Análisis de tráfico con Wireshark

Realizado por:
José Mª 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?

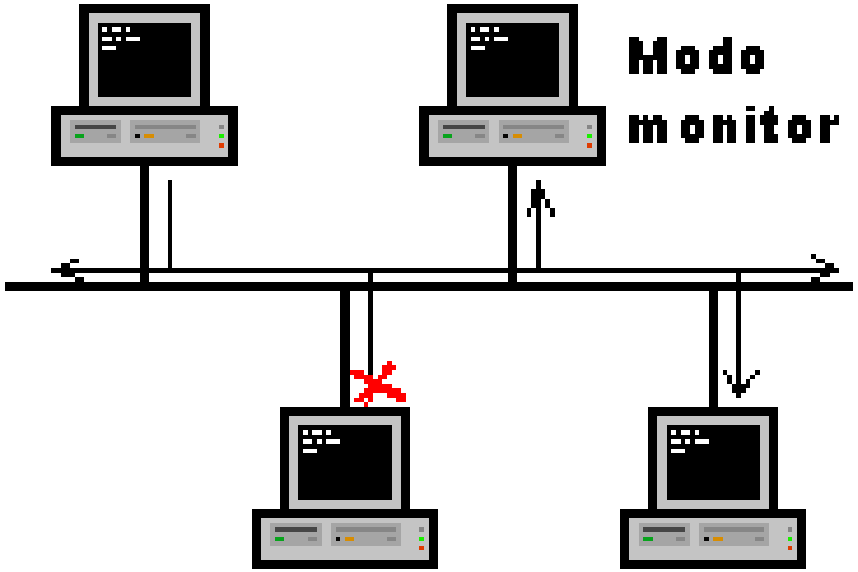
- Antiguo Ethereal, lanzado en 1999.
- Multiplataforma.
- Software libre
- Analizador de protocolos.
- Herramienta didáctica.
- Más de 480 protocolos.

¿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.4
- Existen infinidad de filtros:
  - Por protocolo
  - Por tipo de petición
  - Paquetes que contengan una palabra
  - Filtrado por IP
  - Por MAC
  - Por puerto

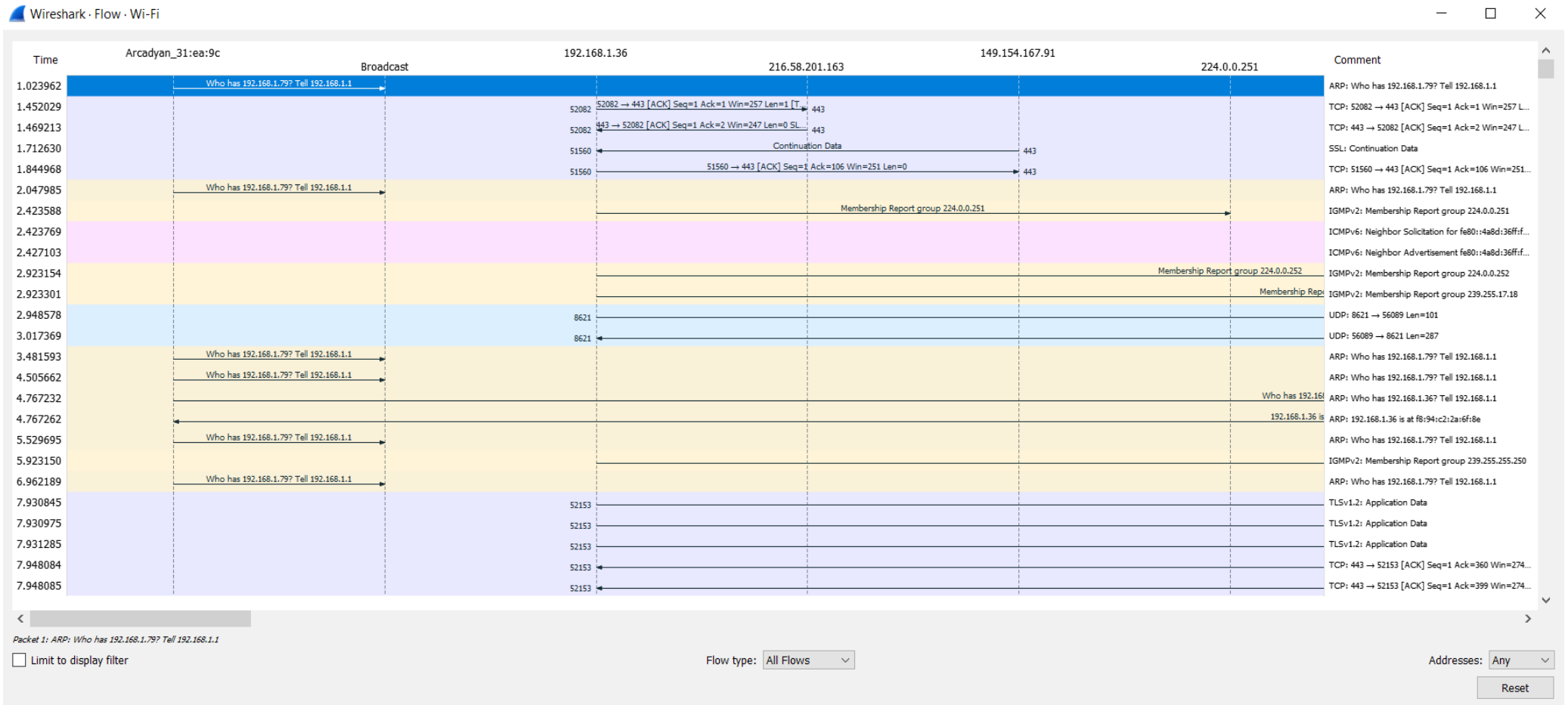
... (entre otros)

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.

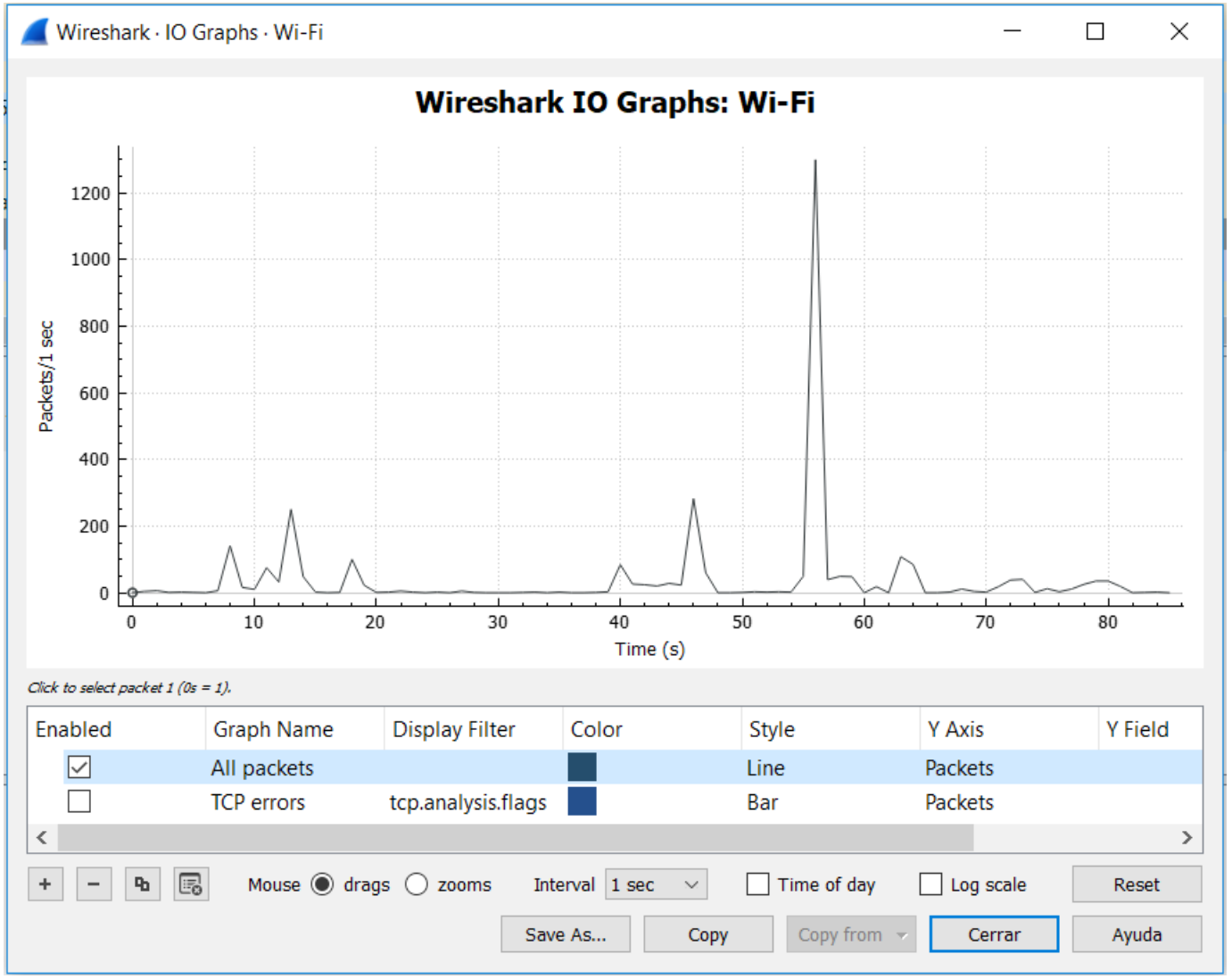
Gráficas

- Grafos de flujo



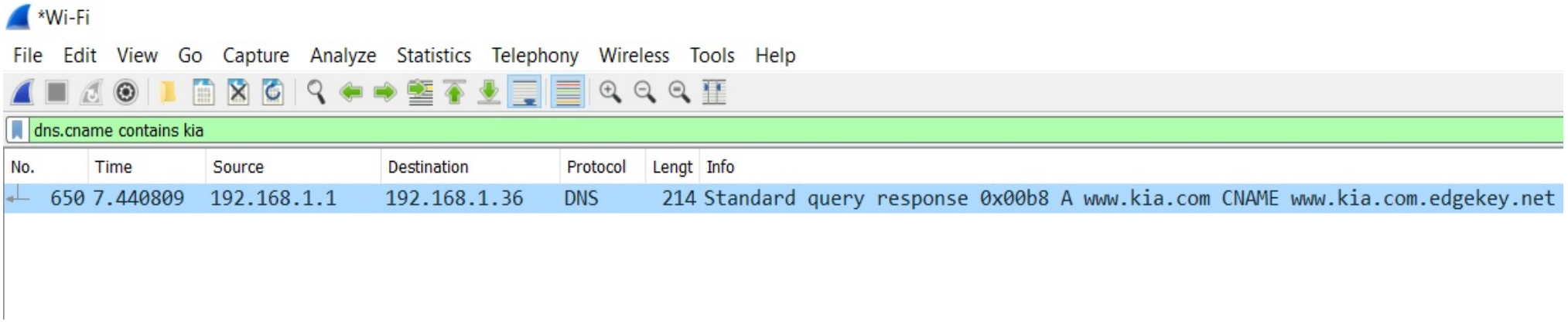
Gráficas

- IO Graphs



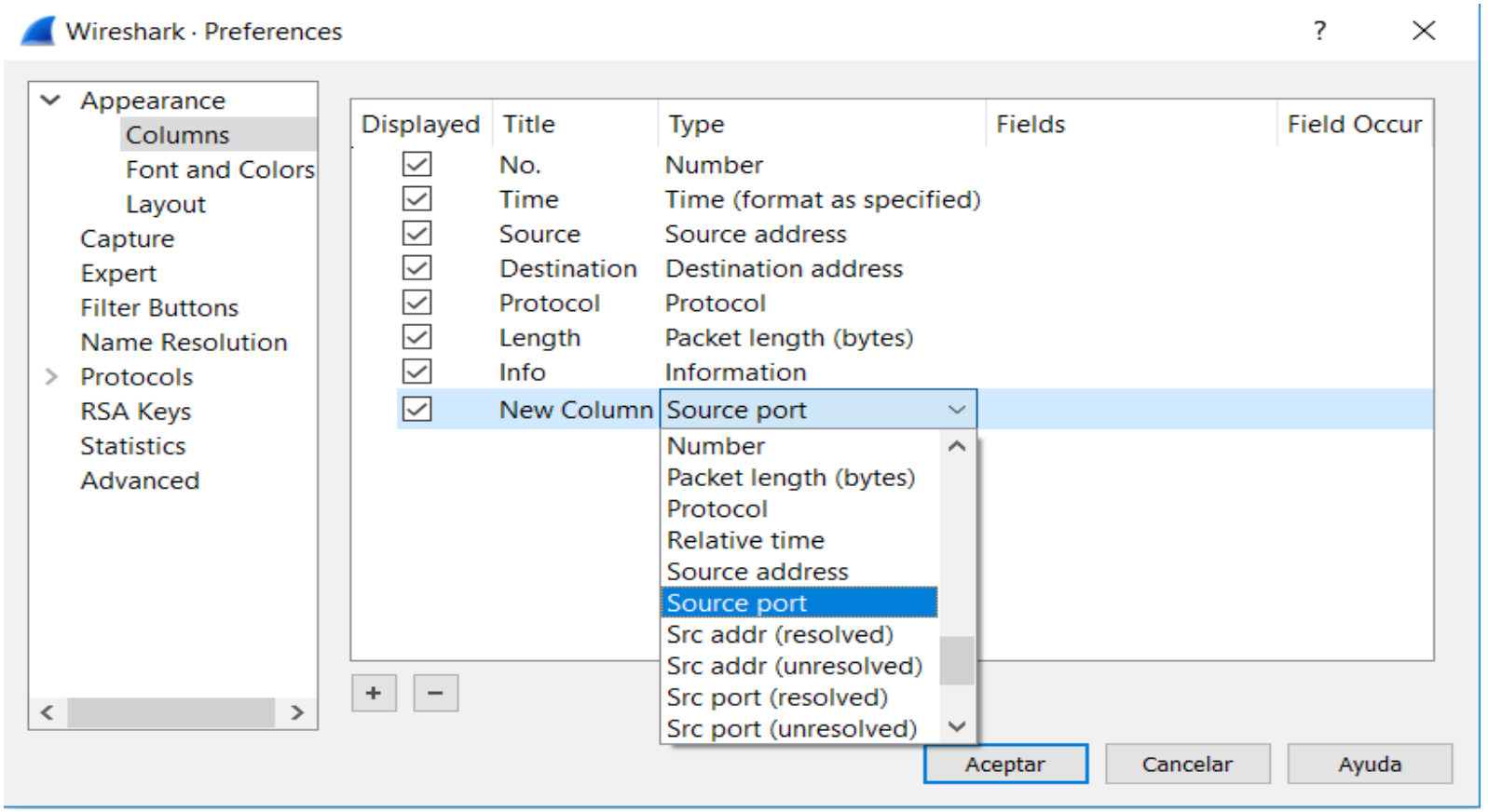
Introducción al uso de Wireshark

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



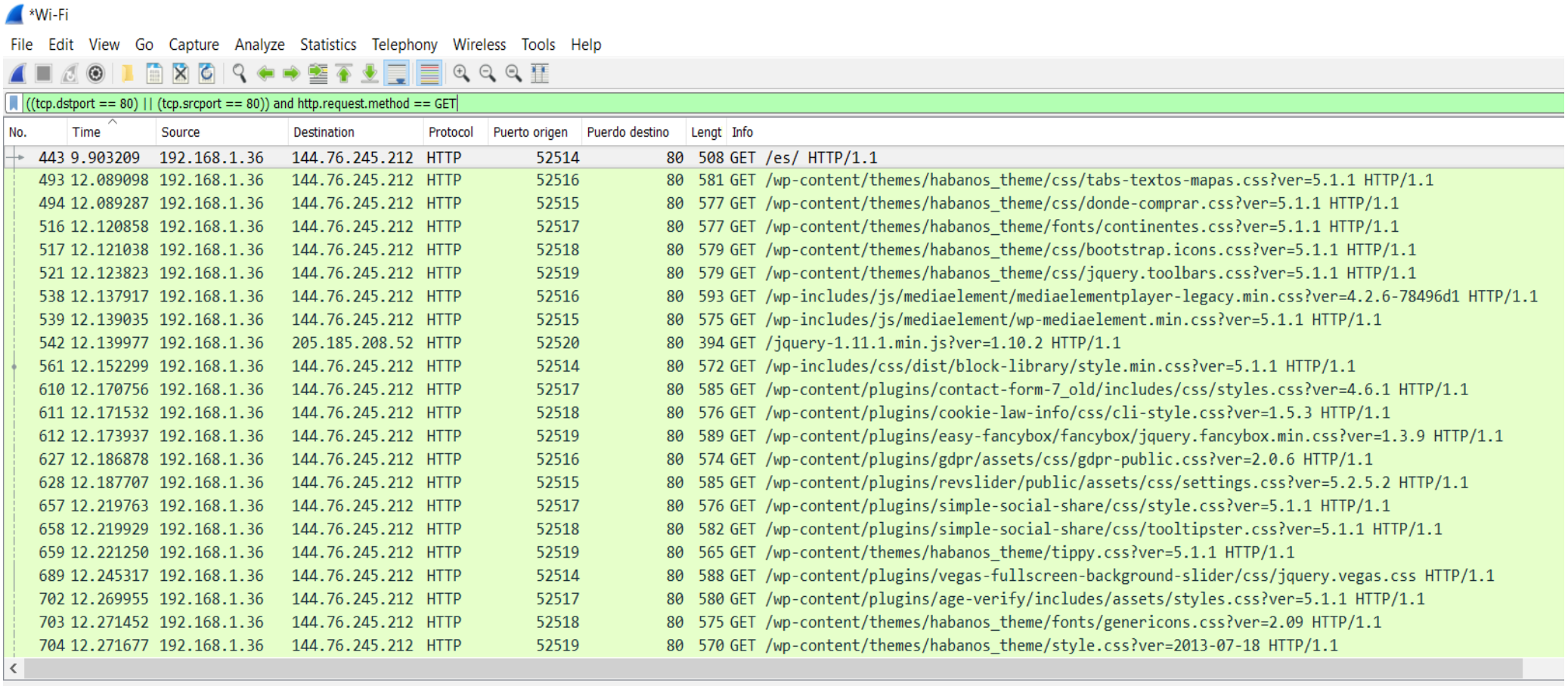
- Identificar la trama DNS donde se traduce una dirección a IP.

Introducción al uso de Wireshark



- Añadir columnas para ver el puerto origen y destino.

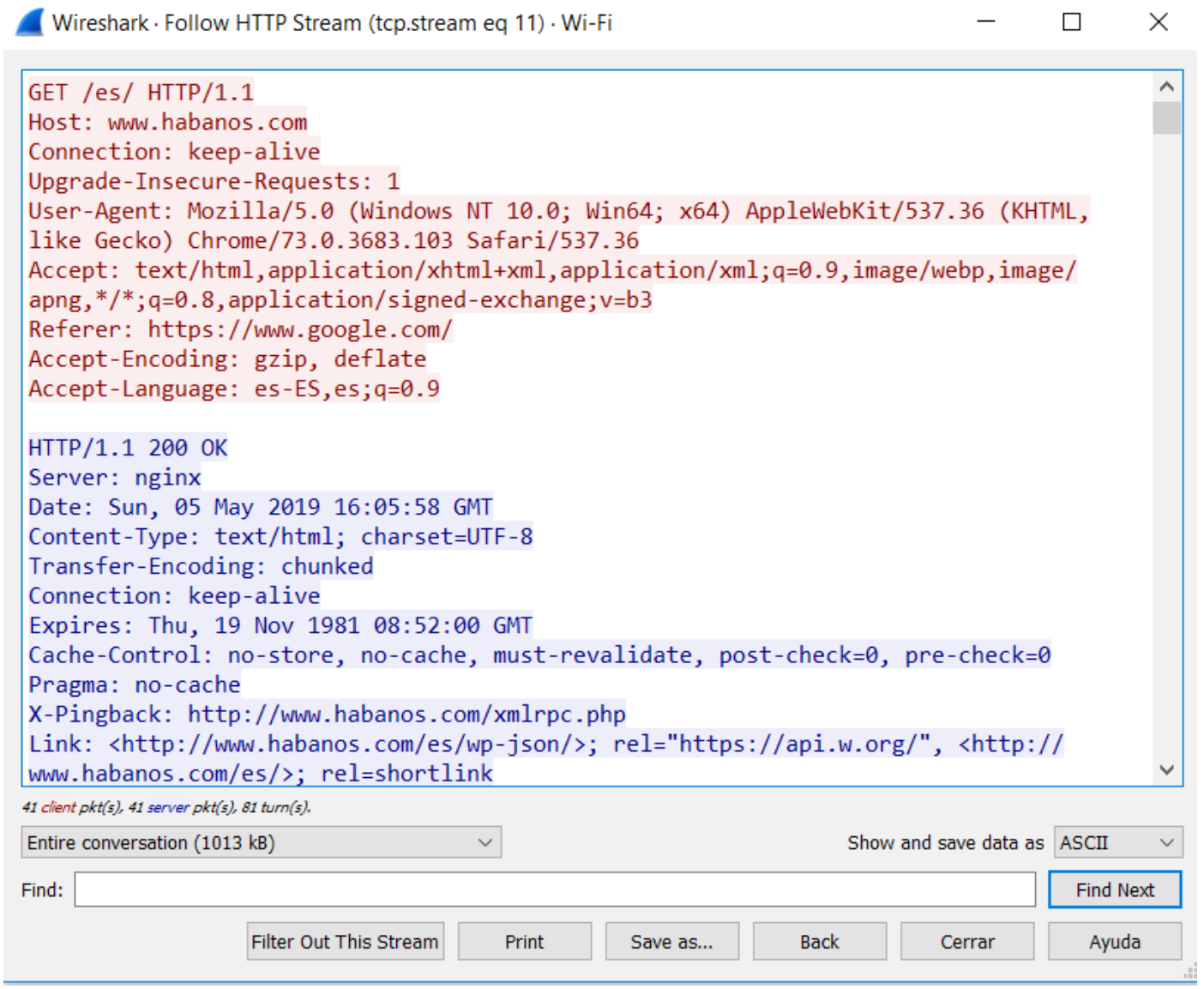
Introducción al uso de Wireshark



- 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.