Estudio sobre software gratuito para peritos tecnológicos

Fco. Javier Marqués Pons
Ingeniero y Máster en Telemática
Vicedecano COGITTCV Colegiado Nº 9724
www.javiermarques.com // javiermarques@coitt.es

La pregunta más extendida siempre es: ¿Cuáles son las mejores herramientas forenses apara trabajar como perito o forense tecnológico? La respuesta, como podréis comprender es casi imposible de contestar porque existen programas, aplicaciones y herramientas que no paran de evolucionar, y de lo que hablemos en este pequeño estudio, en 5 meses habrá cosas mejores y más actualizadas. Aun así, vamos a estudiar algunas herramientas gratuitas y muy pocas de pago que nos ayudaran en el campo del análisis forense en telemática, para casos simples como análisis de memoria, de discos duros, de imágenes, de capturar todo lo que pase por una red… Repito que no es una lista exhaustiva, y que cada caso es diferente con lo que habrá que ampliar a otras herramientas.

ÍNDICE DE LOS GRUPOS DE SOFTWARE ESTUDIADOS

- Herramientas gratuitas de solución de problemas
- Administrar Sistemas y Redes
- Prueba del sistema y solución de problemas
- Archivo y gestión de discos
- Rendimiento y supervisión de disponibilidad
- Herramientas forenses para una pericial tecnología completa

incluyen herramientas de recuperación de la contraseña, herramientas de Internet, herramientas de programación y herramientas del sistema, todos los cuales pueden ser utilizados para la recopilación de información y la resolución de problemas.

Entre las más importantes para el análisis forense esta **USBDeview**, que nos muestra todos los dispositivos USB actuales y conectados anteriormente en un equipo local o remoto con mucha información de cada uno de ellos;

HERRAMIENTAS GRATUITAS DE SOLUCIÓN DE PROBLEMAS

1. Grabación de acciones (Problem Steps Recorder)

En Windows 7 y Windows 8 es una pequeña utilidad muy práctica llamada Problem Steps Recorder (psr.exe). La grabación de acciones registrará las interacciones paso a paso que se producen cuando el usuario reproduce el problema, realizar capturas de pantalla de cada acción. Luego utilizas todo esto en un informe con información detallada y los registros de errores relevantes.

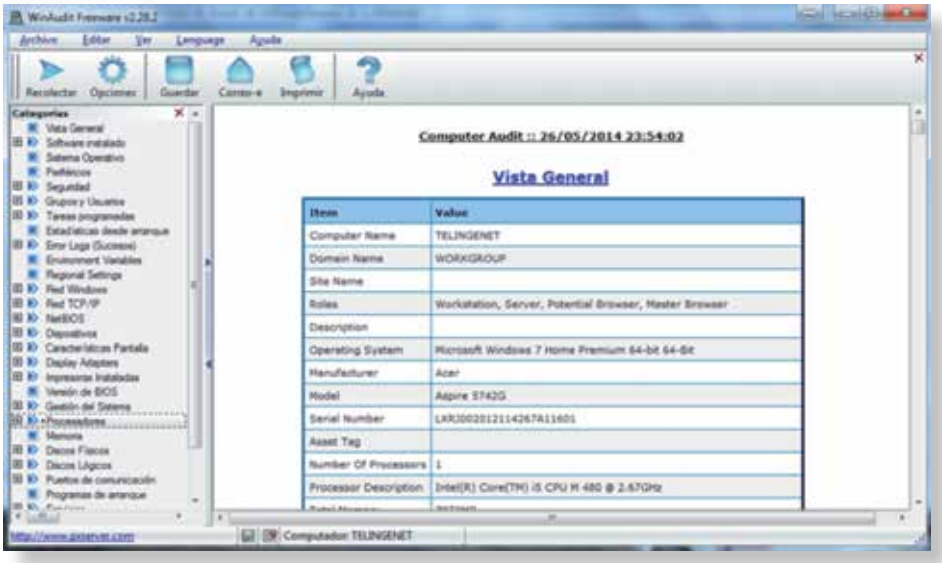
Esta herramienta es ideal para estudiar los problemas de un usuario, o para que un notario, después de dar fe, pueda llevarse pruebas con la consiguiente cadena de custodia.

