Individual Coursework

Sameer Tamang

Student ID:210369 / CU ID:12336463

BSc. (Hons.) Ethical Hacking & Cyber Security, Softwarica College of IT and E-commerce, Coventry University

ST4060CEM Digital Forensic Fundamentals

Ganesh Bhusal

24th July, 2022

Acknowledgement

The methods of gathering, conserving, analyzing, and reporting on data related to a crime or occurrence are just one aspect of digital forensics. A digital forensic scientist must, primarily, be a scientist, and as such, must stay current with the most recent studies on these methods. They might also conduct original research of their own and publish it in peer-reviewed publications to advance the field. Because of inadequate or unsuccessful cybersecurity measures, digital forensics is a thing. Maintaining the privacy and security of your information requires an understanding of both concepts and how they relate to one another.

Abstract

The case study is about a crime and a forensic investigation committed through digital device. In this case a hacker tried to hack sensitives information of people like username, password details and credit information. Here I have tried to evaluate the digital forensic techniques with proper methodology. I have shown how the forensic investigation is performed in a proper way. I have also included proper data acquisition method and chain of custody. Device and evidence integrity is highly maintained. The study also shows that we need to be aware of using public Wireless Access Points.

Table of contents:

Case background

A DELL Cpi notebook laptop is found which was suspected to have committed hackings. The incident was on 20th September, 2004. The machine was equipped with wireless PCMCIA wireless card and external 802.11n antennae. Machine is suspected to have committed digital crime. After a few investigations and inquiries, we found that the machine belongs to Greg Schardt, who is also known as Mr. Evil. Inquiring with his friends and neighbors it is believed that he would park his car to the public places where he could get access to WAP (Wireless Access Point) like T-Mobile hotspots or Starbucks to steal information of peoples using packet gathering techniques.

He would intercept network traffic and attack the usernames, passwords and credit details of people connected to public AP's. He is accused of unauthorized access to electronic communication or intercepting network packets. (CFReDS Project:- Hacking Case Challenge Writeup, 2022)

Suspect Details:

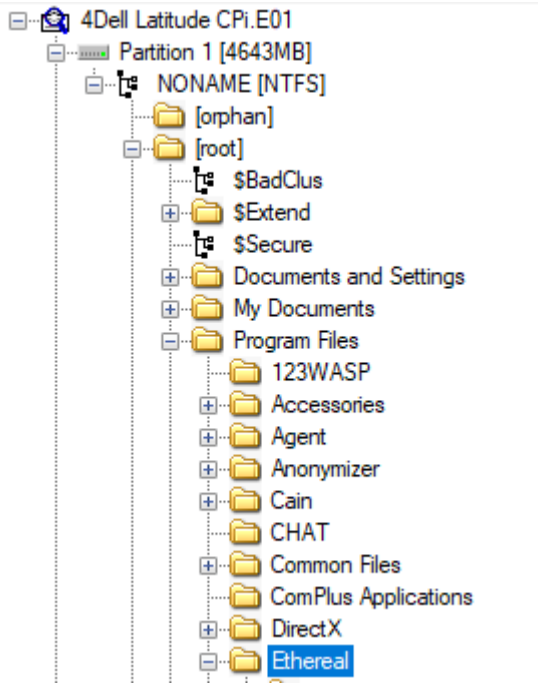
Priority	Suspect	Charge
1.	Greg Schardt Aka Mr. evil	Interception and disclosure of wire, oral, or electronic conversations are illegal under 18 U.S. Code 2511.

Case details:

Objective	To investigate if Greg Schardt, better known as Mr. Evil, illegally monitored the electronic conversations of another user.
Serial Number	VLQLW
Device	Dell CPi laptop
Operating System	Microsoft Windows XP
Offense	Electronic communication intercepted without authorization
Case Agent	Sameer Tamang
Evidence	001
Case Examination Center	Forensic lab of Nepal.
Tools Used	FTK imager

Evidence used in criminal investigation

The presence of the network packet capture tool Ethereal on this computer is confirmed by the information below:



Name: Ethereal

The Ethereal program was set up to run in a promiscuous manner. It would help Mr. Evil to gather and capture packets illegally.

```
# Configuration file for Ethereal 0.10.6.
#
# This file is regenerated each time preferences are saved within
# Ethereal.  Making manual changes should be safe, however.

# Capture in promiscuous mode?
# TRUE or FALSE (case-insensitive).
capture.prom_mode: TRUE
```

Name: Ethereal mode

Information and data were stored in the interception.txt file by the attacker. He would save sensitive information of people in text file.

