

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0
#one = bpy.context.selected_objects[0]
```

# Simulación de análisis forense con herramientas de Kali Linux

ADMINISTRACIÓN DE SISTEMAS Y SEGURIDAD

Álvaro de la Flor Bonilla  
Antonio Manuel Salvat Pérez



```
username;  
password;  
$database;  
$charset;  
  
public function connect()  
{  
    $link = null;  
    if (!$link = mysql_connect(  
        $host, $username, $password,  
        $database, $charset))  
        throw new MySQLException(  
            "Error al conectar a la base de datos: " .  
            mysql_error());  
    mysql_query("SET CHARACTER SET UTF8");  
    mysql_query("SET NAMES UTF8");  
    mysql_query("USE $database");  
}
```



# INTRODUCCIÓN



# *Análisis forense informático*

DERECHO + INFORMÁTICA  
Análisis de datos de:

Sistemas informáticos

Redes y comunicaciones

Dispositivos



Análisis como prueba en tribunal



# *Etapas Análisis forense*

Identificación

Adquisición

Análisis

Presentación de resultados

# *Etapas Análisis forense*

## IDENTIFICACIÓN

Identificar elementos

Volatilidad

Recolectar evidencias

Registros y contenidos de la memoria caché del equipo

Tablas de enrutamiento de redes, caché ARP, tabla de procesos, estadísticas del kernel y memoria

Información temporal del sistema

Datos contenidos en disco

Logs del sistema

Configuración física y topología de la red donde se encuentra el equipo.

Documentos

# *Etapas Análisis forense*

## ADQUISICIÓN

Copias de información

Copias bite a bite

Posibilidad de recuperación





# *Etapas Análisis forense*

## ANÁLISIS

Hardware-Software

Tiempo-Logs-RAM

Criticidad



# *Etapas Análisis forense*

## PRESENTACIÓN

Cuestiones relevantes-críticas

Informe ejecutivo

Informe técnico





# *Tipos Análisis forense*

Sistemas Operativos

Redes

Dispositivos móviles

Cloud



# EL ANÁLISIS FORENSE DIGITAL LLEVA A LOS INVESTIGADORES AL ASESINO DE CRAIGSLIST

Para empezar, el FBI extrajo los registros de las torres de telefonía móvil cerca de la escena de cada crimen durante 15 minutos antes y después de cada incidente. Intentaron encontrar un solo número de teléfono que estuviera activo en cada ubicación en ese momento. Esta fue y sigue siendo una práctica controvertida, que ha hecho sonar las alarmas de la ACLU y el NY Times, entre otros. Al final, resultó ser un callejón sin salida: resultó que Markoff había usado varios teléfonos desechables.

Buscar la dirección de correo electrónico que el asesino usó para contactar a Julissa fue más fructífero. Era una cuenta de correo electrónico desechable, pero, después de una citación, Microsoft entregó la dirección IP de la persona que la registró. El ISP, Comcast, (nuevamente, después de otra citación) luego entregó el nombre y la dirección física de la persona con esa dirección IP: Philip Markoff. Esa fue una prueba condenatoria, pero lejos de ser lo suficientemente concreta como para hacer un arresto y una condena; Dado que Markoff usó un enrutador inalámbrico, la dirección IP podría haber sido utilizada técnicamente por otra persona en su edificio de apartamentos.

El siguiente en la serie de citaciones fue Facebook. A cambio, las autoridades recibieron un expediente de más de 60 páginas sobre Markoff. Este documento de más de 60 páginas incluía una vista completa del perfil de Markoff: fotos etiquetadas, publicaciones en el muro, lista de amigos y un historial completo de sus inicios de sesión y las direcciones IP asociadas con esos inicios de sesión. (Facebook ahora afirma que ya no darían este nivel de detalle basándose solo en una citación, y en su lugar requerirían una orden de registro).

**URGENTE: APAGA TU ORDENADOR YA**

El equipo de Seguridad ha detectado el ingreso a la red de Telefónica de un malware que afecta tus datos y ficheros. Por favor avisa a todos tus compañeros de esta situación.

Apaga el ordenador ya y no vuelvas a encenderlo **hasta nuevo aviso(\*)**.

Te enviaremos un correo que podrás leer a través de tu móvil cuando la situación ya esté normalizada. Además, el martes informaremos en las entradas de los edificios sobre el acceso a la red.

Ante cualquier duda contacta con la Mesa de Ayuda (29000)

(\*) Desconecta el móvil de la red WiFi pero no hace falta que lo apagues

Dirección de Seguridad

**2015: Ataque a la red eléctrica de Ucrania**

En diciembre de 2015, unas 230.000 personas quedaron hasta seis horas en la oscuridad después de que piratas informáticos se infiltraran en tres compañías de energía y cerraran temporalmente los generadores en tres regiones de Ucrania.

El servicio de seguridad de Ucrania culpó al Gobierno ruso por el ataque. Por otra parte, sin nombrar a Moscú, algunas compañías privadas de seguridad de Estados Unidos que investigaron el suceso dijeron que creían que este se había originado en Rusia. Se cree que este ataque es la primera vez que piratas informáticos pueden atacar con éxito una red de distribución de electricidad.



## *Objetivos*

Analizar consecuencias

Averiguar quien ha sido el autor

Causas y metodologías empleada

Detectar debilidades



```
...  
username;  
password;  
$database;  
$charset;  
...  
public function connect()  
{  
    $link = null;  
    if (!$link = mysql_connect(  
        $host, $username, $password,  
        $database, $charset))  
        throw new MySQLException(  
            "Error al conectar con la base de datos: " .  
            mysql_error());  
    return $link;  
}
```



# HERRAMIENTAS

## *Binwalk tool*

Buscar en una imagen binaria determinada:

- Archivos
- Código ejecutable incrustados





## *Binwalk tool*

Extraer archivos del firmware

\$ binwalk <firmware>

\$ binwalk -e <firmware>

```
root@kali:~/Downloads# binwalk xdvi.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	ELF, 64-bit LSB shared object, AMD x86-64, ver
536282	0x82EDA	Unix path: /usr/etc/mime.types:/usr/local/etc/
628878	0x9988E	Copyright string: "copyrightsans"
628892	0x9989C	Copyright string: "copyrightserif"

# Binwalk tool

Diferencias entre archivos del firmware  
\$ binwalk -W <firmware1> <firmware2>

OFFSET	xdvi.bin		xdvi.bin
0x00000000	7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00	.ELF.....	\ 7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00  .ELF.....
0x00000010	03 00 3E 00 01 00 00 00 E0 09 02 00 00 00 00 00	...>.....	/ 03 00 3E 00 01 00 00 00 E0 09 02 00 00 00 00 00  ...>.....
0x00000020	40 00 00 00 00 00 00 00 A0 AD 0B 00 00 00 00 00 00	@.....	\ 40 00 00 00 00 00 00 00 A0 AD 0B 00 00 00 00 00  @.....
0x00000030	00 00 00 00 40 00 38 00 0B 00 40 00 1D 00 1C 00	....@.8...@....	/ 00 00 00 00 40 00 38 00 0B 00 40 00 1D 00 1C 00  ....@.8...@....
0x00000040	06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00	.....@.....	\ 06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x00000050	40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	@.....@.....	/ 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  @.....@.....
0x00000060	68 02 00 00 00 00 00 00 68 02 00 00 00 00 00 00	h.....h.....	\ 68 02 00 00 00 00 00 00 68 02 00 00 00 00 00 00  h.....h.....
0x00000070	08 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00	.....	/ 08 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00  .....
0x00000080	A8 02 00 00 00 00 00 00 A8 02 00 00 00 00 00 00	.....	\ A8 02 00 00 00 00 00 00 A8 02 00 00 00 00 00 00  .....
0x00000090	A8 02 00 00 00 00 00 00 1C 00 00 00 00 00 00 00	.....	/ A8 02 00 00 00 00 00 00 1C 00 00 00 00 00 00 00  .....
0x000000A0	1C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00	.....	\ 1C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  .....
0x000000B0	01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00	.....	/ 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00  .....
0x000000C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	\ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

## *Binwalk tool*

### USOS

INGENIERÍA INVERSA

BUSCAR CONTRASEÑAS (passwd,  
shadow, etc)

DIFERENCIA BINARIA

...



# Binwalk tool

## Bugs in Cisco RV132W and RV134W routers

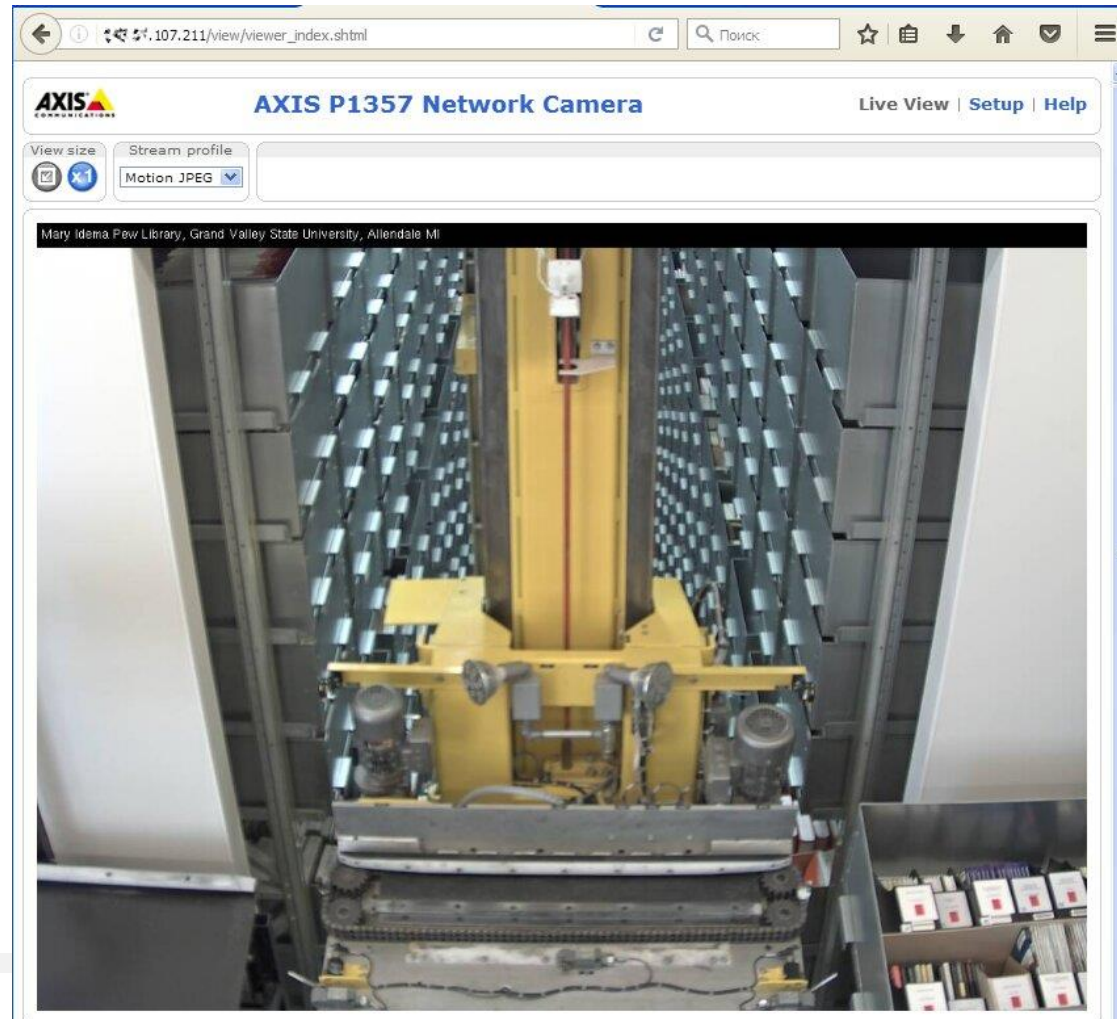
### [CVE-2021-1287 Detail](#)

by NIST March 17, 2021

*"A vulnerability in the web-based management interface of Cisco RV132W ADSL2+ Wireless-N VPN Routers and Cisco RV134W VDSL2 Wireless-AC VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device or cause the device to restart unexpectedly. The vulnerability exists because the web-based management interface does not properly validate user-supplied input.... A successful exploit could allow the attacker to execute arbitrary code as the root user .... "* The attacker needs to be authenticated to the device before they can exploit the flaw. Fixes are available.

