Vendor: AccessData

Exam Code: A30-327

Exam Name: AccessData Certified Examiner

Version: Demo

QUESTION: 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: 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: 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: 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: 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: 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: 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: 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: 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: 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: 11
How can you use FTK Imager to obtain registry files from a live system?

A. You use the Export Files option.
B. You use the Advanced Recovery option.
C. Registry files cannot be exported from a live system.
D. You use the Protected Storage System Provider option.

Answer: A

QUESTION: 12
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.

Answer: A

QUESTION: 13
You used FTK Imager to create several hash list files. You view the location where the files were exported. What is the file extension type for these files?

A. .txt = ASCII Text File
B. .dif = Data Interchange Format
C. .prn = Formatted Text Delimited
D. .csv = Comma Separated Values

Answer: D

QUESTION: 14
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

Answer: A

QUESTION: 15
You successfully export and create a file hash list while using FTK Imager. Which three pieces of information are included in this file? (Choose three.)

A. MD5
B. SHA1
C. filename
D. record date
E. date modified

Answer: A, B, C

QUESTION: 16
During the execution of a search warrant, you image a suspect drive using FTK Imager and store the Raw(dd) image files on a portable drive. Later, these files are transferred to a server for storage. How do you verify that the information stored on the server is unaltered?

A. open and view the Summary file
B. load the image into FTK and it automatically performs file verification
C. in FTK Imager, use the Verify Drive/Image function to automatically compare a calculated hash with a stored hash
D. use FTK Imager to create a verification hash and manually compare that value to the value stored in the Summary file

Answer: D

QUESTION: 17
Which three items are contained in an Image Summary File using FTK Imager? (Choose three.)

A. MD5
B. CRC
C. SHA1
D. Sector Count
E. Cluster Count

Answer: A, C, D

QUESTION: 18
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)

Answer: A, B

QUESTION: 19
While analyzing unallocated space, you locate what appears to be a 64-bit Windows date and time. Which FTK Imager feature allows you display the information as a date and time?

A. INFO2 Filter
B. Base Converter
C. Metadata Parser
D. Hex Value Interpreter

Answer: D

QUESTION: 20
In which Overview tab container are HTML files classified?

A. Archive container
B. Java Code container

C. Documents container
D. Internet Files container

Answer: C

QUESTION: 21
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.

Answer: D

QUESTION: 22
You are using FTK to process e-mail files. In which two areas can E-mail attachments be located? (Choose two.)

A. the E-mail tab
B. the From E-mail container in the Overview tab
C. the Evidence Items container in the Overview tab
D. the E-mail Messages container in the Overview tab

Answer: A, B

QUESTION: 23
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

Answer: C

QUESTION: 24
In FTK, you navigate to the Graphics tab at the Case level and you do not see any graphics. What should you do to see all graphics in the case?

A. list all descendants
B. run the graphic files filter
C. check all items in the current list
D. select the Graphics container button

Answer: A

QUESTION: 25
In FTK, which two formats can be used to export an E-mail message? (Choose two.)

A. raw format
B. XML format
C. PDF format
D. HTML format
E. binary format

Answer: A, D

QUESTION: 26
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.

Answer: A

Submit A Ticket