Forensic Investigation Report: Suspicious Activity at Acme Ltd.

DONNA NAADU BOTCHWAY

03 APRIL 2025

ROBERT GORDON UNIVERSITY

WORD COUNT : 2,705

Table of Contents

1.0 Executive Summary 1

2.0 Scope of Report 2

3.0 Evidence Analysed 2

4.0 Forensic Method 3

4.1 VM Disk Analysis 3

4.2 Memory Analysis 3

4.3 Network Analysis 3

5.0 Initial Analysis Findings 4

5.1 VM Disk Analysis 4

5.1.1 Basic Information 4

5.1.2 User Accounts 4

5.1.3 Stored & Deleted Files 4

5.1.4 Recent Activity 5

5.2 Memory Analysis 6

5.3 Network Analysis 8

6.0 Detail Analysis Findings 9

6.1 VM Disk Analysis 9

6.1.1 Connected Devices 9

6.1.2 Browser Activity 9

6.1.3 Email Analysis 10

6.1.4 File Analysis and Deleted Files 10

6.1.5 Desktop Items and Installed Software 11

6.2 Memory Analysis 12

6.2.1 System Activity 12

6.2.2 Network and Email Activity. 13

6.2.3 File Access 13

6.3 Network Analysis 14

6.3.1 Recent Network Activity 14

6.3.2 Websites Visited 15

6.3.3 Data Sent/Received 15

7.0 Timeline of Events 18

8.0 Conclusions report to the CEO 20

9.0 References 21

10.0 Appendix 22

Appendix A: VM Disk Image Analysis 22

Appendix B: RAM (Memory) Analysis 26

Appendix C: Detailed Timeline of Events 27

Table of Figures

Figure 1: VM Disk Basic Information 4
Figure 2: OS Accounts 4
Figure 3: File type distribution. 5
Figure 4: USB Device Attached 5
Figure 5: Web Search 6
Figure 6: Email Communication 6
Figure 7: Recent Documents 6
Figure 8: Imageinfo 7
Figure 9: Process Analysis (pstree) 7
Figure 10: Command Prompt History 8
Figure 11: Clipboard History 8
Figure 12: Network Traffic 8
Figure 13: Kingston USB 9
Figure 14: Favicon 10
Figure 15: Email titled "A cute kitten" 10
Figure 16: Hidden text found in Autopsy 11
Figure 17: Likely Notable-Kitten 11
Figure 18: Sales Desktop 11
Figure 19: Installed Programs 12
Figure 20: Sessions - RAM Analysis 12
Figure 21: Windows logs - RAM Analysis 13
Figure 22: Timeliner - RAM Analysis 14
Figure 23: HTTP Traffic 14
Figure 24: TLS Traffic-1 15
Figure 25: TLS Traffic-2 15
Figure 26: SMTP Traffic 16
Figure 27: Hidden text found via kali 16
Figure 28: IMAP Traffic 16
Figure 29: Telnet Traffic 17
Figure 30: Timeline of Events-1 18
Figure 31: Timeline of Events-2 19
Figure 32: Directory Tree – Autopsy 22
Figure 33: Kingston USB as Drive D 22
Figure 34: Operating System Info 23
Figure 35: Research and Sales User Info 24
Figure 36: Chrome Extensions 24
Figure 37: Metadata 25
Figure 38: Web Cookies 25
Figure 39: Volatility modules 26
Figure 40: Netscan - RAM Analysis 26
Figure 41: Consoles - RAM Analysis 27
Figure 42:Detailed Timeline 27

1.0 Executive Summary

This report presents the findings of a forensic investigation into potential misconduct, and data breach at ACME Ltd. The investigation focused on examining a virtual machine disk image, memory capture, and network traffic logs using industry-standard forensic tools such as Autopsy, Volatility, and Wireshark.

The investigation revealed that on June 18, 2024, web searches related to steganography and Kali Linux were conducted, indicating an interest in data concealment. At 11:24:43 BST, a “Kingston Data Traveler 100 G2 (8 GiB)” USB was connected, shortly after, a file named kitten.jpg was created and accessed by both the Research and Sales user accounts.

At 11:48:35 BST, an email titled "A cute kitten" was sent from sales@shadowfall.non to alpha@other.non with kitten.jpg attached. Inspecting the image revealed that it contained embedded text related to rocket construction, suggesting potential exfiltration of sensitive information. Memory analysis confirmed clipboard history matching the extracted steganographic content within kitten.jpg.

A Telnet session was initiated from 192.168.101.129 to 192.168.101.128 at 11:49:18 BST, raising concerns of unauthorized remote access, but it occurred after the email was sent, ruling out Telnet as an exfiltration method. At 11:51:13 BST, a New Rich Text Document.rtf was deleted from the Sales desktop. Then at 11:52:03 BST, FTK Imager.exe was executed, possibly by the forensic analyst capturing evidence.

The investigation identified unauthorized data access, possible data exfiltration via steganography, and suspicious USB activity. While no direct evidence of steganography tool was found, the sequence of events: web searches, clipboard history, email activity, and file deletions, suggests deliberate data concealment and transmission.

Further investigation into user intent, access permissions, and potential insider threats is recommended. Additionally, log reviews, user activity monitoring, and enhanced access controls should be implemented to prevent future incidents.

2.0 Scope of Report

The objective of this investigation is to analyse digital evidence for indications of misconduct, data breaches, or unauthorized activity within ACME Ltd.

The analysis aims to:

- Identify stored, deleted, and recently accessed files by examining the VM disk image.
- Analyse the memory capture for active processes, network connections, and user activity.
- Investigate the network capture to identify browsing activity, data transfers, and email communications.

3.0 Evidence Analysed

The forensic analysis was conducted on the following digital evidence:

- **Virtual Machine Disk Image**: Win-7-Forensics1.vmdk (42.95 GB) containing system files, user activity logs, and deleted files.
- **Memory Capture**: RAM dump used to analyse running processes, clipboard history, and volatile system activity.
- **Network Traffic Capture**: PCAP file showing network connections, website visits and email transactions.

4.0 Forensic Method

All timestamps in this report have been converted from UTC to BST for consistency. The forensic methodology focused on reconstructing system activity, identifying potential data exfiltration, and tracing user actions using industry-standard tools: Autopsy, Volatility, and Wireshark. As emphasized in chain of custody (Harris, 2025a), a copy of the evidence was used to ensure that the original evidence remained untouched.

4.1 VM Disk Analysis

Autopsy 4.21.0 was used to examine disk artifacts and system activity.

- A custom rule was created to identify all occurrences of "kitten," allowing for targeted analysis of potentially relevant files.
- System metadata, user accounts, and operating system artifacts were reviewed to understand user behaviour.
- Regripper reports were analysed to extract registry data, including attached USB devices, shellbags, user activity, and system interactions.
- The Recycle Bin was inspected to identify deleted files, and web artifacts such as cookies, cache, searches, history, email communication, recently accessed documents, and favicons were examined to reconstruct the suspect's digital footprint.

4.2 Memory Analysis

Memory analysis was conducted using Volatility, employing multiple plugins to extract system activity, user interactions, and forensic artifacts. Key commands included:

- pslist, pstree, psscan – Identified running, terminated, and hidden processes.
- cmdscan, consoles – Recovered command-line execution history.
- clipboard – Revealed copied content.
- netscan – Analysed network connections and external communications.
- iehistory, shellbags, timeliner – Reconstructed user activity patterns over time.
- mftparser – Examined file system metadata for forensic timeline reconstruction.
- wintree, imageinfo – Provided insights into system processes and memory structure.

4.3 Network Analysis

Network traffic was examined using Wireshark, focusing on 192.168.101.128, the suspect's system.

- Filters such as SMTP, IP address filters, TLS handshake (tls.handshake.type == 1), HTTP, FTP, and TCP were applied to trace communication patterns and data transfers.
- DNS and SNI analysis helped identify visited websites.

Also, the strings command in Kali Linux was used to extract readable text from kitten.jpg, revealing embedded steganographic content.
This structured forensic approach ensured accurate evidence extraction, timeline reconstruction, and identification of unauthorized activities within ACME Ltd.

5.0 Initial Analysis Findings

5.1 VM Disk Analysis

The VM disk image was analysed using Autopsy 4.21.0 revealing the system's basic information, user accounts, files, and recent activity.

5.1.1 Basic Information

Category	Details
Operating System	Windows 7 Enterprise (64-bit)
Architecture	AMD64
Hostname	Networkadmin
IP Address	192.168.101.128
Time zone	Europe/London (BST)
Product ID	00392-918-5000002-85014
Image Name	Win-7-Forensics1.vmdk
Image Size	42.95 GB (29.83 GB unallocated)
Sector Size	512 Bytes
Install Date	May 18, 2022, 11:58:32

Figure 1: VM Disk Basic Information

5.1.2 User Accounts

The system contains multiple user accounts like SYSTEM, NT SERVICE, NETWORK SERVICE, and LOCAL SERVICE, which are built-in system accounts. The Administrator and Guest accounts were created on May 18, 2022. Additional domain accounts, Research and Sales, were created on June 17 and June 18, 2024, respectively.

Name	...	...	...	Login Name	...	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	...	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464			0		...	Local	NT SERVICE	
S-1-5-20				NETWORK SERVICE	...	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	...	Local	NT AUTHORITY	
S-1-5-21-2375367772-2383046927-4008981907-500			0	Administrator	...	Domain		2022-05-18 11:57:04 BST
S-1-5-21-2375367772-2383046927-4008981907-501			0	Guest	...	Domain		2022-05-18 11:57:04 BST
S-1-5-21-2375367772-2383046927-4008981907-1002			0	Research	...	Domain		2024-06-17 15:43:23 BST
S-1-5-21-2375367772-2383046927-4008981907-1003			0	Sales	...	Domain		2024-06-18 11:27:54 BST

Figure 2: OS Accounts

5.1.3 Stored & Deleted Files

The analysis identified 125,692 allocated files and 24,599 deleted files, including 66 files deleted from the file system. New Rich Text Document.rtf and Test folder were found in the recycle bin. Figure 3 shows the detailed breakdown of file types, such as image, video, document, and executable files.

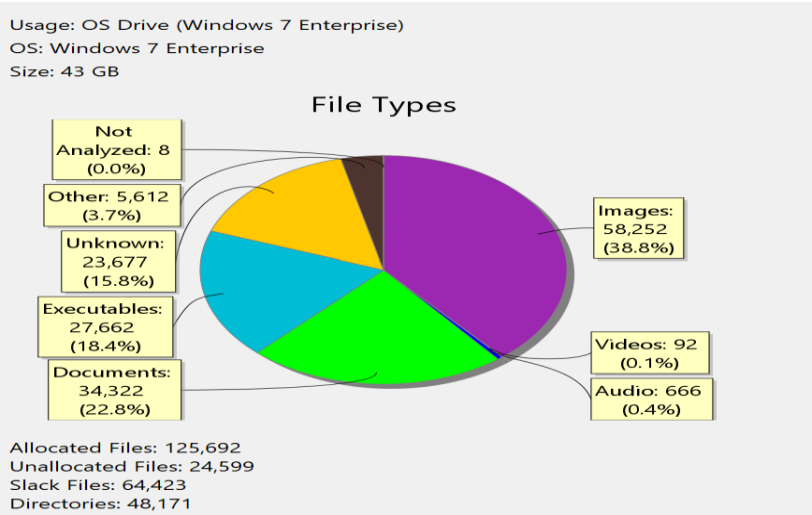

Figure 3: File type distribution.

5.1.4 Recent Activity

The analysis showed that on June 18, 2024, a Kingston Technology Data Traveler 100 G2 (8 GiB) USB was connected at 11:24:43 BST. Multiple VMware Virtual USB hubs and mice were also connected (Figure 4).

USB Device Attached

Table | Thumbnail | Summary

Source Name	...	...	O	Date/Time	Device Make	Device Model	Device ID
SYSTEM			0	2024-06-18 11:24:43 BST	Kingston Technology	Data Traveler 100 G2 8 GiB	0018F30C9FE8EA81C00001EC
SYSTEM			0	2024-06-18 11:24:43 BST	VMware, Inc.	Virtual USB Hub	6&e0b0e60&0&8
SYSTEM			0	2024-06-18 11:24:42 BST	VMware, Inc.	Virtual USB Hub	6&e0b0e60&0&7
SYSTEM			0	2024-06-18 11:14:31 BST	VMware, Inc.	Virtual USB Hub	6&b25d31b&0&2
SYSTEM			0	2024-06-18 11:14:30 BST		ROOT_HUB	5&17df1c1b&0
SYSTEM			0	2024-06-18 11:14:30 BST		ROOT_HUB20	5&2648447&0
SYSTEM			0	2024-06-18 11:14:30 BST	VMware, Inc.	Virtual Mouse	6&e0b0e60&0&5
SYSTEM			0	2024-06-18 11:14:30 BST	VMware, Inc.	Virtual Mouse	7&29078710&0&0000
SYSTEM			0	2024-06-18 11:14:30 BST	VMware, Inc.	Virtual Mouse	7&29078710&0&0001
SYSTEM			0	2024-06-18 11:14:30 BST	VMware, Inc.	Product: 0008	000650268328
SYSTEM			0	2024-06-18 02:58:00 BST	VMware, Inc.	Virtual Mouse	6&b25d31b&0&1
SYSTEM			0	2024-06-18 02:58:00 BST	VMware, Inc.	Virtual Mouse	7&2a63cead&0&0000
SYSTEM			0	2024-06-18 02:58:00 BST	VMware, Inc.	Virtual Mouse	7&2a63cead&0&0001
SYSTEM			0	2024-06-16 12:34:15 BST	VMware, Inc.	Virtual USB Hub	6&b25d31b&0&2
SYSTEM			0	2024-06-16 12:34:14 BST	VMware, Inc.	Virtual Mouse	7&29078710&0&0000
SYSTEM			0	2024-06-16 12:34:14 BST	VMware, Inc.	Virtual Mouse	7&29078710&0&0001
SYSTEM			0	2024-06-16 12:34:14 BST	VMware, Inc.	Product: 0008	000650268328
SYSTEM			0	2024-06-16 12:34:13 BST		ROOT_HUB	5&17df1c1b&0

Figure 4: USB Device Attached

The browser history showed that at 11:47 BST, google.com was the most accessed domain, with additional visits to tutorialspoint.com, freecodecamp.org and springeropen.com. A web search for "How to use steganography and Kali" was performed during this time (Figure 5).

Web Search

Table Thumbnail Summary

Source Name	...	...	...	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	how to install kali linux	Google Chrome	2024-06-18 10:01:06 BST	Win-7-Forensics1.vmdk
History				google.com	how to install kali linux	Google Chrome	2024-06-18 10:01:06 BST	Win-7-Forensics1.vmdk
History				google.com	steganography in files	Google Chrome	2024-06-18 10:01:45 BST	Win-7-Forensics1.vmdk
History				google.com	steganography in files	Google Chrome	2024-06-18 10:01:45 BST	Win-7-Forensics1.vmdk
History				google.com	how to use kali linux	Google Chrome	2024-06-18 11:47:27 BST	Win-7-Forensics1.vmdk
History				google.com	how to use kali linux	Google Chrome	2024-06-18 11:47:27 BST	Win-7-Forensics1.vmdk
History				google.com	how to use steganography to hide data	Google Chrome	2024-06-18 11:47:52 BST	Win-7-Forensics1.vmdk
History				google.com	how to use steganography to hide data	Google Chrome	2024-06-18 11:47:52 BST	Win-7-Forensics1.vmdk

Figure 5: Web Search

As shown in Figure 6, five email messages were recorded.

urce Name	...	...	...	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)
00294823-00000001.eml				research@shadowfall.non;	itsupport@shadowfall.non;	TEST	2024-06-18 10:54:46 BST	TEST
2F3A249F-00000001.eml				itsupport@shadowfall.non;	research@shadowfall.non;	Re: TEST	2024-06-18 10:56:27 BST	REPLYOn 18/06/2024 10:54, Research
67844AE1-00000002.eml				research@shadowfall.non;	alpha@other.non;	Just checking in	2024-06-18 11:07:01 BST	Expect a follow up soon.
00294823-00000001.eml				sales@shadowfall.non;	itsupport@shadowfall.non;	TEST	2024-06-18 11:34:52 BST	TEST
67844AE1-00000002.eml				sales@shadowfall.non;	alpha@other.non;	A cute kitten	2024-06-18 11:48:35 BST	Heres something you'll like

Figure 6: Email Communication

The most recently opened documents were kitten.lnk at 11:50:20 BST and New Rich Text Document.rtf at 11:50:54 BST, by "Sales."

Recent Documents

Table Thumbnail Summary

Save T

Source Name	S	C	O	Path	Date Accessed	Data Source
New Rich Text Document.lnk				C:\Users\Sales\Desktop\New Rich Text Document.rtf	2024-06-18 11:50:54 BST	Win-7-Forensics1.vmdk
kitten.lnk				C:\Users\Sales\Documents\kitten.jpg	2024-06-18 11:50:20 BST	Win-7-Forensics1.vmdk
No preferred path found.lnk				No preferred path found	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Pictures.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Win...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Videos.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Win...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Music.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Win...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Documents.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Win...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Pictures.library-ms.lnk				C:\Users\Sales\AppData\Roaming\Microsoft\Window...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Videos.library-ms.lnk				C:\Users\Sales\AppData\Roaming\Microsoft\Window...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk

Figure 7: Recent Documents

5.2 Memory Analysis

The memory capture was analysed using the Volatility Framework to access system processes and user activity. Figure 8 shows the image was identified as a Windows 7(Win7SP0x64) memory capture.

```
C:\Users\networkuser\Desktop>C:\Users\networkuser\Desktop\volatility-master\vol.py -f C:\Users\networkuser\Desktop\
memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23
418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\networkuser\Desktop\memdump.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c3a070L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80002c3bd00L
                KPCR for CPU 1 : 0xfffff880009ee000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2024-06-18 10:52:29 UTC+0000
     Image local date and time : 2024-06-18 11:52:29 +0100
```

Figure 8: Imageinfo.

The system booted at 11:14:29 BST, with core processes starting as expected. WUDFHost.exe executed at 11:24:45 BST, enabling communication with plug-and-play devices, indicating a connected device (Figure 9). At 11:29:59 BST, user activity became evident with processes like explorer.exe and wlmail.exe for email activity.

```
Name                                                  Pid   PPid   Thds   Hnds Time
---------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa801a6d6580:wininit.exe                        456    336      3     79 2024-06-18 10:14:30 UTC+0000
. 0xfffffa801a79f880:lsm.exe                           584    456     10    141 2024-06-18 10:14:30 UTC+0000
. 0xfffffa801a740b30:services.exe                      560    456      8    216 2024-06-18 10:14:30 UTC+0000
.. 0xfffffa801a8b58e0:svchost.exe                      960    560     35   1305 2024-06-18 10:14:30 UTC+0000
.. 0xfffffa801a83f630:svchost.exe                      788    560      8    276 2024-06-18 10:14:30 UTC+0000
.. 0xfffffa801b07a060:svchost.exe                      536    560     13    146 2024-06-18 10:16:32 UTC+0000
.. 0xfffffa801aa27920:spoolsv.exe                     1160    560     12    272 2024-06-18 10:14:31 UTC+0000
.. 0xfffffa801a991060:svchost.exe                     1052    560     17    416 2024-06-18 10:14:31 UTC+0000
.. 0xfffffa801a89f2d0:svchost.exe                      928    560     13    353 2024-06-18 10:14:30 UTC+0000
... 0xfffffa801af171b0:dwm.exe                        2872    928      5    130 2024-06-18 10:29:59 UTC+0000
... 0xfffffa80197d6b30:WUDFHost.exe                   2428    928      8    226 2024-06-18 10:24:45 UTC+0000
.. 0xfffffa801aa72b30:svchost.exe                     1192    560     18    315 2024-06-18 10:14:31 UTC+0000
.. 0xfffffa8018d751c0:svchost.exe                      924    560      9    320 2024-06-18 10:16:32 UTC+0000
.. 0xfffffa801a805b30:svchost.exe                      688    560      9    358 2024-06-18 10:14:30 UTC+0000
... 0xfffffa801986c2f0:dllhost.exe                    2120    688      8    205 2024-06-18 10:50:20 UTC+0000
... 0xfffffa801aebc910:WmiPrvSE.exe                   2220    688      9    197 2024-06-18 10:14:35 UTC+0000
... 0xfffffa80199ceb30:wlcomm.exe                     2664    688      7    183 2024-06-18 10:30:37 UTC+0000
.. 0xfffffa801ab66630:WLIDSVC.EXE                     1468    560      8    230 2024-06-18 10:14:31 UTC+0000
... 0xfffffa801ac0e6d0:WLIDSVCM.EXE                   1536   1468      4     53 2024-06-18 10:14:31 UTC+0000
.. 0xfffffa801ab5ab30:vmtoolsd.exe                    1440    560      9    298 2024-06-18 10:14:31 UTC+0000
```

Figure 9: Process Analysis (pstree)

Chrome.exe executed at 11:46:56 BST, initiating web activity. Cmd.exe executed Telnet.exe at 11:49 BST, confirmed by cmdscan and network logs, verifying a remote connection (Figure 10).

```
**************************************************
CommandProcess: conhost.exe Pid: 3452
CommandHistory: 0x4410d0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xc
Cmd #0 @ 0x43d650: telnet
Cmd #15 @ 0x3f0158: D
Cmd #16 @ 0x440240: D
**************************************************
CommandProcess: conhost.exe Pid: 3452
CommandHistory: 0x441380 Application: telnet.exe Flags: Allocated, Reset
CommandCount: 4 LastAdded: 3 LastDisplayed: 3
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x54
Cmd #0 @ 0x4171d0: 192.168.101.129
Cmd #1 @ 0x43d690: open
Cmd #2 @ 0x435660: 192.168.101.129
Cmd #3 @ 0x440400: y
```

Figure 10: Command Prompt History

The presence of FTK Imager.exe and FTK Imager.lnk file suggests forensic activity. Iehistory shows file access to kitten.jpg and New Rich Text Document.rtf. Clipboard data extracted from memory contained text related to rockets, which matched hidden content inside kitten.jpg, confirming data concealment (Figure 11,Figure 16).

```
Session    WindowStation Format                          Handle Object             Data
---------- ------------- ------------------ ------------------ ------------------ ---------------------------------
----------------
         1 WinSta0       CF_UNICODETEXT                0x90297 0xfffff900c24e2350 Phase 4: Testing and Lau... and
data transmission.
         1 WinSta0       CF_TEXT                         0x10 ------------------
         1 WinSta0       0xe0121L               0x200000000000 ------------------
         1 WinSta0       CF_TEXT                          0x1 ------------------
         1 ------------- ------------------            0xe0121 0xfffff900c2405fe0
```

Figure 11: Clipboard History

5.3 Network Analysis

The system's network activity was analysed using Wireshark to identify recent activity, websites visited, and data transmissions. A high volume of network traffic was recorded between 11:47 and 11:49 BST on June 18, 2024. The key activities were email communication, web browsing, and a Telnet connection.

The logs confirmed that the system accessed multiple Google services including Google search, YouTube, Play Store, APIs, and authentication servers. Also, visits were made to cybersecurity training sites; tutorialspoint.com and freecodecamp.org, and an academic research site, jems.springeropen.com. These align with web search findings from the VM disk analysis.

At 11:48:35 BST, an email was sent from sales@shadowfall.non to alpha@other.non with an attachment named "kitten.jpg." Shortly afterward, at 11:49:18 BST, a Telnet session was initiated from 192.168.101.129 to 192.168.101.128.

