TEQUILA SO
Jocsan Laguna

FTK Imager

अधिग्रहण, पूर्वावलोकन, हैश और दस्तावेज़ीकरण

व्यावहारिक मार्गदर्शिका 2026 · दस्तावेज़ 8.2



विषय-सूची

1. FTK Imager क्या करता है और क्या नहीं करता 3

1.1 मूल का नियम 3

2. अधिग्रहण की तैयारी 3

2.1 प्रयोगशाला में सुरक्षित अभ्यास 4

3. चरण-दर-चरण इमेज बनाना 4

4. प्रारूप, खंड और संपीड़न चुनना 4

5. परिणाम का सत्यापन और संरक्षण 5

6. स्रोत से संबंध बनाए रखते हुए पूर्वावलोकन और निर्यात 5

7. इमेज माउंट करना: पढ़ना, लिखना और सीमाएँ 6

8. मेमोरी कैप्चर: अलग प्रकार की प्रक्रिया 6

9. सामान्य त्रुटियाँ और सुरक्षित निर्णय 6

10. काल्पनिक फ़ाइलों के साथ अभ्यास 7

11. रिपोर्ट से पहले जाँच-सूची 7

12. आधिकारिक स्रोत और संपादकीय नियंत्रण 7

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

FTK Imager फोरेंसिक इमेज बनाने, साक्ष्य का पूर्वावलोकन, फ़ाइलें निर्यात करने और अखंडता जाँचने के लिए है। इसका मुख्य कार्य विश्लेषण का स्थान लेना नहीं, बल्कि दस्तावेज़ित स्रोत से और मूल पर निर्भर किए बिना विश्लेषण संभव बनाना है।

यह मार्गदर्शिका कार्यप्रवाह को सरल भाषा में समझाती है। यह शाब्दिक अनुवाद या Exterro की आधिकारिक मार्गदर्शिका नहीं है। मेनू 8.2 के दस्तावेज़ पर आधारित हैं और उन्हें स्थापित संस्करण से मिलान करना चाहिए।

1. FTK Imager क्या करता है और क्या नहीं करता

एप्लिकेशन से बिट-दर-बिट प्रतियाँ बनाई जा सकती हैं, सामग्री देखी जा सकती है, पढ़ने के लिए इमेज माउंट की जा सकती हैं, फ़ाइलें निर्यात की जा सकती हैं, हैश सूचियाँ बनाई जा सकती हैं और कुछ परिस्थितियों में मेमोरी कैप्चर की जा सकती है। Autopsy या दूसरे प्लेटफ़ॉर्म से विश्लेषण करने से पहले यह विशेष उपयोगी है।

आवश्यकता	FTK Imager	Autopsy
डिस्क या फ़ाइल का एक छाप बनाना।	यह इसका केंद्रीय काम है।	यह उसके मुख्य कार्यप्रवाह का पहला चरण नहीं है।
फ़ोल्डर और फ़ाइलों का पूर्वावलोकन करें।	साक्ष्य-वृक्ष, सूची, गुण और व्यूअर।	वृक्ष, परिणाम और सामग्री, जोचक विश्लेषण मॉड्यूल सहित।
केस का विश्लेषण और सहसंबंध।	पूर्ण केस प्लेटफ़ॉर्म की तुलना में सीमित।	इनजेस्ट, खोज, कालक्रम, संचार, रिपोर्ट और अधिक।
अखंडता की जाँच करें।	अधिग्रहण के दौरान और बाद में सत्यापन।	समर्थित स्रोतों के लिए Data Source Integrity और अन्य नियंत्रण।

बनी हुई इमेज पूरी जाँच नहीं है। यह संरक्षित प्रस्तुति है, जिसे अभी समीक्षा और संदर्भ चाहिए।

1.1 मूल का नियम

आधिकारिक मार्गदर्शिका ड्राइव की इमेज बनाते समय **हार्डवेयर राइट-ब्लॉकर** की सिफ़ारिश करती है। इससे कनेक्ट करने पर ऑपरेटिंग सिस्टम मूल स्रोत को नहीं बदल पाता।

