ACE STUDY GUIDE

Note *All of the actual exam questions are in multiple choice format. This Study Guide is designed to cover all of the material on the exam,*

1. FTK Imager supports the encryption of forensic image files. What two methods may be used for encryption?
   - Password
   - Certificate (*.pfx, *.p12, *.pem)

2. When creating a File Hash List in Imager, what information is included in the resulting file?
   - MD5 hash
   - SHA1 hash
   - File Names (Including path)

3. Which Imager pane shows information specific to file systems such as HFS+, NTFS, and Ext2?
   - Properties Pane

4. FTK Imager allows what type of evidence to be added?
   - Physical Drive
   - Logical Drive
   - Image File
   - Contents of a folder

5. Name three features of the Image Mounting function in Imager and in FTK.
   - Navigate file systems in Windows Explorer (Ext2, HFS+, etc) normally not recognized.
   - Run antivirus software against mounted images
   - Make "virtual writes" to the mounted image using a cache file
   - Run third party software against the mounted image
   - Navigate the directory structure without making changes using the "Read-Only" mounting option.

6. What types of image file formats can be created by Imager?
   - RAW(DD) - *.001
   - SMART - *.S01
   - EnCase - *.E01
   - Advanced Forensic Format - *.AFF
   - AD Custom Content (Logical Image) - *.AD1

7. Name four characteristics of Custom Content Images.
   - File extension of *.AD1
   - Logical files only – no file slack
   - Can include recursive subdirectories
   - Can include unallocated space

8. Which AccessData forensic tools have Hex Value Interpreter functionality?

- FTK Imager
- FTK
- Registry Viewer

9. Name three functions of a Registry Viewer Summary Report
    - Can display specific values within a registry key
    - Wildcard function allows creation of registry templates
    - Multiple areas of a registry file can be documented.

10. Name two functions of a Registry Viewer Common Area?
    - Provides shortcuts or bookmarks for frequently accessed registry keys
    - Additional keys can be added by the user for customization

11. Name three fields shown for a Windows user's account in the Registry Viewer Properties pane when viewing the SAM file.
    - SID Unique Identifier
    - Last Logon Time
    - User Name
    - Logon Count
    - Last Password Change
    - Password Required

12. What types of searches can be performed in Registry Viewer?
    - Standard Search - next occurrence of a search term
    - Advanced Search - all occurrences of a search term
    - Search for key with a last written date:
        i. during a date range
        ii. during and after a given date
        iii. during and before a given date

13. How is the Golden Dictionary in PRTK created?
    - It is auto-generated from successfully recovered passwords on the local computer.

14. Name the four types of attacks listed in the PRTK Help > Recovery Modules menu?
    - Dictionary
    - Decryption
    - Keyspace
    - Reset

15. Name the four major sections of a PRTK Attack Profile.
    - Dictionaries
    - Rules (levels)
    - Languages
    - Character Groups

16. Which of the 5 registry files (SAM, SYSTEM, SECURITY, SOFTWARE, NTUSER.DAT) can be attacked by PRTK for possible encrypted information or passwords?

- SAM, SECURITY, NTUSER.DAT

17. What types of fields are available in the PRTK Biographical Dictionary?
    - Name, Address, City, State, Zip Code, Country, Phone Number, Date, Number, Word, Phrase.

18. What three types of "traditional" hashing can be done in FTK pre-processing?
    - MD5
    - SHA1
    - SHA256

19. How can an automatically carved item's location and parent be determined in FTK?
    - When clicking on the newly carved item, its parent will be listed in the path shown at the bottom of the screen. The parent name is to the left of the child name.
    - The carved item's location (offset/cursor position) within the parent is indicated by the number in the file name.

20. What are the major sections in the FTK report?
    - Case Information
    - Bookmarks
    - Graphics
    - Videos
    - File Paths
    - File Properties
    - Registry Selections
    - Screen Capture

21. Name three restrictions of a user assigned Case Reviewer status in FTK.
    - Cannot view Privileged Files
    - Cannot Add Evidence
    - Cannot perform Additional Analysis
    - Cannot Decrypt Files
    - Cannot create filters.