Para iniciar el Problem Steps Recorder, vaya a ejecutar y escriba psr. exe. Haga clic en Iniciar Grabación y la herramienta registra cada interacción a partir de ese momento. Se puede agregar comentarios durante el proceso.

2. WELT (Windows Error Lookup Tool).

Windows muchas veces nos arroja un error que no sabemos muy bien lo que significa. Esta herramienta nos indica qué significa el código de error y con que está relacionado.

Parece una herramienta no muy útil si pensamos que poniendo el error en Google nos sale, pero muchas veces no podemos tener conexión a Internet en una pericial, y tampoco podemos utilizar otro ordenador en el momento indicado, por lo que se convierte en una herramienta bastante útil.



3. WinAudit

Como parte del proceso de solución de problemas, es útil saber la mayor información posible sobre la máquina donde reside el problema para ayudar a encontrar una solución más rápidamente. WinAudit analiza el equipo y reúne toda una serie de información sobre el software instalado, TCP/IP, unidades, registros…

Para iniciar una auditoria de su equipo local, sólo tiene que ejecutar WinAudit para iniciar la aplicación. Una vez que la auditoria se haya completado, usted puede comenzar a revisar la información de las diferentes categorías en el panel de la izquierda, o guardar la información en un archivo PDF/CSV/TXT/HTML.

4. NirLauncher Nirsoft

NirLauncher es una aplicación que agrupa a más de 170 utilidades gratuitas portátiles. Las herramientas disponibles

WINDOWS MUCHAS VECES NOS ARROJA UN ERROR QUE NO SABEMOS LO QUE SIGNIFICA. WELT NOS INDICA QUE SIGNIFICA EL CÓDIGO DE ERROR Y CON QUE ESTÁ RELACIONADO

y también **CurrPorts**, que nos muestra una lista de todos los puertos TCP/UDP abiertos actualmente en la máquina local. Información sobre el proceso que abrió el puerto, el momento de crear el proceso y el usuario que lo creó se muestra. También puedes cerrar conexiones abiertas y exportar la información a un archivo.

5. WSCC (Windows System Control center)

WSCC no es una herramienta de solución de problemas en sí, pero sí facilita el tema de solución de problemas. Le permite instalar, actualizar, ejecutar y clasificar toda la colección de herramientas en un solo lugar, de entre más de 270 herramientas.

ADMINISTRAR SISTEMAS Y REDES

6. Xirrus WIFI Inspector

WIFI Inspector es una potente gestión de WIFI y una herramienta de solución de problemas que le permite localizar y verificar los dispositivos WIFI, detectar puntos de acceso, solucionar problemas de conexiones y la búsqueda de redes WIFI.

7. Whois

Whois realiza una búsqueda de la información de registro de una determinada dirección IP o nombre de dominio.

8. ShareEnum

Un aspecto de la seguridad de red de Windows que se suele pasar por alto son los recursos compartidos de archivo. Se produce una brecha de seguridad común cuando los usuarios definen los recursos compartidos del archivo con bajos niveles de seguridad, lo que permite que los usuarios no autorizados vean archivos privados. No existen herramientas integradas para listar los recursos compartidos visibles en una red ni su configuración de seguridad, pero *ShareEnum* llena este vacío y permite bloquear los recursos del archivo de la red.

Cuando se ejecuta *ShareEnum*, usa la enumeración NetBIOS para analizar todos los equipos dentro de los dominios accesibles, y muestra los recursos compartidos de archivo e impresión y su configuración de seguridad. Dado que sólo el administrador del dominio puede obtener acceso a todos los recursos de red, *ShareEnum* es más efectivo si se ejecuta desde una cuenta de administrador de dominio.

9. TCP View

TCPView es un programa de Windows que muestra listados detallados de todos los extremos de TCP y UDP del sistema, incluidas las direcciones locales y remotas y el estado de las conexiones TCP. En Windows TCPView informa también del nombre del proceso que posee el extremo. TCPView ofrece un subconjunto más informativo y perfectamente presentado del programa Netstat incluido con Windows. La descarga de TCPView incluye Tcpvcon, una versión de línea de comandos con la misma funcionalidad.

NO EXISTEN HERRAMIENTAS INTEGRADAS PARA LISTAR LOS RECURSOS COMPARTIDOS VISIBLES EN UNA RED NI SU CONFIGURACIÓN DE SEGURIDAD, ShareEnum LLENA ESTE VACÍO Y PERMITE BLOQUEAR LOS RECURSOS DEL ARCHIVO DE LA RED

10. The Dude de MicroTik

Este software es muy interesante. Puede rastrear automáticamente todos los dispositivos dentro de una subred determinada y luego dibujar y diseñar un mapa de una red, pudiendo después hacer muchas acciones sobre cada elemento, ping, tracert, etc…

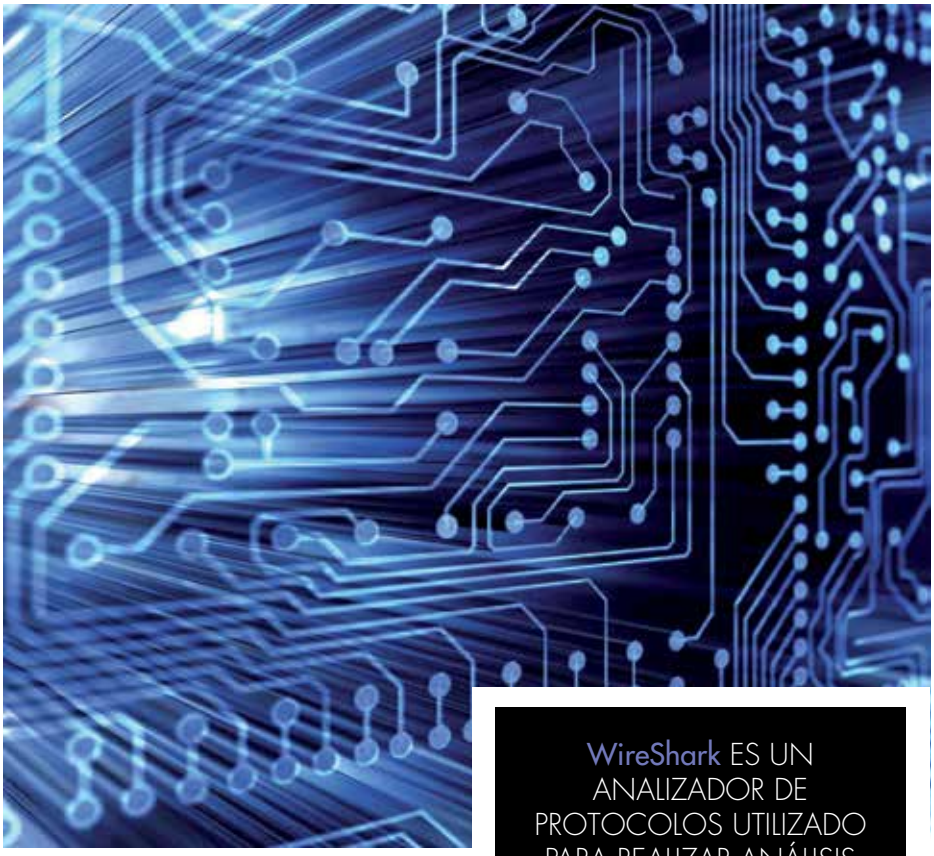
11. Microsoft Baseline Security Analyzer 2.2

Microsoft Baseline Security Analyzer (MBSA) es una herramienta fácil de usar que ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad de acuerdo con las recomendaciones de seguridad de Microsoft y ofrece orientación precisa sobre soluciones. Mejora el proceso de administración de seguridad mediante MBSA para detectar errores de configuración de seguridad habituales e identificar las actualizaciones que faltan en sus sistemas informáticos.

12. Wireshark

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos.

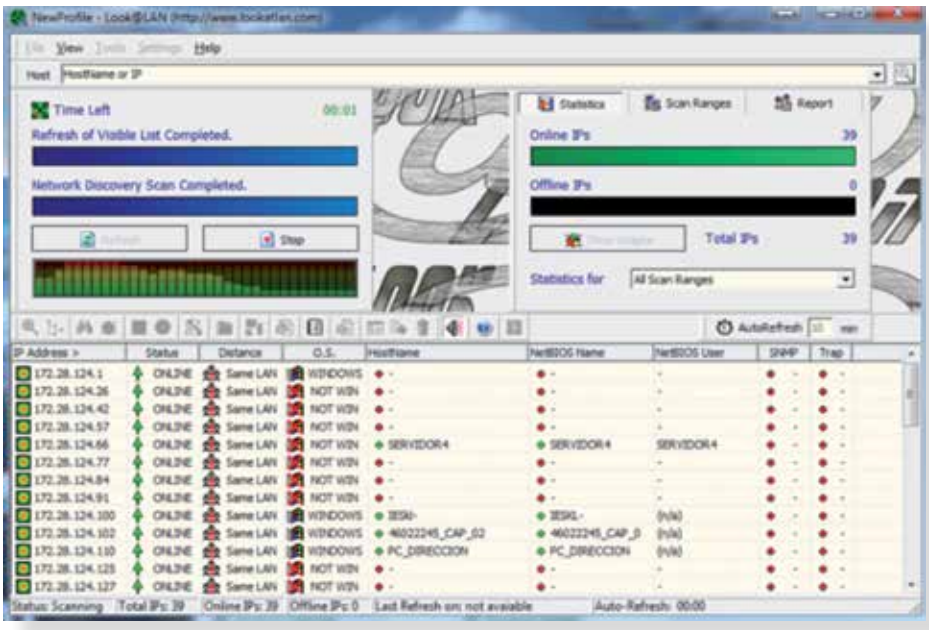
Permite examinar datos de una red en tiempo real o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.



WireShark ES UN ANALIZADOR DE PROTOCOLOS UTILIZADO PARA REALIZAR ANÁLISIS Y SOLUCIONAR PROBLEMAS EN REDES DE COMUNICACIONES, PARA DESARROLLO DE SOFTWARE Y PROTOCOLOS Y COMO HERRAMIENTA DIDÁCTICA

13. Look @LAN

Permite escanear rápidamente su red en busca de nodos activos. Proporciona monitoreo, reporte, registro y funciones de detección de sistema operativo y sus vulnerabilidades.



14. Capsa Network Analyzer

Con esta herramienta se puede monitorizar, diagnosticar y solucionar problemas en la red. Es muy potente, pero es gratuita solo unos días, después se convierte en software de pago.

15. Advanced IP Scanner

Esta herramienta permite realizar un seguimiento y administrar las direcciones IP de la red de forma rápida y sencilla.

16. PingPlotter

Es una aplicación tracert ligera que genera gráficos para ayudarte a visualizar la ruta de los paquetes desde el origen al destino.

17. SolarWinds

Con esta herramienta se puede visualizar rápidamente los permisos de usuario y grupo de una carpeta o unidad comparti-

da en un formato jerárquico. Puede seguir permisos de nivel de acción, ofrecer un desglose del nivel de recurso compartido y permisos a nivel de archivo y ayudar a identificar por qué algunos usuarios tienen los permisos que tienen.

18. WirelessNetView

Supervisa la actividad de las redes inalámbricas en la zona y muestra la información relacionada con ellos, tales como SSID, calidad de señal, MAC, canal, etc…

19. BluetoothView

Supervisa la actividad de los dispositivos Bluetooth en la zona y muestra la información relacionada con ellos, como el nombre del dispositivo, la dirección Bluetooth, tipo de dispositivo, etc…

20. Total Network Inventory

Es una aplicación de monitoreo de red integral que le permite ver el estado de su red. Es personalizable y tiene características de alerta, que le permite ver cuando algo no funciona bien o está mal.

WirelessNetView SUPERVISA LA ACTIVIDAD DE LAS REDES INALÁMBRICAS EN LA ZONA Y MUESTRA LA INFORMACIÓN RELACIONADA CON ELLOS, SSID, CALIDAD DE SEÑAL, MAC, CANAL…