No.	Time	Source	Destination	Protocol	Length	Info
19	2024-06-18 11:46:55.433356	192.168.101.128	192.168.101.2	NBNS	110	Refresh NB WORKGROUP<00>
20	2024-06-18 11:46:56.946475	192.168.101.128	192.168.101.2	NBNS	110	Refresh NB WORKGROUP<00>
21	2024-06-18 11:46:57.441646	192.168.101.128	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
22	2024-06-18 11:46:57.449338	192.168.101.128	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc0e17c46
23	2024-06-18 11:46:57.449446	192.168.101.254	192.168.101.128	DHCP	342	DHCP ACK - Transaction ID 0xc0e17c46
24	2024-06-18 11:46:57.777040	192.168.101.128	192.168.101.2	DNS	76	Standard query 0xe877 A wpad.localdomain
25	2024-06-18 11:46:57.786496	192.168.101.128	192.168.101.2	DNS	76	Standard query 0x7f4c A wpad.localdomain
26	2024-06-18 11:46:57.786496	192.168.101.128	192.168.101.2	DNS	76	Standard query 0x6460 A wpad.localdomain
27	2024-06-18 11:46:58.447323	192.168.101.128	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
28	2024-06-18 11:46:58.705718	192.168.101.128	192.168.101.2	DNS	79	Standard query 0x445d A clients2.google.com
29	2024-06-18 11:46:58.705903	192.168.101.128	192.168.101.2	DNS	79	Standard query 0x9810 HTTPS clients2.google.com
30	2024-06-18 11:46:58.706223	192.168.101.128	192.168.101.2	DNS	79	Standard query 0x35c6 A accounts.google.com
31	2024-06-18 11:46:58.706398	192.168.101.128	192.168.101.2	DNS	79	Standard query 0xa79e HTTPS accounts.google.com
32	2024-06-18 11:46:58.733447	192.168.101.2	192.168.101.128	DNS	95	Standard query response 0x35c6 A accounts.google.com A 64.233.166.84
33	2024-06-18 11:46:58.734018	192.168.101.128	192.168.101.2	DNS	89	Standard query 0x6bd0 A clientservices.googleapis.com
34	2024-06-18 11:46:58.734167	192.168.101.128	192.168.101.2	DNS	89	Standard query 0x1a2a HTTPS clientservices.googleapis.com
35	2024-06-18 11:46:58.734427	192.168.101.2	192.168.101.128	DNS	105	Standard query response 0x6bd0 A clientservices.googleapis.com A 172.217.16.227
36	2024-06-18 11:46:58.738733	192.168.101.2	192.168.101.128	DNS	119	Standard query response 0x445d A clients2.google.com CNAME clients.l.google.com
37	2024-06-18 11:46:58.739108	192.168.101.2	192.168.101.128	DNS	129	Standard query response 0xa79e HTTPS accounts.google.com SOA ns1.google.com
38	2024-06-18 11:46:58.739860	192.168.101.128	64.233.166.84	TCP	66	49196 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
39	2024-06-18 11:46:58.740058	192.168.101.128	172.217.16.227	TCP	66	49197 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
40	2024-06-18 11:46:58.741263	192.168.101.2	192.168.101.128	DNS	153	Standard query response 0x9810 HTTPS clients2.google.com CNAME clients.l.google
41	2024-06-18 11:46:58.741566	192.168.101.128	142.250.200.14	TCP	66	49198 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
42	2024-06-18 11:46:58.764768	172.217.16.227	192.168.101.128	TCP	60	443 → 49197 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
43	2024-06-18 11:46:58.764798	192.168.101.128	172.217.16.227	TCP	54	49197 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
44	2024-06-18 11:46:58.765396	192.168.101.128	172.217.16.227	TLSv1.3	571	Client Hello (SNI=clientservices.googleapis.com)
45	2024-06-18 11:46:58.765603	172.217.16.227	192.168.101.128	TCP	60	443 → 49197 [ACK] Seq=1 Ack=518 Win=64240 Len=0
46	2024-06-18 11:46:58.766022	142.250.200.14	192.168.101.128	TCP	60	443 → 49198 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
47	2024-06-18 11:46:58.766033	192.168.101.128	142.250.200.14	TCP	54	49198 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
48	2024-06-18 11:46:58.766406	192.168.101.128	142.250.200.14	TLSv1.3	571	Client Hello (SNI=clients2.google.com)
49	2024-06-18 11:46:58.766472	142.250.200.14	192.168.101.128	TCP	60	443 → 49198 [ACK] Seq=1 Ack=518 Win=64240 Len=0
50	2024-06-18 11:46:58.770241	64.233.166.84	192.168.101.128	TCP	60	443 → 49196 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
51	2024-06-18 11:46:58.770270	192.168.101.128	64.233.166.84	TCP	54	49196 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
52	2024-06-18 11:46:58.770509	192.168.101.128	64.233.166.84	TLSv1.3	571	Client Hello (SNI=accounts.google.com)
53	2024-06-18 11:46:58.770555	64.233.166.84	192.168.101.128	TCP	60	443 → 49196 [ACK] Seq=1 Ack=518 Win=64240 Len=0
54	2024-06-18 11:46:58.776950	192.168.101.128	192.168.101.2	DNS	76	Standard query 0xe877 A wpad.localdomain
55	2024-06-18 11:46:58.786976	192.168.101.128	192.168.101.2	DNS	76	Standard query 0x7f4c A wpad.localdomain
56	2024-06-18 11:46:58.786988	192.168.101.128	192.168.101.2	DNS	76	Standard query 0x6460 A wpad.localdomain
57	2024-06-18 11:46:58.793196	192.168.101.2	192.168.101.128	DNS	146	Standard query response 0x1a2a HTTPS clientservices.googleapis.com SOA ns1.goog
58	2024-06-18 11:46:58.793225	192.168.101.128	192.168.101.2	ICMP	174	Destination unreachable (Port unreachable)
59	2024-06-18 11:46:58.797457	142.250.200.14	192.168.101.128	TLSv1.3	1466	Server Hello, Change Cipher Spec
60	2024-06-18 11:46:58.797564	142.250.200.14	192.168.101.128	TCP	1466	443 → 49198 [PSH, ACK] Seq=1413 Ack=518 Win=64240 Len=1412 [TCP segment of a rea
61	2024-06-18 11:46:58.797573	192.168.101.128	142.250.200.14	TCP	54	49198 → 443 [ACK] Seq=518 Ack=2825 Win=64240 Len=0
62	2024-06-18 11:46:58.797729	142.250.200.14	192.168.101.128	TCP	1466	443 → 49198 [PSH, ACK] Seq=2825 Ack=518 Win=64240 Len=1412 [TCP segment of a rea
63	2024-06-18 11:46:58.797800	142.250.200.14	192.168.101.128	TCP	1466	443 → 49198 [PSH, ACK] Seq=4237 Ack=518 Win=64240 Len=1412 [TCP segment of a rea
64	2024-06-18 11:46:58.797816	192.168.101.128	142.250.200.14	TCP	54	49198 → 443 [ACK] Seq=518 Ack=5649 Win=64240 Len=0
65	2024-06-18 11:46:58.797974	172.217.16.227	192.168.101.128	TLSv1.3	1466	Server Hello, Change Cipher Spec
66	2024-06-18 11:46:58.798086	172.217.16.227	192.168.101.128	TCP	1466	443 → 49197 [PSH, ACK] Seq=1413 Ack=518 Win=64240 Len=1412 [TCP segment of a rea
67	2024-06-18 11:46:58.798090	192.168.101.128	172.217.16.227	TCP	54	49197 → 443 [ACK] Seq=518 Ack=2825 Win=64240 Len=0
68	2024-06-18 11:46:58.798437	172.217.16.227	192.168.101.128	TCP	1466	443 → 49197 [PSH, ACK] Seq=2825 Ack=518 Win=64240 Len=1412 [TCP segment of a rea
69	2024-06-18 11:46:58.798498	172.217.16.227	192.168.101.128	TLSv1.3	678	Application Data

Figure 12: Network Traffic

6.0 Detail Analysis Findings

6.1 VM Disk Analysis

6.1.1 Connected Devices

The analysis shows multiple VMware virtual devices, such as virtual mice, and USB hubs. The only non-VMware device was a Kingston Technology Data Traveler 100 G2 (8 GiB), connected on June 18, 2024, at 11:24:43 BST. immediately before Research/Documents/kitten.jpg was created.

```
----------------------------------------
Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP,Tue Jun 18 10:24:43 2024,0018F30C9FE8EA81C00001EC&0,Tue Jun 18 10:24:43
2024,Kingston DT 100 G2 USB Device,
----------------------------------------
wpdbusenum v.20141111
(System) Get WpdBusEnumRoot subkey info

DISK&VEN_KINGSTON&PROD_DT_100_G2&REV_PMAP (0018F30C9FE8EA81C00001EC&0)
  LastWrite: Tue Jun 18 10:24:45 2024
  DeviceDesc: DT 100 G2
  Friendly: UNTITLED
  Mfg: Kingston
  Device Parameters LastWrite: [Tue Jun 18 10:24:45 2024]
  LogConf LastWrite          : [Tue Jun 18 10:24:45 2024]
  Properties LastWrite       : [Tue Jun 18 10:24:45 2024]
  InstallDate     : Tue Jun 18 10:24:45 2024 UTC
  FirstInstallDate: Tue Jun 18 10:24:45 2024 UTC

ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
DISK&VEN_KINGSTON&PROD_DT_100_G2&REV_PMAP\0018F30C9FE8EA81C00001EC&0
LastWrite: Tue Jun 18 10:24:45 2024

----------------------------------------
```

Figure 13: Kingston USB

6.1.2 Browser Activity

Google Chrome was the preferred browser, with cookies and browsing history linked to the Sales user. Cookies from google.com and youtube.com last accessed on June 18, 2024, indicate web interaction. Seven unique extensions, including Chrome PDF Viewer, Google Docs Offline, and Chrome Web Store Payments, indicated no unusual activity (Figure 36). Figure 14 shows 20 favicon entries recorded, including https://www.kali.org/docs/installation/hard-disk-install/, https://www.freecodecamp.org/news/what-is-steganography-hide-data-inside-data/, and https://www.tutorialspoint.com/kali_linux/index.htm, related to the search queries.

Suspicious searches on June 18, 2024, included:

- "How to install kali linux" (10:01:06 BST)
- "Steganography in files" (10:01:45 BST)
- "How to use kali linux" (11:47:27 BST)
- "How to use steganography to hide data" (11:47:52 BST).

These searches indicate an interest in using Kali Linux and steganography, outside the Finance Director's role.

Favicon

Table Thumbnail Summary

Save Table

URL	Date Modified	Domain	Program Name
https://google.com/	2024-06-18 10:00:57 BST	google.com	Google Chrome
https://www.google.com/	2024-06-18 10:00:57 BST	google.com	Google Chrome
https://www.google.com/	2024-06-18 10:00:57 BST	google.com	Google Chrome
https://www.kali.org/docs/installation/hard-disk-install/	2024-06-18 10:01:10 BST	kali.org	Google Chrome
https://www.kali.org/docs/installation/hard-disk-install/	2024-06-18 10:01:10 BST	kali.org	Google Chrome
https://www.google.com/search?q=steganography+in+files&oq=how+to+stegnography...	2024-06-18 10:00:57 BST	google.com	Google Chrome
https://www.google.com/search?q=steganography+in+files&oq=how+to+stegnography...	2024-06-18 10:00:57 BST	google.com	Google Chrome
https://www.freecodecamp.org/news/what-is-steganography-hide-data-inside-data/	2024-06-18 10:01:57 BST	freecodecamp.org	Google Chrome
https://www.freecodecamp.org/news/what-is-steganography-hide-data-inside-data/	2024-06-18 10:01:57 BST	freecodecamp.org	Google Chrome
https://google.com/	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://google.com/	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://www.google.com/	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://www.google.com/	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://www.google.com/search?q=how+to+use+kali+linux&sca_esv=e700f3d169f8483...	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://www.google.com/search?q=how+to+use+kali+linux&sca_esv=e700f3d169f8483...	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://www.tutorialspoint.com/kali_linux/index.htm	2024-06-18 11:47:33 BST	tutorialspoint.com	Google Chrome
https://www.tutorialspoint.com/kali_linux/index.htm	2024-06-18 11:47:33 BST	tutorialspoint.com	Google Chrome
https://www.google.com/search?q=how+to+use+steganography+to+hide+data&sca_es...	2024-06-18 11:47:19 BST	google.com	Google Chrome
https://www.google.com/search?q=how+to+use+steganography+to+hide+data&sca_es...	2024-06-18 11:47:19 BST	google.com	Google Chrome

Figure 14: Favicon.

6.1.3 Email Analysis

Email analysis found senders within the domain shadowfall.non, including research@shadowfall.non, itsupport@shadowfall.non, and sales@shadowfall.non. On June 18, 2024, Research and Sales users sent emails externally to alpha@other.non. Research's email was titled *"Just checking in" with* no attachment. The email sent by Sales had subject "A cute kitten" with body text "Here's something you'll like" and a kitten.jpg attachment (Figure 15).

