Illegal Image Possession Investigation Report

Submitted by: Frank Xu

August 14, 2021

Abstract

An abstract condenses the report to concentrate on the essential information of the case that was given, the overall investigation process, and conclusion. More specifically, the section needs to answer different questions that covers different areas of digital forensics. Each answer is captured in 1 or 2 sentences. Here are the questions (1) What I was asked to do? (2) Why I am qualified to do? (3) What information did I received to finish the assignment? (4) What I did? (5) what I have found? (6) What was my conclusion? To convince people the quality of the assignment, you may want to answer a few additional questions: (1) What is the overall approach I choose to do the work? (2) How confident when I make the conclusions? Note that you can access the template here: https://www.overleaf.com/latex/templates/technical-report-for-document-image-analysis-unifr/xhdkbqhhzmyw.

Contents

1 Introduction

1.1 Background

'Iaman Informant' was working as a manager of the technology development division at a famous international company OOO that developed state-of-the-art technologies and gadgets.

One day, at a place which 'Mr. Informant' visited on business, he received an offer from 'Spy Conspirator' to leak of sensitive information related to the newest technology. Actually, 'Mr. Conspirator' was an employee of a rival company, and 'Mr. Informant' decided to accept the offer for large amounts of money, and began establishing a detailed leakage plan.

'Mr. Informant' made a deliberate effort to hide the leakage plan. He discussed it with 'Mr. Conspirator' using an e-mail service like a business relationship. He also sent samples of confidential information though personal cloud storage.

After receiving the sample data, 'Mr. Conspirator' asked for the direct delivery of storage devices that stored the remaining (large amounts of) data. Eventually, 'Mr. Informant' tried to take his storage devices away, but he and his devices were detected at the security checkpoint of the company. And he was suspected of leaking the company data.

At the security checkpoint, although his devices (a USB memory stick and a CD) were briefly checked (protected with portable write blockers), there was no evidence of any leakage. And then, they were immediately transferred to the digital forensics laboratory for further analysis. The information security policies in the company include the following:

- Confidential electronic files1 should be stored and kept in the authorized external storage devices and the secured network drives.
- Confidential paper documents and electronic files can be accessed only within the allowed time range from 10:00 AM to 16:00 PM with the appropriate permissions.
- Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.
- All employees are required to pass through the 'Security Checkpoint' system.
- All storage devices such as HDD, SSD, USB memory stick, and CD/DVD are forbidden under the 'Security Checkpoint' rules.

In addition, although the company managed separate internal and external networks and used DRM(Digital Rights Management) / DLP (Data Loss Prevention) solutions for their information security, 'Mr. Informant' had sufficient authority to bypass them. He was also very interested in IT (Information Technology), and had a slight knowledge of digital forensics.

Note that the case description is from https://www.cfreds.nist.gov/data_leakage_case/data-leakage-case.html. If you use any references, please pay attention to the reference format. Here are two citation examples, including Long Short-Term Memory (LSTM) [1] and Graph Neural Networks (GNN)[3].

1.2 Objectives

This section specifies what are you being asked to do. You will include your hypothesis here. It is especially important to include if you were asked to perform a targeted investigation. Also a good idea to include any specific search terms requested.

1.2.1 Tasks

List what are you being asked to here:

- Task 1: XXX
- Task 2: XXX
- Task 3: XXX

1.2.2 Hypotheses

List hypotheses here:

- Hypothesis 1: XXX
- Hypothesis 2: XXX
- Hypothesis 3: XXX

1.2.3 Domain Terms

List term in the domain. We need define domain related terms, e.g., terms used when we investigate a fraud related to accounting.

- Accounts payable: fill out the definition here.
- Accounts receivable: fill out the definition here.
- Certified public accountant: fill out the definition here.

1.3 Acquired Data

The subsection describes What information I received to finish the assignment beside background information. It focuses on disk images and files that are associate with the crime case. Fig. 1 show one DD image. Although not all attributes are required, you may want to provide as much information as possible. You **HAVE TO** add more attributes as needed. The same principle applies to other tables.

Table 1: DD image

Attribute	**Detailed Information**
Filename	cfreds_2015_data_leakage_pc.dd
MD5	A49D1254C873808C58E6F1BCD60B5BDE
SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
Imaging Software	FTK Imager 3.4.0.1
Total Size	20.00 GB (21,474,836,480 bytes)
Acquired on	2016-01-20T12:31:00.000Z
Acquired by	NIST
Description	This is the DD image created in crime scene

1.4 Suspect Information

Table. 2 shows suspect's information. Although not all attributes are required, you may want to provide as much information as possible.

