Alumno: Dragos Cornel Iván Fecha:23/02/2024

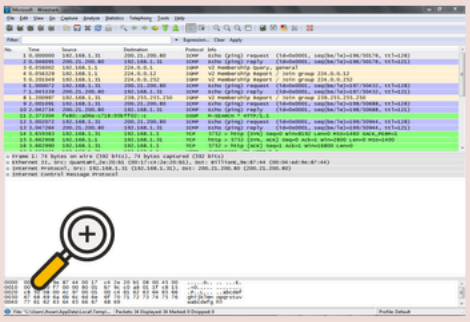
Actividad para el tutor

C4, CE4.3

Monitorizar la actividad de nuestro cortafuegos es algo indispensable para la seguridad de todo el perímetro protegido; la monitorización nos facilitará información sobre los intentos de ataque que estemos sufriendo (origen, franjas horarias, tipos de acceso...), así como la existencia de tramas que aunque no supongan un ataque a priori sí que son al menos sospechosas.

Para las trazas lo común es utilizar algún programa como Wireshark o similares. A partir del contenido estudiado en páginas anteriores, y sirviéndote de la siguiente página para ampliar la información, si lo consideras necesario, señala qué información relevante de trazas puedes detectar a partir de la siguiente imagen de resultados de un filtrado con este programa.

- Análisis de red con Wireshark I. Filtros de captura y visualización
- Análisis de red con Wireshark II. interpretando los datos



Wireshark

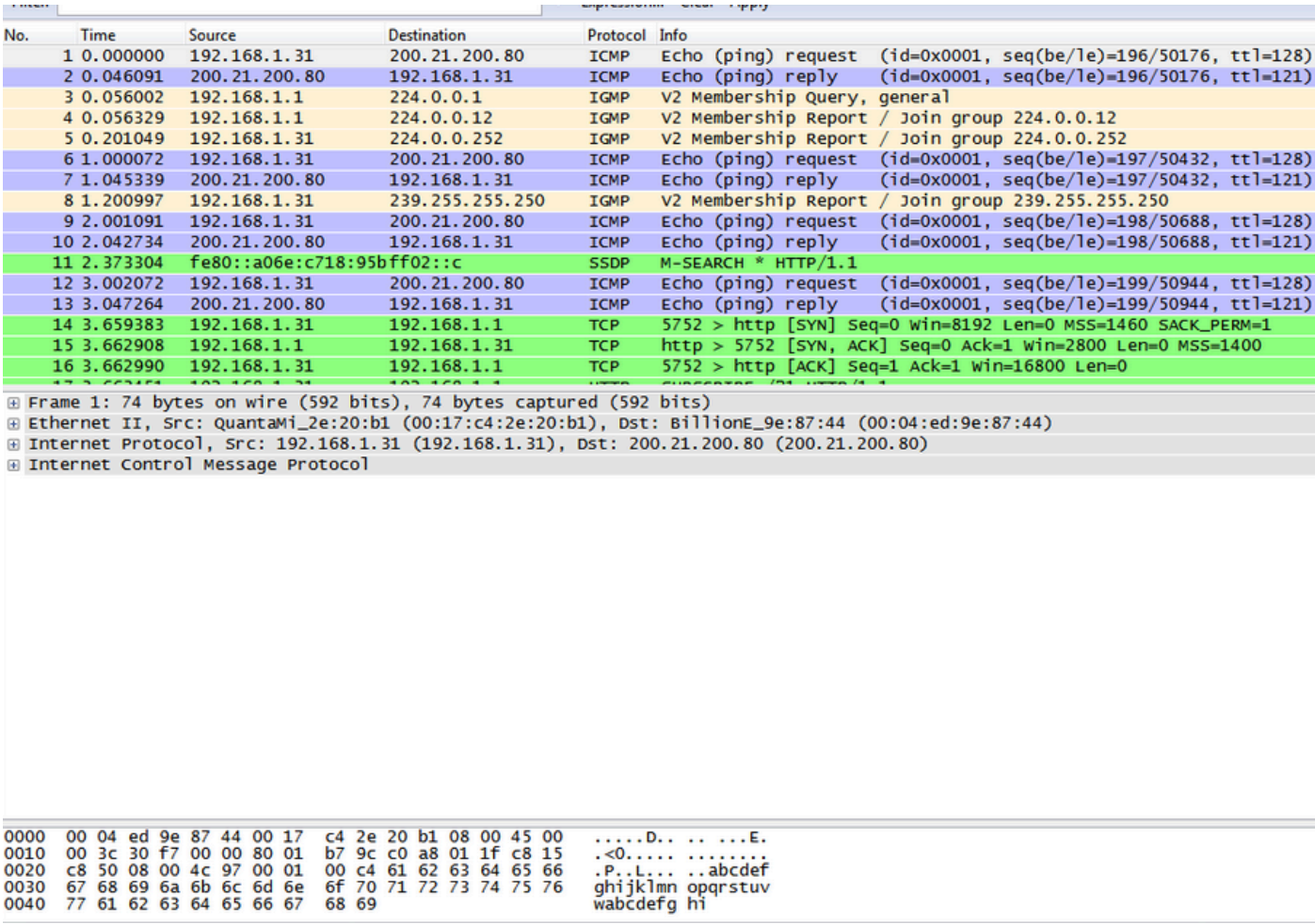
Elaborar un documento descriptivo y enviarlo a su tutor para la valoración del mismo

Envía a tu tutor las conclusiones, en un documento Word (o compatible) con una extensión máxima de 1 página, por los medios establecidos en la plataforma, para su valoración.

https://seguridadyredes.wordpress.com/2008/03/24/analisis-de-red-con-wireshark-filtros-de-captura-y-visualizacian/

https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/

¿qué información relevante de trazas puedes detectar a partir de la siguiente imagen de resultados?

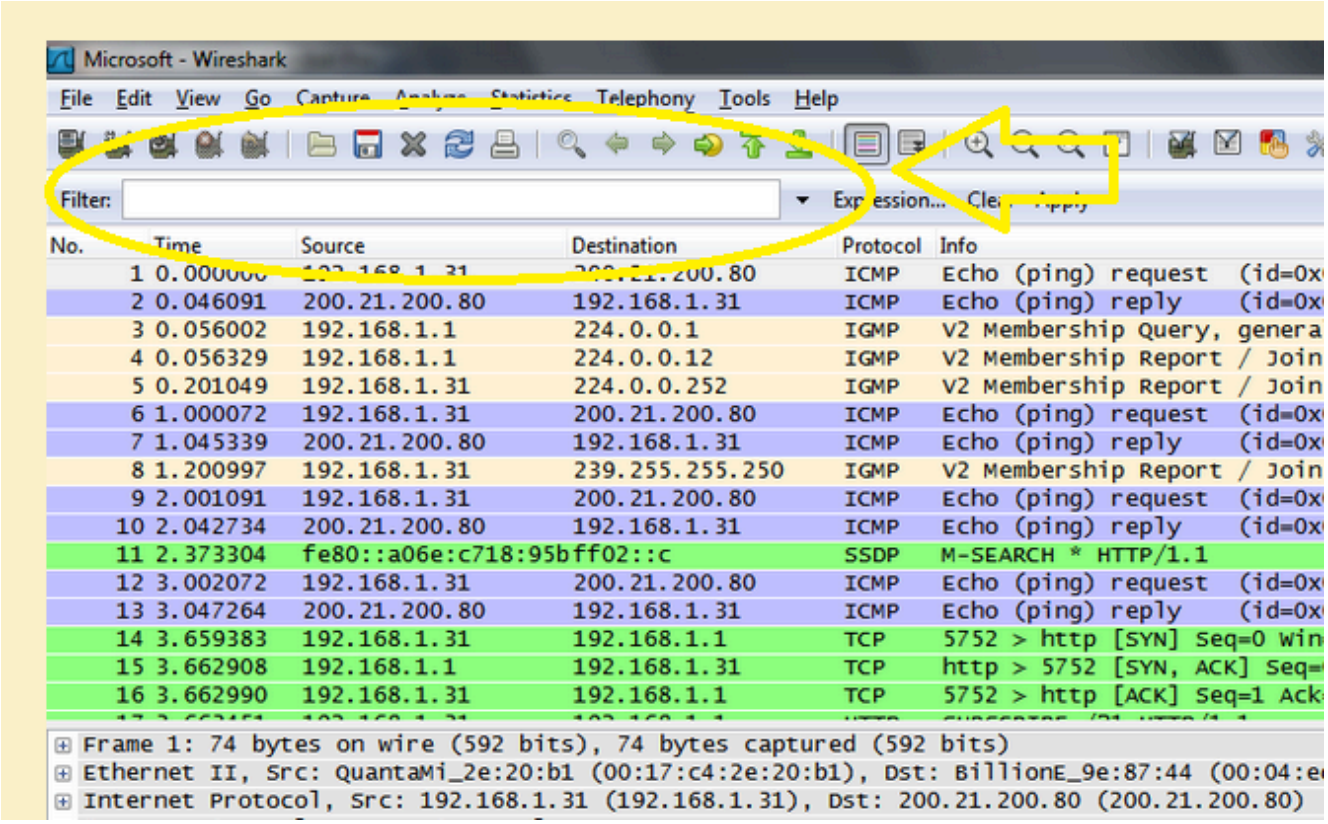


No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.31	200.21.200.80	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=196/50176, ttl=128)
2	0.046091	200.21.200.80	192.168.1.31	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=196/50176, ttl=121)
3	0.056002	192.168.1.1	224.0.0.1	IGMP	V2 Membership Query, general
4	0.056329	192.168.1.1	224.0.0.12	IGMP	V2 Membership Report / Join group 224.0.0.12
5	0.201049	192.168.1.31	224.0.0.252	IGMP	V2 Membership Report / Join group 224.0.0.252
6	1.000072	192.168.1.31	200.21.200.80	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=197/50432, ttl=128)
7	1.045339	200.21.200.80	192.168.1.31	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=197/50432, ttl=121)
8	1.200997	192.168.1.31	239.255.255.250	IGMP	V2 Membership Report / Join group 239.255.255.250
9	2.001091	192.168.1.31	200.21.200.80	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=198/50688, ttl=128)
10	2.042734	200.21.200.80	192.168.1.31	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=198/50688, ttl=121)
11	2.373304	fe80::a06e:c718:95bff02::c		SSDP	M-SEARCH * HTTP/1.1
12	3.002072	192.168.1.31	200.21.200.80	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=199/50944, ttl=128)
13	3.047264	200.21.200.80	192.168.1.31	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=199/50944, ttl=121)
