TEQUILA SO
Jocsan Laguna

FTK Imager

Akquisition, Vorschau, Hashing und Dokumentation

PRAXISLEITFADEN 2026 · DOKUMENTATION 8.2



Inhalt

1. Was FTK Imager leistet – und was nicht ... 3

1.1 Die Regel für das Original ... 3

2. Die Erfassung vorbereiten ... 3

2.1 Sichere Übung mit dem Labor ... 4

3. Ein Image Schritt für Schritt erstellen ... 4

4. Format, Fragmente und Komprimierung wählen ... 4

5. Ergebnis überprüfen und aufbewahren ... 5

6. Vorschau und Export ohne Verlust des Quellenbezugs ... 5

7. Images einbinden: Lesen, Schreiben und Grenzen ... 6

8. Speichererfassung: eine eigene Kategorie von Maßnahmen ... 6

9. Häufige Fehler und sichere Entscheidungen ... 6

10. Übung mit fiktiven Dateien ... 7

11. Checkliste vor dem Bericht ... 7

12. Offizielle Quellen und redaktionelle Kontrolle ... 8

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

FTK Imager dient zur Erstellung forensischer Images, zur Vorschau von Beweismaterial, zum Exportieren von Dateien und zur Integritätsprüfung. Seine Hauptaufgabe ist nicht, die Analyse zu ersetzen, sondern ihr eine dokumentierte Datenquelle bereitzustellen, ohne vom Original abhängig zu sein.

Dieser Leitfaden erläutert den Arbeitsablauf in Alltagssprache. Er ist keine wörtliche Übersetzung und kein offizieller Leitfaden von Exterro. Die Menüs basieren auf der Dokumentation 8.2 und sind mit der installierten Version abzugleichen.

1. Was FTK Imager leistet – und was nicht

Die Anwendung ermöglicht bitweise Kopien, die Prüfung von Inhalten, das Einbinden von Images zur Lesansicht, den Dateiexport, die Erstellung von Hashlisten und unter bestimmten Voraussetzungen die Speichererfassung. Sie ist besonders vor der Analyse mit Autopsy oder einer anderen Plattform nützlich.

Bedarf	FTK Imager	Autopsy
Ein Image des Datenträgers oder von Dateien erstellen.	Zentrale Funktion.	Nicht der erste Schritt im Hauptarbeitsablauf.
Ordner und Dateien in der Vorschau anzeigen.	Beweisbaum, Liste, Eigenschaften und Viewer.	Baum, Ergebnisse und Inhalt mit mehr Analysemodulen.
Fallanalyse und Korrelation durchführen.	Gegenüber einer vollständigen Fallplattform eingeschränkt.	Ingest, Suche, Zeitachse, Kommunikation, Berichte und mehr.
Integrität überprüfen.	Überprüfung bei der Erfassung und nachträgliche Überprüfung.	Data Source Integrity für kompatible Datenquellen und weitere Kontrollen.

Ein erstelltes Image ist keine abgeschlossene Untersuchung. Es ist eine aufbewahrte Darstellung, die noch geprüft und in ihren Kontext eingeordnet werden muss.

1.1 Die Regel für das Original

Das offizielle Handbuch empfiehlt bei der Image-Erstellung von einem Datenträger einen **Hardware-Schreibblocker**. Dadurch wird verhindert, dass das Betriebssystem die Originalquelle beim Anschließen verändert.

Unterscheiden Sie drei Vorgänge:

- **Ein Image erstellen:** erzeugt eine Kopie der Datenquelle.
- **Ein Image zur Lesansicht einbinden:** ermöglicht die Prüfung dieser Kopie; das Image wird dadurch nicht zum Schreibblocker für das Original.
- **Mit einer Kopie arbeiten:** hält das Original außerhalb des Analyseprozesses.

2. Die Erfassung vorbereiten

Bevor Sie FTK Imager öffnen, dokumentieren Sie Fall und Gerät. Die Eile bei der Auswahl von Schaltflächen führt häufig zu einem vollständigen Image des falschen Datenträgers.

1. Autorisieren Sie Umfang, Datenquelle und Methode.
2. Erfassen Sie Modell, Kapazität und Seriennummer, sofern verfügbar.
3. Verwenden Sie einen Hardware-Schreibblocker für die Originalquelle.
4. Wählen Sie ein von der Quelle getrenntes Ziel mit ausreichend Energieversorgung und Speicherplatz.
5. Legen Sie einen Ordner für das Image und einen weiteren für Protokolle und Berichte an.
6. Dokumentieren Sie die Version von FTK Imager, Datum, Zeitzone und Bearbeiter.

