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.