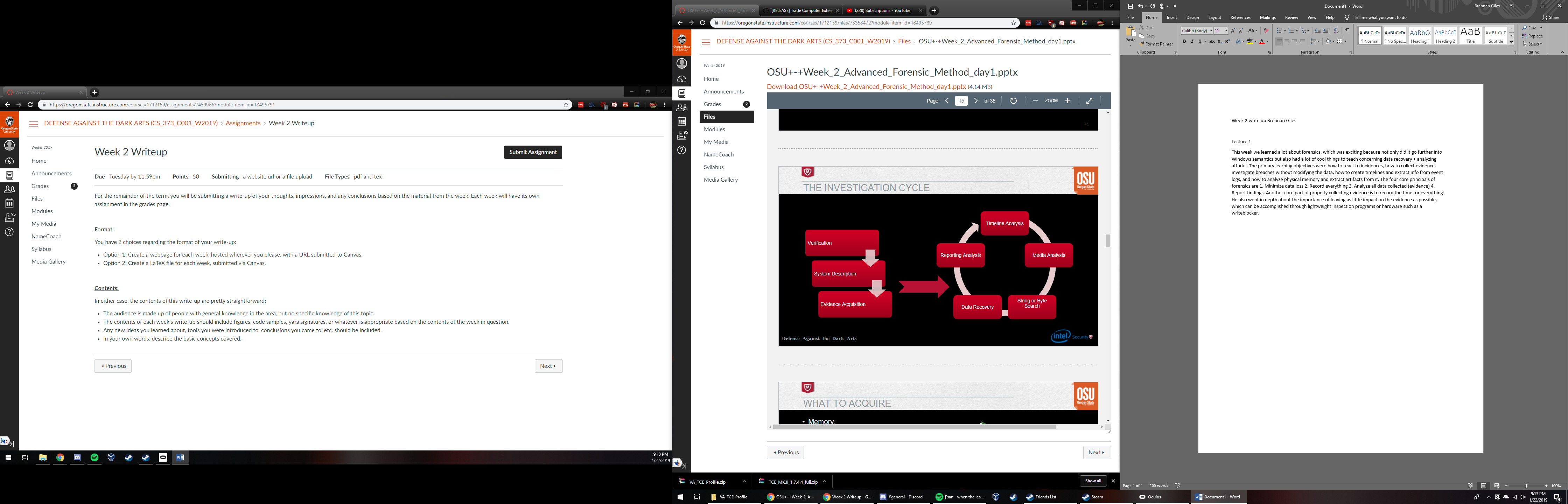
Week 2 write up Brennan Giles

Lecture 1

This week we learned a lot about forensics, which was exciting because not only did it go further into Windows semantics but also had a lot of cool things to teach concerning data recovery + analyzing attacks. The primary learning objectives were how to react to incidences, how to collect evidence, investigate breaches without modifying the data, how to create timelines and extract info from event logs, and how to analyze physical memory and extract artifacts from it. The four core principals of forensics are 1. Minimize data loss 2. Record everything 3. Analyze all data collected (evidence) 4. Report findings. Another core part of properly collecting evidence is to record the time for everything! He also went in depth about the importance of leaving as little impact on the evidence as possible, which can be accomplished through lightweight inspection programs or hardware such as a writeblocker. The following is the investigation cycle which is core to forensics:



I wanted to include this image because it is a succinct explanation of how investigations should proceed. When investigating, the most volatile data should be collected first; this is data that will be lost upon shutdown such as system memory, swapfiles, paging files, process tables and network connections (such as a listening port that the attacker may close soon). After this, all non volatile data should be gathered such as time/date stamps, event logs, web/ application logs, and the registry if applicable. If the attacker is inexperienced, there may be evidence of attacker tools still left on the machine as well. Next he talked about physical memory, and how RAM can often hold invaluable information that an investigator should retrieve. RAM can store artifacts, information about processes that have exited, cache from recently used programs, and more. Tools like pslist can help with this process. Next, he talked about the physical memory of hard drives, which divide itself into pages with “flags” letting the computer know where saved data begins and ends. When deleted, the computer simply removes the flags but that data persists, and with the right software we can carve out that abandoned data for recovery. As stated in class, the only way to properly wipe memory “is with a 12 gauge”. The instructor used a program called “volatility” to help with his forensics.

Lecture 2

We started out by talking about Windows Registry, which is a critical aspect of the operating system and even more important for malware analysis. RegMon can be used to display registry activity, and regedit can be used to edit the registry. The only real hives inside are HKEY\_USERS and HKEY\_LOCAL\_MACHINE. Looking at this data can help understand actions that took place on the machine and the timeline of those actions since everything is timestamped. $MFT and Reg-Ripper are both great tools for automatically created timelines from the registry. Here are some things to look for: Pagefile.sys, index.dat, windows event logs, application config files and logs, prefetch folder, and evidence of malware, rootkits, or anything else malicious. Three other good sources of information are Dr. Watson logs, setupapi.log, and schedlgu.txt. Photorec\_win can be used to recover deleted files from physical memory as discussed in the previous lecture.