NAME: Megan Leonard

TODAY’S DATE: 2/18/2023

# ISEC 375 Homework 4

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]** What is digital evidence? What are the main differences of digital evidence when compared to the physical evidence like a weapon, paper document, or visible injury? You are appointed as the forensics investigator of a hacking case. You seized the computer of the hacker. What digital evidence you may collect from this computer?

Digital evidence is information that is found in a digital form like meta data or computer files. The main difference between digital and physical evidence is how easily it can be changes and altered. If you have a system you are gathering digital evidence from, you need to make sure to follow the proper protocols and record the metadata as it can tell you the time the system was accessed for your case. You need to work with a copy as just logging into the system would change the date of access and could ruin your case. The physical evidence is not as easy to change as holding a gun for evidence in a properly mandated way, does not risk the gun being altered and unable to be used. Digital evidence that I would collect would be the metadata, so we know when it was last used, a copy that we can then edit, files that pertain to the case, and any deleted data we can recover as that is likely to have something.

1. **[12 points]** You are in a crime scene. There is a running Windows 10 computer in the crime scene. What actions do you take to acquire the digital data in the running operating system? (Please write your justifications and assumptions clearly to get the full marks. Because the answer depends on your professional judgment, different actions could be taken for different situations/judgments. So please share not only the actions but also your reasons.)

To acquire the digital data, I would start by making sure that the power is running properly to the system as we need to make sure the power does not cut out before we are finished, sometimes plugs can be found halfway in the wall and can be pulled out easily so we should make sure that is unlikely to happen. As the system is running, we will record any applications that are running and any active windows or shell sessions as they could be important and hold valuable information. Then, we save the data of the currently running programs as safely as we can so we can make sure nothing will interfere with our data collection. We then, record the metadata so we can prove that everything was running prior to our investigation as we need to make sure we can not be accused of bringing any of the programs up and the system. Finally, we close out of the applications and shut down the computer as we can make sure if shuts down properly and does not cause trouble. As we are at the crime scene, it is best to take note of what is running and when as we want to make sure that we have proper documentation before we touch the computer.

1. **[9 points]** What is the primary purpose of hashing digital evidence? What are the three rules for forensic hashes? Assume that the hash function does not meet one of the rules, please select one rule and explain how the forensic investigation can become invalid with the lack of that rule?

The primary purpose of hashing digital evidence is to prove that the file has not changes. If it changes, then the hash value would not be the same. The three rules of forensic hashes are first, you can not predict the hash value of a file or device, second, no two hash values can be the same, and third, if anything changes in the file or device, then the hash value itself must change. If we look at the second rule, no two hash values can be the same, and our file does not meet that rule, we will have some problems. The hash is created as a means of verifying that data has not been changed so by having two files that hold different information but the same hash, we can not prove that the file we are using as evidence has not been altered. If we can not show that the file has not been altered, we would not be able to use that file as evidence within the case as the opposing side could claim that we altered the file.