- [Cisco Small Business RV132W and RV134W Routers Management Interface Remote Command Execution and Denial of Service Vulnerability](#) by Cisco March 17, 2021.
- [Cisco Plugs Security Hole in Small Business Routers](#) by Lindsey O'Donnell for ThreatPost March 17, 2021

# *Binwalk tool*





# Extrae información útil sin analizar el sistema de archivos

# Extrae números de tarjetas de crédito, enlaces URL, IPs, direcciones MACs...

# Funciona con datos comprimidos o dañados

```

marcs@bulk_extractor:~$ ./zeus.vmem -o zeus_extract
error: no outfile must be specified
marcs@bulk_extractor:~$ ./zeus.vmem zeus.vmem
count: 3.43
done
zeus_extract
278
278
00 (0.00%) Done in n/a at 11:42:57
00 (50.00%) Done in 00:00:10 at 11:43:18
waiting for threads to finish...
waiting for 4 threads to finish:
  min 1.00
waiting for 4 threads to finish:
  min 55 min 54 sec.)
avg 07100064
avg 180003296
avg 23000000
avg 117000512
done
edit
not waiting: 8.96469 sec.
time spent waiting: 0.761732 sec.
join scanners
histograms
... can_track2 histogram... domain histogram...
... ether histogram... find histogram...
... top histogram... telephone histogram...
... url microsoft-live... url services...
... url facebook-id... url searches...
42 sec.
per 6.265 MBytes/sec.
not found: 146
marcs$

```



## *Bulk Extractor*

Extracción de información sensible

\$ bulk\_extractor -o <folder\_name> <adress>

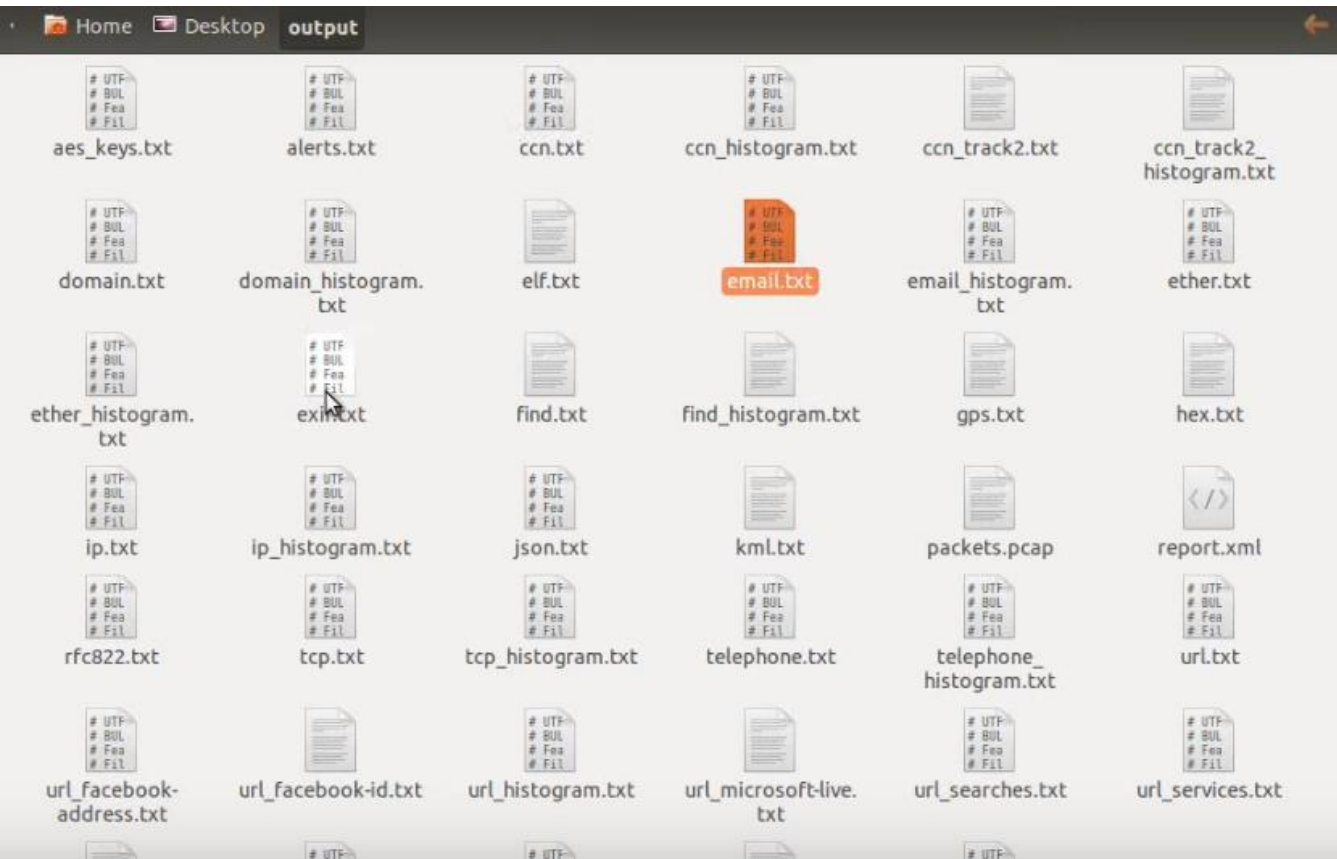
```
lecturesnippets@lecturesnippets-ubuntu:~/Desktop$ sudo bulk_extractor -o output /dev/sdb1
bulk_extractor version: 1.3.1
Hostname: lecturesnippets-ubuntu
Input file: /dev/sdb1
Output directory: output
Disk Size: 64422412288
Threads: 1
16:41:20 Offset 0MB (0.00%) Done in n/a at 16:41:19
```