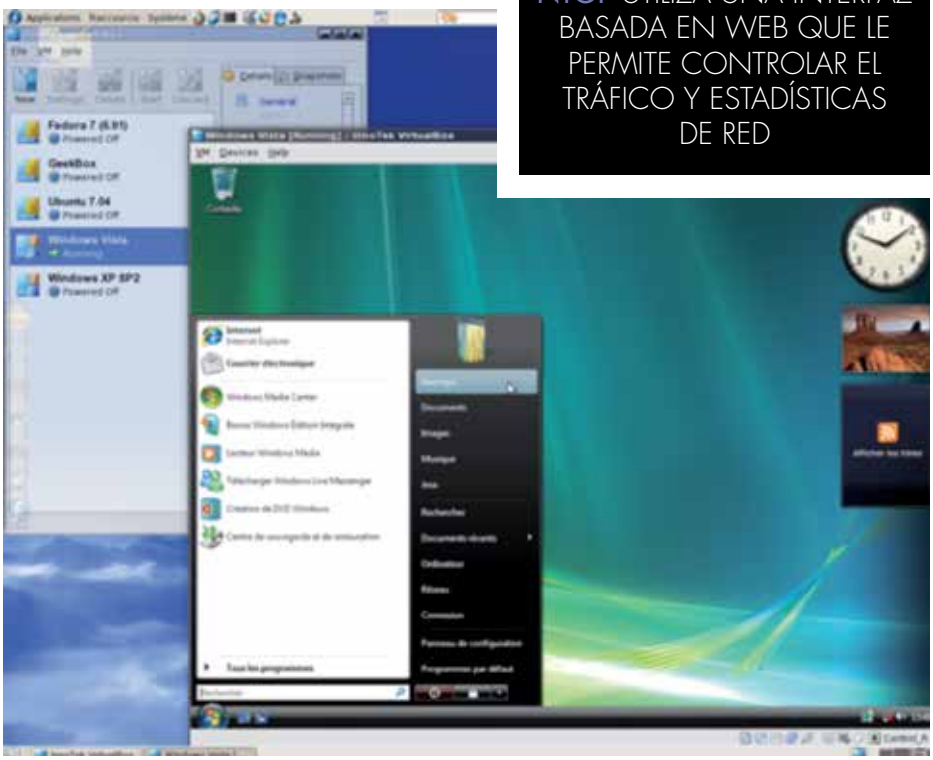
21. IIS Logfile Analyser

Esta herramienta permite analizar los archivos de registro de IIS para determinar estadísticas del sitio web, como el número de visitantes, el número de descargas, etc…

22. Ntop

Utiliza una interfaz basada en web que le permite controlar el tráfico y estadísticas de red.

NTOP UTILIZA UNA INTERFAZ BASADA EN WEB QUE LE PERMITE CONTROLAR EL TRÁFICO Y ESTADÍSTICAS DE RED



PRUEBAS DEL SISTEMA Y SOLUCIÓN DE PROBLEMAS

23. Oracle VirtualBox

Es una solución de virtualización gratuita, multiplataforma de uso general que se puede utilizar para crear y ejecutar múltiples máquinas virtuales. Ideal para entornos de prueba o desarrollo.

24. RAMMap

Permite analizar la asignación de memoria física en el sistema. Es capaz de determinar la cantidad de datos de archivo almacenados en la memoria RAM, la cantidad de RAM que es utilizada por los controladores del dispositivo, etc…

25. AppCrash View

Permite ver el informe de errores de Windows (.wer) archivos en una interfaz de usuario sencilla y luego guardar los resultados en formato de archivo TXT / CVS / HTML / XML.

26. RootkitRevealer

Le permite detectar la presencia de rootkits que funcionan al intentar ocultar sus archivos o entradas del registro.

27. ManagePC

Le permite crear un inventario de todas sus máquinas en el dominio, incluyendo hardware, software, dispositivos, parches, políticas de grupo, etc…

28. Pandora FMS

Es una solución de monitoreo de red que le permite controlar múltiples plataformas, desde máquinas Linux, a la máquina Solaris y a las máquinas Windows. Proporciona alertas e informes de CPU, disco y uso de memoria, la temperatura, o incluso los valores de la aplicación. Se ha convertido de pago, aunque hay una demo.

29. OCS Inventory

Es un inventario automatizado y la implementación de aplicaciones. Esto le permite determinar qué dispositivos o software están instalados en su red e implementar software o configuración de secuencias de comandos con una interfaz basada en la Web.

30. ExtraSpy Employee Monitor

Le permite monitorizar las actividades de los empleados a través de la red para ayudar a detectar el uso indebido de los bienes de la empresa o de las personas improductivas.

31. AdRestore

Permite recuperar objetos de servidor eliminados de Windows Server Active Directory.

ARCHIVO Y GESTIÓN DE DISCOS

32. Disk2vhd

Una herramienta que es capaz de sacar una copia online del disco físico sobre el cual está corriendo un Sistema Operativo posterior a Windows XP SP2 o Windows Server 2003 SP1 y la convierte al formato VHD que usan Windows Virtual PC, Virtual Server e Hyper-V. Y si lo hace sobre el disco de sistema, obviamente también sobre cualquier otro disco/partición de datos presente en el equipo.

