Guide to Computer Forensics and Investigations 7th edition Nelson Test Bank

SKU: 9780357672884-TEST-BANK

Name:_____ Class:_____ Date:_____

Mod 01: Understanding the Digital Forensics Profession and Investigations

1. Mahmood is examining a device for digital evidence. There are two types of evidence he is looking for. Which type of evidence will prove that his client is not guilty?

a. Inculpatory evidence
b. Exculpatory evidence
c. Miaculpatory evidence
d. Discretionary evidence

ANSWER: b

2. What are the main differences between public-sector investigations and private-sector investigations?

a. Private-sector investigations involve government agencies responsible for criminal investigations and prosecution. Public-sector investigations focus more on policy violations.
b. Private-sector investigations can become criminal investigations and public-sector investigations can become civil investigation depending upon the circumstances.
c. Public-sector investigations involve government agencies responsible for criminal investigations and prosecution. Private-sector investigations focus more on policy violations.
d. The private sector can ignore criminal investigations, and the public sector can ignore civil investigations.

ANSWER: b, c

3. When conducting a computer investigation for potential criminal violations of the law, the legal processes you follow depend on local customs, legislative standards, and rules of evidence. In general, however, a criminal case follows three stages. What are those three stages?

a. Complaint, the investigation, and the prosecution
b. Complaint, discovery, and the trial
c. Complaint, service of process, and motions
d. Complaint, answer, discovery, and trial

ANSWER: a

4. You're the head of the executive management committee and as part of your corporate governance duties you must implement a policy to define and limit who has authorization to request a computer investigation and forensics analysis (authorized requestor). Which group or groups should have the authority to request a computer investigation?

a. The human resources department
b. The corporate ethics office
c. The general counsel or legal department
d. The accounting department

ANSWER: b, c

5. Allen works for a small newspaper. There is no corporate security investigations group, no written or verbal acceptable use policy, and the publisher (owner) owns the rights to all the computer hardware and software. One day, the publisher calls him into the office and asks him to help them with an email problem. Upon fixing

the problem Allen discovers that there are illicit photos (no one was underage) on the publisher's laptop. The publisher later asks Allen to sanitize the laptop because the publisher wants to give it to their grandson. Allen must go through the laptop to find all the photos. What can Allen do to stop this work behavior?

a. Report the publisher to Human Resources
b. File a hostile work environment claim
c. Sanitize the laptop and do nothing else
d. Refuse to do the job

ANSWER: b

6. As head of Zenon's corporate IT department, Naya is tasked with analyzing the corporate mobile device policy. She needs to decide which is better, company owned mobile devices or BYOD? As a member of the corporate security team, Naya asks you for advice on which you think will be more appropriate. When you examine all options, which environment do you think works best for Zenon?

a. With company owned devices, it falls on the employee to keep them updated.
b. With company owned devices, all apps, files, and email can be secured.
c. With BYOD employees own the devices so companies are not liable if anything happens to the device.
d. With BYOD, the employee buys the device, and the company can lock it down (mobile device management).

ANSWER: b, d

7. Thanks to the dark web, anybody can access computer programs that will help users exfiltrate (remove) data from any type of computer or network. Because of this activity, white-collar crime and industrial espionage are on the rise. How does white-collar-crime compare to industrial espionage?

a. White-collar crime refers to financial crimes committed in a business or professional setting, while espionage refers to the unauthorized sharing of confidential information to a competitor or foreign entity.
b. Espionage refers to financial crimes committed in a business or professional setting, while white collar crime refers to the unauthorized sharing of confidential information to a competitor or foreign entity.
c. White-collar crime is the same as espionage and are both punishable offenses.
d. White-collar crime and espionage are victimless crimes.

ANSWER: a

8. Kwan is a Digital Evidence Specialist and is looking for a new job. He has an immaculate resume, fantastic references, and an excellent work history. But on the weekends, he likes to go out and get drunk, play beer pong, get high, and to post a lot of selfies to his social media sites. Recently, he applied to Jaffe Corporation for a Digital Evidence Specialist position. The interview went well. In fact, Jaffe is looking to hire him for a project, but upon further investigation, they decide not to. What might the deciding factor have been in Jaffe Corp. not hiring Kwan?

a. Kwan should put all his social media platform settings on private so no one can see his pictures.

b. Kwan can do whatever he wants. What he does with his own time should not affect him professionally.
c. Kwan's selfies of getting drunk and high show a critical lack of judgment. Those images could allow an opposing attorney to discredit him due to his behavior.
d. Kwan can control what pictures of him are put on the Internet.