Table 2: Suspect Information

Attribute	Detailed Information	Description
name	Iaman Informant	A name used to identify this Threat Actor or Threat Actor group.
threat_actor_types	insider-disgruntled	The type(s) of this threat actor. The values for this property SHOULD come from the threat-actor-type-ov open vocabulary.
sophistication	intermediate	The skill, specific knowledge, special training, or expertise a Threat Actor must have to perform the attack. The value for this property SHOULD come from the threat-actor-sophistication-ov open vocabulary.

1.5 Investigator Information

Explain Why I am qualified to do? Table. 2 shows suspect's information. Although not all attributes are required, you may want to provide as much information as possible.

Table 3: Investigator Information

Attribute	Detailed Information	Description
name	Frank Xu	A name used to identify this Investigator.
certificates	Certified forensic examiner	Specifies a list of certificates the investigator has.
has_investigated_case_refs	NIST data leakage case	Specifier a list of x-crime-case.

2 Suspect Action Timeline

2.1 Timeline in Table

This section describes what I have found. I organized my findings in terms of actions performed by the suspect in a chronological order. Table. 4 show the format of the timeline for the reconstructed crime case. A timeline object describes a specific cybercrime case that is represented by a sequence of actions performed by a threat actor in chronological order. Please don't add any activities of investigators here.

Table 4: Reconstructed Timeline of Illegal Image Procession Case

id	Action	Target	Timestamp	Description
1	download	ccleaner	2016-01-20T12:31:00.000Z	download ccleaner software.
2	install	ccleaner	2016-01-20T12:31:12.123Z	install ccleaner software.
3	execute	ccleaner	2016-01-20T12:31:12.123Z	execute ccleaner software.
4	delete	ccleaner	2016-01-20T12:31:12.123Z	delete ccleaner software

2.2 Timeline in Graph

Figure 1 shows the graphical timeline of the Data Leakage scenario. Sometime, the graphic timeline helps readers to understand the reconstructed scenario.

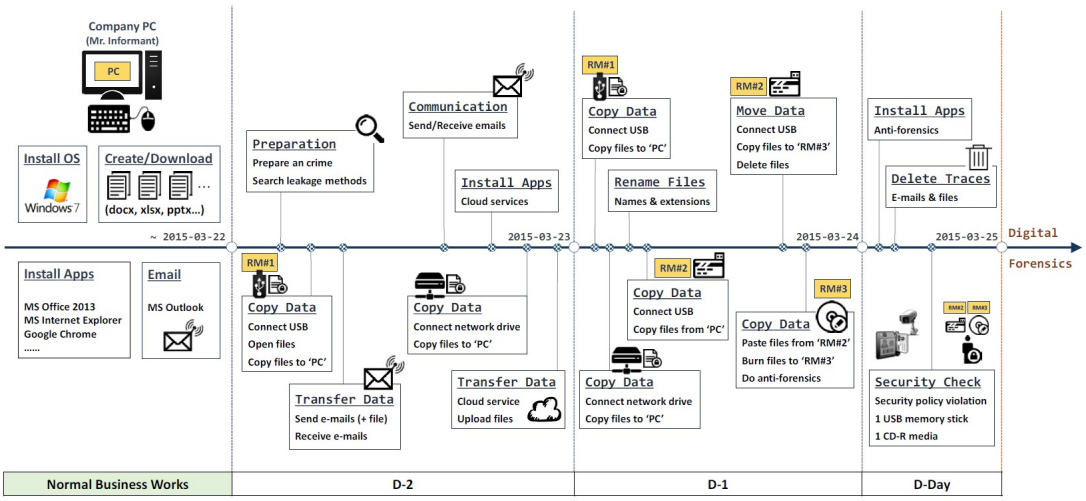

Figure 1: Graphical Timeline of the Data Leakage Scenario

3 Actions

This section describes each action performed by the suspect. Make sure actions are consistent with the all actions in the timeline aforementioned.

3.1 Download ccleaner

3.1.1 Evidence

List all supporting evidence that indicates the suspect downloaded software or files. For each evidence, using an appropriate table to describe the attributes and value of the evidence.

- Download process. The process that downloads a file. The attributes and values of the process is shown in Table 5.
- Downloaded file. The file was downloaded by the process. The attributes and values of the process is shown in Table 6.

Note that we often want to show discovered evidence in graph. Therefore, we attach the download file in Fig. 2

3.1.2 Investigation Tools

List all tools that are used for extracting evidence, such as the tool that is used to show downloading process and tool that is used for find downloaded files. Create a table to describe the attributes and values of the tool. See Wireshark as an example.

- Wireshark: For extracting process information. The attributes and values of the tool that is used to show pid is shown in Table 7.
- Regripper: Describe the tool here. Create a table. See Wireshark as an example.
- WInHex: Describe the tool here. Create a table. See Wireshark as an example.

