Wireshark para novatos - Español

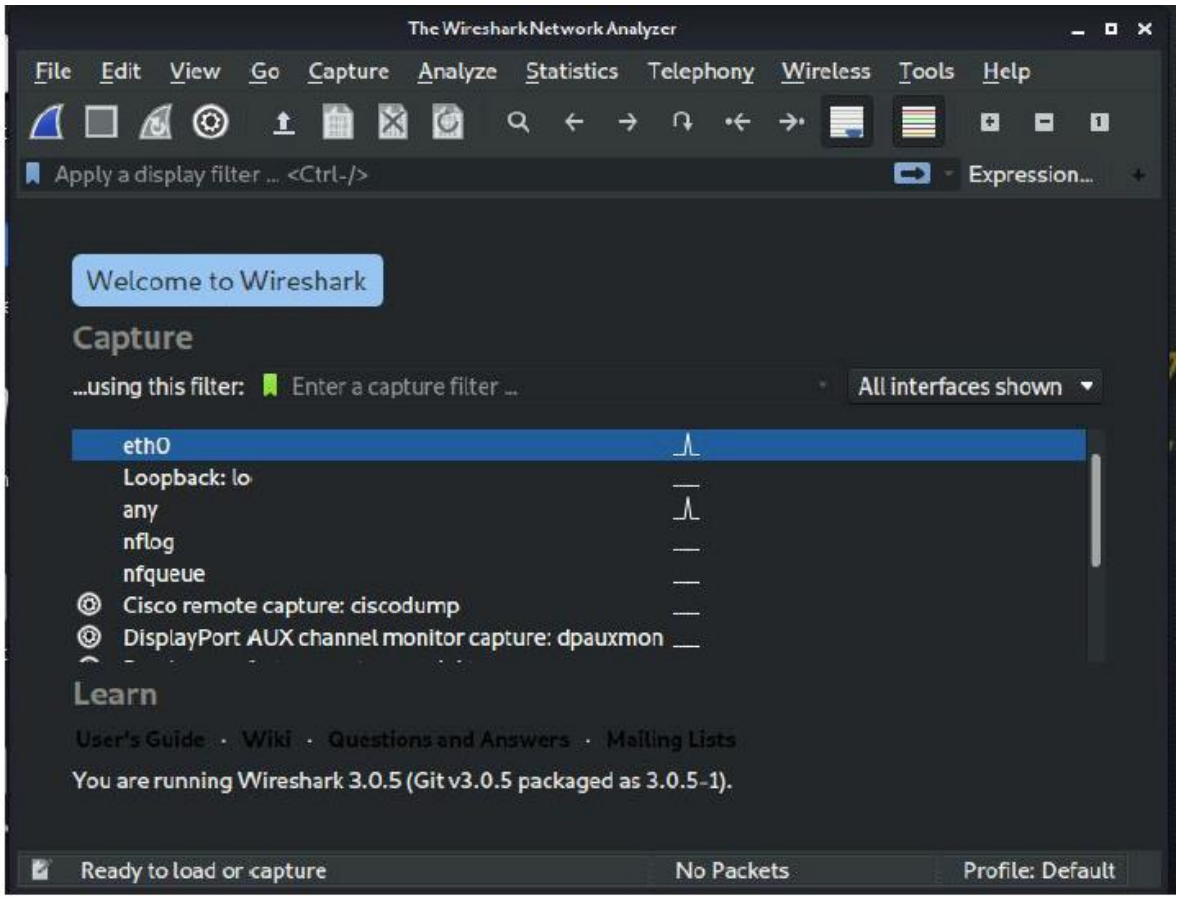
Wireshark para novatos Por Anmol K Sachan

anmol221999@gmail.com
Linkedin: https://linkedin.com/in/anmolksachan/ Ig:
https://instagram.com/the_guy_that_hacks

Traducción por: Carla Cortés y Luis Rodríguez

ÍNDICE

1. Comenzando con Wireshark

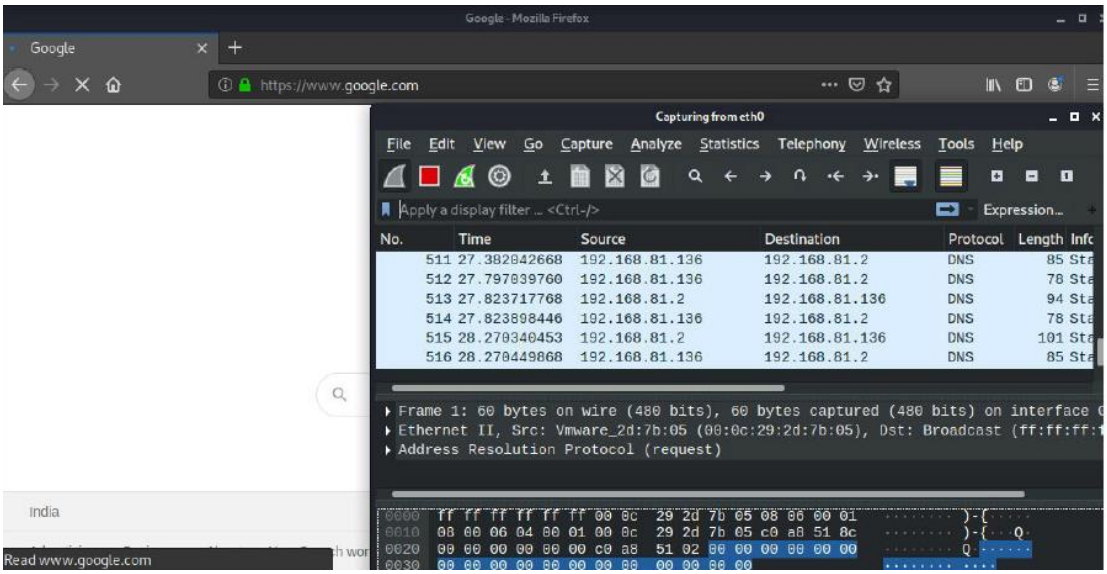


Wireshark está preinstalado en kali linux.

Wireshark es un analizador de paquetes gratuito y de código abierto. Se utiliza para la resolución de problemas de red, el análisis, el desarrollo de software y protocolos de comunicación, y la educación. Originalmente llamado Ethereal, el proyecto fue rebautizado como Wireshark en mayo de 2006 debido a problemas de marca.

La **GUI de wireshark** tiene

1. Barra de título
2. Menú principal
3. Barra de herramientas principal
4. Barra de herramientas del filtro
5. Lista de paquetes
6. Barra de desplazamiento inteligente
7. Detalles del paquete
8. Packet Bytes
9. Barra de estado



Haciendo clic en la interfaz eth0 se inicia la captura de paquetes, mientras que el **sniffing** podemos **analizar** y puede aplicar **filtros** para ver la necesidad exacta.

Definir las **cuatro capas del** modelo de referencia **TCP/IP**.

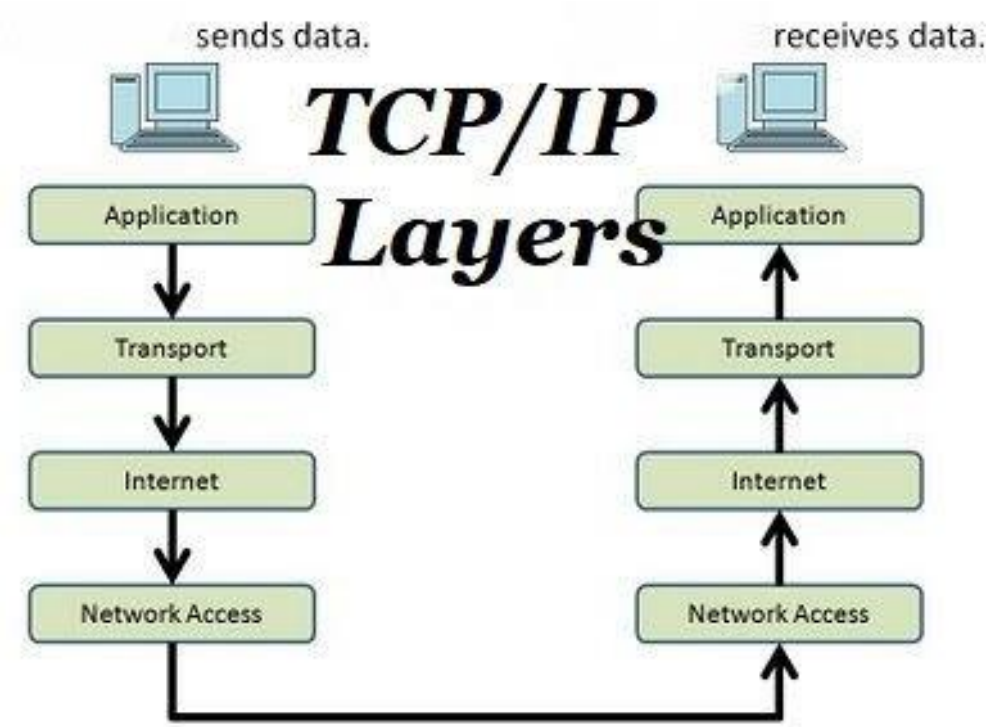
La capa TCP maneja el mensaje que se va a transmitir. Este mensaje se suele dividir en pequeñas unidades. Estas pequeñas unidades se conocen como paquetes. Además, estos paquetes se transmiten por la red.

Estos paquetes son recibidos por la capa TCP correspondiente en el receptor y reensamblados en el mensaje original.

El modelo TCP/IP tiene 4 capas, que son:

- Capa de aplicación
- Capa de transporte
- Capa de Internet

  Capa de red



Capa de aplicación:

La primera capa es la de aplicación. Esta capa proporciona a las aplicaciones un intercambio de datos estandarizado. A continuación se indican los protocolos de estas capas:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo de transferencia de archivos (FTP)
- Protocolo de oficina de correos 3 (POP3)
- Protocolo simple de transferencia de correo (SMTP)
- Protocolo simple de gestión de redes (SNMP)

Este trabajo en capas con todos estos protocolos.

Capa de transporte:

La capa de transporte es la segunda capa del modelo TCP/IP. El trabajo básico de la capa de transporte es mantener las comunicaciones de extremo a extremo. A continuación se indican los protocolos de estas capas:

- TCP
- Protocolo de Datagramas de Usuario (UDP)

Estos dos protocolos se utilizan para la capa de transporte en TCP/IP.

