



The Departure of an Employee - Forensic Report

APPLIED FORENSICS COURSE WORK

AHMED FAROUK MAHMOUD

CU2000512



Introduction and expected learning outcomes

For this course work we were asked to create a forensic report examining a windows XP and an android image of an employee that left a company. The purpose of this report was to look for any intelligent property copied out of the system and investigate whether more legal action is necessary. Some of my expected outcomes for this module are learn how to write a professional forensic report, use high-level forensic tools, and get started in mobile forensics.

Scenario

For this project, I assumed that I was working as a security engineer for a startup named MyFin Tech. After an employee working in a sensitive project left the company, I was asked to create a forensic report examining his computer and phone to make sure that the employee did not copy any sensitive files. And to investigate whether more legal action is necessary.



The Digital Forensic Process

According to the [Digital Forensics Research Workshop](#), a digital forensic process consists of 6 different steps

1. **Identification:** *Finding clues that can be used to track out the attacked and collecting them as evidence in an investigation.*
2. **Preservation:** *Requires preventing any changes or deletions to the evidence.*
3. **Collection:** *The procedure for obtaining digital evidence.*
4. **Examination:** *The process of extracting potentially relevant data from evidence utilizing tools and methodologies.*
5. **Analysis:** *All pertinent data that has been examined is now being evaluated.*
6. **Presentation:** *A thorough report is created that details the steps required to get the evidence and present it in court.*

I divided the report into 2 main sections. Section one includes the first 5 steps Identification, Preservation, Collection, Examination, and Analysis and section Two only includes the Presentation step. The Presentation step is then further divided into an executive summary, Findings, Appended reports, and a Conclusion.



Contents

Introduction and expected learning outcomes	1
Scenario.....	1
The Digital Forensic Process	1
Step 1: Identification.....	4
Step 2: Preservation.....	4
2.1 Hashing Values (Preservation)	4
Step 3: Collection	5
3.1 Chain of Custody (Collection).....	5
Step 4: Examination	6
4.1 The examination tools	6
4.2 Computer Data Extracted	6
4.3 Phone Data Extracted	8
Step 5: Analysis	9
5.1 Steps Taken	9
5.2 Table of Important Data.....	11
5.3 Important Data Timeline	12
5.4 Summary of Analysis	12
Step 6: Presentation.....	13
Executive summary	1
Findings	1
Appended Reports	2



Table Of Figures

Figure 1 Hashing values	4
Figure 2 Chain of custody form from NIST	5
Figure 3 Web related data	6
Figure 4 Media	7
Figure 5 Email.....	7
Figure 6 Documents	7
Figure 7 Installed programs	7
Figure 8 External devices connected	8
Figure 9 Encrypted files.....	8
Figure 10 Phone Data.....	8
Figure 11 Sample of text messages.....	8
Figure 12 Step 1	9
Figure 13 Step 3	10
Figure 14 Step 2	10
Figure 15 Step 4	11
Figure 16 Important Data Timeline.....	12
Figure 17 Image of elements of a digital forensic report by Drive Savers.....	13



Step 1: Identification

Identification

1

The first step refers to identifying the need for a forensic investigation. For example, after a cyber-attack on a network. And in my scenario, it is after a sudden departure of an important employee. This step also includes the identification of the **trace evidence** in my scenario it will be a windows XP and an android image.

Step 2: Preservation

Preservation

2

The next step is to preserve the evidence after it has been recognized. This phase involves protecting the evidence from being tampered with or deleted. Controls may be installed to prevent unauthorized access to a system containing evidence in specific instances, such as isolating the system on the network or restricting physical access. This guarantees that the evidence is not tampered with on purpose or accidentally. A few techniques for preserving the evidence are

- Hashing values
- Imaging drives
- Not changing the current state of the device
- Make sure the evidence is physically secure

Because this is not a real-life investigation (scenario), in this step I was only able to use one of the techniques listed above (Hashing values).

2.1 Hashing Values (Preservation)

Hashing the evidence is a crucial step in the preservation phase, as it ensures that the data has not been tampered with. If any data is tampered or deleted a new hash will be generated and in that case the evidence cannot be used in court. To generate hashes for the 2 evidence files, I have used **MD5 & SHA Checksum Utility (by Raymond Lin)**. The table below highlights the results.

File	Hash algorithm	Result
WinXP.E01	MD5	CFE6F736CE56CD96CB835F0AB891AB9C
WinXP.E01	SHA-256	2773952B1F72A055FB974B6EACF34272BBF9C016D3FD428B2D771C1F305D2636
Android.rar	MD5	F30E0951468A266B5CA8DAE5C9A29465
Android.rar	SHA-256	C10914F754B256DCCA70B80925765459154E15B9FFFB9787E1AE1D579317AD8

