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.leads4pass.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Graphics Interchange Format (GIF) is a _____RGB bitmap Image format for Images with up to 256 distinct colors per frame.

A. 8-bit

B. 16-bit

C. 24-bit

D. 32-bit

Correct Answer: A

QUESTION 2

To preserve digital evidence, an investigator should _____

A. Make two copies of each evidence item using a single imaging tool

B. Make a single copy of each evidence item using an approved imaging tool

C. Make two copies of each evidence item using different imaging tools

D. Only store the original evidence item

Correct Answer: C

QUESTION 3

Jones had been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the system for a period of three weeks. However law enforcement agencies were recording his every activity and this was later presented as evidence. The organization had used a virtual environment to trap Jones. What is a virtual environment?

A. A system using Trojaned commands

B. A honeypot that traps hackers

C. An environment set up after the user logs in

D. An environment set up before an user logs in

Correct Answer: B

QUESTION 4

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

D. Disk editor

Correct Answer: A

QUESTION 5

In Windows 7 system files, which file reads the Boot.ini file and loads Ntoskrnl.exe. Bootvid.dll. Hal.dll, and boot-start device drivers?

A. Ntldr

B. Gdi32.dll

C. Kernel32.dll

D. Boot.in

Correct Answer: A

EC1-349 PDF Dumps EC1-349 Exam Questions EC1-349 Braindumps