www.eysglobal.com

MÓDULO 1
TEMA 13: HERRAMIENTAS

HERRAMIENTAS

Como saben, no sólo los delitos tecnológicos están en auge, sino también los delitos de toda la vida perpetrados mediante el uso de la informática y las nuevas tecnologías. Por ello hay una serie de herramientas de uso común para todo perito informático que paso a enumerar someramente:

LAS CLONADORAS DE DATOS

LAS BLOQUEADORAS

GENERADORES DE CÓDIGOS HASH

SUITES DE HERRAMIENTAS FORENSES

HERRAMIENTAS DE FIRMA ELECTRÓNICA

CARACTERÍSTICAS DE LAS HERRAMIENTAS FORENSES PROFESIONALES

Las características de las herramientas forenses profesionales varían mucho dependiendo de la rama del análisis forense y el mercado al que están orientados. Generalmente, las grandes suites de software forense tienen que ser capaces de hacer lo siguiente:

CARACTERÍSTICAS DE LAS HERRAMIENTAS FORENSES PROFESIONALES

:

- ✓ Support hashing of all files, which allows comparative filtering
- ✓ Hash de disco completo para poder confirmar que los datos no han cambiado (normalmente se utiliza una herramienta para adquirir y otra para confirmar el hash de disco)
- ✓ Localizadores de rutas exactas
- ✓ Borrar los sellos de fecha y hora
- ✓ Tiene que incluir una característica de adquisición
- ✓ Búsqueda y filtrado de artículos
- ✓ La capacidad de cargar copias de seguridad de iOS y analizar sus datos

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

BlackLight de BlackBag:es la herramienta forense para Mac número uno en el mercado en este momento y cuesta aproximadamente $2600. BlackLight comenzó su actividad hace 5 años, desarrollando una herramienta forense sólo para Mac. Ahora se ha convertido en una buena herramienta de inspección para Windows también. Analizará todos los dispositivos iOS, así como Android. Sin embargo, no es capaz de analizar dispositivos BlackBerry. Una cosa que Blacklight no hace por sí sola es la adquisición forense de clones bit por bit. Ofrecen una herramienta adicional llamada MacQuisition.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

AccessData es el principal proveedor de E-Discovery, Informática Forense de Dispositivos Móviles y Ordenadores para corporaciones, bufetes de abogados y agencias gubernamentales. Entre sus soluciones forenses digitales están Forensic ToolKit (FTK), que proporciona un procesamiento e indexación exhaustivos iniciales, por lo que el filtrado y la búsqueda son más rápidos que con cualquier otra solución del mercado.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

Guidance Software, fundada en 1997, desarrolla EnCase Forensic Software que es una herramienta de análisis forense para PC que ha sido el pilar del forense desde hace más de una década. La herramienta ha logrado ocupar los titulares en 2002 cuando se utilizó en el juicio de asesinato de David Westerfield para examinar sus computadoras para encontrar pruebas de pornografía infantil y cuando la policía francesa utilizó EnCase para descubrir correos electrónicos cruciales de Richard Colvin Reid, también conocido como el Shoe Bomber.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

Desarrollada por un ex oficial de policía y programador, Magnet Forensics es una plataforma completa de investigación digital utilizada por más de 3.000 agencias y organizaciones por todo el mundo. Originalmente, comenzó como una herramienta para el análisis forense de Internet, pero ahora se ha expandido para convertirse en una suite forense completa. Magnet Forensics puede hacer adquisiciones de datos físicos de teléfonos donde sea posible (la mayoría de Android y iPhone 4 e inferior, y BlackBerry). Estas adquisiciones físicas pueden ser cargadas en herramientas como Cellebrite.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

X-Ways es relativamente nuevo en el análisis forense, pero la compañía se está volviendo muy popular debido a su velocidad de innovación. Desarrollado por un equipo de ingenieros alemanes, las herramientas forenses de X-Ways hacen un trabajo fantástico cuando se trata de imágenes de disco, clonación de disco, reconstrucción de RAID virtual, análisis de unidad de red remota, acceso remoto a RAM, acceso a almacenamiento en la nube y más. La desventaja es que requieren una experiencia considerable para su uso.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

Una subsidiaria de la Corporación Sun de Japón, Cellebrite Mobile Synchronization es una compañía israelí que se considera ser el líder cuando se trata de software forense móvil. Su principal herramienta móvil viene con un precio muy alto de $ 12.000 USD y una licencia anual alrededor de $ 4000. Es un servicio de primera categoría y de alto precio que proporciona una visión profunda de los dispositivos móviles a través de la plataforma Unified Digital Forensics de Cellebrite.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

CERT significa equipo de respuesta a emergencias informáticas. La organización fue establecida en 2003 en Estados Unidos para proteger la infraestructura de Internet de la nación contra ataques cibernéticos. Ellos han desarrollado varias herramientas utilizadas por la aplicación de la ley, incluyendo CERT Triage Tools. Las herramientas de Triage se utilizan para capturar RAM y realizar adquisiciones en escena. El producto también incluye una extensión de GNU Debugger llamada “exploitable” que es capaz de clasificar los errores de aplicación de Linux por su gravedad. Actualmente, CERT Triage Tools está siendo desarrollado públicamente en GitHub.

PROVEEDORES DE SOFTWARE FORENSE IMPORTANTES

Disk Drill Asume la Recuperación de Datos Forense

Disk Drill es una herramienta de recuperación de datos probada que ha sido utilizada con éxito por innumerables usuarios en todo el mundo para recuperar documentos, imágenes, archivos de vídeo y otros tipos de datos de una variedad de dispositivos de almacenamiento diferentes.