GIAC.GIME.v2026-09-14.q78

Exam Code:	GIME
Exam Name:	GIAC iOS and macOS Examiner
Certification Provider:	GIAC
Free Question Number:	78
Version:	v2026-09-14
# of views:	106
# of Questions views:	780
https://www.freecram.net/torrent/GIAC.GIME.v2026-09-14.q78.html	

NEW QUESTION: 1
When constructing an SQL query to examine application data, what statement is used to retrieve data from a specific table?
A. INSERT INTO
B. UPDATE
C. SELECT FROM
D. DELETE FROM
Answer: (SHOW ANSWER)

NEW QUESTION: 2
During Document and iCloud analysis, what indicates that a document has been altered?
A. Identical content in different versions
B. A change in file size
C. Same version number
D. Constant modification date
Answer: (SHOW ANSWER)

NEW QUESTION: 3
What aspect of user data is critical for distinguishing between different user profiles in system configuration analysis?
A. Screen resolution settings
B. Desktop wallpaper choices
C. Universal Access preferences
D. Per-user daemon configurations
Answer: (SHOW ANSWER)

NEW QUESTION: 4

Which SQL function is used to count the number of items in a selected set?
A. MAX()
B. COUNT()
C. SUM()
D. AVG()
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which acquisition method is preferred for preserving the integrity of data during an incident response?
A. Live system acquisition
B. Remote acquisition
C. Full disk encryption
D. Logical acquisition
Answer: (SHOW ANSWER)

NEW QUESTION: 6
In analyzing iCloud data, what is a key factor in distinguishing between different document versions?
A. File name
B. File color
C. File extension
D. Timestamp
Answer: (SHOW ANSWER)

NEW QUESTION: 7
In application fundamentals, what is the primary function of an SQL JOIN operation?
A. To create new tables
B. To delete data
C. To combine rows from two or more tables
D. To update data
Answer: (SHOW ANSWER)

NEW QUESTION: 8
You are tasked with investigating a series of unauthorized logins on a macOS system over the past week.
What steps will you take to create a timeline of these events and identify the source of the activity? (Choose three)
A. Parse user authentication events from /var/log/secure.log
B. Analyze /var/log/system.log for login entries
C. Cross-reference login times with network activity from /var/log/wifi.log

D. Analyze app error logs to correlate with login attempts
E. Review kernel panics in /Library/Logs/DiagnosticReports/
Answer: (SHOW ANSWER)

NEW QUESTION: 9
During an investigation, you suspect that a suspect's device is syncing critical documents to iCloud.
What steps can you take to confirm and retrieve those documents? (Choose three)
A. Check the Finder app for iCloud-synced files
B. Review iCloud Drive logs in /var/log/icloud/
C. Disable iCloud sync on the device to preserve evidence
D. Use iCloud Extractor to download synced documents
E. Analyze Apple ID credentials to access the suspect's iCloud
Answer: (SHOW ANSWER)

NEW QUESTION: 10
What can be inferred from analyzing the configuration of a Mail application?
A. Graphics card performance
B. User's communication habits and contacts
C. Processor architecture
D. Number of installed browsers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
What triage data helps understand system modifications?
A. Battery cycle count
B. iCloud sync status
C. OS installation logs
D. Recent documents
Answer: (SHOW ANSWER)

NEW QUESTION: 12
How can one use SQL to find the specific data within a database table related to an application's functionality?
A. By updating data formats
B. By creating new data entries
C. By deleting irrelevant data
D. By selecting data based on certain criteria
Answer: (SHOW ANSWER)

