ACME BANK DIGITAL FORENSIC INVESTIGATION TENOR REPORT

Les Grint Student No: 10752013

Digital Forensic and Malware Analysis Comp 3012

Introduction

This tenor report outlines a comprehensive plan for conducting a digital forensic investigation, in response to the discovery of a keylogger attached to a staff PC within Acme, a prominent bank in the United Kingdom. The objective of the digital forensic investigation is to examine and analyse evidence, uncover the cause of the incident, identify potential suspects, and provide actionable, verifiable insights (Quick & Choo, 2018) to aid Acme Bank in its decision-making process regarding the execution, of an official digital forensic investigation.

The structure of the report is designed to guide Acme through the key stages of a digital forensic investigation, which include collection, examination, analysis and presentation (Horsman & Sunde, 2022). Each phase is meticulously outlined to highlight the methodologies, techniques, and tools employed to ensure the integrity, admissibility, and reliability of the evidence collected.

Furthermore, the report addresses operational trade-offs, such as cost considerations and resource allocation, to assist Acme in making informed decisions regarding the scope and execution of the investigation. By providing insights into these trade-offs, Acme can strike a balance between the need for operational thoroughness and practical constraints.

The primary purpose of this tender is to equip Acme with a comprehensive understanding of the investigative process. By explaining in detail, the intricacies of a digital forensic investigation, this report enables Acme to make an informed decision regarding their strategic direction, ultimately determining whether to proceed with an official forensic investigation.

Forensic Acquisition

Identification

Strategy

Given the potential impact on Acme Banks operations an initial covert approach to this forensic investigation is necessary. Seizing the entire HQ's computers indiscriminately isn't operationally practical for the bank or the forensic investigation. A 1TB bit-for-bit image averages 4-5 hours and takes 4-5 days to examine (CER, 2014), multiplied by the quantity of digital evidence calculates the resource request or operational trade-offs. Additionally, open acknowledgment of the investigation could risks triggering anti-forensic countermeasures by suspects compromising vital evidence.

This investigation will begin by covertly analysing independent factors such as staff vetting, network traffic, company email server data, CCTV footage, server access logs, ISP logs including browser history, company mobile device network provider history, and company chat logs. This investigative approach will reduce the number of potential suspects, reducing the scale of the resource request for seizing equipment, enabling an overt investigation to be conducted and the forensic acquisition of any and all suspect computers, mobile devices, external storage mediums, company phones and the keylogger itself.

Covert

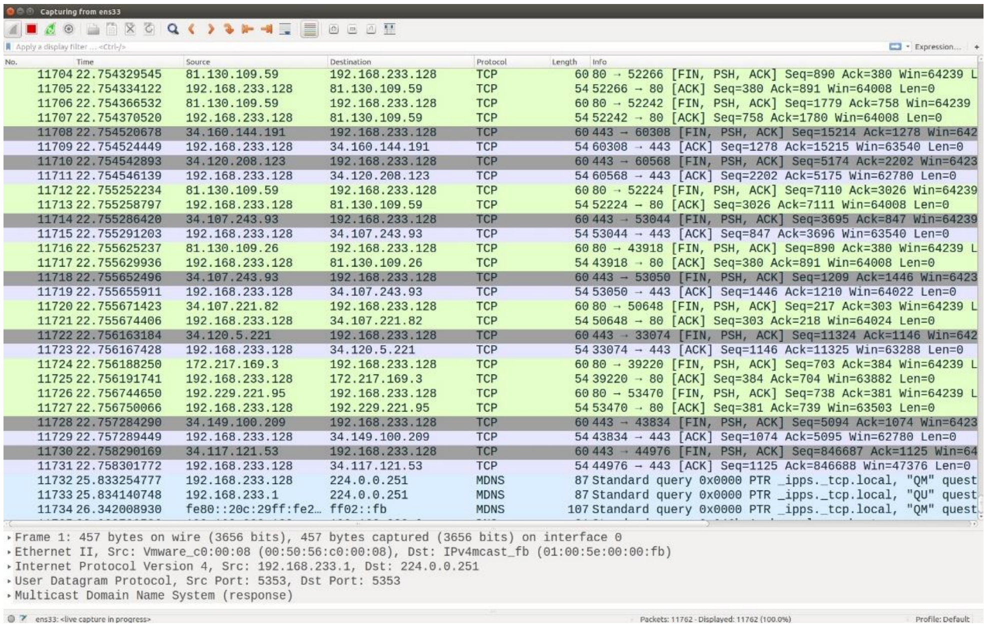
Independent Analysis

A physical examination of the keylogger will be conducted, documenting its type, make and model. The time will be documented and the keylogger will be discreetly reconnected to the compromised PC to maintain covert status. Subsequently the company email servers, chat logs, ISP browser history, and mobile network provider records will be scrutinised for any references to the keylogger. Any corresponding information will be documented, forming an investigative chronology.

HR will be contacted to gather information about changes in employee behaviour, such as unusual working hours or patterns that could indicate suspect activity. Any behavioural insights will be integrated into the investigative chronology.

Surveillance footage from CCTV will be analysed to identify individuals accessing the area where the keylogger was discovered. Server access logs will also be examined to trace user activity on the compromised computer and neighbouring devices, aiming to identify potential suspects or rule out innocent parties from the investigation.

