GIAC

GBFA
GIAC Battlefield Forensics and Acquisition

Latest Version: 6.0

Question: 1

During a dead box acquisition, why is media removal an important step?
Response:

A. To facilitate the device's recycling process
B. To allow for the physical destruction of the media
C. To examine the media independently of the original device
D. To improve the aesthetic appeal of the device

Answer: C

Question: 2

In an NTFS filesystem, which file attribute would you examine to understand more about a file's previous states or versions?
Response:

A. $STANDARD_INFORMATION
B. $FILE_NAME
C. $DATA
D. $LOGGED_UTILITY_STREAM

Answer: D

Question: 3

Which component within the NTFS file system is specifically designed to enhance data recovery capabilities?
Response:

A. Volume Shadow Copy
B. BitLocker
C. Disk Quotas
D. Transactional NTFS

Answer: A

Question: 4

What is a common purpose of acquiring Shadow Copies in a forensic investigation?
Response:

A. To analyze user activities
B. To recover deleted files
C. To update the system
D. To clean the disk

Answer: B

Question: 5

When comparing physical storage devices, why is understanding the interface type important?
Response:

A. It determines the device's color.
B. It affects data transfer speeds and compatibility.
C. It influences the device's physical dimensions.
D. It dictates the device's operational noise.

Answer: B

Question: 6

During an acquisition process, which of the following are essential to ensure the authenticity and integrity of macOS artifacts?
(Choose Three)
Response:

A. Verifying the hash value of the acquired data.
B. Using a certified USB cable.
C. Documenting the process meticulously.
D. Acquiring data in a forensically sound manner.
E. Keeping the device charged during acquisition.

Answer: A,C,D

Question: 7

Regarding data encryption on drives, what is an important factor to consider for forensic analysis?
Response:

A. The brand of the drive
B. The encryption algorithm used
C. The color of the drive LED
D. The cable type connecting the drive

Answer: B

Question: 8

Why is it necessary to know the specific OS version of a mobile device during acquisition?
Response:

A. To choose the right color settings for the display
B. To determine the appropriate data acquisition method
C. To ensure compatibility with the charging cable
D. To adjust the screen brightness correctly

Answer: B

Question: 9

For acquiring RAM, which of the following approaches can be applied to a system running Linux? (Choose Two)
Response:

A. Use of /dev/mem
B. Target Disk Mode
C. Use of LiME
D. Utilizing the dd command on /dev/mem

Answer: A,C

Question: 10

How do modern EXT filesystems, like EXT4, improve file system performance compared to earlier versions like EXT2?
Response:

A. By eliminating the need for file defragmentation
B. By using journaling to protect against corruption
C. By supporting larger files and volumes
D. By introducing a hierarchical directory structure

Answer: B