EC-COUNCIL.312-49v11-JPN.v2026-08-17.q135

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：	135
バージョン：	v2026-08-17
ページの閲覧量：	104
問題集の閲覧量：	1355

https://www.jpnshiken.com/shiken/EC-COUNCIL.312-49v11-JPN.v2026-08-17.q135.html

質問: **1**
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: **D** (コメントを発表する)
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.

質問: **2**
鑑識捜査において、捜査官は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る。
調査員は、ファイルの内容を分析する中で、「00」と「FF」というバイト値がファイル内の様々な箇所に散在していることに気づいた。これらのバイト列は繰り返し出現し、ファイルの大部分を占めている。ファイル分析の観点から、これらの値はどのような意味を持つ可能性があるだろうか？
A. 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。
B. 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配置に達するようにするために使用されます。
C. 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。
D. 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、適切なキーでのみ復号化できます。
正解: **(正解を表示します)**
Option B is the best answer because repeated runs of 00 and FF values across large sections of a file often indicate padding, erased space, alignment bytes, or unused regions rather than meaningful user content.
CHFI v11 includes Understanding Hex Editors and Hexadecimal Notation , OFFSET , and Hex View of Popular Image File Formats and other file formats, so candidates are expected to interpret repeated byte patterns in forensic hex analysis.
In practice, filler bytes are commonly used to pad structures to expected boundaries or to fill slack or reserved regions in a file or data structure. Repeated 00 bytes are especially common as null padding, while FF bytes may appear in erased or filled areas depending on the application, medium, or format. These patterns alone do not automatically prove corruption, encryption, or compression.
Data corruption usually requires stronger evidence than repeated filler values.
Compression and encryption tend to produce more varied or high-entropy byte patterns rather than long simple repetitive runs. Therefore, under CHFI's file-format and hex-analysis objectives, the most reasonable interpretation is file padding or unused data .

質問: **3**
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調査を依頼した。攻撃は同社のMSSQLサーバーに侵入し、リサは複数のソースと場所から同時に実行された高度なSQLインジェクション攻撃が原因だと疑っていた。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、調査する必要があった。この攻撃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. Sqlmap

B. ネッソス
C. ケース化
D. SQLsus
正解: **(**正解を表示します**)**
Option C. EnCase is the best answer because the question is about a forensic investigation of an MSSQL server where Lisa needs to collect and examine evidence files in a defensible manner. CHFI v11 explicitly includes SQL Server Logs , Investigating SQL Injection , and broad use of forensic tools for acquisition and examination of digital evidence.
Among the choices, EnCase is the forensic suite most appropriate for evidence collection, preservation, and detailed analysis . It supports imaging, examination, and evidentiary workflow, which are central to determining attack origin in a legally sound way. Sqlmap and SQLsus are offensive or testing-oriented tools associated with SQL injection activity, not primary forensic evidence examination platforms. Nessus is a vulnerability scanner, useful for assessment but not the best answer for collecting and analyzing MSSQL evidence after a breach.
Because the scenario centers on forensic examination of compromised database-server evidence, the strongest CHFI-aligned answer is EnCase , not exploit or scanning tools. It best supports evidence preservation, analysis, and reporting in a large-scale SQL-injection investigation.

質問: **4**
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ら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.
The other options describe forensic analysis steps that occur after legal access has been granted. Performing them without authorization could invalidate evidence and expose the investigator to legal liability. Therefore, consistent with CHFI v11 best practices and legal requirements, seizing the computer and email accounts is the correct initial step before proceeding with the forensic examination.

質問: **5**
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: **(**正解を表示します**)**
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.

Option A focuses on confidentiality, which is important but does not address post-investigation communication. Option B applies to pre-engagement planning rather than post-investigation reporting. Option D relates to legal review, which may be necessary in some cases but is not the core activity described.
The CHFI Exam Blueprint v4 highlights effective reporting and client communication as key competencies of a forensic investigator, making the feedback and debriefing process the most accurate and exam-aligned answer

質問: **6**
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、システムにさらなる損傷が生じ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互換形式に変換します。
B. Linuxエミュレータを使用して画像を表示します。
C. 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。
D. 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 ツールを展開します。
正解: **(**正解を表示します**)**
Option D is the best answer because the investigator needs a method that allows safe access to a Linux image on a Windows forensic workstation without risking further damage to the evidence. In CHFI methodology, the preferred approach is to use specialized forensic tools that can mount, parse, and inspect images in a read-only, forensically sound manner. That preserves the original evidence and supports controlled analysis.
Converting the image format could alter or complicate the evidence. A Linux emulator is not the most reliable forensic answer for viewing evidence safely on Windows. Using a live boot disk is more appropriate for examining a live system or booting a machine, not for safely inspecting an already acquired image from within a forensic workstation workflow.
Because the problem is specifically about safe evidence handling, cross-platform access, and avoiding further damage, the most effective CHFI-aligned approach is to use a specialized forensic tool designed to view Linux images on Windows . This allows structured analysis, file-system interpretation, and artifact review while preserving evidence integrity.

質問: **7**
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.
Therefore, the correct and CHFI-verified answer is ftp.response.code == 530 (Option C) .

質問: **8**
あなたは、世界的なサイバーセキュリティ企業に所属する、一流のフォレンジック調査官です。最近、大規模なネットワークインフラストラクチャの侵害に関わる重大な事件を担当することになりました。数日にわたる徹底的な調査の結果、サーバー上で奇妙なコードを発見し、初期分析の結果、それが新型マルウェアであることが判明しました。このマルウェアは複数のアンチウイルスプラットフォームで検出率が低く、高度な脅威となっています。ネットワークを危険にさらすことなく、マルウェアの挙動を評価するための制御された環境を構築する必要があります。どのようなアプローチを採用すべきでしょうか？
A. 分析中の帯域幅を向上させるため、感染したサーバーをパブリックネットワークに接続してください。
B. 会社のメインネットワーク内の稼働中のシステム上でマルウェアを分析します。

C. 専用のネットワークセグメントを設定し、それをメインネットワークから切断し、トラフィック監視ツールを使用してマルウェアの挙動を評価します。
D. 感染したサーバーをハニーポットとして使用し、他の脅威アクターを引き寄せ、その行動を分析します。
正解: **(**正解を表示します**)**
Option C is the best answer because malware analysis should be performed in a controlled and isolated environment that prevents the sample from escaping, spreading, or communicating freely with production systems. In CHFI malware forensics, investigators are expected to understand the importance of a malware analysis lab , including sandboxing, network isolation, and controlled monitoring of system and traffic behavior.
A dedicated isolated network segment allows the examiner to watch how the malware behaves while keeping the main corporate network protected. Using a traffic monitoring tool within that isolated environment helps reveal command-and-control attempts, download behavior, beaconing, DNS lookups, or other suspicious actions. This is the safest and most informative approach.
The other options are dangerous or inappropriate. Connecting the infected server to a public network increases risk. Running the malware inside the main network is unsafe. Turning the infected server into a honeypot is not a sound first response for this scenario.
Therefore, the correct CHFI-aligned answer is to use an isolated analysis environment with monitored traffic .

質問: **9**
多国籍企業のフォレンジックチームが、データ漏洩の疑いについて調査を行っています。システムログを徹底的に調査した結果、チームは内部システムからダークウェブ活動に関連する疑わしいIPアドレスへの一貫したアウトバウンドトラフィックを発見しました。該当システムを調査したところ、ユーザーが許可されていない活動にTORを使用していたことが判明しました。TORの使用に関するさらなる証拠を収集するために、次のうち、実質的な成果が得られる可能性が最も低い手法はどれでしょうか？
A. プリフェッチファイルをスキャンして、TOR実行のインスタンスを検出します。
B. Windowsレジストリを検査してTOR関連のエントリを探します。
C. リアルタイムのネットワークトラフィックを監視して、TORノードへの接続を特定します。
D. TOR関連のコマンドの痕跡についてコマンドプロンプトの履歴を分析しています。
正解: **(**正解を表示します**)**
Option D is the best answer because it is the technique least likely to produce substantial evidence of TOR usage in a typical enterprise workstation investigation. CHFI v11 includes Dark Web Forensics , Windows artifact analysis , registry analysis , prefetch analysis , and network traffic analysis as relevant forensic areas. In that context, investigators are expected to prioritize artifacts that commonly record application execution, persistence, and network behavior.

Prefetch files can show whether the TOR executable was launched on a Windows system. The Windows Registry may contain installation traces, user activity references, or other application-related entries. Real- time or captured network traffic can also reveal communications with TOR entry nodes, relays, or patterns consistent with anonymized traffic. These are all recognized and productive artifact sources in a CHFI-style investigation.
By contrast, Command Prompt history is much less reliable because TOR is commonly used through the TOR Browser GUI , not through command-line execution. Unless the user specifically launched TOR- related commands manually, command history may contain nothing useful. Therefore, from a forensic- efficiency standpoint, this is the weakest option.

質問**: 10**
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 time-stomping 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.
The other tools are not appropriate for this task. Regshot is used to compare Windows Registry snapshots, OSForensics is a general forensic suite but is not specifically optimized for low-level MFT timestamp comparison, and Process Explorer is a live system monitoring tool focused on running processes rather than file system metadata.

CHFI v11 explicitly emphasizes NTFS MFT analysis as the authoritative method for identifying manipulated timestamps. Therefore, the most accurate and CHFI-aligned tool for detecting timestamp modifications on NTFS file systems is analyzeMFT , making Option A the correct answer.

質問**: 11**
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 (**コメントを発表する**)**
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.
Options B and C rely on case manipulation and keyword splitting , which are evasion techniques but not double encoding . Option D uses hex-encoded control characters , which is a different obfuscation method and does not represent double URL encoding.
CHFI v11 explicitly highlights double encoding as a common technique used in SQL injection attacks to evade detection and filtering mechanisms. Therefore, the URL that clearly demonstrates double-encoded SQL injection payloads is Option A , making it the correct and CHFI-aligned answer.

質問: **12**
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.
Therefore, the file that contains geolocation data of applications and system services on iOS devices-fully aligned with CHFI v11-is Clients.plist , making Option D the correct answer.

質問: **13**
CHFIの専門家であるシンシアは、多国籍企業のデータ漏洩に関わる重大な事件を担当している。
彼女は調査対象を、侵害されたデータが保存されていると思われる特定のサーバーに絞り込んだ。
しかし、そのサーバーは会社の業務に不可欠なものであり、通常のシステム停止による買収のために停止させることはできません。シンシアはシステムの不安定性を考慮し、適切にデータを取得しなければ重要なデータが失われる可能性があることを認識します。調査に必要な証拠を効果的に収集するために、シンシアは次にどのような行動をとるべきでしょうか？

A. IT部門に分析用のサーバーバックアップを作成するよう依頼してください。
B. 勤務時間外にデッド取得を実施する。
C. ネットワークスニッフィングを使用して受動的にデータを収集します。
D. 直ちにライブキャプチャを実行してください。
正解: **D** (コメントを発表する)
Option D is the best answer because the server is still operational , cannot be shut down , and may contain volatile evidence that could disappear quickly. Under CHFI principles, when a system must remain running and critical data in memory or live state may be lost, the investigator should perform a live acquisition while respecting the order of volatility . This is exactly the kind of situation where live acquisition is required. It allows the examiner to collect RAM contents, active processes, network connections, logged-in sessions, open files, and other transient artifacts that would be lost if the system were powered down or delayed. Since the question explicitly highlights volatility, immediate live acquisition is the most appropriate forensic response.
Option A is not a substitute for forensic acquisition because ordinary backups do not necessarily preserve volatile evidence or forensic integrity in the same way. Option B delays the response and risks losing critical data. Option C may provide useful supporting network information, but it does not capture the server's internal volatile state. Therefore, the correct CHFI-aligned next step is to conduct a live acquisition immediately .

質問: **14**
あなたは法執行機関の鑑識官として、違法なダークネット市場の事件を捜査しています。容疑者のコンピュータは押収されており、あなたは容疑者のハードディスクからデータを取得する任務を負っています。証拠メディアの改ざんを防ぐため、書き込み保護を有効にする必要があることは理解しています。しかし、コンピュータのOSはLinuxであり、あなたの書き込みブロックツールはLinuxと互換性がありません。どのように進めるべきでしょうか？
A. Linux マシンから Windows マシンにデータを転送し、書き込みブロックを適用します。
B. ハードディスクをWindowsマシンに接続し、書き込みブロックツールを適用します。
C. ツールの非互換性を考慮して、書き込みブロックなしでデータ取得を進めます。
D. Linux互換コマンドを使用して、ハードディスクを読み取り専用に手動で設定します。
正解: **D** (コメントを発表する)
Option D is the best answer because CHFI v11 explicitly requires investigators to enable write protection on the evidence media as part of the acquisition methodology. The blueprint lists this step directly under Data Acquisition Methodology , along with selecting the acquisition tool, collecting volatile and non-volatile data, and validating the acquisition. If the standard write-blocking tool is incompatible with Linux, the examiner should still preserve the evidence by using an appropriate Linux-compatible read-only method rather than abandoning write protection altogether. Proceeding without write protection risks altering original evidence and violating core forensic best practices. Likewise, transferring

data first or attaching the drive to another machine without a controlled read-only approach can introduce unnecessary risk or change the evidence state.
CHFI's rules of thumb for acquisition focus on preserving original evidence and choosing the best acquisition method for the system state and environment. In this situation, the correct adaptation is to use a Linux command or method that sets the disk to read-only so the acquisition remains forensically sound. That makes option D the strongest CHFI-aligned answer.

質問: **15**
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.
The other options are unsuitable: Camtasia is a screen recording tool, Rufus is used for creating bootable USB drives, and Dundas BI is a business intelligence and data visualization platform. None provide binary-level forensic analysis functionality. Therefore, consistent with CHFI v11 registry and binary forensic analysis practices, Hex Workshop is the most appropriate tool for examining registry files in this scenario.

質問: **16**

システム管理者は、重要なアプリケーション向けに新しいストレージアレイを構成しており、データストライピングと専用パリティを使用するRAIDレベルを選択します。このRAID構成では、最低3台のディスクが必要で、データがバイトレベルで複数のドライブにストライピングされ、1台のドライブが耐障害性のためのパリティ情報を格納するために確保されます。RAIDシステムの構成後、管理者は単一ドライブの障害に対する耐性をテストし、データ損失なしでシステムが引き続き機能することを確認します。このシナリオでシステム管理者が使用しているRAIDレベルはどれですか？

A. RAID 1
B. RAID 3
C. RAID 10
D. RAID 0

正解: **B** (コメントを発表する)

Option B. RAID 3 is the correct answer because the question describes a RAID level that uses byte-level striping with a dedicated parity disk and requires at least three disks . That combination matches RAID 3.

CHFI v11 explicitly includes RAID Storage System , RAID and Virtualization , and the broader understanding of storage structures under digital evidence fundamentals, so candidates are expected to recognize RAID types and how they affect evidence acquisition and recovery.

The key clues are the dedicated parity drive and the fact that the system can continue functioning after a single disk failure . RAID 3 is designed to provide fault tolerance for one failed drive by reconstructing data from the remaining striped disks and the parity information. This makes it different from RAID 0 , which has no redundancy, RAID 1 , which mirrors data rather than using dedicated parity, and RAID 10 , which combines striping and mirroring in a different way.

Because the scenario precisely describes byte-level striping plus one parity disk with single-disk fault tolerance, RAID 3 is the only answer that fully fits the described configuration.

質問: **17**

ほとんどの従業員がMacBookを使用している組織でサイバーインシデントが発生した後、アレックスという名のフォレンジック調査員が、影響を受けたMacシステムの1つを分析する任務を負った。アレックスは、システムログ、アーティファクト、ファイルシステム、およびユーザーアクティビティを分析できる包括的なMacフォレンジックツールを必要としている。アレックスはどのようなツールを選ぶべきだろうか。
のお気に入りのツールは？
A. Wireshark
B. 磁石の公理
C. メタスプロイト
D. IDA Pro
正解: **(正解を表示します)**
Option B. Magnet AXIOM is the best answer because CHFI v11 explicitly includes MAC Forensic Tools , Collecting and Analyzing macOS Artifacts , Analyzing macOS User Activities , Viewing Log Messages in Mac , and APFS file system analysis as important objectives for operating system forensics.
The question asks for a comprehensive Mac forensic tool that can handle system logs, artifacts, file systems, and user activity. Among the options, Magnet AXIOM is the one that best fits that broad forensic role.
Wireshark is a network traffic analysis tool, not a full Mac forensic suite. Metasploit is a penetration testing and exploitation framework, not an evidence-analysis platform. IDA Pro is used for reverse engineering binaries, which is far narrower than the full-system forensic requirement described here.
Because Alex needs a single tool capable of broad macOS evidence examination, the most suitable CHFI- aligned answer is Magnet AXIOM . It best matches the blueprint's focus on Mac artifact analysis, user activity reconstruction, and forensic tool use across operating systems.

質問: **18**
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.
The other options describe different forensic phases: case evaluation occurs earlier at a strategic level, scene assessment applies to on-site evidence handling, and data acquisition refers specifically to extraction activities. In contrast, documenting and prioritizing exhibits in a controlled environment is a core function of the laboratory assessment , making option C the correct ENFSI-aligned answer.

質問**: 19**
大手ソフトウェア企業のサイバーセキュリティチームは、自社インフラ内の複雑な感染システムネットワークを調査している。調査の結果、感染の根本原因と思われる単一のファイルが特定された。問題のマルウェアは新型と考えられており、これまでの情報は一切入手できていない。
その潜在的な能力と動作モードを理解するための、最も現実的な最初のステップは何でしょうか？
A. コード分析
B. 行動分析
C. 静的解析
D. 署名分析
正解**: (**正解を表示します**)**
Option C. Static Analysis is the best initial step. CHFI v11 covers malware forensics , including methods for examining suspicious files to understand their characteristics, indicators, and probable functions. When investigators encounter a novel malware sample with no prior intelligence available, the safest and most logical first step is usually static analysis . This allows the examiner to inspect the file without executing it , reducing the risk of further infection or unintended damage while still revealing useful information such as file type, strings, embedded resources, headers, imports, suspicious metadata, packing indicators, and other structural clues.

Behavioral analysis is also valuable, but it normally comes after an initial static examination because it requires executing or monitoring the sample in a controlled environment. Code analysis can be deeper and more specialized, but it is not always the first practical step, especially before basic triage. Signature analysis is less useful when the malware is believed to be new and may not yet match known indicators.
Therefore, under CHFI malware investigation principles, the most viable initial step to understand a previously unknown malicious file is static analysis before moving to more advanced dynamic techniques.

質問**: 20**
あなたはフォレンジック調査員として、容疑者のメール通信に関する事件の調査を任されています。調査中、容疑者のゴミ箱フォルダにあるメールに重要な証拠が含まれている可能性があることを発見しました。メールは.pstファイルに保存されており、削除されたものや破損とマークされたものも含め、関連するすべてのメールを抽出して分析する必要があります。データの整合性を確保するには、これらのファイルを効率的に処理し、削除されたメッセージを復元し、分析のためにメールの内容を明確に表示できるツールが必要です。
このタスクに最適なツールは次のうちどれでしょうか？
A. P2LOCATIONのメールヘッダートレーサー
B. メールフォルダ
C. ハンターのメール検証ツール
D. SysTools MailPro+
正解**: (**正解を表示します**)**
According to the CHFI v11 objectives under Email Forensics and Digital Evidence Analysis , investigators must be capable of extracting, recovering, and analyzing email data stored in proprietary formats such as Microsoft Outlook PST files . PST files often contain emails from Inbox, Sent Items, Trash, and Archive folders, and may include deleted or corrupted messages that are highly relevant to an investigation.
SysTools MailPro+ is a forensic-grade email analysis tool designed specifically to handle PST file processing and recovery . It allows investigators to open, parse, and analyze PST files while recovering deleted emails, attachments, and metadata such as headers, timestamps, sender/recipient details, and message paths. CHFI v11 emphasizes the importance of using tools that support evidence integrity, selective extraction, and comprehensive visibility into email contents, all of which are core capabilities of MailPro+.
The other options are not suitable for this task. P2LOCATION ' s Email Header Tracer focuses on tracing email headers for routing analysis, not PST recovery. Email Dossier and Hunter's Email Verifier are OSINT and email validation tools used for profiling and verification, not forensic extraction or recovery of mailbox data.
The CHFI Exam Blueprint v4 highlights email evidence acquisition, deleted email recovery, and PST analysis as key forensic competencies. Therefore, SysTools MailPro+ is the most appropriate and exam- aligned tool for this investigation

質問: **21**
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: **(**正解を表示します**)**
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.
The other options are incorrect. SMTP (Option A) is an email transmission protocol and unrelated to file sharing. iSCSI (Option B) is a block-level storage protocol used for SAN environments, not user-level file sharing. RAID (Option C) is a disk redundancy technology and does not control how files are accessed over the network.
The CHFI Exam Blueprint v4 highlights SMB/CIFS analysis as a key area for investigating shared storage environments, making it the correct and exam-aligned protocol for understanding file access on NAS devices

質問: **22**
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トポロジ
正解: **(**正解を表示します**)**
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.
Disk data and temporary file systems are far less volatile, as their contents persist after shutdown. Archival media is the least volatile and can be collected last. CHFI v11 explicitly teaches that investigators must document and capture volatile network and system configuration details before moving to persistent storage.
Therefore, prioritizing the physical configuration and network topology of the system is the correct and standards-compliant choice.

質問: **23**
フォレンジック調査員が、起動中に障害が発生したシステムを調査しています。調査員は、BIOSがシステムハードウェアを初期化した後に起動プロセスが中断されたことを発見しました。もし障害が発生していなかったら、起動プロセスの次のステップはどれだったでしょうか？
A. ブート マネージャーはブート可能なパーティションを見つけて MBR を読み込みます。
B. カーネルが起動し、システムのハードウェア抽象化レイヤー (HAL) がロードされます。
C. システムはブート パーティションから ntoskrnl.exe ファイルをロードします。
D. ブートローダーはオペレーティング システムのカーネルをロードします。
正解: **A (**コメントを発表する**)**
According to the CHFI v11 Operating System Forensics module, understanding the Windows boot process is essential for diagnosing boot failures and identifying potential tampering, rootkits, or boot-level malware.
In systems using the BIOS-MBR boot method , the boot sequence follows a well-defined order.
After the BIOS (Basic Input/Output System) completes hardware initialization and performs the Power-On Self-Test (POST), its next responsibility is to locate a bootable device based on the configured boot order.

