

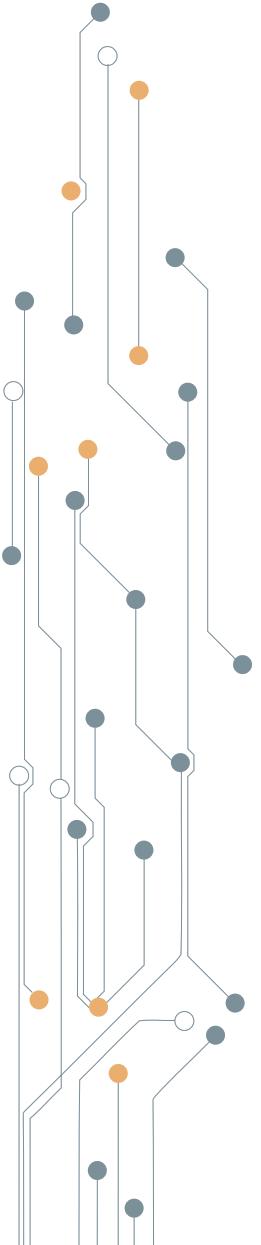


Análisis Forense de red: análisis de log y tráfico de red

Telefónica

EDUCACIÓN DIGITAL

Índice



1 | Análisis de log y tráfico de red

3

1. Análisis de log y tráfico de red

El análisis de la red describe el proceso de captura e interceptación de datos en tiempo real. Registrando todos los paquetes tanto entrantes como salientes que interactúan en un punto de conexión de la red. Esta interceptación de los datos puede dar respuesta a la gran pregunta de qué está ocurriendo en la red.

Los análisis de la red se pueden realizar gracias a la existencia de herramientas que son capaces de monitorizar todo el tráfico de comunicaciones capturando el intercambio de datos. Al proceso de capturar el tráfico de red se le conoce también como sniffing. Estas herramientas capturan los datos en bruto, llamados datos de tipo RAW en inglés, y analizan la información contenida en ellos, ayudando con esta reconstrucción al auditor a entender, de una manera más clara, el flujo de información. Esto permitirá descubrir ciertos comportamientos como pueden ser:

- Actividad maliciosa en la red.
- Ancho de banda inestable con picos y caídas de rendimiento.
- Aplicaciones inseguras en la organización.
- Protocolos inseguros permitidos y sados en la red.
- Por ende, Sistemas inseguros.

Existen en el Mercado numerosas aplicaciones que son capaces de monitorizar la red. Estas herramientas se pueden encontrar en formatos libres o comerciales. Cada aplicación estará diseñada con diferentes características y el auditor será el que saque conclusiones.

Es por tanto que la elección de la herramienta de análisis de red debe ser hecha por el auditor, seleccionando la que mejor se adapte a su forma de trabajar.

A la hora de evaluar un análisis de paquetes se suelen mirar los siguientes aspectos:

- Lista de protocolos soportados y reconocidos en la red.
- Oferta de soporte técnico.
- Escalabilidad de la herramienta para análisis en grandes redes.
- Funcionamiento y arquitectura de la misma evaluar el impacto.
- Capacidad de trabajar bajo línea de comandos para poder configurar scripts automáticos.

Todos los analizadores de paquetes soportan varios tipos de protocolos. La gran mayoría de estas herramientas soportan protocolos conocidos como SMTP, DHCP, DNS o HTTP, pero no todas pueden interpretar protocolos no tan tradicionales. A la hora de elegir un analizador de paquetes, el auditor debe hacer especial énfasis en el soporte a protocolos. En cuanto a la capacidad de trabajo, una opción a tener en cuenta es que la herramienta tenga un soporte extenso a la línea de comandos a fin de poder automatizar ciertas tareas. El soporte técnico y la escalabilidad de la herramienta proporcionarán al auditor seguridad en el trabajo y tranquilidad, a la hora de poder consultar al equipo técnico ante cualquier duda o problema, para así abordar proyectos profesionales con garantías.

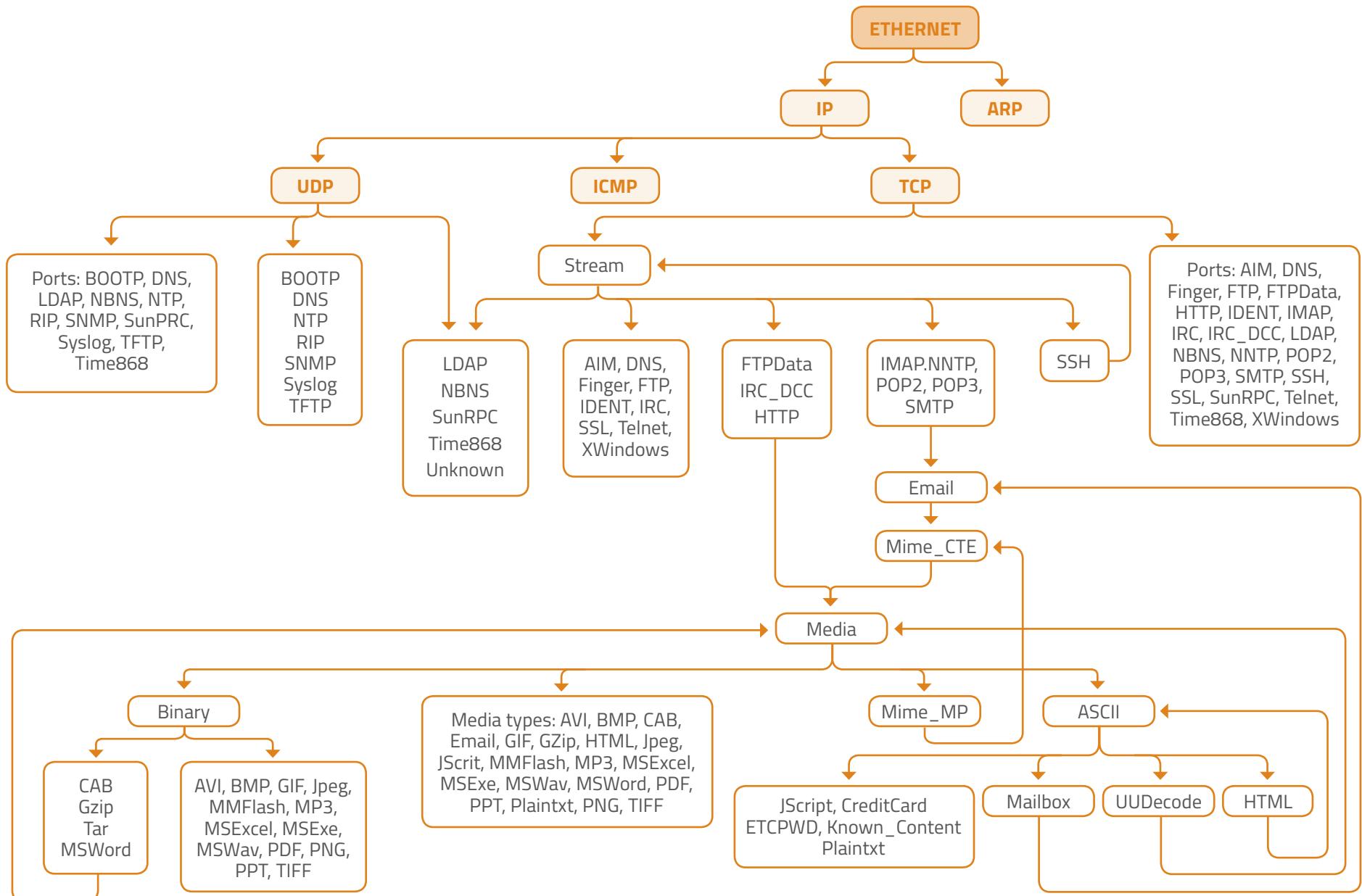


Imagen 64 Protocolos de Red

Un analizador de protocolos opera gracias a la recolección, interpretación y presentación de los paquetes capturados. La recolección la lleva a cabo gracias a un cambio en el comportamiento de la tarjeta de red. Este cambio de funcionamiento de la interfaz de red, llamado Modo Promiscuo, hace que se procese todo el tráfico de red que llegue hasta el equipo.

Una vez que el analizador ha recolectado todos los paquetes de la red, la herramienta intentará ordenar y traducir esta información en datos que el auditor pueda comprender fácilmente. Esta interpretación es el modo inicial en que un analista evaluará el tráfico de la red.

The screenshot displays the Wireshark interface with the following details:

- Title Bar:** *eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
- Menu Bar:** File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
- Toolbar:** Includes icons for file operations, search, and analysis tools.
- Filter Bar:** Shows "Expression..." and "Guardar" buttons.
- Table View:**

No.	Time	Source	Destination	Protocol	Length	Info
38989	1179.614621	213.162.209.61	192.168.10.177	HTTP	676	HTTP/1.1 200 OK (text/plain)
38990	1179.614650	192.168.10.177	213.162.209.61	TCP	54	41160>80 [ACK] Seq=713 Ack=623 Win=29856 Len=0
38991	1180.615810	192.168.10.177	213.162.209.61	TCP	54	41160>80 [FIN, ACK] Seq=713 Ack=623 Win=29856 Len=0
38992	1180.616319	213.162.209.61	192.168.10.177	TCP	60	80>41160 [ACK] Seq=623 Ack=714 Win=64239 Len=0
38993	1180.671353	213.162.209.61	192.168.10.177	TCP	60	80>41160 [FIN, PSH, ACK] Seq=623 Ack=714 Win=64239 Len=0
38994	1180.671408	192.168.10.177	213.162.209.61	TCP	54	41160>80 [ACK] Seq=714 Ack=624 Win=29856 Len=0
38995	1192.498179	fe80::4438:5614:1284: ff02::16		ICMPv6	90	Multicast Listener Report Message v2
- Details Pane:** Shows expanded details for the selected packet, including a summary of the frame, source and destination MAC addresses, and a detailed breakdown of the IP and TCP headers.
- Hex and ASCII Panes:** Displays the raw hex and ASCII representation of the selected packet's payload.
- Bottom Status Bar:** Shows the file path "/tmp/wireshark_pcapan_..._eth0_2...", the total number of packets (42916), the displayed count (42916), and the dropped count (0).

Imagen 65 Wireshark

Como último paso, la herramienta, haciendo uso de su base de conocimientos de protocolos de red, intentará presentar cada trama de red recolectada, decodificando los datos e interpretando lo que significa cada valor en cada posición del paquete.

A la hora de recolectar el tráfico de red existen opciones a tener en cuenta. Las dos más efectivas son:

- Conectar algún tipo de software o hardware de captura a un puerto que haga la función de Port-Mirror en un Switch de comunicaciones que centralice las comunicaciones.
- Evaluar la posibilidad de utilizar algún hardware que podamos añadir a la arquitectura de red existente, como una sonda, y que capture la información.

