Chapter 1,2,3,5

1. By the 1970s electronic crimes were increasing especially in the financial sector.

Ans. True  
2. To be a successful computer forensics investigator you must be familiar with more than one computing platform.

Ans. True  
3. Computer investigations and forensics fall into the same category: public investigations.

Ans. false  
4.The law of search and seizure protects the rights of all people excluding people suspected of crimes.

Ans. false  
5.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.

Ans. true  
6.Maintaining credibility means you must form and sustain unbiased opinions of your cases.

Ans. false  
7.The definition of digital forensics has evolved over the years from simply involving securing and analyzing digital information stored on a computer for use as evidence in civil criminal or administrative cases.

Ans. true  
8.The Fourth Amendment to the U.S. Constitution (and each state's constitution) protects everyone's rights to be secure in their person residence and property from search and seizure.

Ans. true  
9.When you work in the enterprise digital group you test and verify the integrity of standalone workstations and network servers.

Ans. false  
10.The police blotter provides a record of clues to crimes that have been committed previously.

Ans. true  
11.Which entity was formed by the FBI in 1984 to handle the increasing number of cases involving digital evidence?

Ans. Computer analysis and response team.  
12. A technician is trying to recover information on a computer that has been hidden or deleted on purpose in order to hide evidence of a crime. Which type of task is the technician performing?

Ans. Data recovery  
13.Which group often works as part of a team to secure an organization's computers and networks?

Ans. Forensics investigators  
14.Which group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime?

Ans. Digital investigators.  
15.Which agency introduced training on software for forensics investigations by the early 1990s?

Ans. IACIS   
16. Which Pacific Northwest agency meets to discuss problems that digital forensics examiners encounter?

Ans. CTIN  
17. Which type of case involves charges such as burglary murder or molestation?

Ans. criminal  
18. What is the third stage of a criminal case after the complaint and the investigation?

Ans. prosecution  
19. What does the investigator in a criminal or public-sector case submit at the request of the prosecuting attorney if he or she has enough information to support a search warrant?

Ans. An affidavit   
20. When an investigator seeks a search warrant which of the following must be included in an affidavit to support the allegation of a crime?

Ans. exhibits  
21. What must be done under oath to verify that the information in the affidavit is true?

Ans. It must be notarized  
22. What do published company policies provide for a business that enables them to conduct internal investigations?

Ans. Line of authority  
23. What usually appears when a computer starts or connects to the company intranet network or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will?

Ans. A warning banner  
24. What term refers to a person using a computer to perform routine tasks other than systems administration?

Ans. End user  
25. 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?

Ans. Allegation.  
26. Without a warning banner what right might employees assume they have when using a company's computer systems and network accesses?

Ans. Privacy   
27. What term refers to the individual who has the power to conduct digital forensic investigations?

Ans. Authorized requester  
28. What is most often the focus of digital investigations in the private sector?

Ans. Misue of digital assets  
29. Which doctrine found to be unconstitutional was used to allow a civilian or private-sector investigative agent to deliver evidence obtained in a manner that violated the Fourth Amendment to a law enforcement agency?

Ans. Silver-platter  
30. A forensics analysis of a 6 TB disk for example can take several days or weeks.

Ans. true  
31. Requirements for taking the EnCE certification exam depend on taking the Guidance Software EnCase training courses.

Ans. false  
32. If damage occurs to the floor walls ceilings or furniture on your computer forensics lab it does not need to be repaired immediately.

Ans. false  
33. A good working practice is to use less powerful workstations for mundane tasks and multipurpose workstations for the higher-end analysis tasks.

Ans. true  
34. Computing systems in a forensics lab should be able to process typical cases in a timely manner.

Ans. true  
35. By using marketing to attract new customers or clients you can justify future budgets for the lab's operation and staff.

Ans. true  
36. The ANSI-ASQ National Accreditation Board (ANAB) is a wholly owned subsidiary of the American Society of Crime Laboratory Directors (ASCLD).

Ans. false  
37. The lab manager sets up processes for managing cases and reviews them regularly.

Ans. true   
38. 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.

Ans. false  
39. Chapter 5 Section 3 of the NISPOM describes the characteristics of a safe storage container.

Ans. true  
40. At what location does the forensics investigator conduct investigations store evidence and do most of his or her work?

Ans. the digital forensics lab  
41. At what levels should lab costs be broken down?

Ans. monthly,quarterly, and annually  
42. What reports are generated at the local state and federal levels to show the types and frequency of crimes committed?

Ans. uniform crime reports  
43. In addition to FAT16 FAT32 and Resilient File System which file system can Windows hard disks also use?

Ans. NTFS  
44. What organization was created by police officers in order to formalize credentials for digital investigators?

Ans. IACIS   
45. How frequently does IACIS require recertification to demonstrate continuing work in the field of computer forensics?

Ans. every 3 years  
46. What HTCN certification level requires candidates have three years of experience in computing investigations for law enforcement or corporate cases?

Ans. certified computer forensic technician, basic  
47. What kind of forensic investigation lab best preserves the integrity of evidence?

Ans. a secure facility   
48. At what distance can the EMR from a computer monitor be picked up?

Ans. ½ mile  
49. During the Cold War defense contractors were required to shield sensitive computing systems and prevent electronic eavesdropping of any computer emissions. What did the U.S. Department of Defense call this special computer-emission shielding?

Ans. TEMPEST  
50. What material is recommended for secure storage containers and cabinets?

Ans. steel   
51. How frequently should floors and carpets in the computer forensic lab be cleaned to help minimize dust that can cause static electricity?

Ans. at least once a week   
52. Which resource can be helpful when investigating older and unusual computing systems?

Ans. forums and blogs  
53. What type of plan specifies how to rebuild a forensic workstation after it has been severely contaminated by a virus from a drive you're analyzing?

Ans. disaster recovery   
54. Where should your computer backups be kept?

Ans. an off-site facility  
55. What process refers to recording all the updates made to a workstation?

Ans. configuration management  
56. Methods for restoring large data sets are important for labs using which type of servers?

Ans. RAID   
57. Which activity involves determining how much risk is acceptable for any process or operation?

