George Thompson and Donn Shannon

4/11/18

CSC-494

Digital Forensics Project 2: Digital Forensics virtual machine Toolkit

1.0 Introduction

Digital Forensic analysis is a very important sub-field in cybersecurity. Forensic Analysts are tasked with finding digital evidence that a crime has been committed. We live in the technology era, where with each technological advance, more and more aspects of our lives are affected by technology. As a side-effect of this, more and more criminals are using technology to enhance and facilitate their criminal activity. As a result of this, Government agencies including the FBI, CIA and the Department of Defense(DOD) have poured countless amount of money into the best forensic experts as well as investing in the best cutting-edge forensic analysis tools. Some of these tools are rather expensive, costing hundreds and sometimes thousands of dollars. This is just including the commercial tools that we know about, but the government is paying their research laboratories across the country much more money for private, state of the art, government-use only, forensic analysis tools.

Nevertheless, the need for free, accessible forensic tools is clear. For this project, We will try to see if we can create a "toolkit" of forensic analysis tools, to see if it is possible to cover all the bases of forensic analysis without spending a single dollar. This toolkit will be in the format of 2 virtual machines, one Ubuntu VM and one Windows 10 VM. These VM's will host multiple digital forensic analysis tools and we will show users how to use each one. The "bases" of forensic analysis, or the types of tools we will try to find will include: Acquisition, Disk and data capture tools, File viewers, File analysis tools, Registry analysis tools, Email analysis tools, Network forensics tools, Database forensics tools, Memory forensic analysis, Hard drive forensic analysis, Data Recovery, Document Metadata Extraction, and Logfile Analysis. Some tools may fall into multiple categories.

This project will benefit anybody who is interested in forensic analysis and will like to learn more about it, but perhaps does not the resources to purchase commercial forensic analysis tools. This project will also serve as a tutorial for every tool that we choose to incorporate into our toolkit. Also, If anybody is looking for every type of forensic analysis tools, for either windows or Linux, our deliverable will be able to provide that.

2.0 Categories of Digital Forensics Tools

- **Acquisition - Tools which generate forensic image files from devices, for analysis or archival purposes.**

Belkasoft Acquisition Tool is designed to help investigators to obtain data from a hard or removable drive, mobile device, RAM, or even cloud server data. The acquired image can be then analyzed with any third-party forensic analysis tool.

- **File system analysis tools - The file system tools allow you to examine file systems of a suspect computer in a non-intrusive fashion. Tools which examines data in a volume (i.e., a partition or disk) and interprets them as a file system. There are many end results from this process, but examples include listing the files in a directory, recovering deleted content, and viewing the contents of a sector.**

Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones.

- **Registry analysis tools - Tools which extract information about system architecture and installed programs, from**

X-Ways Forensics is an advanced platform for digital forensics examiners. It runs on all available version of Windows. It claims to not be very resource hungry and to work efficiently. It has many features, but can be used as an Internal viewer for Windows registry files.

- **Network forensics tools - Tools which analyze all network traffic going in and out of a computer. It can log all the network protocols used as well as the data sent over the network.**

WireShark is the world's foremost and widely used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and provides Deep inspection of hundreds of network protocols.

EtherApe is a free program built on the structure of Etherman. It is designed as a high level wide range network monitoring tool which provides a graphical display to the user illustrating packet information.

- **Memory forensic analysis- These tools can be used capture and analyze data stored in volatile memory such as RAM.**

Volatility is a memory forensics framework for incident response and malware analysis that allows you to extract digital artefacts from volatile memory (RAM) dumps. Using Volatility you can extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs and more.

- **Data Recovery (including file carving)- Tools which recover deleted or lost files from the hard drive. File Carving involves reassembling computer files from file fragments.**

foremost is a Linux based program data for recovering deleted files and served as the basis for the more modern Scalpel. The program uses a configuration file to specify headers and footers to search for. Intended to be run on disk images, foremost can search through most any kind of data without worrying about the format.

Linux Memory Extractor (LiME) is a Loadable Kernel Module (LKM), which allows the acquisition of volatile memory from Linux and Linux-based devices, such as those powered by Android. The tool supports dumping memory either to the file system of the device or over the network.

3.0 The Digital Forensics Virtual machine

Show screen shots of your machine in action

4.0 Project evaluation

Give written directions on how to use your project and evaluate its usability

5.0 Discuss your project and evaluation results

6.0 Future Work