Assignment 1

CIS425 – Fall Term 2017

Point Value: 100 points

Assignment Due Date: **In class Thursday September 7, 2017**

Submission Instruction

Please write the questions and your answers to those questions on a Microsoft Word document and convert it to a pdf file. The name of the file should be HW1_YourLastname_YourFirstnme.pdf. Please submit the pdf file on *Schoology* by 11:59pm and a hard copy of the file to the instructor in lecture.

Short answers

1. **What are the three elements of forensics? Please explain what is digital forensics in your own words?** (10 points)
   The three elements of forensics include: science, evidence, and law. Digital forensics is the process of using computer science and investigation procedures for legal purposes of digital evidence in order to present findings in an orderly manner to solve a legal problem.

2. **Please list at least five different digital devices that could be investigated and analyzed by a digital forensics practitioner?** (10 points)
   Smart phone
   camara
   laptop
   USB drive
   CD's
3. **What is the difference between expert and non-expert witness on court?** (10 points)

   An expert witness is someone who has proper credentials regarding the case. An expert witness must know more about a particular subject than the average person. For example a doctor, scientist, baker. Therefore, a non-expert witness would be someone who was there at the scene who witness what happened.

4. **What is the use of digital forensics? Please describe at least 4 different uses.** (10 points) Criminal investigations, civil litigation, intelligence, and administrative matters. Criminal investigations including: child pornography, identity theft, homicide, and sexual assault. Civil litigation refers to a legal dispute between two or more parties that experience money damage rather than criminal penalty. An example would be eDiscovery refers to any process in which electronic data is sought, located, secured, and searched w/ the intent of using it as evidence in a civil or criminal legal case. The use of intelligence is important in digital forensics because we do not want terrorists to have it easy by using information technology to communicate, recruit, and plan attacks. Administrative matters because employees should not be operating a personal side business while using company computers while on company time. For example, in 2007 the SEC (Securities and Exchange Commission) opened an investigation into the potential misuse of government computers. They found numerous access denials for pornography for regional staff members, a senior Attorney at Headquarters downloaded so much pornography that he ran out of disk space, etc.
5. **Please explain LOCARD's Exchange Principle in your own words?** (10 points) Edmond Locard, a Pioneer French criminalist, stated that a person who enters a crime scene will bring some type of evidence into the crime scene. Therefore, leaving some type of evidence behind, which can be used as forensic evidence.

6. **Given the following 10 decimal numbers, please find their corresponding binary and hexadecimal formats, and ASCII character**. **In order to find their ASCII character, you can google ASCII table online**. (20 points)

   73 76 105 107 101 67 83 52 57 54

   73- binary:01001001, hex:49, character:I
   76- binary:01001100, hex:4C, character:L
   105-binary:01101001, hex:69, character:i
   107-binary:01101011, hex:6B, character:k
   101-binary:01100101, hex:65, character:e
   67- binary:01000011, hex:43, character:C

83- binary:01010011, hex:53, character: S
52- binary:00110100, hex:34, character: 4
57- binary:00111001, hex:39, character: 9
54- binary:00110110, hex:36, character: 6

7. **What is file signature analysis**? (10 points)

   Each file has a file extension (.doc, .pdf, .jpeg, etc.). A person can actually change a file extension. Using forensic tools to check whether or not the correct content is contained in the file based on the file's extension is part of file signature analysis. When a file whose header does not match the extension (making them easily discovered) it is known as, file signature analysis.

8. Please explain the difference between Volatile and Nonvolatile memory? (10 points)

Volatile memory is data in RAM that only exists as power is supplied. Once the power is removed, the data starts to disappear. Nonvolatile memory is data or files saved on the hard drive. They remain even after the computer is powered down.

9. Please explain the difference between Active Data and Latent Data? (10 points)

Active Data is where the operating system sees and tracks these files. Latent data is deleted or partially overwritten. Therefore, these files are no longer tracked by the operating system and are "invisible" by the user.