Das Ziel muss ausreichend Kapazität für das vollständige Image, die Fragmente, die Erfassungsinformationen und die Arbeitskopien bieten. „Der Datenträger passt“ bedeutet nicht immer „der Prozess passt“.

Speichern Sie das Image niemals auf dem Datenträger, den Sie gerade erfassen. Sie könnten das Beweismaterial verändern oder vernichten, das Sie erhalten möchten.

2.1 Sichere Übung mit dem Labor

Für das herunterladbare Labor muss kein Beweisdatenträger angeschlossen werden. Verwenden Sie den fiktiven Ordner als logische Dateisammlung, um die Oberfläche und die Optionen kennenzulernen. Üben Sie die physische Erfassung weder mit Ihrem Hauptdatenträger noch mit Geräten anderer Personen.

3. Ein Image Schritt für Schritt erstellen

Der grundlegende Weg ist **File > Create Disk Image**. Der Assistent führt durch die Auswahl von Quelle und Ziel.

7. Wählen Sie je nach Fall den Quellentyp: physisches Laufwerk, logisches Laufwerk, vorhandenes Image oder Ordnerinhalt.
8. Bestätigen Sie das genaue Gerät anhand seiner Kennungen, nicht nur anhand des Laufwerksbuchstabens.
9. Wählen Sie einen Zielordner, der von der Quelle getrennt ist.
10. Vergeben Sie einen Namen ohne Erweiterung und verknüpfen Sie die Fallkennung.
11. Füllen Sie die verfügbaren Metadaten aus: Fall, Beweismaterial, Beschreibung, Prüfer und Anmerkungen.
12. Prüfen Sie Imagetyp, Fragmentierung und Komprimierung.
13. Aktivieren Sie **Verify images after they are created**, um die Integrität nach der Erstellung zu prüfen.
14. Ziehen Sie **Create directory listings of all files in the image** in Betracht, um verfügbare Pfade und Metadaten aufzubewahren.
15. Prüfen Sie alle Angaben, bevor Sie **Start** wählen.
16. Bewahren Sie das Protokoll und die Zusammenfassung der Erfassung einschließlich etwaiger Lesefehler auf.

Wählen Sie Start nicht, solange Zweifel an der Quelle bestehen. Kehren Sie zum Entgegennahmeprotokoll zurück und überprüfen Sie die Angaben.

4. Format, Fragmente und Komprimierung wählen

Das Format richtet sich nach der Quelle und dem späteren Arbeitsablauf, nicht nach Gewohnheit.

Auswahl	Bedeutung	Prüfpunkte
Raw / DD	Direkte Kopie, breite Kompatibilität und keine obligatorische Komprimierung.	Erfordert ausreichend Speicherplatz für Quelle und Fragmente.

E01	Beweisimage mit Metadaten und Komprimierungsoptionen je nach Arbeitsablauf.	Kompatibilität mit Analysewerkzeugen und Erhaltung der Metadaten.
AD1	Logisches Image mit benutzerdefiniertem Inhalt.	Kein physisches Image des Datenträgers; enthält nicht dessen gesamte Geometrie.
Fragmentierung	Aufteilung des Ergebnisses in mehrere Dateien begrenzter Größe.	Alle Segmente müssen für Analyse und Überprüfung zusammenbleiben.
Kompression 0–9	Ausgleich zwischen Geschwindigkeit und Dateigröße je nach Format.	Stärkere Komprimierung kann die Verarbeitungszeit erhöhen.

Das Handbuch 8.2 dokumentiert in diesem Arbeitsablauf eine standardmäßige Fragmentgröße von **1500 MB**. Dies ist keine allgemeingültige Regel. Wählen Sie nach Speicherung, Transport und Analyse; der Wert 0 verhindert die Fragmentierung, sofern diese Option zulässig ist.

Ändern Sie das Format nicht in der Erwartung, dass der Inhalt bit für bit identisch bleibt. Eine Darstellung kann sichtbare Informationen bewahren und dennoch Struktur und Hashwerte verändern. Dokumentieren Sie die Beziehung zwischen Original und Derivat.

5. Ergebnis überprüfen und aufbewahren

Prüfen Sie nach Abschluss die Zusammenfassung, bevor Sie das Image als gültig akzeptieren. Die Überprüfung während der Erstellung vergleicht die erzeugten Hashwerte und hilft, Abweichungen zu erkennen. Stimmt das Ergebnis nicht überein, verwenden Sie es nicht als korrekte Kopie.

17. Dokumentieren Sie die Hashwerte von Quelle und Image mit Angabe von Algorithmus und Objekt.
18. Prüfen Sie gelesene Sektoren und Lesefehler.
19. Vergewissern Sie sich, dass alle Fragmente im selben Ordner liegen.
20. Bewahren Sie das Erfassungsprotokoll und gegebenenfalls das Inhaltsverzeichnis auf.
21. Öffnen Sie das Image als Beweiselement, um zu bestätigen, dass es unverändert gelesen werden kann.
22. Führen Sie gegebenenfalls eine nachträgliche Überprüfung durch und vergleichen Sie das Ergebnis mit dem dokumentierten Wert.

Das Handbuch 8.2 dokumentiert **MD5 und SHA-1** für mehrere Hashfunktionen der Anwendung. Benötigt Ihr Verfahren zusätzlich SHA-256, berechnen Sie den Wert mit einem geeigneten Werkzeug und vermerken Sie, dass er aus einem separaten Prozess stammt und nicht aus einer erfundenen Funktion von FTK Imager.

Die Übereinstimmung beweist, dass das Objekt zwischen den Prüfungen unverändert blieb, nicht, dass sein Inhalt wahr oder seine Herkunft rechtmäßig ist.

6. Vorschau und Export ohne Verlust des Quellenbezugs

Der Beweisbaum zeigt Quellen und Ordner; die Dateiliste ändert sich mit der Auswahl; das Eigenschaftenpanel zeigt Typ, Speicherort, Größe und Datumsangaben; der Viewer zeigt den Inhalt.

So prüfen Sie eine Datei:

23. Fügen Sie das Image mit **Add Evidence Item** hinzu.
24. Erweitern Sie die Datenquelle bis zur gewünschten Datei.

25. Prüfen Sie Eigenschaften und Inhalt, nicht nur den Dateinamen.
26. Untersuchen Sie benachbarte Dateien, um den Kontext zu verstehen.
27. Exportieren Sie in einen Arbeitsordner und bewahren Sie den ursprünglichen Pfad auf.
28. Wenn Sie eine Hashliste benötigen, wählen Sie die Objekte aus und verwenden Sie **Export File Hash List**.

Eine exportierte Datei ist ein Derivat. Stellen Sie sie nicht so dar, als befände sie sich am ursprünglichen Speicherort, selbst wenn ihr Inhalt identisch ist.

7. Images einbinden: Lesen, Schreiben und Grenzen

FTK Imager kann bestimmte Images als Gerät oder Laufwerk zur Lesansicht einbinden. Außerdem dokumentiert es Modi mit Schreibcache, in denen Änderungen separat gespeichert werden und der ursprüngliche Inhalt des Images unverändert bleibt.

Modus	Möglichkeit	Warnung
Lesen	Das Image untersuchen, ohne seinen Inhalt zu verändern.	Kein Schreibblocker für den Originaldatenträger.
Schreibcache	Änderungen oder Anmerkungen in einer separaten Datei speichern.	Dokumentieren Sie den Cache und stellen Sie ihn nicht als ursprünglichen Inhalt dar.

Physisches und logisches Einbinden sind nicht austauschbar. AD1 und L01 enthalten Dateistrukturen, aber nicht die gesamte Datenträgergeometrie; daher können sie nicht als physisches Image eingebunden werden.

Nach Abschluss trennen Sie das Image und dokumentieren Sie alle daraus entstandenen Änderungen. Dass Windows ein Laufwerk öffnen kann, beweist nicht, dass Sie darauf schreiben dürfen.

8. Speichererfassung: eine eigene Kategorie von Maßnahmen

Die Speichererfassung in einem laufenden System hat eigene Auswirkungen. Sie kann Prozesse, Inhalte und den Zustand des Geräts verändern. Der Arbeitsspeicher ist flüchtig; die Aufzeichnung muss auf einem separaten Ziel gespeichert und mit Datum und Hashwert dokumentiert werden.

Verwenden Sie diese Funktion nicht als erste Übung auf einem realen Gerät. Benötigt der Fall Arbeitsspeicher, legen Sie zunächst Autorisierung, Ziel, Methode, Auswirkungen, Werkzeug und Beweismittelkette fest. Erfassung und spätere Analyse sind unterschiedliche Vorgänge: FTK Imager erfasst den Speicher; Volatility oder eine andere Plattform kann bei der Untersuchung des Ergebnisses helfen.

9. Häufige Fehler und sichere Entscheidungen

Situation	Verantwortungsvolle Entscheidung
Sie wissen nicht, welcher Datenträger das Original ist	Halten Sie an. Prüfen Sie Modell, Kapazität, Seriennummer und Protokoll; raten Sie nicht anhand des Laufwerksbuchstabens.
Das Ziel hat nicht genügend Speicherplatz	Brechen Sie ab und weisen Sie Speicher neu zu. Bewahren Sie zugehörige Fragmente im selben Ordner auf.

Das Image stimmt nicht mit der Überprüfung überein	Verwenden Sie es nicht als gültige Kopie. Dokumentieren Sie den Fehler und wiederholen Sie den Vorgang mit der geeigneten Methode.
In einer logischen Sammlung werden keine gelöschten Dateien angezeigt	Prüfen Sie, ob Quelle und Methode den Zugriff auf nicht zugewiesenen Speicherplatz ermöglichen. Erfinden Sie keine Wiederherstellung.
Ein AD1-Image lässt sich nicht physisch einbinden	Dies ist eine Einschränkung des Inhaltstyps. Verwenden Sie das zulässige logische Einbinden.
Ein Hashwert unterscheidet sich nach einer Konvertierung	Bestimmen Sie, was sich geändert hat: Struktur, Metadaten, Inhalt oder das verglichene Objekt. Erklären Sie dies nicht automatisch zur Fälschung.
Der Inhalt muss analysiert werden	Fügen Sie das Image zu Autopsy oder einer anderen Plattform hinzu; verwechseln Sie Erfassung nicht mit vollständiger Analyse.

10. Übung mit fiktiven Dateien

Verwenden Sie den Laborordner, um die Optionen kennenzulernen, ohne mit einem realen Datenträger zu arbeiten.

29. Öffnen Sie FTK Imager und wählen Sie Ordnerinhalt, nicht Ihr Hauptlaufwerk.
30. Wählen Sie nur den entpackten fiktiven Ordner aus.
31. Legen Sie ein neues Ziel außerhalb dieses Ordners fest.
32. Fügen Sie Demonstrationsmetadaten ohne Namen von Personen oder Kunden hinzu.
33. Aktivieren Sie Überprüfung und Inhaltsverzeichnis.
34. Prüfen Sie, wie Image, Fragmente und Protokolle gespeichert werden.
35. Öffnen Sie das Ergebnis als Beweiselement und suchen Sie `01_notas.txt`.
36. Exportieren Sie eine Arbeitskopie und eine Hashliste und vermerken Sie, welches Verfahren Sie für jede verwendet haben.
37. Dokumentieren Sie, warum diese Übung weder eine physische Erfassung noch die Wiederherstellung gelöschter Dateien nachweist.

Die Übung vermittelt den Arbeitsablauf der Oberfläche. Sie macht aus dem Ordner keinen Datenträger und aus dem erstellten Image kein gerichtliches Beweismittel.

11. Checkliste vor dem Bericht

- Befugnis und Umfang schriftlich dokumentiert.
- Quelle nach Möglichkeit anhand von Modell, Kapazität und Seriennummer identifiziert.
- Schreibblocker für die Originalquelle verwendet.
- Getrenntes Ziel und ausreichend Speicherplatz.
- Imagetyp, Fragmentierung und Komprimierung begründet.
- Vollständige Metadaten zu Fall und Beweismaterial.
- Überprüfung durchgeführt und Ergebnisse kontrolliert.
- Alle Segmente gemeinsam und lesbar.

- Lesefehler und Einschränkungen dokumentiert.
- Arbeitsdateien mit ihrer Herkunft verknüpft.
- Spätere Analyse von der Erfassung getrennt.
- Schlussfolgerung auf das beschränkt, was die Methode nachweist.

12. Offizielle Quellen und redaktionelle Kontrolle

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, Identifizierung, Sammlung, Erfassung und Erhaltung
44. NIST SP 800-86, forensische Verfahren bei der Reaktion auf Vorfälle

Das Handbuch 8.2 wurde für diese Adaptation vollständig gelesen. Es enthält Funktionen verschiedener Versionen und Produkte; nicht alle gehören zur kostenlosen Edition von FTK Imager. Prüfen Sie vor der Nutzung einer Pro-Funktion oder einer mobilen Erfassungsfunktion die jeweilige Lizenz und Dokumentation.

Dieser Leitfaden ist Lernmaterial von Jocsan Laguna, keine offizielle Veröffentlichung von Exterro und keine Rechtsberatung. Redaktionelle Überprüfung: 15. November 2026.