

Excellent WGU Valid Dumps Files–100% Pass-Rate Digital-Forensics-in-Cybersecurity Reliable Test Sample

12/27/24, 6:31 PM WGU C840 Digital Forensics in Cybersecurity 2025 Complete Questions And Verified Answers/ Complete Solutions With Rati...

Get 20% off Quizlet Plus after free trial Claim discount

WGU C840 Digital Forensics in Cybersecurity 2025 Complete Questions And Verified Answers/ Complete Solutions With Rationales |Get It 100% Accurate!! Already graded A+

Practice questions for this set

Learn

Studied 7 terms

Nice work, you're crushing it

Continue studying in Learn

Terms in this set (182)

The Computer Security Act of 1987	Passed to improve the security and privacy of sensitive information in federal computer systems. The law requires the establishment of minimum acceptable security practices, creation of computer security plans, and training of system users or owners of facilities that house sensitive information.
-----------------------------------	---

<https://quizlet.com/988476600/wgu-c840-digital-forensics-in-cybersecurity-2025-complete-questions-and-verified-answers-complete-solutions-wit...> 1/16

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by DumpsTorrent: <https://drive.google.com/open?id=1uTXZs7zVPOz5jqf2uAU6HoP6KqPoIKrU>

The Digital Forensics in Cybersecurity (D431/C840) Course Exam (Digital-Forensics-in-Cybersecurity) certification exam is a valuable credential that is designed to validate the candidates' skills and knowledge level. The Digital-Forensics-in-Cybersecurity certification exam is one of the high in demand industrial recognized credentials to prove your skills and knowledge level. With the WGU Digital-Forensics-in-Cybersecurity Certification Exam everyone can upgrade their skills and become competitive and updated in the market.

We are a group of IT experts to provide professional study materials to people preparing WGU certification exam. There are free demo you can download to check the accuracy of our Digital-Forensics-in-Cybersecurity Brandumps. It just needs to take one or two days to practice DumpsTorrent Digital-Forensics-in-Cybersecurity dumps torrent and review the key points of our pass guide. Clearing exam is 100% guaranteed.

>> Digital-Forensics-in-Cybersecurity Valid Dumps Files <<

Free PDF Quiz WGU - Digital-Forensics-in-Cybersecurity - Digital Forensics in Cybersecurity (D431/C840) Course Exam Pass-Sure Valid Dumps Files

When you choose Digital-Forensics-in-Cybersecurity valid study pdf, you will get a chance to participate in the simulated exam before you take your actual test. The contents of Digital-Forensics-in-Cybersecurity exam torrent are compiled by our experts through several times of verification and confirmation. So the Digital-Forensics-in-Cybersecurity questions & answers are valid and reliable to use. You can find all the key points in the Digital-Forensics-in-Cybersecurity practice torrent. Besides, the Digital-Forensics-in-Cybersecurity test engine training equipped with various self-assessment functions like exam history, result scores and time setting, etc.

WGU Digital-Forensics-in-Cybersecurity Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> Domain Recovery of Deleted Files and Artifacts: This domain measures the skills of Digital Forensics Technicians and focuses on collecting evidence from deleted files, hidden data, and system artifacts. It includes identifying relevant remnants, restoring accessible information, and understanding where digital traces are stored within different systems.
Topic 2	<ul style="list-style-type: none"> Domain Incident Reporting and Communication: This domain measures the skills of Cybersecurity Analysts and focuses on writing incident reports that present findings from a forensic investigation. It includes documenting evidence, summarizing conclusions, and communicating outcomes to organizational stakeholders in a clear and structured way.
Topic 3	<ul style="list-style-type: none"> Domain Evidence Analysis with Forensic Tools: This domain measures skills of Cybersecurity technicians and focuses on analyzing collected evidence using standard forensic tools. It includes reviewing disks, file systems, logs, and system data while following approved investigation processes that ensure accuracy and integrity.
Topic 4	<ul style="list-style-type: none"> Domain Legal and Procedural Requirements in Digital Forensics: This domain measures the skills of Digital Forensics Technicians and focuses on laws, rules, and standards that guide forensic work. It includes identifying regulatory requirements, organizational procedures, and accepted best practices that ensure an investigation is defensible and properly executed.
Topic 5	<ul style="list-style-type: none"> Domain Digital Forensics in Cybersecurity: This domain measures the skills of Cybersecurity technicians and focuses on the core purpose of digital forensics in a security environment. It covers the techniques used to investigate cyber incidents, examine digital evidence, and understand how findings support legal and organizational actions.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q57-Q62):

NEW QUESTION # 57

Tom saved a message using the least significant bit (LSB) method in a sound file and uploaded this sound to his own website. What is the carrier in this example?

- A. The message
- B. Tom's website
- C. The least significant bit method
- D. The sound file

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In steganography, the carrier is the file or medium used to hide the secret message. In this example, the sound file is the carrier because it contains the hidden message embedded using the least significant bit method. The message is the payload, and the website is merely the distribution platform.

* LSB is the embedding technique, not the carrier.

* The message is the payload, not the carrier.

* The website is not involved in data hiding.

NIST and steganography references clearly define the carrier as the container holding the hidden data.

NEW QUESTION # 58

A forensic examiner is reviewing a laptop running OS X which has been compromised. The examiner wants to know if any shell commands were executed by any of the accounts.

Which log file or folder should be reviewed?

