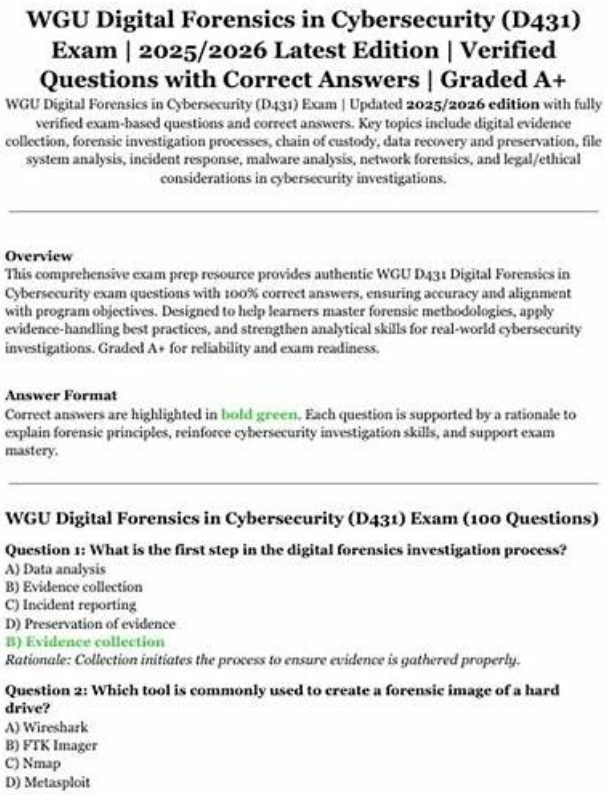
2026 WGU Perfect Exam Digital-Forensics-in-Cybersecurity Tutorial



WGU Digital Forensics in Cybersecurity (D431) Exam | 2025/2026 Latest Edition | Verified Questions with Correct Answers | Graded A+

WGU Digital Forensics in Cybersecurity (D431) Exam | Updated **2025/2026 edition** with fully verified exam-based questions and correct answers. Key topics include digital evidence collection, forensic investigation processes, chain of custody, data recovery and preservation, file system analysis, incident response, malware analysis, network forensics, and legal/ethical considerations in cybersecurity investigations.

Overview

This comprehensive exam prep resource provides authentic WGU D431 Digital Forensics in Cybersecurity exam questions with 100% correct answers, ensuring accuracy and alignment with program objectives. Designed to help learners master forensic methodologies, apply evidence-handling best practices, and strengthen analytical skills for real-world cybersecurity investigations. Graded A+ for reliability and exam readiness.

Answer Format

Correct answers are highlighted in **bold green**. Each question is supported by a rationale to explain forensic principles, reinforce cybersecurity investigation skills, and support exam mastery.

WGU Digital Forensics in Cybersecurity (D431) Exam (100 Questions)

Question 1: What is the first step in the digital forensics investigation process?
A) Data analysis
B) Evidence collection
C) Incident reporting
D) Preservation of evidence
B) Evidence collection
Rationale: Collection initiates the process to ensure evidence is gathered properly.

Question 2: Which tool is commonly used to create a forensic image of a hard drive?
A) Wireshark
B) FTK Imager
C) Nmap
D) Metasploit

BONUS!!! Download part of GuideTorrent Digital-Forensics-in-Cybersecurity dumps for free: https://drive.google.com/open?id=1Pmm7Q_cA9kaqRowvFQj5LRIERq45GeDS

Our experts have devised a set of exam like Digital-Forensics-in-Cybersecurity practice tests for the candidates who want to ensure the highest percentage in real exam. Doing them make sure your grasp on the syllabus content that not only imparts confidence to you but also develops your time management skills for solving the test comprise given time lim. Digital-Forensics-in-Cybersecurity Practice Tests comprise a real exam like scenario and are amply fruitful to make sure a memorable success in Digital-Forensics-in-Cybersecurity exam.

GuideTorrent insists on providing you with the best and high quality exam dumps, aiming to ensure you 100% pass in the actual test. Being qualified with WGU certification will bring you benefits beyond your expectation. Our WGU Digital-Forensics-in-Cybersecurity practice training material will help you to enhance your specialized knowledge and pass your actual test with ease. Digital-Forensics-in-Cybersecurity Questions are all checked and verified by our professional experts. Besides, the Digital-Forensics-in-Cybersecurity answers are all accurate which ensure the high hit rate.

>> Exam Digital-Forensics-in-Cybersecurity Tutorial <<

Digital-Forensics-in-Cybersecurity Exam Pass Guide - Digital-Forensics-in-Cybersecurity Exam Sample

Our Digital-Forensics-in-Cybersecurity practice dumps are suitable for exam candidates of different degrees, which are compatible whichever level of knowledge you are in this area. These Digital-Forensics-in-Cybersecurity training materials win honor for our company, and we treat it as our utmost privilege to help you achieve your goal. Meanwhile, you cannot divorce theory from practice, but do not worry about it, we have Digital-Forensics-in-Cybersecurity stimulation questions for you, and you can both learn and practice at the same time.

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

Topic	Details
Topic 1	• 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 2	• 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	• 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	• 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.
Topic 5	• 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.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q65-Q70):

NEW QUESTION # 65
A company has identified that a hacker has modified files on one of the company's computers. The IT department has collected the storage media from the hacked computer.
Which evidence should be obtained from the storage media to identify which files were modified?

- A. Private IP addresses
- B. Public IP addresses
- C. Operating system version
- D. File timestamps

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
File timestamps, including creation time, last modified time, and last accessed time, are fundamental metadata attributes stored with each file on a file system. When files are modified, these timestamps usually update, providing direct evidence about when changes occurred. Examining file timestamps helps forensic investigators identify which files were altered and estimate the time of unauthorized activity.
* IP addresses (private or public) are network-related evidence, not stored on the storage media's files directly.

* Operating system version is system information but does not help identify specific file modifications.
* Analysis of file timestamps is a standard forensic technique endorsed by NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response) for determining file activity and changes on digital media.

NEW QUESTION # 66
Which type of information does a Windows SAM file contain?

- A. Encrypted network passwords
- B. Hash of local Windows passwords
- C. Hash of network passwords
- D. Encrypted local Windows passwords

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Windows Security Account Manager (SAM) file stores hashed passwords for local Windows user accounts. These hashes are used to authenticate users without storing plaintext passwords.
* The SAM file stores local account password hashes, not network passwords.
* Passwords are hashed (not encrypted) using algorithms like NTLM or LM hashes.
* Network password management occurs elsewhere (e.g., Active Directory).
Reference:NIST SP 800-86 and standard Windows forensics texts explain that the SAM file contains hashed local account credentials critical for forensic investigations involving Windows systems.

NEW QUESTION # 67
An employee sends an email message to a fellow employee. The message is sent through the company's messaging server.
Which protocol is used to send the email message?

- A. SNMP
- B. IMAP
- C. POP3
- D. SMTP

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
SMTP (Simple Mail Transfer Protocol) is the protocol used to send email messages from a client to a mail server or between mail servers. It handles the transmission of outgoing mail. IMAP and POP3 are protocols used for retrieving email, not sending it. SNMP is used for network management.
* IMAP and POP3 are for receiving emails.
* SNMP is unrelated to email delivery.
This is documented in RFC 5321 and supported by all standard email system operations, including forensic analyses.

NEW QUESTION # 68
A police detective investigating a threat traces the source to a house. The couple at the house shows the detective the only computer the family owns, which is in their son's bedroom. The couple states that their son is presently in class at a local middle school.
How should the detective legally gain access to the computer?

- A. Obtain consent to search from the parents
- B. Search immediately without consent due to emergency
- C. Get a warrant without consent
- D. Wait for the son to return and ask for consent

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

To legally search the computer located in the home, the detective must obtain consent from someone with authority over the premises - in this case, the parents. Parental consent is generally sufficient for searches within their household unless other legal considerations apply. This ensures compliance with constitutional protections against unlawful searches.
* Obtaining valid consent is a fundamental requirement under the Fourth Amendment for legal search and seizure.
* Forensic investigators must avoid searches without proper consent or a warrant to maintain admissibility of evidence.
Reference:NIST SP 800-101 and standard forensic ethics protocols emphasize obtaining lawful consent or warrants prior to accessing digital evidence.

NEW QUESTION # 69
A user at a company attempts to hide the combination to a safe that stores confidential information in a data file called vacationdetails.doc.
What is vacationdetails.doc called, in steganographic terms?

- A. Snow
- B. Payload
- C. Carrier
- D. Channel

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In steganography, the file that hides secret information is called thecarrier. The carrier file appears normal and contains embedded hidden data (the payload).
* Payload refers to the actual secret data hidden inside the carrier.
* Snow refers to random noise or artifacts, often in images or files.
* Channel refers to the medium or communication path used to transmit data.
Thus,vacationdetails.docis the carrier file containing the hidden information.
Reference:Standard steganography literature and forensic documentation define the carrier as the file used to conceal payload data.

NEW QUESTION # 70
.....

We know deeply that a reliable Digital-Forensics-in-Cybersecurity exam material is our company's foothold in this competitive market. High accuracy and high quality are the most important things we always looking for. We understand our candidates have no time to waste, everyone wants an efficient learning. So we take this factor into consideration, develop the most efficient way for you to prepare for the Digital-Forensics-in-Cybersecurity exam, that is the real questions and answers practice mode, firstly, it simulates the real Digital Forensics in Cybersecurity (D431/C840) Course Exam test environment perfectly, which offers greatly help to our customers. Secondly, it includes printable PDF Format, also the instant access to download make sure you can study anywhere and anytime. All in all, high efficiency of Digital-Forensics-in-Cybersecurity Exam Material is the reason for your selection.

- Digital-Forensics-in-Cybersecurity Dumps Collection □ Exam Sample Digital-Forensics-in-Cybersecurity Online □ Real Digital-Forensics-in-Cybersecurity Exams □ Easily obtain ⇛ Digital-Forensics-in-Cybersecurity ⇚ for free download through [www.pdfvce.com] □Exam Sample Digital-Forensics-in-Cybersecurity Online
- Excellent Exam Digital-Forensics-in-Cybersecurity Tutorial | Amazing Pass Rate For Digital-Forensics-in-Cybersecurity: Digital Forensics in Cybersecurity (D431/C840) Course Exam | Fast Download Digital-Forensics-in-Cybersecurity Exam Pass Guide □ Immediately open " www.easy4engine.com " and search for [Digital-Forensics-in-Cybersecurity] to obtain a free download □Digital-Forensics-in-Cybersecurity Reliable Test Objectives
- Test Digital-Forensics-in-Cybersecurity Questions Pdf □ Digital-Forensics-in-Cybersecurity Exam Format □ Digital-Forensics-in-Cybersecurity Exam Format □ Immediately open ☀ www.pdfvce.com □☀□ and search for □ Digital-Forensics-in-Cybersecurity □ to obtain a free download □Certification Digital-Forensics-in-Cybersecurity Exam Infor
- Digital-Forensics-in-Cybersecurity Dumps Collection □ Digital-Forensics-in-Cybersecurity Test Guide Online □ Certification Digital-Forensics-in-Cybersecurity Exam Infor □ Search for ⇛ Digital-Forensics-in-Cybersecurity ⇚ and download it for free immediately on ⇛ www.troytecdumps.com ⇚ □Test Digital-Forensics-in-Cybersecurity Questions Pdf
- Quiz 2026 Digital-Forensics-in-Cybersecurity: Digital Forensics in Cybersecurity (D431/C840) Course Exam –Updated Exam Tutorial □ Open 【 www.pdfvce.com 】 and search for □ Digital-Forensics-in-Cybersecurity □ to download exam materials for free □Digital-Forensics-in-Cybersecurity Dumps Collection
- Real Digital-Forensics-in-Cybersecurity Exams □ Digital-Forensics-in-Cybersecurity Reliable Test Question □ Digital-Forensics-in-Cybersecurity Real Dumps Free □ Immediately open □ www.prep4away.com □ and search for { Digital-Forensics-in-Cybersecurity } to obtain a free download □Digital-Forensics-in-Cybersecurity Dumps Collection
- bookmarkalexa.com, reussirobled.com, www.jygame8.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.fanart-central.net, 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, 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, Disposable vapes

What's more, part of that GuideTorrent Digital-Forensics-in-Cybersecurity dumps now are free: https://drive.google.com/open?id=1Pmm7Q_cA9kaqRowvFQj5LRIERq45GeDS