Escuela Técnica Superior de Ingeniería Informática
Universitat Politècnica de València

Clasificación y estudio de herramientas para periciales informáticas

Proyecto Final de Carrera

[INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN]

Autor: Alberto José Pedrera Ros

Director: Juan Vicente Oltra

03/02/2015

Tabla de contenidos

Objeto y objetivos 5
Introducción. 6
Herramientas utilizadas para análisis forense. 10
Tabla de herramientas ordenadas alfabéticamente 116
Legislación relacionada 117
Delitos informáticos 123
Conclusiones. 125
Bibliografía. 127
Enlaces de busquedas de herramientas 127

Objeto y objetivos

Los objetivos que se persiguen con el presente Proyecto de Fin de Carrera son la presentación de diversas herramientas para realizar análisis forense digitales con garantías.

Tras la realización de una incursión en el Peritaje Informático, tras la realización de un curso de tres semana, me parecio una opción muy interesante la realización de este proyecto como ampliación de mis conocimientos en el análisis forense digital.

Mi objetivo con la presentación de este proyecto, aparte de ampliar mis conocimientos y de conocer herramientas importantes para la realización con éxito de un análisis forense digital, en la ayuda a posibles personas que se quieran introducir en este campo, recopilando información útil para un principiante y para que pueda disponer, de forma rápida, de una visión general desde los posibles delitos informáticos que se pueden encontrar, pasando por las herramientas que se pueden utilizar para hacer el análisis hasta la creación de un informe en condiciones para poder presentarlo en un caso, y por ultimo presentando una pequeña recopilación de las leyes mas importantes, Españolas, utilizadas en la actualidad.

He intentado no valorar las herramientas, listadas en el presente documento, porque la funcionalidad es muy dispar y no he podido probarlas como me hubiera gustado, por falta de tiempo, por lo que he decidido presentarlas con las características que tienen en sus páginas web.

Espero que este documento sirva de apoyo a los que quieran iniciarse en el Peritaje Informático.

A nivel personal, el presente Proyecto de Fin de Carrera, además de enriquecer mis conocimientos en la materia investigada, tiene por propósito, la obtención del título de Ingeniería Técnica en Informática de Gestión Expedido por la Universidad Politécnica de Valencia.

Introducción.

Desde los comienzos de la comunicación, ha habido información que se ha querido mantener en secreto, ya sea, por motivos económicos, personales o de otra índole. También han existido individuos que por curiosidad o por cualquier otro motivo, han intentado acceder a esa información "protegida".

En esta lucha constante entre la protección de la información y el intento de acceso a dicha información, es donde encontramos las pruebas y delitos, en los que se basa este proyecto, y más concretamente, en los telemáticos.

El presente documento pretende poner de manifiesto la problemática de los delitos informáticos desde que existe la comunicación a través de las redes telefónicas.

En la primera parte del proyecto, se verá una breve historia de la delincuencia informática, su evolución y los diferentes tipos de delincuentes, explicando brevemente la problemática con casos reales.

A continuación se lista una serie de herramientas utilizadas para seguridad y protección de datos, ya sea para salvaguardar los datos de posibles ataques, o para intentar recuperar los datos, una vez se ha producido un ataque.

Las herramientas mencionadas en el presente documento se utilizan para análisis forenses, ya que permite su utilización, desde hacer clonaciones de discos, pasando por la búsqueda de

ficheros borrados, e-mails enviados, hasta la búsqueda de pruebas en un dispositivo ha sido manipulado con fines ilícitos.

Una vez se tiene una idea básica de las herramientas y de sus usuos se muestra una tabla donde se podrá comprobar, de una manera rápida y sencilla, la clasificación de las herramientas, por orden alfabetico, estudiadas en el documento y sus distintas funcionalidades y precios.

En el siguiente capitulo se muestrán las leyes, más importantes, que actualmente legislan los delitos telemáticos en España. Es una breve muestra de la legislación que se aplica en los posibles delitos que se enjuician.

Por último se muestán los delitos más habituales actualmente, se explica brevemente en que consiste cada uno y la legislación que se emplearía en cada caso.

El documento pretende ser una guía para dar una idea de las herramientas que se utilizan en los análisis digitales forenses, es un listado limitado en el que he pretendido dar una idea de algunas herramientas y mostrar que existen herramientas para cualquier caso y de cualquier precio, desde open source hasta de pago.

Existen Suites completas ya montadas, con las que solo se necesita la instalación para ponerse en marcha, o simples herramientas para realizar alguna operación concreta. Con diferentes niveles de exigencia, desde analistas principiantes hasta profesionales.

Deseo que pueda resultar de ayuda a cualquier persona que necesite iniciarse en el análisis digital forense.

Historia de la Informática y los delitos Informáticos.

Desde que en 1876 Alexander Graham Bell inventó el teléfono, ha habido gente que ha intentado el acceso al servicio y a la información que se transmitía.

En 1878, menos de dos años después de que se pusiera en marcha la red telefónica un grupo de adolescentes la echaron abajo.

En 19858, se creó en EEUU el ARPA (Advanced Research Projects Agency), un proyecto de ciencia y tecnología aplicada al campo militar.

En 1960, aparecieron los primeros Hackers, que utilizaron los primeros mainframes del MIT, y se referían a los individuos que tenían habilidades y el potencial necesarios para utilizar dichos ordenadores. En un principio, el término era considerado como un elogio, al considerarse una persona con grandes conocimientos.

En 1969, el Departamento de Defensa de los EEUU construyo Arpanet, una red, exclusivamente militar, para compartir información.

En 1971, los *phreakers* empezaron a utilizar la extensa base de redes telefónicas. John Draper descubrió que el simple sonido de un silbato permitía acceder a los sistemas de facturación de las llamadas a larga distancia.

En 1973, Khan desarrolló un novedoso protocolo, llamado TCP/IP, *Transmision Control Computer/Internet Protocol,* para controlar la trnamisión de datos a través de la red telefónica.

En 1976, unos miembros de Homebrew Computer Club utilizaron para hackear sistemas telefónicos las llamadas *Blue Box*. También en ese año se fundó Apple Computer, sus creadores fueron Steve Jobs y Steve WozniaK.

En 1983, comienza una lucha entre el FBI y cuerpos de seguridad de EEUU contra los hackers, debido a la invasión del centro de investigación de los Alamos. Da comienzo a los primeros arrestos. También se estrena una película, *Juegos de Guerra,* relacionada con el tema y que dio otra perspectiva de los hackers y además les dio mayor prestigio.

En 1984, se crea un grupo de hackers, llamado *Legion of Doom (LoD).*

En 1987, es arrestado Herber Zinn, de 17 años de edad, después de haber accedido a los sistemas de AT&T, se comentó, que estuvo a punto de bloquear todo el sistema telefónico norteamericano. En este mismo año, se creó el primer virus informático, llamado *Brain*, infectaba el sector de arranque de los disquetes.

En 1988, se bloquearon 6000 ordenadores a través de ARPANET con un virus que se lanzó, según su creador, Robert Morris, de forma accidental. En este mismo año se funda el CERT (Computer Emergency Response Team). También apareció el primer antivirus, desarrollado en Indonesia.

En 1989, aparece el primer caso de ciberespionaje en Alemania Occidental. La publicación *The Mentor* lanzó un manifiesto, llamado *Conscience of a Hacker*, la cual finalizaba con una frase inquietante *"pueden detener a una persona, pero no pueden detenernos a todos"*.

En el año 1990 se lanzó un grupo de apoyo *Freedom on the Internet,* para una libre comunicación en Internet. También se crearos sofisticados virus informáticos, como los polimórficos y los de multipartición, ambos son virus "inteligentes", porque o se van modificando a si mismos mientras se expanden o infectan diversas zonas de una máquina, para tener más probabilidades de llegar a su fin. En este mismo año el *First National Citibank* de Chicago es atacado y sufre un robo de 70 millones de dólares. Después de 17 meses de investigaciones se consigue arrestar a Kevin Lee Poulsen, conocido en el mundillo hacker como *Dark Dante,* por robo de documentos secretos militares. Los hackers Mitnick y Shimomura se enfrentan, por un acceso del primero a las máquinas del segundo, buscando un programa de ocultación de llamadas.

En 1993, se celebró una conferencia, llamada *DefCon*, en las Vegas, para despedir a las BBS, ya obsoletas, pero se convirtió en un evento anual debido al éxito que obtuvo, convirtiéndose en la conferencia más importante en el mundo hacker. En DefCon se reúnen, anualmente, los hackers más importantes del mundo, exponiendo sus conocimientos o aplicándolos en las distintas competiciones que se realizan en la conferencia.

En 1994, son atacados sitios web federales de los EEUU, como la CIA, el departamento de Justicia, la NASA y la Fuerza Aerea. También en este mismo año se produce un robo, de 10 millones de dólares, en el Banco Citibank, presuntamente por Vladimir Lenin, un líder de un grupo de hackers ruso.

En 1995, como ejemplo de la cantidad de ataques que sufren las web más importantes, tanto gubernamentales como de multinacionales, el Departamento de Defensa sufrió 250000 ataques. El hacker Kevin Mitnick fue arrestado por presunto robo de 20000 dólares.

Herramientas utilizadas para análisis forense.

OSFClone

Desarrollador: PassMark Software

Página de la herramienta: http://www.osforensics.com/tools/create-disk-images.html

Tipo de Instalación: Existen dos tipos de instalación iso y zip, se puede instalar en un DVD o en un USB.

Tipo de Herramienta: Clone de Discos.

Uso: Se utiliza como disco de arranque y no necesita ningún sistema Operativo concreto, ya que se arranca desde el DVD o el USB.

Descripción: Es una herramienta libre, auto arracable, que abilita la creación o extracción pura de imágenes de disco rápidamente, es independiente de el sistema operativo. Como añadido OSFClone también es compatible con las unidades de imagen a la intemperie **AFF**, (**Advance Forensics Format**). AFF es de formato abierto y extensible para almacenar imagnes de disco y metadatos asociados. Un standart abierto habilita a los investigadores rápida y eficientemente el uso de sus herramientas favoritas para el análisis de dicos.

Foto descargada de http://www.osforensics.com/tools/create-disk-images.html

OSFClone crea imagines forenses de un disco, preservando los sectores no utilizados, espacio de holgura, de fragmentación de archivos y registros de archivos no eliminados del disco duro original. Arranque en OSFClone y crear clones de disco de FAT, NTFS y unidades USB conectadas! OSFClone se puede arrancar desde CD / DVD, o desde unidades flash USB.

OSFClone puede crear imágenes de disco en formato dc3dd. El formato dc3dd es ideal para la informática forense debido a su mayor nivel de presentación de informes de progreso y errores, y la capacidad para discutir archivos sobre la marcha.

Se puedecComprobar que un clon del disco es idéntica a la unidad de origen, mediante el uso de OSFClone se compara el hash MD5 o SHA1 entre el clon y la unidad de origen. Después de la creación de imágenes, se puede elegir entre una gama de opciones de compresión para reducir el tamaño de la imagen que se acaba de crear, aumentar la portabilidad y el ahorro de espacio en disco.

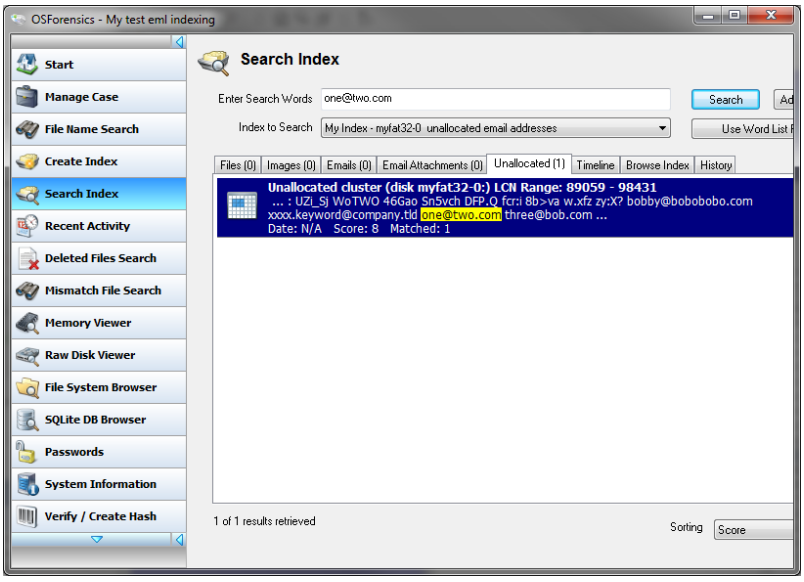


Foto descargada de http://www.passmark.com/forum/showthread.php?3904-Corrupt-Case-Item

Se puede utilizar **OSFClone** para salvar meta-datos forenses (por ejemplo, número de caso, el número de pruebas, el nombre del examinador, descripción y suma de comprobación) de imágenes clonadas o creadas.

Conclusiones: Se trata de un herramienta para crear imágenes de disco, con opciones para el análisis forense, como pueden ser los metadatos que se pueden almacenar, se puede utilizar en diferentes Sisitemas Operativos, etc.

Permite la compresión de las imágenes, además de poder comparar la imagen y el disco.

Se puede considerar una herramienta bastante óptima, y con opciones para el uso en el análisis forense.

DriveClone

Desarrollador: FarStone

Página de la herramienta: http://www.farstone.com/software/drive-clone.php

Tipo de Instalación: Descarga para instalar la herramienta.

Tipo de Herramienta: Clone de Discos.

Uso: Se utiliza directamente desde el dispositivo.

Descripción: Es una herremianta para la clonación de Discos Duros y unidades de estado solido, también permite la migración de software.

DriveClone permite la clonación automática de todo el equipo, entre los que se incuyen lo archivos del sistema, las aplicaciones, correos electrónicos, etc. Pero lo que destaca **CloneDrive** del resto de herramientas similares es que desfragmenta automáticamente todos los archivos, elimina la basura, cambia el tamaño de las particiones, y sólo clonar los archivos que han sido modificados desde la última clonación.

La clonación creada permite el arranque inmediato en equipos diferentes, ya que se crea un disco espejo de arranque universal, para la recuperación inmediata de desastres.

Los pasos a seguir para realizar una clonación de un disco serian:

1. Conecte un disco duro USB externo

Foto descargada de http://www.farstone.com/software/drive-clone.php

2. Instale DriveClone

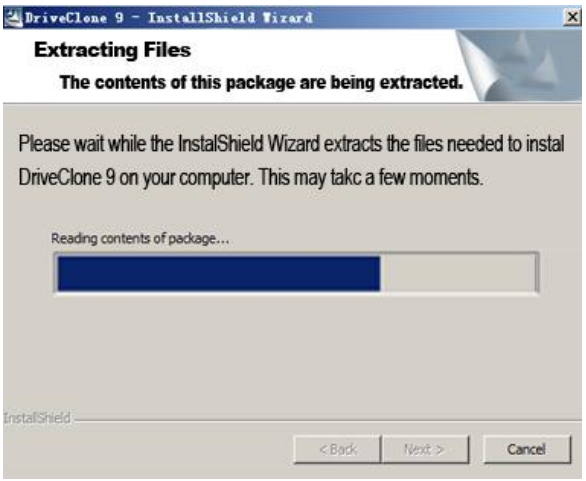


Foto descargada de http://www.farstone.com/software/drive-clone.php

3. DriveClone clonar el disco duro en el disco duro USB externo

Foto descargada de http://www.farstone.com/software/drive-clone.php

4. Retire el disco duro de la caja externa USB

Foto descargada de http://www.farstone.com/software/drive-clone.php

5. Vuelva a colocar la unidad de disco duro en el equipo por el nuevo disco duro.

Foto descargada de http://www.farstone.com/software/drive-clone.php

Conclusiones: Es una herramienta que permite la clonación de dispositivos, discos duros y unidades de estado sólido, dando una serie de ventajas, desfragmentación, clonación versionada, etc.

Es una herramienta que destaca por los añadidos que ayudan para optimizar las clonaciones.

Acronis True Image

Desarrollador: Acronis

Página de la herramienta: http://www.acronis.com/

Tipo de Instalación: Descarga de archivo de instalación en la máquina.

Tipo de Herramienta: Clone e imagenes de discos.

Uso: Herramienta ejecutable desde la que se pueden utilizar sus funcionalidades.

Descripción: Herramienta de pago, para realizar copias de seguridad de imágenes completas y recuperaciónde la totalidad de su sistema: música, fotos, vídeos, documentos, configuraciones personales, marcadores y todo tipo de aplicaciones.

Se puede almacenar la imagen en dispositivos locales o en la nube. Se puede guardar sitemas completos o archivos individuales, y recuperarlos en cualquier momento del tiempo, ya que mantiene un historial de las versiones realizadas.

Si se elije la opción de almacenamiento en la nube, existen diversos planes, que oferta Acronis, donde permite almacenar las imágenes en su propia nube, se necesita una herramienta extra, True Image, para acceder a las imágenes creadas.

Se pueden realizar copiasen un dispositivo y más tarde recuperarlas desde otros dispositivos diferentes. Dispone de una intefaz moderna, desde la que se realizan las copias de una manera sencilla y rápida.

Se puede utilizar la herramienta tanto en PCs Windows, en una gran variedad de versiones, hasta Macs.

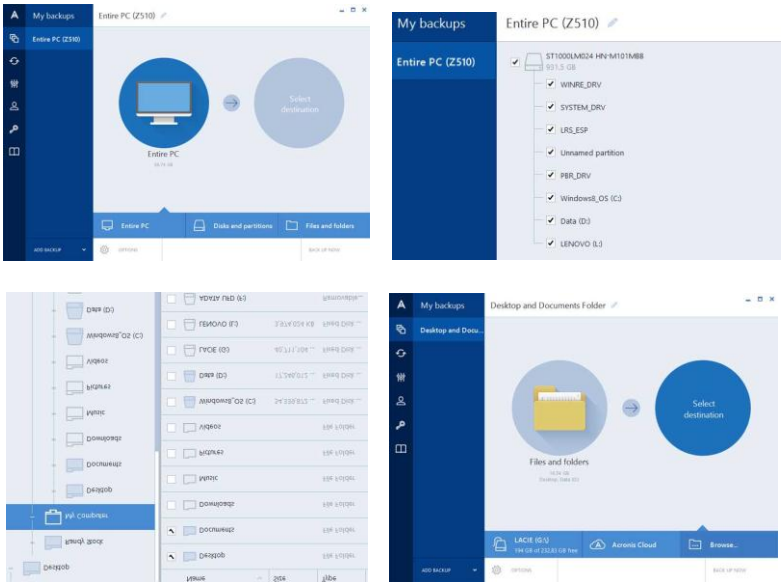


Foto descargada de http://www.whatsabyte.com/P1/ATI_2015_Review.html

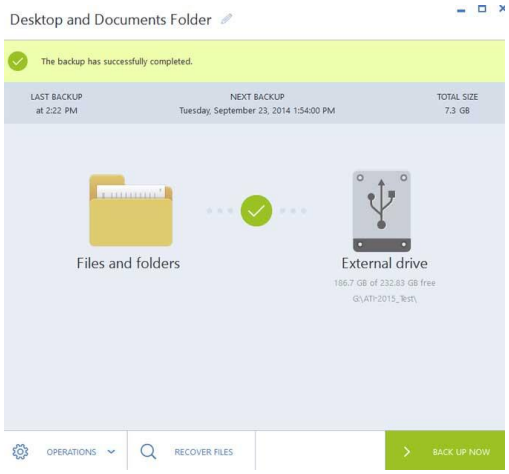


Foto descargada de http://www.whatsabyte.com/P1/ATI_2015_Review.html

Conclusiones: Herramienta de pago, de fácil uso e interfaz grafica, que permite la creación de imágenes de discos y archivos individuales. Al ser de pago, se dispone de un soporte y un mantenimiento, que no está disponible en las opciones Open Source.

El precio no es muy elevado, siendo una opción aceptable, ya que dispone de varias opciones extra, como el almacenamiento en la nube, pero con un sobrecoste ya que se necesita de una herramienta alternativa para acceder a las copias que se almacenen en la nube.

Digital Forensics Framework

Desarrollador: ArxSys

Página de la herramienta: http://www.digital-forensic.org/

Tipo de Instalación: Se puede instalar con un instalador o utilizar como paquete ejecutable portable, en Windows y en Linux, y también como USB Live Flash Drive.

Tipo de Herramienta: Es un framework con varias opciones de uso para el análisis forense. Es Open Source, con licencia GPL.

Uso: Se puede utilizar como disco de arranque, desde un USB o instalado en un equipo.

Descripción: Es una herramienta de investigación forense digital y una plataforma de desarrollo que permite recoger, conservar y revelar la evidencia digita. Es muy popular, es open source, con licencia GPL. Construido bajo una API dedicada, lo pueden utilizar profesionales o novatos sin dificultad, de forma fácil y rápida para recoger, preservar y revelar evidencias digitales sin comprometer los sistemas y datos.

Preserva la cadena digital de custodia con su software de escritura bloqueante y el cálculo del código Hash de los datos recogidos. Se puede acceder a los dispositivos, tanto locales como remotos y puede leer diferentes formatos de archivos estándar forenses digitales como, Raw, Encase EWF, AFF, etc.

Se pueden reconstruir las copias en máquinas compatibles VMware (VMDK). Está disponible tanto en Windows como en Linux. Se guardan metadatos para una rápida búsqueda de contenido, se utilizan expresiones regulares, diccionarios, etiquetas, etc.

Permite la búsqueda de archivos eliminados o escondidos, carpetas, espacios no asignados. Memoria forense volátil, para procesos, archivos locales, extracción binaria y conexiones de red.

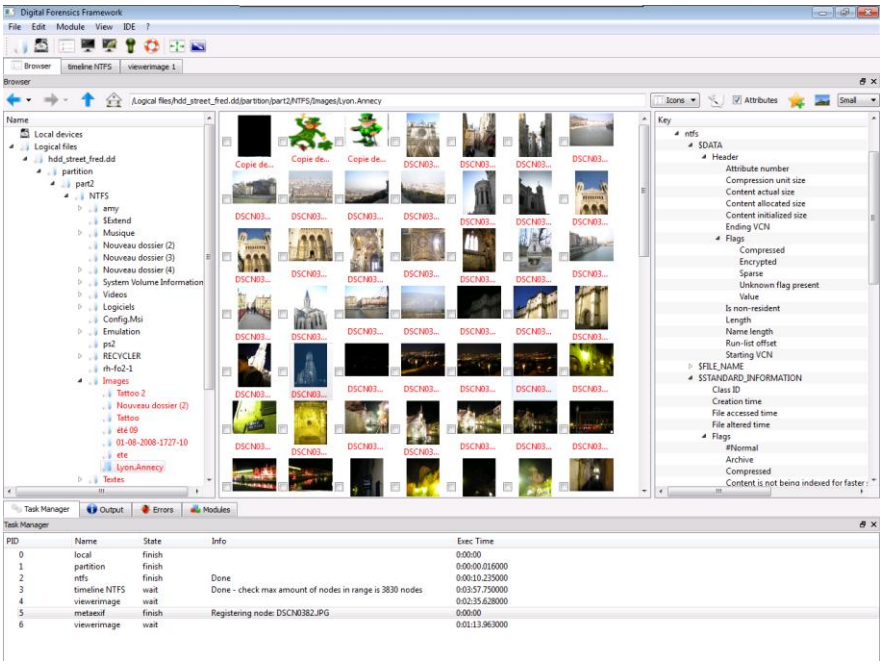


Foto descargada de http://www.100security.com.br/dff-digital-forensics-framework/

Cuando ejecutas DFF, primero necesita cargar un archivo de prueba (es decir, una imagen forense ha adquirido previamente) o abrir un dispositivo listo para su análisis. Entonces puede procesar el archivo de evidencia o dispositivo contra uno de los módulos integrados para comenzar a analizar los datos.

Conclusiones: Framewok de código abierto y licencia GPL, con bastantes opciones de uso. Facilidad de aprendizaje y rapidez de uso debido a su simplicidad.

Respeta la cadena de custodia con una de sus opciones y además añade metadatos a la información, para una mejor claridad en el almacenaje de la información. Permite la reconstrucción de las copias en máquinas virtuales.

X-Ways Forensics

Desarrollador: X-Ways Software Technology AG

Página de la herramienta: http://www.x-ways.net/forensics/index-m.html

Tipo de Instalación: Instalable en el sistema operativo.

Tipo de Herramienta: Es una plataforma avanzada para el análisis forense.

Uso: Herramienta instalable bajo un SO, desde el que se ejecuta la aplicación, para realizar el análisis forense de el/los equipos.

Descripción: X- Ways Forense es una plataforma avanzada para los analistas forenses digitales.

A pesar de no consumir muchos recursos, trabaja de forma eficaz. Las funcionalidades principales de la plataforma se enumeran en la siguiente lista:

.- Toma de imágenes de disco y clonación.

.- Capacidad de leer las estructuras del sistema de archivos dentro de varios archivos de imagenes.

.- Es compatible con la mayoría de los sistemas de archivos incluyendo FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS / ISO9660 / Joliet, UDF.....

.- Detección automática de la partición del disco duro borrado o perdido.

.- Diversas técnicas de recuperación de datos, siendo un proceso usado en computación forense para extraer datos desde un disco u otro dispositivo de almacenamiento sin la asistencia del sistema de ficheros que originalmente creo el fichero.

.-Bulk hash calculation.

.- Visualización y edición de estructuras de datos binarios utilizando plantillas.

.- Fácil detección y acceso a/de NTFS ADS.

.- Buen mantenimiento del fichero de cabezera.

.- Registro automatizado de la actividad.

.- Autenticidad de datos.

.- Gestión completa del caso.

.- Análisis de la memoria y de la RAM.

.- Vision de la galería de fotos.

.- Visor interno para el archivo de registro de Windows.

.- Informe Automatizado de Registro.

.- Extractos metadatos de varios tipos de archivos.

.- Capacidad para extraer correos electrónicos de varios clientes desde los emails disponibles

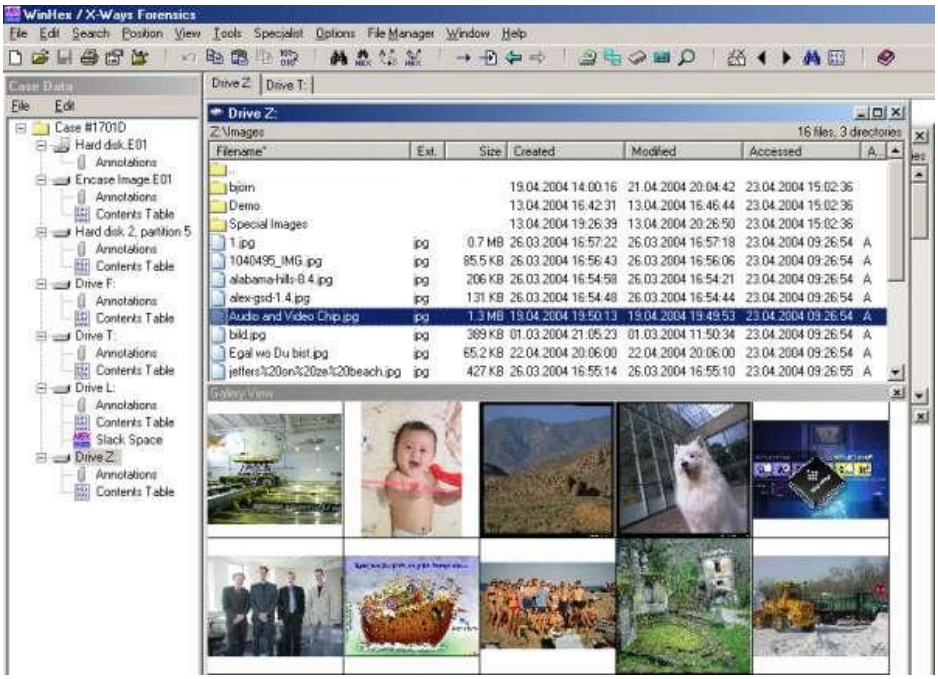


Foto descargada de http://www.hdlab.pl/xways/forensics.php

Conclusiones: Herramienta instalable con numerosas opciones para el análisis forense digital. Acil de utilizar, gracias a su interfaz grafica, a treves de la que podemos seleccionar sus innumerables opciones de análisis.

Es una herramienta ligera y rápida, por lo que se puede usar en casi todos los sistemas, ya que consume pocos recursos.

CloneZilla Live CD

Desarrollador: Steven Shaiu y desarrollado por el NCHC Labs

Página de la herramienta: http://clonezilla.org/clonezilla-live.php

Tipo de Instalación: LiveCD, El software se puede ejecutar ya sea desde un arranque de unidad flash USB o CD/DVD.

Tipo de Herramienta: Clone de Discos.

Uso: Se crea un CD de arranque, de Linux, donde se instala la herramienta.

Descripción: Es una herramienta de clonación y creación de copias de seguridad de discos y de archivos. Como cualquier otro LiveCD, es capaz de arrancar un gran número de configuraciones y de reconocer muchos periféricos.

Foto descargada de http://lukas238.deviantart.com/art/CloneZilla-CD-cover-98786728

Se pueden hacer imágenes ISO y guardarlas en particiones de disco o CD de arranque. Es compatible con casi todos los formatos de archivos de sistema, hace copias de los bloques de disco, que mejoran la velocidad y el rendimiento de la clonación. Para los administradores de red, el modo de multidifusión puede ser muy útil para respaldar y restaurar un conjunto de equipos.

Permite clonar una maquina individual, partición o disco para ser reproducido en otro medio. La clonación puede ser guardada como un archivo de imagen o como una copia exacta de datos. Los datos pueden ser guardados localmente, en un servidor SSH, servidor Samba o un recurso compartido de archivo NFS y luego restaurarlos en una fecha posterior.

También existe Clonezilla Server que se utiliza para clonar simultáneamente muchos computadores a través de red. Esto se hace usando un servidor DRBL y estaciones de trabajo que puedenarrancar desde una red.

Conclusiones: Es una utilidad Open Source, por lo que se puede utilizar de forma gratuita, además permite la clonación de discos, particiones o archivos, por lo que puede ser una opción interesante.

Caine

Desarrollador: Computer Aided InvestigateEnviroment

Página de la herramienta: http://www.caine-live.net/

Tipo de Instalación: Live CD

Tipo de Herramienta: Herramienta para la investigación y el análisis de datos y dispositivos para el análisis forense.

Uso: Es un LiveCD, por lo que se arraca la máquina desde el LiveCD, y es desde este entorno desde el que se hace uso de la herramienta.

Descripción: CAINE es una distro de GNU/Linux Italiana, utilizada en informática forense. Esta herramienta es open source.

CAINE ofrece un entorno forense completo que se organizó para integrar herramientas de software existentes, módulos de software y proporcionar una amigable interfaz gráfica.

Foto descargada de http://www.caine-live.net/

Los principales objetivos del diseño que CAINE garantiza son:

.- un entorno interoperable que apoya al investigador digital durante las cuatro fases de la investigación digital.

.- una interfaz gráfica fácil de usar.

.- herramientas de fácil uso.

CAINE contiene una gran cantidad de herramientas forenses digitales. Incluye un GUI fácil de usar, creación de informes semiautomáticos y herramientas para la investigación móvil forense, análisis forense de red, recuperación de datos y mucho más.

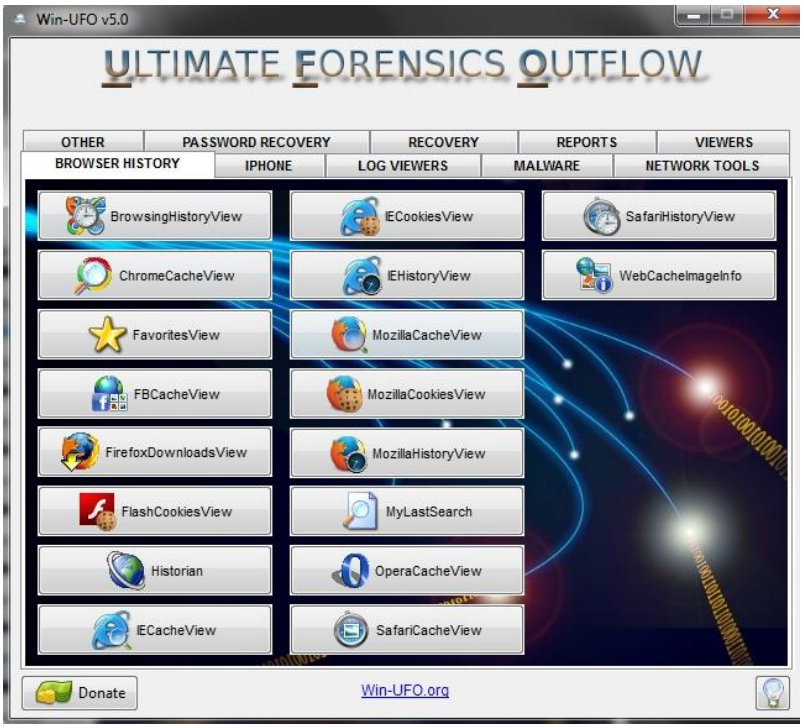


Foto descargada de http://www.caine-live.net/

Cuando arranque el entorno Linux de CAINE, puede lanzar las herramientas forenses digitales desde la interfaz CAINE (directo en el escritorio) o de acceso directo de cada herramienta en la carpeta 'Herramientas forenses' en el menú de aplicaciones.

Foto descargada de http://www.caine-live.net/

Existe una versión para Windows (Wintaylor), con las mismas características que la versión de Linux, también es Open Source.

Conclusiones: Es una herramienta LiveCD, con opciones interesantes para el análisis forense digital, con una interfaz de usuario intuitiva y fácil de usar. Se pueden añadir módulos para ampliar las opciones disponibles de serie.

Gracias a su facilidad de uso y su posibilidad de ampliación, utilizando herramientas existentes, es una buena elección para el análisis forense.

Open Computer Forensics Architecture

Desarrollador: Agencia de Policía Nacional de Holanda

Página de la herramienta: http://ocfa.sourceforge.net/

Tipo de Instalación: LiveCD, con Linux como sistema operativo.

Tipo de Herramienta: Herramienta de uso general, para la automatización de los procesos de análisis forense digital.

Uso: Es un LiveCD, por lo que se debe instalar en un dispositivo autoarrancable, como CD, USB, Disco duro, etc., para poder utilizarla. Es fácil de utilizar y está preparada para automatizar los procesos relacionados con el análisis forense.

Descripción: Open Computer Forensics Architecture (OCFA) es un framework de código abierto, el objetivo principal es la automatización de procesos de análisis forense digital para acelerar la investigación y dar a los investigadoresón y dar a los investigadorestácticos acceso directo a los datos incautados a través de un método que facilite la búsqueda y navegación por la interfaz.

Foto descargada de http://sourceforge.net/projects/deft-linux/

Está disponible para su descarga bajo licencia GPL. El framework fue construido por la Agencia de Policía Nacional de Holanda (KLPD). Este sistema fue construido en la plataforma Linux, y utiliza la base de datos PostgreSQL para almacenar datos, por lo que se requiere de conocimientos avanzados de Linux y de SQL para las consultas a la base de datos.

Conclusiones: Es una herramienta de uso general en el análisis forense. Al ser una herramienta creada por una agencia de la policía, tiene las funciones básicas para realizar los procesos necesarios para el análisis forense, y ademas, cumpliendo las funciones basicas.

Al ser LiveCD se puede utilizar con cualquier tipo de dispositivo y Sistema Operativo. Es versatile y de facil uso, pero es necesario tener conocimientos de administración de Linux y de SQL por que son la base del Sistema.

SANS Investigate Forensics Toolkit Workstation

Desarrollador: SANS Digital Forensics & Incident Response

Página de la herramienta: http://digital-forensics.sans.org/

Tipo de Instalación: LiveCD

Tipo de Herramienta: LiveCD

Uso: Es un LiveCD con multiples herramientas de gran calidad, que se puede utilizer para casi cualquier ámbito de análisis forense.

Descripción: SANS Investigate Forensics Toolkit Workstation es un Kit de herramientas para el análisis forense digital. Un equipo internacional de expertos forenses, liderado por SANS Faculty Fellow Rob Lee, creó los SANS Investigative Forensic Toolkit (SIFT) Workstation y lo puso a disposición de toda la comunidad como un servicio público. El kit de herramientas SIFT libre, que puede adaptarse a cualquier suite de herramientas forense modernas, también está incluido SANS' Advanced Computer Forensic Analysis y en el curso de respuestas a incidentes.

Esto demuestra que el código libre ayuda a las investigaciones avanzadas y a responder a las intrusiones. Esto se puede lograr utilizando herramientas de código abierto de vanguardia que son de libre acceso y se actualizan con frecuencia.

Según la página oficial, "Incluso si SIFT fuera a costar decenas de miles de dólares, todavía sería un producto muy competitivo", dice Alan Paller, director de investigación de SANS. "Sin costo, no hay ninguna razón para que no debería formar parte de la cartera en cada organización que tiene analistas forenses expertos."

Desarrollado y continuamente actualizado por un equipo internacional de expertos forenses, SIFT es un grupo de herramientas gratuitas forenses de código abierto diseñado para realizar exámenes forenses digitales detallados en una variedad de entornos. Con más de 100.000 descargas hasta la fecha, SIFT sigue siendo la Lherramienta más popular de código abierto que se ofrece para el análisis forense junto a soluciones de código comercial.

Foto descargada de http://digital-forensics.sans.org/community/downloads

Las nuevas características clave de SIFT 3 incluyen:

- Ubuntu LTS 14,04 Base
- Sistema de base de 64 bits
- Mejor utilización de la memoria
- Actualizar y personalizaciones paquete Auto-DFIR
- Las últimas herramientas y técnicas forenses
- VMware Appliance listo para hacer frente a la medicina forense
- Compatibilidad entre entre Linux y Windows
- Opción para instalar independiente a través de (.iso) o utilizar a través de VMware Player / Estación de trabajo
- Proyecto de Documentación en línea en http://sift.readthedocs.org/
- Soporte del sistema de archivos Ampliado

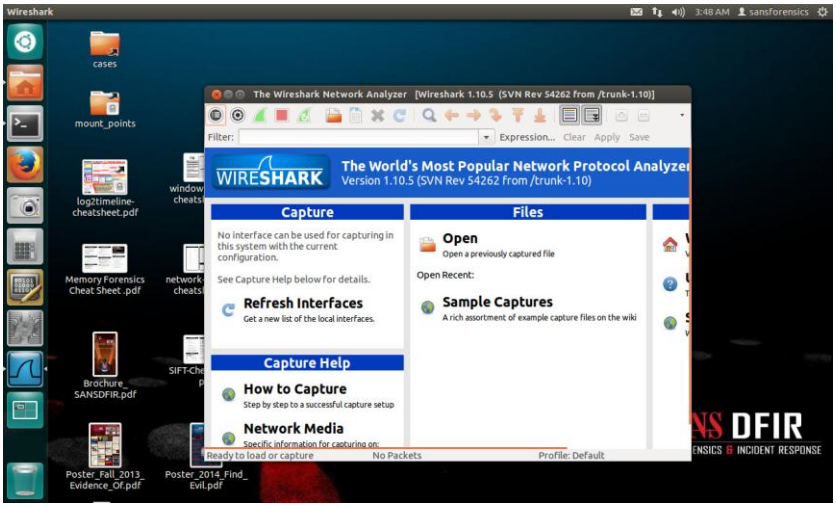


Foto descargada de http://digital-forensics.sans.org/community/downloads

Es una herramienta de análisis forense multiuso, ya que en un mismo sistema operativo vienen incorporadas las herramientas necesarias para el proceso de análisis forense digital.

Se basa en Ubuntu, sobre la que se han montado todas las herramientas para el análisis forense digital. Tiene una versión gratuita y otra de pago, con las diferencias correspondientes al desembolso otra de pago, con las diferencias correspondientes. El contenido del pack contiene herramientas open source, soporta análisis Expert Witness Format (E01), Advanced Forensi, Advanced Forensics Format (AFF), y RAW (dd) como formatos de evidencias. SIFT incluye herramientas tales como log2timeline, eestá diseñada como un marco para la creación de la línea de tiempo de artefactos y análisis, Scalpel, es una herramienta open source para recuperación de datos borrados, originalmente basado en Foremost, aunque significativamente más eficiente, Rifiuti, una herramienta para la recuperación de archivos enviados a la papelera de reciclaje y eliminados, y muchas herramientas más.

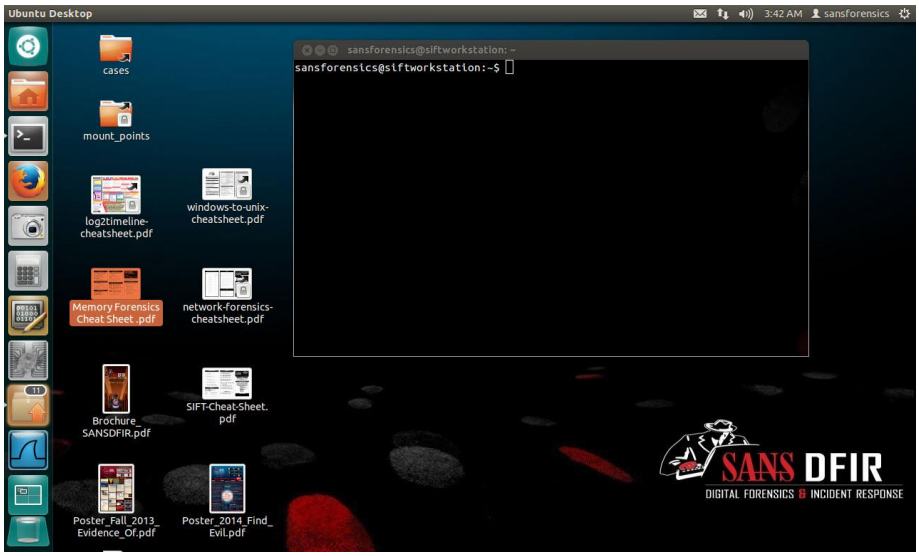


Foto descargada de http://digital-forensics.sans.org/community/downloads

Conclusiones: Es un LiveCD, con dos versions, una de pago y otra gratuita. Aun siendo la de pago más completa, la version de pago incluye suficientes opciones para convertirse en una opción interesante para el análisis forense digital.

Las herramientas incluidas en el LiveCD de forma individual ya son muy valiosas en el análisis forense digital. Cada una dentro de su entorno, podría situarse entre las mejores, por lo que de manera ía situarse entre las mejores, por lo que de manera conjunta forman un pack muy a tener en cuenta para realizar las funciones de peritaje informático, ya que en un mismo Sistema se incorporan las herramientas necesarias para cumplir con su objetivo.

EnCase

Desarrollador: Guidance Software

Página de la herramienta:
https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Search.aspx

Tipo de Instalación: Instalable

Tipo de Herramienta: Suite para el análisis forense digital.

Uso: Herramienta instalable de gran calidad, de las punteras en el mercado. Posee gran cantidad de opciones, con una interfaz de usuario intuitiva y de fácil uso, teniendo un aspecto muy similar a las páginas web, lo que facilita su uso y aprendizaje.

Descripción: EnCase Forensics es el estándar mundial en la tecnolgía de investigación digital para profesionales forenses que necesitan para llevar a cabo la recogida eficaz de datos forenses e investigaciones usando un proceso repetible y defendible.

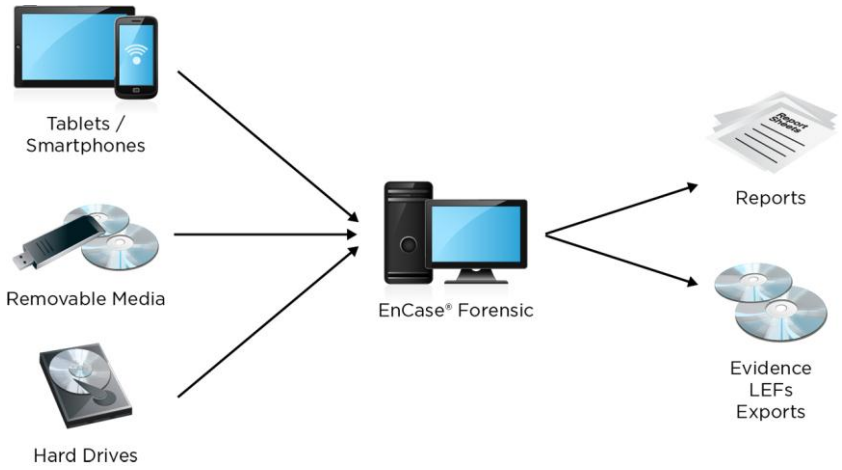


Foto descargada de https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx

Los principales objetivos que persigue Guidance Software en su herramienta de análisis forense son:

- Adquisición rápida de datos de cualquier tipo de dispositivos.
- Descubrir posibles pruebas con el análisis forense a nivel de disco.
- Producir informes detallados de los análisis.
- Mantener la integridad de las pruebas de forma fiable para una possible utilización en algún juicio.

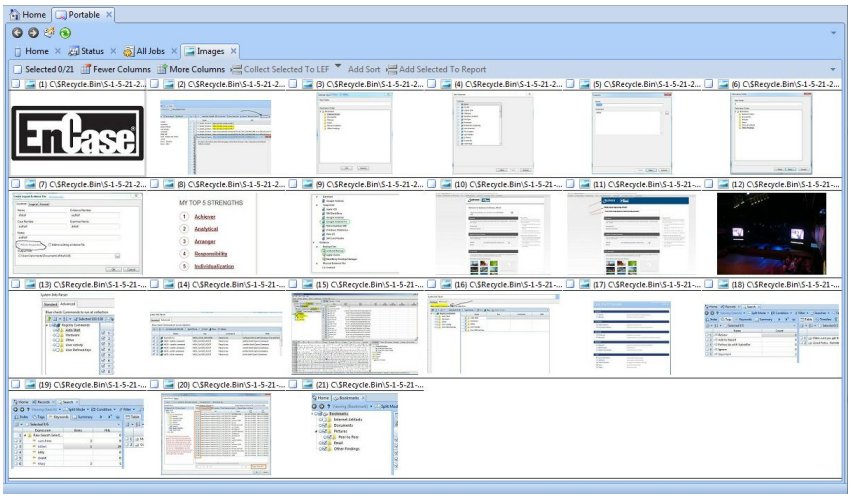


Foto descargada de https://www.guidancesoftware.com/products/Pages/encase-forensic/triage.aspx

Con el estándar de EnCase se gana en velocidad y en poder en el análisis forense digital pero además de estas grandes ventajas dispone de:

- Adquiere y analiza deatos rápidamente de casi cualquier ordenador, teléfonos inteligentes y tabletas de cualquier solución de software de análisis forense digital.
- Aumenta la confianza en los resultados adquiridos con EnCase gracias a que utiliza la probado estándar de corte-referenciado del análisis digital forense.
- Descubre las pruebas potenciales más rápido usando las capacidades de búsqueda avanzada.
- Aumenta la productividad mediante la vista previa de los resultados a medida que se adquieren los datos. Una vez creados los archivos de imagen, se puede buscar y analizar varias unidades o medios de comunicación de forma simultánea.
- Mejorar la eficiencia mediante la automatización de tareas comunes de investigación con EnScript, la solución scripting de en EnCase Forensic.
- Preservar la integridad de las evidencias.

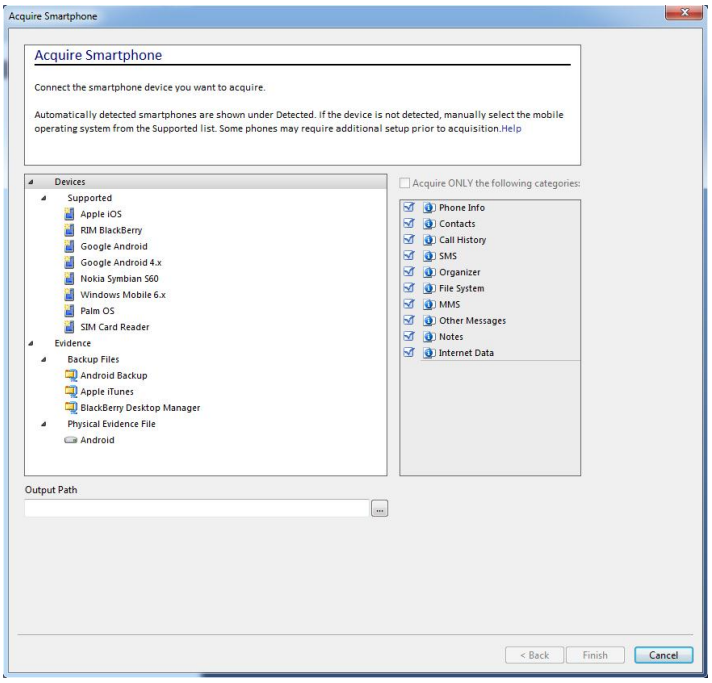


Foto descargada de https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Collect.aspx

La herramienta tiene una interfaz de usuario intuitiva, con una GUI parecida a la de un navegador Web. También permite compartir los resultados con el resto de la gente involucrada en el caso, para facilitar y agilizar los trámites.

Permite la revision simple de e-mails, entendiendo el contexto de correo electrónico basado en la evidencia potencial en el hilo de la conversación y el contexto relacionado.

El nuevo motor de indexación del procesador de pruebas, rediseñado, permite consultas más potentes y un procesamiento más rápido, además de la capacidad de automatizar tareas, crear plantillas basadas en perfiles de casos, y de fácil integración con los resultados forenses.

Amplio tipo de archivo y de sistemas operativoss (OS) soportados por EnCase Forensic. En la versión 7, también están integradas EnCase Decryption Suite, EnCase Physical Disk Emulator, EnCase Virtual File System, and EnCase FastBloc SE.

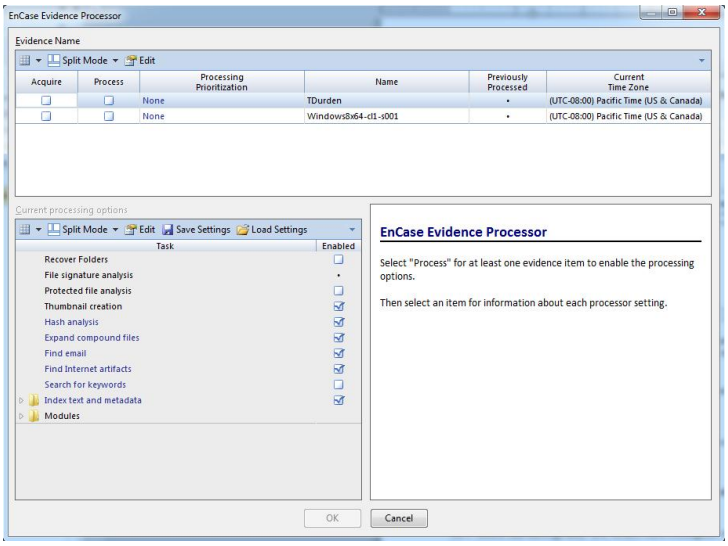


Foto descargada de https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Process.aspx

Se pueden adquirir datos desde el disco o la memoria RAM, documentos, imágenes, correo electrónico, correo web, artefactos de Internet, historial web y la memoria caché, la reconstrucción páginas HTML, sesiones, archivos comprimidos, archivos de copia de seguridad, los archivos cifrados, estaciones de trabajo, servidores, RAID y chat, y además con la versión 7 de smartphones y tabletas.

Visualización de los resultados mientras los datos están siendo adquiridos. Una vez creados los archivos de imagen, se pueden buscar y analizar varias unidades o medios de comunicación de forma simultánea.

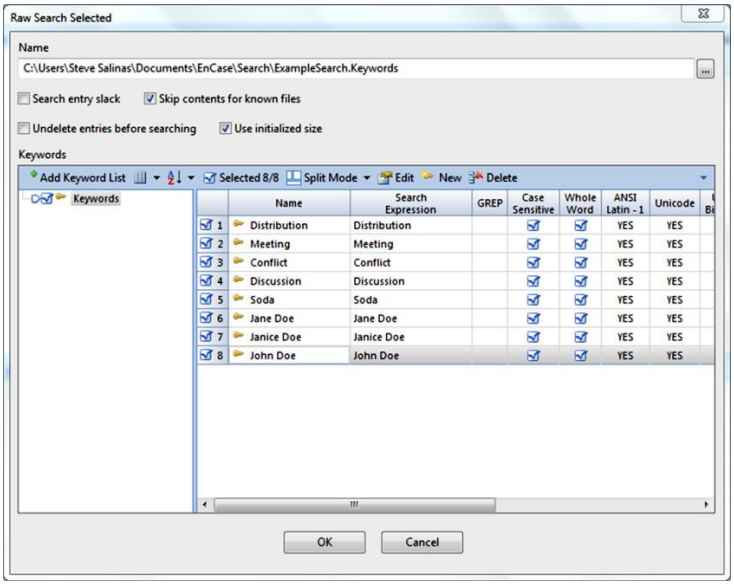


Foto descargada de https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Search.aspx

Conclusiones: Es una herramienta de pago, con una version libre, con menos opciones, de las más conocidas en el sector, con gran cantidad, y de gan calidad, de opciones para el análisis álisis forense digital.

Al ser una herramienta de pago, tiene el respaldo de una empresa con gran experiencia y que ofrece una gran cantidad de extras a la herramienta, desde cursos de aprendizaje, hasta certificaciones de uso.

Registry Recon

Desarrollador: Arsenal Recon

Página de la herramienta: http://www.arsenalrecon.com/apps/recon/

Tipo de Instalación: Instalable en Windows.

Tipo de Herramienta: Herramienta para analizar y recuperar información del Registro de Windows.

Uso: dispone de una interfaz gráfica para realizar el análisis y recuperación del registro de Windows, con sus opciones e informes se puede realizar un exaustivo anáisis del registro de Windows, pudiendo ver, en una línea de tiempo, los cambios que han sucedido durante ese periodo.

Descripción: El análisis forense del Registro durante mucho tiempo ha sido relegado al análisis de sólo lectura del Registro de Windows, de manera que consume tiempo innecesario y trabaja de forma arcaica.

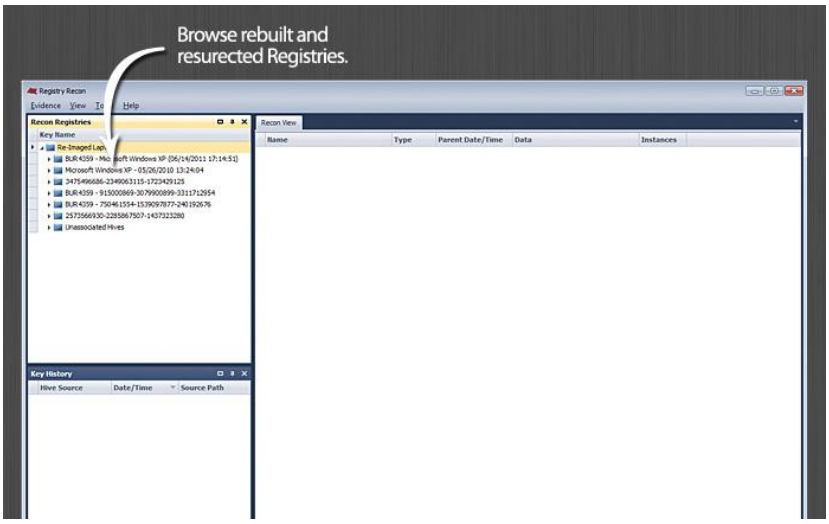


Foto descargada de https://www.arsenalrecon.com/apps/recon/

Registry Recon no es un analizador del registro, se han desarrollado potentes métodos nuevos para analizar los datos del Registro, en lugar de depender de las API de Microsoft, por lo que los registros que han existido en un sistema Windows con el tiempo pueden ser recuperados.

Registry Recon proporciona acceso a un enorme volumen de datos del registro que se ha eliminado de manera efectiva, ya sea que la supresión se produjo debido a la actividad del sistema de forma de forma benigna, prevaricación de un usuario, o incluso re-proyección de imagen por parte del personal de TI.

Sus líneas de tiempo pueden ahora incluir los datos del registro que estaba activo, una copia de seguridad en puntos o instantáneas de volumen de restauración o trozos de espacio no asignado. Registry Recon

Mientras Registry Recon muestra los datos del registro de forma única y predeterminada, un acceso transparente a todas las instancias de claves particulares y los valores del registro que están disponibles(con rutas completas y los offsets del sector) por lo que sus hallazgos pueden ser autenticados de manera eficiente.

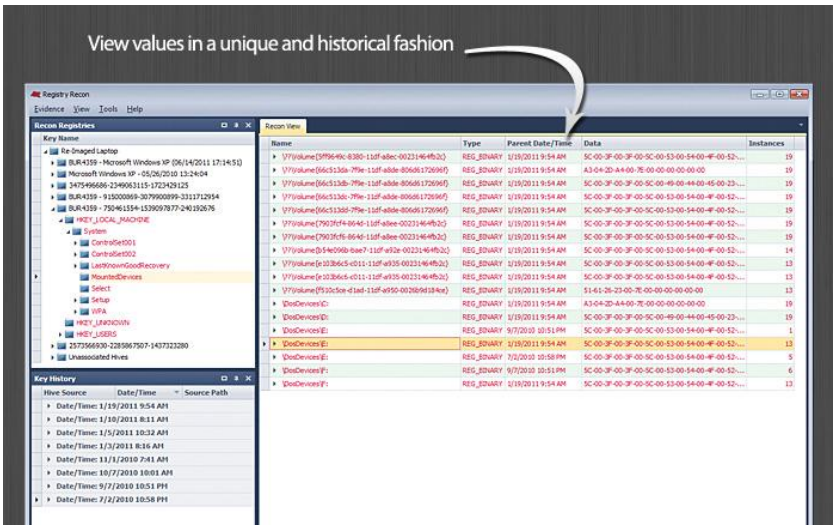


Foto descargada de https://www.arsenalrecon.com/apps/recon/

Las características más importantes de la herramienta son:

- Flujo de trabajo intuitivo y eficiente
- Recuperación de Registros de Windows desde hace mucho tiempo olvidado
- El acceso a enormes cantidades de datos del registro borrado
- Claves únicas y valores que se muestran de forma predeterminada
- Acceso transparente a todas las instancias de claves y valores
- Ventanas para restaurar puntos y volumenes de copias instantaneas
- Capacidad para ver las claves (y sus valores) en puntos determinados en el tiempo

Además de todas estas opciones, en la nueva versión se disponen de las siguientes mejoras:

- "Decodificación automática" de las claves UserAssist
- Integración de la última Arsenal Image Mounter
- Mejor manejo de los valores LastWrite inusuales
- Mejoras en el rendimiento

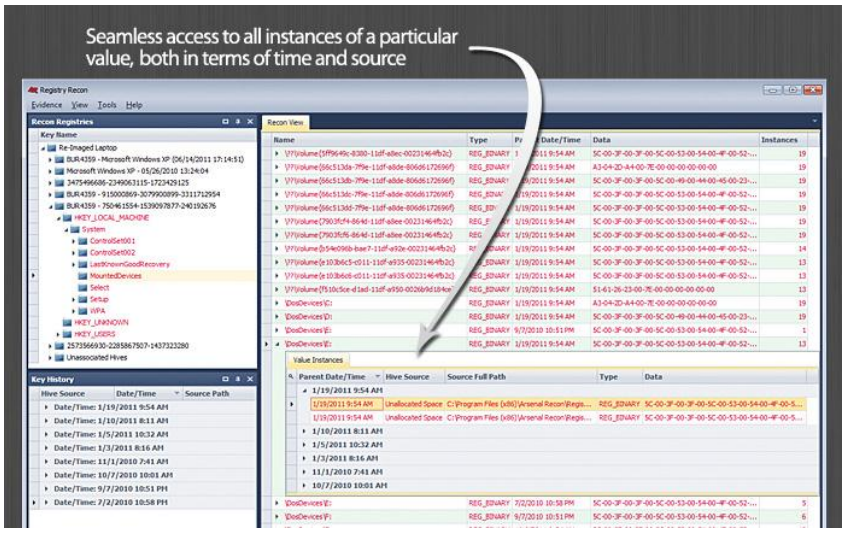


Foto descargada de https://www.arsenalrecon.com/apps/recon/

Registry Recon es una herramienta forense que permite a los usuarios ver cómo los Registros de las instalaciones actuales y anteriores de Microsoft Windows han cambiado con el tiempo.

Fue desarrollado por Arsenal Recon, cuyo lema es "Computer forensics tools by computer forensics experts".

Registry Recon extrae primero la información del registro de una pieza de evidencia (imagen de disco, disco esclavo montado correctamente, etc.), ya que la información estaba activa, apoyado en puntos o restaurar Volumenes o eliminados. Registry Recon luego reconstruye todos los Registros representados por la información extraída. Recon Registro fue la primera (y es actualmente la única) herramienta forense digital para reconstruir los Registros de las instalaciones activas y anteriores de Windows.

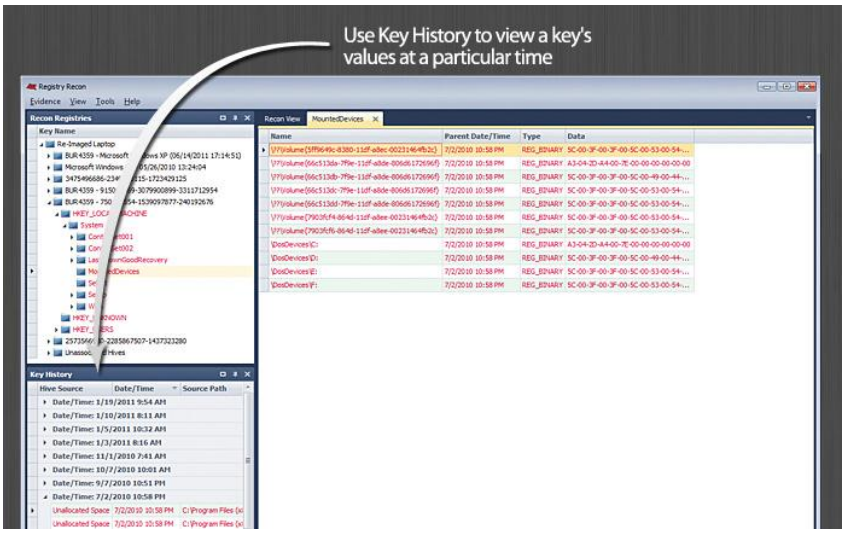


Foto descargada de https://www.arsenalrecon.com/apps/recon/

La herramienta extrae del registro de Windows que se utiliza para reconstruir la línea del tiempo del Registro de un equipo del que se quiere tener una evidencia. La reconstrucción del Registro se visualiza de una manera que permite al usuario ver los valores únicos de forma predeterminada y todas las instancias de esos valores si así se desea. Se dispone de un historial de claves, a traves del cual, se puede visualizer las claves y susu valores en puntos de terminados en el tiempo. Restaura los puntos y las instantáneas del volumen analizado durante la ingestión pruebas.

La herramienta dispone de informes preintegrados, que siguen el formato solicitado por la comunidad informática forense.

Conclusiones: Herramienta de pago para el análisis y recuperación del Registro de Windows, con bastantes caracteristicas. Es una herramienta muy uti para ver las diferencias de registro de Windows durante un espacio de tiempo, disponiendo de manera rápida y facil de los datos del registro de Windows, de manera visual y a traves de informes, aceptados por la comunidad informática forense.

The Sleuth Kit

Desarrollador: **sleuthkit.org**

Página de la herramienta: http://www.sleuthkit.org/sleuthkit/desc.php

Tipo de Instalación: Instalable en Windows y consola de comandos en Linux.

Tipo de Herramienta: Analizador y recuperador de información.

Uso: Se instala en un ordenador y se analizan los dispositivos que se deseen, ya sean discos duros o dispositivos móviles.

Descripción: El Sleuth Kit es una herramienta basada en Windows y Unix, la cual asiste en el análisis forense de las computadoras. Viene con varias herramientas que

favorecen al análisis forense digital, como ayudar en el análisis de imágenes de disco, realizar un análisis en profundidad de los sistemas de archivos, y varias cosas más.

Foto descargada de http://www.toolwar.com/2014/01/the-sleuth-kit-tsk-forensics-framework.html

El Sleuth Kit es open source, con un kit de herramientas que se puede utilizar para realizar un análisis en profundidad de los diversos sistemas de archivos. Autopsy es la interfaz gráfica de usuario de Sleuth Kit. Viene con funciones, tales como:

- Análisis en la línea de tiempo.
- Funcion de filtrado.
- Analisis del Sistema de archivos.
- Busqueda de palabras clave en los archivos.

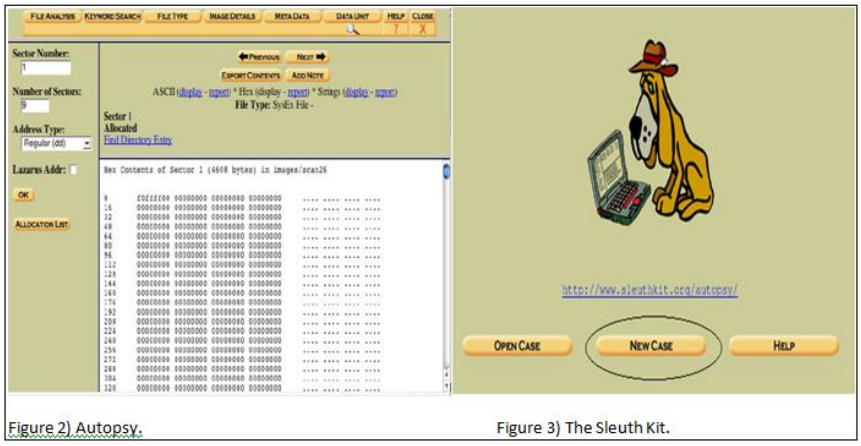


Figure 2) Autopsy. Figure 3) The Sleuth Kit.

Foto descargada de http://blog.hackersonlineclub.com/2013/11/forensic-memory-analysis-and-techniques.html

Con la posibilidad de añadir otros módulos para prolonger y extender sus caracteristicas.

Se puede utilizar Sleuth Kit en una máquina Linux, y Autopsy en máquina Windows.

La versión de Windows, Autopsy, posee una interfaz gráfica, a través de la cual, se realizan las opciones de que dispone Sleuth Kit, como pueden ser el análisis de dsipositivos, de manera manual o automática. Permite examinar un disco duro o dispositivo móvil y recuperar las evidencias del dispositivo.

Al iniciar la aplicación, se puede optar por crear un nuevo caso o cargar uno ya existente. Si se decide crear un nuevo caso, se tendrá que cargar una imagen forense o un disco local para iniciar su análisis.

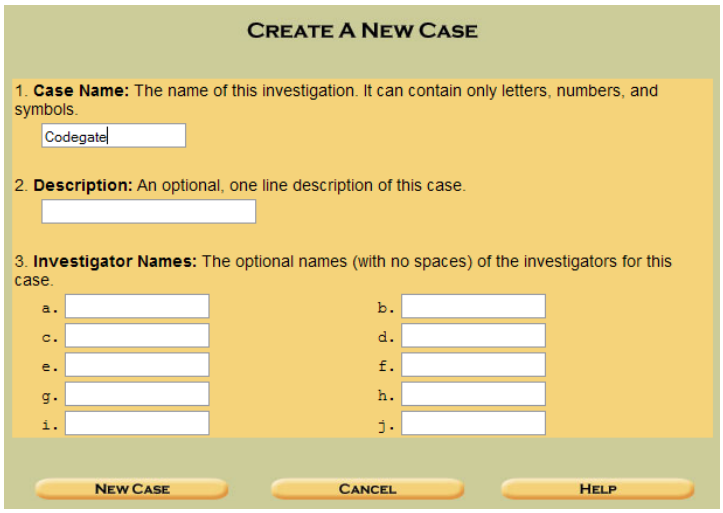


Foto descargada de http://blog.stalkr.net/2010/03/codegate-forensic-sleuthkit-autopsy.html

Las fuentes de datos se agregan a un **caso**. Un caso puede tener una única fuente de datos o puede tener múltiples fuentes de datos. En la actualidad, se genera un único informe de un caso entero, así que si se necesita hacer informes sobre las fuentes de datos individuales, entonces se debe utilizar una fuente de datos por caso. Si hay muchas fuentes, móviles o discos duros para una investigación, entonces su caso debe tener múltiples fuentes de datos.

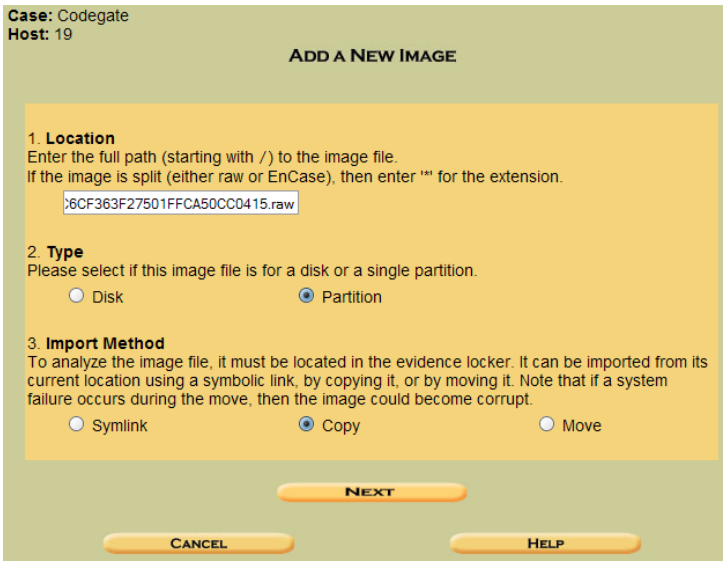


Foto descargada de http://blog.stalkr.net/2010/03/codegate-forensic-sleuthkit-autopsy.html

Los módulos de ingesta de datos analizan archivos en un orden de prioridades para que los archivos en el directorio de un usuario se analizen antes que los archivos de otras carpetas. Los módulos de ingesta pueden ser desarrolladas por terceros. Los módulos de ingesta estándar incluidos en Autopsy son:

- Módulo de actividad reciente.

- Módulo de busqueda de bases de datos hash.
- Módulo de identificación de tipo de archivo.
- Módulo de extracción de archivos integrada.
- Módulo analizador EXIF.
- Módulo de busqueda de palabras clave.
- Módulo Email Parser.
- Módulo detector de extensions perdidas.
- Módulo verificador E01.
- Módulo analizador de Android.
- Módulo identificador de ficheros interesantes.
- Módulo Carver PhotoRecódulo Carver PhotoRec

Foto descargada de http://blog.stalkr.net/2010/03/codegate-forensic-sleuthkit-autopsy.html

Se puede generar un informe final que incluirá todos los resultados de los análisis. Se va a crear un informe HTML o XLS en la carpeta Informes de la carpeta del caso. También hay una opción para exportar archivos de informe en una carpeta independiente fuera de la carpeta caso.

Conclusiones: Herramienta con una interfaz muy amigable, en su version de Windows, desde la que se pueden hacer análisis de dispositivos, tanto discos duros como móviles, rapidamente y con opciones muy interesantes. Ispone de unos infomes bastante completos. Además, se puede ampliar con módulos de terceros, por lo que le da un extra a la herramienta, ya que se puede modelar a gusto del usuario.

Volatility

Desarrollador: The Volatility Foundation

Página de la herramienta: http://www.volatilityfoundation.org/

Tipo de Instalación: Volatility se empaqueta en varios formatos, incluyendo el código fuente en archivo zip o tar (para todas las plataformas), un ejecutable PyInstaller (sólo Windows) y un ejecutable independiente (sólo Windows)

Tipo de Herramienta: Framework

Uso: Volatility es un framework para el desarrollo de análisis forenses digitales. Está desarrollado en Python y viene con varias herramientas para extraer información de los distintos tipos de pruebas. Se puede utulizar en Sistemas Windows, de 32 y 64 bits, Linux, Macs y dispositivos android.

Descripción: Volatility es un framework, open source, escrito en Python. Es un framework de análisis forense para la memoria de los dispositivos. Se utiliza en respuesta a incidentes y análisis de malware que permite extraer artefactos digitales desde volcados de memoria volatil (RAM).

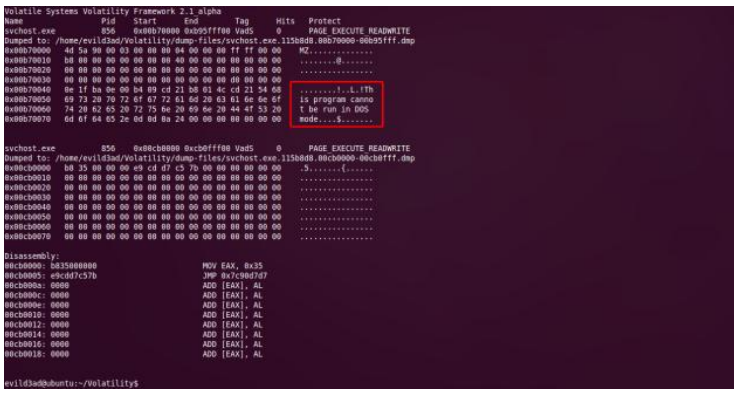


Foto descargada de http://computerforensicsblog.champlain.edu/2012/11/08/volatility-introduction/

Con esta herramienta, se puede extraer información de los procesos en ejecución, sockets de red abiertos, conexión de red, DLL cargadas de cada proceso y secciones del registro de cache, IDs de los procesos y más. También tiene soporte para extraer información de los archivos de volcado de caída de Windows y archivos de hibernación.

Volatility es compatible con volcados de memoria de todas las versiones de Windows de 32 y 64 bits y paquetes de servicios incluyendo XP, 2003 Server, Vista, Server 2008, Server 2008 R2, Siete, 8, 8.1, Server 2012 y 2012 R2. Ya sea que su volcado de memoria esté en formato RAW, un archivo de volcado Microsoft, archivo de hibernación, o una instantánea de la máquina virtual, Volatility es capaz de trabajar con él.

Ahora también es compatible con los volcados de memoria Linux formato RAW o LiMEX e incluimos más de 35 plugins para el análisis de núcleos de Linux de 32 y 64 bits y distribuciones como Debian, Ubuntu, openSUSE, Fedora, CentOS, y Mandrake. También es compatible con 38 versiones de volcados de memoria Mac OSX desde 10,5 a 10.9.4 Mavericks, de 32 y 64 bits. Teléfonos Android con procesadores ARM también son soportados por Volatility.

Esta herramienta está disponible de forma gratuita la bajo licencia GPL.

El diseño modular de Volatility le permite soportar fácilmente nuevos sistemas operativos y arquitecturas que aún no existen.Todos los dispositivos son blancos de posiblesataques o desgracias y gracias a la modularidad de Volatility se puede adaptar a cualquier sistema operativo.

Al estar escrito en Python, un lenguaje de ingeniería inversay forense, establecido, con un montón de librerias que se pueden integrar fácilmente en Volatility.

