312-49$^{\text{Q\&As}}$

ECCouncil Computer Hacking Forensic Investigator (V9)

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

QUESTION 1

If you plan to startup a suspect\\'s computer, you must modify the ____________ to ensure that you do not contaminate or alter data on the suspect\\'s hard drive by booting to the hard drive.

A. deltree command

B. CMOS

C. Boot.sys

D. Scandisk utility

Correct Answer: C

QUESTION 2

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

A. Cracks every password in 10 minutes

B. Distribute processing over 16 or fewer computers

C. Support for Encrypted File System

D. Support for MD5 hash verification

Correct Answer: B

QUESTION 3

You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A. Stringsearch

B. grep

C. dir

D. vim

Correct Answer: B

QUESTION 4

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

A. Cross Examination

B. Direct Examination

C. Indirect Examination

D. Witness Examination

Correct Answer: A

QUESTION 5

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

A. Point-to-point

B. End-to-end

C. Thorough

D. Complete event analysis

Correct Answer: B

312-49 PDF Dumps 312-49 VCE Dumps 312-49 Study Guide