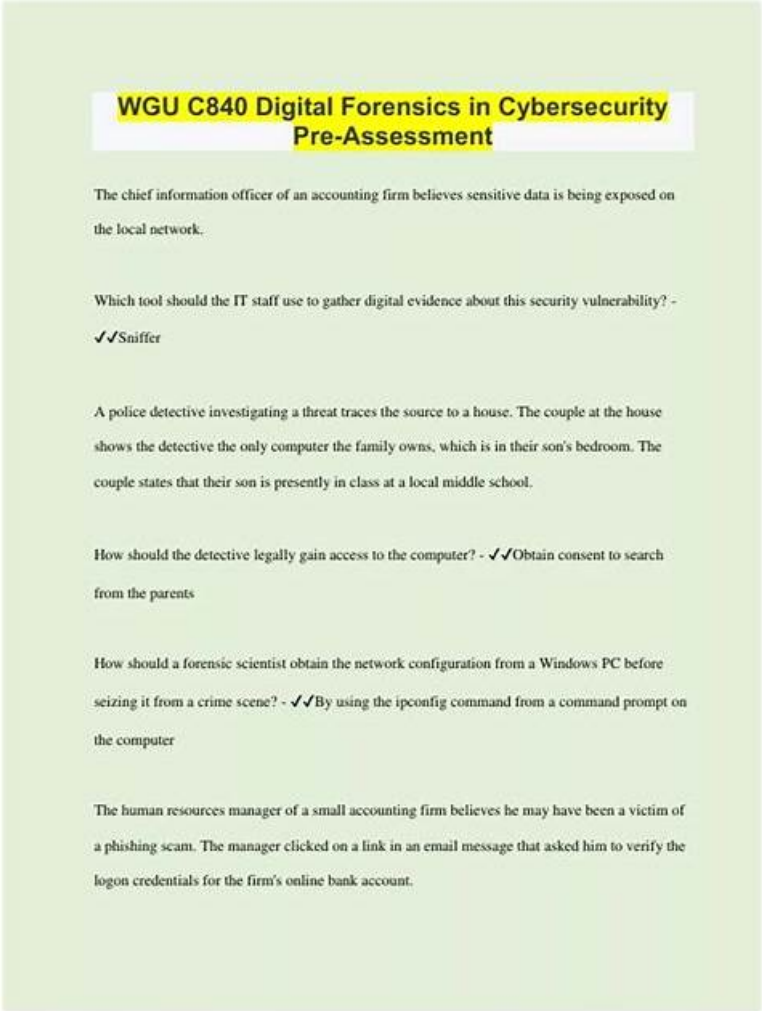
Digital-Forensics-in-Cybersecurity復習過去問 & Digital-Forensics-in-Cybersecurity基礎訓練


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.

2026年CertJukenの最新Digital-Forensics-in-Cybersecurity PDFダンプおよびDigital-Forensics-in-Cybersecurity試験エンジンの無料共有：https://drive.google.com/open?id=1NWJISbBR5IJfCBBjrGgpHkagVjAI4dLu

Digital-Forensics-in-Cybersecurity試験問題の更新を1年以内にクライアントに無料で提供し、1年後にクライアントは50％の割引を受けることができます。クライアントが古いクライアントの場合、一定の割引を享受できます。当社WGUの専門家は、毎日Digital-Forensics-in-Cybersecurityガイドトレントを更新し、Digital-Forensics-in-Cybersecurityスタディガイドの最新の更新をクライアントに提供します。私たちはクライアントに割引を提供し、彼らがより少ないお金を使うようにします。あなたが古いクライアントである場合、あなたは特別割引を享受することができますので、お金を節約することができます。したがって、Digital-Forensics-in-Cybersecurityテストトレントを購入することは非常に価値があります。

ユーザーのプライバシー保護は、インターネット時代の永遠の問題です。多くの違法ウェブサイトはユーザーのプライバシーを第三者に販売するため、多くの購入者は奇妙なウェブサイトを信じることを嫌います。ただし、Digital-Forensics-in-Cybersecurity学習エンジンDigital-Forensics-in-Cybersecurityを購入する際に心配する必要はまったくありません。ユーザーの情報が私たちの評判を傷つけているため、ユーザーの情報を決して販売しないことを保証します。

>> Digital-Forensics-in-Cybersecurity復習過去問 <<

WGU Digital-Forensics-in-Cybersecurity基礎訓練 & Digital-Forensics-in-Cybersecurity資格参考書

CertJukenのWGUのDigital-Forensics-in-Cybersecurity試験トレーニング資料は豊富な経験を持っているIT専門家が研究したもので、問題と解答が緊密に結んでいるものです。それと比べるものがありません。専門的な団体と正確性の高いWGUのDigital-Forensics-in-Cybersecurity問題集があるこそ、CertJukenのサイトは世界的でDigital-Forensics-in-Cybersecurity試験トレーニングによっての試験合格率が一番高いです。CertJukenを選んび、成功を選びます。

WGU Digital-Forensics-in-Cybersecurity 認定試験の出題範囲:

トピック	出題範囲
トピック 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.
トピック 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.
トピック 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.
トピック 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.
トピック 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 認定 Digital-Forensics-in-Cybersecurity 試験問題 (Q59-Q64):

質問 # 59
Which characteristic applies to solid-state drives (SSDs) compared to magnetic drives?

- A. They have moving parts
- B. They are generally slower
- C. They have a lower cost per gigabyte
- D. They are less susceptible to damage

正解：D

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Solid-state drives (SSDs) use flash memory and have no moving mechanical parts, making them more resistant to physical shock and damage compared to magnetic drives, which rely on spinning platters.
* This resilience makes SSDs favorable in environments with higher physical risk.
* However, data recovery from SSDs can be more complex due to wear-leveling and TRIM features.
Reference:NIST and forensic hardware guides highlight SSD durability advantages over traditional magnetic storage.

