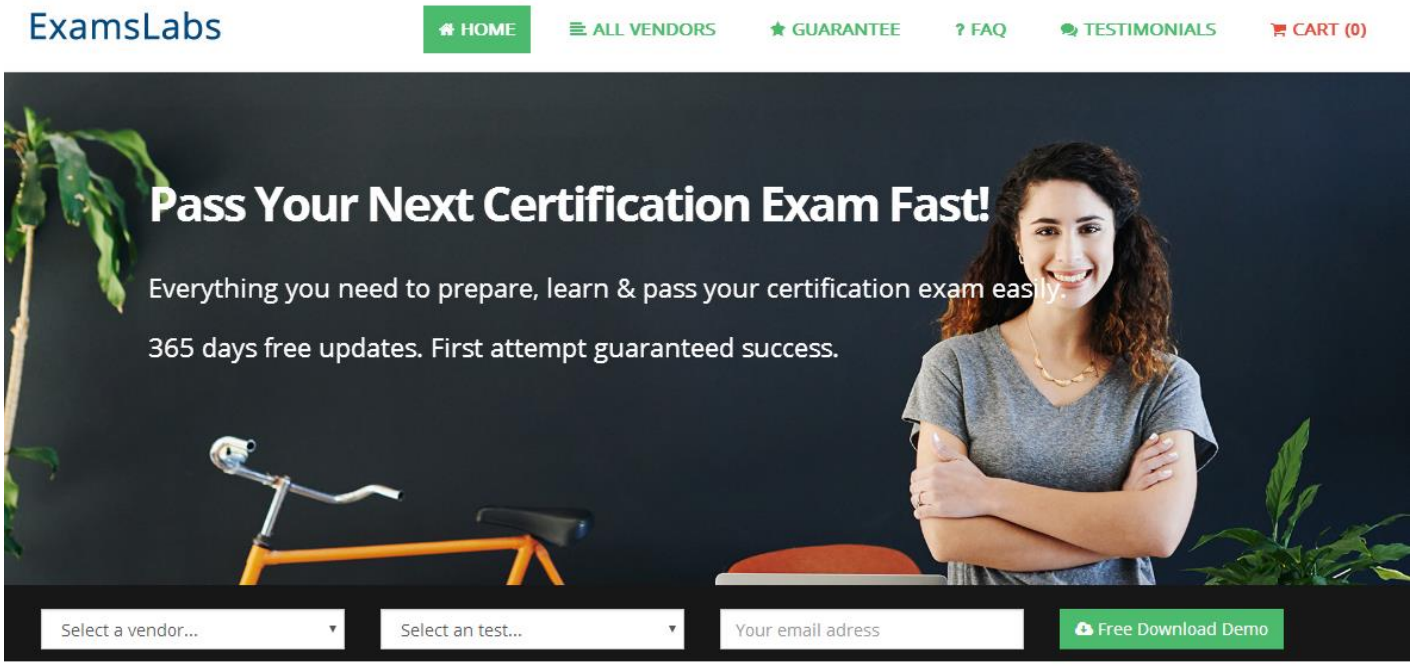
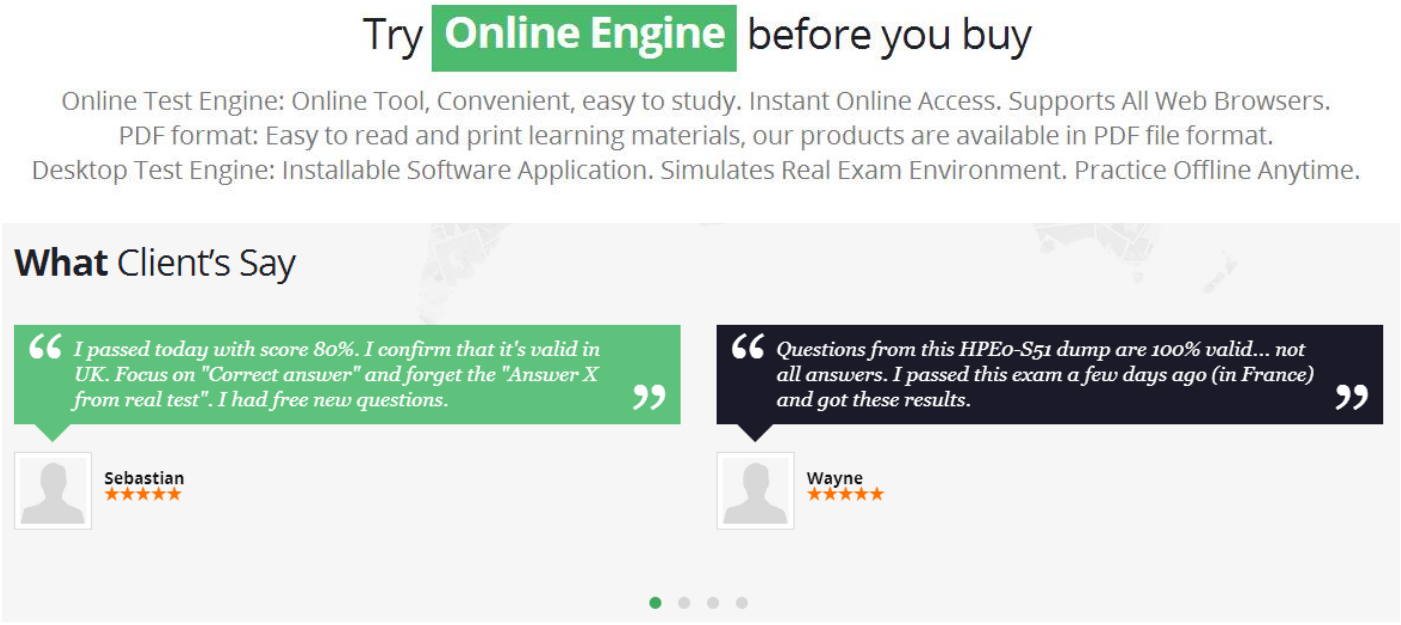
ExamsLabs





http://www.examslabs.com/

Latest Study Materials, Valid Dumps - ExamsLabs

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

Title : Computer Hacking Forensic Investigator (CHFI-v11) (312-49v11日本語版)

Vendor : EC-COUNCIL

Version : DEMO

QUESTION NO: 1
テキサス州オースティンで行われた企業不正調査において、調査官は、復元可能なデジタル証拠の量と質を低下させるような方法で、ファイルが消去され、ログが改ざんされ、タイムスタンプが操作され、コンテンツが隠蔽されていたことを発見した。サイバー犯罪の際に加害者が用いるこのような行為を最も適切に表す用語はどれか？
A. 総当たり攻撃手法
B.鑑識対策技術
C. ディスクの消磁技術
D.バイパス技術
Answer: B
Explanation:
The correct answer is B because the actions described are classic anti-forensics techniques. CHFI v11 explicitly covers anti-forensics as a major topic and includes examples such as data and file deletion, trail obfuscation, artifact wiping, overwriting data or metadata, steganography, encryption, alternate data streams, and other methods intended to frustrate evidence recovery or analysis. The key clue in the question is that the attacker is not merely damaging systems, but deliberately reducing the quantity, quality, and reliability of digital evidence. That is the defining purpose of anti-forensics. Brute-force techniques are aimed at guessing credentials or cracking protections, not concealing traces. Disk degaussing is a specific media-erasure method, not the broader class of conduct described here. Bypassing techniques is too vague and does not capture the forensic-evasion purpose. In CHFI exam logic, whenever the scenario involves deleting artifacts, manipulating timestamps, altering logs, or hiding content to impair an investigation, the correct classification is anti-forensics. This fits directly under the CHFI v11 blueprint area that addresses anti-forensics techniques and the challenges they create for investigators.

QUESTION NO: 2
テキサス州のコンサルティング会社でメール添付ファイルのレビューを行っていた際、署名は問題ないものの、自動実行の可能性がある埋め込みスクリプトが含まれている文書が見つかり、外部ソースからの隠蔽されたダウンロードが懸念されました。ファイルを解析し、難読化された文字列やダウンロードコマンドなどの兆候を、実行せずに特定するには、調査担当者は最初の構造マッピングの後、次にどのようなツールを使用すべきでしょうか？
A. キャスティング
B. oledump
C. 簡単に検出できます
Answer: A
Explanation:
The correct answer is A because olevba is designed to statically extract and analyze VBA macro code from suspicious Office documents without executing them. After initial structure mapping has already been done, the next need in the scenario is to inspect embedded script logic for indicators such as auto-exec triggers, obfuscated strings, suspicious commands, and possible download behavior. That is exactly the type of analysis olevba is commonly used for. Didier Stevens' material and other macro-analysis workflows distinguish between structure-oriented triage and deeper VBA-focused review. oledump is very useful for OLE

stream inspection and mapping, but the question says that initial structure mapping has already been completed. Detect It Easy focuses more on file identification, packers, and executable characteristics than detailed VBA macro review. CHFI v11 includes analysis of suspicious Word, Excel, and PDF documents under malware forensics, so candidates are expected to choose the tool that reveals macro logic and auto- execution indicators without running the file. In this context, olevba is the most precise next step.

QUESTION NO: 3
容疑者の携帯端末が関係する犯罪捜査において、鑑識チームはAndroidとiOSの両方のスマートフォンから得られたデジタル証拠を分析する必要がある。それぞれのプラットフォームには、鑑識分析において特有の課題と手法が存在する。
これらのデバイスからデジタル証拠を効果的に抽出・分析するために、AndroidおよびiOSのフォレンジック分析に関する以下の記述のうち、最も正確なものはどれですか？
A.
iOSは包括的なデジタル証拠抽出のための強力なオープンソースのフォレンジックツールを提供していますが、Androidはフォレンジックソフトウェアのサポートが限られているため、手動による抽出に頼っています。
B. Android デバイスと iOS デバイスはどちらも FAT32
ファイルシステムを使用しているため、クロスプラットフォーム互換性と、広く利用可能なツールによる簡単なフォレンジック分析が容易になります。
C. Android: 単一パーティションによりフォレンジック分析が容易になります。iOS:
サンドボックスと暗号化の複雑さによりデータ抽出が妨げられます。
D. Android デバイスは、標準的なフォレンジック
ツールで簡単にファイルを抽出できるように Ext4 を使用します。一方、iOS
デバイスは、APFS (Apple ファイルシステム)
の暗号化と複雑さのため、特別な技術が必要です。
Answer: D
Explanation:
Option D is the most accurate answer because CHFI v11 explicitly includes Android and iOS forensic analysis , logical and physical acquisition of Android and iOS devices , Android and iOS file systems , and APFS file system analysis as major mobile-forensics objectives. Android devices are commonly associated in forensic contexts with Ext4-based storage structures , while iOS devices use APFS , which introduces additional complexity due to Apple's security model, sandboxing, and strong encryption protections. That makes iOS extraction and examination more dependent on specialized methods and tools. This matches the CHFI view that mobile platforms require different forensic strategies rather than one uniform method.
Option A reverses the practical situation. B is incorrect because FAT32 is not the shared native forensic file- system answer for both platforms. C contains a partially plausible idea about iOS complexity, but it is less precise and less aligned to the file-system-focused wording than D . Therefore, based on CHFI mobile- forensics objectives, the strongest answer is that Android commonly uses Ext4 , while iOS uses APFS and often requires more specialized forensic handling.

QUESTION NO: 4

企業環境において、不正なデータアクセスの兆候が見られたことを受け、上級幹部のAndroidスマートフォンが内部フォレンジック調査のために保護されました。この調査は管理上のものであり、幹部は調査への協力のために待機しています。デバイスはパスコードで保護されており、潜在的な証拠への即時アクセスはできません。調査担当者は、既存のデータを変更したり、高度な技術的措置を講じたりすることなく、アクセス権を取得する必要があります。証拠の完全性を維持しながら合法的に調査を進めるには、どの方法が最も適切でしょうか？

A.従業員の協力を得てパスコードを自主的に開示し、調査の完全性を損なうことなく合法的なデータアクセスを確保する。

B.
法令および倫理基準を遵守しながら、体系的に組み合わせを推測してデータにアクセスする、Android 専用のフォレンジック ソフトウェアを使用する。

C.
リモートMDMソフトウェアを使用してデバイスのパスコードをリセットし、証拠の完全性を維持しながらデータアクセスを有効にします。

D.証拠の完全性を損なうことなくデータへのアクセスを確保するために、専用ツールを使用して物理デバイスの取得に関する管理承認を要求します。

Answer: A

Explanation:

Option A is the most appropriate answer because CHFI v11 places strong emphasis on legal compliance, seeking consent, preserving evidence, chain of custody, and following a sound forensic process . In this scenario, the matter is administrative , the device owner is available , and investigators need access without altering data or resorting to more intrusive technical actions. Under those conditions, obtaining the employee' s voluntary cooperation and passcode disclosure is the most defensible and least disruptive method. The blueprint explicitly includes seeking consent , best practices for handling digital evidence , preserving evidence , and chain of custody under legal and procedural requirements.

This answer also aligns with CHFI's mobile forensics areas covering mobile phone evidence analysis, data acquisition methods, logical and physical acquisition of Android devices, and challenges in mobile forensics . Investigators should first use the least destructive, most lawful, and most forensically sound approach before considering advanced acquisition techniques.

Option B is too intrusive for this fact pattern, C alters device state, and D escalates unnecessarily when consent-based access is already available.

QUESTION NO: 5

フォレンジック調査員であるケイセン氏は、侵害を受けたWindowsマシンを調査していました。調査中、ケイセン氏は侵害の影響を把握するために、マシン上で実行されているアプリケーションとサービスに関する重要な情報を収集する必要がありました。調査員は、データ収集がシステムの状態に影響を与えたり変更したりしないようにしながら、アクティブなプロセスや実行中のサービスなどの揮発性の証拠をリアルタイムで収集する必要があります。上記のシナリオにおいて、ケイセン氏にとって役立つツールは次のうちどれでしょうか？

A. Exifツール

B. ワイヤーシャーク

C. タスクリスト

D. ヘキサネーター

Answer: C

Explanation:

This question aligns with CHFI v11 objectives under Operating System Forensics and Live Data Acquisition .

When investigating a compromised Windows system, collecting volatile data such as running processes and active services is critical, as this information exists only in memory and can be lost if the system is shut down.

CHFI v11 emphasizes the use of native, low-impact system utilities during live forensic response to minimize changes to the system state.

The tasklist command is a built-in Windows utility that displays a list of currently running processes along with associated process IDs (PIDs), memory usage, and service relationships. It is specifically designed for real-time process enumeration and is commonly used in forensic investigations to identify suspicious or malicious processes with minimal system interaction. Because tasklist is native to Windows, it does not introduce external binaries that could alter evidence integrity.

ExifTool is used for metadata analysis, Wireshark captures network traffic rather than process data, and Hexinator is a hex editor used for file-level analysis, not live process enumeration. Therefore, in accordance with CHFI v11 best practices for volatile evidence collection on Windows systems, tasklist is the correct and most forensically sound tool for this scenario.

QUESTION NO: 6

ある組織は、サイバー犯罪捜査における電子証拠の特定、収集、および保全を担当する社内eDiscoveryチームの設立準備を進めています。このチームは、法務部門とIT部門の両方の専門家で構成され、プロセスが効率的であるだけでなく、法的基準に完全に準拠していることを保証します。法務チームは、証拠を収集できる具体的なシナリオ、プロトコル、および法的ガイドラインを定義し、プロセス全体が法的枠組みと要件に合致することを保証する役割を担います。一方、ITチームは、収集プロセスの技術的な側面を管理し、データの改ざんや損失のリスクを回避し、証拠が安全かつフォレンジック的に健全な方法で収集されることを保証します。法務とITの専門家を結集することで、組織はeDiscoveryの技術的側面と法的側面の両方が適切に処理されることを保証できます。eDiscoveryプロセスに法務チームとITチームの両方を関与させることの主な利点は何でしょうか？

A.ITチームは収集した証拠の完全性を保証し、法務チームはそれが法廷で証拠として認められることを保証します。

B.証拠の適切な収集を保証する責任はITチームのみにあり、法務チームは文書化のみに専念します。

C.両チームは証拠の初期分析を担当し、ITチームはハードウェアに、法務チームは事件の検討に重点を置きます。

D.法務チームは証拠収集中の技術的な問題に重点を置き、ITチームは法的ガイダンスを提供する。

Answer: A

Explanation:

Option A is the best answer because it directly matches CHFI v11's treatment of Legal and IT Team Considerations for eDiscovery , the EDRM Cycle , eDiscovery

collections/methodologies , and the need to manage evidence in a way that is both technically sound and legally defensible .
The IT team plays the primary role in ensuring that electronically stored information is identified, preserved, and collected without altering or damaging the evidence. That supports integrity, authenticity, and forensic soundness . The legal team, by contrast, ensures that collection scope, process, privacy considerations, and production decisions comply with the applicable rules so the evidence remains admissible and usable in court . CHFI stresses both the legal and technical dimensions of digital evidence handling, especially in eDiscovery contexts.
Option B is too narrow and misstates the legal team's role. C focuses on analysis rather than the stated primary benefit. D reverses the responsibilities. Therefore, the core advantage of involving both teams is that IT preserves evidentiary integrity while legal protects admissibility and compliance .

QUESTION NO: 7
システム管理者であるアンドリューは、サーバーのUEFIブートプロセスを調べています。その過程で、アンドリューは、システムがブートローダーの整合性を検証し、設定を確認してからオペレーティングシステムのロードに進むことに気づきます。システムは暗号化チェックを実行し、信頼できるソフトウェアのみがロードされるようにします。アンドリューは、このフェーズによってシステムがポリシーに準拠した安全な状態で起動することも確認します。アンドリューが現在実行しているUEFIブートプロセスのフェーズを特定してください。
A. ブートデバイス選択フェーズ
B. EFI初期化前フェーズ
C. ドライバ実行環境フェーズ
D. セキュリティフェーズ
Answer: D
Explanation:
Option D. Security phase is the best answer because the scenario describes cryptographic verification , checking the bootloader integrity , and enforcing policies so that only trusted software is loaded. CHFI v11 includes the booting process and specifically covers the Windows boot process: BIOS-MBR method and UEFI-GPT , which means exam candidates are expected to understand the major phases and security controls associated with modern system startup.
In UEFI-based systems, the phase concerned with validating trust and enforcing secure boot behavior is the security phase . That phase is responsible for ensuring that firmware policy is applied before control is handed to later boot components. This aligns precisely with the description in the question, where the system is not merely selecting a boot device or initializing drivers, but actively verifying trust and compliance.
The other answers are less suitable. Boot device selection focuses on choosing the device to boot from. Pre- EFI initialization prepares early hardware and platform state. Driver execution environment deals more with loading drivers and services in the UEFI environment. Because the emphasis is on trusted boot and cryptographic validation , the correct answer is the security phase .

QUESTION NO: 8
企業で、ソフトウェアエンジニアのボブは、プロジェクトの機密情報を暗号化したメールを、プロジェクトマネージャーのアリスに緊急に送信する必要がありました。ボブは会社のメールクライアントを使って慎重にメールを作成し、送信ボタンを押しました。しかし、会社のメールサーバーが断続的に接続に問題を抱えていることに気づいていませんでした。
ボブは緊急メールを送信している最中に、社内メールサーバーとの接続問題により遅延が発生しました。この遅延は、メール通信プロセスのどの段階で発生すると考えられますか？
A. 電子メールメッセージを復号化するとき
B. メールの作成中
C. MTAサーバー間の転送中
D. アリスのメールドメインを検索中
Answer: C
Explanation:
This question aligns with CHFI v11 objectives under Network and Web Attacks and Email Forensics , specifically focusing on understanding how email communication works.
According to CHFI v11, the email delivery process involves multiple stages, including message composition by the Mail User Agent (MUA), message submission to the outgoing Mail Transfer Agent (MTA), inter-server transfer between MTAs, and final delivery to the recipient's mailbox via the Mail Delivery Agent (MDA).
Once Bob clicks "send," the email is handed off from his email client (MUA) to the corporate email server's MTA. If the corporate server is experiencing intermittent connectivity issues, delays most commonly occur during the transfer between MTAs , where the sending MTA attempts to establish an SMTP connection with the recipient's mail server or relay servers. Network instability, DNS delays, or SMTP retry mechanisms can all cause queued messages and delayed delivery at this stage.
Encryption and decryption processes occur locally or at defined endpoints and do not typically introduce network-related delays. Composition is performed entirely on the sender's system, and domain lookups usually happen quickly before transmission. Therefore, in accordance with CHFI v11 email communication fundamentals, the delay is most likely during the transfer between MTA servers.

QUESTION NO: 9
デジタルフォレンジック調査員が、サイバー犯罪事件の容疑者から回収されたモバイルデバイスを調査しています。
デバイスは、昇格された権限とシステム リソースへの無制限のアクセスを許可するカスタム オペレーティング システム構成を実行しているようです。
この構成を実現するために最も適した方法は何ですか?
A. AndroidデバイスにカスタムROMをインストールする
B. iOSデバイスのファームウェアの脆弱性を悪用する
C. Androidデバイスのルート化
D. iOSデバイスの脱獄
Answer: C
Explanation:
According to the CHFI v11 Mobile and IoT Forensics domain, rooting an Android device is

the most common and direct method used to obtain elevated (superuser) privileges and unrestricted access to system resources. Rooting allows a user to bypass Android's built-in security restrictions and gain full control over the operating system, including access to protected directories, system binaries, kernel parameters, and hardware interfaces.
CHFI v11 explains that once an Android device is rooted, the user can modify system files, install unauthorized applications, disable security controls, manipulate logs, and conceal malicious activity-making rooting a frequent technique in cybercrime and anti-forensics scenarios. From a forensic perspective, rooting significantly impacts evidence integrity and is often identified through artifacts such as the presence of su binaries, modified boot images, or root management applications.
While installing a custom ROM does modify the operating system, it does not inherently guarantee unrestricted system access unless the device is rooted. Jailbreaking applies specifically to iOS devices, not Android. Exploiting an iOS firmware vulnerability may lead to jailbreaking, but the scenario does not indicate an iOS environment.
CHFI v11 emphasizes that identifying whether a device has been rooted is critical during mobile investigations, as it affects data acquisition methods, trustworthiness of artifacts, and anti-forensic risk assessment .
Therefore, the most likely method used to achieve elevated privileges and unrestricted system access in this scenario is rooting the Android device , making Option C the correct answer.

QUESTION NO: 10
ノースカロライナ州ローリーにあるニュースポータルで営業時間外に発生したインシデントにおいて、アナリストは短時間のうちに同じIPアドレスからログインページへのアクセスが多数発生していることを確認した。数分後、以前のパターンとは異なる単一のエントリが検出された。ブルートフォース攻撃の継続と、認証後の管理エリアへのアクセスを区別するために、ログ内のどの要素が後者を最も強く示唆しているだろうか？
A.非常に短い時間枠内でのログイン試行
B. "HTTP 302ステータスはURLリダイレクトを示します"
C. "同じIPアドレスから"
D. "URLが/wordpress/wp-admin/に変更されました"
Answer: D
Explanation:
The correct answer is D because the clearest sign of post-auth navigation is the change in requested resource from the login endpoint to the WordPress admin area. A burst of repeated login attempts from the same IP suggests brute-force activity, but it does not prove successful entry. A 302 redirect can happen in several contexts and is less definitive by itself. The strongest indicator that the attacker moved beyond guessing credentials and into an authenticated area is a subsequent request for /wordpress/wp-admin/, which is the administrative interface path. CHFI v11 includes investigation of brute-force attacks and web application forensic analysis through web server logs, so candidates are expected to distinguish unsuccessful login pressure from navigation that occurs after access is obtained. In forensic interpretation, the requested URL often provides stronger context than timing or source IP alone. Since the question asks what most strongly indicates post-auth activity rather than continued brute-force behavior, the change to the admin URL is the best answer.

