1. When an investigator seeks a search warrant. Which of the following must be included in an affidavit to support the allegation of the crime?
    a. Exculpatory evidence
    b. Authorized requester (Ans)
    c. Exhibits
    d. Subpoena
2. Which group often works as part of a team to secure an organization’s computers and networks?
    a. Forensics investigators
    b. Data recovery engineers
    c. Network monitors
    d. Computer analysts (ans)
3. What questions should an investigator ask to determine whether a computer crime was committed?

Ans: An investigator should ask a variety of questions to determine whether a computer crime was committed, including:

- What type of computer or device was involved?
- What evidence is available?
- How was the computer or device used?
- Who had access to the computer or device?
- What are the potential motives for the crime?

Here are some specific examples of questions that an investigator might ask:

- Was the computer or device hacked or infected with malware?
- Were any files created, modified, or deleted?
- Were any unauthorized accounts created or used?
- Was any sensitive data accessed or exfiltrated?
- Was the computer or device used to commit other crimes, such as fraud or identity theft?
- Who had access to the computer or device at the time of the crime?
- Do any of the suspects have a history of computer crime?
- What could the suspects have gained from committing the crime?

The investigator should also consider the context of the crime. For example, if the crime occurred in a business setting, the investigator should ask questions about the organization's security policies and procedures. If the crime occurred in a personal setting, the investigator should ask questions about the victim's computer usage habits and security practices.

4. Which Pacific Northwest agency meets to discuss problems that digital forensics examiners encounter?
    a. IACIS
    b. CTIN (Ans)
    c. FTK
    d. FLETC
5. Which group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime?

    a. Network intrusion detection
    b. Incident response
    c. Litigation
    d. Digital investigations (ans)

6. To be a successful computer forensics investigator, you must be familiar with more than one computing platform.
    a. True (ans)
    b. False
7. Which term refers to an accusation or supposition of fact that a crime has been committed and is made by the complainant based on the incident?
    a. Allegation (Ans)
    b. Assertion
    c. Declaration
    d. Contention
8. Briefly describe hostile work environment.

A hostile work environment is a workplace in which harassment or discrimination is so severe or pervasive that it creates a work environment that a reasonable person would consider intimidating, hostile, or abusive. This can include harassment based on race, color, religion, sex, national origin, age, disability, or genetic information.

9. The law of search and seizure protects the rights of all people, excluding people suspected of crimes.
    a. False (ans)
    b. True
10. What must be done, under oath, to verify that the information in the affidavit is true?
    a. It must be challenged
    b. It must be notarized (ans)
    c. It must be examined
    d. It must be recorded.
11. After a judge approves and signs a search warrant, it's ready to be executed, meaning you can collect evidence as defined by the warrant.
    a. False
    b. True (ans)
12. Why is confidentiality critical in the private-sector environment?

Confidentiality is critical in the private-sector environment because businesses have a responsibility to protect their customers' personal information, trade secrets, and other proprietary data. Additionally, businesses need to maintain the confidentiality of their employees' personal information, such as medical records and payroll data.

13. Without a warning banner, what right might employees assume they have when using a company's computer systems and network accesses?
    a. Privacy (ans)
    b. Consent
    c. Authority

    d. Anonymity

14. What are some of the most common types of private-sector computer crime?

Some of the most common types of private-sector computer crime include:

- Data breaches: This involves the unauthorized access or theft of sensitive data, such as customer information, financial data, or intellectual property.
- Malware attacks: This involves the use of malware, such as viruses, ransomware, and spyware, to damage or disable computer systems or steal data.
- Phishing attacks: This involves sending fraudulent emails or text messages that appear to be from a legitimate source in order to trick people into revealing sensitive information, such as passwords or credit card numbers.
- Embezzlement: This involves using electronic means to steal money or other assets from a company.

15. Briefly describe the main characteristics of private-sector investigations

Private-sector investigations are often complex and time-sensitive. They may involve multiple jurisdictions and require the collection and analysis of large amounts of electronic data. Private-sector investigators also need to be mindful of the confidentiality of their clients' information.

16. What organization was created by police officers in order to formalize credentials for digital investigators?
    a. HTCN
    b. NISPOM
    c. TEMPEST
    d. IACIS (ans)
17. Chapter 5, Section 3, of the NISPOM describes the characteristics of a safe storage container.
    a. True
    b. False (ans)
18. Computing systems in a forensics lab should be able to process typical cases in a timely manner.
    a. True (ans)
    b. False
19. Methods for restoring large data sets are important for labs using which type of servers?
    a. TEMPEST
    b. WAN
    c. RAID (Ans)
    d. ISDN

20. What are the four levels of certification offered by HTCN?

The High Tech Crime Network (HTCN) offers four levels of certification in digital forensics:

- Certified Computer Forensic Technician, Basic Level
- Certified Computer Forensic Technician, Advanced Level
- Certified Computer Crime Investigator, Basic Level
- Certified Computer Crime Investigator, Advanced Level

Each level has different requirements for education, experience, and training.

21. During the cold War. Defense contractors were required to shield sensitive computing systems and prevent electronic eavesdropping of any computer emissions. What did U.S Department of defense call this special computer-emission shielding?
    a. Raid
    b. Tempest (ans)
    c. Nispom
    d. Emr
22. What are the questions you need to ask when planning the justification step of a business case?

When planning the justification step of a business case for a digital forensics lab, you should ask the following questions:

- What are the specific needs of the organization that the lab will address?
- What are the costs and benefits of establishing a lab?
- How will the lab improve the organization's ability to investigate and prosecute cybercrime?
- How will the lab protect the organization's assets and reputation?

23. How frequently should floors and carpets in the computer forensic lab be cleaned to help minimize dust that can cause static electricity?
    a. At least twice a week
    b. At least four times a week
    c. At least three times a week
    d. At least once a week (ans)

24. Which activity involves determining how much risk is acceptable for any process or operation?
    a. Risk analysis (Ans)
    b. Risk configuration
    c. Risk management
    d. Risk control
25. What is the maximum amount of time computing components are designed to last in normal business operations?
    a. 30 months
    b. 42 months
    c. 36 months (ans)
    d. 24 months
26. How frequently does IACIS require recertification to demonstrate continuing work in the field of computer forensics?
    a. Every 5 years
    b. Every 3 years (ans)
    c. Every 4 years
    d. Every 2 years
27. In addition to FAT16, FAT32 and Resilient File System, which file system can Windows hard disk also use?
    a. Ext3
    b. FAT24
    c. NTFS (ans)
    d. Ext2
28. Requirements for taking the EnCE certification exam depend on taking the Guidance software EnCase training courses.
    a. True
    b. False (ans)
29. For daily work production, several examiners can work together in a large open area, as long as they all have different levels of authority and access needs.
    a. True
    b. False (ans)
30. What kind of forensic investigation lab best preserves the integrity of evidence?
    a. A secure facility (ans)
    b. A shielded enclosure
    c. A fortified workplace
    d. A protected entity
31. When confidential business data are included with the criminal evidence, what are they referred to as?
    a. Pulbic data
    b. Revealed data
    c. Exposed data
    d. Commingled data (ans)
32. What will allow the investigator to arrive at a scene, acquire the needed data, and return to the lab as quickly as possible?
    a. A bit-stream copy utility
    b. An initial-response field kit (ans)

   c. An extensive-response field kit
   d. A seizing order

33. What type of files might lose essential network activity records if power is terminated without a proper shutdown?
    a. Io.sys files
    b. Password logs
    c. Word logs
    d. Event logs (ans)
34. Give some guidelines on how to video record a computer incident or crime scene.

When video recording a computer incident or crime scene, you should follow these guidelines:

- Use a high-quality camera with a tripod to keep the footage steady.
- Pan slowly and methodically around the scene, capturing all relevant details.
- Zoom in on important items, such as evidence markers, computer equipment, and any damage to the scene.
- Narrate the footage as you record it, describing what you are seeing and doing.
- Store the footage in a secure location and label it carefully.

35. Under what circumstances are digital records considered admissible?
    a. They are computer-generated records
    b. They are computer-stored records (ans)
    c. They are business records
    d. They are hearsay records
36. Briefly describe the process of obtaining a serach warrant.

To obtain a search warrant, you must submit a written affidavit to a judge explaining why you believe there is probable cause to believe that evidence of a crime will be found at the location you want to search. The affidavit must include specific facts and circumstances to support your belief.

If the judge is convinced that there is probable cause, they will issue a search warrant. The warrant will specify the location to be searched, the items to be seized, and the time period during which the warrant is valid.

Once you have a search warrant, you can execute it and search the location specified in the warrant. You must be careful to follow all of the procedures outlined in the warrant, and you must seize only the items that are specifically authorized.

37. When seizing computer evidence in criminal investigations. Which organization's standards should be followed?
    a. Department of Homeland Security
    b. US DOD
    c. NSA
    d. US DOJ (ans)
38. Describe how to use a journal when processing a major incident or crime scene.

journal is an essential tool for documenting the digital forensics process during a major incident or crime scene investigation. It should be used to record all actions taken, including:

- Date and time of each step
- Description of the step
- Tools and techniques used
- Results of the step
- Any other relevant information

The journal should be written in a clear and concise manner, and should be signed and dated by the investigator. This documentation will be essential for preserving the integrity of the evidence and for testifying in court, if necessary.

39. What standard is used to determine whether a police officer has the right to make an arrest, conduct a personal or property search. Or obtain a warrant for arrest?
    a. Reasonable cause
    b. Probable cause (ans)
    c. Reasonable suspicion
    d. Burden of Proof
40. Illustrate with an example the problems caused by commingled data.

Commingled data is data from multiple sources that has been mixed together. This can happen accidentally, such as when a user downloads a file from the internet and saves it to their desktop. It can also happen intentionally, such as when a criminal attempts to hide evidence by mixing it in with legitimate data.

Commingled data can make it difficult or impossible to identify and recover evidence. For example, if a criminal mixes a stolen file with a bunch of other files on a victim's computer, it can be difficult to determine which file is the stolen one.

Here is an example of the problems caused by commingled data:

A company is investigating a data breach. They believe that an attacker has stolen customer information from their database. However, the attacker has commingled the stolen data with legitimate customer data. This makes it difficult for the company to identify which customers have been affected by the breach.

41. Corporate investigators always have the authority to seize all computer equipment during a corporate investigation
    a. True
    b. False (ans)
42. ISP's can investigate computer abuse commited by their customers.
    a. True (ans)
    b. False
43. Which technique can be used for extracting evidence form large systems?
    a. Raid imaging
    b. Sparse acquisition (ans)
    c. Large evidence file recovery
    d. Raid copy
    44. What type of evidence do courts consider evidence data in a computer to be?
    a. Virtual
    b. Physical (ans)
    c. Invalid
    d. Logical
45. Describe the process of preparing an investigation team

The process of preparing an investigation team for a major incident or crime scene investigation typically involves the following steps:

1. Identify the members of the team. The team should include individuals with the necessary skills and experience, such as digital forensics investigators, incident responders, and law enforcement personnel.
2. Assign roles and responsibilities. Each member of the team should be assigned specific roles and responsibilities, such as lead investigator, evidence collection, and analysis.
3. Develop a plan of action. The team should develop a plan of action that outlines the steps that will be taken to investigate the incident and collect evidence.
4. Provide training. The team should be provided with training on the specific tools and techniques that will be used during the investigation.
5. Coordinate with other agencies. If necessary, the team should coordinate with other agencies, such as law enforcement or other government agencies.

