

Digital Forensics Lab Guide

Required material	Requirement
Software	FTK Forensic Toolkit installed and licensed
Supporting tool	FTK Imager installed
Evidence	HDD_Image_RedHotPassion.dd or raw image or E01 Image
Storage	Separate folders for evidence, case files, exports, screenshots, and reports
Documentation	Student evidence log sheet
Permissions	Use only authorised lab images

Activity 1: FTK First-Time User Guided Options Tour

Part A: Evidence Intake and FTK Imager Preview

Task A1: Create an evidence intake record

Field	Student entry
Case name	
Examiner name	
Date and time received	
Evidence image filename	
Image format	
Storage location	
Provided hash value, if supplied	
Notes from instructor	

Task A2: Open the image in FTK Imager

1. Open FTK Imager.
2. Select File > Add Evidence Item.
3. Choose the correct source type, such as image file.
4. Browse to the supplied evidence image.
5. Add it to the evidence tree.
6. Expand the image and observe the partition, folders, and files.

Reflections:

- a. What type of image did you open?

Answer: _____

- b. How many partitions or file systems are visible?

Answer: _____

- c. What top-level folders are present?

Answer: _____

- d. Are deleted files visible?

Answer: _____

- e. What hash values are available or generated?

Answer: _____

Part B: Create a New FTK Case

1. Open FTK Forensic Toolkit.
2. From the case manager, create a new case.
3. Use a clear naming convention, for example FTK_Lab01_StudentSurname.
4. Enter examiner information.
5. Set the case folder to a location separate from the original evidence image.
6. Select or review the processing profile.

Reflection:

Do you think that the case folder should be separate from the original evidence image?

Answer: _____

Part C: Explore Processing Options

Open the processing options or detailed options screen and locate as many of the following as your FTK version provides. Some options may depend on licence, version, or the type of evidence image.

Processing option	What it is used for	Available? Yes/No
File hashing	Calculates file hashes for identification and comparison	
Indexing	Supports fast keyword searching	
KFF / Known File Filter	Compares hashes against known or notable files	
Expand compound files	Extracts contents from archives, email containers, and similar files	
Flag bad extensions	Detects extension/file type mismatches	
Data carving	Attempts to recover files from unallocated or slack space	

Graphics thumbnails	Creates thumbnail views for image review	
Video thumbnails	Creates thumbnail previews for video review	
Explicit image detection / image recognition	Flags images according to configured detection options, if licensed	
OCR	Extracts text from supported images, if enabled	
Email processing	Parses supported email containers	
Internet/browser artefact parsing	Extracts browser-related artefacts where supported	
Mobile artefact parsing	Parses mobile extraction data where supported	
Registry/system artefact processing	Parses operating system artefacts where supported	

Reflection:

Which options would make processing slower but analysis easier?

Answer: _____

Which options are useful for a quick first look?

Answer: _____

Which options are most useful for image and video cases?

Answer: _____

Which options are most useful for keyword-heavy cases?

Answer: _____

Part D: Add Evidence to the FTK Case

1. Add the instructor-provided image to the case.
2. Confirm the evidence item name.
3. Confirm the evidence path.
4. Apply the selected processing profile.
5. Start processing.
6. Monitor the processing status window.
7. Record any errors or warnings.

Item	Student entry
Evidence name	
Image path	
Image format	
Processing profile used	
Processing start time	
Processing end time	
Errors or warnings	
Number of files processed, if shown	

Part E: Navigate the Main FTK Review Areas

Tour the main FTK interface. Some tabs may not appear if the evidence does not contain that data type or if a feature is not licensed. Mark unavailable items as N/A.

E1: Explore tab

1. Expand the evidence image.
2. Locate operating system folders.
3. Locate user profile folders.
4. Select at least three files and inspect their content.
5. View each file using different viewers, such as natural view, text view, hex view, and properties view, where available.

File path	File type	Created	Modified	Accessed	Notes

E2: Overview tab

1. Locate file categories such as documents, graphics, executables, folders, archives, email, or system files.
2. Locate file status categories such as deleted files, bad extensions, encrypted files, duplicate files, or email-related items, where available.
3. Select one category and compare it with the same items in Explore view.

Reflection

Which category contains the most files?

Answer: _____

Are there any deleted files?

Answer: _____

Are there any bad extension files?

Answer: _____

Are there any encrypted or password-protected files?

Answer: _____

E3: File List and File Content panes

1. Sort the File List by filename.
2. Sort by file size.
3. Sort by created or modified date.
4. Add or remove visible columns if your FTK version allows it.
5. Select a file and inspect its properties.
6. Compare natural, text, and hex views.

Reflection

Why is sorting by date useful?

Answer: _____

Why is sorting by file size useful?

Answer: _____

What can the hex view show that the natural view may not?

Answer: _____

E4: Graphics tab

1. Open the Graphics tab.
2. Review thumbnails.
3. Change thumbnail size if available.
4. Select one image and record its path and metadata.
5. Check whether the image also appears in the Overview tab under graphics.

File path	Image type	Size	Created/Modified	Relevant? Yes/No	Reason

E5: Email tab

1. Open the Email tab.
2. Locate mailboxes, messages, and attachments.
3. Select one message and view sender, recipient, subject, date, and attachments.
4. If no email exists, mark this section as No email artefacts found.

Sender	Recipient	Subject	Date/time	Attachment?	Notes

E6: Mobile, browser, registry, or system artefact views

1. Check for browser history, downloads, cookies, or cached files.
2. Check for registry or operating system artefacts.
3. Check for mobile data if the evidence is a mobile extraction.
4. Check for parsed application artefacts, if present.

Artefact type	Location in FTK	Example item	Notes
Browser history			
Downloads			

Registry/system			
Mobile/chat			
Application artefact			

Part F: **Searching**

1. Task F1: Run an index search
2. Open the Index Search area.
3. Search for a common term provided by your instructor, such as a username, project name, email domain, or file keyword.
4. Record the number of hits.
5. Open at least two results.
6. Bookmark one relevant result.

F2: **Run a live search**

1. Open the Live Search area.
2. Search for a specific string such as an email address, phone number, username, filename, or short phrase.
3. Compare the results with the index search.
4. Record whether the live search took longer.

F3: **Try a pattern search**

Pattern type	Example use
Email address	Find possible email addresses
URL	Find web addresses
IP address	Find network artefacts
Phone number	Find communication artefacts
File extension	Find specific file types or suspicious renaming

Search type	Search term/pattern	Hits	Useful result?	Notes
Index search				
Live text search				
Pattern search				
Boolean search				

Part G: Filters, KFF, and Labels

G1: Apply built-in filters

1. Apply a filter for graphics, documents, deleted files, or another available category.
2. Apply a date or size filter if available.
3. Compare the filtered result count with the unfiltered count.

G2: Review KFF results

1. Locate KFF-related columns or filters.
2. Identify whether any files are marked as known, ignored, or alert files.
3. Record one example if present.

G3: Create and apply labels

1. Create labels such as Relevant, Needs review, Non-relevant, Exported, and Timeline item.
2. Apply at least two labels to selected files.
3. Record why each label was used.

Label	Purpose
Relevant	Important to the investigation
Needs review	Requires further manual examination
Non-relevant	Reviewed but not useful
Exported	Exported for report or further examination
Timeline item	Important to chronology

Part H: Bookmarks

Bookmark folder	Purpose
Key Documents	Important documents
Key Images	Important graphics
User Activity	Files showing user behaviour
Deleted Items	Deleted or recovered files
Search Hits	Results from keyword or pattern searches
Timeline Events	Items relevant to chronology

H2: Bookmark evidence

1. Select at least five items.
2. Right-click and create bookmarks.

3. Add a short comment explaining why each item was bookmarked.
4. For email evidence, include attachments or parent email where appropriate.
5. For timeline evidence, create timeline bookmarks if your FTK version supports them.

Bookmark name	File path	Reason bookmarked	Related search/filter	Notes

Part I: Timeline Review

1. Open the timeline view, if available.
2. Choose a date range.
3. Identify clusters of file creation, modification, access, download, or email activity.
4. Create at least three timeline notes or timeline bookmarks.

Date/time	Artefact	File path or item	Event type	Interpretation

Part J: Export and Reporting

J1: Export a file list

1. Select a group of files.
2. Export the File List to CSV or TSV, if available.
3. Save it in your lab export folder.
4. Record the filename.

J2: Export selected files

1. Select one or two non-sensitive training files.
2. Export them to a controlled export folder.
3. Record the file path and hash, if available.
4. Do not export unrelated private data.

J3: Generate a case report

Include case information, examiner information, evidence summary, bookmarks, graphics if relevant, file paths, file properties, timeline items if available, and exported file lists.

Report section	Include?
Case information	Yes
Examiner information	Yes
Evidence summary	Yes
Bookmarks	Yes
Graphics, if relevant	Yes
File paths	Yes
File properties	Yes
Timeline items, if available	Yes
Exported file list	Attach separately