TEQUILA SO
Jocsan Laguna

FTK Imager

Acquisition, preview, hashing and documentation

PRACTICAL GUIDE 2026 · DOCUMENTATION 8.2



Contents

1. What FTK Imager does and does not do 3

1.1 The rule for the original source 3

2. Preparing for acquisition 3

2.1 Safe lab practice 4

3. Creating an image step by step 4

4. Choosing the format, splitting, and compression 4

5. Verifying and preserving the result 5

6. Previewing and exporting while preserving source traceability 5

7. Mounting an image: read access, write caching, and limitations 6

8. Memory capture: a different type of operation 6

9. Common errors and safe decisions 6

10. Exercise using fictitious files 7

11. Pre-report checklist 7

12. Official sources and editorial control 7

Machine-assisted translation from the Spanish edition. The Spanish source is the editorial reference.

FTK Imager is used to create forensic images, preview evidence, export files, and verify integrity. Its primary role is not to replace analysis, but to enable analysis using a documented source without relying on the original.

This guide explains the workflow in plain language. It is neither a literal translation nor an official Exterro guide. The menus are based on the 8.2 documentation and should be checked against the installed version.

1. What FTK Imager does and does not do

The application can create bit-for-bit copies, examine content, mount images for read-only access, export files, generate hash lists, and capture memory under certain conditions. It is especially useful before analysis in Autopsy or another platform.

Task	FTK Imager	Autopsy
Create a disk or file image.	This is its core function.	This is not the first step in its primary workflow.
Preview folders and files.	Evidence tree, file list, properties pane, and viewer.	Tree, results, and content views, with additional analysis modules.
Perform case analysis and correlation.	Limited compared with a full case-management platform.	Ingestion, search, timeline analysis, communications, reporting, and more.
Verify integrity.	Verification during acquisition and post-acquisition verification.	Data Source Integrity for compatible data sources, plus other checks.

Creating an image does not complete an investigation. It is a preserved representation that still requires examination and context.

1.1 The rule for the original source

The official guide recommends using a **hardware write blocker** when imaging a drive. This prevents the operating system from modifying the original source when it is connected.

Do not confuse these three actions:

- **Create an image:** produces a copy of the source.
- **Mount an image for read-only access:** lets you examine the copy; it does not turn the image into a write blocker for the original.
- **Work with a copy:** keeps the original out of the analysis process.

2. Preparing for acquisition

Before opening FTK Imager, document the case and the device. Rushing through the options often results in complete images of the wrong disk.

1. Authorize the scope, source, and method.
2. Identify the model, capacity, and serial number when available.
3. Use a hardware write blocker for the original source.

4. Use a destination separate from the source, with sufficient power and storage space.
5. Prepare one folder for the image and another for logs and reports.
6. Record the FTK Imager version, date, time zone, and operator.

The destination must have enough capacity for the full image, image segments, acquisition information, and working copies. “There is room for the disk” does not always mean “there is room for the whole process.”

Never save the image to the same disk you are imaging. You could alter or destroy what you are trying to preserve.

2.1 Safe lab practice

The downloadable lab does not require you to connect an evidence drive. Use the fictitious folder as a logical collection of files to learn the interface and its options. Do not practice physical acquisition on your primary drive or on other people's devices.

3. Creating an image step by step

The basic path is **File > Create Disk Image**. The wizard lets you choose the source and destination.

7. Select the source type as appropriate: physical drive, logical drive, existing image, or folder contents.
8. Confirm the exact device by its identifiers, not just its drive letter.
9. Choose a destination folder separate from the source.
10. Choose a filename without an extension and link it to the case identifier.
11. Complete the available metadata fields: case, evidence, description, examiner, and notes.
12. Review the image type, splitting, and compression settings.
13. Enable **Verify images after they are created** to check integrity when acquisition finishes.
14. Consider **Create directory listings of all files in the image** to preserve available paths and metadata.
15. Review everything before clicking **Start**.
16. Keep the acquisition log and summary, including any read errors.

Do not click Start if you are still unsure which source to use. Go back to the evidence intake record and verify it.

4. Choosing the format, splitting, and compression

The format depends on the source and the downstream workflow, not on habit.

Option	What it means	What to check
Raw / DD	A direct copy with broad compatibility and no mandatory compression.	Requires sufficient space for the source and all segments.
E01	An evidence image with metadata and compression options that depend on the workflow.	Compatibility with analysis tools and preservation of metadata.
AD1	A logical image of custom-selected content.	It is not a physical disk image and does not contain the disk's full geometry.
Splitting	Splits the output into multiple size-limited files.	All segments must be kept together for analysis and verification.

Compression 0–9	Trade-off between speed and size, depending on the selected format.	Higher compression can increase processing time.

The 8.2 guide documents a default fragment size of **1500 MB** for this workflow. Do not treat this as a universal rule. Choose a size based on storage, transport, and analysis requirements; if the value is 0, the output is not split when that option is available.

Do not change formats expecting the content to remain bit-for-bit identical. A representation may preserve visible information while changing its structure and hashes. Document the relationship between the original and the derivative.

5. Verifying and preserving the result

When acquisition finishes, review the summary before accepting the image as valid. Verification during creation compares the generated hashes and helps detect discrepancies. If the results do not match, do not treat the image as valid.