तीन क्रियाओं को भ्रमित न करें:

- **इमेज बनाना:** स्रोत की प्रति बनाता है।
- **पढ़ने के लिए इमेज माउंट करना:** उस प्रति को देखने देता है; इमेज मूल का राइट-ब्लॉकर नहीं बन जाती।
- **कार्य-प्रति पर काम करना:** मूल को विश्लेषण प्रक्रिया से बाहर रखता है।

2. अधिग्रहण की तैयारी

FTK Imager खोलने से पहले केस और डिवाइस दस्तावेज़ित करें। बटन चुनने की जल्दबाजी में अक्सर गलत डिस्क की पूरी इमेज बन जाती है।

1. दायरा, स्रोत और विधि अधिकृत करें।
2. उपलब्ध होने पर मॉडल, क्षमता और क्रमांक पहचानें।
3. मूल स्रोत के लिए हार्डवेयर लेखन ब्लॉकर का उपयोग करें।

4. स्रोत से अलग एक गंतव्य का उपयोग करें, पर्याप्त ऊर्जा और स्थान के साथ।
5. एक फ़ोल्डर इमेज के लिए और दूसरा लॉग और रिपोर्ट के लिए तैयार करें।
6. FTK Imager का संस्करण, दिनांक, समयक्षेत्र और ऑपरेटर दर्ज करें।

गंतव्य में पूरी इमेज, खंड, अधिग्रहण जानकारी और कार्य-प्रतियों के लिए पर्याप्त स्थान होना चाहिए। "डिस्क समाहित हो जाता है" का अर्थ हमेशा "प्रक्रिया समाहित हो जाती है" नहीं होता।

जिस डिस्क का अधिग्रहण कर रहे हैं उसी पर इमेज कभी न सहेजें। इससे जो कुछ संरक्षित करना चाहते हैं वह बदल या नष्ट हो सकता है।

2.1 प्रयोगशाला में सुरक्षित अभ्यास

डाउनलोड करने योग्य लैब में सबूत डिस्क को जोड़ने की आवश्यकता नहीं है। इंटरफ़ेस और विकल्पों को सीखने के लिए फ़ाइलों के एक तार्किक संग्रह के रूप में काल्पनिक फ़ोल्डर का उपयोग करें। अपने मुख्य डिस्क या अन्य लोगों के उपकरणों के साथ भौतिक अधिग्रहण का अभ्यास न करें।

3. चरण-दर-चरण इमेज बनाना

मूल मार्ग **File > Create Disk Image** है। विज़ार्ड से स्रोत और गंतव्य चुना जा सकता है।

7. आवश्यकता अनुसार स्रोत का प्रकार चुनें: भौतिक ड्राइव, तार्किक ड्राइव, मौजूदा इमेज या फ़ोल्डर की सामग्री।
8. केवल ड्राइव अक्षर से नहीं, पहचानकर्ताओं से सटीक डिवाइस की पुष्टि करें।
9. स्रोत से अलग गंतव्य फ़ोल्डर चुनें।
10. बिना एक्सटेंशन का नाम दें और केस पहचानकर्ता से जोड़ें।
11. उपलब्ध मेटाडेटा भरें: केस, साक्ष्य, विवरण, परीक्षक और नोट्स।
12. इमेज प्रकार, खंड और संपीड़न की समीक्षा करें।
13. बनने के बाद अखंडता जाँचने के लिए **Verify images after they are created** सक्रिय करें।
14. उपलब्ध पथ और मेटाडेटा रखने के लिए **Create directory listings of all files in the image** पर विचार करें।
15. **Start** दबाने से पहले सब कुछ जाँचें।
16. पढ़ने की त्रुटियों सहित अधिग्रहण लॉग और सारांश रखें।

