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. Authroized requester
    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
3. What questions should an investigator ask to determine whether a computer crime was committed?
4. Which Pacific Northwest agency meets to discuss problems that digital forensics examiners encounter?
    a. IACIS
    b. CTIN
    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
6. To be a successful computer forensics investigator, you must be familiar with more than one computing platform.
    a. True
    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
    b. Assertion
    c. Declaration
    d. Contention
8. Briefly describe hostile work environment.
9. The law of search and seizure protects the rights of all people, excluding people suspected of crimes.
    a. False
    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

    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
12. Why is confidentiality critical in the private-sector environment?
13. Without a warning banner, what right might employees assume they have when using a company's computer systems and network accesses?
    a. Privacy
    b. Consent
    c. Authority
    d. Anonymity
14. What are some of the most common types of private-sector computer crime?
15. Briefly describe the main characteristics of private-sector investigations
16. What organization was created by police officers in order to formalize credentials for digital investigators?
    a. HTCN
    b. NISPOM
    c. TEMPEST
    d. IACIS
17. Chapter 5, Section 3, of the NISPOM describes the characteristics of a safe storage container.
    a. True
    b. False
18. Computing systems in a forensics lab should be able to process typical cases in a timely manner.
    a. True
    b. False
19. Methods for restoring large data sets are important for labs using which type of servers?
    a. TEMPEST
    b. WAN
    c. RAID
    d. ISDN
20. What are the four levels of certification offered by HTCN?
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
    c. Nispom
    d. Emr
22. What are the questions you need to ask when planning the justification step of a business case?
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

24. Which activity involves determining how much risk is acceptable for any process or operation?
    a. Risk analysis
    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
    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
    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
    d. Ext2
28. Requirements for taking the EnCE certification exam depend on taking the Guidance software EnCase training courses.
    a. True
    b. False
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
30. What kind of forensic investigation lab best preserves the integrity of evidence?
    a. A secure facility
    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
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
    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
34. Give some guidelines on how to video record a computer incident or crime scene.
35. Under what circumstances are digital records considered admissible?
    a. They are computer-generated records
    b. They are computer-stored records
    c. They are business records
    d. They are hearsay records
36. Briefly describe the process of obtaining a serach warrant.
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
38. Describe how to use a journal when processing a major incident or crime scene.
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
    c. Reasonable suspicion
    d. Burden of Proof
40. Illustrate with an example the problems caused by commingled data.
41. Corporate investigators always have the authority to seize all computer equipment during a corporate investigation
    a. True
    b. False
42. ISP's can investigate computer abuse commited by their customers.
    a. True
    b. False
43. Which technique can be used for extracting evidence form large systems?
    a. Raid imaging
    b. Sparse acquisition

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
    c. Invalid
    d. Logical
45. Describe the process of preparing an investigation team
46. When Microsoft created windows95, into what were initialization(.ini) files consolidated?
    a. The ini data
    b. The registry
    c. The metadata
    d. The inirecord
47. Drive slack includes RAM slack(found mainly in older Microsoft Oss) and file slack.
    a. True
    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
    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
    b. False
50. Briefly describe how to delete FAT files.
51. How can you make sure a subject's computer boots to a 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
53. One way to examine a partition's physical level is to use a disk editor, such as WinHex. Or Hex Workshop.
    a. True
    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
    d. Hal.dll
55. Summarize the evolution of FAT versions.

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
    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
    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
    b. BootSec.dos
    c. NTBootdd.sys
    d. NTDetect.com
61. What is forensic linguistics?
62. You can send and receive e-mail in tow enviroments: via the internet or an intranet(an internal network).
    a. True
    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
    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

65. Explain how to handle attachments during an e-mail investigation.
66. Why are network router logs important during an e-mail investigaton?
67. Provide a brief description of Microsoft exchange server.
68. In which directory do UNIX installations typically store logs?
    a. /etc/var/log
    b. /log
    c. /var/log
    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
    d. Communication linguistics
70. For digital investigatiors, tracking intranet e-mail is easier because accounts use standard names the administrator establishes.
    a. True
    b. False
71. Investigating crimes or policy violations involving e-mail is different than investigating other types of computer abuse and crimes.
    a. True
    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
73. E-mail programs either save e-mail messages on the client computer or leave them on the server.
    a. True
    b. False
74. Describe how e-mail account names are created on an intranet environment.
75. What format is used for the flat plaintext files some e-mail systems use for message storage?
    a. Css
    b. Mbox
    c. SMTP
    d. POP3
76. Explain how to use supportive material on a report
77. Provide some guidelines for writing an introduction section for a 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

