ECCouncil

112-53

EC-Council Digital Forensics Essentials (DFE)

Latest Version: 6.0

Question: 1

Which macOS feature poses challenges in forensic analysis because it encrypts data, making recovery of deleted files difficult?

A. FileVault
B. Time Machine
C. Spotlight
D. Fusion Drive

Answer: A

Question: 2

During the investigation phase, the process of evidence acquisition is critical. Which of the following best describes a proper procedure for evidence acquisition?

A. Powering off the device immediately to preserve evidence
B. Documenting the system's physical and digital condition
C. Connecting to the internet to update forensic software
D. Interrogating involved personnel before securing digital evidence

Answer: B

Question: 3

What aspect of Windows memory analysis can provide insights into recently executed programs?

A. File size analysis
B. User account settings
C. Analysis of page file.sys
D. Examination of prefetch files

Answer: D

Question: 4

Why might an investigator choose the Advanced Forensics Format (AFF) over the Raw format?

A. AFF supports metadata storage and compression.
B. AFF is faster to create and process.
C. Raw format cannot be used on Windows systems.
D. Raw format requires more specialized hardware.

Answer: A

Question: 5

In disk partitioning, what is the primary purpose of creating multiple partitions on a single physical disk?

A. To increase the disk speed
B. To physically separate data for security reasons
C. To enable dual booting of different operating systems
D. To create additional physical disks

Answer: B

Question: 6

When investigating Mac forensics, which feature is crucial for understanding user data changes over time?

A. Spotlight indexing
B. Launch Agents and Daemons
C. Time Machine backups
D. FileVault encryption

Answer: C

Question: 7

Which of the following are objectives during the postinvestigation phase?
(Select two)

A. Ensuring all evidence is returned to rightful owners
B. Updating investigation policies based on recent experiences
C. Planning the press conference for case disclosure
D. Archiving all documentation and evidence properly

Answer: B,D

Question: 8

For Linux and Mac forensics, what is the importance of analyzing the /tmp directory?

A. It may contain remnants of malicious scripts.
B. It is where the system stores its kernel logs.
C. It provides a history of installed applications.
D. It includes user download history.

Answer: A

Question: 9

Why is it important to analyze GET and POST requests during a web application forensic investigation?

A. To optimize the multimedia content delivery
B. To determine the load balancing efficiency of the web application
C. To identify potential injection points for attacks
D. To evaluate the effectiveness of the web application's marketing strategies

Answer: C

Question: 10

How can web server logs aid in the forensic investigation of a distributed denial of service (DDoS) attack?

A. By displaying the color depth of visitor displays
B. By revealing the uptime of the server
C. By indicating changes in the advertising click-through rates
D. By showing an unusual increase in traffic from varied sources

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer