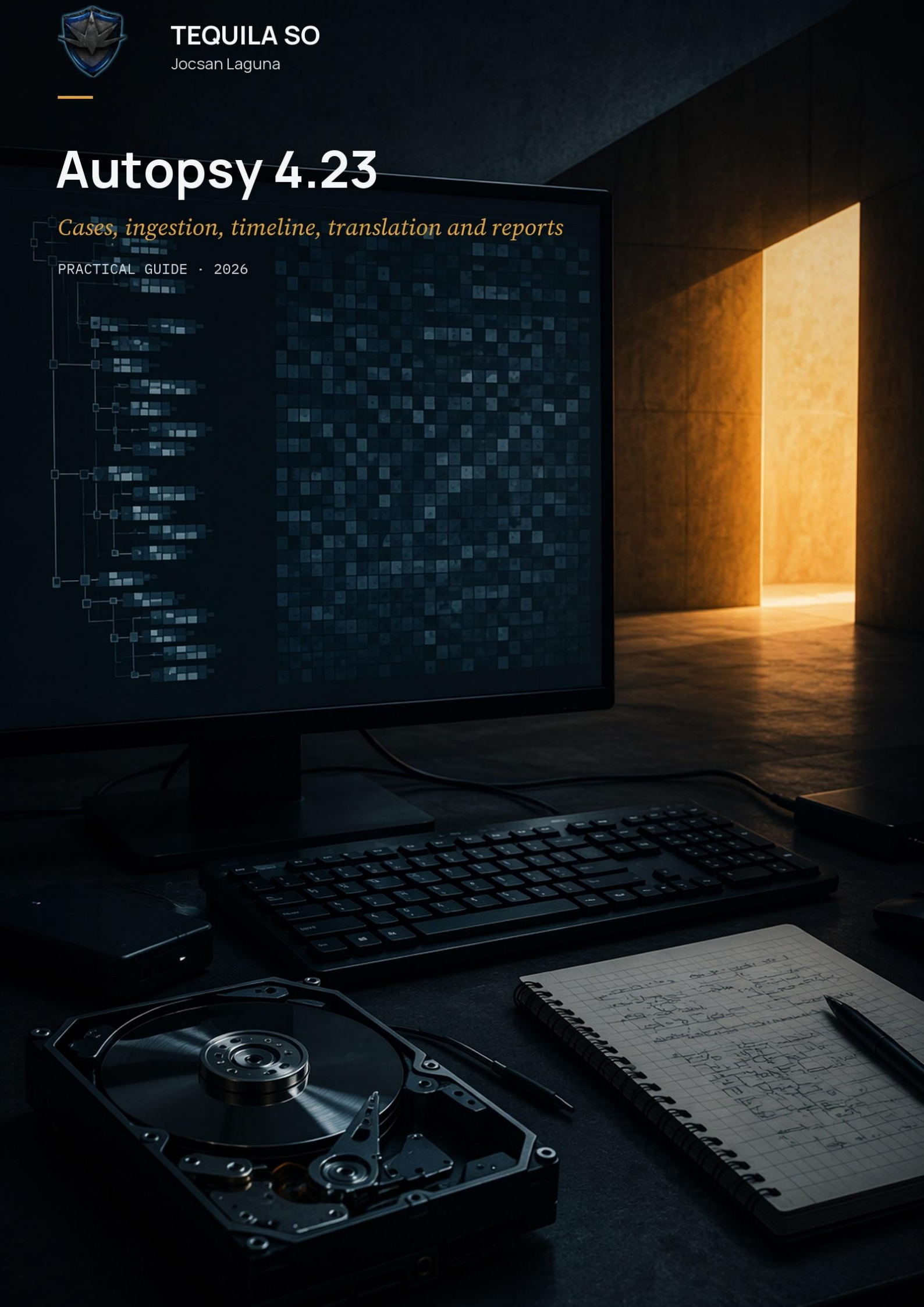


TEQUILA SO

Jocsan Laguna

Autopsy 4.23

Cases, ingestion, timeline, translation and reports

PRACTICAL GUIDE · 2026

Contents

Before handling evidence 3
1. The core concept: case, data source, and ingest 3
1.1 Acquisition is not analysis 3
2. Download and prepare the environment 4
2.1 The original remains outside the workflow 4
3. Create your first case with the lab 4
4. Choose ingest modules deliberately 5
5. Navigate results without losing context 6
5.1 Search exercise: “lavanda” 7
6. Use Timeline without confusing a date with intent 7
6.1 Time zones change interpretation 7
7. Configure translation correctly 8
8. Seek corroboration, not just matches 8
9. Generate a report that others can review 9
10. Common problems and recovery 9
11. Guided exercise with fictitious files 10
12. Glossary in plain language 10
13. Official sources and editorial checks 11

