A30-327Q&As

AccessData Certified Examiner

Pass AccessData A30-327 Exam with 100% Guarantee

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

https://www.leads4pass.com/a30-327.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

QUESTION 2

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

Correct Answer: BCE

QUESTION 3

You are converting one image file format to another using FTK Imager. Why are the hash values of the original image and the resulting new image the same?

A. because FTK Imager\\'s progress bar tracks the conversion

B. because FTK Imager verifies the amount of data converted

C. because FTK Imager compares the elapsed time of conversion

D. because FTK Imager hashes only the data during the conversion

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

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 6

Which file should be selected to open an existing case in FTK?

A. ftk.exe

B. case.ini

C. case.dat

D. isobuster.dll

Correct Answer: C

QUESTION 7

What are three types of evidence that can be added to a case in FTK? (Choose three.)

A. local drive

B. registry MRU list

C. contents of a folder

D. acquired image of a drive

E. compressed volume files (CVFs)

Correct Answer: ACD

QUESTION 8

When using FTK Imager to preview a physical drive, which number is assigned to the first logical volume of an extended partition?

A. 2

B. 3

C. 4

D. 5

Correct Answer: D

QUESTION 9

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.

Correct Answer: A

QUESTION 10

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