EC-Council Security Awareness

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(s): B

---

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(s): C

---

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(s): A

---

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(s): D

---

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(s): C

---

6. The use of warning banners helps a company avoid litigation by overcoming an employees assumed _____when connecting to the company’s intranet, network, or virtual private network (VPN) and will allow the company’s 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(s): A

---

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(s): B

---

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

A. 16

B. 25

C. 256

D. 32

Answer(s): C

---

9. 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

Answer(s): D

---

10. A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists, and the evidence of the specific crime exists at the place to be searched.

A. probable cause

B. a preponderance of the evidence

C. mere suspicion

D. beyond a reasonable doubt

Answer(s): A

---

11. To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

A. Association of Computer Forensics Software Manufactures (ACFSM)

B. Computer Forensics Tools Validation Committee (CFTVC)

C. National Institute of Standards and Technology (NIST)

D. Society for Valid Forensics Tools and Testing (SVFTT)

Answer(s): C

---

12. When investigating a Windows system, it is important to view the contents of the "page" or "swap" file because:

A. Windows stores all of the systems configuration information in this file

B. a large volume of data can exist within the swap file of which the computer user has no knowledge

C. this is the file that Windows uses to store the history of the last 100 commands that were run from the command line

D. this is the file that Windows uses to communicate directly with the Registry

Answer(s): B

---

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

A. a disk editor

B. a firewall

C. a write-blocker

D. a protocol analyzer

Answer(s): C

---

14. If you plan to startup a suspect's computer, you must modify the _____to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

A. CMOS

B. Boot.sys

C. deltree command

D. Scandisk utility

Answer(s): A

---

15. When obtaining a warrant it is important to:

A. particularly describe the place to be searched and particularly describe the items to be seized

B. particularly describe the place to be searched and generally describe the items to be seized

C. generally describe the place to be searched and particularly describe the items to be seized

D. generally describe the place to be searched and generally describe the items to be seized

Answer(s): A

---

16. Printing under a windows computer normally requires which one of the following files types to be created?

A. EME

B. CME

C. MEM

D. EMF

Answer(s): D

17. When you carve an image, recovering the image depends on which of the following skills?

A. recognizing the pattern of the header content

B. recognizing the pattern of the data content

C. recognizing the pattern of a corrupt file

D. recovering the image from a tape backup

Answer(s): A

---

18. What does the superblock in Linux define?

A. location of the firstinode

B. file system names

C. available space

D. disk geometry

Answer(s): A

---

19. You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

A. copyright law

B. IP Law

C. patent law

D. trademark law

Answer(s): A

---

20. Which of the following is NOT a graphics file?

A. Picture3.nfo

B. Picture2.bmp

C. Picture1.tga

D. Picture4.psd

Answer(s): A
