



CERTSWARRIOR

GIAC GCFE

Certified Forensic Examiner

Questions&AnswersPDF

ForMoreInformation:

<https://www.certswarrior.com/>

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Visit us at: <https://www.certswarrior.com/exam/gcfe>

Latest Version: 6.0

Question: 1

What is the forensic relevance of 'alternate data streams' in NTFS filesystems?

Response:

- A. They can be used to store additional data hidden from normal file browsing utilities, posing a challenge for data discovery.
- B. They provide a history of user interface settings adjustments.
- C. They track installation of browser extensions.
- D. They log firewall and antivirus status updates.

Answer: A

Question: 2

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

Response:

- A. Firewall settings
- B. Places.sqlite
- C. Security certificates
- D. Network configuration files

Answer: B

Question: 3

In the context of system and device analysis, why is 'network traffic monitoring' crucial?

Response:

- A. It can identify potential security breaches by analyzing incoming and outgoing traffic for unusual patterns or data transfers.
- B. It details the user's preferences for desktop wallpapers.
- C. It logs the system's uptime and downtime.
- D. It tracks the changes in user account management settings.

Answer: A

Question: 4

Why is the 'Last Known Good Configuration' data important in forensic analysis of Windows systems?
Response:

- A. It contains information about the last system state that booted successfully without errors, which can help identify changes that led to system issues.
- B. It logs details of deleted files.
- C. It monitors the installation of software updates.
- D. It provides data on network connectivity issues.

Answer: A

Question: 5

Which of the following are critical artifacts for tracking user access to files in cloud storage applications like Dropbox and Google Drive?

(Choose two)

Response:

- A. Trash or recycle bin
- B. Sync logs
- C. User profile databases
- D. Configuration files
- E. Version history

Answer: B,E

Question: 6

When analyzing browser data in Google Chrome, which files are useful for understanding download history?

(Choose two)

Response:

- A. Downloads table in History database
- B. Cookies file
- C. Preferences file
- D. Cache files
- E. Bookmarks file

Answer: A,D

Question: 7

For forensic analysis, which file in Chrome provides insights into user actions regarding file downloads?

Response:

- A. History file
- B. Bookmarks file
- C. 'Downloads' table in the 'History' database
- D. 'Extensions' configuration file

Answer: C

Question: 8

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

(Choose Two)

Response:

- A. Form history
- B. Autocomplete files
- C. Cache files
- D. System log files

Answer: A,B

Question: 9

In digital forensics, why is the analysis of 'environment variables' crucial?

Response:

- A. They can provide information about system paths and user settings, which are useful for understanding the configuration and behavior of user accounts.
- B. They log the installation of antivirus programs.
- C. They track the frequency of user password changes.
- D. They monitor the usage of external storage devices.

Answer: A

Question: 10

What type of forensic data can be extracted from a browser's cache?

Response:

- A. Network logon times
- B. Recent system errors
- C. Webpage content and resources
- D. Encryption key usage

Answer: C



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