EDUSUM

#1 Online Certification Guide

GIAC GBFA

GIAC Battlefield Forensics and Acquisition Certification Questions & Answers

Exam Summary – Syllabus –Questions

GBFA

GIAC Battlefield Forensics and Acquisition

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

Table of Contents:

Know Your GBFA Certification Well:

The GBFA is best suitable for candidates who want to gain knowledge in the GIAC Digital Forensics, Incident Response & Threat Hunting. Before you start your GBFA preparation you may struggle to get all the crucial GIAC Battlefield Forensics and Acquisition materials like GBFA syllabus, sample questions, study guide.

But don't worry the GBFA PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the GBFA syllabus?
- How many questions are there in the GBFA exam?
- Which Practice test would help me to pass the GBFA exam at the first attempt?

Passing the GBFA exam makes you GIAC Battlefield Forensics and Acquisition. Having the GIAC Battlefield Forensics and Acquisition certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GBFA GIAC Battlefield Forensics and Acquisition Certification Details:

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	**Pearson VUE**
Sample Questions	**GIAC GBFA Sample Questions**
Practice Exam	**GIAC GBFA Certification Practice Exam**

GBFA Syllabus:

Topic	Details
Acquiring RAM and OS Artifacts	- The candidate will be able to describe the different methods for performing acquisition of RAM, macOS and Shadow copies. This includes using disk copy utilities and target disk mode.
Acquisition Preparation	- The candidate will be able to summarize the goals of scene management, how to assess evidence, recognize tampering, and verify acquisitions.
Computer Fundamentals	- The candidate will be familiar with basic computer concepts, such as machine configuration, boot processes, BIOS, UEFI, IP addressing, and domain registrars, in preparation for acquisition.
Data on Drives	- The candidate will be able to summarize different ways data on drives can be stored and accessed, including encryption and handling deleted files.
Data on the Network	- The candidate will be able to describe different ways that data can exist in motion, such as IoT network traffic and PCAP files. They will also be able to discuss how different network tools can be used to discover networked devices.
Dead Box Acquisition	- The candidate will be able to describe the different methods for performing dead box acquisition, including write blocking and media removal.
Filesystem Fundamentals	- The candidate will be able to describe basic concepts of common filesystems, like NTFS, EXT, and FAT. They will also be able to describe the functionality of major components that comprise these file systems, such as Master File Tables and File Allocation Tables.
Host Based Live Acquisition	- The candidate will be able to describe the different methods for performing host based live acquisition, including the use of software and hardware write blocking and accessing physical drives and volumes.
Manual Triage	- The candidate will be familiar with manual techniques and tools used to select and triage data.
Manually Finding Data	- The candidate will be able to outline the different ways in

Topic	Details
	which data can be manually found. This includes: where data can be found, carving metadata, and file recovery.
Mobile Device Acquisition	- The candidate will be able to describe, at a high level, the different methods used to perform mobile device acquisition. This includes isolating portable devices from radio signals, tools for mobile device acquisition, and identifying specific mobile devices.
Mobile Device Triage	- The candidate will be able to outline the ways in which data can be triaged from mobile devices. This includes Android and Apple specific scenarios and how to triage data found in mobile apps, as well as calendars and emails.
Physical Storage Devices	- The candidate will be able to compare and contrast the different forms of physical storage devices. This includes device interfaces, spinning disk layout, solid state drive fundamentals, and common HDD problems.
Remote Acquisition	- The candidate will be able to describe the different methods for performing remote acquisitions, including acquisitions over the network as well as leveraging common cloud provider products.
Specialty Device Fundamentals	- The candidate will be able to describe basic concepts of common specialty devices, like MacOS, including System Profiler and Device Information Collection.
Storage Technologies	- The candidate will be able to summarize, compare, and contrast common storage technologies, such as the different levels of RAID configurations.
Using Forensic Tools for Triage	- The candidate will be able to compare and contrast the ways in which popular forensic tools can be effectively used in data triage.
Windows Filesystems	- The candidate will be able to compare and contrast major Windows filesystems including FAT, exFAT, and NTFS.
Working With Evidence Files	- The candidate will be able to compare and contrast common evidence file formats, how they can be accessed, and how they can be used in an investigation.

GIAC GBFA Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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

Question: 7

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: 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

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: 10

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

Study Guide to Crack GIAC Battlefield Forensics and Acquisition GBFA Exam:

- Getting details of the GBFA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GBFA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GBFA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GBFA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GBFA practice tests is must. Continuous practice will make you an expert in all syllabus areas.