Ans. risk management   
58. What is the maximum amount of time computing components are designed to last in normal business operations?

Ans. 36 months  
59. In what process is the acquisition of newer and better resources for investigation justified?

Ans. building a business case  
60. If the computer has an encrypted drive a live acquisition is done if the password or passphrase is not available.

Ans. false  
61. The most common and time-consuming technique for preserving evidence is creating a duplicate copy of your disk-to-image file.

Ans. true  
62. Some acquisition tools don't copy data in the host protected area (HPA) of a disk drive.

Ans. true   
63. FTK Imager requires that you use a device such as a USB dongle for licensing.

Ans. true  
64. Unlike RAID 0 RAID 3 stripes tracks across all disks that make up one volume.

Ans. true  
65. In Autopsy and many other forensics tools raw format image files don't contain metadata.

Ans. true  
66. Similar to Linux Windows also has built-in hashing algorithm tools for digital forensics.

Ans. false  
67. A separate manual validation is recommended for all raw acquisitions at the time of analysis.

Ans. true  
68. Acquisitions of RAID drives can be challenging and frustrating for digital forensics examiners because of how RAID systems are designed configured and sized.

Ans. true.  
69. There's no simple method for getting an image of a RAID server's disks.

Ans. true   
70. Which type of format acquisition leaves the investigator unable to share an image between different vendors' computer forensics analysis tools?

Ans. proprietary  
71. What type of acquisition is typically done on a computer seized during a police raid?

Ans. static   
72. What type of acquisition is done if the computer has an encrypted drive and the password or passphrase is available?

Ans. live  
73. What is the most common and flexible data-acquisition method?

Ans. disk-to-image file copy  
74. If your time is limited what type of acquisition data copy method should you consider?

Ans. sparse  
75. By what percentage can lossless compression reduce image file size?

Ans. 50 ./.  
76. What did Microsoft add to its newer operating systems that makes performing static acquisitions more difficult?

Ans. whole disk encryption

77. What term refers to Linux ISO images that can be burned to a CD or DVD?

Ans. linux live CDs

78. What command displays pages from the online help manual for information on Linux commands and their options?

Ans. man  
79. What command creates a raw format file that most computer forensics analysis tools can read?

And. dd  
80. What command works similarly to the dd command but has many features designed for computer forensics acquisitions?

Ans. dcfldd  
81. In addition to md5sum which hashing algorithm utility is included with current distributions of Linux?

Ans. shalsum   
82. What option is used with the dcfldd command to designate a hashing algorithm of md5 sha1 sha256 sha384 or sha512?

Ans. hash  
83. What does Autopsy use to validate an image?

Ans. MD5

84. What older Microsoft disk compression tool eliminates only slack disk space between files?

Ans. drivespace  
85. In addition to RAID 0 what type of RAID configuration is available for Windows XP    2000 and NT servers and workstations?

Ans. RAID 1  
86. In which RAID configuration do two or more disk drives become one large volume so the computer views the disks as a single disk?

Ans. RAID 0   
87. Which RAID configuration also called mirrored striping is a combination of RAID 1 and RAID 0?

Ans. RAID 10  
88. Which RAID configuration offers the greatest access speed and most robust data recovery capability?

Ans. RAID 15  
89. What type of acquisition is used for most remote acquisitions?

Ans. live  
90. ISPs can investigate computer abuse committed by their customers.

Ans. false  
91. If you follow police instructions to gather additional evidence without a search warrant after you have reported the crime you run the risk of becoming an agent of law enforcement.

Ans. true.  
92. A judge can exclude evidence obtained from a poorly worded warrant.

Ans. true.  
93. 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.

Ans. true  
94. Corporate investigators always have the authority to seize all computer equipment during a corporate investigation.

Ans. false   
95. The most common computer-related crime is check fraud.

Ans. true   
96. Private-sector organizations include small to medium businesses large corporations and non-government organizations (NGOs) which always get funding from the government or other agencies.

Ans. false  
97. Some cases involve dangerous settings. For these types of investigations you must rely on the skills of hazardous materials (HAZMAT) teams to recover evidence from the scene.

Ans . true   
98. 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.

Ans. true   
99. When an investigator finds a mix of information judges often issue a limiting phrase to the warrant which allows the police to present all evidence together.

Ans. false   
100. When federal courts are evaluating digital evidence from computer-generated records what exception is applied to hearsay?

Ans. business-records exception  
101. Under what circumstances are digital records considered admissible?

Ans. they are business records   
102. What type of records are considered data that the system maintains such as system log files and proxy server logs?

Ans. computer-generated   
103. When was the Freedom of Information Act originally enacted?

Ans. 1960s   
104. Which is the most accurate statement about investigating and controlling computer incident scenes in private-sector environments as compared to crime scenes?

Ans. investigating and controlling the scene is much easier in private sector environments.   
105. At a minimum what do most company policies require that employers have in order to initiate an investigation?

Ans. Reasonable suspicion that a law or policy is being violated.  
106.When confidential business data are included with the criminal evidence what are they referred to as?

Ans. Commingled data  
107. 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?

Ans. Probable cause  
108. What do law enforcement investigators need in order to remove computers from a crime scene and transport them to a lab?

Ans. A warrant  
109. In addition to environmental issues what issues are the investigator's primary concerns when working at the scene to gather information about an incident or a crime?

Ans. Safety  
110When recovering evidence from a contaminated crime scene the investigator should take measures to avoid damage to the drive from overheating. At what temperature should the investigator take action?

Ans. 80 degrees or higher  
111What will allow the investigator to arrive at a scene acquire the needed data and return to the lab as quickly as possible?

Ans. An initial-response field kit  
112 Which type of kit should include all the tools the investigator can afford to take to the field?

Ans. An extensive-response field kit  
113.What type of evidence do courts consider evidence data in a computer to be?

Ans. Physical  
114.The presence of police officers and other professionals who aren't part of the crime scene-processing team may result in the loss or corruption of data through which process?

Ans. Professional curiosity  
115 .When seizing computer evidence in criminal investigations which organization's standards should be followed?

Ans. U.S. DOJ  
116. Power should not be cut during an investigation involving a live computer unless it is what type of system?

