قائمة الاسئلة

التحقيق الجنائي بإستخدام الحاسوب -المستوى الرابع -تكنولوجيا المعلومات - الكل - كلية الحاسوب وتكنولوجيا المعلومات - درجة الامتحان (224)

د.عبدالله المختار

1) Data acquisition is the process of_____?
   1) + A. Copying data.
   2) - B. Transform data.
   3) - C. Deleting data.
   4) - D. Analyzing data.
2) . Collecting data from magnetic disk media and flash drives _____?
   1) - A. Digital acquisitions.
   2) + B. Static acquisitions.
   3) - C. Live acquisitions.
   4) - D. None of the above.
3) . Collecting any data that's active in a suspect's computer RAM _____?
   1) - A. Static acquisitions.
   2) - B. Digital acquisitions.
   3) + C. Live acquisitions.
   4) - D. None of the above.
4) data acquisition method used when a suspect drive is write-protected and can't be altered.
   1) + A. Static acquisitions.
   2) - B. Digital acquisitions.
   3) - C. A and B.
   4) - D. None of the above.
5) A data acquisition method used when a suspect computer can't be shut down to perform a static acquisition.
   1) - A. Digital acquisitions.
   2) - B. A and C.
   3) + C. Live acquisitions.
   4) - D. None of the above.
6) Data in a forensics acquisition tool is stored as an.
   1) - A. Bit-stream copy.
   2) + B. Image file.
   3) - C. Forensic copy.
   4) - D. Binary file.
7) Storage formats for digital evidence
   1) - A. Raw format.
   2) - B. AFF.
   3) - C. Proprietary formats.
   4) + D. All the above.
8) . A copy technique that creates simple sequential flat files of a suspect drive or data set is a.
   1) + A. Raw format.
   2) - B. Proprietary formats
   3) - C. AFF.
   4) - D. All the above.
9) The output of flat files is referred to as a.
   1) - A. Structured format.
   2) - B. Encrypted format.
   3) + C. Raw format.
   4) - D. Compressed format.

10) One of these is not an advantage of Raw format.
1) - A. Fast data transfers.
2) - B. Ignores minor data read errors on source drive.
3) + C. Can integrate metadata into the image file.
4) - D. Most computer forensics tools can read raw format.

11) . Most forensics tools have _____ formats.
1) - A. Same
2) + B. Their own.
3) - C. Different
4) - D. Standardized

12) Can split an image into smaller segmented files what is format do this?
1) + A. Proprietary formats.
2) - B. Raw format.
3) - C. AFF
4) - D. All the above.

13) One of these isn't design goals of Advanced Forensics Format (AFF).
1) - A. Simple design with extensibility.
2) + B. Provide only uncompressed image files.
3) - C. Open source for multiple platforms and Oss.
4) - D. None of the above.

14) . In Advanced Forensics Format (AFF) the file extensions that is used for segmented image is
1) - A. .afm.
2) + B. .afd.
3) - C. .aff.
4) - D. .afp.

15) In Advanced Forensics Format (AFF) the file extensions that is used for metadata is
1) + A. .afm.
2) - B. .afd.
3) - C. .aff.
4) - D. .afp.

16) Types of acquisitions
1) - A. Static acquisitions.
2) - B. live acquisitions.
3) + C. A and B.
4) - D. Not one of them.

17) . Four methods of data collection, except one.
1) - A. Creating a disk-to-image file
2) - B. Creating a disk-to-disk.
3) + C. Creating a disk-to-USB.
4) - D. Creating a sparse data copy of a file or folder.

18) How can we determine the best acquisition method?
1) - A. By the type of data to be acquired.
2) + B. Based on the circumstances of the investigation.
3) - C. According to the speed of the acquisition tool.
4) - D. By the hardware and software available.

19) It is the most common method for determining the best acquisition and offers most flexibility.
1) + A. Creating a disk-to-image file.
2) - B. Creating a disk-to-disk.
3) - C. Creating a logical disk-to-disk or disk-to-data file.

4) - D. Creating a sparse data copy of a file or folder.

20) When disk-to-image copy is not possible because of hardware or software errors or incompatibilities, we can use.
1) - A. Creating a disk-to-image file.
2) + B. Creating a disk-to-disk.
3) - C. Creating a logical disk-to-disk or disk-to-data file.
4) - D. Creating a sparse data copy of a file or folder.

21) . E-mail investigation is an example of.
1) - A. Creating a disk-to-image file.
2) - B. Creating a disk-to-disk.
3) + C. Creating a logical disk-to-disk or disk-to-data file.
4) - D. Creating a sparse data copy of a file or folder.

22) What acquisition that captures only specific files of interest to the case.
1) - A. sparse acquisition.
2) - B. Static acquisition.
3) + C. Logical acquisition.
4) - D. live acquisition.

23) What acquisition that collects fragments of unallocated (deleted) data.
1) + A. sparse acquisition.
2) - B. Static acquisition.
3) - C. Logical acquisition.
4) - D. live acquisition.

24) When making a copy for data acquisition, consider.
1) - A. Size of the source disk.
2) - B. Using tape backup systems.
3) - C. Retain the disk or must return it to the owner.
4) + D. All of the above.

25) Is an area of a disk drive reserved for booting utilities and diagnostic programs. It's not visible to the computer's OS.
1) - A. Master Boot Record (MBR).
2) - B. Extended Partition Table (EPT).
3) - C. Boot Sector Reserve (BSR).
4) + D. Hidden Partition Area (HPA).

26) . Is an encryption technique that performs a sector-by-sector encryption of an entire drive.
1) - A. BitLocker.
2) - B. File-Level Encryption.
3) + C. whole disk encryption.
4) - D. File-Based Encryption.

27) Write-blocker is a _____ that prevents a computer from writing data to an evidence drive.
1) + A. Hardware device or software program.
2) - B. Software program.
3) - C. Hardware device.
4) - D. None of the above.

28) All of these are Design goals of AFF, except.
1) - A. Provide compressed or uncompressed image files.
2) - B. No size restriction for disk-to-image files.
3) - C. Simple design with extensibility.
4) + D. Split an image into smaller segmented files.

29) Whole disk encryption is a feature in Windows called _____ that makes static acquisitions more

difficult.

1) - A. TrueCrypt.
2) - B. FileVault.
3) + C. BitLocker.
4) - D. VeraCrypt.

30) .All of these is disadvantages of acquisition tools for Windows, except one.
1) - A. Must protect acquired data with a well-tested write-blocking hardware device.
2) - B. Tools can't acquire data from a disk's host protected area.
3) - C. Some countries haven't accepted the use of write-blocking devices for data acquisitions.
4) + D. Make acquiring evidence from a suspect drive more convenient.

31) What are the objectives while attending to a computer incident or crime scene?
1) - Protect the evidence.
2) + Protect such information from outside disclosure .
3) - Establish and secure the area of interest .
4) - All of the above

32) What does the Scientific Working Group on Digital Evidence (SWGDE) do
1) - Develop useful digital evidence.
2) + Develop guidelines for adorning and obtaining digital evidence.
3) - Sanction court decisions.
4) - Educate the investigators.

33) When dealing with a digital investigation case for the first time, what should you look for from the very start?
1) - Equipment required in the case
2) + Classification of the case.
3) - Category of the operating system involved.
4) - The human resources in the class.

34) What are the reasons in which law enforcement investigators will not take the computer out of the crime scene?
1) - To be on the right side of the Fourth Amendment prohibitions.
2) + To protect the business from loss.
3) - To satisfy the rules of the organization.
4) - All of the above.

35) Allows corporate investigators to conduct covert surveillance with little or no cause is a
1) - tools needed to analyze
2) + Corporate policy statement
3) - databases of computer hardware and software
4) - All of the above.

36) .....should know under what circumstances they can examine an employee's computer
1) - employee's
2) - customers
3) + Corporate investigators
4) - All of the above

37) What is the primary goal of scene processing?
1) - To arrest the suspect.
2) - To collect and secure physical evidence.
3) + To collect and secure digital evidence.
4) - To interview witnesses

38) What is the primary goal when securing a computer incident or crime scene?
1) - To identify the suspect.
2) + To preserve the evidence.

3) - To notify the media
4) - To remove all electronic devices.

39) Which of the following is NOT a recommended step in preparing forensic tools?
1) - Using incident and crime scene information to guide tool selection.
2) + Ensuring tools are readily accessible.
3) - Including an extensive-response field kit as a secondary resource.
4) - All of the above

40) What areas might you need specialists in when dealing with an incident or crime scene?
1) - Programming and web design
2) + Operating systems and databases
3) - Marketing and advertising
4) - Art and design

41) What is the standard that determines whether a police officer can make an arrest, conduct a personal search, search property, or obtain a search warrant
1) + Probable cause
2) - Clear evidence
3) - Reasonable suspicion
4) - Written consent

42) What is the first step a law officer should take when preparing a crime scene
1) - Collect evidence and leave the site open to individuals
2) + Secure the area and prevent unauthorized access to preserve evidence
3) - Interview witnesses before searching the area
4) - Arrest suspects before verifying the evidence

43) Why is it important to stop your investigation upon discovering evidence of a crime?
1) - To gather more personal evidence
2) + To ensure compliance with Fourth Amendment restrictions
3) - To avoid notifying management
4) - To conduct a public announcement

44) What is required by the Fourth Amendment regarding the issuance of search warrants
1) - They only need to have probable cause
2) + The warrants must accurately describe the place to be searched and the persons or things to be seized
3) - They can be issued based on rumors only
4) - They must be valid for an unlimited period

45) Judges often issue a limiting phrase to the warrant To
1) + Allows the police to separate innocent information from evidence.
2) - Permits judges to differentiate personal opinions from factual evidence.
3) - Empowers teachers to separate student enthusiasm from academic performance
4) - Allows researchers to identify reliable data from misleading statistics

46) Can be any information stored or transmitted in digital form
1) - Physical evidence
2) + Digital evidence.
3) - Logical evidence.
4) - Not one of them.

47) Which group set standards for recovering and examining digital evidence
1) - International Digital Evidence Organization (IDEO).
2) + Scientific Working Group on Digital Evidence (SWGDE).
3) - Digital Forensics Alliance (DFA).
4) - All of the above.

48) General tasks investigators perform when working with digital evidence
1) - Identify digital information.
2) - Collect, preserve, and document evidence
3) - Analyze, identify, and organize evidence
4) + All of the above.

49) One of these isn't one of general tasks investigators perform when working with digital evidence.
1) - Identify digital information.
2) - Collect, preserve, and document evidence
3) + Evidence should be printed to be presented in court.
4) - Analyze, identify, and organize evidence

50) Collecting digital devices and processing a criminal or incident scene must be done.
1) - Structurally
2) - Architecturally
3) + Systematically
4) - All of the above.

51) Consistent practices for digital evidence handling enhance
1) - Ignoring Federal Rules of Evidence
2) + Verify work and credibility.
3) - Disregarding state guidelines.
4) - Collecting evidence with minimal rulings.

52) What is required when admitting bit-stream copies of digital data in court?
1) - The copies must be printed for evidence.
2) - The copies must be encrypted.
3) + The copies must be created and maintained properly
4) - None of the above.

53) What are non-government organizations required to comply with?
1) - International law enforcement guidelines.
2) + State public disclosure and Federal (FOIA) laws.
3) - Corporate privacy policies only.
4) - None of the above.

54) Special category of private-sector businesses include
1) - Companies that are part of the government
2) - Non-profit organizations
3) + ISPs and other communication companies.
4) - Manufacturing companies.

55) ISPs can investigate computer abuse committed by?
1) - Customers.
2) + Employees.
3) - Both employees and customers.
4) - None of the above.

56) Investigating and controlling computer incident scenes in the corporate environment include:
1) - Much easier than in the criminal environment.
2) - Incident scene is often a workplace.
3) + All of them
4) - None of the above.

57) Collecting Evidence in Private-Sector Incident Scenes businesses have inventory _____ _____ of computer hardware and software.
1) + Databases
2) - Data warehouses.

3) - Data sheets.
4) - Not one of them.

58) Policy statements of corporates about misuse of digital assets that allows corporate investigators to?
1) - A. Conduct covert surveillance with little or no cause
2) - B. Access company systems with a warrant
3) + C. A and D.
4) - D. Access company systems without a warrant

59) What should companies do in response to misuse of digital assets ?
1) - Ignore the issue until it becomes a significant problem .
2) + Display a warning banner
3) - Take no action
4) - Perform a full audit

60) Companies should display a warning banner and publish a policy stating that they reserve the right to _____.
1) - Prevent any future incidents .
2) - Share information with competitors
3) + Inspect computing assets at will.
4) - Encrypt all data.

61) What should corporate investigators know before examining an employee's computer?
1) - The type of software used by the employee
2) + Under what circumstances they can examine the employee's computer.
3) - The personal habits of the employee .
4) - The financial situation of the employee.

62) If a corporate investigator finds that an employee is committing or has committed a crime,what can the employer do?
1) - Handle the matter privately .
2) - Ignore the crime .
3) + File a criminal complaint with the police.
4) - Ignore the company policy.

63) If you discover evidence of a crime during a company policy investigation, you should
1) - Continue the investigation without stopping.
2) + Inform management of the incident
3) - Proceed with a criminal investigation on their own.
4) - Destroy the evidence immediately.

64) Law enforcement officers may search for and seize criminal evidence only with:
1) + Probable cause
2) - A subpoena.
3) - A witness statement
4) - None of the above.

65) The Fourth Amendment specify about search warrants?
1) - Warrants must be issued by the victim.
2) - Warrants must only list innocent information.
3) - Warrants are optional in most cases.
4) + Warrants must describe the place to be searched and items to be seized.

66) Judges often issue limiting phrases in warrants to:
1) - Allow evidence to be seized without restriction.
2) - Avoid evidence from being reviewed.
3) + Allows the police to separate innocent information.
4) - Speed up the investigation process.

67) Preparing for a computer search and seizure includes:
1) - Identifying the suspect's financial assets.
2) + Getting answers from victims and informant
3) - Securing search warrants from multiple states.
4) - All of the above.

68) The nature of a digital investigation case helps investigators:
1) + How you proceed the case.
2) - Avoid interviewing witnesses.
3) - Choose the smallest evidence file to analyze.
4) - Focus solely on hardware components.

69) Identifying the type of OS or Digital Device for
1) - Estimating the size of the drive.
2) - How many devices to process at the scene.
3) - Determine which OSs and hardware are involved.
4) - All of the above.

70) Law enforcement investigators need a warrant to
1) - Examine software logs.
2) + Remove computers from a crime scene
3) - Question suspects directly.
4) - Access encrypted files.

71) Additional complications of determining Whether You Can Seize Computers and Digital Devices, all wrong except one.
1) - Availability of cloud storage, which can be located physically
2) + Files stored offsite that are accessed remotely
3) - All stored files belong to the suspect.
4) - Not one of them.

72) If you aren't allowed to take the computers to your lab determine
1) - the resources you need to acquire digital evidence.
2) - which tools can speed data acquisition.
3) + All of them
4) - None of the above.

73) What should be done in getting a detailed description of a digital crime. :
1) - Get as much information as you can about the location of a digital crime.
2) - Identify potential hazards.
3) - Interact with your HAZMAT team.
4) + All of the above.

74) HAZMAT technician can
1) + Decontaminate evidence bag
2) - Move evidence without checking temperatures
3) - Put the target drive in a special HAZMAT bag
4) - Skip safety procedures.

75) Properties handled at the drive's hardware or firmware level:
1) - A.Zone bit recording (ZBR)
2) - B.Track density
3) - C.Areal density
4) + D.All of above

76) Areal density is:
1) - A.the space between each track
2) + B.the number of bits in one square inch of a disk platter.

3) - C.used to improve disk performance.
4) - D.how most manufacturers deal with a platter's inner tracks having a smaller circumference

77) Geometry, Head, Tracks, Cylinders and Sectors are:
1) - A.The Properties of SSD
2) + B.The components of HDD
3) - C.The Properties of HDD
4) - D.The component of SSD

78) All flash memory devices have a feature called:
1) - A. weary leveling
2) + B. wear-leveling
3) - C. None ot the above
4) - D. All of the above

79) Wear leveling is:
1) + A. is a process that is designed to extend the life of solid-state storage devices
2) - B. is a process designed to shorten the life of solid state storage devices.
3) - C. is a process that is not designed to extend the life of solid state storage devices.
4) - D. None of the above

80) In Microsoft file structures, what are the storage allocation units of one or more sectors called?
1) - A. Sectors
2) + B. Clusters
3) - C. Files
4) - D. Drives

81) -What is the range of sizes for clusters in Microsoft file structures?
1) - A. 128 bytes to 4096 bytes
2) + B. 512 bytes to 32,000 bytes
3) - C. 1024 bytes to 64,000 bytes
4) - D. 2048 bytes to 128,000 bytes

82) What is the maximum size of a cluster in Microsoft file structures?
1) - A. 16,000 bytes
2) - B. 24,000 bytes
3) + C. 32,000 bytes
4) - D. 64,000 bytes

83) If the next available cluster is contiguous to the current cluster file becomes defragmented
1) + TRUE.
2) - FALSE.

84) In Microsoft OSs, when a file is deleted by user:
1) - A. Directory entry is marked as a deleted file
2) - B. Data in the file remains on the disk drive
3) - C. Area of the disk where the deleted file resides becomes unallocated disk space
4) + D. All of them

85) when a file is deleted, data in the file is not available on the disk drive any more
1) - TRUE.
2) + FALSE.

86) Area of the disk where the deleted file resides becomes unallocated disk space
1) + TRUE.
2) - FALSE.

87) In Microsoft OSs, when a file is deleted:
1) + A. The disk is available to receive new data from newly created files or other files needing more

space
2) - B. The disk git rid of the file eventually
3) - C. The operating system hides the file
4) - D. None of the above

88) In Microsoft OSs, when a file is deleted,the directory entry is marked as a deleted file
1) - A. With the HEX E5 character replacing the first letter of the filename
2) - B. FAT chain for that file is set to 0 (0xE5)
3) + C. Both A and B
4) - D. None of above

89) When the first assigned cluster is filled and runs out of room FAT assigns the next busy cluster to the file
1) - TRUE.
2) + FALSE.

90) Microsoft OSs allocate disk space for files by sectors
1) - TRUE.
2) + FALSE.

91) What is the term which means that unused space in a cluster between the end of an active file and the end of the
cluster?
1) - A. Clusters
2) - B. Sector
3) + C. Drive slack
4) - D. Cylinder

92) Which of the following options includes the term "Drive slack"?
1) - A. RAM slack only
2) - B. File slack only
3) + C. RAM slack and File slack
4) - D. RAM slack and Disk slack

93) Drive slack is the used space in a cluster between the end of an active file and the end of the cluster.'"
1) - TRUE.
2) + FALSE.

94) What is the difference between RAM slack and File slack in the context of the FAT16 file system?
1) + A. RAM slack is the last portion of the last sector in the allocated cluster, while File slack is the unused space in the remaining sectors.
2) - B. RAM slack is the unused space in the entire cluster, while File slack is part of the random access memory.
3) - C. RAM slack and File slack are the same thing.
4) - D. RAM slack is used to temporarily store data, while File slack is space allocated only for system files.

95) 41- When you run out of room for an allocated cluster OS allocates another cluster for your file, which leads to:
1) - A. Reducing unused space
2) + B. Increasing unused space on the disk (Slack space)
3) - C. Reducing the file size
4) - D. Deleting the file's old data

96) When the OS stores data in a FAT file system,it assigns a starting cluster position to a file,Data for the file is written to
1) - A. last sector of the cluster

2) - B. next cluster
3) + C. first sector of the assigned cluster
4) - D. the RAM

97) The FAT file system was originally designed for hard drives.
1) - TRUE.
2) + FALSE.

98) The FAT system stores information such as filenames, timestamps, and file attributes.
1) + TRUE.
2) - FALSE.

99) exFAT is an outdated version of the FAT system and is no longer in use.
1) - TRUE.
2) + FALSE.

100) The FAT system is a file database system developed by Apple.
1) - TRUE.
2) + FALSE.

101) ExFAT is the file system used in Xbox gaming systems.
1) + TRUE.
2) - FALSE.

102) Cluster sizes vary depending on the hard drive size and the file system.
1) + TRUE.
2) - FALSE.

103) What factors determine the cluster size on a disk?
1) - a. Hard drive size only
2) - b. File system only
3) + c. Both hard drive size and file system
4) - d. None of the above

104) What are the three main versions of the FAT system?
1) - A. FAT16, FAT32, NTFS
2) + B. FAT16, FAT32, exFAT
3) - C. FAT12, FAT16, FAT32
4) - D. NTFS, exFAT, FAT64

105) Why is a search warrant needed to examine mobile devices?
1) - Because they contain little necessary data.
2) + Because they store a large amount of sensitive information.
3) - Because they are often damaged.
4) - Because they store only text messages.

