312-49^{Q&As}

312-49^Q&As

ECCouncil Computer Hacking Forensic Investigator (V9)

Pass EC-COUNCIL 312-49 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/312-49.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Robust copy

B. Incremental backup copy

C. Bit-stream copy

D. Full backup copy

Correct Answer: C

QUESTION 2

Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

A. Tokenmon

B. PSLoggedon

C. TCPView

D. Process Monitor

Correct Answer: B

QUESTION 3

What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

A. AA55

B. 00AA

C. AA00

D. A100

Correct Answer: A

QUESTION 4

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A. Routing Table

B. Firewall log

C. Configuration files D. Email Header

Correct Answer: D

QUESTION 5

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\\'s 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

Correct Answer: C

[Latest 312-49 Dumps](#)   [312-49 Exam Questions](#)   [312-49 Braindumps](#)