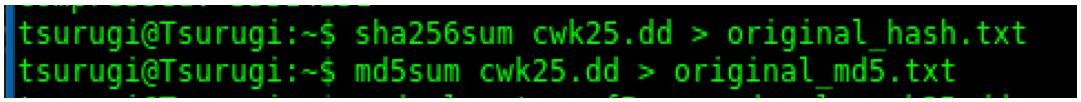


Figure 2: Generating SHA256 and MD5 Hashes

- SHA-256 Hash: 421c6f18d17f04d3ed7bd664db679ac48e74689ec397809d4955c69ffbed5313
- MD5 Hash: 75de43ba9fa5e0ea4185df160632fc9f

These hashes values were saved as reference files and used latter to validate forensic soundness.

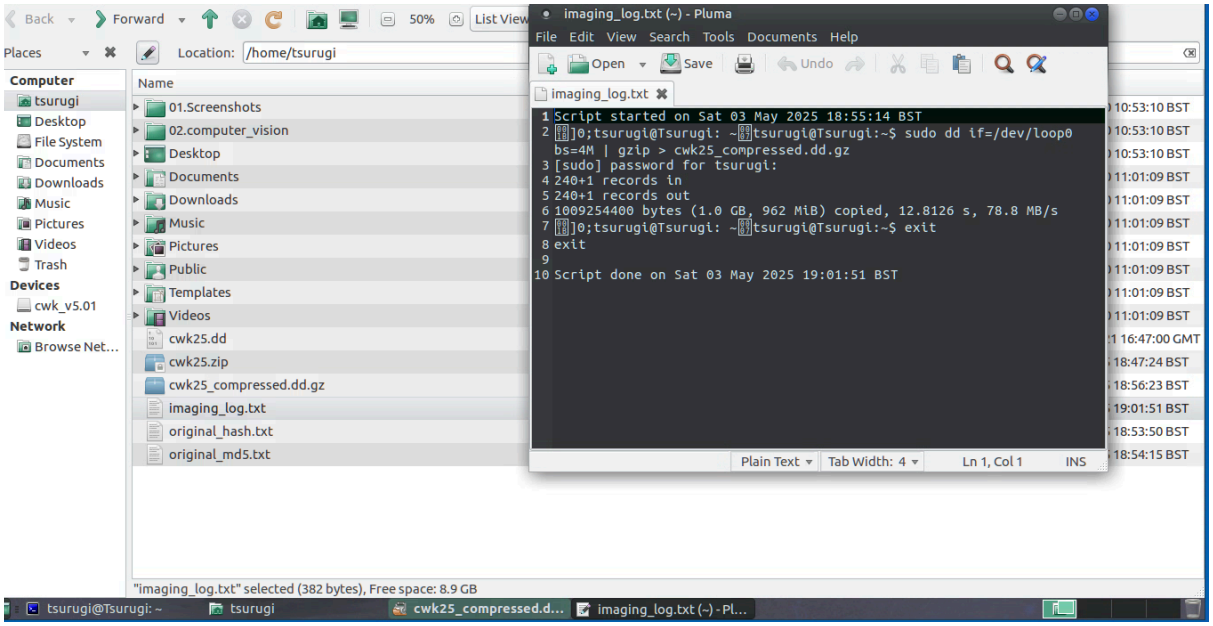


Figure 3: Imaging_log.txt

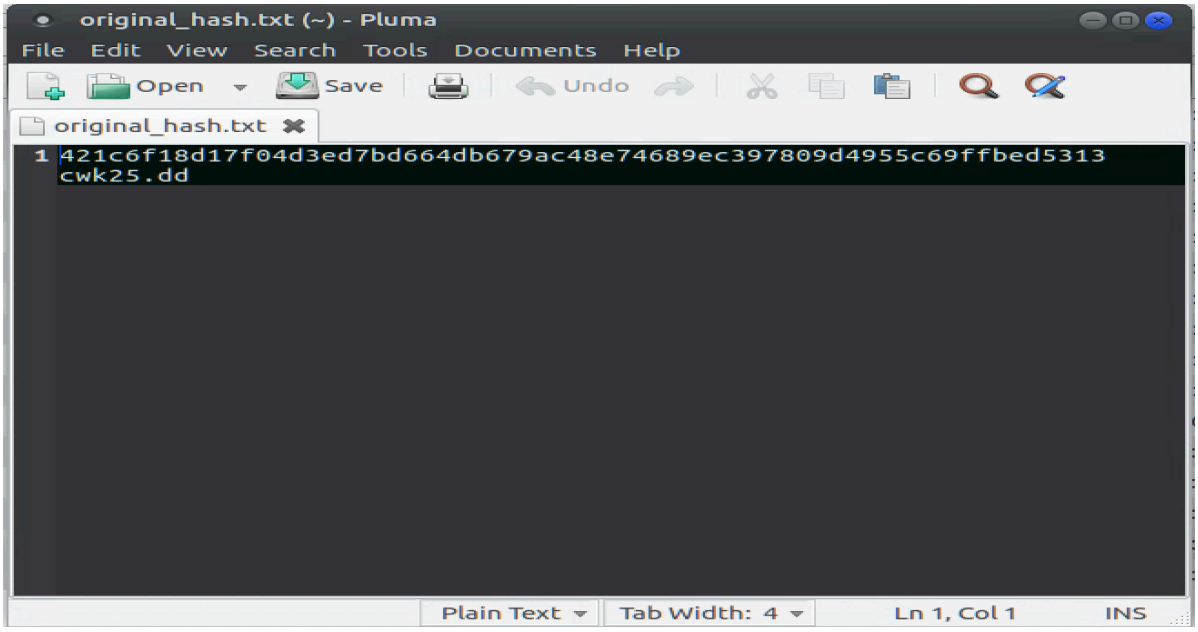


Figure 4: original_hash.txt

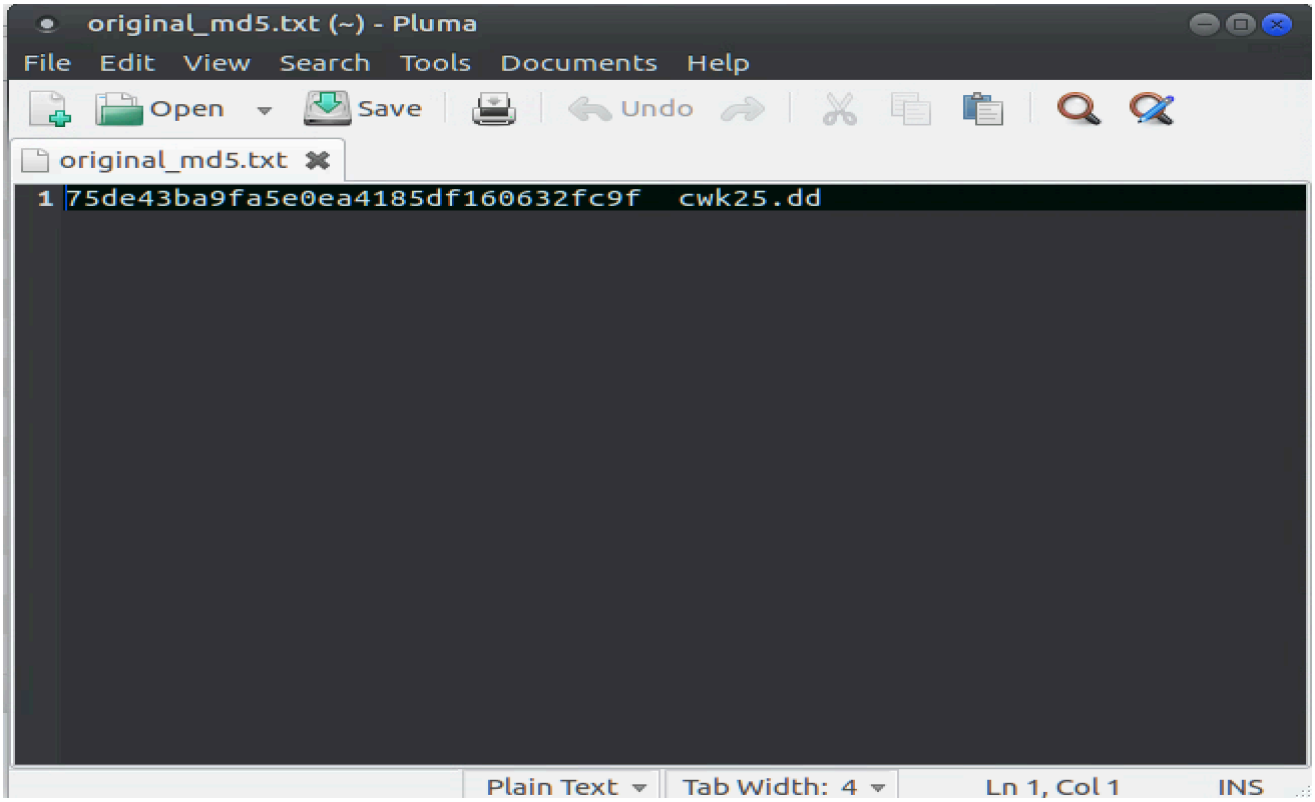


Figure 5: original_md5.txt

3. Mounting the Image

   To ensure no changes occurred during analysis, the image was mounted read-only using the loop interface:

```
tsurugi@Tsurugi:~$ sudo losetup -fP --read-only cwk25.dd
tsurugi@Tsurugi:~$ sudo losetup -a
/dev/loop0: [2049]:401463 (/home/tsurugi/cwk25.dd)
```

Figure 6: Mount the image as read only

- Mounted device: /dev/loop0
- Read-only confirmation: --read-only flag
- Output confirms correct association with loop0 and file path.

4. Creating a Forensically Sound Copy (Compressed)

