Questions 1. Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media.   
H. shuts the system down by pulling the power plug so that he does not disturb the system in any way.   
H. labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?   
A. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media  
B. Prepare the system for acquisition; Connect the target media; Copy the media; Secure the evidence  
C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media  
D. Secure the evidence; Prepare the system for acquisition; Connect the target media; Copy the media  
Answer: B  
Explanation:    
  
Questions 2. Windows identifies which application to open a file with by examining which of the following?   
A. The file attributes  
B. The file signature at the beginning of the file  
C. The file signature at the end of the file  
D. The file extension  
Answer: D  
Explanation:    
  
Questions 3. If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?   
A. True  
B. False  
Answer: A  
Explanation:    
  
Questions 4. In Microsoft file structures, sectors are grouped together to form   
A. drives  
B. bitstreams  
C. clusters  
D. partitions  
Answer: C  
Explanation:    
  
Questions 5. You are working in the Security Department of a law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is a possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the companys SMTP server?   
A. 10  
B. 25  
C. 110  
D. 135  
Answer: B  
Explanation:    
  
Questions 6. When obtaining a warrant it is important to:   
A. particularly describe the place to be searched and generally describe the items to be seized  
B. generally describe the place to be searched and generally describe the items to be seized  
C. generally describe the place to be searched and particularly describe the items to be seized  
D. particularly describe the place to be searched and particularly describe the items to be seized  
Answer: D  
Explanation:    
  
Questions 7. Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their pervious activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?   
A. The manufacture of the system compromised  
B. The logic, formatting and elegance of the code used in the attack  
C. The nature of the attack  
D. The vulnerability exploited in the incident  
Answer: B  
Explanation:    
  
Questions 8. Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?   
A. search warrant  
B. subpoena  
C. wire tap  
D. bench warrant  
Answer: A  
Explanation:    
  
Questions 9. Which of following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?   
A. Sector  
B. Metadata  
C. MFT  
D. Slack Space  
Answer: D  
Explanation:    
  
Questions 10. From the following spam mail header, identify the host IP that sent this spam?   
From [jie02@netvigator.com](mailto:jie02@netvigator.com) [jie02@netvigator.com](mailto:jie02@netvigator.com) Tue Nov 27 17:27:11 2001   
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id   
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)   
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)   
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)   
Message-Id: >[200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk](mailto:200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk)   
From: "china hotel web"   
To: "Shlam"   
Subject: SHANGHAI (HILTON HOTEL) PACKAGE   
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0  
X-Priority: 3 X-MSMail-   
Priority: Normal   
Reply-To: "china hotel web"   
A. 137.189.96.52  
B. 203.218.39.50  
C. 203.218.39.20  
D. 8.12.1.0  
Answer: C  
Explanation:

Questions 11. When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?   
A. on the individual computer's ARP cache  
B. in the Web Server log files  
C. in the DHCP Server log files  
D. there is no way to determine the specific IP address  
Answer: C  
Explanation:    
  
Questions 12. Lance wants to place a honeypot on his network. Which of the following would be your recommendations?   
A. Use a system that has a dynamic addressing on the network  
B. Use a system that is not directly interacing with the router  
C. Use it on a system in an external DMZ in front of the firewall  
D. It doesnt matter as all replies are faked  
Answer: C  
Explanation:    
  
Questions 13. The use of warning banners helps a company avoid litigation by overcoming an employees assumed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ when connecting to the companys intranet, network, or virtual private network (VPN) and will allow the companys investigators to monitor, search, and retrieve information stored within the network.   
A. right to work  
B. right of free speech  
C. right to Internet access  
D. right of privacy  
Answer: D  
Explanation:    
  
Questions 14. You should make at least how many bit-stream copies of a suspect drive?   
A. 1  
B. 2  
C. 3  
D. 4  
Answer: B  
Explanation:    
  
Questions 15. You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?   
A. 70 years  
B. the life of the author  
C. the life of the author plus 70 years  
D. copyrights last forever  
Answer: C  
Explanation:    
  
Questions 16. In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?   
A. policy of separation  
B. chain of custody  
C. rules of evidence  
D. law of probability  
Answer: B  
Explanation:    
  
Questions 17. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.   
A. Network forensics  
B. Computer forensics  
C. Incident response  
D. Event reaction  
Answer: B  
Explanation:    
  
Questions 18. In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?   
A. evidence in a criminal case must be secured more tightly than in a civil case  
B. evidence in a civil case must be secured more tightly than in a criminal case  
C. evidence procedures are not important unless you work for a law enforcement agency  
D. evidence must be handled in the same way regardless of the type of case  
Answer: D  
Explanation:    
  
Questions 19. One way to identify the presence of hidden partitions on a suspects hard drive is to:   
A. add up the total size of all known partitions and compare it to the total size of the hard drive  
B. examine the FAT and identify hidden partitions by noting an H in the Partition Type field  
C. examine the LILO and note an H in the Partition Type field  
D. it is not possible to have hidden partitions on a hard drive  
Answer: A  
Explanation:    
  
Questions 20. What should you do when approached by a reporter about a case that you are working on or have worked on?   
A. refer the reporter to the attorney that retained you  
B. say, "no comment"  
C. answer all the reporters questions as completely as possible  
D. answer only the questions that help your case  
Answer: A  
Explanation:

Questions 31. You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?   
A. The tool hasn't been tested by the International Standards Organization (ISO)  
B. The tool has not been reviewed and accepted by your peers  
C. Only the local law enforcement should use the tool  
D. You are not certified for using the tool  
Answer: B  
Explanation:    
  
Questions 32. A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is one that performed by a computer program rather than the attacker manually performing the steps in the attack sequence.   
A. automated attack  
B. blackout attack  
C. central processing attack  
D. distributed attack  
Answer: A  
Explanation:    
  
Questions 33. While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?   
A. keep the information on file for later review  
B. bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge (court)  
C. destroy the evidence  
D. present the evidence to the defense attorney  
Answer: B  
Explanation:    
  
Questions 34. Microsoft Outlook maintains email messages in a proprietary format in what type of file?   
A. .email  
B. .mail  
C. .pst  
D. .doc  
Answer: C  
Explanation:    
  
Questions 35. In general, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.   
A. network forensics  
B. data recovery  
C. computer forensics  
D. disaster recovery  
Answer: C  
Explanation:    
  
Questions 36. If a suspect's computer is located in an area that may have toxic chemicals, you must   
A. coordinate with the HAZMAT team  
B. determine a way to obtain the suspect computer  
C. assume the suspect machine is contaminated  
D. do not enter alone  
Answer: A  
Explanation:    
  
Questions 37. To preserve digital evidence, an investigator should \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.   
A. make two copies of each evidence item using a single imaging tool  
B. make a single copy of each evidence item using an approved imaging tool  
C. make two copies of each evidence item using different imaging tools  
D. only store the original evidence item  
Answer: C  
Explanation:    
  
Questions 38. You are working as computer forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firms employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?   
A. inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned  
B. inform the owner that conducting an investigation without a policy is a violation of the 4th Amendment  
C. inform the owner that conducting an investigation without a policy is a violation of the employees expectation of privacy  
D. inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies  
Answer: C  
Explanation:    
  
Questions 39. Jones had been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system.   
H. was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?   
A. A system using Trojaned commands  
B. A honeypot that traps hackers  
C. An environment set up after the user logs in  
D. An environment set up before an user logs in  
Answer: B  
Explanation:    
  
Questions 40. Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?   
A. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum  
B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file  
C. A simple DOS copy will not include deleted files, file slack and other information  
D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector  
Answer: C  
Explanation:

Questions 41. What does the acronym POST mean as it relates to a PC?   
A. Power On Self Test  
B. Pre Operational Situation Test  
C. Primary Operating System Test  
D. Primary Operations Short Test  
Answer: A  
Explanation:    
  
Questions 42. Printing under a windows computer normally requires which one of the following files types to be created?   
A. EME  
B. MEM  
C. EMF  
D. CME  
Answer: C  
Explanation:    
  
Questions 43. What information do you need to recover when searching a victims computer for a crime committed with specific e-mail message?   
A. Internet service provider information  
B. E-mail header  
C. Username and password  
D. Firewall log  
Answer: B  
Explanation:    
  
Questions 44. Which of the following filesystem is used by Mac OS X?   
A. EFS  
B. HFS+  
C. EXT2  
D. NFS  
Answer: B  
Explanation:    
  
Questions 45. One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?   
A. the File Allocation Table  
B. the file header  
C. the file footer  
D. the sector map  
Answer: B  
Explanation:    
  
