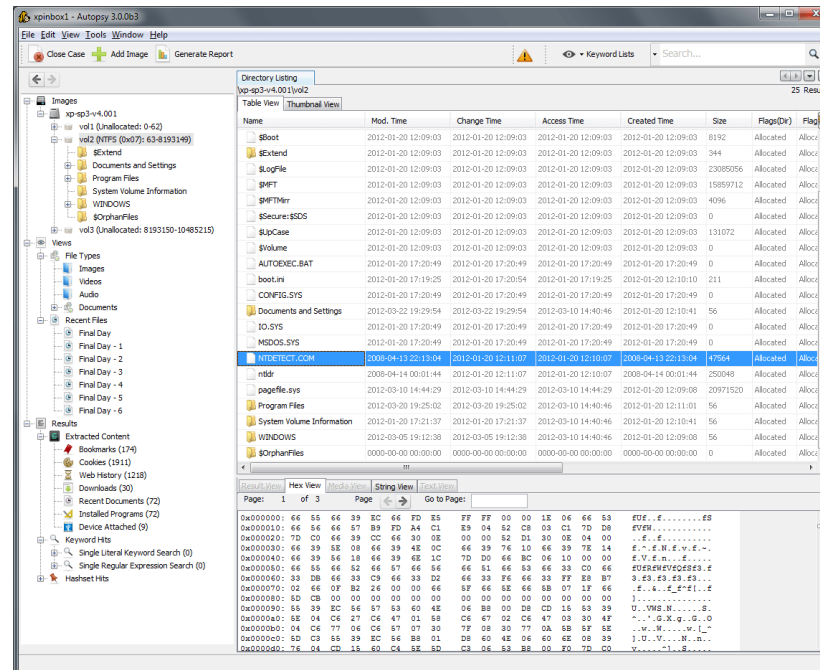


Anexo. Herramientas de investigación forense

Autopsy

[Autopsy](#) es un programa forense digital de código abierto basado en GUI para analizar discos duros y teléfonos inteligentes de manera eficiente. Miles de usuarios en todo el mundo utilizan Autopsy para investigar lo que sucedió en la computadora.



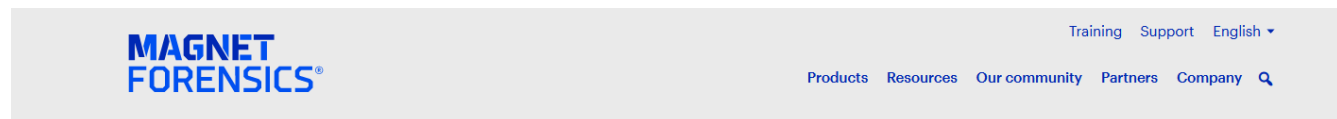
Es ampliamente utilizado por examinadores corporativos, militares para investigar, y algunas de las características lo son.

- Análisis de correo electrónico
- Detección de tipo de archivo
- Reproducción multimedia
- Análisis de registro
- Recuperación de fotos de la tarjeta de memoria
- Extraiga información de la cámara y la ubicación geográfica de archivos JPEG
- Extrae la actividad web de un navegador
- Mostrar eventos del sistema en una interfaz gráfica
- Análisis de la línea de tiempo
- Extraiga datos de Android: SMS, registros de llamadas, contactos, etc.

Tiene informes extensos para generar en formato de archivo HTML, XLS.

Encrypted Disk Detector

[Detector de disco cifrado](#) puede resultar útil para comprobar las unidades físicas cifradas. Es compatible con volúmenes cifrados TrueCrypt, PGP, BitLocker, Safeboot.



Resource Center

Free Tool

Magnet Encrypted Disk Detector

GET FREE TOOL ↓

Encrypted Disk Detector: What does it do?

