EnCase Certified Examiner (EnCE) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is the logical size of a directory entry in a FAT file system?

A. 0 bytes

B. 8 bytes

C. 16 bytes

D. One sector

2. What is one key function of a hash library in EnCase?

A. To enable real-time monitoring of files

B. To store and access known hash values for comparison

C. To generate reports automatically

D. To visualize data graphs

3. In computer systems, what does the abbreviation "RAM" stand for?

A. Read-Always Memory

B. Random Access Memory

C. Read Access Memory

D. Rapid Access Memory

4. Is it always safe to pull the plug on a Windows 7 Enterprise operating system?

A. True

B. False

5. What should you do when creating a storage volume to hold an EnCase evidence file with LinEn?

A. Format the volume with the FAT file system.

B. Give the volume a unique label to identify it.

C. Wipe the volume before formatting to avoid claims of cross-contamination.

D. All of the above.

6. Which selection displays the incorrect method for shutting down a computer?

A. DOS: Pull the plug.

B. Windows 7: Pull the plug.

C. Windows XP: Pull the plug.

D. Linux: Pull the plug.

7. Which type of memory is typically faster, RAM or ROM?

A. RAM

B. ROM

C. They are equally fast

D. Depends on the processor

8. IDE, SCSI, and SATA are interfaces that describe which type of device?

A. RAM chips

B. Flash memory

C. CPUs

D. Hard drives

9. In Windows 7, the date and time of when a file was sent to the Recycle Bin can be found where?

A. INFO2 file

B. Original filename's last access date

C. DOS directory or MFT

D. $I index file

10. Which folder is NOT typically found within the automatically created folders of a new case in EnCase 7?

A. Export

B. Temp

C. Email

D. History

Answers

1. A
2. B
3. B
4. B
5. D
6. D
7. A
8. D
9. D
10. D

Explanations

1. What is the logical size of a directory entry in a FAT file system?

A. 0 bytes

B. 8 bytes

C. 16 bytes

D. One sector

In a FAT file system, the logical size of a directory entry is typically 32 bytes. Each directory entry contains essential information about a file or a subdirectory, such as the file name, file attributes, starting cluster number, file size, and timestamps. Therefore, none of the given choices accurately represent the correct logical size of a directory entry. In the context of your selected answer, 0 bytes would imply that there is no logical size being allocated to a directory entry, which is not accurate since each entry does occupy space. It's essential to understand that the logical structure of the FAT file system allocates specific sizes for its directory entries to function correctly. This consistency helps the file system manage files and directories efficiently, allowing it to keep track of different file system entities. Understanding the correct size is crucial for recognizing how data is structured in file systems and ensuring effective data recovery and forensics practices.

2. What is one key function of a hash library in EnCase?

A. To enable real-time monitoring of files

B. To store and access known hash values for comparison

C. To generate reports automatically

D. To visualize data graphs

A key function of a hash library in EnCase is to store and access known hash values for comparison. Hash libraries are essential in digital forensics as they provide a repository of hash values that represent known files, such as system files, user files, and files that are identified as malicious or innocuous. When investigators analyze data, they can compare the hashes of the files in question against those stored in the hash library. This helps determine if the files are known, potentially speeding up the investigation by allowing examiners to focus on unknown or suspicious files. Using hash values for comparison is critical in identifying duplicates, verifying file integrity, and identifying known malicious content without needing to open each file, thereby preserving the investigative workflow. This process strengthens the reliability and efficiency of the forensic analysis conducted with EnCase software.

3. In computer systems, what does the abbreviation "RAM" stand for?

A. Read-Always Memory

B. Random Access Memory

C. Read Access Memory

D. Rapid Access Memory

The abbreviation "RAM" stands for Random Access Memory. This type of memory is essential in computer systems as it allows for data to be read from and written to any location in a memory chip with equal speed, which is why it is termed "random access." Unlike sequential memory types, where data must be accessed in a predetermined order, random access enables quick retrieval and storage of data which enhances the performance of the computer by allowing fast access to applications and processes currently in use. The other options do not accurately describe RAM: Read-Always Memory implies a non-writable format, which does not reflect RAM's functionality; Read Access Memory also mischaracterizes RAM, as it supports both reading and writing operations; Rapid Access Memory, while suggesting speed, does not capture the critical aspect of random accessibility that defines RAM's capabilities. Therefore, the correct understanding of RAM's function and characteristics solidifies the definition as Random Access Memory.

4. Is it always safe to pull the plug on a Windows 7 Enterprise operating system?

A. True

B. False

The notion that it is always safe to abruptly power off a Windows 7 Enterprise operating system is not accurate. Abrupt shutdowns can lead to various negative consequences, particularly regarding data integrity and system stability. When you "pull the plug," you cut power to the system, bypassing the operating system's normal shutdown procedures, which can result in unsaved data being lost and potentially cause file system corruption. Windows operating systems, including Windows 7, maintain a variety of running processes, and abrupt termination can disrupt them, endangering important data. Additionally, if the system is in the middle of writing data to the disk, such as creating or modifying files, an unexpected shutdown increases the likelihood of issues like corrupted files and the necessity for system repairs upon the next startup. To maintain data integrity and ensure the operating system's proper functioning, it is always advisable to perform a controlled shutdown through the OS's normal procedures rather than an abrupt power cut.

