DUMPSARENA

Certification Exam for EnCE Outside North America

Guidance Software GD0-110

Version Demo

Total Demo Questions: 19

Total Premium Questions: 192

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Topic 0, A	172
Total	192

QUESTION NO: 1

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

A. Credit

B. Card

C. Credit Card

D. credit card

ANSWER: C D

Explanation:

With default EnCase keyword-search settings, the entered text is treated as the two-word search phrase *credit card*. The default search is not case-sensitive, so the same phrase is identified regardless of whether its initial letters appear in uppercase or lowercase. Therefore, both *Credit Card* and *credit card* represent matches for the entered keyword. The significant condition is that the words occur together as the specified phrase, in the entered order, rather than merely occurring independently elsewhere in the data. This behavior supports forensic review by allowing an examiner to enter a natural-language phrase without having to create separate capitalization variants for the same evidentiary term. EnCase's keyword-search workflow is designed to locate relevant text within the acquired evidence and present searchable results for examiner review; the examiner can later refine searches using more explicit criteria when needed. See the OpenText EnCase Forensic product information and the OpenText EnCase overview.

QUESTION NO: 2

RAM is an acronym for:

A. Random Access Memory

B. Relative Address Memory

C. Random Addressable Memory

D. Relative Addressable Memory

ANSWER: A

Explanation:

Random Access Memory is correct. RAM is the computer's short-term working memory: it holds the operating system instructions, program code, and data that the processor needs to access quickly while a system is running. The word "random" refers to the ability to access a memory location directly in approximately the same amount of time regardless of its physical position, rather than having to read through preceding locations sequentially. In digital forensic work, RAM is particularly important because it can contain volatile evidence that may not be preserved on persistent storage, such as running processes, network connections, decrypted material, command history, and other active system artifacts. Since ordinary RAM loses its contents when power is removed, forensic best practice is to consider collecting volatile data before shutting down or otherwise altering a live system, subject to the case's legal authority and documented procedures. The National Institute of Standards and Technology describes volatile data collection as a key component of live-response and incident-handling activities. See NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response and Encyclopaedia Britannica: RAM.

QUESTION NO: 3

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

A. The cluster is allocated

B. The cluster is unallocated

C. The cluster is marked bad

D. The cluster is the end of a file

ANSWER: B

Explanation:

The cluster is unallocated is the intended correct answer, based on the standard FAT interpretation of a zero-valued FAT entry. In a File Allocation Table, each cluster has a corresponding entry that records its allocation status or, for an allocated cluster, identifies the next cluster in that file's chain. A value of zero denotes that no file or directory currently owns the cluster; consequently, it is available for allocation. This is a key distinction during forensic examination: a directory entry may retain metadata for a deleted file, while the clusters formerly associated with it can be identified as free when their FAT entries have been cleared to zero. Examiners should therefore treat a zero FAT entry as evidence that the cluster is presently unallocated, while recognizing that its underlying content may remain recoverable until overwritten. FAT reserved values, bad-cluster markers, and end-of-chain markers use nonzero values that vary by FAT type. The question appears to have omitted the displayed value, but its keyed interpretation corresponds to zero. See the OSDev FAT documentation for FAT entry status values and Microsoft's File Allocation Table overview for FAT structure background.

QUESTION NO: 4

To later verify the contents of an evidence file?

A. EnCase writes an MD5 hash value for every 32 sectors copied.

B. EnCase writes a CRC value for every 64 sectors copied.

C. EnCase writes a CRC value for every 128 sectors copied.

D. EnCase writes an MD5 hash value every 64 sectors copied.

ANSWER: B

Explanation:

EnCase writes a CRC value for every 64 sectors copied. This is the correct statement because the traditional EnCase evidence-file format stores the acquired data in chunks and associates each 64-sector block with a cyclic redundancy check value. During subsequent processing, examination, or verification, EnCase can recalculate the CRC for a stored block and compare it with the value recorded during acquisition. Matching values provide block-level confirmation that the evidence data remains consistent with what was originally written to the evidence file.

