

Digital-Forensics-in-Cybersecurity Echte Fragen, Digital-Forensics-in-Cybersecurity Fragenpool

Digital Forensics in Cybersecurity - C840

FAT - correct answer Stores file locations by sector in a file called the file allocation table. This table contains information about which clusters are being used by which particular files and which clusters are free to be used.

NTFS (New Technology File System) - correct answer File system used by Windows NT 4, 2000, XP, Vista, 7, Server 2003, and Server 2008. One major improvement of this system was the increased volume sizes.

Extended file system - correct answer System created specifically for Linux. There have been many versions; the current version is 4.

ReiserFS - correct answer Popular journaling file system, used primarily with Linux. It was the first file system to be included with the standard Linux kernel, and first appeared in kernel version 2.4.1.

The Berkeley Fast File System - correct answer This is also known as the UNIX file system. Uses a bitmap to track free clusters, indicating which clusters are available and which are not.

Data hiding - correct answer Storage of data where an investigator is unlikely to find it.

Data transformation - correct answer Disguising the meaning of information.

Data contraception - correct answer Storage of data where a forensic specialist cannot analyze it.

Data fabrication - correct answer Uses false positives and false leads extensively.

File system alteration - correct answer Corruption of data structures and files that organize data.

Daubert standard - correct answer Any scientific evidence presented in a trial has to have been reviewed and tested by the relevant scientific community. For a computer forensics investigator, that means that

BONUS!!! Laden Sie die vollständige Version der DeutschPrüfung Digital-Forensics-in-Cybersecurity Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1GYubIWwBXQhw6t_2VaPuCZjyteQIWKEh

DeutschPrüfung spezialisiert sich auf die Schulungsunterlagen zur WGU Digital-Forensics-in-Cybersecurity Zertifizierungsprüfung. Mit DeutschPrüfung brauchen Sie sich keine Sorgen für die WGU Digital-Forensics-in-Cybersecurity Zertifizierungsprüfung zu machen. Die Zertifizierungsantworten von DeutschPrüfung sind qualitativ hochwertig. Sobald Sie DeutschPrüfung wählen, können Sie in kurzer Zeit die Prüfung mit einer hohen Note die WGU Digital-Forensics-in-Cybersecurity Zertifizierungsprüfung effizient bestehen und bessere Resultate bei weniger Einsatz erzielen.

WGU Digital-Forensics-in-Cybersecurity Prüfungsplan:

Thema	Einzelheiten
Thema 1	<ul style="list-style-type: none">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.

Thema 2	<ul style="list-style-type: none"> • 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.
Thema 3	<ul style="list-style-type: none"> • 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.
Thema 4	<ul style="list-style-type: none"> • 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.
Thema 5	<ul style="list-style-type: none"> • 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.

>> Digital-Forensics-in-Cybersecurity Echte Fragen <<

Digital-Forensics-in-Cybersecurity PrüfungGuide, WGU Digital-Forensics-in-Cybersecurity Zertifikat - Digital Forensics in Cybersecurity (D431/C840) Course Exam

Sie können im Internet teilweise die Fragen und Antworten zur WGU Digital-Forensics-in-Cybersecurity Zertifizierungsprüfung von DeutschPrüfung kostenlos als Probe herunterladen. Dann würden Sie finden, dass die Übungen von DeutschPrüfung ist die umfassendsten und genau was, was Sie wollen.

WGU Digital Forensics in Cybersecurity (D431/C840) Course Exam Digital-Forensics-in-Cybersecurity Prüfungsfragen mit Lösungen (Q30-Q35):

30. Frage

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

Antwort: A

Begründung:

Comprehensive and Detailed Explanation From Exact Extract:

The/Library/Receipts folder 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/cups is related to printer spooling.

* /var/log/daily.out contains daily system log summaries but not detailed update records.

* /var/vm contains virtual memory files.

NIST and Apple forensics documentation indicate that/Library/Receipts is a key location for examining software installation history.

31. Frage

A cybercriminal communicates with his compatriots using steganography. The FBI discovers that the criminal group uses white space to hide data in photographs.

Which tool can the cybercriminals use to facilitate this type of communication?

- A. Steganophony
- B. Wolf
- C. QuickStego
- **D. Snow**

Antwort: D

Begründung:

Comprehensive and Detailed Explanation From Exact Extract:

Snow is a tool that encodes hidden messages using whitespace characters (spaces and tabs), which can be embedded in text and sometimes in image file metadata or formats that allow invisible characters. It is commonly used to hide data in plain sight, including within digital images.

* Steganophony focuses on hiding data in VoIP.

* Wolf is not recognized as a steganography tool for whitespace.

* QuickStego is another tool for text-based steganography but less commonly associated with whitespace specifically.

Forensic and cybersecurity literature often cites Snow as the preferred tool for whitespace-based steganography.

32. Frage

Which law or guideline lists the four states a mobile device can be in when data is extracted from it?

- A. Communications Assistance to Law Enforcement Act (CALEA)
- B. Electronic Communications Privacy Act (ECPA)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- **D. NIST SP 800-72 Guidelines**

Antwort: D

Begründung:

Comprehensive and Detailed Explanation From Exact Extract:

NIST Special Publication 800-72 provides guidelines for mobile device forensics and identifies four device states during data extraction: active, idle, powered off, and locked. These states influence how data can be accessed and preserved.

* Understanding these states helps forensic investigators select appropriate acquisition techniques.

* NIST SP 800-72 is a key reference for mobile device forensic methodologies.

Reference:NIST SP 800-72 offers authoritative guidelines on handling mobile device data in forensic investigations.

33. Frage

Which law is related to the disclosure of personally identifiable protected health information (PHI)?

- A. The Privacy Protection Act (PPA)
- B. Communications Assistance to Law Enforcement Act (CALEA)
- **C. Health Insurance Portability and Accountability Act (HIPAA)**
- D. Electronic Communications Privacy Act (ECPA)

Antwort: C

Begründung:

Comprehensive and Detailed Explanation From Exact Extract:

HIPAA establishes standards to protect sensitive patient health information (PHI) and regulates the use and disclosure of such information. Forensic investigators dealing with health data must comply with HIPAA to avoid legal violations.

* HIPAA compliance is critical when handling medical records in investigations.

* Breach of PHI privacy can result in civil and criminal penalties.

Reference:HIPAA is widely referenced in cybersecurity and forensic policies relating to healthcare data protection.

34. Frage

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

Antwort: D

Begründung:

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.

35. Frage

.....

Unsere Schulungsunterlagen können Ihre Kenntnisse vor der WGU Digital-Forensics-in-Cybersecurity Prüfung testen und auch Ihr Verhalten in einer bestimmten Zeit bewerten. Wir geben Ihnen Anleitung zu Ihrer Note und Schwachpunkt, so dass Sie Ihre Schwäche nachholen können. Die Lernhilfe zur WGU Digital-Forensics-in-Cybersecurity Zertifizierungsprüfung von DeutschPrüfung stellen Ihnen unterschiedliche logische Themen vor. So können Sie nicht nur lernen, sondern auch andere Techniken und Subjekte kennen lernen. Wir versprechen, dass unsere WGU Digital-Forensics-in-Cybersecurity Schulungsunterlagen von der Praxis bewährt werden. DeutschPrüfung hat genügend Vorbereitung für Ihre Prüfung getroffen. Unsere Fragen sind umfassend und der Preis ist rational.

Digital-Forensics-in-Cybersecurity Fragenpool: <https://www.deutschpruefung.com/Digital-Forensics-in-Cybersecurity-deutsch-pruefungsfragen.html>

- Digital-Forensics-in-Cybersecurity Prüfungsmaterialien Digital-Forensics-in-Cybersecurity Deutsch Prüfungsfragen Digital-Forensics-in-Cybersecurity Zertifizierung Öffnen Sie die Webseite www.pruefungfrage.de und suchen Sie nach kostenloser Download von ➔ Digital-Forensics-in-Cybersecurity Digital-Forensics-in-Cybersecurity Zertifizierung
- Digital-Forensics-in-Cybersecurity Torrent Anleitung - Digital-Forensics-in-Cybersecurity Studienführer - Digital-Forensics-in-Cybersecurity wirkliche Prüfung Geben Sie www.itzert.com ein und suchen Sie nach kostenloser Download von [Digital-Forensics-in-Cybersecurity] Digital-Forensics-in-Cybersecurity Quizfragen Und Antworten
- Digital-Forensics-in-Cybersecurity Online Tests Digital-Forensics-in-Cybersecurity Examengine Digital-Forensics-in-Cybersecurity Zertifizierung ➔ www.zertpruefung.ch ist die beste Webseite um den kostenlosen Download von Digital-Forensics-in-Cybersecurity zu erhalten Digital-Forensics-in-Cybersecurity Deutsch Prüfungsfragen
- Neuester und gültiger Digital-Forensics-in-Cybersecurity Test VCE Motoren-Dumps und Digital-Forensics-in-Cybersecurity neueste Testfragen für die IT-Prüfungen Erhalten Sie den kostenlosen Download von ➔ Digital-Forensics-in-Cybersecurity mühelos über ⇒ www.itzert.com ⇐ Digital-Forensics-in-Cybersecurity Schulungsangebot
- Digital-Forensics-in-Cybersecurity Prüfungsmaterialien Digital-Forensics-in-Cybersecurity Schulungsangebot Digital-Forensics-in-Cybersecurity Testing Engine Öffnen Sie die Website « de.fast2test.com » Suchen Sie ⇒ Digital-Forensics-in-Cybersecurity ⇐ Kostenloser Download Digital-Forensics-in-Cybersecurity Fragenkatalog
- Digital-Forensics-in-Cybersecurity Deutsch Prüfungsfragen Digital-Forensics-in-Cybersecurity Examengine Digital-Forensics-in-Cybersecurity Online Tests Öffnen Sie die Webseite ✓ www.itzert.com ✓ und suchen Sie nach kostenloser Download von ✨ Digital-Forensics-in-Cybersecurity ✨ Digital-Forensics-in-Cybersecurity Deutsch Prüfung
- Neueste Digital-Forensics-in-Cybersecurity Pass Guide - neue Prüfung Digital-Forensics-in-Cybersecurity braindumps - 100% Erfolgsquote URL kopieren ▶ www.zertfragen.com ◀ Öffnen und suchen Sie [Digital-Forensics-in-Cybersecurity] Kostenloser Download Digital-Forensics-in-Cybersecurity Prüfungsmaterialien
- Digital-Forensics-in-Cybersecurity Torrent Anleitung - Digital-Forensics-in-Cybersecurity Studienführer - Digital-Forensics-