Questions 46. With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches \_\_\_\_\_\_\_\_.   
A. 0  
B. 1  
C. 10  
D. 2  
Answer: A  
Explanation:    
  
Questions 47. How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?   
A. 16  
B. 32  
C. 64  
D. 48  
Answer: B  
Explanation:    
  
Questions 48. How many sectors will a 125 KB file use in a FAT32 file system?   
A. 32  
B. 16  
C. 256  
D. 25  
Answer: C  
Explanation:    
  
Questions 49. If you plan to startup a suspect's computer, you must modify the \_\_\_\_\_\_\_\_\_\_\_ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.   
A. Boot.sys  
B. Scandisk utility  
C. CMOS  
D. deltree command  
Answer: C  
Explanation:    
  
Questions 50. You have been asked to investigate after a user has reported a threatening e-mail theyve received from an external source. Which of the following are you most interested in when trying to trace the source of the message?   
A. The X509 address  
B. The SMTP reply address  
C. The E-mail Header  
D. The Host Domain Name  
Answer: C  
Explanation:

Questions 61. If you plan to startup a suspect's computer, you must modify the \_\_\_\_\_\_\_\_\_\_\_ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.   
A. Boot.sys  
B. Scandisk utility  
C. CMOS  
D. deltree command  
Answer: C  
Explanation:    
  
Questions 62. While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?   
A. keep the information on file for later review  
B. bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge (court)  
C. destroy the evidence  
D. present the evidence to the defense attorney  
Answer: B  
Explanation:    
  
Questions 63. This is the original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.   
A. Master Boot Record (MBR)  
B. Master File Table (MFT)  
C. File Allocation Table (FAT)  
D. Disk Operating System (DOS)  
Answer: C  
Explanation:    
  
Questions 64. In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact the ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?   
A. the ISP can investigate anyone using their service and can provide you with assistance  
B. the ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant  
C. the ISP cannot conduct any type of investigations on anyone and therefore cannot assist you  
D. ISPs never maintain log files so they would be of no use to your investigation  
Answer: B  
Explanation:    
  
Questions 65. The use of warning banners helps a company avoid litigation by overcoming an employees assumed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ when connecting to the companys intranet, network, or virtual private network (VPN) and will allow the companys investigators to monitor, search, and retrieve information stored within the network.   
A. right to work  
B. right of free speech  
C. right to Internet access  
D. right of privacy  
Answer: D  
Explanation:    
  
Questions 66. You are working as computer forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firms employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?   
A. inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned  
B. inform the owner that conducting an investigation without a policy is a violation of the 4th Amendment  
C. inform the owner that conducting an investigation without a policy is a violation of the employees expectation of privacy  
D. inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies  
Answer: C  
Explanation:    
  
Questions 67. Jason is the security administrator of ACMA metal Corporation. One day he notices that the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United States?   
A. Internet Fraud Complaint Center  
B. Local or national office of the U.S. Secret Service  
C. National Infrastructure Protection Center  
D. CERT Coordination Center  
Answer: C  
Explanation:    
  
Questions 68. Which is a standard procedure to perform during all computer forensics investigations?   
A. with the hard drive in the suspect PC, check the date and time in the systems CMOS  
B. with the hard drive removed from the suspect PC, check the date and time in the systems CMOS  
C. with the hard drive in the suspect PC, check the date and time in the File Allocation Table  
D. with the hard drive removed from the suspect PC, check the date and time in the systems RAM  
Answer: B  
Explanation:    
  
Questions 69. Which of the following should a computer forensics investigations lab have?   
A. isolation  
B. restricted access  
C. open access  
D. an entry log  
Answer: B  
Explanation:    
  
Questions 70. The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?   
A. the USA Patriot Act  
B. the Good Samaritan Laws  
C. the Federal Rules of Evidence  
D. the Fourth Amendment  
Answer: D  
Explanation:

Questions 81. What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?   
A. key escrow  
B. steganography  
C. rootkit  
D. offset  
Answer: B  
Explanation:    
  
Questions 82. What file structure database would you expect to find on floppy disks?   
A. FAT12  
B. FAT16  
C. FAT32  
D. NTFS  
Answer: A  
Explanation:    
  
Questions 83. What does the superblock in Linux define?   
A. file system names  
B. disk geometry  
C. location of the first inode  
D. available space  
Answer: C  
Explanation:    
  
Questions 84. Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?   
A. Microsoft Virtual Machine Identifier  
B. Personal Application Protocol  
C. Globally Unique ID  
D. Individual ASCII String  
Answer: C  
Explanation:    
  
Questions 85. Which of the following filesystem is used by Mac OS X?   
A. EFS  
B. HFS+  
C. EXT2  
D. NFS  
Answer: B  
Explanation:    
  
Questions 86. As a CHFI professional, which of the following is the most important to your professional reputation?   
A. Your certifications  
B. The correct, successful management of each and every case  
C. The fee that you charge  
D. The friendship of local law enforcement officers  
Answer: B  
Explanation:    
  
Questions 87. How many sectors will a 125 KB file use in a FAT32 file system?   
A. 32  
B. 16  
C. 256  
D. 25  
Answer: C  
Explanation:    
  
Questions 88. You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?   
A. All forms should be placed in an approved secure container because they are now primary evidence in the   case.  
B. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.  
C. All forms should be placed in the report file because they are now primary evidence in the case.  
D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.  
Answer: D  
Explanation:    
  
Questions 89. In the context of file deletion process, which of the following statement holds true?   
A. When files are deleted, the data is overwritten and the cluster marked as available  
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten  
C. While booting, the machine may create temporary files that can delete evidence  
D. Secure delete programs work by completely overwriting the file in one go  
Answer: C  
Explanation:    
  
Questions 90. The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene is a description of what legal term?   
A. Detection  
B. Hearsay  
C. Spoliation  
D. Discovery  
Answer: D  
Explanation:

Questions 91. When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?   
A. Time-Sync Protocol  
B. SyncTime Service  
C. Network Time Protocol  
D. Universal Time Set  
Answer: C  
Explanation:    
  
Questions 92. What is the name of the standard Linux command that is also available as a Windows application that can be used to create bit-stream images?   
A. mcopy  
B. image  
C. MD5  
D. dd  
Answer: D  
Explanation:    
  
Questions 93. With regard to using an antivirus scanner during a computer forensics investigation, you should:   
A. scan the suspect hard drive before beginning an investigation  
B. never run a scan on your forensics workstation because it could change your systems configuration  
C. scan your forensics workstation at intervals of no more than once every five minutes during an investigation  
D. scan your forensics workstation before beginning an investigation  
Answer: D  
Explanation:    
  
Questions 94. You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?   
A. limited force and library attack  
B. brute force and dictionary attack  
C. maximum force and thesaurus attack  
D. minimum force and appendix attack  
Answer: B  
Explanation:    
  
Questions 95. In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?   
A. policy of separation  
B. chain of custody  
C. rules of evidence  
D. law of probability  
Answer: B  
Explanation:    
  
Questions 96. You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?   
A. trademark law  
B. patent law  
C. copyright law  
D. IP Law  
Answer: C  
Explanation:    
  
Questions 97. When a file is deleted by Windows Explorer or through the MS-DOS Delete command, the operating system inserts \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the first letter position of the filename in the FAT database.   
A. a blank space  
B. a capital X  
C. the underscore symbol (\_)  
D. the lowercase Greek letter sigma (s)  
Answer: D  
Explanation:    
  
Questions 98. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.   
A. Locard Exchange Principle  
B. Clark Standard  
C. Kelly Policy  
D. Silver-Platter Doctrine  
Answer: D  
Explanation:    
  
Questions 99. What does the acronym POST mean as it relates to a PC?   
A. Power On Self Test  
B. Pre Operational Situation Test  
C. Primary Operating System Test  
D. Primary Operations Short Test  
Answer: A  
Explanation:    
  
Questions 100. You have used a newly released forensic investigation tool, which doesnt meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?   
A. The tool hasnt been tested by the International Standards Organization (ISO)  
B. The tool has not been reviewed and accepted by your peers  
C. Only the local law enforcement should use the tool  
D. You are not certified for using the tool  
Answer: B  
Explanation:

Questions 101. When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to   
A. automate collection from image files  
B. avoiding copying data from the boot partition  
C. acquire data from the host-protected area on a disk  
D. prevent contamination to the evidence drive  
Answer: D  
Explanation:    
  