106) Which statement is true about mobile phone networks?
1) - All phones use the same digital network.
2) + The mobile phone industry uses several digital networks.
3) - Analog networks are still widely used today.
4) - Digital networks replaced analog networks in 2005.

107) What is stored in the ROM of a mobile device?
1) - Subscriber information
2) + The operating system (OS)
3) - User files and apps
4) - Peripheral data

108) Which of the following is a primary purpose of a SIM card?
1) - It stores the operating system.
2) + It identifies the subscriber to the network.

3) - It processes signals from the mobile network.
4) - . It stores the device's hardware configuration.

109) Which of the following methods can isolate a mobile device from incoming signals?
1) - Place the device in airplane mode
2) - Place the device in a paint can
3) - None ot them
4) + All of them

110) Which of the following is an example of data that can be retrieved from a SIM card?
1) + Identifiers for the SIM card and the subscriber
2) - Photos and videos
3) - Application settings
4) - None of the above

111) What is required to retrieve data from a network provider?
1) - Airplane mode activation.
2) + A search warrant or subpoena.
3) - Place the device in a paint can.
4) - A SIM card backup file.

112) Which of the following tools is used to Recovers deleted text messages?
1) - BitPam
2) + SIMcon
3) - Device Seizure
4) - MOBILedit Forensic

113) Which of the following is NOT one of the six types of mobile forensics methods listed in NIST guidelines?
1) - Manual extraction
2) - Logical extraction
3) + Malware extraction
4) - Chip-off

114) What is a key challenge with mobile forensics tools like Cellebrite?
1) - They can analyze data from all mobile apps.
2) - They are free to use.
3) + They only support a limited number of mobile apps.
4) - All of the above.

115) What does a file system provide to an OS?
1) - A method to encrypt data.
2) + A road map to data on a disk.
3) - A way to delete unnecessary files.
4) - A tool for programming.

116) The type of file system an OS uses determines.
1) - How data is encrypted
2) - How the CPU processes tasks.
3) + How data is stored on the disk.
4) - How BIOS initializes.

117) The Complementary Metal Oxide Semiconductor (CMOS) stores.
1) + System configuration, date and time information.
2) - The Master Boot Record (MBR).
3) - The entire Windows Registry.
4) - User passwords.

118) BIOS is designed for ____ computers and uses .____
1) - ARM, GUID Partition Table (GPT).

2) - x64, FAT32.
3) + x86, Master Boot Records (MBR).
4) - RISC, NTFS.

119) EFI is designed for ____ computers and uses .____
1) - x86, Master Boot Records (MBR).
2) - ARM, NTFS.
3) - RISC, FAT16.
4) + x64, GUID Partition Table (GPT).

120) The bootstrap process.
1) - Is stored in BIOS.
2) + Tells the computer how to proceed.
3) - Is stored in RAM.
4) - Can only be modified by the operating system.

121) CMOS should be modified to boot from.
1) + A forensic floppy disk or CD.
2) - The fastest available disk.
3) - The cloud storage.
4) - A secure external drive.

122) Disk drive components include the following.
1) + Geometry, Head, Tracks, Cylinders, and Sectors.
2) - BIOS, MBR, RAM, and ROM.
3) - Only RAM, Cache Geometry, Head and Tracks.
4) - None of the above.

123) Zone Bit Recording (ZBR) is.
1) - Improve security of stored data.
2) + Platter’s inner tracks having a smaller circumference.
3) - Encrypt disk partitions.
4) - Store boot records.

124) Wear-leveling is a feature of.
1) - Hard disk drives (HDDs).
2) + Solid-state storage devices (SSDs).
3) - BIOS chips.
4) - Optical drives.

125) When data is deleted on a hard drive.
1) - The original data is removed permanently.
2) - It is moved to another partition.
3) + Only references to it are removed, which leaves data in unallocated space.
4) - It cannot be recovered.

126) .In Microsoft file structures, sectors are grouped to form.
1) - Tracks.
2) - Cylinders.
3) - Logical volumes.
4) + Clusters.

127) In NTFS, clusters are numbered starting at..
1) + 0
2) - 1
3) - 2
4) - 10

128) In FAT, clusters are numbered starting at.

1) - 1
2) - 0
3) + 2
4) - 10

129) A partition is a.
1) + Logical drive.
2) - Physical hard disk.
3) - Type of encryption.
4) - Method to defragment disks.

130) The partition table is located in.
1) - The first sector of a partition.
2) + The Master Boot Record (MBR).
3) - The BIOS memory.
4) - The Windows Registry.

131) File Allocation Table (FAT) was originally designed for
1) - Solid-state drives.
2) - Optical media.
3) + Floppy disks.
4) - SSDs.

132) Microsoft OSs allocate disk space for files using.
1) - Pages.
2) + Clusters.
3) - Cylinders.
4) - LBA addressing.

133) Drive slack includes:
1) - Partition slack and file slack.
2) - Sector slack and file slack.
3) - Directory slack and file slack.
4) + RAM slack and file slack.

134) The three current versions of FAT are.
1) - FAT8, FAT16, and FAT32.
2) + FAT16, FAT32, and exFAT.
3) - FAT32, NTFS, and ext4.
4) - FAT64, FAT128, and FAT256.

135) When a FAT file is deleted?
1) - It is immediately erased from the disk.
2) - The OS encrypts it for security.
3) + The first letter of the filename is replaced with HEX E5.
4) - The file becomes fragmented.

136) A partition gap refers to.
1) - Corrupted files in a partition.
2) - A security vulnerability in MBR.
3) - A feature of the Windows Registry
4) + Unused space between partitions.

137) When you run out of room for an allocated cluster.
1) - Deletes the file.
2) + Allocates another cluster.
3) - Compresses the file.
4) - Moves the file to RAM.

138) The hexadecimal offset for the first partition in MBR is
1) - 0x00.
2) + 0x1BE.
3) - 0xFF.
4) - 0xABC.

139) The file system's hexadecimal code is.
1) - Offset 0x1BE.
2) + Offset 3 bytes from 0x1BE.
3) - Offset 0x00.
4) - Offset 0xFFF.

140) What file system did Microsoft introduce with Windows NT?
1) - FAT32.
2) + NTFS.
3) - ReFS.
4) - HFS+.

141) What is the primary file system for Windows 8?
1) - FAT16.
2) - EXT4.
3) + NTFS.
4) - APFS.

142) What is one of the improvements of NTFS over FAT file systems?
1) - Larger file sizes.
2) - Less control over files.
3) - Only supports ASCII.
4) + More information about a file.

143) What is the first data set on an NTFS disk?
1) + Partition Boot Sector.
2) - Master File Table (MFT).
3) - File Allocation Table.
4) - Root Directory.

144) What structure in NTFS contains information about all files on the disk?
1) - Boot Sector.
2) - FAT Table.
3) + Master File Table (MFT).
4) - Cluster Bitmap.

145) How many records in the MFT are reserved for system files?
1) - 5
2) - 10
3) + 15
4) - 20

146) What is a record field referred to as in an MFT?
1) + Attribute ID.
2) - File ID.
3) - Data Block
4) - Cluster Record

147) Where are files larger than 512 bytes stored in NTFS?
1) - In the MFT.
2) + Outside the MFT.
3) - In the Registry.

4) - In the Boot Sector.

148) What does NTFS use to support international data formats?
1) - ASCII.
2) + Unicode.
3) - Binary.
4) - Hexadecimal.

149) What was Microsoft's goal in moving toward NTFS?
1) - Improve gaming performance.
2) - Increase file system size.
3) + Implement a journaling file system.
4) - Replace Windows Explorer.

150) What NTFS feature keeps track of transactions such as file deleting or saving?
1) - File Encryption.
2) - Defragmentation.
3) - RAID Support.
4) + Journaling.

151) Which feature was introduced with NTFS to encrypt files?
1) - BitLocker.
2) + Encrypting File System (EFS).
3) - Secure Boot.
4) - Firewall.

152) What kind of encryption method does EFS use?
1) - Symmetric encryption only.
2) - XOR encryption.
3) - Hashing.
4) + Public key and private key encryption.

153) When a file is deleted in Windows NT and later, where does it go first?
1) - Deleted permanently.
2) - Moved to a hidden partition.
3) + Renamed and moved to the Recycle Bin.
4) - Converted into a registry key.

154) What command in MS-DOS can be used to delete a file?
1) - ERASE.
2) - RM.
3) + DEL (delete).
4) - REMOVE.

155) What was the new file system introduced in Windows Server 2012?
1) - NTFS.
2) - FAT32.
3) + ReFS.
4) - HFS+.

156) What is a key design feature of ReFS?
1) - Reduced security.
2) + Maximized data availability.
3) - Lower storage capacity.
4) - All of the above.

157) In recent years, there has been more concern about loss of whole disk encryption?
1) - Large hard drive sizes.
2) - Faster processing speeds.

3) + Personal identity information (PII).
4) - Increased internet speeds.

158) What does whole disk encryption typically encrypt?
1) - Only the boot sector.
2) - Only system files.
3) + Each sector of a drive separately.
4) - Only the Recycle Bin.

159) What should be done before examining an encrypted drive?
1) - Run a defragmentation.
2) + Decrypt it first.
3) - Boot into Safe Mode.
4) - Reinstall the operating system.

160) What is an example of a third-party whole disk encryption tool?
1) - Jetico BestCrypt Volume Encryption.
2) - PGP Full Disk Encryption.
3) - Voltage SecureFile.
4) + All of the above.

161) What is the Windows Registry?
1) - A boot sector file
2) + A hierarchical database.
3) - A file compression tool
4) - A temporary file storage

162) Which Windows utility is used to edit the Registry?
1) - CMD.
2) - Notepad.
3) + Regedit.
4) - Disk Cleanup.

163) What is the purpose of the HKEY_LOCAL_MACHINE hive?
1) - Stores temporary files
2) + Contains system settings.
3) - Manages user passwords
4) - Logs error messages

164) What key structure contains user-specific settings?
1) - HKEY_CLASSES_ROOT.
2) + HKEY_USERS.
3) - HKEY_LOCAL_MACHINE.
4) - HKEY_SOFTWARE.

165) What does a virtual machine allow a user to do?
1) + Install multiple operating systems on one physical computer.
2) - Run software at a higher speed.
3) - Increase hard drive storage.
4) - Reduce power consumption.

166) What is stored in a virtual hard disk file?
1) - Only the operating system.
2) + Boot loader program, OS files, and user data.
3) - Encryption keys.
4) - BIOS settings.

167) What is a security concern with virtual machines?
1) - Reduced system memory.

2) - Inability to run software.
3) + Used to attack another system or network.
4) - Limited screen resolution.

168) What Registry component stores information about file extensions?
1) - HKEY_USERS.
2) + HKEY_CLASSES_ROOT.
3) - HKEY_LOCAL_MACHINE.
4) - HKEY_SECURITY.

169) Which of the following is NOT a function of NTFS?
1) - File compression.
2) - Journaling.
3) + Web browsing.
4) - File permissions.

170) What is a trade secret?
1) - A government security measure.
2) + Any information a business keeps confidential to provides a competitive advantage.
3) - A public database.
4) - A digital signature.

171) What tool encrypts entire disk volumes in Windows?
1) - Task Scheduler.
2) + BitLocker.
3) - Notepad++.
4) - Device Manager

172) What encryption algorithm is commonly used in whole disk encryption?
1) - MD5.
2) + AES.
3) - ROT13.
4) - SHA-1

173) What does NTFS use to store access control information?
1) - File name.
2) + Access Control List (ACL).
3) - File path.
4) - Disk size.

174) What happens when a file is deleted from an NTFS partition?
1) - It is completely removed from the disk.
2) + The space is marked as available for new data.
3) - The OS shuts down.
4) - The disk gets reformatted.

175) What kind of data is typically stored on mobile devices?
1) - Incoming and outgoing calls.
2) - MMS and SMS messages.
3) - Email accounts and Instant-messaging (IM) logs.
4) + All of the above.

176) . What is required to examine a mobile device due to the amount of information it contains?
1) - A user's permission.
2) + A search warrant.
3) - A court order.
4) - A forensic analysis tool.

177) Why is investigating mobile devices challenging in digital forensics?

1) + No single standard exists for how and where phones store messages
2) - Phones have unlimited storage.
3) - Phones do not support forensic tools.
4) - Only law enforcement can analyze them.

178) How often do new mobile phones typically appear on the market?
1) - Every month.
2) + Every six months.
3) - Every year.
4) - Every two years.

179) What was introduced with third-generation (3G) mobile networks?
1) - Voice-only calls.
2) - Text messaging.
3) + The ability to download while you were walking or in a moving vehicle
4) - Limited internet access.

180) When was fourth-generation (4G) technology introduced?
1) - 2007
2) - 2008
3) + 2009
4) - 2010

181) What is the primary purpose of EEPROM in mobile devices?
1) - Permanent file storage.
2) + Enables service providers to reprogram phones remotely
3) - Stores user contacts.
4) - Controls screen brightness.

182) What type of memory remains even if a phone loses power?
1) - RAM.
2) - Volatile memory.
3) + ROM
4) - Flash memory.

183) What is a common use of PDAs in modern times?
1) - Personal entertainment.
2) + Medical or industrial PDAs.
3) - Gaming.
4) - Social media browsing.

184) Which memory card type provides extra security features?
1) - Compact Flash (CF).
2) - MultiMediaCard (MMC).
3) + Secure Digital (SD).
4) - USB drive.

185) What is the main function of a SIM card?
1) - Store contacts only
2) + Identify the subscriber to the network.
3) - Increase battery life
4) - Store only multimedia files

186) SIM cards are most commonly found in which type of mobile device?
1) - CDMA phones.
2) + GSM devices.
3) - Satellite phones.
4) - Rotary phones.

187) What should be done immediately if a mobile device is connected to a PC via USB?
1) + Disconnect the device from the PC.
2) - Open forensic software.
3) - Check network connections.
4) - Not one of them

188) What mode helps isolate a mobile device from incoming signals?
1) - Power-saving mode.
2) - Bluetooth mode.
3) + Airplane mode.
4) - Developer mode.

189) .Which item can be used to isolate signals to a mobile device?
1) - A glass container.
2) - A plastic bag.
3) + A paint can.
4) - A freezer.

190) What happens when a mobile device is placed in roaming mode?
1) - It speeds up internet.
2) - It blocks all calls.
3) - It deletes stored messages.
4) + Accelerates battery drainage.

191) What should be done if a seized mobile device is already off?
1) - Turn it on and connect to Wi-Fi.
2) + Attempt a physical static acquisition.
3) - Wipe all data.
4) - Immediately charge the device.

192) What is required to access information from a network provider?
1) - An administrator password.
2) + A search warrant or subpoena.
3) - A forensic certification.
4) - A SIM card reader.

193) What technology do service providers use to erase stolen device data?
1) - Memory compression.
2) + Remote wiping.
3) - Firewall settings.
4) - Over-the-air updates.

194) The file system on a SIM card is _____ in what format?
1) - Random access.
2) + Hierarchical structure.
3) - Encrypted blocks.
4) - Cloud-based.

195) What type of mobile forensics method involves looking at logic gates with an electron microscope?
1) - Logical extraction
2) - Hex dumping
3) + Micro read.
4) - JTAG extraction

196) What can a SIM card reader do?
1) - Increase storage capacity.
2) - Improve battery life.