33. Recuva

Con Recuva puede recuperar archivos que hayas eliminado accidentalmente de su máquina.

34. Bacula

Es un conjunto de aplicaciones que permiten la copia de seguridad, recuperación y verificación de los datos a través de una red.

RENDIMIENTO Y SUPERVISIÓN DE DISPONIBILIDAD

35. Axence Free Net Tools

Conjunto completo de herramientas de seguimiento, análisis de red, seguridad y administración, todo en una interfaz de usuario intuitiva y fácil.

36. Free IP Tools

Es un conjunto de herramientas comunes que se utilizan para solucionar problemas de las aplicaciones y servicios de red en una única interfaz. Incluye herramientas como PortScan, traceroute, SNMPAudit, etc…

HERRAMIENTAS FORENSES PARA UNA PERICIAL TECNOLÓGICA COMPLETA

37. Encase

Posiblemente es el paquete profesional más utilizado. Se trata de una herramienta comercial específica para el análisis forense de sistemas informáticos y telemáticos.

Entre otras muchas posibilidades, EnCase permite escanear discos, crear imágenes de discos para su posterior análisis, recuperar archivos de unidades que hayan sido formateadas, realizar borrado seguro de unidades a bajo nivel, consultas de archivos por tiempos de creación, último acceso y última escritura, identificación de extensiones de archivos, múltiples soporte de archivos. Permite el análisis sobre discos duros, dispositivos USB, tablets, smartphones… Y genera los informes adecuados, además de exportar evidencias.

38. Forensic Toolkit

FTK *(Forensic Tool Kit)* es otro paquete de herramientas forenses muy utilizado por los peritos tecnológicos. Al igual que el anterior, se trata de una distribución

Encase ES EL PAQUETE PROFESIONAL MÁS UTILIZADO. SE TRATA E UNA HERRAMIENTA COMERCIAL ESPECÍFICA PARA EL ANÁLISIS FORENSE DE SISTEMAS INFORMÁTICOS Y TELEMÁTICOS

comercial. Permite el análisis de correo electrónico y de archivos comprimidos, opciones de búsqueda de archivos y restauración de datos, así como múltiples archivos y formatos de adquisición.

39. Caine

Caine *(Computer Aided Investigative Environment)*. Es una distribución Live CD basada en Ubuntu. Ofrece un completo entorno forense, de modo que integra herramientas de software existentes, proporcionando una interfaz gráfica amigable. Precisamente éste es el punto clave de CAINE, su interfaz, que permite una integración sencilla y bastante amigable, con respecto a otras distribuciones Live CD.

Entre otras posibilidades, permite clonar y montar unidades, manipular volúmenes de diferentes sistemas operativos (Windows, Unix, Macintosh), recuperar archivos o borrarlos de forma segura, recuperar unidades de disco, auditar los dispositivos conectados a la red (incluso determinando qué puertos tienen abiertos), editores hexadecimales, recuperar archivos de imágenes y de vídeo, recuperar contraseñas, examinar el contenido de los archivos de respaldo que los móviles iPhone dejan en el disco, recuperar datos de DVDs… Además, incluye otras herramientas como Autopsy.

40. Deft

DEFT *(Digital Evidence & Forensic Toolkit)* es una distribución Live CD basada en Linux. Se trata de un proyecto italiano de gran éxito, y que incluye las mejores herramientas forenses. Además de un número considerable de aplicaciones de Linux y scripts, DEFT también cuenta con la suite de DART que contiene aplicaciones de Windows. Mi software pericial favorito es este. Muy recomendable.

40. Sift

SIFT *(SANS Investigate Forensic Toolkit, SIFT)*. Constituye otra distribución basada en Ubuntu y que también incluye herramientas como SleuthKit/Autopsy, Wireshark, Pasco…

BIBLIOGRAFÍA

COGITTCV (Colegio Oficial de Graduados e Ingenieros Técnicos de Telecomunicación de la Comunidad Valenciana)
http://www.cogittcv.com

COGITT (Colegio Oficial de Graduados e Ingenieros Tecnicos de Telecomunicación)
http://www.cogitt.com

ANTPJI (Asociación Nacional de Tasadores y Peritos Judiciales Informáticos)
www.antpji.com