Once a valid boot device is found, the BIOS loads the Master Boot Record (MBR) from the first sector of that device into memory and transfers execution control to it. This step is critical because the MBR contains the boot code responsible for locating the active partition and invoking the next stage of the boot process.
Only after the MBR executes does the Windows Boot Manager (bootmgr) load, followed later by the Windows OS loader (winload.exe), which then loads ntoskrnl.exe and the Hardware Abstraction Layer (HAL) . Therefore, options B, C, and D represent later stages in the boot process and could not occur immediately after BIOS initialization.
CHFI v11 explicitly covers this sequence under Windows Boot Process: BIOS-MBR Method , emphasizing that failures occurring immediately after BIOS initialization typically point to issues with the MBR or bootable partition discovery .
Hence, the correct and CHFI v11-verified answer is Option A: The boot manager would locate the bootable partition and load the MBR .

質問: **24**
ジェシカは、データ漏洩に関与した疑いのあるWindowsマシンに対してフォレンジック分析を行っています。彼女は、不審なログイン試行を特定し、ログイン失敗回数を追跡して、ブルートフォース攻撃が試みられたかどうかを確認したいと考えています。以下のイベントIDのうち、この情報を提供するものはどれですか？
A. 4727
B. 4732
C. 4758
D. 4625
正解: **(**正解を表示します**)**
Option D. 4625 is the correct answer because this Windows security event is associated with failed logon attempts , which is exactly what Jessica needs to review when looking for signs of a possible brute-force attack. CHFI v11 explicitly includes Types of Logon Events , Windows 11 Event Logs and Other Audit Events , Evaluating Account Management Events , and Event logs as core forensic topics.
In a brute-force scenario, investigators look for repeated failed authentication attempts over time, often tied to the same account, source, or system. The relevant audit evidence is found in Windows event logging, and failed logons are one of the most important indicators when examining suspicious authentication activity. This aligns directly with CHFI's emphasis on using logs as evidence and ensuring log credibility and integrity during an investigation.
The other event IDs listed are not the standard failed-logon event used for this purpose. Because Jessica is specifically trying to count and analyze failed login attempts , event ID 4625 is the best and most forensic- relevant choice under CHFI's Windows log analysis objectives.

質問: **25**

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: **D** (コメントを発表する)
Option D is the best answer because CHFI v11 explicitly includes Seeking Consent , Best Practices for Handling Digital Evidence , Legal Issues, Privacy Issues and Legal Compliance , and Managing Clients or Employers during Investigations .
When consent is not granted, the investigator cannot simply access sensitive client data on their own authority. At the same time, immediately withdrawing may not be the only appropriate response if there are lawful and ethical alternative ways to obtain relevant evidence without violating confidentiality. The CHFI- aligned approach is to respect the client's concerns , remain within legal and ethical boundaries, and explore other permissible evidence-gathering options, such as narrower collection scopes, anonymized review procedures, or additional legal authorization where appropriate.
Options A and B clearly violate consent and confidentiality principles. Option C is too absolute and does not reflect the possibility of lawful alternative approaches. Therefore, the strongest answer under CHFI's consent and legal-compliance principles is to respect the firm's concerns and seek other means of gathering evidence without breaching client confidentiality .

質問: **26**
大規模組織のサイバーセキュリティチームは、定期的なネットワーク監査中に、異常なネットワークトラフィックパターンと機密システムへの不正アクセス試行を検知しました。これは、セキュリティ侵害の可能性を示唆しています。インシデント対応プロセスフローに基づき、様々なサードパーティベンダーやクライアントにインシデントが報告された後、サイバーセキュリティチームが当面優先すべき対応は何でしょうか？
A. 封じ込め
B. 根絶
C. インシデントトリアージ
D. インシデントの記録と割り当て
正解: (正解を表示します)

According to the CHFI v11 Procedures and Methodology domain, the Incident Response Process Flow follows a structured sequence to ensure incidents are handled efficiently, lawfully, and with minimal impact.
Once an incident is detected and stakeholders such as management, third-party vendors, and affected clients are informed , the next immediate priority is containment .
Containment focuses on limiting the scope and impact of the incident to prevent further damage, data loss, or lateral movement by the attacker. This may include isolating affected systems, blocking malicious IP addresses, disabling compromised accounts, segmenting networks, or applying temporary firewall rules.
CHFI v11 emphasizes that containment must be executed swiftly to preserve evidence while stopping the ongoing threat.
The other options represent different phases of the incident response lifecycle. Incident triage and incident recording and assignment occur earlier, during detection and initial response. Eradication is a later phase that involves removing malware, closing vulnerabilities, and eliminating attacker persistence-but only after the threat has been successfully contained.
CHFI v11 explicitly states that failing to prioritize containment after notification can allow attackers to continue exploiting systems, leading to greater organizational and legal consequences. Therefore, the correct and CHFI v11-verified immediate priority is Containment , making Option A the correct answer.

質問**: 27**
IoTフォレンジック調査員として、あなたはスマートテレビやその他のIoTデバイスが侵害されたサイバー犯罪の捜査を任されています。この捜査では、ドローン、ウェアラブル、SDカードなど、様々なIoTデバイスからデータを抽出し、重要な証拠を収集する必要があります。Android、iOS、Tizen OSを搭載したモバイルデバイス、そしてチップオフメモリソースなど、これらのデバイスから物理的および論理的なデータ抽出を実行できるツールが必要です。この捜査に最適なツールは次のうちどれでしょうか？
A. ダブルスペース
B. MD-NEXT
C. エポックコンバータ
D. システムctl
正解**: (**正解を表示します**)**
This question maps directly to CHFI v11 objectives under Mobile and IoT Forensics and Tools for IoT Device Forensics . IoT investigations often involve heterogeneous devices with different operating systems, storage mechanisms, and acquisition challenges. CHFI v11 emphasizes the need for specialized forensic tools that support both logical and physical extraction , including advanced techniques such as chip-off and SD card analysis, to ensure comprehensive evidence collection.

MD-NEXT is a purpose-built digital forensic tool designed for mobile and IoT investigations. It supports forensic acquisition and analysis across a wide range of platforms, including Android, iOS, Tizen OS, wearables, drones, smart TVs, and removable media. Importantly, MD-NEXT provides capabilities for logical extraction, physical imaging, file system parsing, and chip-off memory analysis, which are critical when dealing with damaged, locked, or non-standard IoT devices.
The other options are not suitable for this scenario. DoubleSpace is a disk compression utility, EpochConverter is used for timestamp conversion, and Systemctl is a Linux service management command.
None provide forensic acquisition capabilities. Therefore, MD-NEXT is the most suitable and CHFI v11- aligned tool for comprehensive IoT and mobile device forensic investigations.

質問**: 28**
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: **29**
デジタルフォレンジック調査員は、ペンドライブから抽出されたNTFSイメージファイルの分析を任されています。彼らはこの作業にThe Sleuth Kit(TSK)を活用し、特にfsstatコマンドラインツールを活用します。fsstatを使用することで、メタデータ、inode番号、ブロック情報、クラスタ情報といったファイルシステムの詳細な情報まで掘り下げ、包括的な調査を可能にします。
調査員はどのようにして TSK を使用してディスク イメージを分析できるのでしょうか?
A. ネットワークスキャンを実行することによって
B. 手動検査を実施することで
C. プラグインフレームワークを使用することで
D. カスタムコードを記述することで
正解: **(正解を表示します)**
According to the CHFI v11 Operating System Forensics and Digital Evidence Analysis objectives, The Sleuth Kit (TSK) is a core open-source forensic framework used to analyze disk images and file systems , including NTFS, FAT, EXT, and others. TSK is designed as a modular toolkit , offering both command-line utilities (such as fsstat, fls, and istat) and a plug-in framework that enables structured, extensible analysis.
The fsstat tool is part of this framework and is used to extract file system metadata , including cluster size, inode structure, allocation status, and volume layout-key artifacts required for timeline reconstruction and anomaly detection. CHFI v11 emphasizes that investigators typically analyze disk images using TSK's plug- in-based architecture , which allows multiple forensic modules to operate consistently on the same evidence source without altering it. This architecture is also what enables higher-level forensic platforms (such as Autopsy) to integrate TSK seamlessly.
The other options are incorrect. TSK does not perform network scans , nor does it rely on unstructured manual inspection . While TSK provides APIs for developers, writing custom code is not required for standard disk image analysis and is not the primary method emphasized in CHFI v11.
Therefore, in alignment with CHFI v11, an investigator analyzes disk images using TSK through its plug-in framework , making Option C the correct answer.

質問: **30**
容疑者のAndroidデバイスに対するデジタルフォレンジック調査において、フォレンジック専門家は閲覧履歴、Cookie、キャッシュデータといったChromeの痕跡を抽出する任務を負います。容疑者はサイバー犯罪に関連する閲覧活動にChromeを使用していた可能性があり、捜査官はデバイスからこの種の情報を効率的に抽出できるツールを必要としていま

す。Androidデバイスからこれらの Chrome の痕跡を抽出するために捜査官を支援できるツールは次のうちどれですか？
A. LOIC
B. オーボットプロキシ
C. ドロイドシープ
D. マグネット公理
正解: **(**正解を表示します**)**
Under the CHFI v11 Mobile and IoT Forensics domain, investigators are required to extract and analyze application-level artifacts from mobile devices to reconstruct user activity. Web browsers such as Google Chrome store valuable forensic data on Android devices, including browsing history, cookies, cached files, saved form data, session tokens, and timestamps , which can be critical in cybercrime investigations.
Magnet AXIOM is a comprehensive digital forensics platform explicitly supported and referenced in CHFI v11 for mobile device forensic analysis . It is capable of performing logical and file system extractions from Android devices and includes built-in parsers for Chrome artifacts . Magnet AXIOM can automatically locate Chrome databases (such as History, Cookies, and cache directories), decode SQLite databases, and present the extracted data in a forensically structured and timeline-based view. This makes it highly effective for correlating browser activity with other evidence.
The other tools listed are not suitable for this task. LOIC is a network stress-testing/DoS tool, Orbot Proxy is used to route traffic through the Tor network, and DroidSheep is a network sniffing tool for session hijacking. None of these tools are designed for forensic extraction or analysis of browser artifacts from Android devices.
Therefore, in alignment with CHFI v11 Mobile and IoT Forensics objectives , the correct and most suitable tool for extracting Chrome artifacts from an Android device is Magnet AXIOM , making Option D the correct answer.

質問**: 31**
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**: (**正解を表示します**)**

This scenario aligns with CHFI v11 objectives under Computer Forensics Fundamentals and Insider Threat and Identity Theft Forensics . One of the defining characteristics of an insider threat is that the attacker already possesses authorized or legitimate access to internal systems, applications, or sensitive data. CHFI v11 emphasizes that insider attacks often bypass perimeter defenses because the malicious activity originates from trusted accounts, internal IP ranges, or authenticated sessions.
If sensitive data is altered from within the organization's network using valid credentials, it strongly suggests insider involvement. Insiders may include disgruntled employees, contractors, or partners who misuse their access privileges intentionally or unintentionally. This type of breach is often detected through anomalies in user behavior, access logs, privilege misuse, or violations of least-privilege principles.
The other options point to external attack indicators. Social engineering typically targets users from outside the network, known external IP addresses suggest external threat actors, and DDoS attacks are characteristic of external disruption rather than internal data manipulation. CHFI v11 highlights that distinguishing insiders from external attackers is critical for attribution, legal action, and remediation. Therefore, legitimate internal access to systems and data is the strongest indicator that the breach was carried out by an insider.

質問: **32**
Web アクセシビリティの領域には、標準的な検索エンジンで簡単にアクセスでき、インデックスも作成されるサーフェス Web、機密データベースやプライベート ポータルなどのインデックスが作成されていないコンテンツが含まれるディープ Web、そして、麻薬密売やサイバー犯罪などの違法行為に関係することが多い秘密の環境であるダーク Web の 3 つのレイヤーがあります。ダーク Web には Tor などの専用ブラウザーからアクセスできます。
ダーク ウェブとサーフェス ウェブやディープ ウェブの違いは何ですか?
A. 法的書類と財務記録が含まれています。
B. 暗号化により完全な匿名性を実現します。
C. アクセスするには認証が必要です。
D. 検索エンジンによってインデックスされます。
正解: **B** (コメントを発表する)

According to the CHFI v11 Dark Web Forensics objectives, the defining characteristic that distinguishes the Dark Web from both the Surface Web and the Deep Web is its ability to provide strong anonymity through layered encryption and anonymization techniques . The Dark Web is intentionally designed to conceal the identities and locations of users, services, and hosting infrastructure.
Access to the Dark Web typically requires specialized software such as the Tor Browser , which routes traffic through multiple encrypted relay nodes (entry, middle, and exit relays). This process, known as onion routing , ensures that no single node knows both the source and destination of the communication. CHFI v11 explicitly highlights that this encryption-based anonymity is what makes the Dark Web attractive for activities such as cybercrime marketplaces, illegal trade, anonymous communications, and covert operations.
The other options do not accurately define the Dark Web. Legal dossiers and financial records are commonly found in the Deep Web , such as banking portals and government databases. Requiring authorization alone does not distinguish the Dark Web, as many Deep Web resources also require credentials. The Dark Web is not indexed by search engines , which is the opposite of Option D.
CHFI v11 emphasizes that understanding this anonymity model is critical for investigators, as it directly impacts attribution challenges, legal considerations, and evidence collection strategies in dark web investigations.
Therefore, the correct distinction-fully aligned with CHFI v11-is that the Dark Web enables complete anonymity through encryption , making Option B the correct answer.

質問**: 33**
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: **B** (コメントを発表する)
Option B. Corroborative evidence is the best answer because the question describes logs, metadata, and timestamps being used to support and confirm what happened during the incident. CHFI v11 explicitly includes metadata investigation , event logs , timeline and kill chain analysis , and reconstruction of user or system activity through forensic artifacts. This kind of evidence often does not stand alone as a complete confession-like proof, but it is extremely valuable because it corroborates the sequence of events, supports witness statements, confirms access patterns, and links actions across different systems. For example, file timestamps, logon events, and application logs can help show that a suspect account accessed a document, used a device, or connected to a system at a particular time. That is exactly the role of corroborative evidence.
Option A would help clear the suspect, which is not the focus here. Option C is too absolute because the question emphasizes supporting and reconstructive value. Option D is too narrow. Therefore, under CHFI evidence-analysis principles, the logs, metadata, and timestamps described here serve primarily as corroborative evidence .

質問: **34**
鑑識捜査官はサイバー犯罪捜査に配属され、犯罪現場にある電源の入ったコンピュータから重要な証拠を記録する必要がある。そのコンピュータには、進行中の捜査に関連する重要なファイルやプログラムが含まれていると疑われている。現場に到着した捜査官は、コンピュータのモニターにスクリーンセーバーが表示されており、アクティブなプログラムや開いているファイルが隠されていることに気づく。鑑識チームは、コンピュータ上のデータを改変したり改ざんしたりすることなく、証拠の完全性を維持するというプレッシャーにさらされている。
捜査官は、証拠を適切に記録するために、画面上で実行されているプログラムの鮮明な画像をキャプチャする必要があります。しかし、コンピュータ上の情報を改ざんする可能性のある事態を避けるため、どのように進めるべきか迷っています。捜査官は、画面上で実行中のプログラムをキャプチャし、効果的に証拠を記録するために、どのような手順を踏むべきでしょうか？
A. マシンを再起動して、再起動後に実行中のプログラムをシステムに表示させます。
B. マウスを少しゆっくりと動かしてスクリーンセーバーから画面を起動し、アクティブなプログラムを撮影して記録します。
C. コンピュータの主電源コードを抜いてシステムをリセットし、揮発性データをすべて消去します。
D. 証拠を記録している間は、リモートアクセスを防ぐためにネットワークケーブルを外してください。
正解: (正解を表示します)
Option B is the best answer because the investigator's immediate goal is to document what is currently displayed or active on a powered-on system while causing the least possible disturbance . CHFI v11 emphasizes best practices for handling digital evidence ,

preserving evidence , collecting volatile information , and understanding the consequences of actions taken on a live system.
A slight movement of the mouse to wake the screen is the least disruptive way among the listed options to reveal the active display and allow proper photographic documentation.
Rebooting or unplugging the machine would destroy volatile evidence and significantly alter the system state. Disconnecting the network cable may sometimes be considered in other operational contexts, but it does not solve the immediate issue of documenting the active on-screen evidence hidden by the screensaver.
From a CHFI standpoint, documentation at the scene should preserve the evidence as found as much as possible while minimizing changes. Therefore, the correct response is to gently wake the screen and photograph/document the visible programs without taking destructive actions that would compromise volatile evidence.

質問**: 35**
コンプライアンス担当役員のスカーレットは、最近財務不正の疑いで告発された上場企業で働いています。調査を進める中で、彼女は米国で制定された法律に遭遇します。
2002年の議会では、企業による不正な会計行為から投資家を保護することを目的として制定されました。
この法律は、より厳格な企業の財務報告基準、内部統制、および不正行為に対する罰則を義務付けています。
この場合、スカーレットが検討している可能性が高い法律は次のどれですか。
A. PCI DSS
B. ソックス
C. GLBA
D. ECPA
正解**: (**正解を表示します**)**
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.
The other options are incorrect: PCI DSS applies to payment card data security, GLBA governs customer financial data privacy, and ECPA addresses electronic communications

privacy. Therefore, consistent with CHFI v11 legal frameworks and compliance objectives, the correct law Scarlett is reviewing is SOX (Sarbanes-Oxley Act) .

質問: **36**
フォレンジック調査員であるダリエルは、組織のネットワーク内で最近発生したセキュリティインシデントの調査を任されました。調査の一環として、ダリエルはUnixベースのシステムにコマンドラインインターフェースのパケットスニファーをインストールし、ネットワークトラフィックを監視 -キャプチャして、不正アクセスや悪意のある活動の兆候を探します。キャプチャされたデータは、ダリエルがセキュリティ侵害の発生源を特定し、ネットワークを介した攻撃者の行動を追跡するのに役立ちます。使用するツールは、リアルタイムのネットワークトラフィックを効率的に分析でき、Unixベースのオペレーティングシステムで実行できるものでなければなりません。上記のシナリオにおいて、ダリエルが使用したツールは次のどれですか？
A. tcpdump
B. メタシールドアナライザー
C. タイムストンプ
D. ビルボード
正解: **A (**コメントを発表する**)**
According to the CHFI v11 curriculum under Network Forensics , investigators must be proficient in using packet sniffing tools to capture and analyze live network traffic. tcpdump is a widely used command-line packet analyzer that runs natively on Unix, Linux, and BSD-based systems. It allows investigators to capture packets in real time, apply powerful filters, and save traffic in PCAP format for further offline analysis using tools such as Wireshark.
In forensic investigations, tcpdump is especially valuable because it provides low-level visibility into network communications, including source and destination IP addresses, ports, protocols, TCP flags, and payload data.
This enables investigators to detect suspicious behaviors such as unauthorized connections, port scans, malware command-and-control traffic, data exfiltration attempts, and denial-of-service activities. CHFI v11 specifically highlights tcpdump as a core tool for network traffic investigation and evidence gathering in Unix-based environments.
The other options are incorrect. Metashield Analyzer is used for file-based threat analysis, Timestomp is an anti-forensics tool used to manipulate file timestamps, and Billboard is not a recognized network forensic or packet sniffing tool.
The CHFI Exam Blueprint v4 emphasizes the importance of real-time packet capture tools for network investigations, making tcpdump the correct, forensically sound, and exam-aligned answer

質問: **37**

デジタルフォレンジック企業で調査員として働くマイクは、違法行為に使用された疑いのあるWindowsコンピュータに関する事件を担当することになった。マイクは、多数のファイルのメタデータを調べて、不正行為の痕跡を探すよう指示されている。彼はFTK imager、OSForensics、ExifTool、EnCaseなど、さまざまなツールを検討している。ファイルメタデータの分析というマイクの具体的な要件を満たすには、どのツールを選択すべきだろうか？

A. ExifTool
B. FTKイメージャー
C. OSForensics
D. ケース化

正解: **(**正解を表示します**)**

Option A. ExifTool is the best answer because the task is specifically to analyze file metadata . CHFI v11 includes Metadata Investigation , Understanding EXIF data , and identifies categories of tools used to examine files and metadata during forensic analysis. ExifTool is purpose-built for extracting and examining metadata from many file types, including images, documents, and other digital artifacts. That makes it especially appropriate when the primary investigative requirement is to inspect metadata fields such as creation time, modification details, embedded properties, author information, device information, and other hidden descriptive attributes.

The other tools are broader forensic platforms or imaging utilities. FTK Imager is primarily associated with evidence preview and imaging. OSForensics supports multiple investigative functions, but it is not the most targeted answer when the question asks specifically about metadata analysis. EnCase is also a broad forensic suite rather than the most direct metadata-focused tool in the options. Therefore, based on CHFI's emphasis on metadata investigation and file-type analysis, ExifTool is the most precise and suitable choice for Mike's stated need.

質問: **38**

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. エドワードは元のデータに変更を加えることを避けるべきです。
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、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。

正解: **B (**コメントを発表する**)**

Option B is the best answer because one of the most fundamental forensic acquisition principles is to avoid changing the original evidence . CHFI v11 emphasizes preserving evidence , best practices for handling digital evidence , data acquisition methodology , and maintaining evidence integrity so the results remain defensible in legal or disciplinary proceedings. That principle applies regardless of device type, operating system, or case category.
This rule of thumb is broader and more important than the other options because the correct acquisition approach depends on the system state and circumstances. Live acquisition is not always appropriate.
Focusing only on non-volatile data may cause investigators to miss valuable volatile evidence. Network- based acquisition is not universally the least intrusive or the best approach. What remains constant is the duty to minimize alteration of the original source. By preserving the original data and performing analysis on properly acquired copies, the investigator protects the integrity, repeatability, and admissibility of the evidence.
Therefore, the most accurate CHFI-aligned rule of thumb is that Edward should avoid making changes to the original data during acquisition.

