#CátedrasCiber

Módulo II: Análisis Forense y Esteganografía

30/10/2024

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

Entidad colaboradora:
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Análisis Forense

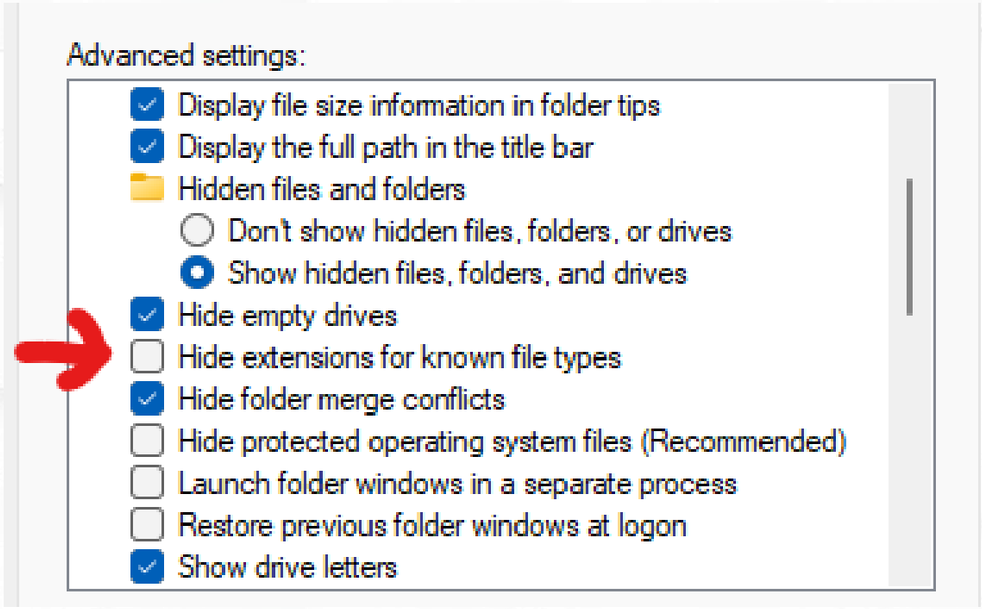
¿Qué es el análisis forense?

- Buscar datos dada una fuente de información sin alterar su estado.
- Las fuentes de información pueden ser muy variadas, nos vamos a centrar en:
  - Análisis de **ficheros** comunes
  - Análisis de sistemas de **almacenamiento**
  - Análisis de **memoria (RAM)**
  - Análisis de **tráfico de red**

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Ficheros: Extensiones y Magic Bytes

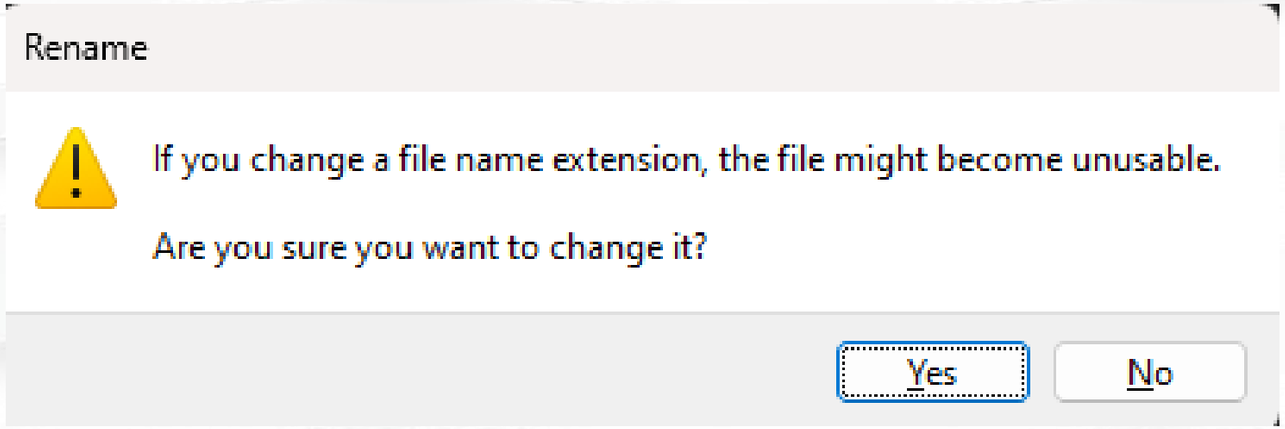
- Windows: antes de nada, configuramos nuestra máquina para que no oculte las extensiones de ficheros.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Ficheros: Extensiones y Magic Bytes

- ¿Cómo sabe el sistema operativo qué tipo de fichero tenemos?
  - Windows: por **extensión** (exe, png, txt, ...)
  - Resto: más frecuente por **magic bytes.**



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Ficheros: Extensiones y Magic Bytes

- ¿Qué son exactamente los magic bytes?

- **Patrón de bytes**
- Generalmente al **comienzo** del fichero
- Identifican el contenido del fichero
- Herramienta **file**: identifica tipo fichero por su patrón de bytes

Ejemplos: https://en.wikipedia.org/wiki/List_of_file_signatures

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Ficheros: Extensiones y Magic Bytes

- Otra herramienta muy potente es **binwalk**

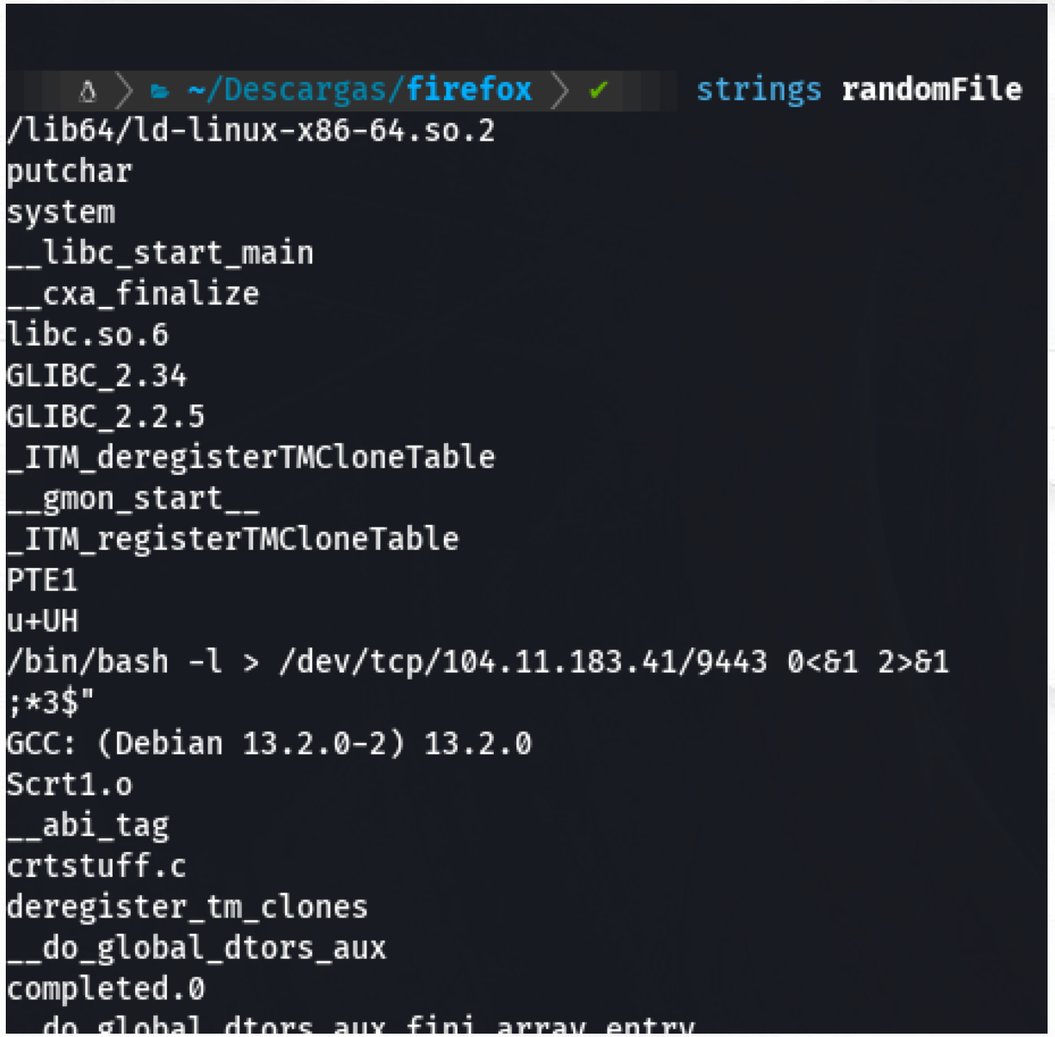
```
root@kali:~# binwalk -B ddwrt-linksys-wrt1200ac-webflash.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TRX firmware header, little endian, image size: 37883904 by
28            0x1C            uImage header, header size: 64 bytes, header CRC: 0x780C274
92            0x5C            Linux kernel ARM boot executable zImage (little-endian)
2460          0x99C           device tree image (dtb)
23432         0x5B88          xz compressed data
23776         0x5CE0          xz compressed data
2117484       0x204F6C        device tree image (dtb)
3145756       0x30001C        UBI erase count header, version: 1, EC: 0x0, VID header off
```

