PassQueen
a.k.a dumpsqueen.com

Certification Exam For ENCE North America

Guidance Software GD0-100

Version Demo

Total Demo Questions: 21

Total Premium Questions: 216

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

If cluster #3552 entry in the FAT table contains a value of ?? this would mean:

A. The cluster is unallocated

B. The cluster is the end of a file

C. The cluster is allocated

D. The cluster is marked bad

ANSWER: A

Explanation:

“The cluster is unallocated” is correct when the intended FAT-table value represented by “??” is `00` (zero). In a File Allocation Table, each entry corresponds to a data cluster and records that cluster’s allocation status or, when allocated, the next cluster in its chain. A zero-valued FAT entry is the defined free-cluster marker: it indicates that no file or directory currently owns cluster #3552. Consequently, the operating system may select that cluster when it needs space to extend or create a file.

This distinction is important during forensic examination. A directory entry may still retain historical metadata that refers to a cluster after deletion, while the FAT entry being zero shows that the filesystem has released that cluster for reuse. The physical contents may therefore remain recoverable until overwritten, but the cluster is no longer allocated according to the active FAT allocation map. FAT uses specific reserved ranges for other conditions, including end-of-chain and defective-cluster indicators; zero is the conventional free/unallocated state. Microsoft’s FAT specification describes the use of FAT entries and reserved allocation values in the FAT File System Specification; additional filesystem background is available in the OSDev FAT documentation.

QUESTION NO: 2

Within EnCase for Windows, the search process is:

A. a search of the physical disk in unallocated clusters and other unused disk areas

B. a search of the logical files

C. both a and b

D. None of the above

ANSWER: C

Explanation:

both a and b is correct because EnCase’s forensic searching is designed to examine evidence at both the logical-file level and the physical-media level. Logical searching evaluates the contents and attributes of files and folders represented by the file system, allowing an examiner to locate relevant material in active, allocated files. Physical searching examines the acquired media data independently of normal file-system presentation, including unallocated clusters and other areas that are not currently assigned to a live file. This is essential because data of evidentiary value can remain after deletion or may reside in file-system slack and other unused areas of a volume.

Using both perspectives provides a more complete forensic search: the logical view supplies file-system context, while the physical view helps identify remnants that are not available through ordinary file browsing. This approach is consistent with forensic best practice to examine allocated and unallocated data when analyzing storage media. OpenText describes EnCase Forensic as a platform for acquiring and examining digital evidence, and NIST’s forensic guidance discusses recovering and analyzing data from storage media, including deleted material. See OpenText EnCase Forensic and NIST SP 800-86.

QUESTION NO: 3

Within EnCase, what is the purpose of the temp folder?

A. This is the folder used to hold copies of files that are sent to external viewers.

B. This is the folder that will automatically store an evidence file when the acquisition is made in DOS.

C. This is the folder that temporarily stores all bookmark and search results.

D. This is the folder that will be automatically selected when the copy/unerase feature is used. This is the folder that will be automatically selected when the copy/unerase feature is used.

ANSWER: A

Explanation:

This is the folder used to hold copies of files that are sent to external viewers. EnCase uses an external viewer when an examiner opens an item with an application outside the EnCase interface, such as a document reader, image viewer, or media player. The external application generally requires an accessible file on the examiner's working system rather than direct access to the evidence object within the case. EnCase therefore creates a temporary working copy in the configured Temp folder and passes that copy to the selected viewer. This design preserves the original evidence and allows the viewer to operate on a separate file copy. The Temp-folder location should consequently have sufficient free space, be writable by the examiner, and be managed according to laboratory procedures because it can contain derived copies of evidentiary material. EnCase's forensic workflow is built around maintaining evidence integrity while supporting review and analysis functions; its product overview describes the platform's forensic examination and evidence-analysis role. See OpenText EnCase Forensic and the OpenText Support portal for product documentation and support resources.

QUESTION NO: 4

What is the purpose of bookmarking an item in an EnCase case?

A. To identify an item for later review and reporting.

B. To modify the original evidence file.

C. To calculate a new hash for the evidence file.

D. To restore the item to the suspect drive.

ANSWER: A

Explanation:

Bookmarking identifies an item as relevant to the examiner's work and preserves it as part of the case-specific examination record. A bookmark can be used to organize notable files, search hits, artifacts, or other evidence items for later review and reporting.

A bookmark does not alter the source evidence file, change the file's hash value, or export the item from the case. The bookmark information is maintained with the examiner's case work product, allowing the examiner to return to the selected item during subsequent analysis. OpenText provides product information for EnCase Forensic; general evidence documentation principles are described in NIST SP 800-86.

QUESTION NO: 5

Which of the following are NTFS metadata artifacts that may be useful during a forensic examination?

A. $MFT

B. $LogFile

C. $UsnJrnl

D. File Allocation Table

ANSWER: A B C

Explanation:

$MFT, **$LogFile**, and **$UsnJrnl** are correct. The Master File Table, or `$MFT`, contains records describing files and directories on an NTFS volume. `$LogFile` records NTFS transactional activity used to maintain file-system consistency. The Update Sequence Number Journal, commonly examined through `$UsnJrnl`, can contain records of file and directory changes.

A FAT is not an NTFS metadata artifact. FAT volumes use a File Allocation Table to track cluster allocation, whereas NTFS uses its own metadata structures. Microsoft provides technical background on NTFS in its NTFS overview.

QUESTION NO: 6

Which of the following are valid reasons to calculate and record hash values during a forensic examination?

A. Verify that an acquired image remains unchanged.

B. Compare a file with a known hash library.

C. Document the integrity of exported evidence.

D. Decrypt an encrypted file.

ANSWER: A B C

Explanation:

Cryptographic hash values provide a fixed-length representation of data. In a forensic workflow, an examiner can compare hash values calculated at different points in handling to determine whether the represented data has remained unchanged. Hashes are also used to identify files matching entries in known-file libraries or investigator-created hash sets.

Accordingly, verifying that an acquired image remains unchanged, comparing a file to a known hash library, and documenting the integrity of exported evidence are valid uses. A hash does not decrypt an encrypted file; it identifies data based on its content. See FIPS 180-4: Secure Hash Standard and the NIST National Software Reference Library.

QUESTION NO: 7

The EnCase default export folder is:

A. A case-specific setting that cannot be changed.

B. A case-specific setting that can be changed.

C. A global setting that can be changed.

D. A global setting that cannot be changed.

ANSWER: C

Explanation:

The correct answer is **"A global setting that can be changed."** In EnCase, the default export folder is an application-level preference used to supply an initial destination when an examiner exports files or other evidence-derived output. Because it is stored as part of EnCase's general configuration rather than being fixed permanently within an individual case, the examiner can modify the configured location to suit an organization's evidence-processing workflow, storage layout, or available disk capacity. A changed default applies as the starting export location for subsequently used cases and export

operations, although an examiner can still select an appropriate destination during a particular export when needed. This distinction is operationally important: the default folder provides consistency and convenience across work, while the actual exported material should be handled in accordance with the case's evidence-management procedures. EnCase Forensic is designed to support configurable forensic workflows and export of evidentiary data; see the OpenText EnCase Forensic product information and the OpenText Support portal for product documentation and version-specific configuration guidance.

QUESTION NO: 8

You are at an incident scene and determine that a computer contains evidence as described in the search warrant. When you seize the computer, you should:

A. Record nothing to avoid inaccuracies that might jeopardize the use of the evidence.

B. Record the location that the computer was recovered from.

C. Record the identity of the person(s) involved in the seizure.

D. Record the date and time the computer was seized.

ANSWER: B C D

Explanation:

Proper seizure documentation establishes the evidence's identity, condition, origin, and chain of custody from the moment it is collected. Recording the location that the computer was recovered from ties the device to its physical context at the incident scene, which may be important to demonstrate relevance to the warrant and subsequent examination. Recording the identity of the person or people involved in the seizure establishes accountability: it identifies who collected and handled the device during the initial transfer into evidence custody. Recording the date and time the computer was seized creates a reliable chronological record and supports a complete chain of custody. Together, these contemporaneous details help show that the computer presented for forensic analysis is the same item seized at the scene and that it was appropriately controlled throughout handling. Digital-evidence best practice also calls for preserving the original evidence and maintaining documentation sufficient for another qualified examiner to understand the collection and handling process. See the U.S. Department of Justice's Electronic Crime Scene Investigation guide and NIST's Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 9

The following keyword was typed in exactly as shown. Choose the answer(s) that would be found. All search criteria have default settings. Tom

A. Tomorrow

B. TomJ@hotmail.com

C. Tom

D. Stomp

ANSWER: A B C D

Explanation:

With default EnCase keyword-search criteria, the entered text *Tom* is treated as a character string rather than being limited to complete words. The default search is also case-insensitive, so the matching sequence can occur at the beginning of a longer word, within an email address or other continuous text, as a standalone value, or within a larger word using a lowercase initial letter. Therefore, *Tomorrow* contains the sequence "Tom" at its start; *TomJ@hotmail.com* begins with that same sequence; and the standalone value *Tom* is an exact match. *Stomp* also contains the sequence "tom," and case-insensitive matching allows it to be located despite the lowercase "t" in that position. This behavior is important when reviewing keyword hits: a simple keyword can produce both exact and embedded-string results unless the examiner explicitly configures a whole-word or other narrowing criterion. EnCase is designed to index and search forensic evidence

efficiently, with keyword-search settings determining how literal text is matched. See the OpenText EnCase Forensic product page and the OpenText Digital Forensics overview for product documentation and capability context.

QUESTION NO: 10

When can an evidence file containing a NTFS partition be logically restored to a FAT 32 partition?

A. Never

B. When the FAT 32 has the same number of sectors / clusters.

C. When the FAT 32 is the same size or bigger.

D. Both B and C

ANSWER: D

Explanation:

An evidence file containing an NTFS partition can be logically restored to a FAT32 partition when the FAT32 destination has the same number of sectors per cluster and is the same size or larger. A logical restore operates at the file-system level rather than writing the original NTFS partition structures sector-for-sector. EnCase must therefore be able to reproduce the file and directory content using an allocation-unit layout compatible with the destination volume. Matching the sectors-per-cluster value preserves the required cluster geometry for the restoration process, while a destination that is at least as large ensures sufficient addressable storage for the restored content and its file-system overhead.

This is distinct from a physical restoration, which reproduces the original disk or partition data directly and consequently requires an appropriate raw target layout. The logical restoration workflow is intended to reconstruct accessible data onto a compatible target file system; FAT32's cluster-based allocation design makes both the allocation-unit requirement and adequate destination capacity material conditions. OpenText identifies EnCase Forensic as a platform for forensic acquisition, examination, and evidence handling: OpenText EnCase Forensic. Microsoft's FAT file-system specification also describes FAT volumes in terms of sectors and clusters: Microsoft FAT Specification.

QUESTION NO: 11

When connecting a suspect hard drive to a forensic workstation for acquisition, which practices help reduce the risk of altering the original evidence?

A. Use a validated write-blocking device.

B. Document the connection and acquisition process.

C. Confirm that the device is operating in read-only mode.

D. Boot the suspect operating system before imaging.

ANSWER: A B C

Explanation:

Using a **validated write-blocking device**, **documenting the connection and acquisition process**, and **verifying that the device is operating in read-only mode** are correct. A write blocker is intended to allow the forensic workstation to read the evidence device while preventing commands that would modify it. Documentation identifies the source device, connection method, tools, settings, and actions used during acquisition. Confirming the read-only state helps demonstrate that the original drive was protected before imaging began.

Booting the suspect operating system is not appropriate for a conventional dead-box acquisition because normal startup can write logs, update metadata, and otherwise change the evidence drive. The acquisition should be performed using a controlled forensic process that preserves the original media. See NIST SP 800-86 for digital-evidence preservation guidance.

