ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: GAQM

Code: CFA-001

Exam: Certified Forensic Analyst (CFA)

https://www.examsnest.com/exam/cfa-001/

QUESTIONS & ANSWERS

DEMO VERSION

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

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: GAQM

Code: CFA-001

Exam: Certified Forensic Analyst (CFA)

https://www.examsnest.com/exam/cfa-001/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation