ECE 570 – Project II: Data Exfiltration

(Weight: 30%; Due: July 9, 2020)

Case Description

Freescale Semiconductor Cybernetics Inc. is the leader of a growing and highly competitive market segment in the mobile device industry. The company has pioneered a revolutionary mobile device architecture called Mobile Extreme Convergence (MXC). Their main competitor on this market segment is Cybernetics Inc. They suspect that Cybernetics has been trying to steal by any means the core Intellectual Property (IP) underlying the MXC architecture. This IP is protected by Freescale by keeping it closely hidden as a trade secret. Employees of the company were instructed not to have any direct communications with key competitors such as Cybernetics and others. As per the company policy, employees are not allowed to bring their own devices at work, and must use only company supplied devices for work related computing tasks.

The company's head office, is located in a secured facility, with a single entry/exit gate, protected 24 hours by security guards with surveillance cameras. Furthermore, the security team of Freescale secretly checks on a regular basis the content of a random sample of incoming/outgoing emails. During one of these routine checks, an email sent to Cybernetics was intercepted. The intercepted email sent by Mr. John Lewis, the Secretary of Dr. Eli Drucker – the Founder and CEO of Freescale, raised suspicion that he might be providing company sensitive material to Cybernetics.

As a matter of precaution, the security team stepped up the surveillance of Mr. Lewis, and noticed the same day in one of the video-surveillance feeds that he brought his personal laptop at work, in violation of the company policy, and discretely transferred some files to the laptop from his (company supplied) workstation using a USB drive.

Dr. Drucker confronted Mr. Lewis with his suspicions, who denied vehemently. Unconvinced, Dr. Drucker decided to fire him with immediate effect for data theft. Mr. Lewis was then escorted immediately out of the premises, and forced to leave behind his personal items. In anticipation of possible lawsuit, the company decided to collect and analyze evidence supporting their case. One of the items left behind by Mr. Lewis was his personal laptop.

Task

A forensic image of the suspect's seized personal Laptop has been made and given to you, as forensic expert, to investigate whether data was stolen by Mr. Lewis, and whether or not there is enough evidence to support such claim.

The image with corresponding hashes can be downloaded here:

https://drive.google.com/open?id=1C7D-I-YtLBcZdmtrjgoRiJLFcN-lQMQs

A copy of the intercepted email is given in the appendix.

Your task is to analyze the evidence, and extract **all** the relevant data for the investigation. You are expected to document your findings in a forensic report to be given to the police (and submitted as your answer to the assignment). A forensic report is a step-by-step list of everything you have done and what the results were. You don't need to actually list all of the failed attempts or crowd it with non-relevant facts. Keep it accurate, relevant and simple.

Ensure that you answer in particular the following questions that the police are interested in:

1. Check the validity of the forensic image using the supplied hashes. [1%]
2. What crucial data are available on the seized device? Indicate the specific files that contain such data and explain the importance of the different pieces of information for the investigation. **All** relevant information must be identified. Explain what processes did you (the investigator) used to successfully examine the image and uncover the evidence, by highlighting explicitly the logical process or thought that led to the discovery of the relevant information. [15%]
3. For each file, what processes were taken by the suspect to mask them from others? **All** masking processes used for relevant information must be identified, even redundant ones. [8%]
4. Investigate and discuss whether or not the email evidence helps in making the case against the suspect. **All** sources of relevant email evidence must be considered [4%]
5. Discuss and justify whether or not the overall evidence is enough to conclude data theft by the suspect. [2%]

Feel free to use any tools you consider as necessary in your investigation. In any case, the following combination of tools can be useful: FTK Imager, Autopsy, Scalpel (or Foremost), QuickStego, MBox Viewer, HxD Hexeditor, and streams (from SysInternals). Indicate the tools used for each of the questions and provide adequate screenshots to back your answers and results.

Appendix: intercepted Email message

```
-------- Sent Message --------
To: jdeer@cybernetics.com
From: John Lewis <jlewis@freescale.com>
Subject: Hey!
Message-ID: <f9065505-bbc5-d8b3-478a-5e6bfb6809d6@freescale.com>
Date: Wed, 20 Dec 2017 14:51:34 -0800
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101
 Thunderbird/52.5.0
MIME-Version: 1.0
Content-Type: multipart/alternative;
 boundary="------------2CB0785977D5F282F06ACAA3"
Content-Language: en-US

This is a multi-part message in MIME format.
--------------2CB0785977D5F282F06ACAA3
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Good Afternoon,

Some great development in the last period. Please visit our common
friend for more. I’ll leave the laptop with him; please return it to the
same location after fetching the data. More details on specific content
to come later in a separate email. Content and pass codes can be
recovered using the usual procedure. Stay tuned!

Thank you,

JL
```