La API extensible y de tipo script, le da el poder de ir más allá y seguir innovando. Por ejemplo, se puede utilizar Volatility para construir una interfaz web personalizadas o GUI, conducir su sandbox malware, realizar la introspección de una máquina virtual o simplemente explorar la memoria del núcleo de forma automatizada. Los analistas pueden añadir nuevos espacios de direcciones, plugins, estructuras de datos, y superposiciones para adaptar verdaderamente el framework a sus necesidades.

Posee un conjunto de características sin igual sobre la base de la ingeniería inversa y la investigación especializada. Volatility proporciona capacidades que el propio depurador de núcleo de Microsoft no permite, como historias talla de mando, entrada de la consola / buffers de salida, objetos de usuario (GUI de memoria), y estructuras de datos relacionados con la red.

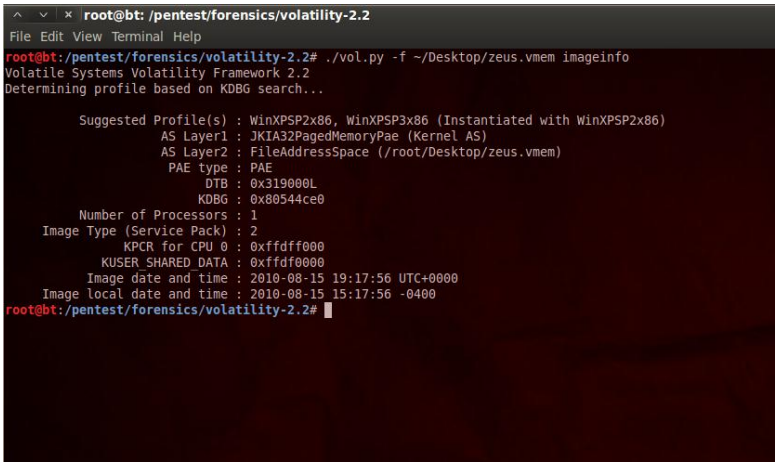


Foto descargada de http://www.senet-int.com/2013/02/volatility-memory-analysis-tool/

Cobertura completa de archivos de diverso formato, Volatility puede analizar vertederos primas, volcados, archivos de hibernación, archivos de VMware con extensión .vmem, archivos VMware salvó los de Estado y archivos (.vmss / .vmsn), núcleo VirtualBox vertederos, LiME (Linux Memoria Extractor), perito suspendido (EWF), y la memoria física directa sobre Firewire. Usted puede incluso convertir de ida y vuelta entre estos formatos. En el calor de tu momento de respuesta a incidentes, no quedar atrapados mirando como un tonto cuando alguien te da un formato de sus otras herramientas no puede analizar.

Algoritmos rápidos y eficientes permiten analizar RAM vertederos de grandes sistemas sin sobrecarga innecesaria o el consumo de memoria. Por ejemplo la volatilidad es capaz de enumerar los módulos del kernel de un sistema de 80 GB en tan sólo unos segundos. Siempre hay margen de mejora, y el tiempo varía según el comando, sin embargo otros marcos de análisis de memoria pueden tardar varias horas para hacer lo mismo en la memoria mucho más pequeños vertederos.

Forensics / IR / malware enfoque - La volatilidad fue diseñado por los forenses, respuesta a incidentes y expertos de malware para centrarse en los tipos de tareas estos analistas forman normalmente. Como resultado, hay cosas que a menudo son muy importantes para un análisis forense analistas que no son tan importantes para una persona depurar un controlador del núcleo (almacenamiento no asignado, artefactos indirectos, etc.).

A continuación se muesta un ejemplo del uso de Volatility para descubrir las direcciones de memoria donde se encuentra la SAM, Security, etcétera, se utiliza el plugin hivelist. La sintaxis es sencilla ***vol -f <fichero captura formato dmp> hivelist***.

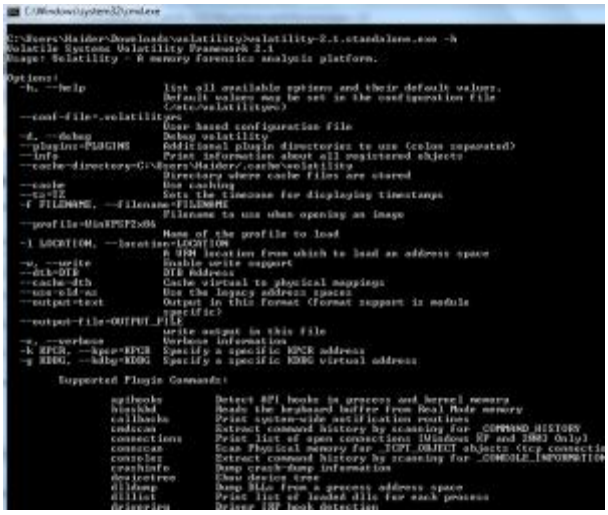


Foto descargada de http://blog.creativeitp.com/posts-and-articles/volatile-memory/introduction-to-the-volatility-framework/

Lo interesante de la ejecución anterior es la dirección virtual obtenida. Con ella podremos utilizar otros plugins para obtener otro tipo de información, por ejemplo en el caso de las LSA Secrets existe un plugin denominado lsadump con el que se puede obtener el contenido de dicho contenedor. Para ello, el plugin pide la dirección virtual de System y Security. La sintaxis es sencilla, ***vol -f <fichero captura ram dmp> -y <dirección SYSTEM> -s <dirección SECURITY>***.

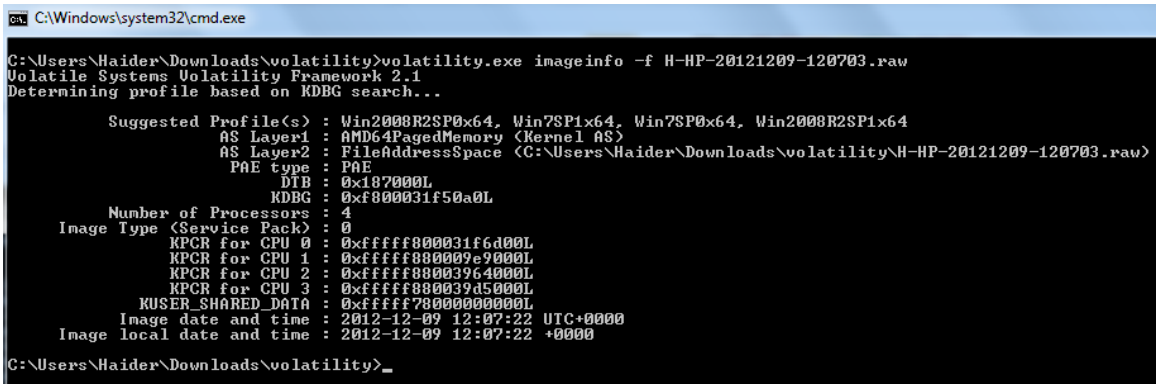


Foto descargada de http://blog.creativeitp.com/posts-and-articles/volatile-memory/introduction-to-the-volatility-framework/

Por último se puede observar el plugin hashdump de Volatility Framework. Con este plugin se puede obtener un volcado de usuarios y hashes de la SAM de Windows. Para llevar a cabo dicha acción la sintaxis es la siguiente ***vol -f <fichero captura ram dmp> -y <dirección SYSTEM> -s <dirección SAM>***.

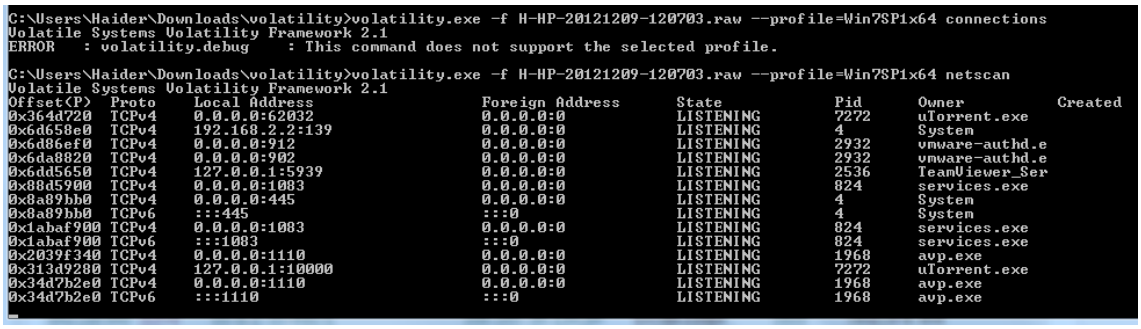


Foto descargada de http://blog.creativeitp.com/posts-and-articles/volatile-memory/introduction-to-the-volatility-framework/

Lo interesante de la ejecución anterior es la dirección virtual obtenida. Con ella podremos utilizar otros plugins para obtener otro tipo de información, por ejemplo en el caso de las LSA Secrets existe un plugin denominado lsadump con el que podremos obtener el contenido de dicho contenedor. Para ello, el plugin nos pide la dirección virtual de System y Security. La sintaxis es sencilla, ***vol -f <fichero captura ram dmp> -y <dirección SYSTEM> -s <dirección SECURITY>***.

Conclusiones: Voliatility es un framework utilizado para el análisis de la memoria de los dispositivos digitales, debido al amplio rango de dispositivos que puede analizar, se puede convertir en una herramienta casi obligatoria para los analistas forenses, en sus investigaciones.

Al ser un framework, se puede utilizar desde consola o integrado en otras herramientas, a las que aporta el análisis de las memoria de los dispositivos ampliando las caracteristicas de las herramientas.

WindowsSCOPE

Desarrollador: Windows SCOPE Forensics & Ciber Security Tools

Página de la herramienta: https://www.windowsscope.com/index.php

Tipo de Instalación: Instalable en Widows.

Tipo de Herramienta: Analizador de memoria de Windows, tanto del sistema como de usuario.

Uso: Sirve para analizar la memoria de Windows y realizar ingeniería inversa como apoyo para el analista forense digital.

Descripción: WindowsSCOPE es otra herramienta forense de análisis de memoria e ingeniería inversa que es utilizada para el análisis de la memoria volátil.

Básicamente se utiliza para el análisis de ingeniería inversa de malware. Proporciona capacidad para analizar el núcleo de Windows, controladores, archivos DLL, memoria virtual y física.

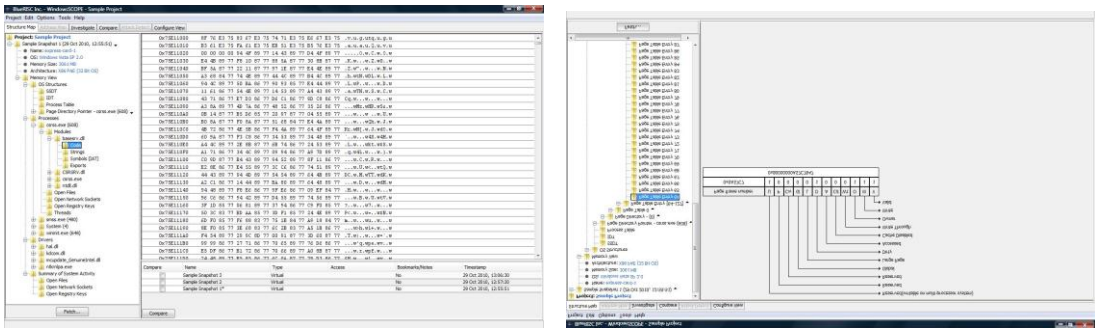


Foto descargada de http://www.windowsscope.com/index.php?option=com_lightgallery&view=list&Itemid=43

La herramienta WindowsSCOPE es utiliza para llevar a cabo, el análisis forenses de ataques cibernéticos en vivo, ingeniería inversa, análisis forense de memoria, informática forense, análisis cibernético, y otras actividades de defensa cibernética en la memoria tanto para el espacio de usuario y como del kernel.

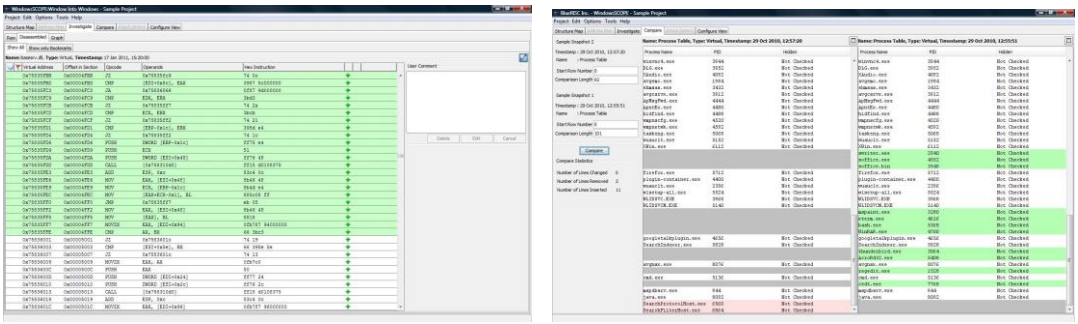


Foto descargada de http://www.windowsscope.com/index.php?option=com_lightgallery&view=list&Itemid=43

Son ideales para ingeniería inversa y/o analizar el funcionamiento interno del sistema operativo Windows y todo lo que se ejecuta en él. WindowsSCOPE Ciber Forense-Ultimate incluye además un marco de aquisición del consumo de memoria y asiste al analista forense, casi desde cero, en el análisis por hardware. WindowsSCOPE Ciber Forense - Appliance es un aparato forense de alto rendimiento capaz de realizar análisis forense de memoria viva de toda la red, archivos forenses y respuesta a incidentes a través de la progresión del análisis del incumplimiento retroactivo.

La galería de productos, la comparacion de productos, y una guía de inicio rápido son accesibles a través de los enlaces del menú superior.

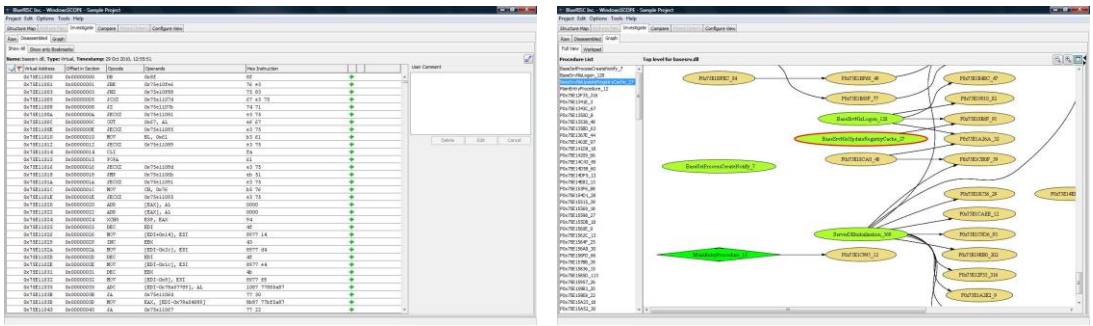


Foto descargada de http://www.windowsscope.com/index.php?option=com_lightgallery&view=list&Itemid=43

Una interfaz, GUI, permite una captura forense de la memoria basada y el análisis conjunto a partir de las herramientas disponibles. Permite la importación de vertederos

estándar de memoria windd, que luego son automáticamente analizados a través de ingeniería inversa y que son presentados en un formato fácil de visualizar para el análisis forense.

Las aplicaciones incluyen análisis forense digital, análisis forense de memoria, la investigación del delito cibernético, defensa cibernética, detección de ataques cibernéticos, análisis cibernético, y otras actividades de ingeniería inversa.

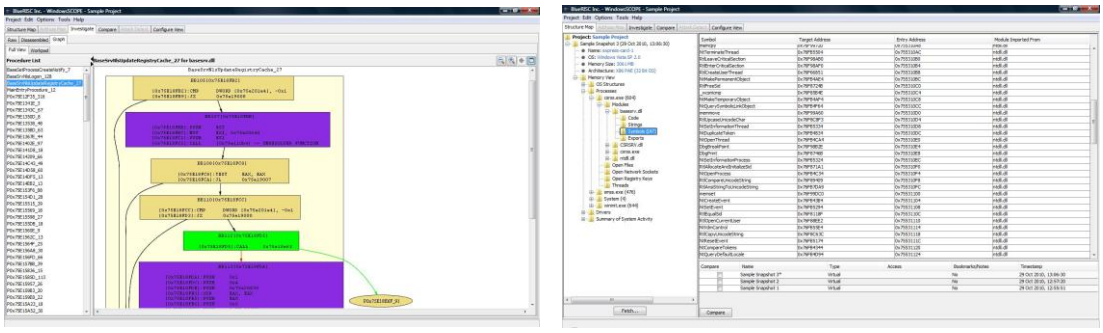


Foto descargada de http://www.windowsscope.com/index.php?option=com_lightgallery&view=list&Itemid=43

Proporciona capacidades integrales para el análisis del kernel y/o de las aplicaciones de software de Windows, controladores y archivos DLL, así como la actividad del usuario. Se pueden generar instantáneas de memoria virtual y física, en comparación, anotados y analizados desde muchos puntos de vista diferentes.

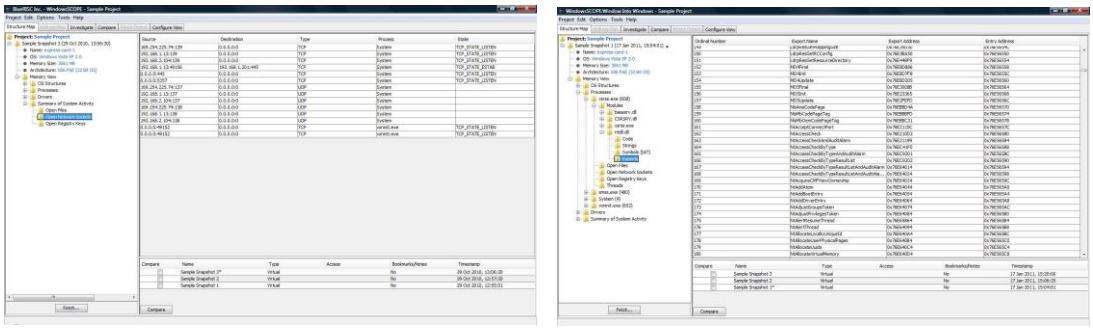


Foto descargada de http://www.windowsscope.com/index.php?option=com_lightgallery&view=list&Itemid=43

El sistema incluye desmontaje sofisticado, anotaciones, y capacidades gráficas de los programas. Viene con windd, mecanismo para buscar compatiblilidades y capacidades de importación. CaptureGUARD, que es opcional, es compatible con la adquisición de la memoria física basada en hardware y Phantom Sonda de memoria USB, dongle que es un mecanismo de busqueda.

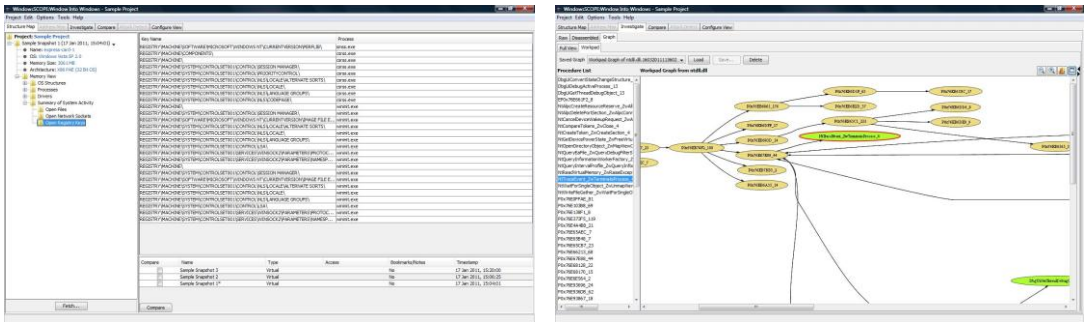


Foto descargada de http://www.windowsscope.com/index.php?option=com_lightgallery&view=list&Itemid=43

Conclusiones: Es otra de las opciones disponibles para el análisis de la memoria de Windows, con las opciones disponibles se pueden hacer análisis de memoria con información completa y informes claros y completos.

Oxygen Forensics Suite

Desarrollador: Oxygen Forensics

Página de la herramienta: http://www.oxygen-forensic.com/es/

Tipo de Instalación: Suite instalable.

Tipo de Herramienta: Herramienta para examinar y analizar dispositivos móviles, compatible con cualquier sistema operativo móvil existente, permite la recuperación y el escaneo de los datos de un dispositivo móvil.

Uso: Análisis de dispositivos móviles, abarcando casi cualquier sistema operativo móvil y la mayoría de dispositivos móviles.

Descripción: La herramienta Oxygen Forensic Suite es un buen software para reunir pruebas de un teléfono móvil para apoyar un caso, ya que esta herramienta ayuda en la recopilación de información (incluyendo fabricante, sistema operativo, número de IMEI, número de serie), los contactos, los mensajes (correos electrónicos, SMS, MMS), recuperar los mensajes borrados, registros de llamadas, asi como tambien la información del calendario. También nos permite acceder y analizar datos de dispositivos móviles y documentos.

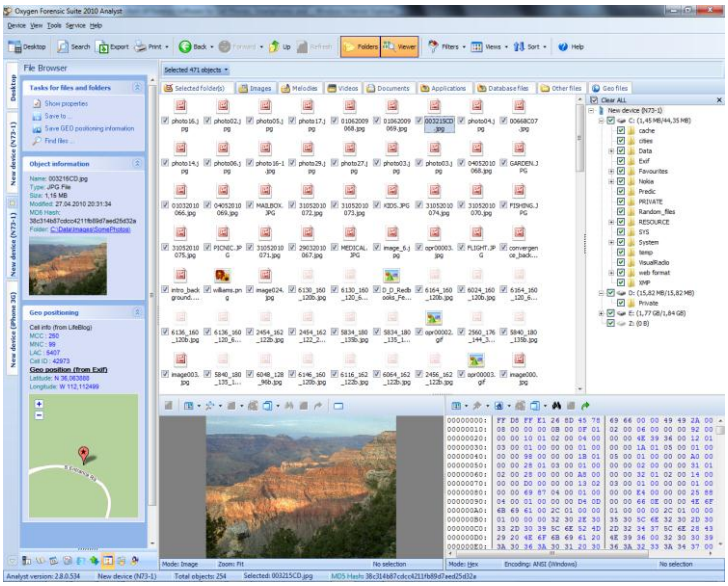


Foto descargada de http://oxygen-forensic-suite.win7dwnld.com/screenshots/

Oxygen Forensics está disponible en diferentes versiones para adaptarse a las necesidades de cada profesional:

- **Oxygen Forensics Suite Pro:** Una opción muy interesante para un analista forense. Pensada para ofrecer un estudio completo de todos los detalles que pueden ser útiles en una investigación forense hasta el más fino detalle, analizando los metadatos de fotografías, historiales de conexión, análisis de caché de navegadores o de aplicaciones como skype. Es decir, aplicaciones de post-análisis de datos que simplificarán más las taréas del forense. Es una versión de pago, el precio de esta licencia es de 899 €.

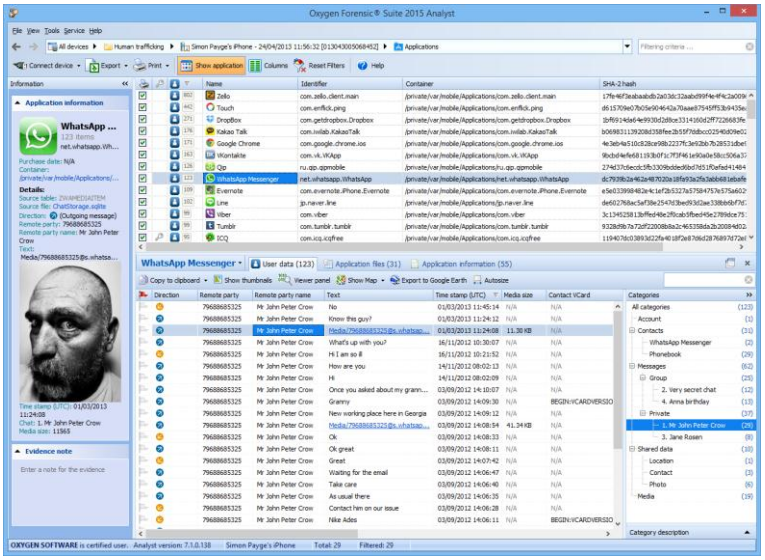


Foto descargada de http://www.oxygen-forensic.com/es/products/oxygen-forensic-suite/features

- **Oxygen Forensics Suite Pro Analyst:** Esta versión añade una gran cantidad de plug-ins y herramientas para agilizar los procesos de análisis forense, tales como herramietnas para recuperación de passwords, añadidos de time-line,

visores de ficheros plist o SQLlite, etc., es una versión bastante completa para el análisis forense. Su precio es de 1.499 €.

- **Oxygen Forensis Suite Pro Analyst with Android Rooting Add-on:** Esta versión, es para situaciones muy concretas, viene con un add-on que permite rootear los terminales con Android, haciendo que el análisis forense del terminal se realice completamente.

Como se puede observar, en la lista de versiones disponibles, mostradas anteriormente, existe una versión para adecuarse a las necesidades de cada analista forense, ya sea de forma profesional como para iniciarse en la materia.

Así, si una empresa tiene solo terminales Apple, por mucho menos de lo que cuesta un terminal puedes tener una versión de Oxygen Forensics que te permita conocer la historia de un dispositivo cuando quieras.

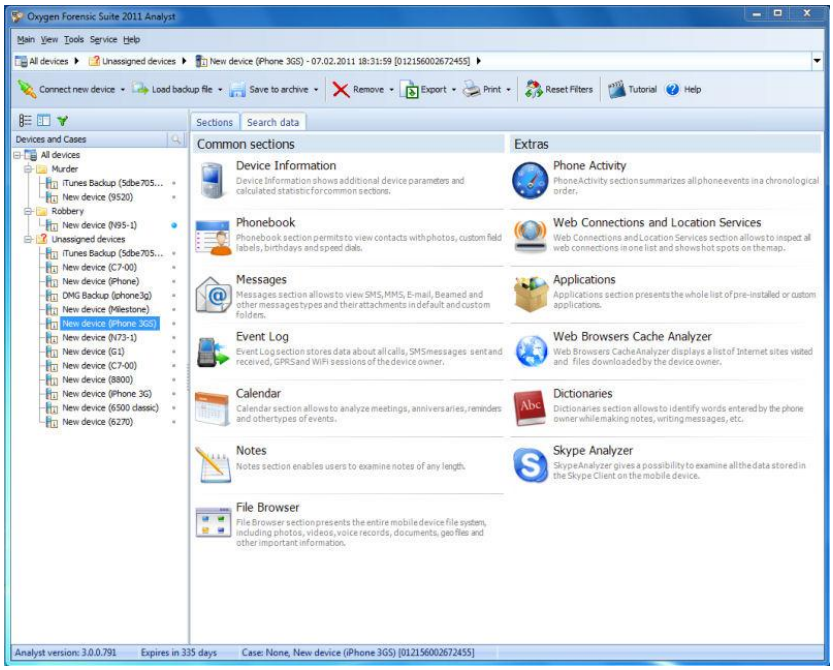


Foto descargada de https://forensiccontrol.com/resources/reviews/oxygen-forensic-suite-2011-training/

La herramienta te permite la adquisición de datos de más de 10350 dispositivos (Android, BlackBerry, iOS, Windows Phone, etc.). Importaciones de Backups de dispositivos e imágenes (iTunes, Android, JTAG y más). Analiza datos de más de 630 aplicaciones, muy populares, y extractos de contraseñas. Recupera una amplia variedad de datos borrados. Ofrece análisis de datos (Contactos Agregados, Grafo Social, Cronología). Exporta datos a formatos de archivo populares, como PDF, RTF, XLS, XML, etc.

Oxygen Forensic Extractor for Clouds es un programa forense que permite extraer datos de servicios en la nube y guardarlos en un dispositivo local, en un formato legible.

La autenticación es necesaria para acceder a los datos en la cloud. Un experto forense debe ingresar las credenciales de la cuenta (login y contraseña) y aceptar el acceso a los datos de la nube.

Oxygen Forensic Call Data Expert es un programa forense que permite importar y analizar archivos CDR (Call Data Records) recibida de los proveedores de servicios móviles sin tener en cuenta la diferencia en sus formatos de columna y diseños de archivo.

La Sección de Conexiones y Ubicaciones Web revela los lugares sospechosos visitados y las rutas de los sitios visitados.

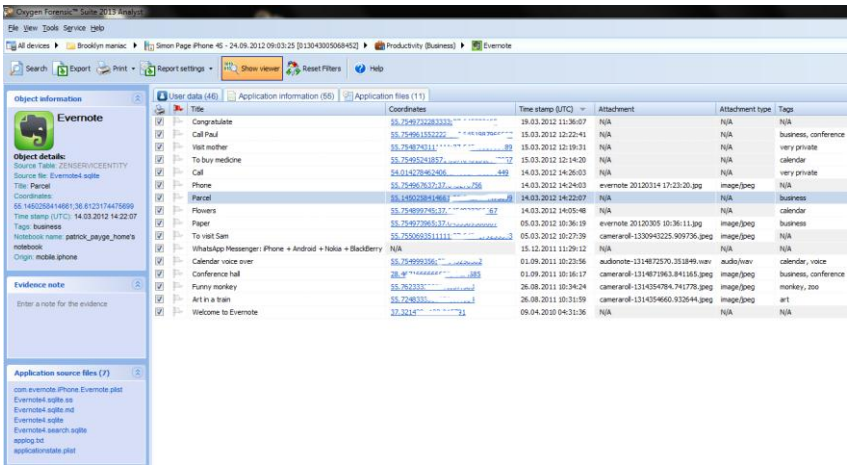


Foto descargada de http://zehndaumen.de/tag/oxygen-forensic-suite/

Los analistas forenses pueden analizar varias fuentes de datos de Geo-Localización: conexiones Wifi, conexiones IP y bases de datos de localizaciones.

Oxygen Forensic Suite recupera todos los datos de las aplicaciones vitales de dispositivos móviles en iOS, Android, BlackBerry 10, Windows Phone 8.

Oxygen Forensic Suite es capaz de descifrar aplicaciones de bases de datos, incluso si tienen seguridades cifradas.

SQLite Viewer permite explorar los archivos de base de datos con las siguientes extensiones: .sqlite, .sqlite3, .sqlitedb, .db, .db3.

Los analistas forenses tienen acceso a los datos reales y eliminados almacenados en las bases de datos creadas por las aplicaciones del sistema y de los usuarios.

El enraizamiento de un dispositivo basado en Android OS revela el conjunto completo de datos de usuario al investigador. Generalmente este procedimiento necesita cierto conocimiento y experiencia en investigación forense, pero Oxígeno Forensic Suite ayuda a los analistas forenses digitales a automatizar estas tareas.

Los Gráficos Sociales permiten visualiza las conexiones complejas, de forma que, a un analista forense le muestra las conexiones de los usuarios en sus grupos sociales.

Este es un trabajo altamente ajustable que permite a los expertos forenses a revisar las conexiones entre los propietarios de dispositivos móviles y sus contactos, identificar conexiones entre múltiples usuarios de dispositivos y detectar sus contactos comunes.

La sección de Contraseñas muestra logins y contraseñas extraídas del almacenamiento seguro por defecto, como las bases de datos keychain.

Los archivos de las aplicaciones también pueden contener datos valiosos. Oxygen Forensic Suite los analiza y los muestra de forma clara y concisa.

La línea de tiempo, permite ver todos los datos de uso de los dispositivos móviles en una lista ordenada, en la cual se observa el cambio de estado de cada dispositivo.

En esta línea de tiempo, se organizan todas las llamadas, mensajes, eventos de calendario, datos geográficos y otras actividades en forma cronológica, así que se puede seguir fácilmente el historial de las conversaciónes sin necesidad de cambiar entre diferentes secciones.

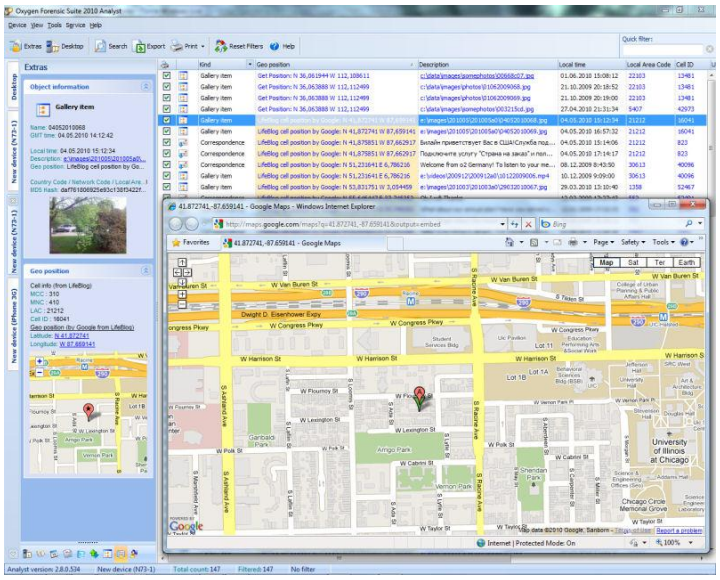


Foto descargada de https://forensiccontrol.com/resources/reviews/oxygen-forensic-suite-2011-training/

BBB e IPD son los archivos backup de dispositivos Blackberry hechos con BlackBerry Desktop Manager. Estos archivos se pueden encontrar en un equipo sospechoso o soportes externos como CD, DVD, discos de memoria y tarjetas, etc.

Oxygen Forensic Suite es capaz de extraer y presentar información forense importante desde los archivos de backup e imágenes de chip-off.

Oxygen Forensic Suite Analyst permite importar y analizar datos de varios archivos de backups de dispositivos y las imágenes creadas por el software de sincronización u otros productos forenses.

La Sección de registro de sucesos contiene la información de la comunicación de voz de los usuarios: llamadas marcadas, recibidas y perdidas. Los expertos encuentran aquí información de la hora de la llamada, la duración y la parte remota.

Recuperar archivos borrados de las llamadas están disponibles en ciertos tipos de dispositivos: smartphones iOS y Android OS.

La Sección de Mensajes contiene la correspondencia de los usuarios incluyendo SMS, MMS, correo electrónico, mensajes de iMessage y otros, dependiendo del tipo de dispositivo.

La recuperación de mensajes eliminados está disponible para ciertos tipos de dispositivos: teléfonos iOS, Android y Symbian OS.

Oxygen Forensic Suite puede detectar aplicaciones spyware instaladas en los dispositivos Android y Apple, y puede descubrir y procesar sus registros y archivos de configuración.

Varios espectadores de datos ayudan a los expertos a analizar los datos extraídos de una manera conveniente.

Oxygen Forensic Suite ha incorporado HEX-espectador, visor de imágenes, reproductores de música y vídeo, visor de texto con convertidor de página de códigos, HTML, SQLite y espectadores plist.

La sección File Browser, es una potente herramienta para acceder y analizar fotos, videos y documentos del usuario y bases de datos del dispositivo.

El texto incorporado, hexagonal, multimedia, SQLite, Plist espectadores, Geo-localización y extractores de archivos EXIF ayudan a los expertos a ver los archivos y sus propiedades.

La sección de la guía telefónica contiene los contactos de los usuarios con todos sus datos: nombre, ocupación, teléfonos, direcciones, correos electrónicos, notas.

Dependiendo de las necesidades de los expertos, y de los dispositivos, se puede acceder a la información privada de los contactos, como cumpleaños, nombres y aniversarios familiares.

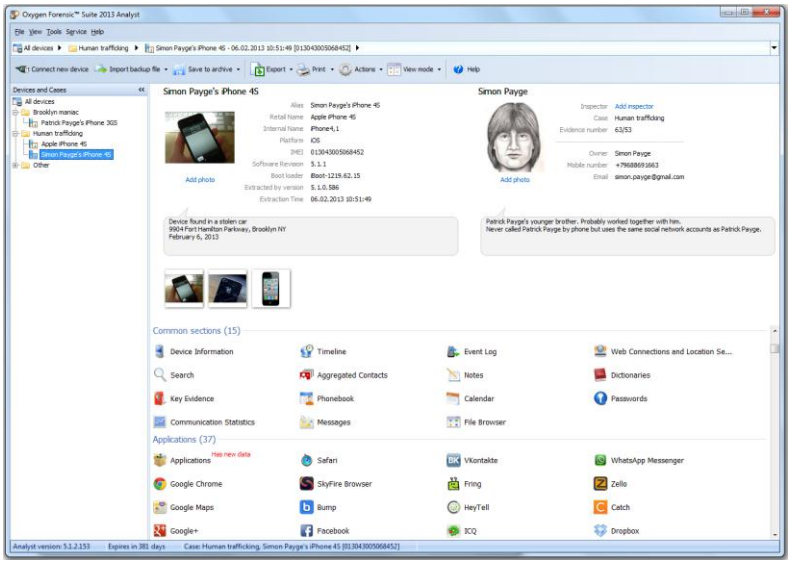


Foto descargada de http://teeltechcanada.com/forensic-tools/oxygen-analyst/

La sección Key Evidence ofrece una vista limpia y despejada de la evidencia marcada como esencial por los investigadores

Los especialistas forenses pueden marcar ciertos elementos pertenecientes a diversas secciones como pruebas esenciales y luego revisarlos todos a la vez independientemente de su ubicación original.

El soporte para los teléfonos provenientes de China permite a los analistas forenses extraer datos de réplicas de teléfonos populares y dispositivos de bajo coste.

Oxygen Forensic Suite es capaz de adquirir, desde los dispositivos provenientes de China, datos de usuario importantes como el registro de eventos, mensajes, contactos y archivos.

Oxygen Forensic Suite soporta una gran cantidad de tipos de aplicaciones de sociales como Skype, Facebook, WhatsApp, Viber y otros.

Oxygen Forensic Suite soporta todos los navegadores web populares para Android OS, Apple OS, BlackBerry OS y Symbian OS.

