Asignatura: Teleinformática y Comunicaciones

TP – Sniffer *WireShark*

Objetivos:

- Familiarizar al estudiante con una herramienta fundamental para el análisis de redes
- Estudiar detalladamente los protocolos más comunes usados en TCP-IP
- Presentar los distintos problemas de seguridad que presenta la suite TCP-IP

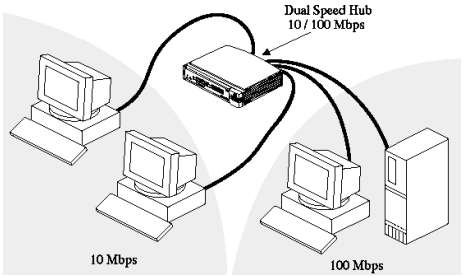
Conocimientos previos:

Para la realización de este TP se considera necesario tener una idea del funcionamiento básico de los protocolos: IEE802.3, ARP, RARP. IP, ICMP, IP, UDP y TCP.
Se recomienda para ello la lectura de **TCP IP** *de Douglas Comer* Capítulos 1 al 13.
Como material complementario: **TCP IP Ilustrated** *de Stevens*, **Redes De computadores** *de A. Tanenbaum*.
Se cuenta también con el *Video explicativo* sobre como iniciar el trabajo con el WireShark del **Ing. Daniel Xinos**, profesor adjunto de la cátedra de Teleinformática y Comunicaciones.

Intro Teórica:

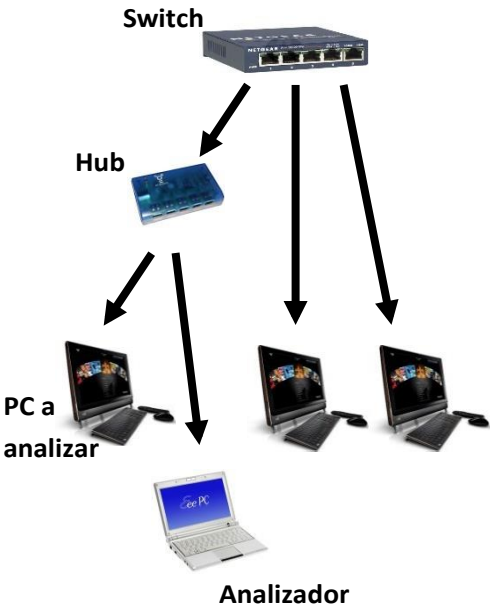
La herramienta básica aquí empleada permite ver los paquetes que circulan por la red y son intercambiados por los protocolos.

Estamos por iniciar un análisis de tráfico y una de las primeras preguntas a contestar será: ¿Donde hacerlo? y eso dependerá de la configuración de nuestra red. Si nuestra red esta armada con Hubs (actualmente poco probable que esto ocurra) estamos en el mejor de los escenarios posibles pues en todos los puertos del hub están presentes todos los paquetes que circulan por la red.



En este caso basta con instalar el sniffer en cualquiera de las máquinas y analizar el tráfico que por la interfaz pasen.

Normalmente no tendremos tanta suerte y lo que habrá será un **Switch** donde cada puerto forma un dominio de colisiones distinto. Una solución es poner un **hub** en la línea donde está la máquina que se desea analizar. Ver dibujo.



Como se ve en el dibujo, la máquina con el sniffer está ahora en posibilidad de capturar todos los paquetes dirigidos o generados por la PC a analizar.

Otra posibilidad es la llamada " Port Mirroring" esta técnica, que debe ser soportada por el Switch, permite que el tráfico de uno o más puertos este también presente en el puerto que queramos.

