Combined Review Questions

Network Technologies (Centennial College)

Chapter 1

Review Questions

1. Digital forensics and data recovery refer to the same activities. True or False?

   False

2. Police in the United States must use procedures that adhere to which of the following?

   b. Fourth Amendment

3. The triad of computing security includes which of the following?

   c. Vulnerability/threat assessment, intrusion detection and incident response, and digital investigation

4. What's the purpose of maintaining a network of digital forensics specialists?

   To develop a list of colleagues who specialize in areas different from your own specialties in case you need help on an investigation.

5. Policies can address rules for which of the following?

   d. Any of the above

6. List two items that should appear on a warning banner.

   Statements that the organization has the right to monitor what users do, that their e-mail is not personal, and so on

7. Under normal circumstances, a private-sector investigator is considered an agent of law enforcement. True or False?

   False

8. List two types of digital investigations typically conducted in a business environment.

   Fraud, embezzlement, insider trading, espionage, and e-mail harassment

9. What is professional conduct, and why is it important?

   Professional conduct includes ethics, morals, and standards of behavior. It affects a professional's credibility.

10. What's the purpose of an affidavit?

    To provide facts in support of evidence of a crime to submit to a judge when requesting a search warrant

11. What are the necessary components of a search warrant?

    A search warrant must specify who, what, when, and where—that is, specifics on place, time, items being searched for, and so forth—and include any supporting materials (affidavits and exhibits, for example). In addition, a search warrant must be signed by an impartial judicial officer. In many cases, a search warrant can limit the scope of what can be seized.

12. What are some ways to determine the resources needed for an investigation?

    Determine the OS of the suspect computer and list the software needed for the examination.

13. List three items that should be on an evidence custody form.

    Answers include case number, name of the investigator assigned to the case, nature of the case, location where evidence was obtained, description of the evidence, and so on.

14. Why should you do a standard risk assessment to prepare for an investigation?

    To list problems that might happen when conducting an investigation, which can help in planning your case

15. You should always prove the allegations made by the person who hired you. True or False?

    False

16. For digital evidence, an evidence bag is typically made of antistatic material. True or False?

    True

17. Why should evidence media be write-protected?

    To make sure data isn’t altered

18. List three items that should be in your case report.

    Answers can include an explanation of basic computer and network processes, a narrative of what steps you took, a description of your findings, and log files generated from your analysis tools.

19. Why should you critique your case after it’s finished?

    To improve your work

20. What do you call a list of people who have had physical possession of the evidence?

    Chain of custody

21. Data collected before an attorney issues a memo for an attorney-client privilege case is protected under the confidential work product rule. True or False?

    False. All data collected before an attorney issues notice of attorney-client privilege is subject to discovery by opposing counsel.

3 Solutions

Review Questions

1. What's the main goal of a static acquisition?

   Preservation of digital evidence

2. Name the three formats for digital forensics data acquisitions.

   Raw format, proprietary formats, and Advanced Forensic Format (AFF)

3. What are two advantages and disadvantages of the raw format?

   Advantages: faster data transfer speeds, ignores minor data errors, and most forensics analysis tools can read it. Disadvantages: requires equal or greater target disk space, doesn't contain hash values in the raw file (metadata), might have to run a separate hash program to validate raw format data, and might not collect marginal (bad) blocks.

