

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

```

tsurugi@Tsurugi:~$ sudo sftp data@10.207.207.155
[sudo] password for tsurugi:
The authenticity of host '10.207.207.155 (10.207.207.155)' can't be established.
ECDSA key fingerprint is SHA256:AVJDwNRffPX6m7yFqUryEqTF0B2UTJ2g0g+0l9Peng.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.207.207.155' (ECDSA) to the list of known hosts.
Connected to 10.207.207.155.
sftp> cd "forensics 2025"
sftp> ls
RugRipper2.8-master.zip  cwk25.zip
sftp> get cwk25.zip
Fetching /usr/home/data/Forensics 2025/cwk25.zip to cwk25.zip
/usr/home/data/Forensics 2025/cwk25.zip
sftp> unzip cwk25.zip
          100%  53MB  52.8MB/s  00:00
sftp> 7z x cwk25.zip
Invalid command.
sftp> 7z x cwk25.zip
Invalid command.
sftp> quit
tsurugi@Tsurugi:~$ 7z x cwk25.zip

7-Zip [64] 9.20 Copyright (c) 1999-2010 Igor Pavlov 2010-11-18
p7zip Version 9.20 (locale=en_GB.UTF-8,Utf16=on,HugeFiles=on,1 CPU)

Processing archive: cwk25.zip

Extracting cwk25.dd
Enter password (will not be echoed) :

Everything is Ok

Size:      1009254400
Compressed: 55314251
tsurugi@Tsurugi:~$
```

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:

```

tsurugi@Tsurugi:~$ sha256sum cwk25.dd > original_hash.txt
tsurugi@Tsurugi:~$ md5sum cwk25.dd > original_md5.txt
```

Figure 2: Generating SHA256 and MD5 Hashes

- SHA-256 Hash:
421c6f18d17f04d3ed7bd664db679ac48e74689ec397809d4955c69ffbed
5313
- MD5 Hash: 75de43ba9fa5e0ea4185df160632fc9f

