ACCESSDATA®

Forensic Toolkit® (FTK®)

Enfóquese con rapidez en la evidencia más relevante.

FTK es reconocido mundialmente como la solución estándar para las investigaciones forenses digitales.

FTK® pone a su disposición una suite completa de herramientas, necesarias para conducir investigaciones digitales de forma mucho más inteligente, rápida y eficiente.

FTK pone a su disposición una suite completa de herramientas, necesarias para conducir investigaciones digitales de forma mucho más inteligente, rápida y eficiente. FTK le permite establecer rápidamente hechos del caso gracias a sus características novedosas y líderes en el mercado como el procesamiento distribuido, el análisis colaborativo de casos, los reportes de visualización de la evidencia y más; todo en una única y completa solución. FTK provee características integrales e innovadoras para respaldar la integridad de los datos en el procesamiento de la información con rapidez y profundidad de análisis.

Reduzca su acumulación de casos, enfocándose rápidamente en la evidencia más relevante.

La lista de casos pendientes acumulados se hace cada vez más grande. No hay suficiente tiempo ni recursos para procesar la información que se necesita examinar en cada caso específico. FTK está diseñado para trabajar con rapidez, estabilidad y facilidad de uso, brindando un procesamiento completo de la información e indexando por adelantado, por lo que el filtrado y la búsqueda se hacen mucho más rápido que con cualquier otro producto en el mercado. Esto equivale a un incremento en la rapidez del análisis, permitiéndole obtener inteligencia procesable en mucho menor tiempo. Adicionalmente, las grandes agencias de investigación de informática forense pueden escalar FTK fácilmente para expandir la capacidad de procesamiento e incorporar un manejo de casos basado en Web y en análisis colaborativo para minimizar la cantidad de casos mediante la división del trabajo con AD Lab.

Tome el Control del Big Data

El uso y la variedad de computadoras y dispositivos digitales han crecido exponencialmente. En la actualidad todos los casos criminales involucran cantidades masivas de evidencia digital que proviene de diferentes fuentes. La arquitectura de FTK, de clase empresarial e impulsada por una base de datos madura, le permite manejar y comprender estas cantidades masivas de información mediante la estabilidad de procesamiento y la visualización de la información, no disponible con otras herramientas. Con FTK, puede separar fácilmente información relevante de la trivial y de manera sencilla explicar los detalles a sus colegas, abogados, procuradores y jurado. Además FTK es la única solución en el mercado que fue desarrollada concretamente para ser interoperable con el portafolio completo de las soluciones de AccessData y así ayudarle a vencer los obstáculos atribuidos a dispositivos móviles, BYOD, e-Discovery y Ciberseguridad.

“Con FTK y AD Lab, somos capaces de entrenar rápidamente a los investigadores para que puedan hacer uso de la interfaz y colaborar en la temprana evaluación de los casos. Esto libera a los analistas forenses más calificados para que puedan enfocarse en el análisis”.

— Major Keith Miller
Officer Commanding, Service Police Crime Bureau, Royal Military Police.

CARACTERÍSTICAS CLAVE

GUI Fácil de usar. Con pre-procesamiento automatizado de la información forense.

Completamente interoperable con MPE+, Summation y la suite completa de soluciones de AccessData.

Interoperabilidad con dispositivos móviles y soluciones de e-Discovery y Ciberseguridad.

El análisis y soporte para Sistemas Operativos más amplio del mercado.

Filtrado avanzado y categorización automatizada de la información.

Hágalo todo. Pre-visualización, adquisición, ensamble y análisis de la información en tiempo real.

Flexibilidad. Disponible en licencia perpetua o por subscripción.

Soporte nativo para Volume Shadow Copy.

Análisis completo de memoria volátil.

Agregue Cerberus para análisis automático de malware.

Rompa contraseñas mediante PRTK / DNA.

Capacidades de visualización que permiten un análisis gráfico de la información de archivos y correos.

Geolocalización que permite mostrar geográficamente varios tipos de información en un mapa, aun estando fuera de línea.

Poderoso motor de búsqueda Indexada con expresiones comunes.

Capacitación de clase mundial.

Beneficios Clave

SOLUCIÓN INTEGRAL DE CÓMPUTO FORENSE

FTK le permite a los usuarios crear imágenes, procesar un amplio rango de diferentes tipos de información, desde imágenes forenses hasta archivos de correo electrónico y dispositivos móviles, analizar el registro, descifrar archivos, romper contraseñas y construir reportes, todo con una sola solución.

PROCESAMIENTO INCOMPARABLE

FTK utiliza un procesamiento distribuido y es la única solución forense que ejerce el uso completo de los múltiples subprocesos y múltiples núcleos de la computadora. Mientras otras herramientas forenses desperdician el potencial de las soluciones de hardware modernas, FTK es capaz de usar el 100% de sus recursos de hardware. Los examinadores en laboratorios distribuidos pueden trabajar en conjunto en el mismo caso al mismo tiempo, utilizando un enfoque de división de trabajo.

MANEJE CANTIDADES MASIVAS DE INFORMACIÓN SIN COLAPSOS O PÉRDIDA DE TRABAJO

Mientras otros productos suelen quedarse sin memoria, alentarse o colapsar durante el procesamiento, FTK es impulsado por una base de datos con arquitectura modular que provee la estabilidad necesaria para manejar cantidades de información de casi cualquier tamaño.

