Vendor: ECCouncil

Exam Code: EC1-349

Exam Name: Computer Hacking Forensic Investigator Exam

Version: Demo

QUESTION 1
What is the First Step required in preparing a computer for forensics investigation?

A. Do not turn the computer off or on, run any programs, or attempt to access data on a computer
B. Secure any relevant media
C. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
D. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Correct Answer: A

QUESTION 2
Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

A. True
B. False

Correct Answer: A

QUESTION 3
Which of the following commands shows you the names of all open shared files on a server and number of file locks on each file?

A. Net sessions
B. Net file
C. Netconfig
D. Net share

Correct Answer: B

QUESTION 4
The Recycle Bin exists as a metaphor for throwing files away, but it also allows user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin.

Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

A. INFO2 file
B. INFO1 file
C. LOGINFO2 file
D. LOGINFO1 file

Correct Answer: A

QUESTION 5
Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
B. Local archives do not have evidentiary value as the email client may alter the message data
C. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
D. Server storage archives are the server information and settings stored on a local system whereas the

local archives are the local email client information stored on the mail server

Correct Answer: A

QUESTION 6
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

A. Errors-To header
B. Content-Transfer-Encoding header
C. Mime-Version header
D. Content-Type header

Correct Answer: A

QUESTION 7
Which of the following commands shows you all of the network services running on Windows-based servers?

A. Net start
B. Net use
C. Net Session
D. Net share

Correct Answer: A

QUESTION 8
Email archiving is a systematic approach to save and protect the data contained in emails so that it can tie easily accessed at a later date.

A. True
B. False

Correct Answer: A

QUESTION 9
Which of the following commands shows you the NetBIOS name table each?

a. nbtstst 束
b. nbtstst 札
c. nbtstst 朾
d. nbtstst 朴

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: A

QUESTION 10
Windows Security Accounts Manager (SAM) is a registry file which stores passwords in a hashed format.

SAM file in Windows is located at:

A. C:\windows\system32\config\SAM
B. C:\windows\system32\con\SAM
C. C:\windows\system32\Boot\SAM
D. C:\windows\system32\drivers\SAM

Correct Answer: A

QUESTION 11
FAT32 is a 32-bit version of FAT file system using smaller clusters and results in efficient storage capacity. What is the maximum drive size supported?

A. 1 terabytes
B. 2 terabytes
C. 3 terabytes
D. 4 terabytes

Correct Answer: B

QUESTION 12
In which step of the computer forensics investigation methodology would you run MD5 checksum on the evidence?

A. Obtain search warrant
B. Evaluate and secure the scene
C. Collect the evidence
D. Acquire the data

Correct Answer: D

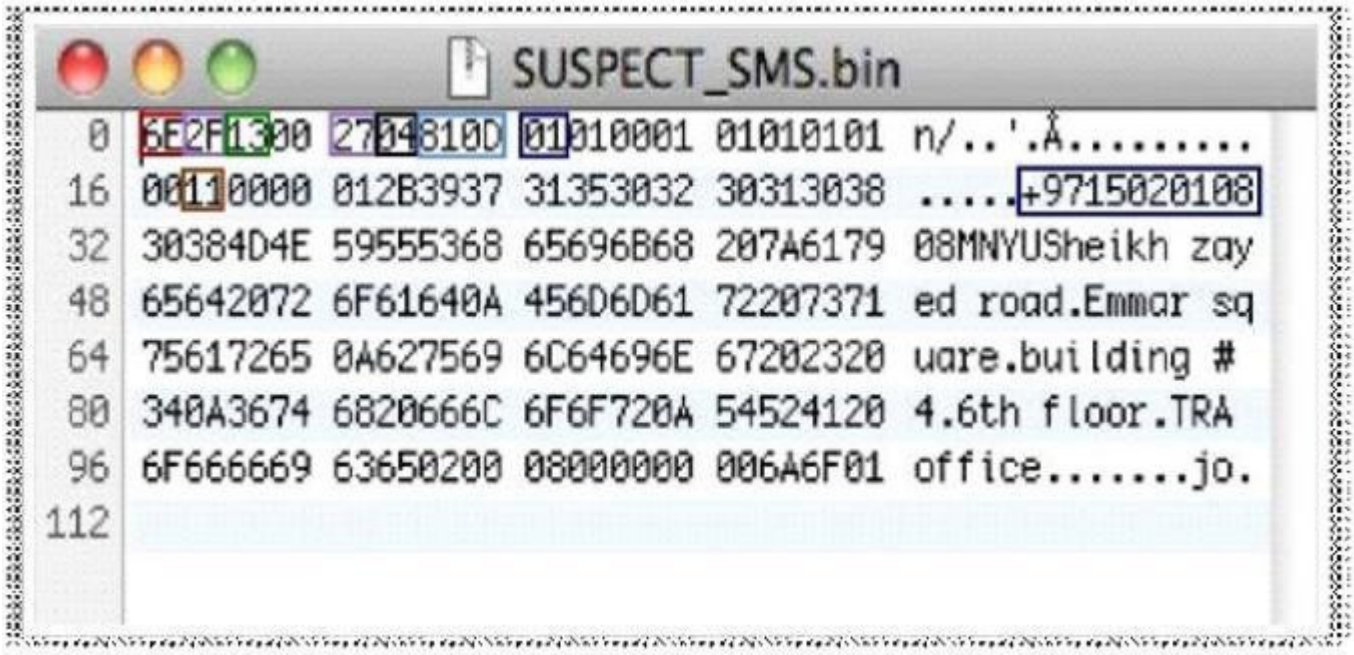
QUESTION 13
Network forensics allows Investigators 10 inspect network traffic and logs to identify and locate the attack system

