

TEQUILA SO

Jocsan Laguna

Autopsy 4.23

केस, इनजेस्ट, समयरेखा, अनुवाद और रिपोर्ट

व्यावहारिक मार्गदर्शिका · 2026

विषय-सूची

साक्ष्य को छूने से पहले 3
1. मूल अवधारणा: केस, स्रोत और इनजेस्ट 3
1.1 अधिग्रहण करना विश्लेषण नहीं है 3
2. डाउनलोड और पर्यावरण की तैयारी 4
2.1 मूल कार्यप्रवाह से बाहर रहता है 4
3. प्रयोगशाला के साथ पहला केस बनाना 5
4. उद्देश्य के अनुसार इनजेस्ट मॉड्यूल चुनना 5
5. संदर्भ खोए बिना परिणामों में नेविगेट करना 7
5.1 खोज-अभ्यास: “lavanda” 7
6. कालक्रम उपयोग करें, पर तारीख को इरादा न समझें 7
6.1 समयक्षेत्र व्याख्या बदल देता है 8
7. अनुवाद को सही ढंग से कॉन्फ़िगर करें 8
8. केवल मिलान नहीं, स्वतंत्र पुष्टि खोजें 9
9. ऐसी रिपोर्ट बनाना जिसकी दूसरा व्यक्ति समीक्षा कर सके 9
10. सामान्य समस्याएँ और पुनर्प्राप्ति 10
11. काल्पनिक फ़ाइलों के साथ निर्देशित अभ्यास 10
12. सरल भाषा में शब्दावली 11
13. आधिकारिक स्रोत और संपादकीय नियंत्रण 11

यह स्पेनिश संस्करण से मशीन-सहायित अनुवाद है। संपादकीय संदर्भ के लिए स्पेनिश मूल देखें।

यह मार्गदर्शिका Autopsy को वैसे समझाती है जैसे प्रयोगशाला के पहले सत्र में समझाया जाता है: यह किस काम आता है, डेटा के साथ क्या करता है और उसके परिणामों की समीक्षा कैसे करें। इसके लिए इंजीनियर होना आवश्यक नहीं, लेकिन सही कार्यविधि आवश्यक है। उपकरण से पहले हमेशा अधिकार और अनुमति आती है।

संदर्भ संस्करण **Autopsy 4.23.0** है। बाद के संस्करणों में मेनू के नाम और फ़ंक्शन बदल सकते हैं। स्क्रीनशॉट Sleuth Kit Labs के आधिकारिक दस्तावेज़ों से लिए गए हैं और प्रत्येक चित्र के साथ उनका श्रेय दिया गया है।

साक्ष्य को छूने से पहले

Autopsy डिजिटल फोरेंसिक विश्लेषण का प्लेटफ़ॉर्म है। इससे केस तैयार किया जा सकता है, स्रोत जोड़े जा सकते हैं, विश्लेषण मॉड्यूल चलाए जा सकते हैं, आर्टिफ़ैक्ट देखे जा सकते हैं, घटनाओं को समयक्रम में रखा जा सकता है और रिपोर्ट बनाई जा सकती हैं। यह किसी फ़ाइल को अपने आप प्रमाणित साक्ष्य नहीं बनाता और न यह तय करता है कि कौन सही है।

केवल अपनी, अधिकृत या सीखने के लिए प्रकाशित सामग्री पर काम करें। मूल को संरक्षित रखें और कार्य-प्रति उपयोग करें। यदि वास्तविक डिस्क प्राप्त करनी है, तो पहले अधिग्रहण-प्रक्रिया और राइट-ब्लॉकिंग समझें; Autopsy इस उत्तरदायित्व को समाप्त नहीं करता।

इस मार्गदर्शिका के साथ मिलने वाली डाउनलोड योग्य प्रयोगशाला में केवल काल्पनिक फ़ाइलें हैं। यह किसी वास्तविक केस, वार्तालाप या न्यायिक साक्ष्य का प्रतिनिधित्व नहीं करती। इसका उद्देश्य इंटरफ़ेस का अभ्यास और चरणों का दस्तावेज़ीकरण है, व्यक्तियों के बारे में निष्कर्ष निकालना नहीं।

1. मूल अवधारणा: केस, स्रोत और इनजेस्ट

Autopsy काम को तीन अवधारणाओं में व्यवस्थित करता है, जिन्हें शुरू से अलग समझना चाहिए।

अवधारणा	इसे सरल भाषा में कैसे समझाया जाए	जिस ग़लती से बचा जाता है
केस	कार्य-फ़ोल्डर जिसमें कॉन्फ़िगरेशन, डेटाबेस और रिपोर्ट सहेजी जाती हैं।	यह सोचना कि केस केवल प्राप्त डिस्क है।
डेटा स्रोत	वह डिस्क, इमेज, वर्चुअल मशीन, फ़ोल्डर या फ़ाइलों का लॉजिकल सेट जिसकी जाँच की जाएगी।	मूल और दोहरी जानकारी कुछ भी जोड़ना।
इनजेस्ट	वे मॉड्यूल जो स्रोत का विश्लेषण करके समीक्षा के लिए आर्टिफ़ैक्ट बनाते हैं।	यह मानना कि इमेज खोलना ही उसका विश्लेषण करना है।

स्रोत निष्कर्ष नहीं है। दिनांक वाली फ़ाइल सिस्टम में दर्ज घटना का वर्णन कर सकती है, लेकिन अकेले यह साबित नहीं करती कि उसे किसने बनाया, क्या इरादा था या घड़ी का समय सही था।

1.1 अधिग्रहण करना विश्लेषण नहीं है

FTK Imager का उपयोग मुख्यतः अधिग्रहण और पूर्वावलोकन के लिए होता है। Autopsy का उपयोग केस का विश्लेषण और व्यवस्थापन के लिए होता है। FTK Imager से इमेज बनाकर बाद में Autopsy में जोड़ सकते हैं, या अभ्यास के लिए Autopsy में लॉजिकल फ़ाइलें जोड़ सकते हैं।

प्रश्न	उपयुक्त उपकरण	अपेक्षित परिणाम
मुझे डिस्क का एक फ़ोरेंसिक कॉपी बनाने की आवश्यकता है।	FTK Imager, जिसमें सत्यापन और राइट-ब्लॉकिंग के साथ।	एक प्रलेखित और सत्यापित छवि।
मुझे फ़ाइल, गतिविधि, मेटाडेटा और कालक्रम देखने हैं।	Autopsy.	आर्टिफ़ैक्ट, खोज, टैग और विश्लेषण रिपोर्ट।
मुझे एक तस्वीर से विशिष्ट मेटाडेटा पढ़ने की आवश्यकता है।	ExifTool	उस फ़ाइल में मौजूद फ़ील्ड, स्थान या फ़ोटो लेने वाले का स्वतः प्रमाण नहीं।
मुझे एक मेमोरी कैप्चर की जाँच करने की आवश्यकता है।	Volatility 3	उस कैप्चर में मौजूद प्रोसेस, कनेक्शन और अन्य आर्टिफ़ैक्ट।

सभी प्रोग्राम इंस्टॉल करने से शुरुआत न करें। पहले प्रश्न तय करें: क्या सिद्ध करना है, किस स्रोत से और न्यूनतम संभव परिवर्तन के साथ।

2. डाउनलोड और पर्यावरण की तैयारी

Autopsy को उसके आधिकारिक पृष्ठ से डाउनलोड करें: autopsy.com/download. पृष्ठ पर Windows के 32 और 64 बिट इंस्टॉलर, Linux/macOS पैकेज और GPG सिग्नेचर फ़ाइलें अलग-अलग दी गई हैं। इंस्टॉलर किसी सॉफ़्टवेयर एग्रीगेटर से डाउनलोड न करें।

स्थापना दस्तावेज sleuthkit.org/autopsy/docs/user-docs/4.23.0/installation_page.html पर उपलब्ध है।

1. सिस्टम आर्किटेक्चर और डाउनलोड की गई फ़ाइल जाँचें।
2. उपलब्ध होने पर प्रोजेक्ट द्वारा दिया गया सिग्नेचर या अखंडता की जानकारी सत्यापित करें।
3. इसे नियंत्रित वर्कस्टेशन पर इंस्टॉल करें, मूल साक्ष्य रखने वाले सिस्टम पर नहीं।
4. तीन स्थान अलग रखें: संरक्षित स्रोत, केस फ़ोल्डर और आउटपुट या रिपोर्ट फ़ोल्डर।
5. भौतिक डिस्क देखनी हों तो Autopsy को आवश्यक अनुमतियों के साथ चलाएँ और स्रोत को राइट-प्रोटेक्टेड रखें। बिना नियंत्रण काम करने के बहाने उन्नत अनुमतियाँ न उपयोग करें।

प्रयोगशाला के लिए उदाहरण संरचना इस प्रकार है; यह अनिवार्य पथ नहीं है:

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

मूल इमेज को बैकअप मानकर केस फ़ोल्डर में न रखें। विश्लेषण के दौरान स्रोत उपलब्ध रहना चाहिए: Autopsy केस में उसका संदर्भ रखता है, पूरी प्रति नहीं।

2.1 मूल कार्यप्रवाह से बाहर रहता है

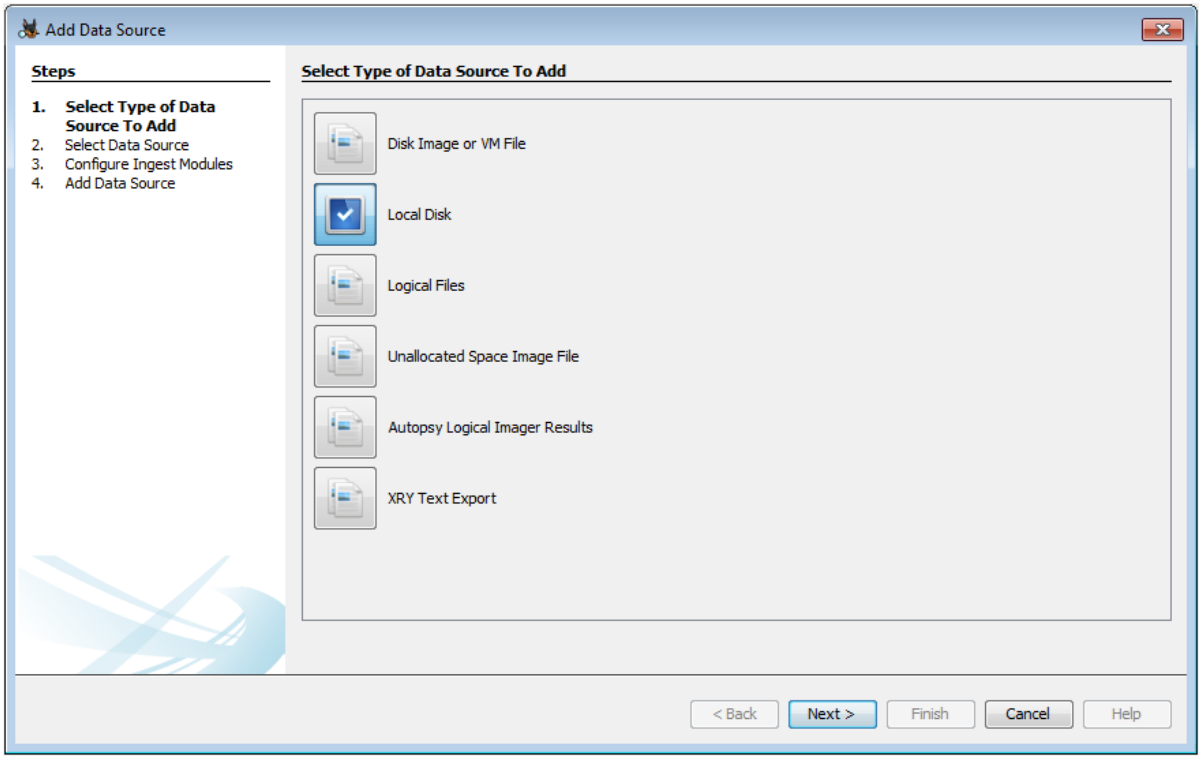
वास्तविक स्रोत जोड़ने से पहले दर्ज करें कि उसे किसने दिया, आप उसकी जाँच क्यों कर सकते हैं, उसका पहचानकर्ता, स्थिति और आवश्यकता अनुसार हैश। यदि इमेज विखंडित है, तो सेट की पहली फ़ाइल चुनें और सभी खंड साथ रखें।

स्क्रीनशॉट या Autopsy निर्यात मूल फ़ाइल का स्थान नहीं लेता। यह समझने के लिए दृश्य है, पूरा साक्ष्य नहीं।

3. प्रयोगशाला के साथ पहला केस बनाना

Autopsy खोलें और **Create New Case** चुनें। ऐसा नाम लिखें जिससे ग्राहक का डेटा उजागर न हो, जैसे `DEMO-2026-001`, और ऐसा फ़ोल्डर चुनें जो अभी मौजूद न हो। इसके बाद स्रोत जोड़ें।

6. विज़ार्ड में प्रयोगशाला के लिए **Logical Files** चुनें।
7. **Add** दबाएँ और काल्पनिक प्रयोगशाला का अनज़िप किया हुआ फ़ोल्डर चुनें।
8. जांचें कि फ़ोल्डर में केवल प्रदर्शन फ़ाइलें हैं।
9. लॉजिकल सेट का नाम रखें या उसे समझने योग्य नाम से बदलें, जैसे `DEMO-archivos`.
10. इनजेस्ट के कॉन्फ़िगरेशन पर आगे बढ़ें।



चित्र 1. विज़ार्ड से इमेज, लोकल डिस्क, लॉजिकल फ़ाइलें और अन्य स्रोत चुने जा सकते हैं। Sleuth Kit Labs का स्क्रीनशॉट, CC BY-SA 3.0.

लॉजिकल फ़ाइलें क्यों उपयोग करें? इनसे साक्ष्य-डिस्क जोड़े बिना इंटरफ़ेस सीखा जा सकता है। दस्तावेज़ चेताता है कि इस विधि से डिवाइस का गैर-आवंटित स्थान या हटाई गई फ़ाइलें नहीं देखी जातीं; केवल चुनी गई आवंटित फ़ाइलों पर काम होता है। इस अभ्यास में हटाई गई फ़ाइलें पुनः प्राप्त होने की उम्मीद न रखें।

लॉजिकल फ़ाइलों की तारीख और समय के प्रति भी सावधानी रखें। आपके सिस्टम पर फ़ाइलें कॉपी करते समय टाइमस्टैम्प बदल गए हों तो Autopsy उन्हें अनुपयोगी मान सकता है। यह खराबी नहीं, एक सीमा है जिसे अपनी रिपोर्ट में बताना चाहिए।

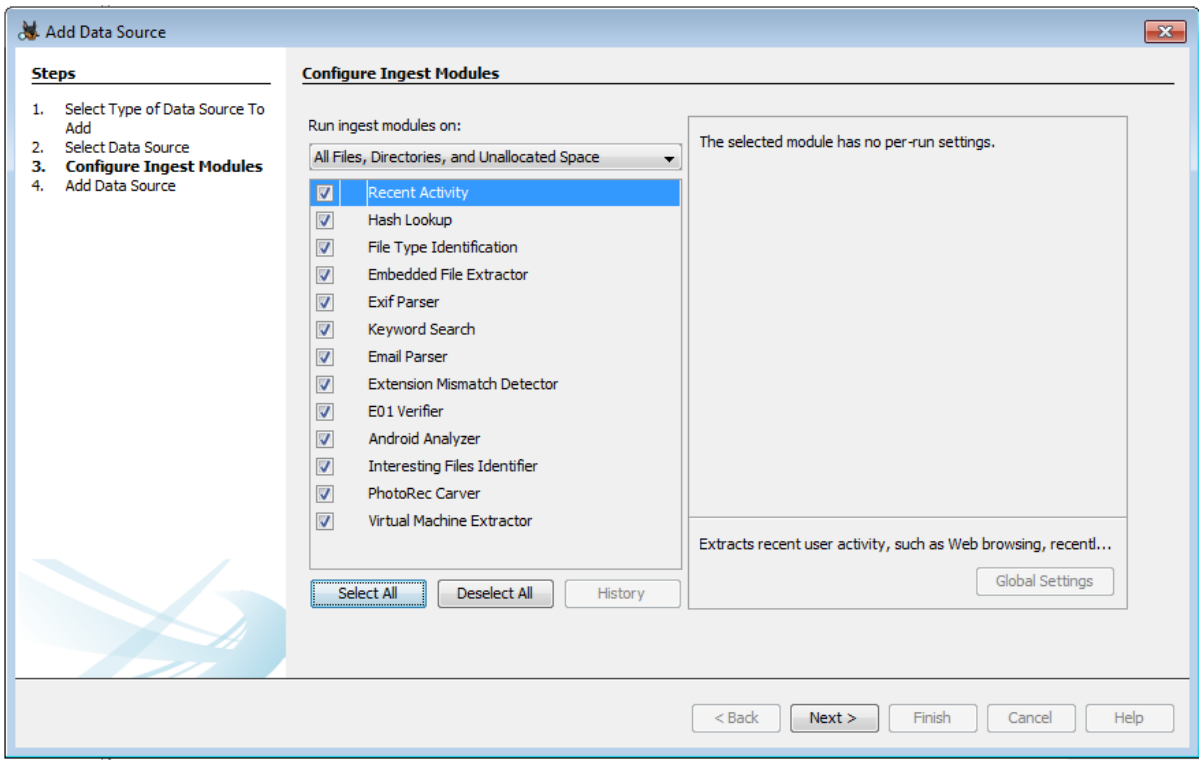
4. उद्देश्य के अनुसार इनजेस्ट मॉड्यूल चुनना

इनजेस्ट मॉड्यूल स्रोत की सामग्री का विश्लेषण करते हैं। ये बैकग्राउंड में चलते हैं और परिणाम धीरे-धीरे आते हैं। उनके चलते समय फ़ाइलें देखी जा सकती हैं, लेकिन जारी विश्लेषण को पूर्ण बताकर नहीं प्रस्तुत करना चाहिए।

प्रयोगशाला के लिए, एक छोटे से चयन के साथ शुरू करें:

मॉड्यूल	आप इसे इस अभ्यास में किस लिए उपयोग	आपको क्या याद रखना चाहिए

	करण	
File Type Identification	केवल एक्सटेंशन से नहीं, फ़ाइल सिग्नेचर से फ़ाइल का प्रकार पहचानना।	सिग्नेचर फ़ॉर्मेट पहचानने में मदद करता है, सामग्री की प्रामाणिकता सिद्ध नहीं करता।
Extension Mismatch Detector	पहचाने गए प्रकार से मेल न खाने वाले एक्सटेंशन पता लगाना।	विसंगति को समीक्षा को जाना चाहिए, यह अपने आप आरोप नहीं है।
Embedded File Extraction	ZIP और Office दस्तावेज़ों जैसे कंटेनर खोलकर उनकी सामग्री प्रोसेस करना।	निकाली गई फ़ाइल व्युत्पन्न फ़ाइल है, उसका मूल से संबंध बनाए रखें।
Keyword Search	सामग्री में कीवर्ड खोजना और सूचियाँ तैयार करना।	मिलान बताता है कि शब्द कहाँ है, उसका इरादा क्या था यह नहीं।
Recent Activity	स्रोत में मौजूद होने पर ब्राउज़र और सिस्टम की गतिविधि निकालना।	लॉजिकल प्रयोगशाला पूरे ऑपरेटिंग सिस्टम को नहीं दोहराती।
Picture Analyzer	समर्थित छवियों के EXIF मेटाडेटा और HEIC/HEIF रूपांतरणों की समीक्षा।	मेटाडेटा मौजूद न भी हो सकता या बदल जा चुका हो सकते हैं।
Email Parser	समर्थित ईमेल प्रारूप पहचानना और सदस्य निकालना।	उदाहरण वाली EML फ़ाइल काल्पनिक है, यह वास्तविक प्रेषण या प्राप्ति सिद्ध नहीं करती।
Data Source Integrity	E01 फ़ाइलों के हैश का तुलना उनके आंतरिक मानों से करना।	यह उसी प्रकार के स्रोत पर लागू होता है, किसी भी लॉजिकल फ़ोल्डर पर नहीं।
PhotoRec Carver	गैर-आवंटित स्थान में फ़ाइल खोजना।	अभ्यास के लॉजिकल फ़ोल्डर के लिए यह प्राथमिक मॉड्यूल नहीं है।



चित्र 2. स्रोत जोड़ते समय इनजेस्ट का चयन। Sleuth Kit Labs का स्क्रीनशॉट, CC BY-SA 3.0.

बिना कारण सब कुछ सक्रिय न करें। अधिक मॉड्यूल का अर्थ है अधिक समय, अधिक शोर और विश्लेषण के लिए अधिक परिणाम। इनजेस्ट केस के प्रश्न का उत्तर देने के लिए होना चाहिए।

किसी कार्य को रद्द भी किया जा सकता है, लेकिन सही ढंग से रद्द होने की प्रक्रिया पूरी होने तक प्रतीक्षा करें और दर्ज करें कि कौन से मॉड्यूल अपना काम पूरा कर चुके हैं। आंशिक इनजेस्ट पूर्ण जाँच के बराबर नहीं है।

5. संदर्भ खोए बिना परिणामों में नेविगेट करना

मुख्य इंटरफ़ेस में तीन क्षेत्र हैं: बाईं ओर ट्री, ऊपर दाईं ओर फ़ाइलों या परिणामों की सूची और नीचे दाईं ओर सामग्री।

- **Data Sources:** केस में जोड़े गए स्रोत।
- **Views:** वही डेटा प्रकार या किसी दूसरे दृष्टिकोण से व्यवस्थित।
- **Results:** इनजेस्ट से प्राप्त परिणाम।
- **Content Viewer:** चयनित तत्व की सामग्री, पाठ, छवि या हेक्साडेसिमल डेटा।

कोई परिणाम महत्वपूर्ण लगे तो कॉन्टेक्स्ट मेनू से फ़ाइल सिस्टम में उसके स्थान पर जाएँ। सूची में नाम दिखना पर्याप्त नहीं है: फ़ोल्डर, पास की फ़ाइलें, प्रारूप और उसे बनाने वाली प्रक्रिया जाँचें।

5.1 खोज-अभ्यास: “lavanda”

ऊपर दिए खोज-बॉक्स में `lavanda` लिखें। काल्पनिक फ़ाइल `01_notas.txt` में वह शब्द है, ताकि अभ्यास का नियंत्रित परिणाम मिले।

सही परिणाम यह नहीं है कि “केस हल हो गया”। सही परिणाम है फ़ाइल खोजना, उसे खोलना, पूरा वाक्य जाँचना और दर्ज करना कि वह खोज क्यों चुनी गई। इसके बाद उसे रिपोर्ट में शामिल करने के लिए टैग कर सकते हैं।

टैग करना निष्कर्ष निकालना नहीं है। टैग उन आइटम को व्यवस्थित करता है जिन्हें आप देखना या निर्यात करना चाहते हैं। इससे वे न्यायिक साक्ष्य सिद्ध नहीं होते।

6. कालक्रम उपयोग करें, पर तारीख को इरादा न समझें

Timeline को बटन या **Tools > Timeline** से खोलें। इस दृश्य से घटनाओं का समय के अनुसार अध्ययन किया जा सकता है, लेकिन संबंधित इनजेस्ट पूरे होने के बाद ही डेटा पूर्ण होगा।

दृश्य	किस काम आता है	इसे बिना जाने भार के कैसे उपयोग करें
Counts	प्रत्येक अवधि में कितना गतिविधि है यह समझना।	रुचि का समय-अवधि खोजने के लिए यहाँ से शुरू करें।
Details	किसी समय-खिड़की में घटनाओं और संबंधित समूहों की जाँच करना।	पहले अवधि और घटना-प्रकार घटाएँ।
List	किसी खोज के पहले और बाद की क्रमबद्ध घटनाएँ देखना।	इसका उपयोग तब करें जब यह तय हो कि किस समय को संदर्भ में देखना है।

अपने स्रोत के लिए उपयुक्त मॉड्यूल सक्रिय करें। Recent Activity वेब और सिस्टम गतिविधि देता है; Picture Analyzer से EXIF घटनाएँ मिलती हैं; Email Parser से संदेश मिलते हैं; अन्य मॉड्यूल अन्य प्रकार की घटनाएँ देते हैं। संबंधित सेट कॉन्फ़िगर करने पर Hash Lookup मॉड्यूल ज्ञात फ़ाइलें छिपाने में मदद कर सकता है।