ANSWER: c

9. Lucy needs to make a forensic initial assessment about a case she is investigating. What are some of the steps she needs to take for the assessment?

a. Has law enforcement apprehended a suspect?
b. Have law enforcement or company security officers already seized the computer, disks, peripherals, and other components?
c. Was a computer or a laptop found?
d. Is the president of the company available?

ANSWER: b

10. Carmon needs to determine what the preliminary approach to a case should be. What are some of the general steps she needs to follow to investigate the case?

a. Create a detailed check list, determine resources you need, obtain, and copy an evidence drive
b. Check fingerprint databases, search rainbow tables, speak with police personnel
c. Identify suspects, check the DMV, talk to crime scene investigators for evidence that might have been missed
d. Identify the risks, mitigate, or minimize the risks, test the design, investigate the data recovered

ANSWER: a, d

11. Joe has been tasked with investigating an incident at Zander Corp. What is the first rule he must follow that is important for all investigations, no matter how big or small?

a. Categorizing the evidence
b. Stabilizing the evidence
c. Preserve the evidence
d. Detain the evidence

ANSWER: c

12. Jennifer is about to take over a computer crime case at Amcore lab. Before she begins, must verify that the chain of custody has not been broken. She discovers that the seal on the container on the suspect's hard drive has been broken and there is no signature on the sign out sheet that someone took the hard drive for analysis. How does this affect the chain of custody?

a. It does nothing to the chain of custody.
b. It only affects authenticity.
c. It breaks the chain of custody.

d. The custody of the data's journey is now refutable but can still be admissible.

ANSWER: c

13. Akikta has been given a Windows 10 computer that needs to be investigated. Mostly, he will be recovering deleted files, and checking unallocated space on the hard drive. What are some software Akikta may want to use?

a. FTK Imager, X-Ways Forensics, and dd
b. EnCase, FTK, and Autopsy
c. Photorec and Scalpel
d. md5sum and sha256sum

ANSWER: b, c

14. Kailani is about to take possession of a Windows 2000 computer for forensic investigation. Why must Kailani use older forensic tools for this Windows 2000 computer?

a. Windows 2000 is too advanced
b. Windows 2000 is a legacy system
c. Windows 2000 is no longer used in production networks
d. Windows 2000 no longer works

ANSWER: b

15. Ethel is transporting a computer to her forensic lab, and she needs to secure the device before transport. What does Ethel need to do to ensure that the computer maintains chain of custody and arrives intact at her lab?

a. Put the entire tower or laptop in a Faraday box or bag
b. Transport the drives in separate vehicles from the tower or laptop
c. Place evidence tape over drive bays and insertion slots for power supply cords and USB cables
d. Place everything in her trunk and lock it so it can't be stolen

ANSWER: c, d

16. Ha-Yoon must do a risk assessment for a client. The client has an employee who does not know computers very well but has recently been taking classes on computer hacking. He has been spending more time on his computer and less time working. Recently their network has seen more traffic and attempted breaches than usual. There is no acceptable use policy in place. What should Ha-Yoon recommend first to mitigate the risk to the client's network?

a. Have the employer create an acceptable use policy and implement it.
b. Fire the employee
c. Remove the employee's computer
d. Replace the employee's computer, give them standard access, and isolate them from any network assets

ANSWER: a, d

Mod 01: Understanding the Digital Forensics Profession and Investigations

17. Haris is presented with a case by a client involving employee termination. He hasn't been told about the case yet, but he can guess. What are some of the predominate types of issues that occur in an employee termination case?

a. Working from home
b. Creating a hostile work environment
c. Playing games
d. Surfing the Internet

ANSWER: b

18. Fumiko will be conducting an investigation involving Internet abuse on a client's internal private network. What will he need to gather from his client's network administrator?

a. The suspect's computer IP address
b. The client's ISP IP address
c. The client's router IP address
d. The organization's Internet proxy server logs

ANSWER: a, d

19. During an investigation, Jerry discovers that there were no matches between the network server logs and the forensic examination showing no contributing evidence that a crime was committed. What does this mean for the investigation?

