Incident Management and Forensics

By

Usiwoghene Ekebor

Table of Content Page Number

Executive Summary

This report underscores potential unauthorized activities by the Finance Director at ACME Ltd. who is suspected of misusing company systems and transferring confidential data to unapproved third parties. The investigation reveals the activities the system was being used for such as web browsing and network traffic history, and email communications. Subsequently, evidence was gathered through the analysis of system disk image, memory dumps and network capture evidence provided. Consequently, some of the suspicious activities uncovered included, the use of remote access tools and unusual email communications. Furthermore, abnormal web searches related to steganography and Kali Linux suggest potential misconduct and untrusted intentions. The detailed analysis of the memory and network traffic revealed unauthorized access and communication, which supports the potential misuse of the system. These findings are critical to understanding the extent of any potential breach of company policy and key steps to take for ensuring the integrity of company systems and information.

1.0 Introduction

Businesses today use digital devices to run daily activities, some of these devices housed sensitive data that can be accessed by a handful of company employee, but sometimes the trust of some employees become doubtful (Constantinides and Quercia 2022). This report is prepared to investigate the potential system misuse by Finance Director of ACME Ltd to the CEO. The investigation will focus on reviewing the digital evidence provided to determine whether there has been any illegal activity that could breach company policy.

2.0 Scope of Investigation

The scope of this investigation covers multiple aspects of digital forensic analysis, which include system and user account activities, network traffic, memory capture, and the potential use of unauthorized software. In contrast, the key focus areas will include a thorough analysis of any suspicious file transfers, email communications, web browsing history, and network interactions. These actions will be extracted from within the memory, disk, and network evidence data extracted from the system.

3.0 Objective of the Investigation

The objectives of this investigation are to:

1. To determine if any sensitive or confidential company data has been accessed or transmitted to unauthorized third parties.
2. Identify any abnormal activities, including the use of unauthorized software, communications, and web activities.
3. Assess whether any malicious activity occurred and provide the evidence necessary to support any findings identified.

The findings in this report will subsequently assist ACME Ltd in understanding the extent of the misuse, if any, and help guide further actions that could be taken to protect company data integrity.

4.0 Evidence Analysed / Data Sources

This investigation of potential system misuse by the Finance Director was completed with multiple data sources to provide a comprehensive understanding of system activity and identify all potential suspicious events that took place. The primary data sources include:

4.1 System Disk (Autopsy Analysis)

A detailed review of the disk image provided insights into the installed software and user account activities. Remarkably, it was identified that the user was engaged in suspicious activities which include unusual domain queries, email communications, and deleting some files.

4.2 Network Traffic (PCAP Analysis)

The network traffic capture (PCAP) file was analysed to track the device communication with external IP addresses. Interesting information was found in the DNS, SMTP, and Telnet protocols, which could support the idea of unauthorized data and access to the system. This

also helped to corroborate the web activities and email communications identified from the disk analysis.

4.3 Memory Image

The memory dump of the system provided a comprehensive breakdown of the processes and user activities at the time of capture. Suspicious activities such as remote access, the execution of potentially malicious processes, and abnormal network connections were inspected to determine if any unauthorized activities were carried out in the system.

By analysing these data sources, a clear picture of the Finance Director's motive was formed, which assisted in the identification of potential system misuse.

5.0 Forensic Method / Tools / Processes

To conduct a thorough forensic investigation into the activities of the Finance Director, a combination of industry standard forensic tools and methods were deployed to analyse the disk, memory, and network data. The following tools and processes were used:

5.1 Autopsy (Disk Analysis)

Autopsy is a user friendly and powerful open-source digital forensics tool Nayak et al. (2023). This tool was used to examine the disk image of the system, and it provided insight into installed software, file access, deleted files, and user account activities. The tool's detailed report highlighted every information about the disk including the metadata and dlls. Consequently, Autopsy also allowed the review of web activity, email communication, and file access by the system users, providing evidence of unusual and unauthorized actions.

5.2 Volatility Master (Memory Forensics)

Volatility Master is a memory forensics tool, it was utilized to analyse the system's memory dump. It enabled the extraction of active processes, network connections, and command-line activities at the time of capture. This helped identify suspicious remote access attempts via Telnet and CMD commands, which suggests a potential unauthorized remote activity.

5.3 Wireshark (Network Analysis)

Soepeno (2023) illustrates that Wireshark is widely used network protocol analyser. This tool was utilised to investigate the network traffic captured in the evidence PCAP file provided. Furthermore, it helped to identify connections using DNS, SMTP, and Telnet protocols, revealing potential unauthorized communications.

These tools, combined with a robust forensic methodology, allowed for a comprehensive analysis of the device activities, which reveals important evidence to support the investigation.

6.0 Basic / Initial Analysis Findings

6.1 Disk Analysis

The system was running Windows 7 Enterprise on an AMD64-bit architecture with the owner being the networkadmin. The operating system had been installed on 2009-07-14, suggesting the machine had been in use for several years. Multiple accounts were registered, including Sales, Research, and Administrator accounts. Notably, the Administrator account had files like Google Chrome and sdelete.exe on the desktop. The Sales account accessed files such as

"kitten.jpg" and "New Rich Text Document.rtf. Furthermore, the machine time zone is GMT Standard Time zone.

Figure 1 registered OS Accounts

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	Win-7-Forensics1.vmdk_1 Host	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-185			0		Win-7-Forensics1.vmdk_1 Host	Local	NT SERVICE	
S-1-5-21-2375367772-2383046927-4008981907-50			0	Administrator	Win-7-Forensics1.vmdk_1 Host	Domain		2022-05-18 11:57:04 BST
S-1-5-21-2375367772-2383046927-4008981907-10			0	Research	Win-7-Forensics1.vmdk_1 Host	Domain		2024-06-17 15:43:23 BST
S-1-5-21-2375367772-2383046927-4008981907-10			0	Sales	Win-7-Forensics1.vmdk_1 Host	Domain		2024-06-18 11:27:54 BST
S-1-5-20				NETWORK SERVICE	Win-7-Forensics1.vmdk_1 Host	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	Win-7-Forensics1.vmdk_1 Host	Local	NT AUTHORITY	
S-1-5-21-2375367772-2383046927-4008981907-50			0	Guest	Win-7-Forensics1.vmdk_1 Host	Domain		2022-05-18 11:57:04 BST

Source Screenshot from Autopsy Disk analysis

6.2 Memory Analysis

The imageinfo command shows the memory dump is from a 64-bit Windows 7 SP1 system. This helps to choose the correct Volatility profile (Win7SP1x64) for accurate analysis. The memory capture timestamp is June 18, 2024, at 10:52:29 UTC, but the local time is 2024-06-18 11:52:29. The command also shows two processors, a valid DTB (0x187000), and a KDBG address (0xf80002c3a070), confirming the memory integrity.

Figure 2 Memory imageinfo

```
PS C:\Users\ekeuz> C:\Users\ekeuz\Desktop\volatility_2.6_win64_standalone.exe -f C:\Users\ekeuz\Desktop\memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\ekeuz\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
```

Source Screenshot from Volatility Master analysis

6.3 Network Analysis

The network analysis revealed several connections from the machine's IP address (192.168.101.128) to different destinations, including Google's IP address. The focus was on the DNS and SMTP protocols, as they indicated potential suspicious communication. Also, activities related to TELNET and SMTP revealed remote access to the system and email communication that involved the user sending emails with one having an attachment named "kitten.jpg."

7.0 Detailed Analysis Findings

7.1 Detailed Disk Analysis

7.1.0 Accounts on the System

Though there are multiple accounts registered to the OS, like the Researcher and Sales accounts, the only account with Admin privileges is the Administrator account. There is also an inactive Guest account. In general, the accounts registered to the machine are the

Administrator, Sales, Research, and Guest accounts. Additionally, there are some network accounts that have been deleted, suggesting that the machine has been in use for some time.

7.1.1 Installed Programs

The machine has 136 installed programs, as displayed by Autopsy. However, some of these programs are repeated in the list, though they have slightly different installation times. There are 53 unique programs, which are mostly non-suspicious Microsoft registry and regular software.

