Vendor: EC-Council

Exam Code: 312-49v11

Exam Name: Computer Hacking Forensic Investigator (CHFI-v11)

Version: DEMO

QUESTION 1
Detective Sarah, a skilled digital forensics investigator, begins probing a compromised computer system linked to a cybercrime ring. Prioritizing volatile data, she meticulously plans her evidence-collection strategy. Amidst the investigation, various data sources emerge, each holding potential clues to unraveling the illicit scheme.

Which data source should you prioritize for collection, considering the order of volatility outlined in the RFC 3227 guidelines?

A. Disk or other storage media containing potentially critical files
B. Temporary file systems where recent activity might be stored
C. Archival media such as a DVD-ROM or a CD-ROM
D. The physical configuration and network topology of the system

Answer: D
Explanation:
This question directly relates to CHFI v11 objectives under Data Acquisition and Duplication and the concept of order of volatility, which is formally defined in RFC 3227 (Guidelines for Evidence Collection and Archiving). CHFI v11 stresses that forensic investigators must collect the most volatile data first, as it is the most likely to be lost or altered during system shutdowns or continued operation.

According to RFC 3227, the order of volatility starts with data that changes most rapidly, such as system state and network-related information. This includes the physical configuration of the system, network topology, routing tables, ARP cache, active network connections, and running processes. These elements can disappear immediately if the system is powered off or network connectivity changes, making them the highest priority during live response.

QUESTION 2
Following a cybercrime incident, a forensic investigator is conducting a detailed examination of a suspect's digital device. The investigator needs to preserve and analyze the disk images without being restricted by various image file formats tied to commercial software, which may limit the investigator's ability to work with a range of analysis platforms. The investigator chooses a simple, straightforward, and uncompressed format that can be easily accessed and analyzed using a wide range of forensic tools and platforms, without the need for specialized software. Which data acquisition format should the investigator use in this case?

A. Adopt the raw format that is commonly used in digital evidence investigations.
B. Choose the AFF4 format, which offers advanced features for comprehensive analysis.
C. Employ the advanced forensics format for storing metadata and disk images.
D. Use a proprietary format that is compatible with specific commercial software.

Answer: A
Explanation:
This question maps directly to CHFI v11 objectives under Data Acquisition and Duplication and Data Acquisition Formats. CHFI v11 clearly explains that the RAW (dd) image format is the most widely used and universally supported forensic image format. RAW images are exact bit-by-bit copies of storage media and do not rely on proprietary structures, compression, or vendor-specific software. This makes them ideal when investigators require maximum compatibility across multiple forensic tools and platforms.

The RAW format is simple, uncompressed, and transparent, allowing it to be analyzed by nearly all forensic suites such as Autopsy, FTK, EnCase, and The Sleuth Kit. CHFI v11 emphasizes that RAW images are preferred when long-term accessibility, court admissibility, and tool

independence are critical requirements.

QUESTION 3
A large multinational corporation, specializing in financial services, recently experienced a potential data breach that affected their critical business systems. As part of the forensic investigation, the organization must quickly restore its servers, both fully and at a granular level, to determine the extent of the breach and verify the integrity of sensitive financial data. The forensic team needs a comprehensive and reliable tool that can perform full image-level backups of their servers, as well as allow for selective file and folder restores in order to investigate individual systems and recover specific documents and configuration files. The tool should be able to handle both physical and virtual environments efficiently, ensuring minimal downtime and accurate data recovery.
Given the organization's need for rapid and reliable recovery, the forensic team must choose a tool that can restore entire systems in case of failure while also offering the flexibility to restore individual files or folders from the backup image. This capability is critical for isolating the compromised systems and recovering vital business records that may have been affected by the breach. The organization requires a solution that not only restores data but also provides the ability to maintain business continuity during the investigation, ensuring that systems are up and running as quickly as possible while maintaining forensic integrity.
Which of the following forensic tools would be best suited for this task?

