TEQUILA SO
Jocsan Laguna

कंप्यूटर फोरेंसिक के लिए निःशुल्क उपकरण

Autopsy · FTK Imager · ExifTool · PhotoRec · Volatility

व्यावहारिक मार्गदर्शिका · 2026



विषय-सूची

1. प्रश्न के अनुसार उपकरण चुनें 3
2. FTK Imager: अधिग्रहण और पूर्वावलोकन 3
प्रारंभिक कार्यप्रवाह 3
3. Autopsy: विश्लेषण और कालक्रम 4
प्रारंभिक कार्यप्रवाह 4
4. ExifTool: विशिष्ट फ़ाइल मेटाडेटा 4
फ़ाइलों को बदले बिना मूल पठन 4
5. PhotoRec: फ़ाइल सिग्नेचर से पुनर्प्राप्ति 5
उत्तरदायी कार्यप्रवाह 5
6. Volatility 3: मेमोरी विश्लेषण 5
7. संक्षिप्त, लेखा-परीक्षण योग्य कार्यप्रवाह 6
8. काल्पनिक प्रयोगशाला और निर्णय लेने का अभ्यास 6
9. गंभीर गलतियों से बचने के लिए नियम 7
10. आधिकारिक स्रोत और सत्यापित संस्करण 7

यह स्पेनिश संस्करण से मशीन-सहायित अनुवाद है। संपादकीय संदर्भ के लिए स्पेनिश मूल देखें।

प्रोग्रामों का संग्रह कार्यविधि का विकल्प नहीं है। यह मैनुअल पाँच उपकरण प्रस्तुत करता है क्योंकि वे अलग प्रश्नों का उत्तर देते हैं: FTK Imager अधिग्रहण और पूर्वावलोकन के लिए, Autopsy विश्लेषण के लिए, ExifTool मेटाडेटा के लिए, PhotoRec फ़ाइल सिग्नेचर से पुनर्प्राप्ति के लिए और Volatility 3 मेमोरी विश्लेषण के लिए।

1. प्रश्न के अनुसार उपकरण चुनें

किसी भी प्रोग्राम को खोलने से पहले, लिखें कि आप क्या जानना चाहते हैं, आपके पास कौन सा स्रोत है और आप क्या नहीं बदल सकते। प्राधिकरण और संरक्षण सॉफ्टवेयर की कीमत पर निर्भर नहीं करते हैं।

प्रश्न	उपकरण	जिस परिणाम की अपेक्षा की जा सकती है	जो सिद्ध नहीं होता
मुझे इमेज बनानी है या उसका मूल सामग्री देखनी है।	FTK Imager	इमेज, पूर्वावलोकन, निर्यात और सत्यापन।	पूरे केस का विश्लेषण।
मुझे फ़ाइलों, गतिविधि और कालक्रम की जांच करने की आवश्यकता है।	Autopsy	आर्टिफ़ैक्ट, खोज, टैग, कालक्रम और रिपोर्ट।	स्वतः प्रामाणिकता या लेखकता।
मुझे यह जानने की ज़रूरत है कि एक फ़ाइल में कौन से मेटाडेटा हैं।	ExifTool	मौजूद फ़ील्ड और फ़ाइलों के बीच अंतर।	तिथि या स्थान आवश्यक रूप से वास्तविक होना।
मुझे फ़ाइल सिग्नेचर से सामग्री पुनः प्राप्त करने का प्रयास करना है।	PhotoRec	संगत प्राप्त या इमेज से पुनः प्राप्त की जा सकने वाली फ़ाइलें।	नाम, फ़ोल्डर, पूर्णता या सफलता की गारंटी नहीं।
मुझे मेमोरी कैप्चर का विश्लेषण करना है।	Volatility 3	उस कैप्चर में मौजूद प्रोसेस, कनेक्शन और आर्टिफ़ैक्ट।	सिस्टम की पूरी स्थिति या उसका इतिहास।

निःशुल्क का अर्थ हानिरहित नहीं है। स्रोत पढ़ने से गोपनीय डेटा उजागर हो सकता है; नमूना चलाने से मैलवेयर सक्रिय हो सकता है; गलत गंतव्य पर लिखने से साक्ष्य नष्ट हो सकता है।

2. FTK Imager: अधिग्रहण और पूर्वावलोकन

FTK Imager इमेज बनाता, फ़ाइलें पूर्वावलोकन करता, सामग्री निर्यात करता और अखंडता सत्यापित करता है। 8.2 आधिकारिक मार्गदर्शिका मूल ड्राइव का अधिग्रहण करते समय हार्डवेयर राइट-ब्लॉकर की सिफ़ारिश करती है।

प्रारंभिक कार्यप्रवाह

1. स्रोत, प्राधिकरण और अलग गंतव्य पहचानें।
2. **File > Create Disk Image** खोलें।
3. मॉडल, क्षमता और क्रमांक से स्रोत की पुष्टि करें, केवल अक्षर से नहीं।
4. बाद के कार्यप्रवाह के अनुसार प्रारूप, खंड और संपीड़न चुनें।
5. बनाते समय सत्यापन सक्रिय करें और आवश्यकता अनुसार सामग्री-सूची रखें।
6. सारांश, हैश और पढ़ने की त्रुटियों की जांच करें।

यदि स्रोत अभी स्पष्ट नहीं है तो विश्लेषण से शुरुआत न करें। मूल डिस्क के राइट-ब्लॉक के विकल्प के रूप में इमेज माउंट करना भी उपयोग न करें।

आधिकारिक स्रोत: Exterro FTK Imager 8.2 User Guide और Exterro FTK Downloads.

3. Autopsy: विश्लेषण और कालक्रम

Autopsy केस व्यवस्थित करता, डेटा स्रोत जोड़ता, इनजेस्ट चलाता और आर्टिफ़ैक्ट बनाता है। इस किट का संदर्भ संस्करण 4.23.0 है।

प्रारंभिक कार्यप्रवाह

7. एक नए फ़ोल्डर के साथ एक मामला बनाएं।
8. एक छवि जोड़ें, एक नियंत्रित डिस्क या अधिकृत लॉजिक फ़ाइलें।
9. केवल प्रश्न के लिए आवश्यक मॉड्यूल चुनें।
10. निष्कर्ष अंतिम करने से पहले इनजेस्ट पूरे होने दें।
11. सामग्री खोजें, उसके स्थान की जाँच करें और प्रासंगिक को टैग करें।
12. Timeline में दस्तावेज़ित समय-खिड़की और समयक्षेत्र उपयोग करें।
13. टैग किए गए तत्वों की रिपोर्ट उत्पन्न करें और स्वचालित परिणाम के बाहर विधि और सीमाएँ जोड़ें।

Logical Files पूर्ण डिस्क के बराबर नहीं है। यह विधि डिवाइस के गैर-आवंटित स्थान या हटाई गई फ़ाइलों की जाँच नहीं करती; इसे अधिकृत दस्तावेज़ों के अभ्यास के लिए उपयोग करें, पुनर्प्राप्ति का वादा करने के लिए नहीं।

अनुवाद करने के लिए, अपने खाते के साथ बिंग या Google सेट करें और **Test** दबाएं। फिर **Translate Text** को View Options में सक्रिय करें। **Original Name** कॉलम को सहेजें और मूल पाठ के साथ अस्वीकरण, नाम और कानूनी शब्दों की जांच करें।

आधिकारिक स्रोत: डाउनलोड, त्वरित प्रारंभ, डेटा स्रोत, Timeline, मशीन अनुवाद और रिपोर्टिंग.

4. ExifTool: विशिष्ट फ़ाइल मेटाडेटा

ExifTool कई प्रारूपों के मेटाडेटा पढ़, लिख और संपादित कर सकता है। इस संस्करण के लिए सत्यापित संदर्भ **13.63, 10 नवंबर 2026 को प्रकाशित** है। आधिकारिक पृष्ठ पर पैकेज और चेकसम उपलब्ध हैं; अन्य साइटों की प्रतियाँ उपयोग न करें।

फ़ाइलों को बदले बिना मूल पठन

प्रयोगशाला की एक प्रति में एक टर्मिनल खोलें और निष्पादित करें:

```
exiftool 03_imagen_demo.png
```

परिणाम मौजूद फ़ील्ड दिखाता है। यह अनुपस्थित तिथि, कैमरा या स्थान नहीं बनाता। प्रयोगशाला की छवि प्रदर्शन के लिए बनाई गई है, इसलिए उसकी सामग्री और मेटाडेटा वास्तविक फ़ोटोग्राफ़ का प्रतिनिधित्व नहीं करते।

केवल कुछ क्षेत्रों को दिखाने के लिए:

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

यदि कोई फ़ील्ड मौजूद नहीं है, तो इसकी अनुपस्थिति भी जानकारी है: यह दावा न करें कि कोई स्थान या कैप्चर डिवाइस मौजूद है।

विवरणों के बजाय टैग के नाम देखने के लिए:

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

सिस्टम और कम्पोजिट टैग के बिना दो फ़ाइलों की तुलना करने के लिएः

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

ये कमांड पढ़ते और तुलना करते हैं; साक्ष्य नहीं बदलते। मेटाडेटा लिखने से पहले हमेशा कार्य-प्रति पर काम करें और मूल रखें; ExifTool लिखते समय `_original` प्रत्यय वाले बैकअप बना सकता है।

मेटाडेटा तथ्य नहीं है। उपयोगकर्ता, एप्लिकेशन या रूपांतरण तिथि, लेखक, GPS या विवरण बदल सकते हैं। स्रोत जाँचें और अन्य स्रोतों से पुष्टि करें।

आधिकारिक स्रोत: ExifTool by Phil Harvey, आवेदन का दस्तावेजीकरण और अक्सर पूछे जाने वाले प्रश्न.

