Las mejores 20 herramientas de Investigación Forense Digital

Fuente: Talk Tech To Me

Traducción: Ing. Mauro D. Gioino y Fernando Raviola del grupo de Investigación SegUTN de la Universidad Tecnológica Nacional FR San Francisco para Segu-Info

Versión: 1.0 (20131026)

1. Introducción

Aquí se presentan 20 de las mejores herramientas gratuitas que le ayudarán a conducir una investigación forense digital.

Ya sea para un caso interno de recursos humanos, una investigación sobre acceso sin autorización a un servidor o solo para aprender algo nuevo, estas suites y utilidades le ayudarán a llevar a cabo análisis forenses de memoria, análisis forenses de disco duro, análisis de exploración de imágenes, obtención de imágenes forenses y análisis forenses de dispositivos móviles. Como tales, todas proveen la posibilidad de recuperar información exhaustiva sobre lo que pasa "detrás de las cortinas" de un sistema de información.

Se debe tener en cuenta que esta lista está lejos de ser extensiva y puede no cubrir todo lo que se necesite para una investigación particular. Además, es posible que necesite utilidades adicionales como visores de archivos, generadores de hash y editores de textos. Para encontrar este tipo de software, puede visitar o artículos como: 101 Herramientas de administración Gratuitas, Top 10 Free Troubleshooting Tools for SysAdmins, Top 20 Free Network Monitoring and Analysis Tools for Sys Admins y Top 20 Free File Management Tools for Sys Admins. Estos artículos tratan muchas de las herramientas que pueden resultar útiles para realizar investigaciones forenses digitales (por ejemplo: BackTrack y la Suite SysInternals o la Suite de herramientas NirSoft).

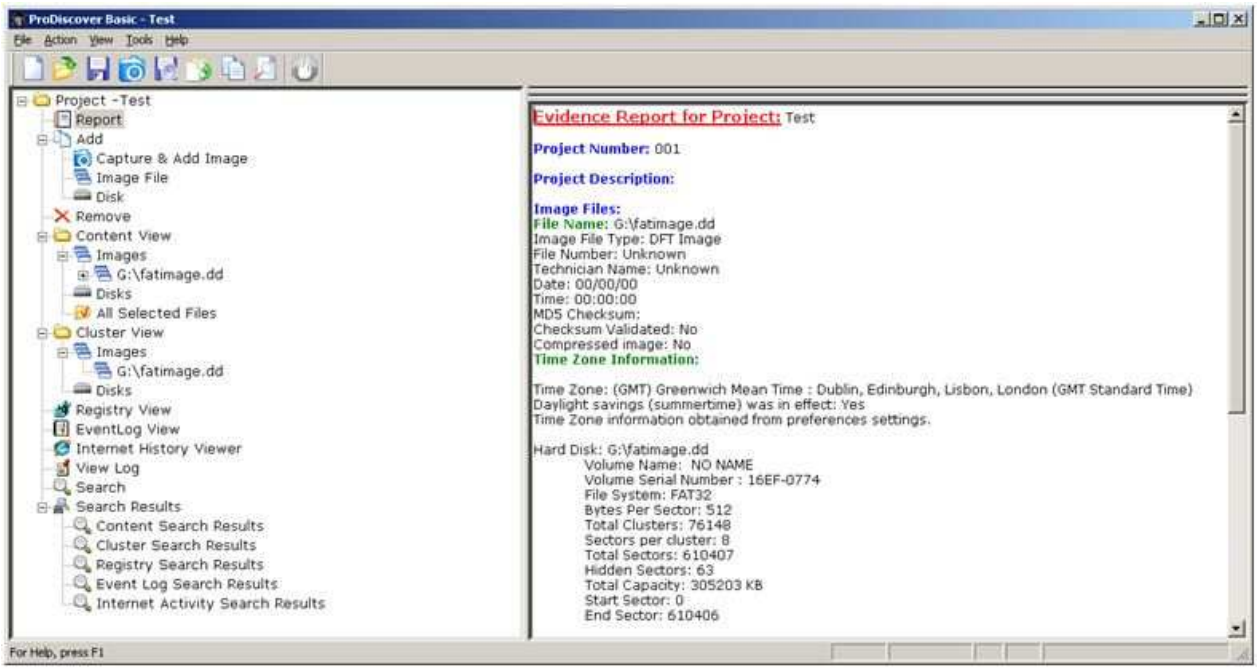
01. SANS SIFT

SANS SIFT (Conjunto de herramientas para investigación forense) es un Live CD basado en Ubuntu que incluye todas las herramientas necesarias para conducir una investigación forense o una investigación de respuesta a incidentes. Soporta análisis de Formato Testigo *Experto (Expert Witness Format E01)*, Formato Forense Avanzado (AFF), y Formatos de evidencia prima (RAW dd evidence formats). SIFT incluye herramientas como *log2timeline* para generar una línea de tiempo a partir de logs del sistema, *Scalpel* para hacer file carving, *Rifiuti* para examinar la papelera de reciclaje, entre otros.

Cuando inicie por primera vez el ambiente de SIFT, es importante explorar la documentación presente en el escritorio para conocer las herramientas disponibles y cómo usarlas. Existe también una buena explicación de dónde encontrar evidencia en un sistema. El menú superior contiene accesos a las distintas herramientas, también se puede ejecutarlas desde la terminal.

02. ProDiscover Basic

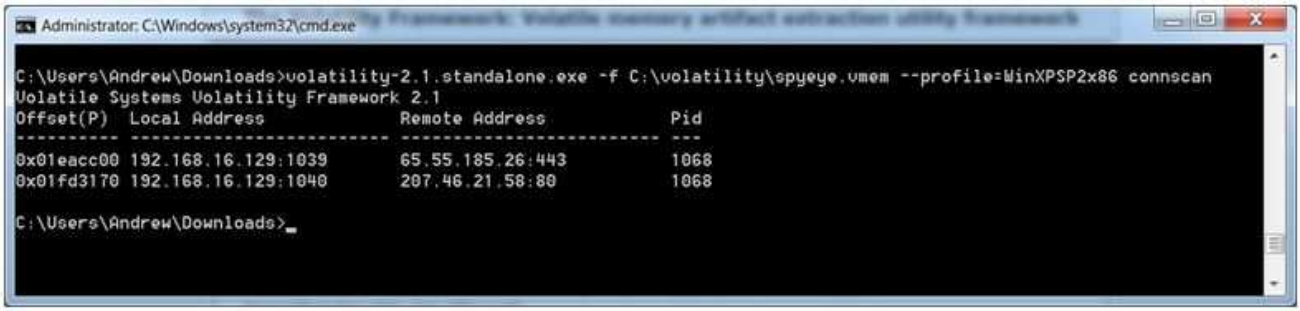
ProDiscover Basic es una herramienta simple para investigación forense digital que permite tomar imágenes, analizarlas y reportar evidencia encontrada en una unidad de disco. Una vez que añada una imagen forense, podrá listar los datos por contenido o accediendo a los *clusters* que contienen los mismos. Puede también buscar datos usando el nodo *Buscar* basándose en los filtros que se especifiquen.



Cuando ejecute la herramienta, necesitará cargar o crear un proyecto y una evidencia usando el nodo Add (Agregar). Luego, podrá usar los nodos 'Content View' o 'Cluster View' para analizar los datos y el menú de Herramientas para realizar acciones contra los mismos. Seleccionando el nodo 'Report' se puede ver información relevante sobre el proyecto.

03. Volatility

Volatility es un *framework* de análisis forense de memoria para respuesta a incidentes y análisis de malware que permite extraer artefactos digitales desde volcados de memorias volátiles (RAM). Usando Volatility podrá extraer información sobre procesos en marcha, sockets y conexiones de redes activas, DLLs cargadas para cada proceso, secciones de registros en caché, IDs de procesos, entre otros.



Si está usando la versión de Volatility autónoma para Windows, hay que ejecutar el archivo volatility-2.1.standalone.exe desde la consola. Para ello, navegue hacia la ubicación del ejecutable y tipee:

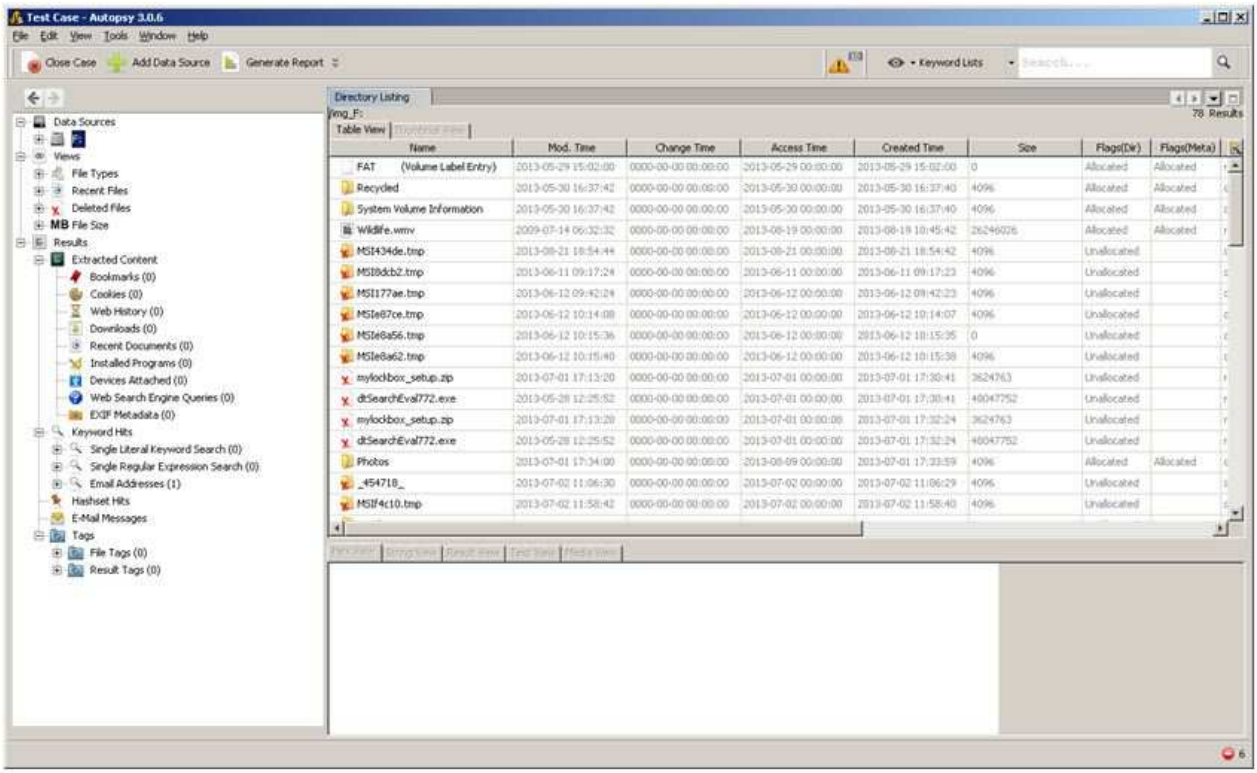
```
volatility-2.1.standalone.exe –f <FILENAME> –profile=<PROFILENAME>
<PLUGINNAME>
```

FILENAME sería el nombre del archivo de volcado de memoria que usted desee analizar, PROFILENAME sería la computadora desde donde el volcado de memoria fué tomado y PLUGINNAME sería el nombre del *plugin* que desee usar para extraer información.

Nota: En el ejemplo, se está usando el *plugin 'connscan'* para buscar información sobre conexiones TCP en el volcado de memoria fisico.

04. The Sleuth Kit (+Autopsy)

The Sleuth Kit es una caja de herramientas de código abierto para el análisis forense digital usado para realizar análisis profundos de varios archivos de sistemas. *Autopsy* es, en esencia, una GUI que se posiciona sobre el SleuthKit. Viene con funcionalidades incorporadas como análisis temporal, filtrado de hash, análisis de archivos del sistema y búsqueda de palabras claves. Además, permite agregar nuevos módulos para extender su funcionalidad.

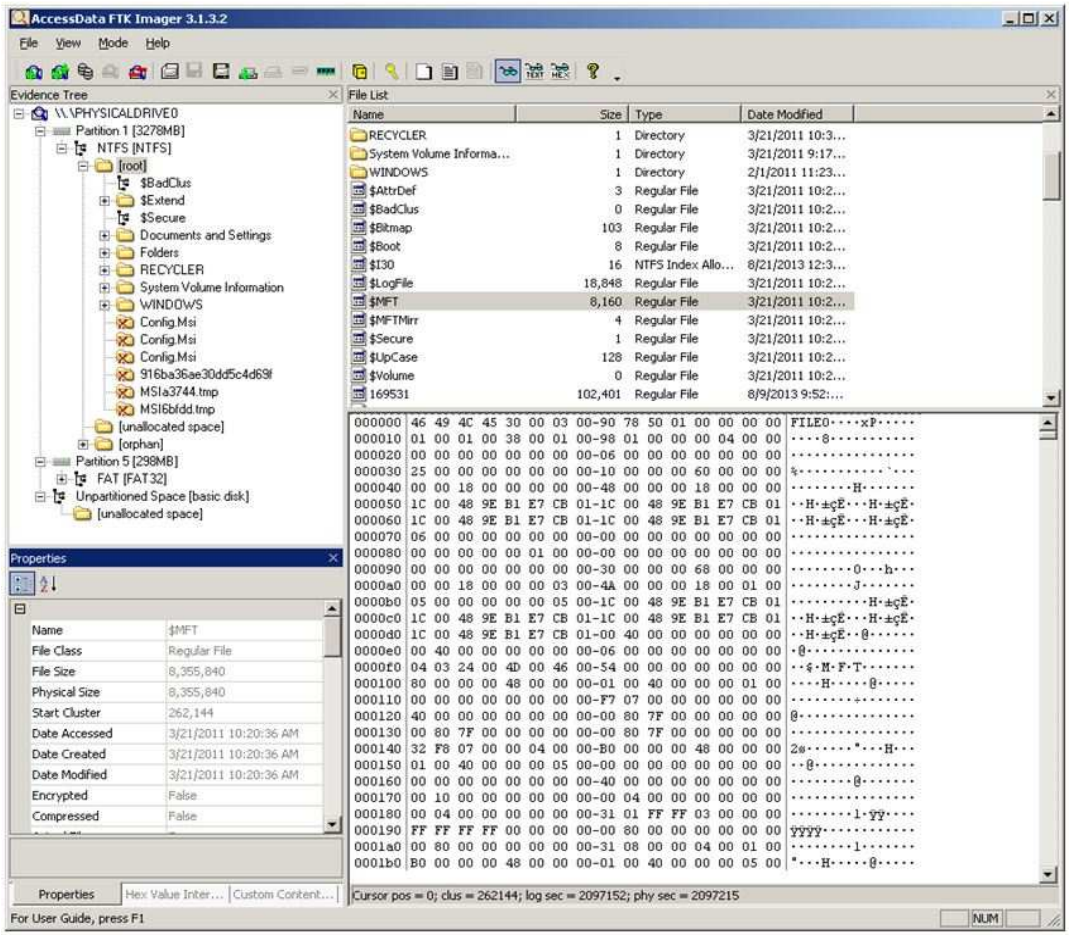


Cuando se ejecuta *Autopsy*, podrá elegir entre crear un nuevo caso o cargar uno existente. Si elige crear uno nuevo, necesitará cargar una imagen forense o disco local para empezar su análisis. Una vez que el proceso de análisis esté completo, deberá que utilizar los nodos del panel izquierdo para seleccionar qué resultados visualizar.

05. FTK Imager

FTK Imager es una herramienta de previsualización de datos y análisis de imágenes que permite examinar archivos y carpetas en discos duros locales, discos de red, CDs/DVDs, y visualizar contenido de imágenes forenses o volcados de memoria. Usando FTK Imager también podrá crear hashes de archivos SHA1 o MD5, exportar archivos y carpetas desde imágenes forenses a discos, revisar y recuperar archivos que fueron eliminados de la papelera (siempre que los bloques de datos no hayan sido sobreescritos), y montar una imagen forense para ver su contenido en Windows Explorer.

Nota: Hay una versión portable de FTK Imager que le permitirá ejecutarla desde un disco USB.



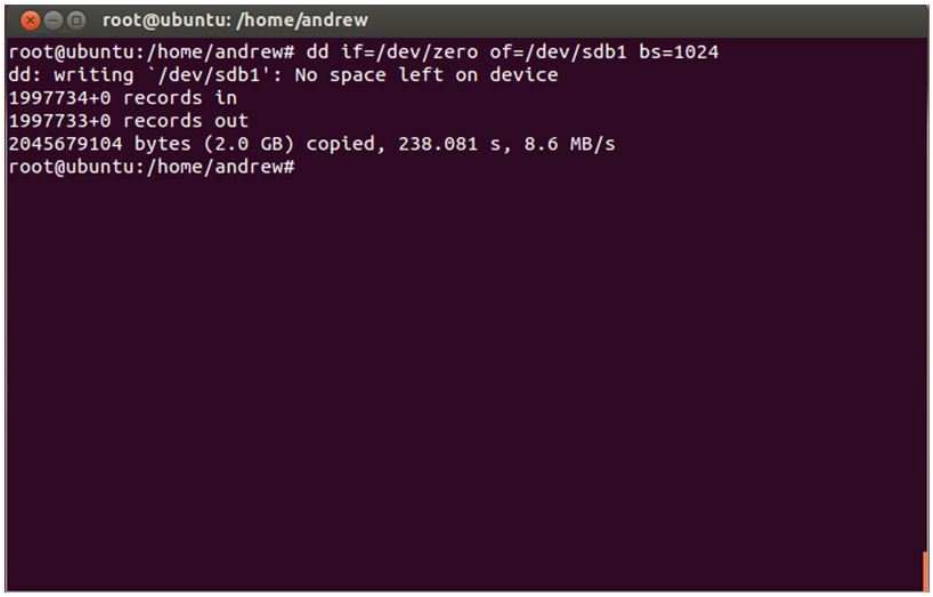
Cuando ejecute FTK Imager, ir a 'Archivo > Añadir Item de Evidencia…", para cargar una evidencia a considerar. Para crear una imagen forense, ir a "Archivo > Crear Imagen de disco…" y elija el destino de la imagen forense a crear.

06. Linux 'dd'

Por defecto, **dd** está incluido en la mayoría de las distribuciones de Linux disponibles hoy en día (Ubuntu, Fedora). Esta herramienta se utiliza para muchas tareas forenses tales como, limpiado de disco forense (puesta a cero de una unidad) y creación de imágenes crudas de unidad.

Nota: dd es una herramienta muy poderosa y puede causar efectos no deseados si no se usa con cuidado. Se recomienda que experimente en un ambiente seguro antes de utilizarla en el mundo real.

Consejo: en http://sourceforge.net/projects/dc3dd/ se puede encontrar una versión modificada de dd, dc3dd incluye características adicionales que fueron agregadas específicamente para tareas de adquisición forense digital.



Para utilizar dd, simplemente abra una terminal y tipee "dd" seguido de una serie de parámetros (los comandos a utilizar dependerán obviamente de la tarea que se quiera realizar). La sintaxis de dd básica para limpiado forense de disco es:

```
dd if=/dev/zero of=/dev/sdb1 bs=1024
```

Donde:

if = archivo de entrada
of = archivo de salida
bs = tamaño en bytes

Nota: reemplazar /dev/sdb1 por el nombre de la unidad que se desee limpiar y 1024 por el tamaño de bloque de bytes que se desee escribir.

La sintaxis básica para crear una imagen forense de unidad es:

```
dd if=/dev/sdb1 of=/home/andrew/newimage.dd bs=512 conv=noerror,sync
```

Donde:

if = archivo de entrada (o en este caso, unidad de entrada)
of = archivo de salida
bs = tamaño de byte
conv = opciones de conversión

Consejo**:** Para más información de uso, tipear “man dd” en la terminal (sin comillas) para abrir el manual de ayuda.

07. CAINE

CAINE (o Ambiente de INvestigación Asistido por Computadora por sus siglas en inglés) es un Live CD Linux que contiene una variedad de herramientas forenses. Entre las características más destacadas: presenta una GUI muy amigable, permite la creación de reportes semi-automáticos y herramientas para análisis forense de dispositivos móviles, redes, recuperación de información, entre otros.

Cuando se inicia el sistema en Linux CAINE, se pueden ejecutar las herramientas para análisis forense, ya sea desde su interfaz (acceso directo en el escritorio) o desde el ícono de acceso de cada herramienta en la carpeta “Herramientas Forenses” desde la barra de menú ‘Aplicaciones’.

08. Oxygen Forensic Suite 2013 Standard

Si se está investigando un caso que requiere reunir información desde un teléfono móvil, **Oxygen Forensics Suite** **(Standard Edition)** será de mucha ayuda.

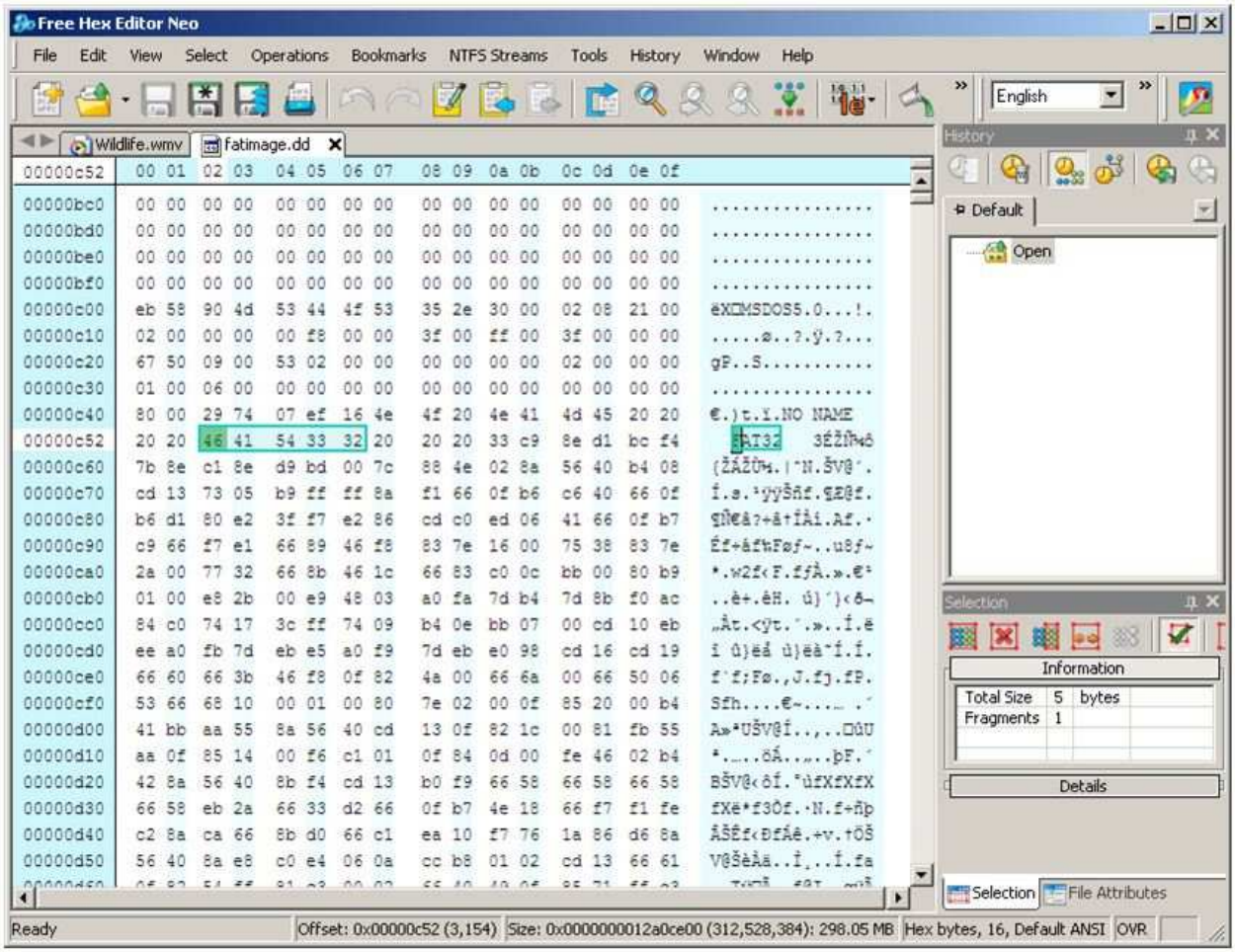
Entre sus funciones encontramos la posibilidad de extraer información de dispositivos (fabricante, plataforma de sistema operativo, IMEI, número de serie, etc) así como contactos y mensajes (e-mails, SMS, MMS, etc). Además es posible recuperar información del calendario, mensajes y registros de llamadas borradas. Viene con un explorador de archivos incorporado que permite acceder y analizar fotos, videos, documentos y bases de datos presentes en el dispositivo.

