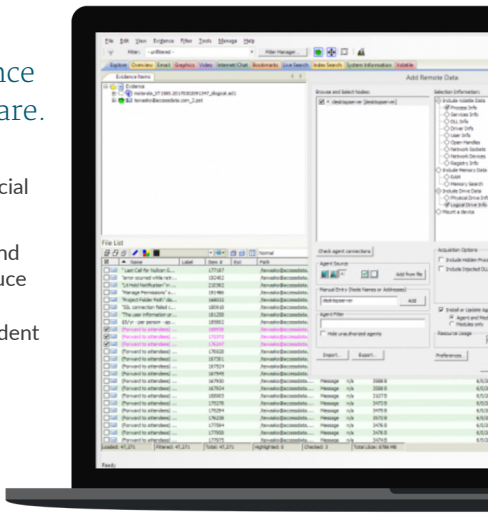
exterro®

FTK® ENTERPRISE

Conduct internal investigations and facilitate legal and regulatory compliance in enterprise environments with the gold standard of digital forensic software.



The **FTK**® family is the most trusted digital forensics software in the world. Purpose-built for the modern corporation, **FTK Enterprise** delivers the power and speed of digital forensic investigations to bear with special features designed for enterprise environments.

Access multiple devices across your network. Gain forensic visibility into data for employee investigations and to support regulatory and legal compliance. Enforce policies, protect data and intellectual property, and reduce costs—regardless of the size or geographical spread of your organization. When your organization needs to respond quickly to an internal misconduct report, address a compliance matter, or respond to a security incident or breach, FTK Enterprise provides access to the data across your network, regardless of location.

With **FTK Enterprise**, you have a forensics solution designed to meet the needs and demands of large, multi-location, public and private organizations today.

Selected Built-In Features

Data Acquisition

Acquire data from disk or RAM, documents, images, email, webmail, Internet artifacts, web history and cache, chat sessions, compressed files, backup files, encrypted files, network shares, deleted files, video, and more.

Secure and Compliant

FIPS 140-2 certified solution maps to the requirements of GLBA 501b, Sarbanes-Oxley (SOX), SB13386, HIPAA, and ISO 27001 and is fully functional in Zero Trust environments.

Scalable Endpoint Collection

Unmatched scalable endpoint collection and processing speeds for significant efficiency gains. Easily collect volatile data from up to 20,000 remote endpoints simultaneously.

Password Recovery and Decryption

Recover, decrypt, or crack passwords and certificates to access locked data with FTK support for Windows BitLocker and ClearKey.

Optimized Mac® Investigations

Discreetly collect from Mac endpoints with performance so smooth as to be imperceptible. Parse artifacts from Apple® Mail, iMessage®, iWork®, Safari®, and Outlook® for Mac faster than ever.

Optical Character Recognition

Unmatched text recognition, accuracy and speed using LEADTOOLS to create searchable, exportable documents. Upgrade your capabilities with new precision document conversion capabilities by ABBYY OCR.

Remote Threat Monitoring and Remediation

Search, monitor, and resolve issues remotely by filtering data, searching on specific keywords, and culling data live at any endpoint, then selectively import selected data for deeper analysis.

Remote Memory Analysis

Conduct live, remote memory analysis of endpoints, including on devices with the most recent builds of Windows OS, like Windows 2019 and Windows 10, as well as MacOS 10 and Linux.

Optional Capabilities

Automated Workflows with FTK Connect API

Integrate with your SIEM, SOAR, or cybersecurity platforms to automate forensic collection, processing, and administrative tasks upon threat detection.

Integrated Offline Translation

Conduct cross-border investigations with multilingual data sets. Collect, process, translate, and review data in a unified forensic platform, saving time and money on contextual translation services.

Interactive, Customizable Cross-Case Dashboards

Compile the information critical to each individual investigator with dashboards customized by role. Gain full transparency and insight into the most important data points across all cases at the same time.

Post-Breach Analysis Console

Rapidly review and analyze key volatile data elements including processes, sockets, drivers, users, ports, DLLs, handles and more across machines and across time.

IoC, YARA, and MISP Support

Identify and investigate incidents for indicators of compromise, including YARA and MISP rules, to determine how and why cyber incidents happened and to respond more rapidly and effectively.