TEQUILA SO
Jocsan Laguna

Autopsy 4.23

Fälle, Ingestion, Zeitleisten, Übersetzung und Berichte

PRAXISLEITFADEN · 2026



Inhalt

Bevor Sie Beweismaterial verarbeiten 3
1. Grundprinzip: Fall, Datenquelle und Ingest 3
1.1 Erfassung ist nicht Analyse 4
2. Herunterladen und Vorbereiten der Umgebung 4
2.1 Das Original bleibt außerhalb des Arbeitsablaufs 5
3. Den ersten Fall mit dem Labor erstellen 5
4. Ingest-Module gezielt auswählen 6
5. Ergebnisse ohne Verlust des Kontexts durchsuchen 7
5.1 Suchübung: „lavanda“ 7
6. Die Zeitachse verwenden, ohne Datum und Absicht zu verwechseln 8
6.1 Die Zeitzone verändert die Interpretation 8
7. Die Übersetzung richtig konfigurieren 8
8. Nach Bestätigungen suchen, nicht nur nach Treffern 9
9. Einen Bericht erstellen, den eine andere Person nachprüfen kann 10
10. Häufige Probleme und Wiederherstellung 10
11. Geführte Übung mit fiktiven Dateien 11
12. Glossar in einfacher Sprache 12
13. Offizielle Quellen und redaktionelle Kontrolle 12

Maschinell unterstützte Übersetzung der spanischen Ausgabe. Redaktionelle Referenz ist das spanische Original.

Dieser Leitfaden erklärt Autopsy so, wie es in einer ersten Laborsitzung erklärt würde: wozu die Plattform dient, wie sie mit Daten arbeitet und wie ihre Ergebnisse überprüft werden. Ingenieurkenntnisse sind nicht erforderlich, wohl aber ein methodisches Vorgehen. Die Autorisierung steht immer vor dem Werkzeug.

Die Referenzversion ist **Autopsy 4.23.0**. Menübezeichnungen und Funktionen können in späteren Versionen abweichen. Die Bildschirmfotos stammen aus der offiziellen Dokumentation von Sleuth Kit Labs und sind bei den jeweiligen Abbildungen gekennzeichnet.

Bevor Sie Beweismaterial verarbeiten

Autopsy ist eine Plattform für die digitale Forensik. Sie ermöglicht es, einen Fall anzulegen, Datenquellen hinzuzufügen, Analysemodule auszuführen, Artefakte zu prüfen, Ereignisse zeitlich einzuordnen und Berichte zu erstellen. Eine Datei wird dadurch nicht zu einem authentischen Beweis, und die Plattform entscheidet nicht, wer recht hat.

Arbeiten Sie ausschließlich mit eigenem Material, mit Material, zu dessen Nutzung Sie berechtigt sind, oder mit für Lernzwecke veröffentlichtem Material. Bewahren Sie das Original auf und verwenden Sie eine Arbeitskopie. Wenn ein echter Datenträger erfasst werden soll, prüfen Sie zunächst das Verfahren zur Erfassung und den Schreibschutz; Autopsy nimmt Ihnen diese Verantwortung nicht ab.

Das herunterladbare Labor zu diesem Leitfaden enthält ausschließlich fiktive Dateien. Es stellt weder einen realen Fall noch ein reales Gespräch dar und ist auch kein gerichtliches Beweismaterial. Es dient dazu, die Benutzeroberfläche zu üben und Arbeitsschritte zu dokumentieren, nicht, Rückschlüsse auf Personen zu ziehen.

1. Grundprinzip: Fall, Datenquelle und Ingest

Autopsy strukturiert die Arbeit anhand dreier Begriffe, die von Anfang an zu unterscheiden sind.

Begriff	Einfach erklärt	Fehler, der vermieden wird
Fall	Der Arbeitsordner mit den Einstellungen, der Datenbank und den Berichten.	Anzunehmen, der Fall bestehe nur aus dem erhaltenen Datenträger.
Datenquelle	Das zu untersuchende Objekt: ein Datenträger, ein Image, eine virtuelle Maschine, ein Ordner oder eine logische Dateisammlung.	Beliebige Inhalte hinzufügen, ohne Herkunft und Umfang zu kennen.
Ingest	Die Module, die diese Datenquelle analysieren und Artefakte zur Prüfung erzeugen.	Anzunehmen, dass das Öffnen eines Images bereits einer Analyse entspricht.

Eine Datenquelle ist keine Schlussfolgerung. Eine Datei mit einem Datum kann ein vom System aufgezeichnetes Ereignis beschreiben, beweist für sich allein jedoch nicht, wer sie erstellt hat, welche Absicht dahinterstand oder ob die Systemzeit korrekt war.

