Download Eccouncil 312-49v11 Exam Dumps Free

Shared by Pickett on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After implementing an eDiscovery tool, the forensic investigator is responsible for ensuring that all user actions, and changes to the system are accurately logged. This tracking is essential to ensure that every action taken during the investigation is fully transparent and accountable. By doing so, the investigator ensures that there is a reliable proof of all activities within the eDiscovery process. What type of metric is the investigator most likely focusing on in this scenario?

Options:

A- Investigator tracks audit trails to ensure a comprehensive record of all modifications.
B- Investigator focuses on tracking the legal hold imposed on the evidence to ensure compliance.
C- Investigator tracks the number of files reviewed during the investigation process to assess the workload.
D- Investigator measures the accuracy of data extraction during the collection phase to ensure data integrity.

Answer:

A

Explanation:

According to the CHFI v11 Procedures and Methodology domain, the eDiscovery process requires strict accountability, transparency, and defensibility of evidence handling. One of the most critical metrics in eDiscovery investigations is the audit trail, which documents every action performed on evidence throughout its lifecycle.

An audit trail records detailed information such as user access, file modifications, data exports, searches performed, timestamps, and system changes. CHFI v11 emphasizes that maintaining complete audit trails ensures chain of custody, supports legal admissibility, and allows investigators to prove that evidence was not altered or mishandled during the investigation. This is especially important in legal proceedings, where investigators may be required to demonstrate who accessed the data, when it was accessed, and what actions were taken.

The other options represent valid forensic considerations but do not directly address the requirement for full transparency and accountability. Legal holds focus on preservation, workload metrics measure efficiency, and data extraction accuracy addresses integrity---but none provide a complete, chronological record of investigator actions.

CHFI v11 explicitly highlights tracking audit logs and maintaining detailed activity records as a

best practice for eDiscovery to ensure defensibility and compliance with legal standards such as the Electronic Discovery Reference Model (EDRM).

Therefore, the investigator is primarily focusing on audit trail metrics, making Option A the correct and CHFI v11--verified answer.

Question 2

Question Type: MultipleChoice

During a forensic investigation into a cyberattack that compromised a company's sensitive data, the investigator discovers that the organization uses a cloud-based solution for managing user access across various internal systems. This solution includes features such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), and detailed access controls, all handled by a third-party service provider. The investigator examines logs from the authentication system and compares them with system access patterns to trace the illegal actions during the breach. What type of cloud service deployment is being utilized by the organization?

Options:

A- The organization uses Desktop-as-a-Service (DaaS) for access controls or authentication management.
B- The organization uses Infrastructure-as-a-Service (IaaS) for managing user access on systems and the network.
C- The organization uses Platform-as-a-Service (PaaS) to deploy and manage custom-built authentication and access control applications.
D- The organization uses Identity-as-a-Service (IDaaS) for enforcing authorization rules.

Answer:

D

Explanation:

As per the CHFI v11 Cloud Forensics objectives, cloud-based identity and access management solutions that provide Single Sign-On (SSO), Multi-Factor Authentication (MFA), centralized authentication, and fine-grained authorization controls---managed entirely by a third-party provider---are classified as Identity-as-a-Service (IDaaS).

IDaaS is a specialized cloud service model designed specifically for identity management, including authentication, authorization, user provisioning, role-based access control, and

centralized logging of authentication events. In forensic investigations, IDaaS platforms are critical evidence sources because they generate detailed authentication logs, login timestamps, MFA challenges, IP addresses, device identifiers, and anomaly alerts. These logs allow investigators to correlate user identities with access patterns and trace unauthorized or malicious actions across multiple systems.

The CHFI v11 blueprint explicitly differentiates IDaaS from other cloud service models. IaaS focuses on infrastructure resources such as virtual machines and networks, not identity enforcement. PaaS is used for developing and deploying custom applications, which is not indicated here since the authentication is handled by a third party. DaaS delivers virtual desktops and does not inherently manage enterprise-wide authentication and authorization.