Ans. An older Windows or MS-DOS system  
117. What type of files might lose essential network activity records if power is terminated without a proper shutdown?

Ans. Event logs  
118. Which technique can be used for extracting evidence from large systems?

Ans. Sparse acquisition  
119. What is required for real-time surveillance of a suspect's computer activity?

Ans. Sniffing data transmissions between a suspect's computer and a network server.  
120. The type of file system an OS uses determines how data is stored on the disk.

Ans. true   
121. One way to examine a partition's physical level is to use a disk editor such as WinHex or Hex Workshop.

Ans. true   
122. As data is added the MFT can expand to take up 75% of the NTFS disk.

Ans. false

123. The first 5 bytes (characters) for all MFT records are FILE.

Ans. false.   
124. Alternate data streams can obscure valuable evidentiary data intentionally or by coincidence.

Ans. true

125. Typically a virtual machine consists of just one file.

Ans. false   
126. From a network forensics standpoint there are no potential issues related to using virtual machines.

Ans. false  
127. In Microsoft file structures sectors are grouped to form clusters which are storage allocation units of one or more sectors.

Ans. true   
128. Drive slack includes RAM slack (found mainly in older Microsoft OSs) and file slack.

Ans. true   
129. It's possible to create a partition add data to it and then remove references to the partition so that it can be hidden in Windows.

Ans. true   
130. What term refers to a column of tracks on two or more disk platters?

Ans. cyclinder   
131. How do most manufacturers deal with a platter's inner tracks having a smaller circumference than its outer tracks?

Ans. ZBR   
132 What term refers to the number of bits in one square inch of a disk platter?

Ans. Areal density  
133. Which acronym refers to the file structure database that Microsoft originally designed for floppy disks?

Ans. FAT  
134. Which acronym refers to the file system that was introduced when Microsoft created Windows NT and that remains the main file system in Windows 10?

Ans. NTFS  
135. What is on an NTFS disk immediately after the Partition Boot Sector?

Ans MFT  
136. What are records in the MFT called?

Ans. Inodedata

137. In the NTFS MFT all files and folders are stored in separate records of how many bytes each?

Ans. 1024  
138. 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?

Ans. Data runs  
139. What is the name of the optional built-in encryption that Microsoft added to NTFS when Windows 2000 was introduced?

Ans. EFS   
140. Which certificate provides a mechanism for recovering files encrypted with EFS if there is a problem with the user's original private key?

Ans. Recovery certificate

141.When Microsoft created Windows 95 into what were initialization (.ini) files consolidated?

Ans. The registry  
142. What specifies the Windows XP path installation and contains options for selecting the Windows version?

Ans. Boot.ini  
143. 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?

Ans. NTDetect.com  
144. 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?

Ans. NTBootdd.sys  
145. What contains instructions for the OS for hardware devices such as the keyboard mouse and video card?

Ans. Device drivers  
146. Which filename refers to a core Win32 subsystem DLL file?

Ans. User32.sys  
147. Which filename refers to the physical address support program for accessing more than 4 GB of physical RAM?

Ans. Ntkrnlpa.exe  
148. Which filename refers to the Windows XP system service dispatch stubs to executables functions and internal support functions?

Ans. Ntdll.dll  
149. 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?

Ans. A virtual machine  
150. When you research for computer forensics tools strive for versatile flexible and robust tools that provide technical support.

Ans. true   
151. In software acquisition there are three types of data-copying methods.

Ans. false   
152. To help determine which computer forensics tool to purchase a comparison table of functions subfunctions and vendor products is useful.

Ans. true.  
153. Computers used several OSs before Windows and MS-DOS dominated the market.

Ans. true   
154. After retrieving and examining evidence data with one tool you should verify your results by performing the same tasks with other similar forensics tools.

Ans. true   
155. Software forensic tools are grouped into command-line applications and GUI applications.

Ans. true   
156. The validation function is the most challenging of all tasks for computer investigators to master.

Ans. false   
157. Although a disk editor gives you the most flexibility in testing it might not be capable of examining a compressed file's contents.

Ans. true   
158. Because there are a number of different versions of UNIX and Linux these OSs are referred to as CLI platforms.

Ans. false   
159. Hardware manufacturers have designed most computer components to last about 36 months between failures.

Ans. false   
160. Which digital forensics tool is categorized as a single-purpose hardware component?

Ans. Tableau T35es-R2 SATA/IDE eSATA bridge  
161. Where do software forensics tools copy data from a suspect's disk drive?

Ans. An image file  
162. Which tool enables the investigator to acquire the forensic image and process it in the same step?

Ans. Magnet AXIOM  
163. What Linux command is used to create the raw data format?

Ans. dd  
164. Which activity involves sorting and searching through investigation findings to separate good data and suspicious data?

Ans. Filtering  
165. Many password recovery tools have a feature for generating potential password lists for which type of attack?

Ans. Password dictionary  
166. Which type of copy from the suspect disk to the target location does the simplest method of duplicating a disk drive make?

Ans. Disk-to-image  
167. What must be created to complete a forensic disk analysis and examination?

Ans. A report  
168. The first MS-DOS tools that analyzed and extracted data from floppy disks and hard disks were used with which type of PC file systems?

Ans. IBM  
169. In Windows 2000 and later which command shows you the file owner if you have multiple users on the system or network?

Ans. dir  
170. Building your own forensics workstation:

Ans. requires the time and skills necessary to support the chosen hardware.  
171. What do you call a forensics workstation consisting of a laptop computer with almost as many bays and peripherals as a stationary workstation?

Ans. A portable workstation  
172. What type of disk is commonly used with Sun Solaris systems?

Ans. SPARC  
173. What is the general term for software or hardware that is used to protect evidence disks by preventing data from being written to them?

Ans. Write-blockers  
174. Devices used to prevent data from being written to a disk can connect to a computer through FireWire SATA PATA and SCSI controllers as well as which other type of controller?

Ans. USB 2.0 and 3.0  
175. Which entity publishes articles provides tools and creates procedures for testing and validating computer forensics software?

Ans. NIST  
176. Which standards document demands accuracy for all aspects of the testing process?

Ans. ISO 5725  
177. Which NIST project manages research on forensics tools?