Figure 15: Email titled "A cute kitten".

6.1.4 File Analysis and Deleted Files

Further analysis identified the presence of "kitten.jpg" in multiple locations, including the Sales and Research users' Documents folder and the Sent Items folder of Windows Live Mail. An inspection of the image text revealed that it contained embedded text related to rockets construction (Figure 16).

Strings Extracted Text Translation

Page: 11 of 11 Page Go to Page: 11 Script: Latin - Basic

L]`p
- EZ
-39gp
>B8sa
6a#X
$t'u·
Phase 1: Gather Materials. Acquire aluminum sheets, copper wiring, and titanium rods. Secure propulsion system components, including rocket fuel and combustion chambers.
Phase 2: Design Blueprints. Collaborate with aerospace engineers to create detailed schematics for the rocket. Ensure the design includes a reinforced frame, aerodynamic nose cone, and stable fins.
Phase 3: Construction. Assemble the rocket's frame using welding techniques to ensure structural integrity. Install the propulsion system and electrical wiring. Conduct preliminary tests on fuel systems and control mechanisms.
Phase 4: Testing and Launch. Perform a series of ground tests to validate the rocket's stability and performance. Schedule a launch window and coordinate with relevant authorities for airspace clearance. Conduct the final launch sequence and monitor the rocket's trajectory and data transmission.

Figure 16: Hidden text found in Autopsy.

kitten.jpg found in Sales/Documents was modified at 11:23:26 BST. It was then accessed at 11:36:07 BST by the Sales user. At 11:50:20 BST, it was changed again, which coincides with the creation of kitten.lnk, a shortcut. The Research version of the file was created at 11:24:51 BST, just after the USB device was connected. Both files contain the same embedded rocket-related text.

kitten 4 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	Conf...	Score	File Path	Modified Time	Accessed Time	Size	MD5 Hash
kitten.lnk	kitten	Likely Notable	/img_Win-7-Forensics1.vmdk/vol_vol3/Users/Sales/AppData/Roaming/Microsoft/Windows/Rece...	2024-06-18 11:50:20 BST	2024-06-18 11:50:20 BST	2297	908243068ce0
kitten.jpg	kitten	Likely Notable	/img_Win-7-Forensics1.vmdk/vol_vol3/Users/Sales/AppData/Local/Microsoft/Windows Live Mail...	0000-00-00 00:00:00	0000-00-00 00:00:00	177357	d9ea3197ff925
kitten.jpg	kitten	Likely Notable	/img_Win-7-Forensics1.vmdk/vol_vol3/Users/Research/Documents/kitten.jpg	2024-06-18 11:23:26 BST	2024-06-18 11:24:51 BST	177357	d9ea3197ff925
kitten.jpg	kitten	Likely Notable	/img_Win-7-Forensics1.vmdk/vol_vol3/Users/Sales/Documents/kitten.jpg	2024-06-18 11:23:26 BST	2024-06-18 11:36:07 BST	177357	d9ea3197ff925

Figure 17: Likely Notable-Kitten

Deleted files include New Rich Text Document.rtf from C:\Users\Sales\Desktop, deleted on 2024-06-18 11:51:13 BST, and the Test folder from C:\Users\Administrator\Desktop, deleted on 2024-06-17 14:55:39 BST. Both Sales and Administrator accounts were involved.

6.1.5 Desktop Items and Installed Software

Desktop items include Recycle Bin, AccessData FTK Imager.lnk (forensic tool) on the public desktop, Google Chrome.lnk on all desktops, and network.pcapng (packet capture file) on Sales' desktop (Figure 18). The Administrator's desktop also contained sdelete.exe (secure deletion tool) and the Test file.

```
itempos v.20130514
(NTUSER.DAT) Shell/Bags/1/Desktop ItemPos* value parsing; Win7 NTUSER.DAT hives

Software\Microsoft\Windows\Shell\Bags\1\Desktop
LastWrite: Tue Jun 18 11:01:35 2024

Value: ItemPos1834x1148x96(1)
Size       |Modified            |Accessed            |Created             |Name
----------|--------------------|--------------------|--------------------|----------
           |                    |                    |                    |Recycle Bin
1992       |2024-06-12 21:23:28 |2024-06-17 11:47:08 |2024-06-17 11:47:08 |AccessData FTK Imager.lnk
2171       |2024-06-18 10:47:06 |2024-06-18 10:30:10 |2024-06-18 10:30:10 |Google Chrome.lnk
9324976    |2024-06-18 10:50:06 |2024-06-18 10:50:06 |2024-06-18 10:50:06 |network.pcapng
```

Figure 18: Sales Desktop

A total of 136 installed programs were identified. Recent installations on June 12, 2024, include AccessData FTK Imager, Wireshark (2.2.17), and WinPcap (4.1.3), indicating forensic or network analysis (Figure 19). Older Software, installed in 2022 includes SumatraPDF, Notepad++, PeaZip, and VMware Tools.

```
Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Wed Jun 12 21:51:56 2024 (UTC)
  Wireshark 2.2.17 (64-bit) v.2.2.17

Wed Jun 12 21:51:53 2024 (UTC)
  WinPcap 4.1.3 v.4.1.0.2980

Wed Jun 12 21:51:42 2024 (UTC)
  Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215 v.14.0.24215.1

Wed Jun 12 21:47:11 2024 (UTC)
  Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 v.12.0.30501.0

Wed Jun 12 21:22:33 2024 (UTC)
  Windows Live Mail v.16.4.3528.0331

Wed Jun 12 21:22:32 2024 (UTC)
  Windows Live Essentials v.16.4.3528.0331
  Windows Live Writer Resources v.16.4.3528.0331
  Photo Common v.16.4.3528.0331
  Windows Live Essentials v.16.4.3528.0331

Wed Jun 12 21:22:31 2024 (UTC)
  Windows Live Photo Common v.16.4.3528.0331
  Windows Live UX Platform Language Pack v.16.4.3528.0331

Wed Jun 12 21:22:30 2024 (UTC)
  Windows Live Writer v.16.4.3528.0331

Wed Jun 12 21:22:15 2024 (UTC)
  Windows Live Mail v.16.4.3528.0331
```

Figure 19: Installed Programs

6.2 Memory Analysis

6.2.1 System Activity

The memory analysis confirmed key system activities, aligning with the findings from the VM disk analysis. The system booted at 11:14:29 BST and initialized core processes. GoogleCrashHandler.exe started at 11:14:45 BST, indicating Google-related software on the system. User login began at 11:29:52 BST, with csrss.exe and winlogon.exe, followed by explorer.exe at 11:29:59 BST, enabling graphical user interactions.

```
Process: 2188 vmtoolsd.exe 2024-06-18 10:30:10 UTC+0000
Process: 1744 wlmail.exe 2024-06-18 10:30:27 UTC+0000
Process: 2664 wlcomm.exe 2024-06-18 10:30:37 UTC+0000
Process: 1176 chrome.exe 2024-06-18 10:46:56 UTC+0000
Process: 3724 taskhost.exe 2024-06-18 10:47:05 UTC+0000
Process: 3524 cmd.exe 2024-06-18 10:49:04 UTC+0000
Process: 3452 conhost.exe 2024-06-18 10:49:04 UTC+0000
Process: 3976 telnet.exe 2024-06-18 10:49:06 UTC+0000
Process: 2120 dllhost.exe 2024-06-18 10:50:20 UTC+0000
Process: 3376 notepad.exe 2024-06-18 10:51:19 UTC+0000
Process: 2968 FTK Imager.exe 2024-06-18 10:52:03 UTC+0000
```

Figure 20: Sessions - RAM Analysis

At 11:24:45 BST, WUDFHost.exe executed indicating a plug and play device has been connected to the system, aligning with the Kingston USB connection identified in disk analysis. Windows Live Mail activity began at 11:30:27 BST, with wlmail.exe launching, followed by wlcomm.exe at 11:30:37 BST. Chrome.exe executed at 11:46:56 BST, establishing a connection to Google's IP (142.250.200.14), confirming web activity.

6.2.2 Network and Email Activity.

Network analysis with netscan identified connections, showing processes like wlmail.exe, svchost.exe, lsass.exe, and services.exe managing various TCP and UDP connections. Wlmail.exe had a TCP connection to 192.168.101.129:143, indicating IMAP-based email activity. Windows system logs captured "Sending email using 'Shadowfall (sales)'" and "Moving message 1 of 1...", verifying an email transmission (Figure 21). The WinTree output revealed CLIPBRDWNDCLASS under wlmail.exe, confirming clipboard activity involving email content or attachments.

```
Window Handle: #201be at 0xfffff900c101dc40, Name: Moving message 1 of 1...
ClassAtom: 0xc051, Class: 6.0.7600.16385!Static
SuperClassAtom: 0xc019, SuperClass: Static
pti: 0xfffff900c2fd8c30, Tid: 2716 at 0xfffffa8019b0aa60
ppi: 0xfffff900c01a4ce0, Process: wlmail.exe, Pid: 1744
Visible: No
Left: 744, Top: 433, Bottom: 1062, Right: 448
Style Flags: WS_MINIMIZEBOX,WS_CHILD,WS_DISABLED,WS_GROUP,WS_OVERLAPPED
ExStyle Flags: WS_EX_LTRREADING,WS_EX_RIGHTSCROLLBAR,WS_EX_LEFT,WS_EX_NOPARENTNOTIFY
Window procedure: 0x74f477cd

Window Handle: #201d0 at 0xfffff900c1019540, Name: Sending email using 'Shadowfall (sales)'...
ClassAtom: 0xc051, Class: 6.0.7600.16385!Static
SuperClassAtom: 0xc019, SuperClass: Static
pti: 0xfffff900c2fd8c30, Tid: 2716 at 0xfffffa8019b0aa60
ppi: 0xfffff900c01a4ce0, Process: wlmail.exe, Pid: 1744
Visible: No
Left: 744, Top: 392, Bottom: 1062, Right: 428
Style Flags: WS_MINIMIZEBOX,WS_CHILD,WS_DISABLED,WS_GROUP,WS_OVERLAPPED
ExStyle Flags: WS_EX_LTRREADING,WS_EX_RIGHTSCROLLBAR,WS_EX_LEFT,WS_EX_NOPARENTNOTIFY
Window procedure: 0x74f477cd
```

Figure 21: Windows logs - RAM Analysis

A Telnet session was executed between 192.168.101.129 and 192.168.101.128. The initial NTLM authentication failed but a manual login was successful. The command history and pstree showed that Telnet was launched from cmd.exe at 11:49:06 BST.