質問**: 39**
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**: B (**コメントを発表する**)**
Option B is the best answer because CHFI v11 explicitly covers Live Acquisition , Order of Volatility , Rules of Thumb for Data Acquisition , and Collecting Volatile Information and Non-Volatile Information . When a Windows system is still running, the investigator should gather the most volatile and easily lost information first .
Among the choices provided, network connections should be collected first because they can disappear immediately if sessions close or the system state changes. Running processes come next because active processes may terminate or change quickly. A list of open ports is also volatile and supports network-state interpretation, but it is slightly less informative on its own than established connections and active processes.

System state is collected after those more transient live indicators.
This ordering is consistent with CHFI's emphasis on preserving volatile evidence before it is altered by shutdown, user activity, or acquisition actions. Although detailed live-response procedures can vary by tool and environment, the option that best matches CHFI's order-of-volatility principle is: network connections, running processes, open ports, then system state .

質問**: 40**
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であることに気付きました。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**: C (**コメントを発表する**)**
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.
Therefore, based on the file's hexadecimal signature, the image format is GIF , making Option C the correct answer.

質問**: 41**

法医学捜査官は、企業の内部ネットワークを標的とした高度なサイバー攻撃に関連する大量のデジタル証拠を分析するよう命じられた。この攻撃は企業全体の複数のシステムに影響を与え、複数の脆弱性を悪用したものであった。事件の複雑さと規模を考慮し、捜査官は捜査プロセスを効率化するためにコンピュータ化されたフォレンジックツールを導入することを決定した。
これらのツールは、複数の疑わしいドライブのビット単位のコピーを作成するために使用され、元の証拠の完全性を確保し、元のデータを変更することなくさらなる分析を可能にします。
フォレンジックイメージの作成に加え、調査官は高度なハッシュ分析技術を用いて、ファイルハッシュを既知の脅威データベースと比較することで、潜在的に悪意のあるファイルを迅速に特定します。さらに、攻撃中に生成される大量のイベントログを管理するため、調査官はフォレンジックツールを使用してタイムスタンプを分析し、詳細な活動タイムラインを作成します。このタイムラインには、最初の侵入、ネットワーク内での横方向の移動、機密データの流出など、攻撃における重要なイベントが示されます。
これらの作業を効率化することで、捜査官は攻撃の全容を把握するために必要な重要な分析に集中できるようになります。ここで説明されているのは、どのフォレンジックプロセスでしょうか？
A. データストレージ管理を統合したフォレンジックオーケストレーション。
B. 複数のタスクを並行して管理するフォレンジックオーケストレーション。
C. 手動分析を支援するフォレンジック自動化ツール。
D. 反復作業を効率的に実行するフォレンジック自動化。
正解: **(**正解を表示します**)**
Option D is the best answer because the scenario describes using tools to automate repetitive, high-volume forensic tasks such as bit-by-bit imaging , hash comparison , and timeline generation so the investigator can concentrate on interpretation and deeper analysis. CHFI v11 explicitly includes Forensics Automation and Orchestration as a core topic.
The key clue is that the tools are being used to streamline repeated technical tasks efficiently across a large dataset. That is the hallmark of forensic automation . Automation reduces manual workload in predictable processes like hashing, imaging, and log parsing. Orchestration , by contrast, usually refers to coordinating multiple tools, workflows, or systems together across a broader process. While there may be some orchestration elements in real environments, the emphasis in this question is clearly on efficient execution of repetitive tasks.
Because the investigator is using computerized tools to handle recurring evidence-processing steps at scale, the most accurate classification is forensic automation performing repetitive tasks efficiently . That aligns directly with the CHFI objective covering automation and orchestration in digital forensics.

質問: **42**

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) 14:35:36.878945] [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. [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
D. [2023年12月11日(月) 14:35:38.878945] [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
正解**: (**正解を表示します**)**
Option D is the most useful answer because it provides the clearest indication that the activity may be part of a larger security issue rather than just routine login failures or missing-file requests. A mod_security entry showing that a rule was triggered for a possible SQL injection attempt directly suggests malicious web- application attack behavior and points to a broader intrusion pattern.
Option C is useful for confirming failed authentication activity, but by itself it may still reflect simple credential guessing or user error. Option B only shows a missing file request, which could be benign or accidental. Option A is the least suspicious of the choices. By contrast, an application firewall or security module explicitly flagging a possible SQL injection attempt strongly indicates that the server may be under targeted attack and that the failed logins could be part of a coordinated campaign.
From a CHFI perspective, log entries that directly indicate known attack techniques are especially valuable during web-server investigations. Therefore, the Apache log entry most likely to help David determine that the failed attempts were tied to a larger security problem is the mod_security alert for possible SQL injection .

質問**: 43**
サイバー犯罪の容疑者が逮捕され、オンライン中にコンピュータが押収された。捜査官は、Torブラウザが起動しており、いくつかのダークウェブサイトにアクセスしていたことを発見した。捜査官はこのアクティブなセッションからできるだけ多くの情報を得たいと考えている。捜査官は、メモリダンプを収集するか、ハードドライブ分析のためにコンピュータの電源を切るかのどちらかを選択する必要がある。この状況で、どちらの選択肢が最も多くの情報をもたらすだろうか？
A. コンピュータをシャットダウンしてハードドライブを分析しています。
B. マシンをセーフモードで再起動し、システムスキャンを実行します。

C. ハードウェアの完全性を維持するため、直ちにマシンの電源プラグを抜いてください。
D. コンピュータを起動したままにしてメモリダンプを収集します。
正解: **(**正解を表示します**)**
Option D is the best answer because the computer was seized while the Tor Browser was actively open , meaning the most valuable evidence may still exist in volatile memory . In CHFI methodology, when a live system contains potentially crucial active-session evidence, investigators should follow the order of volatility and collect the most easily lost evidence first. A memory dump may preserve active browser session data, in- memory artifacts, decrypted content, process information, network connections, and traces of recently accessed dark web activity that might never be written clearly to disk.
Shutting down or unplugging the machine would destroy this volatile evidence immediately. Restarting into safe mode would also alter or erase the active session context. Hard drive analysis remains important later, but it would not capture the full live state of the Tor session as effectively as RAM collection.
Because the goal is to obtain as much information as possible from the active session , the strongest CHFI- aligned answer is to leave the system running and collect a memory dump first before taking further acquisition steps.

質問: **44**
企業オフィス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の一環として、スミス刑事は押収されたハードドライブから証拠を収集する任務を負っています。スミス刑事は、不正アクセスや改ざんの痕跡を明らかにするため、ストレージメディアから不揮発性データを改変されていない状態で抽出することを目指しています。スミス刑事による企業データ漏洩の調査において、押収されたハードドライブから不揮発性データを抽出するデータ取得プロセスはどれですか？
A. 動的取得
B. デッドアクイジション
C. 不安定な買収
D. ライブ取得
正解: **(**正解を表示します**)**
According to the CHFI v11 Data Acquisition Concepts and Rules , dead acquisition is the forensic process specifically used to extract non-volatile data from storage media such as hard drives, SSDs, USB devices, and memory cards after the system has been powered off . This method ensures that the evidence is collected in a forensically sound and unaltered manner , which is essential for maintaining evidence integrity and legal admissibility.
In dead acquisition, the seized system is shut down, and the storage media is accessed using write blockers and forensic imaging tools to create a bit-by-bit copy of the disk. This allows investigators to safely analyze files, file system metadata, logs, deleted data, slack space, and unallocated space without modifying the original evidence. CHFI v11

emphasizes dead acquisition as the preferred approach when dealing with non- volatile data, particularly in corporate breach investigations where data integrity is critical.
The other options are not appropriate in this scenario. Volatile acquisition and live acquisition focus on collecting data from a running system, such as RAM, active processes, and network connections. Dynamic acquisition is not a standard CHFI-defined category for non-volatile disk evidence.
Therefore, since Detective Smith is extracting non-volatile data from a seized hard drive while preserving its original state , the correct CHFI v11-verified answer is Dead acquisition (Option B) .

質問**: 45**
セキュリティ研究チームがマルウェア分析専用のテスト環境を構築しています。チームは、テスト環境が実際のネットワークから隔離されていることを確認し、マルウェアが業務に影響を与えないようにしています。テスト環境には、仮想マシン、構成の異なる(パッチ適用済みと未適用)標的マシン、イメージングツール、ファイル分析ツール、ネットワークキャプチャツールなどの必要なツールが含まれています。マルウェア分析ラボでサンドボックス環境を使用する主な利点は何ですか？
A. サンドボックスは、テスト前にすべての仮想マシンが最新のセキュリティパッチで更新されていることを保証します。
B. サンドボックスを使用すると、ネットワーク全体に感染するリスクなしに、マルウェアを制御された環境で実行できます。
C. サンドボックスは、マルウェアが機能的なネットワークにアクセスして伝播をテストできるようにします。
D. サンドボックスはマルウェアを外部ネットワークから隔離しますが、マルウェアの実行には影響を与えません。
正解**: (**正解を表示します**)**
Option B is the best answer because CHFI v11 explicitly emphasizes the prominence of setting up a controlled malware analysis lab and the need to perform static and dynamic malware analysis in a safe environment. A sandbox is designed to let investigators execute suspicious code in an isolated setting where its behavior can be observed without endangering production systems or the organization's functional network.
This is exactly why the scenario highlights virtual machines, different victim configurations, and monitoring tools such as imaging, file-analysis, and network-capture utilities. These elements exist so the analyst can watch what the malware does, such as file changes, process creation, registry modifications, persistence attempts, and network communications, while containing the risk. The primary benefit is therefore safe execution under controlled conditions .
Option A describes a maintenance activity, not the core benefit of sandboxing. Option C is unsafe and contradicts isolation principles. Option D is incomplete because sandboxing is not only about external isolation; it is about safely observing execution behavior overall.

Therefore, the correct CHFI-aligned answer is that the sandbox allows controlled execution without risking widespread infection.

質問: **46**
フォレンジック調査官のジェイソンは、組織のネットワークインフラストラクチャに対する大規模なサイバー攻撃を調査している。攻撃者は、ネットワーク全体に拡散し、多数のシステムに感染する高度なマルウェアの亜種を展開した。ジェイソンは、対策を講じるために、このマルウェアの挙動を分析する必要がある。彼は、実際のネットワーク環境を模倣し、マルウェアのネットワーク挙動を観察するツールを使用することにしました。ジェイソンはどのツールを使用すべきでしょうか？
A. IDA Pro
B. Sysinternals Suite
C. 解剖
D. カッコウの砂場
正解: **(**正解を表示します**)**
Option D. Cuckoo Sandbox is the best answer because CHFI v11 explicitly includes tools to perform static and dynamic malware analysis , tools to analyze malware behavior on a system and network , and the preparation of a controlled malware analysis lab . Jason's requirement is to mimic a live environment and observe the malware's network behavior , which is exactly the role of a malware sandbox.
A sandbox such as Cuckoo allows the examiner to safely run the malware in an isolated setting while monitoring process activity, file changes, registry behavior, DNS requests, network connections, and other indicators needed to understand propagation and develop countermeasures. That makes it ideal for behavioral malware analysis.
IDA Pro is mainly for reverse engineering code. Sysinternals Suite contains valuable Windows utilities but is not a full isolated malware-behavior lab. Autopsy is used for disk and file-system forensic analysis rather than live behavioral execution. Therefore, under CHFI's malware-forensics and sandbox-analysis objectives, the strongest answer is Cuckoo Sandbox .

質問: **47**

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するための最初のステップを決定する必要があります。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実行する必要がありますか？
A. 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。
B. デバイスをルート化する
C. .1TAGフォレンジックを実行します
D. USD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**: C (**コメントを発表する**)**
Option C. Perform JTAG forensics is the best answer because the scenario clearly states that the Android device is physically damaged , not booting , and not responding to normal recovery procedures . CHFI v11 covers mobile device forensics , Android acquisition methods , and the challenges investigators face when devices are damaged, locked, or otherwise inaccessible. In such cases, the examiner must choose a method that can retrieve data without relying on the normal operating state of the device .
JTAG forensics is specifically suited to situations where a device cannot boot normally but investigators still need to access data directly from memory through hardware-level techniques. This makes it the most appropriate first operation when conventional logical access is not possible.
The other options are weaker. Using the dd command generally requires the device to be sufficiently operational and accessible. Rooting the device can alter evidence and may not even be possible on a damaged device. Simply connecting by USB is also inadequate if the phone does not boot or respond. Therefore, under CHFI mobile forensic principles, JTAG forensics is the correct initial step for a damaged Android evidence device.

質問**: 48**
サイバー攻撃のフォレンジック調査において、チームは侵害されたネットワーク内での攻撃者の行動を追跡するために、一連の出来事の時系列を再構築する任務を負う。しかし、システムログや重要な文書を詳しく調べていくうちに、フォレンジックチームは矛盾点に気づく。攻撃中に変更されたはずのファイルには、攻撃者が既にシステムを離れた後に変更されたことを示すタイムスタンプが表示されているのだ。バックアップやシステムログにはさらに異常なパターンが見られ、一部のファイルは通常の運用時間中に変更されたようで、実際の出来事の順序を隠蔽するために改ざんが行われた可能性が示唆される。
これらの矛盾点から、捜査官は、攻撃者がフォレンジックのタイムラインを混乱させるために、重要なファイルのタイムスタンプを意図的に操作したのではないかという疑念を抱いている。この戦術は、捜査チームを混乱させ、侵害の再現を妨害することを目的としてお

り、悪意のある活動が通常の業務の一部であったかのように見せかけ、捜査を意図的に誤導しようとする意図的な試みを示している。このような行動は、どのフォレンジック対策技術に最も該当する可能性が高いか？
A. システムから不正な活動の痕跡をすべて削除するためのアーティファクト消去。
B. 代替データストリーム(ADS)を使用して、検出を回避する方法で悪意のあるファイルを保存および隠蔽します。
C. ファイルメタデータを破損させることでトレイルを難読化します。
D. プログラムパッカーは実行可能ファイルを圧縮および隠蔽し、分析を困難にします。
正解: **C** (コメントを発表する)
Option C is the best answer because the scenario describes deliberate manipulation of timestamps and metadata to confuse investigators and distort the event timeline. CHFI v11 explicitly lists Trail Obfuscation and Overwriting Data/Metadata among the major anti-forensics techniques , and it also emphasizes timeline analysis , metadata investigation , and the need to detect actions intended to mislead forensic reconstruction.
This kind of behavior is a classic form of trail obfuscation . By altering file times and related metadata, the attacker attempts to make malicious actions appear normal or unrelated, thereby undermining the investigator' s ability to accurately reconstruct the incident. That is more specific than general artifact deletion and better matches the facts in the question. Artifact wiping would focus on removing evidence entirely, ADS hides data in alternate streams, and program packers conceal executable content. None of those directly explain manipulated timestamps intended to falsify chronology. Therefore, within CHFI's anti-forensics framework, the most accurate classification is trail obfuscation through tampering with file metadata .

質問: **49**
経験豊富なモバイルフォレンジック調査官であるジャクソンは、進行中の捜査にとって重要な証拠が含まれている可能性のあるiPhoneの分析を任されました。彼は厳しい期限に追われており、パスコード入力などの従来の方法でユーザーデータにアクセスしたり、デバイスのセキュリティ機能をバイパスしたりする余裕はありません。ジャクソンは、デバイスのIMEI番号、シリアル番号、その他のハードウェアの詳細など、フォレンジック分析に必要なシステムレベルの情報をデバイスから取得する必要があります。また、分析中にユーザーデータが侵害されたり、漏洩したりしないようにする必要もあります。フォレンジック基準を遵守しながら必要な情報にアクセスするには、ジャクソンはどのモードを使用すべきでしょうか？
A. セーフモード
B. 脱獄モード
C. DFUモード
D. リカバリーモード
正解: (正解を表示します)

Option C. DFU Mode is the best answer because the scenario requires access to system-level device information such as IMEI and serial number without interacting with user data or relying on passcode entry. CHFI v11 covers mobile phone evidence analysis , data acquisition methods , logical and physical acquisition of Android and iOS devices , iOS architecture and boot process , and challenges in mobile forensics . These objectives support the need to use controlled acquisition states that minimize user-data interaction while still enabling low-level device communication.
DFU (Device Firmware Update) mode is a low-level state used to communicate with the device before the full operating system and user environment are loaded. That makes it more suitable than methods that would require normal device access. Jailbreaking would alter the device state and is not appropriate here. Safe Mode is not the relevant forensic mode for iPhone hardware identification. Recovery Mode is also used for maintenance, but DFU is the deeper low-level mode and better fits a requirement focused on hardware-level information without exposing user content.
Accordingly, DFU Mode is the strongest CHFI-aligned answer for acquiring essential device-identification details while preserving forensic discipline.

質問**: 50**
フォレンジック調査の後、組織はシステムとネットワーク全体にわたって電子データを効果的に保護するための包括的なポリシーと手順の導入に注力します。これらのポリシーは、適用される法律、規制、および運用基準への準拠を確保するとともに、将来の監査、調査、または法的手続きに備えてデータの整合性を確保するように設計されています。この段階では、データの保持、アクセス管理、および長期保存に関する明確なガイドラインを確立することを目的としています。
このアクティビティは、電子情報開示リファレンス モデル (EDRM) サイクルのどの段階に相当しますか?
A. 法的または規制上の目的で不要になった後の不要なデータの廃棄。
B. データ制御メカニズムの作成を含む情報ガバナンス。
C. 後続の分析のために特定されたソースからデータを収集します。
D. データが関連性があり、レビューに利用できることを確認するためのデータの識別。
正解**: (**正解を表示します**)**
According to the CHFI v11 objectives and the Electronic Discovery Reference Model (EDRM) framework, the activity described in this scenario corresponds to the Information Governance stage. Information governance is the foundational phase of the EDRM cycle and focuses on establishing policies, procedures, controls, and standards to manage electronic information throughout its lifecycle. This includes defining data retention schedules, access control policies, compliance requirements, preservation rules, and audit readiness.
In CHFI v11, information governance is emphasized as a proactive and strategic function that ensures an organization is prepared for future investigations, audits, litigation, or

regulatory inquiries. By implementing governance controls after an investigation, organizations strengthen forensic readiness, reduce legal risk, and ensure that electronic data remains reliable, authentic, and admissible as evidence.
The other options do not accurately match the described activity. Disposal (Option A) refers to defensible deletion after legal hold requirements expire. Collection (Option C) involves acquiring data for analysis, while Identification (Option D) focuses on locating potentially relevant data sources. None of these address long- term policy creation or enterprise-wide data control.
The CHFI v11 Exam Blueprint explicitly includes Information Governance within the eDiscovery process, highlighting its role in compliance, risk mitigation, and evidence integrity management, making Option B the correct and exam-aligned answer

質問**: 51**
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査しています。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を発見しました。さらに調査を進めると、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、復元がより困難になっていることに気づきました。失われたファイルを復元するには、リアムはLinux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ります。リアムは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. cp /proc/$PID/exe /tmp/file
B. cd C:\RECYCLER\S-..User SID
C. D < # > 。
D. $R < # > 。
正解**: A (**コメントを発表する**)**
Option A is the correct answer because the question describes a Linux executable that was running at the time of the attack and then deleted or erased from normal file-system visibility. In Linux forensics, if a process is still running, the executable image may still be accessible through the /proc/$PID/exe link for that process. Copying that path to another location is a recognized way to preserve the executable content for analysis before the process terminates.
This aligns with CHFI v11's coverage of Linux file system analysis tools , Linux memory forensics , tools to collect volatile and non-volatile information on Windows and Linux , and Windows and Linux forensics using Python , all of which reflect the importance of understanding live Linux evidence sources and recovery opportunities.
The other options are unrelated to Linux executable recovery. The RECYCLER path is Windows-specific, and $R < # > style entries are associated with Windows Recycle Bin artifacts, not Linux process recovery.
Therefore, for a deleted-but-still-running Linux executable, the correct CHFI-aligned recovery command is cp

/proc/$PID/exe /tmp/file .

質問: **52**
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: **(正解を表示します)**
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. Therefore, the correct and CHFI v11-verified answer is All of these , making Option B the most accurate choice.

質問: **53**
マルウェアアナリストとして、Windowsワークステーション上の不審なプログラムを精査し、特にシステムレジストリファイルとのやり取りに注目する任務を負っています。レジストリアーティファクトを監視することで、マルウェアの挙動に関する洞察が得られ、永続化メカニズムや悪意のある活動の特定に役立ちます。フォレンジック調査員は、レジスト

リアーティファクトを監視することで、Windowsシステム上のマルウェアの挙動に関する洞察をどのように得るのでしょうか？
A. ネットワークトラフィックパターンの監視
B. ブラウザ履歴ログの確認
C. システムファイルの実行の追跡
D. レジストリキーの変更を分析
正解: **(**正解を表示します**)**
According to the CHFI v11 syllabus under Malware Forensics and System Behavior Analysis , the Windows Registry is one of the most critical sources of forensic evidence when investigating malware activity. Malware frequently interacts with registry keys to achieve persistence , configure execution parameters, disable security controls, or maintain state information across reboots. By analyzing registry key modifications , forensic investigators can identify how malware embeds itself into the operating system and understand its long-term behavior.
Common persistence mechanisms include modifications to registry locations such as Run, RunOnce, Services, Winlogon, and scheduled task-related keys. Changes in these keys can reveal how and when malware is executed, whether it runs at system startup, and which privileges it attempts to obtain. CHFI v11 emphasizes monitoring registry artifacts using tools like Process Monitor, Registry Editor, and registry diff utilities to detect unauthorized additions, deletions, or value changes.
The other options are incorrect in this context. Monitoring network traffic patterns (Option A) is useful for command-and-control analysis but does not directly reveal registry-based persistence. Browser history logs (Option B) are related to user activity, not system-level malware behavior. Tracking system file executions (Option C) focuses on executable activity but does not expose configuration or persistence logic stored in the registry.
The CHFI Exam Blueprint v4 explicitly highlights registry-based malware persistence mechanisms as a key investigative focus, making analyzing registry key modifications the correct and exam-aligned answer

質問: **54**
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: **A (**コメントを発表する**)**

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. The other options are not primary forensic objectives- system performance, malware geography, or network optimization are unrelated to persistence analysis.
Therefore, in accordance with CHFI v11 malware forensics principles, identifying malware persistence is essential to prevent future infections and ensure the long-term security of the system.

