Pass Guaranteed Quiz 112-57 - EC-Council Digital Forensics Essentials (DFE) Marvelous Latest Exam Registration

D|FE
Digital Forensics Essentials
Begin Your Cybersecurity Journey with Hands-On, Foundational Skills in Digital Forensics
Video Lessons • Hands-on Labs • CTF Challenges • Proctored Exam

BONUS!!! Download part of DumpsFree 112-57 dumps for free: https://drive.google.com/open?id=1ED0voDF8WPb5WFSVh2WdExKm6SV9QZMB

There are many other advantages. To gain a full understanding of our product please firstly look at the introduction of the features and the functions of our 112-57 exam torrent. The page of our product provide the demo and the aim to provide the demo is to let the you understand part of our titles before their purchase and see what form the software is after the you open it. The client can visit the page of our product on the website. So the client can understand our 112-57 Quiz torrent well and decide whether to buy our product or not at their wishes. The client can see the forms of the answers and the titles.

Customizable EC-Council Digital Forensics Essentials (DFE) (112-57) practice tests (desktop and web-based) of DumpsFree are made to ensure excellent practice of applicants. Users can take multiple 112-57 practice exams. And the previous exam progress can be saved, so candidates can track it easily whenever they want to see the mistakes. The exam is tough to pass, and that's why 112-57 provides our customers with all the best EC-COUNCIL 112-57 exam dumps to pass the exam on the first try.

>> Latest 112-57 Exam Registration <<

Reliable 112-57 Test Topics & 112-57 Reliable Exam Test

DumpsFree provides EC-Council Digital Forensics Essentials (DFE) (112-57) practice tests (desktop and web-based) to its valuable customers so they get the awareness of the EC-Council Digital Forensics Essentials (DFE) (112-57) certification exam format. Likewise, EC-Council Digital Forensics Essentials (DFE) (112-57) exam preparation materials for EC-Council Digital Forensics Essentials (DFE) (112-57) exam can be downloaded instantly after you make your purchase.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 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.
Topic 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.
Topic 3	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
Topic 4	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.

Topic 5	- 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 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.
Topic 7	- Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Topic 8	- 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.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q12-Q17):

NEW QUESTION # 12
Which of the following folders of macOS stores all the files, documents, applications, library folders, etc.
pertaining to a particular user?

- A. Finder
- B. Spotlight
- C. Home Directory
- D. Time Machine

Answer: C

Explanation:
In macOS, each user account is assigned aHome Directorythat serves as the primary container for that user's data and profile-specific configuration. This directory typically resides under/Users/<username>/and includes standard subfolders such asDesktop,Documents,Downloads,Pictures,Movies,Music, and crucially the user' sLibraryfolder (~/Library). From a digital forensics standpoint, the Home Directory is one of the most important evidence locations because it holds user-generated content and a large volume of user activity artifacts: application preferences and settings (plist files), browser data, caches, saved state, key application databases, recent items, and other per-user traces. Although some applications are installed system-wide under /Applications, macOS also supports per-user application storage and extensive per-user data under the Home Directory's Library structure.
The other options are not user-data containers.Spotlightis a search/indexing service (it creates indexes, not a user's complete data store).Time Machineis a backup mechanism that stores versioned backups rather than the live per-user working directory.Finderis the graphical file manager, not a storage folder. Therefore, the folder that stores files and user-specific libraries for a particular user is theHome Directory (D).

NEW QUESTION # 13
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. ESTABLISHED
- D. CLOSE_WAIT

Answer: B

Explanation:
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.

NEW QUESTION # 14
Wesley, a professional hacker, deleted a confidential file in a compromised system using the "/bin/rm/" command to deny access to forensic specialists.
Identify the operating system on which Don has performed the file carving act.

- A. Linux
- B. Mac OS
- C. Windows
- D. Android

Answer: A

Explanation:
The command path /bin/rm is a hallmark of UNIX/POSIX-style operating systems, where core userland utilities are commonly stored under directories such as /bin, /sbin, and /usr/bin. The utility rm (remove) is the standard UNIX command used to delete directory entries that reference a file's data blocks on disk. This layout and command structure do not match Windows, whichuses different filesystem conventions (drive letters, backslashes, and Windows-native executables) and does not provide /bin/rm as a native path. Android, while Linux-kernel-based, typically exposes shell utilities through environments like /system/bin (and newer systems may use toybox/busybox variants), not the classic /bin hierarchy expected on general-purpose UNIX systems. Between the remaining options, both Linux and macOS are UNIX-like and can include an rm command; however, in digital forensics training and examination contexts, the explicit reference to /bin/rm is most commonly used to indicate a Linux/UNIX command-line environment on a compromised host.
Therefore, the best single-choice answer from the provided options is Linux (D).

NEW QUESTION # 15
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. +0300
- B. 0
- C. 1
- D. 1.0

Answer: C

Explanation:
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.

NEW QUESTION # 16

Sandra, a hacker, targeted Johana, a software professional, to steal her banking details. She started sending frequent, random pop-up messages with malicious links to her social media page. Johana accidentally clicked on a link, causing a malicious program to get installed in her system. Subsequently, when Johana attempted to access her banking website, the URL redirected her to a malicious website controlled by Sandra. Johana entered her banking credentials on the fake website, which Sandra then captured.

Identify the type of attack performed by Sandra on Johana.

- A. Tailgating
- B. Pharming
- C. Shoulder surfing
- D. Dumpster diving

Answer: B

Explanation:

The scenario describes a victim beingredirected from a legitimate banking URL to a fraudulent websitewithout intending to visit it, after malware is installed on the system. This behavior is characteristic ofpharming, an attack in which an adversarycauses redirectionto a malicious destination even when the user types the correct address or clicks a legitimate bookmark. In digital forensics references, pharming is commonly achieved by manipulatingname resolution or routing mechanisms, such as altering the localhosts file, changingDNS server settings, poisoning DNS responses, modifying browser proxy settings, or installing malware that intercepts and rewrites web requests. The key forensic indicator is that the victim's request for the real domain is transparently diverted to attacker-controlled infrastructure, where credentials are harvested through a convincing spoofed login page.

The other options do not match the redirection-and-fake-site mechanism.Tailgatingis physical access abuse (following someone into a secure area).Dumpster divinginvolves retrieving sensitive information from discarded materials.Shoulder surfingis observing credentials by watching the victim type. Because the essential action here ismalicious redirection to a fake site to steal credentials, the correct answer isPharming (A).

NEW QUESTION # 17

......

- Test 112-57 Topics Pdf □ Practice 112-57 Mock □ New 112-57 Dumps Free □ Open website □ www.examcollectionpass.com □ and search for ✔ 112-57 □✔□ for free download □Exam 112-57 Collection
- New 112-57 Dumps Free □ 112-57 Passing Score Feedback □ Practice 112-57 Mock □ □ www.pdfvce.com □ is best website to obtain ➠ 112-57 □ for free download □New 112-57 Dumps Sheet
- Vce 112-57 Free □ Test 112-57 Cram Pdf □ 112-57 Mock Test 〜 Search on ⇛ www.practicevce.com ⇚ for ✔ 112-57 □✔□ to obtain exam materials for free download □Vce 112-57 Free
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.dibiz.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, wjhsd.instructure.com, 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, 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, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by DumpsFree: https://drive.google.com/open?id=1ED0voDF8WPb5WFSVh2WdExKm6SV9QZMB