1.1 Erfassung ist nicht Analyse

FTK Imager dient hauptsächlich zur Erfassung und Vorschau. Autopsy dient zur Analyse und Organisation des Falls. Sie können mit FTK Imager ein Image erstellen und es anschließend in Autopsy einbinden; alternativ können Sie zur Übung logische Dateien zu Autopsy hinzufügen.

Frage	Geeignetes Werkzeug	Erwartetes Ergebnis
Ich muss eine forensische Kopie des Datenträgers erstellen.	FTK Imager, mit geeigneten Maßnahmen zur Aufbewahrung und zum Schreibschutz.	Ein dokumentiertes und verifiziertes Image.
Ich muss Dateien, Aktivitäten, Metadaten und die Chronologie prüfen.	Autopsy.	Artefakte, Suchabfragen, Tags und ein Analysebericht.
Ich muss bestimmte Metadaten aus einem Foto auslesen.	ExifTool.	In dieser Datei vorhandene Felder, kein automatischer Beweis von Ort oder Urheberschaft.
Ich muss ein Speicherabbild untersuchen.	Volatility 3.	Prozesse, Verbindungen und andere in diesem Speicherabbild enthaltene Artefakte.

Installieren Sie nicht zuerst sämtliche Programme. Formulieren Sie zunächst die Frage: Was möchten Sie nachweisen, mit welcher Datenquelle und mit der geringstmöglichen Veränderung?

2. Herunterladen und Vorbereiten der Umgebung

Laden Sie Autopsy von der offiziellen Website herunter: autopsy.com/download. Die Seite unterscheidet Windows-Installationsprogramme für 32 und 64 Bit, Pakete für Linux/macOS und GPG-Signaturdateien. Laden Sie das Installationsprogramm nicht von einer Software-Sammelseite herunter.

Die Installationsdokumentation ist unter sleuthkit.org/autopsy/docs/user-docs/4.23.0/installation_page.html verfügbar.

1. Prüfen Sie die Architektur des Computers und die heruntergeladene Datei.
2. Überprüfen Sie die Signatur oder die vom Projekt bereitgestellten Integritätsinformationen, sofern verfügbar.
3. Installieren Sie die Software auf einer kontrollierten Arbeitsstation, nicht auf dem Computer mit dem Originalbeweismaterial.
4. Halten Sie drei Speicherorte getrennt: aufbewahrte Datenquelle, Fallordner und Ausgabe- bzw. Berichtsordner.
5. Wenn Sie physische Datenträger untersuchen, führen Sie Autopsy mit den erforderlichen Berechtigungen und einer schreibgeschützten Datenquelle aus. Erhöhte Berechtigungen sind keine Rechtfertigung für ein unkontrolliertes Vorgehen.

Eine mögliche Laborstruktur, keine verbindliche Pfadangabe, sieht wie folgt aus:

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

Speichern Sie das Original-Image nicht im Fallordner, als handele es sich dabei um eine Sicherungskopie. Die Datenquelle muss während der Analyse zugänglich bleiben: Autopsy speichert lediglich einen Verweis darauf, keine vollständige Kopie im Fall.

2.1 Das Original bleibt außerhalb des Arbeitsablaufs

Bevor Sie eine echte Datenquelle hinzufügen, dokumentieren Sie, wer sie bereitgestellt hat, warum Sie sie untersuchen dürfen, ihre Kennung, ihren Zustand und gegebenenfalls ihren Hashwert. Bei einem fragmentierten Image wählen Sie die erste Datei des Satzes aus und bewahren alle Segmente gemeinsam auf.

Ein Bildschirmfoto oder ein Export aus Autopsy ersetzt nicht die Originaldatei. Es handelt sich um eine Darstellung zum besseren Verständnis, nicht um das vollständige Beweismaterial.

3. Den ersten Fall mit dem Labor erstellen

Öffnen Sie Autopsy und wählen Sie **Create New Case**. Vergeben Sie einen Namen, der keine Kundendaten offenlegt, beispielsweise `DEMO-2026-001`, und wählen Sie einen noch nicht vorhandenen Ordner aus. Fügen Sie anschließend die Datenquelle hinzu.

6. Wählen Sie im Assistenten **Logical Files** für das Labor aus.
7. Klicken Sie auf **Add** und wählen Sie den entpackten Ordner des fiktiven Labors aus.
8. Vergewissern Sie sich, dass der Ordner ausschließlich die Demonstrationsdateien enthält.
9. Behalten Sie den Namen der logischen Sammlung bei oder ändern Sie ihn in eine verständliche Bezeichnung, etwa `DEMO-archivos`.
10. Fahren Sie mit den Ingest-Einstellungen fort.