यदि स्रोत पर संदेह है तो Start न दबाएँ। प्राप्ति-पत्र पर लौटकर उसकी पुष्टि करें।

4. प्रारूप, खंड और संपीड़न चुनना

प्रारूप स्रोत और बाद के प्रवाह पर निर्भर करता है, न कि आदत पर।

विकल्प	इसका अर्थ	क्या जाँचें
Raw / DD	प्रत्यक्ष प्रति, व्यापक संगतता और जानबूझ कर संपीड़न नहीं।	इसके लिए स्रोत और टुकड़ों के अनुरूप स्थान की आवश्यकता होती है।
E01	मेटाडेटा और फोंपप्रवाह के अनुसार संपीड़न विकल्पों वाली साक्ष्य इमेज।	विश्लेषण उपकरणों के साथ संगतता और मेटाडेटा संरक्षण।
AD1	अनुकूलित सामग्री का तार्किक छोर।	यह डिस्क की भौतिक इमेज नहीं है और उसका पूरा ज्यामिति नहीं रखता।

खंड	परिणाम को सीमित आकार की कई फ़ाइलों में विभाजित करता है।	विश्लेषण और सत्यापन के लिए सभी खंड साथ रहने चाहिए।
संपीड़न 0–9	चयनित प्रारूप के अनुसार गति और आकार के बीच संतुलन।	अधिक संपीड़न में प्रक्रिया का समय अधिक लग सकता है।

मार्गदर्शिका 8.2 उस कार्यप्रवाह में **1500 MB** का डिफ़ॉल्ट खंड-आकार बताती है। इसे सार्वभौमिक नियम न बनाएँ। स्टोरेज, परिवहन और विश्लेषण के अनुसार चुनें; जहाँ विकल्प अनुमत हो, मान 0 होने पर परिणाम खंडों में नहीं बँटता।

सामग्री बिट-दर-बिट समान रहेगी इस उम्मीद में प्रारूप न बदलें। प्रस्तुति दिखने वाली जानकारी रखते हुए भी संरचना और हैश बदल सकती है। मूल और व्युत्पन्न का संबंध दस्तावेज़ित करें।

5. परिणाम का सत्यापन और संरक्षण

समाप्त होने पर इमेज को मान्य मानने से पहले सारांश जाँचें। बनाने के दौरान सत्यापन बने हुए हैश की तुलना करके अंतर पहचानने में मदद करता है। मिलान न हो तो परिणाम को सही मानकर उपयोग न करें।

17. मूल और इमेज के हैश दर्ज करें; एल्गोरिदम और ऑब्जेक्ट बताएँ।
18. पढ़े गए सेक्टर और पढ़ने की त्रुटियाँ जाँचें।
19. जांचें कि सभी टुकड़े एक ही फ़ोल्डर में हैं।
20. अधिग्रहण लॉग और बनाई गई सामग्री-सूची रखें।
21. इमेज को साक्ष्य के रूप में खोलकर पुष्टि करें कि उसे बिना बदलाव पढ़ा जा सकता है।
22. एक बाद की जांच की गणना करें और जब उपयुक्त हो, तो इसे दर्ज किए गए मूल्य के साथ तुलना करें।

मार्गदर्शिका 8.2 एप्लिकेशन के कई हैशिंग कार्यों के लिए **MD5 और SHA-1** बताती है। यदि आपकी प्रक्रिया में अतिरिक्त SHA-256 चाहिए, तो उपयुक्त उपकरण से परिकलित करें और दर्ज करें कि यह दूसरी प्रक्रिया है, FTK Imager का कोई काल्पनिक फ़ंक्शन नहीं।

मिलान सिद्ध करता है कि जाँचों के बीच ऑब्जेक्ट नहीं बदला; सामग्री की सत्यता या स्रोत की वैधता नहीं।

6. स्रोत से संबंध बनाए रखते हुए पूर्वावलोकन और निर्यात

साक्ष्य-वृक्ष स्रोत और फ़ोल्डर दिखाता है; फ़ाइल सूची चयन के अनुसार बदलती है; गुण-पैनल प्रकार, स्थान, आकार और तिथियाँ दिखाता है; व्यूअर सामग्री प्रस्तुत करता है।

किसी फ़ाइल को देखने के लिए:

23. **Add Evidence Item** से इमेज जोड़ें।
24. स्रोत को फ़ाइल तक विस्तार करें।
25. गुणों और सामग्री की जांच करें, केवल नाम नहीं।
26. संदर्भ को समझने के लिए पड़ोसी फ़ाइलों की जांच करें।
27. कार्य-फ़ोल्डर में निर्यात करें और मूल पथ रखें।
28. यदि आपको हैश सूची की आवश्यकता है, तो ऑब्जेक्ट का चयन करें और **Export File Hash List** का उपयोग करें।

एक निर्यातित फ़ाइल एक व्युत्पन्न है। इसे अपने मूल स्थान पर होने की तरह प्रस्तुत न करें, भले ही इसकी सामग्री समान हो।

7. इमेज माउंट करना: पढ़ना, लिखना और सीमाएँ

FTK Imager कुछ इमेज को पढ़ने के लिए डिवाइस या ड्राइव के रूप में माउंट कर सकता है। इसमें राइट-कैश वाले मोड भी होते हैं, जिनमें परिवर्तन अलग फ़ाइल में सहेजे जाते हैं और इमेज की मूल सामग्री नहीं बदलती।

विधि	क्या अनुमति देता है	चेतावनी
पढ़ना	बिना सामग्री को बदले छवि की जाँच करें।	यह मूल डिस्क को राइट-ब्लॉकर नहीं है।
राइट-कैश	किसी अन्य फ़ाइल में परिवर्तन या नोट्स को सहेजें।	आपको कैश को दस्तावेज़ीकृत करना चाहिए और इसे मूल सामग्री के रूप में प्रस्तुत नहीं करना चाहिए।

भौतिक और तार्किक माउंटिंग एक-दूसरे के विकल्प नहीं हैं। AD1 और L01 में फ़ाइल संरचना होती है, लेकिन पूरी डिस्क ज्यामिति नहीं, इसलिए उन्हें भौतिक इमेज के रूप में माउंट नहीं किया जा सकता।

समाप्त होने पर इमेज अनमाउंट करें और व्युत्पन्न परिवर्तन दर्ज करें। Windows में ड्राइव खुलने से यह सिद्ध नहीं होता कि उस पर लिखा जा सकता है।

8. मेमोरी कैप्चर: अलग प्रकार की प्रक्रिया

चालू सिस्टम की मेमोरी कैप्चर करने का अपना प्रभाव होता है। इससे प्रोसेस, सामग्री और डिवाइस की स्थिति बदल सकती है। मेमोरी अस्थिर होती है; कैप्चर अलग गंतव्य में सहेजें और दिनांक तथा हैश दर्ज करें।

वास्तविक डिवाइस पर प्रारंभिक अभ्यास के लिए यह फ़ंक्शन उपयोग न करें। मामले में मेमोरी चाहिए तो पहले प्राधिकरण, उद्देश्य, विधि, प्रभाव, उपकरण और अभिरक्षा-शृंखला तय करें। कैप्चर और बाद का विश्लेषण अलग प्रक्रियाएँ हैं: FTK Imager कैप्चर करता है; Volatility या दूसरा प्लेटफ़ॉर्म परिणाम की जाँच में मदद कर सकता है।

9. सामान्य त्रुटियाँ और सुरक्षित निर्णय

स्थिति	उत्तरदायी निर्णय
आप नहीं जानते मूल डिस्क कौन सी है	एक्सेस मॉडल, दोनतो, क्रेमाक और प्राप्ति-पत्र जाँचें, अंदाज़े से अनुमान न लगाएँ।
गंतव्य में स्थान खत्म हो जाता है	रोककर स्टोरेज पुनः असाइन करें। संबंधित खंड एक ही फ़ोल्डर में रखें।
छवि सत्यापन से मेल नहीं खाती	इसे एक वैध प्रतिलिपि के रूप में उपयोग न करें। त्रुटि को रिकॉर्ड करें और प्रक्रिया को सही विधि से दोहराएं।
लॉजिकल संग्रह में हटाए गए फ़ाइलें दिखाई नहीं देती हैं	जाँच करें कि खोज और विधि गैर-आवंटित स्थान तक पहुँच पाती है या नहीं। पुनर्प्राप्ति का दावा न करें।
AD1 इमेज भौतिक रूप में माउंट नहीं होती	यह सामग्री-प्रकार की सीमा है। अनुमत तार्किक माउंटिंग उपयोग करें।
एक हैश एक रूपांतरण के बाद अलग है	तय करें कि क्या बदला: संरचना, मेटाडेटा, सामग्री या तुलना किया गया ऑब्जेक्ट। अपने आप असत्य घोषित न करें।
सामग्री का विश्लेषण करने की आवश्यकता है	विश्लेषण के लिए इमेज Autopsy या दूसरे प्लेटफ़ॉर्म में जोड़ें, आयात करें और पूर्ण विश्लेषण में भ्रम न करें।

10. काल्पनिक फ़ाइलों के साथ अभ्यास

वास्तविक डिस्क पर काम किए बिना विकल्प सीखने के लिए प्रयोगशाला फ़ोल्डर उपयोग करें।

29. FTK Imager खोलें और अपनी मुख्य ड्राइव के बजाय फ़ोल्डर सामग्री चुनें।
30. केवल अनज़िप किया हुआ काल्पनिक फ़ोल्डर चुनें।
31. उस फ़ोल्डर के बाहर एक नया गंतव्य सेट करें।
32. व्यक्तियों या ग्राहकों के नाम के बिना प्रदर्शन मेटाडेटा जोड़ें।
33. सत्यापन और सामग्री-सूची सक्रिय करें।
34. इमेज, खंड और लॉग कैसे सहेजे जाते हैं यह जाँचें।
35. परिणाम साक्ष्य के रूप में खोलें और `01_notas.txt` खोजें।
36. कार्य-प्रति और हैश सूची निर्यात करें; प्रत्येक के लिए कौन सी प्रक्रिया उपयोग हुई बताएँ।
37. दस्तावेज़ित करें कि यह अभ्यास भौतिक अधिग्रहण या हटाई गई फ़ाइलों की पुनर्प्राप्ति सिद्ध नहीं करता।

अभ्यास इंटरफ़ेस कार्यप्रवाह सिखाता है। इससे फ़ोल्डर डिस्क या बनी इमेज न्यायिक साक्ष्य नहीं बन जाती।

11. रिपोर्ट से पहले जाँच-सूची

- लिखित प्राधिकरण और दायरा।
- जहां संभव हो, मॉडल, क्षमता और श्रृंखला द्वारा पहचाना गया स्रोत।
- मूल स्रोत के लिए राइट-ब्लॉकर उपयोग किया गया।
- अलग-अलग गंतव्य और पर्याप्त स्थान।
- इमेज प्रकार, खंड और संपीड़न उचित ठहराए गए।
- केस और साक्ष्य का मेटाडेटा पूर्ण।
- निष्पादित सत्यापन और समीक्षा किए गए परिणाम।
- सभी खंड एक साथ और पठनीय हैं।
- पढ़ने की त्रुटियाँ और सीमाएँ दर्ज।
- कार्य-फ़ाइलें अपने मूल से संबंधित।
- अधिग्रहण से अलग बाद का विश्लेषण।
- निष्कर्ष उसी तक सीमित है जितना विधि सिद्ध करती है।

12. आधिकारिक स्रोत और संपादकीय नियंत्रण

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, पहचान, संग्रह, अधिग्रहण और संरक्षण
44. NIST SP 800-86, घटना-प्रतिक्रिया में फोरेंसिक तकनीकें

इस अनुकूलन के लिए मार्गदर्शिका 8.2 पूरी पढ़ी गई। इसमें अलग संस्करणों और उत्पादों के फ़ंक्शन शामिल हैं; सभी FTK Imager के निःशुल्क संस्करण में नहीं हैं। Pro या मोबाइल अधिग्रहण फ़ंक्शन उपयोग करने से पहले लाइसेंस और संबंधित दस्तावेज़ जाँचें।

यह मार्गदर्शिका Jocsan Laguna की शैक्षिक सामग्री है; Exterro का आधिकारिक प्रकाशन या कानूनी सलाह नहीं। संपादकीय समीक्षा: 15 नवंबर 2026.