312-49

Computer Hacking Forensic Investigator

DEMO

Topic 1, Volume A

QUESTION NO: 1

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on
B. Turn off the device immediately
C. Remove the battery immediately
D. Remove any memory cards immediately

Answer: A
Explanation:

QUESTION NO: 2

What hashing method is used to password protect Blackberry devices?

A. AES
B. RC5
C. MD5
D. SHA-1

Answer: D
Explanation:

QUESTION NO: 3

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry
B. The swapfile
C. The recycle bin
D. The metadata

Answer: B

Explanation:

QUESTION NO: 4

With regard to using an antivirus scanner during a computer forensics investigation, you should:

A. Scan the suspect hard drive before beginning an investigation
B. Never run a scan on your forensics workstation because it could change your system configurationNever run a scan on your forensics workstation because it could change your system? configuration
C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
D. Scan your forensics workstation before beginning an investigation

Answer: D

Explanation:

QUESTION NO: 5

What layer of the OSI model do TCP and UDP utilize?

A. Data Link
B. Network
C. Transport
D. Session

Answer: C

Explanation:

QUESTION NO: 6

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. One
B. Two
C. Three

D. Four

Answer: B
Explanation:

QUESTION NO: 7

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. On the individual computer ARP cacheOn the individual computer? ARP cache
B. In the Web Server log files
C. In the DHCP Server log files
D. There is no way to determine the specific IP address

Answer: C
Explanation:

QUESTION NO: 8

What type of equipment would a forensics investigator store in a StrongHold bag?

A. PDAPDA?
B. Backup tapes
C. Hard drives
D. Wireless cards

Answer: D
Explanation:

QUESTION NO: 9

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A. Write-blocker
B. Protocol analyzer
C. Firewall