6.2.3 File Access

Windows Photo Viewer, executed under dllhost.exe (PID 2120), accessed kitten.jpg at 11:50:20 BST from C:/Users/Sales/Documents/. This aligns with the VM disk findings. Also, New Rich Text Document.rtf was accessed and deleted at 11:50:54 BST, further indicating potential data manipulation (Figure 22).

```
timeliner.txt - Notepad
File  Edit  Format  View  Help
2024-06-18 10:52:29 UTC+0000|[LIVE RESPONSE]| (System time)|
2024-06-18 10:50:20 UTC+0000|[IEHISTORY]| explorer.exe->Visited: Sales@file:///C:/Users/Sales/Documents/kitten.jpg| PID: 2756/Cache type "URL " at 0x40b5000 End: 2024-06-18 10
2024-06-18 10:50:54 UTC+0000|[IEHISTORY]| explorer.exe->Visited: Sales@file:///C:/Users/Sales/Desktop/New%20Rich%20Text%20Document.rtf| PID: 2756/Cache type "URL " at 0x40b510
2024-06-18 11:50:20 UTC+0000|[IEHISTORY]| explorer.exe->:2024061820240619: Sales@file:///C:/Users/Sales/Documents/kitten.jpg| PID: 2756/Cache type "URL " at 0x40e5000 End: 202
2024-06-18 11:50:20 UTC+0000|[IEHISTORY]| explorer.exe->:2024061820240619: Sales@:Host: Computer| PID: 2756/Cache type "URL " at 0x40e5100 End: 2024-06-18 10:50:20 UTC+0000
2024-06-18 11:50:54 UTC+0000|[IEHISTORY]| explorer.exe->:2024061820240619: Sales@file:///C:/Users/Sales/Desktop/New%20Rich%20Text%20Document.rtf| PID: 2756/Cache type "URL " a
2024-06-18 10:14:30 UTC+0000|[PROCESS]| wininit.exe| PID: 456/PPID: 336/POffset: 0x7e4d6580
2009-07-14 04:49:01 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2024-06-17 14:41:11 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2024-06-18 10:14:30 UTC+0000|[Handle (Key)]| MACHINE| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2022-05-18 19:50:27 UTC+0000|[Handle (Key)]| USER\.DEFAULT\CONTROL PANEL\INTERNATIONAL| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2022-05-18 19:50:27 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2009-07-14 04:49:01 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE\ALTERNATE SORTS| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2009-07-14 04:49:01 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2024-06-18 10:14:30 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2009-07-14 04:53:31 UTC+0000|[Handle (Key)]| USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2024-06-13 13:34:24 UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\APPCOMPATFLAGS| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2022-05-18 12:42:41 UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6
2024-06-12 19:13:29 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2024-06-12 21:21:48 UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5| wininit.exe PID: 456/PPID: 336/POffset: 0x7e4d6580
2009-07-13 23:52:36 UTC+0000|[PE HEADER (exe)]| wininit.exe| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0xff800000
-|[PE DEBUG]| wininit.exe| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0xff800000
1970-01-01 00:00:00 UTC+0000|[DLL LOADTIME (exe)]| wininit.exe| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0xff800000
2009-07-14 01:32:27 UTC+0000|[PE HEADER (dll)]| ntdll.dll| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0x77a10000
2009-07-13 23:22:00 UTC+0000|[PE DEBUG]| ntdll.dll| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0x77a10000
1970-01-01 00:00:00 UTC+0000|[DLL LOADTIME (dll)]| ntdll.dll| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0x77a10000
2009-07-14 01:31:11 UTC+0000|[PE HEADER (dll)]| kernel32.dll| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0x77670000
-|[PE DEBUG]| kernel32.dll| Process: wininit.exe/PID: 456/PPID: 336/Process POffset: 0x7e4d6580/DLL Base: 0x77670000
```

Figure 22: Timeliner - RAM Analysis

FTK Imager.exe execution at 11:52:03 BST confirms forensic tool usage. Clipboard history contained fragments of rocket-related text, which matched the embedded content within "kitten.jpg." This confirms that the user copied the text before embedding it within the image file.

These findings confirm that kitten.jpg was accessed and transmitted externally within a short period. The combination of USB activity, email transmission, and clipboard evidence, provides proof of potential unauthorized data transfer.

6.3 Network Analysis

6.3.1 Recent Network Activity

At 11:47:01 BST, a device with IP 192.168.101.128 accessed www.google.com, initiating Google-related activity. Shortly after, it loaded media content from YouTube and related services, requesting i.ytimg.com and www.youtube.com. The system also connected to Google APIs (jnn-pa.googleapis.com) and ad-related services, including adservice.google.com.

The system accessed technical learning sites TutorialsPoint (www.tutorialspoint.com) at 11:47:32 BST and FreeCodeCamp (www.freecodecamp.org) at 11:48:05 BST. Google services continued at 11:47:57 BST with a TLS 1.3 connection to update.googleapis.com, likely an automatic update for Google software. At the same time, the system accessed SpringerOpen (joems.springeropen.com), a research database. At 11:48:06 BST, it downloaded a Chrome extension update (Figure 23), likely an automatic background process.

http

	Time	Source	Destination	Protocol	Length	Info
84	2024-06-18 11:46:59.256741	192.168.101.128	34.104.35.123	HTTP	456	GET /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJ
27	2024-06-18 11:46:59.397325	34.104.35.123	192.168.101.128	HTTP	1154	HTTP/1.1 200 OK (application/x-chrome-extension)
99	2024-06-18 11:48:06.753353	192.168.101.128	34.104.35.123	HTTP	339	HEAD /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9.49.1/gcmjkmgdlgnkkco
02	2024-06-18 11:48:06.780294	34.104.35.123	192.168.101.128	HTTP	605	HTTP/1.1 200 OK
03	2024-06-18 11:48:06.785173	192.168.101.128	34.104.35.123	HTTP	411	GET /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9.49.1/gcmjkmgdlgnkkcoc
29	2024-06-18 11:48:06.814689	34.104.35.123	192.168.101.128	HTTP	479	HTTP/1.1 206 Partial Content
52	2024-06-18 11:48:10.220543	192.168.101.128	34.104.35.123	HTTP	414	GET /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9.49.1/gcmjkmgdlgnkkcoc
56	2024-06-18 11:48:10.250394	34.104.35.123	192.168.101.128	HTTP	443	HTTP/1.1 206 Partial Content
58	2024-06-18 11:48:11.437881	192.168.101.128	34.104.35.123	HTTP	415	GET /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9.49.1/gcmjkmgdlgnkkcoc
66	2024-06-18 11:48:11.467692	34.104.35.123	192.168.101.128	HTTP	658	HTTP/1.1 206 Partial Content
79	2024-06-18 11:48:12.523052	192.168.101.128	34.104.35.123	HTTP	416	GET /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9.49.1/gcmjkmgdlgnkkcoc
93	2024-06-18 11:48:12.560687	34.104.35.123	192.168.101.128	HTTP	1371	HTTP/1.1 206 Partial Content
11	2024-06-18 11:48:13.569730	192.168.101.128	34.104.35.123	HTTP	416	GET /edgedl/release2/chrome_component/ad3rm3ciqs3fjr4bc4x5vwuildeq_9.49.1/gcmjkmgdlgnkkcoc
25	2024-06-18 11:48:13.604247	34.104.35.123	192.168.101.128	HTTP	1025	HTTP/1.1 206 Partial Content

Figure 23: HTTP Traffic

6.3.2 Websites Visited

Network analysis confirmed that between 11:47 BST and 11:48 BST, the user searched on Google, then visited TutorialsPoint and FreeCodeCamp for technical learning. Springer Open was accessed for research, and YouTube was likely used for instructional content. Background activity indicated automated updates for Google services and Chrome components, indicating routine system maintenance. The network traffic showed significant encrypted communication, primarily through TLS 1.3, making content inspection difficult. However, the activity confirms secure data transmission practices.

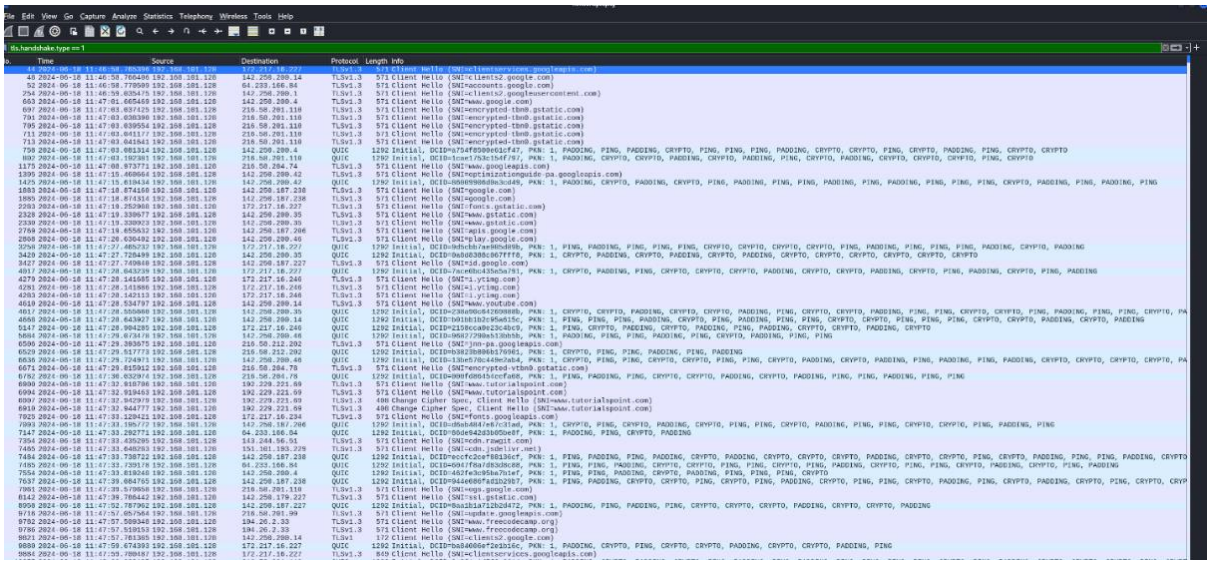

Figure 24: TLS Traffic-1

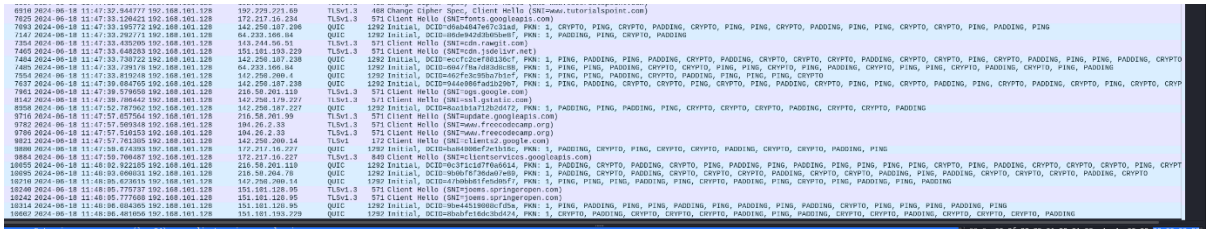

Figure 25: TLS Traffic-2

6.3.3 Data Sent/Received

At 11:48:35 BST, the system with IP 192.168.101.128 initiated an email session. The session was authenticated using sales@shadowfall.non, which was also the sender's email address. The recipient was alpha@other.non, and the email subject was "A Cute Kitten." The email body contained an HTML-formatted message stating, "Here’s something you’ll like." The message structure included multipart/mixed encoding, confirming an attachment. Figure 26 shows the email transmission details.

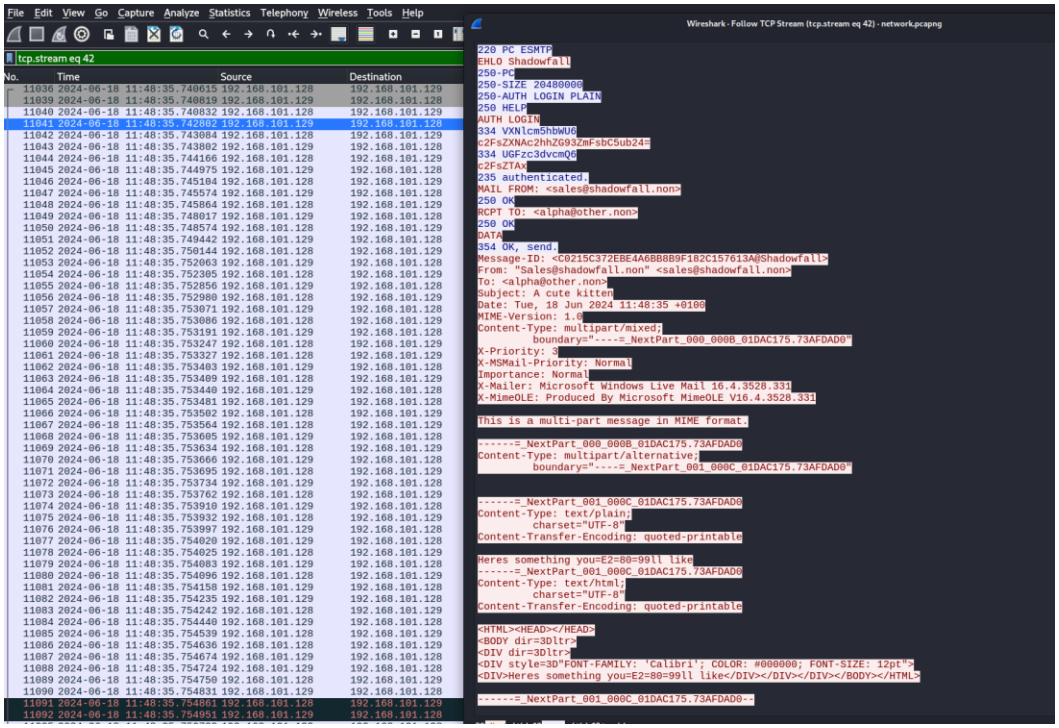

Figure 26: SMTP Traffic

The attachment, kitten.jpg, was transmitted externally as part of the email. Further analysis using Kali Linux's strings command revealed hidden text describing rocket construction phases (Figure 27). This aligns with findings from the VM disk analysis and clipboard history in memory analysis (Figure 11).

