

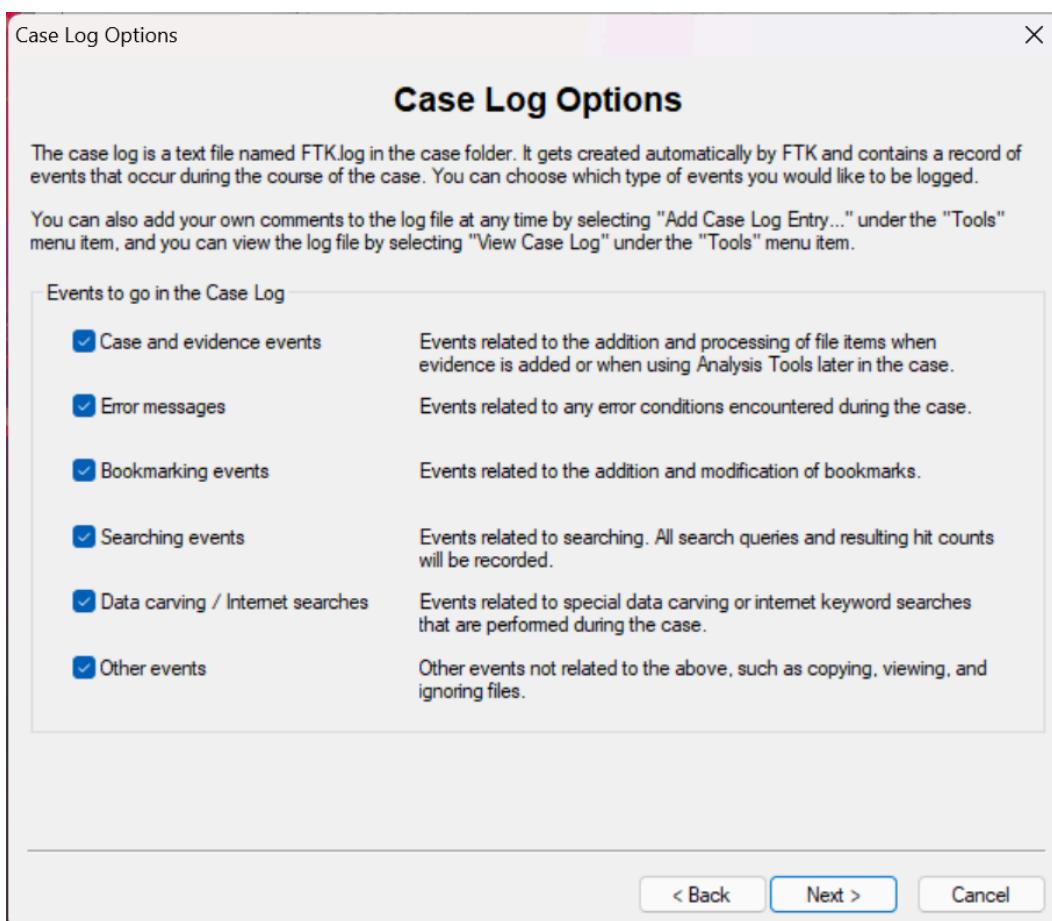
Computer & Network Forensics

Week 5 (Lab3)

Introduction to Forensics Analysis using FTK

Questions

1. Case Log Options



1. What is the format of the FTK.log file?

The FTK.log file is a text file created automatically by FTK in the case folder. It is stored in plain text (.log) format and can be opened and viewed with any text editor.

2. What is a log file used for?

A log file is used to record a detailed history of events and actions that occur during a forensic case. It provides an audit trail showing what was done, when, and by whom – useful for documentation, verification, and accountability.

3. What kind of events can be recorded in a log file?

- Case and evidence events (when evidence is added or processed)
- Error messages
- Bookmarking events
- Searching events (all search queries and hit counts)
- Data carving / Internet search events
- Other events (e.g., copying, viewing, or ignoring files)

