ANÁLISIS DE PROTOCOLO

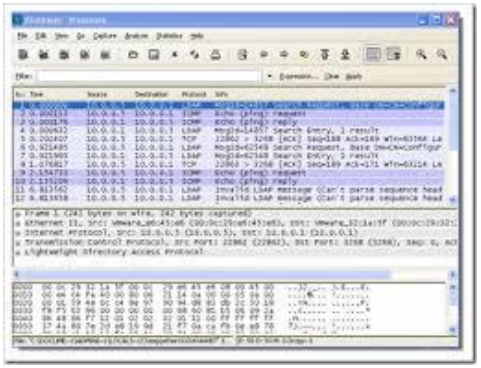
¿Qué es?

¿Qué información proporciona?

¿Qué es un analizador de protocolos?

Es un dispositivo (o software) que **captura** conversaciones entre dos o más sistemas o dispositivos, lo analiza, decodifica e interpreta, brindando una representación de su escucha en lenguaje entendible; por medio de la cual se obtiene la información necesaria para el análisis de una red y las estadísticas que el analizador nos proporciona.

Es una herramienta que provee información acerca del flujo de datos sobre una red, mostrando exactamente qué es lo que está sucediendo en ella, detectando anomalías, problemas o simplemente tráfico innecesario.



¿Qué tipos de información proporciona?

- **Estadísticas** sobre tráfico de datos, estado de los dispositivos y líneas de errores en la LAN. Esta información ayuda a identificar tramas y condiciones generales que pueden señalar un problema inesperado o causar un bajo rendimiento en la red. Permite también determinar nuevas necesidades de Hardware para segmentar o crear subredes dentro de la LAN como podría ser el empleo de Switch o router y la ubicación y configuración correcta de los mismos.
- **Captura de paquetes y decodificación de los mismos** en los distintos protocolos de cada nivel. Debería permitir también el filtrado correspondiente, que posibilite especificar en el mayor grado de detalle lo que se desea estudiar, dejando de lado la información innecesaria.
  Se suele filtrar por Dirección MAC, IP, Nombre NetBIOS, puertos, tipo de protocolo, secuencias de bit, etc.
- **Representación de información histórica** en lapsos diarios, semanales, mensuales o en períodos establecidos por el usuario. Esta información provee una perspectiva histórica para cualquier nuevo problema o indica un problema potencial antes que este suceda.

Para qué analizar el tráfico

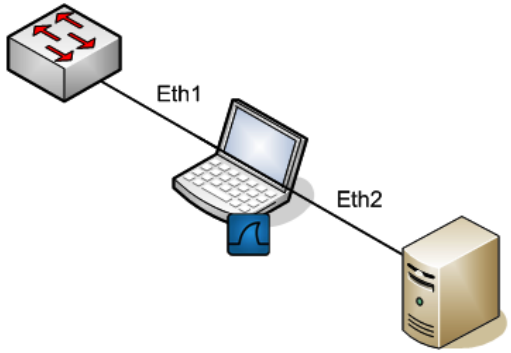
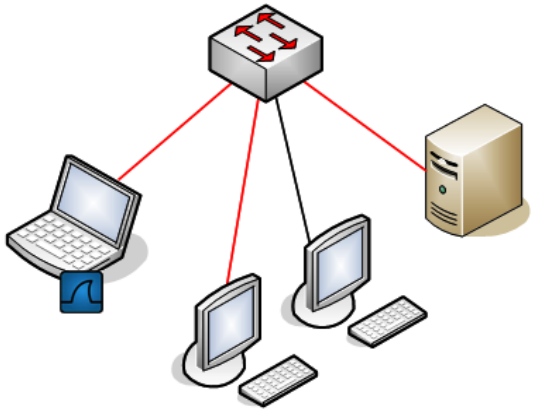
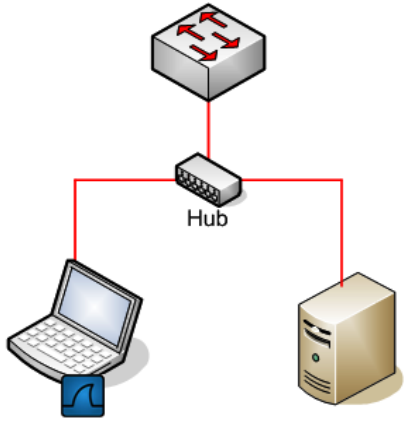
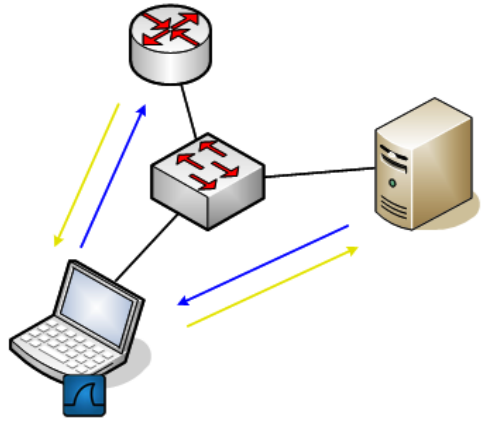
- **Para identificar problemas en la red**
- **Para determinar rendimiento, optimización**
- **Para identificar conectividad**
- **Para determinar problemas de configuración (tormentas de broadcast, spanning-tree mal configurado, enlaces redundantes, etc)**
- **Para identificar ataques de terceros (DoS, envenenamiento ARP, código malicioso, etc)**
- **Para detectar, analizar y correlacionar el tráfico identificando amenazas o problemas para limitar su impacto en la red.**

