Unit VII Worksheet

Please read the assigned readings of your textbook before attempting to answer the following multiple choice and true/false questions regarding the information in your assigned reading. This is not a required test but rather a practice test to assist you in completing the unit for this course. Please contact your professor if you have any questions regarding concepts presented within the required readings.

CHAPTER 11

1. Which crime scene is the most complex to investigate?
   a. single scene
   b. multiple scene
   c. network crime scene
   d. all are equally complex

2. Which network architecture is most closely associated with network crime scenes?
   a. LAN
   b. WAN
   c. internet
   d. none of the above

3. Which of these is an IP Address?
   a. AA-0A-10-AB-AF-00
   b. 192.684.168.255
   c. 192.168.0.5
   d. none of the above

4. The best source for technical information needed in a network investigation is:
   a. any computer expert
   b. an experienced computer crime investigator
   c. the library
   d. the system administrator for the system in question

5. Minimization:
   a. ensures that we do not do more harm than good to the victim
   b. ensures we do not scare future victims with heavy-handed seizures
   c. means reducing the amount of intrusion to the target system
   d. all of the above

6. Which method of seizure is not consistent with minimization?
   a. on the spot imaging of discs containing evidence
   b. seizing the computer system
   c. copying a back up tape
   d. taking images of a working RAID disc.
ANSWER KEY (Chapter 11)
1. c
2. c
3. c
4. d
5. d
6. b
CHAPTER 12

1. What principle should guide the analysis of storage devices?
   a. protect the original evidence
   b. be able to explain every action you take
   c. be aware of the limits of your ability to search legally
   d. all of the above

2. Why should the analyst wipe the analysis drive?
   a. to prove to the court that there could not have been contamination from another drive
   b. to eliminate any intellectual property violations from retaining the suspect’s information
   c. to extend the life of the hard drive
   d. to speed the hard disk’s retrieval of information

3. What two forces have guided the recent development of hard drives?
   a. density and speed
   b. mass and acceleration
   c. rock and hard place
   d. new operating systems and the international standards organization

4. Why don’t we use the evidence drive for analysis?
   a. we could but we would risk losing the original to which we compare copies.
   b. it is faster to copy it several times and then back to another hard drive than to just use it.
   c. there is no way to prevent altering the drive if we perform analyses on it.
   d. it is usually locked away in an evidence locker and we would have to sign it out on the chain of custody every time we use it.

5. When files are deleted from a hard drive:
   a. they are gone forever
   b. the entry in the file allocation table is marked as empty and the files are ignored on the hard drive
   c. the entry in the file allocation table is marked as empty and the files are removed from the hard drive
   d. they cannot be restored without a laboratory

6. An image of a hard drive:
   a. contains all of the data from the drive, including slack space and unallocated clusters
   b. contains irregularities that produce a different hash value than the original
   c. is a still photograph taken of the platters of a hard drive
   d. is not useful to a forensic examiner under the "best evidence" rule

7. File systems provide programs and users with the ability to:
   a. store data
   b. retrieve data
   c. store and retrieve data
   d. none of these are correct
8. Which of the following statements is true of storage media?
   a. storage media come in a variety of sizes, shapes, and capacities
   b. direct access media (e.g. disks) are faster than sequential access media (e.g., tape)
   c. the speed of backup media often provides a clue as to the use the media
   d. all of the above

9. Forensics packages must:
   a. come with built-in support and training
   b. have a report-writing feature
   c. acquire, authenticate, and analyze data
   d. run on any type of computer used by the forensic analyst.

10. Why can’t we point to a hard disk and say where exactly the data came from?
    a. it is written in tracks that are microscopic in size
    b. we can’t say where the data is physically without completely mapping logical structure to physical surface
    c. cylinders place data on multiple disks so there is no one place
    d. all of the above

**ANSWER KEY (Chapter 12)**

1. d  
2. a  
3. a  
4. a  
5. b  
6. a  
7. c  
8. d  
9. c  
10. d