質問 # 60
A forensic scientist is examining a computer for possible evidence of a cybercrime.
Why should the forensic scientist copy files at the bit level instead of the OS level when copying files from the computer to a forensic computer?

- A. Copying files at the OS level fails to copy deleted files or slack space.
- B. Copying files at the OS level will copy extra information that is unnecessary.
- C. Copying files at the OS level takes too long to be practical.
- D. Copying files at the OS level changes the timestamp of the files.

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Bit-level (or bit-stream) copying captures every bit on the storage media, including files, deleted files, slack space (unused space within a cluster), and unallocated space. This ensures all digital evidence, including artifacts not visible at the OS level, is preserved for analysis.
* Copying at the OS level captures only allocated files visible in the file system, missing deleted files and slack space.
* Bit-level copying is a cornerstone of forensic best practices as specified in NIST SP 800-86 and SWGDE guidelines.
* Timestamp changes and unnecessary information issues are secondary concerns compared to the completeness of evidence.

質問 # 61
Which U.S. law criminalizes the act of knowingly using a misleading domain name with the intent to deceive a minor into viewing harmful material?

- A. Electronic Communications Privacy Act (ECPA)
- B. Communications Assistance to Law Enforcement Act (CALEA)
- C. 18 U.S.C. 2252B
- D. The Privacy Protection Act (PPA)

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Title 18 U.S.C. § 2252B addresses the criminal offense of using misleading domain names with the intent to deceive minors into accessing harmful material. This law specifically targets online behavior designed to exploit or expose minors to inappropriate content.
* It is part of broader child protection statutes.
* Enforcement requires digital evidence linking domain misuse to the intent.
Reference:Federal statutes and legal frameworks on cybercrime emphasize the applicability of 18 U.S.C.
2252B in prosecuting online deception aimed at minors.

質問 # 62
An organization is determined to prevent data leakage through steganography. It has developed a workflow that all outgoing data must pass through. The company will implement a tool as part of the workflow to check for hidden data.
Which tool should be used to check for the existence of steganographically hidden data?

- A. Data Doctor
- B. Forensic Toolkit (FTK)
- C. Snow
- D. MP3Stego

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Snow is a specialized steganalysis tool that detects and extracts hidden data encoded in whitespace characters within text files and other mediums. It is widely used in digital forensic investigations for detecting covert data hiding methods such as whitespace

steganography.
* Data Doctor is a general data recovery tool, not specialized in steganalysis.
* FTK is a general forensic suite, not specifically designed for steganography detection.
* MP3Stego is focused on audio steganography.
NIST and digital forensics literature recognize Snow as a valuable tool in workflows designed to detect hidden data in text or similar carriers.

質問 # 63
Which file stores local Windows passwords in the Windows\System32\ directory and is subject to being cracked by using a live CD?

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

正解：A

解説：
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.

質問 # 64
.....

Digital-Forensics-in-Cybersecurity基礎訓練 □ ➡ www.goshiken.com □□□は、✔ Digital-Forensics-in-Cybersecurity □✔□を無料でダウンロードするのに最適なサイトですDigital-Forensics-in-Cybersecurityテスト資料

- Digital-Forensics-in-Cybersecurityトレーリングサンプル □ Digital-Forensics-in-Cybersecurity試験復習 □ Digital-Forensics-in-Cybersecurity日本語資格取得 □ ウェブサイト☀ jp.fast2test.com □☀□から✔ Digital-Forensics-in-Cybersecurity □✔□を開いて検索し、無料でダウンロードしてくださいDigital-Forensics-in-Cybersecurity一発合格
- Digital-Forensics-in-Cybersecurity日本語版サンプル □ Digital-Forensics-in-Cybersecurity最新試験情報 □ Digital-Forensics-in-Cybersecurityトレーリングサンプル ↩ 検索するだけで【 www.goshiken.com 】から□ Digital-Forensics-in-Cybersecurity □を無料でダウンロードDigital-Forensics-in-Cybersecurity試験関連情報
- Digital-Forensics-in-Cybersecurity信頼できる試験問題集、Digital-Forensics-in-Cybersecurity Pdf練習問題集、Digital Forensics in Cybersecurity (D431/C840) Course Examテストオンライン練習 □ □ www.it-passports.com □サイトにて{ Digital-Forensics-in-Cybersecurity }問題集を無料で使おうDigital-Forensics-in-Cybersecurity試験攻略
- Digital-Forensics-in-Cybersecurity試験攻略 □ Digital-Forensics-in-Cybersecurityトレーリングサンプル □ Digital-Forensics-in-Cybersecurity問題サンプル □ ➠ www.goshiken.com □で使える無料オンライン版➡ Digital-Forensics-in-Cybersecurity □□□ の試験問題Digital-Forensics-in-Cybersecurity問題サンプル
- Digital-Forensics-in-Cybersecurityテスト対策書 □ Digital-Forensics-in-Cybersecurity関連日本語版問題集 □ Digital-Forensics-in-Cybersecurity関連日本語版問題集 □ ▹ Digital-Forensics-in-Cybersecurity ◃の試験問題は □ www.topexam.jp □で無料配信中Digital-Forensics-in-Cybersecurity試験攻略
- bbs.t-firefly.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, bbs.t-firefly.com, 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, sincerequranicinstitute.com, 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, bbs.gmncg.com, justpaste.me, Disposable vapes

BONUS！！！ CertJuken Digital-Forensics-in-Cybersecurityダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1NWJISbBR5IJfCBBjrGgpHkagVjAI4dLu