Sniffing

By: Alfa-Omega

Introduccion

En este manual explicare que es el sniffing, como usar un sniffer y que usos le podemos dar, ademas expondré una serie de ejemplos para que veais como trabaja un sniffer.

(para entender algunas partes de este manual es necesario tener algunos conocimientos sobre redes)

Bien, empezemos…

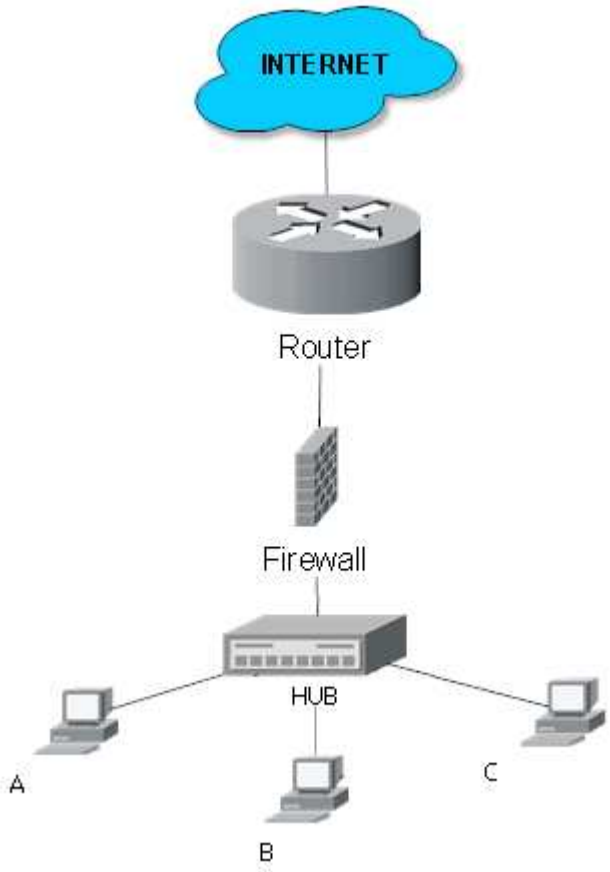
Que es el sniffing ???

El sniffing es la técnica por la cual podemos ver los paquetes de datos que circulan por una red de area local (una red lan o wlan)

Para entenderlo mejor:

Imaginemos que en una red hay 3 pcs (A,B y C), entonces B y C empiezan a hablar entre ellos por medio de un chat, y A quiere saber que se están diciendo, entonces A pone un sniffer a la escucha para ver los paquetes de datos que se están mandando y asi poder saber que están diciendo…

Lo que pasa en verdad es lo siguiente:



Cuando los PCs B y C empiezan a hablar entre ellos, lo hacen por medio del HUB, pero uno de los inconvenientes que tiene el HUB es que manda los paquetes de datos a todos los hosts conectados a el, osea… que cuando B habla con C los paquetes que le manda no solo los recibe C sino que también los recibe A, pero el PC A rechaza el paquete de datos puesto que no le sirve para nada, pero si el PC A tiene un sniffer a la escucha entonces el sniffer acepta ese paquete de datos.

Ahora bien… si en vez de un HUB hubiese un SWITCH el sniffer no funcionaria (aunque hay otro tipo de técnicas para conseguir realizar sniffing aunque halla un SWITCH por el medio), porque el SWITCH es inteligente y solo manda los paquetes de datos al pc que los necesita.. en este caso solo se los mandaria a C.

Hay programas que detectan si hay algún sniffer a la escucha (por ejemplo antisniff) pero , OJO!!! estos programas no neutralizan el sniffer, lo único que hacen es detectar si alguien esta usando un sniffer.

Que uso se le puede dar al sniffing?