Using Wireshark (Fig.1) a detailed analysis of network traffic patterns will be conducted to uncover any suspicious outbound connections from the compromised PC's IP address, potentially at repeating intervals, that stopped when the keylogger was removed, and restarted once it was reconnected. This analysis will include identifying common data transmission protocols and researching external IP addresses using WHOIS databases to determine ownership. The results will be integrated into the investigative chronology providing essential insight on the keyloggers network activities.



```
No.   Time         Source              Destination       Protocol  Length Info
11704 22.754329545 81.130.109.59       192.168.233.128   TCP        60 80 → 52266 [FIN, PSH, ACK] Seq=890 Ack=380 Win=64239 L
11705 22.754334122 192.168.233.128     81.130.109.59     TCP        54 52266 → 80 [ACK] Seq=380 Ack=891 Win=64008 Len=0
11706 22.754366532 81.130.109.59       192.168.233.128   TCP        60 80 → 52242 [FIN, PSH, ACK] Seq=1779 Ack=758 Win=64239
11707 22.754370520 192.168.233.128     81.130.109.59     TCP        54 52242 → 80 [ACK] Seq=758 Ack=1780 Win=64008 Len=0
11708 22.754520678 34.160.144.191      192.168.233.128   TCP        60 443 → 60308 [FIN, PSH, ACK] Seq=15214 Ack=1278 Win=642
11709 22.754524449 192.168.233.128     34.160.144.191    TCP        54 60308 → 443 [ACK] Seq=1278 Ack=15215 Win=63540 Len=0
11710 22.754542893 34.120.208.123      192.168.233.128   TCP        60 443 → 60568 [FIN, PSH, ACK] Seq=5174 Ack=2202 Win=6423
11711 22.754546139 192.168.233.128     34.120.208.123    TCP        54 60568 → 443 [ACK] Seq=2202 Ack=5175 Win=62780 Len=0
11712 22.755252234 81.130.109.59       192.168.233.128   TCP        60 80 → 52224 [FIN, PSH, ACK] Seq=7110 Ack=3026 Win=64239
11713 22.755258797 192.168.233.128     81.130.109.59     TCP        54 52224 → 80 [ACK] Seq=3026 Ack=7111 Win=64008 Len=0
11714 22.755286420 34.107.243.93       192.168.233.128   TCP        60 443 → 53044 [FIN, PSH, ACK] Seq=3695 Ack=847 Win=64239
11715 22.755291203 192.168.233.128     34.107.243.93     TCP        54 53044 → 443 [ACK] Seq=847 Ack=3696 Win=63540 Len=0
11716 22.755625237 81.130.109.26       192.168.233.128   TCP        60 80 → 43918 [FIN, PSH, ACK] Seq=890 Ack=380 Win=64239 L
11717 22.755629936 192.168.233.128     81.130.109.26     TCP        54 43918 → 80 [ACK] Seq=380 Ack=891 Win=64008 Len=0
11718 22.755652496 34.107.243.93       192.168.233.128   TCP        60 443 → 53050 [FIN, PSH, ACK] Seq=1209 Ack=1446 Win=6423
11719 22.755655911 192.168.233.128     34.107.243.93     TCP        54 53050 → 443 [ACK] Seq=1446 Ack=1210 Win=64022 Len=0
11720 22.755671423 34.107.221.82       192.168.233.128   TCP        60 80 → 50648 [FIN, PSH, ACK] Seq=217 Ack=303 Win=64239 L
11721 22.755674406 192.168.233.128     34.107.221.82     TCP        54 50648 → 80 [ACK] Seq=303 Ack=218 Win=64024 Len=0
11722 22.756163184 34.120.5.221        192.168.233.128   TCP        60 443 → 33074 [FIN, PSH, ACK] Seq=11324 Ack=1146 Win=642
11723 22.756167428 192.168.233.128     34.120.5.221      TCP        54 33074 → 443 [ACK] Seq=1146 Ack=11325 Win=63288 Len=0
11724 22.756188250 172.217.169.3       192.168.233.128   TCP        60 80 → 39220 [FIN, PSH, ACK] Seq=703 Ack=384 Win=64239 L
11725 22.756191741 192.168.233.128     172.217.169.3     TCP        54 39220 → 80 [ACK] Seq=384 Ack=704 Win=63882 Len=0
11726 22.756744650 192.229.221.95      192.168.233.128   TCP        60 80 → 53470 [FIN, PSH, ACK] Seq=738 Ack=381 Win=64239 L
11727 22.756750066 192.168.233.128     192.229.221.95    TCP        54 53470 → 80 [ACK] Seq=381 Ack=739 Win=63503 Len=0
11728 22.757284290 34.149.100.209      192.168.233.128   TCP        60 443 → 43834 [FIN, PSH, ACK] Seq=5094 Ack=1074 Win=6423
11729 22.757289449 192.168.233.128     34.149.100.209    TCP        54 43834 → 443 [ACK] Seq=1074 Ack=5095 Win=62780 Len=0
11730 22.758290169 34.117.121.53       192.168.233.128   TCP        60 443 → 44976 [FIN, PSH, ACK] Seq=846687 Ack=1125 Win=64
11731 22.758301772 192.168.233.128     34.117.121.53     TCP        54 44976 → 443 [ACK] Seq=1125 Ack=846688 Win=47376 Len=0
11732 25.833254777 192.168.233.128     224.0.0.251       MDNS       87 Standard query 0x0000 PTR _ipps._tcp.local, "QM" quest
11733 25.834140748 192.168.233.1       224.0.0.251       MDNS       87 Standard query 0x0000 PTR _ipps._tcp.local, "QU" quest
11734 26.342008930 fe80::20c:29ff:fe2… ff02::fb          MDNS      107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" quest

▸ Frame 1: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0
▸ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
▸ Internet Protocol Version 4, Src: 192.168.233.1, Dst: 224.0.0.251
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (response)

ens33: <live capture in progress>          Packets: 11762 · Displayed: 11762 (100.0%)          Profile: Default
```

(Fig.1)

This covert independent analysis phase will efficiently identify potential suspects and devices, reducing the total resource request whilst discreetly gathering crucial evidence. The IP based network traffic analysis will reveal the interval the keylogger transmits data to the suspect server (Clarke et al., 2017). Using Wireshark, filtering by the IP address of the compromised PC, network traffic will be monitored and saved as a Pcap file. When the keylogger transmission begins the overt phase of the investigation will be conducted seizing all suspect equipment, timing for the best possible chance of retrieving digital artifacts from the volatile storage of the compromised computer.

Overt

Preservation

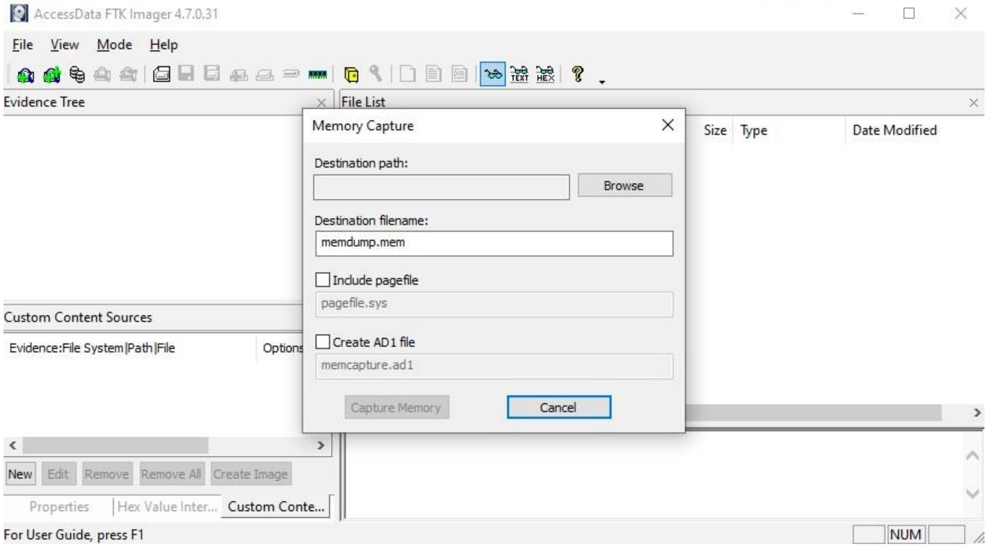
Documenting The Scene

Upon seizing the suspect equipment at ACME Bank, the forensic team will initiate a meticulous documentation process, a fundamental aspect of the forensic methodology. The preservation of evidence begins with the creation of a grid line system, encompassing the scene to provide a comprehensive identification of electronic assets. Cables are marked, and the scene is photographed from various angles, capturing long, mid, and close-range views. This documentation highlights evidenced items in context with their surroundings whilst capturing essential information such as serial numbers, marked cable connections and USB ports (Sammons, 2015).

Order of Volitivity

When a device is powered, conducting a live examination presents a valuable opportunity to document network connections and active programs. At this stage, with the keylogger transmitting data, digital artifacts may be in the computer's volatile memory. Due to the volatile nature of RAM, immediate action will be taken to capture a memory image on-site using FTK Imager (Fig.2) while the computer remains powered, before it is lost due to system shutdown or manipulation (Vidas, 2007).

Additional checks will be conducted for signs of unpowered full drive encryption, if encryption is detected, a logical copy of the decrypted drives will be made while the device is powered. Subsequently, the power cable will be safely disconnected from the computer preserving the state of the system (Kävrestad, 2017).



Memory Capture

Destination path:

Destination filename: memdump.mem

☐ Include pagefile

pagefile.sys

☐ Create AD1 file

memcapture.ad1

(Fig.2)

Chain of Custody

To uphold the integrity and admissibility of acquired evidence, measures will be implemented to maintain a detailed chain of custody. Following the removal of evidence items from ACME Bank, detailed information will be recorded for each item acquired. This includes its location in the scene, physical condition, type, make, model, serial number, name of discoverer, name of collector, method of collection, power status, and network status (Sammons, 2015).

For evidence to be deemed credible the chain of custody must be maintained and enforced. From the point of acquisition at ACME bank, the name of the individual collecting the evidence is recorded, and that evidence remains in that individual’s custody until it’s checked into secure storage for the duration of the investigation. Any movements or transfer of the evidence, whether for analysis or storage, are tracked and logged. This detailed account ensures the integrity and admissibility of evidence in legal proceedings (Sammons, 2015).

Transport

When transporting evidence from ACME to the forensic labs, measures will be implemented to prevent alteration and contamination. Magnetic drives are susceptible to electromagnetism and static electricity, which can corrupt data or render the drive inoperable (Gurkok, 2017). Additionally, powered mobile devices are at risk to incoming signals that could modify data or delete evidence (Daniel & Daniel, 2012).

