TEQUILA SO
Jocsan Laguna

FTK Imager

数据获取、预览、哈希与文档记录

实用指南 2026 · 8.2 文档



目录

1. FTK Imager 能做什么、不能做什么 3

1.1 原始材料规则 3

2. 准备取证获取 4

2.1 使用实验材料进行安全练习 4

3. 逐步创建镜像 4

4. 选择格式、分段和压缩 5

5. 验证并保存结果 5

6. 预览和导出，同时保持与数据源的关联 6

7. 挂载镜像：读取、写入与限制 6

8. 内存捕获：另一类操作 7

9. 常见错误与安全决策 7

10. 使用虚构文件练习 8

11. 报告前核查清单 8

12. 官方来源与编辑核查 9

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。

FTK Imager 用于创建取证镜像、预览证据、导出文件和核验完整性。它的主要作用不是替代分析，而是让分析能够基于有记录的数据源进行，而不必依赖原始材料。

本指南以日常语言说明操作流程，不是逐字翻译，也不是 Exterro 官方指南。菜单以 8.2 版文档为依据，应与已安装版本核对。

1. FTK Imager 能做什么、不能做什么

该应用程序可以创建逐位副本、检查内容、以只读方式挂载镜像、导出文件、生成哈希列表，并在特定条件下捕获内存。在使用 Autopsy 或其他平台分析之前，它尤其有用。

需求	FTK Imager	Autopsy
创建磁盘或文件的镜像。	这是它的核心功能。	这不是其主要工作流程的第一步。
预览文件夹和文件。	证据树、列表、属性和查看器。	树状结构、结果和内容，并配有更多分析模块。
执行案件分析和关联分析。	与完整的案件分析平台相比，功能有限。	摄取、搜索、时间线、通信、报告等。
验证完整性。	取证获取期间验证和事后验证。	Data Source Integrity 适用于兼容数据源，并有其他控制措施。

创建镜像不等于调查已经完成。 它只是经过保全的一种表现形式，仍需复核并结合语境分析。

1.1 原始材料规则

官方指南建议在为驱动器创建镜像时使用**硬件写保护器**，以防止操作系统在连接原始数据源时对其进行修改。

不要混淆以下三种操作：

- **创建镜像：** 生成数据源的副本。
- **以只读方式挂载镜像：** 允许检查该副本，但镜像本身并不会成为原始材料的写保护器。
- **使用副本工作：** 使原始材料置于分析过程之外。

2. 准备取证获取

打开 FTK Imager 之前，先记录案件和设备信息。急于选择按钮，往往会完整镜像错误的磁盘。

1. 授权范围、数据源和方法。
2. 在可用时记录型号、容量和序列号。
3. 对原始数据源使用硬件写保护器。
4. 使用不同于数据源的存储目标，并确保供电和可用空间充足。
5. 分别准备镜像文件夹和日志及报告文件夹。
6. 记录 FTK Imager 版本、日期、时区和操作员。

目标位置必须能够容纳完整镜像、分段文件、取证获取信息和工作副本。“磁盘放得下”不一定意味着“整个过程所需空间都够用”。

绝不能把镜像保存到正在取证获取的同一磁盘上。 否则可能改动或破坏你试图保全的内容。

2.1 使用实验材料进行安全练习

可下载实验材料无需连接证据磁盘。它将虚构文件夹作为逻辑文件集合，用于学习界面和选项。不要在主磁盘或他人设备上练习物理取证获取。

3. 逐步创建镜像

基本路径为 **File > Create Disk Image**。向导允许选择来源和目标位置。

7. 根据实际情况选择来源类型：物理驱动器、逻辑驱动器、现有镜像或文件夹内容。
8. 通过设备标识符确认具体设备，不要只看驱动器号。
9. 选择不同于数据源的目标文件夹。
10. 指定不带扩展名的名称，并关联案件标识符。
11. 填写可用的元数据：案件、证据、描述、检查员和备注。
12. 检查镜像类型、分段和压缩设置。
13. 启用 **Verify images after they are created**，在创建完成后核验完整性。
14. 考虑启用 **Create directory listings of all files in the image**，以保留可用的路径和元数据。
15. 单击 **Start** 前检查所有设置。
16. 保存取证获取日志和摘要，包括读取错误。

如果仍不确定来源，请勿单击 Start。 返回接收记录并核实。

4. 选择格式、分段和压缩

格式取决于数据源和后续工作流程，而不是使用习惯。

选项	含义	检查内容
Raw / DD	直接复制、兼容性广，不强制压缩。	需要与数据源及分段文件相适应的存储空间。
E01	包含元数据的证据镜像，并根据工作流程提供压缩选项。	与分析工具的兼容性以及元数据保存。
AD1	自定义内容的逻辑镜像。	它不是磁盘的物理镜像，也不包含完整的磁盘几何信息。
分段	将结果拆分为多个大小受限的文件。	所有分段必须保存在一起，才能进行分析和验证。
压缩 0–9	根据所选格式，在处理速度和文件大小之间取得平衡。	压缩程度越高，处理时间可能越长。

8.2 版指南记录了该流程的默认分段大小为 **1500 MB**。不要把它当作通用规则。应根据存储、传输和分析需求选择；如果该选项允许取值为 0，则结果不分段。

不要指望更改格式后内容仍逐位完全相同。 一种表现形式可能保留可见信息，却仍改变结构和哈希值。应记录原始材料与派生材料的关系。

5. 验证并保存结果

完成后，先检查摘要，再将镜像视为有效。创建期间的验证会比较生成的哈希值，有助于发现差异。如果结果不一致，不得将其当作正确副本使用。

17. 记录来源和镜像的哈希值，并注明算法和对象。
18. 检查已读取的扇区和读取错误。
19. 确认所有分段都位于同一文件夹。
20. 保存取证获取日志，以及已生成的内容列表。

