

ANÁLISIS DE PROTOCOLO

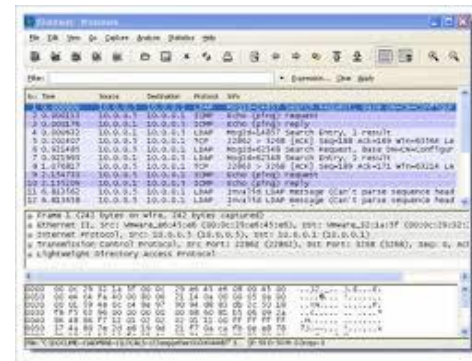
¿Qué es?

¿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.

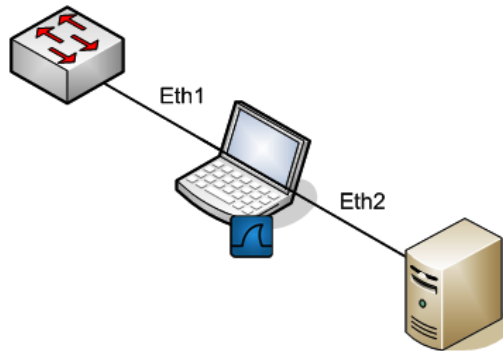
WIRESHARK

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

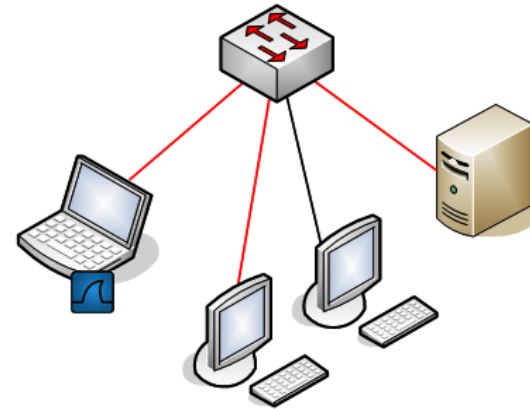
Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente (versión 1.4.3); y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados

Dónde capturar

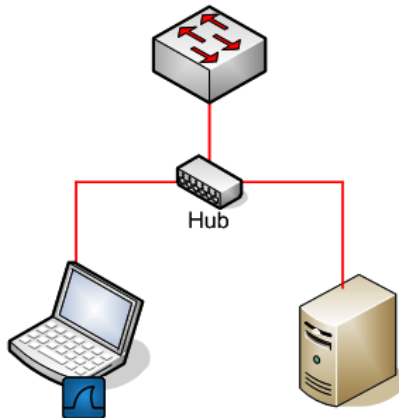
Modo Bridge



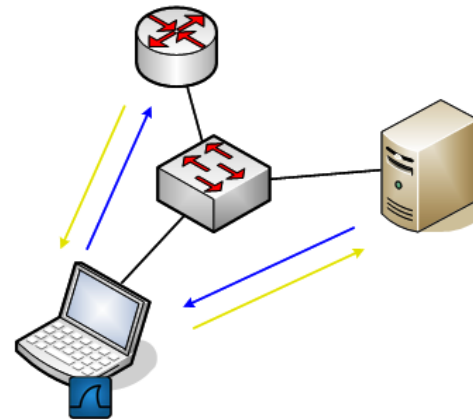
Port Mirroring



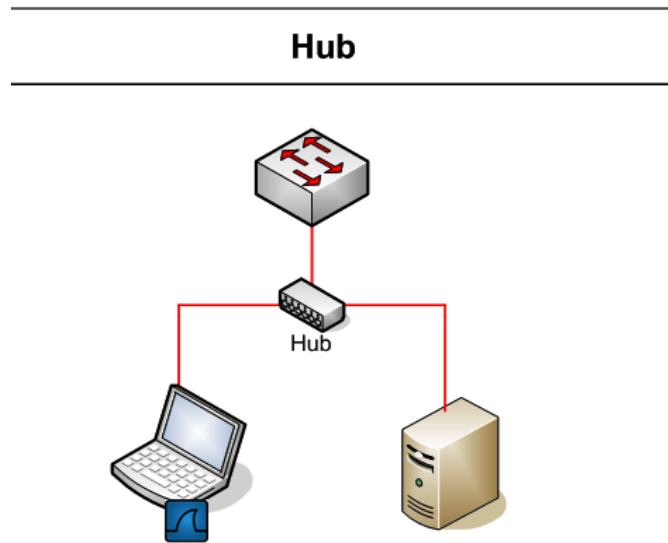
Hub



Arp-Spoof



Dónde capturar

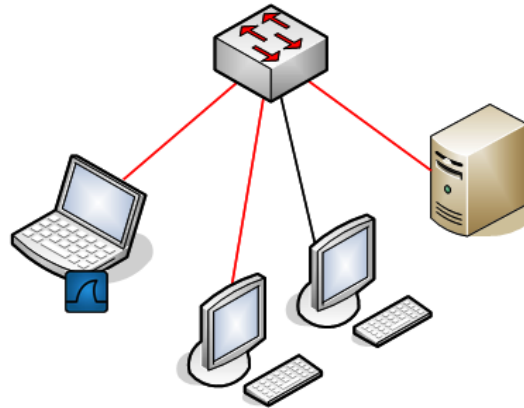


Conectar un HUB al switch es una alternativa para alcanzar nuestro propósito Debemos conectarlo en el mismo segmento de red donde se encuentra nuestro servidor.

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

Dónde capturar

Port Mirroring

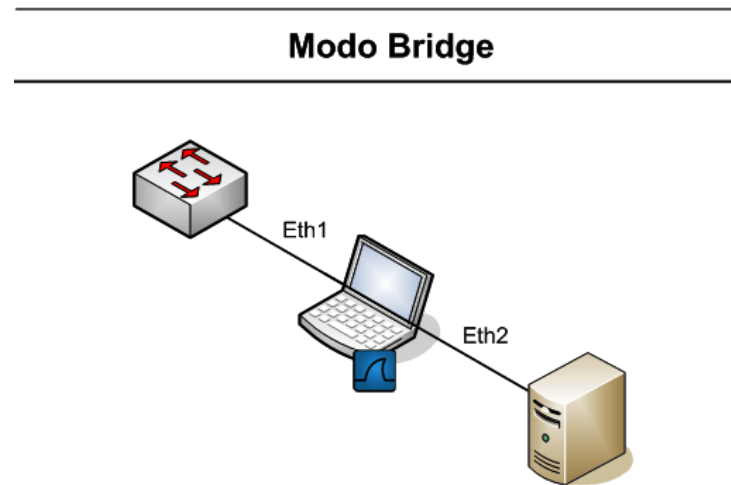


Conectar un switch que soporte Port Mirroring o VACL (Vlan- Based ACLs).

