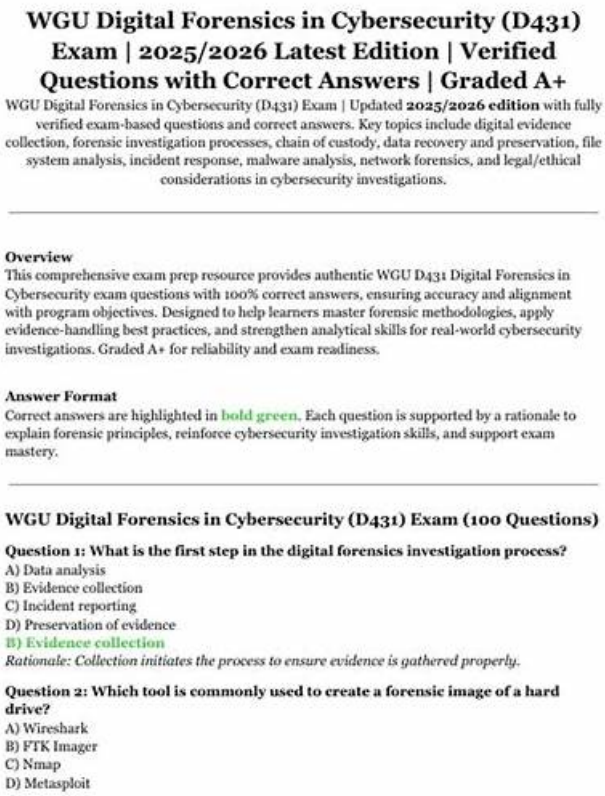
Customizable Exam Questions for Improved Success in WGU Digital-Forensics-in-Cybersecurity Certification Exam



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 PassLeader Digital-Forensics-in-Cybersecurity dumps for free: https://drive.google.com/open?id=1OgqFbZBdO2SRcvoZoGrvT7GJe7eJ-ZHv

Facing all kinds of the Digital-Forensics-in-Cybersecurity learning materials in the market, it's difficult for the candidates to choose the best one. Our Digital-Forensics-in-Cybersecurity learning materials are famous for the high accuracy and high quality. Besides, we provide free update for one year, and pass guarantee and money bach guarantee. We have the free demo for you to know more about our Digital-Forensics-in-Cybersecurity Learning Materials. If you have any questions, you can contact our online service stuff.

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 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 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 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 5	• 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.

Valid Digital Forensics in Cybersecurity (D431/C840) Course Exam Exam Dumps 100% Guarantee Pass Digital Forensics in Cybersecurity (D431/C840) Course Exam Exam

Want to crack the WGU Digital-Forensics-in-Cybersecurity certification test in record time? Look no further than PassLeader! Our updated Digital-Forensics-in-Cybersecurity Dumps questions are designed to help you prepare for the exam quickly and effectively. With study materials available in three different formats, you can choose the format that works best for you. Trust PassLeader to help you pass the WGU Digital-Forensics-in-Cybersecurity Certification test with ease.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q36-Q41):

NEW QUESTION # 36
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. /.Trashes/501
- C. /Private/etc
- D. /lost+found

Answer: B

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 # 37
Which United States law requires telecommunications equipment manufacturers to provide built-in surveillance capabilities for federal agencies?

- A. Communications Assistance to Law Enforcement Act (CALEA)
- B. Electronic Communications Privacy Act (ECPA)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. The Privacy Protection Act (PPA)

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
CALEA mandates that telecommunications equipment and service providers design systems capable of allowing federal law enforcement to conduct authorized electronic surveillance. This includes wiretapping and data interception capabilities.
* This law is essential for lawful monitoring in investigations.
* It affects hardware design and network infrastructure.
Reference:CALEA is consistently referenced in forensic standards concerning lawful interception requirements.

NEW QUESTION # 38
A forensic investigator suspects that spyware has been installed to a Mac OS X computer by way of an update.
Which Mac OS X log or folder stores information about system and software updates?

- A. /var/log/daily.out
- B. /var/spool/cups
- C. /var/vm
- D. /Library/Receipts

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The/Library/Receiptsfolder on Mac OS X contains receipts that track software installation and updates, including system and application updates. This folder helps forensic investigators determine which updates were installed and when, useful for detecting suspicious or unauthorized software installations like spyware.
* /var/spool/cupsis related to printer spooling.
* /var/log/daily.outcontains daily system log summaries but not detailed update records.
* /var/vmcontains virtual memory files.
NIST and Apple forensics documentation indicate that/Library/Receiptsis a key location for examining software installation history.

NEW QUESTION # 39
A digital forensic examiner receives a computer used in a hacking case. The examiner is asked to extract information from the computer's Registry.
How should the examiner proceed when obtaining the requested digital evidence?

- A. Enlist a colleague to witness the investigative process
- B. Investigate whether the computer was properly seized
- C. Download a tool from a hacking website to extract the data
- D. Ensure that any tools and techniques used are widely accepted

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In digital forensics, the use of reliable, validated, and widely accepted tools and techniques is critical to maintain the integrity and admissibility of digital evidence. According to the National Institute of Standards and Technology (NIST) guidelines and the

Scientific Working Group on Digital Evidence (SWGDE) standards, any forensic process must utilize methods that are recognized by the forensic community and have undergone rigorous testing to ensure accuracy and reliability.
* Using validated tools helps prevent evidence contamination or loss and ensures that results can withstand legal scrutiny.
* While proper seizure and witnessing are important, the priority in the extraction phase is to use appropriate, trusted tools.
* Downloading tools from unauthorized or suspicious sources can compromise the evidence and is not an ethical or legal practice.
Reference:NIST SP 800-101 (Guidelines on Mobile Device Forensics) and SWGDE Best Practices emphasize tool validation and adherence to community-accepted methods as foundational principles in forensic examination.

NEW QUESTION # 40
Which storage format is a magnetic drive?

- A. Blu-ray
- B. SATA
- C. SSD
- D. CD-ROM

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
SATA (Serial ATA) refers to an interface standard commonly used for connecting magnetic hard disk drives (HDDs) and solid-state drives (SSDs) to a computer. The term SATA itself describes the connection, but most HDDs that use SATA as an interface are magnetic drives.
* CD-ROM and Blu-ray are optical storage media, not magnetic.
* SSD (Solid State Drive) uses flash memory, not magnetic storage.
* Magnetic drives rely on spinning magnetic platters, which are typically connected via SATA or other interfaces.
This differentiation is emphasized in digital forensic training and hardware documentation, including those from NIST and forensic hardware textbooks.

NEW QUESTION # 41
.....

Exam Practice

- Enhance Your Success Rate with www.pass4test.com's WGU Digital-Forensics-in-Cybersecurity Exam Questions □ The page for free download of ✔ Digital-Forensics-in-Cybersecurity □✔□ on ➤ www.pass4test.com □ will open immediately □Digital-Forensics-in-Cybersecurity Download Demo
- Digital-Forensics-in-Cybersecurity Valid Test Dumps □ New Digital-Forensics-in-Cybersecurity Test Labs □ Digital-Forensics-in-Cybersecurity Exam Torrent □ Easily obtain ☀ Digital-Forensics-in-Cybersecurity □☀□ for free download through ▹ www.pdfvce.com ◃ □Real Digital-Forensics-in-Cybersecurity Question
- Digital-Forensics-in-Cybersecurity Free Test Questions □ Pass Digital-Forensics-in-Cybersecurity Guarantee □ Reliable Digital-Forensics-in-Cybersecurity Exam Practice □ Search for ➥ Digital-Forensics-in-Cybersecurity □ and download it for free on □ www.vceengine.com □ website □Digital-Forensics-in-Cybersecurity Download Demo
- Pass Guaranteed WGU - High Hit-Rate Digital-Forensics-in-Cybersecurity - Dumps Digital Forensics in Cybersecurity (D431/C840) Course Exam Free Download □ ▸ www.pdfvce.com ◂ is best website to obtain □ Digital-Forensics-in-Cybersecurity □ for free download □Reliable Digital-Forensics-in-Cybersecurity Dumps Free
- Hot Dumps Digital-Forensics-in-Cybersecurity Free Download | Valid WGU Digital-Forensics-in-Cybersecurity: Digital Forensics in Cybersecurity (D431/C840) Course Exam 100% Pass □ Download □ Digital-Forensics-in-Cybersecurity □ for free by simply searching on （ www.troytecdumps.com ） ～Digital-Forensics-in-Cybersecurity Reliable Exam Answers
- New Digital-Forensics-in-Cybersecurity Exam Simulator □ Reliable Digital-Forensics-in-Cybersecurity Study Plan □ Questions Digital-Forensics-in-Cybersecurity Pdf □ Search for ➥ Digital-Forensics-in-Cybersecurity □ and obtain a free download on ➥ www.pdfvce.com □ □Digital-Forensics-in-Cybersecurity Reliable Exam Answers
- Hot Dumps Digital-Forensics-in-Cybersecurity Free Download | Valid WGU Digital-Forensics-in-Cybersecurity: Digital Forensics in Cybersecurity (D431/C840) Course Exam 100% Pass □ Enter ✔ www.pass4test.com □✔□ and search for ✔ Digital-Forensics-in-Cybersecurity □✔□ to download for free □Digital-Forensics-in-Cybersecurity Real Dumps
- www.stes.tyc.edu.tw, 47.121.119.212, 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, user.xiaozhongwenhua.top, schoolido.lu, 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.lazxg.top, Disposable vapes

BONUS!!! Download part of PassLeader Digital-Forensics-in-Cybersecurity dumps for free: https://drive.google.com/open?id=1OgqFbZBdO2SRcvoZoGrvT7GJe7eJ-ZHv