46. When Microsoft created windows95, into what were initialization(.ini) files consolidated?
    a. The ini data
    b. The registry (ans)
    c. The metadata
    d. The inirecord
47. Drive slack includes RAM slack(found mainly in older Microsoft Oss) and file slack.
    a. True (ans)
    b. Flase
48. Which filename refers to the physical addess support program for accessing more than 4GB of physical RAM?
    a. Hal.dll
    b. Ntkrnlpa.exe (Ans)
    c. Io.sys
    d. BootSect.docs
49. The type of file system an OS uses determines how data is stored on the disk.
    a. True (ans)
    b. False
50. Briefly describe how to delete FAT files.

To delete a FAT file, the following steps must be taken:

1. The file's entry in the file allocation table (FAT) must be updated to mark the file as deleted.
2. The clusters that the file occupied must be marked as free.
3. The file's data can then be overwritten by new data.

It is important to note that deleting a FAT file does not actually erase the file's data from the disk. The data will remain on the disk until it is overwritten by new data. This means that it is possible to recover deleted FAT files using specialized software.

51. How can you make sure a subject’s computer boots to a forensic floppy disk or CD?

To make sure a subject's computer boots to a forensic floppy disk or CD, you can follow these steps:

1. Change the boot order in the BIOS or UEFI settings. This will ensure that the computer tries to boot from the floppy disk or CD first, before trying to boot from the hard drive.
2. Disable Secure Boot. Secure Boot is a security feature that prevents computers from booting from unauthorized devices. To disable Secure Boot, you will need to enter the BIOS or UEFI settings.
3. Insert the forensic floppy disk or CD into the computer.
4. Turn on the computer.

If you have followed these steps correctly, the computer should boot from the forensic floppy disk or CD.

52. What term refers to a column of tracks on two or more disk platters?
    a. Sector
    b. Head
    c. Track
    d. Cylinder (ans)
53. One way to examine a partition's physical level is to use a disk editor, such as WinHex. Or Hex Workshop.
    a. True (ans)
    b. False
54. Which filename refers to the deivce driver that allows the OS to communicate with SCSI or ATA drives that aren't related to the BIOS?
    a. Ntoskrnl.exe
    b. Boot.ini
    c. NTBootdd.sys (ans)
    d. Hal.dll
55. Summarize the evolution of FAT versions.

The FAT (File Allocation Table) file system was developed by Microsoft in the early 1980s. It was originally designed for floppy disks, but it was later adapted for use on hard drives.

FAT has evolved over time to support larger storage capacities and new features. The following is a summary of the evolution of FAT versions:

- FAT12: This version of FAT was used for early floppy disks and hard drives with up to 16MB of storage capacity.
- FAT16: This version of FAT was introduced in the late 1980s and supported hard drives with up to 2GB of storage capacity.

- FAT32: This version of FAT was introduced in the late 1990s and supported hard drives with up to 2TB of storage capacity.

FAT32 is the most recent version of FAT and is still widely used today. However, it is being gradually replaced by newer file systems, such as NTFS and exFAT.

56. Which certificate provides a mechanism for recovering files encrypted with EFS if there is a problem with the user's original private key?
    a. Administrator certificate
    b. Recovery certificate (ans)
    c. Root certificate
    d. Escrow certificate
57. What are some of the components of a disk drive?
58. Match the following:
    a. Microsoft's move toward a journaling file system
    b. The space between each track
    c. Ways data can be appended to existing files
    d. The unused space between partitions
    e. An international data format
    f. Microsoft's utility for protecting drive data
    g. Gives an OS a road map to data on a disk
    h. Unused space in a cluster between the end of an active file's content and end of the cluster
    i. Concentric circles on a disk platter where data is located
    j. The first data set on an NFTS disk. Which starts at sector[0] of the disk and can expand to 16 sectors
59. What are records in the MFT called?
    a. Metadata (ans)
    b. Hyperdata
    c. Infodata
    d. Inodedata
60. What specifies the Windows xp path installation and contains options for selecting the Windows version?
    a. Boot.ini (ans)
    b. BootSec.dos
    c. NTBootdd.sys
    d. NTDetect.com
61. What is forensic linguistics?

Forensic linguistics is the application of linguistic knowledge and methods to legal investigations. Forensic linguists can analyze text and speech evidence to identify the author, speaker, or recipient of a communication; to determine the meaning and intent of a communication; or to detect deception.

Forensic linguists can also analyze evidence for signs of plagiarism, copyright infringement, and trademarks infringement.

62. You can send and receive e-mail in tow enviroments: via the internet or an intranet(an internal network).
    a. True (ans)
    b. False
63. What is the main information being sought whrn examining e-mail headers?
    a. The originating e-mail’s domain name or an IP address (ans)
    b. The type of attachments included, if any
    c. The date and time the e-mail was sent
    d. The types of encryption used
64. A challenge with using social media data in court is authenticating the author and the information.
    a. False
    b. True (ans)
65. Explain how to handle attachments during an e-mail investigation.

1. Make a copy of the attachment. Do not open the attachment directly, as this could compromise the evidence. Instead, make a copy of the attachment and save it to a secure location.
2. Scan the attachment for malware. Use a reputable antivirus program to scan the attachment for malware. If the attachment is found to be infected with malware, do not open it. Instead, quarantine or delete the attachment.
3. Examine the attachment metadata. The attachment metadata can contain valuable information about the attachment, such as the file type, creation date, and sender. Use a forensic tool to examine the attachment metadata and extract any relevant information.
4. Compare the attachment to other evidence. Compare the attachment to other evidence in the case, such as other emails, documents, and computer files. This can help to identify the source of the attachment and its purpose.

66. Why are network router logs important during an e-mail investigaton?

Network router logs can provide valuable information about email traffic, such as the source and destination of email messages, the time and date of email messages, and the size of email messages. This information can help investigators to track down the sender of a malicious email or identify the source of a data breach.

67. Provide a brief description of Microsoft exchange server.

Microsoft Exchange Server is a mail server developed by Microsoft. It is used by businesses and organizations of all sizes to manage their email, calendars, and contacts. Exchange Server is a complex software product, but it can be configured to meet the specific needs of any organization.

Here are some of the key features of Microsoft Exchange Server:

- Email management:
- Calendaring
- Contacts management:
- Security features:

68. In which directory do UNIX installations typically store logs?
    a. /etc/var/log
    b. /log
    c. /var/log (ans)
    d. /etc/Log
69. In which discipline do professionals listen to voice recordings to determine who’s speacking or read e-mail and other writings knowns to be by a certain person and determine whether the person wrote the e-mail or letter in question?
    a. Forensic linguistics
    b. Linguistic analysis
    c. Communication forensics (ans)
    d. Communication linguistics
70. For digital investigatiors, tracking intranet e-mail is easier because accounts use standard names the administrator establishes.
    a. True (ans)
    b. False
71. Investigating crimes or policy violations involving e-mail is different than investigating other types of computer abuse and crimes.
    a. True (ans)
    b. False
72. Which files provide helpful information to an e-mail investigation?
    a. .rts and .txt files
    b. Log and configuration files
    c. Configuration and batch files
    d. Log files and scripts (ans)
73. E-mail programs either save e-mail messages on the client computer or leave them on the server.
    a. True (ans)
    b. False
74. Describe how e-mail account names are created on an intranet environment.

In most cases, an intranet e-mail system is specific to a company, used only by its employees, and regulated by its business practices, which usually include strict security and acceptable use policies.

To create an e-mail account on an intranet environment, the network or e-mail administrator typically uses a naming convention that is consistent with the company's existing naming conventions for other IT resources. For example, the naming convention might include the employee's first and last name, separated by a period or underscore.

75. What format is used for the flat plaintext files some e-mail systems use for message storage?
    a. Css
    b. Mbox (ans)
    c. SMTP
    d. POP3
76. Explain how to use supportive material on a report

Supportive material is evidence that supports the findings and conclusions of a report. It can include documents, images, screenshots, and other types of data.

To use supportive material in a report, you should first identify the key points that you need to support. Then, you should select supportive material that is relevant to each key point and that is clear and easy to understand.

When including supportive material in your report, you should cite it properly so that the reader can easily find the original source. You should also explain how the supportive material supports your key points.

77. Provide some guidelines for writing an introduction section for a report.

The introduction section of a report is important because it sets the stage for the rest of the report and tells the reader what to expect. The introduction should be clear, concise, and engaging. It should also include the following information:

- The purpose of the report
- The scope of the report

- The methodology used to compile the report
- The key findings of the report
- The conclusions and recommendations of the report

78. Anything an investigator writes down as part of examination for a report in a civil litigation case is subject to which action form the opposing attrorey?
    a. Discovery (ans)
    b. Publication
    c. Subpoena
    d. Deposition
79. What section of a report should contain broader generalizations?
    a. The discussion
    b. The appendixes
    c. The conclusion (ans)
    d. The introduction
80. Briefly explain how to limit your report to specifics

To limit your report to specifics, you should avoid including unnecessary information. This includes information that is not relevant to the purpose of the report, information that is already well-known to the reader, and information that is speculative or subjective.

You should also focus on writing in a concise and to-the-point manner. Avoid using jargon and technical terms that the reader may not understand. If you do need to use technical terms, be sure to define them clearly.

Finally, you should proofread your report carefully to ensure that there are no errors in grammar or spelling.

Set -2

1) The Fourth Amendment of the U.S. Constitution(and each state's constitution) protects everyone's right to be secure in their person, residence, and property from search and seirzure. **True**
2) What investigator characteristic, which includes ethics, morals and standards of behavior, determines the investigator's credibility?
    a. Line of authority
    b. **Professional conduct (Answer)**
    c. Fidelity of oath of office
    d. Investigatory acumen

3) By the 1970s, electronic crimes were increasing, especially in the financial sector. **True**

4) Which agency introduced training on software for forensics investigations by the early 1990s?
    a. CERT
    b. FLETC
    c. DDBIA
    d. **IACIS (Answer)**

5) What does the investigator in a criminal or public-sector case submit, at the request of the prosecuting attorney, if he or she enough information to support a search warrant?
    a. **An affidavit (Answer)**
    b. A blotter
    c. An exhibit report
    d. A litigation report

6) What is the third stage of criminal case, after the complaint and the investigation?
    a. Negotiation
    b. Allegation
    c. **Prosecution (Answer)**
    d. Resolution

7) Computer investigations and forensics fall into the same category: public investigations. **False**

8) What term refers to a person using a computer to perform routine tasks other than systems adminstrartion?
    a. Complainant
    b. Consumer
    c. **End user (Answer)**
    d. Customer

9) Briefly describe the main characteristics of public-sector investigations.

Public-sector digital forensics investigations are characterized by the following:

- Variety of cases: Public-sector investigators handle a wide range of cases, from cybercrime to fraud to national security matters.
- Complex evidence: Digital evidence is often complex and voluminous, and public-sector investigators must be able to collect, analyze, and present it in a clear and concise manner.
- High visibility: Public-sector investigations are often conducted in the public eye, and investigators must be able to withstand scrutiny from the media and the public.
- Strict procedures: Public-sector investigators must follow strict procedures to ensure the integrity of the evidence and the fairness of the investigation.

