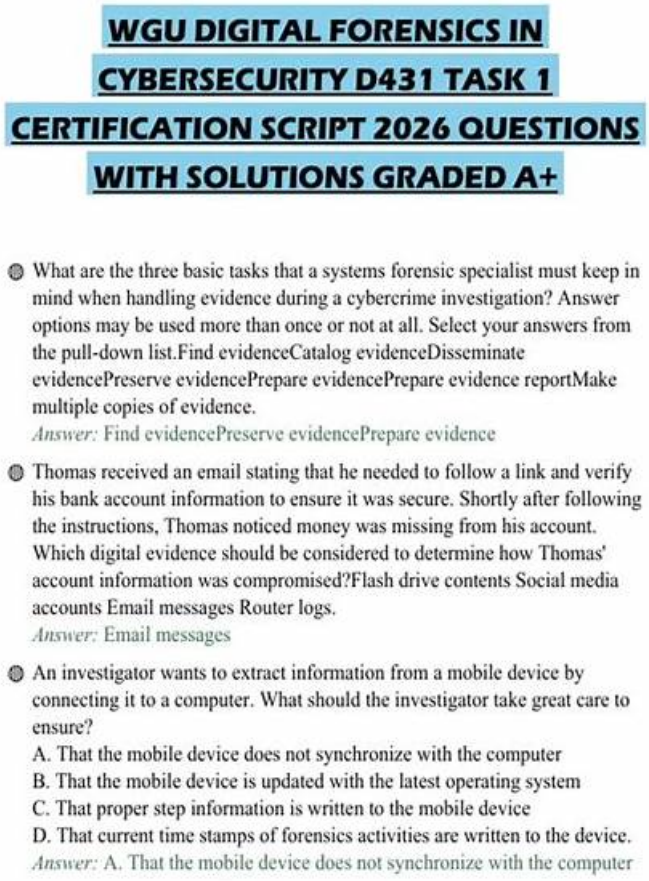
Features of Three Formats WGU Digital-Forensics-in-Cybersecurity Exam Questions


WGU DIGITAL FORENSICS IN CYBERSECURITY D431 TASK 1 CERTIFICATION SCRIPT 2026 QUESTIONS WITH SOLUTIONS GRADED A+

- What are the three basic tasks that a systems forensic specialist must keep in mind when handling evidence during a cybercrime investigation? Answer options may be used more than once or not at all. Select your answers from the pull-down list.Find evidenceCatalog evidenceDisseminate evidencePreserve evidencePrepare evidencePrepare evidence reportMake multiple copies of evidence.
  Answer: Find evidencePreserve evidencePrepare evidence
- Thomas received an email stating that 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?Flash drive contents Social media accounts Email messages Router logs.
  Answer: Email messages
- An investigator wants to extract information from a mobile device by connecting it to a computer. What should the investigator take great care to ensure?
  A. That the mobile device does not synchronize with the computer
  B. That the mobile device is updated with the latest operating system
  C. That proper step information is written to the mobile device
  D. That current time stamps of forensics activities are written to the device.
  Answer: A. That the mobile device does not synchronize with the computer

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=1Ffiucs6PVGvwzNjRuKZZmWgFkZoMiccB

Our WGU Digital-Forensics-in-Cybersecurity Exam Dumps with the highest quality which consists of all of the key points required for the WGU Digital-Forensics-in-Cybersecurity exam can really be considered as the royal road to learning. Lead1Pass has already become a famous brand all over the world in this field since we have engaged in compiling the Digital-Forensics-in-Cybersecurity practice materials for more than ten years and have got a fruitful outcome.

WGU Digital-Forensics-in-Cybersecurity Exam Overview:

Certification Vendor:	WGU (Western Governors University)
Exam Name:	Digital Forensics in Cybersecurity
Exam Number:	D431 / C840
Related Certifications:	Cybersecurity Analyst Digital Forensics Professional
Available Languages:	English
Passing Score:	65%

Exam Format:	Multiple Choice, Multiple Select, Scenario-Based
Certificate Validity Period:	No expiration
Exam Price:	Included in tuition / $0
Exam Duration:	120 minutes
Real Exam Qty:	70–75
Recommended Training:	WGU Course Materials NIST SP 800-86 Guide to Integrating Forensic Techniques
Exam Registration:	WGU Student Portal
Sample Questions:	WGU Digital-Forensics-in-Cybersecurity Sample Questions
Exam Way:	Online proctored assessment
Pre Condition:	Completion of prerequisite IT/cybersecurity courses; enrolled in WGU Cybersecurity program
Official Syllabus URL:	https://www.wgu.edu/online-it-degrees/cybersecurity-information-assurance-bs.html

Valid Digital-Forensics-in-Cybersecurity Vce Dumps - Digital-Forensics-in-Cybersecurity Test Dump

WGU Digital-Forensics-in-Cybersecurity pdf dumps format contains actual Digital-Forensics-in-Cybersecurity exam questions. With WGU Digital-Forensics-in-Cybersecurity pdf questions you don't have to spend a lot of time on Digital Forensics in Cybersecurity (D431/C840) Course Exam Networking Solutions Digital-Forensics-in-Cybersecurity exam preparation. You just go through and memorize these real Digital-Forensics-in-Cybersecurity exam questions. Lead1Pass has designed this set of valid WGU Exam Questions with the assistance of highly qualified professionals. Preparing with these Digital-Forensics-in-Cybersecurity Exam Questions is enough to get success on the first try. However, this format of Lead1Pass Digital-Forensics-in-Cybersecurity exam preparation material is best for those who are too much busy in their life and don't have enough time to prepare for WGU Digital-Forensics-in-Cybersecurity exam.

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 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 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.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q30-Q35):

NEW QUESTION # 30
Which policy is included in the CAN-SPAM Act?

- A. Email sender must include recipient IP address in the email header
- B. Email sender must verify the recipient's consent before sending
- C. Email sender must encrypt all outgoing emails
- D. Email sender must provide a method for recipients to opt out of future emails without charge

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The CAN-SPAM Act requires that commercial emails include a clear and conspicuous mechanism allowing recipients to opt out of receiving future emails. This opt-out method cannot require payment or additional steps that would discourage recipients.
* The act aims to reduce unsolicited commercial emails and spam.
* Compliance is critical for lawful email marketing and forensic investigations involving email misuse.
Reference:U.S. federal law and cybersecurity policies reference CAN-SPAM provisions for email communications.

NEW QUESTION # 31
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. /Private/etc
- B. /lost+found
- C. /etc
- 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 # 32
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. Operating system version
- B. Private IP addresses
- C. File timestamps
- D. Public IP addresses

Answer: C

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 # 33
What is one purpose of steganography?

- A. To encrypt data for security
- B. To deliver information secretly
- C. To compress large files
- D. To delete files securely

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Steganography is used to conceal information within other seemingly innocuous data, such as embedding messages inside image files, allowing secret delivery of information without detection.
* Unlike encryption, steganography hides the existence of the message itself.
* It is an anti-forensic technique used to evade detection.
Reference:NIST and digital forensics literature describe steganography as covert communication methodology.

NEW QUESTION # 34
How should a forensic scientist obtain the network configuration from a Windows PC before seizing it from a crime scene?

- A. By checking the system properties
- B. By using the ipconfig command from a command prompt on the computer
- C. By opening the Network and Sharing Center
- D. By rebooting the computer into safe mode

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The ipconfig command executed at a Windows command prompt displays detailed network configuration information such as IP addresses, subnet masks, and default gateways. Collecting this information prior to seizure preserves volatile evidence relevant to the investigation.
* Documenting network settings supports the understanding of the suspect system's connectivity at the time of seizure.
* NIST recommends capturing volatile data (including network configuration) before shutting down or disconnecting a suspect machine.
Reference:NIST SP 800-86 and forensic best practices recommend gathering volatile evidence using system commands like ipconfig.

NEW QUESTION # 35
.....

obtain a free download on 【 www.dumpsmaterials.com 】 □Digital-Forensics-in-Cybersecurity New Braindumps Free

- 100% Pass WGU - Digital-Forensics-in-Cybersecurity - Authoritative Digital Forensics in Cybersecurity (D431/C840) Course Exam Dumps PDF □ Download ☀ Digital-Forensics-in-Cybersecurity □☀□ for free by simply searching on □ www.pdfvce.com □ □Digital-Forensics-in-Cybersecurity New Braindumps Free
- Latest updated Digital-Forensics-in-Cybersecurity Dumps PDF - Latest Valid Digital-Forensics-in-Cybersecurity Vce Dumps - Useful Digital-Forensics-in-Cybersecurity Test Dump □ Download 《 Digital-Forensics-in-Cybersecurity 》 for free by simply searching on ➽ www.vceengine.com □ □Valid Digital-Forensics-in-Cybersecurity Test Sample
- Training Digital-Forensics-in-Cybersecurity Tools □ Digital-Forensics-in-Cybersecurity VCE Exam Simulator □ Free Digital-Forensics-in-Cybersecurity Exam Dumps □ Open ✔ www.pdfvce.com □✔□ and search for { Digital-Forensics-in-Cybersecurity } to download exam materials for free □Digital-Forensics-in-Cybersecurity Related Exams
- WGU Digital-Forensics-in-Cybersecurity Dumps PDF Exam Pass Once Try | Digital-Forensics-in-Cybersecurity: Digital Forensics in Cybersecurity (D431/C840) Course Exam □ Search for ▹ Digital-Forensics-in-Cybersecurity ◃ and download it for free immediately on ➤ www.prep4sures.top □ □Certification Digital-Forensics-in-Cybersecurity Dumps
- 100% Pass WGU - Digital-Forensics-in-Cybersecurity - Authoritative Digital Forensics in Cybersecurity (D431/C840) Course Exam Dumps PDF □ Easily obtain free download of ➠ Digital-Forensics-in-Cybersecurity □ by searching on ✔ www.pdfvce.com □✔□ □Digital-Forensics-in-Cybersecurity Reliable Exam Simulations
- Latest Digital-Forensics-in-Cybersecurity Dumps Ebook □ Dumps Digital-Forensics-in-Cybersecurity Discount □ New Soft Digital-Forensics-in-Cybersecurity Simulations □ Immediately open ➽ www.practicevce.com □ and search for ➠ Digital-Forensics-in-Cybersecurity □ to obtain a free download □Dump Digital-Forensics-in-Cybersecurity Torrent
- Valid Digital-Forensics-in-Cybersecurity Test Sample □ Dump Digital-Forensics-in-Cybersecurity Torrent □ New Soft Digital-Forensics-in-Cybersecurity Simulations □ The page for free download of □ Digital-Forensics-in-Cybersecurity □ on 【 www.pdfvce.com 】 will open immediately □New Digital-Forensics-in-Cybersecurity Test Sims
- Latest updated Digital-Forensics-in-Cybersecurity Dumps PDF - Latest Valid Digital-Forensics-in-Cybersecurity Vce Dumps - Useful Digital-Forensics-in-Cybersecurity Test Dump □ Search for ➡ Digital-Forensics-in-Cybersecurity □□□ and download it for free immediately on 「 www.prepawaypdf.com 」 □Digital-Forensics-in-Cybersecurity VCE Exam Simulator
- Latest updated Digital-Forensics-in-Cybersecurity Dumps PDF - Latest Valid Digital-Forensics-in-Cybersecurity Vce Dumps - Useful Digital-Forensics-in-Cybersecurity Test Dump □ Go to website [www.pdfvce.com] open and search for ▹ Digital-Forensics-in-Cybersecurity ◃ to download for free □Valid Digital-Forensics-in-Cybersecurity Test Sample
- Certification Digital-Forensics-in-Cybersecurity Dumps □ Latest Digital-Forensics-in-Cybersecurity Dumps Ebook □ Digital-Forensics-in-Cybersecurity Books PDF □ Search for ➽ Digital-Forensics-in-Cybersecurity □ and download exam materials for free through ➡ www.pdfdumps.com □□□ □Certification Digital-Forensics-in-Cybersecurity Dumps
- me.muz.li, 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, scalar.usc.edu, scalar.usc.edu, www.grepmed.com, disqus.com, fortunetelleroracle.com, jobs.electronicsweekly.com, tooter.in, learn.csisafety.com.au, Disposable vapes

DOWNLOAD the newest Lead1Pass Digital-Forensics-in-Cybersecurity PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1Ffiucs6PVGvwzNjRuKZZmWgFkZoMiccB