LAS MEJORES CARACTERISTICAS EN UNA SOLA CAJA

FTK es por mucho la herramienta con mayor valor agregado del mercado, con características como la visualización, la detección de imágenes explicitas (EID), el rompe contraseñas (PRTK/DNA) y el análisis remoto de máquinas, todas incluidas en una sola herramienta por un mismo precio.

BÚSQUEDA BINARIA, INDEXADO RÁPIDO Y COMPLETO

Gracias al procesamiento e indexación por adelantado y haciendo uso de su poderoso motor dtSearch® así como también de un motor completo de expresiones regulares, FTK produce resultados rápidos y precisos.

SOPORTE PARA CIFRADO DE ARCHIVOS Y DISCOS

Con las credenciales adecuadas puede descifrar tecnologías como: like BitLocker®, CREDANT®, SafeBoot®, Utimaco®, PGP®, GuardianEdge®, Sophos® Enterprise, S/MIME y más. FTK puede también descifrar cientos de tipos de archivos. FTK descifrará los archivos durante el procesamiento con las contraseñas que usted provea o también puede seleccionar archivos cifrados dentro de FTK y enviarlos al Password Recovery Toolkit (PRTK/DNA), módulo incluido en FTK para la recuperación de contraseñas.

GALERÍA AVANZADA PARA IMÁGENES Y VIDEO CON EID

Identifica rápidamente imágenes y archivos de video críticos. FTK también identifica automáticamente imágenes con contenido sexual explícito, una característica invaluable para las fuerzas del orden público. No sólo reconoce tonos de color piel sino también formas y posiciones de imágenes que pueden ser pornográficas por naturaleza.

MICROSOFT® PhotoDNA®

Soporta Microsoft® PhotoDNA®, el cual crea una firma única en una imagen digital (como una huella digital) que puede ser comparada con la firma de otras imágenes para encontrar copias y variaciones en las imágenes de interés.

ANÁLISIS DE CORREO SUPERIOR

FTK soporta una amplia variedad de tipos de correo, incluyendo Notes™ NSF, Outlook® PST/OST, Exchange EDB, Outlook Express® DBX, Eudora®, EML (Microsoft Internet Mail, Earthlink®, Thunderbird®, Quickmail®, etc.), Netscape®, AOL® y RFC 833.

UN SOLO NODO ENTERPRISE (INVESTIGACIÓN REMOTA)
Pre-visualiza, adquiere y analiza datos de discos duros, información de dispositivos periféricos y datos de la memoria volátil de sistemas remotos en su red.

ANÁLISIS DE LA MEMORIA VOLÁTIL.
Enlista todos los procesos en ejecución, incluyendo aquellos ocultos mediante un rootkit y muestra los DLL´s asociados, sockets de red y handles. Busca en la memoria, relaciona automáticamente resultados de la búsqueda con un proceso en particular, DLL´s o segmentos del espacio no asignado, con la capacidad de realizar un dump.

Analiza los Virtual Address Descriptors en un formato de árbol que expone artefactos del registro en la memoria, realizando un parseo y mostrando la información del handle. (Soporta Windows® 32- & 64-bit, Apple®, UNIX® y Linux®)

ANÁLISIS DE ARTEFACTOS DE INTERNET.
FTK provee un amplio soporte para navegadores con SQLite® e incluye 40 reconstructores de artefactos de internet para aplicaciones web populares, incluyendo Facebook®, Google Drive™ ("Docs"), Google Chat™, ICQ® 7M, Skype™, Dropbox™, Torrent y muchos más.

AMPLIO SOPORTE Y ANÁLISIS DE SISTEMAS OPERATIVOS.
Reconocido por su análisis superior de máquinas con iOS®, FTK soporta bases de datos B-Trees, PLISTs, bases de datos de SQLite, archivos .JSON e imágenes de discos .DD y .DMG.

VISUALIZACIÓN DE DATOS PARA LA CONSTRUCCIÓN AUTOMÁTICA DE LINEAS DE TIEMPO Y ANÁLISIS SOCIAL.
No hay necesidad de usar una herramienta externa para poder visualizar la correlación de la información, la tecnología de visualización de FTK despliega su información en líneas de tiempo, gráficas de líneas, geolocalización, graficas de pastel y más.

ANÁLISIS DE MALWARE.
Disponible como un complemento para FTK, CERBERUS le permite determinar el comportamiento e intención de binarios sospechosos, proporcionándole inteligencia procesable sin tener que esperar a que el equipo de análisis de malware realice un análisis profundo que consuma tiempo valioso.

ACCESSDATA®

AccessData ha sido pionero en el desarrollo de software e-discovery y forense digital por más de veinticinco años, durante ese tiempo, la compañía ha crecido para proporcionar soluciones tanto stand-alone como empresariales que sinérgicamente pueden trabajar en conjunto para desarrollar investigaciones digitales, informática forense, revisión legal, cumplimiento, auditoría y aseguramiento de la información. Más de 130.000 clientes en las más diversas agencias gubernamentales, corporaciones y firmas de abogados de todo el mundo confían en las soluciones de software de AccessData y en sus principales productos y servicios de investigaciones digitales. AccessData es también el proveedor líder de capacitación y certificación en análisis forense digital, con los programas y certificaciones de AccessData Certified Examiner® y Mobile Phone Examiner Certification. Para mayor información visite www.AccessData.com

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com

LEARN MORE

www.AccessData.com