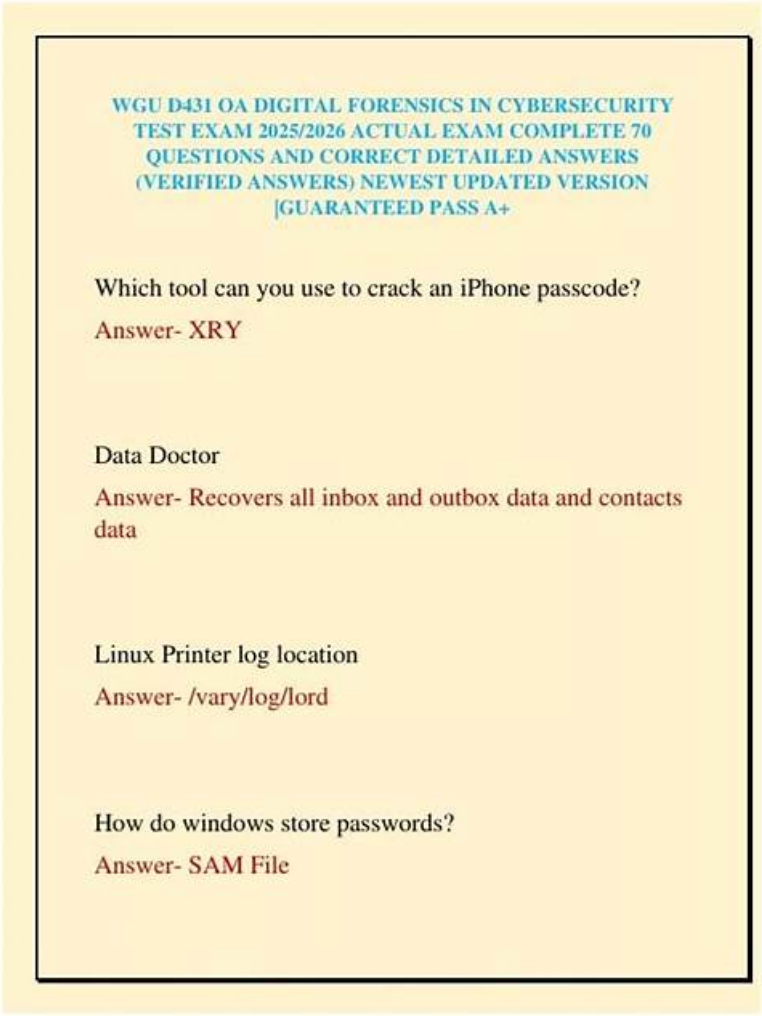
Digital-Forensics-in-Cybersecurity Reliable Test Cost & Latest Digital-Forensics-in-Cybersecurity Test Labs


WGU D431 OA DIGITAL FORENSICS IN CYBERSECURITY TEST EXAM 2025/2026 ACTUAL EXAM COMPLETE 70 QUESTIONS AND CORRECT DETAILED ANSWERS (VERIFIED ANSWERS) NEWEST UPDATED VERSION |GUARANTEED PASS A+

Which tool can you use to crack an iPhone passcode?

Answer- XRY

Data Doctor

Answer- Recovers all inbox and outbox data and contacts data

Linux Printer log location

Answer- /vary/log/lord

How do windows store passwords?

Answer- SAM File

DOWNLOAD the newest VCEPrep Digital-Forensics-in-Cybersecurity PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1VR59PuSpmYuArwb4Z0QspKCykj69zPR4

Preparation should be convenient and authentic so that anyone, be it a working person or a student, can handle the load. But now I have to tell you that all of these can be achieved in our Digital-Forensics-in-Cybersecurity exam preparation materials. The exam preparation materials of VCEPrep Digital-Forensics-in-Cybersecurity are authentic and the way of the study is designed highly convenient. I don't think any other site can produce results that VCEPrep can get. That is why I would recommend it to all the candidates attempting the Digital-Forensics-in-Cybersecurity Exam to use Digital-Forensics-in-Cybersecurity exam preparation materials.

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

Topic	Details
Topic 1	• 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	• 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 3	• 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 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 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.

2026 Digital-Forensics-in-Cybersecurity Reliable Test Cost 100% Pass | High-quality Latest Digital Forensics in Cybersecurity (D431/C840) Course Exam Test Labs Pass for sure

We try our best to renovate and update our WGU Digital-Forensics-in-Cybersecurity study materials in order to help you fill the knowledge gap during your learning process, thus increasing your confidence and success rate. At the same time, WGU Digital-Forensics-in-Cybersecurity Preparation baindumps can keep pace with the digitized world by providing timely application. You will never fell disappointed with our Digital-Forensics-in-Cybersecurity exam quiz.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q55-Q60):

NEW QUESTION # 55
Which file stores local Windows passwords in the Windows\System32\ directory and is subject to being cracked by using a live CD?