Questions 102. A state department site was recently attacked and all the servers had their hard disks erased. The incident response team sealed the area and commenced investigation. During evidence collection, they came across a zip disk that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?   
A. They examined the actual evidence on an unrelated system  
B. They attempted to implicate personnel without proof  
C. They tampered with the evidence by using it  
D. They called in the FBI without correlating with the fingerprint data  
Answer: C  
Explanation:    
  
Questions 103. When conducting computer forensic analysis, you must guard against \_\_\_\_\_\_\_\_\_ so that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.   
A. scope creep  
B. unauthorized expenses  
C. overzealous marketing  
D. hard drive failure  
Answer: A  
Explanation:    
  
Questions 104. Hackers can gain access to the Windows Registry and manipulate user passwords, DNS settings, access rights, or other features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (key) to the following Registry hive:   
A. HKEY\_LOCAL\_MACHINE\Hardware\Windows\Start  
B. HKEY\_LOCAL\_USER\Software\Microsoft\OldVersion\Load  
C. HKEY\_CURRENT\_USER\Microsoft\Default  
D. HKEY\_LOCAL\_MACHINE\Software\Microsoft\CurrentVersion\Run  
Answer: D  
Explanation:    
  
Questions 105. You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?   
A. All forms should be placed in an approved secure container because they are now primary evidence in the   case.  
B. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.  
C. All forms should be placed in the report file because they are now primary evidence in the case.  
D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.  
Answer: D  
Explanation:    
  
Questions 106. As a CHFI professional, which of the following is the most important to your professional reputation?   
A. Your certifications  
B. The correct, successful management of each and every case  
C. The fee that you charge  
D. The friendship of local law enforcement officers  
Answer: B  
Explanation:    
  
Questions 107. Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media.   
H. shuts the system down by pulling the power plug so that he does not disturb the system in any way.   
H. labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?   
A. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media  
B. Prepare the system for acquisition; Connect the target media; Copy the media; Secure the evidence  
C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media  
D. Secure the evidence; Prepare the system for acquisition; Connect the target media; Copy the media  
Answer: B  
Explanation:    
  
Questions 108. You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?   
A. limited force and library attack  
B. brute force and dictionary attack  
C. maximum force and thesaurus attack  
D. minimum force and appendix attack  
Answer: B  
Explanation:    
  
Questions 109. To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?   
A. Computer Forensics Tools Validation Committee (CFTVC)  
B. Association of Computer Forensics Software Manufactures (ACFSM)  
C. Society for Valid Forensics Tools and Testing (SVFTT)  
D. National Institute of Standards and Technology (NIST)  
Answer: D  
Explanation:    
  
Questions 110. What does the superblock in Linux define?   
A. file system names  
B. disk geometry  
C. location of the first inode  
D. available space  
Answer: C  
Explanation:

Questions 111. When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?   
A. Time-Sync Protocol  
B. SyncTime Service  
C. Network Time Protocol  
D. Universal Time Set  
Answer: C  
Explanation:    
  
Questions 112. You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a simple backup copy of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a simple backup copy will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?   
A. bit-stream copy  
B. robust copy  
C. full backup copy  
D. incremental backup copy  
Answer: A  
Explanation:    
  
Questions 113. You are working as computer forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firms employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?   
A. inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned  
B. inform the owner that conducting an investigation without a policy is a violation of the 4th Amendment  
C. inform the owner that conducting an investigation without a policy is a violation of the employees expectation of privacy  
D. inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies  
Answer: C  
Explanation:    
  
Questions 114. What binary coding is used most often for e-mail purposes?   
A. SMTP  
B. Uuencode  
C. IMAP  
D. MIME  
Answer: B  
Explanation:    
  
Questions 115. Printing under a windows computer normally requires which one of the following files types to be created?   
A. EME  
B. MEM  
C. EMF  
D. CME  
Answer: C  
Explanation:    
  
Questions 116. An expert witness may give an opinion if:   
A. the opinion, inferences, or conclusions depend on special knowledge, skill, or training not within the ordinary experience of lay jurors  
B. to define the issues of the case for determination by the finder of fact  
C. to stimulate discussion between the consulting expert and the expert witness  
D. to deter the witness from expanding the scope of his or her investigation beyond the requirements of the case  
Answer: A  
Explanation:    
  
Questions 117. You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer.     While at the corporate office of the company, the CEO demands to know the status of the investigation.     What prevents you from discussing the case with the CEO?   
A. the attorney-work-product rule  
B. Good manners  
C. Trade secrets  
D. ISO 17799  
Answer: A  
Explanation:    
  
Questions 118. In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact the ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?   
A. the ISP can investigate anyone using their service and can provide you with assistance  
B. the ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot  
assist you without a warrant  
C. the ISP cannot conduct any type of investigations on anyone and therefore cannot assist you  
D. ISPs never maintain log files so they would be of no use to your investigation  
Answer: B  
Explanation:    
  
Questions 119. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.   
A. Network forensics  
B. Computer forensics  
C. Incident response  
D. Event reaction  
Answer: B  
Explanation:    
  
Questions 120. When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?   
A. a write-blocker  
B. a protocol analyzer  
C. a firewall  
D. a disk editor  
Answer: A  
Explanation:

Questions 121. In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?   
A. policy of separation  
B. chain of custody  
C. rules of evidence  
D. law of probability  
Answer: B  
Explanation:    
  
Questions 122. To preserve digital evidence, an investigator should \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.   
A. make two copies of each evidence item using a single imaging tool  
B. make a single copy of each evidence item using an approved imaging tool  
C. make two copies of each evidence item using different imaging tools  
D. only store the original evidence item  
Answer: C  
Explanation:    
  
Questions 123. When obtaining a warrant it is important to:   
A. particularly describe the place to be searched and generally describe the items to be seized  
B. generally describe the place to be searched and generally describe the items to be seized  
C. generally describe the place to be searched and particularly describe the items to be seized  
D. particularly describe the place to be searched and particularly describe the items to be seized  
Answer: D  
Explanation:    
  
Questions 124. Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?   
A. search warrant  
B. subpoena  
C. wire tap  
D. bench warrant  
Answer: A  
Explanation:    
  
Questions 125. Sectors in hard disks typically contain how many bytes?   
A. 256  
B. 512  
C. 1024  
D. 2048  
Answer: B  
Explanation:    
  
Questions 126. When a file is deleted by Windows Explorer or through the MS-DOS Delete command, the operating system inserts \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the first letter position of the filename in the FAT database.   
A. a blank space  
B. a capital X  
C. the underscore symbol (\_)  
D. the lowercase Greek letter sigma (s)  
Answer: D  
Explanation:    
  
Questions 127. A law enforcement officer may only search for and seize criminal evidence with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists, and the evidence of the specific crime exists at the place to be searched.   
A. mere suspicion  
B. a preponderance of the evidence  
C. probable cause  
D. beyond a reasonable doubt  
Answer: C  
Explanation:    
  
Questions 128. What should you do when approached by a reporter about a case that you are working on or have worked on?   
A. refer the reporter to the attorney that retained you  
B. say, "no comment"  
C. answer all the reporters questions as completely as possible  
D. answer only the questions that help your case  
Answer: A  
Explanation:    
  
Questions 129. Which is a standard procedure to perform during all computer forensics investigations?   
A. with the hard drive in the suspect PC, check the date and time in the systems CMOS  
B. with the hard drive removed from the suspect PC, check the date and time in the systems CMOS  
C. with the hard drive in the suspect PC, check the date and time in the File Allocation Table  
D. with the hard drive removed from the suspect PC, check the date and time in the systems RAM  
Answer: B  
Explanation:    
  
Questions 130. Why should you note all cable connections for a computer you want to seize as evidence?   
A. to know what cable connections existed  
B. to prepare for shutting down the computer  
C. to document the evidence  
D. to know what hardware existed  
Answer: A  
Explanation:

Questions 131. A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.   
A. Image the disk and try to recover deleted files  
B. Seek the help of co-workers who are eye-witnesses  
C. Check the Windows registry for connection data (You may or may not recover)  
D. Approach the websites for evidence  
Answer: A  
Explanation:    
  
Questions 132. What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?   
A. a compressed file  
B. a data stream file  
C. an encrypted file  
D. a reserved file  
Answer: B  
Explanation:    
  
Questions 133. How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?   
A. 16  
B. 32  
C. 64  
D. 48  
Answer: B  
Explanation:    
  
Questions 134. When examining a file with a Hex Editor, what space does the file header occupy?   
A. the first several bytes of the file  
B. one byte at the beginning of the file  
C. none, file headers are contained in the FAT  
D. the last several bytes of the file  
Answer: A  
Explanation:    
  
