

## **Capítulo 4.**

### **Análisis de protecciones de redes inalámbricas**

#### **Análisis de algunas herramientas de apoyo que muestran las vulnerabilidades de seguridad en las redes WIFI.**

##### **4.1 ¿Qué son los sniffers?**

Ethernet es el protocolo estándar más popular para la comunicación entre computadoras. Es conocido como un protocolo de difusión (broadcast), porque cuando un equipo intenta enviar información, envía los datos a todas las demás computadoras del mismo segmento. Cada paquete tiene un encabezado el cual contiene la dirección de ambos, la computadora destino y origen. Aunque la información es recibida por todas la computadoras del segmento, solo la computadora que coincide con la dirección destino responderá.

Cuando se ejecuta un sniffer, el controlador de captura activa el “modo promiscuo” de la tarjeta de red para impedir que sean desechados automáticamente los paquetes que tienen otra dirección destino. Esto significa que si una computadora del segmento desea monitorear o espiar la comunicación de otros equipos solo tiene que activar el “modo promiscuo”.

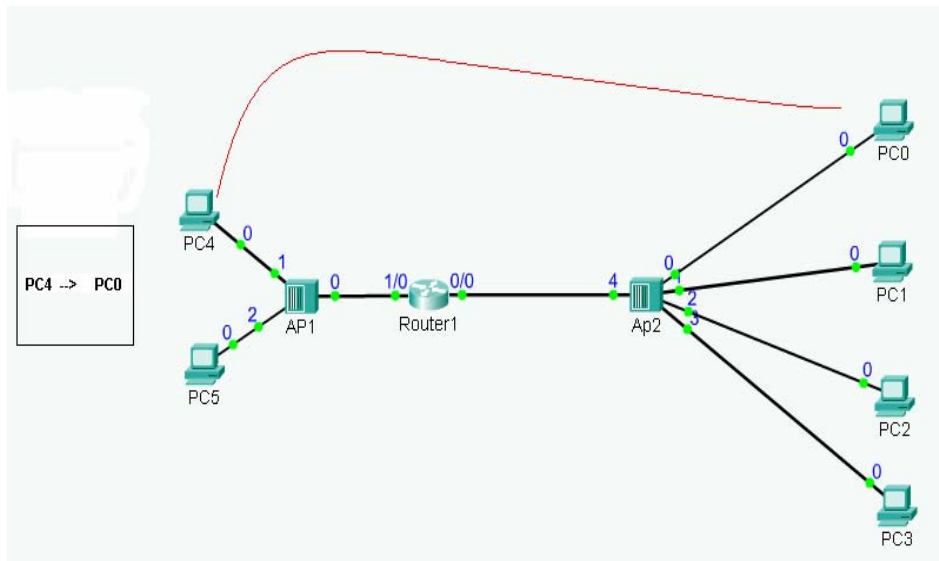
Es por eso que probablemente una de los mayores riesgos de tener una red WIFI abierta, es que cualquier lugar en donde uno este, pueden haber personas que estén corriendo un sniffer en la red.

También a los sniffers se les conoce como analizadores de redes, los cuales son unas herramientas las cuales pueden ver todo el tráfico que se encuentra en la red, pueden dar información crucial como por ejemplo que tipos de datos son los que se están cruzando a través de la red. Pueden desde descifrar un password, hasta ver las

conversaciones en los sitios de mensajería instantánea como el msn, yahoo entre otros. Algunos populares como Ethereal, Network Active, Cain, NetStumbler entre otros.

#### 4.1.2 Funcionamiento de un Sniffer

Supongamos que queremos mandar un paquete de la PC4 a la PC0, la cual se encuentra en otra subred. Observemos como esta compuesta la arquitectura de esta red.



**Figura 4.1 Funcionamiento de un sniffer**

Un sniffer es un programa de captura las tramas de red. Es común que el medio de transmisión sea compartido por varios ordenadores y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer pone la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la MAC de la tarjeta; de esta manera se puede obtener todo tipo de información de cualquier aparato conectado a la red como contraseñas, correo electrónico, conversaciones de mensajería instantánea o cualquier otro tipo de información personal.

Es importante remarcar el hecho de que los sniffers sólo tienen efecto en redes que comparten el medio de transmisión como en redes sobre cable coaxial, cables de par trenzado o redes WIFI.

