Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

# Práctica2 - Analizadores de red: Ethereal y tcpdump. ARP

## 1- Objetivos

Comprender los conceptos básicos del monitoreo de tráfico de red mediante el uso del analizador de protocolos Ethereal y del sniffer tcpdump.

Análisis de tramas Ethernet correspondientes a protocolos de nivel de transporte; TCP y de nivel de red; ICMP, IP y ARP.

## 2- Login

En esta práctica hará uso de su cuenta de Linux en un PC-SC.

## 3- Ethereal: Herramienta de sniffing y analizador de protocolos

Un sniffer es una herramienta que se emplea para observar los mensajes que intercambian dos entidades en comunicación a través de una red. El sniffer (literalmente "olfateador") captura las tramas a nivel de enlace que se envían/reciben a través de los interfaces de red de nuestra computadora.

Un dato importante es que un "sniffer" es un elemento pasivo: observa los mensajes que intercambian aplicaciones y protocolos, pero ni genera información por sí mismo, ni es destinatario de ésta. Las tramas que captura son siempre una copia (exacta) de las que en realidad se envían/reciben en nuestro ordenador.

Un **analizador de protocolos** es un sniffer al que se le ha dotado de funcionalidad suficiente como para entender y traducir los protocolos que se están hablando en la red. Es de utilidad para desarrollar y depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado. Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (HTTP, TCP, ICMP,...) y mostrar al usuario la información decodificada. De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red que se está analizando. Esto último es muy importante para un programador que esté desarrollando un protocolo, o cualquier programa que transmita y reciba datos en una red, ya que le permite comprobar lo que realmente hace el programa. Además de para los programadores, estos analizadores son muy útiles para todos aquellos que quieren experimentar o comprobar cómo funcionan ciertos protocolos de red, analizando la estructura y funcionalidad de las unidades de datos que se intercambian. También, gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos, para así comprender mejor su funcionamiento.

Ethereal es un analizador de protocolos de red, con interfaz gráfico, que nos permitirá capturar las tramas que entran y salen de nuestro ordenador para luego "diseccionarlas" y estudiar el contenido de los mismas. Ethereal, emplea la misma librería de captura de paquetes (libpcap) que otros sniffers conocidos, como tcpdump, aunque es capaz de leer muchos otros tipos de formato de captura.

Además es un software de libre distribución que puede correr en distintas plataformas (Windows, Linux/Unix, y Mac). Pero, probablemente, lo más destacable sea su interfaz gráfica y la potente capacidad de filtrado que presenta.

Nos vamos a centrar ahora en exponer unas nociones básicas de la forma en la que el analizador de protocolos Ethereal presenta la información capturada.

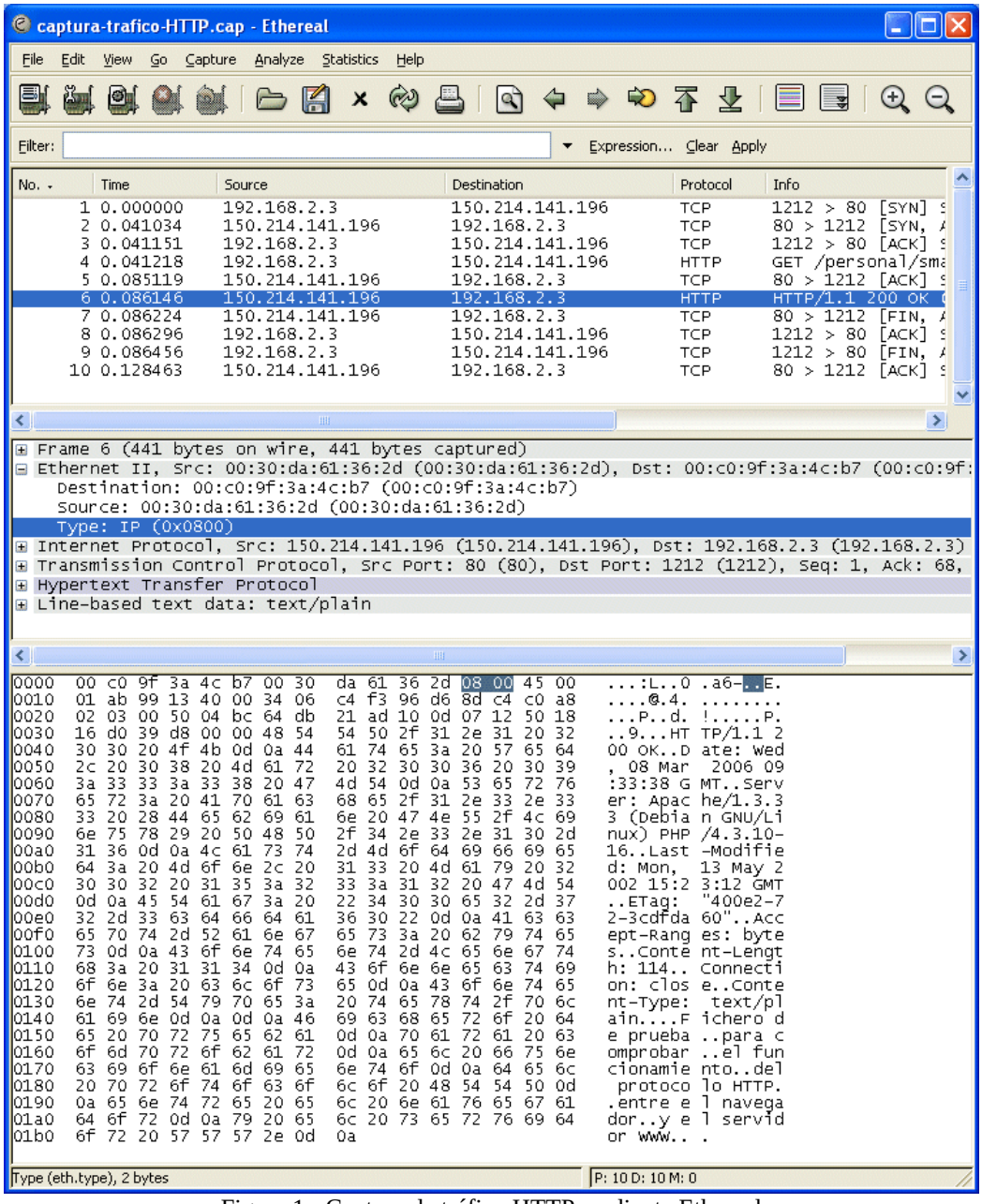


Figura 1.- Captura de tráfico HTTP mediante Ethereal

En la Fig. 1, podemos ver en funcionamiento el analizador de protocolos Ethereal. Nos está mostrando el contenido del archivo “captura-trafico-HTTP.cap”en el que hay 10 tramas previamente capturadas usando también el mismo programa, pues Ethereal sirve para ambas cosas, para capturar el tráfico de la red y para analizarlo, pudiendo salvarlo en un archivo si así se desea. Vamos a fijarnos

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

en detalle en la forma en que Ethereal (y otros analizadores de protocolos) nos muestran las tramas capturadas.

Vemos que la ventana de Ethereal se encuentra dividida en tres paneles: El superior,"Packet List" (según lo denomina el programa), el central, "Packet Details" y el inferior, "Packet Bytes". Hay que hacer notar que Ethereal llama "Packets" a las tramas capturadas. No hay que confundir estos "Packets" (llamados así quizás por razones históricas) con las PDUs de nivel 3. Nosotros nos vamos a referir siempre a los datos capturados por Ethereal como tramas.

El panel superior muestra un listado de las tramas capturadas. En este caso muestra las 10 tramas que tenemos capturadas en el archivo "captura-trafico-HTTP.cap". Nótese que hay una trama, la número 6, "resaltada" en un color más oscuro. Eso es así pues hemos hecho clic sobre ella con el ratón, seleccionándola de entre todas las del listado. La información que el listado de tramas muestra respecto a cada una de las tramas es muy limitada, por razones obvias de espacio. Se reduce a los campos más importantes de la misma y a un breve resumen que permita, de un vistazo, hacerse una idea de lo que está ocurriendo en la red.

El panel central muestra los detalles relativos al contenido de la trama que hayamos seleccionado en el panel superior, en este caso la trama ("Frame") número 6. Los detalles de la trama, que son muchos, son mostrados en forma de árbol, cuyas ramas podemos contraer o expandir, para tener una visión más general (contrayendo las ramas) o una visión más detallada (expandiéndolas). En la imagen podemos ver como hay una primera rama, que está contraída (se sabe porque aparece un signo "+ " que permitiría expandirla). Esta primera rama nos indica el número de orden de la trama con respecto a las demás (Frame 6) y diversa información relacionada con el instante en que la trama fue capturada. Es decir, la información de esta primera rama la aporta el programa Ethereal y NO es algo que tenga que ver con el contenido de la trama. Son cosas como la fecha y la hora de la captura, número de octetos que se han capturado de la trama, número de orden, etc… Las restantes ramas que van apareciendo en el panel central ya **sí** que tienen que ver con el contenido de la trama. Aparece una rama por cada cabecera que se detecta en la trama. En este caso el analizador de protocolos nos indica que en la trama 6 hay una cabecera Ethernet versión 2, luego hay una cabecera IP (Internet Protocol), luego una cabecera TCP (Transmisión Control Protocol) y así sucesivamente.

