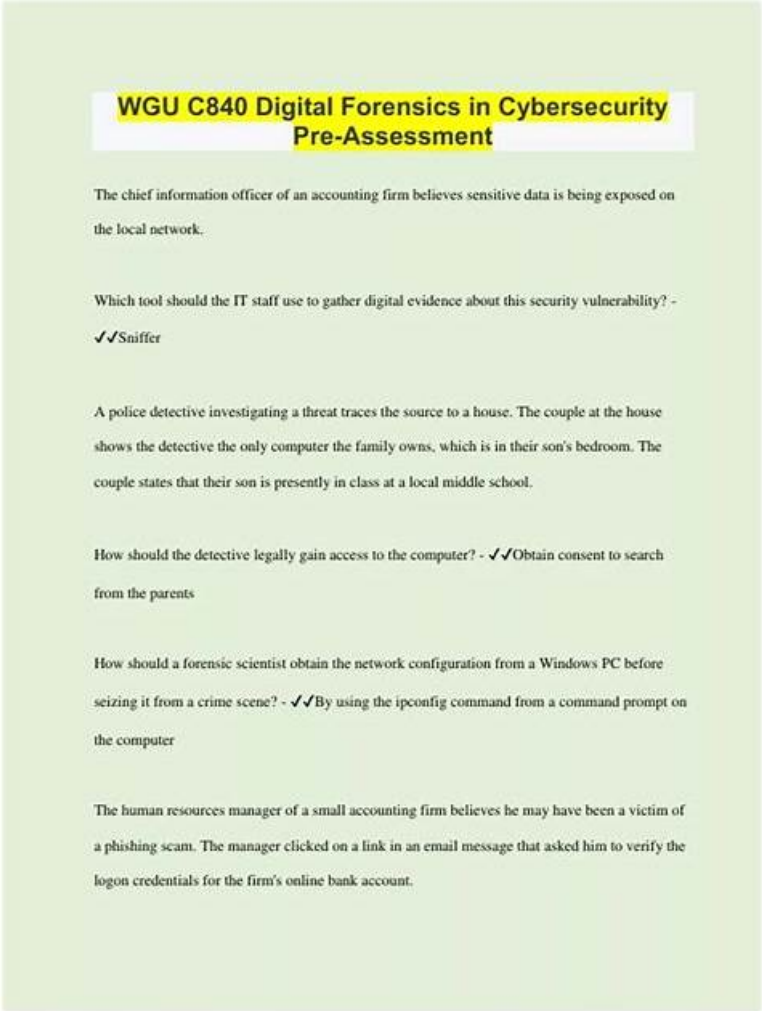
WGU Digital-Forensics-in-Cybersecurity Dumps - Hassle-Free Accomplishment



WGU C840 Digital Forensics in Cybersecurity Pre-Assessment

The chief information officer of an accounting firm believes sensitive data is being exposed on the local network.

Which tool should the IT staff use to gather digital evidence about this security vulnerability? - ✓✓Sniffer

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? - ✓✓Obtain consent to search from the parents

How should a forensic scientist obtain the network configuration from a Windows PC before seizing it from a crime scene? - ✓✓By using the ipconfig command from a command prompt on the computer

The human resources manager of a small accounting firm believes he may have been a victim of a phishing scam. The manager clicked on a link in an email message that asked him to verify the logon credentials for the firm's online bank account.

P.S. Free 2026 WGU Digital-Forensics-in-Cybersecurity dumps are available on Google Drive shared by DumpsFree: https://drive.google.com/open?id=10v6_d8d6b8FEwKqrJ-0ziovm-YFf0lHf

Three versions of Digital-Forensics-in-Cybersecurity test materials are available. You can choose the one you prefer to have a practice. Digital-Forensics-in-Cybersecurity PDF version is printable, and if you prefer to practice on paper, this version will be your best choice. You can print them into hard one, and take them with you. Digital-Forensics-in-Cybersecurity Soft test engine can stimulate the real exam environment, and this version will help you to relieve your nerves. Digital-Forensics-in-Cybersecurity Online test engine supports all web browsers, with this version you can have a brief review of what you have finished last 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 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.

Reliable Digital-Forensics-in-Cybersecurity Test Tutorial, Free Digital-Forensics-in-Cybersecurity Dumps

WGU Digital-Forensics-in-Cybersecurity exam dumps is a surefire way to get success. DumpsFree has assisted a lot of professionals in passing their WGU Digital-Forensics-in-Cybersecurity certification test. In case you don't pass the WGU Digital-Forensics-in-Cybersecurity pdf questions and practice tests, you have the full right to claim your full refund. You can download and test any Digital-Forensics-in-Cybersecurity Exam Questions format before purchase. So don't get worried, start WGU Digital-Forensics-in-Cybersecurity exam preparation and get successful.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Sample Questions (Q18-Q23):

NEW QUESTION # 18
An organization has identified a system breach and has collected volatile data from the system.
Which evidence type should be collected next?

