DUMPSARENA

Computer Hacking Forensic Investigator (v9)

ECCouncil 312-49v9

Version Demo

Total Demo Questions: 12

Total Premium Questions: 547

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which US law does the interstate or international transportation and receiving of child pornography fall under?

A. §18. U.S.C. 1466A

B. §18. U.S.C 252

C. §18. U.S.C 146A

D. §18. U.S.C 2252

ANSWER: D

QUESTION NO: 2

Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

A. SWGDE & SWGIT

B. IOCE

C. Frye

D. Daubert

ANSWER: D

QUESTION NO: 3

What is the name of the first reserved sector in File allocation table?

A. Volume Boot Record

B. Partition Boot Sector

C. Master Boot Record

D. BIOS Parameter Block

ANSWER: C

QUESTION NO: 4

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

QUESTION NO: 5

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order

B. A text file deleted from C drive in fifth sequential order

C. A text file copied from D drive to C drive in fifth sequential order

D. A text file copied from C drive to D drive in fifth sequential order

ANSWER: B

QUESTION NO: 6

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a

denial-of-service attack?

A. Email spamming

B. Phishing

C. Email spoofing

D. Mail bombing

ANSWER: D

QUESTION NO: 7

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

ANSWER: A C D E

QUESTION NO: 8

You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

A. Net sessions

B. Net config

C. Net share

D. Net use

ANSWER: D

QUESTION NO: 9

An expert witness is a who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

A. Expert in criminal investigation

B. Subject matter specialist

C. Witness present at the crime scene

D. Expert law graduate appointed by attorney

ANSWER: B

QUESTION NO: 10

Which of the following should a computer forensics lab used for investigations have?

A. isolation

B. restricted access

C. open access

D. an entry log

ANSWER: B

QUESTION NO: 11

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

ANSWER: D

QUESTION NO: 12

Which code does the FAT file system use to mark the file as deleted?

A. ESH

B. 5EH

C. H5E

D. E5H

ANSWER: D