



A30-327^{Q&As}

AccessData Certified Examiner

Pass AccessData A30-327 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/a30-327.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by AccessData Official Exam Center

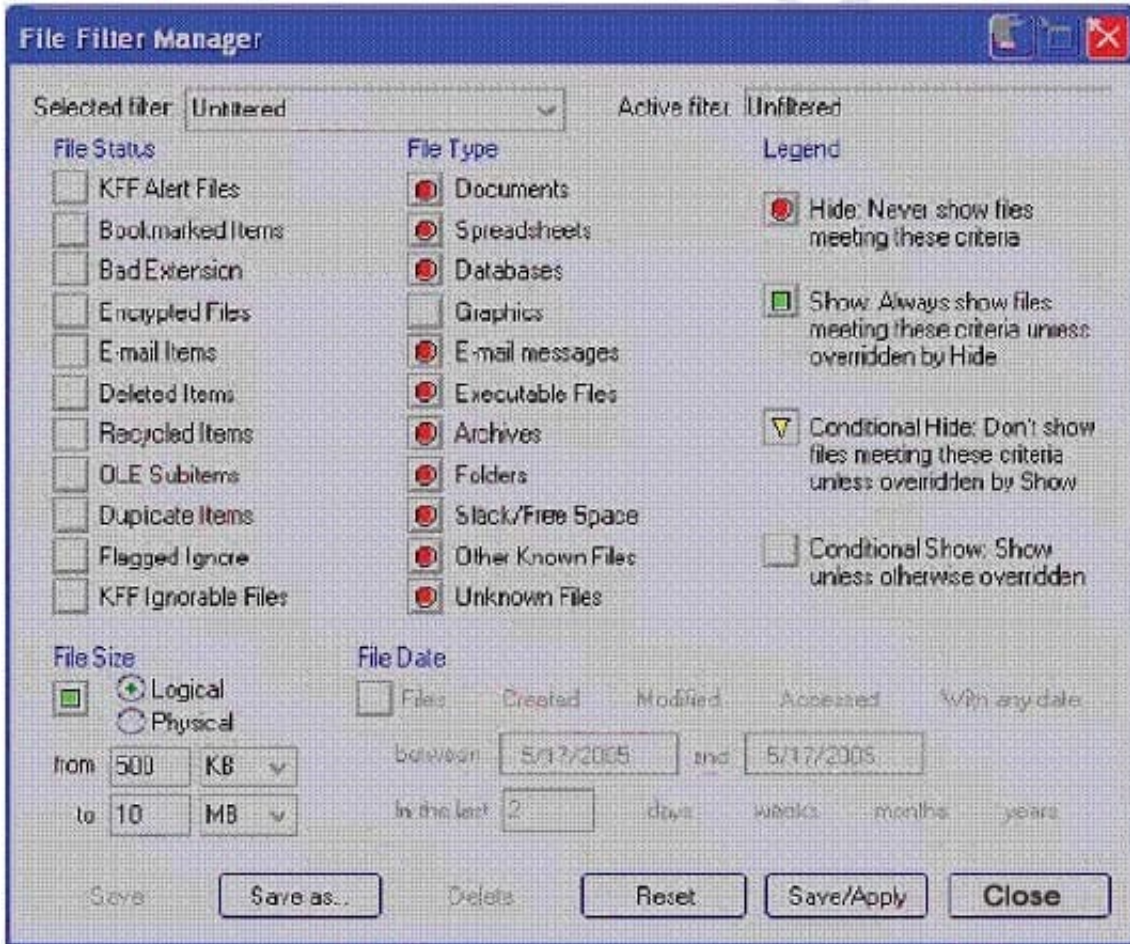
-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

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.

Correct Answer: D

QUESTION 2

What are three image file formats that can be read by FTK Imager? (Choose three.)



- A. E01 files
- B. raw (dd) image files
- C. SafeBack version 2.2 image files
- D. SafeBack version 3.0 image files
- E. Symantec Ghost compressed image files

Correct Answer: ABC

QUESTION 3

You currently store alternate hash libraries on a remote server.

Where do you configure FTK to access these files rather than the default library, ADKFFLibrary.hdb?

- A. Preferences
- B. User Options
- C. Analysis Tools
- D. Import KFF Hashes

Correct Answer: A

QUESTION 4

You are asked to process a case using FTK and to produce a report that only includes selected graphics. What allows you to display only flagged graphics?

- A. List by File Path
- B. List File Properties
- C. Graphic Thumbnails
- D. Supplementary Files

Correct Answer: C

QUESTION 5



When adding data to FTK, which statement about DriveFreeSpace is true?

- A. DriveFreeSpace is merged with deleted files.
- B. DriveFreeSpace is segmented into 10 megabyte items.
- C. DriveFreeSpace is truncated, based on the size of the case.dat file.
- D. DriveFreeSpace is classified with file slack items in the Overview tab.

Correct Answer: D

QUESTION 6

In FTK, which search broadening option allows you to find grammatical variations of the word "kill" such as "killer," "killed," and "killing"?

- A. Phonic
- B. Synonym
- C. Stemming
- D. Fuzzy Logic

Correct Answer: C

QUESTION 7

Which statement is true about Processes to Perform in FTK?

- A. Processing options can be chosen only when adding evidence.
- B. Processing options can be chosen during or after adding evidence.
- C. Processing options can be chosen only after evidence has been added.
- D. If processing is not performed while adding evidence, the case must be started again.

Correct Answer: B

QUESTION 8

You want to search for two words within five words of each other.



Which search request would accomplish this function?

- A. apple by pear w/5
- B. June near July w/5
- C. supernova w/5cassiopeia
- D. supernova bycassiopeia w/5

Correct Answer: C

QUESTION 9

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

Correct Answer: A

QUESTION 10

Using the FTK Report Wizard, which two options are available in the List by File Path window? (Choose two.)

- A. List File Properties
- B. Export to the Report
- C. Apply a Filter to the List
- D. Include Registry Viewer Reports

Correct Answer: BC