5. PhotoRec: फ़ाइल सिग्नेचर से पुनर्प्राप्ति

फ़ाइल सिस्टम क्षतिग्रस्त या पुनः प्रारूपित होने पर भी PhotoRec फ़ाइल सिग्नेचर से डेटा खोजता है। यह निःशुल्क और ओपन-सोर्स है तथा TestDisk के साथ वितरित होता है।

PhotoRec स्रोत को केवल पढ़ने के लिए उपयोग करता है, लेकिन पुनः प्राप्त फ़ाइलों के लिए दूसरा गंतव्य चुनना आवश्यक है। जिस विभाजन में डेटा खोया था उसी पर न लिखें; जिसे पुनः प्राप्त करना चाहते हैं उसे ओवरराइट कर सकते हैं।

उत्तरदायी कार्यप्रवाह

14. ओवरराइटिंग घटाने के लिए स्रोत का उपयोग रोकें।
15. इमेज बनाएँ या अधिकृत कार्य-प्रति चुनें।
16. उस प्रति पर PhotoRec चलाएँ, मूल पर नहीं।
17. परिणामों के लिए एक और गंतव्य चुनें।
18. पुनर्प्राप्त फ़ाइलों, उनकी सामग्री और स्रोत के साथ उनके संबंध की जांच करें।
19. क्या पढ़ा जा सका और क्या अधूरा रहा, दस्तावेज़ित करें।

PhotoRec पूरा अतीत वापस नहीं लाता। नाम और फ़ोल्डर प्रायः खो जाते हैं; खंडन से अधूरी फ़ाइलें बन सकती हैं; सामग्री मिल जाने से उसका निर्माता या घटना सिद्ध नहीं होती।

आधिकारिक स्रोत: PhotoRec ES और TestDisk Download.

6. Volatility 3: मेमोरी विश्लेषण

Volatility 3 प्लगइन से मेमोरी कैप्चर का विश्लेषण करता है। यह अधिग्रहण का विकल्प नहीं है: संगत कैप्चर और जाँचे जा रहे सिस्टम के लिए उपयुक्त प्रतीक चाहिए।

इसे परीक्षण कैप्चर पर चलाएँ, तीसरे पक्ष के व्यक्तिगत डेटा पर नहीं। प्रारंभिक पठन का उदाहरण इस प्रकार है:

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

कैप्चर में दर्ज प्रोसेस देखने के लिए:

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

कैप्चर और प्लगइन जिन कनेक्शनों का विश्लेषण करने देते हैं उन्हें देखने के लिए:

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

`memoria_demo.raw` केवल उदाहरण का नाम है: यह किट मेमोरी कैप्चर नहीं देती। कमांड चलाने के लिए वास्तविक शैक्षिक स्रोत और दस्तावेज़ित आवश्यकताएँ चाहिए। अज्ञात स्रोतों से डंप डाउनलोड न करें, उनमें संवेदनशील डेटा या मैलवेयर हो सकता है।

एक कैप्चर एक पल को दर्शाता है, पूरे इतिहास को नहीं। दृश्य प्रक्रियाएं और कनेक्शन समय, प्राप्ति और प्रतीकों की संगतता पर निर्भर करते हैं।

आधिकारिक स्रोत: GitHub पर Volatility 3 और उत्पन्न दस्तावेज.

7. संक्षिप्त, लेखा-परीक्षण योग्य कार्यप्रवाह

पाँच उपकरणों से अनावश्यक प्रोग्राम जमा किए बिना मूल कार्यप्रवाह पूरा किया जा सकता है।

चरण	कार्रवाई	काम का प्रमाण
प्राधिकरण	लक्ष्य, स्रोत और अनुमतियों को परिभाषित करें।	दायरा, जोखिमकारक और बाहिष्करण।
अधिग्रहण	इमेज या निर्यात्रित प्रति बनाना।	विधि, संस्करण, तिथि, निर्यात और हैश।
समीक्षा	FTK Imager में स्रोत खोल और फ़ाइलों का पता लगाएं।	मार्ग, प्रारूप और प्रारंभिक टिप्पणियाँ।
विश्लेषण	चुने हुए इनजस्ट के साथ Autopsy उपयोग करें।	आर्टिफ़ैक्ट, खोज, टैग और कालक्रम।
मेटाडेटा	ExifTool से विशेषताएँ प्राप्त की जाएँ।	मौजूद फ़ील्ड और अंतर, मूल को दोबारा लिखे बिना।
पुनर्प्राप्ति	PhotoRec का उपयोग करें जब प्रश्न इसे उचित बनाता है।	समीक्षित परिणाम और पुनर्प्राप्ति की सीमाएँ।
मेमोरी	जब आवश्यक हो तो Volatility से कैप्चर का विश्लेषण करें।	समर्थित स्रोत, प्लगइन और आउटपुट।
रिपोर्ट	विधि, निष्कर्ष और सीमाओं को समझाएँ।	दोहराने योग्य समीक्षा और उद्धृत स्रोत।

