



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

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





QUESTION 1

Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?

- A. Melissa
- B. Tequila
- C. Brain
- D. I love you

Correct Answer: C

QUESTION 2

Nathan works as a Computer Hacking Forensic Investigator for SecureEnet Inc. He uses Visual TimeAnalyzer software to track all computer usage by logging into individual users account or specific projects and compile detailed accounts of time spent within each program. Which of the following functions are NOT performed by Visual TimeAnalyzer?

Each correct answer represents a complete solution. Choose all that apply.

- A. It monitors all user data such as passwords and personal documents.
- B. It gives parents control over their children's use of the personal computer.
- C. It tracks work time, pauses, projects, costs, software, and internet usage.
- D. It records specific keystrokes and run screen captures as a background process.

Correct Answer: AD

QUESTION 3

You want to upgrade a partition in your computer's hard disk drive from FAT to NTFS. Which of the following DOS commands will you use to accomplish this?

- A. FORMAT C: /s
- B. CONVERT C: /fs:ntfs
- C. SYS C:
- D. FDISK /mbr

Correct Answer: B



QUESTION 4

Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer. After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting. for ((i = 0;i