A. Snagit
B. Macrium Reflect Server
C. VMware vSphere Hypervisor
D. Ezvid

Answer: B
Explanation:
This scenario directly aligns with CHFI v11 objectives under Data Acquisition and Duplication and Digital Forensic Imaging and Recovery Tools. In large-scale enterprise investigations--especially within financial institutions--CHFI v11 emphasizes the importance of tools that support full disk imaging, rapid system recovery, and granular restoration to ensure both forensic analysis and business continuity.

Macrium Reflect Server is specifically designed for server environments and supports full image-level backups, differential and incremental imaging, and selective file and folder recovery from forensic images. This allows investigators to restore entire systems to operational status quickly while simultaneously extracting specific files, logs, or configuration data needed to assess breach impact and verify data integrity. Importantly, Macrium Reflect supports both physical and virtual systems, making it suitable for complex enterprise infrastructures.

Snagit and Ezvid are multimedia screen-recording tools with no forensic or recovery capability, while VMware vSphere Hypervisor is a virtualization platform rather than a forensic imaging or recovery solution. CHFI v11 stresses that appropriate tool selection is critical to preserving evidence integrity while minimizing operational downtime. Therefore, Macrium Reflect Server is the most suitable and CHFI-aligned tool for rapid, reliable, and forensically sound system and data recovery in this scenario.

QUESTION 4
A cybersecurity firm is conducting a forensic investigation into a suspected data breach at a financial institution. During the investigation, the forensic analysts encounter encrypted files protected by strong passwords, hindering their ability to access critical evidence related to the breach.

Considering the challenges posed by password protection in digital forensics investigations, which anti-forensics technique is being employed to impede the forensic analysis process in this scenario?

A. Data manipulation
B. Data obfuscation
C. Data encryption
D. Data hiding

Answer: C
Explanation:
This scenario aligns with CHFI v11 objectives under Anti-Forensics Techniques, specifically techniques used by attackers to prevent investigators from accessing digital evidence. Data encryption is a well-known and widely used anti-forensic method where files are encrypted using strong cryptographic algorithms and protected with complex passwords. While encryption is a legitimate security control, adversaries often misuse it to deliberately obstruct forensic analysis and delay investigations.

CHFI v11 explains that encrypted files render data unreadable without the correct decryption key, making it extremely difficult for investigators to examine file contents within acceptable timeframes. This can significantly hinder evidence discovery, timeline reconstruction, and incident scoping. Investigators must then rely on password cracking, key recovery, memory forensics, or legal assistance to access the data--each of which introduces complexity, cost, and time delays.

Data manipulation involves altering or deleting evidence, data obfuscation focuses on making data confusing but still accessible, and data hiding conceals information in alternate locations. In contrast, the defining characteristic in this scenario is password-protected encrypted files, which directly corresponds to data encryption. Therefore, consistent with CHFI v11 classifications, data encryption is the correct anti-forensic technique being employed.

QUESTION 5
A digital forensics examiner is investigating a suspected case of corporate espionage involving the theft of sensitive intellectual property from a company's servers. In adherence to ENFSI Best Practices for Forensic Examination of Digital Technology,

what would be the examiner's primary concern?

A. Complying with GDPR data privacy rules.
B. Following ISO/IEC 17025 standards in forensic labs.
C. Establishing secure evidence-handling protocols.
D. Implementing ISO/IEC 27001 for information security.

Answer: C
Explanation:
This question maps directly to CHFI v11 objectives under Computer Forensics Fundamentals and Standards and Best Practices Related to Computer Forensics, specifically the ENFSI Best Practices for the Forensic Examination of Digital Technology. ENFSI (European Network of Forensic Science Institutes) guidelines focus primarily on ensuring that digital evidence is handled in a secure, reliable, and forensically sound manner so that it remains admissible and defensible in legal proceedings.

The examiner's primary concern under ENFSI best practices is the secure handling of digital evidence, which includes proper acquisition, preservation, documentation, storage, and chain of

custody management. These practices ensure evidence integrity, prevent contamination or alteration, and allow results to be independently verified. CHFI v11 emphasizes that forensic investigators must be able to demonstrate that evidence has not been tampered with and that standardized procedures were followed throughout the investigation lifecycle.

While GDPR, ISO/IEC 17025, and ISO/IEC 27001 are important regulatory and security frameworks, they are not the core focus of ENFSI forensic examination guidelines. ENFSI is evidence-centric, prioritizing secure evidence handling and methodological consistency. Therefore, establishing secure evidence-handling protocols is the correct and CHFI-aligned answer.

QUESTION 6
During a cybercrime investigation, the forensic team has seized a large number of devices as part of the evidence collection process. After securing all the devices, the team begins evaluating which exhibits to prioritize for analysis first. The team maintains detailed records of both analyzed and non-analyzed exhibits, ensuring that they can track the progress of the investigation and reference any exhibits that were not immediately analyzed.

Which ENFSI best practice is being followed by the team?

A. The team conducts an initial case evaluation to assess the case's requirements.
B. The team performs a scene assessment to handle evidence at the crime scene.
C. The team carries out a laboratory assessment to document artifacts.
D. The team executes the acquisition of data to extract data from the seized devices.

Answer: C
Explanation:
This scenario aligns with CHFI v11 objectives under Standards and Best Practices Related to Computer Forensics, specifically the ENFSI Best Practices for the Forensic Examination of Digital Technology. According to ENFSI guidelines, once evidence has been seized and secured, a structured laboratory assessment must be conducted before and during analysis. This phase focuses on evaluating exhibits, determining examination priorities, and maintaining detailed documentation of all items--whether analyzed immediately or deferred.

Maintaining records of both analyzed and non-analyzed exhibits is a key ENFSI requirement, as it ensures transparency, traceability, and accountability throughout the forensic process. CHFI v11 emphasizes that proper documentation allows investigators to track investigative progress, justify examination decisions, and demonstrate that no evidence was overlooked or mishandled. This practice also supports effective case management and preserves the integrity and admissibility of evidence in legal proceedings.

QUESTION 7
During a cybersecurity investigation, logs from a Cisco switch, VPN, and DNS server are collected. These logs contain valuable information about network activities and potential security breaches.

In digital forensics, what role do Cisco switch, VPN, and DNS server logs play when analyzing network incidents?

A. Provides insights on network traffic, device connections, and security incidents.
B. Tracks website visits and browser history exclusively.
C. Not pertinent to digital forensics.
D. Details user activities within the local network.

Answer: A
Explanation:
This question aligns with CHFI v11 objectives under Network and Web Attacks and Network Log Analysis. In digital forensics, network infrastructure logs are critical sources of evidence for detecting, analyzing, and reconstructing network-based attacks. CHFI v11 specifically emphasizes the forensic value of logs generated by network devices such as Cisco switches, VPN gateways, and DNS servers.

Cisco switch logs provide information about device connections, port activity, MAC address mappings, VLAN assignments, and potential unauthorized access within the internal network. VPN logs reveal details about remote connections, including authentication attempts, user identities, IP addresses, session durations, and encrypted tunnel activity--crucial for identifying compromised credentials or unauthorized remote access. DNS server logs record domain name queries and responses, which help investigators detect command-and-control communication, data exfiltration attempts, malware beaconing, and access to malicious domains.

QUESTION 8
A cybersecurity analyst is tasked with investigating a series of network anomalies. They employ various event correlation approaches, including graph-based analysis to map system dependencies and neural network-based anomaly detection. Through rule-based correlation and vulnerability-based mapping, they pinpoint potential threats and prioritize response actions effectively.

Which event correlation approach involves constructing a graph with system components as nodes and their dependencies as edges?

A. Rule-Based Approach
B. Codebook-Based Approach
C. Neural Network-Based Approach
D. Graph-Based Approach

Answer: D
Explanation:
This question aligns with CHFI v11 objectives under Procedures and Methodology, specifically event correlation and analysis techniques used to investigate complex incidents. Event correlation is essential for transforming large volumes of logs and alerts into meaningful incident narratives. CHFI v11 describes multiple correlation approaches, each suited to different investigative needs.