- Analiza el **fichero completo** buscando patrones conocidos
- Permite extraer los ficheros identificados
- Viene instalada por defecto en Kali

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Ficheros: Extensiones y Magic Bytes

- ¿Y si falla todo lo anterior?
- **Strings**, xxd, ¡RegEX!
- Podemos obtener pistas gracias a los **caracteres imprimibles** que contiene el fichero.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Almacenamiento

AUTOPSY
DIGITAL FORENSICS

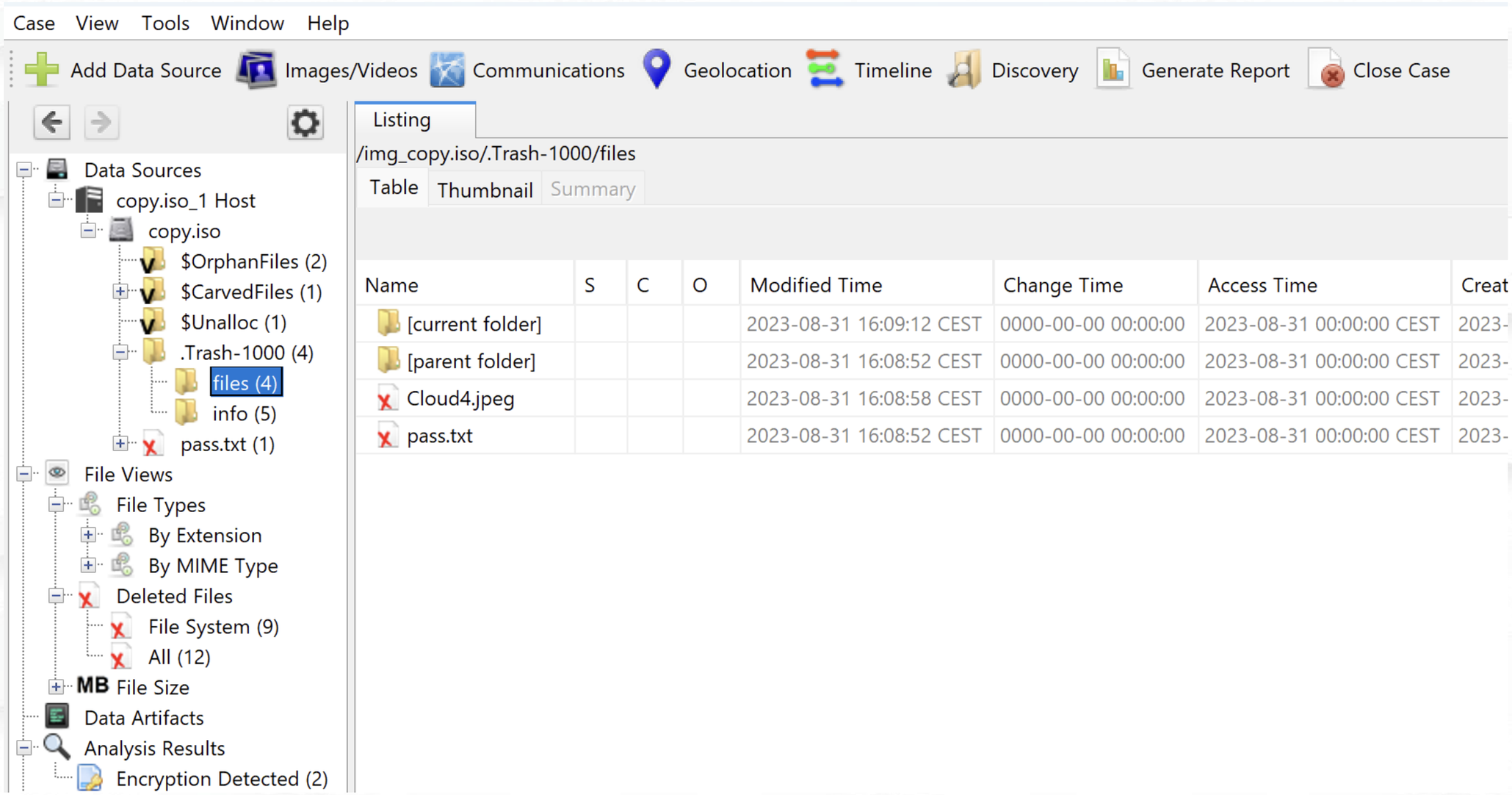
- Con almacenamiento, incluimos:
  - Diferentes **tipos de soporte**
    - Discos duros / sólidos (HDD, SSD)
    - Pendrives
    - Discos virtuales
  - Diferentes **sistemas de ficheros**
    - NTFS, FAT32, EXT4, etc.

- Además, existen múltiples formatos para almacenar la evidencia

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Almacenamiento

AUTOPSY
DIGITAL FORENSICS



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

- Podemos registrar el tráfico de red para su posterior análisis.
- Entre otros, observamos peticiones DNS, tráfico HTTP…

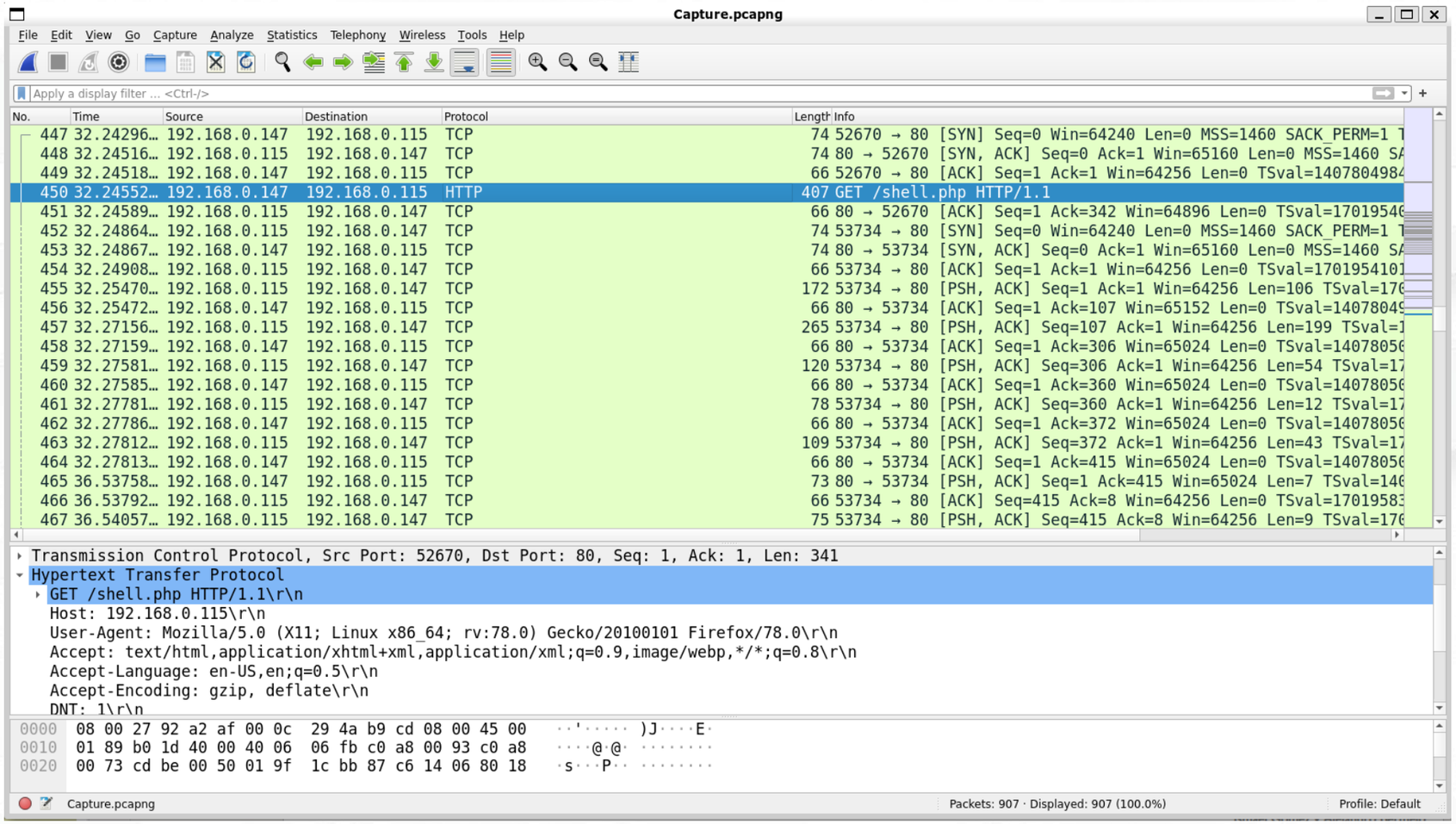
- Nota: Wireshark también puede analizar tráfico USB

