312-49Q&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.passapply.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

QUESTION 1

At what layer of the OSI model do routers function on?

A. 4

B. 3

C. 1

D. 5

Correct Answer: B

QUESTION 2

Which of the following is a device monitoring tool?

A. Capsa

B. Driver Detective

C. Regshot

D. RAM Capturer

Correct Answer: A

QUESTION 3

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

A. Globally unique ID

B. Microsoft Virtual Machine Identifier

C. Personal Application Protocol

D. Individual ASCII string

Correct Answer: A

QUESTION 4

Raw data acquisition format creates _____ of a data set or suspect drive.

A. Segmented image files

B. Simple sequential flat files

C. Compressed image files

D. Segmented files

Correct Answer: B

QUESTION 5

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Circuit-level proxy firewall

B. Packet filtering firewall

C. Application-level proxy firewall

D. Data link layer firewall

Correct Answer: C

QUESTION 6

Which of the following is NOT a physical evidence?

A. Removable media

B. Cables

C. Image file on a hard disk

D. Publications

Correct Answer: C

QUESTION 7

When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

A. Proxify.net

B. Dnsstuff.com

C. Samspade.org

D. Archive.org

Correct Answer: D

QUESTION 8

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

Correct Answer: ACDE

QUESTION 9

Which principle states that "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"?

A. Locard\\'s Exchange Principle

B. Enterprise Theory of Investigation

C. Locard\\'s Evidence Principle

D. Evidence Theory of Investigation

Correct Answer: A

QUESTION 10

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

A. the Microsoft Virtual Machine Identifier

B. the Personal Application Protocol

C. the Globally Unique ID

D. the Individual ASCII String

Correct Answer: C

QUESTION 11

When operating systems mark a cluster as used but not allocated, the cluster is considered as _____

A. Corrupt

B. Bad

C. Lost

D. Unallocated

Correct Answer: C

QUESTION 12

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on

B. Turn off the device immediately

C. Remove the battery immediately

D. Remove any memory cards immediately

Correct Answer: A

QUESTION 13

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A. Any data not yet flushed to the system will be lost

B. All running processes will be lost

C. The /tmp directory will be flushed

D. Power interruption will corrupt the pagefile

Correct Answer: A

QUESTION 14

What is the smallest physical storage unit on a hard drive?

A. Track

B. Cluster

C. Sector

D. Platter

Correct Answer: C

QUESTION 15

Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

A. Two

B. One

C. Three

D. Four

Correct Answer: A