The graph-based approach models systems, applications, users, and network components as nodes, while relationships such as dependencies, communications, or trust relationships are represented as edges. By constructing such graphs, investigators can visualize how events propagate across interconnected systems, identify attack paths, and determine how a compromise in one component impacts others. This approach is particularly effective in analyzing lateral movement, dependency-based failures, and multi-stage attacks in enterprise environments.

Rule-based approaches rely on predefined conditions, codebook-based approaches match patterns against known attack templates, and neural network-based approaches focus on anomaly detection using machine learning. While these are valuable, only the graph-based approach explicitly represents system dependencies and relationships in a node-edge structure. Therefore, consistent with CHFI v11 event correlation methodologies, the correct answer is Graph-Based Approach.

QUESTION 9
During a forensic investigation involving an Android device, the investigator needs to establish communication between the device and a computer running the Android Software Developer Kit (SDK). This communication will allow the investigator to access system files, logs, and other relevant data for analysis. To facilitate this, the investigator enables a specific Android developer feature on the device.

Which feature must be enabled to allow the device to communicate with the workstation running the Android SDK?

A. The forensic investigator can enable USB restriction mode on the Android device connected to the external workstation.
B. The investigator can turn on upgrade mode on the target device to be examined in the lab setup.
C. The forensic investigator can trigger recovery mode on the device before connecting to the workstation.
D. The investigator can activate USB debugging mode on the suspected device being analyzed.

Answer: D
Explanation:
This question maps directly to CHFI v11 objectives under Mobile and IoT Forensics, specifically Android device acquisition and analysis procedures. In Android forensics, communication between the device and a forensic workstation running the Android SDK is primarily achieved using the Android Debug Bridge (ADB). ADB enables investigators to interact with the device's file system, retrieve logs, execute commands, and collect forensic artifacts in a controlled manner.

To use ADB, USB Debugging mode must be enabled on the Android device. CHFI v11 explicitly highlights USB debugging as a critical prerequisite for logical acquisition, live data collection, and application-level analysis on Android devices. When enabled, it allows authenticated communication between the device and the forensic workstation without requiring intrusive methods that could alter evidence unnecessarily.

USB restriction mode limits data communication, recovery mode is used mainly for system repairs or flashing firmware, and "upgrade mode" is not a standard Android forensic feature. None of these allow normal SDK-based interaction for forensic analysis. Therefore, consistent with CHFI v11 Android forensic methodology, enabling USB debugging mode is the correct and essential step to establish communication with the Android SDK workstation.

QUESTION 10
Scarlett, a compliance officer, is working for a publicly traded company that has recently faced accusations of financial misconduct. During her investigation, she comes across a law passed by the A.S.Congress in 2002 aimed at protecting investors from fraudulent accounting practices by corporations. This law mandates stricter corporate financial reporting standards, internal controls, and penalties for fraudulent activities.
Which of the following laws is Scarlett most likely reviewing in this case?

A. PCI DSS
B. SOX
C. GLBA
D. ECPA

Answer: B

Explanation:
This question directly aligns with CHFI v11 objectives under Regulations, Policies, and Ethics, particularly laws that influence forensic investigations and corporate compliance. The law described is the Sarbanes-Oxley Act (SOX), enacted in 2002 in response to major corporate accounting scandals such as Enron and WorldCom. CHFI v11 highlights SOX as a critical regulation governing publicly traded companies in the United States.

SOX mandates strict requirements for corporate financial reporting, internal control assessments, executive accountability, audit independence, and record retention. Sections such as SOX Section 302 require executives to personally certify the accuracy of financial statements, while Section 404 enforces internal control audits to prevent fraud. These requirements are highly relevant in forensic investigations involving financial misconduct, as investigators often rely on audit logs, financial records, and compliance documentation governed by SOX.

QUESTION 11
During dynamic malware analysis, a suspicious executable file is executed in a controlled, sandboxed environment. The malware exhibits behavior indicative of network communication and file encryption.