21. 将镜像作为证据打开，确认能够读取而不会修改镜像。

22. 适用时执行事后验证，并将结果与已记录的值比较。

8.2 版指南说明，该应用程序的多项哈希功能使用 **MD5 和 SHA-1**。如果你的程序还要求额外的 SHA-256，应使用适当工具计算，并记录它属于另一项处理过程，而不是虚构 FTK Imager 具备该功能。

哈希一致证明对象在两次校验之间未发生变化，并不证明内容真实，也不证明来源合法。

6. 预览和导出，同时保持与数据源的关联

证据树显示数据源和文件夹；文件列表随选择变化；属性面板显示类型、位置、大小和日期；查看器显示内容。

检查文件的步骤：

23. 通过 **Add Evidence Item** 添加镜像。

24. 展开数据源，直到找到目标文件。

25. 检查属性和内容，不要只看文件名。

26. 检查相邻文件以了解语境。

27. 导出到工作文件夹，并保留原始路径。

28. 如果需要哈希列表，请选择对象并使用 **Export File Hash List**。

导出的文件属于派生材料。即使内容完全相同，也不得将其表述为仍位于原始位置。

7. 挂载镜像：读取、写入与限制

FTK Imager 允许将某些镜像挂载为只读设备或驱动器。它还记录了带写入缓存的模式：更改会单独保存，不会改变镜像的原始内容。

模式	允许的操作	警示
只读	在不改变镜像内容的情况下检查镜像。	这不等同于原始磁盘的写保护器。
写入缓存	将更改或注释保存到另一个文件。	必须记录缓存，不得将其当作原始内容。

物理挂载和逻辑挂载不能互换。AD1 和 L01 包含文件结构，但不包含完整的磁盘几何信息，因此不能作为物理镜像挂载。

完成后卸载镜像，并记录任何由此产生的更改。Windows 允许打开某个驱动器，并不证明你可以向其中写入。

8. 内存捕获：另一类操作

在运行中的系统上捕获内存会产生特定影响，可能改变进程、内容和设备状态。内存具有易失性，捕获结果必须保存到单独的目标位置，并记录日期和哈希值。

不要在真实设备上将此功能作为入门练习。如果案件需要内存，应先明确授权、目标、方法、影响、工具和保管链。捕获与后续分析是不同操作：FTK Imager 负责捕获；Volatility 或其他平台可以帮助检查结果。

9. 常见错误与安全决策

情形	负责任的决定
不知道哪块磁盘是原始磁盘	停止操作。核对型号、容量、序列号和接收记录；不要凭驱动器号猜测。
目标位置空间不足	停止并重新分配存储空间。将相关分段保存在同一文件夹中。
镜像未通过验证	不得将其作为有效副本。记录失败情况，并采用适当方法重新执行该过程。
逻辑集合中未显示已删除文件	检查数据源和方法是否允许访问未分配空间，不得虚构恢复结果。
无法将 AD1 镜像作为物理镜像挂载	这是内容类型的限制，应使用受支持的逻辑挂载。
转换后哈希值不同	确定发生变化的是结构、元数据、内容还是比较对象，不得自动断言为伪造。
需要分析内容	将镜像添加到 Autopsy 或其他平台；不要把取证获取与完整分析混为一谈。

10. 使用虚构文件练习

使用实验文件夹学习各项选项，无需在真实磁盘上操作。

29. 打开 FTK Imager，选择文件夹内容，不要选择主驱动器。
30. 仅选择解压后的虚构文件夹。
31. 在该文件夹之外设置一个新的目标位置。
32. 添加演示元数据，不得包含个人或客户姓名。
33. 启用验证和内容列表。
34. 检查镜像、分段和日志的存储方式。
35. 将结果作为证据打开，并找到 `01_notas.txt`。
36. 导出一份工作副本和一份哈希列表，并注明各自使用的处理过程。
37. 记录为什么本练习不能证明物理取证获取或已删除文件恢复。

本练习用于学习界面操作流程，不会把文件夹变成磁盘，也不会使创建的镜像成为司法证据。

11. 报告前核查清单

- 授权和范围均有书面记录。
- 尽可能通过型号、容量和序列号识别数据源。
- 原始数据源已使用写保护器。
- 目标位置独立且空间充足。
- 镜像类型、分段和压缩均有合理依据。
- 案件和证据元数据完整。
- 已执行验证并检查结果。
- 所有分段齐全且可读取。
- 读取错误和局限均有记录。
- 工作文件均与其来源关联。
- 后续分析与取证获取分开进行。
- 结论仅限于方法能够证明的内容。

12. 官方来源与编辑核查

38. Exterro FTK Imager 8.2 User Guide

39. Exterro FTK Downloads

40. Autopsy User Documentation 4.23.0: Quick Start Guide

41. Autopsy User Documentation 4.23.0: Data Sources

42. Autopsy User Documentation 4.23.0: Reporting

43. ISO/IEC 27037：识别、收集、取证获取与保存

44. NIST SP 800-86：事件响应中的取证技术

本改编版已完整阅读 8.2 版指南。其内容包括不同版本和产品的功能，并非全部属于 FTK Imager 免费版。使用 Pro 功能或移动设备取证获取功能之前，应核实许可证和专门文档。

本指南是 Jocsan Laguna 编写的学习材料，不是 Exterro 官方出版物，也不构成法律意见。编辑复核：2026 年 11 月 15 日。