TEQUILA SO
Jocsan Laguna

Free tools for computer forensics

Autopsy · FTK Imager · ExifTool · PhotoRec · Volatility

PRACTICAL GUIDE · 2026



Contents

1. Choose the tool based on the question 3
2. FTK Imager: acquisition and preview 3
Initial walkthrough 3
3. Autopsy: analysis and timeline review 4
Initial walkthrough 4
4. ExifTool: specific file metadata 4
Basic read-only inspection 4
5. PhotoRec: signature-based recovery 5
Responsible workflow 5
6. Volatility 3: memory analysis 5
7. A small, auditable workflow 6
8. Fictional lab and decision exercise 6
9. Rules that prevent serious mistakes 7
10. Official sources and verified versions 7

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

A collection of programs is no substitute for a method. This manual brings together five tools because they answer different questions: FTK Imager for acquisition and previewing, Autopsy for analysis, ExifTool for metadata, PhotoRec for signature-based recovery, and Volatility 3 for memory analysis.

1. Choose the tool based on the question

Before opening any program, write down what you want to know, what source you have, and what you must not alter. Authorization and preservation do not depend on the software's price.

Question	Tool	What you can expect	What it does not prove
I need to create an image or examine its basic contents.	FTK Imager	Image, preview, export, and verification.	A complete case analysis.
I need to examine files, activity, and a timeline.	Autopsy	Artifacts, searches, tags, timelines, and reports.	Automatic confirmation of authenticity or authorship.
I need to know what metadata a file contains.	ExifTool	Metadata fields present and differences between files.	That the date or location is necessarily accurate.
I need to attempt signature-based content recovery.	PhotoRec	Files recoverable from a compatible copy or image.	Names, folders, completeness, or guaranteed success.
I need to examine a memory capture.	Volatility 3	Processes, connections, and artifacts present in that capture.	The complete system state or its history.

Free does not mean harmless. Reading a source can expose confidential data; running a sample can activate malware; writing to the wrong destination can destroy evidence.

2. FTK Imager: acquisition and preview

FTK Imager creates images, previews files, exports content, and verifies integrity. The official 8.2 guide recommends using a hardware write blocker when acquiring an original drive.

Initial walkthrough

1. Identify the source, the authorization, and a separate destination.
2. Open **File > Create Disk Image**.
3. Confirm the source by model, capacity, and serial number, not just by drive letter.
4. Choose the appropriate image format, segment size, and compression for the downstream workflow.
5. Enable verification after creation and retain the directory listing when appropriate.
6. Review the summary, hashes, and read errors.

Do not begin analysis until you know what the source is. Mounting an image is not a substitute for write-blocking the original disk.

Official source: Exterro FTK Imager 8.2 User Guide and Exterro FTK Downloads.

3. Autopsy: analysis and timeline review

Autopsy organizes a case, adds data sources, runs ingest modules, and generates artifacts. The reference version for this kit is 4.23.0.

Initial walkthrough

7. Create a case in a new folder.
8. Add an image, a controlled disk, or authorized logical files.
9. Select only the modules needed to answer the question.
10. Wait for all ingest modules to finish before drawing conclusions.
11. Search for content, review its location, and tag relevant items.
12. Use Timeline with a documented time window and time zone.
13. Generate a report of tagged items and document the method and limitations separately from the automated output.

Logical Files is not equivalent to a full disk. This method does not examine unallocated space or deleted files on the device; use it to practice with authorized documents, not to promise recovery.

To translate text, configure Bing or Google with your own account and click **Test**. Then enable **Translate Text** under View Options. Retain the **Original Name** column and check negations, proper names, and legal terms against the original text.

Official sources: Download, Quick Start, Data Sources, Timeline, Machine Translation, and Reporting.

4. ExifTool: specific file metadata

ExifTool reads, writes, and edits metadata in many formats. The verified reference for this edition is **13.63, released on November 10, 2026**. The official site provides packages and checksums; do not use copies from third-party sites.

Basic read-only inspection

Open a terminal in a copy of the lab and run:

```
exiftool 03_imagen_demo.png
```

The output shows the fields present. It does not invent a date, camera, or location if they do not exist. The lab image was created for demonstration purposes, so its content and metadata do not represent an actual photograph.

To display only selected fields:

```
exiftool -filename -imagesize -datetimeoriginal -gps:all -model 03_imagen_demo.png
```

If a field is absent, that absence is also information: do not claim that a location or capture device exists.

To display tag names instead of descriptions:

```
exiftool -s 03_imagen_demo.png
```

To compare two files without including system or composite tags:

```
exiftool archivo_A.jpg -diff archivo_B.jpg --system:all -e
```

These commands read and compare files. They do not modify the evidence. Before writing metadata, always work on a copy and preserve the original; ExifTool can create backups with the `_original` suffix when writing.

