

TEQUILA SO

Jocsan Laguna

Autopsy 4.23

案例、数据摄取、时间线、翻译与报告

实用指南 · 2026

目录

接触证据之前 3

1. 核心概念：案件、数据源与摄取 3

1.1 取证获取不等于分析 4

2. 下载并准备环境 4

2.1 原始载体始终置于工作流程之外 5

3. 使用实验材料创建第一个案件 5

4. 有目的地选择摄取模块 6

5. 浏览结果而不丢失上下文 7

5.1 搜索练习：“lavanda” 7

6. 使用时间线，避免把日期误当作意图 8

6.1 时区会改变事件的解读 8

7. 正确配置翻译功能 8

8. 寻求印证，而不只是匹配 10

9. 生成可供他人复核的报告 10

10. 常见问题与恢复 11

11. 使用虚构文件进行引导练习 11

12. 通俗术语表 12

13. 官方来源与编辑核查 13

本文由西班牙语原版机器辅助翻译。编辑依据以西班牙语原版为准。

本指南以首次实验室课程的讲解方式介绍 Autopsy：它有什么用途、如何处理数据，以及如何检查其输出。读者不必是工程师，但必须遵循方法。授权始终先于工具。

参考版本为 **Autopsy 4.23.0**。后续版本的菜单名称和功能可能有所变化。截图来自 Sleuth Kit Labs 的官方文档，并在相应图注中注明。

接触证据之前

Autopsy 是一个数字取证分析平台。它可用于建立案件、添加数据源、运行分析模块、审查数字痕迹、按时间排列事件并生成报告。它不会把文件变成真实证据，也不会判定谁是谁非。

仅处理自有、已获授权或公开发布用于学习的材料。保存原始载体，使用工作副本。如果目标是对真实磁盘进行取证获取，应先检查获取流程和写保护措施；Autopsy 并不能免除这项责任。

本指南附带的可下载实验材料仅包含虚构文件。它不代表真实案件、真实对话或司法证据。其用途是练习界面操作并记录步骤，而不是据此对任何个人作出结论。

1. 核心概念：案件、数据源与摄取

Autopsy 以三个核心概念组织工作，从一开始就应将它们区分清楚。

概念	如何用通俗语言解释	可避免的错误
案件	用于保存配置、数据库和报告的工作文件夹。	误以为案件只是收到的磁盘。
数据来源	将要检查的磁盘、镜像、虚拟机、文件夹或逻辑文件集合。	在不了解来源和范围的情况下随意添加内容。
摄取	分析该数据源并生成供审查的数字痕迹的模块。	以为打开镜像就等于完成了分析。

数据源不等于结论。 带有日期的文件可以描述系统记录的某个事件，但其本身并不能证明文件由谁创建、行为人出于何种意图，也不能证明系统时钟的日期是否正确。

1.1 取证获取不等于分析

FTK Imager 主要用于取证获取和预览，Autopsy 则用于分析和组织案件。你可以先用 FTK Imager 创建镜像，再将其添加到 Autopsy；也可以向 Autopsy 添加逻辑文件进行练习。

问题	适用工具	预期结果
我需要创建磁盘的取证副本。	FTK Imager，并采取适当的保存和写保护措施。	经过记录和验证的镜像。
我需要检查文件、活动、元数据和时间线。	Autopsy。	数字痕迹、搜索结果、标签和分析报告。
我需要读取某张照片的特定元数据。	ExifTool。	该文件中实际存在的字段，而非地点或作者身份的自动证明。
我需要检查一份内存转储。	Volatility 3。	该内存转储中存在的进程、连接和其他数字痕迹。

不要一开始就安装所有程序。 先明确问题：你想证明什么、使用什么数据源，以及如何尽可能减少改变。

2. 下载并准备环境

从 Autopsy 官方页面下载：autopsy.com/download。该页面区分 32 位和 64 位 Windows 安装程序、Linux/macOS 软件包以及 GPG 签名文件。不要从软件聚合网站下载安装程序。

安装文档见 sleuthkit.org/autopsy/docs/user-docs/4.23.0/installation_page.html。

1. 检查计算机的体系结构和下载的文件。
2. 如项目提供签名或完整性校验信息，应进行验证。
3. 安装在受控工作站上，不要安装在存有原始证据的计算机上。
4. 分开设置三个位置：保全数据源、案件文件夹以及输出或报告文件夹。
5. 检查物理磁盘时，应以必要权限运行 Autopsy，并对数据源实施写保护。不得把提升权限当作无序操作的借口。