- A. Temporary data
- B. Network connections
- C. Running processes
- D. File timestamps

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In incident response, after collecting volatile data (such as contents of RAM), the next priority is often to collect network-related evidence such as active network connections. Network connections can reveal ongoing communications, attacker activity, command and control channels, or data exfiltration paths.
* Running processes and temporary data are also volatile but typically collected simultaneously or immediately after volatile memory.
* File timestamps relate to non-volatile data and are collected later after volatile data acquisition to preserve evidence integrity.
* This sequence is supported by NIST SP 800-86 and SANS Incident Handler's Handbook which emphasize the volatility of evidence and recommend capturing network state immediately after memory.

NEW QUESTION # 19
Which file system is supported by Mac?

- A. Hierarchical File System Plus (HFS+)
- B. EXT4
- C. NTFS
- D. FAT32

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Mac systems traditionally use the Hierarchical File System Plus (HFS+), which supports features such as journaling and metadata handling suited for Mac OS environments. Newer versions use APFS but HFS+ remains relevant.
* NTFS is primarily a Windows file system.
* EXT4 is a Linux file system.
* FAT32 is a generic cross-platform file system but lacks advanced features.
Reference:Apple and NIST documentation confirm HFS+ as a Mac-supported file system for forensic analysis.

NEW QUESTION # 20
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. Wait for the son to return and ask for consent
- B. Obtain consent to search from the parents
- C. Get a warrant without consent
- D. Search immediately without consent due to emergency

Answer: B

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 # 21
On which file does the Windows operating system store hashed passwords?

- A. System
- B. Kerberos
- C. SAM
- D. NTUSER.dat

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Windows stores user account password hashes in theSecurity Account Manager (SAM)file, located inC:\Windows\System32\config. This file contains encrypted NTLM password hashes that can be extracted with forensic tools for analysis.
* SAM is critical for authentication evidence.
* The file is locked when Windows is running and must be acquired via imaging or offline analysis.
* Kerberos is an authentication protocol, not a password storage file.

Reference:NIST Windows Forensic Analysis documentation identifies the SAM file as the location of hashed credentials.

NEW QUESTION # 22
Which Windows component is responsible for reading the boot.ini file and displaying the boot loader menu on Windows XP during the boot process?

- A. NTLDR
- B. BCD
- C. Winload.exe
- D. BOOTMGR

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
NTLDR (NT Loader) is the boot loader for Windows NT-based systems including Windows XP. It reads the boot.ini configuration file and displays the boot menu, initiating the boot process.
* Later Windows versions (Vista and above) replaced NTLDR with BOOTMGR.
* Understanding boot components assists forensic investigators in boot process analysis.
Reference:Microsoft technical documentation and forensic training materials outline NTLDR's role in legacy Windows systems.

NEW QUESTION # 23
.....

Forensics-in-Cybersecurity Exam Registration □ Download " Digital-Forensics-in-Cybersecurity " for free by simply searching on □ www.prepawayexam.com □ □Free Digital-Forensics-in-Cybersecurity Download Pdf

- Digital-Forensics-in-Cybersecurity Test Prep and WGU Reliable Digital-Forensics-in-Cybersecurity Test Tutorial: Digital Forensics in Cybersecurity (D431/C840) Course Exam Pass Certify ↔ ➠ www.pdfvce.com □ is best website to obtain □ Digital-Forensics-in-Cybersecurity □ for free download □Downloadable Digital-Forensics-in-Cybersecurity PDF
- WGU - Accurate Digital-Forensics-in-Cybersecurity - Digital Forensics in Cybersecurity (D431/C840) Course Exam Test Prep □ Search for □ Digital-Forensics-in-Cybersecurity □ and easily obtain a free download on ☀ www.pdfdumps.com □☀□ □Practice Test Digital-Forensics-in-Cybersecurity Pdf
- 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, bbs.t-firefly.com, www.stes.tyc.edu.tw, twin.longemed.com, hhi.instructure.com, www.stes.tyc.edu.tw, 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, Disposable vapes

What's more, part of that DumpsFree Digital-Forensics-in-Cybersecurity dumps now are free: https://drive.google.com/open?id=10v6_d8d6b8FEwKqrJ-0ziovm-YFf0lHf