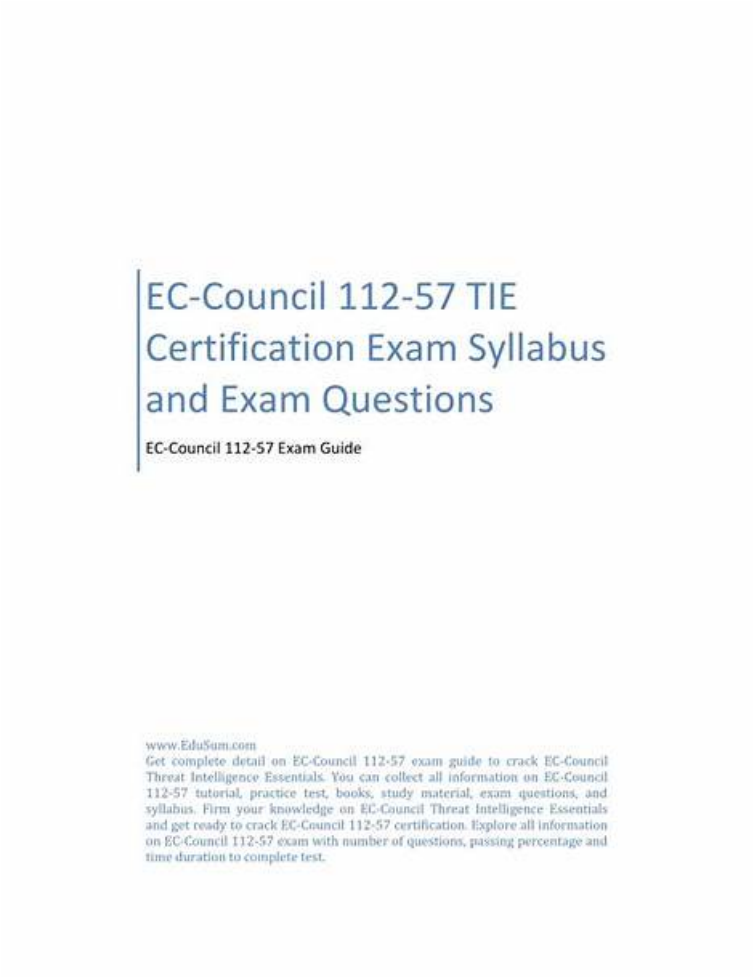
# 112-57 Exam Questions - To Gain Brilliant Result




2026 Latest Exam4Docs 112-57 PDF Dumps and 112-57 Exam Engine Free Share: https://drive.google.com/open?id=1n_lMn32FERPrCPxbGBg_Hz5vSUccLHSY

With the development of the times, the pace of the society is getting faster and faster. If we don't try to improve our value, we're likely to be eliminated by society. Under the circumstances, we must find ways to prove our abilities. For example, getting the 112-57 Certification is a good way. If we had it, the chances of getting a good job would be greatly improved. And our 112-57 exam braindumps are the tool to help you get the 112-57 certification.

## EC-COUNCIL 112-57 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity. |
| Topic 2 | • Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications. |
| Topic 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. |
| Topic 4 | • Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence. |

| | |
|---|---|
| Topic 5 | • 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. |
| Topic 6 | • 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. |
| Topic 7 | • Understanding Hard Disks and File Systems: This module covers disk structures, types of storage drives, and operating system boot processes. It also explains how investigators analyze file systems and recover deleted data. |
| Topic 8 | • Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic. |
| Topic 9 | • Defeating Anti-forensics Techniques: This module discusses anti-forensic methods used to hide or destroy evidence. It also explains techniques investigators use to detect hidden data and recover deleted or protected information. |
| Topic 10 | • 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. |
| Topic 11 | • 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. |



## Reliable EC-COUNCIL 112-57 Test Topics & Test 112-57 Testking

Exam4Docs EC-COUNCIL 112-57 Exam Questions And Answers provide you test preparation information with everything you need. About EC-COUNCIL 112-57 exam, you can find these questions from different web sites or books, but the key is logical and connected. Our questions and answers will not only allow you effortlessly through the exam first time, but also can save your valuable time.

## EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q31-Q36):

**NEW QUESTION # 31**
Cheryl, a forensic expert, was recruited to investigate a malicious activity performed by an anonymous hackers' group on an organization's systems. Using an automated tool, Cheryl was able to extract the malware file and analyze the assembly code instructions, which helped him understand the malware's purpose.
Which of the following tools helped Cheryl extract and analyze the assembly code of the malware?

- A. VMware vSphere
- B. QualNet
- C. OllyDbg
- D. Virtual Box

**Answer: C**

Explanation:
To understand a malware sample's purpose at the instruction level, investigators usereverse-engineering toolsthat candisassemblecompiled binaries intoassembly codeand often allowinteractive debuggingto observe runtime behavior (API calls, unpacking routines, decryption loops, process injection, and control-flow decisions).OllyDbgis a classic Windows user-mode debugger widely referenced in malware analysis workflows because it provides an integrated view ofdisassembly, CPU registers,

memory, breakpoints, and execution tracing. This makes it suitable for extracting behavioral insight from the actual assembly instructions, especially when malware uses obfuscation or packers that require stepping through execution to reach the real payload. The other options do not primarily perform assembly-level analysis.VirtualBoxandVMware vSphereare virtualization platforms; they help safely run malware in isolated environments, but they are not disassemblers /debuggers for examining assembly instructions.QualNetis a network simulation tool used for modeling network behavior, not binary reverse engineering. Because the question specifically emphasizesanalyzing assembly code instructionsto understand malware purpose, the correct tool among the choices isOllyDbg (C).

**NEW QUESTION # 32**
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 1.5
- C. Standards and Criteria 1.1
- D. Standards and Criteria 1.7

**Answer: D**

Explanation:
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.

**NEW QUESTION # 33**
Andrew, a system administrator, is performing a UEFI boot process. The current phase of the UEFI boot process consists of the initialization code that the system executes after powering on the EFI system. This phase also manages platform reset events and sets up the system so that it can find, validate, install, and run the PEI.
Which of the following UEFI boot phases is the process currently in?

- A. Pre-EFI initialization phase
- B. Security phase
- C. Driver execution environment phase
- D. Boot device selection phase

**Answer: B**

Explanation:
In the UEFI/PI boot architecture, the phase that runsimmediately after power-on or resetis theSEC (Security) phase. Digital forensics references include UEFI phases because firmware-level activity can affect the trustworthiness of the platform (e.g., bootkits, persistence, and measured boot artifacts). The SEC phase is responsible for executing the earliest initialization instructions, handlingplatform reset events, and establishing a minimal, controlled execution environment. Critically, SEC prepares the system so it canlocate, verify, and hand off controlto the next stage-PEI (Pre-EFI Initialization)-by setting up temporary memory and foundational CPU/chipset state required for PEI modules to execute.
The wording in the question precisely matches SEC responsibilities: "initialization code executed after powering on," "manages platform reset events," and "sets up the system so it can find, validate, install, and run the PEI." By contrast,PEIfocuses on discovering and initializing permanent memory and producing the Hand-Off Blocks for DXE;DXEloads drivers and boot services; andBDSselects and launches the boot option.
Therefore, the phase described is theSecurity phase (SEC), which corresponds to optionD.

**NEW QUESTION # 34**
While investigating a web attack on a Windows-based server, Jessy executed the following command on her system:
C:> net view <\10.10.10.11>
What was Jessy's objective in running the above command?

- A. Check file space usage to look for a sudden decrease in free space
- B. Review file shares to ensure their purpose
- C. Check whether sessions have been opened with other systems
- D. Verify the users using open sessions

**Answer: B**

Explanation:
The Windowsnet view \\<computer>command is used to enumerateshared resources(SMB shares) that a remote Windows system is publishing. When Jessy runsnet view \\10.10.10.11, her goal is to retrieve a list of the target host's visible shares-such as administrative shares (e.g.,C$,ADMIN$) and any custom shares created for departments, applications, or users. In forensic and incident-response practice, this is important because attackers commonly use SMB shares forlateral movement,staging tools,dropping payloads, andexfiltrating data. By reviewing the shares exposed by a suspected server, the investigator can quickly identify unexpected or overly permissive shares, locate potential repositories of web content or logs, and determine whether a compromised web server is also exposing file resources that expand the attacker's options.
The other options map to different commands and artifacts: disk space usage is checked with storage utilities (notnet view), open sessions are examined with commands likenet session, and identifying users accessing files typically involvesnet fileor server auditing logs. Therefore, Jessy's objective was toreview file shareson the remote host.

**NEW QUESTION # 35**
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. Creating a process for documenting the procedure
- B. Keeping an incident response team ready to review the incident
- C. Identifying the potential evidence required for an incident
- D. Determining the sources of evidence

**Answer: A**

Explanation:
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).

**NEW QUESTION # 36**
.....

- www.dumpsmaterials.com: The Ideal Solution for EC-COUNCIL 112-57 Exam Preparation □ Search for ➠ 112-57 □ and download exam materials for free through ⇛ www.dumpsmaterials.com ⇚ □Exam 112-57 Question
- 2026 EC-COUNCIL 112-57: The Best EC-Council Digital Forensics Essentials (DFE) Real Brain Dumps □ Easily obtain □ 112-57 □ for free download through （ www.pdfvce.com ） □112-57 Actual Exams
- Reliable 112-57 Test Experience □ 112-57 Test Questions □ Reliable 112-57 Test Experience □ Search for 「 112-57 」 and download it for free on 《 www.prepawayete.com 》 website □Reliable 112-57 Test Review
- EC-COUNCIL 112-57 Real Brain Dumps: EC-Council Digital Forensics Essentials (DFE) - Pdfvce High Pass Rate □ Simply search for ⇛ 112-57 ⇚ for free download on 「 www.pdfvce.com 」 □Latest 112-57 Exam Testking
- EC-COUNCIL 112-57 Dumps PDF To Gain Brilliant Result □ Copy URL ➡ www.practicevce.com □□□ open and search for ➤ 112-57 □ to download for free □Reliable 112-57 Test Review
- 112-57 Test Questions □ 112-57 New Dumps Questions □ 112-57 Test Valid □ Search for [ 112-57 ] and download exam materials for free through ▸ www.pdfvce.com ◂ □112-57 Actual Exams
- EC-COUNCIL 112-57 Exam Questions 2026 Tips To Pass □ Enter ✔ www.troytecdumps.com □✔□ and search for ➤ 112-57 □ to download for free □112-57 Actual Exams
- Most workable 112-57 guide materials: EC-Council Digital Forensics Essentials (DFE) Provide you wonderful Exam Braindumps - Pdfvce □ Search for ⇛ 112-57 ⇚ and download it for free on （ www.pdfvce.com ） website □112-57 Exam Guide Materials
- Money-Back Guarantee for EC-COUNCIL 112-57 Exam Questions □ Search for 「 112-57 」 and obtain a free download on （ www.examdiscuss.com ） ☢Reliable 112-57 Test Review
- 112-57 Test Questions □ Latest 112-57 Demo □ Latest 112-57 Demo □ Open ▸ www.pdfvce.com ◂ enter { 112-57 } and obtain a free download □Pdf 112-57 Torrent
- Pdf 112-57 Torrent □ 112-57 Discount □ Reliable Study 112-57 Questions □ Search for □ 112-57 □ and download exam materials for free through ☀ www.troytecdumps.com □☀□ □112-57 Valid Test Sample
- p.me-page.com, www.stes.tyc.edu.tw, www.ganjingworld.com, www.stes.tyc.edu.tw, cpfcordoba.com, www.stes.tyc.edu.tw, wjhsd.instructure.com, dl.instructure.com, writeablog.net, hhi.instructure.com, Disposable vapes

P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by Exam4Docs: https://drive.google.com/open?id=1n_lMn32FERPrCPxbGBg_Hz5vSUccLHSY