4. List two features common with proprietary format acquisition files.

   Can compress or not compress the acquisition data; can segment acquisition output files into smaller volumes, allowing them to be archived to CD or DVD; case metadata can be added to the acquisition file, eliminating the need to keep track of any additional validation documentation or files

5. Of all the proprietary formats, which one is the unofficial standard?

   Expert Witness, used by Guidance Software EnCase

6. Name two commercial tools that can make a forensic sector-by-sector duplicate of a drive to a larger drive.

   EnCase and X-Ways Forensics

7. What does a logical acquisition collect for an investigation?

   only specific files of interest to the case

8. What does a sparse acquisition collect for an investigation?

   fragments of unallocated data in addition to the logical allocated data

9. What should you consider when determining which data acquisition method to use?

   Size of the source drive, whether the source drive is retained as evidence, how long the acquisition will take, and where the disk evidence is located

10. Why is it a good practice to make two images of a suspect drive in a critical investigation?

    To ensure at least one good copy of the forensically collected data in case of any failures

11. When you perform an acquisition at a remote location, what should you consider to prepare for this task?

    Determine whether there's enough electrical power and lighting, and check the temperature and humidity at the location.

12. With newer Linux kernel distributions, what happens if you connect a hot-swappable device, such a USB drive, containing evidence?

    Newer Linux distributions automatically mount the USB device, which could alter data on it.

13. In Linux, the `fdisk -l` command lists the suspect drive as `/dev/hda1`. Is the following `dcfldd` command correct?

```
dcfldd if=image_file.img of=/dev/hda1
```

    No. This command reads the `image_file.img` file and writes it to the evidence drive's `/dev/hda1` partition. The correct command is `dcfldd if=/dev/hda1 of=image_file.img`.

14. What's the most critical aspect of digital evidence?

    validation

15. What's a hashing algorithm?

    A program designed to create a binary or hexadecimal number that represents the uniqueness of a data set, file, or entire disk

16. In the Linux `dcfldd` command, which three options are used for validating data?

    `hash`, `hashlog`, and `vf`

17. What's the maximum file size when writing data to a FAT32 drive?

    2 GB (a limitation of FAT file systems)

18. What are two concerns when acquiring data from a RAID server?

    Amount of data storage needed, type of RAID server (0, 1, 5, and so on), whether the acquisition tool can handle RAID acquisitions, whether the analysis tool can handle RAID data, and whether the analysis tool can split RAID data into separate disk drives, making it easier to distribute large data sets

19. With remote acquisitions, what problems should you be aware of? (Choose all that apply.)

    a. Data transfer speeds

    b. Access permissions over the network

    c. Antivirus, antispyware, and firewall programs

20. Which forensics tools can connect to a suspect's remote computer and run surreptitiously?

    EnCase Enterprise and ProDiscover Incident Response

21. EnCase, FTK, SMART, and iLookIX treat the image file as though it were the original disk. True or False?

    True

22. FTK Imager can acquire data in a drive's host protected area. True or False?

    False

Chapter 4 Solutions

Review Questions

1. Private-sector investigations are typically easier than law enforcement investigations for which of the following reasons?

   a. Most companies keep inventory databases of all hardware and software used.

2. In the United States, if a company publishes a policy stating that it reserves the right to inspect computing assets at will, a private-sector investigator can conduct covert surveillance on an employee with little cause. True or False?

   True

3. If you discover a criminal act while investigating a company policy abuse, the case becomes a criminal investigation and should be referred to law enforcement. True or False?

   True

4. As a private-sector investigator, you can become an agent of law enforcement when which of the following happens? (Choose all that apply.)

   a. You begin to take orders from a police detective without a warrant or subpoena.

   b. Your internal investigation has concluded, and you have filed a criminal complaint and turned over the evidence to law enforcement.

5. The plain view doctrine in computer searches is well-established law. True or False?

   False

6. If a suspect's computer is found in an area that might have toxic chemicals, you must do which of the following? (Choose all that apply.)

   a. Coordinate with the HAZMAT team.

   c. Assume the suspect's computer is contaminated.

7. What are the three rules for a forensic hash?

   It can't be predicted, no two files can have the same hash value, and if the file changes, the hash value changes.