Table 1 List of installed programs

SN	Program Name	Software Description	Status
1	Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.24215 v.14.0.24215	Microsft software	Not suspicious
2	Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.24215 v.14.0.24215	Microsft software	Not suspicious
3	Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 v.12.0.21005	Microsft software	Not suspicious
4	Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 v.12.0.21005	Microsft software	Not suspicious
5	AccessData FTK Imager v.4.2.0.13	A FREE data preview and imaging tool used to acquire electronic evidence in a forensically sound manner by creating copies of computer data without making changes to the original evidence	Not suspicious
6	Windows Live MIME IFilter v.16.4.3528.0331	Microsft software	Not suspicious
7	Microsoft Application Error Reporting v.12.0.6015.5000	Microsft software	Not suspicious
8	Windows Live ID Sign-in Assistant v.7.250.4311.0	Microsft software	Not suspicious
9	MSVCRT110_amd64 v.16.4.1109.0912	Microsft software	Not suspicious
10	Microsoft .NET Framework 4 Extended v.4.0.30319	Microsft software	Not suspicious
11	Microsoft .NET Framework 4 Client Profile v.4.0.30319	Microsft software	Not suspicious
12	MPlayer2	Microsft software	Not suspicious
13	Sumatra PDF v.3.4.1	Microsft software	Not suspicious
14	Notepad++ (64-bit x64) v.8.4.1	Microsft software	Not suspicious
15	PeaZip 8.6.0 (WIN64) v.8.6.0	PDF is a free and open-source document viewer and manager	Not suspicious
16	VMware Tools v.10.0.0.3000743	A text and source code editor	Not suspicious
17	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 v.9.0.30729.6161	PeaZip is an open source file and archive manager	Not suspicious
18	DXM_Runtime	For improvemnt of the performance of virtual machines	Not suspicious
19	AddressBook	Microsft software	Not suspicious
20	Connection Manager	A software library that provides cloud-based endpoint security	Not suspicious
21	DirectDrawEx	Microsft software	Not suspicious
22	Fontcore	A tool used for establishing and managing connections to remote networks	Not suspicious
23	IE40	Used to accelerate rendering of 2D graphics in applications	Not suspicious
24	IE4Data	Trojan identified by Malwarebytes as a variant of the Trojan.Ransom.ED malware.	Suspicious
25	IE5BAKEX	Windows registry program	Not suspicious
26	IEData	Windows registry program	Not suspicious
27	MobileOptionPack	Windows registry program	Not suspicious
28	SchedulingAgent	Windows registry program	Not suspicious
29	WIC	possibly related to a trojan	Suspicious
30	Wireshark 2.2.17 (64-bit) v.2.2.17	Windows program	Not suspicious
31	WinPcap 4.1.3 v.4.1.0.2980	Windows Imaging Component	Not suspicious
32	Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24215 v.14.0.24215.1	Network protocol analyzer	Not suspicious
33	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 v.12.0.30501.0	Used to capture and analyze network packets	Not suspicious
34	Windows Live Mail v.16.4.3528.0331	Microsft software	Not suspicious
35	Windows Live Essentials v.16.4.3528.0331	Microsft software	Not suspicious
36	Windows Live Writer Resources v.16.4.3528.0331	Microsft software	Not suspicious
37	Photo Common v.16.4.3528.0331	Microsft software	Not suspicious
38	Windows Live Photo Common v.16.4.3528.0331	Microsft software	Not suspicious
39	Windows Live UX Platform Language Pack v.16.4.3528.0331	Microsft software	Not suspicious
40	Windows Live Writer v.16.4.3528.0331	Microsft software	Not suspicious
41	Junk Mail filter update v.16.4.3528.0331	Microsft software	Not suspicious
42	Windows Live UX Platform v.16.4.3528.0331	Microsft software	Not suspicious
43	Windows Live PIMT Platform v.16.4.3528.0331	Microsft software	Not suspicious
44	D3DX10 v.15.4.2368.0902	Microsft software	Not suspicious
45	Windows Live Communications Platform v.16.4.3528.0331	Microsft software	Not suspicious
46	Windows Live SOXE v.16.4.3528.0331	Microsft software	Not suspicious
47	Windows Live SOXE Definitions v.16.4.3528.0331	Microsft software	Not suspicious
48	Windows Live Installer v.16.4.3528.0331	Microsft software	Not suspicious
49	MSVCRT_amd64 v.15.4.2862.0708	Microsft software	Not suspicious
50	MSVCRT110 v.16.4.1108.0727	Microsft software	Not suspicious
51	MSVCRT v.15.4.2862.0708	Microsft software	Not suspicious
52	Google Chrome v.109.0.5414.120	Microsft software	Not suspicious
53	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 v.9.0.30729.4148	Microsft software	Not suspicious

Source Autopsy CSV Extract

Thorough research on all the software uncovers those two installed programs, IE40 and WIC are suspected to be malware, likely a Trojan.

7.1.2 Web Activity Analysis

The web activity analysis shows that between 2024-06-18 10:00:57 and 2024-06-18 11:48:06 BST, the machine accessed websites like Google.com, Kali.org, freecodecamp.org,

Tutorialspoint.com, and Springeropen.com. Although Autopsy shows a total of 1,622 web history records, over 90% are index.dat files, which are hidden database files used by Internet Explorer to store browser activity. Only 21 of these records are actual browsing history from the installed Google Chrome browser. Additionally, there were 8 recorded web searches on the Google Chrome browser, between 2024-06-18 10:01:06 BST and 2024-06-18 11:47:52 BST, with search terms like “How to install Kali Linux,” “steganography in files,” and “how to use Kali Linux” among others.

Figure 3 List of Google search history

Source Name	S	C	O	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

Source Screenshot from Autopsy disk analysis

7.1.3 Network Information

Further analysis of the system report reveals the following network information:

- **DhcpIPAddress**: 192.168.101.128
- **DhcpSubnetMask**: 255.255.255.0
- **DhcpDefaultGateway**: 192.168.101.2

The machine's IP was assigned via DHCP, as indicated by Enable DHCP being set to 1.

Figure 4 Regripper system report showing network connection details

```
LastWrite Time: Tue Jun 18 11:01:31 2024 Z
  UseZeroBroadcast            0
  EnableDeadGWDetect          1
  EnableDHCP                  1
  NameServer
  Domain
  RegistrationEnabled         1
  RegisterAdapterName         0
  DhcpIPAddress               192.168.101.128
  DhcpSubnetMask              255.255.255.0
  DhcpServer                  192.168.101.254
  Lease                       1800
```

Source Screenshot from Autopsy disk analysis

7.1.4 File Analysis for Administrator Account

The Administrator account has the following files on the desktop:

Recycle Bin, AccessData FTK imagecank, desktop.ini, Google Chrome, sdelete.exe.

Figure 5 Admin account desktop content

Size	Modified	Accessed	Created	Name
				Recycle Bin
1992	2024-06-12 21:23:28	2024-06-12 21:23:28	2024-06-12 21:23:28	AccessData FTK Imager.lnk
174	2009-07-14 04:54:26	2009-07-14 04:54:24	2009-07-14 04:54:24	desktop.ini
282	2024-06-12 19:34:56	2024-06-12 19:34:54	2024-06-12 19:34:54	desktop.ini
2201	2024-06-12 19:34:56	2024-06-12 19:34:56	2024-06-12 19:34:56	Google Chrome.lnk
193064	2023-09-29 15:44:16	2024-06-14 12:07:36	2024-06-14 12:07:36	sdelete.exe

Source Screenshot from Autopsy disk analysis

7.1.5 File Analysis for Sales Account

The Sales account has the following files on the desktop:

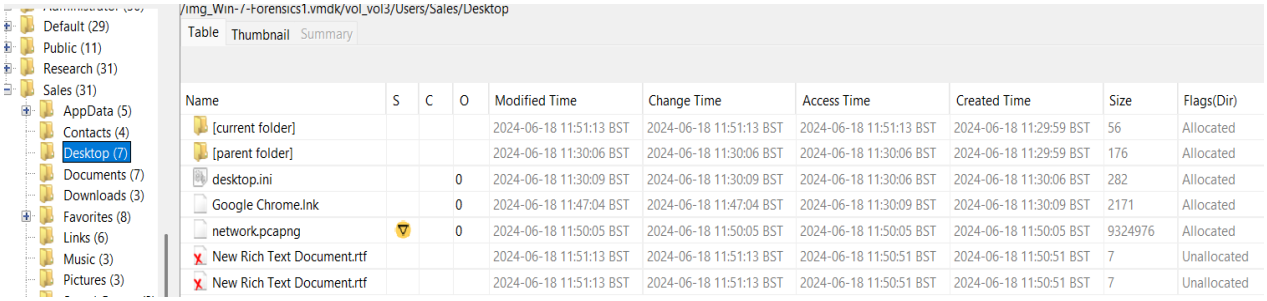
desktop.ini, Google Chrome.lnk, network.pcapng, New Rich Text Document.rtf.