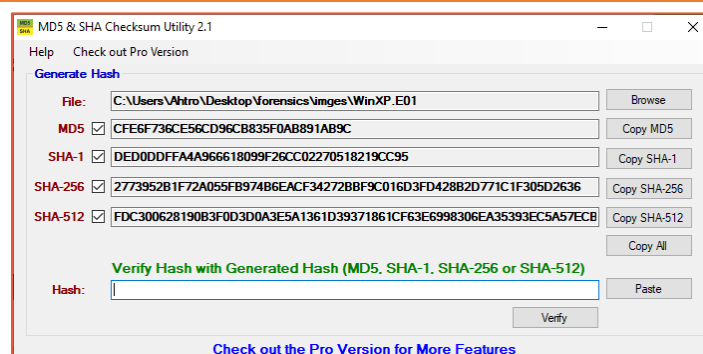


Figure 1 Hashing values



Step 3: Collection

Collection

3

During the collection step, Digital forensics examiners will begin collecting volatile digital evidence. **Volatile evidence** is evidence that can be lost when a system is turned off. Active connections, log data maintained on a network device, operating memory, remotely recorded data, or the Address Resolution Protocol cache are examples of volatile data. After collecting the volatile evidence, it should be transferred to a non-volatile media storage, such as an external hard drive. In his book *The Basics of Digital Forensics (Second Edition)*, John Sammons states “It’s a good idea to prioritize the evidence to be collected. Generally, we want to start with the most volatile evidence first. In computer parlance, this is known as the **order of volatility**”. A good sequence to follow would be

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system/swap space

like the previous step, I was unable to apply all these techniques discussed above because this is not a real investigation.

3.1 Chain of Custody (Collection)

The documenting of the evidence life cycle throughout an investigation is referred to as the **chain of custody**. The evidence life cycle begins when someone initially obtains access of the evidence and ends when the evidence is either destroyed or returned. Figure 2 shows an example of a chain of custody for my scenario.

Property Record Number:				
41587523				
Any Police Department				
EVIDENCE CHAIN OF CUSTODY TRACKING FORM				
Case Number: Cu2000512 Offense: Ahmed farouk				
Submitting Officer: [Name/ID#] Mahmoud EL-Kasas				
Victim: MyFin tech				
Suspect: the employee in MyFin tech				
Date/Time Seized: 1-5-2022 Location of Seizure: Cairo, Egypt				
Description of Evidence				
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)		
1	1	An image of windows XP machine of the employee		
2	1	An image of android phone of the employee		
Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
Null	Null	Null	Null	Null
Null	Null	Null	Null	Null
Final Disposal Authority				
Authorization for Disposal				
Item(s) #: _____ on this document pertaining to (suspect): _____				
is/are no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)				
<input type="checkbox"/> Return to Owner <input type="checkbox"/> Auction/Destroy/Divert				
Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____				
Witness to Destruction of Evidence				
Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#: _____				
in my presence on (date) _____				
Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____				

Figure 2 Chain of custody form from NIST



Step 4: Examination

Examination

4

In the examination step, the forensic analyst extracts data and artifacts using different tools and techniques from the evidence they collected from the previous steps. While examining the evidence files, I was able to extract some documents, media files, emails, and other important files the below section highlights all the findings along with the tools and the techniques I used.

4.1 The examination tools

In terms of software, digital forensics makes extensive use of both commercial and freeware technologies. It's critical to ensure that all tools have been thoroughly tested and are up to date. Every tool employed in a forensic investigation should be recorded and justified. The following are some of the tools I used:

- **Autopsy:** *Is an open-source program for automating digital forensics operations. Brian Carrier designed it.*
- **AXIOM Examine and AXIOM Process:** *Are tools that specify in mobile forensics. It can also create timelines and tables with the found results.*
- **Time Graphs:** *Is a web application that helped me visualize certain events in a timeline.*

4.2 Computer Data Extracted

Using Magnet Axium, I was able to extract a total of 139 web related data, 2250 media files, 6 email files, 54 document files, 4 installed programs, 7 USB devices, and 1 encrypted file. All the findings are listed below with additional figures.

Web Related Data Found

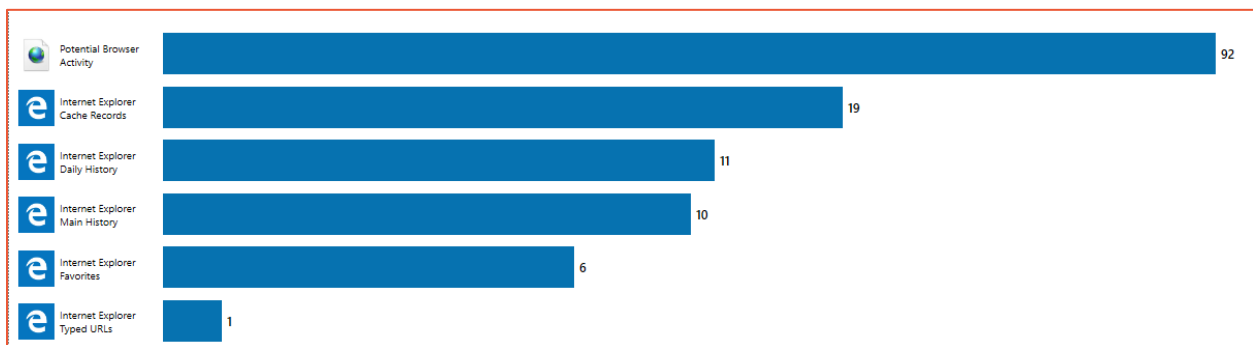


Figure 3 Web related data



Media Found



Figure 4 Media

Emails Found

Item	Type	Artifact ca...	Date...
%s	EML(X) Files	Email & Calendar	
MSN Staff <msn_welcome@msn.com>	EML(X) Files	Email & Calendar	
MSN Staff <msn_welcome@msn.com>	EML(X) Files	Email & Calendar	
MSN Staff <msn_welcome@msn.com>	EML(X) Files	Email & Calendar	
MSN Staff <msn_welcome@msn.com>	EML(X) Files	Email & Calendar	
MSN Staff <msn_welcome@msn.com>	EML(X) Files	Email & Calendar	

Figure 5 Email

Documents found

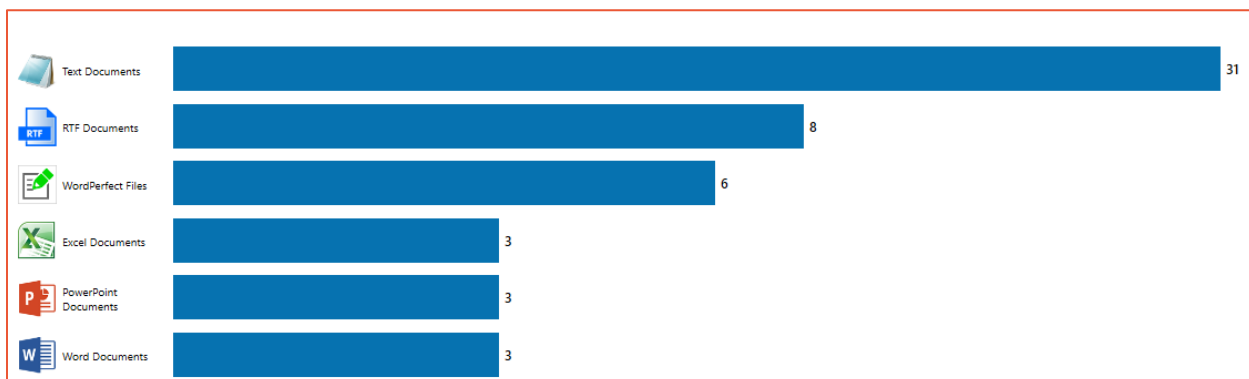


Figure 6 Documents

Installed programs found





	Google Toolbar for Internet Explorer INSTALLED PROGRAMS — Application Usage Potential Location : c:\program files\google CREATE EXPORT / REPORT OPEN SOURCE FILE WITH...	Key Last Updated Date/Time 1/30/2008 2:09:23 PM
	VMware Tools INSTALLED PROGRAMS — Application Usage Company : VMware, Inc.	Key Last Updated Date/Time 1/30/2008 1:58:23 PM
	WinZip 11.1 INSTALLED PROGRAMS — Application Usage Company : WinZip Computing, S.L.	Key Last Updated Date/Time 1/30/2008 2:10:08 PM
	Google Toolbar for Internet Explorer INSTALLED PROGRAMS — Application Usage Company : Google Inc.	Key Last Updated Date/Time 1/30/2008 2:09:23 PM

Figure 7 Installed programs



External devices connected



Figure 8 External devices connected

Encrypted files found



Figure 9 Encrypted files

4.3 Phone Data Extracted

From the mobile data I was able to extract a total of 182 pictures, 91 text messages, 13 people/contacts, 5 web related data, and 1 installed application.

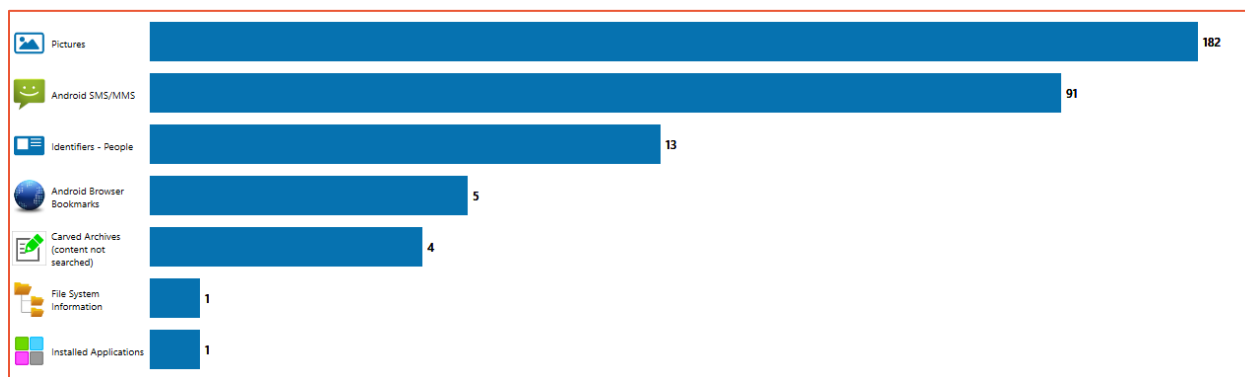


Figure 10 Phone Data

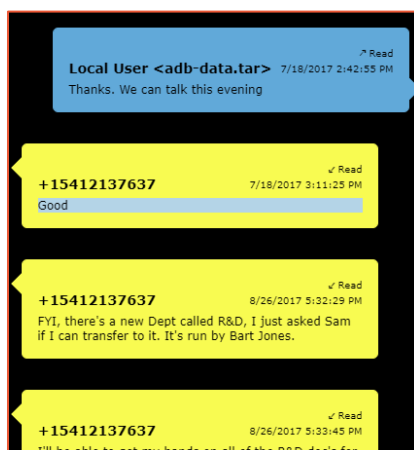


Figure 11 Sample of text messages



Step 5: Analysis

Analysis

5

The analysis step aids in determining the data's origins, including when and where it was generated, edited, accessed, downloaded, or uploaded, as well as any possible links to the file. I started analyzing the important data extracted from the previous step. And depending on the type of digital data extracted, the analysis procedure might be different.

5.1 Steps Taken

This section highlights how I was able to use Magnet Axiom to find and analyze the important data. First, I created a new case and added the 2 evidence files. I then closely examine all the extracted data and try to find any evidence. When I find any evidence, I right click on the file or event and bookmark it as evidence. Another great feature in Magnet Axiom is the connection functionality. This functionality helps me to find any connections between data. I used this multiple times in the investigation. After examining all the data and bookmarking the evidence I moved to the timeline panel where I can see all the bookmarked evidence that I collected and then start deeply analyzing and creating possible scenarios. The figures below show all the steps taken.