8. In forensic hashes, when does a collision occur?

   When two different files have the same hash value

9. List three items that should be in an initial-response field kit.

   Answers can include small computer toolkit, large-capacity drive, IDE ribbon cables, forensic boot media, laptop IDE 40-to-44 pin adapter, laptop or portable computer, FireWire or USB dual write-protect external bay, flashlight, digital camera or 35mm camera, evidence log forms, notebook or dictation recorder, evidence bags (antistatic bags for digital devices), evidence labels, tape, tags, permanent ink marker, USB drives, or large portable hard drive

10. When you arrive at the scene, why should you extract only those items you need to acquire evidence?

    To minimize how much you have to keep track of at the scene

11. Computer peripherals or attachments can contain DNA evidence. True or False?

    True

12. If a suspect computer is running Windows 10, which of the following can you perform safely?

    a. Browsing open applications

13. Describe what should be videotaped or sketched at a digital crime scene.

    Computers, mobile devices, cable connections, overview of scene—anything that might be of interest to the investigation

14. Which of the following techniques might be used in covert surveillance? (Choose all that apply.)

    a. Keylogging

    b. Data sniffing

15. Commingling evidence means what in a private-sector setting?

    Sensitive or confidential information being mixed with data collected as evidence

16. List two hashing algorithms commonly used for forensics purposes.

    MD5 and SHA-1

17. Small companies rarely need investigators. True or False?

    False

18. If a company doesn't distribute a computing use policy stating an employer's right to inspect employees' computers freely, including e-mail and Web use, employees have an expectation of privacy. True or False?

    True

19. You have been called to the scene of a fatal car crash where a laptop computer is still running. What type of field kit should you take with you?

    Initial-response field kit

20. You should always answer questions from onlookers at a crime scene. True or False?

    False

Chapter 5 Solutions

Review Questions

1. On a Windows system, sectors typically contain how many bytes?

   b. 512

2. What does CHS stand for?

   cylinders, heads, sectors

3. Zone bit recording is how manufacturers ensure that the outer tracks store as much data as possible. True or False?

   False

4. Areal density refers to which of the following?

   c. Number of bits per square inch of a disk platter

5. Clusters in Windows always begin numbering at what number?

   2

6. How many sectors are typically in a cluster on a disk drive?

   c. 4 or more

7. List three items stored in the FAT database.

   Answers can include file and directory names, starting cluster numbers, file attributes, and date and time stamps.

8. What does the `Ntuser.dat` file contain?

   This user-protected storage area contains the MRU files list and desktop configuration settings.

9. In FAT32, a 123 KB file uses how many sectors?

   The answer is 246 sectors. 123 x 1024 bytes per KB = 125,952 total bytes in the file. 125,952 bytes / 512 sectors per cluster = 246 sectors

10. What is the space on a drive called when a file is deleted? (Choose all that apply.)

    b. Unallocated space

    d. Free space

11. List two features NTFS has that FAT does not.

    Answers can include Unicode characters, security, and journaling.

12. What does MFT stand for?

    Master File Table

13. In NTFS, files smaller than 512 bytes are stored in the MFT. True or False?

    True

14. In Windows 7 and later, how much data from RAM is loaded into RAM slack on a disk drive?

    No data from RAM is copied to RAM slack on a disk drive.

15. What's a virtual cluster number?

It represents the assigned clusters of files that are nonresident in the MFT. If a file has become fragmented, it can have two or more VCNs. The first VCN for a nonresident file is listed as 0.

16. Why was EFI boot firmware developed?

    To provide better protection against malware than BIOS does

17. Device drivers contain what kind of information?

    Instructions for the OS on how to interface with hardware devices

18. Which of the following Windows 8 files contains user-specific information?

    b. `Ntuser.dat`

19. Virtual machines have which of the following limitations when running on a host computer?

    c. Virtual machines are limited to the host computer's peripheral configurations, such as mouse, keyboard, CD/DVD drives, and other devices.

20. An image of a suspect drive can be loaded on a virtual machine. True or False?

    True

21. EFS can encrypt which of the following?

    a. Files, folders, and volumes

22. What happens when you copy an encrypted file from an EFS-enabled NTFS disk to a non-EFS disk or folder?

    c. The file is unencrypted automatically.

