Defense Documentation

Ryan Hinson

Advisor: Professor Julie Henderson

1) The purpose of my project was to create a simulated Cyber Forensics scenario. This was done to not only learn about the artifacts a forensic analyst looks for, but also to learn about the tools they use to extract these artifacts.

2) I researched the industry standard tools needed to complete this project and what artifacts are commonly extracted during the forensic process.

3) I used a windows machine to create the artifacts. I then used FTK Imager, Access Data Registry viewer, and Exiftool to extract the artifacts and analyze them.

4) The requirements were for me to create the artifacts on a machine, and use the proper tools to image the hard drive and extract the artifacts.

5) The first step I took was creating the artifacts. This included downloading pictures from the internet and from a connected phone. It also included various web searches as well. All of this is contained in the criminal artifact record document.

Next I made a copy of the hard drive using ftk imager. I also used this to create custom content images of various parts of the hard drive

![Graphical user interface, text, application

Description automatically generated]()

![Graphical user interface, text, application, email

Description automatically generated]()

After this I used FTK imager to locate the files I needed. I found the plans document and all the pictures first.

![Graphical user interface, text, application, email

Description automatically generated]()

I then used Exift tool to examine the photos and plans document for metadata.

![Text

Description automatically generated]()

![Text

Description automatically generated]()

After these files were analyzed, I used registry viewer to analyze the registry files in the custom content image. This allowed me to see wifi connections as well as search history.

Table

Description automatically generated

Table

Description automatically generated

Lastly, I used all this data to construct a timeline of when all these artifacts were created. This log is contained in the Forensic log spreadsheet. After this, I filled out a supplemental case report form and chain of custody form. Both of these documents would be used in a real life investigative procedure.

6) My project did not require a test plan.

7) My project did not have test results.

8) I had a few different issues with my project. My first idea, as indicated in the proposal document, was to use two different virtual machines for the project. However, I was not able to figure out how to copy the Vm’s hard drive. This led me to creating a second user on a personal windows machine. The other Issue I had was getting registry viewer to work. I ended up having to remake the image of the hard drive and the custom content images, but was able to get it functional.

9) I would like to be able to make this project work using a Virtual machine so that someone recreating the process does not have to copy personal data. I would also like to expand it to work with more tools and artifacts in the future.