www.eysglobal.com

MÓDULO 1

TEMA 19:HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE PARTE 1

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

HERRAMIENTAS:

Las herramientas de análisis forense digital son todas relativamente nuevas. A medida que los dispositivos se volvieron más complejos y vinculados con más información, el análisis en vivo se volvió inmanejable e improductivo. Posteriormente, el freeware y las tecnologías especializadas aparecieron como hardware y software para extorsionar, localizar o filtrar datos en un dispositivo sin modificarlo ni destruirlo.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Existes diversas categorías de herramientas de análisis forense digital, dentro de las que se incluyen análisis forense de bases de datos, análisis de correo electrónico, apropiación de disco y datos, visores de archivos, análisis de archivos, análisis de Internet, análisis forense de redes, análisis de dispositivos móviles y análisis de registros. Muchas herramientas cumplen más de una función juntas, y una tendencia importante en las herramientas forenses digitales es aquella que agrupa cientos de tecnologías específicas con varias funcionalidades en un conjunto de herramientas general.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Al considerar las herramientas de análisis forense, es difícil cómo elegir una. Al seleccionar entre la amplia gama de opciones, analizamos los siguientes criterios:

Coste razonable: el precio puede no ser un indicador de calidad, pero las revisiones colaborativas pueden serlo. La mayoría de las herramientas son de código abierto, gratuitas y compatibles con un grupo de desarrolladores dedicados.

Accesibilidad: a diferencia de algunas marcas establecidas que solo venden sus productos a las autoridades policiales, el resto son accesibles para las personas.

Responsabilidad: ya sea a través de planes de código abierto o credenciales del mundo real, estas tecnologías han sido evaluadas completamente por especialistas.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Un examinador forense digital experimentado sabrá qué herramienta o herramientas son las mejores para el tipo de dispositivo y el tipo de datos.
Independientemente de la herramienta o software que utilice, debe validarse.
Un examinador forense digital debe asegurarse de que la información producida por el software forense sea precisa.
Un examinador forense tiene que saber dónde se almacena la información y cómo la herramienta forense elegida analiza esa información.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Software de código abierto vs. comercial

Hay veces que, si un examinador forense ve algo que no parece correcto o que no tiene ningún sentido, se puede usar software de código abierto para validar el software comercial mediante la comparación de resultados. Si los resultados de diferentes softwares varían en formas que no se esperaban, entonces es hora de realizar una investigación y / o soporte técnico de software.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Puede ser que ya tengas un software que le resulte de utilidad a tu equipo forense, como Google Vault o Takeout. BlackBag Technology ofrece capacitación gratuita de dos días. El Instituto SANS ofrece un juego de herramientas forenses y seminarios web gratuitos que obtienen créditos de CPE.

Todo buen laboratorio forense debe tener un equilibrio saludable de software forense de calidad por parte de proveedores líderes y de código abierto, y el conocimiento para respaldarlos.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Comparación de herramientas forenses informáticas:

La informática forense es una rama muy vital de la informática en relación con los escándalos relacionados con la informática e Internet. Anteriormente, los ordenadores solo se manejaban para generar datos, pero ahora se ha desarrollado para todos los dispositivos vinculados a datos digitales.

El objetivo de la informática forense es realizar investigaciones de delitos utilizando pruebas de datos digitales para determinar quién es el responsable de ese delito en particular.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

1. EnCase

EnCase es un producto creado para análisis forense, seguridad digital, investigación de seguridad y procesos de descubrimiento electrónico. Generalmente se usa para recuperar pruebas de discos duros robados. Permite a la autoridad dirigir un examen total de las cuentas de los clientes para recopilar evidencia digital que pueda usarse en un tribunal de justicia.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Ventajas

- Con la versión avanzada de pago de Encase que contiene todas las utilidades, también tiene una versión gratuita que se puede aplicar para la adquisición de confirmación, que es muy simple de usar. Esta herramienta se reconoce como Encase Imager.
- En términos de características de procesamiento y análisis, esta herramienta también tiene buenos informes integrados
- Con el aumento de las amenazas cibernéticas, el cifrado representa un papel importante en la defensa de los datos en cualquier tipo o variedad de sistema.
- Encase tiene soporte incorporado para casi todos los tipos de encriptación, incluidas buenas capacidades de búsqueda de palabras clave y funciones de scripting accesibles.
- Hay mucha aceptación de Encase para forense móvil.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Desventajas

- Esta es una herramienta muy costosa.
- El procesamiento de Encase puede llevar mucho tiempo en caso de archivos agregados muy grandes y buzones.
- Las versiones más recientes de Encase a veces no se ajustan a otras herramientas forenses.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Kit de herramientas forenses:

El Kit de herramientas forenses (FTK) es un paquete de software de investigación forense por computadora. Comprueba un disco duro buscando información diferente.

Puede, por ejemplo, encontrar correos electrónicos borrados y también puede examinar el disco en busca de secuencias de contenido. Estos pueden ser utilizados como una palabra clave secreta relacionada con romper cualquier cifrado.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Ventajas

- Tiene una interfaz de usuario sin complicaciones y excelentes capacidades de búsqueda.
- FTK confirma el descifrado de EFS.
- Da un archivo de registro de casos.
- Tiene importantes funciones de marcadores e informes destacados.
- FTK Imager está disponible de forma gratuita.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Desventajas

- FTK no respalda las funciones de secuencias de comandos.
- No tiene habilidades multitarea.
- No hay barra de progresión para ver el tiempo restante.
- FTK no tiene una representación de línea de tiempo.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

XWF (X-Ways): X Ways Forensics :es una robusta herramienta de informática forense empresarial. Es un software autorizado basado en Windows que permite muchas funcionalidades relacionadas con la informática forense. Uno de los mejores beneficios de este software es que se puede usar en modo transportable.

Ventajas

- Las opciones de procesamiento de pruebas se pueden personalizar según las especificaciones del caso.
- Tiene una opción de filtrado muy adaptable y granular, así como fines de búsqueda altamente personalizables.
- Es de naturaleza portátil y revisa constantemente las nuevas innovaciones.

Desventajas

- No es fácil de usar.
- Es un software basado en dongle y no funciona sin él.
- No hay provisión para Bitlocker.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

4. Oxygen Forensic Suite

El paquete Oxygen Forensics es un software forense móvil para el análisis lógico de teléfonos inteligentes, teléfonos celulares y PDA. La suite puede recuperar información del dispositivo, contactos, eventos del calendario, SMS, registros de ocasiones e informes.

Además, también puede derivar diferentes tipos de metadatos que son esenciales en cualquier investigación forense digital. La suite llega al dispositivo utilizando protocolos establecidos.

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE

Ventajas

•Oxygen permite la extracción física de información y datos de dispositivos Android.

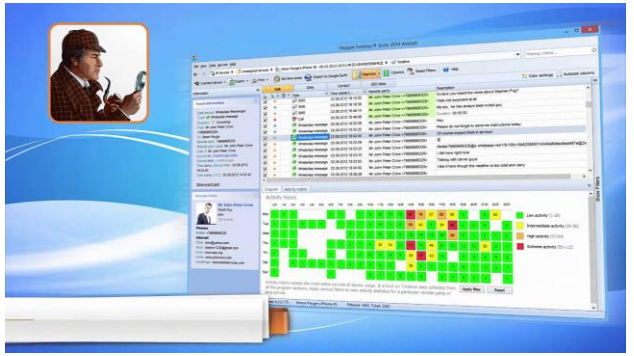
•La interfaz de usuario y las opciones son muy manejables y fáciles de seguir.

•El informe final se puede almacenar en muchos formatos legibles como .xls, .xlsx, .pdf, etc.

•Es una opción económicamente más adecuada en comparación con otras herramientas de análisis forense.

•Tiene una funcionalidad incorporada que se puede utilizar para romper contraseñas para reservas cifradas de iTunes, iPhone bloqueado o Android .

HERRAMIENTAS Y TÈCNICAS DE ANÀLISIS FORENSE



Desventajas

- Su soporte para una gama de dispositivos móviles está limitado.
- Dado que la herramienta está basada en computadora, existe la probabilidad de que el malware penetre dentro del teléfono que se está investigando.
- Utiliza una técnica de fuerza bruta que provoca mucho tiempo para completar el proceso.