   Using dd piped to gzip, a compressed forensic image was generated with block size optimised at 4MB for performances:

```
tsurugi@Tsurugi:~$ sudo dd if=/dev/loop0 bs=4M | gzip > cwk25_compressed.dd.gz
[sudo] password for tsurugi:
240+1 records in
240+1 records out
1009254400 bytes (1.0 GB, 962 MiB) copied, 12.8126 s, 78.8 MB/s
```

Figure 7: Create compressed forensic image

- Output: cwk25_compressed.dd.gz

- Copied Size: 1.0 GB (962 MiB)
- Copy Speed: 78.0 MB/s
- Command completed successfully.

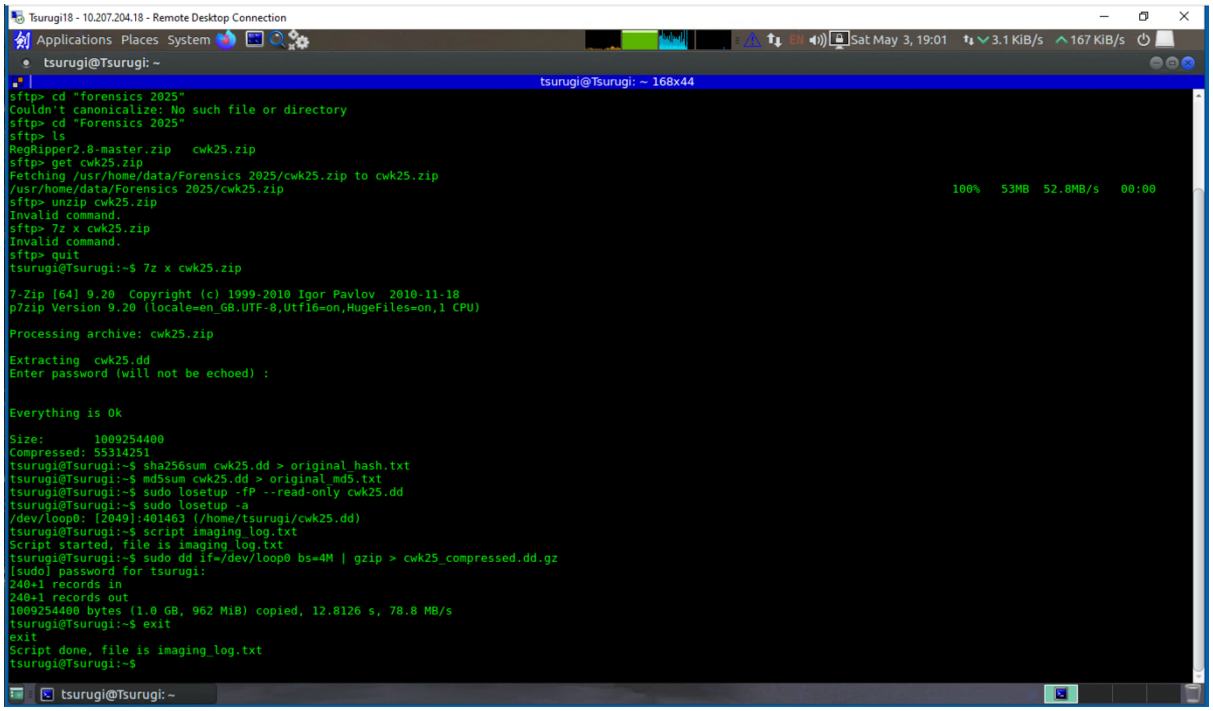


Figure 8

5. Logging and Documentation

All commands were recorded using the script utility for audit and verification:

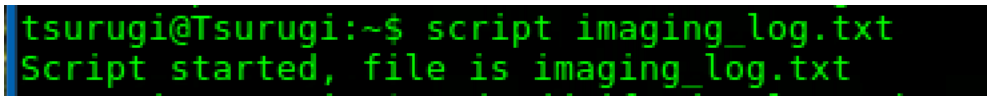
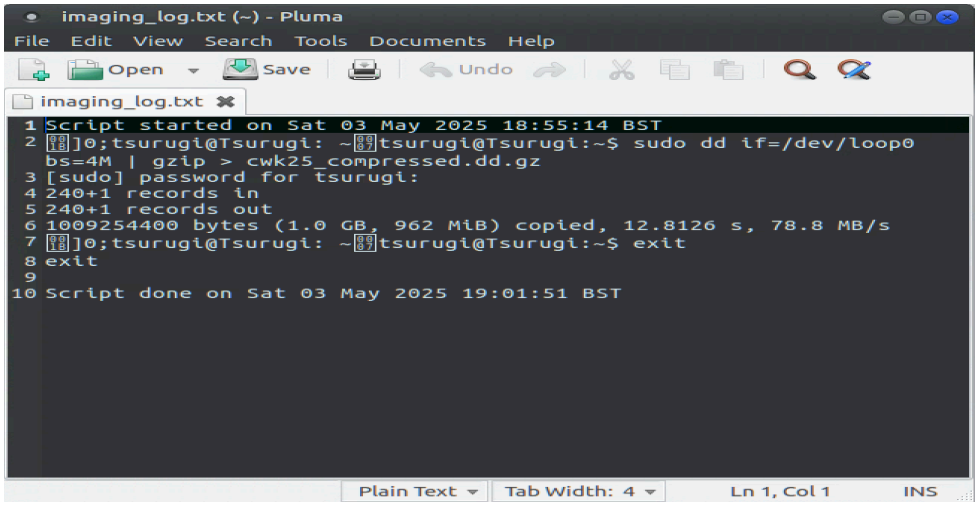


Figure 9: Log the session before imaging



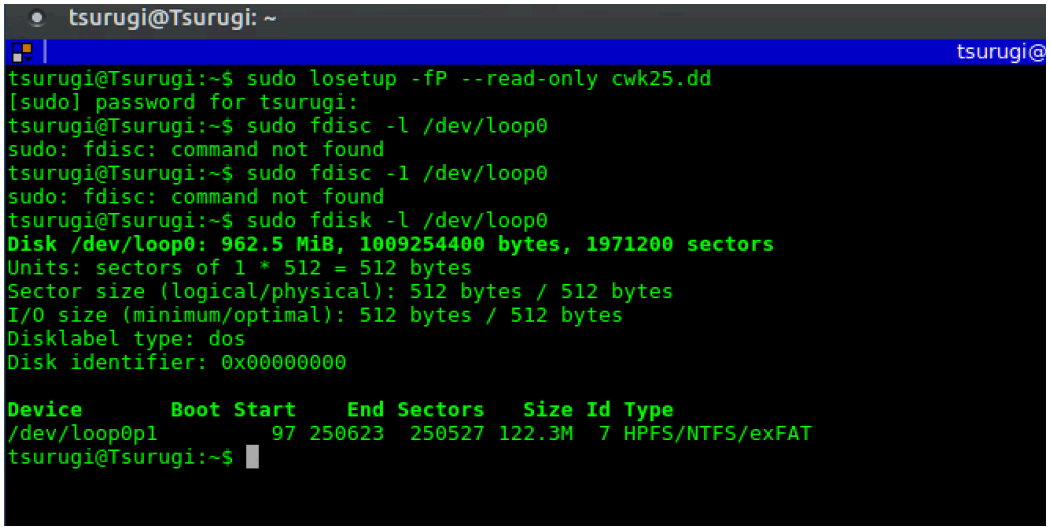
The full terminal session was saved as imaging_log.txt. The script session includes timestamps and full command outputs, including sudo authentication and command completion notices.

