NAME: Megan Leonard

TODAY’S DATE: 3/19/2023

# ISEC 375 Homework 7

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 the Exif format? How do you know that a JPEG file is an Exif JPEG? As the forensic investigator, do you trust the date and time extracted from Exif data? Why? How do you corroborate the date and time obtained from Exif data?

Exif format is the metadata that we can find contained within an image file. We can determine that a JPEG file is an Exif JPEG based on the metadata that is collected as Exif will have the date and different image information such as size. The date and time can not be trusted easily as they can be changed. Depending on the evidence found, you can look at the history timeline to see if there are discrepancies within it.

1. **[6 points]** During a forensic investigation, you extracted a file with an unknown extension. What do you do to find information about the type of file? What do you do to analyze the file further?

The file extension can be identified with different tools ones that either take the file’s unique signature and compares it with known files of its database or hashing to compare it with other files on the system. Once we know the file extension, we can look up some of the sites that cover different extensions to understand more about it and what we could find on the file.

1. **[9 points]** What are the basic steps and tools for locating and recovering deleted, damaged, and defragmented graphics files in a hard drive?

We first locate the graphics fragments using a tool such as autopsy to go through the slack of the drive taking in any fragments that they find. We then check the header as if we find it damaged, we need to reconstruct it by comparing the hexadecimal values of files with the same graphics format pattern. All clusters of the fragmented file will be located and exported. We find the start and end cluster numbers for each group of sectors and copy each into their correct sequence. We make sure the header is readable with a graphics viewer and add on the .txt extension.

1. **[6 points]** Why steganography is generally difficult to detect? What cases and conditions make it easier for a forensic investigator?

Steganography is generally hard to detect because it is hidden inside image files either by inserting it into the data structure or by substituting the bits of the file. Cases that make it easier are when there are duplicates of the file with different hash values, and when the steganography program is still installed on the drive.