Ans. CFTT  
178. What is the primary hash algorithm used by the NIST project created to collect all known hash values for commercial software and OS files?

Ans. SHA-1  
179. Which type of tool can be used to compare results and verify a new tool by viewing data in its raw format?

Ans. A disk editor  
180. If a file contains information it always occupies at least one allocation block.

Ans. true   
181. macOS is built with the new Apple File System (APFS). The current version offers better security encryption and performance speeds but users can't mount HFS+ drives.

Ans. false   
182. Some notable UNIX distributions included Silicon Graphics Inc. (SGI) IRIX Santa Cruz Operation (SCO) UnixWare Sun Solaris IBM AIX and HP-UX.

Ans. true   
183. Does Windows have a kernel?

Ans. false   
184. The pipe (|) character redirects the output of the command preceding it.

Ans. true   
185. All disks have more storage capacity than the manufacturer states.

Ans. true   
186. Before OS X the Hierarchical File System (HFS) was used in which files are stored in directories (folders) that can be nested in other directories.

Ans. true   
187. The HFS and HFS+ file systems have four descriptors for the end of a file (EOF).

Ans. false   
188. Ext3 is a journaling version of Ext2 that has a built-in file recovery mechanism used after a crash.

Ans. true   
189. In macOS volume fragmentation is kept to a minimum by removing clumps from larger files.

Ans. false   
190. with ­­­OS X Macintosh moved to the Intel processor and became UNIX based with which operating system?   
191. In older versions of macOS in which fork are file metadata and application information stored?

Ans. resource   
192. In macOS in addition to allocation blocks what kind of blocks do volumes have?

Ans. logical   
193. In older versions of macOS where is all information about the volume stored?

Ans. Master Directory Block (MDB).  
194. What macOS system application tracks each block on a volume to determine which blocks are in use and which ones are available to receive data?

Ans. Volume Bitmap  
195. In macOS what stores any file information not in the Master Directory Block or Volume Control Block?

Ans. extents overflow file  
196. Which term is often used when discussing Linux because technically Linux is only the core of the OS?

Ans. kernel   
197. What was the early standard Linux file system?

Ans. Ext2  
198. What is the largest disk partition Ext4f can support?

Ans. 16 TB  
199. What contains file and directory metadata and provides a mechanism for linking data stored in data blocks?

Ans . inodes   
200. At what hard link count is a file effectively deleted?

Ans. 0   
201. How many components define the file system on UNIX/Linux?

Ans. four   
202. Where are directories and files stored on a disk drive?

Ans. data block   
203. In Linux in which directory are most system configuration files stored?

Ans. /etc   
204. In Linux in which directory are most applications and commands stored?

Ans. /usr   
205. On a Linux computer by what are file systems exported to remote hosts represented?

Ans. /etc/exports  
206. On a Linux computer what contains group memberships for the local system?

Ans. /etc/group  
207. In a file's inode what are the first 10 pointers called?

Ans. indirect   
208. In macOS which fork typically contains data the user creates?

Ans. data   
209. In macOS when working with an application file which fork contains additional information such as menus dialog boxes icons executable code and controls?

Ans. resource   
210. Bitmap images are collections of dots or pixels in a grid format that form a graphic.

Ans. true   
211. Operating systems do not have tools for recovering image files.

Ans. false   
212. If a graphics file is fragmented across areas on a disk you must recover all the fragments before re-creating the file.

Ans. true   
213. With many computer forensics tools you can open files with external viewers.

Ans. true   
214. Steganography cannot be used with file formats other than image files.

Ans. false   
215. Under copyright laws maps and architectural plans may be registered as pictorial graphic and sculptural works.

Ans. true   
216. A graphics program creates and saves one of three types of image files: bitmap vector or XIF.

Ans. false   
217. The Internet is the best source for learning more about file formats and their extensions.

Ans. true   
218. All TIF files start at position zero (offset 0 is the first byte of a file) with hexadecimal 49 49 3B.

Ans. false   
219. The two major forms of steganography are insertion and substitution.  
220. What kinds of images are based on mathematical instructions that define lines curves text ovals and other geometric shapes?

Ans. vector graphics   
221. What tools are used to create modify and save bitmap vector and metafile graphics?

Ans. graphic editors   
222. Which images store graphics information as grids of pixels?

Ans. bitmap   
223. What is the process of converting raw picture data to another format called?

Ans. demosaicing   
224. In which format are most digital photographs stored?

Ans.. EXIF   
225. Which type of compression compresses data permanently by discarding bits of information in the file?

Ans. lossy   
226. What term refers to recovering fragments of a file?

Ans. carving   
227. Which JFIF format has a hexadecimal value of FFD8 FFE0 in the first four bytes?

Ans. JPEG   
228. If a graphics file cannot be opened in an image viewer what should the next step be?

ANS. HEADER DATA   
229. Which uppercase letter has a hexadecimal value 41?

ANS. “A”  
230. From which file format is the image format XIF derived?

ANS. TIF   
231. What is the simplest way to access a file header?

ANS. HEXADECIMAL   
232. Which header starts with hexadecimal 49 49 2A and has an offset of four bytes of 5C 01 00 00 20 65 58 74 65 6E 64 65 64 20 03?

ANS. XIF   
233. Which term refers to a data-hiding technique that uses host files to cover the contents of a secret message?

ANS. steganography   
234. Which data-hiding technique places data from the secret file into the host file without displaying the secret data when the host file is viewed in its associated program?

Ans. insertion   
235. Which data-hiding technique replaces bits of the host file with other bits of data?

pixelation

Substitution

Replacement

Insertion

Ans. substitution

236. What is another term for steganalysis tools?

Ans. steg tools   
237. What technique has been used to protect copyrighted material by inserting digital watermarks into a file?

Compression  
Steganography  
Encryption  
Archiving

Ans. steganography   
238. What type of laws should computer investigators be especially aware of when working with image files in order to avoid infringement violations?

Ans. copyrights.   
239. .How may computer programs be registered under copyright laws?

As literary works  
As motion pictures  
As architectural works  
As audiovisual works

Ans. As literary works

240. The defense request for full discovery of digital evidence applies only to criminal cases in the United States.

Ans. true.   
241. For target drives use only recently wiped media that have been reformatted and inspected for computer viruses.