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

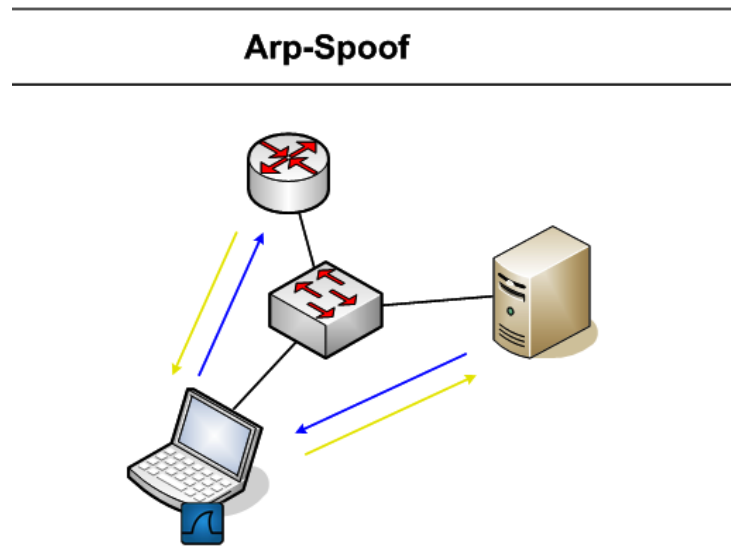
Dónde capturar



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

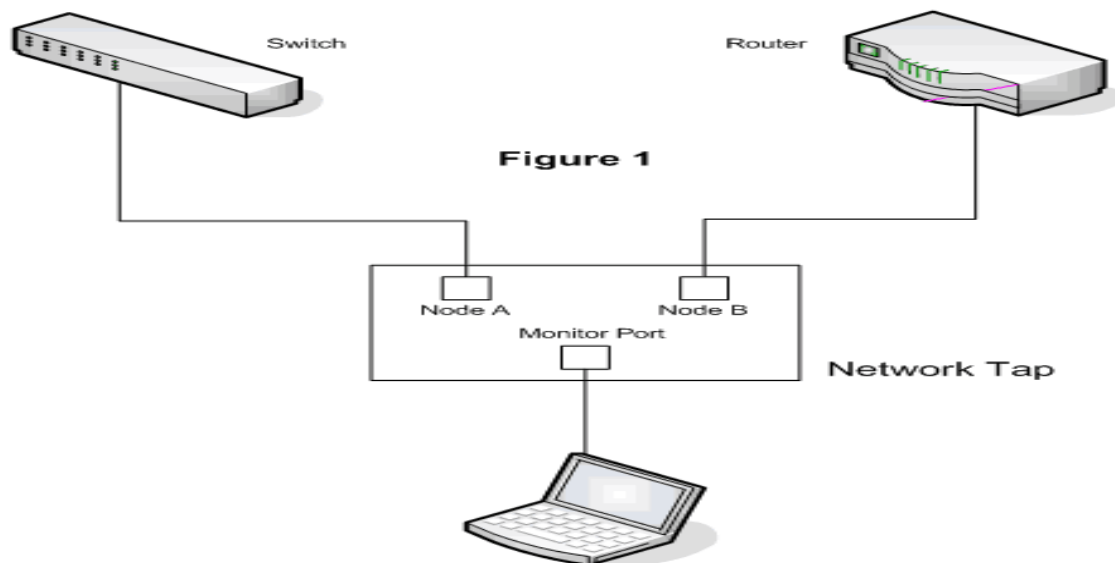


Cuando no se puedan los anteriores, se puede emplear el Arp-spoof.

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 ACCESS PORT



- Esta solución, quizá la más eficiente y aconsejable aunque también más costosa y quizás más incómoda. 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

1

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Limpiar Aplicar

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

2

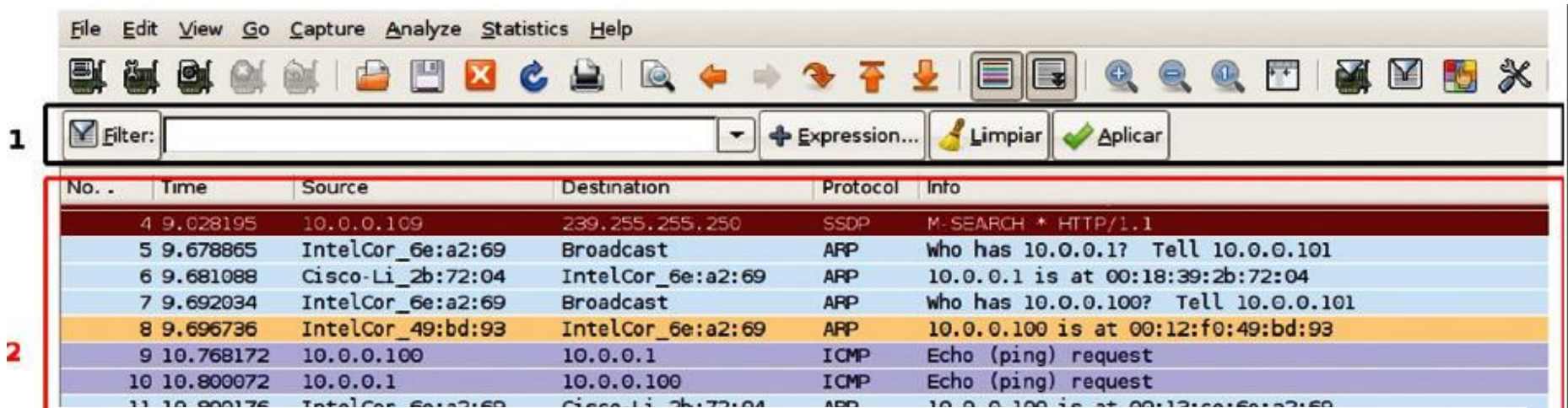
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender MAC address: IntelCor_49:bd:93 (00:12:f0:49:bd:93)
Sender IP address: 10.0.0.100 (10.0.0.100)
Target MAC address: IntelCor_6e:a2:69 (00:13:ce:6e:a2:69)
Target IP address: 10.0.0.101 (10.0.0.101)

3

0000 00 13 ce 6e a2 69 00 12 f0 49 bd 93 08 06 00 01 ...n.1.. .I.....
0010 08 00 06 04 00 02 00 12 f0 49 bd 93 0a 00 00 64 ..I.....
0020 00 13 ce 6e a2 69 0a 00 00 65 ...n.i.. .e

4

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.

