AccessData A30-327

A30-327 AccessData Certified Examiner

Practice Test

Version 1.0

QUESTION NO: 1

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

Answer: A,B,D

QUESTION NO: 2

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

Answer: C

QUESTION NO: 3

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

Answer: D

QUESTION NO: 4

When previewing a physical drive on a local machine with FTK Imager, which statement is true?

A. FTK Imager can block calls to interrupt 13h and prevent writes to suspect media.

B. FTK Imager can operate from a USB drive, thus preventing writes to suspect media.
C. FTK Imager can operate via a DOS boot disk, thus preventing writes to suspect media.
D. FTK Imager should always be used in conjunction with a hardware write protect device to prevent writes to suspect media.

Answer: D

QUESTION NO: 5

Which type of evidence can be added to FTK Imager?

A. individual files
B. all checked items
C. contents of a folder
D. all currently listed items

Answer: C

QUESTION NO: 6

To obtain protected files on a live machine with FTK Imager, which evidence item should be added?

A. image file
B. currently booted drive
C. server object settings
D. profile access control list

Answer: B

QUESTION NO: 7

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

Answer: A,B,C

QUESTION NO: 8

Which statement is true about using FTK Imager to simultaneously create multiple images of a single source?

A. In the Image Creation Wizard, you should select the Add Additional Drives option.
B. You should use the Create Multiple Images option to create server image objects.
C. You should note the evidence item source signature and add it to the Image View pane.
D. In the Image Creation Wizard, you should add multiple destination jobs from the same source prior To beginning image creation.

Answer: D

QUESTION NO: 9

FTK Imager allows a user to convert a Raw (dd) image into which two formats? (Choose two.)

A. E01
B. Ghost
C. SMART
D. SafeBack

Answer: A,C

QUESTION NO: 10

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

Answer: D

QUESTION NO: 11

How can you use FTK Imager to obtain registry files from a live system?