Eccouncil

312-49V8 Exam

Computer Hacking Forensic Investigator v8

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

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

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

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

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

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

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

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

Answer: A

Question: 9

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

A. nbtstat -n
B. nbtstat -c
C. nbtstat -r
D. nbtstat -s

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

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

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

Answer: D

Question: 13

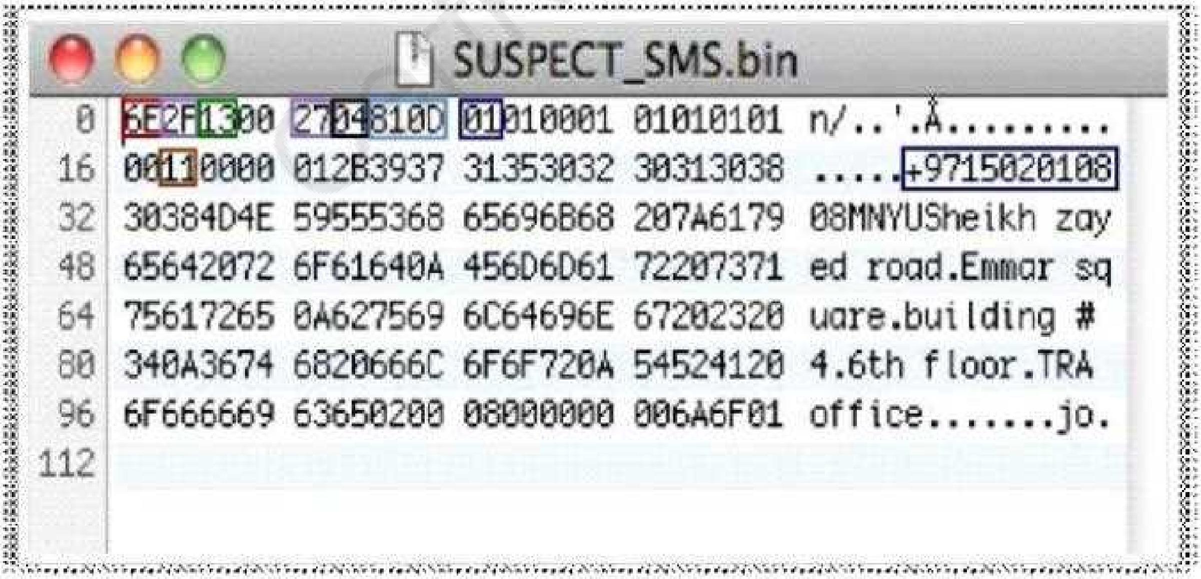
Network forensics allows Investigators to inspect network traffic and logs to identify and locate the attack system. Network forensics can reveal: (Select three answers)

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

Answer: A, B, C

Question: 14

Determine the message length from following hex viewer record:



```
  0 6E2F1300 2704810D 01010001 01010101 n/..'.Å.........
 16 00110000 012B3937 31353032 30313038 .....+9715020108
 32 30384D4E 59555368 65696B68 207A6179 08MNYUSheikh zay
 48 65642072 6F61640A 456D6D61 72207371 ed road.Emmar sq
 64 75617265 0A627569 6C64696E 67202320 uare.building #
 80 340A3674 6820666C 6F6F720A 54524120 4.6th floor.TRA
 96 6F666669 63650200 08000000 006A6F01 office.......jo.
112
```

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

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

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

Answer: C