WGU.Digital-Forensics-in-Cybersecurity.v2025-08-04.q28

試験コード:	Digital-Forensics-in-Cybersecurity
試験名称:	Digital Forensics in Cybersecurity (D431/C840) Course Exam
認定資格:	WGU
無料問題数:	28
バージョン:	v2025-08-04
アクセス数:	430
ページビュー数:	280
https://www.jpnpdf.com/WGU.Digital-Forensics-in-Cybersecurity.v2025-08-04.q28-mondaishu.html	

最新問題: **1**
米国のどの法律が、ジャーナリストが自分の仕事や情報源を、それが一般公開される前に法執行機関に引き渡すことを保護しているのでしょうか?
A. プライバシー保護法（PPA）
B. 医療保険の携行性と責任に関する法律（HIPAA）
C. 電子通信プライバシー法（ECPA）
D. 法執行機関への通信支援法 (CALEA)
Answer: A (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
プライバシー保護法（PPA）は、一定の例外が適用される場合を除き、法執行機関による公開を目的とした資料の捜索または押収を制限することで、ジャーナリストを保護します。また、ジャーナリズムの情報源や未発表の著作物を、政府による不当な介入から保護します。
* PPA は報道の自由を保証し、機密情報を保護します。
* 法執行機関は、ジャーナリズムの資料にアクセスする前に手続き上の保護措置を遵守する必要があります。
参考: 法文書およびデジタルフォレンジックガイドラインでは、調査の必要性と報道の自由のバランスをとる上での PPA の役割について言及されています。

最新問題: **2**
デジタル証拠をコピーするどの方法が適切な証拠収集を保証しますか?
A. ファイルレベルのコピー
B. ビットレベルのコピー
C. クラウドバックアップ

D. 暗号化された転送
Answer: B (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ビットレベル（ビットストリーム）コピーは、元のメディアのセクタ単位の正確な複製を作成し、すべてのファイル、削除されたデータ、および空き領域をキャプチャします。この方法は、デジタル証拠全体を変更せずに保存するために不可欠です。
* ビットレベルのイメージングにより、法医学的健全性が維持されます。
* 調査員は元のデータを変更せずに分析を実行できます。
参考: NIST SP 800-86 およびデジタルフォレンジックのベストプラクティスでは、証拠取得のためのビットレベルのコピーが重視されています。

最新問題**: 3**
モバイル デバイスからデータが抽出されるときにそのデバイスが取り得る 4 つの状態を列挙している法律またはガイドラインはどれですか。
A. 医療保険の携行性と責任に関する法律（HIPAA）
B. NIST SP 800-72 ガイドライン
C. 電子通信プライバシー法（ECPA）
D. 法執行機関への通信支援法 (CALEA)
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
NIST特別刊行物800-72は、モバイルデバイスのフォレンジックに関するガイドラインを提供し、データ抽出時のデバイスの状態をアクティブ、アイドル、電源オフ、ロックの4つに分類しています。これらの状態は、データへのアクセス方法と保存方法に影響を与えます。
* これらの状態を理解することは、法医学調査官が適切な取得手法を選択するのに役立ちます。
* NIST SP 800-72 は、モバイル デバイスのフォレンジック手法に関する重要なリファレンスです。
参考:NIST SP 800-72 は、フォレンジック調査におけるモバイル デバイス データの取り扱いに関する正式なガイドラインを提供します。

最新問題**: 4**
法医学調査員は、アップデートによって Mac OS X コンピュータにスパイウェアがインストールされたと疑っています。
システムとソフトウェアのアップデートに関する情報は、Mac OS X のどのログまたはフォルダに保存されますか?
A. /var/spool/cups
B. /var/log/daily.out
C. /var/vm
D. /ライブラリ/領収書
Answer: D (メーッセージを残す**)**

正確な抜粋からの包括的かつ詳細な説明：
Mac OS Xの/ライブラリ/Receiptsフォルダには、システムやアプリケーションのアップデートを含むソフトウェアのインストールとアップデートを追跡するレシートが保存されています。このフォルダは、フォレンジック調査員がどのアップデートがいつインストールされたかを特定する際に役立ち、スパイウェアなどの疑わしいソフトウェアや不正なソフトウェアのインストールを検出するのに役立ちます。
* /var/spool/cupsis はプリンタのスプールに関連しています。
* /var/log/daily.out には毎日のシステム ログの概要が含まれますが、詳細な更新記録は含まれません。
* /var/vmには仮想メモリファイルが含まれています。
NIST および Apple のフォレンジック ドキュメントによると、/Library/Receipt はソフトウェアのインストール履歴を調べるための重要な場所となっています。

最新問題: **5**
小規模会計事務所の人事部長は、フィッシング詐欺の被害に遭った可能性があると考えています。彼は、会社のオンライン銀行口座へのログイン情報の確認を求めるメール内のリンクをクリックしました。
この事件を調査するために、法医学調査官はどのようなデジタル証拠を収集する必要がありますか?
A. メールヘッダー
B. ブラウザキャッシュ
C. システムログ
D. ネットワークトラフィックログ
Answer: B (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ブラウザキャッシュには、最近アクセスしたウェブページ、画像、Cookieが保存されます。これには、フィッシングサイトのコンテンツや関連アクティビティが含まれる場合があります。フィッシング攻撃を分析する調査員は、ブラウザキャッシュデータを収集し、被害者のウェブアクティビティを再構築して悪意のあるサイトを検出します。
* キャッシュされた Web ページは、被害者の証言を裏付け、タイムラインを確立するのに役立ちます。
* ブラウザの履歴とキャッシュは揮発性なので、すぐに保存する必要があります。
参考: NIST SP 800-101 およびフォレンジック ガイドによると、フィッシングや Web ベースの攻撃の調査にはブラウザ キャッシュが重要です。

最新問題: **6**
ある組織は、ステガノグラフィによるデータ漏洩を防止しようと決意しています。すべての送信データが必ず通過するワークフローを開発しました。このワークフローの一部として、隠蔽されたデータをチェックするツールを導入する予定です。

ステガノグラフィで隠されたデータの存在を確認するにはどのツールを使用すればよいですか?
A. データドクター
B. フォレンジックツールキット（FTK）
C. 雪
D. MP3ステゴ
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
Snowは、テキストファイルやその他の媒体内の空白文字にエンコードされた隠蔽データを検出・抽出する、特殊なステガナリシスツールです。ホワイトスペース・ステガノグラフィなどの隠蔽データ検出のため、デジタルフォレンジック調査において広く利用されています。
* Data Doctor は、ステガナリシスに特化したものではなく、一般的なデータ復旧ツールです。
* FTK は一般的なフォレンジック スイートであり、ステガノグラフィ検出用に特別に設計されたものではありません。
* MP3Stego はオーディオ ステガノグラフィーに重点を置いています。
NIST およびデジタルフォレンジックの文献では、テキストや同様の媒体に隠されたデータを検出するように設計されたワークフローにおいて、Snow が貴重なツールであると認識されています。

最新問題**: 7**
iOS オペレーティング システムを実行している Apple iPhone のパスコードをバイパスするために使用できるフォレンジック ツールはどれですか?
A. iStumbler
B. オフラック
C. LOphtCrack
D. XRY
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
XRYは、Apple iPhoneを含むモバイルデバイスからデータを抽出するために特別に設計された商用フォレンジックツールです。特定の条件下でiOSパスコードをバイパスまたは回避し、フォレンジック分析用のデータを取得する機能を備えています。
* iStumbler は Wi-Fi スキャン ツールです。
* Ophcrack および LOphtCrack は、モバイル デバイスではなく、Windows システム用のパスワード クラッキング ツールです。
XRY は、iOS データ抽出の主要ツールとして、デジタル フォレンジック トレーニングや NIST モバイル デバイス フォレンジック ガイドラインで広く参照されています。

最新問題**: 8**

トムは、最下位ビット (LSB) 方式を使用してメッセージをサウンド ファイルに保存し、このサウンドを自分の Web サイトにアップロードしました。
この例ではキャリアは何ですか?
A. 最下位ビット方式
B. トムのウェブサイト
C. サウンドファイル
D. メッセージ
Answer: C (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ステガノグラフィーにおいて、キャリアとは秘密メッセージを隠すために用いられるファイルまたは媒体のことです。この例では、音声ファイルがキャリアにあたります。これは、音声ファイルには最下位ビット方式で埋め込まれた秘密メッセージが含まれているためです。メッセージはペイロードであり、ウェブサイトは単なる配信プラットフォームです。
* LSB はキャリアではなく埋め込み技術です。
* メッセージはキャリアではなくペイロードです。
※当ウェブサイトはデータの隠蔽には関与しておりません。
NIST およびステガノグラフィのリファレンスでは、キャリアは隠されたデータを保持するコンテナであると明確に定義されています。

最新問題**: 9**
ソリッド ステート ドライブ (SSD) と比較して、磁気ドライブにはどのような特性がありますか?
A. コストが高い
B. コストが低い
C. ダメージを受けにくい
D. 読み取り/書き込み速度が高速化
Answer: B (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
磁気ハードドライブは、一般的に、ソリッドステートドライブ (SSD) に比べて、ギガバイトあたりのコストが低くなります。
ただし、機械的な損傷を受けやすく、データアクセスが遅くなります。
* SSD には可動部品がなく、耐久性と速度に優れていますが、価格は高くなります。
* 法医学の専門家は証拠収集の際にこれらの違いを考慮します。
参考: デジタルフォレンジックのテキストやハードウェアの概要では、磁気ドライブはコスト効率に優れているが、SSD に比べて壊れやすいと説明されています。

最新問題**: 10**
サイバー犯罪者が、ある企業の最高経営責任者（CEO）所有のApple iPadをハッキングしました。サイバー犯罪者は、データボリューム上の重要なファイルをいくつか削除しており、これらのファイルは回復が必要です。

どの隠しフォルダにデジタル証拠が含まれますか?
A. /プライベート/その他
B. /紛失+拾得
C. /.Trashes/501
D. /etc
Answer: C (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
Apple iOSデバイスでは、削除されたファイルは完全に削除される前に、隠しゴミ箱フォルダに移動されることがよくあります。ディレクトリ/.Trashes/501は、ユーザーID501（macOSで最初に作成されたユーザー）の削除されたファイルが保存される隠しフォルダです。
/iOSデバイスなどのデータが一時的に保存されます。
* このフォルダには削除対象としてマークされたファイルが含まれている可能性があるため、回復を試みるための最適な場所です。
* /lost+found は、ファイル システムが破損した後に復元されたファイル フラグメントを格納するために Unix/Linux ファイル システムでよく使用されるディレクトリですが、iOS のデフォルトのゴミ箱の場所ではありません。
* /Private/etc および /etc には、削除されたユーザー ファイルではなく、システム構成ファイルが含まれます。
参考: NIST による Apple のフォレンジック調査や、Cellebrite や BlackBag Technologies などのトレーニングマニュアルによると、iOS デバイス上でユーザーが削除したファイルは、完全に削除されるまで、.Trashes または同様の隠しディレクトリに保存されます。

最新問題**: 11**
必要に応じてメモリからハードドライブに情報を一時的に保存するためにスワップ ファイルを作成するオペレーティング システムはどれですか。
A. Linux
B. マック
C. Unix
D. ウィンドウ
Answer: D (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
Windowsは、物理メモリ（RAM）の容量が不足している場合、スワップファイル（一般的にpagefile.sysと呼ばれます）を使用して、メモリからディスクにデータを一時的に保存することでRAMを拡張します。これにより、システムは利用可能なRAMよりも多くのデータを処理できるようになります。
* Linux と Unix では通常、専用のスワップ パーティションまたはスワップ ファイルが使用されますが、それらの参照方法や管理方法は異なります。
* Mac OS X はページング ファイル システムを使用しますが、通常は Windows の意味での「スワップ ファイル」は使用せず、代わりに動的ページング ファイルを使用します。

* 「スワップ ファイル」という用語は、一般的に Windows に関連付けられます。
参考: Microsoft Windows フォレンジック ガイドラインと NIST ドキュメントでは、Windows オペレーティング システムの仮想メモリ管理におけるページ ファイルの役割について説明しています。

最新問題: **12**
法医学者がサイバー犯罪の証拠となる可能性のあるコンピューターを調べています。フォレンジック科学者がコンピューターからフォレンジック コンピューターにファイルをコピーするときに、OS レベルではなくビット レベルでファイルをコピーする必要があるのはなぜですか?
A. OS レベルでのファイルのコピーでは、削除されたファイルや空き領域のコピーに失敗します。
B. OS レベルでのファイルのコピーは時間がかかりすぎるため、実用的ではありません。
C. OS レベルでファイルをコピーすると、ファイルのタイムスタンプが変更されます。
D. OS レベルでファイルをコピーすると、不要な余分な情報がコピーされます。
Answer: A (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ビットレベル（またはビットストリーム）コピーは、ファイル、削除されたファイル、スラックスペース（クラスター内の未使用領域）、未割り当て領域など、ストレージメディア上のあらゆるビットをキャプチャします。これにより、OSレベルでは確認できないアーティファクトを含むすべてのデジタル証拠が分析のために保存されます。
* OS レベルでのコピーでは、ファイル システムで表示される割り当て済みファイル、失われた削除済みファイル、および空き領域のみがキャプチャされます。
* ビットレベルのコピーは、NIST SP 800-86 および SWGDE ガイドラインで指定されているフォレンジックのベストプラクティスの基礎です。
* タイムスタンプの変更や不要な情報の問題は、証拠の完全性に比べれば二次的な懸念事項です。

最新問題: **13**
法医学者は、犯罪現場から Windows PC を押収する前に、どのようにしてネットワーク構成を取得すればよいでしょうか?
A. システムプロパティを確認することで
B. コンピュータのコマンドプロンプトからipconfigコマンドを使用する
C. ネットワークと共有センターを開く
D. コンピュータをセーフモードで再起動する
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
Windowsのコマンドプロンプトでipconfigコマンドを実行すると、IPアドレス、サブネットマスク、デフォルトゲートウェイなどの詳細なネットワーク構成情報が表示されます。押収前にこれらの情報を収集することで、捜査に関連する揮発性証拠を保全できます。

* ネットワーク設定を文書化しておくと、押収時の被疑システムの接続状況を把握しやすくなります。
* NIST は、疑わしいマシンをシャットダウンまたは切断する前に、揮発性データ (ネットワーク構成を含む) をキャプチャすることを推奨しています。
参考: NIST SP 800-86 およびフォレンジックのベストプラクティスでは、ipconfig などのシステム コマンドを使用して揮発性の証拠を収集することが推奨されています。

最新問題: **14**
Mac OS X を実行しているコンピュータのシステム構成ファイルはどのディレクトリに保存されますか?
A. /var
B. /bin
C. /etc
D. /cfg
Answer: C (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
macOSを含むUnixベースのシステムの/etcディレクトリには、重要なシステム設定ファイルとスクリプトが格納されています。これは、システム全体の設定データの標準的な場所です。
* /var には、ログやスプール ファイルなどの変数データが含まれます。
* /bin には必須のバイナリ実行可能ファイルが含まれています。
* /cfgisはmacOSの標準ディレクトリではありません。
これは標準的な Unix/Linux ディレクトリ構造の知識であり、macOS の NIST およびフォレンジック参照に反映されています。

最新問題: **15**
ユーザーが 64 ビット版の Windows 7 にインストールした 32 ビット プログラムのデフォルトの場所はどこですか?
A. C:\ProgramData
B. C:\Program ファイル
C. C:\Windows
D. C:\Program ファイル (x86)
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
64ビット版Windowsオペレーティングシステム（Windows 7を含む）では、32ビットアプリケーションはデフォルトでC:\Program Files (x86)フォルダにインストールされます。この分離により、OSは64ビットと32ビットを区別することができます。
32 ビット アプリケーションでは、適切なシステム コールとリダイレクトを適用します。
* C:\Program Files はネイティブ 64 ビット アプリケーション用に予約されています。
* C:\ProgramData には、ユーザー間で共有されるアプリケーション データが含まれます。

* C:\Windows にはシステム ファイルが含まれますが、プログラムのインストールは含まれません。
この構造は、Windows フォレンジック調査に関する公式の NIST ガイドラインを含む、Microsoft Windows Internals および Windows Forensics ガイドに記載されています。

最新問題: **16**
Windows Phone 8 のビット単位のコピーを作成するにはどのツールを使用できますか?
A. フォレンジックツールキット（FTK）
B. データドクター
C. パンエイジ
D. ウルフ
Answer: A (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
Forensic Toolkit (FTK) は、Windows Phone 8 を含む様々なデバイスから、物理抽出と論理抽出をサポートし、ビット単位のイメージを取得できる包括的なフォレンジックスイートです。FTK はモバイルデバイスのフォレンジックイメージングに広く受け入れられ、利用されています。
* Data Doctor は主にデータ復旧ツールであり、モバイルフォレンジックイメージングに特化しているわけではありません。
* Pwnage は iOS デバイスのジェイルブレイクに関連しています。
* Wolf は、Windows Phone 8 で認められたフォレンジック イメージング ツールではありません。
NIST モバイル デバイス フォレンジック標準では、モバイル デバイス イメージングの推奨ツールとして FTK が挙げられています。

最新問題: **17**
サイバー犯罪者が情報を隠すために使用できる手法は何ですか?
A. ステガナリシス
B. ステガノグラフィー
C. 暗号化

D. 暗号化
Answer: B (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
ステガノグラフィーとは、情報自体の存在を隠蔽するために、別のファイル、メッセージ、画像、または媒体の中に情報を隠蔽する技術です。暗号化とは異なり、データは単にスクランブル化されるのではなく、隠蔽されます。
* ステガナリシスとは、隠されたデータの検出または分析です。
* 暗号化と暗号法では、データをスクランブルしますが、本質的にはデータの存在を隠すことはありません。
NIST とデジタルフォレンジックのガイドラインでは、ステガノグラフィーを、犯罪者が検出を逃れるために使用する、隠された書き込みやデータの隠蔽の技術と定義しています。

最新問題**: 18**
Windows\System32\ ディレクトリにローカル Windows パスワードを保存し、ライブ CD を使用して解読される可能性があるファイルはどれですか。
A. 私は
B. IPSec
C. HAL
D. ンティドル
Answer: A (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
Windows\System32\configディレクトリにあるSAM セキュリティアカウントマネージャー）ファイルは、ハッシュ化されたローカルユーザーアカウントのパスワードを保存します。ライブCDまたは起動可能なフォレンジックツールを使用してアクセスおよび抽出できるため、フォレンジック調査員は実行中のオペレーティングシステムをバイパスし、証拠の改ざんを回避できます。
* IPSec はパスワードの保存ではなく、ネットワーク セキュリティ ポリシーに関連しています。
* HAL (ハードウェア抽象化レイヤー) は、ハードウェアの相互作用を管理するシステム ファイルです。
* Ntidr は、Windows NT システムのブート ローダー ファイルです。
SAM ファイルから抽出されたパスワード ハッシュをクラッキングすることは、調査中にユーザーのパスワードを回復するための一般的なフォレンジック手法です。
参考: NIST Special Publication 800-86 および Windows フォレンジックの教科書では、SAM ファイルがフォレンジック ライブ CD またはイメージングを介してアクセス可能なローカル パスワード ハッシュのリポジトリであることが確認されています。

最新問題**: 19**
法医学の専門家は、証拠の収集と分析のプロセス中に、デジタル証拠が保護され、安全な方法で取り扱われたことをどのように証明するのでしょうか?

A. すべての証拠を暗号化することで
B. 保管の連鎖を維持することにより
C. 一時ファイルを削除することで
D. バックアップを実行することによって
Answer: B (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
証拠保全記録とは、証拠の押収、保管、管理、移送、分析、処分の詳細を時系列で記録した文書です。この記録を保管することで、証拠が保護され、改ざんされていないことが証明され、裁判での証拠能力の維持に不可欠です。
* 各転送またはアクセスは、日付、時刻、ハンドラーとともに記録される必要があります。
* チェーンが途切れると、証拠の法的有効性が損なわれる可能性があります。
参考: NIST および法医学のベスト プラクティスによれば、信頼できる証拠の取り扱いには保管チェーンの文書化が必須です。

最新問題**: 20**
VoIP 通話の盗聴を許可する規定が含まれている法律はどれですか?
A. 法執行機関への通信支援法 (CALEA)
B. 電子通信プライバシー法（ECPA）
C. 医療保険の携行性と責任に関する法律（HIPAA）
D. 通信保存法
Answer: (解答を表示する)
正確な抜粋からの包括的かつ詳細な説明：
法執行機関に対する通信支援法 (CALEA) は、通信事業者に対し、Voice over IP (VoIP) 通話を含む許可された盗聴の実行において法執行機関を支援することを義務付け、合法的な傍受機能を確保しています。
* CALEA では、通信システムに監視機能が組み込まれている必要があります。
* プライバシーの権利と法執行のニーズとのバランスをとります。
参考:CALEA は、合法的な傍受機能に関連するデジタルフォレンジックおよびサイバーセキュリティ標準で引用されています。

最新問題**: 21**
ある企業の最高情報セキュリティ責任者（CIO）は、攻撃者が社内ネットワークに侵入し、ステガノグラフィを用いて外部との通信を行っていると確信しています。セキュリティチームがこのインシデントを調査しており、まずはステガノグラフィの中核要素に焦点を当てるよう指示されています。
ステガノグラフィの中核となる要素は何ですか?
A. ペイロード、キャリア、チャネル
B. 暗号化、復号化、鍵
C. ファイル、メタデータ、ヘッダー
D. ハッシュ、ノンス、ソルト

Answer: A (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
ステガノグラフィの中核となる要素は次のとおりです。
* ペイロード: 隠されたデータまたはメッセージ、
* キャリア: ペイロードを含む媒体（例：画像音声ファイル）
* チャネル: ペイロードが埋め込まれたキャリアを配信するために使用される方法またはパス。
* これらの要素を理解することは、調査員がステガノグラフィコンテンツを検出して分析するのに役立ちます。
参考: NIST SP 800-101 およびステガノグラフィの研究では、これらのコア コンポーネントがステガノグラフィ通信の基礎となることが特定されています。

最新問題**: 22**
スーザンは自分の信用情報報告書を見ていて、最近自分の名義で新しいクレジットカードがいくつか開設されていることに気づきました。スーザン自身はこれらのクレジットカード口座を開設していません。
スーザンに対してどのような種類のサイバー犯罪が行われたのでしょうか?
A. 個人情報の盗難
B. SQLインジェクション
C. サイバーストーキング
D. マルウェア
Answer: A (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
個人情報窃盗は、攻撃者が他人の個人情報を不法に取得し、それを利用して口座開設、クレジットへのアクセス、あるいは詐欺行為を行うことで発生します。被害者の同意なしにクレジットカードを開設することは、典型的な例です。
※SQLインジェクションはWebアプリケーション攻撃手法であり、今回の件とは直接関係ありません。
* サイバーストーキングはデジタル手段による嫌がらせであり、無関係です。
* マルウェアは悪意のあるソフトウェアであり、個人情報の盗難に使用される可能性がありますが、それ自体は犯罪ではありません。
参考: 米国連邦取引委員会 (FTC) の定義と NIST サイバーセキュリティ フレームワークによれば、個人情報の盗難は、詐欺目的で他人の個人情報を不正に使用することと定義されており、スーザンの状況と完全に一致しています。

最新問題**: 23**
フォレンジック調査員は、電子メール メッセージが Microsoft Exchange サーバーのどこに保存されているかを特定する必要があります。
Exchange 電子メール サーバーがメールボックス データベースを保存するために使用するファイル拡張子はどれですか?

A. .edb
B. .nsf
C. .mail
D. .db
Answer: A (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
Microsoft Exchange Server は、Extensible Storage Engine (ESE) データベース ファイルに .edb ファイル拡張子を使用します。
これらの .edb ファイルには、電子メール、カレンダー項目、連絡先などのメールボックス データが含まれています。
* IBM Lotus Notes で使用される .nsfis。
* .mailand.dbare は汎用拡張子ですが、Exchange の標準ではありません。
* .edb ファイルは、Exchange メールボックスのプライマリ データ ストアです。
参考: Microsoft の技術ドキュメントとフォレンジック マニュアルによると、Exchange メールボックス データベースは .edb ファイルに保存され、フォレンジック調査員はそれを分析して電子メールの証拠を回復します。

最新問題: **24**
リモート コンピューターから収集されたイベントは、どの Windows 7 オペレーティング システムのログに保存されますか?
A. システム
B. アプリケーション
C. 転送されたイベント
D. セキュリティ
Answer: C (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
Windows 7のForwardedEventsログは、イベント転送を介してリモートコンピューターから収集されたイベントを保存するために特別に設計されています。このログは、企業環境でイベント監視を一元化するために使用されるWindowsイベント転送機能の一部です。
* システムログとアプリケーションログには、ローカル システムとアプリケーションのイベントが保存されます。
* Securitylog は、ローカルのセキュリティ関連のイベントを保存します。
* ForwardedEvents は他のマシンから転送されたイベントを収集して保存します。
Microsoft のドキュメントと NIST SP 800-86 では、調査における集中的なイベント ログ収集に ForwardedEvents を使用することが言及されています。

最新問題: **25**
磁気ドライブはどのストレージ形式ですか?
A. CD-ROM
B. SATA

C. ブルーレイ
D. SSD
Answer: B (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
SATA（シリアルATA）は、磁気ハードディスクドライブ（HDD）やソリッドステートドライブ（SSD）をコンピュータに接続するために一般的に使用されるインターフェース規格です。SATAという用語自体は接続方法を表していますが、SATAをインターフェースとして使用するHDDのほとんどは磁気ドライブです。
* CD-ROM および Blu-ray は磁気ではなく光学的な記憶メディアです。
* SSD (ソリッド ステート ドライブ) は磁気ストレージではなくフラッシュ メモリを使用します。
* 磁気ドライブは、通常 SATA またはその他のインターフェースを介して接続される回転する磁気プラッターに依存しています。
この区別は、NIST やフォレンジック ハードウェアの教科書などのデジタル フォレンジックのトレーニングやハードウェア ドキュメントで強調されています。

最新問題: **26**
会社のユーザーは、vacationdetails.doc というデータ ファイルに機密情報を保存する金庫の組み合わせを隠そうとします。
vacationdetails.doc は、ステガノグラフィー用語で何と呼ばれますか?
A. ペイロード
B. 雪
C. キャリア
D. チャネル
Answer: C (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
ステガノグラフィーでは、秘密情報を隠すファイルはキャリアと呼ばれます。キャリアファイルは一見普通のファイルに見えますが、埋め込まれた隠しデータ（ペイロード）が含まれています。
* ペイロードとは、キャリア内に隠された実際の秘密データを指します。
* スノーとは、多くの場合、画像やファイル内に存在するランダムなノイズやアーティファクトを指します。
* チャネルとは、データを送信するために使用される媒体または通信パスを指します。
したがって、vacationdetails.doc は隠し情報を含むキャリア ファイルです。
参考: 標準的なステガノグラフィの文献およびフォレンジック文書では、キャリアはペイロード データを隠すために使用されるファイルとして定義されています。

最新問題: **27**
デジタルフォレンジック調査員は、ハッキング事件で使用されたコンピュータを受け取り、そのコンピュータのレジストリから情報を抽出するよう依頼されます。

要求されたデジタル証拠を取得する場合、審査官はどのように進めるべきでしょうか?
A. 使用するツールや技術が広く受け入れられていることを確認する
B. コンピュータが適切に押収されたかどうかを調査する
C. 調査プロセスに同僚を立ち会わせる
D. ハッキングウェブサイトからツールをダウンロードしてデータを抽出する
Answer: A (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
デジタルフォレンジックにおいて、デジタル証拠の完全性と許容性を維持するためには、信頼性が高く、検証済みで、広く受け入れられているツールと手法の使用が不可欠です。米国国立標準技術研究所（NIST）のガイドラインとデジタル証拠に関する科学ワーキンググループ（SWGDE）の標準によれば、あらゆるフォレンジックプロセスでは、フォレンジックコミュニティで認められ、正確性と信頼性を確保するための厳格なテストを経た手法を使用する必要があります。
* 検証済みのツールを使用すると、証拠の汚染や紛失を防ぎ、結果が法的な精査に耐えられることが保証されます。
* 適切な押収と目撃は重要ですが、抽出段階では適切で信頼できるツールを使用することが優先されます。
* 許可されていないソースや疑わしいソースからツールをダウンロードすると、証拠が危険にさらされる可能性があり、倫理的または法的に許されない行為です。
参考: NIST SP 800-101 (モバイル デバイス フォレンジックに関するガイドライン) および SWGDE ベスト プラクティスでは、フォレンジック調査の基本原則として、ツールの検証とコミュニティで受け入れられている方法の遵守を重視しています。

最新問題**: 28**
ステガノグラフィの存在を識別するツールはどれですか?
A. ディスク調査官
B. ディスクディガー
C. フォレンジックツールキット (FTK)
D. コンピュータCOP
Answer: A (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
Disk Investigator は、ディスク イメージとファイル システムを分析し、スラック スペース、隠しファイル、埋め込みデータを調べてステガノグラフィの存在を含む隠しデータを識別できるフォレンジック ツールです。
* DiskDigger は主にデータ復旧ツールです。
* FTK は包括的なフォレンジック スイートですが、ステガノグラフィの検出に特化しているわけではありません。
* ComputerCOP はペアレンタルコントロールソフトウェアであり、フォレンジックツールではありません。

デジタルフォレンジックのベストプラクティスでは、Disk Investigator がファイルやディスク領域内のステガノグラフィック コンテンツの検出に役立つことが認識されています。