14	3.659383	192.168.1.31	192.168.1.1	TCP	5752 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
15	3.662908	192.168.1.1	192.168.1.31	TCP	http > 5752 [SYN, ACK] Seq=0 Ack=1 Win=2800 Len=0 MSS=1400
16	3.662990	192.168.1.31	192.168.1.1	TCP	5752 > http [ACK] Seq=1 Ack=1 Win=16800 Len=0

```
⊞ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: QuantaMi_2e:20:b1 (00:17:c4:2e:20:b1), Dst: BillionE_9e:87:44 (00:04:ed:9e:87:44)
⊞ Internet Protocol, Src: 192.168.1.31 (192.168.1.31), Dst: 200.21.200.80 (200.21.200.80)
⊞ Internet Control Message Protocol
```

```
0000  00 04 ed 9e 87 44 00 17  c4 2e 20 b1 08 00 45 00   .....D.. .. ...E.
0010  00 3c 30 f7 00 00 80 01  b7 9c c0 a8 01 1f c8 15   .<0..... ........
0020  c8 50 08 00 4c 97 00 01  00 c4 61 62 63 64 65 66   .P..L... ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

En esta imagen parece que estamos ante el resultado de un filtro de captura, ya que los **filtros de captura** son los que se establecen para mostrar solo los paquetes que cumplan los requisitos indicados en el filtro. Si no establecemos ninguno, Wireshark capturará todo el tráfico y lo presentará en la pantalla principal. Como podemos ver en esta imagen, arriba a la izquierda no se ha establecido ningún filtro, por lo que se ha capturado todo el tráfico.

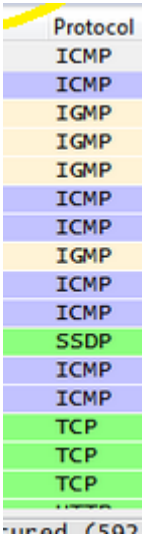


También se puede observar que está conectado a cable Ethernet, y no Wifi.

En la siguiente columna vemos el tiempo cuando se capturaron estos paquetes, y el número de paquetes capturados.

	Time
1	0.000000
2	0.046091
3	0.056002
4	0.056329
5	0.201049
6	1.000072
7	1.045339
8	1.200997
9	2.001091
10	2.042734
11	2.373304
12	3.002072
13	3.047264
14	3.659383
15	3.662908
16	3.662990

La siguiente columna revela el tipo de protocolo que ha filtrado:



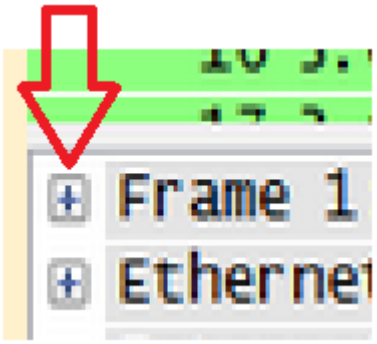
Protocol
ICMP
ICMP
IGMP
IGMP
IGMP
ICMP
ICMP
IGMP
ICMP
ICMP
SSDP
ICMP
ICMP
TCP
TCP
TCP

Las columnas restantes reflejan la IP fuente e IP destino.

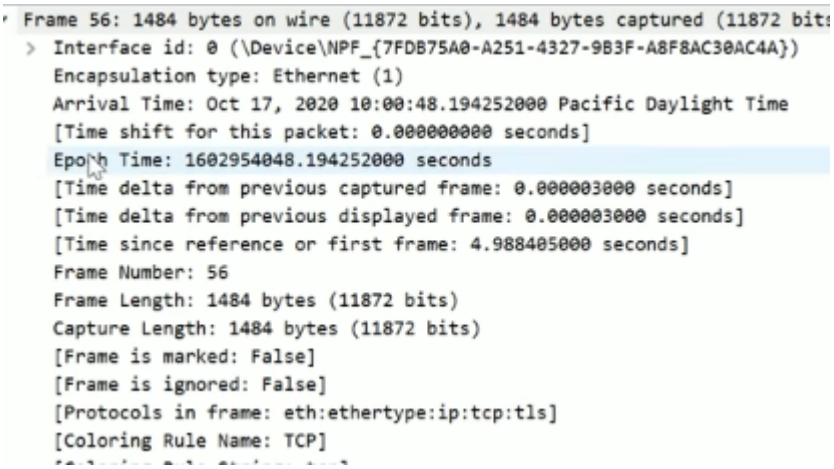
Source	Destination
192.168.1.31	200.21.200.80
200.21.200.80	192.168.1.31
192.168.1.1	224.0.0.1
192.168.1.1	224.0.0.12
192.168.1.31	224.0.0.252
192.168.1.31	200.21.200.80
200.21.200.80	192.168.1.31
192.168.1.31	239.255.255.250
192.168.1.31	200.21.200.80
200.21.200.80	192.168.1.31
fe80::a06e:c718:95b	ff02::c
192.168.1.31	200.21.200.80
200.21.200.80	192.168.1.31
192.168.1.31	192.168.1.1
192.168.1.1	192.168.1.31
192.168.1.31	192.168.1.1

Esto es, “Source” es el servidor desde donde se transmite el paquete de datos (por ejemplo Youtube), y “Destination” es nuestro ordenador o el PC que recibe los paquetes.

Si pulsaramos este botón:



Se desplegará la pestaña, y podríamos ver información como el puerto,

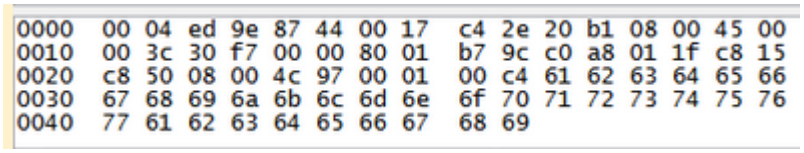


También podemos desplegar la pestana “Transmission” y ver el puerto que estamos usando para un tráfico de datos en concreto, o información extra como el tamaño de los paquetes.

Con este detalle:

vemos que está filtrando mediante Src para capturar todos los paquetes con origen 192.168.1.31 (Host de origen), y Dst los paquetes con destino de Host 200.21.200.80 (Host de destino).

Aquí tenemos la capa de enlace de datos que pertenece a la cabecera Ethernet II:



La actividad capturada en Wireshark muestra una serie de paquetes ICMP (Internet Control Message Protocol) que se utilizan para realizar pruebas de ping entre dos hosts.

En la imagen, podemos observar lo siguiente:

- **Paquete 1:** El primer paquete (número 1) es un paquete ICMP Echo Request enviado desde el host 192.168.1.31 al host 200.21.200.80
- **Paquete 2:** El segundo paquete (número 2) es un paquete ICMP Echo Reply enviado desde el host 200.21.200.80 al host 192.168.1.31
- **Paquete 6:** El primer paquete (número 1) es un paquete ICMP Echo Request enviado desde el host 192.168.1.31 al host 200.21.200.80
- **Paquete 7:** El segundo paquete (número 2) es un paquete ICMP Echo Reply enviado desde el host 200.21.200.80 al host 192.168.1.31
- **Paquete 9:** El primer paquete (número 1) es un paquete ICMP Echo Request enviado desde el host 192.168.1.31 al host 200.21.200.80
- **Paquete 10:** El segundo paquete (número 2) es un paquete ICMP Echo Reply enviado desde el host 200.21.200.80 al host 192.168.1.31
- **Paquete 12:** El primer paquete (número 1) es un paquete ICMP Echo Request enviado desde el host 192.168.1.31 al host 200.21.200.80
- **Paquete 13:** El segundo paquete (número 2) es un paquete ICMP Echo Reply enviado desde el host 200.21.200.80 al host 192.168.1.31
- **Paquetes 3, 4, 5 y 8**: El protocolo IGMP es un protocolo de capa de red que se utiliza para gestionar la membresía a grupos multicast en redes IP.
- En otras palabras, IGMP permite que los hosts se unan y abandonen grupos multicast de manera dinámica. Los grupos multicast son grupos de hosts que pueden recibir simultáneamente el mismo flujo de datos.
- **Paquete 11**: el paquete 11 es una solicitud de búsqueda SSDP que se utiliza para descubrir dispositivos.
- **Paquetes 14, 15y 16**: es un establecimiento de conexión a tres bandas: SYN, SYN-ACK, ACK, para establecer una conexión a un servidor web por el puerto 5752.

Para que te sirva de referencia, el wireshark es una herramienta estupenda para capturar e interpretar el trafico.