EC-COUNCIL 112-57: EC-Council Digital Forensics Essentials (DFE) braindumps PDF & Testking echter Test

2026 Die neuesten ExamFragen 112-57 PDF-Versionen Prüfungsfragen und 112-57 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1UsGZB-ZmQHjWdDIec83-d1ctee6e-LNH

Haben Sie die Schulungsunterlagen zur EC-COUNCIL 112-57 Zertifizierungsprüfung aus unserem ExamFragen, warden Sie den Schlüssel für das Bestehen der EC-COUNCIL 112-57 Zertifizierungsprüfung gewinnen, der Ihnen bessere Entwicklung im IT-Bereich gewährleisten kann. Das Alles bedürft Ihres Vertrauens: Sie müssen auf ExamFragen vertrauen und Sie müssen zudem auf die Schulungsunterlagen zur EC-COUNCIL 112-57 Zertifizierungsprüfung vertrauen. Inhalt unserer Lehrmaterialien ist absolut echt und zuversichtlich. Darüber hinaus beträgt unsere Bestehensrate der EC-COUNCIL 112-57 Zertifizierungsprüfung 100%.

EC-COUNCIL 112-57 Exam Overview:

Certification Vendor:	EC-Council
Exam Name:	EC-Council Digital Forensics Essentials (DFE)
Exam Number:	112-57
Available Languages:	English
Recommended Training:	EC-Council Digital Forensics Essentials Training
Exam Registration:	EC-Council Official Certification Page
Sample Questions:	EC-COUNCIL 112-57 Sample Questions
Exam Way:	Online, self-paced training with assessment (EC-Council iLearn platform or authorized delivery partners)
Pre Condition:	No formal prerequisites required; basic understanding of cybersecurity is recommended.
Official Syllabus URL:	https://www.eccouncil.org/programs/digital-forensics-essentials-dfe/

>> 112-57 Probesfragen <<

112-57 Kostenlos Downloden, 112-57 Examsfragen

Die Zertifizierung der EC-COUNCIL 112-57 zu erwerben bedeutet mehr Möglichkeiten in der IT-Branche. Wir ExamFragen haben schon reichliche Erfahrungen von der Entwicklung der EC-COUNCIL 112-57 Prüfungssoftware. Unsere Technik-Gruppe verbessert beständig die Prüfungsunterlagen, um die Benutzer der EC-COUNCIL 112-57 Prüfungssoftware immer leichter die Prüfung bestehen zu lassen.

EC-COUNCIL 112-57 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Data Acquisition and Duplication: This module focuses on methods for collecting and duplicating digital evidence. It explains acquisition techniques, formats, and procedures used to create forensic images and capture system memory.
Thema 2	• Computer Forensics Fundamentals: This module introduces the core concepts of computer forensics, including digital evidence, forensic readiness, and the role of investigators. It also explains legal and compliance requirements involved in forensic investigations.
Thema 3	• Linux and Mac Forensics: This module explains forensic analysis techniques for Linux and Mac systems. It focuses on analyzing system data, file systems, and memory to recover digital evidence.
Thema 4	• Dark Web Forensics: This module explains the investigation of dark web activities, including analyzing artifacts related to the Tor browser and identifying dark web usage on systems.
Thema 5	• Windows Forensics: This module covers forensic investigation in Windows systems, including analysis of memory, registry data, browser artifacts, and file metadata to identify system and user activities.
Thema 6	• Computer Forensics Investigation Process: This module explains the phases of the forensic investigation process, including pre-investigation, investigation, and post-investigation. It also covers evidence integrity methods such as hashing and disk imaging.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) 112-57 Prüfungsfragen mit Lösungen (Q74-Q79):

74. Frage
Which of the following NTFS system files contains a record of every file present in the system?

- A. $logfile
- B. $quota
- C. $volume
- D. $mft

Antwort: D

Begründung:
In the NTFS file system, theMaster File Table (MFT)is the core metadata structure that tracksevery file and directoryon the volume. NTFS implements this as a special system file named$MFT(shown here as$mft).
Each file or folder on an NTFS partition is represented by at least oneMFT record entry, which stores essential metadata such as file name(s), timestamps, security identifiers/ACL references, file size, attributes, and pointers to the file's data runs (or, for very small files, the content can be stored resident inside the record). Because it is the authoritative "index" of file objects, forensic examiners rely heavily on $MFT to reconstruct user activity and file history, including evidence of deleted files (when records are marked unused but remnants of attributes may remain) and timeline building from timestamp attributes.
The other options are different NTFS metadata files with narrower purposes:$LogFilerecords NTFS transaction logs to support recovery,$Volumestores volume-level information (like version/label), and$Quotamanages disk quota tracking. None of these contain a record for every file on the system.
Therefore, the NTFS system file that contains a record of every file present is$mft (B).

75. Frage
Which of the following file systems is developed by Apple to support Mac OS in its proprietary Macintosh system and replace the Macintosh File System (MFS)?

- A. New Technology File System
- B. Apple File System

- C. Hierarchical File System
- D. Filesystem Hierarchy Standard

Antwort: C

Begründung:
Apple's original Macintosh computers initially usedMFS (Macintosh File System), which had important limitations, including a relatively flat directory model and constraints that became problematic as storage sizes and file organization needs grew. To address these limitations, Apple introducedHFS (Hierarchical File System)-explicitly designed to replace MFS and provide a truehierarchical directory structure(folders within folders), improved metadata handling, and better scalability for the Macintosh platform. From a digital forensics perspective, this historical transition matters because examiners may encounter legacy Macintosh media or disk images where understanding the file system family helps interpret catalog structures, allocation behavior, and metadata artifacts.
The other options do not fit the "replace MFS" requirement.NTFSis Microsoft's Windows file system.APFS (Apple File System)is Apple's modern file system introduced much later (primarily for SSDs, with features like snapshots and strong encryption support) and it replaced HFS+ in newer macOS versions-not MFS.
Filesystem Hierarchy Standard (FHS)is a UNIX/Linux directory layout standard, not a Macintosh disk file system. Therefore, the Apple-developed file system that replaced MFS isHierarchical File System (HFS), which corresponds toOption D.

76. Frage
Which of the following steps in forensic readiness planning provides a backup for future reference and assists in presenting evidence in a court of law?

- A. Identifying the potential evidence required for an incident
- B. Creating a process for documenting the procedure
- C. Keeping an incident response team ready to review the incident
- D. Determining the sources of evidence

Antwort: B

Begründung:
In forensic readiness planning, the goal is to ensure that when an incident occurs, the organization can collect, preserve, and present digital evidence in a manner that remainsreliable, repeatable, and legally defensible. A key requirement for courtroom acceptance is cleardocumentation-often referred to as proper documentation and chain-of-custody support-showing what actions were taken, by whom, when, using which tools, and under what conditions. Creating a defined process for documenting procedures ensures investigators consistently record acquisition steps, handling methods, hashing/verification results, storage locations, access history, and any changes in evidence possession. This documentation becomes a "backup" in the sense that it preserves institutional memory of the investigation steps, allowing future reviewers (auditors, opposing experts, courts) to reconstruct and validate what occurred even long after the incident.
While identifying potential evidence (B) and determining evidence sources (C) are important readiness tasks, they do not themselves create the structured record needed to defend evidence integrity. Keeping an incident response team ready (D) supports operational response, but does not directly ensure admissibility. Therefore, the step that provides future reference and supports court presentation isCreating a process for documenting the procedure (A).

77. Frage
Which of the following techniques is used to compute the hash value for a given binary code to uniquely identify malware or periodically verify changes made to the binary code during analysis?

- A. Malware disassembly
- B. Local and online malware scanning
- C. File fingerprinting
- D. Strings search

Antwort: C

Begründung:
File fingerprintingis the forensic technique of generating acryptographic hash(such as MD5, SHA-1, SHA-256) for a file to create aunique, repeatable identifierfor that exact byte sequence. In malware forensics, analysts compute hashes to (1)uniquely identifya suspicious binary across cases and tools, (2) confirm whether two samples are identical or different variants, and (3)verify integrity over time-for example, ensuring the sample did not change during copying, extraction, sandbox handling, or

during an analysis workflow that might inadvertently modify the file (e.g., patching, unpacking outputs, or tool-side normalization). Re-hashing at different stages provides a defensible way to demonstrate that the analyzed artifact is the same as the acquired artifact, supporting evidentiary integrity and chain-of-custody principles commonly emphasized in digital forensics documentation.
The other techniques do not primarily serve this purpose.Strings searchextracts readable text fragments but does not produce a unique integrity identifier.Local and online malware scanninguses signatures/reputation and may identify families, but it is not an integrity verification mechanism for the exact file bytes.Malware disassemblyhelps understand logic and instructions, not compute an identity hash. Therefore, the correct answer isFile fingerprinting (A).

78. Frage
Which of the following standards and criteria version of SWGDE mandates that any action with the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner?

- A. Standards and Criteria 1.3
- B. Standards and Criteria 1.7
- C. Standards and Criteria 1.1
- D. Standards and Criteria 1.5

Antwort: B

Begründung:
The statement in the question matchesSWGDE Principle 1, Standards and Criteria 1.7, which explicitly requires thatany action that could alter, damage, or destroy original digital evidence must be performed by qualified personnel in a forensically sound manner. In digital forensics doctrine, this requirement exists because digital evidence is highly fragile: routine interactions (booting a system, opening a file, connecting storage, running commands) can change timestamps, overwrite unallocated space, modify logs, or trigger encryption/key rotation. SWGDE's emphasis on "qualified persons" and "forensically sound manner" aligns with core evidentiary expectations: minimizing changes to original media, using controlled and repeatable methods (e.g., write-blocking, validated imaging, documented procedures), and ensuring actions are defensible under scrutiny.
Options 1.1, 1.3, and 1.5 relate to broader quality and procedural requirements (quality systems, SOP review, appropriate tools), but they do not contain the specific mandate about potentially altering original evidence.
The exact phrasing about alteration/damage/destruction and qualified handling is associated withStandards and Criteria 1.7, makingBthe correct choice.

79. Frage
.....

www.deutschpruefung.com 》 nach ➡ 112-57 □□□ und erhalten Sie den kostenlosen Download mühelos □112-57 Praxisprüfung

- learn.csisafety.com.au, scalar.usc.edu, connect.garmin.com, notefolio.net, buyerseller.xyz, hashnode.com, learn.csisafety.com.au, aprenderfotografia.online, fortunetelleroracle.com, www.askmap.net, Disposable vapes

BONUS!!! Laden Sie die vollständige Version der ExamFragen 112-57 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1UsGZB-ZmQHjWdDIec83-d1ctee6e-LNH