TEQUILA SO
Jocsan Laguna

免费计算机取证工具

Autopsy · FTK Imager · ExifTool · PhotoRec · Volatility

实用指南 · 2026



目录

1. 根据问题选择工具 3

2. FTK Imager：获取与预览 3

首次操作流程 3

3. Autopsy：分析与时间线 4

首次操作流程 4

4. ExifTool：文件的具体元数据 4

基本读取，不修改文件 5

5. PhotoRec：按文件签名恢复 5

负责任的操作流程 5

6. Volatility 3：内存分析 6

7. 精简且可审计的工作流程 6

8. 虚构实验室与判断练习 7

9. 避免严重错误的规则 7

10. 官方来源与已核实版本 8

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。

收集程序不能替代方法。本手册介绍五种工具，因为它们分别回答不同问题：FTK Imager 用于获取和预览，Autopsy 用于分析，ExifTool 用于元数据，PhotoRec 用于按文件签名恢复，Volatility 3 用于内存分析。

1. 根据问题选择工具

打开任何程序之前，先写明你想了解什么、手头有什么数据源，以及哪些内容不能改动。授权和保全与软件价格无关。

问题	工具	可以预期的结果	无法证明的内容
我需要创建镜像或查看其基本内容。	FTK Imager	镜像、预览、导出和验证。	完整的案件分析。
我需要检查文件、活动和时间线。	Autopsy	取证痕迹、搜索、标签、时间线和报告。	自动判定真实性或作者身份。
我需要了解文件包含哪些元数据。	ExifTool	文件中存在的字段及文件之间的差异。	日期或位置必然真实。
我需要尝试按文件签名恢复内容。	PhotoRec	从兼容副本或镜像中恢复的文件。	不保证保留文件名和文件夹，不保证内容完整或恢复成功。
我需要分析内存捕获文件。	Volatility 3	该捕获文件中存在的进程、连接和取证痕迹。	系统的完整状态或其历史。

免费并不意味着无害。读取数据源可能暴露机密数据；运行样本可能激活恶意软件；写入错误的目标位置可能破坏证据。

2. FTK Imager：获取与预览

FTK Imager 可创建镜像、预览文件、导出内容并验证完整性。8.2 版官方指南建议，在获取原始驱动器时使用硬件写保护器。

首次操作流程

1. 确定数据源、授权和单独的目标位置。

2. 打开 **File > Create Disk Image**。
3. 通过型号、容量和序列号确认来源，不能只看盘符。
4. 根据后续工作流程选择合适的格式、分片和压缩方式。
5. 创建时启用验证，并在适用时保留内容清单。
6. 检查摘要、哈希值和读取错误。

如果还不清楚数据源是什么，不要直接开始分析。也不要用挂载镜像代替对原始磁盘的写保护。

官方来源：Exterro FTK Imager 8.2 User Guide 和 Exterro FTK Downloads。

3. Autopsy：分析与时间线

Autopsy 可组织案件、添加数据源、运行数据导入模块并生成取证痕迹。本工具包的参考版本为 4.23.0。

首次操作流程

7. 使用新文件夹创建案件。
8. 添加镜像、受控磁盘或经授权的逻辑文件。
9. 只选择回答问题所需的模块。
10. 等待数据导入完成后再下结论。
11. 搜索内容，检查其位置，并标记相关内容。
12. 使用 Timeline，并记录所选时间窗口和时区。
13. 生成已标记项目的报告，并在自动输出之外补充方法和限制。

Logical Files 不等同于完整磁盘。此方法不会检查设备上的未分配空间或已删除文件；它只应用于练习经授权的文档，不能据此承诺能够恢复数据。

如需翻译，请使用自己的账户配置 Bing 或 Google，然后点击 **Test**。接着在 View Options 中启用 **Translate Text**。保留 **Original Name** 列，并对照原文检查否定词、专有名词和法律术语。

官方来源：下载、快速入门、数据源、Timeline、机器翻译 和 报告。

4. ExifTool：文件的具体元数据

ExifTool 可读取、写入和编辑多种格式的元数据。本版核实的参考版本为 **13.63，发布于 2026 年 11 月 10 日**。官方网站提供软件包和校验和；不要使用其他网站的副本。

基本读取，不修改文件

在实验室副本中打开终端并执行：

```
exiftool 03_imagen_demo.png
```

结果显示文件中存在的字段，不会凭空生成不存在的日期、相机或位置。实验室图像是为演示而创建的，因此其内容和元数据并不代表真实照片。

仅显示部分字段：

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

如果某个字段不存在，其缺失本身也是信息：不要声称存在某个位置或捕获设备。

显示标签名称而非描述：

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

比较两个文件，但不包括系统标签和复合标签：

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

这些命令只用于读取和比较，不会修改证据。写入元数据前，务必在工作副本上操作并保留原始件；ExifTool 写入时可以创建带有 `_original` 后缀的备份。