6.1 समयक्षेत्र व्याख्या बदल देता है

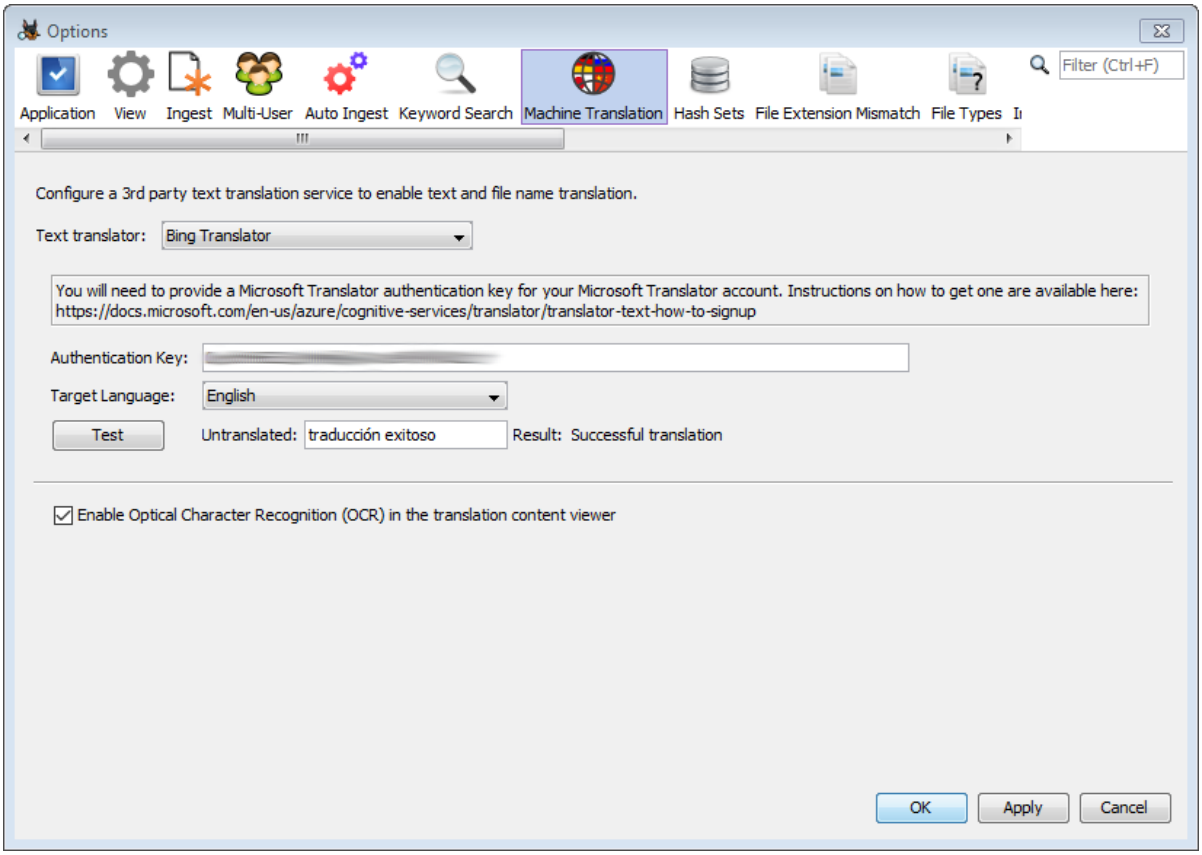
Timeline से घटनाएँ स्थानीय समय या UTC में देखी जा सकती हैं। दर्ज करें कि कौन सा विकल्प चुना और क्यों। FAT इमेज में स्रोत जोड़ते समय Autopsy समयक्षेत्र भी पूछता है, क्योंकि फ़ाइल सिस्टम यह जानकारी संग्रहीत नहीं करता।

टाइमस्टैम्प एक अवलोकन है, इरादा नहीं। घड़ी की सेटिंग, कॉपी, प्रारूप, रूपांतरण या समयक्षेत्र इसे प्रभावित कर सकते हैं। महत्वपूर्ण घटनाओं की पुष्टि अन्य स्रोतों से करें।

7. अनुवाद को सही ढंग से कॉन्फ़िगर करें

Autopsy का मशीनी अनुवाद Bing या Google की बाहरी सेवा उपयोग करता है। आपके अपने खाते और क्रेडेंशियल चाहिए; मार्गदर्शिका कोई साझा कुंजी नहीं देती।

11. **Options > Tools > Machine Translation** पर जाएं।
12. अपने संगठन के लिए अधिकृत सेवा का चयन करें।
13. खाते की जानकारी दर्ज करें। उसे स्क्रीनशॉट, रिपोर्ट या साझा केस में प्रकाशित न करें।
14. **Test** दबाएं और जांचें कि सेवा सही ढंग से प्रतिक्रिया करती है।
15. यदि आपको OCR की आवश्यकता है, तो इसे केवल तभी सक्रिय करें जब संबंधित भाषा पैकेज स्थापित हों।



चित्र 3. मशीनी अनुवाद का कॉन्फ़िगरेशन। आधिकारिक स्क्रीनशॉट में कुंजी धुंधली की गई है। Sleuth Kit Labs, CC BY-SA 3.0.

फ़ाइलों और फ़ोल्डरों के नामों का अनुवाद करने के लिए **View Options** खोलें और **Translate Text** सक्रिय करें। Autopsy अनुवाद दिखाएगा और **Original Name** नामक कॉलम रखेगा। यह कॉलम आवश्यक है: अपने दस्तावेज़ीकरण में मूल नाम न बदलें।

सामग्री के लिए व्यूअर में **Text > Translation** टैब खोलें। संदेशों में भी **Original Text** और **Translated Text** के बीच बदला जा सकता है।

अनुवाद पढ़ने में मदद करता है; अर्थ को प्रमाणित नहीं करता। मूल के साथ नाम, संक्षिप्ताक्षर, निषेध और कानूनी शब्दों की जाँच करें। गोपनीय सामग्री बाहरी सेवा को भेजने से पहले अनुमति, गोपनीयता नीति और प्रदाता की शर्तें जाँचें।