Here are some specific examples of public-sector digital forensics investigations:

- Investigating a cyberattack on a government agency
- Examining the digital evidence in a corruption case
- Tracing the online activity of a terrorist suspect
- Recovering data from a lost or stolen government device

10) In what process is the acquisition of newer and better resources for investigation justified?

   a. Conducting a risk evaluation
   b. Creating an upgrade policy
   c. Modifying the configuration plan
   d. **Building a business case (Answer)**

11) How frequently should floors and carpets in the computer forensic lab be cleaned to help minimize data that can cause static electricity?

   a. At least twice a week
   b. At least fout times a week
   c. **At least once a week (Answer)**
   d. At least three times a week

12) What are the duities of a lab manager

The duties of a digital forensics lab manager vary depending on the size and structure of the lab, but typically include:

- Managing staff: Hiring, training, and supervising digital forensics examiners.
- Overseeing casework: Prioritizing cases, assigning work to examiners, and reviewing their reports.
- Ensuring quality: Ensuring that all casework is conducted in accordance with best practices and that all evidence is properly handled and stored.
- Developing and maintaining lab procedures: Developing and maintaining policies and procedures for all aspects of the lab's operations, including casework, evidence management, and quality assurance.
- Managing budget and resources: Managing the lab's budget and resources, including equipment, software, and training.
- Representing the lab to external stakeholders: Representing the lab to external stakeholders, such as law enforcement agencies, courts, and the media.

13) What material is recommened for secure storage containers and cabinets?

   a. Gypsum
   b. Wood
   c. Expaned metal
   d. **Steel (Answer)**

14) What peripheral devices ahould be stocked in your computer forensics lab?

The following peripheral devices should be stocked in a computer forensics lab:

- Write blockers: Write blockers are devices that prevent data from being written to a storage device. This is important to prevent evidence from being modified or destroyed during the examination process.
- Forensic imaging devices: Forensic imaging devices are used to create bit-for-bit copies of storage devices. This ensures that the original evidence is preserved and that the examination process does not alter the data in any way.
- Forensic data analysis tools: Forensic data analysis tools are used to examine digital evidence for artifacts and other information that can be used to support an investigation.

15) A good working practice is to use less powerful workstations for mundane tasks and multipurpose workstations for the higher-end analysis tasks. **True**

16) By using marketing to attract new customers or clients , you can justify future budgets for the lab's operation and staff. **True**

17) At what distance can the EMR from a computer monitor be picked up?

   a. ½ mile (Answer)
   b. 1 mile
   c. ¾ mile
   d. ¼ mile

18) Briefly describe the process of obtaining a search warrant.

The process of obtaining a search warrant varies depending on the jurisdiction. However, the general process is as follows:

1. The investigator must submit a sworn affidavit to a judge or magistrate that describes the evidence being sought and the probable cause for believing that the evidence is located at the place to be searched.
2. The judge or magistrate will review the affidavit and determine whether there is probable cause to issue a search warrant.
3. If the judge or magistrate finds probable cause, they will issue a search warrant.
4. The investigator must then serve the search warrant on the person whose property is being searched.
5. The investigator can then search the property for the evidence described in the search warrant.

19) The reason for the standard practice of securing an incident or crime scene is to expand the area of control beyond the scene's immediate location. **True**

20) Give some guidelines on how to video record a computer incident or crime scene

The following are some guidelines on how to video record a computer incident or crime scene:

- Identify the purpose of the recording: What do you want to capture with the recording? Are you trying to document the scene, show the location of evidence, or demonstrate how to perform a certain task?
- Start recording as soon as possible: Don't wait until you've finished your work to start recording. This will help you capture any important information that you might otherwise miss.
- Speak clearly and slowly: It's important to speak clearly and slowly so that your recording is easy to understand.
- Pan the camera around the scene: This will give viewers a good sense of the layout of the scene and the location of evidence.
- Zoom in on important details: If you see something important, zoom in on it so that it's clear and visible in the recording.
- Label the recording: Once you're finished recording, label it with the date, time, and location of the recording.

21) The presence of police officers and other professionals who aren’t part of the crime scene-processiong team may result in the loss or corruption of data through which process?
   a. Deliberate destruction
   b. Data drift
   c. **Professional curiosity (Answer)**
   d. Police malfeasance

22) What is the plain view doctrine?

The plain view doctrine is a legal exception to the Fourth Amendment warrant requirement. It allows law enforcement officers to seize evidence that is in plain view without a warrant, as long as the officer is lawfully in the place where the evidence is discovered.

To satisfy the plain view doctrine, the following conditions must be met:

- The officer must be lawfully in the place where the evidence is discovered.
- The evidence must be in plain view.
- The officer must recognize the evidence as contraband or otherwise immediately apparent to the officer as criminal evidence.

The plain view doctrine is a powerful tool for law enforcement, but it is important to note that it has its limits. For example, the plain view doctrine cannot be used to justify a search that is otherwise unlawful.

23) When recovering evidence from a contaminated crime scene, the investigator should take measures to avoid damage to drive from overheating. At what temperature should the investigator take action?

  a. 95 degrees or higher
  b. 105 degrees or higher
  c. 90 degrees or higher
  d. **80 degrees or higher (Answer)**

24) How can you determine who is in charge of an investigation?

The person in charge of a digital forensics investigation is typically the lead investigator. This is the person who has the overall responsibility for the investigation, including planning, execution, and reporting. The lead investigator is usually a senior digital forensics examiner with extensive experience.

To determine who is in charge of an investigation, you can ask the following questions:

- Who is the lead investigator?
- Who is the primary contact for the investigation?
- Who has the authority to make decisions about the investigation?

If you are unsure who is in charge of an investigation, you should contact your supervisor or another senior member of your organization.

25) If a company does not publish a policy stating that it reserves the right to inspect computing assets at will or display a warning banner, employees have an expectation of privacy. **True**

26) Which is the most accurate statement about investigating and controlling computer incident scenes in private-sector environments as compared to crime scencs?

  a. Investigating and controlling the scene is equally difficult in both environments.
  b. Investigating and controlling the scene is more difficult in private sector environments
  c. Investigating and controlling the scene is equally easy in both environments.

    d. **Investigating and controlling the scene is much easier in private sector environments. (Answer)**

27) What do law enforcement investigators need in order to remove computers from a crime scene and transport them to a lab?
    a. A FOIA form
    b. **A warrant(Answer)**
    c. An evidence custody form
    d. An affidavit

28) Which acronym refers to the file structure database that Microsoft originally designed for floppy disks?
    a. **FAT (Answer)**
    b. VFAT
    c. NTFS
    d. FAT32

29) Which filename refers to the device driver that allows the OS to communicate with SCSI or ATA drives that aren’t related to the BIOS?
    a. Hal.dll
    b. Ntoskrnl.exe
    c. Boot.ini
    d. **NTBootdd.sys (Answer)**

30) Typically, a virtual machine consists of just one file. **False.**

31) How do most manufacturers deal with a platter’s inner tracks having a smaller circumference than its outer tracks?
    a. **ZBR (Answer)**
    b. Cylinder skew
    c. Areal density
    d. Head skew

32) How are disk clusters numbered by Microsoft file structures?

