ICS 428: Digital Forensics

Quiz 2 (100 POINTS)

*This quiz is based on the digital forensics concepts so far covered in part 2 of the course. It is designed to motivate you to revisit and review the course text as well as the other course material.*

**Answer 5 Questions Only.**

*Submit answers in PDF Format*

|  |
| --- |
| **Question 1**   1. Explain the differences in resource and data forks used in the Mac OS (6pts) 2. How does the Mac OS reduce file fragmentation?(4pts) 3. What is the function of superblock in the Linux file system? (4pts) 4. On most Linux systems, where is current user login information contained? (2pts) 5. What's the Disk Arbitration feature used for in Mac OS X? (2pts) 6. For digital evidence, why is an evidence bag typically made of antistatic material? (2pts) |
| **Question 2**   1. What purpose do rainbow tables serve in digital forensics examinations? (2pts) 2. What is bit-shifting and how might a file with bits shifted be different from the original? (2pts) 3. What is block-wise hashing (1pt) 4. How might a forensic examiner use block-wise hashing technique during an investigation?(3pts) 5. How are hash value databases such as Known File Filter (KFF) used in the digital evidence gathering process?(3pts) 6. How can a digital forensic examiner detect if there are hidden partitions in the hard drive (3pts) 7. Name and describe two steganalysis techniques (“attacks”). (6pts) |
| **Question 3**   * 1. A forensic image of a VM includes all snapshots. True or False?(1pt)   2. Which Registry key contains associations for file extensions?(1pt)   3. Differentiate between type 1 and type 2 hypervisors(1pt)   4. Where does a layered defense strategy put the most valuable data?(1pt)   5. What layers of the OSI model does a packet analyzer examine?(1pt)  1. Name and describe briefly each of the three modes of the NSA defense in depth (DiD) strategy (9pts) 2. Briefly describe the procedure for conducting forensic analysis of virtual machines (6pts) |
| **Question 4**   1. Give 3 examples of information that might be obtainable from email logs on an email server (3pts) 2. What information is contained in an email header? (2pts) 3. Name and describe any three tasks involved in investigating e-mail crimes and violations (9 pts) 4. Describe at least two challenges forensic investigators may face when conducting social media investigations (6pts) |
| **Question 5**   1. List at least six pieces of information available on a mobile device that might be useful to a forensic investigator (4pts) 2. What is the purpose of a subscriber identity module (SIM) card? (4pts) 3. List at least four areas where data can be retrieved from in a mobile device (2pts) 4. Briefly describe some steps involved in setting up and conducting a forensic investigation on a suspect mobile device (4pts) 5. Name and briefly describe any 3 mobile forensic methods that are within NIST guidelines (6pts) |
| **Question 6**   1. What is an *examination plan* in the context of digital forensic reporting?(1pt) 2. Describe 3 of the conditions that must be met in order for the expert witness to testify to an opinion or a conclusion? (6pts) 3. What information does a written preliminary report contain?(4pts) 4. What is the purpose of hypothetical questions in litigation?(2pts) 5. What do the following terms mean?(6pts)    1. deposition banks    2. high-risk document    3. lay witness |
| **Question 7**   1. Briefly describe 5 of the ways in which integrity of digital evidence can be assessed and maintained?(10pts) 2. Briefly describe five of the considerations that can help an expert witness avoid deposition problems that could affect the client negatively?(5pts) 3. List the steps in the typical order of trial proceedings, whether civil or criminal (5pts) |
| **Question 8**   1. What are some of the questions a court may ask in determining whether to disqualify an expert in a case?(5pts) 2. Give five examples of ethical errors that can lead to future liability or ethical complaints about an expert’s report (5pts) 3. What are some of the ethical responsibilities owed to you as an expert witness by the attorney who has retained you? (5pts) 4. What are some of the considerations in deciding whether to use commercial or personally created tools for investigations e.g. what might be the benefits and disadvantages of either choice?(5pts) |