



# Análisis de tráfico con Wireshark

Realizado por:

José M<sup>a</sup> López Serrano  
Silvia Cazalla Bazán



# Contenido de la presentación

- ¿Qué es Wireshark?
- ¿Qué utilidades podemos darle?
- Modo promiscuo
- Filtros
- Gráficas e interpretación
- Introducción al uso de Wireshark
- Conclusión

## ¿Qué es Wireshark?

- Antiguo Ethereal, lanzado en 1999.
- Multiplataforma.
- Software libre
- Analizador de protocolos.
- Herramienta didáctica.
- Más de 480 protocolos.



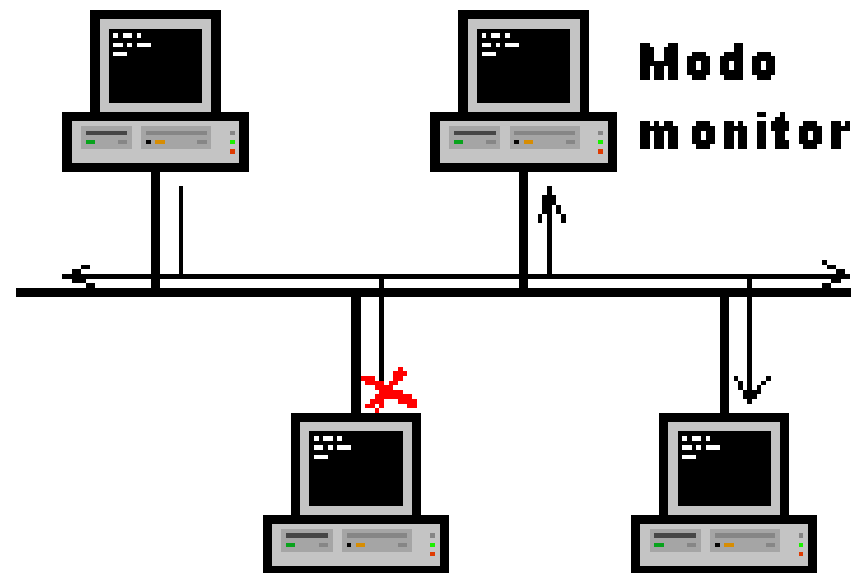


## ¿Qué utilidades podemos darle?

- Analizar tráfico en una red nos permite multitud de utilidades, como:
  - Detección de intrusos en nuestra red.
  - Descubrir cuellos de botella.
  - Analizar las operaciones que realizan nuestras aplicaciones.
  - Descubrir virus o denegación de servicios.
  - Resolución de problemas en la red.
- Ampliamente usado como herramienta didáctica, como ya hemos hablado.

## Modo promiscuo

- Es una manera de capturar todo el tráfico que circula por nuestra red.
- Necesario configurar una tarjeta de red como modo promiscuo.





# Filtros

- En Wireshark se utilizan filtros para poder interpretar de forma correcta conversaciones entre sistemas finales o paquetes específicos.<sup>4</sup>
- Existen infinidad de filtros:
  - Por protocolo
  - Por tipo de petición
  - Paquetes que contengan una palabra
  - Filtrado por IP
  - Por MAC
  - Por puerto

... (entre otros)



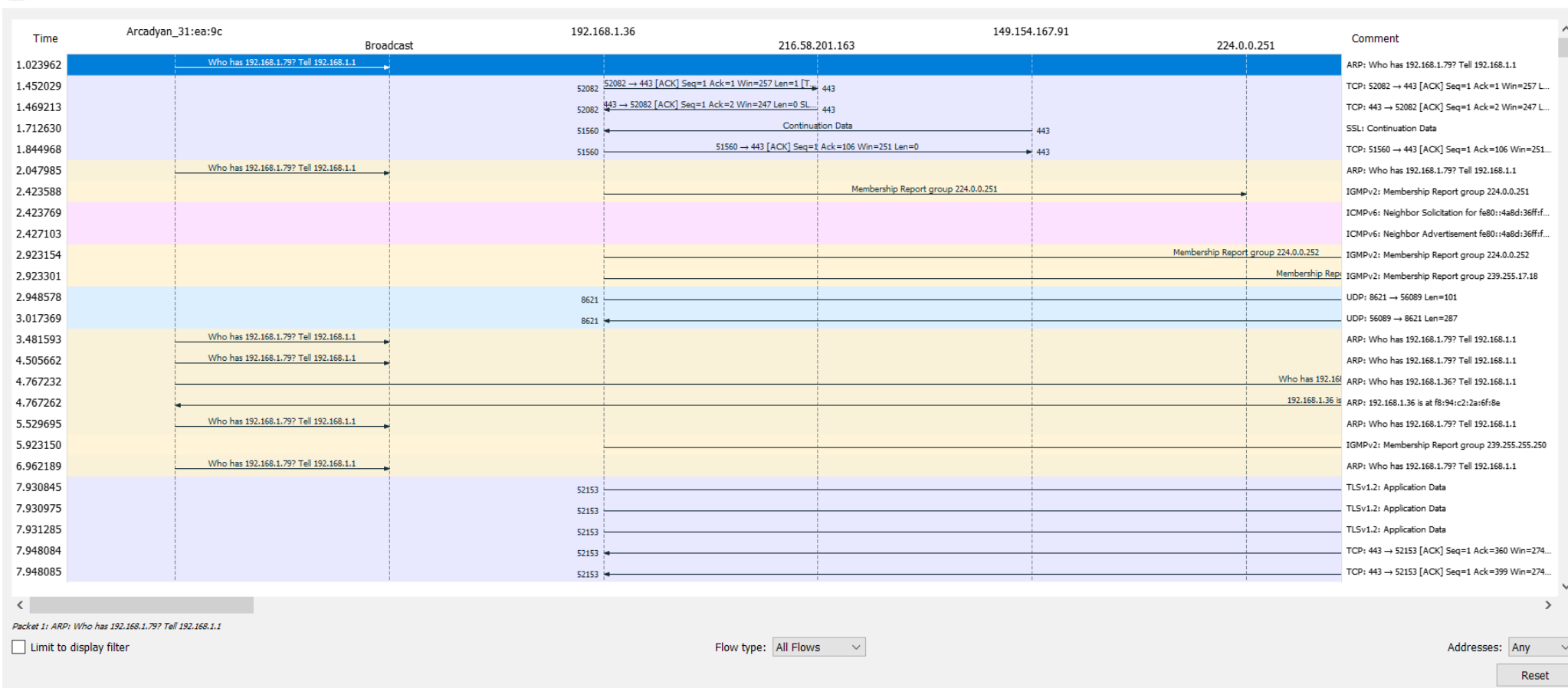
## Gráficas e interpretación

- Todos los problemas en una red se reflejan en los paquetes, pero de nada sirve capturar paquetes sin saber interpretar resultados.
- El conocimiento de las herramientas e interpretación de datos en Wireshark es lo que marca la diferencia entre capturar simples datos y conocer el estado de la red analizando estos datos.
- Wireshark nos brinda una serie de gráficos que nos permiten tener una visión general de los datos.
- De esta forma podemos decir que Wireshark no es un sistema de detección de intrusos, pero puede ayudar a descubrirlo si ocurren situaciones extrañas en nuestro tráfico de datos habitual.

# Gráficas

- Grafos de flujo

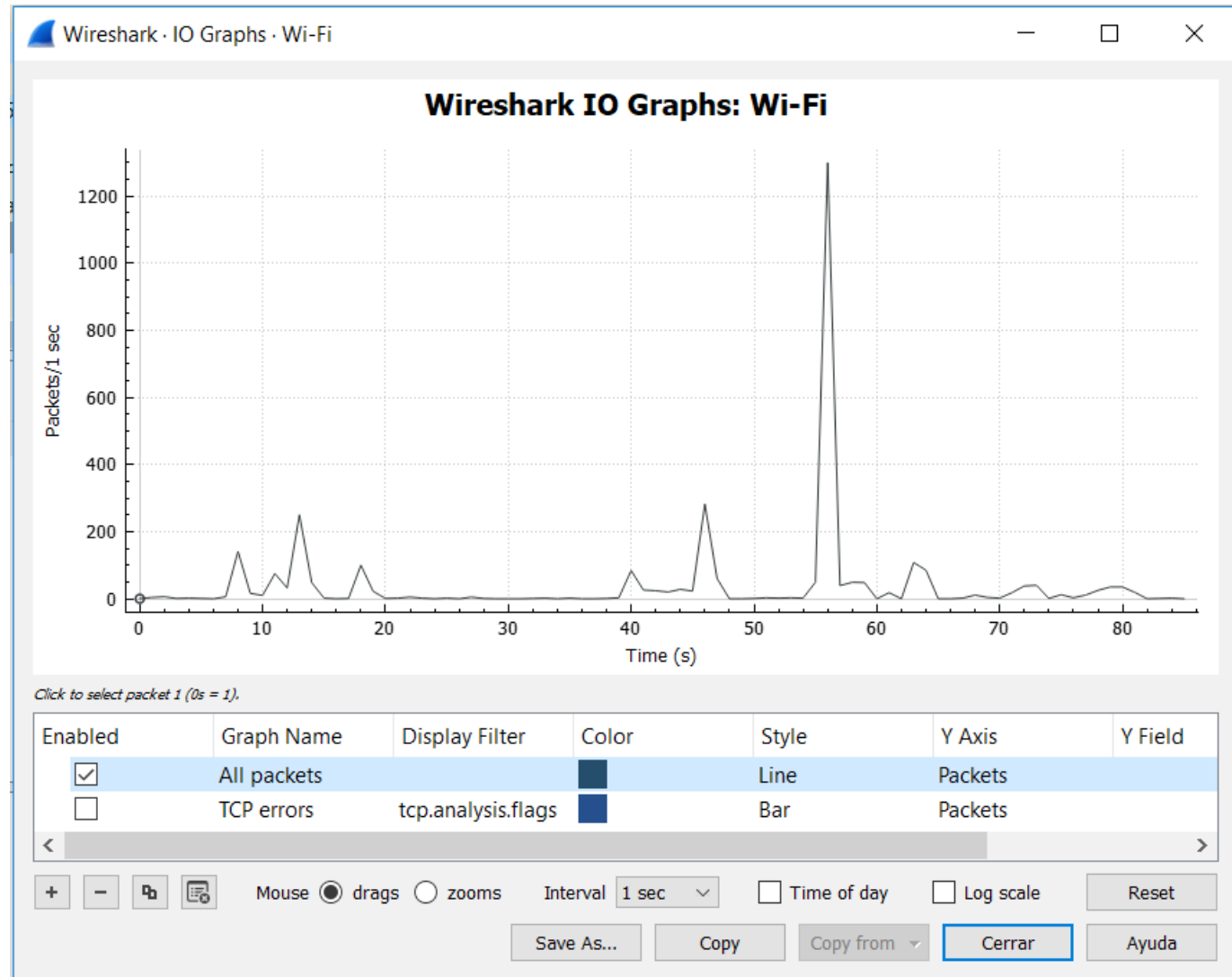
Wireshark · Flow · Wi-Fi





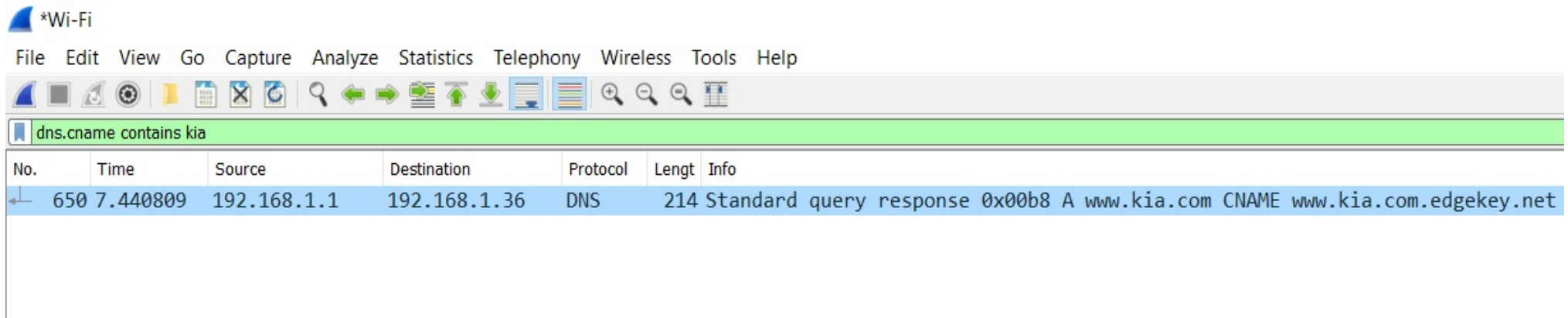
# Gráficas

- IO Graphs



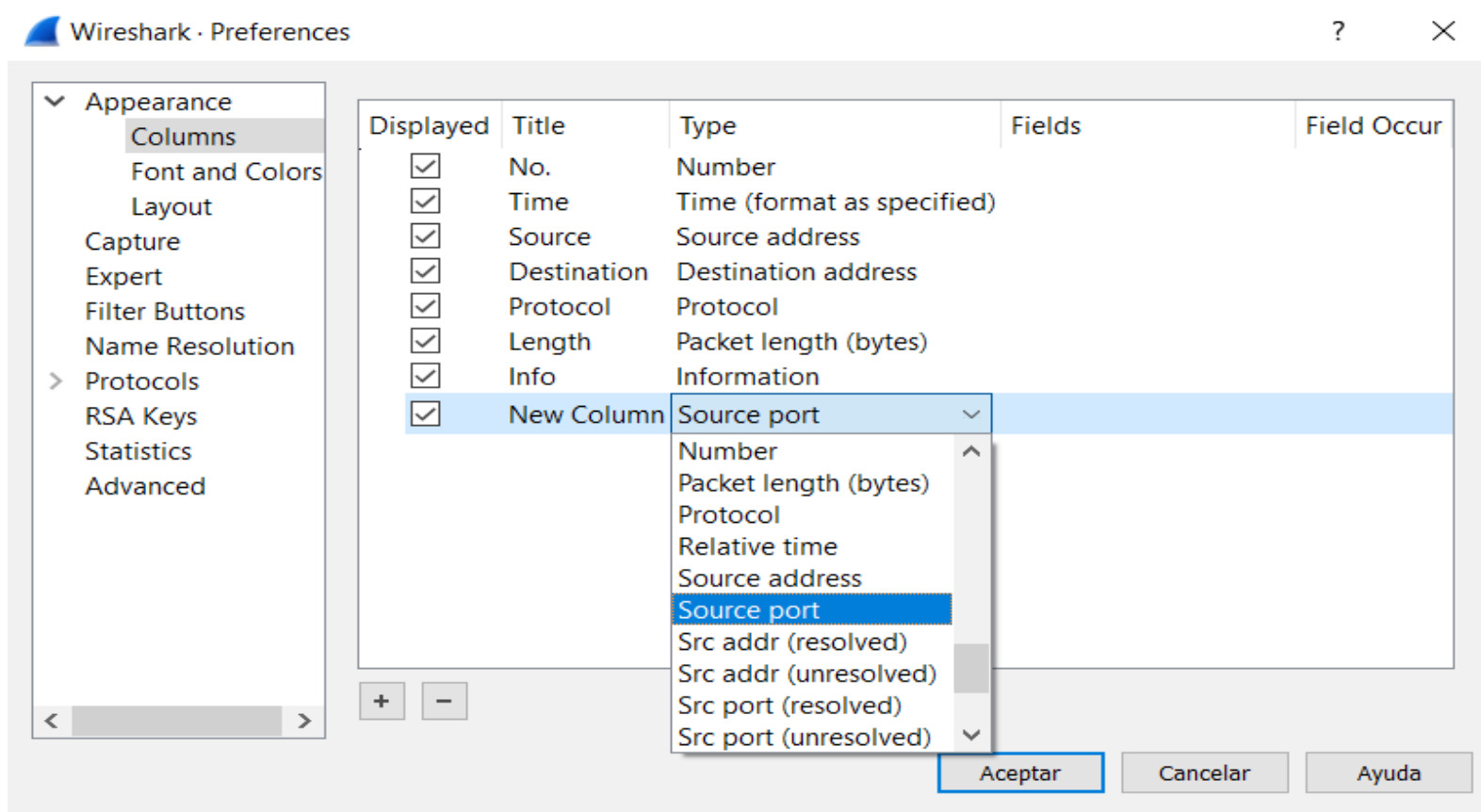
# Introducción al uso de Wireshark

- A continuación mostramos el resultado de varias prácticas simples realizadas con Wireshark en nuestro ordenador personal:



- Identificar la trama DNS donde se traduce una dirección a IP.

# Introducción al uso de Wireshark



- Añadir columnas para ver el puerto origen y destino.

# Introducción al uso de Wireshark



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



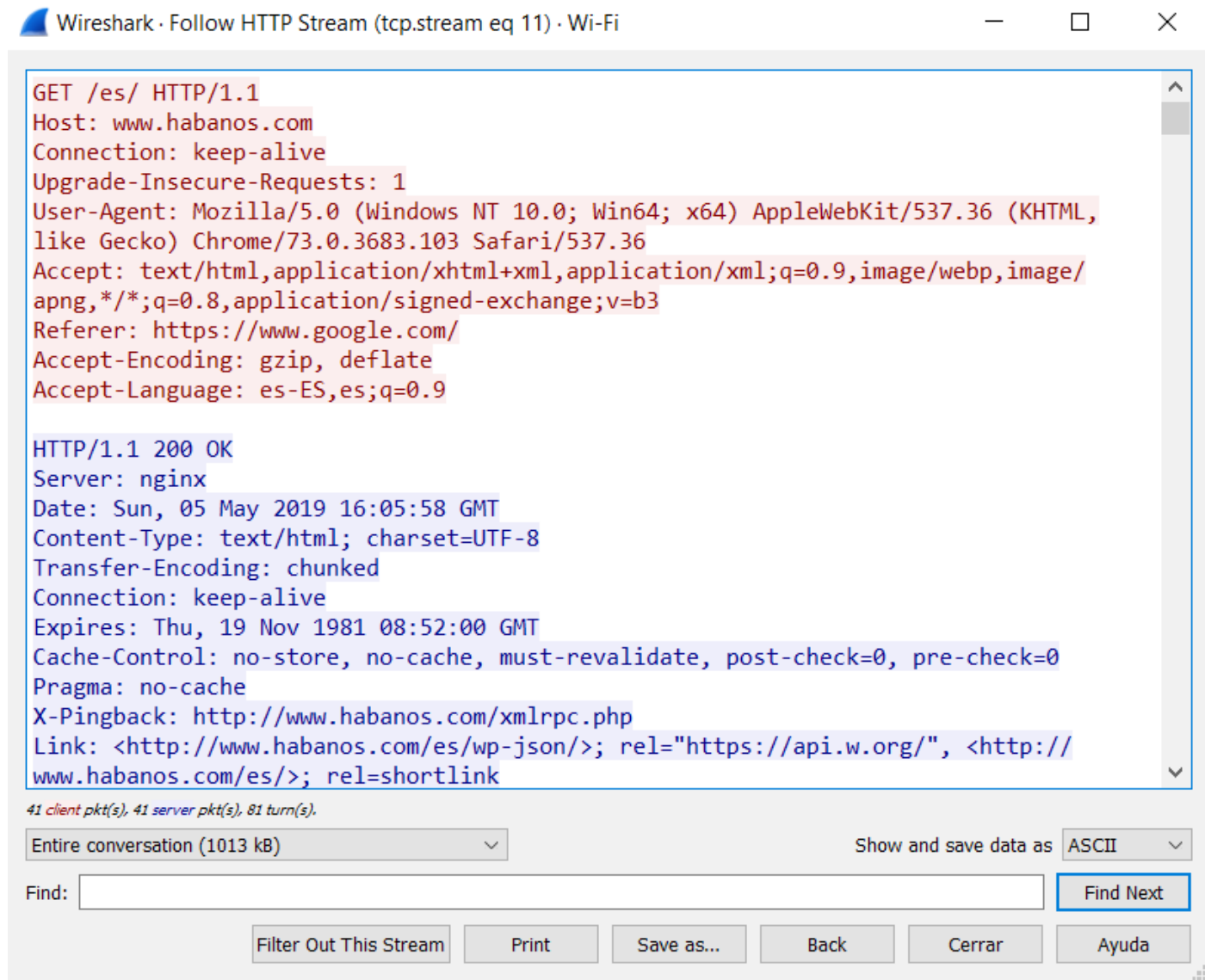
(((tcp.dstport == 80) || (tcp.srcport == 80)) and http.request.method == GET)

No.	Time	Source	Destination	Protocol	Puerto origen	Puerto destino	Lengt	Info
443	9.903209	192.168.1.36	144.76.245.212	HTTP	52514	80	508	GET /es/ HTTP/1.1
493	12.089098	192.168.1.36	144.76.245.212	HTTP	52516	80	581	GET /wp-content/themes/habanos_theme/css/tabs-textos-mapas.css?ver=5.1.1 HTTP/1.1
494	12.089287	192.168.1.36	144.76.245.212	HTTP	52515	80	577	GET /wp-content/themes/habanos_theme/css/donde-comprar.css?ver=5.1.1 HTTP/1.1
516	12.120858	192.168.1.36	144.76.245.212	HTTP	52517	80	577	GET /wp-content/themes/habanos_theme/fonts/continentes.css?ver=5.1.1 HTTP/1.1
517	12.121038	192.168.1.36	144.76.245.212	HTTP	52518	80	579	GET /wp-content/themes/habanos_theme/css/bootstrap.icons.css?ver=5.1.1 HTTP/1.1
521	12.123823	192.168.1.36	144.76.245.212	HTTP	52519	80	579	GET /wp-content/themes/habanos_theme/css/jquery.toolbars.css?ver=5.1.1 HTTP/1.1
538	12.137917	192.168.1.36	144.76.245.212	HTTP	52516	80	593	GET /wp-includes/js/mediaelement/mediaelementplayer-legacy.min.css?ver=4.2.6-78496d1 HTTP/1.1
539	12.139035	192.168.1.36	144.76.245.212	HTTP	52515	80	575	GET /wp-includes/js/mediaelement/wp-mediaelement.min.css?ver=5.1.1 HTTP/1.1
542	12.139977	192.168.1.36	205.185.208.52	HTTP	52520	80	394	GET /jquery-1.11.1.min.js?ver=1.10.2 HTTP/1.1
561	12.152299	192.168.1.36	144.76.245.212	HTTP	52514	80	572	GET /wp-includes/css/dist/block-library/style.min.css?ver=5.1.1 HTTP/1.1
610	12.170756	192.168.1.36	144.76.245.212	HTTP	52517	80	585	GET /wp-content/plugins/contact-form-7_old/includes/css/styles.css?ver=4.6.1 HTTP/1.1
611	12.171532	192.168.1.36	144.76.245.212	HTTP	52518	80	576	GET /wp-content/plugins/cookie-law-info/css/cli-style.css?ver=1.5.3 HTTP/1.1
612	12.173937	192.168.1.36	144.76.245.212	HTTP	52519	80	589	GET /wp-content/plugins/easy-fancybox/fancybox/jquery.fancybox.min.css?ver=1.3.9 HTTP/1.1
627	12.186878	192.168.1.36	144.76.245.212	HTTP	52516	80	574	GET /wp-content/plugins/gdpr/assets/css/gdpr-public.css?ver=2.0.6 HTTP/1.1
628	12.187707	192.168.1.36	144.76.245.212	HTTP	52515	80	585	GET /wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.2.5.2 HTTP/1.1
657	12.219763	192.168.1.36	144.76.245.212	HTTP	52517	80	576	GET /wp-content/plugins/simple-social-share/css/style.css?ver=5.1.1 HTTP/1.1
658	12.219929	192.168.1.36	144.76.245.212	HTTP	52518	80	582	GET /wp-content/plugins/simple-social-share/css/tooltipster.css?ver=5.1.1 HTTP/1.1
659	12.221250	192.168.1.36	144.76.245.212	HTTP	52519	80	565	GET /wp-content/themes/habanos_theme/tippy.css?ver=5.1.1 HTTP/1.1
689	12.245317	192.168.1.36	144.76.245.212	HTTP	52514	80	588	GET /wp-content/plugins/vegas-fullscreen-background-slider/css/jquery.vegas.css HTTP/1.1
702	12.269955	192.168.1.36	144.76.245.212	HTTP	52517	80	580	GET /wp-content/plugins/age-verify/includes/assets/styles.css?ver=5.1.1 HTTP/1.1
703	12.271452	192.168.1.36	144.76.245.212	HTTP	52518	80	575	GET /wp-content/themes/habanos_theme/fonts/genericons.css?ver=2.09 HTTP/1.1
704	12.271677	192.168.1.36	144.76.245.212	HTTP	52519	80	570	GET /wp-content/themes/habanos_theme/style.css?ver=2013-07-18 HTTP/1.1

- Ver sólo peticiones GET transmitidas por el puerto 80.

# Introducción al uso de Wireshark

- Seguir el tráfico HTTP o TCP de una conversación con Follow Stream.





## Conclusión

- Wireshark es una herramienta muy útil en manos de un experto en redes, pero también permite una primera toma de contacto fácil para personas con conocimientos básicos sobre redes.
- Esto sumado a su infinidad de funciones y herramientas, su licencia libre y a su posibilidad de funcionar en casi cualquier sistema operativo hace que muchos lo consideren uno de los mejores analizadores de red que existen en la actualidad.