8. केवल मिलान नहीं, स्वतंत्र पुष्टि खोजें

उपयोगी जाँच में स्रोतों की तुलना और वैकल्पिक व्याख्याएँ की जाती हैं। पुनः प्राप्त फ़ाइल अधूरी हो सकती है; मिलान शोर हो सकता है; कॉपी करते समय तारीख बदल सकती है।

खोज	उत्तरदायी व्याख्या	और क्या जाँचें
खोजशब्द मिला	शब्द उस सामग्री में मौजूद है।	पूरा वाक्य, फ़ाइल, स्थान और केस से संबंध।
EXIF के साथ छवि	फ़ाइल में कुछ घोषित फ़ील्ड हैं।	क्या ये फ़ील्ड सुरक्षित रहे और क्या स्वतंत्र पुष्टि मौजूद है।
हटाई गई फ़ाइल	ऐसी संरचनाएँ मौजूद हैं जिनसे पुनर्प्राप्ति का प्रयास संभव है।	क्या सामग्री पूरी है और कोई दूसरा स्रोत उसके अंश की पुष्टि करता है।
हैश मिलान	दोनों जाँचों के बीच ऑब्जेक्ट नहीं बदला।	किस ऑब्जेक्ट की तुलना हुई, एल्गोरिदम, दिनांक और अभिरक्षा।
परिणाम न मिलना	जाँचे गए दायरे में नहीं देखा गया।	उपलब्ध स्रोत, फ़िल्टर, इनजेस्ट और विधि की सीमाएँ।

जब आप केवल "इस समीक्षा में नहीं मिला" कह सकते हों, तब "मौजूद नहीं था" न लिखें। इस अंतर से रिपोर्ट की गुणवत्ता सुरक्षित रहती है।

9. ऐसी रिपोर्ट बनाना जिसकी दूसरा व्यक्ति समीक्षा कर सके

Generate Report बटन से HTML, XLS, KML और अन्य प्रारूपों में रिपोर्ट बनाई जा सकती हैं। बाद में ट्री के **Reports** नोड से उन्हें खोजा जा सकता है।

शैक्षिक प्रारंभिक रिपोर्ट के लिए:

16. उन्हीं आइटम को टैग करें जिन्हें समझाना वास्तव में आवश्यक है।
17. **Tagged Results** चुनें, ताकि बिना चयन के पूरा केस रिपोर्ट में न डाल दें।
18. उत्पन्न रिपोर्ट की जांच करें और देखें कि लिंक काम कर रहे हैं।
19. स्वचालित आउटपुट से अलग, केस का संदर्भ, स्रोत, संस्करण, मॉड्यूल और सीमाएँ जोड़ें।

Autopsy की रिपोर्ट अंतिम विद्वत्परक निष्कर्ष नहीं है। यह उपकरण का आउटपुट है। व्यावसायिक व्याख्या में बताना चाहिए कि आर्टिफ़ैक्ट का क्या अर्थ है और निष्कर्ष कहाँ तक जाता है।

अपने दस्तावेजों में शामिल करें:

- केस पहचानकर्ता और अधिकृत दायरा।
- मूल स्रोत और कार्य प्रतिलिपि से संबंध।

- Autopsy संस्करण और चलाए गए मॉड्यूल।
- दिनांक, समय क्षेत्र और किए गए रूपांतरण।
- जहाँ उपयुक्त हो, हैश दर्ज करें; ऑब्जेक्ट और एल्गोरिदम बताएँ।
- नकारात्मक परिणाम, त्रुटियां और अनुपलब्ध स्रोत।
- सीमित निष्कर्ष और विचार किए गए विकल्प।

10. सामान्य समस्याएँ और पुनर्प्राप्ति

समस्या	संभावित कारण	क्या करना है
संभावित डिस्क नहीं दिखाई देते हैं	अपर्याप्त अनुमतियाँ या डिवाइस पहचाना नहीं गया।	अनुमतियाँ और कनेक्शन जाँचें, मूल को बिना सुरक्षा के न जोड़ें।
विखंडित इमेज नहीं खुल रही	कोई खंड गायब है या पहली फ़ाइल का चयन नहीं किया गया है।	सभी खंड एक साथ रखें और पहली चुनें।
Logical Files में हटाए गए फ़ाइलें दिखाई नहीं दे रही हैं	यह विधि केवल आवंटित फ़ाइलों के साथ काम करती है।	मूल को छूए बिना गैर-आवंटित स्थान का विश्लेषण करने के लिए उपयुक्त स्रोत उपयोग करें।
Timeline में बहुत अधिक घटनाएँ हैं	फ़िल्टर और निश्चित अवधि का अभाव।	समयसीमा, घटना-प्रकार और विवरण घटाएँ, शुरुआत में सब कुछ अधिकतम न करें।
अनुवाद काम नहीं करता है	क्रेडेंशियल, सेवा, कनेक्शन या अपूर्ण सेटिंग्स।	अधिकृत खाता जाँचें और Test दबाएँ, मूल सामग्री बनाए रखें।
सिस्टम धीमा हो जाता है	बहुत अधिक स्रोत, मॉड्यूल, इंडेक्स या सुरक्षा सॉफ़्टवेयर।	दायरा घटाएँ, स्टोरेज जाँचें और सुरक्षा-सॉफ़्टवेयर के अधिकृत अपवाद समन्वित करें; उसे कभी पूरी तरह अक्षम न करें।
हैश मेल नहीं खाता	ऑब्जेक्ट बदल गया है या अपेक्षित ऑब्जेक्ट नहीं है।	उस प्रति का उपयोग रोकें और घटना दस्तावेज़ित करें; उसे जबरन मिलाने का प्रयास न करें।