Figure 6 Sales account Desktop content from regripper

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

Source Screenshot from Autopsy disk analysis

Figure 7 Sales account Desktop content



Source Screenshot from Autopsy disk analysis

Also, Google Chrome is the default web browser of the machine.

7.1.6 Email Accounts

Further analysis into the communication section reveals 5 email accounts linked to the machine.

Figure 8 Email accounts

Source Name	S	C	O	Account Type	ID	Data Source
00294823-00000001.eml				EMAIL	research@shadowfall.non	Win-7-Forensics1.vmdk
2F3A249F-00000001.eml				EMAIL	itsupport@shadowfall.non	Win-7-Forensics1.vmdk
00294823-00000001.eml				EMAIL	itsupport@shadowfall.non	Win-7-Forensics1.vmdk
2F3A249F-00000001.eml				EMAIL	research@shadowfall.non	Win-7-Forensics1.vmdk
67844AE1-00000002.eml				EMAIL	research@shadowfall.non	Win-7-Forensics1.vmdk
67844AE1-00000002.eml				EMAIL	alpha@other.non	Win-7-Forensics1.vmdk
00294823-00000001.eml				EMAIL	sales@shadowfall.non	Win-7-Forensics1.vmdk
00294823-00000001.eml				EMAIL	itsupport@shadowfall.non	Win-7-Forensics1.vmdk
67844AE1-00000002.eml				EMAIL	sales@shadowfall.non	Win-7-Forensics1.vmdk
67844AE1-00000002.eml				EMAIL	alpha@other.non	Win-7-Forensics1.vmdk

Source Screenshot from Autopsy disk analysis

7.1.7 Attached USB Devices

The attached USB devices include ROOT_HUB, ROOT_HUB20, Virtual USB hub, and VMware devices, suggesting a virtual environment was running.

Figure 9 Attached USB devices

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			0	2024-06-16 12:34:13 BST		ROOT_HUB	5&17df1c1b&0	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-16 12:34:13 BST		ROOT_HUB20	5&2648447&0	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-16 12:34:15 BST	VMware, Inc.	Virtual USB Hub	6&b25d31b&0&2	Win-7-Forensics1.vmdk
SYSTEM			0	2022-05-26 08:54:02 BST	VMware, Inc.	Virtual Mouse	6&b25d31b&0&1	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-16 12:34:13 BST	VMware, Inc.	Virtual Mouse	6&e0b0e60&0&5	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-16 12:34:14 BST	VMware, Inc.	Virtual Mouse	7&29078710&0&0000	Win-7-Forensics1.vmdk
SYSTEM			0	2022-05-26 08:54:02 BST	VMware, Inc.	Virtual Mouse	7&2a63cead&0&0000	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-16 12:34:14 BST	VMware, Inc.	Virtual Mouse	7&29078710&0&0001	Win-7-Forensics1.vmdk
SYSTEM			0	2022-05-26 08:54:02 BST	VMware, Inc.	Virtual Mouse	7&2a63cead&0&0001	Win-7-Forensics1.vmdk
SYSTEM			1	2024-06-16 12:34:14 BST	VMware, Inc.	Product: 0008	000650268328	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-18 11:14:30 BST		ROOT_HUB	5&17df1c1b&0	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-18 11:14:30 BST		ROOT_HUB20	5&2648447&0	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-18 11:24:43 BST	Kingston Technology	Data Traveler 100 G2 8 GiB	0018F30C9FE8EA81C00001EC	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-18 11:14:31 BST	VMware, Inc.	Virtual USB Hub	6&b25d31b&0&2	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-18 11:24:42 BST	VMware, Inc.	Virtual USB Hub	6&e0b0e60&0&7	Win-7-Forensics1.vmdk
SYSTEM			0	2024-06-18 11:24:43 BST	VMware, Inc.	Virtual USB Hub	6&e0b0e60&0&8	Win-7-Forensics1.vmdk

Source Screenshot from Autopsy disk analysis

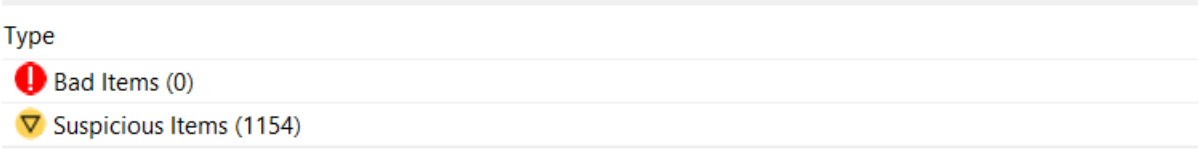
Additionally, a Kingston Technology Data Traveler 100 G2 8GB device was attached. The following details were noted in the Regripper system report for the USB device:

- **LastWrite**: Tue Jun 18 10:24:45 2024
- **Mfg**: Kingston
- **InstallDate**: Tue Jun 18 10:24:45 2024 UTC
- **FirstInstallDate**: Tue Jun 18 10:24:45 2024 UTC

7.1.8 Suspicious Items

Further investigation in the Autopsy score section shows that there are no "bad" files on the machine, but over 1,150 suspicious items were found.

Figure 10 Suspicious items



Source Screenshot from Autopsy disk analysis

7.1.9 Recent Accessed Documents

The recent access documents section shows that the Sales account accessed the "kitten.jpg" and "New Rich Text Document.rtf" files at 2024-06-18 11:50:20 BST and 2024-06-18 11:50:54 BST, respectively.

Figure 11 Recently accessed files

Source Name	S	C	O	Path	Date Accessed	Data Source
kitten.lnk				C:\Users\Sales\Documents\kitten.jpg	2024-06-18 11:50:20 BST	Win-7-Forensics1.vmdk
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
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\Wind...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Videos.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Wind...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Music.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Wind...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Documents.library-ms.lnk				C:\Users\Research\AppData\Roaming\Microsoft\Wind...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Pictures.library-ms.lnk				C:\Users\Sales\AppData\Roaming\Microsoft\Windows\...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Videos.library-ms.lnk				C:\Users\Sales\AppData\Roaming\Microsoft\Windows\...	0000-00-00 00:00:00	Win-7-Forensics1.vmdk
Desktop.lnk				C:\Users\Sales\Desktop	0000-00-00 00:00:00	Win-7-Forensics1.vmdk

Source Screenshot from Autopsy disk analysis

7.1.10 Deleted Files

The Administrator deleted the "Test" file, while the Sales account deleted the "New Rich Text Document.rtf." The deleted files section of Autopsy shows a total of 24,599 deleted files, with 66 of these files are found in the file system section of the Autopsy report. Most of the deleted files are system files from the Sales account, which could suggest potential suspicious activities on the machine.

