Defense Documentation

Ryan Hinson

Advisor: Professor Julie Henderson

**Statement of Purpose**

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. The simulated Scenario I put together sees a criminal leaving digital artifacts while planning a bank heist. I set it up for the criminal to be the Riddler from Batman, just to add some fun to the project. I then mocked up some police report documents to show that the computer was given to me as a forensic analyst.

**Research and Background**

I researched the industry standard tools needed to complete this project and what artifacts are commonly extracted during the forensic process. I was able to find that they often look for web searches that can show motive as well as documents or metadata from pictures (Murphy, 2019). Professor Henderson was able to point me in the right direction to find the tools I needed like FTK Imager and Registry Viewer.

**Software and Hardware**

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. I used FTK imager version 4.5, Registry Viewer 2.0, and Exiftool 12.09.

**Project Requirements**

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. I created web searches on two different WI-FI networks, downloaded images from the internet included two different security cameras and a bank floorplan. I copied six images from a smartphone connected by a USB, and I created a word document containing plans for the bank robbery. I then used FTK imager to image the hard drive and the RAM. I also created a triage image using FTK imager. I then found the plans document and the pictures using FTK imager. I analyzed these and the lnk files using Exiftool. Once this was done, I used registry viewer to analyze the registry files to see the web searches and the WI-FI connections.

**Project Implementation**

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.

Below are two screenshots of my Forensic Log. This shows a complete list of the artifacts I found and what tool I used.

Graphical user interface

Description automatically generated with low confidence

Text

Description automatically generated

**Test Plan**

My test plan was to compare the times I found the artifacts to when they were created. Therefore I took down the date and times of creation for the artifacts. The document showing these is included on the Github. I then took my forensic log and compared it to this document to ensure that everything matched.

**Test Results**

I was able to successfully recover all of the documents and show that they matched. If you compare the forensic log and the criminal artifact record the dates and times match. The included screenshots from Exiftool show how I got the information for the forensic log.

**Challenges Overcome**

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.

**Future Improvements**

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.

# References

Murphy, C. (2019). *WHAT ARE FORENSIC ARTIFACTS? – MY FAVORITE ARTIFACTS, PART 0.* Retrieved from Tetra Defense: https://www.tetradefense.com/digital-forensics-services/what-are-forensic-artifacts-my-favorite-artifacts-part-0/#:~:text=Things%20like%20registry%20keys%2C%20files,you%20do%20while%20using%20it.