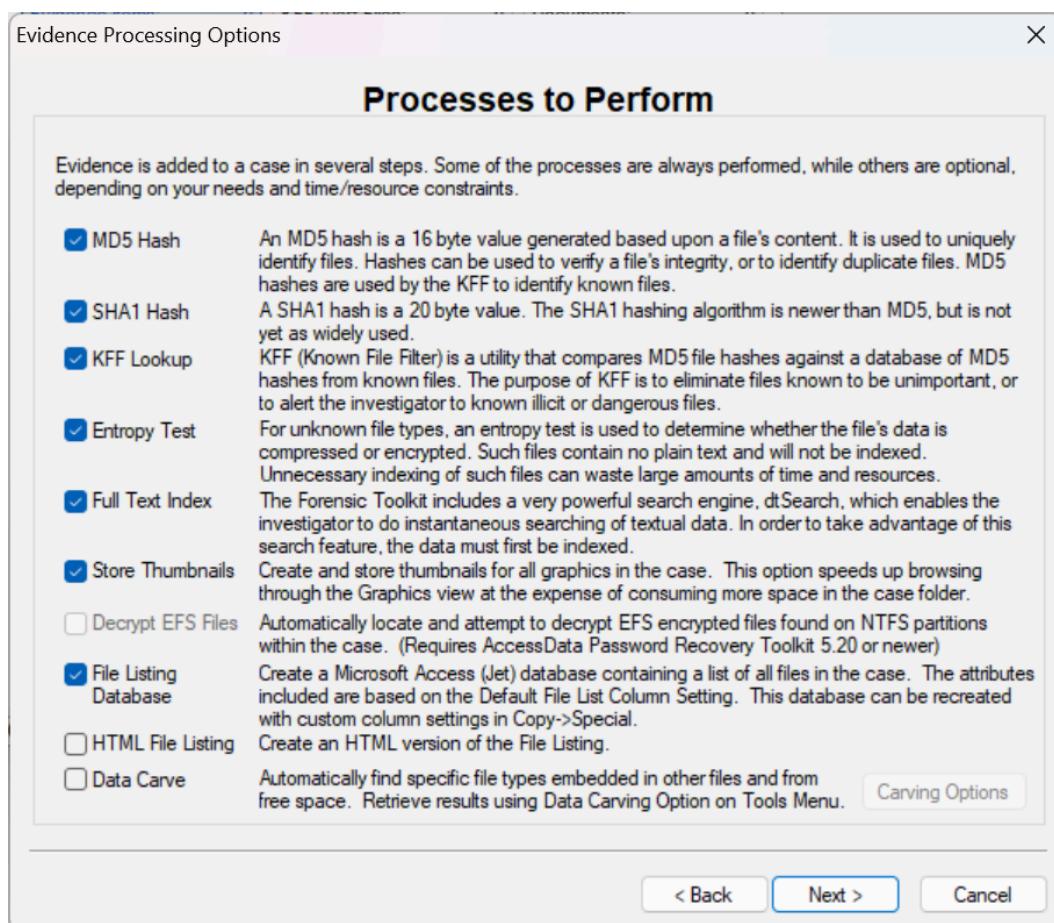
4. How can you add comments to a log file?

Comments can be added by selecting “Add Case Log Entry...” under the Tools menu in FTK.

5. List 3 events that can go in a Case Log.

- Adding or processing evidence files
- Recording search queries and results
- Logging error messages or warnings

2. Process to Perform



1. How many bits in a MD5 and SHA1 key? List 3 other Hash Algorithms

- MD5: 128 bits (16 bytes)
- SHA-1: 160 bits (20 bytes)
- Other hash algorithms: SHA-256, SHA-512, CRC32

2. What is the function of the KFF utility?

The KFF (Known File Filter) utility compares MD5 file hashes against a database of known file hashes.

Its main purpose is to:

- Eliminate files known to be unimportant (like standard system files).
- Identify known illicit or dangerous files by matching their hashes to known bad entries.

3. What is an Entropy Test?

An entropy test is used to measure the randomness of data in a file.

- It helps determine whether a file's data is compressed or encrypted.
- Files with high entropy likely contain encrypted or compressed data and therefore contain no plain text, meaning they will not be indexed by FTK.

4. How can we check if a file is compressed?

- Running an entropy test — high entropy indicates compression or encryption.
- Checking the file header or extension (e.g., .zip, .rar, .gz).
- Looking at FTK's file details or properties (FTK identifies compressed files during analysis).

5. Why does data need to be indexed?

Data is indexed to enable fast and efficient keyword searching.

FTK uses its built-in search engine (dtSearch) to quickly locate text or data across all files.

Without indexing, searches would be very slow because FTK would need to scan each file individually.

6. What does HTML File Listing function do?

The HTML File Listing function creates an HTML version of the file listing – a browsable webpage that shows all files and their metadata.

This allows examiners or reviewers to view the case contents in a browser without using FTK.

7. What is a thumbnail?

A thumbnail is a small preview image automatically generated for each picture file in the case.

It allows the examiner to quickly view and identify images without opening each one individually.

FTK stores these thumbnails to speed up browsing in the Graphics view.

8. What other types of databases can be used to store lists of files?

FTK uses a Microsoft Access (Jet) database for file listings, but other databases can also be used, such as: MySQL, PostgreSQL, SQLite

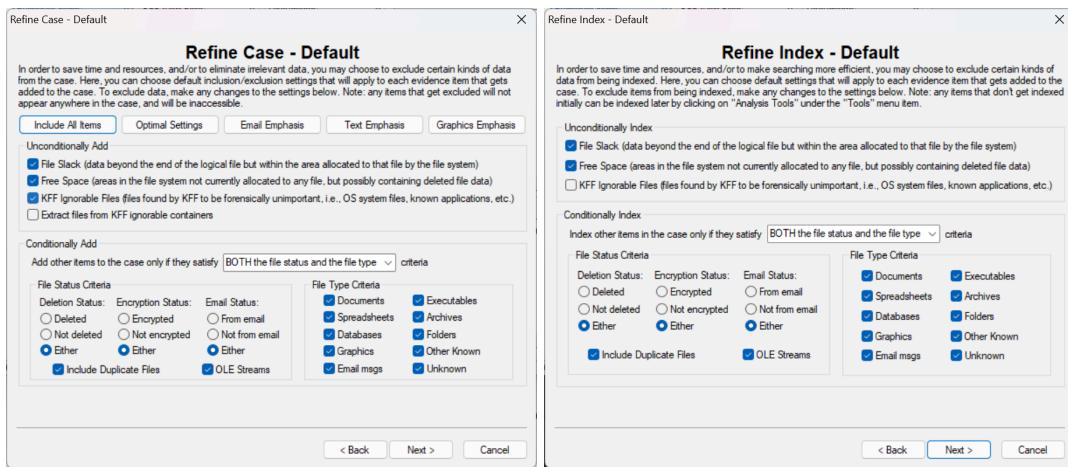
9. What is data carving? “Research further”

Data carving is the forensic process of recovering files from unallocated or free space on a disk by searching for known file signatures (headers and footers).

It does not rely on file system metadata – instead, it reconstructs files based on their binary patterns.

This technique is especially useful for recovering deleted, damaged, or partially overwritten files.

3. Refine Case - Default



1. What are the options for excluding certain kinds of data?

- File Slack: Data beyond the end of a logical file but still within the allocated cluster.
- Free Space: Unallocated areas of the file system that may still contain deleted data.
- KFF Ignorable Files: Files identified by the Known File Filter as forensically unimportant (e.g., system or common application files).
- Conditional filters:
 - File Status (deleted, encrypted, email-related).
 - File Type (documents, graphics, executables, archives, etc.).
 - Duplicate files (optionally include or exclude duplicates).

2. What is the difference Slack Space and Free Space? Expand your answer with additional research.

Slack space exists within allocated clusters of existing files, while free space consists of unallocated clusters that can still hold recoverable deleted data.

Aspect	Slack Space	Free Space
Definition	The unused area within an allocated cluster after the end of a file's actual data	Disk space not currently assigned to any file or folder
Location	Inside the last cluster of an existing file	Outside of allocated files – part of unallocated disk area
Created When	A file does not completely fill its last cluster (e.g., file size = 6 KB, cluster size = 8 KB → 2 KB slack)	Files are deleted, partitions formatted, or space never used
Contents	May contain fragments of old data from previously stored files	May contain full deleted files or remnants of earlier data
Forensic Value	Useful for finding hidden data fragments inside active files	Useful for data carving and recovering entire deleted files

3. What utility compares file hashes against a reference database to eliminate known files?

It matches the hash values of files in the case against a database of known good or known bad hashes to:

- Automatically exclude common system files (known good).
- Identify known illegal or malicious files (known bad).

4. What is difference between File Status and File Type?

- File Status – Describes the current state or condition of a file within the file system. (*tells how the file exists*)
 - Deleted, Encrypted, From Email, etc.
- File Type – Describes the kind or format of the file, determined by its content or extension. (*tells what the file is*)
 - Documents (.docx, .pdf), Executables (.exe), Archives (.zip), Graphics (.jpg)

4. Verify Data Integrity

