

EC-COUNCIL.312-49v11-JPN.v2026-10-19.q206

試験コード : 312-49v11-JPN
試験名称 : Computer Hacking Forensic Investigator (CHFI-v11) (312-49v11日本語版)
認証ベンダー : EC-COUNCIL
無料問題の数 : 206
バージョン : v2026-10-19
ページの閲覧量 : 102
問題集の閲覧量 : 2090
<https://www.jpnsiken.com/shiken/EC-COUNCIL.312-49v11-JPN.v2026-10-19.q206.html>

質問: 1

スティーブは、自分の銀行から送られてきたと思われるメールを受け取りました。そのメールには、口座の停止を避けるためにリンクをクリックして情報を提供するように指示する内容が記載されていました。メール内のリンクをクリックすると、名前、電話番号、生年月日、クレジットカード番号または暗証番号、CVVコード、SNN、メールアドレスなどの詳細情報を要求するフォームにリダイレクトされました。よく見てみると、そのフォームのURLが自分の銀行のURLと異なっていることに気づきました。上記のシナリオで攻撃者が行った外部攻撃の種類を特定してください。

- A. スパイ活動
- B. カずく
- C. テールゲーティング
- D. フィッシング

正解: D ([コメントを发表する](#))

質問: 2

捜査官は、企業サーバーに保存されている機密データへの不正アクセスを伴う複雑なサイバー犯罪事件を担当することになった。捜査は、厳格なプライバシー法とデジタル証拠に関するガイドラインが適用される法域で行われている一方、容疑者は独自のプライバシー法と証拠法が適用される別の法域に所在している。捜査官は、特殊なデジタルフォレンジックツールを使用して、容疑者のデバイスから証拠を収集・保全する必要がある。しかし、捜査官は、2つの法域におけるデジタル証拠の収集と取り扱いを規定する異なる法的枠組みを理解する上で、大きな課題に直面する。

捜査の一環として、捜査官は鑑識ツールを用いて容疑者のデバイスのフォレンジックイメージを作成し、侵害されたシステムからデータを収集します。法的な要件が異なるため、捜査官は証拠の完全性を維持しながら両管轄区域の法律を遵守する方法が分からず困惑しています。この場合、捜査官は証拠の取り扱いにおいてどのような法的課題に直面する可能性があるでしょうか？

- A. 新しいファイルシステムやデバイスと互換性のない、時代遅れのフォレンジックツールを使用することの課題。
- B. 証拠の取り扱いの均一性を確保するため、関係するすべてのデバイスで同じ鑑識ツールを使用する必要がある。
- C. 証拠を輸送中に保護するために、鑑識ツールに暗号化機能が必要である。

D. 捜査中に使用される鑑識ツールが、関係する両地域の規制に従って検証されていることを確認する必要がある。

正解: [\(正解を表示します\)](#)

In multi-jurisdictional investigations, different regions may require that forensic tools be tested, validated, and accepted according to their own legal standards. Ensuring that the tools used meet the evidentiary requirements of both jurisdictions is essential for maintaining admissibility and compliance.

質問: 3

フォレンジック調査員のレイチェルは、企業で使用されている共有ストレージシステムからファイルを復旧するため、ネットワーク接続ストレージ(NAS)デバイスを調査しています。レイチェルは、異なるユーザー間でファイルがどのようにアクセスされ、共有されているかを把握する必要があります。この環境におけるファイルへのアクセス方法を理解するために、レイチェルは次のどのファイル共有プロトコルを調査すべきでしょうか？

A. SMTP

B. iSCSI

C. RAID

D. SMB/CIFS

正解: **D** ([コメントを発表する](#))

According to the CHFI v11 objectives under Digital Evidence, Operating System Forensics, and Network-Based Evidence, understanding file-sharing protocols is essential when investigating Network-Attached Storage (NAS) systems. NAS devices are designed to provide shared file access to multiple users over a network, and the most commonly used protocol for this purpose--especially in Windows-based and mixed environments--is SMB/CIFS (Server Message Block / Common Internet File System).

SMB/CIFS governs how files, folders, printers, and other resources are accessed and shared across the network. By examining SMB/CIFS activity, a forensic investigator can determine which users accessed specific files, when the access occurred, what operations were performed (read, write, delete), and from which systems the access originated. These details are crucial for reconstructing user activity, identifying unauthorized access, and correlating actions across multiple endpoints connected to the NAS.

質問: 4

SWDGEの「基準と要件」のうち、「機関は押収または検査手順に適した効果的なハードウェアとソフトウェアを使用しなければならない」と規定しているのはどれですか？

A. 基準と要件 1.7

B. 基準と要件 1.5

C. 基準と要件 1.4

D. 基準と要件 1.6

正解: **B** ([コメントを発表する](#))

質問: 5

あなたは大手製薬会社の情報セキュリティアナリストです。監査ログの定期的なレビュー中に、ピーク時間外に宛先ポート22のさまざまなIPアドレスへの大量の送信トラフィックが発生していることに気づきました。いくつかのIPアドレスを調査したところ、その多くが東ヨーロッパにあることがわかりました。このトラフィックの最も可能性の高い原因は何ですか？

- A. 内部システム上の悪意のあるソフトウェアが、東欧の提携先のSFTPサーバーから研究データをダウンロードしています。
- B. 高度な持続的脅威(APT)によってデータが外部に持ち出されています
- C. 組織の主要内部DNSサーバーが侵害され、悪意のある外部エンティティにDNSゾーン転送を実行しています。
- D. 内部システムがWindowsの自動アップデートをダウンロードしています

正解: ([正解を表示します](#))

質問: 6

管轄区域によって、異なる事件に適用される法律は異なります。次のうち、コンピュータに関連する詐欺および関連行為に関する法律はどれですか？

- A. 合衆国法典第18編第1029条
- B. 米国法典第18編第1030条
- C. 合衆国法典第18編第1371条
- D. 18 USC §1361

正解: ([正解を表示します](#))

質問: 7

法医学捜査官のマークは、容疑者のマシンから取得したディスクイメージの調査を任されました。証拠を収集するために、ディスクイメージ内のファイルとディレクトリにアクセスする必要があります。そのため、マークはSleuthKitと連携するPythonベースのツールを使用し、ディスクイメージの内容にアクセスして分析します。マークは、ディスクイメージを調べ、関連するファイルとディレクトリを表示するために、どのPythonベースのツールを使用すべきでしょうか？

- A. py.apipkg
- B. PyTSK
- C. FTKイメージャー
- D. 解剖

正解: ([正解を表示します](#))

PyTSK provides Python bindings for The Sleuth Kit, enabling programmatic access to disk images to browse and analyze files and directories.

質問: 8

調査員のジャネットは、コンピュータハッキングのフォレンジック調査中に、疑わしいWindowsレジストリキーを発見しました。彼女は、このキーの変更が、最近発生した会社のサーバーへのサイ

バー攻撃に関連していると考えています。これを確かめるために、ジャネットはレジストリキーに埋め込まれたタイムスタンプを参照する必要があります。このタイムスタンプの正しい名称は何ですか？

- A. 最終書き込み時刻
- B. ユーザーアクティビティ時間
- C. システム変更時間
- D. 現在のシステム時刻

正解: ([正解を表示します](#))

Windows registry keys store a timestamp known as Last Write Time, indicating the last time the key (or its values) was modified. This is the standard forensic timestamp used to correlate registry changes with incident timelines.

質問: 9

サイバーセキュリティアナリストは、一連のネットワーク異常を調査する任務を負っています。彼らは、グラフベースの分析によるシステム依存関係のマッピングや、ニューラルネットワークベースの異常検知など、様々なイベント相関分析手法を駆使します。ルールベースの相関分析と脆弱性ベースのマッピングを通じて、潜在的な脅威を特定し、効果的な対応策の優先順位付けを行います。

システムコンポーネントをノードとして、その依存関係をエッジとしてグラフを構築するイベント相関アプローチはどれですか。

- A. ルールベースのアプローチ
- B. コードブックベースのアプローチ
- C. ニューラルネットワークベースのアプローチ
- D. グラフベースのアプローチ

正解: ([正解を表示します](#))

This question aligns with CHFI v11 objectives under Procedures and Methodology, specifically event correlation and analysis techniques used to investigate complex incidents. Event correlation is essential for transforming large volumes of logs and alerts into meaningful incident narratives. CHFI v11 describes multiple correlation approaches, each suited to different investigative needs. The graph-based approach models systems, applications, users, and network components as nodes, while relationships such as dependencies, communications, or trust relationships are represented as edges. By constructing such graphs, investigators can visualize how events propagate across interconnected systems, identify attack paths, and determine how a compromise in one component impacts others. This approach is particularly effective in analyzing lateral movement, dependency-based failures, and multi-stage attacks in enterprise environments. Rule-based approaches rely on predefined conditions, codebook-based approaches match patterns against known attack templates, and neural network-based approaches focus on anomaly detection using machine learning. While these are valuable, only the graph-based approach explicitly represents system dependencies and relationships in a node-edge structure.

Therefore, consistent with CHFI v11 event correlation methodologies, the correct answer is Graph-Based Approach.

質問: 10

捜査官はTorブラウザの活動を調査するためにフォレンジック分析を実施します。メモリダンプを精査してメールの痕跡を抽出し、Torブラウザが開いている状態と閉じている状態の両方で、ストレージデバイスからメールの添付ファイルを分析します。さらに、Torブラウザをアンインストールした後のフォレンジックオプションを検討し、残存する証拠を明らかにします。

Torブラウザが関係するシナリオにおけるフォレンジック分析の主な目的は何ですか？

- A. Torブラウザが閉じているときにのみ電子メールの添付ファイルを分析する
- B. Torブラウザでさまざまな状態の電子メールアーティファクトと添付ファイルを探索する
- C. Torブラウザが開いているときにのみ電子メールアーティファクトを検査する
- D. Torブラウザのアンインストール後に分析を実行する

正解: ([正解を表示します](#))

This question aligns directly with CHFI v11 objectives under Dark Web Forensics and Tor Browser Forensics. The Tor Browser is specifically designed to minimize persistent artifacts and anonymize user activity, which makes forensic investigations particularly challenging. CHFI v11 emphasizes that the primary objective in Tor Browser-related investigations is to identify and extract residual artifacts across multiple operational states of the browser.

Investigators must analyze evidence when the Tor Browser is open, closed, and even after uninstallation, because artifacts may exist in different locations depending on the browser's state. Memory dumps can reveal live artifacts such as email content, session data, credentials, and attachments when the browser is running. Storage analysis can uncover downloaded email attachments, cached files, and remnants left behind after normal usage or uninstallation.

CHFI v11 specifically highlights scenarios involving email forensics with Tor Browser open and closed, memory acquisition, and post-uninstallation analysis as complementary techniques rather than isolated tasks. Focusing on only one browser state would result in incomplete evidence collection. Therefore, the overarching forensic objective is to explore email artifacts and attachments across various Tor Browser states, making option B the correct and CHFI-aligned answer.

質問: 11

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

正解: ([正解を表示します](#))

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.

質問: 12

法医学捜査官のヘンリーは、巧妙なルートキットによって侵害された疑いのあるシステムを分析している。そのルートキットは高度なもので、検出を回避するためにファイルやプロセスを隠蔽しているようだ。ヘンリーは、隠されたルートキットを暴くため、メモリとレジストリの分析を行うことにした。

ヘンリーの作業に最適なツールは次のうちどれでしょうか？

A. RegRipper

B. 変動性

C. ダンプル

D. 解剖

正解: ([正解を表示します](#))

Volatility is specifically designed for analyzing memory dumps and can uncover hidden processes, injected code, and rootkit activity that evade disk-based tools, making it the most effective choice for detecting stealthy rootkits.

質問: 13

調査担当者はjv16ツールを使用してどのようなマルウェア解析操作を実行できますか？

A. インストールモニター

B. レジストリ分析／モニタリング

C. ネットワークトラフィックの監視／分析

D. ファイルとフォルダの監視

正解: B ([コメントを发表する](#))

質問: 14

フォレンジック調査員のエレナは、マルウェア感染の疑いのある動作を分析しています。分析中に、Windowsイベントログに複数の異常なエントリ、特にイベントID 5156が記録されていることに

気づきました。エレナはこれらのログから、悪意のある活動を追跡するのに役立つ重要な情報としてどのような情報が得られると期待できるでしょうか？

- A. 不正アクセスに使用されたユーザー名とパスワード
- B. マルウェアによって削除されたファイルの場所
- C. 悪意のあるプロセスによるレジストリキーの変更の詳細
- D. プロセスの名前と通信したIPアドレス

正解: ([正解を表示します](#))

According to the CHFI v11 Operating System and Malware Forensics objectives, Windows Event ID 5156 is generated by the Windows Filtering Platform (WFP) and indicates that a network connection has been permitted. This event is highly valuable in malware investigations because it records detailed information about process-level network activity, which is a common indicator of compromise.

Event ID 5156 logs typically include:

Process name and Process ID (PID) that initiated the network connection
Source and destination IP addresses
Source and destination ports
Protocol used (TCP/UDP)
Direction of the connection (inbound or outbound)
CHFI v11 explicitly highlights the importance of Windows Security Event Logs in tracing malware behavior, especially for identifying command-and-control (C2) communications, data exfiltration attempts, and lateral movement. By analyzing Event ID 5156, investigators can directly correlate a specific executable or malicious process with external IP addresses, helping establish attacker infrastructure and timelines.

質問: 15

法医学捜査官のアレックスは、サイバー犯罪に関連する重要な証拠が含まれている可能性のある、損傷したAndroid端末の調査を命じられた。端末は物理的に損傷しており、起動せず、通常の復旧手順にも反応しない。アレックスは、この損傷した端末からデータを取得する最善の方法を見つける必要がある。

状況を踏まえ、アレックスはAndroidフォレンジックプロセスにおいて、データが適切に抽出されるように最初に行うべき手順を決定しなければなりません。証拠となるデバイスが破損している場合、アレックスはAndroidフォレンジックプロセスにおいて、次のうちどの操作を最初に行う必要がありますか？

- A. デバイスをルート化する
- B. JTAGフォレンジックを実施する
- C. 'dd'コマンドを使用して物理的なデータ取得を実行します。
- D. USBケーブルを使用してデバイスをフォレンジックワークステーションに接続します。

正解: B ([コメントを发表する](#))

When an Android device is physically damaged and cannot boot or be accessed through normal interfaces, JTAG forensics is the appropriate first step. It allows direct access to memory chips to extract data without relying on the device's operating system.

質問: 16

マルウェア分析は様々な方法で実施できます。調査担当者は疑わしい実行可能ファイル入手し、VirusTotalにアップロードして、そのファイルが悪意のあるファイルかどうかを確認し、その機能に関する情報を提供し、簡単なネットワークシグネチャを作成できる情報を提供します。ここではどのような種類のマルウェア分析が行われたのでしょうか？

- A. ハイブリッド
- B. ダイナミック
- C. 揮発性
- D. 静的

正解: D ([コメントを發表する](#))

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

ファイルシステム階層標準(FHS)において、作業に必要なバイナリファイルが格納されているディレクトリは次のうちどれですか？

- A. /sbin
- B. /proc
- C. /mnt
- D. /media

正解: ([正解を表示します](#))

質問: 18

以下のAndroidライブラリのうち、2D(SGL)または3D(OpenGL/ES)グラフィックコンテンツを画面にレンダリングするために使用されるものはどれですか？

- A. WebKit
- B. メディアフレームワーク
- C. サーフェスマネージャー
- D. OpenGL/ESおよびSGL

正解: D ([コメントを發表する](#))

質問: 19

スマートホームの窃盗事件には、フォレンジック調査員が対応します。IoTデバイスを特定、収集、保管し、クラウドサービスや同期されたスマートフォンから取得したデータを分析します。法廷提出用に、捜査プロセスと収集された証拠の概要をまとめた詳細な報告書を作成します。IoT フォレンジック プロセスのどの段階で、収集前に改ざんを防止することで証拠の整合性が維持されますか？

- A. プレゼンテーションとレポート
- B. データ分析
- C. 証拠の特定と収集
- D. 保存

正解: [D \(コメントを发表する\)](#)

According to the CHFI v11 Mobile and IoT Forensics domain, the preservation stage is specifically responsible for ensuring that digital evidence remains unaltered, intact, and legally admissible throughout the forensic lifecycle. Preservation begins immediately after evidence is identified and continues until the investigation is concluded and evidence is presented in court.

In IoT investigations, preservation is especially critical because IoT devices--such as smart locks, cameras, sensors, and hubs--often contain volatile data, limited storage, and continuous network connectivity. CHFI v11 emphasizes that investigators must take steps such as isolating devices from networks, disabling remote access, preventing firmware updates, maintaining power states when necessary, and documenting handling procedures to avoid unintentional data modification or loss.

While evidence identification and collection focuses on locating and acquiring devices and data sources, it does not by itself guarantee protection against alteration. Data analysis and presentation/reporting occur later and rely on evidence that has already been preserved correctly. Any failure in preservation can compromise chain of custody and result in evidence being challenged or excluded.

CHFI v11 explicitly states that preservation safeguards evidence integrity before, during, and after collection, making it the foundation of a defensible IoT forensic investigation.

質問: 20

SMTPサーバーに関して、次の記述のうち正しいものはどれですか？

- A. SMTPサーバーは、受信者のアドレスを受信者名とドメイン名に分解してからDNSサーバーに渡します。
- B. SMTPサーバーは、受信者のアドレスを受信者の名前と役職に分解してからDNSサーバーに渡します。
- C. SMTPサーバーは、受信者のアドレスを受信者の名前とイニシャルに分解してからDNSサーバーに渡します。
- D. SMTPサーバーは、受信者のアドレスを受信者名と受信者のアドレスに分割してからDNSサーバーに渡します。

正解: [\(正解を表示します\)](#)

質問: 21

ある企業のオンラインバンキングプラットフォームで最近、セキュリティ侵害が発生し、顧客アカウントへの不正アクセスが相次いでいる。調査の結果、ブルートフォース攻撃によって侵入が試みられている疑いがある。

上記のシナリオにおいて、「ブルートフォース攻撃」という用語は、おそらく何を指していると考えられますか？

- A. ハッカーがユーザーインターフェース要素を操作して機密データにアクセスする攻撃。
- B. 従業員を騙してログイン認証情報を漏洩させるソーシャルエンジニアリングの手法。
- C. 企業のネットワークインフラストラクチャの脆弱性を悪用する方法。
- D. 攻撃者が不正アクセスを得るために、パスワードや暗号鍵を組織的に推測する手法。

正解: [D \(コメントを发表する\)](#)

A brute force attack involves systematically trying numerous combinations of passwords or keys until the correct one is found, enabling unauthorized access.

質問: 22

フォレンジック調査員のマディソンは、メール詐欺事件の捜査を任されました。容疑者は、不正アクセスされたメールアカウントを利用して複数の被害者にフィッシングメールを送信したとされています。捜査の一環として、マディソンはまず、容疑者のパソコンと、詐欺メールの送信に使用されたメールサーバーの現地調査を行う許可を得なければなりません。

法医学的検査を進める前にマディソンが最初に取りなければならないステップは何ですか？

- A. コンピュータと電子メールアカウントの押収
- B. メールヘッダーの取得
- C. 削除された電子メールメッセージを回復する
- D. メールヘッダーの分析

正解: [\(正解を表示します\)](#)

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.

質問: 23

フォレンジック調査員のイーサンは、容疑者のコンピュータを分析していたところ、サイバー犯罪に関連する可能性のある不審なファイルを発見しました。ファイルのメタデータを調べたところ、ファイルは複数回変更されており、最後にアクセスされたのは犯罪発生の直前でした。ファイルが改ざんまたは操作されたかどうかを判断するために、イーサンにとって最も有用なフォレンジック手法は次のうちどれでしょうか？

- A. ファイルのファイルシステムログを確認します
- B. 隠し属性または代替データストリームを探す
- C. ファイルのアクセス制御リスト(ACL)を確認します
- D. ファイルのハッシュ値を調べる

正解: ([正解を表示します](#))

Within the CHFI v11 curriculum, verifying the integrity of digital evidence is a core responsibility of a forensic investigator. The most reliable method to determine whether a file has been tampered with is by examining its cryptographic hash value. A hash value (such as MD5 or SHA-256) is a fixed-length digital fingerprint generated from the file's contents. Even the smallest change to the file--whether intentional or accidental--will produce a completely different hash value, making hash comparison a definitive method for detecting manipulation.

File system logs (Option A) can help reconstruct timelines by showing access or modification events, but logs can be deleted, altered, or incomplete and do not directly validate file content integrity. Hidden attributes or alternate data streams (Option B) are indicators of possible anti-forensics techniques, yet their presence does not confirm that the primary file data was altered. Access Control Lists (Option C) only describe permission settings and ownership, not whether the file itself was modified.

According to the CHFI v11 objectives under Digital Evidence, Data Acquisition, and Evidence Validation, investigators must calculate and verify hash values during acquisition and analysis to maintain chain of custody, ensure evidence integrity, and support legal admissibility. This makes hash examination the most appropriate and forensically sound choice in this scenario

質問: 24

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。

正解: D ([コメントを发表する](#))

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.

質問: 25

企業の機密データを侵害したサイバー攻撃に関するフォレンジック調査において、調査員は、当該組織が様々な社内システムにおけるユーザーアクセス管理にクラウドベースのソリューションを使用していることを発見しました。このソリューションには、シングルサインオン(SSO)、多要素認証(MFA)、詳細なアクセス制御といった機能が含まれており、これらはすべてサードパーティのサービスプロバイダーによって管理されています。調査員は認証システムのログを解析し、システムアクセスパターンと比較することで、侵害時の不正行為を追跡します。当該組織ではどのような種類のクラウドサービスが利用されているのでしょうか？

- A. 組織は、アクセス制御または認証管理に Desktop-as-a-Service (DaaS) を使用します。
- B. 組織は、システムおよびネットワーク上のユーザー アクセスを管理するために Infrastructure-as-a-Service (IaaS) を使用します。
- C. 組織は、Platform-as-a-Service (PaaS) を使用して、カスタム構築された認証およびアクセス制御アプリケーションを展開および管理します。
- D. 組織は、承認ルールを適用するために Identity-as-a-Service (IDaaS) を使用します。

正解: ([正解を表示します](#))

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) .

質問: 26

技術的に権限のない人物がコンピュータを調査すると、ほぼ必ず以下の結果になります。

- A. 検査結果が完全に正確
- B. 保管管理の連鎖が完全に維持されている
- C. 法廷で証拠として認められないものとする
- D. 法廷で証拠として認められるものを法廷で証拠能力のあるものとする

正解: ([正解を表示します](#))

質問: 27

次のうち、データベースの開始点とみなされ、MS SQLサーバーにユーザーデータとデータベースオブジェクトを格納するものはどれですか？

- A. プライマリデータファイル(MDF)
- B. ibdata1
- C. アプリケーションデータファイル(ADF)
- D. トランザクションログデータファイル(LDF)

正解: ([正解を表示します](#))

質問: 28

企業データ侵害に関する徹底的なフォレンジック調査を完了した後、フォレンジック調査員はクライアントのために詳細かつ包括的なレポートを作成します。このレポートには、調査で得られたすべての知見と、使用された調査手法の明確な説明が含まれています。また、調査員は、クライアントが将来同様のインシデントを未然に防ぐための、体系的な推奨事項も提供します。調査員は、クライアントが知見を完全に理解し、推奨事項に基づいて行動できるよう支援します。このケースにおいて、調査員はどのベストプラクティスを実践しているのでしょうか？

- A. 調査段階では機密情報の機密性を確保し、指定されたチャネル以外で詳細を話し合わないこと。
- B. 調査を開始する前に、潜在的な結果について明確な期待を設定します。
- C. 報告会中にフィードバック ループを提供し、質問に答えます。
- D. 調査結果を検討し、法令遵守を確保するために法律顧問を雇用します。

正解: **C** ([コメントを发表する](#))

According to the CHFI v11 objectives under Reporting, Managing Clients or Employers during Investigations, and Testifying and Presenting Findings, an essential forensic best practice is ensuring that investigation results are clearly communicated and properly understood by stakeholders. The scenario described aligns directly with the practice of offering a feedback loop and conducting a debriefing session, where the investigator explains findings, methodologies, conclusions, and recommendations to the client in a structured and understandable manner. CHFI v11 emphasizes that a forensic report is not sufficient on its own; investigators must also ensure that clients can interpret the results correctly and take informed action. A debriefing session allows clients to ask questions, clarify technical details, and understand the impact of the findings on business operations, risk posture, and compliance requirements. This practice strengthens trust, improves decision-making, and demonstrates professional responsibility.

