AccessData®

Forensic Toolkit®

Forensic Toolkit® (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. The database-driven, enterprise-class architecture allows you to handle massive data sets, as it provides stability and processing speeds not possible with other tools. Furthermore, because of this architecture, FTK can be upgraded easily to expand distributed processing and incorporate web-based case management and collaborative analysis.

Unmatched Processing

FTK utilizes distributed processing and is the only forensics solution to fully leverage multi-threaded / multi-core computers. While other forensics tools waste the potential of modern hardware solutions, FTK is able to use 100% of its hardware resources.

Processing Profiles

Create and reuse processing templates with predefined processing options.

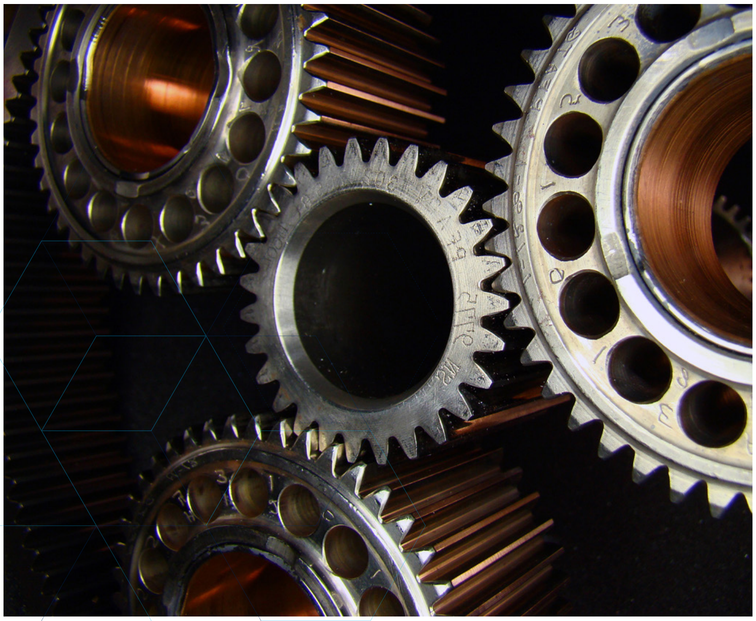
Handle Massive Data Sets without the Crashing and Lost Work

While other products can run out of memory and slow or crash during processing, FTK is database driven which provides the stability necessary to handle large data sets. In addition, FTK components are compartmentalized allowing processing workers to continue processing data even if the GUI stalls.

Fast, Comprehensive Index and Binary Searching

By processing and indexing data up front and leveraging the powerful dtSearch engine, as well as a full-featured regular expression engine, FTK produces fast and accurate results.

High
Performance
Computing &
Sophisticated
Data Analysis



File and Disk Encryption Support

With proper credentials you can decrypt technologies, such as Credant, SafeBoot, Utimaco, PGP, Guardian Edge, Sophos Enterprise and S/MIME and more. FTK can also decrypt hundreds of file types. It will decrypt files during processing with passwords you provide, or you can select encrypted files within FTK and send them to the built-in Password Recovery Toolkit® module for password recovery.

Advanced Gallery View for Images and Video with Automatic Identification of Explicit Images

Quickly identify critical image and video files. In addition FTK identifies pornographic images automatically, which is an invaluable feature for law enforcement. It not only recognizes flesh tones, but shapes and image orientations that could be pornographic in nature.

Superior Email Analysis

FTK supports 18 different email types, including Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.), Netscape, AOL and RFC 833.

Single-Node Enterprise

Get the full remote analysis and incident response capabilities of AD Enterprise. Preview, acquire and analyze hard drive data, peripheral device data, and volatile/memory data.

Volatile and Memory Analysis

Enumerate all running processes, even those hidden by rootkits, and display associated DLLs, network sockets and handles in context. Search memory, automatically map hits back to a given process, DLL or piece of unallocated space, and dump the corresponding item. VAD tree analysis exposes registry artifacts in memory, parsing and displaying handle information. (Supports Windows® 32- & 64-bit, Apple®, UNIX® and Linux®)

Internet Artifact Analysis

FTK® provides broad browser support with SQLite parsing and includes 40 Internet artifact carvers for popular web applications, including Facebook, Google Drive (“Docs”), Google Chat, ICQ 7M, Skype, DropBox, Torrent and many, many more.