Cuando se ejecuta Oxygen Forensic Suite, hacer click en el boton ‘Conectar nuevo dispositivo’ que se encuentra en el menú superior para correr el asistente de extracción de

Oxygen Forensic que guiará en el proceso de selección del dispositivo y el tipo de información a extraer.

09. Free Hex Editor Neo

Free Hex Editor Neo es un editor básico hexadecimal diseñado para manejar archivos de gran tamaño. Aunque la mayoría de las características adicionales se encuentran en las versiones comerciales, esta herramienta es útil para cargar archivos de gran tamaño (base de datos o imágenes forenses) y realizar acciones como *data carving* manual, edición de archivos a bajo nivel, rejunte de información y búsqueda de datos ocultos.



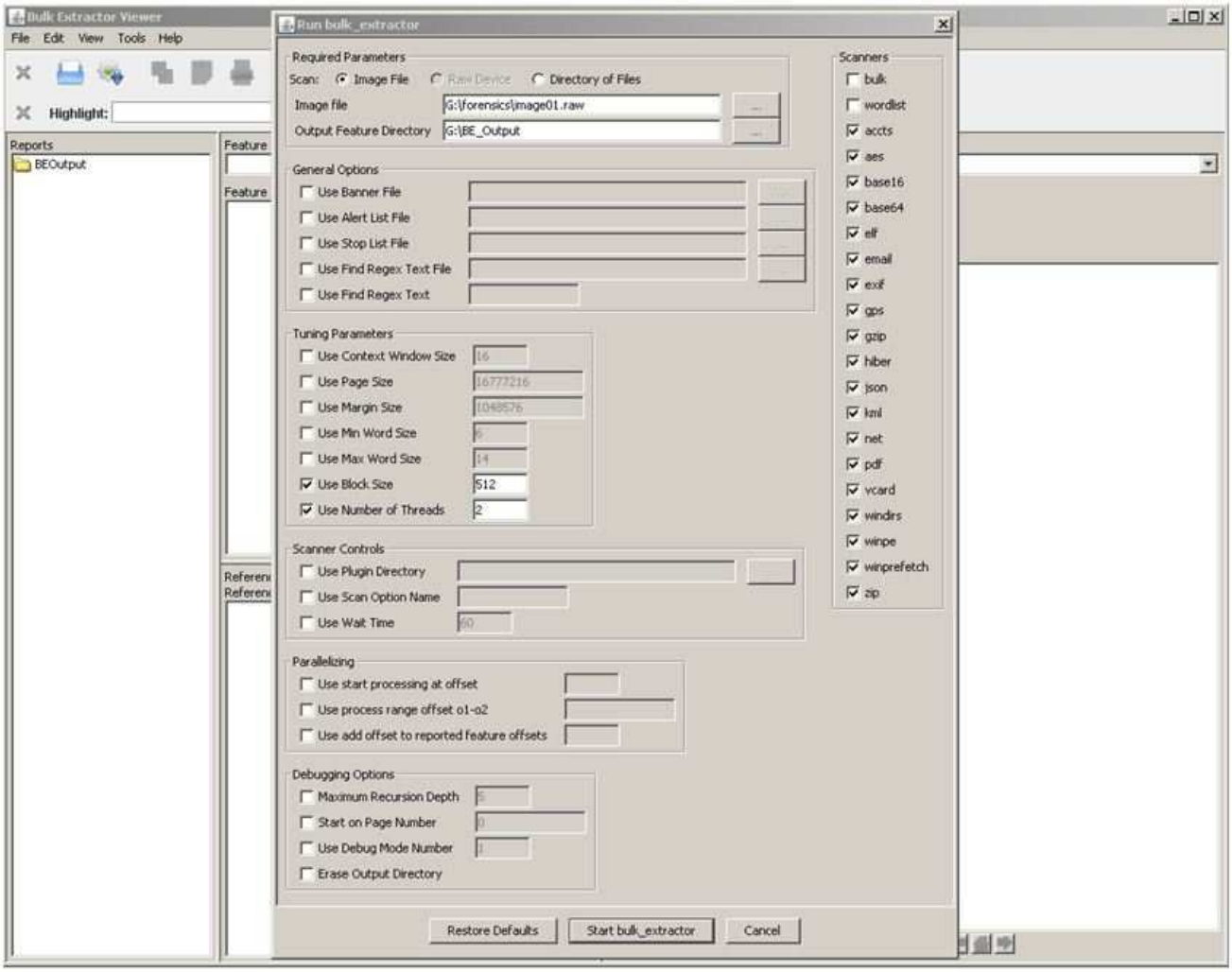
Ir a “Archivo > Abrir” para cargar un archivo en Hex Editor Neo. Los datos aparecerán en la ventana central donde puede navegar de forma manual o presionando CTRL + F para realizar una búsqueda.

10. Bulk Extractor

Bulk_extractor es una herramienta forense (existe una versión de línea de comandos y otra con GUI.) que escanea una imagen de disco, archivo o directorio de archivos en búsqueda de información como números de tarjetas de crédito, dominios, direcciones de e-mail, URLs y archivos ZIP.

La información extraída se muestra como una serie de archivos de texto (que pueden ser revisados manualmente o analizados usando otras herramientas forenses o scripts).

Consejo: dentro de los archivos de texto de salida se encontrarán registros de datos que se parecen a números de tarjetas de crédito, un e-mail, nombre de dominio, etc. Se verá también un valor decimal en la primera columna del archivo de texto que, cuando se convierte a hexadecimal, se puede usar como el puntero en el disco donde el registro fue encontrado.



En el ejemplo anterior se configura el extractor para extraer información de una imagen forense y mostrar los resultados en una carpeta llamada “BE_Output”. Los resultados se pueden ver en el visualizador de Bulk Extractor y en los archivos de texto mencionados anteriormente.

