Name: _____ **Class:** _____ **Date:** _____ **ID: A**

Execise2

Multiple Choice
Identify the choice that best completes the statement or answers the question.

____ 1. The FBI ____ was formed in 1984 to handle the increasing number of cases involving digital evidence.
a. Federal Rules of Evidence (FRE)
b. Department of Defense Computer Forensics Laboratory (DCFL)
c. DIBS
d. Computer Analysis and Response Team (CART)

____ 2. ____ involves recovering information from a computer that was deleted by mistake or lost during a power surge or server crash, for example.
a. Data recovery
b. Network forensics
c. Computer forensics
d. Disaster recovery

____ 3. ____ involves preventing data loss by using backups, uninterruptible power supply (UPS) devices, and off-site monitoring.
a. Computer forensics
b. Data recovery
c. Disaster recovery
d. Network forensics

____ 4. The ____ group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime.
a. network intrusion detection
b. computer investigations
c. incident response
d. litigation

____ 5. By the early 1990s, the ____ introduced training on software for forensics investigations.
a. IACIS
b. FLETC
c. CERT
d. DDBIA

____ 6. In the Pacific Northwest, ____ meets monthly to discuss problems that law enforcement and corporations face.
a. IACIS
b. CTIN
c. FTK
d. FLETC

____ 7. In a ____ case, a suspect is tried for a criminal offense, such as burglary, murder, or molestation.
a. corporate
b. civil
c. criminal
d. fourth amendment

____ 8. In general, a criminal case follows three stages: the complaint, the investigation, and the ____.
a. litigation
b. allegation
c. blotter
d. prosecution

____ 9. Based on the incident or crime, the complainant makes a(n) ____, an accusation or supposition of fact that a crime has been committed.
a. litigation
b. allegation
c. blotter
d. prosecution

____ 10. In a criminal or public case, if you have enough information to support a search warrant, the prosecuting attorney might direct you to submit a(n) ____.
a. blotter
b. exhibit report
c. litigation report
d. affidavit

____ 11. It's the investigator's responsibility to write the affidavit, which must include ____ (evidence) that support the allegation to justify the warrant.
a. litigation
b. prosecution
c. exhibits
d. reports

____ 12. The affidavit must be ____ under sworn oath to verify that the information in the affidavit is true.
a. notarized
b. examined
c. recorded
d. challenged

____ 13. Published company policies provide a(n) ____ for a business to conduct internal investigations.
a. litigation path
b. allegation resource
c. line of allegation
d. line of authority

____ 14. A ____ usually appears when a computer starts or connects to the company intranet, network, or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will.
a. warning banner
b. right of privacy
c. line of authority
d. right banner

____ 15. A(n) ____ is a person using a computer to perform routine tasks other than systems administration.
a. complainant
b. user banner
c. end user
d. investigator

____ 16. Without a warning banner, employees might have an assumed ____ when using a company's computer systems and network accesses.
a. line of authority
b. right of privacy
c. line of privacy
d. line of right

____ 17. In addition to warning banners that state a company's rights of computer ownership, businesses should specify a(n) ____ who has the power to conduct investigations.
a. authorized requester
b. authority of line
c. line of right
d. authority of right

____ 18. Most computer investigations in the private sector involve ____.
a. e-mail abuse
b. misuse of computing assets
c. Internet abuse
d. VPN abuse

____ 19. Corporations often follow the ____ doctrine, which is what happens when a civilian or corporate investigative agent delivers evidence to a law enforcement officer.
a. silver-tree
b. gold-tree
c. silver-platter
d. gold-platter

____ 20. Your ____ as a computer investigation and forensics analyst is critical because it determines your credibility.
a. professional policy
b. oath
c. line of authority
d. professional conduct

____ 21. Maintaining ____ means you must form and sustain unbiased opinions of your cases.
a. confidentiality
b. objectivity
c. integrity
d. credibility

____ 22. The ____ is the route the evidence takes from the time you find it until the case is closed or goes to court.
a. acquisition plan
b. chain of custody
c. evidence path
d. evidence custody

____ 23. When preparing a case, you can apply ____ to problem solving.
a. standard programming rules
b. standard police investigation
c. standard systems analysis steps
d. bottom-up analysis

____ 24. The list of problems you normally expect in the type of case you are handling is known as the ____.
a. standard risk assessment
b. chain of evidence
c. standard problems form
d. problems checklist form

____ 25. The basic plan for your investigation includes gathering the evidence, establishing the ____, and performing the forensic analysis.
a. risk assessment
b. nature of the case
c. chain of custody
d. location of the evidence

____ 26. A(n) ____ helps you document what has and has not been done with both the original evidence and forensic copies of the evidence.
a. evidence custody form
b. risk assessment form
c. initial investigation form
d. evidence handling form

____ 27. Use ____ to secure and catalog the evidence contained in large computer components.
a. Hefty bags
b. regular bags
c. paper bags
d. evidence bags

____ 28. ____ prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab.
a. An antistatic wrist band
b. Padding
c. An antistatic pad
d. Tape

____ 29. ____ investigations typically include spam, inappropriate and offensive message content, and harassment or threats.
a. VPN
b. Internet
c. E-mail
d. Phone

____ 30. To conduct your investigation and analysis, you must have a specially configured personal computer (PC) known as a ____.
a. mobile workstation
b. forensic workstation
c. forensic lab
d. recovery workstation

____ 31. You can use ____ to boot to Windows without writing any data to the evidence disk.
a. a SCSI boot up disk
b. a Windows boot up disk
c. a write-blocker
d. Windows XP

____ 32. To begin conducting an investigation, you start by ____ the evidence using a variety of methods.
a. copying
b. analyzing
c. opening
d. reading

____ 33. A ____ is a bit-by-bit copy of the original storage medium.
a. preventive copy
b. recovery copy
c. backup copy
d. bit-stream copy

____ 34. A bit-stream image is also known as a(n) ____.
a. backup copy
b. forensic copy
c. custody copy
d. evidence copy

____ 35. To create an exact image of an evidence disk, copying the ____ to a target work disk that's identical to the evidence disk is preferable.
a. removable copy
b. backup copy
c. bit-stream image
d. backup image

____ 36. ____ from Technology Pathways is a forensics data analysis tool. You can use it to acquire and analyze data from several different file systems.
a. Guidance EnCase
b. NTI SafeBack
c. DataArrest SnapCopy
d. ProDiscover Basic

____ 37. Forensics tools such as ____ can retrieve deleted files for use as evidence.
a. ProDiscover Basic
b. ProDelete
c. FDisk
d. GainFile

____ 38. When analyzing digital evidence, your job is to ____.
a. recover the data
b. destroy the data
c. copy the data
d. load the data

____ 39. ____ can be the most time-consuming task, even when you know exactly what to look for in the evidence.
a. Evidence recovery
b. Data recovery
c. Data analysis
d. Evidence recording

____ 40. When you write your final report, state what you did and what you ____.
a. did not do
b. found
c. wanted to do
d. could not do

____ 41. In any computing investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as ____.
a. checked values
b. verification
c. evidence backup
d. repeatable findings

____ 42. After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and ____.
a. critique the case
b. repeat the case
c. present the case
d. read the final report

____ 43. For computer forensics, ____ is the task of collecting digital evidence from electronic media.
a. hashing
b. data acquisition
c. lossy compression
d. lossless compression

____ 44. One major disadvantage of ____ format acquisitions is the inability to share an image between different vendors' computer forensics analysis tools.
a. proprietary
b. raw
c. AFF
d. AFD

____ 45. Typically, a(n) ____ acquisition is done on a computer seized during a police raid, for example.
a. live
b. online
c. real-time
d. static

____ 46. If the computer has an encrypted drive, a ____ acquisition is done if the password or passphrase is available.
a. passive
b. static
c. live
d. local

____ 47. The most common and flexible data-acquisition method is ____.
a. Disk-to-disk copy
b. Disk-to-network copy
c. Disk-to-image file copy
d. Sparse data copy

____ 48. SafeBack and SnapCopy must run from a(n) ____ system.
a. UNIX
b. MS-DOS
c. Linux
d. Solaris

____ 49. If your time is limited, consider using a logical acquisition or ____ acquisition data copy method.
a. lossless
b. disk-to-disk
c. sparse
d. disk-to-image

____ 50. Image files can be reduced by as much as ____% of the original.
a. 15
b. 25
c. 30
d. 50

____ 51. Microsoft has recently added ____ in its Vista Ultimate and Enterprise editions, which makes performing static acquisitions more difficult.
a. whole disk encryption
b. backup utilities
c. recovery wizards
d. NTFS

____ 52. Linux ISO images are referred to as ____.
a. ISO CDs
b. Live CDs
c. Forensic Linux
d. Linux in a Box

____ 53. The ____ command displays pages from the online help manual for information on Linux commands and their options.
a. cmd
b. hlp
c. inst
d. man

____ 54. The ____ command creates a raw format file that most computer forensics analysis tools can read, which makes it useful for data acquisitions.
a. fdisk
b. dd
c. man
d. raw

____ 55. The ____ command, works similarly to the dd command but has many features designed for computer forensics acquisitions.
a. raw
b. bitcopy
c. dcfldd
d. man

____ 56. Current distributions of Linux include two hashing algorithm utilities: md5sum and ____.
a. rcsum
b. shasum
c. hashsum
d. sha1sum

____ 57. The ____ DOS program En.exe requires using a forensic MS-DOS boot floppy or CD and a network crossover cable.
a. ProDiscover
b. ILook
c. DIBS USA
d. EnCase

____ 58. EnCase Enterprise is set up with an Examiner workstation and a Secure Authentication for EnCase (____) workstation
a. ILook
b. SAFE
c. Incident Response
d. Investigator

____ 59. SnapBack DatArrest runs from a true ____ boot floppy.
a. UNIX
b. Linux
c. Mac OS X
d. MS-DOS

____ 60. SnapBack DatArrest can perform a data copy of an evidence drive in ____ ways.
a. two
b. three
c. four
d. five

____ 61. ____ is the only automated disk-to-disk tool that allows you to copy data to a slightly smaller target drive than the original suspect's drive.
a. SafeBack
b. EnCase
c. SnapCopy
d. SMART

____ 62. SafeBack performs a(n) ____ calculation for each sector copied to ensure data integrity
a. SHA-1
b. MC5
c. SHA-256
d. MC4

____ 63. ____ has developed the Rapid Action Imaging Device (RAID) to make forensically sound disk copies.
a. DIBS USA
b. EnCase
c. ProDiscover
d. ILook

____ 64. Most federal courts have interpreted computer records as ____ evidence.
a. conclusive
b. regular
c. hearsay
d. direct

____ 65. Generally, computer records are considered admissible if they qualify as a ____ record.
a. hearsay
b. business
c. computer-generated
d. computer-stored

____ 66. ____ records are data the system maintains, such as system log files and proxy server logs.
a. Computer-generated
b. Business
c. Computer-stored
d. Hearsay

____ 67. The FOIA was originally enacted in the ____.
a. 1940s
b. 1950s
c. 1960s
d. 1970s

____ 68. Investigating and controlling computer incident scenes in the corporate environment is ____ in the criminal environment.
a. much easier than
b. as easy as
c. as difficult as
d. more difficult than

____ 69. Every business or organization must have a well defined process that describes when an investigation can be initiated. At a minimum, most corporate policies require that employers have a ____ that a law or policy is being violated.
a. confirmed suspicion
b. proof
c. court order stating
d. reasonable suspicion

____ 70. Confidential business data included with the criminal evidence are referred to as ____ data.
a. commingled
b. exposed
c. public
d. revealed

____ 71. ____ is facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed.
a. Reasonable cause
b. Probable cause
c. A subpoena
d. A warrant

____ 72. Law enforcement investigators need a(n) ____ to remove computers from a crime scene and transport them to a lab.
a. evidence custody form
b. FOIA form
c. affidavit
d. warrant

____ 73. Environmental and ____ issues are your primary concerns when you're working at the scene to gather information about an incident or a crime.
a. legal
b. safety
c. corporate
d. physical

____ 74. When recovering evidence from a contaminated crime scene, if the temperature in the contaminated room is higher than ____ degrees, you should take measures to prevent a hard disk from overheating to prevent damage.
a. 80
b. 90
c. 95
d. 105

____ 75. With a(n) ____ you can arrive at a scene, acquire the data you need, and return to the lab as quickly as possible.
a. bit-stream copy utility
b. extensive-response field kit
c. initial-response field kit
d. seizing order

____ 76. A(n) ____ should include all the tools you can afford to take to the field.
a. initial-response field kit
b. extensive-response field kit
c. forensic lab
d. forensic workstation

____ 77. Courts consider evidence data in a computer as ____ evidence.
a. physical
b. invalid
c. virtual
d. logical

____ 78. Evidence is commonly lost or corrupted through ____, which involves police officers and other professionals who aren't part of the crime scene processing team.
a. onlookers
b. HAZMAT teams
c. FOIA laws
d. professional curiosity

____ 79. When seizing computer evidence in criminal investigations, follow the ____ standards for seizing digital data.
a. Homeland Security Department
b. Patriot Act
c. U.S. DoJ
d. U.S. DoD

____ 80. During an investigation involving a live computer, do not cut electrical power to the running system unless it's an older ____ or MS-DOS system.
a. Windows XP
b. Windows 9x
c. Windows NT
d. Windows Me

____ 81. Certain files, such as the ____ and Security log in Windows XP, might lose essential network activity records if the power is terminated without a proper shutdown.
a. Password log
b. Word log
c. Io.sys
d. Event log

____ 82. One technique for extracting evidence from large systems is called ____.
a. RAID copy
b. RAID imaging
c. large evidence file recovery
d. sparse acquisition

____ 83. Real-time surveillance requires ____ data transmissions between a suspect's computer and a network server.
a. poisoning
b. sniffing
c. blocking
d. preventing

____ 84. The most common computer-related crime is ____.
a. homicide
b. check fraud
c. car stealing
d. sniffing

____ 85. A ____ is a column of tracks on two or more disk platters.
a. cylinder
b. sector
c. track
d. head

____ 86. ____ is how most manufacturers deal with a platter's inner tracks being shorter than its outer tracks.
a. Head skew
b. Cylinder skew
c. ZBR
d. Areal density

____ 87. ____ refers to the number of bits in one square inch of a disk platter.
a. Head skew
b. Areal density
c. Cylinder skew
d. ZBR

____ 88. ____ is the file structure database that Microsoft originally designed for floppy disks.
a. NTFS
b. FAT32
c. VFAT
d. FAT

____ 89. ____ was introduced when Microsoft created Windows NT and is the primary file system for Windows Vista.
a. FAT32
b. VFAT
c. NTFS
d. HPFS

____ 90. On an NTFS disk, immediately after the Partition Boot Sector is the ____.
a. FAT
b. HPFS
c. MBR
d. MFT

____ 91. Records in the MFT are referred to as ____.
a. hyperdata
b. metadata
c. inodes
d. infodata

____ 92. In the NTFS MFT, all files and folders are stored in separate records of ____ bytes each.
a. 1024
b. 1512
c. 2048
d. 2512

____ 93. The file or folder's MFT record provides cluster addresses where the file is stored on the drive's partition. These cluster addresses are referred to as ____.
a. virtual runs
b. metada
c. metaruns
d. data runs

____ 94. When Microsoft introduced Windows 2000, it added built-in encryption to NTFS called ____.
a. EFS
b. VFAT
c. LZH
d. RAR

____ 95. The purpose of the ____ is to provide a mechanism for recovering encrypted files under EFS if there's a problem with the user's original private key.
a. certificate escrow
b. recovery certificate
c. administrator certificate
d. root certificate

____ 96. When Microsoft created Windows 95, it consolidated initialization (.ini) files into the ____.
a. IniRecord
b. Inidata
c. Registry
d. Metadata

____ 97. ____, located in the root folder of the system partition, specifies the Windows XP path installation and contains options for selecting the Windows version.
a. Boot.ini
b. BootSec.dos
c. NTDetect.com
d. NTBootdd.sys

____ 98. ____ is a 16-bit real-mode program that queries the system for device and configuration data, and then passes its findings to NTLDR.
a. Hal.dll
b. Boot.ini
c. NTDetect.com
d. BootSect.dos

____ 99. ____, located in the root folder of the system partition, is the device driver that allows the OS to communicate with SCSI or ATA drives that aren't related to the BIOS.
a. Hal.dll
b. NTBootdd.sys
c. Boot.ini
d. Ntoskrnl.exe

____ 100. ____ contain instructions for the OS for hardware devices, such as the keyboard, mouse, and video card, and are stored in the *%system-root%*\Windows\System32\Drivers folder.
a. Hal.dll
b. Pagefile.sys
c. Ntoskrnl.exe
d. Device drivers

____ 101. ____ is a hidden text file containing startup options for Windows 9x.
a. Pagefile.sys
b. Hal.dll
c. Msdos.sys
d. Ntoskrnl.exe

____ 102. The ____ file provides a command prompt when booting to MS-DOS mode (DPMI).
a. Io.sys
b. Autoexec.bat
c. Config.sys
d. Command.com

____ 103. ____ is a text file containing commands that typically run only at system startup to enhance the computer's DOS configuration.
a. Autoexec.bat
b. Config.sys
c. BootSect.dos
d. Io.sys

____ 104. ____ is a batch file containing customized settings for MS-DOS that runs automatically.
a. Autoexec.bat
b. Config.sys
c. Io.sys
d. Command.com

____ 105. A ____ allows you to create a representation of another computer on an existing physical computer.
a. virtual file
b. logic drive
c. logic machine
d. virtual machine

____ 106. Computer forensics tools are divided into ____ major categories.
a. 2
b. 3
c. 4
d. 5

____ 107. Software forensics tools are commonly used to copy data from a suspect's disk drive to a(n) ____.
a. backup file
b. firmware
c. image file
d. recovery copy

____ 108. To make a disk acquisition with En.exe requires only a PC running ____ with a 12-volt power connector and an IDE, a SATA, or a SCSI connector cable.
a. UNIX
b. MAC OS X
c. Linux
d. MS-DOS

____ 109. Raw data is a direct copy of a disk drive. An example of a Raw image is output from the UNIX/Linux ____ command.
a. rawcp
b. dd
c. d2dump
d. dhex

____ 110. ____ of data involves sorting and searching through all investigation data.
a. Validation
b. Discrimination
c. Acquisition
d. Reconstruction

____ 111. Many password recovery tools have a feature that allows generating potential lists for a ____ attack.
a. brute-force
b. password dictionary
c. birthday
d. salting

____ 112. The simplest method of duplicating a disk drive is using a tool that does a direct ____ copy from the original disk to the target disk.
a. partition-to-partition
b. image-to-partition
c. disk-to-disk
d. image-to-disk

____ 113. To complete a forensic disk analysis and examination, you need to create a ____.
a. forensic disk copy
b. risk assessment
c. budget plan
d. report

____ 114. The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for ____ PC file systems.
a. Apple
b. Atari
c. Commodore
d. IBM

____ 115. In Windows 2000 and XP, the ____ command shows you the owner of a file if you have multiple users on the system or network.
a. Dir
b. ls
c. Copy
d. owner

____ 116. In general, forensics workstations can be divided into ____ categories.
a. 2
b. 3
c. 4
d. 5

____ 117. A forensics workstation consisting of a laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation is also known as a ____.
a. stationary workstation
b. field workstation
c. lightweight workstation
d. portable workstation

____ 118. ____ is a simple drive-imaging station.
a. F.R.E.D.
b. SPARC
c. FIRE IDE
d. DiskSpy

____ 119. ____ can be software or hardware and are used to protect evidence disks by preventing you from writing any data to the evidence disk.
a. Drive-imaging
b. Disk editors
c. Workstations
d. Write-blockers

____ 120. Many vendors have developed write-blocking devices that connect to a computer through FireWire,____ 2.0,and SCSI controllers.
a. USB
b. IDE
c. LCD
d. PCMCIA

____ 121. The ____ publishes articles, provides tools, and creates procedures for testing and validating computer forensics software.
a. CFTT
b. NIST
c. FS-TST
d. NSRL

____ 122. The standards document, ____, demands accuracy for all aspects of the testing process, meaning that the results must be repeatable and reproducible.
a. ISO 3657
b. ISO 5321
c. ISO 5725
d. ISO 17025

____ 123. The NIST project that has as a goal to collect all known hash values for commercial software applications and OS files is ____.
a. NSRL
b. CFTT
c. FS-TST
d. PARTAB

____ 124. The primary hash algorithm used by the NSRL project is ____.
a. MD5
b. SHA-1
c. CRC-32
d. RC4

____ 125. One way to compare your results and verify your new forensic tool is by using a ____, such as HexWorkshop, or WinHex.
a. disk imager
b. write-blocker
c. bit-stream copier
d. disk editor

____ 126. Although a disk editor gives you the most flexibility in ____, it might not be capable of examining a ____ file's contents.
a. testing, compressed
b. scanning, text
c. testing, pdf
d. testing, doc

____ 127. Macintosh OS X is built on a core called ____.
a. Phantom
b. Panther
c. Darwin
d. Tiger

____ 128. In older Mac OSs, a file consists of two parts: a data fork, where data is stored, and a ____ fork, where file metadata and application information are stored.
a. resource
b. node
c. blocks
d. inodes

____ 129. The maximum number of allocation blocks per volume that File Manager can access on a Mac OS system is ____.
a. 32,768
b. 45,353
c. 58,745
d. 65,535

____ 130. On older Macintosh OSs all information about the volume is stored in the ____.
a. Master Directory Block (MDB)
b. Volume Control Block (VCB)
c. Extents Overflow File (EOF)
d. Volume Bitmap (VB)

____ 131. With Mac OSs, a system application called ____ tracks each block on a volume to determine which blocks are in use and which ones are available to receive data.
a. Extents overflow file
b. Volume Bitmap
c. Master Directory Block
d. Volume Control Block

____ 132. On Mac OSs, File Manager uses the ____ to store any information not in the MDB or Volume Control Block (VCB).
a. volume information block
b. extents overflow file
c. catalog
d. master directory block

____ 133. Linux is probably the most consistent UNIX-like OS because the Linux kernel is regulated under the ____ agreement.
a. AIX
b. BSD
c. GPL
d. GRUB

____ 134. The standard Linux file system is ____.
a. NTFS
b. Ext3fs
c. HFS+
d. Ext2fs

____ 135. Ext2fs can support disks as large as ____ TB and files as large as 2 GB.
a. 4
b. 8
c. 10
d. 12

____ 136. Linux is unique in that it uses ____, or information nodes, that contain descriptive information about each file or directory.
a. xnodes
b. extnodes
c. infNodes
d. inodes

____ 137. To find deleted files during a forensic investigation on a Linux computer, you search for inodes that contain some data and have a link count of ____.
a. -1
b. 0
c. 1
d. 2

____ 138. ____ components define the file system on UNIX.
a. 2
b. 3
c. 4
d. 5

____ 139. The final component in the UNIX and Linux file system is a(n) ____, which is where directories and files are stored on a disk drive.
a. superblock
b. data block
c. boot block
d. inode block

____ 140. LILO uses a configuration file named ____ located in the /Etc directory.
a. Lilo.conf
b. Boot.conf
c. Lilo.config
d. Boot.config

____ 141. Erich Boleyn created GRUB in ____ to deal with multiboot processes and a variety of OSs.
a. 1989
b. 1991
c. 1994
d. 1995

____ 142. On a Linux computer, ____ is the path for the first partition on the primary master IDE disk drive.
a. /dev/sda1
b. /dev/hdb1
c. /dev/hda1
d. /dev/ide1

____ 143. There are ____ tracks available for the program area on a CD.
a. 45
b. 50
c. 99
d. 100

____ 144. The ____ provides several software drivers that allow communication between the OS and the SCSI component.
a. International Organization of Standardization (ISO)
b. Advanced SCSI Programming Interface (ASPI)
c. CLV
d. EIDE

____ 145. All Advanced Technology Attachment (ATA) drives from ATA-33 through ATA-133 IDE and EIDE disk drives use the standard ____ ribbon or shielded cable.
a. 40-pin
b. 60-pin
c. 80-pin
d. 120-pin

____ 146. ATA-66,ATA-____, and ATA-133 can use the newer 40-pin/80-wire cable.
a. 70
b. 83
c. 96
d. 100

____ 147. IDE ATA controller on an old 486 PC doesn't recognize disk drives larger than 8.4 ____.
a. KB
b. MB
c. GB
d. TB

____ 148. ____ increases the time and resources needed to extract,analyze,and present evidence.
a. Investigation plan
b. Scope creep
c. Litigation path
d. Court order for discovery

____ 149. You begin any computer forensics case by creating a(n) ____.
a. investigation plan
b. risk assessment report
c. evidence custody form
d. investigation report

____ 150. In civil and criminal cases, the scope is often defined by search warrants or ____, which specify what data you can recover.
a. risk assessment reports
b. investigation plans
c. scope creeps
d. subpoenas

____ 151. There are ____ searching options for keywords which FTK offers.
a. 2
b. 3
c. 4
d. 5

____ 152. ____ search can locate items such as text hidden in unallocated space that might not turn up in an indexed search.
a. Online
b. Inline
c. Active
d. Live

____ 153. The ____ search feature allows you to look for words with extensions such as "ing,""ed," and so forth.
a. fuzzy
b. stemming
c. permutation
d. similar-sounding

____ 154. In FTK ____ search mode, you can also look for files that were accessed or changed during a certain time period.
a. live
b. indexed
c. active
d. inline

____ 155. FTK and other computer forensics programs use ____ to tag and document digital evidence.
a. tracers
b. hyperlinks
c. bookmarks
d. indents

____ 156. Getting a hash value with a ____ is much faster and easier than with a(n) ____.
a. high-level language, assembler
b. HTML editor, hexadecimal editor
c. computer forensics tool, hexadecimal editor
d. hexadecimal editor, computer forensics tool

____ 157. AccessData ____ compares known file hash values to files on your evidence drive or image files to see whether they contain suspicious data.
a. KFF
b. PKFT
c. NTI
d. NSRL

____ 158. Data ____ involves changing or manipulating a file to conceal information.
a. recovery
b. creep
c. integrity
d. hiding

____ 159. One way to hide partitions is to create a partition on a disk, and then use a disk editor such as ____ to manually delete any reference to it.
a. Norton DiskEdit
b. PartitionMagic
c. System Commander
d. LILO

____ 160. Marking bad clusters data-hiding technique is more common with ____ file systems.
a. NTFS
b. FAT
c. HFS
d. Ext2fs

____ 161. The term ____ comes from the Greek word for“hidden writing.”
a. creep
b. steganography
c. escrow
d. hashing

____ 162. ____ is defined as the art and science of hiding messages in such a way that only the intended recipient knows the message is there.
a. Bit shifting
b. Encryption
c. Marking bad clusters
d. Steganography

____ 163. Many commercial encryption programs use a technology called ____, which is designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system data failure.
a. steganography
b. key escrow
c. password backup
d. key splitting

____ 164. People who want to hide data can also use advanced encryption programs, such as PGP or ____.
a. NTI
b. BestCrypt
c. FTK
d. PRTK

____ 165. ____ recovery is a fairly easy task in computer forensic analysis.
a. Data
b. Partition
c. Password
d. Image

____ 166. ____ attacks use every possible letter, number, and character found on a keyboard when cracking a password.
a. Brute-force
b. Dictionary
c. Profile
d. Statistics

____ 167. ____ are handy when you need to image the drive of a computer far away from your location or when you don't want a suspect to be aware of an ongoing investigation.
a. Scope creeps
b. Remote acquisitions
c. Password recovery tools
d. Key escrow utilities