Pues usando la tenica del sniffing podemos conseguir contraseñas, (de webs, ftps ….etc) interceptar conversaciones, o simplemente investigar como funciona un programa…

Imaginemos que estas con un amigo en la misma red y sabes que tu amigo se va a logear en una pagina en la cual hace falta una cuenta para entrar, entonces cojes y pones un sniffer a la escucha e interceptas los paquetes que manda tu amigo para logearse, en esos paquetes que ha mandado tu amigo estarán su ID y su contraseña de la pagina en cuestión

pero el 90% de las webs lo que hacen es cifrar las contraseñas y después mandarlas.. osea, que cuando te hagas con los paquetes de datos lo mas seguro es que no te salga la contraseña como tal sino que saldrá un algoritmo, que tendras que crakear para saber la autentica contraseña.

Hay algunas webs que permiten la opción de recordar contraseña, cuando marcas esta opción lo que hace la web es crear un cookie con la información de tu cuenta, entonces la próxima vez que entres en la web se mandara el cookie con la información y te logeara automáticamente

Si en este caso ponemos un sniffer a la escucha e interceptamos el cookie lo único que tendríamos que hacer seria un cookie poison y ya tendríamos acceso a la web…

En resumen… podeis usar un sniffer para tantas cosas como se os ocurran, el limite esta en la imaginación..

Usando un sniffer

Ahora pondré un par de ejemplo sobre la utilización de un sniffer, en este caso utilizare el wireshark (uno de los mejores sniffers que hay..)

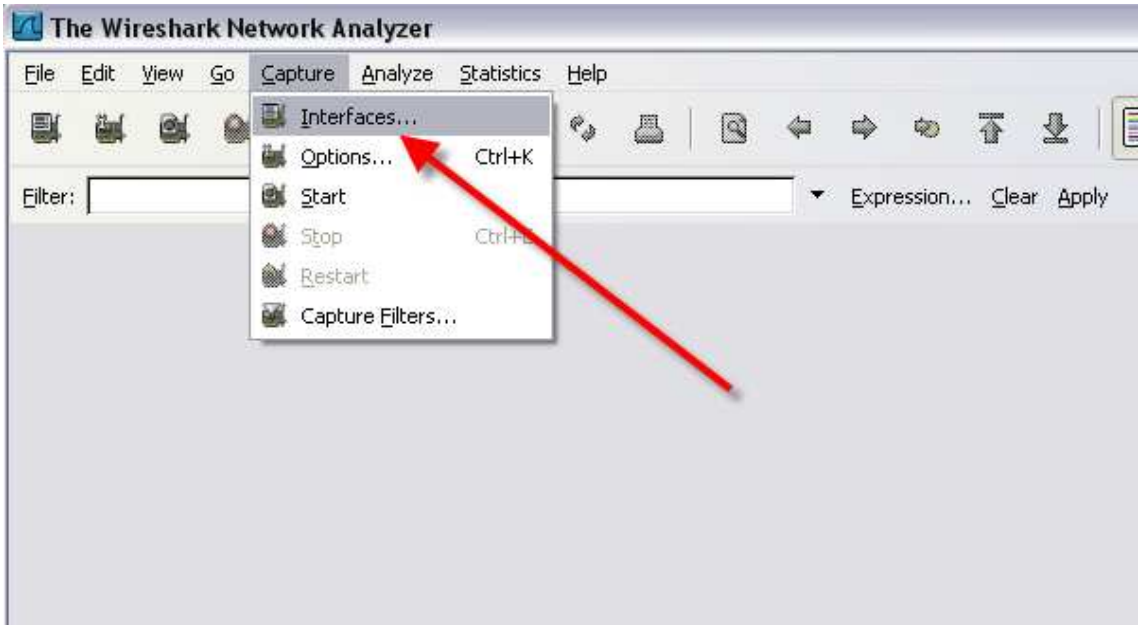
Antes de nada decir que para entender los paquetes de datos que muestra el sniffer hay que tener algunos conocimientos sobre paquetes de datos, flags, protocolos… etc

Observando la negociación de una conversación

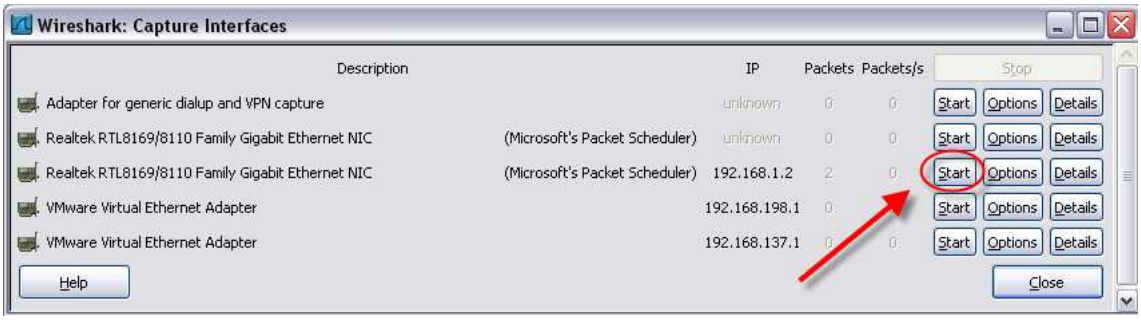
En este ejemplo veremos como se produce la negociación de una conversación

El programa que voi a usar para que envie los paquetes es un chat que cree hace un tiempo…

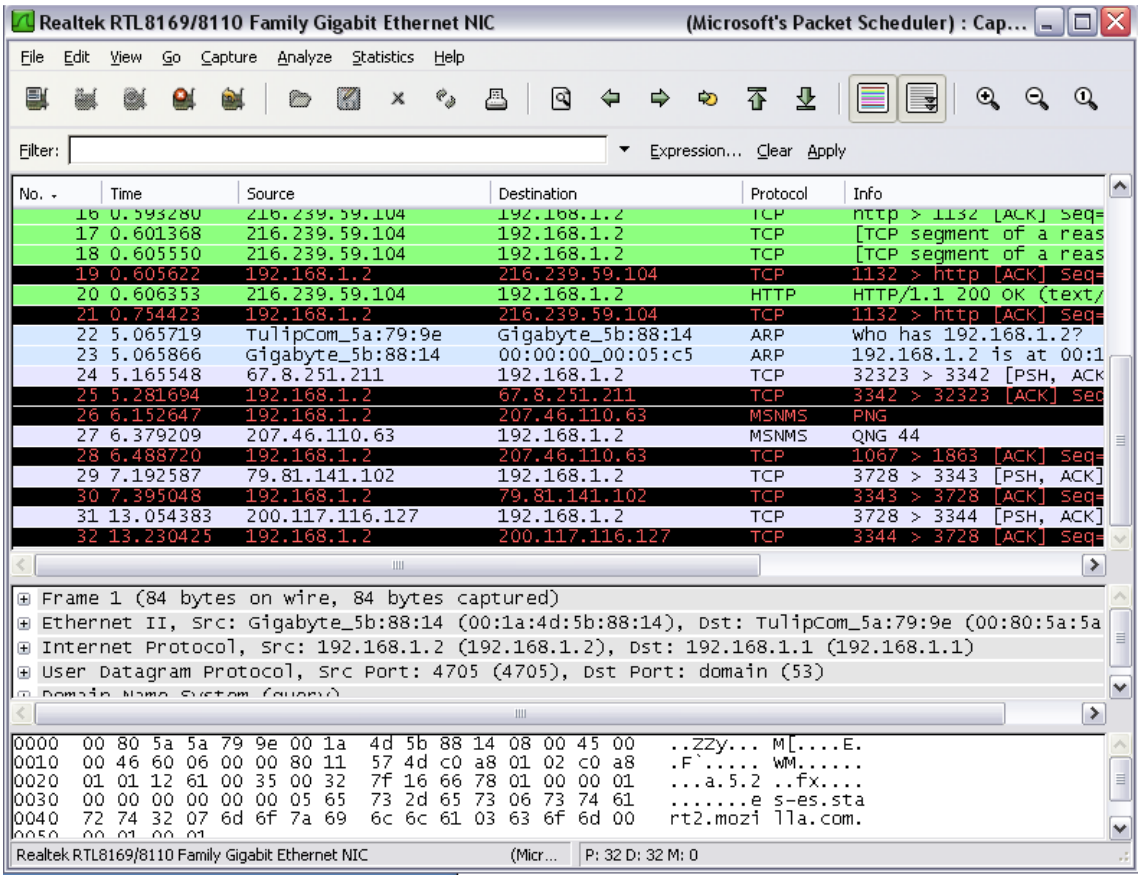
Bien, lo primero es abrir el sniffer y ponerlo a funcionar, para ello pinchamos en capture > interfaces