Microsoft file structures number disk clusters in a linear fashion, starting at the beginning of the disk and working their way to the end. This means that the first cluster in a file is always cluster 0, the second cluster is always cluster 1, and so on.

This numbering scheme is simple and straightforward, but it can be inefficient for storing large files. For example, if a large file is fragmented, its clusters will be scattered all over the disk. This can slow down performance when the file is being accessed.

To improve performance, Microsoft file structures use a technique called cluster allocation. This technique groups clusters together into larger units called allocations. Allocations are numbered sequentially, starting at the beginning of the disk.

33) Which filename refers to the Windows XP system service dispatch stubs to executables functions and internal support functions?
   a. Advapi32.dll
   b. **Ntdll.dll**
   c. Gdi32.dll
   d. User32.dll

34) What is on an NTFS disk immediately after the Partition Boot Sector?
   a. **MFT**
   b. MBR
   c. HPFS
   d. FAT

35) The file or folder’s MFT record provides cluster addresses where the file is stored on the drive’s partition. What are these cluster addresses called?
   a. Virtual runs
   b. Metadata
   c. **Data runs (Answer)**
   d. Metaruns

36) What enables the user to run another OS on an existing physical computer(known as the host computer) by emulating a computer’s hardware environment?
   a. **A virtual machine(Answer)**
   b. A logic machine
   c. A logic drive
   d. A virtual file

37) How can you make sure a subject’s computer boots to a forensic floopy disk or CD?

To make sure a subject's computer boots to a forensic floppy disk or CD, you can use the following steps:

1. Change the boot order in the computer's BIOS or UEFI settings to prioritize the floppy disk or CD drive.
2. Insert the forensic floppy disk or CD into the computer and boot the computer.
3. If the computer boots to the forensic floppy disk or CD, you can proceed with the digital forensics examination.
4. If the computer does not boot to the forensic floppy disk or CD, you may need to use a boot loader such as PXE or Ghost Boot Wizard.

38) Which filename refers to a 16-bit real-mode program that queries the system for device and configuration data, and then passes its findings to Ntldr?
   a. Hal.dll
   b. BootSect.dos
   c. Boot.ini

   d. **NTDetect.com (Answer)**

39) Describe some third-party disk encryption tools

- BitLocker
- VeraCrypt
- DiskCryptor
- TrueCrypt
- Cryptomator
- Boxcryptor
- Tresorit

40) Which type of logging allocates space for a the server, and then starts overwriting from the beginning when logging reaches the end of the time frame or the specified log size?

   a. Automatic logging
   b. Server logging
   c. Continuous logging
   d. **Circular logging (Answer)**

41) All e-mail servers use databases that store multiple users' e-mails. **False**

42) In Exchange, what type of file is inserted in the transaction log to mark the last point at which the database was written to disk in order to prevent loss of data?

   a. **Checkpoint (Answer)**
   b. Temporary
   c. Tracking
   d. Milestone

43) Describe how e-mail account names are created on an intranet environment

In an intranet environment, e-mail account names are typically created by the e-mail administrator. The administrator may use a variety of naming conventions, such as first initial and last name, full name, or employee ID number. The administrator may also add a domain name to the end of the account name, such as `jsmith@company.com`.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

120) When you're aware of a possible disqualification issue, bring it to the attention of the opposing attorney.
Ans) False

119) Why would the use of standard tools, such as those that are commercially created, be preferable over personally created tools?

here are several reasons why the use of standard digital forensics tools is preferable over personally created tools. First, standard tools have been thoroughly tested and validated by the community, which means that they are more reliable and accurate. Second, standard tools are more likely to be compatible with other tools and systems, which can make it easier to share data and collaborate with other investigators. Third, standard tools are more likely to be accepted by courts, which is important if the evidence is to be used in a legal proceeding.

118) What are some of factors courts have used in determining whether to disqualify an expert?

Courts have used a variety of factors in determining whether to disqualify an expert, including:

- Bias or prejudice: If the expert has a personal or financial interest in the outcome of the case, they may be disqualified.
- Lack of expertise: If the expert does not have the necessary education, training, and experience in their field, they may be disqualified.
- Failure to follow standard procedures: If the expert did not follow standard digital forensics procedures, their testimony may be inadmissible.
- Communication problems: If the expert is unable to clearly and concisely explain their findings to the jury, they may be disqualified.

117) which outcome , when caused by an ethical lapse , could effectively be a death sentence for a career as an expert witness ?
Or
A(n) __ based on an ethical lapse could effectively be a death sentence for a career as an expert witness.
ans) Disqualification

116) Describe some of the traps for unwary experts ?

There are a number of traps that unwary experts can fall into, including:

- Assuming that the evidence is what it appears to be. Experts should always carefully examine evidence to ensure that it has not been tampered with or modified.
- Reaching conclusions based on incomplete information. Experts should always gather as much information as possible before forming an opinion.
- Failing to consider all of the possible explanations for the evidence. Experts should be open to the possibility that there are multiple explanations for the

evidence, and they should consider all of the possibilities before forming an opinion.

- Failing to disclose their biases or limitations. Experts should be honest about their biases and limitations, and they should disclose these to the court or to the parties in the case.

