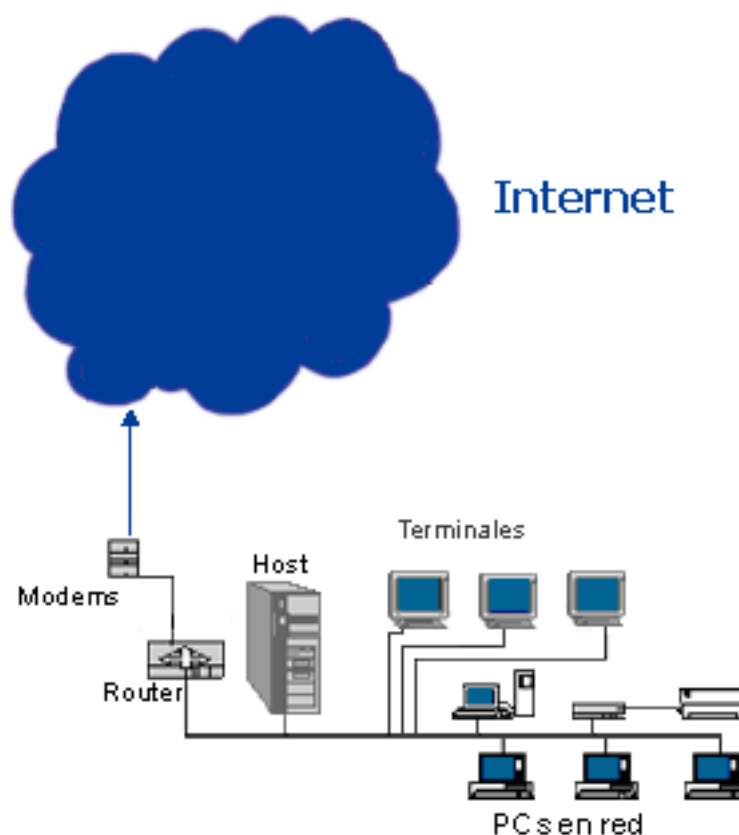


En el siguiente informe intentaré explicarles que es y como funciona un **sniffer**, pero para poder comprenderlo tenemos que tener idea de cómo esta diagramada una red con sus componentes básicos como ser un modem, un router, un swicht, un hub, etc. Un claro ejemplo de un diagrama de una red estructurada estándar, con conexión a Internet, se aproximaría a la siguiente imagen



El MODEM es el gestor de la conexión a Internet, el medio para repartir Internet a las terminales es por medio del ROUTER.

La palabra "**MODEM**" es la abreviatura de "MODulador - DEModulador"; y es aquél equipo utilizado para conectar computadoras por medio de la línea, a ser de microondas, cable canal ó telefónica. Como su nombre lo dice, el módem, se encarga de transformar la señal digital que sale de la computadora, u otro dispositivo sea Hub, router o swicht, en analógica, que es en la forma que viaja a través de las líneas de teléfono comunes (modula

la señal); y a su vez, el módem receptor se encarga de "demodular" la señal, transformándola de analógica a digital para ser recibida de nuevo por la computadora (esta definición es en general en la actualidad hay mas tipos de MODEM que se comunican de diferentes maneras pero ese no es el punto en este articulo así que sigamos).

El **ROUTER** es, como la palabra lo dice, un rutador/encaminador. Es un dispositivo para la interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

Otro elemento, que no se encuentra en el gráfico superior, que se utilizaría en una arquitectura un poco mas grande es el **SWITCH**. Es un dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. Opera en la capa dos (nivel de red) del modelo OSI. Término general que se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

Por último, el **HUB** es un concentrador, un dispositivo que permite centralizar el cableado de una red. Funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión.

Ya conocemos las definiciones de **MODEM**, **ROUTER**, **SWITCH** y **HUB**. Además, hemos visto en forma grafica, la conexión de una red.

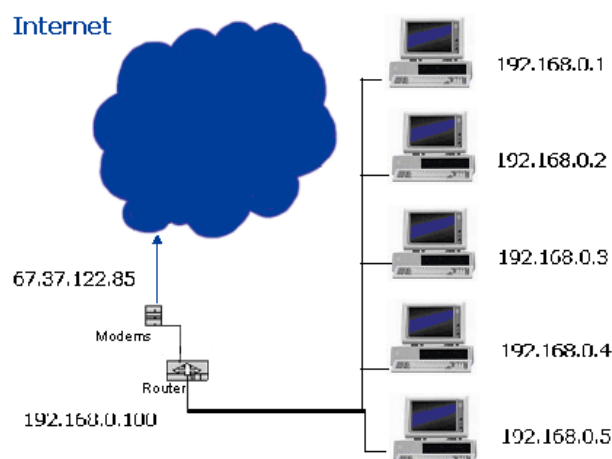
Repasemos un poco de teoría para ir ingresando al mundo de un **sniffer**. Desde adentro de la red para afuera (Internet), una Terminal/PC debe poseer una placa de Red sea alámbrica ó inalámbrica, esta se debe conectar al **ROUTER** ó en su defecto a un **SWITCH**. Este

último (sea el router ó el switch) se conecta al **MODEM**, y así a Internet; de esta forma tenemos descripta una red con Internet.

Para poder continuar, necesitamos comprender las diferencias entre un **ROUTER**, **SWITCH** y **HUB**. Sirven para los mismo (conectar varias terminales en red), pero no son lo mismo. Como se definió anteriormente, el router y el switch tienen una ventaja que brindan el ancho de banda a cada boca de acuerdo a la demanda de la Terminal (limitándola si es necesario), en cambio el hub repite los paquetes en cada boca de él aunque la terminal no lo demande. Además, el ROUTER y el SWITCH pueden filtrar determinados paquetes y detener abusos en el trafico de la red como de ser amplia disminución en el ancho de banda por requerimiento de una Terminal.

Conociendo que el router puede filtrar paquetes de una Terminal, nos preguntamos: **¿Como identificamos a una terminal en la red?** Simplemente por su dirección IP, esto es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red. Dicho número no se ha de confundir con la dirección MAC, que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar.