Ans. true.  
242. Autopsy for Windows cannot perform forensics analysis on FAT file systems.

Ans. false   
243. Autopsy for Windows cannot analyze data from image files from other vendors.

Ans. false  
244. When two files look the same when viewed but one has an invisible digital watermark they appear to be the same file except for their sizes.

Ans. false  
245. Several password-cracking tools are available for handling password-protected data or systems.

Ans true  
246. MOST ORGANIZATIONS KEEP E-MAIL FOR LONGER THAN 90 DAYS.

Ans. false.  
247. Some encryption schemes are so complex that the time to crack them can be measured in days weeks years and even decades.

Ans true   
248. Private-sector cases such as employee abuse investigations might not specify limitations in recovering data.

Ans. true.   
249. For static acquisitions remove the original drive from the computer if practical and then check the date and time values in the system's CMOS.

Ans. true.   
250. What does scope creep typically do?

Ans. Increases the time and resources needed to extract, analyze, and present data  
251. What should be created in order to begin a digital forensics case?

Ans. an investigation plat  
252. In addition to search warrants what defines the scope of civil and criminal cases?

Ans. subpoenas  
253. Which program has an indexed version of the NIST NSRL of MD5 hashes that can be imported to enhance searching for and eliminating known OS and application files?

Ans. autopsy  
254. Because digital forensics tools have limitations in performing hashing what tools should be used to ensure data integrity?

a.

High-level language assemblers

b.

HTML editors

c.

Hexadecimal editors

d.

Steganalysis tools

Ans. hexadecimal editors  
255. Which AccessData feature compares known file hash values to files on your evidence drive or image files to see whether they contain suspicious data?

Ans. KFF  
256. Which activity involves changing or manipulating a file to conceal information?

Ans. data hiding   
257. Which Windows disk partition utility can be used to hide partitions?

Ans. diskpart  
258. The data-hiding technique involving marking bad clusters is more commonly used with what type of file system?

Ans. FAT   
259. Which term comes from the Greek word for "hidden writing" ?

Ans. steganography  
260. When both the original file with no hidden message and the converted file with the hidden message are available what analysis method is recommended by Johnson and Jajodia?

Ans. known cover attack   
261. What technology is designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure?

Ans. key-escrow  
262. Which program incorporates an advanced encryption technique that can be used to hide data?

Ans. bestcrypt  
263. Which type of recovery is becoming more common in digital forensic analysis?

Ans. password  
264. What type of attacks use every possible letter number and character found on a keyboard when cracking a password?

Ans. brute-force  
265. Many password-protected OSs and applications store passwords in the form of which type of hash values?

AES  
SSH  
SSL  
MD5

Ans. MD5  
266. Which action alters hash values making cracking passwords more difficult?

Ans. salting passwords  
267. What limits the data that can be sought in a criminal investigation?

Ans. the search warrant  
268. Which data-hiding technique changes data from readable code to data that looks like binary executable code?

Ans. bit shifting  
269. Which hashing algorithm is provided by WinHex?

Ans. SHA-1  
270. When intruders break into a network they rarely leave a trail behind.

Ans. false  
271. Network forensics is a fast easy process.

Ans. false  
272. Virtual machines are now common for both personal and business use.

Ans. true  
273. Virtual machines (VMs) help offset hardware costs for companies.

Ans. true  
274. Type 2 hypervisors cannot be used on laptops.

Ans. false   
275. Type 1 hypervisors are usually the ones you find loaded on a suspect machine.

Ans. false  
276. Before attempting to install a type 2 hypervisor you need to enable virtualization in the BIOS before attempting to create a VM.

Ans. true  
277. In network forensics you have to restore the drive to see how malware that attackers have installed on the system works.

Ans. true  
278. A honeywall is a computer set up to look like any other machine on your network but it lures the attacker to it.

Ans. false  
279. Network logs record traffic in and out of a network.

Ans. true  
280.Which type of forensics can help you determine whether a system is truly under attack or a user has inadvertently installed an untested patch or custom program?

Ans. network forensics  
281. Which type of strategy hides the most valuable data at the innermost part of the network?

Ans. layered network defense strategies  
282. What type of software runs virtual machines?

Ans. hypervisor  
283. Which type of virtual machine software is typically but not exclusively loaded on servers or workstations with a lot of RAM and storage?

Ans. type 1 hyepervison  
284. Which product responded to the need for security and performance by producing different CPU designs?

Ans. virtualization technology  
285. Which program can be used to examine network traffic?

Ans. tcpdump  
286. Which tool lists all open network sockets including those hidden by rootkits?

Ans. mandian memoryze  
287. What determines how long a piece of information lasts on a system?

Ans. order of volatility(oov)  
288. Which network defense strategy developed by the National Security Agency (NSA) has three modes of protection?

Ans. defense in depth  
289. Which tool allows network traffic to be viewed graphically?

Ans. etherape

289. Which network protocol analyzer can be programmed to examine TCP headers to find the SYN flag?

Ans. tethereal  
290. Which tool is useful for extracting information from large Libpcap files?

