CS 373 summer 2019

Week 2 write up

Kirsten Wollam

Incident response & Forensic methods:

There are many situations where an investigation might be warranted. These include crimes like fraud, IP theft, and child exploitation, as well as corporate situations like data breaches or intrusions and inappropriate use of the internet by employees.

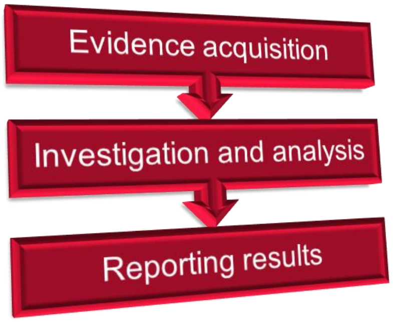

Figure 1 - Advanced Forensic Methods Slide 7

The goal of an investigation is not to prove someone guilty or innocent. It is to understand what happened and be able to explain it.

The first step it to get the evidence as safely and accurately as possible. This is a balance between preserving the data and making sure that it is not compromised and the crew is safe in the environment. You want to minimize any potential data loss. It is important to keep in mind that actions may be damaging useful data like memory which can get over written with every action taken. It is also necessary to record every step you take in the process so that you know what might have been impacted. In particular recording the actual time as well as the system time immediately is important to be able to compare what happened when. On an incident team there should be someone appointed to just document a forensics journal for the team. Date will need to be gathered from all levels of the larger system, such as application data, physical data storage, and network and server logs among others. It is very important to consider the volatility of the different sorts of data when gathering evidence. System memory, temporary files, and network connection information is all very volatile and should be gathered first. Command line prompt or tools like FTK imager can be used to capture a memory dump as well as other volatile files before anything else is done to the machine.

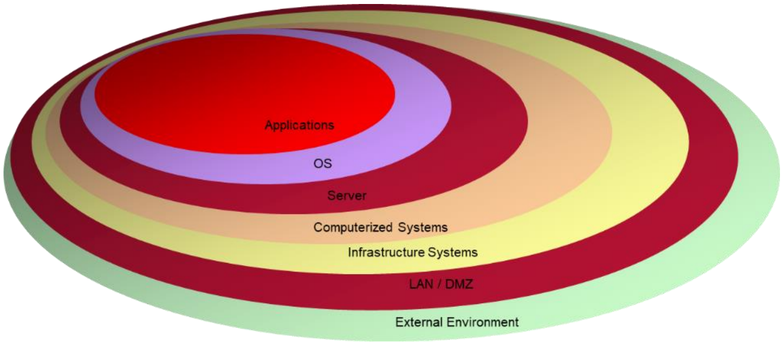

Figure 2 - Advanced Forensic Methods Slide 13

The next step is to investigate and analyze what you found. This work will typically be done on copies of the recovered data and the steps involved in this will depend on the type of incident and what was recovered. It is also important to prove the same things in multiple ways to be sure that the analysis is correct. Investigations can take a significant amount of time since they involve larger and larger amounts of data and multiple kinds of devices. One important type of analysis will be to study the memory dump.

Volatility is an excellent tool for this with many plug-ins to dissect the data so that you don't have to try to manually pull strings. Another important thing to look at is the registries. This is because windows logs almost everything that happens in the registry. For instance using a registry tool you can see when devices were attached to the machine, when things were set to auto run, and what the most recently run programs were. Another good item to look at is the $MFT master file table. This will let you really look into the timeline of what happened on the machine. This will often become central to the investigation.

Lastly the results will need to be reported. This is much more difficult that it might seem. The findings usually need to be explained to an audience that does not have any technical expertise on the subject. This could be as part of a criminal investigation or trial, or a corporate investigation, but they all require explaining to people who will make determinations based on the evidence provided.