100% Money Back Guarantee

Vendor:EC-COUNCIL

Exam Code:EC0-349

Exam Name: Computer Hacking Forensic Investigator

Version: Demo

QUESTION 1

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

A. 18 U.S.C. 1029 Possession of Access Devices

B. 18 U.S.C. 1030 Fraud and related activity in connection with computers

C. 18 U.S.C. 1343 Fraud by wire, radio or television

D. 18 U.S.C. 1361 Injury to Government Property

E. 18 U.S.C. 1362 Government communication systems

F. 18 U.S.C. 1831 Economic Espionage Act

G. 18 U.S.C. 1832 Trade Secrets Act

Correct Answer: B

QUESTION 2

Area density refers to:

A. the amount of data per disk

B. the amount of data per partition

C. the amount of data per square inch

D. the amount of data per platter

Correct Answer: A

QUESTION 3

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

A. The ISP can investigate anyone using their service and can provide you with assistance

B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C. The ISP can\\'t conduct any type of investigations on anyone and therefore can\\'t assist you

D. ISP\\'s never maintain log files so they would be of no use to your investigation

Correct Answer: B

QUESTION 4

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

Correct Answer: B

QUESTION 5

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

A. Civil litigation testimony

B. Expert testimony

C. Victim advocate testimony

D. Technical testimony

Correct Answer: D

QUESTION 6

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network

B. Satellite television

C. 2.4Ghz Cordless phones

D. CB radio

Correct Answer: C

QUESTION 7

An on-site incident response team is called to investigate an alleged case of computer tampering within their company.

Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

A. One working day

B. Two working days

C. Immediately

D. Four hours

Correct Answer: A

QUESTION 8

Why should you never power on a computer that you need to acquire digital evidence from?

A. When the computer boots up, files are written to the computer rendering the data nclean

B. When the computer boots up, the system cache is cleared which could destroy evidence

C. When the computer boots up, data in the memory buffer is cleared which could destroy evidence

D. Powering on a computer has no affect when needing to acquire digital evidence from it

Correct Answer: A

QUESTION 9

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

A. one who has NTFS 4 or 5 partitions

B. one who uses dynamic swap file capability

C. one who uses hard disk writes on IRQ 13 and 21

D. one who has lots of allocation units per block or cluster

Correct Answer: D

QUESTION 10

When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?

A. 202

B. 404

C. 606

D. 999

Correct Answer: B

QUESTION 11

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues

B. Avoid over-saturation of wireless signals

C. So that the access points will work on different frequencies

D. Avoid cross talk

Correct Answer: D

QUESTION 12

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