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
    d. The introduction
80. Briefly explain how to limit your report to specifics

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. T or F
2) What investigator characteristic, which includes ethics, morals and standards of behavior, determines the investigator's credibility?
    a. Line of authority
    b. Professional conduct
    c. Fidelity of oath of office
    d. Investigatory acumen
3) By the 1970s, electronic crimes were increasing, especially in the financial sector. T or F
4) Which agency introduced training on software for forensics investigations by the early 1990s?
    a. CERT
    b. FLETC
    c. DDBIA
    d. IACIS
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
    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
    d. Resolution
7) Computer investigations and forensics fall into the same category: public investigations. T or F
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
d. Customer

9) Briefly describe the main characteristics of public-sector investigations.
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
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
    d. At least three times a week
12) What are the duities of a lab manager
13) What material is recommened for secure storage containers and cabinets?
    a. Gypsum
    b. Wood
    c. Expaned metal
    d. Steel
14) What peripheral devices ahould be stocked in your computer forensics lab?
15) A good working practice is to use less powerful workstations for mundane tasks and multipurpose workstations for the higher-end analysis tasks. T or F
16) By using marketing to attract new customers or clients , you can justify future budgets for the lab's operation and staff. T or F
17) At what distance can the EMR from a computer monitor be picked up?
    a. ½ mile
    b. 1 mile
    c. ¾ mile
    d. ¼ mile
18) Briefly describe the process of obtaining a 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. T or F
20) Give some guidelines on how to video record a computer incident or crime scene
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
    d. Police malfeasance
22) What is the plain view doctrine?
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

24) How can you determine who is in charge of an investigation?
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. T or F
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.
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
    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
    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
30) Typically, a virtual machine consists of just one file. T or F
31) How do most manufacturers deal with a platter's inner tracks having a smaller circumference than its outer tracks?
    a. ZBR
    b. Cylinder skew
    c. Areal density
    d. Head skew
32) How are disk clusters numbered by Microsoft file structures?
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
    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
    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?
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
39) Describe some third-party disk encryption tools
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
41) All e-mail servers use databases that store multiple users' e-mails. T or F
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
    b. Temporary
    c. Tracking
    d. Milestone
43) Describe how e-mail account names are created on an intranet environment

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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?

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

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 ?

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"

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.
Options
Conflicting out
Admonition
Recertification
Disqualification

Ans) Disqualification

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

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?
Options :
Direct and professional
Fact and expert
Expert and discovery
Expert and direct

108) Which Federal Rules of Evidence is used to determine whether the basis for testimony is adequate?
Options :
703
702
701
700
Possible answer : 702

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

Standards
Codes
Norms
Ethics
Answer : Ethics
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
b. watermarks
c. steganography
d. digital certificates

Ans) a

103) What should you do when you find exculpatory evidence

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

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
c. compound
d. repid-fire

Ans) b

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

98) What term refers to rejecting potential jurors?
Options :
Venire
Striking
Voir dire
Rebuttal
Ans) striking

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

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.
Options:
The deposition
His or her CV
The examination plan
His or her testimony

95) Briefly describe judicial hearings

94) How close should be a microphone be to the person testifying
Options:
6 to 8 inches
3 to 4 inches
5 to 6 inches
4 to 5 inches
Answer : 6 to 8 inches

93) what is the most important part of an investigators testimony at a trial ?
Options:
Cross examination
Rebuttal
Direct examination
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

Options:
Discovery
Deposition
Publication
Subpoena
Answer : Discovery
89 : what is basic structure of a report

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
Options:
ROMAN sequential
Letter- sequential
Legal- sequential
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
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?

83) Because opposijh counsel can demand discovery on them . What are written preliminary reports considered to be ?
Options
Middle risk docs
Low risk docs
High risk docs
No risk docs
Ans : probaby High risk(once check yourself)

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

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)

78) what are the report requirements for civil cased specified on Rule 26 , FRCP
77) How many words should an abstracy contain
Options :
250 to 300
300 to 350
200 to 250
150 to 200

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
Options
.pst
.ost
.msg
.eml

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

70) what name is used for configuration typically used for email messages that are distributed from a central server to many connected client computers
Options
Client server architecture
Client architecture
Peer to peer architecture
Central distribution architecture