____ 168. ____ is a remote access program for communication between two computers. The connection is established by using the DiskExplorer program (FAT or NTFS) corresponding to the suspect (remote) computer's file system.
a. HDHOST
b. DiskHost
c. DiskEdit
d. HostEditor

____ 169. ____ are based on mathematical instructions that define lines, curves, text, ovals, and other geometric shapes.
a. Bitmap images
b. Metafile graphics
c. Vector graphics
d. Line-art images

____ 170. You use ____ to create, modify, and save bitmap, vector, and metafile graphics files.
a. graphics viewers
b. image readers
c. image viewers
d. graphics editors

____ 171. ____ images store graphics information as grids of individual pixels.
a. Bitmap
b. Raster
c. Vector
d. Metafiles

____ 172. The process of converting raw picture data to another format is referred to as ____.
a. JEIDA
b. rastering
c. demosaicing
d. rendering

____ 173. The majority of digital cameras use the ____ format to store digital pictures.
a. EXIF
b. TIFF
c. PNG
d. GIF

____ 174. ____ compression compresses data by permanently discarding bits of information in the file.
a. Redundant
b. Lossy
c. Huffman
d. Lossless

____ 175. Recovering pieces of a file is called ____.
a. carving
b. slacking
c. saving
d. rebuilding

____ 176. A(n) ____ file has a hexadecimal header value of FF D8 FF E0 00 10.
a. EPS
b. BMP
c. GIF
d. JPEG

____ 177. If you can't open an image file in an image viewer, the next step is to examine the file's ____.
a. extension
b. name
c. header data
d. size

____ 178. The uppercase letter ____ has a hexadecimal value of 41.
a. "A"
b. "C"
c. "G"
d. "Z"

____ 179. The image format XIF is derived from the more common ____ file format.
a. GIF
b. JPEG
c. BMP
d. TIFF

____ 180. The simplest way to access a file header is to use a(n) ____ editor
a. hexadecimal
b. image
c. disk
d. text

____ 181. The ____ header starts with hexadecimal 49 49 2A and has an offset of four bytes of 5C01 0000 2065 5874 656E 6465 6420 03.
a. TIFF
b. XIF
c. JPEG
d. GIF

____ 182. ____ is the art of hiding information inside image files.
a. Steganography
b. Steganalysis
c. Graphie
d. Steganos

____ 183. ____ steganography places data from the secret file into the host file without displaying the secret data when you view the host file in its associated program.
a. Replacement
b. Append
c. Substitution
d. Insertion

____ 184. ____ steganography replaces bits of the host file with other bits of data.
a. Insertion
b. Replacement
c. Substitution
d. Append

____ 185. In the following list, ____ is the only steg tool.
a. EnCase
b. iLook
c. DriveSpy
d. Outguess

____ 186. ____ has also been used to protect copyrighted material by inserting digital watermarks into a file.
a. Encryption
b. Steganography
c. Compression
d. Archiving

____ 187. When working with image files, computer investigators also need to be aware of ____ laws to guard against copyright violations.
a. international
b. forensics
c. copyright
d. civil

____ 188. Under copyright laws, computer programs may be registered as ____.
a. literary works
b. motion pictures
c. architectural works
d. audiovisual works

____ 189. Under copyright laws, maps and architectural plans may be registered as ____.
a. pantomimes and choreographic works
b. artistic works
c. literary works
d. pictorial, graphic, and sculptural works

____ 190. ____ can help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program.
a. Broadcast forensics
b. Network forensics
c. Computer forensics
d. Traffic forensics

____ 191. ____ hide the most valuable data at the innermost part of the network.
a. Layered network defense strategies
b. Firewalls
c. Protocols
d. NAT

____ 192. ____ forensics is the systematic tracking of incoming and outgoing traffic on your network.
a. Network
b. Computer
c. Criminal
d. Server

____ 193. ____ can be used to create a bootable forensic CD and perform a live acquisition.
a. Helix
b. DTDD
c. Inquisitor
d. Neon

____ 194. Helix operates in two modes:Windows Live (GUI or command line) and ____.
a. command Windows
b. remote GUI
c. command Linux
d. bootable Linux

____ 195. A common way of examining network traffic is by running the ____ program.
a. Netdump
b. Slackdump
c. Coredump
d. Tcpdump

____ 196. ____ is a suite of tools created by Sysinternals.
a. EnCase
b. PsTools
c. R-Tools
d. Knoppix

____ 197. ____ is a Sysinternals command that shows all Registry data in real time on a Windows computer.
a. PsReg
b. RegExplorer
c. RegMon
d. RegHandle

____ 198. The PSTools ____ kills processes by name or process ID.
a. PsExec
b. PsList
c. PsKill
d. PsShutdown

____ 199. ____ is a popular network intrusion detection system that performs packet capture and analysis in real time.
a. Ethereal
b. Snort
c. Tcpdump
d. john

____ 200. ____ is the U.S. DoD computer forensics lab's version of the dd command that comes with Knoppix-STD.
a. chntpw
b. john
c. memfetch
d. dcfldd

____ 201. The Knoppix STD tool ____ enables you to reset passwords on a Windows computer, including the administrator password
a. chntpw
b. john
c. oinkmaster
d. memfetch

____ 202. ____ are devices and/or software placed on a network to monitor traffic.
a. Packet sniffers
b. Bridges
c. Hubs
d. Honeypots

____ 203. Most packet sniffers operate on layer 2 or ____ of the OSI model.
a. 1
b. 3
c. 5
d. 7

____ 204. Most packet sniffer tools can read anything captured in ____ format.
a. SYN
b. DOPI
c. PCAP
d. AIATP

____ 205. In a(n) ____ attack, the attacker keeps asking your server to establish a connection.
a. SYN flood
b. ACK flood
c. brute-force attack
d. PCAP attack

____ 206. ____ is the text version of Ethereal, a packet sniffer tool.
a. Tcpdump
b. Ethertext
c. Etherape
d. Tethereal

____ 207. ____ is a good tool for extracting information from large Libpcap files.
a. Nmap
b. Tcpslice
c. Pcap
d. TCPcap

____ 208. The ____ Project was developed to make information widely available in an attempt to thwart Internet and network hackers.
a. Honeynet
b. Honeypot
c. Honeywall
d. Honeyweb

____ 209. Machines used on a DDoS are known as ____ simply because they have unwittingly become part of the attack.
a. ISPs
b. soldiers
c. zombies
d. pawns

____ 210. A ____ is a computer set up to look like any other machine on your network, but it lures the attacker to it.
a. honeywall
b. honeypot
c. honeynet
d. honeyhost

____ 211. E-mail messages are distributed from one central server to many connected client computers, a configuration called ____.
a. client/server architecture
b. central distribution architecture
c. client architecture
d. peer-to-peer architecture

____ 212. In an e-mail address, everything after the ____ symbol represents the domain name.
a. #
b. .
c. @
d. -

____ 213. With many ____ e-mail programs, you can copy an e-mail message by dragging the message to a storage medium, such as a folder or disk.
a. command-line
b. shell-based
c. prompt-based
d. GUI