Network forensics can reveal: (Select three answers)

A. Source of security incidents' and network attacks
B. Path of the attack
C. Intrusion techniques used by attackers
D. Hardware configuration of the attacker's system

Correct Answer: ABC

QUESTION 14
Determine the message length from following hex viewer record:



A. 6E2F
B. 13
C. 27
D. 810D

Correct Answer: D

QUESTION 15
TCP/IP (Transmission Control Protocol/Internet Protocol) is a communication protocol used to connect different hosts in the Internet. It contains four layers, namely the network interface layer. Internet layer, transport layer, and application layer.

Which of the following protocols works under the transport layer of TCP/IP?

A. UDP
B. HTTP
C. FTP
D. SNMP

Correct Answer: A

QUESTION 16
Which of the following statements does not support the case assessment?

A. Review the case investigator's request for service
B. Identify the legal authority for the forensic examination request
C. Do not document the chain of custody
D. Discuss whether other forensic processes need to be performed on the evidence

Correct Answer: C

QUESTION 17
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls.

Which of the following wireless access control attacks allows the attacker to set up a rogue access point outside the corporate perimeter, and then lure the employees of the organization to connect to it?

A. War driving
B. Rogue access points
C. MAC spoofing
D. Client mis-association

Correct Answer: D

QUESTION 18
File deletion is a way of removing a file from a computer's file system. What happens when a file is deleted in windows7?

A. The last letter of a file name is replaced by a hex byte code E5h
B. The operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted
C. Corresponding clusters in FAT are marked as used
D. The computer looks at the clusters occupied by that file and does not avails space to store a new file

Correct Answer: B

QUESTION 19
What is cold boot (hard boot)?

A. It is the process of starting a computer from a powered-down or off state
B. It is the process of restarting a computer that is already turned on through the operating system
C. It is the process of shutting down a computer from a powered-on or on state
D. It is the process of restarting a computer that is already in sleep mode

Correct Answer: A

QUESTION 20
When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called "INF02" in the Recycled folder. If the INF02 file is deleted, it is re-created when you_____.

A. Restart Windows
B. Kill the running processes in Windows task manager
C. Run the antivirus tool on the system
D. Run the anti-spyware tool on the system

Correct Answer: A

QUESTION 21
WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?

A. RC4-CCMP
B. RC4-TKIP
C. AES-CCMP
D. AES-TKIP

Correct Answer: C

QUESTION 22
The disk in the disk drive rotates at high speed, and heads in the disk drive are used only to read data.

A. True
B. False

Correct Answer: B

QUESTION 23
What is a bit-stream copy?

A. Bit-Stream Copy is a bit-by-bit copy of the original storage medium and exact copy of the original disk
B. A bit-stream image is the file that contains the NTFS files and folders of all the data on a disk or partition
C. A bit-stream image is the file that contains the FAT32 files and folders of all the data on a disk or partition
D. Creating a bit-stream image transfers only non-deleted files from the original disk to the image disk

Correct Answer: A

QUESTION 24
System software password cracking is defined as cracking the operating system and all other utilities that enable a computer to function

A. True
B. False

Correct Answer: A

QUESTION 25
Which of the following Steganography techniques allows you to encode information that ensures creation of cover for secret communication?

A. Substitution techniques
B. Transform domain techniques
C. Cover generation techniques
D. Spread spectrum techniques

Correct Answer: C

QUESTION 26
Ron. a computer forensics expert, Is Investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in on condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations he can use to recover the IMEI number?

A. #*06*#
B. *#06#
C. #06r
D. *1MEI#

Correct Answer: B

QUESTION 27
Who is responsible for the following tasks?

A. Non-Laboratory Staff
B. System administrators
C. Local managers or other non-forensic staff
D. Lawyers

Correct Answer: A

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

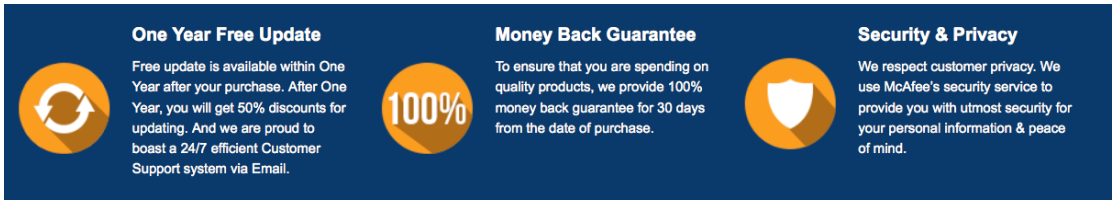
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions