PassQueen
a.k.a dumpsqueen.com

AccessData Certified Examiner

AccessData A30-327

Version Demo

Total Demo Questions: 9

Total Premium Questions: 90

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which statement is true about using FTK Imager to export a folder and its subfolders?

A. Exporting a folder will copy all its subfolders.

B. Each subfolder must be exported individually.

C. Exporting a folder copies only the folder without any files.

D. Exporting a folder will copy all subfolders without the system attribute.

ANSWER: A

Explanation:

Exporting a folder will copy all its subfolders. FTK Imager's folder-export capability preserves the directory hierarchy beneath the folder selected for export. Consequently, the exported output includes the selected directory's nested folders and the files contained within that tree, rather than requiring an examiner to repeat the operation for each child folder. This is important in forensic workflow because a folder's evidentiary context frequently depends on its relative location and organization; retaining the hierarchy makes the exported material easier to review and correlate with the source evidence. The examiner should still choose and document an appropriate destination, verify the resulting export, and maintain the original evidence in a protected state. FTK Imager is designed for previewing and acquiring/exporting evidence while supporting forensic handling practices, and its export functions are intended to facilitate collection of selected filesystem content as a coherent set. See the FTK Imager product information from Exterro and the digital-evidence handling guidance published by the National Institute of Justice.

QUESTION NO: 2

After creating a case, the Encrypted Files container lists EFS files. However, no decrypted

sub- items are present. All other necessary components for EFS decryption are present in the case. Which two files must be used to recover the EFS password for use in FTK?

(Choose two.)

A. SAM

B. system

C. SECURITY

D. Master Key

E. FEK Certificate

ANSWER: A B

Explanation:

SAM and **system** must be supplied together to recover a Windows user password for subsequent EFS processing in FTK. The SAM registry hive contains local-account credential material, including the account password hashes used by Windows. Those hashes are not independently usable for this purpose: Windows protects them using cryptographic keying information derived from the SYSTEM hive, commonly described as the system boot key. FTK can use the paired hives to obtain or validate the applicable user password, which in turn enables access to the user's DPAPI-protected EFS key material already present in the case. Once that password-based protection is unlocked, FTK can use the available EFS components to decrypt files and populate the decrypted content beneath the Encrypted Files container. This dependency reflects the Windows credential and DPAPI design: encrypted user key material is protected in relation to the user's credentials, while system-level secrets are protected through information stored in the SYSTEM hive. Microsoft's overview of EFS is available

at EFS overview, and its DPAPI documentation provides background on Windows data-protection key handling at Data Protection API.

QUESTION NO: 3

You examine evidence and flag several graphic images found in different folders. You now want to bookmark these items into a single bookmark. Which tab in FTK do you use to view only the flagged thumbnails?

A. Explore tab

B. Graphics tab

C. Overview tab

D. Bookmark tab

ANSWER: C

Explanation:

The **Overview tab** is the appropriate place to narrow the evidence display to flagged graphics. FTK's Overview workflow provides summary and category-based views of the current case evidence, including graphics-related groupings. Selecting the flagged-graphics view limits the displayed results to image files that have already been marked with a flag, regardless of the folders in which those files reside. This avoids having to revisit each source folder individually and gives the examiner a consolidated thumbnail set for review. From that filtered set, the examiner can select the relevant images and apply one bookmark to the selected items, preserving a consistent review classification and making the material easier to locate later in the case. This use of evidence-status filtering is consistent with FTK's purpose of organizing and reviewing large evidence collections efficiently. Exterro describes FTK as a forensic examination platform for processing, reviewing, and managing digital evidence; see the FTK product page. For version-specific interface behavior and workflow details, examiners should consult the applicable FTK documentation through Exterro Support.

QUESTION NO: 4

What happens when a duplicate hash value is imported into a KFF database?

A. It will not be accepted.

B. It will be marked as a duplicate.

C. The database will be corrupted.

D. The database will hide the duplicate.

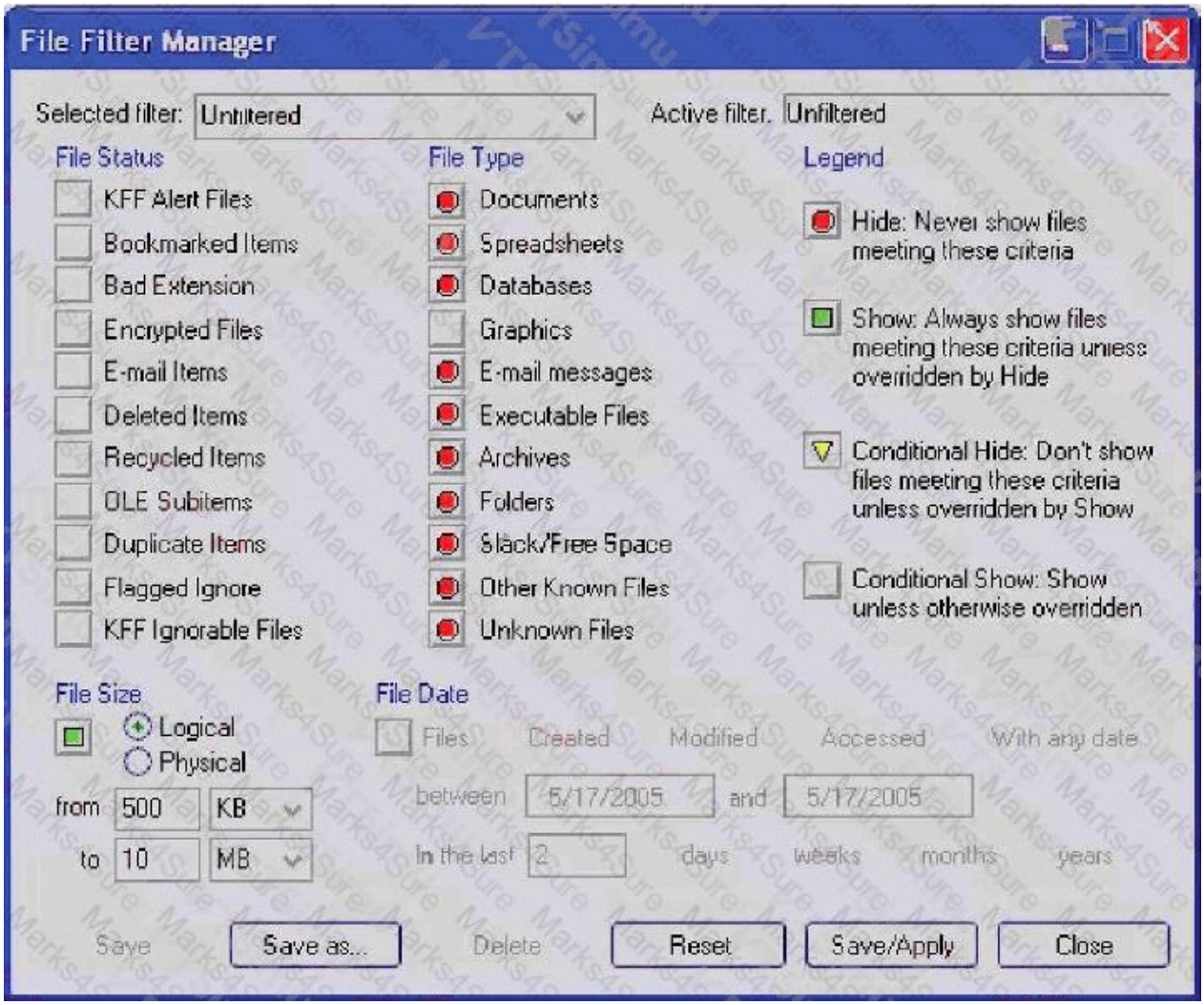
ANSWER: A

Explanation:

It will not be accepted. A Known File Filter (KFF) database is designed to use a file hash as its unique lookup key. During import, FTK checks the incoming hash against the hashes already stored in the selected KFF database. If the same hash is already present, there is no distinct known-file record to add, so FTK rejects the duplicate entry rather than creating a second record for the identical hash. This preserves the database's unique hash index and ensures that known-file filtering produces consistent results during evidence processing. In practice, an examiner should maintain clear source records and use a single authoritative entry for each hash, since the KFF database is intended to identify files by their cryptographic hash values. This behavior is especially important when combining lists from multiple sources, such as organizational known-good lists and reference hash sets. The National Software Reference Library describes the use of reference hashes to identify known software files, which aligns with the unique-hash purpose of a KFF database. See the NIST National Software Reference Library and Exterro's FTK Forensic Toolkit overview.

QUESTION NO: 5

Click the Exhibit button.



What change do you make to the file filter shown in the exhibit in order to show only graphics with a logical size between 500 kilobytes and 10 megabytes?

A. You change all file status items to a red circle.

B. You change all file status items to a yellow triangle.

C. You make no change. The filter is correct as shown.

D. You change Graphics in the File Type column to a yellow triangle.

ANSWER: D

Explanation:

You change Graphics in the File Type column to a yellow triangle. The logical-size criterion already limits the displayed items to files from 500 KB through 10 MB. The remaining requirement is to constrain the file-type portion of the filter to graphics. In the FTK filter display, changing the Graphics file-type entry to the yellow-triangle state applies the required selection state for that category while preserving the existing logical-size range. Consequently, the combined filter returns items that meet both conditions: they are identified as graphics and their logical size falls within the specified interval. This illustrates FTK's use of multiple filter columns as combined criteria: a file must satisfy the relevant configured conditions rather than merely match one independently. File-type classification is particularly useful in examination workflows because it allows an examiner to focus review on a content category while retaining a targeted size range. Exterro's FTK product information describes FTK as a forensic-analysis platform supporting investigation and evidence review workflows: Exterro FTK. Additional product and documentation resources are available from Exterro FTK product downloads.