> *En lo que a la práctica se refiere no tendremos problemas pues analizaremos la misma máquina que tiene cargado el* ***WireShark****.*

Software:

Emplearemos el software conocido como **WireShark,** que se puede bajar desde su página de Internet www.wireshark.org No presenta dificultades para su instalación y en la misma página se encuentran videos y material explicativo de su funcionamiento

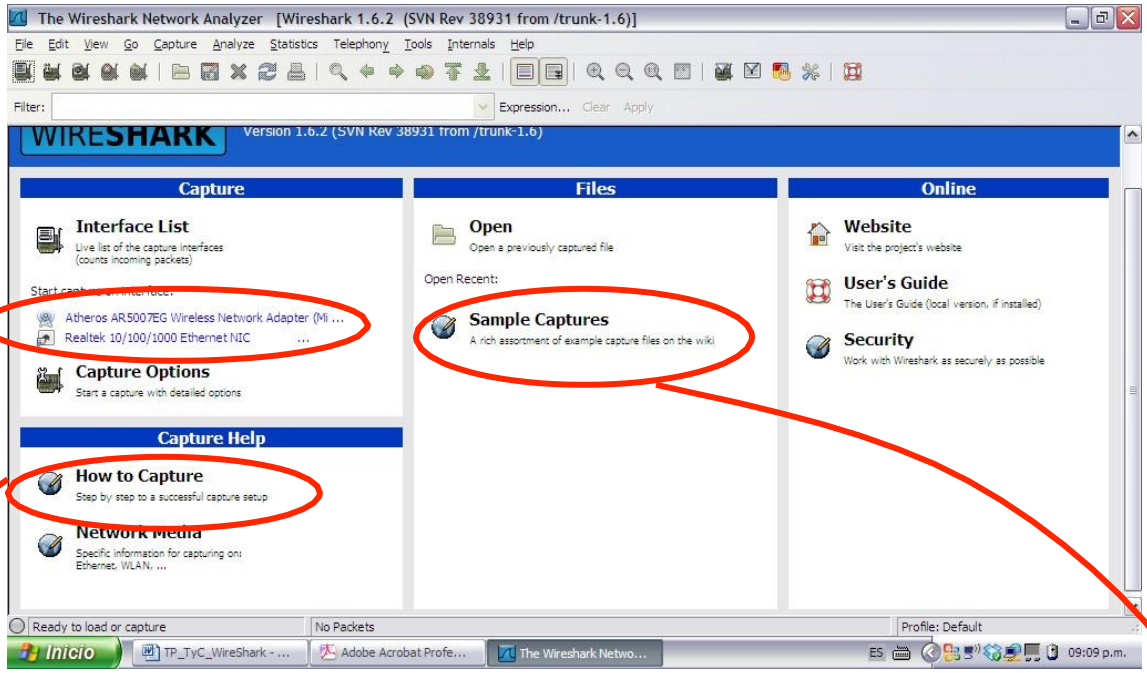
Los TPs que se dan a continuación fueron desarrollados en base a lo presentado en el libro **Computer Networking: a Top Down Approach** *de Kurose y Ross*.

Las prácticas fueron desarrolladas para la asignatura **Teleinformática y Comunicaciones** del 3er año de la carrera de **Ingeniería en Sistemas Informáticos** de la **facultad de Tecnología Informática** de la **Universidad Abierta Interamericana**.

Introducción Práctica.

Los TPs tiene la finalidad de permitir una interacción profunda con los protocolos los cuales serán ¨*vistos en acción*¨ cuando intercambian mensajes.
Tal como se estudió en las clases los protocolos tiene una implementación normalmente caracterizada por un **header** y un **payload** de tamaño especificado, de forma que cada bit tiene un significado único y reconocible. Los sniffer tienen como funcionalidad ¨*olfatear*¨ la red y presentar la combinación de ceros y unos que por ella viajan de forma tal que sean fácilmente identificables.

Una vez iniciado el sniffer (en este caso el **WireShark Legacy**) tendremos una pantalla como la indicada a continuación.