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

This guide introduces Autopsy as it would be presented in a first lab session: what it is for, what it does with data, and how to review its output. You do not need to be an engineer, but you do need a methodical approach. Authorization always comes before the tool.

The reference version is **Autopsy 4.23.0**. Menu names and features may vary in later versions. Screenshots are taken from Sleuth Kit Labs' official documentation and are credited alongside each figure.

Before handling evidence

Autopsy is a digital forensic analysis platform. It lets you set up a case, add data sources, run analysis modules, review artifacts, arrange events chronologically, and generate reports. It does not turn a file into authentic evidence or decide who is right.

Work only with your own material, material you are authorized to examine, or material published for learning. Preserve the original and use a working copy. If your goal is to acquire a real disk, first review the acquisition procedure and write blocking; Autopsy does not remove that responsibility.

The downloadable lab accompanying this guide contains only fictitious files. It does not represent a real case, a real conversation, or evidence in court. It is for practicing with the interface and documenting steps, not for drawing conclusions about people.

1. The core concept: case, data source, and ingest

Autopsy organizes work around three concepts that should be distinguished from the outset.

Concept	How to explain it in plain language	Mistake it prevents
Case	The working folder where settings, the database, and reports are stored.	Thinking that the case is merely the disk received.
Data source	The disk, image, virtual machine, folder, or logical collection of files to be examined.	Adding anything without knowing its origin and scope.
Ingest	The modules that analyze the source and produce artifacts for review.	Assuming that opening an image is equivalent to analyzing it.

A data source is not a conclusion. A file with a date may describe an event recorded by the system, but by itself it does not prove who created it, what intent was involved, or whether the system clock was correct.

1.1 Acquisition is not analysis

FTK Imager is used primarily for acquisition and previewing. Autopsy is used to analyze and organize the case. You can create an image with FTK Imager and then add it to Autopsy, or add logical files to Autopsy for practice.

Question	Suitable tool	Expected result
I need to create a forensic copy of a disk.	FTK Imager, with appropriate preservation and write blocking.	A documented and verified image.
I need to review files, activity, metadata,	Autopsy	Artifacts, searches, tags, and an analysis

and a timeline.		report.
I need to read specific metadata from a photo.	ExifTool.	Fields present in that file, not automatic proof of location or authorship.
I need to examine a memory capture.	Volatility 3.	Processes, connections and other artifacts present in that capture.

Do not start by installing every program. Start by defining the question: what you want to demonstrate, which source you will use, and how to minimize alteration.

2. Download and prepare the environment

Download Autopsy from its official page: autopsy.com/download. The page distinguishes 32-bit and 64-bit Windows installers, Linux/macOS packages, and GPG signature files. Do not download the installer from a software aggregator.

The installation documentation is available at sleuthkit.org/autopsy/docs/user-docs/4.23.0/installation_page.html.

1. Check the architecture of the computer and the downloaded file.
2. Verify the signature or integrity information provided by the project when available.
3. Install Autopsy on a controlled workstation, not on the system containing the original evidence.
4. Separate three locations: the preserved source, the case folder, and the output or reports folder.
5. If you are going to examine physical disks, run Autopsy with the necessary permissions and use a write-protected source. Do not use elevated privileges as an excuse to work without controls.

One possible lab structure, not a mandatory path, is:

```
C:\Forense\Fuentes\Laboratorio_Forense_Jocsan
C:\Forense\Casos\DEMO-2026-001
C:\Forense\Salidas
```

Do not store the original image inside the case folder as if it were a backup. The source must remain accessible during analysis: Autopsy maintains a reference to it, not a complete copy within the case.

2.1 The original remains outside the workflow

Before adding a real source, record who provided it, why you are authorized to examine it, its identifier, its condition, and its hash when applicable. If an image is split into segments, select the first file in the set and keep all segments together.

A screenshot or an Autopsy export does not replace the original file. It is a way to view and understand the data, not the entirety of the evidence.

3. Create your first case with the lab

Open Autopsy and choose **Create New Case**. Enter a name that does not expose client data, such as `DEMO-2026-001`, and select a folder that does not yet exist. Then add the data source.

6. In the wizard, select **Logical Files** for the lab.

7. Click **Add** and choose the extracted folder for the fictitious lab.
8. Verify that the folder contains only the demonstration files.
9. Keep the logical set name or change it to something meaningful, such as `DEMO-archivos`.
10. Continue to the ingest module configuration.

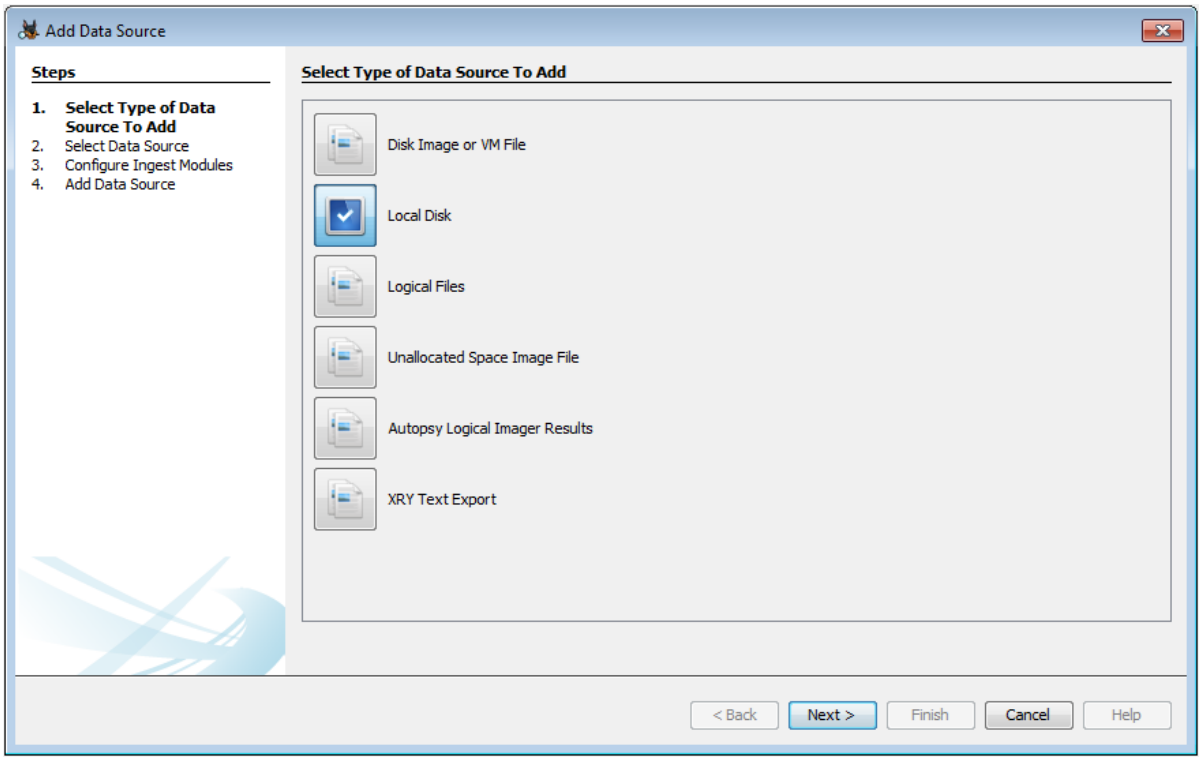


Figure 1. The wizard lets you choose an image, local disk, logical files, and other data sources. Screenshot from Sleuth Kit Labs, CC BY-SA 3.0.

Why use logical files? They let you learn the interface without connecting an evidence disk. The documentation warns that this method does not examine unallocated space or deleted files on the device; it works only with the selected allocated files. Do not expect to recover deleted files in this exercise.

Timestamps on logical files also require care. Autopsy may disregard them because they changed when the files were copied to your computer. This is not a malfunction: it is a limitation you must document.

4. Choose ingest modules deliberately

Ingest modules analyze the content of the data source. They run in the background, and results become available progressively. You can review files while they run, but do not present an analysis as complete while it is still ongoing.

For the lab, start with a small selection:

Module	Why you would use it in this exercise	What to remember
File Type Identification	Recognize file types by signature, not just by extension.	The signature helps identify the format, not the authenticity of the content.
Extension Mismatch Detector	Detect extensions that do not match the type detected.	A discrepancy warrants review, not an automatic accusation.
Embedded File Extraction	Open containers such as ZIP files and Office documents and process their	An extracted file is a derivative; preserve its relationship to its source.

	contents.	
Keyword Search	Locate words in the content and prepare lists.	A hit shows where a word appears, not the intent behind it.
Recent Activity	Extract browser and system activity when the source contains it.	The logical lab does not reproduce the entire operating system.
Picture Analyzer	Review EXIF metadata for supported images and HEIC/HEIF conversions.	Metadata may be missing or may have changed.
Email Parser	Identify supported email formats and extract messages.	The sample EML is fictitious; it does not prove actual sending or receipt.
Data Source Integrity	Compare hashes of E01 files with their internal values.	It applies to that type of data source, not to just any logical folder.
PhotoRec Carver	Search for files in unallocated space.	It is not the starting module for a practice logical folder.

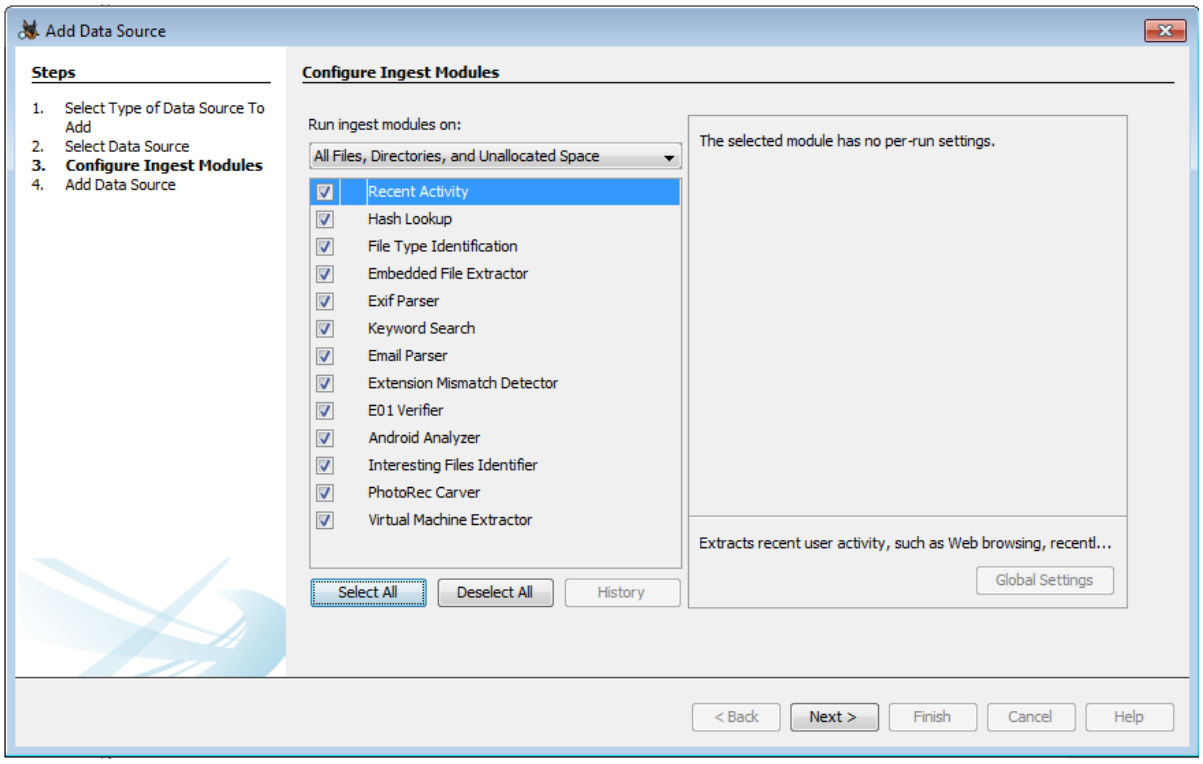


Figure 2. Selecting ingest modules when adding a data source. Screenshot from Sleuth Kit Labs, CC BY-SA 3.0.