以下是一种实验室目录结构示例，并非强制路径：

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

不要把原始镜像当作备份存入案件文件夹。分析期间必须能够访问数据源：Autopsy 保存的是对该数据源的引用，而不是案件内的完整副本。

2.1 原始载体始终置于工作流程之外

添加真实数据源之前，应记录交付人、你有权检查它的依据、标识符、状态，以及适用时的哈希值。如果镜像分段存储，应选择该组的第一个文件，并将所有分段保存在一起。

截图或 Autopsy 导出结果不能替代原始文件。 它们只是便于理解的可视化内容，并非证据的全部。

3. 使用实验材料创建第一个案件

打开 Autopsy，选择 **Create New Case**。输入不会泄露客户数据的名称，例如 `DEMO-2026-001`，并选择一个尚不存在的文件夹。然后添加数据源。

6. 在向导中，为本实验选择 **Logical Files**。
7. 单击 **Add**，选择虚构实验材料解压后的文件夹。
8. 确认该文件夹仅包含演示文件。
9. 保留逻辑集合的名称，或改成易于理解的名称，例如 `DEMO-archivos`。
10. 继续进行摄取配置。

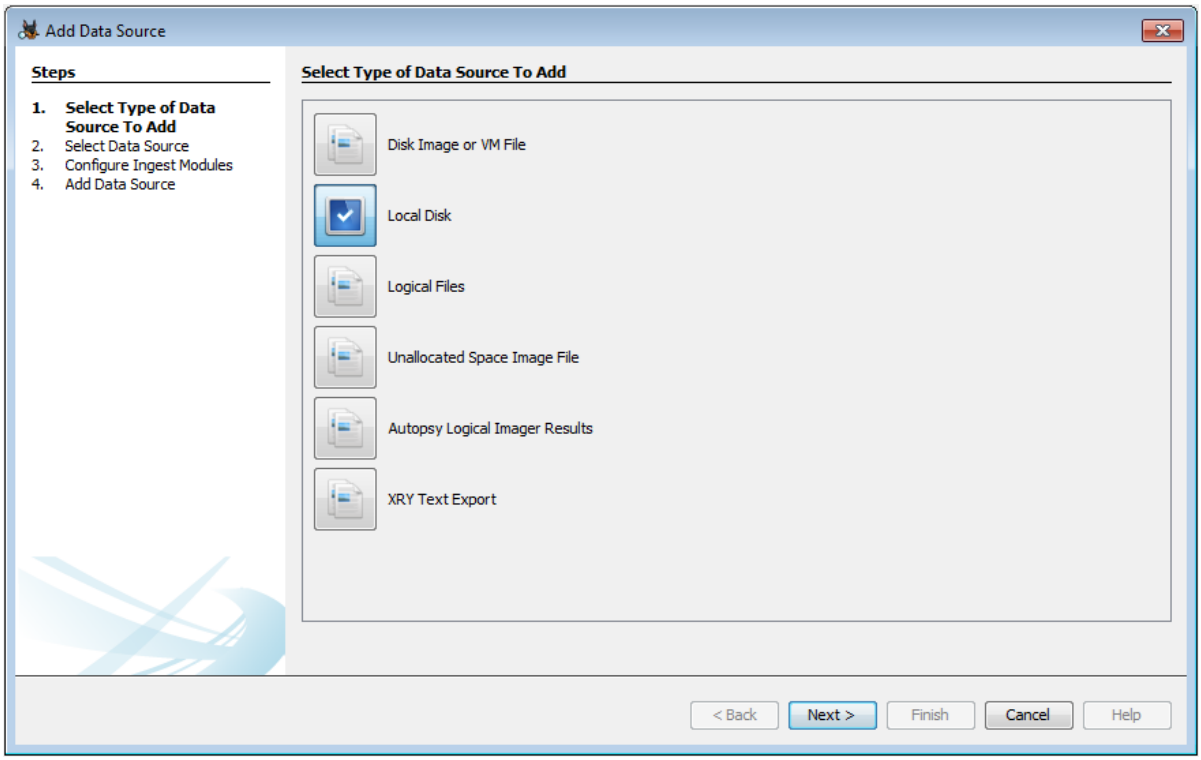


图 1 向导允许选择镜像、本地磁盘、逻辑文件和其他数据源。截图：Sleuth Kit Labs，CC BY-SA 3.0。

为什么使用逻辑文件？ 因为无需连接证据磁盘即可学习界面操作。文档提醒，这种方法不会检查设备上的未分配空间或已删除文件，只处理所选的已分配文件。不要指望在本练习中恢复已删除文件。