7.1.11 Email Addresses and RID Numbers

Potential email addresses and RID numbers associated with the OS accounts on the machine are listed below:

- Administrator: RID 500, could associated with itsupport@shadowfall.non
- Research: RID 1002, could associated with research@shadowfall.non
- Sales: RID 1003, could associated with sales@shadowfall.non

7.1.12 Email Communications

Emails were exchanged between the following accounts:

- research@shadowfall.non and itsupport@shadowfall.non
- research@shadowfall.non and alpha@other.non (no response)
- sales@shadowfall.non and both itsupport@shadowfall.non and alpha@other.non (no response)

Figure 12 Email communications

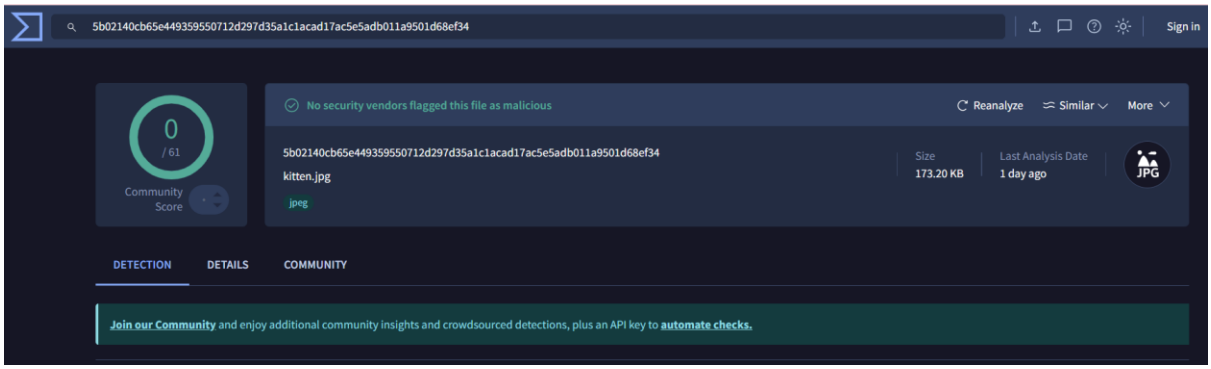
Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)
00294823-00000001.eml				research@shadowfall.non;	itsupport@shadowfall.non;	TEST	2024-06-18 10:54:46 BST	TEST
2F3A249F-00000001.eml				itsupport@shadowfall.non;	research@shadowfall.non;	Re: TEST	2024-06-18 10:56:27 BST	REPLYOn 18/06/2024 10:54, Research wrote:> TEST
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

Source Screenshot from Autopsy disk analysis

7.1.13 Machine Usage and Potential Misuse

The machine appears to belong to Shadowfall, which explains the use of the "shadowfall.non" domain for the sales, itsupport, and research email addresses. The investigation reveals that the Sales account user was using the device for malicious activities. The user was learning how to install and use Kali Linux and steganography techniques to hide data in files. The user also sent an email with an attachment, "kitten.jpg," to the alpha@other.non account. Given the user's research on hiding data, this .jpg file could potentially be more than just an image. Although the file was extracted uploaded to Virustotal.com, the result showed that the file was clean.

Figure 13 kitten.jpg malware search

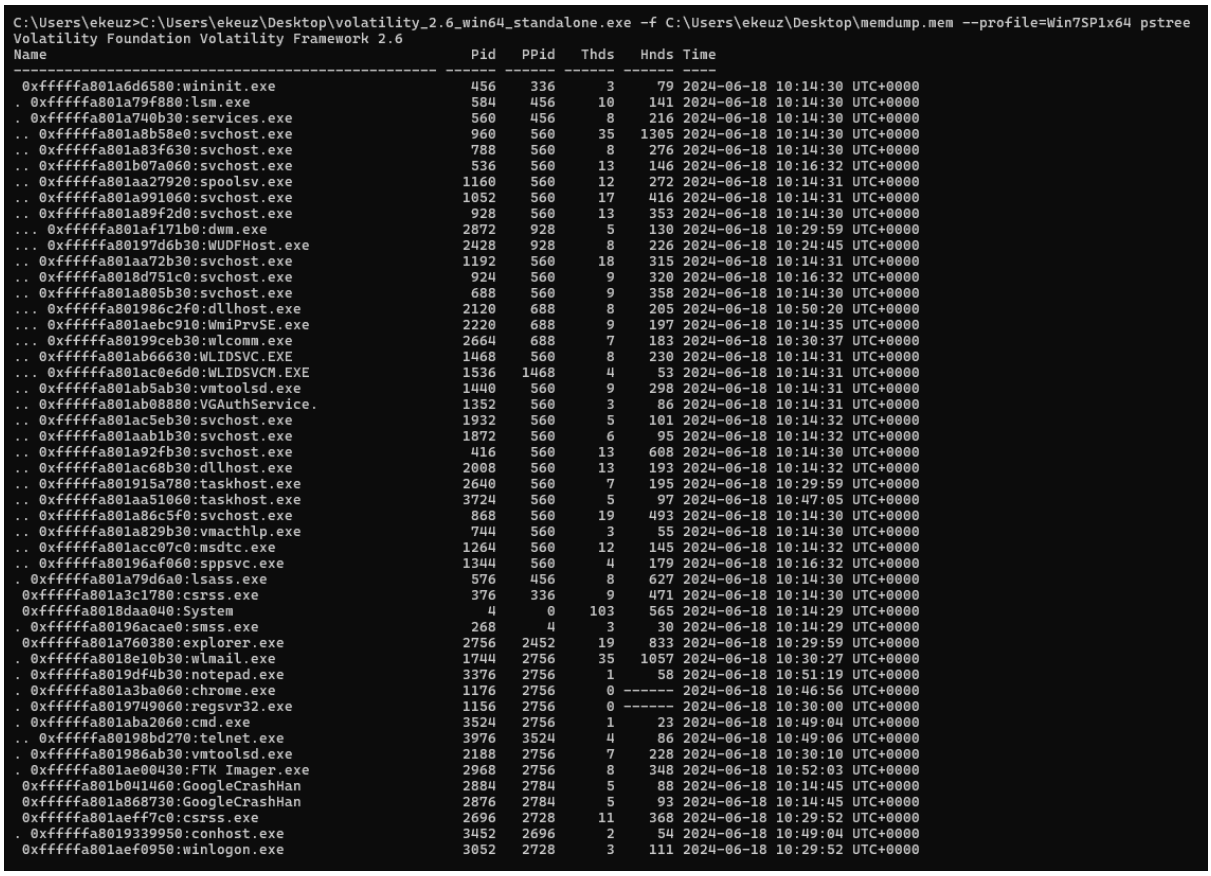


Source Virustotal.com

7.2 Detailed Memory Analysis

The pstree output shows the Windows process hierarchy, revealing some suspicious user actions. At 2024-06-18 10:49:04 UTC, cmd.exe (PID 3524) was active, followed by telnet.exe (PID 3976) at 2024-06-18 10:49:06 UTC, which may suggest manual remote access—a red flag. Additionally, FTK Imager.exe (PID 2968) is running, indicating forensic activity. Chrome.exe at 2024-06-18 10:46:56 UTC and regsvr32.exe at 2024-06-18 10:30:00 UTC appear with zero threads, which is unusual and may point to abnormal or terminated processes. In general, the pstree provides insight into background services and highlights potentially suspicious user-level behaviour.

