GIAC GCFA

GIAC Forensic Analyst Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

GCFA

GIAC Certified Forensic Analyst (GCFA)

82-115 Questions Exam – 72% Cut Score – Duration of 180 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the GCFA Certification

Are you interested in passing the GIAC GCFA exam? First discover, who benefits from the GCFA certification. The GCFA is suitable for a candidate if he wants to learn about Incident Response and Forensics. Passing the GCFA exam earns you the GIAC Certified Forensic Analyst (GCFA) title.

While preparing for the GCFA exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The GCFA PDF contains some of the most valuable preparation tips and the details and instant access to useful **GCFA study materials just at one click.**

GCFA GIAC Forensic Analyst Certification Details:

Exam Name	GIAC Certified Forensic Analyst (GCFA)
Exam Code	GCFA
Exam Price	$2499 (USD)
Duration	180 mins
Number of Questions	82-115
Passing Score	72%
Books / Training	FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
Schedule Exam	Pearson VUE
Sample Questions	GIAC GCFA Sample Questions
Practice Exam	**GIAC GCFA Certification Practice Exam**

GCFA Syllabus:

Topic	**Details**
Enterprise Environment Incident Response	- The candidate will demonstrate an understanding of the steps of the incident response process, attack progression, and adversary fundamentals and how to rapidly assess and analyze systems in an enterprise environment scaling tools to meet the demands of large investigations.

Topic	Details
File System Timeline Artifact Analysis	- The candidate will demonstrate an understanding of the Windows filesystem time structure and how these artifacts are modified by system and user activity.
Identification of Malicious System and User Activity	- The candidate will demonstrate an understanding of the techniques required to identify and document indicators of compromise on a system, detect malware and attacker tools, attribute activity to events and accounts, and identify and compensate for anti-forensic actions using memory and disk resident artifacts.
Identification of Normal System and User Activity	- The candidate will demonstrate an understanding of the techniques required to identify, document, and differentiate normal and abnormal system and user activity using memory and disk resident artifacts.
Introduction to File System Timeline Forensics	- The candidate will demonstrate an understanding of the methodology required to collect and process timeline data from a Windows system.
Introduction to Volatile Data Forensics	- The candidate will demonstrate an understanding of how and when to collect volatile data from a system and how to document and preserve the integrity of volatile evidence.
NTFS Artifact Analysis	- The candidate will demonstrate an understanding of core structures of the Windows filesystems, and the ability to identify, recover, and analyze evidence from any file system layer, including the data storage layer, metadata layer, and filename layer.
Volatile Data Artifact Analysis of Malicious Events	- The candidate will demonstrate an understanding of abnormal activity within the structure of Windows memory and be able to identify artifacts such as malicious processes, suspicious drivers and malware techniques such as code injection and rootkits.
Volatile Data Artifact Analysis of Windows Events	- The candidate will demonstrate an understanding of abnormal activity within the structure of Windows memory and be able to identify artifacts such as malicious processes, suspicious drivers and malware techniques such as code injection and rootkits.
Windows Artifact Analysis	- The candidate will demonstrate an understanding of Windows system artifacts and how to collect and analyze data such as system back up and restore data and evidence of application execution.

Broaden Your Knowledge with GIAC GCFA Sample Questions:

Question: 1

Which of the following file systems supports the hot fixing feature?

a) FAT16
b) exFAT
c) FAT32
d) NTFS

Answer: d

Question: 2

Which of the following statements about SD cards are true?

a) It is used with mobile phones and digital cameras.
b) It is a type of non-volatile memory card.
c) It is a 184-pin memory module.
d) It is used as RAM on client computers and servers.

Answer: a, b

Question: 3

Which of the following tools are used to determine the hop counts of an IP packet?

a) Netstat
b) TRACERT
c) IPCONFIG
d) Ping

Answer: b, d

Question: 4

What are the purposes of audit records on an information system?

a) Backup
b) Investigation
c) Upgradation
d) Troubleshooting

Answer: b, d

Question: 5

Which of the following directories cannot be placed out of the root filesystem?

a) /sbin
b) /etc
c) /var
d) /lib

Answer: a, b, d

Question: 6

In which of the following files does the Linux operating system store passwords?

a) Password
b) Passwd
c) Shadow
d) SAM

Answer: c

Question: 7

Which of the following types of virus makes changes to a file system of a disk?

a) Master boot record virus
b) Stealth virus
c) Cluster virus
d) Macro virus

Answer: c

Question: 8

Which of the following are the benefits of information classification for an organization?

a) It ensures that modifications are not made to data by unauthorized personnel or processes.
b) It helps identify which information is the most sensitive or vital to an organization.
c) It helps reduce the Total Cost of Ownership (TCO).
d) It helps identify which protections apply to which information.

Answer: b, d

Question: 9

In a Windows computer, which of the following utilities is used to convert a FAT16 partition to FAT32?

a) CVT16.EXE
b) CVT1.EXE
c) CONVERT16.EXE
d) CONVERT.EXE

Answer: b

Question: 10

You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

a) Netcraft
b) Ettercap
c) Ethereal
d) Nmap

Answer: a

Avail the Study Guide to Pass GCFA GIAC Forensic Analyst Exam:

- Find out about the GCFA syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **GCFA syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the GCFA training. Joining the GIAC provided training for GCFA exam helps a candidate to strengthen his practical knowledge base from the certification.

- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **GCFA sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. GCFA practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the GCFA exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the GCFA Certification

EduSum.Com is here with all the necessary details regarding the GCFA exam. We provide authentic practice tests for the GCFA exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **GCFA practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the GIAC Certified Forensic Analyst (GCFA).

Start Online Practice of GCFA Exam by visiting URL
https://www.edusum.com/giac/gcfa-giac-forensic-analyst