Writeup 1

Kevin Turkington

I. Advanced Forensics

During last weeks lectures we learned the appropriate tools to conduct both live and file analysis of malware on samples provided by Mr. Beek. This week with the samples Mr. Beek has provided, we analyzed the status of a system after a given case. As well as reasons for tampering with systems or using them to access illegal or inappropriate things such as the following:

- Fraud
- Intellectual Property Theft
- General Attack Intrusions
- Inappropriate use of internet
- Child Exploitation
- eDiscovery Supporting

Without the objective to look into malware, we were challenged with the task of thinking out side of the box uncovering the missing pieces of a story. Through a fabricated story with a simple USB image from a North Korean solider.

The purpose of forensic computing is not to determine the guilty status of an individual, but rather what happened to the system itself, according to Mr. Beek. However before we could dive into a system and start exploring we needed to learn the four principles of advanced forensics:

- Minimize data loss
- Record Everything
- Analyze all data collected
- Report findings

In order to minimize data loss of a given system is to preserve it through the use of cryptography hashes. The exact reason for this is to prevent attackers from tampering with potential evidence, as well as prevents analysts from unknowingly changing data. After creating a hash of the system it is important to begin recording times when evidence was found so a time line can be created later in the forensic investigation. Then a forensics analyst can begin collection data from a system. During a live (physical) takeover of a system an analyst must collect data on the order of volatility(RFC 3227). This begins with capturing:

- System memory
- temp file system
- process tables
- network connections

- network routing
- Acquisition of disks
- Remote logging
- Physical configuration
- Backups

All need to be researched, recorded, and copied to a target disk. This can be done with tools such as FTK Imager or Fast Dump. Once deemed unsafe or the following have been recorded the system can then be taken to a lab for further analysis.

In the lab a hard drive can be connected to a write blocker to read system files without altering them. With an image of the system memory a forensic analyst can find last known key strokes, as well as passwords from websites or other protected systems. In addition analysts can gather evidence via ”data carving”. The method is intend for recovery of data on a given hard disk. Through the use of these methods evidence can be recovered on the kernel level by using both photorec_win as well as stealthkits.

This these tools we were able to uncover data from a usb image that contained the Korean national anthem, malware that could be installed on a target system of the perpetrators choice. As well as a list of potential targets of the North Korean government.