This per-block integrity information is especially useful for identifying the location of a read, storage, or transfer problem without treating the entire image as an indivisible unit. It complements the broader acquisition-level hash values used to establish the identity and integrity of the evidence item as a whole. The design reflects the forensic requirement to preserve acquired evidence and be able to demonstrate that its contents have not changed throughout handling and analysis. OpenText identifies EnCase Forensic as a platform for collecting and preserving digital evidence; see the OpenText EnCase Forensic product page. For general forensic guidance on maintaining evidence integrity and verification, see NIST SP 800-86.

QUESTION NO: 5

Before utilizing an analysis technique on computer evidence, the investigator should:

A. Be trained in the employment of the technique.

B. Test the technique on simulated evidence in a controlled environment to confirm that the results are consistent.

C. Both be trained in the employment of the technique and test the technique on simulated evidence in a controlled environment to confirm that the results are consistent.

D. Neither a or b.

ANSWER: C

Explanation:

Both being trained in the technique and testing it on simulated evidence in a controlled environment to confirm consistent results are essential prerequisites to applying a forensic analysis technique to actual computer evidence. Training gives the examiner the competence to select, configure, execute, and interpret the technique properly, while controlled validation establishes that the method produces repeatable, reliable results under known conditions. Together, these practices support sound forensic methodology: evidence should be examined using documented processes that are understood by the examiner and whose output can be demonstrated, reproduced, and defended. This is particularly important because forensic conclusions may be reviewed by another examiner, challenged in legal proceedings, or relied on for investigative decisions. NIST's guidance on integrating forensic techniques emphasizes using validated tools and methods, preserving the integrity of evidence, and ensuring that examination results can be appropriately analyzed and reported. NIST's more general testing guidance also frames validation as establishing that a method performs as intended for its defined use. See NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response and NIST Forensic Science Methods and Practices.

QUESTION NO: 9

In hexadecimal notation, one byte is represented by _____ character(s).

A. 1

B. 2

C. 4

D. 8

ANSWER: B

Explanation:

2 is correct. A byte consists of 8 bits. Each hexadecimal character represents exactly 4 bits, because hexadecimal is a base-16 numbering system with 16 possible values per digit: 0 through 9 and A through F. Therefore, two hexadecimal characters represent 4 bits + 4 bits, totaling 8 bits, which is one byte. For example, the byte value 11111111 in binary is written as FF in hexadecimal; similarly, the binary byte 01001010 is written as 4A. This compact representation is fundamental in computer forensics because raw disk data, memory contents, file signatures, offsets, and hash values are frequently displayed and examined in hexadecimal. Reading a hexadecimal view accurately requires recognizing that each pair of adjacent hexadecimal characters corresponds to one underlying byte of data. Guidance Software EnCase presents raw evidence data in forms that include hexadecimal representations, making this conversion a basic prerequisite for interpreting artifact values and byte-level structures. The relationship is also documented in the NIST reference material on binary quantities and the Hexadecimal number system overview.

QUESTION NO: 10

Will EnCase allow a user to write data into an acquired evidence file?

A. Yes, but only case information.

B. Yes, but only bookmarks.

C. Yes, but only to resize the partitions.

D. No, unless the user established a writing privilege when the evidence was acquired.

E. No. Data cannot be added to the evidence file after the acquisition is made.

ANSWER: E

Explanation:

No. Data cannot be added to the evidence file after the acquisition is made. EnCase's forensic-evidence workflow is designed to preserve the acquired evidence as an immutable forensic record. Once an acquisition has produced an evidence file, the examiner analyzes that preserved data rather than writing user data, case artifacts, or analysis results back into it. This separation protects the integrity of the original acquired content and supports repeatable verification through hashes and auditability. Examiner-generated material, such as bookmarks, notes, reports, and case-management information, is maintained as case or examination data rather than becoming new content in the acquired evidence file. Maintaining this distinction is essential to forensic soundness: the source evidence must remain stable so that later examination and validation can demonstrate that the acquired data has not changed. OpenText describes EnCase Forensic as a solution for collecting and preserving digital evidence; see OpenText EnCase Forensic. The same preservation principle is reflected in NIST guidance, which emphasizes preserving the integrity of collected digital evidence throughout forensic handling; see NIST SP 800-86.

QUESTION NO: 11

EnCase is able to read and examine which of the following file systems?

A. NTFS

B. FAT

C. EXT3

D. HFS

ANSWER: A B C D

Explanation:

EnCase forensic examination support extends across the principal file systems encountered on Windows, legacy removable-media and DOS/Windows volumes, Linux/UNIX systems, and Apple Macintosh media. NTFS is the standard Windows file system and can be examined for its metadata, directory structures, allocated content, and recoverable unallocated data. FAT encompasses the FAT-family formats commonly found on older Windows systems and removable storage, whose directory entries and allocation structures can likewise be interpreted during an EnCase examination. EXT3 is a Linux file system supported for examination, including its native file-system structures and journal-related artifacts where present. HFS refers to the Macintosh HFS family; EnCase supports examination of Apple-formatted volumes, allowing an examiner to navigate their structures and recover relevant evidence. These capabilities allow a single case to include images from heterogeneous operating systems without requiring the examiner to convert the evidence to a different format first. EnCase's forensic workflow is designed around preserving the original evidence while parsing supported file-system metadata for review and reporting. OpenText describes EnCase Forensic as a platform for collecting, processing, and examining digital evidence across varied endpoint environments: OpenText EnCase Forensic. Independent forensic-tool testing context is available from the NIST Computer Forensics Tool Testing Program.

QUESTION NO: 12

EnCase marks a file as overwritten when _____ has been allocated to another file.

A. any part of the file

B. all of the file

C. the starting cluster of the file

D. the directory entry for the file

ANSWER: C

Explanation:

the starting cluster of the file is correct. In EnCase forensic analysis, a deleted file's recoverability is evaluated from the allocation status of the clusters needed to reconstruct it. The starting cluster is the initial location recorded for the file's data stream and is the entry point EnCase uses to follow the file's cluster chain. Once that starting cluster has been reallocated to a different file, the original file's data chain can no longer be reliably followed from its recorded beginning. EnCase therefore identifies the deleted file as overwritten. This status is important when assessing whether a deleted item can be recovered intact and when documenting the limits of recovered evidence. The underlying principle follows filesystem allocation structures: directory metadata identifies the beginning of file content, while allocation information links the remaining storage units. For background on examining filesystem metadata and allocated or unallocated content in forensic tools, see The Sleuth Kit documentation. For EnCase's forensic-product context and capabilities, see OpenText EnCase Forensic.

QUESTION NO: 13

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 the location that the computer was recovered from.

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

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

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

ANSWER: A B C

Explanation:

Recording the location that the computer was recovered from, the identity of the person(s) involved in the seizure, and the date and time the computer was seized establishes essential chain-of-custody and evidence-provenance information. The recovery location ties the device to its physical context at the scene, which can be important when demonstrating why the device fell within the warrant's scope and how it was associated with the investigation. Identifying the personnel who seized or handled the computer creates accountability and supports a continuous record of possession. Documenting the seizure date and time establishes when control of the device transferred to investigators and helps correlate the device with scene activity, photographs, notes, transport records, and later forensic processing.

These details should be captured contemporaneously in seizure documentation and maintained with the evidence record. Digital-evidence best practice emphasizes preserving the original item, documenting every handling event, and maintaining records sufficient to demonstrate that the item examined is the same item recovered. This documentation supports reliable evidence handling from the incident scene through storage, forensic acquisition, examination, and any legal proceeding. See the U.S. National Institute of Standards and Technology's Guide to Integrating Forensic Techniques into Incident Response and the U.S. Department of Justice's Electronic Crime Scene Investigation guide.

QUESTION NO: 14

The EnCase evidence file logical filename can be changed without affecting the verification of the acquired evidence.

A. True

B. False

ANSWER: A

Explanation:

True is correct. In an EnCase evidence file, the logical filename is descriptive case metadata rather than part of the acquired source data used to establish evidence integrity. It identifies the evidence item meaningfully within the examination, but it does not alter the sectors or files captured from the original media. EnCase verification evaluates the integrity of the acquisition through the evidence data and its stored integrity values, including the acquisition hash and the format's internal

chunk-level checks. Therefore, changing this logical label does not change the acquired content and does not invalidate successful verification of that content.