Metadata is not proof of fact. A user, application, or conversion process can change the date, author, GPS data, or description. Verify the source and corroborate the information with other sources.

Official sources: ExifTool by Phil Harvey, application documentation, and FAQ.

5. PhotoRec: signature-based recovery

PhotoRec searches for data using file signatures even when the file system is damaged or has been reformatted. It is free, open source, and distributed with TestDisk.

PhotoRec accesses the source read-only, but you must choose a different destination for recovered files. Do not write to the same partition where the data was lost: you could overwrite what you are trying to recover.

Responsible workflow

14. Stop using the source to reduce overwriting.
15. Create an image or select an authorized working copy.
16. Run PhotoRec on that copy, not on the original.
17. Choose another destination for the results.
18. Review the recovered files, their contents, and their relationship to the source.
19. Document what could be read and what remained incomplete.

PhotoRec cannot restore the complete past. File names and folder structures are often lost; fragmentation can produce incomplete files; recovering content does not prove who created it or what happened.

Official source: PhotoRec ES and TestDisk Download.

6. Volatility 3: memory analysis

Volatility 3 analyzes memory captures using plugins. It is not a substitute for acquisition: you need a compatible capture and the appropriate symbols for the system being examined.

The analysis should be performed on a test capture, not on other people's personal data. An example of an initial inspection is:

```
python vol.py -f memoria_demo.raw windows.info
```

To examine processes recorded in the capture:

```
python vol.py -f memoria_demo.raw windows.pslist
```

To examine connections that the capture and plugin can analyze:

```
python vol.py -f memoria_demo.raw windows.netscan
```

The `memoria_demo.raw` file is for illustration only: this kit does not include a memory capture. To run these commands, you need a real source for training and the documented prerequisites. Do not download dumps from unknown sources that may contain sensitive data or malware.

A capture shows a moment in time, not the entire history. Visible processes and connections depend on the timing, acquisition method, and symbol compatibility.

Official sources: Volatility 3 on GitHub and generated documentation.

7. A small, auditable workflow

Five tools can support a basic workflow without accumulating unnecessary software.

Stage	Action	Work record
Authority	Define the objective, source, and permissions.	Scope, custodian, and exclusions.
Acquisition	Create an image or controlled copy.	Method, version, date, destination, and hash.
Review	Open the source in FTK Imager and locate files.	Path, format, and initial observations.
Analysis	Use Autopsy with selected ingest modules.	Artifacts, searches, tags, and timeline.
Metadata	Inspect specific copies with ExifTool.	Fields present and differences, without modifying the original.
Recovery	Use PhotoRec when warranted by the question.	Reviewed results and recovery limitations.
Memory	Analyze a capture with Volatility when necessary.	Compatible source, plugins, and outputs.
Report	Explain the method, findings, and limitations.	Reproducible review and cited sources.

You do not have to use every tool in every case. Occam's razor applies here too: choose the tool that best answers the question with the least alteration.

8. Fictional lab and decision exercise

The ZIP contains documents, an EML file, an image, and notes created specifically for teaching. It is not a capture from a real case.

20. Calculate the ZIP hash before extracting it and compare it with `SHA256SUMS.txt`.
21. Add the folder as Logical Files in Autopsy.
22. Search for `lavanda` and open the corresponding file.
23. Examine `03_imagen_demo.png` with ExifTool and note which fields are present and which are absent.
24. Open `02_correo_demo.eml` and verify that the sender uses a domain reserved for examples.
25. Document why these files do not prove transmission, authenticity, location, or intent.
26. Write a five-line summary: source, method, finding, limitation, and next verification step.

Do not run memory commands against that nonexistent test image. The lab teaches file reading and analysis; memory analysis requires another authorized source.

9. Rules that prevent serious mistakes

- Obtain authorization before accessing data, even when the technique is simple.
- Preserve the original and analyze a copy.
- Use a separate destination for images and recovered files.
- Download only from official websites and verify integrity whenever possible.
- Do not run unknown samples on your personal computer or production networks.
- Record the version, date, time zone, parameters, and operator.
- Distinguish findings, interpretations, and conclusions.
- Do not present metadata as automatically establishing authorship, an actual date, or a location.
- Do not promise complete recovery or claim that files are absent merely because they do not appear in a search.
- Do not share keys, credentials, or confidential data with an external translator without authorization.

10. Official sources and verified versions

27. Autopsy 4.23.0: user documentation
28. Exterro FTK Imager 8.2 User Guide
29. ExifTool 13.63: official website and downloads
30. ExifTool Application Documentation
31. PhotoRec ES, CGSecurity
32. Volatility 3: official repository
33. Volatility 3: documentation
34. ISO/IEC 27037
35. NIST SP 800-86

The versions were checked on November 15, 2026. Interfaces and formats change: always consult the current documentation before applying a procedure in a real case. This guide is educational and is not a substitute for legal advice, authorization, or professional review.