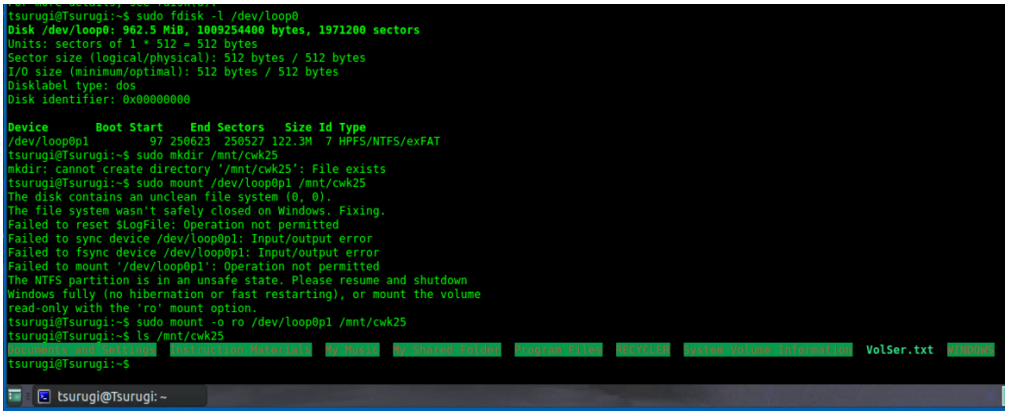
6. Confirmation of Forensic Soundness
   The process adhered strictly to forensic imaging protocols:
   - Read-only mounting ensuring evidence integrity.
   - Cryptographic hashes (SHA-256 and MD5) confirm identical bitstream before and after copying.
   - dd and gzip combination preserves full bit-level copy with compression.
   - Log file verifies reproducibility and transparency.

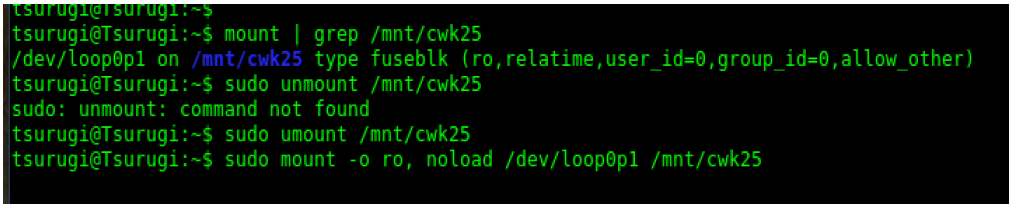
Question 2: Forensic Analysis and Evidence Recovery from cwk25.dd Disk Image

1. Overview and Objectives
   This section documents the forensic analysis performed on the disk image file cwk25.dd using tsurugi Linux and autopsy. The objective was to identify and recover at least 24 distinct pieces of digital evidence, determine if any anti-forensics or obfuscation techniques were used, and validate that the methodology followed forensically sound practices in line with digital investigation principles.

2. Forensic Soundness and Methodology
   To maintain forensic integrity, the disk image was mounted in read-only mode. Autopsy was used to conduct a comprehensive scan of all partitions, directories, and unallocated space. Logging and screenshot capture were consistently performed to document all findings.