逻辑文件的日期同样需要谨慎对待。由于文件复制到你的计算机时时间戳可能发生变化，Autopsy 可能会忽略这些时间戳。这不是故障，而是必须声明的局限。

4. 有目的地选择摄取模块

摄取模块会分析数据源的内容。它们在后台运行，结果逐步生成。你可以在模块运行时检查文件，但不得将仍在进行的分析称为完整分析。

本实验可先选择少量模块：

模块	本练习中使用它的目的	需要牢记的事项
File Type Identification	通过文件签名识别文件类型，而不只是看扩展名。	签名有助于识别格式，但不能证明内容的真实性。
Extension Mismatch Detector	检测与识别出的文件类型不匹配的扩展名。	不一致需要复核，不能据此自动作出指控。
Embedded File Extraction	打开 ZIP 和 Office 文档等容器，并处理其中的内容。	提取出的文件属于派生材料；应保留其与原始来源的对应关系。
Keyword Search	在内容中查找词语并编制列表。	匹配只表明某个词语出现的位置，不表明其意图。
Recent Activity	当数据源包含浏览器和系统活动信息时，提取这些活动。	逻辑实验材料并不能重现整个操作系统。
Picture Analyzer	检查兼容图像的 EXIF 元数据和 HEIC/HEIF 转换。	元数据可能缺失或已经改变。
Email Parser	识别受支持的电子邮件格式并提取邮件。	示例 EML 是虚构的；不能证明实际发送或接收。
Data Source Integrity	将 E01 文件的哈希值与其内部值进行比较。	适用于此类数据源，而非任意逻辑文件夹。
PhotoRec Carver	在未分配空间中搜索文件。	对于练习用逻辑文件夹，它不是初始应启用的模块。

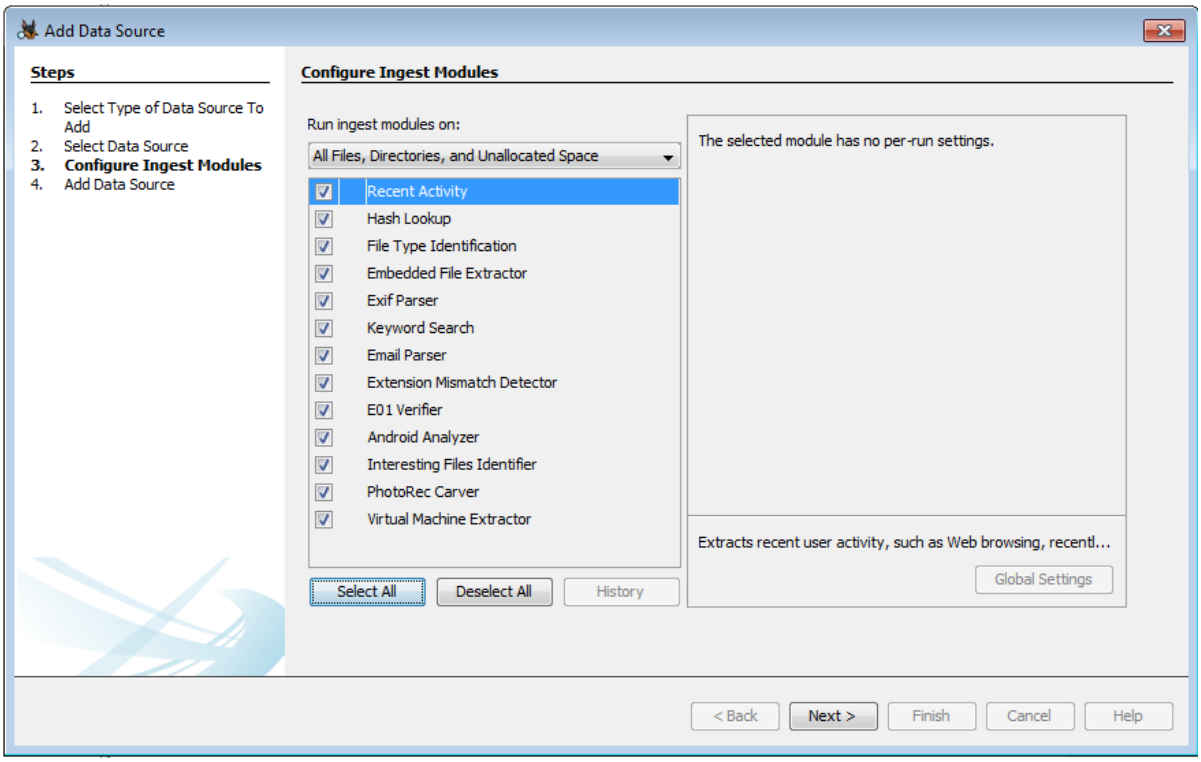


图 2 添加数据源时选择摄取模块。截图：Sleuth Kit Labs，CC BY-SA 3.0。

不要毫无目的地启用所有模块。 模块越多，耗时越长、噪声越多，需要解读的结果也越多。摄取应围绕案件问题展开。

你也可以取消任务，但应等待取消过程正常结束，并记录哪些模块已完成工作。部分摄取不等于完整检查。

5. 浏览结果而不丢失上下文

主界面分为三个区域：左侧树状结构、右上方文件或结果列表，以及右下方内容区。

- **Data Sources：** 添加到案件的数据源。
- **Views：** 按类型或其他视角组织的同一批数据。
- **Results：** 摄取模块生成的结果。
- **Content Viewer：** 所选对象的内容、文本、图像或十六进制数据。

当某项结果看似重要时，使用上下文菜单跳转到其在文件系统中的位置。仅凭列表中的名称并不足够：还要检查所在文件夹、相邻文件、格式及其生成过程。

5.1 搜索练习：“lavanda”

在上方搜索框中输入 `lavanda`。虚构文件 `01_notas.txt` 包含该词，以便本练习得到受控结果。

正确的结果不是“案件已经侦破”，而是定位并打开文件、核对完整语句，并记录选择该搜索词的原因。随后可以为其添加标签，以便纳入报告。

添加标签不等于得出结论。 标签用于组织需要检查或导出的对象，并不能证明这些对象属于司法证据。

6. 使用时间线，避免把日期误当作意图

通过按钮或 **Tools > Timeline** 打开 **Timeline**。该视图可按时间研究事件，但只有相关摄取完成后，数据才会完整。

视图	用途	如何避免信息过载
Counts	了解各时间段内的活动数量。	从这里开始，定位值得关注的时间窗口。
Details	检查某一时间窗口内的事件及相关事件组。	先缩小时间范围和事件类型。
List	按顺序查看某项发现前后的事件。	已确定需要了解哪个时点的上下文时，使用该视图。

根据数据源启用合适的模块。Recent Activity 可提供 Web 和系统活动；Picture Analyzer 可提供 EXIF 事件；Email Parser 可提供邮件；其他模块可提供其他类型的事件。配置相应的哈希集合后，Hash Lookup 模块还可帮助隐藏已知文件。

6.1 时区会改变事件的解读

Timeline 允许按本地时间或 UTC 查看事件。记录所选方式及理由。对于 FAT 镜像，添加数据源时 Autopsy 还会要求选择时区，因为该文件系统不存储此项信息。

时间戳是一项观察结果，而不是行为意图。 它可能受时钟设置、复制、格式、转换或时区影响。重要事件应与其他数据源相互印证。

7. 正确配置翻译功能

Autopsy 的机器翻译使用 Bing 或 Google 的外部服务。你需要自己的账户和凭据，本手册不会提供共享密钥。

11. 打开 **Options > Tools > Machine Translation**。
12. 选择你所在组织获准使用的服务。
13. 输入账户信息。不得在截图、报告或共享案件中公开这些信息。
14. 单击 **Test**，确认服务响应正常。
15. 如需 OCR，仅在安装相应语言包后启用。