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

Lista paquetes

Paquete analizado



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

- Generalmente tenemos cientos de paquetes
- Es importante aprender a **filtrar la información** relevante
  - Por protocolo: usar el nombre. Ej: HTTP

    `http`
  - Por puerto origen / destino

    `tcp.port == 12345`
  - Paquetes UDP que contengan ciertos bytes:

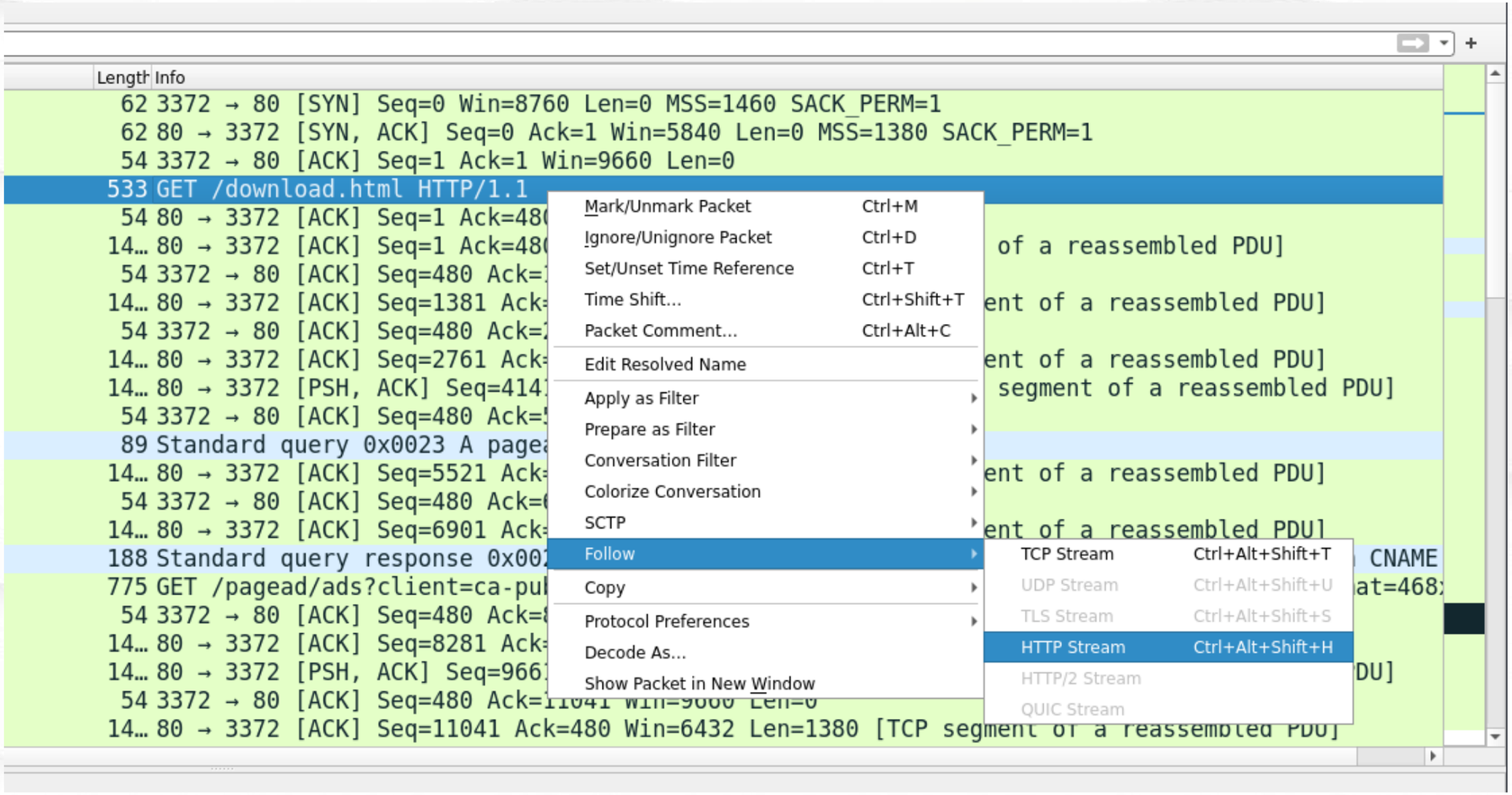
    `udp contains AA:BB:CC`
  - Referencia completa:

    https://wiki.wireshark.org/DisplayFilters

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

- Para ver paquetes relacionados con otros usamos “**Follow**”