a. The allegations were unsubstantiated and there was no misconduct
b. The allegations were substantiated and there was misconduct
c. There were no allegations, just conjecture
d. It was all a misunderstanding

ANSWER: a

20. Quan-Van is working on a case that's attorney-client privilege (ACP). The attorney asks that all correspondence with them be verbal. What is the reason behind this request?

a. The attorney doesn't like to read
b. There will be too much paperwork
c. Anything written down is subject to discovery
d. Anything written down must be done in a very specific way

ANSWER: c

21. Olga is about to embark on her first overseas Internet abuse case. She knows the privacy laws of her state as she has worked on Internet abuse cases on a regular basis. The client she is working for is in Germany so she can easily perform the investigation the same way in Germany as she does in the United States.

a. True
b. False

ANSWER: b

22. Dakarai has many legacy operating systems on his forensic workstation as well as the newest OSs, but he has only the most up-to-date software on his day-to-day workstation. Why does Dakarai need legacy operating systems?

a. It's not taking up much space on his forensic station, so why bother?
b. It's cheaper to keep the older software around.
c. Dakarai hasn't gotten around to getting rid of the old software yet.
d. Older computer systems may not be compatible with modern software.

ANSWER: d

23. Rivka is building a forensic workstation and needs to buy some hardware to get started. What are some of the types of hardware she will need to buy?

a. A workstation running Windows 7
b. A write-blocker device, spare PATA and SATA ports
c. Network interface card (NIC)
d. Graphics card

ANSWER: b, c

24. Kevin is about to begin an examination of a hard drive. Out of all the tools available to him, which one is the most important to keep the OS from writing data to the hard drive?

a. SCSI card
b. Network interface card (NIC)
c. Write-blocker
d. Target drive

ANSWER: c

25. Gerald is using MS-DOS 6.22 to examine a legacy hard drive. Why would Gerald use such an old operating system?

a. Other DOS OSs are no longer available.
b. Other DOS OSs do not have the appropriate tools.
c. It's the only DOS OS that works with older digital forensic tools.
d. It is the only DOS OS that's least intrusive to disks.

ANSWER: d

26. Isabella is conducting an investigation for a client. She will need to copy evidence from a disk using multiple methods. Why can't she use just one method?

a. It's just for backup purposes.
b. No one media type can be trusted.
c. No single method retrieves all data from a disk.

d. Analyzing data is a tricky job.

ANSWER: c

27. Sammy needs to return to the office to retrieve some antistatic bags and wrist straps before handling digital evidence. Why are these items important for handling digital evidence?

a. Static electricity doesn't do anything to digital evidence. It's just a precaution.
b. Static electricity can hurt the user.
c. Static electricity can make your hair stand up.
d. Static electricity can destroy digital evidence.

ANSWER: d

28. Zoey is new to the field of computer forensics. Her boss has asked her to make a bit-stream copy of a disk drive for an investigation her company is working on. Zoey is curious why she can't make a backup copy instead. She comes to you for advice. What do you tell her?

a. A bit-stream copy is used because it is an exact duplicate of the original drive.
b. A backup copy has most of the files necessary; you just need to take extra steps.
c. A backup copy doesn't have deleted files and emails or recovered file fragments.
d. A bit-stream copy needs multiple forensic tools to get all the data off it.

ANSWER: a, c

29. Kenneth is creating a bit-stream image from a bit-stream copy of an evidence drive, but he's confused as to what the difference is. To Kenneth, there isn't much difference. Please help him out and tell him what makes a bit-stream image different from a bit-stream copy.

a. A bit-stream image and a bit-copy are identical.
b. A bit-stream image replicates the evidence drive but is not an exact copy.
c. There only has to be one bit-stream copy made when working on an image drive.
d. A bit-stream image creates an exact copy of the evidence disk down to the physical drive level.

ANSWER: d

30. Stella just finished writing a report for Tera Corp. and reviews her report one more time to check the steps she took to be sure her findings are repeatable. The problem is she used a new tool in her findings that has not been vetted by industry experts yet, so it may not adhere to industry standards. Why is this an issue?

a. New tools that are not vetted may not return repeatable data.
b. It doesn't change anything.
c. New tools are used all the time.
d. It's not important to repeat results.

ANSWER: a