La sección de información del dispositivo, muestra información completa sobre el dispositivo. Esto incluye Fabricante, Modelo de venta, Plataforma y su revisión, IMEI, direcciones MAC, IMSI, número de serie, número de teléfono y los datos específicos del modelo.

Permite rápidamente revelar conexiones sociales entre los usuarios de dispositivos móviles bajo investigación y sus contactos.

La sección de enlaces y estadísticas proporciona una herramienta para explorar las conexiones sociales entre los usuarios de dispositivos mediante el análisis de llamadas, texto, multimedia y mensajes de correo electrónico y conexiones de Skype.

Analizar los contactos desde múltiples lugares como la guía telefónica, mensajes, registro de eventos, Skype, chat y aplicaciones de mensajería agregados en Contactos.

Busca automáticamente a las mismas personas en diferentes fuentes y los agrupa en un solo meta-contacto.

Global Search permite descubrir datos de usuario en cada sección del dispositivo.

La sección de Herramienta ofrece busquedas de texto, números telefónicos, correos electrónicos, geocoordenadas, direcciones IP, direcciones MAC, números de tarjeta de crédito. También dispone de una biblioteca de expresiones regulares para una búsqueda más personalizada.

La sección Organizador muestra notas, tareas y entradas de calendario creados o sincronizados por el usuario del dispositivo.

El conjunto de sub-secciones y sus funciones depende del fabricante del dispositivo confiscado y modelo exacto.

Cuando se trata de resolver un crimen informático, los informes son una de las cosas más importantes para el investigador. Formatos de archivo populares y capacidad de exportar o imprimir todo el conjunto de datos o sólo partes importantes ayuda a los expertos a mostrar el resultado de su trabajo de la mejor manera.

Archivos plist, conocido como Property List XML Files, contienen una gran cantidad de valiosa información forense en los dispositivos de Apple. Historial del navegador, puntos de acceso Wi-Fi, marcaciones, Bluetooth ajustes de aplicaciones globales, Apple Store y, aún más datos se pueden extraer de archivos .plist.

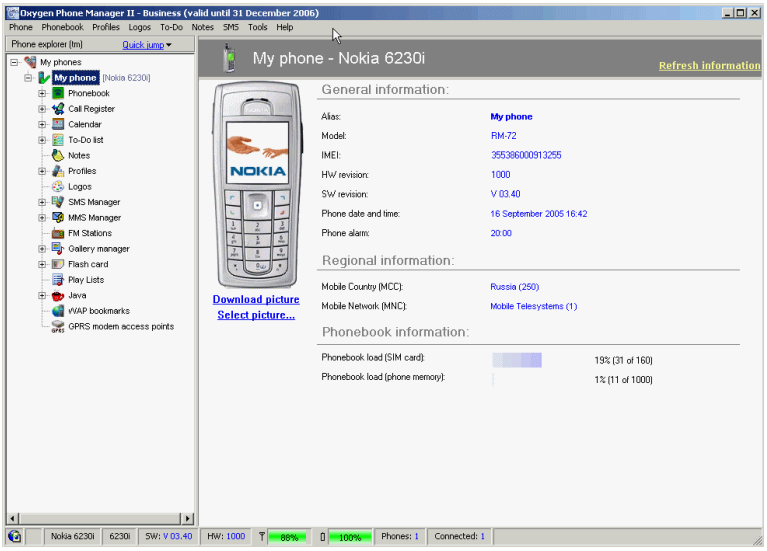


Foto descargada de http://software.ivertech.com/OxygenForensicSuite2010forNokiaphones_software77176.htm

La sección Diccionarios muestra todas las palabras alguna vez introducidos en los mensajes del dispositivo, notas y calendario.

Oxygen Forensic Suite concede el acceso a las aplicaciones de navegación populares y revela POIs, rutas y busca que el usuario del dispositivo hizo.

Los usuarios de smartphones tienden a tener una copia de seguridad de sus datos en la nube, proporcionadas por el fabricante del dispositivo o una tercera parte. La plataforma Windows Phone tiene su propio almacenamiento para guardar de forma segura los contactos de los usuarios, mensajes, datos de aplicaciones, configuraciones, archivos y más. Oxygen Forensic Suite es capaz de extraer datos de Windows Phone Cloud.

Los backups de iTunes se pueden encontrar en un equipo sospechoso, es una práctica regular debido a la popularidad de los dispositivos de Apple. Oxygen Forensic Suite ofrece a los analistas forenses una manera fácil de extraer los datos privados de los sospechosos de los archivos de backup de iTunes.

Conclusiones: Se trata de una herramienta para el análisis forense digital de dispositivos móviles con muchas opciones. Aunque es una herramienta de pago, es una inversion acceptable ya que dispone de bastantes opciones de escaneo y en casi todos los dispositivos móviles, desde móviles a tablets.

Se han expuesto las caracteristicas que posee Oxygen Forensic para el análisis forense digital de dispositivos móviles, se pueden extraer informaciones valiosas de los distintos dispositivos móviles, desde Android a Iphone, pasando por Blackberry.

Bulk Extactor

Desarrollador: Garfinkel, Simson

Página de la herramienta: http://digitalcorpora.org/downloads/bulk_extractor/

Tipo de Instalación: Ejecutable, se descarga un ejecutable y se ejecuta.

Tipo de Herramienta: Escanea y analiza dispositivos y archivos.

Uso: Sirve para recuperar y analizar dispositivos en busca de archivos borrados, cuentas de correo, números de tarjetas de crédito, etc. Muy útil en el análisis forense digital.

Descripción: Bulk Extractor Viewer (BEviewer) es la interfaz gráfica de Bulk Extractor, un programa escrito en C ++, que escanea imagenes de disco, archivos o directorios de archivos y extrae información útil sin necesidad de analizar el sistema de archivos o del sistema de estructuras de archivos completa.

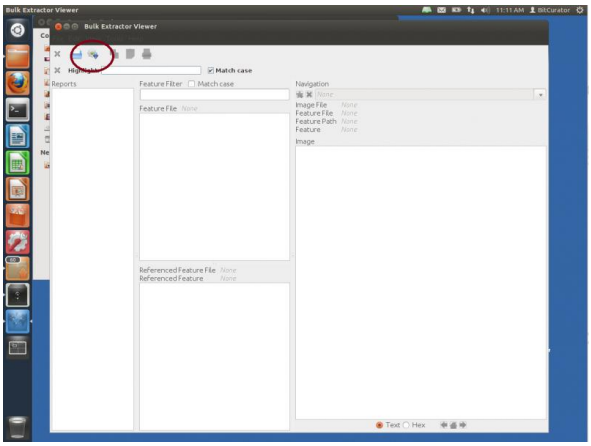


Foto descargada de http://wiki.bitcurator.net/index.php?title=Using_Bulk_Extractor_Viewer_to_Find_Potentially_Sensitive_Information_on_a_Disk_Image

Los resultados pueden ser fácilmente revisados, analizados y procesados directamente o con herramientas de automatización.

Bulk Extractor también crea un histograma de características que encuentra, las características más comunes, que pueden ser más importantes para el análisis forense digital.

Mientras que originalmente fue destinado al análisis forense digital, Bulk Extractor puede ser utilizado por gestores documentales para examinar una imagen de disco, de forma rápida y completa, para extraer una amplia variedad de información de la información extraida.

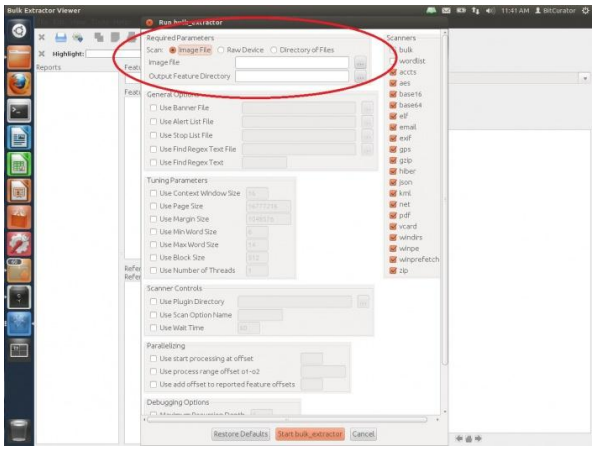


Foto descargada de http://wiki.bitcurator.net/index.php?title=Using_Bulk_Extractor_Viewer_to_Find_Potentially_Sensitive_Information_on_a_Disk_Image

El uso más común para este tipo de análisis es la localización de la información de identificación personal (PII) que un usuario puede querer redactar antes de que se hagan públicos sus materiales, pero Bulk Extractor puede localizar otros tipos de información potencialmente sensible.

Los analistas pueden ver los resultados a través de la interfaz gráfica de usuario y también procesarlos utilizando las herramientas forenses digitales en el entorno BitCurator.

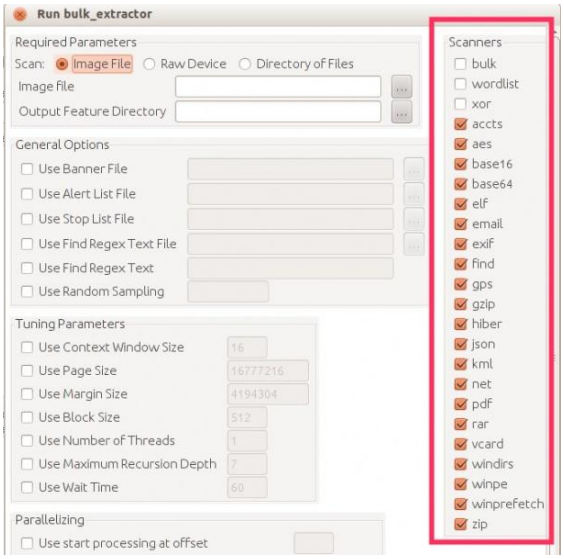


Foto descargada de http://wiki.bitcurator.net/index.php?title=Using_Bulk_Extractor_Viewer_to_Find_Potentially_Sensitive_Information_on_a_Disk_Image

Bulk Extractor es un programa que extrae características tales como direcciones de correo electrónico, números de tarjetas de crédito, direcciones URL, y otros tipos de información de archivos de evidencia digitales. Es una herramienta de investigación forense útil para muchas tareas, tales como malware, investigaciones de intrusión, investigaciones de identidad, investigaciones cibernéticas, así como el análisis de las imágenes.

El programa ofrece varias capacidades inusuales, incluyendo:

- Encuentra direcciones de correo electrónico, URL y números de tarjetas de crédito, ya que puede procesar datos comprimidos (como ficheros ZIP, PDF y GZIP) y datos incompletos o parcialmente dañados. Se pueden recuperar JPEG, documentos de oficina y otros tipos de fragmentos de archivos de datos comprimidos. Detectará y recuperará archivos RAR encriptados.

- Construye listas de palabras basado en todas las palabras que se encuentran dentro de los datos, incluso los que están en los archivos comprimidos que se encuentran en el espacio no asignado. Esas listas de palabras pueden ser útiles para la obtención ilegal de contraseñas.

- Es multi-hilo, corriendo Bulk Extractor en un equipo con el doble de la cantidad de núcleos, hace que completar una ejecución se realice en la mitad del tiempo.

- Crea histogramas que muestran las direcciones de correo electrónico más comunes, URLs, dominios, términos de búsqueda y otros tipos de información en el disco.

Bulk Extractor funciona con imágenes de disco, archivos o un directorio de archivos y extrae la información útil sin necesidad de analizar el sistema de ficheros o las estructuras de ficheros del sistema.

La entrada se divide en páginas y es procesada por uno o más escáneos. Los resultados se almacenan en archivos de características que pueden ser fácilmente inspeccionados, analizandos, o procesados con otras herramientas automatizadas.

Bulk Extractor también crea histogramas de características, que son útiles porque tales características, como direcciones de correo electrónico y términos de búsqueda en Internet, son de las actividades más comunes realizadas por los usuarios y en de las cuales se puede extraer información muy útil para el análisis forense digital.

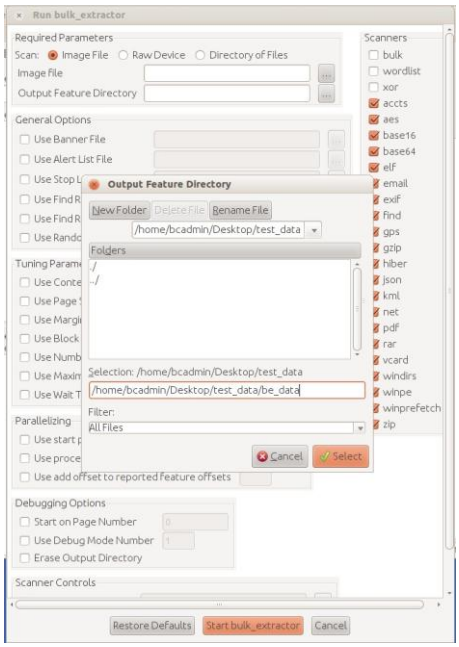


Foto descargada de http://wiki.bitcurator.net/index.php?title=Using_Bulk_Extractor_Viewer_to_Find_Potentially_Sensitive_Information_on_a_Disk_Image

Además de las capacidades descritas anteriormente, Bulk Extractor también incluye:

- Una interfaz gráfica de usuario, Bulk Extractor Viewer, para la navegación por los menús de la aplicación.
- Un pequeño número de programas en Python para la realización de un análisis adicional en función de los archivos.

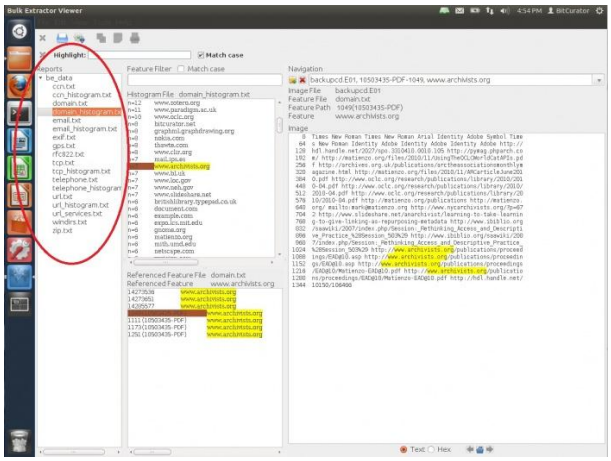


Foto descargada de http://wiki.bitcurator.net/index.php?title=Using_Bulk_Extractor_Viewer_to_Find_Potentially_Sensitive_Information_on_a_Disk_Image

Conclusiones: Bulk Extractor es una herramienta para extraer información ineresante de archivos, carpetas e imágenes de disco, sin necesidad de recorrer la estructura completa des sistema, ahorrando tiempo y sólo buscando en los lugares concretos, necesarios, para el análisis forense digital.

Download it here: http://digitalcorpora.org/downloads/bulk_extractor/

Xplico

Desarrollador: CapAnalisysy

Página de la herramienta: http://www.xplico.org/

Tipo de Instalación: Es un paquete para Linux, aunque también viene en una imagen para Virtual Box, con Ubuntu.

Tipo de Herramienta: Es una herramienta para monitorizar una red.

Uso: Se utiliza desde una máquina Linux y sirve para monitorizar una red, ver descargas, analizar paquetes que viajan por la red, etc.

Descripción: **Xplico** es una herramienta para el análisis forense de la red (NFAT), es un software que reconstruye el contenido de las adquisiciones realizadas con un analizador de paquetes (por ejemplo, Wireshark, tcpdump, Netsniff-ng).

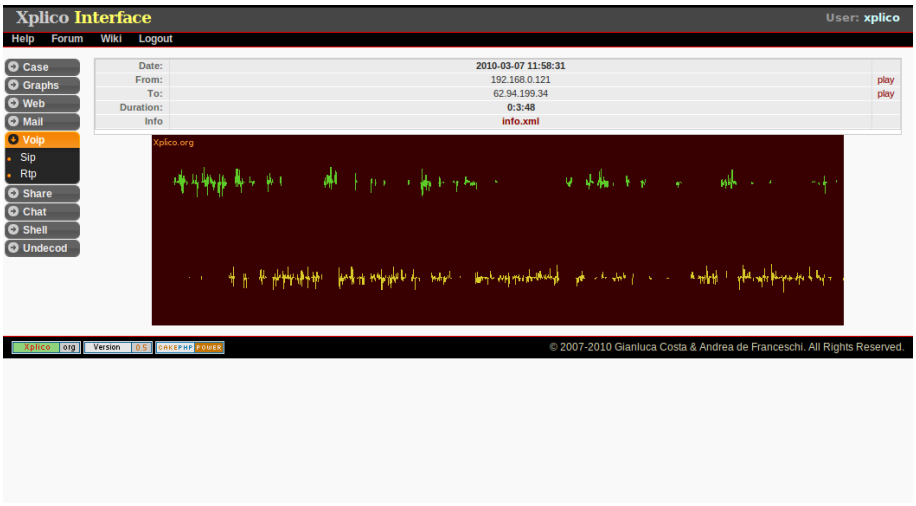


Foto descargada de http://www.xplico.org/screenshot

A diferencia de los analizadores de protocolos, cuya característica principal no es la reconstrucción de los datos transportados por los protocolos, Xplico nace expresamente con el objetivo de reconstruir los datos de la aplicación de los protocolos y es capaz de reconocer los protocolos con una técnica llamada Puerto identificación Protocolo Independiente (PIPI).

El objetivo de Xplico es extraer el un tráfico de Internet y capturar los datos de las aplicaciones contenidas.

Xplico no es un analizador de protocolos de red. Xplico es una herramienta para el análisis forense de la red (NFAT).

Xplico se distribuye bajo la **Licencia Pública General de GNU** y con algunas secuencias de comandos bajo licencia Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported (CC BY-NC-SA 3.0).

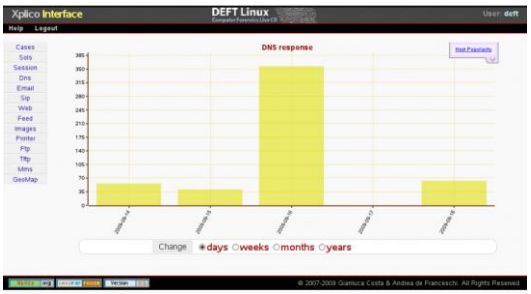


Foto descargada de http://www.xplico.org/screenshot

Para aclarar lo que Xplico nos ofrece, podemos imaginar a tener los datos en bruto (Ethernet o PPP) de una navegación web (protocolo HTTP), en este caso Xplico es capaz de extraer y reconstruir todas las páginas Web y los contenidos (imágenes, archivos, cookies, etcétera). Del mismo modo Xplico es capaz de reconstruir la dirección de correo de intercambiado con los protocolos IMAP, POP y SMTP. Por ejemplo, a partir de un archivo pcap Xplico extrae cada correo electrónico (protocolos POP, IMAP y SMTP), todos los contenidos HTTP, cada llamada VoIP (SIP), FTP, TFTP, y así sucesivamente.

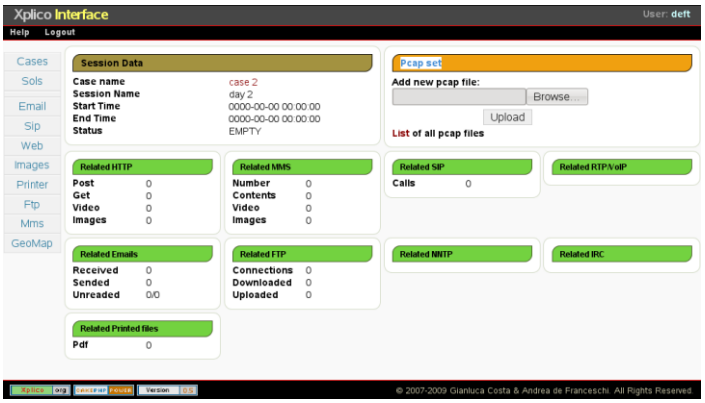


Foto descargada de http://www.xplico.org/screenshot

Entre los protocolos que Xplico identifica y reconstruye hay VoIP, MSN, IRC, HTTP, IMAP, POP, SMTP y FTP.

La arquitectura de software de Xplico ofrece:

- un *módulo de entrada* para manejar la entrada de datos (de sondas o analizador de paquetes)
- un *módulo de salida* para organizar los datos decodificados y presentarlos al usuario final
- un conjunto de *módulos de decodificación* , llamada *disector de protocolo* para la decodificación del protocolo de red individual

Con el *módulo de salida* Xplico puede tener diferentes interfaces de usuario, de hecho, puede ser utilizado desde la línea de comandos y desde una interfaz de usuario web llamado "Xplico Interface". El *disector de protocolo* contiene los módulos para la decodificación del protocolo individual, cada *disector de protocolo* pueden reconstruir y extraer los datos del protocolo.

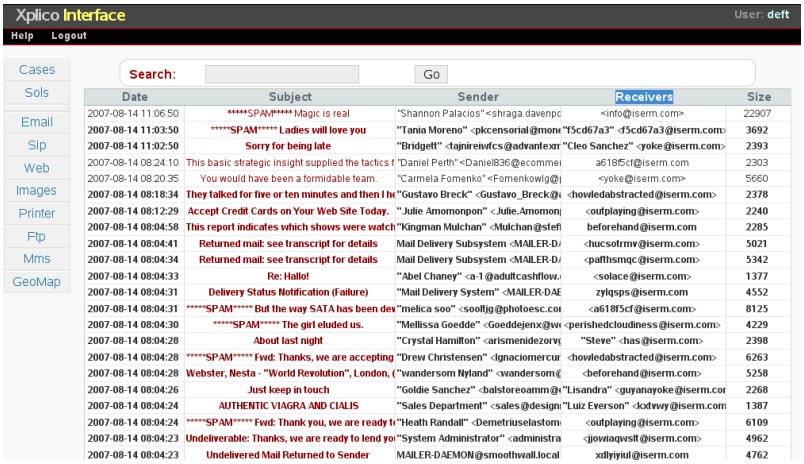


Foto descargada de http://www.xplico.org/screenshot

Todos los módulos son plug-in añadidos a la herramienta, a través del archivo de configuración, que se pueden cargar o no durante la ejecución del programa. Esto permite enfocar la decodificación, es decir, si desea decodificar sólo llamadas de VoIP

pero no el tráfico web, que acompañan a las llamadas, se configura Xplico para cargar sólo los módulos RTP y SIP, excluyendo el módulo HTTP.

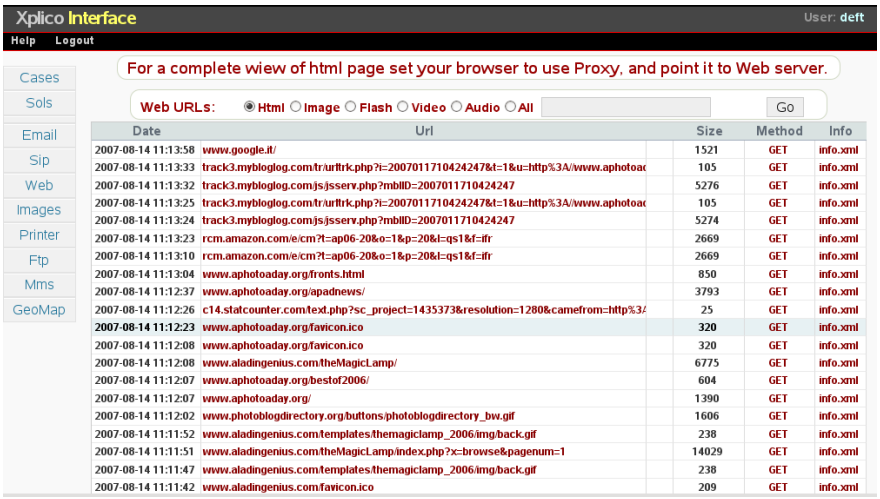


Foto descargada de http://www.xplico.org/screenshot

Otra característica de Xplico es su capacidad para procesar (reconstruir) enormes cantidades de datos, es capaz de manejar archivos pcap de muchos Gbyte y también Tbyte y de múltiples sondas de captura a la vez, esto gracias a la utilización de diversos tipos de "módulos de entrada". Los archivos pcap se pueden cargar de muchas maneras, directamente desde la interfaz de usuario Web de Xplico o con SFTP o con un canal de transmisión llamado PCAP sobre IP.

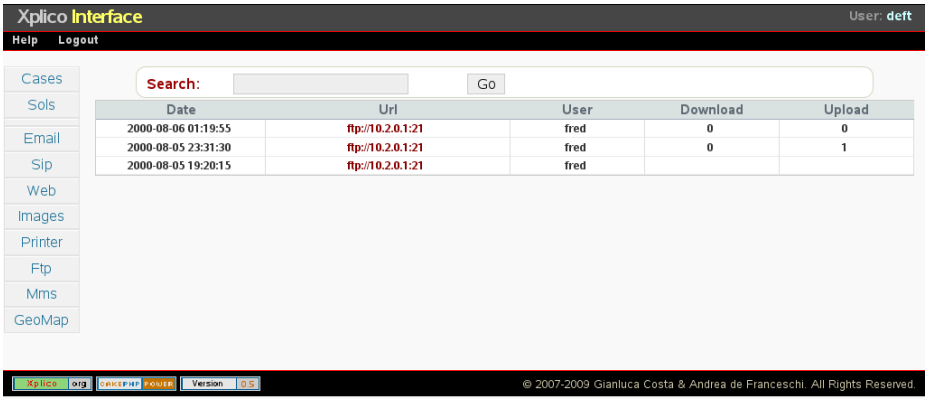


Foto descargada de http://www.xplico.org/screenshot

Para ello Xplico se puede usar en contextos de interceptación legal y en el análisis forense de la red.

Las características más destacadas de Xplico son:

- Protocolos soportados: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, ...;
- Puerto de Identificación Protocolo Independiente (PIPI) para cada protocolo de aplicación;
- Multithreading;

- Datos de salida y almacenamiento de la información en la base de datos SQLite o base de datos y/o archivos Mysql;
- En cada dato reensamblado por Xplico está asociado un archivo XML que identifica de manera única los flujos y la pcap que contiene los datos reensamblados;
- Elaboración en tiempo real (depende de la cantidad de los flujos, los tipos de protocolos y por el desempeño de -RAM ordenador, CPU, tiempo de acceso de alta definición, ... -);
- Reensamblaje TCP ACK con la verificación de cualquier paquete o verificación ACK suave;
- Búsqueda de DNS inversa, de paquetes DNS contenida en los archivos de entrada (pcap), no desde un servidor DNS externo;
- No hay límite de tamaño en la entrada de datos o el número de entrada de archivos (el único límite es el tamaño de alta definición);
- IPv4 e IPv6;
- La modularidad. Cada componente Xplico es modular. La interfaz de entrada, el decodificador de protocolo (Disector) y la interfaz de salida (despachador) son todos los módulos;

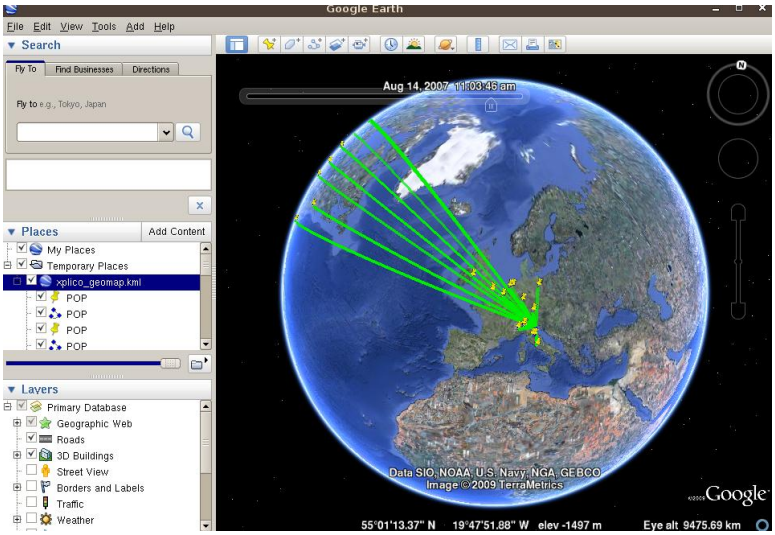


Foto descargada de http://www.xplico.org/screenshot

- La posibilidad de crear fácilmente cualquier tipo de distribuidor con el que organizar los datos extraídos de la manera más adecuada y útil;

Conclusiones: Es una herramienta para extraer la información de una red. Lo que permite monitorizar la transmission de los datos, pudiendo extraer cualquier tipo de información que ha sido transmitida, en un momento determinado en una Red.

Es una herramienta muy util para un analista forense, ya que, a partir de un fichero pcap extrae desde la navegación Web que se ha realizado, hasta correos enviados, pasando por cualquier dato interesante relacionado con ese momento de tiempo.

Read more about this tool here: http://www.xplico.org/about

Mandiant RedLine

Desarrollador: Mandiant A Fire Eye Company

Página de la herramienta: https://www.mandiant.com/resources/download/redline

Tipo de Instalación: Archivo con extensión Zip

Tipo de Herramienta: Analizador de actividades en la memoria y archivos de los dispositivos.

Uso: Análisis de memoria y estructura de archivos de un equipo.

Descripción: Redline, es una herramienta gratuita, la más importante de Mandiant, ofrece la capacidad de investigación, a los analistas forenses, para encontrar signos de actividad maliciosa a través de la memoria y el análisis de archivos, y el desarrollo de un perfil de evaluación de amenazas.

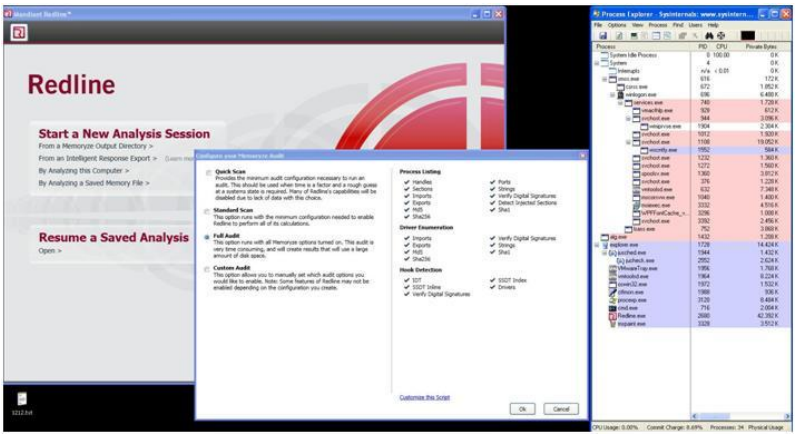


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Con Redline, los usuarios pueden:

- Auditar y recoger, completamente, todos los procesos y los drivers que se están ejecutando en la memoria, los metadatos del sistema de archivos, los datos del registro, registros de eventos, información de la red, los servicios, las tareas y el historial web.
- Analizar y ver los datos de auditoría importados, incluyendo estrechamiento y filtrado de los resultados alrededor de un plazo determinado utilizando la funcionalidad de la línea de tiempo de Redline con las características TimeWrinkle ™ y TimeCrunch ™.

- Agilizar el análisis de memoria con un flujo de trabajo probado para analizar malware basado en la prioridad relativa.
- Identificar los procesos más probables para investigar en base al Índice de Riesgo Malware Redline (MRI).
- Realizar un análisis de Indicador de Compromiso (Indicator of Compromise, IOC). Se suministra con un conjunto de IOC, el Agente portátil Redline se configura automáticamente para reunir los datos necesarios para realizar el análisis del IOC y un resultado de opinión del IOC.

Además, los usuarios de la herramienta de FireEye, **Punto Amenaza Plataforma Prevención (HX),** pueden abrir colecciones de elección directamente en Redline para llevar a cabo análisis en profundidad que permite al usuario establecer una línea de tiempo y el alcance de un incidente.

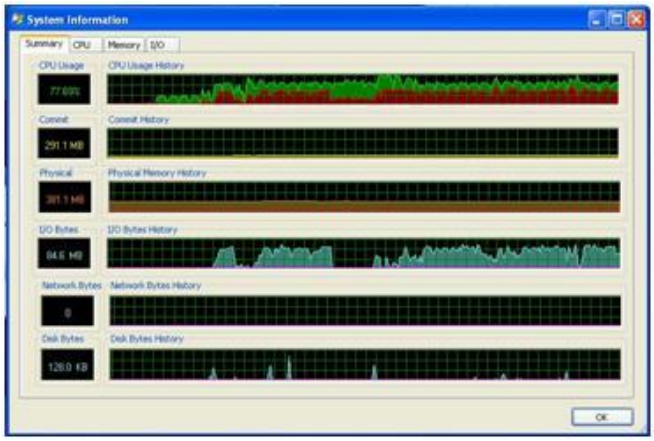


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Redline, es un analizador de la memoria, como si fuera "Volatility" pero con GUI.

El trabajo de Redline consiste en analizar la memoria y valorándola mostrar qué proceso tiene más posibilidad de ser malware y cuál menos, contando puntos MRI (Malware Risk Index).

Al instalar nos muestra varias opciones de análisis, muy interesante tiene la opción de análisis sobre un "*Saved memory File",* que parece a Volatility. Si seleccionas la opción de análisis de la maquina local "*Analyzing this Computer*", nos permite analizar muchas cosas interesantes como por ejemplo: Hooks, Drivers con sus Exports e Imports, Procesos con sus actividades, etc.

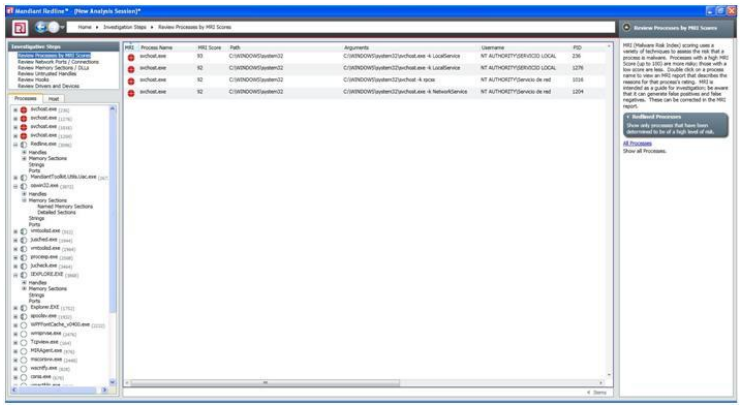


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Se puede seleccionar la opción "*Full Audit*" que analiza todo. Es muy curioso observar, que aunque las características de la máquina sean escasas, Redline escapaz de realizar un análisis en unos 25-30 minutos, la memoria casi no la toca, pero el procesador es el que realiza el proceso. Un equipo de escasos recursos puede utilizarse para realizar análisis.

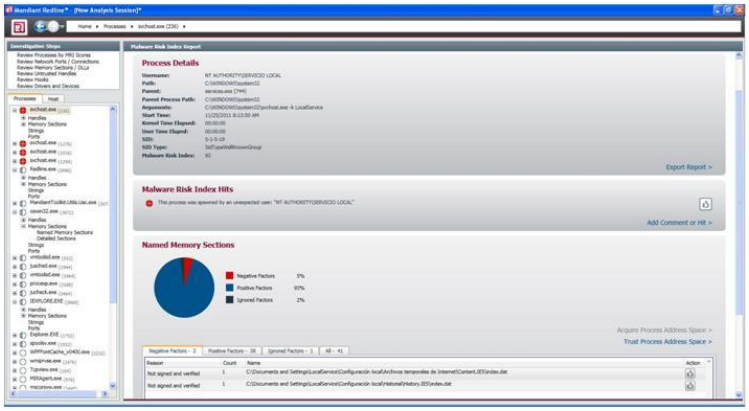


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Una vez finalizado el análisis, se puede observar que nos muestra una lista de procesos, algunos se marcan en rojo.

Un review de los procesos con su valoración, pinchando en cada uno de ellos nos mostrara info más detallada del veredicto.

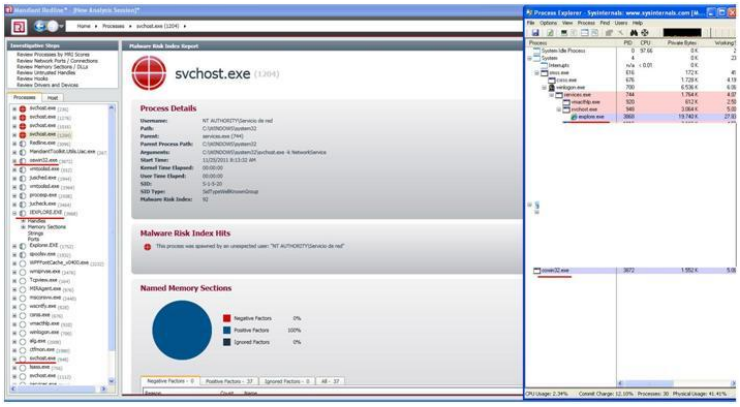


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Los procesos que están marcados en rojo, si accedemos a uno, nos muestra los factores positivos y negativos por los que valora los procesos. Cuantos más factores negativos mas posibilidad a que lo marque en rojo como sospechoso, son los posibles malware.

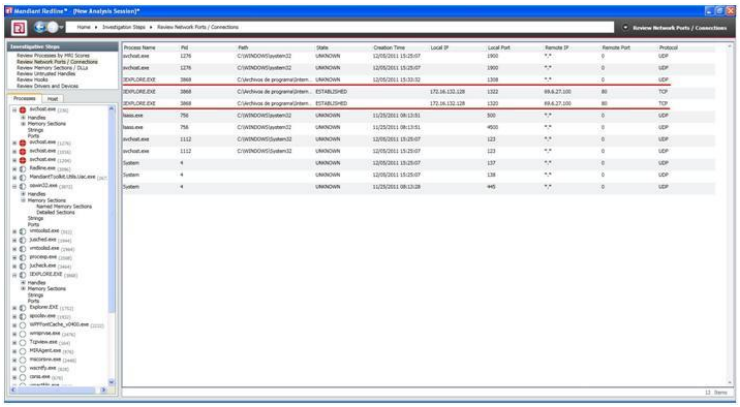


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

También se puede, con Redline, verificar las conexiones.

