Análisis de comunicaciones TCP/IP con Ethereal

Taller

Federico Lazcano
flazcano@eie.fceia.unr.edu.ar

Área Comunicaciones
Escuela de Ingeniería Electrónica
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario

Índice de contenido

1.- Introducción a Ethereal....4
1.1.- Características....4
1.2.- Ventana principal....4
1.3.- Instalación de Ethereal....5
2.- Objetivos....5
3.- Desarrollo del taller....5
3.1.- Requisitos....5
3.2.- Diagrama de red....5
4.- Experiencias....6
4.1.- Paquetes IP....6
4.2.- Datagramas TCP....9
4.3.- Datagrama UDP....12
5.- Información complementaria....14

Índice de ilustraciones

Ilustración 1 - Vista de la aplicación Ethereal....4
Ilustración 2 - Diagrama de la red de la experiencia....6
Ilustración 3 - Trama Ethernet (802.3)....6
Ilustración 4 - Estructura de un paquete IP....6
Ilustración 5 - Ventana de Captura....7
Ilustración 6 - Captura de paquetes IP....8
Ilustración 7 - Detalle de paquete IP....8
Ilustración 8 - Encapsulado de TCP en IP....9
Ilustración 9 - Estructura de un datagrama TCP....9
Ilustración 10 - Volcado de sesión telnet....10
Ilustración 11 - TCP 3-Way Handshaking....11
Ilustración 12 - Números de secuencia TCP....11
Ilustración 13 - Volcado de sesión SSH....12
Ilustración 14 - Encapsulado de UDP en IP....12
Ilustración 15 - Estructura de un datagrama UDP....13
Ilustración 16 - Resolución de nombre (DNS)....14

Referencias

[1] Sitio Web Ethereal, http://www.ethereal.com.
[2] Wikipedia, la enciclopedia libre, http://es.wikipedia.org.
[3] TCP/IP Tutorial and Technical Overview, http://www.redbooks.ibm.com/redbooks/GG243376.html.
[4] PuTTY: A Free Telnet/SSH Client, http://www.chiark.greenend.org.uk/~sgtatham/putty/.

Enviar sugerencias o comentarios sobre este taller a flazcano@eie.fceia.unr.edu.ar

1.- Introducción a Ethereal

Ethereal [1] es un analizador de protocolos de red, implementado en software. Un analizador de protocolos es una herramienta para capturar paquetes de red y mostrarlos de la manera más detallada posible. Se puede pensar un analizador de protocolos como un electroscopio aplicado a un cable, cuando necesitamos conocer las señales eléctricas que se encuentran en él.
Este software permite localizar fallas, desarrollar software y protocolos, y también se utiliza, como veremos aquí, con fines educativos. Posee una licencia libre[1], y está disponible para las plataformas más populares, como Unix, GNU/Linux y MS Windows.

1.1.- Características

- Captura datos en vivo desde una placa de red
- Muestra los datos con un alto nivel de detalle
- Permite guardar y recuperar los datos capturados
- Permite importar y exportar desde y hacia numerosos programas
- Posee reglas de filtrado muy versátiles, incluyendo búsqueda de paquetes

