Ryan Hinson

Advisor: Professor Henderson

Expected Graduation Date: May 2021

Description of Project:

This project will be a cyber forensics project. I will use two virtual machines, one posing as a criminal, the Riddler from Batman, the other as a cyber forensics analyst. The criminal system will hide different artifacts in the system. These will all be files to emulate the planning of a jewelry store heist. Included in these files will be documents, photos, and emails. The investigator system will be used to find these artifacts. I will employ different forensics tools in order to find the artifacts and build a case against the criminal. I will also record each step of the process, for instance the installation and use of the tools. This will serve as a step by step process to allow others to replicate the forensic process.

Proposed Implementation Languages:

I will be using two Linux based virtual machines to do this project. One will be a Kali system, and the other will be an Ubuntu system.

Any Software/Hardware needed:

Two Linux virtual machines, the investigator system will be using Kali. The criminal's system will be set up using an ubuntu Virtual machine, I will use my personal computer to set up these virtual machines. I also have electronic versions of sample chain of custody forms and case report forms that I will fill out as I do things on the system.

Motivation:

I want to do this project because I would like to work in the cyber forensics field. This project will give me some experience working with the forensic tools used to recover evidence on systems and analyze it. I will also be pulling in criminal justice aspects by using case report and chain of custody forms for my process. This will give me experience in what a real forensics officer may do in order to get evidence in a case.

Outline of Future Research Efforts:

I will complete this project by setting up two virtual machines. The first will be an Ubuntu virtual machine, and it will represent a criminal's computer that was seized by a police department. The criminal being the Riddler from Batman. This system will be used to hide artifacts to be uncovered that show the planning of a jewelry store heist. I will vary the software used when creating artifacts. Examples of this include word documents, excel spreadsheets, PowerPoints, photos, and emails. The documents included will be a heist planning list, a list of associates who can help with the crime, and a riddle leaving clues about the crime. The photos will include pictures of the jewelry store, maps of the surrounding areas, and a getaway plan. The emails will be mock emails sent to the Riddler's associates about the heist plans. I will keep a record of dates and times when these artifacts are created. This will allow me to compare the

metadata that is recorded in the discovery phase with when the original creation was done. I will also use flash drives on this virtual machine to copy files as another artifact I can find.

The second virtual machine will be a Kali virtual machine. This machine will represent a Cyber forensics analyst who is given the system by an investigator. This system will use different forensics tools, that are included in Kali, to look for the artifacts and recover them. I will record the process on how to install and use each tool. This will serve as a teaching tool for others to follow. I will keep a record of times and dates on which I find each artifact and keep notes on exactly what I did. I will include some screenshots of the tools running. After the entire forensics process is done, I will also fill out a supplemental case report, include copies of the notes I take. I will also fill out the chain of custody form that will keep a record of who has custody of the evidence. This will be done to emulate the real-world process that a cyber forensics analyst may go through.

Schedule:

CSCI 498:

Week 1: Construction of the Riddler's VM.

Week 2: Begin hiding artifacts in the system. This will include some traveling to other places to utilize different Wi-Fi networks.

Week 3: Continue the process of creating artifacts.

Week 4: Finish all the Artifacts.

Week 5: Construct the VM for forensics.

Week 6: Install tools and record the process for this.

Week 7: Finish installing all the tools.

Week 8: Use forensic VM to make a copy of the criminal's hard drive and begin forensic analysis and extract artifacts.

Week 9: Continue using tools to extract the artifacts and ensure that notes are kept on use of the tools and on the process.

Week 10: Continue extracting the artifacts from the VM.

Week 11: Finish extraction of the artifacts.

Week 12: Compile my notes together and ensure they fit what is needed.

Week 13: Fill out the case report forms and finish the chain of custody form for the evidence and my notes and forms.

CSCI 499:

January – March 1st: Finish recovering artifacts and finalize paper work.

March 2nd – April 5th make presentation and record it.