質問: **55**
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: **D (**コメントを発表する**)**
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**: 56**
最近のサイバー攻撃に関するフォレンジック調査において、アナリストは検出を回避するために意図的に偽装されたマルウェアを発見した。このマルウェアは暗号化レイヤーで覆われており、通常のセキュリティソフトウェアでは内容を読み取ることができなかった。復号技術を用いてこのレイヤーが削除されると、マルウェアの真の悪意ある機能が明らかになった。この難読化に最も関与している可能性が高いコンポーネントは次のうちどれか？
A. パッカー
B. エクスプロイト
C. ペイロード
D. ドロッパー
正解**: A (**コメントを発表する**)**
Option A. Packer is the correct answer because CHFI v11 explicitly identifies program packers as an anti- forensics technique and also covers program packers unpacking tools as a way to reverse that concealment during analysis.
A packer is used to wrap or obfuscate an executable so that its real content is hidden from straightforward inspection. This often makes the malware appear unreadable or significantly harder to analyze until the packed layer is removed or unpacked. That fits the scenario exactly: the malicious functionality only became clear after the outer encrypted or packed layer was removed.
An exploit is code used to take advantage of a vulnerability, not primarily to hide malware. A payload is the malicious function delivered or executed after infection. A dropper is designed to install or deliver other malware components, but it is not the best term for the

specific concealment layer described here. Therefore, within CHFI's anti-forensics framework, the component most responsible for this type of obfuscation is a packer .

質問: **57**
フォレンジック調査員のサラは、機密データを含む企業のサーバーで、侵害後の調査を行っています。削除されたファイルが悪意のある人物の手に渡らないようにするため、彼女はメディアサニタイズ手順を採用しています。この手順では、削除されたデータを0x00と0xFFのシーケンスで6回上書きし、最後に0xAAのパターンで上書きします。
このシナリオでサラが従ったメディアサニタイズ基準は次のどれですか?
A. NAVSO P-5239-26 (MFM)
B. GOST P50739-95
C. VSITR
D. DoD 5220.22-M
正解: **(正解を表示します)**
According to the CHFI v11 Computer Forensics Fundamentals and Evidence Handling and Sanitization guidelines, media sanitization is a critical process used to ensure that deleted or sensitive data cannot be recovered using forensic techniques. Different international standards define specific overwrite patterns and the number of passes required to securely sanitize storage media.
The procedure described- six overwrite passes alternating between 0x00 and 0xFF, followed by a final overwrite with 0xAA -exactly matches the VSITR (Verschlusssache IT Richtlinien) standard. VSITR is a German government-approved data sanitization method that mandates 7 overwrite passes :
* Passes 1-6: Alternating 0x00 and 0xFF
* Pass 7: Final overwrite with the pattern 0xAA
CHFI v11 explicitly references VSITR as a high-assurance sanitization standard , suitable for environments handling classified or highly sensitive information. This method is more rigorous than commonly used standards such as DoD 5220.22-M , which typically uses 3 passes (or a legacy 7-pass variant with different patterns). NAVSO P-5239-26 (MFM) uses different overwrite schemes, and GOST P50739-95 generally involves fewer passes.
From a forensic and legal standpoint, following a recognized sanitization standard like VSITR demonstrates due diligence, compliance, and defensibility , especially when preventing data leakage after incidents.
Therefore, based on the overwrite pattern and number of passes described, the media sanitization standard followed by Sarah is VSITR , making Option C the correct and CHFI v11-verified answer.

質問: **58**
あなたは、インターネット インフォメーション サービス (IIS) ウェブ サーバーにおける潜在的なセキュリティ侵害の分析を任されたフォレンジック調査員です。あなたの目標

は、IIS ログを収集 ·分析し、攻撃がどのように、どこから発生したかを特定することです。Windows Server オペレーティング システムでは、IIS ログ ファイルは通常、デフォルトでどこに保存されますか？
A. %AppData%\Microsoft\IIS\Logs
B. %ProgramFiles%\IIS\Logs
C. %SystemDrive%\inetpub\logs\LogFiles
D. %SystemRoot%\Logs\IIS
正解: **(**正解を表示します**)**
According to the CHFI v11 objectives under Web Application Forensics and Log Analysis , knowing the default storage locations of web server logs is essential for reconstructing web-based attacks. On Windows Server operating systems, Internet Information Services (IIS) stores its HTTP and HTTPS request logs by default in the directory:
%SystemDrive%\inetpub\logs\LogFiles
This directory contains subfolders such as W3SVC1, W3SVC2, etc., where each folder corresponds to a specific IIS website instance. The log files stored here record critical forensic details including client IP addresses, timestamps, HTTP methods, requested URLs, status codes, user agents, and referrers . These artifacts allow investigators to identify attack vectors such as SQL injection, command injection, directory traversal, brute-force attempts, and web shell uploads.
The other options are incorrect because they do not represent default IIS log locations. %AppData% is user- profile specific, %ProgramFiles% contains application binaries rather than logs, and %SystemRoot%
\Logs\IIS is not a standard IIS logging path.
The CHFI Exam Blueprint v4 explicitly covers IIS web server architecture and log analysis , emphasizing familiarity with default log paths to ensure timely evidence acquisition and accurate incident reconstruction.
Therefore, %SystemDrive%\inetpub\logs\LogFiles is the correct and exam-aligned answer

質問: **59**
ある企業が、クラウドサービスプロバイダー(CSP)側の重大な障害により、クラウドインフラストラクチャ内で大規模なデータ侵害に見舞われた。この侵害は、CSPのインフラストラクチャがマルチテナント環境において、異なる顧客のデータを適切に分離 ·保護できていなかったために発生した。攻撃者はこの脆弱性を悪用し、同じクラウドシステムを共有する複数のクライアントから機密データへの不正アクセスを取得した。その結果、複数のアカウントにわたる顧客データが漏洩し、攻撃者はこのアクセスを利用してシステム内を横断的に移動し、権限を昇格させ、さらに機密情報にアクセスした。
この侵害は長期間にわたり検知されず、攻撃者は痕跡を隠蔽し、大量のデータを流出させることができた。この問題の原因として最も可能性が高い脅威は何だろうか？
A. クラウドサービス選定時のデューデリジェンスの不備。
B. クラウドインフラストラクチャとデータに対するクライアントの制御の喪失

C. 監視不足により、気づかれないままデータ漏洩が発生する。
D. リソースの分離が不十分なため、テナント間でデータが漏洩しています。
正解: **(**正解を表示します**)**
Option D is the strongest answer because the scenario clearly describes a multi-tenant cloud environment in which the provider failed to properly separate one customer's resources from another's. That is the classic problem of insufficient resource isolation . When tenant separation is weak, an attacker can cross boundaries between customer environments, access unauthorized data, and potentially move laterally across shared infrastructure.
This fits the fact pattern far better than the other options. Failure in due diligence concerns poor vendor selection, but the direct technical cause here is not selection error; it is the isolation failure itself. Loss of client control is a general cloud concern but does not specifically explain how the breach occurred. Lack of monitoring may explain why the attack went unnoticed, but it is not the root threat described in the question.
From a CHFI cloud-forensics perspective, investigators must recognize threats linked to multi-tenancy , data segregation failures , and provider-side weaknesses in shared environments. Since the breach affected several accounts because tenant boundaries failed, the correct answer is insufficient resource isolation causing cross-tenant data exposure .

質問: **60**
デジタルフォレンジック調査員が、サイバー犯罪事件の容疑者から回収されたモバイルデバイスを調査しています。
デバイスは、昇格された権限とシステム リソースへの無制限のアクセスを許可するカスタム オペレーティング システム構成を実行しているようです。
この構成を実現するために最も適した方法は何ですか?
A. Androidデバイスにカスタム ROMをインストールする
B. iOSデバイスのファームウェアの脆弱性を悪用する
C. Androidデバイスのルート化
D. iOSデバイスの脱獄
正解: **(**正解を表示します**)**
According to the CHFI v11 Mobile and IoT Forensics domain, rooting an Android device is the most common and direct method used to obtain elevated (superuser) privileges and unrestricted access to system resources. Rooting allows a user to bypass Android's built-in security restrictions and gain full control over the operating system, including access to protected directories, system binaries, kernel parameters, and hardware interfaces.
CHFI v11 explains that once an Android device is rooted, the user can modify system files, install unauthorized applications, disable security controls, manipulate logs, and conceal malicious activity-making rooting a frequent technique in cybercrime and anti-forensics scenarios. From a forensic perspective, rooting significantly impacts evidence integrity and

is often identified through artifacts such as the presence of su binaries, modified boot images, or root management applications.
While installing a custom ROM does modify the operating system, it does not inherently guarantee unrestricted system access unless the device is rooted. Jailbreaking applies specifically to iOS devices, not Android. Exploiting an iOS firmware vulnerability may lead to jailbreaking, but the scenario does not indicate an iOS environment.
CHFI v11 emphasizes that identifying whether a device has been rooted is critical during mobile investigations, as it affects data acquisition methods, trustworthiness of artifacts, and anti-forensic risk assessment .
Therefore, the most likely method used to achieve elevated privileges and unrestricted system access in this scenario is rooting the Android device , making Option C the correct answer.

質問**: 61**
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**: (**正解を表示します**)**
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: **62**
サイバーセキュリティを専門とするフォレンジック調査員として、あなたは「infected.pdf」という不審なPDF文書の分析を任されました。この文書は会社のサーバー上で発見され、組織のシステムとネットワークに脅威をもたらす可能性のある悪意のあるスクリプトが含まれている疑いがあります。PDF文書の調査の一環として、ファイル内の潜在的な悪意のあるコンポーネントを特定するために、どのような初期手順を踏みますか？
A. Linux ターミナルでコマンド python pdfid.py infected.pdf を実行して、ファイルの構造を確認し、埋め込まれたスクリプトを特定します。
B. 仮想マシン環境で PDF ドキュメントを開き、潜在的な悪意のある動作を観察します。
C. Web ベースのツールを使用して PDF ドキュメントからメタデータを抽出し、異常を分析します。
D. 16 進エディターを使用して、PDF ドキュメントの内容に疑わしいパターンがないか手動で検査します。
正解: **(**正解を表示します**)**
According to the CHFI v11 objectives under Malware Forensics and Static Malware Analysis , the correct initial step when analyzing a suspicious document-such as a potentially malicious PDF-is to perform static analysis before any execution . Running the tool PDFiD using the command python pdfid.py infected.pdf is a standard and CHFI-aligned first action. PDFiD is designed to quickly scan a PDF file and identify suspicious elements such as /JavaScript, /OpenAction, /Launch, /EmbeddedFile, and /AA, which are commonly abused by attackers to deliver malware through PDF documents.
This approach is non-intrusive and ensures the investigator does not accidentally trigger malicious code, thereby preserving evidence integrity and maintaining forensic soundness. Opening the file in a virtual machine (Option B) constitutes dynamic analysis , which

should only be performed after initial static indicators suggest malicious intent and after proper containment controls are in place. Metadata extraction (Option C) is useful but limited, as metadata alone does not reliably expose embedded exploit code. Manual hex inspection (Option D) is advanced and time-consuming and is not recommended as the first step.
The CHFI v11 Exam Blueprint emphasizes a structured malware analysis workflow , starting with static analysis tools like PDFiD for suspicious documents, making Option A the most appropriate and exam- accurate answer

質問: **63**
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: **D (**コメントを発表する**)**
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: **64**

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. 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。
B. アンパックツールを使用して、パック処理を逆に行い、元のコードを表示します。
C. 安全なコーディング手法を実装してください。
D. ネットワーク脆弱性スキャンの頻度を増やします。
正解: **B** (コメントを発表する)
Option B is the correct answer because CHFI v11 explicitly identifies program packers as an anti-forensics technique and separately lists program packers unpacking tools among the relevant forensic tools used to defeat or analyze such techniques.
Packers are commonly used to compress, obfuscate, or wrap malicious code so that its real contents are hidden from static inspection and some security tools. To investigate packed malware effectively, the examiner must reverse or remove that wrapper so the original executable code can be examined. That is exactly the role of unpacking tools .
This aligns with CHFI's focus on anti-forensics countermeasures and tools , and with malware-analysis objectives that require investigators to identify and extract malicious content before deeper examination.
The other options do not directly defeat the packing technique itself. Updating antivirus may improve detection in some cases, but it does not reveal the concealed code. Secure coding practices and vulnerability scanning are useful security measures, but they are not the forensic countermeasure for packed malware.
Therefore, the most effective response is to use unpacking tools to expose the underlying program for analysis.

質問: **65**
連邦捜査中、弁護士が意図せず連邦機関に機密情報を開示してしまいました。開示された情報には、企業クライアントの進行中の法的紛争に関する機密情報が含まれていました。上記のシナリオでは、意図しない開示によって弁護士 -依頼者間の秘匿特権または作業成果物の保護の放棄が連邦および州の訴訟手続きにおける未開示の通信にまで及ぶためには、どのような条件を満たす必要がありますか?
A. 公開された通信と非公開の通信は、異なる主題に関するものでなければなりません。
B. 権利放棄は意図的なものであってはなりません。
C. 漏洩は偶発的なものでなければなりません。
D. 権利放棄は意図的なものであり、開示された通信と開示されていない通信は同じ主題に関するものでなければなりません。
正解: **D** (コメントを発表する)
This question aligns with CHFI v11 objectives related to legal compliance, rules of evidence, and handling privileged information during forensic investigations. In digital

forensics, investigators frequently work alongside legal teams, making it critical to understand when attorney-client privilege or work-product protection may be waived. Under the U.S. Federal Rules of Evidence (Rule 502), an unintentional or inadvertent disclosure does not automatically extend the waiver of privilege to undisclosed communications.
For a waiver to extend beyond the disclosed material, strict conditions must be met. The waiver must be intentional , the disclosed and undisclosed communications must concern the same subject matter , and fairness must require that the undisclosed information also be considered. CHFI v11 emphasizes that forensic investigators must preserve confidentiality, respect legal protections, and avoid actions that could improperly broaden legal exposure during investigations.
Options B and C are incorrect because unintentional or accidental disclosures are explicitly protected from subject-matter waiver under Rule 502. Option A is incorrect because waiver extension only applies when communications involve the same subject matter. Therefore, Option D correctly reflects both legal standards and CHFI-aligned best practices for evidence handling and legal awareness during forensic investigations.

質問: **66**
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. ADB (Android Debug Bridge)
B. UFED Cellebrite
C. FTKイメージャー
D. iPhoneバックアップ抽出ツール
正解: **B (**コメントを発表する**)**
Option B. UFED Cellebrite is the strongest answer because CHFI v11 explicitly includes Logical Acquisition of Android and iOS Devices , Physical Acquisition of Android and iOS Devices , and Android and iOS Forensic Analysis under mobile forensics. The question asks for a tool that can perform a thorough logical acquisition of both Android and iOS , and among the listed options, UFED Cellebrite is the one most clearly suited to cross-platform mobile forensic collection.
ADB is Android-specific and does not address iOS acquisition. FTK Imager is primarily used for disk imaging and evidence preview rather than full mobile logical acquisition across both ecosystems. iPhone Backup Extractor focuses on iPhone backup data and does not cover Android in the same way.
Because the scenario requires a single solution that supports both major mobile platforms, the most appropriate CHFI-aligned answer is UFED Cellebrite . It matches the blueprint's

mobile acquisition objectives and the practical need for a forensic tool capable of structured logical collection from both Android and iOS devices.

質問: **67**
デジタルフォレンジックチームは、サイバー犯罪捜査において電子証拠の改ざんの可能性を含む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、彼らの主な懸念事項は何でしょうか？
A. IP 追跡によるサイバー攻撃の起源の分析。
B. ファイルの回復に高度な技術を採用しています。
C. 証拠改ざんに対するサイバー犯罪者の動機を特定する。
D. フォレンジックイメージングツールの精度を検証しています。
正解: **D (**コメントを発表する**)**
According to the CHFI v11 syllabus under Standards and Best Practices Related to Computer Forensics , the ENFSI (European Network of Forensic Science Institutes) Best Practices for Forensic Examination of Digital Technology place strong emphasis on the reliability, accuracy, and validation of forensic tools and methods . When investigating potential evidence tampering, the foremost concern is ensuring that the tools used to acquire, image, and analyze digital evidence are forensically sound and produce repeatable, verifiable results .
Verifying forensic imaging tools for accuracy ensures that the data acquired is an exact and complete representation of the original evidence , with no alteration introduced during the acquisition or analysis process. This directly supports evidence integrity, chain of custody, and legal admissibility-core principles repeatedly highlighted in CHFI v11. Tool validation also helps investigators defend their findings in court by demonstrating that industry-recognized, tested, and approved tools were used.
The other options do not align with ENFSI's primary focus. IP tracking (Option A) relates to attribution, not evidence integrity. File recovery techniques (Option B) are investigative actions but secondary to tool reliability. Determining criminal motive (Option C) falls under criminal profiling rather than forensic examination standards.
Therefore, consistent with CHFI v11 objectives and ENFSI best practices , verifying the accuracy and reliability of forensic imaging tools is the primary concern when addressing potential evidence tampering

質問: **68**
経験豊富なCHFI(認定情報セキュリティ専門家)であるグレッグは、大手ソフトウェア会社における知的財産窃盗事件の調査を依頼された。調査を進める中で、彼は同社のメールサーバーに重要な証拠が隠されている可能性があることを発見した。しかし、そのサーバーは別の会社と共有されており、アクセスするとその会社のプライバシー権を侵害する恐れがある。証拠の捜索と押収に関する規則や規制を遵守するために、グレッグはこの状況でどのような初期対応を取るべきだろうか？

A. 法律専門家および会社の経営陣と相談し、最善の解決策を探る。
B. メールサーバーは避け、他の潜在的な証拠源に焦点を当てる
C. 潜在的なプライバシー侵害を無視してサーバーを押収する
D. 直ちにサーバーを捜索 押収するための令状を取得する
正解: **(**正解を表示します**)**
Option A is the best answer because CHFI v11 explicitly includes Rules of Evidence , Best Practices for Handling Digital Evidence , Seeking Consent , Obtaining a Warrant for Search and Seizure , Legal Issues, Privacy Issues and Legal Compliance , and the Role of Local/International Agencies during Cybercrime Investigation . When a server is shared with another company , privacy and ownership concerns become especially important, and the initial step should be to consult the appropriate legal and organizational stakeholders before taking action.
Immediately seizing the server or ignoring privacy implications could violate legal boundaries and compromise admissibility. Avoiding the server entirely may also be inappropriate if it contains critical evidence. Likewise, jumping straight to a warrant may not be the most suitable first move until counsel and management clarify ownership, scope, privacy exposure, and the least intrusive legally defensible path.
Therefore, the strongest CHFI-aligned initial approach is to consult legal experts and company management to determine the correct lawful path forward before attempting access or seizure. That protects privacy rights, preserves admissibility, and aligns the investigation with proper search-and-seizure procedure.

質問: **69**
CHFIの調査員であるサラは、プライベートネットワークを通じて配布されている可能性のある児童搾取資料に関する事件を担当することになった。このネットワークは、ある市民が発見し、当局に通報したものである。
サラの仕事は、法律や規制に違反することなく、このネットワークを調査し、証拠を収集することだ。
事件の重大性と関係者への厳しい処罰の可能性を考慮すると、サラは収集した証拠が法廷で通用することを確実にしなければならない。サラはこの捜査において、まずどのような行動をとるべきだろうか？
A. ソーシャルエンジニアリングの手法を活用してネットワークに侵入し、関係するユーザーを特定する。
B. ネットワークトラフィックを監視して、潜在的な容疑者を特定します。
C. 容疑者に気づかれることなく、ネットワークに秘密裏にアクセスして証拠を収集する。
D. 最初の報告に基づいて捜索令状を取得し、ネットワークから合法的に証拠を収集する。
正解: **(**正解を表示します**)**
Option D is the best answer because the question explicitly emphasizes legal compliance , court admissibility , and the sensitive nature of the investigation. In CHFI methodology, the forensic examiner must first ensure there is proper legal authority before collecting

evidence, especially when investigating criminal conduct involving private systems or networks. A lawful foundation is necessary to protect the integrity and admissibility of the evidence.
Obtaining a search warrant before proceeding ensures that the collection process is authorized and defensible. This is especially important in cases involving severe criminal allegations, where improper access could undermine the entire prosecution. Once legal authority is secured, the investigator can then proceed with monitoring, evidence preservation, and deeper technical analysis under the proper process.
Options A and C involve deceptive or unauthorized access and would create legal and ethical problems.
Option B may be useful later, but it should not come before obtaining formal legal authorization. Therefore, the most appropriate first step is to obtain a search warrant based on the initial report and proceed through proper forensic and legal channels.

質問**: 70**
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 == 530
B. ftp.response.code == 213
C. ftp.response.code == 230
D. ftp.response.code == 550
正解**: (**正解を表示します**)**
Option C is correct because Taylor is trying to confirm whether the brute-force activity against the FTP service eventually resulted in a successful login . CHFI v11 explicitly includes network protocols and packet analysis , gathering evidence via sniffers , and analyze traffic for FTP and SMB password cracking attempts under network-forensics objectives.
In FTP analysis, the response code 230 indicates that the user has been logged in successfully. That makes it the key value an investigator would filter for after observing repeated failed attempts. By contrast, 530 is associated with failed authentication or not logged in, 213 is commonly related to file status information, and

550 typically indicates file unavailability or access issues rather than successful authentication.
Because CHFI emphasizes recognizing indicators of brute-force attempts and validating attack success through packet analysis, the correct Wireshark filter is ftp.response.code == 230 . This directly confirms whether the attacker moved from repeated FTP login failures to a successful authenticated session.

質問: **71**
マルウェア分析調査中に、疑わしいMicrosoft Officeドキュメントが潜在的な脅威として特定されました。このドキュメントにはマクロが埋め込まれており、開くと異常な動作を引き起こします。デジタルフォレンジックにおいて、疑わしいMicrosoft Officeドキュメントを分析する主な目的は何ですか？
A. 著者の身元を確認する
B. 文書の書式とレイアウトを最適化する
C. 文書内に埋め込まれた潜在的なマルウェアや悪意のあるコードを識別する
D. Microsoft Officeアプリケーションのパフォーマンスを向上させるため
正解: **C (**コメントを発表する**)**
According to the CHFI v11 objectives under Malware Forensics and Static and Dynamic Malware Analysis , Microsoft Office documents are one of the most common delivery mechanisms for malware, especially through malicious macros, embedded scripts, and exploit-laden objects . Attackers frequently weaponize Word, Excel, and PowerPoint files to execute malicious code when a user opens the document or enables macros.
The primary forensic purpose of analyzing suspicious Microsoft Office documents is to identify embedded malware or malicious code and understand how it executes. Investigators examine macro code (VBA), embedded objects, OLE streams, and document metadata to detect indicators such as obfuscated scripts, PowerShell execution commands, shellcode loaders, or downloader functionality. CHFI v11 emphasizes that this analysis helps determine the infection chain , execution triggers, and potential impact on the compromised system.
Options A, B, and D are not valid forensic goals in this context. Identifying the document author (Option A) may be supplementary but does not address the core threat. Formatting optimization (Option B) and performance improvement (Option D) are unrelated to forensic or security investigations.
The CHFI Exam Blueprint v4 explicitly includes analyzing suspicious Word, Excel, and PDF documents as part of malware investigations, highlighting the need to detect hidden malicious logic and prevent further compromise. Therefore, identifying embedded malware or malicious code is the correct and exam-aligned objective

質問: **72**

調査員は、疑わしいメディアからデータを取得した後、画像ファイルの互換性に関する問題に遭遇する可能性があります。
このセクションでは、E01形式のLinux用変換、起動可能なVMの作成、Linux上でのWindowsファイルシステムの扱い、APFSファイルシステムの扱いといったシナリオを概説します。各シナリオにおける解決策を解説し、最後にWindows、Linux、Macでのイメージ表示方法について解説します。捜査官は、検査用のイメージファイルを準備する際にどのような課題に直面する可能性があるでしょうか？
A. E01形式をWindows用に変換しています
B. WindowsワークステーションでのAPFSファイルシステムの取り扱い
C. 取得した証拠から起動可能なVMを作成する
D. Macワークステーションで画像ファイルを表示する
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.
The other options describe scenarios that are typically manageable with standard forensic workflows.
Converting E01 images (Option A) is well-supported using tools like ewfmount. Creating bootable VMs (Option C) is an advanced but solvable task using virtualization tools. Viewing images on macOS (Option D) is generally straightforward with native or commercial forensic software.
The CHFI Exam Blueprint v4 explicitly mentions APFS file system analysis challenges and cross-platform compatibility issues as key considerations during forensic image preparation. Therefore, handling APFS file systems on a Windows workstation represents a genuine and commonly encountered challenge, making Option B the correct and exam-aligned answer

質問**: 73**
デジタルフォレンジックチームは、複数のデバイスが侵害されたサイバー攻撃を調査しています。
押収されたデバイスの中には、Windows と Linux の両方のシステムとやり取りしたことを示す証拠がある Android スマートフォンが含まれていました。

Android および iOS のフォレンジック分析において、Windows および Linux デバイスに関連付けられたファイルを分析することが重要なのはなぜですか?
A. 侵害されたスマートフォンで使用されているオペレーティングシステムを確認する
B. WindowsおよびLinuxシステムの製造元を識別する
C. サイバー攻撃に関与する異なるデバイス間の接続を確立する
D. Androidスマートフォンのブランドとモデルを特定する
正解: **(**正解を表示します**)**
This scenario aligns with CHFI v11 objectives under Mobile and IoT Forensics and Cross-Platform Digital Evidence Correlation . Modern cyberattacks frequently involve multiple devices and operating systems working together as part of a single attack chain. In mobile forensic investigations, Android and iOS devices often store artifacts that reflect interactions with external systems such as Windows and Linux machines.
These artifacts may include USB connection logs, file transfer records, SSH keys, shared application data, cloud sync traces, or remnants of malware propagation.
CHFI v11 emphasizes the importance of event correlation and timeline analysis across heterogeneous environments. By analyzing Windows- and Linux-related files found on a mobile device, investigators can establish relationships between compromised endpoints, reconstruct attacker movement, and identify how data or malware was transferred between systems. This cross-device correlation is essential for attributing actions, understanding lateral movement, and proving coordinated activity during an incident.
The other options focus on device identification details, which are typically obtained through mobile hardware and OS artifacts, not through external system files. Therefore, the correct forensic purpose is to establish connections between multiple devices involved in the cyberattack, making option C the correct and CHFI-aligned answer.

質問: **74**
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. エズヴィッド
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: **75**
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.
CHFI v11 explicitly highlights ShellBags and BagMRU keys as essential artifacts for reconstructing user behavior, especially in cases involving data exfiltration or insider misuse. Therefore, the correct and CHFI- verified answer is BagMRU key (Option A) .

質問: **76**
イベント相関では、2つのタイプが議論されています。1つは同一プラットフォーム(Microsoft Windowsなど)で、もう1つは異なるOSとハードウェアが使用されるクロスプラットフォーム(Windowsクライアントと Linuxファイアウォールなど)です。クロスプラットフォーム相関の適用例として、どのシナリオが最も適切でしょうか？
A. ネットワーク全体で統一されたソフトウェアバージョンを実装する
B. WindowsサーバーとLinuxベースのファイアウォールを活用する
C. Linuxベースのサーバーのみを使用する
D. デバイスごとに異なるウイルス対策ソフトウェアを使用する
正解: **B (**コメントを発表する**)**
Event correlation in CHFI v11 is a critical investigative technique used to reconstruct attack timelines by analyzing and correlating events from multiple log sources. The CHFI blueprint clearly distinguishes between Same-Platform Correlation and Cross-Platform Correlation under the domain of Image/Evidence Examination and Event Correlation .
Cross-Platform Correlation applies when an investigation involves heterogeneous environments , meaning different operating systems, hardware platforms, or network devices are involved in the incident. A common real-world example-explicitly referenced in CHFI training-is an enterprise environment where Windows-based client systems or servers interact with Linux-based infrastructure components such as firewalls, IDS/IPS devices, or proxies . In such cases, investigators must correlate Windows Event Logs with

Linux syslogs, firewall logs, and network device records to build a unified timeline of attacker activity.
Option B correctly reflects this scenario by describing the use of Windows servers alongside Linux-based firewalls , which is a textbook example of Cross-Platform Correlation. Option A relates to standardization, not correlation. Option C represents a single-platform environment, and Option D refers to security tooling diversity rather than operating system or platform diversity.
CHFI v11 emphasizes Cross-Platform Correlation as essential for detecting multi-stage attacks , lateral movement, and perimeter breaches in modern hybrid infrastructures, making Option B the correct and exam- aligned answer

質問: **77**
ジョンという名のサイバーセキュリティアナリストは、度重なる攻撃に直面している組織で働いています。ジョンは、Windowsオペレーティングシステムを実行しているサーバーの1つで異常な動作に気づきました。そのサーバーは、ランダムなIPアドレスへの接続を繰り返し試みていました。調査の結果、組み込みの管理者アカウントが侵害され、これらの接続に使用されていることがわかりました。そこでジョンは、pwdump7を使用してシステムからハッシュを抽出することにしましたが、抽出されたハッシュがどのような種類のものか解読できませんでした。
ハッシュ値は「8846f7eaee8fb117ad06bdd830b7586c」でした。このハッシュ値を解読するのに最適なパスワード解析ツールは次のうちどれですか？
A. ハッシュキャット
B. 切り裂きジョン
C. レインボークラック
D. L0phtCrack
正解: **(**正解を表示します**)**
Option D. L0phtCrack is the best answer because the scenario specifically involves a Windows account hash extracted using pwdump7 , and the question asks for the tool best suited to crack that type of Windows password hash in a CHFI context. CHFI v11 explicitly includes password cracking tools and using rainbow tables to crack hashed passwords among its anti-forensics and analysis-related objectives.

Among the listed tools, L0phtCrack is the one most classically associated with Windows password hash auditing and cracking , especially in enterprise and forensic contexts involving local account credentials.
While Hashcat and John the Ripper are very powerful general-purpose password-cracking tools, the phrasing of the question points most directly to the Windows-focused choice.
RainbowCrack is oriented toward rainbow-table-based attacks rather than being the best general answer for this specific Windows hash scenario.
Therefore, under CHFI's treatment of Windows password analysis and cracking tools, the most appropriate answer is L0phtCrack .

質問**: 78**
データ収集前に、媒体をサニタイズして以前の情報を消去する必要があります。業界標準では、機密レベルに基づいてデータ破壊方法が規定されています。調査員は、VSITR、NAVSO、DoD、NIST SP 800-88などの標準に準拠しています。物理的な破壊方法には、データの取得を防止し機密性を保護するためのクロスカットシュレッディングが含まれます。
デジタルフォレンジックでデータを取得する前にデータのセキュリティを確保するための重要なステップは何ですか?
A. 対象メディア上のデータを上書きする
B. 対象メディアのリサイクル
C. 対象メディアのフォーマット
D. データサニタイズを無視
正解**: A (**コメントを発表する**)**
This question aligns with CHFI v11 objectives under Data Acquisition and Duplication , specifically media preparation and data sanitization standards . Before using any storage media for forensic acquisition, investigators must ensure that it does not contain residual data that could contaminate evidence or cause data leakage. CHFI v11 stresses that data sanitization is mandatory prior to acquisition to maintain confidentiality, integrity, and forensic soundness.
According to standards such as NIST SP 800-88 , DoD, NAVSO, and VSITR, simply formatting a disk is insufficient because formatting only removes file system references while leaving underlying data intact and potentially recoverable. Recycling media without sanitization poses severe security risks, and ignoring sanitization violates forensic and legal best practices.
Overwriting the target media -also known as data wiping-is a recognized and approved sanitization method. It replaces existing data with predefined patterns (e.g., zeros, ones, or random data), ensuring previous information cannot be recovered. CHFI v11 highlights overwriting as a logical sanitization technique suitable when physical destruction is not required.

Therefore, consistent with CHFI v11 and industry standards, overwriting the data on the target media is the crucial step to ensure data security before forensic data acquisition.

質問: **79**
企業に対する大規模なマルウェア攻撃の後、フォレンジックアナリストのボブは調査を依頼された。マルウェアは痕跡を消すために、システム全体のファイルとフォルダに多数の変更を加えていた。ボブはマルウェアの動作を理解するために、これらの変更を綿密に監視することにした。ボブは、システム内のファイルとフォルダで発生しているすべての変更を監視し、ログに記録するために、どのようなツールを使用できるだろうか？
A. IDA Pro
B. EnCase
C. Sysmon
D. FTKイメージャー
正解: **(正解を表示します)**
Option C. Sysmon is the best answer because CHFI v11 explicitly includes system behavior analysis involving monitoring files and folders , along with monitoring processes, services, startup programs, Windows event logs, API calls, and device drivers . In this scenario, Bob needs a tool that can log file and folder changes on a Windows system so he can understand how the malware modified the environment to hide itself.
Sysmon is designed to generate detailed system activity logs that can help investigators track suspicious changes and correlate them with process execution and other indicators of compromise. That makes it much more appropriate than the other choices. IDA Pro is primarily for reverse engineering binaries, EnCase is a broad forensic suite rather than a dedicated real-time system activity monitor, and FTK Imager focuses on imaging and evidence preview rather than ongoing change logging.
Because the question is specifically about monitoring and logging changes to files and folders , Sysmon is the most direct and CHFI-aligned answer for observing malware behavior at the system level.

質問: **80**
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** (コメントを発表する)
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.
While deletion events are logged separately (e.g., Event ID 4660), and general logon activity is captured by different event IDs (such as 4624), Event ID 4663 focuses specifically on object access attempts . Option C is partially descriptive but too broad; the defining characteristic of Event ID 4663 is the attempt to open an object with specific access rights , making option A the most precise and CHFI v11-aligned answer.

質問: **81**
フォレンジック調査員のアリアは、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、ア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: (正解を表示します)
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.

Autopsy (Option B) is a forensic analysis platform but does not perform E01-to-raw mounting itself. UFS Explorer (Option C) is a commercial forensic tool used for file system analysis, not image conversion. fdisk (Option D) is a disk partitioning utility and cannot mount or convert forensic image formats.
The CHFI Exam Blueprint v4 emphasizes proper forensic image handling, validation, and analysis on Linux systems , making ewfmount the correct, forensically sound, and exam-aligned tool for converting and mounting E01 images

質問: **82**
あなたはサイバーセキュリティ企業のデジタルフォレンジック専門家として、データ漏洩事件の捜査に深く関わっています。
あなたは、情報漏洩に関連するマルウェアが潜んでいる可能性があると思われる顧客のコンピュータのWindowsレジストリを精査する任務を負っています。潜在的なマルウェアのエントリを見つけるために、レジストリのどの部分を重点的に調べるべきでしょうか？
A. HKEY_CLASSES_ROOT
B. HKEY_LOCAL_MACHINE
C. HKEY_CURRENT_USER
D. HKEY_USERS
正解: **B (**コメントを発表する**)**
Option B. HKEY_LOCAL_MACHINE is the best answer because CHFI v11 specifically emphasizes Windows memory and registry analysis as part of evidence examination and operating system forensics.
The blueprint also highlights registry-based malware persistence mechanisms and system behavior analysis , including monitoring registry artifacts, startup programs, processes, services, and event logs to identify suspicious or malicious activity.
In practical forensic work, HKEY_LOCAL_MACHINE (HKLM) is one of the most important hives because it contains system-wide configuration settings that affect the whole computer, not just one user.
Malware commonly establishes persistence there through machine-level startup locations, service entries, driver references, and other autostart mechanisms. That makes HKLM a primary place to examine when trying to identify malware that survives reboots or affects all users on the system. This fits CHFI's focus on analyzing Windows artifacts and identifying persistence mechanisms.
The other hives can also contain useful evidence, especially user-specific activity, but for main focus in spotting broad malware persistence, HKLM is the strongest CHFI-aligned answer.

質問: **83**
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: **A (**コメントを発表する**)**
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: **84**
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すが、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: **(**正解を表示します**)**
According to the CHFI v11 Dark Web Forensics domain, Tor bridge nodes are specifically designed to help users bypass censorship and surveillance in restrictive environments. Governments and ISPs often block access to Tor by identifying and filtering traffic destined for publicly listed Tor entry (guard) nodes .
Once these entry nodes are blocked, users can no longer connect to the Tor network using standard configurations.
Bridge nodes solve this problem by acting as unlisted entry relays whose IP addresses are not published in the public Tor directory . As a result, censorship mechanisms cannot easily identify them. From a forensic and technical perspective, CHFI v11 explains that bridges effectively disguise the initial connection point , making Tor traffic appear less distinguishable from normal internet traffic-especially when combined with pluggable transports such as obfs4 or meek.
While Tor uses layered encryption (onion routing), that function applies to all Tor connections and is not unique to bridges. Bridge nodes do not host websites, and they are explicitly not publicly listed , making Option D incorrect. The key advantage bridges provide is concealing the Tor entry point , which prevents IP-based blocking.
CHFI v11 emphasizes understanding Tor infrastructure-including bridges, relays, and exit nodes-to correctly interpret dark web traffic and censorship circumvention techniques during investigations.
Therefore, bridge nodes assist users in accessing the Tor network by disguising their IP addresses and entry points , making Option C the correct and CHFI v11-verified answer.

質問: **85**
ある組織は、大規模な電子データセットの広範な分析に伴うeDiscoveryコストの最小化に取り組んでいます。この目標達成のため、同組織は高度な手法と自動化プロセスを導入し、詳細な調査が必要なデータの量を効果的に絞り込み、コンプライアンスを維持しながら効率性を向上させています。また、特定のプラットフォームとプロセスを活用することで、ワークフローの早い段階で関連データのみを分析し、重複データを除外しています。
組織は効率的なデータ検査を確実に実行するためにどのようなベストプラクティスを実装していますか?
A. 組織は、不要になったデータを安全に廃棄するためのデータ保持ツールを実装します。
B. 組織は、テクノロジー支援レビュー (TAR) とデータ削減ツールを使用して、レビュー プロセスから無関係なデータを除外します。

C. 組織は、eDiscovery プロセス全体を通じて安全な保管チェーンを確保するためのツールを採用しています。
D. 組織はデータ マッピング ツールを使用して管理者を識別し、関連データの場所を追跡します。
正解: **B (**コメントを発表する**)**
This question aligns with CHFI v11 objectives under Computer Forensics Fundamentals and eDiscovery and Digital Evidence Management . CHFI v11 emphasizes that one of the most effective ways to reduce eDiscovery costs and timelines is through early data reduction and intelligent filtering . Organizations increasingly rely on Technology-Assisted Review (TAR) , also known as predictive coding, combined with data reduction techniques such as deduplication, de-NISTing, keyword filtering, and relevance scoring.
TAR leverages machine learning algorithms to identify patterns in relevant documents and automatically prioritize or exclude data that is unlikely to be responsive. This significantly reduces the volume of data requiring manual review while maintaining defensibility and compliance with legal and regulatory requirements. CHFI v11 highlights TAR as a best practice for handling large-scale electronic evidence efficiently, especially in litigation and regulatory investigations.
The other options support eDiscovery but do not directly reduce review scope: data retention focuses on lifecycle management, chain of custody ensures evidence integrity, and data mapping identifies data sources.
None directly address excluding irrelevant data early in the review process . Therefore, consistent with CHFI v11 eDiscovery best practices, using technology-assisted review (TAR) and data reduction tools is the correct answer.

質問: **86**
国際的なソフトウェア開発会社のシニアフォレンジックアナリストとして、あなたは内部脅威の疑いに関する進行中の調査を担当しています。複数のプロジェクトファイルが会社のセキュリティ保護されたサーバーから紛失したと報告されています。あるケースでは、ジュニアチームメンバーが、上司を装ったメールを受け取り、特定のファイルを共有ネットワークの場所に移動するように指示されたと報告しました。指示に従ったところ、ファイルは消えてしまいました。調査の一環として、関係するすべてのシステムのディスクイメージを取得しました。次に取るべき行動は何ですか？
A. ディスクイメージの即時分析を実行し、分析対象となる可能性のあるマルウェアを特定して抽出することに重点を置きます。
B. ファイルを移動したチームメンバーにインタビューして、データ損失に何らかの役割を果たしたかどうかを確認します。
C. ディスクイメージから削除されたファイルの復元を優先し、それらの削除につながった可能性のあるソフトウェアやプロセスを精査します。
D. 不正なメールの発信元を特定するために、メールヘッダーとサーバーログの詳細な分析を実施します。

正解: **D** (コメントを発表する)
Option D is the best answer because the scenario strongly suggests a deceptive email-based social engineering event that triggered the movement and disappearance of the files. The most important next step is to identify whether the email was genuinely sent by the manager or whether it was spoofed, relayed, or otherwise malicious. In CHFI terms, this aligns with examining the source of the incident , correlating email artifacts with server logs , and reconstructing the sequence of events to determine attribution and attack method.
Although disk images have already been acquired, the question asks for the next step in the investigation.
Since the trigger was a suspicious instruction sent by email, analyzing email headers can reveal sender path, relay details, spoofing indicators, and authentication issues. Reviewing server logs can then confirm access activity, file movement, and related actions around the same timeframe. That gives the investigator a clearer understanding of whether this was phishing, impersonation, or insider misuse.
Option A is too broad, B is premature, and C focuses on consequences rather than the initiating cause.
Therefore, header and log analysis is the strongest first analytical move.

質問: **87**
複数のユーザーから一連の不審な活動が報告されたことを受け、ある有名eコマース企業が調査を受けている。あるユーザーは不正購入を報告し、別のユーザーは個人情報の変更を報告した。
社内のセキュリティチームは、複数のセッションが重複していることを発見し、複数のユーザーが異なる地理的な場所で同じセッションを使用している可能性を示唆しました。チームは、セッションクッキーが攻撃者によって傍受され、悪用されたに違いないと結論付けました。フォレンジック調査官として、このセキュリティインシデントの最も可能性の高い原因として、どのような種類の攻撃が考えられますか？
A. クロスサイトスクリプティング(XSS)攻撃。
B. ブルートフォース攻撃。
C. SQLインジェクション攻撃。
D. パラメータ改ざん攻撃。
正解: (正解を表示します)
Option A. Cross-Site Scripting (XSS) attack is the most probable answer because the scenario centers on session cookies being intercepted and reused by an attacker , leading to overlapping sessions and unauthorized actions. CHFI v11 explicitly includes Investigating Cross-Site Scripting, SQL Injection, and Directory Traversal Attacks and also Investigating Brute Force Attack and Cookie Poisoning Attack under web application forensics.

Among the options provided, XSS is the best fit because it is a common method used to steal or abuse session cookies . Once an attacker obtains a valid session cookie, they can hijack a logged-in session and act as the victim without needing to know the password. That explains unauthorized purchases, profile changes, and simultaneous use of the same session from different locations.
Brute force focuses on guessing passwords, not using intercepted session cookies. SQL injection targets database queries and does not directly explain cookie reuse. Parameter tampering involves modifying request values, but the stronger clue here is stolen session cookies , which aligns more closely with XSS- driven session hijacking. Therefore, under CHFI's web-attack investigation objectives, XSS is the most likely cause among the listed choices.