WIRESHARK

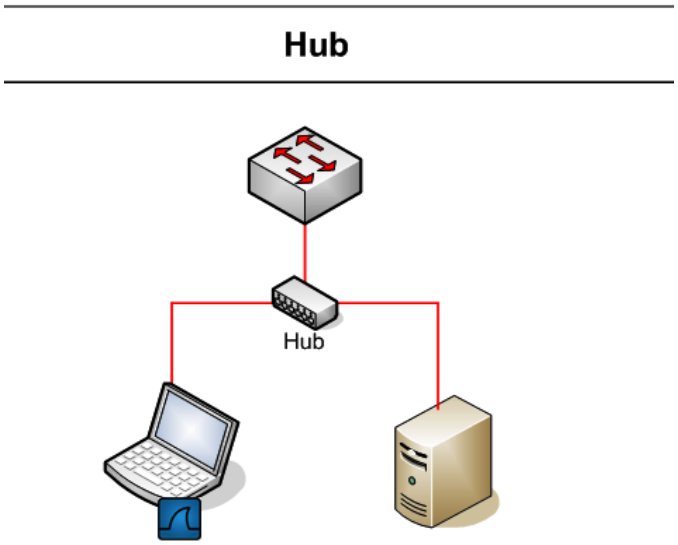
Wireshark es un analizador de protocolos *open-source* diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente (versión 1.4.3); y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados

Dónde capturar

Modo Bridge	Port Mirroring
	
Hub	**Arp-Spoof**
	

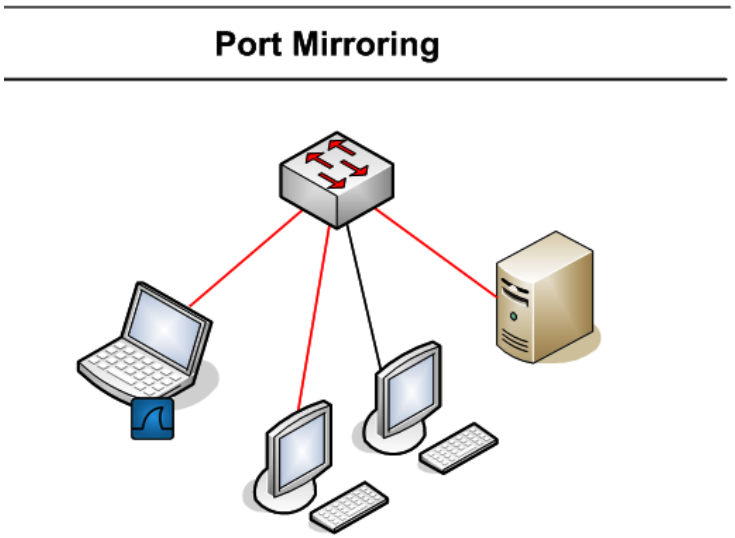
Dónde capturar



Conectar un HUB al switch es una alternativa para alcanzar nuestro propósito Debemos conectarlo en el mismo segmento de red donde se encuentra nuestro servidor.

Al tratarse de un medio compartido, todo el tráfico entre el *switch* y el servidor podrá analizarse en nuestro equipo.

Dónde capturar

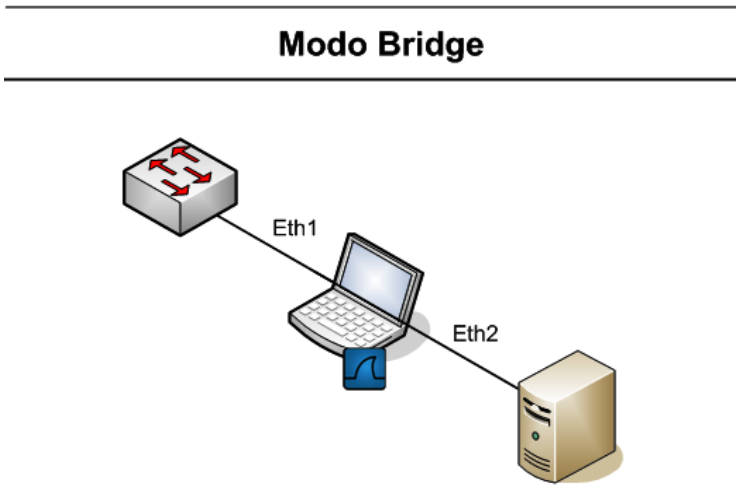


Conectar un switch que soporte Port Mirroring o VACL (Vlan- Based ACLs).

Es una alternativa que combina Vlans con ACLs para duplicar tráfico para alcanzar nuestro propósito.

