EC-COUNCIL.312-49v11-JPN.v2026-08-15.q189

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：	189
バージョン：	v2026-08-15
ページの閲覧量：	102
問題集の閲覧量：	1958

https://www.jpnshiken.com/shiken/EC-COUNCIL.312-49v11-JPN.v2026-08-15.q189.html

質問: **1**
あなたは多国籍企業で発生したデータ漏洩の疑いに関するフォレンジック調査を行っています。調査中に、世界各地の複数のシステムで、一見無関係に見える複数のインシデントが発生していることが判明しました。これらのインシデントを理解し、潜在的な関連性を確立するために、どのようなアプローチを採用すべきでしょうか？
A. 各事件ごとに個別の調査を実施する
B. 調査全体を最初からやり直す
C. 最も深刻なインシデントの詳細な分析を実施する
D. イベント相関を利用して、事件間の関連性を見つける
正解: **(**正解を表示します**)**
Option D is the best answer because CHFI v11 explicitly includes Types of Event Correlation , Event Correlation Approaches , and the use of correlated evidence to reconstruct activity across systems. When multiple incidents appear disconnected across different hosts, regions, or time periods, event correlation is the forensic method used to identify shared patterns, related indicators, timing relationships, and common sources.
In a multinational data-exfiltration case, investigators need to determine whether the incidents are truly separate or part of one coordinated campaign. Correlation helps combine logs, timestamps, network events, authentication records, and other artifacts into a unified picture. This is far more effective than treating each event in isolation or focusing only on the most severe case.
Option A risks missing the broader connection. B is unnecessary and inefficient. C may help with one host, but it does not establish relationships across the larger environment.
Therefore, from a CHFI perspective, the correct investigative approach is to use event correlation to link the incidents and build a coherent view of the suspected exfiltration activity.

質問: **2**

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: **(**正解を表示します**)**

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: **3**

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

ムディレクトリを調べる必要があります。システム上で実行されたアプリケーションの痕跡を見つけるために、イーサンは次のどのディレクトリを調べるべきでしょうか？
A. プロセスダンプツール
B. プリフェッチ
C. Rp.log
D. Change.log.x
正解: **B** (コメントを発表する)
Option B. Prefetch is the correct answer because CHFI v11 explicitly identifies Prefetch Files as an important Windows artifact source. The blueprint includes Extracting Additional Windows OS Artifacts and specifically mentions Identifying TOR Browser Artifacts: Command Prompt, Windows Registry, and Prefetch Files , showing that Prefetch is a recognized source for evidence of program execution.
In Windows investigations, Prefetch artifacts help examiners determine whether an application was executed on the system, and they can support timeline analysis by showing execution-related traces. That makes Prefetch especially valuable when the goal is to identify whether suspicious or malicious software ran on the machine.
The other options are not the standard Windows artifact location used for this purpose. Process Dumper refers more to tooling than a system directory. Rp.log and Change.log.x are not the well-known Windows execution-trace artifact being tested here. Therefore, under CHFI operating-system forensic objectives, the most appropriate place to examine for traces of executed applications is the Prefetch area.

質問: **4**
コロラド州デンバーで行われた詐欺捜査中に、2つの断片が発見されました。1つは「D0 CF 11 E0 A1 B1 1A E1」で始まり、もう1つは「%PDF」で始まります。最初の断片を16進数で表示すると、WordDocumentという名前のストリームであることが判明しました。「D0 CF 11 E0 A1 B1 1A E1」という署名に最も関連している可能性が高いファイルの種類は何ですか？
A. Microsoft Excel ワークブック xls
B. ポータブルドキュメントフォーマット PDF
C. モダンオフィス XML ドキュメント docx
D. Microsoft Word 文書 doc
正解: **D** (コメントを発表する)
The correct answer is D because the signature D0 CF 11 E0 A1 B1 1A E1 identifies the older Microsoft Compound File Binary Format, which can contain several legacy Office file types. The clue that resolves the exact file type here is the presence of a stream named WordDocument, which is characteristic of the legacy binary Microsoft Word document structure. By contrast, a PDF would begin with the text signature %PDF, and a modern .docx file uses the ZIP-based Office Open XML format rather than the older compound binary format. CHFI v11 includes analysis of Word, PDF, and other file formats

through hex views, so this question fits directly into that objective. The exam logic is to combine the magic number with the internal stream name rather than relying on the container header alone. Since the fragment is a compound binary file and specifically exposes a WordDocument stream, the most likely associated file type is a Microsoft Word .doc file.

質問: **5**
経験豊富な鑑識捜査官が、国際的な麻薬密売組織に関わる事件を担当することになった。事件の主犯格は、ダークウェブを使ってネットワークと連絡を取っているとされている。捜査官は容疑者のコンピュータを分析中に、「LC. CTYPE=en_US.UTF-8」という文字列を発見した。捜査官がこの文字列に遭遇する可能性が最も高いのは、どのような証拠物だろうか？
A. TORコマンドプロンプトの履歴
B. TOR Windows レジストリ キー
C. TORプリフェッチファイル
D. マルウェアバイナリ
正解: **C** (コメントを発表する)
Option C. TOR Prefetch file is the strongest answer. CHFI v11 explicitly includes Identifying TOR Browser Artifacts: Command Prompt, Windows Registry, and Prefetch Files as part of dark web forensics. That means the exam expects investigators to recognize where Tor-related execution traces can appear on a Windows system.
The string LC_CTYPE=en_US.UTF-8 is associated with locale or environment information and is more likely to appear among the execution-related traces and referenced strings tied to program startup artifacts than in a simple command-history record or a registry key. Prefetch files are especially valuable because they provide evidence that an executable ran on the system and may include file and execution context information useful to artifact-based analysis. That makes them a more plausible location for this kind of string in a Tor-related investigation.
Command Prompt history would more commonly show typed commands, not this type of runtime locale detail. Registry keys may show installation or configuration traces but are less likely to contain this exact environment-style string as the key artifact being tested. Therefore, within CHFI's Tor artifact framework, TOR Prefetch file is the best answer.

質問: **6**
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**: 7**
企業不正調査において、アナリストは、ユーザーが複数の最新ブラウザのプライベートブラウジング機能を利用してウェブ活動を隠蔽しようとしたワークステーションを調査した。ブラウザレベルの痕跡は限られているように見えるが、調査員は、ユーザーが入力したクエリやブラウジングの断片がアクティブなセッションのライフサイクルを超えて残存し

ていたことを示す痕跡を発見した。調査員は、複数のブラウザにわたるこの種の痕跡を最も確実に復元できるのは、どのアーティファクトからだろうか？
A. クッキー
B. pagefile.sys
C. DNSキャッシュ
D. 一時データベースファイル
正解: **(**正解を表示します**)**
The correct answer is B because pagefile.sys is one of the most useful cross-browser residual evidence sources when private browsing is used. Research on private browsing repeatedly shows that, even when standard browser artifacts are minimized, remnants of queries, visited content, and browsing fragments can still persist in operating system artifacts such as paging data and memory-related storage. Studies of private mode forensics found that evidence may remain in RAM and disk artifacts even when browser traces are reduced, and this is especially valuable because pagefile.sys is not tied to one specific browser implementation. CHFI v11 includes browser artifact recovery and private browsing analysis under operating system and file artifact examination, so candidates are expected to think beyond obvious browser stores.
Cookies and temporary databases are more browser-dependent and may be cleared or limited by private mode. DNS cache can reveal domain resolution history, but it usually does not preserve the richer search- query and browsing-fragment evidence described in the scenario. Therefore, pagefile.sys is the strongest and most reliable source among the listed options.

質問: **8**
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: **D (**コメントを発表する**)**
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**: 9**
ナッシュビルの医療機関のサンドボックス環境で動的マルウェア解析を行ったところ、サンプルにはネットワークアクティビティがすぐには見られませんでした。制御された再起動後、実行ファイルはユーザーの操作なしにログオン時に自動的に起動しました。再起動サイクル全体にわたってこの動作を引き起こすシステム変更を把握するために、調査担当者はシステムアクティビティのどの領域を監視すべきでしょうか？
A. 監視プロセス
B. レジストリアーティファクトの監視
C. 監視サービスとスタートアッププログラム
D. イベントログの監視
正解**: (**正解を表示します**)**
The correct answer is C because the behavior described is reboot-persistent auto-start execution, which most directly points to services and startup programs. CHFI v11 explicitly includes malware persistence mechanisms and system behavior analysis through monitoring services, startup programs, registry artifacts, and related operating system changes. When malware launches automatically after restart and logon, investigators should focus first on the execution mechanisms that survive reboot and trigger program start without manual action. Services and startup entries are classic persistence locations for this kind of behavior.
Registry artifacts can also be involved, especially through Run keys, but the question asks what area of system activity should be monitored to capture the reboot-linked execution behavior itself. That makes services and startup programs the best fit because they directly govern automatic launch at system boot or user logon. In dynamic malware analysis, tracing these persistence points across a restart cycle helps investigators understand how the malware reappears, whether it is service-based, startup-folder based, or tied to another auto-launch mechanism.

質問: **10**
ユタ州ソルトレイクシティにある製造会社で発生した内部犯行によるデータ漏洩事件の調査中、捜査官はキャプチャしたパケットファイルをNetworkMinerに読み込み、オフライン分析を行いました。トラフィックには様々なアプリケーション層プロトコルが含まれており、チームはファイル再構築やホストプロファイリングに進む前に、トラフィックから解析されたユーザー名とパスワードをまとめて表示する必要があります。どのタブを開くべきでしょうか？
A. ファイル
B. 認証情報
C. ホスト
D. セッション
正解: **B** (コメントを発表する)
The correct answer is B because the Credentials tab in NetworkMiner is specifically used to display usernames, passwords, and other credential material extracted from packet captures. NetworkMiner documentation and walkthroughs describe the tool as capable of parsing PCAP data to extract higher-layer artifacts, including files, emails, certificates, and credentials. Since the investigators want a consolidated view of usernames and passwords before moving on to other analysis tasks, the Credentials tab is the most direct place to look. Files would be used for reconstructed transferred objects, Hosts for endpoint and traffic summaries, and Sessions for conversation-level details, but none of those is the dedicated credential view.
CHFI v11 includes network forensics and packet analysis, so candidates are expected to know not only which tools are useful, but also which specific interfaces within those tools support a given investigative objective.
When the aim is quick triage of possible usernames and passwords observed in network traffic, the proper NetworkMiner tab is Credentials.

質問: **11**
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: **A** (コメントを発表する)

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**: 12**
デジタルフォレンジックアナリストのザカリーは、古いワークステーションが関わるサイバースパイ事件の捜査に取り組んでいる。そのワークステーションはIDE(Integrated Drive Electronics)方式のハードディスクドライブを使用していたが、電力サージによって故障し、読み取り不能な状態になっていた。
ザカリーは、そのドライブに捜査に役立つ重要な証拠が含まれていると確信している。しかし、事件でワークステーションのマザーボードも損傷しており、ザカリーが利用できるシステムはすべて最新型でSATAコネクタしか搭載していない。そのため、IDEドライブをこれらのシステムに直接接続することができない。
この状況で、ザカリーはIDEハードドライブからデータを取得するために何をすべきでしょうか？
A. ザカリーは、SATA-IDE変換アダプタを使用して、IDEハードドライブを最新のシステムに接続する必要があります。
B. ザカリーはIDEドライブを専門のデータ復旧サービスに送るべきです。
C. ザカリーはIDEドライブからプラッタを取り出し、正常に動作するSATAドライブに挿入するべきです。
D. ザカリーは損傷したワークステーションのマザーボードを修理するべきです
正解**: (**正解を表示します**)**
Option A is the best answer because CHFI v11 specifically covers disk interfaces , understanding hard disks and SSDs , sources of potential evidence , and the methodology for choosing the best data acquisition method before evidence collection begins. When the issue is simply that the examiner's current systems have SATA connectors while the

evidence drive is IDE , the most practical and forensically sound response is to use an appropriate adapter so the examiner can access the drive using modern hardware.
This approach aligns with CHFI's acquisition principles because it supports controlled evidence access while preserving the drive for imaging and analysis. Sending the drive to a specialized recovery service may be necessary only if the drive itself is physically damaged beyond ordinary access, but the question's main obstacle is the interface mismatch. Extracting platters and placing them into another drive is highly inappropriate and risks destroying evidence. Repairing the old motherboard is also unnecessary and less efficient when an interface adapter can solve the connection problem safely.
Therefore, based on CHFI data acquisition concepts and disk-interface awareness, the correct first choice is to use a SATA-to-IDE adapter .

質問**: 13**
法医学鑑定士のマイケルは、容疑者のマシンから入手したイメージファイルの法医学的分析を行っています。16進エディタを使用してファイルを調べているうちに、ファイルの16進数値が 89 50 4c」というシーケンスで始まっていることが分かりました。このファイルは疑わしいと思われるため、マイケルはファイルの構造を理解し、悪意のあるコンテンツが含まれているかどうかを判断するために、ファイルの種類を特定する必要があります。この情報に基づいて、マイケルが調べているファイルの種類は何でしょうか？
A. BMP
B. JPEG
C. PDF
D. PNC
正解**: D (**コメントを発表する**)**
Option D is the intended answer. The question appears to contain a typo: "PNC" is almost certainly meant to be PNG . CHFI v11 explicitly includes Understanding Hex Editors and Hexadecimal Notation , Image File Analysis: JPEG and BMP , and Hex View of Popular Image File Formats , which means candidates are expected to recognize file types from signature bytes in hex view.
The well-known PNG file signature begins with the bytes 89 50 4E 47 . The sequence shown in the question,
"89 50 4c" , looks incomplete or slightly mistyped, but it is clearly intended to point toward the PNG signature pattern rather than BMP, JPEG, or PDF. BMP files begin differently, JPEG files usually start with FF D8 FF , and PDF files begin with 25 50 44 46 corresponding to %PDF.
Because CHFI expects forensic investigators to identify file types through hexadecimal file-header analysis , the only reasonable answer from the choices is the typoed D , representing PNG . Therefore, Michael is looking at what the exam item intends to be a PNG image file .

質問: **14**
テクノロジー企業のサイバーセキュリティアナリストであるアレックスは、同社のCEOにメールで送られてきた不審なWord文書を傍受しました。予備調査では文書に問題はないように見えましたが、同社が最近サイバー攻撃の脅威にさらされていることを考慮し、アレックスはさらに調査することにしました。彼は、文書に隠れたマルウェアがないかを確認するために、静的解析を実行できるツールを必要としています。以下の選択肢の中から、アレックスのニーズに最も適したツールはどれでしょうか？
A. FireEyeのFLOSS
B. PEStudio
C. キャスティング
D. カッコウの砂場
正解: **C** (コメントを発表する)
Option C. Olevba is the best answer because CHFI v11 explicitly includes Analyzing Suspicious Word, Excel, and PDF Documents and Tools to Analyze Suspicious Word and PDF Documents as part of malware forensics and static/dynamic analysis.
The suspicious file here is a Word document , and the question asks for a tool suitable for static analysis to detect hidden malicious content. Olevba is specifically known for analyzing Office documents and extracting or inspecting VBA macro content , suspicious strings, and obfuscation indicators without executing the document. That fits the requirement exactly.
FLOSS is mainly used for extracting obfuscated strings from binaries. PEStudio is more appropriate for PE files such as Windows executables and DLLs. Cuckoo Sandbox is a dynamic analysis environment, not the most direct tool for static Office document inspection. Therefore, within CHFI's malware-document analysis scope, the most effective choice is Olevba for static analysis of the suspicious Word file.

質問: **15**
大手金融機関がランサムウェア攻撃を受け、重要なデータが暗号化され、業務が中断し、法的措置のために証拠収集が急務となった。組織の事前策定されたポリシーにより、デジタル証拠の迅速な特定、外部専門家との連携、そしてバックアップ復元プロセスと証拠収集を統合することでダウンタイムを最小限に抑えることが可能になった。この準備により、フォレンジック活動が業務復旧をさらに妨げることなく、証拠の完全性を維持しながらサービスを再開できるようになった。このシナリオで示されている、調査ニーズと業務のバランスを取る上で重要な概念とは何か？
A. トレーニングと意識向上
B. データバックアップとデータの整合性
C. インシデント対応統合
D. テストと訓練
正解: (正解を表示します)

The correct answer is C because the scenario highlights the integration of forensic activity into the organization's broader incident response and business recovery process. CHFI v11 specifically includes forensic readiness and business continuity, computer forensics as part of the incident response plan, overview of incident response process flow, and forensic readiness planning and procedures. Those blueprint areas are all reflected here. The organization is not merely restoring backups or training staff; it has already designed a process in which evidence collection, external coordination, and restoration can happen together without undermining recovery. That is the essence of incident response integration in a forensic context. Data backups are part of the story, but the core concept is the coordinated incorporation of evidence handling into operational response. Training and drills support readiness, but they are not the primary concept demonstrated in the active scenario. In CHFI-style reasoning, when forensic collection is deliberately embedded within response and continuity actions so the business can recover while preserving evidence, the best answer is incident response integration.

質問: **16**
ある企業が、進行中の調査に関連するデータを収集、処理、提出するために、大規模なeディスカバリープロセスを実施しています。法務チームとITチームは、データの完全性と正確性を確保するために、これらの段階の進捗状況を監視する任務を負っています。また、プロセス全体を通して関連コストを効果的に管理する必要もあります。eディスカバリープロセスの複雑さと規模を考慮すると、適切な追跡は不可欠です。これらの目標を達成するために、企業はどの側面を優先すべきでしょうか？
A. 主要業績評価指標 (KPI) を定義し、eDiscovery プロセスの各段階における情報量を測定します。
B. 収集した電子証拠へのアクセスと管理を効率化するために、中央集権型データリポジトリを導入する。
C. eDiscoveryプロセス中に法務部門とIT部門間の調整を監督するクロスファンクショナルチームを設立する。
D. eDiscoveryプロセスに関わるスタッフ向けの包括的なトレーニングプログラムを開発する。
正解: **(**正解を表示します**)**
Option A is the best answer because CHFI v11 explicitly states that organizations should monitor and maintain accurate metrics and detailed tracking information related to eDiscovery . The question also emphasizes progress monitoring , data integrity and accuracy , and cost control , all of which are best supported by clearly defined metrics and stage-by-stage measurement.
By defining KPIs and measuring the volume of information at each stage , the company can track bottlenecks, evaluate collection and processing scope, manage costs, and ensure that the eDiscovery lifecycle remains defensible and organized. This is directly

aligned with the CHFI blueprint's eDiscovery objectives, which treat measurement and tracking as core best practices rather than optional administrative tasks.
The other options can still add value, but they do not address the question as directly. A centralized repository, cross-functional oversight, and training all help operations, yet the CHFI-aligned priority for monitoring effectiveness and controlling cost is accurate metrics and detailed tracking information .
Therefore, the strongest answer is to define KPIs and measure information volume throughout the eDiscovery process.

質問: **17**
マイアミのテクノロジー企業で行われたマルウェア調査において、フォレンジックアナリストは、攻撃者が侵害されたワークステーション上で以前に実行されたプログラムの痕跡を削除することで、活動を隠蔽しようとした疑いがあるとみている。
捜査官が処刑行為や過去のプログラムの痕跡を消そうとする試みを再現する上で、最も有効な証拠源は何か？
A. Openfilesコマンドの出力
B. クリップボードの内容
C. ハッシュ値
D. ファイルのプリフェッチ
正解: **(**正解を表示します**)**
The best answer is D because Prefetch files are one of the most useful Windows artifacts for reconstructing which programs were executed, when they were run, and how often they were launched. Magnet Forensics notes that Prefetch files provide insight into applications that have been run on a system and include valuable execution-history data. That makes them especially important when investigators suspect an attacker tried to remove other traces of program activity. Even if binaries are later deleted, Prefetch artifacts may still help establish that execution occurred. CHFI v11 includes analysis of Windows files and execution-related artifacts, and Prefetch is a classic source used to support malware execution timelines. Openfiles output is transient and not a historical artifact, clipboard contents are unrelated to prior program execution history, and hash values only verify file identity or integrity if the file is available. Since the question asks for the source that best

reconstructs prior execution activity and supports analysis of trace-removal attempts, Prefetch files are the strongest forensic artifact among the listed options.

質問**: 18**
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**: 19**
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**: A (**コメントを発表する**)**
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**: 20**
経験豊富なデジタルフォレンジック調査員であるエミリーは、ext2ファイルシステムを実行しているLinuxシステムの調査を依頼されました。このシステムはデータ漏洩の疑いのある事件に関与しており、エミリーは攻撃中にアクセスまたは変更された可能性のある特定のファイルのメタデータに関する詳細な情報を収集する必要があります。システムのファイルシステム構造を確認した後、エミリーはタイムスタンプ、パーミッション、ファイルサイズなどのファイルのメタデータを含むソースに焦点を当てることを目指しています。この重要な情報を得るための最適なソースは次のうちどれでしょうか？
A. ファイルのデータブロック
B. dentry キャッシュ
C. スーパーブロック

D. inodeテーブル
正解: **(**正解を表示します**)**
Option D. The inode table is the correct answer because, in Linux file systems such as ext2, file metadata including timestamps, permissions, ownership, and file size is stored in the file's inode , not in the file's content blocks. CHFI v11 explicitly includes Windows, Linux, and macOS File Systems , Linux File System Analysis Tools , and File System Analysis using The Sleuth Kit (TSK) , showing that exam candidates are expected to understand file-system structures and where key forensic metadata resides.
The data blocks contain file content, while the superblock stores overall file-system-level information such as layout and status. The dentry cache is a kernel memory structure related to name lookups and is not the primary persistent source for file metadata in this context. For detailed per-file forensic metadata, the examiner must look at the inode information.
Therefore, when Emily wants the most critical metadata about a specific ext2 file, the best source is the inode table , because that is where the file's core descriptive attributes are maintained.

質問: **21**
法医学専門家のウィリアムは、被害者のマシンから取得したメモリダンプからTorブラウザに関連するアーティファクトを抽出することで、システム侵害の調査を担当しました。調査の一環として、ウィリアムはメモリダンプを分析し、Torブラウザに関連するアーティファクトが可能な限り最大数含まれていることを発見しました。ウィリアムは、証拠の範囲を完全に理解するには、メモリダンプにアーティファクトが最大数含まれる条件を特定する必要があることを理解しました。次の条件のうち、ウィリアムが可能な限り最大数のアーティファクトを取得できたのはどれですか？
A. Torブラウザが開きました
B. Torブラウザがアンインストールされました
C. Torブラウザがインストールされています
D. Torブラウザが閉じられました
正解: **A (**コメントを発表する**)**
Option A. Tor browser opened is the best answer because a memory dump captures the live contents of RAM, and the richest set of Tor-related evidence will exist when the Tor Browser is actively running .
CHFI v11 explicitly includes Dark Web Forensics , TOR Browser artifacts , and analysis of memory and system artifacts to identify user activity and applications in use.
When Tor is open, memory may contain process data, loaded modules, active connections, recently rendered pages, configuration details, session-related artifacts, and fragments of user activity that may not be fully preserved elsewhere. If Tor is merely installed , the examiner may only find static installation artifacts. If it is closed , many live-

session artifacts may already be gone from memory. If it is uninstalled , evidence may be even more limited.
Because the question asks which condition results in the maximum possible number of artifacts in a memory dump , the answer is clearly the state in which the application is actively executing. Therefore, under CHFI dark web and memory-forensics principles, the correct answer is Tor browser opened .

質問: **22**
シアトルの活気ある医療機関でランサムウェア攻撃が発生し、法医学捜査官のテイラー・ブルックスが現場に到着すると、患者の記録が暗号化され、テラバイト規模のデータにチームが圧倒されているのを発見する。刻一刻と時間が迫り、人命がかかっている中、彼女はAIを活用して膨大なデータ量を迅速に精査し、異常なパターンを特定し、手動による調査では見逃してしまうような悪意のある痕跡を分離することで、復号化と犯人特定のための重要な手がかりを絞り込む。テイラーは、このデータ洪水を実用的な洞察へと変換するために、どのようなAI技術を活用しているのだろうか？
A. 知識表現
B. 自動データ分析
C. 推論プロセス
D. 知識発見
正解: **(**正解を表示します**)**
The correct answer is B because the scenario describes AI being used to rapidly process very large amounts of evidence, detect anomalies, and highlight suspicious patterns that investigators can act on immediately. That is the essence of automated data analysis. CHFI v11 explicitly includes integration of artificial intelligence with digital forensics, and the exam often frames AI in operational terms rather than theoretical ones. Here, the emphasis is on speed, scale, and the automated identification of relevant traces across massive datasets.
Knowledge representation is more about structuring information so systems can reason over it. Reasoning process refers to inference and decision logic. Knowledge discovery is related, but it usually points more toward extracting broader hidden relationships or insights from data rather than the immediate automated triage and pattern flagging described in the incident response context. In a ransomware event with overwhelming evidence volume, the most directly applicable AI capability is automated data analysis because it reduces manual effort, prioritizes suspicious artifacts, and helps investigators convert raw evidence into a manageable set of forensic leads. That makes B the best CHFI-aligned answer.

質問: **23**
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: **A** (コメントを発表する)
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: **24**
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**: 25**
カリフォルニア州サンノゼの金融会社で行われたデジタルフォレンジック調査において、アナリストは容疑者のハードディスクの最初の512バイトセクターが悪意のあるインストーラによって上書きされていることを発見した。ハードウェアチェックが完了した後、システムはオペレーティングシステムを見つけることも、アクティブパーティション上のスタートアッププログラムに制御を移すこともできない。このセクターで見つかった構造に基づいて、どのコンポーネントの破損が障害の原因である可能性が最も高いか？
A. パーティションテーブル
B. ブート署名 0x55AA
C. ブートローダー
D. マスターブートコード
正解**: D (**コメントを発表する**)**
The correct answer is D because the Master Boot Code in the first sector of an MBR disk is the executable code that runs after BIOS hands off control. Its job is to examine the partition table, identify the active partition, and transfer execution to that partition's boot sector. If that code is corrupted, the system can no longer locate and hand off to the startup program on the active partition, which matches the failure described in the question. The partition table is also present in the same sector and is important, but the wording specifically focuses on failure to transfer control after hardware checks, which is the role of the executable boot code. The boot signature 0x55AA only indicates that the sector is bootable in format terms; it does not perform the control transfer. CHFI v11 includes Windows boot process and logical disk structures, so candidates are expected to understand what each MBR component does. Since the startup failure is tied to the executable handoff function within the first sector, the most likely corrupted component is the Master Boot Code.

質問: **26**
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: **27**
シアトルのデザイン会社で発生したデータ漏洩事件において、捜査官は、Mac、アプリ、サーバー、ウェブサイトのユーザーアカウント名とパスワードを安全に保存し、クレジットカード番号や銀行の暗証番号などの機密情報も格納できるmacOSの暗号化コンテナを必要としています。捜査官は、どのMacフォレンジックデータソースを調査すべきでしょうか？
A. Apple Mail

B. タイムマシン
C. プロパティリストまたはplistファイル
D. キーホルダー
正解: **(**正解を表示します**)**
The correct answer is D because Keychain is the macOS secure storage mechanism used to hold sensitive credentials and other protected secrets. Apple states that Keychain stores website usernames and passwords, and related secure information such as credit card details, while Keychain Access on Mac allows viewing keys, certificates, and other stored items. That matches the scenario exactly. CHFI v11 includes macOS forensic data, log files, and directories, so candidates are expected to know where valuable user authentication material and confidential account data are stored. Apple Mail contains email artifacts, Time Machine contains backup history, and plist files store many configuration details, but none of those is the primary encrypted credential container described in the question. From a forensic perspective, Keychain can be highly significant in data-theft, access-abuse, and credential-misuse investigations because it may reveal stored account relationships and secrets relevant to attacker activity or user actions. When the exam asks for the macOS source that securely holds account names, passwords, and other confidential values, the answer is Keychain.

質問: **28**
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: **(**正解を表示します**)**
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**: 29**
法医学鑑定士のジョンは、容疑機器から取得した証拠画像ファイルの分析を任されました。捜査を進める中で、彼は疑わしいと思われるファイルを発見しました。
彼は16進エディタでファイルを開き、「89 50 4E」で始まるファイルの16進値を発見しました。彼の分析によると、この16進値はどのファイルタイプに対応しているのでしょうか？
A. PDF
B. JPEG
C. BMP
D. PNG
正解**: D (**コメントを発表する**)**
This question aligns with CHFI v11 objectives under Operating System Forensics and File Type and Encoding Analysis . In digital forensics, file signature analysis-also known as magic number analysis -is a critical technique used to identify the true file type regardless of its extension. Attackers often rename or disguise files to evade detection, making hex-level inspection essential during forensic examinations.
Each file format begins with a unique hexadecimal header that identifies its structure. The hex value "89 50
4E 47" corresponds to the ASCII representation of ‰PNG , which is the standard file signature for Portable Network Graphics (PNG) files. CHFI v11 specifically emphasizes the use of hex editors to analyze file headers and detect file extension mismatches during investigations.
The other options have different signatures: PDF files start with 25 50 44 46 (%PDF) , JPEG files typically begin with FF D8 FF , and BMP files start with 42 4D (BM) . Since the observed hex value matches the PNG signature, the correct identification is PNG. This technique is vital for uncovering hidden or obfuscated evidence and ensuring accurate file classification in forensic investigations.

質問**: 30**

ネットワークフォレンジック調査官のデビッドは、セキュリティチームから潜在的なセキュリティインシデントの報告を受け、ファイアウォールのログを調べている。同社は最近、特に外部ソースからの異常なトラフィックパターンを経験しており、IT部門は標的型攻撃が行われているのではないかと懸念している。ファイアウォールのログを調べているうちに、デビッドは見慣れないIPアドレスからの着信接続試行が複数拒否されていることに気づいた。これらの試行は、想定されるネットワーク範囲外から発信されているようだ。接続試行はファイアウォールによって一貫して拒否されているが、異常な時間に発生しているため、懸念が生じている。
警戒態勢が強化されている状況下で、デイビッドはこれらの不審な接続試行が、より広範な侵入攻撃の一部なのか、それとも単なる無害なスキャン活動なのかを判断しなければなりません。ログの詳細を調べる際、彼は状況の深刻度を評価するためにいくつかの要素を考慮します。ファイアウォールログの詳細の中で、これらの拒否された試行が潜在的な侵入攻撃の一部であるかどうかをデイビッドが判断する上で、最も重要な情報を提供するものはどれでしょうか？
A. ソースポート番号
B. 宛先IPアドレス
C. 接続試行時刻
D. ファイアウォールアクションが実行されました
正解: **(**正解を表示します**)**
Option C. Time of the Connection Attempt is the strongest answer because CHFI v11 emphasizes analyzing firewall logs , types of event correlation , timeline and kill chain analysis , and understanding how multiple events fit together during an incident investigation.
In this scenario, the firewall has already denied the connections, so Firewall Action Taken adds little new value. The Destination IP Address may show which internal asset was targeted, and the Source Port Number is usually less useful for judging intent. What most helps determine whether the activity is part of a broader intrusion attempt is the timing of the events: whether they align with other suspicious logs, occur in repeated patterns, coincide with activity on targeted hosts, or match known scanning or attack windows. Time data is essential for correlating firewall entries with IDS alerts, authentication failures, endpoint events, or other signs of coordinated activity.
Because CHFI teaches investigators to build timelines and correlate events across evidence sources, the time of the connection attempt provides the most critical context for distinguishing random scanning from a potentially coordinated intrusion attempt.

質問: **31**
コロラド州デンバーにある複数の機関が共同で運営するデジタルフォレンジック研究所では、捜査官が共同捜査の一環として、ドローン、スマートテレビ、ウェアラブルデバイスから証拠を抽出する必要があります。これらのデバイスは、消費者向けプラットフォームと組み込みプラットフォームの両方を含む多様な構成となっており、チームは、専用ツール

を切り替えることなく、このような混在環境全体で低レベルとファイルシステムレベルの両方の取得を実行できる単一のフォレンジックソリューションを必要としています。これらの要件を最も満たすツールはどれでしょうか？
A. MOBILedit スマートウォッチ キット
B. MO-NEXT
C. MO ドローン
D. IoTインスペクター
正解: **(**正解を表示します**)**
The best answer is B. The product name is commonly presented as MD-NEXT, and it is described by the vendor as forensic extraction software for diverse mobile and digital devices, including drones, smart TVs, wearables, and IoT devices, with support for both physical and logical extraction methods. That makes it the only option in the list that matches the requirement for one tool covering several heterogeneous device categories without switching to separate specialty products. MOBILedit Smartwatch Kit is limited in scope to smartwatch work. MO-Drone or MD-DRONE is focused on drone evidence rather than mixed-device acquisition. IoT Inspector is aimed at observing smart-home device behavior and privacy/network activity, not broad forensic extraction across drones, televisions, and wearables. CHFI v11 includes IoT forensics and mobile device acquisition methods, so this type of tool-selection question is really testing whether the candidate can match the platform mix to the right forensic capability. Because the scenario requires one solution spanning multiple smart and embedded device classes with low-level and filesystem-level acquisition support, MD-NEXT is the strongest fit.

質問: **32**
シカゴで発生したバンキング型トロイの木馬事件を調査する際、フォレンジックアナリストは制御された分析環境内で疑わしいサンプルを実行しました。すると、プログラムは即座に終了し、実行フローを変更したため、アナリストは本来の動作を観察することができませんでした。この動作は、マルウェア分析のどの側面を反映しているでしょうか？
A. 暗号化、コード難読化、アーティファクト除去などの技術の使用
B. 分析環境の検出と実行動作の変更
C. 正確で一貫性のある分析結果を保証する

D. マルウェアの構成要素と動作特性の特定
正解: **(**正解を表示します**)**
The correct answer is B because the malware is displaying analysis-environment awareness and changing its behavior when it detects that it is being observed. MITRE documents virtualization and sandbox evasion as a technique where malware checks for signs of a virtual machine or sandbox and then disengages, terminates, or conceals its true functions. That is exactly what the scenario describes. CHFI v11 includes malware analysis challenges, controlled malware analysis labs, and general rules for malware analysis, all of which prepare candidates to recognize anti-analysis behavior as a practical obstacle. Option A refers to obfuscation and concealment techniques inside the malware itself, which are different from runtime detection of the analysis environment. Option C is not a challenge or tactic, and option D is the goal of analysis rather than the behavior being observed. In a forensic sandbox, when a specimen stops, sleeps, or changes its path because it detects a monitored environment, the key concept is sandbox or analysis-environment evasion. Therefore, the best answer is detection of analysis environments and modification of execution behavior.

質問: **33**
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: **(**正解を表示します**)**
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: **34**
ワシントン州シアトルの病院で発生しているランサムウェア攻撃において、捜査官は厳しい時間的制約の中でストリーミングログを分析し、出力結果に基づいて判断を下さなければならない。この要件に合致するログのフォレンジック調査のカテゴリーはどれか？
A. 進行中の攻撃中にリアルタイム分析が実行され、その結果も生成されます。
B. インシデントの正確な原因の詳細と、将来同様の事態が発生しないようにするために必要な一連のアクションを含む成果物が作成されます。
C. 調査員は、ネットワーク内で既に発生したインシデントを検出および調査するために、事後分析を実施します。
D. 調査員はログファイルを複数回調べることができます
正解: **A (**コメントを発表する**)**
Answer A is correct because the question explicitly describes analysis during an active incident, with logs being examined as they stream in and findings generated immediately to support operational decisions. That is the definition of real-time log analysis, not postmortem review. CHFI v11 covers both postmortem and real- time analysis, and this distinction is important in exam scenarios. Real-time analysis is used when the incident is still unfolding and investigators need immediate visibility into attacker behavior, system impact, and response priorities. Postmortem analysis, by contrast, happens after the event and is focused on understanding what already occurred. Option B describes a later reporting or lessons-learned outcome, and option D is too generic to represent a specific examination category. In a ransomware crisis, streaming evidence must often be reviewed continuously to guide containment, isolate affected systems, and identify ongoing malicious actions. Since the scenario emphasizes active attack conditions and immediate analytical output, the correct CHFI-aligned category is real-time analysis. That is the only choice that matches both the timing and purpose of the examination described.

質問: **35**
ジョージア州アトランタの医療機関で発生した重大なデータ侵害事件の調査において、フォレンジックチームは、文書に隠されたペイロード、システムから消去されたアーティファクト、侵入のタイムラインを不明瞭にする改ざんされたタイムスタンプなど、複数の回避策の証拠に遭遇した。これらの多層的な障害に体系的に対処し、単一の方法に頼るこ

となく包括的な証拠抽出を確実に行うために、チームは分析の信頼性と徹底性を高めるために、どの対策を優先すべきか？
A. 高度なデータ復旧ツールと方法を使用して、隠されたデータ、削除されたデータ、または上書きされたデータを抽出します。
B. ステガノ解析ツールと技術を用いて、ファイルに隠された情報や秘匿された情報を分析する
C. 鑑識捜査官に対し、鑑識妨害技術に関する訓練と教育を行う。
D. パッカー検出ツールを使用して、証拠データに適用された難読化手法を特定し、解凍します。
正解: **(**正解を表示します**)**
The best answer is C because the scenario involves several different anti-forensic tactics at once rather than one isolated concealment method. Concealed payloads, wiped artifacts, and timestomping each require different technical responses, so the most effective overarching countermeasure is to ensure investigators are trained to recognize and respond to a broad range of anti-forensic techniques. CHFI v11 covers anti-forensics techniques, the challenges they create, and countermeasures, and exam questions often distinguish between a tool for one problem and a broader capability that improves the entire investigation. Option A helps with deleted or overwritten data, option B addresses hidden content such as steganography, and option D targets packed or obfuscated material. All are useful, but each is narrow. The question asks what should be prioritized to enhance reliability and thoroughness without relying on a single method. That wording points to investigator awareness and education as the cross-cutting countermeasure that enables the team to choose the right technical method for each evasion tactic encountered. Therefore, training and educating investigators about anti-forensic techniques is the strongest answer.

質問**: 36**
ある組織は、著名なハッカー集団によるものと思われる一連のサイバー攻撃を調査している。これらの攻撃は高度に組織化されており、高度なマルウェアが使用されている。また、コマンド&コントロールのインフラストラクチャは、特定の地政学的意図を持つ組織のものと類似している。しかし、調査官は、攻撃者がハッカー集団の確立された戦術を模倣し、真の身元を隠すためにツールを使用している可能性があると疑っている。この組織が最も直面する可能性が高い帰属特定上の課題はどれか？
A. 既知のグループになりすますために偽旗作戦を用いる攻撃者。
B. マルウェアのシグネチャやコマンド&コントロールインフラストラクチャなどの技術的な指標にアクセスできないこと。
C. 攻撃者の国からの協力が得られないため、国境を越えた活動の調査が困難になる。
D. 攻撃の背後にある地政学的動機を特定することの難しさ
正解**: A (**コメントを発表する**)**

Option A is the best answer because the scenario clearly describes attackers who are mimicking the tactics, tools, and infrastructure style of a known group in order to mislead investigators about their true identity.
CHFI v11 includes cyber attribution , cybercrime investigation , indicators of compromise , and the broader challenges investigators face when determining who is really behind an attack.
A false-flag operation is an attribution challenge in which attackers deliberately imitate another threat actor's methods, malware patterns, geopolitical style, or command-and-control behavior to shift blame. This makes attribution difficult because the visible indicators may have been planted or intentionally shaped to deceive analysts. That fits the question precisely.
The other options do not match as closely. The scenario does not say investigators lack access to technical indicators; in fact, they already have malware and infrastructure clues. Cross-border cooperation and geopolitical motive may matter in some cases, but the central problem described here is intentional impersonation . Therefore, from a CHFI perspective on cyber attribution and investigative challenges, the organization is most likely facing a false-flag attribution problem .

質問: **37**
侵害されたUbuntuウェブサーバーに対するライブレスポンス調査において、アナリストは実行中のプロセス内で観測された不審な動作を調査するためにメモリイメージをキャプチャします。その目的は、特定のプロセスのアドレス空間内で不正なコード実行を示唆する可能性のある異常なメモリ領域の証拠を特定することです。調査担当者は、このようなメモリ異常を特定するためにVolatilityをどのように使用すべきでしょうか？
A. linux.lsof
B. linux.pslist
C. linux.mount
D. linux.malfind
正解: **D (**コメントを発表する**)**
The correct answer is D because malfind is the Volatility plugin specifically intended to locate suspicious memory regions that may contain injected or otherwise unauthorized executable content inside a process address space. Volatility documentation describes malfind as a way to identify hidden or injected code by examining memory protections and suspicious VAD or mapped regions, which is exactly the forensic goal in the question. linux.pslist can enumerate processes, linux.lsof lists open files, and linux.mount shows mount information, but none of those plugins is designed to identify anomalous executable memory regions. CHFI v11 includes Linux memory forensics and malware behavior analysis, so candidates are expected to select the analysis method that directly matches the target artifact. In memory forensics, code injection or unauthorized execution often leaves traces in regions with unusual permissions or content patterns, and malfind is built to surface those anomalies for further review. Because the investigators want to find

suspicious in-process memory areas that may reveal unauthorized code execution, the correct Volatility choice is linux.malfind.

質問**: 38**
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**: 39**
鑑識捜査において、捜査官は容疑者のスマートフォンからデータを収集する必要があります。捜査官は、収集したデータが法廷で証拠として認められるよう、適切な手続きに従う必要があることを認識しています。また、個人情報や機密情報が含まれている可能性のある携帯端末を取り扱う際には、法的および倫理的な問題にも留意しなければなりません。捜

査官は、携帯端末からデータを収集する際に、法的要件を確実に遵守するために、どのような措置を講じるべきでしょうか？
A. デバイスの所有者から許可を得て、証拠収集プロセスが適用される規制に準拠していることを確認してください。
B. データ収集中に外部からの干渉を避けるため、デバイスをインターネットから切断しますが、この操作を記録しないでください。
C. 互換性や規制遵守を確認せずに、利用可能なフォレンジックツールを何でも使用します。
D. 調査を迅速化するため、プロセスを文書化せずにモバイルデバイスからデータを収集します。
正解: **(**正解を表示します**)**
Option A is correct because CHFI v11 gives strong importance to legal and ethical handling of evidence , especially in contexts where data may contain personal or sensitive information. The blueprint explicitly includes seeking consent , best practices for handling digital evidence , legal issues, privacy issues and legal compliance , preserving evidence , and chain of custody . These requirements apply directly to mobile devices, which often contain highly private data and therefore demand careful lawful handling.
Obtaining permission from the device owner , or otherwise ensuring proper legal authority, is foundational to admissibility and professional forensic practice. Just as important, the evidence collection process must comply with applicable regulations and be documented properly. CHFI also covers the mobile forensics process and stresses that sound forensic work requires procedure, documentation, and defensible evidence handling.
Option B may sometimes be operationally useful, but failing to document the action is a major forensic weakness. Option C ignores tool suitability and legal compliance. Option D directly undermines admissibility because undocumented collection damages evidentiary credibility. Therefore, the most CHFI-aligned and legally defensible response is to obtain permission and ensure the process complies with relevant legal requirements.

質問: **40**
テキサス州ヒューストンのeコマースサイトで深夜に発生したインシデントにおいて、アナリストはIISログにデータベースエラーの急増と処理時間の長期化を確認しました。これは、攻撃者がURLにエンコードされた入力を追加したとされるリクエストと一致しています。これらの急増とペイロード文字列を正確に特定して比較するために、調査担当者はどのIIS W3Cフィールドを解析すべきでしょうか？
A. sc-status
B. csメソッド
C. ステムCS
D. cs-uri-query
正解: **(**正解を表示します**)**

The correct answer is D because the cs-uri-query field records the query portion of the requested URI, which is where appended attacker-supplied input typically appears. Microsoft's IIS W3C logging documentation identifies cs-uri-query as the URI query field used to log the query string for dynamic requests. That is exactly the field investigators need when they want to isolate payloads appended to the URL and compare them against time-taken spikes or error bursts. The other fields do not provide the actual appended payload. sc- status records the HTTP status code, cs-method records the request method such as GET or POST, and cs-uri- stem captures only the path portion without the query string. CHFI v11 includes IIS web server architecture and logs as well as investigation of SQL injection and other web-based attacks, so candidates should know that malicious parameters are often preserved in the query component. When the forensic task is to inspect the exact strings appended to the URL, the proper IIS W3C field is cs-uri-query.

質問**: 41**
サイバー攻撃の疑いがあるケースのフォレンジック調査では、調査員はインシデント発生期間中に収集されたネットワークログを確認します。調査員の目的は、これらのログを精査し、発生したイベントの正確な順序を特定し、攻撃元を特定し、インシデントの性質を理解することです。この分析は、何が、どのように、そして誰がその責任者であったかを明らかにするのに役立ちます。
この場合、調査員は次のどの手法を使用していますか?
A. 調査員は通信を盗聴して機密情報を傍受します。
B. 調査員はシステム記録の事後分析を実行し、過去のセキュリティ侵害を評価します。
C. 調査員は、ネットワーク トラフィック ログをリアルタイムで分析して、インシデントの性質を検出します。
D. 調査者は、攻撃元を特定するために IP アドレスのスプーフィングを実行します。
正解**: B (**コメントを発表する**)**
This scenario aligns closely with CHFI v11 objectives under Procedures and Methodology , specifically postmortem analysis and log-based forensic investigation . Postmortem analysis refers to the examination of collected system, application, and network logs after an incident has occurred , with the goal of reconstructing events and determining the root cause of a security breach.
In this case, the investigator is reviewing historical network logs collected during the incident window , not monitoring live traffic. CHFI v11 emphasizes that postmortem analysis is essential for answering the core forensic questions: what happened, how it happened, when it happened, and who was responsible . By correlating timestamps, IP addresses, protocols, and event sequences across logs, investigators can identify attack vectors, trace the origin of the attack, and understand attacker behavior.
Option C is incorrect because real-time analysis applies to live monitoring during an active incident. Option A describes an illegal activity unrelated to forensics, and option D refers to an attack technique rather than an investigative method. Therefore, consistent with CHFI

v11 forensic methodologies, the investigator is performing a postmortem analysis of system records , making option B the correct answer.

質問: **42**
Microsoft Azure環境における設定ミスによる侵害に関するフォレンジック調査において、調査担当者は、クライアント組織がユーザーID、エンドポイントデバイス、およびデータを管理し、Microsoftが物理ホスト、ネットワーク、およびデータセンターの運用を担当していることを確認しました。このような責任分担を最もよく表しているクラウドサービスモデルはどれでしょうか？
A. オンプレミス展開
B. サービスとしてのソフトウェア (SaaS)
C. サービスとしてのインフラストラクチャ (IaaS)
正解: **C (**コメントを発表する**)**
The correct answer is C because the responsibility split described in the question aligns most closely with Infrastructure as a Service. Microsoft's Azure shared responsibility documentation explains that responsibilities differ depending on whether the service model is SaaS, PaaS, or IaaS. In IaaS, the provider is responsible for the physical datacenter, physical hosts, networking fabric, and core infrastructure, while the customer remains responsible for significant portions of what runs in the environment, including identities, endpoints, data, operating systems, and workload configuration. That matches the scenario much more closely than SaaS, where Microsoft would handle substantially more of the stack. On-premises deployment would place nearly all responsibility on the organization itself, which also does not fit. CHFI v11 includes cloud computing service models, cloud threats, and cloud forensics, so candidates are expected to connect a forensic scenario to the correct service model by examining who manages which layers. Since Microsoft handles the physical cloud infrastructure while the customer manages core usage-side components and data, the best answer is Infrastructure as a Service.

質問: **43**
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**: 44**
クリーブランドの医療ポータルで発生したインシデントにおいて、アナリストは、攻撃者が16進数エンコードされた文字をXMLエンドポイントに送信し、それを翻訳すると完全なXML構造が形成されることを発見しました。チームは、攻撃者が送信したペイロードをデコードして復元し、タイムスタンプが一致するように、単一の証拠ソースを使用して同じリクエストに対するサーバーの処理結果を検証する必要があります。この2つのタスクを1か所で実行するために、どのアイテムに頼るべきでしょうか？
A. ステータスコード200
B. クエリ文字列
C. Apacheアクセスログ
D. GETリクエスト
正解**: C (**コメントを発表する**)**
The correct answer is C because the Apache access log is the single evidentiary source that can tie together the request details and the server's response outcome in one timestamped record. The question requires two things from one place: recovering the attacker-supplied payload and confirming how the server responded. A query string may contain the encoded XML payload, but by itself it does not provide the full evidentiary context such as status code, request timing, source host, and request line. A 200 status code is only one field, not a source. A GET request is a request method, not the artifact

repository. Apache access logs routinely record the request line, which can include the query string, along with the response status code and related metadata. That makes them ideal for reconstructing both what the attacker sent and how the server processed it, while keeping timestamps aligned within the same record. In CHFI v11, web application forensics depends heavily on interpreting web server logs to investigate malicious requests, making the Apache access log the strongest answer here.

質問: **45**
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: **(**正解を表示します**)**
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: **46**
デンバーの混雑した国際交通拠点では、捜査官は長時間の調査が不可能な運用状況下で、容疑者のデバイスからデジタル証拠を入手する必要がある。証拠価値を維持しつつ、こうした制約に適合した方法で証拠取得方法を選択しなければならない。

この状況において、データ取得方法の選択に最も直接的に影響を与える要因は何でしょうか？
A. 必須のライブデータ
B. 削除されたデータの復元
C. 利用可能なツール
D. データ抽出を実行するための時間制約
正解: **(**正解を表示します**)**
The best answer is D because the scenario explicitly centers on limited time for examination. CHFI v11 teaches that the choice of acquisition method depends on practical investigative constraints, including the nature of the evidence, volatility, legal scope, and the time available to perform extraction. Here, the dominant operational factor is that investigators cannot spend long periods examining the devices at the scene. That means the acquisition approach must be chosen primarily with time constraints in mind, possibly favoring targeted or faster collection options over slower, more exhaustive methods. Required live data could also influence the method in some cases, but the question does not emphasize volatile memory or active-system state as the main issue. Recovery of deleted data is a goal that may matter later, and available tools are always relevant, but neither is the direct constraint highlighted by the scenario. In CHFI-style reasoning, when the examination setting itself limits how long responders can work, the most immediate deciding factor for acquisition strategy is the time available for extraction. Therefore, time constraints should most directly guide the method selection.

質問: **47**
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: **(**正解を表示します**)**
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: **48**
法医学捜査官のリアムは、財務マネージャーのシステム上で発生した異常なインターネットバンキング取引を調査していた。マネージャーは、デバイスに不正アクセスがあった事実はないと断言したため、リアムはリモートアクセスが関与しているのではないかと疑った。犯人を特定するため、リアムはネットワークトラフィックをキャプチャし、取引に関連するネットワーク活動を分析した。リアムは現在、無線ネットワークのフォレンジック調査のどの段階に取り組んでいるか？
A. アクティブな接続を識別する
B. 不正/悪意のあるアクセスポイントを検出する
C. ワイヤレスアクセスポイントを検出します
D. パケットを傍受して分析する
正解: **D (**コメントを発表する**)**
Option D. Sniff and analyze packets is the best answer because the scenario states that Liam captured network traffic specifically to examine the activity associated with the suspicious transaction. In CHFI v11, network and wireless forensic work includes identifying access points, discovering active connections, and performing packet capture and analysis to reconstruct events and detect suspicious communications.

Once the investigator is actually collecting and examining traffic content, he has moved beyond discovery into the packet-sniffing and analysis phase . This is where the examiner looks for suspicious sessions, authentication attempts, remote-access behavior, protocol anomalies, and other evidence that may show how the transaction was performed remotely.
Option A is narrower and would focus more on enumerating current sessions. Options B and C are earlier wireless-network investigative activities related to locating infrastructure. Since Liam is already capturing and analyzing the actual traffic, the most accurate phase is sniff and analyze packets . That aligns best with CHFI's traffic-analysis and network-forensics objectives.

質問: **49**
ニューヨークの出版社で知的財産権侵害の調査が行われた際、取締役は調査員が会社のノートパソコンを検査することに同意した。機器の取り扱いを開始する前に、別の担当者が立ち会い、承認が適切に行われたことを確認した。この担当者が立ち会った目的を最もよく表しているのは、どの責任か？
A. 証人の署名が1つ以上必要かどうかを決定します
B. 当事者が自発的に契約に署名したことを確認します
C. 必要に応じて証言を行うか、法廷に出廷する
D. 捜査官の役割に基づいて押収権限を確保する
正解: **(**正解を表示します**)**
The correct answer is B because, in a consent-based forensic examination, the role of the witness is to confirm that the consent was knowingly and voluntarily given by the person authorizing the search. Under the CHFI v11 blueprint, investigators are expected to understand seeking consent, obtaining witness signatures, search and seizure procedures, and best practices for handling digital evidence. A witness is not primarily present to decide legal authority, and the witness does not create seizure powers for the examiner. Instead, the witness helps support the validity of the consent process by confirming that the agreement was actually signed and that it was not coerced or improperly obtained. This can become especially important later if the defense challenges whether the examination was authorized. Option A refers to deciding procedural requirements, which is not the witness's core function. Option C may happen in some cases, but it is not the main reason the witness is present at the time of signing. CHFI emphasizes defensibility and proper evidence-handling foundations, so validating voluntary consent is the best answer.

質問: **50**
フォレンジック調査員のヘンリーは、Ubuntuシステム上で稼働するApacheサーバー上でホストされているウェブアプリケーションで発生したサイバー攻撃の分析を任されています。攻撃者はアプリケーションの脆弱性を悪用した疑いがあり、ヘンリーはサーバーのログを調査して不審なアクティビティを特定する必要があります。

調査の一環として、ヘンリーはまずログファイルの保存場所に移動し、Apacheのアクセスログとエラーログを分析します。これらのログは、攻撃の性質を理解し、送信元IP、攻撃の正確な時刻、実行された攻撃の種類を特定するために不可欠です。
ヘンリーは、Ubuntu上のApacheの設定ファイルを見つけて、ログファイルの保存場所を見つける必要があります。ヘンリーがApacheのログファイルに関する有用な情報を入手できるUbuntuマシン上の保存場所は、次のうちどれでしょうか？
A. /var/log/httpd/access_log
B. /usr/local/etc/apache22/httpd.conf
C. /etc/httpd/conf/httpd.conf
D. /etc/apache2/apache2.conf
正解**: (**正解を表示します**)**
According to the CHFI v11 Web Application and Linux Forensics objectives , understanding default web server configurations and log locations is essential for investigating web-based attacks. On Ubuntu systems , the Apache web server package is typically installed as apache2 , and its primary configuration file is located at /etc/apache2/apache2.conf .
This configuration file plays a central role in Apache forensics because it defines or references critical settings, including log file locations , logging formats, enabled modules, virtual host configurations, and included configuration directories (such as sites-enabled and conf-enabled). The actual access and error logs are usually stored in /var/log/apache2/access.log and /var/log/apache2/error.log , but the paths to these logs are defined or confirmed through the apache2.conf file and its included configuration files.
The other options are incorrect in the context of Ubuntu. Paths such as /etc/httpd/conf/httpd.conf and /var /log/httpd/ are associated with Red Hat-based distributions like CentOS and RHEL, not Ubuntu. The path /usr/local/etc/apache22/httpd.conf is typically seen in BSD-based systems or custom Apache installations, not default Ubuntu deployments.
CHFI v11 emphasizes correlating Apache configuration files with access and error logs to accurately analyze attack vectors, timestamps, and source IP addresses during web application forensic investigations.
Therefore, the correct and CHFI-verified answer is /etc/apache2/apache2.conf (Option D) .

質問**: 51**
企業環境において、不正なデータアクセスの兆候が見られたことを受け、上級幹部のAndroidスマートフォンが内部フォレンジック調査のために保護されました。この調査は管理上のものであり、幹部は調査への協力のために待機しています。デバイスはパスコードで保護されており、潜在的な証拠への即時アクセスはできません。調査担当者は、既存のデータを変更したり、高度な技術的措置を講じたりすることなく、アクセス権を取得する

必要があります。証拠の完全性を維持しながら合法的に調査を進めるには、どの方法が最も適切でしょうか？
A. 従業員の協力を得てパスコードを自主的に開示し、調査の完全性を損なうことなく合法的なデータアクセスを確保する。
B. 法令および倫理基準を遵守しながら、体系的に組み合わせを推測してデータにアクセスする、Android 専用のフォレンジック ソフトウェアを使用する。
C. リモートMDMソフトウェアを使用してデバイスのパスコードをリセットし、証拠の完全性を維持しながらデータアクセスを有効にします。
D. 証拠の完全性を損なうことなくデータへのアクセスを確保するために、専用ツールを使用して物理デバイスの取得に関する管理承認を要求します。
正解: **A (**コメントを発表する**)**
Option A is the most appropriate answer because CHFI v11 places strong emphasis on legal compliance, seeking consent, preserving evidence, chain of custody, and following a sound forensic process . In this scenario, the matter is administrative , the device owner is available , and investigators need access without altering data or resorting to more intrusive technical actions. Under those conditions, obtaining the employee' s voluntary cooperation and passcode disclosure is the most defensible and least disruptive method. The blueprint explicitly includes seeking consent , best practices for handling digital evidence , preserving evidence , and chain of custody under legal and procedural requirements.
This answer also aligns with CHFI's mobile forensics areas covering mobile phone evidence analysis, data acquisition methods, logical and physical acquisition of Android devices, and challenges in mobile forensics . Investigators should first use the least destructive, most lawful, and most forensically sound approach before considering advanced acquisition techniques.
Option B is too intrusive for this fact pattern, C alters device state, and D escalates unnecessarily when consent-based access is already available.

質問: **52**
CHFIの調査員であるロバートは、複雑な企業詐欺事件を担当している。彼は、異なる場所、異なる時間に複数のデジタル機器を証拠として押収した。彼の課題は、押収時から法廷提出時までの間に、証拠が改ざんまたは変更されていないことを法廷で証明することである。
ロバートがこれを達成する上で、重要な要素は何でしょうか？
A. 堅牢な保管管理記録
B. ACPOのデジタル証拠原則に依拠する
C. 対象メディアの徹底的な消毒
D. 関係者全員の同意を得る
正解: **(**正解を表示します**)**

Option A. A robust Chain of Custody is the best answer because the issue in the question is proving that evidence remained untampered with from seizure through courtroom presentation . CHFI v11 directly identifies chain of custody as a core requirement under rules and regulations for search, seizure, evidence preservation, and examination. It also emphasizes best practices for handling digital evidence , preserving evidence , and legal requirements tied to admissibility.
The purpose of chain of custody is to document who collected the evidence, when it was collected, how it was stored, who accessed it, and how it moved throughout the investigation . This creates a defensible record showing continuity, integrity, and accountability. In court, that record is critical to demonstrating that the evidence presented is the same evidence originally seized.
The other options are not the central answer. ACPO principles are important guiding principles, but the specific mechanism used to prove handling history is the chain of custody record itself. Sanitizing target media relates to acquisition preparation, not courtroom continuity. Seeking consent may matter legally in some cases, but it does not prove evidence integrity over time. Therefore, chain of custody is the key component.

質問: **53**
捜査官は、企業サーバーに保存されている機密データへの不正アクセスを伴う複雑なサイバー犯罪事件を担当することになった。捜査は、厳格なプライバシー法とデジタル証拠に関するガイドラインが適用される法域で行われている一方、容疑者は独自のプライバシー法と証拠法が適用される別の法域に所在している。捜査官は、特殊なデジタルフォレンジックツールを使用して、容疑者のデバイスから証拠を収集 保全する必要がある。しかし、捜査官は、2つの法域におけるデジタル証拠の収集と取り扱いを規定する異なる法的枠組みを理解する上で、大きな課題に直面する。
捜査の一環として、捜査官は鑑識ツールを用いて容疑者のデバイスの鑑識イメージを作成し、侵害されたシステムからデータを収集します。法的な要件が異なるため、捜査官は証拠の完全性を維持しながら両管轄区域の法律を遵守する方法が分からず困惑しています。この場合、捜査官は証拠の取り扱いにおいてどのような法的課題に直面する可能性があるでしょうか？
A. 新しいファイルシステムやデバイスと互換性のない、古いフォレンジックツールを使用することの課題。
B. 証拠を輸送中に保護するために、鑑識ツールに暗号化機能が必要である。
C. 証拠の取り扱いの均一性を確保するために、関係するすべてのデバイスで同じ鑑識ツールを使用する必要がある。
D. 捜査中に使用される鑑識ツールが、関係する両地域の規制に従って検証されていることを確認する必要がある。
正解: **(**正解を表示します**)**
Option D is the strongest answer because CHFI v11 explicitly includes Legal Issues, Privacy Issues and Legal Compliance , Role of Local/International Agencies during

Cybercrime Investigation , and Validating Laboratory Software and Hardware as important parts of a defensible forensic process.
When an investigation crosses jurisdictions, the examiner must ensure not only that the evidence is preserved correctly, but also that the tools and methods used are legally acceptable and properly validated under the relevant standards or regulations of the involved regions. A tool or process accepted in one jurisdiction may face challenges in another if validation, handling, or privacy requirements differ. That makes validation and legal defensibility a real challenge in cross-border evidence handling.
The other options are less accurate. Tool compatibility, transport encryption, and uniform tool usage may all matter operationally, but they are not the core legal issue described here. The question is about complying with different legal frameworks while maintaining evidence integrity. Therefore, the most accurate CHFI- aligned challenge is ensuring that the forensic tools are validated according to the regulations of both jurisdictions .

質問**: 54**
シカゴの金融サービス会社でマルウェア感染の疑いのある事案が発生し、調査員は、同社のメールサーバーが複数のシステムにわたって不審なトラフィックを中継し、異常なメッセージエラーを生成していることを確認した。この挙動は、システムが侵害され、迷惑メールが配信されている可能性を示唆している。この疑いを検証するために、調査員はどのマルウェアの兆候を優先的に確認すべきか？
A. 原因不明のバウンスメール
B. システムまたは電子メールからのスパムメッセージのアラート
C. 多数の迷惑メールとソーシャルメディアへの投稿
D. システム速度の低下と再起動時間の延長
正解**: (**正解を表示します**)**
Option B is the strongest answer because it directly points to a host or mail system being used to send spam, which is a common operational sign of malware compromise. The CHFI v11 blueprint includes malware behavior, malware artifacts and indicators, and system and network level analysis. In a case where a mail server is relaying suspicious traffic and message errors are appearing, investigators should focus first on alerts showing that spam is being sent from the affected system or associated email environment. That is more specific and more probative than general performance symptoms such as slowdown. Unexplained bounced emails can occur as a side effect, but they are less direct than confirmed alerts of outbound spam activity.
Numerous unwanted emails and social posts is too broad and less tied to forensic validation of the suspect host. From an examiner's perspective, the key is to identify evidence that the compromised machine is actively participating in spam distribution or botnet-style messaging behavior. That aligns with CHFI's expectation that analysts recognize malware indicators not just by file artifacts, but also by suspicious communications and abnormal message-sending patterns across the environment.

質問: **55**
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: **56**
ノースカロライナ州シャーロットにある金融会社でクラウド移行作業が行われている際、調査担当者は、高度なデータ永続性と管理機能を備えつつ、分析のスケールアウトをサポートし、高いパフォーマンスを提供する必要のあるミッションクリティカルなSQL Serverワークロード向けに、Google Cloudのストレージオプションを評価しています。これらの要件に最も適したGoogle Cloudのデータストレージサービスはどれでしょうか？
A. ローカルSSD
B. 永続ディスク
C. ハイパーディスク

正解: **(**正解を表示します**)**
The correct answer is C because Google Cloud positions Hyperdisk as its recommended durable block storage and specifically describes Hyperdisk Throughput as a fit for scale-out analytics workloads. Google's documentation states that Hyperdisk is the fastest and most efficient durable disk for Compute Engine, and its block storage guidance highlights Hyperdisk Throughput for scale-out analytics use cases. That aligns well with a mission-critical SQL Server environment that needs strong persistence, scalable performance, and advanced storage management. Local SSD is very fast but is tied to the host and does not offer the same persistence characteristics expected for this kind of workload. Standard Persistent Disk is durable and broadly useful, but the question emphasizes scaling out analytics and high performance, which points more strongly to Hyperdisk's workload-optimized offerings. CHFI v11 includes cloud platforms and storage-related evidence considerations, so candidates are expected to recognize when a cloud service's performance and durability profile best matches the scenario. Here, Hyperdisk is the most appropriate answer.

質問: **57**
テキサス州ヒューストンで開催されたサイバー犯罪啓発ワークショップで、デジタルフォレンジックアナリストのエブリン・カーバーは、新人に対し、学術アーカイブや医療データベースなど、オンライン情報の大部分は従来の検索エンジンではインデックス化されていないと説明した。さらに彼女は、インターネットのごく一部、意図的に隠蔽されたセグメントでは、匿名性を維持するために、複数の暗号化されたリレーを経由してトラフィックをルーティングする特殊なソフトウェアが必要であることを強調した。エブリンが最後の説明で述べていたのは、インターネットのどの層のことだったのだろうか？
A. ディープウェブ
B. サーフェスウェブ
C. ダークウェブ
D. Torネットワーク
正解: **(**正解を表示します**)**
The correct answer is C because the final explanation describes the dark web, which is the intentionally hidden portion of the internet that commonly requires specialized tools such as Tor Browser for access. The deep web is broader and includes content not indexed by standard search engines, such as academic databases and medical systems, but that alone does not make it the dark web. The key clue is the use of anonymity- preserving software that routes traffic through multiple encrypted relays. That points to access technologies associated with the dark web. Tor Network is the transport mechanism or anonymity network, not the internet layer being asked for in the question. CHFI v11 explicitly covers the dark web, TOR relays, TOR bridge nodes, and how the TOR browser works, so the exam expects candidates to distinguish between the hidden content environment and the underlying anonymity technology used to reach it. Since the question

asks which layer of the internet is being described, the right answer is dark web rather than Tor itself.

質問: **58**
ネットワークセキュリティアナリストのリンダは、セキュリティチームが社内ネットワーク上で異常なアクティビティを検出したことを受け、ファイアウォールのログを確認している。ファイアウォールのログには、ブロックされた複数の着信接続試行が記録されており、リンダはこれらのログの送信元IPアドレスが、組織の通常のネットワーク範囲外のアドレスに対応していることに気づく。この見慣れないIPアドレスは警戒すべき兆候であり、リンダはこれがネットワークへの侵入を試みる可能性のあるものだと認識する。
トラフィックの不審な性質と、会社が最近セキュリティ対策の強化に注力していることを踏まえ、リンダは調査の次の段階に進み、この活動がより広範な攻撃の一環であるのか、それとも誤ってフラグ付けされた正当なリクエストなのかを判断する必要がある。
この時点で、リンダはいくつかの選択肢を検討しています。この疑わしい外部IPアドレスによって引き起こされた可能性のあるセキュリティ侵害をさらに調査するために、彼女は次にどの手順を踏むべきでしょうか？
A. ファイアウォールのサービス状態を調査し、正しく動作していることを確認します。
B. 同じIPアドレスからの最後のログイン成功時のタイムスタンプを確認します。
C. IP アドレスが既知の脅威インテリジェンスソースに関連付けられているかどうかを確認します。
D. 将来の分析のために、すべての外部トラフィックがログに記録されるようにします。
正解: **(**正解を表示します**)**
Option C is the best answer because CHFI v11 emphasizes the Role of Threat Intelligence in Computer Forensics , Indicators of Compromise (IoC) , and the analysis of firewall and network logs during attack investigations. When an unfamiliar external IP appears repeatedly in blocked inbound attempts, one of the most useful next steps is to determine whether that address is linked to known malicious infrastructure or threat intelligence feeds.
Checking threat-intelligence associations helps the investigator decide whether the activity is likely part of a broader intrusion campaign, commodity scanning, botnet behavior, or a known hostile source. That is more directly useful than checking firewall health, which does not address the source's intent. Looking for prior successful logins from the same IP may be helpful later, but it is less immediate than determining whether the IP is already known to be suspicious. Logging all traffic for the future is good practice, but it does not answer the present investigative question.
Therefore, under CHFI's network-forensics and threat-intelligence principles, Linda should next verify whether the source IP is associated with known threat intelligence sources .

質問: **59**

ペンシルベニア州フィラデルフィアにある出版社で発生した職場ハラスメント調査の一環として、フォレンジック調査官は、macOSシステム上での勤務時間外のアプリケーション使用状況と標的型メッセージの活動との相関関係を分析する必要があります。この分析では、集中管理インターフェースを通じて、ユーザーアクティビティ、システムログ、アプリケーション起動、エラーメッセージ、その他のイベント記録を確認する必要があります。調査官は、この分析を行うために何を開くべきでしょうか？
A. コンソール
B. ~/Library/Mail/ および ~/Library/Messages/ ディレクトリ
C. ターミナルに表示
D. /Users//フォルダ
正解: **(**正解を表示します**)**
The correct answer is A because the macOS Console application is the centralized interface used to review log messages, activities, errors, and related system event information. Apple's documentation states that Console collects log messages and reports, and it allows investigators to search log messages and activities from the system and connected devices. That fits the question's requirement to examine user activities, application launches, errors, and other event records in one place. The Mail and Messages directories contain application data and content artifacts, which may still be useful later, but they are not the centralized log- viewing interface described here. Terminal can access logs through commands, but the question asks what should be opened for this type of review, and Console is the native macOS tool directly built for that purpose.
CHFI v11 includes macOS forensic data, log files, directories, and user activity analysis, so candidates should recognize that Console is the primary entry point for reviewing event and activity logs on macOS. For cross- checking off-hours usage and system events, Console is the best starting interface.

質問: **60**
テネシー州メンフィスの物流会社で認証情報が盗まれた事件を受け、捜査官はパケットキャプチャとイベントログを分析し、攻撃者がVPNゲートウェイから複数の中間ホストを経由して内部データベースにどのようにアクセスしたかを把握しようとしています。彼らの当面の目標は、攻撃者がセグメント間で使用したネットワークホップのシーケンスを再構築することです。ネットワークフォレンジックのどの結果がこの目標に最も適していますか？
A. 侵入経路
B. セキュリティインシデントの発生源
C. 攻撃者が使用した侵入技術
D. 痕跡と証拠
正解: **(**正解を表示します**)**
The best answer is A because the question is focused on reconstructing the route the attacker followed through the environment. The wording emphasizes movement from the

VPN gateway to an internal database through intermediate hosts, which is a classic path-reconstruction problem. In CHFI v11, network forensics includes examining packet captures, correlating logs, tracing attack progression, and understanding how malicious activity moves across systems. While identifying the source of the incident can also matter, this scenario is not primarily asking where the attack began. It asks for the sequence of hops used after entry.
Likewise, intrusion techniques concern methods such as credential abuse, lateral movement protocols, or exploitation mechanisms, but those are secondary to the immediate objective stated in the question. Traces and evidence is too general and does not describe a specific analytical outcome. In exam reasoning, when the investigator's task is to map the movement chain across devices and segments, the most precise result is the path of intrusion. That outcome helps analysts understand lateral movement, affected assets, and the order in which the attacker progressed through the network.

質問**: 61**
ニューヨークのテクノロジー企業で発生した企業内部脅威調査において、フォレンジックアナリストはワークステーションのセキュリティイベントログを分析し、不正アクセス試行の痕跡をたどった。ログには、ユーザーがネットワークを介さずにキーボードで認証情報を物理的に入力し、認証に成功したことが示されていた。
このローカルでの対面アクセス方法に対応するログオンタイプはどれですか？
A. ネットワーク
B. 対話型
C. サービス
D. バッチ
正解**: (**正解を表示します**)**
The correct answer is B because Windows defines Interactive logon as the type used when a user logs on locally at the computer by entering credentials at the keyboard. Microsoft's auditing documentation lists Logon Type 2 as Interactive and explains that it is used for local logons at the system console. That matches the question exactly. Network logon refers to remote resource access over the network, Service logon is used by service accounts, and Batch logon is associated with scheduled or batch job execution. CHFI v11 includes types of logon events and event-log analysis, so candidates are expected to identify the proper Windows logon type from the behavior described. In forensic timeline reconstruction, distinguishing interactive logons from network or service activity is important because it helps determine whether a person was physically present at the machine or whether access occurred indirectly. Since the user entered credentials locally with no network involvement, the correct logon type is Interactive. (learn.microsoft.com)

質問: **62**
フォレンジック調査員のルーカスは、Linuxベースのシステムに感染したマルウェアサンプルの挙動を分析する任務を負っています。マルウェアを実行した後、ルーカスはマルウェアがシステムファイルの改ざん、制限されたリソースへのアクセス、カーネルとのやり取りといった不審な動作を行っているのではないかと疑っています。マルウェアとオペレーティングシステムのやり取りを追跡するため、ルーカスはマルウェア実行中に実行されるシステムコールを監視することにしました。このデータを収集するために、マルウェアによって開始されたシステムコールを効果的に追跡・分析し、マルウェアがOSとどのように通信し、悪意のある動作を実行するかについての洞察を得るために、ルーカスは次のどのツールを使用すべきでしょうか？
A. プロセスエクスプローラー
B. strace
C. 自動実行
D. レジショット
正解: **(**正解を表示します**)**
According to the CHFI v11 objectives under Malware Forensics and Linux Memory and System Behavior Analysis , monitoring system calls is a core technique for understanding how malware interacts with the operating system at a low level. On Linux systems, strace is the primary and most effective tool for this purpose.
strace intercepts and records system calls made by a process, along with the signals received and return values. Since all interactions between user-space programs and the Linux kernel occur via system calls, tracing them provides deep visibility into malware behavior. Using strace, investigators can observe actions such as file creation or modification (open, write), privilege escalation attempts (setuid), network communications (connect, sendto), process creation (fork, execve), and access to protected system resources.
This makes strace indispensable for dynamic malware analysis on Linux , as emphasized in CHFI v11.
The other options are incorrect. Process Explorer and Autoruns are Windows-based tools and do not operate on Linux systems. Regshot is also Windows-specific and is used to compare registry snapshots, which are irrelevant in Linux environments.

The CHFI Exam Blueprint v4 explicitly includes Linux malware behavior analysis and monitoring system- level activity , making strace the correct, forensically sound, and exam-aligned tool for tracking malware system calls

質問: **63**
デジタルフォレンジック調査員であるデイビッドは、会社のサーバーから機密データが盗難されたサイバー犯罪事件を調査しています。調査の一環として、デジタル証拠の取り扱い手順が国際的に認められた標準に準拠していることを確認する必要があります。組織内のデジタルフォレンジック能力の構築、維持、および改善に関するガイドラインを提供するISO規格はどれですか？
A. ISO 27043: インシデント調査ガイドライン
B. ISO 27001: 情報セキュリティマネジメントシステム
C. ISO 27037: デジタル証拠の識別、収集、取得、および保存に関するガイドライン
D. ISO 27041: デジタルフォレンジック準備のためのガイドライン
正解: **(**正解を表示します**)**
The correct answer is ISO 27041 , which provides formal guidance for establishing, maintaining, and continuously improving a digital forensic capability within an organization. According to the CHFI v11 syllabus and Exam Blueprint v4, ISO standards play a critical role in ensuring that forensic processes are repeatable, reliable, legally defensible, and aligned with global best practices .
ISO 27041 specifically focuses on forensic readiness , which involves preparing an organization in advance to efficiently respond to digital incidents. This includes defining forensic policies, identifying evidence sources, ensuring tool and process validation, assigning roles and responsibilities, and integrating forensic procedures into incident response and business continuity plans. CHFI v11 emphasizes forensic readiness as a proactive approach that reduces investigation time, lowers costs, and improves evidence quality during cybercrime investigations.
By contrast, ISO 27037 (Option C) addresses only the identification, collection, acquisition, and preservation of digital evidence, not the broader capability-building aspect. ISO 27043 (Option A) focuses on incident investigation principles and processes , while ISO 27001 (Option B) defines an information security management system (ISMS) and is not specific to digital forensics operations.
Therefore, for ensuring organizational-level forensic capability aligned with internationally recognized standards, ISO 27041 is the most appropriate and CHFI v11-aligned answer

質問: **64**
ニューヨーク市で発生した注目度の高い詐欺事件において、捜査官は標準リカバリモードでの復元が繰り返し失敗するiPhoneを入手しました。通常の復元プロセスが失敗した場合でもファームウェアの再ロードを可能にする、より低レベルの復元状態に進むには、どのオプションを使用すべきでしょうか？

A. SecureROM
B. リカバリーモード
C. iBoot
D. デバイスファームウェアアップデートDFUモード
正解: **(**正解を表示します**)**
Answer D is correct because Device Firmware Update mode is the special low-level state used on Apple mobile devices when a standard recovery process is not enough. In practical forensic and device-handling terms, DFU mode allows the examiner or technician to reload firmware at a deeper level than ordinary recovery mode. That makes it the proper choice when the device fails to restore normally. Recovery mode is a higher-level troubleshooting state, so it does not fit the question's wording about proceeding to a lower-level firmware restore condition. SecureROM and iBoot are important elements in Apple's boot chain, but they are not user-selectable operating modes for performing the kind of restore action described here. The CHFI v11 blueprint includes iOS architecture, boot process, and mobile device evidence handling, so candidates are expected to recognize core Apple device startup and recovery concepts. In an exam setting, when the scenario says the normal restore process has failed and asks for the lower-level option used to reload firmware, the verified answer is DFU mode.

質問: **65**
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**: 66**
侵害対応中、チームは容疑者が無線信号を介して押収した携帯端末に変更を加える可能性があることを懸念している。このリスクを直接軽減する保全措置はどれか？
A. 取得した証拠のフォレンジックイメージを作成し、データにアクセスする際には書き込みブロッカーを使用する。
B. 証拠を保管する際は適切な環境を確保してください。例えば、証拠は乾燥した温度管理された環境に保管することができます。
C. あらゆるネットワークに接続可能な遠隔改ざんから証拠を保護する。例えば、ファラデーバッグを使用して信号を回避する。
D. MD5やSHA-256などの暗号学的ハッシュ関数を使用して、保存されたデータの整合性を検証します。
正解**: C (**コメントを発表する**)**
The correct answer is C because Faraday isolation directly addresses the threat described in the question:
remote alteration through wireless communication. Mobile devices can still receive network commands, wipes, synchronization changes, or other signal-triggered activity after seizure unless radio communications are blocked. Guidance from the U.S. Department of Justice states that Faraday isolation bags are used to prevent mobile phones and devices from connecting to communication signals. That makes this the most direct preservation measure for preventing remote changes. Option A is an important general forensic practice, but it does not stop wireless communication to a still-active mobile device. Option B concerns environmental storage conditions, and option D supports integrity verification after collection, but neither blocks remote access. CHFI v11 includes evidence preservation, first response, and mobile forensics processes, all of which require examiners to recognize how to secure live mobile devices against external interference. When the risk is remote signal-based tampering, the best immediate mitigation is to isolate the device from communications using a Faraday bag or equivalent shielding.

質問**: 67**
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: **(**正解を表示します**)**
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: **68**
高度なクラウド攻撃では、攻撃者は標的サーバーの近くに仮想マシン(VM)を戦略的に配置します。共有物理リソースを悪用し、サイドチャネル攻撃を実行し、タイミングの脆弱性を突いて機密データを抽出します。その後、窃取した認証情報を悪用して正規ユーザーになりすまし、深刻なセキュリティリスクをもたらします。攻撃者は、標的サーバーに仮想マシン(VM)が近接していることを悪用して、どのようにクラウドセキュリティを侵害するのでしょうか？
A. サイドチャネル攻撃のための標的型VMオーバーロード
B. DNSハイジャックによるクラウドインフラストラクチャの侵害
C. サイドチャネル攻撃のための共有リソースの悪用
D. SQLインジェクションのためのアプリケーション層の悪用
正解: **C (**コメントを発表する**)**
According to the CHFI v11 Cloud Forensics objectives, cloud environments rely heavily on virtualization , where multiple virtual machines share the same underlying physical

hardware such as CPU caches, memory, storage, and network interfaces. Attackers can exploit this shared-resource model by intentionally placing malicious VMs on the same physical host as the victim VM, a technique often referred to as co-residency attacks . Once co-residency is achieved, attackers perform side-channel attacks that analyze indirect indicators such as cache timing, memory access patterns, or CPU usage to infer sensitive information.
This scenario precisely describes the exploitation of shared resources for side-channel attacks . Timing vulnerabilities in shared CPU caches or memory buses allow attackers to extract cryptographic keys, credentials, or other sensitive data without directly breaching the target system. After obtaining credentials, attackers may impersonate legitimate users, escalating the impact of the attack.
Other options are incorrect because DNS hijacking (Option B) targets name resolution, SQL injection (Option D) operates at the application layer, and VM overloading (Option A) is typically associated with denial-of- service rather than covert data extraction.
The CHFI v11 blueprint explicitly addresses cloud computing threats and attacks , emphasizing risks introduced by multi-tenancy, shared infrastructure, and virtualization , making side-channel exploitation a critical forensic and security concern in cloud investigations

質問**: 69**
セキュリティ侵害の疑いがある企業IISウェブサーバー上で、ネットワークアクティビティとユーザー操作を分析する調査担当者が任命されました。この任務では、調査担当者は大量のIISログデータを処理し、不審なトラフィック傾向、ユーザーアクセス、および潜在的な悪用試行を特定することに重点を置く必要があります。使用するツールは、効率的なログ解析、異常検出、およびイベントのタイムライン再構築に役立つ詳細なレポートの生成を可能にするものでなければなりません。これらの要件を踏まえ、調査担当者はIISログを効果的に分析するためにどのツールを選択すべきでしょうか？
A. 製材所
B. DSInternals PowerShell
C. ジャルホン
D. ハンチリー
正解**: (**正解を表示します**)**
Option A. Sawmill is the best answer because the scenario specifically requires a tool for parsing large volumes of IIS logs , identifying suspicious patterns, and generating detailed reports to support timeline reconstruction. In CHFI-style web-server investigations, examiners are expected to use specialized log- analysis tools to process IIS and Apache logs efficiently rather than relying only on manual review.
Sawmill is well suited to this type of work because it is designed for log analysis and reporting across web- server environments. That makes it the most appropriate choice among the listed options. DSInternals PowerShell is more associated with Active Directory

and internal Windows directory analysis, not IIS log parsing. Hunchly is more focused on web capture and investigation support, not enterprise IIS log analytics.
Jalheon is not the strongest fit for the specific requirements described.
Because the question emphasizes efficient parsing , anomaly detection , and report generation for IIS logs, the most accurate CHFI-aligned answer is Sawmill . It best supports structured web log analysis during breach investigations.

質問: **70**
データ侵害の疑いがある案件のフォレンジック調査において、eDiscoveryチームは侵害を受けたコンピュータシステムからデジタル証拠を収集し、保全する任務を負います。チームは、メール、ファイル、システムログなどの関連データをマシンから抽出するために、専用のツールを導入する必要があります。チームメンバーの1人が、これらのツールの導入、調査の特定のニーズに合わせた設定、そしてデータ収集プロセス全体を通しての保守を担当します。この担当者は、フォレンジック分析中にツールが正しく動作し、有効性を維持することを保証します。eDiscoveryチームのメンバーのうち、このタスクを担当するのは誰ですか？
A. eDiscovery 弁護士は、eDiscovery チームに不可欠なツールの導入をサポートできます。
B. 処理担当者は、eDiscovery チームに必要なツールを展開するプロセスを支援できます。
C. レビュー担当者は、eDiscovery チームに必要なツールの実装を支援できます。
D. eDiscovery ソフトウェアの専門家は、eDiscovery チームに必要なツールのセットアップをお手伝いします。
正解: **(**正解を表示します**)**
According to the CHFI v11 curriculum and Exam Blueprint v4, the eDiscovery process involves multiple specialized roles, each with clearly defined responsibilities to ensure evidence is collected, preserved, processed, and reviewed in a forensically sound manner. The role described in this scenario aligns specifically with that of an eDiscovery software expert .
An eDiscovery software expert is responsible for the deployment, configuration, validation, and maintenance of forensic and eDiscovery tools used during evidence collection and analysis. This includes ensuring that tools used for acquiring emails, files, logs, and system artifacts are properly configured for the target environment, function correctly throughout the investigation, and comply with forensic best practices.
CHFI v11 emphasizes the importance of tool reliability, validation, and proper configuration to maintain evidence integrity and legal admissibility .
Other roles listed are not appropriate in this contex t. An eDiscovery attorney (Option A) focuses on legal oversight, scope definition, and compliance. Processing personnel (Option B) handle data normalization, indexing, and preparation after collection. Review personnel (Option C) analyze processed data for relevance and privilege. None of these roles are responsible for tool deployment or maintenance.

Therefore, based on CHFI v11 eDiscovery role definitions and responsibilities, the correct and exam-aligned answer is An eDiscovery software expert

質問: **71**
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: **72**
ペンシルベニア州フィラデルフィアの金融サービス会社で、電子メールで社内に配布された不審なExcelスプレッドシートを調査したところ、最近の変更がいくつか見られたものの、最後に保存したユーザーの身元が不明であることが判明した。ドキュメントを最後に

保存したユーザーを特定するには、どの埋め込みメタデータプロパティを調べるべきだろうか？
A. 著者
B. 改訂番号
C. 最終保存者
D. 合計編集時間
正解: **C** (コメントを発表する)
The correct answer is C because the metadata field specifically intended to record the identity associated with the most recent save operation is Last Saved By. Microsoft's support documentation for inspecting Office file properties lists standard document properties such as Author and other descriptive fields, and in forensic practice Office metadata commonly distinguishes the original creator from the user who most recently saved the file. The Author field may identify the original creator or default profile owner, but that is not necessarily the person responsible for the latest modification. Revision Number tracks version increments, and Total Editing Time reflects duration rather than identity. CHFI v11 includes analysis of Word, PowerPoint, and Excel files and their metadata, so candidates are expected to know which property best answers a specific attribution question. When the dispute concerns who performed the most recent save rather than who created the spreadsheet, the most relevant embedded metadata property is Last Saved By. That field directly supports attribution of the latest document-save action.
(support.microsoft.com)

質問: **73**
あなたはデジタルフォレンジック企業の主任フォレンジックアナリストです。あなたの主要顧客の1つである政府機関がセキュリティ侵害を受け、機密文書が不正に漏洩しました。初期調査の結果、攻撃者は従業員であると疑われ、匿名暗号化メールサービスを使用して複数の未知の受信者にこれらの文書を送信したことが判明しました。調査の一環として、容疑者のワークステーションからディスクイメージを入手しました。あなたの任務は、未知の受信者の特定につながる可能性のある関連証拠を抽出し、分析することです。最初にとるべき手順は何ですか？
A. データ漏洩に使用された可能性のあるトロイの木馬やその他のマルウェアの痕跡がないか、ディスクイメージを確認してください。
B. インターネット履歴ファイルを分析し、匿名で暗号化されたメールサービスの痕跡の可能性を探ります。
C. ディスクイメージ全体を検索し、匿名暗号化メールサービスに関連するファイルアーティファクトを検出します。
D. ディスクイメージ上のメールクライアントを検査し、受信者の情報が含まれている可能性のある暗号化されていないデータがないか確認します。
正解: **B** (コメントを発表する)

Option B is the best first step because the scenario already points to the use of an anonymous, encrypted email service , and the most direct source of evidence on the disk image is likely to be internet history and browser artifacts associated with access to that service. In forensic investigations, the first priority after acquiring the image is to identify the user's interaction with the suspected communication platform. Browser history, cached pages, cookies, form entries, session remnants, and related web artifacts can reveal service usage patterns, access times, account identifiers, or other traces that help identify unknown recipients or at least narrow the communication path.
Option C is broader and may be useful later, but a full search of all artifacts is less targeted as an initial move.
Option D is weaker because the question specifically refers to an anonymous encrypted email service, which is often web-based rather than tied to a traditional email client. Option A shifts attention to malware without evidence that malware was the primary method of exfiltration. Therefore, the most logical CHFI-style first step is to examine internet history files and related web-use artifacts for traces of the anonymous email activity.

質問**: 74**
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**: 75**
CHFI認定調査員のローラは、ソフトウェア開発会社で発生した重大な事件の調査を依頼された。不満を抱いた従業員が複数の基幹製品に悪意のあるコードを注入し、会社の評判と収益に深刻な損害を与えたのだ。ローラは、容疑者が何週間も連続稼働させており、RAMに重要な証拠が含まれている可能性のある、頻繁に使用されているワークステーションから証拠を収集する最善の方法を決定しなければならなかった。ローラは、収集できる証拠を最大化するために、どのようなデータ収集戦略を採用すべきだろうか？
A. ワークステーションをシャットダウンした後、取得が失敗しました。
B. 重要なファイルを外部ストレージデバイスにコピーしています。
C. ネットワーク経由のリモート取得。
D. 実行中のワークステーションからのライブ取得。
正解**: D (**コメントを発表する**)**
Option D is the strongest answer because the workstation has been running continuously for weeks and may contain critical evidence in RAM . CHFI emphasizes the importance of live acquisition when a running system may hold volatile artifacts such as memory-resident malware, open sessions, unsaved work, active processes, encryption keys, or network connections. In this scenario, shutting the system down would likely destroy some of the most valuable evidence.
A live acquisition allows the examiner to preserve memory and other transient data before moving on to broader collection steps. This is particularly important in a case involving malicious code injection, where evidence may exist only in RAM, temporary locations, or active process space. Because the workstation is heavily used and active, live acquisition maximizes the amount of evidence that can be preserved at the time of collection.
Option A sacrifices volatile evidence. B is incomplete and not forensically comprehensive. C may be useful in some environments but is less appropriate than a direct live acquisition from the running system. Therefore, the best CHFI-aligned strategy is live acquisition from the running workstation .

質問**: 76**

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

A. 時間ベースの相関

B. 対数ベースの相関

C. アラートに基づく相関関係

D. ルールに基づく相関関係

正解: **(**正解を表示します**)**

Option A. Time-based correlation is the best answer because the scenario involves multiple servers , each generating separate logs and events, and the investigator needs to reconstruct the breach efficiently and identify its root cause . CHFI v11 explicitly includes Types of Event Correlation , Event Correlation Approaches , Timeline and Kill Chain Analysis , and centralized logging using SIEM solutions as part of evidence examination and network/log analysis.

When several systems are involved, the most effective first way to connect the activity is to correlate events by time so the examiner can determine the sequence of actions across hosts. This helps answer critical questions such as what happened first, which server was initially affected, how the attacker moved, and when key indicators appeared. That is exactly how investigators build a timeline and isolate the origin or progression of an incident.

Log-based correlation groups similar logs, alert-based correlation focuses on alerts, and rule-based correlation applies predefined logic, but the question stresses identifying the root cause across multiple servers and logs , which is most directly supported by constructing a chronological event sequence .

Therefore, under CHFI event-correlation and timeline-analysis objectives, time-based correlation is the strongest answer.

質問: **77**

ボストンのデータセンターで営業時間外に発生した侵害事件において、当直の対応担当者は、アクティブなプロセス状態、セッションデータ、暗号化データなどのメモリ内ランタイム情報を、後で分析するために保存することに懸念を抱いています。これらの情報の保存を最も危険にさらす行動はどれでしょうか？
A. 被害者のコンピュータに関する基本ドキュメントにアクセスできない
B. 被害者のコンピュータをシャットダウンまたは再起動します。この場合、揮発性データはすべて失われます。
C. データ収集プロセスを文書化していない
D. 被害を受けたコンピュータの一部のコンポーネントは信頼性が高く使用可能であると仮定します。
正解**: (**正解を表示します**)**
This question is directly tied to the CHFI v11 objectives on live acquisition, volatile evidence, and order of volatility. The most damaging action is shutting down or rebooting the victim computer because volatile data exists only while the system is powered and running. Information such as active processes, open network sessions, memory-resident malware, encryption keys, clipboard contents, and temporary runtime artifacts can disappear immediately once power is interrupted or the system restarts. In a forensic setting, that loss can prevent investigators from reconstructing attacker activity or identifying how a compromise was maintained in memory. The CHFI blueprint specifically emphasizes live acquisition, collecting volatile information before non-volatile data, and following rules of thumb for acquisition. Choices like poor documentation are serious procedural mistakes, but they do not instantly destroy the in-memory evidence itself. Likewise, lack of baseline information may complicate interpretation, yet the volatile evidence could still be preserved if collected correctly. The core lesson expected by CHFI is that memory and other high-volatility artifacts must be captured first, before any shutdown, reboot, or other disruptive action is taken.

質問**: 78**
Microsoft Azure 環境でのランサムウェアのトリアージ中に、フォレンジックアナリストは、Azure ポータルを通じて侵害された azure-ubuntu 仮想マシンの OS ディスクのスナップショットを作成することで、その証拠を保全するように指示されます。次の手順のうち、このタスクを正確に完了するのはどれですか？
A. 疑わしい仮想マシンのOSディスクのスナップショットを作成し、そのスナップショットを別のリソースグループ下のストレージアカウントにコピーし、ソースリソースグループからスナップショットを削除し、バックアップコピーを作成してから、フォレンジックワークステーションにスナップショットをマウントします。
B. リモートのフォレンジックワークステーションにAzure CLIをインストールし、az loginを実行し、storageProfile.osDisk.nameを指定してaz vm showコマンドを実行してソースディスクIDを表示し、必要なパラメーターを指定してaz snapshot createコマンドを実行します。

C. Production-group から azure-ubuntu OS ディスクを見つけてクリックし、[スナップショットの作成] をクリックし、[確認と作成] をクリックして、[作成] をクリックします。
D. azure-ubuntu VM を停止し、Production-group から azure-ubuntu OS ディスクを見つけてクリックし、[スナップショットの作成] をクリックします。[スナップショットの作成] ページで、OS スナップショットに任意の名前を付け、スナップショットの種類を読み取り専用に選択し、ストレージの種類を選択してから、[確認] と [作成] をクリックします。
正解: **(**正解を表示します**)**
The correct answer is D because it describes the Azure portal workflow for creating a forensic-style snapshot of the OS disk while preserving the source in a read-only state. Microsoft's Azure documentation explains that a snapshot can be created from a managed disk, and choosing a read-only style is the appropriate preservation-oriented approach for evidentiary handling. Option C is incomplete because it skips the important configuration details that define the snapshot properly, including naming, snapshot characteristics, and storage selection. Option B uses Azure CLI rather than the Azure portal, while the question explicitly asks for the portal-based sequence. Option A adds unnecessary and potentially misleading steps that are not part of the basic snapshot creation task. CHFI v11 includes cloud forensics, Azure evidence acquisition, and VM snapshot acquisition using Azure Portal and PowerShell, so candidates are expected to identify the correct, defensible preservation workflow. Since the scenario focuses on portal-based preservation of a compromised VM's OS disk, the sequence that includes creating a read-only snapshot from the disk in the portal is the best answer.

質問: **79**
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: **(**正解を表示します**)**
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**: 80**
通信サービスプロバイダーは、通話設定時に、発信者と着信者双方の身元確認を多面的なアプローチで行い、関係するユーザーの正当性を確保しています。プロバイダーのセキュリティアナリストであるサラは、このプロセスを監督し、複数の固有識別子を組み合わせて加入者情報を取得し、位置追跡を行っています。
通話セットアップ中にサービス プロバイダーがユーザーの ID を確認するための主な手段として際立っている特定のメカニズムは何ですか。
A. 通話時間を分析します。
B. 発信者の位置のみを追跡します。
C. 通話内容を監視します。
D. IMSI および IMEI 情報を利用します。
正解**: D (**コメントを発表する**)**
According to the CHFI v11 Mobile and IoT Forensics domain, the primary mechanism used by telecommunications service providers to verify user identity during call setup is the use of IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity) . These identifiers are fundamental to cellular network authentication and subscriber management.
The IMSI uniquely identifies the subscriber and is stored on the SIM card, while the IMEI uniquely identifies the mobile device itself. During call setup, the cellular network authenticates the subscriber by validating the IMSI against the provider's Home Location Register (HLR) or Home Subscriber Server (HSS).

Simultaneously, the IMEI is checked to ensure the device is legitimate and not blacklisted. CHFI v11 highlights these identifiers as critical forensic artifacts for subscriber attribution, call detail record (CDR) analysis, and location tracking .
The other options are incorrect because call duration and call content are not used for identity verification.
Monitoring call content is also restricted due to privacy and legal constraints. Tracking location alone does not establish identity; it only provides positional data once authentication has already occurred.
CHFI v11 emphasizes that IMSI and IMEI correlation is essential for mobile forensics investigations, enabling investigators to link calls, devices, locations, and subscribers accurately. Therefore, the correct and CHFI v11-verified mechanism for ensuring user identity during call setup is utilizing IMSI and IMEI information , making Option D the correct answer.

質問**: 81**
疑わしいAndroidアプリケーションのトリアージを行う際、調査担当者はフォレンジックワークステーション上でMobSFを使用してローカル静的解析環境をセットアップします。アプリケーションのアーティファクトを送信したり、結果を確認したりする前に、調査担当者はMobSFのインターフェースが使用可能になるように解析環境を初期化する必要があります。
この環境を稼働可能にするには、どのような操作が必要ですか？
A. 開く
ウェブブラウザを開き、ホームページにアクセスするには http://localhost:8000 にアクセスしてください。
B. python manage.py runserver を実行します。
C. 分析に必要な疑わしいAPKファイルをアップロードしてください
D. ダッシュボード上のアプリケーションハッシュ値、コンポーネントの種類と数などの情報を確認します。
正解**: B (**コメントを発表する**)**
The correct answer is B because MobSF must first be started as a local web application before the interface can be reached in a browser. The installation and startup workflow for MobSF includes launching the server process so that the web interface becomes available. Opening a browser to localhost is the next step only after the application is already running. Uploading an APK and reviewing dashboard data are later actions that depend on the service being operational first. CHFI v11 includes malware analysis and mobile application forensics, and this kind of question tests whether the examiner can distinguish initialization steps from later analytical use. In practical forensic triage, the analysis environment must be brought online before any application submission or review can take place. That makes the server-start action the correct operational enabler. The exact command can vary slightly by installation method or version, but among the listed options,

the one that actually initializes the local analysis environment is running the server process. Therefore, the best answer is running python manage.py runserver.
(github.com)

質問: **82**
内部犯行調査に関与したワークステーションからNTFSメタデータアーティファクトを分析する中で、アナリストは、イベントの順序を偽装するためにファイルタイムスタンプが意図的に操作されたのではないかと疑っている。メタデータの上書きが行われたかどうかを検証するために、アナリストは異なるNTFS属性によって保持されているタイムスタンプ値を比較する。タイムスタンプの改ざんが行われたことを最も確実に示すのは、どの観察結果か？
A. 一貫性のある更新トランザクションエントリ
B. STANDARD_INFORMATION属性と$FILE_NAME属性に格納されているタイムスタンプが一致しません
C. 割り当てられたクラスタ内に削除されたファイルレコードが存在する
D. すべてのNTFS属性において、作成、変更、およびアクセス時間が同一である。
正解: **(正解を表示します)**
The correct answer is B because one of the strongest forensic indicators of NTFS timestomping is a discrepancy between the timestamps held in the STANDARD_INFORMATION attribute and those held in the $FILE_NAME attribute. MITRE's description of timestomping explains that adversaries modify file time attributes to hide changes or make a malicious file blend in with legitimate ones. In practical NTFS forensics, analysts often compare these two metadata sources because they may not be altered in the same way or at the same time. That mismatch can reveal that timestamps were intentionally manipulated. CHFI v11 covers anti- forensics techniques, overwritten metadata, and the challenges such actions create for investigators.
Consistent transaction entries do not indicate tampering by themselves, deleted file records in allocated clusters are unrelated to timestamp manipulation, and identical timestamps everywhere could happen normally or be suspicious only with more context. The most reliable direct sign in the choices given is the mismatch between the two NTFS attribute timestamp sets. That pattern is widely used in forensic validation of timestomping suspicions.

質問: **83**
捜査官が不審なトラフィックがないかApacheアクセスログを調べている。彼女は一連のリクエストに気付いた。
通常、管理者権限に関連付けられていないIPアドレスから/admin.phpへのアクセスがありました。これが不正アクセス試行かどうかを判断するために、彼女は次に何をすべきでしょうか？

A. IPアドレスをサーバーのDNSログと照合して、既知のネットワークの一部であるかどうかを確認します。
B. リクエストに関連付けられたユーザーエージェント文字列を分析して、使用されているブラウザを特定します。
C. これらのリクエストのログエントリにある HTTP ステータス コードを確認して、リクエストが成功したかどうかを識別します。
D. リクエストのタイムスタンプを確認し、営業時間内に発生したかどうかを判断します。
正解: **(**正解を表示します**)**
Option C is the best answer because the immediate next step in evaluating suspicious Apache requests is to determine whether the access attempts were successful or unsuccessful . CHFI v11 explicitly includes Apache Web Server Architecture and Logs , Apache Access and Error Logs , and Tools for Analyzing IIS Logs and Apache Logs , as well as the investigation of web-based attacks by examining log evidence.
The most direct way to assess whether /admin.php was actually accessed is to review the HTTP status codes
. For example, a successful response can indicate actual access, while unauthorized, forbidden, or not-found responses suggest the requests were blocked or unsuccessful. This helps the investigator decide whether the event is merely reconnaissance, brute-force browsing, or a true unauthorized access attempt.
The other actions may still be useful later. DNS context , user-agent analysis , and timing analysis can provide supporting evidence, but they do not answer the primary question as directly as the HTTP response result does. Therefore, under CHFI's Apache-log and web-forensics objectives, checking the status codes is the most important next action.

質問: **84**
カリフォルニア州サンノゼで発生したIntelベースのMacの起動時のフォレンジック調査において、調査官はオペレーティングシステムが起動する前にmacOSブートローダーを検証する段階を特定する必要があります。この検証を実行するコンポーネントはどれでしょうか？
A. boot-efi
B. Boot ROM
C. UEFI firmware
D. iBoot
正解: **(**正解を表示します**)**
In CHFI v11, this question maps to the Operating System Forensics objective that requires understanding Macintosh boot processes and the overall booting process. The correct answer is C because, in an Intel-based Mac startup sequence, the UEFI firmware is the component that verifies the macOS bootloader Boot.efi before handing control toward the operating system. From a forensic perspective, this matters because an examiner must

know which component is being validated and which component performs the validation. Boot.
efi is the bootloader itself, so it cannot be the verifier. Boot ROM participates earlier in the startup trust chain as a low-level hardware-rooted element, while iBoot is also part of Apple's secure startup architecture, but the specific verification of the macOS bootloader on Intel-based Macs is performed by UEFI firmware. This distinction is important during forensic reconstruction because understanding the trust sequence helps investigators interpret secure boot behavior, startup integrity, and possible tampering points. The CHFI blueprint explicitly includes Macintosh boot processes under operating system evidence analysis, so recognizing UEFI firmware's role is directly aligned with the exam objective.

質問: **85**
ニューヨークの金融機関で発生した標的型フィッシング攻撃のフォローアップ調査において、フォレンジックアナリストは侵害されたエンドポイントのイベントログファイル形式の生データを解析し、タイムラインを検証します。シャットダウン前後に書き込み遅延が発生したかどうかを確認するため、イベントごとのタイムスタンプとファイルレベルのステータスフラグを区別する必要があります。この形式で、比較に必要なイベントごとのタイムスタンプを提供するコンポーネントはどれでしょうか？
A. EVENTLOGRECORD構造
B. ELF_LOGFILE_HEADER_WRAP
C. ELF_LOGFILE_HEADER構造体
正解: **A (**コメントを発表する**)**
The correct answer is A because per-event timestamps are stored within the EVENTLOGRECORD structure, not in the file header. Microsoft's EVENTLOGRECORD definition includes fields such as TimeGenerated and TimeWritten, which provide the event-level timing needed to compare when an event occurred versus when it was written to the log. That is exactly what the question is asking for. By contrast, ELF_LOGFILE_HEADER and flags such as ELF_LOGFILE_HEADER_WRAP describe overall file-level state and logging conditions, not timestamps for individual event entries. CHFI v11 covers event log file format, EVENTLOGRECORD structure, and ELF_LOGFILE_HEADER structure, so this distinction is directly within scope. In a timeline validation scenario, analysts must separate the metadata that describes the health or status of the whole log file from the record fields that describe each event. Since the investigators need event-by-event timestamps to evaluate possible late writes around shutdown, the only correct component among the options is the EVENTLOGRECORD structure.

質問: **86**
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: **87**
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**: 88**
多国籍企業による不正調査において、フォレンジックアナリストは、Microsoft Azureに保存されている証拠が法的にどこに保管されるべきかを判断するよう求められています。組織のAzure環境には、冗長性とコンプライアンスを考慮して設計された複数のリージョンペアが含まれており、それぞれがデータ所在地の所在に関する同じ市場レベルのポリシーに基づいて運用されています。この構成を最もよく表すAzureコンポーネントはどれでしょうか？
A. 非地域サービス
B. 利用可能ゾーン
C. 領域
D. 地理
正解**: (**正解を表示します**)**
The correct answer is D because in Azure, a geography is the higher-level boundary that groups one or more regions and represents the data residency boundary for legal, compliance, and sovereignty purposes.
Microsoft's current documentation explains that regions are organized into geographies and that each geography functions as a data residency boundary. It also notes that most Azure region pairs stay within the same geography to satisfy residency requirements. That matches the question exactly, since it describes multiple paired regions operating under shared market-level residency rules. A region is only one physical area containing datacenters, while an availability zone is an isolated location within a single region. A non-regional service does not represent the residency boundary being asked about. In CHFI v11, cloud forensics requires understanding where cloud evidence can exist and how cloud service design affects legal and investigative scope. When the concern is where evidence

may legally reside across paired Azure regions under one compliance umbrella, the best answer is geography, not region or availability zone.

質問: **89**
サンフランシスコで発生した企業スパイ事件で、侵害されたWindowsワークステーションから証拠を調査した結果、フォレンジックアナリストは、容疑者がタスクバーにピン留めされたExcelショートカットを介して機密性の高いスプレッドシートに繰り返しアクセスしていたことを発見しました。使用パターンを再構築するために、チームはアプリケーションに関連付けられたジャンプリストファイルを調べます。タスクバーにピン留めされたプログラムを介して開かれたドキュメントを特定するには、どのような種類のジャンプリストファイルを調査する必要がありますか？
A. 自動目的地
B. AppID アプリケーション識別子
C. カスタム目的地
D. 悪意のあるLNK
正解: **A (**コメントを発表する**)**
The correct answer is A because AutomaticDestinations files are the primary Jump List artifacts used to record documents opened through an application, including programs accessed from the taskbar. In this scenario, Excel is pinned to the taskbar, but the question asks which artifact type helps identify the spreadsheets opened through that program. That points to the Jump List records that store recent and frequent document usage for the application, which are found in AutomaticDestinations files. CustomDestinations are different; they are used for developer-defined or manually customized Jump List behavior and are more associated with custom pinned items or application-specific structures. AppID is not a Jump List file type at all; it is the identifier used to associate a Jump List with a specific application. A malicious LNK is also not the correct artifact category here. The CHFI v11 blueprint includes analysis of LNK files and Jump Lists under Windows artifact examination, so candidates are expected to know which artifact reveals document access history tied to user activity. For opened documents through a pinned application, AutomaticDestinations is the best forensic source.

質問: **90**
経験豊富なフォレンジックアナリストであるあなたは、侵害された疑いのあるLinuxサーバーの調査を依頼されました。あなたはThe Sleuth Kit(TSK)を使用してファイルシステム分析を行い、異常を検出しています。分析中に、データ量が膨大で、各ファイルを手動でチェックするのは非現実的であることに気づきました。プロセスを自動化し、潜在的な証拠をより効果的に特定するために、TSKのどの機能を使用すべきでしょうか？
A. ファイル彫刻
B. ハッシュデータベース検索
C. ファイルシステムのタイムライン

D. ディスクイメージング
正解: **(**正解を表示します**)**
Option B. Hash database lookup is the best answer because the question is specifically about automating the review of a very large number of files and identifying potential evidence more efficiently. CHFI v11 includes hash analysis , identifying suspicious or known files through hashes , and the use of forensic tools to streamline evidence examination across large datasets.
A hash database lookup allows the investigator to compare file hashes against known-good or known-bad sets, quickly filtering out benign system files and highlighting files that are suspicious, altered, or already associated with malicious activity. This is exactly the kind of automation that reduces manual effort in a large- scale file-system analysis.
File carving is useful for recovering deleted content, but it does not primarily automate file triage. File system timeline helps reconstruct activity order, and disk imaging is an acquisition task rather than a feature for rapidly identifying potential evidence. Therefore, under CHFI forensic-analysis principles, the most effective TSK feature for automating identification of relevant evidence is hash database lookup .

質問: **91**
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: **C (**コメントを発表する**)**
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: **92**
捜査官はTorブラウザの活動を調査するためにフォレンジック分析を実施します。メモリダンプを精査してメールの痕跡を抽出し、Torブラウザが開いている状態と閉じている状態の両方で、ストレージデバイスからメールの添付ファイルを分析します。さらに、Torブラウザをアンインストールした後のフォレンジックオプションを検討し、残存する証拠を明らかにします。
Tor ブラウザが関係するシナリオにおけるフォレンジック分析の主な目的は何ですか?
A. Torブラウザが閉じているときにのみ電子メールの添付ファイルを分析する
B. Torブラウザでさまざまな状態の電子メールアーティファクトと添付ファイルを探索する
C. Torブラウザが開いているときにのみ電子メールアーティファクトを検査する
D. Torブラウザのアンインストール後に分析を実行する
正解: **B** (コメントを発表する)
This question aligns directly with CHFI v11 objectives under Dark Web Forensics and Tor Browser Forensics
. The Tor Browser is specifically designed to minimize persistent artifacts and anonymize user activity, which makes forensic investigations particularly challenging. CHFI v11 emphasizes that the primary objective in Tor Browser-related investigations is to identify and extract residual artifacts across multiple operational states of the browser.
Investigators must analyze evidence when the Tor Browser is open , closed , and even after uninstallation , because artifacts may exist in different locations depending on the

browser's state. Memory dumps can reveal live artifacts such as email content, session data, credentials, and attachments when the browser is running.
Storage analysis can uncover downloaded email attachments, cached files, and remnants left behind after normal usage or uninstallation.
CHFI v11 specifically highlights scenarios involving email forensics with Tor Browser open and closed, memory acquisition, and post-uninstallation analysis as complementary techniques rather than isolated tasks.
Focusing on only one browser state would result in incomplete evidence collection.
Therefore, the overarching forensic objective is to explore email artifacts and attachments across various Tor Browser states , making option B the correct and CHFI-aligned answer.

質問: **93**
インターネット活動を匿名化しようとする攻撃者は、Torネットワークを利用します。Torネットワークは、トラフィックを一連のリレー経由でルーティングすることで、発信元を隠蔽します。この方法は、ユーザーの身元と位置情報を保護することを目的としています。しかし、これらの対策にもかかわらず、攻撃者のトラフィックは出口リレーで追跡され、特定されるため、法的措置の対象となる可能性があります。これに対し、攻撃者は、Torネットワークへのアクセスがブロックされている地域で厳しいネットワーク検閲を回避するためにブリッジノードを利用し、Torへのアクセスを回復して匿名性を維持しようとします。ブリッジノードは、攻撃者が検閲を回避しようとする試みにおいて、どのような役割を果たしているのでしょうか？
A. データを中間リレーに送信する前に暗号化します。
B. 検出不可能なエントリーポイントとして機能し、ローカルネットワークの制限を回避するのに役立ちます。
C. 検出を防ぐために、出口リレーのIPアドレスを隠します。
D. 暗号化されたトラフィックを復号化し、宛先サーバーに転送します。
正解: **B (**コメントを発表する**)**
Option B is correct because CHFI v11 explicitly includes TOR Relays and TOR Bridge Node and how the TOR Browser works within the dark web objectives. A bridge node is used when direct access to public Tor entry nodes is blocked or censored. Its role is to function as a less obvious entry point into the Tor network so that users in restricted environments can still connect.
This makes bridge nodes especially important in environments where governments, enterprises, or network administrators attempt to block known Tor infrastructure. The bridge does not primarily perform encryption on behalf of the user, nor does it decrypt traffic for final delivery. Instead, it helps the user get into the Tor network without relying on a publicly listed entry relay that may be blocked.
Option A is inaccurate because Tor encryption is part of the broader Tor routing process, not a unique function of the bridge node. Option C misunderstands the bridge's purpose,

and D describes a role more closely related to traffic exiting the Tor path. Therefore, the bridge node's role is to help bypass censorship by serving as a less detectable entry point.

質問: **94**
ヒューストンの金融機関で発生したデータ侵害調査において、法医学調査官はシステムクラッシュ後のイベントログファイルの整合性状態を判断するためにログを分析しました。ログには記録が書き込まれたものの、ファイルが適切に閉じられていないことが示されており、破損の可能性が示唆されています。ヘッダー構造のどのフラグが、この未コミットの変更状態を反映しているでしょうか？
A. ELF_LOGFILE_ARCHIVE_SET
B. ELF_LOGFILE_HEADER_WRAP
C. ELF_LOGFILE_HEADER_DIRTY
D. ELF_LOGFILE_LOGFULL_WRITTEN
正解: **C** (コメントを発表する)
The correct answer is C because the dirty flag indicates that the event log file was not cleanly finalized and may contain uncommitted or inconsistently updated header information. Technical documentation for the Windows EVT structure identifies ELF_LOGFILE_HEADER_DIRTY as the flag value that marks the file as dirty. It also notes dirty-file scenarios in which the log was in use and the header was not updated correctly, which matches the question's description of a crash after records were written but before the file closed properly. CHFI v11 includes event log file format, ELF_LOGFILE_HEADER structure, and the importance of logs as evidence, so understanding these flags is directly relevant to log integrity assessment. The wrap flag refers to log wrapping behavior, archive set indicates archival state, and logfull written reflects a write failure due to insufficient space. None of those captures the condition of possible uncommitted changes after an improper close. For forensic exam logic, when the log may be inconsistent because the system crashed before normal closure, the correct header flag is ELF_LOGFILE_HEADER_DIRTY.

質問: **95**
ニューヨークの金融機関で行われたマルウェア調査中、フォレンジック調査員はWindowsフォレンジックワークステーション上で疑わしいファイルを実行した。netstat -anコマンドを使用して、ポートが
ポート1177は開設され、アクティブに接続されていました。捜査官は、観測されたポート活動が正当なサービスに関連するものか、悪意のある行為を示すものかを判断する必要があります。捜査官はこのポート活動の重要性をどのように評価すべきでしょうか？
A. ワークステーションで開かれている疑わしいポート番号がないかリストを確認してください。
B. オンラインの港湾データベースを参照してください
C. フォレンジックワークステーションで疑わしいファイルを実行する

D. netstat -an を使用して、アクティブなすべての TCP/IP 接続とアクティブなポートの一覧を表示します。
正解: **(**正解を表示します**)**
The correct answer is B because once investigators have already identified the active port with netstat, the next step is to determine what that port is commonly associated with and whether its use is expected in the environment. Referring to online port databases or trusted service-port references helps analysts map a port number to known applications, registered services, or suspicious historical usage patterns. CHFI v11 includes malware behavior analysis at the system and network level, including monitoring ports and network activities, so candidates are expected to move from observation to interpretation. Option D only repeats the step that has already been performed. Option A is too vague because simply calling a port suspicious does not explain why.
Option C is unsafe and unnecessary because the file has already been executed and the relevant network artifact has been observed. In a forensic workflow, after identifying an unknown active port, investigators should validate its meaning through recognized service-port references and then correlate that knowledge with process, destination, and timing evidence. That makes online port databases the best answer.

質問: **96**
テキサス州オースティンにあるソフトウェア会社で行われた同意に基づく捜索において、捜査官は特定の電子システムを調査する許可を得ました。許可範囲を超えないようにし、収集された証拠の合法性を確保するため、同意書は十分に詳細なものでなければなりません。このニーズに最も適した要件はどれでしょうか？
A. 同意は関係する内部当局によって承認されなければならない。
B. 同意は組織またはデバイスの所有者によって付与されなければなりません。
C. 同意書には、許可された捜索および押収活動の範囲を明確に記載しなければならない。
D. 検索を開始する前に、同意を正式に文書化する必要があります。
正解: **C (**コメントを発表する**)**
The correct answer is C because the main legal risk in a consent-based search is exceeding the permission that was actually granted. For that reason, the consent documentation must clearly define the scope of what systems may be searched, what actions are permitted, and what evidence may be seized or examined. CHFI v11 includes seeking consent, search and seizure, and best practices for handling digital evidence, so candidates are expected to recognize that detailed scope control is what keeps the search lawful and defensible. Formal documentation is important, and valid authority to consent also matters, but neither addresses the specific problem in the question as directly as a clearly defined scope. In digital investigations, devices and systems often contain far more data than is relevant, so ambiguity in consent can quickly create legal problems. Since the question asks what requirement best prevents investigators from going beyond the

authorized boundaries, the strongest answer is that the consent must clearly outline the scope of permitted search and seizure activities.

質問: **97**
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: **98**
貴社はEmotetマルウェア攻撃を受けました。サンドボックス環境での動的解析中に、マルウェアのペイロードがディスク上に存在せず、メモリ上でのみ実行されていることが判明しました。この種のマルウェアの検出と解析が特に困難な理由は何でしょうか？
A. 多態性コードを採用しています。

B. ボットネットを利用して拡散します。
C. これはファイルレスマルウェアの一種です。
D. 二次ペイロードとしてランサムウェアを使用します。
正解: **(**正解を表示します**)**
Option C is correct because malware that executes solely in memory without leaving a conventional file on disk is characteristic of fileless malware . CHFI v11 includes Malware Analysis: Static and Dynamic , memory analysis , and the use of controlled labs to inspect malware behavior, all of which are especially important when dealing with threats that avoid leaving traditional disk artifacts.
Fileless malware is challenging because many traditional security and forensic techniques rely on file-based indicators such as suspicious executables, hashes, or disk-resident payloads. When the malware lives primarily in memory, investigators must rely more heavily on live response, memory dumps, process analysis, and volatile artifact examination . That makes detection and reconstruction more difficult, especially after the system is shut down.
Option A may describe a separate evasion method, but it does not directly explain the lack of disk artifacts.
Option B concerns propagation, not stealth in memory. Option D could be a later stage in some infections, but the core challenge described here is the absence of a file-based payload. Therefore, the best CHFI-aligned answer is that this is fileless malware , which is harder to detect and analyze because it executes in memory.

質問: **99**
あるサイバーセキュリティ企業は最近、インターネット上で蔓延している新たなランサムウェアを発見しました。このランサムウェアは世界中の組織にとって重大な脅威となっています。非常に高度な技術を駆使しており、従来のウイルス対策ソフトを回避する能力を持っています。この脅威に効果的に対処するため、サイバーセキュリティ企業は詳細な分析を行うためにマルウェアサンドボックスを活用することにしました。
上記のような状況において、マルウェアサンドボックスを使用する主な目的は何でしょうか？
A. 管理された環境でランサムウェアを実行し、その動作を観察する。
B. ランサムウェアを他のシステムに配布して、さらに分析を行う。
C. ランサムウェア感染を防ぐために、ホストシステム上の機密データを暗号化します。
D. 感染したシステムからランサムウェアを完全に削除します。
正解: **(**正解を表示します**)**
Option A is the best answer because CHFI v11 explicitly includes "Perform Static and Dynamic Malware Analysis in a Sandboxed Environment," "Malware Analysis: Static and Dynamic," and the

"Prominence of Setting up a Controlled Malware Analysis Lab." These objectives show that the purpose of a sandbox is to let investigators safely run malware and observe what it does without putting production systems at risk.
A ransomware sample that evades traditional antivirus must be studied through controlled execution so analysts can identify file-encryption behavior, persistence mechanisms, dropped files, registry changes, process activity, and network communications. That is exactly what a malware sandbox is built for. It provides containment while allowing the forensic team to gather behavioral indicators and build defensive countermeasures.
Option B is unsafe and contrary to forensic practice. Option C misunderstands the purpose of sandboxing, and D refers to remediation rather than analysis. Therefore, under CHFI's malware-forensics objectives, the primary objective of using a malware sandbox is to execute and observe the ransomware in a controlled environment so its behavior can be understood and documented.

質問**: 100**
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: **101**
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: **C (**コメントを発表する**)**
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: **102**
あなたはデジタルフォレンジックアナリストで、Portable Document Format(PDF)ファイルを解析し、その構造と内容に関する情報を抽出する任務を負っています。徹底的な解析を行うには、PDFファイルの構造を理解することが不可欠です。PDFファイルにおいて、オブ

ジェクトへのランダムアクセスを可能にし、ファイル内のすべてのオブジェクトへのリンクを含み、PDFファイルへの更新履歴の追跡を支援するコンポーネントは何でしょうか？
A. ヘッダー
B. 相互参照表 (xref table)
C. 本文
D. フッター
正解**: (**正解を表示します**)**
According to the CHFI v11 objectives under File Type Analysis and Malware Forensics , understanding the internal structure of a PDF file is critical when investigating malicious documents. A standard PDF file consists of four main components: Header, Body, Cross-reference table (xref), and Trailer (Footer) .
Among these, the cross-reference table (xref table) plays a pivotal forensic role.
The xref table contains byte offsets for every object stored in the PDF file , allowing the PDF reader-and forensic investigators-to locate objects directly without reading the entire file sequentially. This enables random access to objects such as text streams, images, embedded files, JavaScript, and form objects.
Additionally, the xref table supports incremental updates , a mechanism frequently abused by attackers to append malicious content to a legitimate PDF without altering the original data. By analyzing multiple xref sections, investigators can identify document revisions, hidden objects, and malicious insertions .
The Header (Option A) only specifies the PDF version, the Body (Option C) contains the actual objects, and the Footer/Trailer (Option D) points to the xref table but does not provide object indexing itself.
CHFI v11 explicitly emphasizes xref table analysis when examining suspicious PDF documents, as it is essential for detecting embedded malware, tracing document modifications, and reconstructing attack timelines. Therefore, the cross-reference table (xref table) is the correct and exam-aligned answer

質問**: 103**
捜査官は、企業スパイ事件に関連して、容疑者のコンピュータを分析しています。捜査官は、デバイスから関連するすべてのデータを収集する必要があります。これには、最近のユーザー行動に関する洞察につながる可能性のある暫定的な情報も含まれます。捜査を進める中で、捜査官は、テキスト、画像、最近コピーされたリンクなど、過去のユーザー行動に関する様々なデータがシステムに保存されていることを発見しました。この状況で捜査官が調査しているのは、どのような種類の揮発性データでしょうか？
A. 潜在的な証拠を探すために、ネットワーク全体で共有されているリソースに関連するデータを調べます。
B. システムレベルの構成のドライバー/サービス情報を調べています。
C. 印刷スプール ファイルを調べて、印刷操作に関連する情報を探します。

D. ユーザー操作中に一時的に保持された情報について、クリップボードの内容を調べます。
正解: **(**正解を表示します**)**
According to the CHFI v11 Computer Forensics Fundamentals and Data Acquisition objectives, volatile data refers to information that is stored temporarily in system memory and is lost when the system is powered off or restarted. One of the most valuable and commonly overlooked forms of volatile data is the clipboard contents .
The clipboard temporarily stores text, images, URLs, file paths, credentials, commands, and other data that a user copies or cuts during normal system interaction. In corporate espionage and insider threat investigations, clipboard data can reveal recent user intent , such as copied confidential documents, links to exfiltration sites, snippets of sensitive emails, or commands prepared for execution. CHFI v11 highlights clipboard analysis as an important part of live forensic investigations , especially when investigators need to understand recent user activity that may not yet be written to disk.
The other options represent different forensic artifacts but do not match the scenario. Network shared resources, driver/service configurations, and print spool files are not designed to store recently copied text or images. They are either non-volatile or unrelated to direct user copy-paste actions.
Therefore, the volatile data being examined in this case is the clipboard contents , making Option D the correct and CHFI v11-verified answer.

質問: **104**
フォレンジック調査員であるケイセン氏は、侵害を受けたWindowsマシンを調査していました。調査中、ケイセン氏は侵害の影響を把握するために、マシン上で実行されているアプリケーションとサービスに関する重要な情報を収集する必要がありました。調査員は、データ収集がシステムの状態に影響を与えたり変更したりしないようにしながら、アクティブなプロセスや実行中のサービスなどの揮発性の証拠をリアルタイムで収集する必要があります。上記のシナリオにおいて、ケイセン氏にとって役立つツールは次のうちどれでしょうか？
A. Exifツール
B. ワイヤーシャーク
C. タスクリスト
D. ヘキサネーター
正解: **(**正解を表示します**)**
This question aligns with CHFI v11 objectives under Operating System Forensics and Live Data Acquisition .
When investigating a compromised Windows system, collecting volatile data such as running processes and active services is critical, as this information exists only in memory and can be lost if the system is shut down.

CHFI v11 emphasizes the use of native, low-impact system utilities during live forensic response to minimize changes to the system state.
The tasklist command is a built-in Windows utility that displays a list of currently running processes along with associated process IDs (PIDs), memory usage, and service relationships. It is specifically designed for real-time process enumeration and is commonly used in forensic investigations to identify suspicious or malicious processes with minimal system interaction. Because tasklist is native to Windows, it does not introduce external binaries that could alter evidence integrity.
ExifTool is used for metadata analysis, Wireshark captures network traffic rather than process data, and Hexinator is a hex editor used for file-level analysis, not live process enumeration. Therefore, in accordance with CHFI v11 best practices for volatile evidence collection on Windows systems, tasklist is the correct and most forensically sound tool for this scenario.

質問**: 105**
カリフォルニア州ロサンゼルスで発生したボットネット摘発事件において、あるISPの不正対策デスクは、Torインフラストラクチャに属するIPアドレスに追跡された悪意のあるトラフィックに関する法的苦情を継続的に受け取っている。調査担当者は、トラフィックの発信元はTorではないものの、宛先サーバーはこのTorコンポーネントを発信元と認識するため、ほとんどの不正利用に関する苦情や停止要求が寄せられると説明している。彼らが言及しているTorコンポーネントとは、一体どれのことだろうか？
A. 中間中継
B. 入口警備リレー
C. 出口リレー
D. ブリッジノード
正解**: C (**コメントを発表する**)**
The correct answer is C because the exit relay is the final Tor relay that sends traffic out to the destination service. Tor's own documentation states that the website, chat service, email provider, or other destination will see the IP address of the exit relay instead of the actual Tor user. That is exactly why abuse complaints and takedown pressure usually focus on exit relays. Entry guards see the user first, middle relays pass traffic inside the circuit, and bridge nodes help users connect to Tor when normal entry points are blocked, but those components are not normally the publicly visible source IP presented to outside services. CHFI v11 includes dark web concepts, TOR relays, TOR bridge nodes, and the forensic risks of investigating anonymized environments, so understanding relay roles is directly relevant to the exam. In attribution or infrastructure investigations, analysts must know which relay type will appear in third-party logs or external complaints.
Since destination systems see the exit node as the apparent source of outbound traffic, the best answer is exit relay.

質問: **106**
ノースカロライナ州シャーロットの投資銀行で発生した長期にわたる横領事件の捜査において、押収された帳簿や保管機器は、受付担当者、鑑識官、監査人など、複数の担当者を経由して移動した。証言中に証拠改ざんの疑いが生じた場合に備え、それぞれの移動を記録しておく必要がある。この継続的な取り扱いと移動の記録を確立する文書要素はどれか？
A. 証拠の取り扱いに関与した個人とその行動を一覧表示します
B. 証拠の収集と保管の手順について説明します。
C. 証拠の発生源から検査に至るまでの流れを記録する
D. 収集者と基本的な証拠記述子を識別します
正解: **C** (コメントを発表する)
The correct answer is C because this describes chain of custody documentation, whose purpose is to record the movement and handling of evidence from the moment it is collected through transfer, storage, examination, and presentation. CHFI v11 explicitly includes chain of custody, preserving evidence, and best practices for handling digital evidence. In a case involving multiple custodians, the essential need is not just to list who was involved, but to maintain a continuous documented history showing where the evidence went, who possessed it, when transfers occurred, and under what conditions. That continuous record is what allows an examiner to rebut claims that the evidence was altered, substituted, or tampered with. Option A captures part of that idea but is incomplete because it does not emphasize the end-to-end movement of the evidence.
Option B describes procedures, and option D describes initial collection details, but neither establishes the full transfer history. For CHFI exam purposes, the key documentation element that proves continuity of possession is the record documenting the movement of evidence from origin through examination.

質問: **107**
メリーランド州ボルチモアでの情報収集活動中に入手した不審な画像を調査した結果、捜査官は隠蔽されたデータの存在を疑っている。入手可能なのはステゴオブジェクトのみであり、元のカバーファイルや使用されたステガノグラフィアルゴリズムに関する情報は一切ない。このような状況では、どのようなステガノグラフィ解析手法を適用すべきか？
A. チョーズンステゴ

B. 既知のステゴ
C. 既知被覆
D. ステゴのみ
正解: **(**正解を表示します**)**
The correct choice is D because stego-only analysis is the method used when investigators have access only to the suspected stego-object and do not possess the original cover object or the embedding algorithm. This is exactly the limitation described in the question. In CHFI v11, anti-forensics techniques include steganography, and exam questions often test whether the examiner can identify the correct analytical model based on what evidence is available. Known-cover analysis would require both the clean original cover file and the modified stego-object. Chosen-stego would require knowledge of the steganographic tool or algorithm. Since neither is available here, those methods do not fit. The challenge in stego-only analysis is that the examiner must infer concealed content or detect statistical anomalies using only the suspicious object itself. That makes it one of the more difficult steganalysis situations. In exam logic, whenever the question states that only the suspect media exists and there is no baseline file and no algorithm knowledge, the correct classification is stego-only. That is the option that most accurately matches the evidence conditions described.

質問: **108**
中規模企業のIT部門は、ネットワークトラフィックの急増と、社内サーバーから発信される異常なDNSリクエストに気づきました。マルウェア攻撃の可能性に気づいた彼らは、経験豊富なフォレンジック調査員であるリサを雇い、状況を調査させました。リサは、この異常なネットワーク動作を分析し、特にDNSリクエストの監視に重点を置くためにツールを使用することにしました。リサはこのためにどのツールを使用すべきでしょうか？
A. Wireshark
B. Nmap
C. 鼻を鳴らす
D. ネッソス
正解: **(**正解を表示します**)**
Option A. Wireshark is the best answer because the task is to analyze unusual network behavior and specifically monitor DNS requests . Wireshark is designed for packet capture and protocol-level inspection, allowing the investigator to examine DNS queries, responses, timing, source systems, suspicious domains, and other traffic details in depth. This makes it more appropriate than the other options. Nmap is primarily a network scanning tool, useful for discovery and service enumeration, not deep DNS traffic inspection. Snort is an intrusion detection and alerting tool, and while it may detect suspicious activity, it is not the best primary choice for directly inspecting DNS packet contents in a forensic investigation. Nessus is a vulnerability scanner, not a live packet-analysis utility.

From a CHFI network-forensics viewpoint, packet capture and protocol analysis are central to understanding malware-related traffic patterns such as DNS tunneling, beaconing, command-and-control lookups, or suspicious domain resolution behavior. Since Lisa needs detailed visibility into abnormal DNS requests, Wireshark is the most suitable and effective tool for this investigation.

質問: **109**
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: **110**
イリノイ州シカゴの金融機関で発生したサイバー攻撃を受け、調査チームは複数の監視プラットフォームで生成された多数のアラートと重複したログエントリに圧倒されました。相関分析を試みる前に、チームはノイズを減らし分析効率を向上させるための手順を適用しました。この手順はどのようなアクションを表していますか？

A. データの圧縮、重複エントリの削除、またはフィルタリング
B. 複数のソースからのログを中央システムに収集する
C. データ収集中にデータを暗号化および認証する
D. 異なるログタイプのデータを単一のログ形式にフォーマットする。
正解: **(**正解を表示します**)**
The correct answer is A because the step described is log and event reduction before correlation, which focuses on decreasing noise by filtering, compressing, or removing duplicate information. In the CHFI v11 blueprint, event correlation and event deconfliction are specifically listed under image and evidence examination, and that includes preparing data so analysts can identify meaningful patterns without being distracted by repetitive or irrelevant entries. Option B refers more to centralization or aggregation of logs, which can be useful, but it does not directly describe the action of reducing repeated entries. Option C concerns secure transmission and integrity protections during collection, which is unrelated to the analytical problem described. Option D points to normalization, where logs from different systems are transformed into a common structure, but the question is focused on reducing alert duplication and noise. From a forensic operations perspective, this preprocessing step improves the quality of later correlation by trimming the data to what matters most. That is why the best answer is the choice describing filtering, compression, and deletion of repeated entries.

質問**: 111**
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**: 112**
テキサス州ダラスのデータセンターを標的としたサービス拒否攻撃の調査の結果、ネットワークアナリストは、攻撃者が特定のTCPフラグの組み合わせを持つパケットを継続的に送信し、接続が完了する前にサーバーのリソースを枯渇させる、非常に多くの半開TCPセッションを確認した。
パケットキャプチャの結果、SYNフラグとFINフラグの両方が同時に設定されたパケットが時折使用されていることも明らかになった。
観測された挙動を最もよく表す攻撃パターンはどれですか？
A. TCP SYNフラッド攻撃
B. TCP RSTフラッド攻撃
C. TCP ACKフラッド攻撃
D. TCP SYN-FIN フラッド攻撃
正解**: (**正解を表示します**)**
The most accurate answer is D because the question explicitly mentions two distinct indicators together: half- open TCP sessions typical of SYN flooding and packets that have both SYN and FIN flags set. A normal TCP packet would not use SYN and FIN together in a legitimate connection setup, so that flag combination is highly suspicious and maps directly to a SYN-FIN flood pattern. A pure SYN flood would explain the half- open sessions, but it would not fully account for the stated observation that packet captures show SYN and FIN set simultaneously. CHFI v11 expects candidates to analyze network traffic for denial-of-service behaviors and to recognize packet-level evidence from abnormal TCP flag combinations. In forensic review, the exact flags matter because they help distinguish common handshake abuse from crafted packets designed to exhaust resources, evade simplistic filtering, or confuse defensive logic. Since the scenario includes the uncommon SYN-FIN combination as a defining artifact, the best answer is not the broader SYN flood label but the more precise TCP SYN-FIN flood attack. That choice best reflects the traffic evidence described in the packet capture.

質問: **113**
コロラド州デンバーにある防衛関連企業の研究施設で行われたフォレンジック復旧作業において、アナリストはラックマウント型ワークステーションから破損した証拠ドライブを復元している。ドライブには双方向のデータ転送が同時実行され、複数のコントローラ間で冗長性を確保することで、いずれかの経路が故障した場合でも可用性を維持できる必要がある。これらの運用要件に基づき、この環境において最も信頼性の高い接続を提供するディスクインターフェイスはどれか？
A. シリアルATA SATA
B. 周辺機器相互接続エクスプレス PCIe
C. スモールコンピュータシステムインターフェース SCSI
D. シリアル接続SCSI SAS
正解: **(**正解を表示します**)**
The best answer is D because Serial Attached SCSI is designed for enterprise environments where reliability, throughput, and path redundancy matter. The scenario describes dual-controller style resilience and continued availability if one path fails, which points to multipath-capable storage connectivity rather than a simpler desktop-oriented interface. CHFI v11 includes disk interfaces and storage concepts under digital evidence fundamentals, so candidates are expected to distinguish enterprise forensic workstation and server storage characteristics from ordinary consumer storage. SATA is common and cost-effective, but it does not match the same level of enterprise redundancy and controller-path resilience suggested here. PCIe is a bus architecture used by devices such as NVMe storage, but it is not the disk interface concept being tested in this option set. Traditional parallel SCSI is older and less aligned with the modern rack-mounted, high-availability context described. SAS supports robust enterprise drive connectivity, simultaneous communication behavior, and high-availability storage designs, which makes it the strongest fit for a forensic recovery workstation that must maintain dependable access even when one path or controller encounters a problem.

質問: **114**
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: **D (**コメントを発表する**)**

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: **115**
企業の機密データを侵害したサイバー攻撃に関するフォレンジック調査において、調査員は、当該組織が様々な社内システムにおけるユーザーアクセス管理にクラウドベースのソリューションを使用していることを発見しました。このソリューションには、シングルサインオン(SSO)、多要素認証(MFA)、詳細なアクセス制御といった機能が含まれており、これらはすべてサードパーティのサービスプロバイダーによって管理されています。調査員は認証システムのログを解析し、システムアクセスパターンと比較することで、侵害時の不正行為を追跡します。当該組織ではどのような種類のクラウドサービスが利用されているのでしょうか？
A. 組織は、アクセス制御または認証管理に Desktop-as-a-Service (DaaS) を使用します。
B. 組織は、システムおよびネットワーク上のユーザー アクセスを管理するために Infrastructure-as-a-Service (IaaS) を使用します。
C. 組織は、Platform-as-a-Service (PaaS) を使用して、カスタム構築された認証およびアクセス制御アプリケーションを展開および管理します。
D. 組織は、承認ルールを適用するために Identity-as-a-Service (IDaaS) を使用します。
正解: **(**正解を表示します**)**
As per the CHFI v11 Cloud Forensics objectives , cloud-based identity and access management solutions that provide Single Sign-On (SSO) , Multi-Factor Authentication (MFA) , centralized authentication, and fine-grained authorization controls-managed entirely by a third-party provider -are classified as Identity- as-a-Service (IDaaS) .
IDaaS is a specialized cloud service model designed specifically for identity management , including authentication, authorization, user provisioning, role-based access control, and centralized logging of authentication events. In forensic investigations, IDaaS platforms are critical evidence sources because they generate detailed authentication logs , login timestamps, MFA challenges, IP addresses, device identifiers, and anomaly alerts. These

logs allow investigators to correlate user identities with access patterns and trace unauthorized or malicious actions across multiple systems.
The CHFI v11 blueprint explicitly differentiates IDaaS from other cloud service models. IaaS focuses on infrastructure resources such as virtual machines and networks, not identity enforcement. PaaS is used for developing and deploying custom applications, which is not indicated here since the authentication is handled by a third party. DaaS delivers virtual desktops and does not inherently manage enterprise-wide authentication and authorization.
Therefore, based on the presence of third-party-managed SSO, MFA, centralized access control, and authentication log analysis, the correct answer-fully aligned with CHFI v11 documentation-is Identity-as- a-Service (IDaaS) .

質問**: 116**
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**: C (**コメントを発表する**)**
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**: 117**

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: **(**正解を表示します**)**
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: **118**
容疑者の携帯端末が関係する犯罪捜査において、鑑識チームはAndroidとiOSの両方のスマートフォンから得られたデジタル証拠を分析する必要がある。それぞれのプラットフォームには、鑑識分析において特有の課題と手法が存在する。
これらのデバイスからデジタル証拠を効果的に抽出 ·分析するために、AndroidおよびiOSのフォレンジック分析に関する以下の記述のうち、最も正確なものはどれですか？
A. iOSは包括的なデジタル証拠抽出のための強力なオープンソースのフォレンジックツールを提供していますが、Androidはフォレンジックソフトウェアのサポートが限られているため、手動による抽出に頼っています。
B. Android デバイスと iOS デバイスはどちらも FAT32 ファイルシステムを使用しているため、クロスプラットフォーム互換性と、広く利用可能なツールによる簡単なフォレンジック分析が容易になります。

C. Android: 単一パーティションによりフォレンジック分析が容易になります。iOS: サンドボックスと暗号化の複雑さによりデータ抽出が妨げられます。
D. Android デバイスは、標準的なフォレンジック ツールで簡単にファイルを抽出できるように Ext4 を使用します。一方、iOS デバイスは、APFS (Apple ファイルシステム) の暗号化と複雑さのため、特別な技術が必要です。
正解: **(**正解を表示します**)**
Option D is the most accurate answer because CHFI v11 explicitly includes Android and iOS forensic analysis , logical and physical acquisition of Android and iOS devices , Android and iOS file systems , and APFS file system analysis as major mobile-forensics objectives.
Android devices are commonly associated in forensic contexts with Ext4-based storage structures , while iOS devices use APFS , which introduces additional complexity due to Apple's security model, sandboxing, and strong encryption protections. That makes iOS extraction and examination more dependent on specialized methods and tools. This matches the CHFI view that mobile platforms require different forensic strategies rather than one uniform method.
Option A reverses the practical situation. B is incorrect because FAT32 is not the shared native forensic file- system answer for both platforms. C contains a partially plausible idea about iOS complexity, but it is less precise and less aligned to the file-system-focused wording than D . Therefore, based on CHFI mobile- forensics objectives, the strongest answer is that Android commonly uses Ext4 , while iOS uses APFS and often requires more specialized forensic handling.

質問: **119**
鑑識捜査官のリアムは、容疑者のWindows 11搭載マシンから情報を抽出する任務を負っている。
彼は、容疑者の活動に関する情報が含まれている可能性のある付箋アプリの関連データを調査する必要があります。これを実現するために、リアムはPythonを使用して付箋データベースファイルにアクセスし、分析用のデータを抽出することにしました。リアムは、容疑者のWindows 11システム上で付箋データベースファイルを見つけるために、次のうちどのパスを使用すべきでしょうか？
A. C:\Windows\System32\plum.sqlite
B. C:\Program Files\Microsoft Sticky Notes\plum.sqlite
C. C:\Users\AppData\Local\Packages\Microsoft.MicrosoftSticky Notes.8wekyb3d8bbwe\LocalState\plum.sqlite
D. C:\Users\Documents\StickyNotes.db
正解: **(**正解を表示します**)**
Option C is the correct answer because modern Windows Sticky Notes data is stored in a SQLite database named plum.sqlite within the application's package-specific LocalState path under the user profile. CHFI v11 supports this type of analysis by explicitly including

Windows and Linux forensics using Python , SQLite Database Extraction , Windows File Analysis , and examination of Windows artifacts as part of operating system forensics and Python-based digital forensics.
The question specifically mentions using Python to extract application data, which aligns neatly with CHFI's objective of using Python in digital forensics and with analyzing application-stored databases. Since Sticky Notes persists user note content in a SQLite file rather than in System32, Program Files, or a generic Documents folder, the package-local path is the most accurate location.
The other options are not consistent with how modern Windows Store-style applications usually store their per-user state. Therefore, for CHFI-style Windows artifact analysis and SQLite extraction, the correct path is the user's Packages...\LocalState\plum.sqlite location.

質問: **120**
ジョージア州アトランタのデジタルマーケティング会社で行われたファイルカービング作業中、フォレンジック調査官は、バイナリデータを16進数とASCIIの両方のビューで検査するユーティリティを使用し、0x0000などの特定のバイト位置にあるファイルシグネチャを特定し、未割り当て領域から断片化されたイメージファイルを復元します。低レベルの証拠調査に使用されるこのツールを最もよく表す特徴はどれですか？
A. 16進数表記
B. 16進数領域
C. 16進エディタ
D. 文字エリア
正解: **(正解を表示します)**
The correct answer is C because a hex editor is the actual tool used to inspect raw binary data at a low level in both hexadecimal and character views. CHFI v11 includes understanding hex editors and hexadecimal notation as part of file and data analysis, and this question clearly describes the functionality of the tool itself rather than one section or display region inside it. Hexadecimal notation is the representation system being used, not the utility. Hexadecimal area and Character Area refer to portions of a hex editor's interface, but they are not the full tool. In forensic work, hex editors are used to identify file signatures, inspect offsets, analyze file headers and trailers, and support carving from unallocated or fragmented space. Since the question asks which feature best characterizes the utility used for this type of evidence examination, the most accurate answer is hex editor. That term captures the complete tool that allows investigators to work directly with binary data and locate signatures such as JPEG, PNG, or document headers at exact offsets.

質問: **121**

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: **C** (コメントを発表する)
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: **122**
カリフォルニア州サンノゼにあるテクノロジー企業で発生した内部脅威調査において、ネットワーク監視により、セキュリティ担当者が従業員の電子メールやチャットメッセージの内容を通信中に傍受し、社内メールサーバーに保存されていたコピーにアクセスしていたことが明らかになった。これらの通信の収集と確認が米国法に準拠していることを保証するために、最も直接的に適用される法令はどれか？
A. 1986年電子通信プライバシー法(ECPA)
B. 1974年プライバシー法
C. 外国情報監視法
D. 2007年アメリカ保護法
正解: **A (**コメントを発表する**)**
The correct answer is A because the Electronic Communications Privacy Act of 1986 is the main U.S. statute that addresses both interception of electronic communications and access to stored electronic communications. The scenario involves two separate but related activities: capturing messages in transit and reviewing copies stored on a mail server. Justice Department materials explain that ECPA includes protections for intercepted electronic communications under the Wiretap Act and for stored communications under the Stored Communications Act. That makes it the most directly applicable law for this type of email and chat evidence handling. The Privacy Act of 1974 focuses on federal agency records rather than general workplace monitoring of electronic communications. FISA and the Protect America Act deal with foreign intelligence and national security contexts, not standard corporate insider-threat investigations. CHFI v11 covers legal issues, privacy issues, and legal compliance affecting digital investigations, so candidates are expected to identify the statute that governs electronic communications content both in transit and in storage.
For that reason, ECPA is the strongest and most defensible answer.

質問: **123**
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: **(**正解を表示します**)**

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: **124**
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**: 125**
多国籍企業向けにサイバー犯罪捜査の専門チームを編成します。担当する役割は、写真家、インシデント対応者、証拠鑑定士、弁護士などです。複雑な事件については外部からの支援も活用します。犯人の特定、証拠収集、そして正義の実現を目指します。
専門的なサイバー犯罪捜査チームを結成する上で重要なステップは何ですか?
A. 法的アドバイスの提供
B. 外部からのサポートの獲得
C. デジタルフォレンジック分析の実施
D. チームメンバーに役割を割り当てる
正解**: D (**コメントを発表する**)**
According to the CHFI v11 Computer Forensics Fundamentals and Investigation Process , one of the most critical steps in forming a specialized cybercrime investigation team is clearly assigning roles and responsibilities to team members . This step ensures that every aspect of the investigation is handled efficiently, lawfully, and without overlap or conflict.
CHFI v11 emphasizes that cybercrime investigations are multidisciplinary by nature and require role-based coordination . Typical roles include first responders, incident responders, forensic examiners, evidence handlers, photographers, documentation specialists, and legal advisors. Clearly defining these roles at the outset ensures proper evidence handling, adherence to legal procedures, and effective incident response .
It also supports maintaining the chain of custody , minimizing contamination of evidence, and ensuring accountability throughout the investigation lifecycle.
While legal advice and external support are important, they are supplementary functions that support the investigation after the core team structure is established. Conducting digital forensics analysis is an operational activity that occurs later in the forensic process, not during team formation.
CHFI v11 explicitly highlights building the investigation team and assigning responsibilities as foundational steps before evidence collection and analysis begin. Without clearly defined roles, investigations risk procedural errors, legal challenges, and inefficiencies.
Therefore, the most crucial step in forming a specialized cybercrime investigation team-fully aligned with CHFI v11 objectives-is assigning roles to team members , making Option D the correct answer.

質問: **126**
テキサス州オースティンにあるテクノロジー企業で無線ネットワークのフォレンジック調査が行われている最中、調査員は標準的なキャプチャツールを用いて、内部侵入が疑われる箇所からのリアルタイムトラフィックを収集しました。影響を受けたエリアに近接していたにもかかわらず、パケットキャプチャは部分的なものしか得られず、抽出されたログには大きな欠落があり、デバイス識別子とタイムスタンプを関連付けることができませんでした。この制限を最も直接的に説明できる条件は何でしょうか？
A. 他の無線ネットワークとの相互運用性
B. 結果の不正確さ
C. 複数のアクセスポイントからトラフィックを収集できない
D. なりすまし攻撃の場合、確固たる証拠を集めるのが難しい
正解: **(正解を表示します)**
The best answer is C because wireless traffic in enterprise environments may be distributed across multiple access points and channels, which means a single capture position or standard capture setup can miss portions of the conversation. That creates the exact symptom described in the question: partial captures and gaps that make it difficult to correlate timestamps and device activity. CHFI v11 includes wireless network investigation and detection of access point issues, spoofing, and related wireless attack conditions, so candidates are expected to understand that collection limitations often arise from the architecture of the wireless environment itself. The problem here is not simply that results are inaccurate in a general sense. It is that the investigator cannot see all relevant traffic when it is spread across different infrastructure points.
Interoperability with other networks does not explain the missing packets, and impersonation attacks may complicate attribution but do not best explain incomplete capture visibility. In forensic practice, incomplete observation across multiple access points is a direct and common reason wireless evidence becomes fragmented and correlation becomes difficult.

質問: **127**
イリノイ州シカゴに本社を置く多国籍企業における重大な独占禁止法違反訴訟において、法務チームは処理の遅延と予算の精査に直面している。フォレンジックコーディネーターは、進行中のレビューを中断することなく、プロセス中のすべての活動と変更を追跡し、透明性と責任を確保する監視管理を導入するよう求められている。eディスカバリー監視フレームワークの中核要素として確立すべき基本的実践はどれか？
A. 指標とKPIを定義する
B. コストを追跡する
C. 監査証跡
D. 保管管理記録を維持する
正解: **(正解を表示します)**

The correct answer is C because audit trails are the core oversight mechanism used to record who did what, when it was done, and what changed during the eDiscovery process. Sources on eDiscovery and legal data handling consistently describe audit trails as essential for transparency, traceability, and defensibility. That matches the scenario's emphasis on tracking activities and changes without interrupting review. CHFI v11 includes eDiscovery process flow, detailed tracking information, and best practices to mitigate cost and risk, all of which align with maintaining a complete audit history. Metrics and KPIs help measure performance, and cost tracking helps budget oversight, but neither provides a chronological accountability record of actions and changes. Chain of custody is also important, especially for evidence handling, yet the question is broader and asks for an oversight control across the ongoing process. Audit trails are what allow later reviewers to see user actions, processing steps, exports, and modifications in a defensible sequence. For that reason, audit trails are the strongest foundation for an eDiscovery oversight framework.

質問**: 128**
デジタルフォレンジック調査員は、サイバー犯罪現場から回収された侵入されたMacコンピュータの分析を任されました。しかし、調査の結果、重要な証拠を含むログメッセージが改ざんまたは削除されていることが分かりました。
Mac コンピュータ上のログ メッセージが改ざんまたは削除されていることを考慮すると、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る可能性がありますか?
A. データ暗号化
B. データの難読化
C. データの隠蔽
D. データ操作
正解**: (**正解を表示します**)**
This scenario directly aligns with CHFI v11 objectives under Anti-Forensics Techniques , specifically techniques used to alter or destroy forensic artifacts to obstruct investigations. Log files on macOS systems- such as system logs, application logs, and security logs-are critical sources of evidence that help investigators reconstruct user activity, detect intrusions, and build event timelines.
When an attacker alters, deletes, or modifies log entries , the anti-forensic technique employed is classified as data manipulation . CHFI v11 defines data manipulation as the intentional modification, deletion, or corruption of data or metadata to mislead investigators or erase traces of malicious activity. Log tampering is a classic example, as attackers often remove evidence of unauthorized access, privilege escalation, or persistence mechanisms. Data encryption would make logs unreadable but not selectively altered or deleted. Data hiding involves concealing information in alternate locations (e.g., steganography or hidden files), while data obfuscation focuses on making data confusing but still present. In

contrast, the complete deletion or alteration of log messages is a deliberate attempt to falsify or erase evidence. Therefore, consistent with CHFI v11 anti- forensics classifications, data manipulation is the correct and most accurate answer.

質問: **129**
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: **130**
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: **131**
シカゴにある金融分析会社で発生した国境を越えた不正調査において、フォレンジック担当者はAmazon EC2インスタンスが侵害された疑いがあると判断しました。証拠の完全性を確保しつつシステムの状態を維持するために、フォレンジックチームはインスタンスのスナップショットを取得する直前にどの手順を実行すべきでしょうか？
A. 侵害されたEC2インスタンスを本番環境から隔離する
B. スナップショットから証拠ボリュームを作成する
C. 証拠ボリュームを鑑識ワークステーションに接続します
D. フォレンジックワークステーションをプロビジョニングして起動します
正解: **(**正解を表示します**)**
The correct answer is A because isolating the compromised EC2 instance helps preserve its state and reduces the chance that the attacker, users, or normal production traffic will continue altering evidence before the snapshot is taken. Current AWS guidance describes incident-response and forensics workflows that isolate affected instances as part of preserving artifacts and protecting the integrity of later acquisition. AWS documentation on forensic orchestration notes that affected EC2 instances are isolated and then disk and

memory acquisition actions proceed. AWS incident-response guidance also recommends isolating potentially compromised EC2 instances by associating an isolation security group. The other options happen later in the forensic workflow. Creating an evidence volume, attaching it to a forensic workstation, and provisioning an analysis host are post-snapshot or downstream examination steps. CHFI v11 includes cloud forensics and data acquisition in the cloud, so the exam logic is to stabilize and preserve the source system first, then acquire evidence from that preserved state. Therefore, the immediate step before snapshotting is to isolate the compromised EC2 instance.

質問**: 132**
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**: 133**
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**: C (**コメントを発表する**)**
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**: 134**
エネルギー企業におけるインシデント発生後の調査において、アナリストはネットワーク防御やサーバーシステムなど、複数の制御ポイントから生成されたセキュリティデータを分析することで、組織的な悪意のある活動を特定する任務を負っています。この調査には、多様なイベントソースを取り込み、それらのソース間で発生した活動を関連付け、統一されたインターフェースを通じてアナリスト主導の調査を支援する実用的な調査結果を提示できるプラットフォームが必要です。アナリストは、このようなリアルタイムかつ複数のソースにわたるイベント分析と調査をどのように実現すべきでしょうか？
A. ELKスタック(Elasticsearch、Logstash、Kibana)
B. ManageEngine EventLog Analyzer
C. OSSEC HIDS
D. IBM QRadar

正解: **(**正解を表示します**)**
The correct answer is D because IBM QRadar is built around real-time ingestion, normalization, and correlation of events and flows from many different sources, then presenting those results through a unified investigative interface. The CHFI v11 blueprint includes centralized logging, SIEM solutions, and event correlation approaches, so the exam expects candidates to identify tools that can combine diverse evidence streams into actionable security findings. IBM documentation states that QRadar consolidates log source and network flow data, performs immediate normalization and correlation, and provides dashboards, offenses, log activity, and network activity views for analysts. That lines up closely with the scenario's need for real-time, cross-source analysis. ELK can aggregate and visualize data effectively, but the question stresses built-in correlation of activity across sources as it occurs. OSSEC is host-focused, and EventLog Analyzer is more centered on log monitoring and analysis rather than the broader SIEM-style cross-source correlation platform described here. For CHFI-style tool selection, a requirement for unified, real-time event correlation across network and system telemetry points most directly to IBM QRadar.

質問: **135**
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**: 136**
法医学捜査官のソフィアは、重大な企業データ窃盗事件を担当している。容疑者はIT部門の従業員で、数百もの機密ファイルを自分のノートパソコンにダウンロードした後、突然退職したとされている。
ソフィアは捜索差押令状を取得し、執行中に容疑者のノートパソコン、デスクトップコンピュータ、および複数の記憶装置を発見しました。証拠品の保管管理の連鎖を維持し、ACPO(米国検察庁)のデジタル証拠に関する原則を遵守するために、彼女は次にどのような行動をとるべきでしょうか？
A. 捜査を迅速化するために、容疑者にデバイスのパスワードを尋ねるべきです。
B. 彼女は直ちに現場でデジタル機器の分析を開始すべきです。
C. 令状に記載されている情報に従って、彼女は個人のノートパソコンのみを押収すべきです。
D. 彼女は全ての機器を押収し、分析のために鑑識研究所に送るべきです。
正解**: (**正解を表示します**)**
Option D is the best answer because CHFI v11 places strong emphasis on search and seizure , preserving evidence , chain of custody , and best practices for handling digital evidence . Once lawful authority exists and multiple potentially relevant devices are found, the proper next step is to seize the devices in a controlled manner , document them carefully, and move them to a forensic environment for structured analysis.
Analyzing devices on-site can increase the risk of contamination, incomplete documentation, or unintended alteration. Asking for passwords may be considered in some cases, but it is not the primary next step being tested here. Seizing only the laptop would be too narrow if the warrant and circumstances support collection of other relevant storage devices tied to the offense.
This approach aligns with CHFI's legal and procedural objectives because it preserves evidence integrity, supports a proper chain of custody, and ensures later analysis occurs in a controlled forensic lab environment.
Therefore, the correct action is to seize all relevant devices and send them to the forensic lab for examination .

質問: **137**
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: **138**
あなたは、機密データの漏洩の可能性を調査している大手テクノロジー企業で、コンピュータフォレンジック調査官として働いています。最重要容疑者は、最近退職した従業員です。会社は、容疑者の業務用ノートパソコン(Windows OS搭載)を押収しました。あなたの責任は、調査に必要なデータを取得することです。事件の重大性を考慮すると、証拠の完全性を維持しなければなりません。システムはまだ稼働しており、揮発性データの収集が最優先事項です。揮発性データを収集するための最も正確な手順は何ですか？
A. システムの状態、開いているポートのリスト、実行中のプロセス、およびネットワーク接続。
B. ネットワーク接続、実行中のプロセス、開いているポートのリスト、システムの状態。
C. 開いているポート、実行中のプロセス、ネットワーク接続、システム状態のリスト。
D. 実行中のプロセス、システムの状態、ネットワーク接続、および開いているポートのリスト。
正解: **(正解を表示します)**
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: **139**
イリノイ州シカゴで行われた大規模な金融捜査において、フォレンジックアナリストは、取引記録のアーカイブに使用されている企業向けRAIDアレイを発見した。アレイを調査した結果、データとパリティ情報が複数のディスクに分散されており、2台のドライブが同時に故障してもシステムが動作し続けることがわかった。このフォレンジック分析で明らかになったデュアルドライブの耐障害性という状況に最も合致するRAID構成はどれか？

A. RAID 5
B. RAID 0
C. RAID 6
D. RAID 1
正解: **(**正解を表示します**)**
The correct answer is C because RAID 6 uses distributed parity and is designed to tolerate the failure of any two drives in the array. Storage references and vendor documentation describe RAID 6 as similar to RAID 5 but with an additional parity block arrangement that allows continued operation after two simultaneous disk failures. That matches the scenario exactly. RAID 5 also distributes parity, but it only tolerates a single drive failure. RAID 0 offers striping with no redundancy at all, and RAID 1 relies on mirroring rather than the distributed data-plus-parity design described in the question. CHFI v11 includes RAID storage systems and the logical structure of disks, so candidates are expected to know how fault tolerance differs across RAID levels. In forensic analysis of enterprise storage, recognizing the correct RAID configuration matters because it affects data availability, reconstruction strategy, and interpretation of how evidence survives hardware faults. Since the array continues functioning after two drive failures with distributed parity, the correct answer is RAID 6. (ibm.com)

質問: **140**
テキサス州オースティンで行われた組織的なおとり捜査において、捜査官はダークネット市場を支援する複数のプロバイダーに対し、法的手続きを実施した。複数のサービスからログや登録情報を入手したにもかかわらず、アカウント記録と加入者情報を関連付ける試みは繰り返し失敗し、犯人の特定は依然として困難を極めている。この障害を最もよく説明できるダークウェブフォレンジックの課題はどれか？
A. ダークウェブは犯人の身元を隠すため、犯人の特定は困難である。
B. 専門ツールの使用に関する訓練と専門知識の不足がダークネット分析の課題となっている。
C. 暗号化されたネットワークのため、犯人の物理的な位置を特定することは困難です。
D. 最新技術を用いてサイバー犯罪者が開発したダークウェブアプリケーションの検出は、従来の証拠抽出 ·分析ツールでは困難になる。
正解: **A (**コメントを発表する**)**
The correct answer is A because the core obstacle in the scenario is failed attribution. Investigators already have logs and service-side records, yet they still cannot reliably connect those artifacts to a real-world identity. That is one of the defining forensic difficulties of the dark web: its anonymity mechanisms are intentionally designed to obscure user identity and frustrate tracing. The CHFI v11 blueprint includes dark web concepts, TOR operation, risks of investigating the dark web, and dark web forensic challenges. Those objectives prepare candidates to recognize that the biggest barrier is often not the absence of data, but the inability to tie pseudonymous activity to a specific

person with confidence. Option C mentions physical location and encrypted networks, which is related, but the question is centered more directly on identity correlation and attribution failure than geolocation. Option B focuses on analyst capability, and option D focuses on tool limitations, neither of which is the main issue described. In CHFI terms, when evidence exists but perpetrators remain unidentifiable because anonymity conceals them, the best answer is that tracing the perpetrators is difficult because the dark web hides their identities.

質問: **141**
フロリダ州マイアミで発生した恐喝事件の捜査で、Android端末から収集した証拠を精査した後、アナリストはメッセージングアプリのSQLiteストアを解析した。目撃者のスクリーンショットには直前のメッセージがいくつか写っていたが、それらのエントリは直後に取得したメインデータベースファイルには存在しなかった。このアプリはパフォーマンス最適化されたジャーナリングモードを使用していることが知られている。アナリストは、メインデータベースにまだ統合されていない最新のレコードを復元するために、まずどこを調べるべきだろうか？
A. ライトアヘッドログWALファイル
B. フリーリスト
C. 未割り当て領域
D. ジャーナルファイル
正解: **(正解を表示します)**
The correct answer is A because SQLite in WAL mode writes recent transaction content to the write-ahead log before those changes are checkpointed back into the main database file. SQLite's documentation explains that during transactions, if the database is operating in WAL mode, additional information is stored in a write- ahead log file rather than immediately merged into the main database. That matches the scenario exactly: screenshots show recent messages, but the primary database file does not yet contain them. In a mobile forensic context, this is a common reason the newest chat entries appear missing unless the examiner also parses the companion WAL file. CHFI v11 includes SQLite database extraction and mobile forensic analysis, so candidates are expected to understand where recent application records may reside. The freelist concerns reusable pages, unallocated space may contain remnants, and generic journal files would apply to rollback- journal mode rather than WAL mode. Since the app is specifically said to use the performance-optimized journaling mode, the first place to examine for the missing recent messages is the Write-Ahead Log file.

質問: **142**
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. 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。
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. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **143**
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: **144**
ロサンゼルスの小売チェーンでマルウェア感染の疑いのある事件が発生した後、フォレンジック調査官は、侵害されたサーバーのパフォーマンス低下と、不正な外部通信を示唆する兆候を確認した。システムに影響を与える悪意のある活動の存在を立証するために、調査官はまずどのような証拠を調べて、侵害が実際に発生していることを裏付けるべきだろうか？
A. 異常な交通の流れ
B. ウェブブラウザの設定変更
C. 不明なプロセスが実行されています
D. システム速度の低下と再起動時間の延長
正解: **(正解を表示します)**
The best answer is A because the scenario already points toward unauthorized external communications, so the strongest first corroborating evidence is abnormal network traffic flow. CHFI v11 emphasizes malware indicators, system and network behavior analysis, and monitoring network activities, ports, and DNS as part of malware forensics. While unknown processes running can also be important, the question specifically asks what should be examined first to substantiate an active compromise when suspicious outbound communications are already suspected. Abnormal traffic flows directly support that hypothesis by showing whether the host is beaconing, exfiltrating data, contacting command-and-control infrastructure, or communicating in patterns inconsistent with normal business operations. Browser configuration changes and general system slowdown are weaker, less direct indicators. Slow performance can occur for many benign reasons, whereas suspicious traffic patterns provide stronger evidence of live malicious activity and can also guide scoping across the environment. In CHFI-style reasoning, when network compromise indicators are already present, the most probative next evidence source is the network behavior itself. That makes abnormal traffic flows the strongest answer.

質問: **145**
デトロイトで行われた企業秘密捜査において、捜査官は容疑者の自宅サーバーのイメージングを行うための裁判所の許可を得た。捜索が裁判所の承認した範囲に限定されるようにするためには、令状にその範囲を明確に定義する必要がある。この制限を規定する令状の要件はどれか？
A. 捜索対象場所と押収対象物を指定します。
B. 司法命令に基づき、法執行機関に証拠捜索を指示する
C. 令状の有効期間を定める。
D. 調査員がサービスプロバイダーに相談することを許可する
正解: **(正解を表示します)**
The best answer is A because the requirement that a warrant specify the place to be searched and the items to be seized is what limits the search to the court-approved scope. CHFI v11 covers search and seizure, obtaining a warrant, preserving evidence, and legal

requirements affecting forensic work. In practice, this is the particularity requirement that prevents overly broad searches and helps ensure the examination stays focused on authorized evidence only. That limitation is especially important in digital forensics because a device may contain large amounts of unrelated personal or business information. Option B is too general and does not explain how scope is limited. Option C concerns timing rather than the boundaries of the search itself. Option D is not a core warrant requirement that defines what may be searched or seized. In CHFI-style legal reasoning, whenever the question asks what keeps a warrant narrowly tailored and tied to judicial approval, the correct answer is the provision that identifies the exact place to search and the exact items to seize. That is the central safeguard against an overbroad digital search.

質問: **146**
企業で、ソフトウェアエンジニアのボブは、プロジェクトの機密情報を暗号化したメールを、プロジェクトマネージャーのアリスに緊急に送信する必要がありました。ボブは会社のメールクライアントを使って慎重にメールを作成し、送信ボタンを押しました。しかし、会社のメールサーバーが断続的に接続に問題を抱えていることに気づいていませんでした。
ボブは緊急メールを送信している最中に、社内メールサーバーとの接続問題により遅延が発生しました。この遅延は、メール通信プロセスのどの段階で発生すると考えられますか？
A. 電子メールメッセージを復号化するとき
B. メールの作成中
C. MTAサーバー間の転送中
D. アリスのメールドメインを検索中
正解: **(正解を表示します)**
This question aligns with CHFI v11 objectives under Network and Web Attacks and Email Forensics , specifically focusing on understanding how email communication works. According to CHFI v11, the email delivery process involves multiple stages, including message composition by the Mail User Agent (MUA), message submission to the outgoing Mail Transfer Agent (MTA), inter-server transfer between MTAs, and final delivery to the recipient's mailbox via the Mail Delivery Agent (MDA).
Once Bob clicks "send," the email is handed off from his email client (MUA) to the corporate email server's MTA. If the corporate server is experiencing intermittent connectivity issues, delays most commonly occur during the transfer between MTAs , where the sending MTA attempts to establish an SMTP connection with the recipient's mail server or relay servers. Network instability, DNS delays, or SMTP retry mechanisms can all cause queued messages and delayed delivery at this stage.
Encryption and decryption processes occur locally or at defined endpoints and do not typically introduce network-related delays. Composition is performed entirely on the sender's system, and domain lookups usually happen quickly before transmission.

Therefore, in accordance with CHFI v11 email communication fundamentals, the delay is most likely during the transfer between MTA servers.

質問: **147**
経験豊富なフォレンジック調査員であるレベッカは、一流テクノロジー企業で発生した可能性のあるデータ漏洩の調査に呼ばれた。漏洩した情報には、非常に価値の高い機密設計図ファイルが含まれているようだ。同社のネットワークは侵害されており、漏洩は継続中であると思われる。レベッカのチームの若手メンバーは、さらなる漏洩を防ぐためにサーバーを停止することを提案する。しかし、レベッカはそれがデジタルフォレンジックの重要な原則に反することを知っている。その原則とは何だろうか？
A. デール保存の原則
B. 連邦証拠規則
C. 最良証拠ルール
D. 対象メディアを消毒する原則
正解: **(**正解を表示します**)**
Option A is the best answer. The wording appears to contain a typo, and in CHFI context this clearly points to the principle of data preservation . CHFI v11 emphasizes live acquisition , order of volatility , evidence preservation , and the need to collect volatile information before actions are taken that may destroy it. In an active breach on a running server, abruptly shutting the system down may destroy critical volatile evidence such as RAM contents, active network connections, running processes, logged-in sessions, encryption artifacts, and other transient indicators that may explain how the leak is occurring.
This is why CHFI distinguishes between live acquisition and dead acquisition and teaches investigators to determine the best acquisition method before taking action. Federal Rules of Evidence and the Best Evidence Rule are legal concepts, but they do not directly describe the operational mistake of powering off a live compromised server. Sanitizing target media applies to preparing destination media for acquisition, not preserving a live source system. Therefore, the key violated principle is the preservation of data, especially volatile evidence on a live system.

質問: **148**
複雑なサイバーセキュリティ環境において、アナリストはKippoハニーポットを戦略的に展開し、これらの欺瞞システムを活用して潜在的な攻撃者を誘い込み、罠にかけます。これらの洗練された囮は、本物のネットワーク資産を模倣するように綿密に設計されており、脆弱性を装って攻撃者を罠にかけます。攻撃者がハニーポットを操作すると、その行動は綿密に記録され、攻撃者の手法、戦術、ツールに関する貴重な知見が得られます。アナリストはこれらのハニーポットのログを綿密に分析し、悪意のある行動の複雑なパターンを解読し、このインテリジェンスを活用して、現実世界のサイバー脅威に対する組織の防御を強化します。

動的に変化するサイバーセキュリティ環境の中で、サイバーセキュリティ運用におけるハニーポットのログ分析の最大の目的は何でしょうか?
A. ネットワークに侵入する攻撃者が使用する方法論と戦略を綿密に識別、追跡、理解します。
B. 組織のセキュリティ システムのパフォーマンスを監視および評価し、サイバー脅威に対する防御メカニズムを最適化します。
C. 規制基準とフレームワークへの準拠を保証する包括的なコンプライアンス レポートを生成します。
D. 組織のネットワーク インフラストラクチャ内の潜在的な脆弱性を識別し、プロアクティブなリスク軽減戦略を促進します。
正解: **(**正解を表示します**)**
According to the CHFI v11 Network and Web Attacks domain, the primary purpose of deploying and analyzing honeypots , such as Kippo , is to observe, capture, and understand attacker behavior in a controlled environment . Honeypots are intentionally vulnerable systems designed to attract attackers so their actions can be studied without risking production assets.
CHFI v11 emphasizes that honeypot logs provide high-fidelity intelligence because any interaction with a honeypot is inherently suspicious . By analyzing these logs, investigators can identify attack techniques, tools, malware payloads, command sequences, exploitation patterns, brute-force attempts, and post- compromise activities . This information is invaluable for understanding attacker tactics, techniques, and procedures (TTPs) and for strengthening detection, prevention, and response strategies.
While honeypot data may indirectly reveal vulnerabilities or support security optimization, these are secondary benefits . Honeypots are not primarily deployed for compliance reporting or performance monitoring of security controls. CHFI v11 clearly positions honeypot analysis as a threat intelligence and attacker profiling mechanism , enabling organizations to anticipate real-world attacks and improve defensive readiness.
Therefore, the paramount objective of analyzing honeypot logs-fully aligned with CHFI v11-is to identify, track, and understand attacker methodologies and strategies , making Option A the correct answer.

質問: **149**
イリノイ州シカゴの病院で発生したインシデント対応において、疑わしいアプリケーションサーバーがアクティブなユーザーセッションが稼働したままの状態であることが判明しました。チームは、システムがシャットダウンすると失われてしまうRAM、キャッシュ、動的なプロセス状態などの脆弱で不安定な情報を優先的に取得する必要があります。この要件を最も満たす取得方法はどのようなものでしょうか？
A. ライブアクイジション
B. 論理取得
C. スパース取得

D. デッドアクイジション
正解: **A** (コメントを発表する)
The correct answer is A because live acquisition is the method used when a system is still running and investigators must capture volatile evidence before it disappears. CHFI v11 explicitly includes live acquisition, order of volatility, and collection of volatile information such as memory contents, active processes, cache data, and session information. Those are exactly the artifacts named in the question. Logical acquisition focuses on selected file-system level data and does not specifically address volatile runtime state.
Sparse acquisition is a targeted collection method used to gather selected portions of data, not in-memory artifacts. Dead acquisition is performed after a system is powered down and is therefore unsuitable when the most important evidence would be lost at shutdown. In forensic practice, active servers may contain critical evidence in RAM, open network connections, injected code, encryption material, or running process details that cannot be reconstructed later from disk alone. Since the question centers on preserving volatile evidence from a still-powered system, the correct and most CHFI-aligned answer is live acquisition.

質問: **150**
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**: 151**
大規模なサイバー犯罪捜査において、フォレンジック調査チームは様々なデジタル証拠の詳細な分析を行う責任を負います。このプロセスを効果的に実施するために、チームは分析手法の選択と設計において、認められたベストプラクティスを遵守する必要があります。さらに、チームは証拠の取り扱いに必要な熟練度と能力を備え、その手法が堅牢であり、結果が信頼できることを保証する必要があります。
どの ISO 規格がこれらのプロセスに必要なガイダンスとベストプラクティスを提供し、チームの分析プロセスが正確で、かつ実証可能な能力を備えていることを保証しますか?
A. ISO/IEC 27042
B. ISO/IEC 27050
C. ISO/IEC 27037
D. ISO/IEC 27043
正解**: (**正解を表示します**)**
This question maps directly to CHFI v11 objectives under Standards and Best Practices Related to Computer Forensics . ISO/IEC 27042 specifically addresses the analysis and interpretation of digital evidence , making it the most relevant standard in this scenario.
CHFI v11 emphasizes that forensic analysis must be performed using well-defined, repeatable, and scientifically sound methodologies, and that investigators must be able to demonstrate their technical competence and analytical proficiency .
ISO/IEC 27042 provides guidance on selecting appropriate analytical techniques, validating forensic tools, interpreting results correctly, and ensuring that conclusions are based on reliable and reproducible processes.
It also stresses analyst competence, documentation, peer review, and the avoidance of bias-key factors in ensuring that forensic results are defensible in legal proceedings.
The other standards serve different purposes: ISO/IEC 27037 focuses on evidence identification, collection, and preservation; ISO/IEC 27043 addresses incident investigation principles; and ISO/IEC 27050 relates to eDiscovery processes. None of these focus primarily on analytical method design and interpretation.
Therefore, consistent with CHFI v11 forensic standards, ISO/IEC 27042 is the correct standard for ensuring accurate, competent, and reliable digital forensic analysis.

質問: **152**
サイバーセキュリティアナリストのトーマスは、不審なアクティビティに関するアラートを受け取った後、Webサーバーへの侵入の可能性を調査しています。IISログを確認したところ、短時間のうちに同じIPアドレスから異常に多くのリクエストが送信されていることに気付きました。これらのリクエストは1日のさまざまな時間帯に分散しており、サーバー上の複数のリソースを標的にしているようです。トーマスは、これらのリクエストが脆弱性をスキャンしたり、特定の弱点を悪用したりする大規模な試みの一部である可能性があると疑っています。これらのリクエストの性質をよりよく理解するために、トーマスは次のどのログフィールドに注目すべきでしょうか？
A. sc-status (ステータスコード)
B. cs-uri-stem (リクエストされたURI)
C. cs-ip (クライアントIPアドレス)
D. cs-user-agent (ユーザーエージェント文字列)
正解: **(**正解を表示します**)**
Option B. cs-uri-stem (Requested URI) is the best answer because the question is about understanding what resources were being targeted and whether the pattern suggests scanning, probing, or exploitation. CHFI v11 explicitly includes IIS Web Server Architecture and Logs , Analyzing IIS Logs , and investigating web attacks by examining server logs. The requested URI tells the investigator exactly which pages, scripts, directories, or endpoints the client attempted to access. That is crucial when determining whether a single IP is walking through administrative paths, probing known vulnerable resources, or repeatedly targeting a specific application component. It provides more insight into the nature of the activity than simply knowing the client IP, which is already known from the scenario.
sc-status is useful for checking whether requests succeeded, and cs-user-agent can help identify tools or automation, but neither is as central as the requested resource path when the goal is to understand the intent and pattern of the requests. Therefore, under CHFI web-log analysis objectives, the most informative field here is cs-uri-stem .

質問: **153**

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: **(**正解を表示します**)**
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: **154**
ニューヨーク市のクリエイティブエージェンシーにおける企業ポリシー違反調査の一環として、調査担当者はユーザーの ~/Library/Preferences/ ディレクトリ内のアーティファクトを調査し、不審なファイル転送に関連するアクティビティを関連付けます。調査担当者は、調査対象期間に関連するアプリケーションの使用状況を記録したユーザー固有の plist ファイルを必要としています。この分析を最も効果的にサポートするアーティファクトはどれでしょうか？
A. アプリケーションサポート/
B. com.apple.recentitems.plist
C. com.apple.desktop.plist
D. com.apple.dock.plist

正解: (正解を表示します)
The correct answer is B because com.apple.recentitems.plist is the user-level preference artifact associated with recently used items and application-related recent activity in macOS. Community and forensic references identify this plist in the user's Preferences directory as storing recent-items information that can support timeline reconstruction of user activity. This makes it the best fit when the investigator wants a user-specific plist that reflects application usage around a suspicious time window. Application Support is a directory rather than the specific plist artifact being asked for. com.apple.desktop.plist and com.apple.dock.plist may contain useful configuration or interface state, but they are not the most directly relevant source for recent-item style application usage. CHFI v11 includes macOS forensic data, log files, and directories, so candidates are expected to know where user-activity artifacts reside inside the home profile. Since the question explicitly points to ~/Library/Preferences and asks for the plist that records usage relevant to recent activity, com.apple.
recentitems.plist is the most appropriate answer.

質問: **155**
大規模なデータ侵害に関わるサイバー犯罪捜査において、捜査官は証拠が複数のクラウドベースプラットフォームに分散しており、データが複数の国のサーバーにホストされていることを発見しました。捜査官は国際令状やデータアクセス承認など必要な法的権限を取得しているものの、複数の管轄区域にまたがるクラウドリポジトリの複雑さにより、データの回収に大きな障害に直面しています。これらの問題により、捜査に大幅な遅延が生じ、犯人特定に必要な重要な証拠を迅速に収集することが困難になっています。
この事件で捜査官が直面している主な課題は何ですか?
A. さまざまなクラウドベースのサービスや管轄区域に関係する法律に関する法的理解が限られており、技術的知識も不十分です。
B. クラウド環境ではフォレンジックの準備が整っておらず、証拠収集が妨げられています。
C. 証拠の揮発性により、クラウド環境では重要なログが失われたり上書きされたりすることがあります。
D. 複数の管轄区域にデータが保存されているため、証拠へのアクセスに問題が発生します。
正解: (正解を表示します)
According to the CHFI v11 Cloud Forensics domain, one of the most significant challenges in cloud-based investigations is data residency and multi-jurisdictional storage . Cloud service providers often distribute customer data across multiple geographic regions and countries for redundancy, performance optimization, and availability. As a result, evidence relevant to a single investigation may reside in different legal jurisdictions , each governed by its own data protection laws, privacy regulations, and disclosure requirements.

In the given scenario, the investigator has already obtained the necessary legal authorizations, which rules out lack of legal understanding as the primary issue. However, despite these approvals, accessing data spread across multiple jurisdictions introduces procedural delays , coordination challenges with cloud service providers, and dependencies on international legal frameworks. CHFI v11 explicitly highlights that cross-border data access is a major obstacle in cloud forensics, often slowing investigations even when warrants and mutual legal assistance mechanisms are in place.
While volatility of logs and forensic readiness are valid cloud challenges, the scenario emphasizes delays caused by geographic and jurisdictional dispersion of data , not data loss or lack of preparation. CHFI v11 stresses that investigators must plan for jurisdictional complexity, sovereignty issues, and provider cooperation timelines when handling cloud-hosted evidence.
Therefore, the primary challenge faced by the investigator is data storage in multiple jurisdictions leading to issues in accessing evidence , making Option D the correct and CHFI v11-verified answer.

質問**: 156**
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**: A (**コメントを発表する**)**
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**: 157**
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: **158**
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: **159**
あなたはサイバーセキュリティアナリストとして、Webアプリケーションファイアウォール(WAF)の機能と、Webアプリケーションを様々な攻撃から保護する役割を理解する任務を負っています。WAFの利点と限界を理解し、ModSecurityなどのWAFツールによって生成されるログファイルを分析してWebベースの攻撃を検出する方法を学ぶ必要があります。
Web アプリケーション ファイアウォール (WAF) の主な機能は何ですか?
A. Webアプリケーションの受信および送信HTTPトラフィックの検査とフィルタリング
B. ウェブトラフィックを暗号化して機密性を確保する
C. DDoS攻撃からネットワークインフラストラクチャを保護する
D. システムログを監視および分析して不審なアクティビティを検出します
正解: **(正解を表示します)**

According to the CHFI v11 Web Application Forensics and WAF module , the primary function of a Web Application Firewall (WAF) is to inspect, monitor, and filter HTTP/HTTPS traffic between a web application and its users. Unlike traditional network firewalls, which operate at the network or transport layer, WAFs function at the application layer (Layer 7) and are specifically designed to protect web applications from attacks such as SQL injection, Cross-Site Scripting (XSS), command injection, file inclusion, parameter tampering, and cookie poisoning .
WAFs such as ModSecurity analyze web requests and responses using rule-based logic, signatures, anomaly detection, and behavioral analysis . CHFI v11 emphasizes that WAF logs are critical forensic artifacts, as they record blocked requests, rule violations, payload details, source IP addresses, timestamps, and attack patterns. These logs allow investigators to detect, reconstruct, and attribute web-based attacks during forensic investigations.
The other options do not describe the primary function of a WAF. Encryption of web traffic is handled by SSL/TLS, not WAFs. DDoS protection is typically managed by network-level or cloud-based mitigation systems, although some WAFs may offer limited support. System log monitoring is the role of SIEM solutions, not WAFs.
Therefore, as defined in CHFI v11, the core purpose of a Web Application Firewall is inspecting and filtering HTTP traffic to protect web applications , making Option A the correct and verified answer.

質問**: 160**
ある企業のオンラインバンキングプラットフォームで最近、セキュリティ侵害が発生し、顧客アカウントへの不正アクセスが相次いでいる。調査の結果、ブルートフォース攻撃によって侵入が試みられている疑いがある。
上記のシナリオにおいて、「ブルートフォース攻撃」という用語は、おそらく何を指していると考えられますか？
A. ハッカーがユーザーインターフェース要素を操作して機密データにアクセスする攻撃。
B. 従業員を騙してログイン認証情報を漏洩させるソーシャルエンジニアリングの手法。
C. 企業のネットワークインフラストラクチャの脆弱性を悪用する方法。
D. 攻撃者が不正アクセスを得るために、パスワードや暗号鍵を組織的に推測する手法。
正解**: (**正解を表示します**)**
Option D is the correct answer because a brute force attack refers to a process in which attackers systematically guess passwords or encryption keys until they obtain valid access. CHFI v11 explicitly includes Investigating Brute Force Attack as part of its network and web attack objectives, making this a core concept candidates are expected to recognize.
This differs from social engineering, parameter manipulation, or exploitation of technical vulnerabilities. The defining feature of brute force is repeated trial-and-error authentication attempts , often automated, using many possible password combinations or key values. In

online banking scenarios, this can manifest as repeated login attempts against customer accounts, frequently from the same source or through distributed infrastructure.
Option A describes interface manipulation, B is social engineering, and C is exploitation of vulnerabilities more generally. None of those captures the essential meaning of brute force. Therefore, under CHFI's attack- investigation framework, the most accurate interpretation is that attackers are systematically guessing credentials or keys to gain unauthorized access .

質問**: 161**
企業ワークステーションにおけるマルウェア侵入調査において、フォレンジックアナリストはMagnet AXIOMを使用して、疑わしい実行ファイルがどのように導入され、時間経過とともに実行されたかを再構築します。この調査では、元のバイナリがディスク上に存在しない場合でも、実行されたプログラムに関するメタデータ(ファイルパスや実行コンテキストなど)を記録するアーティファクトが必要です。このアーティファクトは、他のシステム証拠と併せて実行タイムライン分析をサポートするために使用されます。調査担当者は、この目的のためにどのアーティファクトを優先すべきでしょうか？
A. UserAssistエントリ
B. ShimCache AppCompatCache
C. Amcache
D. ファイルのプリフェッチ
正解**: (**正解を表示します**)**
The best answer is D because Prefetch files are one of the strongest Windows artifacts for reconstructing program execution history and building execution timelines. Magnet notes that Prefetch files are valuable because Windows creates them when an application runs from a particular location, and they preserve useful metadata about that application history. They can remain available even if the original executable is no longer present, which makes them especially helpful in malware cases where binaries are deleted after use. In CHFI v11, Windows artifact analysis includes executed-program evidence and timeline reconstruction, so candidates are expected to identify the artifact that most directly supports execution analysis. UserAssist is useful but is more limited to certain user-driven GUI activity. ShimCache and Amcache are important artifacts, yet they are often better treated as evidence of presence or compatibility tracking rather than definitive proof of execution by themselves. Since the question emphasizes executed programs, file paths, and timeline support in AXIOM, Prefetch files are the most precise and defensible answer. They are commonly correlated with other artifacts to strengthen the narrative of malware launch and persistence.

質問**: 162**

パテル刑事は、米国とヨーロッパの被害者に影響を与えた国境を越えたサイバー犯罪を捜査している。このシナリオにおいて、タイムリーな証拠を入手し、管轄区域をまたいだ行動を調整するために、国際機関のどの主要機能が重要となるか？
A. コラボレーション
B. 管轄権の対応
C. 政策と規制
D. 調査
正解: **(**正解を表示します**)**
The best answer is A because the scenario emphasizes timely evidence sharing and coordinated action across more than one jurisdiction. In CHFI v11, the role of local and international agencies in cybercrime investigation is tied closely to cooperation, coordination, and cross-border support. International cybercrime cases often involve different legal systems, different evidence holders, and separate law enforcement or regulatory bodies. Because of that, the most critical function is collaboration between agencies so requests can be aligned, evidence can be preserved quickly, and investigative actions can be coordinated without duplication or delay. Option D sounds plausible, but investigation is a broad activity performed by many parties and does not specifically capture the cross-jurisdiction function highlighted by the question. Option C relates more to governance than operational evidence handling. Option B is not the standard function being tested here. In CHFI-style reasoning, when the issue is multinational evidence coordination and synchronized action, collaboration is the central capability that makes the rest of the process possible. That is why collaboration is the strongest answer.

質問: **163**
金融機関におけるデータ侵害に関するサイバーセキュリティ調査において、調査員は侵害の根本原因を特定し、インシデントに至るまでの一連の出来事を時系列で記録する任務を負います。調査員は、フォレンジックプロセスのどのステップが、悪用された脆弱性、攻撃時刻、攻撃者が行った具体的な行動など、一連の活動を明らかにするのに役立つかを判断する必要があります。この目標を達成するために
最も効果的な法医学技術は次のどれですか?
A. データの重複
B. 犯罪現場の撮影
C. データ分析
D. データ取得
正解: **C (**コメントを発表する**)**
According to the CHFI v11 Forensic Investigation Process and Event Correlation objectives , the forensic technique that enables investigators to reconstruct the sequence of events and determine the root cause of an incident is data analysis . Data analysis is the phase where collected evidence is examined, correlated, and interpreted to extract meaningful insights about attacker behavior.

During data analysis, investigators examine logs, timestamps, file system metadata, registry entries, network traffic, memory artifacts, and security alerts to perform timeline analysis , event correlation , and kill chain reconstruction . CHFI v11 explicitly highlights techniques such as timeline creation, event deconfliction, and correlation analysis as essential for identifying the time of attack , vulnerabilities exploited , methods used , and actions performed by the attacker .
The other options represent different forensic phases but do not directly achieve the stated goal. Data acquisition focuses on collecting evidence in a forensically sound manner, not interpreting it. Data duplication involves creating forensic copies to preserve evidence integrity. Photographing the crime scene applies primarily to physical forensics and documentation, not digital event reconstruction.
CHFI v11 emphasizes that without proper data analysis , raw evidence remains unstructured and cannot support attribution, root cause analysis, or legal prosecution. Therefore, to uncover the complete sequence of malicious activities and generate an accurate incident timeline, Data analysis is the most effective forensic technique.
Hence, the correct and CHFI-verified answer is Option C .

質問**: 164**
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**: C (**コメントを発表する**)**
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**: 165**
コンピュータフォレンジック調査官のライアンは、大企業内で機密データが不正に拡散された事件を担当することになった。容疑者の従業員は、全員がネットワーク接続ストレージ(NAS)デバイスにアクセスできるオフィスで勤務しており、NASは調査対象となった。NASはLinuxベースのファイルシステムを使用していた。最近のアップグレードにより、NAS上のデータが完全に消去され、復元された。さらに事態を複雑にしているのは、その企業がストレージエリアネットワーク(SAN)も使用しており、これも機密データ漏洩の別の原因である疑いがあることだ。NASとSANストレージシステムの特異性を理解した上で、ライアンが調査を開始するのに最適なアプローチは何だろうか？
A. ライアンは、データ復旧を試みる前に、NASおよびSANシステムのRAID構成(存在する場合)を再構築することを目指すべきです。
B. ライアンはまずSANに注力すべきです。なぜなら、SANは大規模なデータ漏洩の原因である可能性が高いからです。
C. Ryan は、NAS と SAN デバイスの両方の物理イメージを直ちに作成する必要があります。
D. Ryanは、一般的なWindowsベースの復元ツールを使用して、NASデバイスから削除されたファイルを復元する必要があります。
正解**: A (**コメントを発表する**)**
Option A is the best answer because NAS and SAN environments often rely on RAID-based storage architectures , and CHFI v11 explicitly includes RAID Storage System and RAID and Virtualization as important evidence-related storage topics. When investigating wiped, restored, or distributed storage, understanding the underlying RAID layout, disk order, parity scheme, and storage organization is critical before attempting meaningful recovery or deeper examination.
This is especially true here because the NAS uses a Linux-based filesystem and the SAN may also hold relevant evidence. Without first determining how the data is organized at the storage level, recovery attempts may be incomplete, misleading, or even damaging to the investigation workflow. That makes RAID reconstruction or storage-layout understanding the most logical starting point.

Option B assumes too much about which system matters more. Option C may become necessary later, but the question asks for the best approach to begin given the storage idiosyncrasies. Option D is too narrow and inappropriate for a Linux-based NAS environment. Therefore, the strongest CHFI-aligned starting point is to reconstruct the RAID configurations before attempting recovery .

質問**: 166**
テネシー州メンフィスの物流会社で発生した職場暴力事件の調査中、警備員が容疑者のバックパックを押収した。バックパックの中には、荷積み場の映像が録画されていると思われる小型デバイスが入っていた。この事例において、証拠の収集と取り扱いがISO/IECのガイドラインに準拠していることを確実にするため、証拠の取り扱いにおいて最も重視すべき状況はどれか？
A. デジタル静止画カメラおよびビデオカメラ(CCTVを含む)
B. 携帯電話、携帯情報端末(PDA)、個人用電子機器(PED)、およびメモリーカード
C. ネットワーク接続を備えた標準的なコンピュータ
D. TCP/IPおよびその他のデジタルプロトコルに基づくネットワーク
正解**: (**正解を表示します**)**
The correct answer is A because the device is believed to store recorded footage from the loading bay, which places the evidence source in the video-recording category rather than general mobile or computer categories.
CHFI v11 includes multimedia basics and evidence-source awareness, and ISO/IEC-aligned handling expects investigators to classify the device according to the kind of digital evidence it most directly contains. A compact recording device used to retain surveillance footage is most consistent with digital still and video camera style evidence, including CCTV-related material. The mobile-device option would be more appropriate if the question focused on a phone, tablet, or wearable used mainly for communications or app data. Standard computers and network categories do not fit the physical evidence source described. In forensic practice, the classification matters because imaging, access, storage media handling, and metadata expectations can differ depending on whether the examiner is dealing with video-recording equipment or another device class. Since the scenario centers on a compact device storing recorded footage from a surveillance area, the best-fitting category is digital still and video cameras including CCTV.

質問: **167**
テキサス州オースティンのデジタル出版会社で行われたフォレンジック監査において、調査員は復元された複数のファイルを16進エディタで分析した。ある断片のヘッダーには16進数シーケンス「50 4B 03 04 0A 00 02 00」が表示され、別の断片は「52 61 72 21 1A 07 00」で始まっている。これらの特徴に基づいて、最初の断片はどのファイル形式を表しているか？
A. ZIPファイル形式
B. RARファイル形式
C. CABファイル形式
D. JNTファイル形式
正解: **(**正解を表示します**)**
The correct answer is A because the header 50 4B 03 04 is the well-known magic number for a ZIP local file header. In forensic file analysis, CHFI v11 expects candidates to recognize common file signatures in hexadecimal form, since these headers help identify file types even when extensions are missing, altered, or intentionally disguised. The second sequence in the question, 52 61 72 21 1A 07 00, corresponds to a RAR archive signature, which further reinforces that the first fragment is the ZIP one. This kind of recognition is important when examining partial files, carved fragments, suspicious archives, or extension mismatches. ZIP containers are also widely used as the basis for many other formats such as DOCX, XLSX, JAR, and APK, but the raw signature itself still identifies the underlying ZIP structure. In CHFI-style reasoning, when a question gives multiple magic numbers and asks specifically about the first fragment, the correct approach is to map the exact header bytes to the associated archive format. Here, 50 4B 03 04 identifies a ZIP file format.

質問: **168**
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: **(**正解を表示します**)**
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: **169**
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: **B (**コメントを発表する**)**
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**: 170**
国境を越えたサイバー犯罪を捜査しているパテル刑事は、管轄の違いと攻撃の遠隔地での性質により、証拠収集の課題に直面している。
国境を越えたサイバー犯罪に関して、パテル刑事が起訴のための証拠収集で直面する主な課題は何ですか?
A. 管轄区域全体にわたるデジタル証拠に関する多様な法的枠組みを理解します。
B. 国境を越えて遠隔地の攻撃者を追跡するために物理的な監視を実行します。
C. 国際的な襲撃を同時に調整します。
D. 安全なデータ転送のために高度な暗号化を使用します。
正解**: (**正解を表示します**)**
This scenario aligns with CHFI v11 objectives under Computer Forensics Fundamentals and Legal Issues and Compliance in Digital Forensics . Cross-border cybercrime investigations are inherently complex because digital evidence is often stored, transmitted, or processed across multiple countries, each governed by its own legal system. CHFI v11 emphasizes that one of the most significant challenges investigators face in such cases is navigating diverse legal frameworks and jurisdictional requirements .
Different countries have varying laws related to data privacy, evidence seizure, admissibility, retention, and disclosure. Investigators must often rely on international cooperation mechanisms such as Mutual Legal Assistance Treaties (MLATs), letters rogatory, or coordination with international law enforcement agencies.
These processes can be time-consuming and may delay evidence acquisition, risking data loss due to retention limits imposed by service providers.
The other options do not reflect primary forensic challenges. Physical surveillance and coordinated raids are operational law enforcement activities, not core digital evidence issues, and encryption is a technical safeguard rather than a legal obstacle. CHFI v11 highlights that understanding and complying with international legal requirements is critical to ensuring evidence is lawfully obtained and admissible in court.

Therefore, navigating diverse legal frameworks across jurisdictions is the primary challenge in cross-border cybercrime investigations.

質問: **171**
調査中に、調査員が拡張子.xlsmのExcelファイルを開きました。これは、その文書に悪意のあるコードが含まれている可能性があることを示しています。さらに詳しく調べた結果、調査員はファイルが脅威となるかどうかを判断する必要があります。潜在的なリスクを特定するために、調査員はどのような点に注目すべきでしょうか？
A. ファイル内のストリームにマクロが含まれているかどうかを確認します。
B. ドキュメントにリンクやネットワーク呼び出しなどの外部リソースが埋め込まれているかどうか、ファイルを検査します。
C. ファイルサイズが異常に大きいか小さいかを確認してください。これは隠しデータが存在する可能性を示しています。
D. ファイルのメタデータを調べて、作成者、作成日、最終更新日などの詳細を確認します。
正解: **(正解を表示します)**
Option A is the best answer because the .xlsm extension specifically indicates a macro-enabled Excel document . In malware forensics, the most direct indicator of risk in such a file is the presence of macro- containing streams or embedded VBA content . When investigators suspect a malicious Office document, they first determine whether executable macro content exists, because that is often the primary mechanism used to deliver or launch malicious behavior.
While external links, metadata, and unusual size can all be useful supporting indicators, they are not as central to the threat profile of an XLSM file as macro content is. The extension itself points the examiner toward macro analysis as the most relevant first focus. If macros are present, they can be reviewed for suspicious functions, obfuscation, PowerShell or shell commands, downloader behavior, and other signs of malicious intent. Therefore, from a CHFI-style malware-document analysis perspective, the investigator should first focus on whether the file contains macro-related streams , because that is the clearest and most direct source of malicious functionality in a macro-enabled Excel document.

質問: **172**
カリフォルニア州サンディエゴにあるバイオテクノロジー系スタートアップ企業で発生した侵入事件の調査において、アナリストはLinuxウェブサーバーのアプリケーションログとシェルログを精査しました。その結果、先行するコマンドがゼロ以外の終了ステータスで失敗した場合にのみ、2番目のコマンドが実行されるというパターンが確認されました。この終了ステータスは、アプリケーションがシステムシェルに転送したユーザー入力の中に現れています。攻撃者が使用したコマンド連鎖メカニズムを確認するために、調査担当者はログに記録された入力の中でどの演算子を探すべきでしょうか？
A. Logical operator: ||

B. Logical operator: & &
C. List Terminator: ;
D. Pipe Operator: |
正解**: (**正解を表示します**)**
The correct answer is A because in shell command chaining, the operator double pipe executes the second command only if the first command fails and returns a non-zero exit status. That behavior matches the question exactly. By contrast, double ampersand runs the second command only if the first succeeds, the semicolon simply separates commands without making execution conditional on success or failure, and the pipe passes output from one command to another rather than expressing failure-based logic. CHFI v11 includes command injection and web-application attack investigation, so candidates are expected to understand how attacker-supplied shell operators can change execution flow and help reveal intent in log analysis. In a forensic context, identifying the specific operator used in user-controlled input can help analysts determine whether the attacker was attempting fallback execution, probing, or chaining commands based on server behavior. Since the evidence shows the second command ran only when the first one failed, the operator investigators should look for is the logical OR operator double pipe.

質問**: 173**
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**: 174**
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**: (**正解を表示します**)**
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**: 175**
システム管理者のアレックスは、Linuxマシン上の既存のEXT2ファイルシステムをEXT3ファイルシステムに変換するという任務を負っています。EXT2ファイルシステムは現在使用されており、アレックスはこれをEXT3に変換するためジャーナリングを有効にする必要があります。この変換を行うには、アレックスは以下のどのコマンドを使用すべきでしょうか？
A. C:>ECHO text_message > myfile.txt:stream1
B. C:>MORE < myfile.txt:stream1
C. dd if=mbr.backup of=/dev/xxx bs=512 count=1
D. # /sbin/tune2fs -j
正解**: (**正解を表示します**)**
According to the CHFI v11 syllabus under Operating System Forensics and Linux File System Analysis , understanding Linux file systems and their conversion methods is essential for both system administration and forensic investigations. The EXT2 file system is a non-journaling file system, whereas EXT3 extends EXT2 by adding journaling capabilities , which significantly improve system recovery and forensic traceability after crashes or improper shutdowns.
The correct command to convert an existing EXT2 file system into EXT3 is:
/sbin/tune2fs -j
This command enables journaling on the EXT2 file system without reformatting or destroying existing data , making it a safe and efficient conversion method. CHFI v11 explicitly highlights this command as the standard approach for adding a journal to an EXT2 partition. Once journaling is enabled, the file system is recognized as EXT3.
The other options are incorrect and unrelated to Linux file system conversion. Options A and B involve NTFS Alternate Data Streams , which are Windows-specific. Option C is a disk-level command used for copying raw sectors, such as backing up or restoring an MBR, and does not modify file system journaling features.
The CHFI Exam Blueprint v4 emphasizes knowledge of Linux file systems (EXT2, EXT3, EXT4) and administrative commands like tune2fs , as they are frequently referenced in forensic analysis and recovery scenarios, making Option D the correct and exam-aligned answer

質問**: 176**

組織がチャットログ、アプリケーションデータ、電子メールなどのデジタル記録を司法手続きで使用するために準備する場合、eDiscoveryプロセスは電子的に保存された情報をどのように処理するのでしょうか？
A. デジタルイベントを関連付けて攻撃のシーケンスを再構築する
B. 電子的に保存された情報が法廷で証拠として認められることを保証する。
C. 電子的に保存された情報の発見、保護、収集、レビュー、および提示
D. 封じ込めと復旧を通じてセキュリティインシデントを特定し、対応する
正解: **(**正解を表示します**)**
The best answer is C because CHFI v11 treats eDiscovery as a structured process for handling electronically stored information across its full legal lifecycle, not as a single technical activity. The blueprint specifically includes the eDiscovery process flow, the Electronic Discovery Reference Model cycle, collection methodologies, and best practices for controlling cost and risk. That directly supports the idea that organizations must discover relevant data, preserve and protect it, collect it in a defensible way, review it for relevance, and then present it for legal or regulatory use. Option B sounds partially correct, but admissibility is an outcome supported by proper handling rather than the full definition of the process. Option A is event correlation, which belongs more to forensic analysis and timeline reconstruction. Option D describes incident response activities rather than eDiscovery. In exam terms, whenever the question focuses on preparing emails, chats, application records, and other business data for judicial proceedings, CHFI expects you to think in terms of the EDRM-style workflow. That makes option C the only complete answer aligned with the blueprint objective.

質問: **177**
カリフォルニア州サンディエゴのメディアサイトでデータベースエラーが多発し、処理時間が長くなった際、ユーザーはURLを追加した入力に関連するブラウザ内ポップアップが表示されると報告しました。調査担当者はApacheのアクセスログに着目し、ペイロードの内容とこれらの急増したリクエストを比較するために、正確なリクエスト行を示すフィールドを必要としています。メソッド、クエリ文字列を含むパス、およびプロトコルを、結合ログ形式と共通ログ形式で取得するApacheログディレクティブはどれでしょうか？
A. %r
B. %{Refer}i
C. %h
D. %u
正解: **(**正解を表示します**)**
The correct answer is A because Apache uses the %r directive to log the full request line exactly as sent by the client. Apache's official logging documentation explains that the request line includes the method, the requested resource, and the protocol version, which is precisely what investigators need when reviewing suspicious URL-appended input. In practical forensic terms, this field helps analysts compare the attacker's submitted payload

with corresponding spikes in application errors or timing anomalies. %{Referer}i records the HTTP Referer header, %h logs the client host, and %u records the authenticated remote user, so none of those captures the full request line. CHFI v11 includes Apache access and error logs, web-application attack investigation, and analysis of log evidence, so recognizing what each directive represents is directly within scope. When the objective is to recover the exact request syntax used in a possible injection or cross-site scripting attempt, the request-line directive is the most valuable field. Therefore, the correct Apache log directive is %r.

質問: **178**
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: **179**
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**: 180**
マサチューセッツ州ボストンで行われた金融捜査において、フォレンジックアナリストが容疑者のハードドライブを複製した。複製されたイメージがオリジナルと完全に一致することを確認するために、アナリストはどの検証方法を用いるべきか？
A. MD5やSHA-256などの暗号学的ハッシュ値を計算します。
B. 画像ファイルのサイズを小さくするために圧縮を適用します
C. 取得したドライブのRAID再構築を実行する
D. 対象メディアでデータサニタイズを実行する
正解: **(**正解を表示します**)**

The correct answer is A because hashing is the standard validation method used to confirm that a forensic image exactly matches the original source. CHFI v11 includes data acquisition validation tools and emphasizes validating acquired evidence as part of sound forensic methodology. By calculating cryptographic hash values such as MD5 or SHA-256 on both the original media and the acquired duplicate, the examiner can demonstrate that the contents are identical at the time of acquisition. This is one of the most important ways to support evidentiary integrity and courtroom defensibility. Compression does not validate equivalence, RAID reconstruction is unrelated unless the source itself is a RAID system requiring assembly, and data sanitization applies to preparing media, not proving a copied image is exact. In forensic practice, the duplicate is trusted only when a validation process confirms there has been no alteration during acquisition or storage.
Since the question asks for the method that proves the duplicate image is an exact copy, the correct answer is computing cryptographic hash values such as MD5 or SHA-256.

質問**: 181**
複雑な捜査に関わる複数のIoTデバイスからデータを抽出する任務を、法医学捜査官が任されました。これらのデバイスには、事件の解決に不可欠なドローン、スマートテレビ、ウェアラブル端末などが含まれます。これらのデバイスには、ビデオ映像、センサーデータ、ユーザー操作など、貴重な証拠が含まれている可能性があります。捜査官は、さまざまなIoTデバイスに対応し、物理的および論理的な抽出方法の両方をサポートすることで、証拠の見落としを防ぐツールを必要としています。IoTフォレンジックの複雑さを考慮すると、捜査官はこれらのデバイスから効果的に証拠を収集するために、次のうちどのツールを使用すべきでしょうか？
A. 貨物
B. Promqry
C. ゲフィ
D. MD-NEXT
正解**: (**正解を表示します**)**
Option D. MD-NEXT is the best answer because the question is specifically about a forensic tool suitable for collecting evidence from multiple IoT device types while supporting broad extraction needs. CHFI v11 includes IoT forensics , evidence extraction from embedded and smart devices , and understanding the methods used to acquire and analyze data from nontraditional digital systems. In that context, the correct choice is the tool that is actually designed for device-level forensic extraction rather than one intended for unrelated analytical or cloud-focused purposes.
The other options are less appropriate. Freta is associated with cloud-scale memory analysis concepts rather than hands-on IoT extraction. Gephi is a graph visualization and network-analysis tool, not a forensic acquisition platform. Promqry is not the established choice for this type of physical and logical evidence extraction scenario. MD-NEXT , by

contrast, fits the role of a specialized forensic solution for handling diverse devices and collecting evidence in a structured manner.
Because the scenario emphasizes variety of IoT devices , forensic extraction , and the need not to miss evidence, the most suitable CHFI-aligned answer is MD-NEXT .

質問: **182**
企業調査の一環として、フォレンジック調査員のメリッサは、容疑者のノートパソコンのウェブブラウザの履歴、Cookie、キャッシュを調査するよう依頼されました。ノートパソコンには、Google Chrome、Firefox、Safariなど、複数のウェブブラウザがインストールされています。メリッサは、複数のウェブブラウザからこれらのデジタルアーティファクトを包括的に抽出・分析できるツールを必要としています。彼女はどのツールを使用すべきでしょうか？
A. ネットアナリシス
B. 探偵キット
C. ケース化
D. ディスクエクスプローラー
正解: **(**正解を表示します**)**
Option A. NetAnalysis is the best answer because the question is specifically about extracting and analyzing browser history, cookies, and cache across multiple web browsers . CHFI v11 explicitly includes Tools to Examine the Cache, Cookie, and History Recorded in Web Browsers and Private Browsing and Browser Artifact Recovery under its tool-based operating-system and artifact analysis objectives.
A dedicated browser-artifact tool is the most appropriate choice when the focus is on cross-browser internet activity reconstruction. NetAnalysis is designed for that kind of work and is far more targeted than the other options for analyzing Chrome, Firefox, Safari, and similar browser traces in one workflow.
Sleuth Kit is excellent for file system analysis, but it is not the most direct answer for comprehensive browser- artifact examination. EnCase is a broad forensic suite, but the question asks for the tool best suited specifically for browser history, cookies, and cache. DiskExplorer is not the strongest fit for this requirement.

Therefore, based on CHFI's browser-artifact tool objectives, NetAnalysis is the most precise and appropriate answer.

質問: **183**
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: **184**

法医学捜査官のマークは、悪意のある活動の兆候がないか、疑わしい実行可能ファイルを調査しています。彼は、URL、ファイルパス、レジストリキーなど、ファイルの悪意のある動作を示す可能性のある埋め込み文字列をファイルから検索する必要があります。マークは、実行可能ファイルから文字列を抽出してさらに分析するために、次のうちどのツールを使用できますか？
A. バイナリテキスト
B. PEエクスプローラー
C. HashMyFiles
D. 依存性ウォーカー
正解: **A** (コメントを発表する)
Option A. BinText is the correct answer because the task is specifically to extract embedded strings from an executable file. In malware analysis, strings such as URLs, domain names, file paths, mutex names, registry keys, command fragments, or suspicious messages can provide valuable clues about the malware's functionality without requiring immediate execution. A string-extraction tool is therefore one of the most useful early triage methods.
BinText is designed for exactly this purpose. It scans binaries and extracts readable strings that may indicate malicious intent or reveal indicators of compromise. This makes it far more suitable than the other options for the specific requirement stated in the question.
PE Explorer is more focused on inspecting PE file structure and metadata. HashMyFiles generates hashes for integrity and identification, not embedded-string extraction. Dependency Walker helps analyze imported libraries and dependencies, which can also be useful, but it does not directly serve the same role as a strings tool. Therefore, for a CHFI-style first-pass review of a suspicious executable to uncover embedded text artifacts, BinText is the most appropriate choice.

質問: **185**
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**: 186**
サイバー犯罪捜査において、捜査官はハッキング活動の証拠を探すために容疑者のコンピュータシステムを捜索するための令状を取得します。容疑者の電子機器からデータを収集する際に、システムに接続している他のユーザーの身元を明らかにする情報に意図せずアクセスしてしまうことがあります。
サイバー犯罪捜査プロセスのどのステップでプライバシーの問題に関する懸念が生じますか?
A. ネットワークセキュリティ対策の実装
B. 法医学的分析の実施
C. 他のユーザーの匿名性を維持する
D. 捜索令状の取得
正解**: (**正解を表示します**)**
According to the CHFI v11 Regulations, Policies, and Ethics domain, privacy issues most commonly arise during the forensic analysis phase of a cybercrime investigation. While search warrants legally authorize investigators to collect and examine specific digital evidence, they are typically scope-limited to the suspect, systems, data types, and timeframes defined in the warrant.
During forensic analysis , investigators may inadvertently encounter personal or sensitive information belonging to third parties , such as usernames, email addresses, chat records, credentials, or identifiers of other users connected to the system. CHFI v11 explicitly highlights this phase as legally and ethically sensitive because analysts must ensure that non-relevant data and third-party information are handled carefully to avoid violations of privacy laws and data protection regulations.
Implementing network security measures is a preventive activity, not an investigative one. Obtaining search warrants is a legal safeguard designed to protect privacy, not create privacy concerns. Preserving anonymity is a mitigation action, not the step that introduces the risk.

CHFI v11 stresses the importance of minimization, access control, proper documentation, and legal oversight during forensic analysis to prevent misuse or overexposure of unrelated personal data. Failure to manage privacy during this phase can result in legal challenges, evidence exclusion, or regulatory violations.
Therefore, the step that raises privacy-related concerns in this scenario is conducting forensic analysis , making Option B the correct and CHFI v11-verified answer.

質問**: 187**
コンピューターフォレンジックセミナーにおいて、ミラー捜査官は急速な技術進歩に伴う法的複雑さについて懸念を表明しました。彼は、効果的な捜査のためには、新しい技術への継続的な適応が重要であると強調しました。理解度を測るため、彼は以下のシナリオを提示しました。
スミス捜査官は、容疑者のハードドライブに保存されていた暗号化されたデータに遭遇しました。復号の合法性が不明なため、スミス捜査官はどうすればよいのでしょうか？
A. 法的問題を回避するために、他の証拠に焦点を当てます。
B. 復号化の合法性に関する法的助言を得る。
C. 法的な相談なしに、捜査判断に基づいてデータを復号化する。
D. 暗号化が疑わしいため、オンライン ツールを使用してデータを復号化します。
正解**: (**正解を表示します**)**
Under CHFI v11 Computer Forensics Fundamentals , investigators are required to operate within strict legal and ethical boundaries , especially when dealing with sensitive actions such as decrypting protected data . Encryption itself is not illegal, and encrypted data may contain both incriminating evidence and protected personal or third-party information . Therefore, improper or unauthorized decryption can lead to legal violations , evidence suppression, or civil liability.
CHFI v11 emphasizes that when investigators encounter legal ambiguity , particularly with encryption, passwords, or access controls, the correct course of action is to seek legal guidance . This may involve consulting legal counsel, prosecutors, or obtaining additional warrants or court orders that explicitly authorize decryption or compel key disclosure. This ensures that the investigation remains compliant with applicable laws, privacy protections, and due process requirements.
The other options are not aligned with CHFI principles. Avoiding the evidence altogether may compromise the investigation. Decrypting data without legal consultation-or using online tools-can violate laws related to unauthorized access, privacy, and evidence handling , potentially rendering the evidence inadmissible in court.
CHFI v11 consistently reinforces that legal oversight is a cornerstone of defensible digital investigations , particularly as encryption becomes more prevalent. Therefore, the correct and professionally responsible action is to obtain legal advice regarding the legality of decryption , making Option B the correct answer.

質問: **188**
小売テクノロジー企業におけるインシデント後の調査において、フォレンジックアナリストは、複数のAWSアカウントにわたるクラウド リソースへの不正な変更のタイムラインを再構築する必要があります。この調査では、コントロール プレーンのアクティビティを可視化し、アナリストが特定のIDにアクションを関連付け、構成変更がどのように開始され、環境全体に伝播されたかを理解できるようにする必要があります。調査担当者は、タイムラインの再構築を支援するために、アカウント全体の管理アクティビティの記録をどのように取得すべきでしょうか？
A. Amazon S3サーバーアクセスログ
B. AWS CLI
C. Amazon CloudWatch
D. AWS CloudTrail
正解: **(正解を表示します)**
The correct answer is D because AWS CloudTrail is the AWS service that records management activity across an account, including actions taken through the AWS Management Console, CLI, SDKs, and APIs.
AWS documentation explains that CloudTrail provides a history of account activity and captures management events, which is exactly what investigators need when reconstructing who changed cloud resources, when those changes occurred, and how they were initiated. That makes it the key source for control-plane timeline analysis. Amazon S3 Server Access Logging is limited to S3 request logging and does not provide broad account-wide management visibility. The AWS CLI is a tool for interacting with AWS, not the forensic record itself. Amazon CloudWatch can collect metrics and logs, but the question specifically asks for the authoritative account-wide record of management actions. CHFI v11 includes cloud forensics and AWS evidence sources, so candidates are expected to distinguish platform activity logs from service-specific or tooling components. For unauthorized modifications across AWS accounts, CloudTrail is the primary source for identity-linked management event reconstruction.

質問: **189**
多面的なサイバーセキュリティ運用において、アナリストはJuniper、Check Point、Snortといった最先端の侵入検知システム(IDS)ツール群を導入し、ログを綿密に精査します。ネットワークイベントに関する複雑なデータが詰まったこれらのログは、防御の要として機能し、アナリストが膨大な情報の中から微細な異常を見抜くことを可能にします。
サイバーセキュリティ防御の迷宮の中で、侵入検知システム (IDS) は、イベントの監視と分析の役割に加えて、主にどのような多面的な機能を担っているのでしょうか。
A. 進化する脅威に対抗するために、攻撃シグネチャを反復的に改良します。
B. 電子メール、ページ、SNMP トラップなど、さまざまなチャネルを通じてセキュリティ管理者に警告を発します。

C. 監視対象のイベントから得られた微妙な洞察をまとめた包括的なグラフィカル レポートを合成します。
D. 分散ログ インフラストラクチャへのデータのシームレスな転送をオーケストレーションします。
正解: **(**正解を表示します**)**
This question aligns with CHFI v11 objectives under Network and Web Attacks , specifically the role and functionality of Intrusion Detection Systems (IDS) in network security monitoring and incident response.
CHFI v11 emphasizes that IDS solutions such as Snort, Juniper IDS, and Check Point are designed not only to monitor and analyze network traffic but also to actively alert security personnel when suspicious or malicious activity is detected .
An IDS continuously inspects packets, sessions, and events against predefined signatures, behavioral models, or anomaly thresholds. When a potential intrusion, policy violation, or attack pattern is identified, the system' s primary operational response is to generate real-time alerts . These alerts are delivered through multiple channels-such as email notifications, pager alerts, dashboards, syslog messages, and SNMP traps -to ensure timely awareness and rapid response by security administrators.
While IDS platforms may support reporting, log forwarding, or signature updates, these are secondary or supporting capabilities. The critical value of IDS in a forensic and operational context lies in its ability to promptly notify defenders of threats as they occur or are detected. Therefore, consistent with CHFI v11 IDS principles, the correct answer is vigilantly alerting security administrators via multiple notification channels .