# 312-49V8 Q&As

Computer Hacking Forensic Investigator Exam

## Pass EC-COUNCIL 312-49V8 Exam with 100% Guarantee

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

**https://www.leads4pass.com/312-49v8.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

Which of the following approaches checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Graph-based approach

B. Neural network-based approach

C. Rule-based approach

D. Automated field correlation approach

Correct Answer: D

**QUESTION 2**

First response to an incident may involve three different groups of people, and each will have differing skills and need to carry out differing tasks based on the incident. Who is responsible for collecting, preserving, and packaging electronic evidence?

A. System administrators

B. Local managers or other non-forensic staff

C. Forensic laboratory staff

D. Lawyers

Correct Answer: C

**QUESTION 3**

Centralized logging is defined as gathering the computer system logs for a group of systems in a centralized location. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

A. True

B. False

Correct Answer: A

**QUESTION 4**

When a system is compromised, attackers often try to disable auditing, in Windows 7; modifications to the audit policy are recorded as entries of Event ID_____.

A. 4902

B. 3902

C. 4904

D. 3904

Correct Answer: A

**QUESTION 5**

Which of the following is not a part of data acquisition forensics Investigation?

A. Permit only authorized personnel to access

B. Protect the evidence from extremes in temperature

C. Work on the original storage medium not on the duplicated copy

D. Disable all remote access to the system

Correct Answer: C