En el Port Mirroring se duplica en un determinado puerto, en el VACL se duplica pero se filtra

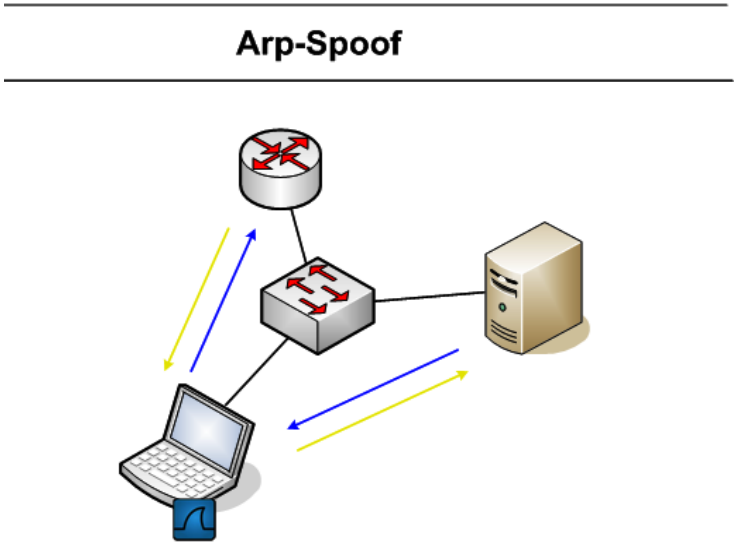
Dónde capturar



Se debe disponer de 2 placas de red para situarnos tipo *Man in the Middle* a nivel físico

Demanda una configuración de un bridge entre las placas físicas.

Dónde capturar

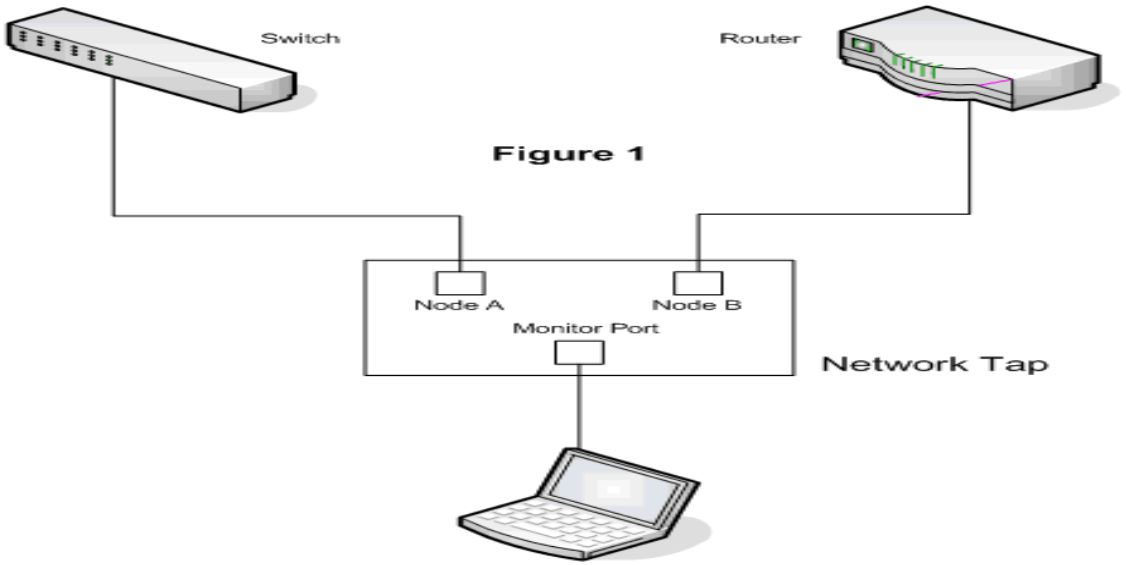


Cuando no se puedan los anteriores, se puede emplear el Arp-spoof.

Se debe configurar para que el equipo que se desea monitorizar envíe todas las tramas a través de nuestra PC donde tendremos Wireshark ejecutándose.

