

Concentre su atención en la evidencia rápidamente - reconocido en todo el mundo como el estándar en software forense informático

Con el crecimiento de los macrodatos provenientes de una amplia variedad de dispositivos y sistemas, puede resultar complicado encontrar y recopilar evidencia relevante de manera oportuna y eficiente. Ya sea que se trate de un organismo policial que se enfrenta a la creciente acumulación de dispositivos a la espera de ser procesados o de una empresa que busca entre enormes cantidades de datos de múltiples fuentes, FTK® reduce el tiempo de investigación y los recursos necesarios al brindarle una solución forense integrada preferida por los investigadores digitales expertos.

Qué es FTK

FTK es una solución de investigación digital galardonada y citada por los tribunales, diseñada para ofrecer velocidad, estabilidad y facilidad de uso. Localiza rápidamente pruebas y recopila y analiza de manera forense cualquier dispositivo o sistema digital que produzca, transmita o almacene datos mediante una única aplicación desde varios dispositivos. Conocido por su interfaz intuitiva, análisis de correo electrónico, vistas de datos personalizables, velocidades de procesamiento y estabilidad, FTK también establece el marco para que su solución pueda crecer con las necesidades de su organización para una expansión sin problemas.

A diferencia de otros productos del mercado, FTK ofrece:

Una base de datos de casos compartida

Toda la evidencia digital se almacena en una base de datos de casos, lo que proporciona a los equipos acceso a la evidencia del caso más actualizada. Reduce el tiempo, el costo y la complejidad de gestionar sus casos. No experimentará fallas asociadas con herramientas basadas en memoria como puede ocurrir con otros productos del mercado. Por ejemplo, si la GUI falla, el procesamiento continuará y, lo mejor de todo, existe una transferencia de datos continua entre las soluciones forenses y de descubrimiento electrónico de Exterro, lo que permite una verdadera colaboración entre todas las partes que trabajan en el caso.

Velocidad de procesamiento inigualable y un entorno más confiable

Con un procesamiento personalizable, tiene la capacidad de establecer estándares de procesamiento para toda la empresa, lo que genera coherencia en sus investigaciones y reduce la posibilidad de que se pierdan datos. Dado que la evidencia se procesa por adelantado, no tiene que esperar a que se ejecuten las búsquedas durante la fase de análisis. FTK está diseñado para proporcionar el procesamiento más rápido, preciso y consistente con procesamiento distribuido y verdadera compatibilidad con múltiples subprocesos y núcleos.

¿Por qué compatibilidad con subprocesos múltiples y núcleos múltiples?

FTK utiliza el 100 por ciento de sus recursos de hardware y es más confiable en caso de fallas de hardware o software. También puede beneficiarse de procesar datos más rápido, ya que FTK utiliza todos los recursos de hardware.

Búsqueda más rápida con resultados consistentes

La indexación se realiza por adelantado, por lo que el filtrado y la búsqueda son más rápidos que con cualquier otra solución. FTK ofrece la flexibilidad de realizar revisiones de datos en varias pasadas y cambiar las opciones de indexación sin tener que volver a procesar los datos. Ya sea que se encuentre en la fase de investigación o realizando una revisión de documentos, tiene un archivo de índice compartido, lo que elimina la necesidad de recrear o duplicar el archivo. Lo más importante es que recibirá resultados de búsqueda consistentes.

Además, obtenga todas estas características importantes...

FTK permite a los usuarios crear imágenes, procesar y analizar una amplia gama de tipos de datos, desde imágenes forenses hasta archivos de correo electrónico y dispositivos móviles, crear secuencias de comandos personalizadas, revisar datos sin conexión y escalar con procesamiento distribuido y la nube, todo dentro de una única solución.

Integración con QView®

Disfrute de la interfaz de revisión simple, intuitiva y personalizable basada en paneles de QView. Diseñado teniendo en cuenta al revisor, QView utiliza funciones de múltiples casos, como etiquetado, búsqueda, rotulación y marcadores en múltiples casos. Además, la sencilla aplicación de chat móvil y la revisión multimedia, junto con la detección de rostros e imágenes similares, están respaldadas por una base de datos unificada.

Reconocimiento Facial y de Imágenes

Entrene su sistema para buscar personas específicas o encontrar objetos dentro de imágenes y luego filtre los resultados para que solo observe esas imágenes. Agilice las investigaciones y establezca conexiones sin tener que revisar cada imagen o miniatura.

Detección Facial y de Objetos

Localice rápidamente todas las imágenes de una persona u objeto en el caso sin tener que entrenar el sistema. Además, tiene la capacidad de cargar una imagen desde fuera del caso y compararla con imágenes dentro del caso actual sin ingerirla.

Administre Datos Móviles

Localice, administre y filtre datos móviles más fácilmente con una pestaña móvil dedicada y un filtro de aplicación de mensajes para aislar los datos de aplicaciones de mensajería como WhatsApp® y Facebook®. Además, podrá revisar de manera intuitiva los informes de UFED, los archivos de casos de XRY y las conversaciones de correo electrónico y chat en un visor casi nativo.

Evidencias de correo electrónico basadas en la Web y en el navegador de Internet

Casi todas las investigaciones implican el análisis de artefactos de Internet. Los cachés de navegación web almacenan registros de los sitios que ha visitado un sospechoso; los

correos electrónicos basados en la Web pueden ayudar a demostrar la intención o correlacionar otros eventos y las conversaciones de mensajería instantánea o los sitios de redes sociales pueden contener evidencia. FTK agrupa el historial de búsqueda de URL de todos los navegadores en una sección, organizado por fecha, hora y categoría (por ejemplo, Adultos, Chat, Dark Web, Noticias, etc.)

Cree secuencias de comandos Python® personalizadas

Ejecute su propia secuencia de comandos Python dentro de FTK y elimine el riesgo de pérdida de datos al mantenerlos en una sola ubicación.

Procesamiento Distribuido

Agregue hasta tres motores de procesamiento distribuido sobre la marcha con escalado automático, lo que genera una mejor asignación de recursos.

Estuche Portátil

Exporte sus datos a un estuche portátil para revisarlos sin conexión. No es necesario perder tiempo generando informes que solo se pueden ver en un par de formatos diferentes. El estuche portátil le facilita la vida con una exportación rápida. Además, las etiquetas y los marcadores creados por los revisores se sincronizan con el estuche original.

Utilice el Poder de la Nube

Logre flexibilidad y ahorre dinero utilizando el poder de la nube para escalar su entorno: solo lleve su propia licencia al mercado.

Compatibilidad con Sistemas de Archivos de Apple®

A medida que BYOD se ha apoderado del mercado, las organizaciones necesitan procesar datos de dispositivos Apple con frecuencia. Con FTK, puede analizar rápidamente los datos de cualquier sistema operativo de Apple hasta macOS® 10.15 (Catalina).

Visualización

Construya automáticamente cronogramas e ilustre gráficamente las relaciones entre las partes interesadas en un caso. Con Email, Social and File Visualization, puede ver datos en múltiples formatos de visualización, incluidos cronogramas, gráficos de clúster, gráficos circulares, geolocalizaciones y más, para ayudarlo a determinar relaciones y encontrar piezas clave de información. Luego, genere informes que sean fácilmente utilizados por abogados, CIO's u otros investigadores.