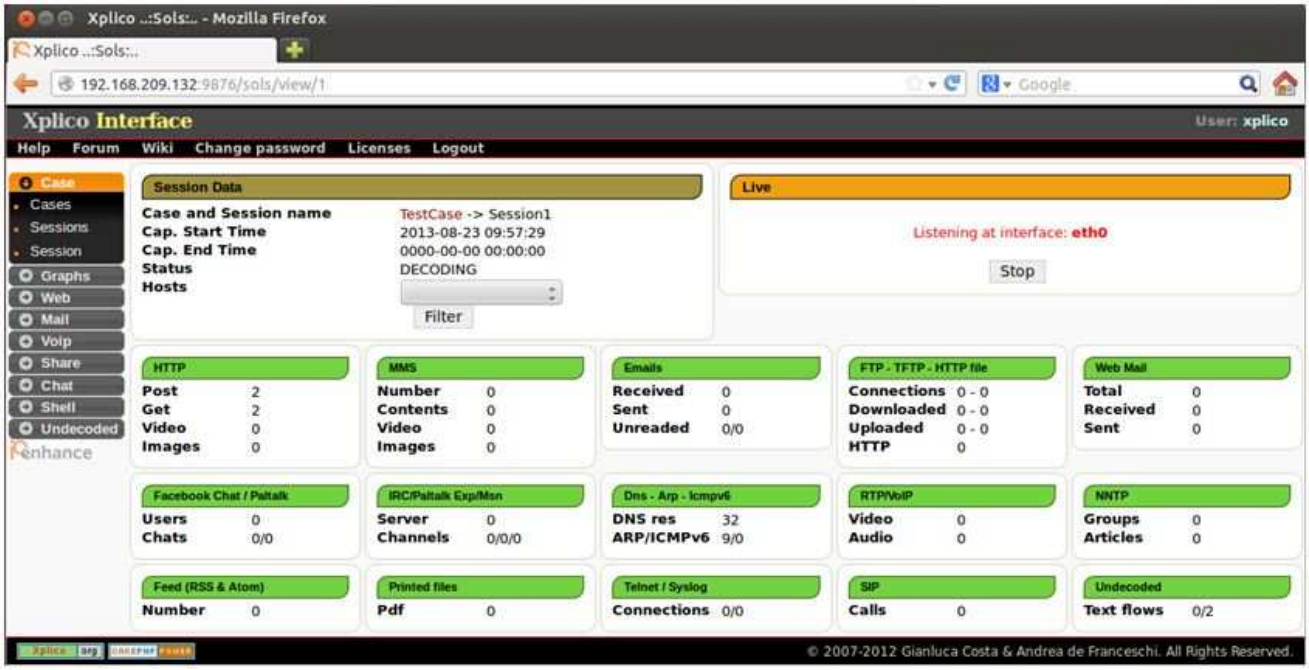
11. DEFT

DEFT es otro Live CD Linux que empaqueta algunas de las más populares herramientas gratuitas y Open Source disponibles. Está orientado a escenarios de respuesta a incidentes, ciber-inteligencia y computación forense. Además, contiene herramientas para análisis forense de móviles y de redes, recuperación de datos, hashing, entre otras.

Cuando inicia el sistema utilizando DEFT, se le preguntará si desea cargar el ambiente LIVE o instalar DEFT en el disco. Si carga el ambiente live, puede usar los accesos directos en la barra de menú de la aplicación para ejecutar las herramientas requeridas.

12. Xplico

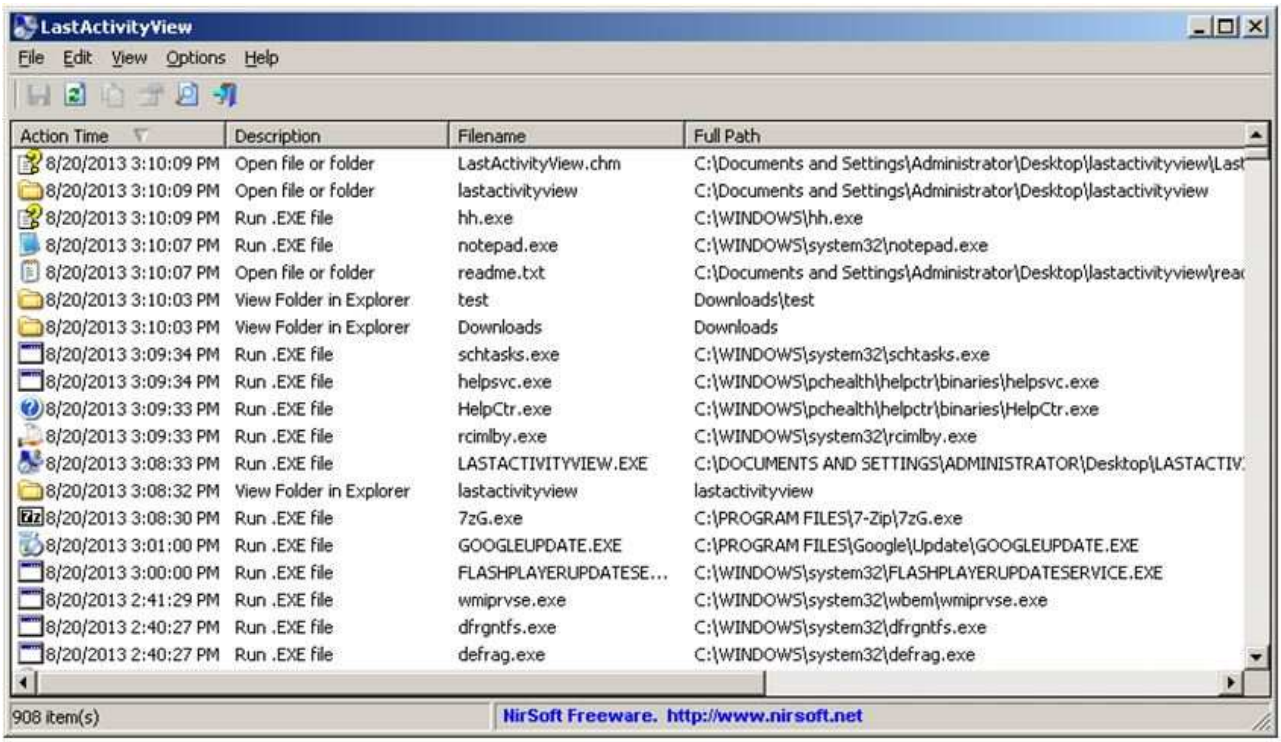
Xplico es una herramienta Open Source para el análisis forense de redes que apunta a extraer datos de aplicaciones desde tráfico de internet (por ejemplo, Xplico puede extraer un mensaje de e-mail desde tráfico POP, IMAP o SMTP). Sus características incluyen: soporte para una variedad de protocolos (HTTP, SIP, IMAP, TCP, UDP), reensamblaje TCP y la habilidad de mapear los datos extraídos a una base de datos MySQL o SQLite, entre otras.



Una vez que se haya instalado Xplico, se accede a la interfaz web en *http://<IPADDRESS>:9876* e identificándose con una cuenta de usuario normal. Lo primero que se necesita será crear un portafolio y añadir una nueva sesión. Cuando se crea la nueva sesión podrá cargar un archivo PCAP (obtenido de Wireshark, por ejemplo) o ejecutar una captura *live*. Una vez que la sesión haya finalizado de decodificar, en el menú de navegación de la izquierda puede ver los resultados.

13. LastActivityView

LastActivityView permite ver qué acciones fueron realizadas por un usuario y qué eventos ocurrieron en la máquina. Cualquier actividad tal como ejecutar un archivo, abrir un archivo/carpeta con el explorador, ejecutar una aplicación, una caída del sistema o una instalación de software, quedará registrada. La Información se puede exportar a archivos CSV, XML o HTML. Esta herramienta es útil para probar que un usuario (o cuenta de usuario) realizó una acción cuando la persona lo esté negando.