Figure 14 pstree memory analysis



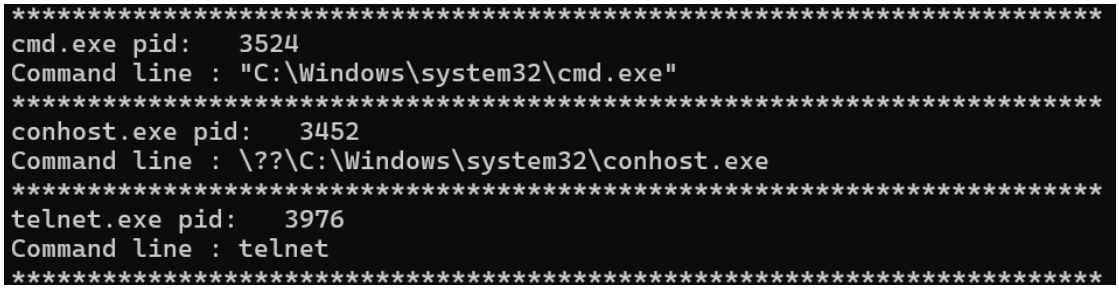
```
C:\Users\ekeuz>C:\Users\ekeuz\Desktop\volatility_2.6_win64_standalone.exe -f C:\Users\ekeuz\Desktop\memdump.mem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 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
.. 0xfffffa801ab08880:VGAuthService.                 1352    560      3     86 2024-06-18 10:14:31 UTC+0000
.. 0xfffffa801ac5eb30:svchost.exe                    1932    560      5    101 2024-06-18 10:14:32 UTC+0000
.. 0xfffffa801aab1b30:svchost.exe                    1872    560      6     95 2024-06-18 10:14:32 UTC+0000
.. 0xfffffa801a92fb30:svchost.exe                     416    560     13    608 2024-06-18 10:14:30 UTC+0000
.. 0xfffffa801ac68b30:dllhost.exe                    2008    560     13    193 2024-06-18 10:14:32 UTC+0000
.. 0xfffffa801915a780:taskhost.exe                   2640    560      7    195 2024-06-18 10:29:59 UTC+0000
.. 0xfffffa801aa51060:taskhost.exe                   3724    560      5     97 2024-06-18 10:47:05 UTC+0000
.. 0xfffffa801a86c5f0:svchost.exe                     868    560     19    493 2024-06-18 10:14:30 UTC+0000
.. 0xfffffa801a829b30:vmacthlp.exe                    744    560      3     55 2024-06-18 10:14:30 UTC+0000
.. 0xfffffa801acc07c0:msdtc.exe                      1264    560     12    145 2024-06-18 10:14:32 UTC+0000
.. 0xfffffa80196af060:sppsvc.exe                     1344    560      4    179 2024-06-18 10:16:32 UTC+0000
. 0xfffffa801a79d6a0:lsass.exe                        576    456      8    627 2024-06-18 10:14:30 UTC+0000
 0xfffffa801a3c1780:csrss.exe                         376    336      9    471 2024-06-18 10:14:30 UTC+0000
 0xfffffa8018daa040:System                              4      0    103    565 2024-06-18 10:14:29 UTC+0000
. 0xfffffa80196acae0:smss.exe                         268      4      3     30 2024-06-18 10:14:29 UTC+0000
 0xfffffa801a760380:explorer.exe                     2756   2452     19    833 2024-06-18 10:29:59 UTC+0000
. 0xfffffa8018e10b30:wlmail.exe                      1744   2756     35   1057 2024-06-18 10:30:27 UTC+0000
. 0xfffffa8019df4b30:notepad.exe                     3376   2756      1     58 2024-06-18 10:51:19 UTC+0000
. 0xfffffa801a3ba060:chrome.exe                      1176   2756      0 ------ 2024-06-18 10:46:56 UTC+0000
. 0xfffffa8019749060:regsvr32.exe                    1156   2756      0 ------ 2024-06-18 10:30:00 UTC+0000
. 0xfffffa801aba2060:cmd.exe                         3524   2756      1     23 2024-06-18 10:49:04 UTC+0000
.. 0xfffffa80198bd270:telnet.exe                     3976   3524      4     86 2024-06-18 10:49:06 UTC+0000
. 0xfffffa801986ab30:vmtoolsd.exe                    2188   2756      7    228 2024-06-18 10:30:10 UTC+0000
. 0xfffffa801ae00430:FTK Imager.exe                  2968   2756      8    348 2024-06-18 10:52:03 UTC+0000
 0xfffffa801b041460:GoogleCrashHan                   2884   2784      5     88 2024-06-18 10:14:45 UTC+0000
 0xfffffa801a868730:GoogleCrashHan                   2876   2784      5     93 2024-06-18 10:14:45 UTC+0000
 0xfffffa801aeff7c0:csrss.exe                        2696   2728     11    368 2024-06-18 10:29:52 UTC+0000
. 0xfffffa8019339950:conhost.exe                     3452   2696      2     54 2024-06-18 10:49:04 UTC+0000
 0xfffffa801aef0950:winlogon.exe                     3052   2728      3    111 2024-06-18 10:29:52 UTC+0000
```

Source Screenshot from Volatility Master analysis

7.2.0 Process Details and Loaded Modules

To investigate the system's loaded modules, the cmdline plugin in Volatility was used. This plugin lists the command-line arguments of running processes in the memory image, helping to identify unusual executions or LOLBins abuse. Key findings include telnet.exe, suggesting potential remote access, and cmd.exe, which might have been used for manual commands or scripts.

Figure 15 cmdline memory analysis



```
**************************************************************************
cmd.exe pid:   3524
Command line : "C:\Windows\system32\cmd.exe"
**************************************************************************
conhost.exe pid:   3452
Command line : \??\C:\Windows\system32\conhost.exe
**************************************************************************
telnet.exe pid:   3976
Command line : telnet
**************************************************************************
```

Source Screenshot from Volatility Master analysis

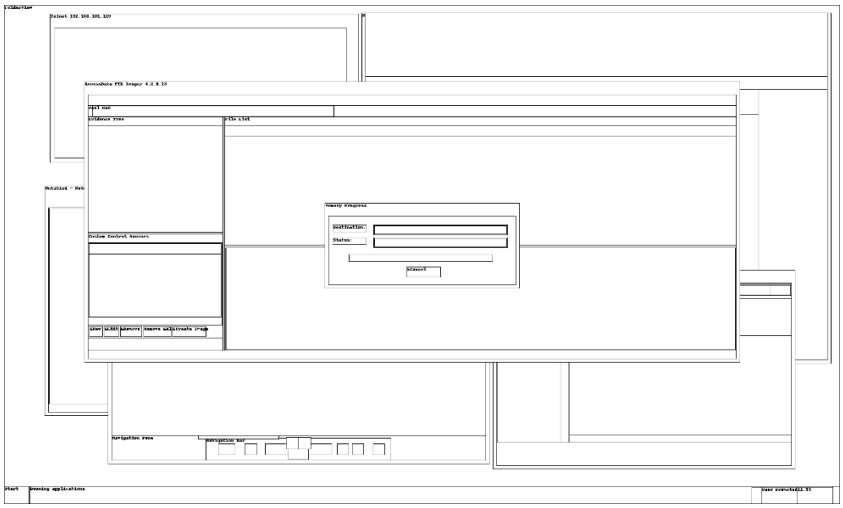
Furthermore, running the dlllist plugin shows all the loaded DLLs per process, which provided insights into both legitimate and suspicious activities. Most of the Windows core system processes were loading, but there were some abnormalities. For example, networking-related

DLLs were found in several service processes, indicating active communications or security services.

7.2.1 Live User Activity

First, the screenshot was captured using the screenshot –dump-dir command. The screenshot reveals that Telnet (IP: 192.168.101.129), untitled Notepad, and AccessData FTK Imager 4.2.013 were running on the day the machine was imaged, with the memory imaging process in progress.

Figure 16 Image screenshot dump



Source Volatility Master analysis

Additionally, running the cmdscan plugin reveals interactive command-line activity. It shows that cmd.exe executed telnet, and telnet.exe attempted to connect to IP address 192.168.101.129. The commands "open" and a second instance of the IP confirm an attempted or active Telnet session. The final "y" suggests user confirmation, possibly for login or a trust prompt. This indicates potential manual remote access or lateral movement.