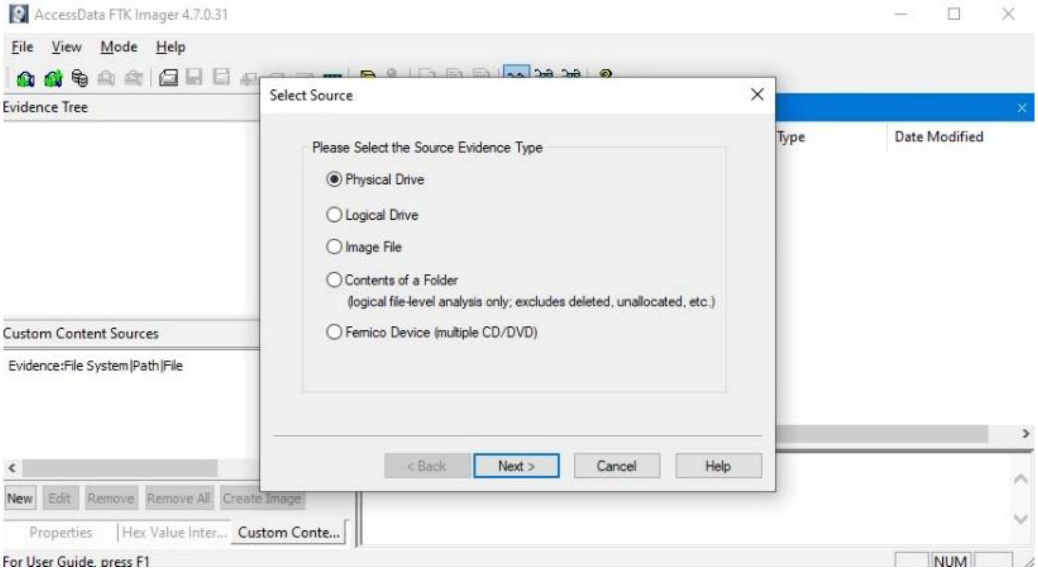
To mitigate these risks, evidence items will be placed in antistatic Faraday bags during transportation. These bags shield the devices from electromagnetic interference and static electricity, safeguarding the integrity of the data stored on magnetic drives and prevents unauthorised access to powered mobile devices. Adherence to these transportation protocols preserves the integrity of the evidence, ensuring its reliability for forensic analysis (Daniel & Daniel, 2012).

Collection

Computers

In accordance with ACPO guidelines (AF, 2023) measures will be implemented to eliminate the possibility of modifying or contaminating digital evidence, rendering it inadmissible. A write blocker will be connected to each drive blocking potential write signals and preserving its integrity. Subsequently, FTK imager (Fig.3) will be used to create a forensically sound bitstream image of the digital evidence (Kävrestad, 2017).

To ensure the integrity of all acquired bitstream images and their fidelity to the original evidence, a hash comparison will be conducted. Hashing allows a variable length input to be output as a fixed length, and is used to maintain integrity through the avalanche effect (Upadhyay et al., 2022). Initially, the digital evidence will be hashed, generating a unique cryptographic hash value. Then the copy will be hashed resulting in a second hash value, these hash values will undergo comparison, if they match, it confirms that the bitstream image is bit-for-bit identical to the original. This is an essential benchmark known as the forensic gold standard (Daniel & Daniel, 2012).



Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

(Fig.3)

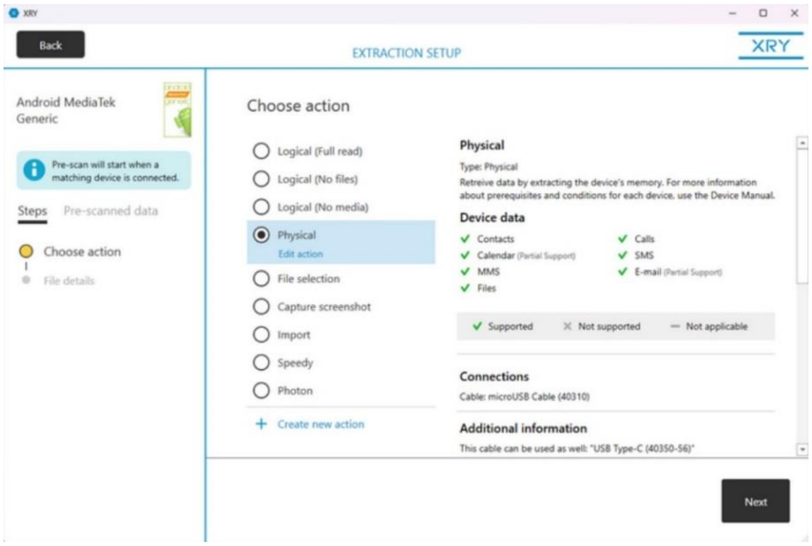
Keylogger

FTK imager (Fig.3) will be used to create a bitstream image of the keylogger, implementing a write blocker to prevent alterations to the data (Kävrestad, 2017) with the resulting image undergoing the same hashing process and the same comparison. This procedure ensures that the integrity of the digital evidence is maintained, adhering to best practices in the digital forensics process (Daniel & Daniel, 2012).

Mobile Device

To ensure the preservation of encryption keys crucial for accessing data on mobile devices, they must remain powered on in an AFU (After First Use) state. This prevents the loss of encryption keys, which occurs when the device reverts to a BFU (Before First Use) state upon losing power (Owen & Thomas, 2011).

For the acquisition of data from mobile devices, forensic software XRY (Fig.4) will be used to perform a physical acquisition bypassing the devices operating system granting access to the device image (Owen & Thomas, 2011). If a physical image isn’t possible, XRY will be used to acquire a logical image based on the manufacturer's drivers, ensuring all data retrievable by the driver is captured, maintaining the integrity of the evidence (Daniel & Daniel, 2012).



Android MediaTek
Generic

Pre-scan will start when a matching device is connected.

Steps   Pre-scanned data

Choose action
File details

Choose action

○ Logical (Full read)
○ Logical (No files)
○ Logical (No media)
● Physical
Edit action
○ File selection
○ Capture screenshot
○ Import
○ Speedy
○ Photon
+ Create new action

Physical

Type: Physical
Retreive data by extracting the device's memory. For more information about prerequisites and conditions for each device. use the Device Manual.

Device data

✓ Contacts	✓ Calls
✓ Calendar (Partial Support)	✓ SMS
✓ MMS	✓ E-mail (Partial Support)
✓ Files	

✓ Supported   ✕ Not supported   — Not applicable

Connections

Cable: microUSB Cable (40310)

Additional information

This cable can be used as well: "USB Type-C (40350-56)"

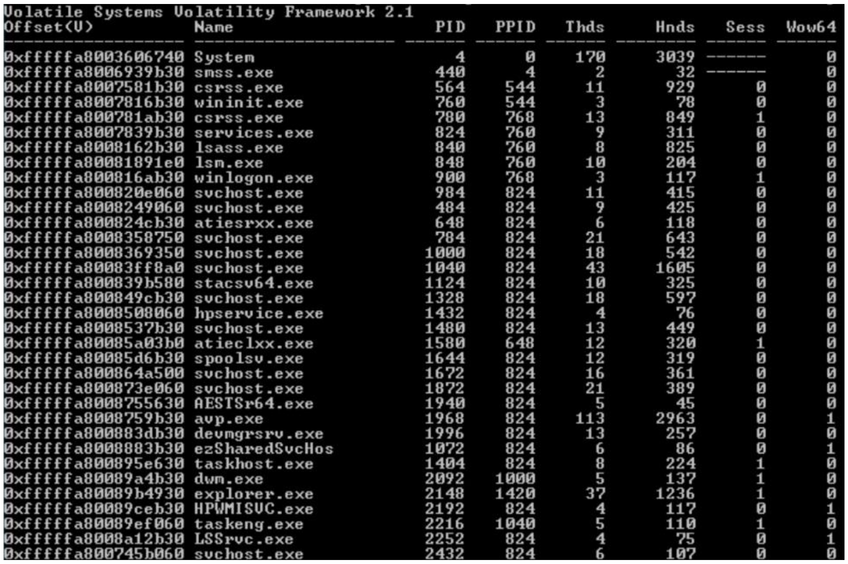
(Fig.4)

Examination and Analysis

Examination

Memory dump

The memory dump extracted from the compromised computer's volatile memory will be analysed using specialised memory forensic analysis tool Volatility (Fig.5). In addition to potentially extracting the transmissions destination IP address, the analysis will focus on identifying any keystroke data present in the memory dump (Nguyen-Phuoc, 2021). If keystroke data is detected, it will confirm the suspect IP address is the destination for the transmitted data, making it malicious in nature.