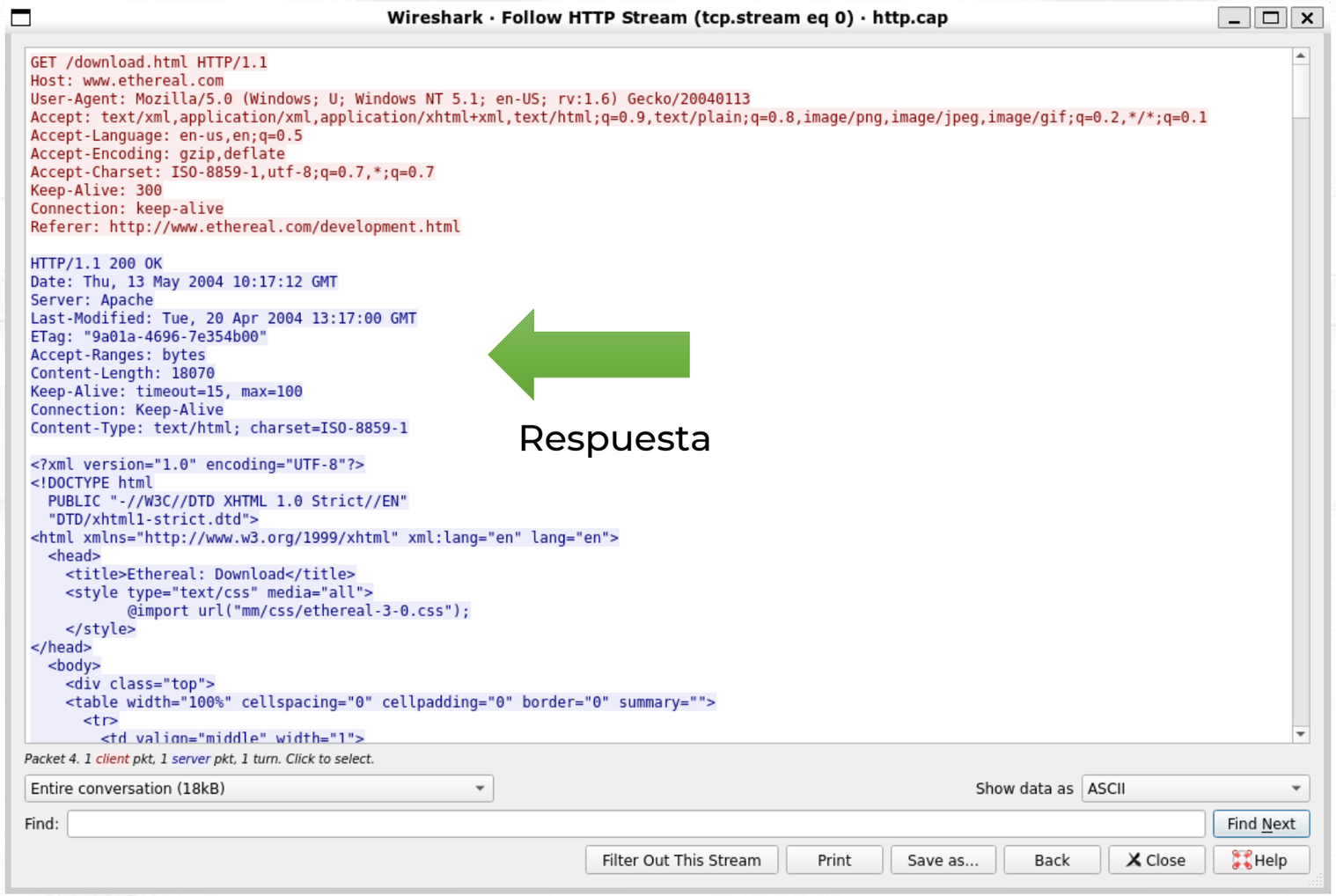


Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

- Ejemplo: petición y respuesta HTTP

Petición



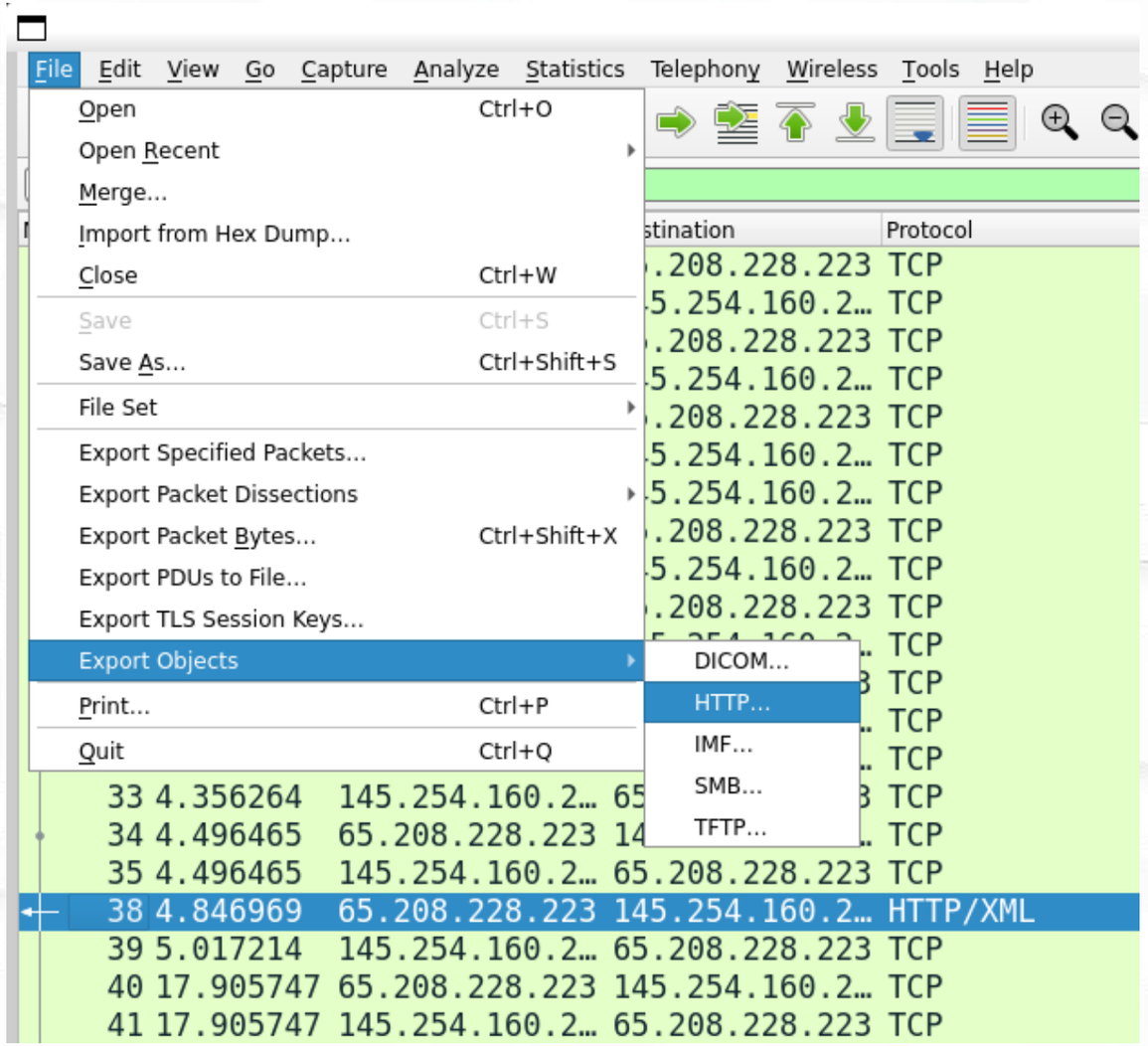
Respuesta

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

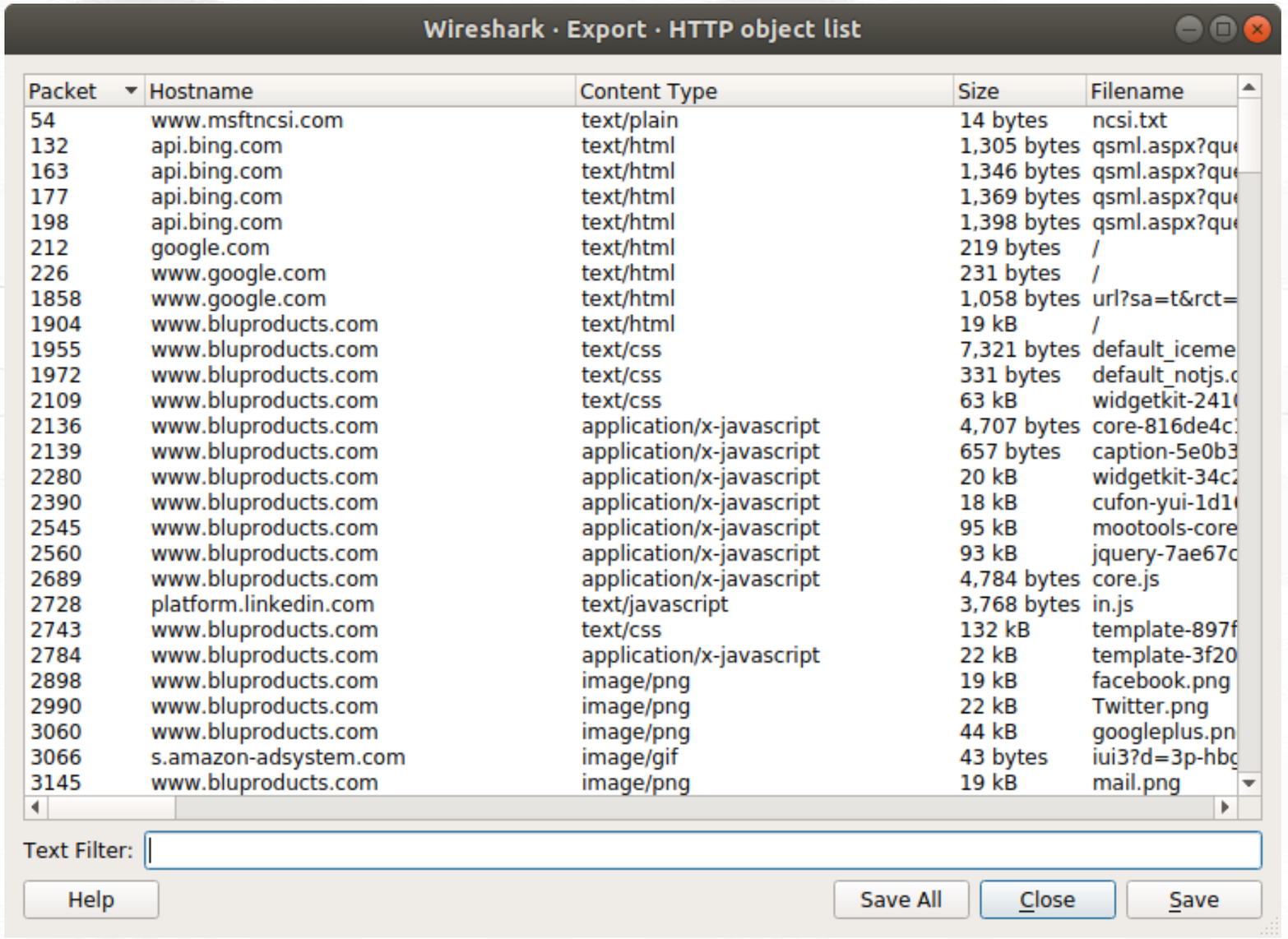
Podemos **exportar** rápidamente **objetos**.

