



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.geekcert.com/gcfa.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with a project to investigate a computer in the network of SecureEnet Inc. The compromised system runs on Windows operating system. Adam decides to use Helix Live for Windows to gather data and electronic evidences starting with retrieving volatile data and transferring it to server component via TCP/IP. Which of the following application software in Helix Windows Live will he use to retrieve volatile data and transfer it to the server component via TCP/IP?

- A. FSP
- B. Drive Manager
- C. FTK imager
- D. FAU

Correct Answer: A

QUESTION 2

Which of the following wireless network standards operates on the 5 GHz band and transfers data at a rate of 54 Mbps?

- A. 802.11a
- B. 802.11u
- C. 802.11g
- D. 802.11b

Correct Answer: A

QUESTION 3

Which of the following Windows XP system files handles memory management, I/O operations, and interrupts?

- A. Ntoskrnl.exe
- B. Win32k.sys
- C. Advapi32.dll
- D. Kernel32.dll

Correct Answer: D



QUESTION 4

An organization wants to mitigate the risks associated with the lost or stolen laptops and the associated disclosure laws, while reporting data breaches. Which of the following solutions will be best for the organization?

- A. Hashing function
- B. Digital signature
- C. Trusted Platform Module
- D. Whole disk encryption

Correct Answer: D

QUESTION 5

Which of the following files in LILO booting process of Linux operating system stores the location of Kernel on the hard drive?

- A. /boot/map
- B. /boot/boot.b
- C. /etc/lilo.conf
- D. /sbin/lilo

Correct Answer: A

[Latest GCFA Dumps](#)

[GCFA Practice Test](#)

[GCFA Exam Questions](#)