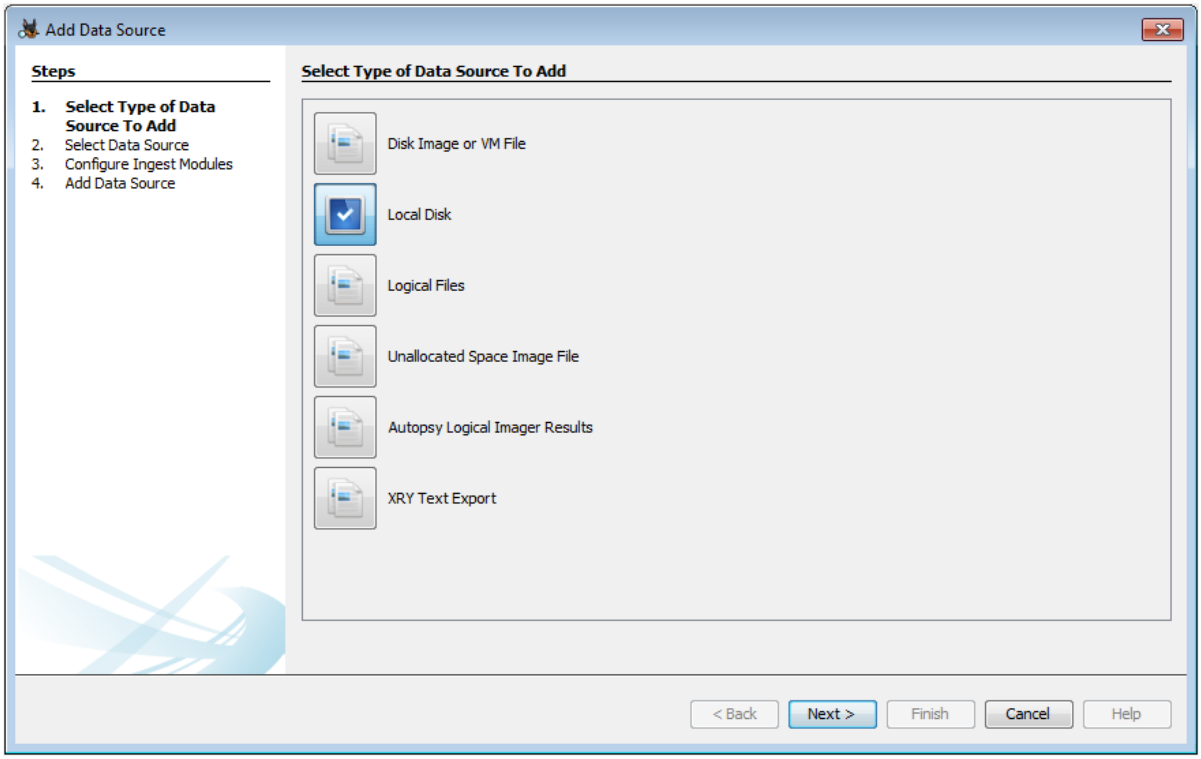


Abbildung 1. Der Assistent ermöglicht die Auswahl zwischen Image, lokalem Datenträger, logischen Dateien und anderen Datenquellen. Bildschirmfoto von Sleuth Kit Labs, CC BY-SA 3.0.

Warum logische Dateien verwenden? Sie ermöglichen es, die Benutzeroberfläche kennenzulernen, ohne einen Beweisdatenträger anzuschließen. Die Dokumentation weist darauf hin, dass diese Methode weder

nicht zugewiesenen Speicherplatz noch gelöschte Dateien auf dem Gerät untersucht; sie verarbeitet nur die ausgewählten allokierten Dateien. Erwarten Sie in dieser Übung keine Wiederherstellung gelöschter Dateien.

Auch bei den Datumsangaben logischer Dateien ist Vorsicht geboten. Autopsy kann die Zeitstempel ignorieren, weil sich diese beim Kopieren der Dateien auf Ihren Computer verändert haben. Das ist kein Programmfehler, sondern eine Einschränkung, die Sie ausweisen müssen.

4. Ingest-Module gezielt auswählen

Ingest-Module analysieren den Inhalt der Datenquelle. Sie laufen im Hintergrund, und ihre Ergebnisse werden nach und nach verfügbar. Sie können Dateien währenddessen prüfen, dürfen eine noch laufende Analyse jedoch nicht als abgeschlossen darstellen.