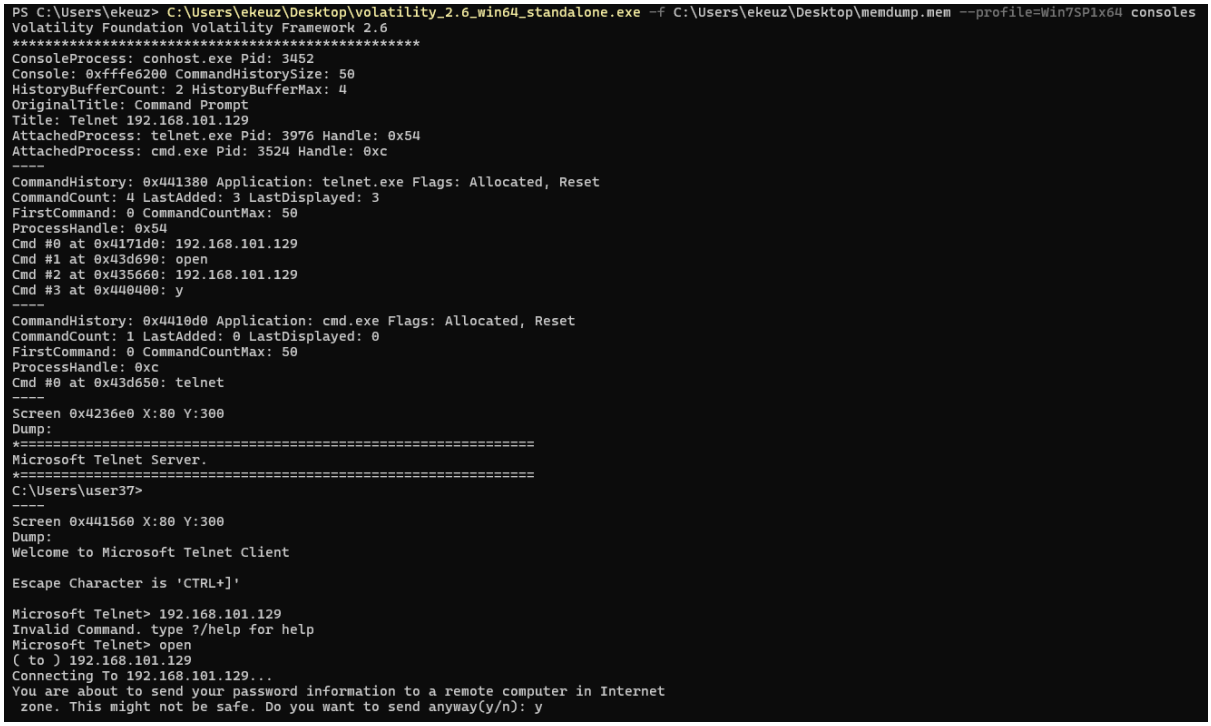
Figure 17 Command line activity

Source Screenshot from Volatility Master analysis

The consoles plugin further confirms interactive use of cmd.exe and telnet.exe. It shows a Telnet session initiated to 192.168.101.129, with open commands and user confirmation (y) to proceed despite a security warning. The screen dump confirms a successful Telnet connection with access to C:\Users\user37>, indicating potential unauthorized remote access. This

evidence suggests manual intrusion or lateral movement. Combined with the cmdscan results, this strongly indicates attacker remote access activity.

Figure 18 Active TELNET session



Source Screenshot from Volatility Master analysis

7.2.2 User Activity Tracking

The userassist plugin tracks executed programs through the Windows registry. The command shows the executed programs by the Sales and Administrator accounts. From the report, some programs launched from the Sales account suggest possible suspicious activity. Notably, the programs and their last updated timestamps include:

- Microsoft Windows Remote Desktop - 2024-06-18 10:28:22 UTC
- Chrome - 2024-06-18 10:46:56 UTC
- cmd - 2024-06-18 10:49:04 UTC
- magnify.exe - 2024-06-18 10:28:22 UTC

7.2.3 File Objects and Data Recovered

To retrieve file data, the filescan and clipboard plugin in Volatility were used. The filescan command produced a large amount of system files along with their access permissions and the associated device paths. Most of these files were linked to the Sales user account, but nothing suspicious was identified in the filescan or clipboard command results. The figure below shows the clipboard contents of the machine.

Figure 19 Clipboard data

```
PS C:\Users\ekeuz> C:\Users\ekeuz\Desktop\volatility_2.6_win64_standalone.exe -f C:\Users\ekeuz\Desktop\memdump.mem --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6
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
```

Source Screenshot from Volatility Master analysis

7.2.4 Network Connections

The netscan plugin revealed both active and closed network connections. Notably, telnet.exe (PID 3976) has an established connection to 192.168.101.129:23, confirming a Telnet session. Additionally, wlmail.exe shows multiple connections, including to port 143 (IMAP), indicating email access. Chrome.exe had a closed HTTPS connection, and numerous svchost.exe processes are listening on common ports. These results support earlier evidence of remote access and user activity, particularly through Telnet.

Figure 20 Active and Closed network activities

```
PS C:\Users\ekeuz> C:\Users\ekeuz\Desktop\volatility_2.6_win64_standalone.exe -f C:\Users\ekeuz\Desktop\memdump.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7c7546b0         TCPv4    192.168.101.128:49267          192.168.101.129:143  CLOSED           1744     wlmail.exe
0x7dacadf0         UDPv4    0.0.0.0:52633                  *:*                                   140092   hZ             2024-06-18 10:47:28 UTC+0000
0x7daea5b0         UDPv4    0.0.0.0:51255                  *:*                                   1052     svchost.exe    2024-06-18 10:48:04 UTC+0000
0x7dd85010         UDPv4    0.0.0.0:58368                  *:*                                   140092   hZ             2024-06-18 10:47:29 UTC+0000
0x7de73010         UDPv4    0.0.0.0:0                      *:*                                   1932     svchost.exe    2024-06-18 10:14:32 UTC+0000
0x7de74ec0         UDPv4    0.0.0.0:0                      *:*                                   1932     svchost.exe    2024-06-18 10:14:32 UTC+0000
0x7de74ec0         UDPv6    :::0                           *:*                                   1932     svchost.exe    2024-06-18 10:14:32 UTC+0000
0x7de81010         UDPv4    0.0.0.0:5355                   *:*                                   1052     svchost.exe    2024-06-18 10:59:31 UTC+0000
0x7dff0220         UDPv4    0.0.0.0:0                      *:*                                   1744     wlmail.exe     2024-06-18 10:31:10 UTC+0000
0x7dff0220         UDPv6    :::0                           *:*                                   1744     wlmail.exe     2024-06-18 10:31:10 UTC+0000
0x7e100440         UDPv4    0.0.0.0:500                    *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e100440         UDPv6    :::500                         *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e1008f0         UDPv4    0.0.0.0:4500                   *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e1008f0         UDPv6    :::4500                        *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e101la0         UDPv4    0.0.0.0:500                    *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e104ec0         UDPv4    0.0.0.0:4500                   *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e119830         UDPv4    0.0.0.0:0                      *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e141c40         UDPv4    0.0.0.0:0                      *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e141c40         UDPv6    :::0                           *:*                                   960      svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e3bd840         UDPv4    192.168.101.128:137            *:*                                   4        System         2024-06-18 10:14:31 UTC+0000
0x7e3de520         UDPv4    0.0.0.0:0                      *:*                                   1052     svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7e3de520         UDPv6    :::0                           *:*                                   1052     svchost.exe    2024-06-18 10:14:31 UTC+0000
0x7de0d670         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        560      services.exe
0x7de0d670         TCPv6    :::49156                       :::0                 LISTENING        560      services.exe
0x7de73bd0         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        1932     svchost.exe
0x7de73bd0         TCPv6    :::49157                       :::0                 LISTENING        1932     svchost.exe
0x7de73d70         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        1932     svchost.exe
0x7df243f0         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING        576      lsass.exe
0x7df4f960         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING        576      lsass.exe
0x7df4f960         TCPv6    :::49158                       :::0                 LISTENING        576      lsass.exe
0x7e011650         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        960      svchost.exe
0x7e011650         TCPv6    :::49154                       :::0                 LISTENING        960      svchost.exe
0x7e1ea010         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x7e1ea010         TCPv6    :::445                         :::0                 LISTENING        4        System
0x7e1eaef0         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        560      services.exe
0x7e24c010         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        788      svchost.exe
0x7e24c010         TCPv6    :::135                         :::0                 LISTENING        788      svchost.exe
0x7e24ed30         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        788      svchost.exe
0x7e2565c0         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        456      wininit.exe
0x7e25b8c0         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        456      wininit.exe
0x7e25b8c0         TCPv6    :::49152                       :::0                 LISTENING        456      wininit.exe
0x7e284460         TCPv4    192.168.101.128:139            0.0.0.0:0            LISTENING        4        System
0x7e2ab010         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        868      svchost.exe
0x7e2ab470         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        868      svchost.exe
0x7e2ab470         TCPv6    :::49153                       :::0                 LISTENING        868      svchost.exe
0x7e3f79c0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        960      svchost.exe
0x7dc0d480         TCPv4    -:0                            232.88.139.26:0      CLOSED           1468     WLIDSVC.EXE
0x7dc6acf0         TCPv4    -:0                            56.11.225.24:0       CLOSED           1744     wlmail.exe
0x7dedd090         TCPv4    192.168.101.128:49266          192.168.101.129:23   ESTABLISHED      3976     telnet.exe
0x7e1d2450         TCPv6    -:0                            e858:8b1a:80fa:ffff:e858:8b1a:80fa:ffff:0 CLOSED          4        System
0x7e1e4960         TCPv4    192.168.101.128:49184          192.168.101.129:143  ESTABLISHED      1744     wlmail.exe
0x7e4d4530         UDPv4    0.0.0.0:5355                   *:*                                   1052     svchost.exe    2024-06-18 10:59:31 UTC+0000
0x7e4d4530         UDPv6    :::5355                        *:*                                   1052     svchost.exe    2024-06-18 10:59:31 UTC+0000
0x7e4fbe40         UDPv4    192.168.101.128:138            *:*                                   4        System         2024-06-18 10:14:31 UTC+0000
0x7e5c5010         UDPv6    ::1:49479                      *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7efead90         UDPv4    0.0.0.0:0                      *:*                                   1744     wlmail.exe     2024-06-18 10:31:00 UTC+0000
0x7efead90         UDPv6    :::0                           *:*                                   1744     wlmail.exe     2024-06-18 10:31:00 UTC+0000
0x7f21d270         UDPv4    127.0.0.1:60757                *:*                                   1744     wlmail.exe     2024-06-18 10:30:36 UTC+0000
0x7f2299b0         UDPv4    0.0.0.0:64857                  *:*                                   140092   hZ             2024-06-18 10:47:59 UTC+0000
0x7f2f0920         UDPv4    0.0.0.0:0                      *:*                                   1744     wlmail.exe     2024-06-18 10:31:10 UTC+0000
0x7f536910         UDPv4    127.0.0.1:56060                *:*                                   1744     wlmail.exe     2024-06-18 10:34:51 UTC+0000
0x7f540dc0         UDPv4    0.0.0.0:0                      *:*                                   1744     wlmail.exe     2024-06-18 10:31:00 UTC+0000
0x7f0baaf0         TCPv4    -:49242                        142.250.200.14:443   CLOSED           1036     chrome.exe
0x7f3fbc20         TCPv4    192.168.101.128:49265          192.168.101.129:143  CLOSED           1744     wlmail.exe
0x7fc06d70         UDPv4    127.0.0.1:49481                *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7fc08300         UDPv4    192.168.101.128:1900           *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7fc08450         UDPv6    ::1:1900                       *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7fc09750         UDPv4    127.0.0.1:1900                 *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7fc125c0         UDPv4    192.168.101.128:49480          *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7fe6cc20         UDPv6    fe80::d8a0:500b:8cc3:eb6f:1900 *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
0x7fe6d010         UDPv6    fe80::d8a0:500b:8cc3:eb6f:49478 *:*                                   536      svchost.exe    2024-06-18 10:16:32 UTC+0000
```