Therefore, based on the presence of third-party-managed SSO, MFA, centralized access control, and authentication log analysis, the correct answer---fully aligned with CHFI v11 documentation---is Identity-as-a-Service (IDaaS).

Question 3

Question Type: MultipleChoice

During a cybersecurity investigation involving a data breach at a financial institution, an investigator is tasked with identifying the root cause of the breach and generating a timeline of events that led to the incident. The investigator needs to determine which step in the forensic process will help uncover the sequence of activities, including the vulnerabilities exploited, the time of attack, and the specific actions taken by the attacker. Which of the following forensic techniques is most effective for achieving this goal?

Options:

A- Data duplication
B- Photographing the crime scene
C- Data analysis
D- Data acquisition

Answer:

C

Explanation:

According to the CHFI v11 Forensic Investigation Process and Event Correlation objectives, the

forensic technique that enables investigators to reconstruct the sequence of events and determine the root cause of an incident is data analysis. Data analysis is the phase where collected evidence is examined, correlated, and interpreted to extract meaningful insights about attacker behavior.

During data analysis, investigators examine logs, timestamps, file system metadata, registry entries, network traffic, memory artifacts, and security alerts to perform timeline analysis, event correlation, and kill chain reconstruction. CHFI v11 explicitly highlights techniques such as timeline creation, event deconfliction, and correlation analysis as essential for identifying the time of attack, vulnerabilities exploited, methods used, and actions performed by the attacker.

The other options represent different forensic phases but do not directly achieve the stated goal. Data acquisition focuses on collecting evidence in a forensically sound manner, not interpreting it. Data duplication involves creating forensic copies to preserve evidence integrity. Photographing the crime scene applies primarily to physical forensics and documentation, not digital event reconstruction.

CHFI v11 emphasizes that without proper data analysis, raw evidence remains unstructured and cannot support attribution, root cause analysis, or legal prosecution. Therefore, to uncover the complete sequence of malicious activities and generate an accurate incident timeline, Data analysis is the most effective forensic technique.

Hence, the correct and CHFI-verified answer is Option C.

Question 4

Question Type: MultipleChoice

A user in an authoritarian country seeks to access the Tor network but faces heavy internet censorship. By utilizing bridge nodes, the user's connection is disguised, allowing them to bypass restrictions. Bridge nodes are not listed in public Tor directories, making it difficult for ISPs and governments to identify and block Tor traffic.

How do bridge nodes assist users in accessing the Tor network despite censorship?

Options:

A- By encrypting user data multiple times
B- By hosting websites anonymously
C- By disguising their IP addresses
D- By publicly listing their addresses

Answer:

C

Explanation:

According to the CHFI v11 Dark Web Forensics domain, Tor bridge nodes are specifically designed to help users bypass censorship and surveillance in restrictive environments. Governments and ISPs often block access to Tor by identifying and filtering traffic destined for publicly listed Tor entry (guard) nodes. Once these entry nodes are blocked, users can no longer connect to the Tor network using standard configurations.

Bridge nodes solve this problem by acting as unlisted entry relays whose IP addresses are not published in the public Tor directory. As a result, censorship mechanisms cannot easily identify them. From a forensic and technical perspective, CHFI v11 explains that bridges effectively disguise the initial connection point, making Tor traffic appear less distinguishable from normal internet traffic---especially when combined with pluggable transports such as obfs4 or meek.

While Tor uses layered encryption (onion routing), that function applies to all Tor connections and is not unique to bridges. Bridge nodes do not host websites, and they are explicitly not publicly listed, making Option D incorrect. The key advantage bridges provide is concealing the Tor entry point, which prevents IP-based blocking.

CHFI v11 emphasizes understanding Tor infrastructure---including bridges, relays, and exit nodes---to correctly interpret dark web traffic and censorship circumvention techniques during investigations.

Therefore, bridge nodes assist users in accessing the Tor network by disguising their IP addresses and entry points, making Option C the correct and CHFI v11--verified answer.

Question 5

Question Type: MultipleChoice

Alice, a seasoned iOS developer, dives into her latest project, an immersive gaming app. She delves into utilizing cutting-edge technologies like OpenGL ES, OpenAL, and AV Foundation. As the lines of code intertwine with her creativity, she inches closer to realizing her dream of delivering an app that mesmerizes users on every level. Which layer of the iOS architecture is Alice primarily focusing on for implementing functionalities?

Options:

A- Cocoa Touch Layer
B- Core OS Layer
C- Core Services Layer
D- Media Services Layer

Answer:

D

Explanation:

According to the CHFI v11 objectives under Mobile and IoT Forensics, understanding the iOS architecture stack is essential for both application analysis and forensic investigations. The iOS architecture is divided into four primary layers: Cocoa Touch, Media Services, Core Services, and Core OS. Each layer provides specific frameworks and capabilities.

In this scenario, Alice is working with OpenGL ES, OpenAL, and AV Foundation, which are all core frameworks associated with graphics rendering, audio processing, and multimedia handling. These technologies reside in the Media Services Layer, making Option D the correct answer. The Media Services layer is responsible for supporting 2D/3D graphics, audio, video playback, and media capture---critical components for immersive gaming and multimedia applications.

The Cocoa Touch layer (Option A) focuses on user interface elements and application-level interactions. The Core Services layer (Option C) provides foundational services such as data persistence, networking, and location services. The Core OS layer (Option B) operates closest to the hardware, handling memory management, security, and low-level system operations. None of these layers directly provide the multimedia frameworks highlighted in the scenario.

CHFI v11 explicitly includes iOS architecture and boot process as part of mobile forensics, emphasizing the Media Services layer as the source of multimedia frameworks commonly examined during application and malware analysis on iOS devices

Question 6

Question Type: MultipleChoice

In the realm of web accessibility, there are three layers: the Surface Web, which is easily accessible and indexed by standard search engines; the Deep Web, which contains unindexed content such as confidential databases and private portals; and the Dark Web, a clandestine environment often associated with illegal activities like drug trafficking and cybercrime, accessible through specialized browsers such as Tor.

What distinguishes the Dark Web from the Surface and Deep Web?

Options:

A- It contains legal dossiers and financial records.
B- It enables complete anonymity through encryption.
C- It requires authorization to access.
D- It is indexed by search engines.

Answer:

B

Explanation:

According to the CHFI v11 Dark Web Forensics objectives, the defining characteristic that distinguishes the Dark Web from both the Surface Web and the Deep Web is its ability to provide strong anonymity through layered encryption and anonymization techniques. The Dark Web is intentionally designed to conceal the identities and locations of users, services, and hosting infrastructure.

Access to the Dark Web typically requires specialized software such as the Tor Browser, which routes traffic through multiple encrypted relay nodes (entry, middle, and exit relays). This process, known as onion routing, ensures that no single node knows both the source and destination of the communication. CHFI v11 explicitly highlights that this encryption-based anonymity is what makes the Dark Web attractive for activities such as cybercrime marketplaces, illegal trade, anonymous communications, and covert operations.

The other options do not accurately define the Dark Web. Legal dossiers and financial records are commonly found in the Deep Web, such as banking portals and government databases. Requiring authorization alone does not distinguish the Dark Web, as many Deep Web resources also require credentials. The Dark Web is not indexed by search engines, which is the opposite of Option D.

CHFI v11 emphasizes that understanding this anonymity model is critical for investigators, as it directly impacts attribution challenges, legal considerations, and evidence collection strategies in dark web investigations.

Therefore, the correct distinction---fully aligned with CHFI v11---is that the Dark Web enables complete anonymity through encryption, making Option B the correct answer.

Question 7

Question Type: MultipleChoice

Sarah, a forensic investigator, is conducting a post-compromise investigation on a company's server that contains sensitive dat

a. To ensure the deleted files do not fall into the wrong hands, she follows a media sanitization procedure. The process involves overwriting the deleted data 6 times with alternating sequences of 0x00 and 0xFF, followed by a final overwrite using the pattern 0xAA.