3



```
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender MAC address: IntelCor_49:bd:93 (00:12:f0:49:bd:93)
Sender IP address: 10.0.0.100 (10.0.0.100)
Target MAC address: IntelCor_6e:a2:69 (00:13:ce:6e:a2:69)
Target IP address: 10.0.0.101 (10.0.0.101)
```

Bloques de Wireshark

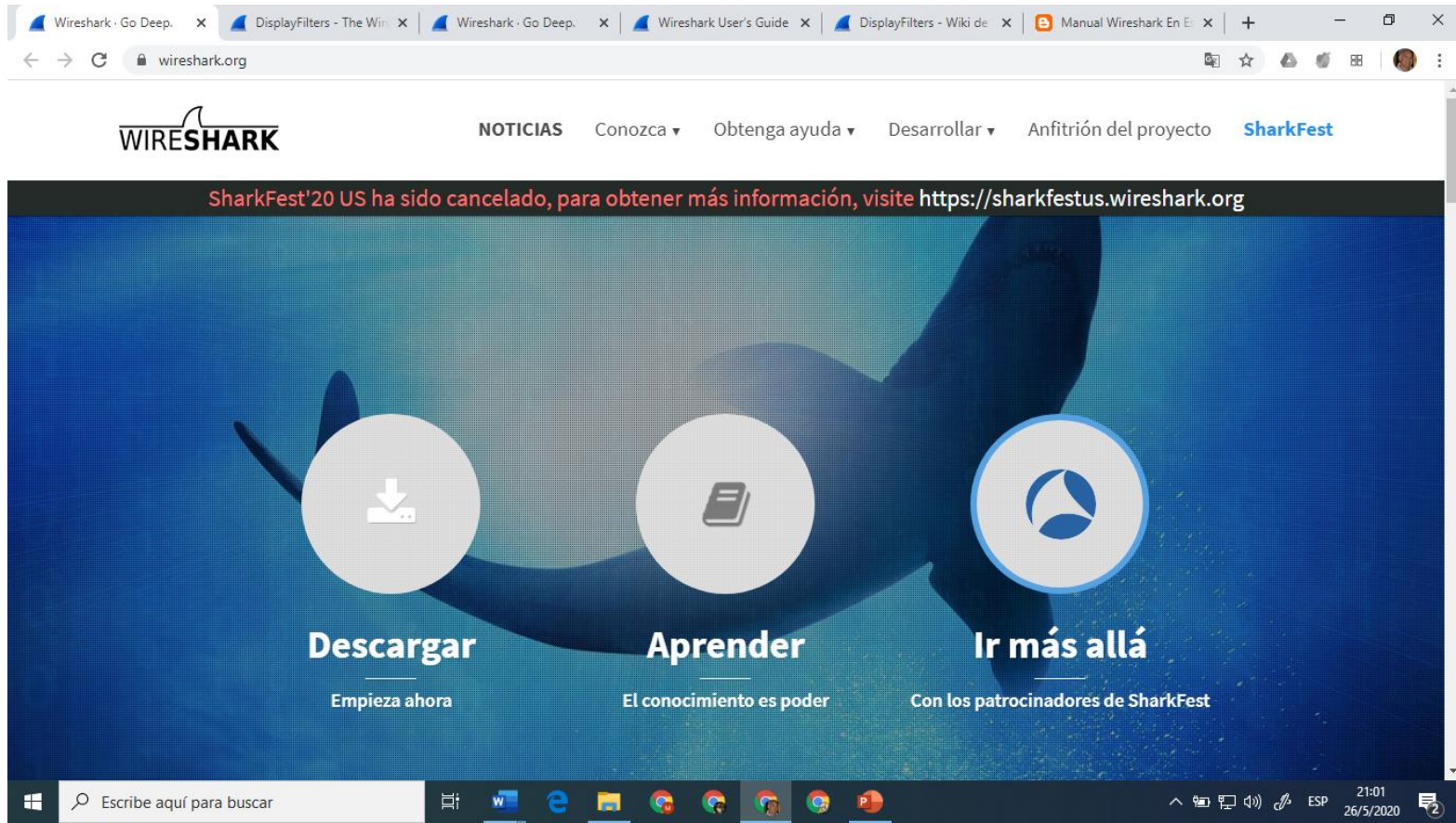
Por último, el bloque 4 representa, en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por nuestra placa de red.

