Week 2 Writeup

This week there were several topics that struck a note with me. The lectures had a strong focus on standard procedures for obtaining computer forensic evidence. We also discussed the following:

* Challenges in obtaining forensic data from a standard/conventional hard drive vs an SSD hard drive
* The order of volatility with data in a computer
* Important files to capture when performing forensics on volatile data in a Windows environment
* What data we expect to retrieve from these files that are considered important and volatile
* Windows Registry and the critical data that can be found in the files, and a good tool to use to review these files, RegEdit

The procedures for obtaining forensic evidence on a computer is not much different when obtaining evidence from other crimes. As an investigator you must do the following:

* Create a journal, with dates and times, of your actions and observations
* Gather evidence in a secure environment, and with a sense of urgency, capture any volatile data first while keeping a light footprint on the machine in question
* Establish a chain of custody with the evidence
* Note all checksum hashes of the data collected to ensure it can be compared at a later time, further adding credence to the integrity of the data
* Make backup copies of the information retrieved to safeguard against loss, theft, or destruction of the valuable information
* When running forensics on the machine, search for deleted/erased files for evidence
* Ensure the evidence is stored a secure location where only individuals with clearance can access the data

Doing a quick Google search I found various publications, both from the public and private sectors, on how to handle malware evidence. You may click on the link for find this information:

<https://www.google.com/search?q=standard+procedures+for+malware+forensics&oq=standard+procedures+for+malware+forensics&aqs=chrome..69i57.12309j0j7&sourceid=chrome&ie=UTF-8>

Another thing I was completely unware of was the challenges in collecting forensics evidence from SSD drives. As explained by forensicmag.com in this article (link: <https://www.forensicmag.com/article/2013/05/forensic-insight-solid-state-drives>), SSD’s require you to write data in blocks. This is always true. Every time we want to write new data to the SSD, it takes a copy of that information, clears a block hence clearing the bits in that block, and writes the data. The same is true if we modify data that already exists in a block. Per the article, the best example to illustrate this is a Etch-A-Sketch model:

In my research, most malware investigators have yet to solve this problem with SSD’s. However if you wish to find more information below is a link to a Google search with various articles and white papers:

<https://www.google.com/search?q=forensics+with+hard+disk+drive+vs+ssd&oq=forensics+with+hard+disk+drive+vs+ssd+&aqs=chrome..69i57.15357j1j7&sourceid=chrome&ie=UTF-8>

Artifacts are objects or areas within a computer system that hold important information relevant to the activities performed on the computer by the user. Below is a table of files, and their locations, that are critical to malware forensics:

In particular, the Registry can contain incredibly valuable information for a forensic investigator. It is a hierarchical database that contains the default and user-defined setting in a Windows system. It serves a repo, that monitors and records the activities that a user performs on a system in the form of registry entries. This includes programs installed and uninstalled, USB devices connected, most recently accessed files, IP addresses and more. Most of this can be viewed with RegEdit.

PICTURE OF REGISTRY

Another key take away for the week is the order of volatility for data. This is imperative for all malware investigators since it dictates what analysis you’ll be performing first on a suspect machine.

Lastly, I searched for cases that have been imperative in establishing case law for computer crimes, particularly with the presentment of digital artifacts as evidence. Below are some interesting case law and rules regarding digital evidence: