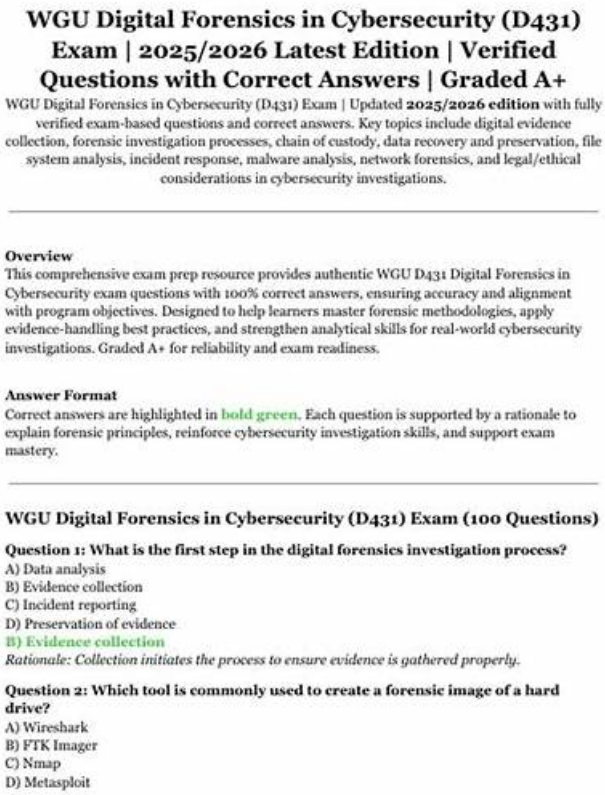
Digital-Forensics-in-Cybersecurity Practice Exams, Latest Edition Test Engine



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

BTW, DOWNLOAD part of ActualVCE Digital-Forensics-in-Cybersecurity dumps from Cloud Storage: https://drive.google.com/open?id=168UAto8d1v86zT1fMjZdUzbX4y7-JF-J

The efficiency of our Digital-Forensics-in-Cybersecurity study materials can be described in different aspects. Digital-Forensics-in-Cybersecurity practice guide is not only financially accessible, but time-saving and comprehensive to deal with the important questions trying to master them efficiently. You can obtain our Digital-Forensics-in-Cybersecurity Preparation engine within five minutes after you pay for it successfully and then you can study with it right away. Besides, if you have any question, our services will solve it at the first time.

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

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 5	• 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.

Digital-Forensics-in-Cybersecurity Test Result | Digital-Forensics-in-Cybersecurity Real Exam

We have three different versions of Digital Forensics in Cybersecurity (D431/C840) Course Exam prep torrent for you to choose, including PDF version, PC version and APP online version. Different versions have their own advantages and user population, and we would like to introduce features of these versions for you. There is no doubt that PDF of Digital-Forensics-in-Cybersecurity exam torrent is the most prevalent version among youngsters, mainly due to its convenience for a demo, through which you can have a general understanding and simulation about our Digital-Forensics-in-Cybersecurity Test Braindumps to decide whether you are willing to purchase or not, and also convenience for paper printing for you to do some note-taking.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q28-Q33):

NEW QUESTION # 28
An organization believes that a company-owned mobile phone has been compromised.
Which software should be used to collect an image of the phone as digital evidence?

- A. Forensic Toolkit (FTK)
- B. Data Doctor
- C. Forensic SIM Cloner
- D. PTFinder

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Forensic Toolkit (FTK) is a widely recognized and trusted software suite in digital forensics used to acquire and analyze forensic images of devices, including mobile phones. FTK supports the creation of bit-by-bit images of digital evidence, ensuring the integrity and admissibility of the evidence in legal contexts. This imaging process is crucial in preserving the original state of the device data without alteration.
* FTK enables forensic investigators to perform logical and physical acquisitions of mobile devices.
* It maintains the integrity of the evidence by generating cryptographic hash values (MD5, SHA-1) to prove that the image is an exact copy.
* Other options such as PTFinder or Forensic SIM Cloner focus on specific tasks like SIM card cloning or targeted data extraction but do not provide full forensic imaging capabilities.

* Data Doctor is more aligned with data recovery rather than forensic imaging.
Reference:According to standard digital forensics methodologies outlined by NIST Special Publication 800-101(Guidelines on Mobile Device Forensics) and the SANS Institute Digital Forensics and Incident Response guides, forensic tools used to acquire mobile device images must be capable of bit-stream copying with hash verification, which FTK provides.

NEW QUESTION # 29
A cybercriminal hacked into an Apple iPad that belongs to a company's chief executive officer (CEO). The cybercriminal deleted some important files on the data volume that must be retrieved.
Which hidden folder will contain the digital evidence?

- A. /etc
- B. /Private/etc
- C. /lost+found
- D. /.Trashes/501

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
On Apple iOS devices, deleted files are often moved to a hidden Trash folder before permanent deletion. The directory/.Trashes/501is a hidden folder where deleted files for user ID 501 (the first user created on macOS /iOS devices) are temporarily stored.
* This folder can contain files marked for deletion and thus is a prime location for recovery attempts.
* /lost+foundis a directory commonly used on Unix/Linux file systems for recovered file fragments after file system corruption but is not the default trash location on iOS.
* /Private/etcand/etccontain system configuration files, not deleted user files.
Reference:Apple forensic investigations per NIST and training manuals such as those from Cellebrite and BlackBag Technologies indicate that user-deleted files on iOS devices reside in.Trashesor similar hidden directories until permanently removed.

NEW QUESTION # 30
A forensics investigator is investigating a Windows computer which may be collecting data from other computers on the network.
Which Windows command line tool can be used to determine connections between machines?

- A. Openfiles
- B. Telnet
- C. Netstat
- D. Xdetect

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Netstatis a standard Windows command line utility that displays active network connections, routing tables, and network interface statistics. It is widely used in forensic investigations to identify current and past TCP/IP connections, including IP addresses and port numbers associated with remote hosts. This information helps investigators identify if the suspect computer has active connections to other machines potentially used for data collection or command and control.
* Telnet is a protocol used to connect to remote machines but does not display current network connections.
* Openfiles shows files opened remotely but not network connection details.
* Xdetect is not a standard Windows tool and not recognized in forensic investigations.
Reference:According to NIST SP 800-86 and SANS Digital Forensics guidelines,netstatis an essential tool for gathering network-related evidence during system investigations.

NEW QUESTION # 31
Thomas received an email stating he needed to follow a link and verify his bank account information to ensure it was secure. Shortly after following the instructions, Thomas noticed money was missing from his account.
Which digital evidence should be considered to determine how Thomas' account information was compromised?

- A. Browser cache
- B. Email messages
- C. Bank transaction logs
- D. Firewall logs

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The email messages, including headers and content, contain information about the phishing attempt, such as sender details and embedded links. Analyzing these messages can help trace the source of the scam and determine the method used to deceive the victim.
* Email headers provide metadata for tracking the origin.
* Forensic examination of emails is fundamental in investigating social engineering and phishing attacks.
Reference:NIST SP 800-101 and forensic email analysis protocols recommend thorough email message examination in phishing investigations.

NEW QUESTION # 32
Which directory contains the system's configuration files on a computer running Mac OS X?

- A. /cfg
- B. /etc
- C. /bin
- D. /var

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The/etcdirectory on Unix-based systems, including macOS, contains important system configuration files and scripts. It is the standard location for system-wide configuration data.
* /varcontains variable data like logs and spool files.
* /bincontains essential binary executables.
* /cfgis not a standard directory in macOS.
This is standard Unix/Linux directory structure knowledge and is reflected in NIST and forensic references for macOS.

NEW QUESTION # 33
.....

Because the effect is outstanding, the Digital-Forensics-in-Cybersecurity study materials are good-sale, every day there are a large number of users to browse our website to provide the Digital-Forensics-in-Cybersecurity study materials, through the screening they buy material meets the needs of their research. Every user cherishes the precious time, seize this rare opportunity, they redouble their efforts to learn, when others are struggling, why do you have any reason to relax? So， quicken your pace, follow the Digital-Forensics-in-Cybersecurity Study Materials, begin to act, and keep moving forward for your dreams!

Digital-Forensics-in-Cybersecurity Passing Score Feedback □ Enter □ www.pdfvce.com □ and search for ➤ Digital-Forensics-in-Cybersecurity □ to download for free □Digital-Forensics-in-Cybersecurity Test Questions Answers

- Exam Digital-Forensics-in-Cybersecurity Flashcards □ Sample Digital-Forensics-in-Cybersecurity Test Online ✏ Digital-Forensics-in-Cybersecurity Reliable Test Practice □ Open 「 www.testkingpass.com 」 enter " Digital-Forensics-in-Cybersecurity " and obtain a free download □Exam Digital-Forensics-in-Cybersecurity Flashcards
- Digital-Forensics-in-Cybersecurity Valid Test Labs □ Digital-Forensics-in-Cybersecurity Exam Outline ☯ Digital-Forensics-in-Cybersecurity Passing Score Feedback □ Easily obtain free download of { Digital-Forensics-in-Cybersecurity } by searching on 《 www.pdfvce.com 》 □Digital-Forensics-in-Cybersecurity Test Questions Answers
- Digital-Forensics-in-Cybersecurity Vce Test Simulator □ Digital-Forensics-in-Cybersecurity Test Fee □ Digital-Forensics-in-Cybersecurity Test Fee □ Enter " www.prepawaypdf.com " and search for ➤ Digital-Forensics-in-Cybersecurity □ to download for free □Sample Digital-Forensics-in-Cybersecurity Test Online
- Digital-Forensics-in-Cybersecurity Vce Test Simulator □ Digital-Forensics-in-Cybersecurity Test Questions Answers □ Test Digital-Forensics-in-Cybersecurity Simulator ↕ Download □ Digital-Forensics-in-Cybersecurity □ for free by simply searching on （ www.pdfvce.com ） □Digital-Forensics-in-Cybersecurity PDF Questions
- Digital-Forensics-in-Cybersecurity PDF Cram Exam □ Digital-Forensics-in-Cybersecurity Vce Test Simulator □ Digital-Forensics-in-Cybersecurity Exam Dumps.zip ☑ Enter 【 www.examcollectionpass.com 】 and search for { Digital-Forensics-in-Cybersecurity } to download for free □Digital-Forensics-in-Cybersecurity Certification Materials
- Digital-Forensics-in-Cybersecurity Dump Check □ Valid Digital-Forensics-in-Cybersecurity Test Cram □ Digital-Forensics-in-Cybersecurity Certification Materials ❊ Easily obtain □ Digital-Forensics-in-Cybersecurity □ for free download through （ www.pdfvce.com ） ↩Digital-Forensics-in-Cybersecurity PDF Questions
- Top Digital-Forensics-in-Cybersecurity Training Questions | Reliable WGU Digital-Forensics-in-Cybersecurity: Digital Forensics in Cybersecurity (D431/C840) Course Exam 100% Pass □ Copy URL □ www.examdiscuss.com □ open and search for ➽ Digital-Forensics-in-Cybersecurity □ to download for free □Digital-Forensics-in-Cybersecurity PDF Cram Exam
- bushranecn450474.wikilentillas.com, alexiaebov958949.wikilinksnews.com, graysonddbb506523.wikinarration.com, carlyexpi840939.bloggazzo.com, www.stes.tyc.edu.tw, joanfkfk757189.wikilowdown.com, ariabookmarks.com, katrinatyxg743702.estate-blog.com, estrategiadedados.evag.com.br, tesseovv002547.losblogos.com, Disposable vapes

P.S. Free & New Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by ActualVCE: https://drive.google.com/open?id=168UAto8d1v86zT1fMjZdUzbX4y7-JF-J