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.passapply.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

Using the FTK Report Wizard, which two options are available in the Bookmarks - A window? (Choose two.)

A. Apply a filter to the list

B. Group all filenames at end of report

C. Yes, include all graphics in the case

D. No, do not include a bookmark section

E. Export full-size graphics and link them to the thumbnails

Correct Answer: DE

QUESTION 2

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

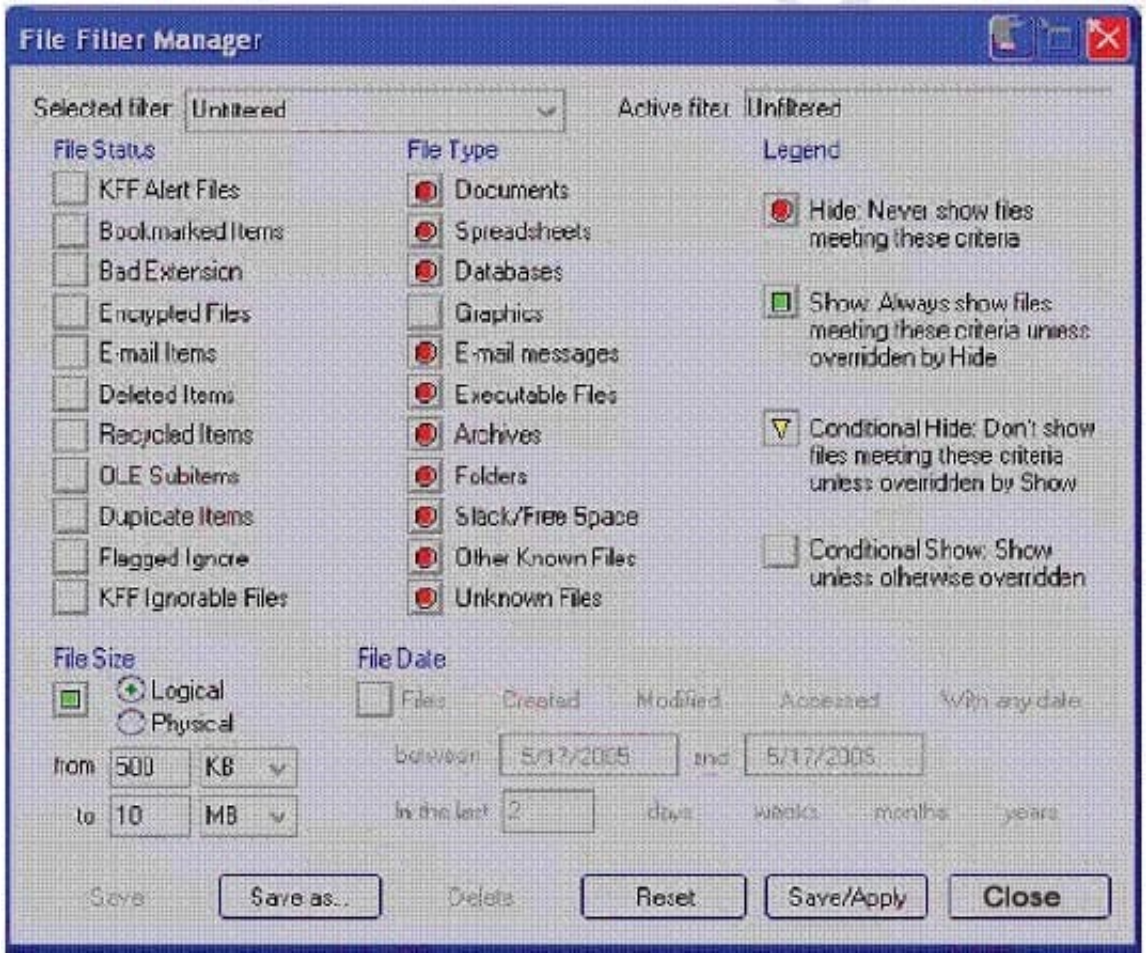
C. Analysis Tools

D. Import KFF Hashes

Correct Answer: A

QUESTION 3

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 4

Which Registry Viewer function would allow you to automatically document multiple unknown user names?

A. Add to Report

B. Export User List

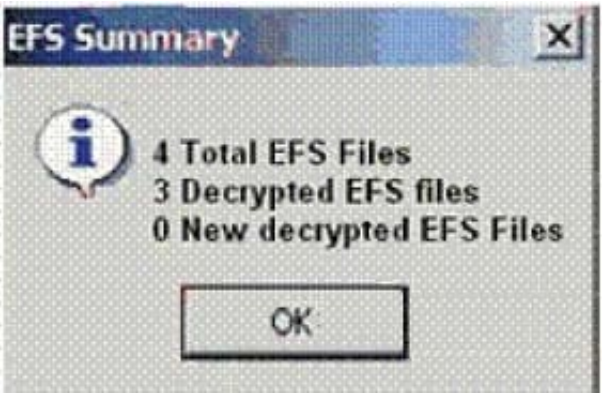
C. Add to Report with Children

D. Summary Report with Wildcard

Correct Answer: D

QUESTION 5

Click the Exhibit button.



When decrypting EFS files in a case, you receive the result shown in the exhibit.

What is the most plausible explanation for this result?

A. The encrypted file was corrupt.

B. A different user encrypted the remaining encrypted file.

C. The hash value of the remaining encrypted file did not match.

D. The remaining encrypted file had previously been bookmarked.

E. An incorrect CRC value for the $EFS certificate was applied by the user.

Correct Answer: B

QUESTION 6

You have processed a case in FTK using all the default options. The investigator supplies you with a list of 400 names in an electronic format. What is the quickest way to search unallocated space for all of these names?

A. build adtSearch string with all 400 names

B. create a Regular Expression with all the names

C. make an imported text file of the names in Live Search

D. use an imported text file containing the names in Indexed Search

Correct Answer: D

QUESTION 7

Which three items are displayed in FTK Imager for an individual file in the Properties window? (Choose three.)

A. flags

B. filename

C. hash set

D. timestamps

E. item number

Correct Answer: ABD

QUESTION 8

In PRTK, which type of attack uses word lists?

A. dictionary attack

B. key space attack

C. brute-force attack

D. rainbow table attack

Correct Answer: A

QUESTION 9

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 10

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