1. Digital forensics is commonly applied to which of the following activities? **1 point**

- ○ Criminal investigation
- ○ Incident handling
- ○ Data recovery
- ◉ All of the above

2. NIST includes which three (3) as steps in collecting data? (Select 3) **1 point**

- ☑ Acquire the data
- ☑ Develop a plan to aquire the data
- ☑ Verify the integrity of the data
- ☐ Normalize the data

3. What is the primary purpose of maintaining a chain of custody? **1 point**

- ○ To keep valuable hardware securely locked to tables or floors.
- ○ So a person in possession of evidence will know who they are allowed to give it to next
- ○ To allow for accurate client billing
- ◉ To avoid allegations of mishandling or tampering of evidence.

4. True or False. Digital forensics had been used to solve a number of high-profile violent crimes. **1 point**

- ◉ True
- ○ False

5. True or False. Digital forensics report is a summary of your findings. If your case goes to trial, your testimony can, and usually does, involve far more detail than is in the report. **1 point**

- ○ True
- ◉ False

6. Which section of a digital forensics report would include using the best practices of taking lots of screenshots, use built-in logging options of your digital forensics tools, and exporting key data items into a .csv or .txt file? **1 point**

- ○ Overview & Case Summary
- ○ Forensic Acquisition & Examination Preparation
- ◉ Findings & Analysis
- ○ Conclusion

7. Which types of files are appropriate subjects for forensic analysis? **1 point**

- ○ Data files
- ○ Image and video files
- ○ Application files
- ◉ All of the above

8. Deleting a file results in what action by most operating systems? **1 point**

- ○ Random data is immediately copied into the memory registers used by the file to obfuscate the previous contents.
- ○ The memory registers used by the file are erased and marked as available for new storage.
- ○ The file is copied to a trash or recycle folder and the original memory registers are erased.
- ◉ The memory registers used by the file are marked as available for new storage but are otherwise not changed.

9. Forensic analysis should always be conducted on a copy of the original data. What type of copying is appropriate for getting data from a live system that cannot be taken offline? **1 point**

- ○ A disk-to-disk backup
- ○ An incremental backup
- ○ A disk-to-file backup
- ◉ A logical backup

10. How does a forensic analysis use hash sets acquired from NIST's Software Reference Library project? **1 point**

- ○ Hashes will help you quickly zero in on deleted files.
- ◉ They can quickly eliminate known good operating system and application files from consideration.
- ○ They are useful in identifying files that were created outside the United States.
- ○ They provide a record of known encrypted malware.

11. Which three (3) of the following data types are considered non-volatile? (Select 3) **1 point**

- ☑ Logs
- ☑ Dump files
- ☐ Free space
- ☑ Swap files

12. Configuration files are considered which data type? **1 point**

- ○ Dynamic
- ◉ Non-volatile
- ○ Volatile
- ○ Static

13. True or False. When collecting forensic data from a running system, you should always attempt to collect non-volatile data first. **1 point**

- ○ True
- ◉ False

14. Which three (3) of the following are application components? (Select 3) **1 point**

- ☑ Data files
- ☑ Authentication mechanisms
- ☐ OSI Application Layer protocols
- ☑ Application architecture

15. Which of these applications would likely be of the least interest in a forensic analysis? **1 point**

- ○ Web host data
- ○ Chat
- ○ Email
- ◉ Patch files

16. The Internet layer of the TCP/IP stack, also known as the Network layer in the OSI model, contains which two (2) protocols that are very useful to a forensic investigation? (Select 2) **1 point**

- ☑ ICMP
- ☐ LDAP
- ☐ UDP
- ☑ IPv4 / IPv6

17. Which device would you inspect if you were looking for event data correlated across a number of different network devices? **1 point**

- ○ Firewall
- ○ Intrusion detection system
- ○ Packet sniffer
- ◉ Remote access server

18. Which of these sources might require a court order in order to obtain the data for forensic analysis? **1 point**

- ◉ ISP records
- ○ Intrusion detection systems
- ○ System Event Management systems
- ○ Firewalls

Coursera Honor Code Learn more

☑ I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit **Save draft**