Práctica 1: Análisis de tráfico con Wireshark

Sumario

Introducción

La siguiente práctica realizada en la asignatura de planificación y administración de redes trata sobre analizar el tráfico de la red (del instituto y del hogar) capturado por medio del programa **Wireshark**. Así pues, se trata de que el alumno tenga una primera toma de contacto con dicho programa y se familiarice con su interfaz, así como también de la encapsulación de protocolos que se establece en la red y pueda encontrar aquella información más relevante en ella.

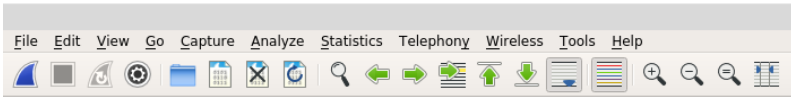
En el instituto se ha empleado una máquina virtual de Linux Mint 19 para realizar la práctica, mientras que en el hogar también se ha empleado Linux Mint 19, pero sin una virtualización de por medio. Para poder usar el analizador de red **Wireshark**, se ha instalado esta herramienta a través de la terminal, escribiendo el siguiente comando:

```
$ sudo apt-get install wireshark
```

Y para ejecutarlo (con derechos de administrador), el siguiente:

```
$ sudo wireshark
```

Ya instalado y ejecutado como administrador, se ha procedido a capturar la red con la primera opción del menú superior, la del símbolo azul que parece una aleta de tiburón y, tras el paso de unos minutos, se ha pausado la captura con el cuadrado que se torna rojo de su derecha:



***Menú de Wireshark**, con las opciones de captura de paquetes, pausa de la captura, reinicio de captura y opciones de captura, entre otros.*

Hecha esta breve introducción, vamos a proceder a la resolución de los ejercicios mandados.

Ejercicio 1: Protocolos de nivel 2

- Monitoriza la red durante uno o dos minutos.
- Haz una lista de los protocolos de nivel 2 que encuentres.
- Compara esos protocolos entre sí:
  - ¿Cuáles son más modernos?
  - Compara los datos de su cabecera, ¿qué informaciones incluye cada uno?

– Los protocolos de segundo nivel que he podido encontrar han sido los siguientes (el primero, tanto en la red del hogar como en la del instituto; el segundo, solo en la del instituto):

- **Ethernet II**, que fue publicado en 1982[1].
- **IEEE 802.3 Ethernet**, que fue creado un año más tarde, en 1983[1].

– Tanto **Ethernet II** como **IEEE 802.3 Ethernet** incluyen una cabecera MAC[2] (*Media Access Control*, un identificador único de una tarjeta o dispositivo en red), que a su vez contiene la dirección MAC del destinatario de la trama (6 bytes), la dirección MAC del origen de la trama (6 bytes) y el protocolo encapsulado (2 bytes), en el caso de **Ethernet II,** o la longitud (2 bytes) en el caso de **IEEE 802.3 Ethernet**; en este orden.

He aquí un ejemplo de una trama **Ethernet II** recogida en el hogar (*ZTE* es la marca del *router* y *Giga-Byt* se refiere a la tarjeta de red incluida en la placa base del ordenador empleado):

```
Ethernet II, Src: Zte_d8:23:ef (9c:6f:52:d8:23:ef), Dst: Giga-Byt_07:f5:22
(1c:1b:0d:07:f5:22)
```

Viendo la trama en el conjunto del paquete recibido, **Ethernet II** se compone de los siguientes 14 bytes (los cuatro primeros *0000* se refieren a la línea de los valores hexadecimales donde se encuentran estos bytes):

```
0000   1c 1b 0d 07 f5 22 9c 6f 52 d8 23 ef 08 00
```

Como bien hemos dicho, los primeros 6 bytes (*1c 1b 0d 07 f5 22*) se refieren a la dirección MAC del receptor, los 6 siguientes (*9c 6f 52 d8 23 ef*) se refieren a la dirección MAC del emisor y, los 2 últimos bytes (*08 00*), especifican el protocolo de la capa superior que recibe los datos (en este caso, el protocolo que recibe los datos es **IPv4**, pero en la red del hogar también pueden aparecer **IPv6** [*86 dd*] o **ARP** [*08 06*]).