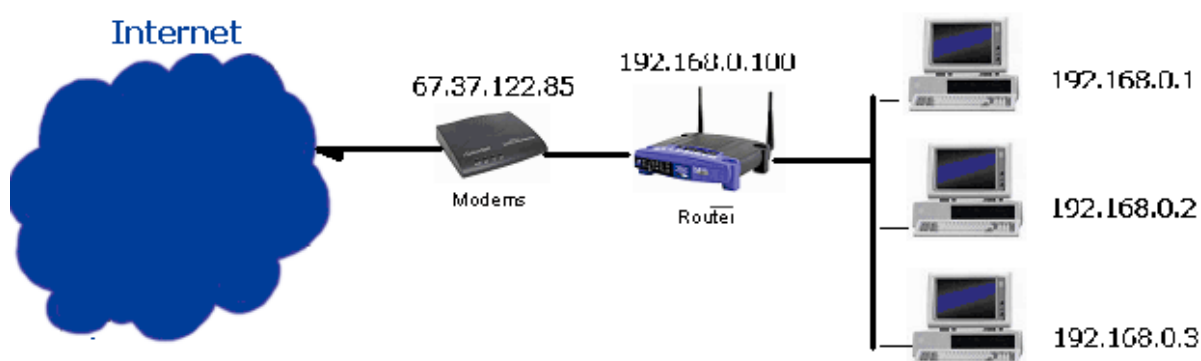
Ahora que tenemos el concepto de lo que hace una dirección IP, les informo que básicamente la mayoría de los dispositivos informáticos se interconectan mediante una dirección IP, como se muestra en el siguiente grafico



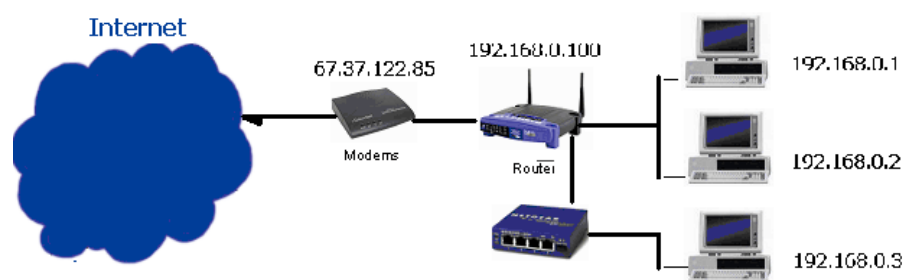
Con los conceptos anteriormente descriptos, vamos a ver la definición de **SNIFFER**. Un sniffer captura los paquetes que envía nuestra Red (ya sea una computadora en la LAN o nuestro PC), en esos paquetes transporta toda la información que se envía por Internet, así como usuarios y contraseñas de muchos servicios de Internet. Algunos de estos servicios que utilizan usuarios y contraseñas, o datos confidenciales, están encriptados o codificados para que no se puedan leer. Muchos otros como el servicio de FTP (File Transfer Protocol) viajan en texto plano, de manera que cualquiera que intercepte esos paquetes puede llegar a interpretar los datos.

Existe un sniffer, **Cain & Abel** (<http://www.oxid.it>), el cual es una herramienta de recuperación de passwords para sistemas operativos de Microsoft. Permite recuperar fácilmente varios tipos de passwords mediante el sniffing de la red, lográndolo por medio de Crackear passwords encriptados usando diccionarios, fuerza bruta y ataques mediante criptoanálisis. También graba conversaciones VoIP, decidifica passwords, recupera claves de red o claves almacenadas en caché. El programa no hace exploit de ninguna vulnerabilidad software, en cambio lo que hace es cubrir algunos aspectos de seguridad presentes en los protocolos estándares, métodos de autenticación y mecanismos de caché. Su principal propósito es el de recoger passwords de diversos lugares. Como se afirma en la página web de la herramienta; esta ha sido desarrollada con la esperanza de que sea útil a los administradores de redes, profesores, testeadores de intrusiones en el sistema y a cualquier otro profesional de seguridad.

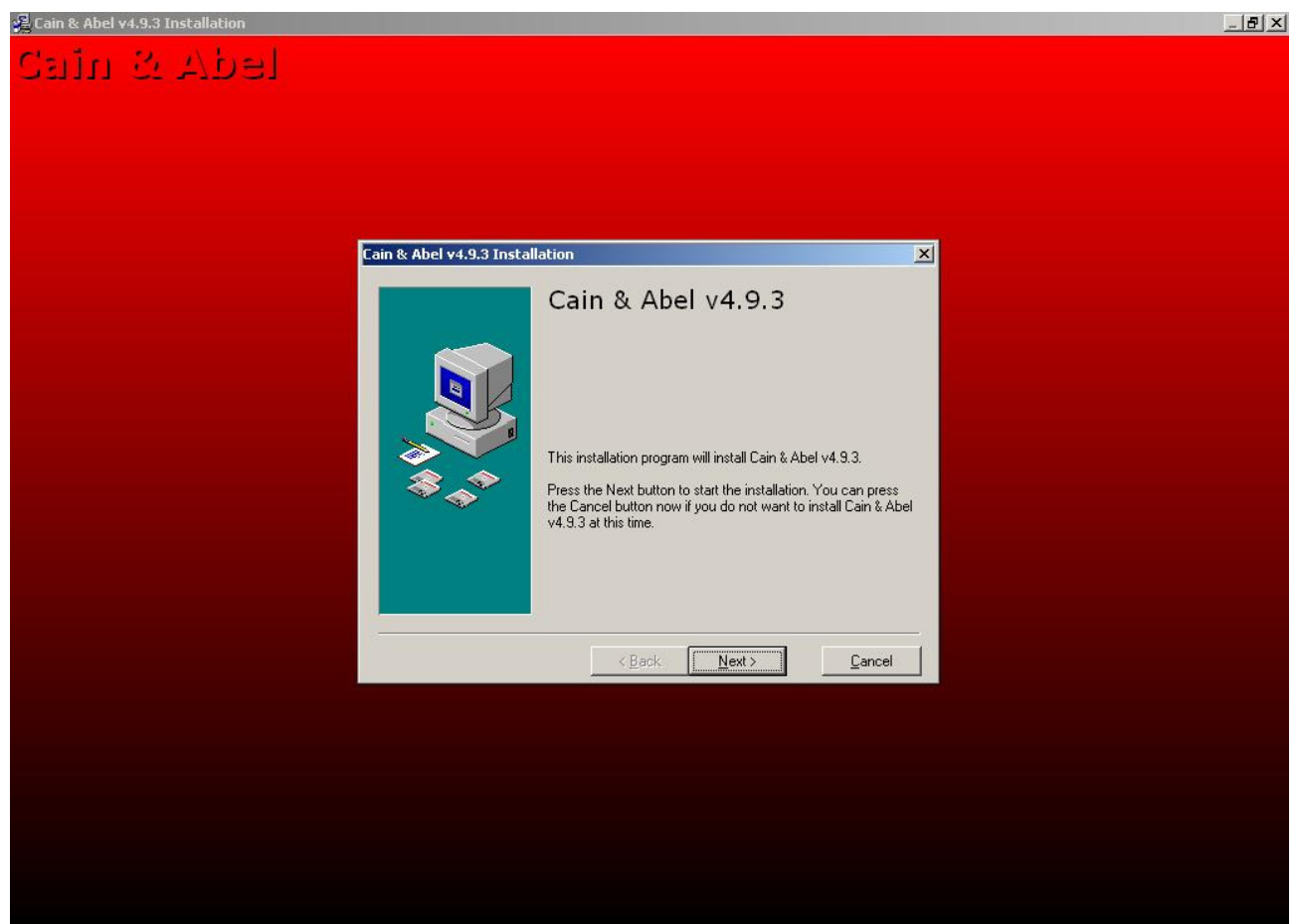
Los pasos para configurar un sniffer en una Red, recordemos lo que estuvimos viendo, ya sabemos que una configuración de este tipo es la estándar para conectar una red a Internet es básicamente así:



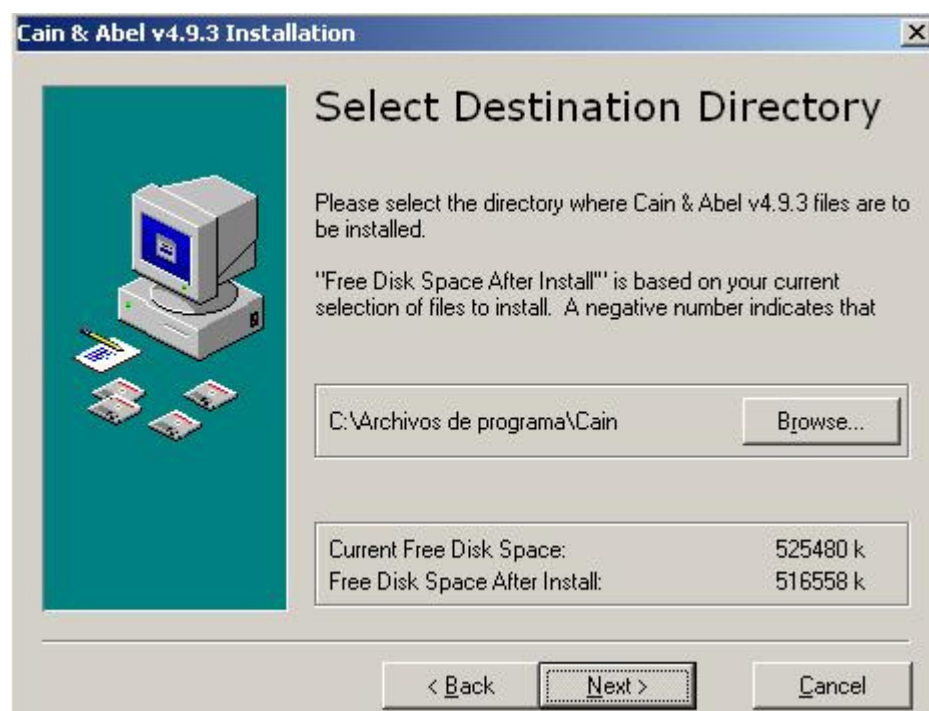
Pero lamentablemente, un sniffer no funcionaría en esta arquitectura, ¿Por que? simplemente porque el router es inteligente y filtra al sniffer. Entonces, ¿como hay que hacer para lograr hacer andar el sniffer en esta arquitectura? Simple hay que colocar un HUB antes del ROUTER, quedando entonces así:

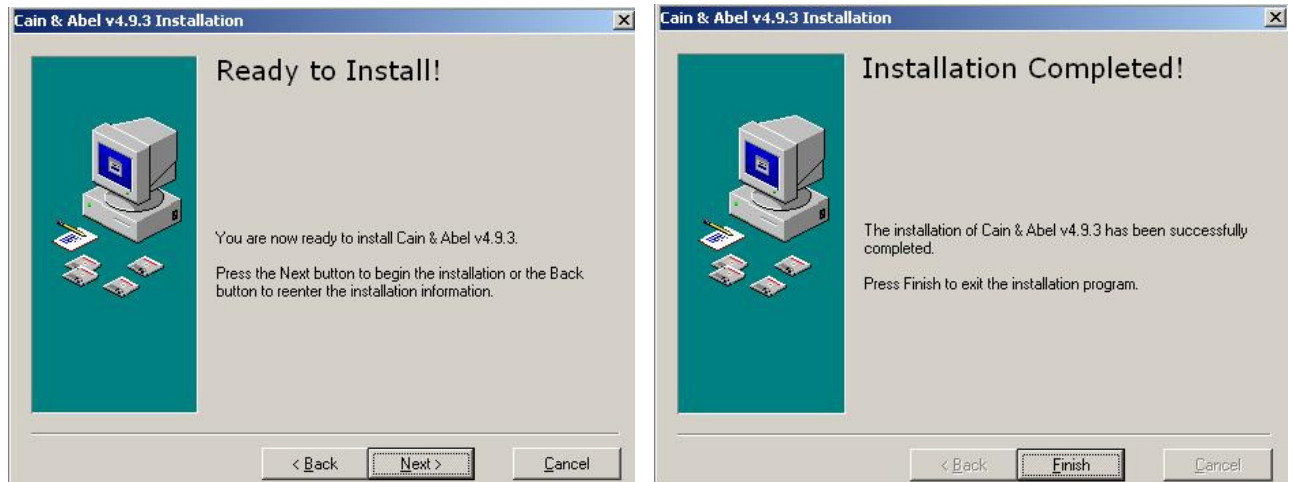


Ahora que ya tenemos el hardware listo para utilizar un sniffer iniciemos la Instalación del sniffer **Cain & Abel**.