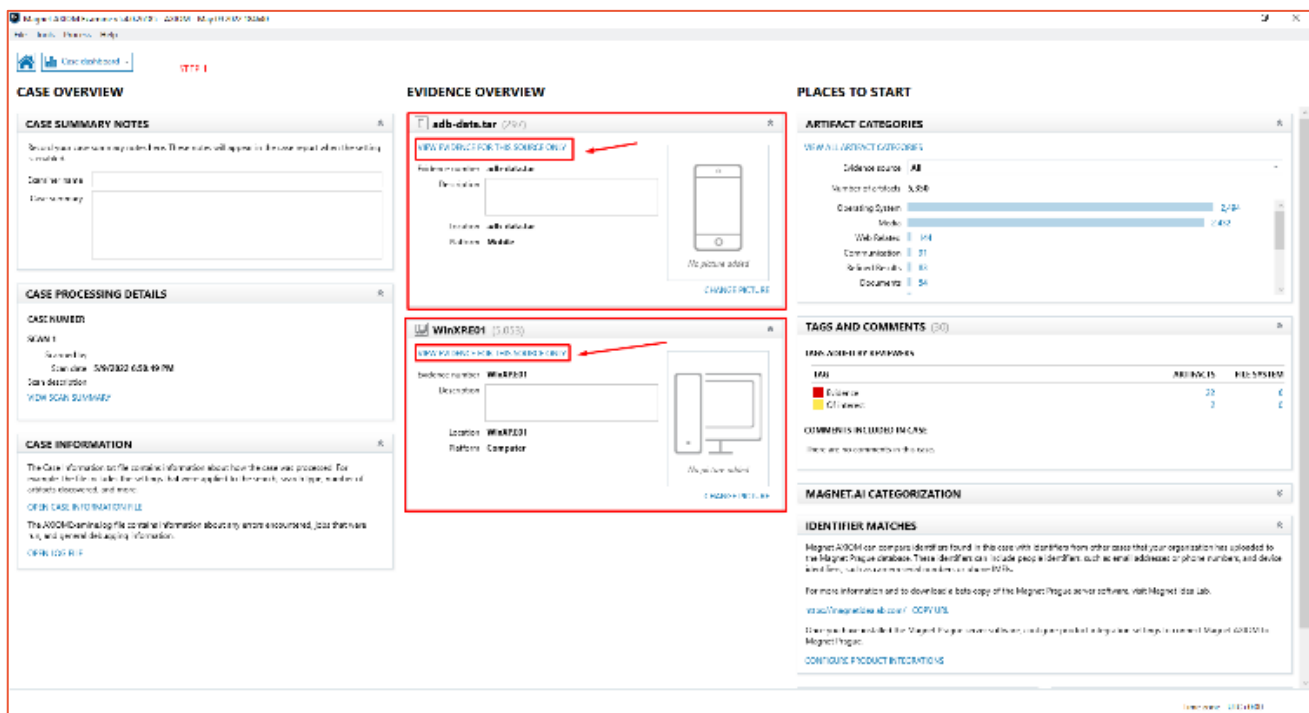
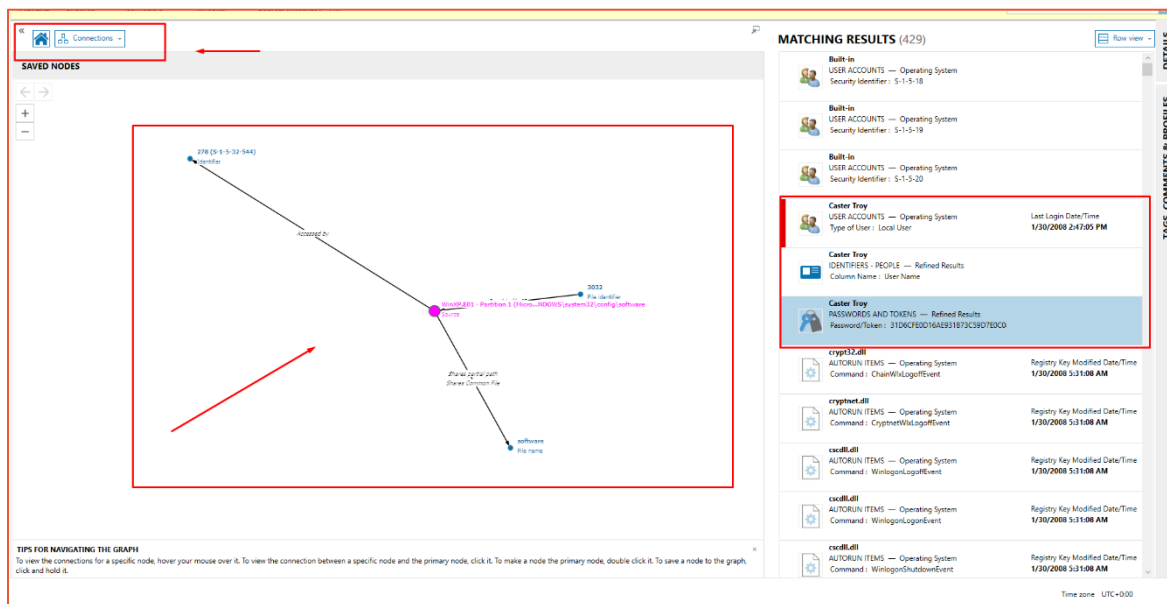
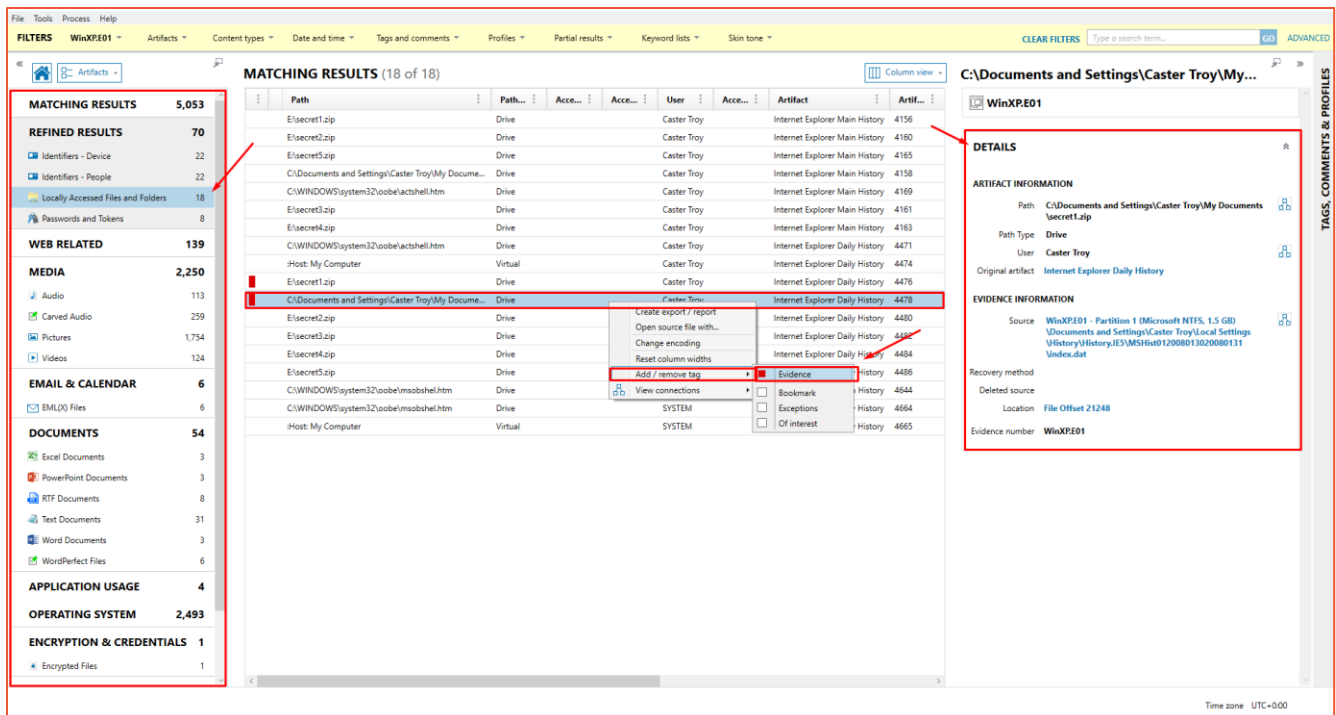


Figure 12 Step 1



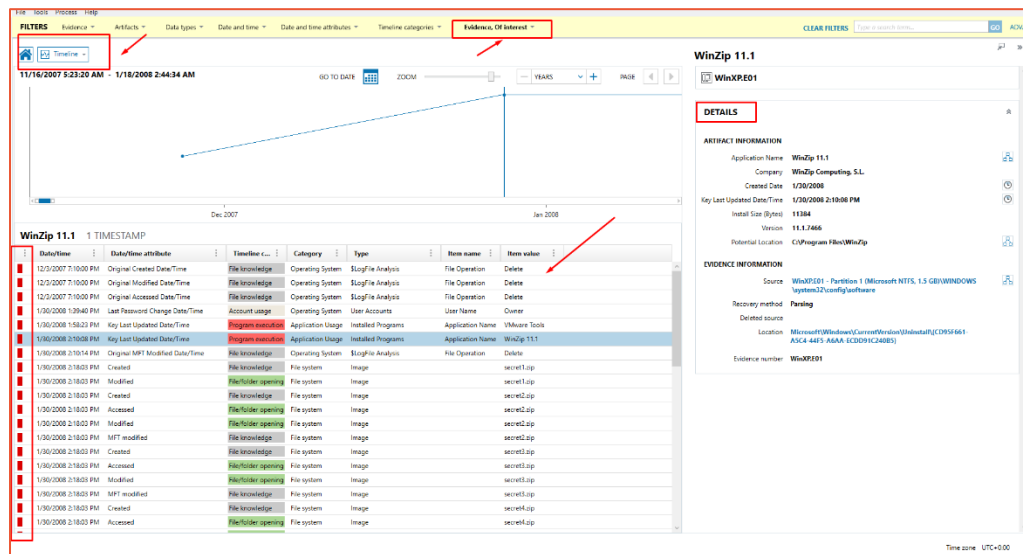


Figure 15 Step 4

5.2 Table of Important Data

The Below table Highlights the important data that I was able to extract for the full table I have attached another file named **importantdata.csv** where it includes all the extra details.

Record	Data and Time	Category	Type	Item Name
1	1/30/2008 13:58	Application Usage	Installed Programs	VMware Tools
2	1/30/2008 14:10	Application Usage	Installed Programs	WinZip 11.1
3	1/30/2008 14:10	File knowledge	Deleted file	Winzip.exe
4	1/30/2008 14:18	File system	File Created	Secret1.zip
5	1/30/2008 14:18	File system	File Created	Secret2.zip
6	1/30/2008 14:18	File system	File Created	Secret3.zip
7	1/30/2008 14:18	File system	File Created	Secret4.zip
8	1/30/2008 14:18	File system	File Created	Secret5.zip
9	1/30/2008 14:27	Web Related	Internet Explorer History	file:///E:/secret1.zip
10	1/30/2008 14:27	File system	File Accessed	secret1.zip
11	1/30/2008 14:27	Web Related	Internet Explorer History	file:///E:/secret2.zip
12	1/30/2008 14:27	File system	File Accessed	Secret2.zip
13	1/30/2008 14:28	Web Related	Internet Explorer History	file:///E:/secret5.zip
14	1/30/2008 14:28	File system	File Accessed	Secret5.zip
15	1/30/2008 14:41	File knowledge	Created	sdelete.exe
16	1/30/2008 14:41	File/folder opening	Accessed	sdelete.exe
17	1/30/2008 14:47	Account usage	Login	Caster Troy
18	1/30/2008 14:47	Operating System	Local Area Connection	Network activity
19	1/30/2008 14:50	Connected Devices	USB Devices	Device disconnected
20	1/30/2008 15:13	Operating System	Deleted file	explorer.exe
21	1/31/2008 4:32	Operating System	Password change	Caster Troy
22	7/18/2017 0:00	Communication	Android SMS/MMS	adb-data.tar
23	7/18/2017 14:42	Communication	Android SMS/MMS	adb-data.tar

5.3 Important Data Timeline

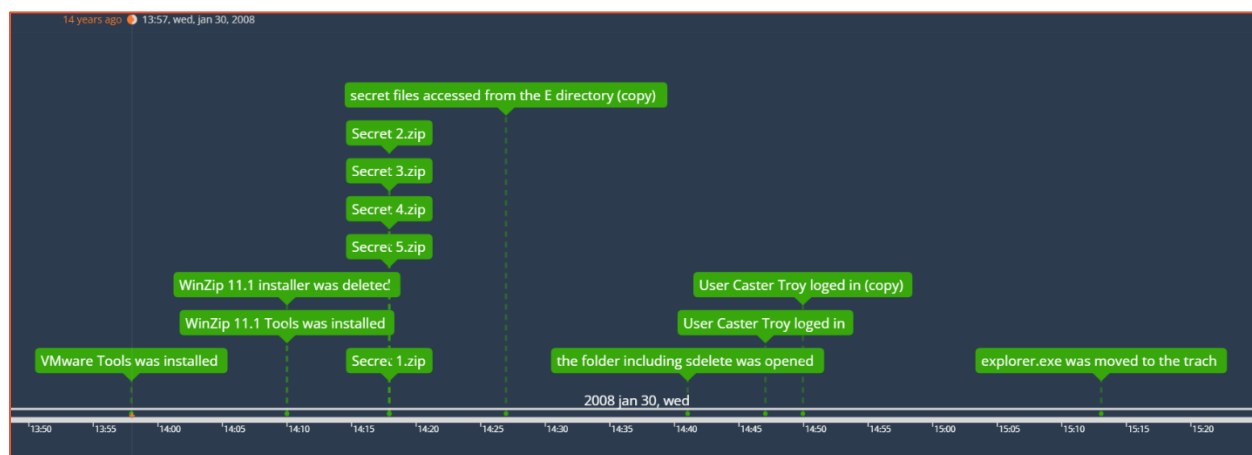


Figure 16 Important Data Timeline

5.4 Summary of Analysis

From the above analysis I can infer that at 13:58 VMware the application was installed. Following the VMware installation, I was unable to find anything relevant which means that the VMware installation had nothing to do with the case. At 14:10 Winzip (an application used to add files to a zip). After installing Winzip the user deleted the Winzip installer. After exactly 8 minutes the user created 5 zip files named secret 1 to 5. The user then accessed the zip files from internet explorer at 14:27 located on the E directory (the files were in the documents folder but the user accessed them in the E directory which means that the user copied the 5 files from the document folder to the E directory the E directory is a USB which also means that the user copied all the files to the USB). At 14:41 a folder including Sdelete.exe was accessed but could not find any evidence that the Sdelete.exe file was executed sdelete could have been used to remove some of the evidence as there are no data to what happened to this file. At 14:50 the USB with the E directory was unplugged from the device. After that Caster Trony changed the password for his account. After that by 9 year I was able to find messages on the android image discussing a file that he will send it to +15412137637 via email and encrypted with gpg encryption.

I was able to infer from the collected data that Caster Trony is guilty of copying sensitive data from the computer's company to a USB. There was a total of 5 zip files copied to the USB with device class id Disk&Ven_USB_NAND&Prod_FLASH_DISK&Rev_1.00.

Although There were chat messages with +15412137637 that he would send him files, the messages were in 2017 and all the other data were in 2008. Furthermore, from the messages I was also able to infer that he was going to send the files in the gpg encryption and via email but could not find any files with the gpg encryption and all the email files were clean. which means that there is no link between the mobile image and the windows image.



Step 6: Presentation

Presentation

6

Throughout the presentation step, forensic examiners must provide a complete written report outlining the measures used to collect the evidence, as well as any limits discovered during the investigation. This report must be succinct, straightforward, and objective. It will be utilized to help investigators figure out what caused the tragedy. The following is a typical format for digital forensics report that I will follow:

- Executive summary
- Findings
- Appended Reports

EXECUTIVE SUMMARY
Language: Non-technical Purpose: High-level description of analysis findings in easily understood, non-technical language.
FINDINGS
Language: Technical Purpose: Technical details of analysis to clearly describe the repeatable and defensible process. Include diagrams, charts, pictures.
APPENDED REPORTS
Language: Technical Purpose: Further support the analysis of relevant information through presentation of highly detailed technical information, including evidence that can produce a tremendous amount of data such as email or chat message analysis.

Figure 17 Image of elements of a digital forensic report by Drive Savers

As mentioned Above, I assumed that I was working for FinTech and was asked to create a forensic report to identify if Caster Trony is guilty. The following section is a forensic report (The Presentation Step)



Caster Trony - Forensic Report

To: HR@MyFin-Tech.com

Prepared by: Ahmed.farouk@MyFin-Tech.com

Executive summary

Caster Troy, a former employee at MyFin Tech left the company while working on sensitive files. This forensic report is examining if Caster Troy is guilty of copying or deleting any intellectual data of the company. After collecting all the evidence there are traces of copied files on a USB. Other traces also show a conversation with a person discussing sending encrypted files.

Findings

At 14:10 Winzip (an application used to add files to a zip). After installing Winzip the user deleted the Winzip installer. After exactly 8 minutes the user created 5 zip files named secret 1 to 5. The user then accessed the zip files from internet explorer at 14:27 located on the E directory (the files where in the documents folder but the user accessed them in the E directory which means that the user copied the 5 files from the document folder to the E directory the E directory is a USB witch also means that the user copied all the files to the USB). At 14:41 a folder including Sdelete.exe was accessed but could not find any evidence that the Sdelete.exe file was executed sdelete could have been used to remove some of the evidence as there are no data to what happened to this file. At 14:50 the USB with the E directory was unplugged from the device. After that Caster Trony changed the password for his account. After that by 9 year I was able to find messages on the android image discussing a file that he will send it to +15412137637 via email and encrypted with gpg encryption.

I was able to infer from the collected data that Caster Trony is guilty of coping sensitive data from the computers company to a USB. There was a total of 5 zip files copied to the USB with device class id Disk&Ven_USB_NAND&Prod_FLASH_DISK&Rev_1.00.

Although There were chat messages with +15412137637 that he would send him files, the messages where in 2017 and all the other data where in 2008. Furthermore, from the messages I was also able to infer that he was going to send the files in the gpg encryption and via email but could not find any files with the gpg encryption and all the email files where clean. which means that there is no link between the mobile image and the windows image.

Appended Reports

Property Record Number:	
41587523	

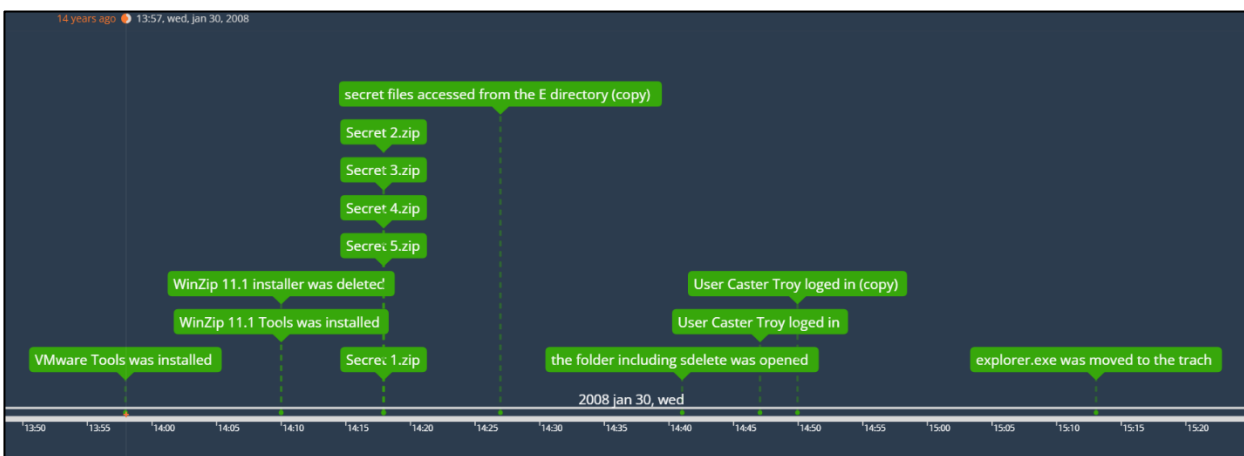
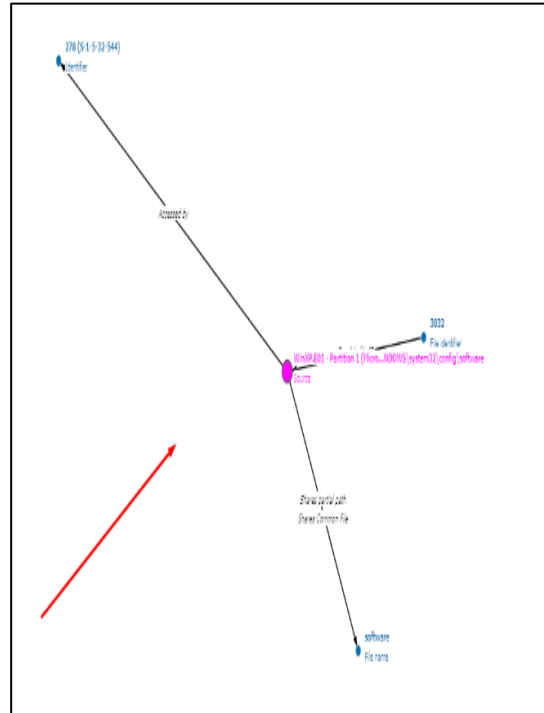
Any Police Department
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: Cu2000512 Offense: Ahmed farouk
Submitting Officer: (Name/ID#) Mahmoud EL-Kasas
Victim: MyFin tech
Suspect: the employee in MyFin tech
Date/Time Seized: 1-5-2022 Location of Seizure: Cairo, Egypt

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	An image of windows XP machine of the employee
2	1	An image of android phone of the employee

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
Null	Null	Null	Null	Null
Null	Null	Null	Null	Null

Final Disposal Authority	
Authorization for Disposal Item(s) # _____ on this document pertaining to (suspect), (date) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method) <input type="checkbox"/> Return to Owner <input type="checkbox"/> Auction/Destroy/Divert Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____	
Witness to Destruction of Evidence Item(s) # _____ on this document were destroyed by Evidence Custodian _____ ID# _____ in my presence on (date) _____ Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____	



importantdata.csv

References

1. *MD5 & SHA Checksum Utility*. (2020, September 14). Raymond's WordPress.
<https://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility/>
2. *Deadlines and reviews - nist.gov*. (n.d.). Retrieved May 11, 2022, from <https://www.nist.gov/system/files/documents/2020/07/30/SOLICIT-2021-final-signature-20200406.pdf>
3. National Institute of Standards and Technology | NIST. (n.d.). Retrieved May 11, 2022, from <https://www.nist.gov/system/files/documents/2017/04/28/Sample-Chain-of-Custody-Form.docx>
4. Hagan, A. (2018, September 10). *Digital Forensic process-presentation*. DriveSavers Data Recovery Services. Retrieved May 11, 2022, from <https://drivesaversdatarecovery.com/digital-forensic-process-presentation/>