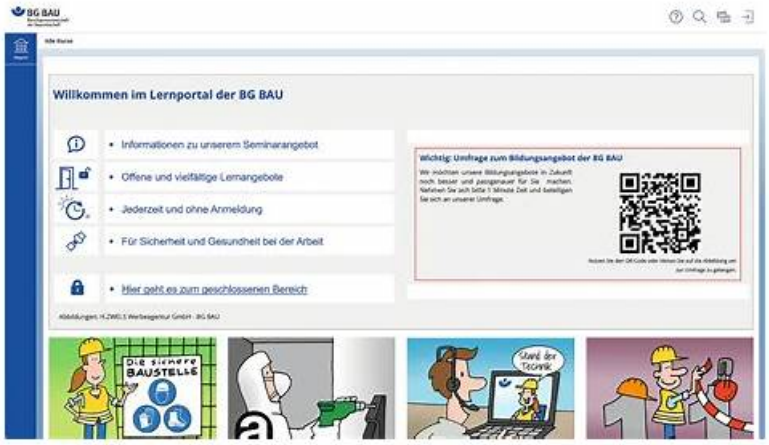
112-57 Musterprüfungsfragen & 112-57 Zertifizierungsantworten



Damit Sie DeutschPrüfung sicher wählen, wird nur Teil der online optimalen EC-COUNCIL 112-57 Zertifizierungsprüfungsmaterialien zur Verfügung gestellt. So können Sie sie kostenlos als Probe herunterladen und die Zuverlässigkeit unserer Produkte testen. Wir helfen Ihnen nicht nur, die Prüfung zum ersten Mal zu bestehen, sondern Ihnen auch viel Zeit und Energie zu ersparen. DeutschPrüfung stehen Ihnen die echten und originalen Prüfungsfragen und Antworten zur Verfügung, damit Sie die EC-COUNCIL 112-57 Prüfung 100% bestehen können. Mit EC-COUNCIL 112-57 Zertifikat werden Sie in der IT-Branche leichter befördert. Und Ihre Zukunft werden immer schöner sein.

EC-COUNCIL 112-57 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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 2	• 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 3	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
Thema 4	• 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 5	• 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.
Thema 6	• 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.
Thema 7	• 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 8	• 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 9	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Thema 10	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.

>> 112-57 Musterprüfungsfragen <<

112-57 Fragen & Antworten & 112-57 Studienführer & 112-57 Prüfungsvorbereitung

Um keine Reue und Bedauern in Ihrem Leben zu hinterlassen, sollen Sie jede Gelegenheit ergreifen, um das Leben zu vebessern. Haben Sie das gemacht? Die Fragenkataloge zur EC-COUNCIL 112-57 Zertifizierungsprüfung von DeutschPrüfung helfen den IT-Fachleuten, die Erfolg erzielen wollen, die EC-COUNCIL 112-57 Zertifizierungsprüfung zu bestehen. Um den Erfolg nicht zu verpassen, machen Sie doch schnell.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) 112-57 Prüfungsfragen mit Lösungen (Q67-Q72):

67. Frage
Bob, a forensic investigator, was instructed to review a Windows machine and identify any anonymous activities performed using it. In this process, Bob used the command "netstat -ano" to view all the active connections in the system and determined that the connections established by the Tor browser were closed.
Which of the following states of the connections established by Tor indicates that the Tor browser is closed?

- A. LISTENING
- B. TIME_WAIT
- C. CLOSE_WAIT
- D. ESTABLISHED

Antwort: B

Begründung:
In Windows network forensics,netstat -anois commonly used to correlateTCP connection stateswithprocess identifiers (PIDs)to understand which application created or used a connection. When Tor Browser is actively communicating, outbound circuits typically appear asESTABLISHEDconnections to Tor relays (entry/guard nodes) or local loopback endpoints used by Tor components. After the browser is closed and the application tears down connections, Windows TCP/IP behavior often leaves recently closed sockets inTIME_WAIT.
TIME_WAITis a normal TCP state that appears after a connection has been actively closed. It exists to ensure delayed packets from the old session are not misinterpreted as belonging to a new session and to allow proper retransmission of the final ACK if needed. From an investigative standpoint, seeing Tor-related endpoints transition from ESTABLISHED toTIME_WAITstrongly indicates the sessions were terminated and the application is no longer maintaining live network traffic.
By contrast,CLOSE_WAITusually means the remote side has closed but the local application has not fully closed its socket yet,LISTENINGindicates a service waiting for inbound connections, andESTABLISHEDmeans the session is still active.
Therefore,TIME_WAIT (B)best indicates Tor Browser connections have been closed.

68. Frage
Benoy, a security professional at an organization, extracted Apache access log entries to view critical information about all the operations performed on a web server. The Apache access log extracted by Benoy is given below:
"10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458"
Identify the HTTP status code in the Apache access log entry above that indicates the response was successful.

- A. 0
- B. 1.0
- C. +0300

- D. 1

Antwort: D

Begründung:
In the Apache Combined/Custom access log format, the value immediately after the quoted request (here," GET ... HTTP/1.0") is theHTTP status codereturned by the server. In the provided entry, that field is500.
From a forensic analysis standpoint, recognizing field positions matters because investigators correlate client IPs, timestamps, requested resources, and server outcomes to reconstruct attack timelines and identify failed exploitation attempts or misconfigurations.
It is important to note thatsuccessful HTTP responses are typically in the 2xx range, most commonly200 (OK), while3xxindicates redirects,4xxindicates client-side errors (such as 404 Not Found), and5xxindicates server-side failures. Specifically,500represents anInternal Server Error, meaning the server encountered an unexpected condition and could not fulfill the request successfully.
The other options are not HTTP status codes in this entry:+0300is the timezone offset in the timestamp,1.0is the HTTP protocol version, and2019is part of the date. Therefore, the only HTTP status code present-and the correct choice among the options-is500 (B), even though it reflects an error rather than success.

69. Frage
Which of the following data acquisition formats supports the Lempel-Ziv-Markov chain (LZMA) algorithm for compression?

- A. Advanced ForensicFramework 4
- B. Proprietary Format
- C. Advanced Forensics Format
- D. Raw Format

Antwort: A

Begründung:
In digital forensics, acquisition formats differ mainly in how they store evidence data, metadata, and whether they support features like compression, segmentation, and integrity verification. ARaw formatis a sector-by- sector bitstream image (often called "dd" style) and typically doesnotdefine built-in compression or structured metadata; any compression would be external to the format. "Proprietary format" is not a single defined standard-some proprietary images may compress data, but the option is too generic and not tied to a specific, documented compression method.
The format known in forensic documentation for explicitly supporting modern compression such asLZMAisAFF4 (Advanced Forensic Format 4), which is designed as a next-generation container supporting rich metadata, hashing, chunked storage, and pluggable compression options. AFF4's architecture stores evidence in compressed chunks/streams and commonly associates LZMA with efficient, high-ratio compression while preserving forensic requirements such as repeatable verification through cryptographic hashes.
The option "Advanced ForensicFramework 4" corresponds toAFF4in many exam question banks and training materials. Therefore, the correct choice isC, because AFF4 is the acquisition format recognized for supportingLZMA compressionas part of its standardized capabilities.

70. Frage
Below is the syntax of a command-line utility that displays active TCP connections and ports on which the computer is listening.
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
Identify the netstat parameter that displays active TCP connections and includes the process ID (PID) for each connection.

- A. [-s]
- B. [-n]
- C. [-a]
- D. [-o]

Antwort: D

Begründung:
In Windows forensics and incident response, investigators often need to linknetwork activity(remote IPs, ports, connection states) to theresponsible processto determine whether traffic is legitimate or associated with malware, unauthorized tools, or data exfiltration.
The Windowsnetstatutility can enumerate current TCP connections and listening ports, but the key flag that enables attribution to a running program is-o. The-o parameter instructs netstat to include theOwning Process ID (PID)with each connection or listening

socket.
Once the PID is known, examiners can correlate it with process listings (e.g., Task Manager,tasklist, memory forensics output) to identify the executable name, path, user context, and parent process-critical steps in reconstructing attacker behavior and persistence.
The other options do not provide PID mapping:-nshows addresses and ports in numeric form (useful for speed and to avoid DNS lookups),-adisplays all connections and listening ports but without PID attribution by itself, and-sshows protocol statistics rather than per-connection ownership. Therefore, the parameter that shows active connectionsandincludes the PID for each is[-o](Option C).

71. Frage
Which of the following file systems of Windows replaces the first letter of a deleted file name with the hex byte code "e5h"?

- A. EFS
- B. FAT
- C. NTFS
- D. FHS

Antwort: B

Begründung:
InFAT (File Allocation Table)file systems (FAT12/16/32), directory entries are fixed-size records that include an8.3 filename field. When a file is deleted, FAT typically does not immediately erase the file's content; instead, it marks the directory entry as deleted by replacing thefirst character of the filenamewith the special marker byte0xE5(often written asE5h). This is a key forensic behavior because it means the file's metadata entry may still be present in the directory table, and the data clusters may remain recoverable until they are reused and overwritten. Examiners can often reconstruct the original filename's first character only through context or by correlating other artifacts, but the remainder of the directory entry (timestamps, size, starting cluster) can still assist recovery.
The other options do not match this mechanism.NTFSuses Master File Table records and marks deletions differently (file record flags and index changes), not by overwriting the first filename byte with E5h.EFSis an encryption feature layered on NTFS, not a distinct file system deletion marker.FHSis a UNIX/Linux directory layout standard, unrelated to Windows disk structures.
Therefore, the correct answer isFAT (A).

72. Frage
.....

- 112-57 Ressourcen Prüfung - 112-57 Prüfungsguide - 112-57 Beste Fragen □ Suchen Sie auf der Webseite （ www.zertpruefung.ch ） nach ➽ 112-57 □ und laden Sie es kostenlos herunter □112-57 Schulungsangebot
- 112-57 Ressourcen Prüfung - 112-57 Prüfungsguide - 112-57 Beste Fragen □ Suchen Sie auf □ www.itzert.com □ nach ➥ 112-57 □ und erhalten Sie den kostenlosen Download mühelos □112-57 Lerntipps
- Wir machen 112-57 leichter zu bestehen! □ [www.deutschpruefung.com] ist die beste Webseite um den kostenlosen Download von 「 112-57 」 zu erhalten □112-57 Deutsche
- flynnesjw673910.estate-blog.com, tiffanymmgl597037.blog-eye.com, www.fuxinwang.com, laytnksba684369.bloggazza.com, cormacaodl783421.izrablog.com, sabrinaslsi134149.bloggerchest.com, denisfewb671157.buyoutblog.com, www.stes.tyc.edu.tw, umairfnxe335483.wikitelevisions.com, funny-lists.com, Disposable vapes