Eccouncil 312-49v11 Practice Questions

Shared by Avery on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During a malware analysis investigation, a suspicious Microsoft Office document is identified as a potential threat. The document contains embedded macros and triggers unusual behavior when opened. In digital forensics, what is the primary purpose of analyzing suspicious Microsoft Office documents?

Options:

A- To determine the author's identity
B- To optimize the formatting and layout of the document
C- To identify potential malware or malicious code embedded within the document
D- To improve the performance of Microsoft Office applications

Answer:

C

Explanation:

According to the CHFI v11 objectives under Malware Forensics and Static and Dynamic Malware Analysis, Microsoft Office documents are one of the most common delivery mechanisms for malware, especially through malicious macros, embedded scripts, and exploit-laden objects. Attackers frequently weaponize Word, Excel, and PowerPoint files to execute malicious code when a user opens the document or enables macros.

The primary forensic purpose of analyzing suspicious Microsoft Office documents is to identify embedded malware or malicious code and understand how it executes. Investigators examine macro code (VBA), embedded objects, OLE streams, and document metadata to detect indicators such as obfuscated scripts, PowerShell execution commands, shellcode loaders, or downloader functionality. CHFI v11 emphasizes that this analysis helps determine the infection chain, execution triggers, and potential impact on the compromised system.

Options A, B, and D are not valid forensic goals in this context. Identifying the document author (Option A) may be supplementary but does not address the core threat. Formatting optimization (Option B) and performance improvement (Option D) are unrelated to forensic or security investigations.

The CHFI Exam Blueprint v4 explicitly includes analyzing suspicious Word, Excel, and PDF documents as part of malware investigations, highlighting the need to detect hidden malicious logic and prevent further compromise. Therefore, identifying embedded malware or malicious code is the correct and exam-aligned objective

Question 2

Question Type: MultipleChoice

As a forensic investigator specializing in cybersecurity, you've been assigned to analyze a suspicious PDF document named ''infected.pdf.'' This document was discovered on a company server and is suspected to contain malicious scripts that could pose a threat to the organization's systems and network. As part of your investigation into the PDF document, what initial step would you take to identify potential malicious components within the file?

Options:

A- Run the command python pdfid.py infected.pdf in a Linux terminal to review the file's structure and identify any embedded scripts.
B- Open the PDF document in a virtual machine environment to observe potential malicious behavior.
C- Utilize a web-based tool to extract metadata from the PDF document and analyze any anomalies.
D- Use a hex editor to manually inspect the contents of the PDF document for suspicious patterns.

Answer:

A

Explanation:

According to the CHFI v11 objectives under Malware Forensics and Static Malware Analysis, the correct initial step when analyzing a suspicious document---such as a potentially malicious PDF---is to perform static analysis before any execution. Running the tool PDFiD using the command python pdfid.py infected.pdf is a standard and CHFI-aligned first action. PDFiD is designed to quickly scan a PDF file and identify suspicious elements such as /JavaScript, /OpenAction, /Launch, /EmbeddedFile, and /AA, which are commonly abused by attackers to deliver malware through PDF documents.

This approach is non-intrusive and ensures the investigator does not accidentally trigger malicious code, thereby preserving evidence integrity and maintaining forensic soundness. Opening the file in a virtual machine (Option B) constitutes dynamic analysis, which should only be performed after initial static indicators suggest malicious intent and after proper containment controls are in place. Metadata extraction (Option C) is useful but limited, as metadata alone does not reliably expose embedded exploit code. Manual hex inspection (Option D) is advanced and time-consuming and is not recommended as the first step.

The CHFI v11 Exam Blueprint emphasizes a structured malware analysis workflow, starting with static analysis tools like PDFiD for suspicious documents, making Option A the most appropriate and exam-accurate answer

Question 3

Question Type: MultipleChoice

You're a forensic investigator tasked with analyzing a potential security breach on an Internet Information Services (IIS) web server. Your objective is to collect and analyze IIS logs to determine how and from where the attack occurred. Where are IIS log files typically stored by default on Windows Server operating systems?

Options:

A- %AppData%\Microsoft\IIS\Logs
B- %ProgramFiles%\IIS\Logs
C- %SystemDrive%\inetpub\logs\LogFiles
D- %SystemRoot%\Logs\IIS

Answer:

C

Explanation:

According to the CHFI v11 objectives under Web Application Forensics and Log Analysis, knowing the default storage locations of web server logs is essential for reconstructing web-based attacks. On Windows Server operating systems, Internet Information Services (IIS) stores its HTTP and HTTPS request logs by default in the directory:

%SystemDrive%\inetpub\logs\LogFiles

This directory contains subfolders such as W3SVC1, W3SVC2, etc., where each folder corresponds to a specific IIS website instance. The log files stored here record critical forensic details including client IP addresses, timestamps, HTTP methods, requested URLs, status codes, user agents, and referrers. These artifacts allow investigators to identify attack vectors such as SQL injection, command injection, directory traversal, brute-force attempts, and web shell uploads.

