



Exam Code: ec0-349

Exam Name: Computer Hacking Forensic Investigator

Vendor: EC-Council

Version: DEMO

1: What is the last bit of each pixel byte in an image called?

- A.Last significant bit
- B.Least significant bit
- C.Least important bit
- D.Null bit

Correct Answers: B

2: Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

- A.Point-to-point
- B.End-to-end
- C.Thorough
- D.Complete event analysis

Correct Answers: B

3: When a router receives an update for its routing table, what is the metric value change to that path?

- A.Increased by 2
- B.Decreased by 1
- C.Increased by 1
- D.Decreased by 2

Correct Answers: C

4: Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

- A.Search warrant
- B.Subpoena
- C.Wire tap
- D.Bench warrant

Correct Answers: A

5: What hashing method is used to password protect Blackberry devices?

- A.AES
- B.RC5
- C.MD5
- D.SHA-1

Correct Answers: D

6: 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.Bit-stream copy
- B.Robust copy
- C.Full backup copy
- D.Incremental backup copy

Correct Answers: A

7: 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 the 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 cannot conduct any type of investigations on anyone and therefore cannot assist you
- D.ISPs never maintain log files so they would be of no use to your investigation

Correct Answers: B

8: The efforts to obtain information before a trial by demanding documents, depositions, questions 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

Correct Answers: D

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

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

Correct Answers: B

10: A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

- A.Blu-Ray single-layer
- B.HD-DVD
- C.Blu-Ray dual-layer
- D.DVD-18

Correct Answers: C

11: Sectors in hard disks typically contain how many bytes?

- A.256
- B.512
- C.1024
- D.2048

Correct Answers: B

12: A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.

- A.Image the disk and try to recover deleted files
- B.Seek the help of co-workers who are eye-witnesses
- C.Check the Windows registry for connection data (You may or may not recover)
- D.Approach the websites for evidence

Correct Answers: A

13: In the following Linux command, what is the outfile?

```
dd if=/usr/bin/personal/file.txt of=/var/bin/files/file.txt
```

- A./usr/bin/personal/file.txt
- B./var/bin/files/file.txt
- C./bin/files/file.txt
- D.There is not outfile specified

Correct Answers: B

14: What will the following Linux command accomplish?

```
dd if=/dev/mem of=/home/sam/mem.bin bs=1024
```

- A.Copy the master boot record to a file
- B.Copy the contents of the system folder mem to a file
- C.Copy the running memory to a file
- D.Copy the memory dump file to an image file

Correct Answers: C

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

- A.The 10th Amendment
- B.The 5th Amendment
- C.The 1st Amendment
- D.The 4th Amendment

Correct Answers: D