17. Record the source and image hashes, specifying the algorithm and the object hashed.
18. Review the sectors read and any read errors.
19. Verify that all segments are in the same folder.
20. Retain the acquisition log and the content listing, if generated.
21. Open the image as evidence to confirm that it can be read without being modified.
22. Run a subsequent verification when appropriate and compare the result with the recorded value.

The 8.2 guide documents **MD5 and SHA-1** for several of the application's hashing functions. If your procedure also requires SHA-256, calculate it with an appropriate tool and record that it belongs to a separate process; do not present it as an FTK Imager feature.

Matching hashes prove that the object did not change between checks; they do not prove that the content is truthful or that the source is legitimate.

6. Previewing and exporting while preserving source traceability

The evidence tree displays sources and folders; the file list changes with the selection; the properties pane shows the type, location, size, and dates; and the viewer displays the content.

To examine a file:

23. Add the image using **Add Evidence Item**.
24. Expand the source and navigate to the file.
25. Review its properties and content, not just its name.
26. Examine neighboring files to understand the context.
27. Export it to a working folder and retain its original path.
28. If you need a hash list, select the objects and use **Export File Hash List**.

An exported file is a derivative. Do not present it as though it were still in its original location, even if its content is identical.

7. Mounting an image: read access, write caching, and limitations

FTK Imager can mount certain images as a device or drive for read-only access. It also documents write-cache modes in which changes are stored separately and do not alter the image's original content.

Mode	What it allows	Caution
Read-only access	Examine the image without changing its content.	This is not equivalent to a write blocker for the original disk.
Write cache	Save changes or annotations to a separate file.	Document the cache and do not present it as the original content.

Physical and logical mounting are not interchangeable. AD1 and L01 images contain file structures but not the disk's full geometry, so they cannot be mounted as physical images.

When finished, unmount the image and record any changes made. The fact that Windows lets you open a drive does not prove that you can write to it.

8. Memory capture: a different type of operation

Capturing memory on a live system has its own effects. It can change processes, content, and the system's state. Memory is volatile, and the capture must be saved to a separate destination, with its date and hash recorded.

Do not use this feature as an introductory exercise on a real system. If the case requires a memory capture, first establish the authorization, objective, method, impact, tool, and chain of custody. Capture and subsequent analysis are distinct operations: FTK Imager performs the capture; Volatility or another platform can help examine the result.

9. Common errors and safe decisions

Situation	Responsible action
You do not know which disk is the original	Stop. Verify the model, capacity, serial number, and intake record; do not guess based on the drive letter.
The destination runs out of space	Stop and reallocate storage. Keep all related segments in the same folder.
The image fails verification	Do not use it as a valid copy. Document the failure and repeat the process using the appropriate method.
No deleted files appear in a logical collection	Check whether the source and method provide access to unallocated space. Do not claim a recovery that did not occur.
You cannot mount an AD1 image as a physical image	This is a limitation of the content type. Use the supported logical mounting option.
A hash differs after conversion	Determine what changed: the structure, metadata, content, or object being compared. Do not automatically conclude that the evidence has been falsified.
The content needs to be analyzed	Add the image to Autopsy or another platform; do not confuse

	acquisition with full analysis.

10. Exercise using fictitious files

Use the lab folder to explore the options without working on a real disk.

29. Open FTK Imager and select folder contents, not your primary drive.
30. Select only the extracted folder of fictitious files.
31. Configure a new destination outside that folder.
32. Add demonstration metadata without using people's or clients' names.
33. Enable verification and content listing.
34. Review how the image, segments, and logs are stored.
35. Open the result as evidence and locate `01_notas.txt`.
36. Export a working copy and a hash list, indicating which process you used for each.
37. Document why this exercise demonstrates neither physical acquisition nor recovery of deleted files.

The exercise teaches the interface workflow. It neither turns the folder into a disk nor makes the resulting image legal evidence.

11. Pre-report checklist

- Authorization and scope documented in writing.
- Source identified by model, capacity, and serial number whenever possible.
- Write blocker used for the original source.
- Separate destination with sufficient space.
- Image type, splitting, and compression settings justified.
- Complete case and evidence metadata.
- Verification performed and results reviewed.
- All segments kept together and readable.
- Read errors and limitations documented.
- Working files linked to their source.
- Subsequent analysis kept separate from acquisition.
- Conclusions limited to what the method demonstrates.

12. Official sources and editorial control

38. Exterro FTK Imager 8.2 User Guide
39. Exterro FTK Downloads
40. Autopsy User Documentation 4.23.0: Quick Start Guide
41. Autopsy User Documentation 4.23.0: Data Sources
42. Autopsy User Documentation 4.23.0: Reporting
43. ISO/IEC 27037, identification, collection, acquisition, and preservation
44. NIST SP 800-86, forensic techniques for incident response

The 8.2 guide was read in full for this adaptation. Its contents include features from different versions and products; not all of them are included in the free edition of FTK Imager. Before using a Pro or mobile acquisition feature, verify the license and consult the relevant documentation.

This guide is learning material by Jocsan Laguna, not an official Exterro publication or legal advice. Editorial review: November 15, 2026.