PassQueen
a.k.a dumpsqueen.com

Digital Forensics in Cybersecurity (D431/C840) Course Exam

WGU Digital-Forensics-in-Cybersecurity

Version Demo

Total Demo Questions: 9

Total Premium Questions: 98

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

What is a reason to use steganography?

A. To conceal secret data within an innocuous file

B. To highlight secret data

C. To erase secret data

D. To delete secret data

ANSWER: A

Explanation:

To conceal secret data within an innocuous file is a reason to use steganography. Steganography embeds a hidden message or payload into a seemingly ordinary carrier, such as an image, audio file, video, document, or network traffic, so that the existence of the secret communication is less noticeable. Its central purpose is concealment: a person viewing the carrier should generally perceive it as a normal file rather than recognize that it contains additional information. In digital forensics, this matters because investigators may need to identify suspicious files whose size, metadata, structure, or statistical characteristics suggest that hidden content could be present. Steganography can be used alongside encryption: encryption protects the readability of data, while steganography aims to avoid drawing attention to the data or its transmission in the first place. The National Institute of Standards and Technology describes steganography as concealing information in other information, and forensic practitioners use this concept when assessing potential hidden-data techniques. See the NIST definition of steganography and the UK NCSC cryptography guidance for related security context.

QUESTION NO: 2

Which tool identifies the presence of steganography?

A. Disk Investigator

B. DiskDigger

C. Forensic Toolkit (FTK)

D. ComputerCOP

ANSWER: A

Explanation:

Disk Investigator is the correct tool because it is designed to examine data at the disk and file-system level, including data that is not apparent through ordinary file browsing. In a forensic examination, steganography may be indicated by hidden content, unexpected data within a file, or file-system artifacts that warrant further analysis. Disk Investigator supports low-level inspection and searching of disk contents, helping an examiner identify concealed or anomalous data that can indicate the presence of steganographic material. This is an identification step: the examiner uses the tool to locate suspicious hidden data and then preserves and analyzes the relevant evidence using sound forensic procedures. The vendor describes Disk Investigator as a utility for discovering information hidden on a hard disk and recovering data, which aligns with its use in identifying concealed content during an examination. NIST likewise emphasizes examining media systematically and preserving evidence so findings can be validated and reproduced. See the Disk Investigator product information and NIST's Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 3

A forensic examiner is investigating a Windows computer suspected of containing a deleted spreadsheet. The examiner needs to determine the file's former name, directory path, size, and relevant timestamps before attempting content recovery.

Which NTFS artifact should the examiner examine first?

A. The Master File Table (MFT)

B. Unallocated space

C. The Windows Registry

D. The paging file

ANSWER: A

Explanation:

The Master File Table (MFT) is correct because NTFS stores a record for each file and directory in the MFT. An MFT record can contain metadata such as a file name, parent-directory reference, file size, timestamps, and allocation information. Even after deletion, the record may remain available until it is reused.

Unallocated space may contain remnants of the spreadsheet's content, but it does not provide the same structured file metadata. The Windows Registry stores system and configuration information rather than NTFS file records, and the pagefile may contain memory remnants but is not the primary source for deleted-file metadata.

QUESTION NO: 4

Which operating system (OS) uses the NTFS (New Technology File System) file operating system?

A. Linux

B. Mac OS X v10.5

C. Mac OS X v10.4

D. Windows 8

ANSWER: D

Explanation:

Windows 8 is correct because it uses NTFS as its standard, native file system for Windows installation volumes. NTFS was introduced with the Windows NT family and remains the primary Windows file system in modern desktop versions, including Windows 8. It provides the features expected for a contemporary operating system and for forensic examination, including support for access-control permissions, file and directory metadata, journaling that assists with recovery after system interruptions, compression, encryption through the Encrypting File System, and large volumes and files. In a digital-forensics context, recognizing NTFS is important because an examiner may encounter artifacts such as the Master File Table, the USN change journal, alternate data streams, and NTFS timestamps on Windows storage media. Microsoft’s Windows documentation identifies NTFS as the default file system for Windows installations and describes its reliability, security, and recovery capabilities. Microsoft also documents that NTFS is the file system used when installing Windows on a typical internal drive. See Microsoft’s NTFS overview and Microsoft’s file-system documentation.

QUESTION NO: 5

A forensic investigator is examining a Windows computer for evidence that unauthorized removable storage devices were connected to it. The investigator needs an artifact that can help identify USB mass-storage devices recognized by Windows.

Which Registry location is most relevant?

