Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Computer Forensics Exam**

|  |  |  |  |
| --- | --- | --- | --- |
| **Matching** |  |  |  |
| a. Bit | | l. | Operating System |
| b. Byte | | m. Partition | |
| c. Central Processing Unit | | n. RAM Slack | |
| d. Cluster | | o. Random Access Memory | |
| e. File Slack | | p. Sector | |
| f. | Hard Disk Drive | q. Software | |
| g. | Hardware | r. | Swap File |
| h. | Internet | s. | Temporary Files |
| i. | Latent Data | t. | Unallocated Space |
| j. | Message Digest 5 Secure Hash Algorithm | u. | Visible Data |

* 1. Motherboard

1. \_\_\_\_\_ The smallest unit of data addressable by a hard disk drive, generally consisting of 512 bytes
2. \_\_\_\_\_ The location in a computer where the operating system that is in use can be stored and retrieved for quick reference by the CPU
3. \_\_\_\_\_ A file or defined space on the HDD to which data is written, or swapped, to free RAM for applications that are in use
4. \_\_\_\_\_ The software that directs basic functions and operations within a computer
5. \_\_\_\_\_ The space on a hard drive that contains available space; the space may also contain temporary and deleted files
6. \_\_\_\_\_ Data from a computer that is openly visible and available to users
7. \_\_\_\_\_ The area beginning at the end of the logical file and terminating at the end of that sector; in some older operating systems, this area is padded with information in

RAM

1. \_\_\_\_\_ Programs and operations that are used by a computer
2. \_\_\_\_\_ Files temporarily written by an application to perform a function
3. \_\_\_\_\_ A group of eight bits
4. \_\_\_\_\_ Short for binary digit; takes the form of either a one or a zero, and is the smallest unit of information on a machine
5. \_\_\_\_\_ The central component of a computer where all of the data is processed
6. \_\_\_\_\_ The area that begins at the end of the last sector that contains logical data and terminates at the end of the cluster
7. \_\_\_\_\_ A group of sectors in multiples of two, typically the minimum space allocated in a file
8. \_\_\_\_\_ A computer network that provides information globally
9. \_\_\_\_\_ A software algorithm used to “fingerprint” a file or contents of a disk; used to verify the integrity of data
10. \_\_\_\_\_ Consists of the physical material that comprises a computer
11. \_\_\_\_\_ The location in a computer where data is stored and retrieved
12. \_\_\_\_\_ Areas of files and disks that are typically not apparent to the computer user (and often not to the operating system), but contain data nonetheless
13. \_\_\_\_\_ The process of dividing a hard disc drive into different independent sections
14. \_\_\_\_\_ The primary board that contains the circuitry for the computer

Answer the following multiple-choice questions

1. \_\_\_\_\_ Which of the following is not considered a hardware device?
   1. The hard disk drives
   2. The mouse
   3. The Random-Access Memory
   4. The monitor
   5. The operating system
2. \_\_\_\_\_ Which of the following describes a motherboard?
   1. Connects to every device used by the system
   2. Has a socket to accept ram
   3. Is the main circuit board within a computer?
   4. All of the above
   5. None of the above
3. \_\_\_\_\_ The term “bit” is short for which of the following?
   1. Byte
   2. Tidbit
   3. Binary digit
   4. Database
   5. Beneath image threshold
4. \_\_\_\_\_ The primary form of data storage within a personnel computer is which of the following?
   1. The hard disk drives
   2. The CD-ROM
   3. A thumb drives
   4. The recycle bin
   5. A zip drives
5. \_\_\_\_\_ The first thing a crime scene investigator should do when encountering computer forensic evidence is which of the following?
   1. Unplug every device from the CPU to preserve the hard disk drive
   2. Take the system to the laboratory for processing
   3. Procure a warrant to search
   4. Tape each cable to its adjoining component in an effort to preserve the integrity of the physical connections
   5. Document the scene
6. \_\_\_\_\_ The ultimate goal of obtaining an image of a hard disk drive is to do which of the following?
   1. Locate as much incriminating information as possible
   2. Obtain information without altering the drive in any way
   3. Preserve the photographs and video stored on the drive
   4. Attempt to determine the owner of the computer in question
   5. Give priority to the text files on the drive
7. \_\_\_\_\_ Which of the following is one of the most common places to begin to look for evidential data?
   1. A CAD packages
   2. The word processing or text based document files
   3. Any learn to type tutorial
   4. The spreadsheet files
   5. A photograph editing program
8. \_\_\_\_\_ Which of the following is the best definition of latent data?
   1. Unallocated space
   2. Anything readily available to the use, also known as visible data
   3. An automatically saved copy of a file that was recently modified
   4. Those data which are typically of little use to forensic investigators
   5. Those data that are hidden from view
9. \_\_\_\_\_ Which of the following describes what happens once a file is deleted by a user?
   1. It is obliterated from the system and cannot be recovered
   2. It is retained until the disk space it occupies is allocated for another use
   3. It may be identified using forensic image acquisition software
   4. A and B
   5. B and C
10. \_\_\_\_\_ Evidentiary data may be recovered from which of the following?
    1. Unallocated space on the HDD
    2. Slack space on the HDD
    3. Ram swap files
    4. All of the above
    5. None of the above
11. \_\_\_\_\_ A cluster is a group of \_\_\_\_\_ in multiples of \_\_\_\_\_\_?
    1. Sectors, two
    2. Partitions, two
    3. Disks, four
    4. Cylinders, three
    5. Tracks, three
12. \_\_\_\_\_ Which of the following is not considered software?
    1. Accounting applications
    2. Operating systems
    3. Web browsers
    4. Word processors
    5. Floppy discs
13. \_\_\_\_\_ Sectors are typically \_\_\_\_\_\_\_\_\_\_\_\_ bytes in size.
    1. 1024
    2. 126
    3. 256
    4. 512
    5. 2050
14. \_\_\_\_\_ One should not search for visible data in which of the following?
    1. Quicken
    2. Temporary files
    3. Swab files
    4. Windows
    5. Unallocated spaces