QUESTION NO: 12

You are investigating a case of child pornography on a hard drive containing Windows XP. In the C:\Documents and Settings\Bad Guy\Local Settings \Temporary Internet Files folder you find three images of child pornography. You find no other copies of the images on the suspect hard drive, and you find no other copies of the filenames. What can be deduced from your findings?

A. The presence and location of the images is not strong evidence of possession.

B. The presence and location of the images is strong evidence of possession.

C. The presence and location of the images proves the images were intentionally downloaded.

D. Both a and c

ANSWER: A

Explanation:

The presence and location of the images is not strong evidence of possession. Under Windows XP, Internet Explorer's Temporary Internet Files cache can receive and retain content automatically when a web page is visited. Images displayed as page elements, embedded advertising, redirected content, or other browser-requested resources may therefore be written to this folder without a separate, deliberate save action by the user. The fact that the three images appear only in this browser-cache location, with no duplicate files and no additional occurrences of their filenames elsewhere on the drive, provides limited evidence from which to infer knowing acquisition, control, or intentional retention.

A sound forensic conclusion must distinguish an artifact's existence from the user activity it can reliably establish. Here, the cache artifacts can support the narrower finding that the browser obtained the image data during web activity, subject to normal forensic validation of timestamps, browser records, and file metadata. They do not, by themselves, establish the level of knowledge or control generally needed to characterize the finding as strong possession evidence. NIST's guidance stresses that forensic conclusions should be based on validated examination and careful interpretation of artifacts in context: NIST SP 800-86. Additional browser-cache context is described in the SANS browser forensics paper.

QUESTION NO: 13

Which of the following Windows artifacts can provide information related to local user accounts or user activity?

A. The SAM database

B. User profile directories

C. The Windows Security event log

D. The Master Boot Record

ANSWER: A B C

Explanation:

The **SAM database**, **user profile directories**, and the **Windows Security event log** can provide relevant information. The Security Accounts Manager database contains local account and group information. User profile directories can contain files and application data associated with particular users. Security-event records can include logon and account-related activity when the applicable auditing has been enabled.

The Master Boot Record is not an account or user-activity artifact. It contains boot and partitioning information for a traditional MBR disk. A complete examination should correlate artifacts from multiple sources because the availability and meaning of records depend on system configuration, audit policy, and user behavior. Microsoft provides background on Windows event logging through its Event Logging documentation.

QUESTION NO: 14

The BIOS chip on an IBM clone computer is most commonly located on:

A. The RAM chip

B. The controller card

C. The motherboard

D. The microprocessor

ANSWER: C

Explanation:

The motherboard is correct because the BIOS firmware is stored in non-volatile memory mounted directly on the system board. On older IBM-compatible ("clone") computers, this firmware was commonly held in a dedicated ROM, EPROM, or flash-ROM chip. During startup, the processor begins executing the firmware code from this system firmware storage. The BIOS performs fundamental initialization, including checking and configuring key hardware, running the power-on self-test process, and locating a bootable device before transferring control to an operating system boot loader.

Modern systems often use the term UEFI rather than BIOS, and the firmware is generally stored in a flash-memory device soldered to or otherwise installed on the motherboard. Despite changes in firmware design and terminology, the essential architectural point remains the same: system startup firmware belongs to the motherboard because it must initialize the platform's processor, memory, chipset, and onboard hardware before normal software can run. Intel's overview of UEFI firmware architecture describes firmware as platform-level code responsible for early boot functions, while the UEFI specification defines the firmware interfaces used during system initialization and boot. See Intel's BIOS and UEFI overview and the UEFI Specifications.

QUESTION NO: 15

How does EnCase verify that the evidence file contains an exact copy of the suspect hard drive? How does

EnCase verify that the evidence file contains an exact copy of the suspect's hard drive?