QUESTION NO: 11
法医学専門家のソフィアは、マルウェアの痕跡がないかシステムを分析している。彼女は、マルウェアがWindowsのサービスや実行中のプロセスを改変し、検出されずにバックグラウンドで動作するようにしていることに気づく。彼女は、システムの起動時に自動的に開始されるサービスを特定する必要がある。
ソフィアは、自動起動するように設定されているWindowsサービスを調べるために、どのツールを使用すべきでしょうか？
A. イベントビューアー
B.タスクマネージャー
C. 自動実行
D. プロセスエクスプローラ
Answer: C
Explanation:
Option C. Autoruns is the best answer because the question is specifically about identifying services and other components configured to start automatically during boot . In CHFI-style Windows forensics and malware persistence analysis, investigators focus on auto-start mechanisms , including services, registry run keys, startup folders, drivers, scheduled tasks, and related launch points. Autoruns is designed to enumerate these persistence locations in a comprehensive way, making it the most appropriate tool among the options.
Event Viewer is useful for examining logs and system events, but it is not the primary tool for enumerating all boot-start and auto-start entries. Task Manager can show currently running processes and some startup items, but it is less complete than Autoruns for deep persistence analysis. Process Explorer is excellent for analyzing active processes and parent-child relationships, yet it is not focused on full startup enumeration.
Because Sophia wants to identify which Windows services are configured to start automatically , the most effective forensic tool is Autoruns , which directly supports malware persistence investigation and startup analysis.

QUESTION NO: 12
経験豊富なフォレンジック調査員であるレベッカは、一流テクノロジー企業で発生した可能性のあるデータ漏洩の調査に呼ばれた。漏洩した情報には、非常に価値の高い機密設計図ファイルが含まれているようだ。同社のネットワークは侵害されており、漏洩は継続中であると思われる。レベッカのチームの若手メンバーは、さらなる漏洩を防ぐためにサーバーを停止することを提案する。しかし、レベッカはそれがデジタルフォレンジックの重要な原則に反することを知っている。その原則とは何だろうか？
A. デール保存の原則
B.連邦証拠規則
C. 最良証拠ルール
D.対象メディアを消毒する原則
Answer: A
Explanation:
Option A is the best answer. The wording appears to contain a typo, and in CHFI context this clearly points to the principle of data preservation . CHFI v11 emphasizes live acquisition , order of volatility , evidence preservation , and the need to collect volatile information before

actions are taken that may destroy it. In an active breach on a running server, abruptly shutting the system down may destroy critical volatile evidence such as RAM contents, active network connections, running processes, logged-in sessions, encryption artifacts, and other transient indicators that may explain how the leak is occurring.
This is why CHFI distinguishes between live acquisition and dead acquisition and teaches investigators to determine the best acquisition method before taking action. Federal Rules of Evidence and the Best Evidence Rule are legal concepts, but they do not directly describe the operational mistake of powering off a live compromised server. Sanitizing target media applies to preparing destination media for acquisition, not preserving a live source system. Therefore, the key violated principle is the preservation of data, especially volatile evidence on a live system.

QUESTION NO: 13
あなたはサイバーセキュリティ企業のデジタルフォレンジック専門家として、データ漏洩事件の捜査に深く関わっています。
あなたは、情報漏洩に関連するマルウェアが潜んでいる可能性があると思われる顧客のコンピュータのWindowsレジストリを精査する任務を負っています。潜在的なマルウェアのエントリを見つけるために、レジストリのどの部分を重点的に調べるべきでしょうか？
A. HKEY_CLASSES_ROOT
B. HKEY_LOCAL_MACHINE
C. HKEY_CURRENT_USER
D. HKEY_USERS
Answer: B
Explanation:
Option B. HKEY_LOCAL_MACHINE is the best answer because CHFI v11 specifically emphasizes Windows memory and registry analysis as part of evidence examination and operating system forensics.
The blueprint also highlights registry-based malware persistence mechanisms and system behavior analysis , including monitoring registry artifacts, startup programs, processes, services, and event logs to identify suspicious or malicious activity.
In practical forensic work, HKEY_LOCAL_MACHINE (HKLM) is one of the most important hives because it contains system-wide configuration settings that affect the whole computer, not just one user.
Malware commonly establishes persistence there through machine-level startup locations, service entries, driver references, and other autostart mechanisms. That makes HKLM a primary place to examine when trying to identify malware that survives reboots or affects all users on the system. This fits CHFI's focus on analyzing Windows artifacts and identifying persistence mechanisms.
The other hives can also contain useful evidence, especially user-specific activity, but for main focus in spotting broad malware persistence, HKLM is the strongest CHFI-aligned answer.

QUESTION NO: 14
調査員は、疑わしいメディアからデータを取得した後、画像ファイルの互換性に関する問題に遭遇する可能性があります。

このセクションでは、E01形式のLinux用変換、起動可能なVMの作成、Linux上でのWindowsファイルシステムの扱い、APFSファイルシステムの扱いといったシナリオを概説します。各シナリオにおける解決策を解説し、最後にWindows、Linux、Macでのイメージ表示方法について解説します。捜査官は、検査用のイメージファイルを準備する際にどのような課題に直面する可能性があるでしょうか？

A. E01形式をWindows用に変換しています

B. Windowsワークステーションでの APFSファイルシステムの取り扱い

C. 取得した証拠から起動可能なVMを作成する

D. Macワークステーションで画像ファイルを表示する

Answer: B

Explanation:

According to the CHFI v11 objectives under Image/Evidence Examination and Operating System Forensics , one of the most significant challenges investigators face when preparing image files for examination is file system compatibility across operating systems . APFS (Apple File System) is the default file system used by modern macOS devices, and it is not natively supported on Windows workstations . This creates a clear challenge when investigators attempt to analyze APFS-based forensic images on Windows platforms.

CHFI v11 highlights that special tools, drivers, or forensic platforms are required to mount, parse, and analyze APFS volumes on non-macOS systems. Without proper support, investigators may be unable to access directories, metadata, snapshots, or encrypted APFS containers, potentially delaying investigations or risking incomplete analysis.

The other options describe scenarios that are typically manageable with standard forensic workflows.

Converting E01 images (Option A) is well-supported using tools like ewfmount. Creating bootable VMs (Option C) is an advanced but solvable task using virtualization tools. Viewing images on macOS (Option D) is generally straightforward with native or commercial forensic software.

The CHFI Exam Blueprint v4 explicitly mentions APFS file system analysis challenges and cross-platform compatibility issues as key considerations during forensic image preparation. Therefore, handling APFS file systems on a Windows workstation represents a genuine and commonly encountered challenge, making Option B the correct and exam-aligned answer

QUESTION NO: 15

法医学捜査官は、企業の内部ネットワークを標的とした高度なサイバー攻撃に関連する大量のデジタル証拠を分析するよう命じられた。この攻撃は企業全体の複数のシステムに影響を与え、複数の脆弱性を悪用したものであった。事件の複雑さと規模を考慮し、捜査官は捜査プロセスを効率化するためにコンピュータ化されたフォレンジックツールを導入することを決定した。

これらのツールは、複数の疑わしいドライブのビット単位のコピーを作成するために使用され、元の証拠の完全性を確保し、元のデータを変更することなくさらなる分析を可能にします。

フォレンジックイメージの作成に加え、調査官は高度なハッシュ分析技術を用いて、ファイルハッシュを既知の脅威データベースと比較することで、潜在的に悪意のあるファイルを迅速に特定します。さらに、攻撃中に生成される大量のイベントログを管理するため、調査官はフォレンジックツールを使用してタイムスタンプを分析し、詳細な活動タイムラインを作