## **¿Por qué es importante contar con herramientas de apoyo para asegurar la seguridad de nuestra red?**

Hoy en día los piratas informáticos, llamados hackers, llegan a ser cada vez más sofisticada, haciendo cada vez más difícil de proteger la integridad de las aplicaciones y la información de estas. Proteger estas aplicaciones poniendo parches manualmente es una estrategia que tarde o temprano fallará. La seguridad Web, en la actualidad, debe de ser construida de abajo hacia arriba, desde el desarrollo de la aplicación, pruebas de calidad, el despliegue y mantenimiento. Por estas razones es importante que todos aquellos interesados en la seguridad de las redes cuenten con herramientas de apoyo, para mantener su seguridad, confiabilidad y calidad en sus servicios. Es por eso que en la siguiente tabla se darán a conocer los aspectos a evaluar en este trabajo.

### **Aspectos de seguridad a evaluar**

<b>Aspectos de seguridad</b>	<b>Herramientas</b>
Obtención de claves	Cain
Observar puertos abiertos	SuperScan
Snooping	Ethereal, NetworkActive
Infiltración a routers	Default passwords
I	
Analizar TCP, UDP detalladamente	NetworkActive
Interceptar comunicaciones vía Chat.	NetworkActive
Obtener claves de configuraciones	<a href="http://www.cirt.net/cgi-bin/passwd.pl">http://www.cirt.net/cgi-bin/passwd.pl</a>

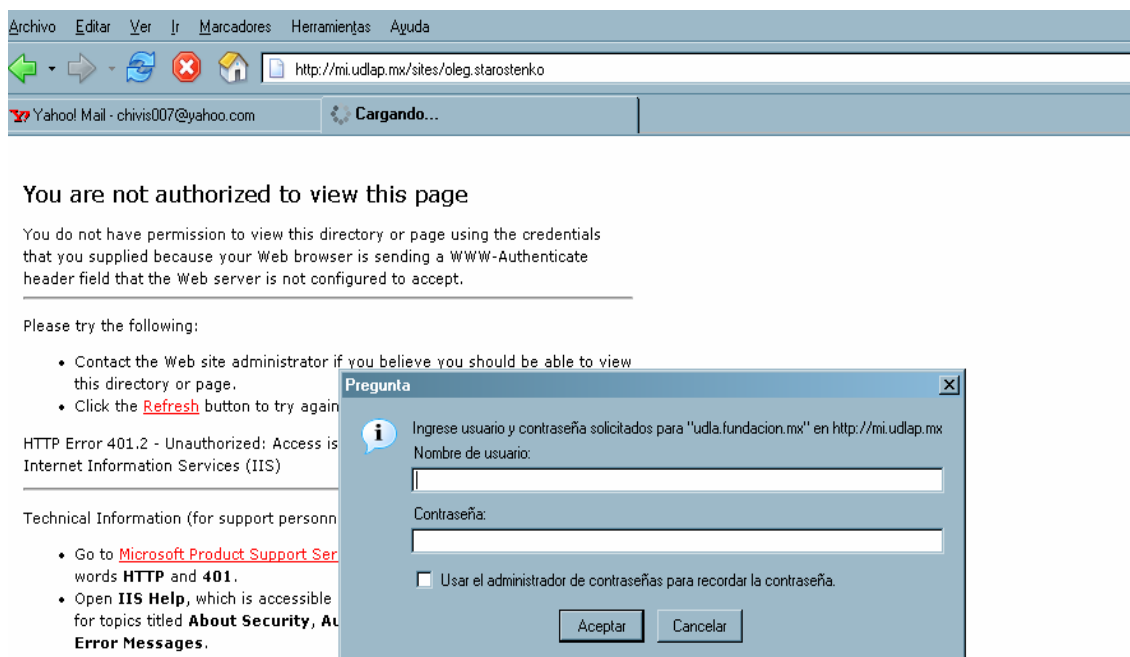
## 4.2 Análisis de la red con Ethereal

Es un potente analizador libre de protocolos de redes, para máquinas Unix y Windows. Nos permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco puede leer más de 20 tipos de formato distintos.

### Caso

**Situación:** Un profesor se encuentra en su oficina y esta apunto de entrar a la página del curso que da para poder ver los documentos que tiene archivados en la web.

Aquí antes de que podamos acceder al sistema se hace la petición del navegador de un nombre de usuario y contraseña. **Figura 4.2**



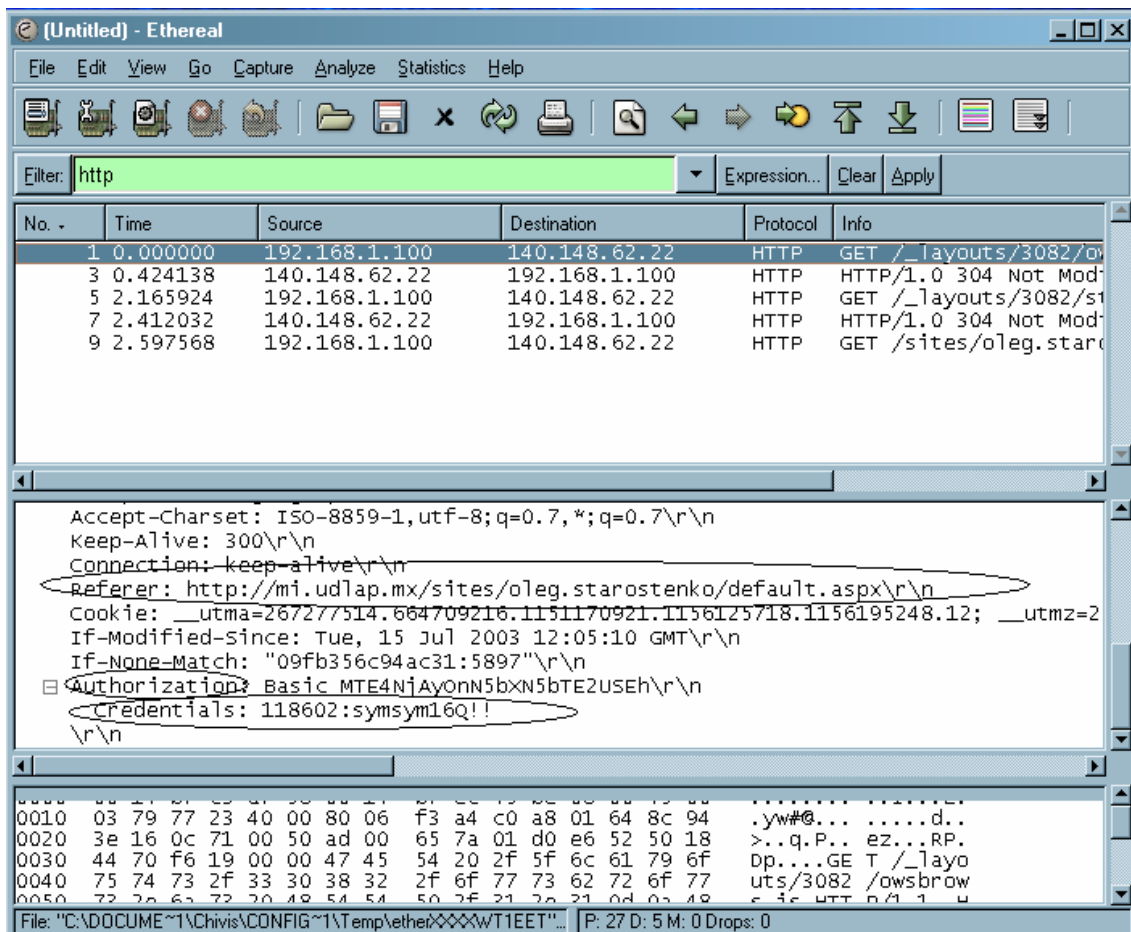
**Figura 4.2** Página de Oleg Starostenko

#### 4.2.1 Proceso de Ethereal: Autenticación en documentos HTML

En esta parte accedemos a una página HTML de la UDLA protegida con una contraseña, esto con el fin de observar el proceso de autenticación entre el servidor y el host. Los pasos a realizar se enlistan a continuación. **Figura 4.2.1**

- a) Iniciar el navegador de Web.
- b) Iniciar el Ethereal Packet Sniffer.
- c) Introducir http en la ventana de filtros.
- d) Introducir el URL en el navegador:  
http://mi.udlap.mx/sites/oleg.starostenko
- e) Introducir el nombre de usuario y la contraseña en la ventana mostrada arriba

Ahora analizaremos el ethereal:



[Ethereal, 2006]

**Figura 4.2.1 HTTP GET con Autorización requerida**

El nombre de usuario y la contraseña que se escribieron están codificados en un conjunto de caracteres, siguiendo el encabezado “Authorization: Basic” del mensaje del cliente HTTP GET. Esto puede parecer que su nombre de usuario y la contraseña están encriptados, sin embargo el usuario y contraseña no lo están. Ahí podemos observar claramente el usuario y la contraseña, que fueron las claves con las que se acceso al sistema.