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

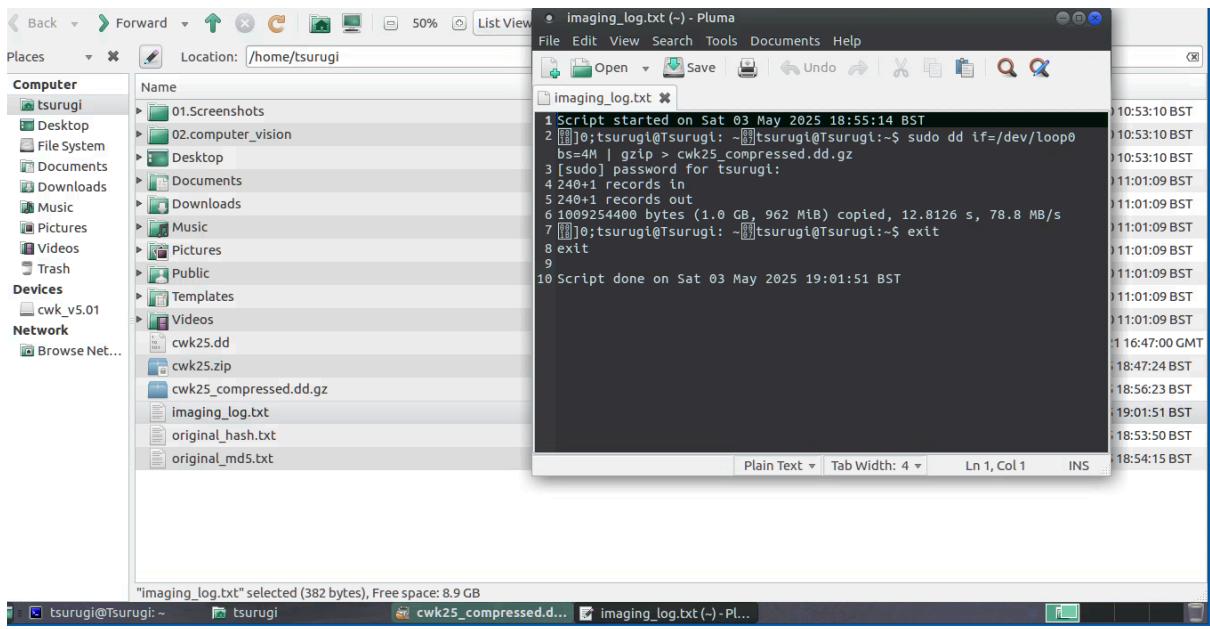


Figure 3: Imaging_log.txt

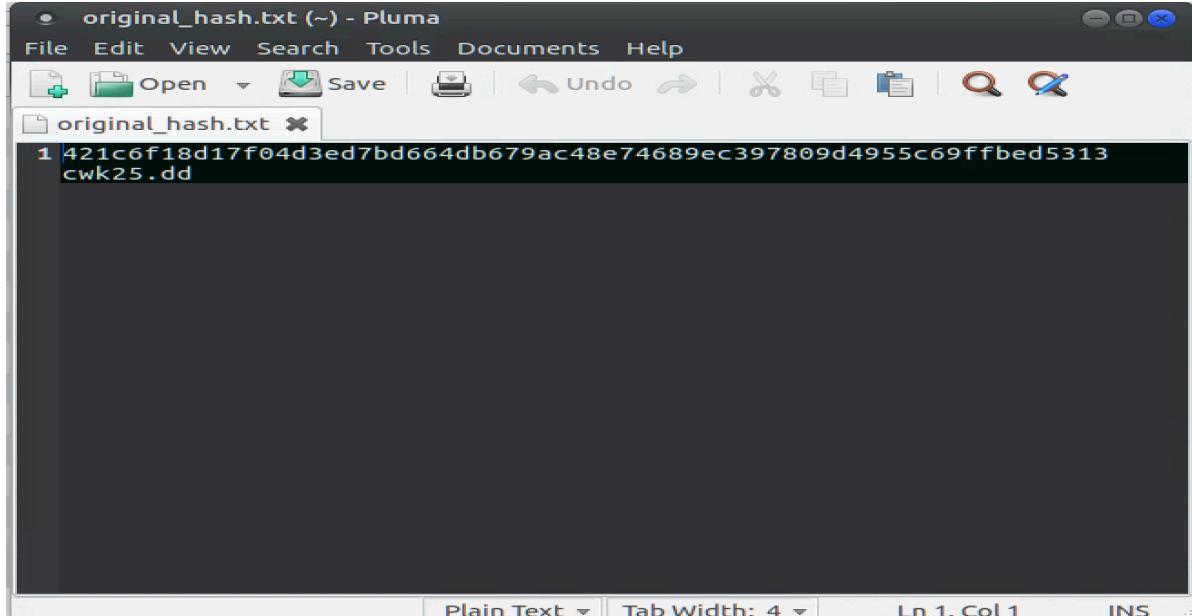


Figure 4: original_hash.txt

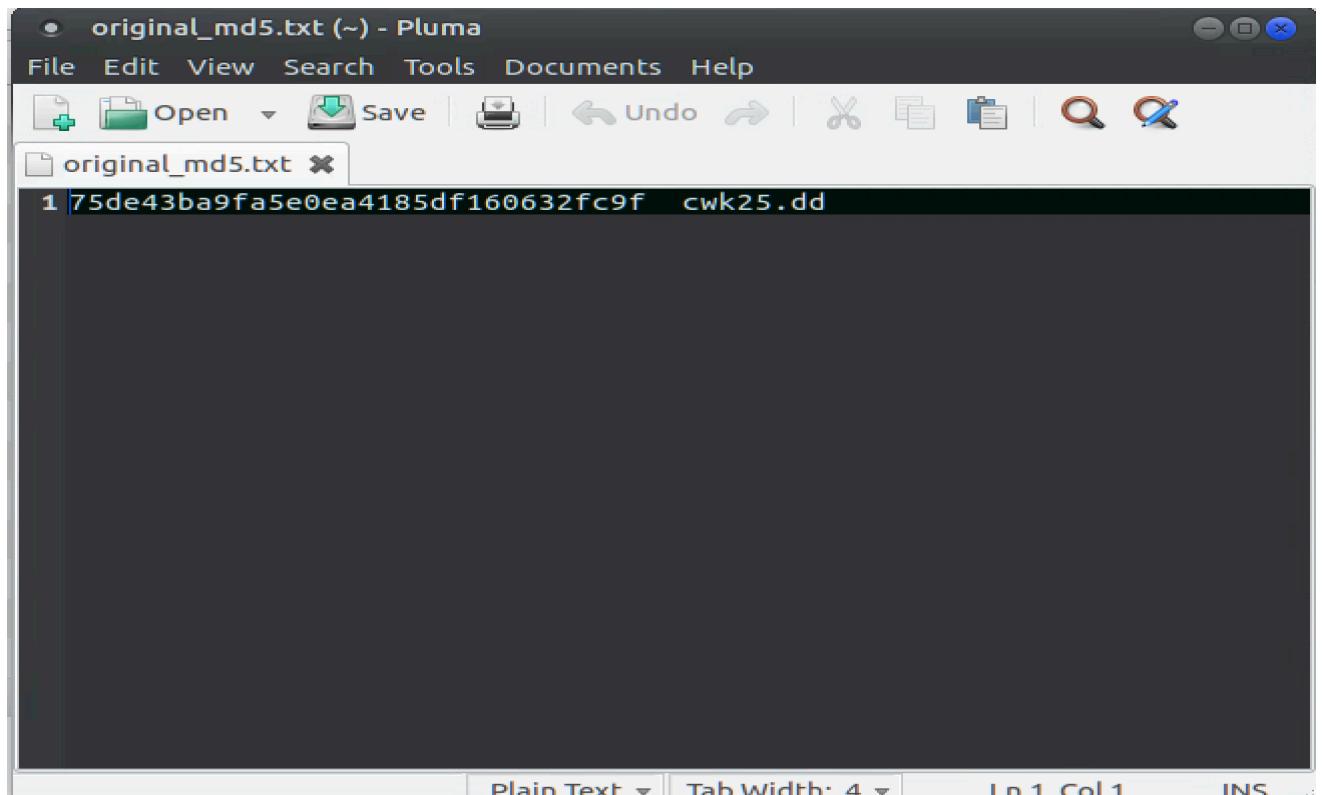


Figure 5: original_md5.txt

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:

```
|tsurugi@Tsurugi:~$ script imaging_log.txt  
|Script started, file is imaging_log.txt
```

Figure 9: Log the session before imaging

```
• imaging_log.txt (~) - Pluma
File Edit View Search Tools Documents Help

imaging_log.txt x
1 Script started on Sat 03 May 2025 18:55:14 BST
2 [0;32m[0;32m0;tsurugi@Tsurugi: ~[0;32m[0;32mtsurugi@Tsurugi:~$ sudo dd if=/dev/loop0
bs=4M | gzip > cwk25_compressed.dd.gz
3 [sudo] password for tsurugi:
4 240+1 records in
5 240+1 records out
6 1009254400 bytes (1.0 GB, 962 MiB) copied, 12.8126 s, 78.8 MB/s
7 [0;32m[0;32m0;tsurugi@Tsurugi: ~[0;32m[0;32mtsurugi@Tsurugi:~$ exit
8 exit
9
10 Script done on Sat 03 May 2025 19:01:51 BST
```

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.

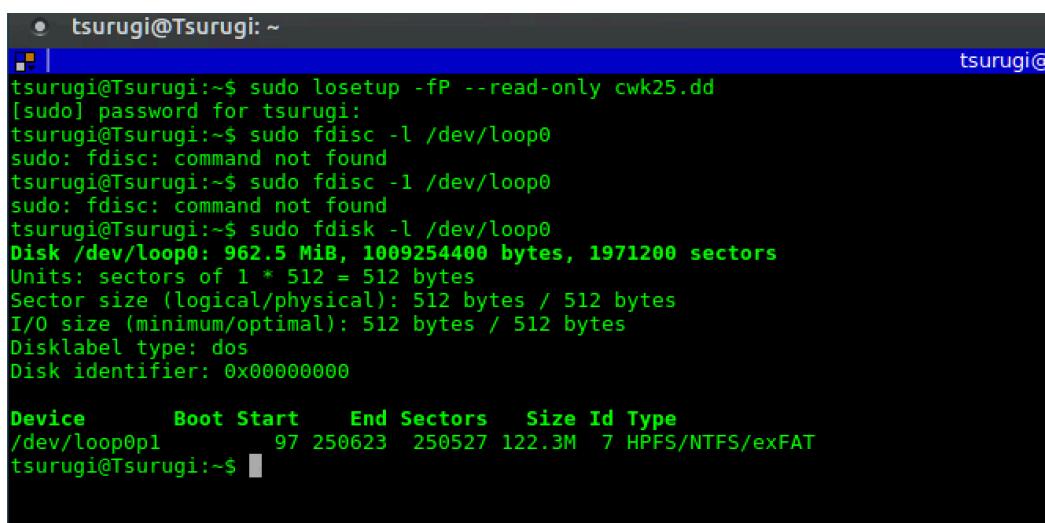
Question 2: Forensic Analysis and Evidence Recovery from cwk25.dd Disk Image

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.



A terminal window titled 'tsurugi@Tsurugi: ~' showing the following command sequence:

```
tsurugi@Tsurugi:~$ sudo losetup -fP --read-only cwk25.dd
[sudo] password for tsurugi:
tsurugi@Tsurugi:~$ sudo fdisc -l /dev/loop0
sudo: fdisc: command not found
tsurugi@Tsurugi:~$ sudo fdisc -l /dev/loop0
sudo: fdisc: command not found
tsurugi@Tsurugi:~$ sudo fdisk -l /dev/loop0
Disk /dev/loop0: 962.5 MiB, 1009254400 bytes, 1971200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device      Boot Start    End Sectors  Size Id Type
/dev/loop0p1        97 250623  250527 122.3M  7 HPFS/NTFS/exFAT
tsurugi@Tsurugi:~$
```

```

tsurugi@Tsurugi:~$ sudo fdisk -l /dev/loop0
Disk /dev/loop0: 962.5 MiB, 1009254400 bytes, 1971200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device      Boot Start   End Sectors  Size Id Type
/dev/loop0p1          97 250623 250527 122.3M 7 HPFS/NTFS/exFAT
tsurugi@Tsurugi:~$ sudo mkdir /mnt/cwk25
mkdir: cannot create directory '/mnt/cwk25': File exists
tsurugi@Tsurugi:~$ sudo mount /dev/loop0p1 /mnt/cwk25
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
Failed to reset $LogFile: Operation not permitted
Failed to sync device /dev/loop0p1: Input/output error
Failed to sync device /dev/loop0p1: Input/output error
Failed to mount '/dev/loop0p1': Operation not permitted
The NTFS partition is in an unsafe state. Please resume and shutdown
Windows fully (no hibernation or fast restarting), or mount the volume
read-only with the 'ro' mount option.
tsurugi@Tsurugi:~$ sudo mount -o ro /dev/loop0p1 /mnt/cwk25
tsurugi@Tsurugi:~$ ls /mnt/cwk25
Documents and Settings  Instruction Materials  My Music  My Shared Folder  Program Files  RECYCLE  System Volume Information  VolSer.txt  Windows
tsurugi@Tsurugi:~$
```

```

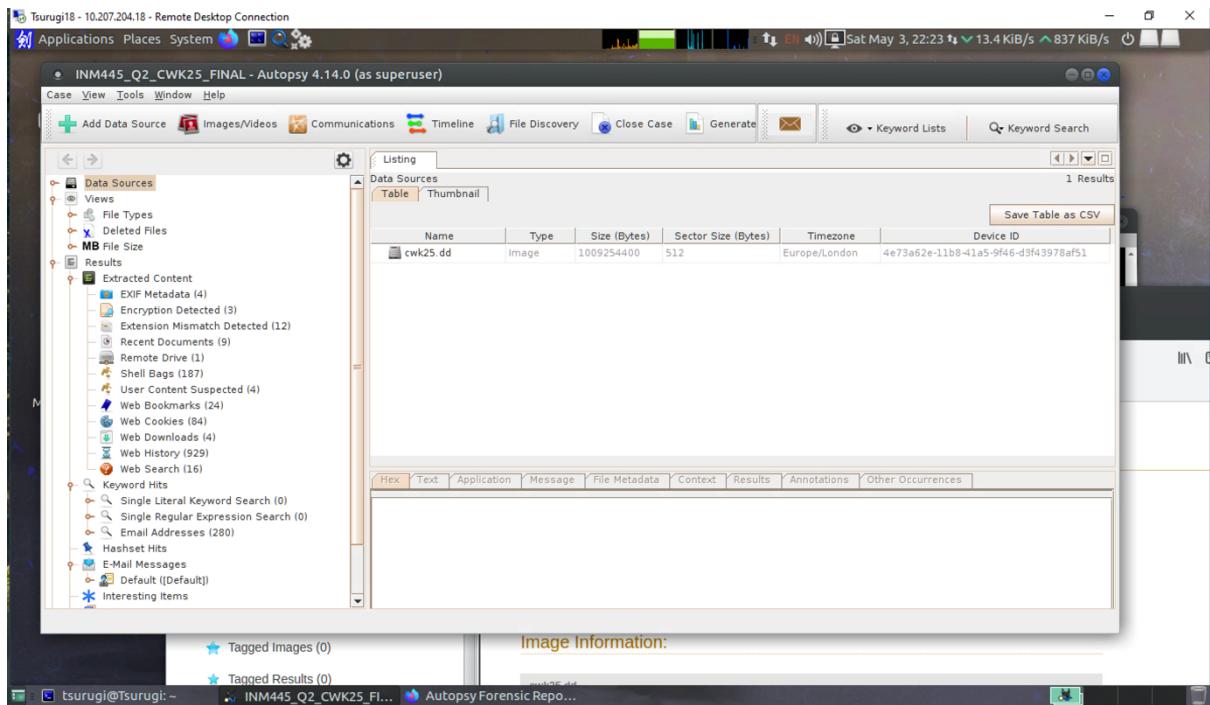
tsurugi@Tsurugi:~$ mount | grep /mnt/cwk25
/dev/loop0p1 on /mnt/cwk25 type fuseblk (ro,relatime,user_id=0,group_id=0,allow_other)
tsurugi@Tsurugi:~$ sudo umount /mnt/cwk25
sudo: umount: command not found
tsurugi@Tsurugi:~$ sudo umount /mnt/cwk25
tsurugi@Tsurugi:~$ sudo mount -o ro, noload /dev/loop0p1 /mnt/cwk25
```

3. Evidence Summary

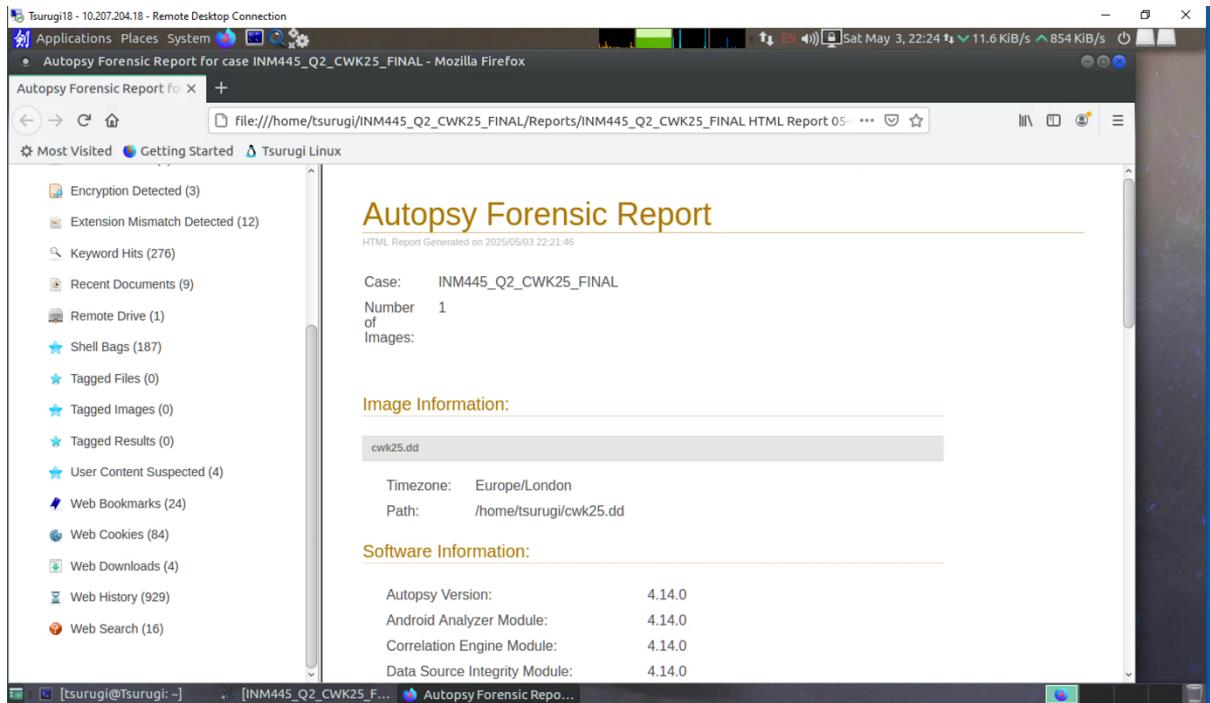
The following 24+ pieces of evidence were extracted from the cwk25.dd, each from a unique location:

- 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.



The screenshot shows a Mozilla Firefox browser window displaying an "Autopsy Forensic Report for case INM445_Q2_CWK25_FINAL". The report page has a sidebar titled "Report Navigation" with links to Case Summary, Accounts: Email (18), E-Mail Messages (39), EXIF Metadata (4), Encryption Detected (3), Extension Mismatch Detected (12), Keyword Hits (276), Recent Documents (9), Remote Drive (1), Shell Bags (187), Tagged Files (0), Tagged Images (0), Tagged Results (0), and User Content Suspected (4). The main content area is titled "Autopsy Forensic Report" and shows the following details:
Case: INM445_Q2_CWK25_FINAL
Number of Images: 1
Image Information:
cwk25.dd
Timezone: Europe/London
Path: /home/tsurugi/cwk25.dd
Software Information:
Autopsy Version: 4.14.0
Android Analyzer Module: 4.14.0
Correlation Engine Module: 4.14.0
Data Source Integrity Module: 4.14.0

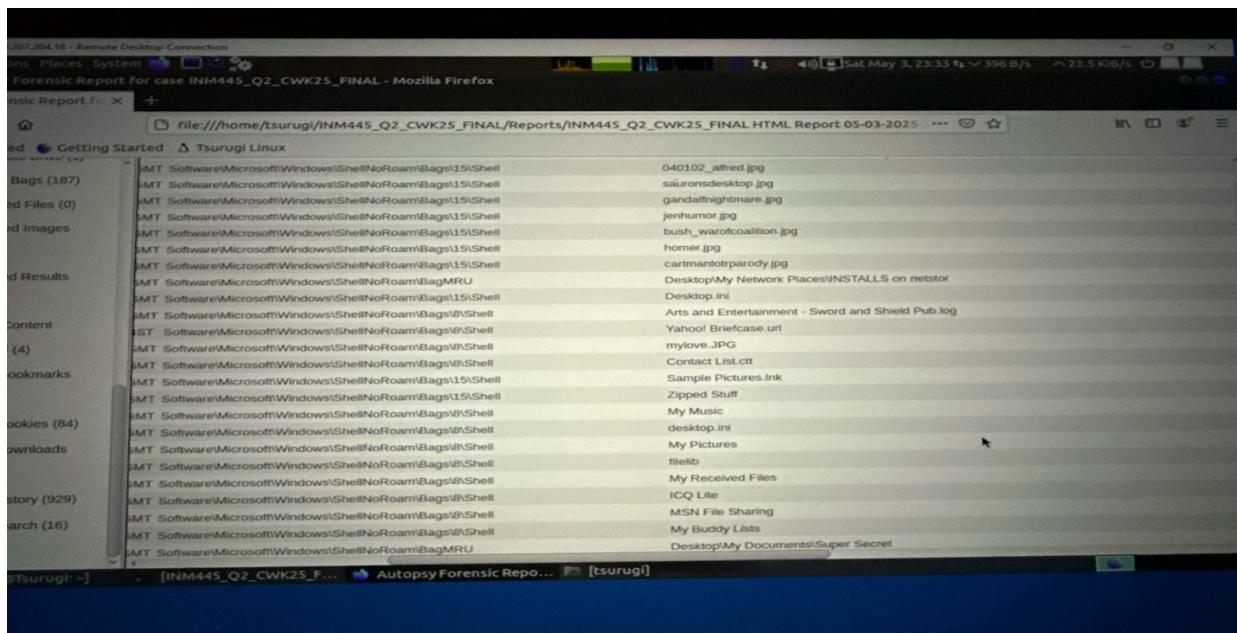
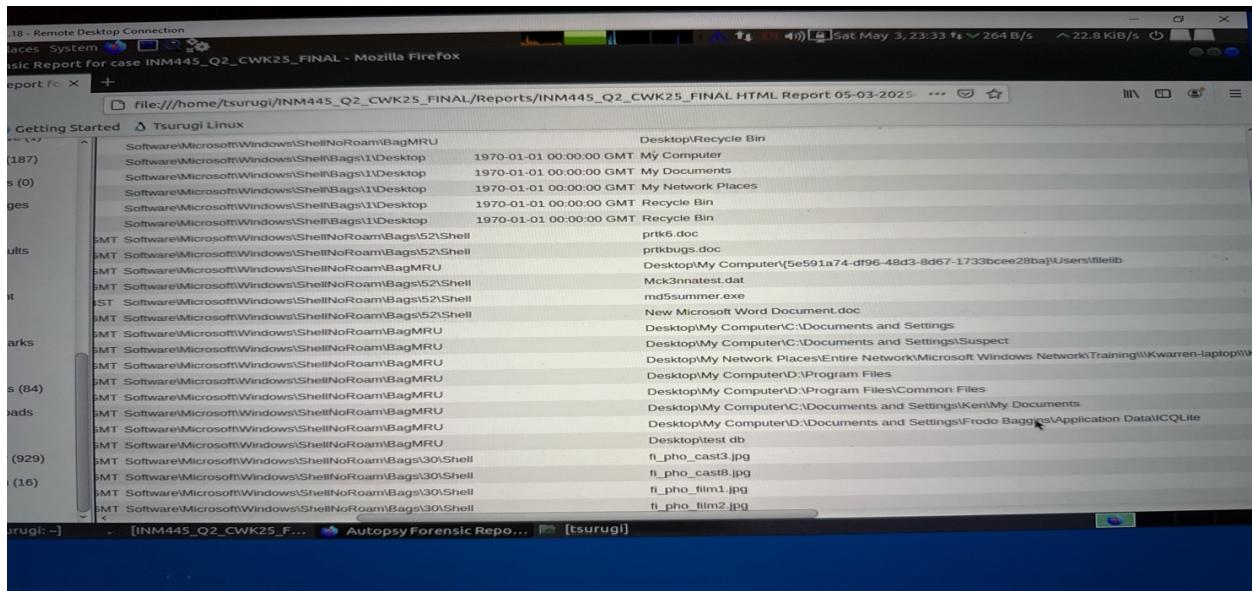