成します。このタイムラインには、最初の侵入、ネットワーク内での横方向の移動、機密データの流出など、攻撃における重要なイベントが示されます。
これらの作業を効率化することで、捜査官は攻撃の全容を把握するために必要な重要な分析に集中できるようになります。ここで説明されているのは、どのフォレンジックプロセスでしょうか？
A. データストレージ管理を統合したフォレンジックオーケストレーション。
B.複数のタスクを並行して管理するフォレンジックオーケストレーション。
C.手動分析を支援するフォレンジック自動化ツール。
D.反復作業を効率的に実行するフォレンジック自動化。
Answer: D
Explanation:
Option D is the best answer because the scenario describes using tools to automate repetitive, high-volume forensic tasks such as bit-by-bit imaging , hash comparison , and timeline generation so the investigator can concentrate on interpretation and deeper analysis. CHFI v11 explicitly includes Forensics Automation and Orchestration as a core topic.
The key clue is that the tools are being used to streamline repeated technical tasks efficiently across a large dataset. That is the hallmark of forensic automation . Automation reduces manual workload in predictable processes like hashing, imaging, and log parsing.
Orchestration , by contrast, usually refers to coordinating multiple tools, workflows, or systems together across a broader process. While there may be some orchestration elements in real environments, the emphasis in this question is clearly on efficient execution of repetitive tasks.
Because the investigator is using computerized tools to handle recurring evidence-processing steps at scale, the most accurate classification is forensic automation performing repetitive tasks efficiently . That aligns directly with the CHFI objective covering automation and orchestration in digital forensics.

QUESTION NO: 16
ニューヨークの出版社で知的財産権侵害の調査が行われた際、取締役は調査員が会社のノートパソコンを検査することに同意した。機器の取り扱いを開始する前に、別の担当者が立ち会い、承認が適切に行われたことを確認した。この担当者が立ち会った目的を最もよく表しているのは、どの責任か？
A. 証人の署名が1つ以上必要かどうかを決定します
B. 当事者が自発的に契約に署名したことを確認します
C.必要に応じて証言を行うか、法廷に出廷する
D.捜査官の役割に基づいて押収権限を確保する
Answer: B
Explanation:
The correct answer is B because, in a consent-based forensic examination, the role of the witness is to confirm that the consent was knowingly and voluntarily given by the person authorizing the search. Under the CHFI v11 blueprint, investigators are expected to understand seeking consent, obtaining witness signatures, search and seizure procedures, and best practices for handling digital evidence. A witness is not primarily present to decide legal authority, and the witness does not create seizure powers for the examiner. Instead, the

witness helps support the validity of the consent process by confirming that the agreement was actually signed and that it was not coerced or improperly obtained. This can become especially important later if the defense challenges whether the examination was authorized. Option A refers to deciding procedural requirements, which is not the witness's core function. Option C may happen in some cases, but it is not the main reason the witness is present at the time of signing. CHFI emphasizes defensibility and proper evidence-handling foundations, so validating voluntary consent is the best answer.

QUESTION NO: 17
フォレンジック調査員のヘイゼルは、最近いくつかのファイルが削除されたWindowsコンピューターを扱っています。彼女の任務は、これらの削除されたファイルの内容を復元できるかどうかを確認することです。
最初の分析を実行した後、ヘイゼルはファイルがファイル
エクスプローラーに表示されなくなったことを知りましたが、データが本当に消えたかどうかはわかりません。
削除されたファイルがまだ回復可能であると考えられる理由は何でしょうか?
A. ファイルへのポインターは残りますが、コンテンツは削除されます。
B. ファイルはディスクから削除されると回復できません。
C. ファイルの内容は削除され、回復できません。
D. ファイルへのポインターは削除されますが、コンテンツはディスク上に残ります。
Answer: D
Explanation:
This question aligns with CHFI v11 objectives under Data Acquisition and Duplication and File Deletion and Recovery Concepts . In Windows file systems such as NTFS, deleting a file does not immediately erase its data from the disk. Instead, the operating system removes the file system pointer (metadata entry) that references the file's location and marks the occupied disk clusters as available for reuse.
CHFI v11 explains that until these disk sectors are overwritten by new data, the actual file content remains intact on the storage media . This is why deleted files often remain recoverable using forensic tools such as file carving utilities and disk analysis tools. Investigators can scan unallocated space to reconstruct files based on known file headers and footers, even when directory entries no longer exist.
Option A is incorrect because file content is not immediately deleted. Options B and C contradict fundamental forensic principles taught in CHFI v11 regarding logical deletion. Understanding this behavior is critical for forensic investigators, as it enables recovery of evidence that suspects may believe is permanently removed.
Therefore, the correct explanation is that the file pointer is deleted, but the content still remains on the disk, making recovery possible.

QUESTION NO: 18
金融機関におけるデータ侵害に関するサイバーセキュリティ調査において、調査員は侵害の根本原因を特定し、インシデントに至るまでの一連の出来事を時系列で記録する任務を負います。調査員は、フォレンジックプロセスのどのステップが、悪用された脆弱性、攻撃時刻、攻撃者が行った具体的な行動など、一連の活動を明らかにするのに役立つかを判断する必要があります。この目標を達成するために

最も効果的な法医学技術は次のどれですか？
A. データの重複
B. 犯罪現場の撮影
C. データ分析
D. データ取得
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 NO: 19
シカゴの金融サービス会社で行われた内部監査において、フォレンジックアナリストは、不審な管理者ログインとその後の複数のアカウント管理イベントを調査した。ログには、短時間のうちにグループの作成、メンバーの追加、およびメンバーの削除が記録されていた。一連のアクティビティを再構築し、その後の権限昇格を可能にしたアクションを特定するために、アナリストはどのイベントを最初のステップとして優先すべきか？
A. 4730 セキュリティが有効になっているグローバルグループが削除されました
B. 4728 セキュリティが有効なグローバルグループにメンバーが追加されました
C. 4727 セキュリティが有効なグローバルグループが作成されました
D. 4729
セキュリティが有効になっているグローバルグループからメンバーが削除されました
Answer: C
Explanation:
The correct answer is C because group creation is the earliest enabling action in the sequence described.

Microsoft's audit references identify Event ID 4727 as the creation of a security-enabled global group, while
4728 records a member being added, 4729 records a member being removed, and 4730 records deletion of the group. If analysts are reconstructing the privilege-escalation path, the creation of the group is the foundational event that makes later membership changes possible. In other words, the add and remove operations depend on the group already existing. CHFI v11 covers account-management events, evaluation of event logs, and using logs as evidence, so candidates are expected to reason not only from event meaning but also from event order. In a timeline analysis, identifying the first action that established the structure later used for privilege expansion is essential. That makes Event ID 4727 the correct answer. It represents the initial administrative action that enabled the subsequent changes captured in the following events.

QUESTION NO: 20
テキサス州オースティンで発生した企業サイバースパイ事件において、フォレンジック調査官は、データ流出時に同社のストレージシステムがどのようにアクセスされたかを分析しました。その結果、攻撃者が複数の部門からSMBプロトコル経由でアクセス可能な共有フォルダをマッピングしていた一方で、重要なデータベースは別の高速ファイバーチャネルストレージファブリック上に残されていたことが判明しました。この共有フォルダシステムは、どのストレージモデルを表しているでしょうか？
A. ストレージエリアネットワーク SAN
B.RAIDストレージシステム
C. JBOD Just a Bunch of Disks
D. ネットワーク接続ストレージ(NAS)
Answer: D
Explanation:
The correct answer is D because a shared folder accessed over SMB from multiple departments is the typical behavior of Network-Attached Storage. NAS provides file-level access over the network using protocols such as SMB or NFS, making it ideal for shared departmental folders and common user access. That matches the scenario exactly. By contrast, the question separately mentions a high-speed Fibre Channel storage fabric for databases, which is characteristic of a Storage Area Network rather than the shared folder system being asked about. RAID is a disk redundancy or performance arrangement, not a network storage access model, and JBOD simply refers to a grouping of disks without describing a networked file-sharing architecture. CHFI v11 includes NAS and SAN storage concepts under digital evidence fundamentals, so candidates are expected to distinguish file-level network storage from block-level storage fabrics. In exam terms, when the clue is SMB-accessible shared folders used by multiple departments, the correct storage model is NAS. The Fibre Channel reference is included to contrast it with SAN and test whether the candidate can separate the two architectures correctly.

