DFSC 1316: Digital Forensics and Information Assurance I

Exam Review 1, 2017 Fall

Format: Multiple choices, true and false, short answers.

Time: 80 minutes.

Data: Oct 3, 2017, 8:00 – 9:20.

Introduction to DF and IA

Review topics:

1. What is DF?
2. What are typical application of DF?
3. What are the basic steps to conduct DF?
4. Examples of digital evidences?
5. Why digital evidence needs special handling, how to conduct such special handling?
6. What is imaging? How it differs from regular file copy, and how to verify images?
7. Things to consider when writing report?
8. What is IA?
9. What are the goals of IA? What are the meaning of each of them? How to enforce them?
10. What are the 3 types of non-repudiation?

Sample questions:

1. (true of false) the best practice for digital forensic investigation is to directly examine the original evidence, e.g., computer or smart phone, instead of examining a duplicate of the originals.
2. Give real-life examples for the 3 types of non-repudiation?

Chapter 2: Numbering System

Review topics:

1. What are the *positional notation* for base 10, base 16, and base 2?
2. How to convert among decimal, hexadecimal, and binary numbers (table will be provided)?
3. Simple calculations (addition) with two numbers in any of these three bases.

Sample questions:

1. Write the positional notation for the binary number 1001 0110.
2. Convert above binary number to decimal and hexadecimal number.
3. Convert the decimal number 234 into binary.
4. Calculation: C7(h) + C8(h) = ?

Basics of the Internet

Review topic:

1. What is ISO-OSI?
2. Layers and functions of OSI?
3. What is the TCP/IP protocol suite? How it differs from and related to ISO-OSI?
4. Layers and functions of TCP/IP protocol suite?
5. What address types we have discussed in class, which layers they associate with?
6. When a message is routed from one host to another, how is this messages addressed, and how do addresses change?

Sample questions:

1. What is MAC address, which network layer it associates with, and how it is useful in forensic investigation?
2. What is the function of the IP protocol, and what is the function of the TCP protocol? How do they differ?

IP Addressing

Review topic:

1. What is classful IP address, how does it work?

2. What is classless IP address, how does it work?

Sample questions:

1. Give an example of a class-B IP address.

2. For the following classful IP address, find out the Net ID and Host ID: 180.8.17.9.

3. For the following classless IP address, find out the Net ID and Host ID: 230.8.24.56/19.

Email and Browser Forensics

Review topic:

1. The protocols used for email exchange between servers, and between servers and client.

2. Understand the concept of email header, and able to retrieve basic information out of an email header.

3. The basic concept of how HTTP works, i.e., the client-server architecture.

4. The basic concept of how cookie works.

Sample questions:

1. What is email header, what information is contained in an email header?

2. When conducting browser forensic investigation, what are the items that may contains useful information?