QUESTION NO: 6

In FTK, when you view the Total File Items container (rather than the Actual Files container), why are there more items than files?

A. Total File Items includes files that are in archive files, while Actual Files does not.

B. Total File Items includes all unfiltered files while Actual Files includes only checked files.

C. Total File Items includes all KFF Ignorables while Actual Files includes only the KFFAlerts.

D. Total File Items includes files that are in the Graphics and E-Mail tabs, while Actual Filesonly includes files in the Graphics tab while excluding attachments in the E-mail tab.

ANSWER: A

Explanation:

Total File Items includes files that are in archive files, while Actual Files does not. FTK processes supported archives and compound containers by enumerating their contents as individual file items. Those embedded entries are searchable, can be examined, and may have metadata or hash status just like other processed items. They contribute to the Total File Items count because that container represents the complete set of file items generated during evidence processing, including items discovered within parent archive files.

The Actual Files container instead represents the files that exist as direct, top-level file-system items in the evidence source. An archive itself is an actual file, but the documents, images, or other entries stored inside it are child items created when FTK expands the archive for analysis. Consequently, a case containing ZIP, RAR, CAB, Office compound files, or similar supported containers can show a Total File Items count that exceeds the Actual Files count. This distinction is important when reconciling item counts and when ensuring that searches and review scope include embedded content, not merely direct file-system entries. See Exterro's FTK product information and the FTK support documentation portal for FTK processing and review documentation.

QUESTION NO: 7

Which three items are contained in an Image Summary File using FTK Imager? (Choose

three.)

A. MD5

B. CRC

C. SHA1

D. Sector Count

E. Cluster Count

ANSWER: A C D

Explanation:

FTK Imager's Image Summary File records both verification information and key acquisition metadata. **MD5** is included as a cryptographic hash value used to document the acquired image's integrity. The summary records the hash calculated for the source evidence and the hash calculated for the created image, allowing an examiner to demonstrate that the acquired data remained consistent through the imaging process. **SHA1** is likewise included as an additional cryptographic hash value, providing a second independently calculated integrity identifier for the evidence image. Using documented hash values is fundamental to repeatable forensic verification and chain-of-custody reporting.

Sector Count is also contained in the summary because it identifies the number of sectors represented by the source or acquired data. This acquisition-size metadata helps an examiner document the scope of the image and confirm that the imaging operation covered the expected amount of media. Together, MD5, SHA1, and Sector Count provide the essential

integrity and size details an examiner needs when reviewing or validating an FTK Imager acquisition. FTK Imager is designed to create forensic images and provide associated evidence details; see Exterro FTK Imager and the NIST hash-functions project.

QUESTION NO: 8

When exporting selected evidence files from FTK Imager, which two practices help preserve the forensic context of the export? (Choose two.)

A. Document the source path of each exported item.

B. Calculate and record hash values for the exported files.

C. Rename the exported files to remove their original filenames.

D. Delete the source evidence after confirming the export.

ANSWER: A B

Explanation:

Document the source path of each exported item and **calculate and record hash values for the exported files** are correct. The original source path establishes where an item was located within the evidence source and can be necessary to understand its relationship to surrounding files and folders. Hash values provide a repeatable way to identify the exported derivative and to determine whether it has changed after export.

Exports are derivative working copies and should be clearly distinguished from original evidence. The examiner should also document the destination, date and time, export method, and any processing applied. General digital-evidence handling guidance is available from the National Institute of Justice.

QUESTION NO: 9

Which data in the Registry can the Registry Viewer translate for the user? (Choose three.)

A. calculate MD5 hashes of individual keys

B. translate the MRUs in chronological order

C. present data stored in null terminated keys

D. present the date and time of each typed URL

E. View Protected Storage System Provider (PSSP) data

ANSWER: B C E

Explanation:

Registry Viewer's translation capability is intended to make several registry artifacts immediately readable and useful during forensic review, rather than requiring the examiner to manually decode their native storage format. It can translate most-recently-used (MRU) information into chronological order, allowing activity represented by MRU entries to be reviewed in a meaningful sequence. It can also present data held in null-terminated keys, interpreting the terminated string format so that the stored content is displayed cleanly to the examiner. In addition, Registry Viewer can view Protected Storage System Provider (PSSP) data. PSSP was used by older Windows components and applications to hold protected user information; being able to expose this artifact in the viewer supports analysis of legacy Windows evidence. These translations are presentation and interpretation features performed on registry evidence, helping investigators recognize relevant user-activity and protected-storage artifacts without manually parsing each value's raw representation. Microsoft documents the registry's structured storage of values and data types at Windows Registry, and provides background on Protected Storage through its legacy platform documentation at Protected Storage.