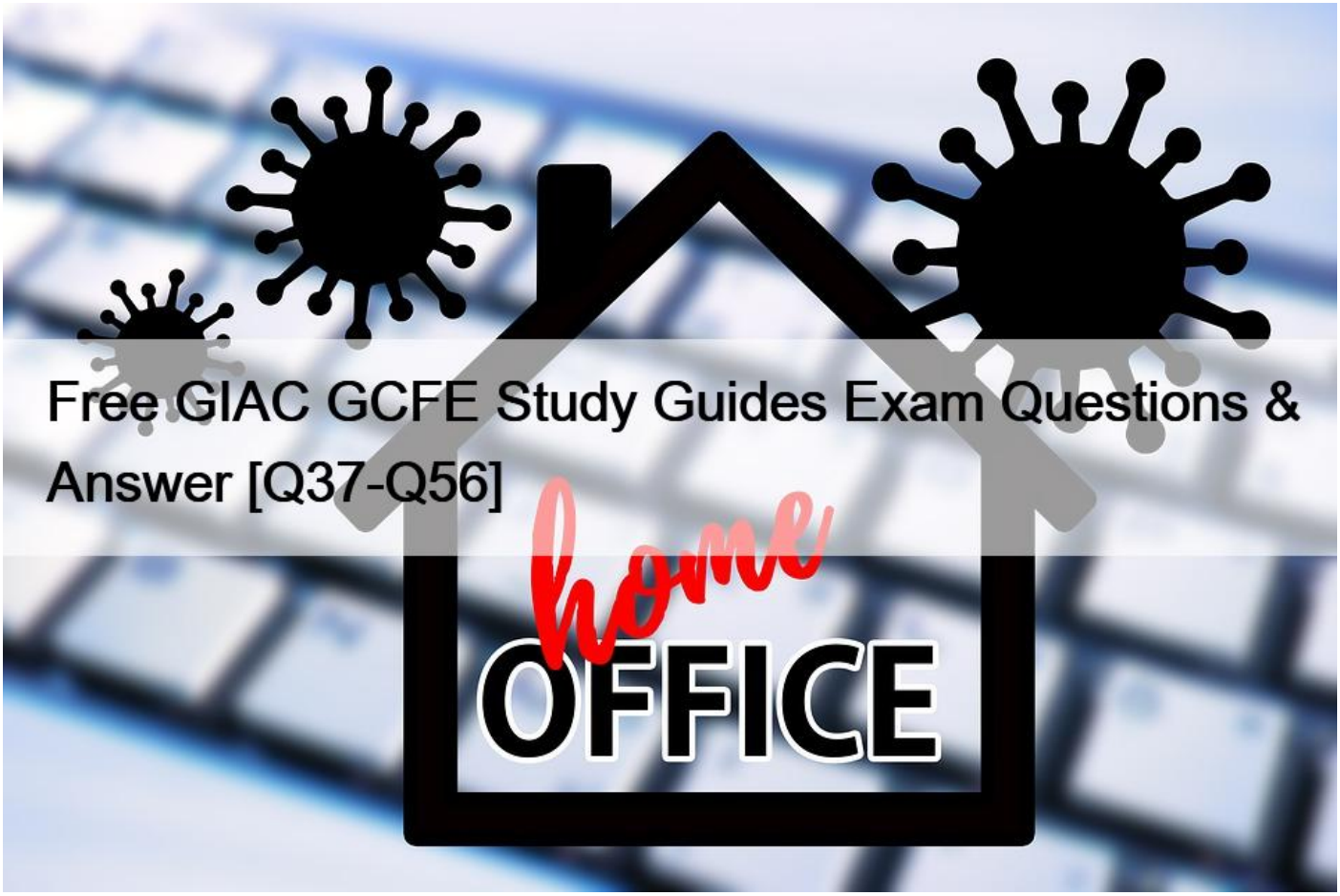
Free GIAC GCFE Study Guides Exam Questions & Answer [Q37-Q56



Free GIAC GCFE Study Guides Exam Questions and Answer
GCFE Exam Dumps, GCFE Practice Test Questions

What is the exam cost of GIAC GCFE Certification

The exam cost of GIAC GCFE Certification is $999.

Prerequisites of GIAC GCFE Exam

For those who want to become a Certified Forensics Examiner, they need to meet some specific requirements before they can take the GCFE exam.

- 10 years of experience in handling cases involving computer hardware and software issues.- Experience in the IT industry.- Ability to estimate the probable impact on business unless there is a significant problem that must be addressed immediately by IT personnel.- Understanding of data collection and analysis techniques used during incident response.- Understanding the various types of attacks that can be made by an intruder.- Knowledge of basic computer forensics skills, such as understanding how hackers work and how to detect their clues during investigations.- Awareness of the steps to take when a computer is attacked. **Q37.** What is the primary function of hashing in digital forensics?

Response:

* To compress data for storage efficiency

* To identify duplicate files
* To verify the integrity of forensic evidence
* To track user access times

Q38. In the context of Google Chrome, where are bookmark and user settings typically stored for forensic analysis?

Response:
* In the ‘Preferences’ file
* In the ‘Cookies’ file
* In the ‘System.log’ file
* In the ‘Network Security’ file

Q39. What is the forensic value of analyzing the ‘Windows Event Viewer’ in the context of system analysis?

Response:
* It provides a detailed record of system, application, and security events, which can help trace user actions and system changes.
* It tracks the installation of new operating systems.
* It monitors changes to the graphical user interface settings.
* It logs the frequency of network disconnections.

Q40. What is the importance of the ‘Last Access Time’ timestamp in the context of forensic investigations?

(Choose Two)

Response:
* It shows the last time a file was accessed, helping to establish a timeline of user activity
* It records the last system update
* It details changes in file permissions
* It can indicate potential tampering with evidence

Q41. What can be revealed by analyzing the metadata of email attachments?

Response:
* The subject of the email
* The original file creation and modification dates
* The recipient’s login times
* The email client’s version number

Q42. How do forensic analysts use the information from ‘system snapshots’ in their investigations?

Response:
* They provide a historical view of the system, which can be useful for identifying changes made over time, including malware installation or unauthorized modifications.
* They monitor the performance of hardware components.
* They log the installation of mobile apps.
* They provide a backup of user emails.

Q43. A forensic investigator is analyzing a Windows system suspected of containing malware. The user claims they did not install any suspicious programs. Which artifacts would you analyze to confirm or refute this claim?

(Select three)

Response:
* Prefetch files
* Master File Table (MFT)
* System log
* Recycle Bin contents
* Application error logs

Q44. How can ‘scheduled tasks’ in a user profile indicate malicious activity?

Response:
* They may include tasks set to run software at specific times, potentially for malicious purposes like data exfiltration or launching attacks.
* They provide a log of software uninstallation events.
* They detail the history of connected Bluetooth devices.
* They track changes in user access levels.

Q45. Which artifacts are essential for identifying URLs that were typed manually by a user during a browsing session?

(Choose Two)

Response:
* Form history
* Autocomplete files
* Cache files
* System log files

Q46. What is the primary purpose of Windows event logs in the context of digital forensics?

Response:
* To record user interface customizations
* To provide a detailed record of system, application, and security events
* To list all installed applications and their usage statistics
* To monitor network connection speeds and stability

Q47. How do forensic investigators use slack space to recover data?

Response:
* By retrieving logs of failed login attempts
* By examining unallocated disk space for remnants of deleted files
* By analyzing encrypted files
* By reviewing the file’s access permissions

Q48. What role do ‘system snapshots’ play in forensic analysis of file activities?

Response:
* They provide a historical view of the system at various points, helping to identify changes over time.
* They log user login attempts and durations.
* They track changes in user interface themes.

* They detail the network security protocols in use.

Q49. In the context of cloud storage analysis, what does examining the ‘.dat’ files within the application’s directory aid in discovering?

Response:
* Patterns of external device usage
* Details of network settings adjustments
* Information on security protocol changes
* Data regarding file synchronization status

Q50. Which of the following browser artifacts can help identify the websites visited by a user?

Response:
* Firewall settings
* Places.sqlite
* Security certificates
* Network configuration files

Q51. In Windows, which artifact provides a history of files and folders recently accessed by a user?

Response:
* Event logs
* Prefetch files
* RecentDocs registry key
* Application error logs

Q52. How can an analyst use ‘DNS logs’ from Windows event logs to track malicious activity?

Response:
* By identifying unusual patterns of DNS queries, which may suggest phishing or malware communication.
* By monitoring changes to network configurations.
* By tracking the frequency of application updates.
* By listing all connected USB devices.

Q53. Why is the analysis of ‘user-specific event logs’ significant in a forensic investigation?

Response:
* They provide a record of events triggered by specific user actions, which can help link activities to a particular user account.
* They monitor the frequency of network disconnections.
* They log details of system firmware updates.
* They track changes in user interface settings.

Q54. In forensic analysis, how can the ‘Top Sites’ file in Safari be used?

(Choose Two)

Response:
* To determine the most frequently visited sites
* To track downloaded files and their sources

* To reveal user preferences for site settings
* To show thumbnails of frequently visited pages

Q55. How can the analysis of browser sync data aid in forensic investigations?

Response:
* It can reveal user preferences across devices.
* It provides data about external media connected.
* It shows changes in system security settings.
* It includes information about system errors.

Q56. Which browser structure is essential for understanding user interaction with various multimedia elements within the browser?

Response:
* Plugin data
* Security certificates
* Network configuration logs
* System update files