**Vulnerabilidad:** Que pasaría si alguien obtuvo la clave del profesor y puede acceder a documentos que el profesor no querían que fueran vistos, como por ejemplo tareas o exámenes pasados.

**Daño:** Pues sabemos que el daño puede ser terrible si las personas intentan hacer algún tipo de cambios a los archivos o inclusive pueden llegar a borrar la información.

Para saber más acerca de cómo usar este programa, ver el **Apéndice A: Ethereal**

### **4.3 Análisis de seguridad con NetworkActive**

**NetworkActive:** Es una herramienta la cual le permite al usuario no solo ver el contenido de los paquetes que van a través de la red, sino que también reacomoda los archivos que están siendo transferidos.

#### **4.3.1 Proceso de NetworkActive.**

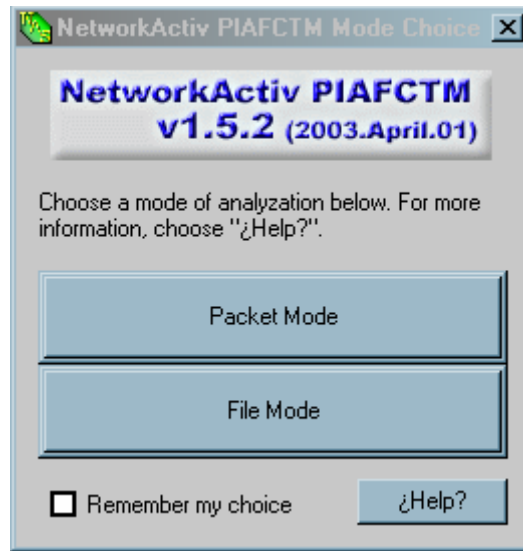
Encuentra las vulnerabilidades en una red que no es segura  
Una vez que NetworkActive vea si se puede conectar a una red, éste recolectará los datos que se encuentren en esa misma subred.

### 4.3.2 NetworkActive: Modo de Archivo

**Figura 4.3.0**, ésta herramienta te permite escanear los paquetes que viajan por la red. Este programa te permite que visualices de una manera gráfica el contenido de lo que se capturó.

Ahora mostrare ejemplos y casos de cómo con esta herramienta puede ser fácilmente ejecutada para obtener información de otros usuarios la cual es confidencial.

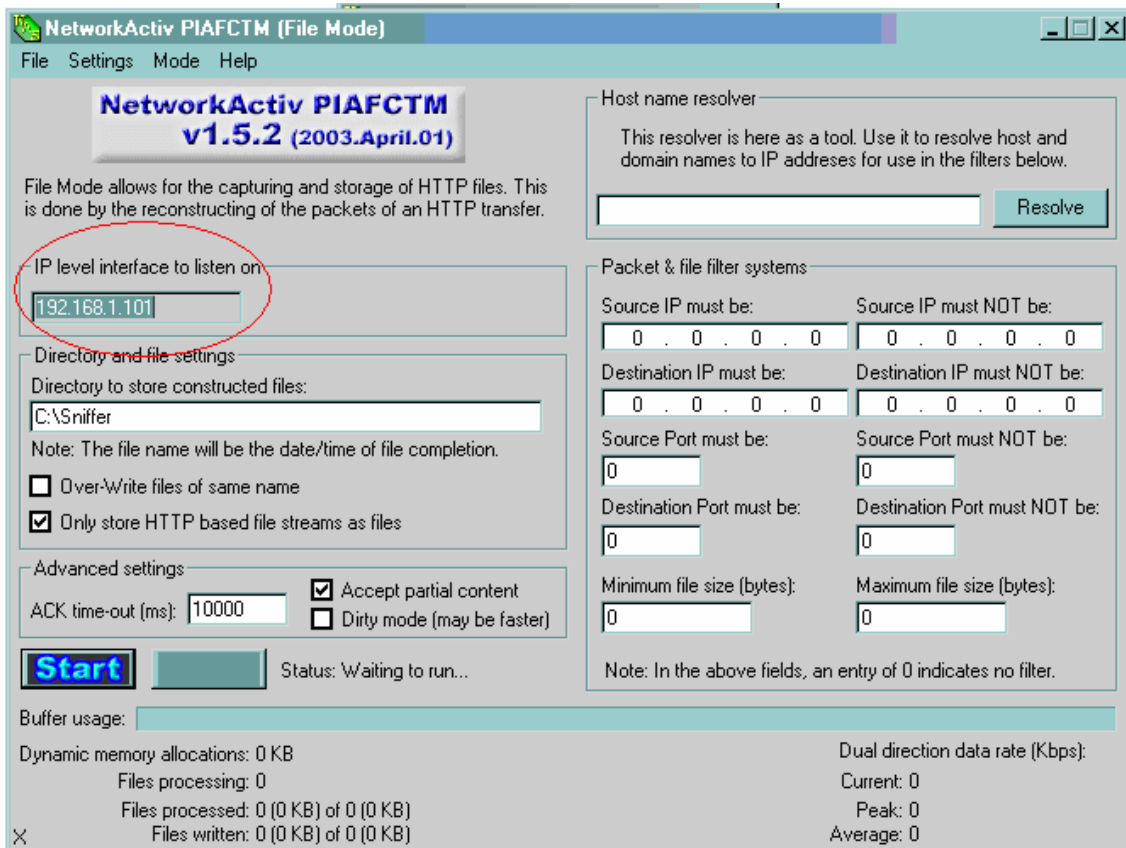
#### a) Capturar datos por medio del modo de Archivos.



[NetworkActive, 2005]

**Figura 4.3.0 Ventana de NetworkActive**

Las redes WIFI que son inseguras son a las que el software puede entrar sin ningún problema. Lo primero que se hace es escoger a que nivel de IP se va a “olfatear”.

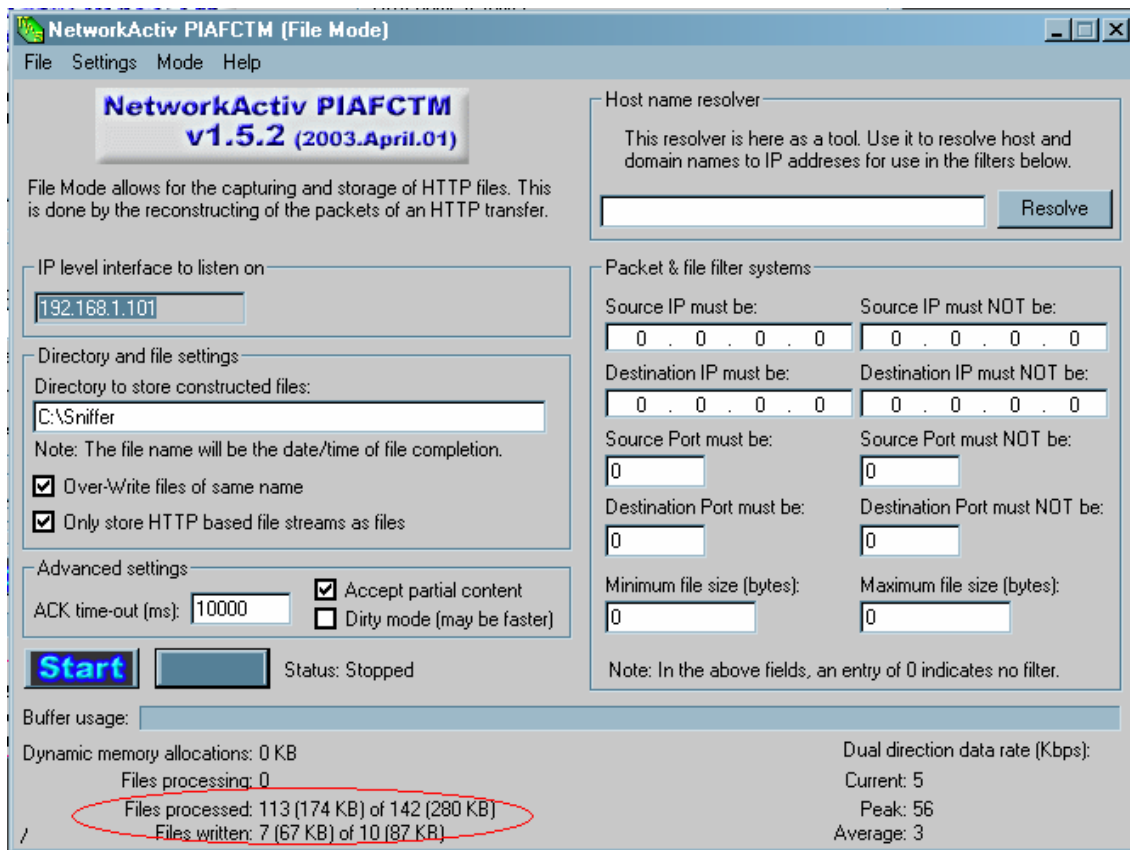


[NetworkActive, 2005]

**Figura 4.3.1 Inicializando**

Como se puede observar en la **Figura 4.3.1**, luego de seleccionar la subred se empieza hacer el escaneo de archivos de la misma. También seleccionamos en que directorio queremos que se guarde toda la información.





[NetworkActive, 2005]

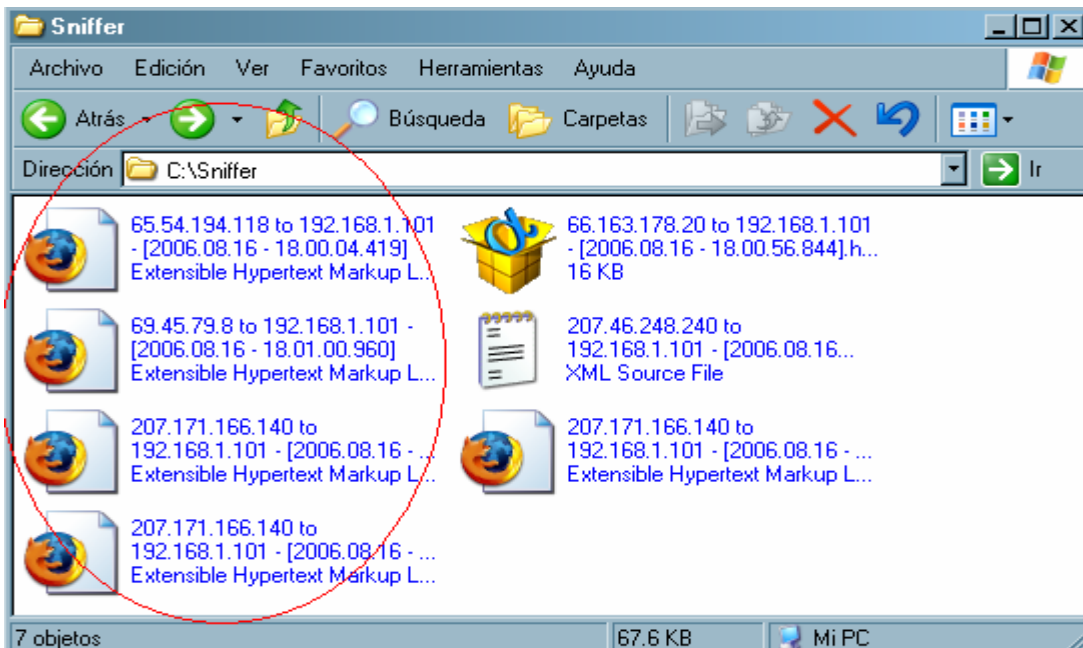
**Figura 4.3.2 Captura de datos**

Aquí podemos observar como es que se empieza a hacer el procesamiento de los datos.

### Caso

**Situación:** Una persona navegando pacíficamente la web.

**Vulnerabilidad:** Cualquiera que haya sido la persona que se metió a la red, pudo obtener los archivos de las páginas Web que el usuario estaba visitando en el momento del escaneo.



**Figura 4.3.3 Archivos guardados**

Y podemos observar que donde pusimos que se guardaran los archivos en donde aparecen las direcciones de IP de la página Web a la que el usuario acceso.

**Daño:** Al abrir uno de los archivos de Mozilla Firefox nos encontraremos con las páginas Web visitadas por el usuario. De tal manera que en vez de ver la información que captura la herramienta por paquetes la vemos ya reacomodada en un archivo con texto e imágenes, ver **Figura 4.3.4**



**Figura 4.3.4 Visualización de los archivos**

Aquí podemos ver como es que después de que se hizo la captura con el programa, podemos ver como se nos muestra todo lo que fue capturado ya esta todo acomodado de manera que lo podemos abrir en el propio explorador y ver exactamente que es lo que el usuario estaba viendo.

### **4.3.3 NetworkActive: Modo de Paquetes**

El modo de captura de paquetes es la manera más eficiente de observar lo que otros usuarios conectados a la red WIFI están haciendo. Con esta herramienta podemos analizar todo tipo de tráfico de la red, podemos observar los diferentes protocolos como son TCP, UDP, etc. Desde que puerto se esta mandando la información, la dirección IP de origen y destino de un paquete entre otras cosas.