- A. /var/log
- B. /var/vm
- C. /Users/<user>/.bash_history
- D. /Users/<user>/Library/Preferences

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The .bash_history file located in each user's home directory (e.g., /Users/<user>/.bash_history) records the history of shell commands entered by the user in bash shell sessions. Reviewing this file allows investigators to see the commands executed by a specific user.

* /var/vm contains virtual memory swap files, not command history.

* /var/log contains system logs but not individual user shell command history.

* /Users/<user>/Library/Preferences stores application preferences.

NIST guidelines and macOS forensics literature confirm .bash_history as the standard location for shell command histories on OS X systems.

NEW QUESTION # 59

Which tool should a forensic investigator use to determine whether data are leaving an organization through steganographic methods?

- A. Data Encryption Standard (DES)
- B. Netstat
- C. MP3Stego
- D. Forensic Toolkit (FTK)

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Netstat is a command-line network utility tool used to monitor active network connections, open ports, and network routing tables.

In the context of detecting data exfiltration potentially using steganographic methods, netstat can help a forensic investigator identify suspicious or unauthorized network connections through which hidden data may be leaving an organization.

* While netstat itself does not detect steganography within files, it can be used to monitor data flows and connections to external hosts, which is critical for identifying channels where steganographically hidden data could be transmitted.

* Data Encryption Standard (DES) is a cryptographic algorithm, not a forensic tool.

* MP3Stego is a steganography tool for embedding data in MP3 files and is not designed for detection or monitoring.

* Forensic Toolkit (FTK) is a forensic analysis software focused on acquiring and analyzing data from storage devices, not network monitoring.

Reference: NIST Special Publication 800-86 (Guide to Integrating Forensic Techniques into Incident Response) emphasizes the importance of network monitoring tools like netstat during forensic investigations to detect unauthorized data transmissions. Although steganographic detection requires specialized analysis, identifying suspicious network activity is the first step in uncovering covert channels used for data exfiltration.

NEW QUESTION # 60

Which file stores local Windows passwords in the Windows\System32\ directory and is subject to being cracked by using a live CD?

- A. IPsec
- B. SAM
- C. Ntldr
- D. HAL

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The SAM (Security Account Manager) file located in the Windows\System32\config directory stores hashed local user account passwords. It can be accessed and extracted using a live CD or bootable forensic tool, which allows the forensic investigator to bypass the running operating system and avoid altering the evidence.

* IPsec is related to network security policies, not password storage.

* HAL (Hardware Abstraction Layer) is a system file managing hardware interaction.

* Ntldr is a boot loader file in Windows NT systems.

Cracking password hashes extracted from the SAM file is a common forensic practice to recover user passwords during investigations.

Reference: NIST Special Publication 800-86 and Windows forensic textbooks confirm that the SAM file is the repository of local password hashes accessible via forensic live CDs or imaging.

NEW QUESTION # 61

A forensic scientist arrives at a crime scene to begin collecting evidence.

What is the first thing the forensic scientist should do?

- A. Run antivirus scans
- B. Seize the computer immediately
- C. Photograph all evidence in its original place
- D. Document user passwords

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Documenting the scene through photographs preserves the original state of evidence before it is moved or altered. This supports chain of custody and evidence integrity, providing context during analysis and court proceedings.

* Photographic documentation is a standard step in forensic protocols.

* It ensures the scene is accurately recorded.

Reference: According to forensic investigation standards (NIST SP 800-86), photographing the scene is the initial action upon arrival.

NEW QUESTION # 62

.....

Maybe you often come up with great new ideas from daydream, but you can not do anything. Do you have some trouble passing WGU Digital-Forensics-in-Cybersecurity Exam? Turn on your computer, click DumpsTorrent. Then, you will find the dumps torrent you need. After you purchase our products, we provide free updates for a year. 100% guarantee to get the certification.

Digital-Forensics-in-Cybersecurity Reliable Test Sample: <https://www.dumpstorrent.com/Digital-Forensics-in-Cybersecurity-exam-dumps-torrent.html>

- Download Digital-Forensics-in-Cybersecurity Demo Digital-Forensics-in-Cybersecurity Examcollection Vce Relevant Digital-Forensics-in-Cybersecurity Questions Go to website www.pdfdumps.com open and search for Digital-Forensics-in-Cybersecurity to download for free Digital-Forensics-in-Cybersecurity Valid Practice Questions
- Valid Digital-Forensics-in-Cybersecurity Exam Tutorial Digital-Forensics-in-Cybersecurity Examcollection Vce Digital-Forensics-in-Cybersecurity Valid Exam Sims Search on www.pdfvce.com for { Digital-Forensics-in-Cybersecurity } to obtain exam materials for free download Digital-Forensics-in-Cybersecurity Detailed Study Dumps
- Digital-Forensics-in-Cybersecurity Free Download Pdf - Digital-Forensics-in-Cybersecurity Exam Study Guide - Digital-Forensics-in-Cybersecurity Exam Targeted Training The page for free download of Digital-Forensics-in-Cybersecurity on www.examcollectionpass.com will open immediately Digital-Forensics-in-Cybersecurity Vce Torrent
- 2026 The Best 100% Free Digital-Forensics-in-Cybersecurity – 100% Free Valid Dumps Files | Digital Forensics in Cybersecurity (D431/C840) Course Exam Reliable Test Sample Search for Digital-Forensics-in-Cybersecurity on www.pdfvce.com immediately to obtain a free download Digital-Forensics-in-Cybersecurity Vce Torrent
- Latest Digital-Forensics-in-Cybersecurity Valid Dumps Files - Passing Digital-Forensics-in-Cybersecurity Exam is No More