- A. Ntidr
- B. SAM
- C. HAL
- D. IPSec

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The SAM (Security Account Manager) file located in theWindows\System32\configdirectory 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.
* Ntidr 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 # 56
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. Firewall logs
- B. Email messages
- C. Browser cache
- D. Bank transaction 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 # 57
Which operating system (OS) uses the NTFS (New Technology File System) file operating system?

- A. Windows 8
- B. Linux
- C. Mac OS X v10.4
- D. Mac OS X v10.5

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
NTFS is the primary file system used by Microsoft Windows operating systems starting from Windows NT and continuing through modern versions including Windows 8. NTFS supports advanced features like file permissions, encryption, and journaling, which are critical for modern OS file management.
* Linux typically uses ext3, ext4, or other native file systems, not NTFS as a primary system.
* Mac OS X v10.4 and v10.5 use HFS+ as the native file system, not NTFS.
* Windows 8 uses NTFS as its default file system.
This is documented in official Microsoft and NIST digital forensics resources.

NEW QUESTION # 58
Which type of information does a Windows SAM file contain?

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

Answer: D

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 # 59
A cybercriminal communicates with his compatriots using steganography. The FBI discovers that the criminal group uses white space to hide data in photographs.
Which tool can the cybercriminals use to facilitate this type of communication?

- A. Steganophony
- B. QuickStego
- C. Wolf
- D. Snow

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Snow is a tool that encodes hidden messages using whitespace characters (spaces and tabs), which can be embedded in text and sometimes in image file metadata or formats that allow invisible characters. It is commonly used to hide data in plain sight, including within digital images.
* Steganophony focuses on hiding data in VoIP.
* Wolf is not recognized as a steganography tool for whitespace.
* QuickStego is another tool for text-based steganography but less commonly associated with whitespace specifically.
Forensic and cybersecurity literature often cites Snow as the preferred tool for whitespace-based steganography.

NEW QUESTION # 60
.....

If you want to pass the exam in the shortest time, our Digital-Forensics-in-Cybersecurity study materials can help you achieve this dream. Our Digital-Forensics-in-Cybersecurity learning quiz according to your specific circumstances, for you to develop a suitable schedule and learning materials, so that you can prepare in the shortest possible time to pass the exam needs everything. If you use our Digital-Forensics-in-Cybersecurity training prep, you only need to spend twenty to thirty hours to practice our Digital-Forensics-in-Cybersecurity study materials, then you are ready to take the exam and pass it successfully.

www.pdfvce.com ） immediately to obtain a free download □Reliable Digital-Forensics-in-Cybersecurity Exam Simulator

- Valid Digital-Forensics-in-Cybersecurity exam dumps ensure you a high Digital-Forensics-in-Cybersecurity passing rate □ Search for □ Digital-Forensics-in-Cybersecurity □ and easily obtain a free download on ➡ www.pass4test.com □□□ □ □Digital-Forensics-in-Cybersecurity PDF Download
- Valid Digital-Forensics-in-Cybersecurity exam dumps ensure you a high Digital-Forensics-in-Cybersecurity passing rate □ Search for { Digital-Forensics-in-Cybersecurity } and easily obtain a free download on ➠ www.pdfvce.com □ □Digital-Forensics-in-Cybersecurity Latest Exam Labs
- 2026 Unparalleled Digital-Forensics-in-Cybersecurity Reliable Test Cost Help You Pass Digital-Forensics-in-Cybersecurity Easily □ Search for （ Digital-Forensics-in-Cybersecurity ） and download it for free immediately on ☀ www.pass4test.com □☀□ □Valid Digital-Forensics-in-Cybersecurity Test Practice
- Quiz Digital-Forensics-in-Cybersecurity - Reliable Digital Forensics in Cybersecurity (D431/C840) Course Exam Reliable Test Cost □ “ www.pdfvce.com ” is best website to obtain { Digital-Forensics-in-Cybersecurity } for free download ➡Valid Real Digital-Forensics-in-Cybersecurity Exam
- New Digital-Forensics-in-Cybersecurity Exam Pattern □ Digital-Forensics-in-Cybersecurity Advanced Testing Engine □ New Digital-Forensics-in-Cybersecurity Exam Pattern □ Search for “ Digital-Forensics-in-Cybersecurity ” and download exam materials for free through □ www.prep4away.com □ □Latest Digital-Forensics-in-Cybersecurity Questions
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, lecture.theibdcbglobal.org, 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, bbs.t-firefly.com, www.stes.tyc.edu.tw, portal.mathtutorofflorida.com, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest VCEPrep Digital-Forensics-in-Cybersecurity PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1VR59PuSpmYuArwb4Z0QspKCykj69zPR4