In dynamic malware analysis, what is the primary objective of executing a suspicious file in a sandboxed environment?

A. To observe the behavior and interactions of the malware without risking damage to the host system
B. To enhance the performance of the operating system
C. To determine the author's identity
D. To optimize the storage utilization of the system

Answer: A
Explanation:
This question aligns with CHFI v11 objectives under Malware Forensics, specifically static vs. dynamic malware analysis and the use of sandboxed environments. Dynamic malware analysis involves executing a suspicious file in a controlled and isolated environment to safely observe its real-time behavior. CHFI v11 emphasizes that many modern malware samples use obfuscation, packing, or fileless techniques that conceal their functionality unless they are actually executed.

The primary objective of running malware in a sandbox is to monitor its behavior without endangering production systems. Investigators can observe network communications (such as command-and-control traffic), file system changes, registry modifications, process injection, persistence mechanisms, and encryption activity. These behaviors provide critical indicators of compromise (IoCs) and help investigators understand the malware's capabilities, intent, and impact.

QUESTION 12
Emily, a network security analyst, is reviewing the logs generated by a Cisco firewall after a suspected attack on the company's network. She encounters a log message related to a connection attempt that seems suspicious. The log shows an entry with mnemonic 106022. Based on the firewall's logging patterns, which of the following best describes the log message Emily found?

A. Deny protocol connection spoof from source_address to dest_address on interface interface_name
B. ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest

outside_address
C. Deny protocol reverse path check from source_address to dest_address on interface interface_name
D. Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address

Answer: A
Explanation:
This question aligns with CHFI v11 objectives under Network and Web Attacks and Network Log Analysis, particularly the interpretation of Cisco firewall (ASA) log messages. Cisco ASA firewalls use numeric mnemonics to categorize and describe specific security events. Understanding these mnemonics is critical for forensic investigators when reconstructing attack attempts and identifying malicious network behavior.

The Cisco ASA message ID 106022 corresponds to a "Deny protocol connection spoof" event. This log entry is generated when the firewall detects a packet with a spoofed source address, meaning the packet's source IP does not match the expected routing or interface from which it was received. Such behavior is commonly associated with reconnaissance, evasion attempts, or denial-of-service attacks.

CHFI v11 emphasizes that spoofed connection attempts are strong indicators of malicious activity and are frequently logged by perimeter security devices. By analyzing this log, investigators can identify attempted impersonation, trace attack origins, and correlate events across network devices.

QUESTION 13
During a forensic investigation into a suspected cyberattack, the investigator checks network logs that were collected during the period of the incident. The investigator's objective is to examine these logs to determine the exact sequence of events that took place, identify the source of the attack, and understand the nature of the incident. This analysis helps in uncovering what occurred, how it happened, and who was responsible for it.

Which of the following techniques is the investigator using in this case?

A. The investigator performs eavesdropping on communications to intercept sensitive information.
B. The investigator performs a postmortem analysis of system records to evaluate previous security breaches.
C. The investigator conducts a real-time analysis of network traffic logs to detect the nature of the incident.
D. The investigator carries out IP address spoofing to identify the source of the attack.

Answer: B
Explanation:
This scenario aligns closely with CHFI v11 objectives under Procedures and Methodology, specifically postmortem analysis and log-based forensic investigation. Postmortem analysis refers to the examination of collected system, application, and network logs after an incident has occurred, with the goal of reconstructing events and determining the root cause of a security breach.

In this case, the investigator is reviewing historical network logs collected during the incident window, not monitoring live traffic. CHFI v11 emphasizes that postmortem analysis is essential for answering the core forensic questions: what happened, how it happened, when it happened, and who was responsible. By correlating timestamps, IP addresses, protocols, and event sequences across logs, investigators can identify attack vectors, trace the origin of the attack, and understand attacker behavior.