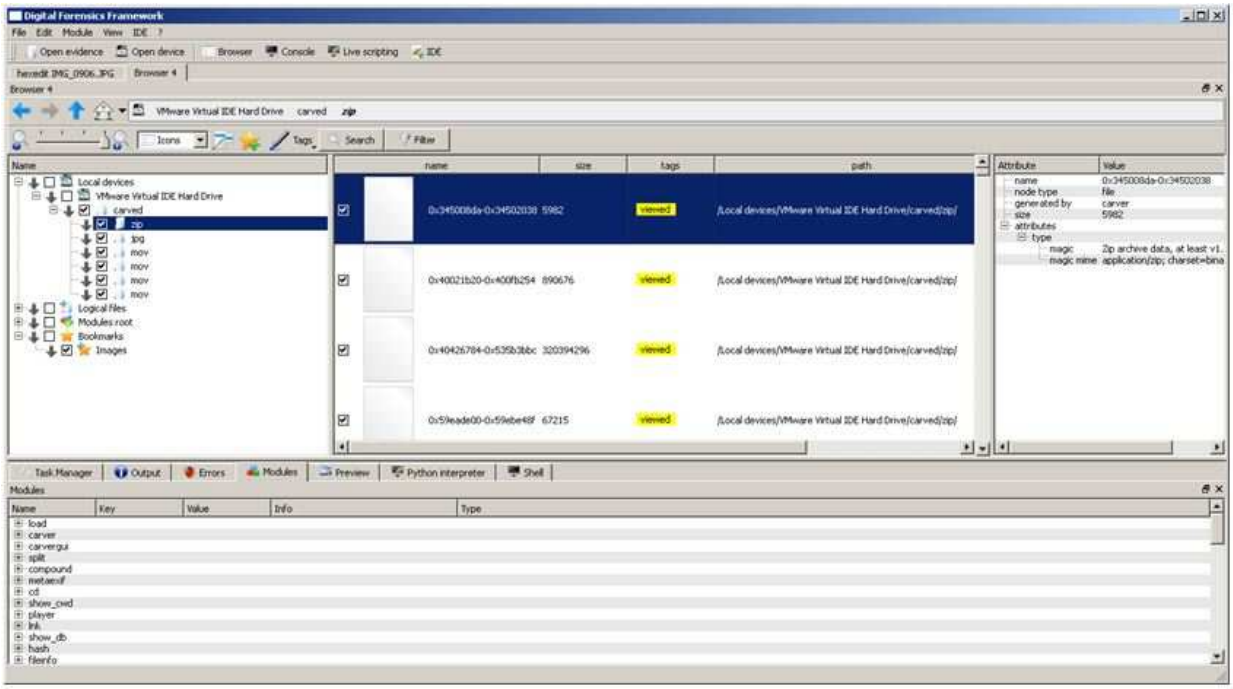


Cuando ejecuta LastActivityView, se vizualizarán automáticamente una lista de acciones realizadas en la máquina en la que se está corriendo el software. Filtre por tiempo de acción o use el botón Buscar para empezar a investigar qué acciones se realizaron en la computadora.

14. Digital Forensic Framework

El **Framework Forense Digital (DFF)** es una herramienta de investigación forense y una plataforma de desarrollo que permite recolectar, preservar y revelar evidencia digital.

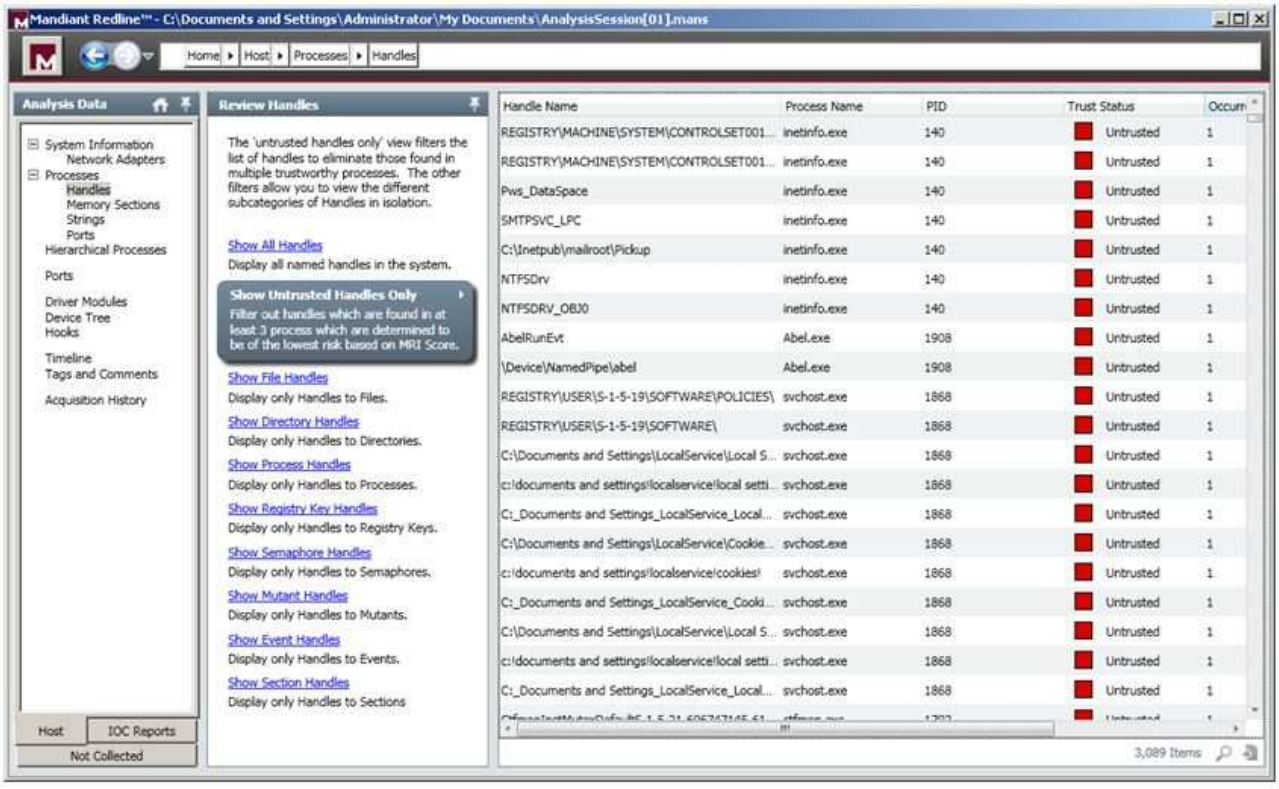
Entre otras características de DFF, incluyen la habilidad de leer formatos de archivos RAW, EWF y AFF, acceder a dispositivos remotos, analizar el registro, bandeja de entrada de e-mail, archivos de datos de sistemas y recuperar archivos escondidos o eliminados.



Cuando ejecute DFF, necesitará cargar un archivo de evidencia (por ejemplo, una imagen forense que haya obtenido previamente) o abrir un dispositivo listo para ser analizado. Luego, puede procesar el archivo de evidencia contra alguno de los módulos incorporados para empezar a analizar datos.

15. Mandiant RedLine

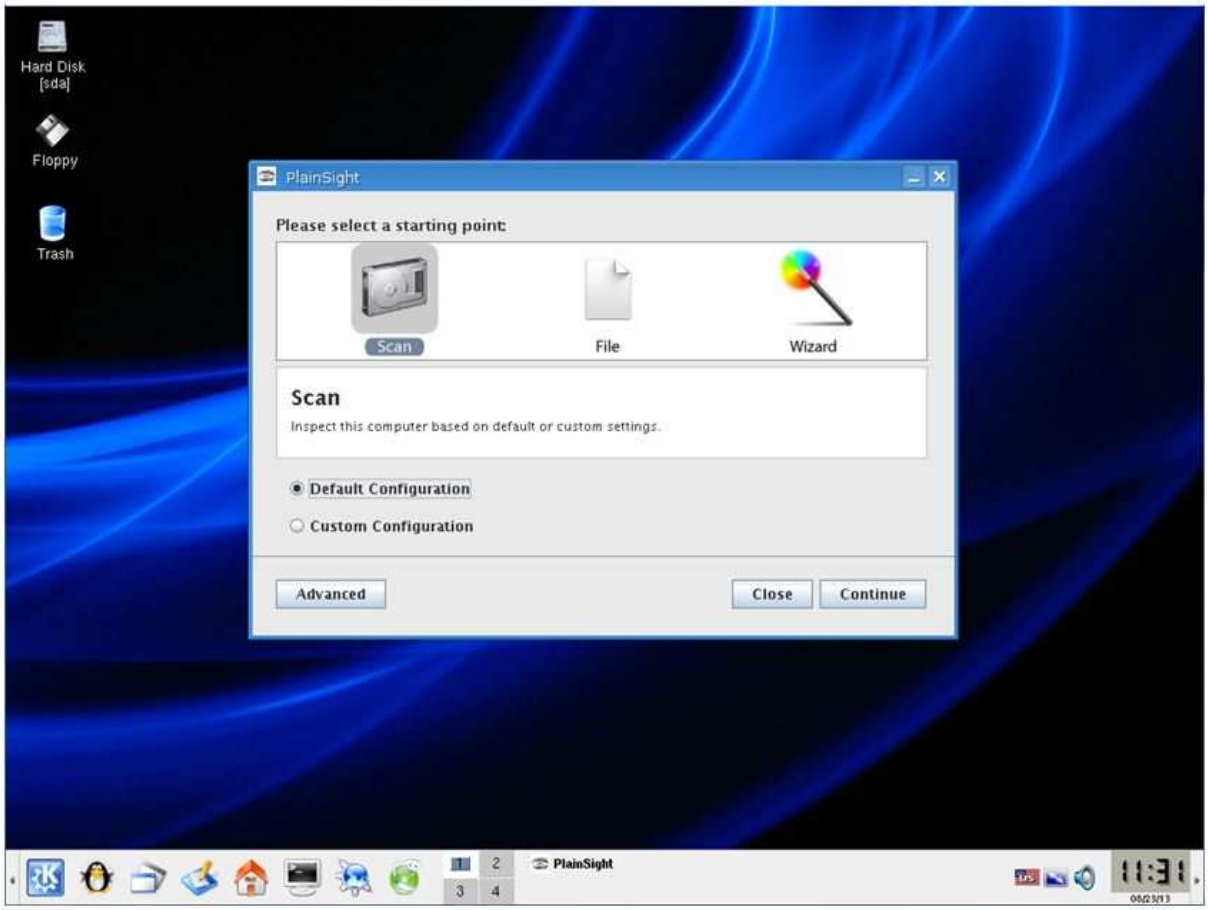
RedLine permite realizar análisis de memoria y archivos en un host específico. Recolecta información desde la memoria sobre los procesos en ejecución y drivers, busca archivos con metadatos de sistema, datos del registro, logs de eventos, información de red, servicios, tareas e historial de internet para ayudar a construir un perfil general de evaluación de amenazas.



