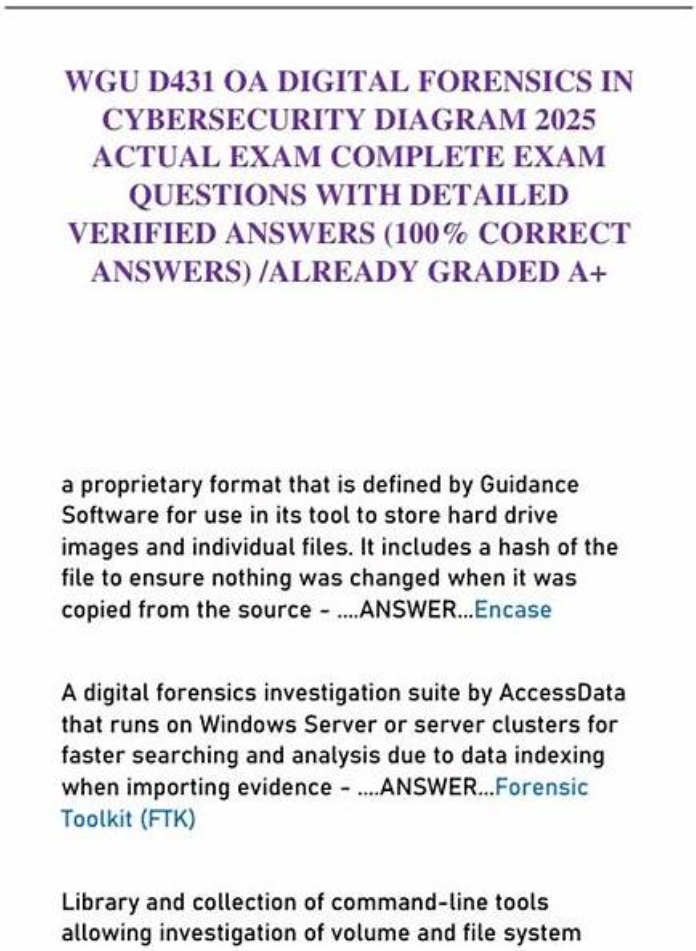
WGU Digital-Forensics-in-Cybersecurity資格認定試験 & Digital-Forensics-in-Cybersecurity復習問題集



2026年Pass4Test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=1IST63rZrdsOhlm0N4w1iJfgdkWyVpUPa

Digital-Forensics-in-Cybersecurity認定資格を取得して、専門能力を高めてください。認定資格を取得すると、より良い仕事の機会とより高い給料を得ることができます。それでは、Digital-Forensics-in-Cybersecurity試験トレーニングガイドから準備を始めましょう。 Pass4Testが提供するDigital-Forensics-in-Cybersecurity実践PDFは、すべてのお客様に適した最新かつ有効なものです。無料デモは、特に購入前に無料でダウンロードして試してみることができます。 Digital-Forensics-in-Cybersecurity模擬試験ダンプから多くを取得し、Digital-Forensics-in-Cybersecurity認定を簡単に取得できます。

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 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 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.
トピック 3	• 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.
トピック 4	• 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 5	• 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.

試験の準備方法-更新するDigital-Forensics-in-Cybersecurity資格認定試験試験-ユニークなDigital-Forensics-in-Cybersecurity復習問題集

社会の発展と相対的な法律と規制の完成により、私たちのキャリア分野でのDigital-Forensics-in-Cybersecurity証明書は私たちの国にとって必要になります。 Digital-Forensics-in-Cybersecurityに合格して証明書を取得することが、あなたの立場を変えて目標を達成するための最も迅速で直接的な方法かもしれません。そして、私たちはあなたを助けるためにちょうどここにいます。このキャリアで最も本物のブランドと見なされているプロの専門家は、お客様に最新の有効なDigital-Forensics-in-Cybersecurity試験シミュレーションを提供するために絶え間ない努力を行っています。

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam 認定 Digital-Forensics-in-Cybersecurity 試験問題 (Q66-Q71):

質問 # 66
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. Ensure that any tools and techniques used are widely accepted
- B. Enlist a colleague to witness the investigative process
- C. Download a tool from a hacking website to extract the data
- D. Investigate whether the computer was properly seized

正解：A

解説：
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.

質問 # 67
Which policy is included in the CAN-SPAM Act?

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

正解：B

解説：
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.

質問 # 68
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/spool/cups
- B. /Library/Receipts
- C. /var/vm
- D. /var/log/daily.out

正解：B

解説：
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.

質問 # 69
A computer involved in a crime is infected with malware. The computer is on and connected to the company's network. The forensic investigator arrives at the scene.
Which action should be the investigator's first step?

- A. Run malware removal tools
- B. Unplug the computer's Ethernet cable
- C. Turn off the computer
- D. Copy files to external media

正解：B

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Disconnecting the computer from the network by unplugging the Ethernet cable prevents further spread of malware and stops external communication that could lead to data exfiltration. This containment step is vital before further evidence collection.
* Maintaining system power preserves volatile memory.

* Network disconnection is recommended by incident response guidelines.
Reference:NIST SP 800-61 recommends isolating affected systems from networks early in incident response.

質問 # 70
A forensic investigator is acquiring evidence from an iPhone.
What should the investigator ensure before the iPhone is connected to the computer?

- A. That the phone is powered off
- B. That the phone has root privilege
- C. That the phone is in jailbreak mode
- D. That the phone avoids syncing with the computer

正解： D

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Before connecting an iPhone to a forensic workstation, the investigator must ensure that the phone doesnotsync with the computer automatically. Automatic syncing may alter, delete, or overwrite evidence stored on the device or the computer, compromising forensic integrity.
* Jailbreak mode is not necessary and can complicate forensic analysis.
* Powering off the device prevents acquisition of volatile data.
* Root privileges (jailbreak) may aid access but are not mandatory before connection.
NIST mobile device forensic guidelines emphasize disabling automatic sync to preserve data integrity during acquisition.

質問 # 71
.....

- 試験の準備方法-一番優秀なDigital-Forensics-in-Cybersecurity資格認定試験試験-有効的なDigital-Forensics-in-Cybersecurity復習問題集 □ ✔ www.japancert.com □✔□の無料ダウンロード▶ Digital-Forensics-in-Cybersecurity ◀ページが開きますDigital-Forensics-in-Cybersecurity資格取得講座
- Digital-Forensics-in-Cybersecurity問題と解答 □ Digital-Forensics-in-Cybersecurity参考書内容 □ Digital-Forensics-in-Cybersecurity関連資格試験対応 □ 《 www.goshiken.com 》で[Digital-Forensics-in-Cybersecurity]を検索して、無料で簡単にダウンロードできますDigital-Forensics-in-Cybersecurity出題内容
- Digital-Forensics-in-Cybersecurity資格取得講座 □ Digital-Forensics-in-Cybersecurity最新試験 □ Digital-Forensics-in-Cybersecurityテスト模擬問題集 ↕ ⇒ www.shikenpass.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問題と解答
- bbs.t-firefly.com, motionenergy.com.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

BONUS！！！ Pass4Test 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=1IST63rZrdsOhlm0N4w1iJfgdkWyVpUPa