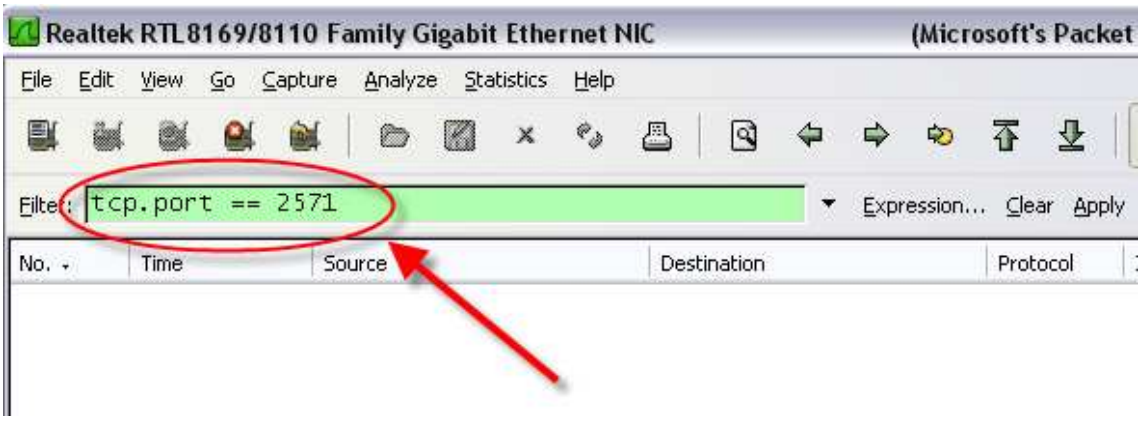
Y pinchamos start de la interfaz de la cual queremos capturar los paquetes, en este caso voi a sniffar desde el mismo pc que voi a mandar los paquetes de datos.



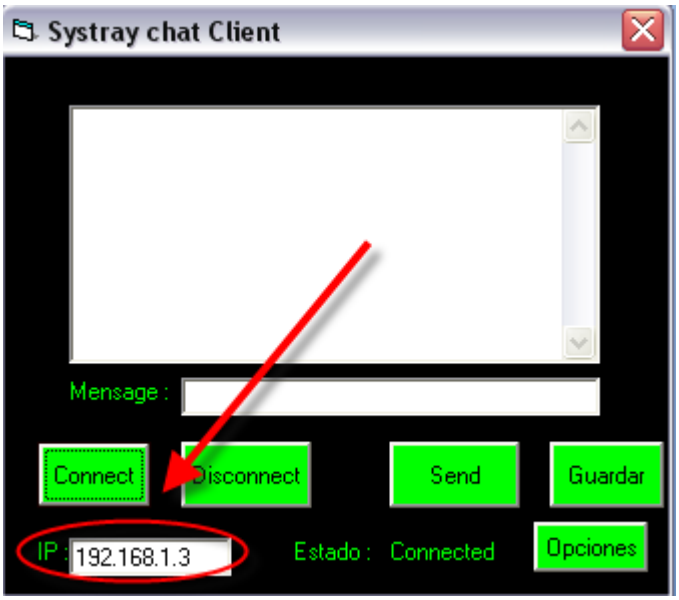
Como se puede ver en la siguiente imagen, en pocos segundos se ha llenado la pantalla de paquetes de datos puesto que tengo algunos programas corriendo y están intercambiando paquetes de datos continuamente:



Para que podamos ver claramente los paquetes que queremo voi a usar un filtro, para que se muestren solo los paquetes que estean dirigidos al puerto 2571 que es el puerto que voi a usar.



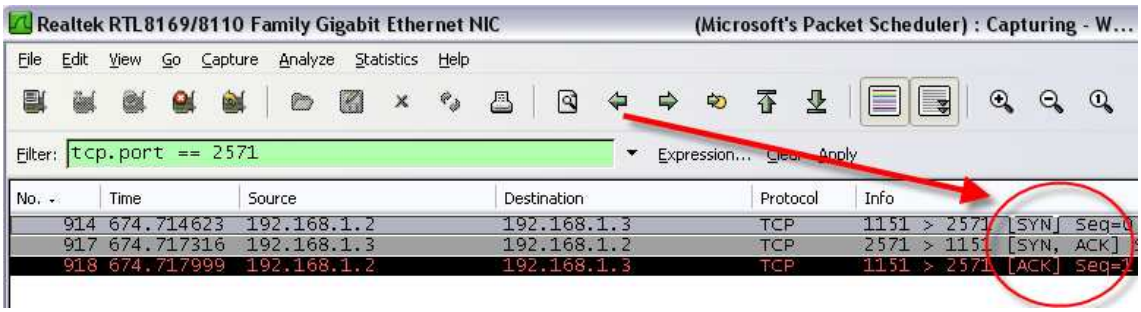
Bien, el sniffer ya esta a la escucha ahora solo falta poner a funciona el chat:



Como se puede ver en la imagen de arriba en la ip del cliente he puesto la ip del otro pc en el que tengo el chat a la escucha

Bien, ahora el chat ya esta conectado, pero…. Y que ha pasado en el sniffer??

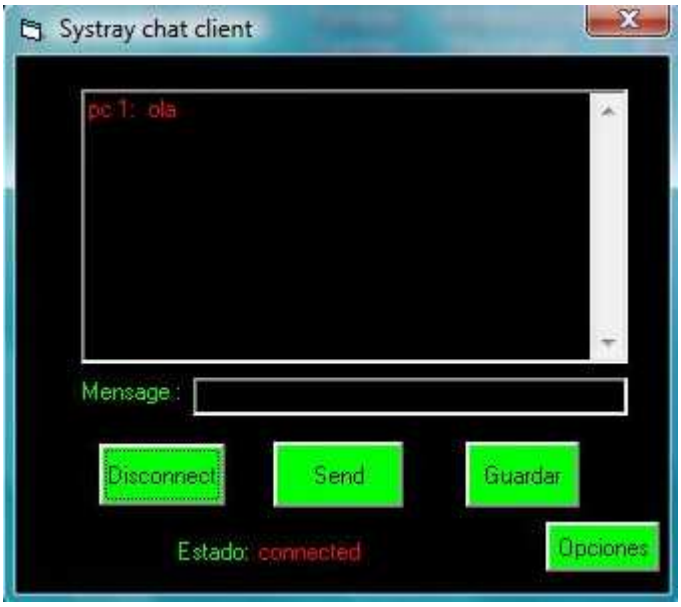
Pues como vemos en la siguiente imagen, el sniffer ha capturado los 3 paquetes de la negociación de la conexión:



Como podemos ver, el cliente manda un paquete con el flag SYN activado, el server le responde con un SYN ACK y finalmente el cliente responde con un ACK para confirmar que sigue ai.

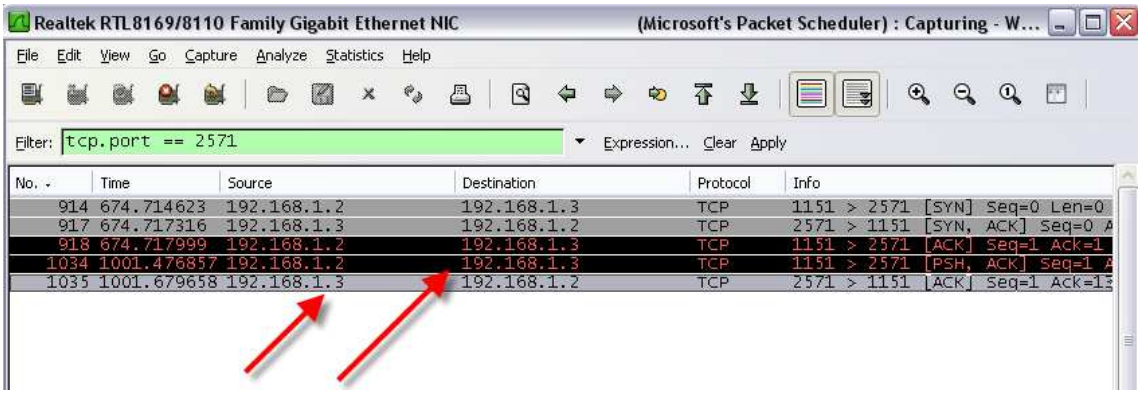
Ahora vamos a intercambiar datos entre los chats para que veamos lo que pasa….

El cliente tiene el “Nick” de “pc 1” y el server tiene el “Nick” de “pc 2”



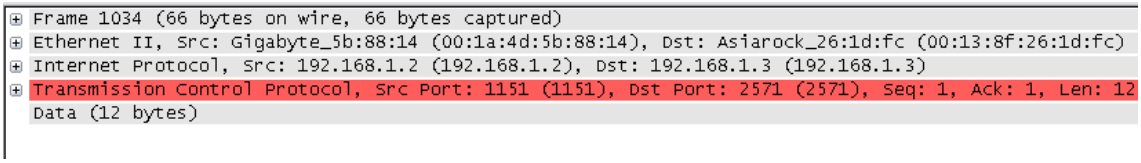
Como vemos en la imagen el cliente envía un mensaje al server diciendo “ola” (por lo que podemos deducir que el cliente es analfabeto puesto que hola se escribe con “H” xD)

Y en el sniffer se muestra lo siguiente:



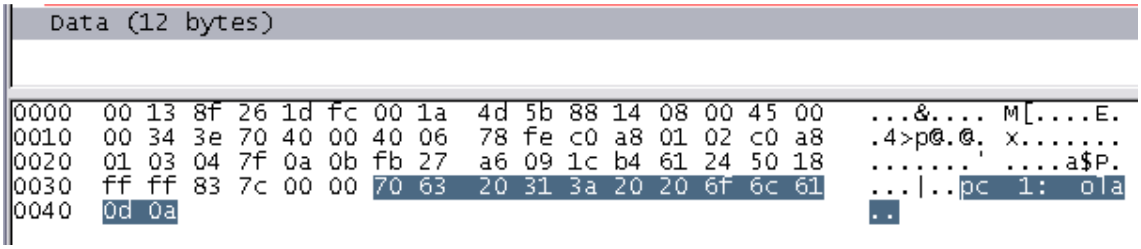
Si nos fijamos en el sniffer podemos ver que ahora hay dos paquetes nuevos, pero… porque aparecen dos paquetes si solo se ha enviando un mensaje ?? pues muy sencillo.. si os fijais en la imagen el primer paquete es el que contiene los datos, el segundo paquete es del server que manda ese paquete al cliente para indicar que sigue ai, en caso de que el cliente no recibiese este paquete, cerraría la conexión.

Bien, ahora voi a ver toda la información que le ha mandado el cliente al server para decir “ola”, para ello pinchamos en el paquete e inmediatamente nos salen los datos de este.



Como se ve en la imagen aparecen varios campos, donde podemos ver los flags que tiene activados el paquete, la dirección de destino, la dirección mac de la tarjeta de red… etc

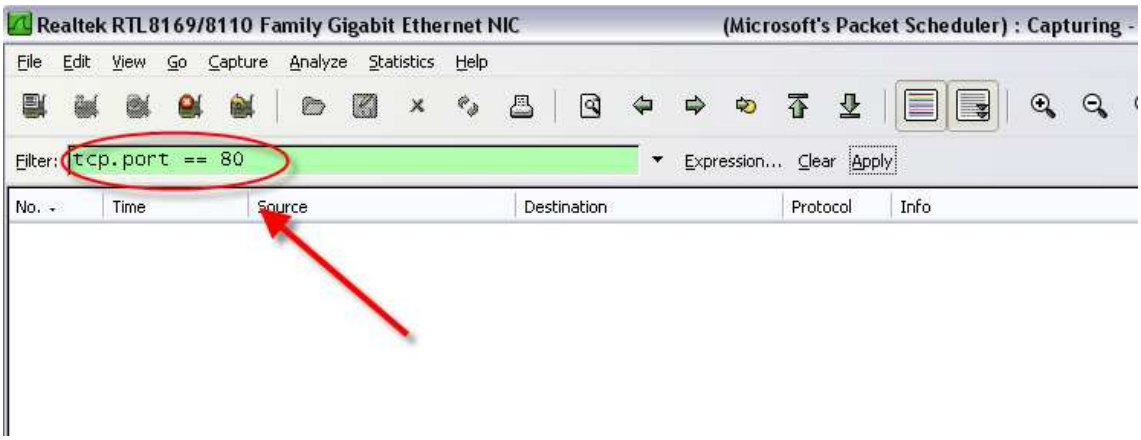
Ahora voi a pinchar en data…



Como se ve en la imagen al pinchar en Data no selecciona la parte del paquete que contiene los datos, a la izquieda están los datos en hexadecimal y a la derecha en ASCII, como podemos ver los datos que ha mandado son “ pc 1: ola” osea.. que lo que acabamos de hacer ha sido interceptar una conversación…

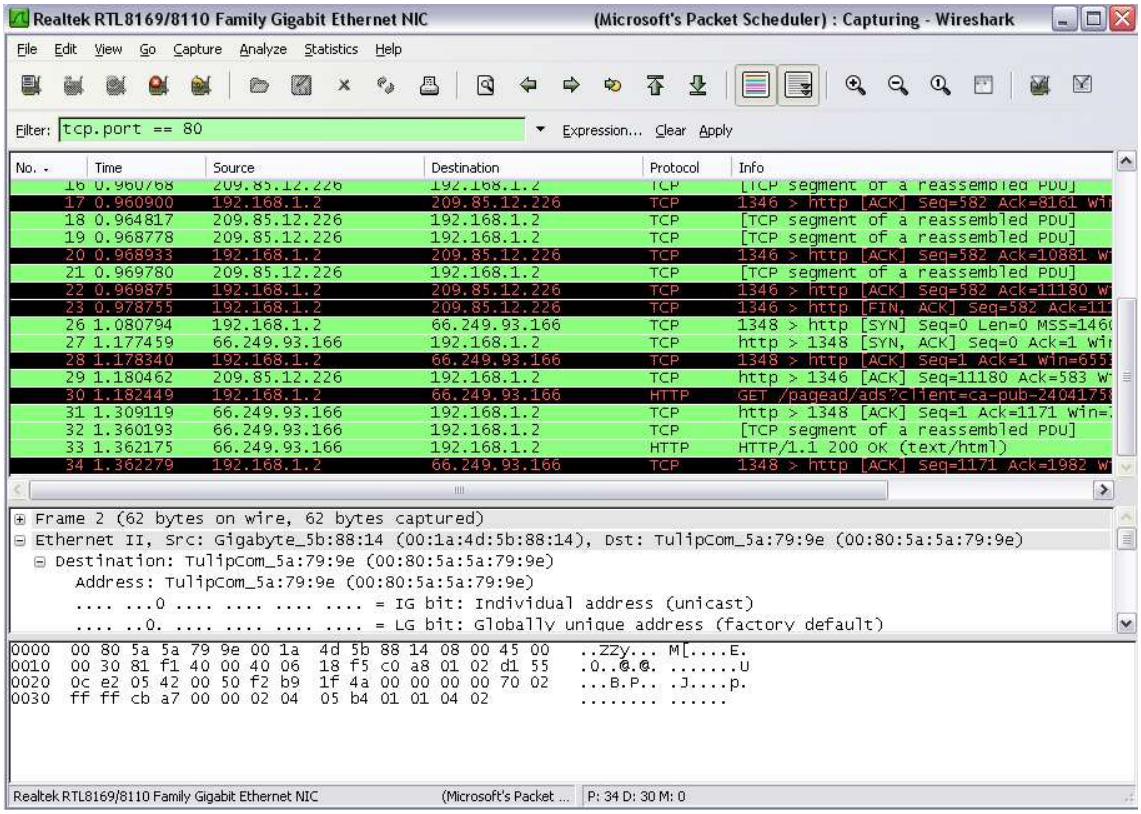
<u>Robando una cookie con un sniffer</u>

Tan simple como hemos hecho anteriormente, para hacer la prueba me he registrado en un foro que permite recordar contraseña, ahora lo único que tengo que hacer es poner a la escucha el sniffer por el puerto 80 y meterme en el foro…

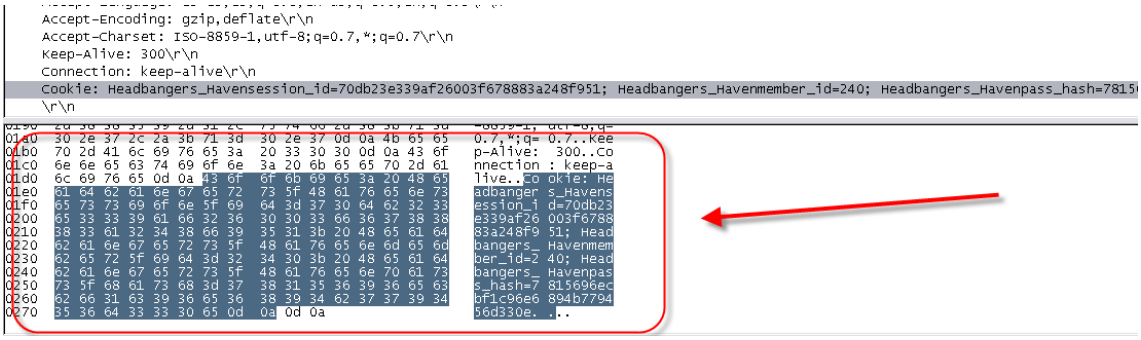


Como veis he puesto un filtro nuevamente, pero esta vez por el puerto 80 que es el que usa el navegador para conectarse a la web

Ahora me logeo en el foro…



Como veis me han salido muchos paquetes de datos, asi que tendre que ir analizándolos para encontrar el cookie…



Ai tenemos el cookie, ahora lo único que tendríamos que hacer seria un cookie poison y tendríamos acceso al foro con esa cuenta…

Y hasta aquí este manual.

ESTE MANUAL HA SIDO ESCRITO PARA LA COMUNIDAD DE PROGRAMADORES DE 666

WWW.CP666GROUP.COM

WWW.CP666GROUP.COM/foro

Manual escrito por Alfa-Omega