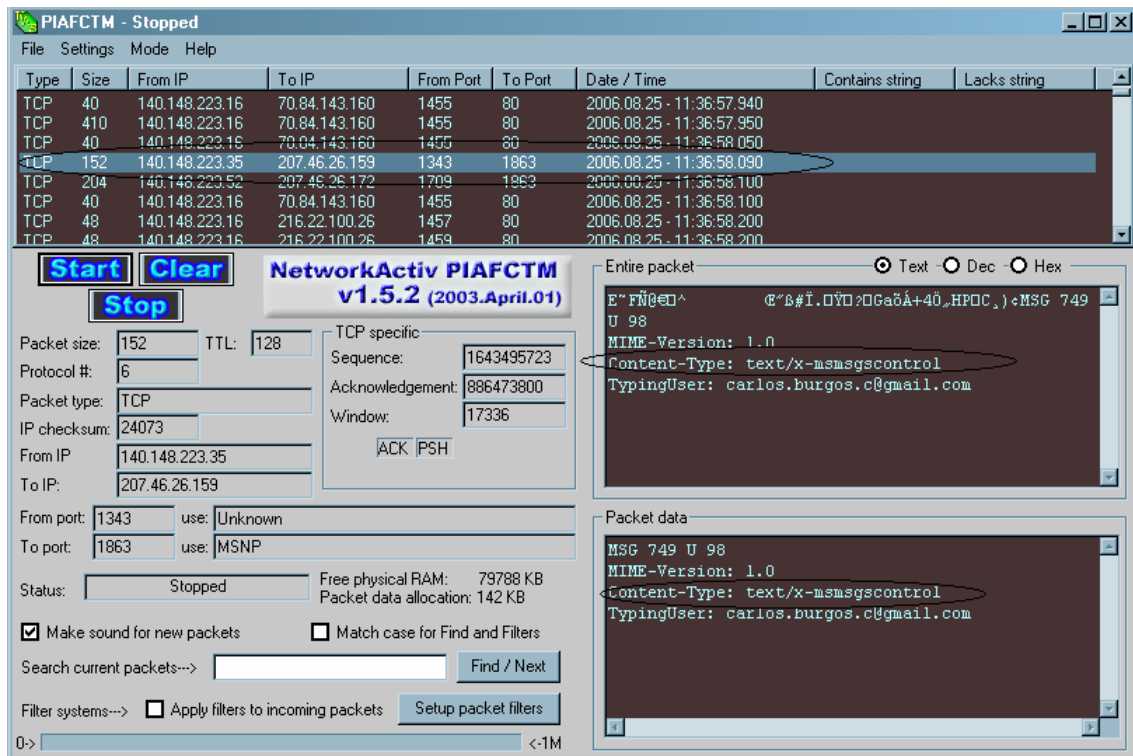
Las siguientes pruebas se hicieron en diferentes áreas de la escuela. En donde se analizó la seguridad en las redes inalámbricas.

#### **Caso**

**Situación:** Diferentes usuarios en sala HU navegaban en la red.

**Vulnerabilidad:** En este caso se analiza el protocolo TCP, en donde como podemos observar en la **Figura 4.3.5** el Content-Type significa que tipo de contenido es el que se está mandando al servidor, existen del tipo text/html, image/png, image/gif etc. En este caso nos muestra que es de tipo text/x-msmsgscontrol, el cual se usa para poder usar la aplicación del Messenger.

Podemos observar cuales son las computadoras que están interactuando en esta aplicación.



[NetworkActive, 2005]

**Figura 4.3.5** Análisis de protocolo TCP

En la **Figura 4.3.6** podemos observar como es que podemos obtener la dirección de correo electrónico de la persona que esta iniciando la conversación por el Messenger. Un dato útil que se nos da es también la hora y fecha y puerto en la que el proceso está siendo ejecutado.