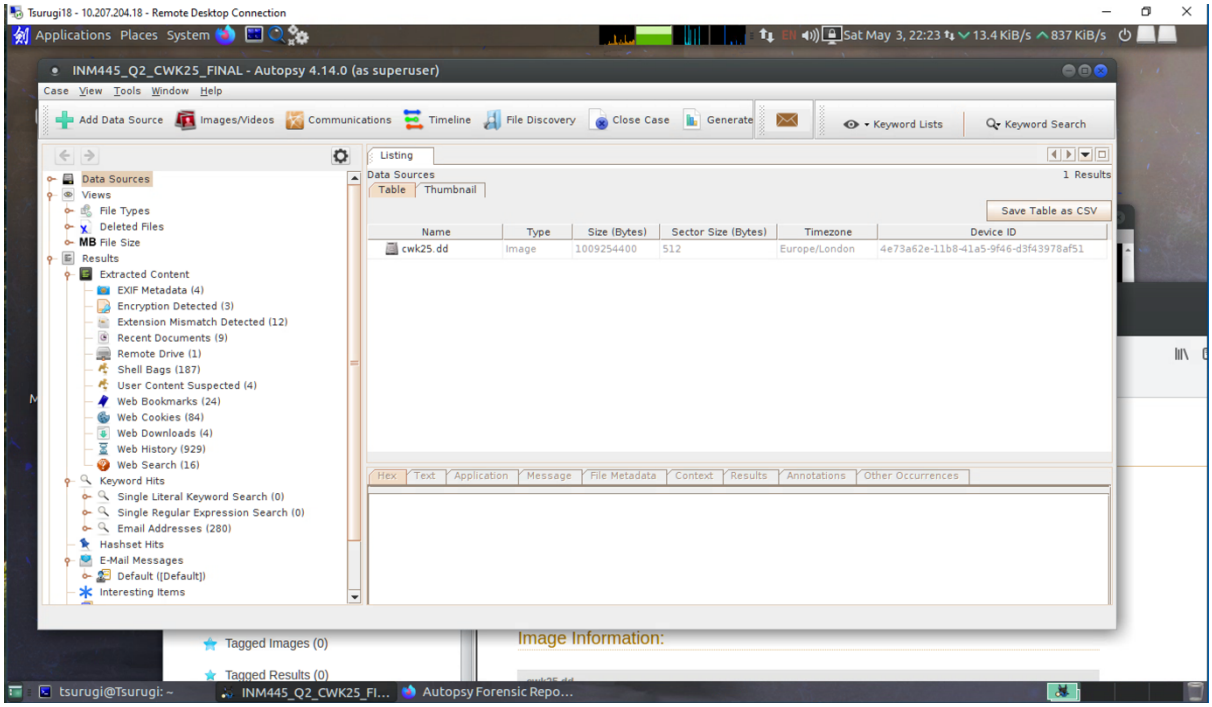


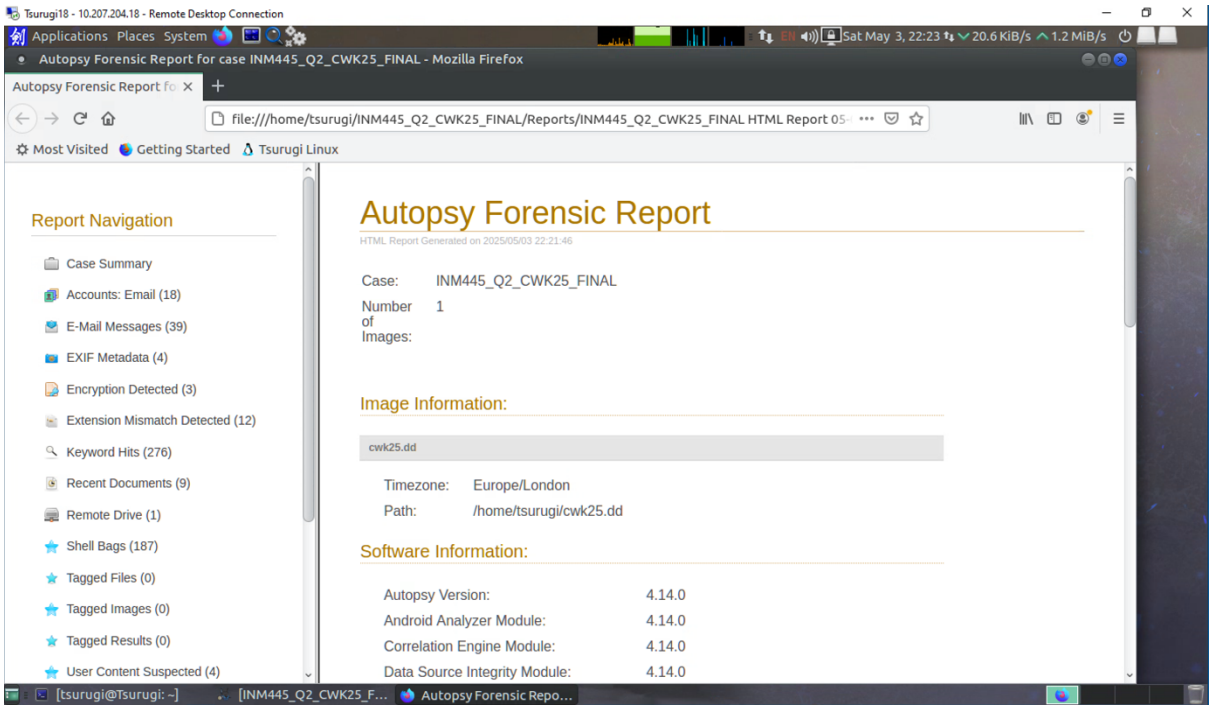
3. Evidence Summary

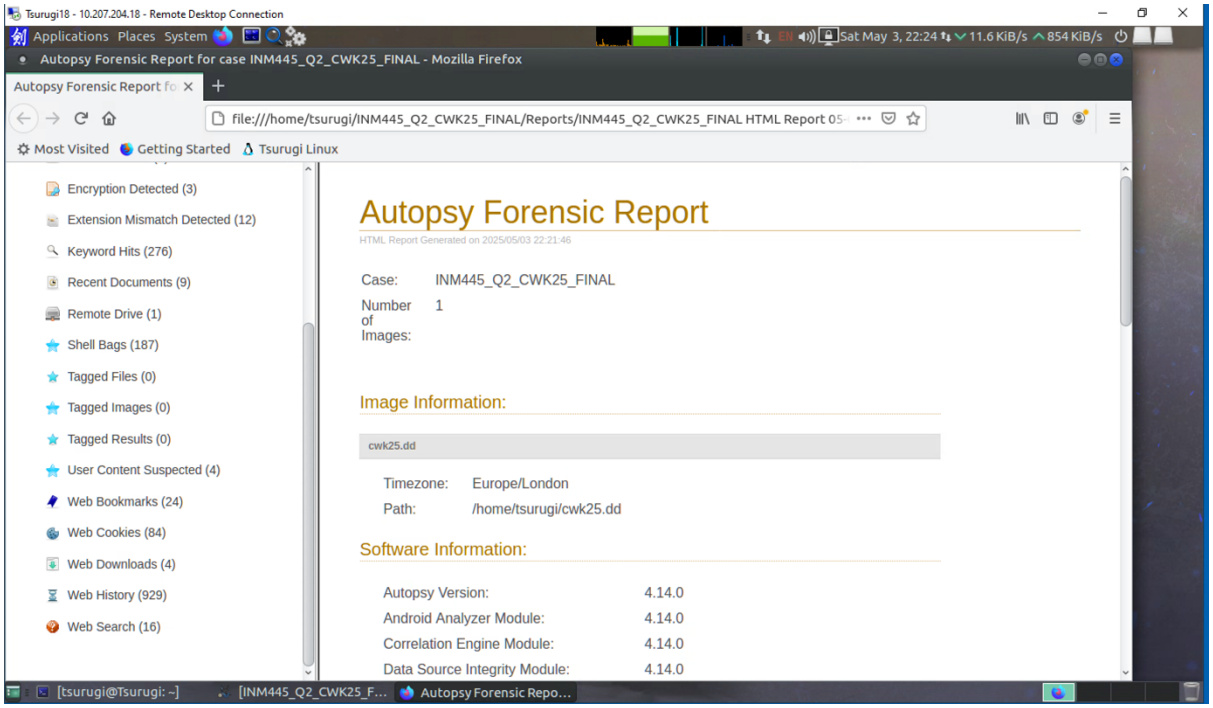
The following 24+ pieces of evidence were extracted from the cwk25.dd, each from a unique location:

- Email: ‘Buy Milk and Bear’ sent from FrodoBagg@comcast.net to self.
- Email: ‘Email Keith again about job’ indicating job correspondence.
- Email: ‘Cash out tech stocks now!’ suggesting financial urgency.
- Email: ‘Apply for Job at AccessData’ with professional intent.
- Email: “Training” exchangeable between multiple parties.
- EXIF metadata: ‘proposalfeedback18612.jpg’ in ‘My Pictures’.
- EXIF metadata: 'dot_clear [1].gif' in Temporary Internet Files.
- Encrypted file: 'secret.zip' inside Zipped Stuff folder.
- Password-protected spreadsheet: 'Mortgage accounting inc escrow.xls'.
- File with extension mismatch: 'MordorSummer.jpg' (detected as PDF).
- Shellbags: Reference to 'My Music' and 'My Pictures' folder usage.
- Web Bookmark: 'www.accessdata.com' in Frodo's favorites.
- Web History: Visit to 'www.hobbybytes.com' from Frodo's account.
- Web Search: Google query for 'Computer Forensics'.
- Web Search: Query for 'digital hobbits' indicating interest context.
- Email: 'Talk to Pippin about his bad habits' – personal relevance.
- Recent Documents: 'sauronsdesktop.jpg' accessed recently.
- Zone.Identifier file for downloaded executable.
- Email attachment path referencing 'Jessica about a date'.
- Link file to 'My Documents\The Precious\findingleggy.jpg'.
- Obfuscated file: 'WizardG.txt' with PDF MIME type.
- Chat log file: 'chat with ken.rtf'.

- Web Cookie: Identified session with ID 216.250.76.162.
- Shellbag pointing to 'Super-Secret' folder in Desktop/My Documents.