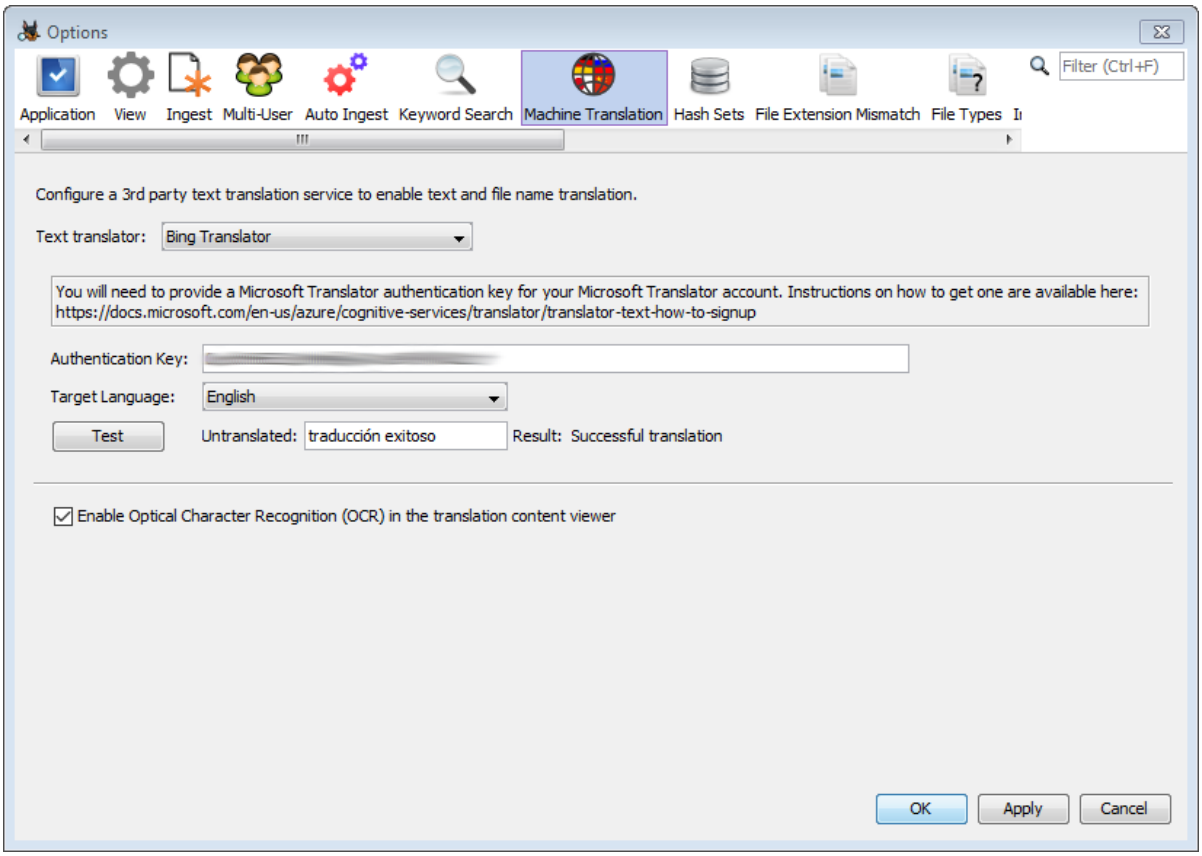


图 3 机器翻译配置。官方截图中的密钥已模糊处理。Sleuth Kit Labs，CC BY-SA 3.0。

要翻译文件和文件夹名称，请打开 **View Options** 并启用 **Translate Text**。Autopsy 会显示译文，同时保留名为 **Original Name** 的列。此列至关重要：在文档中不得替换原始名称。

要翻译内容，请在查看器中打开 **Text > Translation** 选项卡。邮件还可以在 **Original Text** 与 **Translated Text** 之间切换。

翻译有助于阅读，但不能验证含义。 应对照原文核查专有名词、缩写、否定表述和法律术语。将保密内容发送给外部服务之前，应确认授权、隐私政策和服务条款。

8. 寻求印证，而不只是匹配

有效的调查应比较不同数据源并解释其他可能性。恢复的文件可能不完整；匹配结果可能只是噪声；日期也可能在复制时发生变化。

发现	审慎解读	还需检查什么
找到关键词	该词存在于相应内容中。	完整语句、文件、位置及其与案件的关系。
含 EXIF 的图像	该文件包含若干已声明的字段。	这些字段是否得到保留，以及是否存在独立印证。
已删除的文件	存在可据以尝试恢复的结构。	内容是否完整，以及其他数据源能否确认其含义。
哈希值匹配	该对象在两次校验之间未发生变化。	比较的对象、算法、日期和保管情况。
未检出结果	在已检查的范围内未观察到。	可用数据源、筛选条件、摄取模块和方法局限。

只能表述“本次检查未发现”时，不要写成“不存在”。 这种区分有助于保证报告质量。

9. 生成可供他人复核的报告

Generate Report 按钮可生成 HTML、XLS、KML 等格式的报告。之后可通过树状结构中的 **Reports** 节点找到这些报告。

制作初步学习报告时：

16. 为确实需要说明的对象添加标签。
17. 选择 **Tagged Results**，避免不加甄别地导出整个案件。
18. 检查生成的报告，确认其中的链接可用。
19. 在自动生成的结果之外，补充案件背景、数据源、版本、模块和局限。