Questions 135. You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?   
A. make a bit-stream disk-to-disk file  
B. make a bit-stream disk-to-image file  
C. create a sparse data copy of a folder or file  
D. create a compressed copy of the file with DoubleSpace  
Answer: C  
Explanation:    
  
Questions 136. If you plan to startup a suspect's computer, you must modify the \_\_\_\_\_\_\_\_\_\_\_ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.   
A. Boot.sys  
B. Scandisk utility  
C. CMOS  
D. deltree command  
Answer: C  
Explanation:    
  
Questions 137. From the following spam mail header, identify the host IP that sent this spam?   
From [jie02@netvigator.com](mailto:jie02@netvigator.com) [jie02@netvigator.com](mailto:jie02@netvigator.com) Tue Nov 27 17:27:11 2001   
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id  
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)   
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)   
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)   
Message-Id: >[200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk](mailto:200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk)   
From: "china hotel web"   
To: "Shlam"   
Subject: SHANGHAI (HILTON HOTEL) PACKAGE   
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0   
X-Priority: 3 X-MSMail-   
Priority: Normal   
Reply-To: "china hotel web"   
A. 137.189.96.52  
B. 203.218.39.50  
C. 203.218.39.20  
D. 8.12.1.0  
Answer: C  
Explanation:    
  
Questions 138. What happens when a file is deleted by a Microsoft operating system using the FAT file system?   
A. the file is erased and cannot be recovered  
B. the file is erased but can be recovered  
C. a copy of the file is stored and the original file is erased  
D. only the reference to the file is removed from the FAT  
Answer: D  
Explanation:    
  
Questions 139. The offset in a hexadecimal code is:   
A. The 0x at the beginning of the code  
B. The 0x at the end of the code  
C. The first byte after the colon  
D. The last byte after the colon  
Answer: A  
Explanation:    
  
Questions 140. Law enforcement officers are conducting a legal search for which a valid warrant was obtained. While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?   
A. plain view doctrine  
B. corpus delicti  
C. Locard Exchange Principle  
D. Ex Parte Order  
Answer: A  
Explanation:

Questions 141. Corporate investigations are typically easier than public investigations because   
A. the users have standard corporate equipment and software  
B. the investigator does not have to get a warrant  
C. the investigator has to get a warrant  
D. the users can load whatever they want on their machines  
Answer: B  
Explanation:    
  
Questions 142. Which of the following filesystem is used by Mac OS X?   
A. EFS  
B. HFS+  
C. EXT2  
D. NFS  
Answer: B  
Explanation:    
  
Questions 143. E-mail logs contain which of the following information to help you in your investigation?   
A. contents of the e-mail message  
B. attachments sent with the e-mail message  
C. date and time the message was sent  
D. user account that was used to send the message  
E. unique message identifier  
Answer: A,B,C,D  
Explanation:    
  
Questions 144. What does mactime, an essential part of the coroner's toolkit do?   
A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps  
B. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them  
C. The tools scans for i-node information, which is used by other tools in the tool kit  
D. It is a tool specific to the MAC OS and forms a core component of the toolkit  
Answer: A  
Explanation:    
  
Questions 145. Which of the following should a computer forensics investigations lab have?   
A. isolation  
B. restricted access  
C. open access  
D. an entry log  
Answer: B  
Explanation:    
  
Questions 146. You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?   
A. trademark law  
B. patent law  
C. copyright law  
D. IP Law  
Answer: C  
Explanation:    
  
Questions 147. If a suspect's computer is located in an area that may have toxic chemicals, you must   
A. coordinate with the HAZMAT team  
B. determine a way to obtain the suspect computer  
C. assume the suspect machine is contaminated  
D. do not enter alone  
Answer: A  
Explanation:    
  
Questions 148. A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is one thats performed by a computer program rather than the attacker manually performing the steps in the attack sequence.   
A. automated attack  
B. blackout attack  
C. central processing attack  
D. distributed attack  
Answer: A  
Explanation:    
  
Questions 149. You have used a newly released forensic investigation tool, which doesnt meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?   
A. The tool hasnt been tested by the International Standards Organization (ISO)  
B. The tool has not been reviewed and accepted by your peers  
C. Only the local law enforcement should use the tool  
D. You are not certified for using the tool  
Answer: B  
Explanation:    
  
Questions 150. How many sectors will a 125 KB file use in a FAT32 file system?   
A. 32  
B. 16  
C. 256  
D. 25  
Answer: C  
Explanation:

Questions 151. What happens when a file is deleted by a Microsoft operating system using the FAT file system?   
A. the file is erased and cannot be recovered  
B. the file is erased but can be recovered  
C. a copy of the file is stored and the original file is erased  
D. only the reference to the file is removed from the FAT  
Answer: D  
Explanation:    
  
Questions 152. This organization maintains a database of hash signatures for known software   
A. International Standards Organization  
B. Institute of Electrical and Electronics Engineers  
C. National Software Reference Library  
D. American National Standards Institute  
Answer: C  
Explanation:    
  
Questions 153. What information do you need to recover when searching a victims computer for a crime committed with specific e-mail message?   
A. Internet service provider information  
B. E-mail header  
C. Username and password  
D. Firewall log  
Answer: B  
Explanation:    
  
Questions 154. You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?   
A. make a bit-stream disk-to-disk file  
B. make a bit-stream disk-to-image file  
C. create a sparse data copy of a folder or file  
D. create a compressed copy of the file with DoubleSpace  
Answer: C  
Explanation:    
  
Questions 155. Windows identifies which application to open a file with by examining which of the following?   
A. The file attributes  
B. The file signature at the beginning of the file  
C. The file signature at the end of the file  
D. The file extension  
Answer: D  
Explanation:    
  
Questions 156. The MD5 program is used to:   
A. verify that a disk is not altered when you examine it  
B. make directories on a evidence disk  
C. wipe magnetic media before recycling it  
D. view graphics files on an evidence drive  
Answer: A  
Explanation:    
  
Questions 157. If a suspect's computer is located in an area that may have toxic chemicals, you must   
A. coordinate with the HAZMAT team  
B. determine a way to obtain the suspect computer  
C. assume the suspect machine is contaminated  
D. do not enter alone  
Answer: A  
Explanation:    
  
Questions 158. Jones had been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system.   
H. was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?   
A. A system using Trojaned commands  
B. A honeypot that traps hackers  
C. An environment set up after the user logs in  
D. An environment set up before an user logs in  
Answer: B  
Explanation:    
  
Questions 159. With regard to using an antivirus scanner during a computer forensics investigation, you should:   
A. scan the suspect hard drive before beginning an investigation  
B. never run a scan on your forensics workstation because it could change your systems configuration  
C. scan your forensics workstation at intervals of no more than once every five minutes during an investigation  
D. scan your forensics workstation before beginning an investigation  
Answer: D  
Explanation:    
  
Questions 160. Printing under a windows computer normally requires which one of the following files types to be created?   
A. EME  
B. MEM  
C. EMF  
D. CME  
Answer: C  
Explanation:

[Pre-Page](http://www.testsnow.net/txt/3/3549/42097.html) ← [List](http://www.testsnow.net/txt/3/3549/) → [Next-Page](http://www.testsnow.net/txt/3/3549/42099.html)

© 2009-2015 http://www.testsnow.net TestsNow

Questions 161. How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?   
A. 16  
B. 32  
C. 64  
D. 48  
Answer: B  
Explanation:    
  
Questions 162. Which part of the Windows Registry contains the user's password file?   
A. HKEY\_CURRENT\_USER  
B. HKEY\_USER  
C. HKEY\_LOCAL\_MACHINE  
D. HKEY\_CURRENT\_CONFIGURATION  
Answer: B  
Explanation:    
  
Questions 163. When investigating a potential e-mail crime, what is your first step in the investigation?   
A. Determine whether a crime was actually committed  
B. Recover the evidence  
C. Trace the IP address to its origin  
D. Write a report  
Answer: C  
Explanation:    
  
Questions 164. When cataloging digital evidence, the primary goal is to   
A. make bit-stream images of all hard drives  
B. preserve evidence integrity  
C. not remove the evidence from the scene  
D. not allow the computer to be turned off  
Answer: B  
Explanation:    
  
Questions 165. In the context of file deletion process, which of the following statement holds true?   
A. When files are deleted, the data is overwritten and the cluster marked as available  
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten  
C. While booting, the machine may create temporary files that can delete evidence  
D. Secure delete programs work by completely overwriting the file in one go  
Answer: C  
Explanation:    
  