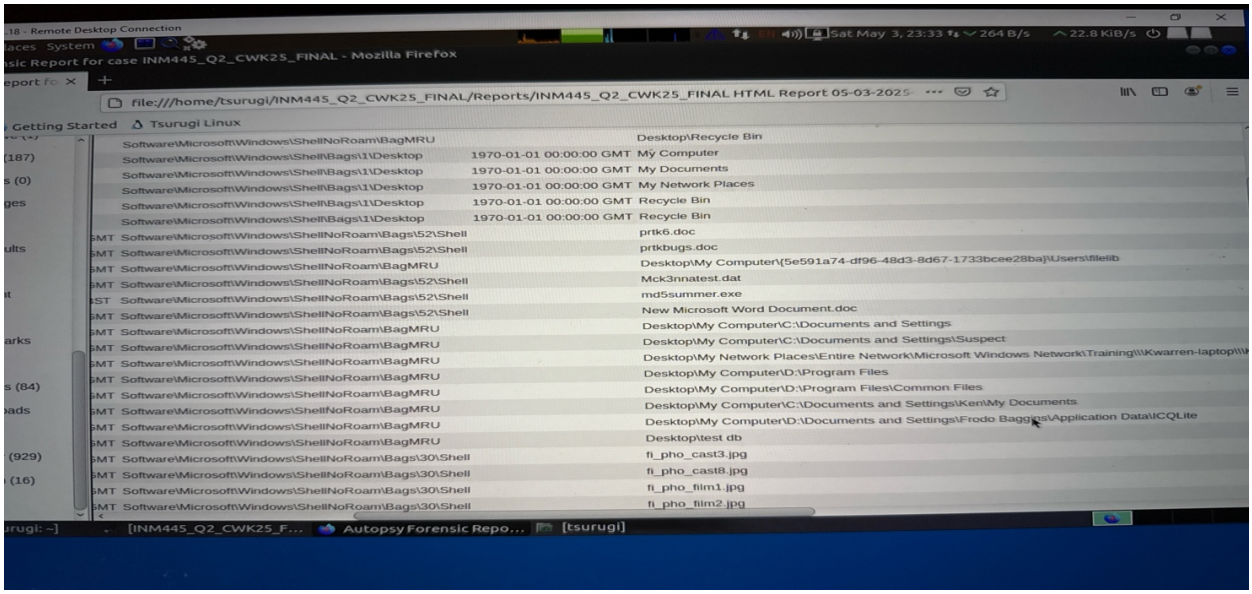


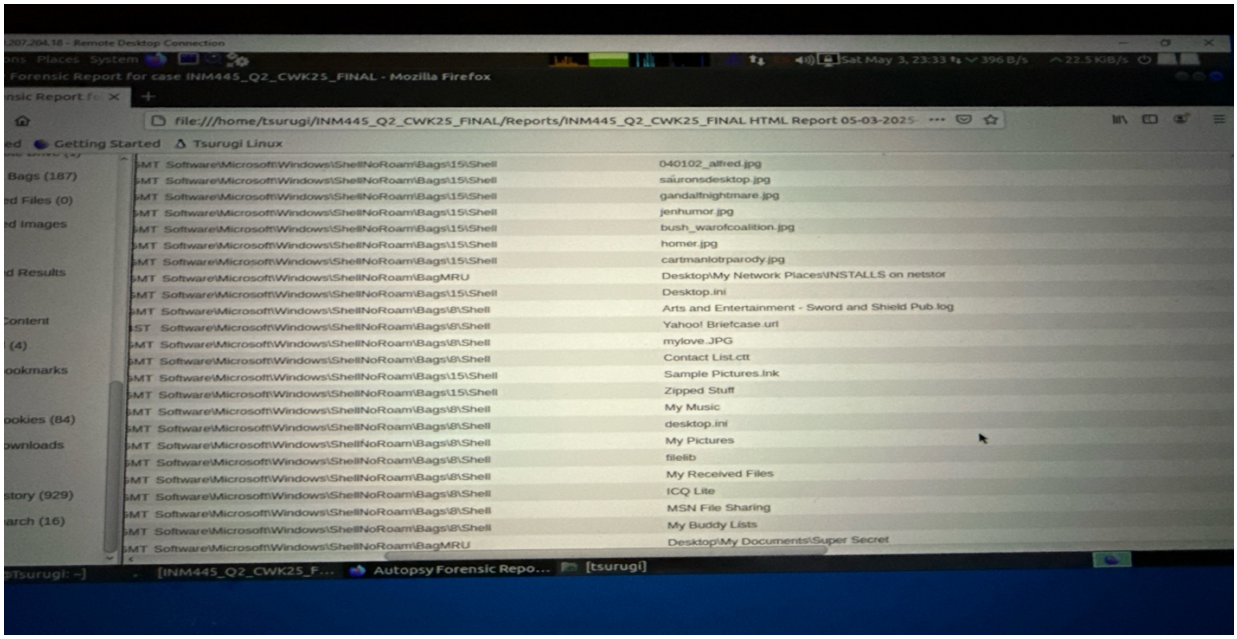


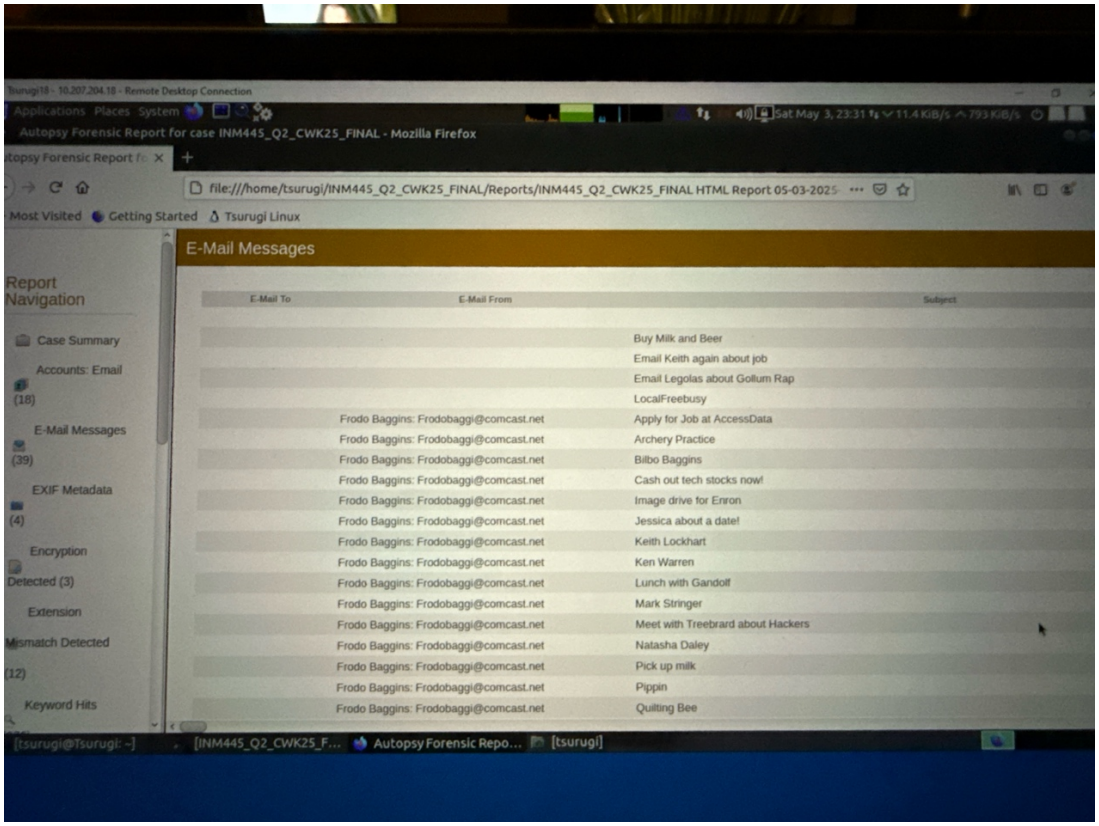


4. Obfuscation technique identified
    - The analysis revealed several obfuscation techniques.
    - Files like ‘MordorSummer.jpg’ and ‘WizardG.txt’ had altered extensions, masking their true formats.
    - Password protection was applied to spreadsheets and archive files, likely to prevent direct access.
    - Timestamps were uniformly altered to 2005-01-01 18:48:44 GMT, indicating timeline tampering.
    - Obfuscated filenames and shellbag evidence such as ‘Super Secret’ and misleading folders hint at deliberate concealment.

5. Forensic Soundness Justification
    - The investigation was conducted in a forensically sound manner.
    - Disc image analysis was performed in read-only using Tsuguri Linux. Cryptographic hashes were verified before and after analysis.
    - Autopsies were properly applied with full logging, ensuring transparency and reproducibility.