Autopsy 生成的报告不是最终鉴定意见，只是工具输出。专业解读必须说明数字痕迹的含义以及结论的适用边界。

文档中应包括：

- 案件标识符和授权范围。
- 原始数据源及其与工作副本的关系。
- Autopsy 版本和已运行的模块。
- 日期、时区和已执行的转换。
- 适用时记录哈希值，并注明对象和算法。
- 未发现结果、错误及不可用的数据源。
- 限定性结论和已考虑的其他解释。

10. 常见问题与恢复

问题	可能原因	处理方法
未显示所有磁盘	权限不足或设备未被识别。	检查权限和连接；不要在未加保护的情况下连接原始磁盘。
无法打开分段镜像	缺少某个分段，或未选择第一个文件。	集齐所有分段并选择第一个。
Logical Files 中未显示已删除文件	该方法仅处理已分配文件。	使用适当的数据源分析未分配空间，同时不得改动原始载体。
Timeline 中的事件过多	缺少筛选条件和明确的时间范围。	缩小时间窗口、事件类型和描述范围；不要一开始就最大化显示所有内容。
翻译功能无法使用	凭据、服务、连接或配置不完整。	检查获授权的账户并单击 Test；保留原文。
计算机运行变慢	数据源、模块或索引过多，或者安全软件造成影响。	缩小范围、检查存储，并协调实施经授权的安全软件排除设置；切勿全局禁用安全软件。
哈希值不匹配	对象已发生变化，或并非预期对象。	停止使用该副本并记录异常；不得强行使其匹配。

11. 使用虚构文件进行引导练习

使用实验材料的 ZIP 文件完成以下流程。目标是证明你能够重复该方法，而不是形成一项指控。

20. 创建案件 `DEMO-2026-001`。

21. 将解压后的文件夹作为 **Logical Files** 添加。
22. 仅运行 File Type Identification、Embedded File Extraction、Keyword Search 和 Picture Analyzer。
23. 记录版本、日期、操作员和所选模块。
24. 搜索 `lavanda`，并打开包含该词的文件。
25. 检查 `03_imagen_demo.png` 的元数据，不要预设其中存在相机或 GPS 字段。
26. 打开 `02_correo_demo.eml`，并在文件内容中确认发件人使用的是示例专用保留域名。
27. 使用 Timeline 区分真实系统事件与实验材料中的虚构笔记。
28. 仅为解释本练习所需的对象添加标签。
29. 生成已标记对象的报告并核查其内容。

不要把虚构历史记录当作真实的浏览器导出数据。`05_navegador/history-demo.txt` 是用于练习手动时间线分析的阅读文档，不是真实的 Chrome 数据库。

12. 通俗术语表

术语	实用解释
数字痕迹	由系统或工具生成、可能有助于回答某个问题的数据。
数据源	你决定分析的对象：镜像、磁盘、文件夹、虚拟机或其他集合。
摄取	将模块应用于该数据源以提取和分析内容的过程。
未分配空间	存储设备中当前未被系统用于存放活动文件的区域。
哈希值	用于比较内容的值，不能证明作者身份或内容真实性。
工作副本	用于分析的副本，可避免修改已保全的原始材料。
标签	用于在案件内组织对象或将其纳入报告的标记。
时区	用于正确解读日期、避免将其错误换算为其他时间的背景信息。
OCR	光学字符识别，用于从图像中提取文字，但可能产生错误。
未发现结果	在有记录的检查范围内未发现相关结果，并不证明其不存在。
可复现性	他人在有记录的条件下重复该程序的可能性。

局限	数据源或方法无法证明的信息。

13. 官方来源与编辑核查

本指南的参考版本和路径已对照以下文档核查：

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：识别、收集、取证获取与保存
40. NIST SP 800-86：事件响应中的取证技术

图 1、2 和 3 来自上述官方文档，该文档以 **Creative Commons Attribution-ShareAlike 3.0 United States** 许可发布。保留 Sleuth Kit Labs 的署名和许可链接：CC BY-SA 3.0。

本指南是 Jocsan Laguna 编写的教学改编资料，不是 Sleuth Kit Labs 的官方出版物，也不构成法律意见。编辑版本于 2026 年 11 月 15 日复核。在真实案件中应用任何功能之前，应核查现行文档并确认你拥有相应权限。