The other options are incorrect because they do not represent default IIS log locations. %AppData% is user-profile specific, %ProgramFiles% contains application binaries rather than logs, and %SystemRoot%\Logs\IIS is not a standard IIS logging path.

The CHFI Exam Blueprint v4 explicitly covers IIS web server architecture and log analysis, emphasizing familiarity with default log paths to ensure timely evidence acquisition and accurate incident reconstruction. Therefore, %SystemDrive%\inetpub\logs\LogFiles is the correct and exam-aligned answer

Question 4

Question Type: MultipleChoice

You're a digital forensics investigator tasked with analyzing a bitmap image file (BMP) to gather information about its structure and contents. Understanding the file structure and data components is essential for conducting a thorough analysis. Which component of a bitmap image file contains data about the type, size, and layout of the file?

Options:

A- File header
B- Image data
C- Information header
D- RGBQUAD array

Answer:

C

Explanation:

According to the CHFI v11 objectives under Analyzing Various File Types and Image File Analysis (BMP), understanding bitmap (BMP) file structure is critical for identifying hidden data, detecting tampering, and validating file integrity during forensic investigations. A BMP file is composed of multiple structured components, each serving a specific purpose.

The Information Header (also known as the DIB header) is the component that contains detailed metadata about the bitmap image. This includes essential attributes such as image width and height, color depth (bits per pixel), compression method, image size, resolution, and pixel layout. These attributes define how the image data should be interpreted and rendered, making the information header central to forensic analysis. Investigators rely on this header to verify whether image properties are consistent with expectations or have been manipulated.

The File Header (Option A) primarily identifies the file as a BMP and provides the offset to the image data, but it does not describe the image layout in detail. Image data (Option B) contains the actual pixel values, while the RGBQUAD array (Option D) defines the color palette for indexed images and does not describe file structure.

The CHFI Exam Blueprint v4 explicitly covers BMP file analysis and hex-level examination, highlighting the Information Header as the key structure for understanding bitmap characteristics, making Option C the correct and exam-aligned answer

Question 5

Question Type: MultipleChoice

Madison, a forensic investigator, has been assigned to investigate a case of email fraud, where the suspect allegedly used a compromised email account to send phishing emails to several victims. As part of the investigation, Madison must first obtain permission to conduct an on-site examination of the suspect's machine and the email server used for the fraudulent emails.

What is the initial step that Madison must take before proceeding with the forensic examination?

Options:

A- Seizing the computer and email accounts
B- Retrieving email headers
C- Recovering deleted email messages
D- Analyzing email headers

Answer:

A

Explanation:

This question aligns with CHFI v11 objectives under Regulations, Policies, and Ethics and Search and Seizure of Digital Evidence. Before any forensic examination can legally take place---especially an on-site examination involving computers and email servers---the investigator must obtain proper legal authorization. In practice, this authorization is enforced through the lawful seizure of systems and accounts, either via a search warrant, court order, or explicit consent from the system owner.

CHFI v11 emphasizes that digital forensic investigations must strictly follow legal procedures to ensure evidence admissibility and avoid violations of privacy or due process. Seizing the computer systems and email accounts establishes lawful control over the evidence, enables proper chain of custody documentation, and prevents further tampering or destruction of data. Only after seizure and authorization can investigators safely proceed with technical tasks such as retrieving email headers, recovering deleted messages, or analyzing email content.

The other options describe forensic analysis steps that occur after legal access has been granted. Performing them without authorization could invalidate evidence and expose the investigator to legal liability. Therefore, consistent with CHFI v11 best practices and legal requirements, seizing the computer and email accounts is the correct initial step before proceeding with the forensic examination.

Question 6

Question Type: MultipleChoice

You, as a forensic investigator, have been assigned to investigate a case involving the suspect's email communication. During the investigation, you discover that the emails from the suspect's Trash folder may contain crucial evidence. The emails are stored in .pst files, and you must extract and analyze all relevant email messages, including those that were deleted or marked as corrupted. To ensure the integrity of the data, you need a tool that can efficiently process these files, recover any deleted messages, and provide a clear view of the email contents for analysis. Which option best tools would be best suited for this task?

Options:

A- P2LOCATION's Email Header Tracer
B- Email Dossier
C- Hunter's Email Verifier
D- SysTools MailPro+

Answer:

D

Explanation:

According to the CHFI v11 objectives under Email Forensics and Digital Evidence Analysis, investigators must be capable of extracting, recovering, and analyzing email data stored in proprietary formats such as Microsoft Outlook PST files. PST files often contain emails from Inbox, Sent Items, Trash, and Archive folders, and may include deleted or corrupted messages that are highly relevant to an investigation.