Ans. tcpslice  
What are packet analyzers?  
On which OSI model layers do most packet analyzers operate?  
Which format can be read by most packet analyzer tools?  
In which type of attack does the attacker keep asking the server to establish a connection?  
Which tool was designed as an easy-to-use interface for inspecting and analyzing large tcpdump files?  
Which tool probes collects and analyzes session data?  
Which project was developed to make information widely available in an attempt to thwart Internet and network hackers?  
What term is used for the machines used in a DDoS attack?  
For digital investigators tracking intranet e-mail is easier because accounts use standard names the administrator establishes.  
Investigating crimes or policy violations involving e-mail is different than investigating other types of computer abuse and crimes.  
E-mail programs either save e-mail messages on the client computer or leave them on the server.  
All e-mail servers use databases that store multiple users' e-mails.  
Like UNIX e-mail servers Exchange maintains logs to track e-mail communication.  
Forensic linguistics encompasses civil cases criminal cases cyberterrorism cases and other legal proceedings.  
E-mail crimes and violations rarely depend on the city state and country in which the e-mail originated.  
Evidence artifacts vary depending on the social media channel and the device.  
A challenge with using social media data in court is authenticating the author and the information.  
You can send and receive e-mail in two environments: via the Internet or an intranet (an internal network).  
What name is used for the configuration typically used for e-mail messages that are distributed from a central server to many connected client computers?  
In an e-mail address what symbol separates the domain name from the rest of the address?  
In what type of e-mail programs can the user copy an e-mail message by dragging the message to a storage medium such as a folder or drive?  
What is the main information being sought when examining e-mail headers?  
To retrieve e-mail headers in Microsoft Outlook what option should be clicked after the e-mail has been selected?  
In Web-based e-mail how are messages displayed and saved?  
In which discipline do professionals listen to voice recordings to determine who's speaking or read e-mail and other writings known to be by a certain person and determine whether that person wrote the e-mail or letter in question?  
To view Gmail Web e-mail headers what should be clicked after the e-mail has been opened and the down arrow next to the Reply circular arrow has been clicked?  
To view e-mail headers on Yahoo! what should be clicked on after "More" has been selected?  
In Microsoft Outlook what file extension is used with saved sent drafted deleted and received e-mails?  
Which site can be used to verify the names of domains a message is flowing through?  
Which type of logging allocates space for a log file on the server and then starts overwriting from the beginning when logging reaches the end of the time frame or the specified log size?  
Which files provide helpful information to an e-mail investigation?  
Which location contains configuration information for Sendmail?  
In which directory do UNIX installations typically store logs?  
In which log does Exchange log information about changes to its data?  
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?  
In Microsoft Exchange which file is responsible for messages formatted with MAPI?  
Which information from Facebook simply tells you the last time a person logged on the person's e-mail address and mobile number and whether the account can be viewed publicly?  
What format is used for the flat plaintext files some e-mail systems use for message storage?  
Many people store more information on smartphones and tablets than on computers.  
Investigating smartphones and other mobile devices is a relatively easy task in digital forensics.  
TDMA can operate in the cell phone (800 to 1000 MHz) or PCS (1900 MHz) frequency.  
Most basic phones use the same OSs as PCs.  
Portability of information is what makes SIM cards so versatile.  
In 2010 both VMware and BlackBerry were thinking of developing type 2 hypervisors for mobile devices.  
Because bring your own device (BYOD) has become a business standard investigators must consider how to keep employees' personal data separate from case evidence.  
The IoA will eventually include 4G smart devices and 4G mobile networks.  
Gaming consoles such as the Sony PlayStation and Xbox are safe because they don't contain information hackers might try to intercept and collect.  
Research on wearable computers has been conducted at MIT labs for more than a decade and these computers are now moving into working reality.  
What technology developed during WWII uses the full radio spectrum to define channels and is now used in the U.S. by Sprint U.S. Cellular and Verizon?  
Which type of digital network divides a radio frequency into time slots?  
Which type of network is a digital version of the original analog standard for cell phones?  
Which type of digital network is a faster version of GSM designed to deliver data?  
Which standard introduced sleep mode to enhance battery life?  
Where do phones typically store system data?  
What type of cards consisting of a microprocessor and internal memory are usually found in GSM devices?  
Which devices have been replaced by iPods iPads and other mobile devices for personal use?  
What structure is used for the file system for a SIM card?  
What does the SIM file structure begin with?  
Which tool provided by Paraben Software examines Internet of Things (IoT) devices has a bootloader for locked mobile devices and can perform data parsing and cloud data capture?  
In a Windows environment what is the default storage location used by BitPim?  
Which forensics software tool contains a built-in write blocker?  
The Enhanced Data GSM Environment (EDGE) standard was developed specifically for which type of service?  
What entity created the Interim Standards used in mobile communications?  
What technique in which multiple phones take turns sharing a channel does the Global System for Mobile Communications (GSM) use?  
What entity developed the 3G standard?  
How much internal memory do mobile devices have?  
Which tool used by government agencies retrieves data from smartphones GPS devices tablets music players and drones?  
Which Cellebrite mobile forensics tool is often used by law enforcement and the military?  
The Internet is the successor to the Advanced Research Projects Agency Network (ARPANET).  
A search warrant can be used in any kind of case either civil or criminal.  
Specially trained system and network administrators are often a CSP's first responders.  
The law requires search warrants to contain specific descriptions of what's to be seized. For cloud environments the property to be seized usually describes physical hardware rather than data unless the CSP is a suspect.  
In the United States the Electronic Communications Privacy Act (ECPA) describes five mechanisms the government can use to get electronic information from a provider.  
In 1999 Salesforce.com developed a customer relationship management (CRM) Web service that applied digital marketing research to business subscribers so that they could do their own market analysis; this service eventually led the way to the cloud.  
The platform as a service cloud service is most likely found on a desktop or a server although it could also be found on a company network or the remote service provider's infrastructure.  
Homomorphic encryption uses an "ideal lattice" mathematical formula to encrypt data.  
Remote acquisitions are often easier because you're usually dealing with large volumes of data.  
Magnet AXIOM Cloud can retrieve information from Skype Instagram Twitter iCloud but not from Facebook Messenger.  
Metadata in a prefetch file contains an application's \_\_\_\_ times in UTC format and a counter of how many times the application has run since the prefect file was created.  
Which organization has developed resource documentation for cloud service providers and their staff and provides guidance for privacy agreements security measures and other issues?  
In which cloud service level are applications delivered via the Internet?  
What cloud application offers a variety of cloud services including automation and CRM cloud application development and Web site marketing?  
What document issued by a judge compels the recipient to do or not do something?  
What files created by Microsoft contain the DLL pathnames and metadata used by applications and reduce the time it takes to start applications?  
What is Microsoft's SkyDrive now called?  
With cloud systems running in a virtual environment what can be used to give the investigator valuable information before during and after an incident?  
Which type of order requires that the government offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication or the records or other information sought are relevant and material to an ongoing criminal investigation?  
A government entity must show that there is probable cause to believe the contents of a wire communication an electronic communication or other records are relevant to an ongoing criminal investigation to obtain which type of order?  
Which tool can be used to bypass a virtual machine's hypervisor and can be used with OpenStack?  
What cloud service provides a freeware type 1 hypervisor used for public and private clouds?  
Which folder is most likely to contain Dropbox files for a specific user?  
Which type of tool has application programming interfaces (APIs) that allow reconfiguring a cloud on the fly and is accessed through the application's Web interface?  
Which Dropbox file stores information on shared directories associated with a Dropbox user account and file transfers between Dropbox and the client's system?  
At what offset are the application's last access date and time located in a prefetch file?  
At what offset is a prefetch file's create date and time located?  
Which cloud forensics training program is limited to law enforcement personnel?  
Where is the snapshot database created by Google Drive located in Windows?  
Which Google Drive file contains a detailed list of a user's cloud transactions?  
Besides presenting facts reports can communicate expert opinion.  
A verbal report is more structured than a written report.  
If you must write a preliminary report use words such as "preliminary copy", "draft copy", or "working draft"  
As with any research paper write the report abstract last.  
When writing a report use a formal technical style.  
When writing a report style means the tone of language you use to address the reader.  
The decimal numbering system is frequently used when writing pleadings.  
Lawyers use services called deposition banks (libraries) which store examples of expert witnesses' previous testimony.  
Signposts assist readers in scanning the text quickly by highlighting the main points and logical development of information.  
For civil cases including those involving digital forensics investigations U.S. district courts consider optional that expert witnesses submit written reports.  
What is the standard format in U.S. federal courts for the electronic submission of documents?  
Which document serves as a guideline for knowing what questions an investigator should expect when testifying?  
What is most appropriately used to help an attorney learn the terms and functions used in digital forensics?  
A written report is often submitted as what type of document?  
What should be provided if a report is long and complex?  
Which document is sworn to under oath and penalty of perjury or a comparable false swearing statute?  
What type of question should an attorney ask to allow an investigator to offer an opinion?  
Which Federal Rule of Evidence rule governs expert opinions?  
Anything an investigator writes down as part of examination for a report in a civil litigation case is subject to which action from the opposing attorney?  
Because opposing counsel can demand discovery on them what are written preliminary reports considered to be?  
How many words should an abstract contain?  
Under FRCP Rule 26 where must the investigator's curriculum vitae be placed unless the bona fides are integrated elsewhere?  
In addition to decimal numbering what numbering system can be used in a written report?  
Which numbering system is being used if the report writer divides material into sections and restarts numbering with each main section?  
What format is typically used to cite references in the main body of a report?  
What section of a report should contain broader generalizations?  
What section of a report should restate the objectives aims and key questions and summarize the findings with clear concise statements?  
What section of a report can be used for material such as raw data figures not used in the body of the report and anticipated exhibits?  
In addition to text word processing and spreadsheet formats which format is used for forensic reports and logs generated by forensic tools?  
What sections of a report are included in the report body?  
As an expert witness you have opinions about what you have found or observed.  
You should create a formal checklist of your procedures that's applied to all your cases or include such a checklist in your report.  
As a standard practice collect evidence and record the tools you used in designated file folders or evidence containers.  
Like a job resume your CV should be geared for a specific trial.  
Part of what you have to deliver to the jury is a person they can trust to help them figure out something that's beyond their expertise.  
The chain of custody of evidence supports the integrity of your evidence.  
Depending on your attorney's needs you might give him or her just your opinion and technical expertise instead of testifying in court; this role is called an expert witness.  
Motion in limine includes voir dire of venireman strikes and seating of jurors.  
During opening statements both attorneys provide an overview of the case with the plaintiff's attorney going last.  
Whether you're serving as an expert witness or a fact witness be professional and polite when presenting yourself to any attorney or the court.  
How many roles might a forensics examiner play in a trial?  
In which type of testimony does the investigator present evidence and explain what it is and how it was obtained?  
What should you use to verify evidence and thus ensure its integrity?  
What should the forensics specialist keep updated and complete in order to support his or her role as an expert and document enhancement of skills through training teaching and experience?  
How often should the document describing your expertise and used to quality your testimony be updated to reflect new cases and additional training?  
Which motion provides a written list of objections to certain testimony or exhibits?  
What term refers to rejecting potential jurors?  
What optional phase of a trial typically involves an issue raised during cross-examination of a witness?  
How close should a microphone be to the person testifying?  
How many years of education does the typical juror have?  
What method might be used by opposing attorneys to prevent an investigator from serving on an important case?  
What term refers to evidence that exonerates or diminishes the defendant's liability?  
What type of testimony occurs when the investigator answers questions from the attorney who hired the investigator?  
What is the most important part of an investigator's testimony at a trial?  
Generally the best approach an attorney can take in direct examination is to ask the investigator what type of questions?  
Leading questions such as "Isn't it true that forensics experts always destroy their handwritten notes", are referred to as what type of questions?  
What type of questions ask several questions inside one question?  
How is a deposition different from trial testimony?  
Which type of deposition is used to give an opposing attorney the chance to conduct what amounts to a direct examination and cross-examination of a witness?  
Which practice is advisable when an investigator gives a deposition?  
People need ethics to help maintain their balance especially in difficult and contentious situations.  
In the United States there's no state or national licensing body for digital forensics examiners.  
Experts should be paid in full for all previous work and for the anticipated time required for testimony.  
Expert opinions cannot be presented without stating the underlying factual basis.  
The American Bar Association (ABA) is a licensing body.  
When searching for specific record information sometimes you see duplicate files with the same name that have different data runs meaning the file was written to disk more than once on separate occasions.  
As an expert witness you can't testify if you weren't present when the event occurred.  
When you're aware of a possible disqualification issue bring it to the attention of the opposing attorney.  
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.  
There are inherent conflicts between the goals of attorneys and the goals of scientists or technicians (experts).  
What are the most important laws applying to attorneys and witnesses?  
Forensic examiners may serve as what types of witnesses?  
What resource might attorneys use to search for information on expert witnesses?  
What type of questions can give the investigator the factual structure to support and defend his or her opinion?  
Which Federal Rule of Evidence is used to determine whether the expert is qualified and whether the expert opinion can be helpful?  
Which Federal Rule of Evidence is used to determine whether the basis for testimony is adequate?  
Which organization has stated that unlike attorneys expert witnesses do not owe a duty of loyalty to their clients?  
Which document offers comprehensive guidance for psychologists with an entire section devoted to forensics activities?  
Which standard states that to provide reliable and valid testimony the expert has the "ethical responsibility to present a complete and unbiased picture of the . . . research relevant to the case at hand?"  
Attorneys who contact many experts as a ploy to disqualify them or prevent opposing counsel from hiring them are using what practice?  
Which outcome when caused by an ethical lapse could effectively be a death sentence for a career as an expert witness?  
How can an investigator minimize any challenges an opposing attorney could make to discredit the investigator's report or testimony?  
In what court case did the court summarize the process of determining whether an expert should be disqualified because of previous contact with an opposing party?  
Suppose you have been hired to determine whether a corrupted file was intentionally altered or altered by a virus. Your forensic examination did not find evidence of a virus and did not find evidence of intentional alteration. What conclusion can you offer?  
Which action isn't usually punitive but can be embarrassing for the professional and potentially for the attorney who retained the professional?  
Which term refers to internalized rules used to measure one's own performance?  
Requesting which of these will deter attorneys from communicating with an investigator solely for the purpose of disqualifying that investigator?  
Which of the following options would represent a valid retainer?  
What is reduced by knowing who the parties in a case are?  
What can a consultant who doesn't testify earn for finding testifying experts or investigative leads?