Beginnen Sie im Labor mit einer kleinen Auswahl:

Modul	**Wofür Sie es in dieser Übung einsetzen würden**	**Was Sie beachten sollten**
File Type Identification	Dateitypen anhand ihrer Signatur erkennen, nicht nur anhand der Erweiterung.	Die Signatur hilft bei der Identifizierung des Formats, nicht bei der Beurteilung der Authentizität des Inhalts.
Extension Mismatch Detector	Erweiterungen erkennen, die nicht zum ermittelten Dateityp passen.	Eine Abweichung erfordert eine Prüfung, keine automatische Anschuldigung.
Embedded File Extraction	Container wie ZIP- und Office-Dokumente öffnen und ihren Inhalt verarbeiten.	Eine extrahierte Datei ist ein Derivat; die Verbindung zu ihrer Herkunft muss erhalten bleiben.
Keyword Search	Wörter im Inhalt finden und Listen erstellen.	Ein Treffer zeigt, wo ein Wort vorkommt, nicht welche Absicht dahintersteht.
Recent Activity	Browser- und Systemaktivitäten extrahieren, sofern sie in der Datenquelle enthalten sind.	Das logische Labor bildet nicht das gesamte Betriebssystem ab.
Picture Analyzer	EXIF-Metadaten kompatibler Bilder und HEIC/HEIF-Konvertierungen prüfen.	Metadaten können fehlen oder verändert worden sein.
Email Parser	Unterstützte E-Mail-Formate erkennen und Nachrichten extrahieren.	Die Beispiel-EML-Datei ist fiktiv; sie beweist weder einen tatsächlichen Versand noch einen tatsächlichen Empfang.
Data Source Integrity	Hashwerte von E01-Dateien mit ihren internen Werten vergleichen.	Gilt für diese Art von Datenquelle, nicht für beliebige logische Ordner.
PhotoRec Carver	Dateien in nicht zugewiesenem Speicherplatz suchen.	Nicht das Modul der ersten Wahl für einen logischen Übungsordner.

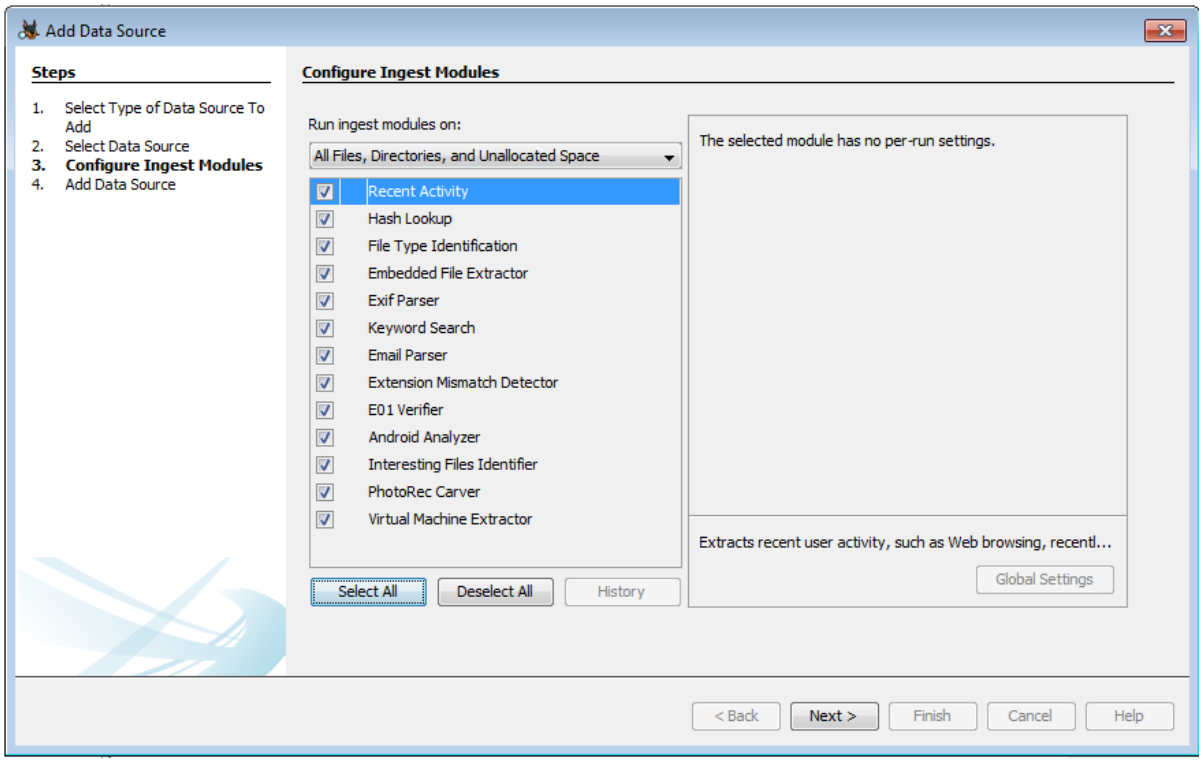


Abbildung 2. Auswahl der Ingest-Module beim Hinzufügen einer Datenquelle. Bildschirmfoto von Sleuth Kit Labs, CC BY-SA 3.0.

Aktivieren Sie nicht grundlos alle Module. Mehr Module bedeuten mehr Zeit, mehr Rauschen und mehr Ergebnisse, die interpretiert werden müssen. Der Ingest muss der Fragestellung des Falls dienen.