Ahora vamos a ver una trama del otro protocolo encontrado, el **IEEE 802.3 Ethernet**. Así aparece el nombre del segundo nivel, algo más escueto que nuestro ejemplo anterior:

```
IEEE 802.3 Ethernet
```

Si miramos en su valor hexadecimal, su cabecera también está compuesta por 14 bytes:

```
0000   01 80 c2 00 00 00 00 1a c1 ac 58 97 00 27
```

La estructura es muy similar a la anterior: en primer lugar tenemos la dirección MAC del receptor (*01 80 c2 00 00 00*), en segundo lugar, la dirección MAC del emisor (*00 1a c1 ac 58 97*) y, por último, la longitud (cantidad de bytes) de los datos que siguen a continuación (*00 27*).

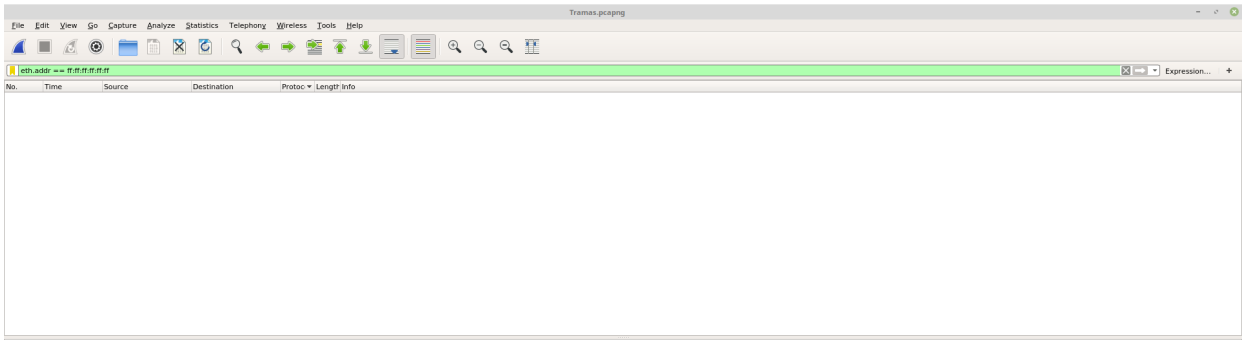
Nota: la trama del protocolo *Ethernet II* fue capturada en la red del hogar, mientras que la trama *IEEE 802.3* fue tomada en la red del instituto, por eso varían las direcciones.

Ejercicio 2: Tramas de *broadcast*

Las tramas de *broadcast* son las que tienen la dirección del nivel de enlace `FF:FF:FF:FF:FF:FF`.

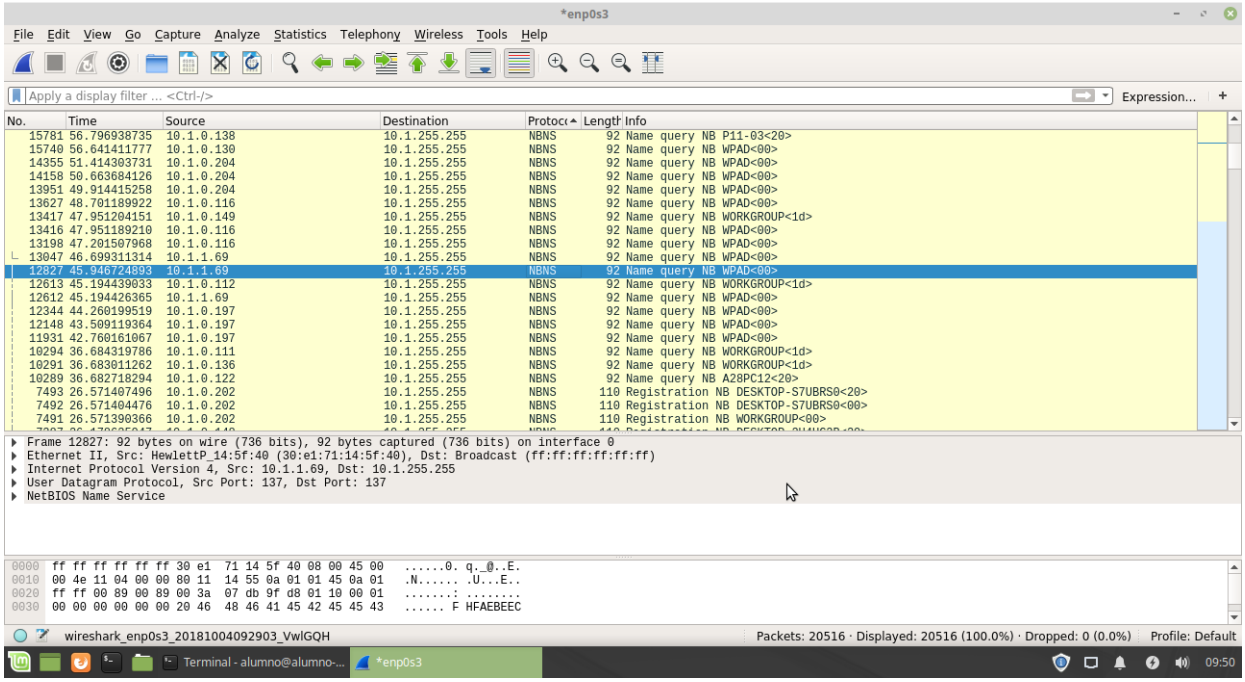
Monitoriza la red durante uno o dos minutos y determina qué tramas de las recibidas son de *broadcast*. Haz una lista de las pilas de protocolos que *viajan* sobre tramas de *broadcast*, e incluye al menos 3 pantallazos de estas pilas como ejemplo.

– En la red del hogar no he podido encontrar ninguna trama de tipo *broadcast*, ni revisándolas manualmente ni estableciendo el filtro `eth.addr == ff:ff:ff:ff:ff:ff`:



Filtro activado: `eth.addr == ff:ff:ff:ff:ff:ff` en la red del hogar. Sirve para extraer aquellas tramas que sean de tipo* broadcast*, pero no se ha encontrado ninguna de entre 15 000. (Hacer* zoom *para agrandar)

Sin embargo, en la red del instituto sí había podido encontrar varias, pero solo he podido recuperar una de ellas, en la que se puede observar la pila de protocolos que hay sobre la trama:



Trama* broadcast *y pila de protocolos sobre esta* *en la red del instituto. (Hacer* zoom *para agrandar)

La pila de protocolos que *viajan* por encima de esta trama son **Internet Protocol Version 4** (**IPv4**), **User Datagram Protocol** (**UDP**) y **NetBIOS** (**Network Basic Input/Output System**).

Ejercicio 3: ¿Qué protocolos viajan sobre el nivel 2?

Captura el tráfico de la red durante uno o dos minutos. Haz una lista de los protocolos que viajen sobre un nivel 2 que encuentres, y crea una tabla con el nombre de protocolo y su código. Como ejemplo:

- Hay tramas *Ethernet* que llevan *IP* (0x0800). Hay que apuntar *IP*.
- Pero no apuntes el Transmission Control Protocol, porque no va directamente sobre el nivel 2 (*ethernet*), sino dentro de un nivel 3 (*IP*).

Nota: puede que alguno de los protocolos que viajen sobre el nivel 2 no sean de nivel 3 OSI.

– Los protocolos que van sobre el nivel 2 se pueden localizar desglosando la trama de este mismo nivel, en mi caso la de **Ethernet II** (en la red del hogar). Desglosada, aparecen tres apartados, que son el destino, el origen y el tipo:

```
▶ Frame 534: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on
  interface 0
▼ Ethernet II, Src: Zte_d8:23:ef (9c:6f:52:d8:23:ef), Dst: Giga-Byt_07:f5:22
  (1c:1b:0d:07:f5:22)
    ▶ Destination: Giga-Byt_07:f5:22 (1c:1b:0d:07:f5:22)
    ▶ Source: Zte_d8:23:ef (9c:6f:52:d8:23:ef)
      Type: IPv6 (0x86dd)
▶ Internet Protocol Version 6, Src: fe80::1, Dst: fe80::24c3:f725:8807:4cbd
▶ User Datagram Protocol, Src Port: 53, Dst Port: 55593
▶ Domain Name System (response)
```

Hay que fijarse en el tercero, el de *Type*, ya que es aquí donde se nos indica qué protocolo es el que viaja por encima de esta trama. Los protocolos que he podido encontrar en la red del hogar han sido los siguientes:

Protocolo	Código
IPv4[3]	0x0800
IPv6[3]	0x86dd
ARP[3]	0x0806

Nota: *0x* indica que los siguientes números están en base hexadecimal.

Ejercicio 4 (opcional): Haz una redacción alternativa del ejercicio anterior

– Si el tercer ejercicio lo he hecho de la manera correcta, creo que su enunciado está bien explicado, ya que también el profesor en clase lo detalla un poco más. Yo únicamente especificaría que es en el apartado *Type* del nivel 2 en el que se encuentra dicha información, pero gracias al ejemplo que hay puesto de *IP*, esto es más intuitivo. Aparte, esto se refuerza con que no hay que apuntar el *Transmission Control Protocol*.

Referencias

1. Tabla de estándares ethernet y sus fechas.
2. Cabecera MAC de Ethernet II.
3. Tabla de protocolos que viajan sobre el nivel 2.