Ej: el fichero que se ha descargado un usuario por HTTP.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Tráfico de red

- Truco 1: Para ahorrar tiempo es interesante ver los **resúmenes** que genera Wireshark: **participantes y protocolos**

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	267	100.0	303137	17 k
Ethernet	100.0	267	1.4	4328	247
Internet Protocol Version 6	16.1	43	0.6	1720	98
User Datagram Protocol	16.1	43	0.1	344	19
Simple Service Discovery Protocol	16.1	43	2.1	6278	358
Internet Protocol Version 4	81.6	218	1.4	4388	250
User Datagram Protocol	10.1	27	0.1	216	12
NetBIOS Name Service	9.0	24	0.8	2400	137
NetBIOS Datagram Service	0.7	2	0.1	164	9
SMB (Server Message Block Protocol)	0.7	2	0.1	260	14
SMB MailSlot Protocol	0.7	2	0.0	50	2
Microsoft Windows Browser Protocol	0.7	2	0.0	88	5
Dynamic Host Configuration Protocol	0.4	1	0.1	300	17
Transmission Control Protocol	68.9	184	1.3	4016	229
Hypertext Transfer Protocol	10.5	28	91.9		
Media Type	1.9	5	88.2		
Internet Group Management Protocol	2.6	7	0.0		
Address Resolution Protocol	2.2	6	0.1		

Ethernet · 11 | IPv4 · 8 | IPv6 · 2 | TCP · 15 | UDP · 8

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.1.1	28	4 kB	28	4 kB	0	0 bytes
192.168.1.151	190	290 kB	102	15 kB	88	276 kB
192.168.1.200	184	289 kB	88	276 kB	96	14 kB
192.168.1.255	26	4 kB	0	0 bytes	26	4 kB
224.0.0.1	4	240 bytes	0	0 bytes	4	240 bytes
224.0.0.252	2	120 bytes	0	0 bytes	2	120 bytes
239.255.255.250	1	60 bytes	0	0 bytes	1	60 bytes
255.255.255.255	1	342 bytes	0	0 bytes	1	342 bytes

- Truco 2: Ordenar por tamaño

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Análisis de RAM

- **La RAM es volátil:**

  el contenido se pierde al apagar el ordenador
- Contiene información muy interesante:
  - **Procesos en ejecución**, y sus datos asociados
  - **Conexiones** entrantes y salientes
  - **Ficheros** cacheados

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Análisis de RAM

Instrucciones de instalación en Kali:

1. **Clonamos el repositorio:**

```
git clone https://github.com/volatilityfoundation/volatility3
```

2. **Entramos a la carpeta y creamos entorno virtual (venv):**

```
cd volatility3
python3 -m venv venv
```

3. **Activamos el entorno y instalamos dependencias**

```
source venv/bin/activate
pip3 install -r requirements.txt
```

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Análisis de RAM

- ¡Cuidado con los tutoriales!

  Muchos están anticuados ☹

- Imprimir opciones y ver listado de plugins:

  ```
  python3 vol.py -h
  ```

- Uso general

  ```
  python3 vol.py -f fichero.raw os.plugin [parameters]
  ```

- Opciones de un plugin:

  ```
  python3 vol.py os.plugin -h
  ```

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Análisis de RAM

- Ejemplo 1: procesos en ejecución:

```
┌──(venv)─(rmartin㉿palalel)-[~/Tools/volatility3]
└─$ python3 vol.py -f '/home/rmartin/Desktop/Parallels Shared Folders/shared/memdump.raw' windows.pslist
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTimeFile output

4       0       System  0xa68ffbc7f080  159     -       N/A     False   2024-09-27 02:25:09.000000 UTC  N/A     Disabled
124     4       Registry        0xa68ffee02080  4       -       N/A     False   2024-09-27 02:25:07.000000 UTC  N/A     Disabled
432     4       smss.exe        0xa6810086d040  2       -       N/A     False   2024-09-27 02:25:09.000000 UTC  N/A     Disabled
544     532     csrss.exe       0xa68104ed3080  12      -       0       False   2024-09-27 02:25:14.000000 UTC  N/A     Disabled
620     532     wininit.exe     0xa68105028140  2       -       0       False   2024-09-27 02:25:14.000000 UTC  N/A     Disabled
628     612     csrss.exe       0xa68104cb6240  14      -       1       False   2024-09-27 02:25:14.000000 UTC  N/A     Disabled
692     612     winlogon.exe    0xa68105040080  5       -       1       False   2024-09-27 02:25:14.000000 UTC  N/A     Disabled
764     620     services.exe    0xa6810520e240  5       -       0       False   2024-09-27 02:25:14.000000 UTC  N/A     Disabled
784     620     lsass.exe       0xa6810507d080  11      -       0       False   2024-09-27 02:25:14.000000 UTC  N/A     Disabled
912     764     svchost.exe     0xa681061d7240  16      -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
948     692     fontdrvhost.ex  0xa68105111140  6       -       1       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
940     620     fontdrvhost.ex  0xa681061c1080  6       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
412     764     svchost.exe     0xa6810624f2c0  9       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
548     764     svchost.exe     0xa681062772c0  4       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
76      692     dwm.exe 0xa681062bc080  22      -       1       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
1056    764     svchost.exe     0xa6810604e340  5       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
1148    764     svchost.exe     0xa6810607e300  5       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
1204    764     svchost.exe     0xa681060ac300  4       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
1212    764     svchost.exe     0xa681060aa300  3       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
1244    764     svchost.exe     0xa681060b6300  8       -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
1264    764     svchost.exe     0xa681060d4240  11      -       0       False   2024-09-27 02:25:15.000000 UTC  N/A     Disabled
```