Concretamente vemos que la rama correspondiente a la cabecera Ethernet versión 2 está expandida y podemos ver los tres campos que la componen. Está resaltado en un color más oscuro el campo Tipo ("Type") y podemos ver su valor (que es 0x0800, número hexadecimal pues empieza por 0x) y su significado, en este caso IP (es correcto, pues ya sabemos que el valor 0x0800 en el campo tipo de una trama Ethernet versión 2 quiere decir que la trama contiene datos del protocolo IP).

Por último, el panel inferior muestra, sin ninguna información extra, los octetos ("bytes") de los que está compuesta la trama que se ha seleccionado en el panel superior y cuyos detalles ya estamos viendo en el panel central. Esos octetos se muestran en hexadecimal (cada octeto son dos dígitos hexadecimales) organizados en filas de 16 octetos. Como ayuda podemos ver que cada fila de 16 octetos viene precedida de un número en hexadecimal que nos indica la posición que ocupa el primero octeto de la fila en la trama. Por ejemplo, la primera fila viene precedida por el número 0000 (hexadecimal) lo que quiere decir que el primer octeto de esa fila es el que estaba en la posición primera de la trama (la cero). La segunda fila está etiquetada con el número 0010 (hexadecimal), que es el 16 en decimal. Luego el primer octeto de esa segunda fila ocupa la posición 16 en la trama. Si nos fijamos nos damos cuenta que estas etiquetas de ayuda que aparecen al principio de cada fila van

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

de 16 en 16 (de 0010 en 0010 en hexadecimal) porque las filas tienen 16 octetos exactamente. Por comodidad, este panel inferior nos muestra también, en su parte derecha, una copia de los octetos de la trama pero en formato ASCII. Es decir, cada octeto es traducido al carácter equivalente según el código ASCII. Los caracteres no imprimibles (los que no equivalen a letras, números o símbolos) se representan como un punto. Esto puede ser útil en ciertas tramas que contengan PDUs con datos en modo texto. Nótese que el panel inferior y el panel central son la misma cosa vista de dos modos diferentes. No hay más que ver como al haber seleccionado el campo "Type" en el panel central, en el panel inferior podemos ver resaltado un par de octetos de la trama, que son precisamente el 08 y 00, el valor que tiene dicho campo "Type". Hay que precisar que el analizador nos muestra en este panel inferior toda la trama Ethernet versión 2 o IEEE 802.3 salvo los 64 bits primeros del preámbulo. Es decir, que el octeto primero que podremos ver será el primer octeto de la dirección MAC destino. Otro campo que muchas veces no aparece será la cola de la trama (el FCS, "Frame Check Sequence) pues hay tarjetas que son incapaces de proporcionar este dato en el momento de la captura.

Finalmente, por encima de estas tres secciones aparecen otros dos elementos: los menús de comandos (menús desplegables y barra de herramientas) y el campo de filtrado de visualización.

## 4- ¿Qué necesito para estar en red?

Un ordenador que vaya a funcionar en red necesita una dirección para que la red pueda dirigir hacia él los datos que le envían el resto de ordenadores, es la dirección IP. Para ver la dirección IP de su ordenador (S.O. Linux) puede usar el comando `ifconfig`.

```
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:2F:72:2B:9E
          inet addr:10.1.1.51  Bcast:10.1.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:241448 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84926 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43488888 (41.4 Mb)  TX bytes:18249053 (17.4 Mb)
          Interrupt:10 Base address:0xd800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3489 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3489 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2786870 (2.6 Mb)  TX bytes:2786870 (2.6 Mb)
```

Puede observar que su ordenador tiene dos interfaces:

- `eth0` es una conexión a una red de área local Ethernet y es la verdadera conexión de red de ese ordenador.

- `lo` es un interfaz ficticio llamado interfaz de `loopback`, todo lo que se envía por ese interfaz se vuelve a recibir en el ordenador. Es típico de los sistemas UNIX tener este interfaz y vale para enviarse datos a sí mismo incluso cuando el ordenador no está conectado a la red. En los

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

sistemas UNIX muchas partes del sistema operativo funcionan como servicios de red, de ahí que el interfaz de `loopback` sea muy útil. Pero de momento no se preocupe por él.

Así pues su ordenador tiene un interfaz conectado a una red Ethernet y en dicho interfaz utiliza la dirección IP que se ve en el campo `inet addr:`. Compruebe cuál es su dirección IP. Esa dirección es suficiente para identificar a su ordenador en Internet. En nuestro caso, al estar la red del Laboratorio separada de Internet (es una Intranet) la dirección sólo le identifica entre los ordenadores del dominio del Área de Telemática (o sea este laboratorio[Telemática 1] y el de abajo[Telemática 2]). Pero para todos los efectos funciona igual que Internet.

Pruebe el comando `ping`. El comando `ping` es una utilidad que le permite comprobar si existe conectividad de red entre dos máquinas. Con ayuda de ping podremos determinar si el nivel de red funciona adecuadamente, así como los niveles de enlace y físico sobre los que descansa. Para ello la máquina que lanza el comando `ping` envía paquetes del protocolo ICMP que el sistema operativo de la máquina destino está obligada a responder al origen. El comando `ping` recibe estos paquetes y nos los muestra indicándonos también el tiempo que tardan en ir y volver (`Round Trip Time, RTT`) y contando los que se pierden. Mire la dirección IP que tiene su vecino de mesa y haga ping a su propio ordenador y al del vecino.

```
$ ping direccion_IP_de_mi_vecino
$ ping mi_direccion_IP
```

Observe la diferencia de tiempos. Pruebe con otros vecinos. ¿Cómo hace ping para saber que los paquetes se pierden?

## 5- Utilizando Ethereal

Para ejecutar ethereal, podemos lanzarlo desde el menú principal (Programs > Internet > Ethereal) o bien desde una consola de comandos (xterm) tecleando ethereal(recuerden la práctica1-LINUX).

Por ahora, en nuestras pantallas, las distintas áreas que hemos comentado anteriormente aparecen en blanco. Capturemos los primeros paquetes y veamos qué sucede.

- ✓ Desde un terminal: `$ ping direccion_IP_de_mi_vecino`
- ✓ Para comenzar la captura abrimos el menú Capture y seleccionamos Start. Ahí aparecen todas las opciones de captura.
- ✓ Dejamos las opciones por defecto y pulsamos OK.
- ✓ A continuación aparece una ventana de seguimiento de la captura. Indica los tipos de paquetes encontrados y el botón de parada de la captura. Ethereal ya está capturando todas las tramas que traspasan nuestro interfaz de red.

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

- ✓ Observe que mientras `ethereal` captura, le muestra que está reconociendo paquetes de diversos protocolos. Cuando tenga algún paquete ICMP, los causados por el comando `ping`, detenga la captura y busque en estos paquetes ICMP qué dirección origen y destino llevan.

- ✓ Puede indicarle al programa `ethereal` que filtre el tráfico que ve de forma que sólo muestre los paquetes ICMP. Para ello en la casilla de texto junto al botón *Filter* escriba *icmp*. Del mismo modo puede introducir este mismo filtro en la ventana de programación de la captura de forma que sólo capture los paquetes que cumplan el filtro.

Analicen, a continuación, las tramas capturadas ayudándose para ello de las siguientes cuestiones.

⇒ Para la trama Ethernet que contiene el mensaje "echo request":
1. ¿Cuál es la dirección Ethernet de 48-bit del interfaz de red de tu ordenador?
2. ¿Cuál es la dirección Ethernet destino dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?
3. ¿Cuál es el valor hexadecimal del campo Tipo de Trama (Frame Type)?
4. ¿Qué tamaño tiene el campo de datos de esta trama Ethernet?

⇒ Y para la trama Ethernet que contiene el mensaje de respuesta "echo reply":
1. ¿Cuál es la dirección Ethernet origen dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?
2. ¿Cuál es la dirección destino dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?
3. ¿Cuál es el valor hexadecimal del campo Tipo de Trama (Frame Type)?
4. ¿Qué tamaño tiene el campo de datos de esta trama Ethernet?

Checkpoint 2.1: Muestre al profesor de prácticas la posición, dentro de la cabecera IP, del campo que ha permitido saber al analizador que el contenido del paquete IP era un paquete ICMP**.**

## 6- Nivel de transporte: TCP

En este apartado veremos el comportamiento de TCP en detalle. Para ello, vamos a analizar una traza de segmentos enviados y recibidos en la transferencia de un archivo de 150 KB de nuestro de PC a un servidor remoto.

- ✓ Abre el navegador y ve a la siguiente dirección:
  - http://gaia.cs.umass.edu/ethereal-labs/alice.txt

- ✓ Guarda una copia del archivo txt en el ordenador del laboratorio.

- ✓ A continuación ve a la dirección:
  - http://gaia.cs.umass.edu/ethereal-labs/TCP-ethereal-file1.html

- ✓ Presiona "Examinar…" y selecciona el archivo anteriormente guardado en tu ordenador, pero NO PRESIONES todavía "Upload alice.txt file".

- ✓ Abre Ethereal y comienza la captura de paquetes.

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

- ✓ Vuelve al navegador y presiona "Upload alice.txt file". De esta manera el archivo alice.txt irá al servidor de gaia.cs.umass.edu. Una vez que el fichero se haya cargado en el servidor obtendrás un mensaje de finalización.
- ✓ Para la captura de paquetes de Ethereal y ***filtra el resultado para ver únicamente los paquetes del tipo `tcp`.***

Utilice las siguientes cuestiones para analizar la captura resultante:

1. Observa la secuencia de establecimiento de la conexión ¿Cuántos paquetes la forman?
2. ¿Cuál es la dirección IP y el puerto origen?
3. ¿Cuál es la dirección IP y el puerto destino?
4. ¿Cuál es el número de secuencia del segmento TCP SYN que inicia la conexión?
5. ¿Cuál es el número de secuencia que aparece en el segmento TCP que contiene el comando HTTP POST?
6. ¿A qué se debe el valor que aparece en el campo ACK de mensajes de confirmación?
7. ¿Cuál es el tamaño de los segmentos que llevan el contenido del fichero?
8. ¿Qué puede apreciar en cuanto al tamaño de la ventana deslizante?

Checkpoint 2.2: ¿Se confirman todos y cada uno de los paquetes enviados?¿Por qué?.

## 7- Empleo de tcpdump

Hemos estado revisando el contenido de paquetes desde una herramienta gráfica y de muy fácil manejo, como es Ethereal. Esta vez vamos a ver el contenido desde una herramienta de consola de comandos: `tcpdump`.

Como ya comentamos con anterioridad, la librería de captura de Ethereal (libpcap) es la misma que emplea tcpdump, y la sintaxis de filtrado es muy similar; pero para un mejor conocimiento de la herramienta, consultad las páginas de manual disponibles para tcpdump:

- En Linux → $man tcpdump
- Online → http://www.tcpdump.org/tcpdump_man.html

Este último apartado de la práctica no es tan guiado como los anteriores, sino que has de tomar un poco más la iniciativa. Se indica qué debes hacer; el cómo ya es cosa tuya.

Puede resultarle de utilidad la herramienta `nc` (netcat). En resumen netcat realiza y acepta conexiones TCP Y UDP. Consulte su manual (`man nc`). La línea básica de comandos para Netcat es `nc [opciones] host puertos`, donde `host` es la dirección IP que se desea analizar y `puertos` es o un determinado puerto o un rango de puertos o una serie de puertos separados por espacios.

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Sirva como ejemplo la siguiente secuencia para el establecimiento del típico chat:

⇒ PC-SC(ip:10.1.1.11) – ARMARIO1:(Escuchando en el puerto 7700)
```
$nc -l -p 7700
$hola
```
⇒ PC-SC – ARMARIO 2:(Conectando con la ip 10.1.1.11 en el puerto 7700)
```
$nc 10.1.1.11 7700
$hola
```

Los pasos a seguir son: (***Léalos completamente antes de realizarlos***)

- ✓ Establecer una conexión mediante una aplicación cliente/servidor que utilice TCP como protocolo de transporte.
- ✓ Enviar información a través de dicha conexión y finalizarla.
- ✓ Realizar una captura de todo el proceso anterior con `tcpdump`.
- ✓ Filtrar los *paquetes que intervienen* en las negociaciones de ***establecimiento de conexión*** y volcarlos a un archivo de texto (**arssXYp2_INICIO.txt**).
- ✓ Filtrar los *paquetes que intervienen* en las negociaciones de ***fin de conexión*** y volcarlos a un archivo de texto (**arssXYp2_FIN.txt**).

  ***Nota:*** *Dispone de los conocimientos necesarios para realizar los 2 pasos anteriores*

- ✓ Editar los archivos anteriores y marcar la siguiente información:
  - ⇒ (en amarillo) los campos que indiquen que el paquete pertenece a las negociaciones de establecimiento/fin de conexión
  - ⇒ (en verde) los campos que indiquen la máquina origen/destino
  - ⇒ (en azul) los campos que indiquen los puertos origen/destino
- ✓ Guarden los archivos y preparen el siguiente punto de control.

Checkpoint 2.3: Indique la secuencia de comandos empleada para ejecutar el establecimiento y fin de la conexión mediante la captura correspondiente de tcpdump, y muestre un esquema de la secuencia de ambos mecanismos.