4

```
0000  00 13 ce 6e a2 69 00 12 f0 49 bd 93 08 06 00 01  ...n.l.. .I.....
0010  08 00 06 04 00 02 00 12 f0 49 bd 93 0a 00 00 64  ..[..... .I.....d
0020  00 13 ce 6e a2 69 0a 00 00 65  ....n.i.. .e
```


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:

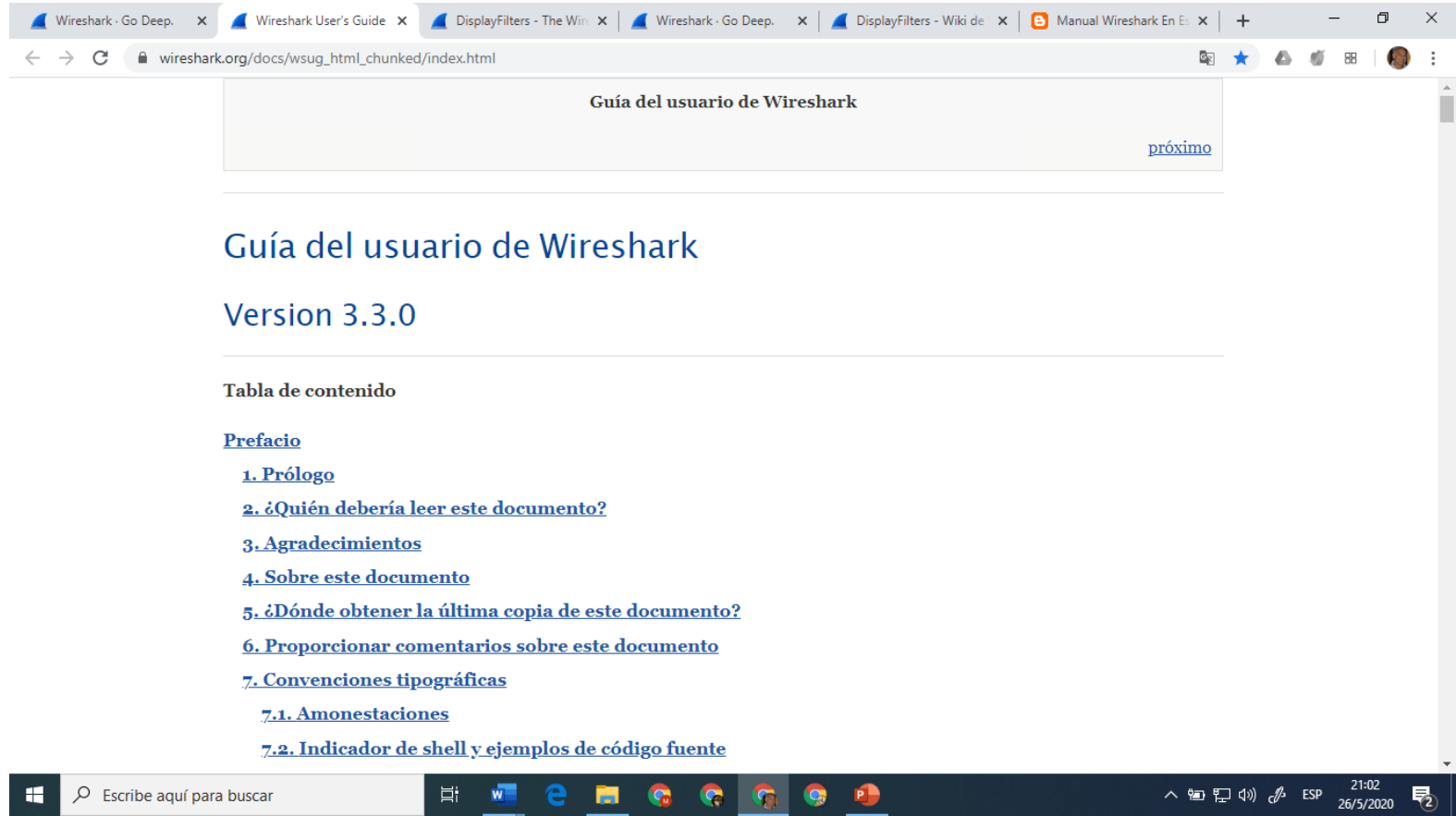
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