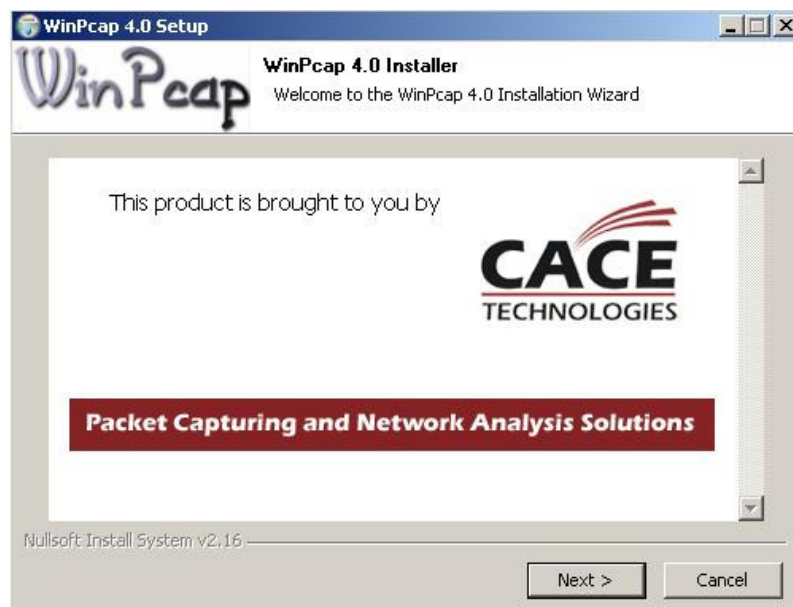


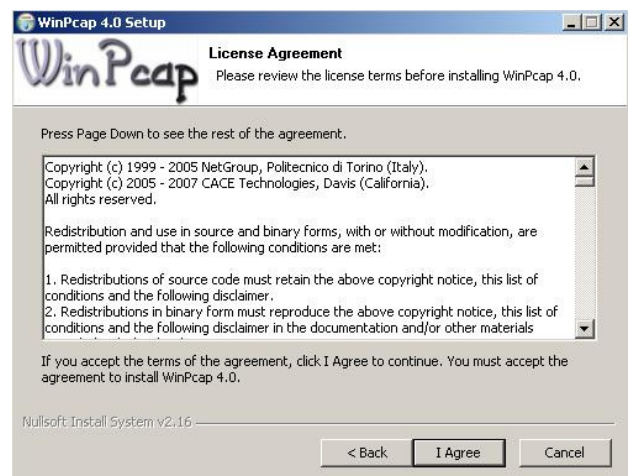
Como lo indica la imagen instalamos el Cain & Abel versión 4.9.3 en la Terminal que se encuentra conectada al HUB.





Una vez finalizada la instalación del sniffer automáticamente le solicitará que instale el WinPcap este software sirve para configurar la Placa de Red en **modo escucha**.



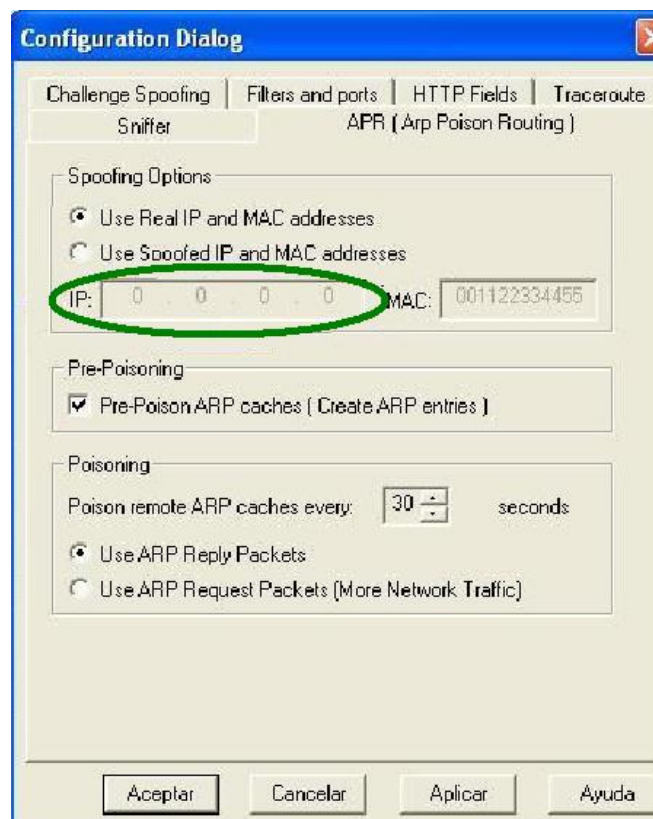


Ahora que a finalizado la instalación del sniffer, y reiniciado la maquina, iniciaremos con su configuración. Ejecutar el **Cain & Abel**, ahora hay que configurar la Placa de Red para que capture los paquetes que transmiten en la red.

Dirigirse a la solapa "Configure" y seleccionar la placa de red a utilizar y ahí filtrar los protocolos que queremos captar (este filtrado se realiza desde la solapa "Filtres and ports").

Ahora esconderemos nuestra IP, ARP Envenenamiento del enrutado Arp, donde dice IP colocaremos una dirección de IP que no exista en nuestra subred pero que este en el rango

de la misma para pretender ante los demás que somos otra terminal y de esta manera ocultar nuestra IP.



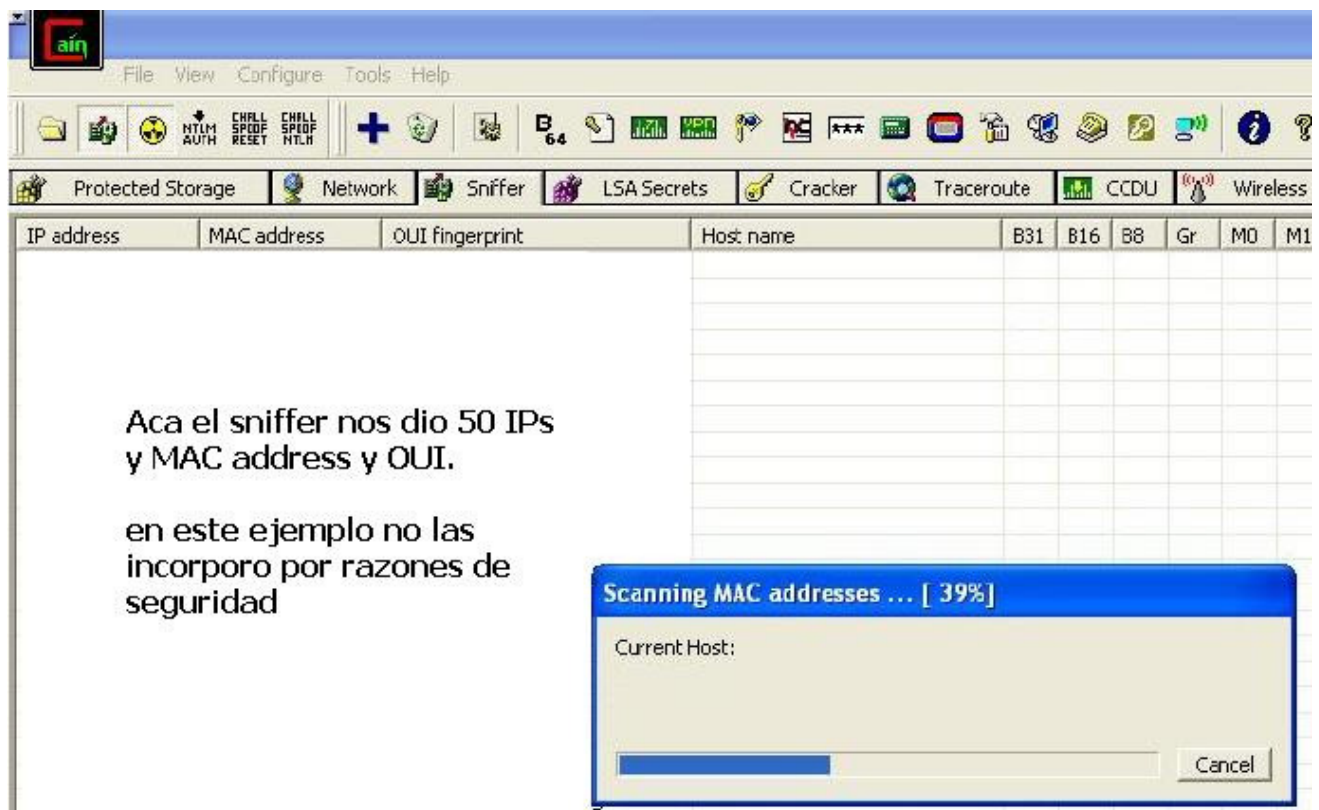
Bueno, iniciaremos el sniffer.



Iniciemos un escaneo de la red en búsqueda de direcciones MAC las cuales queremos esnifear hay que ir a la solapa Sniffer y a la pestaña inferior de nombre Hosts.



Como podemos ver, nos muestra un listado de Pcs en nuestra RED

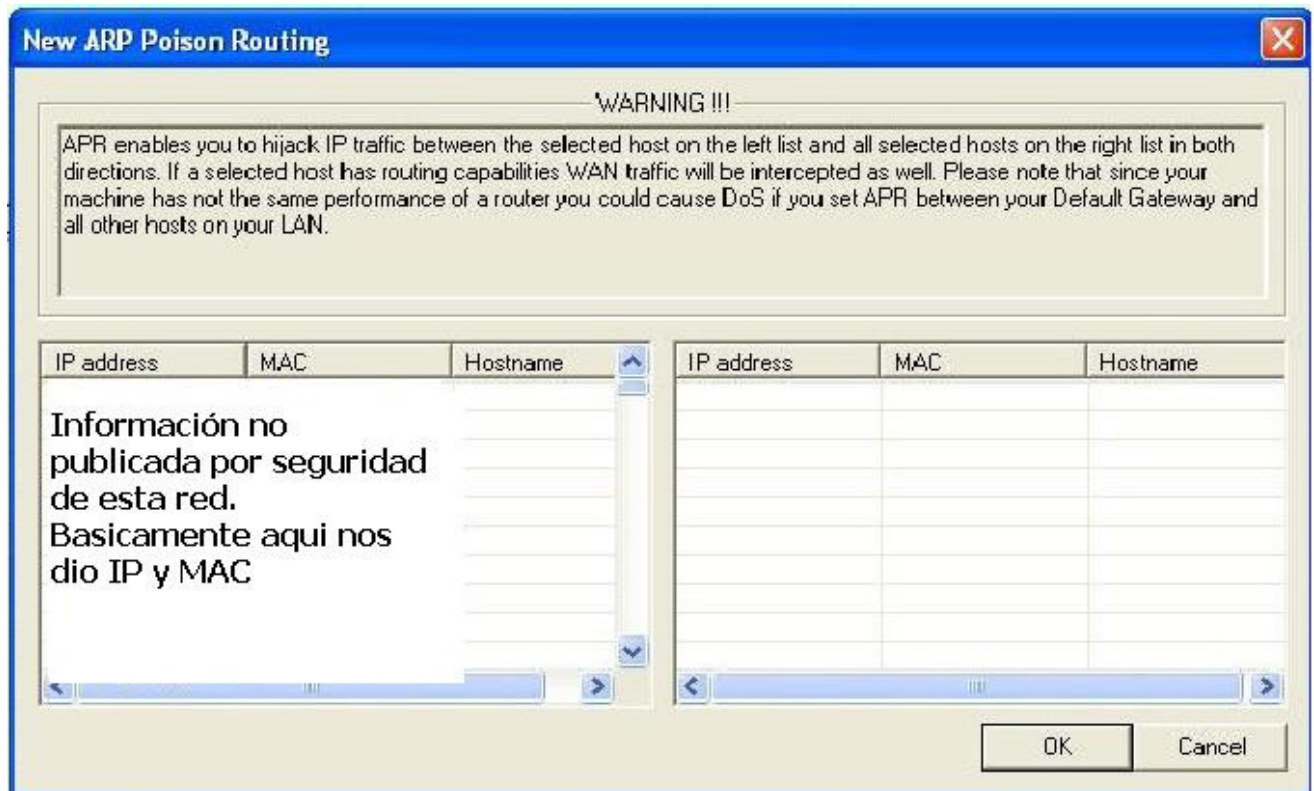


Pasemos a ver la técnica "man in the middle", es simple, hay que ir a la solapa APR



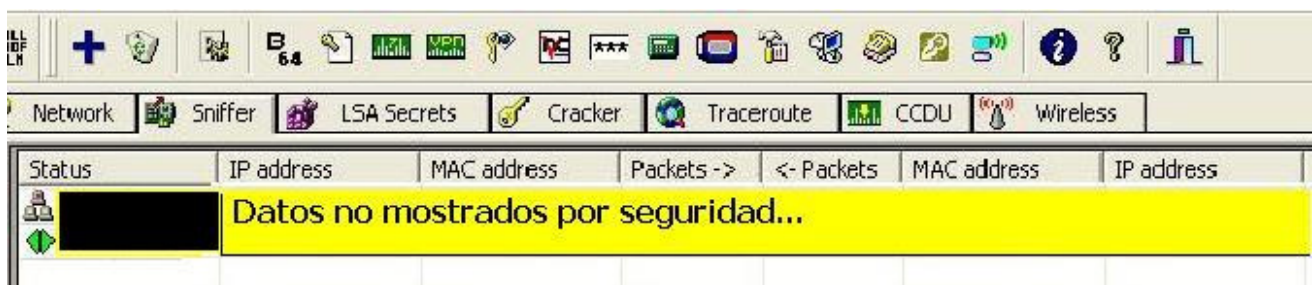
y presionar el símbolo "+" de arriba (así inicie el sniffer).



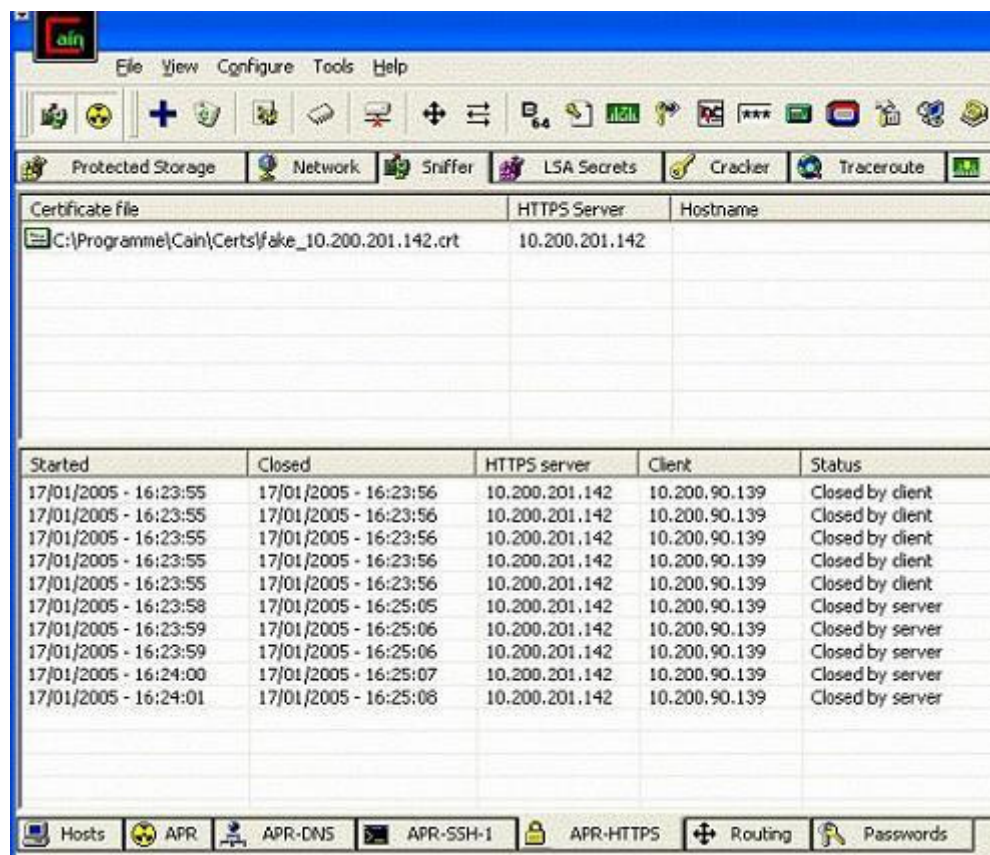


Seleccionando una dirección de IP del lado izquierdo, automáticamente se llenan los campos del lado derecho del grafico, logrando de esta manera interceptar cualquier dato que valla desde la IP seleccionada a cualquier destino detectado. (Quedando toda la información registrada en el sniffer)

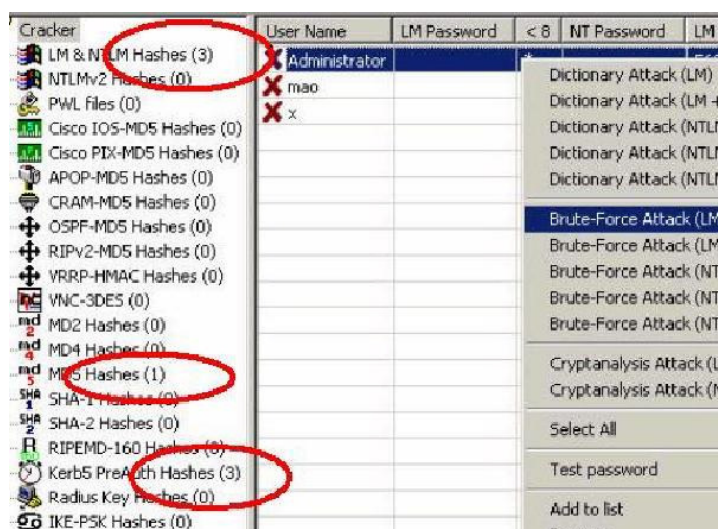
Ya funcionando el sniffer y el envenenamiento APR, les mostraré como capturar los Ips y paquetes en la RED.

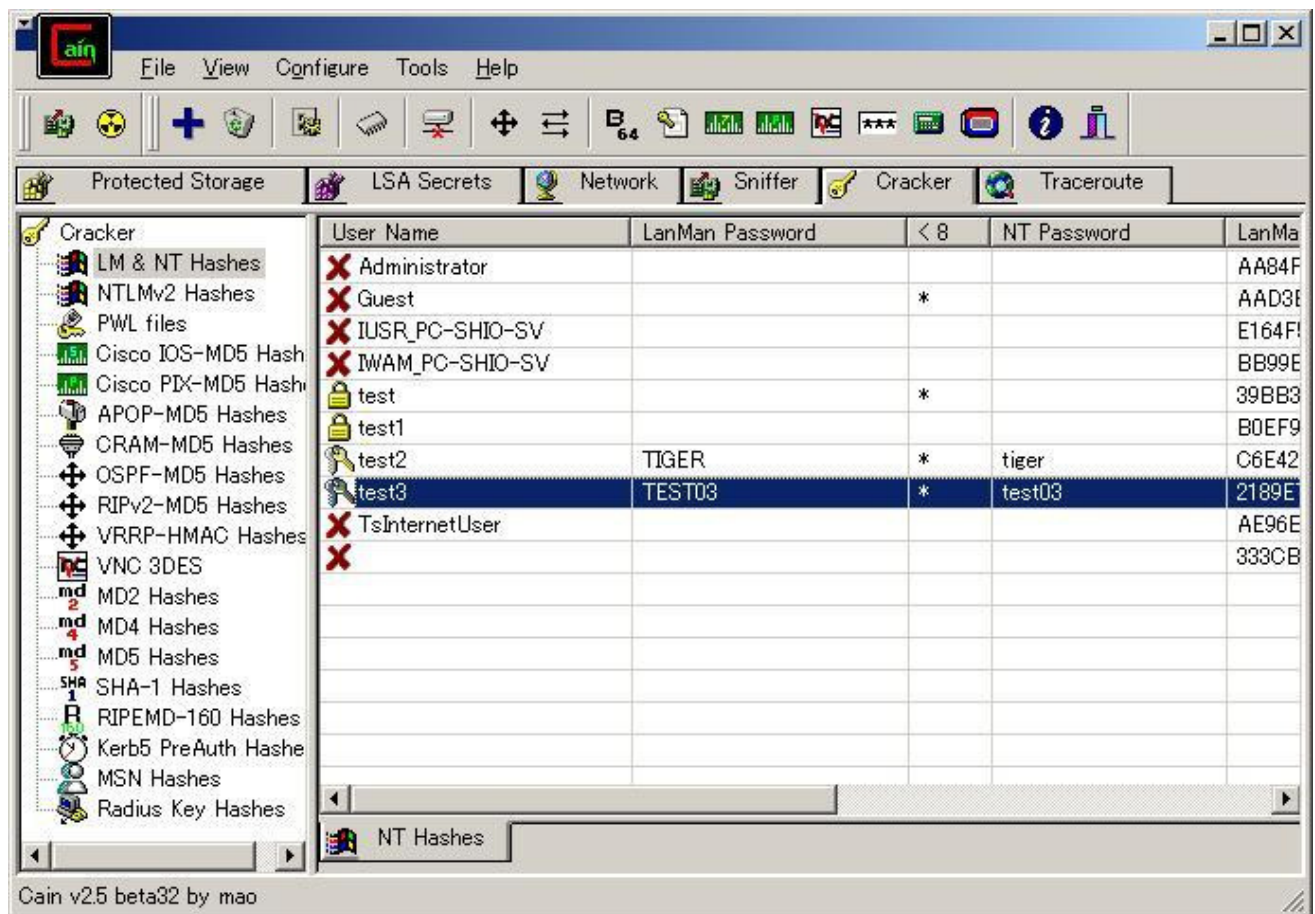


Para adquirir mejor los conocimientos, veamos un ejemplo práctico:



El programa va recogiendo usuarios y contraseñas. En el caso de encontrar contraseñas encriptadas, son enviadas automáticamente al Cracker.

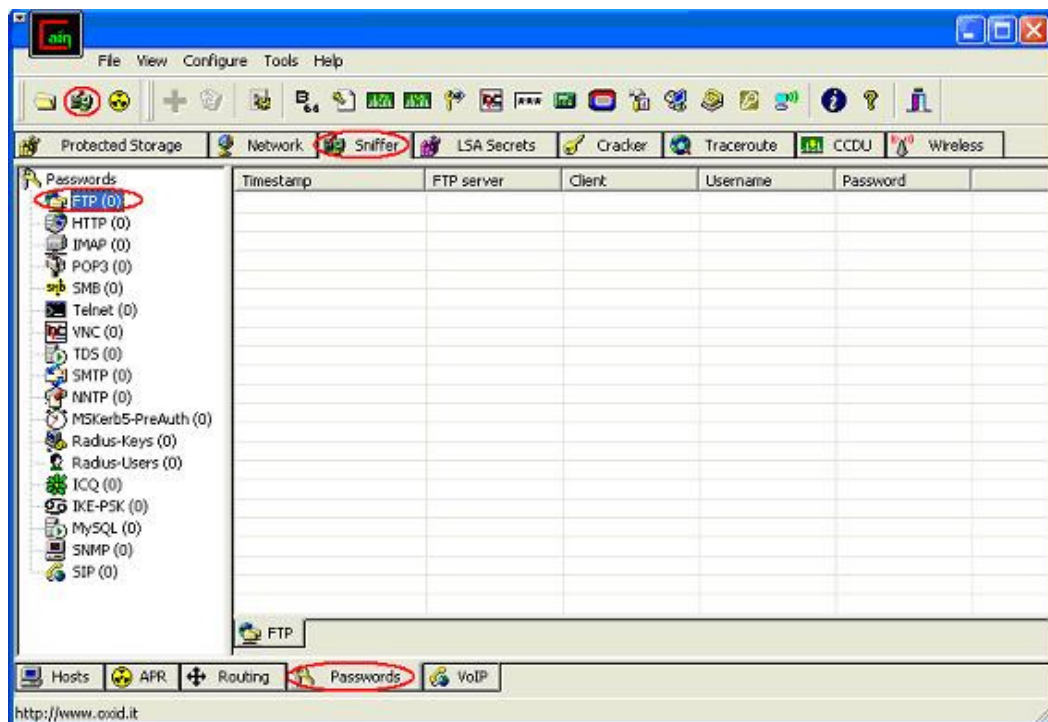




Con lo anterior, los Diccionarios o con el ataque por fuerza bruta, salen aproximadamente el 90% de las claves esnifiadas.

Para utilizar **el sniffer en los paquetes del protocolo FTP** no vamos a tener que realizar ningún tipo de Crack, ya que estos viajan en la RED en formato de Texto plano.

Veamos un ejemplo: Iniciemos el sniffer, vamos a la solapa "Sniffer" y luego a donde dice "Passwords" (ver imagen inferior).

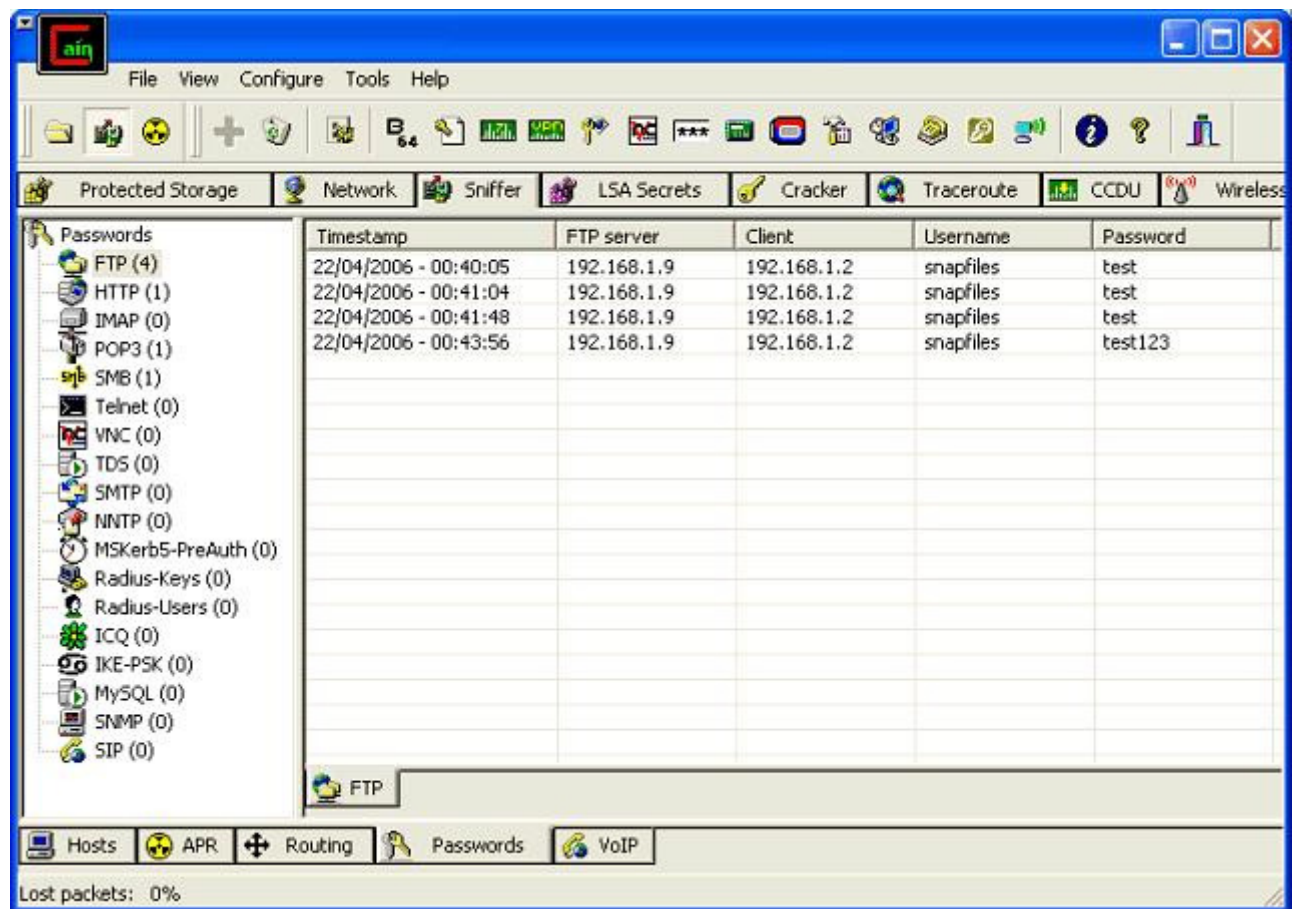


Una vez iniciado el sniffer, solo hay que esperar hasta que se inicie una sesión de FTP (esto es muy importante). Una sesión FTP puede iniciar por intermedio de un Gestor (sea el CuteFTP, Filezilla o otros), para subir información "habilitada por la empresa" a un espacio de un servidor de Internet, o **aun más peligroso**, ser gestionado por programas espías, como ser Keyloggers (los mas utilizados en la argentina son el Ardamax Keylogger v1., Perfect keylogger v1.472, Key-Logger, Ill Logger, RPKeylogger v0.1., Key-Logger Teclas, Key-Logger Xlog 2.21).

Para encontrar si existe algun Keylogger en nuestra RED, iniciemos el sniffer.

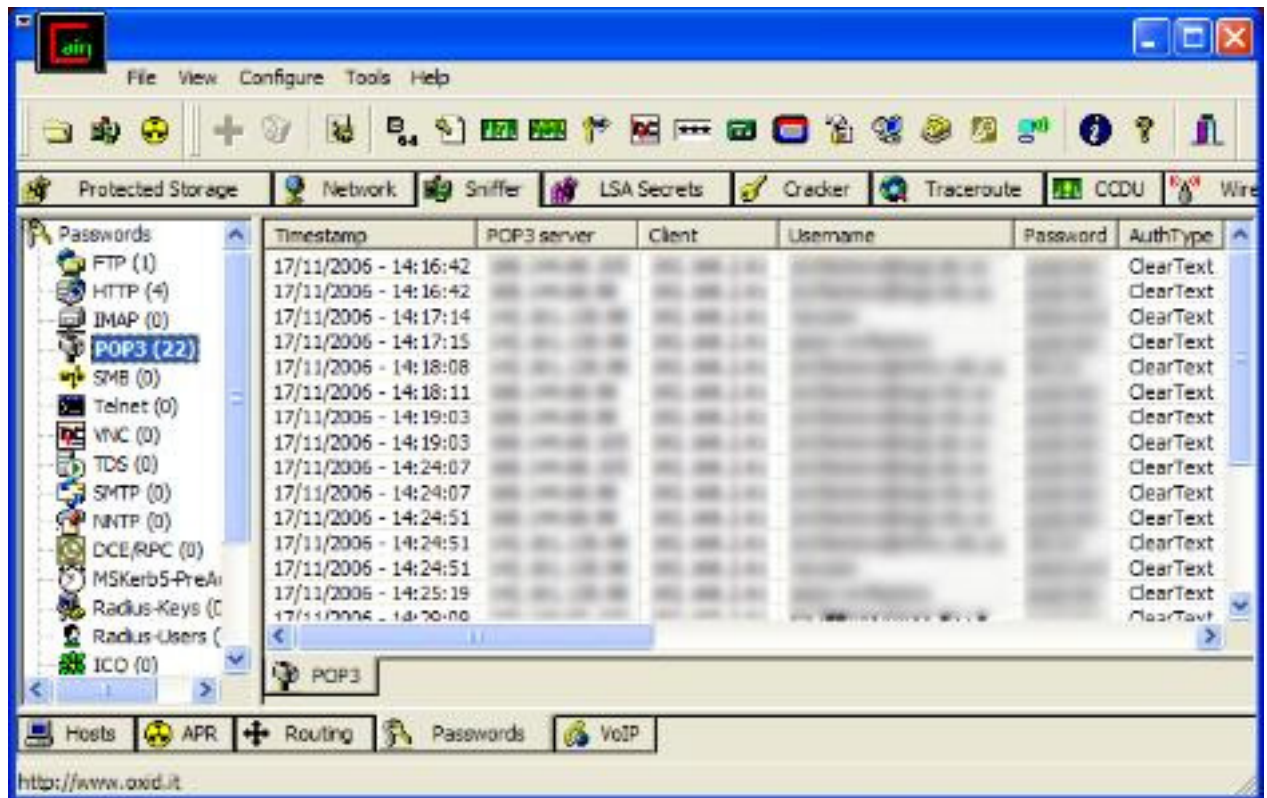
Timestamp	FTP server	Client	Username	Password
Los Datos no se muestran por seguridad.				

Y veamos un ejemplo:



Se puede visualizar la captura de un paquete. En la columna "Timestamp", se muestra la fecha y hora en que se inició la sesión; En la columna "FTP Server", se muestra la IP del servidor FTP; En la columna "Client", se muestra la IP de la PC que inicia sesión; En las columnas de "Username" y "Password", se muestra lo correspondiente. Se podran capturar los distintos tipos de contraseña que aparecen en la lista (Telnet, ICQ, MySQL, etc.), siempre y cuando se elijan los puertos apropiados para dichos procesos.

Para capturar las cuentas POP, o sea, correo electrónico, debemos realizar lo siguiente:



Arranquemos el Sniffer, ir a la solapa "POP3". En el recuadro derecho, nos muestra todas las cuentas POP, la IP del cliente, el nombre de usuario y la contraseña. Simple ¿no?

Estimados, esta es la Primera Parte del Manual de Cain & Abel versión criolla y bien argentina. Intentamos ir desde los conceptos básico generales hasta el entendimiento del correcto funcionamiento del sniffer. Remarco que un sniffer utilizado sin autorización de la conducción de su empresa es completamente ilegal; y en caso de que los directivos de la empresa lo autoricen, verifiquen que en los contratos figure la cláusula en donde permite al empleador monitorear la red y las PC en cuestión (el área de RRHH puede brindarles esta información). En una segunda parte, profundizaremos mas técnicamente en el análisis de los paquetes. Espero que les halla sido útil. Muchas Gracias y hasta la próxima. Martín (<http://www.informaticavip.com.ar>)