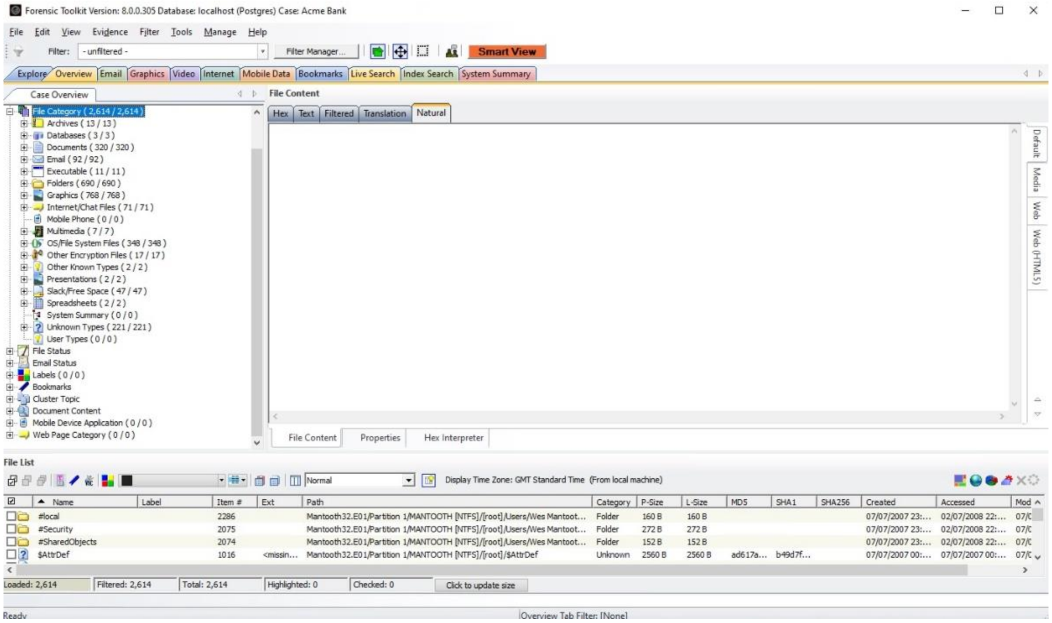
```
Volatile Systems Volatility Framework 2.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64
------------------ -------------------- ------ ------ ------ -------- ------ ------
0xfffffa8003606740 System                    4      0    170     3039 ------      0
0xfffffa8006939b30 smss.exe                440      4      2       32 ------      0
0xfffffa8007581b30 csrss.exe               564    544     11      929      0      0
0xfffffa8007816b30 wininit.exe             760    544      3       78      0      0
0xfffffa800781ab30 csrss.exe               780    768     13      849      1      0
0xfffffa8007839b30 services.exe            824    760      9      311      0      0
0xfffffa8008162b30 lsass.exe               840    760      8      825      0      0
0xfffffa80081891e0 lsm.exe                 848    760     10      204      0      0
0xfffffa800816ab30 winlogon.exe            900    768      3      117      1      0
0xfffffa800820e060 svchost.exe             984    824     11      415      0      0
0xfffffa8008249060 svchost.exe             484    824      9      425      0      0
0xfffffa800824cb30 atiesrxx.exe            648    824      6      118      0      0
0xfffffa8008358750 svchost.exe             784    824     21      643      0      0
0xfffffa8008369350 svchost.exe            1000    824     18      542      0      0
0xfffffa80083ff8a0 svchost.exe            1040    824     43     1605      0      0
0xfffffa800839b580 stacsv64.exe           1124    824     10      325      0      0
0xfffffa800849cb30 svchost.exe            1328    824     18      597      0      0
0xfffffa8008508060 hpservice.exe          1432    824      4       76      0      0
0xfffffa8008537b30 svchost.exe            1480    824     13      449      0      0
0xfffffa80085a03b0 atieclxx.exe           1580    648     12      320      1      0
0xfffffa80085d6b30 spoolsv.exe            1644    824     12      319      0      0
0xfffffa800864a500 svchost.exe            1672    824     16      361      0      0
0xfffffa800873e060 svchost.exe            1872    824     21      389      0      0
0xfffffa8008755630 AESTSr64.exe           1940    824      5       45      0      0
0xfffffa8008759b30 avp.exe                1968    824    113     2963      0      1
0xfffffa800883db30 devmgrsrv.exe          1996    824     13      257      0      0
0xfffffa8008883b30 ezSharedSvcHos         1072    824      6       86      0      1
0xfffffa800895e630 taskhost.exe           1404    824      8      224      1      0
0xfffffa80089a4b30 dwm.exe                2092   1000      5      137      1      0
0xfffffa80089b4930 explorer.exe           2148   1420     37     1236      1      0
0xfffffa80089ceb30 HPWMISVC.exe           2192    824      4      117      0      1
0xfffffa80089ef060 taskeng.exe            2216   1040      5      110      1      0
0xfffffa8008a12b30 LSSrvc.exe             2252    824      4       75      0      1
0xfffffa800745b060 svchost.exe            2432    824      6      107      0      0
```

(Fig.5)

Further network analysis will be conducted to identify any other company IP addresses that have connected to the malicious external IP address. A HAS-IP-CONNECTED list will be compiled, documenting all the drives associated with the IPs that have made connections to the malicious address. These findings will be documented and integrated into the investigative chronology, providing valuable insights into the scope of the incident.

Suspect Drive Images

All suspect drive images will undergo comprehensive analysis in FTK (Fig.6), a leading forensic analysis tool known for its ability perform dead analysis to extract evidence from drives without booting them, preventing any alterations to the drive's contents (BCC, 2017). Initially, any compressed folders will be decompressed to ensure access to the complete set of files contained within.



Forensic Toolkit Version: 8.0.0.305 Database: localhost (Postgres) Case: Acme Bank

Filter: - unfiltered -

File Category (2,614 / 2,614)
- Archives (13 / 13)
- Databases (3 / 3)
- Documents (320 / 320)
- Email (92 / 92)
- Executable (11 / 11)
- Folders (690 / 690)
- Graphics (768 / 768)
- Internet/Chat Files (71 / 71)
- Mobile Phone (0 / 0)
- Multimedia (7 / 7)
- OS/File System Files (348 / 348)
- Other Encryption Files (17 / 17)
- Other Known Types (2 / 2)
- Presentations (2 / 2)
- Slack/Free Space (47 / 47)
- Spreadsheets (2 / 2)
- System Summary (0 / 0)
- Unknown Types (221 / 221)
- User Types (0 / 0)

File Status
Email Status
Labels (0 / 0)
Bookmarks
Cluster Topic
Document Content
Mobile Device Application (0 / 0)
Web Page Category (0 / 0)

Normal

Display Time Zone: GMT Standard Time (From local machine)