Sie können eine Aufgabe auch abbrechen; warten Sie jedoch den ordnungsgemäßen Abbruch ab und dokumentieren Sie, welche Module ihre Arbeit abgeschlossen haben. Ein partieller Ingest entspricht keiner vollständigen Untersuchung.

5. Ergebnisse ohne Verlust des Kontexts durchsuchen

Die Hauptoberfläche besteht aus drei Bereichen: dem Baum links, der Datei- bzw. Ergebnisliste rechts oben und der Inhaltsanzeige rechts unten.

- **Data Sources:** zum Fall hinzugefügte Datenquellen.
- **Views:** dieselben Daten, nach Typ oder einer anderen Perspektive geordnet.
- **Results:** von den Ingest-Modulen erzeugte Ergebnisse.
- **Content Viewer:** Inhalt, Text, Bild oder Hexadezimaldaten des ausgewählten Elements.

Wenn ein Ergebnis wichtig erscheint, öffnen Sie über das Kontextmenü seinen Speicherort im Dateisystem. Ein Name in einer Liste genügt nicht: Prüfen Sie den Ordner, benachbarte Dateien, das Format und den Prozess, der das Element erzeugt hat.

5.1 Suchübung: „lavanda“

Geben Sie im oberen Suchfeld `lavanda` ein. Die fiktive Datei `01_notas.txt` enthält dieses Wort, damit die Übung ein kontrolliertes Ergebnis liefert.

Das richtige Ergebnis lautet nicht „der Fall ist gelöst“. Ziel ist es, die Datei zu finden, zu öffnen, den vollständigen Satz zu prüfen und zu dokumentieren, warum diese Suchanfrage gewählt wurde. Anschließend können Sie die Datei mit einem Tag versehen, um sie in einen Bericht aufzunehmen.

Eine Markierung ist keine Schlussfolgerung. Mit einem Tag organisieren Sie Objekte, die Sie prüfen oder exportieren möchten. Dadurch werden diese Objekte nicht zu gerichtlichen Beweismitteln.

6. Die Zeitachse verwenden, ohne Datum und Absicht zu verwechseln

Öffnen Sie **Timeline** über die Schaltfläche oder über **Tools > Timeline**. Die Ansicht ermöglicht die zeitliche Untersuchung von Ereignissen; die Daten sind jedoch erst vollständig, wenn die relevanten Ingest-Vorgänge abgeschlossen sind.

Ansicht	Wofür sie dient	Nutzung ohne Informationsüberflutung
Counts	Nachvollziehen, wie viel Aktivität in einem Zeitraum vorliegt.	Beginnen Sie hier, um relevante Zeitfenster zu finden.
Details	Ereignisse und zusammenhängende Gruppen innerhalb eines Zeitfensters untersuchen.	Begrenzen Sie zunächst den Zeitraum und die Ereignistypen.
List	Chronologisch geordnete Ereignisse vor und nach einem Fund anzeigen.	Verwenden Sie diese Ansicht, wenn Sie den zu kontextualisierenden Zeitpunkt bereits kennen.

Aktivieren Sie geeignete Module für Ihre Datenquelle. Recent Activity unterstützt die Analyse von Web- und Systemaktivitäten; Picture Analyzer liefert EXIF-Ereignisse; Email Parser liefert Nachrichten; andere Module liefern weitere Ereignistypen. Das Modul Hash Lookup kann helfen, bekannte Dateien auszublenden, wenn Sie die entsprechenden Hash-Sets konfigurieren.

6.1 Die Zeitzone verändert die Interpretation

Timeline ermöglicht die Anzeige von Ereignissen in lokaler Zeit oder UTC. Dokumentieren Sie Ihre Wahl und ihre Begründung. Bei FAT-Images fragt Autopsy die Zeitzone bereits beim Hinzufügen der Datenquelle ab, weil das Dateisystem diese Information nicht speichert.

Ein Zeitstempel ist eine Beobachtung, keine Absicht. Er kann durch die Uhreneinstellung, das Kopieren, das Format, die Konvertierung oder die Zeitzone beeinflusst sein. Bestätigen Sie wichtige Ereignisse mit anderen Datenquellen.

7. Die Übersetzung richtig konfigurieren

Die maschinelle Übersetzung von Autopsy nutzt einen externen Dienst von Bing oder Google. Sie benötigen ein eigenes Konto und eigene Anmeldedaten; dieser Leitfaden stellt keinen gemeinsam genutzten Schlüssel bereit.

11. Öffnen Sie **Options > Tools > Machine Translation**.
12. Wählen Sie den für Ihre Organisation zugelassenen Dienst aus.
13. Geben Sie die Kontoinformationen ein. Veröffentlichen Sie diese nicht in Bildschirmfotos oder Berichten und speichern Sie sie nicht im gemeinsam genutzten Fall.

14. Klicken Sie auf **Test** und prüfen Sie, ob der Dienst ordnungsgemäß antwortet.
15. Falls Sie OCR benötigen, aktivieren Sie es nur, wenn die entsprechenden Sprachpakete installiert sind.

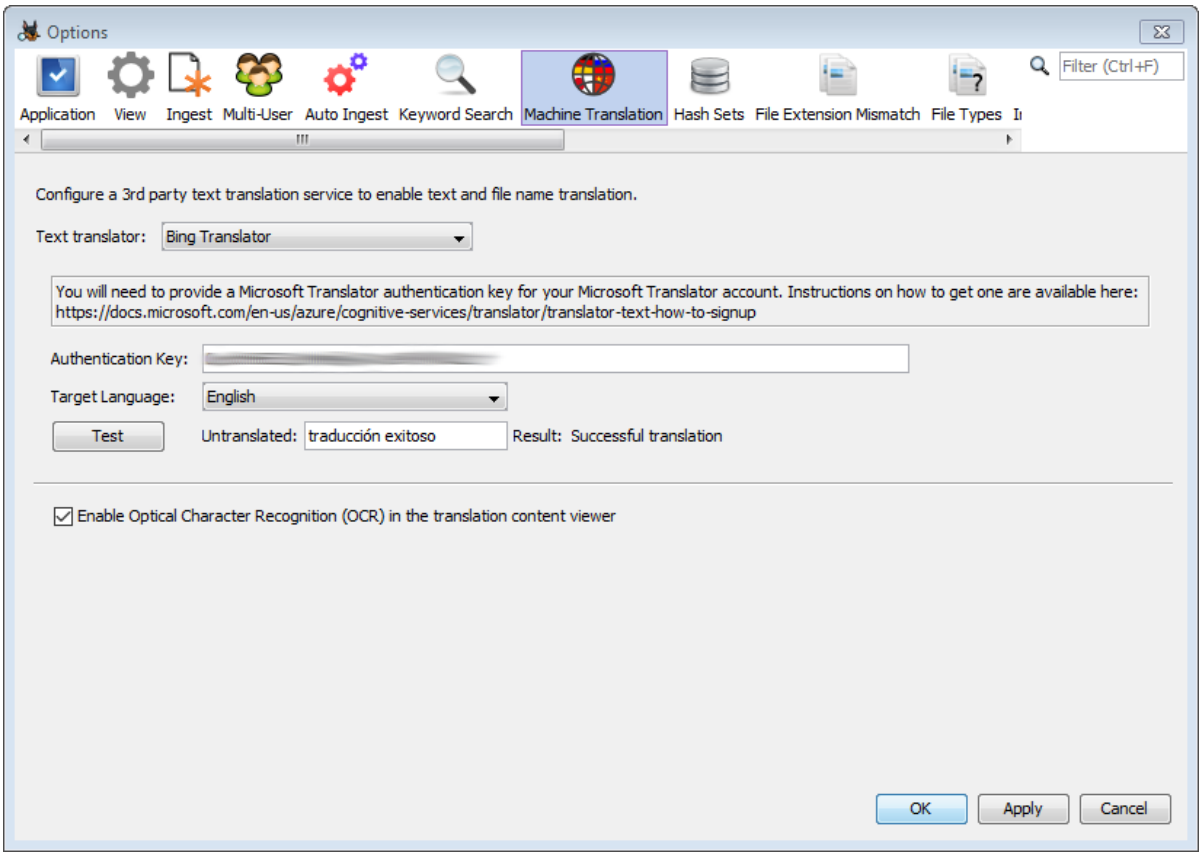


Abbildung 3. Konfiguration der maschinellen Übersetzung. Der Schlüssel ist im offiziellen Bildschirmfoto unkenntlich gemacht. Sleuth Kit Labs, CC BY-SA 3.0.

Um Datei- und Ordnernamen zu übersetzen, öffnen Sie **View Options** und aktivieren Sie **Translate Text**. Autopsy zeigt die Übersetzung an und behält eine Spalte mit der Bezeichnung **Original Name** bei. Diese Spalte ist unverzichtbar: Ersetzen Sie den Originalnamen in Ihrer Dokumentation nicht.

Öffnen Sie für den Inhalt im Viewer die Registerkarte **Text > Translation**. Bei Nachrichten können Sie ebenfalls zwischen **Original Text** und **Translated Text** wechseln.

Die Übersetzung erleichtert das Lesen, bestätigt aber nicht die Bedeutung. Prüfen Sie Eigennamen, Abkürzungen, Verneinungen und juristische Begriffe anhand des Originals. Bevor Sie vertrauliche Inhalte an einen externen Dienst übermitteln, klären Sie die Autorisierung, die Datenschutzrichtlinie und die Nutzungsbedingungen des Anbieters.

8. Nach Bestätigungen suchen, nicht nur nach Treffern

Eine fundierte Untersuchung vergleicht Datenquellen und erläutert alternative Erklärungen. Eine wiederhergestellte Datei kann unvollständig sein; ein Treffer kann Rauschen sein; ein Datum kann sich beim Kopieren verändert haben.

Fund	Verantwortungsvolle Interpretation	Was außerdem geprüft werden sollte
Gefundenes Schlüsselwort	Der Begriff kommt in diesem Inhalt vor.	Vollständiger Satz, Datei, Speicherort und Bezug zum Fall.

Bild mit EXIF-Daten	Die Datei enthält bestimmte Metadatenfelder.	Ob diese Felder erhalten geblieben sind und ob eine unabhängige Bestätigung vorliegt.
Gelöschte Datei	Vorhandene Strukturen ermöglichen einen Wiederherstellungsversuch.	Ob der Inhalt vollständig ist und eine andere Datenquelle seine Bedeutung bestätigt.
Übereinstimmender Hashwert	Das Objekt blieb zwischen den beiden Prüfungen unverändert.	Verglichenes Objekt, Algorithmus, Datum und Beweismittelkette.
Ausbleibendes Ergebnis	Innerhalb des untersuchten Umfangs wurde nichts beobachtet.	Verfügbare Datenquellen, Filter, Ingest-Vorgänge und Grenzen der Methode.

Formulieren Sie nicht „es existierte nicht“, wenn Sie nur sagen können „es wurde bei dieser Prüfung nicht gefunden“. Diese Unterscheidung sichert die Qualität des Berichts.

9. Einen Bericht erstellen, den eine andere Person nachprüfen kann

Über die Schaltfläche **Generate Report** können Berichte in den Formaten HTML, XLS, KML und weiteren Formaten erstellt werden. Über den Knoten **Reports** im Baum können sie später aufgefunden werden.

Für einen ersten Übungsbericht:

16. Versehen Sie nur die tatsächlich zu erläuternden Objekte mit Tags.
17. Wählen Sie **Tagged Results**, damit nicht der gesamte Fall ohne Auswahlkriterien exportiert wird.
18. Prüfen Sie den erstellten Bericht und stellen Sie sicher, dass die Links funktionieren.
19. Ergänzen Sie außerhalb der automatisch erzeugten Ausgabe den Kontext des Falls, die Datenquelle, die Versionen, die Module und die Einschränkungen.

Der Autopsy-Bericht ist nicht das abschließende Gutachten. Er ist eine Werkzeugausgabe. Die fachliche Interpretation muss erläutern, was die Artefakte bedeuten und wie weit die Schlussfolgerung reicht.

Ihre Dokumentation sollte Folgendes enthalten:

- Fallkennung und autorisierter Umfang.
- Originalquelle und ihr Bezug zur Arbeitskopie.
- Version von Autopsy und ausgeführte Module.
- Datumsangaben, Zeitzone und vorgenommene Konvertierungen.
- Gegebenenfalls Hashwerte mit Angabe von Objekt und Algorithmus.
- Negative Ergebnisse, Fehler und nicht verfügbare Datenquellen.
- Begrenzte Schlussfolgerung und berücksichtigte Alternativen.

10. Häufige Probleme und Wiederherstellung

Problem	Wahrscheinliche Ursache	Vorgehen
Nicht alle Datenträger werden angezeigt	Unzureichende Berechtigungen oder ein nicht erkanntes Gerät.	Prüfen Sie Berechtigungen und Verbindung; schließen Sie das Original nicht ungeschützt an.
Ein fragmentiertes Image wird nicht	Ein Segment fehlt oder die erste Datei	Führen Sie alle Segmente zusammen und

geöffnet	wurde nicht ausgewählt.	wählen Sie die erste Datei aus.
In Logical Files werden keine gelöschten Dateien angezeigt	Diese Methode verarbeitet nur allokierte Dateien.	Verwenden Sie eine geeignete Datenquelle, um nicht zugewiesenen Speicherplatz zu analysieren, ohne das Original zu verändern.
Timeline enthält zu viele Ereignisse	Fehlende Filter und ein nicht abgegrenzter Zeitraum.	Grenzen Sie Zeitfenster, Ereignistypen und Beschreibungen ein; zeigen Sie nicht von Anfang an alles gleichzeitig an.
Die Übersetzung funktioniert nicht	Probleme mit Anmeldedaten, Dienst oder Verbindung oder eine unvollständige Konfiguration.	Prüfen Sie das autorisierte Konto und klicken Sie auf Test; bewahren Sie das Original auf.
Der Computer wird langsamer	Viele Datenquellen, Module, Indizes oder Sicherheitssoftware.	Reduzieren Sie den Umfang, prüfen Sie den Speicher und koordinieren Sie autorisierte Ausnahmen, statt Sicherheitsfunktionen global zu deaktivieren.
Ein Hashwert stimmt nicht überein	Das Objekt wurde verändert oder ist nicht das erwartete Objekt.	Verwenden Sie diese Kopie nicht weiter und dokumentieren Sie die Abweichung; erzwingen Sie keine Übereinstimmung.

11. Geführte Übung mit fiktiven Dateien

Führen Sie den folgenden Ablauf mit der ZIP-Datei des Labors durch. Ziel ist zu zeigen, dass Sie die Methode wiederholen können, nicht, eine Anschuldigung zu formulieren.

20. Erstellen Sie den Fall `DEMO-2026-001`.
21. Fügen Sie den entpackten Ordner als **Logical Files** hinzu.
22. Führen Sie nur File Type Identification, Embedded File Extraction, Keyword Search und Picture Analyzer aus.
23. Dokumentieren Sie Version, Datum, Bearbeiter und ausgewählte Module.
24. Suchen Sie nach `lavanda` und öffnen Sie die Datei, die dieses Wort enthält.
25. Prüfen Sie die Metadaten von `03_imagen_demo.png`, ohne das Vorhandensein von Kamera- oder GPS-Feldern anzunehmen.
26. Öffnen Sie `02_correo_demo.eml` und bestätigen Sie anhand des Inhalts, dass der Absender eine für Beispiele reservierte Domain verwendet.
27. Verwenden Sie Timeline, um tatsächliche Systemereignisse von den fiktiven Notizen des Labors zu unterscheiden.
28. Versehen Sie nur die Elemente mit Tags, die Sie zur Erläuterung der Übung benötigen.
29. Erstellen Sie einen Bericht über die markierten Elemente und überprüfen Sie seinen Inhalt.

Verwenden Sie den fiktiven Verlauf nicht wie einen echten Browserexport. `05_navegador/history-demo.txt` ist ein Lesedokument für Übungen zur manuellen Chronologie, keine echte Chrome-Datenbank.

12. Glossar in einfacher Sprache

Begriff	Praktische Erklärung
Artefakt	Ein vom System oder einem Werkzeug erzeugtes Datenelement, das zur Beantwortung einer Frage nützlich sein kann.
Datenquelle	Das Objekt, das Sie für die Analyse auswählen: ein Image, ein Datenträger, ein Ordner, eine virtuelle Maschine oder eine andere Sammlung.
Ingest	Prozess, der Module auf diese Datenquelle anwendet, um Inhalte zu extrahieren und zu analysieren.
Nicht zugewiesener Speicherplatz	Bereich des Speichers, den das System derzeit nicht für aktive Dateien verwendet.
Hashwert	Wert zum Vergleichen von Inhalten, nicht zum Beweisen von Urheberschaft oder Wahrheitsgehalt.
Arbeitskopie	Repräsentation, die für die Analyse verwendet wird, ohne das aufbewahrte Original zu verändern.
Tag	Markierung zur Organisation von Objekten innerhalb des Falls oder zur Aufnahme in einen Bericht.
Zeitzone	Kontext, der die Interpretation eines Datums ermöglicht, ohne es fehlerhaft in eine andere Uhrzeit umzurechnen.
OCR	Optische Zeichenerkennung zur Gewinnung von Text aus Bildern; Fehler sind möglich.
Negatives Ergebnis	Fehlender Fund innerhalb eines dokumentierten Umfangs, kein Beweis des Nichtvorhandenseins.
Reproduzierbarkeit	Möglichkeit, dass eine andere Person das Verfahren unter dokumentierten Bedingungen wiederholen kann.
Einschränkung	Information, deren Nachweis die Datenquelle oder die Methode nicht zulässt.

13. Offizielle Quellen und redaktionelle Kontrolle

Die Referenzversion und die in diesem Leitfaden genannten Pfade wurden anhand der folgenden Dokumente geprüft:

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, Identifizierung, Sammlung, Erfassung und Erhaltung

40. NIST SP 800-86, forensische Verfahren bei der Reaktion auf Vorfälle

Die Abbildungen 1, 2 und 3 stammen aus dieser offiziellen Dokumentation, die unter der Lizenz **Creative Commons Attribution-ShareAlike 3.0 United States** veröffentlicht wurde. Die Nennung von Sleuth Kit Labs und der Lizenzlink bleiben erhalten: CC BY-SA 3.0.

Dieser Leitfaden ist eine didaktische Adaptation von Jocsan Laguna, keine offizielle Veröffentlichung von Sleuth Kit Labs und keine Rechtsberatung. Die redaktionelle Fassung wurde am 15. November 2026 geprüft. Bevor Sie eine Funktion in einem realen Fall einsetzen, prüfen Sie die aktuelle Dokumentation und die zuständige Stelle.