Tu Lam

CS 373 (Defense Against the Dark Arts)

Dr. Bram Lewis

October 6, 2021

Homework #2 Write-Up

Week #2 of the class was a way to see how to use ***forensic*** to identify problem and preserve evidence for cases such as thing in the world of cybersecurity. On top of that, we dive into the topic of ***different cases of forensics we can study***, ***memory analysis***, and ***volatility***.

Starting off the topic of ***forensic computing*** is a way to identify, preserving, analyzing, and presenting digital evidence where it is legally use. These types of forensics can be classified in three ways: ***live***, ***post-mortem (memory/disk)***, and ***network-based*** forensics. Forensics follow the four basic principle that was listed in a couple sentence ago and that was record everything (identify), minimize data loss (preserving), analyze all evidence (analyzing), and report finding (presenting). From here, the ***evidence*** can then be used to prove or disprove fact. During forensic, evidence collection can come in form of network, operating system, database/application, peripheral, removeable media, and human testimony.

Through the power of forensic and evidence in cybersecurity, we can use see what the process would be like and how data are collected. Below are two figures showing the ***incident response (IR)*** and the process of IR collecting evidence, and these are base from the lecture.

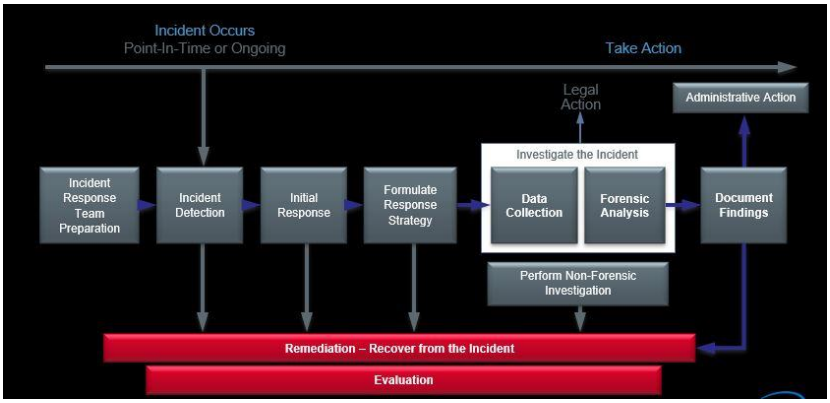

Figure #1: The IR process

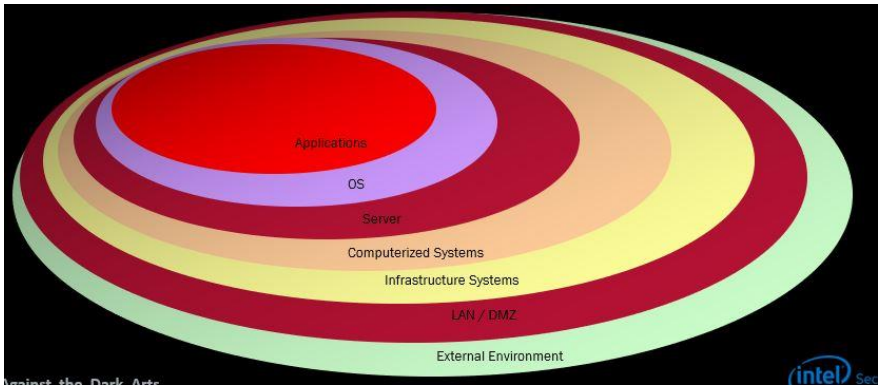

Figure #2: Digital evidence via the IR

Beside all about the IR process, we are taught about the ***APT-case*** where we learn how to map the evidence of it through the process of 7 steps. We were also diving into the ***investigation cycle*** where it the cycle of finding the timeline, media analyzing, byte search, data recovery, and reporting analysis. On top of that, we look at ***Locard's Exchange Principle*** where it is a principle describing that when two objects interact with each other, there will a transfer of material that exert from each object onto the other. This is telling us that if the evidence has been tampering with, the evidence will become compromised evidence.

Moving on to ***volatility***, when collecting evidence, we should see the scale of the evidence from volatile to less volatile. This mean that look at data that can easily be loss if something happens to the machine to something that can be save without losing data. This is an important part when it comes to collecting evidence and know the state of the evidence.

Last is the ***memory analysis*** where we look at both the physical and virtual memory as part of forensic. Physical memory is display as short-term memory in a computer (RAM) where the data will slowly decay and lost as soon as it disconnects from power or clock source. Virtual memory is part of mapping on page and page are part of physical memory that has been divided. These pages will then allocate virtual memory from it and can put data and transfer thing over. The case of memory, the evidence of it can have a lot of things from running processes at the time of the memory snapshot, open files for each process, including path to file on disk, open registry keys for each process, and more.

Through this week lesson on the topic of advanced forensics. We were able to learn about the way how to collect evidence and the process of how to do it through the IR process in the case of a cyber-attack. We also dive into on how identify the evidence to see the severity of it and how much we should be careful of preserving it and kept it as a way to prove/disprove something from a cyberattack.