हर मामले में सभी उपकरण उपयोग करना आवश्यक नहीं है। ओकहम का उस्तरा यहाँ भी लागू होता है: न्यूनतम परिवर्तन के साथ सर्वोत्तम उत्तर देने वाला उपकरण चुनें।

8. काल्पनिक प्रयोगशाला और निर्णय लेने का अभ्यास

ZIP में विशेष रूप से शिक्षण के लिए बनाए गए दस्तावेज़, एक EML, एक छवि और नोट्स हैं। यह वास्तविक मामले का कैप्चर नहीं है।

20. ZIP के हैश की गणना करें और `SHA256SUMS.txt` के साथ तुलना करें।
21. Autopsy में Logical Files के रूप में फ़ोल्डर जोड़ें।
22. `lavanda` खोजें और संबंधित फ़ाइल खोलें।
23. `03_imagen_demo.png` को ExifTool के साथ देखें और नोट करें कि कौन से फ़ील्ड मौजूद हैं और कौन से नहीं।
24. `02_correo_demo.eml` खोलें और जांचें कि प्रेषक उदाहरणों के लिए एक आरक्षित डोमेन का उपयोग करता है।
25. रिकॉर्ड करें कि आप उन फ़ाइलों से प्रेषण, प्रामाणिकता, स्थान या इरादे का निष्कर्ष क्यों नहीं निकाल सकते हैं।
26. पांच पंक्तियों का एक आउटपुट लिखें: स्रोत, विधि, खोज, सीमा और अगले सत्यापन।

उस अनुपस्थित परीक्षण मेमोरी इमेज पर मेमोरी कमांड न चलाएँ। प्रयोगशाला फ़ाइल पठन और विश्लेषण सिखाती है; मेमोरी के लिए दूसरा अधिकृत स्रोत चाहिए।

9. गंभीर गलतियों से बचने के लिए नियम

- तकनीक सरल हो तो भी पहुँच से पहले अनुमति लें।
- मूल को सहेजें और एक प्रतिलिपि का विश्लेषण करें।
- पुनर्प्राप्त छवियों और फ़ाइलों के लिए एक अलग गंतव्य का उपयोग करें।
- केवल आधिकारिक साइट से डाउनलोड करें और उपलब्ध होने पर इसकी अखंडता की जांच करें।
- अपने व्यक्तिगत उपकरण या उत्पादन नेटवर्क पर अज्ञात नमूने न चलाएं।
- संस्करण, तिथि, समय क्षेत्र, पैरामीटर और ऑपरेटर रिकॉर्ड करें।
- खोज, व्याख्या और निष्कर्ष में भेद करें।
- मेटाडेटा को लेखकता, वास्तविक तिथि या स्वतः स्थान के रूप में प्रस्तुत न करें।
- पूर्ण पुनर्प्राप्ति का वादा न करें और खोज में न दिखने पर फ़ाइलें अस्तित्व में न होने का दावा न करें।
- बिना अनुमति के किसी बाहरी अनुवादक के साथ कुंजी, क्रेडेंशियल या गोपनीय डेटा साझा न करें।

10. आधिकारिक स्रोत और सत्यापित संस्करण

27. Autopsy 4.23.0: उपयोगकर्ता दस्तावेज
28. Exterro FTK Imager 8.2 User Guide
29. ExifTool 13.63: आधिकारिक पृष्ठ और डाउनलोड
30. ExifTool Application Documentation
31. PhotoRec ES, CGSecurity
32. Volatility 3: आधिकारिक रिपॉज़िटरी
33. Volatility 3: प्रलेखन
34. ISO/IEC 27037
35. NIST SP 800-86

15 नवंबर, 2026 को संस्करणों की समीक्षा की गई थी। इंटरफ़ेस और प्रारूप बदलते हैं: एक वास्तविक मामले में प्रक्रिया लागू करने से पहले हमेशा मौजूदा दस्तावेजों की जांच करें। यह मार्गदर्शिका शैक्षिक है और कानूनी सलाह, प्राधिकरण या पेशेवर समीक्षा की जगह नहीं लेती है।