Questions 166. The rule of the thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?   
A. Any data not yet flushed to the system will be lost  
B. All running processes will be lost  
C. The /tmp directory will be flushed  
D. Power interruption will corrupt the pagefile  
Answer: A,B  
Explanation:    
  
Questions 167. When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?   
A. 202  
B. 404  
C. 606  
D. 909  
Answer: B  
Explanation:    
  
Questions 168. Which of the following is NOT a graphics file?   
A. Picture1.tga  
B. Picture2.bmp  
C. Picture3.nfo  
D. Picture4.psd  
Answer: C  
Explanation:    
  
Questions 169. When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?   
A. Time-Sync Protocol  
B. SyncTime Service  
C. Network Time Protocol  
D. Universal Time Set  
Answer: C  
Explanation:    
  
Questions 170. If you plan to startup a suspect's computer, you must modify the \_\_\_\_\_\_\_\_\_\_\_ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.   
A. Boot.sys  
B. Scandisk utility  
C. CMOS  
D. deltree command  
Answer: C  
Explanation:

[Pre-Page](http://www.testsnow.net/txt/3/3549/42098.html) ← [List](http://www.testsnow.net/txt/3/3549/) → [Next-Page](http://www.testsnow.net/txt/3/3549/42100.html)

Questions 171. Hackers can gain access to the Windows Registry and manipulate user passwords, DNS settings, access rights, or other features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (key) to the following Registry hive:   
A. HKEY\_LOCAL\_MACHINE\Hardware\Windows\Start  
B. HKEY\_LOCAL\_USER\Software\Microsoft\OldVersion\Load  
C. HKEY\_CURRENT\_USER\Microsoft\Default  
D. HKEY\_LOCAL\_MACHINE\Software\Microsoft\CurrentVersion\Run  
Answer: D  
Explanation:    
  
Questions 172. What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?   
A. ARP redirect  
B. physical attack  
C. digital attack  
D. denial of service  
Answer: D  
Explanation:    
  
Questions 173. When investigating a Windows system, it is important to view the contents of the "page" or "swap" file because:   
A. Windows stores all of the systems configuration information in this file  
B. this is the file that Windows uses to communicate directly with the Registry  
C. a large volume of data can exist within the swap file of which the computer user has no knowledge  
D. this is the file that Windows uses to store the history of the last 100 commands that were run from the command line  
Answer: C  
Explanation:    
  
Questions 174. When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?   
A. a write-blocker  
B. a protocol analyzer  
C. a firewall  
D. a disk editor  
Answer: A  
Explanation:    
  
Questions 175. You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?   
A. All forms should be placed in an approved secure container because they are now primary evidence in the   case.  
B. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.  
C. All forms should be placed in the report file because they are now primary evidence in the case.  
D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.  
Answer: D  
Explanation:    
  
Questions 176. When conducting computer forensic analysis, you must guard against \_\_\_\_\_\_\_\_\_ so that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.   
A. scope creep  
B. unauthorized expenses  
C. overzealous marketing  
D. hard drive failure  
Answer: A  
Explanation:    
  
Questions 177. During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as:   
A. Inculpatory evidence  
B. Terrible evidence  
C. Exculpatory evidence  
D. Mandatory evidence  
Answer: C  
Explanation:    
  
Questions 178. An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are \_\_\_\_\_\_\_\_\_\_\_\_\_\_ media used to store large amounts of data and are not affected by the magnet.   
A. magnetic  
B. optical  
C. anti-magnetic  
D. logical  
Answer: B  
Explanation:    
  
Questions 179. A state department site was recently attacked and all the servers had their hard disks erased. The incident response team sealed the area and commenced investigation. During evidence collection, they came across a zip disk that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?   
A. They examined the actual evidence on an unrelated system  
B. They attempted to implicate personnel without proof  
C. They tampered with the evidence by using it  
D. They called in the FBI without correlating with the fingerprint data  
Answer: C  
Explanation:    
  
Questions 180. Jason is the security administrator of ACMA metal Corporation. One day he notices that the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crimes investigations throughout the United States?   
A. Internet Fraud Complaint Center  
B. Local or national office of the U.S. Secret Service  
C. National Infrastructure Protection Center  
D. CERT Coordination Center  
Answer: C  
Explanation:

Questions 181. Lance wants to place a honeypot on his network. Which of the following would be your recommendations?   
A. Use a system that has a dynamic addressing on the network  
B. Use a system that is not directly interacing with the router  
C. Use it on a system in an external DMZ in front of the firewall  
D. It doesnt matter as all replies are faked  
Answer: C  
Explanation:    
  
Questions 182. What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?   
A. a compressed file  
B. a data stream file  
C. an encrypted file  
D. a reserved file  
Answer: B  
Explanation:    
  
Questions 183. Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their pervious activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?   
A. The manufacture of the system compromised  
B. The logic, formatting and elegance of the code used in the attack  
C. The nature of the attack  
D. The vulnerability exploited in the incident  
Answer: B  
Explanation:    
  
Questions 184. Which of following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?   
A. Sector  
B. Metadata  
C. MFT  
D. Slack Space  
Answer: D  
Explanation:    
  
Questions 185. You should make at least how many bit-stream copies of a suspect drive?   
A. 1  
B. 2  
C. 3  
D. 4  
Answer: B  
Explanation:    
  
Questions 186. You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer.     While at the corporate office of the company, the CEO demands to know the status of the investigation.     What prevents you from discussing the case with the CEO?   
A. the attorney-work-product rule  
B. Good manners  
C. Trade secrets  
D. ISO 17799  
Answer: A  
Explanation:    
  
Questions 187. With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches \_\_\_\_\_\_\_\_.   
A. 0  
B. 1  
C. 10  
D. 2  
Answer: A  
Explanation:    
  
Questions 188. In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?   
A. evidence in a criminal case must be secured more tightly than in a civil case  
B. evidence in a civil case must be secured more tightly than in a criminal case  
C. evidence procedures are not important unless you work for a law enforcement agency  
D. evidence must be handled in the same way regardless of the type of case  
Answer: D  
Explanation:    
  
Questions 189. What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?   
A. key escrow  
B. steganography  
C. rootkit  
D. offset  
Answer: B  
Explanation:    
  
Questions 190. When examining a hard disk without a write-blocker, you should not start Windows because Windows will write data to the:   
A. MSDOS.SYS  
B. Recycle Bin  
C. BIOS  
D. Case files  
Answer: B  
Explanation:

Questions 191. You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?   
A. limited force and library attack  
B. brute force and dictionary attack  
C. maximum force and thesaurus attack  
D. minimum force and appendix attack  
Answer: B  
Explanation:    
  
Questions 192. One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?   
A. the File Allocation Table  
B. the file header  
C. the file footer  
D. the sector map  
Answer: B  
Explanation:    
  
Questions 193. To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?   
A. Computer Forensics Tools Validation Committee (CFTVC)  
B. Association of Computer Forensics Software Manufactures (ACFSM)  
C. Society for Valid Forensics Tools and Testing (SVFTT)  
D. National Institute of Standards and Technology (NIST)  
Answer: D  
Explanation:    
  
Questions 194. When you carve an image, recovering the image depends on which of the following skills?   
A. recovering the image from a tape backup  
B. recognizing the pattern of the data content  
C. recognizing the pattern of the header content  
D. recognizing the pattern of a corrupt file  
Answer: C  
Explanation:    
  
Questions 195. Sectors in hard disks typically contain how many bytes?   
A. 256  
B. 512  
C. 1024  
D. 2048  
Answer: B  
Explanation:    
  
Questions 196. E-mail logs contain which of the following information to help you in your investigation?   
A. contents of the e-mail message  
B. attachments sent with the e-mail message  
C. date and time the message was sent  
D. user account that was used to send the message  
E. unique message identifier  
Answer: A,B,C,D  
Explanation:    
  
Questions 197. When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?   
A. on the individual computer's ARP cache  
B. in the Web Server log files  
C. in the DHCP Server log files  
D. there is no way to determine the specific IP address  
Answer: C  
Explanation:    
  
Questions 198. When examining a file with a Hex Editor, what space does the file header occupy?   
A. the first several bytes of the file  
B. one byte at the beginning of the file  
C. none, file headers are contained in the FAT  
D. the last several bytes of the file  
Answer: A  
Explanation:    
  
Questions 199. You have completed a forensic investigation case. You would like to destroy the data contained in various hard disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disks? (Recovery of data should be impossible)   
A. Run powerful magnets over the hard disk  
B. Format the hard disk multiple times using a low level disk utility  
C. Overwrite the contents of the hard disk with junk data  
D. Smash the hard disk with a hammer  
E. Throw the hard disk into the fire  
Answer: E  
Explanation:    
  