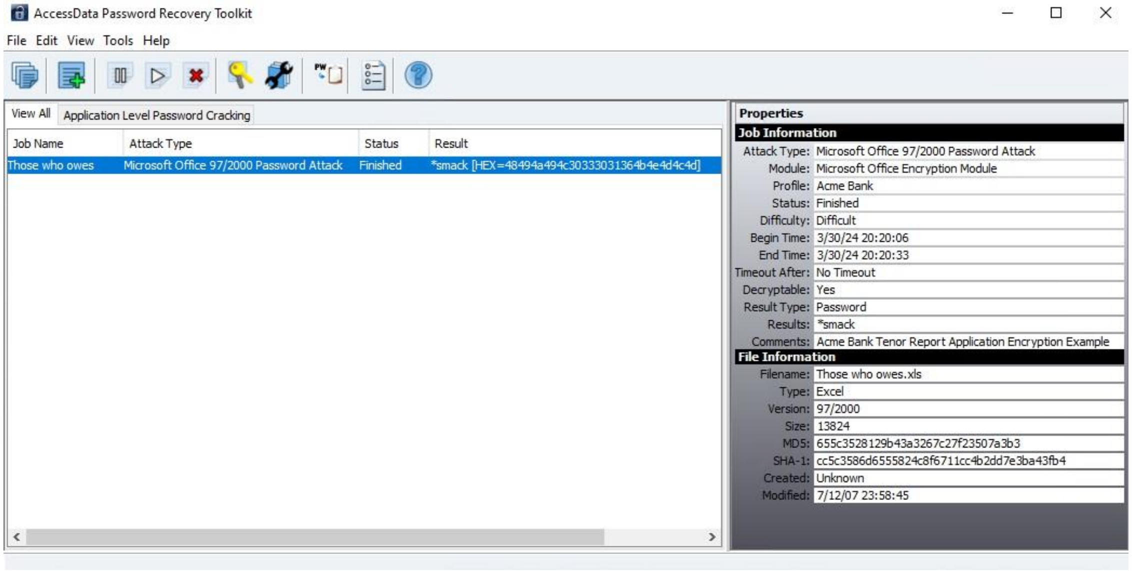
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Mod
□	#local		2286		Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantoot...	Folder	160 B	160 B				07/07/2007 23:...	02/07/2008 22:...	07/C
□	#Security		2075		Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantoot...	Folder	272 B	272 B				07/07/2007 23:...	02/07/2008 22:...	07/C
□	#SharedObjects		2074		Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantoot...	Folder	152 B	152 B				07/07/2007 23:...	02/07/2008 22:...	07/C
□	$AttrDef		1016	<missin...	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/$AttrDef	Unknown	2560 B	2560 B	ad617a...	b49d7f...		07/07/2007 00:...	07/07/2007 00:...	07/C

Loaded: 2,614 | Filtered: 2,614 | Total: 2,614 | Highlighted: 0 | Checked: 0

Ready | Overview Tab Filter: [None]

(Fig.6)

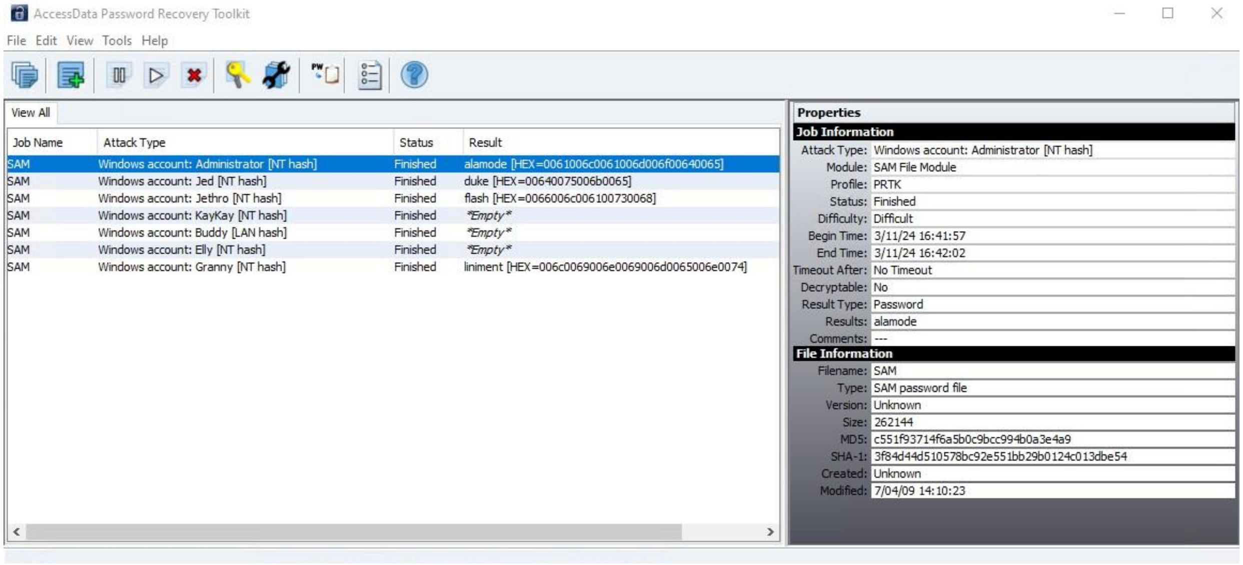
Application-level password-protected files will be accessed using password cracking tool PRTK (Fig.7) which uses a dictionary rule-based approach for decryption (Hranický, 2021). Additionally, system level password-protected files will be accessed using data from the SAM and SYSTEM registry files (Fig.8). While these methodologies can grant access to the files on the drives, there are limitations to their effectiveness against highly complex or strong passwords. In such cases, password cracking may fail.


AccessData Password Recovery Toolkit
File Edit View Tools Help
View All
Application Level Password Cracking

Job Name	Attack Type	Status	Result
Those who owes	Microsoft Office 97/2000 Password Attack	Finished	*smack [HEX=48494a494c3033031364b4e4d4c4d]

Properties	
Job Information	
Attack Type:	Microsoft Office 97/2000 Password Attack
Module:	Microsoft Office Encryption Module
Profile:	Acme Bank
Status:	Finished
Difficulty:	Difficult
Begin Time:	3/30/24 20:20:06
End Time:	3/30/24 20:20:33
Timeout After:	No Timeout
Decryptable:	Yes
Result Type:	Password
Results:	*smack
Comments:	Acme Bank Tenor Report Application Encryption Example
File Information	
Filename:	Those who owes.xls
Type:	Excel
Version:	97/2000
Size:	13824
MD5:	655c3528129b43a3267c27f23507a3b3
SHA-1:	cc5c3586d6555824c8f6711cc4b2dd7e3ba43fb4
Created:	Unknown
Modified:	7/12/07 23:58:45

(Fig.7)


AccessData Password Recovery Toolkit
File Edit View Tools Help
View All

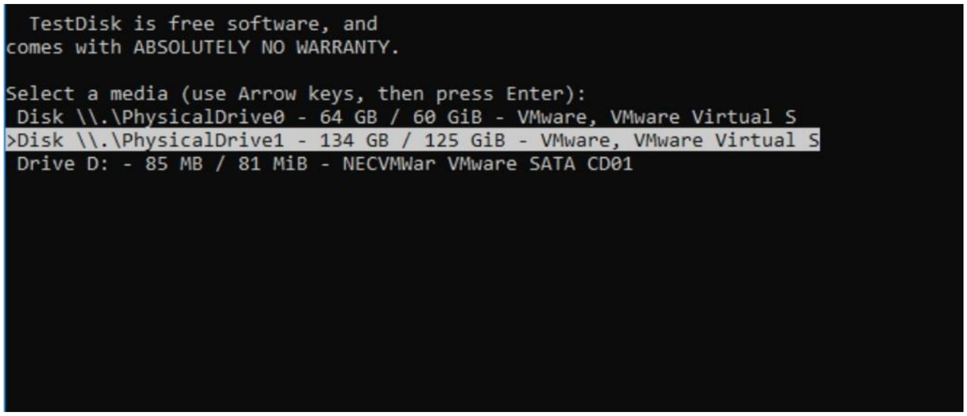
Job Name	Attack Type	Status	Result
SAM	Windows account: Administrator [NT hash]	Finished	alamode [HEX=0061006c0061006d006f00640065]
SAM	Windows account: Jed [NT hash]	Finished	duke [HEX=00640075006b0065]
SAM	Windows account: Jethro [NT hash]	Finished	flash [HEX=0066006c006100730068]
SAM	Windows account: KayKay [NT hash]	Finished	*Empty*
SAM	Windows account: Buddy [LAN hash]	Finished	*Empty*
SAM	Windows account: Elly [NT hash]	Finished	*Empty*
SAM	Windows account: Granny [NT hash]	Finished	liniment [HEX=006c0069006e0069006d0065006e0074]