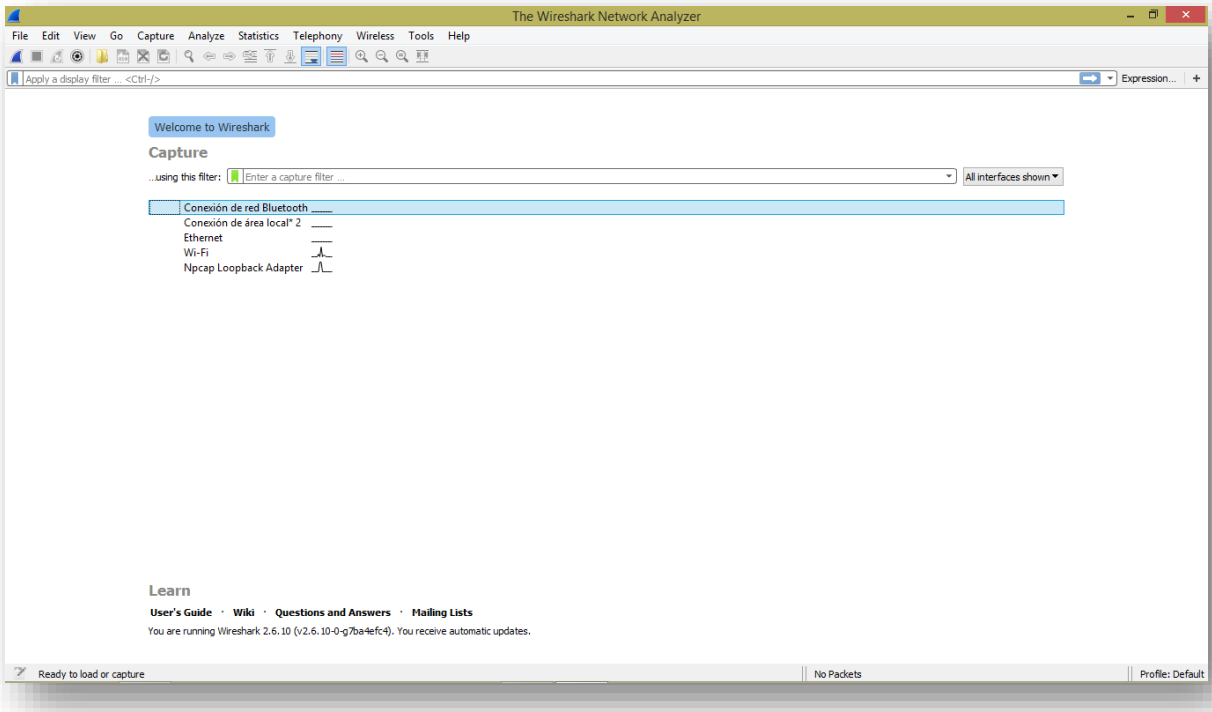


Aquí tenemos la posibilidad de acceder al **Help on line** (dado que se trata de un software que se volverá a emplear en asignaturas de redes de 5to año y que además es de mucho interés para aquellos que en su vida profesional trabajaran con redes de comunicaciones parece una buena práctica hacer una recorrida por el),

Una buena forma de aprender *en profundidad* el funcionamiento de los protocolos es analizarlos cuando están en ejecución, ver el contenido de sus header y la forma en que mueven la información

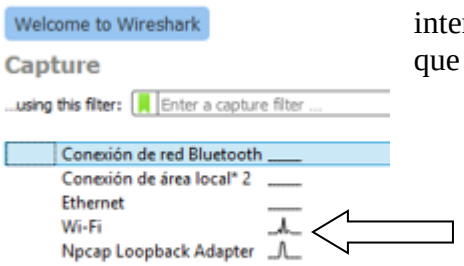
Para iniciar con la captura debe elegir previamente la **interface** en la cual se capturarán los paquetes. Hay placas Wireless que les cuesta entrar en *modo promiscuo*, que es el modo en que aceptan cualquier paquete, aunque no estén dirigidas a ellas.

Si en lugar de la **versión legacy** de la figura anterior, opta por la versión actual (2.6.10 al momento de este TP) la pantalla será la que se indica

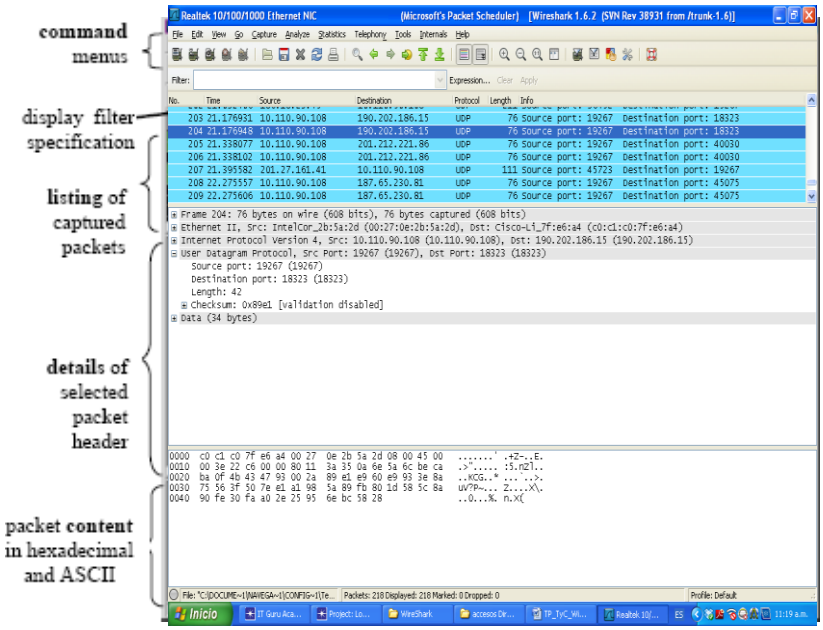


En cualquier caso, luego de unos momentos tendremos una pantalla como la indicada abajo. (en algunas versiones legacy debe dar clic en start).

De aquí en más nos manejaremos con la **versión 2.6.10**

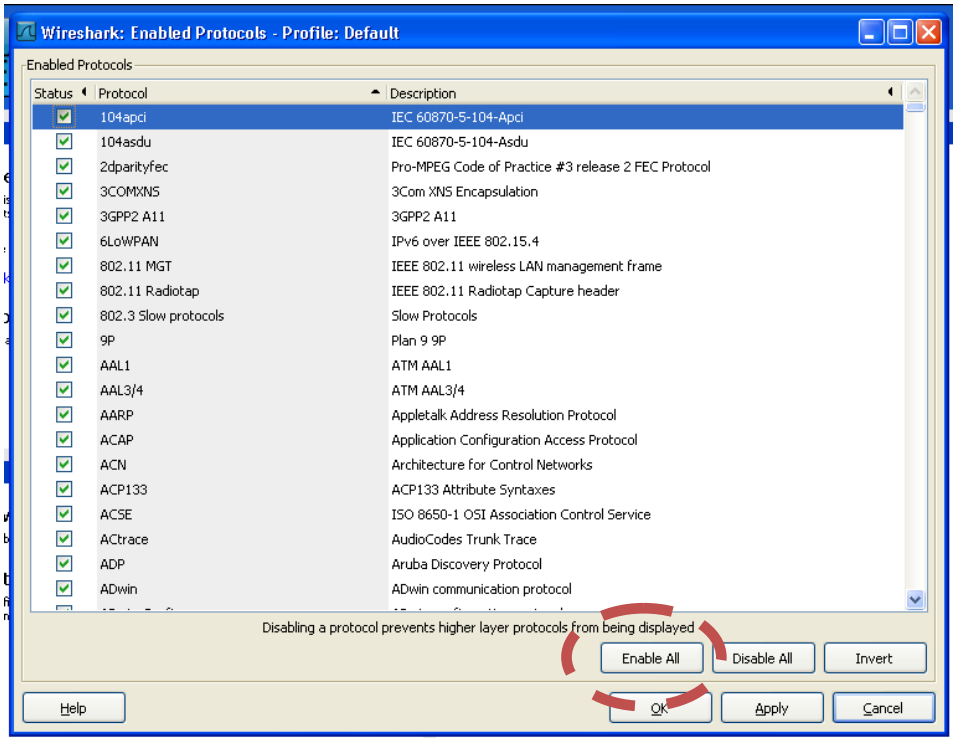


Como estoy con una conexión WiFi doy clic sobre esa interfaz (si está en una red cableada lo más probable es que deba hacer clic sobre Ethernet)

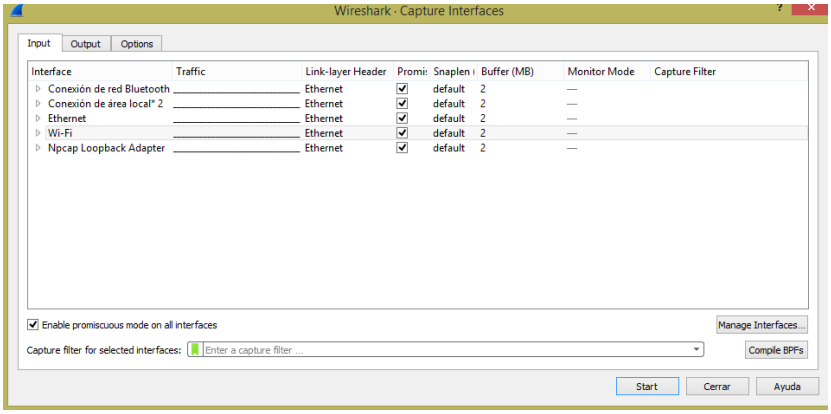


En la figura se observan las distintas áreas de trabajo del Sniffer, no parece conveniente ahora dar el significado de cada una sino se ve como más indicado que se aprenda a medida que vamos trabajando con el TP.

Antes de comenzar, acceda a la pestaña “Analize”, y vaya a la opción “Enabled protocols”, y tilde “Enable All”, como se ve en la siguiente figura:



Accediendo al menú opciones nos encontraremos con más posibilidades de trabajo, por ahora basta con dejar las opciones por default



En caso de estar en modo captura, deténgala.

`Capture` ➔ `Stop`

Antes de nada, anotemos datos de nuestra máquina, para ello tecla:

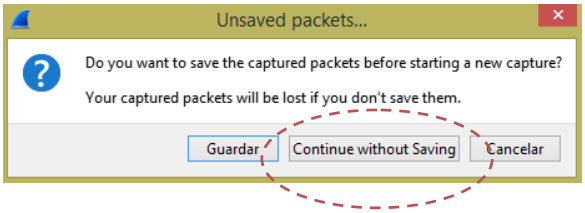
`Windows + R` ➔ escriba en el cuadro de texto `cmd`, y luego `ipconfig`.

Dirección IP IPv4: _____

Mascara de subred: _____

Puerta determinada IPv4: _____

Comencemos a trabajar. Inicie una nueva captura sin guardar



Puede ocurrir que la pantalla comience a capturar paquetes no deseados … ignórelos

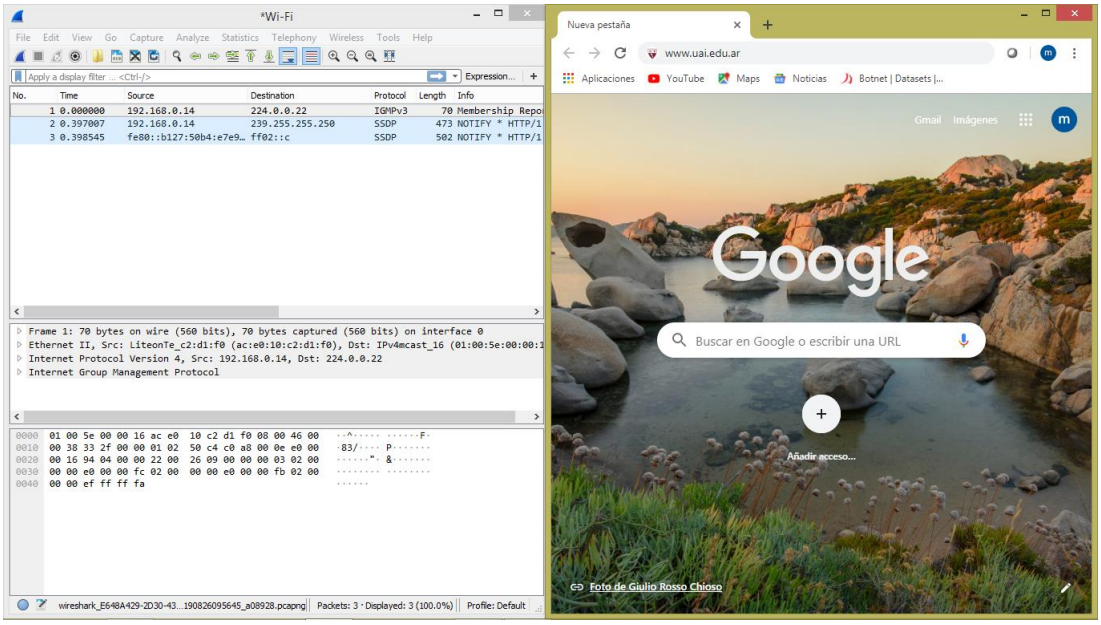
Ingresemos a nuestro browser, por ejemplo, la dirección:

www.uai.edu.ar

Al presionar ENTER se lleva a cabo a una conexión con el servidor http de la página solicitada, una vez que la pagina este en el browser detenga la captura de paquetes.

Muy posiblemente se encuentre Ud. con que la cantidad de paquetes capturados sea demasiado grande y difícil de manejar. Veamos algunas posibles soluciones.

Mas sencilla y menos eficiente: Abra en paralelo en la pantalla el Browser y el Wireshark de forma tal que pueda pasar rápidamente de uno a otro.



- *Escriba en el browsr* [*www*.uai.edu.ar](http://www.uai.edu.ar) (NO LO INGRESE AUN)
- *Inicie la captura en Wireshark*
- *Inicie la conexión de browser*
- Cuando termine la carga de la página, detenga el wireshark

Se tendrá una pantalla muy parecida a la ya mostrada como ejemplo, en la cual entre otras capturas se encontrarán las http buscadas, para simplificar la visualización escriba **http** dentro del campo filtro y oprima el botón *apply*. Solo se mostrarán los paquetes http.

Dado que podemos filtrar no es realmente necesario hacer el procedimiento de ventanas en paralelo antedicho aunque facilita la tarea.

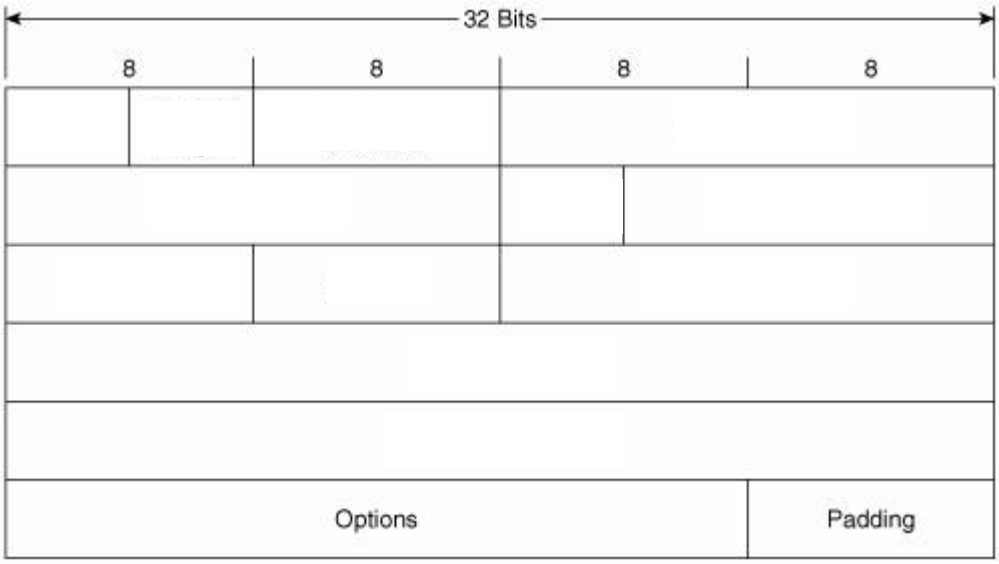
Puede ocurrir que vea muy pocos paquetes (o ninguno), los motivos más usuales son:

- Ya tiene la página cargadas en cache ….. Bórrelo (*Borrar historial*)
- Tiene seguimiento de conversaciones …. Anularla. (Analize ➔ *Folow*)

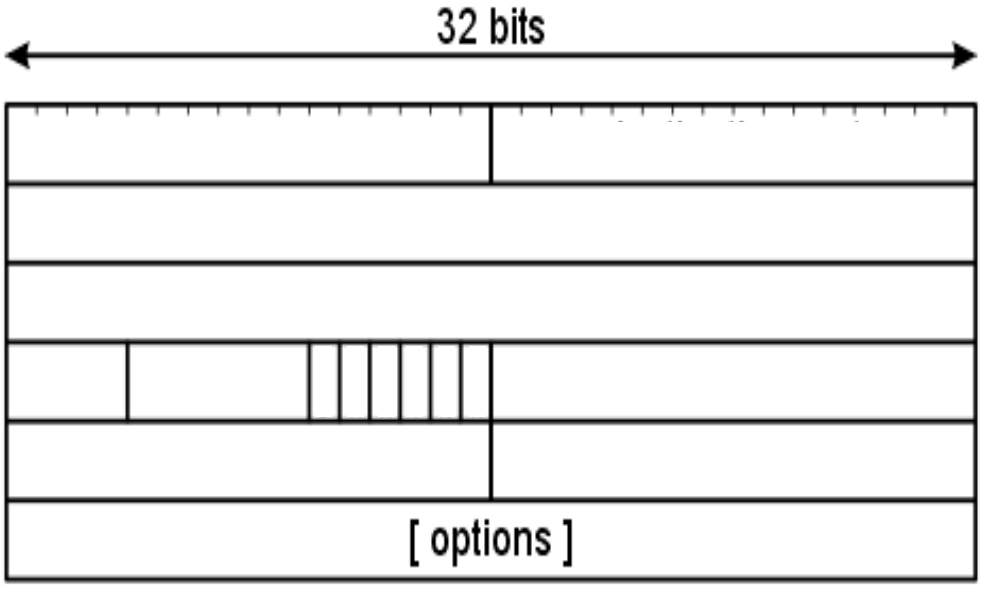
Seleccione el primer paquete http que deberá ser un **HTTP GET** enviado desde nuestra maquina al servidor. De esta manera se puede ver en detalle tanto la **trama ETHERNET** como el **paquete IP** y el **segmento TCP** y el **mensaje HTTP** con solo presionar el botón +.

Complete los Header con los **valores obtenidos**.

IP



TCP



Cuestionario

1. ¿Qué protocolos aparecen en el listado? ¿Qué función cumple cada uno? Liste 5. Posiblemente deba quitar toso los filtros.

Protocolo	**Función**

PARTE 1

Ethernet y ARP

Con lo visto ya estamos en condiciones para empezar a trabajar.

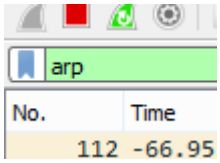
Primeramente, vacié el buffer del explorador (la forma de hacerlo varía según el explorador usado).

Prepare el sniffer para una nueva captura y visite

http://es.wikipedia.org/wiki/Argentina (o cualquier página que prefiera) .

Solo verifique que no se trata de un sitio seguro.

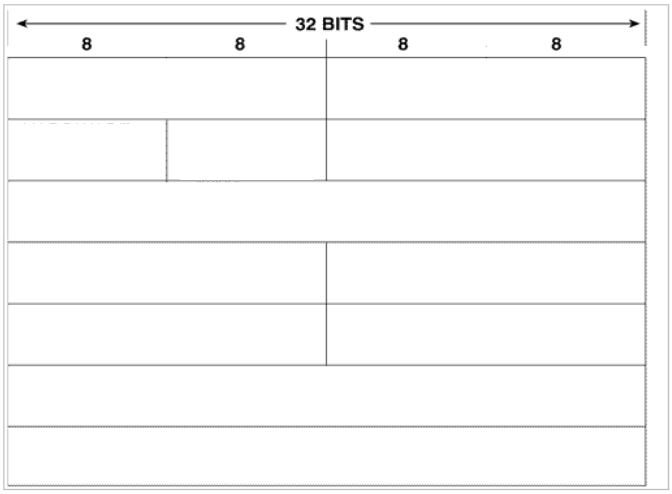
Dado que nos interesa únicamente **ARP**, lo escribimos en la línea de filtros,



Cuide escribir en minúscula y que el fondo de color verde

De la captura ARP elija dos consecutivos (Pedido – Respuesta)

Complete el contenido de los campos.

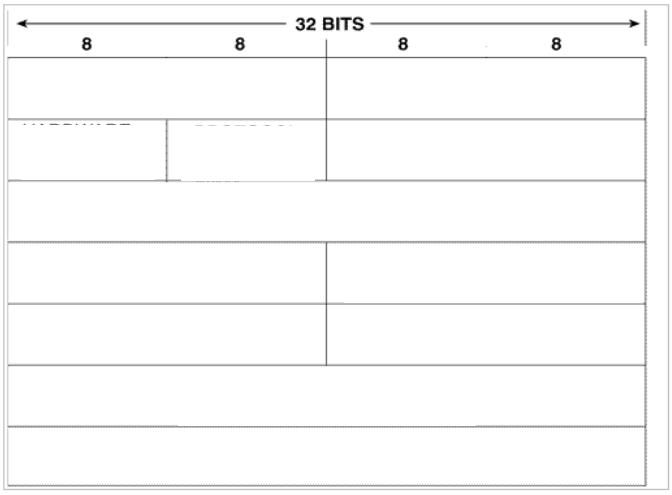


Pedido ARP

Complete con los valores de cada campo

Cual es la MAC Origen:
La IP Origen:

La MAC destino:
La IP destino:



Respuesta ARP

Complete con los valores de cada campo

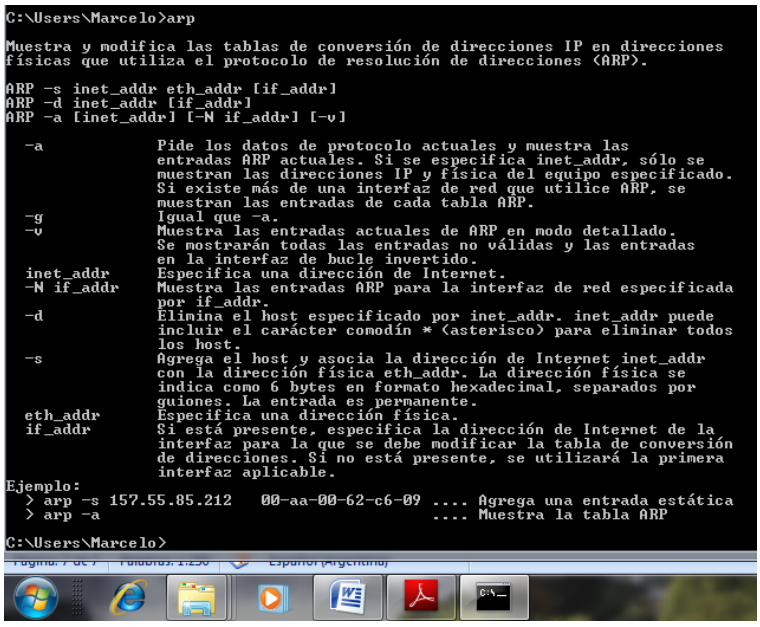
Cuál es la MAC Origen:
La IP Origen:

La MAC destino:
La IP destino:

Veamos ahora el funcionamiento del **protocolo ARP**.

Comencemos distinguiendo el **comando ARP** cuya función es visualizar y manipular el contenido del cache ARP, del **protocolo ARP** que define los formatos y contenidos de los mensajes que se intercambian.

En **Windows** se encuentra en *c:\windows\system32\arp*. También puede entrar en la línea de comandos y tipear *arp* sin argumento para ver todas las opciones.



Se sugiere leer detenidamente cada una de las opciones y familiarizarse con su funcionamiento mediante la ejecución de los comandos

Escriba el contenido que obtiene Ud. al tipear ***arp –a*** en la línea de comandos de su PC. Indicando el significado de cada campo. En caso de tener una tabla muy extensa transcriba solamente algunas entradas.

¿Contiene el mensaje pedido ARP la dirección IP del Origen? _____

Tareas Complementarias. Busque en el drive el caso de estudio ***ethernet-ethereal-trace-1*** cárguelo en el sniffer y responda:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	startron > ipp [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	startron > ipp [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	startron > ipp [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	nim > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	http > nim [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	nim > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	http > nim [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	[TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	[TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	nim > http [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	[TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	nim > http [ACK] Seq=633 Ack=4816 Win=64240 Len=0

*El primer y segundo paquete **ARP** del caso de estudio corresponde al pedido de **ARP** enviado por el PC que corre WireShark y la respuesta **ARP** correspondiente. Pero hay otro computador en la red, como se indica en el paquete 6 – otra solicitud **ARP**. ¿Por qué no tiene respuesta?*

Más preguntas generales

1. ¿Cuál es el comando que permite el ingreso manual de resoluciones de **IP** en **MAC** en el cache **ARP**? ¿Qué pasaría si por error se ingresa la **IP** correcta con la **MAC** incorrecta?

2. ¿Cuál es el tiempo que permanece un dato cargado en el cache ARP? Indique el método usado para contestar esta pregunta.