質問: **29**

フォレンジック調査官がAndroidデバイスとフォレンジックワークステーション間の通信を確立し、デバイスからデータを取得するために使用できるコマンドラインツールは何ですか？

- A. Android Debug Bridge
- B. SDKマネージャー
- C. APKアナライザー
- D. Xcode

正解: ([正解を表示します](#))

質問: **30**

サイバー犯罪捜査中、スミス刑事は元のデータにアクセスしましたが、その影響を理解する専門知識が不足していたため、証拠の完全性が損なわれました。プロセスが文書化されていないため、法廷における証拠の許容性に懸念が生じます。上記のシナリオにおいて、スミス刑事は警察長官協会 (ACPO) のデジタル証拠原則のどの原則に違反しましたか？

- A. 原則 2: データにアクセスする個人は有能でなければなりません。
- B. 原則 4: 調査リーダーは原則の遵守を確実にします。
- C. 原則 3: プロセスの監査証跡は保存される必要があります。
- D. 原則 1: 依存するデータはいかなるアクションによっても変更されるべきではありません。

正解: ([正解を表示します](#))

According to the CHFI v11 syllabus under Rules and Regulations Pertaining to Search and Seizure of Evidence and ACPO Principles of Digital Evidence, Principle 2 states that any person accessing original digital evidence must be competent to do so and able to explain the relevance and implications of their actions. This principle is critical because improper handling of digital evidence--even without malicious intent--can result in accidental alteration, loss of context, or misinterpretation, ultimately jeopardizing evidence integrity and admissibility.

In the given scenario, Detective Smith accessed original data without sufficient expertise to understand the implications of his actions. This directly violates Principle 2, as competence is a

mandatory requirement when interacting with digital evidence. While the failure to document processes also raises concerns related to auditability, the primary violation highlighted is the lack of competency in handling original evidence.

Principle 1 focuses on preventing changes to original data, Principle 3 emphasizes maintaining an audit trail, and Principle 4 assigns responsibility to the investigation lead for overall compliance. However, the root issue here is that an unqualified individual accessed evidence without the necessary knowledge or skills.

質問: 31

鑑識調査中、調査官は16進エディタを使用してファイルを開き、バイナリデータを調べます。内容を分析している際に、調査官は「00」と「

ファイル内のさまざまなセクションに「FF」バイト値が散在しています。これらのバイト列は繰り返し出現し、ファイルの広い領域を占めています。ファイル解析の観点から、これらの値はどのような意味を持つのでしょうか？

- A. ファイルパディングまたは未使用データ。多くの場合、ファイルが必要なサイズまたはアライメントに達するようにするために使用されます。
- B. ファイル圧縮。圧縮されたデータまたは繰り返しパターンのブロックが存在することを示します。
- C. 暗号化されたデータ。これらのバイト値はエンコードされたコンテンツを表し、適切な鍵でのみ復号化できます。
- D. データ破損。ファイルが破損しているか、不完全である可能性があります。

正解: A ([コメントを发表する](#))

Repeated "00" and "FF" byte values commonly indicate padding or unused space within a file, used for alignment or to fill allocated storage regions rather than representing meaningful data.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637**問、**30%**ディスカウント、特別な割引コード: **JPNshiken**」

質問: 32

ディスクドライブのデータ密度は、_____を使用して計算されます。

- A. トラックスペース、ビットエリア、スラックスペース。
- B. トラック密度、面積密度、およびスラック密度。
- C. スラック空間、ビット密度、スラック密度。
- D. トラック密度、面密度、ビット密度。

正解: ([正解を表示します](#))

質問: 33

デジタルフォレンジック調査員として、ディスクデータを分析して削除されたファイルの証拠やその他の関連情報を発見することが任務です。16進エディターは、ディスクの物理的な内容を調べ、削除されたファイルの残骸を探すために不可欠なツールです。

16 進エディタのどの領域に、16 進領域に表示されている各バイトの ASCII 表現が表示されますか？

- A. アドレス領域
- B. 16進数領域
- C. フッター領域
- D. 文字領域

正解: ([正解を表示します](#))

According to the CHFI v11 Computer Forensics Fundamentals and File Analysis modules, a hex editor is a critical forensic tool used to view and analyze raw disk data at the byte level. Hex editors typically present data in three main columns or areas: the address (offset) area, the hexadecimal area, and the character (ASCII) area.

The character area displays the ASCII interpretation of each byte shown in the hexadecimal area. This allows investigators to visually identify readable text strings, file headers, metadata, embedded scripts, usernames, URLs, file signatures, and fragments of deleted files that may still reside in unallocated space or slack space. Printable characters are shown as readable text, while non-printable bytes are usually represented by dots (.).

The address area shows the offset or location of the data within the file or disk. The hexadecimal area displays the raw byte values in hexadecimal format, which is essential for precise byte-level analysis. A footer area is not a standard component of hex editor layouts as defined in CHFI v11.

質問: 34

セキュリティアナリストのオリビアは、銀行のウェブサイトで潜在的な脆弱性を特定するため、ペネトレーションテストを実施しています。入力フィールドを確認しているうちに、サイトがSQLインジェクション攻撃に対して脆弱である可能性があると疑いました。テスト中に、通常とは異なるエンコード手法が適用されていると思われるURLを発見しました。特に目立つURLの1つでは、入力データが二重エンコードされているように見えます。これは、SQLインジェクションを防止する検出フィルターを回避し、バイパスするためである可能性があります。次のURLのうち、SQLインジェクション攻撃を実行するために二重エンコードが使用されていることを示すものはどれですか？

- A. `http://www.bank.com/accounts.php?id=1%252f%252a*/union%252f%252a*/select%252f%252a*/1,2,3%252f%252a*/ユーザーから--`
- B. `http://www.bank.com/accounts.php?id=1+UnIoN/**/SeLeCT/**/1,2,3--`
- C. `http://www.bank.com/accounts.php?id=1+UNunionION+SEselectLECT+1,2,3--`
- D. `http://www.bank.com/accounts.php?id=1+uni%0bon+se%0blect+1,2,3--`

正解: **A** ([コメントを发表する](#))

According to the CHFI v11 Web Application Forensics and Network & Web Attacks module, attackers commonly use encoding and obfuscation techniques to bypass input validation mechanisms, web application firewalls (WAFs), and intrusion detection systems. One such advanced technique is double URL encoding, which involves encoding already URL-encoded characters a second time.

In URL encoding, the forward slash / is represented as %2F. When this value is encoded again, % becomes %25, resulting in %252F. In Option A, multiple occurrences of %252f clearly indicate that characters such as / and comment markers (/ * /) have been double encoded. When processed by the web server or application, the input may be decoded twice, ultimately reconstructing a valid SQL injection payload like UNION SELECT, thereby bypassing security filters.

質問: **35**

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のでしょうか？

- 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

正解: ([正解を表示します](#))

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.

質問: **36**

SSD(ソリッドステートドライブ)に関して、次の記述のうち正しいものはどれですか？

- A. 高速なデータアクセス、低消費電力、高信頼性は、HDDに比べてSSDが持つ主な利点のひとつです。

- B. HDDと同様に、SSDにも可動部品があります。
- C. SSDは、データを保存するためのトラック、クラスタ、セクタを備えています。
- D. SSDは不揮発性データを保存できません

正解: **A** ([コメントを发表する](#))

質問: 37

政府によるインターネットアクセスの厳格な規制が敷かれた国で、サイバーセキュリティアナリストは機密性の高い通信が監視されているのではないかと疑っています。この監視を回避するため、アナリストはTorネットワークの利用を検討します。しかし、政府の規制により、Torネットワークに直接アクセスすることはできません。このような状況で、サイバーセキュリティアナリストはどのようにして政府の監視を回避し、Torネットワークにアクセスすることができるのでしょうか？

- A. ブリッジノードを使用して Tor ネットワークにアクセスする
- B. 公開されているTorリレーノードを利用する
- C. Tor出口ノードとの直接通信を確立する
- D. 政府当局と協力してTorネットワークへのアクセスを取得する

正解: ([正解を表示します](#))

According to the CHFI v11 Dark Web Forensics objectives, governments that enforce strict internet censorship often block access to publicly listed Tor entry (guard) relays by using IP blacklisting, deep packet inspection (DPI), and traffic fingerprinting. In such environments, connecting directly to the Tor network using standard relay information becomes ineffective.

To overcome this restriction, Tor provides bridge nodes (Tor bridges). Bridges are unlisted Tor entry relays whose IP addresses are not published in the public Tor directory, making them significantly harder for censors to detect and block. CHFI v11 explicitly identifies Tor bridges as a key mechanism for bypassing government surveillance and censorship. Bridges may also use pluggable transports (such as obfs4, meek, or snowflake) that disguise Tor traffic to appear like normal HTTPS or other benign traffic, further evading detection.

質問: 38

ハリス刑事は地元銀行のデータベースへのサイバー攻撃に関するデジタルフォレンジック調査を指揮している。

捜査中、ハリス刑事は証拠の完全性を維持することの重要性を強調しています。彼はチームに対し、法廷での証拠能力を確保するため、データ取得に関する確立された経験則に従うよう指示しています。銀行のデータベースへのサイバー攻撃に関するハリス刑事のデジタルフォレンジック捜査において、元の証拠を保存し、その完全性を確保するために不可欠な手順は何ですか？

- A. 疑わしいドライブまたはファイルの複製ビットストリームイメージを作成する
- B. 複数のフォレンジックツールを同時に使用してデータを取得する
- C. 複製プロセスを無視し、元の証拠に基づいて直接分析を進める
- D. 元の証拠に対して直接フォレンジック分析を実行する

正解: **A** ([コメントを发表する](#))

According to the CHFI v11 objectives under Data Acquisition Concepts and Rules and Digital Evidence Handling, the most critical step in preserving original evidence integrity is the creation of a duplicate bit-stream image of the suspect media. A bit-stream image (also known as a forensic image) is an exact sector-by-sector copy of the original storage device, including allocated space, unallocated space, slack space, and hidden data. This ensures that no data is altered, added, or omitted during acquisition.

CHFI v11 clearly states one of the fundamental rules of thumb for data acquisition: never perform analysis on original evidence. Instead, investigators must work exclusively on verified copies while the original evidence is preserved in a secured state. Hash values are calculated before and after imaging to confirm that the duplicate image is an exact replica, thereby supporting chain of custody and court admissibility.

質問: 39

コンピューターフォレンジック調査官のレイチェルは、ある法律事務所で発生したデータ窃盗事件を調査している。彼女は、データ漏洩の原因と思われる特定のコンピューターに存在するデータを取得して分析する必要がある。しかし、そのコンピューターは重要な業務に継続的に使用されている。

レイチェルはデータ取得方法について検討している。状況の緊急性を考慮すると、レイチェルはどのタイプのデータ取得方法を選択すべきだろうか？

- A. ライブアクイジション
- B. 遠隔取得
- C. 静的取得
- D. 差分取得

正解: ([正解を表示します](#))

Live acquisition allows Rachel to collect data from the system while it is still running and in use, enabling access to both volatile and non-volatile data without interrupting critical operations.

質問: 40

世界的な金融機関でデータ漏洩が発生したことを受け、同社のインシデント対応チームは漏洩源の特定に尽力してきた。データベース管理者は、同社のSQL Serverデータベース内のいくつかのテーブルが変更されていることに気づいた。注文履歴、財務情報、顧客情報に変更が加えられていることが判明した。トランザクションログには、通常では考えられない多数のクエリによる変更が記録されていた。攻撃者はリモート接続を介してアクセスしたようで、ログイン情報が漏洩した可能性が示唆された。

法医学捜査官として、情報漏洩の原因を特定するために次にどのような手順を踏みますか？

- A. 接続が開始された送信元IPアドレスを特定する必要があります。
- B. 最近アクセスされたファイルを評価する必要があります。
- C. 異常なログインパターンがないか、サーバーログを評価する必要があります。
- D. システム全体のスキャンを実行する必要があります。

正解: ([正解を表示します](#))

Identifying the source IP of the remote connection directly helps trace where the unauthorized access originated, providing a key lead to the attacker's location or entry point.

質問: 41

ウェブブラウザは、ユーザーの活動に関する関連情報を保存できます。フォレンジック調査官は、ファイル、リスト、アクセス履歴、Cookieなど、さまざまなデジタル痕跡を復元できます。この作業に役立つツールはどれでしょうか？

- A. MZCacheView
- B. タスクマネージャー
- C. Google Chrome リカバリーユーティリティ
- D. 最近使用したリスト(MRUリスト)

正解: **A** ([コメントを發表する](#))

質問: 42

サイバー攻撃を受け、大手eコマースプラットフォームは広範囲にわたるシステムダウンを経験し、甚大な経済的損失と顧客からの信頼失墜につながりました。制御回復に奔走する中で、顧客の機密データが漏洩したことが明らかになり、データセキュリティとプラットフォームの評判が脅かされました。eコマースプラットフォームへのサイバー攻撃の余波の中で、フォレンジック対策の不足に起因するものではないのは、次のうちどれでしょうか？

- A. データの改ざん、削除、盗難
- B. システムのダウンタイム
- C. 法務部門とIT部門の連携は限定的
- D. 法的に健全な証拠を収集できない

正解: **B** ([コメントを發表する](#))

According to the CHFI v11 objectives under Computer Forensics Fundamentals, Forensic Readiness, and Incident Response Integration, forensic readiness refers to an organization's ability to efficiently collect, preserve, analyze, and present digital evidence while minimizing the cost and impact of investigations. A lack of forensic readiness primarily affects how well an organization can respond to, investigate, and legally defend itself after an incident--not whether the incident causes operational disruption.

System downtime (Option B) is a direct operational impact of a cyberattack, such as a DDoS attack, ransomware infection, or system compromise. While poor preparedness may prolong recovery, downtime itself is not caused by the absence of forensic readiness; it is caused by the attack's technical and operational effects. Therefore, system downtime is not a consequence of lacking forensic readiness.

質問: 43

ある多国籍テクノロジー企業は、元幹部が社内の機密情報に不正アクセスした可能性があると考えている。この幹部は、AndroidからiOSスマートフォンに機種変更した後に機密データを送信した疑

いで調査を受けている。鑑識チームは、疑惑を裏付けるためにデジタルデータを綿密に検証する必要がある。

この状況を踏まえると、iOSとAndroidのファイルシステムに関する以下の主張のうち、最も正しいのはどれでしょうか？

- A. iOSのファイルシステムにはFile-Vaultなどの暗号化メカニズムが組み込まれており、データセキュリティは強化されていますが、フォレンジック調査は複雑になります。
- B. Androidのファイルシステムは、特別なツールを必要とせずにユーザーデータに直接アクセスできるため、iOSに比べてフォレンジック分析が容易です。
- C. AndroidのファイルシステムはExt4に依存していますが、iOSのファイルシステムはAPFSを使用しています。
- D. AndroidとiOSのファイルシステムはどちらも、データの整合性を維持し、復旧を容易にするためにジャーナリングメカニズムを採用しています。

正解: ([正解を表示します](#))

Android commonly uses the Ext4 file system, while iOS uses APFS, which is designed with strong encryption and security features, impacting forensic analysis approaches.

質問: 44

Windows OSのファイルシステムからファイルが削除されると、ファイルのヘッダーはどうなりますか？

- A. OSはファイルの16進バイトコード全体を置き換えます
- 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は削除されたファイル名の2文字目を16進バイトコードEh5に置き換えます。
- D. ファイルの16進バイトコードは同じだが、ファイルの場所が異なる

正解: ([正解を表示します](#))

質問: 45

CHFIの経験豊富な専門家であるエドワードは、大手企業における知的財産窃盗の可能性について調査を行っていた。同社は疑わしいシステムを特定しており、エドワードはデータ収集を担当していた。調査の重大性を考慮すると、エドワードは収集したデータがフォレンジック的に健全であり、完全性を維持し、法廷での精査に耐えうるものであることを確認する必要があった。これを実現するために、エドワードはデータ取得に関してどの経験則に従うべきだろうか？

- A. エドワードは、システムの状態に関係なく、ライブデータ取得を選択すべきです。
- B. エドワードは、侵入性が低いネットワークベースの取得方法に頼るべきです。
- C. エドワードは、一貫性を保つ非揮発性データに注力すべきです。
- D. エドワードは元のデータに変更を加えることを避けるべきです。

正解: D ([コメントを發表する](#))

The fundamental principle in forensic data acquisition is to preserve the original evidence in its exact state. Avoiding any modification ensures integrity, maintains evidentiary value, and guarantees that the data remains admissible in court.

質問: 46

調査員がハードディスクを調査したところ、2つのパーティションの間に大量の未使用領域があることが分かりました。この領域には、オペレーティングシステムが認識できない隠しデータが含まれています。

法医学調査中にこの隠されたデータにアクセスするために使用できる方法はどれですか？

- A. ディスク全体のバックアップを実行しています
- B. ディスクを再フォーマットして隠しデータを削除します
- C. ディスククリーンアップユーティリティを実行しています
- D. ディスクエディタツールを使用してパーティション間のギャップを調べる

正解: ([正解を表示します](#))

This scenario aligns with CHFI v11 objectives under Anti-Forensics Techniques and Disk and File System Analysis. Attackers and sophisticated users may intentionally hide data in areas of a disk that are not addressed by the operating system, such as inter-partition gaps, slack space, or unallocated space. These techniques are commonly used as anti-forensic methods to conceal illicit data from standard file system views and basic forensic tools.

CHFI v11 emphasizes that such hidden data cannot be accessed through normal OS utilities, disk cleanup tools, or backups that rely on file system structures. Instead, forensic investigators must use disk editor tools or low-level forensic utilities that allow direct sector-by-sector examination of the storage media. Disk editors enable investigators to view raw hexadecimal data, inspect unallocated areas, analyze partition tables, and uncover hidden or deliberately concealed content stored outside recognized partitions.

Reformatting or cleaning the disk would destroy potential evidence and violate forensic principles, while full disk backups alone do not inherently reveal hidden inter-partition data without further low-level analysis. Therefore, consistent with CHFI v11 best practices for uncovering hidden data and countering anti-forensic techniques, using disk editor tools to examine the inter-partition gap is the correct and forensically sound approach.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637問、30%ディスカウント、特別な割引コード: **JPNshiken****」

質問: 47

進行中のサイバー犯罪捜査の一環として、捜査官がダークウェブのチャットルームの通信内容を調査する任務に就きました。チャットログは数週間にわたり、難解な言葉、暗号化された表現、そして検出を回避するために意図的に作られた誤解を招くような発言が多数含まれています。この膨大な

量のメッセージを精査して有益な情報を抽出することは、非常に時間と労力を要する作業であり、ノイズを除去して重要な詳細に焦点を当てるためには、高度な分析ツールと体系的なアプローチが必要です。このシナリオは、ダークウェブのフォレンジックにおけるどのような課題を浮き彫りにしているのでしょうか？

- A. ダークウェブのようなグローバルな匿名プラットフォームから証拠を収集する際の法的課題。
- B. 難読化されたコンテンツを含む大量のチャットルーム通信を処理するという課題。
- C. チャットルームでのコミュニケーションと現実世界の身元を関連付けるという課題。
- D. チャットルームでの真正なコミュニケーションと欺瞞的なコミュニケーションを区別することの難しさ。

正解: ([正解を表示します](#))

The scenario emphasizes the overwhelming volume of chat data combined with obfuscated and coded language, making it difficult to process and extract relevant information efficiently. This directly reflects the challenge of handling extensive communications with hidden or disguised content.

質問: 48

デビーは、既知の小児性愛者の家を検索するための令状を取得しました。デビーはその家に行き、違法な画像のダウンロードに使用されていると記録されているデジタル機器を押収するために捜索令状を執行しました。彼女はデジタルカメラを除くすべてのデジタル機器を押収しました。なぜ彼女はデジタルカメラを押収しなかったのでしょうか？

- A. デジタルカメラは古く、画面にひびが入っており、電池も入っていませんでした。そのため、犯罪に使用されたとは考えられません。
- B. デビーが証拠品を運ぶために使用していた車両は既に満載で、これ以上物を運ぶことができなかった。
- C. デビーはデジタルカメラがコンピュータシステムではないため、それを見落とした。
- D. デジタルカメラは、令状に記載されているデジタル機器の一つとしてリストされていませんでした。

正解: C ([コメントを發表する](#))

質問: 49

サイバー犯罪捜査において、捜査官はハッキング活動の証拠を探すために容疑者のコンピュータシステムを検索するための令状を取得します。容疑者の電子機器からデータを収集する際に、システムに接続している他のユーザーの身元を明らかにする情報に意図せずアクセスしてしまうことがあります。

サイバー犯罪捜査プロセスのどのステップでプライバシーの問題に関する懸念が生じますか？

- A. ネットワークセキュリティ対策の実装
- B. 法医学的分析の実施
- C. 他のユーザーの匿名性を維持する
- D. 捜索令状の取得

正解: ([正解を表示します](#))

According to the CHFI v11 Regulations, Policies, and Ethics domain, privacy issues most commonly arise during the forensic analysis phase of a cybercrime investigation. While search warrants legally authorize investigators to collect and examine specific digital evidence, they are typically scope-limited to the suspect, systems, data types, and timeframes defined in the warrant. During forensic analysis, investigators may inadvertently encounter personal or sensitive information belonging to third parties, such as usernames, email addresses, chat records, credentials, or identifiers of other users connected to the system. CHFI v11 explicitly highlights this phase as legally and ethically sensitive because analysts must ensure that non-relevant data and third-party information are handled carefully to avoid violations of privacy laws and data protection regulations.

Implementing network security measures is a preventive activity, not an investigative one. Obtaining search warrants is a legal safeguard designed to protect privacy, not create privacy concerns. Preserving anonymity is a mitigation action, not the step that introduces the risk. CHFI v11 stresses the importance of minimization, access control, proper documentation, and legal oversight during forensic analysis to prevent misuse or overexposure of unrelated personal data. Failure to manage privacy during this phase can result in legal challenges, evidence exclusion, or regulatory violations.