115) The most important laws applying to attorneys and witness are the __.
Ans) Rules of Evidence

114) Briefly describe the issues related to the attorneys "opinion shopping"

Opinion shopping is the practice of attorneys seeking out experts who will give them the opinion that they want. This can be a problem because it can lead to experts who are biased or who are not qualified to give an opinion on the matter at hand.

One of the main issues with opinion shopping is that it can lead to experts giving false or misleading testimony. When experts are pressured to give a certain opinion, they may be more likely to stretch the facts or to ignore evidence that contradicts their opinion.

Another issue with opinion shopping is that it can undermine the public's trust in the legal system. When people see that attorneys are shopping for experts who will give them the opinion that they want, they may come to believe that the legal system is not fair.

113) No single source offers a definitive code of ethics for expert witnesses, so you must draw on standards from other organizations to form your own ethical standards T/F
Ans) True

112) which action isn't usually punitive, but can be embarrassing for the professional and potentially for the attorney who retained the professional.

1. Conflicting out
2. Admonition
3. Recertification
4. **Disqualification(Answer)**

111) What are the some of standards for IACIS members that apply to testifying?

he International Association for Computer Investigation Specialists (IACIS) has a number of standards that apply to its members when testifying in court. These standards include:

- Members must be truthful and objective in their testimony.
- Members must base their testimony on sound scientific principles and on their own personal knowledge and experience.
- Members must avoid expressing opinions that are beyond the scope of their expertise.
- Members must disclose any biases or limitations that they have.
- Members must be respectful of the court and of the other parties in the case.

IACIS members who violate these standards may be subject to disciplinary action, including expulsion from the organization.

110) As an expert witness, you can't testify if you weren't present when the event occurred.
Ans) False

109) Foresnsic examiners may serve as what types of witnesses?

1. Direct and professional
2. **Fact and expert (Answer)**
3. Expert and discovery
4. Expert and direct

108) Which Federal Rules of Evidence is used to determine whether the basis for testimony is adequate?

1. **703 (Answer)**
2. 702
3. 701
4. 700

Possible answer : 702

Rule 701. Opinion Testimony by Lay Witnesses

If a witness is not testifying as an expert, testimony in the form of an opinion is limited to one that is:

(a) rationally based on the witness’s perception;

(b) helpful to clearly understanding the witness’s testimony or to determining a fact in issue; and

(c) not based on scientific, technical, or other specialized knowledge within the scope of Rule 702.

Rule 703. Bases of an Expert

An expert may base an opinion on facts or data in the case that the expert has been made aware of or personally observed. If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.

Rule 702. Testimony by Expert Witnesses

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case.

26(a)(2): Disclosure of Expert Testimony (A) ...[A] party shall disclose to other parties the identity of any person who may be used at trial to present evidence under Rules 702, 703, or 705 of the Federal Rules of Evidence. (B) ... [T]his disclosure shall, with respect to a witness who is retained or specially employed to provide expert testimony in the case or whose duties as an employee of the party regularly involve giving expert testimony, be accompanied by a written report prepared and signed by the witness. The report shall contain a complete statement of all opinions to be expressed and the basis and reasons therefor; the data or other information considered by the witness in forming the opinions; any exhibits to be used as a summary of or support for the opinions; the qualifications of the witness, including a list of all publications authored by the witness within the preceding ten years; the compensation to be paid for the study and testimony; and a listing of any other cases in which the witness has testified as an expert at trial or by deposition within the preceding four years. I do not have to give opinion work product, just the other work product Based on this, Rule 701 allows you to hit the ground running

107) Which term refers to internalized rules used to measure ones own performance

1. Standards
2. Codes
3. Norms
4. **Ethics (Answer)**

106) Expert opinions cannot be presented without stating the underlying factual basis.
Ans) False
105) As an expert witness, you have opinions about what you have found or observed.
Ans) True

104) Validate your tools and verify your evidence with __ to ensure its integrity.
a. **hashing algorithms(Answer)**
b. watermarks
c. steganography
d. digital certificates

103) What should you do when you find exculpatory evidence

When you find exculpatory evidence, you should:

- Preserve the evidence. This means taking steps to ensure that the evidence is not altered or destroyed. This may involve creating a forensic copy of the evidence, storing it in a secure location, and maintaining a chain of custody.
- Disclose the evidence to the opposing party. This is required by law in most jurisdictions. You should disclose the evidence to the opposing party as soon as possible, so that they have an opportunity to review it and respond.
- Analyze the evidence. Once you have preserved and disclosed the evidence, you should carefully analyze it to determine its significance. You may need to consult with other experts to assist you with this analysis.
- Use the evidence to support your case. If the exculpatory evidence is significant, you may be able to use it to support your case in court. This may involve presenting the evidence to the jury or using it to negotiate a plea agreement with the prosecution.

102) How can you deal with rapid fire questions during a cross examination

To deal with rapid fire questions during a cross examination, you should:

- Listen carefully to each question. Make sure you understand the question before you answer it.

- Take your time. Don't feel pressured to answer a question immediately. If you need more time to think about your answer, you can ask the attorney to repeat the question or give you a moment to collect your thoughts.
- Be concise. Avoid giving long, rambling answers. Instead, focus on giving clear, direct answers to the questions.
- Be honest. Don't try to lie or evade the questions. It's better to admit that you don't know the answer to a question than to give a false answer.
- Object if necessary. If the attorney asks you an unfair or irrelevant question, you can object. The judge will then decide whether or not to allow the question.

101) whether you are serving as an expert witness or a fact witness , be professional and polite when presenting yourself to any attorney or the court
Ans) True

100) Generally, the best approach your attorney can take in direct examination is to ask you __ questions and let you give your testimony.
a. setup
b. **open-ended(Answer)**
c. compound
d. repid-fire

Ans) b

99) What are some of the questions you should consider when preparing your testimony

When preparing your testimony, you should consider the following questions:

- What is the purpose of your testimony? What are you trying to prove or disprove?
- What is your audience? Who will be listening to your testimony?
- What are the key points that you want to make?
- What evidence do you have to support your claims?
- How can you present your testimony in a clear, concise, and persuasive manner?