Which of the following media sanitization standards has Sarah followed in this scenario?

Options:

A- NAVSO P-5239-26 (MFM)
B- GOST P50739-95
C- VSITR
D- DoD 5220.22-M

Answer:

C

Explanation:

According to the CHFI v11 Computer Forensics Fundamentals and Evidence Handling and Sanitization guidelines, media sanitization is a critical process used to ensure that deleted or sensitive data cannot be recovered using forensic techniques. Different international standards define specific overwrite patterns and the number of passes required to securely sanitize storage media.

The procedure described---six overwrite passes alternating between 0x00 and 0xFF, followed by a final overwrite with 0xAA---exactly matches the VSITR (Verschlusssache IT Richtlinien) standard. VSITR is a German government--approved data sanitization method that mandates 7 overwrite passes:

Passes 1--6: Alternating 0x00 and 0xFF

Pass 7: Final overwrite with the pattern 0xAA

CHFI v11 explicitly references VSITR as a high-assurance sanitization standard, suitable for environments handling classified or highly sensitive information. This method is more rigorous than commonly used standards such as DoD 5220.22-M, which typically uses 3 passes (or a legacy 7-pass variant with different patterns). NAVSO P-5239-26 (MFM) uses different overwrite schemes, and GOST P50739-95 generally involves fewer passes.

From a forensic and legal standpoint, following a recognized sanitization standard like VSITR demonstrates due diligence, compliance, and defensibility, especially when preventing data

leakage after incidents.

Therefore, based on the overwrite pattern and number of passes described, the media sanitization standard followed by Sarah is VSITR, making Option C the correct and CHFI v11--verified answer.

Question 8

Question Type: MultipleChoice

After a cybercrime investigation involving a compromised Windows system, an investigator is tasked with recovering private browsing artifacts. The investigator decides to retrieve data from the pagefile.sys and other live memory captures to identify traces of activity from private browsing modes.

Which tool should the investigator use to analyze the live system and recover these private browsing artifacts?

Options:

A- PsLoggedOn
B- Exeinfo
C- FTK Imager
D- zsteg

Answer:

C

Explanation:

This question aligns with CHFI v11 objectives under Operating System Forensics and Volatile and Non-Volatile Data Analysis, particularly the recovery of artifacts from live memory and system files such as pagefile.sys. Private browsing modes (e.g., InPrivate, Incognito) are designed to minimize persistent artifacts on disk; however, CHFI v11 emphasizes that memory, page files, and swap files often retain remnants of browsing activity, including URLs, session data, cached content, and credentials.

FTK Imager is a forensically sound tool widely used for live data acquisition, memory capture, and analysis of volatile artifacts. It allows investigators to acquire RAM, pagefile.sys, hiberfil.sys, and other critical system files without altering evidence integrity. CHFI v11 specifically highlights FTK Imager as a preferred tool for collecting and examining live system data and recovering artifacts

that are not available through traditional disk-only analysis.

PsLoggedOn is used to identify logged-in users, Exeinfo analyzes executable file formats, and zsteg is a steganography detection tool. None of these are suitable for live memory or pagefile analysis. Therefore, consistent with CHFI v11 forensic best practices, FTK Imager is the correct tool to recover private browsing artifacts from live Windows systems.

Question 9

Question Type: MultipleChoice

You are a cybersecurity analyst tasked with performing dynamic malware analysis on a suspicious file received by your organization. Your objective is to understand the behavior of the malware by running it in a controlled environment and monitoring its actions without allowing it to propagate to the production network. As a cybersecurity analyst conducting dynamic malware analysis, what is a key aspect of designing the testing environment to ensure the safety of the production network?

Options:

A- Implementing host integrity monitoring to track system changes caused by the malware.
B- Disabling antivirus software to prevent interference with the malware's execution.
C- Running the malware on physical machines to minimize the risk of network propagation.
D- Using outdated operating systems to reduce compatibility issues with the malware.