質問**: 88**
フォレンジック調査員のジャンナは、容疑者のハードドライブから作成したフォレンジックイメージファイルの整合性を確認する任務を負っています。イメージファイルが元のドライブと一致することを確認するには、イメージファイルと元のメディアを比較するコマンドを使用する必要があります。
検証を実行するには、次のどの dcfldd コマンドを使用する必要がありますか?
A. dcfldd if=/dev/sda vf=image.dd
B. dcfldd if=/dev/sda 分割=2M of=usbimg ハッシュ=md5 ハッシュログ=usbhash.log
C. dcfldd if=/dev/sda of=usbimg.dat
D. dd if=/dev/sdb | split -b 650m - image_sdb
正解**: (**正解を表示します**)**
This question aligns with CHFI v11 objectives under Data Acquisition and Duplication , specifically image validation and forensic integrity verification . After acquiring a forensic image, it is a mandatory best practice to verify that the image is an exact bit-for-bit replica of the original evidence source. CHFI v11 stresses that verification protects evidence integrity and supports legal admissibility by proving that no data was altered during acquisition.
The dcfldd tool-an enhanced version of the Unix dd utility-supports forensic features such as hashing, logging, splitting, and image verification . The vf (verify file) parameter in the command dcfldd if=/dev/sda vf=image.dd directly compares the original input device (/dev/sda) with the previously created image file (image.dd). This ensures that both sources match exactly, sector by sector.
Option B performs imaging with hashing but does not verify an existing image against the original drive.
Option C simply creates an image without validation, and Option D uses dd with file splitting, which lacks forensic verification features. Therefore, consistent with CHFI v11 acquisition validation standards, Option A is the correct command to verify the forensic image against the original medium.

質問: **89**
CHFI資格を持つマーサは、大手オンライン小売企業に対するサイバー攻撃に関する重要な案件を担当することになった。マーサは、この攻撃に関連するデジタル証拠を収集し、調査する任務を負っている。
しかし、この小売企業は世界各地にサーバーを設置しており、グローバルな事業展開を行っている。
ACPO(米国刑事検察官協会)のデジタル証拠に関する原則を考慮すると、マーサはこの複数の法域にまたがる事件を扱う際に、何を最も重視すべきでしょうか？
A. 収集したすべての証拠を彼女のローカルワークステーションに保存する。
B. 同意の必要性を放棄し、すべてのサーバーの調査を直ちに開始する
C. 彼女の管轄区域にあるサーバーのみに焦点を当てる
D. 各管轄区域の地方当局と連携して証拠を収集する
正解: **D (**コメントを発表する**)**
Option D is the best answer because CHFI v11 emphasizes that investigators must follow rules of evidence , search and seizure requirements , privacy and legal compliance , and the role of local/international agencies during cybercrime investigation . In a multi-jurisdictional case, Martha cannot simply access all servers on her own authority. She must ensure that evidence collection is lawful and admissible in each country involved. Coordinating with local authorities in each jurisdiction is the most defensible approach because it respects local laws, preserves evidence properly, and helps maintain chain of custody. This also aligns with ACPO- style evidence principles that emphasize preserving integrity and acting within proper authority. Collecting evidence without jurisdictional coordination could create legal challenges and risk exclusion of evidence later.
Option A is unsafe and improper for primary evidence handling. Option B ignores consent and legal process.
Option C is too limited and may overlook critical evidence outside her own jurisdiction.
Therefore, under CHFI legal and procedural objectives, the correct priority is to coordinate with relevant authorities in each jurisdiction before gathering evidence .

質問: **90**
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捜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への同意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ます。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. 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。
B. 捜索令状を放棄し、入手可能なデータに基づいて捜査を開始する。

C. 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。
D. 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
正解**: (**正解を表示します**)**
Option D is the correct answer because CHFI v11 places major emphasis on rules of evidence , seeking consent , obtaining a warrant for search and seizure , legal issues, privacy issues and legal compliance , and the role of local/international agencies during cybercrime investigation . In a case involving multiple jurisdictions , cross-border systems , and lack of client consent, the investigator's first duty is to ensure the evidence-gathering process is legally valid in every relevant jurisdiction.
Working closely with legal counsel is essential because improper access can compromise admissibility, violate privacy laws, and expose the firm to legal liability. CHFI also highlights best practices for handling digital evidence , preserving evidence , and the importance of lawful authority before conducting intrusive forensic activity.
Option A is too limited and may ignore critical evidence. B would violate legal procedures. C is clearly improper because ownership claims do not override consent, privacy, or jurisdictional requirements.
Therefore, the most defensible and CHFI-aligned initial approach is to coordinate with the legal team, understand each legal regime, and obtain the necessary warrants or permissions before proceeding.

質問**: 91**
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**: (**正解を表示します**)**
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: **92**
フォレンジック調査中、ロバートは攻撃者が特定の悪意あるファイルのファイル拡張子を改変し、無害に見えるように見せかけていることを発見しました。これらのファイルは元々実行ファイルでしたが、本来のファイルの性質を隠すために拡張子が変更されていました。ロバートは、紛らわしい拡張子を持つこれらのファイルを識別し、抽出する必要があります。調査中にファイル拡張子の不一致を検出し、実際のファイルタイプを復元するのに役立つツールは次のどれですか？
A. OSForensics
B. タイムストンプ
C. 剖検
D. ステゴハント
正解: **(**正解を表示します**)**
According to the CHFI v11 objectives under Digital Forensics Review and Anti-Forensics Techniques , attackers frequently use file extension manipulation as an anti-forensic technique to conceal malicious executables by renaming them with harmless-looking

extensions such as .txt, .jpg, or .pdf. This tactic relies on the assumption that investigators or users will trust the file extension rather than verifying the file's true structure.
Autopsy , which is built on The Sleuth Kit (TSK) , provides a dedicated capability to detect file extension mismatches by analyzing file headers (magic numbers) and comparing them against the file's extension. If a file's internal signature does not match its extension, Autopsy flags it as suspicious, allowing investigators to identify hidden executables and recover their true file types. CHFI v11 explicitly highlights "Detecting File Extension Mismatch using Autopsy" as a key forensic technique for defeating anti-forensics.
OSForensics is primarily used for detecting data hiding techniques such as alternate data streams and overwritten metadata, while Timestomp is itself an anti-forensic tool used to manipulate timestamps.
StegoHunt focuses on steganography detection rather than file type validation.
The CHFI Exam Blueprint v4 emphasizes the importance of file type analysis and extension mismatch detection when investigating disguised malware, making Autopsy the most appropriate and exam-aligned tool in this scenario

質問: **93**
大規模企業内で発生したデータ侵害の疑いを受け、調査担当者が膨大なネットワークログの分析を任されました。このタスクには、複数のネットワークデバイスからログを収集・管理するだけでなく、リアルタイムのアラート管理、メタデータ分析、異常なトラフィックパターンの明確な表示を可能にするツールが必要です。調査担当者は、ログを整理し、ネットワークイベントを関連付けて攻撃の全容を把握するための最も効果的なソリューションを特定する必要があります。このタスクに最も適したツールは次のうちどれでしょうか？
A. セキュリティオニオン
B. OSFClone
C. インテラプロ
D. 表
正解: **(正解を表示します)**
Option A. Security Onion is the best answer because the question requires a solution for collecting and managing logs from multiple devices , supporting real-time alerting , enabling metadata analysis , and helping investigators correlate events across the environment. CHFI v11 explicitly includes centralized logging using SIEM solutions , SIEM solutions , types of event correlation , event correlation approaches , and incident detection and examination with SIEM tools .
Security Onion fits that need because it is built around enterprise-scale monitoring, alerting, and network visibility. It is far more suitable than the other options for incident-centric log aggregation and correlation.
OSFClone is a bootable acquisition utility, not a log-correlation platform. Intella Pro is oriented toward eDiscovery and evidence review rather than network event monitoring.

Tableau is commonly associated with write-blocking hardware, not SIEM-style network analysis.
Because the task is to organize logs, examine anomalous traffic patterns, and correlate network events to understand the attack timeline and scope, the most CHFI-aligned choice is Security Onion . It best matches the blueprint's network-forensics and SIEM-focused objectives.

質問: **94**
ネットワークセキュリティアナリストのエミリーは、社内ネットワークへの疑わしい攻撃を受け、シスコのファイアウォールによって生成されたログを確認しています。そこで、疑わしい接続試行に関するログメッセージを発見しました。ログには、ニーモニック106022のエントリが表示されています。ファイアウォールのログパターンに基づいて、エミリーが発見したログメッセージを最もよく表すものは次のうちどれですか？
A. インターフェース interface_name 上の source_address から dest_address へのプロトコル接続スプーフィングを拒否します。
B. ICMPパケットタイプICMP_typeは送信リストacl_ID src inside_address dest outside_addressによって拒否されました
C. インターフェース interface_name 上の source_address から dest_address へのプロトコル逆パスチェックを拒否します。
D. IP_addressからIP_addressへのIPティアドロップフラグメント(サイズ = 数値、オフセット = 数値)を拒否します。
正解: **A (**コメントを発表する**)**
This question aligns with CHFI v11 objectives under Network and Web Attacks and Network Log Analysis , particularly the interpretation of Cisco firewall (ASA) log messages . Cisco ASA firewalls use numeric mnemonics to categorize and describe specific security events. Understanding these mnemonics is critical for forensic investigators when reconstructing attack attempts and identifying malicious network behavior.
The Cisco ASA message ID 106022 corresponds to a "Deny protocol connection spoof" event. This log entry is generated when the firewall detects a packet with a spoofed source address , meaning the packet's source IP does not match the expected routing or interface from which it was received. Such behavior is commonly associated with reconnaissance, evasion attempts, or denial-of-service attacks.
CHFI v11 emphasizes that spoofed connection attempts are strong indicators of malicious activity and are frequently logged by perimeter security devices. By analyzing this log, investigators can identify attempted impersonation, trace attack origins, and correlate events across network devices.
The other options represent different Cisco ASA mnemonics, such as ICMP filtering, reverse path forwarding (RPF) failures, and teardrop attack detection. Therefore, based on Cisco firewall logging patterns, the correct description for mnemonic 106022 is "Deny

protocol connection spoof from source_address to dest_address on interface interface_name."

質問: **95**
鑑識捜査官のエブリンは、重要な証拠データを保管するための安全なストレージシステムを構築しています。彼女は、大容量ディスクに対応し、CRC(巡回冗長検査)と64ビット論理ブロックアドレス(LBA)を使用してデータの整合性を確保できる新しいストレージシステムを購入しました。このシステムは、最大8 ZiBのパーティションに対応し、最大128個のパーティションを処理できます。仕様を確認した後、エブリンは、システムで使用されているパーティショニング方式がこれらの機能をサポートしていることを確認しました。エブリンは、ストレージシステムにどのようなパーティショニング方式を使用していますか？
A. BPB
B. GPT
C. MBR
D. クラスター
正解: **(正解を表示します)**
Option B. GPT is the correct answer because the features described in the question match the GUID Partition Table standard rather than the older MBR scheme. CHFI v11 includes storage fundamentals such as partitioning structures , booting process , and system layout concepts relevant to forensic acquisition and evidence handling.
The strongest clues are the use of 64-bit LBAs , support for very large partitions up to 8 ZiB , protection mechanisms such as CRCs , and support for as many as 128 partitions . Those are characteristic GPT capabilities. By contrast, MBR is much more limited in partition count and addressable disk size and does not provide the same structural protection through CRC-based integrity checking. BPB refers to the BIOS Parameter Block within certain file-system structures, not the overall partitioning scheme. Clusters are file-system allocation units, not a partition table format.
Because the scenario is specifically about a partitioning method that supports modern large-disk and integrity features, the answer that best aligns with CHFI storage and system-structure objectives is GPT .

質問: **96**
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: **97**
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. すべてのシステムに対して厳格なアクセス制御を実装します。
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. 潜在的な脆弱性を修正するために、すべてのデバイスにシステムアップデートを展開します。
正解: **(**正解を表示します**)**
Option C is the best first course of action because, in a complex intrusion involving anti-forensics , the investigation must first establish the scope and impact of the breach before deeper reverse engineering or broad remediation decisions are made. CHFI v11 emphasizes the forensic investigation process , including first response , evidence

preservation , case analysis , and understanding indicators of compromise and anti-forensics challenges .
Determining exactly what data was compromised is foundational. It helps investigators define the severity of the incident, identify affected systems and stakeholders, prioritize evidence collection, and support legal, regulatory, and business response requirements. Without first establishing the compromised data set, later activities such as reverse engineering attacker methods or deploying broad controls may be less targeted and less effective.
Option A may become important later, but it is not the most immediate first step in understanding breach impact. B and D are response measures, yet prematurely changing the environment can complicate forensic analysis. Therefore, under CHFI's investigation-process and anti-forensics principles, the most appropriate first action is to identify the exact data that has been compromised .

質問**: 98**
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**: (**正解を表示します**)**
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.
In contrast, the other options are well-documented consequences of poor forensic readiness in CHFI v11.

Lack of preparation often results in inability to collect legally sound evidence (Option D), which affects court admissibility. Limited collaboration with legal and IT teams (Option C) occurs when roles, procedures, and escalation paths are not predefined. Additionally, without proper controls and monitoring, data manipulation, deletion, and theft (Option A) may go undetected or untraceable.
The CHFI Exam Blueprint v4 emphasizes forensic readiness as a strategic capability focused on evidence integrity, compliance, and investigative efficiency , not on preventing or causing system downtime, making Option B the correct and exam-aligned answer

質問**: 99**
ある多国籍企業は、財務記録や顧客情報などの重要な業務データを保存するために、Google Cloud Storage(CCS)を利用しています。最近、同社はCCS環境内で機密文書への不正アクセスを発見し、データ漏洩の可能性について懸念を抱いています。
Google Cloud Storageのアクセスログとメタデータには、どのような種類の情報が含まれていますか？
A. ファイルへのアクセスと変更のタイムスタンプ。
B. 従業員のログイン認証情報。
C. 保存されたファイルの暗号化キー。
D. ネットワークインフラストラクチャ構成の詳細
正解**: (**正解を表示します**)**
Option A is the correct answer because CHFI v11 explicitly includes Cloud Storage Forensics , Google Cloud Forensics , Cloud Digital Evidence Analysis , and data acquisition in the cloud . In cloud investigations, logs and metadata are essential evidence sources because they help reconstruct who accessed an object, when it was accessed, and what actions were performed. For that reason, timestamps of file access and modification are the most relevant and expected contents of cloud access logs and metadata.
This aligns with standard forensic objectives of identifying unauthorized access, establishing a timeline, and preserving evidence in a defensible format. Access logs are meant to record events, not reveal highly sensitive secrets such as employee login credentials or encryption keys . Likewise, network infrastructure configuration is a different category of information and is not the primary purpose of object access logs in cloud storage.
From a CHFI perspective, cloud forensics relies heavily on event records, timestamps, metadata, and activity history to establish whether files were viewed, modified, copied, or accessed from suspicious sources. Therefore, when examining cloud storage for signs of breach activity, timestamps associated with access and modification are the strongest and most forensic-relevant answer.

質問**: 100**

フォレンジック調査員は、複数のオンラインプラットフォームにまたがる企業の機密情報の流出に関わるデータ漏洩の調査を任されています。被疑者は、様々な公開チャネルを通じてデータを密かに共有していたと考えられています。証拠を発見するために、調査員は複数のネットワークから投稿、写真、動画、ユーザーインタラクションを収集する必要があります。調査員は、これらのデータを効率的に収集、整理、分析し、さらなる調査のための証拠の完全性を確保できるツールを必要としています。このタスクに最適なツールはどれでしょうか？
A. ライム
B. エラスティックスタック
C. ソーシャルネットワークハーベスター
D. ガイマガー
正解: **(正解を表示します)**
This scenario aligns with CHFI v11 objectives under Network and Web Attacks and Social Media Forensics , where investigators are required to collect and analyze digital evidence from online platforms while preserving evidentiary integrity. When sensitive data is leaked through public or semi-public online channels, social media and online network artifacts such as posts, multimedia content, comments, likes, and user relationships become critical sources of evidence.
Social Network Harvester is specifically designed for social media and online platform investigations. It allows forensic investigators to systematically collect data such as posts, images, videos, timestamps, usernames, and interaction metadata from multiple social networks. CHFI v11 emphasizes the importance of using purpose-built tools that support structured collection, proper documentation, and evidence preservation to maintain chain of custody and admissibility.
LiME is a volatile memory acquisition tool, Elastic Stack is primarily used for log aggregation and analysis, and Guymager is a forensic disk imaging tool. None of these are suitable for harvesting social media content.
Therefore, Social Network Harvester is the most appropriate CHFI-aligned tool for efficiently gathering, organizing, and analyzing social network evidence in data leakage investigations.

質問: **101**
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.
Option A is incorrect because file content is not immediately deleted. Options B and C contradict fundamental forensic principles taught in CHFI v11 regarding logical deletion. Understanding this behavior is critical for forensic investigators, as it enables recovery of evidence that suspects may believe is permanently removed.
Therefore, the correct explanation is that the file pointer is deleted, but the content still remains on the disk, making recovery possible.

質問: **102**
複雑な調査において、調査員は組織のメールクライアントによって生成された破損したファイル形式からメールデータを抽出するという任務を負います。調査員は、このファイルを広く互換性のあるEML形式に変換し、分析のためにデータに容易にアクセスできるようにするツールを必要としています。また、ツールは、関連するデータのみを選択的に移行するための高度なフィルタリングオプションを備え、様々なメールサーバーやWebベースのプラットフォームへの移行をサポートする必要があります。このタスクに最適なツールはどれでしょうか？
A. OST から PST へのカーネル
B. メールチェッカー
C. ゼロバウンス
D. シャーロックにメールを送信
正解: **A (**コメントを発表する**)**
According to the CHFI v11 objectives under Email Forensics and Digital Evidence Examination , investigators must be capable of extracting, converting, and analyzing email data stored in proprietary or corrupt formats. Microsoft Outlook commonly stores mailbox data in OST (Offline Storage Table) files, which can become inaccessible or corrupt during incidents such as system crashes, insider attacks, or malware infections.
Kernel for OST to PST is a specialized forensic and eDiscovery tool designed to recover and convert OST files into accessible formats such as PST, EML, MSG, and MBOX . Its

ability to export emails into EML format is particularly important in forensic investigations, as EML is widely supported by multiple forensic tools and email analysis platforms. CHFI v11 highlights the importance of using reliable tools that support selective extraction, filtering, and migration , allowing investigators to isolate relevant emails, attachments, headers, and metadata while maintaining evidence integrity.
Additionally, Kernel for OST to PST supports migration to various email servers and web-based platforms
, aligning with CHFI requirements for handling enterprise email evidence across heterogeneous environments.
The other options are unsuitable: Email Checker and ZeroBounce are email validation tools, and EmailSherlock focuses on email address investigation rather than mailbox data extraction.
Therefore, consistent with CHFI v11 best practices for email evidence acquisition and conversion , Kernel for OST to PST is the correct and exam-aligned answer

質問**: 103**
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、次のうちどのツールを使用すべきか？
A. Wireshark
B. カッコウの砂場
C. IDA Pro
D. プロセスモニター
正解**: (**正解を表示します**)**
Option B. Cuckoo Sandbox is the best answer because CHFI v11 explicitly includes Malware Analysis:
Static and Dynamic , the Prominence of Setting up a Controlled Malware Analysis Lab , Preparing Testbed for Malware Analysis , and Tools to Perform Static and Dynamic Malware Analysis . The question specifically asks for behavioral analysis in a secure and controlled environment , which is the hallmark of sandbox-based dynamic malware analysis.
A polymorphic worm that changes structure rapidly is difficult to analyze with signature-based approaches alone, so observing its behavior in a sandbox is the most effective next step. Cuckoo Sandbox is designed for this type of controlled execution and can reveal process activity, file changes, registry modifications, network communications, and persistence behavior without exposing the production environment. Wireshark only captures network traffic. IDA Pro is a reverse engineering tool for code analysis. Process

Monitor is useful for local system monitoring but does not provide the same isolated malware-analysis lab capability.
Therefore, under CHFI malware-forensics objectives, Cuckoo Sandbox is the strongest answer for secure behavioral analysis of the worm.

質問: **104**
大手テクノロジー企業のサイバーセキュリティアナリストが、社内ネットワーク内で不審なファイルを発見した。マルウェアの可能性を懸念したアナリストは、そのファイルがもたらす潜在的な脅威を評価するため、静的解析と動的解析の両方を実施することにした。上記のシナリオにおいて、疑わしいファイルに対して静的解析を実施する主な目的は何でしょうか？
A. ファイルを実行せずにコードを解析し、潜在的なセキュリティ上の脅威を特定します。
B. 制御された環境でファイルを実行して、その動作を観察します。
C. 動的実行を通じてファイルの動作に関する初期情報を収集します。
D. ファイルの機能を理解するために、コードを手動でリバースエンジニアリングします。
正解: **(正解を表示します)**
Option A is the best answer because CHFI v11 explicitly includes Malware Analysis: Static and Dynamic and the use of a controlled malware analysis lab to examine suspicious files safely. The defining purpose of static analysis is to inspect a file without executing it , allowing the investigator to identify indicators such as strings, imports, headers, embedded resources, suspicious metadata, obfuscation, or other structural signs of malicious intent. This is different from dynamic analysis , which involves running the file in a sandbox or controlled environment to observe behavior. Option B and C therefore describe dynamic analysis, not static analysis.
Option D may be part of deeper reverse engineering, but it is narrower and more advanced than the broader primary purpose of static analysis, which is safe, non-executing inspection to identify likely threats.
Because the question asks for the main reason to perform static analysis, the most accurate CHFI-aligned answer is analyzing the suspicious file's code and structure without running it in order to identify potential security threats.

質問: **105**
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.
Other options listed are not objectives of computer forensics as defined by CHFI. Weather analysis, market forecasting, and physical security assessments fall outside the scope of digital forensic investigations. CHFI v11 explicitly identifies data recovery and reconstruction of erased digital footprints as essential for establishing accountability and ensuring evidence admissibility in legal proceedings.
Therefore, to effectively identify and prosecute perpetrators who attempted to erase evidence, investigators must focus on recovering deleted files and hidden data , making Option D the correct and CHFI-verified answer.

質問: **106**
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スマートフォンであり、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。彼女は、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する必要がある。エマが端末から最も広範なデータにアクセスできる取得方法はどれだろうか？
A. クラウドデータ取得
B. ファイルシステムの取得
C. 論理取得
D. 物理的取得
正解: (正解を表示します)
Option D. Physical acquisition is the best answer because the question asks for the method that provides the most extensive access to Android device data, including existing data, deleted data, and system-level files .

CHFI v11 explicitly covers Data Acquisition Methods , Mobile Phone Evidence Analysis , Android and iOS Forensic Analysis , and both Logical Acquisition of Android and iOS Devices and Physical Acquisition of Android and iOS Devices .
A physical acquisition captures the raw contents of device storage at a lower level than logical or file-system- only approaches. Because of that, it offers the best chance of recovering deleted artifacts and examining system areas that are not normally exposed through higher-level acquisition methods. This makes it the most comprehensive choice when the goal is to maximize evidentiary coverage.
Logical acquisition is more limited and generally focuses on accessible user data. File system acquisition can be broader than logical collection, but it still does not usually provide the same depth as a full physical image. Cloud acquisition may complement the investigation, but it does not replace direct device acquisition.
Therefore, under CHFI mobile-forensics objectives, physical acquisition is the strongest answer.

質問: **107**
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.
Option B (IPACCESSLOGRL) refers to rate-limited ACL logging, not standard packet logging. Option A is specific to IPv6 ACL logging and does not apply unless IPv6 traffic is explicitly involved. Option D (TOOMANY) relates to excessive event conditions and is not tied to ACL packet matching.
The CHFI v11 Exam Blueprint highlights analyzing Cisco router and firewall logs , including ACL-based messages, as a key skill for detecting network attacks and reconstructing intrusion timelines. Therefore, % SEC-6-IPACCESSLOGP is the correct and exam-aligned answer

質問**: 108**
データ侵害が発生すると、機密情報にアクセスした従業員が疑われます。内部脅威ツールが導入され、従業員のデジタル活動を精査し、異常な行動があればフラグを立てることで、調査と将来の侵害の防止に役立ちます。
特定のシナリオにおいて、内部脅威ツールはサイバーセキュリティにどのように貢献しますか?
A. 組織内の不審な行動を監視し、検出することにより
B. 競合他社の戦略を分析することで
C. 市場動向を予測することで
D. ソーシャルメディアの存在感を高めることで
正解**: A (**コメントを発表する**)**
According to the CHFI v11 Network and Web Attacks and Insider Threat Forensics objectives, insider threats represent a significant risk because trusted users already have legitimate access to systems, data, and networks. As a result, detecting malicious activity by insiders requires continuous monitoring and behavioral analysis , rather than traditional perimeter-based security controls.
Insider threat tools are specifically designed to monitor user activities , such as file access, data transfers, login behavior, privilege escalation, email usage, USB activity, and abnormal network connections. CHFI v11 emphasizes that these tools establish a baseline of normal user behavior and then identify deviations that may indicate data exfiltration, sabotage, fraud, or policy violations. Alerts generated by these tools help investigators quickly identify suspicious actions and correlate them with timelines and access rights.
The other options are unrelated to the purpose of insider threat tools. Analyzing competitor strategies and predicting market trends fall under business intelligence, not cybersecurity.

Enhancing social media presence is a marketing function and has no relevance to forensic investigations or breach prevention.
CHFI v11 highlights insider threat monitoring as a critical component of post-breach investigations and proactive defense , enabling organizations to both investigate incidents and reduce the risk of recurrence.
Therefore, in this scenario, insider threat tools contribute to cybersecurity by monitoring and detecting suspicious behavior within the organization , making Option A the correct and CHFI v11-verified answer.

質問**: 109**
人気オンライン小売店で最近発生したセキュリティインシデントを受け、インシデント対応チームが調査を行っています。調査の結果、攻撃者がわずか数分で、異なるクレジットカード情報の組み合わせを用いて数千件の購入試行を行ったことが判明しました。また、これらの取引はすべて同一のIPアドレスから行われたことも明らかになりました。コンピュータハッキングのフォレンジック調査員として、あなたはどのような種類の攻撃に遭遇する可能性が最も高いとお考えですか？
A. クッキー中毒攻撃。
B. ブルートフォース攻撃。
C. パラメータ改ざん攻撃。
D. XML外部エンティティ(XXE)攻撃。
正解**: (**正解を表示します**)**
Option B. Brute Force attack is the most appropriate answer because the scenario describes an attacker making thousands of rapid attempts using many different combinations of payment data from the same IP address. CHFI v11 includes Investigating Brute Force Attack as part of its network and web attack coverage.
The defining characteristic of a brute-force style attack is repeated automated trial-and-error attempts until valid data is found. In this case, the attacker is not relying on stolen session state, changing parameters in a single trusted request, or abusing XML parsing. Instead, the attacker is systematically testing combinations at scale, which is consistent with brute-force or card-testing behavior.
Cookie poisoning would focus on modifying session or cookie values. Parameter tampering involves altering request parameters to manipulate application logic. XXE targets XML parsers. None of those fit the described pattern as directly as repeated automated attempts from one source using numerous combinations.
Therefore, under CHFI's attack-investigation objectives, the strongest answer is Brute Force attack .

質問**: 110**
サイバー犯罪捜査において、捜査官はNTFSファイルシステムを調査し、ファイルアクティビティの証拠を探しています。捜査官はThe Sleuth Kitのfls およびmactimeツールを使用し

て、ファイル操作に関連するタイムスタンプを抽出 分析しています。これらのタイムスタンプは、インシデント発生前後の一連の出来事に関する重要な情報を提供します。捜査官はタイムラインを再構築するために、どのようなファイル情報に注目しているのでしょうか？
A. 調査員は、ファイルの作成時刻、最終アクセス時刻、およびファイルの変更時刻に焦点を当てます。
B. 調査員は、ファイル システムの内部構造、時間関連のメタデータ、およびファイル ストレージのブロック割り当ての詳細を分析します。
C. 調査員はシステムの起動時間とシャットダウンのタイムスタンプをチェックして、システムの動作期間を把握します。
D. 調査員は、Windows イベント ログのタイムスタンプを調べて、記録されたファイル アクセスまたは変更時刻を確認します。
正解**: A (**コメントを発表する**)**
Within the CHFI v11 syllabus under Operating System Forensics and Image/Evidence Examination and Event Correlation , timeline reconstruction is a core forensic technique used to understand what happened, when it happened, and in what order . When analyzing NTFS file systems, investigators rely heavily on MAC times - Modified, Accessed, and Created timestamps-to establish file activity.
The Sleuth Kit tools fls and mactime are specifically designed for this purpose. The fls tool extracts file and directory metadata from a forensic image, while mactime processes this metadata to generate a chronological timeline of file system events. This timeline typically includes file creation time, last modification time, and last access time , allowing investigators to correlate file activity with known incident times, user actions, or attacker behavior.
Option B describes low-level file system analysis, which is useful in other contexts but is not the primary focus of mactime . Option C relates to system-level operational timelines rather than file activity. Option D focuses on Windows event logs, which are valuable for corroboration but are separate from NTFS file system timestamp analysis.
The CHFI v11 Exam Blueprint explicitly highlights file system timeline creation and analysis using The Sleuth Kit , emphasizing MAC timestamps as the foundational data used to reconstruct sequences of events during digital investigations

質問**: 111**
企業のデータ漏洩に関する調査において、フォレンジック調査員は容疑者のハードドライブから削除されたファイルを復旧する任務を負います。調査員は、ハードドライブが改変されておらず、信頼できる状態であることを慎重に確認し、デバイスのフォレンジックイメージを作成し、将来の分析のために整合性を保つために安全な場所に保管します。このステップは、調査プロセス中に元のデータが改ざんされていないことを保証するために非常に重要です。
このシナリオでは、法医学調査官のどのような責任が果たされているのでしょうか?

A. 証拠の適切な取り扱いと保存を確保する。
B. 調査中に法執行機関や関係者と連携します。
C. 裁判所向けの構造化されたレポートを作成します。
D. 破損したストレージ デバイスを再構築して、隠された情報を回復します。
正解: **A** (コメントを発表する)
According to the CHFI v11 Computer Forensics Fundamentals module, one of the core responsibilities of a forensic investigator is to ensure the proper handling, preservation, and integrity of digital evidence .
This responsibility is foundational to the entire forensic process and directly impacts the admissibility of evidence in court .
In the given scenario, the investigator creates a forensic image of the suspect's hard drive rather than working directly on the original media. CHFI v11 explicitly states that investigators must always perform analysis on a bit-by-bit forensic copy while preserving the original evidence in a secure, controlled environment. This practice prevents accidental modification, contamination, or destruction of original data and ensures compliance with the best evidence rule and chain of custody requirements .
The act of securely storing the original drive and working only on the forensic image demonstrates strict adherence to evidence preservation principles. While recovering deleted files is an investigative goal, the scenario emphasizes maintaining integrity and preventing alteration , which aligns directly with evidence handling and preservation-not reporting, stakeholder engagement, or device reconstruction.
CHFI v11 consistently reinforces that failure to preserve evidence properly can lead to legal challenges, evidence exclusion, or case dismissal , regardless of the quality of the technical analysis performed.
Therefore, the responsibility being fulfilled in this scenario-fully aligned with CHFI v11-is ensuring appropriate handling and preservation of evidence , making Option A the correct answer.

質問: **112**
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: **A** (コメントを発表する)

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.
Focusing only on native mobile files (Options B and C) risks overlooking critical evidence that may demonstrate lateral movement, data exfiltration, or coordination between devices.
Ignoring Windows- or Linux-related artifacts (Option D) directly contradicts forensic best practices and may lead to incomplete or flawed conclusions.
The CHFI Exam Blueprint v4 explicitly highlights Android and iOS forensic analysis , cross-platform evidence correlation , and file system analysis as key competencies. Therefore, analyzing cross-OS artifacts is essential for uncovering hidden relationships, validating investigative hypotheses, and ensuring legally defensible findings, making Option A the correct and exam-aligned answer

質問**: 113**
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. 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。
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. 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。
正解**: D (**コメントを発表する**)**
Option D is the strongest answer because the scenario specifically emphasizes the large volume of messages

, the presence of obscured language and coded references , and the effort required to extract useful intelligence from noisy communications. The central problem is not primarily legal authority or identity attribution, but the sheer processing and analytical burden involved in reviewing extensive dark web communications that are intentionally obfuscated. From a CHFI perspective, dark web investigations often involve huge datasets, deceptive terminology, indirect references, slang, and deliberate evasion techniques. This creates a major forensic challenge because investigators must separate meaningful evidence from distractions, false leads, and coded language. The need for structured filtering, prioritization, and advanced analysis tools is a hallmark of such cases.
Option B overlaps slightly, but it is narrower than the broader issue described. The problem is not just distinguishing genuine from deceptive messages; it is managing and analyzing a massive communication corpus with obfuscated content. Option C may arise later during attribution, and A is not the main focus of the question. Therefore, the best answer is the challenge of processing extensive chat room communications containing obfuscated content .

質問**: 114**
フォレンジック調査員のパテル氏は、サイバー攻撃に関連するネットワークトラフィックを分析しています。トラフィックはTorネットワークを経由していたため、悪意のある活動の発信元を追跡することは困難でした。調査中、パテル氏は特定のリレーを経由してTorネットワークから発信される不審なトラフィックを特定しました。調査において、悪意のあるトラフィックの発信元ではないとしても、宛先サーバーへの可視性が高いため、法的調査や苦情の対象となる可能性が高いTorリレーの種類はどれでしょうか？
A. 出口リレー
B. エントリーリレー
C. 転送リレー
D. 中間リレー
正解**: (**正解を表示します**)**
According to the CHFI v11 Dark Web and Tor Browser Forensics objectives, the Tor network anonymizes user traffic by routing it through a series of relays: Entry (Guard) Relay # Middle Relay # Exit Relay .
Each relay plays a distinct role in preserving anonymity, but only one relay is directly visible to the destination server.
The Exit Relay is the final node in the Tor circuit and is responsible for forwarding decrypted traffic from the Tor network to the target destination on the regular internet. As a result, destination servers see the IP address of the exit relay , not the original attacker. This makes exit relays highly visible and frequently misattributed as the source of malicious activity such as hacking attempts, scanning, spam, or data exfiltration.
CHFI v11 explicitly notes that exit relays commonly face legal complaints, abuse reports, and law enforcement scrutiny , even though they do not originate the traffic. Investigators

must understand this distinction to avoid false attribution during dark web investigations. Entry relays only see the client IP but not the destination, and middle relays see neither source nor destination. "Transfer relay" is not a valid Tor relay type.
From a forensic and legal perspective, recognizing the role of exit relays is critical when analyzing Tor- related incidents, as they represent the point of exposure to external networks.
Therefore, the Tor relay most likely to face legal scrutiny due to its visibility to destination servers-fully aligned with CHFI v11-is the Exit Relay , making Option A the correct answer.

質問**: 115**
警察官が国境検問所の犯罪現場に到着しました。そこでは、金融詐欺事件の容疑者が逮捕されていました。逮捕手続き中、警察官は容疑者の所持品の中にノートパソコンを発見しました。ノートパソコンには、肉眼で確認できる犯罪の明確な証拠が含まれていました。警察官は令状を持っていませんが、改ざんの可能性を防ぐため、直ちに機器を押収する必要があります。このような状況で警察官が取るべき適切な措置は何でしょうか？
A. 警官は、ラップトップを捜索する前に、両国の国境問題を扱う最高責任者から令状を直ちに取得する必要があります。
B. 警察官は令状なしでラップトップを捜索することができます。
C. 警察官は、ラップトップがロックされていてアクセスできない場合にのみ、令状なしでラップトップを捜索できます。
D. 警官は証拠の写真を撮影し、ノートパソコンを捜索するための令状が取得されるまで待たなければなりません。
正解**: (**正解を表示します**)**
Under CHFI v11 Computer Forensics Fundamentals , investigators must understand the legal principles governing search and seizure of digital evidence , especially in exceptional environments such as national border crossings . Two key legal doctrines apply directly to this scenario: the Border Search Exception and the Plain View Doctrine .
The Border Search Exception allows law enforcement officers to conduct searches at international borders without a warrant or probable cause to protect national security and prevent cross-border crime. CHFI v11 highlights border environments as special jurisdictions where warrant requirements are relaxed due to the government's heightened authority to regulate entry and exit of persons and goods.
Additionally, the Plain View Doctrine permits officers to seize and examine evidence immediately visible during a lawful arrest, provided the officer is legally present and the incriminating nature of the evidence is obvious. In this case, the laptop is in the suspect's immediate possession, and evidence of the crime is visible without manipulation.
CHFI v11 emphasizes that delaying action in such situations could result in evidence destruction, encryption, or remote wiping , especially with digital devices. Therefore, securing and searching the laptop immediately is justified and legally defensible.

The other options are incorrect because they impose unnecessary delays or conditions not required under border search authority. Therefore, fully aligned with CHFI v11 principles, the correct action is that the officer may search the laptop without a warrant , making Option B the correct answer.

質問: **116**
鑑識捜査において、捜査官は容疑者のWindowsマシンを分析しており、最近開いたファイルに関する情報を提供する可能性のあるWindowsショートカットファイル(LNKファイル)を探す必要があります。捜査官はこれらのLNKファイルを見つけるために、どのディレクトリを調べるべきでしょうか？
A. C:\Users\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite
B. C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache
C. C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent
D. C:\Users\Admin\AppData\Local\Microsoft\Windows\History
正解: **C** (コメントを発表する)
Option C is correct because CHFI v11 explicitly includes Analyze LNK Files and Jump Lists and also lists Tools to Examine Windows Files, Metadata, ShellBags, LNK files, and Jump Lists as important Windows artifact-analysis objectives. LNK files are commonly associated with user activity and recently accessed items, making the Recent folder the most relevant location among the options.
The path C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent is the standard user-specific location associated with many recently accessed shortcut artifacts. This makes it a valuable source when reconstructing user behavior, identifying recently opened files, or linking a suspect to specific documents and file paths.
The other options are not the right artifact location for LNK files. Firefox cookies.sqlite is browser-related, WebCache is tied to cached browsing data, and the History location is not the best answer for Windows shortcut evidence. Therefore, from a CHFI perspective on Windows artifact analysis, the examiner should focus on the Recent folder to locate LNK files.

質問: **117**
熟練したハッカーであるオリバーは、競合他社に雇われ、企業の幹部であるサラから機密情報を収集する任務を負った。標的は、機密性の高いビジネス取引や個人の財務データを含むサラのメールアカウントだった。オリバーはパスワードを解読することで、サラのメールアカウントへの不正アクセスを試みた。彼は、サラが使用していると思われる単純な組み合わせを含む、よく使われるパスワードの大規模なリストを含むテキストファイルを入手した。このリストを使用して、彼はログインページに対して各組み合わせを系統的にテストし、最終的にサラのアカウントにログインして彼女の個人情報にアクセスすることに成功した。上記のシナリオでオリバーが用いた手法は次のうちどれか？
A. キーロガー攻撃

B. 辞書攻撃
C. 総当たり攻撃
D. 暗号解読攻撃
正解: **(**正解を表示します**)**
Option B. Dictionary attack is the best answer because the attacker used a precompiled list of common passwords and tested them against the login page. That is the defining pattern of a dictionary attack: trying likely password candidates from a prepared wordlist rather than exhaustively attempting every possible combination. CHFI v11 includes password-related attack and analysis concepts within its investigation scope, and this scenario matches the classic distinction between dictionary and brute-force methods.
A brute-force attack would attempt all possible character combinations systematically, which is broader and usually more time-consuming than using a list of common passwords. A keylogger would capture keystrokes from the victim's device, which is not what happened here. Cryptanalytic attack refers to attacking cryptographic mechanisms, not simply testing common passwords against a login page.
From a CHFI perspective, understanding the difference between password-guessing methods is important because it helps investigators interpret authentication logs and attacker behavior. Since Oliver relied on a text file of frequently used passwords and tested them one by one, the technique most accurately described is a dictionary attack .

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**)**
According to the CHFI v11 objectives under Analyzing Various File Types and Image File Analysis (BMP)
, understanding bitmap (BMP) file structure is critical for identifying hidden data, detecting tampering, and validating file integrity during forensic investigations. A BMP file is composed of multiple structured components, each serving a specific purpose.
The Information Header (also known as the DIB header) is the component that contains detailed metadata about the bitmap image. This includes essential attributes such as image width and height, color depth (bits per pixel), compression method, image size,

resolution, and pixel layout . These attributes define how the image data should be interpreted and rendered, making the information header central to forensic analysis. Investigators rely on this header to verify whether image properties are consistent with expectations or have been manipulated.
The File Header (Option A) primarily identifies the file as a BMP and provides the offset to the image data, but it does not describe the image layout in detail. Image data (Option B) contains the actual pixel values, while the RGBQUAD array (Option D) defines the color palette for indexed images and does not describe file structure.
The CHFI Exam Blueprint v4 explicitly covers BMP file analysis and hex-level examination , highlighting the Information Header as the key structure for understanding bitmap characteristics, making Option C the correct and exam-aligned answer

質問**: 119**
フォレンジック調査員が、EDRMフレームワークに従って組織内でeDiscoveryプロセスを実行しています。調査員は、不要なデータを削除し、分析や調査が容易な管理しやすい形式に変換することで、電子的に保存された情報(ESI)の量を絞り込むことに重点を置いています。調査員は、eDiscoveryの次の段階に向けてデータが適切に準備されていることを確認しています。上記のシナリオで、調査員はEDRMのどの段階を実行しているのでしょうか？
A. 調査員は、データの意義を解釈するための分析段階を実施しています。
B. 調査員は、法的利用のためにデータを最終化するための生産段階を実行しています。
C. 調査担当者は、データを評価するためのレビュー段階を実施しています。
D. 調査員は、データの処理を容易にするために、処理段階を担当しています。
正解**: D (**コメントを発表する**)**
Option D is correct because the scenario describes the stage where electronically stored information is being filtered, reduced, transformed, and prepared into a form that is easier to review. In the EDRM model, that is the processing phase. CHFI v11 includes eDiscovery , electronically stored information , and handling large volumes of digital evidence in a legally defensible way. Within that framework, processing is the stage that reduces irrelevant or redundant material and converts data into a manageable form for later examination.
This is different from review , where the investigator or legal team examines the processed data for relevance, responsiveness, privilege, or evidentiary value. It is also different from production , which involves delivering the selected materials in the required legal or procedural format. Analysis is a broader interpretive activity focused on meaning, context, and conclusions.
Because the question specifically states that the investigator is narrowing the data volume , eliminating unnecessary data , and converting it into a manageable format for the next phase , the task clearly matches the processing stage of the EDRM workflow. That makes option D the most accurate and CHFI- aligned answer.

質問: **120**
サイバーセキュリティ企業が、金融機関におけるデータ侵害の疑いについてフォレンジック調査を実施しています。調査中、フォレンジックアナリストは強力なパスワードで保護された暗号化ファイルに遭遇し、侵害に関連する重要な証拠にアクセスできなくなりました。
デジタルフォレンジック調査におけるパスワード保護の課題を考慮すると、このシナリオではフォレンジック分析プロセスを妨げるためにどのようなアンチフォレンジック手法が採用されているのでしょうか。
A. データ操作
B. データの難読化
C. データ暗号化
D. データの隠蔽
正解: **(**正解を表示します**)**
This scenario aligns with CHFI v11 objectives under Anti-Forensics Techniques , specifically techniques used by attackers to prevent investigators from accessing digital evidence. Data encryption is a well-known and widely used anti-forensic method where files are encrypted using strong cryptographic algorithms and protected with complex passwords. While encryption is a legitimate security control, adversaries often misuse it to deliberately obstruct forensic analysis and delay investigations.
CHFI v11 explains that encrypted files render data unreadable without the correct decryption key, making it extremely difficult for investigators to examine file contents within acceptable timeframes. This can significantly hinder evidence discovery, timeline reconstruction, and incident scoping. Investigators must then rely on password cracking, key recovery, memory forensics, or legal assistance to access the data-each of which introduces complexity, cost, and time delays.
Data manipulation involves altering or deleting evidence, data obfuscation focuses on making data confusing but still accessible, and data hiding conceals information in alternate locations. In contrast, the defining characteristic in this scenario is password-protected encrypted files , which directly corresponds to data encryption. Therefore, consistent with CHFI v11 classifications, data encryption is the correct anti-forensic technique being employed.

質問: **121**
ネットワーク管理者のミアは、ネットワークのパフォーマンスが低下していることに気づき、Ciscoルーターのログを確認していました。ログを確認しているうちに、 必要なIPヘッダーオプションをすべて格納できる十分なスペースがなかったため、システムはパケットを処理できませんでした。」というメッセージに遭遇しました。ミアは、Cisco IOSログのどのニーモニックがこの問題に該当するかを特定する必要があります。
このメッセージを見つけるために、ミアは次のどの logニーモニックを探す必要がありますか?

A. %SEC-4-多すぎる
B. %IPV6-6-ACCESSLOGP
C. %SEC-6-IPACCESSLOGP
D. %SEC-6-IPACCESSLOGRL
正解: **A (**コメントを発表する**)**
According to the CHFI v11 Network Forensics and Log Analysis objectives, Cisco IOS log messages use standardized mnemonics to describe specific security and packet-processing conditions. The message indicating that "there was not enough room for all of the desired IP header options" is associated with abnormal or excessive IP header options , which can be indicative of malformed packets, reconnaissance activity, or denial-of-service (DoS) attempts .
The mnemonic %SEC-4-TOOMANY is generated when a router receives packets containing too many IP options for the available buffer space. Cisco devices impose limits on IP header options to protect system resources, and when these limits are exceeded, the packet is dropped and logged with this mnemonic. CHFI v11 highlights such logs as important artifacts when investigating network performance degradation, packet manipulation, and potential attack traffic .
The other options are unrelated to this condition. %IPV6-6-ACCESSLOGP applies to IPv6 access control logging. %SEC-6-IPACCESSLOGP and %SEC-6-IPACCESSLOGRL relate to access-list permit/deny logging and rate-limited ACL messages, not IP header option exhaustion.
From a forensic perspective, identifying %SEC-4-TOOMANY helps investigators correlate performance issues with malformed or malicious traffic patterns and supports attribution during network attack investigations.
Therefore, the correct Cisco IOS log mnemonic corresponding to this issue-fully aligned with CHFI v11-is
%SEC-4-TOOMANY (Option A) .

質問: **122**
組織のAWS環境における不審なアクティビティに関するフォレンジック調査において、調査担当者はAmazon CloudWatchを使用して特定のログデータセットの保存期間を調整します。このアクションは、ログの保存期間を管理し、調査中の更なる分析のために重要なロ

グを確実に保存するために不可欠です。このシナリオにおいて、調査担当者はAmazon CloudWatchのどの機能を使用していますか？
A. ログ データを通じてシステムとアプリケーションを分析および監視します。
B. CloudWatch Logs Insights を使用してログデータを効率的に検索および分析します。
C. 個々のログ グループの保持ポリシーを変更します。
D. さらなる調査とトラブルシューティングのために、特定の API アクティビティの通知アラートを設定します。
正解: **(**正解を表示します**)**
Under the CHFI v11 objectives related to Cloud Forensics and AWS Forensics , log preservation is a critical requirement for effective investigation and legal admissibility. In Amazon Web Services, CloudWatch Logs retention policies allow investigators to control how long log data is stored before it is automatically deleted.
Modifying retention policies for individual log groups ensures that relevant forensic artifacts-such as authentication logs, API activity records, and system events-remain available for analysis throughout the investigation lifecycle.
In this scenario, the investigator's goal is not to analyze or query logs immediately, but to extend or manage the lifespan of log data so that it is not lost due to default retention limits. This aligns precisely with the feature that allows investigators to modify retention policies for individual log groups . CHFI v11 highlights the importance of preserving cloud-based evidence early, as cloud logs may be ephemeral and subject to automatic deletion if not properly configured.
Option A refers to general monitoring capabilities, while Option B focuses on querying and searching log data using Logs Insights-both are analytical functions, not retention management. Option D involves alerting mechanisms and does not control log storage duration.
The CHFI Exam Blueprint v4 explicitly includes logs in AWS and cloud evidence acquisition , emphasizing retention configuration as a key forensic readiness and investigation task, making Option C the correct and exam-aligned answer

質問: **123**
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.
While options A and C restrict log output to specific time ranges and option B follows logs in real time, the question specifically asks which command should be executed to view the SSH key fingerprint in the SSH unit logs . CHFI v11 best practices recommend starting with the base unit log query to ensure no relevant artifacts are missed before applying filters.
Therefore, to reliably extract SSH key fingerprints and correlate authentication activity during forensic analysis, Hazel should execute journalctl -u ssh , making Option D the correct and CHFI v11-verified answer.

質問**: 124**
法医学専門家のソフィアは、マルウェアの痕跡がないかシステムを分析している。彼女は、マルウェアがWindowsのサービスや実行中のプロセスを改変し、検出されずにバックグラウンドで動作するようにしていることに気づく。彼女は、システムの起動時に自動的に開始されるサービスを特定する必要がある。
ソフィアは、自動起動するように設定されているWindowsサービスを調べるために、どのツールを使用すべきでしょうか？
A. イベントビューアー
B. タスクマネージャー
C. 自動実行
D. プロセスエクスプローラ
正解**: (**正解を表示します**)**
Option C. Autoruns is the best answer because the question is specifically about identifying services and other components configured to start automatically during boot . In CHFI-style Windows forensics and malware persistence analysis, investigators focus on auto-start mechanisms , including services, registry run keys, startup folders, drivers, scheduled tasks, and related launch points. Autoruns is designed to enumerate these persistence locations in a comprehensive way, making it the most appropriate tool among the options.

Event Viewer is useful for examining logs and system events, but it is not the primary tool for enumerating all boot-start and auto-start entries. Task Manager can show currently running processes and some startup items, but it is less complete than Autoruns for deep persistence analysis. Process Explorer is excellent for analyzing active processes and parent-child relationships, yet it is not focused on full startup enumeration.
Because Sophia wants to identify which Windows services are configured to start automatically , the most effective forensic tool is Autoruns , which directly supports malware persistence investigation and startup analysis.

質問**: 125**
あなたは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、「infected_doc」という不審なMicrosoft Officeドキュメントの分析を任されています。このドキュメントは、大企業の複数の従業員に送信されたメールの添付ファイルで発見されました。このドキュメントには、特にVBAマクロに関連するマルウェアが埋め込まれている可能性があるという懸念が高まっています。
「infected_doc」という Microsoft Office ドキュメントを調査するフォレンジック調査員として、ファイル内の疑わしいコンポーネントや悪意のあるコンポーネントを特定するために、どのような最初の手順を実行しますか?
A. Linux ワークステーションでコマンド oleid "" を実行して、すべてのコンポーネントで疑わしい要素を確認します。
B. サンドボックス環境でドキュメントを開き、異常な動作がないか観察します。
C. コマンド analyze_doc "" を実行して、ドキュメントをスキャンし、潜在的な脅威を探します。
D. ブラウザベースのツールを使用して、ドキュメントのメタデータに異常がないか検査します。
正解**: (**正解を表示します**)**
This question aligns with CHFI v11 objectives under Malware Forensics and Static Malware Analysis of Suspicious Documents . When analyzing potentially malicious Microsoft Office documents, CHFI v11 emphasizes that investigators should always begin with static analysis before attempting any form of execution. This approach minimizes risk and helps identify embedded threats such as VBA macros, OLE objects, exploits, and obfuscation techniques without activating the payload.
The oleid tool (part of the oletools suite) is specifically designed for the initial inspection of OLE-based Microsoft Office documents . It quickly identifies indicators of compromise such as the presence of macros, embedded objects, suspicious file formats, encryption, and known exploit characteristics. CHFI v11 highlights oleid as a safe, non-intrusive first step to triage Office documents and determine whether deeper analysis (e.g., macro extraction or sandbox execution) is warranted.
Opening the document in a sandbox is a dynamic analysis step and should only occur after static indicators confirm malicious intent. The other options are either non-standard or

insufficient for detecting embedded macro-based malware. Therefore, consistent with CHFI v11 malware forensics methodology, executing oleid to review suspicious components is the correct initial step.

質問: **126**
サイバーセキュリティアナリストであるあなたは、最近、組織ネットワーク内の複数のエンドポイントから発信されるネットワークトラフィックの異常な増加を検出しました。さらに調査を進めた結果、複数の従業員が、一見無害に見える添付ファイルを含むフィッシングメールを受信していたことが判明しました。しかし、これらの添付ファイルは、悪名高いマルウェア配布手法であるGootLoaderキャンペーンの一部である疑いがあります。
添付ファイルに関して、どのような結論が導き出せるだろうか？
A. 添付ファイルは、GootLoader キャンペーンの第一段階のペイロードとして機能している可能性があります。
B. 添付ファイルは、ゼロデイ脆弱性を悪用してネットワークへの不正アクセスを取得している可能性があります。
C. 添付ファイルには、組織から機密情報を盗むように設計されたスパイウェアが含まれている可能性があります。
D. 添付ファイルには、機密データを暗号化するランサムウェアが含まれている可能性があります。
正解: **A** (コメントを発表する)
Option A is the best answer because the question explicitly identifies the attachments as being associated with a GootLoader campaign , which is commonly understood as a malware delivery mechanism that uses deceptive content to stage later malicious activity. In this context, the attachment is most logically interpreted as a first-stage payload or infection vector rather than the final malware objective itself.
From a CHFI-style malware forensics perspective, investigators first determine how malicious code was delivered , then analyze what subsequent payloads or behaviors followed. In phishing-driven infection chains, the initial attachment often acts as the first phase that enables download, execution, or delivery of additional malware. That fits the fact pattern far better than assuming the attachment itself must specifically be spyware, ransomware, or a zero-day exploit.
Options B , C , and D may describe possible later effects in some campaigns, but the most defensible conclusion from the wording is that these attachments are part of the initial delivery stage of GootLoader.
Therefore, the correct answer is that the attachments are likely serving as the first-stage payload in the campaign and should be analyzed as the initial malicious component in the infection chain.

質問: **127**

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** (コメントを発表する)
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: **128**
侵害を受けたシステムのフォレンジック調査において、調査員は様々なフォレンジック アーティファクトを分析し、攻撃の性質と範囲を特定します。調査員は特に、失敗したサインイン試行、セキュリティポリシーの変更、侵入検知システムからのアラート、異常なアプリケーションの誤動作に関する情報を探します。
この重要な情報が含まれている可能性が高い法医学的証拠品の種類はどれですか?
A. 暗号化および復号化操作に関する情報を保存する暗号化アーティファクト。
B. ユーザーの閲覧履歴と Web サイトの操作を追跡するブラウザー アーティファクト。
C. 実行中のプロセスとシステム メモリに関する情報を含むプロセスおよびメモリ アーティファクト。
D. デバイス上のイベントとエラーの詳細な記録を提供するログ ファイルの異常。
正解: **D** (コメントを発表する)

This question aligns directly with CHFI v11 objectives under Computer Forensics Fundamentals and Log Analysis . Log files are among the most critical forensic artifacts because they provide a chronological and authoritative record of system, security, and application events . CHFI v11 emphasizes that logs are essential for reconstructing attack timelines, identifying unauthorized access attempts, and determining the scope of a compromise.
Artifacts such as failed sign-in attempts , security policy modifications , IDS alerts , and application errors are routinely recorded in log sources including Windows Security logs, system logs, application logs, firewall logs, and IDS/IPS logs. These logs allow investigators to correlate events across systems, identify brute-force attacks, detect privilege escalation, and recognize abnormal behavior caused by malware or misconfiguration.
Cryptographic artifacts focus on key usage and encryption operations, browser artifacts relate to user web activity, and process or memory artifacts provide insight into live execution states-but none provide the comprehensive, event-based historical visibility required to answer all aspects of the question. CHFI v11 highlights log analysis as the primary method for understanding what happened, when it happened, how it happened, and who was involved . Therefore, log file anomalies are the most relevant and reliable forensic artifacts in this scenario.

質問: **129**
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を受けた。
事件後、組織は外部のフォレンジック調査員を雇うことを決定しました。しかし、取締役会は外部調査員の選定基準について意見が対立しています。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. 会社の内部システムに関する知識。
B. 法医学における専門職倫理規定の遵守。
C. 類似のケースを扱った経験。
D. 業界における評判。
正解: **(**正解を表示します**)**
Option C is the strongest answer because, in a major breach involving sensitive customer data and a large attack scope, the most important practical hiring factor is whether the external investigator has experience handling similar incidents . CHFI v11 emphasizes the roles and responsibilities of forensic investigators , what makes a good computer forensics investigator , and the importance of choosing personnel with the right skills and investigative capability for the case at hand.
Adherence to ethics is important, and reputation can matter, but the question asks for a key factor in the context of a high-stakes breach investigation. Experience with similar

cases directly affects the investigator's ability to preserve evidence, scope the breach, handle legal sensitivity, manage cross-system analysis, and produce defensible findings efficiently. That makes it more operationally decisive than general reputation or internal-system familiarity.
Therefore, from a CHFI standpoint, the board should prioritize an external investigator with proven experience in dealing with similar cyber breach and forensic cases , as that is most likely to produce reliable, court-defensible, and technically sound results.

質問: **130**
侵害されたWindowsシステムに関するサイバー犯罪捜査の後、捜査官はプライベートブラウジングの痕跡を復元する任務を負います。捜査官はページファイルからデータを取得することを決定しました。
sys やその他のライブ メモリ キャプチャを使用して、プライベート ブラウジング モードからのアクティビティの痕跡を識別します。
ライブ システムを分析し、これらのプライベート ブラウジングのアーティファクトを回復するには、調査員はどのツールを使用する必要がありますか?
A. PsLoggedOn
B. 実行情報
C. FTKイメージャー
D. ズステグ
正解: **(**正解を表示します**)**
This question aligns with CHFI v11 objectives under Operating System Forensics and Volatile and Non-Volatile Data Analysis, particularly the recovery of artifacts from live memory and system files such as pagefile.sys. Private browsing modes (e.g., InPrivate, Incognito) are designed to minimize persistent artifacts on disk; however, CHFI v11 emphasizes that memory, page files, and swap files often retain remnants of browsing activity, including URLs, session data, cached content, and credentials.
FTK Imager is a forensically sound tool widely used for live data acquisition, memory capture, and analysis of volatile artifacts. It allows investigators to acquire RAM, pagefile.sys, hiberfil.sys, and other critical system files without altering evidence integrity. CHFI v11 specifically highlights FTK Imager as a preferred tool for collecting and examining live system data and recovering artifacts that are not available through traditional disk-only analysis.
PsLoggedOn is used to identify logged-in users, Exeinfo analyzes executable file formats, and zsteg is a steganography detection tool. None of these are suitable for live memory or pagefile analysis. Therefore, consistent with CHFI v11 forensic best practices, FTK Imager is the correct tool to recover private browsing artifacts from live Windows systems.

質問: **131**

あなたはコンピュータハッキングのフォレンジック調査官として、大手銀行における金融記録の不正改ざん事件を担当しています。ネットワーク管理者は、改ざんの発生源と思われる特定の端末を特定しました。あなたは、このワークステーションを調査するよう命じられました。
管理者から、さらなる改変を恐れてマシンの電源を切ったとの連絡がありました。このような状況で、最初にとるべき行動は次のうちどれでしょうか？
A. マシンを起動し、ライブ分析を実行して、不正な変更に関与した可能性のある実行中のプロセスを特定します。
B. マシンを別のネットワークに接続し、ネットワークパケットアナライザーを使用して進行中のトラフィックを監視します。
C. システムの電源をオフにしたまま、オフラインでの詳細な分析のためにフォレンジックイメージングプロセスを開始します。
D. ハードドライブの起動可能なコピーを作成し、別の安全なマシンで分析します。
正解: **(**正解を表示します**)**
Option C is the correct answer because the workstation has already been powered down , so the priority is now to preserve the remaining non-volatile evidence and acquire it in a forensically sound manner. Powering the system back on could alter timestamps, logs, temporary files, registry artifacts, and other evidence. CHFI emphasizes choosing the correct acquisition method based on the state of the device and preserving integrity during evidence collection.
Since volatile data is already lost due to shutdown, the correct first step is not to boot the machine, but to begin forensic imaging for later offline analysis. This allows the investigator to create an exact duplicate of the storage media and conduct the examination on the copy rather than the original source.
Option A would unnecessarily modify the system state. B is irrelevant because a powered-down workstation has no ongoing traffic to monitor. D is weaker because creating a bootable copy is not the immediate forensic priority; the first requirement is a proper evidence image. Therefore, the best CHFI-aligned response is to leave the system off and initiate forensic imaging for offline analysis.

質問: **132**
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.
The other options are incorrect. Public Tor relay nodes are typically the first targets of censorship and are already blocked. Direct communication with an exit node is not possible because Tor circuits must always begin with an entry point. Collaborating with government authorities contradicts the goal of bypassing surveillance and is not a technical solution discussed in CHFI v11.
CHFI v11 emphasizes that investigators and analysts must understand Tor infrastructure, including bridges, to properly investigate dark web activity and censorship circumvention techniques. Therefore, the correct and CHFI-aligned method is to use bridge nodes to access the Tor network , making Option A the correct answer.

質問: **133**
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.
CHFI v11 emphasizes correlating the hexadecimal values with their ASCII representations to accurately interpret raw data and identify meaningful forensic artifacts. Therefore, the area that displays the ASCII representation of each byte is the Character area , making Option D the correct and CHFI v11-verified answer.

質問**: 134**
組織内で最近発生したセキュリティインシデントに関するフォレンジック調査において、調査員は証拠に対するあらゆる行動を記録し、適切な証拠管理の連鎖を確保するという任務を負っています。調査員は証拠に対するあらゆる行動をログブックに注意深く記録します。証拠には、混乱を防ぐため固有の識別子が付与されます。また、調査全体を通して証拠の移動と取り扱いを追跡するために、詳細な証拠管理の連鎖記録も作成されます。このシナリオにおいて、調査員はどの調査ステップを実行しているのでしょうか？
A. 捜査官は事件現場から収集した証拠を保存しています。
B. 調査員は、セキュリティ インシデントが発生した場所の調査を行っています。
C. 調査員は、侵害に関連する可能性のある発見のために証拠に関するデータ分析を行っています。
D. 捜査官は、セキュリティインシデントに関連する証拠の捜索と押収を行っています。
正解**: (**正解を表示します**)**
According to the CHFI v11 Procedures and Methodology domain, evidence preservation is a critical step in the forensic investigation process and is closely tied to maintaining a proper chain of custody .
Preservation ensures that digital evidence remains unaltered, authentic, and legally admissible from the moment it is collected until it is presented in court or a disciplinary proceeding.
In the given scenario, the investigator is documenting every action , assigning unique identifiers , and maintaining a chain of custody log that records who handled the evidence, when it was handled, and for what purpose. CHFI v11 explicitly defines these actions as part of the evidence preservation phase , which occurs immediately after evidence identification and collection. This phase is designed to prevent evidence tampering, loss, contamination, or misidentification.

The other options do not align with the described activities. Scoping focuses on defining investigation boundaries, data analysis involves examining evidence for findings, and search and seizure refers to the legal act of collecting evidence-none of which emphasize documentation and custody tracking.
CHFI v11 stresses that failure to properly preserve evidence and document its handling can result in evidence being challenged or ruled inadmissible . Therefore, the investigator's actions clearly correspond to preserving the evidence , making Option A the correct and CHFI v11-verified answer.

質問**: 135**
金融機関のコンプライアンス担当者であるジェームズは、規制要件を満たしていることを確認するため、会社のデータ保護ポリシーを精査する任務を負っている。同社は、ローン、投資アドバイス、保険など、幅広い金融商品とサービスを提供している。ジェームズは精査の中で、同社が顧客にデータ共有に関する明確な情報を提供し、機密データを保護するための措置を実施していることに気づいた。彼は、金融機関に対し情報共有の実態を説明し、機密データを保護することを義務付ける1999年制定の法律を同社が遵守していると確信している。
ジェームズは、以下のどの法律の遵守を確保しようとしているのか？
A. GDPR
B. HIPAA
C. PCI DSS
D. GLBA
正解**: (**正解を表示します**)**
Option D. GLBA is the correct answer. The Gramm-Leach-Bliley Act (GLBA) is the U.S. law enacted in
1999 that requires financial institutions to explain their information-sharing practices and protect sensitive customer data through safeguards. That description matches the scenario exactly. Within CHFI v11, legal awareness is a core competency: the blueprint includes legal issues, privacy issues and legal compliance , other laws that may influence computer forensics , and rules tied to the admissibility and handling of digital evidence.
The other options do not fit the facts. GDPR is a European data protection regulation, not a 1999 U.S.
financial law. HIPAA governs protected health information in the healthcare sector. PCI DSS is an industry security standard for payment card data, not a law enacted in 1999 requiring disclosure of information-sharing practices. Because the company is a financial institution and the question highlights both privacy notice and safeguarding customer information , GLBA is the only answer that fully matches the scenario.
From a CHFI perspective, recognizing applicable legal frameworks is important because investigators and compliance personnel must understand which laws govern digital evidence, privacy obligations, and organizational handling of sensitive information.