98) What term refers to rejecting potential jurors?

1. Venire
2. **Striking(Answer)**
3. Voir dire
4. Rebuttal

97) Explain the differences between discovery deposition and testimony preservation deposition.

A discovery deposition is a deposition that is taken for the purpose of gathering information and evidence from a witness. Discovery depositions are typically taken before trial, and they are used by attorneys to prepare their cases.

A testimony preservation deposition is a deposition that is taken for the purpose of preserving a witness's testimony in case the witness is unable to testify at trial. Testimony preservation depositions are typically taken after trial has begun, and they are used to ensure that the witness's testimony is available to the jury, even if the witness is unable to appear in person.

The main difference between discovery depositions and testimony preservation depositions is their purpose. Discovery depositions are used to gather information and evidence, while testimony preservation depositions are used to preserve a witness's testimony.

96) What should the forensics specialist keep updated and complete in order to support his role as an expert and document enhancement of skills through training , teaching and experience.

1. The deposition
2. **His or her CV (Answer)**
3. The examination plan
4. His or her testimony

95) Briefly describe judicial hearings

Judicial hearings are formal proceedings held in a court of law, presided over by a judge. They can be held for a variety of reasons, such as to determine whether there is enough evidence to proceed to trial, to settle pretrial disputes, or to hear evidence during a trial.

94) How close should be a microphone be to the person testifying

1. **6 to 8 inches(Answer)**
2. 3 to 4 inches
3. 5 to 6 inches
4. 4 to 5 inches

Answer : 6 to 8 inches

93) what is the most important part of an investigators testimony at a trial ?

1. Cross examination
2. Rebuttal
3. **Direct examination (Answer)**

4. Redirect Examination

91,92 : match the following

90: Anything as investigator writes aown as a part of examination for a report in a civil ligation case is subject to which action from opposing attorney

1. **Discovery (Answer)**
2. Deposition
3. Publication
4. Subpoena

89 : what is basic structure of a report

A digital forensics report should typically include the following sections:

- Introduction: The introduction should identify the case, the investigator, and the purpose of the report. It should also provide a brief overview of the findings.
- Examination and data collection methods: This section should describe the methods used to examine the digital evidence, including the tools and techniques used.
- Findings: This section should present the findings of the investigation in a clear and concise manner. It should include any relevant data or analysis.
- Conclusions and recommendations: This section should summarize the findings of the investigation and provide any recommendations for further action.

88: If you must write a preliminary report, use words such as "preliminary copy," "draft copy," or "working draft.
Ans False

87: in addition to decimal numbering , what numbering system can be used in a written report

1. ROMAN sequential
2. Letter- sequential
3. **Legal- sequential (Answer)**
4. Arabic- sequential

86. When writing a report , use a formal , technical style .
Ans False

85. What format is typically used to cite references in main body of a report ?

a) **the full name of the author and year of publication are included in paranthesis (Answer)**
b) the last name of author is included in paranthesis
C) the authors last name and year of publication are included in paranthesis.

d) the year of publication are included in paranthesis

84) How you should explain examination and data collective methods?

When explaining examination and data collection methods in a digital forensics report, it is important to be clear and concise. Avoid using technical jargon that the reader may not understand. Instead, focus on explaining the methods in a way that is easy to understand. You may also want to include diagrams or illustrations to help illustrate your points.

83) Because oppposijh counsel can demand discovery on them . What are written preliminary reports considered to be ?

1. Middle risk docs
2. Low risk docs
3. **High risk docs(Answer)**
4. No risk docs

Ans : probaby High risk(once check yourself)

82) provide some guidelines for writing an introduction section for a report .

Here are some guidelines for writing an introduction section for a digital forensics report:

- Identify the case, the investigator, and the purpose of the report.
- Provide a brief overview of the findings.
- State the thesis statement of the report. The thesis statement should summarize the main point of the report in a clear and concise manner.
- Hook the reader's attention. You may want to start the introduction with a strong statement or anecdote to grab the reader's attention.

81) Besides presenting facts, reports can communicate expert opinion
Ans : True

80) the decimal numbering system is frequently used when writing pleadings

Ans False

79) what is standard format in US federal courts for electronic submission of docs
Ans : probably PDF
a) Microsoft doc
b) Encapsulated postscript (EPS)
c) Post scripts (PS)
d) Portable document format (PDF) (Approx)

78) what are the report requirements for civil cased specified on Rule 26 , FRCP

77) How many words should an abstract contain

1. 250 to 300
2. 300 to 350
3. 200 to 250
4. **150 to 200(Abstract)**

76) Lawyers use services called deposition banks (libraries), which store examples of expert witnesses' previous testimony.
Ans : True

75) E-mail programs either save e-mail messages on the client computer or leave them on the server
Ans True
74) In an e-mail address, what symbol separates the domain name from the rest of the address?
Ans: @
73) E-mail crimes and violations rarely depend on the city, state, and country in which the e-mail originated.
Ans False

72) In Microsoft outlook which file extension is used with saved sent drafted deleted and received emails

1. **.pst(Answer)**
2. .ost
3. .msg
4. .eml

71) what are steps for copying an email msg in outlook or outlook express.

To copy an email message in Outlook or Outlook Express, follow these steps:

1. Open the email message that you want to copy.
2. Click the File menu and select Save As.
3. In the Save As dialog box, select the location where you want to save the copied email message.
4. In the File name field, type a new name for the copied email message.
5. Click the Save button.

The copied email message will be saved in the location that you selected. You can then open the copied email message in Outlook or Outlook Express and view it or edit it as needed.

70) what name is used for configuration typically used for email messages that are distributed from a central server to many connected client computers

1. **Client server architecture (Answer)**
2. Client architecture
3. Peer to peer architecture
4. Central distribution architecture