

ACE STUDY GUIDE QUESTIONS



1. To obtain protected files on a live machine with FTK Imager, which evidence item should be added?
 - a) server object settings
 - b) currently booted volume
 - c) image file
 - d) profile access control list

2. When converting one evidence file format to another using FTK Imager, the hash values of the original image and the resulting new image are the same. Why is this?
 - a) because FTK Imager verifies the amount of data converted
 - b) because FTK Imager compares the elapsed time of conversion
 - c) because FTK Imager's progress bar tracks the conversion
 - d) because FTK Imager hashes only the data during the conversion

3. After successfully exporting and creating a file hash list using FTK Imager, which piece of information is NOT included in this file?
 - a) MD5
 - b) filename
 - c) date modified
 - d) SHA1

4. Which item in the Properties window is NOT displayed in FTK Imager for an individual file?
 - a) Item number
 - b) filename
 - c) flags
 - d) timestamp

5. What type of evidence can be added to FTK Imager?
 - a) contents of a folder
 - b) individual files
 - c) all currently listed items
 - d) all checked items

6. While analyzing unallocated space, a 64-bit Windows date and time stamp is located. Which FTK Imager feature allows you display the information as a date and time?
 - a) INFO2 filter
 - b) Base Converter
 - c) Hex Value Interpreter
 - d) Metadata Parser

7. Which two evidence file formats contain an embedded hash value for file verification?
 - a) 001 (dd)
 - b) CUE
 - c) ISO
 - d) S01
 - e) E01

8. Which statement is true about using FTK Imager to simultaneously create multiple images of a single source?
 - a) In the Image Creation Wizard, add multiple destination jobs from the same source prior to beginning image creation
 - b) In the Image Creation Wizard, select the Add Additional Drives option
 - c) Use the Create Multiple Images option to create server image objects
 - d) Multiple images can't be simultaneously created from a single source

9. Which evidence file format CAN NOT be mounted by FTK Imager?
 - a) raw (dd) image files
 - b) SafeBack version 2 image files
 - c) Norton™ Ghost compressed image files
 - d) E01 files

10. After creating two evidence images from the suspect's drive: suspect.E01 and suspect.001, a user wants 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.001.csv
 - c) suspect.E01.csv
 - d) suspect.E01.txt

11. Which statement is true about using FTK Imager to export a folder and its subfolders?
 - a) Exporting a folder copies only the folder without any files
 - b) Each subfolder must be exported individually
 - c) Exporting a folder will copy all subfolders without the system attribute
 - d) Exporting a folder will copy all its subfolders

12. When using FTK Imager to preview a hard drive attached to a local machine, which statement is true?
 - a) FTK Imager can operate from a USB drive, thus preventing writes to suspect media
 - b) FTK Imager should always be used in conjunction with a hardware write protect device to prevent writes to suspect media
 - c) FTK Imager can block calls to interrupt 13h and prevent writes to suspect media
 - d) FTK Imager can operate via a DOS boot disk, thus preventing writes to suspect media

13. When using FTK Imager to preview a physical drive, which number is assigned to the first logical volume of an extended partition?
 - a) 4
 - b) 3
 - c) 2
 - d) 5

14. Which item is NOT contained in an Image Summary File using FTK Imager?
 - a) Cluster Count
 - b) SHA1
 - c) MD5
 - d) Sector Count

15. FTK Imager was used to create several hash list files. 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

16. When using Registry Viewer to view a key with 20 values, what option can be used to display only 5 of the 20 values in a report?
 - a) Report
 - b) Add to Report With Children
 - c) Summary Report
 - d) Special Reports

17. Which data in the Registry can the Registry Viewer translate for the user?
 - a) present the date and time for each typed URL
 - b) calculate the MD5 hashes of individual keys
 - c) view the Protected Storage System Provider area for IE6
 - d) present data stored in deleted keys

18. Which Registry Viewer function would allow you to automatically document multiple unknown user names?
 - a) Summary Report with WildCard
 - b) Add to Report with Children
 - c) Export User List
 - d) Add to Report

19. Which of the following is a function of the Summary Report in Registry Viewer?
 - a) permits searching of registry values based on key headers
 - b) creates a template for future registry files
 - c) displays investigator keyword search results
 - d) lists all keys with a specified modified time

20. Registry Viewer can search for which of the following?
 - a) All deleted keys within the specified registry file
 - b) All occurrences of a search term in a registry file
 - c) Keys with values stored in Big Endian format
 - d) Keys containing encrypted data

21. What is the purpose of the PRTK Golden Dictionary?
- maintains previously created level information
 - maintains a list of the 100 most likely passwords
 - maintains previously recovered passwords
 - maintains previously created profile information
22. When using PRTK to attack encrypted files exported from a case, which statement is true?
- Additional interoperability between PRTK and NTAccess becomes available when files begin decrypting
 - FTK will stop all active jobs to allow PRTK to decrypt the exported files
 - PRTK will generate temporary copies of decrypted files for printing
 - PRTK will request the user access control list from FTK
 - File hash values will change when they are saved in their decrypted format
23. In PRTK, which type of attack uses word lists?
- hash table attack
 - keyspace attack
 - brute-force attack
 - dictionary attack
24. What is the most effective method to facilitate successful password recovery?
- Advanced EFS Attack
 - Primary Dictionary Attack
 - Entropy Test
 - AccessData Methodology (Art of War)
25. How is IE6 Protected Storage System Provider (PSSP) data accessed using PRTK?
- You drop the SAM file onto the PRTK interface
 - You drop the NTUSER.dat file onto the PRTK interface
 - You use the PSSP Attack Marshall from Registry Viewer
 - This area can not be accessed with PRTK as it is a registry file
26. Which statement is true?
- PRTK and FTK must be installed on the same machine to decrypt EFS files
 - PRTK must run in conjunction with DNA workers to decrypt EFS files
 - PRTK can recover Windows logon passwords
 - EFS files must be exported from a case and provided to PRTK for decryption
27. What type of information is provided via the Help > Recovery Modules menu option in PRTK?
- Estimated Recovery Time
 - Attack Types
 - Difficulty Level
 - Bit Strength
28. Which statement is true concerning the Biographical Dictionary in PRTK?
- It helps to create an overall picture of the computer user
 - Data can be input in any category without affecting effectiveness
 - The resulting dictionary creates permutations of input terms
 - The Biographical Dictionary contains locally recovered passwords

29. Which of the following is NOT listed as a Pre-Processing Option in FTK?
- a) SHA1 Hash
 - b) Concatenate DriveFreeSpace
 - c) Data Carving
 - d) Entropy Test
30. The FTK Data Carving option can restrict files to be carved by which of the following?
- a) Minimum File Size (bytes/KB)
 - b) Maximum File Size (bytes/KB)
 - c) Maximum Height (pixels)
 - d) MD5 Hash Value
31. Which of the following is NOT an option available in the FTK Report?
- a) Include PRTK Output List
 - b) File Paths
 - c) File Properties
 - d) Create an HTML version of the report
32. Which tab in FTK would show how many Microsoft Word 2000 documents were in a case?
- a) Graphics Tab
 - b) Explore Tab
 - c) Overview Tab
 - d) Documents Tab
33. Which of the following is not one of the containers/nodes on the Overview Tab of FTK?
- a) (Total) File Items
 - b) Bad Extension
 - c) Archives
 - d) Databases
 - e) MFT record number
34. When adding data to FTK, which statement about unallocated space is true?
- a) Unallocated space is truncated, based on the size of the case.dat file
 - b) Unallocated space is segmented into 10 megabyte items
 - c) Unallocated space is classified with the file slack items in the Overview tab
 - d) Unallocated space is merged with deleted files
35. Which statement is true about Evidence Processing in FTK?
- a) If processing is not performed while adding evidence, the case must be started again
 - b) Processing options can be chosen only after evidence has been added
 - c) Processing options can be chosen during or after adding evidence
 - d) Processing options can be chosen only when adding evidence
36. In which FTK Overview tab container/node are HTML files classified?
- a) Documents container
 - b) Archive container
 - c) Java Code container
 - d) Internet Files container

37. Which statement is true concerning Column Settings in FTK?
- Custom Column Settings can be used in the Report function
 - Column Settings must be specified during pre-processing
 - Column settings are selected during FTK installation
 - Column Settings can not be changed
38. Which of the following is NOT a section in an FTK report?
- Bookmarks
 - Thumbnails
 - Case Information
 - File Paths
39. Which pattern does the following regular expression recover? $(\d{4}[\-]){3}\d{4}$
- ddd-4-3-dddd-4-3
 - 000-00000-000-ABC
 - 0000-0000-0000-0000
 - 000-000-000
40. Which statement is true concerning bookmarks in an FTK report?
- All bookmarks in the case can be included in a report
 - FTK will only allow bookmarks containing graphics to be included a report
 - Bookmarks can be included in a report must be chosen before the report function is started
 - Filters can not be applied to bookmarks in a report
41. What type of evidence CAN NOT be added to a case in FTK?
- logical drive
 - contents of a folder
 - compressed volume files (CVFs)
 - acquired image of drive
42. After processing a case in FTK using all of the default options, a list of 400 names is supplied in electronic format. What is the quickest way to search unallocated space for all of these names?
- use an imported text file containing the names in Live Search
 - use an imported text file containing the names in Indexed Search
 - create a Regular Expression with all of the names
 - build a dtSearch string with all 400 names
43. After creating a case in FTK, the Encrypted Files container/node lists EFS files. No decrypted sub-items are present. All other necessary components for EFS decryption are present in the case. Which file must be used to recover the EFS password for use in FTK?
- SECURITY
 - Master Key
 - FEK Certificate
 - SAM

44. Which Registry Viewer operation can be conducted from FTK?
- a) create subitems of individual keys for FTK
 - b) view all registry files from within FTK
 - c) decrypt passwords from the SAM file
 - d) display all encrypted registry content
45. FTK Imager can be invoked from within which program?
- a) DNA
 - b) PRTK
 - c) Registry Viewer
 - d) FTK
46. What is the advantage of including registry files in the Export Word List function of FTK?
- a) The content of the registry files would not otherwise be included in the wordlist
 - b) Inclusion of registry files may include decrypted null-terminated values
 - c) Inclusion of registry files may include decrypted Protected Storage values
 - d) Inclusion of registry files may include decrypted SAM account passwords
47. In which file format can a list of hash values be imported into FTK?
- a) CSV
 - b) ISO
 - c) AD1
 - d) DD
48. FTK Imager allows a user to convert a raw (dd) image into which format?
- a) SMART
 - b) Norton Ghost™
 - c) Safeback
 - d) LO1
49. In FTK, into which two categories can an imported hash set be assigned?
- a) ignore
 - b) contraband
 - c) alert
 - d) system files
50. 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) Fuzzy Logic
 - c) Synonym
 - d) Stemming
51. FTK uses Data Carving to find which three file types?
- a) WPD (Word Perfect Documents)
 - b) Yahoo!® Chat Archives
 - c) Enhanced Windows Meta Files (EMF)
 - d) JPEG Files
 - e) OLE Archive Files (Office Documents)

52. In FTK, which tab provides specific information on file items, file status and file category?
- a) Overview Tab
 - b) Explore Tab
 - c) Graphics Tab
 - d) Email Tab
53. In FTK, you want to search for the words “apple” and “pear” within five words of each other. Which search request would accomplish this function?
- a) apple w/5 pear
 - b) apple by pear w/5
 - c) apple not w/5 pear
 - d) apple near pear w/5
54. In FTK, which two formats can be used to export an E-mail message?
- a) PDF format
 - b) raw format
 - c) HTML format
 - d) XML format
 - e) binary format
55. What type of file can be decrypted within FTK?
- a) EFS
 - b) BestCrypt ®
 - c) Zip archives
 - d) AES