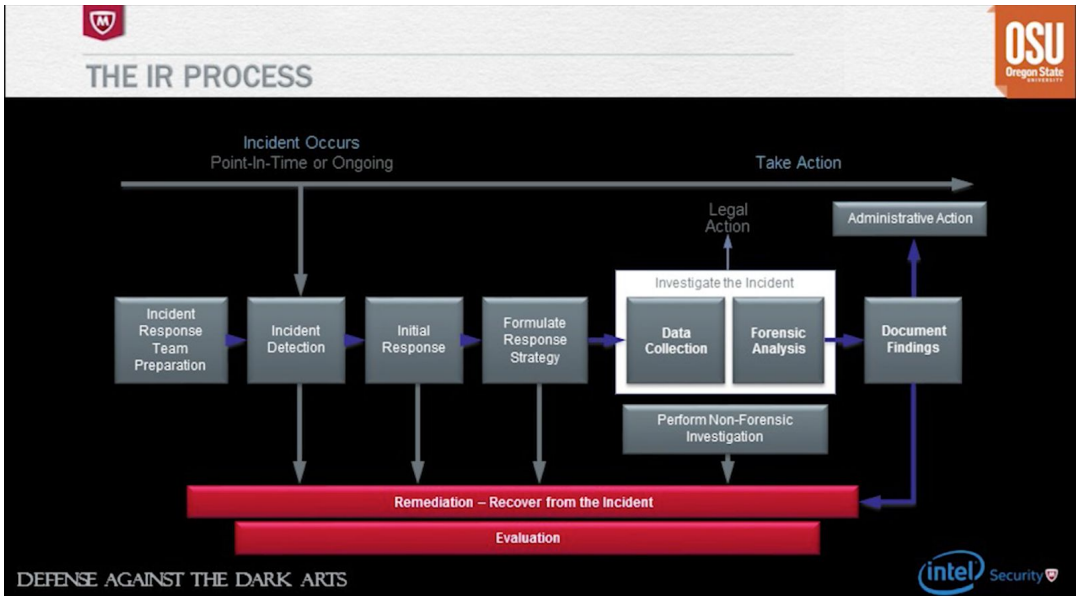
Nicolas Barraclough
10/11/2020
CS373 - Defense Against the Dark Arts

Week 2 Write-Up

This week I learned and practiced basic computer forensics. I became more informed about the system registry, forensic tools and commands, and about the process of investigating a system. I learned about good practice when performing a forensic investigation by logging a timeline of events, minimizing system memory loss, and keeping physical and digital safety in mind. In the incident response process, there is an important sequence that the team should follow. The team should be prepared for a possible incident so that if/when something goes wrong, a prompt response can be initiated. The incident response process is diagrammed below:



Advanced Forensics - Part 4 Lecture Video

When looking into a system, it can help to make a timeline of events. First, recording the moment of access by the investigator and then each subsequent event. The master file table indicates when files were created, accessed, and deleted on the machine. Physically writing down these events and their timestamps can help stand against litigation/scrutiny and malpractice accusations and will help log the investigation. Noting the system clock and if within a network, noting the system time of all accessible devices will help associate specific files and keep the investigation log accurate.

I learned that by looking into a system, I could inadvertently overwrite important data. A good way to minimize memory loss is to be mindful of which tools are being used and if the same investigatory action can be doable via the command prompt. Also, investigating or copying certain areas before others can minimize the amount of data

lost. According to RFC 3227, the order of volatility goes: system memory, temporary file systems (swapfile / paging file), process table and network connections (specific process information could be dumped), network routing information and ARP cache, forensics acquisition of disks, remote logging and monitoring data, physical configuration and network topology, and backups. A few things that I didn't know were stored in the system memory are keystrokes, clipboard data, wireless network keys, even things labeled "secondary" data like email attachments.

Aside from logging activity and creating a timeline for the investigation, the lecture videos covered other tips for good-practice forensics. For example, one should never install forensic software onto a suspect's machine. This immediately influences evidence which makes it inadmissible in court. As a forensic investigator, there should be no "fishing" for evidence to a predetermined "guilty" party. The goal is to simply prove actions performed by the user (or abuser) of a system. It is very important to stick to the relevant information when investigating another person's private computer. Another practice that a good forensic analyst does is to always create a memory dump on an external device. I didn't quite understand why that is, but I assume it is to prevent any tampering to the memory dump file.

I feel like I will need to review this week's material again, because there was a lot to unpack. I didn't get a chance to do the lab at the end of the second set of lecture videos, but I assume we will be doing that as an assignment - I haven't checked yet. If not, it seems like a fun challenge and an effective way to practice the tools and techniques I learned this week.