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Análisis de RAM

- Ejemplo 2: conexiones abiertas

```
┌──(venv)─(rmartin㉿palalel)-[~/Tools/volatility3]
└─$ python3 vol.py -f '/home/rmartin/Desktop/Parallels Shared Folders/shared/memdump.raw' windows.netscan
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×a68100565910  UDPv4   0.0.0.0 0       *       0               8384    powershell.exe  2024-09-26 17:30:04.000000 UTC
0×a68100565910  UDPv6   ::      0       *       0               8384    powershell.exe  2024-09-26 17:30:04.000000 UTC
0×a68100565dc0  UDPv4   0.0.0.0 0       *       0               8384    powershell.exe  2024-09-26 17:30:04.000000 UTC
0×a68100566720  UDPv4   0.0.0.0 0       *       0               8384    powershell.exe  2024-09-26 17:30:04.000000 UTC
0×a68100566720  UDPv6   ::      0       *       0               8384    powershell.exe  2024-09-26 17:30:04.000000 UTC
0×a68100566a40  UDPv4   0.0.0.0 0       *       0               8384    powershell.exe  2024-09-26 17:30:04.000000 UTC
0×a68100906050  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       620     wininit.exe     2024-09-27 02:25:15.000000 UTC
0×a68100906050  TCPv6   ::      49665   ::      0       LISTENING       620     wininit.exe     2024-09-27 02:25:15.000000 UTC
0×a681009069f0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       784     lsass.exe       2024-09-27 02:25:15.000000 UTC
0×a68100907910  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       784     lsass.exe       2024-09-27 02:25:15.000000 UTC
0×a68100907910  TCPv6   ::      49664   ::      0       LISTENING       784     lsass.exe       2024-09-27 02:25:15.000000 UTC
0×a68100907a70  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       412     svchost.exe     2024-09-27 02:25:15.000000 UTC
0×a68100907bd0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       412     svchost.exe     2024-09-27 02:25:15.000000 UTC
0×a68100907bd0  TCPv6   ::      135     ::      0       LISTENING       412     svchost.exe     2024-09-27 02:25:15.000000 UTC
0×a68100907e90  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       620     wininit.exe     2024-09-27 02:25:15.000000 UTC
0×a681048e1200  UDPv4   0.0.0.0 5353    *       0               7192    msedge.exe      2024-09-26 17:28:28.000000 UTC
0×a681048e1200  UDPv6   ::      5353    *       0               7192    msedge.exe      2024-09-26 17:28:28.000000 UTC
0×a6810518da20  TCPv4   10.0.2.15       49725   20.190.177.21   443     CLOSED  7180    OneDrive.exe    2024-09-26 17:25:41.000
0×a681061148a0  TCPv4   10.0.2.15       49784   185.89.208.19   443     CLOSE_WAIT      7336    msedge.exe      2024-09-26 17:2
0×a681061995c0  UDPv4   10.0.2.15       138     *       0               4       System  2024-09-27 02:25:15.000000 UTC
```

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía

¿Qué es la esteganografía?

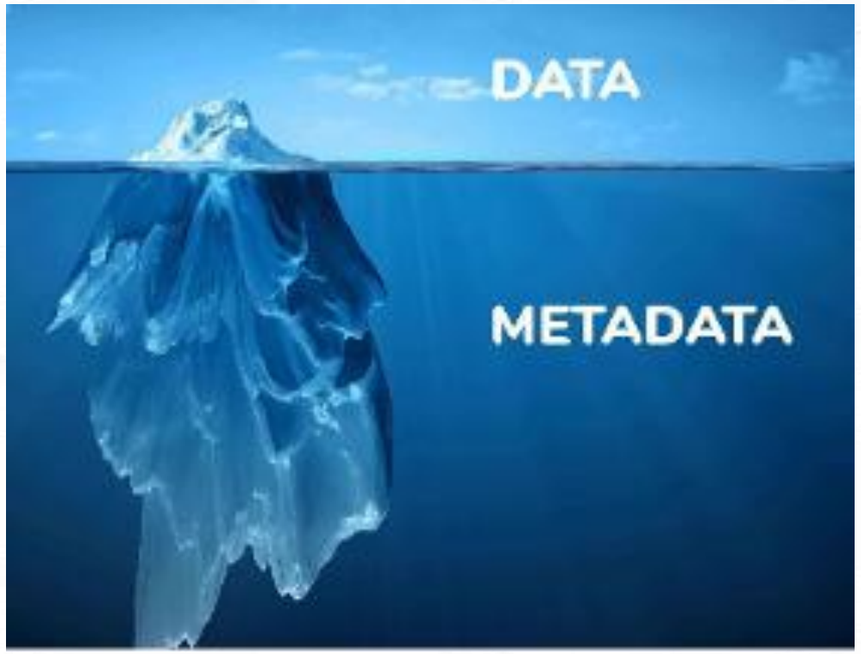
La **esteganografía** trata el estudio y aplicación de técnicas que permiten ocultar información dentro de otra de diferente tipo (o no), de modo que no se perciba su existencia.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Metadatos

“Datos sobre los datos”. Son la primera fuente de información sobre lo que estamos analizando. Nos puede dar información acerca del contenido, la calidad, histórico...

A veces, incluso flags.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Metadatos – Herramientas: Exiftool

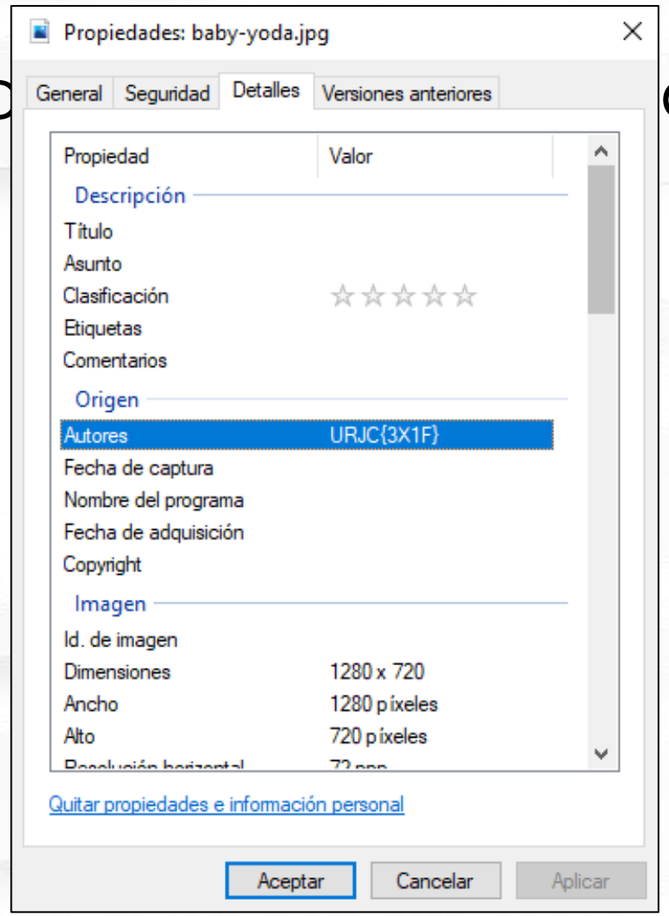
Exiftool es una de las herramientas más extendidas para analizar metadatos en Linux.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Metadatos – Herramientas: Exiftool

Exiftool es una de las herramientas más extendidas

p da




```
└─$ exiftool baby-yoda.jpg
ExifTool Version Number         : 12.16
File Name                       : baby-yoda.jpg
Directory                       : .
File Size                       : 82 KiB
File Modification Date/Time     : 2021:10:22 00:17:08+02:00
File Access Date/Time           : 2021:10:22 00:17:08+02:00
File Inode Change Date/Time     : 2021:10:22 00:17:08+02:00
File Permissions                : rw-------
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Artist                          : URJC{3X1F}
XP Author                       : URJC{3X1F}
Padding                         : (Binary data 2060 bytes, use -b option to extract)
About                           : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator                         : URJC{3X1F}
Image Width                     : 1280
Image Height                    : 720
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1280x720
Megapixels                      : 0.922
```


Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

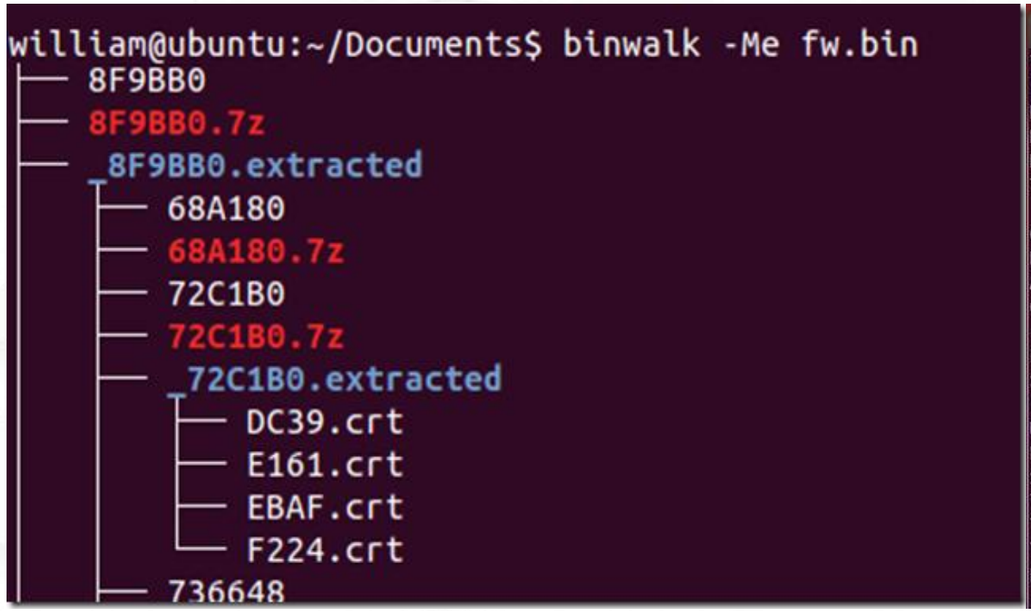
Una técnica común en esteganografía es aquella que consiste en ocultar ficheros dentro de otros (ya sean del mismo tipo o no).

Ocultar un fichero entre los bytes de otro es una técnica que debe hacerse con cuidado, especialmente si el objetivo es minimizar la detección del uso de esta técnica.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros - Herramientas

Dos de las herramientas más extendidas para operar sobre información oculta en ficheros son Binwalk y Foremost.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

En las competiciones, lo más habitual en la categoría de esteganografía es que se aplique sobre imágenes (JPG, PNG, BMP...).

Para tratar con imágenes, hay una suit de herramientas muy útil: stego-toolkit.

https://github.com/DominicBreuker/stego-toolkit

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Es una colección de herramientas de esteganografía de gran utilidad para los CTF.
En su repositorio de GitHub, podemos ver una lista detallada de las herramientas que podríamos utilizar según los distintos casos, y el uso de cada una de ellas.
En concreto, serán de gran utilidad sus scripts *check_jpg.sh* y *check_png.sh*

Tool	Description	How to use
file	Check out what kind of file you have	`file stego.jpg`
exiftool	Check out metadata of media files	`exiftool stego.jpg`
binwalk	Check out if other files are embedded/appended	`binwalk stego.jpg`
strings	Check out if there are interesting readable characters in the file	`strings stego.jpg`
foremost	Carve out embedded/appended files	`foremost stego.jpg`
pngcheck	Get details on a PNG file (or find out is is actually something else)	`pngcheck stego.png`
identify	GraphicMagick tool to check what kind of image a file is. Checks also if image is corrupted.	`identify -verbose stego.jpg`
ffmpeg	ffmpeg can be used to check integrity of audio files and let it report infos and errors	`ffmpeg -v info -i stego.mp3 -f null -` to recode the file and throw away the result

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Una alternativa online a tener muy en cuenta es Aperi'Solve.
Esta herramienta tiene la funcionalidad de analizar diferentes perfiles de color de una imagen, lo cual puede ser muy útil.
Además, incluye algunas herramientas como Zsteg (también incluida en stego-toolkit).

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Un detalle a observar es que, tanto en Aperi'Solve como en algunas de las herramientas de stego-toolkit se solicita una contraseña.
Esto es así porque algunas herramientas de esteganografía protegen el contenido oculto de manera que, si no se posee la contraseña con la que se ocultó, no podremos recuperarlo.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

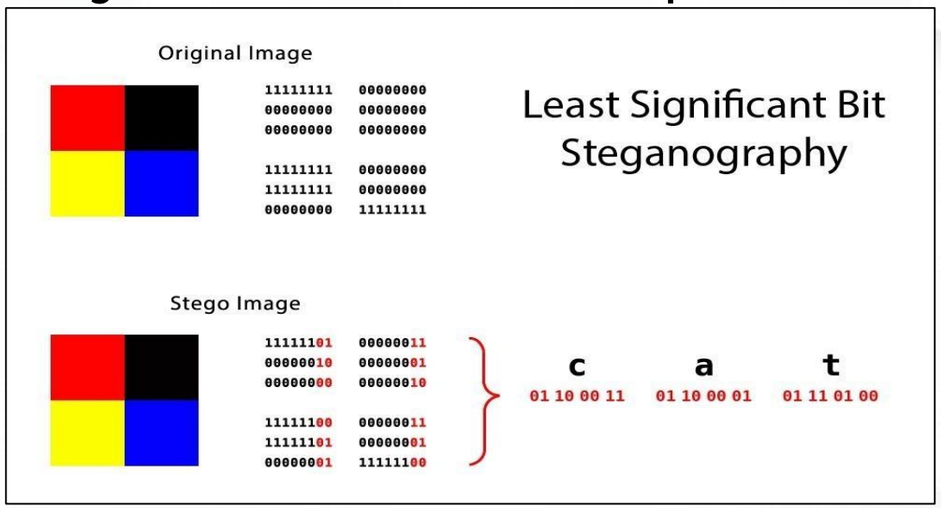
Esteganografía sobre ficheros

Por ello, es de gran utilidad contar con una herramienta como Stegseeek.
Esta herramienta permite realizar ataques de diccionario sobre imágenes en formato JPG.
También permite un ataque de fuerza bruta sobre las imágenes que hayan utilizado Steghide (otra herramienta de esteganografía sobre imágenes) y su funcionalidad de *contraseña segura* para ocultar la información.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Least Significant Bit (LSB)

Otra técnica bastante extendida en el arte de ocultar información dentro de información es la de LSB.
Se trata de modificar los bits menos significativos de cada píxel de una imagen o vídeo, de forma que el mensaje se oculte en esos bits.
Esta técnica tiene múltiples variantes, como por ejemplo escoger sólo el canal rojo/verde/azul/alpha de una imagen.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

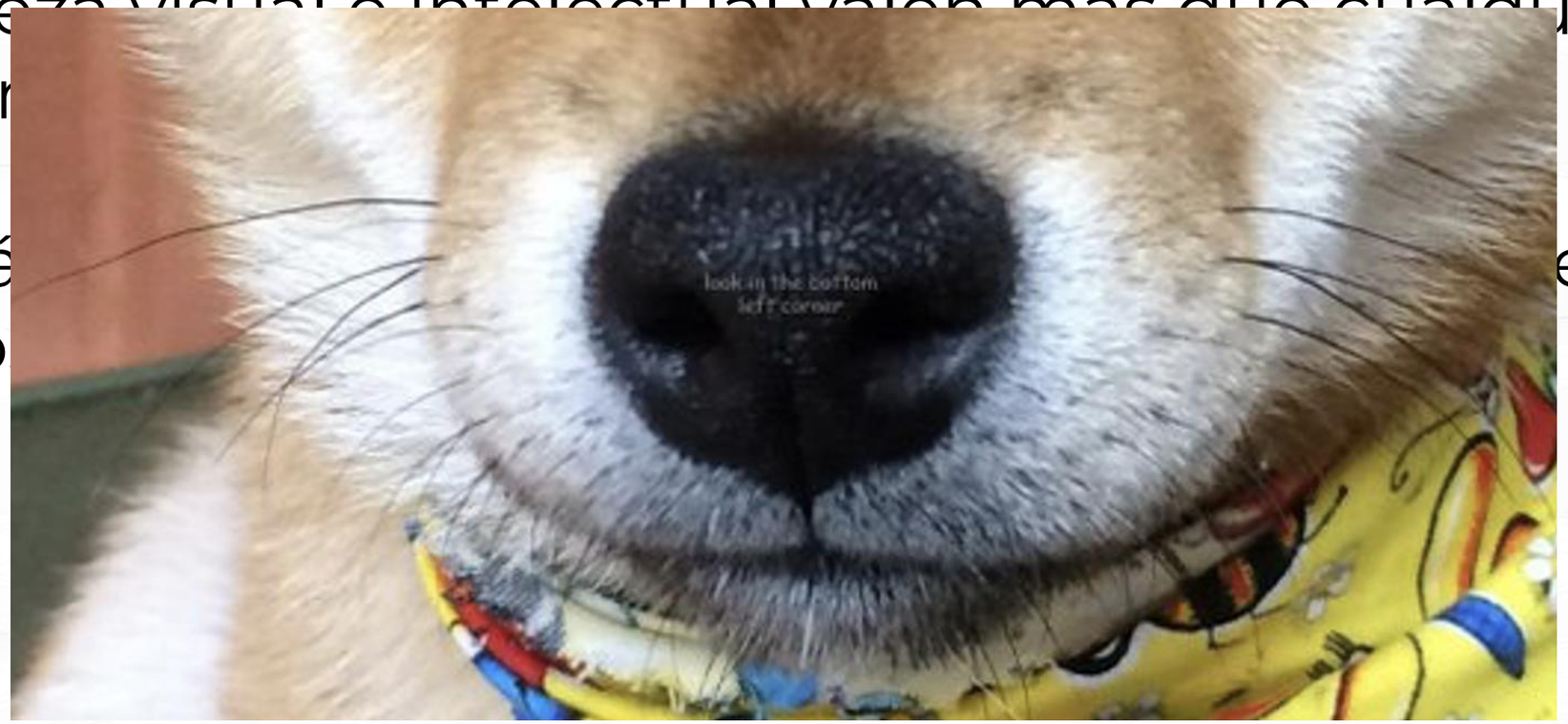
Además de todo esto, hay que pensar que a veces la agudeza visual e intelectual valen más que cualquier herramienta.

