GIAC

GCFE

Certified Forensic Examiner

Questions&AnswersPDF

ForMoreInformation:

https://www.certswarrior.com/

Latest Version: 6.0

Question: 1

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

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: 2

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

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: 3

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

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: 4

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

A. Application log
B. Setup log
C. System log
D. Forwarded Events log

Answer: A,C

Question: 5

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

A. Bookmarks file
B. History database
C. Network configuration file
D. Memory dump

Answer: A,B

Question: 6

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

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: 7

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

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: 8

Which of the following artifacts are used to determine the devices connected to a cloud storage account?
(Choose Three)
Response:

A. Device sync logs
B. Access logs
C. Network configuration files
D. Device identifiers
E. Application error logs

Answer: A,B,D

Question: 9

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

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: 10

What can be inferred from the high frequency of certain event IDs in the security logs?
(Choose Two)
Response:

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