# Bulk Extractor

```
23:16:10 Offset 64357MB (99.90%) Done in 0:00:23 at 23:16:33
All Data is Read; waiting for threads to finish...
Time elapsed waiting for 1 thread to finish:
    (timeout in 60 min .)
All Threads Finished!
Producer time spent waiting: 22724.2 sec.
Average consumer time spent waiting: 0.429018 sec.
*****
** bulk_extractor is probably CPU bound. **
**   Run on a computer with more cores   **
**   to get better performance.          **
*****
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
    ccn histogram...    ccn_track2 histogram...    domain histogram...
    email histogram...  ether histogram...    find histogram...
    ip histogram...    tcp histogram...    telephone histogram...
    url histogram...    url microsoft-live...    url services...
    url facebook-address...    url facebook-id...    url searches...

Elapsed time: 2.372e+04 sec.
Overall performance: 2.716 MBytes/sec.
Total email features found: 2043
```

# Bulk Extractor



```
# histogram file version: 1.1
n=63 administrator@www.ac (utf16=63)
n=46 premium-server@thawte.com (utf16=4)
n=21 info@valicert.com (utf16=2)
n=17 administrator@at.at (utf16=17)
n=17 support@accessdata.com (utf16=17)
n=14 cps-requests@verisign.com
n=9 administrator@cl.at (utf16=9)
n=5 administrator@marketing.ac (utf16=5)
n=5 rico@ricostacruz.com (utf16=5)
n=4 txtadministrator@www.ac (utf16=4)
n=3 administrator@addthis.com
n=3 jeffsmith@redmond.corp.microsoft.com (utf16=3)
n=3 vshubin@ntdev.microsoft.com
n=2 administrator@www.ge (utf16=2)
n=2 eay@cryptsoft.com
n=2 gtk-devel-list@gnome.org
n=2 info@prof-uis.com (utf16=2)
n=2 meishu1981@gmail.com
n=1 l.txtadministrator@c.at (utf16=1)
n=1 administrator@adobe.de (utf16=1)
n=1 administrator@c.at (utf16=1)
n=1 administrator@c.bi (utf16=1)
n=1 administrator@d.ad (utf16=1)
n=1 administrator@ox-d.ad (utf16=1)
```

# Bulk Extractor

20 20Minutos

## Condenado en Valladolid a cinco años de cárcel el pedófilo detenido con 'durísimos' archivos

La detención del pedófilo se produjo cuando la aplicación 'Quijote' ... de 85 archivos de contenido pedófilo efectuados desde una IP utilizada por ... al que se incautaron tres ordenadores, cuatro pendrive y cinco discos duros ...

Hace 2 semanas

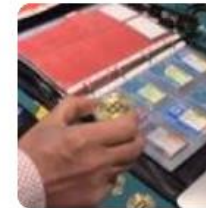


ep Europa Press

## Detenido un hombre con amplios conocimientos informáticos que usurpaba identidades para estafar en ban...

Entre los distintos anuncios que localizaron provenientes de la misma IP, se localizó uno en un portal de Internet, donde el ahora detenido ...

Hace 2 semanas



E EL PAÍS

## Condenan a dos años de prisión a un cura de Málaga que guardaba más de 400.000 imágenes de pornografía in...

El condenado fue detenido por la Policía Nacional en verano de ... de una serie de direcciones IP con conexiones en la provincia de Málaga.

