Forensic Toolkit® 4

Forensic Toolkit (FTK) is the most innovative and advanced computer forensics solution available, giving you enterprise-class capabilities for a stand-alone price.

SC MAGAZINE INNOVATOR 2011

The True Meaning of Next-Generation Digital Investigations

Unmatched Analysis

- Apple® OS
- Email
- Images
- Memory
- Remote Analysis
- Password Cracking

Stability

The backend database and compartmentalized components virtually eliminate crashing and lost work.

Scalability

FTK scales to handle massive data sets and can be easily upgraded to expand distributed processing and incorporate web-based case management and collaborative analysis.

Security

Industry-standard x509 certificates and a FIPS 140-2 certified SSL encryption engine.

ENTERPRISE-CLASS ARCHITECTURE…

Handle Massive Data Sets without Crashing

The backend database scales to handle massive data sets and the FTK components are compartmentalized so , for example, if the GUI does crash, the workers continue to process data. This design virtually eliminates the crashing and lost work associated with memory-based tools.

Experience Fast Searching and Easy Data Navigation

FTK provides comprehensive processing and indexing up front so filtering and searching is faster than any other product. This means you zero in on the relevant evidence quickly, dramatically increasing your analysis speed.

Distributed Processing & Fully Leveraging Your Hardware

FTK processes data faster than any other computer forensics solution. It delivers true distributed processing, allowing you to divide your processing across four workers. Furthermore, FTK is the only computer forensics solution to fully leverage multi-threaded / multi-core computers. So while common forensics tools waste the potential of modern hardware solutions, FTK will fully utilize anything you throw at it.

- Faster more efficient processing
- Cancel/Pause/Resume functionality
- Better real-time processing status
- CPU resource throttling
- Email notification upon processing completion

NEW IN FTK 4:

Single Node Enterprise

Remotely investigate a computer with the full capabilities of AD Enterprise, saving time and reducing or eliminating travel.

Gain Incident Response Capabilities with Deep Analysis of a Live System

FTK delivers advanced memory and volatile analysis to aid forensic investigators and incident responders.

Memory Analysis:
Enumeration of all running Processes (including those hidden)
DLL list
Network Sockets
Drivers loaded in memory
Device driver layering identification
Handles
Enumeration and hook detection of SCT,IDT and IRP
Devices
Registry enumeration
VAD tree

Memory string search allows you to identify hits in memory and automatically map them back to a given process, DLL or piece of unallocated and dump the corresponding item.

OS View (Volatile)
Processes (including hidden)
DLLs
Sockets
Devices
Drivers
Services
Users
Open Handles
Registry Enumeration

AccessData®

Apple OS Analysis

FTK provides the most comprehensive Apple OS analysis of any Windows forensics product.

- Process B-Trees attributes for metadata
- PLIST support
- SQLite database support
- Apple DMG and DD_DMG disk image support
- Crack Sparse Images or Sparse Bundles
- JSON file support

Email Analysis

Currently supported email types are: Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.), Netscape, AOL and RFC 833

Encryption Support

FTK supports popular encryption technologies, such as Credant, SafeBoot, Utimaco, EFS, PGP, Guardian Edge, Sophos Enterprise and S/MIME.

NEW ADD-ONS TO EXPAND YOUR DIGITAL INVESTIGATIONS HORIZONS…

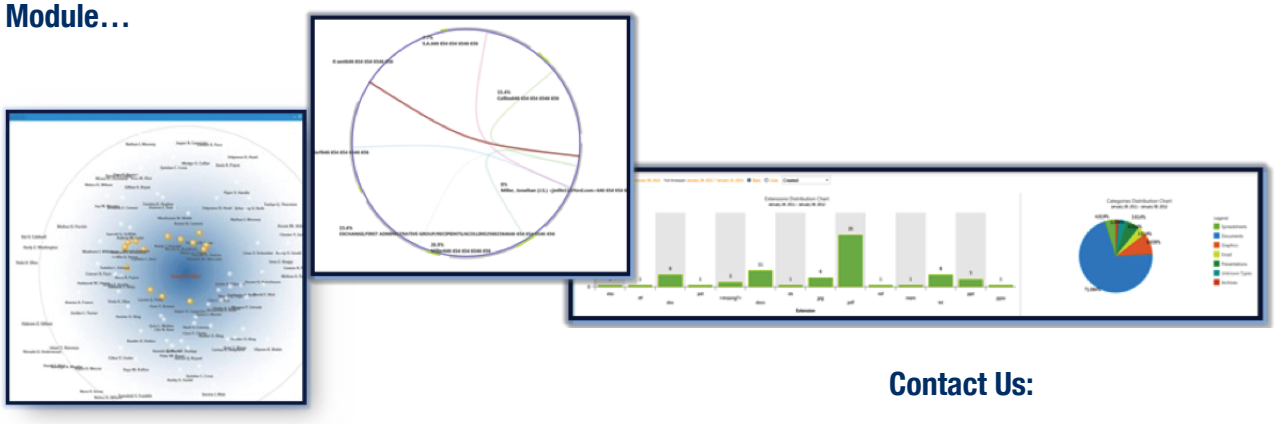
Cerberus Malware Analysis Technology

Cerberus is a malware triage technology that is available as an add-on for FTK 4. The first step towards automated reverse engineering, Cerberus provides threat scores and disassembly analysis to determine both the behavior and intent of suspect binaries.

Visualization

With our new visualization module you can view data in seconds in multiple display formats, including timelines, cluster graphs, pie charts and more. This not only allows users to quickly determine relationships in the data and find key pieces of information, but it also enables the quick generation of reports that are easily consumed by attorneys, CIOs or other investigators.

Analytics in AccessData's New Visualization Module…



Contact Us:

NORTH AMERICA SALES
800.574.5199
801.765.4370 (fax)
sales@accessdata.com

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

AccessData®