23. What are the functions of a data run's field components in an MFT record?

    Data runs have three components; the first declares how many bytes are required in the attribute field to store the number of bytes needed for the second and third components. The second component stores the number of clusters assigned to the data run, and the third component contains the starting cluster address value (the LCN or the VCN).

Chapter 6 Solutions

Review Questions

1. Forensics software tools are grouped into _________ and _______________ applications.

   GUI, command-line

2. According to ISO standard 27037, which of the following is an important factor in data acquisition? (Choose all that apply.)

   a. The DEFR's competency

   c. Use of validated tools

3. An encrypted drive is one reason to choose a logical acquisition. True or False?

   True

4. Hashing, filtering, and file header analysis make up which function of computer forensics tools?

   a. Validation and verification

5. Hardware acquisition tools typically have built-in software for data analysis. True or False?

   False; most are used only for acquisition.

6. The reconstruction function is needed for which of the following purposes? (Choose all that apply.)

   a. Re-create a suspect drive to show what happened.

   b. Create a copy of a drive for other investigators.

   d. Re-create a drive compromised by malware.

7. List three subfunctions of the extraction function.

   Answers can include data viewing, keyword searching, decompressing, carving, decrypting, and bookmarking.

8. Data can't be written to disk with a command-line tool. True or False?

   False

9. Hash values are used for which of the following purposes? (Choose all that apply.)

   b. Filtering known good files from potentially suspicious data

d. Validating that the original data hasn't changed

10. In testing tools, the term "reproducible results" means that if you work in the same lab on the same machine, you generate the same results. True or False?

    False

11. The verification function does which of the following?

    c. Proves that two sets of data are identical via hash values

12. What's the advantage of a write-blocking device that connects to a computer through a FireWire or USB controller?

    It enables you to remove and reconnect drives without having to shut down your workstation, which saves time in processing the evidence drive.

13. Building a forensic workstation is more expensive than purchasing one. True or False?

    False

14. A live acquisition can be replicated. True or False?

    False

15. Which of the following is true of most drive-imaging tools? (Choose all that apply.)

    b. They ensure that the original drive doesn't become corrupt and damage the digital evidence.

    c. They create a copy of the original drive.

16. The standards for testing forensics tools are based on which criteria?

    c. ISO 17025

17. A log report in forensics tools does which of the following?

    c. Records an investigator's actions in examining a case

18. When validating the results of a forensics analysis, you should do which of the following? (Choose all that apply.)

    a. Calculate the hash value with two different tools.

    b. Use a different tool to compare the results of evidence you find.

19. The primary hashing algorithm the NSRL project uses is SHA-1. True or False?

    True

Chapter 7 Solutions

Review Questions

1. Explain the differences in resource and data forks used in macOS.

   Both contain a file's resource map and header information, window locations, and icons. The data fork stores a file's actual data, however, and the resource fork contains file metadata and application information.

2. Which of the following is the main challenge in acquiring an image of a system running macOS? (Choose all that apply.)

   b. Vendor training is needed.

   d. You need special tools to remove drives from a system running macOS or open its case.

3. To recover a password in macOS, which tool do you use?

   c. Keychain Access

4. What are the major improvements in the Linux Ext4 file system?

   It added support for partitions larger than 16 TB, improved management of large files, and offered a more flexible approach to adding file system features.

5. How does macOS reduce file fragmentation?

   By using clumps, which are groups of contiguous allocation blocks

6. Linux is the only OS that has a kernel. True or False?

   False

7. Hard links work in only one partition or volume. True or False?

   True

8. Which of the following Linux system files contains hashed passwords for the local system?

   d. `/etc/shadow`

9. Which of the following describes the superblock's function in the Linux file system? (Choose all that apply.)

   b. Specifies the disk geometry and available space

   c. Manages the file system, including configuration information

10. What's the Disk Arbitration feature used for in macOS?

    It's used to disable and enable automatic mounting when a drive is connected via a USB or FireWire device.