Hace 3 semanas





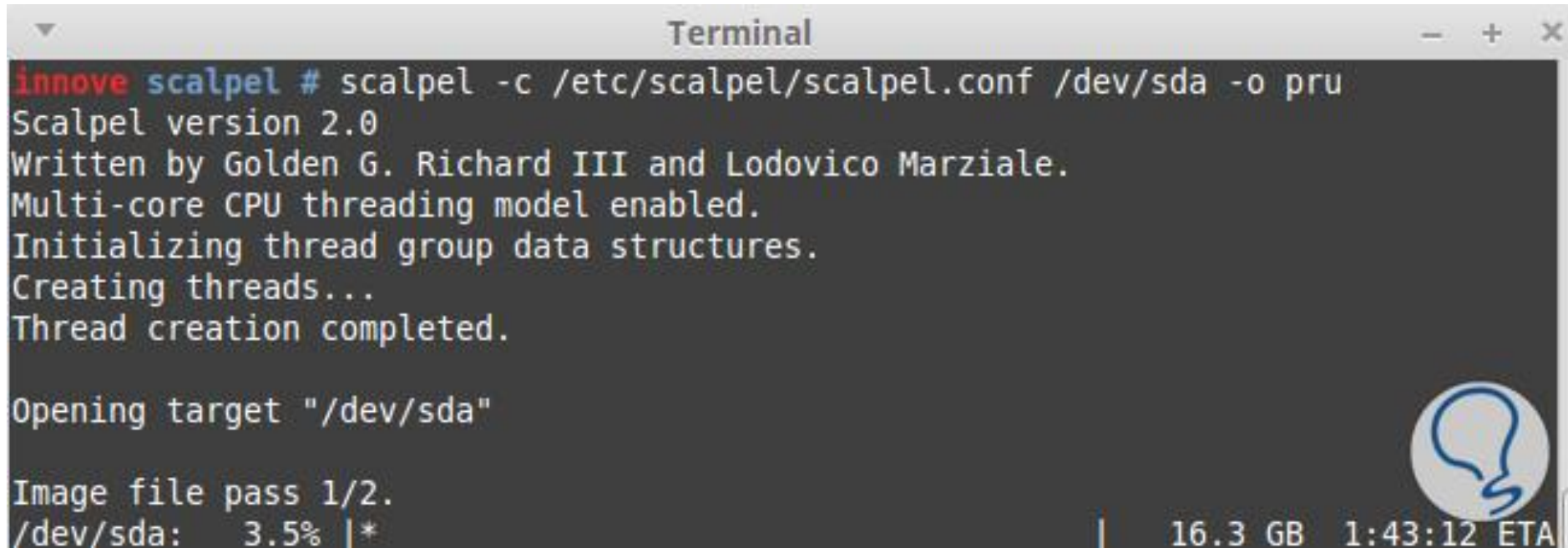
## *Scalpel tool*

Permite restaurar información que puede haber eliminado



## *Scalpel tool*

```
$ scalpel -c /etc/scalpel/scalpel.conf <device_directory> -o <output>
```

A screenshot of a terminal window titled "Terminal". The window shows the execution of the Scalpel tool. The command entered is "scalpel -c /etc/scalpel/scalpel.conf /dev/sda -o pru". The output shows the tool's version (2.0), its authors (Golden G. Richard III and Lodovico Marziale), and that multi-core CPU threading is enabled. It then shows the process of initializing thread group data structures, creating threads, and completing thread creation. Finally, it shows the target "/dev/sda" being opened and the first pass of the image file being processed. A progress bar at the bottom indicates 3.5% completion, with a total size of 16.3 GB and an estimated time to completion of 1:43:12. A lightbulb icon is visible in the bottom right corner of the terminal window.

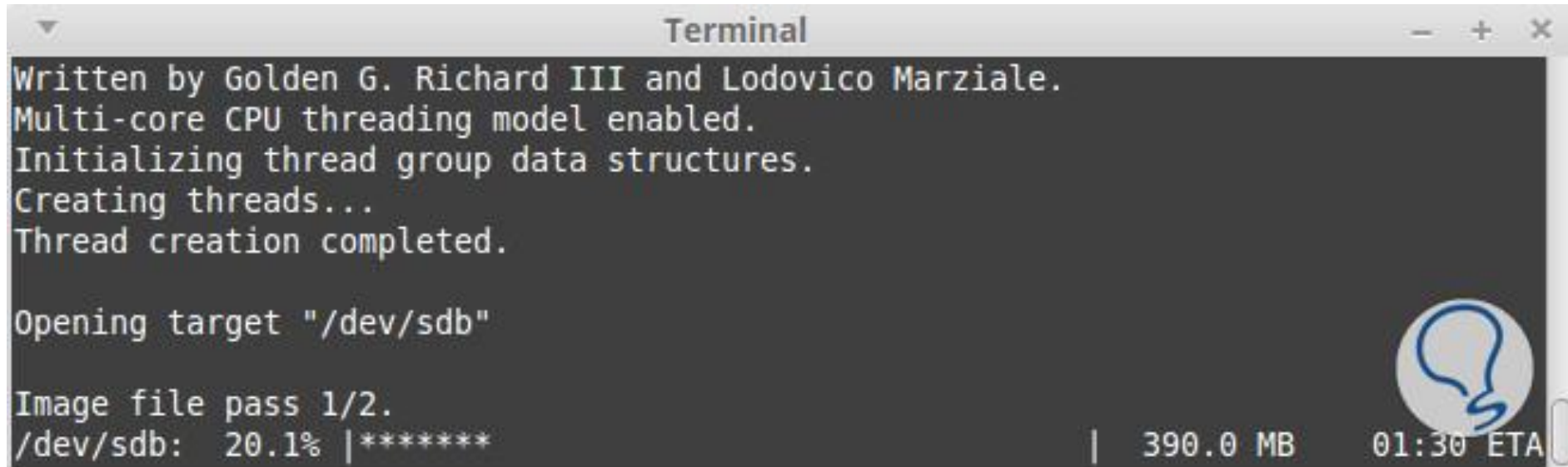
```
innove scalpel # scalpel -c /etc/scalpel/scalpel.conf /dev/sda -o pru
Scalpel version 2.0
Written by Golden G. Richard III and Lodovico Marziale.
Multi-core CPU threading model enabled.
Initializing thread group data structures.
Creating threads...
Thread creation completed.

Opening target "/dev/sda"

Image file pass 1/2.
/dev/sda:  3.5% |*                               | 16.3 GB  1:43:12 ETA
```

## *Scalpel tool*

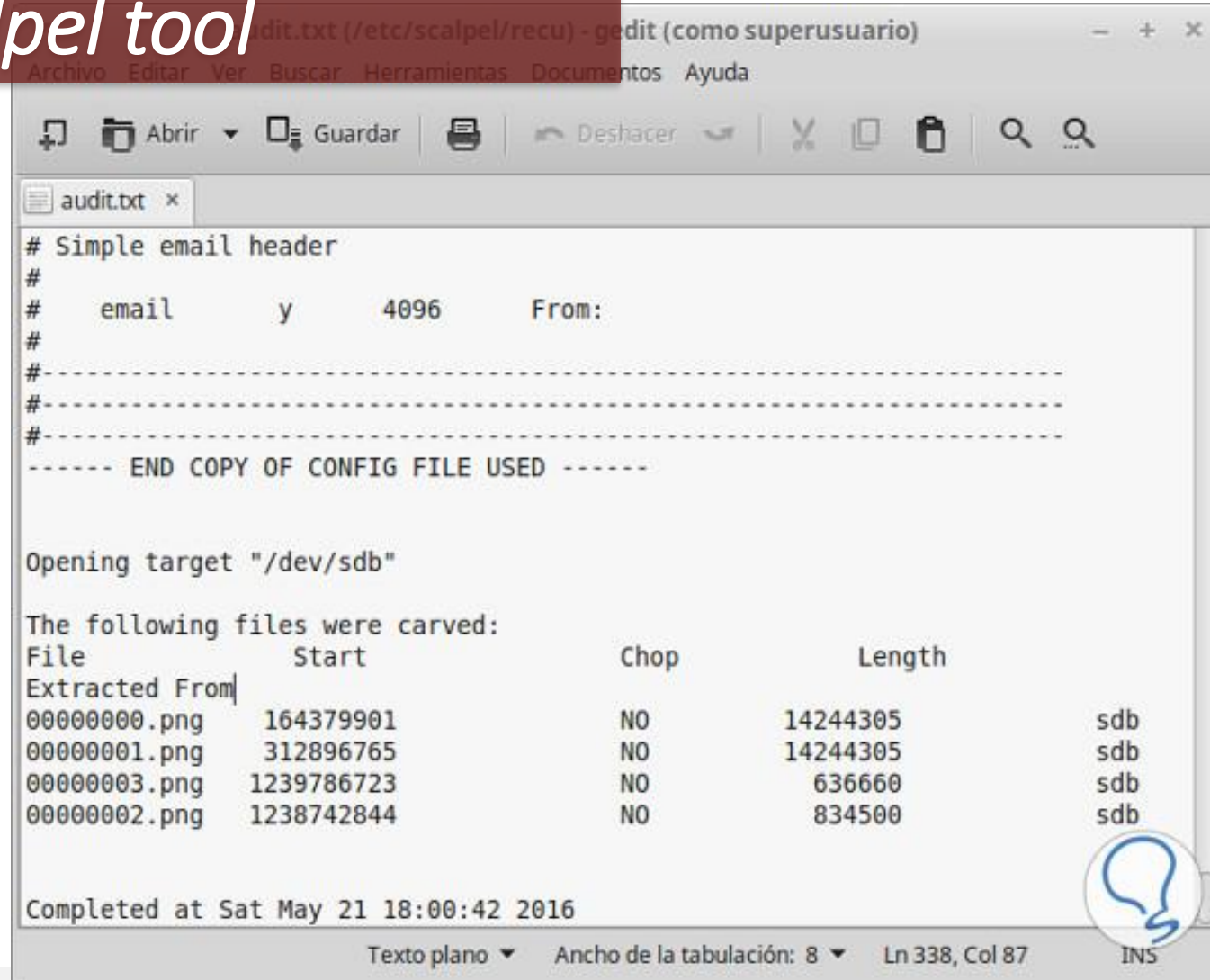
```
$ scalpel -c /etc/scalpel/scalpel.conf <device_directory> -o <output>
```

