# Forensic Email Collector™
# Product Overview

Forensic Email Collector (FEC) is designed to preserve email evidence from cloud and on-premises email servers accurately. Top law firms, law enforcement agencies, and digital forensics and eDiscovery service providers use FEC worldwide to acquire emails for digital forensics investigations and eDiscovery.

Developed for forensic use, FEC connects to servers in a read-only manner, collects server metadata needed for forensic authentication, and keeps detailed logs of all activity for your case documentation.

## Email Preservation without The Pain

While preserving emails, forensic examiners often have to overcome challenges such as large acquisitions being interrupted by server throttling and multi-factor authentication related issues. FEC has numerous features designed to make your life easier.

**In-Place Search**
FEC allows you to run instant searches on Gmail / G Suite, Office 365, Exchange, and IMAP mailboxes directly on the server. Search results can be collected quickly, saving valuable time.

**Resume & Auto-Retry Ability**
FEC ensures that every message is accounted for during the acquisition. Remaining items are automatically retried, and projects can be resumed at a later time. This provides great flexibility in preserving large mailboxes from low-performance email servers.

**Two-Factor Authentication Support**
FEC supports two-factor authentication when connecting to Gmail, G Suite, and Office 365. Additionally, custodians can authenticate FEC into their email accounts on their own computers, without having to share their credentials.

**Delegation**
Tracking down end users in a large organization to acquire their mailboxes is no fun. FEC makes things easier by allowing you to use delegation on Office 365, Exchange servers, and G Suite. With delegation, you can use administrative credentials to preserve custodian mailboxes.

**Google Drive Attachments**
Google allows end users to insert attachments into emails as hyperlinks that point to files on Google Drive. FEC allows you to acquire the linked Drive attachments during Gmail and G Suite acquisitions.

**Not Just Emails**
In addition to emails, FEC can acquire Google Calendars as well as notes, contacts, and calendar events from Exchange servers.

### Acquisition Using Existing Login Sessions

During a search warrant, law enforcement agents can use FEC to authenticate with Gmail / G Suite mailboxes on a suspect's computer using an existing login session on the suspect's web browser. Agents can then quickly search the mailbox and acquire the results while on-site.

### Multi-Format Output

FEC is capable of outputting to EML, MSG, and PST formats simultaneously—formats that are ready to be ingested into digital forensic investigation tools. This saves time that would typically be spent performing conversions after the fact and minimizes the possibility of conversion issues.

### Detailed Logging

Effective documentation is crucial in forensic investigations. FEC helps you document the acquisition process by keeping detailed logs of its communications with the server as well as any issues encountered.

### Output Hashing

FEC hashes the collected items automatically using the MD5, SHA-1 or the SHA-256 algorithm. Hashing is done on multiple CPU cores, taking advantage of modern processors.

### Server Metadata

Server metadata is often a critical piece of the puzzle when forensically authenticating emails. FEC preserves server metadata such as the IMAP internal date and unique identifier message attributes so you have the information you need.

### Exchange Autodiscover

FEC has built-in support for the Exchange Autodiscover service. This allows you to determine the Exchange Web Services URL and target Exchange server version automatically using the target email address and password.

### Flexible Connectivity

FEC can acquire from Gmail / G Suite, Office 365, hosted and on-premises Exchange servers as well as IMAP-compatible servers such as Yahoo, AOL, and iCloud.

### Licensing Options

FEC can be used with a soft license key or a hardware USB dongle.

## About Metaspike

Metaspike is a software company based in Los Angeles, CA that develops digital forensics software for the cloud. For more information about Metaspike, visit www.metaspike.com.

Learn more at www.metaspike.com/forensic-email-collector/

www.metaspike.com
Twitter: twitter.com/MetaspikeHQ
LinkedIn: www.linkedin.com/company/metaspike/