Answer:

A

Explanation:

According to the CHFI v11 Malware Forensics and Malware Analysis objectives, dynamic malware analysis must be performed in a controlled, isolated, and well-monitored environment to both observe malicious behavior and prevent unintended spread to production systems. A key requirement of such an environment is the ability to monitor and record all system-level changes made by the malware during execution.

Host Integrity Monitoring (HIM) plays a critical role in dynamic malware analysis by tracking modifications to files, registry keys, services, processes, startup locations, system calls, and configuration settings. CHFI v11 emphasizes system behavior analysis as a core component of malware forensics, including monitoring registry artifacts, file system changes, persistence

mechanisms, and process activity. HIM enables investigators to safely analyze malware impact while maintaining forensic visibility and containment.

The other options are not aligned with CHFI v11 best practices. Disabling antivirus software weakens security controls but does not ensure containment or safety. Running malware on physical machines increases the risk of permanent damage and network propagation, which contradicts CHFI guidelines favoring sandboxed or virtualized environments. Using outdated operating systems does not contribute to safety and may introduce irrelevant vulnerabilities.

CHFI v11 strongly advocates controlled malware analysis labs with monitoring mechanisms that capture behavioral indicators without exposing production assets. Therefore, implementing host integrity monitoring is a key design aspect that supports both safe containment and effective behavioral analysis, making Option A the correct and CHFI-verified answer.

Question 10

Question Type: MultipleChoice

Mia, a network administrator, is reviewing the logs of a Cisco router after noticing some performance degradation in her network. While examining the logs, she encounters a particular message that states: ''The system was not able to process the packet because there was not enough room for all of the desired IP header options.'' Mia needs to identify which mnemonic in the Cisco IOS logs corresponds to this specific issue. Which of the following log mnemonics should Mia look for to find this message?

Options:

A- %SEC-4-TOOMANY
B- %IPV6-6-ACCESSLOGP
C- %SEC-6-IPACCESSLOGP
D- %SEC-6-IPACCESSLOGRL

Answer:

A

Explanation:

According to the CHFI v11 Network Forensics and Log Analysis objectives, Cisco IOS log messages use standardized mnemonics to describe specific security and packet-processing conditions. The message indicating that ''there was not enough room for all of the desired IP

header options'' is associated with abnormal or excessive IP header options, which can be indicative of malformed packets, reconnaissance activity, or denial-of-service (DoS) attempts.

The mnemonic %SEC-4-TOOMANY is generated when a router receives packets containing too many IP options for the available buffer space. Cisco devices impose limits on IP header options to protect system resources, and when these limits are exceeded, the packet is dropped and logged with this mnemonic. CHFI v11 highlights such logs as important artifacts when investigating network performance degradation, packet manipulation, and potential attack traffic.

The other options are unrelated to this condition. %IPV6-6-ACCESSLOGP applies to IPv6 access control logging. %SEC-6-IPACCESSLOGP and %SEC-6-IPACCESSLOGRL relate to access-list permit/deny logging and rate-limited ACL messages, not IP header option exhaustion.

From a forensic perspective, identifying %SEC-4-TOOMANY helps investigators correlate performance issues with malformed or malicious traffic patterns and supports attribution during network attack investigations.

Therefore, the correct Cisco IOS log mnemonic corresponding to this issue---fully aligned with CHFI v11---is %SEC-4-TOOMANY (Option A).

Question 11

Question Type: MultipleChoice

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?

Options:

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.

The other options do not reflect primary forensic challenges. Physical surveillance and coordinated raids are operational law enforcement activities, not core digital evidence issues, and encryption is a technical safeguard rather than a legal obstacle. CHFI v11 highlights that understanding and complying with international legal requirements is critical to ensuring evidence is lawfully obtained and admissible in court. Therefore, navigating diverse legal frameworks across jurisdictions is the primary challenge in cross-border cybercrime investigations.