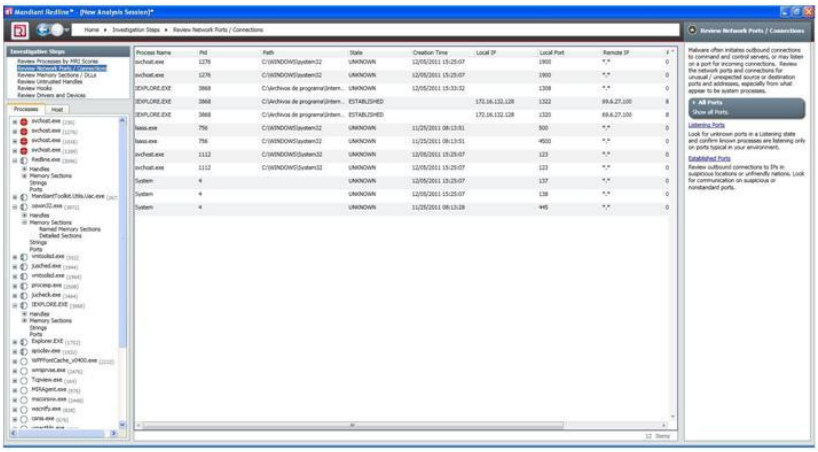


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Podemos elegir alguno de los filtros de las conexiones: puertos en escucha, conexiones establecidas o todos.

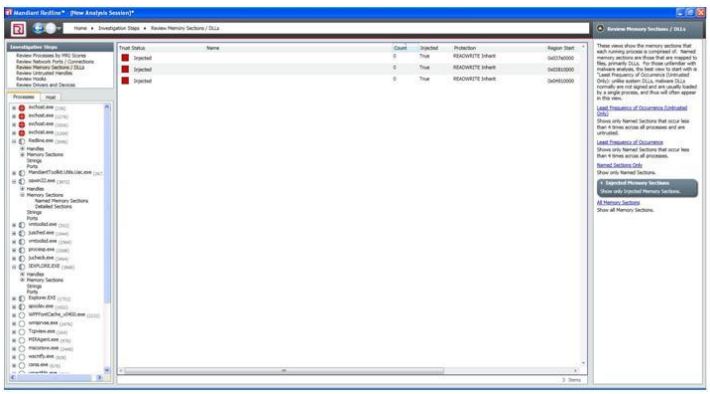


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Otra opción que nos permite Redline, es revisar los handles desconfiados. Aquí también hay filtros de “solo desconfiados” o todos.

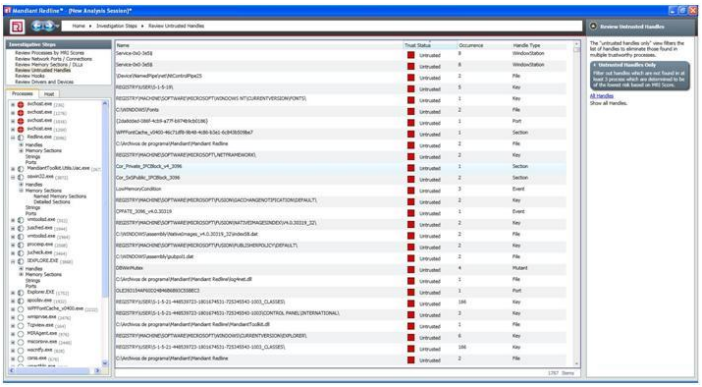


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Otra de las opciones disponibles los Hooks, tenemos varios filtros de diferentes tipos de hooks.

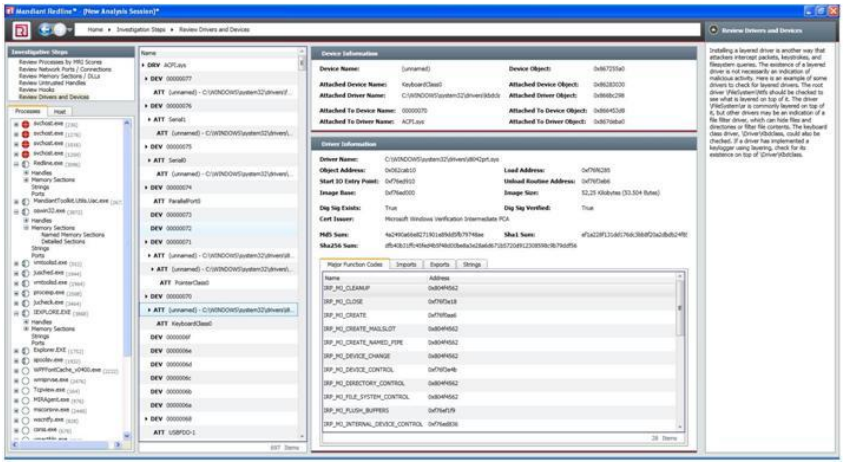


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Más cosas interesantes, se pueden ver secciones de memoria, strings, puertos utilizados o handles de todo tipo por cada proceso.

Muy interesante en la parte de *Detailed Sections* están todas las secciones del proceso, a la derecha podremos hacer búsquedas en cada uno de ellos y ver qué es lo que exporta, importa, etc.

De los strings de cada proceso, se pueden buscar patrones, simplemente se necesita buscar cadenas.

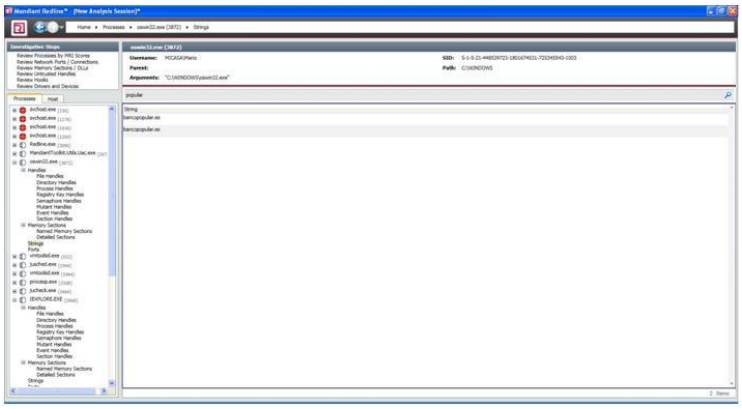


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

La pestaña Host, proporciona la información completa sobre los procesos, un punto muy interesante son los procesos en jerarquía, conexiones establecidas, drivers, hooks, información detallada del equipo y el SO, información genérica del equipo.

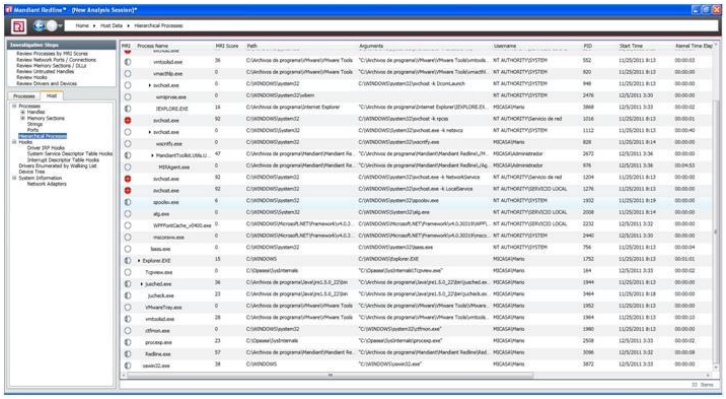


Foto descargada de http://blog.buguroo.com/analisis-binarios-con-mandiant-redline/

Algunos de los puntos más positivos son: la aplicacion permite crear un Agente portable directamente desde el menú de la aplicación, muy útil para un análisis externo y sin necesidad de instalarlo, permite guardar el análisis y seguir con el mismo en otro momento.

Conclusiones: La aplicación no está nada mal, pero es como utilizar Volatility con GUI o SysInternals TODO EN 1.

La interfaz gráfica es muy amigable y fácil de manejar. Para un análisis, no es aconsejable basarse solo en los veredictos de la aplicación, seria muy interesante apoyarse en otras herramientas para verificar los resultados.

Es útil en algunas ocasiones y cómoda para utilizar. Gracias a su interfaz gráfica, aunque sería necesaria una revisión en versiones posteriores, ya que los resultados no son todo lo satisfactorios que deberían.

Read more here: https://www.mandiant.com/resources/download/redline

P2 eXplorer

Desarrollador: Paraben Corporation

Página de la herramienta: https://www.paraben.com/p2-explorer.html

Tipo de Instalación: Ejecutable que instala la herramienta en un ordenador.

Tipo de Herramienta: Monta imágenes de discos duros, tanto de forma lógica como física.

Uso: Para realizar el montaje de imágenes de muy diversa procedencia, lo que permite con una sola herramienta montar imágenes diferentes y no tener que disponer una por cada tipo de imagen.

Descripción: P2 Explorer es una herramienta de software de montaje de imagenes que le permite montar cualquier imagen o disco duro para el análisis forense. Esta aplicación le permite explorar imágenes o unidades de disco duro como si fuera una unidad local en su ordenador mientras se mantiene fiel a su naturaleza forense, mantener la integridad de los datos.

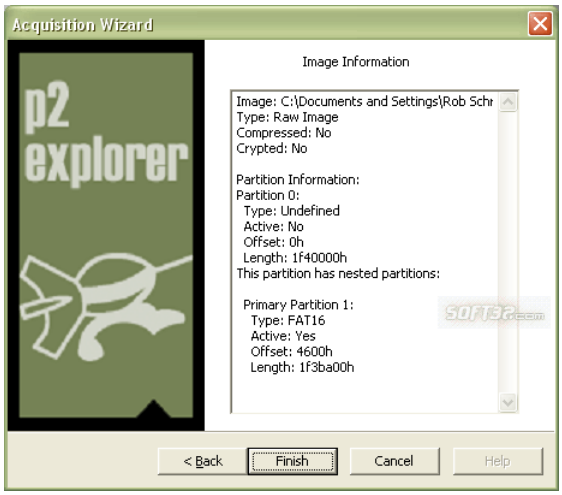


Foto descargada de http://p2-explorer.soft32.com/

P2 Explorer es una herramienta de gran alcance capaz montaje de imágenes tanto de forma lógica y como física a un disco. Este producto también es capaz de montar imágenes, con Replicator Forenses, comprimidas y encriptadas, imágenes PFR, imágenes EnCase y SafeBack 1,2 y 3.

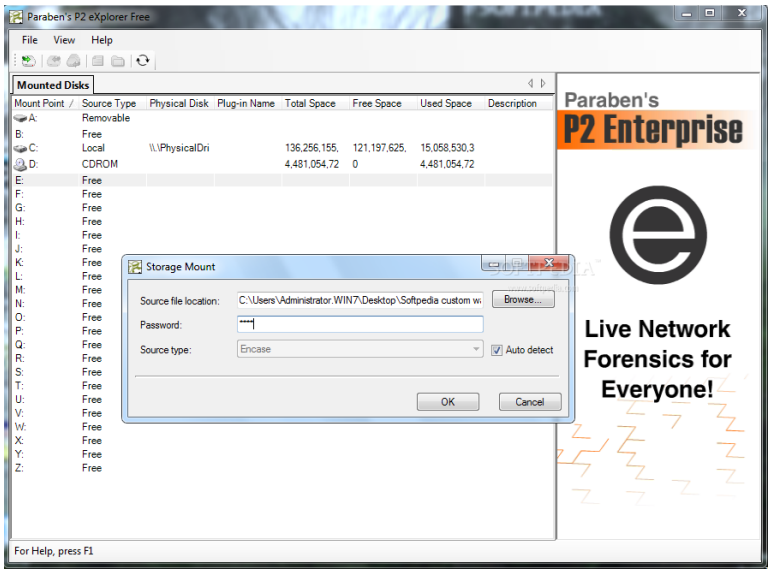


Foto descargada de http://www.softpedia.com/get/System/Hard-Disk-Utils/P2-eXplorer.shtml#sgal_0

Este programa de software es capaz de montar otros archivos de imagen como imágenes FTK DD, imágenes FTK EnCase, imágenes WinImage no comprimidas y las imágenes RAW de Linux DD y herramientas similares.

P2 Explorer es un programa inteligente capaz de detectar automáticamente los formatos de la imagen. Tiene hash MD5 y verificación de suma de comprobación. Esta herramienta también es capaz de soportar scripts de shell para facilitar el montaje y desmontaje.

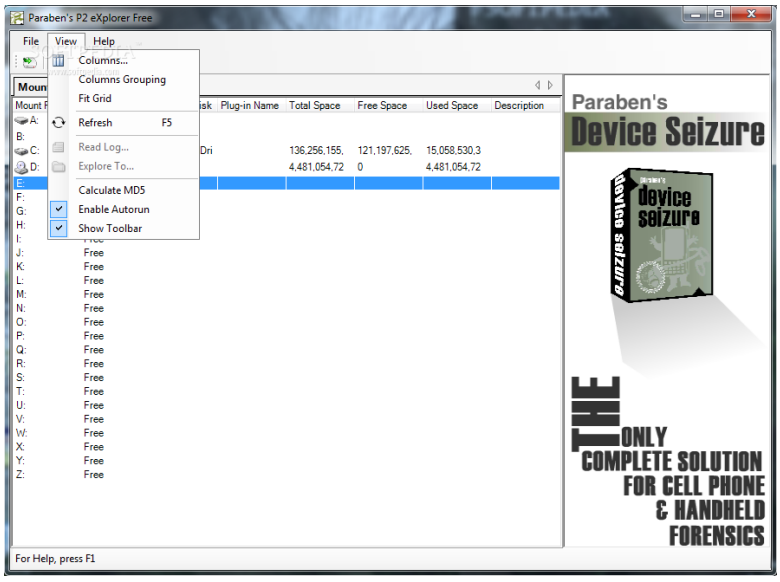


Foto descargada de http://www.softpedia.com/get/System/Hard-Disk-Utils/P2-eXplorer.shtml

Paraben P2 Explorer permite montar una imagen forense (o Linux DD, RAW, u otras imágenes de discos) y explorar como si se tratara de una unidad del equipo, mientras preserva, como un principio de la naturaleza del análisis forense, las evidencias. Esto significa que una imagen no sólo está montada para ver los archivos lógicos, se monta como la imagen real de flujo de bits, preservando sin asignar, holgura, y borrar datos.

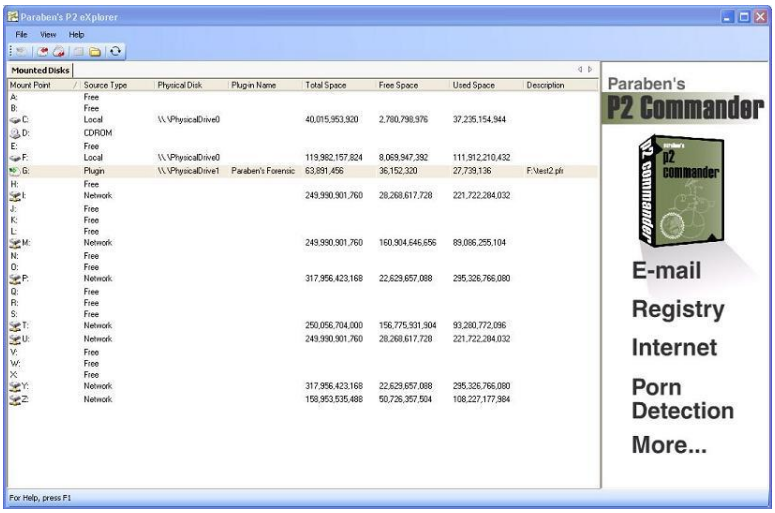


Foto descargada de http://www.suggestsoft.com/soft/paraben-corporation/p2-explorer/

CARACTERÍSTICAS:

- Montaje de imágenes Replicator Forenses (PFR).
- Monta, comprime y encripta imágenes PFR.
- Montaje de imágenes EnCase (E01).
- Montaje de imágenes SafeBack 1 y 2.
- Montaje de imágenes WinImage no comprimidas.
- Montaje de imagenes RAW, de Linux DD & otras herramientas.
- Soporta imágenes de discos dinámicos.
- Auto-detecta el formato de la imagen.
- Soporta imágenes tanto de tipos lógicos y físicos.
- La verificación de hash MD5.
- El apoyo de Shell para facilitar el montaje / desmontaje.
- Protección contra escritura para preservar la evidencia.
- Verificación de la suma de comprobación MD5.
- Soporta el montaje sobre una red.
- Montar varias imágenes a la vez.

Conclusiones: Es una herramienta para hacer análisis forenses sin tener que utilizar el material original y preserver las evidencias.

Crea imagines, lógicas o físicas, de los discos que se han de analizar para tener una copia exacta del dispositivo y no tener que realizer los análisis en el mismo dispositivo origen.

Read more here: https://www.paraben.com/p2-explorer.html

PlainSight

Desarrollador: PlainSight

Página de la herramienta: http://www.plainsight.info/

Tipo de Instalación: Iso para crear un CD/DVD donde se instala el entorno.

Tipo de Herramienta: Entorno informático

Uso: Uso general en el análisis forense debido a la forma en que ha sido diseñada. Permite incluir más opciones a las ya preinstaladas.

Descripción: PlainSight es un entorno de informática forense versátil que permite a los analistas forenses inexpertos realizar tareas comunes utilizando potentes herramientas de código abierto.

La herramienta ha tomado las mejores herramientas de código abierto forense y de seguridad, a medida, y los ha combinado con una interfaz de usuario intuitiva para crear un increíblemente potente entorno forense.

Foto descargada de http://www.plainsight.info/

Con PlainSight puede realizar operaciones tales como:

- Obtener información del disco duro y de las particiónes
- Extraer información de usuarios y grupos
- Ver el historial de la navegación por Internet
- Examinar la configuración del firewall de Windows
- Descubrir documentos recientes
- Recuperar más de 15 tipos diferentes de archivos
- Información de almacenamiento en dispositivos USB
- Examina volcados de memoria física
- Examina la información de UserAssist
- Extraer contraseñas de LanMan hash
- Vista previa de un sistema antes de adquirirlo

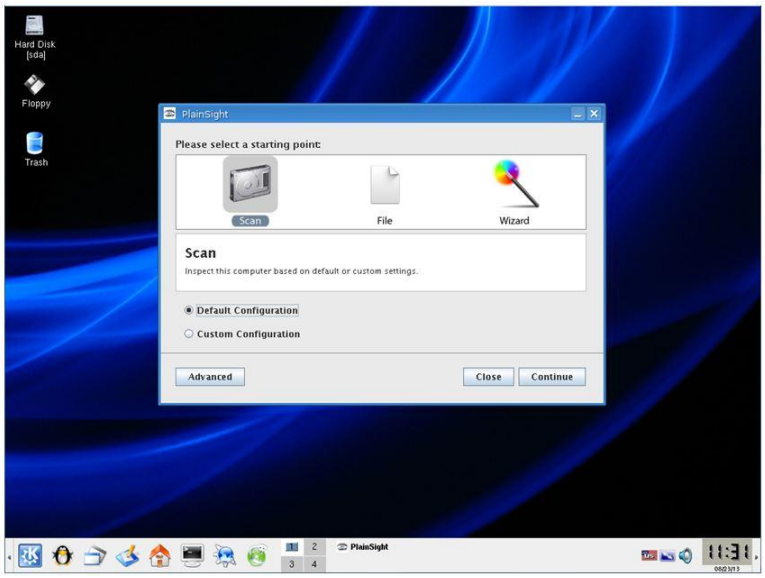


Foto descargada de http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

Para extraer información de dispositivos se utiliza:

- **hdparm** y disktype para ver detalles de discos duros y particiones.
- **RegRipper** para extraer información de USB desde el Registro.
- **RegRipper** para extraer información de clase de dispositivos desde el registro.

Para el Sistema operativo

- **RegRipper** para recuperar la versión actual del Registro de Windows.
- **RegRipper** para recuperar la versión nombre del equipo del registro.
- **RegRipper** para extraer información UserAssist del Registro.
- **RegRipper** para recuperar los últimos documentos del registro.
- **RegRipper** para extraer información de usuario y de grupos de Registro.
- **BKhive** y **Samdump2** para extraer contraseñas de XP / 2000 / NT a través de SAM y SYSKEY.

En red

- **RegRipper** para extraer la configuración el registro del firewall de Windows.

Historial de Internet

- **Pasco** para recuperar historias de Internet Explorer.
- **Mork** para recuperar historias FireFox / Netscape.
- **RegRipper** para ver URL escritas.

Volatile Memory Examination, utiliza el Framework Volatility para extraer la información a partir de muestras de memoria física como se detalla a continuación:

- Fecha y hora de la Imagen
- Ejecución de procesos
- Conectores de red abierta
- Conexiones de red abiertas
- DLL cargados por cada proceso
- Abrir archivos para cada proceso
- Abrir manejador del Registry para cada proceso
- Un proceso de memoria direccionable
- Módulos del kernel del sistema operativo
- Cartografía desplazamientos físicos a direcciones virtuales (cadenas a proceso)
- Información de Virtual Address Descriptor
- Ejemplos de escaneo: procesos, hilos, sockets, conexiones, módulos
- Transparentemente soporta una variedad de formatos de muestra (es decir, Crash dump, Hibernation, DD)

File Recovery / Carving se utiliza ante todo para recuperar los tipos de archivo. Incluyendo los siguientes:

- Jpg, png, gif, bmp, mpg, wav, avi, wmv, mov, pdf, htm, ole, zip, rar, exe

Sensitive Data Audit se utiliza Spider para escanear un sistema de datos sensibles.

Otra información

- Se ejecutar desde CD o USB.
- Guardar los resultados en HTML y / o texto plano.
- Ejecutar contra una imagen de disco o discos locales.

Conclusiones: Es un entorno de códogo abierto, en el que se han añadido otras herramientas, también open source, para crear un conjunto muy completo para realizar análisis forenses con garantias.

Al ser open source, permite la inclusión de todo tipo de herramientas para completer el conjunto. El entrono está compuesto por un conjunto de herramientas de gran calidad, con lo que forma un conjunto estable y de calidad.

Read more here: http://www.plainsight.info/index.html

XRY

Desarrollador: MSAB

Página de la herramienta: https://www.msab.com/products/office/

Tipo de Instalación: Es un todo-en-uno, o sea, herramienta que se compone de software y hardware. Se controla con un ordenador con Windows instalado.

Tipo de Herramienta: Herramienta para analizar dispositivos móviles, tablets, GPS, etc.

Uso: Se conecta a un ordenador con Windows instalado y se tiene disponible una herramienta bastante completa para analizar dispositivos móviles.

Descripción: **XRY** es una herramienta para análisis forense digital y análisis forense de dispositivos móviles, es un producto creado por la empresa sueca Micro Systemation, utilizada para analizar y recuperar información de dispositivos móviles, como teléfonos móviles, teléfonos inteligentes, herramientas de navegación GPS y tablet.

Consiste en un dispositivo hardware en el que conectar los teléfonos a un PC y el software para extraer los datos.

XRY está diseñado para recuperar el contenido de un dispositivo en un análisis forense, de manera que el contenido de los datos pueden ser invocadas por el usuario.

Normalmente se utiliza en investigaciones civiles/criminales, operaciones de inteligencia, el cumplimiento de los datos y de los casos de descubrimiento electrónico.

El software está disponible para las agencias policiales, militares y de inteligencia. Ha llegado a ser bien conocido en la comunidad forense digital como una de sus herramientas comunes para este tipo de trabajo.

Hay muchos desafíos más complejos al examinar los teléfonos móviles en comparación con el examen forense de los ordenadores normales. Muchos teléfonos móviles tienen sus propios sistemas operativos propietarios, lo que hace la ingeniería inversa de tales dispositivos una operación muy compleja.

Foto descargada de https://www.msab.com/products/office/

La extracción de datos de los teléfonos celulares es una habilidad especializada y no el mismo que la recuperación de datos de los equipos tradicionales. La mayoría de los dispositivos móviles no comparten los mismos sistemas operativos y dispositivos embebidos son propietarias que tienen configuraciones únicas. ¿Qué significa eso en términos de conseguir los datos fuera de ellos? Bueno, en términos simples, significa que es muy difícil de hacer.

XRY ha sido diseñado y desarrollado para hacer el proceso mucho más fácil, con el apoyo de miles de diferentes perfiles de dispositivos móviles y cientos de versiones de aplicaciones de teléfonos inteligentes.

La velocidad del mercado de dispositivos móviles también significa que hay muchos más nuevos dispositivos que se fabrican de forma regular, por lo que una herramienta de análisis forense móvil debe hacer frente a todas estas cuestiones antes de ser apto para la tarea.

El sistema XRY permite, exámenes lógicos (comunicación directa con el sistema operativo del dispositivo) y también exámenes físicos (sin pasar por el sistema operativo y dumping memoria disponible).

Mientras que la recuperación lógica de los datos es generalmente compatible en más dispositivos. El examen físico ofrece la posibilidad de recuperar la información suprimida, tales como mensajes de texto SMS, imágenes y registros de llamadas etc.

Las últimas versiones incluyen soporte para recuperar datos de aplicaciones de teléfonos inteligentes como el Android, iPhone y Blackberry. Los datos recuperados por XRY han sido utilizados con éxito en varios jucios de tribunales de todo el mundo. XRY ha sido probado por un número de diferentes organizaciones gubernamentales.

Foto descargada de http://www.esato.com/news/just-20-seconds-to-figure-out-the-iphone-digit-lock-code-or-android-2296

XRY, pronunciado "ex-arr-por qué", el software está diseñado para ejecutarse en un equipo con Windows y recuperar información de dispositivos móviles.

Permite la visualización inmediata de los resultados o guardarla en archivos que se pueden utilizar para su posterior análisis.

XRY viene como un paquete que contiene tanto el hardware como el software para leer la información del dispositivo.

XRY actualmente incluye el siguiente hardware en el paquete; Unidad XRY de Comunicaciones, lector de tarjetas SIM, Clone Tarjetas SIM, lector de tarjetas de memoria protegidas contra escritura y Juego completo de cables.

El hardware está conectado a un ordenador con Windows mediante un cable USB y es capaz de mostrar resultados inmediatos de la extracción del dispositivo.

El software se puede tomar la información del teléfono, SMS y otros mensajes de texto, MMS, listas de llamadas, entradas de calendario, elementos de tarea, imágenes, archivos multimedia, y la información de la tarjeta SIM.

XRY también recupera una gran cantidad de información sobre el teléfono en sí, como el IMEI / ESN, IMSI, modelo no., Igualando entre el reloj en el teléfono y el ordenador, etc.

La última versión incluye soporte para algunas aplicaciones de teléfonos inteligentes como Facebook, Myspace, Skype y Gmail.

El sistema genera un archivo cifrado llamado .XRY que contiene una copia de toda la información recuperada desde el teléfono.

La compañía también otorga licencias a los clientes para liberar y emitir su lector de archivos XRY, por lo que estos archivos cifrados seguros pueden ser leídos por terceros autorizados.

Foto descargada de http://www.esato.com/news/just-20-seconds-to-figure-out-the-iphone-digit-lock-code-or-android-2296

XRY permite la extracción de hasta 3 dispositivos móviles diferentes al mismo tiempo en el mismo equipo de una sola clave de licencia.

La herramienta es compatible con más de 5.000 perfiles de dispositivos móviles diferentes, incluyendo GSM, UMTS, CDMA y teléfonos iDEN. También se admiten diferentes tarjetas SIM y se admiten smartphones como Android, BlackBerry, iPhone, Symbian y Windows Mobile.

XRY es uno entre un número limitado de productos forenses móviles, que también ofrece capacidades de extracción física en los dispositivos para obtener acceso a, potencialmente, más información de un dispositivo, incluyendo datos eliminados.

XRY crea un informe que contiene el propio logotipo del usuario, dirección, etc., y la información requerida básica. El informe generado, o bien se puede imprimir, exportados en su totalidad o en parte, o transmitirlo electrónicamente con .XRY Reader, que se distribuye de forma gratuita.

Existe una función de búsqueda simplifica la tarea de la búsqueda de un nombre / número en particular o algún otro tipo de texto.

Algunas de las características únicas de XRY incluyen:

- Tres extracciones simultáneas a partir de 3 dispositivos móviles diferentes con una sola licencia
- El mayor apoyo a las aplicaciones de teléfonos inteligentes en el mercado
- Un archivo de registro forense completo para asegurarse de tener una pista de auditoría para el proceso de extracción
- Los tiempos de extracción más rápidos posibles para los dispositivos
- Formato de archivo seguro con construido en el cifrado para proteger los datos de origen

A continuación se describen las aplicaciones utilizadas para la parte lógica y física:

.- XRY Logical

Diseñado para realizar una extracción "lógica" de los datos desde el dispositivo móvil. Al comunicarse con el sistema operativo del dispositivo, se puede solicitar información al sistema. En términos generales esto le permitirá recuperar la mayor parte de los datos en tiempo real y el sistema de archivos del dispositivo y es un equivalente automatizado de examinar manualmente cada pantalla disponible en el dispositivo mismo y grabar lo que se muestra.

.- XRY Física

La solución más avanzada que le permite realizar una extracción "física" desde un dispositivo móvil, la recuperación de todos los datos en bruto disponibles. Normalmente, esto se realiza sin pasar por el sistema operativo y esto le ofrece la oportunidad de ir más profundo y recuperar datos borrados desde el dispositivo.

Una extracción física se separa en dos etapas distintas, el 'dump' inicial por lo que los datos en bruto se recuperan del dispositivo y luego de la segunda etapa de "decodificar" donde XRY puede reconstruir automáticamente los datos en algo significativo; tales como datos eliminados sin necesidad de talla manual. XRY física es particularmente útil cuando se enfrentan a los dispositivos con clave de seguridad.

.- XRY PinPoint

PinPoint es una solución dedicada a dispositivos móviles no estándar, a veces se refiere como China Chipsets o teléfonos Clon. Es una solución avanzada compuesta de hardware compacto y potente software. Totalmente integrado con XRY para permitir a los usuarios extraer y decodificar datos desde móviles donde el pin-out varia y puede incluso no ser conocido. PinPoint es capaz de detectar automáticamente la configuración de pines de salida, con el fin de comunicarse con el dispositivo móvil. El soporte adicional para la extracción física de los dispositivos no estándar está activado tras la activación del módulo PinPoint.

.- XRY Visor

XRY Viewer es una herramienta fácil de usar para la visualización de archivos XRY. Diseñado específicamente para ver archivos.xry, en su formato de archivo nativo, es una aplicación muy ligera sin dependencias de instalación. Esto significa que es ideal para distribuir archivos XRY y permitir la visualización de todos los datos extraídos de un dispositivo móvil.

Visor permite, a los usuarios no entrenados, acceso inmediato a los datos en una pantalla simple y fácil de entender. Se ejecuta en modernos dispositivos con sistema operativo de Windows, sin necesidad de ninguna autoridad administrativa para pre-instalar componentes en el ordenador.

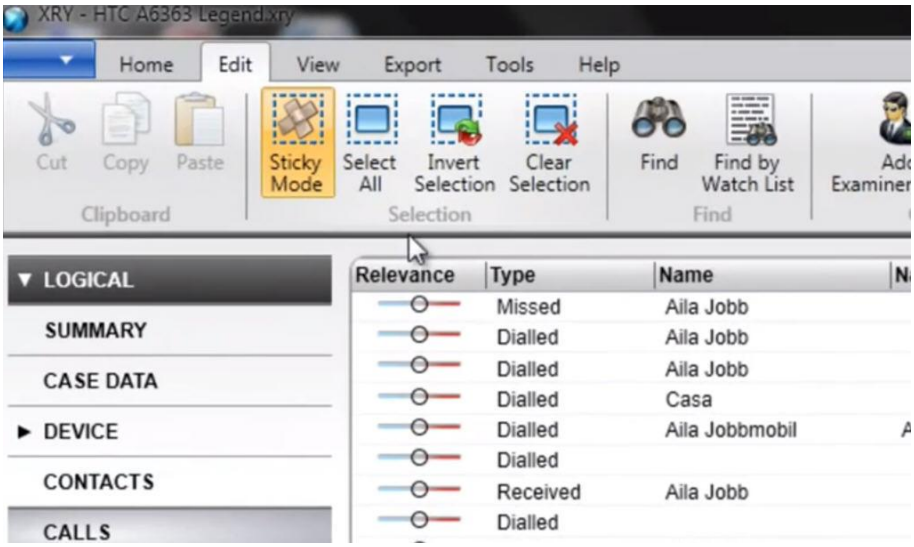


Foto descargada de http://micro-systemation-xry-forensic-pack.software.informer.com/screenshot/306745/

Visor es ideal para grabar en disco o memoria USB junto con los archivos generados por XRY y luego proporcionar dicha información a terceras partes que no son usuarios habituales XRY. Los usuarios también pueden seleccionar diferentes categorías de archivos de forma simultánea en una vista combinada y luego ordenar todos los datos de una variedad de categorías para ayudar a localizar la información más rápido que nunca.

XRY Office es un sistema forense móvil todo-en-uno. La combinación de ambas soluciones lógicas y físicas en un solo paquete, permite a los investigadores el acceso completo a todos los métodos posibles para recuperar los datos desde un dispositivo móvil.

XRY es una solución basada en software especialmente diseñado, con todo el hardware necesario, para la recuperación de datos de los dispositivos móviles de manera segura. Con XRY Office se puede lograr y profundizar más en un dispositivo móvil para recuperar datos vitales. Con una combinación de herramientas de análisis lógicos y físicos disponibles para los dispositivos compatibles; XRY Office puede producir un informe combinado que contiene datos tanto en vivo como borrados del mismo teléfono.

El sistema XRY es una de las primeras opciónes entre los organismos encargados de hacer cumplir la ley en todo el mundo, y representa un sistema forense móvil completo, se suministra con todo el equipamiento necesario que necesita para llevar a cabo un examen forense de un dispositivo móvil.

Conclusiones: Es un todo-en-uno, que contiene tanto software como hardware, para hacer análisis de dispositivos móviles.

Es compatible con la mayoria de los dispositivos móviles del Mercado, y al ser una opción de pago, está muy actualizada.

Permite el análisis de los dispositivos móviles tanto de forma lógica como física, permitiendo un análisis más exaustivo del dispositivo, desde el acceso a archivos y

acceso al Sistema operativo como a los datos que han sido eliminados accediendo a ellos de forma física.

Read more about it: http://www.msab.com/xry/what-is-xry

HELIX3

Desarrollador: e-fense Carpe Datum

Página de la herramienta: http://www.e-fense.com/h3-enterprise.php

Tipo de Instalación: Ejecutable, para instalar en el sistema operativo.

Tipo de Herramienta: Herramienta para la monitorización de redes, se suele utilizar para analizar y controlar posibles ataques desde Internet.

Uso: Aplicación con intefaz de usuario, que permite controlar el trafico a través de redes, como Internet. Su interfaz sencilla permite controlar de forma intuitiva las opciones disponibles, que van desde el escaneo hasta la creación de informes completos.

Descripción: Helix3 Enterprise es una solución, fácil de usar, de ciberseguridad integrado en la red, que da visibilidad a través de toda su infraestructura revelando actividades maliciosas como el abuso de Internet, intercambio de datos y el acoso. H3E también permite aislar y responder a los incidentes o amenazas de forma rápida y sin detección del usuario a través de una herramienta de administración central.

Helix3 Enterprise le permite detectar rápidamente, identificar, analizar, preservar y crear un informe que muestra las evidencias que revelan lo sucedido y ayudan a proteger su negocio.

Características de Helix3 Enterprise:

.- Fácil de usar, Helix3 Enterprise se controla a través de una interfaz gráfica fácil de usar, que funciona con cualquier sistema operativo. Es tan fácil de usar que apenas requiere un mínimo entrenamiento.

Foto descargada de http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

.- Implementación rápida, la instalación se realiza de forma rápida y puede ser descargado a través de la red mediante sus herramientas de instalación existentes.

.- Revisa la navegación a través de Internet, revisa el historial de uso de Internet de una forma rápida, al monitorizar las búsquedas y lo que los sitios que se visitan.

.- Capturas de pantalla y del registro de Keys, Con un simple clic se puede realizar una captura de pantalla o logging key en cualquier sistema dentro de su red. Con solo seleccionar el sistema que se desea supervisar y elegir la captura de pantalla en el menú se obtiene una captura de lo que está en la pantalla del sistema en un momento dado.

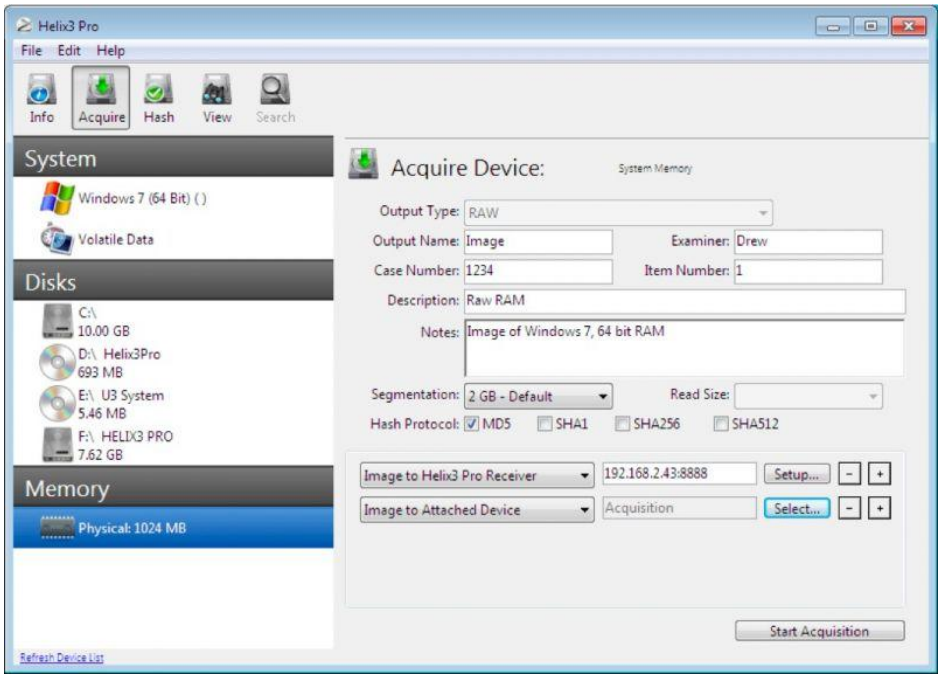


Foto descargada de https://www.e-fense.com/store/index.php?_a=viewProd&productId=6

.- e-Discovery, con Helix3 Enterprise puede buscar en toda la red cualquier archivos con tres métodos diferentes:

1. Fecha y hora
2. Palabras claves en nombres de archivo, el contenido del archivo y expresiones regulares
3. Valores hash - un método más en informática forense

El aumento de la legislación, especialmente la ley de Protección de Datos está causando problemas a las empresas cuando se monitoriza el flujo de una red. La solución de Helix3 Entreprise simplifica los problemas al permitir que el personal de seguridad de la información pueda realizar la búsqueda con criterios de datos definidos, y, o bien copiar los datos en una ubicación central o informe sobre su presencia.

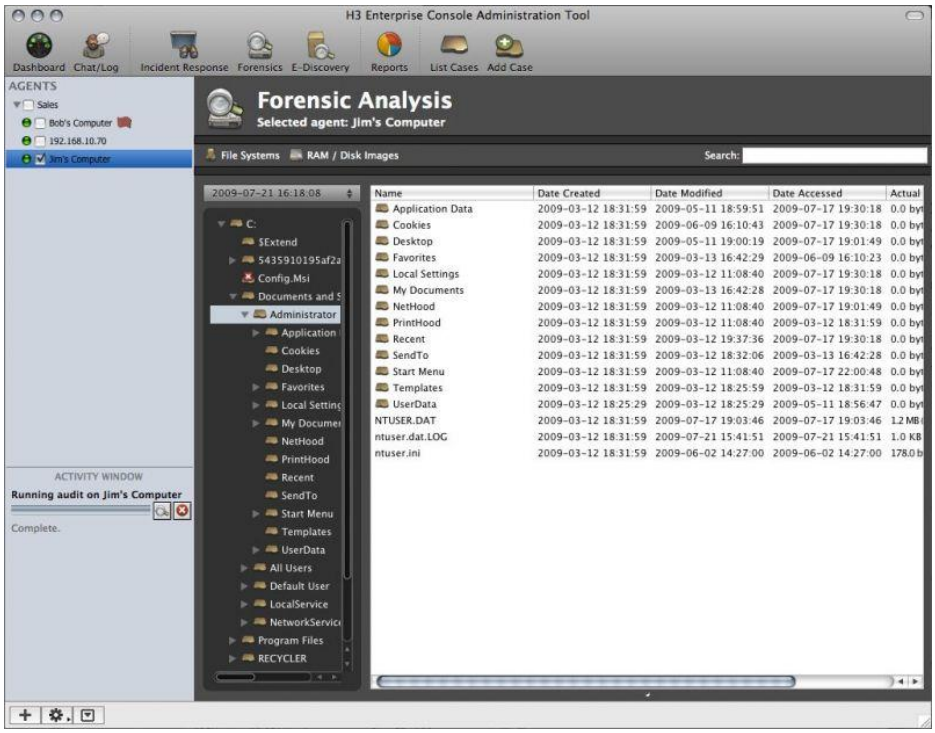


Foto descargada de https://www.e-fense.com/store/index.php?_a=viewProd&productId=5

Sofisticadas capacidades informáticas forenses, Helix3 Enterprise fue desarrollado por expertos en informática forense y investigadores de delitos cibernéticos.

Recoge imágenes forenses de sistemas, incluyendo la memoria RAM a través de múltiples plataformas, procesos en ejecución, las variables de entorno y mucho más.

.- Informes, el reporting es una parte importante de cualquier aplicación de software, el software de seguridad de red no es diferente. Puede crear informes concisos sobre las auditorías realizadas y los informes de ejecución Ad-hoc basado en criterios muy diversos.

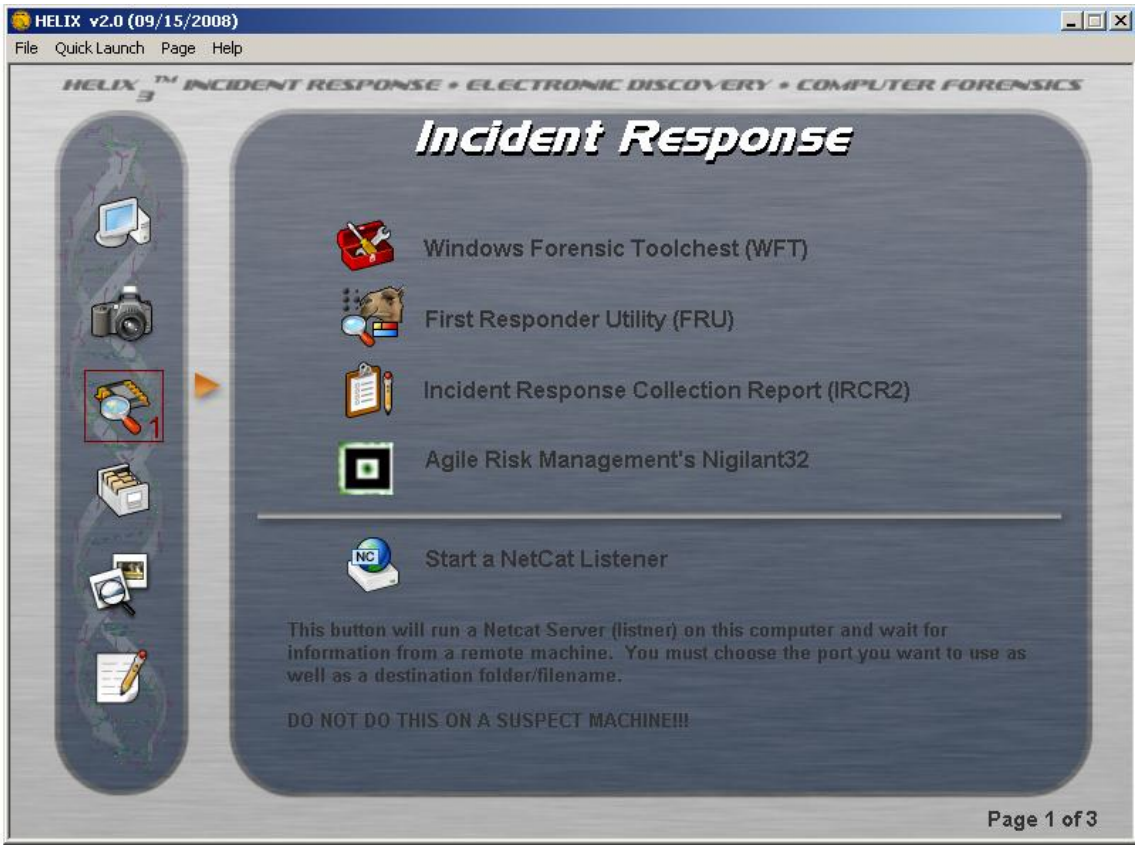


Foto descargada de https://www.404techsupport.com/2009/03/helix-computer-security-forensics/

.- Compliance Management, la implementación de software y procedimientos de seguridad de la red proporcionan a las empresas los medios para satisfacer los requisitos de cumplimiento.

.- Seguridad cibernética, la Seguridad Cibernética ha sido de gran interés en los últimos años a medida que más computadoras con datos sensibles o de propiedad están conectados a Internet y la ciberdelincuencia va en aumento. Hay muchas normas y buenas prácticas como se indica en la norma ISO/IEC, COBIT, normas de buenas prácticas de ITIL y que abogan por la importancia de fuertes soluciones de seguridad de red.

Protección del comportamiento malicioso del Empleado,

- Sólo el 20% de la pérdida de datos se debe a la piratería
- El 80% de la pérdida de datos es debido a las amenazas internas, incluyendo acciones de los empleados
- El incidente medio debido a la piratería puede costar $67.000 (Fte. Deloitte)
- El promedio de pérdidas debido a la violación de la seguridad interna es $2.300.000 (Fte. Deloitte)
- Las multas gubernamentales asociadas con la falta de seguridad tienden a estar en el rango "de siete cifras".

- LOS DATOS DE SEGURIDAD NO SON UNA OPCIÓN PARA PENSAR en una fecha posterior

Foto descargada de https://www.e-fense.com/store/index.php?_a=viewProd&productId=5

.- Apoyo de Litigios, en el mundo de hoy cada vez se producen más litigios. Las empresas se encuentran en el medio de la acción legal y deben ser capaces de tener los datos disponibles de forma rápida, por lo general en almacenamiento digital.

Investigaciones como la mala conducta del empleado requieren de e-Discovery y de la computación forense, con el fin de tener éxito. Estos requisitos ponen presión sobre los equipos de seguridad de IT. Con Helix3 Enterprise dando respuesta a los incidentes y con e-discovery mostrando correctamente los resultados de las evidencias.

.- Los equipos de seguridad de la información pueden gestionar responsabilidades legales desde una ubicación central utilizando H3E para garantizar la integridad de los datos informático forense. Los equipos de la empresa pueden ser examinados, crear imágenes de los discos duros para el examen forense y la vigilancia necesaria realizadas desde una herramienta en la administración central.

.- Red de Monitoreo Inteligente, El personal de seguridad puede monitorizar cada ordenador o servidor en la red desde una herramienta de administración central cuando se instala un agente lite. El agente permite desde la consola conectarse a ella mediante la autenticación cifrada y proporciona al operador la capacidad de recopilar evidencias volátiles, capturas de pantalla, pulsaciones de teclas, utilización de la memoria RAM – incluso de todo el disco duro. El agente también proporciona

habilidades para controlar el equipo para la actividad anómala que se puede establecer por el operador.

Conclusiones: Útil herramienta para controlar el tráfico de redes, fácil de usar y completa, gracias a sus opciones disponibles.

Permite monitorizar redes, como Internet, para controlar el acceso y la navegación por una red, controlando todo el tráfico o parte, con los filtros que se pueden utilizar para discriminar cierta información.

Se pueden crear informes con los resultados, que debido a la información disponible se pueden utilizar en juicios.

Helix3 2008R1 can be downloaded here: https://e-fenseinc.sharefile.com/d/sda4309a624d48b88

The enterprise version is available here: http://www.e-fense.com/h3-enterprise.php

ProDiscover Basic

Desarrollador: ARC Group

Página de la herramienta: http://www.arcgroupny.com/products/prodiscover-basic/

Tipo de Instalación: La utilidad se instala desde un archivo descargado, que instala el programa ProDiscover así como ActivePerl para los scripting forenses. El archivo de licencia se copia en el directorio del programa y la instalación se realiza de forma automática.

Tipo de Herramienta: Herramienta que permite a los profesionales de la informática localizar todos los datos en un disco duro y al mismo tiempo proteger la evidencia y crear informes de pruebas de calidad para su uso en un procedimiento judicial.

Uso: Detectar y localizar datos en disco y crear informes completos para poder gestionar los datos análizados.

Descripción: Solución de próxima generación, del Grupo ARC, al crimen cibernético está respaldado por un empresa líder en la industria, ProDiscover®.

Las características de vanguardia en la última versión del ProDiscover edición Forensics exceden los estándares de la industria para la informática forense proactiva.

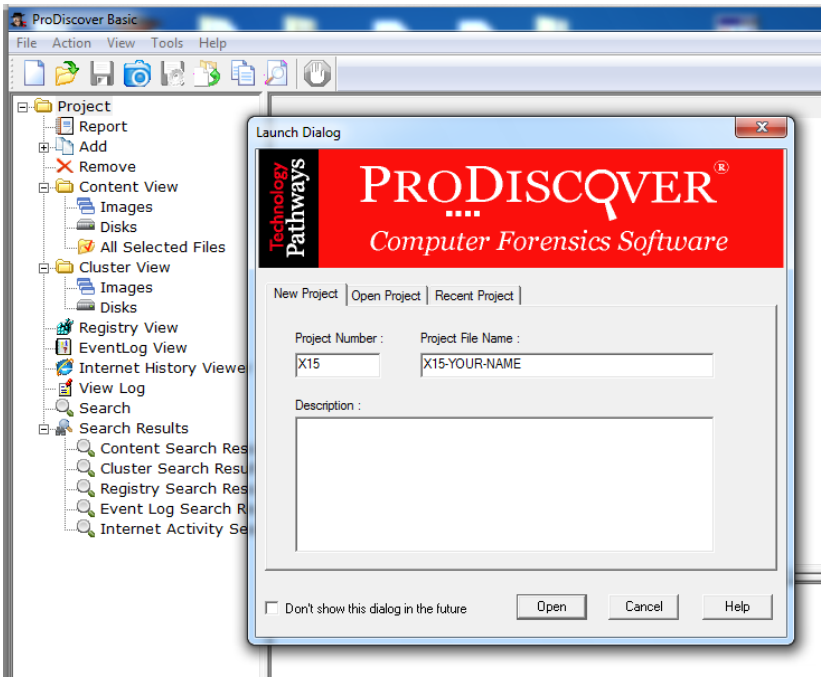


Foto descargada de https://samsclass.info/121/proj/pX15-121-Carving.html

ProDiscover Forensics es una potente herramienta de seguridad informática que permite a los profesionales de la informática localizar todos los datos en un disco duro y al mismo tiempo proteger la evidencia y crear informes de pruebas de calidad para su uso en un procedimiento judicial.

Mediante el uso de las mejores prácticas de la industria y un enfoque de la metodología menos destructiva, ProDiscover Forensics permite el examen de los archivos sin alterar metadatos valiosos, como la última vez visitada.

ProDiscover Forensics puede recuperar archivos borrados, examina el espacio desperdiciado, acceso de Windows Alternate Data Streams, y permitir dinámicamente una vista previa, la búsqueda y captura de imágenes del Hardware Área Protegida (HPA) del disco que utiliza su propia tecnología pionera. No es posible ocultar los datos a ProDiscover Forensics porque lee el disco a nivel sectorial.

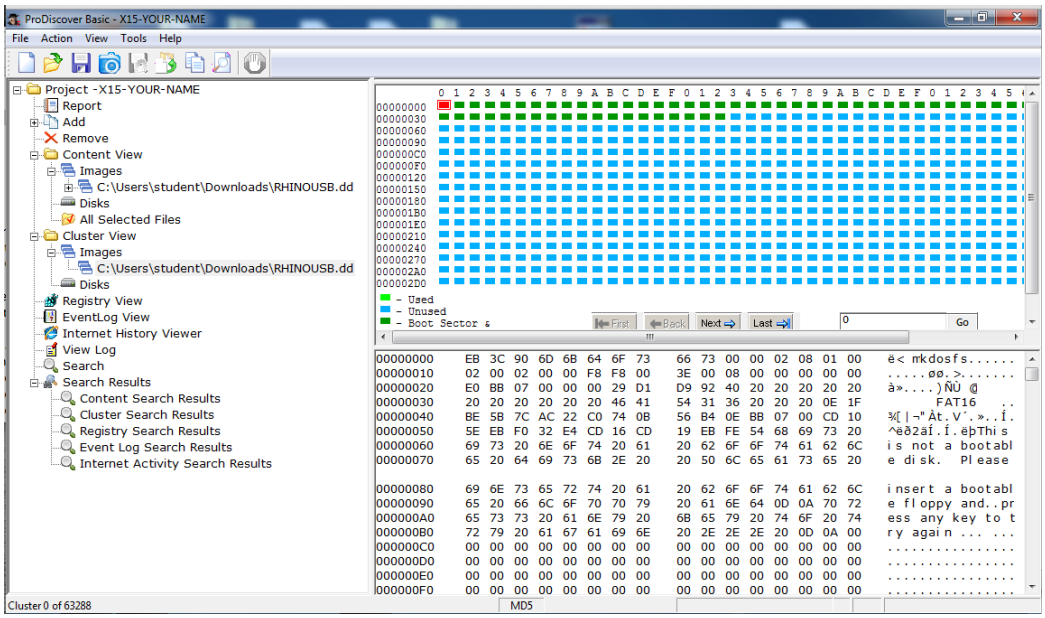


Foto descargada de https://samsclass.info/121/proj/pX15-121-Carving.html

ProDiscover Forensics permite una búsqueda a través de todo el disco para las palabras clave, expresiones regulares, y frases con capacidad completa de búsqueda de Boole para encontrar los datos necesarios.

Capacidad de comparación hash que se puede utilizar para encontrar archivos ilegales conocidos o para eliminar archivos conocidos buenos, como archivos del sistema operativo estándar, mediante la utilización de la base de datos Hashkeeper incluido desde el National Drug Intelligence Center.

La poderosa capacidad de búsqueda de ProDiscover Forensics es rápida y flexible, lo que permite una búsqueda de palabras o frases en cualquier lugar del disco, incluyendo el espacio desperdiciado.

La amplia capacidad de ayuda en línea y una interfaz fácil de usar, interfaz gráfica de usuario, hacen que el proceso de aprendizaje de ProDiscover Forensics sea simple y fácil.

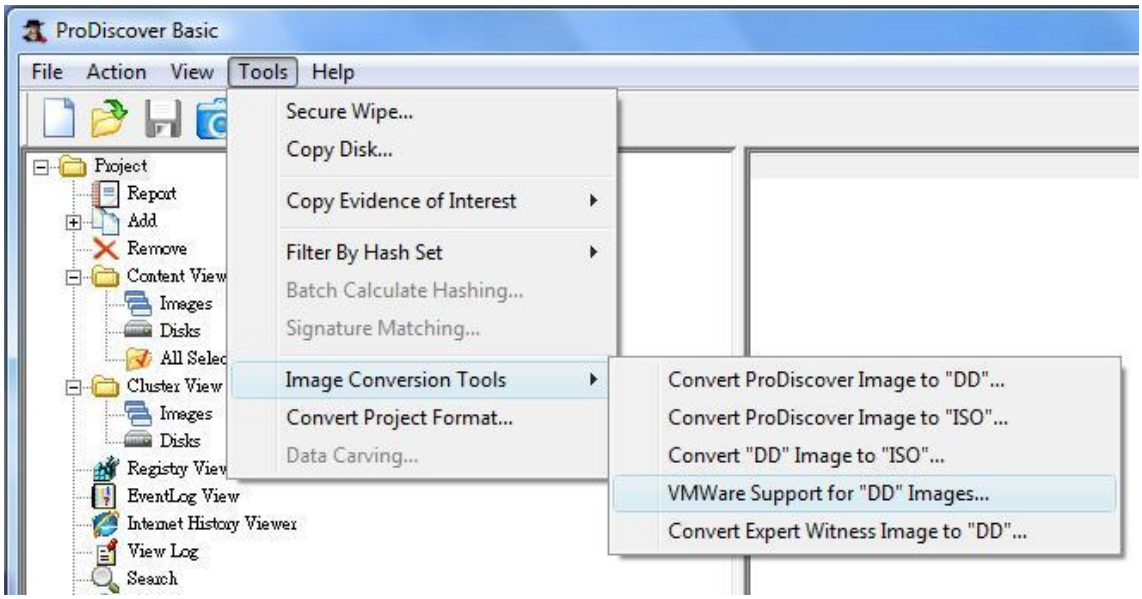


Foto descargada de https://irhowto.wordpress.com/tag/prodiscover/

ProDiscover Forensics se puede utilizar para un mejor análisis de todo un sistema. Incluye utilidades para ver el registro, registro de eventos y la actividad de Internet de una imagen capturada. Tiene todo lo necesario para el análisis forense, incluye una interfaz limpia, que se asemeja al Explorador de Windows.

ProDiscover permite secuencias de comandos utilizando Perl. Los scripts pueden ser útiles para automatizar tareas que se realizan de forma rutinaria como parte de una investigación forense.

El producto es rico en características, pero los espectadores internos - a diferencia de la carga de las aplicaciones – te proporcionan un ahorro importante de tiempo.

La utilidad ProDiscover necesita, en torno, a tres minutos para crear una imagen forense de una unidad de un GB. Importar el archivo de imagen en ProDiscover es muy rápido. ProDiscover recupera archivos borrados, incluyendo algunos archivos que fueron supuestamente borrados mediante un programa de limpieza de conocidos fabricantes.

ProDiscover encontra muchos ejecutables borrados, directorios borrados y archivos de imágenes eliminadas. Los archivos protegidos con contraseña serían abiertos simplemente haciendo doble clic sobre el archivo para abrirlo. ProDiscover también detecta la presencia de cualquier archivo steganographed. Con los archivos de imagenes crea una vista previa de ellos.

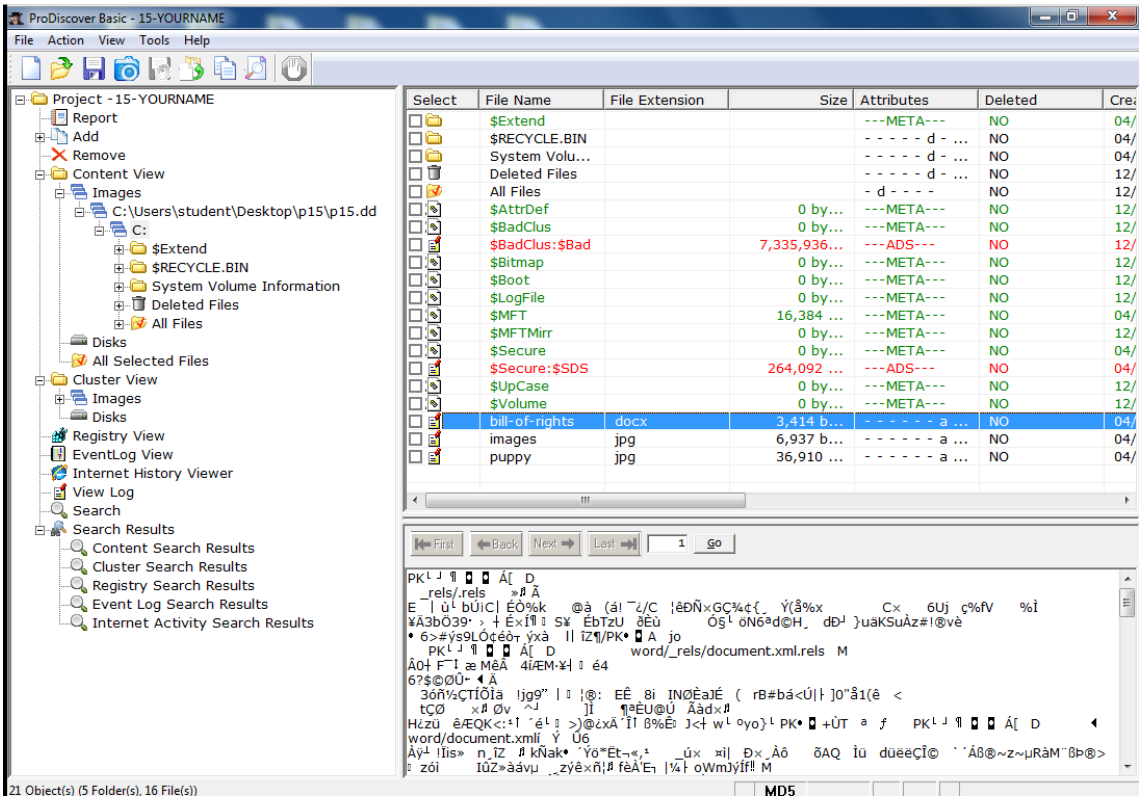


Foto descargada de https://samsclass.info/121/proj/p15-pd-install.htm

ProDiscover está diseñado para leer una imagen de un disco de sistema y no archivos individuales como entradas.

El archivo de ayuda para ProDiscover es superior a la media y cubre la mayor parte del uso común del producto. La lectura de las primeras secciones proporcionan los conocimientos necesarios para realizar tareas básicas con el sistema.

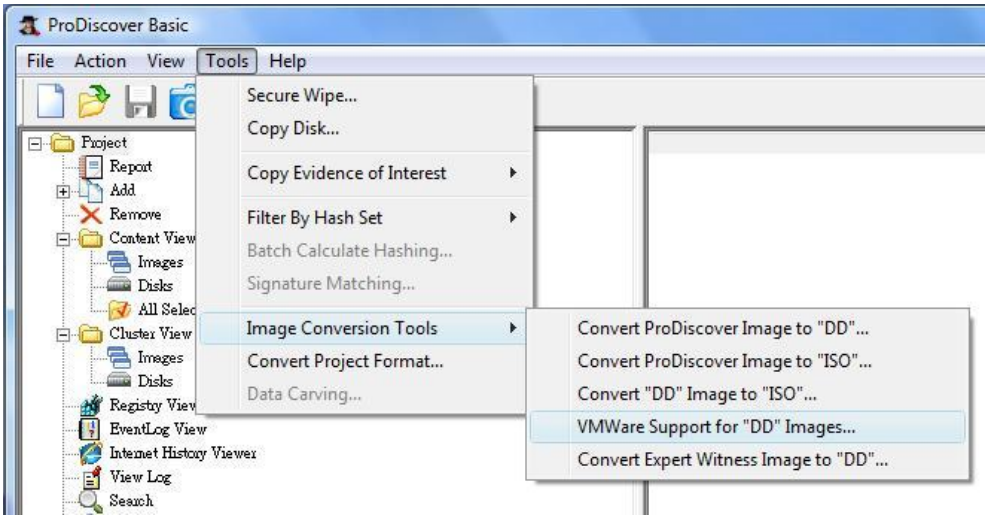


Foto descargada de https://irhowto.wordpress.com/2010/07/05/booting-a-dd-image-with-vmware/

Conclusiones: Una herramienta de pago, que puede pagar su uso debido a su alto coste, con buenas características y que realiza las funciones para las que se creo de una manera correcta.

Tiene buenas opciones y crea informes de calidad, pero sería una segunda opción ya que existen herramientas open source que realizan sus funciones de manera más que correcta y aunque es una opción a tomar en cuenta, ya que destaca en algunas de sus funciones, su precio puede echar para atrás a más de un analista.

FTK

Desarrollador: AccessData

Página de la herramienta: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

Tipo de Instalación: Descarga de una ISO para instalar todo el conjunto de herramientas en un CD/DVD o en un ordenador.

Tipo de Herramienta: Se utilizar para la creación de imágenes, búsqueda de datos en un dispositivo, monitorización de transvase de información a través de redes, etc. Una completa solución que te permite realizar un análisis desde la creación de una imagen de un dispositivo hasta la búsqueda de pruebas, en una amplia variedad de entronos, ordenadores, móviles, redes, etc.

Uso: Se utiliza desde el inicio del análisis, pudiendo crear una imagen, hasta el final del análisis, creando informes bastante completos.

Foto descargada de http://forensicstore.com/product/access-data/forensic-toolkit-5/

Su uso, teniendo en cuenta que es una herramienta de pago, es variado y permite realizar las funciones para las que se creo con soltura. Sus principales características son la velocidad y facilidad de uso.

Descripción: FTK es una plataforma de investigaciones digitales, construido en base a la velocidad, estabilidad y facilidad de uso.

Proporciona procesamiento integral y la indexación por adelantado, por lo que el filtrado y la búsqueda es más rápida que con cualquier otro producto. Esto significa que puede encontrar las pruebas pertinentes con rapidez, lo que aumenta considerablemente su velocidad de análisis.

Por otra parte, debido a su arquitectura, FTK se puede configurar para el procesamiento distribuido e incorporar el manejo de casos basado en la web y el análisis colaborativo.

Visualice Big Data, Encuentra las pruebas pertinentes rápido

La base de datos impulsada de FTK, la arquitectura de clase empresarial le permite manejar grandes conjuntos de datos, ya que proporciona velocidades de procesamiento y estabilidad, que no son posibles con otras herramientas.

Proporciona una función de visualización de datos y la tecnología de detección de imágenes explícitas, permite discernir y reportar el material más relevante en su investigación rápidamente.

La interoperabilidad de FTK con las soluciones de todos los AccessData, le permite correlacionar los conjuntos de datos masivos de diferentes fuentes, como por ejemplo, discos duros de ordenador, dispositivos móviles, datos de red de almacenamiento de Internet y más. Esta capacidad hace de FTK la única solución de investigación digital capaz de reducir los tiempos de casos de investigación por lo que le permite revisar los datos e identificar las pruebas pertinentes, todo en una ubicación centralizada.

Automatización del filtrado y análisis de malware

Disponible como un add-on para FTK, Cerberus le permite determinar el comportamiento y la intención de binarios sospechosos, dándole inteligencia procesable sin tener que esperar a que el equipo de malware realice el análisis de consumo más en profundidad. Esta clasificación de malware automatizado y análisis le permite:

- Ganancia de inteligencia procesable en segundos, permite validar las amenazas y tomar medidas decisivas.

- Lograr la detección de malware con los análisis de amenazas proactivos.

Soluciones de descifrado de AccessData

AccessData ha desarrollado otras soluciones líderes en la industria para ayudar en la recuperación de las contraseñas. Estas soluciones se utilizan en muchos entornos diferentes para proporcionar, funciones específicas relacionadas con agrietamiento de contraseñas. Profesionales Policiales y de seguridad corporativa que realizan las

investigaciones forenses informáticas, utilizan estas soluciones para acceder a los archivos protegidos por contraseña.

Del mismo modo, los administradores también pueden utilizar estas soluciones para recuperar contraseñas de sistema, contraseñas personales perdídas y más.

AccessData Password Recovery Toolkit (PRTK) y Distributed Network Attack (DNA) proporcionan acceso a las contraseñas de un gran número de aplicaciones de software populares. PRTK se ejecuta en una sola máquina. ADN utiliza varias máquinas a través de la red o en todo el mundo para llevar a cabo el espacio clave y los ataques de diccionario.

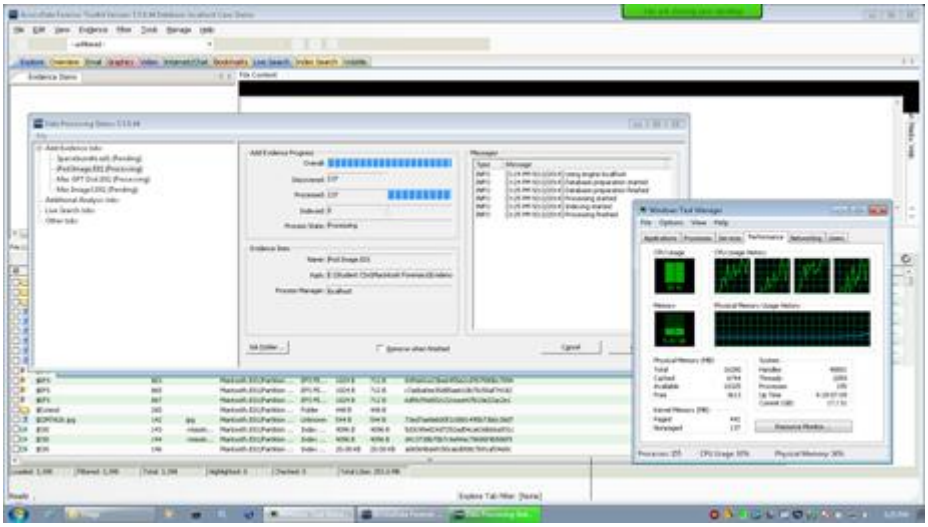


Foto descargada de http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/capabilities

Los siguientes complementos están disponibles para mejorar la potencia y velocidad de craqueo de las contraseñas con PRTK y / o ADN.

Rainbow (hash) Tables

Las Rainbow Tables son pre-computados, ataques de fuerza bruta. En criptografía, un ataque de fuerza bruta es un intento de recuperar una clave criptográfica o la contraseña intentando en cada combinación de teclas las posibles convinaciones hasta encontrar la correcta. La rapidez con que esto se puede hacer depende del tamaño de la clave, y los recursos de computación aplicada.

Un sistema fijado en el cifrado de 40 bits, tiene un billón de teclas disponibles. Un ataque de fuerza bruta de 500.000 claves por segundo tomaría aproximadamente 25 días para agotar las combinaciones espaciales claves utilizando un simple ordenador Pentium 4 a 3 GHz, con un Rainbow Tables, porque todas las claves posibles en el espacio de claves de 40 bits ya están calculados, claves de archivos que se encuentran en cuestión de segundos-a-minuto; mucho más rápido que con otros medios. ADN y PRTK se integran a la perfección con Rainbow Tables.

Portable Office Rainbow Tables (PORT)

AccessData Portable Office Rainbow Tables (PORT) es completamente diferente de las tablas hash establecidas. Un análisis estadístico se realiza en el propio archivo para

determinar las teclas disponibles. Esto toma mucho menos espacio que las tablas hash, pero también lleva algo más tiempo y cuesta un pequeño porcentaje en la precisión.

FTK aprovecha las capacidades de procesamiento multi-máquina, reduciendo los tiempos de procesamiento de casos más del 400% frente a otras herramientas disponibles, reduciendo acumulación de procesos pendientes de manera significativa; se realiza por procesamiento integral adelantado, aumentando considerablemente la velocidad, con lo que un analista puede centrarse en la investigación real.

FTK Imager de AccessData, es una herramienta para realizar réplicas y visualización previa de datos, la cual permite una evaluación rápida de la evidencia electrónica para determinar si se garantiza un análisis posterior con una herramienta forense como AccessData Forensic Toolkit. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de ordenadores sin realizar cambios en la evidencia original.

Es importante mencionar el uso de un bloqueador de escritura al utilizar FTK Imager para crear la imagen forense desde un disco duro u otro dispositivo electrónico. Esto asegura que el sistema operativo no alterará la unidad fuente original.

Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realiza una imagen bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacios desperdicados o residuales y el espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense.

Solución forense digital integrada

La herramienta permite crear imágenes, procesar una amplia gama de tipos de datos de muchas fuentes, desde datos del disco duro a los dispositivos móviles, los datos de red y de almacenamiento de Internet en una ubicación centralizada. Descifrar archivos, descifrar contraseñas, y construir un informe de todos con una única solución.

- Recupera las contraseñas de más de 100 aplicaciones
- Biblioteca hash KFF con 45 millones de hashes
- Análisis automatizado sin scripting

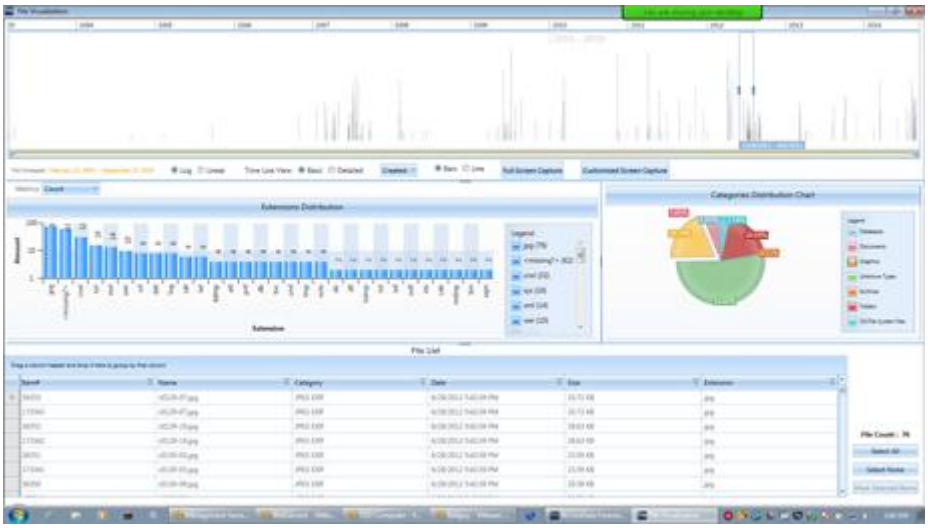


Foto descargada de http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/capabilities

La arquitectura única FTK proporciona estabilidad

FTK es impulsado, por lo que no experimentará la pérdida de trabajo asociado con herramientas basadas en memoria en el caso de un accidente en GUI o en base de datos.

Los componentes FTK están compartimentados permitiendo que los trabajadores de procesamiento puedan continuar el procesamiento de datos sin interrupción.

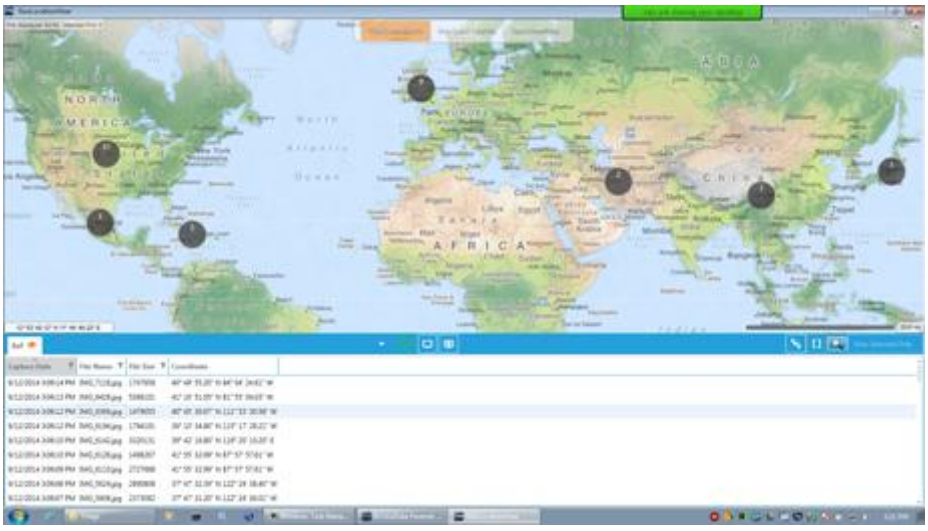


Foto descargada de http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/capabilities

Procesamiento Incomparable

- Procesamiento distribuido con un total de 4 motores
- Verdadero soporte multi-core/multi-hilo
- Procesamiento basado en asistente, garantiza que ningún dato se pierde
- Refinamiento pre y post-procesamiento

- Motor de avanzada filtrado de datos le permite especificar criterios, como el tamaño del archivo, tipo de datos y tamaño de píxel para reducir la cantidad de datos irrelevantes filtrados al tiempo que aumenta la minuciosidad general
- Crear perfiles de procesamiento reutilizables, de importación y exportación, con opciones predefinidas de procesamiento para las diferentes necesidades de investigación

Conclusiones: Entorno de análisis forense digital, rápido y fácil de usar, que cumple con las expectativas, debido a su posible uso en casi todo el recorrido del análisis forense, empezando en la creación de una imagen, y su protección de las evidencias gracias a su protección contra escritura en ella, pasando por el análisis de los datos recogidos y las finalización del recorrido creando informes con los resultados.

Permite la monitorización de redes para el análisis de posibles evidencias y la recopilación de datos de dispositivos móviles.

Una opción a tomar en cuenta, siempre teniendo en cuenta que es una herramienta de paga y se tendría que sopesar el costa y compararlo con las ventajas sobre otras herramientas open source similares.

Comando Linux "dd"

Desarrollador: Open Source, viene integrada en Linux

Página de la herramienta: No tiene, porque es una herramienta incluida en todas las versiones de Linux.

Tipo de Instalación: En cualquier instalación de Linux viene incluida, por lo que no se tiene que realizar una instalación a parte.

Tipo de Herramienta: Creación de imágenes de discos.

Uso: Se utiliza para la creación de Backups e imágenes de disco.

Descripción: **dd** es un comando de la familia de los sistemas operativos Unix que permite copiar y convertir datos de archivos a bajo nivel.

Es generalmente usado para realizar operaciones avanzadas sobre dispositivos o archivos, como pueden ser:

- Transferencias de datos específicos.
- Copias de seguridad de la información «en crudo» (*raw data*).
- Conversión de algunas codificaciones soportadas y/o caracteres predefinidos.

Es importante señalar que, en sistemas operativos Unix, cualquier dispositivo se trata y gestiona como un archivo. Por tanto, el comando dd puede ser utilizado con diversos dispositivos y volúmenes (particiones), más allá de los archivos propiamente dichos.

Según la especificación POSIX, dd copia el archivo indicado como origen en el archivo indicado como destino, teniendo en cuenta la conversión de los datos y el tamaño de bloque requerido. Si no se hubiera especificado el origen o el destino, dd por defecto utilizaría la entrada o la salida estándar, respectivamente, para llevar a cabo la operación.

Si se ha especificado el tamaño de bloque a transferir (mediante el parámetro bs) y no se ha indicado conversión alguna salvo noerror, notrunc o sync, se procede a la lectura, bloque por bloque, del archivo origen, y a su correspondiente escritura en el destino. El tamaño del bloque a escribir es idéntico al del bloque leído, salvo que se indique la conversión sync, en cuyo caso se procede a rellenar con ceros el bloque de destino. Si no se utiliza sync, el último bloque escrito puede ser de tamaño inferior al resto.

Por último, en caso de que no se haya especificado un tamaño de bloque, dd usa 512 bytes como tamaño por defecto.

La invocación del comando dd tiene el siguiente formato:

dd [PARÁMETRO] ...

Los principales parámetros son:

if=origen

Lee desde el archivo indicado como origen. Por defecto lee de la entrada estándar.

of=destino

Escribe al archivo indicado como destino. Por defecto escribe en la salida estándar.

ibs=N

Lee N bytes del archivo origen.

obs=N

Escribe N bytes en el archivo destino.

bs=N

Lee y escribe N bytes. Alternativa a usar ibs y obs con un mismo valor.

cbs=N

Establece en N bytes al tamaño del bloque de conversión para block y unblock.

skip=N

Se salta N bloques del archivo origen antes realizar la operación de copiado. El tamaño del bloque es indicado por ibs.

seek=N

Se salta N bloques del archivo destino antes realizar la operación de copiado. El tamaño del bloque es indicado por obs.

count=N

Copia N bloques del archivo origen, en vez de procesar hasta el final. El tamaño del bloque es indicado por ibs.

conv=modo[, modo,...]

Realiza las operaciones de conversión, según se indique. Se puede indicar más de una conversión, separándolas por comas.

Conversiones soportadas:

ascii

Convierte los caracteres EBCDIC a ASCII.

ebcdic

Convierte los caracteres ASCII a EBCDIC.

ibm

Convierte los caracteres ASCII al EBCDIC de IBM.

lcase

Intercambia las mayúsculas por minúsculas.

ucase

Intercambia las minúsculas por mayúsculas.

swab

Intercambia cada par de bytes de la entrada. Para el caso especial del último byte, este se copia directamente.

noerror

No se detiene el proceso ante errores de lectura en el origen.

notrunc

No se trunca el archivo utilizado como destino.

sync

Rellena cada bloque leído con ceros, hasta el tamaño determinado por ibs.

block

Rellenar con espacios en blanco la línea leída, hasta el tamaño indicado por cbs. Reemplaza el carácter de nueva línea por espacios, convirtiendo la línea en un bloque (o registro).

unblock

Reemplazar los últimos espacios en blanco por un carácter de salto de línea del registro leído, que posea el tamaño indicado por cbs. Realiza la operación inversa a block.

Dada la naturaleza del comando dd de operar a bajo nivel (bytes), es posible utilizarlo para diversos fines.

.- Eliminación de datos [editar]

Se realiza un formateo a medio nivel (sustituir todos los bits del disco archivo o carpeta por 0) mediante (con permisos de root) dd if=/dev/zero of = (archivo, directorio o disco a borrar). Sin embargo esto deja abierta la posibilidad de leer los datos presentes antes del borrado en el disco mediante métodos avanzados. Si se quiere una protección completa, en lugar de escribir ceros en el disco, se recomienda escribir datos aleatorios utilizando dd if=/dev/urandom of = (archivo, directorio, o disco a borrar). El generador de números aleatorios urandom funcionará de forma ligeramente diferente en los distintos tipos de sistemas UNIX, por lo que es recomendable verificarlo antes de utilizarlo.

.-Otros usos [editar]

Otro de los principales usos del comando dd es la creación de unidades USB autoarrancables, mediante la sintaxis:

dd if=/<ruta_imagen.iso> of=/dev/sdN

Donde N es la unidad USB que necesitamos autoarrancar.

Conclusiones: Es un comando de Linux que permite la creación de copias de dispositivos, como si fueran archivos, ya que Linux trata los dispositivos como archivos. Es fácil de usar, con muchas opciones para realizar las copias de diversas formas y tipos de salida. Cumple con su cometido, ya que es simple y eficaz y no se complica en opciones innecesarias, además, al estar incluido en todas las distribuciones de Linux, ya que es una herramienta del core de Linux, no es necesario ni su instalación ni la, a veces complicada, configuración de las herramientas.

Free Hex Editor Neo

Desarrollador: HDD Software

Página de la herramienta: http://www.new-hex-editor.com/

Tipo de Instalación: Descarga de un paquete de instalación, gratuito.

Tipo de Herramienta: Editor de documentos en hexadecimal, que permite ver, editar, deshacer y rehacer cambios, buscar, selección multiple, etc.

Uso: Edicion de documentos para la búsqueda de cualquier tipo de información oculta.

Descripción: Hex Editor Neo es un conjunto de herramientas de desarrollo hexadecimal para Windows, que combina archivos binarios avanzadas de edición de capacidad con un nuevo nivel de rendimiento y facilidad de uso.

Las características básicas incluyen, edición de datos, intercambio de datos con otras aplicaciones a través del portapapeles, la inserción de nuevos datos y eliminación de los datos existentes y otros.

Las características avanzadas incluyen la selección múltiple, historia visual con operaciones de ramificación, potente comando de "Find All" y "Replace All" los comandos, soporte para múltiples codificaciones, comandos "Goto" y "Fill", apoyo a alternativas de los Sreams de datos de NTFS, bookmarks, data inspector, cálculo de checksum, estadísticas y capacidades de análisis de la estructura de archivos .

Hex Editor está muy optimizado para realizar rápidamente las medidas solicitadas y abre fácilmente archivos de cualquier tamaño. También permite continuar trabajando con un documento mientras otro documento está realizando una operación larga.

Posee una serie de características en la interfaz de usuario, tales como barras de herramientas y ventanas de herramientas, creadas para simplificar las tareas mas comunes y hacer la edición más rápida y sencilla.

Cada aspecto de la interfaz de usuario es personalizable.

La herramienta se encarga de la excavación monótona en código hexadecimal.

Las características en las que destqaca **Hex Editor** son:

- Permite encontrar patrones de datos en archivos de varios gigabytes en cuestión de segundos. Es potente.
- Soporta búsqueda de expresiones regulares a través de los archivos. Es muy práctico.
- Permite hacer parches de archivos en un solo clic. Es inteligente.
- Permite sintonizar casi cualquier aspecto de la interfaz de usuario. Es flexible.
- Soporta el procesamiento multi-core. Es eficiente.

Free Hex Editor Neo esta optimizado para todos los que trabajan con ASCII, hexadecimal, decimal, float, double y datos binarios.

Freeware Hex Editor Neo le permite ver, modificar, analizar los datos hexadecimales y archivos binarios, editar, intercambiar datos con otras aplicaciones a través del portapapeles, insertar nuevos datos y borrar los datos existentes, así como realizar otras acciones de edición.

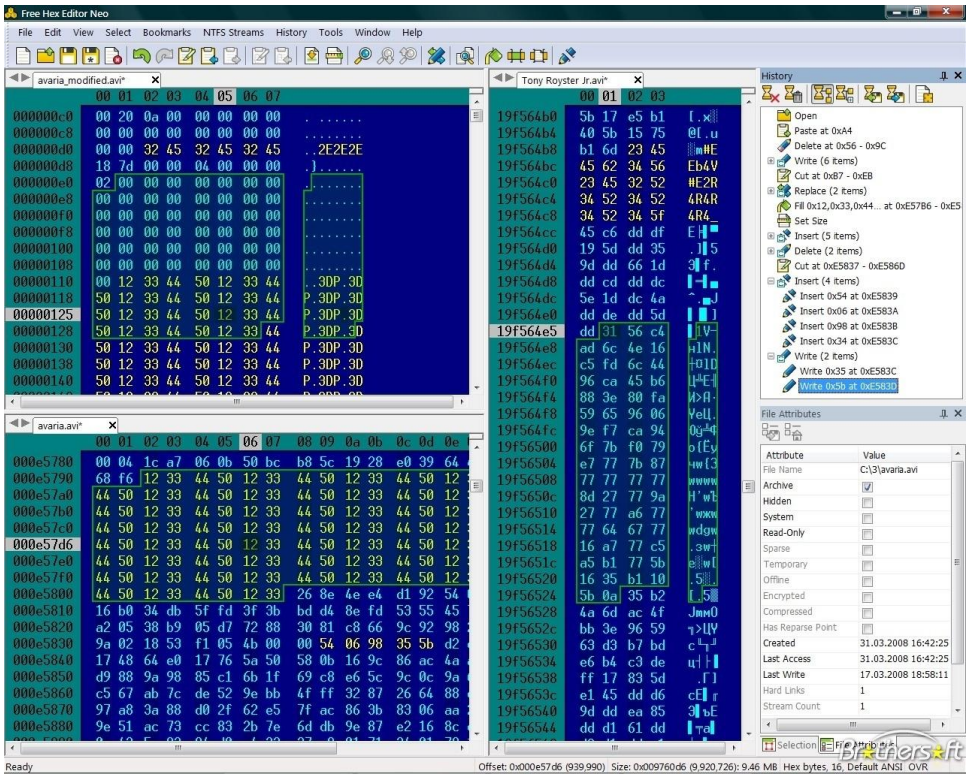


Foto descargada de http://www.brothersoft.com/free-hex-editor-40299.html

Hacer parches con sólo dos clics del ratón; manipular sus archivos EXE, DLL, DAT, AVI, MP3, JPG de forma ilimitada pudiendo deshacer/rehacer. Tiene un historial, visual, de las operaciónes con ramificaciones.

Esta utilidad de software de edición de datos para Windows incluye las siguientes funcionalidades básicas:

.- Funcion ilimitada de deshacer/rehacer;

.- Opción de búsqueda avanzada;

.- Historial visual de guardado y carga;

.- Creación de parches;

.- Operaciones con el Portapapeles;

.- Bytes, palabras, palabras dobles, Palabras Quad, flotadores y el modo de edición de dobles.

Hex Editor ofrece la característica única llamada *selección múltiple*. A diferencia de la mayoría de los editores, en la que sólo se permite seleccionar un texto *contiguo* o datos, Hex Editor permite tener varios rangos contiguos (o *bloques*) en una selección. Además, no está limitado en un número de bloques contiguos, puede haber tantos bloques como sea necesario.

Por defecto, la función de selección múltiple está habilitada. Cuando se inicia la selección de datos, permanece seleccionado todos los datos previamente seleccionada.

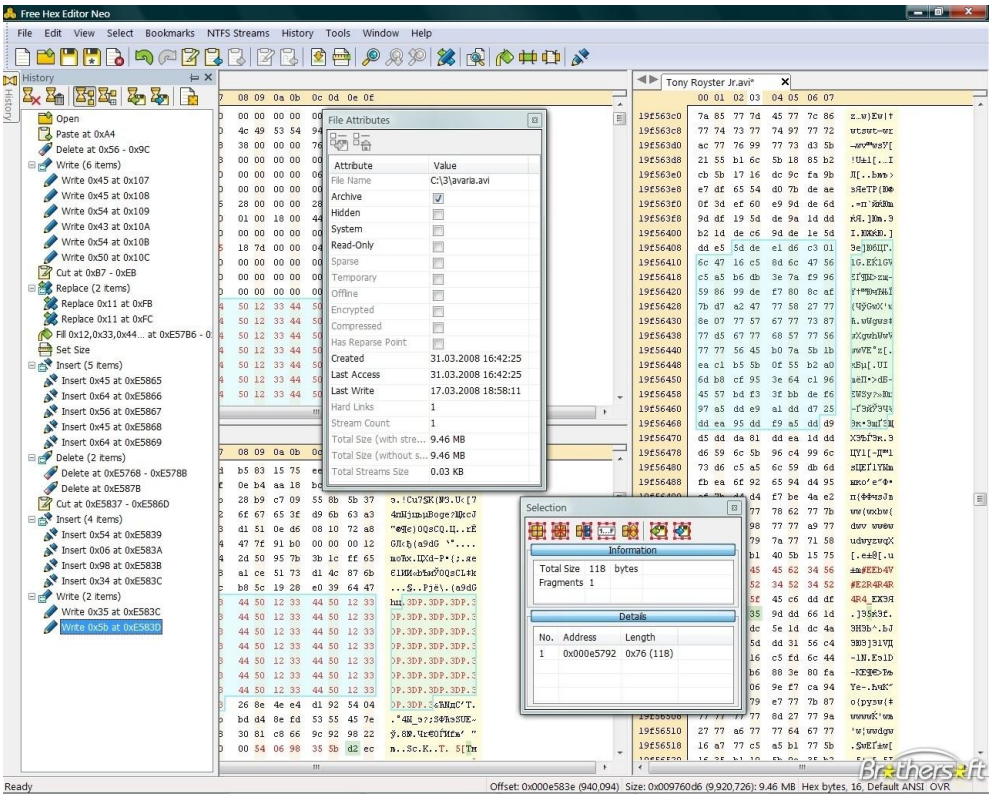


Foto descargada de http://www.brothersoft.com/free-hex-editor-40299.html

Hex Editor proporciona una manera muy conveniente de organizar el espacio de trabajo cuando se trabaja con más de un documento o con más de una ventana del editor.

El espacio de trabajo se divide en una o más tramas. Cada trama contiene una o más ventanas del editor.

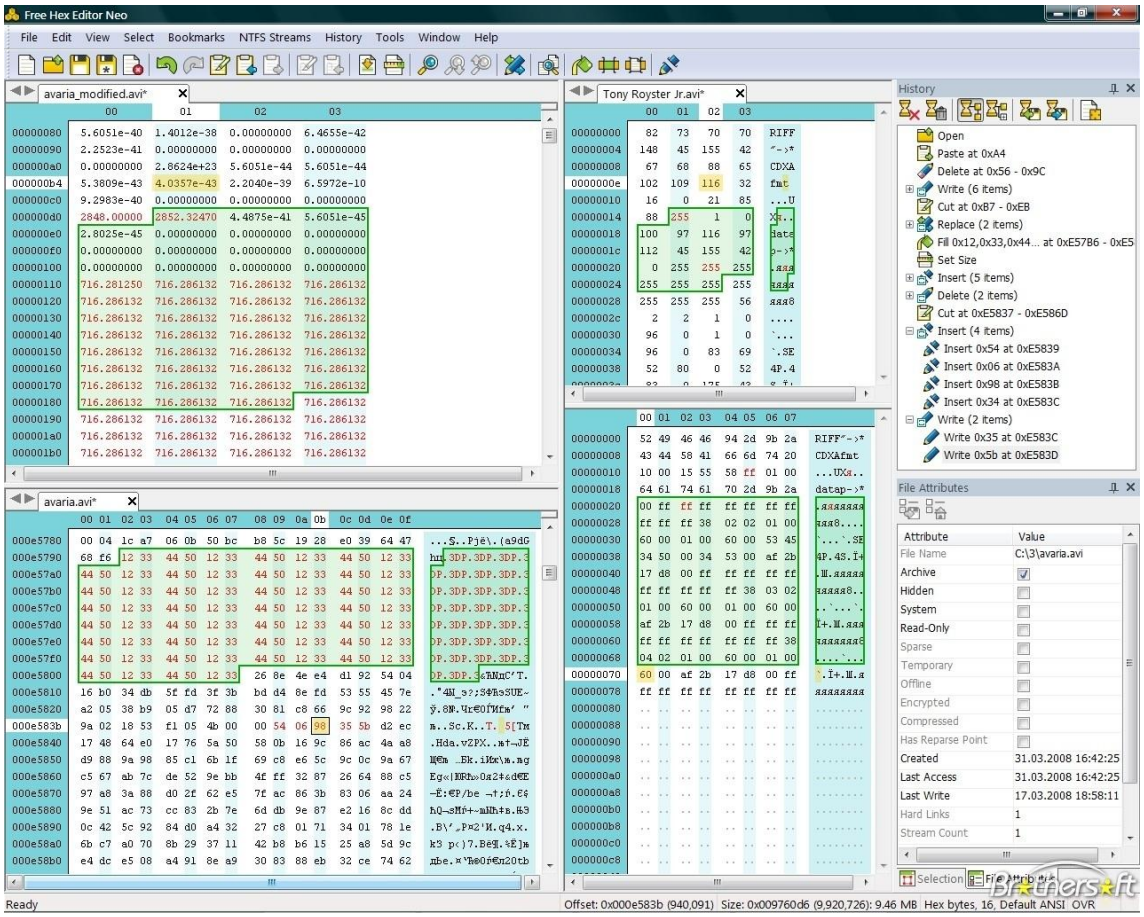


Foto descargada de http://www.brothersoft.com/free-hex-editor-40299.html

Cada ventana del editor está representado por una ficha en un marco. El nombre de archivo del documento se muestra en cada ficha.

Conclusiones: Editor de documentos en hexadecimal, que permite la edición de varios tipos de documentos, muy útil para averiguar la información interna de los archivos aunque en un formato poco entendible, ya que no se asemeja nada al lenguaje humano, pero si llegas a entenderlo es útil porque permite ver código de archivos incluso encriptados.

Es una herramienta complicada de manejar para los iniciados ya que ver el código en formato hexadecimal no da mucha información, pero en manos expertas tiene muchas utilidades.

Deft

Desarrollador: DEFT Association

Página de la herramienta: http://www.deftlinux.net/

Tipo de Instalación: Descarga de una ISO, para hacer un montaje en un CD/DVD o en una máquina virtual o local.

Tipo de Herramienta: Es un todo en uno, entorno en el que s eintegran todas las herramientas open source, recompiladas por el equipo de DEFT, se puede realizar cualquier tipo de actividad relacionada con el análisis forense digital.

Uso: Su utilidad va desde la toma de pruebas, creando imágenes u otro tipo de acción, hasta la creación de informes para entregarlos en un juicio o a una empresa como resultado de la investigación, pasando por cualquier paso intermedio en la investigación.

Descripción: **DEFT** es un Live CD montado sobre Xubuntu con herramientas para el análisis informático forense y para dar respuesta a incidentes.

La suite de DART se puede ejecutar en todos los sistemas de 32 bits de Microsoft Windows. Se han encontrado algunas limitaciones menores para la ejecutación de algunas herramientas que no garantizan el pleno apoyo a los sistemas de 64 bits.

DART puede ejecutar directamente en DEFT Linux usando Wine8.

Foto descargada de https://indonesianbacktrack.or.id/forum/thread-6139.html

Es un sistema vivo muy ligero y rápido creado por especialistas en Informática Forense.

DEFT Linux v5 se basa en el nuevo kernel 2.6.31 (Linux) y DEFT extra 2.0 (GUI Informática Forense) con las mejores herramientas forenses informáticas de Windows freeware.

DEFT tiene un nuevo concepto de sistema Forense en vivo, que utiliza LXDE como entorno de escritorio y Thunar como administrador de archivos y administrador de montaje como herramienta para la gestión de dispositivos.

Es un sistema muy sencilla de usar, que incluye una excelente detección de hardware y utiliza las mejores aplicaciones de código libre y abierto dedicadas a la respuesta a incidentes y análisis forense informático.

Foto descargada de http://distrowatch.com/table.php?distribution=deft

Con una lista de más de 130 herramientas gratuitas se ofrece como un recurso gratuito para cualquier usuario. El listado se actualiza varias veces al año con lo que se dispone de una amplia cantidad de herramientes disponibles en un solo entorno capaz de realizar cualquier analisis forense digital con garantias.

La realización de un analisis forense no proporciona ningún apoyo o garantía en la utilización de software sin verificar los acuerdos de licencia, por lo que la utilización de algun software de la lista sin haber aceptado dichos acuerdos es responsabilidad del usuario y hace que la evidencia que sea admitida, o no, en un caso judicial si no se han validado los acuerdo de uso de las herramientas por un analista profesional de informática forense.

Foto descargada de https://inforensicsuex.wordpress.com/2014/03/28/24/

La inclusión en la lista de una herramienta no equivale a una recomendación. El uso de software forense no lo hace, por sí solo, sino que lo tieneque hacer el usuario.

Tenga en cuenta que en la sección modo de referencia se enumeran, incluso, las aplicaciones antiguas, que parecen ser ya no ser validas ni actualizables, pero todavía puede ser de utilidad para un analisis forense digital.

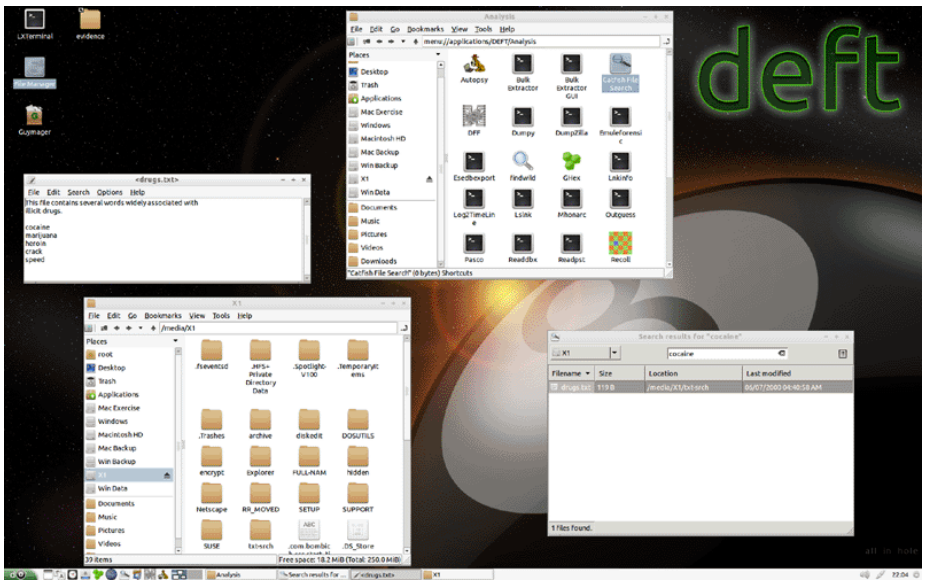


Foto descargada de http://www.compuforensics.com/training.htm

Ademas de las aplicaciones ya instaladas, al ser un entorno Linux se le pueden añadir nuevas aplicaciones de cualquier tipo, por lo que la ampliación y su uso prolongado queda asegurado.

Al incluir un elenco tan grande y variado de herramientas, el entorno es una buena elección tanto para principiantes como para profesionales, cada un adaptando el entorno a sus necesidades y ampliando o eliminando las herramientas innecesarias.

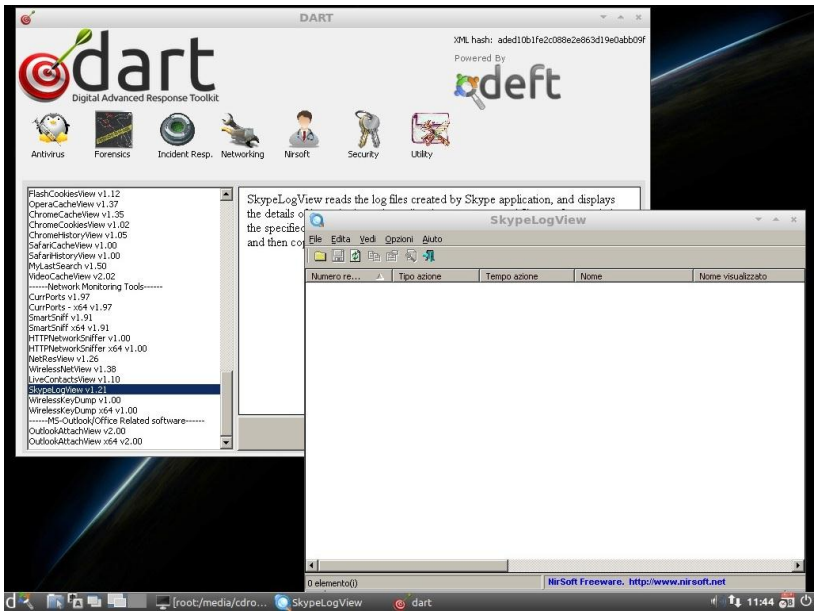


Foto descargada de http://www.kitploit.com/2013/05/deft-7-distribution-with-best-freeware.html

Conclusiones: Una buena elección para cualquier tipo de usuario, ya que al estar constituido por una variedad tan grande de herramientas, tanto el analista principiante como el profesional encontraran la herramienta que se ajuste a sus necesidades.

Posee una lista con las herramientas disponibles que se va actualizando constantemente, por lo que se añade una ventaja, al tener las aplicaciones open source a la última casi sin esfuerzo.

LastActivity View

Desarrollador: NirSoft

Página de la herramienta:
http://www.nirsoft.net/utils/computer_activity_view.html

Tipo de Instalación: Descarga de un archivo con extensión .zip, en el que se incluye un instalable, al ejecutarlo se instala la herramienta en el ordenador.

Tipo de Herramienta: Herramienta de monitorización, para observar las acciones que ocurrieron en un espacio de tiempo relacionadas con un usuario y un dispositivo.

Uso: Localizar eventos, ocurridos en un espacio de tiempo, que puedan ser sospechosos, monitorizando la actividad de una fuente.

Descripción: LastActivityView es una herramienta para el sistema operativo Windows, que recopila información de varias fuentes en un sistema en funcionamiento, y muestra un registro de las acciones realizadas por el usuario y los eventos que ocurrieron en este equipo durante un periodo de tiempo.

La actividad desplegada por LastActivityView incluye:

.- Running archivos .exe,

.- apertura de cuadros de diálogo

.- apertura desde el Explorador o cualquier otro software de guardar archivo/carpeta,

.- instalación de software,

.- el apagado del sistema,

.- fallo del sistema o de alguna aplicación,

.- conexión/desconexión de red

.- y más. ..

Se puede exportar esta información en archivos csv/html delimitado por tabuladores, xml o copiar al portapapeles y luego pegarlo en Excel u otro software similar.

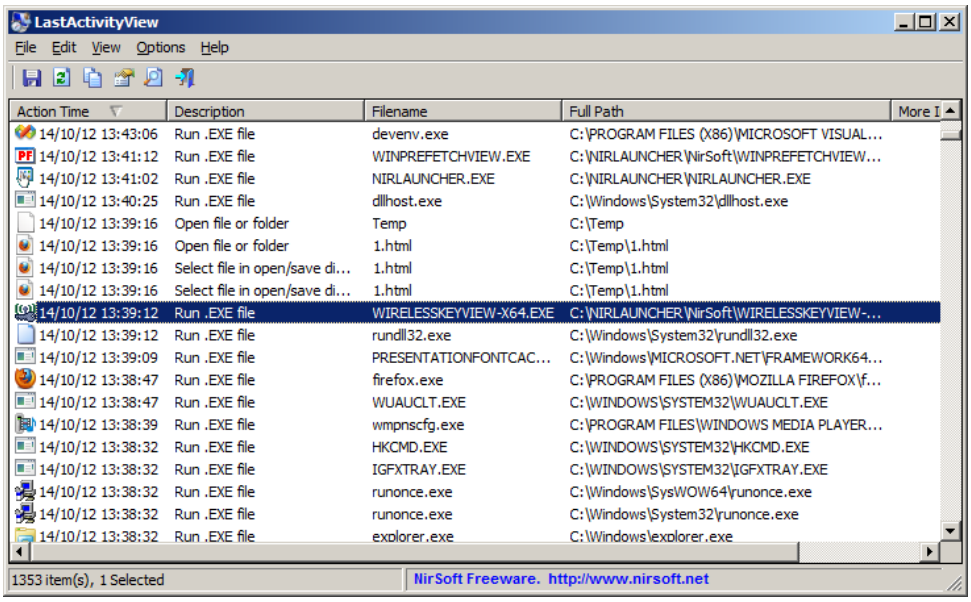


Foto descargada de http://www.nirsoft.net/utils/computer_activity_view.html

Esta utilidad funciona en cualquier versión de Windows, desde Windows 2000 y hasta Windows 8. Y es compatible con los sistemas de 32 bits y 64 bits.

Esta herramienta recopila información de varias fuentes, incluyendo el registro, el registro de eventos de Windows, la carpeta Prefetch de Windows (C:\Windows\Prefetch), la carpeta de Minivolcado de Windows (C:\Windows\Minidump), y más.

La precisión y la disponibilidad de la información mostrada por LastActivityView podrían ser diferentes de un sistema a otro. Por ejemplo, siel usuario o un software hace los cambios en el Registro, el tiempo de la acción desplegada por LastActivityView podría estar equivocado, porque se basa en la hora de modificación de algunas claves de registro.

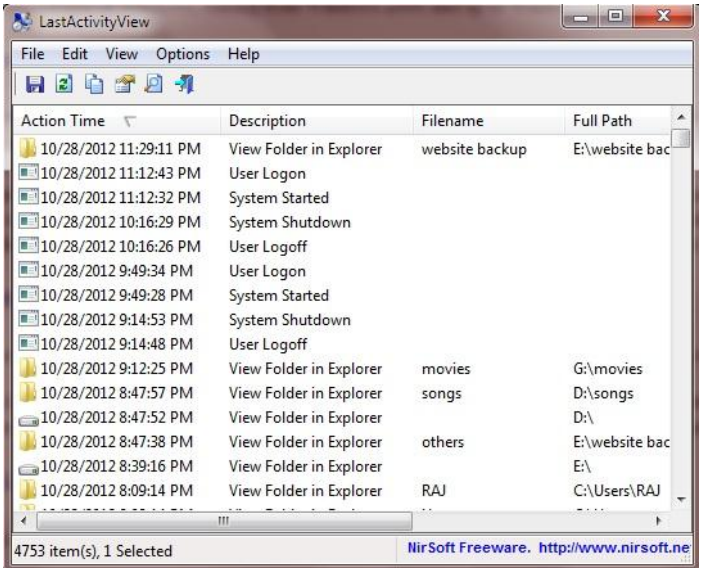


Foto descargada de http://ankhacktips.blogspot.com.es/2012/11/last-activity-view.html

Además, para cada tipo de acción/evento, hay una cierta limitación de acuerdo a la forma en que la información se guarda en el sistema. Por ejemplo, la acción está limitada por una acción de cada extensión de archivo "Seleccionar archivo en abierto/de cuadro de diálogo Guardar ', por lo que si el usuario abre 2 archivos .doc con el mismo explorador, sólo el último será visualizado.

LastActivityView no requiere ningún proceso de instalación o archivos DLL adicionales. Con el fin de comenzar a usarlo, simplemente ejecute el archivo ejecutable - LastActivityView.exe

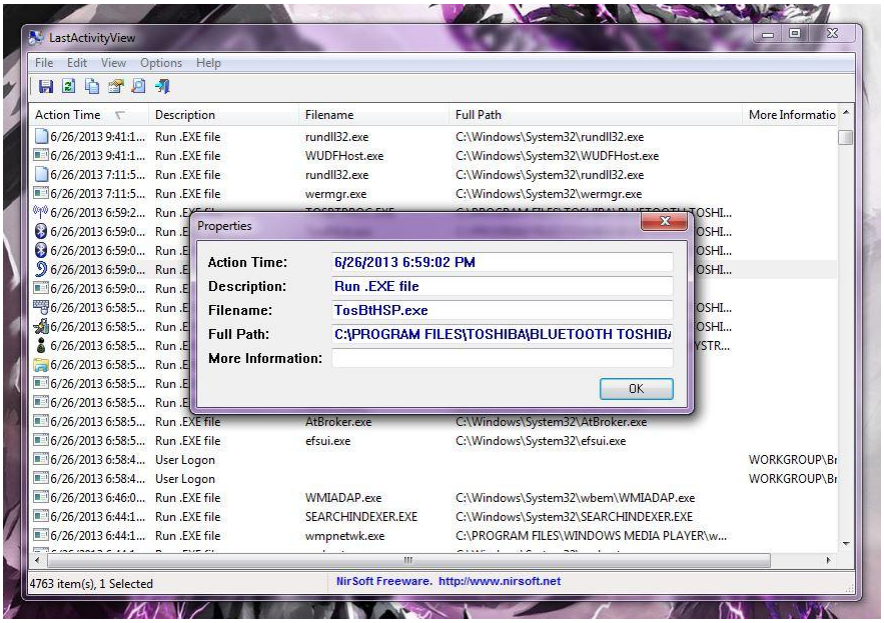


Foto descargada de http://dottech.org/113894/windows-review-lastactivityview/

Después de ejecutar LastActivityView, escanea el ordenador y muestra todas las acciones y eventos que se encuentran en su sistema. Puede seleccionar uno o más elementos y luego guardarlos en xml/html/csv/ archivo delimitando por tabuladores cada registro (Ctrl + S) o copiarlos al portapapeles (Ctrl + C) y, a continuación, pegar los datos a una hoja de calculo u otro software.

Las siguientes acciones y eventos están actualmente soportadas por LastActivityView:

- **Ejecutar archivo .EXE:** run archivo .EXE directamente por el usuario, o por otro software/servicio que se ejecuta en segundo plano.
- **Seleccionar archivo en cuadro de diálogo de guardar:** El usuario selecciona el nombre del archivo especificado del cuadro de diálogo estándar de Windows con la opción Save/Open
- **Abrir el archivo o carpeta:** El usuario abre el archivo especificado desde el Explorador de Windows o desde otro software.
- **Ver carpeta en el Explorador:** El usuario ve la carpeta especificada en el Explorador de Windows.

- **Instalación del software:** El software especificado se ha instalado o actualizado.
- **Sistema de iniciación:** El ordenador se ha iniciado.
- **Apagado del sistema:** El sistema se ha cerrado, directamente por el usuario o por un software que inició un reinicio.
- **Continuación de la suspensión del equipo:** La computadora se ha reanudado del modo de suspensión.