Cuando ejecute RedLine, se le ofrecerá la opción de recolectar datos o analizarlos. A menos que ya se tenga un archivo de volcado de memoria disponible, necesitará crear un colector para reunir datos desde la computadora. Una vez que tenga el archivo de volcado de memoria, puede comenzar su análisis.

16. PlainSight

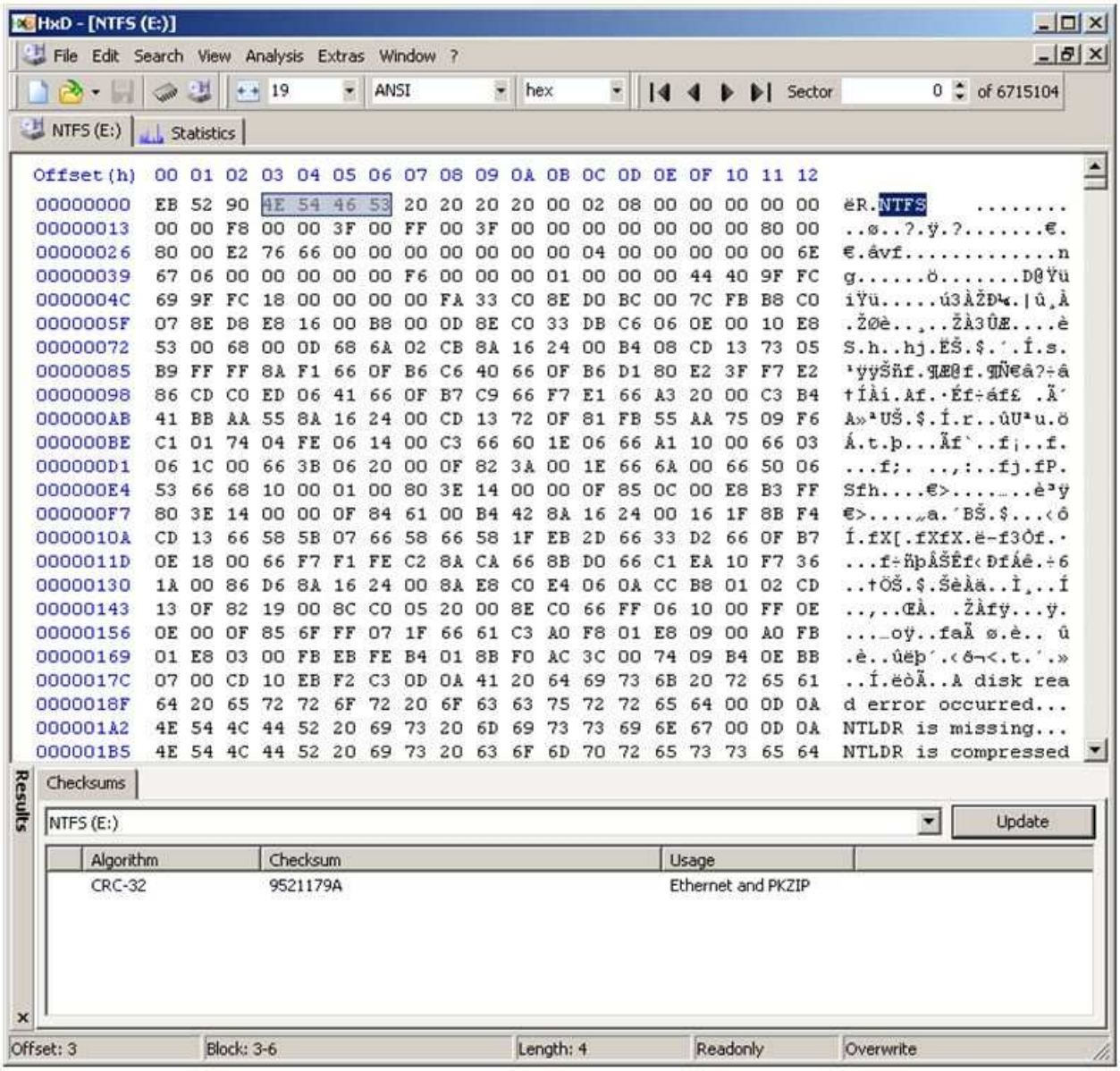
PlainSight es un Live CD basado en Knoppix (una distribución Linux) que permite realizar tareas forenses digitales como: visualización de historiales de Internet, recuperación de datos, recolección de información de uso de dispositivos USB, examinación de volcados de memoria física, extracción de passwords hashes y más.



Cuando *bootee* PlainSight, se le presentará una ventana preguntando si desea realizar un escaneo, cargar un archivo o correr el asistente. Seleccione una de las opciones para comenzar el proceso de extracción y análisis.

17. HxD

HxD es un editor hexadecimal amigable al usuario que permite realizar ediciones y modificaciones de discos o memorias principales (RAM) a bajo nivel. Hxd fué diseñado para ser fácil de usar y se desempeña perfectamente incluso con archivos de gran tamaño. Algunas de las características que posee son búsqueda y reemplazo, exportación, checksums/digests, un triturador de archivos incorporado, concatenación o división de archivos, generación de estadísticas y más.



En interfaz de inicio de HxD se puede abrir un archivo desde File > Open, cargar un disco desde Extras > Open disk, o cargar un proceso de la RAM desde Extras > Open RAM.

18. HELIX3 Free

HELIX3 es una LiveCD basado en Linux que fue construido para ser usado en Respuesta a incidentes, computación forense y escenarios de e-Descubrimiento. Tiene muchas herramientas de código abierto que van desde editores hexadecimales a software de *carving* de datos a utilidades de *crackeo* de contraseñas y mucho más.

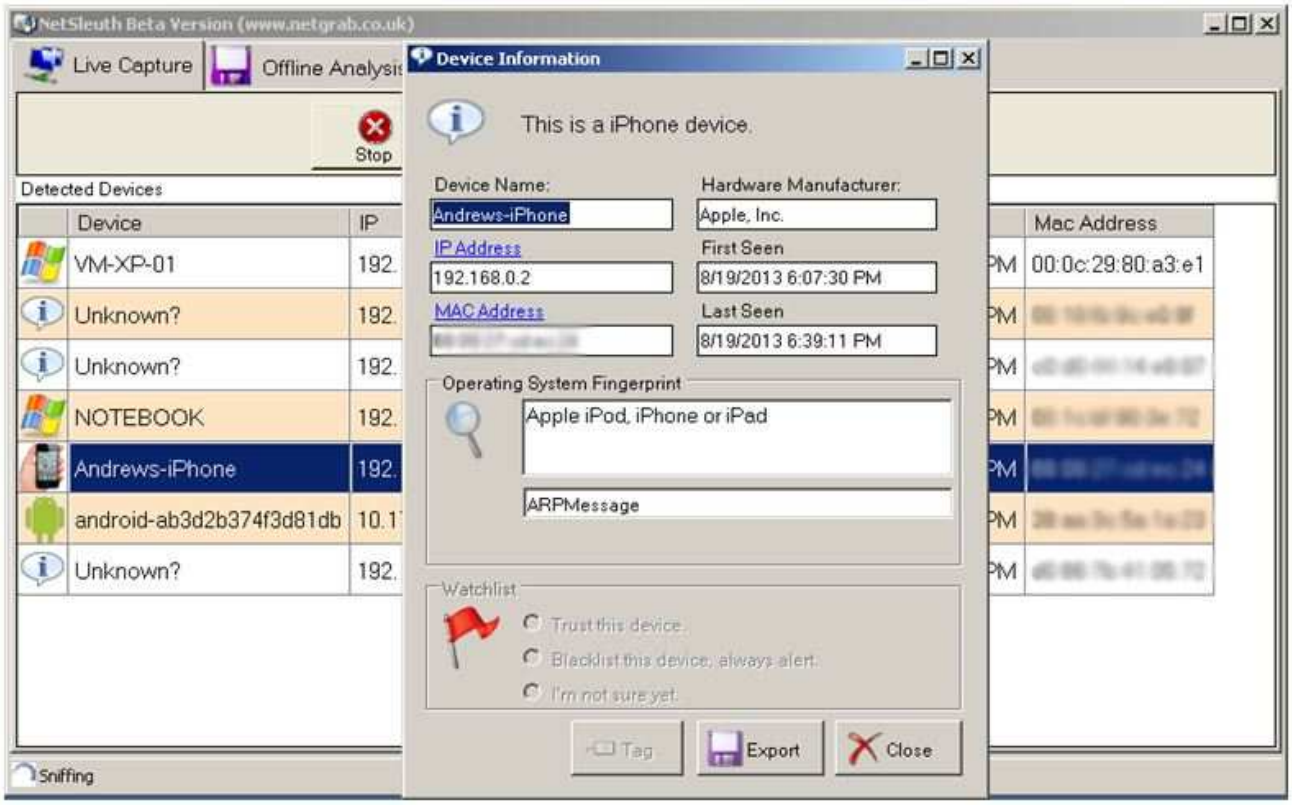
Nota: la versión de HELIX3 que se necesita es 2009R1. Esta versión fue la última disponible antes que HELIX fuera tomada por un proveedor comercial.

Cuando bootea, pregunta si uno quiere cargar la GUI o instalar HELIX3 en el disco. Si se elige cargar la GUI directamente (lo recomendado), una pantalla basada en Linux aparecerá dando la opción de ejecutar la versión gráfica del conjunto de herramientas incluidas.

19. NetSleuth

NetSleuth es una herramienta de análisis forense en red que identifica los dispositivos sobre la red. Opera en modo 'live' (donde activamente captura los paquetes de la red e interpreta la información de los dispositivos) o en modo 'offline' donde procesará un archivo PCAP que el usuario importe.

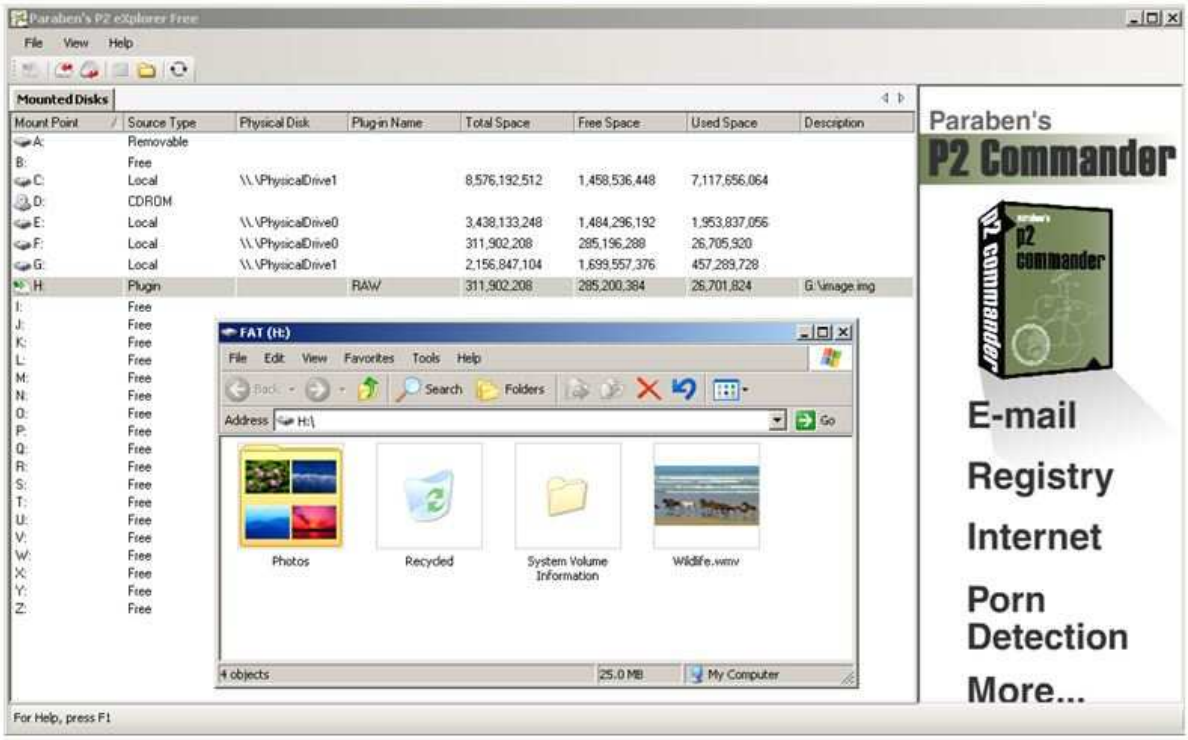
Nota: al momento de escribir este documento dicha herramienta está en Beta. Entonces no se recomienda ejecutar en entorno de producción. Se incluyó a la lista porque promete ser un interesante agregado al *toolkit* forense. El autor de esta herramienta está actualmente solicitando el *feedback* de la comunidad por lo tanto ahora está la chance de contribuir.



Cuando se ejecuta la herramienta, es posible iniciar un análisis 'live' desde la pestaña Live Capture o cargar un archivo PCAP desde la pestaña Offline Analysis. Una vez que NetSleuth ha identificado al menos un dispositivo, se podrá hacer doble click sobre el item para abrir una ventana con la información del mismo.

20. P2 eXplorer Free

Paraben P2 eXplorer es una herramienta forense para montar imágenes que permite montar las mismas como un disco físico y ver el contenido de esa imagen en Windows Explorer o cargarla dentro de una herramienta de análisis forense externa. Soporta imágenes en formatos RAW, DD, IMG, EX01, SMART y SafeBackt, entre otros.



Cuando se ejecuta la herramienta, se debe elegir una letra disponible para montar la imagen y luego ir a File > Mount Image… para elegirla. Una vez montada, con doble click sobre la letra asociada permitirá ver el contenido de esa imagen en Windows Explorer.

Consejo**:** en **Top 20 Free Disk Tools for SysAdmins** se menciona otra herramienta para montar imágenes llamada **OSFMount**. Es muy similar a P2 eXplorer pero también soporta montar archivos VMWare y la creación de discos RAM. Parte de la familia de OSFMount es una suite forense digital llamada OSForensics (la versión freewre de esta aplicación está disponible para uso personal, educativo o de hogar para permitir experimentar y familiarizarse a los conceptos forenses digitales).