Questions 200. The use of warning banners helps a company avoid litigation by overcoming an employees assumed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ when connecting to the companys intranet, network, or virtual private network (VPN) and will allow the companys investigators to monitor, search, and retrieve information stored within the network.   
A. right to work  
B. right of free speech  
C. right to Internet access  
D. right of privacy  
Answer: D  
Explanation:

Questions 201. While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?   
A. keep the information on file for later review  
B. bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge (court)  
C. destroy the evidence  
D. present the evidence to the defense attorney  
Answer: B  
Explanation:    
  
Questions 202. The MD5 program is used to:   
A. verify that a disk is not altered when you examine it  
B. make directories on a evidence disk  
C. wipe magnetic media before recycling it  
D. view graphics files on an evidence drive  
Answer: A  
Explanation:    
  
Questions 203. Volatile memory is one of the leading problems for forensics. Worms such as Code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?   
A. Use VMware to be able to capture the data in memory and examine it  
B. Give the operating system a minimal amount of memory, forcing it to use a swap file  
C. Create a separate partition of several hundred megabytes and place the swap file there  
D. Use intrusion forensic techniques to study memory resident infections  
Answer: C  
Explanation:    
  
Questions 204. You have completed a forensic investigation case. You would like to destroy the data contained in various hard disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disks? (Recovery of data should be impossible)   
A. Run powerful magnets over the hard disk  
B. Format the hard disk multiple times using a low level disk utility  
C. Overwrite the contents of the hard disk with junk data  
D. Smash the hard disk with a hammer  
E. Throw the hard disk into the fire  
Answer: E  
Explanation:    
  
Questions 205. What does mactime, an essential part of the coroner's toolkit do?   
A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps  
B. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them  
C. The tools scans for i-node information, which is used by other tools in the tool kit  
D. It is a tool specific to the MAC OS and forms a core component of the toolkit  
Answer: A  
Explanation:    
  
Questions 206. An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are \_\_\_\_\_\_\_\_\_\_\_\_\_\_ media used to store large amounts of data and are not affected by the magnet.   
A. magnetic  
B. optical  
C. anti-magnetic  
D. logical  
Answer: B  
Explanation:    
  
Questions 207. A state department site was recently attacked and all the servers had their hard disks erased. The incident response team sealed the area and commenced investigation. During evidence collection, they came across a zip disk that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?   
A. They examined the actual evidence on an unrelated system  
B. They attempted to implicate personnel without proof  
C. They tampered with the evidence by using it  
D. They called in the FBI without correlating with the fingerprint data  
Answer: C  
Explanation:    
  
Questions 208. When examining a hard disk without a write-blocker, you should not start Windows because Windows will write data to the:   
A. MSDOS.SYS  
B. Recycle Bin  
C. BIOS  
D. Case files  
Answer: B  
Explanation:    
  
Questions 209. Which is a standard procedure to perform during all computer forensics investigations?   
A. with the hard drive in the suspect PC, check the date and time in the systems CMOS  
B. with the hard drive removed from the suspect PC, check the date and time in the systems CMOS  
C. with the hard drive in the suspect PC, check the date and time in the File Allocation Table  
D. with the hard drive removed from the suspect PC, check the date and time in the systems RAM  
Answer: B  
Explanation:    
  
Questions 210. What does the superblock in Linux define?   
A. file system names  
B. disk geometry  
C. location of the first inode  
D. available space  
Answer: C  
Explanation:

Questions 211. Jones had been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system.   
H. was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?   
A. A system using Trojaned commands  
B. A honeypot that traps hackers  
C. An environment set up after the user logs in  
D. An environment set up before an user logs in  
Answer: B  
Explanation:    
  
Questions 212. Why should you note all cable connections for a computer you want to seize as evidence?   
A. to know what cable connections existed  
B. to prepare for shutting down the computer  
C. to document the evidence  
D. to know what hardware existed  
Answer: A  
Explanation:    
  
Questions 213. Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?   
A. Microsoft Virtual Machine Identifier  
B. Personal Application Protocol  
C. Globally Unique ID  
D. Individual ASCII String  
Answer: C  
Explanation:    
  
Questions 214. Which of the following should a computer forensics investigations lab have?   
A. isolation  
B. restricted access  
C. open access  
D. an entry log  
Answer: B  
Explanation:    
  
Questions 215. If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?   
A. True  
B. False  
Answer: A  
Explanation:    
  
Questions 216. You have used a newly released forensic investigation tool, which doesnt meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?   
A. The tool hasnt been tested by the International Standards Organization (ISO)  
B. The tool has not been reviewed and accepted by your peers  
C. Only the local law enforcement should use the tool  
D. You are not certified for using the tool  
Answer: B  
Explanation:    
  
Questions 217. What happens when a file is deleted by a Microsoft operating system using the FAT file system?   
A. the file is erased and cannot be recovered  
B. the file is erased but can be recovered  
C. a copy of the file is stored and the original file is erased  
D. only the reference to the file is removed from the FAT  
Answer: D  
Explanation:    
  
Questions 218. The use of warning banners helps a company avoid litigation by overcoming an employees assumed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ when connecting to the companys intranet, network, or virtual private network (VPN) and will allow the companys investigators to monitor, search, and retrieve information stored within the network.   
A. right to work  
B. right of free speech  
C. right to Internet access  
D. right of privacy  
Answer: D  
Explanation:    
  
Questions 219. You are working in the Security Department of a law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is a possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the companys SMTP server?   
A. 10  
B. 25  
C. 110  
D. 135  
Answer: B  
Explanation:    
  
Questions 220. Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?   
A. Network-based IDS systems (NIDS)  
B. Host-based IDS systems (HIDS)  
C. Anomaly detection  
D. Signature recognition  
Answer: C  
Explanation:

Questions 221. A law enforcement officer may only search for and seize criminal evidence with \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists, and the evidence of the specific crime exists at the place to be searched.   
A. mere suspicion  
B. a preponderance of the evidence  
C. probable cause  
D. beyond a reasonable doubt  
Answer: C  
Explanation:    
  
Questions 222. An expert witness may give an opinion if:   
A. the opinion, inferences, or conclusions depend on special knowledge, skill, or training not within the ordinary experience of lay jurors  
B. to define the issues of the case for determination by the finder of fact  
C. to stimulate discussion between the consulting expert and the expert witness  
D. to deter the witness from expanding the scope of his or her investigation beyond the requirements of the case  
Answer: A  
Explanation:    
  
Questions 223. What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?   
A. a compressed file  
B. a data stream file  
C. an encrypted file  
D. a reserved file  
Answer: B  
Explanation:    
  
Questions 224. You are assisting in the investigation of a possible Web Server hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a pornographic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?   
A. ARP Poisoning  
B. DNS Poisoning  
C. HTTP redirect attack  
D. IP Spoofing  
Answer: B  
Explanation:    
  
Questions 225. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.   
A. Locard Exchange Principle  
B. Clark Standard  
C. Kelly Policy  
D. Silver-Platter Doctrine  
Answer: D  
Explanation:    
  
Questions 226. You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?   
A. 70 years  
B. the life of the author  
C. the life of the author plus 70 years  
D. copyrights last forever  
Answer: C  
Explanation:    
  
Questions 227. In the context of file deletion process, which of the following statement holds true?   
A. When files are deleted, the data is overwritten and the cluster marked as available  
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten  
C. While booting, the machine may create temporary files that can delete evidence  
D. Secure delete programs work by completely overwriting the file in one go  
Answer: C  
Explanation:    
  
Questions 228. When conducting computer forensic analysis, you must guard against \_\_\_\_\_\_\_\_\_ so that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.   
A. scope creep  
B. unauthorized expenses  
C. overzealous marketing  
D. hard drive failure  
Answer: A  
Explanation:    
  
Questions 229. In general, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.   
A. network forensics  
B. data recovery  
C. computer forensics  
D. disaster recovery  
Answer: C  
Explanation:    
  
Questions 230. Before you are called to testify as an expert, what must an attorney do first?   
A. engage in damage control  
B. read your curriculum vitae to the jury  
C. qualify you as an expert witness  
D. prove that the tools you used to conduct your examination are perfect  
Answer: C  
Explanation:

Questions 231. When a file is deleted by Windows Explorer or through the MS-DOS Delete command, the operating system inserts \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the first letter position of the filename in the FAT database.   
A. a blank space  
B. a capital X  
C. the underscore symbol (\_)  
D. the lowercase Greek letter sigma (s)  
Answer: D  
Explanation:    
  
