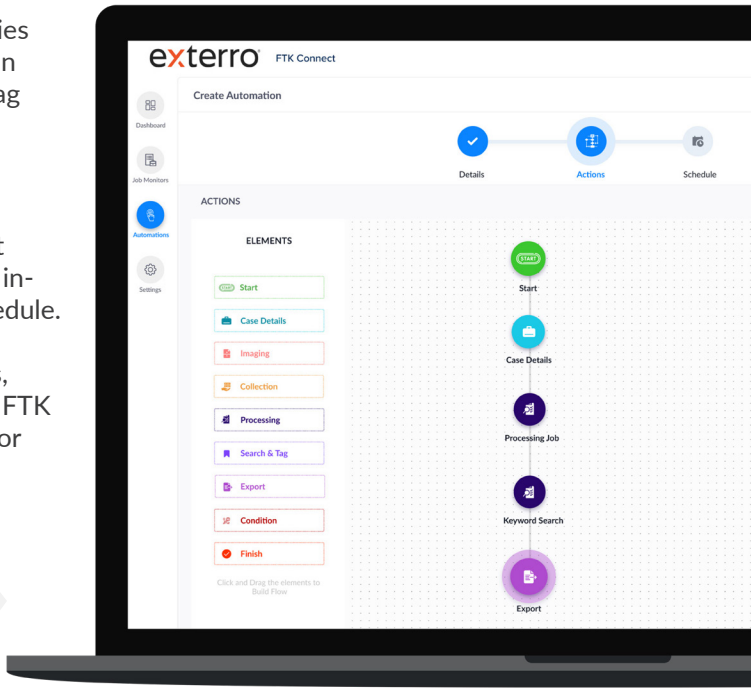
exterro®

FTK® CONNECT

Automate the power and speed of Exterro's industry-leading FTK Solutions when performing forensic investigations, incident response workflows, or securing corporate assets.

FTK Connect enables corporations and law enforcement agencies to easily automate and accelerate key processes and tasks within forensic DFIR investigations. With its dramatically simplified drag and drop interface, users can create powerful time and money saving automations.

Integrate with industry-leading intrusion detection software to automate the immediate preservation of evidence from the first moments an incident is detected. Forensically collect data from in-network and off-network endpoints, based on triggers or a schedule. Automate tasks like case creation and evidence processing, then automate next steps such as searching and labeling results, exporting data, and more – all without any user interaction. Let FTK Connect handle the mundane tasks, saving investigators' time for what they do best: forensic analysis and review.



The Exterro FTK Connect UI allows corporations and agencies to create custom automation workflows without the need for complicated API scripting.

Selected Features

Create Automations with Unprecedented Ease

Built for non-programmers, the intuitive interface allows users to easily create automations for any case type with a drag and drop interface. Be instantly productive with minimal training.

Automated Forensic Collections

Automate remote forensic data collection from in-network and off-network endpoints for routine investigations and securing corporate assets. Collect covertly and remotely.

Automated Processing and Review

Law enforcement agencies can configure FTK Connect to watch directories and automatically process any forensic image placed there. Then automatically search cases for preconfigured search terms, apply labels or bookmarks, and export the resulting files.

Automated Notifications

Keep users informed of case progress with automated processing status updates that notify reviewers via text message or email.

Unite SIEM & SOAR with Forensic Investigations

Orchestrate your forensic collection workflow by integrating your cyber infrastructure tools together. Instantly preserve electronic evidence upon detection of an intrusion. FTK Connect can automate collection from remote endpoints based on triggers from solutions like Splunk SOAR and Palo Alto SOAR.

Custom Workflows

Leverage the FTK Connect APIs to build your own workflows or integrations that fit your exact needs and specifications.

Compatibility

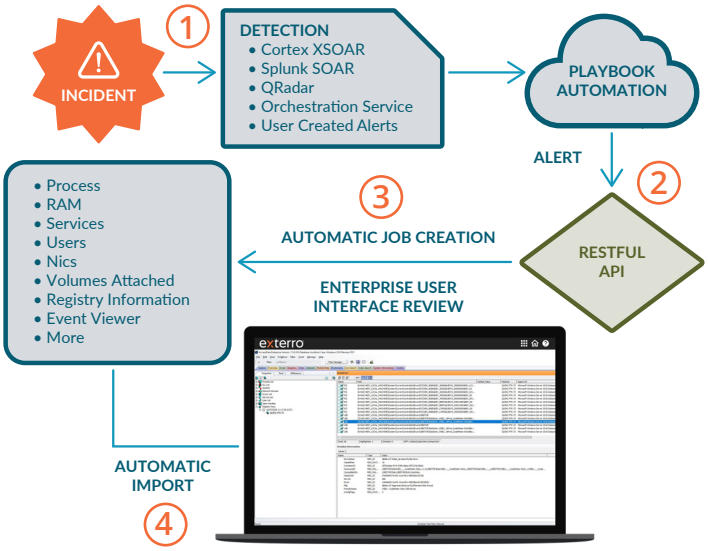
FTK Connect seamlessly integrates with FTK® Lab, FTK® Enterprise, and FTK® Central. Bring unrivaled speed, power, and security to your corporate network. For law enforcement agencies utilizing FTK Lab or FTK Central, FTK Connect will allow for more cases to be closed in less time.

FTK® CONNECT

The **FTK Connect API** enables a secure connection between your cyber platform (e.g., Palo Alto SOAR ®, Splunk SOAR®, etc.) and a compatible FTK product such as FTK Lab, FTK Enterprise, or FTK Central. If the cybersecurity software detects an attack, it sends an alert that is received by the FTK software, which initiates a collection job at a designated endpoint based on pre-defined collection criteria. This saves time in the initial stages of incident response by preserving data related to the root cause of the breach.

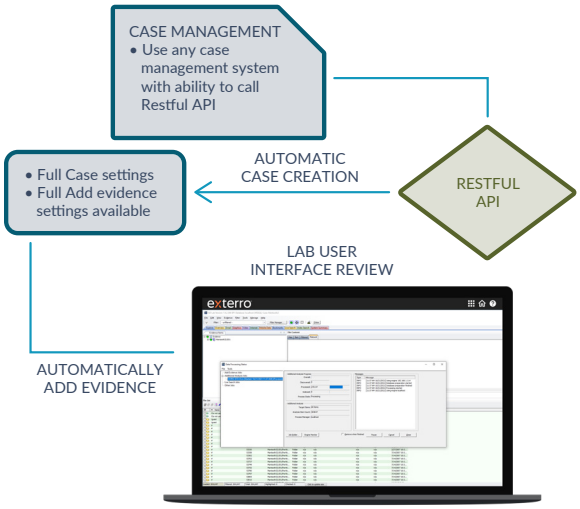
HOW IT WORKS

1. An incident is detected via your cyber platform, orchestration services, or user-created alerts.
2. Automation rules create a job through the FTK Connect API.
3. An automatic job collection is initiated by FTK Enterprise at a specified endpoint.
4. The information is passed into FTK Enterprise for review.



FTK CONNECT AUTOMATES FORENSIC REVIEW

Use the FTK Connect API to automate tasks like case creation, and to automatically kick off processing jobs and keep the investigator informed when their job is finished. This will cut the time spent waiting for jobs to be completed and increase the forensic review and analysis time able to be completed by each investigator.



> "FTK Connect contains a critical API option that will allows our team to integrate our SIEM platform with our forensic platform. This capability enables us to perform automated response to events detected with SIEM platforms, such as Arcsight® or Splunk®. This feature will save us about 40 minutes of analyst time per incident. The API integration with our SIEM is an important force multiplier for our existing staff by leveraging the power of automation."
>
> — Scott Sattler, forensic consultant for SecureLabs.net