元数据不等于事实。用户、应用程序或格式转换都可能更改日期、作者、GPS 或描述。请核实来源，并与其他数据源交叉验证。

官方来源：ExifTool by Phil Harvey、应用程序文档 和 常见问题。

5. PhotoRec：按文件签名恢复

即使文件系统损坏或已被重新格式化，PhotoRec 仍可通过文件签名查找数据。它免费且开源，并与 TestDisk 一同分发。

PhotoRec 对来源仅进行只读访问，但恢复的文件必须保存到不同的目标位置。不要写入丢失数据所在的同一分区，否则可能覆盖正要恢复的内容。

负责任的操作流程

14. 停止使用数据源，以减少覆盖。
15. 创建镜像，或选择经授权的工作副本。
16. 在该副本上运行 PhotoRec，不要在原始件上运行。

17. 为恢复结果选择另一个目标位置。

18. 检查恢复的文件、其内容及其与数据源的关系。

19. 记录哪些内容可以读取，哪些内容不完整。

PhotoRec 无法完整还原过去。文件名和文件夹通常会丢失；碎片化可能导致文件不完整；恢复到内容并不能证明其创建者或实际发生的事件。

官方来源：PhotoRec ES 和 TestDisk Download。

6. Volatility 3：内存分析

Volatility 3 通过插件分析内存捕获文件。它不能替代获取过程：你需要兼容的内存捕获文件，以及与受检系统相匹配的符号文件。

应在测试用内存捕获文件上运行，而不是在第三方的个人数据上运行。初始读取示例如下：

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

查看捕获文件中记录的进程：

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

查看内存捕获文件和插件支持分析的连接：

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

`memoria_demo.raw` 只是一个示例文件名：本工具包不提供内存捕获文件。执行这些命令需要真实的教学数据源，并满足文档所列要求。不要下载来源不明的内存转储，其中可能包含敏感数据或恶意软件。

内存捕获只反映一个时刻，而不是全部历史。可见的进程和连接取决于捕获时间、获取过程以及符号文件的兼容性。

官方来源：GitHub 上的 Volatility 3 和 生成的文档。

7. 精简且可审计的工作流程

使用这五种工具即可完成基本流程，无需堆砌不必要的程序。

阶段	操作	工作证据
授权	明确目标、数据源和权限。	范围、保管人和排除项。
获取	创建镜像或受控副本。	方法、版本、日期、目标位置和哈希值

		。
检查	在 FTK Imager 中打开数据源并定位文件。	路径、格式和初步观察。
分析	使用 Autopsy 并选择所需的数据导入模块。	取证痕迹、搜索、标签和时间线。
元数据	使用 ExifTool 检查指定副本。	现有字段及差异，不改写原始件。
恢复	在问题确有需要时使用 PhotoRec。	经检查的结果及恢复限制。
内存	必要时使用 Volatility 分析内存捕获文件。	兼容的数据源、插件和输出。
报告	说明方法、发现和限制。	可复现的复核和引用来源。

并非每个案件都必须使用全部工具。奥卡姆剃刀原则同样适用：选择既能最佳回答问题、又能将改动降至最低的工具。

8. 虚构实验室与判断练习

ZIP 包含专门为教学创建的文档、一个 EML 文件、一张图片和笔记，并非真实案件的捕获数据。

20. 解压前计算 ZIP 的哈希值，并与 `SHA256SUMS.txt` 进行比对。
21. 在 Autopsy 中将该文件夹添加为 Logical Files。
22. 搜索 `lavanda`，并打开相应文件。
23. 使用 ExifTool 检查 `03_imagen_demo.png`，记录哪些字段存在、哪些不存在。
24. 打开 `02_correo_demo.eml`，确认发件人是否使用示例专用保留域名。
25. 记录为什么不能仅凭这些文件断定邮件确已发送、内容真实、所处位置或行为意图。
26. 写一份五行的输出记录：数据源、方法、发现、限制和下一项核查。

不要针对不存在的测试内存镜像执行内存分析命令。实验室用于练习文件读取与分析；内存分析需要另一份经授权的数据源。

9. 避免严重错误的规则

- 即使技术操作简单，也必须先获得授权再访问。

- 保留原始件，分析副本。
- 镜像和恢复的文件应使用单独的目标位置。
- 只从官方网站下载，并在提供完整性信息时进行验证。
- 不要在个人设备或生产网络中运行未知样本。
- 记录版本、日期、时区、参数和操作员。
- 区分发现、解释和结论。
- 不要将元数据视为作者身份、真实日期或自动定位的证明。
- 不要承诺能够全部恢复，也不要因为搜索未显示文件就断言文件不存在。
- 未经授权，不要与外部翻译服务共享密钥、凭据或机密数据。

10. 官方来源与已核实版本

27. Autopsy 4.23.0：用户文档
28. Exterro FTK Imager 8.2 User Guide
29. ExifTool 13.63：官方网站与下载
30. ExifTool Application Documentation
31. PhotoRec ES，CGSecurity
32. Volatility 3：官方仓库
33. Volatility 3：文档
34. ISO/IEC 27037
35. NIST SP 800-86

各版本于 2026 年 11 月 15 日核实。界面和格式会变化：在真实案件中应用任何流程前，务必查阅现行文档。本指南仅用于教学，不能替代法律咨询、授权或专业审查。