exterro®

FTK®

DIGITAL INVESTIGATIONS

FTK® helps you find relevant evidence faster, dramatically increases analysis speed and reduce backlogs

FTK—General Overview

Business Case

FTK is a court-accepted digital investigation tool built for speed, stability and ease of use that provides comprehensive processing and indexing up front, so filtering and searching is faster than with any other product, dramatically decreasing time to actionable results. FTK's database architecture allows you to handle massive data sets and is optimized for distributed processing. FTK examines devices and media in a forensically sound manner allowing acquisition, preservation, analysis, and presentation of evidence.

Customer Pain Points

- Backlog of computers and devices waiting for examination.
- Learning curve traditionally associated with computer forensics tools.
- Lack of access or the ability to integrate all the digital data associated with an investigation, causing details to be overlooked and expend resources needlessly.

Business Benefit

- FTK is built for speed, stability and ease of use. It provides comprehensive processing and indexing up front, so filtering and searching is faster than with any other product. This means you can zero in on the relevant evidence quickly, dramatically increasing your analysis speed.
- Interoperates with existing investments like FTK Enterprise® and FTK Lab®. It is the only solution on the market that shares the same core engine and database with other tools.
- Includes many additional features other products charge more to access, like visualization, explicit image detection and distributed processing.

It is important to mention that:

1. FTK is part of a suite that works seamlessly throughout the lifecycle of a case. Since all data is stored in one case database, you can reduce the cost and complexity of managing your cases.

2. FTK is one of the few tools available today that is optimized for distributed processing (up to a total of 4 Processing Engines) providing a more reliable operational environment.

Key Features

- Ability to forensically acquire, analyze, report on forensic data.
- Easy-to-use GUI with automated pre-processing of forensic data.
- Advanced filtering, and automated data categorization.
- Native support for Volume Shadow Copy and Geolocation.
- FTK works with leading mobile device acquisition tools to deliver comprehensive analysis of mobile devices, including smart phones, IOS® and Android devices.
- Password cracking through included PRTK and DNA tools.
- Visualization capabilities to graphically analyze both file and email data, viewing data in timelines, cluster graphs, pie charts and more. Geolocation Visualization, allowing various types of data to be shown geographically on a map, even offline!
- Powerful index search engine with regular expression support to search for advanced combinations of characters in indexed data, as well as a proper fullfeature regular expression engine for binary searches.
- Supports the leading encryption technologies
- World-class training.
- Comprehensive Apple® OS support.

Who Uses FTK?

- Computer Forensic Examiners
- Law Enforcement
- Military
- E-Discovery Teams
- Fraud Examiners
- Homeland Security
- Corporate Investigation Units
- Three Letter Government agencies

How is FTK different from the competition?

1. FTK is built for speed, stability and ease of use. It provides comprehensive processing and indexing up front, so filtering and searching is faster than with any other product. This means you can zero in on the relevant evidence quickly, dramatically increasing your analysis speed.
2. Provides the fastest, most accurate and consistent forensic processing possible with distributed processing and true multi-threaded/multi-core support.
3. The only solution that can identify encrypted PDFs.
4. Delivers industry-first malware analysis capability using Cerberus.
5. See relationships and patterns that help make decisions faster with state-of-the-art data visualization.
6. Includes many additional features other products charge more to access, like visualization, explicit image detection and distributed processing.

How Is It Used?

- FTK is a Windows® program that runs on a database back-end (PostgreSQL, Microsoft SQL).
- Use to import, collect and analyze data such as physical/logical images and files.
- Examiners can rely on the preconfigured processing buttons when it comes to processing evidence, or create and run their own custom profiles.
- Live search and Index search allow end users to search for relevant files easily.
- FTK supports a remote agent that can be pushed or manually installed in the LAN to retrieve evidence and volatile data from a target machine.
- With PRTK and DNA it is possible to recover passwords from 100's of applications.
- Malware triage and analysis on static executable binaries is easy with Cerberus Add-On.
- Visualization in a Graphical timeline with social analysis of email and files.
- Custom reporting.

Golden Questions:

- Describe your current investigative process?
- What kind of data will you process?
- How will you store and access your data?
- How big will your collected data be?
- How long does it take you to process your cases?
- Who will manage the content of the cases?
- Will you need concurrent users?
- What kind of searches will you run on the data?
- Are you currently using distributed processing to minimize processing times?

Objection Handling

Objection: We already use FTK Imager.
Response: FTK Imager allows you to capture the device/evidence but it does not allow you to do anything with with what you have collected.

Objection: We already use Encase.
Response: EnCase is a great tool but we find most Investigators use another tool to validate EnCase's findings. Our customers tell us that FTK is faster and easier to use than EnCase.

Objection: We already use Magnet Axiom.
Response: Axiom is a great tool but we find most Investigators use another tool to validate Axiom's findings.

Objection: We just copy files when doing an investigation.
Response: Copying a file using the OS alters the file and means that it can't be presented in court: it is not forensically sound.

Objection: We don't have anyone trained to use a forensic tool.
Response: Our customers tell us that FTK is one of the easiest tools to use "out of the box". Furthermore, we have some very affordable, world class training available online or in person.

Objection: It's too expensive.
Response: Being able to collect digital evidence securely and in a way that can be presented to a court of law is invaluable.

Objection: We outsource our Forensic Investigations.
Response: Outsourcing generally will give you confidence that the investigation is performed thoroughly however the cost models around outsourcing can be very expensive (per GB / per hour models) and we see that budget needs to be found to service this model. By 'insourcing' you are controlling your investigation, budget whilst upskilling staff member(s) to be proficient in investigations.

Objection: We only have a handful of investigations each year.
Response: How do you deal with these currently? (see above). Even when investigating just a few cases a year, the cost of investing in a tool such as FTK and training can bring a very quick ROI, even in just one or two investigations.

Objection: We use open source and free tools.
Response: There are some great free tools that can assist with a forensic investigation, the concern you may find is around support of these tools should you need assistance or if something goes wrong. FTK has been on the market for over 30 years and the tools is supported by a global team giving you the confidence in the results of the acquisition, analysis and results of your investigation.

Objection: We need a mobile device investigation tool.
Response: Exterro support and encourage competitive product environment, no single tool can provide the answer to all of a forensic investigators needs. However by investing in a mobile device acquisition tool and FTK, not only can you analyse the mobile images you also can acquire and review computers / laptops etc, all through a consistant window in FTK.

FTK: Key Features and Messages to the Market

You need options—more ways to control your investigation environment, your workflow, and your access to data—to get exactly the results you want for your organization. FTK provides more flexibility than ever before, with improved collections and processing, and new tools to manage risk. We're even pushing into the cloud, to bring limitless scalability to your investigation environment.

The FTK Suite includes:

- 4 Workers (DPE's)/1 worker on examiner machine/3 distributed.
- Embedded PostgreSQL Database.
- FTK Imager to create forensic images of computer data, mount and browse nearly any image.
- FTK Registry Viewer to provide access to registry data..

Password Recovery Toolkit® (PRTK®):

- Recovers passwords from 100+ different applications.
- Enables password management.
- Analyzes files and their passwords with an optional report file.
- Recovers all types of passwords regardless of length.
- Analyzes multiple files at one time.
- Recovers multilingual passwords.

Visualization

- Detailed timeline view.
- More granular view of the files and emails in your data set.
- Quickly identify the files and emails that are relevant and assess gaps in communication exchanges.
- Toggle time bands for more granular view of the files: Years, Months, Days, Hours, Minutes, Seconds and Milliseconds.

Distributed Network Attack (50 DNA Workers):

- Harness idle CPUs to perform robust dictionary attacks.
- Easy-to-read statistics and graphs.
- Add user dictionaries.
- Optimize password attacks for specific languages.
- Customize user dictionaries.
- Stealth client installation functionality.
- Automatic Client Update when updating the DNA Server.

Cerberus (Optional Add-In)

- Cerberus is the first step toward automated reverse engineering to analyze executable binaries and assess the priority of treatment before sending them for further analysis. Cerberus examines things that are immediately apparent about the binary, for example:
- Does the binary contain a digital signature?
- Is this binary packed?
- What OS function does this binary import?
- Cerberus performs a 2-stage analysis:
- Threat Analysis: Identify malicious code and generate threat score.
- Static Analysis: Cerberus learns how executable works without running it to find out what the binary is capable of.