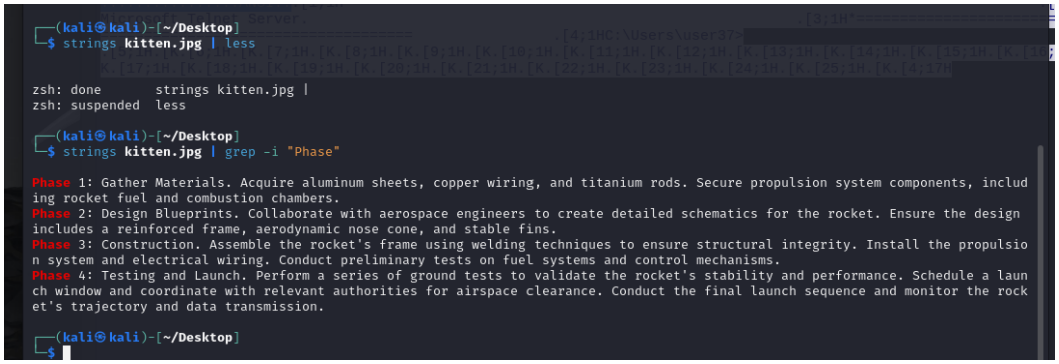

Figure 27: Hidden text found via kali.

Figure 28 confirms that an email with the subject "A Cute Kitten" from sales@shadowfall.non to alpha@other.non at 11:48:35 BST was successfully delivered and read.

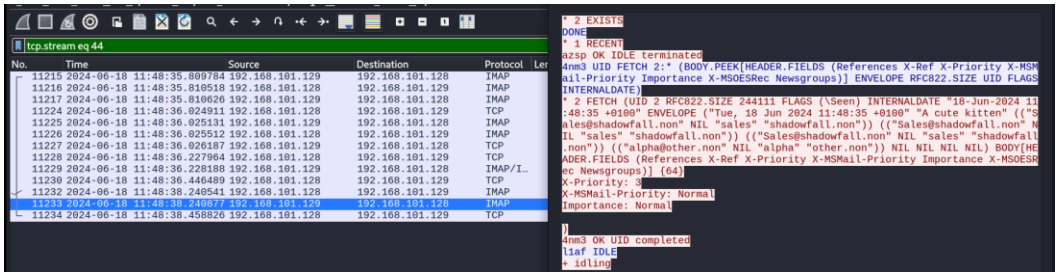

Figure 28: IMAP Traffic

At 11:49:18 BST, a Telnet session was initiated from the same system to 192.168.101.128. The first login attempt using Windows NTLM authentication failed, with the message: "Telnet server could not log you in using NTLM authentication. Your password may have expired." However, a manual login attempt followed, using the credentials uusseerr3377, which succeeded, granting access to a Windows command prompt (C:\Users\user37>). Figure 29 shows the Telnet session details. There were no data transfers or unauthorized access attempts via Telnet.

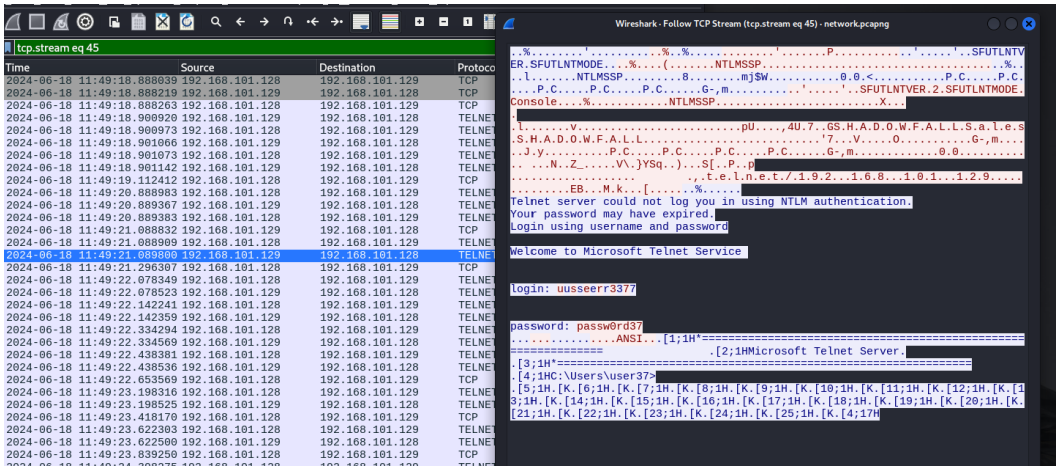

Figure 29: Telnet Traffic

The network activity shows a combination of routine system updates, technical research, and video content access. However, the email transmission with the kitten.jpg attachment with hidden text indicate potential data exfiltration.

7.0 Timeline of Events

Figure 30 show the timeline, outlining key activities related to the investigation, reconstructed from forensic analysis of the system's disk image, memory capture, and network traffic.

Time (BST)	Event Description	Source
18/05/2022 11:57:04	Created Administrator and Guest accounts	VM Disk Analysis(OS Accounts)
17/06/2024 12:44:37 - 13:13:05	Opened FTKImager_UserGuide.pdf, accessed three audio files, and opened USB network guide (.rtf). No user account linked.	VM Disk Analysis(Metadata)
17/06/2024 13:55:51 - 14:43:10	Admin accessed Recycle Bin, Google Chrome, FTK Imager(forensic tool), SDelete(secure file deletion tool), and User Accounts settings in Control Panel.	VM Disk Analysis(Shellbags)
17/06/2024 14:55:39	Deleted file named Test from Administrator's Desktop	VM Disk Analysis(Recycle Bin)
17/06/2024 15:43:23	Created Research account	VM Disk Analysis(OS Accounts)
18/06/2024 10:00:52	System set to open FTP, HTTP, and HTTPS links using Google Chrome for research account.	VM Disk Analysis(USRCLASS.DAT Registry)
18/06/2024 10:01:06	Performed a Google search for "how to install Kali Linux" via google.com, visited youtube.com, and accessed multiple Kali Linux setup images along with the "Installing Kali Linux" documentation. (No user account linked)	VM Disk Analysis(Web History, Web Cache, Web Search, Favicon)
18/06/2024 10:01:45	Performed a Google search for "steganography in files" via google.com, accessing gstatic.com and DV, SNID cookies (No user account linked)	VM Disk Analysis(Web History, Web Search, Web Cache, Cookies)
18/06/2024 10:01:50	Accessed "What is Steganography? How to Hide Data Inside Data" from freecodecamp.org	VM Disk Analysis(Web History, Web Cache, Favicon)
18/06/2024 10:27:56	Admin accessed User Accounts settings in Control Panel	VM Disk Analysis(Shellbags)
18/06/2024 10:54:46 - 11:07:01	Research account sent test email to IT support and another email ("Just checking in") to external address "alpha@other.non".	VM Disk Analysis(Metadata, Email)
18/06/2024 11:14:29	System booted, initializing core processes (System, wininit.exe, lsm.exe, smss.exe, services.exe).	RAM Analysis (Pstree, Psscan)
18/06/2024 11:14:42	Research account last login	VM Disk Analysis
18/06/2024 11:24:15	Research account modified the system's Documents Library structure	VM Disk Analysis(Shellbags)
18/06/2024 11:24:43	Kingston DataTraveler 100 G2 (8GB, Volume D drive) and Virtual USB Hub connected.	VM Disk Analysis(USB Connected)
18/06/2024 11:24:45	WUDFHost.exe executed, indicating a plug-and-play device connection (possibly linked to Kingston USB activity).	RAM Analysis (pstree, Psscan)
18/06/2024 11:24:47	Research account wrote to "My Computer" and D drive (Kingston USB)	VM Disk Analysis(Shellbags)
18/06/2024 11:24:51	"kitten.jpg" created in C:\Users\Research\Documents.	VM Disk Analysis(Likely Notable)
18/06/2024 11:27:54	Created Sales account.	VM Disk Analysis(OS Accounts)
18/06/2024 11:29:59	Sales account logged in.	VM Disk Analysis

Figure 30: Timeline of Events-1

Time (BST)	Event Description	Source
18/06/2024 11:30:27	Windows Live Mail (wlmail.exe) launched, followed by wlcomm.exe, confirming email activity.	RAM Analysis (Pstree, Psscan, Netscan)
18/06/2024 11:34:52	Email sent from Sales@shadowfall.non to itsupport@shadowfall.non with subject "TEST"(00294823-00000001.eml).	VM Disk Analysis(Metadata, Email)
18/06/2024 11:36:00	Sales account wrote to the D: drive via "My Computer," created "kitten.jpg" in C:\Users\Sales\Documents, and modified the system's Documents Library structure	VM Disk Analysis(Shellbags, Likely Notable)
18/06/2024 11:46:56	Google Chrome (Chrome.exe) launched , initiating web browsing for sales account with FTP, HTTP, and HTTPS links set to open.	RAM Analysis (Pstree) & VM Disk Analysis(USRCLASS.DAT Registry)
18/06/2024 11:47:19	Sales account Google search for 'how to use Kali Linux' and 'how to use steganography to hide data' , interacting with SNID cookie.	VM Disk Analysis(Web History, Web Search, Cookies, Favicon)
18/06/2024 11:47:28	Sales account accessed YouTube (youtube.com,i.ytimg.com), interacted with cookies (VISITOR_INFO1_LIVE, VISITOR_PRIVACY_METADATA), and triggered Google ads/tracking.	Network Analysis & VM Disk Analysis(Web Cache, Cookies)
18/06/2024 11:47:32	Sales account accessed Kali Linux tutorial via tutorialspoint.com	Network Analysis & VM Disk Analysis(Web Cache, Web Search, Favicon)
18/06/2024 11:47:53	Sales account performed a Google search for "how to use steganography to hide data," interacting with cookies (NID, DV) and ytimg.com.	VM Disk Analysis(Web History, Web Search, Web Cache, Cookies)
18/06/2024 11:48:05	Sales account accessed freecodecamp.org and "An efficient steganographic technique for hiding data" via joems.springeropen.com	Network Analysis & VM Disk Analysis(Web History, Web Cache)
18/06/2024 11:48:35	Email sent from sales@shadowfall.non to alpha@other.non with the subject "A cute kitten" and attachment "kitten.jpg" (67844AE1-00000002.eml). The attachment was found in the Windows Live Mail folder.	VM Disk Analysis(Metadata, Email, Likely Notable)
18/06/2024 11:48:35	Email sent from sales@shadowfall.non to alpha@other.non with kitten.jpg attachment	Network Analysis
18/06/2024 11:49:06	Telnet.exe was executed via Command prompt (cmd.exe)	RAM Analysis (Pstree, Netscan)
18/06/2024 11:49:18	Telnet login attempt failed, then manual login succeeded between IPs 192.168.101.129 → 192.168.101.128.	Network Analysis
18/06/2024 11:50:20	Kitten.jpg from C:\Users\Sales\Documents was opened via a shortcut (kitten.lnk) in Windows Photo Viewer (dllhost.exe), and "New Rich Text Document.rtf" from C:\Users\Sales\Desktop was accessed via a shortcut.	VM Disk Analysis (Recent Documents, Likely Notable) & RAM Analysis (Iehistory, Pstree, Wintree, Timeliner)
18/06/2024 11:51:13	New Rich Text Document.rtf deleted from C:\Users\Sales\Desktop.	VM Disk Analysis(Recycle Bin)
18/06/2024 11:52:03	Administrator account last login recorded.	VM Disk Analysis
18/06/2024 11:52:03	FTK Imager.exe executed, indicating forensic imaging activity.	RAM Analysis (Pstree, Psscan)
18/06/2024 12:01:35	Accessed Recycle Bin, sdelete.exe, Google Chrome.lnk, AccessData FTK Imager.lnk, network.pcapng	VM Disk Analysis(Shellbags)

Figure 31: Timeline of Events-2

8.0 Conclusions report to the CEO

The analysis indicates suspicious activity within ACME Ltd., involving potential unauthorized data access and distribution. The investigation strongly suggests that the Research and Sales user accounts engaged in activities outside their typical job responsibilities, specifically researching steganography and transferring an image file with hidden data via email.