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



The screenshot shows a web browser window with multiple tabs. The active tab is titled "Wireshark User's Guide" and displays the URL "https://www.wireshark.org/docs/wsug_html_chunked/index.html". The page content includes a header "Guía del usuario de Wireshark" with a "próximo" link. Below this is the main title "Guía del usuario de Wireshark" followed by "Version 3.3.0". A "Tabla de contenido" (Table of Contents) section lists the following items:

- [Prefacio](#)
- [1. Prólogo](#)
- [2. ¿Quién debería leer este documento?](#)
- [3. Agradecimientos](#)
- [4. Sobre este documento](#)
- [5. ¿Dónde obtener la última copia de este documento?](#)
- [6. Proporcionar comentarios sobre este documento](#)
- [7. Convenciones tipográficas](#)
 - [7.1. Amonestaciones](#)
 - [7.2. Indicador de shell y ejemplos de código fuente](#)

The browser's taskbar at the bottom shows the Windows logo, a search bar, and several application icons including Word, Edge, File Explorer, and Chrome. The system tray on the right indicates the date and time as 26/5/2020, 21:02.

Enlaces de interés

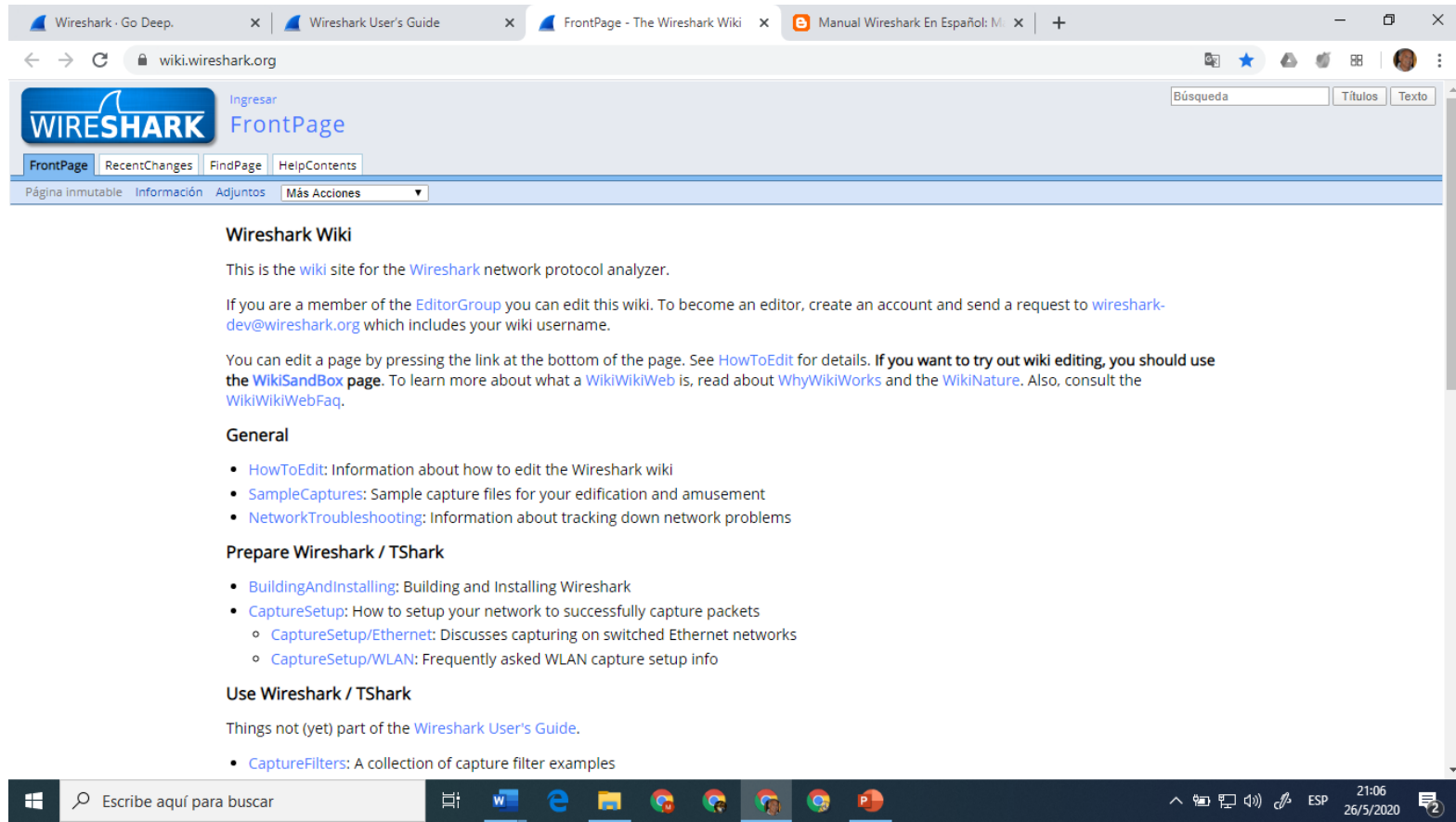
<https://www.youtube.com/watch?v=Y5rZImmQVQk&t=663s>