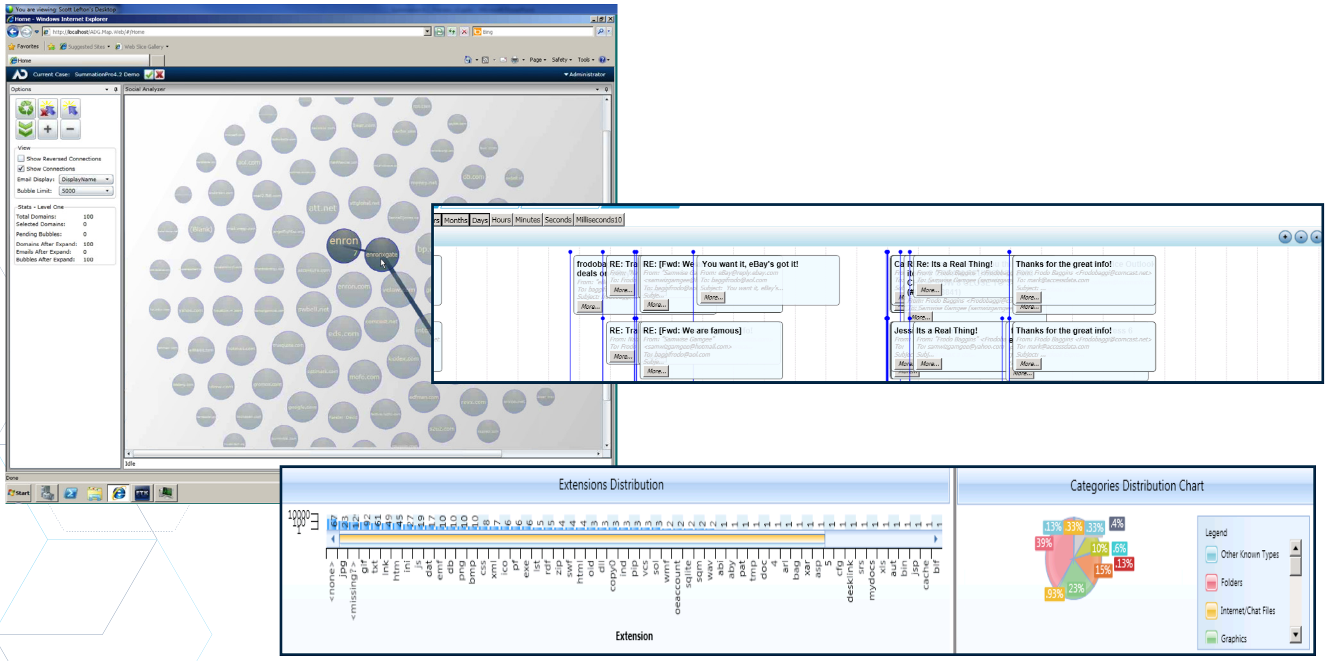
Apple® OS Analysis

Recognized for its superior analysis of Apple OS machines, FTK supports B-Trees, .PLISTs, SQLite databases, .JSON files and .DMG and .DD disk images.

Data Visualization for Automated Timeline Construction and Social Analysis

Stop relying on third-party tools to see visual relationships within data. The Visualization technology in FTK displays your data in timelines, cluster graphs, pie charts and more.

> “Mac features… …that can’t be found in any other Windows analysis tool.”
>
> -- Ryan Kubasiak
> www.AppleExaminer.com



Automatically construct timelines and establish relationships among parties of interest in an investigation.

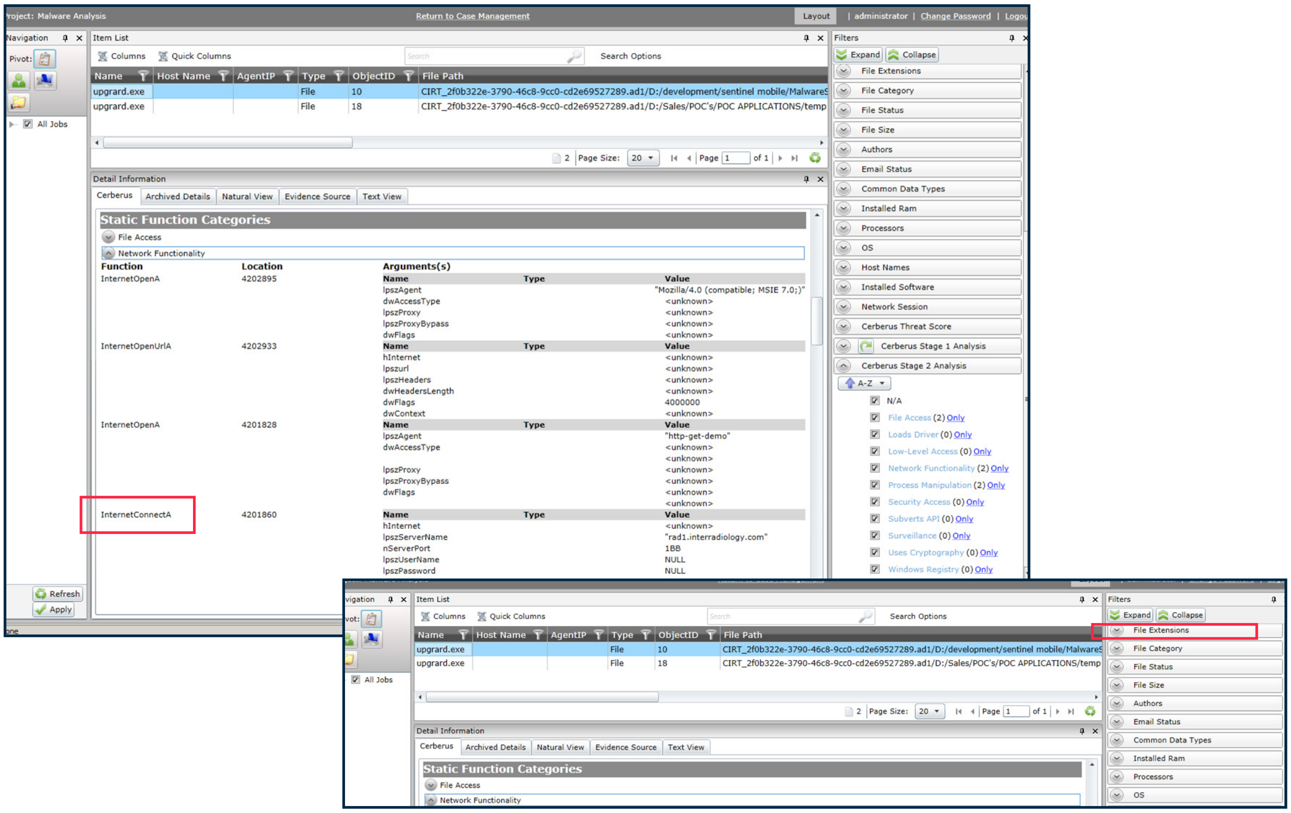
Add Malware Triage & Analysis to Forensic Toolkit®

Perform immediate malware triage with Cerberus, and gain actionable intelligence prior to engaging a malware team.

Cerberus is the malware analysis component of AccessData's integrated incident response platform, CIRT (Cyber Intelligence & Response Technology). This module is also available as an add-on to FTK. The first step towards automated reverse engineering, Cerberus allows you to determine the behavior and intent of suspect binaries, giving you actionable intelligence without having to wait for a malware team to perform deeper, more time consuming analysis.

Identify new, undefined malware without the sandbox.

Cerberus is able to disassemble and simulate the functionality of a suspect binary, without actually running the code. It does not rely on white lists or black lists and it does run the binary in a sandbox. This is of great value to first and second responders, because it not only allows you to take decisive action more quickly, but it reveals behavior and intent without running the risk of triggering defense mechanisms commonly found in malware.



Name	Host Name	AgentIP	Type	ObjectID	File Path
upgrard.exe			File	10	CIRT_2f0b322e-3790-46c8-9cc0-cd2e69527289.ad1/D:/development/sentinel mobile/MalwareS
upgrard.exe			File	18	CIRT_2f0b322e-3790-46c8-9cc0-cd2e69527289.ad1/D:/Sales/POC's/POC APPLICATIONS/temp

Static Function Categories

File Access

Network Functionality

Function	Location	Arguments(s) Name	Type	Value
InternetOpenA	4202895	lpszAgent		"Mozilla/4.0 (compatible; MSIE 7.0;)"
		dwAccessType		<unknown>
		lpszProxy		<unknown>
		lpszProxyBypass		<unknown>
		dwFlags		<unknown>
InternetOpenUrlA	4202933	hInternet		<unknown>
		lpszurl		<unknown>
		lpszHeaders		<unknown>
		dwHeadersLength		<unknown>
		dwFlags		4000000
		dwContext		<unknown>
InternetOpenA	4201828	lpszAgent		"http-get-demo"
		dwAccessType		<unknown>
				<unknown>
		lpszProxy		<unknown>
		lpszProxyBypass		<unknown>
		dwFlags		<unknown>
				<unknown>
InternetConnectA	4201860	hInternet		<unknown>
		lpszServerName		"rad1.interradiology.com"
		nServerPort		1BB
		lpszUserName		NULL
		lpszPassword		NULL

- ☑ N/A
- ☑ File Access (2) Only
- ☑ Loads Driver (0) Only
- ☑ Low-Level Access (0) Only
- ☑ Network Functionality (2) Only
- ☑ Process Manipulation (2) Only
- ☑ Security Access (0) Only
- ☑ Subverts API (0) Only
- ☑ Surveillance (0) Only
- ☑ Uses Cryptography (0) Only
- ☑ Windows Registry (0) Only

AccessData®

CORPORATE HEADQUARTERS
801.377.5410
588 West 400 South
Suite 350
Lindon, UT 84042 USA

NORTH AMERICAN SALES
800.574.5199
Fax: 801.765.4370
sales@accessdata.com

INTERNATIONAL SALES
+44 (0)20 7010 7800
internationalsales@accessdata.com

www.accessdata.com