



GIAC GBFA STUDY GUIDE PDF

Grab the GIAC GBFA Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

GBFA

[GIAC Battlefield Forensics and Acquisition \(GBFA\)](#)

75 Exam Questions – 69% Cut Score – Duration of 120 minutes

Table of Contents:

Get an Overview of the GBFA Certification:	2
Why Should You Earn the GIAC GBFA Certification?	2
GIAC GBFA Exam Structure	2
Enhance Knowledge with GBFA Sample Questions:	3
What Study Guide Works Best in acing the GIAC GBFA Certification?	6
Explore the Syllabus Topics and Learn from the Core:	6
Make Your Schedule:	6
Get Expert Advice from the Training:	6
Get Access to the PDF Sample Questions:	6
Avoid Dumps and utilize the GIAC GBFA Practice Test:	7

Get an Overview of the GBFA Certification:

Who should take the [GBFA exam](#)? This is the first question that comes to a candidate's mind when preparing for the GBFA certification. The GBFA certification is suitable for candidates who are keen to earn knowledge on the Digital Forensics, Incident Response & Threat Hunting and grab their GIAC Battlefield Forensics and Acquisition (GBFA). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But GBFA study guide PDF is here to solve the problem. GBFA PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the GIAC GBFA Certification?

There are several reasons why one should grab the GBFA certification.

- The GBFA certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the GIAC Battlefield Forensics and Acquisition (GBFA) is a powerful qualification for a prosperous career.

GIAC GBFA Exam Structure

Exam Name	GIAC Battlefield Forensics and Acquisition (GBFA)
Exam Code	GBFA
Exam Price	\$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	69%
Books / Training	FOR498: Digital Acquisition and Rapid Triage
Schedule Exam	GIAC
Sample Questions	GIAC GBFA Sample Questions
Practice Exam	GIAC GBFA Certification Practice Exam

Enhance Knowledge with GBFA Sample Questions:

Question: 1

During an acquisition process, which of the following are essential to ensure the authenticity and integrity of macOS artifacts?

(Choose Three)

- a) Verifying the hash value of the acquired data.
- b) Using a certified USB cable.
- c) Documenting the process meticulously.
- d) Acquiring data in a forensically sound manner.
- e) Keeping the device charged during acquisition.

Answer: a, c, d

Question: 2

How do modern EXT filesystems, like EXT4, improve file system performance compared to earlier versions like EXT2?

- a) By eliminating the need for file defragmentation
- b) By using journaling to protect against corruption
- c) By supporting larger files and volumes
- d) By introducing a hierarchical directory structure

Answer: b

Question: 3

For acquiring RAM, which of the following approaches can be applied to a system running Linux?

(Choose Two)

- a) Use of /dev/mem
- b) Target Disk Mode
- c) Use of LiME
- d) Utilizing the dd command on /dev/mem

Answer: a, c

Question: 4

Why is it necessary to know the specific OS version of a mobile device during acquisition?

- a) To adjust the screen brightness correctly
- b) To ensure compatibility with the charging cable
- c) To determine the appropriate data acquisition method
- d) To choose the right color settings for the display

Answer: c

Question: 5

Which component within the NTFS file system is specifically designed to enhance data recovery capabilities?

- a) Volume Shadow Copy
- b) BitLocker
- c) Disk Quotas
- d) Transactional NTFS

Answer: a

Question: 6

When comparing physical storage devices, why is understanding the interface type important?

- a) It affects data transfer speeds and compatibility.
- b) It determines the device's color.
- c) It influences the device's physical dimensions.
- d) It dictates the device's operational noise.

Answer: a

Question: 7

What is a common purpose of acquiring Shadow Copies in a forensic investigation?

- a) To clean the disk
- b) To update the system
- c) To recover deleted files
- d) To analyze user activities

Answer: c

Question: 8

Regarding data encryption on drives, what is an important factor to consider for forensic analysis?

- a) The brand of the drive
- b) The encryption algorithm used
- c) The color of the drive LED
- d) The cable type connecting the drive

Answer: b

Question: 9

In an NTFS filesystem, which file attribute would you examine to understand more about a file's previous states or versions?

- a) \$STANDARD_INFORMATION
- b) \$FILE_NAME
- c) \$DATA
- d) \$LOGGED_UTILITY_STREAM

Answer: d

Question: 10

During a dead box acquisition, why is media removal an important step?

- a) To facilitate the device's recycling process
- b) To allow for the physical destruction of the media
- c) To examine the media independently of the original device
- d) To improve the aesthetic appeal of the device

Answer: c

What Study Guide Works Best in acing the GIAC GBFA Certification?

The GBFA study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the GBFA exam, getting in full touch of the [syllabus](#) is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the GIAC GBFA training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a PDF format or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the GIAC GBFA Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, GBFA practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven GBFA Practice Test for Success!!!

Do you want to pass the GBFA exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your GIAC Battlefield Forensics and Acquisition preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium [GBFA practice tests](#). Our expert-designed questions help you to improve performance and pass the exam on your first attempt.