DUMPSQUEEN

Computer Hacking Forensic Investigator (CHFI-v10)

ECCouncil 312-49v10

Version Demo

Total Demo Questions: 12

Total Premium Questions: 714

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

What is the first step taken in an investigation for laboratory forensic staff members?

A. Packaging the electronic evidence

B. Securing and evaluating the electronic crime scene

C. Conducting preliminary interviews

D. Transporting the electronic evidence

ANSWER: B

QUESTION NO: 2

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS

B. Active IDS

C. Progressive IDS

D. NIPS

ANSWER: B

QUESTION NO: 3

Corporate investigations are typically easier than public investigations because:

A. the users have standard corporate equipment and software

B. the investigator does not have to get a warrant

C. the investigator has to get a warrant

D. the users can load whatever they want on their machines

ANSWER: B

QUESTION NO: 4

A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

A. Class B

B. Class D

C. Class C

D. Class A

ANSWER: C

Explanation:

Reference: http://www.ilpi.com/safety/extinguishers.html

QUESTION NO: 5

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: 6

What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda

B. hdd

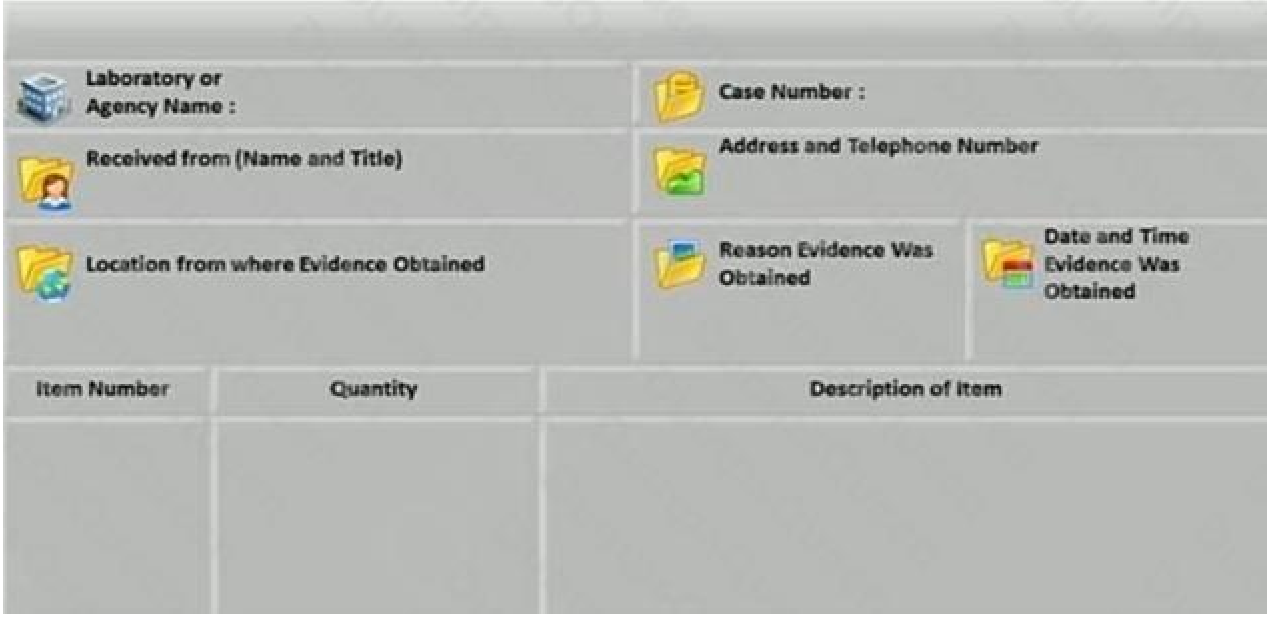
C. hdb

D. hdc

ANSWER: B

QUESTION NO: 7

What document does the screenshot represent?



Laboratory or Agency Name :

Case Number :

Received from (Name and Title)

Address and Telephone Number

Location from where Evidence Obtained

Reason Evidence Was Obtained

Date and Time Evidence Was Obtained

Item Number	Quantity	Description of Item

A. Expert witness form

B. Search warrant form

C. Chain of custody form

D. Evidence collection form

ANSWER: D

QUESTION NO: 8

The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A. Detection

B. Hearsay

C. Spoliation

D. Discovery

ANSWER: D

QUESTION NO: 9

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

A. filecache.db

B. config.db

C. sigstore.db

D. Sync_config.db

ANSWER: D

QUESTION NO: 10

Which part of the Windows Registry contains the user's password file?

A. HKEY_LOCAL_MACHINE

B. HKEY_CURRENT_CONFIGURATION

C. HKEY_USER

D. HKEY_CURRENT_USER

ANSWER: A

QUESTION NO: 11

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: 12

______allows a forensic investigator to identify the missing links during investigation.

A. Evidence preservation

B. Chain of custody

C. Evidence reconstruction

D. Exhibit numbering

ANSWER: B