____ 214. When working on a Windows environment you can press ____ to copy the selected text to the clipboard.
a. Ctrl+A
b. Ctrl+C
c. Ctrl+V
d. Ctrl+Z

____ 215. To retrieve e-mail headers in Microsoft Outlook, right-click the e-mail message, and then click ____ to open the Message Options dialog box. The Internet headers text box at the bottom of the dialog box contains the message header.
a. Options
b. Details
c. Properties
d. Message Source

____ 216. To retrieve an Outlook Express e-mail header right-click the message, and then click ____ to open a dialog box showing general information about the message.
a. Properties
b. Options
c. Details
d. Message Source

____ 217. For older UNIX applications, such as mail or mailx, you can print the e-mail headers by using the ____ command.
a. prn
b. print
c. prnt
d. prt

____ 218. To view AOL e-mail headers click Action, ____ from the menu.
a. More options
b. Message properties
c. Options
d. View Message Source

____ 219. To view e-mail headers on Yahoo! click the ____ link in the Mail Options window, and then click Show all headers on incoming messages.
a. Advanced
b. General Preferences
c. Message Properties
d. More information

____ 220. In Microsoft Outlook, you can save sent, drafted, deleted, and received e-mails in a file with a file extension of ____.
a. .ost
b. .eml
c. .msg
d. .pst

____ 221. ____ is a comprehensive Web site that has options for searching for a suspect, including by e-mail address, phone numbers, and names.
a. www.freeality.com
b. www.google.com
c. www.whatis.com
d. www.juno.com

____ 222. ____ allocates space for a log file on the server, and then starts overwriting from the beginning when logging reaches the end of the time frame or the specified log size.
a. Continuous logging
b. Automatic logging
c. Circular logging
d. Server logging

____ 223. The files that provide helpful information to an e-mail investigation are log files and ____ files.
a. batch
b. configuration
c. scripts
d. .rts

____ 224. ____ contains configuration information for Sendmail, allowing the investigator to determine where the log files reside.
a. /etc/sendmail.cf
b. /etc/syslog.conf
c. /etc/var/log/maillog
d. /var/log/maillog

____ 225. Typically, UNIX installations are set to store logs such as maillog in the ____ directory.
a. /etc/Log
b. /log
c. /etc/var/log
d. /var/log

____ 226. Exchange logs information about changes to its data in a(n) ____ log.
a. checkpoint
b. communication
c. transaction
d. tracking

____ 227. In Exchange, to prevent loss of data from the last backup, a ____ file or marker is inserted in the transaction log to mark the last point at which the database was written to disk.
a. tracking
b. checkpoint
c. temporary
d. milestone

____ 228. The Novell e-mail server software is called ____.
a. Sendmail
b. GroupWise
c. Sawmill
d. Guardian

____ 229. GroupWise has ____ ways of organizing the mailboxes on the server.
a. 2
b. 3
c. 4
d. 5

____ 230. The GroupWise logs are maintained in a standard log format in the ____ folders.
a. MIME
b. mbox
c. QuickFinder
d. GroupWise

____ 231. Some e-mail systems store messages in flat plaintext files, known as a(n) ____ format.
a. POP3
b. mbox
c. MIME
d. SMTP

____ 232. Developed during WWII, this technology,____, was patented by Qualcomm after the war.
a. iDEN
b. CDMA
c. GSM
d. EDGE

____ 233. The ____ digital network divides a radio frequency into time slots.
a. TDMA
b. CDMA
c. FDMA
d. EDGE

____ 234. The ____ network is a digital version of the original analog standard for cell phones.
a. TDMA
b. EDGE
c. CDMA
d. D-AMPS

____ 235. The ____ digital network, a faster version of GSM, is designed to deliver data.
a. TDMA
b. iDEN
c. EDGE
d. D-AMPS

____ 236. TDMA refers to the ____ standard, which introduced sleep mode to enhance battery life.
a. IS-136
b. IS-195
c. IS-236
d. IS-361

____ 237. Typically, phones store system data in ____, which enables service providers to reprogram phones without having to physically access memory chips.
a. EROM
b. PROM
c. EEPROM
d. ROM

____ 238. ____ cards are found most commonly in GSM devices and consist of a microprocessor and from 16 KB to 4 MB of EEPROM.
a. SD
b. MMC
c. SDD
d. SIM

____ 239. ____ can still be found as separate devices from mobile phones. Most users carry them instead of a laptop to keep track of appointments, deadlines, address books, and so forth.
a. SDHCs
b. PDAs
c. CFs
d. MMCs

____ 240. The file system for a SIM card is a ____ structure.
a. volatile
b. circular
c. hierarchical
d. linear

____ 241. The SIM file structure begins with the root of the system (____).
a. EF
b. MF
c. DF
d. DCS

____ 242. Paraben Software is a leader in mobile forensics software and offers several tools, including ____, which can be used to acquire data from a variety of phone models.
a. BitPim
b. DataPilot
c. MOBILedit!
d. Device Seizure

____ 243. In a Windows environment, BitPim stores files in ____ by default.
a. My Documents\BitPim
b. My Documents\Forensics Files\BitPim
c. My Documents\BitPim\Forensics Files
d. My Documents\BitPim\Files

____ 244. ____ is a forensics software tool containing a built-in write blocker.
a. GSMCon
b. MOBILedit!
c. SIMedit
d. 3GPim

Execise2
Answer Section

MULTIPLE CHOICE

1.	ANS: D	PTS: 1	REF: 2
2.	ANS: A	PTS: 1	REF: 4
3.	ANS: C	PTS: 1	REF: 4
4.	ANS: B	PTS: 1	REF: 5
5.	ANS: A	PTS: 1	REF: 6
6.	ANS: B	PTS: 1	REF: 8
7.	ANS: C	PTS: 1	REF: 11
8.	ANS: D	PTS: 1	REF: 12
9.	ANS: B	PTS: 1	REF: 13
10.	ANS: D	PTS: 1	REF: 14
11.	ANS: C	PTS: 1	REF: 14
12.	ANS: A	PTS: 1	REF: 14
13.	ANS: D	PTS: 1	REF: 16
14.	ANS: A	PTS: 1	REF: 16
15.	ANS: C	PTS: 1	REF: 16
16.	ANS: B	PTS: 1	REF: 16
17.	ANS: A	PTS: 1	REF: 18
18.	ANS: B	PTS: 1	REF: 19
19.	ANS: C	PTS: 1	REF: 20
20.	ANS: D	PTS: 1	REF: 21
21.	ANS: B	PTS: 1	REF: 21
22.	ANS: B	PTS: 1	REF: 30
23.	ANS: C	PTS: 1	REF: 32
24.	ANS: A	PTS: 1	REF: 33
25.	ANS: C	PTS: 1	REF: 35
26.	ANS: A	PTS: 1	REF: 36
27.	ANS: D	PTS: 1	REF: 39
28.	ANS: B	PTS: 1	REF: 39
29.	ANS: C	PTS: 1	REF: 41
30.	ANS: B	PTS: 1	REF: 48
31.	ANS: C	PTS: 1	REF: 49
32.	ANS: A	PTS: 1	REF: 51
33.	ANS: D	PTS: 1	REF: 52
34.	ANS: B	PTS: 1	REF: 52
35.	ANS: C	PTS: 1	REF: 52
36.	ANS: D	PTS: 1	REF: 53
37.	ANS: A	PTS: 1	REF: 56
38.	ANS: A	PTS: 1	REF: 56
39.	ANS: C	PTS: 1	REF: 58

40. ANS: B PTS: 1 REF: 64
41. ANS: D PTS: 1 REF: 64
42. ANS: A PTS: 1 REF: 65
43. ANS: B PTS: 1 REF: 103
44. ANS: A PTS: 1 REF: 105
45. ANS: D PTS: 1 REF: 106
46. ANS: C PTS: 1 REF: 106
47. ANS: C PTS: 1 REF: 107
48. ANS: B PTS: 1 REF: 107
49. ANS: C PTS: 1 REF: 107
50. ANS: D PTS: 1 REF: 108
51. ANS: A PTS: 1 REF: 109
52. ANS: B PTS: 1 REF: 113
53. ANS: D PTS: 1 REF: 113
54. ANS: B PTS: 1 REF: 120
55. ANS: C PTS: 1 REF: 123
56. ANS: D PTS: 1 REF: 132
57. ANS: D PTS: 1 REF: 138
58. ANS: B PTS: 1 REF: 142
59. ANS: D PTS: 1 REF: 144
60. ANS: B PTS: 1 REF: 144
61. ANS: C PTS: 1 REF: 144
62. ANS: C PTS: 1 REF: 144
63. ANS: A PTS: 1 REF: 145
64. ANS: C PTS: 1 REF: 158
65. ANS: B PTS: 1 REF: 158
66. ANS: A PTS: 1 REF: 158
67. ANS: C PTS: 1 REF: 163
68. ANS: A PTS: 1 REF: 164
69. ANS: D PTS: 1 REF: 165
70. ANS: A PTS: 1 REF: 166
71. ANS: B PTS: 1 REF: 167
72. ANS: D PTS: 1 REF: 170
73. ANS: B PTS: 1 REF: 171
74. ANS: A PTS: 1 REF: 171
75. ANS: C PTS: 1 REF: 173
76. ANS: B PTS: 1 REF: 174
77. ANS: A PTS: 1 REF: 175
78. ANS: D PTS: 1 REF: 176
79. ANS: C PTS: 1 REF: 176
80. ANS: B PTS: 1 REF: 179
81. ANS: D PTS: 1 REF: 179
82. ANS: D PTS: 1 REF: 181
83. ANS: B PTS: 1 REF: 189
84. ANS: B PTS: 1 REF: 190

85. ANS: A PTS: 1 REF: 209
86. ANS: C PTS: 1 REF: 210|211
87. ANS: B PTS: 1 REF: 212
88. ANS: D PTS: 1 REF: 216
89. ANS: C PTS: 1 REF: 220
90. ANS: D PTS: 1 REF: 220
91. ANS: B PTS: 1 REF: 221
92. ANS: A PTS: 1 REF: 222
93. ANS: D PTS: 1 REF: 222
94. ANS: A PTS: 1 REF: 228
95. ANS: B PTS: 1 REF: 228
96. ANS: C PTS: 1 REF: 232
97. ANS: A PTS: 1 REF: 241
98. ANS: C PTS: 1 REF: 241
99. ANS: B PTS: 1 REF: 242
100. ANS: D PTS: 1 REF: 242
101. ANS: C PTS: 1 REF: 244
102. ANS: D PTS: 1 REF: 244
103. ANS: B PTS: 1 REF: 245
104. ANS: A PTS: 1 REF: 245
105. ANS: D PTS: 1 REF: 246
106. ANS: A PTS: 1 REF: 264
107. ANS: C PTS: 1 REF: 265
108. ANS: D PTS: 1 REF: 266
109. ANS: B PTS: 1 REF: 267
110. ANS: B PTS: 1 REF: 268
111. ANS: B PTS: 1 REF: 274
112. ANS: C PTS: 1 REF: 275
113. ANS: D PTS: 1 REF: 276
114. ANS: D PTS: 1 REF: 278
115. ANS: A PTS: 1 REF: 279
116. ANS: B PTS: 1 REF: 284
117. ANS: D PTS: 1 REF: 284
118. ANS: C PTS: 1 REF: 285
119. ANS: D PTS: 1 REF: 285
120. ANS: A PTS: 1 REF: 286
121. ANS: B PTS: 1 REF: 287
122. ANS: C PTS: 1 REF: 288
123. ANS: A PTS: 1 REF: 289
124. ANS: B PTS: 1 REF: 289
125. ANS: D PTS: 1 REF: 289
126. ANS: A PTS: 1 REF: 289
127. ANS: C PTS: 1 REF: 306
128. ANS: A PTS: 1 REF: 306
129. ANS: D PTS: 1 REF: 308

130. ANS: A PTS: 1 REF: 311
131. ANS: B PTS: 1 REF: 311
132. ANS: B PTS: 1 REF: 312
133. ANS: C PTS: 1 REF: 321
134. ANS: D PTS: 1 REF: 324
135. ANS: A PTS: 1 REF: 324
136. ANS: D PTS: 1 REF: 324
137. ANS: B PTS: 1 REF: 325
138. ANS: C PTS: 1 REF: 325
139. ANS: B PTS: 1 REF: 325
140. ANS: A PTS: 1 REF: 333
141. ANS: D PTS: 1 REF: 333
142. ANS: C PTS: 1 REF: 333
143. ANS: C PTS: 1 REF: 345
144. ANS: B PTS: 1 REF: 346
145. ANS: A PTS: 1 REF: 347
146. ANS: D PTS: 1 REF: 347
147. ANS: C PTS: 1 REF: 347
148. ANS: B PTS: 1 REF: 360
149. ANS: A PTS: 1 REF: 360
150. ANS: D PTS: 1 REF: 362
151. ANS: A PTS: 1 REF: 363
152. ANS: D PTS: 1 REF: 363
153. ANS: B PTS: 1 REF: 364
154. ANS: B PTS: 1 REF: 364
155. ANS: C PTS: 1 REF: 365
156. ANS: D PTS: 1 REF: 366
157. ANS: A PTS: 1 REF: 369
158. ANS: D PTS: 1 REF: 371
159. ANS: A PTS: 1 REF: 371
160. ANS: B PTS: 1 REF: 373
161. ANS: B PTS: 1 REF: 376
162. ANS: D PTS: 1 REF: 376
163. ANS: B PTS: 1 REF: 377
164. ANS: B PTS: 1 REF: 377
165. ANS: C PTS: 1 REF: 378
166. ANS: A PTS: 1 REF: 378
167. ANS: B PTS: 1 REF: 382
168. ANS: A PTS: 1 REF: 383
169. ANS: C PTS: 1 REF: 398
170. ANS: D PTS: 1 REF: 398
171. ANS: A PTS: 1 REF: 398
172. ANS: C PTS: 1 REF: 401
173. ANS: A PTS: 1 REF: 401
174. ANS: B PTS: 1 REF: 404