NEW QUESTION: 13

In incident response, why is the analysis of volatile system artifacts important?
A. They are unaffected by system updates.
B. They can be easily recovered after shutdown.
C. They provide information on system state at incident time.
D. They contain permanent system settings.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
During an investigation of an iPhone, you need to gather evidence of a suspect's recent locations. The Maps application shows several recent trips, but you are unsure of their exact destinations. Which steps will you take to analyze the Maps application data to confirm the locations? (Select three correct answers)
A. Review call logs for related phone numbers
B. Use timestamp data to correlate trips with other device activities
C. Compare GPS data with the suspect's physical movements via Wi-Fi connection logs
D. Analyze web browsing history for location-based searches
E. Extract GPS coordinates from the Maps application history
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 15
Which tool can be used to download and examine iCloud backups during a forensic investigation?
A. Activity Monitor
B. Blacklight
C. Terminal
D. iCloud Extractor
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which log type is essential for understanding application behavior on a Mac?
A. Firewall logs
B. Console logs
C. Security logs
D. System logs
Answer: (SHOW ANSWER)

NEW QUESTION: 17
What artifact can indicate the use of removable media devices on a macOS system?
A. Network logs
B. I/O registry entries
C. Kernel panics
D. System configuration files
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which macOS tool is typically used to analyze APFS volumes for file system artifacts?
A. XCode
B. Disk Utility
C. fsck_apfs
D. Terminal
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What kind of artifact can be analyzed from the Contacts application on an Apple device?
A. Contact names and call records
B. Browser cookies
C. GPS tracking data
D. File download history
Answer: (SHOW ANSWER)

NEW QUESTION: 20
During memory analysis, why is it important to understand the different states of memory allocation?
A. To categorize file types
B. To identify potential data remnants
C. To assess network activity
D. To optimize data retrieval
Answer: (SHOW ANSWER)

NEW QUESTION: 21
What type of information can be gleaned from analyzing Photos application data?
A. User communication patterns
B. Location metadata and timestamps
C. Software installation history
D. Wi-Fi network connections

Answer: (SHOW ANSWER)

NEW QUESTION: 22
What is a common use of SQL queries in forensic analysis of mobile apps?
A. Extracting call logs and messaging data from databases
B. Recovering deleted system logs
C. Modifying app permissions
D. Monitoring network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 23
How can file system operations leave behind critical evidence?
A. By updating the system clock
B. Through changes in network settings
C. Through the creation of log files
D. By modifying user preferences
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
Which data structure is primarily used by iOS apps for persistent storage?
A. UFS
B. RAM
C. EXT4
D. plist (Property List)
Answer: (SHOW ANSWER)

NEW QUESTION: 25
What data points should be included when creating a forensic timeline based on macOS log analysis? (Select two)
A. Frequency of app updates
B. Timestamp of system kernel panics
C. Timestamps of user login and logout events
D. MAC address of connected devices
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What artifact within the Apple File System indicates application usage?
A. System logs
B. Spotlight index
C. Kernel extensions
D. User preferences

Answer: (SHOW ANSWER)

NEW QUESTION: 27
What artifact is essential in understanding user interactions within productivity applications?
A. Boot sequence
B. Peripheral devices list
C. Kernel version
D. Document modification timestamps
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
For productivity application analysis, how can forensic examiners utilize metadata from Calendar events?
A. To understand user's time management
B. To gauge Internet speed
C. To assess graphic design preferences
D. To determine device orientation
Answer: (SHOW ANSWER)

NEW QUESTION: 29
In incident response, what indicates a potential security breach in an Apple operating system?
A. Regularly scheduled backups
B. Consistent network performance
C. Frequent system updates
D. Unexpected new user accounts
Answer: (SHOW ANSWER)

NEW QUESTION: 30
What piece of triage information assists in identifying applied management profiles?
A. Bluetooth connectivity logs
B. Safari browsing history
C. Installed printers
D. Configuration profiles
Answer: (SHOW ANSWER)

NEW QUESTION: 31
What is a crucial step in log analysis within incident response?
A. Archiving all logs to external storage
B. Changing log retention settings
C. Deleting outdated logs
D. Correlating events from different log sources

Answer: (SHOW ANSWER)

NEW QUESTION: 32
What type of data can be extracted from the Wallet application?
A. Transaction history
B. Email correspondences
C. Health data
D. Passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which methods can be used to extract memory on a live macOS system? (Select two)
A. Run sudo fsck to scan memory
B. Analyze backup logs for memory data
C. Use Volatility to analyze a live memory dump
D. Use dd to copy raw memory data
Answer: (SHOW ANSWER)

NEW QUESTION: 34
What type of data can be found in the com.apple.TimeMachine plist file?
A. Bluetooth connection logs
B. System file permissions
C. Recent user login attempts
D. Time Machine backup schedules and status
Answer: (SHOW ANSWER)

NEW QUESTION: 35
For system triage, how can one identify the presence of network profiles?
A. Checking the firewall status
B. Reviewing browser cookies
C. Analyzing email configurations
D. Inspecting network preferences

Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which log file is essential for identifying malware behavior on macOS during an incident response?
A. /private/etc/hosts
B. /Library/Preferences/SystemConfiguration/
C. /var/log/mail.log
D. /var/log/system.log
Answer: (SHOW ANSWER)

NEW QUESTION: 37
During the analysis of user data from productivity applications, what is a primary focus?
A. Evaluating network speed
B. Monitoring CPU temperature
C. Checking compliance with licensing terms
D. Understanding the applications' role in the user's activities
Answer: (SHOW ANSWER)

NEW QUESTION: 38
What type of artifact is crucial to identify when examining systems for signs of malicious code?
A. Unusual executable files
B. Network configurations
C. Application logs
D. User preferences
Answer: (SHOW ANSWER)

NEW QUESTION: 39
What types of data can be analyzed from iCloud backups for forensic purposes? (Select two)
A. Bluetooth pairing logs
B. Photos
C. Messages
D. Kernel panics
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which Apple application is crucial for analyzing user's location history?
A. Notes
B. Mail
C. Maps
D. Safari

Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which method can be used to bypass encrypted containers on a macOS device during forensic analysis?
A. Brute-force decryption
B. Using sudo chmod command
C. Reinstalling the operating system
D. Logical extraction
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Which tool is commonly used for memory acquisition on macOS devices?
A. Volatility
B. Terminal
C. Cellebrite
D. MemDump
Answer: (SHOW ANSWER)

NEW QUESTION: 43
In Apple Systems Triage, what artifact might show when the system was last managed or configured remotely?
A. Mobile device management (MDM) logs
B. User login times
C. Screen sharing sessions
D. Peripheral device connections
Answer: (SHOW ANSWER)

NEW QUESTION: 44
You are investigating a macOS device that shows signs of compromise, including abnormal network activity and unauthorized system modifications.
What steps should you take to gather evidence of the malware's presence and determine how it compromised the system? (Choose three)
A. Capture memory dumps to analyze volatile data
B. Check /var/log/system.log for suspicious activity
C. Reboot the system to restore normal functionality
D. Use ps -A to identify unusual processes running in the background
E. Inspect the /Library/LaunchDaemons/ directory for malicious startup items
Answer: (SHOW ANSWER)

NEW QUESTION: 45

How do Apple Operating Systems differentiate in terms of system acquisition?
A. By the programming language used for system calls
B. By user interface design
C. By the availability of source code
D. By the methods available to extract system data
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which file system is commonly used in macOS for better space optimization and encryption support?
A. HFS+
B. FAT32
C. NTFS
D. APFS
Answer: (SHOW ANSWER)

NEW QUESTION: 47
How does the analysis of file system artifacts assist in a forensic investigation?
A. By revealing user activities and preferences
B. By evaluating the graphics performance
C. By determining the efficiency of the storage system
D. By assessing the speed of the operating system
Answer: (SHOW ANSWER)

NEW QUESTION: 48
You are investigating a macOS device that is suspected to contain encrypted containers with valuable evidence. The suspect has used FileVault 2 encryption, and you need to access the data stored in these containers.
What steps can you take to gain access and analyze the contents? (Choose three)
A. Extract the encryption key from volatile memory
B. Disable FileVault to prevent further encryption
C. Attempt brute-force decryption using forensic tools

D. Mount the encrypted container using the suspect's credentials
E. Analyze logs for previous decryption attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 49
You are investigating a macOS device that uses the APFS file system. The suspect has deleted critical files, but you believe the data can still be recovered.
What steps should you take to recover the deleted files? (Choose three)
A. Use macOS's native Disk Utility to repair the disk
B. Examine the free space and unallocated blocks for remnants of deleted files
C. Extract the Master Boot Record (MBR) for detailed file metadata
D. Mount the file system in read-only mode using hdiutil attach
E. Use APFS snapshots to revert the file system to an earlier state
Answer: (SHOW ANSWER)

NEW QUESTION: 50
How can an investigator use Unified Logs in macOS for timeline creation?
A. By correlating system events across different log levels
B. By tracking user logins only
C. By analyzing hardware-related messages exclusively
D. By focusing solely on application crash reports
Answer: (SHOW ANSWER)

NEW QUESTION: 51
What data can be analyzed to track a user's physical movements across different locations on an iOS device?
A. Wi-Fi connection logs
B. iCloud backup data
C. User account activity
D. Location services data
Answer: (SHOW ANSWER)

NEW QUESTION: 52
During system triage, what indicates the initial installation date of the OS?
A. Firmware version
B. Time Machine backup
C. System log creation date
D. Kernel extension
Answer: (SHOW ANSWER)

NEW QUESTION: 53

What artifact is crucial for tracking user behavior in "Pattern of Life" analysis?
A. CPU temperature logs
B. Installed applications
C. System logins and activity timestamps
D. BIOS version
Answer: (SHOW ANSWER)

NEW QUESTION: 54
What is the primary goal of analyzing memory captures in digital forensics?
A. To identify inactive memory regions
B. To evaluate the physical condition of memory
C. To extract real-time operational data
D. To increase storage space
Answer: (SHOW ANSWER)

NEW QUESTION: 55
When analyzing Safari data, what information is crucial for understanding user behavior?
A. Firewall settings
B. Browser history and bookmarks
C. Application installation dates
D. Disk usage statistics
Answer: (SHOW ANSWER)

NEW QUESTION: 56
In macOS, what mechanism provides system-level and user-specific settings that can influence forensic analysis?
A. Launch Agents and Daemons
B. Mission Control
C. Spotlight
D. Notification Center
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which macOS feature can be analyzed to determine the amount of time a user spends on specific applications?
A. Activity Monitor
B. Keychain Access
C. Screen Time
D. Launchpad
Answer: (SHOW ANSWER)

NEW QUESTION: 58
What type of metadata is stored in APFS snapshots?
A. Wi-Fi connection history
B. System event logs
C. File permissions
D. File and directory states at specific points in time
Answer: (SHOW ANSWER)

NEW QUESTION: 59
During system triage, what information can provide insights into device management?
A. Media library
B. Screen saver settings
C. Installed games
D. Management profiles
Answer: (SHOW ANSWER)

NEW QUESTION: 60
What can iCloud data analysis reveal in a forensic context?
A. Power consumption patterns
B. CPU usage
C. User's data backup habits
D. Network bandwidth
Answer: (SHOW ANSWER)

NEW QUESTION: 61
In the context of encrypted container analysis, what is the purpose of using a brute force technique?
A. To repair corrupted files
B. To verify data integrity
C. To enhance encryption protocols
D. To bypass encryption mechanisms
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Where are Safari browser downloads typically stored on macOS?
A. /Users/[username]/Downloads
B. /System/Library/Downloads
C. /private/var/tmp
D. /Library/Safari/Downloads
Answer: (SHOW ANSWER)

NEW QUESTION: 63
How can calendar application data assist in a forensic investigation?
A. By showing Wi-Fi passwords
B. By providing software version information
C. By revealing scheduled events and associated metadata
D. By displaying graphic card specifications
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
What type of data would be analyzed in the Reminders application?
A. Network throughput rates
B. System error logs
C. Encryption algorithms
D. Reminder notes and due dates
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which data point is crucial when analyzing the Photos application on iOS devices?
A. Battery usage data
B. Timestamps and geolocation metadata
C. Application permissions
D. File access times
Answer: (SHOW ANSWER)

NEW QUESTION: 66
How can investigators use data from communication applications in their analysis?
A. To understand user's communication patterns
B. To assess audio settings
C. To check the power supply unit
D. To determine the CPU model

Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which artifact indicates the OS backup frequency during system triage?
A. System migration assistant
B. Application update logs
C. Disk utility reports
D. Time Machine settings
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which command can you use to gather detailed system information about a macOS device during a triage?
A. sudo system_profiler
B. sudo sysdiagnose
C. sudo systeminfo
D. sudo systemctl status
Answer: (SHOW ANSWER)

NEW QUESTION: 69
What type of data can be found in volatile memory on macOS devices?
A. Web browser bookmarks
B. System logs
C. User contacts
D. Application passwords and encryption keys
Answer: (SHOW ANSWER)

NEW QUESTION: 70
What type of data can be extracted from the Maps application in iOS for forensic purposes?
A. Text messages
B. Browser history
C. Location history and routes
D. Contact details
Answer: (SHOW ANSWER)

NEW QUESTION: 71
Which log file provides details on Safari browser usage on macOS?
A. /Users/[username]/Library/Safari/History.db
B. /Library/Logs/SafariHistory.log
C. /private/var/log/httpd
D. /var/log/safari.log

Answer: (SHOW ANSWER)

NEW QUESTION: 72
When analyzing encrypted containers, why is knowledge of the specific encryption algorithm used important?
A. It influences the brute force attack time.
B. It changes the container's metadata structure.
C. It affects file naming conventions.
D. It determines the color depth of files.
Answer: (SHOW ANSWER)

NEW QUESTION: 73
In productivity application analysis, what data can be extracted from the Mail application?
A. Network configuration
B. Printing preferences
C. Email content and metadata
D. Web browsing history
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which macOS tool can be used to create a forensic disk image of a target drive?
A. Disk Utility
B. iCloud Drive
C. Activity Monitor
D. Time Machine
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
While conducting a forensic investigation on a macOS device, you discover that the user has deleted a large number of files. You need to determine which files were deleted and when. How can you use file system artifacts to recover this information? (Choose three)
A. Reconstruct file system changes using the APFS transaction logs
B. Analyze APFS snapshots for prior versions of the deleted files
C. Use Time Machine backups to restore deleted files
D. Extract logs from /var/log/fsck.log for file deletion events
E. Review Spotlight metadata for recently accessed files
Answer: (SHOW ANSWER)

NEW QUESTION: 76
What is the primary role of the Master File Table (MFT) in file systems like NTFS?
A. Storing file contents

B. Encrypting user data
C. Tracking file attributes and metadata
D. Managing disk partitions
Answer: (SHOW ANSWER)

NEW QUESTION: 77
Which of the following is a fundamental system identifier in Apple Systems Triage?
A. Application version
B. Wi-Fi SSID
C. User's email address
D. Device serial number
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Where can the primary macOS system logs be found for analysis?
A. /System/Library/Logs/
B. /private/var/log/
C. /etc/syslog/
D. /usr/local/log/
Answer: (SHOW ANSWER)

Valid GIME Dumps shared by EduDump.com for Helping Passing GIME Exam!
EduDump.com now offer the **newest GIME exam dumps**, the EduDump.com GIME exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com GIME dumps with Test Engine here:
https://www.edudump.com/exams/GIAC/GIME/premium/ (**157** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)