Properties	
Job Information	
Attack Type:	Windows account: Administrator [NT hash]
Module:	SAM File Module
Profile:	PRTK
Status:	Finished
Difficulty:	Difficult
Begin Time:	3/11/24 16:41:57
End Time:	3/11/24 16:42:02
Timeout After:	No Timeout
Decryptable:	No
Result Type:	Password
Results:	alamode
Comments:	---
File Information	
Filename:	SAM
Type:	SAM password file
Version:	Unknown
Size:	262144
MD5:	c551f93714f6a5b0c9bcc994b0a3e4a9
SHA-1:	3f84d44d510578bc92e551bb29b0124c013dbe54
Created:	Unknown
Modified:	7/04/09 14:10:23

(Fig.8)

Keylogger Image

Using FTK (Fig.6) the keylogger image will be analysed for any signs that indicate a hidden partition, such as differences in advertised storage capacity versus available capacity or inconsistencies in file system analysis. TestDisk (Fig.9) will be used to further examine the USB drive image to detect hidden partitions or encrypted volumes. Passwords for encrypted volumes again can be accessed using password cracking tools such as PRTK (Fig.7) (Hranický, 2021).

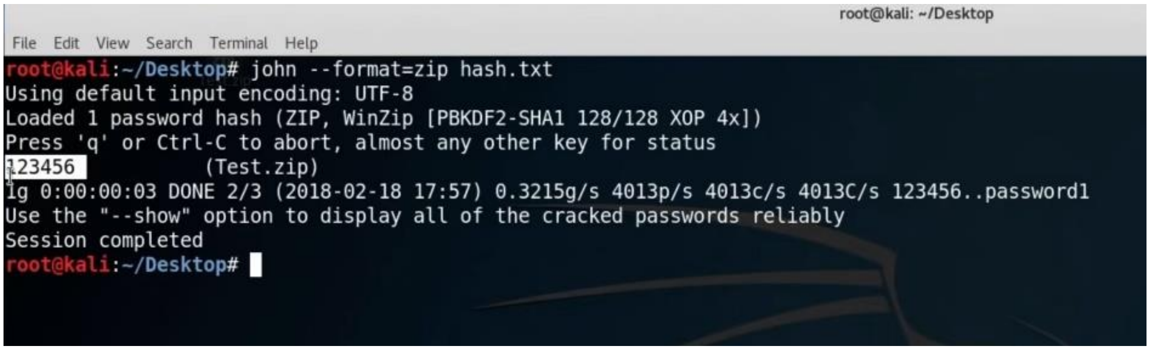


```
  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
 Disk \\.\PhysicalDrive0 - 64 GB / 60 GiB - VMware, VMware Virtual S
>Disk \\.\PhysicalDrive1 - 134 GB / 125 GiB - VMware, VMware Virtual S
 Drive D: - 85 MB / 81 MiB - NECVMWar VMware SATA CD01
```

(Fig.9)

Alternatively, tools like John the Ripper (Fig.10) could be deployed, using a hybrid approach combining dictionary rule-based methods with brute-force techniques to guess or crack passwords (NWU, 2024). However, it's important to acknowledge that there are limitations to password cracking tools, particularly when faced with strong password conventions, which may render them ineffective.



```
root@kali:~/Desktop# john --format=zip hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 XOP 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (Test.zip)
1g 0:00:00:03 DONE 2/3 (2018-02-18 17:57) 0.3215g/s 4013p/s 4013c/s 4013C/s 123456..password1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop# 
```

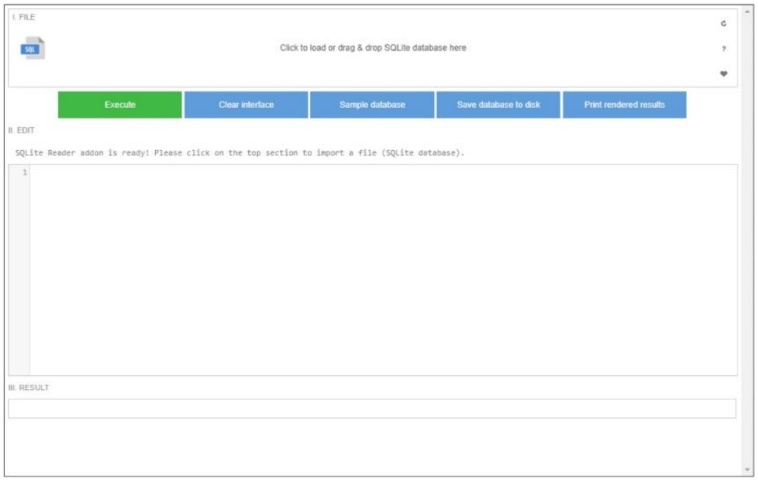
(Fig.10)

Additionally, a rainbow table attack could be considered if the USB encryption method involves hashing the password. Rainbow tables use precomputed tables for reversing cryptographic hash functions that could find a matching password. However, rainbow tables are only effective for certain types of hashes and may require considerable storage space (Horálek et al., 2017).

Mobile Device Images

Mobile device images will undergo thorough examination using FTK (Fig.6). However, it's important to note that mobile devices typically use SSDs, which have the trim command enabled which permanently erases deleted data. As a result, there is no unallocated space containing deleted files that can be recovered (Nimmala, 2020).

However, mobile devices often use SQLite databases. When data is deleted from SQLite databases the database file still exists on the file system, as no file is deleted, no data is trimmed, meaning the deleted data remains recoverable. Any SQLite databases identified through FTK analysis will be exported and loaded into SQLite database reader (Fig.11). This process will grant full access to any databases of information created by applications on the mobile device, including any deleted data (Nimmala, 2020).



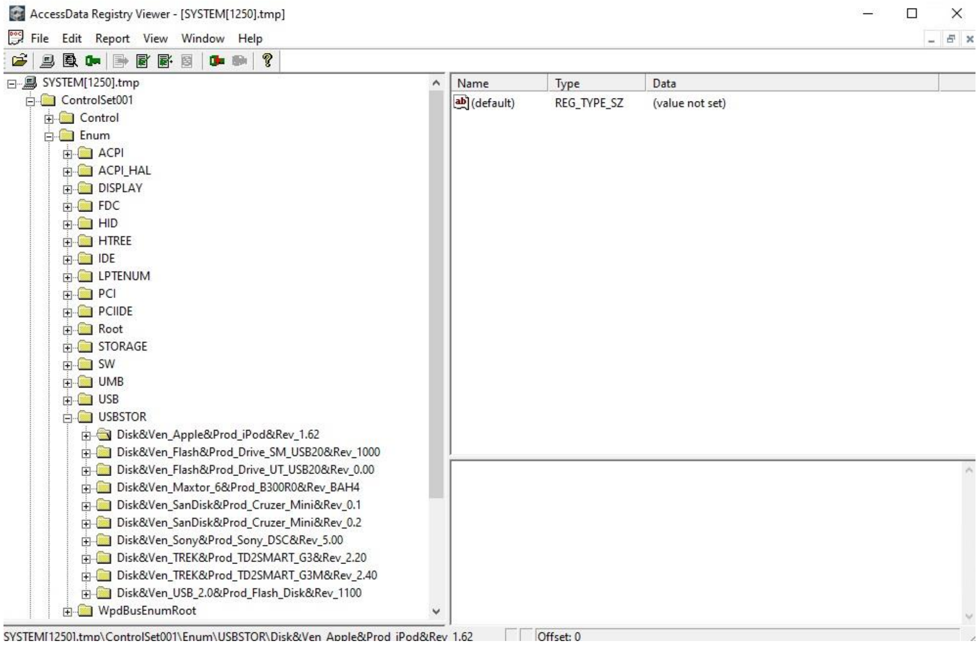
```
SQLite Reader addon is ready! Please click on the top section to import a file (SQLite database).
```

(Fig.11)

Additionally, the Oxygen Forensics digital forensic software will be used to analyse the mobile device images. This will provide a chronological overview of the device's use across applications, which is invaluable for reconstruction and analysis of cross application communication with any corresponding results being added to the investigative chronology (Onditi, 2019).

Analysis

The compromised computer's drive image provides access to crucial information stored in the SYSTEM registry file (Fig.12). This file contains records of timestamps and serial numbers associated with the USB keylogger. The timestamp from the SYSTEM registry file will be matched with CCTV footage and server access-control records from the corresponding time and date. This will accurately reconstruct the events surrounding the connection of the keylogger, enabling documentation of the movement of individuals who had access to deploy the keylogger and the identification of users who were logged in at the time of connection. This essential information will be integrated into the investigative chronology potentially revealing instances of stolen credentials or exposing the identity of the suspect.



```
SYSTEM[1250].tmp
  ControlSet001
    Control
    Enum
      ACPI
      ACPI_HAL
      DISPLAY
      FDC
      HID
      HTREE
      IDE
      LPTENUM
      PCI
      PCIIDE
      Root
      STORAGE
      SW
      UMB
      USB
      USBSTOR
        Disk&Ven_Apple&Prod_iPod&Rev_1.62
        Disk&Ven_Flash&Prod_Drive_SM_USB20&Rev_1000
        Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00
        Disk&Ven_Maxtor_6&Prod_B300R0&Rev_BAH4
        Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.1
        Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.2
        Disk&Ven_Sony&Prod_Sony_DSC&Rev_5.00
        Disk&Ven_TREK&Prod_TD2SMART_G3&Rev_2.20
        Disk&Ven_TREK&Prod_TD2SMART_G3M&Rev_2.40
        Disk&Ven_USB_2.0&Prod_Flash_Disk&Rev_1100
      WpdBusEnumRoot
```

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

```
SYSTEM[1250].tmp\ControlSet001\Enum\USBSTOR\Disk&Ven_Apple&Prod_iPod&Rev_1.62    Offset: 0
```

(Fig.12)

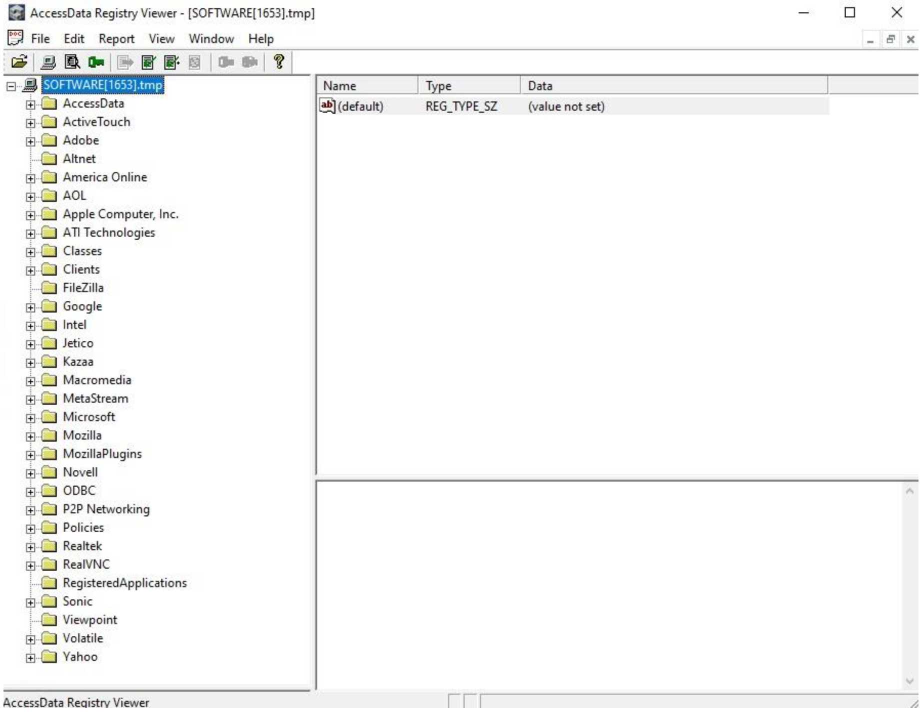
The USB serial number will be cross-referenced with the SYSTEM registry files from other suspect drives to determine if the keylogger has been connected to multiple systems. A HAS-KEYLOG-CONNECTED list will be compiled documenting all drives that contain the serial number associated with the keylogger. These connections will be recorded and added to the investigative chronology.

Subsequently, the HAS-KEYLOG-CONNECTED list will be compared against the HAS-IP-CONNECTED list. If a drive appears on both lists a retrospective network analysis will be undertaken comparing its network traffic pattern, with the Pcap containing the confirmed network traffic pattern of the keylogger. If the patterns match the computer had been compromised by the keylogger, meaning additional data may have been transmitted from other PC’s.

If the traffic patterns do not match, such as a different interval of connections indicating a computer accessing the server rather than transmitting data to it, it may indicate that the computer was involved in the development or testing of the keylogger, potentially connecting to the server to retrieve data.

Furthermore, if a computer appears only on the HAS-KEYLOG-CONNECTED list, it suggests that the computer may have been directly involved in the development or deployment of the keylogger. Additionally, if a computer appears solely on the HAS-IP-CONNECTED list, it indicates that the computer has connected to the malicious IP address without the presence of the keylogger potentially connecting to retrieve data. This list comparison methodology effectively narrows down the suspect list to computers known to have connected to either the keylogger, the malicious IP address, or both.

A SUSPECT-DRIVE list will be compiled from drives present only on the HAS-KEYLOG-CONNECTED list, drives only on the HAS-IP-CONNECTED list and drives present on both lists, but their network traffic patterns do not match the keyloggers transmission patterns. These images will undergo analysis using FTK's registry viewer (Fig.13) to examine registry keys and values related to installed applications, to reveal information such as application names, version numbers, installation paths, and uninstallation entries to determine what applications are installed on the image.


AccessData Registry Viewer - [SOFTWARE[1653].tmp]
File
Edit
Report
View
Window
Help
AccessData Registry Viewer

SOFTWARE[1653].tmp
- AccessData
- ActiveTouch
- Adobe
- Altnet
- America Online
- AOL
- Apple Computer, Inc.
- ATI Technologies
- Classes
- Clients
- FileZilla
- Google
- Intel
- Jetico
- Kazaa
- Macromedia
- MetaStream
- Microsoft
- Mozilla
- MozillaPlugins
- Novell
- ODBC
- P2P Networking
- Policies
- Realtek
- RealVNC
- RegisteredApplications
- Sonic
- Viewpoint
- Volatile
- Yahoo

Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

(Fig.13)

This information will provide insights into the drive's usage history, potentially uncovering software indicating malicious activities, such as anti-forensic tools, steganography applications or development environments including IDEs or code editors. Potentially revealing the original keylogger software or identifying the user account responsible for creating the keylogger.

Additionally, unallocated space on the drives will be examined to recover any deleted data. In the case of modern SSDs, where trim commands ensure complete deletion of data, deleted data may not be recoverable (Nimmala, 2020). However, in the case of magnetic drives, deleted data may reside in slack space (Kävrestad, 2017). Recovering and analysing this deleted data could reveal older iterations of the keylogger software or other information relevant to the investigation.

Conclusion

The covert independent analysis phase includes a physical examination of the keylogger and analysis of various data sources such as email servers, chat logs and ISP browser history. While this analysis could yield results it’s increasingly unlikely that a suspect would reveal such sensitive information on the company network. However, the CCTV surveillance footage would adequately reduce the pool of suspects and the network traffic analysis would reveal critical information on the malicious IP address, along with the stolen data’s transmission interval, with WHOIS lookup potentially revealing the identity of the suspect, again increasingly unlikely.

During the overt phase, the preservation of digital evidence, documenting the scene and maintaining the chain of custody followed established forensic protocols and methodologies. During digital evidence collection forensic tools and techniques were employed to acquire gold standard bitstreams and memory images, which combined ensures the integrity and admissibility of all acquired evidence.

During the examination phase an analysis of the memory dump could contain the malicious IP address, but would contain the keylogger data confirming the malicious IP address. The examination of the suspect drive images SYSTEM registry files yielded essential insights into the chronology of the incident. By correlating timestamps, serial numbers and network connections the lists HAS-KEYLOG-CONNECTED, HAS-IP-CONNECTED and SUSPECT-DRIVE were compiled, and a detailed chronology of events was developed and matched with CCTV footage and server access-control records, accurately reconstructing the events surrounding the connection of keylogger.

The SUSPECT-DRIVE list revealed the computers involved in the incident and registry keys were examined for indications of installed anti-forensic tools or development environments providing insight into the drive's usage history.

In conclusion, the success of a digital forensic investigation at Acme Bank relies heavily on the network analysis results and SYSTEM registry files, specifically the digital artifacts revealed within them.

If the network analysis performed in the independent phase failed to identify the transmission of the keylogger, there would be no memory dump or HAS-IP-CONNECTED list. If the SYSTEM registry file on the seized drives had been modified to delete evidence of the keylogger there would be no HAS-KEYLOG-CONNECTED list. Which would mean no comparison to compile the SUSPECT-DRIVE list, which led to the search for anti-forensic tools and development environments.

The key digital artifacts discovered through network analysis and SYSTEM registry file examination combined with the detailed chronology would result in the suspects responsible for the keylogger being identified and their activities being reconstructed with a high degree of accuracy. However, if anti-forensics has been performed and these digital artifacts have been deleted of modified there is no guarantee this methodology would accurately identify the suspects.

Reference List

AF (2023) *An explanation of ACPO Guidelines for digital based evidence, The ACPO Principles of Digital Based Evidence*. Available at: https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/ (Accessed: 28 March 2024).

BCC (2017) *FTK User Guide*, *Computer Information Systems - Bristol Community College*. Available at: http://cisweb.bristolcc.edu/~ik/t155t/FTK_UG.pdf (Accessed: 30 March 2024).

CER (2014) *How long does a forensic exam take?, Computer Evidence Recovery*. Available at: https://www.computerpi.com/resources/how-long-does-a-forensic-exam-take/#:~:text=In%20the%20case%20of%20using,to%204.5%20hours%20to%20image. (Accessed: 26 March 2024).

Clarke, N., Li, F. and Furnell, S. (2017) *'A novel privacy preserving user identification approach for network traffic'*, *Computers &amp; Security*, 70, pp. 335–350. doi:10.1016/j.cose.2017.06.012.

Daniel, Larry and Daniel, Lars (2012) *Digital Forensics for legal professionals: Understanding Digital evidence from the warrant to the courtroom*. Waltham, MA: Syngress.

Gurkok, C. (2017) *'Cyber forensics and incidence response', Computer and Information Security Handbook*, pp. 603–628. doi:10.1016/b978-0-12-803843-7.00041-7.

Horsman, G. and Sunde, N. (2022) *'Unboxing the Digital Forensic Investigation process', Science &amp; Justice*, 62(2), pp. 171–180. doi:10.1016/j.scijus.2022.01.002.

Horálek, J. *et al.* (2017) *'Analysis of the use of rainbow tables to break hash', Journal of Intelligent &amp; Fuzzy Systems*, 32(2), pp. 1523–1534. doi:10.3233/jifs-169147.

Hranický, R. (2021) *Digital Forensics: The Acceleration of Password Cracking*. PhD dissertation, Vysoké učení technické v Brně, Fakulta informačních technologií, Brno, p. 24.

Kävrestad, J. (2017) *Guide to digital forensics a concise and practical introduction*. Cham, Germany: Springer.

Nguyen-Phuoc, G. (2021) *Memory CTF with Volatility, University of Hawaii - West Oahu*. Available at: https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/memory-ctf-with-volatility-part-2/ (Accessed: 30 March 2024).

Nimmala, R.R. (2020) *'Forensic Research on Solid State Drives using Trim Analysis', Culminating Projects in Information Assurance*, (106). Available at: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1141&context=msia_etds (Accessed: 30 March 2024).

NWU (2024) *Password Cracking Tutorial*, *Introduction to system security*. Available at: http://hamsa.cs.northwestern.edu/readings/password-cracking/ (Accessed: 30 March 2024).

Onditi, R.J. (2019). *Comparative Evaluation Of The Effectiveness Of Smartphone Forensics Tools [Thesis]*. University Of Nairobi. Available at: http://erepository.uonbi.ac.ke/handle/11295/109875 (Accessed: 31 March 2024).

Owen, P. and Thomas, P. (2011) *‘An analysis of digital forensic examinations: Mobile devices versus Hard Disk Drives utilising ACPO & NIST Guidelines’*, *Digital Investigation*, 8(2), pp. 135–140. doi:10.1016/j.diin.2011.03.002.

Quick, D. and Choo, K.-K.R. (2018) ‘*Digital Forensic Intelligence: Data subsets and Open Source Intelligence (DFINT’, Future Generation Computer Systems,* 78, pp. 558–567. doi:10.1016/j.future.2016.12.032.

Sammons, J. (2015) *The basics of Digital Forensics: The primer for getting started in Digital Forensics*. San Diego, California: Syngress.

Upadhyay, D. *et al.* (2022) *‘Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications’*, *IEEE Access*, 10, pp. 112472–112486. doi:10.1109/access.2022.3215778.

Vidas , T. (2007) *The acquisition and analysis of Random Access Memory, RAM FORENSICS*. Available at: https://users.ece.cmu.edu/~tvidas/papers/JDFP06.pdf (Accessed: 28 March 2024).

Image List

Fig. 1. Grint, L. (2024) *Fig. 1. Wireshark Network Traffic Analysis.* Personal Collection.

Fig. 2. Grint, L. (2024) *Fig. 2. FTK Imager Memory Dump.* Personal Collection.

Fig. 3. Grint, L. (2024) *Fig. 3. FTK Imager Bitstream Image.* Personal Collection.

Fig. 4. Grint, L. (2024) *Fig. 4. XRY Mobile Forensic Tool.* Personal Collection.

Fig. 5. Grint, L. (2024) *Fig. 5. Volatility Memory Forensic Tool.* Personal Collection.

Fig. 6. Grint, L. (2024) *Fig. 6. FTK Data Carve Image Analysis.* Personal Collection.

Fig. 7. Grint, L. (2024) *Fig. 7. PRTK.* Personal Collection.

Fig. 8. Grint, L. (2024) *Fig. 8. PRTK SAM + SYSTEM.* Personal Collection.

Fig. 9. Grint, L. (2024) *Fig. 9. TestDisk Data/Partition Recovery Tool.* Personal Collection.

Fig. 10. Grint, L. (2024) *Fig. 10. John The Ripper Password Cracker.* Personal Collection.

Fig. 11. Grint, L. (2024) *Fig. 11. SQLite Database Reader.* Personal Collection.

Fig. 12. Grint, L. (2024) *Fig. 12. FTK Registry Viewer SYSTEM Registry File.* Personal Collection.

Fig. 13. Grint, L. (2024) *Fig. 13. FTK Registry Viewer Application Evidence.* Personal Collection.