Table 5: Download Process

Attribute	Detailed Information	Description
pid	314	Specifies the Process ID, or PID, of the process.
created_time	2016-01-20T14:11:25.55Z	Specifies the date/time at which the process was created.
command_line	./gedit-bin –new-window	Specifies the full command line used in executing the process, including the process name (which may be specified individually via the image_ref.name property) and any arguments.
image_ref	firefox.exe	Specifies the executable binary that was executed as the process image, as a reference to a File object. The object referenced in this property MUST be of type file.

Table 6: Downloaded ccleaner

Attribute	Detailed Information	Description
name	ccsetup.exe	Specifies the name of the file.
MD-5	76610b7bdb85e5f65e96df3f7e417a74	Specifies the date/time at which the process was created.
size	56653	Specifies the size of the file, in bytes.

Table 7: Investigation Tool: Wireshark

Attribute	Detailed Information	Description
name	wireshark	A short name of the investigation tool.
description	Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.	A description that provides more details and context about the investigation tool.
inputs_refs	log.pcap	Specifies a list of function inputs. It Should come from any STIX objects or CFOs.
outputs_refs	pid3553, ccsetup.exe	Specifies a list of function outputs or partial outputs. It Should come from any objects that an Observed Data references to.
version	3.4.5	The version identifier associated with the investigation tool.

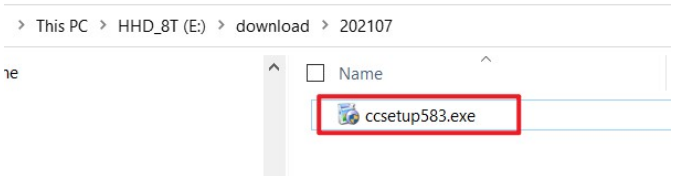

Figure 2: ccleaner installer

3.2 Install ccleaner

Same as previous subsection.

3.3 Execute ccleaner

Same as previous subsection.

3.4 Delete ccleaner

Same as previous subsection.

4 Investigator Activity logs

The section describes what you did during the investigation. You must record your interaction with the digital evidence and the steps taken to preserve and forensically acquire the evidence.

Any activities that you perform (e.g. forensically wiping storage/examination media, etc.) should be notated in this section of your report. The logs ensure the integrity of the digital evidence and your chain of custody. Here are some sample logs [2]:

- On today's date, Detective Max Fox contacted the UB Forensics Laboratory in regards to extracting data from Google Pixel 4XL that had been recovered from a crime scene. Detective Max is requesting a forensic examination to see what information by the suspect may have been deleted. He is requesting a full forensic examination and report for possible criminal charges.
- On today's date I began the forensic acquisition/imaging process of the stolen laptop. Prior to imaging the stolen laptop, I photographed the laptop, documenting any identifiers (e.g., make, model, serial #), unique markings, visible damage, etc. while maintaining chain of custody.
- Using a sterile storage media (examination medium) that had been previously forensically wiped and verified by this examiner (MD5 hash value: ed6be165b631918f3cca01eccad378dd) using ABC tool version 1.0. The MD5 hash value for the examination medium yielded the same MD5 hash value as previous forensic wipes to sterilize this media.
- At this point, I removed the hard drive from the stolen laptop and connected it to my hardware write-blocker, which is running the most recent firmware and has been verified by this examiner. After connecting the hardware write blocker to the suspect hard drive, I connected the hardware write blocker via USB 2.0 to my forensic examination machine to begin the forensic imaging process?
- Etc, etc.

5 Conclusion

The section summarize the case. Here is an example from https://www.duncanwinfrey.com/wp-content/uploads/2012/CSI_Investigation.pdf.

You mainly focus on two check lists, including the task and hypothesis check lists, which you have described in the introduction section?

5.1 Task Check List

Have you completed the tasks you described in introduction section?

- Task 1: XXX
- Task 2: XXX
- Task 3: XXX

5.2 Hypothesis Check List

Are your hypotheses true or false?

- Hypothesis 1: XXX
- Hypothesis 2: XXX
- Hypothesis 3: XXX

In conclusion, Ian has used stenography and password protection techniques to hide evidence from investigators. Ten unique illegal rhino images were recovered from network traffic logs. During the investigation, several software tools are used for extracting evidence, including Wireshark and WinHex.

Appendices

References

[1] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural Computation*, 9(8):1735–1780, 1997.

[2] Bill Nelson, Amelia Phillips, and Christopher Steuart. *Guide to computer forensics and investigations*. Cengage Learning, 2014.

[3] A. Sperduti and A. Starita. Supervised neural networks for the classification of structures. *IEEE Transactions on Neural Networks*, 8(3):714–735, 1997.