1.2.- Ventana principal

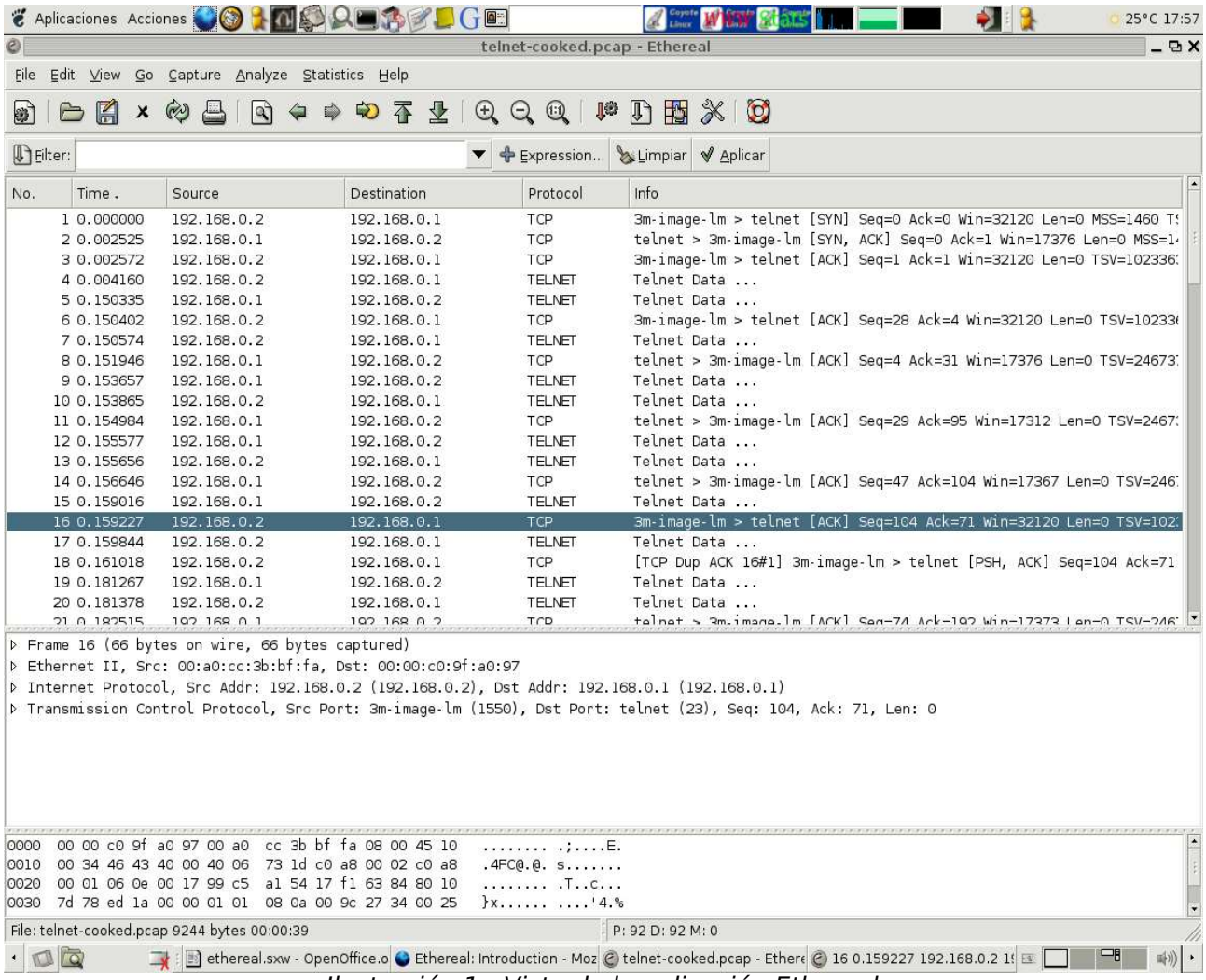

Ilustración 1 - Vista de la aplicación Ethereal

1 Ethereal se distribuye mediante la licencia GPL, utilizada frecuentemente en GNU/Linux.

1.3.- Instalación de Ethereal

1.3.1.- GNU/Linux

Generalmente Ethereal es provisto por la distribución de GNU/Linux que estemos utilizando. En las distribuciones compatibles con el administrador de paquetes RPM (Red Hat, Fedora, Mandrake) ejecutar con permisos administrativos:

```
host:~# rpm -ivh ethereal-0.10.XX-0.X.X.i386.rpm
```

Si existen dependencias insatisfechas, será necesario primero instalar dichas depedencias, y reintentar.
Bajo Debian GNU/linux, simplemente ejecutar con permisos administrativos:

```
host:~# apt-get install ethereal
```

1.3.2.- MS Windows

Para poder utilizar Ethereal en MS Windows es necesario instalar la última versión estable de WinPcap[2]. Para toda instalación se necesitarán permisos administrativos sobre el equipo.
Una vez finalizado el paso anterior, descargar de la página de Ethereal el paquete auntoinstalable y ejecutarlo.

2.- Objetivos

El objetivo de este taller es que los alumnos puedan incorporar los siguientes conocimientos:

- Reconocer la estructura interna de un paquete IP.
- Analizar los datagramas TCP, incluyendo el 3-Way Handshaking, observando las banderas y secuencias respectivas.
- Analizar los datagramas UDP.

3.- Desarrollo del taller

3.1.- Requisitos

- Equipo con MS Windows o GNU/Linux, ubicado en el laboratorio EIE
- Privilegios administrativos en dicho equipo
- Analizador de protocolos Ethereal
- WinPcap en caso de utilizar MS Windows
- Conexión a la red eie.fceia.unr.edu.ar
- Emulador de terminal PuTTY

3.2.- Diagrama de red

A continuación vemos un diagrama de la red en la cual se llevará a cabo la experiencia.
En el las capturas de red, las direcciones correspondientes al tipo 172.16.0.X se supondrán internas a la red eie.fceia.unr.edu.ar.

2 WinPcap es una implementación bajo MS Windows de las librerías necesarias para capturar datos de una placa de red. http://winpcap.polito.it/install/default.htm

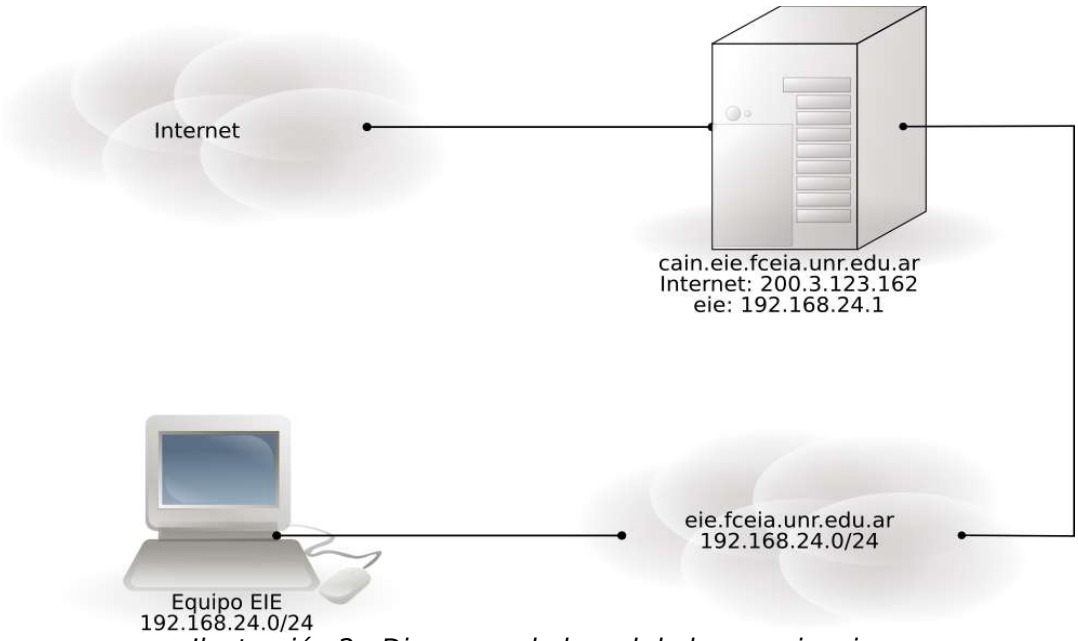

Ilustración 2 - Diagrama de la red de la experiencia

4.- Experiencias

En este taller, desarrollado en el ámbito de la Escuela de Ingeniería Electrónica, todos los paquetes y datagramas a analizar, estarán encapsulados en datagramas Ethernet, reguladas por el estándar IEEE 802.3. A continuación se muestra la estructura de la trama.

