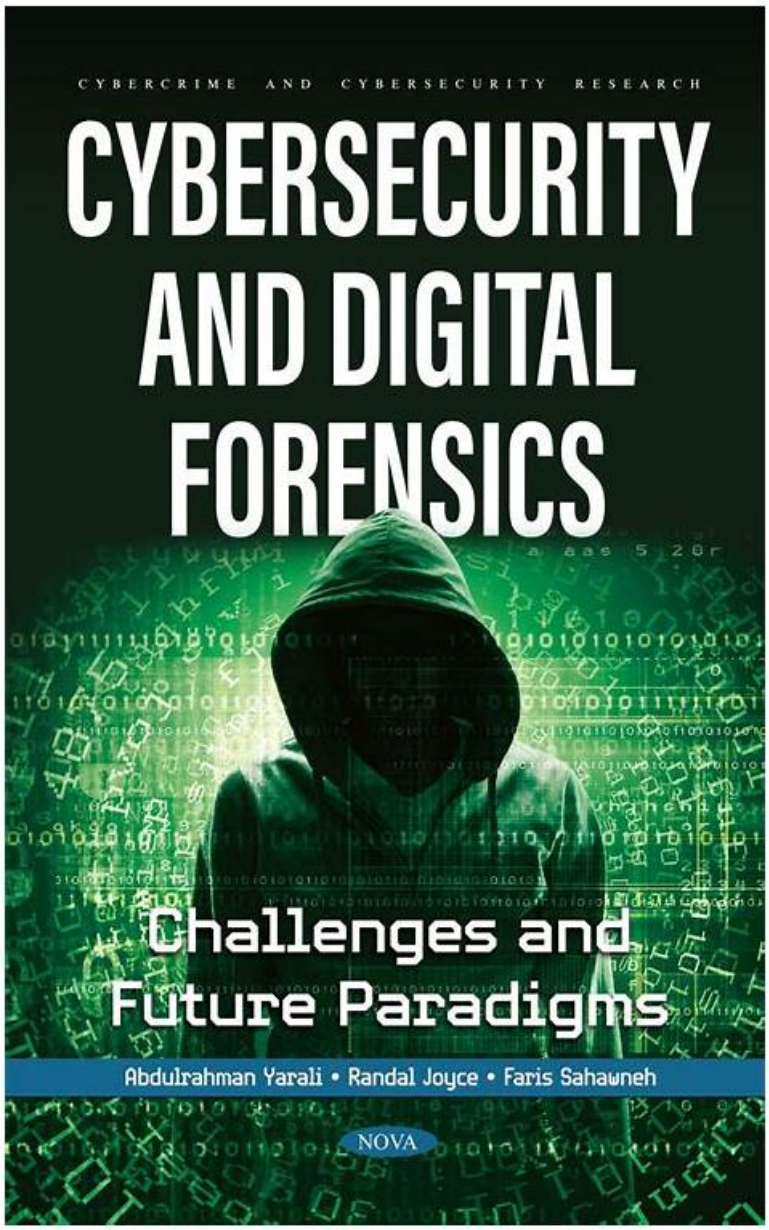
世界基準のDigital-Forensics-in-Cybersecurity問題集



P.S. JpshikenがGoogle Driveで共有している無料かつ新しいDigital-Forensics-in-Cybersecurityダンプ：https://drive.google.com/open?id=1duYroe76HBMvAUFQ5ECu67AQfN7WCMAv

現在でWGUのDigital-Forensics-in-Cybersecurity試験を受かることができます。JpshikenにWGUのDigital-Forensics-in-Cybersecurity試験のフルバージョンがありますから、最新のWGUのDigital-Forensics-in-Cybersecurityのトレーニング資料をあちこち探す必要がないです。Jpshikenを利用したら、あなたはもう最も良いWGUのDigital-Forensics-in-Cybersecurityのトレーニング資料を見つけたのです。弊社の質問と解答を安心にご利用ください。あなたはきっとWGUのDigital-Forensics-in-Cybersecurity試験に合格できますから。

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	• 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 2	• 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。
トピック 3	• 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 4	• 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 5	• 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。

信頼できるDigital-Forensics-in-Cybersecurity模擬トレーリング & 合格スムーズDigital-Forensics-in-Cybersecurity日本語対策 | 真実的なDigital-Forensics-in-Cybersecurity試験問題集

私たちの努力は自分の人生に更なる可能性を増加するためのことであるとよく思われます。あなたは弊社JpshikenのWGU Digital-Forensics-in-Cybersecurity試験問題集を利用し、試験に一回合格しました。WGU Digital-Forensics-in-Cybersecurity試験認証証明書を持つ皆様は面接のとき、他の面接人員よりもっと多くのチャンスがあります。その他、Digital-Forensics-in-Cybersecurity試験認証証明書も仕事昇進にたくさんのメリットを与えられます。

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam 認定 Digital-Forensics-in-Cybersecurity 試験問題 (Q68-Q73):

質問 # 68
Which technique allows a cybercriminal to hide information?

- A. Cryptography
- B. Encryption
- C. Steganography
- D. Steganalysis

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Steganography is the technique of hiding information within another file, message, image, or medium to conceal the existence of the

information itself. It differs from encryption in that the data is hidden, not just scrambled.
* Steganalysis is the detection or analysis of hidden data.
* Encryption and cryptography involve scrambling data but do not inherently hide its existence.
NIST and digital forensics guidelines define steganography as the art of concealed writing or data hiding, used by criminals to evade detection.

質問 # 69
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. Winload.exe
- C. BOOTMGR
- D. BCD

正解：A

解説：
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.

質問 # 70
A forensic examiner is reviewing a laptop running OS X which has been compromised. The examiner wants to know if any shell commands were executed by any of the accounts.
Which log file or folder should be reviewed?

- A. /Users/<user>/.bash_history
- B. /var/log
- C. /Users/<user>/Library/Preferences
- D. /var/vm

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract:
The.bash_historyfile located in each user's home directory (e.g.,/Users/<user>/.bash_history) records the history of shell commands entered by the user in bash shell sessions. Reviewing this file allows investigators to see the commands executed by a specific user.
* /var/vmcontains virtual memory swap files, not command history.
* /var/logcontains system logs but not individual user shell command history.
* /Users/<user>/Library/Preferencesstores application preferences.
NIST guidelines and macOS forensics literature confirm.bash_historyas the standard location for shell command histories on OS X systems.

質問 # 71
Which tool identifies the presence of steganography?

- A. Forensic Toolkit (FTK)
- B. DiskDigger
- C. ComputerCOP
- D. Disk Investigator

正解：D

解説：

Comprehensive and Detailed Explanation From Exact Extract:
Disk Investigator is a forensic tool that can analyze disk images and file systems to identify hidden data, including the presence of steganography by examining slack space, hidden files, and embedded data.
* DiskDigger is mainly a data recovery tool.
* FTK is a comprehensive forensic suite but does not specialize in steganography detection.
* ComputerCOP is a parental control software, not a forensic tool.
Digital forensic best practices recognize Disk Investigator as useful for detecting steganographic content in files and disk areas.

質問 # 72
Susan was looking at her credit report and noticed that several new credit cards had been opened lately in her name. Susan has not opened any of the credit card accounts herself.
Which type of cybercrime has been perpetrated against Susan?

- A. Cyberstalking
- B. Malware
- C. Identity theft
- D. SQL injection

正解：C

解説：
Comprehensive and Detailed Explanation From Exact Extract:
Identity theft occurs when an attacker unlawfully obtains and uses another person's personal information to open accounts, access credit, or commit fraud. The opening of credit cards without the victim's consent is a classic example.
* SQL injection is a web application attack method that does not directly relate to this case.
* Cyberstalking involves harassment via digital means and is unrelated.
* Malware is malicious software and may be used to facilitate identity theft but is not the crime itself.
Reference:According to the U.S. Federal Trade Commission (FTC) definitions and NIST Cybersecurity Framework, identity theft is defined as the unauthorized use of someone's personal information for fraudulent purposes, perfectly matching Susan's situation.

質問 # 73
.....

中Digital-Forensics-in-Cybersecurity関連合格問題

- Digital-Forensics-in-Cybersecurity資格模擬 □ Digital-Forensics-in-Cybersecurity合格問題 □ Digital-Forensics-in-Cybersecurityファンデーション □ Open Webサイト“www.xhs1991.com”検索“Digital-Forensics-in-Cybersecurity”無料ダウンロードDigital-Forensics-in-Cybersecurity模擬試験サンプル
- Digital-Forensics-in-Cybersecurity問題数 □ Digital-Forensics-in-Cybersecurity関連合格問題 □ Digital-Forensics-in-Cybersecurity合格問題 □ ➤ www.goshiken.com □サイトにて最新“Digital-Forensics-in-Cybersecurity”問題集をダウンロードDigital-Forensics-in-Cybersecurity試験情報
- 権威のある-効率的なDigital-Forensics-in-Cybersecurity模擬トレーリング試験-試験の準備方法Digital-Forensics-in-Cybersecurity日本語対策 □“www.xhs1991.com”サイトにて最新《Digital-Forensics-in-Cybersecurity》問題集をダウンロードDigital-Forensics-in-Cybersecurity試験情報
- 真実的なDigital-Forensics-in-Cybersecurity模擬トレーリングと信頼できるDigital-Forensics-in-Cybersecurity日本語対策 □《www.goshiken.com》に移動し、【Digital-Forensics-in-Cybersecurity】を検索して、無料でダウンロード可能な試験資料を探しますDigital-Forensics-in-Cybersecurity学習資料
- 試験の準備方法-便利なDigital-Forensics-in-Cybersecurity模擬トレーリング試験-最高のDigital-Forensics-in-Cybersecurity日本語対策 □ ➤ www.mogiexam.com □にて限定無料の➡ Digital-Forensics-in-Cybersecurity □□□問題集をダウンロードせよDigital-Forensics-in-Cybersecurity復習攻略問題
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, eastwest-lms.com, codepress.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, app.csicosnet.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, schoolrevise.com, www.stes.tyc.edu.tw, Disposable vapes

2026年Jpshiken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=1duYroe76HBMvAUFQ5ECu67AQfN7WCMAv