EC1-349 Q&As

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.pass4itsure.com/ec1-349.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following attributes of a forensics report can render it inadmissible in a court of law?

A. It includes metadata about the incident

B. It includes relevant extracts referred to In the report that support analysis or conclusions

C. It is based on logical assumptions about the incident timeline

D. It maintains a single document style throughout the text

Correct Answer: C

QUESTION 2

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

A. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum

B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file

C. A simple DOS copy will not include deleted files, file slack and other information

D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector

Correct Answer: C

QUESTION 3

_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics

B. Computer Forensics

C. Incident Response

D. Event Reaction

Correct Answer: B

QUESTION 4

Which of the following is not correct when documenting an electronic crime scene?

A. Document the physical scene, such as the position of the mouse and the location of components near the system

B. Document related electronic components that are difficult to find

C. Record the condition of the computer system, storage media, electronic devices and conventional evidence, including power status of the computer

D. Write down the color of shirt and pant the suspect was wearing

Correct Answer: D

QUESTION 5

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

A. FF D8 FF E0 00 10

B. FF FF FF FF FF FF

C. FF 00 FF 00 FF 00

D. EF 00 EF 00 EF 00

Correct Answer: A