QUESTION 14
Sophia, a cybersecurity analyst, is investigating a data breach within a company. The breach is suspected to have come from an insider, as sensitive company data was altered from within the company's network. Sophia needs to determine whether the breach was caused by an insider (someone within the company) or an external attacker (someone from outside the company).

Which of the following factors would most likely indicate that the breach was carried out by an insider?

A. The attack used advanced social engineering tactics to exploit external vulnerabilities.
B. The attack was launched from a known external IP address associated with a hacker group.
C. The attacker used a distributed denial-of-service (DDoS) attack to overwhelm the network.
D. The attacker had legitimate access to the company's internal systems and data.

Answer: D
Explanation:
This scenario aligns with CHFI v11 objectives under Computer Forensics Fundamentals and Insider Threat and Identity Theft Forensics. One of the defining characteristics of an insider threat is that the attacker already possesses authorized or legitimate access to internal systems, applications, or sensitive data. CHFI v11 emphasizes that insider attacks often bypass perimeter defenses because the malicious activity originates from trusted accounts, internal IP ranges, or authenticated sessions.

If sensitive data is altered from within the organization's network using valid credentials, it strongly suggests insider involvement. Insiders may include disgruntled employees, contractors, or partners who misuse their access privileges intentionally or unintentionally. This type of breach is often detected through anomalies in user behavior, access logs, privilege misuse, or violations of least-privilege principles.

QUESTION 15
During a large-scale cybercrime investigation, the forensic investigation team is responsible for performing detailed analysis on a variety of digital evidence. To ensure the process is conducted effectively, the team needs to adhere to recognized best practices for selecting and designing analytical methods. Additionally, the team must demonstrate that they have the necessary proficiency and competence to handle the evidence, ensuring that their methodologies are robust and their results are reliable.

Which ISO standard provides the necessary guidance and best practices for these processes, ensuring that the team's analytical processes are both accurate and demonstrably competent?

A. ISO/IEC 27042
B. ISO/IEC 27050
C. ISO/IEC 27037
D. ISO/IEC 27043

Answer: A
Explanation:
This question maps directly to CHFI v11 objectives under Standards and Best Practices Related to Computer Forensics. ISO/IEC 27042 specifically addresses the analysis and interpretation of digital evidence, making it the most relevant standard in this scenario. CHFI v11 emphasizes that forensic analysis must be performed using well-defined, repeatable, and scientifically sound methodologies, and that investigators must be able to demonstrate their technical competence

and analytical proficiency.

ISO/IEC 27042 provides guidance on selecting appropriate analytical techniques, validating forensic tools, interpreting results correctly, and ensuring that conclusions are based on reliable and reproducible processes. It also stresses analyst competence, documentation, peer review, and the avoidance of bias--key factors in ensuring that forensic results are defensible in legal proceedings.

QUESTION 16
Detective Patel, investigating a cross-border cybercrime, faces challenges in gathering evidence due to jurisdictional differences and the remote nature of the attack.

In the context of cross-border cybercrimes, what primary challenge does Detective Patel encounter in collecting evidence for prosecution?

A. Navigate diverse legal frameworks for digital evidence across jurisdictions.
B. Perform physical surveillance to track remote attackers across borders.
C. Coordinate international raids simultaneously.
D. Use advanced encryption for secure data transmission.

Answer: A
Explanation:
This scenario aligns with CHFI v11 objectives under Computer Forensics Fundamentals and Legal Issues and Compliance in Digital Forensics. Cross-border cybercrime investigations are inherently complex because digital evidence is often stored, transmitted, or processed across multiple countries, each governed by its own legal system. CHFI v11 emphasizes that one of the most significant challenges investigators face in such cases is navigating diverse legal frameworks and jurisdictional requirements.

Different countries have varying laws related to data privacy, evidence seizure, admissibility, retention, and disclosure. Investigators must often rely on international cooperation mechanisms such as Mutual Legal Assistance Treaties (MLATs), letters rogatory, or coordination with international law enforcement agencies. These processes can be time-consuming and may delay evidence acquisition, risking data loss due to retention limits imposed by service providers.

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**