Ilustración 3 - Trama Ethernet (802.3) [3]

El objeto de análisis de este taller es la zona de carga de la trama Ethernet, que se encuentra marcado en la figura, con una longitud entre 46 y 1500 bytes.

4.1.- Paquetes IP

En esta primera experiencia analizaremos un paquete IP, observando sus encabezados.

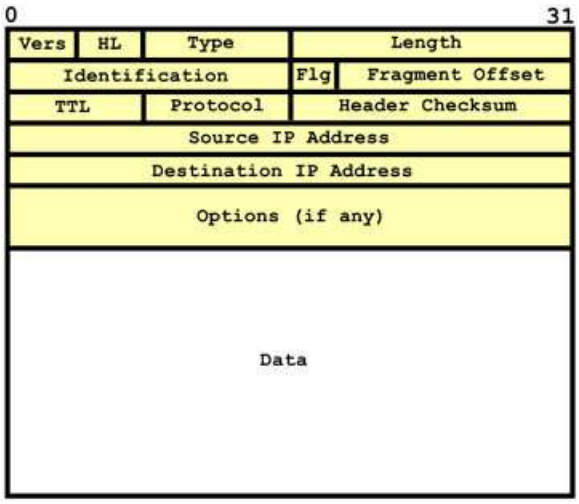

Ilustración 4 - Estructura de un paquete IP

3 Extraído de http://www.etse.urv.es/~cmolina/XCI/files/Network Packet Formats.htm

Para realizar esto haremos un *ping*[4] [2] a la dirección de Internet eie.fceia.unr.edu.ar al mismo tiempo que capturamos los paquetes mediante Ethereal.
Abrimos la aplicación Ethereal maximizada, y apretando *Ctrl+K* iniciamos una nueva captura de datos.

Para esta experiencia no utilizaremos la captura en modo promiscuo, habilitaremos la resolución de nombres (*Enable network name resolution*) y detendremos la captura luego de 1 minuto.

Antes de comenzar la captura, abriremos una ventana de consola, donde escribiremos lo siguiente, pero sin ejecutarlo:

```
host:~$ ping eie.fceia.unr.edu.ar -c 1
```

```
c:\windwos\ ping eie.fceia.unr.edu.ar -n 1
```

Este comando hará una solicitud de eco ICMP a dicho sitio.

Luego, desde la ventana anterior iniciamos la captura, y posteriormente ejecutamos el comando. De esta manera nos aseguramos de capturar la totalidad de los paquetes generados. Si fuera necesario, es posible finalizar prematuramente la captura antes del tiempo estipulado.

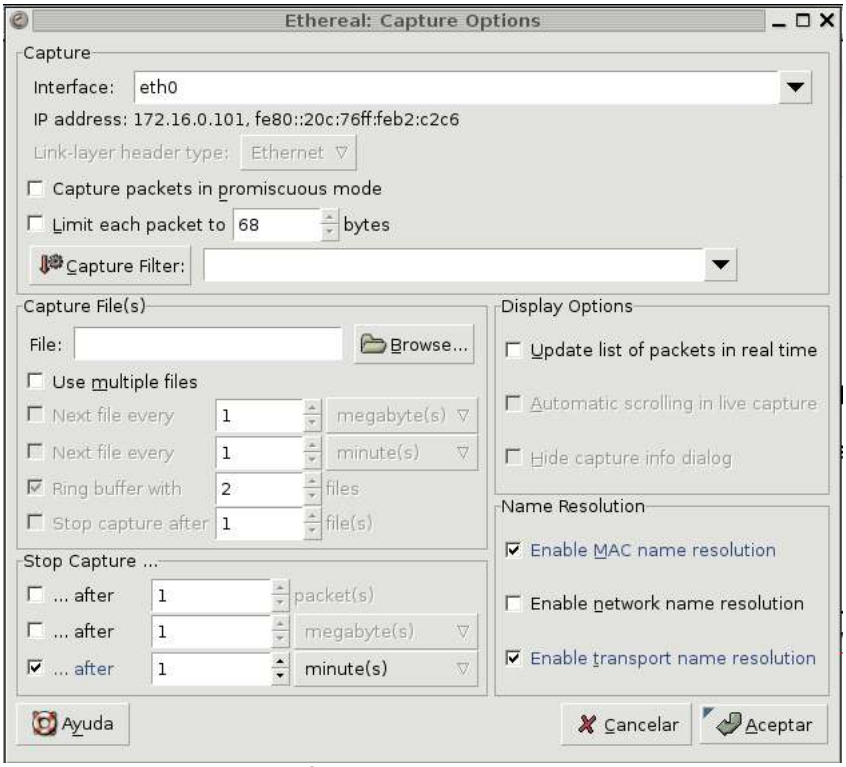

Ilustración 5 - Ventana de Captura

La ventana principal de Ethereal debería mostrar ahora algo similar a lo siguiente:

4 La utilidad *ping*, presente en casi todos los sistemas operativos comprueba las conexiones con uno o varios equipos remotos. El comando ping utiliza los paquetes de solicitud de eco (protocolo ICMP) y de respuesta de eco para determinar si un sistema IP específico funciona en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

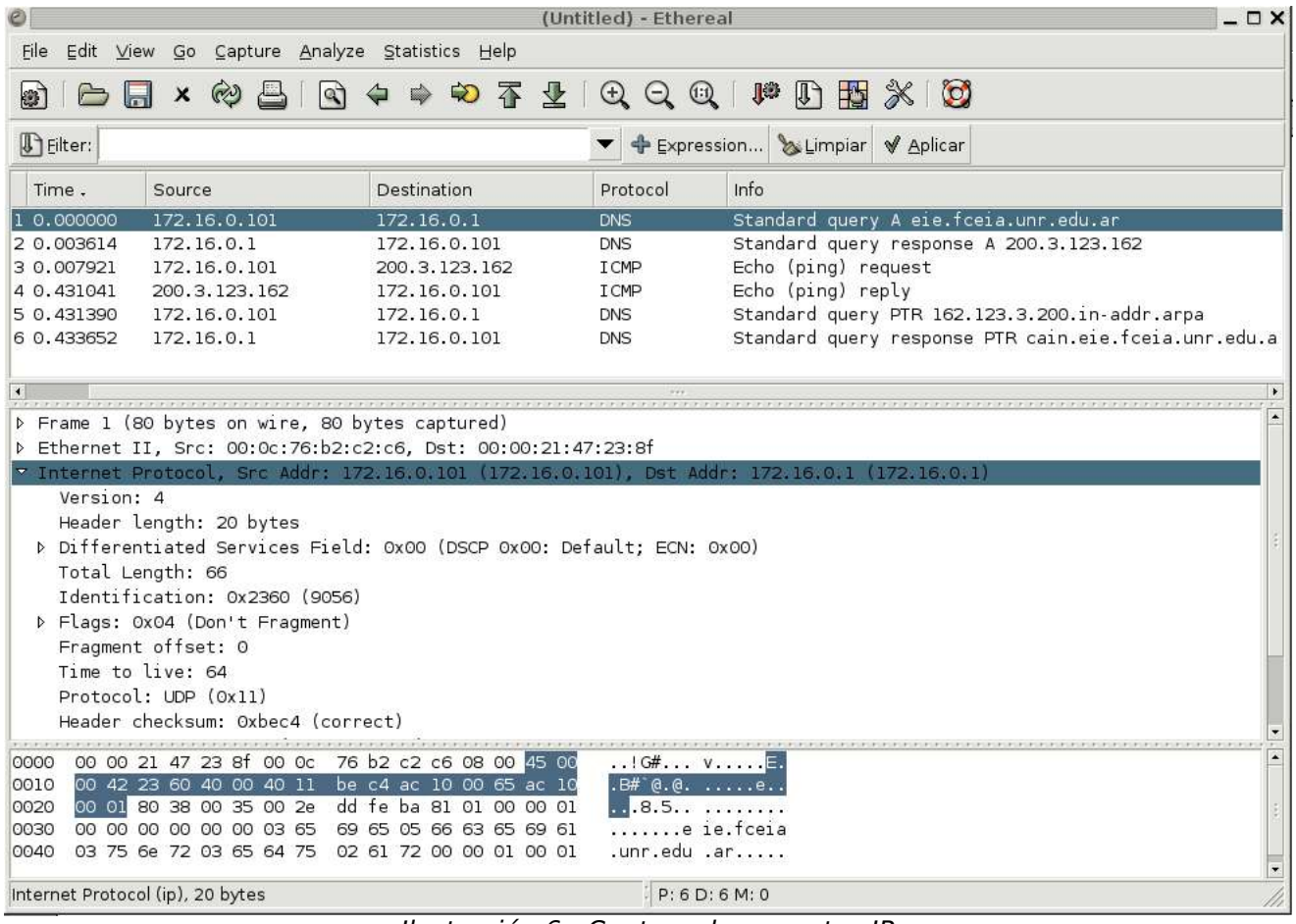

Ilustración 6 - Captura de paquetes IP

Haciendo click derecho sobre el tercer paquete IP, lo abrimos en ventana nueva (*Show packet in New Window*).

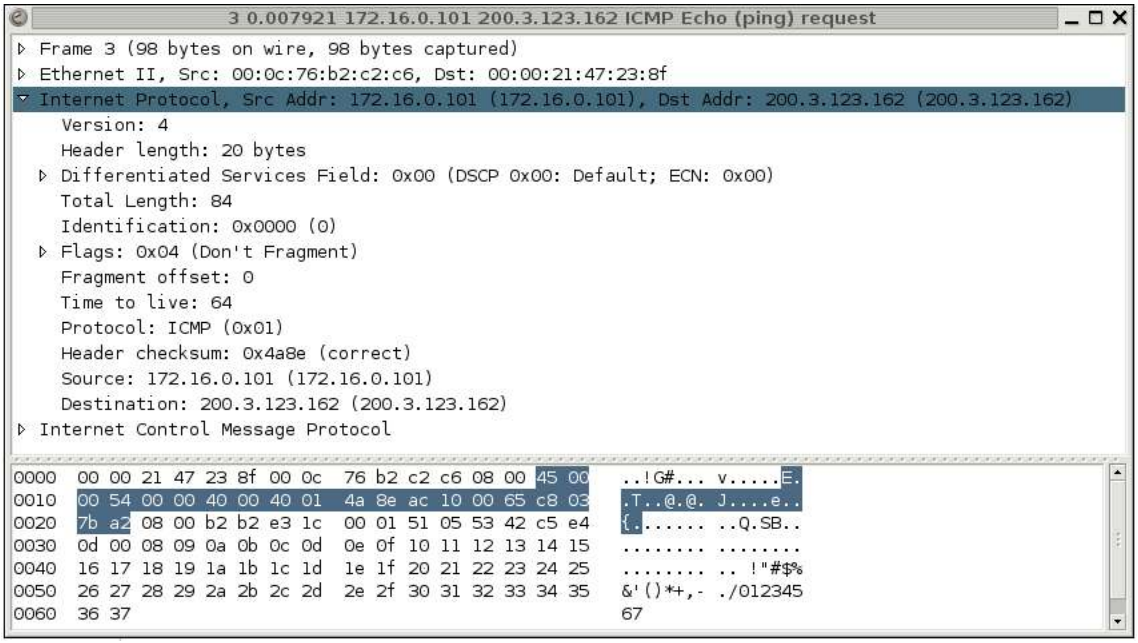

Ilustración 7 - Detalle de paquete IP

Con la ayuda de una calculadora científica, es posible convertir los datos hexadecimales y verificar los datos mostrados. Especialmente, podemos destacar el valor de la dirección IP

origen, la dirección IP destino, el protocolo de la zona de carga (en este caso ICMP).

```
Source IP Address: ac 10 00 65 (172 16 0 101)
Destination IP Addres: c8 03 7b a2 (200 3 123 162)
Protocol: 01 (ICMP)
```

4.2.- Datagramas TCP

Un datagrama TCP es encapsulado en un paquete IP, como muestra la siguiente figura:

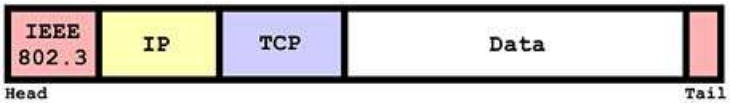

Ilustración 8 - Encapsulado de TCP en IP

La estructura de un datagrama TCP la podemos ver en la siguiente ilustración.

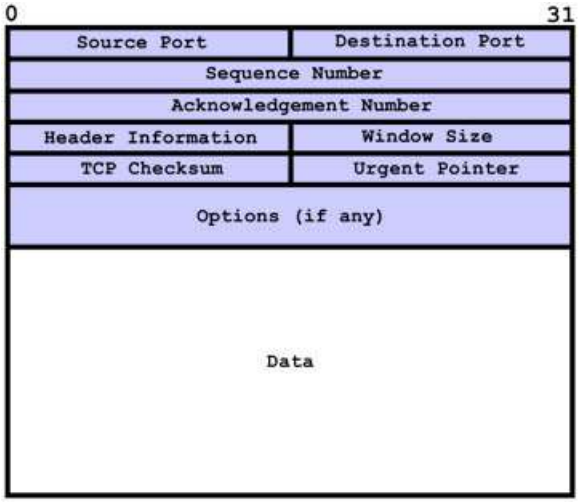

Ilustración 9 - Estructura de un datagrama TCP

Para analizar los datagramas TCP, iniciaremos una sesión *telnet*[5] a lucre.fceia.unr.edu.ar, el cual es un servidor de correo electrónico destinado a estudiantes de la FCEIA.

Iniciamos en Ethereal una nueva captura apretando *Ctrl+K.* Desde la línea de comandos, ejecutamos:

```
host:~$ telnet lucre.fceia.unr.edu.ar
```

Ingresamos *alumno* como nombre de usuario y *123456* como contraseña. En este punto detenemos la captura.
En la ventana principal de Ethereal, ordenamos la lista de datagramas por *Protocol* y hacemos click derecho sobre cualquier paquete que sea del tipo TELNET y seleccionamos Seguir flujo TCP (*Follow TCP Stream*).
En este momento podemos ver una nueva ventana donde vemos en texto plano los datos intercambiados entre los dos equipos, en color rojo el tráfico saliente y en azul el entrante.

5 Telnet es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se accedía debe tener un programa especial que reciba y gestione las conexiones. Sólo sirve para acceder en modo terminal. La conexión se establece utilizando TCP en el puerto 23.

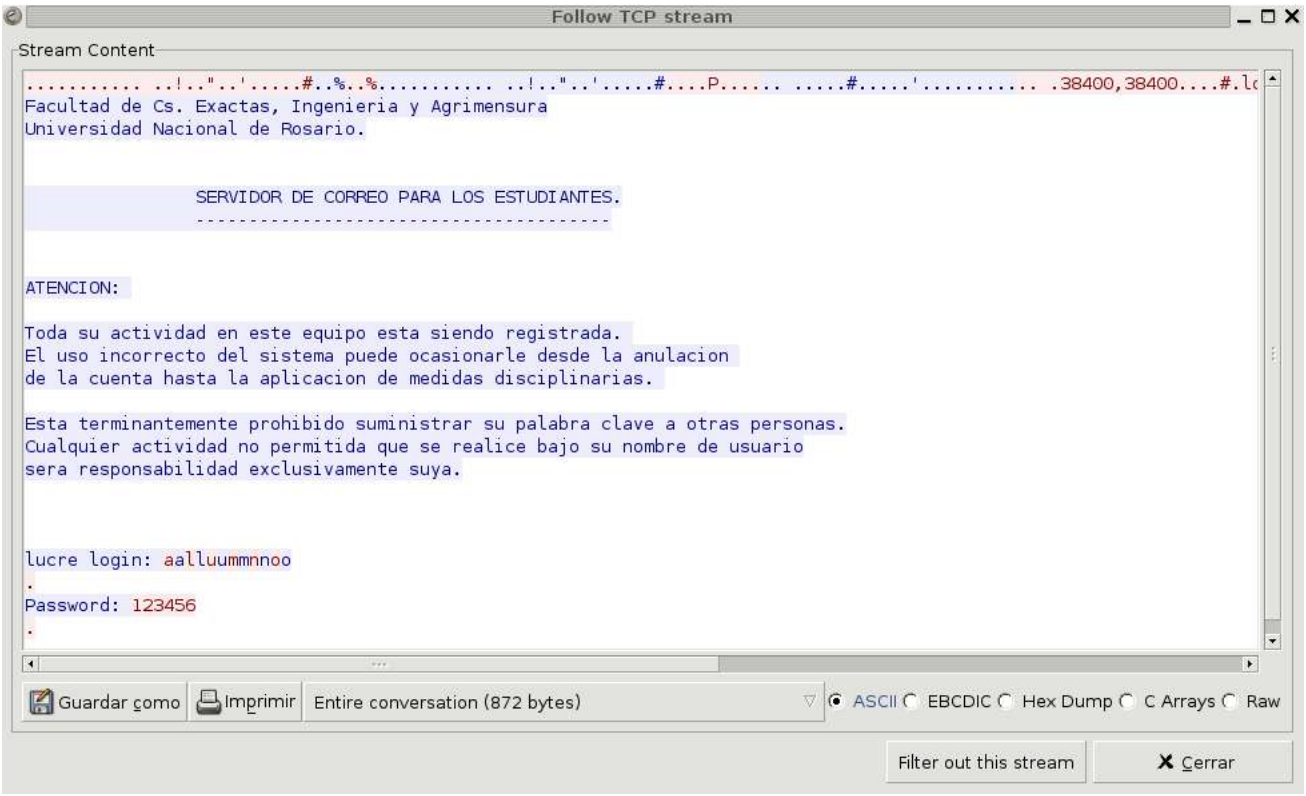

Ilustración 10 - Volcado de sesión telnet

Haciendo click en Filtrar este flujo (*Filter out this stream*) se aplica automáticamente un filtro de vista que elimina la sesión telnet y deja visible el tráfico restante.

Si invertimos el filtro

```
!((ip.addr eq 172.16.0.101 and ip.addr eq 200.3.123.30) and (tcp.port eq 33161 and tcp.port eq 23))
```

eliminando el signo de admiración y aplicamos este cambio, tenemos filtrado todo el tráfico restante, quedando sólo visible nuestro objeto de análisis.

Abriendo cualquier paquete en una nueva ventana, podemos ver los datos que contiene el paquete IP y parámetros que definen la conexión TCP.

```
Source IP Address: ac 10 00 65 (172 16 0 101)
Destination IP Addres: c8 03 7b a2 (200 3 123 130)
Protocol: 0x06 (TCP)
Source Port: 81 89 (33161)
Destination Port: 00 17 (23)
```

Analicemos ahora el establecimiento de la comunicación, conocido como *three way handshaking* [3].

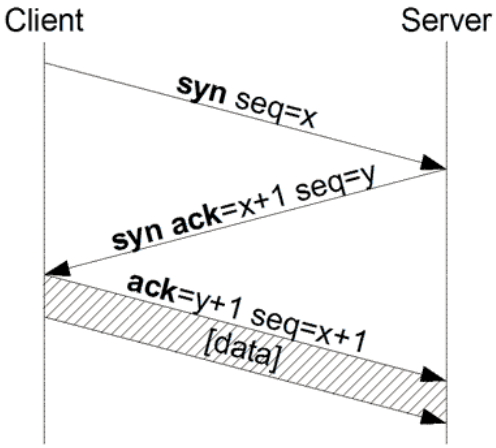

Ilustración 11 - TCP 3-Way Handshaking

Si abrimos en una nueva ventana los tres primeros paquetes podemos observar cómo se modifican los números de secuencia TCP.

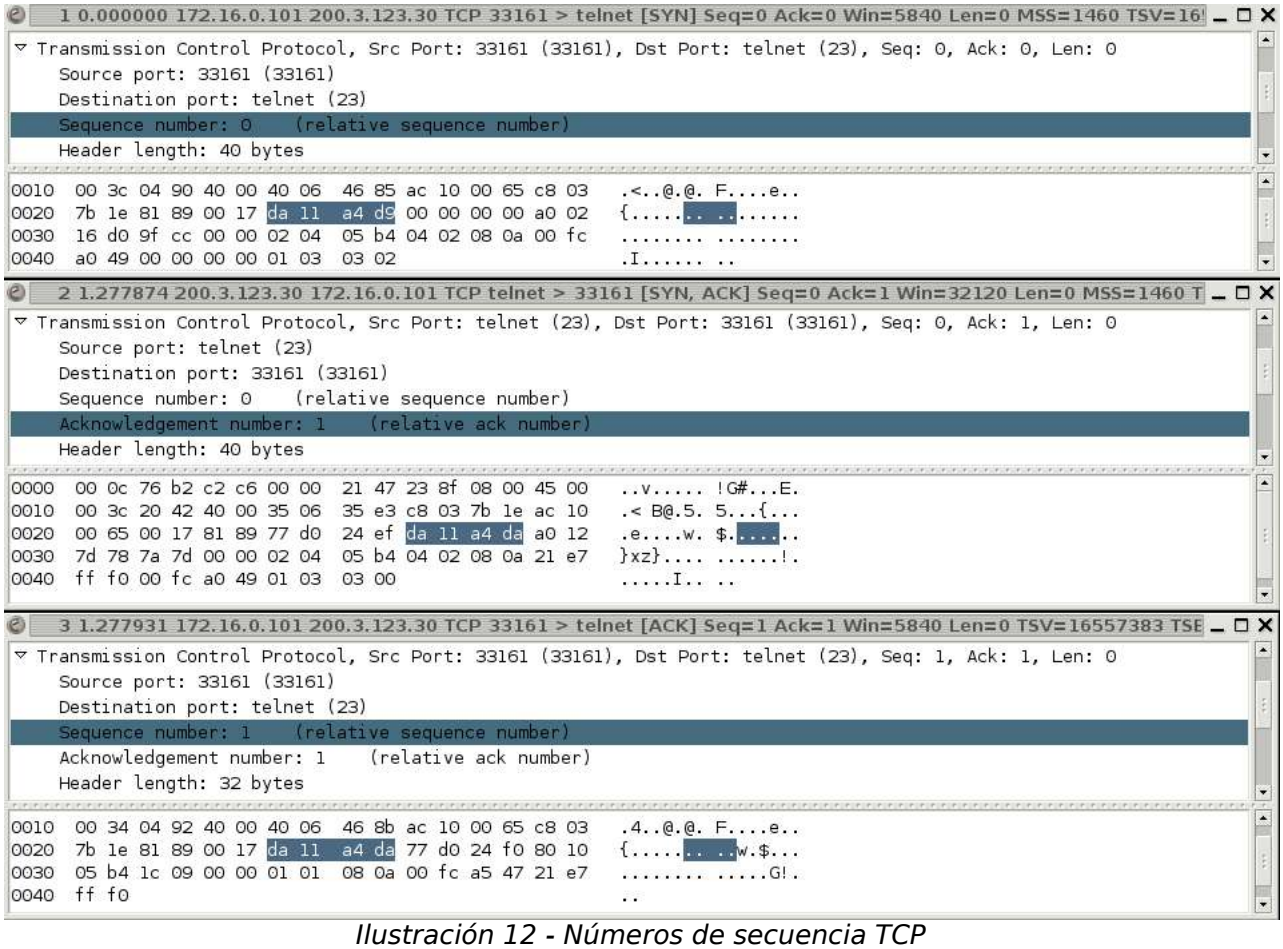

Ilustración 12 - Números de secuencia TCP

En la primera ventana, donde la bandera SYN está activada, vemos que el número de secuencia es 0xda11a4d9, que corresponde al número decimal 3.658.589.401. En la siguiente ventana, donde ambas banderas SYN y ACK se encuentran activadas, el número de secuencia es 0x77d024ef, que en formato decimal es 2,010.129.647 y el número de reconocimiento es 0xda11a4da, que equivale al número de secuencia del datagrama anterior más uno. El tercer datagrama, tiene sólo activada la bandera ACK, ya que se han inicializado las secuencias. En este último datagrama, el número de secuencia es

0xda11a4da y el número de reconocimiento es 0x77d024f0.

En los siguientes datagramas puede verse cómo se negocian las características de la sesión telnet, y a partir del datagrama 18 empiezan los datos que forman la pantalla mostrada en la página 9. Cabe destacar que los datos no son encriptados, y que cualquier sistema que se encuentre en la ruta de esta comunicación puede analizar la sesión, incluyendo el momento en que se transmite el usuario [20, 23, 26, 29, 32, 35] y la contraseña [43, 45, 47, 49, 51, 53].

En cambio, utilizando OpenSSH (GNU/Linux) o PuTTY [4] (MS Windows) para acceder a dicho servidor, a través del protocolo SSH[6], la comunicación no puede ser analizada por un nodo intermedio. Se muestra a continuación la ventana de sesión equivalente a telnet.

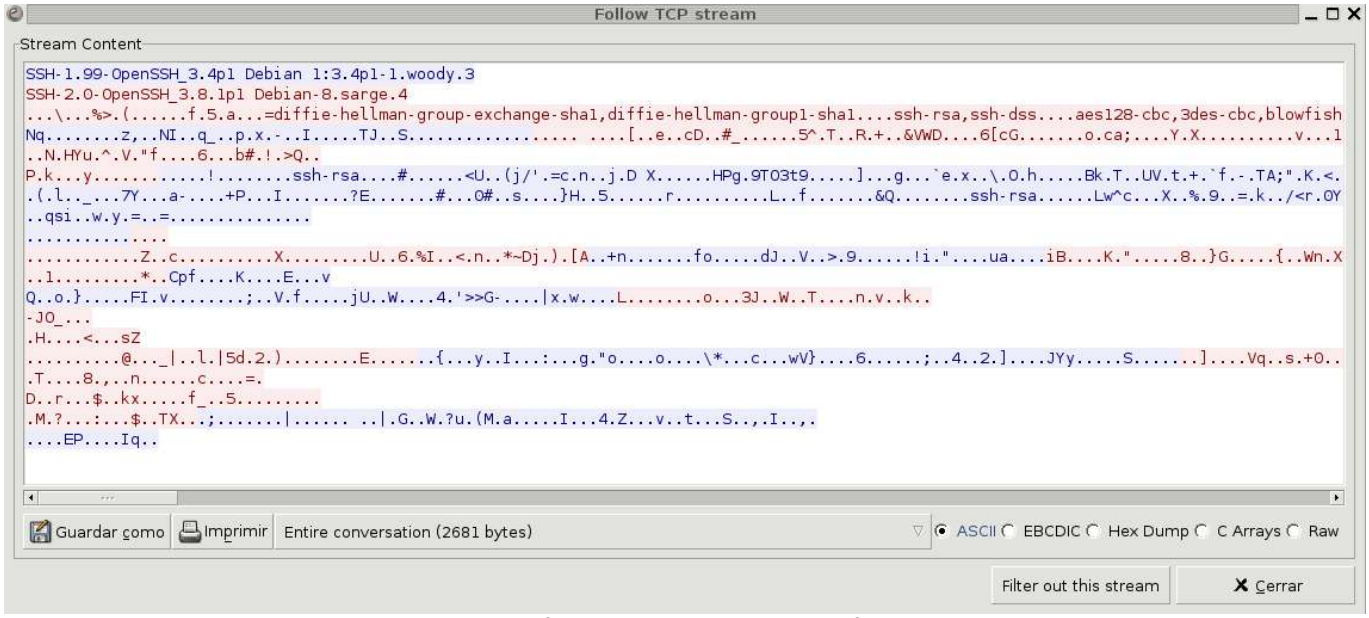

Ilustración 13 - Volcado de sesión SSH

Como podemos ver en la figura anterior, el tráfico es encriptado, y sólo pueden verse las versiones de los servidores OpenSSH utilizados (inclusive esto puede deshabilitarse del archivo de configuración del servidor OpenSSH).

4.3.- Datagrama UDP

Un datagrama UDP es encapsulado en un paquete IP, como muestra la siguiente figura:

Ilustración 14 - Encapsulado de UDP en IP

La estructura de un datagrama UDP la podemos ver en la siguiente ilustración.

6 SSH se utiliza para acceder a máquinas a través de una red, de forma similar a como se hacía con telnet. La diferencia principal que se usa encriptación para que ningún atacante pueda descubrir el usuario y contraseña ni lo que se escribe durante la sesión; aunque es posible atacar por medio de ataques de otros tipos. Al igual que telnet, sólo permite conexiones tipo terminal de texto.

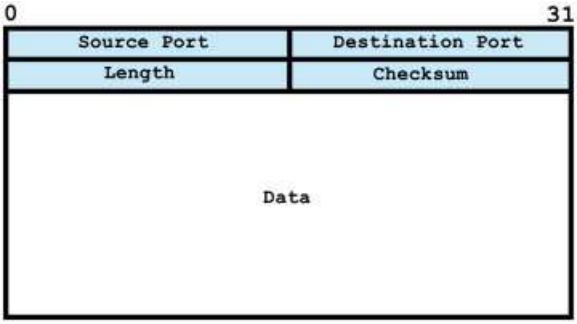

Ilustración 15 - Estructura de un datagrama UDP

Para analizar los datagramas UDP, haremos una consulta DNS[7], que utiliza el transporte antes mencionado, utilizando el puerto 53. Iniciamos la captura de paquetes mediante el acceso rápido Ctrl+K, y en una consola de texto, ejecutamos el siguiente comando:

```
host:~$ nslookup www.eie.fceia.unr.edu.ar 200.3.123.162
```

```
c:\windows
nslookup> server=200.3.123.162
nslookup> www.eie.fceia.unr.edu.ar
```

donde hacemos una petición de resolución de nombre de la dirección www.eie.fceia.unr.edu.ar al servidor DNS 200.3.123.162, que es la dirección IP del mismo. O sea, le estamos pidiendo a dicho servidor que se resuelva a sí mismo.

Abriendo estos dos paquetes IP capturados en una nueva ventana, podemos ver la siguiente figura:

7 DNS (Domain Name System) es un conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

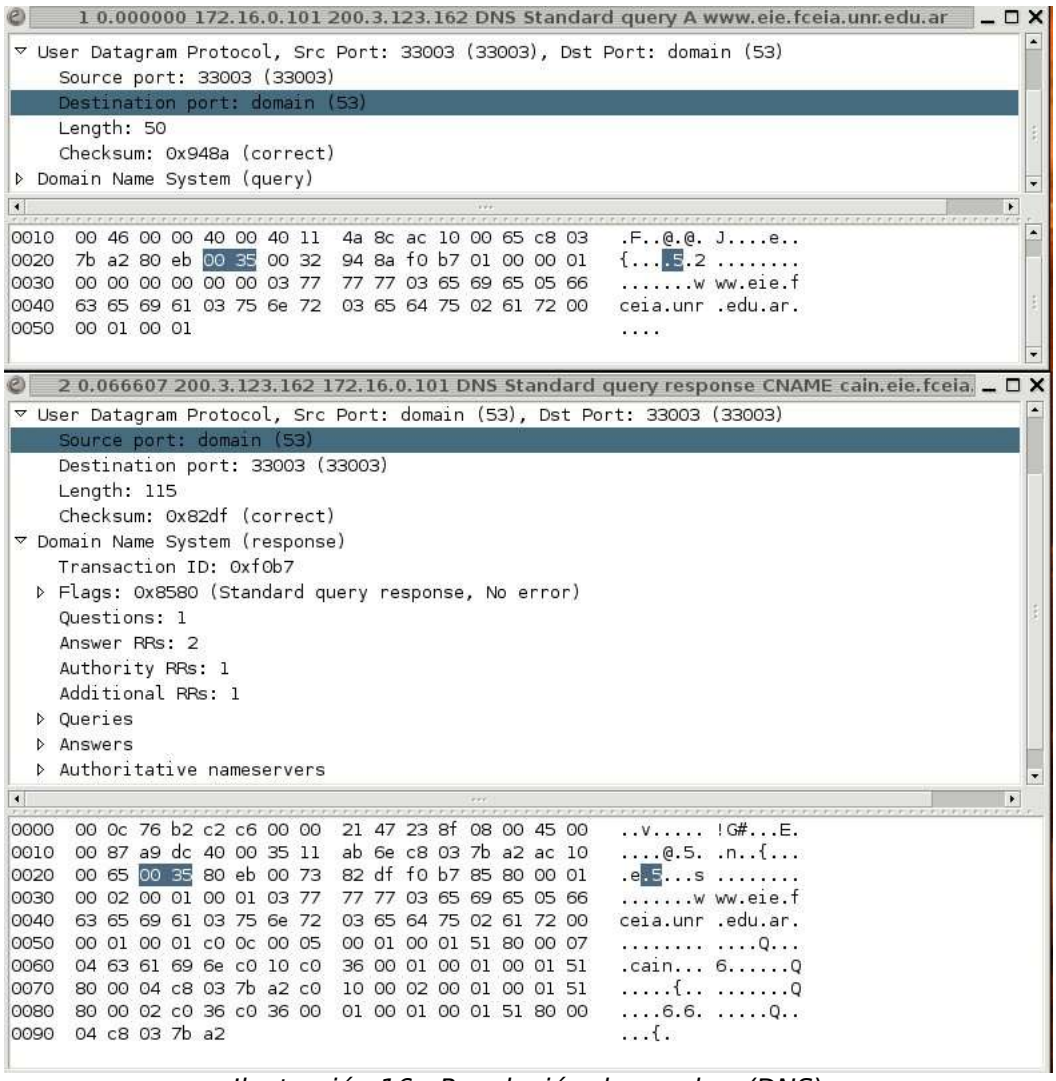

Ilustración 16 - Resolución de nombre (DNS)

Comparando el esquema y el volcado de los datagramas, podemos ver:

```
Source IP Address: ac 10 00 65 (172 16 0 101)
Destination IP Addres: c8 03 7b a2 (200 3 123 162)
Protocol: 01 (ICMP)
Source Port: 80 eb (33003)
Destination Port: 00 35 (53)
```

5.- Información complementaria

El analizador de protocolos Ethereal permite guardar las capturas realizadas para su posterior análisis, incluso en equipos diferentes a donde se produjo la captura. Desde la página web de Ethereal pueden descargarse ejemplos diversos de capturas.
http://wiki.ethereal.com/SampleCaptures

Por otro lado, un completo manual de usuario puede descargarse desde aquí:
http://www.ethereal.com/distribution/docs/user-guide.pdf