The screenshot shows a YouTube video player with the following details:

- Video Title:** Video 1 Curso wireshark en español
- Views:** 300.715 visualizaciones
- Date:** 31 mar. 2014
- Engagement:** 1844 likes, 97 comments
- Actions:** COMPARTIR, GUARDAR, and a menu icon (three dots).
- Next Video:** Siguiendo: Analizando tráfico con Wireshark (INCIBE)
- Video Content:** The video displays the Wireshark 1.6.7 interface. The main window is titled "The Wireshark Network Analyzer [Wireshark 1.6.7]". It features a sidebar on the left with icons for various functions. The main area is divided into three columns:
 - Capture:** Includes "Interface List" (Live list of the capture interfaces), "Start capture on interface:" (with options like eth0, wlan1, Pseudo-device, and lo), "Capture Options" (Start a capture with detailed options), "Capture Help", "How to Capture" (Step by step to a successful capture setup), and "Network Media" (Specific information for capturing on: Ethernet, WLAN, ...).
 - Files:** Includes "Open" (Open a previously captured file), "Open Recent:" (listing /home/roberknight/primer-captura [not found]), and "Sample Captures" (A rich assortment of example capture files on the wiki).
 - Online:** Includes "Website" (Visit the project's website), "User's Guide" (The User's Guide [online version]), and "Security" (Work with Wireshark as securely as possible).

Enlaces de interés

<https://wiki.wireshark.org/>



The screenshot shows a web browser window with the Wireshark Wiki homepage. The browser has four tabs: 'Wireshark - Go Deep.', 'Wireshark User's Guide', 'FrontPage - The Wireshark Wiki', and 'Manual Wireshark En Español: M...'. The address bar shows 'wiki.wireshark.org'. The page features the Wireshark logo and a navigation bar with links: 'FrontPage', 'RecentChanges', 'FindPage', and 'HelpContents'. Below the navigation bar is a search bar with the text 'Búsqueda' and two buttons: 'Títulos' and 'Texto'. The main content area is titled 'Wireshark Wiki' and contains the following text:

This is the [wiki](#) site for the [Wireshark](#) network protocol analyzer.

If you are a member of the [EditorGroup](#) you can edit this wiki. To become an editor, create an account and send a request to wireshark-dev@wireshark.org which includes your wiki username.

You can edit a page by pressing the link at the bottom of the page. See [HowToEdit](#) for details. If you want to try out wiki editing, you should use the [WikiSandBox](#) page. To learn more about what a [WikiWikiWeb](#) is, read about [WhyWikiWorks](#) and the [WikiNature](#). Also, consult the [WikiWikiWebFaq](#).

General

- [HowToEdit](#): Information about how to edit the Wireshark wiki
- [SampleCaptures](#): Sample capture files for your edification and amusement
- [NetworkTroubleshooting](#): Information about tracking down network problems

Prepare Wireshark / TShark

- [BuildingAndInstalling](#): Building and installing Wireshark
- [CaptureSetup](#): How to setup your network to successfully capture packets
 - [CaptureSetup/Ethernet](#): Discusses capturing on switched Ethernet networks
 - [CaptureSetup/WLAN](#): Frequently asked WLAN capture setup info

Use Wireshark / TShark

Things not (yet) part of the [Wireshark User's Guide](#).

- [CaptureFilters](#): A collection of capture filter examples

The Windows taskbar at the bottom shows the Start button, a search bar with the text 'Escribe aquí para buscar', and several application icons including Word, Edge, File Explorer, and Chrome. The system tray on the right shows the time as 21:06 and the date as 26/5/2020.