

# Características y funciones de EnCase® Forensic

## Toda investigación es importante



Los investigadores de datos digitales necesitan una solución que capture con facilidad los datos relevantes para respaldar investigaciones o requisitos de cumplimiento y que brinde capacidades de análisis técnico elaboradas para hallar datos ocultos. EnCase® Forensic es una poderosa plataforma de investigación que recolecta datos digitales, realiza análisis, informa sobre descubrimientos y los preserva en un formato válido a efectos legales y validado por los tribunales.

### Cómo funciona EnCase® Forensic:

#### 1) Obtenga adquisiciones válidas a efectos legales

EnCase® Forensic produce una duplicación binaria exacta del dispositivo o medio original y luego la verifica generando valores hash MD5 de las imágenes y asignando valores de CRC a los datos. Estas verificaciones revelan cuándo la evidencia ha sido alterada o manipulada indebidamente, ayudando a mantener toda la evidencia digital con validez a efectos legales para su uso en procedimientos judiciales.

#### 2) Ahorre tiempo valioso con funciones de productividad avanzadas

Los examinadores pueden obtener una vista previa de los datos mientras se obtiene acceso a las unidades u otros medios. Una vez creados los archivos de imagen, los examinadores pueden buscar y analizar varias unidades u otros medios simultáneamente. EnCase Forensic también ofrece un indexador de casos. Esta poderosa herramienta crea un índice completo en varios idiomas, lo que permite realizar consultas de forma rápida y sencilla. Los índices se pueden asociar entre sí para buscar palabras clave comunes a otras investigaciones. Este índice compatible con Unicode contiene documentos personales, archivos eliminados, artefactos de sistemas de archivos, demora de archivos, archivos intercambiados, espacio no asignado, correos electrónicos y páginas web. Además, EnCase ofrece una amplia compatibilidad con distintos sistemas de archivos, brindándoles a las organizaciones la posibilidad de analizar todo tipo de datos.

#### 3) Personalice EnCase® Forensic con la programación EnScript®

EnCase Forensic ofrece las capacidades de programación EnScript®. EnScript, un lenguaje de programación orientada a objetos y similar a Java o C++, les permite a los usuarios crear programas personalizados que los ayuden a automatizar las tareas de investigación que demandan mucho tiempo, como la búsqueda y el análisis de tipos de documentos específicos u otros procesos y procedimientos que requieren mucho trabajo. Esta función puede ser implementada por investigadores de cualquier nivel mediante el uso de las herramientas de Forensic, como "Case Developer" o uno de los diversos filtros y condiciones integrados.

#### 4) Proporcione datos procesables, genere informes y continúe con el siguiente caso

Una vez que los investigadores han detectado los datos relevantes, pueden crear un informe apto para la presentación ante los tribunales, la gerencia u otra autoridad legal. Los datos también se pueden exportar en diversos formatos de archivo para su revisión.

## Lista de características y funciones de EnCase Forensic

### Adquisición

- Granularidad de adquisición:
  - Errores: especifica la cantidad de sectores que muestran ceros cuando se encuentra un error.
  - Bloques de adquisición: define el tamaño del bloque.
- Reinicio de adquisición: continúa con una adquisición basada en Windows desde su punto de interrupción.
- Archivos de evidencia lógica: un contenedor de evidencia que incluye sólo los archivos y carpetas que necesita.
- CRC: imagen verificada por comprobación de redundancia cíclica (CRC) y MD5.
- Utilidad LinEn: adquiere evidencia a través del disco de inicio.
- Utilidad WinEn: adquiere evidencia de RAM.

### Herramientas de automatización: aceleran el proceso de investigación.

- EnScript: genera secuencias de comandos o utiliza las secuencias de comandos creadas previamente.
- Filtros y condiciones: más de 150 filtros y condiciones disponibles.
- Combina filtros para crear consultas completas utilizando la lógica simple "OR" o "AND".
- Extractor de información de directorio activo
- Análisis de hardware: selecciona automáticamente los archivos de registro y configuración.
- Recuperar particiones: reconstruye automáticamente la estructura de volúmenes NTFS y FAT con formato.
- Recuperar archivos/carpetas eliminados

### Funciones de análisis

- Analizador de registro de eventos de Windows
- Vincular analizador de archivos: realiza búsquedas en espacio no asignado.
- Documentos y archivos compuestos (por ejemplo, archivos comprimidos)
- Análisis de firmas de archivos
- Análisis de hash
- Buscador de archivos: busca archivos en espacio no asignado.

