Vendor: GIAC

Exam Code: GCFE

Exam Name: GIAC Certified Forensic Examiner

Version: DEMO

QUESTION 1
What can be revealed by analyzing the metadata of email attachments?

A. The subject of the email
B. The original file creation and modification dates
C. The recipient's login times
D. The email client's version number

Answer: B

QUESTION 2
Which Windows file contains user-specific settings and configuration data, making it crucial for forensic analysis?

A. Prefetch files
B. NTUSER.DAT
C. Application logs
D. System log

Answer: B

QUESTION 3
What role does 'hashing' play in the integrity of digital evidence? (Choose Two)

A. It verifies that data has not been altered since the hash was generated.
B. It compresses data to save storage space.
C. It encrypts data to protect sensitive information.
D. It provides a unique digital fingerprint of files.

Answer: AD

QUESTION 4
How do forensic analysts use the information from 'system snapshots' in their investigations?

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

Answer: A

QUESTION 5
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: BC

QUESTION 6
How do forensic analysts use 'anomaly detection' techniques in their investigations?

A. By identifying patterns in data that deviate from normal behavior, suggesting potential security incidents or malicious activity.
B. By monitoring the efficiency of the system cooling components.
C. By tracking the installation of third-party software.
D. By logging the updates to user profiles and settings.

Answer: A

QUESTION 7
In browser structure analysis, what is the significance of analyzing 'Local Storage' files in modern web browsers?

A. They provide insights into user-specific data stored by websites.
B. They detail the browser's network security configurations.
C. They log user-installed applications and usage.
D. They show changes to browser security levels.

Answer: A

QUESTION 8
How can 'scheduled tasks' in a user profile indicate malicious activity?

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

Answer: A

QUESTION 9
What is a primary focus of forensic analysis when examining emails from a client application?

A. The format of email headers and their origin information
B. The frequency of email checks by the client
C. The customization of the email client interface
D. The security protocols for incoming messages

Answer: A

QUESTION 10

Which cloud storage artifact is crucial for identifying the origin of accessed files during an investigation? (Choose Two)

A. Sync logs
B. Configuration files
C. User profile databases
D. Metadata files

Answer: AD

QUESTION 11
What fundamental principle of digital forensics involves ensuring that the evidence remains unaltered from the time of collection to presentation in court?

A. Chain of custody
B. Data reduction
C. Systematic sampling
D. Cross-validation

Answer: A

QUESTION 12
What does analyzing the 'registry hives' reveal in the context of system analysis?

A. It provides insights into user configurations and installed software, which can be crucial in understanding system usage patterns.
B. It details the frequency of password changes.
C. It logs user interactions with cloud storage services.
D. It tracks the installation of network adapters.

Answer: A

QUESTION 13
What role does the Master Boot Record (MBR) play in a forensic investigation of a storage device?

A. It stores file system permissions
B. It logs system crashes and failures
C. It holds information on partition layout and boot sequence
D. It tracks user login attempts

Answer: C

QUESTION 14
How can an analyst use 'DNS logs' from Windows event logs to track malicious activity?

A. By identifying unusual patterns of DNS queries, which may suggest phishing or malware communication.
B. By monitoring changes to network configurations.

C. By tracking the frequency of application updates.
D. By listing all connected USB devices.

Answer: A

QUESTION 15
How do 'version history' files in services like Microsoft OneDrive assist in forensic investigations?

A. They track changes in system hardware.
B. They provide historical data of file edits and deletions.
C. They monitor user's web browsing habits.
D. They log security certificate updates.

Answer: B

QUESTION 16
Which of the following artifacts are valuable for tracking user access to a web-based email service? (Choose Two)

A. Browser history
B. Firewall logs
C. Email sync logs
D. Session cookies

Answer: AD

QUESTION 17
In Mozilla Firefox, what is the purpose of the sessionstore.js file during a forensic analysis?

A. To store browsing history
B. To log system errors
C. To record open tabs and windows at the time of closure
D. To store passwords

Answer: C

QUESTION 18
What is the purpose of using 'timeline analysis' in forensic investigations?

A. It helps in establishing a chronological order of events based on the creation, modification, and access times of files and other digital artifacts.
B. It provides a continuous log of system uptime and downtime.
C. It details changes in system security settings.
D. It tracks the frequency of password changes.

Answer: A

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**