A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

B. HKEY_LOCAL_MACHINE\SAM

C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

D. HKEY_CURRENT_USER\Control Panel\Desktop

ANSWER: A

Explanation:

The USBSTOR Registry key is correct because Windows uses it to store information about USB mass-storage devices that have been installed or recognized by the system. The artifact can provide investigative leads about device manufacturer, product, and serial-number information, which can then be correlated with other system artifacts.

The SAM hive contains local account security information. The SOFTWARE hive contains application and operating-system configuration data, while the SYSTEM hive contains broader system configuration; however, USB mass-storage device entries are specifically associated with the USBSTOR key within the SYSTEM hive.

QUESTION NO: 6

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. BOOTMGR

B. NTLDR

C. Winload.exe

D. BCD

ANSWER: B

Explanation:

NTLDR is the correct Windows XP boot component. In the Windows NT boot architecture used by Windows XP and earlier NT-based versions, the system BIOS loads the NT Loader (NTLDR) from the active system partition. NTLDR switches the processor into the mode needed by Windows, reads the boot configuration contained in `boot.ini`, and presents a boot-selection menu when the file contains multiple operating-system entries or when its timeout setting requires the menu to be displayed. After an operating system is selected, NTLDR loads and works with the other required startup components to continue initialization of the selected Windows installation. This makes NTLDR and the contents of `boot.ini` relevant forensic artifacts when examining legacy Windows XP startup configuration, dual-boot choices, and potential boot-setting tampering. Microsoft's Windows XP deployment documentation identifies `Boot.ini` as the file used by the Windows NT boot loader to determine available operating systems and startup options. See Microsoft documentation on Boot.ini and Microsoft documentation on the Windows XP startup process.

QUESTION NO: 7

A forensic examiner receives a forensic image of a Windows computer. The examiner needs to determine whether a user opened a particular file from a mapped network share, even though the network share is no longer available.

Which artifact is most likely to provide the relevant evidence?

A. The Windows SAM hive

B. The pagefile

C. A shortcut file

D. The hosts file

ANSWER: C

Explanation:

A shortcut file is most likely to provide the relevant evidence because Windows commonly creates LNK files when users open documents through the graphical interface. A shortcut can retain the target's former network path and information about the associated volume or network location, even if the shared file is no longer accessible.

The Windows SAM stores local-account security data. The pagefile can contain residual memory data but is not the primary artifact for identifying a document's prior network path. The hosts file maps names to IP addresses and does not record documents opened by a user.

QUESTION NO: 8

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:

Ensure that any tools and techniques used are widely accepted is correct because Registry evidence may ultimately need to be explained, reproduced, and defended in a legal or organizational investigation. A forensic examiner should use validated, reliable methods that are recognized within the digital-forensics community and apply them in a manner that preserves evidentiary integrity. Widely accepted tools and techniques support repeatability: another qualified examiner should be able to review the acquired forensic image or Registry artifacts, use the documented method, and reach materially consistent results. This practice also helps establish that the findings were derived through a sound process rather than through an untested or improvised approach. The examiner should document the tool name and version, relevant settings, hashes for acquired evidence where applicable, the source Registry hive or artifact examined, timestamps, and each action taken. Such documentation connects the reported Registry findings to a transparent chain of handling and provides a basis for technical and legal scrutiny. The National Institute of Standards and Technology describes computer-forensic work as involving validated methods for acquisition, examination, analysis, and reporting. The Scientific Working Group on Digital Evidence likewise emphasizes validation and documentation of forensic processes. See NIST SP 800-86 and SWGDE published documents.

QUESTION NO: 9

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

ANSWER: B

Explanation:

That the phone avoids syncing with the computer is correct because automatic synchronization can change the contents and state of an iPhone as soon as it is connected to a host system. A sync process may write data to the device, such as updated metadata, backups, application-related information, media-management records, or other configuration artifacts. Those changes can compromise forensic soundness by altering potential evidence before it is documented and acquired. Before making the connection, the investigator should configure the forensic workstation to prevent automatic iPhone synchronization and should use a controlled acquisition process that minimizes writes to the device. This supports preservation of the original evidentiary state, repeatability of the acquisition, and a defensible chain of custody. NIST guidance for mobile-device forensics emphasizes preserving evidence and carefully controlling interactions with a mobile device during collection and examination. Apple also documents the ability to prevent iPhones from syncing automatically, a setting that is particularly important when attaching a device for forensic handling rather than ordinary device management. See NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics and Apple Support: Change device preferences in iTunes.