Questions 232. How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?   
A. 16  
B. 32  
C. 64  
D. 48  
Answer: B  
Explanation:    
  
Questions 233. During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as:   
A. Inculpatory evidence  
B. Terrible evidence  
C. Exculpatory evidence  
D. Mandatory evidence  
Answer: C  
Explanation:    
  
Questions 234. Which of following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?   
A. Sector  
B. Metadata  
C. MFT  
D. Slack Space  
Answer: D  
Explanation:    
  
Questions 235. E-mail logs contain which of the following information to help you in your investigation?   
A. contents of the e-mail message  
B. attachments sent with the e-mail message  
C. date and time the message was sent  
D. user account that was used to send the message  
E. unique message identifier  
Answer: A,B,C,D  
Explanation:    
  
Questions 236. You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer.     While at the corporate office of the company, the CEO demands to know the status of the investigation.     What prevents you from discussing the case with the CEO?   
A. the attorney-work-product rule  
B. Good manners  
C. Trade secrets  
D. ISO 17799  
Answer: A  
Explanation:    
  
Questions 237. What does the acronym POST mean as it relates to a PC?   
A. Power On Self Test  
B. Pre Operational Situation Test  
C. Primary Operating System Test  
D. Primary Operations Short Test  
Answer: A  
Explanation:    
  
Questions 238. In Microsoft file structures, sectors are grouped together to form   
A. drives  
B. bitstreams  
C. clusters  
D. partitions  
Answer: C  
Explanation:    
  
Questions 239. When investigating a potential e-mail crime, what is your first step in the investigation?   
A. Determine whether a crime was actually committed  
B. Recover the evidence  
C. Trace the IP address to its origin  
D. Write a report  
Answer: C  
Explanation:    
  
Questions 240. You have been asked to investigate after a user has reported a threatening e-mail theyve received from an external source. Which of the following are you most interested in when trying to trace the source of the message?   
A. The X509 address  
B. The SMTP reply address  
C. The E-mail Header  
D. The Host Domain Name  
Answer: C  
Explanation:

Questions 241. When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?   
A. 202  
B. 404  
C. 606  
D. 909  
Answer: B  
Explanation:    
  
Questions 242. When examining a file with a Hex Editor, what space does the file header occupy?   
A. the first several bytes of the file  
B. one byte at the beginning of the file  
C. none, file headers are contained in the FAT  
D. the last several bytes of the file  
Answer: A  
Explanation:    
  
Questions 243. In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?   
A. evidence in a criminal case must be secured more tightly than in a civil case  
B. evidence in a civil case must be secured more tightly than in a criminal case  
C. evidence procedures are not important unless you work for a law enforcement agency  
D. evidence must be handled in the same way regardless of the type of case  
Answer: D  
Explanation:    
  
Questions 244. What file structure database would you expect to find on floppy disks?   
A. FAT12  
B. FAT16  
C. FAT32  
D. NTFS  
Answer: A  
Explanation:    
  
Questions 245. Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media.   
H. shuts the system down by pulling the power plug so that he does not disturb the system in any way.   
H. labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?   
A. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media  
B. Prepare the system for acquisition; Connect the target media; Copy the media; Secure the evidence  
C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media  
D. Secure the evidence; Prepare the system for acquisition; Connect the target media; Copy the media  
Answer: B  
Explanation:    
  
Questions 246. Lance wants to place a honeypot on his network. Which of the following would be your recommendations?   
A. Use a system that has a dynamic addressing on the network  
B. Use a system that is not directly interacing with the router  
C. Use it on a system in an external DMZ in front of the firewall  
D. It doesnt matter as all replies are faked  
Answer: C  
Explanation:    
  
Questions 247. When investigating a Windows system, it is important to view the contents of the "page" or "swap" file because:   
A. Windows stores all of the systems configuration information in this file  
B. this is the file that Windows uses to communicate directly with the Registry  
C. a large volume of data can exist within the swap file of which the computer user has no knowledge  
D. this is the file that Windows uses to store the history of the last 100 commands that were run from the command line  
Answer: C  
Explanation:    
  
Questions 248. An employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the employees computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the employee before he leaves the building and recover the floppy disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?   
A. EFS uses a 128-bit key that cannot be cracked, so you will not be able to recover the information.  
B. The EFS Revoked Key Agent can be used on the computer to recover the information.  
C. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.  
D. When the encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.  
Answer: C  
Explanation:    
  
Questions 249. What should you do when approached by a reporter about a case that you are working on or have worked on?   
A. refer the reporter to the attorney that retained you  
B. say, "no comment"  
C. answer all the reporters questions as completely as possible  
D. answer only the questions that help your case  
Answer: A  
Explanation:    
  
Questions 250. Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?   
A. search warrant  
B. subpoena  
C. wire tap  
D. bench warrant  
Answer: A  
Explanation:

Questions 251. You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question wheather evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?   
A. sign a statement attesting that the evidence is the same as it was when it entered the lab  
B. there is no reason to worry about this possible claim because state labs are certified  
C. make an MD5 hash of the evidence and compare it to the standard database developed by NIST  
D. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab  
Answer: D  
Explanation:    
  
Questions 252. What is the name of the standard Linux command that is also available as a Windows application that can be used to create bit-stream images?   
A. mcopy  
B. image  
C. MD5  
D. dd  
Answer: D  
Explanation:    
  
Questions 253. While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?   
A. keep the information on file for later review  
B. bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge (court)  
C. destroy the evidence  
D. present the evidence to the defense attorney  
Answer: B  
Explanation:    
  
Questions 254. In the context of file deletion process, which of the following statement holds true?   
A. When files are deleted, the data is overwritten and the cluster marked as available  
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten  
C. While booting, the machine may create temporary files that can delete evidence  
D. Secure delete programs work by completely overwriting the file in one go  
Answer: C  
Explanation:    
  
Questions 255. One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?   
A. the File Allocation Table  
B. the file header  
C. the file footer  
D. the sector map  
Answer: B  
Explanation:    
  
Questions 256. You are working in the Security Department of a law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is a possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the companys SMTP server?   
A. 10  
B. 25  
C. 110  
D. 135  
Answer: B  
Explanation:    
  
Questions 257. When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to   
A. automate collection from image files  
B. avoiding copying data from the boot partition  
C. acquire data from the host-protected area on a disk  
D. prevent contamination to the evidence drive  
Answer: D  
Explanation:    
  
Questions 258. You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?   
A. trademark law  
B. patent law  
C. copyright law  
D. IP Law  
Answer: C  
Explanation:    
  
Questions 259. What does the acronym POST mean as it relates to a PC?   
A. Power On Self Test  
B. Pre Operational Situation Test  
C. Primary Operating System Test  
D. Primary Operations Short Test  
Answer: A  
Explanation:    
  
Questions 260. When obtaining a warrant it is important to:   
A. particularly describe the place to be searched and generally describe the items to be seized  
B. generally describe the place to be searched and generally describe the items to be seized  
C. generally describe the place to be searched and particularly describe the items to be seized  
D. particularly describe the place to be searched and particularly describe the items to be seized  
Answer: D  
Explanation:

Questions 261. When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?   
A. on the individual computer's ARP cache  
B. in the Web Server log files  
C. in the DHCP Server log files  
D. there is no way to determine the specific IP address  
Answer: C  
Explanation:    
  
Questions 262. You are assisting in the investigation of a possible Web Server hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a pornographic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?   
A. ARP Poisoning  
B. DNS Poisoning  
C. HTTP redirect attack  
D. IP Spoofing  
Answer: B  
Explanation:    
  
Questions 263. If a suspect's computer is located in an area that may have toxic chemicals, you must   
A. coordinate with the HAZMAT team  
B. determine a way to obtain the suspect computer  
C. assume the suspect machine is contaminated  
D. do not enter alone  
Answer: A  
Explanation:    
  
Questions 264. An employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the employees computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the employee before he leaves the building and recover the floppy disk and secure his computer. Will you be able to break the encryption so that you can verify that the employee was in possession of the proprietary information?   
A. EFS uses a 128-bit key that cannot be cracked, so you will not be able to recover the information.  
B. The EFS Revoked Key Agent can be used on the computer to recover the information.  
C. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.  
D. When the encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.  
Answer: C  
Explanation:    
  
Questions 265. You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a simple backup copy of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a simple backup copy will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?   
A. bit-stream copy  
B. robust copy  
C. full backup copy  
D. incremental backup copy  
Answer: A  
Explanation:    
  
