EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **EC0-349**

Title : Computer Hacking Forensic Investigator

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
Answer: 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
Answer: 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
Answer: 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
Answer: A

5. What hashing method is used to password protect Blackberry devices?
A.AES
B.RC5
C.MD5
D.SHA-1
Answer: 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
Answer: 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 ustomers 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
Answer: 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
Answer: 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
Answer: 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
Answer: C

11. Sectors in hard disks typically contain how many bytes?
A.256
B.512
C.1024
D.2048
Answer: 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
Answer: 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
Answer: 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
Answer: C

15. Madison is on trial for allegedly breaking into her universitys internal network. The police raided her dorm room and seized all of her computer equipment. Madisons lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madisons lawyer trying to prove the police violated?
A.The 10th Amendment

B.The 5th Amendment
C.The 1st Amendment
D.The 4th Amendment
Answer: D

16. While searching through a computer under investigation, you discover numerous files that appear to have had
the first letter of the file name replaced by
the hex code byte E5h. What does this indicate on the computer?
A.The files have been marked as hidden
B.The files have been marked for deletion
C.The files are corrupt and cannot be recovered
D.The files have been marked as read-only
Answer: B

17. Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?
A.The data is still present until the original location of the file is used
B.The data is moved to the Restore directory and is kept there indefinitely
C.The data will reside in the L2 cache on a Windows computer until it is manually deleted
D.It is not possible to recover data that has been emptied from the Recycle Bin
Answer: A

18. A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?
A.He should search in C:\Windows\System32\RECYCLED folder
B.The Recycle Bin does not exist on the hard drive
C.The files are hidden and he must use a switch to view them
D.Only FAT system contains RECYCLED folder and not NTFS
Answer: C

19. When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?
A.All virtual memory will be deleted
B.The wrong partition may be set to active
C.This action can corrupt the disk
D.The computer will be set in a constant reboot state
Answer: C

20. A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The pictures quality is not degraded at all from this process. What kind of picture is this file?
A.Raster image

B.Vector image
C.Metafile image
D.Catalog image
Answer: B