Study Questions from Saferstein 4e Chapters 18 and 19

1) Which of the following is *not* considered a hardware device?
A) Monitor
B) Hard disk drive
C) Mouse
D) Operating system

2) Which of the following is *not* considered a type of software?
A) Linux
B) Firefox
C) Excel
D) Random-access memory

3) What is the primary form of data storage within a personal computer?
A) CD-ROM
B) Hard disk drive
C) Zip drive
D) Recycle bin

4) A network interface card (NIC) enables a personal computer to communicate with other computers via what type of connection?
A) Wired
B) Wireless
C) Satellite
D) Both A and B

5) What is the first thing a crime-scene investigator should do when encountering computer forensic evidence?
A) Unplug every device from the central processing unit to preserve the hard disk drive
B) Procure a warrant to search
C) Remove the system to the laboratory for processing
D) Document the scene

6) What is the ultimate goal of obtaining an image of a hard disk drive?
A) To locate as much incriminating information as possible
B) To preserve the photographs and video stored on the drive
C) To give priority to the text files on the drive
D) To obtain information without altering the drive in any way

7) What is one of the most common places to begin searching for evidential data?
A) Spreadsheet files
B) A photograph-editing program
C) A CAD package
D) Word-processing or text-based document files

8) Which of the following is the best definition of latent data?
A) Anything readily available to the user, also known as visible data
B) Those data that are hidden from view
C) An automatically saved copy of a file that was recently modified
D) Those data that are typically of little use to forensic investigators

9) Once a file is deleted by a user, it:
A) is obliterated from the system and cannot be recovered.
B) is retained until the disk space it occupies is allocated for another use.
C) may be identified using forensic image acquisition software.
D) both B and C.

10) Evidentiary data may be recovered from which of the following?
A) Slack space on the HDD
B) Unallocated space on the HDD
C) RAM swap files
D) All of the above

11) One gigabyte equals what?
A) 1,000 bytes
B) 1,000 megabytes (MB)
C) 1,000 kilobytes (KB)
D) 8,000 bits

12) Which of the following is *not* associated with the partitioning of an HDD?
A) Quadrant
B) Sector
C) Track
D) Cluster

13) When is it necessary to make a "fingerprint" of an HDD?
A) In most cases
B) Only sometimes
C) Before and after imaging its contents
D) Rarely

14) The boot (i.e., start-up) process for a computer is controlled by what?
A) Hard disc drive
B) ROM
C) RAM
D) USB thumb drives

15) Sectors are typically how many bytes in size?
A) 126
B) 256
C) 512
D) 1,024

16) Where should one *not* search for "visible" data?
A) Swap files
B) Temporary files
C) Unallocated space
D) Windows

17) Where should one *not* look for "latent" data?
A) RAM slack
B) File slack
C) Unallocated space
D) Temporary files

18) Hard drive partitions are typically divided into which of the following?
A) Sectors
B) Clusters
C) Tracks
D) All of the above

19) What do most web browsers use to expedite and streamline browsing?
A) Area network
B) Cable modem
C) Domain
D) Caching system

20) Unauthorized intrusion into a computer is called what?
A) Crashing
B) Whacking
C) Hacking
D) Spamming

21) Which of the following will *not* be useful to investigators seeking to determine a user's Internet history?
A) Cookies
B) Cache
C) Favorite sites
D) Slack files

22) Where are files containing chat and instant messaging most likely stored?
A) Swab files
B) RAM
C) ROM
D) Slack files

23) Which of the following carries data from one hardware device to another?
A) System bus
B) Central processing unit (CPU)
C) Random-access memory (RAM)
D) Network interface card (NIC)

24) In which of the following places would a computer forensic investigator look for latent data?
A) RAM slack
B) File slack
C) Unallocated space
D) All of the above

25) What is the best way to initially handle a mobile device to preserve data?
A) Turn the mobile device off.
B) Leave the mobile device on.
C) Leave the mobile device on, but place it in a Faraday shield.
D) None of the above

26) Which of the following is *not* a type of RAM?
A) SSIM
B) DDIM
C) SD
D) DAB

27) If a file system defines a cluster as six sectors, how many bytes of information can be stored on each cluster?
A) 24,576
B) 512
C) 3,072
D) 307.2

28) Which of the following actions taken at the crime scene that involves a computer are incorrect?
A) On arrival, sketching the overall layout as well as photographing it
B) Photographing any running monitors
C) Removing the plug from the back of the computer, not from the wall
D) None of the above

29) The two types of slack space are _____ slack and _____ slack.
A) file; RAM
B) RAM; ROM
C) cluster; file
D) IP; TTI

30) What is placed on a hard disk drive by a website to track certain information about its visitors?
A) Phish
B) IP address
C) E-mail
D) Cookie

31) A device that permits only requested traffic to enter a computer system is known as what?
A) Central processing unit (CPU)
B) Firewall
C) Cookie
D) Internet cache

32) All data readily available to a computer user is known as what?
A) Swap data
B) Latent data
C) Visible data
D) Allocated data

33) What is the complex network of wires that carry data from one hardware device to another called?
A) Motherboard
B) Central processing unit (CPU)
C) Hard disk drive
D) Operating system

34) 2G consists of:
A) analog networks.
B) digital networks.
C) broadband networks.
D) native IP networks.

35) 4G consists of:
A) analog networks.
B) digital networks.
C) broadband networks.
D) native IP networks.

36) In 2001, mobile Broadband networks (3G) arrived on the scene in what country?
A) North Korea

B) China
C) Japan
D) India

37) The Smartphone was developed under the following technology:
A) digital networks.
B) broadband networks.
C) native IP networks.
D) analog networks.

38) What type of network devices started using operating systems?
A) 1G
B) 2G
C) 3G
D) 4G

39) Feature phones have divergent (based upon the phone) feature sets. These core features usually were:
A) phone and text.
B) e-mail and camera.
C) applications and media.
D) both A and B.

40) Working on what type of surface increases the danger of static electricity?
A) Metal tables
B) Hardwood floors
C) Carpet
D) Lab desk

41) It may not be possible to recover deleted file items from a mobile device such as:
A) e-mails.
B) text messages.
C) photographs.
D) all of the above.

42) There are how many types of chains of evidence?
A) 1
B) 2
C) 4
D) 5

43) What would an investigator do the SIM card to retain a perfect copy for evidentiary purposes?
A) Take a picture
B) Upload to a PC
C) Clone the SIM
D) Properly store in evidence

44) What does the ICCID contain?
A) IIN (issuer identification number)
B) UPC (universal purchase code number)
C) PID (phone identification number)
D) IP address

45) Because a mobile device is similar to a computer and transmits wireless signals, what laws does an investigator need to follow?
A) Radio laws
B) First Amendment rights
C) Computer laws
D) Both A and C

46) What feature on a mobile device can help an investigator establish a timeline?
A) GPS
B) NFC
C) Android Beam
D) Bluetooth