22. When can Data Carving be performed in FTK?
    - During Pre-processing
    - After case creation

23. What would be the advantage of performing Data Carving after case creation?
    - It can be performed on a smaller group of files (checked, Quick Picked) instead of on the entire case.

24. Which of the following files would NOT be found in the Internet/Chat files container in the FTK Overview Tab?
    a. Firefox places.sqlite

b. Internet Explorer Index.dat
c. **Skype main.db**
d. Yahoo *.DAT

25. The numerical string "123-422-17365" would be found by which Regular Expression?
    a. (\d{3}[\-]){2}\d{17365}
    b. **(\d{3}[\-]){2}\d{5}**
    c. (\d{3}[\-]){3}\d{5}
    d. (\d{3}[\-]){422}\d{5}

26. What are the advantages of importing a list of search terms into FTK's Indexed Search Tab?
    - Faster than manual entry
    - A list of commonly searched terms can be used in multiple cases.

27. List the steps needed for recovery of an EFS encrypted file in FTK.
    1. Identify the encrypted file (Overview > File Status > Encrypted Files)
    2. View the file in the Explore Tab tree; view the $EFS stream in File List
    3. Note the Windows user who in encrypted the file in $EFS stream
    4. Export the SAM and SYSTEM files for decryption in PRTK. (dictionary attack)
    5. After obtaining Windows password from SAM file, input the password into FTK
    6. View decrypted file as a subitem of encrypted file or File Status > Decrypted Files

28. When can the Expand Compound Files processing option be performed?
    - In pre-processing
    - After case creation - Evidence > Additional Analysis

29. What types of files benefit from the Expand Compound Files processing option?
    - Zip files, EVTX, Mail (PST, mbox, msg, NSF), MS Office OLE, Registry, SQLite)

30. What five types of customized settings can be shared among cases via the Manage menu in FTK?
    - KFF Hash Sets and Groups
    - Labels
    - Carvers
    - Filters
    - Columns

31. What are the two options for generating thumbnails of video files in FTK?
    - Percentage (Every "n" percent)
    - Interval (Every "n" seconds)

32. How is the Volatile tab in FTK populated?
    - Through the Manage > Add Remote Data menu
    - Through the Manage > Import Memory Dump

33. Name two ways the scope of an Indexed search in FTK can be limited?
    - Use filters
    - Use checked files

Updated Aug 2013

34. What is the advantage of opening registry files using Registry Viewer within a case in FTK?
    - A more detailed view is available than the FTK default view.
    - Reports generated in Registry Viewer can be linked to the FTK report.

35. Which applications can be launched from within FTK?
    - FTK Imager
    - Registry Viewer
    - PRTK
    - License Manager
    - Language Selector

36. Which registry files will display content in a HTML table in FTK using default processing?
    - SAM (User account info)
    - SOFTWARE (install info)
    - SYSTEM (time zone info)

37. What is the purpose of the Registry Reports processing option in FTK?
    - Auto-processes Registry Summary Reports
    - File Signature Analysis must be selected
    - Only RSR files in the designated directory are run.
    - Can be incorporated into FTK report.

38. What formats of hash sets can be imported into FTK?
    - AccessData Hash Database (*.HDB)
    - FTK Imager Hash List (*.CSV)
    - FTK Copy Special Hash List (tab-delimited)
    - HashKeeper Hash Set (*.HKE, HKT.TXT)
    - National Software Reference Library (NSRL)
    - Tab-delimited files (TSV)
    - Hash file (.hash)
    - FTK (KFF)

Additional Knowledge Points to be familiar with:

1. How to access EXIF information for a graphic file in FTK
2. Use the Filter Manager to apply multiple filters in FTK.
3. How to run a Regular Expression and examine the results.
4. Recognizing files which are email attachments.
5. Determining the actual File Type of a file with an incorrect file extension.
6. Capturing RAM – changes may occur to source (no write protection)

Updated Aug 2013

7. Visualization and Social Analyzer screen capture
8. PhotoDNA – general concept
9. Language ID – Options, multiple languages within document.
10. Decrypting Files within PRTK
11. Sending files directly to PRTK from FTK
12. RSR File pre-processing in FTK