QUESTION NO: 21
テキサス州ダラスのデータセンターを標的としたサービス拒否攻撃の調査の結果、ネットワークアナリストは、攻撃者が特定のTCPフラグの組み合わせを持つパケットを継続的に送信し、接続が完了する前にサーバーのリソースを枯渇させる、非常に多くの半開TCPセッショ

ンを確認した。
パケットキャプチャの結果、SYNフラグとFINフラグの両方が同時に設定されたパケットが時折使用されていることも明らかになった。
観測された挙動を最もよく表す攻撃パターンはどれですか？
A. TCP SYNフラッド攻撃
B. TCP RSTフラッド攻撃
C. TCP ACKフラッド攻撃
D. TCP SYN-FIN フラッド攻撃
Answer: D
Explanation:
The most accurate answer is D because the question explicitly mentions two distinct indicators together: half- open TCP sessions typical of SYN flooding and packets that have both SYN and FIN flags set. A normal TCP packet would not use SYN and FIN together in a legitimate connection setup, so that flag combination is highly suspicious and maps directly to a SYN-FIN flood pattern. A pure SYN flood would explain the half- open sessions, but it would not fully account for the stated observation that packet captures show SYN and FIN set simultaneously. CHFI v11 expects candidates to analyze network traffic for denial-of-service behaviors and to recognize packet-level evidence from abnormal TCP flag combinations. In forensic review, the exact flags matter because they help distinguish common handshake abuse from crafted packets designed to exhaust resources, evade simplistic filtering, or confuse defensive logic. Since the scenario includes the uncommon SYN-FIN combination as a defining artifact, the best answer is not the broader SYN flood label but the more precise TCP SYN-FIN flood attack. That choice best reflects the traffic evidence described in the packet capture.

QUESTION NO: 22
サイバーセキュリティ専門家のリアムは、機密性の高い企業データが保存されていた複数のハードドライブのデータを消去する任務を任された。ドライブ上にデータが一切残らないようにするため、リアムは特定のメディア消去基準に従う必要がある。彼は、最初の処理でゼロを書き込み、次の処理でランダムなバイトを書き込む消去方法を選択しなければならない。これにより、最小限の検証で最高レベルのデータ消去を実現できる。
リアムはこの要件を満たすために、以下のメディアサニタイズ基準のうちどれを使用すべきでしょうか？
A. (アメリカ) NAVSO P-5239-26 (MFM) (3回合格)
B. (アメリカ) NAVSO P-5239-26 (RLL) (3回合格)
C. (ドイツ語) VSITR (7 パス)
D. (ロシア語) GOST R 50739-95 (2回合格)
Answer: D
Explanation:
Option D. GOST R 50739-95 (2 passes) is the best answer because the question specifically describes a sanitization method that writes zeros on the first pass and random bytes on the second pass . Among the listed choices, that pattern matches the 2-pass GOST method . CHFI v11 includes sanitize the target media under rules and procedures related to evidence handling, showing that candidates are expected to understand how media sanitization

supports secure handling of sensitive storage devices and prevents residual data exposure. This question is focused on the operational detail of a wiping standard. The other options involve more passes and therefore do not match the exact requirement stated. NAVSO P-5239-26 (MFM) and NAVSO P-5239-26 (RLL) are 3-pass methods, while VSITR is a 7-pass method. Since the scenario emphasizes first zeros, then random bytes , and wants the correct standard associated with that sequence, GOST R 50739-95 is the only option that fits.
From a CHFI perspective, sanitization matters because investigators and security teams must know how to prepare or dispose of media securely while protecting evidence integrity and sensitive data.

QUESTION NO: 23
デジタル調査の一環として、フォレンジック専門家は違法コンテンツをホスティングしている疑いのあるサーバーを分析する必要があります。サーバーには複数のボリュームとパーティションがあります。分析を進めるには、調査員はサーバー上のユーザーファイル、ドキュメント、システムメタデータが通常保存されている場所から証拠を収集する必要があります。
この目的のために調査員が主に重点を置くべき保管場所はどれですか?
A. 揮発性メモリには一時データが保存されます。
B. 外部バックアップ
デバイスにはデータが保存されますが、必ずしも関連情報が含まれているとは限りません。
C. ネットワーク ストレージ
システムでは、追加のアクセス制御が必要になる場合があります。
D. 不揮発性ストレージは、電源を切ってもデータを保持します。
Answer: D
Explanation:
This question aligns with CHFI v11 objectives under Computer Forensics Fundamentals and Digital Evidence and Storage Media . In forensic investigations involving servers suspected of hosting illicit content, investigators must focus on storage locations that reliably preserve data over time. CHFI v11 emphasizes that non-volatile storage -such as hard disk drives (HDDs), solid-state drives (SSDs), RAID arrays, and other persistent storage media-is the primary repository for user files, documents, system files, logs, and file system metadata. Non-volatile storage retains data even when the system is powered off, making it essential for post-incident forensic analysis. This includes directory structures, timestamps, access control lists, deleted file remnants, and application data, all of which are critical for reconstructing user activity and determining the presence and origin of illicit content.
Volatile memory (RAM) contains temporary data such as running processes and network connections, which is useful during live analysis but does not store long-term user files. External backups and network storage may contain copies of data but are secondary sources and may not reflect the system's current state.
Therefore, consistent with CHFI v11 forensic principles, the investigator should primarily focus on non- volatile storage , as it is the most reliable and comprehensive source of persistent digital evidence.

QUESTION NO: 24

テネシー州メンフィスの物流会社で認証情報が盗まれた事件を受け、捜査官はパケットキャプチャとイベントログを分析し、攻撃者がVPNゲートウェイから複数の中間ホストを経由して内部データベースにどのようにアクセスしたかを把握しようとしています。彼らの当面の目標は、攻撃者がセグメント間で使用したネットワークホップのシーケンスを再構築することです。ネットワークフォレンジックのどの結果がこの目標に最も適していますか？

A. 侵入経路

B. セキュリティインシデントの発生源

C. 攻撃者が使用した侵入技術

D.痕跡と証拠

Answer: A

Explanation:

The best answer is A because the question is focused on reconstructing the route the attacker followed through the environment. The wording emphasizes movement from the VPN gateway to an internal database through intermediate hosts, which is a classic path-reconstruction problem. In CHFI v11, network forensics includes examining packet captures, correlating logs, tracing attack progression, and understanding how malicious activity moves across systems. While identifying the source of the incident can also matter, this scenario is not primarily asking where the attack began. It asks for the sequence of hops used after entry.

Likewise, intrusion techniques concern methods such as credential abuse, lateral movement protocols, or exploitation mechanisms, but those are secondary to the immediate objective stated in the question. Traces and evidence is too general and does not describe a specific analytical outcome. In exam reasoning, when the investigator's task is to map the movement chain across devices and segments, the most precise result is the path of intrusion. That outcome helps analysts understand lateral movement, affected assets, and the order in which the attacker progressed through the network.

QUESTION NO: 25

経験豊富なCHFI(認定情報セキュリティ専門家)であるグレッグは、大手ソフトウェア会社における知的財産窃盗事件の調査を依頼された。調査を進める中で、彼は同社のメールサーバーに重要な証拠が隠されている可能性があることを発見した。しかし、そのサーバーは別の会社と共有されており、アクセスするとその会社のプライバシー権を侵害する恐れがある。証拠の捜索と押収に関する規則や規制を遵守するために、グレッグはこの状況でどのような初期対応を取るべきだろうか？

A.法律専門家および会社の経営陣と相談し、最善の解決策を探る。

B. メールサーバーは避け、他の潜在的な証拠源に焦点を当てる

C. 潜在的なプライバシー侵害を無視してサーバーを押収する

D.直ちにサーバーを捜索・押収するための令状を取得する

Answer: A

Explanation:

Option A is the best answer because CHFI v11 explicitly includes Rules of Evidence , Best Practices for Handling Digital Evidence , Seeking Consent , Obtaining a Warrant for Search and Seizure , Legal Issues, Privacy Issues and Legal Compliance , and the Role of Local/International Agencies during Cybercrime Investigation . When a server is shared with

another company , privacy and ownership concerns become especially important, and the initial step should be to consult the appropriate legal and organizational stakeholders before taking action.
Immediately seizing the server or ignoring privacy implications could violate legal boundaries and compromise admissibility. Avoiding the server entirely may also be inappropriate if it contains critical evidence. Likewise, jumping straight to a warrant may not be the most suitable first move until counsel and management clarify ownership, scope, privacy exposure, and the least intrusive legally defensible path.
Therefore, the strongest CHFI-aligned initial approach is to consult legal experts and company management to determine the correct lawful path forward before attempting access or seizure. That protects privacy rights, preserves admissibility, and aligns the investigation with proper search-and-seizure procedure.

QUESTION NO: 26
eDiscoveryツールを導入した後、フォレンジック調査員は、すべてのユーザーアクションとシステムへの変更が正確に記録されていることを確認する責任を負います。この追跡は、調査中に行われたすべてのアクションが完全に透明性と説明責任を果たせるようにするために不可欠です。これにより、調査員はeDiscoveryプロセスにおけるすべての活動の信頼できる証拠を確保できます。このシナリオにおいて、調査員はどのような指標に最も重点を置くでしょうか？
A. 調査員は監査証跡を追跡し、すべての変更の包括的な記録を確保します。
B.
調査員は、コンプライアンスを確保するために証拠に課せられた法的保留を追跡することに重点を置いています。
C.
調査員は、調査プロセス中に確認されたファイルの数を追跡して、作業負荷を評価します。
D.
調査員は、データの整合性を確保するために、収集フェーズ中にデータ抽出の精度を測定します。
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 NO: 27
企業において、セキュリティオペレーションセンター(SOC)は組織のデジタル資産の監視と保護を担っています。組織が一連の不審なネットワークアクティビティを経験している状況を考えてみましょう。SOCチームは、これらの潜在的な脅威を効果的に検知し、軽減するために適切なテクノロジーを特定する必要があります。SOCチームは、セキュリティイベントをリアルタイムで監視および分析するために、主にどのテクノロジーを活用すべきでしょうか？
A. パスワード管理ソフトウェア
B. セキュリティ情報イベント管理(SIEM)システム
C. 脆弱性評価ツール
D. データ損失防止 (DLP) ソリューション
Answer: B
Explanation:
According to the CHFI v11 objectives related to Network Forensics, Incident Detection, and SOC Operations , the primary technology used by a Security Operations Center (SOC) to monitor, correlate, and analyze security events in real time is a Security Information and Event Management (SIEM) system .
A SIEM system centrally collects logs and events from multiple sources such as firewalls, IDS/IPS, servers, endpoints, applications, authentication systems, and network devices. It then performs real-time correlation, normalization, alerting, and analysis to identify suspicious patterns such as brute-force attacks, lateral movement, malware activity, data exfiltration attempts, and insider threats. CHFI v11 emphasizes SIEM solutions as a core component for incident detection, investigation, and evidence correlation within SOC environments.
The other options do not meet this requirement. Password Management Software focuses on credential storage and rotation, not threat monitoring. Vulnerability Assessment Tools are used for periodic scanning to identify weaknesses, not real-time event analysis. Data Loss Prevention (DLP) solutions are designed to prevent unauthorized data leakage but do not provide comprehensive, centralized security event correlation across the enterprise.
CHFI v11 explicitly highlights the use of SIEM solutions for centralized logging, real-time monitoring, and forensic investigation support , making them essential for SOC teams dealing with active threats.
Therefore, the correct and CHFI-verified answer is Security Information and Event Management (SIEM) System (Option B) .

QUESTION NO: 28
カリフォルニア州サンノゼにあるソフトウェア会社で発生した内部犯行によるデータ窃盗事件の捜査において、フォレンジック調査官は、分析ツールとの幅広い互換性を確保しつつ、圧縮やメタデータのオーバーヘッドを回避するために、最も適切なデータ取得フォーマット

を選択する必要があります。調査官はどのフォーマットを選択すべきでしょうか？
A.生フォーマット
B. 独自フォーマット
C. AFF形式
D. AFF4形式
Answer: A
Explanation:
The correct answer is A because raw format is the most straightforward acquisition format when the priority is maximum compatibility and minimum format-related overhead. In CHFI v11, candidates are expected to understand acquisition formats and choose the one that best fits the investigation. A raw image is essentially a direct bit-for-bit copy of the data without added container features such as embedded metadata structures or compression layers. That simplicity makes it widely supported across forensic tools and platforms. By contrast, AFF and AFF4 were designed to add features such as metadata support, segmentation, and optional compression, which can be useful in many cases but do introduce additional format overhead. Proprietary formats may also include useful features, yet they can limit interoperability depending on the tool ecosystem.
The scenario specifically asks for a format that avoids compression and metadata overhead while remaining broadly compatible, which points directly to raw format. In CHFI-style reasoning, when a question emphasizes universality, simplicity, and minimal encapsulation, raw is the strongest answer because it preserves the evidence in the most tool-neutral and uncomplicated image representation.

QUESTION NO: 29
サイバーセキュリティ調査中に、Cisco スイッチ、VPN、DNS
サーバーからのログが収集されます。
これらのログには、ネットワーク
アクティビティや潜在的なセキュリティ侵害に関する貴重な情報が含まれています。
デジタルフォレンジックにおいて、ネットワークインシデントを分析する際に、Cisco
スイッチ、VPN、DNS サーバーのログはどのような役割を果たしますか?
A. ネットワーク トラフィック、デバイス接続、セキュリティ
インシデントに関する分析情報を提供します。
B. ウェブサイトの訪問とブラウザの履歴のみを追跡します。
C. デジタルフォレンジックには関係ありません。
D. ローカル ネットワーク内のユーザー アクティビティの詳細を示します。
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.
Together, these logs allow investigators to correlate events across the network, trace attacker movement, identify affected systems, and establish timelines of security incidents.
The other options are incorrect because browser history is host-based evidence, and these logs are highly relevant to forensic investigations.
Therefore, consistent with CHFI v11 network forensics principles, these logs provide insights into network traffic, device connections, and security incidents.

QUESTION NO: 30
あるサイバーセキュリティ企業は最近、インターネット上で蔓延している新たなランサムウェアを発見しました。このランサムウェアは世界中の組織にとって重大な脅威となっています。非常に高度な技術を駆使しており、従来のウイルス対策ソフトを回避する能力を持っています。この脅威に効果的に対処するため、サイバーセキュリティ企業は詳細な分析を行うためにマルウェアサンドボックスを活用することにしました。
上記のような状況において、マルウェアサンドボックスを使用する主な目的は何でしょうか？
A.管理された環境でランサムウェアを実行し、その動作を観察する。
B. ランサムウェアを他のシステムに配布して、さらに分析を行う。
C.ランサムウェア感染を防ぐために、ホストシステム上の機密データを暗号化します。
D.感染したシステムからランサムウェアを完全に削除します。
Answer: A
Explanation:
Option A is the best answer because CHFI v11 explicitly includes "Perform Static and Dynamic Malware Analysis in a Sandboxed Environment," "Malware Analysis: Static and Dynamic," and the
"Prominence of Setting up a Controlled Malware Analysis Lab." These objectives show that the purpose of a sandbox is to let investigators safely run malware and observe what it does without putting production systems at risk.
A ransomware sample that evades traditional antivirus must be studied through controlled execution so analysts can identify file-encryption behavior, persistence mechanisms, dropped files, registry changes, process activity, and network communications. That is exactly what a malware sandbox is built for. It provides containment while allowing the forensic team to gather behavioral indicators and build defensive countermeasures.
Option B is unsafe and contrary to forensic practice. Option C misunderstands the purpose of sandboxing, and D refers to remediation rather than analysis. Therefore, under CHFI's malware-forensics objectives, the primary objective of using a malware sandbox is to execute and observe the ransomware in a controlled environment so its behavior can be understood and documented.

QUESTION NO: 31

大規模企業内で発生したデータ侵害の疑いを受け、調査担当者が膨大なネットワークログの分析を任されました。このタスクには、複数のネットワークデバイスからログを収集・管理するだけでなく、リアルタイムのアラート管理、メタデータ分析、異常なトラフィックパターンの明確な表示を可能にするツールが必要です。調査担当者は、ログを整理し、ネットワークイベントを関連付けて攻撃の全容を把握するための最も効果的なソリューションを特定する必要があります。このタスクに最も適したツールは次のうちどれでしょうか？

A. セキュリティオニオン

B. OSFClone

C. インテラプロ

D. 表

Answer: A

Explanation:

Option A. Security Onion is the best answer because the question requires a solution for collecting and managing logs from multiple devices , supporting real-time alerting , enabling metadata analysis , and helping investigators correlate events across the environment. CHFI v11 explicitly includes centralized logging using SIEM solutions , SIEM solutions , types of event correlation , event correlation approaches , and incident detection and examination with SIEM tools .

Security Onion fits that need because it is built around enterprise-scale monitoring, alerting, and network visibility. It is far more suitable than the other options for incident-centric log aggregation and correlation.

OSFClone is a bootable acquisition utility, not a log-correlation platform. Intella Pro is oriented toward eDiscovery and evidence review rather than network event monitoring. Tableau is commonly associated with write-blocking hardware, not SIEM-style network analysis.

Because the task is to organize logs, examine anomalous traffic patterns, and correlate network events to understand the attack timeline and scope, the most CHFI-aligned choice is Security Onion . It best matches the blueprint's network-forensics and SIEM-focused objectives.

QUESTION NO: 32

ボストンの医療機関における不正アカウント活動の調査中、フォレンジックアナリストは生のイベントログファイルを解析し、不審な活動が発生した日時を特定します。彼らは、イベントレコードに異なるタイムスタンプフィールドが含まれていることに気づきます。1つはソースアプリケーションによってイベントが最初に生成された日時を示し、もう1つはイベントが実際にログに書き込まれた日時を示しています。イベントが生成された時刻を示すEventLogRecordフィールドはどれですか？

A. データオフセット

B. タイムライティング

C. タイムジェネレート

D. UserSidOffset

Answer: C

Explanation:

The correct answer is C because the TimeGenerated field records when the event was

originally created by the source application or service, while TimeWritten reflects when the event was actually written into the log.
This distinction matters in forensic timeline analysis because there can be slight differences between generation and log-write time, especially when buffering, service delays, or collection mechanisms are involved. CHFI v11 includes event log file format, event record structure, and the use of logs as evidence, so candidates are expected to understand what each field represents rather than treating all timestamps as interchangeable. DataOffset and UserSidOffset are structural offsets within the event record and do not represent time at all. In a case involving suspicious account activity, identifying the precise moment the event was generated can help analysts correlate it more accurately with authentication attempts, policy changes, or process execution. Since the question specifically asks for the field that records when the event was generated by the source application, the correct EventLogRecord field is TimeGenerated. (learn.microsoft.com)

QUESTION NO: 33
ワシントン州シアトルで行われたデジタル詐欺捜査の一環として、フォレンジック調査官はWindowsワークステーションを調査し、ファイル削除によるディスクレベルへの影響を調べました。分析の結果、ファイルへの参照は削除されるものの、同じストレージ領域が再利用されるまでは、基となるデータは復元可能であることが判明しました。Windowsシステムにおけるこのファイルシステムの動作を最も適切に表しているのは、次のうちどれでしょうか？
A. 削除されたファイルに割り当てられていたクラスタは、$BitMap
で空き領域としてマークされ、コンピュータはその領域を新しいファイルのために使用します。
B. OS は削除されたファイル名の最初の文字を 16 進バイトコード E5h に置き換えます。
C. OS はマスター ファイル テーブル MFT でファイル
エントリを未割り当てとしてマークしますが、実際のファイルの内容は削除しません。
D.
削除されたファイルは、その領域が他のファイルに割り当てられていない場合に復元できます。
Answer: C
Explanation:
The best answer is C because it captures the core NTFS behavior most directly. When a file is deleted on NTFS, the file's MFT record is marked unused or unallocated, while the underlying file content on disk usually remains in place until those clusters are reused by another file. The Sleuth Kit documentation notes that, on deletion, the MFT entry is marked unused and the relevant bitmaps are updated, but the data itself is not immediately erased. This is why deleted files may remain recoverable for some time. Option A is partially true because cluster allocation is updated in the bitmap, but it describes only part of the mechanism and not the key forensic point that the actual content is still present. Option D describes the consequence of deletion rather than the file-system behavior itself. Option B is associated with older FAT-style deletion concepts, not the NTFS behavior being tested here. Under CHFI v11, understanding how deleted files persist until overwritten is central to file recovery and anti-forensics analysis.

QUESTION NO: 34
サイバーセキュリティアナリストのソフィアは、ある企業内で発生したデータ侵害を調査しています。機密性の高いデータが社内ネットワーク内から改ざんされたことから、この侵害は内部者によるものと疑われています。ソフィアは、この侵害が内部者(社内の人物)によるものか、外部の攻撃者(社外の人物)によるものかを判断する必要があります。
侵害が内部者によって実行されたことを最も示唆する要因は次のどれですか?
A. この攻撃では、高度なソーシャル
エンジニアリング戦術を使用して外部の脆弱性を悪用しました。
B. 攻撃は、ハッカー グループに関連付けられた既知の外部 IP
アドレスから開始されました。
C. 攻撃者は分散型サービス拒否 (DDoS) 攻撃を使用してネットワークを圧倒しました。
D. 攻撃者は会社の内部システムとデータに正当にアクセスできました。
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.
The other options point to external attack indicators. Social engineering typically targets users from outside the network, known external IP addresses suggest external threat actors, and DDoS attacks are characteristic of external disruption rather than internal data manipulation. CHFI v11 highlights that distinguishing insiders from external attackers is critical for attribution, legal action, and remediation. Therefore, legitimate internal access to systems and data is the strongest indicator that the breach was carried out by an insider.

QUESTION NO: 35
ネットワーク管理者のエリアナは、組織のネットワーク上のFTPトラフィックの監視を任されています。彼女は、FTPサーバーを標的としたパスワードクラッキングの試みが進行中である可能性があると疑っています。状況を効果的に監視するには、FTPサーバーへのすべての失敗したログイン試行を追跡する必要があります。ネットワークトラフィックを考慮すると、FTPサーバーへのすべての失敗したログイン試行を特定するために、エリアナは次のWiresharkの表示フィルターのどれを適用すべきでしょうか？
A. ftp.response.code == 532
B. ftp.response.code == 230
C. ftp.response.code == 530
D. ftp.response.code == 521
Answer: C

Explanation:
According to the CHFI v11 Network Forensics and Log Analysis objectives , monitoring authentication failures is a critical technique for detecting brute-force and password cracking attacks against network services such as FTP. FTP servers communicate authentication outcomes using standardized FTP response codes , which can be filtered and analyzed using tools like Wireshark .
The FTP response code 530 explicitly indicates "Not logged in" , which commonly occurs when a user provides invalid credentials (incorrect username or password). During brute-force or password spraying attacks, repeated failed login attempts generate multiple 530 response codes , making this filter highly effective for identifying malicious authentication activity.
In contrast, ftp.response.code == 230 indicates a successful login , which is not relevant when tracking failed attempts. The 532 response code means that an account is required for login, not necessarily a password failure. The 521 response code indicates that the FTP service is unavailable, which reflects server-side issues rather than authentication failures.
CHFI v11 specifically emphasizes correlating network traffic patterns and protocol response codes to identify unauthorized access attempts and credential-based attacks. Filtering for ftp.response.code == 530 allows investigators to isolate failed authentication attempts accurately and build evidence of potential password cracking activity.
Therefore, the correct and CHFI-verified answer is ftp.response.code == 530 (Option C) .