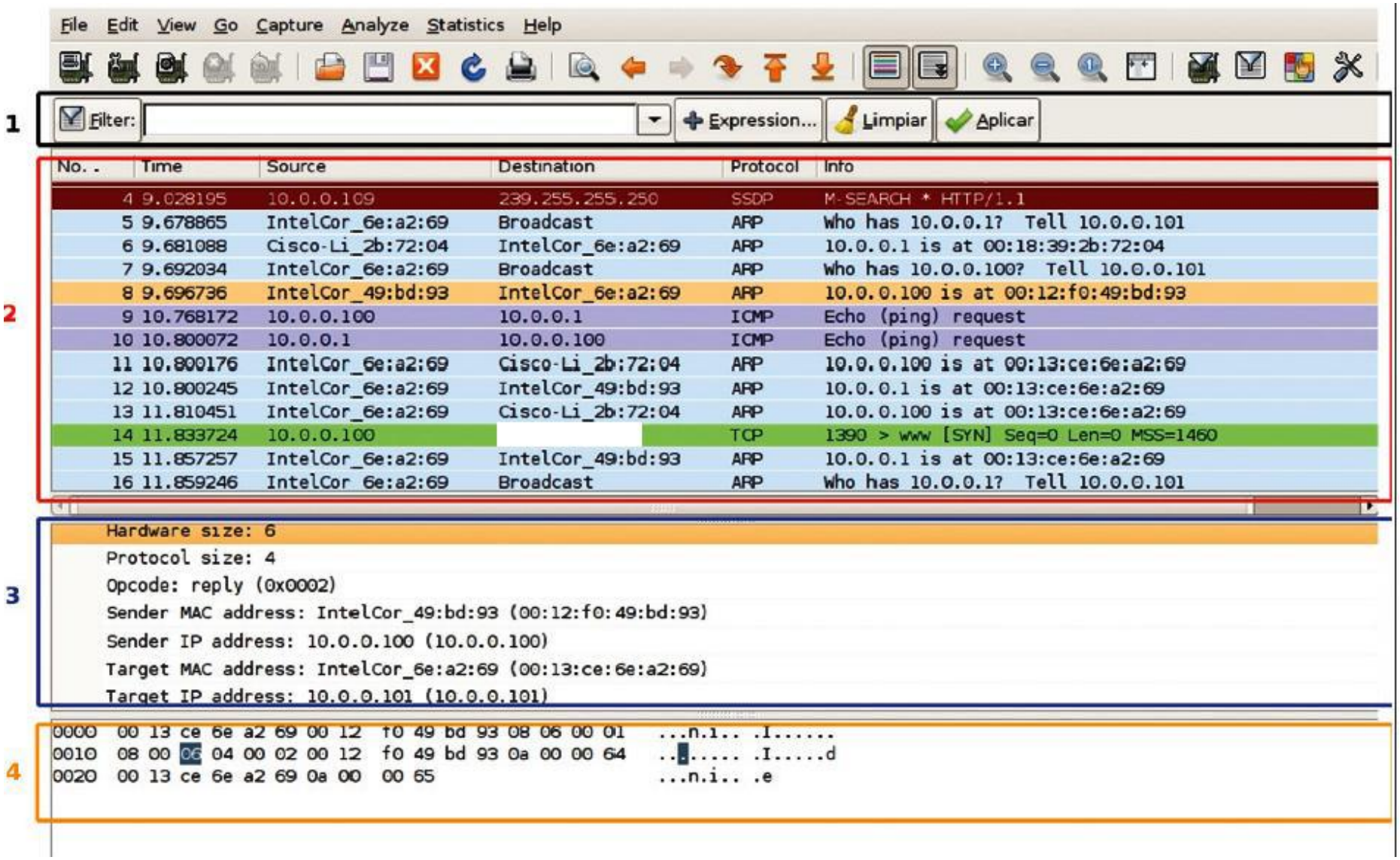
El proceso se lleva a cabo contaminando la cache de los equipos involucrados con una asociación IP/MAC falsa.