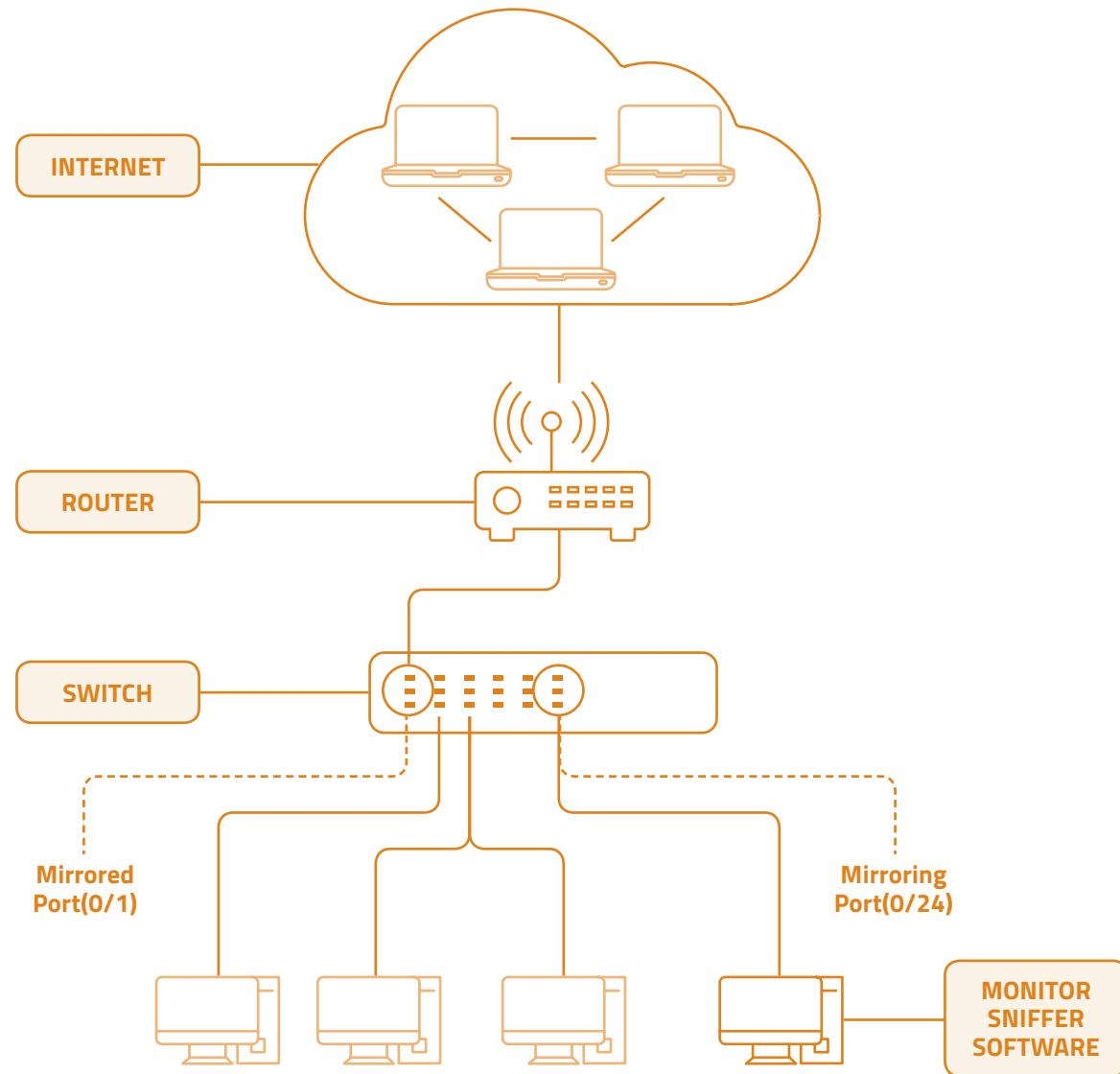


Imagen 66 Mirroring Port

Los sniffers más utilizados son:

- **Wireshark**, analizador de protocolos utilizado para el análisis de las comunicaciones y solucionar problemas existentes. Dispone de las características estándar de un analizador de protocolos muy completo.
- **Ettercap**, permite realizar análisis a redes con dispositivos switch. Soporta direcciones activas y pasivas de varios protocolos, así como la posibilidad de realizar ataques Man-in-the-middle.
- **Kismet**, es un analizador y detector de intrusiones para redes inalámbricas 802.11.
- **Tcpdump**, es un analizar de tráfico a través de línea de comandos. Permite la captura en tiempo real e ir mostrando los paquetes recibidos y enviados en la red.

Una de las aplicaciones más conocidas que realizan una recolección de paquetes es la herramienta Wireshark. Esta herramienta está disponible tanto para sistemas operativos Linux, como para Windows. Es una utilidad versátil y potente.

Una de las ventajas que tiene Wireshark es que captura los paquetes en tiempo real, y se puede exportar e importar dichas capturas para un posterior análisis.

Con Wireshark se puede elegir la interfaz a través de la cual se va a realizar el proceso de captura de paquetes y análisis del tráfico de red.



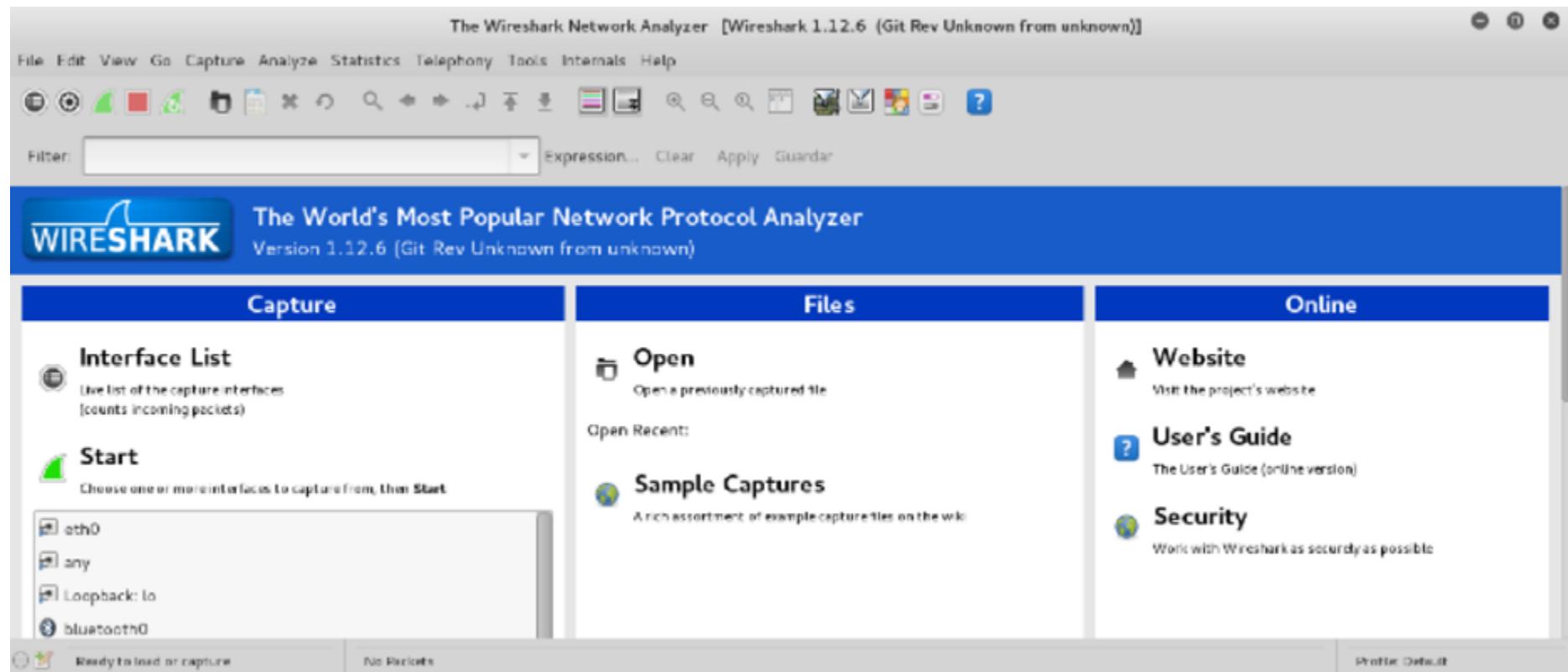
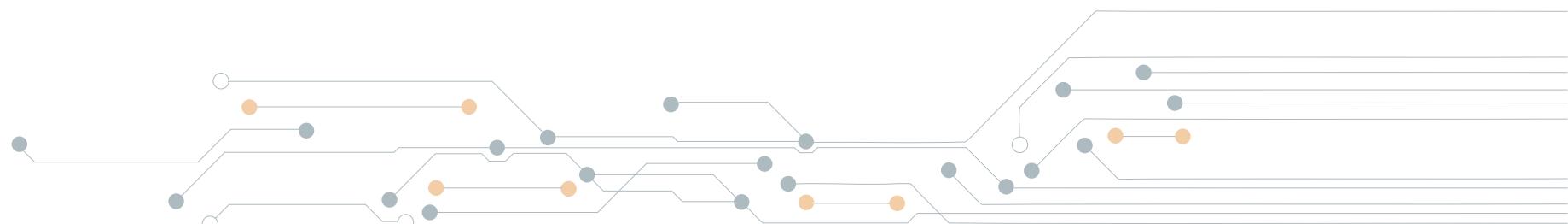


Imagen 67 Wireshark - Interfaz en Linux



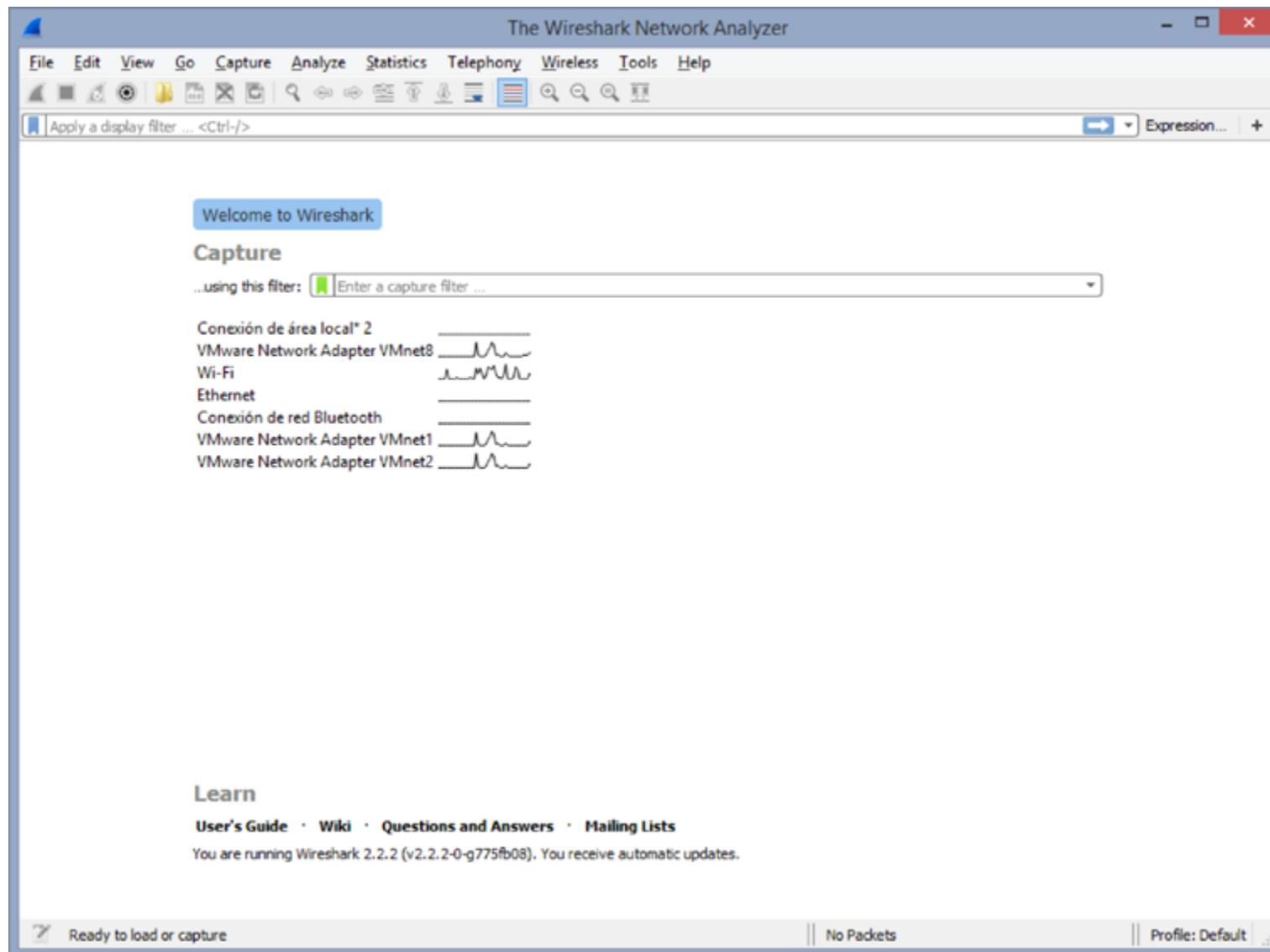


Imagen 67 Wireshark - Interfaz en Linux

Cuando se elija la interfaz por la que analizar el tráfico comenzará a capturar paquetes. Por defecto, en las interfaces inalámbricas se activará el modo promiscuo.

Una vez tengamos suficientes paquetes podemos detener la captura y empezar a analizar el contenido.

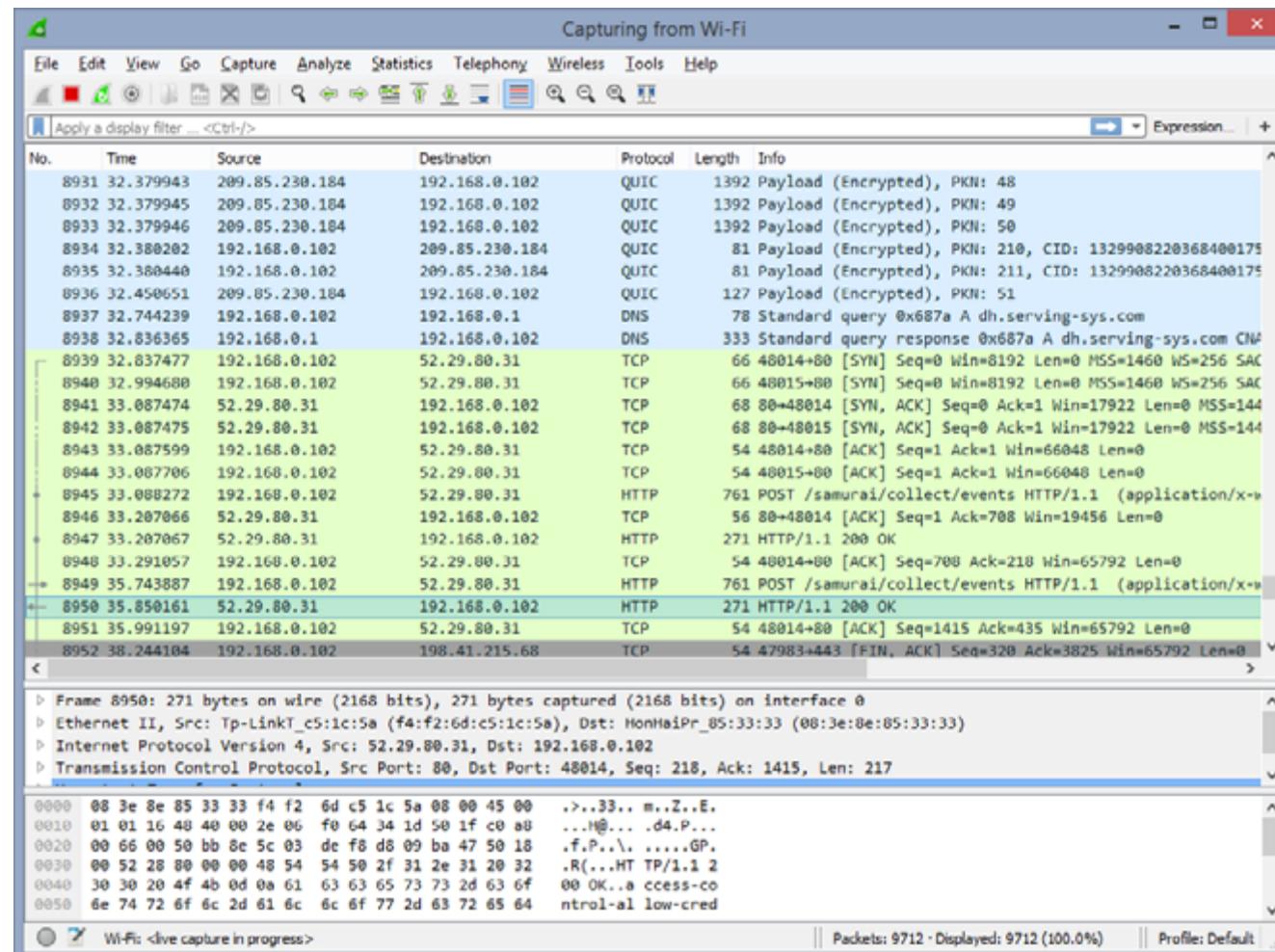


Imagen 69 Wireshark - Captura de tráfico de red

Como puede observarse los paquetes vienen identificados por colores, indicando el tipo de paquete y si se ha realizado correctamente la captura. Además, nos muestra información de dicho paquete, como puede ser el numero identificativo, la ip origen y destino, el protocolo,

la longitud e información resumida del paquete. Si seleccionamos uno de ellos, en la parte inferior aparece detallado según la capa, además de mostrar en bruto, en hexadecimal la información, el paquete capturado.

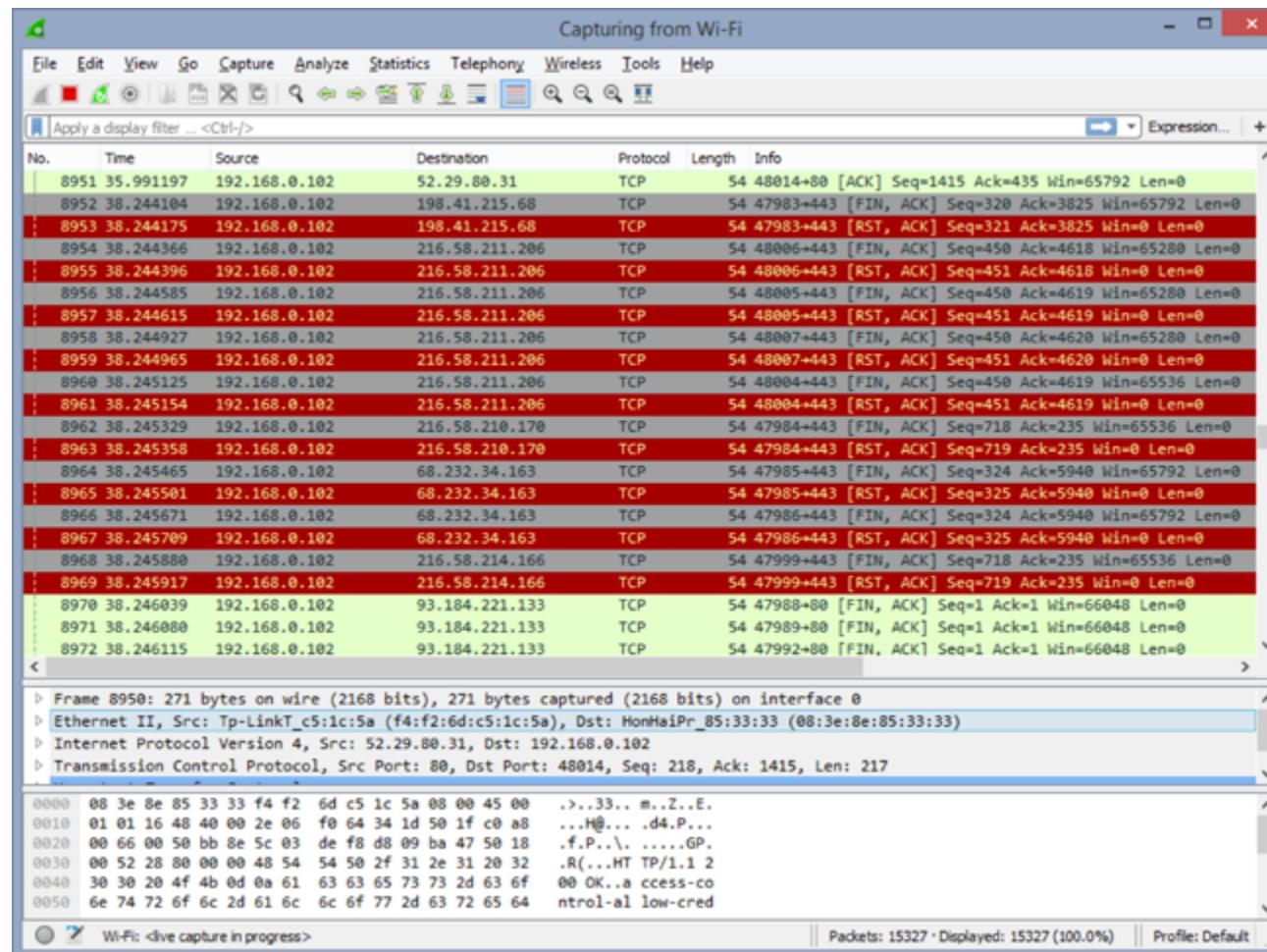


Imagen 70 Wireshark - Identificación de los paquetes

Podemos en cualquier momento cambiar de interfaz, así como poder importar un archivo almacenado con anterioridad desde el menú File - Open, así como realizar la copia de los datos capturados.

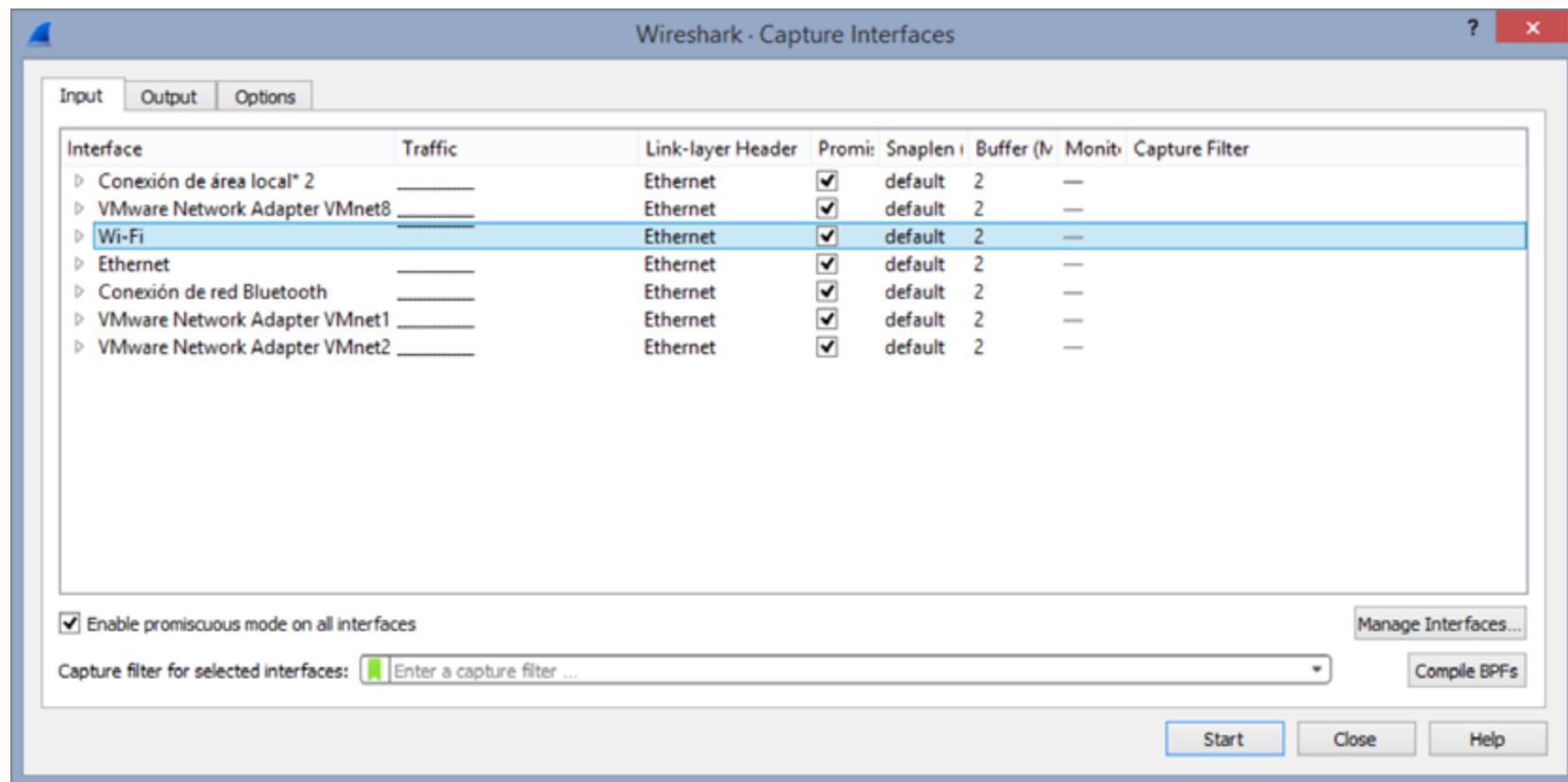


Imagen 71 Wireshark - Selección Interfaz

Wireshark permite filtrar la información obtenida para un mejor manejo de los datos y poder analizar más fácilmente la información, ya que después de un tiempo la información capturar puede ser importante.

Los filtros de tipo Display permiten filtrar los paquetes obtenidos mostrando aquellos que cumplen unas determinadas condiciones. Para utilizarlos se debe indicar, por ejemplo, el protocolo por el cual se quiere filtrar: http, tcp, arp, ip,...

La forma más sencilla a la hora de aplicar un filtro es escribir en la parte superior el protocolo junto con los atributos determinados para cada uno de ellos. Si se escribe http se filtrará la información solo de los paquetes http que existan.

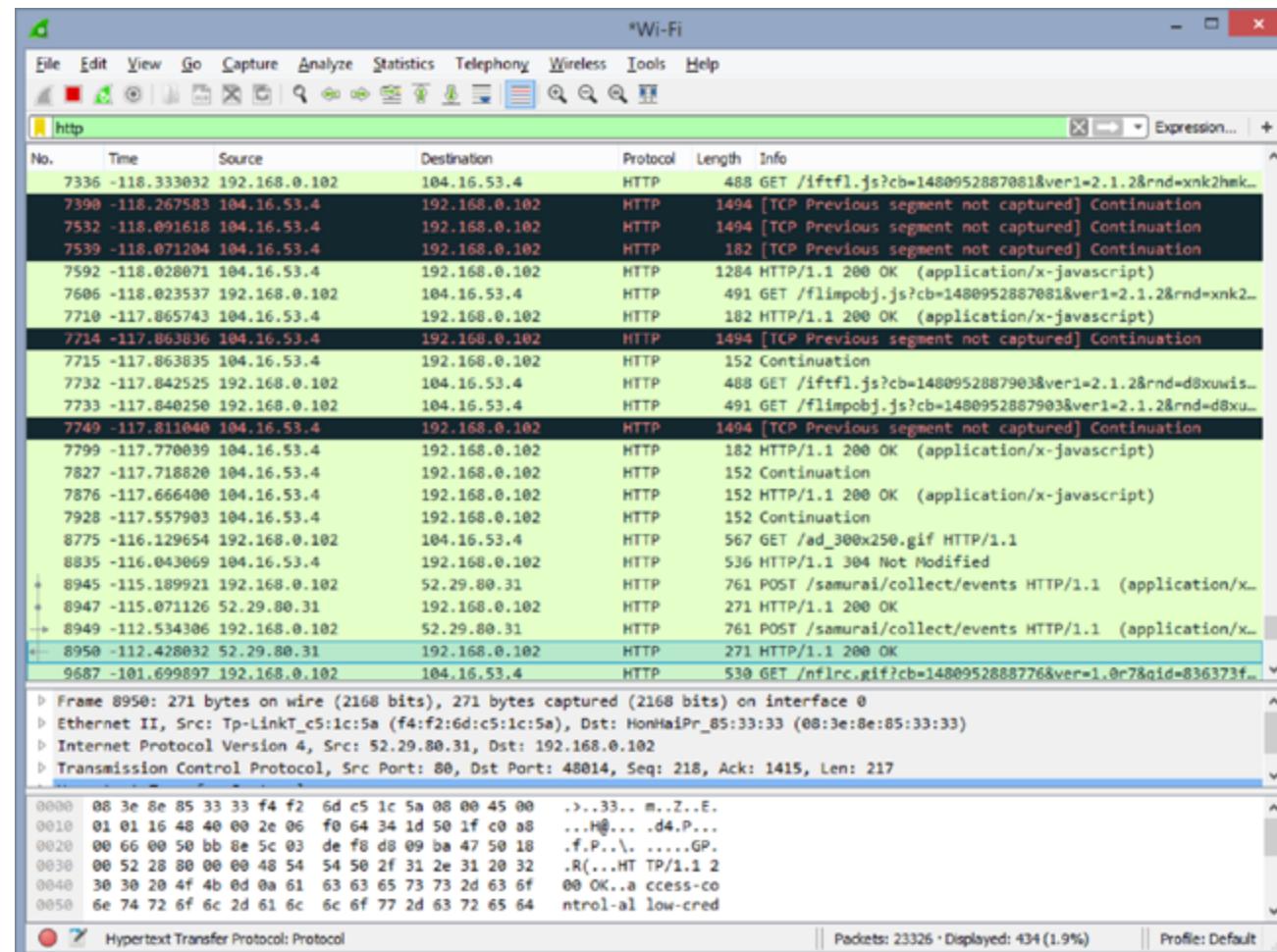


Imagen 72 Wireshark - Filtro http

Se pueden consultar preestablecidos y crear nuevos filtros desde el menú Analyze – Display Filters.

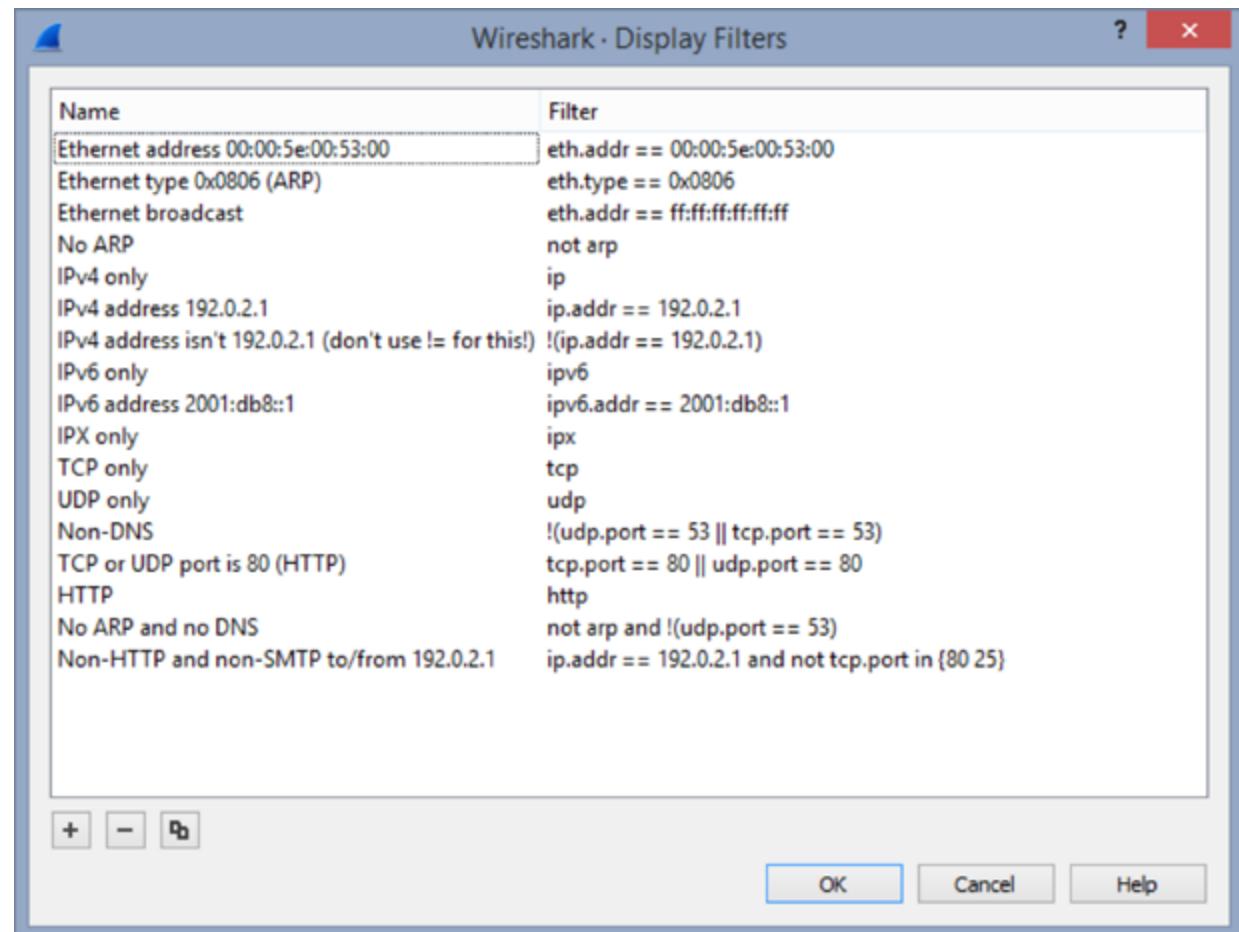


Imagen 73 Wireshark - Filtros

Con la opción Follow TCP Stream se puede observar la conexión entre dos máquinas y cuál ha sido el flujo de información entre ellos.

A través de esta opción se pueden visualizar las comunicaciones y seguir las, e incluso reconstruir archivos.

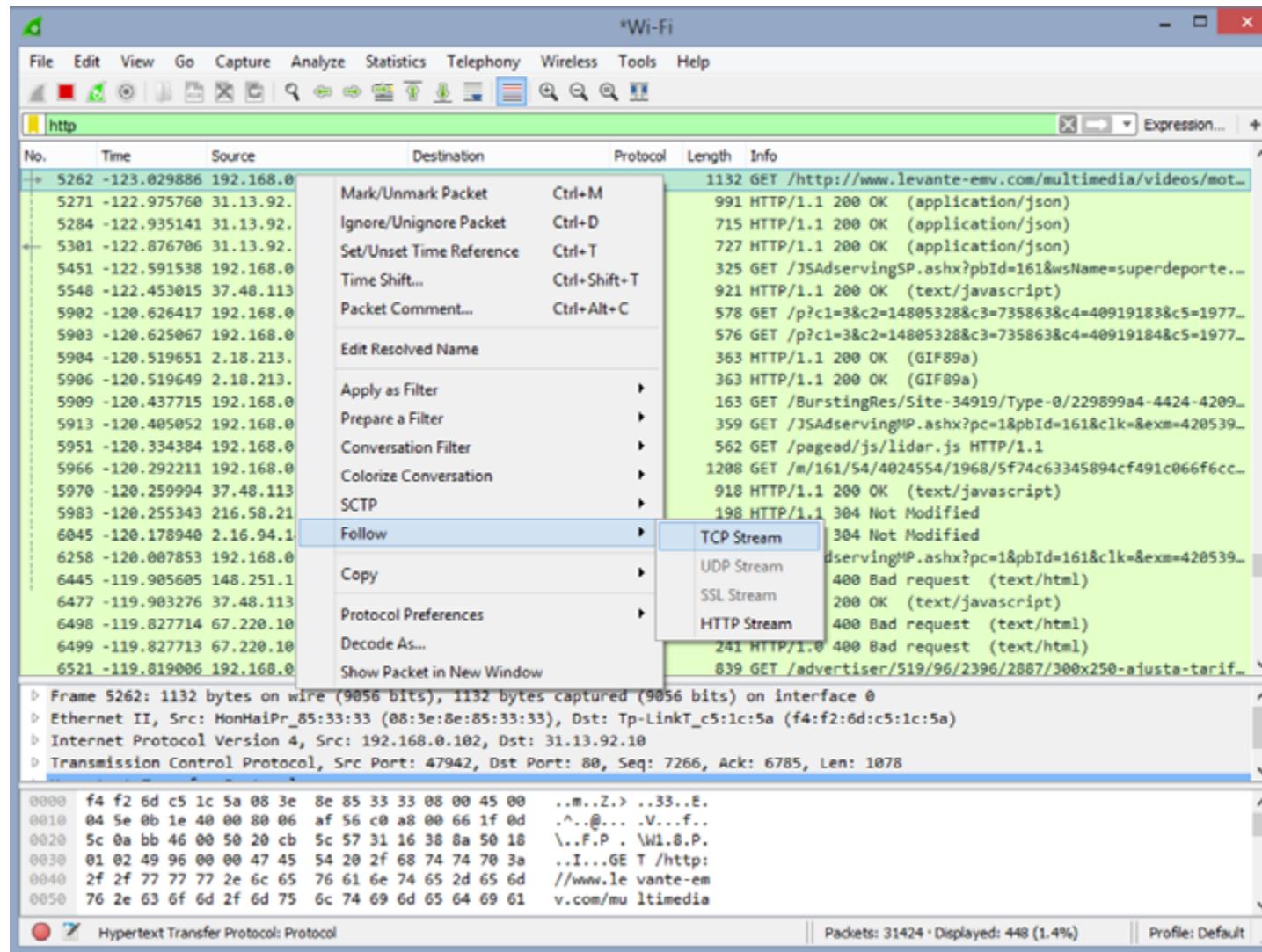


Imagen 74 Wireshark - Follow TCP Stream

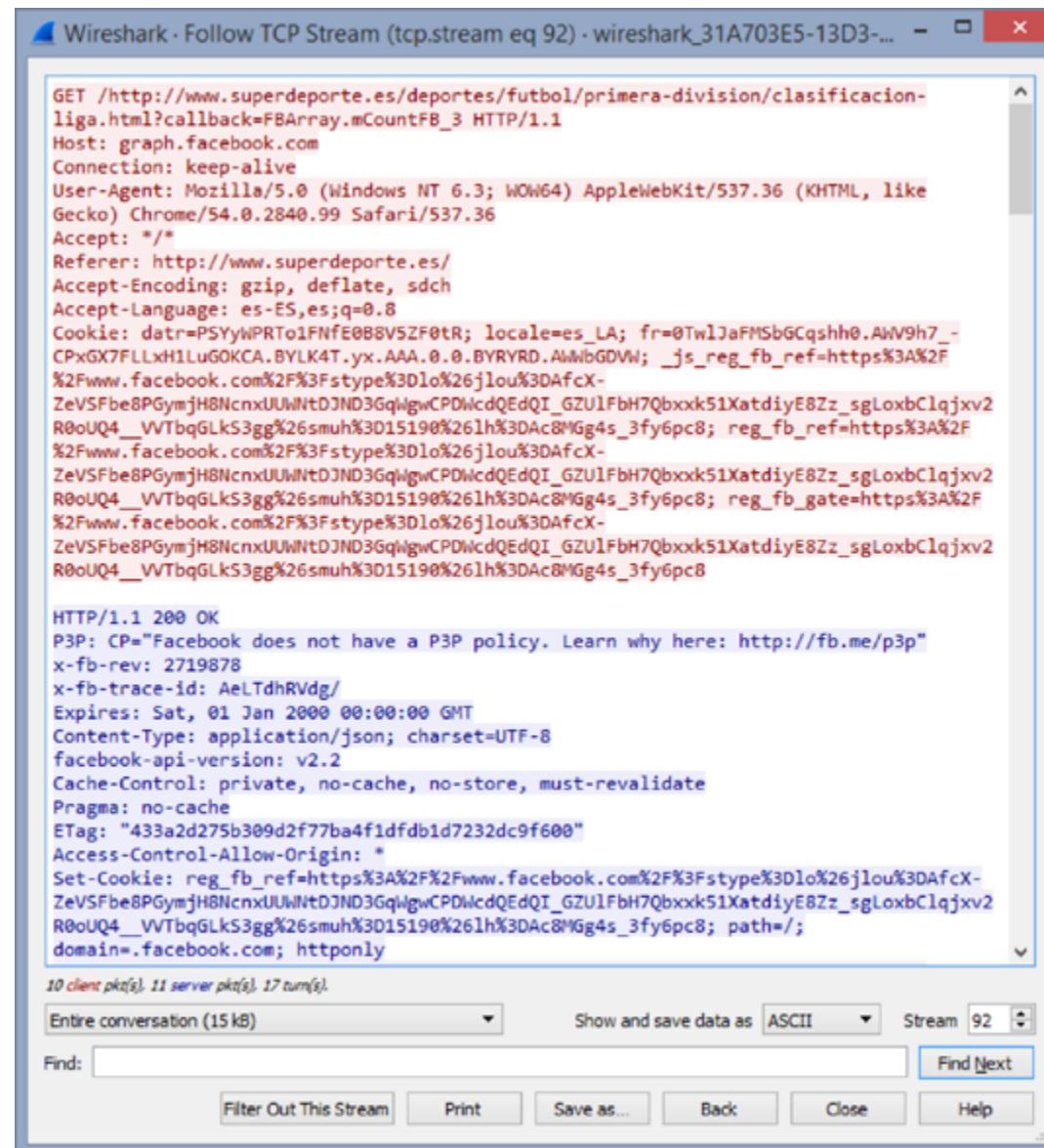


Imagen 75 Wireshark - Detalle Follow TCP Stream

Al cerrar la ventana, en la zona de filtros muestra el filtro aplicado para conseguir el seguimiento anterior.

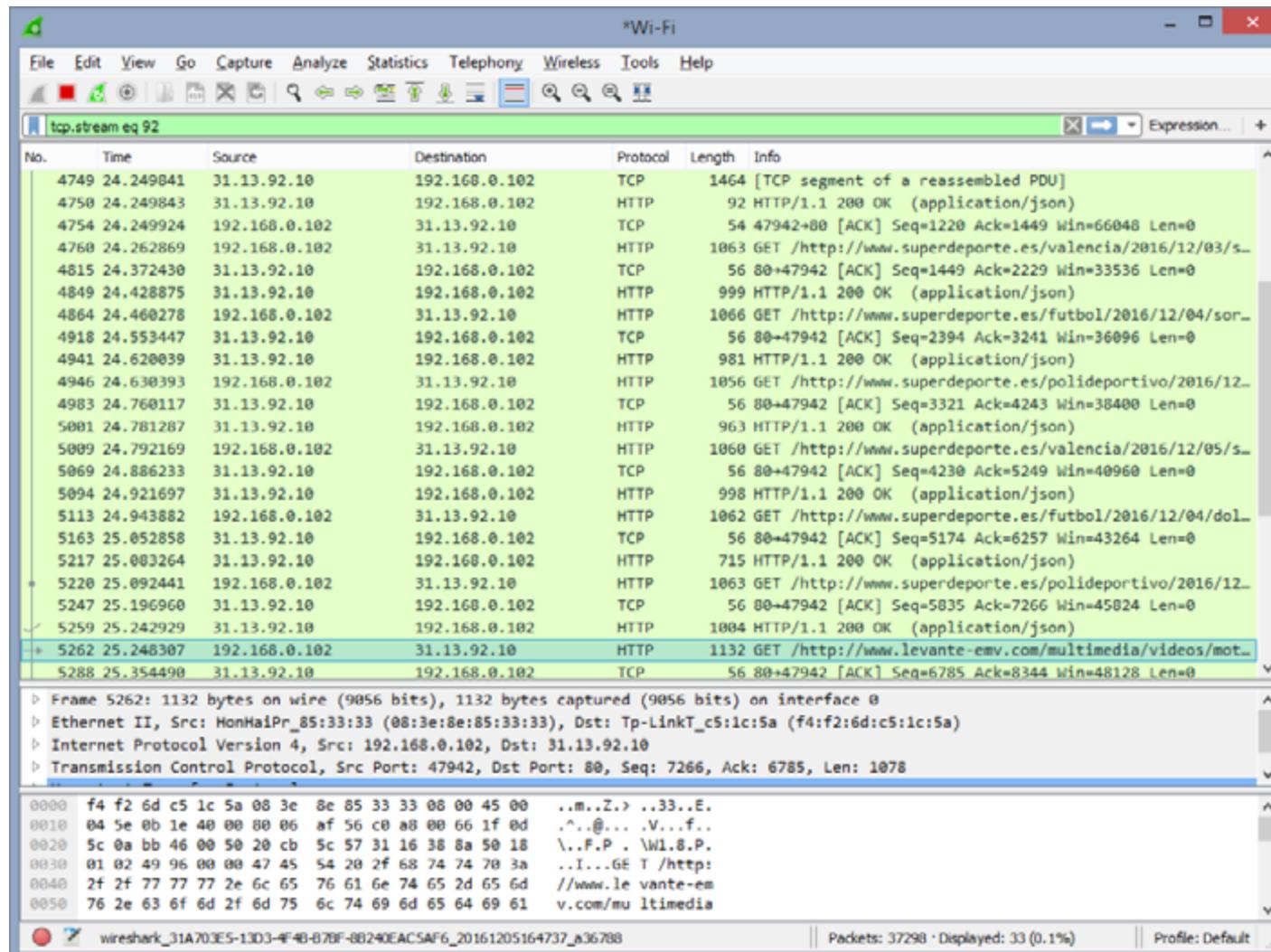


Imagen 76 Wireshark - Filtro Follow TCP Stream

Al seleccionar un paquete, en la parte inferior permite ver en detalle el contenido de ese paquete a través de las distintas capas.

Esta opción es muy interesante ya que nos permite analizar en profundidad la información a nivel más bajo de las comunicaciones.

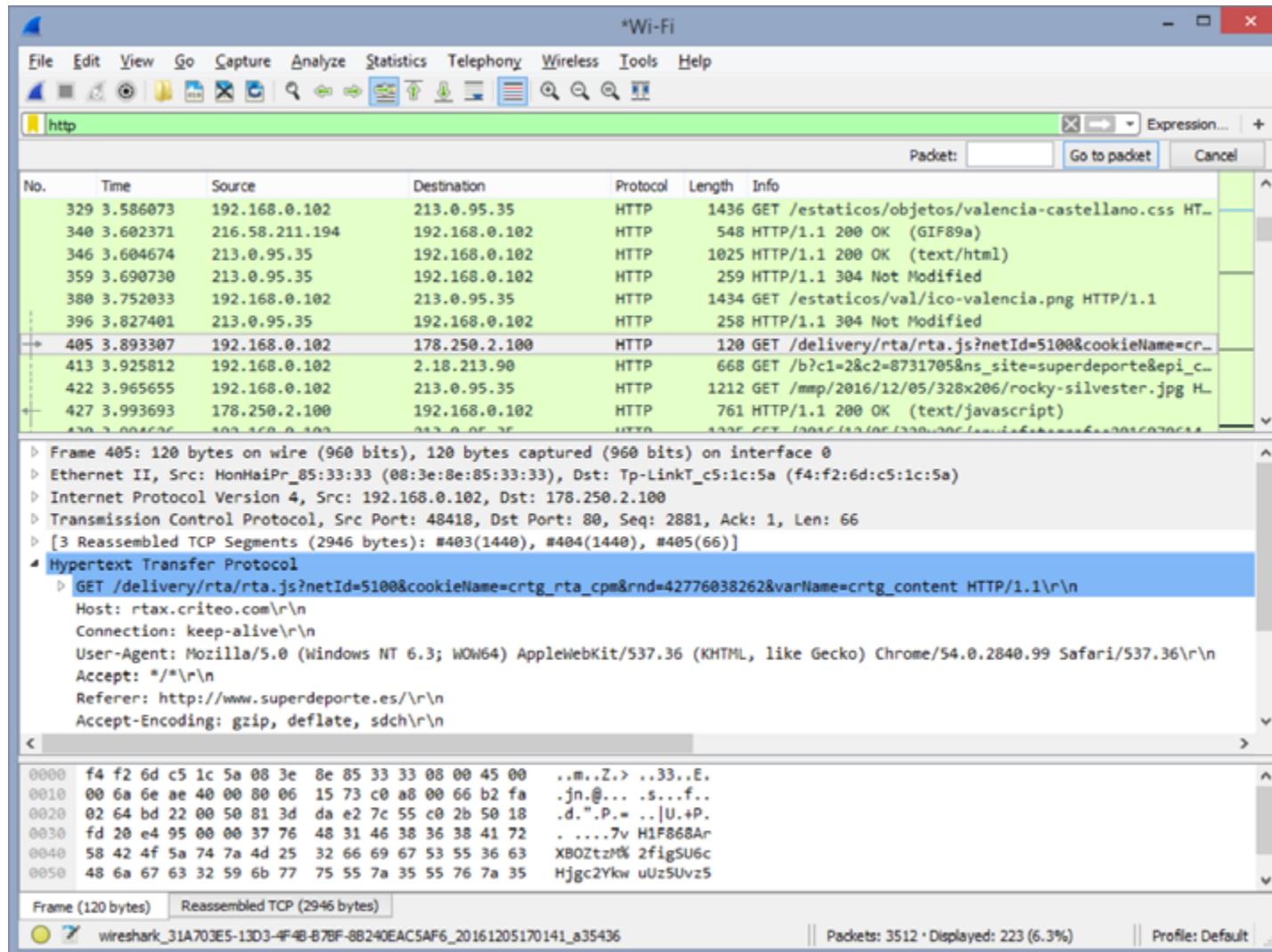


Imagen 77 Wireshark - Detalle paquete

Al seleccionar un paquete podemos crear un filtro de la comunicación que ese paquete ha realizado aplicando un filtro a dicho paquete y ver los pasos que se han realizado.

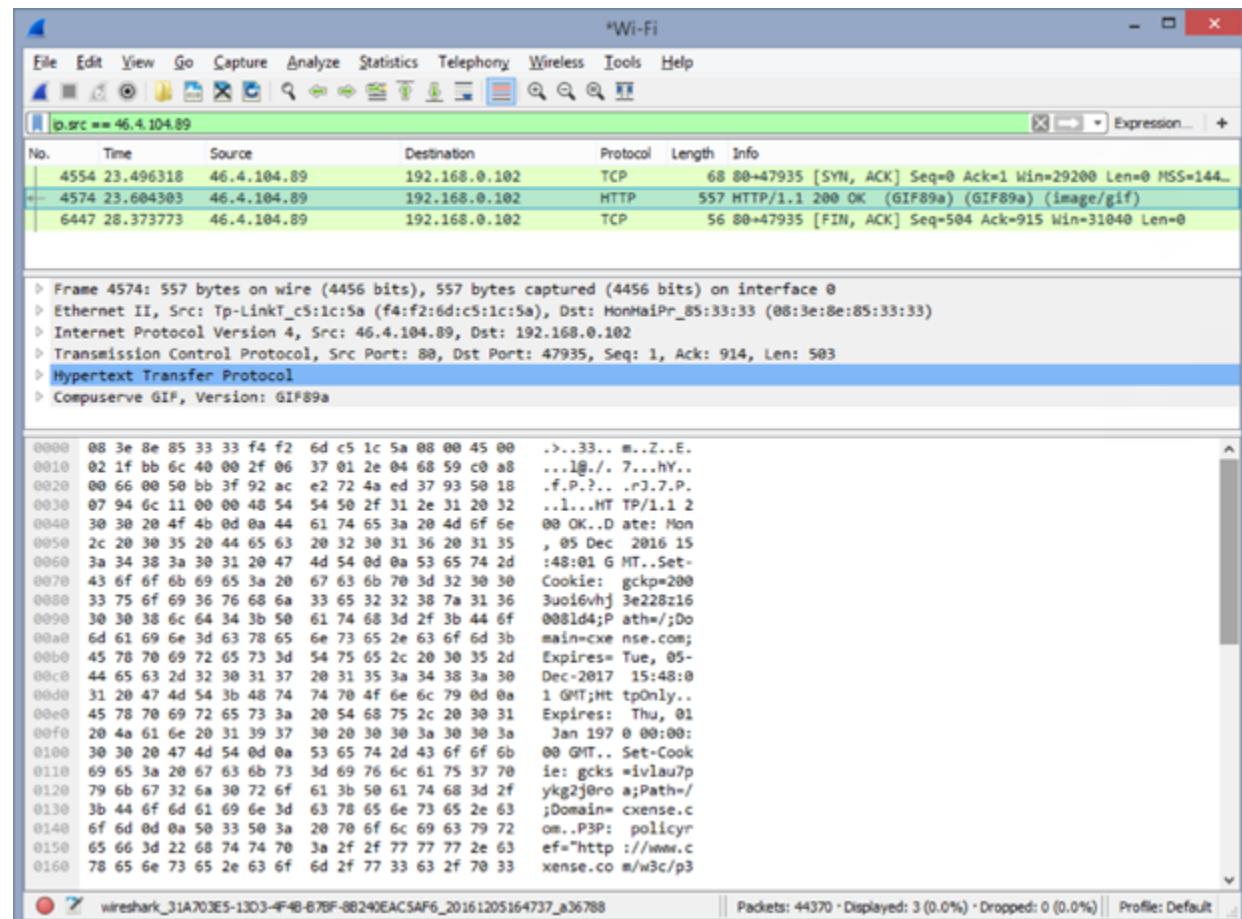


Imagen 78 Wireshark - Filtro por IP

Wireshark dispone de varios módulos de estadísticas muy interesantes, capaces de mostrar en tiempo real porcentajes y estadísticas sobre tramas capturadas. En la pestaña Statistics se

pueden encontrar distintas opciones, entre las que destacamos Protocol Hierarchy que muestra en porcentajes los paquetes capturados de qué tipo son, a qué nivel de red pertenecen, ...

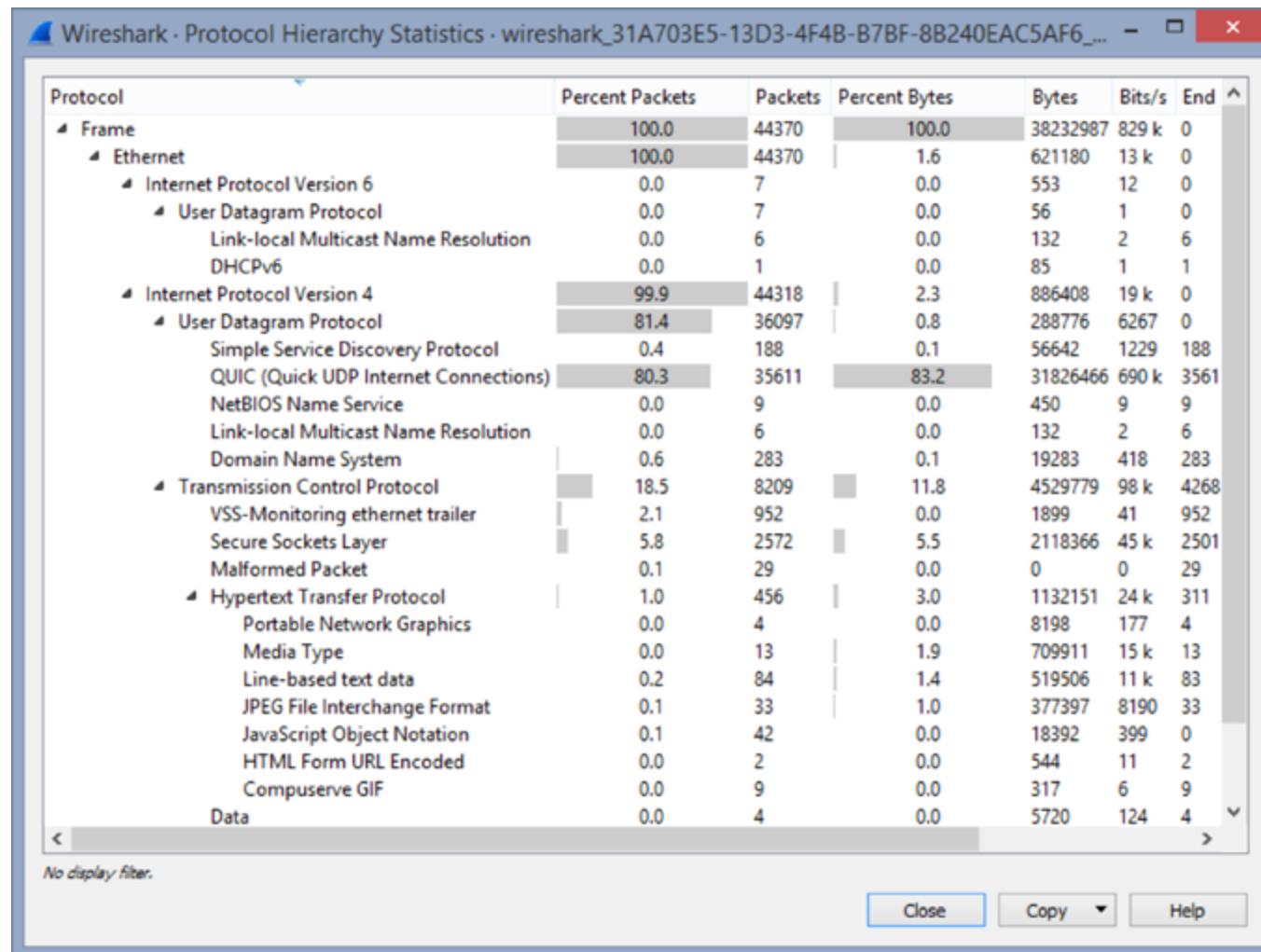


Imagen 79 Wireshark - Protocol Hierarchy

Otra opción interesante e la que nos permite visualizar la comunicación con el tráfico TCP o general, con la opción Flow Graph.

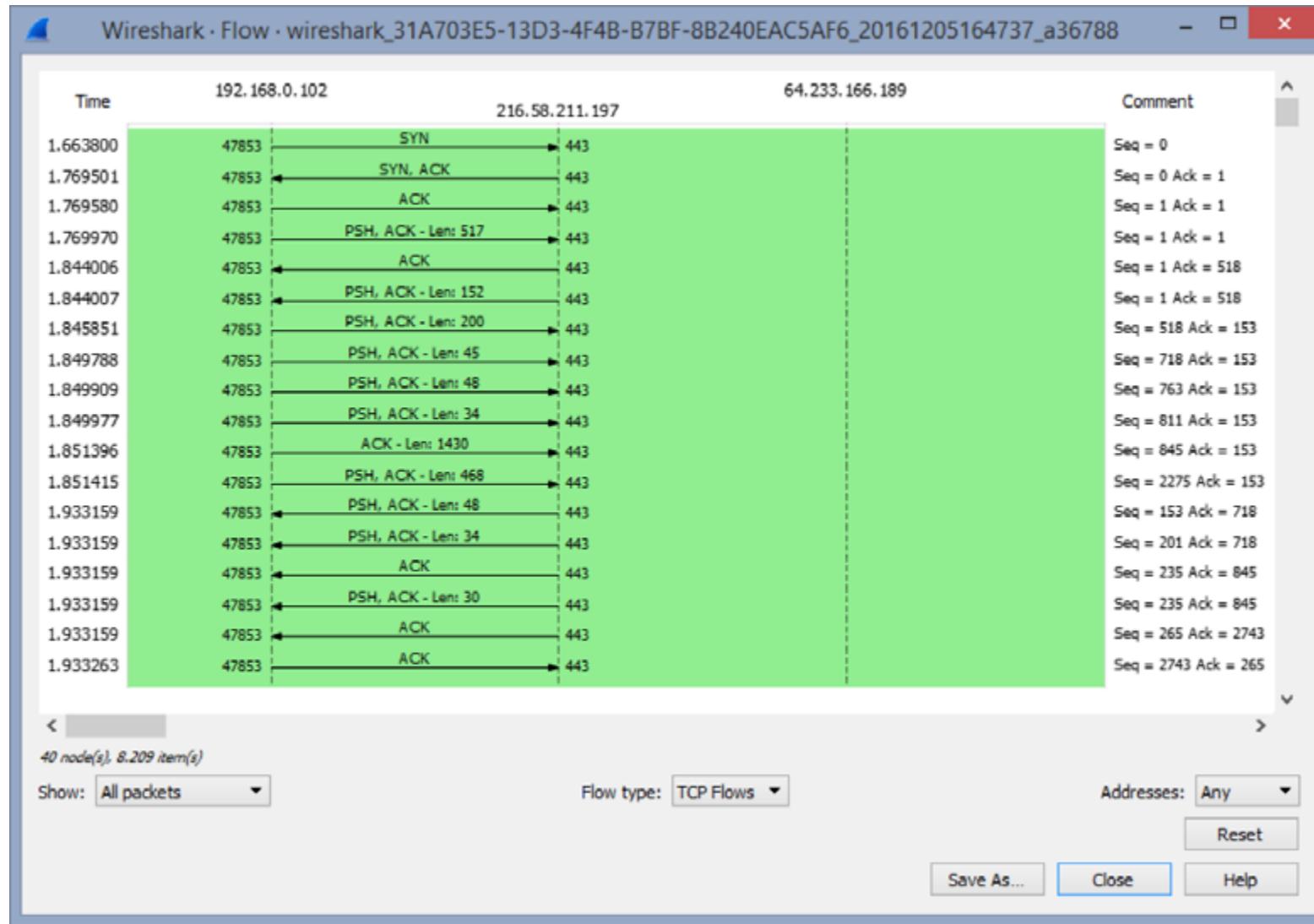


Imagen 80 Wireshark - Secuencia comunicación TCP

Wireshark permite de una forma rápida obtener los archivos capturados en la comunicación y poder almacenarlos a través de la opción File – Export Objects – HTTP.

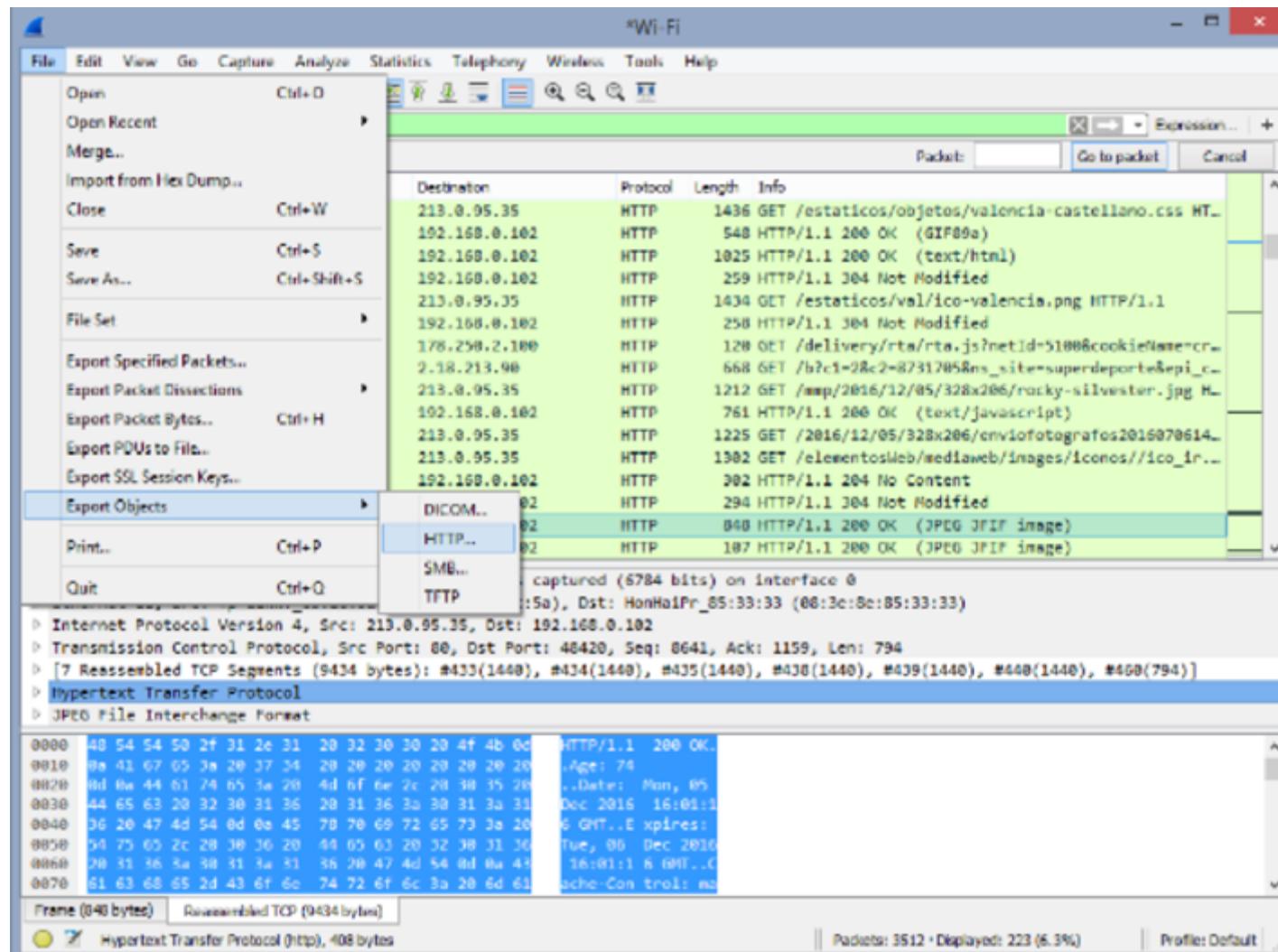


Imagen 81 Wireshark - Exportar archivos

Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
120	pagead2.googlesyndication.com	image/gif	42 bytes	activeview?avi=BNMnFTY9FWMX3BcHHxgLfzYT
125	www.e-katec.com	text/plain	19 kB	?_task=mail&_mbox=INBOX&_folderlist=1&_list=
300	pagead2.googlesyndication.com	image/gif	42 bytes	activeview?avi=B3AR0TY9FWK-bDMGHtge4xL3D
340	pagead2.googlesyndication.com	image/gif	42 bytes	activeview?avi=BNMnFTY9FWMX3BcHHxgLfzYT
346	www.superdeporte.es	text/html	198 kB \	
427	rtax.criteo.com	text/javascript	169 bytes	rtaj.js?netId=5100&cookieName=crtg_rta_cpm&n
460	fotos01.superdeporte.es	image/jpeg	9026 bytes	rocky-silvester.jpg
466	fotos00.superdeporte.es	image/jpeg	9725 bytes	enviofotografos20160706144531606.jpg
523	api2ed.renr.es	text/html	5243 bytes	pG_5800bdb0cf2898c2671581c
561	www.superdeporte.es	text/html	16 kB	resultados-mini.html
572	estaticos.levante-emv.com	application/javascript	27 kB	widgets.js?20160927
573	estaticos.levante-emv.com	text/css	8744 bytes	widgets_galeria.css?cca
581	estaticos.levante-emv.com	text/css	1653 bytes	estilos_videos.css
583	estaticos.levante-emv.com	text/css	556 bytes	videojs-resolution-switcher.css
584	estaticos.levante-emv.com	text/css	1946 bytes	videojs.vast.vpaid.min.css
590	comcluster.cxense.com	image/gif	43 bytes	rep.gif?ver=1&typ=pgv&rnd=iwc9lgsf0gp8uon
616	api.superdeporte.es	application/javascript	5160 bytes	pC_56a8e19c0cf244693a741830
621	estaticos.levante-emv.com	text/css	44 kB	video-js.css
626	estaticos.levante-emv.com	text/css	2165 bytes	videojs.social.css
633	estaticos.levante-emv.com	application/javascript	12 kB	videojs.social.js?cca
654	estaticos.levante-emv.com	application/javascript	10 kB	videojs-resolution-switcher.js
667	api.superdeporte.es	text/html	1852 bytes	pG_581dae2c0cf25b91dc62a367
673	estaticos.levante-emv.com	application/javascript	9379 bytes	cabecera.js
675	estaticos.levante-emv.com	application/javascript	3036 bytes	jquery.popupWindow.js
694	estaticos.levante-emv.com	application/javascript	87 kB	videojs_5.vast.vpaid.min.js

< >

Save Save All Close Help

Imagen 82 Wireshark - Archivos en la comunicación

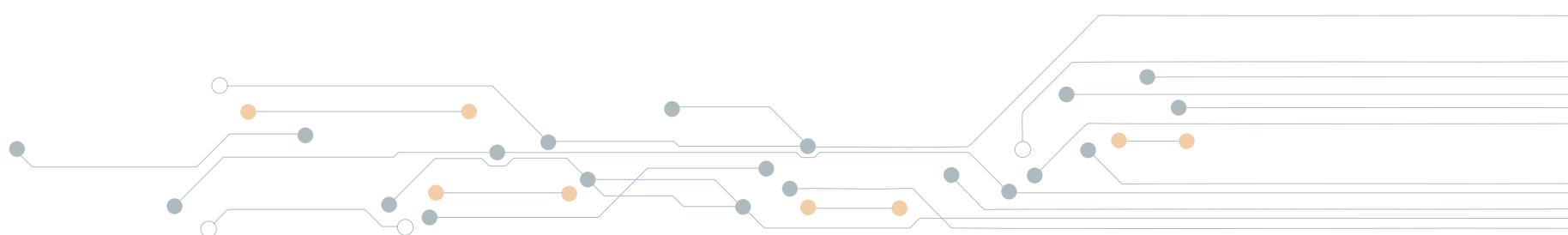




Imagen 83 Wireshark - Imagen obtenida de la comunicación



Imagen 84 Logo NetworkMiner

La herramienta Network Miner¹ es de la rama de análisis forense de red para sistemas Microsoft Windows. Su propósito es recolectar información tras el procesado de las capturas de red.

La herramienta filtra todo tipo de información, y es capaz de obtener versiones de aplicaciones, de sistemas operativos, ficheros, conexiones abiertas, credenciales, sesiones,...

¹ <http://www.netresec.com/?page=NetworkMiner>



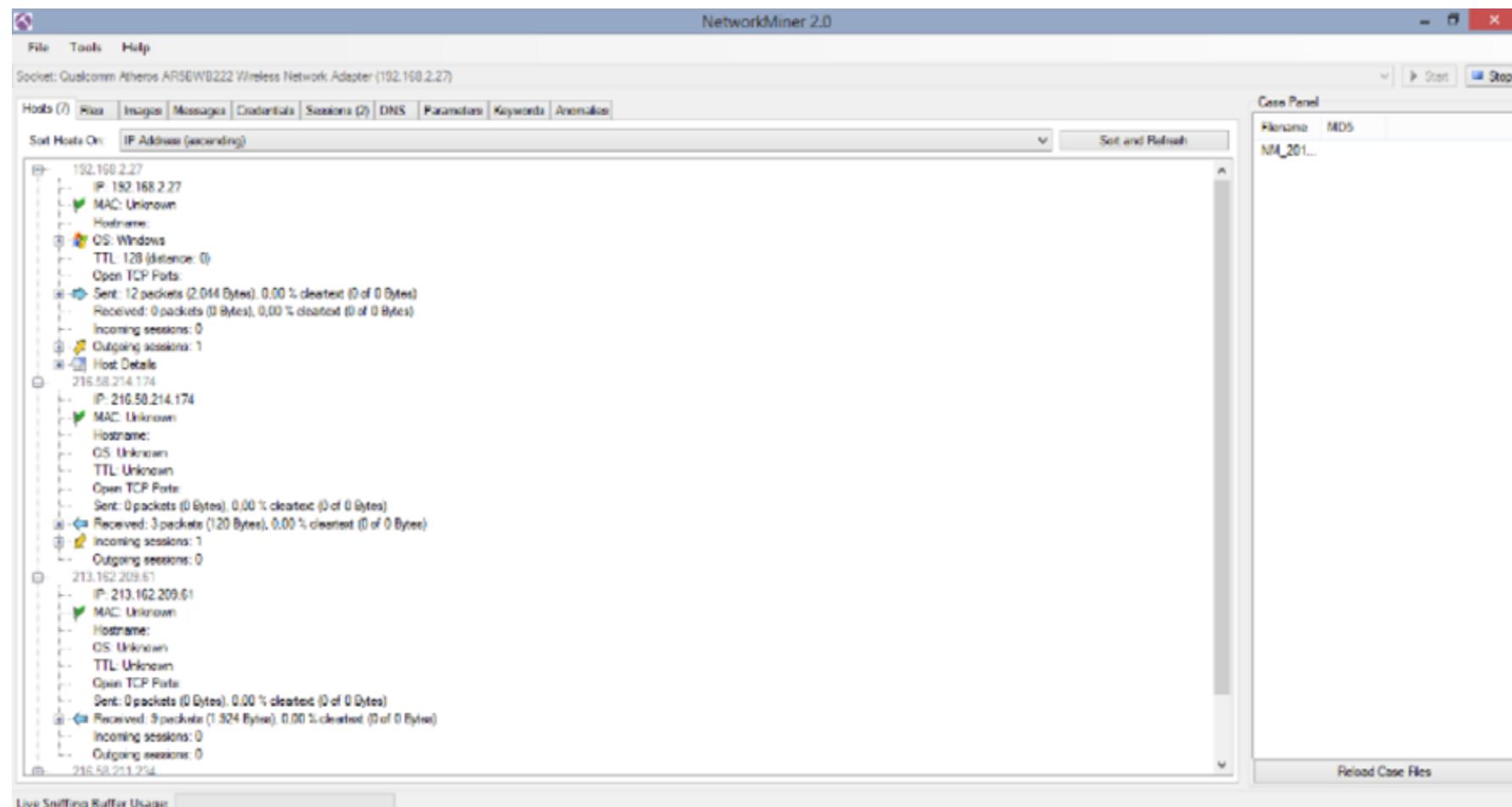


Imagen 85 Network Miner

Una de las utilidades interesantes es que permite importar archivos PCAP para su análisis off-line y rehacer archivos transferidos entre otras. También es muy utilizado en el análisis de tráfico de malware,

así como la posibilidad de realizar búsquedas en la información analizada en busca de usuario, contraseñas, etc... disponibles en la pestaña Credentials.

Otra de las herramientas que permite visualizar de forma gráfica y ordenada las capturas de red recopiladas, y que además permite trabajar con gran cantidad de datos y protocolos es Xplico.

El framework trabaja con archivos de captura de datos tipo Pcap, o permite también la captura en tiempo real del tráfico de red.

Obtiene gran cantidad de información relacionada con sitios web, DNS, chats, emails, imágenes, ... y puede utilizarse como herramienta durante el análisis dinámico de un código malicioso o malware.

The screenshot shows the Xplico Interface with the following details:

- User:** deft
- Cases:** Case name: case 2; Session Name: day 2; Start Time: 0000-00-00 00:00:00; End Time: 0000-00-00 00:00:00; Status: EMPTY
- Pcap set:** Add new pcap file: Browse... Upload List of all pcap files
- Related HTTP:**
 - Post: 0
 - Get: 0
 - Video: 0
 - Images: 0
- Related MMS:**
 - Number: 0
 - Contents: 0
 - Video: 0
 - Images: 0
- Related SIP:** Calls: 0
- Related RTP/VoIP:**
- Related Emails:**
 - Received: 0
 - Sended: 0
 - Unreaded: 0/0
- Related FTP:**
 - Connections: 0
 - Downloaded: 0
 - Uploaded: 0
- Related NNTP:**
- Related IRC:**
- Related Printed files:** Pdf: 0

At the bottom, there is a footer with links to Xplico.org, GnuGPL License, Version 0.5, and copyright information: © 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Imagen 86 Xplico Interface

Telefónica EDUCACIÓN DIGITAL