175. ANS: A PTS: 1 REF: 405
176. ANS: D PTS: 1 REF: 408
177. ANS: C PTS: 1 REF: 414
178. ANS: A PTS: 1 REF: 417
179. ANS: D PTS: 1 REF: 423
180. ANS: A PTS: 1 REF: 423
181. ANS: B PTS: 1 REF: 425
182. ANS: A PTS: 1 REF: 425
183. ANS: D PTS: 1 REF: 426
184. ANS: C PTS: 1 REF: 426
185. ANS: D PTS: 1 REF: 429
186. ANS: B PTS: 1 REF: 430
187. ANS: C PTS: 1 REF: 430
188. ANS: A PTS: 1 REF: 430
189. ANS: D PTS: 1 REF: 430
190. ANS: B PTS: 1 REF: 442
191. ANS: A PTS: 1 REF: 442
192. ANS: A PTS: 1 REF: 442
193. ANS: A PTS: 1 REF: 445
194. ANS: D PTS: 1 REF: 445
195. ANS: D PTS: 1 REF: 448
196. ANS: B PTS: 1 REF: 450
197. ANS: C PTS: 1 REF: 450
198. ANS: C PTS: 1 REF: 450
199. ANS: B PTS: 1 REF: 451
200. ANS: D PTS: 1 REF: 451
201. ANS: A PTS: 1 REF: 451
202. ANS: A PTS: 1 REF: 454
203. ANS: B PTS: 1 REF: 454
204. ANS: C PTS: 1 REF: 455
205. ANS: A PTS: 1 REF: 455
206. ANS: D PTS: 1 REF: 455
207. ANS: B PTS: 1 REF: 455
208. ANS: A PTS: 1 REF: 458
209. ANS: C PTS: 1 REF: 458
210. ANS: B PTS: 1 REF: 459
211. ANS: A PTS: 1 REF: 469
212. ANS: C PTS: 1 REF: 470
213. ANS: D PTS: 1 REF: 472
214. ANS: B PTS: 1 REF: 473
215. ANS: A PTS: 1 REF: 473
216. ANS: A PTS: 1 REF: 473
217. ANS: B PTS: 1 REF: 477
218. ANS: D PTS: 1 REF: 478
219. ANS: B PTS: 1 REF: 480

220. ANS: D PTS: 1 REF: 483
221. ANS: A PTS: 1 REF: 484
222. ANS: C PTS: 1 REF: 485
223. ANS: B PTS: 1 REF: 487
224. ANS: A PTS: 1 REF: 487
225. ANS: D PTS: 1 REF: 488
226. ANS: C PTS: 1 REF: 489
227. ANS: B PTS: 1 REF: 489
228. ANS: B PTS: 1 REF: 491
229. ANS: A PTS: 1 REF: 491
230. ANS: D PTS: 1 REF: 491
231. ANS: B PTS: 1 REF: 500
232. ANS: B PTS: 1 REF: 515
233. ANS: A PTS: 1 REF: 515
234. ANS: D PTS: 1 REF: 515
235. ANS: C PTS: 1 REF: 515
236. ANS: A PTS: 1 REF: 516
237. ANS: C PTS: 1 REF: 517
238. ANS: D PTS: 1 REF: 517
239. ANS: B PTS: 1 REF: 518
240. ANS: C PTS: 1 REF: 520
241. ANS: B PTS: 1 REF: 520
242. ANS: D PTS: 1 REF: 522
243. ANS: A PTS: 1 REF: 522
244. ANS: B PTS: 1 REF: 522

Execise2 [Answer Strip] **ID: A**

D 1.

A 2.

C 3.

B 4.

A 5.

B 6.

C 7.

D 8.

B 9.

D 10.

C 11.

A 12.

D 13.

A 14.

C 15.

B 16.

A 17.

B 18.

C 19.

D 20.

B 21.

B 22.

C 23.

A 24.

C 25.

A 26.

D 27.

B 28.

C 29.

B 30.

C 31.

B 43.

A 32.

D 33.

B 34.

C 35.

D 36.

A 37.

A 38.

C 39.

B 40.

D 41.

A 42.

A 44.

D 45.

C 46.

C 47.

B 48.

C 49.

D 50.

A 51.

B 52.

D 53.

B 54.

Execise2 [Answer Strip] **ID: A**

C 55.
D 56.
D 57.
B 58.
D 59.
B 60.
C 61.
C 62.
A 63.
C 64.
B 65.
A 66.
C 67.
A 68.
D 69.
A 70.
B 71.
D 72.
B 73.
A 74.
C 75.
B 76.
A 77.
D 78.
C 79.
B 80.
D 81.
D 82.
B 83.
B 84.
A 85.
C 86.
B 87.
D 88.
C 89.
D 90.
B 91.
A 92.
D 93.
A 94.
B 95.
C 96.
A 97.
C 98.
B 99.
D 100.
C 101.
D 102.
B 103.
A 104.
D 105.
A 106.
C 107.
D 108.
B 109.
B 110.
B 111.

Execise2 [Answer Strip] **ID: A**

C 112. A 123. D 134. A 145. D 156.

A 135.
D 113. B 124. D 146.
A 157.

D 136.
D 114. D 125. C 147.

D 158.

B 137. B 148.
A 115. A 126.
A 159.

A 149.
C 138.
B 116. C 127.

B 160.
D 150.
B 139.
D 117. A 128.

B 161.

A 151.
A 140.
C 118. D 129.
D 162.

D 152.
D 141.
D 119.

A 130.
B 163.

C 142. B 153.

A 120. B 131.

B 164.
C 143.
B 154.

B 121. B 132.
C 165.
B 144.
C 155.

A 166.
C 122. C 133.

Execise2 [Answer Strip] **ID: A**

B 167.
D 179.
A 191.
B 203.
A 215.

A 180.
A 192.
C 204.
A 168.
A 216.

B 181.
A 193.
A 205.

C 169.
B 217.
D 194.
D 206.
A 182.

D 170.
D 195.
B 207.
D 218.
D 183.

A 171.
B 196.
A 208.
B 219.
C 184.

C 172.
C 197.
C 209.
D 220.
D 185.

A 173.
C 198.

B 186.
B 210.
A 221.
B 174.
B 199.

C 187.
A 211.
A 175.
C 222.
D 200.

D 176.
A 188.
C 212.
A 201.
B 223.

C 177.
D 189.
D 213.
A 224.
A 202.

A 178.
B 190.
B 214.

Execise2 [Answer Strip] **ID: A**

D 225.

C 226.

B 227.

B 228.

A 229.

D 230.

B 231.

B 232.

A 233.

D 234.

C 235.

A 236.

C 237.

D 238.

B 239.

C 240.

B 241.

D 242.

A 243.

B 244.