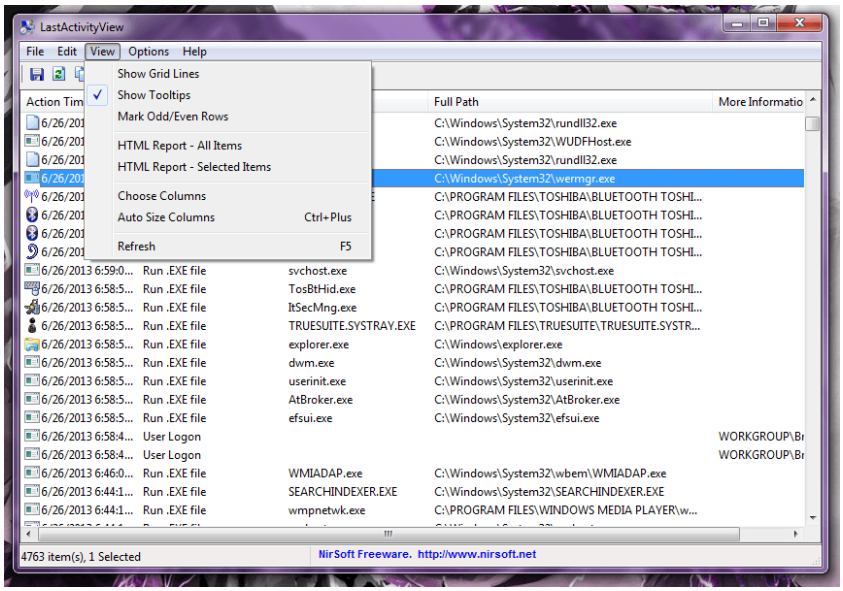
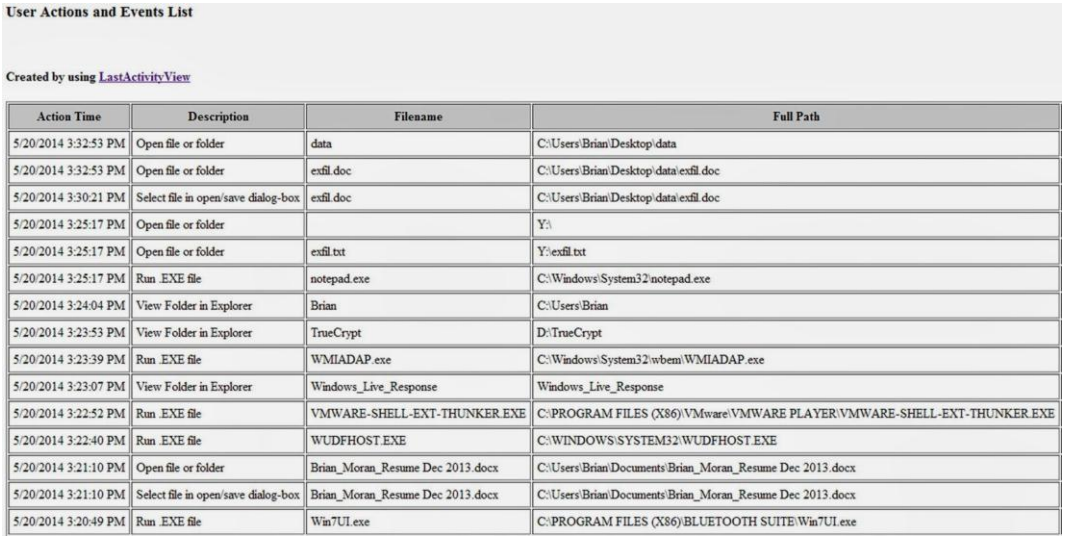


Foto descargada de http://dottech.org/113894/windows-review-lastactivityview/

- **Red conectada:** Red conectada, después de desconectar previamente.
- **Red desconectada:** Red se ha desconectado.
- **Crash de Software:** El software especificado ha fallado producuiendo un error.
- **Software dejó de responder (se bloquea):** El software especificado dejó de responder.
- **Pantalla Azul:** Evento de pantalla azul se ha producido en el sistema.
- **Inicio de sesión de usuario:** El usuario ha iniciado sesión en el sistema.
- **Cierre de sesión de un usuario:** El usuario cerró la sesión del sistema. Esto incluso podría ser causado por un software que inició un reinicio.
- **Punto de restauración Creado:** Restaurar punto que ha sido creado por el sistema operativo Windows.
- **Windows Installer Started:** Inicio de la instalación de una aplicación con el instalador de Windows.

- **Windows Installer Ended:** Fin de la instalación de una aplicación con el instalador de Windows.



User Actions and Events List

Created by using LastActivityView

Action Time	Description	Filename	Full Path
5/20/2014 3:32:53 PM	Open file or folder	data	C:\Users\Brian\Desktop\data
5/20/2014 3:32:53 PM	Open file or folder	exfil.doc	C:\Users\Brian\Desktop\data\exfil.doc
5/20/2014 3:30:21 PM	Select file in open/save dialog-box	exfil.doc	C:\Users\Brian\Desktop\data\exfil.doc
5/20/2014 3:25:17 PM	Open file or folder		Y:\
5/20/2014 3:25:17 PM	Open file or folder	exfil.txt	Y:\exfil.txt
5/20/2014 3:25:17 PM	Run .EXE file	notepad.exe	C:\Windows\System32\notepad.exe
5/20/2014 3:24:04 PM	View Folder in Explorer	Brian	C:\Users\Brian
5/20/2014 3:23:53 PM	View Folder in Explorer	TrueCrypt	D:\TrueCrypt
5/20/2014 3:23:39 PM	Run .EXE file	WMIADAP.exe	C:\Windows\System32\wbem\WMIADAP.exe
5/20/2014 3:23:07 PM	View Folder in Explorer	Windows_Live_Response	Windows_Live_Response
5/20/2014 3:22:52 PM	Run .EXE file	VMWARE-SHELL-EXT-THUNKER.EXE	C:\PROGRAM FILES (X86)\VMware\VMWARE PLAYER\VMWARE-SHELL-EXT-THUNKER.EXE
5/20/2014 3:22:40 PM	Run .EXE file	WUDFHOST.EXE	C:\WINDOWS\SYSTEM32\WUDFHOST.EXE
5/20/2014 3:21:10 PM	Open file or folder	Brian_Moran_Resume Dec 2013.docx	C:\Users\Brian\Documents\Brian_Moran_Resume Dec 2013.docx
5/20/2014 3:21:10 PM	Select file in open/save dialog-box	Brian_Moran_Resume Dec 2013.docx	C:\Users\Brian\Documents\Brian_Moran_Resume Dec 2013.docx
5/20/2014 3:20:49 PM	Run .EXE file	Win7UI.exe	C:\PROGRAM FILES (X86)\BLUETOOTH SUITE\Win7UI.exe

Foto descargada de http://www.brimorlabsblog.com/2014_05_01_archive.html

Conclusiones: Herramienta para monitorización del sistema operativo, en el que se controla cualquier tipo de movimiento realizado en el sistema operativo, desde cambios en archivos hasta en el registro de Windows.

Es una herramienta valida para controlar los posibles cambios realizados y verificar si se han cambiado o eliminado registros en el sistema, tarea muy importante en las invetigaciones para poder analizar los posibles cambios que ayuden a encontrar evidencias.

HxD

Desarrollador: mh-nexus

Página de la herramienta: http://mh-nexus.de/en/hxd/

Tipo de Instalación: Ejecutable, se instala en un dispositivo o en un USB.

Tipo de Herramienta: Editor de archivos en formato Hex.

Uso: La edición de archivos o trozos de memoria en formato Hex, para cambiar o ver el contenido de la memoria o del archivo.

Descripción: HxD Hex Editor proporciona herramientas para inspeccionar y editar archivos, memoria principal, discos/imágenes de disco y su estructura.

Se puede utilizar para analizar los archivos de registro, trozos grandes archivos ROM para emuladores, reparación de estructuras de disco, validar los datos y mucho más.

HxD es un editor hexadecimal diseñado cuidadosamente y rápido que, además, de la edición del disco en crudo y de la modificación de la memoria principal (RAM), maneja archivos de cualquier tamaño.

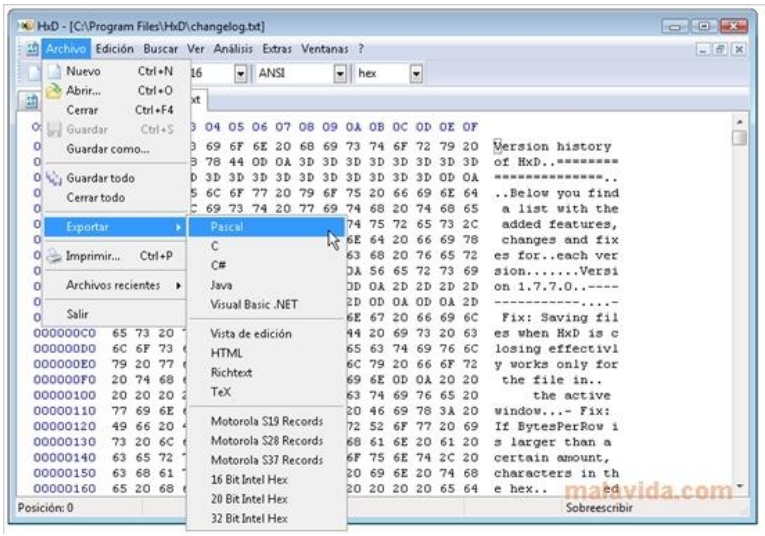


Foto descargada de http://hxd.malavida.com/

La interfaz es fácil de usar y ofrece características tales como buscar y reemplazar, exportar sumas de comprobación/digiere, la inserción de los patrones de bytes, un destructor de archivos, concatenación o división de archivos, estadísticas y mucho más.

HxD Hex Editor funciona como un editor de texto, enfocado en una operación simple y orientado a la tarea, por ejemplo, las unidades y la memoria se presentan de forma similar a un archivo y se muestran como un todo, en contraste con una vista de un sector/región limitada que corta los datos potencialmente juntos a los que pertenece.

Las unidades de disco y de memoria se pueden editar de la misma manera que un archivo normal incluyendo soporte para deshacer los cambios. Además las secciones de memoria definen una región plegable y muestra secciones inaccesibles que están ocultas por defecto.

Además se pueden hacer operaciones rápidas y eficientes, en lugar de tener que utilizar funciones especializadas por razones técnicas o limitar arbitrariamente tamaños de archivo por culpa de demasiado esfuerzo.

HxD Hex Editor incluye una interfaz de usuario y de progreso sensibles con indicadores para operaciones prolongadas.

Características

- Disponible como edición portátil e instalable
- RAM-Editor
    - Para editar la memoria principal
    - Secciones de memoria etiquetadas con data-folds
- Disk-Editor (discos duros, disquetes, discos ZIP, unidades flash USB, CD, ...)
    - Lectura RAW y escritura de discos y unidades

  - para Win9x, WinNT y superior
- Apertura instantánea independientemente del tamaño del archivo
  - Hasta 8EB; la apertura y la edición es muy rápida
- Compartir archivos de forma segura con otros programas
- Búsqueda/sustitución de varios tipos de datos de forma flexible y rápida
  - Los tipos de datos: texto (incluyendo Unicode), valores hex, números enteros y flotantes
  - Busqueda de una dirección: adelante, atrás, todo (empezando desde el principio)
- Compara archivos (simple)
- Puede mostrar conjuntos de caracteres Ansi, DOS, EBCDIC y Macintosh
- Generador de Checksum: Checksum, CRCs, Custom CRC, SHA-1, SHA-512, MD5, etc.
- Exportación de los datos a varios formatos
  - El código fuente (Pascal, C, Java, C #, VB.NET)
  - Salida con formato (texto, HTML, Richtext, TeX)
  - Archivos Hex (Intel HEX, Motorola S-registro)
- Inserción de patrones de bytes

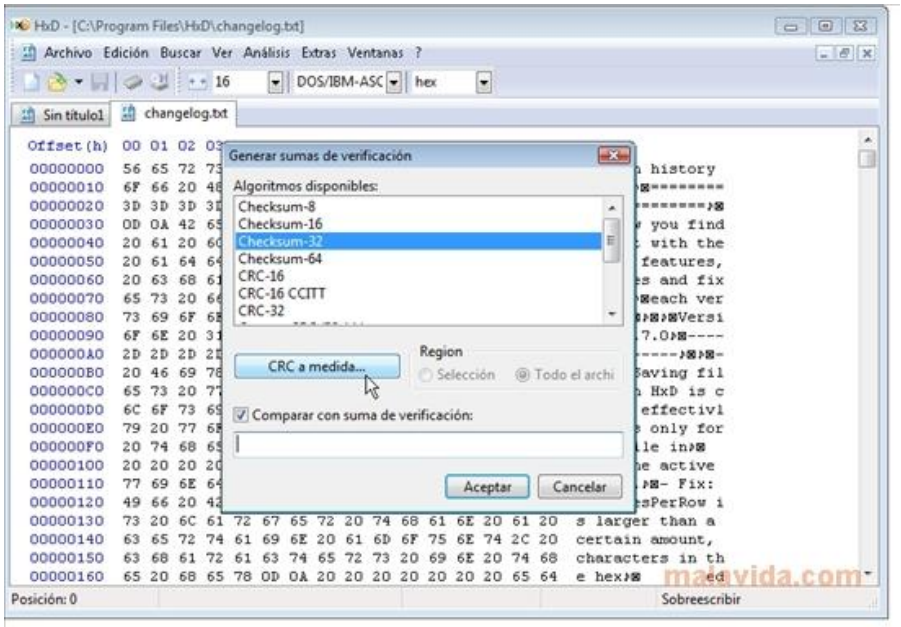


Foto descargada de http://hxd.malavida.com/

- Herramientas de archivo

    - Trituradora de archivos para eliminación de archivos segura
    - La división o concatenación de archivos
- Análisis de datos básicos (estadísticas)
    - Representación gráfica de la distribución de byte/caracteres
    - Ayuda a identificar el tipo de datos de una selección
- Agrupación Byte
    - 1, 2, 4, 8 o 16 bytes empaquetados juntos en una columna
- Modos "Hex-only" o "Text-only"
- Ventana de progreso para operaciones largas
    - Muestra el tiempo restante
    - Botón para cancelar
- Datos modificados destacados
- La operación de deshacer sin límite
- Función de "Buscar actualizaciones ..."
- Interfaz fácil de usar y moderna
- Dirección de Goto
- Impresión
- Modo de sobrescritura o de inserción
- Cortar, copiar, pegar inserción, pegar escritura
- Apoyo Portapapeles para otros editores hexadecimales
    - Visual Studio/Visual C ++, WinHex, HexWorkshop, ...
- Bookmarks
    - Ctrl + Shift + Número (0-9) establece un marcador
    - Ctrl + Número (0-9) va a un marcador
- Navegación a saltos con Ctrl + Izquierda o Ctrl + Derecha
- Visualización sin parpadeo y dibujo rápido

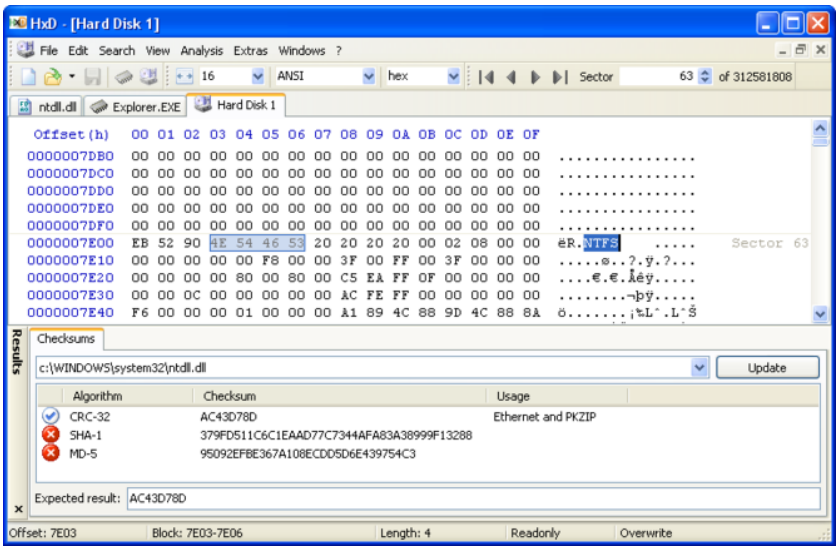


Foto descargada de http://mh-nexus.de/en/hxd/

Se pueden editar archivos binarios y sectores de disco sin procesar. Se pueden editar archivos compilados con está herramienta sin problemas. HXD Hex Editor. Es una herramienta de edición binaria para Windows.

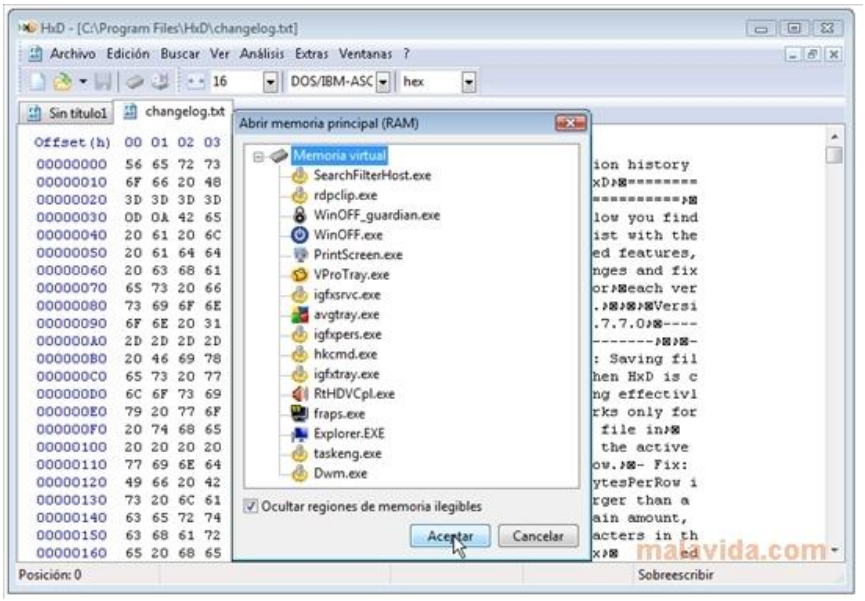


Foto descargada de http://hxd.malavida.com/

Conclusiones: HXD Hex Editor es bueno en lo que hace. La aplicación es fácil de usar; y también está disponible en una edición portable e instalable. Puede instalar la aplicación en una memoria USB, por ejemplo, y utilizarlo en cualquier sitio y con cualquier equipo.

Esta es probablemente una muy buena herramienta para un experto en tecnología y para el desarrollador o hackers, sobre todo para un analista forense digital, permitiendo la edición de ficheros que de otra forma no se podría.

Es una herramienta muy útil y no debería faltar una de este tipo a un analista forense profesional.

NetSleuth

Desarrollador: Net Grab Ltd

Página de la herramienta: http://netsleuth.software.informer.com/1.6b/

Tipo de Instalación: Descarga de un ejecutable

Tipo de Herramienta: Monitorización de redes para la detección de evidencias.

Uso: Se utiliza en la detección de evidencias en redes, monitorizando una red a analizando los archivos PCAP.

Descripción: **NetSleuth** es una herramienta open source de monitoreo de red y análisis forense. NetSleuth identifica huellas de dispositivos de red, monitorizando la red en silencio o por el procesamiento de datos de archivos PCAP.

Características NetSleuth:

- Muestra una visión general, en tiempo real, de los dispositivos conectados a una red.
- Sin necesidad de hardware o reconfiguración de redes.
- "Portscanning silenciosa" y supervisión de la red indetectable.
- Análisis desconectado de archivos pcap, para ayudar en la respuesta de intrusiones y análisis forense de la red.
- Identificación automática de una amplia gama de tipos de dispositivos, incluyendo teléfonos inteligentes, tabletas, consolas de juegos, impresoras, routers, equipos de escritorio y más

.- PortScanning silencioso:

Muchos dispositivos de red transmiten información diversa a través de la red. A menudo esto es para "configuración inicial" de los servicios de estilo, para el protocolo Bonjour, por ejemplo, de Apple. Esta información a menudo contiene información sobre la máquina, y los servicios que se ejecutan en ese dispositivo - información interesante para la toma de huellas.

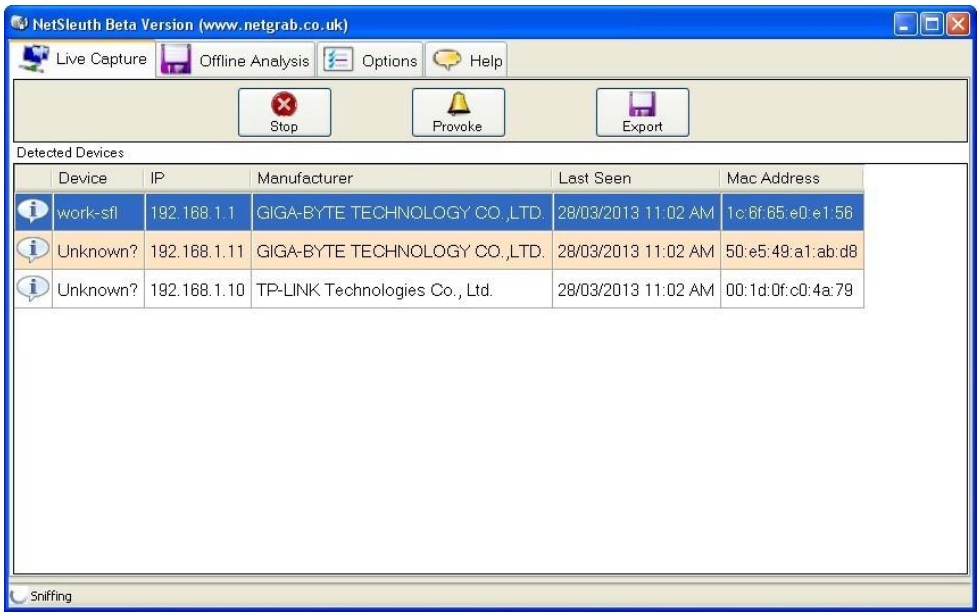


Foto descargada de http://netsleuth.software.informer.com/1.6b/

Por esta razón, es posible obtener información de este estilo haciendo una exploración de puertos completamente en silencio. NetSleuth tampoco pone los adaptadores de red en modo promiscuo, mitigando algunas técnicas para detectar sniffing en los adaptadores de red.

.- Análisis Desconectado:

Una captura de red desde cualquier red con dispositivos de consumo contiene una enorme cantidad de tráfico de difusión rica para el análisis. NetSleuth puede analizar y extraer estos datos de archivos .pcap de Snort, Wireshark u otras herramientas. También puede analizar los datos interceptados por archivos Kismet (la .pcapdump).

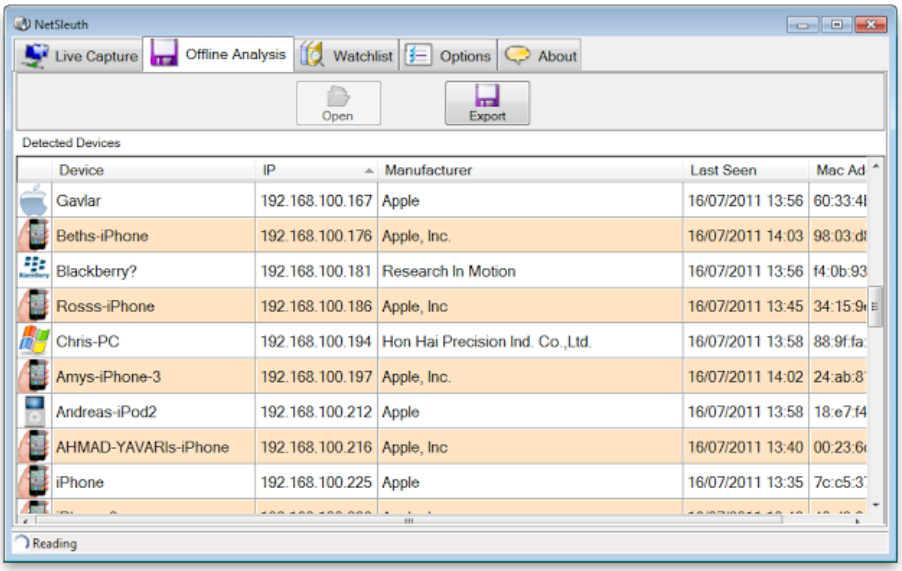


Foto descargada de http://santoshdudhade.blogspot.com.es/2013/02/netsleuth-open-source-network-forensics.html

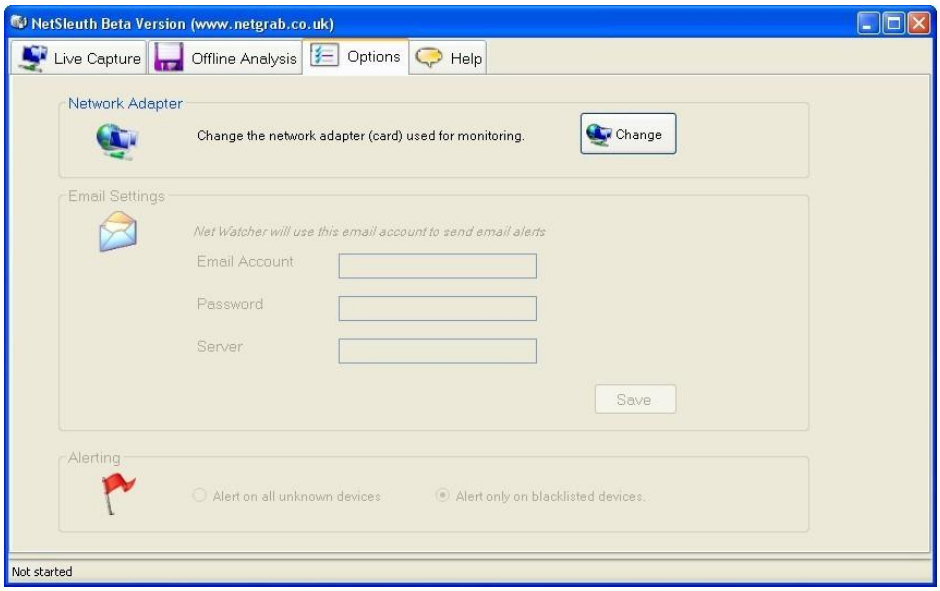


Foto descargada de http://netsleuth.software.informer.com/1.6b/

Conclusiones: Herramienta para el monitoreo de una red, permite la detección de la transmisión de cualquier tipo de transmisión y desde cualquier tipo de dispositivo, desde ordenadores, pasando por tablets y hasta consolas de juegos.

Es una herramienta útil, ya que escanea sin dejar rastro ni ser detectada, permitiendo la monitorización aun cuando se utilizan técnicas de sniffing en los adaptadores de red.

Tabla de herramientas ordenadas alfabéticamente

Acronis True Image	Clone e imagenes de disco	49,90€
Bulk Extactor	Recuperación Datos	Open Source
Caine	Live CD	Open Source
CloneZilla Live CD	LiveCD	Open Source
Comando Linux "dd"	Clone e imágenes de disco	Open Source
Deft	Live CD	Open Source
Digital Forensics Framework	Framework	Free, 700€ ó 1000€
DriveClone	Clonador de discos	Free, $50 ó $149
EnCase	Suite	Demo y Pago
Free Hex Editor Neo	Editor archivos	Open Source
FTK	Live CD	Open Source
HELIX3	Suite	Demo y Pago
HxD	Editor archivos	Open Source
LastActivity View	Monitorización procesos	Open Source
Mandiant RedLine	Analizador de Memoria	Open Source
NetSleuth	Monitorización redes	Freeware
Open Computer Forensics Architecture	Live CD	Open Source
OSFClone	Clonador de discos	Open Source
Oxygen Forensics Suite	Suite	Pago
P2 eXplorer	Imágenes de disco	Demo y Pago
PlainSight	Live CD	Open Source
ProDiscover Basic	Seguridad en Disco	$50 ó $150
Registry Recon	Analizador Registro	$599
SANS Investigate Forensics Toolkit Workstation	Live CD	???
The Sleuth Kit	Framework	Common Public License
Volatility	Framework	Open Source
WindowsSCOPE	Analizador de Memoria	$3899
Xplico	Análisis de Red	Open Source
XRY	Office	Pago
X-Ways Forensics	Suite	1369€

Legislación relacionada

Aunque los **delitos informáticos** no están contemplados como un tipo especial de delito en la legislación española, existen varias normas relacionadas con este tipo de conductas:

- Ley Orgánica de Protección de Datos de Carácter Personal.
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.
- Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley General de Telecomunicaciones.
- Ley de Propiedad Intelectual.
- Ley de Firma Electrónica.

Además de estas normas, en el Código Penal español, se incluyen multitud de conductas ilícitas relacionadas con los delitos informáticos. Las que más se aproximan a la clasificación propuesta por el "Convenio sobre la Ciberdelincuencia" se reflejan en los siguientes artículos:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**
    - El **Artículo 197** contempla las penas con las que se castigará:
        - A quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación.
        - A quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.
        - Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.

          En el **artículo 278.1** se exponen las penas con las que se castigará a quien lleve a cabo las mismas acciones expuestas anteriormente, pero con el fin de descubrir secretos de empresa.

    - El **Artículo 264.2** trata de las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
- **Delitos informáticos:**
    - Los artículos 248 y 249 tratan las estafas. En concreto el **artículo 248.2** considera las estafas llevadas a cabo mediante manipulación informática o artificios semejantes.
    - Los **artículos 255 y 256** mencionan las penas que se impondrán a quienes cometan defraudaciones utilizando, entre otros medios, las telecomunicaciones.

- **Delitos relacionados con el contenido:**
  - El **artículo 186** cita las penas que se impondrán a aquellos, que por cualquier medio directo, vendan, difundan o exhiban material pornográfico entre menores de edad o incapaces.
  - El **artículo 189** trata las medidas que se impondrán quien utilice a menores de edad o a incapaces con fines exhibicionistas o pornográficos, y quien produzca, venda, distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico, en cuya elaboración se hayan utilizado menores de edad o incapaces.
- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**
  - El **Artículo 270** enuncia las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad, de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros.
  - El **artículo 273** trata las penas que se impondrán a quienes sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio, objetos amparados por tales derechos, con fines comerciales o industriales.

Artículos del Código Penal Español referentes a Delitos Informáticos
(Ley-Orgánica 10/1995, de 23 de Noviembre/
BOE número 281, de 24 de Noviembre de 1.995)

- ***Artículo 197***

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personalque revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de
este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

- ***Artículo 198***

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

- ***Artículo 199***

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

- ***Artículo 200***

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

- ***Artículo 201***

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

- ***Artículo 211***

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

- ***Artículo 212***

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

- ***Artículo 238***

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1º.- Escalamiento.
2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.
3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.
4º.- Uso de llaves falsas.
5º.- Inutilización de sistemas específicos de alarma o guarda.

- ***Artículo 239***

Se considerarán llaves falsas:
1º.- Las ganzúas u otros instrumentos análogos.
2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.
A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

- ***Artículo 248***

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

- ***Artículo 255***

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º.- Valiéndose de mecanismos instalados para realizar la defraudación.
2º.- Alterando maliciosamente las indicaciones o aparatos contadores.
3º.- Empleando cualesquiera otros medios clandestinos.

- ***Artículo 256***

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

- ***Artículo 263***

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

- ***Artículo 264***

1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:
1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
2º.- Que se cause por cualquier medio infección o contagio de ganado.
3º.- Que se empleen sustancias venenosas o corrosivas.
4º.- Que afecten a bienes de dominio o uso público o comunal.
5º.- Que arruinen al perjudicado o se le coloque en grave situación económica.
2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

- ***Artículo 270***

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

- ***Artículo 278***

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

- ***Artículo 400***

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

- ***Artículo 536***

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.
Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

Delitos informáticos

Con la expresión delito informático se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

La clasificación de dichos delitos se puede enumerar en (fuente: Policía Nacional Española):

. Ataques que se producen contra el derecho a la intimidad

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

. Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor

Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

. Falsedades

Concepto de documento como todo soporte material que exprese o incorpore datos.

Extensión de la falsificación de moneda a las tarjetas de débito y crédito.

Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.

(Artículos 386 y ss. del Código Penal)

. Sabotajes informáticos

Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

. Fraudes informáticos

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

. Amenazas

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

. Calumnias e injurias

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

. Pornografía infantil

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art. 187)

La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art. 189)

El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (art. 189)

La posesión de dicho material para la realización de dichas conductas. (art. 189)

Conclusiones.

Desde los comienzos del uso generalizado de las tecnologías de la información han existido intenos por acceder a informacion confidencial. En muchas ocasiones los intentos han llegado a convertirse en delitos, ya que se ha conseguido el acceso a dicha información.

Como se puede observar en la primera parte del presente documento, se han producido gran cantidad de delitos informáticos durante la breve historia de la Informatica, de diversa índole y con diferentes fines.

Para contrarestar dichos delitos, se han especializado en la resolución de dichos delitos ciertas personas, y se han creado herramientas para ayudar a resolver dichos delitos.

Las herramientas, que se describen en el presente documento, son capaces de garantizar la integridad de las estructuras de archivos y metadata en los sistemas que están siendo investigadas con el fin de proporcionar un análisis preciso.

Garantizan unos resultados de analizar las pruebas que puedan ser validos, como pruebas, en los juicios contra los delincuentes informáticos. Creando informes validos y con resultados contrastados y fiables.

En el presente documento se describen ciertas herramientas utilizadas en el análisis forense digital, utilizadas en diversas partes de la investigación, dependiendo de la herramienta.

Existen suites, en las que se puede conseguir el análisis desde el principio de la investigación hasta el final, con la creación de un informe pericial que puede presentarse como prueba en un caso.

Tambien se describen herramientas concretas para una tarea determinada, en la que destaca por la realización de su funcionalidad de una manera destacada.

El presente documento es una pequeña guía para una persona que quiere iniciarse en el análisis forense, describiendo los posibles delitos que se puede encotrar en su trayectoria.

Se puede encontrar una breve descripción de lo que hacen las herramientas, descritas en el documento, y el tipo de licencia que tiene su uso.

Posteriormente se muestra un apartado en el que muestro las principales leyes Españolas para que se tenga una idea de que tipo de prueba puede ser valida y que tipo de investigación se tiene que realizar en cada momento. Además de los delitos más habituales hoy en dia, en los que se documenta la legislación que se aplicaría.

En conclusión, he pretendido recoger una pequeña muestra de herramientas utilizadas en el análisis forense digital para ayudar a la gente que pretenda introducirse en este mundo tan apasionante como es el Peritaje Informático.

Bibliografía.

Enlaces de busquedas de herramientas

Infosec Institute (2015). “Computer Forensics Tools”. http://resources.infosecinstitute.com/computer-forensics-tools/ España. 13/09/15

Recobery Labs (2015). “Legislación”. http://www.delitosinformaticos.info/delitos_informaticos/legislacion.html España. 13/09/15

delitosinformaticos.com (2015). “Legislación”. http://delitosinformaticos.com/legislacion/espana.shtml España. 13/09/15

PassMark Software (2015). “Create Disk Images”. http://www.osforensics.com/tools/create-disk-images.html España. 13/09/15

FarStone (2015). “Drive Clone”. http://www.farstone.com/software/drive-clone.php España. 13/09/15

Acronis (2015). “Acronis”. http://www.acronis.com/ España. 13/09/15

Digital Forensics Framework (2015). “Digital Forensic”. http://www.digital-forensic.org/ España. 13/09/15

X-Ways (2015). “Forensic”. http://www.x-ways.net/forensics/index-m.html España. 13/09/15

Clonezilla (2015). “Clonezilla Live”. http://clonezilla.org/clonezilla-live.php España. 13/09/15

Caine (2015). “Caine Live”. http://www.caine-live.net/ España. 13/09/15

Open Computer Forensics Architecture (2015). “Ocfa Source”. http://ocfa.sourceforge.net/ España. 13/09/15

SANS DFIR (2015). “Digital Forensics”. http://digital-forensics.sans.org/ España. 13/09/15

Guidance Software (2015). “EnCase Forensic”. https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Search.aspx España. 13/09/15

Arsenal Recon (2015). “Recon”. http://www.arsenalrecon.com/apps/recon/ España. 13/09/15

Brian Carrier (2015). “The Sleuth Kit”. http://www.sleuthkit.org/sleuthkit/desc.php España. 13/09/15

Volatility Foundation (2015). "Volatility". http://www.volatilityfoundation.org/ España. 13/09/15

Windows Scope Forensics & Cyber Security Tools (2015). "Windows Scope". https://www.windowsscope.com/index.php España. 13/09/15

Oxygen Forensics (2015). "Oxygen Forensics". http://www.oxygen-forensic.com/es/ España. 13/09/15

digitalcorpora.org (2015). "Bulk Extractor". http://digitalcorpora.org/downloads/bulk_extractor/ España. 13/09/15

Gianluca Costa & Andrea De Franceschi (2015). "Xplico". http://www.xplico.org/ España. 13/09/15

FireEye (2015). "Redline". https://www.mandiant.com/resources/download/redline España. 13/09/15

Paraben Corporation (2015). "P2 eXplorer". https://www.paraben.com/p2-explorer.html España. 13/09/15

Plainsight (2015). "Plainsight". http://www.plainsight.info/ España. 13/09/15

MSAB (2015). "XRY Office". https://www.msab.com/products/office/ España. 13/09/15

e-fense Carpe Datum (2015). "Helix3 Enterprise". http://www.e-fense.com/h3-enterprise.php España. 13/09/15

ARC (2015). "ProDiscover Basic". http://www.arcgroupny.com/products/prodiscover-basic/ España. 13/09/15

Access Data (2015). "Forensics Toolkit ftk". http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk España. 13/09/15

HDD Software (2015). "Hex Editor Neo". http://www.new-hex-editor.com/ España. 13/09/15

Associazione DEFT (2015). "deft". http://www.deftlinux.net/ España. 13/09/15

NirSoft (2015). "Computer Activity View". http://www.nirsoft.net/utils/computer_activity_view.html España. 13/09/15

mh-nexus (2015). "HxD". http://mh-nexus.de/en/hxd/ España. 13/09/15

Net Grab Ltd (2015). "NetSleuth". http://netsleuth.software.informer.com/1.6b/ España. 13/09/15