EC0-349

EC-Council Computer Hacking Forensic Investigator

DEMO

QUESTION NO: 1

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

A. evidence procedures are not important unless you work for a law enforcement agency
B. evidence must be handled in the same way regardless of the type of case
C. evidence in a civil case must be secured more tightly than in a criminal case
D. evidence in a criminal case must be secured more tightly than in a civil case

Answer: B

QUESTION NO: 2

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: C

QUESTION NO: 3

If a suspect's computer is located in an area that may have toxic chemicals, you must

A. coordinate with the HAZMAT team
B. do not enter alone
C. assume the suspect machine is contaminated
D. determine a way to obtain the suspect computer

Answer: A

QUESTION NO: 4

Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their pervious activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

A. The vulnerability exploited in the incident
B. The manufacture of the system compromised

C. The nature of the attack
D. The logic, formatting and elegance of the code used in the attack

Answer: D

QUESTION NO: 5

What information do you need to recover when searching a victims computer for a crime committed with specific e-mail message?

A. Username and password
B. Firewall log
C. E-mail header
D. Internet service provider information

Answer: C

QUESTION NO: 6

The use of warning banners helps a company avoid litigation by overcoming an employees assumed ____________________ when connecting to the companys intranet, network, or virtual private network (VPN) and will allow the companys investigators to monitor, search, and retrieve information stored within the network.

A. right of privacy
B. right to Internet access
C. right to work
D. right of free speech

Answer: A

QUESTION NO: 7

When examining a hard disk without a write-blocker, you should not start Windows because Windows will write data to the:

A. Case files
B. Recycle Bin
C. BIOS
D. MSDOS.SYS

Answer: B

QUESTION NO: 8

How many sectors will a 125 KB file use in a FAT32 file system?

A. 16
B. 25
C. 256
D. 32

Answer: C

QUESTION NO: 9

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

A. HKEY_CURRENT_CONFIGURATION
B. HKEY_USER
C. HKEY_CURRENT_USER
D. HKEY_LOCAL_MACHINE

Answer: B

QUESTION NO: 10

You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a simple backup copy of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a simple backup copy will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?

A. incremental backup copy
B. full backup copy
C. robust copy
D. bit-stream copy