Do not enable everything indiscriminately. More modules mean more time, more noise, and more results to interpret. The ingest process should address the question posed by the case.

You can also cancel a job, but wait for the cancellation to finish cleanly and record which modules completed their work. Partial ingestion is not equivalent to a complete examination.

5. Navigate results without losing context

The main interface has three areas: the tree on the left, the file or results list at the upper right, and the content viewer at the lower right.

- **Data Sources:** data sources added to the case.

- **Views:** the same data organized by type or another perspective.
- **Results:** results produced by ingest modules.
- **Content Viewer:** content, text, images, or hexadecimal data for the selected item.

When a result appears important, use the context menu to go to its location in the file system. A name in a list is not enough: review the folder, neighboring files, format, and process that produced it.

5.1 Search exercise: “lavanda”

In the top search box, type `lavanda`. The fictitious file `01_notas.txt` contains that word so that the exercise has a controlled result.

The correct outcome is not “the case is solved.” It is locating the file, opening it, checking the complete sentence, and recording why you selected that search. You can then tag it for inclusion in a report.

Tagging is not the same as reaching a conclusion. A tag organizes objects you want to review or export. It does not establish that they are evidence in court.

6. Use Timeline without confusing a date with intent

Open **Timeline** using the button or **Tools > Timeline**. The view lets you study events over time, but the data will be complete only after the relevant ingest modules have finished.

View	What it is for	How to use it without becoming overwhelmed
Counts	Understand how much activity occurred in each period.	Start here to identify time windows of interest.
Details	Examine related events and groups within a time window.	First narrow the period and event types.
List	View events in chronological order before and after a finding.	Use it when you already know which moment you want to contextualize.

Enable modules appropriate for your data source. Recent Activity helps with web and system activity; Picture Analyzer contributes EXIF events; Email Parser contributes messages; other modules contribute other event types. The Hash Lookup module can help hide known files if you configure the corresponding hash sets.

6.1 Time zones change interpretation

Timeline lets you view events in local time or UTC. Record which option you chose and why. For FAT images, Autopsy also requests the time zone when you add the data source because the file system does not store that information.

A timestamp is an observation, not evidence of intent. It can be affected by clock settings, copying, format, conversion, or time zone. Corroborate important events with other sources.

7. Configure translation correctly

Autopsy's machine translation uses an external Bing or Google service. You need your own account and credentials, not a key shared by this guide.

11. Open **Options > Tools > Machine Translation**.
12. Select the service authorized for your organization.
13. Enter the account information. Do not disclose it in screenshots, reports, or the shared case.
14. Click **Test** and verify that the service responds correctly.
15. If you need OCR, enable it only after installing the corresponding language packs.

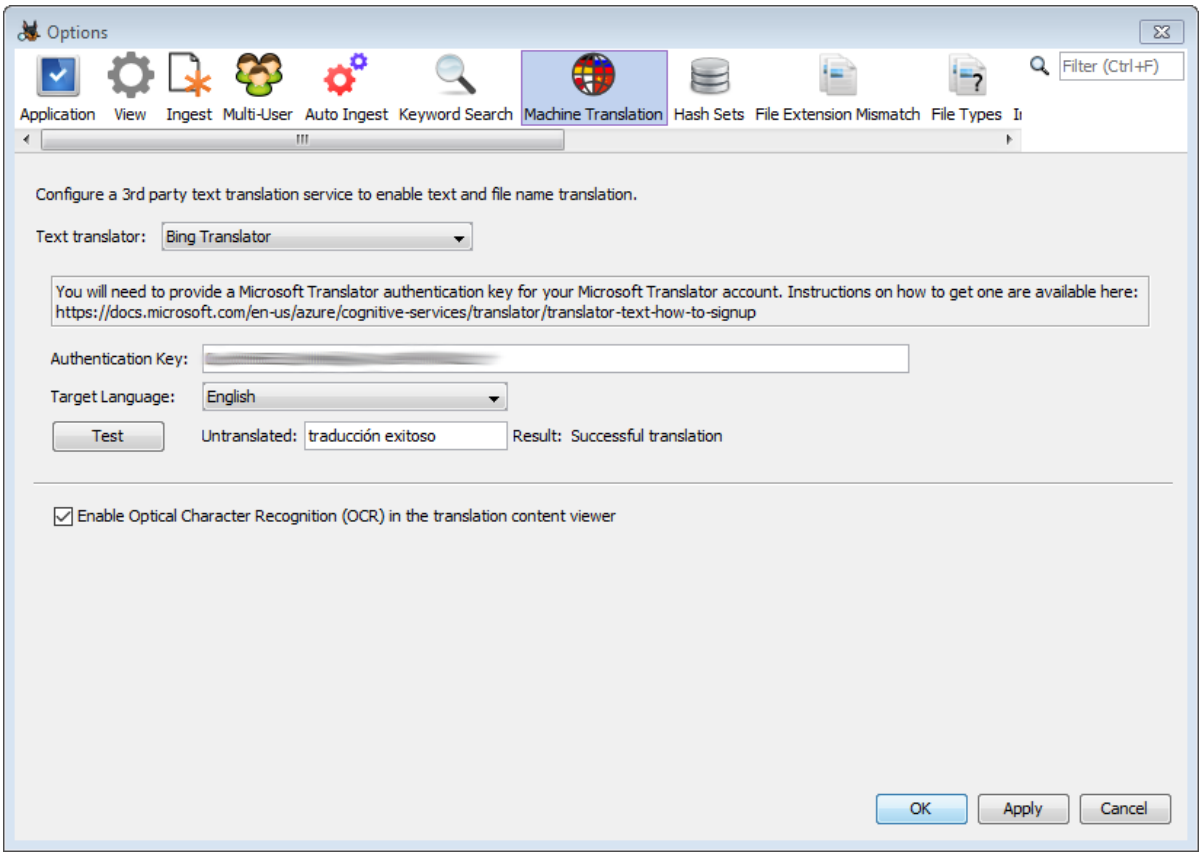


Figure 3. Machine translation configuration. The key is blurred in the official screenshot. Sleuth Kit Labs, CC BY-SA 3.0.

To translate file and folder names, open **View Options** and enable **Translate Text**. Autopsy will display the translation and retain a column called **Original Name**. This column is essential: do not replace the original name in your documentation.

For content, open the **Text > Translation** tab in the viewer. Messages also let you switch between **Original Text** and **Translated Text**.

Translation helps you read; it does not validate meaning. Check proper names, abbreviations, negations, and legal terms against the original. Before sending confidential content to an external service, verify authorization, the privacy policy, and the provider's terms.

8. Seek corroboration, not just matches

A sound investigation compares sources and explains alternatives. A recovered file may be incomplete; a match may be noise; a date may have changed during copying.

Finding	Responsible interpretation	What else to review
Keyword hit	The term appears in that content.	Complete sentence, file, location, and relationship to the case.
Image with EXIF	The file contains certain recorded fields.	Whether those fields were preserved and whether there is independent corroboration.
Deleted file	Structures exist that may allow recovery.	Whether the content is complete and whether another source confirms its meaning.
Matching hash	The object did not change between the two checks.	Which object was compared, the algorithm, date, and custody.
Missing result	It was not observed within the scope reviewed.	Available sources, filters, ingest modules, and method limitations.

Do not write "it did not exist" when all you can say is "it did not appear in this review." This distinction protects the quality of the report.

9. Generate a report that others can review

The **Generate Report** button generates reports in HTML, XLS, KML, and other formats. The **Reports** node in the tree lets you locate them later.

For an initial practice report:

16. Tag only the objects you actually need to explain.
17. Choose **Tagged Results** to avoid exporting the entire case indiscriminately.
18. Review the generated report and verify that the links work.
19. Outside the automated output, add the case context, source, versions, modules, and limitations.

An Autopsy report is not the final expert opinion. It is tool output. Professional interpretation must explain what the artifacts mean and how far the conclusion extends.