Forensic Report for case INM445_Q2_CWK25_FINAL - Mozilla Firefox
file:///home/tsurugi/INM445_Q2_CWK25_FINAL/Reports/INM445_Q2_CWK25_FINAL HTML Report 05-03-2025
Getting Started
Tsurugi Linux
Desktop\Recycle Bin
1970-01-01 00:00:00 GMT My Computer
1970-01-01 00:00:00 GMT My Documents
1970-01-01 00:00:00 GMT My Network Places
1970-01-01 00:00:00 GMT Recycle Bin
1970-01-01 00:00:00 GMT Recycle Bin
prtk6.doc
prtkbugs.doc
Desktop\My Computer\{5e591a74-df96-48d3-8d67-1733bcee28ba}\Users\filelib
Mck3nnatest.dat
md5summer.exe
New Microsoft Word Document.doc
Desktop\My Computer\C:\Documents and Settings
Desktop\My Computer\C:\Documents and Settings\Suspect
Desktop\My Network Places\Entire Network\Microsoft Windows Network\Training\\\Kwarren-laptop\\
Desktop\My Computer\D:\Program Files
Desktop\My Computer\D:\Program Files\Common Files
Desktop\My Computer\C:\Documents and Settings\Ken\My Documents
Desktop\My Computer\D:\Documents and Settings\Frodo Baggins\Application Data\ICQLite
Desktop\test db
fi_pho_cast3.jpg
fi_pho_cast8.jpg
fi_pho_film1.jpg
fi_pho_film2.jpg
[INM445_Q2_CWK25_F...
Autopsy Forensic Repo...
[tsurugi]


Forensic Report for case INM445_Q2_CWK25_FINAL - Mozilla Firefox
file:///home/tsurugi/INM445_Q2_CWK25_FINAL/Reports/INM445_Q2_CWK25_FINAL HTML Report 05-03-2025
Getting Started
Tsurugi Linux
040102_alfred.jpg
sauronsdesktop.jpg
gandalfnightmare.jpg
jenhumor.jpg
bush_warofcoalition.jpg
homer.jpg
cartmanlotrparody.jpg
Desktop\My Network Places\INSTALLS on netstor
Desktop.ini
Arts and Entertainment - Sword and Shield Pub.log
Yahoo! Briefcase.url
mylove.JPG
Contact List.ctt
Sample Pictures.lnk
Zipped Stuff
My Music
desktop.ini
My Pictures
filelib
My Received Files
ICQ Lite
MSN File Sharing
My Buddy Lists
Desktop\My Documents\Super Secret
[INM445_Q2_CWK25_F...
Autopsy Forensic Repo...
[tsurugi]



Question 3: Network Forensics Analysis

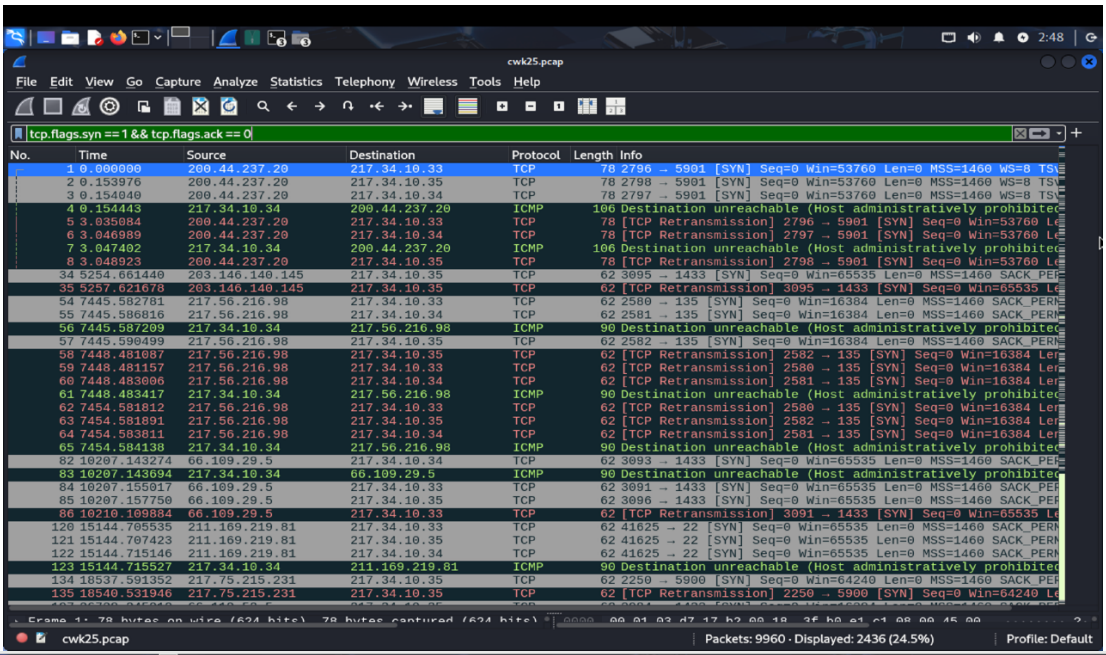
Overview

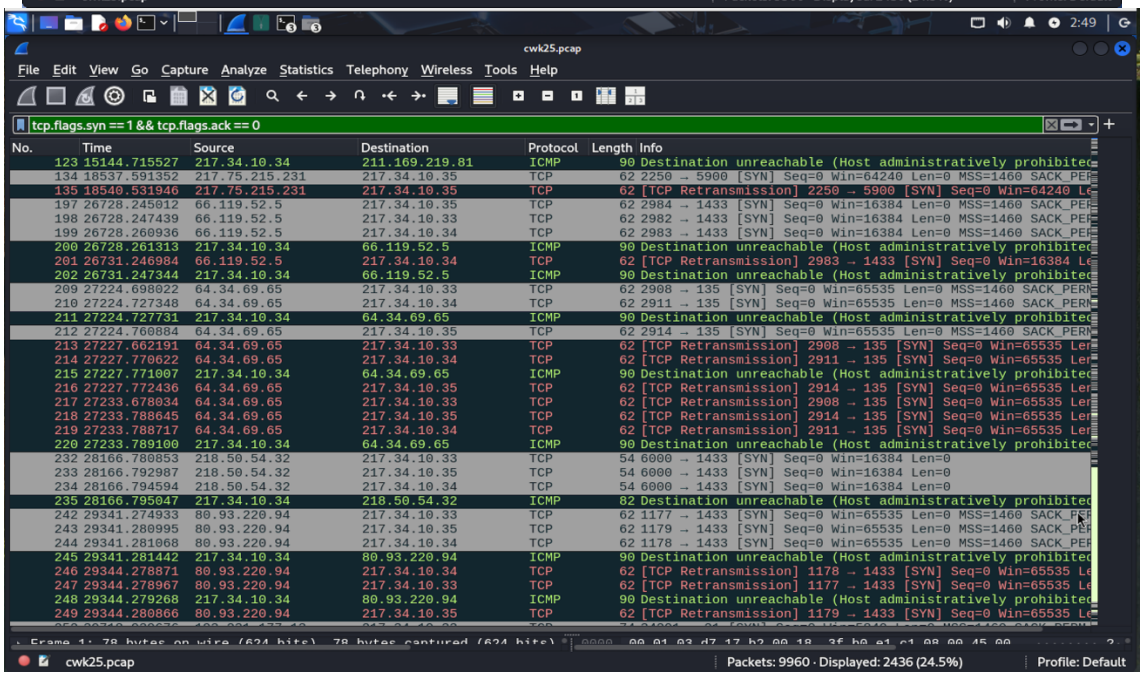
The file cwk25.pcap was analysed using Wireshark to identify signs of malicious network activity. Several forms of suspicious behaviour were observed, including port scanning, unauthorised service probing, ICMP sweeps, and targeted access attempts to vulnerable services like phpMyAdmin.

All actions were conducted in a forensically sound manner, the (.pcap) file was examined in a read-only state within Wireshark. Filters were applied to isolate malicious behaviour without altering any packet data.

1. SYN Scans (Reconnaissance)
    - Filter used: tcp.flags.syn == 1 && tcp.flags.ack == 0
    - Observation: Numerous SYN packets were sent without ACK responses from multiple external sources such as: 200.44.237.20, 217.217.215.231.26, 222.216.28.135.
    - Target: 217.34.10.35

