真実的なDigital-Forensics-in-Cybersecurity難易度試験-試験の準備方法-更新するDigital-Forensics-in-Cybersecurity受験記

ちなみに、It-Passports Digital-Forensics-in-Cybersecurityの一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=10prKFho1m_tS8k20O1HSVGefcI6w-FYF

WGUのDigital-Forensics-in-Cybersecurity認定試験に合格するのは簡単なことではありませんか。It-PassportsのWGUのDigital-Forensics-in-Cybersecurity試験トレーニング資料を選ぶなら、一回で認定試験に合格するの可能性は高いです。It-Passports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業種の専門家が長年の研究を通じて、作成したものです。その権威性が高いと言えます。It-Passportsを選ぶなら、絶対に後悔させません。

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	• 削除されたファイルとアーティファクトの復旧：このドメインは、デジタルフォレンジック技術者のスキルを測定し、削除されたファイル、隠されたデータ、システムアーティファクトからの証拠収集に焦点を当てます。関連する残存情報の特定、アクセス可能な情報の復元、そして異なるシステム内でデジタル痕跡がどこに保存されているかの把握が含まれます。
トピック 2	• サイバーセキュリティにおけるデジタルフォレンジック：このドメインは、サイバーセキュリティ技術者のスキルを測定し、セキュリティ環境におけるデジタルフォレンジックの中核的な目的に焦点を当てています。サイバーインシデントの調査、デジタル証拠の検証、そして調査結果が法的および組織的な行動にどのように役立つかを理解するために用いられる手法を網羅しています。
トピック 3	• インシデント報告とコミュニケーション：このドメインは、サイバーセキュリティアナリストのスキルを測定し、フォレンジック調査の結果をまとめたインシデントレポートの作成に焦点を当てています。これには、証拠の文書化、結論の要約、そして組織のステークホルダーへの明確かつ構造化された方法での成果の伝達が含まれます。
トピック 4	• デジタルフォレンジックにおける法的および手続き上の要件：この領域では、デジタルフォレンジック技術者のスキルを測定し、フォレンジック業務を導く法律、規則、標準に焦点を当てます。調査が正当かつ適切に実行されることを保証する規制要件、組織的手続き、そして認められたベストプラクティスの特定が含まれます。

トピック 5	• フォレンジックツールを用いたドメイン証拠分析：このドメインでは、サイバーセキュリティ技術者のスキルを測定し、標準的なフォレンジックツールを用いて収集された証拠を分析することに焦点を当てます。正確性と整合性を確保する承認済みの調査プロセスに従いながら、ディスク、ファイルシステム、ログ、システムデータをレビューすることが含まれます。

>> Digital-Forensics-in-Cybersecurity難易度 <<

Digital-Forensics-in-Cybersecurity受験記 & Digital-Forensics-in-Cybersecurity試験合格攻略

IT業界の一人として、IT領域の現状をよく知っているのでしょう？現在のIT業界でWGUの資格認証はますます重要になっています。多くの人はDigital-Forensics-in-Cybersecurity試験に悩んでいます。あなたもその中の一員かもしれません。試験に迅速に合格する方法を探していますか？我々のDigital-Forensics-in-Cybersecurity資料を試しましょう。無料のサンプルを提供して、あなたはダウンロードして試すことができます。あなたの要求を満たすなら、弊社のDigital-Forensics-in-Cybersecurity参考書を利用してください。

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam 認定 Digital-Forensics-in-Cybersecurity 試験問題 (Q47-Q52):

質問 # 47
A user at a company attempts to hide the combination to a safe that stores confidential information in a data file called vacationdetails.doc.
What is vacationdetails.doc called, in steganographic terms?

- A. Snow
- B. Channel
- C. Payload
- D. Carrier

正解：D

解説：
Comprehensive and Detailed Explanation From Exact Extract:
In steganography, the file that hides secret information is called thecarrier. The carrier file appears normal and contains embedded hidden data (the payload).
* Payload refers to the actual secret data hidden inside the carrier.
* Snow refers to random noise or artifacts, often in images or files.
* Channel refers to the medium or communication path used to transmit data.
Thus,vacationdetails.docis the carrier file containing the hidden information.
Reference:Standard steganography literature and forensic documentation define the carrier as the file used to conceal payload data.

質問 # 48
Which universal principle must be observed when handling digital evidence?

- A. Keep the evidence in a plastic bag
- B. Make a copy and analyze the original
- C. Get the signatures of two witnesses
- D. Avoid making changes to the evidence

正解：D

解説：
Comprehensive and Detailed Explanation From Exact Extract:
The foremost principle in digital forensics isnever altering the original evidence. This ensures integrity, authenticity, and admissibility in court.

* Investigators analyze forensic copies, not originals.
* Write-blockers and hashing are used to prevent changes.
* Any alteration-intentional or accidental-can invalidate evidence.
Reference:NIST SP 800-86 and SP 800-101 define the unaltered preservation of evidence as the first and most essential forensic rule.

質問 # 49
Which directory contains the system's configuration files on a computer running Mac OS X?

- A. /bin
- B. /etc
- C. /var
- D. /cfg

正解：B

解説：
Comprehensive and Detailed Explanation From Exact Extract:
The/etcdirectory on Unix-based systems, including macOS, contains important system configuration files and scripts. It is the standard location for system-wide configuration data.
* /varcontains variable data like logs and spool files.
* /bincontains essential binary executables.
* /cfgis not a standard directory in macOS.
This is standard Unix/Linux directory structure knowledge and is reflected in NIST and forensic references for macOS.

質問 # 50
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 in jailbreak mode
- B. That the phone avoids syncing with the computer
- C. That the phone is powered off
- D. That the phone has root privilege

正解：B

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 # 51
An organization has identified a system breach and has collected volatile data from the system.
Which evidence type should be collected next?

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

正解：A

解説：

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.

質問 # 52
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, wefunder.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, portfolium.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, gis.zhangh.tech, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

さらに、It-Passports Digital-Forensics-in-Cybersecurityダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=10prKFho1m_tS8k20O1HSVGefcI6w-FYF