KaozhengPro

# IT認證考試題庫

# 專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

**Exam** : **312-49v11**

**Title** : Computer Hacking Forensic Investigator (CHFIv11)

**Version** : DEMO

1.In a financial institution's computer forensic investigation, suspicious activity reveals unauthorized access to GLBA (Gramm-Leach-Bliley Act)-protected customer data, raising concerns for customer safety. However, identifying the breach's source and extent poses significant challenges, complicating compliance with GLBA guidelines.
What steps should be taken in a GLBA-covered computer forensic investigation when unauthorized access to sensitive customer data is discovered?
A. Ignore the incident if it does not directly threaten financial activities.
B. Share information with third parties for analysis.
C. Inform law enforcement without notifying affected customers.
D. Notify affected customers of opt-out rights and safeguard data.
**Answer:** D
**Explanation:**
According to CHFI v11 objectives under Computer Forensics Fundamentals and Regulations, Policies, and Ethics, a forensic investigator must ensure that technical investigation activities align with applicable legal and regulatory requirements. The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions protect customers' nonpublic personal information (NPI) and respond appropriately to any unauthorized access or disclosure.
When a breach involving GLBA-protected data is identified, the organization must follow a structured incident response and forensic investigation process while maintaining compliance with privacy laws. CHFI v11 emphasizes forensic readiness, legal compliance, and ethical handling of digital evidence. Notifying affected customers of their opt-out rights and implementing safeguards to protect compromised data are core requirements of GLBA's Privacy Rule and Safeguards Rule.
Ignoring the incident violates forensic and legal responsibilities, while sharing sensitive data with third parties risks further disclosure. Informing law enforcement alone is insufficient if customer notification obligations are not met. Proper customer notification demonstrates due diligence, supports transparency, and reduces legal risk. From a CHFI perspective, this approach ensures lawful evidence handling, regulatory compliance, and preservation of organizational credibility during forensic investigations.

2.Lucas, a forensic investigator, is working on an investigation involving a compromised hard drive. To analyze the disk image and extract relevant forensic data, he decides to use a tool that integrates the powerful capabilities of Sleuth Kit with Python scripting. Lucas wants to automate the process of analyzing disk structures, file systems, and file recovery using Python scripts.
Which of the following tools can help Lucas leverage Sleuth Kit's capabilities while using Python to perform these analysis tasks efficiently?
A. PyTSK
B. NumPy
C. PyTorch
D. PySpark
**Answer:** A
**Explanation:**
According to CHFI v11 objectives under Computer Forensics Fundamentals and Digital Forensics using Python, investigators are encouraged to automate forensic analysis tasks to improve efficiency, accuracy, and repeatability. The Sleuth Kit (TSK) is a widely used open-source forensic toolkit for analyzing disk images, file systems, and recovering deleted files. To extend these capabilities using

Python, CHFI v11 highlights the use of Python bindings specifically designed for forensic purposes. PyTSK (also known as pytsk3) is the official Python binding for The Sleuth Kit. It allows forensic investigators to programmatically access disk images, partitions, file systems, directories, and file metadata directly from Python scripts. This enables automation of tasks such as file enumeration, timeline creation, deleted file recovery, and artifact extraction—core activities in disk and file system forensics.
The other options are not suitable in this context. NumPy is designed for numerical computation, PyTorch is used for machine learning, and PySpark is intended for big data processing. None of these tools integrate with Sleuth Kit or provide native disk forensic analysis capabilities. Therefore, PyTSK is the correct and CHFI-aligned choice for Python-based Sleuth Kit forensic automation.

3.During a federal investigation, a lawyer unintentionally discloses privileged information to a federal agency. The disclosure includes sensitive details related to a corporate client's ongoing legal dispute. In the scenario described, what conditions must be met for the unintentional disclosure to extend the waiver of attorney-client privilege or work-product protection to undisclosed communications in both federal and state proceedings?
A. The disclosed and undisclosed communications must concern different subject matters.
B. The waiver must be unintentional.
C. The disclosure must be accidental.
D. The waiver must be intentional, and the disclosed and undisclosed communications must concern the same subject matter.
**Answer:** D
**Explanation:**
This question aligns with CHFI v11 objectives related to legal compliance, rules of evidence, and handling privileged information during forensic investigations. In digital forensics, investigators frequently work alongside legal teams, making it critical to understand when attorney-client privilege or work-product protection may be waived. Under the U.S. Federal Rules of Evidence (Rule 502), an unintentional or inadvertent disclosure does not automatically extend the waiver of privilege to undisclosed communications.
For a waiver to extend beyond the disclosed material, strict conditions must be met. The waiver must be intentional, the disclosed and undisclosed communications must concern the same subject matter, and fairness must require that the undisclosed information also be considered. CHFI v11 emphasizes that forensic investigators must preserve confidentiality, respect legal protections, and avoid actions that could improperly broaden legal exposure during investigations.
Options B and C are incorrect because unintentional or accidental disclosures are explicitly protected from subject-matter waiver under Rule 502.
Option A is incorrect because waiver extension only applies when communications involve the same subject matter. Therefore, Option D correctly reflects both legal standards and CHFI-aligned best practices for evidence handling and legal awareness during forensic investigations.

4.A forensic investigator is assigned to investigate a data leak involving the distribution of sensitive corporate information across multiple online platforms. The suspect is believed to have shared the data discreetly through various public channels. To uncover evidence, the investigator needs to collect posts, photos, videos, and user interactions from multiple networks. The investigator requires a tool that can

efficiently gather, organize, and analyze this data, ensuring the integrity of the evidence for further investigation.
Which tool would be best suited for this task?
A. LiME
B. Elastic Stack
C. Social Network Harvester
D. Guymager
**Answer:** C
**Explanation:**
This scenario aligns with CHFI v11 objectives under Network and Web Attacks and Social Media Forensics, where investigators are required to collect and analyze digital evidence from online platforms while preserving evidentiary integrity. When sensitive data is leaked through public or semi-public online channels, social media and online network artifacts such as posts, multimedia content, comments, likes, and user relationships become critical sources of evidence.
Social Network Harvester is specifically designed for social media and online platform investigations. It allows forensic investigators to systematically collect data such as posts, images, videos, timestamps, usernames, and interaction metadata from multiple social networks. CHFI v11 emphasizes the importance of using purpose-built tools that support structured collection, proper documentation, and evidence preservation to maintain chain of custody and admissibility.
LiME is a volatile memory acquisition tool, Elastic Stack is primarily used for log aggregation and analysis, and Guymager is a forensic disk imaging tool. None of these are suitable for harvesting social media content. Therefore, Social Network Harvester is the most appropriate CHFI-aligned tool for efficiently gathering, organizing, and analyzing social network evidence in data leakage investigations.

5.During a live data acquisition procedure, forensic investigators are tasked with analyzing a suspected breach of a corporate network. The breach involves unauthorized access to sensitive files stored on the company's servers. Investigators aim to gather volatile data to trace the origin of the breach and identify potential network vulnerabilities.
In a live data acquisition scenario, which types of volatile data would investigators prioritize capturing to trace the intrusion's origin and identify network vulnerabilities?
A. Printer driver versions and configurations
B. Current system uptime and DLLs loaded
C. Open connections and routing information
D. Mouse click activity and cursor movements
**Answer:** C
**Explanation:**
This question directly maps to CHFI v11 objectives under Data Acquisition and Duplication, specifically live data acquisition and the order of volatility. Live forensics is critical when systems cannot be powered down without losing crucial evidence, particularly during active or recent network intrusions. CHFI v11 emphasizes that investigators must prioritize volatile data that can quickly disappear when a system is shut down or network conditions change.
Open network connections, active sessions, routing tables, ARP cache, and listening ports provide immediate insight into how an attacker accessed the system, whether lateral movement occurred, and which external or internal IP addresses were involved. Capturing this data helps investigators trace the

intrusion’s origin, identify command-and-control communications, and uncover misconfigurations or exposed services that enabled the breach.
Printer configurations and mouse activity have little forensic value in network intrusion analysis, while system uptime and loaded DLLs are useful but secondary compared to real-time network artifacts. CHFI v11 clearly prioritizes network-related volatile data during live acquisition to support intrusion analysis, vulnerability identification, and incident reconstruction. Therefore, capturing open connections and routing information is the most critical and correct choice in this scenario.