This distinction is important in forensic workflow: examiners may need to correct a naming error, apply a clearer exhibit identifier, or standardize evidence-item labels after acquisition. Such administrative metadata maintenance can be performed while preserving the ability to demonstrate that the actual acquired evidence remains unchanged. The evidentiary significance rests on repeatable integrity verification of the captured data, not on the display name assigned to the evidence object. OpenText describes EnCase Forensic as supporting defensible forensic collection and analysis; see OpenText EnCase Forensic. For background on the EnCase/EWF evidence format's separation of stored data, metadata, and integrity information, see the libewf EWF format project.

QUESTION NO: 15

Which of the following would most likely be an add-in card?

A. A motherboard

B. The board that connects to the power supply

C. A video card that is connected to the motherboard in the AGP slot

D. Anything plugged into socket 7

ANSWER: C

Explanation:

A video card that is connected to the motherboard in the AGP slot is an add-in card because it is a separate expansion circuit board installed into an expansion slot on the system motherboard. Add-in cards extend or provide hardware capabilities that are not necessarily built directly into the motherboard, such as graphics, network connectivity, sound, storage control, or specialized acquisition interfaces. In this case, AGP (Accelerated Graphics Port) was a dedicated motherboard expansion interface designed specifically for graphics adapters. A video adapter inserted into that slot is therefore a classic example of an add-in card. Although AGP is now obsolete and has largely been replaced by PCI Express, systems contemporary with AGP used it to connect discrete graphics hardware to the motherboard. Understanding the distinction matters in computer hardware identification and forensic examination: an add-in card is generally removable and interfaces with the motherboard through a defined expansion connector, while the motherboard itself is the primary system board. Intel's AGP overview describes AGP as an interface for graphics adapters, and the PC architecture reference below provides additional context on expansion cards and slots. See Intel Support: Accelerated Graphics Port and The PC Guide: Expansion Slots.

QUESTION NO: 17

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. Tom

C. Stomp

D. TomJ@hotmail.com

ANSWER: A B C D

Explanation:

With EnCase's default keyword-search behavior, a plain keyword is evaluated as text occurring anywhere within a searchable item rather than as a whole-word-only expression. The default search is also not restricted to matching the capitalization used when the keyword was entered. Consequently, the contiguous character sequence "tom" is detected in

“Tomorrow,” in the standalone word “Tom,” within “Stomp,” and in the local part of “TomJ@hotmail.com.” No wildcard or regular-expression syntax is needed for these results: each item contains the entered character sequence directly. This behavior is important during forensic review because a basic keyword can identify occurrences embedded within longer words, file content, and textual artifacts such as email addresses; investigators should add word-boundary or other criteria only when they need to narrow the result set. EnCase is a forensic platform designed to search and analyze collected evidence, including text-based artifacts. See OpenText’s EnCase Forensic product information and its product documentation and support portal for the applicable EnCase documentation.

QUESTION NO: 18

Which of the following items could contain digital evidence?

A. Cellular phones

B. Digital cameras

C. Personal assistant devices

D. Credit card readers

ANSWER: A B C D

Explanation:

Cellular phones, digital cameras, personal assistant devices, and credit card readers can all be sources of digital evidence because each is capable of processing, storing, transmitting, or recording electronically represented information. A cellular phone may hold call records, messages, contacts, application data, location information, photographs, and cloud-account artifacts. Digital cameras can preserve image and video files along with metadata such as creation times, camera settings, and, where enabled, location details. Personal assistant devices—including PDAs and similar handheld devices—may contain calendars, notes, emails, contacts, synchronized files, and communications records. Credit card readers and related point-of-sale hardware may retain transaction records, timestamps, device configuration, identifiers, logs, and data relevant to payment activity or device use. The forensic principle is not limited to traditional computers: any electronic device that can retain relevant information may need to be identified, preserved, and examined using appropriate forensic procedures. NIST’s mobile-device forensic guidance specifically recognizes handheld devices and their associated data as important evidence sources, while its general forensic guidance describes collecting and examining digital evidence from diverse information systems and media. See NIST SP 800-101 Rev. 1 and NIST SP 800-86.