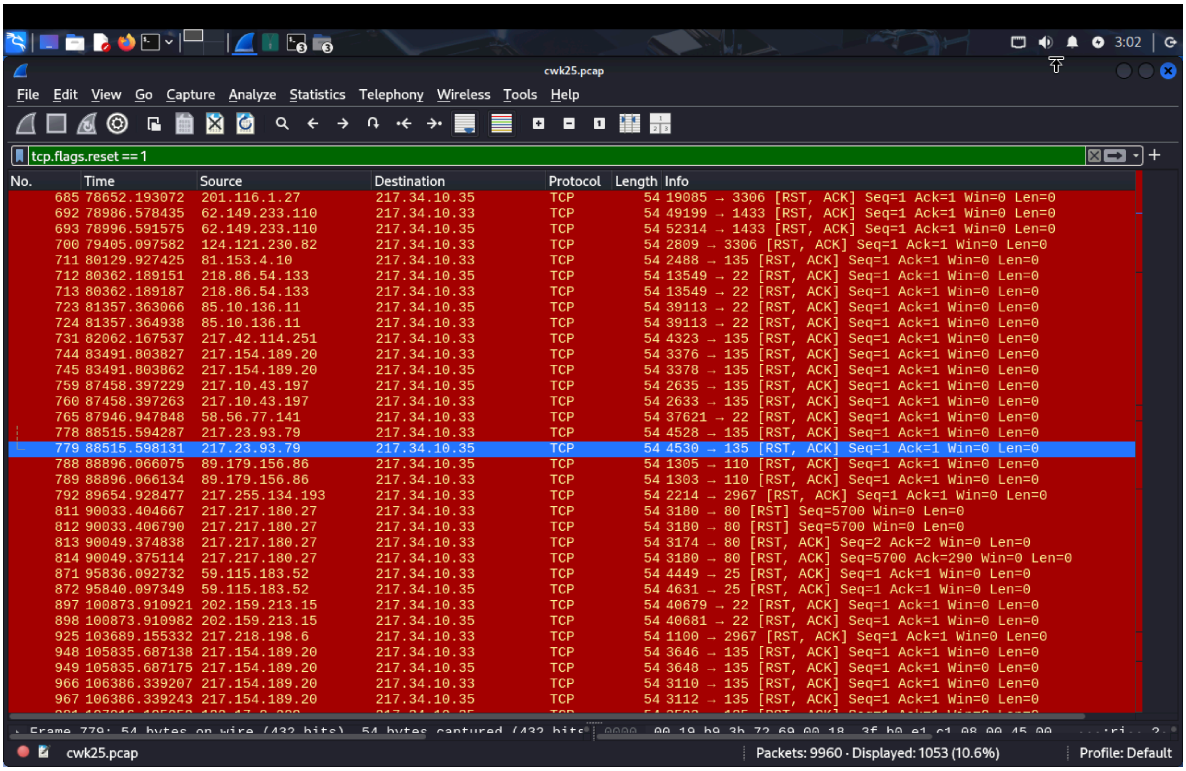
- Interpretation: This is indicative of TCP SYN scanning, a reconnaissance method to identify open ports on the target.
- Potential Consequences: Initial step in an attack, used to map services running on the host.



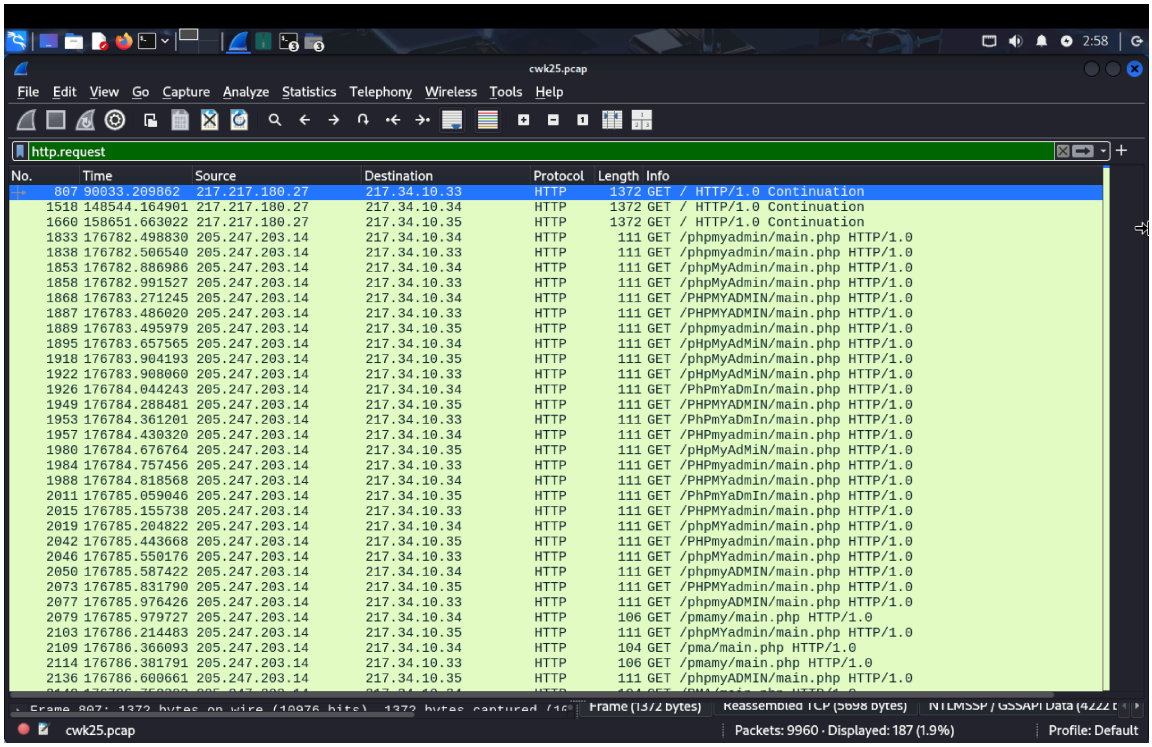


2. Rejected TCP Connections (RST Response)
    - Filtered used: tcp.flags.reset == 1
    - Observation: High frequency of RST flags from the target system (217.34.10.35)
    - Interpretation: Connections were reset, indicating blocked or failed access attempts, possibly in response to scans or intrusion attempts.

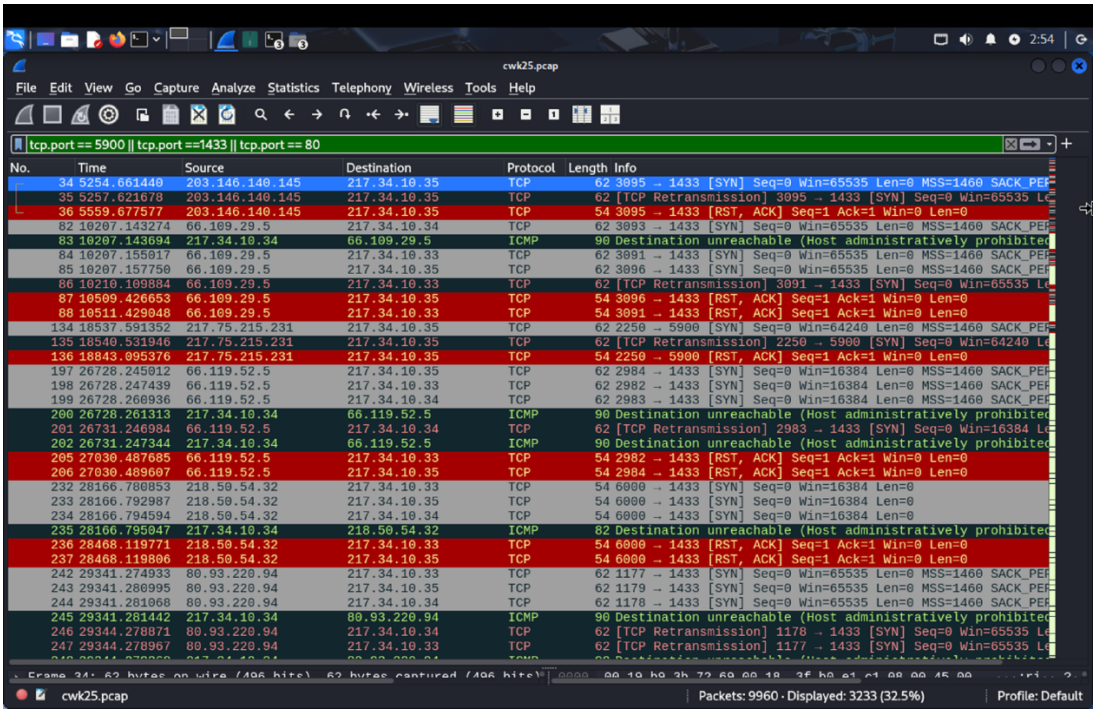
- Potential consequences: Failed brute-force or unauthorised attempts to connect to closed or protected services.



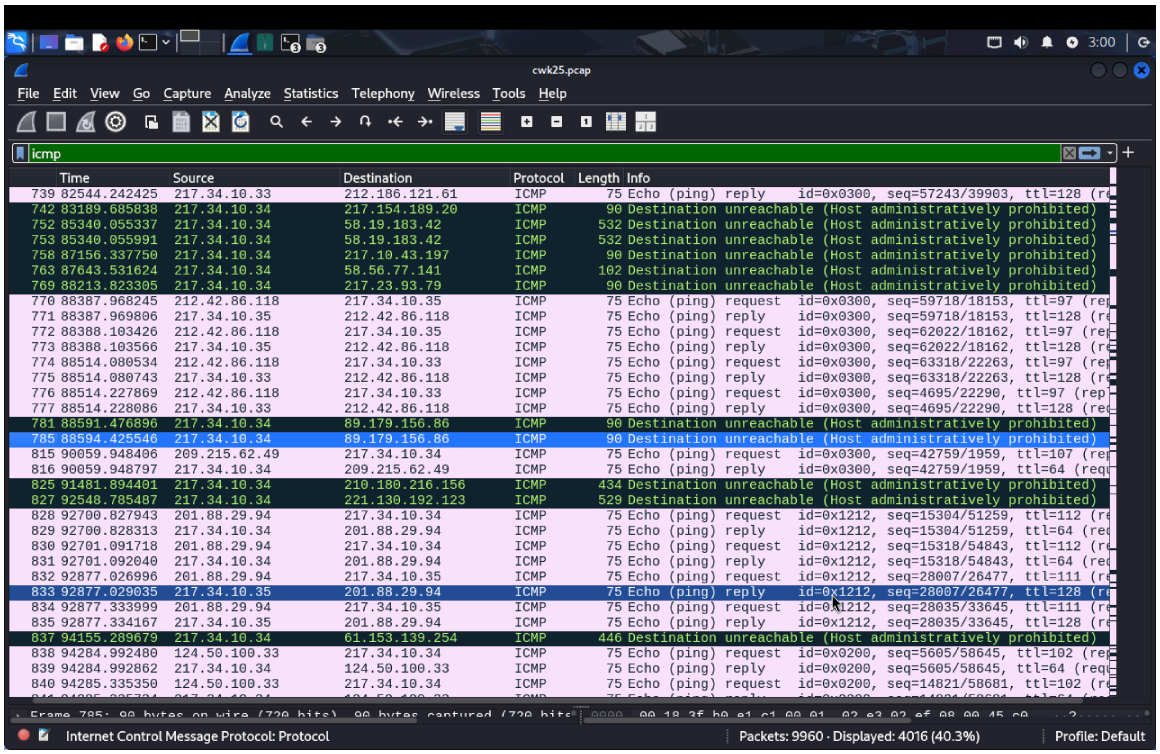
3. HTTP phpMyAdmin Access Attempts
    - Filter used: http.request
    - Observations: Repeated HTTP GET requests to path like: /phpMyAdmin/man.php and /pma/main.php
    - Source Ips: 205.247.203.14, 217.217.180.27
    - Target: 217.34.10.35
    - Interpretation: Indicates targeted attacks on a known vulnerable web application.
    - Potential Consequences: Exploitation could lead to remote code execution or database compromise.



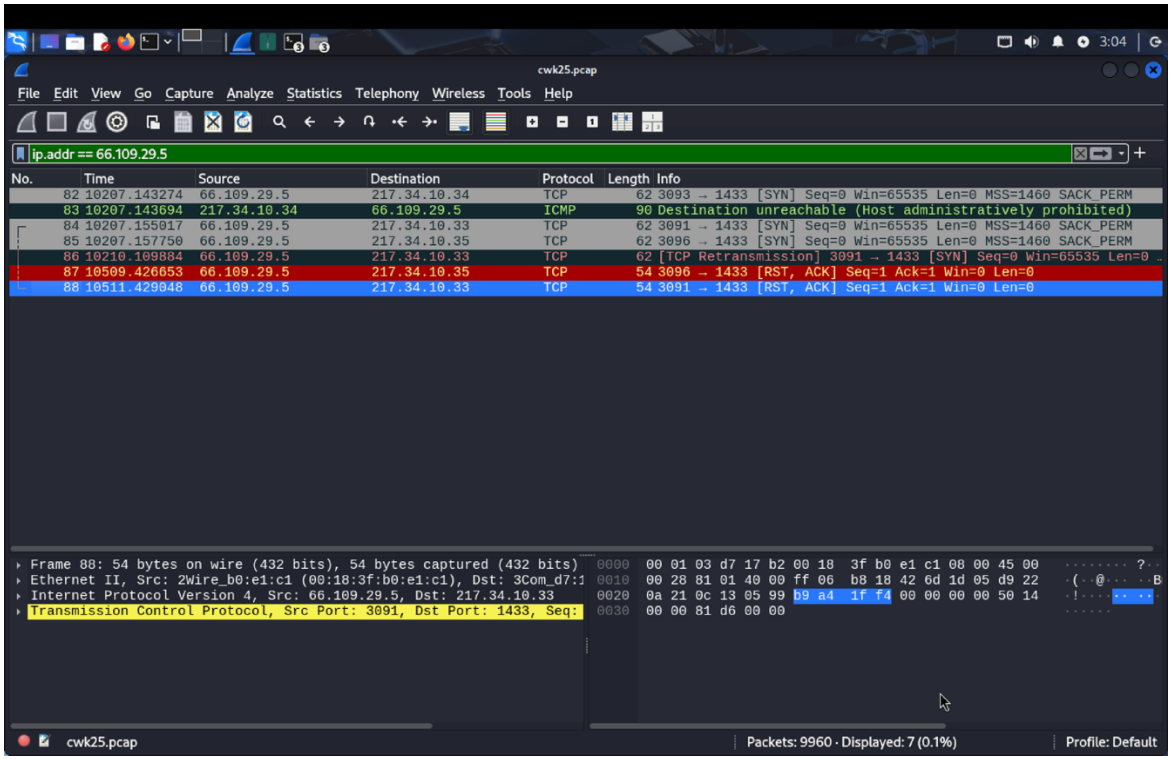
4. Targeted High-Risk Ports
    - Filter used: tcp.port ==5900 || tcp.port == 1433 || tcp.port == 80
    - Observation:
        - Attempts to port 5900 (VNC) from 66.109.29.5.
        - Attempts to port 1433 (SQL Server) from multiple sources.
- Interpretation: These ports are frequently attacked due to their remote access and database services.
- Potential Consequence: Gaining remote desktop access or stealing confidential data.



5. ICMP Echo Requests and Destination Unreachable
    - Filter used: icmp
    - Observation: Repeated ping sweeps and “Destination Unreachable (Administratively Prohibited)” replies.
    - Source: 217.34.10.34, 66.109.29.5, 89.179.156.86
    - Interpretation: Indicates network mapping or DoS attempts.
    - Potential Consequence: Gathering host availability or firewall responses.



6. Source-Focused Analysis
    - Filter Used: ip.addr == 66.109.29.5
    - Observation:
        - Probing multiple ports (1433, 5900)
        - ICMP requests
    - Interpretation: This IP is behaving like a coordinated attacker node.
    - Action: Can be marked as a high-risk external source.



Forensic Soundness

- I used Wireshark to gather all the evidence and the cwk25.pcap file.
- Filters were logged and screenshots were taken to support the findings.
- Packet payloads and headers were reviewed to verify activity without alternation.

Conclusion

The .pcap file contains strong indicators of:

- External reconnaissance (SYN scan)
- Failed intrusion attempts (RSTs)
- Targeted application-layer exploitation (phpMyAdmin probes)
- Attempts to reach high-value services (VNC, SQL)
- Suspicious ICMP sweeps

References:

1. National Institute of Standards and Technology (NIST), 2006. *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf [Accessed 26 April 2025].
2. SleuthKit, 2024. *The Sleuth Kit & Autopsy Forensic Browser*. [online] Available at: https://www.sleuthkit.org/ [Accessed 28 April 2025].
3. Wireshark, 2024. *Wireshark User Guide*. [online] Available at: https://www.wireshark.org/docs/ [Accessed 30 April 2025].
4. Scientific Research Publishing (SCIRP), n.d. *References – SCIRP*. [online] Available at: https://www.scirp.org/reference/referencespapers?referenceid=706471 [Accessed 1 May 2025].