Source Screenshot from Volatility Master analysis

7.3 Detailed Network Analysis

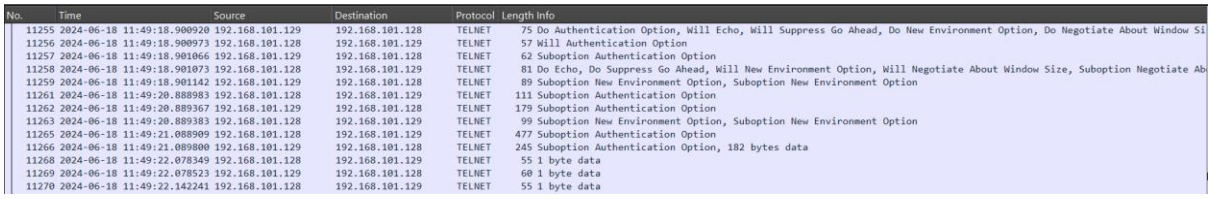
The provided pcap evidence file contains over 11,000 captured connections. These connections, which are to different destination IP addresses, have the machine's IP address (192.168.101.128) as the source IP. Some of the connection protocol types observed include TCP, TELNET, SMTP, DNS, and HTTP. Some of this information is scrambled for security reasons. The source machine (192.168.101.128) made connections to multiple different destinations. For example, one connection was made to IP address 142.250.200.42, which was discovered to belong to Google. Additionally, some connections were found to be related to Windows updates.

To further investigate the misuse case identified in the autopsy investigation, this pcap investigation will focus only few relevant protocol connections. Wireshark was used to filter DNS and SMTP connections to concentrate on the key aspects of the investigation and to support the misuse case identified in the autopsy.

7.3.0 Recent Network Activities

The pcap evidence file analysis in Wireshark suggests potential malicious activity on the machine. A series of Telnet and TCP protocol connections were observed between the source machine (IP 192.168.101.228) and a destination machine (IP 129.168.101.129). These connections occurred from 2024-06-18 11:49:18 to 2024-06-18 11:49:28. Telnet is an insecure, text-based virtual terminal protocol used to connect to other devices.

Figure 21 Telnet packet capture



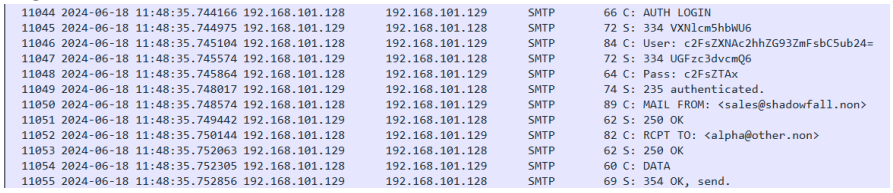
No.	Time	Source	Destination	Protocol	Length	Info
11255	2024-06-18 11:49:18.900920	192.168.101.129	192.168.101.128	TELNET	75	Do Authentication Option, Will Echo, Will Suppress Go Ahead, Do New Environment Option, Do Negotiate About Window Si
11256	2024-06-18 11:49:18.900973	192.168.101.128	192.168.101.129	TELNET	57	Will Authentication Option
11257	2024-06-18 11:49:18.901066	192.168.101.129	192.168.101.128	TELNET	62	Suboption Authentication Option
11258	2024-06-18 11:49:18.901073	192.168.101.128	192.168.101.129	TELNET	81	Do Echo, Do Suppress Go Ahead, Will New Environment Option, Will Negotiate About Window Size, Suboption Negotiate Ab
11259	2024-06-18 11:49:18.901142	192.168.101.129	192.168.101.128	TELNET	89	Suboption New Environment Option, Suboption New Environment Option
11261	2024-06-18 11:49:20.888983	192.168.101.128	192.168.101.129	TELNET	111	Suboption Authentication Option
11262	2024-06-18 11:49:20.889367	192.168.101.129	192.168.101.128	TELNET	179	Suboption Authentication Option
11263	2024-06-18 11:49:20.889383	192.168.101.128	192.168.101.129	TELNET	99	Suboption New Environment Option, Suboption New Environment Option
11265	2024-06-18 11:49:21.088909	192.168.101.128	192.168.101.129	TELNET	477	Suboption Authentication Option
11266	2024-06-18 11:49:21.089800	192.168.101.129	192.168.101.128	TELNET	245	Suboption Authentication Option, 182 bytes data
11268	2024-06-18 11:49:22.078349	192.168.101.128	192.168.101.129	TELNET	55	1 byte data
11269	2024-06-18 11:49:22.078523	192.168.101.128	192.168.101.129	TELNET	60	1 byte data
11270	2024-06-18 11:49:22.142241	192.168.101.128	192.168.101.129	TELNET	55	1 byte data

Source Screenshot from Wireshark pcap evidence analysis

The investigation also revealed that the machine was used to access various websites, possibly for learning about steganography, for example, at 2024-06-18 11:48:05, a query was made to springeropen.com. Additionally, multiple visits were made to Google and other Google related domains. The first Google query occurred at 2024-06-18 11:46:58, and the last visit was at 2024-06-18 11:48:05. Other websites visited included tutorialspoint.com (at 2024-06-18 11:47:32) and freecodecamp.org (at 2024-06-18 11:47:57).

By examining the SMTP protocol, it was found that there was a login authentication at 2024-06-18 11:48:35, followed by email communication between sales@shadowfall.non and alpha@other.non, as seen in the autopsy report.

Figure 22 Email communications

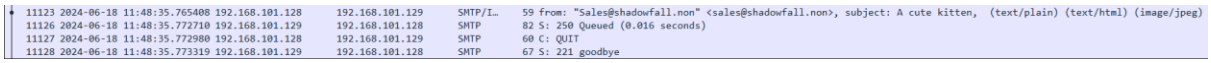


No.	Time	Source	Destination	Protocol	Length	Info
11044	2024-06-18 11:48:35.744166	192.168.101.128	192.168.101.129	SMTP	66	C: AUTH LOGIN
11045	2024-06-18 11:48:35.744975	192.168.101.129	192.168.101.128	SMTP	72	S: 334 VXNlcm5hbWU6
11046	2024-06-18 11:48:35.745104	192.168.101.128	192.168.101.129	SMTP	84	C: User: c2FsZXNAc2hhZG93ZmFsbC5ub24=
11047	2024-06-18 11:48:35.745574	192.168.101.129	192.168.101.128	SMTP	72	S: 334 UGFzc3dvcmQ6
11048	2024-06-18 11:48:35.745864	192.168.101.128	192.168.101.129	SMTP	64	C: Pass: c2FsZTAx
11049	2024-06-18 11:48:35.748017	192.168.101.129	192.168.101.128	SMTP	74	S: 235 authenticated.
11050	2024-06-18 11:48:35.748574	192.168.101.128	192.168.101.129	SMTP	89	C: MAIL FROM: <sales@shadowfall.non>
11051	2024-06-18 11:48:35.749442	192.168.101.129	192.168.101.128	SMTP	62	S: 250 OK
11052	2024-06-18 11:48:35.750144	192.168.101.128	192.168.101.129	SMTP	82	C: RCPT TO: <alpha@other.non>
11053	2024-06-18 11:48:35.752063	192.168.101.129	192.168.101.128	SMTP	62	S: 250 OK
11054	2024-06-18 11:48:35.752305	192.168.101.128	192.168.101.129	SMTP	60	C: DATA
11055	2024-06-18 11:48:35.752856	192.168.101.129	192.168.101.128	SMTP	69	S: 354 OK, send.

Source Screenshot from Wireshark pcap evidence analysis

The email with the subject 'A cute kitten' was sent from sales@shadowfall.non to alpha@other.non, which was captured in the network traffic associated with the source IP 192.168.101.228.

Figure 23 Emails communication



Source Screenshot from Wireshark pcap evidence analysis

7.3.1 Website Visited

As noted in the autopsy investigation, the DNS protocol from the pcap evidence file shows that the machine accessed websites such as google.com, freecodecamp.org, tutorialspoint.com, and springeropen.com. Based on the autopsy evidence, the purpose of these web visits appears to be related to learning Kali Linux and using steganography to hide data. Furthermore, the SMTP protocol confirms that the emails shown in the autopsy report were sent, and these communications were captured in the network traffic.

8.0 Timeline of Events

8.1 Autopsy Timeline of Events

2024-06-18 10:01:06 BST: Research account accessed Google.com and searched "how to install Kali Linux."

2024-06-18 10:01:45 BST: Research account accessed Google.com and searched "steganography in files."

2024-06-18 10:01:50 BST: Research account accessed the domain freecodecamp.org to learn about steganography.

2024-06-18 10:54:46 BST: **research@shadowfall.non** sent a plain test email "TEST" with the subject "TEST" to **itsupport@shadowfall.non**.

2024-06-18 10:56:27 BST: **itsupport@shadowfall.non** responded to the email with "REPLY."

2024-06-18 11:07:01 BST: **research@shadowfall.non** sent a plaintext email "Expect a follow up soon" with the subject "Just checking in" to **alpha@other.non**.

2024-06-18 11:27:54 BST: Sales account got created and immediately accessed Tutorialspoint to potentially learn how to use Kali Linux.

2024-06-18 11:27:54 BST: Sales account accessed the domain tutorialspoint.com (an online educational provider) to learn Kali Linux.

2024-06-18 11:34:52 BST: **sales@shadowfall.non** sent a plaintext email "TEST" with the subject "TEST" to **itsupport@shadowfall.non** (no response).

2024-06-18 11:47:27 BST: Sales account accessed Google.com and searched "how to use Kali Linux."

2024-06-18 11:47:52 BST: Sales account accessed Google.com and searched "how to use steganography to hide data."

2024-06-18 11:47:52 BST: Sales account accessed Springeropen for the academic journal "An efficient steganographic technique for hiding data."

2024-06-18 11:48:06 BST: Sales account accessed the website springeropen.com (academic journal) for "An efficient steganographic technique for hiding data."

2024-06-18 11:48:35 BST: **sales@shadowfall.non** sent an email with the subject "A cute kitten" and attached the "kitten.jpg" file to **alpha@other.non**.

2024-06-18 11:51:13 BST: Sales account deleted the "New Rich Text Document.rtf" (created and accessed on 2024-06-18 at 11:50:51 BST).

2024-06-18 11:52:29 UTC (2024-06-18 11:52:29 local time): Memory capture timestamp.

8.2 Memory Timeline of Events

2024-06-18 10:28:22 UTC: **Microsoft Windows Remote Desktop** is launched from the Sales account.

2024-06-18 10:46:56 UTC: **Chrome.exe** is running with zero threads (unusual behaviour).

2024-06-18 10:49:04 UTC: **cmd.exe** (PID 3524) is executed, possibly for manual commands or scripts. Also, **telnet.exe** (PID 3976) is executed, indicating potential remote access.

2024-06-18 10:51:19 UTC: **Notepad** is launched from the Sales account.

2024-06-18 10:49:06 UTC: **telnet.exe** attempts to connect to IP address **192.168.101.129**, suggesting active Telnet session.

8.3 Network Timeline of Events

2024-06-18 11:46:58: The First Google query made from the source machine.

2024-06-18 11:47:32: Visit to tutorialspoint.com from the source machine.

2024-06-18 11:47:57: Visit to freecodecamp.org from the source machine.

2024-06-18 11:48:05: Query made to springeropen.com from the source machine. Also, the last Google query made from the source machine.

2024-06-18 11:49:18 to 2024-06-18 11:49:28: Series of Telnet and TCP protocol connections between the source machine (IP 192.168.101.228) and the destination machine (IP 129.168.101.129).

2024-06-18 11:49:30: Email communication between sales@shadowfall.non and alpha@other.non, with the subject "A cute kitten," sent from the source machine as seen in the SMTP protocol capture.

9.0 Conclusion

In conclusion, the investigation into the potential unauthorized actions of ACME Ltd's Finance Director reveals suspicious activities which potentially breached company policy. This forensic investigation uncovered the misuse of company device for malicious activities such as the visit of websites that are not work related. The evidence also revealed unsecured activities, such as the use of Telnet for remote access. Also, suspicious email communications to an external email address were also uncovered. Furthermore, the device user was involved in learning about steganography techniques, which could be an indication of attempts to conceal data before transfer. These findings provide strong evidence of misconduct and highlight significant security vulnerabilities, which will inform the company's future actions to safeguard its critical data.

References

. *IE40 Trojan.* [online]. Available from: https://answers.microsoft.com/en-us/windows/forum/all/i-found-these-applications-installed-in-windows-7/a4df4b0a-717c-4484-bafe-5d37ef628893

CONSTANTINIDES, M. and QUERCIA, D., 2022. Good intentions, bad inventions: How employees judge pervasive technologies in the workplace. *IEEE Pervasive Computing,* 22(1), pp. 69–76.

NAYAK, S.C., TIWARI, V. and SAMANTHULA, B.K., 2023. Review of ransomware attacks and a data recovery framework using autopsy digital forensics platform. *2023 IEEE 13th annual computing and communication workshop and conference (CCWC).* 2023. IEEE, pp. 605.

SOEPENO, R., 2023. Wireshark: An Effective Tool for Network Analysis. *CYBV-Introd.Methods Netw.Anal,* , pp. 1–15.