Capa de red:

La tercera capa de TCP IP es una capa de red. También se conoce como capa de Internet. La capa de red se ocupa de los paquetes. Los siguientes son los protocolos que se utilizan en esta capa.

- IP
- Protocolo de mensajes de control de Internet (ICMP) Capa física

La última capa es la capa física. Esta capa trabaja con los siguientes protocolos.

- Ethernet para LAN (redes de área local)
- Protocolo de resolución de direcciones (ARP)

Examinar **los datos de la cabecera del paquete** con Wireshark

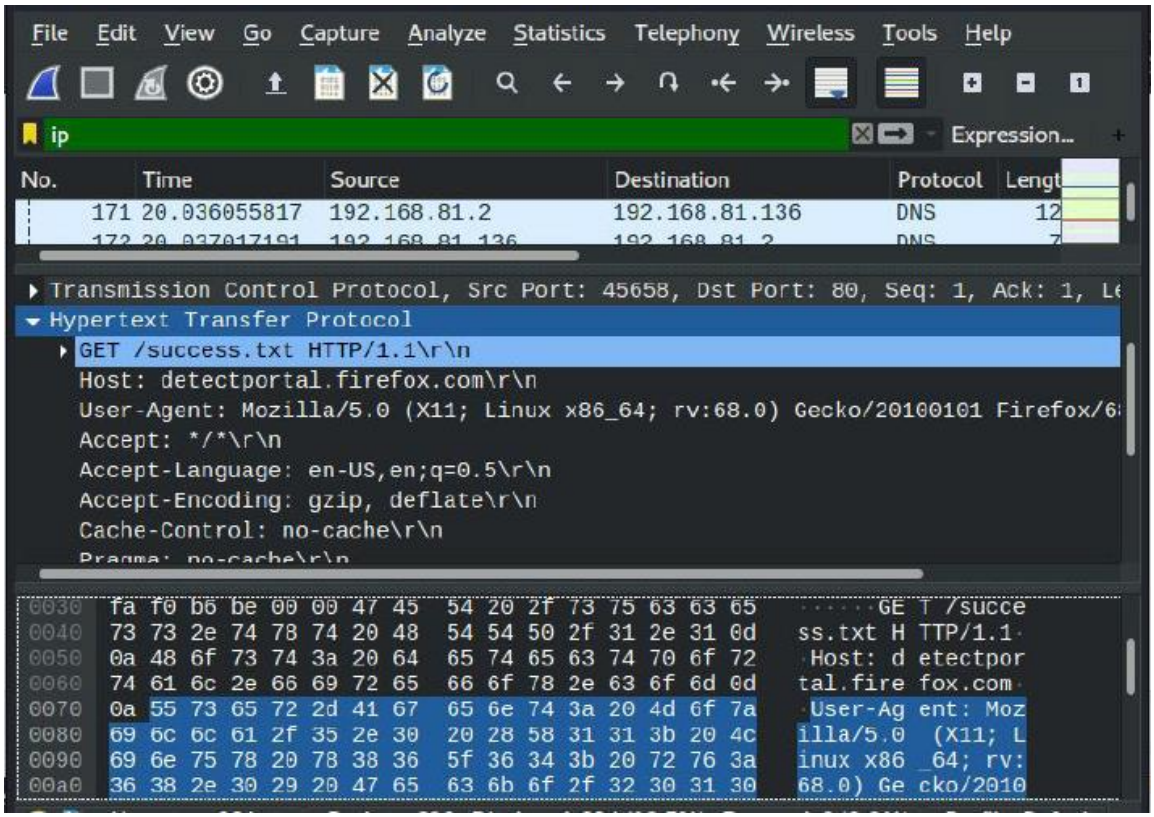
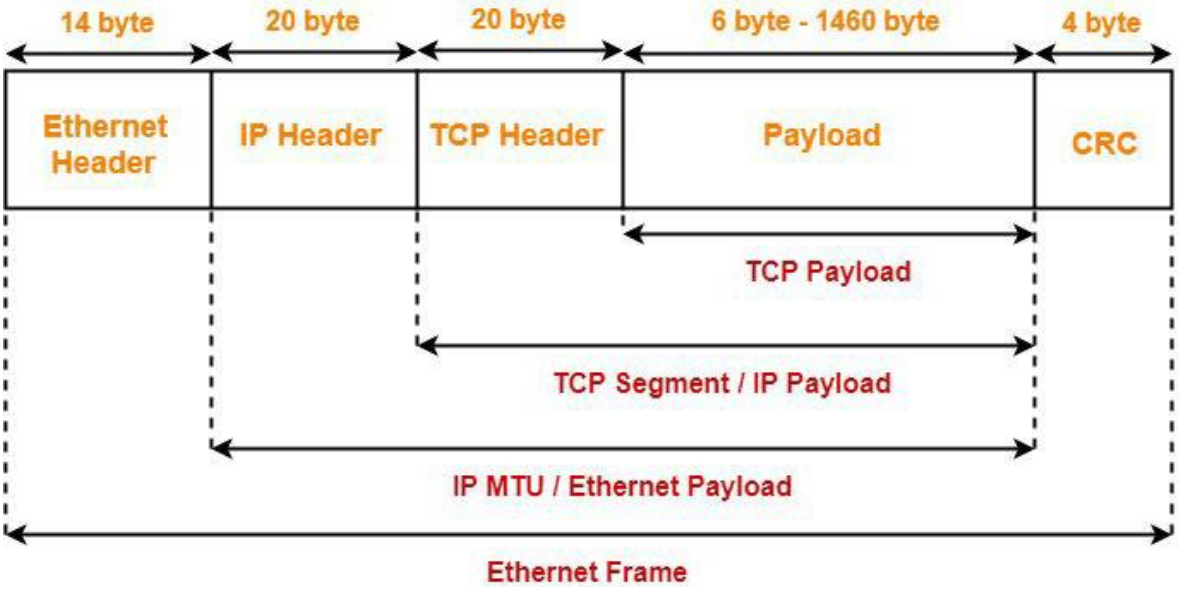
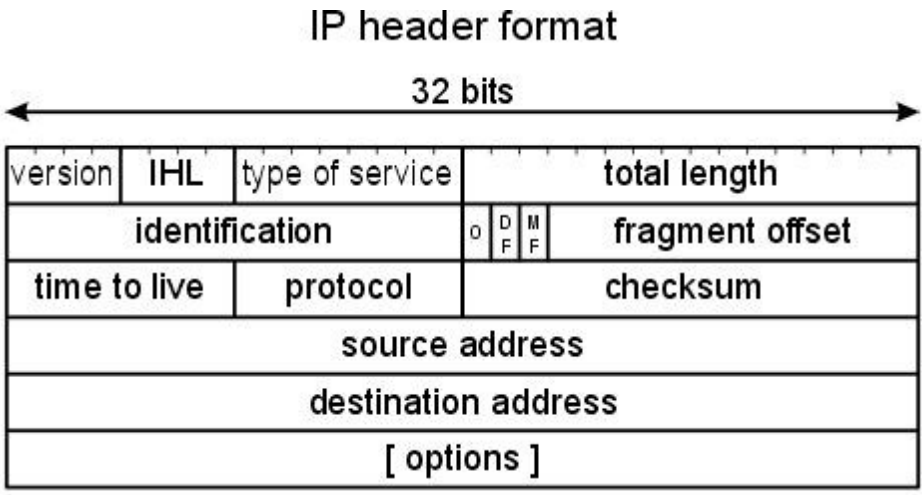


Imagen. Encabezados de los paquetes de datos mostrados arriba

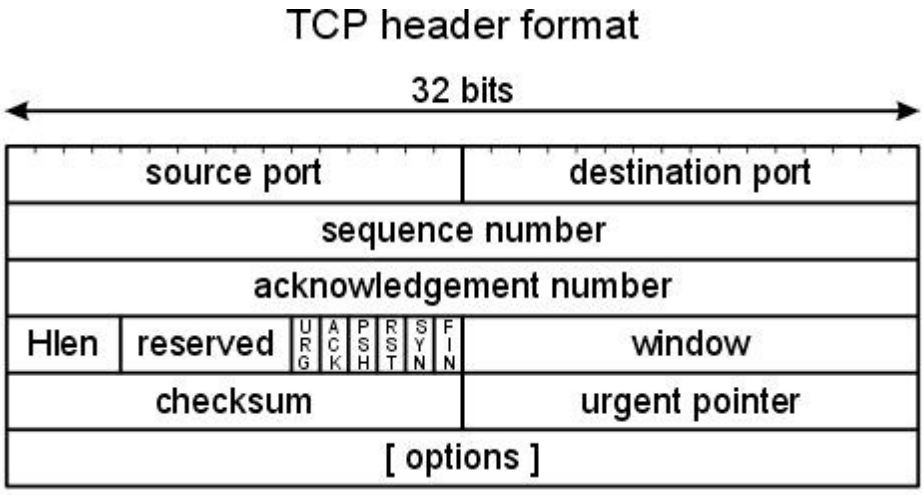
Definir los **campos de cabecera** de las **tramas Ethernet**, del **Protocolo de Internet** (IP), **del Protocolo de Control de Transporte** (TCP) y **del Protocolo de Datagramas de Usuario** (UDP) / diferentes tipos de cabeceras de paquetes, incluyendo los campos de cabecera y sus valores.