Share

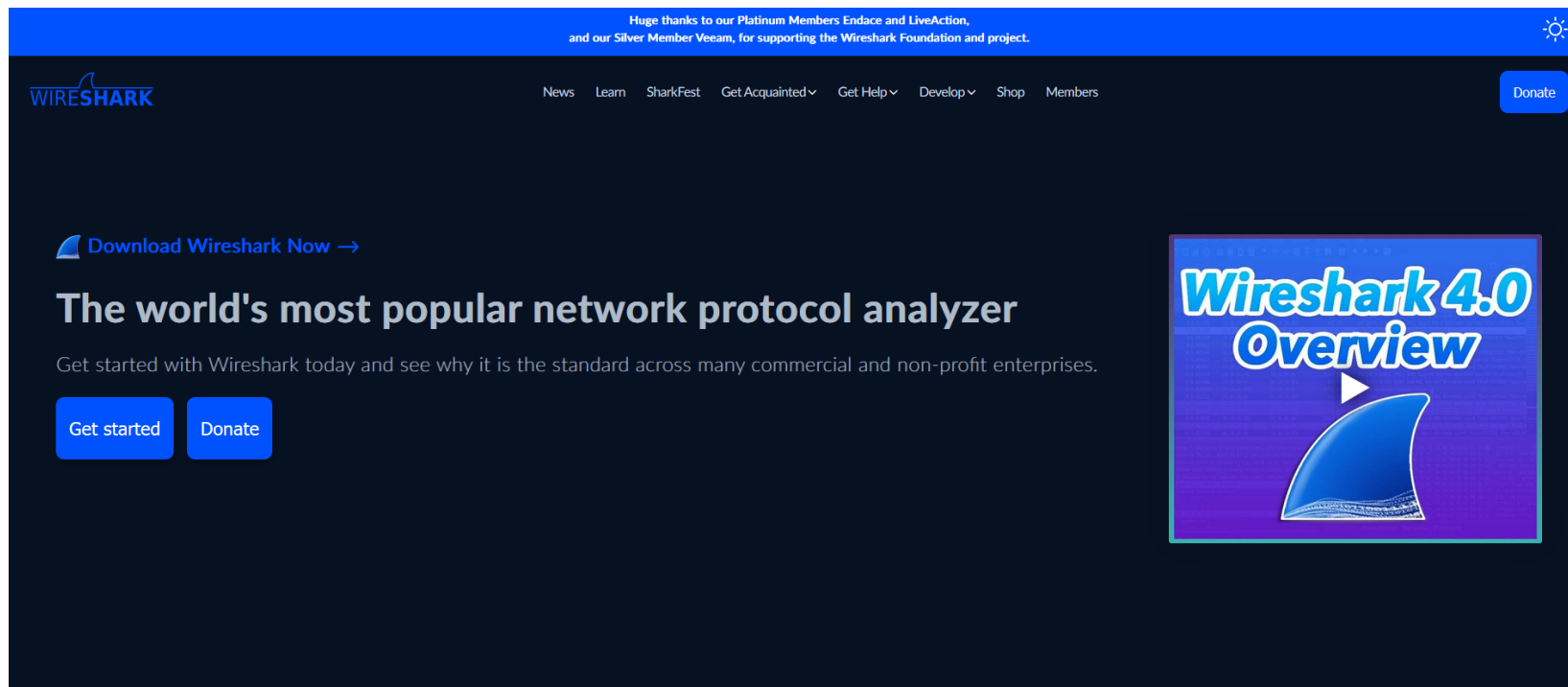


Magnet Encrypted Disk Detector (v3.10 released June 19th, 2022) is a command-line tool that can quickly and non-intrusively check for encrypted volumes on a computer system during incident response. The decision can then be made to investigate further and determine whether a live acquisition needs to be made in order to secure and preserve the evidence that would otherwise be lost if the plug was pulled .

Encrypted Disk Detector checks the local physical drives on a system for TrueCrypt, PGP®, VeraCrypt, Check Point related processes, SafeBoot, or Bitlocker® encrypted volumes. If no disk encryption signatures are found in the MBR, EDD also displays the OEM ID and, where applicable, the Volume Label for partitions on that drive, checking for Bitlocker® volumes.