A. By means of a CRC value of the suspect hard drive compared to a CRC value of the data stored in the evidence file.

B. By means of an MD5 hash of the suspect hard drive compared to an MD5 hash of the data stored in the evidence file.

C. By means of a CRC value of the evidence file itself.

D. By means of an MD5 hash value of the evidence file itself.

ANSWER: B

Explanation:

By means of an MD5 hash of the suspect hard drive compared to an MD5 hash of the data stored in the evidence file is correct. EnCase acquisition is designed to preserve forensic integrity by calculating a cryptographic hash value for the acquired source data and recording verification information in the evidence file. After acquisition, EnCase can calculate the MD5 value for the data represented by the evidence file and compare it with the value obtained from the original drive. Matching values provide strong evidence that the evidence data is an exact bit-for-bit representation of the acquired source at the time the hashes were calculated. This verification process is fundamental to maintaining evidentiary integrity, because it provides a repeatable, documented method for detecting any change to the acquired data. In the era covered by this certification exam, MD5 was a standard EnCase verification hash; modern forensic workflows commonly also record stronger hashes, such as SHA-256, for additional assurance. The underlying principle remains that verification depends on comparing the source-data hash with the acquired evidence-data hash. See OpenText's EnCase Forensic product information and NIST's hash functions guidance.

QUESTION NO: 16

What information should be obtained from the BIOS during computer forensic investigations?

A. The video caching information

B. The date and time

C. The port assigned to the serial port

D. The boot sequence

ANSWER: B D

Explanation:

During initial forensic handling, the BIOS date and time should be documented because they establish the system clock setting at the time of examination. Investigators can compare this hardware-maintained setting with a trusted reference time and record any offset. That information is essential when later interpreting file-system MAC timestamps, event logs, application records, and other time-based artifacts; it supports a defensible explanation of whether displayed timestamps may be shifted from actual time.

The boot sequence should also be obtained and documented. BIOS/firmware boot-order settings identify the device the computer is configured to start from and help the examiner plan a controlled acquisition. In particular, this information helps ensure that a forensic boot device is used only in a manner that does not unintentionally boot the installed operating system and alter evidence. Recording relevant firmware configuration before making changes also preserves the original system state in contemporaneous examination notes. NIST's computer-forensics guidance emphasizes documenting system information and preserving evidence during collection, while the NIJ guide addresses careful handling and documentation during seizure and examination. See NIST SP 800-86 and NIJ Electronic Crime Scene Investigation guide.

QUESTION NO: 17

This question addresses the EnCase for Windows search process. If a target word is located in the unallocated space, and the word is fragmented between clusters 10 and 15, the search:

A. Will not find it because the letters of the keyword are not contiguous.

B. Will not find it because EnCase performs a physical search only.

C. Will find it because EnCase performs a logical search.

D. Will not find it unless file slack is checked on the search dialog box.

ANSWER: A

Explanation:

Will not find it because the letters of the keyword are not contiguous. In unallocated space, the filesystem no longer provides reliable file-record information that associates separated clusters as parts of one logical file. A standard keyword search of this area evaluates the byte stream available at each physical location and requires the keyword's characters or encoded bytes to occur consecutively. If part of the target word is in cluster 10 and the remainder is in cluster 15, with noncontiguous storage between them, the complete byte sequence is absent from the search stream and cannot match as one keyword occurrence.

This distinction is important in forensic examinations because deleted or unallocated data can be fragmented. Recovering such content may require file carving, examination of filesystem metadata where it remains available, or reconstruction techniques rather than reliance on a simple literal keyword hit. NIST's forensic guidance discusses the need to preserve and examine data at the physical-media level, including deleted and unallocated areas: NIST SP 800-86. OpenText provides current information on the EnCase Forensic platform and its forensic-analysis capabilities at OpenText EnCase Forensic.

QUESTION NO: 18

What files are reconfigured or deleted by EnCase during the creation of an EnCase boot disk?

