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.pass2lead.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

You currently store alternate hash libraries on a remote server.
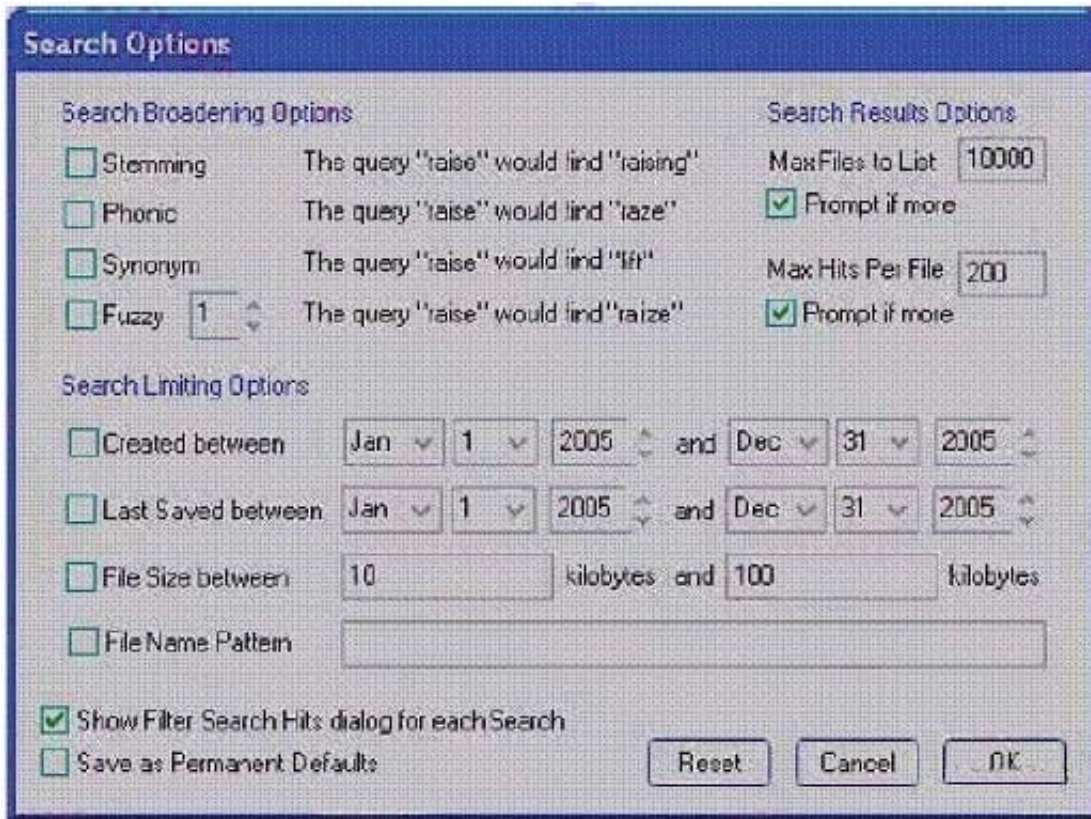
Where do you configure FTK to access these files rather than the default library, ADKFFLibrary.hdb?

A. Preferences

B. User Options

C. Analysis Tools

D. Import KFF Hashes

Correct Answer: A

QUESTION 2

Click the Exhibit button.

You need to search for specific data that are located in a Microsoft Word document. You do not know the exact spelling of this datA. Using the Index Search Options as displayed in the exhibit, which changes do you make in the Broadening Options and Search Limiting Options containers?

A. check the Fuzzy box;check the File Name Pattern box; type *.doc in the pattern container

B. check the Stemming box; check the File Name Pattern box; type *.doc in the pattern container

C. check the Synonym box;check the File Name Pattern box; type *.doc in the pattern container

D. check the Stemming box; check the File Name Pattern box;type %.doc in the pattern container

Correct Answer: A

QUESTION 3

In Registry Viewer, which steps initiate the Hex Interpreter?

A. highlight the data and select the Hex Value Interpreter tab

B. highlight the data, right-click on the highlighted data and select the Show Hex Interpreter Window

C. select the Hex Value Interpreter tab, highlight the data, right-click on the data to initiate the Hex Interpreter

D. right-click on the data area and select the Show Hex Interpreter Window and highlight the data you want to interpret

Correct Answer: B

QUESTION 4

Which pattern does the following regular expression recover? (\d{4}[\-]){3}\d{4}

A. 000-000-0000

B. ddd-4-3-dddd-4-3

C. 000-00000-000-ABC

D. 0000-0000-0000-0000

Correct Answer: D

QUESTION 5

Which type of evidence can be added to FTK Imager?

A. individual files

B. all checked items

![Pass2Lead](https://Pass2Lead.com)
C. contents of a folder

D. all currently listed items

Correct Answer: C

QUESTION 6

Into which two categories can an imported hash set be assigned? (Choose two.)

A. alert

B. ignore

C. contraband

D. system files

Correct Answer: AB

QUESTION 7

Which two statements are true? (Choose two.)

A. PRTK can recover Windows logon passwords.

B. PRTK must run in conjunction with DNA workers to decrypt EFS files.

C. PRTK and FTK must be installed on the same machine to decrypt EFS files.

D. EFS files must be exported from a case and provided to PRTK for decryption.

Correct Answer: AC

QUESTION 8

In FTK, which tab provides specific information on the evidence items, file items, file status and file category?

A. E-mail tab

B. Explore tab

C. Overview tab

D. Graphics tab

Correct Answer: C

QUESTION 9

Which two image formats contain an embedded hash value for file verification? (Choose two.)

A. E01

B. S01

C. ISO

D. CUE

E. 001 (dd)

Correct Answer: AB

QUESTION 10

You create two evidence images from the suspect\\'s drive: suspect.E01 and suspect.001.

You want to be able to verify that the image hash values are the same for suspect.E01 and suspect.001 image files. Which file has the hash value for the Raw (dd) image?

A. suspect.001.txt

B. suspect.E01.txt

C. suspect.001.csv

D. suspect.E01.csv

Correct Answer: A

[A30-327 VCE Dumps](#)   [A30-327 Study Guide](#)   [A30-327 Braindumps](#)