Wireshark

[Wireshark](#) es una herramienta de captura y análisis de redes para ver qué está sucediendo en su red. Wireshark será útil para investigar el incidente relacionado con la red.



Magnet RAM Capture

Puede usar el [Magnet RAM Capture](#) para capturar la memoria física de una computadora y analizar los artefactos en la memoria.

Es compatible con el sistema operativo Windows.



TrainingSupportEnglish ▾

ProductsResourcesOur communityPartnersCompany🔍

Resource Center

Free Tool

Magnet RAM Capture

GET FREE TOOL ▾

Magnet RAM Capture: What does it do?

Share

[X](#)[in](#)[✉](#)

Magnet RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyze valuable artifacts that are often only found in memory.

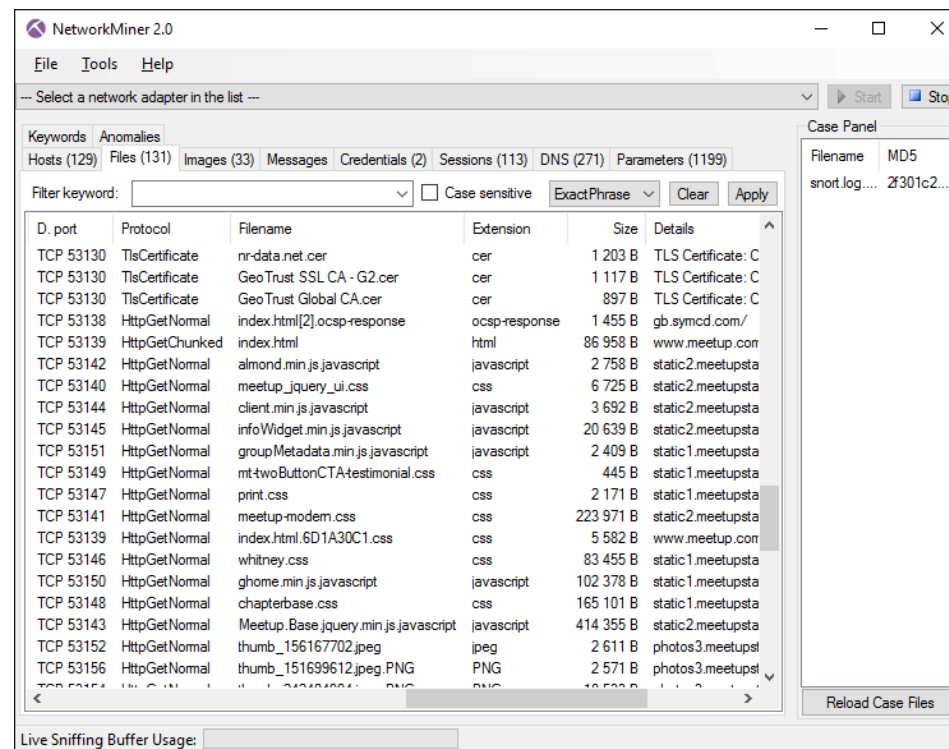
Magnet RAM Capture has a small memory footprint, meaning investigators can run the tool while minimizing the data that is overwritten in memory. You can export captured memory data in Raw (.DMP/.RAW/.BIN) format and easily upload into leading analysis tools including Magnet AXIOM and Magnet IEF.

Evidence that can be found in RAM includes processes and programs running on the system, network connections, evidence of malware intrusion, registry hives, usernames and passwords, decrypted files and keys, and evidence of activity not typically stored on the local hard disk.



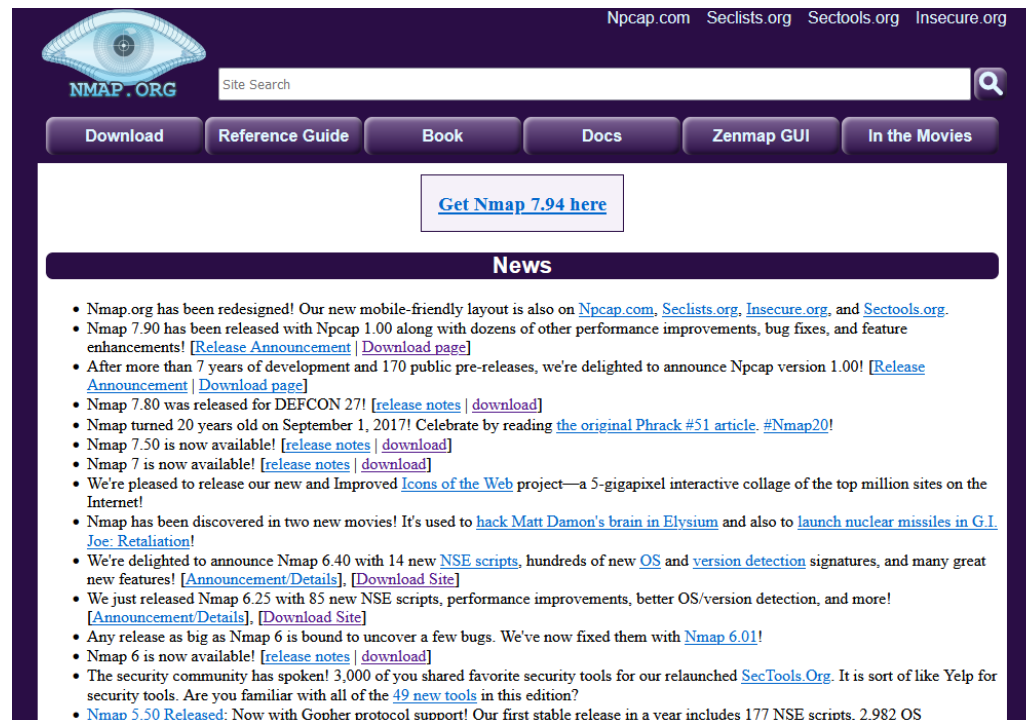
Network Miner

Un interesante analizador forense de redes para Windows, Linux y MAC OS X para detectar el sistema operativo, el nombre de host, las sesiones y los puertos abiertos a través del rastreo de paquetes o mediante un archivo PCAP. [Network Miner](#) proporciona artefactos extraídos en una interfaz de usuario intuitiva.



NMAP

[Nmap](#) (Network Mapper) es una de las herramientas de auditoría de seguridad y redes más populares. NMAP es compatible con la mayoría de los sistemas operativos, incluidos Windows, Linux, Solaris, Mac OS, HP-UX, etc. Es de código abierto y gratuito.



The screenshot shows the Nmap.org website. At the top, there's a navigation bar with links to [Npcap.com](#), [Seclists.org](#), [Sectools.org](#), and [Insecure.org](#). Below this is a search bar and a row of buttons: [Download](#), [Reference Guide](#), [Book](#), [Docs](#), [Zenmap GUI](#), and [In the Movies](#). A prominent button in the center says [Get Nmap 7.94 here](#). Below the navigation is a "News" section with a list of updates:

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on [Npcap.com](#), [Seclists.org](#), [Insecure.org](#), and [Sectools.org](#).
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [\[Release Announcement\]](#) [\[Download page\]](#)
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [\[Release Announcement\]](#) [\[Download page\]](#)
- Nmap 7.80 was released for DEFCON 27! [\[release notes\]](#) [\[download\]](#)
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading [the original Phrack #51 article](#). #Nmap20!
- Nmap 7.50 is now available! [\[release notes\]](#) [\[download\]](#)
- Nmap 7 is now available! [\[release notes\]](#) [\[download\]](#)
- We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elvysium](#) and also to [launch nuclear missiles in G.I. Joe: Retaliation](#)!
- We're delighted to announce Nmap 6.40 with 14 new [NSE scripts](#), hundreds of new [OS](#) and [version detection](#) signatures, and many great new features! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with [Nmap 6.01](#)!
- Nmap 6 is now available! [\[release notes\]](#) [\[download\]](#)
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of like Yelp for security tools. Are you familiar with all of the [49 new tools](#) in this edition?
- [Nmap 5.50 Released](#): Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS

RAM Capturer

[Capturador de RAM de Belkasoft](#) es una herramienta gratuita para volcar los datos de la memoria volátil de una computadora. Es compatible con el sistema operativo Windows. Los volcados de memoria pueden contener la contraseña del volumen cifrado y las credenciales de inicio de sesión para los correos web y los servicios de redes sociales.



Capture Live RAM Contents with Free Tool from Belkasoft!

DOWNLOAD NOW

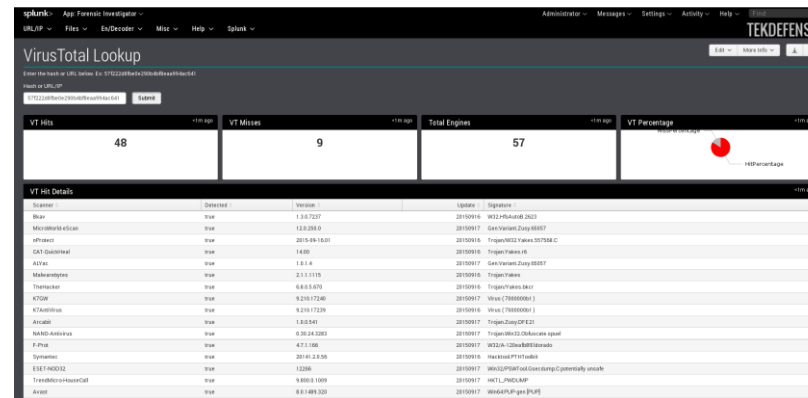
Belkasoft Live RAM Capturer is a tiny free forensic tool that allows to reliably extract the entire contents of computer's volatile memory—even if protected by an active anti-debugging or anti-dumping system. Separate 32-bit and 64-bit builds are available in order to minimize the tool's footprint as much as possible. Memory dumps captured with Belkasoft Live RAM Capturer can be analyzed with Live RAM Analysis in Belkasoft Evidence Center. Belkasoft Live RAM Capturer is compatible with all versions and editions of Windows including XP, Vista, Windows 7, 8 and 10, 2003 and 2008 Server.

Why Memory Dump Is the First Thing To Do During the Acquisition

Memory dumps are a valuable source of ephemeral evidence and volatile information. Memory dumps may contain passwords to encrypted volumes (TrueCrypt, BitLocker, PGP Disk), account login credentials for many webmail and social network services such as Gmail, Yahoo Mail, Hotmail, Facebook, Twitter; file sharing services such as Dropbox, Flickr, OneDrive, etc.

Forensic Investigator

Si está usando Splunk, entonces [Investigador forense](#) será una herramienta conveniente. Es una aplicación de Splunk y tiene muchas herramientas combinadas.

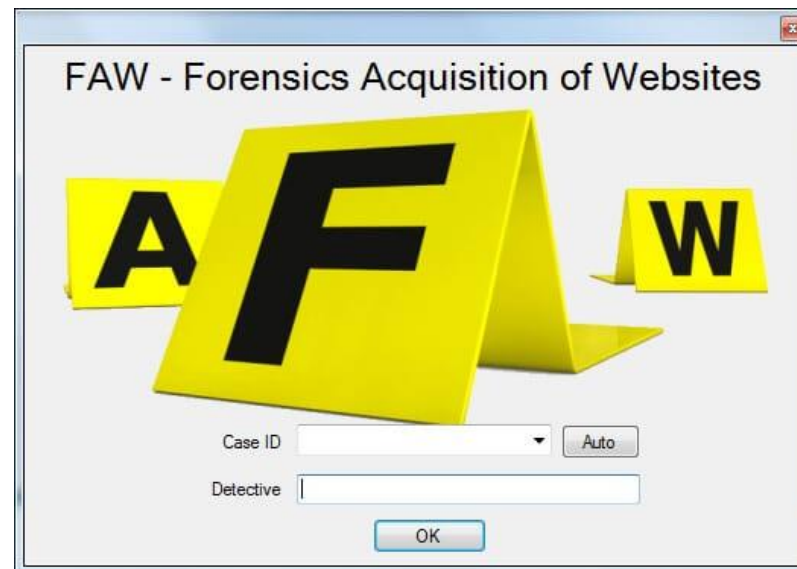


- Búsqueda de WHOIS / GeolIP
- Ping
- Escáner de puertos
- Capturador de banner
- Decodificador / analizador de URL
- Convertidor XOR / HEX / Base64
- Visor de recursos compartidos SMB / NetBIOS
- Búsqueda total de virus

FAW

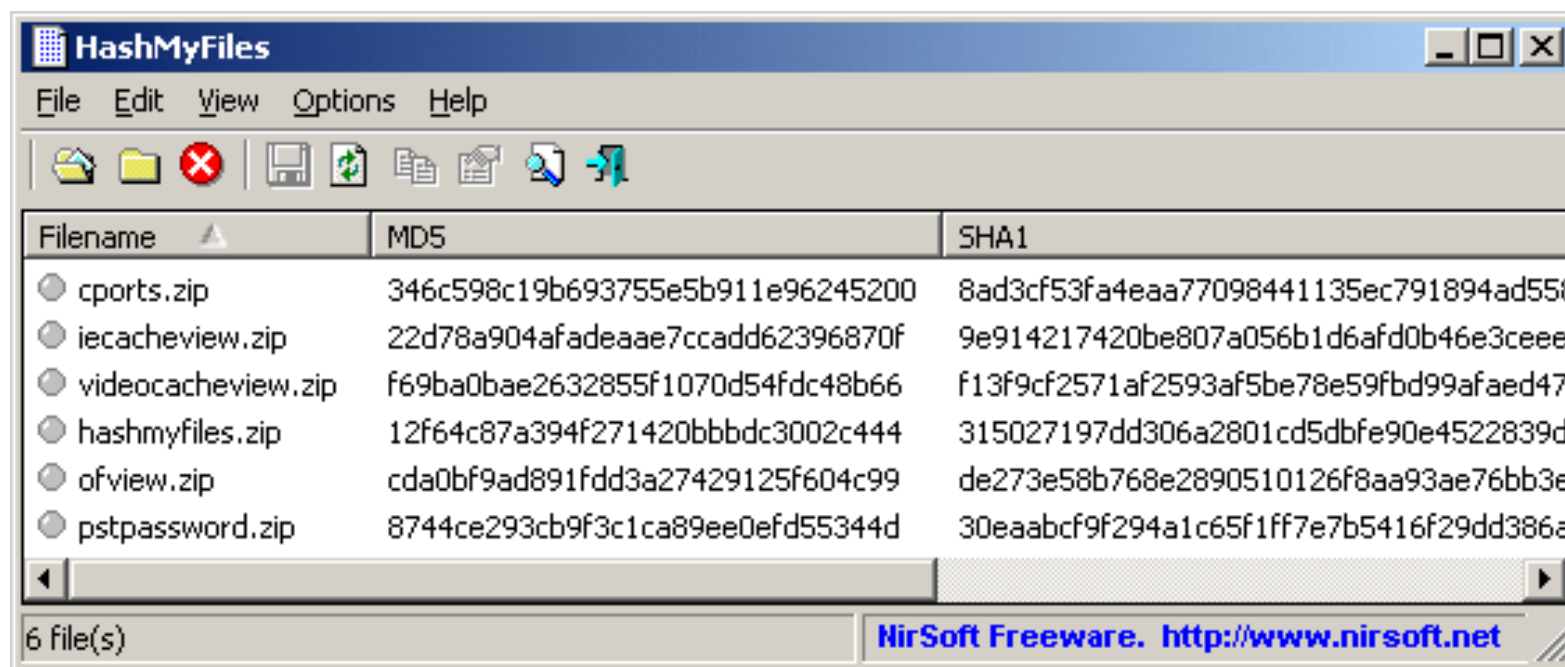
[FAW](#) (Adquisición forense de sitios web) consiste en adquirir páginas web para investigación forense, que tiene las siguientes características.

- Capture la página completa o parcial
- Captura todo tipo de imágenes
- Capturar el código fuente HTML de la página web
- Integrar con Wireshark



HashMyFiles

[HashMyFiles](#) le ayudará a calcular los valores hash MD5 y SHA1. Funciona en casi todos los últimos sistemas operativos Windows.




Crowd Response

[Respuesta](#) de Crowd Strike es una aplicación de Windows para recopilar información del sistema para respuesta a incidentes y compromisos de seguridad. Puede ver los resultados en XML, CSV, TSV o HTML con la ayuda de CRConvert. Se ejecuta en Windows XP de 32 o 64 bits anterior.

Crowd Strike tiene otras herramientas útiles para la investigación.


- Totrtilla: enruta de forma anónima el tráfico TCP / IP y DNS a través de Tor.
- Shellshock Scanner: escanee su red en busca de vulnerabilidades de shellshock.
- Escáner Heartbleed: escanee su red para OpenSSL [vulnerabilidad al sangrado del corazón](#).

Let us show you how we stop breaches




Learn how to prevent, detect, and respond to all attack types in real time with CrowdStrike Falcon.

SEE DEMO



Request information about next-gen endpoint protection, threat intelligence, or incident response services.

REQUEST INFO



Need immediate assistance? Get back to business faster with CrowdStrike's pre and post incident response services.

EXPERIENCED A BREACH?

NFI Defraser

[Defrasador](#) La herramienta forense puede ayudarlo a detectar archivos multimedia completos y parciales en los flujos de datos.

ExifTool

[ExifTool](#) le ayuda a leer, escribir y editar metainformación para varios tipos de archivos. Puede leer EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Photoshop IRB, FlashPix, etc.

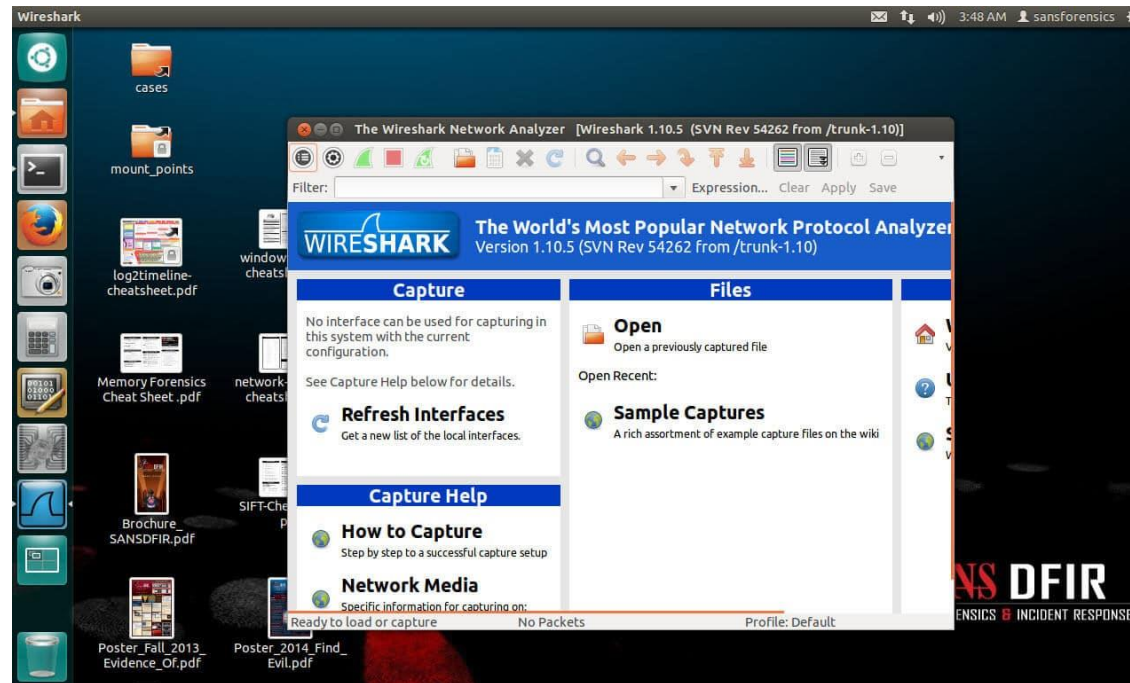
Toolsley

[herramientasley](#) obtuve más de diez herramientas útiles para la investigación.

- Verificador de firmas de archivos
- Identificador de archivo
- Hash y validar
- Inspector binario
- Codificar texto
- Generador de URI de datos
- Generador de contraseñas

SIFT

[SIFT](#) La estación de trabajo (kit de herramientas forenses de investigación SANS) está disponible gratuitamente como Ubuntu 14.04. SIFT es un conjunto de herramientas forenses que necesita y una de las plataformas de respuesta a incidentes de código abierto más populares.



Dumpzilla

Extraiga toda la información interesante del navegador Firefox, Iceweasel y Seamonkey para analizarla con [Dumpzilla](#).



Browser History

Foxton tiene dos interesantes herramientas gratuitas.

1. Capturador del historial del navegador: captura el historial del navegador web (Chrome, Firefox, IE y Edge) en el sistema operativo Windows.
2. Visor de historial del navegador: extraiga y analice el historial de actividad de Internet de la mayoría de los navegadores modernos. Los resultados se muestran en el gráfico interactivo y los datos históricos se pueden filtrar.

ForensicUserInfo

Extraiga la siguiente información con [Información de usuario forense](#).

- RID
- Hash LM / NT
- Restablecimiento de contraseña / fecha de vencimiento de la cuenta
- Número de inicio de sesión / fecha de error
- Grupos
- Ruta del perfil

Kali Linux

[Kali Linux](#) es uno de los sistemas operativos más populares para pruebas de seguridad y penetración, pero también tiene capacidad forense. Hay más de 100 herramientas, así que estoy seguro de que encontrará una para su necesidad.



Paladin

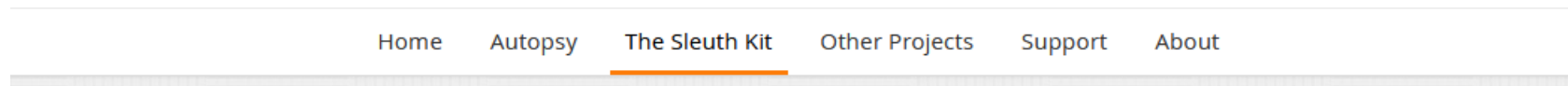
[PALADÍN](#) suite forense: la suite forense de Linux más famosa del mundo es una distribución de Linux modificada basada en Ubuntu disponible en 32 y 64 bits.



Paladin tiene más de **100 herramientas en 29 categorías**, casi todo lo que necesita para investigar un incidente. Autopsy está incluido en la última versión: Paladin 6.

Sleuth Kit

[El kit de detectives](#) es una colección de herramientas de línea de comandos para investigar y analizar volúmenes y sistemas de archivos para encontrar la evidencia.



Overview

The Sleuth Kit® (TSK) is a library and collection of command line tools that allow you to investigate disk images. The core functionality of TSK allows you to analyze volume and file system data. The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence.

- [Volume and File System Analysis](#)
- [Download](#)
- [Documents](#)
- [History](#)
- [Licenses](#)

CAINE

CAINE (Computer Aided Investigative Environment) es una distribución de Linux que ofrece la plataforma forense completa que tiene más de 80 herramientas para analizar, investigar y crear un informe procesable.