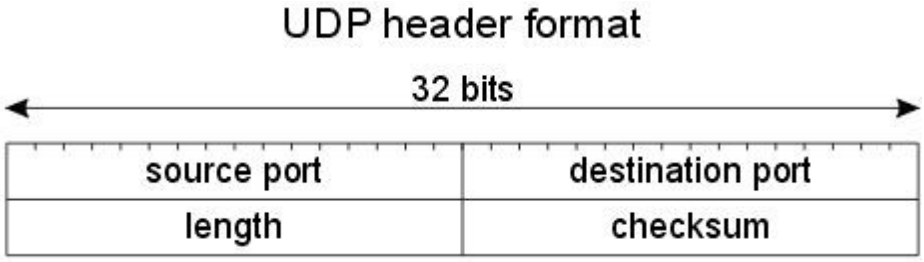
Ethernet



Protocolo IP



Cabecera TCP



Cabecera UDP

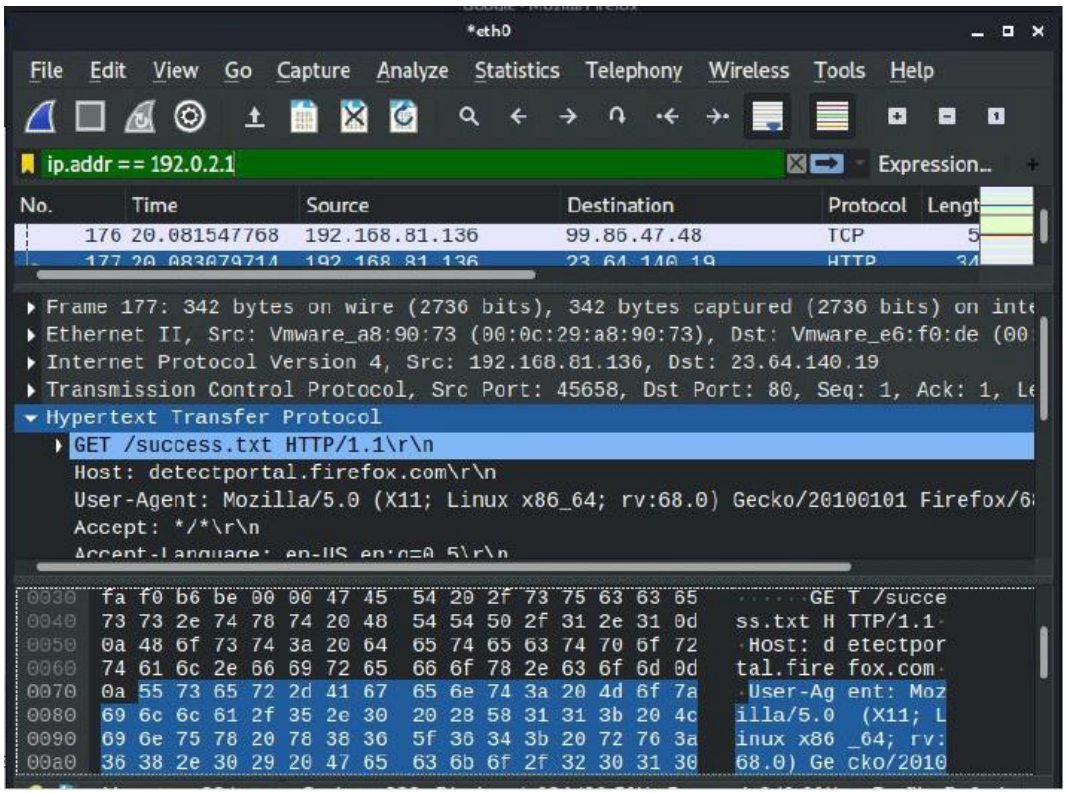
Compare y contraste **TCP** y **UDP**.

Differences are-

Properties	TCP	UDP
Header	Dynamic header (20 – 60 B)	Static header of 8 Bytes
Max segment	any size or 2^30 B	short message 65536 Bytes
Flow Control	Yes, Window and seq. no.	NO
Checksum	Compulsory	Optional
Connection nature	TCP+ IP = connection oriented	UDP+ IP= connection less
Error control	Own mechanism	Depends on ICMP (No self feature)
Support multicast	NO	YES
Support broadcast	NO	Yes
Examples service	HTTP,SMTP,FTP,TELNET	TFTP,DNS,SNMP

2. Empezar el análisis: Realice una captura en vivo del tráfico de red/tráfico web

2.1 Filtrar los paquetes con la barra de filtros durante la captura y explicar todos los posibles filtros utilizados por usted.



Capturar sólo el tráfico hacia o desde la dirección IP
172.18.5.4: host 172.18.5.4

Capturar el tráfico hacia o desde un rango de direcciones IP:
192.168.0.0/24 o 192.168.0.0 máscara 255.255.255.0

Capturar el tráfico de un rango de direcciones IP:
192.168.0.0/24 o 192.168.0.0 máscara de red 255.255.255.0

Capturar el tráfico hacia un rango de direcciones IP:
192.168.0.0/24 o 192.168.0.0 máscara de red 255.255.255.0

Capturar sólo el tráfico DNS (puerto 53): puerto 53

Capture el tráfico no HTTP y no SMTP en su servidor (ambos son equivalentes):

host www.example.com y no (puerto 80 o puerto 25)
host www.example.com y no puerto 80 y no puerto 25

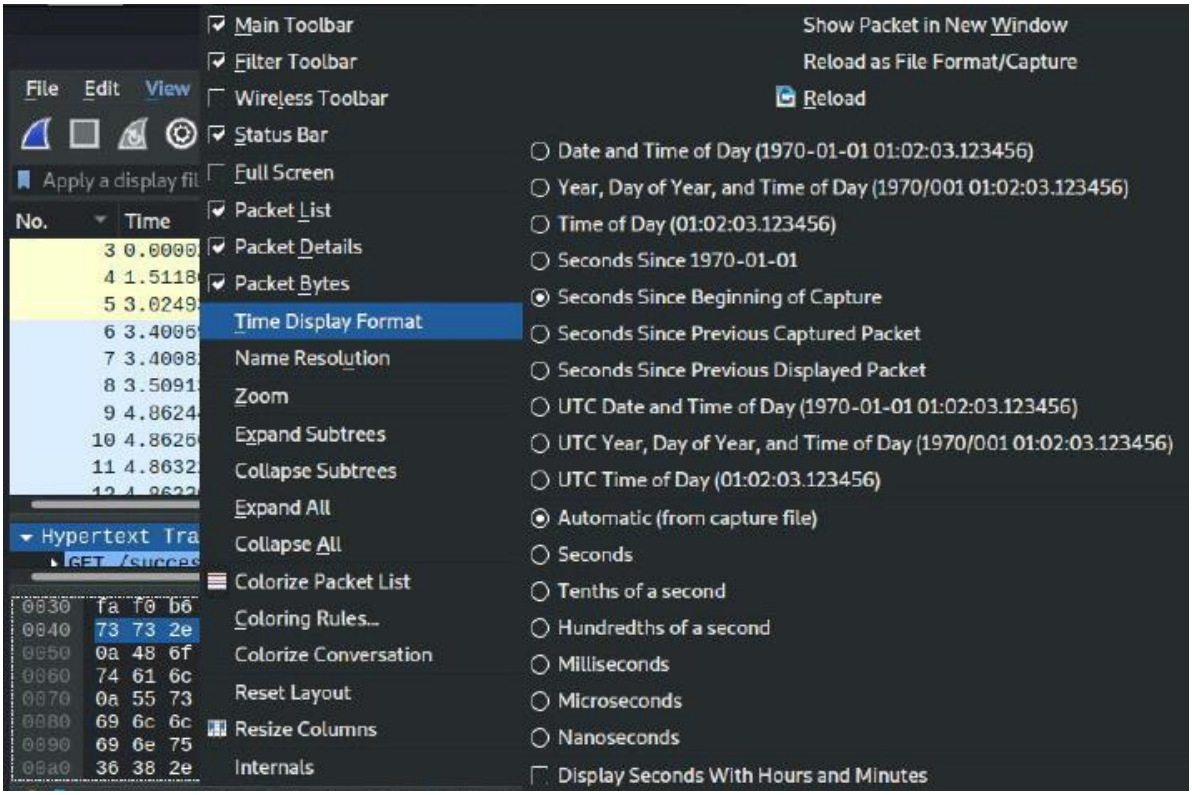
Captura excepto todo el tráfico ARP y DNS: puerto no 53 y no arp

Para capturar el tráfico de la vlan

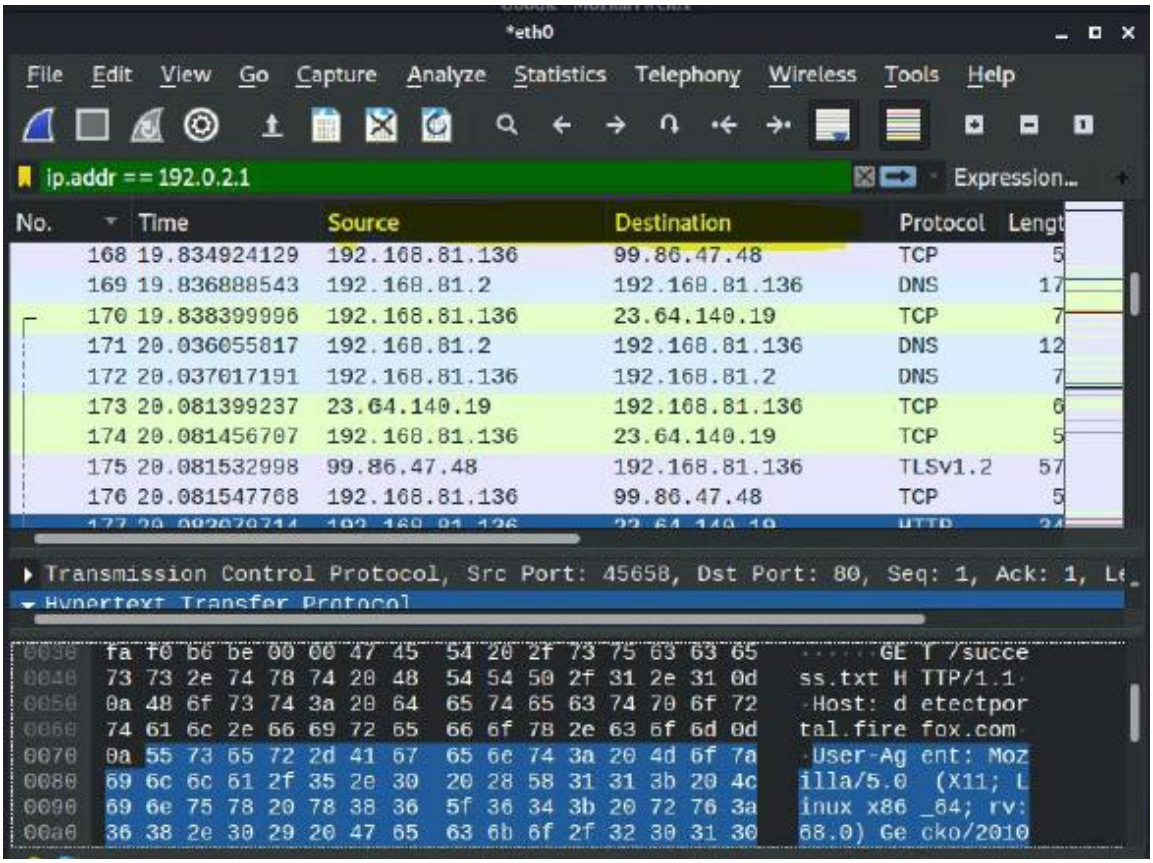
3. Ver los resúmenes de los paquetes con la ventana de la lista de paquetes

No.	Time	Source	Destination	Protocol	Lengt
3	0.000020180	192.168.81.140	192.168.81.2	NBNS	11
4	1.511808997	192.168.81.140	192.168.81.2	NBNS	11
5	3.024931189	192.168.81.140	192.168.81.2	NBNS	11
6	3.400696460	192.168.81.136	192.168.81.2	DNS	8
7	3.400823404	192.168.81.136	192.168.81.2	DNS	8
8	3.509137922	192.168.81.2	192.168.81.136	DNS	24
9	4.862447872	192.168.81.136	192.168.81.2	DNS	7
10	4.862660426	192.168.81.136	192.168.81.2	DNS	7
11	4.863220065	192.168.81.136	192.168.81.2	DNS	7
12	4.863306621	192.168.81.136	192.168.81.2	DNS	7

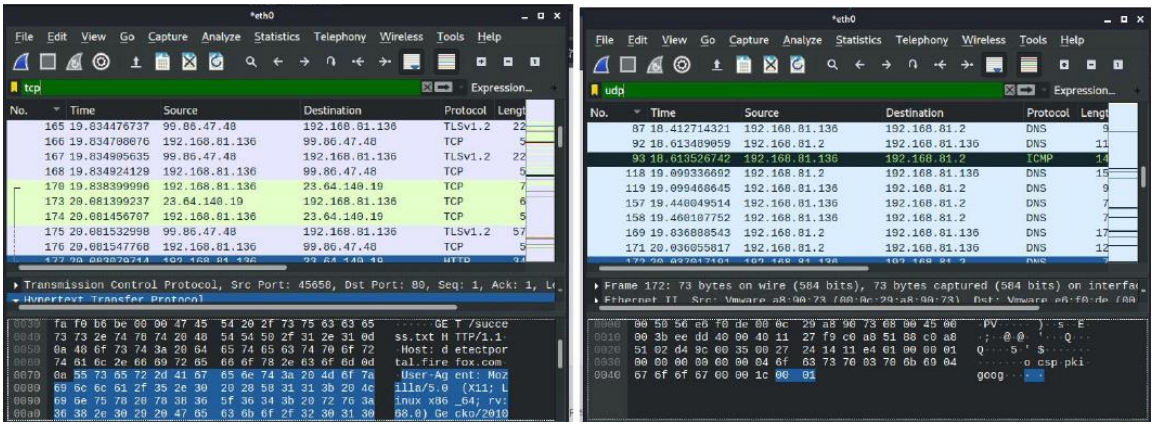
Número de paquete (No.): Los números de cada paquete comienzan con 1 para el primer paquete.

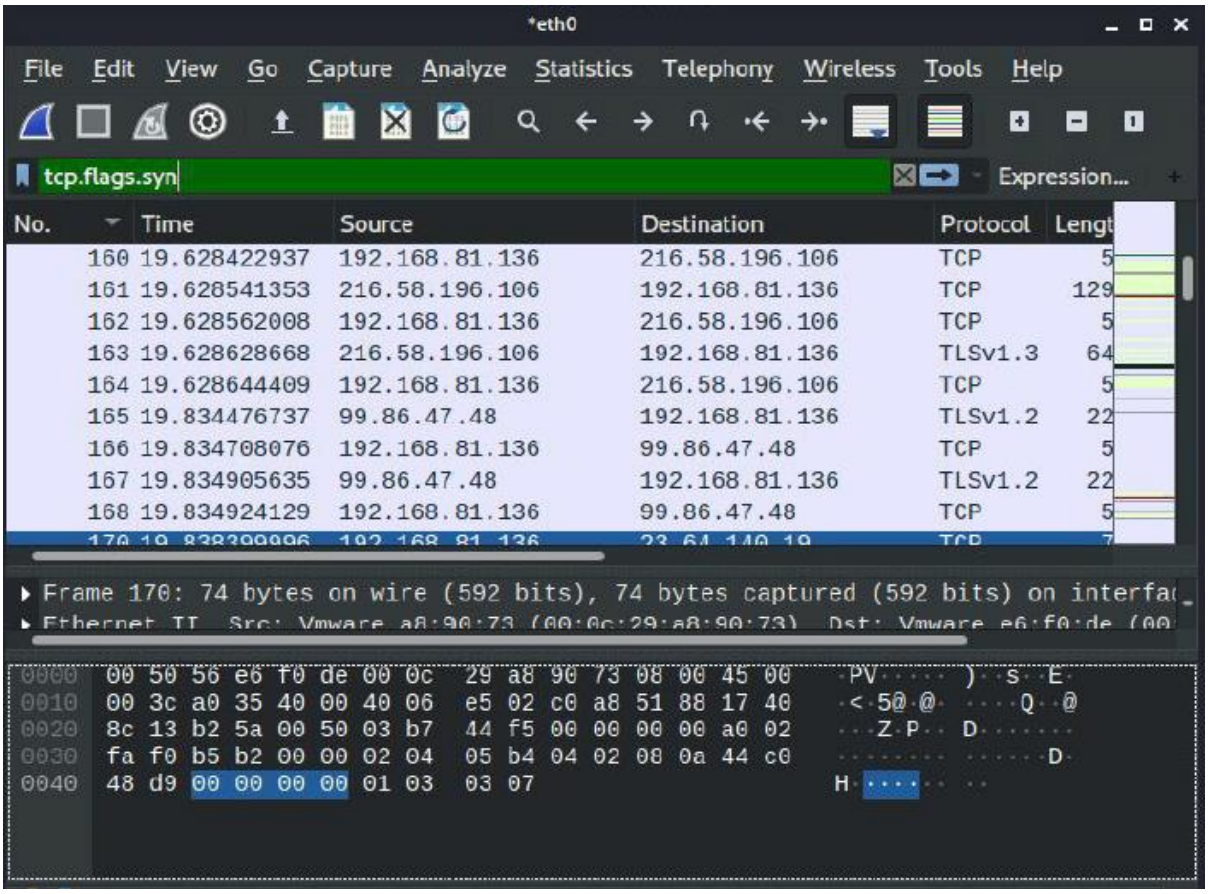


Timestamp (Time): Por defecto es el número de segundos desde el inicio de la captura



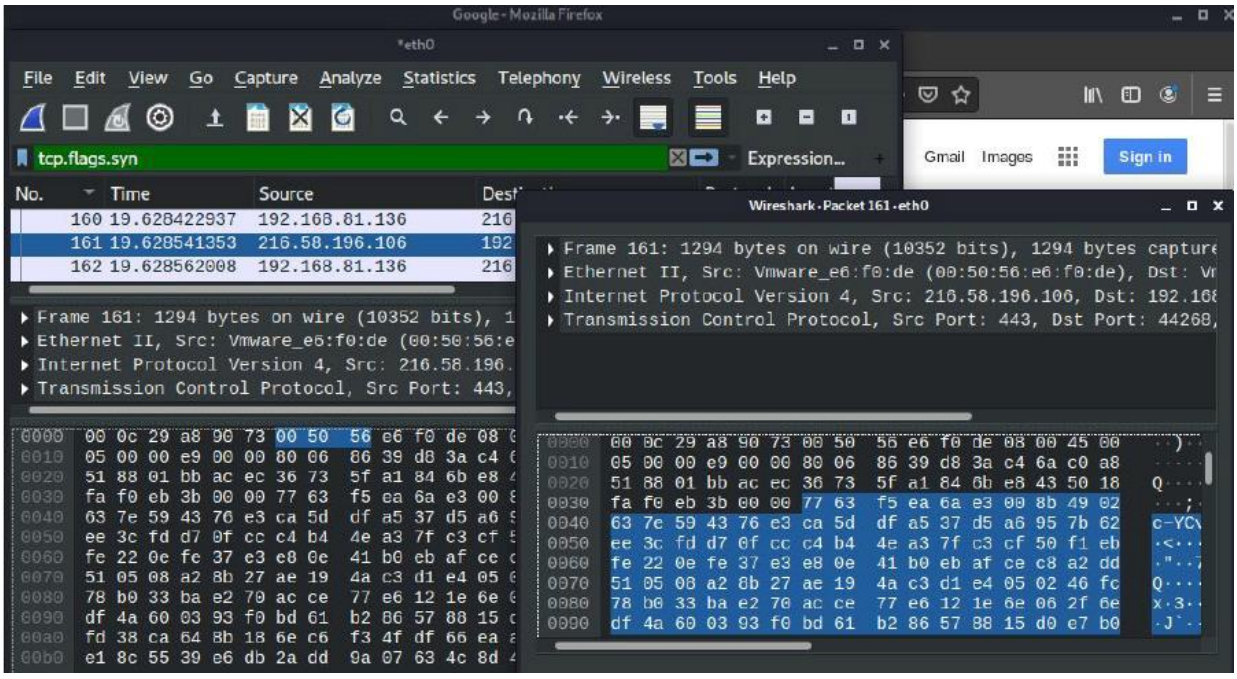
Direcciones IP (Origen: Source, Destino: Destination): La dirección de origen y destino del paquete.



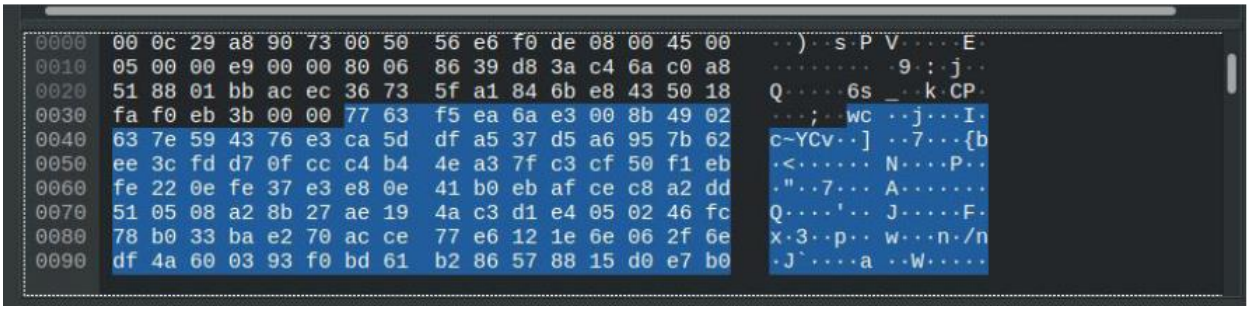


Información adicional del protocolo (info): Ejemplo: para un paquete TCP, este campo indica si es un paquete SYN, ACK o FIN.

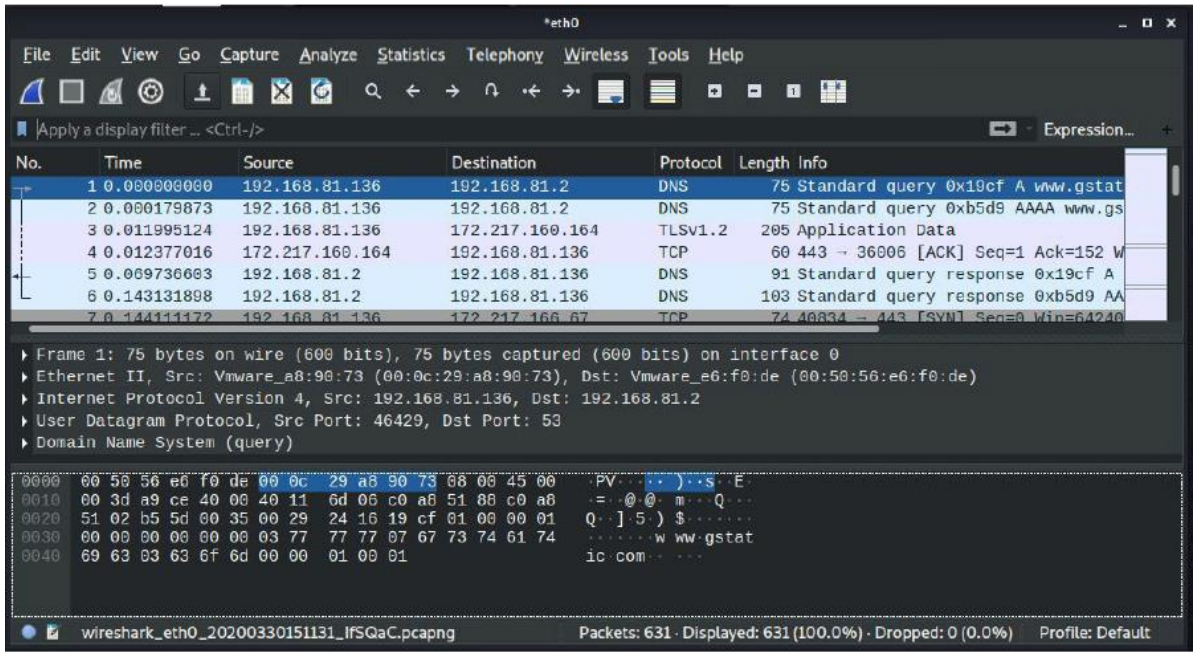
4. Estudiar los detalles del paquete con la ventana de detalles del paquete



