TEQUILA SO
Jocsan Laguna

Kostenlose Tools für die Computerforensik

Autopsy · FTK Imager · ExifTool · PhotoRec · Volatility

PRAXISLEITFADEN · 2026



Inhalt

1. Das Werkzeug richtet sich nach der Frage ... 3
2. FTK Imager: Erfassung und Vorschau ... 3
Erster Arbeitsablauf ... 3
3. Autopsy: Analyse und Zeitachse ... 4
Erster Arbeitsablauf ... 4
4. ExifTool: konkrete Metadaten von Dateien ... 4
Grundlegende Lektüre ohne Dateiveränderung ... 4
5. PhotoRec: signaturbasierte Wiederherstellung ... 5
Verantwortungsvoller Arbeitsablauf ... 5
6. Volatility 3: Arbeitsspeicher unter Analyse ... 5
7. Ein kleiner, überprüfbarer Arbeitsablauf ... 6
8. Fiktives Labor und Entscheidungsübung ... 7
9. Regeln zur Vermeidung schwerer Fehler ... 7
10. Offizielle Quellen und geprüfte Versionen ... 7

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

Eine Sammlung von Programmen ersetzt keine Methode. Dieser Leitfaden stellt fünf Werkzeuge vor, weil sie unterschiedliche Fragen beantworten: FTK Imager für Erfassung und Vorschau, Autopsy für die Analyse, ExifTool für Metadaten, PhotoRec für die signaturbasierte Wiederherstellung und Volatility 3 für Arbeitsspeicher.

1. Das Werkzeug richtet sich nach der Frage

Bevor Sie ein Programm öffnen, notieren Sie, was Sie wissen möchten, welche Quelle vorliegt und was nicht verändert werden darf. Autorisierung und Beweissicherung hängen nicht vom Preis der Software ab.

Frage	Werkzeug	Erwartbares Ergebnis	Was nicht bewiesen wird
Ich muss ein Image erstellen oder grundlegende Inhalte prüfen.	FTK Imager	Image, Vorschau, Export und Überprüfung.	Keine vollständige Fallanalyse.
Ich muss Dateien, Aktivitäten und Chronologie untersuchen.	Autopsy	Artefakte, Suchvorgänge, Tags, Zeitachse und Berichte.	Keine automatische Authentizität oder Urheberschaft.
Ich muss wissen, welche Metadaten eine Datei enthält.	ExifTool	Vorhandene Felder und Unterschiede zwischen Dateien.	Dass Datum oder Ort zwangsläufig zutreffen.
Ich muss versuchen, Inhalte anhand von Signaturen wiederherzustellen.	PhotoRec	Wiederherstellbare Dateien aus einer kompatiblen Kopie oder einem kompatiblen Image.	Keine Namen, Ordner, Vollständigkeit oder Erfolgsgarantie.
Ich muss ein Speicherabbild untersuchen.	Volatility 3	Prozesse, Verbindungen und Artefakte in diesem Speicherabbild.	Nicht den vollständigen Systemzustand oder dessen Verlauf.

Kostenlos bedeutet nicht harmlos. Das Lesen einer Quelle kann vertrauliche Daten offenlegen; das Ausführen einer Datei kann Malware aktivieren; das Schreiben an das falsche Ziel kann Beweise vernichten.

2. FTK Imager: Erfassung und Vorschau

FTK Imager erstellt Images, zeigt Dateien in der Vorschau, exportiert Inhalte und überprüft die Integrität. Das offizielle Handbuch 8.2 empfiehlt einen Hardware-Schreibblocker für die Erfassung eines Originaldatenträgers.

Erster Arbeitsablauf

1. Bestimmen Sie Quelle, Autorisierung und ein getrenntes Ziel.
2. Öffnen Sie **File > Create Disk Image**.
3. Bestätigen Sie die Quelle anhand von Modell, Kapazität und Seriennummer, nicht nur anhand des Laufwerksbuchstabens.
4. Wählen Sie Format, Fragmentierung und Komprimierung passend zum späteren Arbeitsablauf.

5. Aktivieren Sie die Überprüfung bei der Erstellung und bewahren Sie gegebenenfalls das Inhaltsverzeichnis auf.
6. Prüfen Sie Zusammenfassung, Hashwerte und Lesefehler.

Beginnen Sie nicht mit der Analyse, solange die Quelle nicht eindeutig bestimmt ist. Das Einbinden eines Images ersetzt keinen Schreibschutz für den Originaldatenträger.

Offizielle Quellen: Exterro FTK Imager 8.2 User Guide und Exterro FTK Downloads.

3. Autopsy: Analyse und Zeitachse

Autopsy organisiert einen Fall, fügt Datenquellen hinzu, führt Ingest-Vorgänge aus und erzeugt Artefakte. Die Referenzversion dieses Kits ist 4.23.0.

Erster Arbeitsablauf

7. Erstellen Sie einen Fall mit einem neuen Ordner.
8. Fügen Sie ein Image, einen kontrollierten Datenträger oder autorisierte logische Dateien hinzu.
9. Wählen Sie nur die für die Frage erforderlichen Module aus.
10. Warten Sie den Abschluss der Ingest-Vorgänge ab, bevor Sie Schlussfolgerungen ziehen.
11. Suchen Sie Inhalte, prüfen Sie ihren Speicherort und versehen Sie relevante Objekte mit Tags.
12. Verwenden Sie Timeline mit einem dokumentierten Zeitfenster und einer dokumentierten Zeitzone.
13. Erstellen Sie einen Bericht über markierte Elemente und ergänzen Sie Methode und Einschränkungen außerhalb der automatischen Ausgabe.

Logical Files entspricht nicht einem vollständigen Datenträger. Diese Methode untersucht weder nicht zugewiesenen Speicherplatz noch gelöschte Dateien auf dem Gerät; verwenden Sie sie für Übungen mit autorisierten Dokumenten, nicht für das Versprechen einer Wiederherstellung.

Konfigurieren Sie für die Übersetzung Bing oder Google mit einem eigenen Konto und wählen Sie **Test**. Aktivieren Sie anschließend **Translate Text** in View Options. Behalten Sie die Spalte **Original Name** bei und prüfen Sie Verneinungen, Eigennamen und juristische Begriffe anhand des Originaltexts.

Offizielle Quellen: Download, Quick Start, Data Sources, Timeline, Machine Translation und Reporting.

4. ExifTool: konkrete Metadaten von Dateien

ExifTool liest, schreibt und bearbeitet Metadaten in zahlreichen Formaten. Die für diese Ausgabe geprüfte Referenz ist **13.63, veröffentlicht am 10. November 2026**. Die offizielle Website bietet Pakete und Prüfsummen; verwenden Sie keine Kopien von fremden Websites.

Grundlegende Lektüre ohne Dateiveränderung

Öffnen Sie ein Terminal in einer Kopie des Labors und führen Sie Folgendes aus:

```
exiftool 03_imagen_demo.png
```

Das Ergebnis zeigt die vorhandenen Felder. Es erfindet keine Datums-, Kamera- oder Ortsangaben, wenn diese fehlen. Das Bild des Labors wurde als Demonstration erstellt; sein Inhalt und seine Metadaten stellen keine echte Fotografie dar.

Um nur bestimmte Felder anzuzeigen:

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

Wenn ein Feld fehlt, ist auch sein Fehlen eine Information: Behaupten Sie nicht, dass ein Standort oder ein Aufnahmegerät vorhanden ist.

Um Etikettennamen statt Beschreibungen anzuzeigen:

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

Um zwei Dateien ohne System- und zusammengesetzte Etiketten zu vergleichen:

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

Diese Befehle lesen und vergleichen, ohne die Beweise zu verändern. Schreiben Sie Metadaten nur in einer Arbeitskopie und bewahren Sie das Original auf; ExifTool kann beim Schreiben Sicherungskopien mit dem Suffix `_original` erstellen.

Metadaten sind keine Tatsachen. Ein Benutzer, eine Anwendung oder eine Konvertierung kann Datum, Autor, GPS oder Beschreibung verändern. Prüfen Sie die Herkunft und bestätigen Sie sie mit anderen Quellen.

Offizielle Quellen: ExifTool by Phil Harvey, Anwendungsdokumentation und Häufige Fragen.

5. PhotoRec: signaturbasierte Wiederherstellung

PhotoRec sucht anhand von Dateisignaturen nach Daten, auch wenn das Dateisystem beschädigt oder neu formatiert wurde. Es ist kostenlos, quelloffen und wird zusammen mit TestDisk vertrieben.

Der Zugriff auf die Quelle erfolgt schreibgeschützt, dennoch müssen Sie ein anderes Ziel für die wiederhergestellten Dateien wählen. Schreiben Sie nicht in dieselbe Partition, in der die Daten verloren gingen: Sie könnten die wiederherzustellenden Daten überschreiben.

Verantwortungsvoller Arbeitsablauf

14. Beenden Sie die Nutzung der Quelle, um Überschreibungen zu reduzieren.
15. Erstellen Sie ein Image oder wählen Sie eine autorisierte Arbeitskopie.
16. Führen Sie PhotoRec auf dieser Kopie aus, nicht auf dem Original.
17. Wählen Sie ein anderes Ziel für die Ergebnisse.
18. Prüfen Sie die wiederhergestellten Dateien, ihren Inhalt und ihre Beziehung zur Quelle.
19. Dokumentieren Sie, was gelesen werden konnte und was unvollständig blieb.

PhotoRec stellt nicht die gesamte Vergangenheit wieder her. Namen und Ordner gehen häufig verloren; Fragmentierung kann zu unvollständigen Dateien führen; die Wiederherstellung von Inhalten beweist weder, wer sie erstellt hat, noch, was geschehen ist.

Offizielle Quellen: PhotoRec ES und TestDisk Download.

6. Volatility 3: Arbeitsspeicher unter Analyse

Volatility 3 analysiert Speicherabbilder mithilfe von Plugins. Es ersetzt nicht die Erfassung: Sie benötigen ein kompatibles Speicherabbild und die passenden Symbole für das untersuchte System.

Führen Sie die Befehle mit einem Testabbild aus, nicht mit personenbezogenen Daten Dritter. Ein Beispiel für eine erste Lektüre ist:

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

So prüfen Sie die im Speicherabbild aufgezeichneten Prozesse:

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

So prüfen Sie Verbindungen, die das Speicherabbild und das Plugin analysieren können:

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

Die Datei `memoria_demo.raw` ist nur ein illustrativer Name: Dieses Kit enthält kein Speicherabbild. Für die Befehle benötigen Sie eine echte Lernquelle und die dokumentierten Voraussetzungen. Laden Sie keine Dumps aus unbekannten Quellen herunter, die sensible Daten oder Malware enthalten könnten.

Ein Speicherabbild zeigt einen Moment, nicht die gesamte Geschichte. Sichtbare Prozesse und Verbindungen hängen vom Zeitpunkt, der Erfassung und der Kompatibilität der Symbole ab.

Offizielle Quellen: Volatility 3 auf GitHub und Generierte Dokumentation.

7. Ein kleiner, überprüfbarer Arbeitsablauf

Mit fünf Werkzeugen können Sie einen grundlegenden Arbeitsablauf abdecken, ohne unnötige Programme zu installieren.

Schritt	Maßnahme	Arbeitsnachweis
Befugnis	Ziel, Quelle und Berechtigungen abgrenzen.	Umfang, Verwahrer und Ausschlüsse.
Erfassung	Ein Image oder eine kontrollierte Kopie erstellen.	Methode, Version, Datum, Ziel und Hashwert.
Überprüfung	Quelle in FTK Imager öffnen und Dateien finden.	Pfad, Format und erste Beobachtungen.
Analyse	Autopsy mit ausgewählten Ingest-Modulen verwenden.	Artefakte, Suchvorgänge, Tags und Zeitachse.
Metadaten	ExifTool für bestimmte Kopien verwenden.	Vorhandene Felder und Unterschiede, ohne das Original zu verändern.
Wiederherstellung	PhotoRec verwenden, wenn die Frage es rechtfertigt.	Geprüfte Ergebnisse und Grenzen der Wiederherstellung.
Arbeitsspeicher	Bei Bedarf ein Speicherabbild mit Volatility analysieren.	Kompatible Quelle, Plugins und Ausgaben.
Bericht	Methode, Befunde und Einschränkungen erläutern.	Reproduzierbare Überprüfung und zitierte Quellen.

Nicht in jedem Fall müssen alle Werkzeuge verwendet werden. Ockhams Rasiermesser gilt auch hier: Wählen Sie das Werkzeug, das die Frage mit der geringsten Veränderung beantwortet.

8. Fiktives Labor und Entscheidungsübung

Die ZIP-Datei enthält Dokumente, eine EML-Datei, ein Bild und eigens für den Unterricht erstellte Notizen. Es handelt sich nicht um die Aufzeichnung eines realen Falls.

20. Berechnen Sie den Hashwert der ZIP-Datei vor dem Entpacken und vergleichen Sie ihn mit `SHA256SUMS.txt`.
21. Fügen Sie den Ordner in Autopsy als Logical Files hinzu.
22. Suchen Sie nach `lavanda` und öffnen Sie die entsprechende Datei.
23. Prüfen Sie `03_imagen_demo.png` mit ExifTool und notieren Sie, welche Felder vorhanden sind und welche fehlen.
24. Öffnen Sie `02_correo_demo.eml` und prüfen Sie, ob der Absender eine für Beispiele reservierte Domain verwendet.
25. Dokumentieren Sie, warum diese Dateien keine Rückschlüsse auf Versand, Authentizität, Standort oder Absicht zulassen.
26. Schreiben Sie eine Ausgabe aus fünf Zeilen: Quelle, Methode, Befund, Einschränkung und nächste Überprüfung.

Führen Sie keine Arbeitsspeicherbefehle mit diesem nicht vorhandenen Testabbild aus. Das Labor vermittelt das Lesen und Analysieren von Dateien; für Arbeitsspeicher wird eine andere autorisierte Quelle benötigt.

9. Regeln zur Vermeidung schwerer Fehler

- Autorisieren Sie vor jedem Zugriff, auch wenn die Technik einfach ist.
- Bewahren Sie das Original auf und analysieren Sie eine Kopie.
- Verwenden Sie ein getrenntes Ziel für Images und wiederhergestellte Dateien.
- Laden Sie nur von der offiziellen Website herunter und überprüfen Sie die Integrität, sofern verfügbar.
- Führen Sie unbekannte Dateien weder auf Ihrem persönlichen Gerät noch in Produktionsnetzen aus.
- Dokumentieren Sie Version, Datum, Zeitzone, Parameter und Bearbeiter.
- Unterscheiden Sie Befund, Interpretation und Schlussfolgerung.
- Stellen Sie Metadaten nicht als Urheberschaft, tatsächliches Datum oder automatischen Standort dar.
- Versprechen Sie weder eine vollständige Wiederherstellung noch das Nichtvorhandensein von Dateien, nur weil diese in einer Suche nicht erscheinen.
- Geben Sie Schlüssel, Anmeldedaten oder vertrauliche Daten ohne Autorisierung nicht an einen externen Übersetzungsdienst weiter.

10. Offizielle Quellen und geprüfte Versionen

27. Autopsy 4.23.0: Benutzerdokumentation
28. Exterro FTK Imager 8.2 User Guide
29. ExifTool 13.63: offizielle Website und Downloads
30. ExifTool Application Documentation
31. PhotoRec ES, CGSecurity
32. Volatility 3: offizielles Repository
33. Volatility 3: Dokumentation

34. ISO/IEC 27037
35. NIST SP 800-86

Die Versionen wurden am 15. November 2026 überprüft. Oberflächen und Formate ändern sich: Konsultieren Sie vor der Anwendung eines Verfahrens in einem realen Fall stets die aktuelle Dokumentation. Dieser Leitfaden dient der Schulung und ersetzt weder Rechtsberatung noch Autorisierung oder fachliche Prüfung.