SysTools MailPro+ is a forensic-grade email analysis tool designed specifically to handle PST file processing and recovery. It allows investigators to open, parse, and analyze PST files while recovering deleted emails, attachments, and metadata such as headers, timestamps, sender/recipient details, and message paths. CHFI v11 emphasizes the importance of using tools that support evidence integrity, selective extraction, and comprehensive visibility into email contents, all of which are core capabilities of MailPro+.

The other options are not suitable for this task. P2LOCATION's Email Header Tracer focuses on tracing email headers for routing analysis, not PST recovery. Email Dossier and Hunter's Email Verifier are OSINT and email validation tools used for profiling and verification, not forensic extraction or recovery of mailbox data.

The CHFI Exam Blueprint v4 highlights email evidence acquisition, deleted email recovery, and PST analysis as key forensic competencies. Therefore, SysTools MailPro+ is the most appropriate and exam-aligned tool for this investigation

Question 7

Question Type: MultipleChoice

Following a data breach, suspicion falls on an employee who had access to sensitive information. Insider threat tools are deployed to scrutinize the employee's digital activities and flag any anomalous behavior, aiding both the investigation and the prevention of future breaches.

How do insider threat tools contribute to cybersecurity in the given scenario?

Options:

A- By monitoring and detecting suspicious behavior within the organization
B- By analyzing competitor strategies
C- By predicting market trends
D- By enhancing social media presence

Answer:

A

Explanation:

According to the CHFI v11 Network and Web Attacks and Insider Threat Forensics objectives, insider threats represent a significant risk because trusted users already have legitimate access to systems, data, and networks. As a result, detecting malicious activity by insiders requires continuous monitoring and behavioral analysis, rather than traditional perimeter-based security controls.

Insider threat tools are specifically designed to monitor user activities, such as file access, data transfers, login behavior, privilege escalation, email usage, USB activity, and abnormal network connections. CHFI v11 emphasizes that these tools establish a baseline of normal user behavior and then identify deviations that may indicate data exfiltration, sabotage, fraud, or policy violations. Alerts generated by these tools help investigators quickly identify suspicious actions and correlate them with timelines and access rights.

The other options are unrelated to the purpose of insider threat tools. Analyzing competitor strategies and predicting market trends fall under business intelligence, not cybersecurity. Enhancing social media presence is a marketing function and has no relevance to forensic investigations or breach prevention.

CHFI v11 highlights insider threat monitoring as a critical component of post-breach investigations and proactive defense, enabling organizations to both investigate incidents and

reduce the risk of recurrence.

Therefore, in this scenario, insider threat tools contribute to cybersecurity by monitoring and detecting suspicious behavior within the organization, making Option A the correct and CHFI v11--verified answer.

Question 8

Question Type: MultipleChoice

In a critical investigation, forensic experts aim to perform physical acquisition on a rooted Android device using the dd command. This method ensures comprehensive replication of all data, including hidden and deleted files, demanding precise execution. What steps are involved in physical acquisition on a rooted Android device using the dd command?

Options:

A- Establish a secure connection, navigate to the root directory, and execute DD remotely.
B- Use custom hardware, connect directly, and execute DD for acquisition.
C- Connect via Bluetooth, gain root access, and execute DD with source and destination.
D- Connect the device, acquire the root shell, identify the source and destination, and execute DD.

Answer:

D

Explanation:

According to the CHFI v11 Mobile Device Forensics objectives, physical acquisition of an Android device aims to obtain a bit-by-bit image of the device's storage, allowing investigators to recover deleted files, unallocated space, and hidden artifacts. When a device is rooted, investigators can leverage low-level Linux utilities such as the dd command to perform this acquisition.

The correct forensic procedure involves first connecting the Android device to the forensic workstation, typically via USB using ADB. The investigator must then obtain a root shell, as root privileges are mandatory to access raw block devices (for example, /dev/block/mmcblk0). Next, the investigator must identify the correct source (the physical partition or block device) and define the destination, which may be an external storage location or a streamed image file captured on the forensic workstation. Finally, the dd command is executed with precise input (if=) and output (of=) parameters to create a forensic image.

CHFI v11 stresses that this process must be conducted carefully to avoid data alteration and to maintain evidentiary integrity. The other options are incorrect because Bluetooth is not used for forensic imaging, custom hardware is not required for dd-based acquisition, and vague ''remote execution'' does not reflect the structured steps mandated by CHFI methodology.

Therefore, the CHFI v11--verified and forensically sound procedure is to connect the device, acquire the root shell, identify the source and destination, and execute dd, making Option D the correct answer.