5. Ver los datos de los paquetes con la ventana de bytes de paquetes individuales

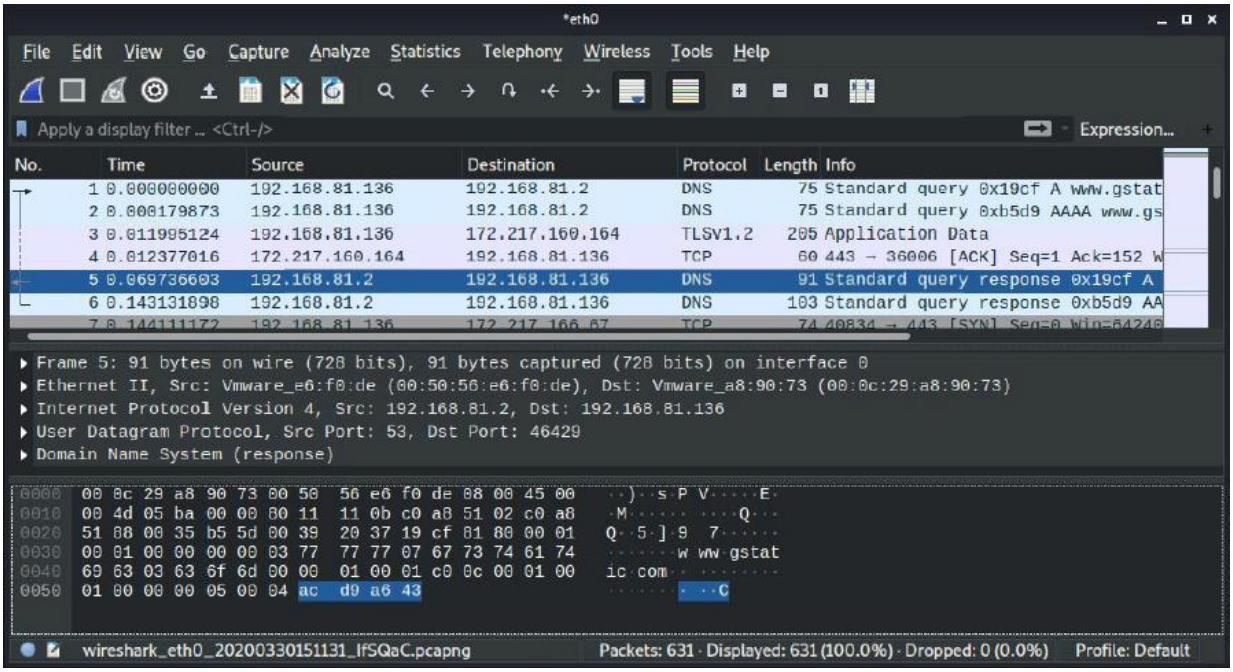


6. Simplemente navegar por Internet



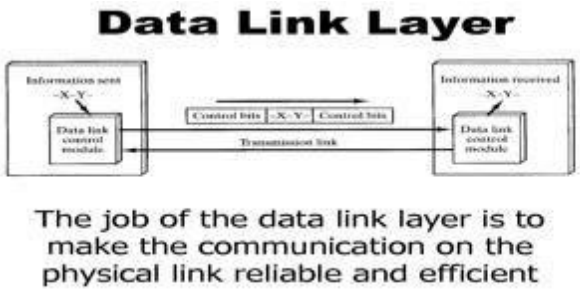
Datos después de navegar por Internet

7. Visualización de los datos de la cabecera del paquete

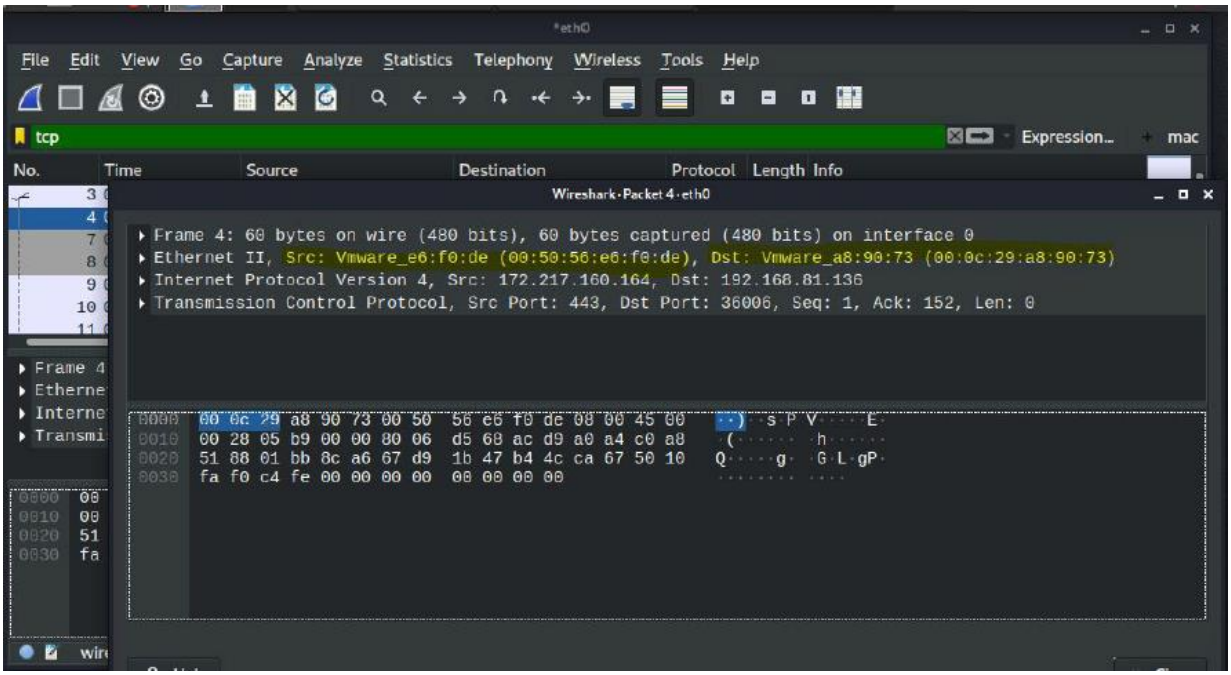


7.1 Captura de paquetes con Wireshark

7.2. Explorar la capa de interfaz de red / capa de enlace de datos



7.2.2. Ver datos de tramas Ethernet capturados con Wireshark

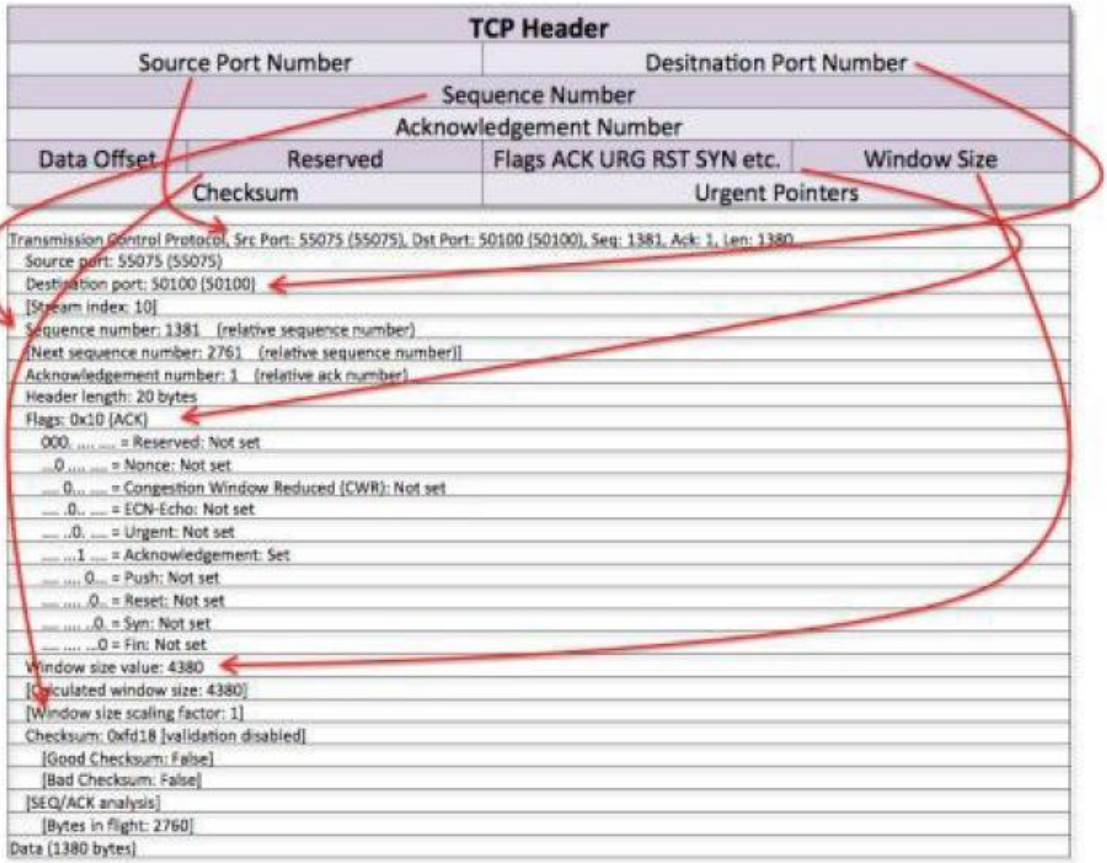


8.1 Exploración de la capa de Internet

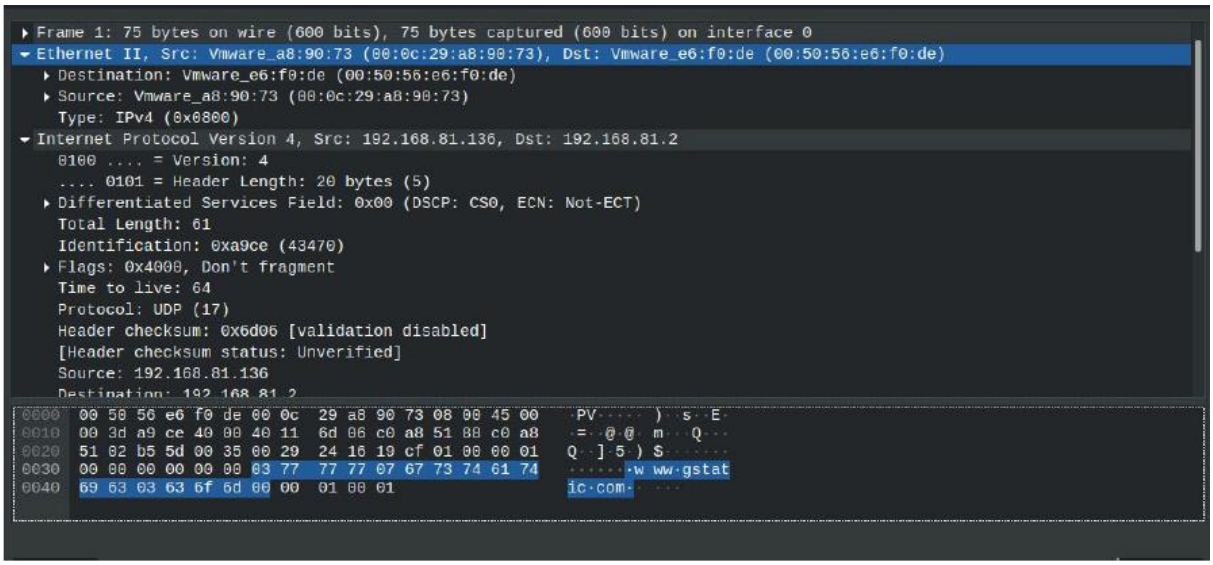
8.1.1. Cabecera IPv4: En la imagen de abajo

Version = 4	HL	Type Of service	Total Length	
Identification			Flag	Fragment offset
Time to Live		Protocol	Header Checksum	
Home Address : home agent address 130.45.10.20/16				
Destination Address : 14.56.8.9/8				
Protocol	S	Reserved	Header Checksum	
Destination Address mobile host home address130.45.6.7/16				
Source Address (remote host) 200.4.7.14/24				
Payload				

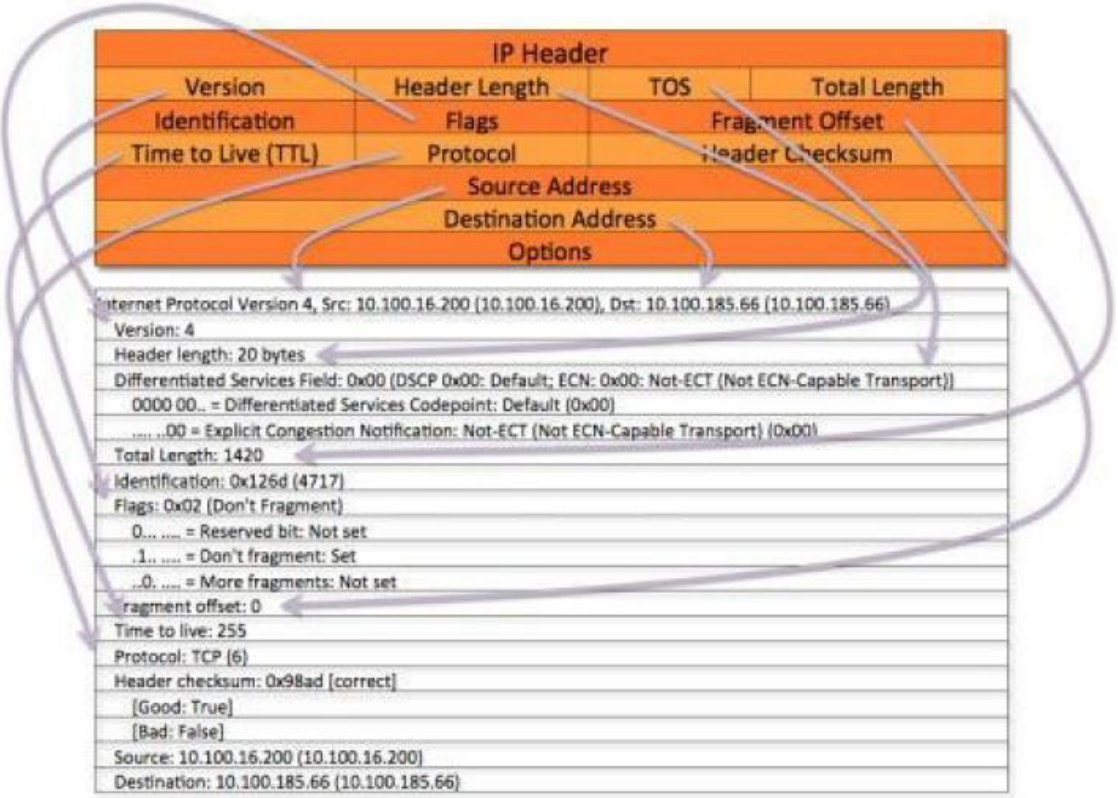
8.1.2. Ver los datos de la cabecera IP de un paquete TCP capturado con Wireshark



