Exam Questions A30-327

AccessData Certified Examiner

https://www.2passeasy.com/dumps/A30-327/

NEW QUESTION 1
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: ABC

NEW QUESTION 2
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

NEW QUESTION 3
A. E01 files

A. raw (dd) image files
B. SafeBack version 2.2 image files
C. SafeBack version 3.0 image files
D. Symantec Ghost compressed image files

Answer: ABC

NEW QUESTION 4
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 calculatedhash with a stored hash
D. use FTK Imager to create a verification hash and manually compare that value to the valuestored in the Summary file

Answer: D

NEW QUESTION 5
A. highlight the data and select the Hex Value Interpreter tab

A. highlight the data, right-click on the highlighted data and select the Show Hex Interpreter Window
B. select the Hex Value Interpreter tab, highlight the data, right-click on the data to initiate theHex Interpreter
C. right-click on the data area and select the Show Hex Interpreter Window and highlight thedata you want to interpret

Answer: B

NEW QUESTION 6
When using PRTK to attack encrypted files exported from a case, which statement is true?

A. PRTK will request the user access control list from FTK.
B. PRTK will generate temporary copies of decrypted files for printing.
C. FTK will stop all active jobs to allow PRTK to decrypt the exported files.
D. File hash values will change when they are saved in their decrypted format.
E. Additional interoperability between PRTK and NTAccess becomes available when files begin decrypting.

Answer: D

NEW QUESTION 7
Which two Registry Viewer operations can be conducted from FTK? (Choose two.)

A. list SAM file account names in FTK
B. view all registry files from within FTK
C. create subitems of individual keys for FTK
D. export a registry report to the FTK case report

Answer: BD

NEW QUESTION 8

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: ABD

NEW 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: AC

NEW QUESTION 10
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 toprevent writes to suspect media.

Answer: D

NEW QUESTION 10
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 KFF Ignorables 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

NEW QUESTION 14
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

NEW QUESTION 17
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.

Answer: AC

NEW QUESTION 20
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

NEW QUESTION 23
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 chang
D. The filter is correct as shown.
E. You change Graphics in the File Type column to a yellow triangle.

Answer: D

NEW QUESTION 24
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

NEW QUESTION 25
In PRTK, which type of attack uses word lists?

A. dictionary attack
B. key space attack
C. brute-force attack
D. rainbow table attack

Answer: A

NEW QUESTION 30
FTK uses Data Carving to find which three file types? (Choose three.)

A. JPEG files
B. Yahoo! Chat Archives
C. WPD (Word Perfect Documents)
D. Enhanced Windows Meta Files (EMF)
E. OLE Archive Files (Office Documents)

Answer: A

Explanation:
What happens when a duplicate hash value is imported into a KFF database?
A. It will not be accepted.
B. It will be marked as a duplicate.
C. The database will be corrupted.
D. The database will hide the duplicate.

NEW QUESTION 32
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

NEW QUESTION 37
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

Answer: BCE

NEW QUESTION 40
You are asked to process a case using FTK and to produce a report that only includes selected graphics. What allows you to display only flagged graphics?

A. List by File Path
B. List File Properties
C. Graphic Thumbnails
D. Supplementary Files

Answer: C

NEW QUESTION 45
What are two functions of the Summary Report in Registry Viewer? (Choose two.)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 50
When adding data to FTK, which statement about DriveFreeSpace is true?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 52
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

NEW QUESTION 53
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

NEW QUESTION 54
FTK Imager can be invoked from within which program?

A. FTK
B. DNA
C. PRTK
D. Registry Viewer

Answer: A

NEW QUESTION 59
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: ACD

NEW QUESTION 61
Which file should be selected to open an existing case in FTK?

A. ftk.exe
B. case.ini
C. case.dat
D. isobuster.dll

Answer: C

NEW QUESTION 63
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: AD

NEW QUESTION 67

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual A30-327 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the A30-327 Product From:

https://www.2passeasy.com/dumps/A30-327/

Money Back Guarantee

A30-327 Practice Exam Features:

* A30-327 Questions and Answers Updated Frequently

* A30-327 Practice Questions Verified by Expert Senior Certified Staff

* A30-327 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* A30-327 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year