



---

# GIAC GCFE

---

**GIAC Certified Forensic Examiner Certification Questions & Answers**

---

Exam Summary – Syllabus – Questions

---

**GCFE**

**[GIAC Certified Forensic Examiner](#)**

**82 Questions Exam – 70% Cut Score – Duration of 180 minutes**

## Table of Contents:

|   |   |
|---|---|
| Know Your GCFE Certification Well: .....                                  | 2 |
| GCFE GIAC Certified Forensic Examiner Certification<br>Details: .....     | 2 |
| GCFE Syllabus: .....  | 3 |
| GIAC GCFE Sample Questions: .....   | 4 |
| Study Guide to Crack GIAC Certified Forensic Examiner<br>GCFE Exam: ..... | 7 |

## Know Your GCFE Certification Well:

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

But don't worry the GCFE 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 GCFE syllabus?
- How many questions are there in the GCFE exam?
- Which Practice test would help me to pass the GCFE exam at the first attempt?

Passing the GCFE exam makes you GIAC Certified Forensic Examiner. Having the GIAC Certified Forensic Examiner certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

## GCFE GIAC Certified Forensic Examiner Certification Details:

|                     |   |
|---------------------|---|
| Exam Name           | GIAC Certified Forensic Examiner (GCFE)               |
| Exam Code           | GCFE  |
| Exam Price          | \$979 (USD)   |
| Duration            | 180 mins  |
| Number of Questions | 82  |
| Passing Score       | 70%   |
| Books / Training    | <a href="#">FOR500: Windows Forensic Analysis</a>     |
| Schedule Exam       | <a href="#">Pearson VUE</a>                           |
| Sample Questions    | <a href="#">GIAC GCFE Sample Questions</a>            |
| Practice Exam       | <a href="#">GIAC GCFE Certification Practice Exam</a> |

## GCFE Syllabus:

| <b>Topic</b>                   | <b>Details</b>   |
|--------------------------------|--|
| Browser Forensic Artifacts     | - The candidate will demonstrate understanding of the forensic value of browser artifacts.   |
| Browser Structure and Analysis | - The candidate will demonstrate understanding of common browser structure and analysis techniques.  |
| Cloud Storage Analysis         | - The candidate will demonstrate an understanding of the artifacts created by the installation and use of cloud storage solutions and how they can be used during forensic examinations. |
| Digital Forensic Fundamentals  | - The candidate will demonstrate an understanding of forensic methodology and key concepts, and be familiar with Windows filesystems and registry structure.                             |
| Email Analysis                 | - The candidate will demonstrate an understanding of the forensic examination of email communications, including client, web-based, mobile, and M365.                                    |
| Event Log Analysis             | - The candidate will demonstrate an understanding of the purpose of the various types of Windows event, service and application logs, and the forensic value that they can provide.      |
| File and Program Analysis      | - The candidate will demonstrate an understanding of the artifacts created by the Windows operating system during the execution of programs, or activity specific to folders and files.  |
| Forensic Artifact Techniques   | - The candidate will demonstrate an understanding of the approach and tools used to collect forensic evidence required for triage analysis.  |
| System and Device Analysis     | - The candidate will demonstrate an understanding of file access artifacts created by the Windows operating system and USB devices.  |
| User Artifact Analysis         | - The candidate will demonstrate an understanding of the artifacts created by user account(s) and activity on current Windows operating systems.   |

## GIAC GCFE Sample Questions:

### Question: 1

How can the analysis of browser sync data aid in forensic investigations?

- a) It can reveal user preferences across devices.
- b) It provides data about external media connected.
- c) It shows changes in system security settings.
- d) It includes information about system errors.

**Answer: a**

### Question: 2

In forensic analysis, how can the 'Top Sites' file in Safari be used?  
(Choose Two)

- a) To determine the most frequently visited sites
- b) To track downloaded files and their sources
- c) To reveal user preferences for site settings
- d) To show thumbnails of frequently visited pages

**Answer: a, d**

### Question: 3

When examining browser artifacts, which of the following files are crucial for reconstructing a user's search history?  
(Choose Two)

- a) Bookmarks file
- b) History database
- c) Network configuration file
- d) Memory dump

**Answer: a, b**

### Question: 4

For forensic investigations, what crucial information does the analysis of M365 email logs provide?

- a) User interface customizations
- b) Data about file access requests
- c) Details on email transactions and user activities
- d) Information on hardware configurations used

**Answer: c**

**Question: 5**

Why is it important to analyze the 'Outbox' and 'Drafts' folders in an email forensic investigation?

- a) They can show emails that were intended to be sent but were not successfully transmitted.
- b) They provide data on files downloaded from emails.
- c) They list the security updates applied to the email client.
- d) They detail the user's changes to email display settings.

**Answer: a**

**Question: 6**

In the context of cloud storage analysis, what does examining the '.dat' files within the application's directory aid in discovering?

- a) Patterns of external device usage
- b) Details of network settings adjustments
- c) Information on security protocol changes
- d) Data regarding file synchronization status

**Answer: d**

**Question: 7**

Which event log would be most useful for understanding application failures or crashes?  
(Choose Two)

- a) Application log
- b) Setup log
- c) System log
- d) Forwarded Events log

**Answer: a, c**

**Question: 8**

During a forensic examination, how can log files from cloud storage applications be used to track user activity?

- a) They can show the history of connected printers.
- b) They provide a timeline of files accessed and modified.
- c) They list installed browser extensions.
- d) They detail changes to firewall settings.

**Answer: b**

**Question: 9**

What can be inferred from the high frequency of certain event IDs in the security logs?

(Choose Two)

- a) Repeated system updates
- b) Frequent user logins and logouts or failed security events
- c) Regular changes in user account privileges
- d) Consistent application usage patterns

**Answer: b, c**

**Question: 10**

Which of the following artifacts are used to determine the devices connected to a cloud storage account?

(Choose Three)

- a) Device sync logs
- b) Access logs
- c) Network configuration files
- d) Device identifiers
- e) Application error logs

**Answer: a, b, d**

## Study Guide to Crack GIAC Certified Forensic Examiner GCFE Exam:

- Getting details of the GCFE 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 GCFE 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 GCFE 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 GCFE 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 GCFE practice tests is must. Continuous practice will make you an expert in all syllabus areas.

### Reliable Online Practice Test for GCFE Certification

Make EduSum.com your best friend during your GIAC Certified Forensic Examiner exam preparation. We provide authentic practice tests for the GCFE exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GCFE exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the GCFE exam.

**Start Online practice of GCFE Exam by visiting URL**

**<https://www.edusum.com/giac/gcfe-giac-certified-forensic-examiner>**