5. What should you do when creating a storage volume to hold an EnCase evidence file with LinEn?

A. Format the volume with the FAT file system.

B. Give the volume a unique label to identify it.

C. Wipe the volume before formatting to avoid claims of cross-contamination.

D. All of the above.

When creating a storage volume to hold an EnCase evidence file with LinEn, several key practices ensure the integrity and proper management of the evidence. Formatting the volume with the FAT file system is a suitable choice because FAT is widely supported and compatible with various operating systems, making it easier to access the evidence file across different environments. This format is also straightforward to implement for forensic investigations. Assigning a unique label to the volume is crucial for easy identification. Unique labels help forensic examiners quickly recognize the purpose and contents of the volume, facilitating better organization and reducing the risk of errors when handling multiple pieces of evidence. Wiping the volume before formatting is an essential step that serves to eliminate any pre-existing data that could lead to claims of cross-contamination. This practice preserves the evidential integrity by ensuring that the new data being stored does not intermingle with any residual data from prior usage. Incorporating all these measures enhances both the reliability and credibility of the forensic process, ultimately upholding the standards required in digital investigations. Each aspect contributes to creating a well-defined and secure environment for preserving digital evidence.

6. Which selection displays the incorrect method for shutting down a computer?

A. DOS: Pull the plug.

B. Windows 7: Pull the plug.

C. Windows XP: Pull the plug.

D. Linux: Pull the plug.

The selection highlighting the method for shutting down a computer that is incorrect is the one related to Linux and the practice of "pulling the plug." Properly shutting down a Linux operating system involves using command line tools or graphical user interface options specifically designed for shutting down the system. This ensures that all processes terminate correctly and that the filesystem is properly unmounted, preventing potential data loss or corruption. In contrast, while "pulling the plug" is noted as an improper method across multiple operating systems, it's particularly emphasized here in the context of Linux, as this practice can lead to a lack of system integrity and issues on reboot. Systems like Windows 7 and Windows XP also have user-friendly shutdown options that should be used instead of abruptly cutting power. DOS, while older and less complex, still operates under principles that advise against this method. The correct approach across all operating systems is to utilize their built-in shutdown features, ensuring that the system can safely terminate processes and prevent future problems.

7. Which type of memory is typically faster, RAM or ROM?

A. RAM

B. ROM

C. They are equally fast

D. Depends on the processor

RAM (Random Access Memory) is typically faster than ROM (Read-Only Memory). RAM is designed for high-speed read and write operations, providing quick access to data that the processor needs for active tasks and applications. Its structure allows for rapid data retrieval and manipulation, which is essential for performance during active computing processes. In contrast, ROM is mainly used to store firmware or software that is not intended to be changed frequently, such as the BIOS in a computer. It is primarily read-only, meaning that it doesn't support frequent writing and rewriting like RAM does. This characteristic makes RAM more suitable for tasks that require quick data access and manipulation. The other options involve considerations that don't apply directly to the inherent speed characteristics of RAM and ROM. Therefore, the choice of RAM as the faster memory type is substantiated by its capacity for rapid data handling compared to ROM.

8. IDE, SCSI, and SATA are interfaces that describe which type of device?

A. RAM chips

B. Flash memory

C. CPUs

D. Hard drives

The correct choice identifies IDE, SCSI, and SATA as interfaces specifically related to hard drives. These interface standards are crucial for connecting storage devices to a computer's motherboard and facilitate communication between the hard drives and other components of the system. IDE (Integrated Drive Electronics) is an older interface that was widely used for connecting hard disks and CD-ROM drives. It integrates the controller directly on the drive itself, simplifying the design and installation process for storage devices. SCSI (Small Computer System Interface) is a standard that not only supports hard drives but also various other devices such as scanners and printers. It allows multiple devices to be connected in a shared system and historically has been known for its speed and flexibility in enterprise-level applications. SATA (Serial Advanced Technology Attachment) is a more modern interface that offers a faster data transfer rate compared to both IDE and SCSI. It is commonly found in contemporary hard drives and solid-state drives, providing a reliable and efficient means of connecting storage to a computer. Overall, these interfaces are all integral to the functioning of hard drives, enabling data transfer and communication with the rest of the computer system, which is why this choice is the most accurate.

9. In Windows 7, the date and time of when a file was sent to the Recycle Bin can be found where?

A. INFO2 file

B. Original filename's last access date

C. DOS directory or MFT

D. $I index file

The date and time of when a file was sent to the Recycle Bin in Windows 7 can indeed be found in the $I index file. When a file is deleted and moved to the Recycle Bin, the system does not just remove it from the file system; instead, it creates a special file that retains information about the deleted file. The $I index files are specifically responsible for storing metadata about the files in the Recycle Bin, including their original paths and the date and time that they were sent to the Recycle Bin. This is crucial for recovery processes, allowing users to know when exactly a file was deleted. By examining these index files, forensic investigators can track deleted files, which can be pivotal in an investigation. On the other hand, while the INFO2 file has historically contained metadata for files in the Recycle Bin in earlier versions of Windows, Windows 7 transitioned this data management to the $I index files. The original filename's last access date and the DOS directory or Master File Table (MFT) do not provide the requisite information about when files were moved to the Recycle Bin, as they deal with different aspects of file system management and metadata.

10. Which folder is NOT typically found within the automatically created folders of a new case in EnCase 7?

A. Export

B. Temp

C. Email

D. History

When a new case is created in EnCase 7, several automatically generated folders are established to help organize the various types of data that will be processed and analyzed. Among these folders typically found are the Export, Temp, and Email folders, each serving specific purposes. The Export folder is used to store any files that are exported from the case for reporting or sharing purposes. The Temp folder is a workspace for temporary files that may be needed during the forensic analysis but are not intended for long-term storage. The Email folder is specifically created to manage email evidence and associated artifacts that the investigator might need for case reconstruction and analysis. In contrast, the History folder is not created automatically within a new case. This folder is meant to store logs and historical data about the forensic process and actions taken within the case but is not part of the initial setup. Its absence from the automatically generated folders reflects that it may be created manually if needed for documentation purposes. This distinction highlights the intent behind the organization of folders within EnCase, where the initial structure supports core functionality for managing evidence efficiently.