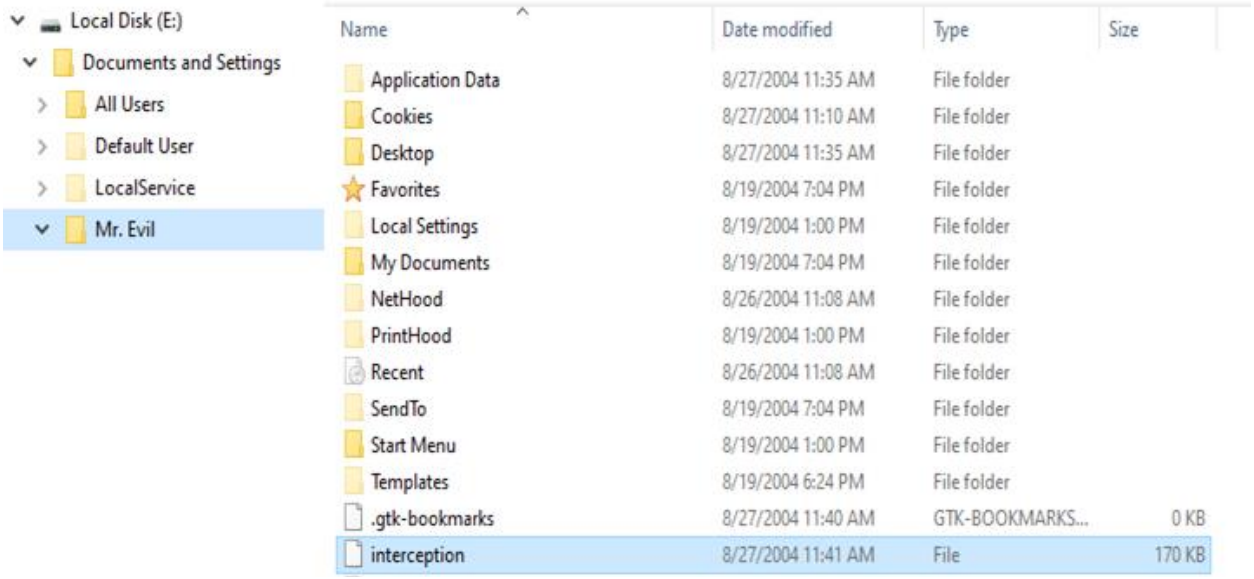
```
# Recent settings file for Ethereal 0.10.6.
#
# This file is regenerated each time Ethereal is quit.
# So be careful, if you want to make manual changes here.

######## Recent capture files (latest last) ########

recent.capture_file: C:\Documents and Settings\Mr. Evil\interception
```

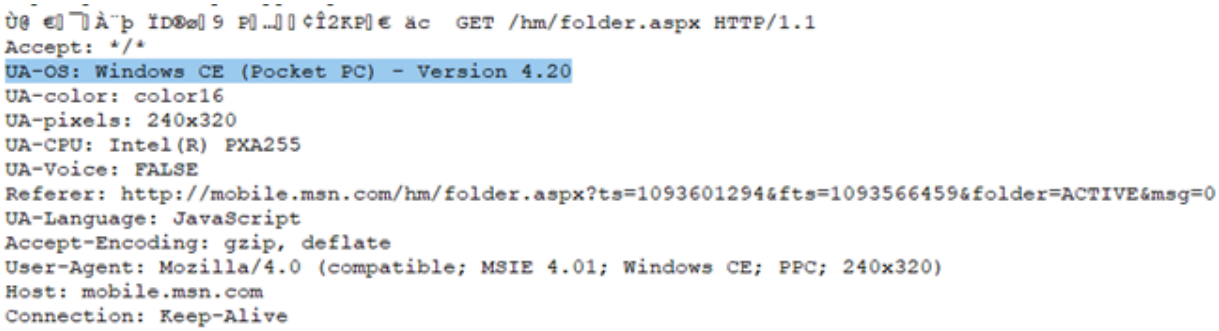
Name: Interception evidence

Ethereal capture text file's actual location:



Name: Interceptional file location

Confirmation of the packet capturing:



Name: Packet Capturing confirmation

From the investigation we performed we accused Mr. Evil of interception of the network and stealing sensitive and personal information from people. We checked on all the logs and data of system and confirmed that he used packet sniffing tool called Ethereal and gathered public information. He could have used the information to hack social media, financial balance, ransomware attacks and more.

Investigation process

First response: After our team got the call from a person who said laptop was abandoned in the parking lot by suspicious person our team sent a first responder in the scene. Responder investigated thoroughly and reported that a laptop was found in the scene with no other traces.

Search & Seizure: We seized the laptop and took it to the investigation lab for further investigation. To investigate digital devices in pubic place would be difficult without proper means of technology and devices. So, we seized the machine and took it to the lab for further investigation process.

Evidence: We investigated the device thoroughly and collected enough evidence. From the investigation process we know Greg Schardt is hacker who connects to public WIFI and steals the sensitive information of people attacking network layer. He has collected packets from the network and analyzed them. We found that he has used Ethereal for packet sniffing. We also found that he

has saved the packets analyzed information in specific file as interception.txt. He used Ethereal in illegal mode for packet capturing. We also found that his device was logged in as Mr. Evil during our investigation process.

Evidence protection: After the confirmation that Mr. Evil has attacked the network illegally, we urge you to protect the evidence. We highly observed evidence and protected confidentially. No other people could alter the case and the evidence we collected. We also protected original evidence as a part of integrity. We placed evidence in a safe environment. Without authentication no one could alter or damage evidence. The data can be verified as correct and usable in a secure environment and then authorized. For the investigation we created a disk image of the device so that overwriting should not be done to original evidence.

Data acquisition: From the device, our forensics team was able to recover electronically stored information (ESI). To prevent tampering with the data and validation of evidence, we followed the right procedures and took care.

Data analysis: To find and transform information that will be beneficial in court, team members sort and review the verified ESI.

Evidence assessment: We evaluate ESI considering the security event once it has been identified as evidence. In this stage, the information acquired is related to the case.

Documentation: After the case was investigated, we had proper documentation along with all the team members. Documentation and evidence are reported with proper procedure in accordance to the law and court.

According to the evidence, Mr. Evil has intercepted the network and captured packets from various access points in public places like T-Mobile Hotspot and Starbucks. He also captured

usernames, password details, credit details of the users who use public network. Evidence shows us it is level 3 attack of OSI model where network model is targeted. Packets are captured by using Ethereal program and information is gathered and stored in interception.txt file. Mr. Evil wants to hack sensitive information of people like username, passwords and credit details which can be used for hacking accounts, social media accounts, ransomware attacks etc. (The Phases of Digital Forensics | University of Nevada, Reno, 2022)

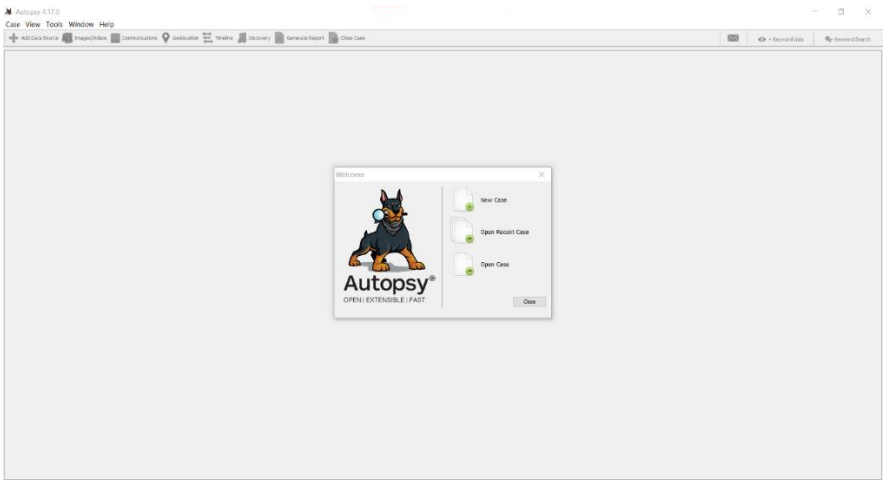
Data Acquisition Integrity

To maintain the integrity of evidence, we have not damaged any evidence. As digital evidence is sensitive which can be altered and destroyed, me and my team have applied ACPO principle to maintain integrity of data.

1. Data on laptop is not changed and altered as it must be presented in the court. To maintain integrity, we performed bit streaming image and preserved original evidence.
2. We were all well capable of handling cases. We collected and gathered all the evidence of the abandoned device and maintained its integrity.
3. Evidence was captured and documented in audit trial and preserved to present in the court. When a 3rd party examines the case, the report should be the same. So, we have kept the evidence safe and have not damaged any of files to maintain device and evidence integrity.
4. Me and my team are fully responsible for accounting the law of evidence and case.

We have not only applied the ACPO principle but also maintained in preserving actual evidence. We preserved the evidence from alternation and being damaged. Chain of custody is maintained.

Logs of the machine were copied and preserved. The timeline of machine was captured and preserved as evidence. We used Autopsy to maintain record and document case.



Name: Autopsy

To maintain the volatility level of evidence, we have prepared the order of volatility as some evidence does not last long. The level of volatility is maintained from most volatile to least. Different guidelines should be followed to maintain the integrity of evidence. Without proper data and acquisition and investigation no one should alter the evidence. Digital evidence is difficult to recover once it is altered and damaged. There is highly possible that evidence will get destroyed when evidence is not protected and observed properly. Proper guidelines have followed to all the evidence such as guidelines for computing, storage, network topologies etc. To collect information and data in proper way to maintain integrity. The digital device which we found during the scenario was turned off so to maintain integrity without losing original data our team had to performed offline data acquisition.

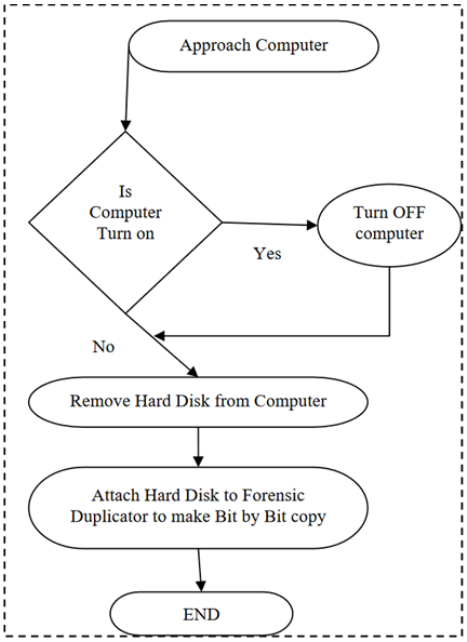


Fig.2 Dead Forensic Image Acquisition [1]

Name: Offline Acquisition

We removed the hard drive from the device and performed bit streaming image to preserve the actual hard drive. FTK Imager was the tool used during the investigation process to perform bit streaming. In the lab, RAM was also accessed using bit streaming process to know and gather evidence of running process in the machine. (Technology, 2022)

Recommendation & Approach

Comparing all the evidence left by Mr. Evil we do not know actual purpose of hacking though. We should interrogate him in a person that why has be committed such crime. According to the situation we have done our best to sort out the crime and solve the investigation. We have used all the possible tools to accused him as guilty but still as he is missing, we should interrogate him in person for further details of his crime. We have checked all the logs and queries of the machine and we have collected all the digital evidence, still we do not know him personally. Sometimes, digital evidence cannot be trusted. The attacker may have been forced to do it or it

was his/her intention. But as a part of digital investigation, we have applied all the possible techniques to vary out investigation. We have maintained a chain of custody, data integrity, evidence integrity etc. We have followed ACPO principle for the investigation. We have taken crime as a serious part of technology. We presented evidence to the court with proper solution and assault.

Digital devices are much more used in many crimes. Most of the crimes happening are committed through devices. We run many awareness programs with proper knowledge to reduce digital crimes. Most digital crimes are the result of people misusing and neglecting proper security on their smart devices. As an investigator, we should not neglect various programs installed on the device. We should be aware of malicious attacks. So, we should not directly approach the evidence before we keep both evidence and our system clean and safe. Updated drivers and tools should be used for appropriate results and investigation. Systems get updated daily so hardware as well as software tools of digital forensics should also be updated. First responder should be aware of all things and evidence at crime scene. Proper law and action should be taken to the people who commit crime with digital devices.

References:

Medium. 2022. *CFReDS Project:- Hacking Case Challenge Writeup*. [online] Available at: https://medium.com/@sshekhar01/cfreds-project-hacking-case-challenge-writeup-6a52883eac0b

[Accessed 24 July 2022].

University of Nevada, Reno. 2022. *The Phases of Digital Forensics | University of Nevada, Reno*. [online] Available at: https://onlinedegrees.unr.edu/blog/digital-forensics/

[Accessed 24 July 2022].

Technology, D., 2022. *schoolworkspro.com*. [online] Schoolworkspro.com. Available at: https://schoolworkspro.com/modules/digital-forensic-fundamentals/evidence-acquisition-and-media-analysis

[Accessed 24 July 2022].