TAP- TEST ACCES PORT

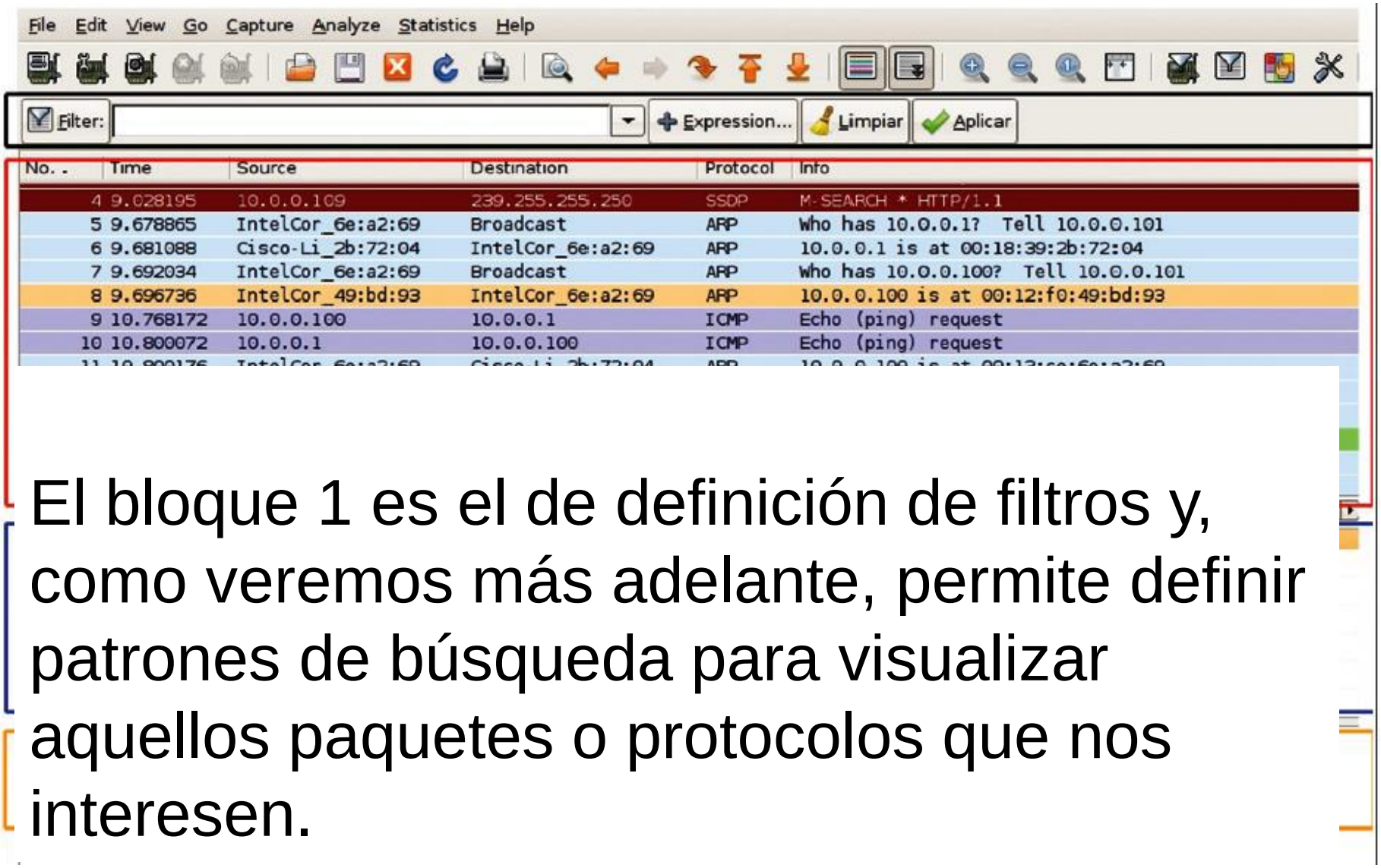


- **Esta solución, quizá la más eficiente y aconsejable aunque también más costosa y quizás más incomoda. Consiste en hacer uso de un Network TAP o "Test Access Port" (Puerto de acceso de pruebas). Con este dispositivo podemos capturar el tráfico de una red conmutada de forma pasiva, es decir, no interfiere en el flujo o tráfico de nuestra red.**
- **Los TAPs de red (Terminal Access Point por sus siglas en inglés) son el dispositivo de hardware más común a la hora de capturar tráfico de red.**
- **Un TAP de red es básicamente un hardware diseñado para acceder al tráfico entre dos nodos de red y reflejarlo en un puerto de monitor donde podemos conectar una herramienta de análisis de terceros para escuchar.**

Bloques de Wireshark

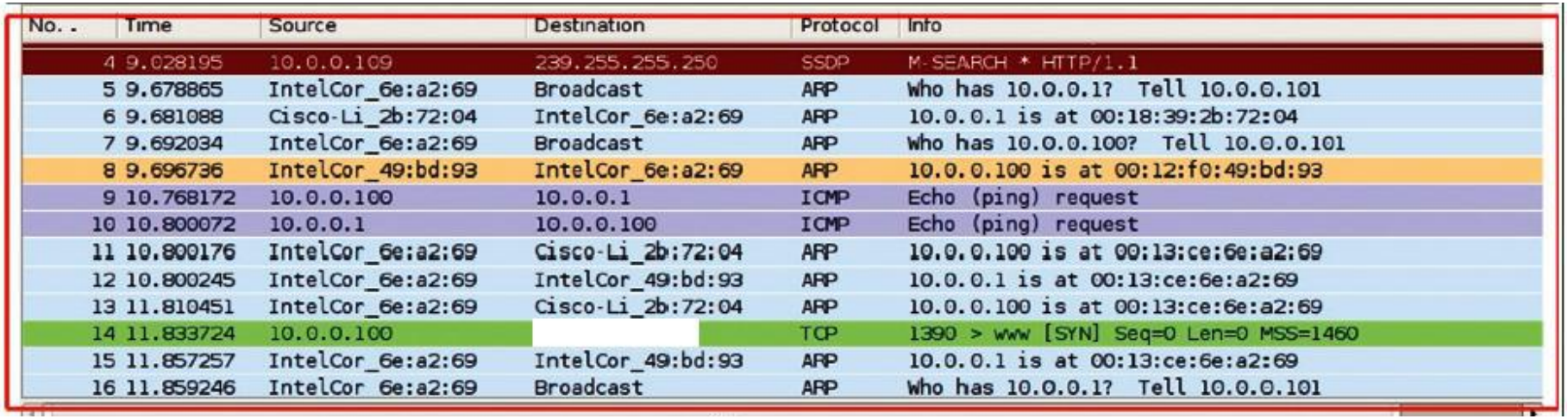


Bloques de Wireshark



El bloque 1 es el de definición de filtros y, como veremos más adelante, permite definir patrones de búsqueda para visualizar aquellos paquetes o protocolos que nos interesen.

Bloques de Wireshark



No. .	Time	Source	Destination	Protocol	Info
4	9.028195	10.0.0.109	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
5	9.678865	IntelCor_6e:a2:69	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.101
6	9.681088	Cisco-Li_2b:72:04	IntelCor_6e:a2:69	ARP	10.0.0.1 is at 00:18:39:2b:72:04
7	9.692034	IntelCor_6e:a2:69	Broadcast	ARP	Who has 10.0.0.100? Tell 10.0.0.101
8	9.696736	IntelCor_49:bd:93	IntelCor_6e:a2:69	ARP	10.0.0.100 is at 00:12:f0:49:bd:93
9	10.768172	10.0.0.100	10.0.0.1	ICMP	Echo (ping) request
10	10.800072	10.0.0.1	10.0.0.100	ICMP	Echo (ping) request
11	10.800176	IntelCor_6e:a2:69	Cisco-Li_2b:72:04	ARP	10.0.0.100 is at 00:13:ce:6e:a2:69
12	10.800245	IntelCor_6e:a2:69	IntelCor_49:bd:93	ARP	10.0.0.1 is at 00:13:ce:6e:a2:69
13	11.810451	IntelCor_6e:a2:69	Cisco-Li_2b:72:04	ARP	10.0.0.100 is at 00:13:ce:6e:a2:69
14	11.833724	10.0.0.100		TCP	1390 > www [SYN] Seq=0 Len=0 MSS=1460
15	11.857257	IntelCor_6e:a2:69	IntelCor_49:bd:93	ARP	10.0.0.1 is at 00:13:ce:6e:a2:69
16	11.859246	IntelCor_6e:a2:69	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.101

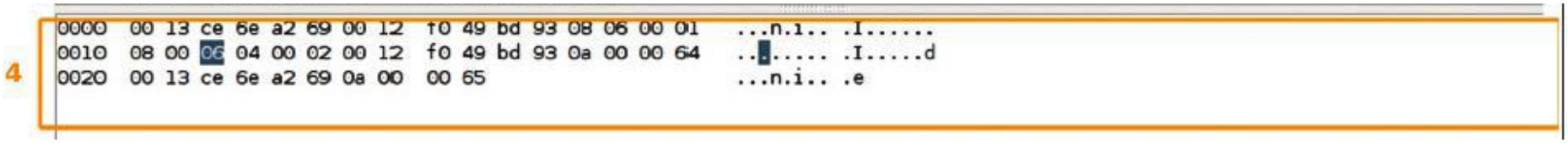
El bloque 2 se corresponde con la lista de visualización de todos los paquetes que se están capturando en tiempo real. Los datos proporcionados en esta zona son tipo de protocolo, números de secuencia, *flags*, marcas de tiempo, puertos, etc.

Bloques de Wireshark

El bloque 3 permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados en el bloque 2 y nos facilitará movernos por cada uno de los campos de las mismas.

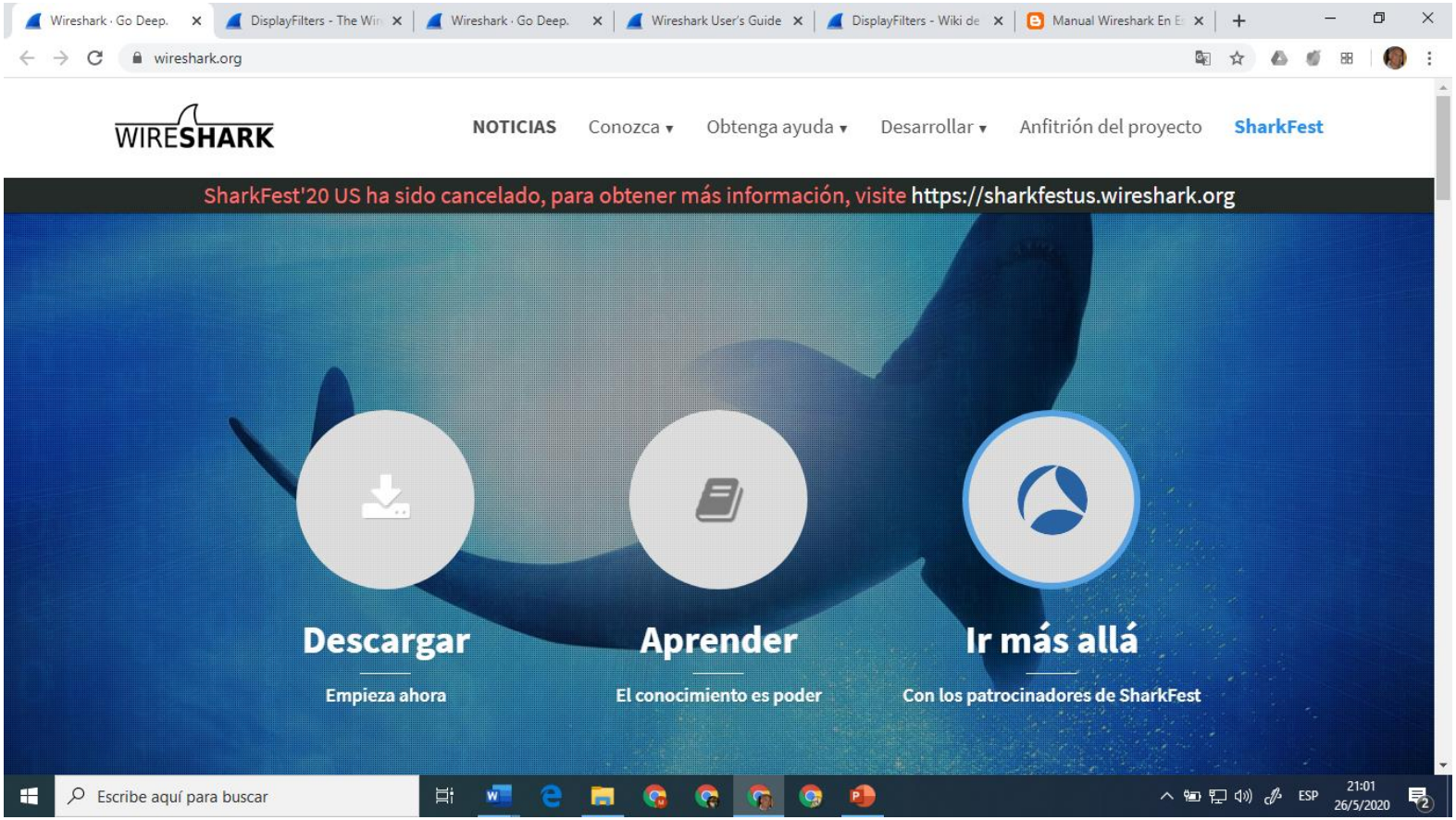
Bloques de Wireshark

Por último, el boque 4 representa, en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por nuestra placa de red.



Enlaces de interés

https://www.wireshark.org/



Software **Wireshark, versión 3.X.X**
https://www.wireshark.org/

Archivos de apoyo a la autopreparación:
https://www.wireshark.org/docs/wsug_html_chunked/index.html

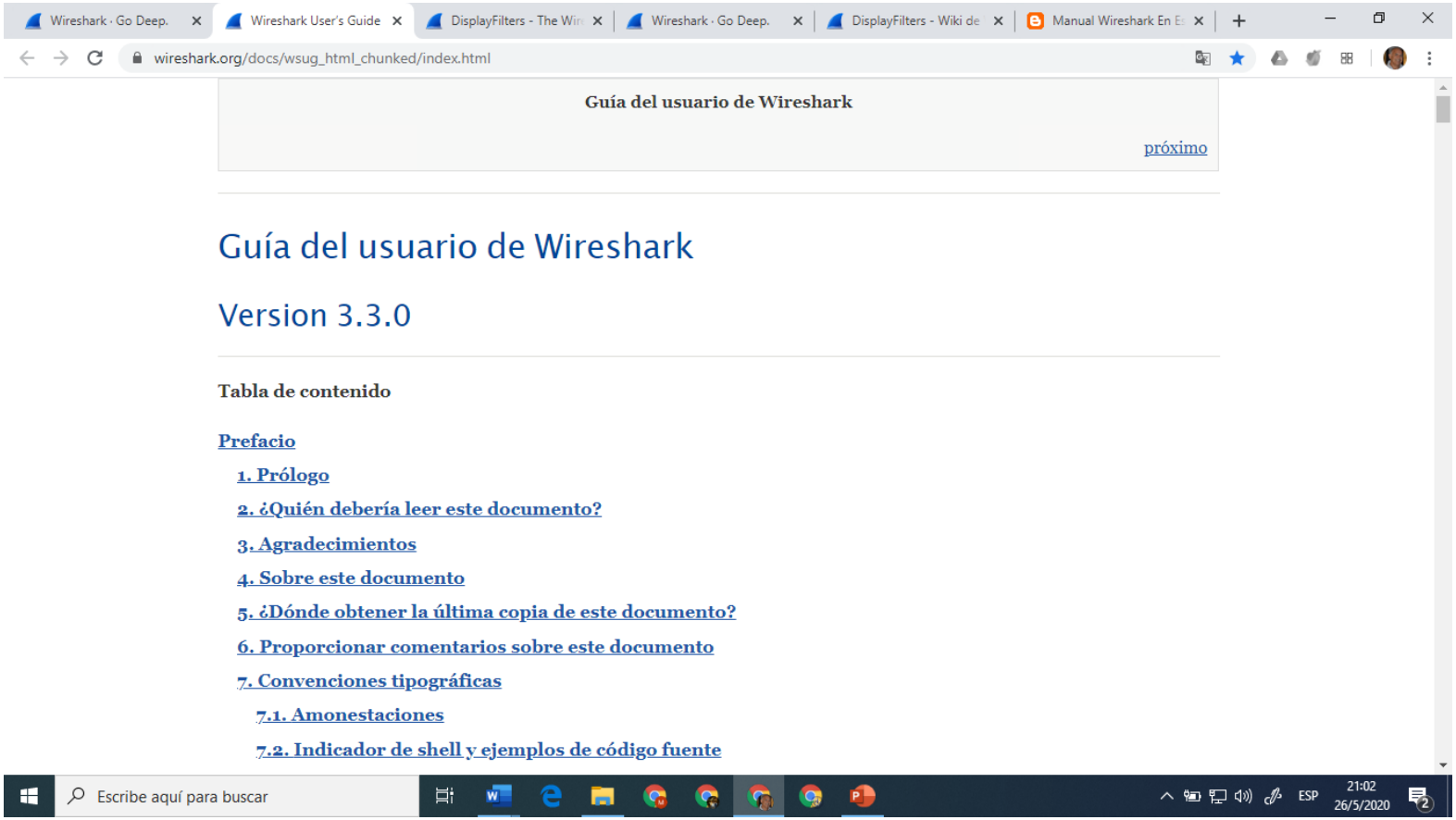
Video online
https://www.youtube.com/watch?v=shp42M7gbDE

Otros materiales sobre modos de captura y análisis de seguridad con Wireshark:
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Puede ser muy útil apoyar el estudio en los recursos en línea de Wireshark:
https://wiki.wireshark.org/

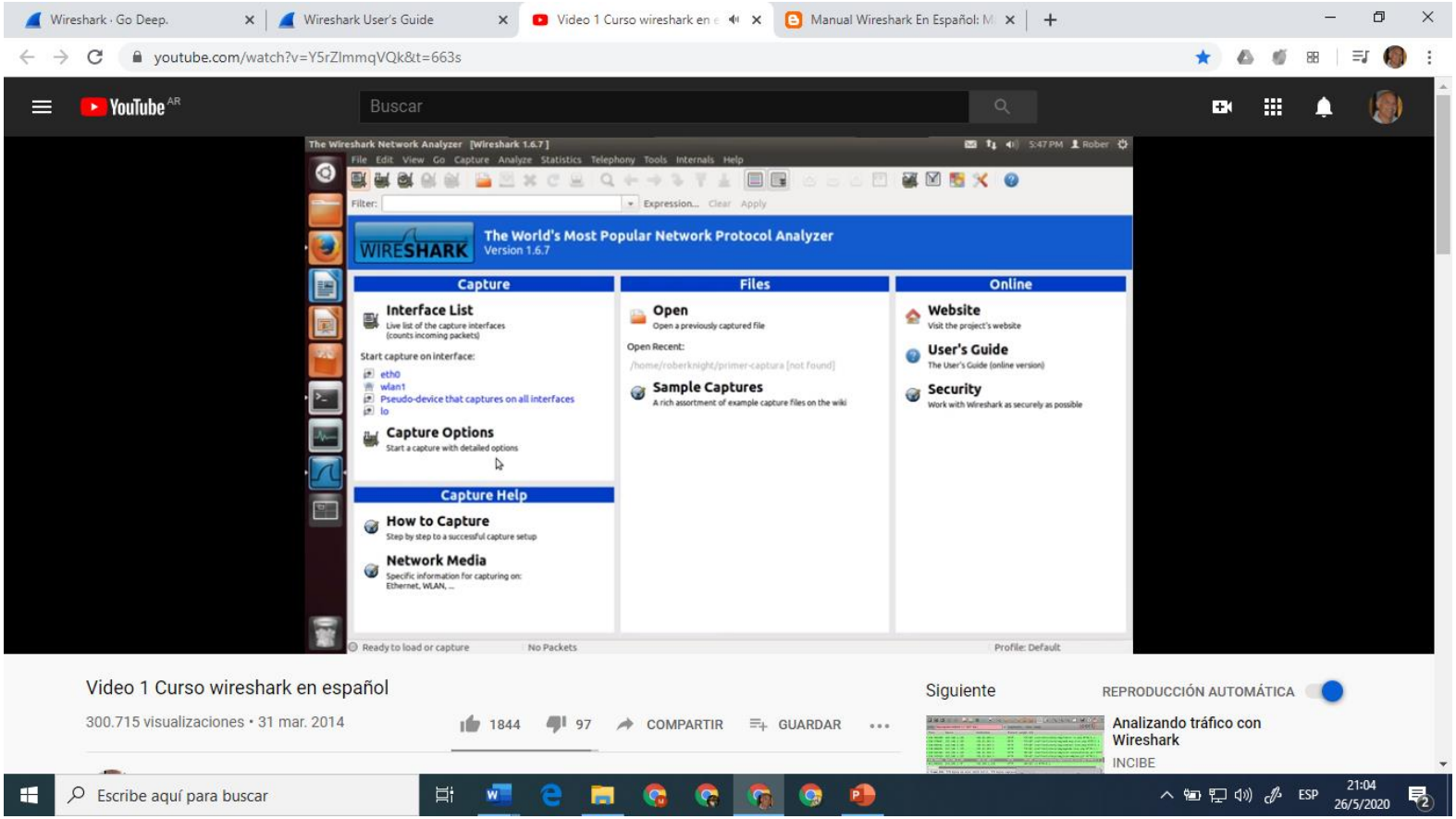
Enlaces de interés

https://www.wireshark.org/docs/wsug_html_chunked/index.html



Enlaces de interés

https://www.youtube.com/watch?v=Y5rZlmmqVQk&t=663s



Enlaces de interés

https://wiki.wireshark.org/