### Visores

- Visualización nativa para 400 formatos de archivo
- Visor de registro integrado
- Visores de archivos externos
- Visor de imágenes integrado con vista de galería
- Visor de línea de tiempo/calendario

### Búsqueda

- Búsqueda por índice Unicode: busca texto extraído de documentos.
- Búsqueda binaria: busca datos binarios sin procesar.
- Búsqueda por proximidad
- Búsqueda en Internet y correo electrónico
- Distinguir entre mayúsculas y minúsculas • GREP • Lectura de derecha a izquierda
- Página de código activo: palabras clave en varios idiomas

- Big Endian/Little Endian, UTF-8/UTF-7
- Buscar demoras de archivos y espacio no asignado

### Generación de informes: informes automáticos

- Lista de todos los archivos y carpetas en un caso
- Lista detallada de todas las direcciones URL y las correspondientes fechas y horas de visitas a sitios web
- Documentar informes de respuesta a incidentes
- Almacenar registros
- Registro
- Información detallada del disco duro respecto de las particiones físicas y lógicas
- Ver datos acerca de la adquisición, geometría de unidades, estructuras de carpetas y archivos e imágenes seleccionados
- Exportar informes en formato RTF o HTML

### Funciones de marcador

- Datos resaltados
- Notas
- Información de carpetas
- Archivos relevantes
- Grupos de archivos

### Investigación del uso de Internet y del correo electrónico

#### Análisis del historial navegador web

- Artefactos de Internet
- Análisis de la memoria caché y del historial WEB
- Analizador de HTML
- Reconstrucción de páginas HTML
- Kit de herramientas Kazaa
- Kit de herramientas de mensajería instantánea: Microsoft® Internet Explorer, Mozilla Firefox, Opera y Apple Safari

#### La compatibilidad con correo electrónico incluye

- Archivos PST/OST de Outlook ('97-'03)
- Archivos DBX de Outlook Express
- Analizador de archivos EDB de Microsoft Exchange
- Lotus Notes versión 6.0.3, 6.5.4 y 7
- Archivos PFC de AOL 6.0, 7.0, 8.0 y 9.0
- Yahoo
- Hotmail
- Netscape Mail
- Archivos MBOX

### Compatibilidad del sistema

- Conjuntos redundantes de discos independientes (RAID) de hardware y software
- Compatibilidad de disco dinámico para Windows 2000/XP/2003 Server
- Interpretar y analizar formatos de imágenes de VMware, Microsoft Virtual PC, DD y SafeBack versión 2
- Sistemas de archivos: FAT12/16/32 y NTFS de Windows; HFS y HFS+ de Macintosh; UFS y ZFS de Sun Solaris; EXT2/3 de Linux; Reiser; BSD FFS, Fast File System 2 (FFS2) de FreeBSD y UFS2 de FreeBSD; NSS & NWFS de Novell; AIX jfs de IBM, JFS y JFS con LVM8; TiVo serie uno y dos; CDFS; Joliet; DVD; UDF; ISO 9660; y Palm

## Acerca de Guidance Software (GUID)

Guidance Software es reconocida en todo el mundo como una empresa líder en soluciones de investigación digital. La plataforma EnCase® brinda la base para que las organizaciones gubernamentales y empresariales y las organizaciones encargadas del cumplimiento de la ley lleven a cabo investigaciones informáticas exhaustivas, habilitadas para redes y validadas por tribunales de cualquier tipo, como respuesta a solicitudes de medios de prueba de fuentes electrónicas, investigaciones internas, respuesta a consultas reglamentarias o auditorías de datos y cumplimiento, y, al mismo tiempo, puedan mantener la integridad de los datos. Existen más de 30.000 usuarios con licencia de la tecnología EnCase en todo el mundo y miles asisten anualmente a los renombrados programas de capacitación de Guidance Software. Validado por varios tribunales, departamentos legales de empresas, agencias gubernamentales y organizaciones encargadas del cumplimiento de la ley de todo el mundo, EnCase ha sido distinguido con muchos premios y reconocimientos de la industria por parte de eWEEK, SC Magazine, Network Computing y Socha-Gelbmann. Para obtener más información acerca de Guidance Software, visite [www.guidancesoftware.com](http://www.guidancesoftware.com).

©2009 Guidance Software, Inc. Reservados todos los derechos. EnCase y Guidance Software son marcas registradas o marcas comerciales de Guidance Software en los Estados Unidos y en otras jurisdicciones y no se pueden utilizar sin autorización previa por escrito. Todas las otras marcas pueden ser reclamadas como propiedad de sus respectivos propietarios.