GCFA Q&As

GIAC Certified Forensics Analyst

Pass GIAC GCFA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gcfa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Which of the following data is NOT listed as a volatile data in RFC 3227 list for Windows based system?

A. Kernel statistics

B. Temporary file system

C. Data on a hard disk

D. Routing table

Correct Answer: C

QUESTION 2

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

A. Chain of evidence

B. Chain of custody

C. Incident response policy

D. Evidence access policy

Correct Answer: B

QUESTION 3

Which of the following statements about the compression feature of the NTFS file system are true?

Each correct answer represents a complete solution. Choose two.

A. Users can work with NTFS-compressed files without decompressing them.

B. It supports compression only on volumes.

C. Compressed files on an NTFS volume can be read and written by any Windows-based application after they are decompressed.

D. It supports compression on volumes, folders, and files.

Correct Answer: AD

QUESTION 4

Sandra wants to create a full system state backup of her computer, which is running on Microsoft Windows XP operating system. Which of the following is saved in full state system backup? Each correct answer represents a

complete solution. Choose all that apply.

A. file system information

B. Registry

C. Windows boot files

D. Active Directory (NTDS)

Correct Answer: BCD

QUESTION 5

What is the name of the group of blocks which contains information used by the operating system in Linux system?

A. logblock

B. Systemblock

C. Bootblock

D. Superblock

Correct Answer: D