KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **Digital Forensics in Cybersecurity**

Title : Digital Forensics in Cybersecurity (D431/C840) Course Exam

Version : DEMO

1.An organization believes that a company-owned mobile phone has been compromised.
Which software should be used to collect an image of the phone as digital evidence?
A. PTFinder
B. Forensic SIM Cloner
C. Forensic Toolkit (FTK)
D. Data Doctor
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Forensic Toolkit (FTK) is a widely recognized and trusted software suite in digital forensics used to acquire and analyze forensic images of devices, including mobile phones. FTK supports the creation of bit-by-bit images of digital evidence, ensuring the integrity and admissibility of the evidence in legal contexts. This imaging process is crucial in preserving the original state of the device data without alteration.
FTK enables forensic investigators to perform logical and physical acquisitions of mobile devices.
It maintains the integrity of the evidence by generating cryptographic hash values (MD5, SHA-1) to prove that the image is an exact copy.
Other options such as PTFinder or Forensic SIM Cloner focus on specific tasks like SIM card cloning or targeted data extraction but do not provide full forensic imaging capabilities.
Data Doctor is more aligned with data recovery rather than forensic imaging.
Reference: According to standard digital forensics methodologies outlined by NIST Special Publication 800-101 (Guidelines on Mobile Device Forensics) and the SANS Institute Digital Forensics and Incident Response guides, forensic tools used to acquire mobile device images must be capable of bit-stream copying with hash verification, which FTK provides.

2.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. Investigate whether the computer was properly seized
C. Enlist a colleague to witness the investigative process
D. Download a tool from a hacking website to extract the data
Answer: A
Explanation:
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.

3.A victim of Internet fraud fell for an online offer after using a search engine to find a deal on an expensive software purchase. Once the victim learned about the fraud, he contacted a forensic investigator for help.
Which digital evidence should the investigator collect?
A. Virus signatures
B. Whois records
C. Computer logs
D. Email headers
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In Internet fraud investigations, computer logs are critical because they provide a record of user activity, including browsing history, downloads, and system events. These logs can help establish a timeline, identify malicious access, and confirm fraudulent transactions.
Computer logs may include browser history, system event logs, and application logs that document the victim’s interaction with the fraudulent offer.
Whois records help identify domain registration details but are secondary evidence.
Email headers are relevant if communication via email was part of the fraud but less critical than logs that show direct interaction.
Virus signatures are used in malware investigations, not directly relevant to fraud evidence collection.
Reference: According to guidelines by the International Journal of Digital Crime and Forensics and the SANS Institute, capturing logs is essential in building a case for Internet fraud as it provides objective data about the victim’s system and activities.

4.A cybercriminal hacked into an Apple iPad that belongs to a company's chief executive officer (CEO). The cybercriminal deleted some important files on the data volume that must be retrieved.
Which hidden folder will contain the digital evidence?
A. /Private/etc
B. /lost+found
C. /.Trashes/501
D. /etc
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
On Apple iOS devices, deleted files are often moved to a hidden Trash folder before permanent deletion. The directory /.Trashes/501 is a hidden folder where deleted files for user ID 501 (the first user created on macOS/iOS devices) are temporarily stored.
This folder can contain files marked for deletion and thus is a prime location for recovery attempts.

/lost+found is a directory commonly used on Unix/Linux file systems for recovered file fragments after file system corruption but is not the default trash location on iOS.
/Private/etc and /etc contain system configuration files, not deleted user files.
Reference: Apple forensic investigations per NIST and training manuals such as those from Cellebrite and BlackBag Technologies indicate that user-deleted files on iOS devices reside in .Trashes or similar hidden directories until permanently removed.

5.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. Identity theft
B. SQL injection
C. Cyberstalking
D. Malware
Answer: A
Explanation:
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.