質問: 50

被害者のコンピュータから取得したメモリダンプに対して、フォレンジック調査官がマルウェア分析を行っているシナリオを考えてみましょう。調査官はVolatility Frameworkを使用してRAMの内容を分析しますが、メモリダンプ内の隠されたプロセスや注入されたコード/DLLを特定するのに役立つプラグインはどれでしょうか？

- A. マルフィンド
- B. モデル
- C. マルスキャン
- D. pslist

正解: ([正解を表示します](#))

質問: 51

被害者、目撃者、または容疑者の電子機器上のデジタル証拠にアクセスする前に、捜査官は法的プライバシー要件を尊重するためにまず何をすべきでしょうか？

- A. 検索を行うための正式な書面による同意を得る
- B. バッテリーを取り外すか、デバイスの電源を切ってください。
- C. 地方自治体または雇用主に事実を通知する
- D. デバイスを外部通信から保護します

正解: ([正解を表示します](#))

質問: 52

大規模なデータ漏洩事件において、サイバー攻撃者がフォレンジック対策としてプログラムパッカーを使用している疑いがあります。あなたは主任サイバーセキュリティ調査官として、この事態に対処するよう命じられました。このフォレンジック対策を無効化するために、次のうちどの対策が最も効果的でしょうか？

- A. ネットワーク脆弱性スキャンの頻度を増やします。
- B. 解凍ツールを使用して、パッキングプロセスを逆転させ、元のコードを明らかにします。
- C. 安全なコーディング手法を導入する。
- D. すべてのシステムでウイルス対策ソフトウェアを定期的に更新してください。

正解: ([正解を表示します](#))

Program packers conceal the original executable by compressing or encrypting it. Using unpacking tools reverses this process, revealing the original code for analysis and enabling effective investigation.

質問: 53

あなたは、機密データの漏洩の可能性を調査している大手テクノロジー企業で、コンピュータフォレンジック調査官として働いています。最重要容疑者は、最近退職した従業員です。会社は、容疑者の業務用ノートパソコン(Windows OS搭載)を押収しました。あなたの責任は、調査に必要なデータを取得することです。事件の重大性を考慮すると、証拠の完全性を維持しなければなりません。システムはまだ稼働しており、揮発性データの収集が最優先事項です。揮発性データを収集するための最も正確な手順は何ですか？

- A. システムの状態、開いているポートのリスト、実行中のプロセス、およびネットワーク接続。
- B. ネットワーク接続、実行中のプロセス、開いているポートのリスト、システムの状態。
- C. 開いているポート、実行中のプロセス、ネットワーク接続、システム状態のリスト。
- D. 実行中のプロセス、システムの状態、ネットワーク接続、および開いているポートのリスト。

正解: ([正解を表示します](#))

Volatile data should be collected in order of most rapidly changing to least. Network connections change the fastest and must be captured first, followed by running processes, then open ports, and finally the broader system state which is comparatively more stable.

質問: 54

あるアパレル会社は、コンバージョン率と顧客基盤の拡大を目指し、最新製品ラインに関するウェブサイトを実近開設しました。同社に最近任命されたネットワーク管理者であるアンドリューは、ウェブサイトを不正侵入や脆弱性から保護する任務を任されています。この状況において、アンドリューは次のどのツールを導入することを検討すべきでしょうか？

- A. コン・ブート
- B. レキュバ
- C. CryptaPix
- D. ModSecurity

正解: ([正解を表示します](#))

質問: 55

フォレンジック調査員のヘイゼルは、journalctlを使用してLinuxサーバーのSSHログを分析しています。不正アクセスの可能性を追跡するため、ログからSSHキーのフィンガープリントを抽出する必要があります。ヘイゼルがSSHユニットログでSSHキーのフィンガープリントを表示するには、以下のコマンドのうちどれを実行すればよいでしょうか？

- A. journalctl -u ssh --昨日から
- B. journalctl -fu ssh
- C. journalctl -u ssh --since -1h
- D. journalctl -u ssh

正解: ([正解を表示します](#))

According to the CHFI v11 Operating System Forensics objectives, Linux system logs are a critical source of evidence for identifying unauthorized access, brute-force attempts, and SSH key based authentication activities. On modern Linux systems that use systemd, SSH-related events are logged and managed by the system journal, which can be queried using the journalctl utility. The command journalctl -u ssh retrieves all log entries associated with the SSH service unit, making it the most appropriate command when an investigator needs a complete and unfiltered view of SSH activity. SSH key fingerprints are typically logged during public key authentication events, including successful and failed login attempts, and may appear alongside details such as usernames, source IP addresses, and authentication methods.

質問: 56

法医学捜査官のイーサンは、悪意のあるオンライン活動に使用されている疑いのあるコンピュータシステムの調査を命じられました。調査の一環として、彼はシステム上で実行されたアプリケーションを特定する必要があります。このデータを分析することで、悪意のあるソフトウェアがインストールされているかどうかを確認できます。この情報を収集するために、イーサンは実行されたアプリケーションの痕跡が保存されている適切なシステムディレクトリを調べる必要があります。システム上で実行されたアプリケーションの痕跡を見つけるために、イーサンは次のどのディレクトリを調べるべきでしょうか？

- A. プロセスダンプ
- B. プリフェッチ
- C. Rplog
- D. 変更履歴

正解: ([正解を表示します](#))

The Prefetch directory in Windows stores files that record information about executed applications, including execution times and frequency, making it valuable for identifying program activity.

質問: 57

会社のクラウド管理者であるフランクは、業務上重要なデータが保存されている2台のAzure VMのOSディスクのバックアップを取る必要があります。この目的のために、彼はどのタイプのAzure Blobストレージを使用できますか？

- A. 中サイズの塊
- B. ページブロブ
- C. ブロックブロブ
- D. ブロブを追加する

正解: **B** ([コメントを發表する](#))

質問: 58

Windowsベースのシステムから揮発性データを取得するのに最も効果的なツールは次のうちどれですか？

- A. エセリアル
- B. データグラブ
- C. 振付
- D. らせん構造

正解: ([正解を表示します](#))

質問: 59

コンピュータフォレンジック調査官が、犯罪行為の証拠が含まれている疑いのあるハードディスクドライブ(HDD)を分析しています。このHDDは、20,000シリンダ、16ヘッド、1トラックあたり63セクタ(各セクタは512バイト)で構成されています。分析中に、調査官はディスク上に1.5KBのファイルを発見しました。このファイルに割り当てられるセクタ数はいくつでしょうか？また、このようなセクタ割り当ては、調査にどのような影響を与える可能性がありますか？

- A. 2セクター。ファイルが断片化されている可能性があり、復元が困難になる場合があります。
- B. 4セクター。ディスク上のスペース利用効率が低下する可能性があります。
- C. 3セクター。セクターオーバーヘッドの増加により、取得時間が長くなる可能性があります。
- D. 3セクター。ファイルが断片化されている可能性があり、復元が困難になる場合があります。

正解: ([正解を表示します](#))

Although 1.5KB equals 1536 bytes (which is 3 sectors at 512 bytes/sector), file systems often allocate storage in clusters/blocks larger than a single sector (e.g., 2KB or 4KB blocks). If the allocation unit is 2KB, the file may occupy 4 sectors (2048 bytes), creating slack space and inefficient utilization. That slack space can also contain remnants of prior data-relevant for investigation.

質問: 60

悪質なハッカーであるアンバーは、魅力的な小さな広告にマルウェアを埋め込み、様々なウェブサイトに表示される人気の広告ネットワークに掲載しました。彼女は何をしているのでしょうか？

- A. 正規サイトを侵害する
- B. クリックジャッキング
- C. マルバタイジング
- D. スピアフィッシング

正解: **C** ([コメントを發表する](#))

質問: 61

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

正解: ([正解を表示します](#))

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.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637問、30%ディスカウント、特別な割引コード: JPNshiken**」

質問: 62

鑑識捜査において、捜査官は容疑者のスマートフォンからデータを収集する必要があります。捜査官は、収集したデータが法廷で証拠として認められるよう、適切な手続きに従う必要があることを認識しています。また、個人情報や機密情報が含まれている可能性のある携帯端末を取り扱う際には、法的および倫理的な問題にも留意しなければなりません。

調査員は、モバイルデバイスからデータを収集する際に、法的要件を確実に遵守するためにどのような措置を講じるべきでしょうか？

- A. 互換性や規制遵守を確認せずに、利用可能なフォレンジックツールを何でも使用する。
- B. 調査を迅速化するため、プロセスを文書化せずにモバイルデバイスからデータを収集します。
- C. デバイス所有者から許可を得て、証拠収集プロセスが適用される規制に準拠していることを確認してください。
- D. データ収集中に外部からの干渉を避けるため、デバイスをインターネットから切断しますが、この操作を記録しないでください。

正解: [\(正解を表示します\)](#)

Obtaining proper authorization and ensuring the collection process follows applicable laws and regulations guarantees that the evidence is legally obtained and admissible in court while respecting privacy and ethical standards.

質問: 63

サイバー犯罪インシデントのフォレンジック調査において、捜査官は取得したレジストリファイルから犯罪に関連する証拠を回収する任務を負います。レジストリファイルには、犯罪行為を解明する鍵や値など、重要な証拠が含まれています。これらのデータを適切に分析・抽出するには、詳細かつユーザーフレンドリーな環境でバイナリデータを操作・分析できるツールが必要です。

次のツールのうち、このタスクに最適なものはどれでしょうか？

- A. カムタジア
- B. ルーファス
- C. ダンダス BI
- D. ヘックスワークショップ

正解: [\(正解を表示します\)](#)

This question aligns with CHFI v11 objectives under Operating System Forensics, specifically Windows Registry forensics and binary data analysis. Windows registry hive files (such as SYSTEM, SOFTWARE, SAM, and NTUSER.DAT) are stored in binary format and contain valuable forensic artifacts related to user activity, program execution, persistence mechanisms, and system configuration. CHFI v11 emphasizes that forensic investigators must use tools capable of low-level binary inspection to accurately analyze these files.

Hex Workshop is a professional hex editor designed for detailed examination, interpretation, and manipulation of binary data. It allows investigators to view registry hive files at the hexadecimal level, search for specific byte patterns, validate offsets, and correlate raw binary structures with known registry data formats. This capability is essential when registry files are corrupted, partially deleted, or need manual verification beyond automated tools.

質問: 64

CHFI の専門家が、コンピュータ フォレンジック調査中に AccessData FTK Imager を使用してペンドライブのフォレンジック イメージを作成します。調査員は The Sleuth Kit (TSK) を使用して Linux ディスク イメージ上の ext4 ファイルシステムを調べ、データ改ざんの疑いがあると判断します。専門家は、重要なファイルの inode メタデータを確認することにしました。しかし、inode の詳細に予期しないブロック割り当てがあることに気づきました。疑わしい inode に割り当てられているすべてのディスク ユニットのアドレスを調べるには、調査員はどの TSK コマンドライン ツールと引数を使用すべきでしょうか。

- A. fsstat -f ext4
- B. img_stat -i raw
- C. fls -o imgoffset
- D. 状態 -B 番号

正解: **D** ([コメントを发表する](#))

In TSK, istat displays inode metadata. The -B option shows the list of allocated block addresses associated with that inode. This is exactly what's needed to examine unexpected block allocation patterns and detect tampering.

質問: 65

サイバー犯罪事件発生後、フォレンジック調査員は容疑者のデジタル機器の詳細な調査を行っています。調査員は、市販ソフトウェアに紐づく様々なイメージファイル形式の制約を受けることなく、ディスクイメージを保存・分析する必要があります。こうした制約は、様々な分析プラットフォームでの作業を制限する可能性があります。そこで調査員は、専用ソフトウェアを必要とせず、幅広いフォレンジックツールやプラットフォームから容易にアクセス・分析できる、シンプルで分かりやすく、非圧縮の形式を選択しました。この場合、どのデータ取得形式を使用すべきでしょうか？

- A. デジタル証拠調査で一般的に使用される生の形式を採用します。
- B. 包括的な分析のための高度な機能を提供する AFF4 形式を選択します。
- C. メタデータとディスク イメージを保存するために、高度なフォレンジック形式を採用します。
- D. 特定の商用ソフトウェアと互換性のある独自の形式を使用します。

正解: **A** ([コメントを发表する](#))

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

The RAW format is simple, uncompressed, and transparent, allowing it to be analyzed by nearly all forensic suites such as Autopsy, FTK, EnCase, and The Sleuth Kit. CHFI v11 emphasizes that

RAW images are preferred when long-term accessibility, court admissibility, and tool independence are critical requirements.

質問: 66

以下の法律のうち、企業による不正会計行為の可能性から投資家を保護するために米国議会で可決されたのはどれですか？

- A. 1996年健康保険確率 説明責任法
- B. 2002年連邦情報セキュリティ管理法
- C. グラム・リーチ・ブライリー法
- D. 2002年サーベンス・オクスリー法

正解: ([正解を表示します](#))

質問: 67

フォレンジック専門家のテイラーは、組織のホストサーバーに対するサイバー攻撃の調査を担当しています。サーバーは侵害されており、調査中、テイラーはネットワークトラフィックを分析して攻撃の侵入ポイントを特定する任務を負っています。テイラーはWiresharkを使用してパケットキャプチャファイルを検査し、FTPプロトコルを介したログイン失敗の試行が繰り返される異常なパターンに気づきました。これらの失敗試行に基づいて、テイラーはFTPサービスを標的としたブルートフォース攻撃を疑います。テイラーの次のステップは、これらの失敗の後、攻撃者がFTPサーバーに正常にログインできたかどうかを確認することです。攻撃の成功を確認するために、テイラーはログイン成功を示すFTPサーバーからの特定の応答コードを特定する必要があります。次のWiresharkフィルタのうち、テイラーがFTPログイン試行の成功を確認するのに役立つのはどれですか？

- A. ftp.response.code == 550
- B. ftp.response.code == 530
- C. ftp.response.code == 213
- D. ftp.response.code == 230

正解: D ([コメントを发表する](#))

FTP response code 230 indicates a successful login, confirming that authentication was completed and access to the server was granted.

質問: 68

CHFI の専門家が Windows 10 システムにおけるデータ侵害を調査しています。初期分析の結果、システムイベントログにいくつかの変更が見られました。調査の一環として、専門家はコマンドラインツール「wevtutil」を使用しました。「wevtutil q Security」コマンドを実行しましたが、結果が異常に見えました。この結果の考えられる原因として、次のうちどれが考えられますか？

- A. コマンド「wevtutil q Security」は「wevtutil」コマンドセットに存在しません。
- B. 'wevtutil' コマンドは XML ベースの EVTX ファイル形式からデータを取得できません
- C. イベントログサービスが一時的に応答しないか、ダウンしています
- D. セキュリティログを保存しているEVTXファイルが破損または改ざんされています

正解: **D** ([コメントを發表する](#))

wevtutil gl is a valid command and works with EVTX. If results are abnormal in a context where logs may have been altered, a corrupted or tampered EVTX Security log file is a strong explanation. This fits the scenario's premise of event log manipulation.

質問: **69**

イベント相関とは、最終結果を生み出すイベント間の関連性を見出すプロセスです。組織がサーバー、システム、ルーター、ネットワーク全体にわたるイベントを相関させるには、どのような種類の相関が役立つでしょうか？

- A. 同一プラットフォームの相関関係
- B. ネットワークプラットフォームの相関関係
- C. クロスプラットフォーム相関
- D. マルチプラットフォーム相関

正解: ([正解を表示します](#))

質問: **70**

経験豊富な鑑識捜査官であるエマは、犯罪行為に使用された疑いのある携帯端末に関する事件を担当することになった。その端末はAndroidスマートフォンで、エマは分析のために包括的なデータを抽出する必要がある。捜査の証拠となる可能性のあるシステムレベルのファイルを含め、既存のデータと削除されたデータの両方を復元しなければならない。

エマがデバイスから最も多くのデータにアクセスできる取得方法はどれですか？

- A. クラウドデータ取得
- B. 論理取得
- C. ファイルシステムの取得
- D. 物理的取得

正解: ([正解を表示します](#))

Physical acquisition captures a complete bit-by-bit image of the device's storage, including allocated and unallocated space, enabling recovery of both existing and deleted data as well as system-level files.

質問: **71**

大手多国籍企業のネットワーク管理者であるスミスは、不正アクセスされたコンピュータが犯罪に使用された疑いのある現場に最初に到着した。証拠の保全を維持しながら、彼が最初に取り組むべき対応は何だろうか？

- A. システムを開き、ハードディスクを取り外して固定します
- B. システムの状態を乱すことなくデータ取得を実行する
- C. システムをオフにして、それらを研究室に運びます。
- D. 物理システムとディスプレイの写真を撮影して、システムの状態を記録します。

正解: **D** ([コメントを發表する](#))

質問: 72

データ侵害の疑いのある事件に関するフォレンジック調査において、調査員は、攻撃者が証拠を消去するためにデジタルストレージメディアを意図的に改ざんしたことを発見しました。調査の結果、ストレージデバイス上のアドレス指定可能なすべての場所が任意の文字に置き換えられており、高度なフォレンジックツールを用いても、ドライブに元々保存されていた正当なファイルを復元することは不可能であることが判明しました。

この場合、攻撃者はどのようなフォレンジック対策技術を使用しましたか？

- A. 攻撃者は暗号化を使用してファイルデータを保護し、回復を防止します。
- B. 攻撃者は強力な磁場を使用して、回復可能な痕跡を残さずにファイルデータを消去します。
- C. 攻撃者は、ファイルデータが回復できないようにデバイスを物理的に損傷します。
- D. 攻撃者は、無関係なエントリを使用してファイル内のデータを置き換え、回復を阻止します。

正解: ([正解を表示します](#))

This scenario aligns with CHFI v11 objectives under Anti-Forensics Techniques, specifically data destruction and data wiping methods. The key indicator in the question is that all addressable locations on the storage device have been replaced with arbitrary characters, rendering the original data permanently unrecoverable--even using advanced forensic tools. CHFI v11 explains that this outcome is characteristic of intentional data overwriting, where original data is substituted with meaningless or random values to destroy evidentiary content.

This technique is commonly referred to as data wiping or data substitution, an anti-forensic method designed to defeat file recovery, carving, and residual data analysis. By overwriting every sector of the disk with irrelevant data patterns, the attacker ensures that neither file system metadata nor raw disk analysis can reconstruct the original files.

質問: 73

CHFI(犯罪情報専門家)は、Windowsシステム上で押収されたMicrosoft Edgeブラウザからブラウザ履歴を復元するよう依頼されました。これは、容疑者のオンライン活動を特定するために重要です。容疑者はブラウザ履歴を頻繁に削除していたことが知られています。必要なデータを最も効率的に復元するには、どのツールと手順が最適でしょうか？

A. MZCacheViewツール; パス:

C:\Users\WAppData\Local\Mozilla\Firefox\Profiles\XXXXXXXXX.default\cache2

B. MZHistoryViewツール; パス:

C:\Users\WAppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXXX.default\places.sqlite

C. 閲覧履歴ビューツール; パス: C:\Users\Admin\AppData\Local\Microsoft\Windows\History

D. ブラウジング履歴ビューツール; パス: C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache

正解: D ([コメントを发表する](#))

Microsoft Edge/IE artifacts and related browsing records are commonly stored under the Windows WebCache (ESE database). BrowsingHistoryView can parse these artifacts from the WebCache location, making D the most direct and efficient option for Edge history recovery.

質問: 74

フォレンジックラボの計画と予算編成は、コンピュータフォレンジック調査プロセスのどの段階に属しますか？

- A. 調査段階
- B. 事前調査段階
- C. 調査後段階
- D. 報告フェーズ

正解: **B** ([コメントを發表する](#))

質問: 75

金融機関で大規模なデータ漏洩が発生した後、漏洩の原因と範囲を特定するためにフォレンジック調査員が派遣されました。調査員は調査において法的基準を遵守する必要があります。調査中に、調査員は金融機関が保管していた顧客の非公開個人情報を発見し、この情報が無関係の第三者と違法に共有された疑いがあると判断しました。このシナリオにおいて、調査員が最も重視すべき法律／規制はどれでしょうか？

- A. 1996年医療保険の携行性と説明責任に関する法律
- B. 2014年連邦情報セキュリティ近代化法
- C. 一般データ保護規則
- D. グラム・リーチ・ブライリー法

正解: ([正解を表示します](#))

The Gramm-Leach-Bliley Act (GLBA) governs how financial institutions protect and share customers' non-public personal information (NPI). Suspected improper sharing with non-affiliated third parties squarely triggers GLBA privacy and safeguarding concerns.

質問: 76

デジタルフォレンジックラボでは、ソフトウェアとハードウェアツールの厳格な検証によって精度が確保されています。業界標準の遵守、定期的なメンテナンス、継続的なトレーニングによって、卓越した品質が維持されています。ASCLD/LABやISO/IEC 17025などの認定資格は、ラボの信頼性と信用性を証明しています。

デジタルフォレンジック研究所で精度と信頼性を確保するために重要なことは何ですか？

- A. 定期的な機器メンテナンス
- B. これらすべて
- C. 業界標準への準拠
- D. 継続的な調査員トレーニング

正解: **B** ([コメントを發表する](#))

According to the CHFI v11 Procedures and Methodology domain, ensuring precision and reliability in a digital forensic laboratory requires a holistic approach that integrates multiple best practices rather than relying on a single control. CHFI v11 explicitly emphasizes that forensic accuracy and legal defensibility are achieved only when all critical quality assurance components work together.

Regular equipment maintenance ensures that forensic hardware and software operate correctly and consistently, preventing errors caused by malfunctioning tools. Adherence to industry standards, such as ISO/IEC 17025 and ASCLD/LAB accreditation, establishes validated procedures, standardized workflows, and documented methodologies that courts recognize as trustworthy. These standards ensure repeatability, reproducibility, and credibility of forensic results. Equally important is continuous investigator training, as digital technologies, file systems, operating systems, and attack techniques evolve rapidly. CHFI v11 stresses that investigators must stay current with new tools, emerging threats, and updated forensic methods to avoid analytical errors and misinterpretation of evidence.

CHFI v11 clearly states that the absence of any one of these elements--maintenance, standards compliance, or training--can compromise forensic integrity, lead to inaccurate conclusions, and result in evidence being challenged or rejected in legal proceedings.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 77

調査員がファイルを調べて、潜在的に悪意のあるコンテンツを特定しようとしています。コードの実行を回避しつつ、隠れた侵害の兆候(IOC)を発見するために、調査員はどのような種類の調査を行うべきでしょうか？

- A. 脅威分析
- B. 脅威ハンティング
- C. 動的解析
- D. 静的解析

正解: ([正解を表示します](#))

質問: 78

通話詳細記録(CDR)は、電話サービスで行われた通話に関するメタデータを提供します。次のデータフィールドのうち、CDRに含まれていないものはどれですか。

- A. 着信を受けた電話番号
- B. 通話時間
- C. 通話の言語
- D. レコードを識別する固有のシーケンス番号

正解: ([正解を表示します](#))

質問: 79

当該金融機関の法務チームは、訴訟に対応するため、関連する電子情報(ESI)の収集、処理、審査、および提出を担当する。ESIには、複数のサーバーやデータベースに保存されている膨大な量の財務記録、電子メール、および文書が含まれる。

電子情報開示を効果的に管理し、法的義務を果たすためには、組織は電子情報開示参照モデル(EDRM)サイクルに沿った包括的な戦略を採用する必要があります。

- A. eDiscovery のレビューと作成段階を迅速化するために、メタデータの保存を省略して、ESI の迅速な収集を優先します。
- B. データ管理と法務サービスを提供するベンダーにeDiscoveryをアウトソーシングし、EDRMサイクルのコンプライアンスを外部に移行します。
- C. 主要な保管者とデータソースを特定するために、早期ケース評価 (ECA) を実施し、集中的な収集と電子情報開示の効率化を可能にします。
- D. 厳格なデータ保持ポリシーを適用して、発見可能なESIの量を削減し、eDiscoveryとリソースの必要性を簡素化します。

正解: ([正解を表示します](#))

Early Case Assessment identifies key custodians and relevant data sources at the outset, allowing targeted collection and efficient processing in line with the EDRM, reducing scope and cost while maintaining compliance.

質問: 80

高度なデジタルフォレンジック専門家であるジェームズは、オンライン犯罪事件の捜査に取り組んでいる。容疑者は、侵害されたデバイスのネットワークを通じて不正行為を行ったとみられている。証拠はデジタルデータであり、ログ、メタデータ、システム/アプリケーションのタイムスタンプなど、さまざまなシステムにわたる複雑なデータネットワークが残されている。ジェームズは、容疑者のデバイスからメタデータを収集し、システム/アプリケーションのログを精査し、犯罪が行われたとみられる時間帯に発生したファイルや操作のタイムスタンプを分析することに捜査の焦点を絞っている。

ジェームズはデジタル上の痕跡を精査しながら、容疑者と犯罪を直接結びつけるデータ、あるいは発生した出来事を裏付ける証拠となるデータを探し出そうとしている。彼は、メタデータやログからファイルへのアクセス、文書の作成、アプリケーションの使用、ネットワーク活動といった行動が明らかになり、これらが容疑者の行動の時系列を解明するのに役立つことを理解している。この証拠は捜査においてどのような役割を果たすのだろうか？

- A. 無罪を証明する証拠
- B. 裏付けとなる証拠
- C. 容疑者の行動の証拠
- D. 本人確認

正解: ([正解を表示します](#))

Metadata, logs, and timestamps are used to support and validate events by reconstructing activity timelines. This type of evidence strengthens and confirms other findings in the investigation, serving to substantiate what occurred rather than independently proving the entire case.

質問: 81

マークは政府機関でサイバーフォレンジック調査官として働いている。彼はハードドライブからデータを復元する任務を与えられた。ハードドライブのパーティションは、不正行為を隠蔽するために不満を抱いた従業員によって削除されていた。マークはデータを復元するためにどのツールを使用すべきか？

- A. ディスクビュー
- B. EFSDump
- C. ディスクモン
- D. R-Studio

正解: **D** ([コメントを發表する](#))

質問: 82

以下のものを、変動性の高い順から低い順に並べなさい。

- A. レジスタとキャッシュ、ルーティングテーブル、一時ファイルシステム、ディスクストレージ、アーカイブメディア
- B. レジスタとキャッシュ、ルーティングテーブル、一時ファイルシステム、アーカイブメディア、ディスクストレージ
- C. レジスタとキャッシュ、一時ファイルシステム、ルーティングテーブル、ディスクストレージ、アーカイブメディア
- D. アーカイブメディア、一時ファイルシステム、ディスクストレージ、アーカイブメディア、レジスタおよびキャッシュ

正解: ([正解を表示します](#))

質問: 83

デジタルフォレンジック調査官のリアムは、Linuxベースのシステムを標的としたサイバー攻撃の証拠を調べている。システムを分析する中で、彼はいくつかのファイルが欠落していることに気づく。

さらに詳しく調べた結果、攻撃時に実行されていた特定の実行ファイルが自身の内容を消去しており、復旧がより困難になっていることが判明した。失われたファイルを復旧するには、リアムはLinux上でファイルを取得するのに役立つ適切なコマンドを特定する必要がある。

LiamはLinuxシステム上で失われたファイルを復元するために、以下のどのコマンドを使用すべきでしょうか？

- A. `cd C:\RECYCLER\S-<ユーザーSID>`
- B. `D<#>`。
- C. `cp /proc/$PID/exe /tmp/file`
- D. `$R<#>`。

正解: ([正解を表示します](#))

According to the CHFI v11 objectives under Operating System Forensics, Linux Memory and Process Analysis, and Anti-Forensics Techniques, attackers sometimes use a technique where a malicious executable deletes or overwrites itself after execution to evade detection. Although the file may be erased from disk, if the process is still running, Linux maintains a reference to the executable in memory through the /proc filesystem.

Each running process in Linux has a directory under /proc/<PID>/, and the symbolic link /proc/<PID>/exe points to the executable image currently loaded into memory. By copying this link using the command:

```
cp /proc/$PID/exe /tmp/file
```

an investigator can successfully recover the in-memory version of the executable, even if it has been deleted from disk. This is a well-documented forensic technique in CHFI v11 for recovering malware binaries and analyzing fileless or self-deleting malware.

質問: 84

法医学捜査官のサラは、侵害された疑いのあるmacOSデバイスの調査を行っています。彼女の任務は、システムへの不正アクセスに関する証拠を収集することです。調査の一環として、システムにアクセスした日時と人物に関する情報を見つける必要があります。サラは、一般的なシステムログを確認するだけでなく、不正アクセスに関する詳細なデータを提供する可能性のある特定の種類のシステムファイルにも注目する必要があることを認識しています。macOSファイルシステムのどの領域が、ログオン試行やその他の認証イベントに関する最も関連性の高い情報を提供するのでしょうか？

- A. ユーザーアカウントデータ
- B. サファリの歴史
- C. ホームフォルダ
- D. LaunchDaemonsディレクトリ

正解: ([正解を表示します](#))

User account data on macOS contains records related to logins, authentication attempts, and user activity, making it the most relevant source for identifying unauthorized access events.

質問: 85

あなたは地方銀行のインシデント対応マネージャーです。Webアプリケーションログの定期監査を実施中に、以下の文字列を含むログイン試行が複数見つかりました。

```
< SCRIPT type="text/javascript">
```

```
var adr = '../evil.php?cakemonster=' + escape(document.cookie);
```

```
</SCRIPT>
```

どのような攻撃が発生したのですか？

- A. クロスサイトリクエストフォージェリ
- B. バッファオーバーフロー
- C. クロスサイトスクリプティング

D. SQLインジェクション

正解: C ([コメントを发表する](#))

質問: 86

ある国際機関が、機密性の高い顧客データを含むデータベースへの重大な侵害被害に遭った。その後、同機関は外部のフォレンジック調査員を雇うことを決定した。

しかし、同社の取締役会は、外部調査員の選定基準に異議を唱えている。

彼らはあなたに助言を求めています。漏洩したデータの機密性の高さと攻撃の規模を考慮すると、外部のフォレンジック調査員を雇う際に考慮すべき重要な要素は何でしょうか？

- A. 業界における評判。
- B. 会社の内部システムに関する知識。
- C. 類似の事例への対応経験。
- D. 法医学における専門倫理規定の遵守。

正解: C ([コメントを发表する](#))

Experience with similar large-scale breaches ensures the investigator understands the complexity, methodologies, and challenges involved, enabling effective handling of the incident and reliable evidence collection.

質問: 87

あなたは鑑識研究所の建設を依頼され、上司から壁、天井、床の内張りに銅を使用するように指示されました。壁、天井、床を銅で覆う主な目的は何ですか？

- A. 室温を調節するため
- B. 実験室を防音にする
- C. 電磁波の放出を避けるため
- D. 壁、天井、床を補強する

正解: B ([コメントを发表する](#))

質問: 88

デジタルフォレンジック調査員が、企業のサーバーから機密性の高い知的財産が盗難された企業スパイの疑いのある事件を調査しています。ENFSIの「デジタル技術のフォレンジック調査に関するベストプラクティス」に則り、調査員の主な懸念事項は何でしょうか？

- A. GDPR データ プライバシー ルールに準拠しています。
- B. 法医学研究所における ISO/IEC 17025 標準に準拠。
- C. 安全な証拠処理プロトコルを確立する。
- D. 情報セキュリティのための ISO/IEC 27001 を実装します。

正解: C ([コメントを发表する](#))

This question maps directly to CHFI v11 objectives under Computer Forensics Fundamentals and Standards and Best Practices Related to Computer Forensics, specifically the ENFSI Best Practices for the Forensic Examination of Digital Technology. ENFSI (European Network of Forensic Science Institutes) guidelines focus primarily on ensuring that digital evidence is handled

in a secure, reliable, and forensically sound manner so that it remains admissible and defensible in legal proceedings.

The examiner's primary concern under ENFSI best practices is the secure handling of digital evidence, which includes proper acquisition, preservation, documentation, storage, and chain of custody management. These practices ensure evidence integrity, prevent contamination or alteration, and allow results to be independently verified. CHFI v11 emphasizes that forensic investigators must be able to demonstrate that evidence has not been tampered with and that standardized procedures were followed throughout the investigation lifecycle.

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

質問: 89

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

正解: ([正解を表示します](#))

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.

質問: 90

あなたは、最近証拠として押収されたハードドライブを分析している鑑識捜査官です。ファイルシステム内で有意義な証拠を見つけることができず、ドライブ消去ユーティリティが使用された可能性があると疑っています。Windowsレジストリのソフトウェアハイブ内のキーを確認しましたが、

ドライブ消去ユーティリティは見つかりませんでした。ハードドライブにドライブ消去ソフトウェアが使用されたことをどのように確認できますか？

- A. インストールされているプログラムの一覧を確認してください
- B. ハードドライブ上のビットレベルで明確な繰り返しパターンを探します
- C. ドライブ消去ユーティリティが使用された疑いがあるが、証拠は見つからなかったことを報告書に記載してください。
- D. 各種ドライブ消去ユーティリティをオフラインでロードし、過去の実行レポートをエクスポートする

正解: ([正解を表示します](#))

質問: 91

起動プロセス後の悪意のあるプログラムの影響を理解し、ディスクパーティションから最新の情報を収集するために、調査担当者は次の内容を評価する必要があります。

- A. UEFI
- B. BIOS
- C. MBR
- D. GRUB

正解: C ([コメントを発表する](#))

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格すること
に役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供しま
す。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題
集のテストエンジンを手に入れます。最新版のアクセ
ス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637**問、**30%**ディスカウント、
特別な割引コード: **JPNshiken**」

質問: 92

鑑識捜査官のソフィアは、重大な企業データ窃盗事件を担当している。容疑者はIT部門の従業員で、突然退職する前に数百もの機密ファイルをノートパソコンにダウンロードしたとされる。ソフィアは搜索差押令状を取得し、執行中に容疑者のノートパソコン、デスクトップパソコン、および複数の記憶装置を発見した。証拠の保管管理の連鎖を維持し、ACPO(米国検察庁)のデジタル証拠に関する原則を遵守するために、ソフィアは次にどのような行動をとるべきだろうか？

- A. 彼女は直ちに現場でデジタル機器の分析を開始すべきです。
- B. 捜査を迅速化するために、容疑者にデバイスのパスワードを尋ねるべきです。
- C. 彼女は令状に記載されている情報に従って、個人のノートパソコンのみを押収すべきです。
- D. 彼女は全ての機器を押収し、分析のために鑑識研究所に送るべきです。

正解: ([正解を表示します](#))

Following proper forensic procedures and ACPO principles, all relevant devices should be seized, documented, and transported to a controlled forensic lab environment for analysis. This ensures evidence integrity, proper handling, and maintenance of the chain of custody.

質問: 93

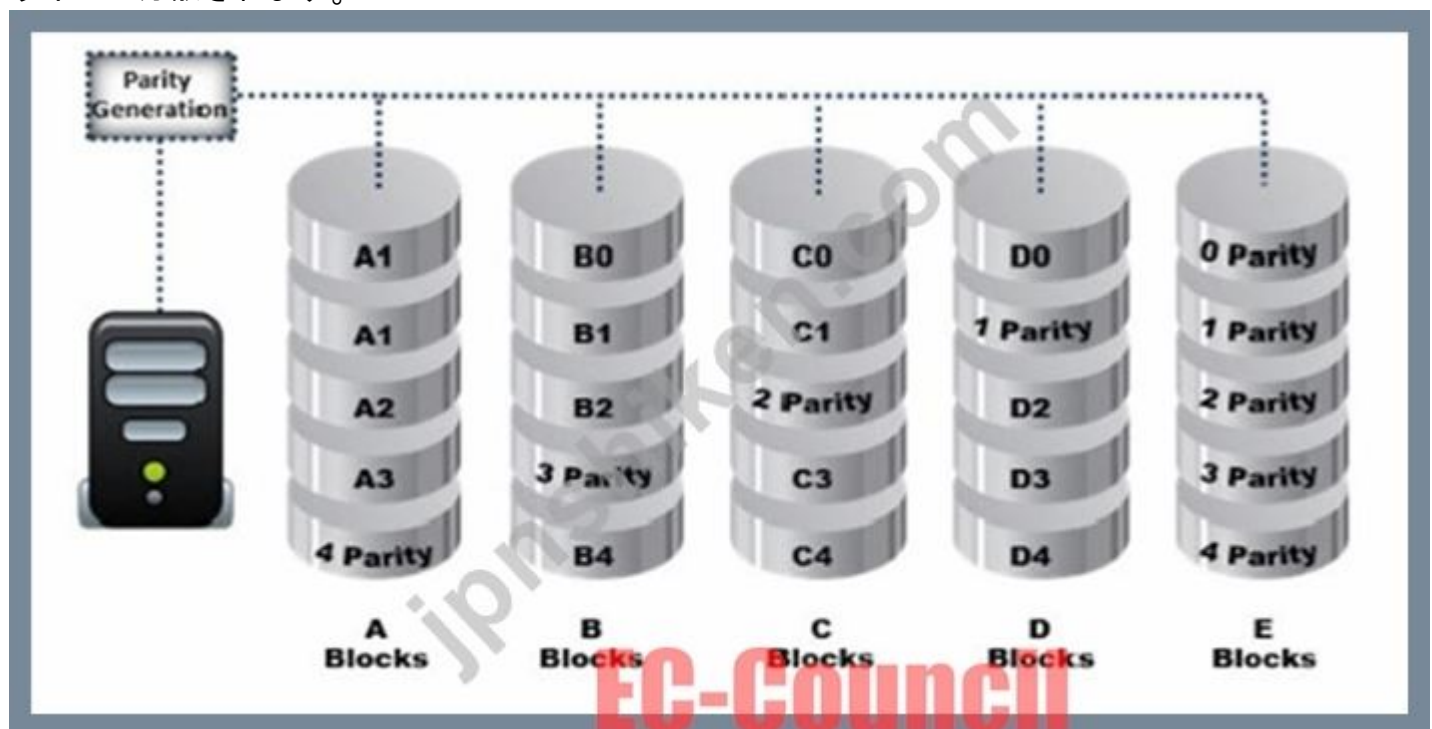
マリアは管理された環境で疑わしい実行可能ファイルを実行し、Windows イベント ビューアーを使用して、実行後にそのファイルがレジストリ値を追加または変更するかどうかを確認したいと考えています。このシナリオでは、彼女は次のうちのイベント ID を探すべきでしょうか？

- A. イベントID 4657
- B. イベントID 7040
- C. イベントID 4688
- D. イベントID 4624

正解: ([正解を表示します](#))

質問: 94

データはバイト単位で複数のドライブにストライピングされ、パリティ情報はすべてのメンバードライブに分散されます。



これはどのRAIDレベルを表していますか？

- A. RAIDレベル1
- B. RAIDレベル5
- C. RAIDレベル3
- D. RAIDレベル0

正解: ([正解を表示します](#))

質問: 95

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

正解: ([正解を表示します](#))

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.

質問: 96

フォレンジック専門家のルーカス氏は、被害者のシステムから取得したメモリダンプからTorブラウザに関連するアーティファクトを抽出していました。調査中、彼はフォレンジックツールを使用して関連情報を抽出し、ダンプに含まれる証拠となるアーティファクトの数が最も少ないことに気づきました。彼の観察に基づく、メモリダンプで発見されるアーティファクトの数が最も少なかったのは、以下のどの条件でしたか？

- A. Torブラウザが開きました
- B. Torブラウザがアンインストールされました
- C. Torブラウザが閉じられました
- D. Torブラウザがインストールされています

正解: ([正解を表示します](#))

In CHFI v11, memory dump analysis focuses on identifying volatile artifacts, such as running processes, loaded modules, decrypted data, network connections, and application-specific memory remnants. The availability of Tor Browser artifacts in memory is highly dependent on the execution and installation state of the Tor Browser at the time of acquisition.

When the Tor Browser is opened, it generates the highest number of artifacts in memory. These include active Tor processes, circuit information, encryption keys, temporary buffers, and cached session data. Even when the Tor Browser is closed but still installed, some residual artifacts may remain in memory or be partially recoverable due to delayed memory reuse, along with indirect indicators such as prefetch references and previously allocated memory pages.

However, when the Tor Browser is uninstalled, there are no active Tor-related processes or associated memory segments loaded into RAM. As explicitly covered in the CHFI v11 blueprint under Tor Browser Forensics and Forensic Analysis: Tor Browser Uninstalled, uninstalling Tor significantly reduces both volatile and non-volatile artifacts. Consequently, memory dumps acquired after uninstallation contain the least possible number of recoverable Tor artifacts, often limited to overwritten or non-attributable memory fragments.

質問: 97

デジタル捜査中に、容疑者がクラウドストレージプラットフォームに証拠となるデータを保存していた可能性を示唆する証拠が見つかりました。捜査チームは、クラウドストレージサービスのログとメタデータにアクセスしました。クラウドストレージフォレンジックにおいて、ログとメタデータは捜査プロセスにおいてどのような役割を果たすのでしょうか？

- A. 保存されたデータに使用される暗号化アルゴリズムを決定します。
- B. 容疑者の物理的な位置に関する洞察を提供します。
- C. クラウドストレージにアクセスするために使用されるデバイスの種類を識別するのに役立ちます。
- D. ユーザー認証とアクセス アクティビティに関する詳細を提供します。

正解: **D** ([コメントを发表する](#))

According to the CHFI v11 Cloud Forensics objectives, logs and metadata are among the most critical sources of digital evidence in cloud-based investigations. Unlike traditional on-premises systems, investigators often do not have direct access to physical storage in cloud environments. As a result, service-provider-generated logs and metadata become primary evidence artifacts. Cloud service logs typically record user authentication events, including login timestamps, user IDs, authentication methods (such as passwords or MFA), IP addresses, session durations, and access outcomes (success or failure). Metadata associated with cloud storage objects further provides information such as file creation time, modification time, access time, ownership details, sharing activity, and access permissions. Together, these artifacts allow investigators to reconstruct who accessed the cloud data, when it was accessed, and what actions were performed, which is essential for attribution and timeline analysis.

While logs and metadata may sometimes indirectly hint at device or location information, CHFI v11 emphasizes their primary forensic value as evidence of authentication and access activity, not

encryption algorithms or physical whereabouts. Encryption mechanisms are typically abstracted and managed by the cloud provider, and determining physical location is not a reliable or guaranteed outcome of log analysis.

Therefore, in cloud storage forensics, logs and metadata are chiefly used to analyze user authentication and access behavior, making Option D the correct and CHFI-verified answer.

質問: 98

あなたは、大規模なサイバー攻撃が発生した大企業のフォレンジックアナリストです。調査の結果、攻撃の発生源と疑われるLinuxベースのシステムのイメージが見つかりました。あなたの任務は、Windowsフォレンジックワークステーションでこのイメージを分析することです。イメージは破損しているように見えますが、重要な証拠が含まれています。イメージの閲覧プロセスによって、これ以上の損害が発生しないようにする必要があります。これを実現するための最も効果的なツールまたは方法は何ですか？

- A. 画像をWindows互換フォーマットに変換します。
- B. Windows上でLinuxイメージを表示するために設計された専用のフォレンジックツールを導入する。
- C. Linuxエミュレータを使用して画像を表示します。
- D. ライブブートディスクを使用してイメージを表示します。

正解: ([正解を表示します](#))

A specialized forensic tool designed to handle Linux file systems on a Windows workstation allows safe, read-only access to the image. This preserves evidence integrity and prevents further corruption while enabling proper analysis.

質問: 99

複雑なサイバー犯罪捜査において、フォレンジック専門家は、使用可能なファイルシステムのメタデータが欠落した、深刻に断片化されたハードドライブに遭遇しました。高度なファイルカービング技術を駆使することで、ファイル拡張子を意図的に操作してデータを難読化した容疑者によって隠されていた重要な証拠を復元することに成功しました。

ファイルシステムのメタデータが欠落している断片化されたハードドライブから隠しファイルを復元するために、法医学調査員はどのような高度な方法を採用するのでしょうか？

- A. ファイル システム アーキテクチャを最初から再構築します。
- B. 高度なアルゴリズムを使用して暗号化されたファイルを復号化します。
- C. ファームウェア レベルのアクセスを使用して、アクセスできないセクターからファイルを抽出します。
- D. 未割り当て領域内のファイル署名とパターンを分析しています。

正解: D ([コメントを发表する](#))

According to the CHFI v11 Anti-Forensics Techniques and Digital Evidence Analysis objectives, attackers often attempt to evade detection by deleting files, corrupting file system metadata, fragmenting data, or manipulating file extensions. When file system structures such as the MFT,

FAT, or directory entries are missing or damaged, traditional file recovery methods fail. In such scenarios, investigators rely on file carving.

File carving is an advanced forensic technique that recovers files based on file signatures (headers and footers) and content patterns, rather than file system metadata. CHFI v11 explains that file carving scans unallocated space, slack space, and raw disk sectors to identify known byte patterns associated with specific file types (for example, JPEG headers FFD8FFE0 or PDF headers %PDF). This allows investigators to recover files even when filenames, extensions, and directory information have been intentionally altered or destroyed.

質問: 100

捜査官はSAMとシステムファイルからパスワードを抽出したいと考えています。この場合、捜査官はどのツールを使用して、ユーザー、パスワード、およびそれらのハッシュのリストを取得できますか？

- A. PWdump7
- B. ファイルマーリン
- C. ハッシュキー
- D. Nuix

正解: ([正解を表示します](#))

質問: 101

最近、ある政府機関が利用している内部ウェブアプリが応答しなくなった。

政府機関のネットワークエンジニアであるベティは、Webアプリケーションが応答しなくなった原因を突き止めるよう指示された。ベティはWiresharkを起動し、ローカルネットワーク上のトラフィックのキャプチャを開始した。結果を分析しているうちに、ベティはSYNフラッド攻撃が行われていることに気づいた。ベティはどのようにしてSYNフラッド攻撃が発生していることを知ったのだろうか？

- A. Wiresharkキャプチャでは、単一または複数のIPアドレスからの複数のSYNリクエストとRSTレスポンスが表示されます。
- B. Wiresharkのキャプチャでは異常は見られず、問題はWebアプリケーションに関連しています。
- C. Wiresharkキャプチャでは、単一または複数のIPアドレスからの複数のSYNリクエストとACKレスポンスが表示されます。
- D. Wiresharkキャプチャでは、単一または複数のIPアドレスからの複数のACK要求とSYN応答が確認できます。

正解: ([正解を表示します](#))

質問: 102

ジェーンは、一流のサイバーセキュリティ企業に勤務するフォレンジック調査員です。データ漏洩の可能性に関連する証拠を探すため、容疑者のコンピューターを分析していたところ、改ざんされたと思われるログファイルを発見しました。ファイルのタイムスタンプが変更されており、ファイ

ルの一部が意図的に削除されているようです。ジェーンは、デジタル証拠の保全と真正性を確保するために、まず何をすべきでしょうか？

- A. 彼女はログファイルの削除された部分を復元しようと試みるべきです
- B. 彼女はハードドライブのビットストリームイメージコピーを作成する必要がある
- C. 彼女は改ざんに注意しながら分析を続けるべきである
- D. 彼女は直ちに上司に連絡し、改ざんされたログファイルを提示すべきである

正解: ([正解を表示します](#))

The first priority in any digital forensic investigation is evidence preservation. Creating a bit-stream (forensic) image of the hard drive captures an exact sector-by-sector copy of the entire storage media, including active data, deleted data, slack space, and unallocated space.

質問: 103

一連の動作や出来事の後、システムや機械に生じた変化を調査するプロセスを何と呼びますか？

- A. Windowsサービス監視
- B. システムベースライン設定
- C. スタートアッププログラムのモニタリング
- D. ホスト整合性監視

正解: ([正解を表示します](#))

Host integrity monitoring is the process of studying the changes that have taken place across a system after a series of actions or incidents. Involves monitoring ports, processes, registry, event logs, etc.

質問: 104

企業の重要なデータを保存していたEC2インスタンスがマルウェアに感染しました。フォレンジックチームは、さらなる分析を行うために、感染したインスタンスのEBSボリュームのスナップショットを取得し、証拠価値のあるその他のデータを収集しました。彼らは次にどのような行動をとるべきでしょうか？

- A. 重要なデータが保存されているため、インスタンスは実行状態を維持する必要があります。
- B. 実行中のインスタンスを一時停止する必要があります
- C. 同じVPC経由で接続されているすべてのインスタンスを終了する必要があります
- D. 必要なバックアップを取得した後、インスタンスを終了する必要があります。

正解: ([正解を表示します](#))

質問: 105

デジタルフォレンジック調査中に、Android OSを搭載したモバイルデバイスが容疑者から押収されました。調査の結果、WindowsとLinuxの両方のシステムとのやり取りを示すファイルが見つかりました。AndroidとiOSのフォレンジック分析において、WindowsとLinuxのシステムに関連するファイルを調査する際に重要なステップは次のうちどれですか？

- A. ファイルを分析して、異なるオペレーティングシステム間での相互作用と潜在的な証拠を特定します。

- B. モバイルデバイスにネイティブなファイルのみに焦点を当てる
- C. Android および iOS ファイルからのみデータを抽出する
- D. WindowsおよびLinuxに関連するファイルを無視します

正解: ([正解を表示します](#))

According to the CHFI v11 objectives under Mobile and IoT Forensics and Operating System Forensics, mobile devices often act as cross-platform interaction points, storing artifacts related to communications, file transfers, backups, or synchronization with Windows and Linux systems. These artifacts may include shared documents, SSH keys, SMB access traces, USB connection records, cloud sync remnants, or application logs indicating interaction with external operating systems.

A crucial forensic step in such cases is analyzing files to identify interactions and potential evidence across different operating systems. This enables investigators to reconstruct user activity beyond the mobile device itself and establish links between the mobile device and other systems involved in the incident. CHFI v11 emphasizes the importance of correlating evidence across heterogeneous platforms to build a complete and accurate timeline of events.

質問: 106

デジタルフォレンジック調査において、侵入されたシステム上で、何度も削除を試みたものの、永続的なマルウェアが発見されました。マルウェアはシステムの再起動時に再インストールされ、高度な永続化メカニズムが存在していることが示唆されています。

デジタルフォレンジックにおいて、マルウェアの持続性を特定することが重要なのはなぜですか？

- A. 将来の感染を防ぎ、システムの長期的なセキュリティを確保するため
- B. システムパフォーマンスを向上させるため
- C. マルウェアの地理的起源を特定する
- D. ネットワーク帯域幅を最適化し、遅延を減らす

正解: ([正解を表示します](#))

This question maps directly to CHFI v11 objectives under Malware Forensics, specifically malware persistence mechanisms and behavior analysis. Persistent malware is designed to survive system reboots and removal attempts by embedding itself into startup locations, registry keys, scheduled tasks, services, boot sectors, or firmware. CHFI v11 emphasizes that identifying persistence mechanisms is a critical step in malware analysis and incident response.

From a forensic perspective, understanding how malware maintains persistence allows investigators to fully eradicate the threat and prevent reinfection. If persistence artifacts are not identified and removed, the malware can continuously reinstall itself, rendering cleanup efforts ineffective and allowing attackers to maintain long-term access. CHFI v11 highlights registry-based persistence, startup folders, services, cron jobs, launch agents, and boot-level persistence as common techniques that must be analyzed.

Additionally, identifying persistence helps investigators reconstruct the attack timeline, understand attacker intent, and determine the scope of compromise.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 107

iOSデバイスのフォレンジック調査中に、様々なアプリケーションやシステムサービスの位置情報データを取得する任務を負っています。デバイスを調査した結果、いくつかのファイルが見つかりました。iOSデバイス上のアプリケーションやシステムサービスの位置情報データが含まれているファイルはどれですか？

- A. Cookies.plist
- B. Sms.db
- C. ドラフトメッセージ.plist
- D. クライアント.plist

正解: ([正解を表示します](#))

According to the CHFI v11 Mobile and IoT Forensics objectives, iOS devices maintain geolocation-related artifacts through the location services subsystem (locationd). One of the key forensic artifacts associated with this subsystem is Clients.plist.

The Clients.plist file stores information about applications and system services that have requested or used location services. It contains identifiers for apps, service names, permission states, and timestamps indicating when location data was accessed. This makes it highly valuable for investigators attempting to determine which apps accessed location data and when, which is crucial in cases involving surveillance, stalking, fraud, or physical movement reconstruction.

The other files listed do not store geolocation data. Cookies.plist contains browser cookie information, Sms.db stores SMS and iMessage content, and DraftMessage.plist holds unsent message drafts. None of these files are related to GPS or location services.

CHFI v11 emphasizes correlating Clients.plist with other artifacts such as location caches, application logs, and timestamps to reconstruct user movement and application behavior on iOS devices.

質問: 108

法医学捜査官のエブリンは、悪意のある活動が行われている疑いのあるLinuxマシンを分析する任務を負っています。彼女は開いているファイルを調べ、それらのファイルに関連付けられているプロセスを特定する必要があります。エブリンは、RAMイメージから開いているファイルとその関連プロセスを一覧表示するために、どのVolatility Frameworkプラグインを使用すべきでしょうか？

- A. linux.pslist

- B. linux.mount
- C. linux.lsof
- D. linux.malfind

正解: ([正解を表示します](#))

Volatility provides the linux.lsof plugin, which lists open files and maps them to the processes that have them open, enabling correlation between files and running processes in a memory image.

質問: 109

次のうち、ウェブサイトから送信され、ユーザーのウェブブラウザによってユーザーのコンピュータに保存され、特定のユーザー情報を追跡、検証、維持するために使用される小さなデータはどれですか？

- A. 一時ファイル
- B. クッキー
- C. ウェブブラウザのキャッシュ
- D. ファイルを開く

正解: ([正解を表示します](#))

質問: 110

デジタル証拠が、その正確性と信頼性を確保する方法で収集、保存、調査、または転送されることを保証するために、法執行機関および鑑識機関は、効果的な品質システムを確立し、維持しなければならない」は、以下の機関によって確立された原則である。

- A. NIST
- B. NCIS
- C. 提案
- D. EC評議会

正解: ([正解を表示します](#))

質問: 111

独裁国家のユーザーがTorネットワークにアクセスしようとしませんが、厳しいインターネット検閲に直面します。ブリッジノードを利用することで、ユーザーの接続は偽装され、制限を回避できます。ブリッジノードは公開Torディレクトリに登録されていないため、ISPや政府によるTorトラフィックの特定とブロックが困難になります。

ブリッジノードは、検閲にもかかわらずユーザーがTorネットワークにアクセスできるようにどのように支援しますか？

- A. ユーザーデータを複数回暗号化することで
- B. 匿名でウェブサイトをホストすることで
- C. IPアドレスを偽装することで
- D. 住所を公開することで

正解: C ([コメントを发表する](#))

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.

質問: 112

サイバーフォレンジック調査官のエミリーは、スマートフォンの証拠に関する事件の調査を依頼されました。対象となるデバイスはAndroidとiOSのスマートフォンです。エミリーは、両方のデバイスで論理的なデータ取得を実行して証拠を収集することにしました。提示された選択肢の中から、AndroidとiOSの両方のデバイスで徹底的な論理的データ取得を実行できるツールはどれでしょうか？

- A. iPhoneバックアップ抽出ツール
- B. UFED Cellebrite
- C. FTKイメージャー
- D. ADB (Android Debug Bridge)

正解: **B** ([コメントを發表する](#))

UFED Cellebrite supports logical acquisition across both Android and iOS devices, enabling comprehensive extraction of user data in a forensically sound manner.

質問: 113

ある注目度の高いサイバー犯罪事件の捜査において、法執行機関は専門的なコンピュータフォレンジック捜査官の必要性を認識した。所属する通常のフォレンジック捜査官は、コンピュータフォレンジック特有の要求に対応するのに苦労していた。外部のフォレンジック捜査官を雇うことも検討したが、予算上の制約から断念した。この窮状に対する潜在的な解決策は何だろうか？

- A. 現在の捜査官にコンピュータフォレンジックの研修を実施する。
- B. 調査を民間企業に委託する。
- C. 現在の捜査官を支援するために、高度な鑑識ツールに投資する。

D. 国際的な法執行機関と協力して支援を要請する。

正解: ([正解を表示します](#))

Training existing investigators in computer forensics builds in-house expertise, enabling them to handle specialized digital investigations effectively without incurring the higher costs of outsourcing.

質問: 114

法医学アナリストのフランクは、Linuxサーバーに関する事件を担当している。サーバーは侵害されており、フランクは攻撃者が活動の痕跡を隠すためにファイルシステムを操作したと疑っている。彼はLinuxシステム上で詳細なファイルシステム分析が可能なツールを必要としている。フランクはこの作業にどのツールを使用すべきか？

- A. 解剖
- B. 削除解除
- C. ディスクエクスプローラー
- D. 探偵キット

正解: ([正解を表示します](#))

The Sleuth Kit provides comprehensive file system analysis capabilities for Linux systems, allowing investigators to examine disk images, recover deleted files, and uncover hidden artifacts.

質問: 115

スミスは、鑑識捜査の一環として、携帯端末を押収した。彼は携帯端末内の加入者識別モジュール(SIMカード)データを復元するよう依頼された。スミスは、SIMカードが個人識別番号(PIN)コードで保護されていることを発見したが、人々は通常PIN番号をデフォルトのままにするか、簡単に推測できる番号を使用していることも知っていた。

1234. 彼は3回試行しましたが失敗し、SIMカードがロックされてしまいました。このような状況で、ジェイソンはPINをリセットしてSIMデータにアクセスするために何ができるでしょうか？

- A. 24時間後にPIN推測を試みることができます
- B. 彼はネットワーク事業者に連絡して、一時ロック解除コード(TUK)を入手する必要があります。
- C. システムおよびハードウェアツールを使用してアクセスします
- D. 彼はネットワーク事業者に連絡して個人ロック解除番号(PUK)を入手する必要があります

正解: ([正解を表示します](#))

質問: 116

ログを分析する際には、すべてのネットワーク機器の時計が同期していることが重要です。これらの時計を同期させるには、どのプロトコルが役立ちますか？

- A. NTP
- B. PTP
- C. UTC
- D. UCT

正解: ([正解を表示します](#))

質問: 117

重大なマルウェア調査中に、チームは侵害されたサーバー上で不審なデバイスドライバを発見しました。サンドボックス環境でドライバの動作を分析したところ、正規のドライバでは通常必要とされない低レベルのシステムリソースに頻繁にアクセスしていることがわかりました。このドライバがルートキットとして使用されている可能性があると考えられます。ルートキットは検出を回避するためにどのような手法を用いていると考えられますか？

- A. 正当なシステムプロセスでそのプロセスを隠蔽している可能性があります。
- B. ゼロデイ脆弱性を利用している可能性があります。
- C. 正規のドライバーにフックしている可能性があります。
- D. カーネルパッチを使用している可能性があります。

正解: ([正解を表示します](#))

Kernel patching allows a rootkit to modify core operating system functions at the kernel level, enabling it to hide processes, files, and activities from detection by security tools.

質問: 118

あなたはデジタルフォレンジック調査員で、ビットマップ画像ファイル(BMP)を分析し、その構造と内容に関する情報を収集する任務を負っています。徹底的な分析を行うには、ファイル構造とデータコンポーネントを理解することが不可欠です。ビットマップ画像ファイルのどのコンポーネントに、ファイルの種類、サイズ、レイアウトに関するデータが含まれていますか？

- A. ファイルヘッダー
- B. 画像データ
- C. 情報ヘッダー
- D. RGBQUAD配列

正解: ([正解を表示します](#))

The BMP file begins with a file header (BITMAPFILEHEADER), which contains the signature identifying the file type, the overall file size, and the offset to the image data.

質問: 119

次のうち、企業による不正会計行為の可能性から投資家を保護するために、2002年に米国議会で可決された法律はどれですか？

- A. GLBA
- B. SOX
- C. FISMA
- D. HIPAA

正解: ([正解を表示します](#))

質問: 120

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

正解: **D** ([コメントを發表する](#))

The described step involves verifying the integrity of the bootloader using cryptographic checks and enforcing trusted boot policies. This corresponds to the Security phase of the UEFI process, where Secure Boot ensures that only trusted and signed components are allowed to load, maintaining a secure boot state.

質問: 121

コンピュータフォレンジック調査官またはフォレンジックアナリストは、法執行機関や民間企業と協力してコンピュータやその他のデータストレージデバイスから情報を取得する、特別に訓練された専門家です。そのためには、アナリストはコンピュータのあらゆる側面について優れた実務知識を持っている必要があります。犯罪捜査中にアナリストの職務ではないものは次のうちどれですか？

- A. 疑わしいデバイスからデータを復元する
- B. 現場における全てのデバイスとソフトウェアのセキュリティを強化する
- C. 調査報告書を作成する
- D. 保管記録を記入する

正解: ([正解を表示します](#))

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637問、30%ディスカウント、特別な割引コード: **JPNshiken****」

質問: 122

コンピュータフォレンジック調査において、調査官は最近シャットダウンされたシステムを扱っています。必要なデータは不揮発性です。このような状況で、調査官はどのようなデータ取得方法を採用すべきでしょうか？また、その理由は？

- A. システムは既に電源が切れているため、調査者はデータ取得を行わないでください。

B. 調査担当者は、ライブデータ取得とデッドデータ取得のどちらの方法もシステムから不揮発性データを収集できるため、ライブデータ取得とデッドデータ取得のどちらかを使用する必要があります。

C. 調査者は、コンピュータのメモリ、キャッシュ、レジストリから動的なデータを取得することを目的としたライブデータ取得を使用する必要があります。

D. 調査員はデッドデータ取得を使用すべきである。なぜなら、これはハードドライブやUSBメモリなどのストレージデバイスから改変されていないデータを収集するように設計されているからである。

正解: ([正解を表示します](#))

Since the system is shut down and the required data is non-volatile (on storage), dead acquisition is appropriate. It minimizes changes to the target media and is designed to collect data from disks/USBs in a controlled manner (typically via imaging with write blockers).

質問: 123

調査中に、フォレンジックアナリストは、送信ネットワークトラフィックの異常な増加、非標準ポートを通過するネットワークトラフィック、およびホストシステムへの複数回のログイン失敗を発見しました。アナリストはまた、特定のプログラムがこれらの非標準ポートを使用しており、正規のプログラムであるように見えることも発見しました。これらが侵害の主な兆候である場合、侵入を効果的に封じ込めるために、調査において次を取るべき緊急の手順は何でしょうか？

A. 厳格なパスワードポリシーを適用し、すべてのユーザーを再認証して、さらなるログイン異常を防止する

B. ログを調べて同じファイルへの繰り返しリクエストを特定し、悪用未遂の可能性を示唆する。

C. フィッシングやスパム行為の兆候がないか、Uniform Resource Locator(URL)を分析する

D. ユーザーエージェント文字列を詳細に分析し、デバイスのOSやブラウザ情報が偽装されているかどうかを判断する。

正解: ([正解を表示します](#))

A practical immediate containment-oriented next step is to identify whether an exploit is being actively leveraged. Repeated requests for the same resource/file often indicate scanning or exploitation attempts (e.g., repeated hits to vulnerable endpoints). This helps quickly pinpoint the entry vector and supports rapid blocking/containment actions.

質問: 124

調査員がデータベースからプライマリデータファイルとログを収集する過程で、`sqlcmd -S WIN-CQQMK62867E -e -s"," -E` というコマンドを入力しました。WIN-CQQMK62867E」は何を表していますか？

A. SQL Serverの名前

B. データベースのネットワーク認証情報

C. データベース名

D. システムのオペレーティングシステム

正解: ([正解を表示します](#))

質問: 125

フォレンジックアナリストのソフィアは、侵害されたサーバーのイベントログファイルを調査しています。調査中に、イベントログヘッダーに異常と思われるエントリを発見しました。そのエントリのELF_LOGFILE_HEADER値は、ログにレコードが書き込まれたものの、イベントログファイルが正しく閉じられていないことを示しています。この情報に基づいて、ソフィアはどのELF_LOGFILE_HEADER値を特定するのでしょうか？

- A. ELF_LOGFILE_HEADER_DIRTY0x0001
- B. ELF_LOGFILE_ARCHIVE_SET0x0008
- C. ELF_LOGFILE_HEADER_WRAP0x0002
- D. ELF_LOGFILE_LOGFULL_WRITTEN0x0004

正解: ([正解を表示します](#))

The DIRTY flag indicates that the event log contains records but was not properly closed, meaning the log file may be in an inconsistent state due to improper shutdown or tampering.

質問: 126

ウェブアプリケーションのセキュリティ監査中に、サーバーログにディレクトリトラバーサル攻撃を示唆する不審なアクティビティが検出されました。この攻撃は、脆弱性を悪用して機密ファイルやディレクトリへの不正アクセスを試みるものであると考えられます。

デジタルフォレンジックにおいて、ディレクトリトラバーサル攻撃を調査する主な目的は何ですか？

- A. サーバーのハードウェア構成における潜在的な抜け穴を特定する
- B. ネットワーク帯域幅を最適化し、遅延を減らす
- C. 不正アクセスとデータ侵害の範囲を判断する
- D. Webアプリケーションでのユーザーエクスペリエンスを向上させる

正解: ([正解を表示します](#))

According to the CHFI v11 Network and Web Attacks domain, a directory traversal attack (also known as path traversal) is a web-based attack in which an attacker manipulates input parameters (such as ../ sequences) to access files and directories outside the intended web root.

This can expose sensitive resources such as configuration files, credentials, source code, system files, and application logs.

The primary forensic objective when investigating a directory traversal attack is to determine the scope and impact of unauthorized access. CHFI v11 emphasizes that investigators must analyze web server logs, application logs, and access records to identify:

Which files or directories were accessed

Whether sensitive or confidential data was exposed

The time frame of the attack

The attacker's source IP and request patterns

Whether data was viewed, downloaded, or potentially modified

Understanding the extent of data compromise is critical for incident response, regulatory notification, damage assessment, and legal proceedings. It also helps determine whether further attacks (such as privilege escalation or lateral movement) may have occurred following the traversal exploit.

質問: 127

この法律は、商用メールに関する規則を定め、商用メッセージの要件を規定し、受信者にメールの送信停止を求める権利を与え、違反に対する厳しい罰則を定めています。

- A. CAN-SPAM法
- B. 電話勧誘販売法
- C. 欧州迷惑メール対策法
- D. 連邦スパム法

正解: ([正解を表示します](#))

質問: 128

法医学調査中、チームは法医学研究室のセキュリティを確保する責任を負います。セキュリティプロトコルの一環として、研究室ではすべての訪問者の氏名、住所、訪問時間、訪問目的などの詳細情報を記録するシステムを導入しています。これにより、正確な入室記録を維持し、許可された職員のみが施設に入ることができるようになります。研究室でこのレベルのセキュリティを維持するために、以下のどの考慮事項が遵守されていますか？

- A. ラボ内の人員を管理するための人事上の考慮事項。
- B. 作業スペースと機器の設計に重点を置いた作業領域の考慮事項。
- C. 敷地内への立ち入りを許可されたすべての個人の文書化に関するプロトコルを定義する物理的なアクセスに関する考慮事項。
- D. ラボの物理的な設定がセキュリティと入場制御をどのようにサポートするかを考慮した物理的および構造的な設計上の考慮事項。

正解: ([正解を表示します](#))

According to the CHFI v11 objectives under Setting Up a Computer Forensics Lab and Ensuring Quality Assurance, maintaining strict control over who can access the forensic laboratory is a fundamental security requirement. The scenario described clearly aligns with physical access considerations, which focus on controlling, monitoring, and documenting entry into the forensic facility. Recording visitor details such as identity, time of entry, and purpose of visit ensures accountability and helps protect sensitive evidence, forensic tools, and investigation data from unauthorized access or tampering.

CHFI v11 emphasizes that forensic labs must implement visitor logs, access authorization procedures, and monitoring mechanisms as part of best practices. These measures directly support the chain of custody by demonstrating that evidence was only accessible to authorized individuals, which is essential for legal admissibility. In the event of an audit or court proceeding, access records can be used to prove that evidence integrity was preserved throughout the investigation lifecycle.

Human resource considerations (Option A) relate to staffing, training, and role assignments, not visitor access. Work area considerations (Option B) address workspace layout and equipment placement. Physical and structural design considerations (Option D) involve building architecture and security infrastructure such as locks or surveillance systems, but not the administrative tracking of visitors.

Therefore, in accordance with CHFI v11 forensic lab security guidelines, physical access considerations best describe the security control being implemented

質問: 129

サイバー攻撃の疑いがあるケースのフォレンジック調査では、調査員はインシデント発生期間中に収集されたネットワークログを確認します。調査員の目的は、これらのログを精査し、発生したイベントの正確な順序を特定し、攻撃元を特定し、インシデントの性質を理解することです。この分析は、何が、どのように、そして誰がその責任者であったかを明らかにするのに役立ちます。

この場合、調査員は次のどの手法を使用していますか？

- A. 調査員は通信を盗聴して機密情報を傍受します。
- B. 調査員はシステム記録の事後分析を実行し、過去のセキュリティ侵害を評価します。
- C. 調査員は、ネットワークトラフィックログをリアルタイムで分析して、インシデントの性質を検出します。
- D. 調査者は、攻撃元を特定するためにIPアドレスのスプーフィングを実行します。

正解: **B** ([コメントを发表する](#))

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

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

質問: 130

CHFIの調査員であるアリソンは、顧客データの漏洩事件を扱う法律事務所から依頼を受けました。アリソンは、漏洩の証拠と犯人を特定するために、事務所のデジタル資産を調査する必要があります。調査を開始する前に、アリソンは事務所のパートナーに同意を求めますが、パートナーたちは顧客の機密保持を懸念して同意を与えることに消極的です。CHFIの調査における同意取得の原則に沿って、アリソンはどのようなアプローチを取るべきでしょうか？

- A. 犯人を迅速に特定するため、秘密裏に捜査を進めてください。
- B. CHFIの調査員としての権限を利用して、同意なしに必要なデータにアクセスする

C. 同意が得られないため、訴訟から撤退する

D. 会社の懸念を尊重し、顧客の機密保持義務に違反することなく証拠を収集する他の手段を模索する。

正解: ([正解を表示します](#))

A CHFI investigator must respect legal and ethical boundaries, including consent and confidentiality. Seeking alternative lawful methods ensures compliance while maintaining the integrity and admissibility of any evidence collected.

質問: 131

次のマルウェアのうち、Androidモバイルデバイスを標的とし、攻撃者が制御するサーバーからリモートでアプリケーションをインストールするバックドアをインストールするものはどれですか？

A. アンフロッド

B. xHelper

C. XcodeGhost

D. フェリックス

正解: ([正解を表示します](#))

質問: 132

CHFIの経験豊富な調査員であるジェニファーは、世界中の複数の企業に対して数々の攻撃を仕掛けてきた国際的なサイバー犯罪組織が関わる事件を担当している。

攻撃の一つは、大手銀行のセキュリティシステムを突破し、数百万ドルを追跡不可能なオフショア口座に送金するというものだった。捜査は数ヶ月にわたり、複数の管轄区域にまたがって行われている。最近、ある情報提供により、ジェニファーは地元の容疑者の自宅にたどり着き、そこに重要なデジタル証拠が保管されている可能性があると考えた。しかし、容疑者は外国籍であり、その自宅は外交特権によって保護されている。銀行が解決を急ぐ一方で、容疑者はプライバシー権を主張しているため、状況はさらに複雑化している。ジェニファーは、法的境界線を尊重することと、事件を早急に解決することとのバランスを取らなければならない。彼女はすべきだろうか？

A. 彼女は容疑者が留守の間に彼の家に忍び込み、証拠を集めるべきです。

B. 彼女は容疑者が国外に出るまで待つから、彼のコンピューターを押収すべきだ。

C. 彼女は弁護士に相談し、国際法に基づいて令状を取得するよう努めるべきです。

D. 彼女は復号ツールを使って容疑者のコンピューターにリモートアクセスし、証拠を収集すべきです。

正解: C ([コメントを發表する](#))

When dealing with international jurisdictions and diplomatic protections, the investigator must follow proper legal channels. Consulting legal counsel and pursuing authorization through appropriate international legal mechanisms ensures the investigation remains lawful and the evidence admissible.

質問: 133

成長中のeコマース企業のシステム管理者であるジョンは、増大するデータストレージニーズに対応するため、RAID 5アレイの構成を任されています。3台のハードドライブを使用してアレイをセットアップし、ドライブ障害発生時にもデータが保護され、アクセス可能であることを確保する必要があります。アレイを構成するにあたり、ジョンはRAID 5システムがどのようにデータの冗長性を処理し、パリティデータがドライブ間でどのように分散されるかを理解する必要があります。RAID 5では、パリティデータはどのように保存され、分散されるのでしょうか？

- A. パリティ データは冗長性なしで 1 つのドライブに保存されます。
- B. パリティ データはアレイ内のすべてのドライブに分散されます。
- C. パリティ データは 2 つのドライブ間でミラーリングされます。
- D. パリティ データは専用のパリティ ドライブに保存されます。

正解: ([正解を表示します](#))

According to the CHFI v11 Digital Evidence and Storage Fundamentals, RAID (Redundant Array of Independent Disks) configurations are critical for investigators to understand because they directly impact data availability, fault tolerance, and evidence reconstruction during forensic analysis. RAID 5 is one of the most commonly deployed RAID levels in enterprise environments due to its balance between performance, storage efficiency, and redundancy.

In a RAID 5 configuration, data and parity information are striped across all disks in the array.

This means that parity blocks are not stored on a single dedicated drive; instead, parity is rotated among all participating drives. This design eliminates the bottleneck associated with a single parity disk and improves read performance while still providing fault tolerance.

If one drive fails, RAID 5 uses the distributed parity information along with the remaining data blocks to reconstruct the missing data on-the-fly, ensuring continued access to information. From a forensic perspective, this distributed parity mechanism is significant because investigators must correctly identify the RAID structure to rebuild the array and recover digital evidence accurately.

質問: 134

ロバートは、評判の良い組織で働く地域マネージャーです。ある日、コンピュータにログインした後、不要なプログラムがポップアップ表示されるようになったため、マルウェア攻撃を疑いました。ネットワーク管理者が呼ばれ、コンピュータへの侵入を調査したところ、自動起動の場所で不審なアクティビティが発生していることがわかりました。このような状況で、ネットワーク管理者はシステムへの侵入を検出するために、次のうちどのツールを使用しますか？

- A. レポートビューア
- B. インターネット証拠検索ツール
- C. プロセスモニター
- D. 16進エディタ

正解: ([正解を表示します](#))

質問: 135

セキュリティアナリストのサラは、Windowsマシンのセキュリティ監査ログを確認し、不正なアクティビティを検出しようとしています。Windowsイベントビューアーで、ID 4663のイベントを見つ

けました。これは特定の種類のシステムインタラクションに対応しています。さらに分析した結果、このイベントは重要なシステムオブジェクトに関連するアクティビティに関連していることが判明しました。

イベント ID 4663 は、Windows セキュリティに関して具体的に何を示していますか？

- A. オブジェクトを変更目的で開こうとしています。
- B. ユーザーがシステム構成にアクセスするためにログインしました。
- C. レジストリ キーやファイルなどの保護されたオブジェクトとの対話を試行します。
- D. システム オブジェクトが削除されました。

正解: [A \(コメントを發表する\)](#)

This question aligns with CHFI v11 objectives under Operating System Forensics, specifically Windows Security Event Log analysis and object access auditing. In Windows systems, Event ID 4663 is generated when an attempt is made to access an object (such as a file, folder, registry key, or other securable object) and detailed auditing is enabled. CHFI v11 emphasizes the importance of this event in identifying unauthorized or suspicious access attempts to sensitive system resources.

Event ID 4663 provides granular information about the type of access requested, such as read, write, modify, delete, or permission changes. This makes it particularly valuable in forensic investigations, as it allows investigators to determine whether a user or process attempted to modify critical system objects, which is often indicative of malicious activity, privilege abuse, or insider threats.

質問: 136

あなたは多国籍企業で発生したデータ漏洩の疑いに関するフォレンジック調査を行っています。調査中に、世界各地の複数のシステムで、一見無関係に見える複数のインシデントが発生していることが判明しました。これらのインシデントを理解し、潜在的な関連性を確立するために、どのようなアプローチを採用すべきでしょうか？

- A. 各事件ごとに個別の調査を実施する
- B. 調査全体を最初からやり直す
- C. 最も深刻なインシデントの詳細な分析を実施する
- D. イベント相関を利用して、事件間の関連性を見つける

正解: [\(正解を表示します\)](#)

Event correlation allows the investigator to analyze and link multiple incidents across different systems and locations, helping identify patterns, relationships, and a unified attack sequence.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセ

ス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> 637問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 137

コンピュータフォレンジック研究所のセキュリティと有効性を向上させるため、経営陣はベストプラクティスに基づいた一連の変更を実施することを検討しています。提示された情報に基づくと、どの対策が効果的または適切ではないでしょうか？

- A. 試験および／または校正(サンプリングを含む)を実施する試験所の公平性、能力、および均一な運用に関する一般的な要件を規定するISO/IEC 17025認証の取得を目指しています。
- B. TEMPEST規格を適用し、実験室の壁、天井、床を良質な金属導体で覆い、ワークステーションから電磁信号が伝わらないように遮蔽する。
- C. 研究室に侵入警報システムを設置して追加の保護を提供するとともに、研究室内および周辺に監視用の閉回路カメラを設置する。
- D. 法医学分析官、法医学技術者、研究所サイバー犯罪捜査官、研究所長からなるチームを編成する際に、それぞれの職務に関連する資格認定の確認を行わないこと

正解: ([正解を表示します](#))

質問: 138

デジタルフォレンジックの専門家であるクリスは、BIOS-MBRブート方式を使用して侵害されたWindowsシステムを調査している。システムのブートプロセスを確認したところ、電源投入時自己診断テスト(POST)が正常に完了していることが判明した。BIOSはハードウェアをチェックし、CPU、メモリ、ストレージデバイスなどの重要なシステムコンポーネントの整合性を検証した。その後、BIOSは起動可能なデバイスからマスターブートレコード(MBR)をロードする。この段階では、システムのブートマネージャが処理を引き継ぐことが想定されています。MBR上に存在するブートマネージャは、適切なブートローダーを見つけて起動する役割を担っています。クリスは、ブートマネージャがWindowsオペレーティングシステムの起動に不可欠なシステムファイルを見つけることを知っています。次のステップでは、OSをメモリにロードするのに役立つ重要なシステムファイルをロードします。

システムがBIOS-MBR方式を使用していることを考えると、BIOSがPOSTを完了してMBRがロードされた後、次のタスクはブートプロセスに不可欠なこの重要なファイルのロードであるということをクリスは知っています。ブートシーケンスで次に何が起こると予想すべきでしょうか？

- A. システムはWinload.exeをロードします
- B. システムはHAL.dllを初期化します
- C. システムはカーネルの整合性チェックを実行します
- D. システムはWinlogon.exeに制御を渡します

正解: ([正解を表示します](#))

After the BIOS loads the MBR and the boot manager takes control, the next step in the Windows boot sequence is loading Winload.exe. This component is responsible for loading the Windows kernel, essential drivers, and system components into memory to start the operating system.

質問: 139

Javaでは、複数のアプリケーションが起動されると、複数のDalvik仮想マシンインスタンスが発生し、メモリと時間を消費します。これを回避するため、Androidはメモリ消費量を抑え、起動時間を短縮するプロセスを実装しています。このプロセスは何と呼ばれますか？

- A. 接合子
- B. 開始
- C. デーモン
- D. メディアサーバー

正解: ([正解を表示します](#))

質問: 140

鑑識捜査官のルーカスは、捜査中にBIOSパスワードでロックされたノートパソコンに遭遇した。ノートパソコンの所有者はBIOSパスワードを覚えておらず、ルーカスは鑑識分析を続けるためにパスワードを解除する必要がある。彼はCMOSバッテリーを取り外して再度挿入する方法を用いることにした。このシナリオにおいて、CMOSバッテリーを取り外す目的は何だろうか？

- A. ハードドライブの暗号化を解除する
- B. ユーザーアカウントのパスワードを回避する
- C. BIOSでシステムパスワードをリセットする
- D. BIOSパスワードをリセットするには

正解: ([正解を表示します](#))

Removing and reinserting the CMOS battery clears the stored BIOS settings, including the BIOS password, effectively resetting it and allowing access to the system firmware configuration.

質問: 141

あなたのチームは、社内ネットワーク内のサーバーから異常なトラフィックパターンを検出しました。調査の結果、見慣れない外部IPアドレスへの接続が複数確立されていることが判明しました。ネットワークトラフィックをキャプチャして分析したところ、トラフィックの内容はランダムで、既知のプロトコルと一致しないことがわかりました。これは何を示唆しているのでしょうか？

- A. サーバーはDDoS攻撃を受けています。
- B. サーバーはコマンド&コントロールサーバーと通信しています。
- C. サーバーがランサムウェアに感染しています。
- D. サーバーはボットネットの一部です。

正解: ([正解を表示します](#))

Random, non-standard traffic to unfamiliar external IPs suggests encrypted or obfuscated communications typical of command-and-control channels, where compromised systems communicate with attacker-controlled servers.

質問: 142

ウィリアムソンは法医学捜査官です。彼はある企業のデータ漏洩事件を捜査する中で、収集した証拠に適用された法医学的手法、証拠を扱った人物の詳細、証拠を扱った日時、証拠の保管場所などを記録した文書を作成しています。この文書を何と呼びますか？

- A. ログブック
- B. 保管管理記録
- C. 同意書
- D. 承認書

正解: ([正解を表示します](#))

質問: 143

RAID 1構成では、企業の重要なデータベースが2台のミラーリングされたハードドライブに保存されています。定期的なシステムチェック中に、一方のハードドライブがハードウェアの故障により突然故障しました。しかし、もう一方のドライブに保存された冗長データにより、データベースは完全な状態でアクセス可能であり、企業はデータ損失なく業務を継続できます。RAID 1は、ハードドライブ故障時にどのようにしてデータの整合性と可用性を確保するのでしょうか？

- A. 冗長性の回復には完全な再構築が必要です。
- B. データを複製し、即時のアクセスと保護を保証します。
- C. 単一のドライブを優先し、読み取り/書き込み速度に影響します。
- D. データの回復にはパリティに依存します。

正解: ([正解を表示します](#))

According to the CHFI v11 objectives under Digital Evidence and Operating System Forensics, understanding RAID configurations is essential for both evidence acquisition and incident analysis. RAID 1, also known as disk mirroring, ensures data integrity and availability by duplicating identical data across two or more physical drives. Every write operation is simultaneously written to both drives, creating an exact replica of the data at all times.

In the event of a single hard drive failure, RAID 1 allows the system to continue operating seamlessly using the remaining drive, with no interruption to data access and no data loss. This immediate failover capability is what ensures high availability and strong data integrity, making RAID 1 especially suitable for mission-critical systems such as databases and forensic evidence repositories. From a forensic perspective, investigators can still access complete and consistent data even after a hardware failure.

質問: 144

CHFIの調査員であるロバートは、複雑な企業詐欺事件を担当している。彼は、異なる場所、異なる時間に複数のデジタル機器を証拠として押収した。彼の課題は、押収時から法廷提出時までの間に、証拠が改ざんまたは変更されていないことを法廷で証明することである。

ロバートがこれを達成する上で、重要な要素は何でしょうか？

- A. 堅牢な保管管理記録
- B. ACPOのデジタル証拠原則に依拠する
- C. 対象メディアの徹底的な消毒

D. 関係者全員の同意を得る

正解: ([正解を表示します](#))

A chain of custody documents every step of evidence handling--from seizure through analysis to presentation--ensuring traceability, accountability, and proof that the evidence remained unaltered.

質問: 145

ある日、ある評判の良い金融機関の従業員が、ある日の業務中にネットワークの異常な挙動に気づきました。すると突然、不安を抱いた顧客から、不審なログイン試行や奇妙なポップアップメッセージを報告するメールが大量に届きました。IT部門が調査を進めると、ネットワークセキュリティを狙った外部からの攻撃の兆候が見つかり、大混乱に陥りました。

企業ネットワークに脅威をもたらす外部からの攻撃の例にはどのようなものがありますか？

- A. ソフトウェアのバグとシステムの不具合**
- B. 暗号化とランサムウェア攻撃**
- C. 分散型サービス拒否(DDoS)攻撃とフィッシング**
- D. 内部脅威とソーシャルエンジニアリング**

正解: ([正解を表示します](#))

This question aligns with CHFI v11 objectives under Network and Web Attacks, specifically the classification and identification of external threats targeting organizational networks. External attacks originate outside the organization's trusted boundary and are carried out by threat actors who do not have legitimate internal access. CHFI v11 highlights that recognizing the nature of such attacks is essential for incident detection, response, and forensic investigation.

Distributed Denial of Service (DDoS) attacks are a classic example of external attacks, where attackers overwhelm network resources with massive traffic volumes to disrupt availability. These attacks often originate from botnets distributed across the internet. Phishing attacks are another common external threat, involving deceptive emails or messages designed to trick users into revealing credentials, clicking malicious links, or downloading malware. The scenario described--customers reporting suspicious login attempts and pop-ups--strongly aligns with phishing and externally driven compromise attempts.

Software bugs are internal technical issues, insider threats originate from within the organization, and while ransomware is a type of malware, the option pairing encryption and ransomware is too broad and not explicitly external. Therefore, consistent with CHFI v11 classifications, DDoS attacks and phishing are clear examples of external attacks that pose serious threats to corporate networks.

質問: 146

SQL Server Management Studioを使用してアクティブトランザクションログを収集しているときに、クエリSelect

* ::fn_dblog(NULL, NULL) からトランザクションログファイルのアクティブな部分を表示します。

ここで、NULL 値を割り当てることは何を意味しますか？

- A. ログファイルの開始点と終了点が指定されています。**

- B. ログシーケンス番号の開始点と終了点が指定されています。
- C. ログシーケンス番号の開始点と終了点が指定されていません
- D. ログファイルの開始点と終了点が指定されていません

正解: ([正解を表示します](#))

質問: 147

フォレンジック調査員のエマは、攻撃者がいくつかのファイルのタイムスタンプメタデータを改ざんしており、ファイルがいつ作成、アクセス、または変更されたかを正確に判断することが困難になっていることを発見しました。

エマは、隠された証拠を発見するために、タイムスタンプが操作されたファイルを特定する必要があります。NTFSファイルシステムのタイムスタンプの変更を検出するために、エマが使用できるツールは次のどれですか？

- A. MFTを分析する
- B. レジショット
- C. OSForensics
- D. プロセスエクスプローラー

正解: ([正解を表示します](#))

According to the CHFI v11 Operating System Forensics curriculum, timestamp manipulation is a common anti-forensics technique used by attackers to obscure activity timelines. On NTFS file systems, each file maintains multiple sets of timestamps--such as \$STANDARD_INFORMATION and \$FILE_NAME attributes--stored within the Master File Table (MFT). Discrepancies between these timestamp sets are strong indicators of timestamp tampering.

analyzeMFT is a specialized forensic tool designed explicitly to parse and analyze the NTFS Master File Table. CHFI v11 highlights MFT analysis as a critical method for detecting timestamping attacks, where attackers alter file timestamps using utilities like timestomp. analyzeMFT allows investigators to compare multiple timestamp attributes, identify anomalies, reconstruct timelines, and detect inconsistencies that standard file system views cannot reveal.

質問: 148

サイバー犯罪に関与している疑いのあるシステムのフォレンジック調査中に、調査官は \$STANDARD_INFORMATION と

\$FILE_NAME 一部のファイルの作成日時が判明しました。調査の一環として、調査員はBCWipeというユーティリティがシステムにインストールされていることも確認しました。これらの観察結果に基づくと、調査員が最も妥当と考える結論は何でしょうか？

- A. システムユーザーはBCWipeを使用して特定のファイルを安全に削除しました
- B. システムがマルウェアに感染し、メタデータが改ざんされました
- C. ファイルはBCWipeユーティリティを使用して暗号化されました
- D. 一部のファイルのタイムスタンプが改ざんされています。これは鑑識対策の一環である可能性があります。

正解: ([正解を表示します](#))

Differences between NTFS \$STANDARD_INFORMATION and \$FILE_NAME timestamps are a known indicator of timestamp manipulation. The presence of BCWipe (a secure deletion/privacy tool) strengthens the inference of anti-forensic activity aimed at obscuring timelines and evidence.

質問: 149

フォレンジック調査員のエリアは、Linuxベースのシステム上でE01ディスクイメージファイルをRAWイメージファイル形式に変換する案件に取り組んでいます。彼女は、イメージをマウントして変換し、その中のファイルを分析するための信頼性の高いツールを必要としています。このタスクを実行するために、エリアは次のどのツールを使用すべきでしょうか？

- A. ewfmount
- B. 剖検
- C. UFSエクスプローラー
- D. fdisk

正解: **A** ([コメントを發表する](#))

According to the CHFI v11 objectives under Data Acquisition, Digital Evidence, and Image/Evidence Examination, forensic investigators must be able to work with different disk image formats. The E01 format (Expert Witness Format) is widely used in digital forensics because it supports compression, metadata storage, and integrity verification through hashing.

However, many Linux-based forensic tools require the image to be mounted or accessed in a raw (dd) format for direct analysis.

ewfmount is a Linux utility from the libewf toolkit that allows investigators to mount E01 (and other EWF) images as raw disk images. Once mounted, the image appears as a raw device, enabling investigators to analyze partitions, file systems, and artifacts using standard forensic tools without altering the original evidence. This approach preserves forensic integrity and aligns with CHFI v11 best practices.

質問: 150

法医学捜査官のマークは、悪意のある活動の兆候がないか、疑わしい実行可能ファイルを調査しています。彼は、URL、ファイルパス、レジストリキーなど、ファイルの悪意のある動作を示す可能性のある埋め込み文字列をファイルから検索する必要があります。マークは、実行可能ファイルから文字列を抽出してさらに分析するために、次のうちどのツールを使用できますか？

- A. HashMyFiles
- B. PEエクスプローラー
- C. BinText
- D. 依存性ウォーカー

正解: ([正解を表示します](#))

質問: 151

フォレンジック調査員のルーカスは、Linuxベースのシステムに感染したマルウェアサンプルの挙動を分析する任務を負っています。マルウェアを実行した後、ルーカスはマルウェアがシステム

ファイルの改ざん、制限されたリソースへのアクセス、カーネルとのやり取りといった不審な動作を行っているのではないかと疑っています。マルウェアとオペレーティングシステムのやり取りを追跡するため、ルーカスはマルウェア実行中に実行されるシステムコールを監視することにしました。このデータを収集するために、マルウェアによって開始されたシステムコールを効果的に追跡・分析し、マルウェアがOSとどのように通信し、悪意のある動作を実行するかについての洞察を得るために、ルーカスは次のどのツールを使用すべきでしょうか？

A. プロセスエクスプローラー

B. strace

C. 自動実行

D. レジショット

正解: ([正解を表示します](#))

According to the CHFI v11 objectives under Malware Forensics and Linux Memory and System Behavior Analysis, monitoring system calls is a core technique for understanding how malware interacts with the operating system at a low level. On Linux systems, strace is the primary and most effective tool for this purpose.

Strace intercepts and records system calls made by a process, along with the signals received and return values. Since all interactions between user-space programs and the Linux kernel occur via system calls, tracing them provides deep visibility into malware behavior. Using strace, investigators can observe actions such as file creation or modification (open, write), privilege escalation attempts (setuid), network communications (connect, sendto), process creation (fork, execve), and access to protected system resources. This makes strace indispensable for dynamic malware analysis on Linux, as emphasized in CHFI v11.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **152**

ネットワークセキュリティアナリストのソフィアは、Ciscoルーターのログを確認し、不審なトラフィックパターンを特定しようとしています。アクセス制御リスト(ACL)フィルタの条件に一致するログエントリを見つけました。これは、適用されたルールに基づいてTCPまたはUDPパケットが検出されたことを示しています。ログエントリの説明に基づいて、このログメッセージの正しいニーモニックは次のどれですか？

A. %IPV6-6-ACCESSLOGP

B. %SEC-6-IPACCESSLOGRL

C. %SEC-6-IPACCESSLOGP

D. %SEC-4-多すぎる

正解: ([正解を表示します](#))

Within the CHFI v11 syllabus under Network Forensics and Log Analysis, understanding Cisco router log mnemonics is essential for investigating network-based attacks and policy violations.

Cisco devices generate structured log messages that include a facility, severity level, and mnemonic, which together describe the event detected by the device.

The mnemonic %SEC-6-IPACCESSLOGP specifically indicates that a packet (TCP or UDP) matched an IP Access Control List (ACL) rule and was logged accordingly. The "SEC" facility denotes a security-related event, the severity level "6" represents an informational message, and "IPACCESSLOGP" confirms that the log entry was generated due to an ACL permit or deny rule matching a packet. This type of log is commonly used in forensic investigations to trace suspicious traffic, identify unauthorized access attempts, and correlate firewall or router behavior with other network logs.

質問: 153

ハリーは感染したシステムから疑わしい実行ファイルを入手し、そのマシンコードをアセンブリ言語で記述された命令に変換しようとしています。この目的のために、彼はどのツールを使用すべきでしょうか？

A. BinText

B. ハッシュ計算

C. oledump

D. Ollydbg

正解: ([正解を表示します](#))

質問: 154

実行中のプロセスのメモリを、即時またはエラー発生時にダンプするために使用されるツールは次のうちどれですか？

A. CacheInf

B. Belkasoft Live RAM Capturer

C. 振付

D. FATキット

正解: ([正解を表示します](#))

質問: 155

サイバー犯罪捜査において、フォレンジックチームは証拠収集プロセスの一環として、多数のデバイスを押収しました。すべてのデバイスを確保した後、チームはどの証拠を優先的に分析すべきかを評価し始めます。チームは分析済みの証拠と未分析の証拠の両方について詳細な記録を保持し、捜査の進捗状況を追跡し、すぐに分析されなかった証拠を参照できるようにしています。

チームはどの ENFSI ベストプラクティスに従っていますか？

- A. チームはケースの要件を評価するために初期ケース評価を実施します。
- B. チームは犯罪現場の証拠を処理するために現場評価を実行します。
- C. チームは、成果物を文書化するために実験室評価を実行します。
- D. チームは押収したデバイスからデータを抽出するためにデータ取得を実行します。

正解: ([正解を表示します](#))

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

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

質問: 156

管理者が疑わしいネットワークトラフィックについてCisco IOSログを確認している際に、「%SEC-6-IPACCESSLOGP」というニーモニックを含むログメッセージに遭遇した。このメッセージは、TCPまたはUDPトラフィックのいずれかにおいて、指定されたアクセスリストのログ基準に一致するパケットが検出されたことを示す。

次のうち、ログエントリを最も適切に説明しているのはどれですか？

- A. アクセスリストで定義された基準に一致するパケットが許可または拒否され、監視のためにログに記録されました。
- B. アクセス制御リスト(ACL)ルールによりパケットが破棄されました。
- C. ネットワークトラフィック過多に関連するシステムレベルのエラーが発生しました。
- D. ネットワーク上で接続試行の失敗が検出されました。

正解: ([正解を表示します](#))

The "%SEC-6-IPACCESSLOGP" message indicates that a packet matched an ACL entry and was logged, meaning the traffic was either permitted or denied based on the rule, with logging enabled for monitoring purposes.

質問: 157

ウェブアプリケーションを運用する組織が侵害され、攻撃者はデータベース全体をダウンロードすることに成功しました。フォレンジック調査員がログの初期レビューを行ったところ、「%2e%2e%2f」という文字列が複数回出現していることが判明しました。この侵害はどのような種類の攻撃によって発生したと考えられますか？

- A. クロスサイトスクリプティング(XSS)攻撃。

- B. ディレクトリトラバーサル攻撃。
- C. SQLインジェクション攻撃。
- D. 力任せの攻撃。

正解: ([正解を表示します](#))

The string "%2e%2e%2f" is URL-encoded for "../", which is used to traverse directories outside the intended path. This pattern is characteristic of a directory traversal attack aimed at accessing restricted files or directories.

質問: 158

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。

正解: ([正解を表示します](#))

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.

質問: 159

ボリューム上の使用済みおよび未使用のクラスタをすべて追跡するために\$BitMapファイルを使用するファイルシステムを特定します。

- A. FAT32
- B. EXT
- C. 脂肪
- D. NTFS

正解: ([正解を表示します](#))

質問: 160

プロセスを停止せずにプロセスメモリの内容をダンプできるツールはどれですか？

- A. pdump.exe
- B. processdump.exe
- C. psdump.exe
- D. pmdump.exe

正解: [\(正解を表示します\)](#)

質問: 161

デジタルフォレンジックアナリストのザカリーは、古いワークステーションが関わるサイバースパイ事件の捜査に取り組んでいる。そのワークステーションはIDE(Integrated Drive Electronics)ハードディスクドライブを使用していたが、電源サージによって故障し、読み取り不能になってしまった。ザカリーは、このドライブに捜査に役立つ重要な証拠が含まれていると考えている。しかし、この事件でワークステーションのマザーボードも損傷しており、ザカリーが利用できるシステムはすべて最新型でSATAコネクタしか搭載していない。そのため、IDEドライブをこれらのシステムに直接接続することはできない。このような状況で、ザカリーはIDEハードドライブからデータを復元するためにどのような行動をとるべきだろうか？

- A. ザカリーはIDEドライブを専門のデータ復旧サービスに送るべきです。
- B. ザカリーは、SATA-IDE変換アダプタを使用してIDEハードドライブを最新のシステムに接続する必要があります。
- C. ザカリーは、損傷したワークステーションのマザーボードを修理するべきです。
- D. ザカリーはIDEドライブからプラッタを取り出し、正常に動作するSATAドライブに挿入するべきです。

正解: **B** ([コメントを発表する](#))

Using a SATA-to-IDE adapter allows the legacy IDE drive to be connected to modern systems with SATA interfaces, enabling data access without modifying the original evidence.

質問: 162

サイバー犯罪捜査において、フォレンジックアナリストは企業のネットワークからデータ窃盗の証拠を発見しました。攻撃者は高度な技術を用いて痕跡を隠蔽し、デジタルフットプリントを消去しているため、侵害の発生源の追跡は困難です。このシナリオにおいて、捜査官が犯人を効果的に特定し訴追するために、コンピュータフォレンジックのどのような目的に重点を置くべきでしょうか？

- A. 地域の気象パターンの評価
- B. 財務予測のための市場動向の分析
- C. 物理的なセキュリティ評価の実施
- D. 削除されたファイルと隠しデータの回復

正解: **D** ([コメントを発表する](#))

According to the CHFI v11 Computer Forensics Fundamentals, one of the primary objectives of computer forensics is to identify, preserve, analyze, and present digital evidence, even when

adversaries deliberately attempt to conceal or destroy it. In cybercrime cases involving data theft, attackers often employ anti-forensics techniques such as file deletion, log wiping, data overwriting, encryption, and artifact obfuscation to evade detection and attribution.

The ability to recover deleted files and hidden data is therefore critical. CHFI v11 emphasizes that deleted data is rarely immediately destroyed; instead, file system pointers are removed while the underlying data may still exist in unallocated space, slack space, or backup structures. Forensic techniques such as file carving, analysis of unallocated disk space, examination of shadow copies, and recovery of hidden or encrypted containers allow investigators to reconstruct attacker activity and uncover intent, timelines, and methods used during the breach.

質問: 163

ある企業のネットワークが、一見正規のサービスを提供しているように見えるウェブサイトから発信されたマルウェア攻撃によって侵害されました。ユーザーは知らず知らずのうちにそのサイトにアクセスし、その後、システムに異常な動作が現れ始めました。企業は、ユーザーがサイトにアクセスした直後にマルウェアが実行され、それ以上の操作は不要だったことを発見しました。この攻撃の原因として最も可能性が高いのは、どの手法でしょうか？

- A. ブラックハットSEOの手法を利用して、ターゲットネットワークにマルウェアを仕込む。
- B. ドライブバイダウンロード方式でターゲットシステムにマルウェアをインストールする。
- C. スピアフィッシングサイトを利用して、ターゲットネットワークにマルウェアをインストールする。
- D. マルバタイジングを通じて標的ネットワークにマルウェアを配布する。

正解: ([正解を表示します](#))

Drive-by download attacks execute malware automatically when a user visits a compromised or malicious website, without requiring additional user interaction.

質問: 164

サイバー犯罪事件の現場に、コンピュータハッキング鑑識捜査官(CHFI)が到着した。捜査官は現場の初期搜索中に、GPS機器、キーボード、発信者番号表示ボックスに接続された電話回線を発見した。証拠搜索の手順を考慮すると、捜査官はまずどの行動をとるべきだろうか？

- A. キーボードを固定して、指紋が付着するのを防ぎます。
- B. 搜索および押収証拠記録を開始し、特定された機器の詳細を記録する。
- C. 現場の現状に関する観察結果を記録する
- D. GPSデバイスを調査し、デジタル情報の潜在的な情報源を探る

正解: ([正解を表示します](#))

As soon as potential evidence is identified, the investigator should begin formal documentation (search and seizure/evidence log) to maintain chain of custody. Securing items and making detailed observations are important, but the evidence log is foundational for defensibility and accountability from the start.

質問: 165

- A. ネットワークセキュリティプロトコルの強化
- B. サイバー攻撃の発信源を特定する
- C. ネットワークパフォーマンスの最適化
- D. 従業員のインターネット利用状況の監視

正解: [\(正解を表示します\)](#)

According to the CHFI v11 curriculum under Network Forensics and Analyzing Network Attacks, the primary purpose of using network log analysis tools during a suspected Distributed Denial-of-Service (DDoS) attack is to identify the source and nature of the attack traffic. DDoS attacks overwhelm network resources by flooding them with a massive volume of malicious traffic originating from multiple compromised systems.

By analyzing firewall logs, IDS/IPS logs, router logs, and server access logs, investigators can detect abnormal traffic patterns such as unusually high connection rates, repeated requests from multiple IP addresses, malformed packets, or protocol misuse. These indicators help forensic investigators trace the origin of attack traffic, identify botnet behavior, determine attack vectors (e.g., SYN flood, UDP flood, HTTP flood), and assess the scope and impact of the attack.

質問: 168

シモナは、Webアプリケーション固有の攻撃試行を検出するための正規表現を `/((\%3C)|<)((\%2F)|V)*[a-z0-9\%]+((\%3E)|>)/ix` と記述しました。 `((\%3E)|>)` の部分は、次のうちどれを探しますか？

- A. 英数字文字列またはその16進数表記
- B. 開口アングルブラケットまたはそれに相当する六角ブラケット
- C. 閉じるアングルブラケット、またはそれに相当する六角ブラケット
- D. 閉じタグを表すスラッシュ、またはその16進数表記

正解: [C \(コメントを发表する\)](#)

質問: 169

デジタルフォレンジック調査において、調査員は組織のインフラストラクチャ内のサーバーや共有ドライブからデータを収集する任務を負います。調査員は、これらの中央ストレージから関連する電子証拠にアクセスし、取得することで調査を支援します。収集されるデータには、インシデントの範囲を把握するために必要なファイル、ユーザーログ、その他のシステムアーティファクトが含まれます。このシナリオにおいて、調査員はどのようなeDiscovery収集手法を採用していますか？

- A. 調査員はネットワーク収集を使用して、ネットワーク全体の内部リポジトリおよび組織のデータ ハブから直接データを収集します。
- B. 調査員はクラウドベースの収集を使用して、クラウドストレージおよびプラットフォームからデータを取得します。
- C. 調査員は電子メール収集を使用して、電子メール システムから関連する通信と添付ファイルを抽出します。
- D. 調査員はモバイル デバイス コレクションを使用して、スマートフォン、タブレット、その他のモバイル デバイスからデータを取得します。

正解: [\(正解を表示します\)](#)

Under the CHFI v11 objectives related to the eDiscovery process , investigators must understand and correctly apply various eDiscovery collection methodologies based on where data resides and how it is accessed. In this scenario, the investigator is collecting evidence from internal servers and shared drives that are part of the organization's on-premises infrastructure. These repositories typically store centralized data such as user files, audit logs, access records, and application artifacts.

This approach directly aligns with network collection , an eDiscovery methodology in which data is acquired remotely over the organizational network from file servers, database servers, shared storage, and internal repositories . Network collection is commonly used in enterprise investigations because it allows investigators to gather large volumes of data efficiently without physically seizing individual endpoint devices.

Cloud-based collection (Option B) applies only when data is hosted on third-party cloud platforms such as AWS, Azure, or Google Cloud. Email collection (Option C) is limited to mail servers and messaging systems, while mobile device collection (Option D) focuses on smartphones and tablets. None of these accurately describe the centralized, internal infrastructure outlined in the scenario.

The CHFI v11 Exam Blueprint emphasizes eDiscovery collection methodologies as part of forensic readiness and investigation workflows, highlighting network collection as the appropriate technique for acquiring evidence from organizational servers and shared drives while maintaining integrity and chain of custody

質問: 170

熟練したデジタルフォレンジック調査員であるサラ刑事は、サイバー犯罪組織に関連する侵入されたコンピュータシステムの調査を開始する。彼女は、不安定なデータを優先し、綿密に証拠収集戦略を立案する。捜査を進める中で、様々なデータソースが浮上し、それぞれが違法な計画を解明する手がかりとなる可能性を秘めている。

RFC 3227 ガイドラインで概説されている変動性の順序を考慮して、どのデータ ソースを収集の優先順位にすべきでしょうか。

- A. 潜在的に重要なファイルを含むディスクまたはその他の記憶媒体
- B. 最近のアクティビティが保存される可能性のある一時ファイルシステム
- C. DVD-ROMやCD-ROMなどのアーカイブメディア
- D. システムの物理構成とネットワークポロジ

正解: **D** ([コメントを发表する](#))

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

According to RFC 3227, the order of volatility starts with data that changes most rapidly, such as system state and network-related information. This includes the physical configuration of the

system, network topology, routing tables, ARP cache, active network connections, and running processes. These elements can disappear immediately if the system is powered off or network connectivity changes, making them the highest priority during live response.

質問: 171

ある組織は、法的調査のためのデータ収集を効率的に管理することに重点を置いたeDiscovery戦略を策定しました。この戦略の一環として、法務チームは、適切な情報源から関連データのみが収集されるようにする責任を負っています。法務チームは、調査に必要な電子的に保存された情報(ESI)を含むデータソースを特定する責任があります。この場合、法務チームはeDiscoveryのどのベストプラクティスに従っているのでしょうか？

- A. 明確なガイドラインを提供せずに、保管者による自己回収に依存している。
- B. データのマッピングを行い、管理者を特定し、収集するデータの場所を決定します。
- C. 指示された収集を使用して、無関係なファイルも含め、管理者から入手可能なすべてのデータを取得します。
- D. 収集時間とリソースを最小限に抑えるため、データは1つのソースからのみ収集します。

正解: **B** ([コメントを发表する](#))

Mapping data to identify custodians and data locations ensures that only relevant electronically stored information is targeted for collection, improving efficiency and maintaining compliance with eDiscovery best practices.

質問: 172

あなたはコンピュータハッキングフォレンジック調査官(CHFI)として、Webアプリケーションファイアウォール(WAF)で保護されているWebアプリケーションへの侵害の可能性を調査しています。WAFのログに、SQLインジェクション保護を回避しようとする試みが繰り返し行われたことを示唆する記述があることに気づきました。

ウェブサーバーとMySQLデータベースを検査した結果、データ操作の痕跡は見つかりませんでした。そこで、さらに深く調査し、データベースサーバーのログを調べることにしました。クエリコマンドを示すログエントリに気づいた場合、次のうちどれが最も可能性が高いと推測しますか？

"1' OR '1'='1'; --"?

- A. WAFはSQLインジェクション攻撃を正常にブロックし、不正なデータ操作は発生しませんでした。
- B. SQLインジェクションが成功し、不正なデータ操作が発生した可能性が高い。
- C. WAFのSQLインジェクション保護を回避するための構文が正しくないため、SQLインジェクションの試みは失敗しました。
- D. WAFはSQLインジェクションの試みを検出できませんでした。MySQLの組み込み保護機能によりデータ操作が防止されました。

正解: ([正解を表示します](#))

The payload 1' OR '1'='1'; -- is a classic SQL injection technique used to force a condition to evaluate as true and comment out the remainder of a query. If it appears in the database server logs, it strongly suggests the malicious input reached and was executed by the database engine-

indicating a successful injection attempt and potential unauthorized access/manipulation, even if obvious changes are not immediately visible.

質問: 173

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. 法務チームは証拠収集時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します。
- B. 両チームとも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く。
- C. ITチームは証拠の適切な収集を保証する責任を単独で負い、法務チームは文書作成のみに専念します。
- D. ITチームは収集した証拠の完全性を確保し、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。

正解: [\(正解を表示します\)](#)

The IT team ensures that electronic evidence is collected and preserved in a forensically sound manner, maintaining its integrity, while the legal team ensures that the collection process complies with legal requirements so the evidence is admissible in court.

質問: 174

大規模なデータ侵害に関わるサイバー犯罪捜査において、捜査官は証拠が複数のクラウドベースプラットフォームに分散しており、データが複数の国のサーバーにホストされていることを発見しました。捜査官は国際令状やデータアクセス承認など必要な法的権限を取得しているものの、複数の管轄区域にまたがるクラウドリポジトリの複雑さにより、データの回収に大きな障害に直面しています。これらの問題により、捜査に大幅な遅延が生じ、犯人特定に必要な重要な証拠を迅速に収集することが困難になっています。

この事件で捜査官が直面している主な課題は何ですか？

- A. さまざまなクラウドベースのサービスや管轄区域に関係する法律に関する法的理解が限られており、技術的知識も不十分です。
- B. クラウド環境ではフォレンジックの準備が整っておらず、証拠収集が妨げられています。
- C. 証拠の揮発性により、クラウド環境では重要なログが失われたり上書きされたりすることがあります。

D. 複数の管轄区域にデータが保存されているため、証拠へのアクセスに問題が発生します。

正解: **D** ([コメントを发表する](#))

According to the CHFI v11 Cloud Forensics domain, one of the most significant challenges in cloud-based investigations is data residency and multi-jurisdictional storage. Cloud service providers often distribute customer data across multiple geographic regions and countries for redundancy, performance optimization, and availability. As a result, evidence relevant to a single investigation may reside in different legal jurisdictions, each governed by its own data protection laws, privacy regulations, and disclosure requirements.

In the given scenario, the investigator has already obtained the necessary legal authorizations, which rules out lack of legal understanding as the primary issue. However, despite these approvals, accessing data spread across multiple jurisdictions introduces procedural delays, coordination challenges with cloud service providers, and dependencies on international legal frameworks. CHFI v11 explicitly highlights that cross-border data access is a major obstacle in cloud forensics, often slowing investigations even when warrants and mutual legal assistance mechanisms are in place.

While volatility of logs and forensic readiness are valid cloud challenges, the scenario emphasizes delays caused by geographic and jurisdictional dispersion of data, not data loss or lack of preparation. CHFI v11 stresses that investigators must plan for jurisdictional complexity, sovereignty issues, and provider cooperation timelines when handling cloud-hosted evidence.

質問: **175**

ネットワークセキュリティアナリストのデイビッドは、Apache Webサーバーに関連する可能性のある侵害の調査を任されました。ログを確認したところ、ログイン試行の失敗が複数回発生しており、ファイルが利用できないことに関連するHTTPエラーメッセージが表示されていることに気づきました。これらのログイン失敗がより大きなセキュリティ問題の一部であったかどうかをデイビッドが判断する上で、最も有用な情報を提供するApacheログエントリは次のうちどれでしょうか？

A. [2023年12月11日(月) 14:35:38.878945] [core:notice] [pid 12356:tid 8689896234] [client 10.0.0.8] 接続が正常に閉じられました

B. [2023年12月11日(月) 14:35:38.878945] [core:error] [pid 12356:tid 8689896234] [client 10.0.0.8] ファイルが見つかりません: /images/folder/pic.jpg

C. [月 12月 11 14:35:38 878945 2023] [mod_security:info] [pid 12356:tid 8689896234] [client 10.0.0.8] ルールがトリガーされました: SQLインジェクション攻撃の可能性

D. [2023年12月11日(月) 14:35:38.878945] [auth:debug] [pid 12356:tid 8689896234] [client 10.0.0.8] 無効なユーザーによる試行

正解: **C** ([コメントを发表する](#))

An entry indicating a triggered security rule for a possible SQL injection attempt directly highlights malicious activity. This provides clear evidence of exploitation attempts beyond simple failed logins or missing files, helping determine if the activity is part of a broader attack.

質問: 176

コンプライアンス担当者のスカーレットは、最近財務上の不正行為の疑いをかけられた上場企業に勤務している。調査を進める中で、彼女は2002年に米国議会で可決された、企業による不正会計から投資家を保護することを目的とした法律を発見する。この法律は、より厳格な企業財務報告基準、内部統制、そして不正行為に対する罰則を義務付けている。

この事件において、スカーレットが最も検討している可能性が高い法律は次のうちどれですか？

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

正解: **B** ([コメントを發表する](#))

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

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

質問: 177

ある国際航空会社が最近、予約システムへのサイバー攻撃を発見しました。この攻撃は綿密に計画・実行され、痕跡はほとんど残っていません。攻撃者は、データ難読化やログ操作などの高度なフォレンジック対策技術を使用しており、社内のサイバーセキュリティチームが攻撃の発生源を特定し、その影響全体を把握することは困難です。このような複雑な調査に直面した場合、サイバーセキュリティチームが最初にとるべき行動は次のうちどれでしょうか？

- A. 脅威アクターが用いた手法をリバースエンジニアリングする。
- B. すべてのデバイスにシステムアップデートを展開し、潜在的な脆弱性を修正します。
- C. 侵害された正確なデータを特定することに集中します。
- D. すべてのシステムに対して厳格なアクセス制御を実施する。

正解: ([正解を表示します](#))

The first priority in a breach investigation is to determine what data has been compromised. Identifying the affected data defines the scope and impact of the incident, which then guides further forensic analysis, containment, and remediation actions.

質問: 178

Torブラウザの動作は、以下のどの概念に基づいていますか？

- A. スタティックルーティング
- B. 静的ルーティングとデフォルトルーティングの両方
- C. デフォルトルーティング
- D. オニオンルーティング

正解: ([正解を表示します](#))

質問: 179

セキュリティ侵害の疑いが発生したことを受け、調査担当者が企業IISウェブサーバー上のネットワークアクティビティとユーザー操作の分析を担当することになった。この任務では、調査担当者は大量のIISログデータを処理し、不審なトラフィック傾向、ユーザーアクセス、および潜在的な悪用試行を特定することに重点を置く必要がある。使用するツールは、効率的なログ解析、異常検知、およびイベントのタイムライン再構築に役立つ詳細なレポートの生成を可能にするものでなければならない。

これらの要件を踏まえると、調査担当者はIISログを効果的に分析するためにどのツールを選択すべきでしょうか？

- A. 製材所
- B. DSInternals PowerShell
- C. ジェイソン
- D. ハンチリー

正解: ([正解を表示します](#))

Sawmill is designed for high-volume log analysis, including IIS logs. It provides efficient parsing, trend analysis, anomaly detection, and detailed reporting capabilities, which are essential for reconstructing timelines and identifying suspicious activity in web server logs.

質問: 180

Windows OSがマシン上のショートカットファイルに使用する拡張子は何ですか？

- A. .pf
- B. .lnk
- C. .dat
- D. .log

正解: ([正解を表示します](#))

質問: 181

企業調査の一環として、フォレンジック調査員のメリッサは、容疑者のノートパソコンのウェブブラウザの履歴、Cookie、キャッシュを調査するよう依頼されました。ノートパソコンには、Google Chrome、Firefox、Safariなど、複数のウェブブラウザがインストールされています。メリッサは、複数のウェブブラウザからこれらのデジタルアーティファクトを包括的に抽出・分析できるツールを必要としています。彼女はどのツールを使用すべきでしょうか？

- A. エンケース
- B. ネットアナリシス

C. ディスクエクスプローラー

D. 探偵キット

正解: ([正解を表示します](#))

NetAnalysis is specifically designed to extract and analyze web browser artifacts such as history, cookies, and cache from multiple browsers, making it ideal for this task.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格すること
に役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供しま
す。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題
集のテストエンジンを手に入れます。最新版のアクセ
ス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637**問、**30%ディスカウント**、
特別な割引コード: **JPNshiken**」

質問: **182**

調査担当者は、データの完全性を維持するために、ストレージメディアの内容を変更することなく
データ取得を行う必要があります。調査担当者が採用する手法は、ストレージメディアへの読み取
り専用アクセスを可能にする機能に依存しています。このタスクを実行するために、調査担当者は
どのツールを手順に組み込むべきでしょうか？

A. 書き込みブロッカー

B. BitLocker

C. データ複製ツール

D. バックアップツール

正解: **A** ([コメントを发表する](#))

質問: **183**

ゲイリーは捜査中に、容疑対象システムのUSBポートに接続されているデバイスを確認していま
す。接続されているすべてのデバイスを記録するのに役立つ適切なツールを選択してください。

A. デブコン

B. fsutil

C. Reg.exe

D. DevScan

正解: ([正解を表示します](#))

質問: **184**

次の攻撃のうち、攻撃者がアプリケーションのソースコード、設定ファイル、重要なシステムファ
イルなどの制限されたディレクトリにアクセスし、Webサーバーのルートディレクトリ外でコマン
ドを実行できるのはどれですか？

A. ディレクトリ走査

- B. 未検証の入力
- C. セキュリティ設定ミス
- D. パラメータ／フォームの改ざん

正解: A ([コメントを发表する](#))

質問: 185

フォレンジックアナリストは、日常的なデジタル調査において、一見無害なファイルの中に機密情報が隠されている可能性を疑います。徹底的なスキャンと分析にもかかわらず、従来の監視技術では異常を検出できません。

攻撃者は、一見普通のファイル内に機密情報を隠し、法医学調査員による検出を困難にするために、どのような手法を使用する可能性がありますか？

- A. 試験的な難読化
- B. ファイルシステム構造にデータを隠す
- C. ファイル拡張子が一致しません
- D. ステガノグラフィー

正解: D ([コメントを发表する](#))

According to the CHFI v11 Anti-Forensics Techniques domain, steganography is a sophisticated method used by attackers to conceal sensitive or malicious information within seemingly normal files such as images, audio files, video files, or documents. Unlike encryption, which makes data unreadable but visibly suspicious, steganography hides the existence of the data itself, making detection significantly more challenging during forensic analysis.

In steganography, data is embedded into unused or less noticeable parts of a file--such as the least significant bits (LSB) of image pixels or audio samples--without noticeably altering the file's appearance or functionality. As a result, standard antivirus tools, intrusion detection systems, and basic forensic scans may not flag these files as suspicious. CHFI v11 highlights steganography as a common anti-forensic tactic used for covert data exfiltration, command-and-control communication, and storage of illegal or confidential information.

質問: 186

マルウェア攻撃によってシステム侵害が発生しました。この攻撃は検出を回避し、ソフトウェアのインストールやハードドライブへのアクセスなしにマシンメモリを侵害しました。攻撃者はどのような手法を用いて攻撃を実行したのでしょうか？

- A. スパイウェア
- B. JavaScript
- C. ファイルレス
- D. トロイの木馬

正解: C ([コメントを发表する](#))

質問: 187

容疑者の携帯端末が関係する犯罪捜査において、鑑識捜査チームは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。

各プラットフォームは、フォレンジック分析においてそれぞれ固有の課題と手法を提示します。これらのデバイスからデジタル証拠を効果的に抽出 調査するために、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しょうか？

A. Android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が容易になり、広く利用可能なツールで簡単にフォレンジック分析を行うことができます。

B. 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。

C. 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 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、特殊な技術が必要です。

D. 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。

正解: [\(正解を表示します\)](#)

Android commonly uses the Ext4 file system, which is well supported by standard forensic tools and allows relatively straightforward data extraction. iOS devices use APFS with strong encryption and security controls, requiring specialized forensic techniques and tools to access and analyze the data.

質問: 188

金融サービスを専門とする大手多国籍企業は最近、重要な業務システムに影響を与えるデータ侵害の可能性を経験しました。フォレンジック調査の一環として、組織は侵害の範囲を特定し、機密性の高い金融データの整合性を検証するために、サーバーを完全かつ詳細なレベルで迅速に復元する必要があります。フォレンジックチームには、サーバーの完全なイメージレベルのバックアップを実行できるだけでなく、個々のシステムを調査し、特定のドキュメントや設定ファイルを復元するために、ファイルとフォルダーを選択的に復元できる、包括的で信頼性の高いツールが必要です。このツールは、物理環境と仮想環境の両方を効率的に処理し、ダウンタイムを最小限に抑え、正確なデータ復旧を実現できる必要があります。

組織は迅速かつ確実な復旧を必要としているため、フォレンジックチームは、障害発生時にシステム全体を復旧できるだけでなく、バックアップイメージから個々のファイルやフォルダを復元できる柔軟性も備えたツールを選択する必要があります。この機能は、侵害されたシステムを隔離し、侵害の影響を受けた可能性のある重要な業務記録を復旧するために不可欠です。組織は、データの復旧だけでなく、調査期間中も事業継続性を維持し、フォレンジックの整合性を維持しながらシステムを可能な限り迅速に復旧できるソリューションを必要としています。

次のフォレンジックツールのうち、このタスクに最適なものはどれでしょうか？

A. スナジット

- B. Macrium Reflect サーバー
- C. VMware vSphere ハイパーバイザー
- D. エズヴィット

正解: ([正解を表示します](#))

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

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

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

質問: 189

ある大手金融機関は最近、重要なサーバーで異常に多くのログイン失敗試行が発生していることを確認しました。セキュリティアナリストはSplunk Enterprise Security(ES)を使用してログを調査し、ブルートフォース攻撃の可能性を疑いました。Windowsイベントビューアーのログを調べた結果、アナリストは一連のイベントID 4625(ログイン失敗)とイベントID 4624(ログイン成功)を検出しました。

潜在的な攻撃の発生源を正確に特定し、さらに調査を進める上で、アナリストにとって最も有益なSIEM機能はどれでしょうか？

- A. Splunk ESのリスクベースアラート機能
- B. Splunk ESの高度な分析機能による検出と調査
- C. IBM QRadar SIEMのリアルタイム脅威検出機能
- D. IBM QRadar SIEMにより、オンプレミス、SaaS、IaaS 環境全体にわたって一元化されたインサイトが提供されます。

正解: ([正解を表示します](#))

To pinpoint the source of brute-force activity, the analyst benefits most from Splunk ES capabilities such as correlation searches, entity analytics, event aggregation, and investigative workflows that connect 4625 spikes with subsequent 4624 successes, source IPs, accounts, and time windows.

質問: 190

ある組織が重大なデータ侵害を受け、証拠収集のためにコンピュータハッキングフォレンジック調査員(CHFI)を招集しました。調査員は、侵害されたシステムから不揮発性データを収集するために、デッドアクイジション手法を使用することにしました。この種のフォレンジックデータ取得プロセスにおいて、通常取得されないデータは次のうちどれでしょうか？

- A. ウェブブラウザのキャッシュ
- B. 未割り当てのドライブ領域
- C. アクティブなネットワーク接続
- D. ブートセクター

正解: **C** ([コメントを发表する](#))

Dead acquisition is performed when the system is powered off (or storage is acquired offline). It captures non-volatile data from disk such as browser cache, unallocated space, and boot sectors. Active network connections are volatile/live-state artifacts and cannot be captured via dead acquisition.

質問: 191

ジェームズは、複雑な産業スパイ事件を扱う国際法律事務所に所属する、経験豊富なデジタルフォレンジック調査官です。攻撃者は不満を抱いた元従業員とみられ、高度なネットワークを悪用して機密データを盗み出した疑いがあります。複数の法域と規制が関係しており、システムは様々な国に所在しています。事務所の法務チームは、証拠規則や、異なる法制度における搜索差押令状の取得について懸念を抱いています。さらに事態を複雑にしているのは、事務所の顧客の一部がジェームズによるシステムへのアクセスと調査を拒否していることで、証拠収集プロセスがさらに困難になっていることです。このような複雑な状況において、ジェームズはまずどのようなアプローチを取るべきでしょうか？

- A. 搜索令状を放棄し、入手可能なデータに基づいて捜査を開始する。
- B. データは会社が所有しているため、顧客のシステムに秘密裏にアクセスする。
- C. 法務チームと協力して各管轄区域の法律を理解し尊重し、必要な令状を取得する
- D. 法的問題を避けるため、調査対象を企業の内部システムに限定する

正解: ([正解を表示します](#))

In multi-jurisdictional investigations, the priority is to ensure all actions comply with applicable laws and regulations. Coordinating with the legal team to understand jurisdictional requirements and obtain proper warrants ensures the investigation remains lawful and that any collected evidence is admissible in court.

質問: 192

サイバーセキュリティ企業のフォレンジックアナリストとして、あなたはクライアントのオフィスで発生した情報漏洩事件の調査を任されました。この漏洩は複数のサーバーに影響を及ぼしており、各サーバーにはそれぞれ独自のログとイベントが記録されています。分析を効率化し、漏洩の根本原因を特定するために、どのようなイベント相関分析手法を用いるべきでしょうか？

- A. 時間ベースの相関

- B. 対数ベースの相関
- C. アラートに基づく相関関係
- D. ルールに基づく相関関係

正解: ([正解を表示します](#))

Time-based correlation aligns events from multiple systems using timestamps, enabling the investigator to reconstruct the sequence of activities across servers and identify the root cause of the breach.

質問: 193

マルウェアのフォレンジック調査中に、侵害されたシステム上でマルウェアが実行された後、Windowsの自動起動レジストリキーに新たに追加されたエントリが特定されました。このエントリは、「CaoClboog.vbs」という名前のVBスクリプトファイルが「Run」キーにインストールされ、永続化を実現し、ユーザーログイン時に自動的に実行されることを示しています。コンピュータハッキングフォレンジック調査官(CHFI)として、レジストリハイブのどこにこの疑わしいエントリがあると予想しますか？

- A. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
- B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup

正解: ([正解を表示します](#))

The HKCU...\Run key is a common per-user persistence location that triggers programs/scripts at user logon. Since the question specifies it was installed in the Run key to execute upon user login and implies per-user context, HKCU is the expected hive path.

質問: 194

CHFI認定調査員のローラは、ソフトウェア開発会社で発生した重大な事件の調査を依頼された。不満を抱いた従業員が複数の基幹製品に悪意のあるコードを注入し、会社の評判と収益に深刻な損害を与えたのだ。ローラは、容疑者が何週間も連続稼働させていた、RAMに重要な証拠が含まれている可能性のある、頻繁に使用されていたワークステーションから証拠を収集する最善の方法を決定しなければならなかった。ローラは、収集できる証拠を最大化するために、どのようなデータ収集戦略を採用すべきだろうか？

- A. キーファイルを外部ストレージデバイスにコピーします。
- B. ネットワーク経由のリモート取得。
- C. 稼働中のワークステーションからのライブ取得。
- D. ワークステーションをシャットダウンした後、取得が失敗しました。

正解: ([正解を表示します](#))

Since the workstation is running and may contain critical evidence in RAM, live acquisition allows capturing volatile data such as active processes and memory contents before it is lost.

質問: 195

フォレンジック調査官が、OSのインストールに失敗し、マスターブートレコード(MBR)またはパーティションセクタが破損したコンピュータに遭遇しました。ディスク内のファイルと情報を検索して復元できるツールは次のうちどれですか？

- A. ネットキャット
- B. R-Studio
- C. Wireshark
- D. ヘリックス

正解: ([正解を表示します](#))

質問: 196

法医学調査員のソフィアは、画像と疑われるファイルを分析しています。彼女はファイルの16進数シグネチャを調べて形式を特定しようとしています。調査の結果、ファイルの最初の3バイトが16進数で47 49 46であることに気がきました。この情報に基づいて、このファイルの画像形式として最も可能性が高いのはどれでしょうか？

- A. PNG
- B. BMP
- C. GIF
- D. JPEG

正解: ([正解を表示します](#))

According to the CHFI v11 Computer Forensics Fundamentals and File Analysis modules, identifying file types using file signatures (magic numbers) is a core forensic technique. File extensions can be easily manipulated by attackers as an anti-forensics tactic, so investigators rely on hexadecimal headers to determine the true file format.

The hexadecimal sequence 47 49 46 corresponds to the ASCII characters "GIF". This signature appears at the beginning of all Graphics Interchange Format (GIF) files and is typically followed by version identifiers such as GIF87a or GIF89a. CHFI v11 explicitly lists GIF file headers as a common example when teaching file signature verification using hex editors.

For comparison:

PNG files start with the signature 89 50 4E 47

BMP files start with 42 4D (ASCII "BM")

JPEG files typically start with FF D8 FF

Because the investigator observes 47 49 46 at the beginning of the file, this conclusively identifies the file as a GIF image, regardless of its filename or extension.

CHFI v11 emphasizes that hexadecimal signature analysis is essential when investigating disguised files, malware hidden as images, or data exfiltration attempts using file extension mismatch techniques.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> **637**問、**30%**ディスカウント、特別な割引コード: **JPNshiken**」

質問: 197

金融機関のコンピュータフォレンジック調査において、GLBA(グラム・リーチ・ブライリー法)で保護されている顧客データへの不正アクセスが疑わしい活動として発見され、顧客の安全に対する懸念が高まっています。しかし、侵害の発生源と範囲を特定することは非常に困難であり、GLBAガイドラインの遵守を困難にしています。

機密性の高い顧客データへの不正アクセスが発見された場合、GLBAの対象となるコンピューターフォレンジック調査ではどのような手順を踏む必要がありますか？

- A. 金融活動に直接的な脅威がない場合は、インシデントを無視します。
- B. 分析のために情報を第三者と共有します。
- C. 影響を受ける顧客に通知せずに法執行機関に通知します。
- D. 影響を受ける顧客にオプトアウトの権利を通知し、データを保護します。

正解: ([正解を表示します](#))

According to CHFI v11 objectives under Computer Forensics Fundamentals and Regulations, Policies, and Ethics , a forensic investigator must ensure that technical investigation activities align with applicable legal and regulatory requirements. The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions protect customers' nonpublic personal information (NPI) and respond appropriately to any unauthorized access or disclosure.

When a breach involving GLBA-protected data is identified, the organization must follow a structured incident response and forensic investigation process while maintaining compliance with privacy laws. CHFI v11 emphasizes forensic readiness, legal compliance, and ethical handling of digital evidence. Notifying affected customers of their opt-out rights and implementing safeguards to protect compromised data are core requirements of GLBA's Privacy Rule and Safeguards Rule. Ignoring the incident violates forensic and legal responsibilities, while sharing sensitive data with third parties risks further disclosure. Informing law enforcement alone is insufficient if customer notification obligations are not met. Proper customer notification demonstrates due diligence, supports transparency, and reduces legal risk. From a CHFI perspective, this approach ensures lawful evidence handling, regulatory compliance, and preservation of organizational credibility during forensic investigations.

質問: 198

ウェブサイトのフォレンジック調査中に、アナリストはIISログエントリを調べてウェブトラフィックに関する情報を収集します。ログエントリには次のような内容が示されています。

2023-07-12 06:11:41 192.168.0.10 GET /images/content/bg_body_1.jpg - 80 - 192.168.0.27
Mozilla/12.0+ (Windows+NT+6.3;+WOW64)+AppleWebKit/537.36+(KHTML,+like
+Gecko)+Chrome/48.0.2564.103
+サファリ/537.36

http://www.techsite.com/assets/img/logo.png

200 0 0 365

アナリストは値を含むフィールドを特定する必要がある

http://www.techsite.com/assets/img/logo.png

ログエントリに。

この値は次のどのフィールドに属しますか？

A. cs(Referer)

B. server port

C. cs-method

D. cs(User-Agent)

正解: [\(正解を表示します\)](#)

According to the CHFI v11 Network and Web Application Forensics objectives, IIS (Internet Information Services) logs are a primary source of evidence for reconstructing web activity, identifying attack paths, and understanding user behavior. IIS logs follow the W3C Extended Log File Format, where each field represents a specific attribute of the HTTP request or response. The field cs(Referer) records the referring URL, which indicates the web page from which the client accessed the requested resource. In this scenario, the value

http://www.techsite.com/assets/img/logo.png

represents the page that referred the request for /images/content/bg_body_1.jpg. This information is crucial in forensic investigations to determine navigation paths, embedded content usage, malicious redirects, cross-site scripting attempts, or unauthorized resource loading.

質問: 199

鑑識捜査官のリアムは、容疑者のWindows 11マシンから情報を抽出する任務を負っています。彼は、容疑者の活動に関する情報が含まれている可能性のあるSticky Notesアプリケーションから関連データを調べる必要があります。この目的を達成するために、リアムはPythonを使用してSticky Notesデータベースファイルにアクセスし、分析用のデータを抽出することにしました。リアムは、容疑者のWindows 11システム上でSticky Notesデータベースファイルを見つけるために、次のうちのどのパスを使用すべきでしょうか？

A. C:\Program Files\Microsoft Sticky Notes\plum.sqlite

B. C:\Users\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState\plum.sqlite

C. C:\Users\Documents\StickyNotes.db

D. C:\Windows\System32\plum.sqlite

正解: B ([コメントを发表する](#))

On Windows 10/11, Sticky Notes stores its data in a SQLite database named plum.sqlite within the user's AppData Local Packages directory. This path contains the application's LocalState folder where the database file resides, making it the correct location for forensic extraction.

質問: 200

多国籍企業において、イントラネットからのシステムクラッシュやデータ漏洩の報告が増加している。フォレンジック調査官は、ネットワーク全体に拡散している高度に多形性のワームを発見した。このワームは構造を急速に変化させるため、その挙動を分析してシグネチャを作成することが困難である。サイバーセキュリティアナリストのスーザンは、安全で管理された環境でワームの挙動分析を実施する必要がある。彼女はこの目的のために、次のうちのどのツールを使用すべきか？

- A. IDA Pro
- B. Wireshark
- C. プロセスモニター
- D. カッコウサンドボックス

正解: ([正解を表示します](#))

Cuckoo Sandbox provides an isolated environment where the polymorphic worm can be safely executed and its behavior observed. This enables detailed behavioral analysis despite the worm's changing structure.

質問: 201

ジェフは政府機関のサイバーセキュリティ部門に所属する鑑識調査官です。ジェフは、政府機関のウェブアプリケーションに対するDDoS攻撃に関与したWindows 10コンピュータのメモリダンプを取得する任務を負っています。ジェフはメモリ収集のため現場に赴いています。ジェフはどのようなツールを使用できるでしょうか？

- A. 変動性
- B. 解剖
- C. メムチェック
- D. RAMフォルダ

正解: ([正解を表示します](#))

質問: 202

大規模な組織的サイバー攻撃を受け、多国籍企業はベテランのフォレンジック調査員であるリサに協力を依頼した。攻撃は同社のMSSQLサーバーに侵入し、リサは、この侵害が複数のソースと場所から同時に実行された高度なSQLインジェクション手法によるものと疑っていた。攻撃の発生源を特定するため、リサはMSSQLサーバー上の証拠ファイルを収集するだけでなく、調査する必要がある。この侵害の規模と巧妙さに対処するために、リサはどのツールに頼るべきだろうか？

- A. ネッソス
- B. エンケース
- C. SQLsus
- D. Sqlmap

正解: ([正解を表示します](#))

sqlmap is specifically designed to automate detection and exploitation of SQL injection vulnerabilities and supports advanced techniques, including handling complex, multi-source attacks. It enables analysis of MSSQL databases, extraction of data, and reconstruction of attack patterns, making it well-suited for investigating sophisticated SQL injection breaches.

質問: **203**

フォレンジック調査員のノラは、潜在的な内部脅威の調査の一環として、侵害を受けたシステムの Windows レジストリを調査しています。彼女は、ユーザーが最後にアクセスしたフォルダを特定したいと考えています。レジストリを確認した結果、特定のレジストリキーに、ユーザーが最近アクセスしたフォルダに関する情報(フォルダ名やファイルシステム内のパスなど)が格納されていることを発見しました。彼女の調査結果に基づき、この情報が含まれているレジストリキーは次のどれですか？

- A. BagMRU キー
- B. MRUListEx キー
- C. バッグキー
- D. NodeSlot 値

正解: ([正解を表示します](#))

According to the CHFI v11 Operating System Forensics objectives, the Windows Registry is a critical source of evidence for reconstructing user activity, particularly in insider threat investigations. One of the most important Registry artifacts for identifying recently accessed folders is the BagMRU key.

The BagMRU key is part of the Windows ShellBags artifact structure and is specifically designed to track folder navigation history. It stores hierarchical information about folders accessed by a user, including folder names, directory paths, and access order relationships. These keys allow forensic investigators to determine which directories a user browsed, even if the folders were accessed via Windows Explorer and later deleted from the system.

While the MRUListEx value exists within ShellBag-related keys, it only defines the order of access and does not store the actual folder path or name. The Bags key, on the other hand, stores folder view settings such as icon size, window position, and display preferences--not access history. The NodeSlot value is associated with Jump Lists and application usage tracking rather than directory navigation.

質問: **204**

重要な調査において、フォレンジック専門家は、dd コマンドを用いてルート化された Android デバイス上で物理的なデータ取得を行うことを目指しています。この方法は、隠しファイルや削除済みファイルを含むすべてのデータの包括的な複製を保証するため、正確な実行が求められます。dd コマンドを用いたルート化された Android デバイス上での物理的なデータ取得には、どのような手順が含まれますか？

- A. 安全な接続を確立し、ルート ディレクトリに移動して、DD をリモートで実行します。

- B. カスタム ハードウェアを使用して直接接続し、DD を実行して取得します。
- C. Bluetooth 経由で接続し、ルート アクセスを取得し、ソースと宛先を指定して DD を実行します。
- D. デバイスを接続し、ルートシェルを取得し、ソースと宛先を識別して、DD を実行します。

正解: ([正解を表示します](#))

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.

質問: 205

捜査官は、データ漏洩の疑いがあるデジタルフォレンジック案件に取り組んでいます。捜査官は、容疑者のハードドライブからデータを取得する任務を負っています。データ抽出プロセスを開始する前に、捜査官はドライブからすべての機密データを安全に削除します。ドライブから残留データが復元できないようにするため、捜査官はドライブ上のデータを連続した0と1で上書きする方法を適用し、捜査のプライバシーと整合性を保護します。捜査官はどのフォレンジックデータ取得手順を実行していますか？

- A. 完全かつ正確なデータ収集を保証するためにデータ取得を検証します。
- B. システムから一時的なライブ データをキャプチャするために揮発性データを取得します。
- C. 障害発生時にバックアップ手順が確実に実施されるように、緊急時対応計画を立てます。
- D. 対象メディアをサニタイズして、コンテンツを回復不可能にします。

正解: D ([コメントを发表する](#))

According to the CHFI v11 Data Acquisition Concepts and Rules , sanitizing the target media is a critical preparatory step performed before acquiring forensic data, especially when reusing storage media or handling sensitive information. Sanitization refers to the process of securely erasing data so that it cannot be recovered using forensic techniques. This is typically achieved by overwriting the storage media with predefined patterns , such as sequential zeros and ones, or by using approved data wiping algorithms.

CHFI v11 clearly distinguishes sanitization from other acquisition steps. Validating data acquisition ensures the integrity and completeness of collected evidence through hash verification and comparison, not data destruction. Acquiring volatile data focuses on capturing live information such as RAM contents, running processes, and network connections before shutdown. Planning for

contingency involves preparing backups, alternate tools, and procedures in case the acquisition process fails.

The scenario explicitly describes overwriting the drive to prevent any residual data recovery, which directly aligns with the CHFI v11 guideline "Sanitize the Target Media" listed under evidence handling and acquisition best practices. This step ensures privacy, prevents data leakage, and maintains legal and ethical compliance during forensic operations.

Therefore, based strictly on CHFI v11 objectives and terminology, the investigator is performing sanitization of the target media , making Option D the correct and verified answer.

質問: 206

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。

正解: D ([コメントを发表する](#))

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.

有効的な**312-49v11-JPN**問題集はJPNTTest.com提供され、**312-49v11-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**312-49v11-JPN**試験問題集を提供します。JPNTTest.com 312-49v11-JPN試験問題集はもう更新されました。ここで**312-49v11-JPN**問題集のテストエンジンを手に入れます。最新版のアクセ

ス、<https://www.jpntest.com/shiken/312-49v11-JPN-mondaishu> 637問、30%ディスカント、
特別な割引コード: **JPNshiken**」