Eccouncil

EC1-349 Exam

Computer Hacking Forensic Investigator

Question: 1

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on
B. Turn off the device immediately
C. Remove the battery immediately
D. Remove any memory cards immediately

Answer: A

Question: 2

What hashing method is used to password protect Blackberry devices?

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

Answer: D

Question: 3

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry
B. The swapfile
C. The recycle bin
D. The metadata

Answer: B

Question: 4

With regard to using an antivirus scanner during a computer forensics investigation, you should:

A. Scan the suspect hard drive before beginning an investigation
B. Never run a scan on your forensics workstation because it could change your system configurationNever run a scan on your forensics workstation because it could change your system?

configuration
C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
D. Scan your forensics workstation before beginning an investigation

Answer: D

Question: 5

What layer of the OSI model do TCP and UDP utilize?

A. Data Link
B. Network
C. Transport
D. Session

Answer: C

Question: 6

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. One
B. Two
C. Three
D. Four

Answer: B

Question: 7

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. On the individual computer ARP cacheOn the individual computer? ARP cache
B. In the Web Server log files
C. In the DHCP Server log files
D. There is no way to determine the specific IP address

Answer: C

Question: 8

What type of equipment would a forensics investigator store in a StrongHold bag?

A. PDAPDA?
B. Backup tapes
C. Hard drives
D. Wireless cards

Answer: D

Question: 9

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

A. Write-blocker
B. Protocol analyzer
C. Firewall
D. Disk editor

Answer: A

Question: 10

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

A. Lossful compression
B. Lossy compression
C. Lossless compression
D. Time-loss compression

Answer: B

Question: 11

When marking evidence that has been collected with the aa/ddmmyy/nnnn/zz?format, what does the nnn?denote?When marking evidence that has been collected with the ?aa/ddmmyy/nnnn/zz?format, what does the ?nnn?denote?

A. The year the evidence was taken
B. The sequence number for the parts of the same exhibit
C. The initials of the forensics analyst
D. The sequential number of the exhibits seized

Answer: D

Question: 12

You are working in the Security Department of a law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is a possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?fake email to the attorney that appears to come from his boss. What port do you send the email to on the company? SMTP server?

A. 10
B. 25
C. 110
D. 135

Answer: B

Question: 13

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

Question: 14

An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A. Smurf
B. Ping of death
C. Fraggle
D. Nmap scan

Answer: B

Question: 15

What type of file is represented by a colon (:) with a name following it in the Master File Table (MFT) of an NTFS disk?

A. Compressed file
B. Data stream file
C. Encrypted file
D. Reserved file

Answer: B

Question: 16

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

Question: 17

When using an iPod and the host computer is running Windows, what file system will be used?

A. iPod+
B. HFS
C. FAT16
D. FAT32

Answer: D

Question: 18

What is one method of bypassing a system BIOS password?

A. Removing the processor
B. Removing the CMOS battery
C. Remove all the system memoryRemove all the system? memory
D. Login to Windows and disable the BIOS password

Answer: B

Thank You for trying EC1-349 PDF Demo

To Buy Latest EC1-349 Full Version Download visit link below

https://www.certkillers.net/Exam/EC1-349

Start Your EC1-349 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your EC1-349 preparation with actual exam questions.