1.) What are the four phases in a complete computer forensic examination?

1. Collection and storage
2. Preservation Process
3. Analysis and Testing
4. Reporting and testifying

2.) What is the difference between criminal and civil offensives?

Criminal law deals with offenses against the state. The burden of proof is beyond a reasonable doubt and its punishment can include time in jail.

Civil law deals with violation of contracts, lawsuits, divorce, and custody. Civil cases often have a financial aspect. The burden of proof is a preponderance of the evidence.

3.) What does the fourth guarantee people?

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Violations of the 4th Amendment result in the evidence being thrown out.

4.) What is a consent search and can consent be withdrawn?

A person can give permission for an official to seize and search property. Consent should be given in writing; it must be given freely without any coercion. Consent can be withdrawn at any time.

5.) What is a preservation request?

May request provider to, for 90 days, preserve records in its possession pending the issuance of legal process. Only for information already in their possession, not future information. Must have a date and time with IP address to request records. May need to provide Account ID number or other information.

6.) What is a search warrant?

A search warrant is a legal document authorizing search and/or seizure of property. Search Warrants are issued upon the legal standard of probable cause supported by oath. A search warrant authorizes the search of a place to look for evidence, contraband or stolen property to be used as evidence in a criminal case.

7.) Explain the Daubert Rule.

The Daubert Rule is a test regarding the admissibility of scientific evidence. The Daubert Rule requires that a technique used to obtain evidence has been tested and verified, has been subject to peer review and publication, has a known rate of error, and the method has been accepted by the scientific community.

8.) What are ethics and how do they relate to digital forensics?

Ethics are a set of principles that guide a person's behavior. Information security professionals that make poor ethical decisions may ruin a case or their careers. Unethical behavior may also severely disrupt the lives or businesses of those being investigated. Unethical behavior may lead to civil actions.

9.) What is Lockard's Exchange Principle?

Cross-transfer of evidence when a person comes in contact with an object or another person. Exchange can link a perpetrator of a crime to a particular place, victims, or evidence. Locard's Principle applies to computer forensics Electronic activities produce artifacts detectable through digital forensic examination.

10.)List the stages of the Scientific Method.

- Observation –inspects what evidence he can obtain from the crime scene.
- Developing Hypothesis –based on observations.
- Testing Hypothesis –check the authenticity and reliability of evidence.
- Verify Hypothesis – If a hypothesis is true, then a conclusion is made-If not, a new hypothesis will need to be formed.

11.) What is the difference between a witness and an expert witness.

A witness is a person who provides testimony under oath and is subject to perjury laws. A witness Has a connection to the incident and/or information about the incident.

An expert witness is a witness with expert knowledge, skill, experience, and training. They are considered an expert in a specific field and are usually paid.

12.) What are the "3V's" of Big Data forensics?

- Volume - the complexity and size
- Velocity - speed that modern data travels
- Variety – unstructured and multi structured.

13.) Give examples of how a crime scene can be documented.

- Photographs
- Video
- Diagrams

14.) What is digital evidence?

Digital evidence is anything that can hold data, such as: Computers &Tablets, Cell Phones, Routers, Watches, Cameras, Internal & External Drives, Smart Devices (Refrigerator, TV's, Nest & Echo devices).

15.)What facts should be documented when collecting evidence?

- Who collected the evidence.
- Where was the evidence found.
- When was the evidence found (date&time).
- What is the evidence.
- Why is it being seized.

16.)What does preservation of digital evidence entail?

- Prevent destruction of original evidence.
- Make no changes to original evidence.
- Maintaining the integrity of original from collection through court proceedings.

17.)If you find a device that is turned off in general, what should you do?

If you encounter a device/computer turned off, leave it off.

18.)If you find a device that is turned on in general, you should do what?

Photograph all open windows, note any running applications/processes, destructive processes, and Encryption. Then Collect RAM. If you encounter a destructive process pull the plug from the back of the device.

19.)When should an examiner use write protection and why would an examiner use write protection?

Always use Write Protection when working with original evidence. When previewing or live imaging. Forensic examiners use write protection to prevent changes to the original evidence.

20.) What is Volatile Data?

Data that is eradicated when the device loses power. Data not written to the hard drive.

Examples:

- RAM (Random access memory)
- Malware
- Certain Registry keys
- Running processes
- Network connections

21.) What is encryption? What data types can encryption be applied to?

The process of randomizing data making it unreadable. Securing the data to prevent unauthorized access.

Encryption can be applied to:

- Files
- Containers
- Volumes
- Disks

22.)What would be some reasons to conduct live imaging?

- Encryption
- System Cannot be shutdown.
- Collecting RAM

23.)When and why do forensic examiners only use sterile media for evidence collection?

Forensic examiners only use sterile media for evidence collection to ensure no pre-existing data is on target drive and avoid cross contamination.

Forensic examiners use sterile when collecting evidence and when copying evidence onto a storage drive.

24.)Why do forensic examiners validate their hardware and software tools?

Forensic examiners validate their hardware and software tools to ensure accuracy of their findings and conclusions, become aware of software issues, and avoid having their findings being called into question.

25.) What does a full forensic image of a physical disk contain?

A full forensic copy (image) contains, Allocated Files, File Slack, Deleted Files, Unallocated space,

Unused space, HPA/DOC.

26.) What is a hash value?

A hash value is A way to represent data with a unique numerical value using a mathematical algorithm.

27.) Will the size of the data change the length of a hash value?

Regardless of the size of the data the result is a fixed-length hexadecimal value.

Common hash types:

- MD5 -128-bit value - 32 charters long
- SHA1 – 160-bit value – 40 charters long
- SHA256 – 256-bit value – 64 charters long

28.) **List some of the common uses of hashing**

- Ensure Data Integrity during transmission
- Sector checking
- File integrity
- Validate forensic copies of hard drives.

29.)Describe the TCP (Transmission Control Protocol) handshake used to initiate data transfer.

The device requesting the communications sends an packet with the SYN bit turned on, the receiving device sends back a packet with the SYN and ACK bits turned on, The device requesting communication then sends back a packet with the ACK bit turned on and then communication starts.

30.)What is the function of DNS (Domain Name Service)?

DNS translated alphanumeric web addresses into IP addresses.

31.) What is a MAC address?

A MAC address is a hardware identification number that uniquely identifies each device on a network.

32.)What are case specific keywords?

Case specific keywords are Keywords that relate to one specific case.

Some examples are names of persons of interest, usernames, addresses (email or physical), phone numbers, slang that suspect uses, URLs they frequent, and filenames of interest.

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

An IP Address

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

- Bit-shifted (altering file data at a binary level)
- Encrypted
- Compressed
- Using non word charters

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

A well written report should be written for the target audience, clear and unambiguous, detailed, Concise, facts-based, and unbiased. The report should also Include any exculpatory findings.