The sequence of events began with web searches on Kali Linux and steganography, followed by the connection of a Kingston USB device. Shortly after, kitten.jpg appeared on the system under the Research account. This image, later found to contain hidden rocket-related text, appeared also under the Sales account and then emailed externally from “sales@shadowfall.non” to “alpha@other.non”. The web searches indicate intent and preparation. While no direct evidence of file transfer or steganography tools was found, access to Drive D (the USB) before the image's creation suggests a possible connection. Clipboard history confirmed that the hidden content within the image was accessed. A deleted rich text file, though unrecovered, raises possible concealment attempts.

Although Telnet was used, it occurred after the email was sent, ruling it out as a method for data exfiltration. The network and memory analysis corroborates the timeline, confirming the creation and transmission of the suspicious image file (kitten.jpg).

The user activity does not align with normal business operations, raising concerns about insider threat and possible data leakage. Given these risks, ACME Ltd. should review its security policies, enforce controls over USB usage, and enhance monitoring of communication channels. Immediate steps should include reviewing system access logs, interviewing involved personnel, and implementing data loss prevention (DLP) measures. Providing employee training on data security and compliance will also be critical in preventing similar incidents.

In summary, the combination of USB use, account behaviour, steganography indicators, and external email activity strongly suggests deliberate data concealment and unauthorized distribution, despite the exact method of embedding the data remains unclear.

9.0 References

Autopsy (2025) *Download*. Available at: https://www.autopsy.com/download/ (Accessed: 30 January 2025).

Firoj, M. (2025) 'How to install Volatility 2 and how to use it'. *Medium*. Available at: https://mahim-firoj.medium.com/how-to-install-volatility-2-and-how-to-use-it-8d7335e2c26c (Accessed: 18 March 2025).

Harris, I. (2025a) *CMM519 Incident Management and Forensics: Analysing Data and Reporting, Lecture 3*. [Lecture notes]. Available at: https://campusmoodle.rgu.ac.uk/course/view.php?id=109167 (Accessed: 4 February 2025).

Harris, I. (2025b) *CMM519 Incident Management and Forensics: Corroboration, Lecture 5*. [Lecture notes]. Available at: https://campusmoodle.rgu.ac.uk/course/view.php?id=109167 (Accessed: 25 February 2025).

Harris, I. (2025c) *CMM519 Incident Management and Forensics: Lab 9 – Steganography – Create and Detect*. [Lab instructions]. Available at: https://campusmoodle.rgu.ac.uk/course/view.php?id=109167 (Accessed: 25 March 2025).

Hendrix, B. (2022) *Learning Autopsy for Digital Forensics: Searching for Keywords and Files*. LinkedIn Learning. Available at: https://www.linkedin.com/learning/learning-autopsy-for-digital-forensics/searching-for-keywords-and-files (Accessed: 11 February 2025).

IANA (2025) *Port assignments*. Available at: https://campusmoodle.rgu.ac.uk/pluginfile.php/7200527/mod_resource/content/1/common_ports.pdf (Accessed: 22 February 2025).

Volatility Foundation (n.d.) *Command reference*. Available at: https://github.com/volatilityfoundation/volatility/wiki/Command-Reference (Accessed: 18 March 2025).

Wireshark (2025) *Download*. Available at: https://www.wireshark.org/download.html (Accessed: 22 February 2025).

10.0 Appendix

Appendix A: VM Disk Image Analysis

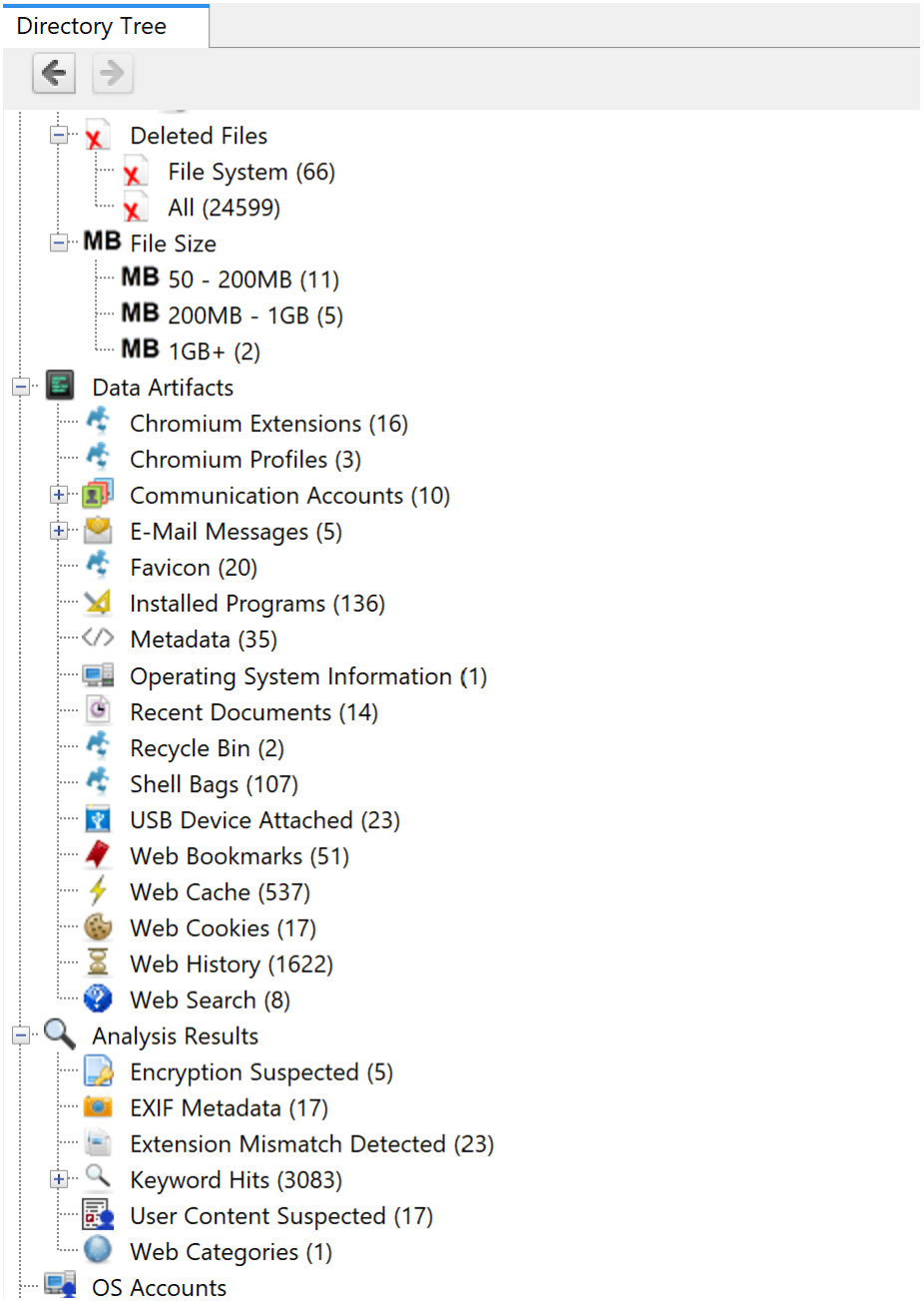

Figure 32: Directory Tree – Autopsy

```
Device: _??_USBSTOR#Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP#0018F30C9FE8EA81C00001EC&0#{53f56307-
b6bf-11d0-94f2-00a0c91efb8b}
  \DosDevices\D:
  \??\Volume{8c06db3e-2d5b-11ef-b2af-1c9957ec61b5}
```

Figure 33: Kingston USB as Drive D

Operating System Information

Table | Thumbnail | Summary

Source Name	S	C	O	Name	Program Name	Processor Architecture	Tempora
Win-7-Forensics1.vmdk				FORENSICS	Windows 7 Enterprise	AMD64	%System

Data Content

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other

Metadata

Name:	/img_Win-7-Forensics1.vmdk
Type:	VMDK
Size:	42949672960
MD5:	dfc85127195b36410ee682f273fa5451
SHA1:	692fcb85a9f74b147d66c14bcd8fb4cf5528cbd7
SHA-256:	6693d8331a880f9cbc7b91a8c3dcfd09038839542c66ca83d35391817e6691f5
Sector Size:	512
Time Zone:	Europe/London
Acquisition Details:	Unknown
Device ID:	beee0777-7566-4af8-b7b6-e8763680b996
Internal ID:	1
Local Path:	D:\Forensics\One\Win-7-Forensics1.vmdk

Figure 34: Operating System Info

```
Username        : Research [1002]
SID             : S-1-5-21-2375367772-2383046927-4008981907-1002
Full Name       : Research
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Mon Jun 17 14:43:23 2024 Z
Name            :
Last Login Date : Tue Jun 18 10:14:42 2024 Z
Pwd Reset Date  : Mon Jun 17 14:43:36 2024 Z
Pwd Fail Date   : Tue Jun 18 10:27:54 2024 Z
Login Count     : 2
  --> Password does not expire
  --> Normal user account

Username        : Sales [1003]
SID             : S-1-5-21-2375367772-2383046927-4008981907-1003
Full Name       : Sales
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Tue Jun 18 10:27:54 2024 Z
Name            :
Last Login Date : Tue Jun 18 10:29:59 2024 Z
Pwd Reset Date  : Tue Jun 18 10:28:09 2024 Z
Pwd Fail Date   : Never
Login Count     : 1
```

Figure 35: Research and Sales User Info

Chromium Extensions 16

Table Thumbnail Summary

Save Table as

Name	Description	Version	Flag	Permissions
Web Store	Discover great apps, games, extensions and themes...	0.2	Enabled	management, system.display, system.storage, webst...
Chrome PDF Viewer		1	Enabled	contentSettings, fileSystem, fileSystem.write, metric...
Google Network Speech	Component extension providing speech via the Goo...	1.0	Enabled	systemPrivate, ttsEngine
Google Hangouts		1.3.21	Enabled	desktopCapture, processes, webrtcAudioPrivate, we...
Web Store	Discover great apps, games, extensions and themes...	0.2	Enabled	management, system.display, system.storage, webst...
Google Docs Offline	Edit, create and view your documents, spreadsheets...	1.62.0	Enabled	alarms, storage, unlimitedStorage
Chrome PDF Viewer		1	Enabled	contentSettings, fileSystem, fileSystem.write, metric...
Google Network Speech	Component extension providing speech via the Goo...	1.0	Enabled	systemPrivate, ttsEngine
Google Hangouts		1.3.21	Enabled	desktopCapture, processes, webrtcAudioPrivate, we...
Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	Enabled	identity, webview
Web Store	Discover great apps, games, extensions and themes...	0.2	Enabled	management, system.display, system.storage, webst...
Google Docs Offline	Edit, create and view your documents, spreadsheets...	1.62.0	Enabled	alarms, storage, unlimitedStorage
Chrome PDF Viewer		1	Enabled	contentSettings, fileSystem, fileSystem.write, metric...
Google Network Speech	Component extension providing speech via the Goo...	1.0	Enabled	systemPrivate, ttsEngine
Google Hangouts		1.3.21	Enabled	desktopCapture, processes, webrtcAudioPrivate, we...
Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	Enabled	identity, webview

Figure 36: Chrome Extensions

Metadata

Table Thumbnail Summary

Save T

Source Name	...	...	...	Owner	...	Date Created	Version
67844AE1-00000002.eml				Sales@shadowfall.non <sales@shadowfall.non>	...	2024-06-18 10:48:35 BST	
00294823-00000001.eml				Sales@shadowfall.non <sales@shadowfall.non>	...	2024-06-18 10:34:52 BST	
67844AE1-00000002.eml				Research <research@shadowfall.non>	...	2024-06-18 10:07:01 BST	
2F3A249F-00000001.eml				itsupport <itsupport@shadowfall.non>	...	2024-06-18 09:56:27 BST	
00294823-00000001.eml				Research <research@shadowfall.non>	...	2024-06-18 09:54:46 BST	
peazip_help.pdf				PeaZip free archiver utility	...	2022-04-10 15:22:49 BST	1.4
f1434032_peazip_help.pdf				PeaZip free archiver utility	...	2022-04-10 15:22:49 BST	1.4
ADG_EULA.rtf				DGT	...	2016-02-24 18:55:00 GMT	
FTKImager_UserGuide.pdf				jgreen	...	2012-03-21 11:26:46 GMT	1.6
eula.rtf				karenor	...	2010-03-05 10:46:00 GMT	
eula.rtf				karenor	...	2010-03-05 10:46:00 GMT	
privacy.rtf					...	2009-04-20 14:07:00 BST	
privacy.rtf					...	2009-04-20 14:07:00 BST	
vofflps.rtf					...	2009-04-20 14:06:00 BST	
vofflps.rtf					...	2009-04-20 14:06:00 BST	
OOBE_HELP_Opt_in_Details.rtf					...	2009-03-31 11:40:00 BST	
OOBE_HELP_Opt_in_Details.rtf					...	2009-03-31 11:40:00 BST	
OOBE_HELP_What_is_User_Account.rtf					...	2009-03-05 11:21:00 GMT	
OOBE_HELP_What_is_User_Account.rtf					...	2009-03-05 11:21:00 GMT	

Figure 37: Metadata.

Web Cookies

Table Thumbnail Summary

Sa

Source Name	...	...	...	URL	Date Accessed	Name	Value	Program Name	Domain
Cookies			0	www.google.com	2024-06-18 11:47:53 BST	DV		Google Chrome	www.google.com
Cookies			0	.google.com	2024-06-18 11:47:52 BST	NID		Google Chrome	google.com
Cookies			0	.google.com	2024-06-18 11:47:41 BST	OGP		Google Chrome	google.com
Cookies			0	.google.com	2024-06-18 11:47:39 BST	OGPC		Google Chrome	google.com
Cookies			0	ogs.google.com	2024-06-18 11:47:39 BST	OTZ		Google Chrome	ogs.google.com
Cookies			0	.youtube.com	2024-06-18 11:47:28 BST	VISITOR_INFO1_LIVE		Google Chrome	youtube.com
Cookies			0	.youtube.com	2024-06-18 11:47:28 BST	VISITOR_PRIVACY_METADATA		Google Chrome	youtube.com
Cookies			0	.google.com	2024-06-18 11:47:27 BST	SNID		Google Chrome	google.com
Cookies			0	.google.com	2024-06-18 11:47:20 BST	SOCS		Google Chrome	google.com
Cookies			0	.google.com	2024-06-18 11:47:09 BST	AEC		Google Chrome	google.com
Cookies			0	.google.com	2024-06-18 10:01:46 BST	SNID		Google Chrome	google.com
Cookies			0	www.google.com	2024-06-18 10:01:45 BST	DV		Google Chrome	www.google.com
Cookies			0	.google.com	2024-06-18 10:01:07 BST	NID		Google Chrome	google.com
Cookies			0	.youtube.com	2024-06-18 10:01:07 BST	VISITOR_INFO1_LIVE		Google Chrome	youtube.com
Cookies			0	.youtube.com	2024-06-18 10:01:07 BST	VISITOR_PRIVACY_METADATA		Google Chrome	youtube.com
Cookies			0	.google.com	2024-06-18 10:00:58 BST	SOCS		Google Chrome	google.com
Cookies			0	.google.com	2024-06-18 10:00:57 BST	AEC		Google Chrome	google.com

Figure 38: Web Cookies

Appendix B: RAM (Memory) Analysis

```
C:\Users\networkuser\Desktop>C:\Users\networkuser\Desktop\volatility-master\vol.py -f C:\Users\networkuser\Desktop\
memdump.mem --profile=Win7SP0x64 pstree >  C:\Temp\coursework_pstree1.txt
Volatility Foundation Volatility Framework 2.6.1

C:\Users\networkuser\Desktop>C:\Users\networkuser\Desktop\volatility-master\vol.py -f C:\Users\networkuser\Desktop\
memdump.mem --profile=Win7SP0x64 cmdscan >  C:\Temp\coursework_cmd1.txt
Volatility Foundation Volatility Framework 2.6.1

C:\Users\networkuser\Desktop>C:\Users\networkuser\Desktop\volatility-master\vol.py -f C:\Users\networkuser\Desktop\
memdump.mem --profile=Win7SP0x64 filescan >  C:\Temp\coursework_filescan1.txt
Volatility Foundation Volatility Framework 2.6.1

C:\Users\networkuser\Desktop>C:\Users\networkuser\Desktop\volatility-master\vol.py -f C:\Users\networkuser\Desktop\
memdump.mem --profile=Win7SP0x64 iehistory >  C:\Temp\coursework_iehistory1.txt
Volatility Foundation Volatility Framework 2.6.1

C:\Users\networkuser\Desktop>C:\Users\networkuser\Desktop\volatility-master\vol.py -f C:\Users\networkuser\Desktop\
memdump.mem --profile=Win7SP0x64 clipboard >  C:\Temp\coursework_clipboard1.txt
Volatility Foundation Volatility Framework 2.6.1
```

Figure 39: Volatility modules.

```
:7e1d2450        TCPv6    -:0                          e858:8b1a:80fa:ffff:e858:8b1a:80fa:ffff:0 CLOSED          4        System
:7e1e4960        TCPv4    192.168.101.128:49184        192.168.101.129:143  ESTABLISHED      1744     wlmail.exe
:7e4d4530        UDPv4    0.0.0.0:5355                 *:*                                   1052     svchost.exe    2024-06-18 10:59:31 UTC+0000
:7e4d4530        UDPv6    :::5355                      *:*                                   1052     svchost.exe    2024-06-18 10:59:31 UTC+0000
:7e4fbe40        UDPv4    192.168.101.128:138          *:*                                   4        System         2024-06-18 10:14:31 UTC+0000
:7e5c5010        UDPv6    ::1:49479                    *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7efead90        UDPv4    0.0.0.0:0                    *:*                                   1744     wlmail.exe     2024-06-18 10:31:00 UTC+0000
:7efead90        UDPv6    :::0                         *:*                                   1744     wlmail.exe     2024-06-18 10:31:00 UTC+0000
:7f21d270        UDPv4    127.0.0.1:60757              *:*                                   1744     wlmail.exe     2024-06-18 10:30:36 UTC+0000
:7f2299b0        UDPv4    0.0.0.0:64857                *:*                                   140092   hZ             2024-06-18 10:47:59 UTC+0000
:7f2f0920        UDPv4    0.0.0.0:0                    *:*                                   1744     wlmail.exe     2024-06-18 10:31:10 UTC+0000
:7f536910        UDPv4    127.0.0.1:56060              *:*                                   1744     wlmail.exe     2024-06-18 10:34:51 UTC+0000
:7f540dc0        UDPv4    0.0.0.0:0                    *:*                                   1744     wlmail.exe     2024-06-18 10:31:00 UTC+0000
:7f0baaf0        TCPv4    -:49242                      142.250.200.14:443   CLOSED           1036     chrome.exe
:7f3fbc20        TCPv4    192.168.101.128:49265        192.168.101.129:143  CLOSED           1744     wlmail.exe
:7fc06d70        UDPv4    127.0.0.1:49481              *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7fc08300        UDPv4    192.168.101.128:1900         *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7fc08450        UDPv6    ::1:1900                     *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7fc09750        UDPv4    127.0.0.1:1900               *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7fc125c0        UDPv4    192.168.101.128:49480        *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7fe6cc20        UDPv6    fe80::d8a0:500b:8cc3:eb6f:1900 *:*                                 536      svchost.exe    2024-06-18 10:16:32 UTC+0000
:7fe6d010        UDPv6    fe80::d8a0:500b:8cc3:eb6f:49478 *:*                                 536      svchost.exe    2024-06-18 10:16:32 UTC+0000
```

Figure 40: Netscan - RAM Analysis

```
consoles.txt - Notepad
File  Edit  Format  View  Help
**************************************************
ConsoleProcess: conhost.exe Pid: 3452
Console: 0xfffe6200 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: Telnet 192.168.101.129
AttachedProcess: telnet.exe Pid: 3976 Handle: 0x54
AttachedProcess: cmd.exe Pid: 3524 Handle: 0xc
----
CommandHistory: 0x441380 Application: telnet.exe Flags: Allocated, Reset
CommandCount: 4 LastAdded: 3 LastDisplayed: 3
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x54
Cmd #0 at 0x4171d0: 192.168.101.129
Cmd #1 at 0x43d690: open
Cmd #2 at 0x435660: 192.168.101.129
Cmd #3 at 0x440400: y
----
CommandHistory: 0x4410d0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xc
Cmd #0 at 0x43d650: telnet
----
Screen 0x4236e0 X:80 Y:300
Dump:
*==============================================================
Microsoft Telnet Server.
*==============================================================
C:\Users\user37>
----
Screen 0x441560 X:80 Y:300
Dump:
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> 192.168.101.129
Invalid Command. type ?/help for help
Microsoft Telnet> open
( to ) 192.168.101.129
Connecting To 192.168.101.129...
You are about to send your password information to a remote computer in Internet
 zone. This might not be safe. Do you want to send anyway(y/n): y
```

Figure 41: Consoles - RAM Analysis

Appendix C: Detailed Timeline of Events

ACME Ltd Incident Timeline.xlsx

Time (BST)	Event Description	Source
18/05/2022 11:57:04	Created Administrator and Guest accounts	VM Disk Analysis(OS Accounts)
17/06/2024 12:44:37	Opened FTKImager_UserGuide.pdf (*forensic tool guide*) – No user account linked	VM Disk Analysis(Metadata)
17/06/2024 13:06:01	Accessed three audio files – No user account linked	VM Disk Analysis(Metadata)
17/06/2024 13:13:05	Opened USB network guide (.rtf) – No user account linked	VM Disk Analysis(Metadata)
17/06/2024 13:55:51	Admin accessed Recycle Bin, Google Chrome, FTK Imager (forensic tool), and SDelete (secure file deletion tool).	VM Disk Analysis(Shellbags)
17/06/2024 14:43:10	Admin accessed User Accounts settings in Control Panel	VM Disk Analysis(Shellbags)
17/06/2024 14:55:39	Deleted file named Test from Administrator's Desktop	VM Disk Analysis(Recycle Bin)
17/06/2024 15:43:23	Created Research account	VM Disk Analysis(OS Accounts)
18/06/2024 02:58:00	Virtual Mouse connected	VM Disk Analysis(USB Connected)
18/06/2024 10:00:52	The system is set to open FTP, HTTP, and HTTPS links using Google Chrome for research account.	VM Disk Analysis(USRCLASS.DAT Registry)
18/06/2024 10:00:57	Accessed Google Chrome and cookies (AEC AND SOCS) via google.com	VM Disk Analysis(Web history, Cookies, Favicon)
18/06/2024 10:01:06	Performed a Google search for "how to install Kali Linux" via google.com, then accessed youtube.com, ytimg.com, and gstatic.com (No user account linked)	VM Disk Analysis(Web History, Web Cache, Web Search)
18/06/2024 10:01:07	Accessed cookies: VISITOR_INFO1_LIVE, VISITOR_PRIVACY_METADATA (google.com) and NID (google.com) from YouTube	VM Disk Analysis(Cookies)
18/06/2024 10:01:09	Accessed multiple Kali Linux setup images and scripts from Kali Linux Documentation (Installing Kali Linux), modifying kali.org favicon	VM Disk Analysis(Web History, Web Cache, Favicon)
18/06/2024 10:01:45	Performed a Google search for "steganography in files" via google.com, accessing gstatic.com and DV, SNID cookies (No user account linked)	VM Disk Analysis(Web History, Web Search, Web Cache, Cookies)
18/06/2024 10:01:50	Accessed "What is Steganography? How to Hide Data Inside Data" from freecodecamp.org, gstatic.com, modifying its favicon	VM Disk Analysis(Web History, Web Cache, Favicon)
18/06/2024 10:27:56	Admin accessed User Accounts settings in Control Panel	VM Disk Analysis(Shellbags)
18/06/2024 10:30:06	Multiple access index.dat file through Internet Explorer (Internet Explorer Analyzer)	VM Disk Analysis(Web History)
	Email sent from Research@shadowfall.non to itsupport@shadowfall.non with	VM Disk Analysis(Metadata, Email)

Key Activities | APPENDIX_Full Timeline | +

Figure 42:Detailed Timeline