NAME: Megan Leonard

TODAY’S DATE: 2/12/2023

# ISEC 375 Homework 3

Answer the following questions based on your reading of the textbook, the module key points, and the instructor’s presentation this week.

1. **[9 points]** The file server of your company is hacked, and sensitive financial data is sold to the competitors. You are appointed as the forensics investigator of the security incident by your company. The forensic investigation may cause civil litigation and has to be done as soon as possible. Your company lawyer requested the “images” of all hard drives, which are related to the cyber incident. He has limited knowledge of information technologies. When you arrive at the crime scene, you see that all of the files are stored in a Storage Area Network of total size 200 Terabytes and configured RAID 5. Which type of data collection method do you prefer? (a disk-to-image file, a disk-to-disk copy, a logical disk-to-disk, a disk-to-data file, a sparse copy, a logical copy) If the company lawyer insists on acquiring the images of all hard drives at the SAN infrastructure, which justifications would you bring to persuade him that it'd not be possible?

The data collection methods we can use are limited because of the size we are working with, and the lawyer having a limited knowledge of technology. To determine which methods to use, we can start by getting rid of ones that are not possible. The disk-to-image file would take a lot of time as we are working with a lot of data. A disk-to-data-file would be hard as well as the file would be too large to reasonably work with as we have a lot of data. For giving a copy to the lawyer, I would use the disk-to-disk copy as it would make sure the lawyer got a full copy and can take it to any technical person on his side to look over should he so desire. For working, I would choose the logical and sparse copies as it will limit the amount of files we need to look through and can save a lot of time. I would as well give copies of these to the lawyer explaining what each disk has like how the logical disk have specific files that are for the case, the sparse disk has fragments of deleted data, and the first disk he got is a copy of the original data. The best way to explain to him is by first explaining how much data we are working with. Using a screenshot for with 300kb for example, I would walk him through the conversions that it takes from the kilobyte up to the Terabyte. If each byte on the hard drives are images, with 1 billion kilobytes being in a single terabyte, and each image is 300 kilobytes, then we would have 666,666,666.66666667 images. If we are using 100 megabits per second with the 200 terabytes, it would take about 204 days without any pauses which is not possible for the case.

1. **[9 points]** You will do forensics investigation of a laptop computer, which has an embedded hard drive (an onboard solid-state hard drive that cannot be removed from the laptop). Please write the steps to acquire an image of the hard drive of the laptop. Please list the hardware and software you need to acquire the image.

To acquire an image from the hard drive of the laptop, you start with what type the laptop is so you know if there are specific tools you need like how windows has their own acquisition tools. We will need an external drive to copy to and use Mini-WinFE to protect the external drive. If the laptop runs Linux instead of Windows, we will still need the external drive and instead use a Linux Live CDs such as Kali Linux or CAINE. We can also use the AccessData FTK Imager to copy the image to the external drive while using the Linux or Windows external drive protections. After this, we will need another system to upload the image to.

1. **[6 points]** You acquired the image file of the embedded hard drive of the laptop computer in question-2, what is the next step of the forensics investigation? Why? If you don’t want to use any third-party tool for the operations in this step, which utility would you prefer to use?

After acquiring the image file, we want to validate the evidence because we need to know that the image file was successfully gotten and the information lines up with what we wanted to get. If I do not want to use any third-party tool I would use Linux validation as Windows does not have its own hashing algorithm. If I am already working within the FTK Imager, then I would use that for validation.

1. **[6 points]** As forensics investigator of the case explained in question-1, would you consider making remote network acquisition?

I would not consider making a remote network acquisition because while it would be very useful, we are still dealing with a lawyer who does not understand technology well and he could use not being knowledgeable to his advantage and end up getting the copying postponed as he could claim that we were messing with the hard drives and would either have to wait for someone else to come in to make sure that we are only copying the drives. There is also the case of security measures being in place against remote access and having to install a remote agent on the suspect computer or turn off the safety measures would lead to trouble with the lawyer as his only real understanding is that we are messing with the suspect computer downloading things onto it that he does not understand. There is also the fact in the name remote, he may not understand it’s a way to download the data and may think it is a way of altering the hard drives without physically touching them. Overall, I would not consider this choice as it would most likely lead to a headache because of the lawyer’s lack of knowledge about technology.