## Chapter 2

### True/False

1. A file system is a hierarchy of files and their respective directories.
   **True –** The type of operating system and file system determines the way that digital evidence is acquired and analyzed for both software and hardware.

2. When a file on a personal computer is deleted, it is physically erased from the volume (disk) but now becomes available space.
   **False --** When a file is deleted, it is still physically stored on a volume. However, that space is now available to be overwritten.

3. Application software is a set of programs used to control and manage a computer's hardware and system resources.
   **False –** This describes an operating system. Forensic software tools display many different files from the operating system on a suspect's or victim's computer, so investigators must know how to recognize these files.

4. NTFS is the primary file system that has been included with Windows since the advent of Windows 2000.
   **True --** Windows 2000 and subsequent Windows operating systems still support FAT.

5. Disk cleaning is the process of eliminating the amount of fragmentation in a file system to make file chunks (512K blocks) closer together and increase free space areas on a disk.
   **False—**This describes defragmentation. Fragments of files are not always stored contiguously on a hard drive but are often scattered. This defragmentation process can improve the read/write performance of the file system.

6. The Windows application used to view event logs is Event Viewer.
   **True--** An event is a communication between one application and another program or user on a computer. An event can include the following occurrences: successful authentication and login of a user on a system, a defragmentation, an instant messaging chat session, or the download of an application.

7. Microsoft Edge was introduced with Windows 10.
   **True –** Microsoft's Edge was introduced with Windows 10 as a replacement for Internet Explorer.

8. The binary numbering system uses 16 symbols, which includes the number 0 to 9 and letters A to F.
   **False –** This describes the hexadecimal numbering system. The binary system uses two symbols: 0 and 1.

9. Kernelling is the process of running a small piece of code to activate other parts of the operating system during the boot process.
   **False –** This describes bootstrapping. The bootstrap process is contained in the ROM chip.

10. FTK Imager is a professional computer forensics bit-stream imaging tool.
    **True –** FTK Imager is available for free.

**Multiple Choice**

1. A _____ is a logical storage unit on a disk.
   a. Partition
   b. Hard drive
   c. Platter
   d. None of the above
   **Answer: A.** In computer forensics, we often hear this notion of physical versus logical when it comes to file storage or files retrieved from a computer or media storage.

2. A(n) _____ is composed of 8 bits and is the smallest addressable unit in memory.
   a. Unit
   b. Byte
   c. Track
   d. Sector
   **Answer: B.** A sector on a magnetic hard disk represents 512 bytes or 2048 bytes on optical disks.

3. The decimal number 12 is represented in the hexadecimal system as _____.
   a. A
   b. B
   c. C
   d. D
   **Answer: C.** The hexadecimal system uses characters A, B, C, and D to represent 10, 11, 12, and 13, respectively.

4. The Windows _____ is a hierarchical database that stores system configuration information. It maintains files used to control the operating system's hardware and software and keeps track of the system's users.
   **Answer: Registry.** In terms of evidence, the Windows Registry can provide a wealth of information, including Internet searches, sites visited, passwords, and user activity.

5. The _____.sys is a file that contains a copy of the contents of RAM and is saved to a computer's hard drive when the computer goes into hibernate mode.
    a. Hiberfil
    b. Ram
    c. Mem
    d. Config

    **Answer: Hiberfil.** Because the Hyberfil.sys file is a mirror image of the contents of RAM, the size of this file is generally equal to the size of the computer's RAM. When the computer is restarted, the contents of Hiberfil.sys are reloaded into RAM. RAM can be of great importance to a forensics investigator because it often contains Internet searches, a history of websites visited, and other valuable evidence. This file is found in the root directory of the drive where the operating system is installed.

**Short Answer**

1. The binary number 0001 represents the decimal number _____.
   **Answer: 1 or 01.** The binary numbering system is represented by the characters 0 and 1.

2. The first sector on a hard disk (Sector 0) is known as the _____.
   **Answer: Master Boot Record.** The Master Boot Record (MBR) is involved in the boot process and stores information about the partitions on a disk, including how many exist and their locations.

3. Filenames in FAT16 are limited to _____ characters.
   **Answer: Eight**. This file system supports disk partitions with a maximum storage of 2 GB. File extensions are limited to three characters.

4. The Windows Registry is composed of two elements: _____and values.
   **Answer: Keys.** Keys are akin to folders and are easily identified by noting the folder icon. Most keys contain subkeys (or folders). These subkeys can contain multiple subkeys.

5. _____is a tool first introduced with Vista that enables a user to extend a system's virtual memory through the use of a USB drive.
   **Answer: ReadyBoost.** The purpose of ReadyBoost is to make a computer and its processes run faster.

6. _____Browsing, a feature of Windows Internet Explorer 8, helps to protect data and privacy by preventing the browsing history, temporary Internet files, form data, cookies, and usernames/passwords from being stored or retained locally by the browser, leaving virtually no evidence of the user's browsing or

search history.
**Answer: InPrivate.** During an InPrivate Browsing session, files that are saved to the hard disk and websites that are added to the user's Favorites are preserved. The most successful retrieval of Internet forensics always comes from a live system because Internet files and search information often reside in RAM, which is volatile memory.

7. The _____ File Table maintains file and folder metadata in NTFS.
**Answer: Master.** The data includes the filename, creation date, location, size, and permission for every file and folder.

8. BitLocker was developed to encrypt at the file and folder level. BitLocker_____ is a more advanced tool that encrypts removable USB storage devices.
**Answer: To Go.** The application BitLocker To Go Reader enables the investigator to view the files from a USB drive using XP or Vista.

9. Volume _____ Copy Service is a backup infrastructure for volumes that was developed by Microsoft for Windows XP and Windows Server 2003.
**Answer: Shadow.** Two types of shadow copy exist: a complete copy or clone of the original volume, and a copy that contains only the changes to the volume.

10. File_____ enables the user to reduce the number of bits in a file, which allows for faster transmission of the file.
**Answer: Compression.** The NTFS file system supports file compression, but older Windows file systems do not.

Matching

A. Alternate data stream (ADS)
B. Basic Input/Output System (BIOS)
C. Event
D. Read-only memory (ROM)
E. Tracks
F. Partition
G. FAT
H. Component Object Model (COM)
I. Byte
J. Binary

a. A file's set of attributes
b. Starts an operating system by recognizing and initialing system devices
c. A communication between one application and another program or user on a computer

d. Nonvolatile storage that is generally not modified and is used during the boot process
e. Thin, concentric bands on a disk that are composed of sectors, where data is stored
f. A logical storage unit on a disk
g. A file system developed by Microsoft that utilizes a table to store information about where files are stored, where file space is available, and where files cannot be stored
h. Enables nonprogrammers to write scripts for managing Windows operating systems
i. The smallest addressable unit in memory composed of 8 bits
j. The language that computers understand