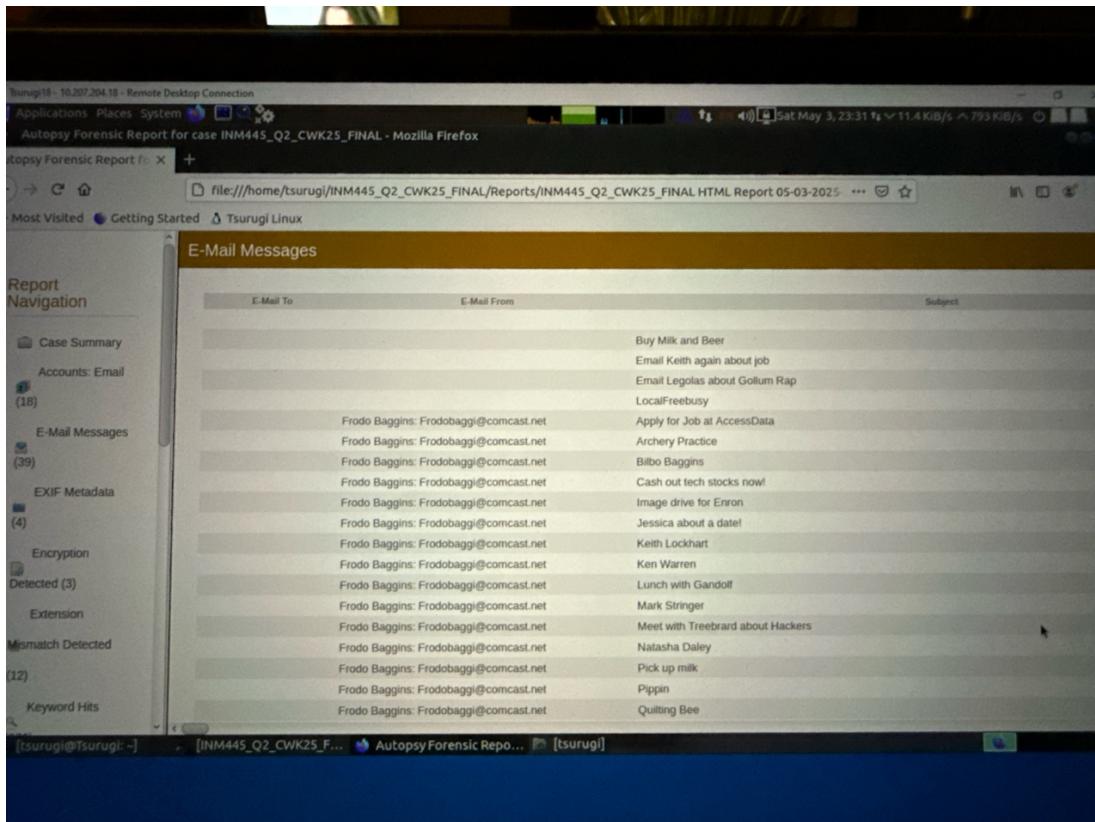
4. Obfuscation technique identified

- 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 Tsurugi Linux. Cryptographic hashes were verified before and after analysis.
- Autopsies were properly applied with full logging, ensuring transparency and reproducibility.





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.

tcp.flags.syn == 1 & tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	200.44.237.20	217.34.10.33	TCP	78 2798 - 5901 [SYN] Seq=0 Win=53760 Len=0 MSS=1460 WS=8 TSL
2	0.153976	200.44.237.20	217.34.10.35	TCP	78 2798 - 5901 [SYN] Seq=0 Win=53760 Len=0 MSS=1460 WS=8 TSL
3	0.154046	200.44.237.20	217.34.10.34	TCP	78 2797 - 5901 [SYN] Seq=0 Win=53760 Len=0 MSS=1460 WS=8 TSL
4	0.154443	217.34.10.34	200.44.237.20	ICMP	106 Destination unreachable (Host administratively prohibited)
5	0.035084	200.44.237.20	217.34.10.33	TCP	78 [TCP Retransmission] 2796 - 5901 [SYN] Seq=0 Win=53760 Len=0 MSS=1460 WS=8 TSL
6	0.046980	200.44.237.20	217.34.10.34	TCP	78 [TCP Retransmission] 2797 - 5901 [SYN] Seq=0 Win=53760 Len=0 MSS=1460 WS=8 TSL
7	0.047402	217.34.10.34	200.44.237.20	ICMP	106 Destination unreachable (Host administratively prohibited)
8	0.048683	200.44.237.20	217.34.10.35	TCP	78 [TCP Retransmission] 2798 - 5901 [SYN] Seq=0 Win=53760 Len=0 MSS=1460 WS=8 TSL
34	0.5545601449	200.44.140.145	217.34.10.35	TCP	62 3095 - 1433 [SYN] Seq=0 Win=53535 Len=0 MSS=1460 SACK_PERF
35	0.557421679	203.146.140.145	217.34.10.35	TCP	62 [TCP Retransmission] 3095 - 1433 [SYN] Seq=0 Win=53535 Len=0 MSS=1460 SACK_PERF
54	7445.592781	217.56.216.98	217.34.10.33	TCP	62 2580 - 135 [SYN] Seq=0 Win=16384 SACK_PERF
55	7445.596816	217.56.216.98	217.34.10.34	TCP	62 2581 - 135 [SYN] Seq=0 Win=16384 SACK_PERF
56	7445.727009	217.34.10.34	217.56.216.98	ICMP	90 Destination unreachable (Host administratively prohibited)
57	7445.599499	217.56.216.98	217.34.10.35	TCP	62 2582 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
58	7448.481867	217.56.216.98	217.34.10.35	TCP	62 [TCP Retransmission] 2582 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
59	7448.481157	217.56.216.98	217.34.10.33	TCP	62 [TCP Retransmission] 2580 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
60	7448.483006	217.56.216.98	217.34.10.34	TCP	62 [TCP Retransmission] 2581 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
61	7448.483417	217.34.10.34	217.56.216.98	ICMP	90 Destination unreachable (Host administratively prohibited)
62	7454.581812	217.56.216.98	217.34.10.33	TCP	62 [TCP Retransmission] 2580 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
63	7454.581891	217.56.216.98	217.34.10.35	TCP	62 [TCP Retransmission] 2582 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
64	7454.583611	217.56.216.98	217.34.10.34	TCP	62 [TCP Retransmission] 2581 - 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
65	7454.584138	217.34.10.34	217.56.216.98	ICMP	90 Destination unreachable (Host administratively prohibited)
82	18297.143274	66.169.29.5	217.34.10.34	TCP	62 3093 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
83	18297.143694	217.34.10.34	66.169.29.5	ICMP	90 Destination unreachable (Host administratively prohibited)
84	18297.143700	66.169.29.5	217.34.10.33	TCP	62 3091 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
85	18297.157690	66.169.29.5	217.34.10.35	TCP	62 3092 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
86	18297.169934	66.169.29.5	217.34.10.33	TCP	62 [TCP Retransmission] 3093 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
126	18297.785355	217.169.219.81	217.34.10.33	TCP	62 4162 - 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
121	15144.797423	217.169.219.81	217.34.10.35	TCP	62 4162 - 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
122	15144.715146	217.169.219.81	217.34.10.34	TCP	62 4162 - 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
123	15144.715527	217.34.10.34	211.169.219.81	ICMP	90 Destination unreachable (Host administratively prohibited)
134	18537.591352	217.75.215.231	217.34.10.35	TCP	62 2250 - 5900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERF
135	18548.531946	217.75.215.231	217.34.10.35	TCP	62 [TCP Retransmission] 2250 - 5900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERF
197	26728.245912	66.119.52.5	217.34.10.35	TCP	62 2984 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
198	26728.247439	66.119.52.5	217.34.10.33	TCP	62 2982 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
199	26728.266936	66.119.52.5	217.34.10.34	TCP	62 2983 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
200	26728.271166	66.119.52.5	217.34.10.34	ICMP	90 Destination unreachable (Host administratively prohibited)
201	26731.246984	66.119.52.5	217.34.10.34	TCP	62 [TCP Retransmission] 2983 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
202	26731.247344	217.34.10.34	66.119.52.5	ICMP	90 Destination unreachable (Host administratively prohibited)
209	27224.698022	64.34.69.65	217.34.10.33	TCP	62 2908 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
210	27224.727348	64.34.69.65	217.34.10.34	TCP	62 2911 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
211	27224.727331	217.34.10.34	64.34.69.65	ICMP	90 Destination unreachable (Host administratively prohibited)
212	27224.780884	64.34.69.65	217.34.10.35	TCP	62 2922 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
213	27227.662191	64.34.69.65	217.34.10.33	TCP	62 [TCP Retransmission] 2908 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
214	27227.770622	64.34.69.65	217.34.10.34	TCP	62 [TCP Retransmission] 2911 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
215	27227.771007	217.34.10.34	64.34.69.65	ICMP	90 Destination unreachable (Host administratively prohibited)
216	27227.772436	64.34.69.65	217.34.10.35	TCP	62 [TCP Retransmission] 2914 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
217	27233.679034	64.34.69.65	217.34.10.33	TCP	62 [TCP Retransmission] 2908 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
218	27233.788645	64.34.69.65	217.34.10.35	TCP	62 [TCP Retransmission] 2914 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
219	27233.788717	64.34.69.65	217.34.10.34	TCP	62 [TCP Retransmission] 2911 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
220	27233.789100	217.34.10.34	64.34.69.65	ICMP	90 Destination unreachable (Host administratively prohibited)
232	28166.780853	218.50.54.32	217.34.10.33	TCP	54 6000 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
233	28166.792987	218.50.54.32	217.34.10.35	TCP	54 6000 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
234	28166.794594	218.50.54.32	217.34.10.34	TCP	54 6000 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
235	28166.795047	217.34.10.34	218.50.54.32	ICMP	82 Destination unreachable (Host administratively prohibited)
242	29341.274933	80.93.220.94	217.34.10.33	TCP	62 1177 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
243	29341.280995	80.93.220.94	217.34.10.35	TCP	62 1179 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
244	29341.281068	80.93.220.94	217.34.10.34	TCP	62 1178 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
245	29341.281442	217.34.10.34	80.93.220.94	ICMP	90 Destination unreachable (Host administratively prohibited)
246	29344.278871	80.93.220.94	217.34.10.34	TCP	62 [TCP Retransmission] 1178 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
247	29344.278967	80.93.220.94	217.34.10.33	TCP	62 [TCP Retransmission] 1177 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
248	29344.279268	217.34.10.34	80.93.220.94	ICMP	90 Destination unreachable (Host administratively prohibited)
249	29344.280866	80.93.220.94	217.34.10.35	TCP	62 [TCP Retransmission] 1179 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF

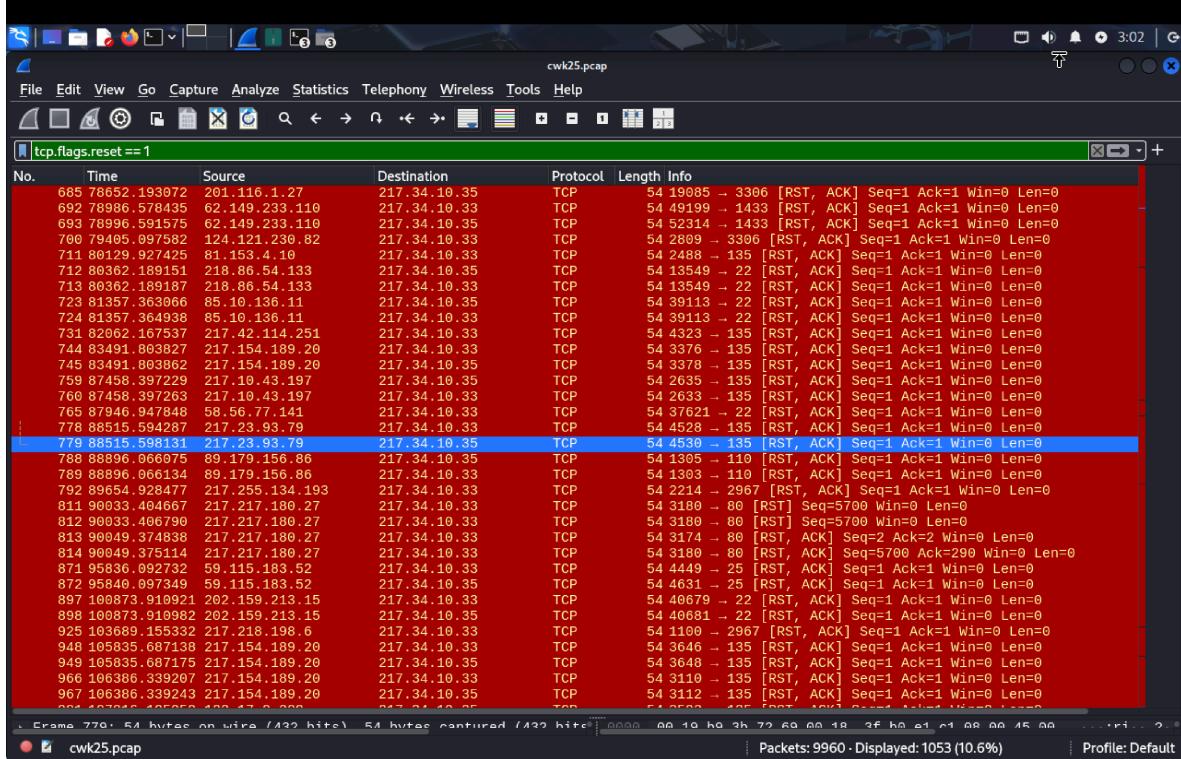
tcp.flags.syn == 1 & tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length Info
123	15144.715527	217.34.10.34	211.169.219.81	ICMP	90 Destination unreachable (Host administratively prohibited)
134	18537.591352	217.75.215.231	217.34.10.35	TCP	62 2250 - 5900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERF
135	18548.531946	217.75.215.231	217.34.10.35	TCP	62 [TCP Retransmission] 2250 - 5900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERF
197	26728.245912	66.119.52.5	217.34.10.35	TCP	62 2984 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
198	26728.247439	66.119.52.5	217.34.10.33	TCP	62 2982 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
199	26728.266936	66.119.52.5	217.34.10.34	TCP	62 2983 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
200	26728.271166	66.119.52.5	217.34.10.34	ICMP	90 Destination unreachable (Host administratively prohibited)
201	26731.246984	66.119.52.5	217.34.10.34	TCP	62 [TCP Retransmission] 2983 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
202	26731.247344	217.34.10.34	66.119.52.5	ICMP	90 Destination unreachable (Host administratively prohibited)
209	27224.698022	64.34.69.65	217.34.10.33	TCP	62 2908 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
210	27224.727348	64.34.69.65	217.34.10.34	TCP	62 2911 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
211	27224.727331	217.34.10.34	64.34.69.65	ICMP	90 Destination unreachable (Host administratively prohibited)
212	27224.780884	64.34.69.65	217.34.10.35	TCP	62 2922 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
213	27227.662191	64.34.69.65	217.34.10.33	TCP	62 [TCP Retransmission] 2908 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
214	27227.770622	64.34.69.65	217.34.10.34	TCP	62 [TCP Retransmission] 2911 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
215	27227.771007	217.34.10.34	64.34.69.65	ICMP	90 Destination unreachable (Host administratively prohibited)
216	27227.772436	64.34.69.65	217.34.10.35	TCP	62 [TCP Retransmission] 2914 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
217	27233.679034	64.34.69.65	217.34.10.33	TCP	62 [TCP Retransmission] 2908 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
218	27233.788645	64.34.69.65	217.34.10.35	TCP	62 [TCP Retransmission] 2914 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
219	27233.788717	64.34.69.65	217.34.10.34	TCP	62 [TCP Retransmission] 2911 - 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
220	27233.789100	217.34.10.34	64.34.69.65	ICMP	90 Destination unreachable (Host administratively prohibited)
232	28166.780853	218.50.54.32	217.34.10.33	TCP	54 6000 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
233	28166.792987	218.50.54.32	217.34.10.35	TCP	54 6000 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
234	28166.794594	218.50.54.32	217.34.10.34	TCP	54 6000 - 1433 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERF
235	28166.795047	217.34.10.34	218.50.54.32	ICMP	82 Destination unreachable (Host administratively prohibited)
242	29341.274933	80.93.220.94	217.34.10.33	TCP	62 1177 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
243	29341.280995	80.93.220.94	217.34.10.35	TCP	62 1179 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
244	29341.281068	80.93.220.94	217.34.10.34	TCP	62 1178 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
245	29341.281442	217.34.10.34	80.93.220.94	ICMP	90 Destination unreachable (Host administratively prohibited)
246	29344.278871	80.93.220.94	217.34.10.34	TCP	62 [TCP Retransmission] 1178 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
247	29344.278967	80.93.220.94	217.34.10.33	TCP	62 [TCP Retransmission] 1177 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF
248	29344.279268	217.34.10.34	80.93.220.94	ICMP	90 Destination unreachable (Host administratively prohibited)
249	29344.280866	80.93.220.94	217.34.10.35	TCP	62 [TCP Retransmission] 1179 - 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERF

2. Rejected TCP Connections (RST Response)

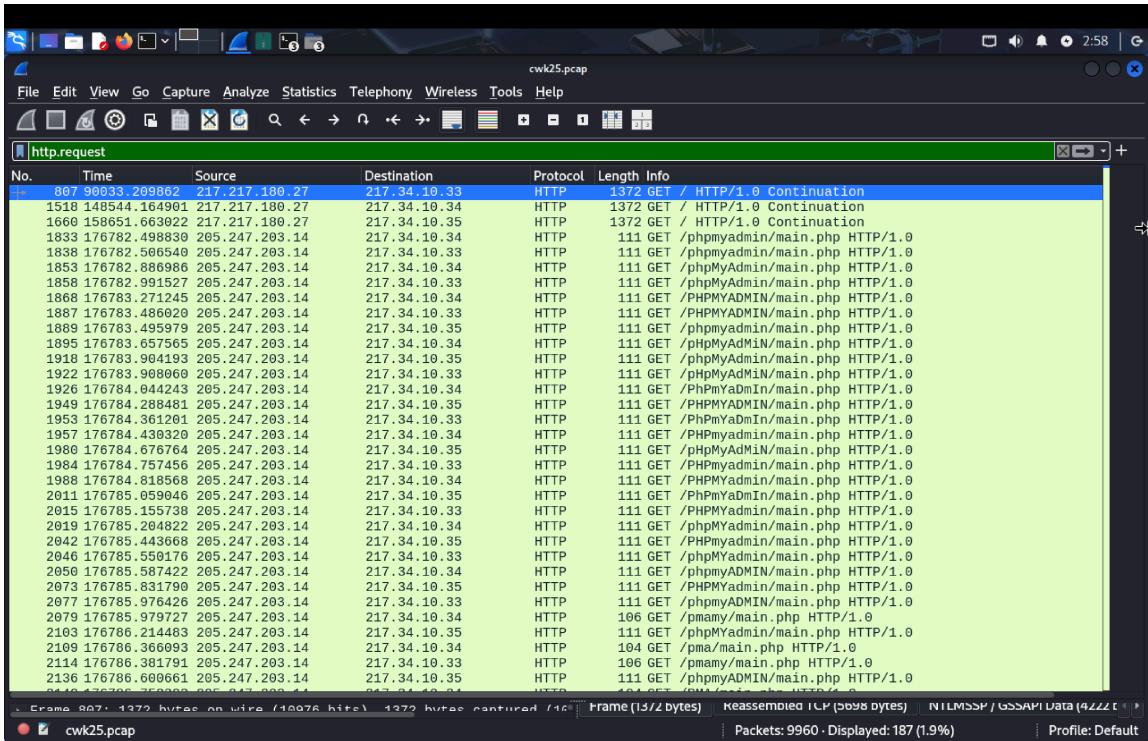
- Filtered used: `tcp.flags.reset == 1`
- Observation: High frequency of RST flags from the target system (217.34.10.35)
- Interpretation: Connections were reset, indicating blocked or failed access attempts, possibly in response to scans or intrusion attempts.

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



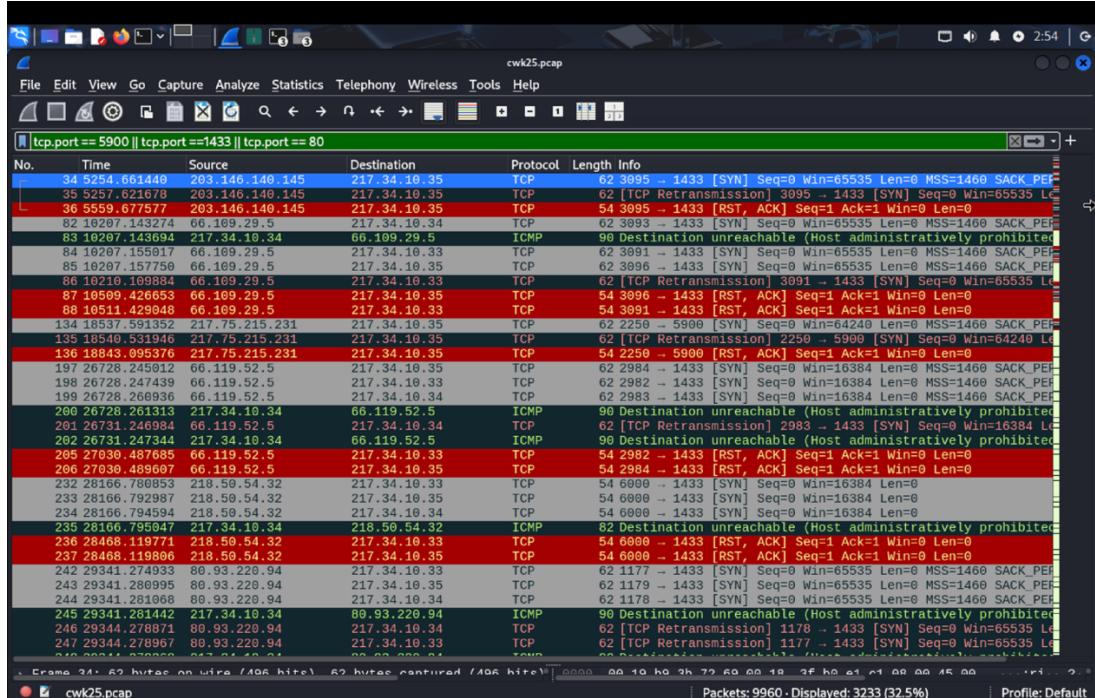
3. HTTP phpMyAdmin Access Attempts

- 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.



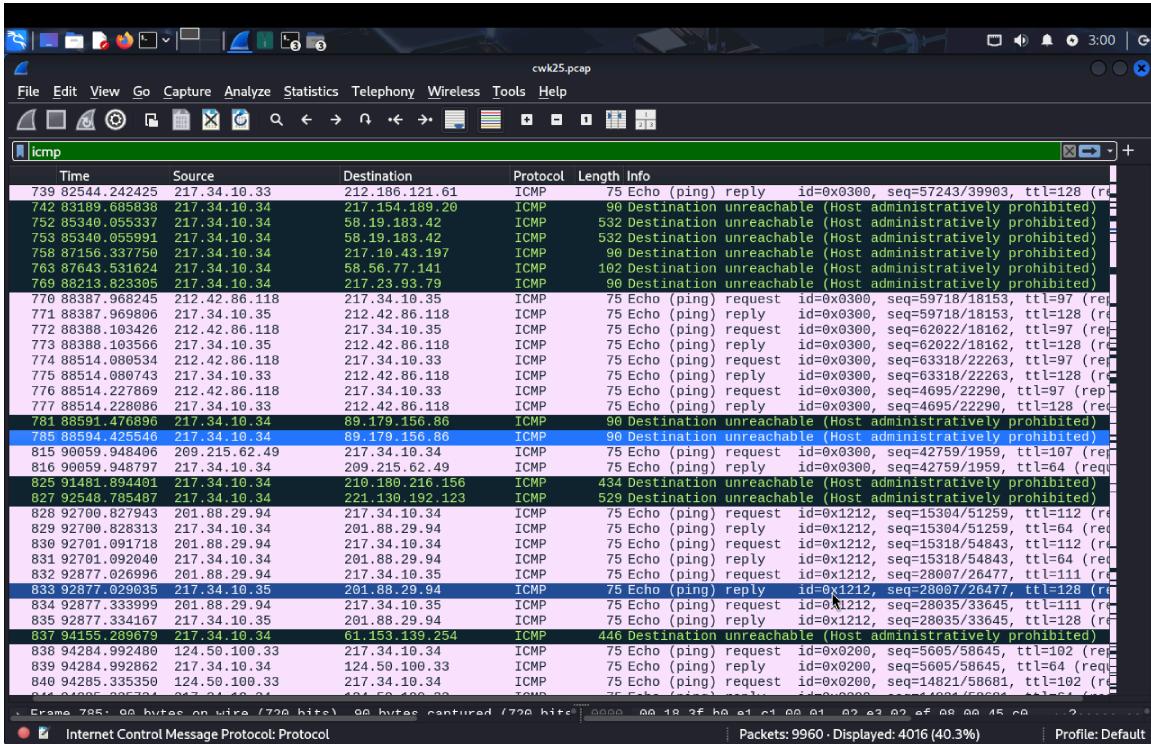
4. Targeted High-Risk Ports

- 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.



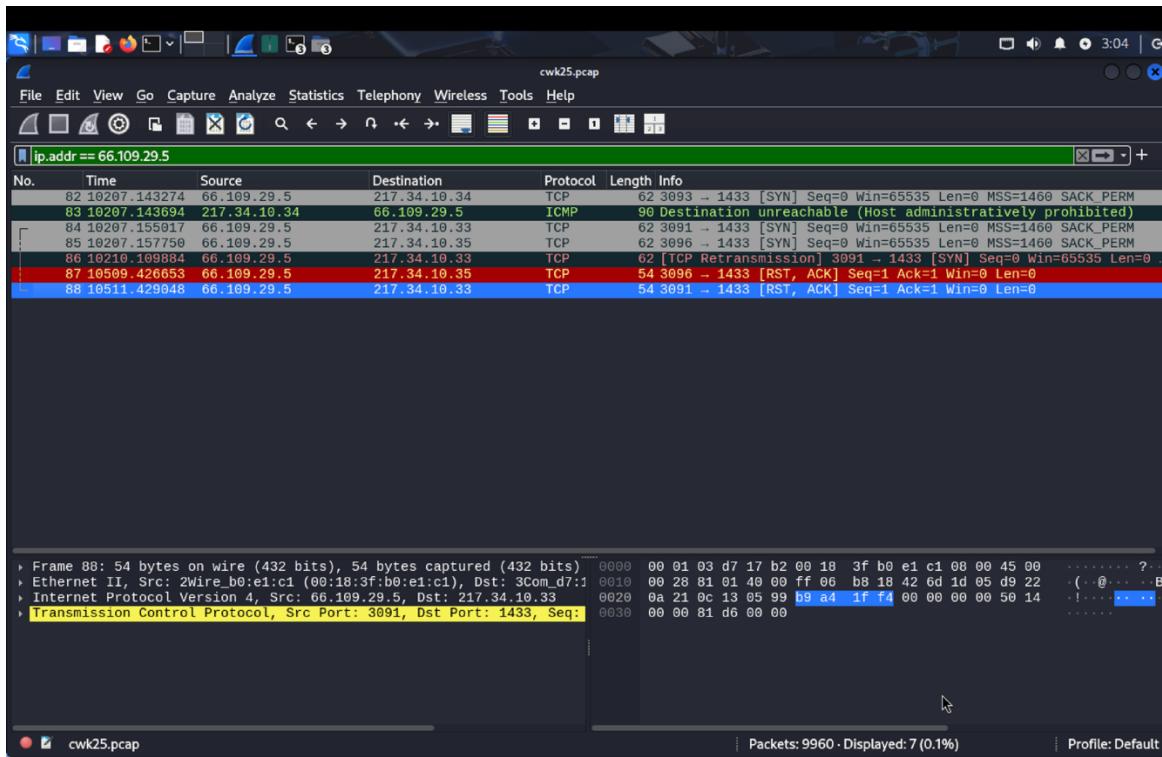
5. ICMP Echo Requests and Destination Unreachable

- 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 alteration.

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].