Habrá ocasiones en que la información esté ahí, pero no nos hemos fijado lo suficiente.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Además de todo esto, hay que pensar que a veces la agudeza visual e intelectual valen más que cualquier herra

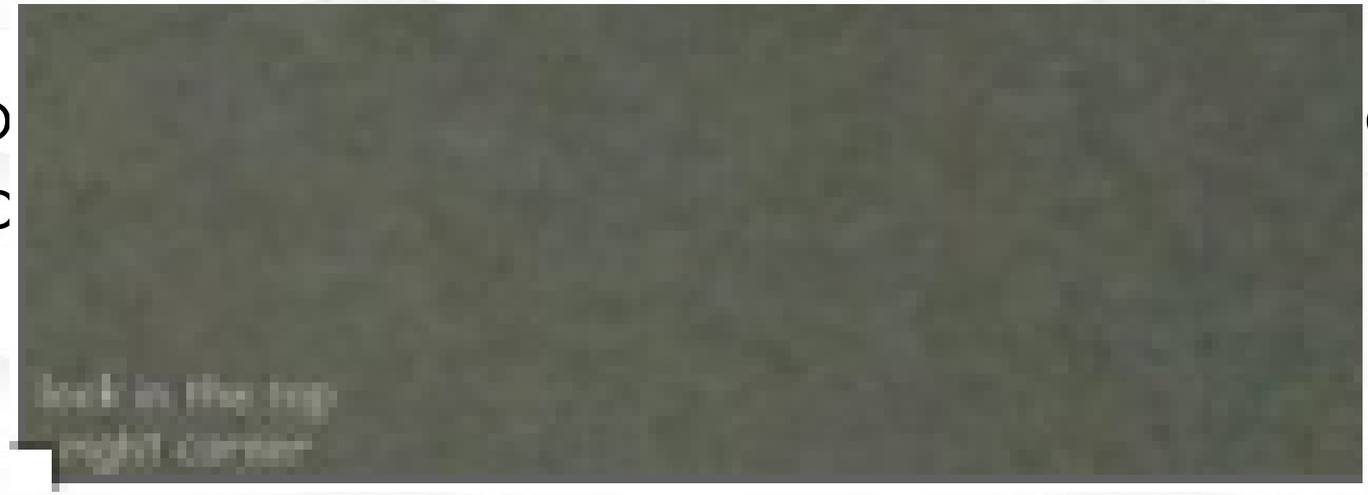


Habrá ero no no

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Además de todo esto, hay que pensar que a veces la agudeza visual e intelectual valen más que cualquier herramienta.

Habrá ocasio 

ero no nos hemc

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Además de todo esto, hay que pensar que a veces la agudeza visual e intelectual valen más que cualquier herramienta.

Habrá ocasiones  esté ahí, pero no nos hemos fija

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Otras veces, será suficiente con jugar con los ajustes de curvas y niveles de herramientas de edición como GIMP para lograr ver mejor lo que oculta una imagen.

Esteganografía es de las pocas categorías en las que una idea feliz puede ser la solución al reto. ¡Aplica todas las que se te ocurran!

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

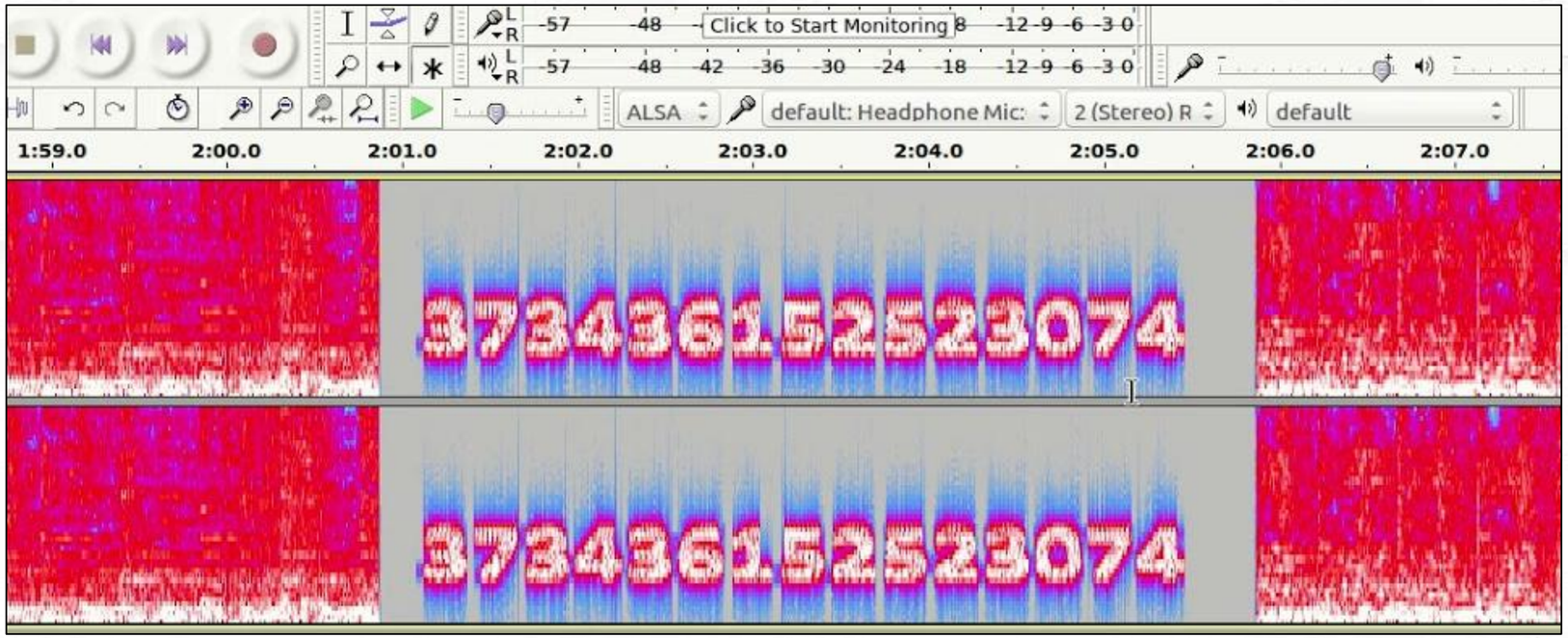
Pero no todo se reduce a imágenes. También es habitual encontrar retos con vídeo/audio con información oculta de alguna manera.

Por ejemplo, es habitual encontrar retos que esconden información en los espectogramas de las ondas de audio.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

Esteganografía sobre ficheros

Para estos casos, herramientas de edición de audio como Audacity o Sonic Visualiser pueden sernos de gran utilidad.



Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

La realidad de la categoría: 99% Guess The Tool, 1% habilidad

Por desgracia, los retos de esteganografía, salvo que estén bien configurados, la mayoría de las veces tratan más de romperse la cabeza buscando la herramienta que resuelva el reto que de desarrollar alguna habilidad.

No es una categoría que goce de mucha popularidad entre los participantes de las competiciones, pero hay muchas que la incluyen y debéis estar preparados.

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

¡SORPRESA! Premios en el CTF Final

Gracias a la colaboración de la entidad CIC Consulting Informático ofreceremos dos premios a los primeros puestos de la competición.

CIC Consulting Informático

Raúl Martín Santamaría
Isaac Lozano Osorio
Sergio Pérez Peló

#CátedrasCiber

Módulo II:
Análisis Forense y Esteganografía

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

Entidad colaboradora:
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria