

You have been given a forensic image from a training investigation. The image may contain user files, deleted data, web activity, images, communications, or system artefacts. Your task is to examine the image using FTK and produce a structured forensic analysis report.

Note: Use careful forensic language. For example, write "The evidence image contains a file named..." rather than "The suspect definitely created..." unless the evidence clearly supports that conclusion.

Investigation Questions

1. What operating system or file system appears to be present?
2. What user accounts or user folders are present?
3. What files appear relevant to the case scenario?
4. Are there deleted files, bad extensions, encrypted files, or archives?
5. Is there evidence of web browsing, downloads, email, chat, or external device use?
6. Are there images, videos, or documents that require closer review?
7. What timeline of activity can be reconstructed?
8. What evidence supports each conclusion?
9. What limitations remain?

Recommended Workflow

Stage	Actions	Output
1. Intake and verification	Record image filename, format, size, location; preview in FTK Imager; verify or record hashes; note partitions and file systems.	Evidence intake table and screenshot
2. Case creation and processing	Create FTK case; add evidence image; select processing profile; enable suitable options; allow processing to complete.	Case record and processing log
3. Initial triage	Review image type, file system, user folders, major file categories, deleted data, archives, encrypted files, and bad extensions.	Triage table
4. Artefact review	Review user profiles, documents, images, browser	Artefact checklist

	artefacts, email, deleted data, archives, registry/system artefacts, and timeline items.	
5. Search strategy	Run index, live, Boolean/refined, file category, and date/timeline searches.	Search results table
6. Bookmarking and validation	Bookmark key findings and record file path, timestamps, hash values, relevance, confidence, and limitations.	Bookmark log
7. Timeline reconstruction	Build chronology from file timestamps, browser activity, email dates, downloads, and deleted/recovered items.	Timeline table
8. Final report	Write case summary, evidence handling, methodology, findings, timeline, exported evidence, limitations, and conclusion.	Forensic report

Initial Triage Table

Triage question	Answer	Supporting artefact
What image type is this?		
What file system is present?		
What user folders exist?		
What time zone is suggested?		
What major file categories exist?		
Are deleted files present?		
Are encrypted files present?		
Are archives present?		

Are bad extensions present?		
-----------------------------	--	--

Artefact Review Checklist

Artefact area	What to check	Evidence to record
User profiles	Desktop, Documents, Downloads, Pictures, AppData	Paths, filenames, timestamps
Documents	Office files, PDFs, text files	Metadata, content, keywords
Images/videos	Thumbnails, EXIF, file paths	Image name, path, created/modified time
Browser artefacts	History, downloads, cache, cookies	URLs, download paths, timestamps
Email	Mailboxes, messages, attachments	Sender, recipient, subject, dates
Deleted data	Recycle Bin, deleted folders, carved files	Original path if available
Archives	ZIP, RAR, 7z, compressed files	Contents and timestamps
Encrypted files	Password-protected files, encrypted containers	Location and type
Bad extensions	Extension mismatch	Original extension and detected type
Registry/system	UserAssist, USB artefacts, MRUs, event logs, if parsed	User/system activity
Timeline	Created, modified, accessed, email, browser, download events	Chronology

Search Strategy

Search group	Example terms	Purpose
People	Username, names, initials	Identify user-related artefacts

Communication	Email addresses, domains, phone numbers	Find contact evidence
Web	URLs, domains, search terms	Find browsing/download evidence
Documents	Project names, case words, file names	Find relevant documents
Dates	Important dates or years	Connect activity to timeline
File types	.jpg, .pdf, .docx, .zip	Locate specific categories
Concealment	password, delete, hidden, backup	Identify possible concealment

1. One Index Search.
2. One Live Search.
3. One Boolean or refined search.
4. One file category or extension search.
5. One date-based review using timeline or filters.

Search type	Term or pattern	Hits	Most relevant file path	Bookmark created?
Index				
Live				
Boolean/refined				
Extension/category				
Date/timeline				

Evidence Bookmarking and Validation

Category	Minimum required
Key documents	2
Key images or media	1
Deleted/recovered items	1, if present
Browser/download artefacts	1, if present

Email/message artefacts	1, if present
Timeline events	3
Other relevant artefacts	As needed

Required detail	Example
File path	Users/Alex/Documents/report.docx
Filename	report.docx
File type	Microsoft Word document
Created/modified/accessed times	Record exactly as FTK displays
Hash value, if available	MD5/SHA1/SHA256 if shown
Why it matters	Explain relevance
Supporting view	Natural/text/hex/properties/timeline
Bookmark name	Key Documents > Report.docx
Confidence level	High / Medium / Low
Limitation	File existence does not prove authorship

Timeline Reconstruction

Date/time	Event	Artefact	Path/source	Interpretation
	File created			
	Web download			
	File modified			
	Email/message			
	File deleted/recovered			

Key Facts

What is the earliest relevant event?

Answer:

What is the latest relevant event?

Answer:

Are there clusters of activity?

Answer:

Do file timestamps support or contradict other artefacts?

Answer:

Are any timestamps missing, inconsistent, or suspicious?

Answer:

Final Report Structure

1. Case summary

Case name

Examiner

Date of examination

Evidence image name

Tool used

Scope of examination

2. Evidence handling

Image filename

Image type

Hash values

Storage location

Processing profile used

Processing options selected

3. Methodology

FTK Imager preview

FTK case creation

Evidence processing

Searching

Filtering

Bookmarking

Timeline analysis

Export/report generation

4. Findings

Finding no.	Finding	Supporting evidence	Interpretation	Confidence	Limitation
1					
2					
3					
4					
5					

5. Timeline of relevant activity

Insert the completed timeline table from the timeline reconstruction stage.

6. Exported evidence

Exported item	Original path	Export path	Reason exported

7. Limitations

- + Some artefacts may not have been parsed by the selected processing profile.
- + Some files may be encrypted or corrupted.
- + A timestamp alone does not prove who performed an action.
- + Deleted data may be incomplete.
- + Some FTK features may be version-dependent or licence-dependent.

8. Conclusion

Summarise what was found, what was not found, and how strongly the evidence supports the investigation questions.

Resources

Exterro FTK Forensic Toolkit product information: <https://www.exterro.com/digital-forensics-software/ftk-forensic-toolkit>

Exterro FTK Imager product information: <https://www.exterro.com/digital-forensics-software/ftk-imager>

Exterro FTK 8.1 User Guide PDF:

<https://d1kpmuwb7gvu1i.cloudfront.net/8.x/8.1.0/1/Exterro%20FTK%208.1%20-%20User%20Guide.pdf>

Exterro FTK Imager 8.2 User Guide PDF:

<https://d1kpmuwb7gvu1i.cloudfront.net/Imager/8.2/Exterro%20FTK%20Imager%208.2%20-%20User%20Guide%20.pdf>