11. काल्पनिक फ़ाइलों के साथ निर्देशित अभ्यास

प्रयोगशाला के ZIP से निम्न चरण पूरे करें। उद्देश्य यह दिखाना है कि आप विधि दोहरा सकते हैं, आरोप बनाना नहीं।

20. `DEMO-2026-001` केस बनाएँ।
21. अनज़िप किए हुए फ़ोल्डर को **Logical Files** के रूप में जोड़ें।
22. केवल File Type Identification, Embedded File Extraction, Keyword Search और Picture Analyzer चलाएँ।
23. संस्करण, दिनांक, ऑपरेटर और चुने गए मॉड्यूल दर्ज करें।
24. `lavanda` खोजें और उस फ़ाइल को खोलें जिसमें यह है।
25. `03_imagen_demo.png` के मेटाडेटा जाँचें; यह न मानें कि कैमरा या GPS फ़ील्ड मौजूद हैं।
26. `02_correo_demo.eml` खोलें और उसकी सामग्री में पुष्टि करें कि प्रेषक उदाहरणों के लिए आरक्षित डोमेन उपयोग करता है।
27. Timeline से सिस्टम की वास्तविक घटनाओं और प्रयोगशाला के काल्पनिक नोट्स में भेद करें।
28. केवल उन्हीं आइटम को टैग करें जिन्हें अभ्यास समझाने के लिए चाहिए।

29. टैग किए गए आइटम की रिपोर्ट बनाएँ और उसकी सामग्री सत्यापित करें।

काल्पनिक इतिहास को वास्तविक ब्राउज़र निर्यात की तरह उपयोग न करें। `05_navegador/history-demo.txt` मैन्युअल कालक्रम के अभ्यास के लिए पढ़ने का दस्तावेज़ है, Chrome का वास्तविक डेटाबेस नहीं।

12. सरल भाषा में शब्दावली

पद	व्यावहारिक स्पष्टीकरण
आर्टिफ़ैक्ट	सिस्टम या उपकरण द्वारा बनाया गया ऐसा डेटा जो किसी प्रश्न का उत्तर देने में उपयोगी हो सकता है।
स्रोत	वह ऑब्जेक्ट जिसका विश्लेषण करना तय करें: इमेज, डिस्क, फ़ोल्डर, वर्चुअल मशीन या दूसरा सेट।
इनजेस्ट	सामग्री निकालने और उसका विश्लेषण करने के लिए स्रोत पर मॉड्यूल लागू करने की प्रक्रिया।
गैर-आवंटित स्थान	स्टोरेज का वह क्षेत्र जिसे सिस्टम वर्तमान में सक्रिय फ़ाइलों के लिए उपयोग नहीं कर रहा है।
हैश	ऐसा मान जिससे सामग्री की तुलना हो सके, निर्माता या सत्यता सिद्ध करने के लिए नहीं।
केवल-पठन	संरक्षित मूल को बदले बिना विश्लेषण के लिए उपयोग की जाने वाली प्रति।
टैग	केस में आइटम व्यवस्थित करने या रिपोर्ट में शामिल करने का निशान।
समयक्षेत्र	ऐसा संदर्भ जो तारीख को गलत समय में बदले बिना उसकी सही व्याख्या करने देता है।
OCR	छवियों से पाठ निकालने के लिए अक्षरों की ऑप्टिकल पहचान; त्रुटियाँ संभव हैं।
नकारात्मक परिणाम	दस्तावेज़ित दायरे में कोई खोज न मिलना, अस्तित्व न होने का प्रमाण नहीं।
पुनरुत्पादनीयता	दस्तावेज़ित परिस्थितियों में दूसरे व्यक्ति द्वारा प्रक्रिया दोहराने की संभावना।
सीमा	वह जानकारी जिसे स्रोत या उपाय सिद्ध करने की अनुमति नहीं देता।

13. आधिकारिक स्रोत और संपादकीय नियंत्रण

इस मार्गदर्शिका का संदर्भ संस्करण और पथ निम्न दस्तावेज़ों से जाँचे गए:

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, पहचान, संग्रह, अधिग्रहण और संरक्षण
40. NIST SP 800-86, घटना-प्रतिक्रिया में फोरेंसिक तकनीकें

चित्र 1, 2 और 3 उसी आधिकारिक दस्तावेज़ से लिए गए हैं, जो **Creative Commons Attribution-ShareAlike 3.0 United States** लाइसेंस के साथ प्रकाशित है। Sleuth Kit Labs का श्रेय और लाइसेंस का लिंक बनाए रखा गया है: CC BY-SA 3.0.

यह मार्गदर्शिका Jocsan Laguna का शैक्षिक अनुकूलन है; Sleuth Kit Labs का आधिकारिक प्रकाशन या कानूनी सलाह नहीं है। संपादकीय संस्करण की समीक्षा 15 नवंबर 2026 को हुई। वास्तविक केस में कोई फ़ंक्शन उपयोग करने से पहले प्रचलित दस्तावेज़ और संबंधित प्राधिकरण जाँचें।