Include in your documentation:

- Case identifier and authorized scope.
- Original source and its relationship to the working copy.
- Autopsy version and modules run.
- Dates, time zone, and conversions performed.
- Hashes where applicable, identifying the object and algorithm.
- Negative results, errors, and unavailable sources.
- A limited conclusion and the alternatives considered.

10. Common problems and recovery

Problem	Likely cause	What to do
Not all disks appear	Insufficient permissions or an	Check permissions and the connection; do not connect the original without

	unrecognized device.	protection.
A segmented image will not open	A segment is missing or the first file was not selected.	Gather all segments and select the first one.
No deleted files appear in Logical Files	That method works only with allocated files.	Use the appropriate source to analyze unallocated space without altering the original.
Timeline has too many events	Filters and a specific time period have not been set.	Narrow the time window, event types, and description; do not maximize everything at the start.
Translation does not work	Credentials, service, connection or incomplete configuration.	Check the authorized account and click Test; retain the original.
The computer slows down	Multiple data sources, modules, or indexes, or security software.	Reduce the scope, check storage, and coordinate authorized exclusions; never disable security software globally.
A hash does not match	The object changed or is not the expected object.	Stop using that copy and document the incident; don't force it to match.

11. Guided exercise with fictitious files

Complete the following walkthrough using the lab ZIP file. The goal is to demonstrate that you can repeat the method, not to make an accusation.

20. Create the case `DEMO-2026-001`.
21. Add the extracted folder as **Logical Files**.
22. Run only File Type Identification, Embedded File Extraction, Keyword Search, and Picture Analyzer.
23. Record the version, date, operator, and selected modules.
24. Search for `lavanda` and open the file that contains it.
25. Review the metadata in `03_imagen_demo.png` without assuming that camera or GPS fields are present.
26. Open `02_correo_demo.eml` and confirm within the content itself that the sender uses a domain reserved for examples.
27. Use Timeline to distinguish actual system events from the lab's fictitious notes.
28. Tag only what you need to explain the exercise.
29. Generate a report of tagged items and verify its contents.

Do not treat the fictitious history as if it were a real browser export. `05_navegador/history-demo.txt` is a reading document for practicing manual timeline analysis, not a real Chrome database.

12. Glossary in plain language

Term	Practical explanation
Artifact	A piece of data produced by the system or a tool that may help answer a question.
Source	The object you choose to analyze: an image, disk, folder, virtual machine, or another collection.

Ingest	The process that applies modules to the source to extract and analyze content.
Unallocated space	An area of storage that the system is not currently using for active files.
Hash	A value used to compare content, not to establish authorship or truthfulness.
Working copy	A representation used for analysis without modifying the preserved original.
Tag	A marker used to organize objects within the case or include them in a report.
Time zone	Context that lets you interpret a date without incorrectly converting it to another time.
OCR	Optical character recognition used to extract text from images, with the possibility of errors.
Negative result	The absence of a finding within a documented scope, not proof of nonexistence.
Reproducibility	The ability for another person to repeat the procedure under documented conditions.
Limitation	Information that the source or method cannot establish.

13. Official sources and editorial checks

The reference version and paths in this guide were checked against the following documents:

30. Autopsy Download, Sleuth Kit Labs
31. Autopsy User Documentation 4.23.0: Quick Start Guide
32. Autopsy User Documentation 4.23.0: Cases
33. Autopsy User Documentation 4.23.0: Data Sources
34. Autopsy User Documentation 4.23.0: Ingest Modules
35. Autopsy User Documentation 4.23.0: Timeline
36. Autopsy User Documentation 4.23.0: Machine Translation
37. Autopsy User Documentation 4.23.0: Reporting
38. Exterro FTK Imager 8.2 User Guide
39. ISO/IEC 27037, identification, collection, acquisition, and preservation
40. NIST SP 800-86, forensic techniques in incident response

Figures 1, 2 and 3 come from that official documentation, published under the **Creative Commons Attribution-ShareAlike 3.0 United States** license. Sleuth Kit Labs is credited and the license link is retained: CC BY-SA 3.0.

This guide is an educational adaptation by Jocsan Laguna, not an official Sleuth Kit Labs publication or legal advice. The editorial version was reviewed on 15 November 2026. Before applying a feature in a real case, check the current documentation and confirm that you have the necessary authorization.