3) - Change device firmware.
4) + Analyze SIM file content

197) What forensic tool is used to recover files on a GSM/3G SIM or USIM card?
1) - FTK Imager.
2) + SIMcon
3) - BitLocker.
4) - Windows Defender.

198) What is the function of AccessData FTK Imager?
1) + Forensically acquire mobile data.
2) - Unlock devices.
3) - Delete SIM card data.
4) - Bypass network authentication.

199) Which organization provides forensic guidelines for mobile forensics?
1) - FBI.
2) + NIST.
3) - Microsoft.
4) - Verizon.

200) . What is the primary concern when handling mobile forensic cases?
1) + Loss of power.
2) - File compression
3) - Video playback.
4) - Network speed.

201) What method involves physically removing a phone’s flash memory chip?
1) - JTAG extraction.
2) + Chip-off.
3) - Logical extraction.
4) - Memory dump.

202) What is one challenge of mobile forensics?
1) - Lack of forensic software.
2) + Constantly changing phone models.
3) - Small screen sizes
4) - Lack of processing power.

203) What is one drawback of forensic software?
1) - They are mostly free.
2) - They don’t support encryption.
3) - They work only on old phones.
4) + They require frequent updates

204) How do mobile forensics tools document unread messages?
1) + By taking pictures of each screen.
2) - By running a security scan.
3) - By storing messages in binary format.
4) - By copying them to cloud storage.

205) What is one of the most commonly used mobile forensic tools?
1) - Microsoft Word.
2) - Windows Defender.
3) + Cellebrite UFED Forensic System.
4) - Adobe Acrobat.

206) What is the primary function of a SIM card reader?
1) - To reset the phone

2) + To recover deleted data from SIM cards.
3) - To hack into the network
4) - To increase mobile storage

207) Which of the following is not one of six types of NIST guidelines of mobile forensics?
1) - Chip-off.
2) - Hex dumping.
3) - Manual extraction.
4) + Physical imaging.

208) What does JTAG extraction allow forensic examiners to access?
1) + RAM and flash memory.
2) - Internet history.
3) - Call logs only.
4) - SIM card settings.

209) What is a major limitation of forensic software in mobile investigations?
1) + Limited device compatibility.
2) - Inability to acquire contacts.
3) - Cannot analyze text messages.
4) - Only works on Android devices.

210) What is one feature of Cellebrite UFED?
1) + Bypassing lock screens.
2) - Enhancing battery life.
3) - Detecting malware.
4) - Increasing mobile speed.

211) Why is mobile forensics a continuously evolving field?
1) - Due to slow advancements in security
2) - Because digital forensics is no longer useful
3) + Due to rapid changes in phone technology.
4) - Because people use fewer mobile devices

212) What type of mobile forensic tool helps capture data from various phone models?
1) + Paraben Device Seizure.
2) - Windows Firewall.
3) - Chrome Developer Tools.
4) - BitLocker.

213) What should forensic examiners avoid when acquiring data from mobile devices?
1) + Remote wiping.
2) - Using a SIM card reader
3) - Placing the device in a Faraday bag
4) - Removing the battery

214) How can forensic examiners prevent a mobile device from syncing with the cloud?
1) - Keep the device connected to a PC.
2) - Turn on airplane mode only.
3) - Use default phone settings.
4) + Disable Wi-Fi and Bluetooth.

215) Which device is commonly used to prevent mobile signals from interfering with forensic investigations?
1) - Firewall.
2) + Faraday cage.
3) - Wi-Fi booster.
4) - USB hub.

216) What is the purpose of BitPam in mobile forensics?
1) + View data on CDMA phones.
2) - Unlock iPhones
3) - Delete mobile logs
4) - Backup app data

217) What forensic tool includes a built-in write-blocker for mobile investigations?
1) + MOBILedit Forensic.
2) - Notepad++
3) - AccessData FTK
4) - Microsoft Edge

218) Which forensic technique involves extracting data at the binary level?
1) - Logical extraction.
2) + Chip-off.
3) - Manual extraction.
4) - Screenshot capture.

219) What forensic tool is useful for GPS and tablet forensics?
1) - Photoshop.
2) - Windows Registry Editor.
3) + Cellebrite UFED.
4) - File Explorer.

220) How can mobile forensic tools generate evidence reports?
1) + Using MD5 and SHA-1 hash values.
2) - Saving data as a text file only.
3) - Encrypting the entire phone.
4) - Automatically uploading data to the internet.

221) What is the main challenge in extracting data from new smartphones?
1) - Lack of forensic tools
2) - No forensic interest in smartphones
3) + Advanced encryption and security features.
4) - No valuable data stored on them

222) Which forensic tool specializes in analyzing SIM card data?
1) + SIMcon.
2) - Cellebrite UFED.
3) - MacLockPick 3.0.
4) - Task Manager.

223) What is the best approach when handling encrypted mobile data?
1) + Use vendor-specific decryption tools
2) - Guess the encryption key.
3) - Delete the encrypted data.
4) - Ignore the encryption.

224) What is a critical step in mobile forensics investigations?
1) + Documenting all actions taken.
2) - Turning the device off immediately.
3) - Ignoring unread messages.
4) - Changing device passwords.