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.pass4itsure.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

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in an approved secure container because they are now primary evidence in the case.

B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.

C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.

D. All forms should be placed in the report file because they are now primary evidence in the case.

Correct Answer: B

QUESTION 2

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System

B. ReFS

C. exFAT

D. NTFS File System

Correct Answer: D

QUESTION 3

Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

A. Identifying File Dependencies

B. Strings search

C. Dynamic analysis

D. File obfuscation

Correct Answer: B

QUESTION 4

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL

B. Surface Manager

C. Media framework

D. WebKit

Correct Answer: A

QUESTION 5

What does the 56.58.152.114(445) denote in a Cisco router log? Jun 19 23:25:46.125 EST: %SEC-4-IPACCESSLOGP: list internet-inbound denied udp 67.124.115.35 (8084) -> 56.58.152.114(445), 1 packet

A. Source IP address

B. None of the above

C. Login IP address

D. Destination IP address

Correct Answer: D

QUESTION 6

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

A. Civil Investigation

B. Administrative Investigation

C. Both Civil and Criminal Investigations

D. Criminal Investigation

Correct Answer: B

QUESTION 7

What layer of the OSI model do TCP and UDP utilize?

A. Data Link

B. Network

C. Transport

D. Session

Correct Answer: C

QUESTION 8

Madison is on trial for allegedly breaking into her university internal network. The police raided her dorm room and seized all of her computer equipment. Madison lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison lawyer trying to prove the police violated?

A. The 10th Amendment

B. The 5th Amendment

C. The 1st Amendment

D. The 4th Amendment

Correct Answer: D

QUESTION 9

Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then

discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A. Phreaking

B. Squatting

C. Crunching

D. Pretexting

Correct Answer: A

QUESTION 10

In a FAT32 system, a 123 KB file will use how many sectors?

A. 34

B. 25

C. 11

D. 56

Correct Answer: B

QUESTION 11

Where is the startup configuration located on a router?

A. Static RAM

B. BootROM

C. NVRAM

D. Dynamic RAM

Correct Answer: C

QUESTION 12

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

A. IDS attack

B. APT

C. Web application attack

D. Network attack

Correct Answer: D

QUESTION 13

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A. a write-blocker

B. a protocol analyzer

C. a firewall

D. a disk editor

Correct Answer: A

QUESTION 14

When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred

B. If employees do not care for their boss management techniques

C. If sales drop off for no apparent reason for an extended period of time

D. If a financial institution is burglarized by robbers

Correct Answer: A

QUESTION 15

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