A screenshot of a terminal window titled "Terminal". The window has a dark background and a light gray title bar with standard window controls. The text inside the terminal shows the Scalpel tool's startup sequence: "Written by Golden G. Richard III and Lodovico Marziale.", "Multi-core CPU threading model enabled.", "Initializing thread group data structures.", "Creating threads...", and "Thread creation completed.". It then shows "Opening target \"/dev/sdb\"", followed by "Image file pass 1/2.". The bottom line shows a progress bar for "/dev/sdb:" at 20.1%, with a lightbulb icon in the bottom right corner. The status bar at the bottom right of the terminal shows "390.0 MB" and "01:30 ETA".

```
Written by Golden G. Richard III and Lodovico Marziale.  
Multi-core CPU threading model enabled.  
Initializing thread group data structures.  
Creating threads...  
Thread creation completed.  
  
Opening target "/dev/sdb"  
  
Image file pass 1/2.  
/dev/sdb: 20.1% |*****| 390.0 MB 01:30 ETA
```

```
$ scalpel -c /etc/scalpel/scalpel.conf /dev/sdb -o recu
```

# Scalpel tool



The screenshot shows a gedit window titled "audit.txt (/etc/scalpel/recu) - gedit (como superusuario)". The window contains the following text:

```
# Simple email header
#
# email y 4096 From:
#
#-----
#-----
#-----
----- END COPY OF CONFIG FILE USED -----

Opening target "/dev/sdb"

The following files were carved:
File          Start          Chop          Length
Extracted From
00000000.png  164379901        NO           14244305      sdb
00000001.png  312896765        NO           14244305      sdb
00000003.png  1239786723       NO           636660        sdb
00000002.png  1238742844       NO           834500        sdb

Completed at Sat May 21 18:00:42 2016
```

The status bar at the bottom indicates "Texto plano", "Ancho de la tabulación: 8", "Ln 338, Col 87", and "INS".



## *Scalpel tool*

# Recuperados los archivos informáticos borrados sobre los sumarios relacionados con Jesús Gil



MÁLAGA. Agencias



GUARDAR



Los especialistas informáticos de la Junta de Andalucía han conseguido recuperar los archivos informáticos borrados en relación con los sumarios relacionados con el alcalde de Marbella, Jesús Gil. El también presidente del Atlético de Madrid restó importancia al hecho y se preguntó a quién le puede beneficiar el robo de esta documentación. El Consejo General del Poder Judicial (CGPJ) está estudiando los hechos, después de que todos los partidos de la oposición pidiesen la