8.1.3 Ver los datos de la cabecera IP de un paquete UDP

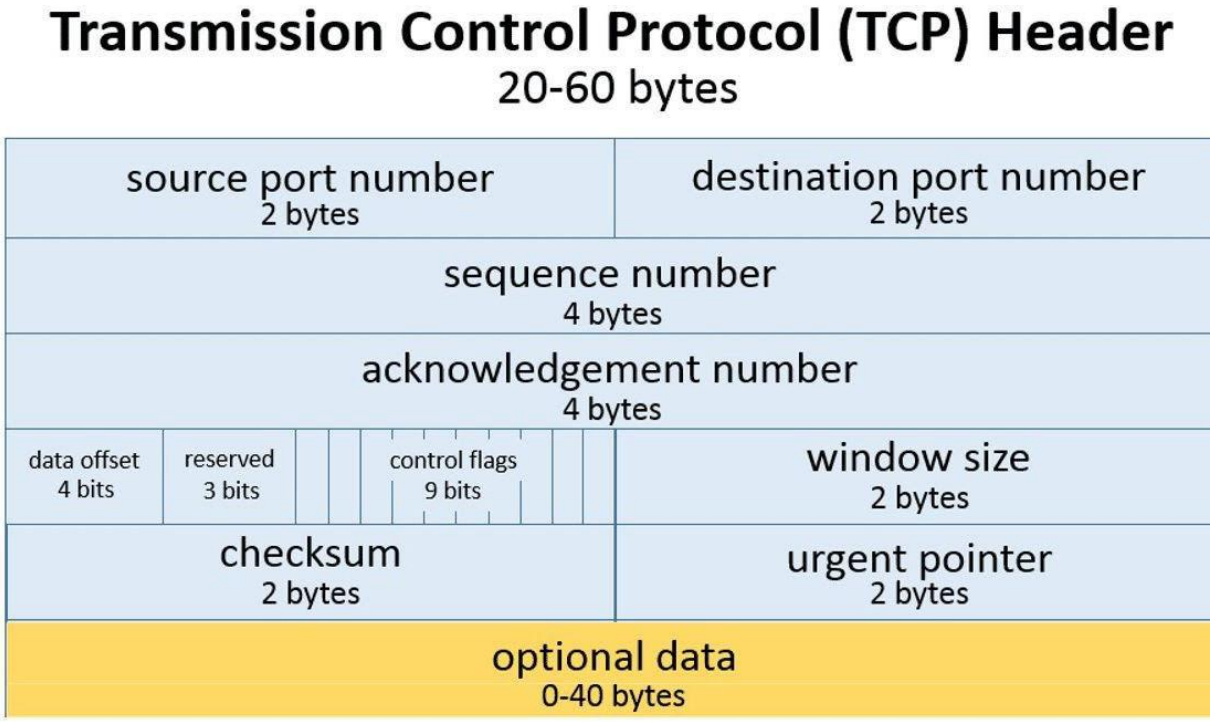


8.1.4. Ver los datos de la cabecera IP de un paquete ARP

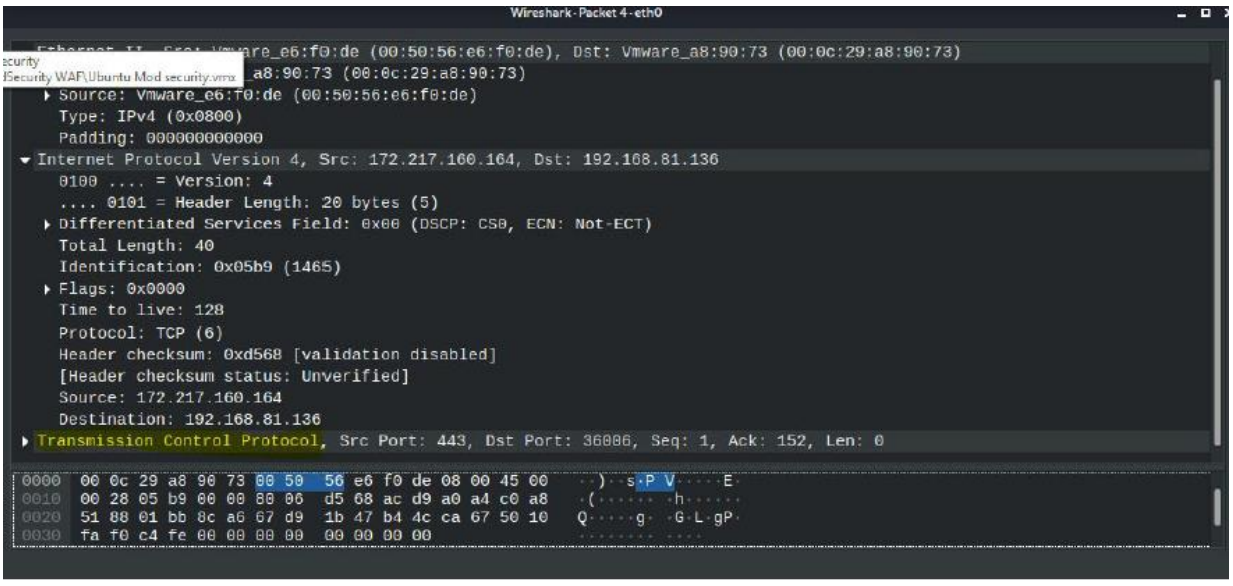


9 Exploración de la capa de transporte

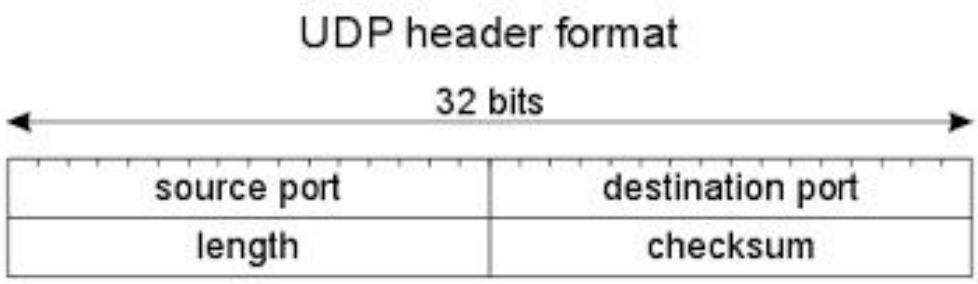
9.1.1. Cabecera TCP: Imagen de abajo



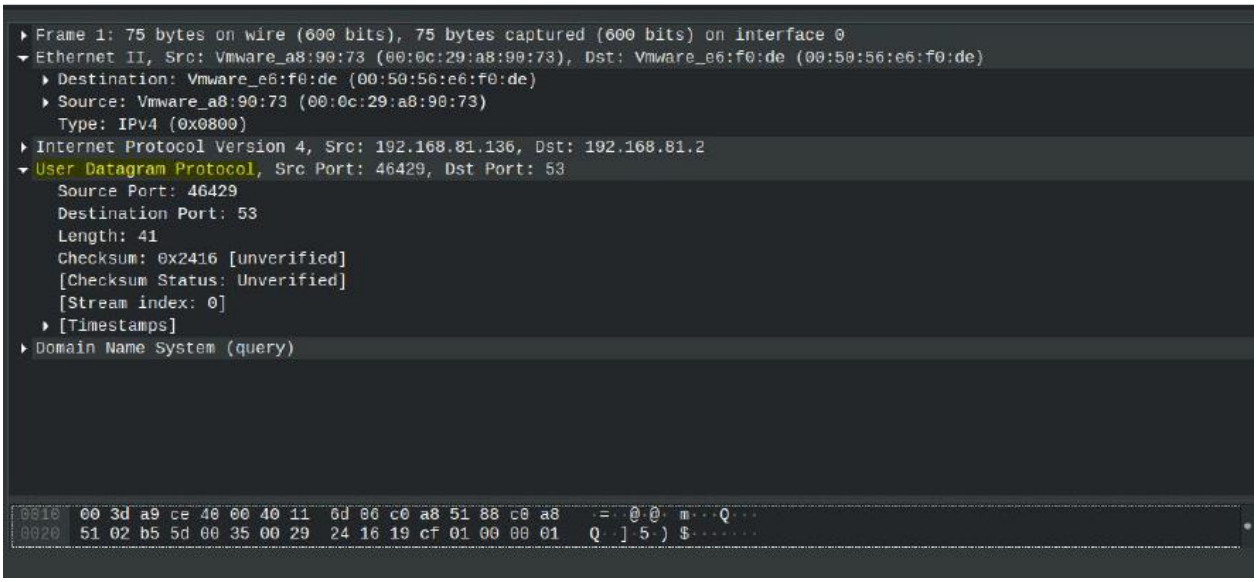
9.1.2 Ver los datos de la cabecera TCP de un paquete TCP capturado con Wireshark



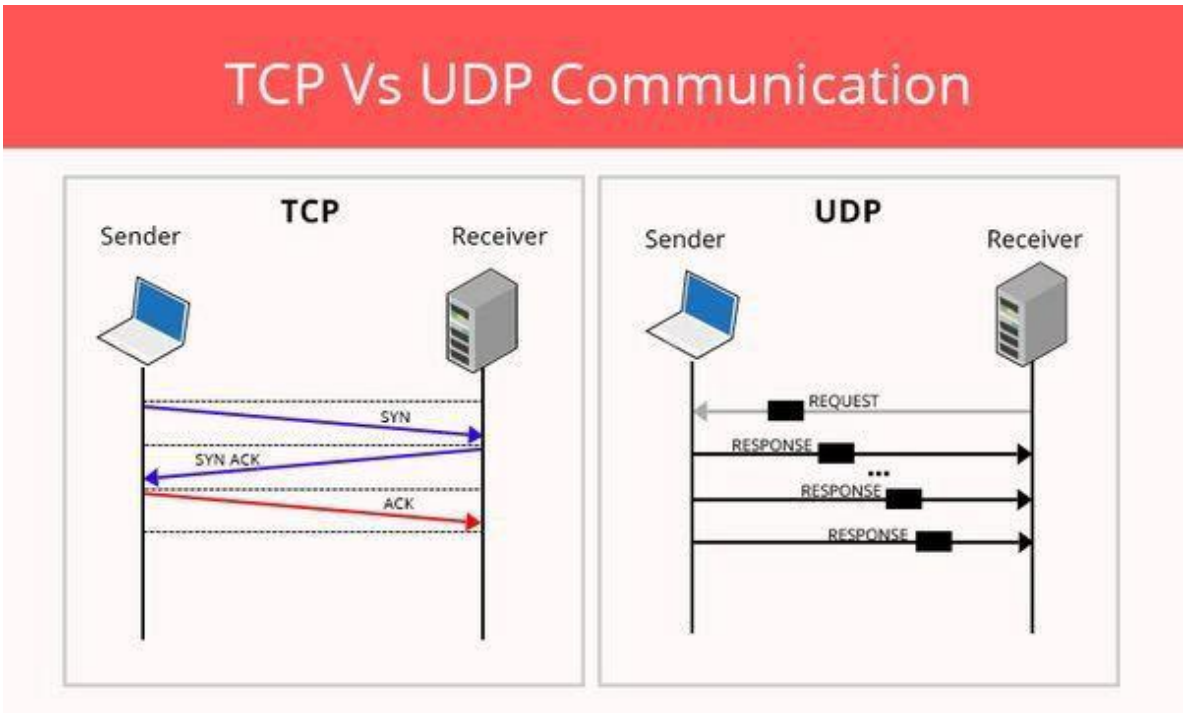
9.1.3 Cabecera UDP: En la imagen de abajo



9.1.4 Ver los datos de la cabecera UDP de un paquete UDP capturado con Wireshark

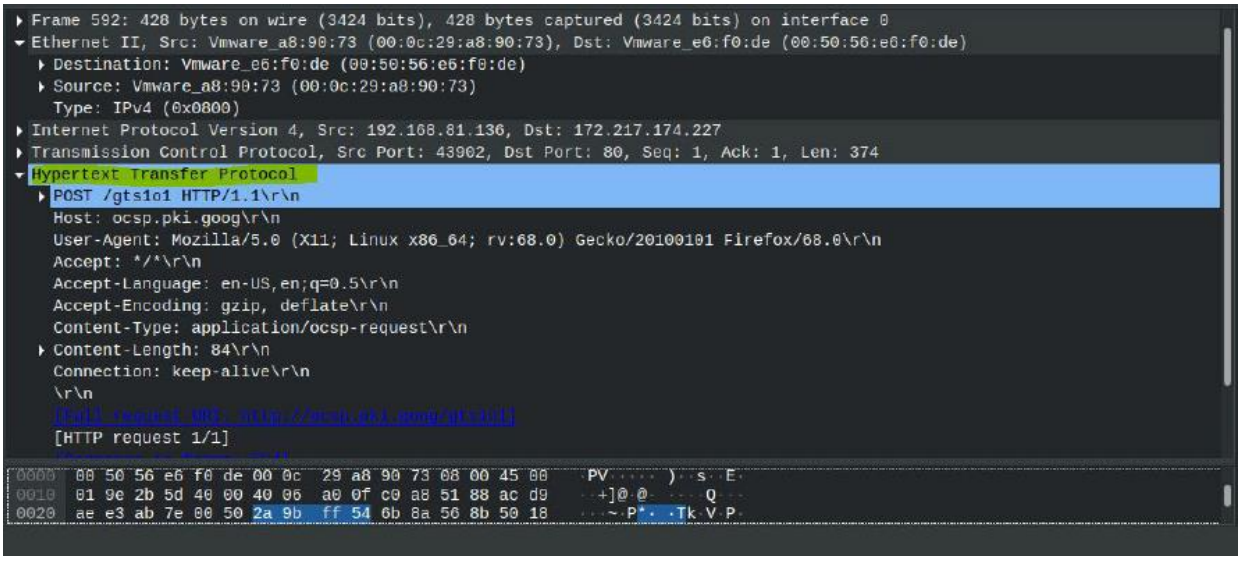


9.1.5 Comparar y contrastar IP, TCP y UDP

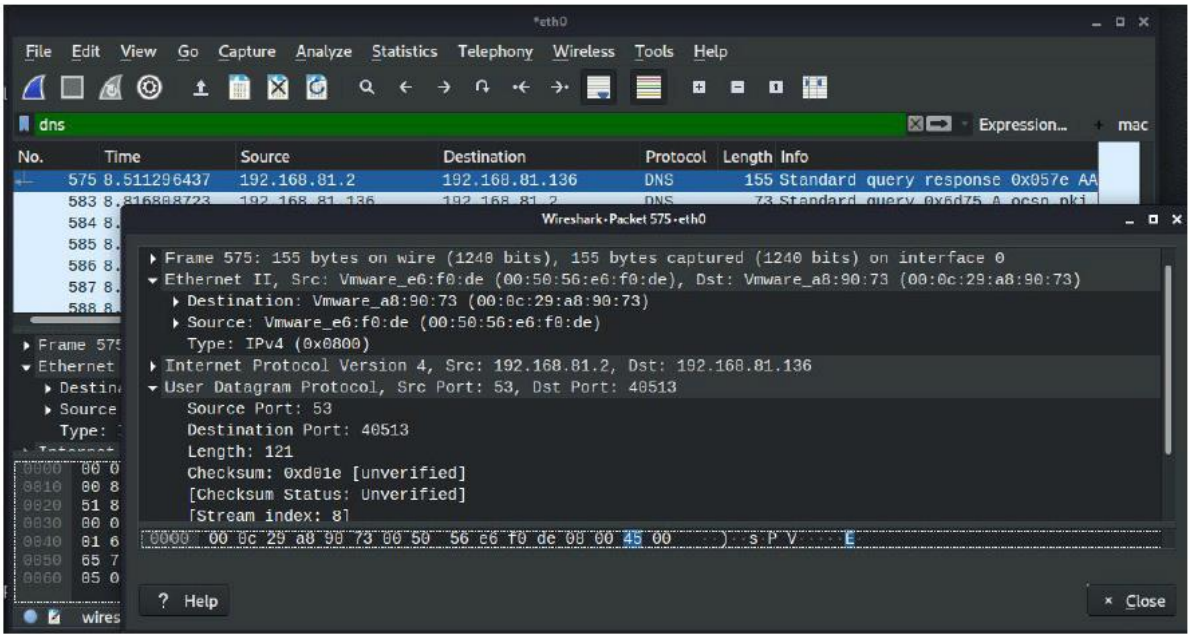


10. Explorar la capa de aplicación

10.1.1 Analizar un paquete HTTP



10.1.2 Analizar un paquete DNS



11. Preguntas comunes

Que. 1. ¿Captura Wireshark todo el tráfico de Internet? Si es así, explica por qué. Si no es así, ¿qué tráfico captura?

Respuesta: Lo más probable es que sólo vea el tráfico en el que participa su máquina, o que se difunde a todas las máquinas.

Esto se debe a que, durante años, la mayoría de las redes LAN se han construido sobre la base de la tecnología Ethernet conmutada, a diferencia de las redes basadas en concentradores o en buses. En esas tecnologías más antiguas, todos los equipos de la LAN veían todo el tráfico, simplemente porque todos estaban conectados eléctricamente entre sí. Con Ethernet conmutada, el conmutador decide qué paquetes enviar a cada puerto. Esto hace que la red sea más rápida y ligeramente más segura.
(La Ethernet conmutada no es una muy buena medida de seguridad, porque es fácil de derrotar con el envenenamiento ARP).
Ahora bien, es posible que todavía estés en una Ethernet basada en un hub, o algo similar. Eso sólo puede ocurrir con redes de 100 Mbit/s y más lentas. Parte de la especificación de Gigabit Ethernet es un requisito para los conmutadores. No encontrarás un concentrador GigE.

También hay que tener en cuenta que las redes inalámbricas se comportan efectivamente como las LAN de antaño: todos los equipos conectados a una determinada red Wi-Fi pueden ver todo el tráfico, debido puramente a la naturaleza de la comunicación por radio.
Si estás en una LAN cableada con switches gestionados y tienes acceso administrativo a esos switches, probablemente encontrarás una característica que puedes activar en ellos llamada port mirroring. Esa característica existe específicamente para restaurar el antiguo comportamiento de la LAN preconmutada: designa un puerto como especial, dirigiendo copias de todo el tráfico hacia él, incluso los paquetes que no están dirigidos a las direcciones MAC conectadas a ese puerto.

Que. 2. Escriba los filtros de Wireshark para: Ver el tráfico UDP cuando se realiza la exploración.

Respuesta: simplemente escriba UDP y presione enter, y podrá ver todos los paquetes udp que fueron capturados.

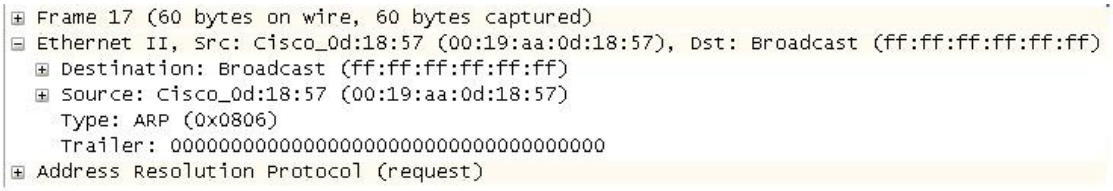
Que. 3. Vea el tráfico ICMP de cualquier dirección.

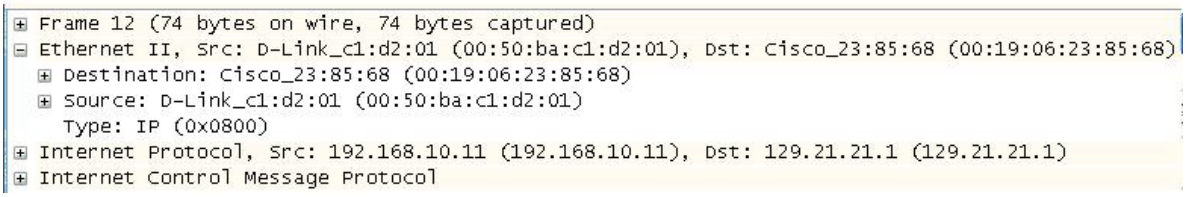
Respuesta: Para analizar el tráfico ICMP Echo Request:
1. Observe el tráfico capturado en el panel superior de la lista de paquetes de Wireshark. Busque el tráfico con ICMP como protocolo. Para ver sólo el tráfico ICMP, escriba **icmp** (en minúsculas) en el cuadro Filtro y pulse **Intro.**
2. Seleccione el primer paquete ICMP, etiquetado como **Echo (ping) request**.
3. Observe los detalles del paquete en el panel central de detalles del paquete de Wireshark. Observe que se trata de una trama Ethernet II / Protocolo de Internet versión 4 / Protocolo de mensajes de control de Internet.
4. Expanda el Protocolo de Mensajes de Control de Internet para ver los detalles de ICMP.
5. Observe el tipo. Observe que el tipo es 8 (solicitud de eco (ping)).

6. Seleccione Datos en el panel central de detalles de paquetes de Wireshark para resaltar la parte de datos de la trama.
7. Observe el contenido del paquete en el panel inferior de bytes de paquetes de Wireshark. Observe que Windows envía una secuencia alfabética durante las solicitudes de ping.

Que. 4. ¿Por qué los paquetes ARP no tienen cabeceras IP?

Respuesta: Aunque hay direcciones IP o de protocolo utilizadas en este mensaje, en realidad no tiene una cabecera IP. Las direcciones IP que se ven son simplemente parte de la cabecera ARP. Esto significa que los mensajes ARP no son enrutables y que los routers no pasarán el tráfico ARP a otra red.
En consecuencia, no se puede determinar la dirección MAC de un nodo que no esté en la LAN del nodo de origen.
También significa que el Ethertype en una trama Ethernet que lleva un mensaje ARP es diferente que en el tráfico de datos estándar. Esta diferencia se muestra a continuación





Que. 5. Compare y contraste las cabeceras UDP y TCP.

Respuesta:

Item	TCP	UDP
Stands For	Transmission Control Protocol	User Datagram Protocol
Protocol	Connection Oriented	Connectionless
Security	Makes Checks For Errors And Reporting	Makes Error Checking But No Reporting
Data Sending	Slower	Faster
Header Size	20 Bytes	8 Bytes
Segments	Acknowledgement	No Acknowledgement
Typical Applications	- Email	- VoIP

Que. 6. ¿Los paquetes ICMP especifican un puerto? Busca en Internet y explica por qué sí o por qué no.

Respuesta: **ICMP** es un protocolo diseñado específicamente para fines de diagnóstico y **el ping** no es más que una solicitud de eco ICMP y una respuesta de eco, por lo que no existe el concepto de números de puerto en **ICMP**. Los números de **puerto** son direcciones de la capa de transporte utilizadas por algunos protocolos de transporte.