11. In Linux, which of the following is the home directory for the superuser?

    b. `root`

12. Which of the following certifies when an OS meets UNIX requirements?

    c. The Open Group

13. On most Linux systems, current user login information is in which of the following locations?

d. `/var/log/utmp`

14. Hard links are associated with which of the following?

    b. A specific inode

15. Which of the following describes plist files? (Choose all that apply.)

    a. You must have a special editor to view them.

    c. They're preference files for applications.

16. Data blocks contain actual files and directories and are linked directly to inodes. True or False?

    True

17. Which of the following is a new file added in macOS? (Choose all that apply.)

    c. `/var/db/diagnostics`

    d. `/var/db/uuid.text`

Chapter 8 Solutions

Review Questions

1. Graphics files stored on a computer can't be recovered after they are deleted. True or False?

   False

2. When you carve a graphics file, recovering the image depends on which of the following skills?

   c. Recognizing the pattern of the file header content

3. Explain how to identify an unknown graphics file format that your digital forensics tool doesn't recognize.

   You need to examine a copy of the unknown file with a hexadecimal editor to find the hex code for the first several bytes of the file. Then you need to examine other known file types with similar or identical header values to see whether you can confirm its file type.

4. What type of compression uses an algorithm that allows viewing the graphics file without losing any portion of the data?

   lossless

5. When investigating graphics files, you should convert them into one standard format. True or False?

   False

6. Digital pictures use data compression to accomplish which of the following goals? (Choose all that apply.)

   a. Save space on a hard drive.

   d. Produce a file that can be e-mailed or posted on the Internet.

7. The process of converting raw images to another format is called which of the following?

   d. Demosaicing

8. In JPEG files, what's the starting offset position for the JFIF label?

   c. Offset 6

9. Each type of graphics file has a unique header containing information that distinguishes it from other types of graphics files. True or False?

   True

10. Copyright laws don't apply to Web sites. True or False?

    False

11. When viewing a file header, you need to include hexadecimal information to view the image. True or False?

    True

12. When recovering a file with ProDiscover, your first objective is to recover cluster values. True or False?

    True

13. Bitmap (`.bmp`) files use which of the following types of compression?

    d. Lossless

14. A JPEG file uses which type of compression?

    b. Lossy

15. Only one file format can compress graphics files. True or False?

    False

16. A JPEG file is an example of a vector graphic. True or False?

    False

17. Which of the following is true about JPEG and TIF files?

    b. They have different values for the first 2 bytes of their file headers.

18. What methods do steganography programs use to hide data in graphics files? (Choose all that apply.)

    a. Insertion

    b. Substitution

19. Some clues left on a drive that might indicate steganography include which of the following? (Choose all that apply.)

    a. Multiple copies of a graphics file

    b. Graphics files with the same name but different file sizes

    c. Steganography programs in the suspect's All Programs list

20. What methods are used for digital watermarking?

    b. Invisible modification of the LSBs in the file

    c. Layering visible symbols on top of the image

Chapter 9 Solutions

Review Questions

1. Which of the following represents known files you can eliminate from an investigation? (Choose all that apply.)

   b. Files associated with an application

   c. System files the OS uses

2. For which of the following reasons should you wipe a target drive?

   d. Both a and b

3. The Known File Filter (KFF) can be used for which of the following purposes? (Choose all that apply.)

   a. Filter known program files from view.

   c. Compare hash values of known files to evidence files.

4. Password recovery is included in all forensics tools. True or False?

   False

5. After you shift a file's bits, the hash value remains the same. True or False?

   False

6. Which forensic image file format creates or incorporates a validation hash value in the image file? (Choose all that apply)

   a. Expert Witness

   b. SMART

   c. AFF

7. ____________________ happens when an investigation goes beyond the bounds of its original description.

   Scope creep

8. Suppose you're investigating an e-mail harassment case. Generally, is collecting evidence for this type of case easier for an internal corporate investigation or a criminal investigation?

   c. Internal corporate investigation because corporate investigators typically have ready access to company records

9. You're using Disk Management to view primary and extended partitions on a suspect's drive. The program reports the extended partition's total size as larger than the sum of the sizes of logical partitions in this extended partition. What might you infer from this information?

   b. There's a hidden partition.

10. Commercial encryption programs often rely on ______________________ technology to recover files if a password or passphrase is lost.

    key escrow

11. Steganography is used for which of the following purposes?

    b. Hiding data

12. The National Software Reference Library provides what type of resource for digital forensics examiners?

    b. A list of MD5 and SHA1 hash values for all known OSs and applications

13. In steganalysis, cover-media is which of the following?

    c. The file a steganography tool uses to host a hidden message, such as a JPEG or an MP3 file

14. Rainbow tables serve what purpose for digital forensics examinations?

    a. Rainbow tables contain computed hashes of possible passwords that some password-recovery programs can use to crack passwords.

15. The likelihood that a brute-force attack can succeed in cracking a password depends heavily on the password length. True or False?

    True

16. If an application uses salting when creating passwords, what concerns should a forensics examiner have when attempting to recover passwords?

    b. Salting can make password recovery extremely difficult and time consuming.

17. Block-wise sector analysis has which of the following benefits for forensics examiners?

    d. Provides a method for hashing sectors of a known good file that can be used to search for data remnants on a suspect’s drive

Chapter 10 Solutions

Review Questions

1. Virtual Machine Extensions (VMX) are part of which of the following?

   c. Intel Virtualized Technology

2. You can expect to find a type 2 hypervisor on what type of device? (Choose all that apply.)

   a. Desktop

   b. Smartphone

   c. Tablet

3. Which of the following file extensions are associated with VMware virtual machines?

   a. `.vmx`, `.log`, and `.nvram`

4. In VirtualBox, a(n) ____________________ file contains settings for virtual hard drives.

   c. `.vbox`

5. The number of VMs that can be supported per host by a type 1 hypervisor is generally determined by the amount of __________ and ______________.

   RAM, storage

6. A forensic image of a VM includes all snapshots. True or False?

   False

7. Which Registry key contains associations for file extensions?

   b. HKEY_CLASSES_ROOT

8. Which of the following is a clue that a virtual machine has been installed on a host system?

   b. Virtual network adapter

9. To find network adapters, you use the ________ command in Windows and the _______________ command in Linux.

   `ipconfig`, `ifconfig`

10. What are the three modes of protection in the DiD strategy?

    People, technology, operations

11. A layered network defense strategy puts the most valuable data where?

    c. In the innermost layer

12. `Tcpslice` can be used to retrieve specific timeframes of packet captures. True or False?

    True

13. Packet analyzers examine what layers of the OSI model?

    c. Layers 2 and 3

14. When do zero day attacks occur? (Choose all that apply.)

    b. Before a patch is available

    c. Before the vendor is aware of the vulnerability

Chapter 11 Solutions

Review Questions

1. E-mail headers contain which of the following information? (Choose all that apply.)

   a. The sender and receiver e-mail addresses

   b. An ESMTP number or reference number

   c. The e-mail servers the message traveled through to reach its destination

2. What's the main piece of information you look for in an e-mail message you're investigating?

   b. Originating e-mail domain or IP address

3. In Microsoft Outlook, e-mails are typically stored in which of the following?

   a. `.pst` and `.ost` files

4. When searching a victim's computer for a crime committed with a specific e-mail, which of the following provides information for determining the e-mail's originator? (Choose all that apply.)

   a. E-mail header

   c. Firewall log

5. Phishing does which of the following?

   b. Lures users with false promises

6. Which of the following is a current formatting standard for e-mail?

   b. MIME

7. After examining e-mail headers to find an e-mail's originating address, investigators use forward lookups to track an e-mail to a suspect. True or False?

   True

8. When you access your e-mail, what type of computer architecture are you using?

   c. Client/server

9. To trace an IP address in an e-mail header, what type of lookup service can you use? (Choose all that apply.)

   c. A domain lookup service, such as *www.arin.net*, *www.internic.com*, or *www.whois.net*

   d. Any Web search engine

10. Router logs can be use for validating what types of e-mail data?

    c. Tracking flows through e-mail server ports

11. Logging options on e-mail servers can be which of the following? (Choose all that apply.)

    b. Set up in a circular logging configuration

    c. Configured to a specified size before being overwritten

12. On a UNIX-like system, which file specifies where to save different types of e-mail log files?

c. `syslog.conf`

13. What information is *not* in an e-mail header? (Choose all that apply.)

    a. Blind copy (bcc) addresses

    d. Contents of the message

14. Which of the following types of files can provide useful information when you're examining an e-mail server?

    c. `.log` files

15. E-mail accessed with a Web browser leaves files in temporary folders. True or False?

    True

16. When confronted with an e-mail server that no longer contains a log with the date information you require for your investigation, and the client has deleted the e-mail, what should you do?

    b. Restore the e-mail server from a backup.

17. You can view e-mail headers in Notepad with all popular e-mail clients. True or False?

    False

18. To analyze e-mail evidence, an investigator must be knowledgeable about an e-mail server's internal operations. True or False?

    True

19. Sendmail uses which file for instructions on processing an e-mail message?

    a. `Sendmail.cf`

20. A forensic linguist can determine an author's gender by analyzing chat logs and social media communications. True or False?

    False

Chapter 12 Solutions

Review Questions

1. List four places where mobile device information might be stored.

   internal memory, SIM card, external/removable memory cards, the network provider

2. Typically, you need a search warrant to retrieve information from a service provider. True or False?

   True

3. The term TDMA refers to which of the following? (Choose all that apply.)

   a. A technique of dividing a radio frequency so that multiple users share the same channel

   c. A specific cellular network standard

4. What's the most commonly used cellular network worldwide?

   GSM

5. Which of the following relies on a central database that tracks account data, location data, and subscriber information?

   b. MSC

6. GSM divides a mobile station into ______________ and __________________.

   SIM card and ME (mobile equipment)

7. SD cards have a capacity of up to which of the following?

   c. 64 GB

8. Describe two ways you can isolate a mobile device from incoming signals.

   Answers can include placing the device in airplane mode, placing it in paint cans, using Faraday bags, and turning the device off.

9. Which of the following categories of information is stored on a SIM card? (Choose all that apply.)

   b. Call data

   c. Service-related data

10. Most SIM cards allow ___________ access attempts before locking you out.

    three

11. SIM card readers can alter evidence by showing that a message has been read when you view it. True or False?

    True

12. The uRLLC 5G category focuses on communications in smart cities. True or False?

    False

13. When acquiring a mobile device at an investigation scene, you should leave it connected to a laptop or tablet so that you can observe synchronization as it takes place. True or False?

    False

14. Remote wiping of a mobile device can result in which of the following? (Choose all that apply.)

    a. Removing account information

    c. Returning the phone to the original factory settings

    d. Deleting contacts

15. In which of the following cases did the U.S. Supreme Court require using a search warrant to examine the contents of mobile devices?

    c. *Riley v. California*

16. The Internet of Things includes ________________ as well as wired, wireless, and mobile devices.

    radio frequency identification (RFID) sensors

17. Which of the following is a mobile forensics method listed in NIST guidelines? (Choose all that apply.)

    a. Logical extraction

    c. Physical extraction

    d. Hex dumping

18. According to SANS DFIR Forensics, which of the following tasks should you perform if a mobile device is on and unlocked? (Choose all that apply.)

    a. Isolate the device from the network.

    b. Disable the screen lock.

    c. Remove the passcode.

19. Which organization is setting standards for 5G devices?

    International Mobile Telecommunications working group

Chapter 13 Solutions

Review Questions

1. Amazon was an early provider of Web-based services that eventually developed into the cloud concept. True or False?

   True

2. What are the three levels of cloud services defined by NIST?

   c. SaaS, PaaS, and IaaS

3. What capabilities should a forensics tool have to acquire data from a cloud? (Choose all that apply.)

   a. Identify and acquire data from the cloud.

   b. Expand and contract data storage capabilities as needed for service changes.

   d. Examine virtual systems.

4. Commingled data isn't a concern when acquiring cloud data. True or False?

   False

5. A(n) ________________________ is a contract between a CSP and the customer that describes what services are being provided and at what level.

   CSA or cloud service agreement

6. Which of the following is a mechanism the ECPA describes for the government to get electronic information from a provider? (Choose all that apply.)

   a. Subpoenas with prior notice

   c. Search warrants

   d. Court orders

7. In which cloud service level can customers rent hardware and install whatever OSs and applications they need?

   IaaS or infrastructure as a service

8. What are the two states of encrypted data in a secure cloud?

   d. Data in motion and data at rest

9. Evidence of cloud access found on a smartphone usually means which cloud service level was in use?

   d. SaaS

10. Which of the following cloud deployment methods typically offers no security?

    b. Public cloud

11. The multitenancy nature of cloud environments means conflicts in privacy laws can occur. True or False?

    True

12. To see Google Drive synchronization files, you need a SQL viewer. True or False?

    True

13. A CSP's incident response team typically consists of which staff? List at least three positions.

system administrators, network administrators, and legal advisors

14. The cloud services Dropbox, Google Drive, and OneDrive have Registry entries. True or False?

    True

15. When should a temporary restraining order be requested for cloud environments?

    d. When a search warrant requires seizing a CSP's hardware and software used by other parties not involved in the case

16. Updates to the EU Data Protection Rules will affect how data is moved regardless of location. True or False?

    True

17. NIST document SP 500-322 defines more than 75 cloud services, including which of the following? (Choose all that apply.)

    a. Backup as a service

    b. Security as a service

    c. Drupal as a service

18. Public cloud services such as Dropbox and OneDrive use what encryption applications?

    Sophos Safeguard and Sophos Mobile Control

Chapter 14 Solutions

Review Questions

1. Which of the following rules or laws requires an expert to prepare and submit a report?

   a. FRCP 26

2. For what purpose have hypothetical questions traditionally been used in litigation?

   a. To frame the factual context of rendering an expert witness's opinion

3. If you were a lay witness at a previous trial, you shouldn't list that case in your written report. True or False?

   True

4. Which of the following is an example of a written report?

   b. An affidavit

5. What is destroying a report before the final resolution of a case called?

   spoliation

6. An expert witness can give an opinion in which of the following situations?

   d. All of the above

7. Which of the following is the standard format for reports filed electronically in U.S. federal courts and most state courts?

   c. PDF

8. When writing a report, what's the most important aspect of formatting?

   d. Consistency

9. Automated tools help you collect and report evidence, but you're responsible for doing which of the following?

   b. Explaining the significance of the evidence

10. What can be included in report appendixes?

    Answers can include additional resource material not included in the text, raw data, figures not used in the body of the report, and anticipated exhibits.

11. Which of the following statements about the legal-sequential numbering system in report writing is true?

    c. It doesn't indicate the relative importance of information.

12. What's a major advantage of automated forensics tools in report writing?

    You can incorporate the log files and reports these tools generate into your written reports. Generally, these generated files are in a format that's easy to incorporate into an electronic document.