

- 1.) What are the four phases in a complete computer forensic examination?
- 2.) What is the difference between criminal and civil offenses?
- 3.) What does the Fourth Amendment guarantee people?
- 4.) What is a consent search and can consent be withdrawn?
- 5.) What is a preservation request?
- 6.) What is a search warrant?
- 7.) Explain the Daubert Rule.
- 8.) What are Ethics and how do they relate to digital forensics?
- 9.) What is Lockard's Exchange Principle?
- 10.) List the stages of the Scientific Method.
- 11.) What is the difference between a witness and an expert witness?
- 12.) What are the "3V's" of Big Data forensics?
- 13.) Give examples of how a crime scene can be documented.
- 14.) What is digital evidence?
- 15.) What facts should be documented when collecting evidence?
- 16.) What does preservation of digital evidence entail?

- 17.) If you find a device that is turned off in general, you should do what?
- 18.) If you find a device that is turned on in general, you should do what?
- 19.) When should an examiner use write protection and why would an examiner use write protection?
- 20.) What is Volatile Data?
- 21.) What is encryption? What data types can encryption be applied to?
- 22.) What would be some reasons to conduct live imaging?
- 23.) When and why do forensic examiners only use sterile media for evidence collection?
- 24.) Why do forensic examiners validate their hardware and software tools?
- 25.) What does a full forensic image of a physical disk contain?
- 26.) What is a hash value?
- 27.) Will the size of the data change the length of a hash value?
- 28.) List some of the common uses of hashing
- 29.) Describe the TCP (Transmission Control Protocol) handshake used to initiate data transfer.
- 30.) What is the function of DNS (Domain Name Service)?
- 31.) What is a MAC address?
- 32.) What are case specific keywords?

33.) What would a forensic examiner be looking for using this GREP search?

Grep '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' Test.txt

34.) What are some of the limitations of text based key word searches?

35.) What are some of the considerations and qualities a forensic examiner must think about to produce a well written report?