EC-COUNCIL 112-57合格問題:無料ダウンロードEC-Council Digital Forensics Essentials (DFE)

2026年JPTestKingの最新112-57 PDFダンプおよび112-57試験エンジンの無料共有：https://drive.google.com/open?id=1MrRRJoiFJCNoCZ4OMmZ3raMY9TsWaGQa

112-57スタディガイドは、多くのメリットと機能を高めます。購入前に112-57テスト問題をダウンロードして自由に試すことができます。当社製品を購入した後、すぐに当社製品を使用できます。選択できる3つのバージョンが用意されており、112-57トレーニング資料を学習して試験を準備するのに20〜30時間しかかかりません。EC-COUNCIL合格率とヒット率は両方とも高いです。 1年以内に24時間のオンラインカスタマーサービスと無料アップデートを提供しています。そして、112-57試験問題を試してみると、112-57トレーニング資料には多くの利点があることがわかります。

1年以内に112-57テスト準備を更新し、必要なものを無料でダウンロードします。 1年後、購入者がサービスの保証を延長してお金を節約できるようにしたい場合、EC-COUNCILクライアントに50％の割引特典を提供します。 あなたが古いクライアントである場合、112-57試験トレントを購入する際に特定の割引を享受できるため、より多くのサービスとより多くのメリットを享受できます。 このアップデートでは、最新かつ最も有用な112-57準備トレントを提供できます。さらに学習して、EC-Council Digital Forensics Essentials (DFE)の112-57試験に合格することができます。

>> 112-57合格問題 <<

112-57予想試験 & 112-57学習教材

自分自身のIT技能を増強したいか。一回だけでEC-COUNCILの112-57認定試験に合格したいか。JPTestKingは最も質の良いEC-COUNCILの112-57問題集を提供できるし、君の認定試験に合格するのに大変役に立ちます。もし君はいささかな心配することがあるなら、あなたはうちの商品を購入する前に、JPTestKingは無料でサンプルを提供することができます。無料サンプルのご利用によってで、もっと自信を持って認定試験に合格することができます。

EC-COUNCIL 112-57 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• ダークウェブフォレンジック：このモジュールでは、Torブラウザに関連するアーティファクトの分析やシステム上でのダークウェブの使用状況の特定など、ダークウェブ活動の調査について説明します。
トピック 2	• コンピュータフォレンジックの基礎：このモジュールでは、デジタル証拠、フォレンジック準備、捜査官の役割など、コンピュータフォレンジックの中核となる概念を紹介します。また、フォレンジック調査に関わる法的要件とコンプライアンス要件についても説明します。

トピック 3	• マルウェアフォレンジック：このモジュールでは、静的解析や動的解析、システムやネットワークの動作調査など、マルウェア調査の手法を紹介し、悪意のある活動を理解するための方法論を解説します。
トピック 4	• Windowsフォレンジック：このモジュールでは、Windowsシステムにおけるフォレンジック調査について説明します。これには、システムおよびユーザーのアクティビティを特定するためのメモリ、レジストリデータ、ブラウザーの痕跡、ファイルメタデータの分析が含まれます。
トピック 5	• データ取得と複製：このモジュールでは、デジタル証拠の収集と複製の方法に焦点を当てます。フォレンジックイメージの作成やシステムメモリのキャプチャに使用される取得技術、フォーマット、手順について説明します。
トピック 6	• LinuxおよびMacのフォレンジック：このモジュールでは、LinuxおよびMacシステムのフォレンジック分析手法について説明します。システムデータ、ファイルシステム、メモリを分析してデジタル証拠を復元することに重点を置いています。
トピック 7	• 鑑識対策技術への対抗：このモジュールでは、証拠を隠蔽または破壊するために使用される鑑識対策手法について説明します。また、捜査官が隠されたデータを検出し、削除または保護された情報を復元するために使用する技術についても解説します。

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) 認定 112-57 試験問題 (Q46-Q51):

質問 # 46
Which of the following commands can an investigator use to parse GPTs of both types of hard disks, including those formatted with either UEFI or MBR?

- A. Get-BootSector
- B. Get-ForensicPartitionTable
- C. Get-GPT
- D. Get-PartitionTable

正解：B

解説：
In forensic examinations, investigators must correctly interpret a disk'spartitioning schemebecause it determines where volumes begin, where file systems reside, and how to validate acquisition completeness.
Modern systems may useGPT(commonly associated with UEFI) while legacy systems often useMBR. A practical forensic command therefore needs to detect and parse partition informationregardless of whether the disk uses MBR or GPT, and present the results in a consistent, investigator-friendly output for verification and downstream analysis (e.g., selecting the correct partition offsets for imaging or mounting).
Get-ForensicPartitionTableis designed for exactly this role in forensic PowerShell tooling: it parses partition table structures in a forensically oriented manner and supports disks partitioned usingeither MBR or GPT.
That "forensic" emphasis typically means it reads raw structures directly, reports partition entries and offsets, and helps avoid ambiguity when the protective MBR (present on GPT disks) could confuse simplistic parsers.
By contrast,Get-BootSectortargets boot sector/VBR data rather than the full partition layout;Get-GPTis GPT- specific and does not cover MBR-only disks; andGet-PartitionTableis a more generic label that may not guarantee dual-scheme forensic parsing.
Therefore, the correct option isC.

質問 # 47
Bob, a forensic investigator, is investigating a live Windows system found at a crime scene. In this process, Bob extracted subkeys containing information such as SAM, Security, and software using an automated tool called FTK Imager.
Which of the following Windows Registry hives' subkeys provide the above information to Bob?

- A. HKEY_CLASSES_ROOT
- B. HKEY_LOCAL_MACHINE

- C. HKEY_CURRENT_CONFIG
- D. HKEY_CURRENT_USER

正解：B

解説：
In Windows forensics, the Registry is organized into logical root keys ("hives") that aggregate configuration and security data. The items named in the question-SAM,SECURITY, andSOFTWARE-aresystem-wide registry hivesstored on disk (typically under the system's configuration directory) and loaded at runtime underHKEY_LOCAL_MACHINE (HKLM). Investigators rely on these hives because they contain high- value evidence: theSAMhive stores local account database information (including user and group identifiers and credential-related material), theSECURITYhive holds system security policy and LSA-related settings, and theSOFTWAREhive contains installed software, application configuration, and many operating system settings relevant for program execution and persistence analysis.
Tools likeFTK Imagercan extract these hives (or their live-memory representations) during triage to preserve volatile context and enable offline parsing while maintaining evidentiary integrity. The other root keys do not match these specific hives:HKEY_CURRENT_USERis per-user profile data, HKEY_CURRENT_CONFIGreflects current hardware profile, andHKEY_CLASSES_ROOTis primarily file association/COM class mapping (largely derived from HKLM\Software\Classes and HKCU\Software\Classes). Therefore, the correct hive root that provides SAM, SECURITY, and SOFTWARE subkeys isHKEY_LOCAL_MACHINE (B).

質問 # 48
A system that a cybercriminal was suspected to have used for performing an anti-social activity through the Tor browser. James reviewed the active network connections established using specific ports via Tor.
Which of the following port numbers does Tor use for establishing a connection via Tor nodes?

- A. 31/456
- B. 9150/9151
- C. 1026/64666
- D. 3024/4092

正解：B

解説：
In Tor Browser deployments, Tor typically runs a local client ("tor" process) that exposes aSOCKS proxyfor applications (the browser) to send traffic into the Tor network and, optionally, acontrol interfacefor managing circuits and obtaining runtime status. In many forensic lab guides and Tor Browser bundle configurations, the default local SOCKS listening port is9150, and the associated Tor control port is commonly9151. This pairing is frequently referenced in investigations because endpoint triage (e.g., netstat outputs, firewall logs, EDR socket telemetry) may show local loopback connections from the browser to127.0.0.1:9150(SOCKS) and management communications involving9151(control).
From a network-forensics viewpoint, these ports help distinguish Tor Browser activity from other proxy tools:
the browser does not directly connect to Tor relays; instead, it hands traffic to the local SOCKS proxy, which then establishes encrypted circuits to Tor nodes. While Tor can be configured to use different ports, the question asks about the specific ports used for establishing Tor connections in typical Tor Browser setups, which aligns with9150/9151. Therefore, the correct option isD.

質問 # 49
Which of the following hives in the Windows Registry hierarchical database is volatile in nature and contains file-extension association information and programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data?

- A. HKEY_CLASSES_ROOT
- B. HKEY_LOCAL_MACHINE
- C. HKEY_CURRENT_CONFIG
- D. HKEY_CURRENT_USER

正解：A

解説：
HKEY_CLASSES_ROOT (HKCR)is the Windows Registry location that storesfile-association and COM registration data, including mappings forfile extensions(e.g.,.docx) toProgIDs, and COM object identifiers such asCLSIDand interface-related identifiers likeIID. In forensic examinations, HKCR is frequently consulted to determine which application is registered to open a

specific file type, to identify COM objects that may enable persistence or abuse (e.g., through COM hijacking), and to correlate suspicious registry-based execution mechanisms with installed software.
HKCR is often described asvolatile in naturebecause it is not a single standalone hive file stored independently in the same way as SAM or SYSTEM; instead, it is amerged, runtime viewcreated by the OS primarily fromHKLM\Software\Classes(machine-wide registrations) andHKCU\Software\Classes(per-user overrides). This means what you see under HKCR can vary depending on the current user context and system state, and the effective associations/registrations may change when software is installed, updated, or when per- user settings override machine defaults.
The other options represent different scopes: HKLM is system configuration, HKCU is user profile configuration, and HKCC reflects the current hardware profile-not the primary COM/file association repository.

質問 # 50
Jennifer, a forensics investigation team member, was inspecting a compromised system. After gathering all the evidence related to the compromised system, she disconnected the system from the network to stop the spread of the incident to other systems.
Identify the role played by Jennifer in the forensics investigation.

- A. Expert witness
- B. Evidence manager
- C. Incident responder
- D. Incident analyzer

正解：C

解説：
Jennifer's actions match the responsibilities of anincident responder, whose job spans immediatecontainment, preservation, and stabilizationactivities during an active or recently active security incident. In standard digital forensics and incident response (DFIR) procedures, responders first take steps topreserve evidence(e.g., documenting the scene, capturing volatile data when appropriate, and collecting relevant system artifacts) and then executecontainment measuresto prevent further harm. Disconnecting a compromised host from the network is a classic containment control used to stop malware propagation, block command-and-control communications, and prevent lateral movement to other systems.
Anincident analyzertypically focuses on deeper technical analysis-timeline reconstruction, root cause determination, and correlating artifacts across hosts and logs-rather than performing immediate containment.
Anevidence manageris primarily responsible for maintaining evidence integrity, chain of custody, storage, labeling, and access control, not operational containment. Anexpert witnessprovides formal testimony and interpretation in legal or disciplinary proceedings and is not usually involved in live containment actions.
Since Jennifer bothgathered evidenceand thenisolated the system to stop spread, the role most consistent with documented DFIR responsibilities isIncident responder (A).

質問 # 51
.....

(DFE) □【 www.goshiken.com 】から簡単に⇛ 112-57 ⇚を無料でダウンロードできます112-57最新テスト

- ハイパスレートの112-57合格問題 - 合格スムーズ112-57予想試験 | 実際的な112-57学習教材 □▸ www.it-passports.com◂から【 112-57 】を検索して、試験資料を無料でダウンロードしてください112-57認定試験
- 112-57トレーリングサンプル □112-57試験勉強攻略 □112-57模擬試験サンプル □検索するだけで▸ www.goshiken.com◂から《 112-57 》を無料でダウンロード112-57合格問題
- 試験の準備方法-更新する112-57合格問題試験-認定する112-57予想試験 □【 www.goshiken.com 】サイトで{ 112-57 }の最新問題が使える112-57資格受験料
- 112-57試験の準備方法丨更新する112-57合格問題試験丨一番優秀なEC-Council Digital Forensics Essentials (DFE)予想試験 □ウェブサイト▸ www.goshiken.com◂から“ 112-57 ”を開いて検索し、無料でダウンロードしてください112-57合格受験記
- 112-57合格受験記 □112-57試験勉強攻略 □112-57関連受験参考書 □☀ www.topexam.jp □☀□を入力して{ 112-57 }を検索し、無料でダウンロードしてください112-57日本語試験対策
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, lexieegvd796482.wikitron.com, sachinfvtx101264.plpwiki.com, craigshav311962.wannawiki.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, socialaffluent.com, getidealist.com, marleyqtvx559753.wikimidpoint.com, startupxplore.com, Disposable vapes

P.S. JPTestKingがGoogle Driveで共有している無料かつ新しい112-57ダンプ：https://drive.google.com/open?id=1MrRRJoiFJCNoCZ4OMmZ3raMY9TsWaGQa