Which hashing algorithm is provided by WinHex?

When intruders break into a network they rarely leave a trail behind.

Ans:- False

Network forensics is a fast easy process

Ans:- False

Virtual machines are now common for both personal and business use.

True

Virtual machines (VMs) help offset hardware costs for companies.

True

Type 2 hypervisors cannot be used on laptops.

False

Type 1 hypervisors are usually the ones you find loaded on a suspect machine.

False

Before attempting to install a type 2 hypervisor you need to enable virtualization in the BIOS before attempting to create a VM.

True

In network forensics you have to restore the drive to see how malware that attackers have installed on the system works.

true

A honeywall is a computer set up to look like any other machine on your network but it lures the attacker to it.

False

Network logs record traffic in and out of a network.

true

Which type of forensics can help you determine whether a system is truly under attack or a user has inadvertently installed an untested patch or custom program?

Network forensics

Which type of strategy hides the most valuable data at the innermost part of the network?

What type of software runs virtual machines?

hypervisor

Which type of virtual machine software is typically but not exclusively loaded on servers or workstations with a lot of RAM and storage?

Type 1 hypervisors, also known as bare-metal hypervisors, are typically, but not exclusively, loaded on servers or workstations with a substantial amount of RAM and storage. Hypervisors refers to a type of software that creates and runs virtual machines.

Which product responded to the need for security and performance by producing different CPU designs?

Intel Virtualization Technology

Which program can be used to examine network traffic?

Tcpdump

Which tool lists all open network sockets including those hidden by rootkits?

Mandian Memoryze

What determines how long a piece of information lasts on a system?

Order of volatility

Which network defense strategy developed by the National Security Agency (NSA) has three modes of protection?

defense in depth (DiD) strategy

Which tool allows network traffic to be viewed graphically?

etherape

Which network protocol analyzer can be programmed to examine TCP headers to find the SYN flag?

Ans tethereal

Which tool is useful for extracting information from large Libpcap files?

Tcpslice

What are packet analyzers?

On which OSI model layers do most packet analyzers operate?

data link layer

Which format can be read by most packet analyzer tools?

pcap files

In which type of attack does the attacker keep asking the server to establish a connection?

Ans Syn flood

Which tool was designed as an easy-to-use interface for inspecting and analyzing large tcpdump files?

Which tool probes collects and analyzes session data?

ANS :- argus

Which project was developed to make information widely available in an attempt to thwart Internet and network hackers?

Ans:- Honeynet

What term is used for the machines used in a DDoS attack?

Ans zombies

For digital investigators tracking intranet e-mail is easier because accounts use standard names the administrator establishes.

True

Investigating crimes or policy violations involving e-mail is different than investigating other types of computer abuse and crimes.

False

E-mail programs either save e-mail messages on the client computer or leave them on the server.

True

All e-mail servers use databases that store multiple users' e-mails.

False

Like UNIX e-mail servers Exchange maintains logs to track e-mail communication.

True

Forensic linguistics encompasses civil cases criminal cases cyberterrorism cases and other legal proceedings.

True

E-mail crimes and violations rarely depend on the city state and country in which the e-mail originated.

False

Evidence artifacts vary depending on the social media channel and the device.

True

A challenge with using social media data in court is authenticating the author and the information.

True

You can send and receive e-mail in two environments: via the Internet or an intranet (an internal network).

True

What name is used for the configuration typically used for e-mail messages that are distributed from a central server to many connected client computers?

Client/server architecture

In an e-mail address what symbol separates the domain name from the rest of the address?

@

In what type of e-mail programs can the user copy an e-mail message by dragging the message to a storage medium such as a folder or drive?

GUI

What is the main information being sought when examining e-mail headers?

To retrieve e-mail headers in Microsoft Outlook what option should be clicked after the e-mail has been selected?

File, properties

In Web-based e-mail how are messages displayed and saved?

True

In which discipline do professionals listen to voice recordings to determine who's speaking or read e-mail and other writings known to be by a certain person and determine whether that person wrote the e-mail or letter in question?

Ans Forensic linguistics

To view Gmail Web e-mail headers what should be clicked after the e-mail has been opened and the down arrow next to the Reply circular arrow has been clicked?

Show original

To view e-mail headers on Yahoo! what should be clicked on after "More" has been selected?

Ans view raw message.

In Microsoft Outlook what file extension is used with saved sent drafted deleted and received e-mails?

.pst

Which site can be used to verify the names of domains a message is flowing through?

WWW.DKIM.org

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

Circular logging

Which files provide helpful information to an e-mail investigation?

Configuration

Which location contains configuration information for Sendmail?

/etc/mail/sendmail.cf

In which directory do UNIX installations typically store logs?

/var/log