A. command.com

B. autoexec.bat

C. drvspace.bin

D. io.sys

ANSWER: A C D

Explanation:

During EnCase boot-disk creation, **command.com**, **drvspace.bin**, and **io.sys** are handled as part of preparing a controlled DOS boot environment. **command.com** is the DOS command interpreter needed to provide the shell from which the acquisition environment runs. **io.sys** is a core DOS startup file, loaded early in the boot sequence, so its presence and configuration must be appropriate for the boot media to start reliably. **drvspace.bin** is associated with DriveSpace disk compression; EnCase eliminates or reconfigures it so that compression-related behavior does not interfere with direct, predictable access to storage devices during forensic acquisition. This preparation supports a known boot state and reduces the risk that pre-existing boot-media configuration affects evidence collection. Microsoft's overview of the DOS boot process identifies IO.SYS and COMMAND.COM as essential operating-system startup components: Windows 98 Resource Kit: Boot Process. Product background and current EnCase forensic resources are available from OpenText EnCase Forensic.

QUESTION NO: 19

The following GREP expression was typed in exactly as shown. Choose the answer(s) that would result. [^a-z] Tom[^a-z]

A. Tomato

B. Tom

C. Toms

D. Stomp

ANSWER: B

Explanation:

Tom is the intended result because the expression uses a negated character class, `[^a-z]`, to establish delimiters around the target text. A caret at the beginning of a bracket expression negates the specified range, so this construct represents a character that is not a lowercase letter from `a` through `z`. The literal text `Tom` is case-sensitive as written and is therefore sought with an uppercase `T` followed by lowercase `om`. In practical GREP searching, this pattern is used to locate the standalone name Tom when it is bounded by non-lowercase-letter context, rather than locating that character sequence as part of a longer lowercase word. The expression is particularly useful in forensic text searches where an examiner needs a more precise hit than a simple search for the three characters alone. Bracket expressions and negated character classes are standard regular-expression mechanisms; the GNU GREP manual describes bracket expressions and their matching behavior at GNU GREP: Character Classes and Bracket Expressions. Additional background on negated character classes is available from Regular-Expressions.info: Character Classes.

QUESTION NO: 20

The following keyword was typed in exactly as shown. Choose the answer(s) that would result. All search criteria have default settings. Tom Jones

A. tom jones

B. Tom

C. Jones

D. Tom Jones

ANSWER: A D

Explanation:

With the default EnCase keyword-search settings, the entered text is treated as the two-word keyword phrase “Tom Jones,” and matching is not case-sensitive. Therefore, a document occurrence written as “tom jones” is returned even though its capitalization differs from the entered keyword. An occurrence written as “Tom Jones” is also returned because it matches the entered phrase exactly. The space between the terms remains part of the entered keyword phrase; the search is evaluating the phrase as typed rather than changing capitalization into a distinct criterion. This behavior supports common forensic review workflows, where an examiner normally needs to locate a person’s name regardless of how a document author capitalized it. EnCase’s keyword-search and indexing capabilities are part of its forensic analysis workflow; keyword settings can be refined when a case requires case-sensitive or other more restrictive matching. See the OpenText EnCase Forensic product information and the OpenText EnCase platform overview for product context and investigative-search capabilities.

QUESTION NO: 21

Which of the following items could contain digital evidence?

A. Credit card readers

B. Personal assistant devices

C. Cellular phones

D. Digital cameras

ANSWER: A B C D

Explanation:

Credit card readers, personal assistant devices, cellular phones, and digital cameras can all contain digital evidence because each is a digital device that may store data locally, retain data in nonvolatile memory, or record information relevant to an investigation. Credit card readers and point-of-sale peripherals can retain transaction-related records, configuration information, device identifiers, and event data. Personal assistant devices and cellular phones commonly contain contacts, calendars, messages, call information, application data, location-related artifacts, and user-created files. Digital cameras can hold image and video files, removable-media contents, file-system metadata, and potentially location data recorded with photographs. From an EnCase examination perspective, potentially relevant evidence is not limited to conventional computers: any device capable of processing, storing, or transmitting digital information should be identified, preserved, and examined using appropriate acquisition methods. The nature and location of the evidence will depend on the device model, its storage media, its operating state, and whether associated removable media or synchronized systems are available. NIST’s mobile-device forensic guidance similarly recognizes that handheld and mobile devices can provide substantial evidentiary data and require sound preservation and collection procedures. See NIST SP 800-101 Rev. 1 and NIST Computer Forensics Tool Testing Program.