## *Autopsy tool*

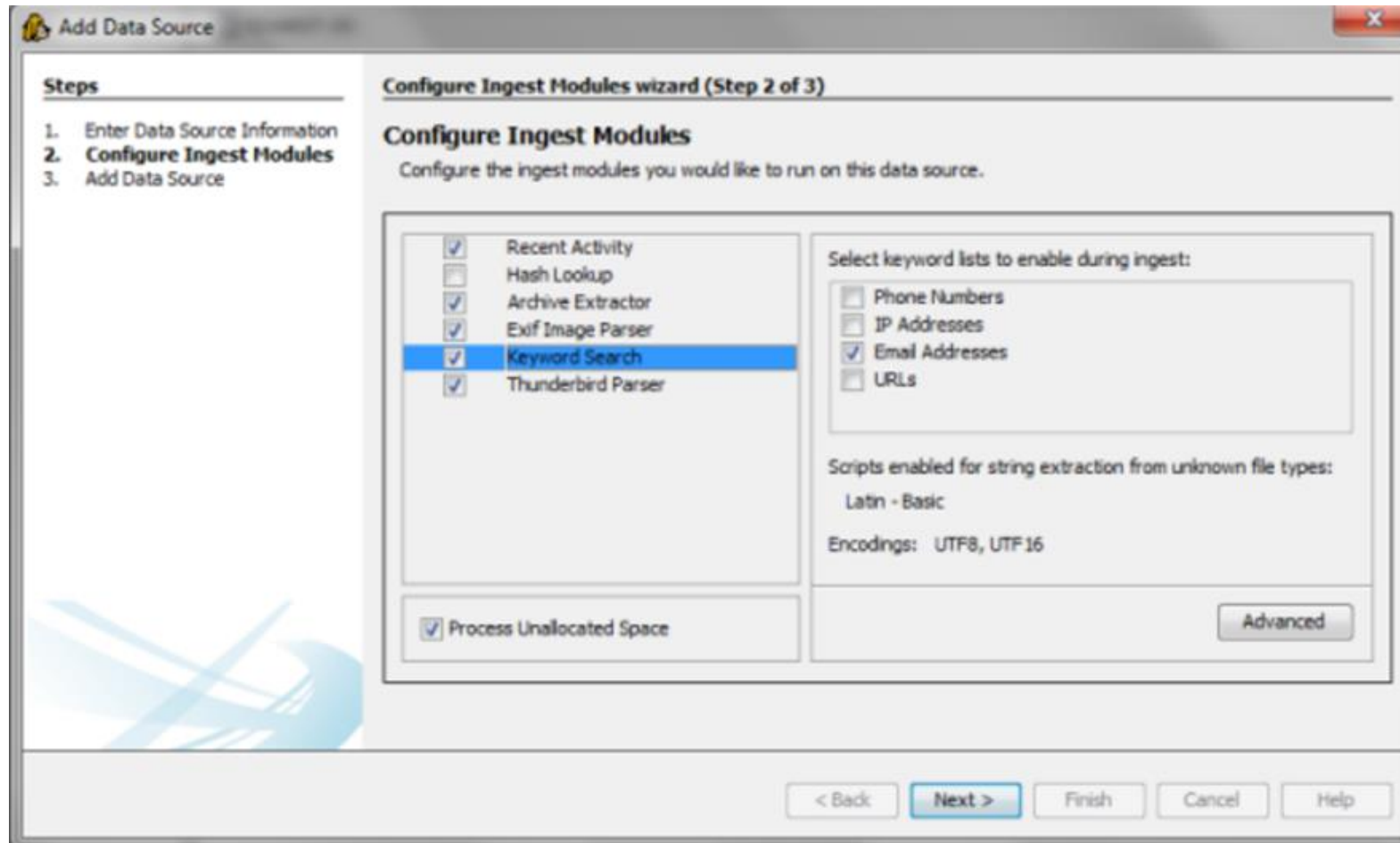
Es una de las herramientas más utilizada  
en España

The Sleuth Kit



Autopsy®  
OPEN | EXTENSIBLE | IT

# Autopsy tool



## *Scalpel tool*

Recent Activity

Hash Lookup

Archive Extractor

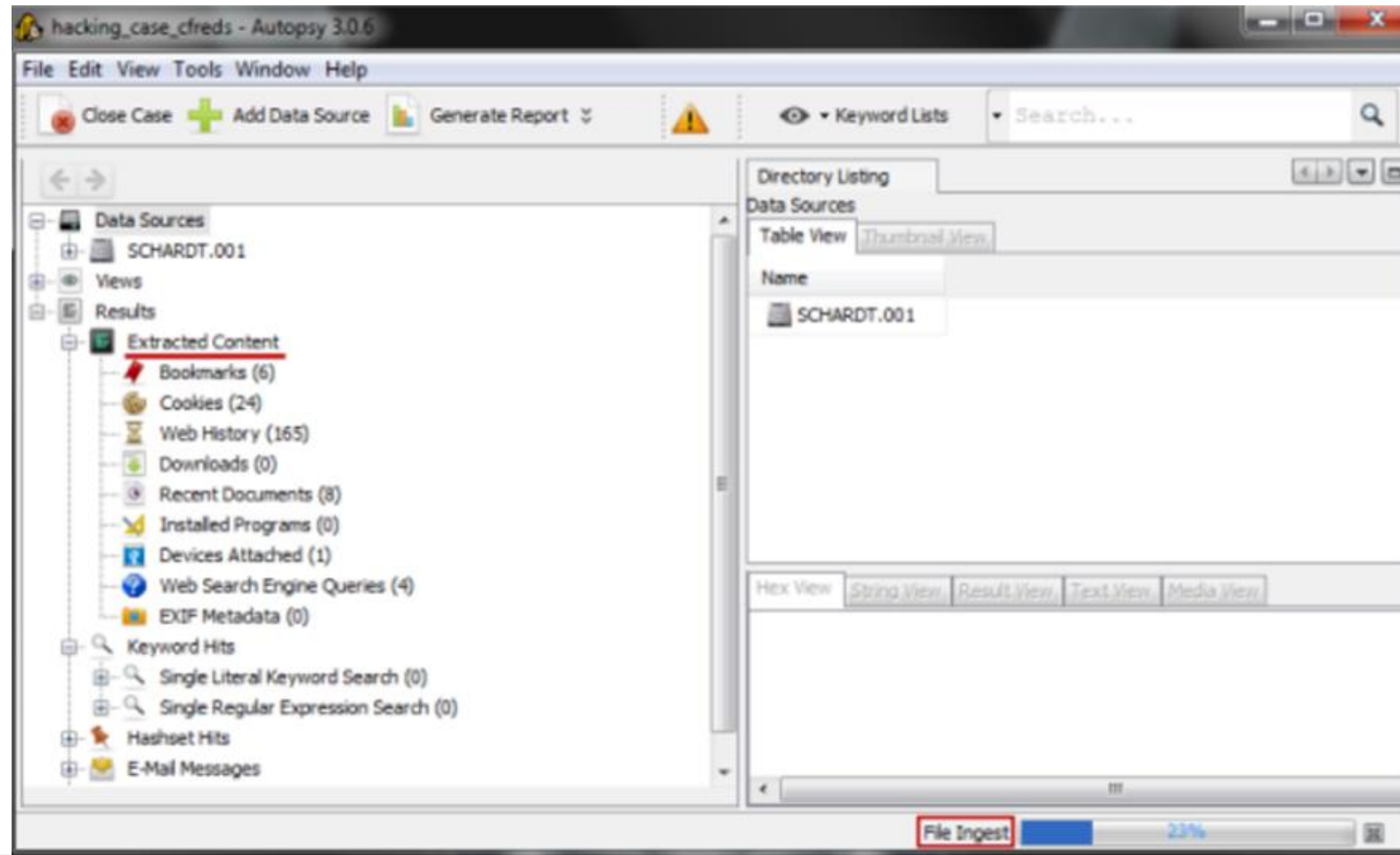
Exif Image Parser

Keyword Search





# Autopsy tool



David del Olmo tuvo un caso de un empleado directivo de una gran empresa tecnológica que iba a ser despedido. “Se negaba entregar los medios tecnológicos que le proporcionó la empresa (portátil y disco externo)”, por lo que la empresa **empieza a sospechar que está realizando proyectos para otra de la competencia**”.

Para intentar corroborar esta tesis, se cita al empleado en una notaría mediante un burofax, para que el notario pudiera dar fe de lo que allí iba a ocurrir. “El representante legal de la empresa preguntó a este empleado si hacía entrega de todos los datos y si había borrado algo”. ¿La respuesta delante del notario? Que no había borrado nada.

Sin embargo, y una vez realizada la clonación del disco y la posterior recuperación de datos, “obtuve un “timeline” del usuario donde conseguí demostrar que **el usuario durante la madrugada previa había borrado archivos de la empresa y correos electrónicos**”. De hecho, se había levantado a las 5 de la mañana para proceder a todo esta eliminación de archivos antes de presentarse en la notaria donde, probablemente, no se esperaba la presencia de un perito.



David del Olmo

# *Chkrootkit*

Permite localizar “*rootkits*”



## *Chkrootkit*

Chkrootkit

check\_wtmpx.c -> UNIX

Ifpromisc.c (modo  
promiscuo)

chkproc.c -> LKM

chklastlog.c -> LOGINS  
(lastlog)

chkdirs.c -> KERNEL

Chkwtmp.c ->  
LOGINS(wtmp)



# Chkrootkit

\$ sudo chkrootkit

```
Searching for anomalies in shell history files...      nothing found
Checking `asp'...                                    not infected
Checking `bindshell'...                              not infected
Checking `lkm'...                                    chkproc: nothing de
tedected
chkdirs: nothing detected
Checking `rexedcs'...                                not found
Checking `sniffer'...                                lo: not promisc and
no packet sniffer sockets
wlp3s0: PACKET SNIFFER(/usr/sbin/dhclient[14526], /usr/sbin/wpa_supplicant[773]
, /usr/sbin/wpa_supplicant[773])
Checking `w55808'...                                 not infected
Checking `wted'...                                   chkwtmp: nothing de
leted
Checking `scalper'...                                not infected
Checking `slapper'...                                not infected
Checking `z2'...                                     chklastlog: nothing
deleted
Checking `chkutmp'...                                The tty of the fol
lowing user process(es) were not found
in /var/run/utmp !
! RUID      PID TTY   CMD
! linuxhi+  14958 pts/0  bash
! linuxhi+  14964 pts/0  su
```

# Chkrootkit

\$ sudo chkrootkit > resultados  
\$ less resultados

```
ROOTDIR is '/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
:
```

# Lo que hizo Sony

El 31 de octubre del 2005, el experto en seguridad informática Mark Russinovich publicó su descubrimiento en [su blog](#) sobre un software espía, conocido como rootkit, que se había instalado secretamente en su ordenador. Dedujo que el rootkit estaba conectado con el reproductor de música que venía incluido en CDs de música de Sony. El programa oculto rootkit se usaba para espiar a los usuarios y sus hábitos de escucha, compartiendo esta información con Sony, así como evitaba la lectura [del disco](#) por parte de terceros.

En el proceso de espionaje, el rootkit [creaba fallos adicionales de seguridad](#) que abrían las puertas para otros ataques peores. Incluso si los usuarios detectaban el rootkit, desinstalarlo de forma segura sin dañar la máquina era otro problema.

El rootkit se cargó en un total de [aproximadamente 25 millones de CDs](#) e [infectó más de 550.000 redes en más de cien países, incluyendo miles de redes militares y de defensa de los EE.UU.](#)

Pero el presidente de Sony BMG, Thomas Hesse, desestimó totalmente el problema, y declaró [textualmente "La mayoría de la gente, creo, ni siquiera sabe lo que es un Rootkit, así que ¿por qué han de preocuparse?"](#). La prensa publicó lo que Sony estaba haciendo de forma secreta a la propiedad privada de los usuarios y Sony se vio forzada a pagar [numerosos procesos judiciales](#) y recuperar la confianza de los usuarios tan pronto como fuese posible.

## *Foremost*

Permite recuperar archivos borrados en  
linux





## *Foremost*

**Desarrollada por el Gobierno de EEUU**

**Borrar archivo  $\neq$  Eliminación definitiva**

**Multitud de formatos**

jpg, gif, png, bmp, avi, tiff, mp4, exe, mpg,  
wav, asf, wma, mp3, fws, riff, wmv, mov,  
pdf, ole, doc, docx, xls,etc

# Foremost

```
$ foremost -v -t <file_type> -i <disk_location> -o <output>
```

```
solvetic@solvetic-Ubuntu:~$ foremost -v -t docx -i /dev/sda1 -o ~/recovery/
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Oct  7 15:33:24 2019
Invocation: foremost -v -t docx -i /dev/sda1 -o /home/solvetic/recovery/
Output directory: /home/solvetic/recovery
Configuration file: /etc/foremost.conf
Processing: stdin
|-----
File: stdin
Start: Mon Oct  7 15:33:24 2019
Length: Unknown

Num      Name (bs=512)      Size      File Offset      Comment
```

# Prisión para detenido en Cornellá por integrar la red de captación del Dáesh

Al detenido, además, se le intervino diverso material con archivos borrados referentes a acciones terroristas: vídeos propagandísticos y de apología de la organización terrorista, así como cánticos árabes de llamamiento y ánimo a practicar la yihad o guerra santa.

Este hombre fue arrestado junto a otro presunto terrorista, también de origen marroquí, que quedó en libertad ayer después de declarar ante la Guardia Civil.

Según el Ministerio del Interior, los dos detenidos mantenían contactos con individuos en zonas de conflicto, a los que ofrecían su apoyo y animaban a continuar con sus actividades para el terrorismo yihadista.

1. w  
2. w  
3. w  
w  
w  
w  
o  
o  
o

**¡GRACIAS!**

**¿ALGUNA DUDA?**

IV  
DAS

Video module

H1-Headline

Menu

|||

|||