Questions 266. E-mail logs contain which of the following information to help you in your investigation?   
A. contents of the e-mail message  
B. attachments sent with the e-mail message  
C. date and time the message was sent  
D. user account that was used to send the message  
E. unique message identifier  
Answer: A,B,C,D  
Explanation:    
  
Questions 267. What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?   
A. key escrow  
B. steganography  
C. rootkit  
D. offset  
Answer: B  
Explanation:    
  
Questions 268. Sectors in hard disks typically contain how many bytes?   
A. 256  
B. 512  
C. 1024  
D. 2048  
Answer: B  
Explanation:    
  
Questions 269. When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?   
A. 202  
B. 404  
C. 606  
D. 909  
Answer: B  
Explanation:    
  
Questions 270. When conducting computer forensic analysis, you must guard against \_\_\_\_\_\_\_\_\_ so that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.   
A. scope creep  
B. unauthorized expenses  
C. overzealous marketing  
D. hard drive failure  
Answer: A  
Explanation:

Questions 271. Which of the following is NOT a graphics file?   
A. Picture1.tga  
B. Picture2.bmp  
C. Picture3.nfo  
D. Picture4.psd  
Answer: C  
Explanation:    
  
Questions 272. You should make at least how many bit-stream copies of a suspect drive?   
A. 1  
B. 2  
C. 3  
D. 4  
Answer: B  
Explanation:    
  
Questions 273. From the following spam mail header, identify the host IP that sent this spam?   
From [jie02@netvigator.com](mailto:jie02@netvigator.com) [jie02@netvigator.com](mailto:jie02@netvigator.com) Tue Nov 27 17:27:11 2001   
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id   
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)   
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)   
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)   
Message-Id: >[200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk](mailto:200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk)   
From: "china hotel web"   
To: "Shlam"   
Subject: SHANGHAI (HILTON HOTEL) PACKAGE   
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0   
X-Priority: 3 X-MSMail-   
Priority: Normal   
Reply-To: "china hotel web"   
A. 137.189.96.52  
B. 203.218.39.50  
C. 203.218.39.20  
D. 8.12.1.0  
Answer: C  
Explanation:    
  
Questions 274. You are working as computer forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firms employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?   
A. inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned  
B. inform the owner that conducting an investigation without a policy is a violation of the 4th Amendment  
C. inform the owner that conducting an investigation without a policy is a violation of the employees expectation of privacy  
D. inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies  
Answer: C  
Explanation:    
  
Questions 275. In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?   
A. policy of separation  
B. chain of custody  
C. rules of evidence  
D. law of probability  
Answer: B  
Explanation:    
  
Questions 276. Why should you note all cable connections for a computer you want to seize as evidence?   
A. to know what cable connections existed  
B. to prepare for shutting down the computer  
C. to document the evidence  
D. to know what hardware existed  
Answer: A  
Explanation:    
  
Questions 277. When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?   
A. a write-blocker  
B. a protocol analyzer  
C. a firewall  
D. a disk editor  
Answer: A  
Explanation:    
  
Questions 278. You are working as a computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact local law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subjects computer. You inform the officer that you will not be able to comply with that request because doing so would:   
A. violate your contract  
B. cause network congestion  
C. make you an agent of law enforcement  
D. write information to the subjects hard drive  
Answer: C  
Explanation:    
  
Questions 279. The police believe that Mevin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions. They also suspect that he has been stealing, copying, and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?   
A. the USA Patriot Act  
B. the Good Samaritan Laws  
C. the Federal Rules of Evidence  
D. the Fourth Amendment  
Answer: D  
Explanation:    
  
Questions 280. Which part of the Windows Registry contains the user's password file?   
A. HKEY\_CURRENT\_USER  
B. HKEY\_USER  
C. HKEY\_LOCAL\_MACHINE  
D. HKEY\_CURRENT\_CONFIGURATION  
Answer: B  
Explanation:

Questions 281. When investigating a Windows system, it is important to view the contents of the "page" or "swap" file because:   
A. Windows stores all of the systems configuration information in this file  
B. this is the file that Windows uses to communicate directly with the Registry  
C. a large volume of data can exist within the swap file of which the computer user has no knowledge  
D. this is the file that Windows uses to store the history of the last 100 commands that were run from the command line  
Answer: C  
Explanation:    
  
Questions 282. You are a computer forensics investigator working with a local police department and you are called to assist in an investigation of threatening emails. The complainant has printed out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in order to track the emails back to the suspect.   
A. routing table  
B. firewall log  
C. configuration files  
D. email headers  
Answer: D  
Explanation:    
  
Questions 283. What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?   
A. a compressed file  
B. a data stream file  
C. an encrypted file  
D. a reserved file  
Answer: B  
Explanation:    
  
Questions 284. What happens when a file is deleted by a Microsoft operating system using the FAT file system?   
A. the file is erased and cannot be recovered  
B. the file is erased but can be recovered  
C. a copy of the file is stored and the original file is erased  
D. only the reference to the file is removed from the FAT  
Answer: D  
Explanation:    
  
Questions 285. Printing under a windows computer normally requires which one of the following files types to be created?   
A. EME  
B. MEM  
C. EMF  
D. CME  
Answer: C  
Explanation:    
  
Questions 286. The use of warning banners helps a company avoid litigation by overcoming an employees assumed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ when connecting to the companys intranet, network, or virtual private network (VPN) and will allow the companys investigators to monitor, search, and retrieve information stored within the network.   
A. right to work  
B. right of free speech  
C. right to Internet access  
D. right of privacy  
Answer: D  
Explanation:    
  
Questions 287. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.   
A. Network forensics  
B. Computer forensics  
C. Incident response  
D. Event reaction  
Answer: B  
Explanation:    
  
Questions 288. When investigating a potential e-mail crime, what is your first step in the investigation?   
A. Determine whether a crime was actually committed  
B. Recover the evidence  
C. Trace the IP address to its origin  
D. Write a report  
Answer: C  
Explanation:    
  
Questions 289. If you plan to startup a suspect's computer, you must modify the \_\_\_\_\_\_\_\_\_\_\_ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.   
A. Boot.sys  
B. Scandisk utility  
C. CMOS  
D. deltree command  
Answer: C  
Explanation:    
  
Questions 290. You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?   
A. strsearch  
B. grep  
C. dir  
D. grem  
Answer: B  
Explanation:

Questions 291. What file structure database would you expect to find on floppy disks?   
A. FAT12  
B. FAT16  
C. FAT32  
D. NTFS  
Answer: A  
Explanation:    
  
Questions 292. Volatile memory is one of the leading problems for forensics. Worms such as Code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?   
A. Use VMware to be able to capture the data in memory and examine it  
B. Give the operating system a minimal amount of memory, forcing it to use a swap file  
C. Create a separate partition of several hundred megabytes and place the swap file there  
D. Use intrusion forensic techniques to study memory resident infections  
Answer: C  
Explanation:    
  
Questions 293. Which of the following filesystem is used by Mac OS X?   
A. EFS  
B. HFS+  
C. EXT2  
D. NFS  
Answer: B  
Explanation:    
  
Questions 294. If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?   
A. True  
B. False  
Answer: A  
Explanation:    
  
Questions 295. Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?   
A. search warrant  
B. subpoena  
C. wire tap  
D. bench warrant  
Answer: A  
Explanation:    
  
Questions 296. When you carve an image, recovering the image depends on which of the following skills?   
A. recovering the image from a tape backup  
B. recognizing the pattern of the data content  
C. recognizing the pattern of the header content  
D. recognizing the pattern of a corrupt file  
Answer: C  
Explanation:    
  
Questions 297. You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacturer.     While at the corporate office of the company, the CEO demands to know the status of the investigation.     What prevents you from discussing the case with the CEO?   
A. the attorney-work-product rule  
B. Good manners  
C. Trade secrets  
D. ISO 17799  
Answer: A  
Explanation:    
  
Questions 298. This is the original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.   
A. Master Boot Record (MBR)  
B. Master File Table (MFT)  
C. File Allocation Table (FAT)  
D. Disk Operating System (DOS)  
Answer: C  
Explanation:    
  
Questions 299. Microsoft Outlook maintains email messages in a proprietary format in what type of file?   
A. .email  
B. .mail  
C. .pst  
D. .doc  
Answer: C  
Explanation:    
  
Questions 300. Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?   
A. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum  
B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file  
C. A simple DOS copy will not include deleted files, file slack and other information  
D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector  
Answer: C  
Explanation: