Collin Williams

Week 2 Reading Assignment 2

Incident Response and Handling (ITSY-2442-007)

Brian Stuhl

The investigation process of a Forensic Analysis is very complicated with lots of steps. Instead of listing every step, it is more useful to break it into 4 high-level sections of the investigation phase.

1. Background Information

In this phase, the investigator does not have access to any physical devices yet. They document everything, even if it seems obvious in the moment. They might interview people, if it helps in gathering background information. They might collect information from social networks or other internet activity.

If search and seizure warrants are required, this is when the investigator would apply for them.

2. Collect Evidence

In this phase, the investigator is "in the room where it happened." They stay extremely careful to not destroy evidence–digital or physical. This might include turning off a computer, or possibly leaving it on if it would destroy evidence to turn it off. For example, if the computer was logged in to the Tor network, turning it off would destroy evidence. When collecting digital evidence, they create image backups of ALL data, even if it doesn't seem important. They continue to document everything.

As the amount of evidence increases, it is imperative that the investigator stay organized. They might consider adopting a naming scheme for different pieces of evidence to stay organized (DFIRScience, 2020).

3. Analyze Evidence

Good forensic investigators NEVER do analysis on the original machine. It is dangerous to do so because analysis procedures might accidentally deteriorate the evidence, and this would be detrimental to an investigation.

The analysis procedure will always be different depending on the case, but forensic investigators might do some of these things in an analysis: Analyzing the file content for data usage, Analyzing the date and time of file creation and modification, Finding users associated with file creation, access, and file modification, Determining the physical storage location of the file (EC-Council, 2016).

4. Case Analysis

In the final step, forensic investigators take the information that they learned from the evidence and apply it to the case as a whole. For example, they might ask: What were the intentions of this person? or, Why did they have an account on this website? This kind of reflective analysis is the end result of a forensic analysis.

Bibliography

DFIRScience. (2020, October). *DFS101: 6.3 Data Acquisition.* https://www.youtube.com/watch?v=EebalZ0jI64

EC-Council. (2016). *Computer forensics: Investigation procedures and response (CHFI)* (11th ed., p. 152). Cengage Learning.