The screenshot shows the NetworkActiv PIACTM v1.5.2 interface. At the top, a table lists network traffic:

Type	Size	From IP	To IP	From Port	To Port	Date / Time	Contains string	Lacks string
TCP	48	140.148.223.16	216.22.100.26	1461	80	2006.08.25 - 11:36:58.220		
TCP	48	140.148.223.16	216.22.100.26	1463	80	2006.08.25 - 11:36:58.240		
TCP	40	140.148.223.52	207.46.26.172	1709	1863	2006.08.25 - 11:36:58.270		
TCP	576	140.148.223.52	207.46.26.172	1709	1863	2006.08.25 - 11:36:58.340		
TCP	168	140.148.223.52	207.46.26.172	1709	1863	2006.08.25 - 11:36:58.340		
TCP	40	140.148.223.16	216.22.100.26	1457	80	2006.08.25 - 11:36:58.350		
TCP	768	140.148.223.16	216.22.100.26	1457	80	2006.08.25 - 11:36:58.350		
TCP	40	140.148.223.16	216.22.100.26	1459	80	2006.08.25 - 11:36:58.350		

The main interface includes controls for starting/stopping the tool and displaying packet details. The 'Entire packet' section shows the following content:

```

P2P-Dest: emil.santos@hotmail.com
00000000  Dtmil.com MSMSLP/1.0
To: <msnmsgr:emil.santos@hotmail.com>
From: <msnmsgr:rolivasg@hotmail.com>
Via: MSMSLP/1.0/TLP
;branch={11C50E23-AF1D-4924-98EA-4F0BB876111A}
CSeq: 0
Call-ID: {C779152E-1F16-4B35-9E96-4DBBD4BC447}

```

The 'Packet data' section shows:

```

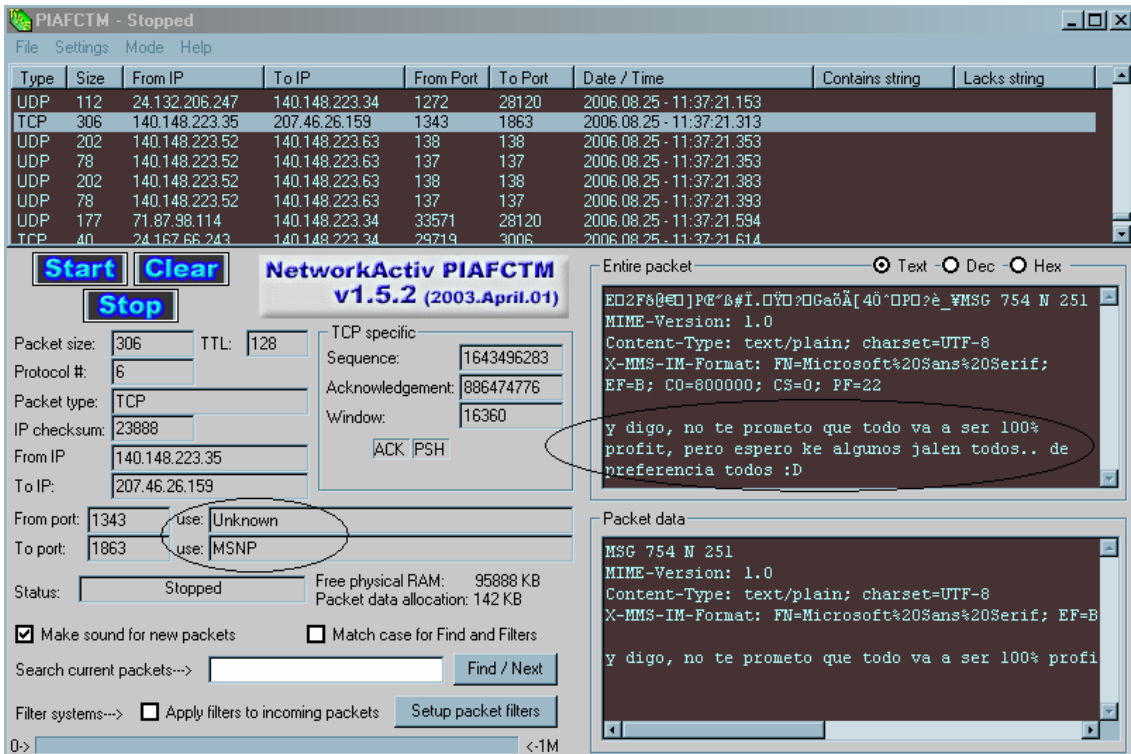
MSG 1494 D 648
MIME-Version: 1.0
Content-Type: application/x-msnmsgrp2p
P2P-Dest: emil.santos@hotmail.com
00000000  Dtmil.com MSMSLP/1.0
To: <msnmsgr:emil.santos@hotmail.com>
From: <msnmsgr:rolivasg@hotmail.com>

```

[NetworkActive, 2005]

**Figura 4.3.6** Obtención de correo electrónico

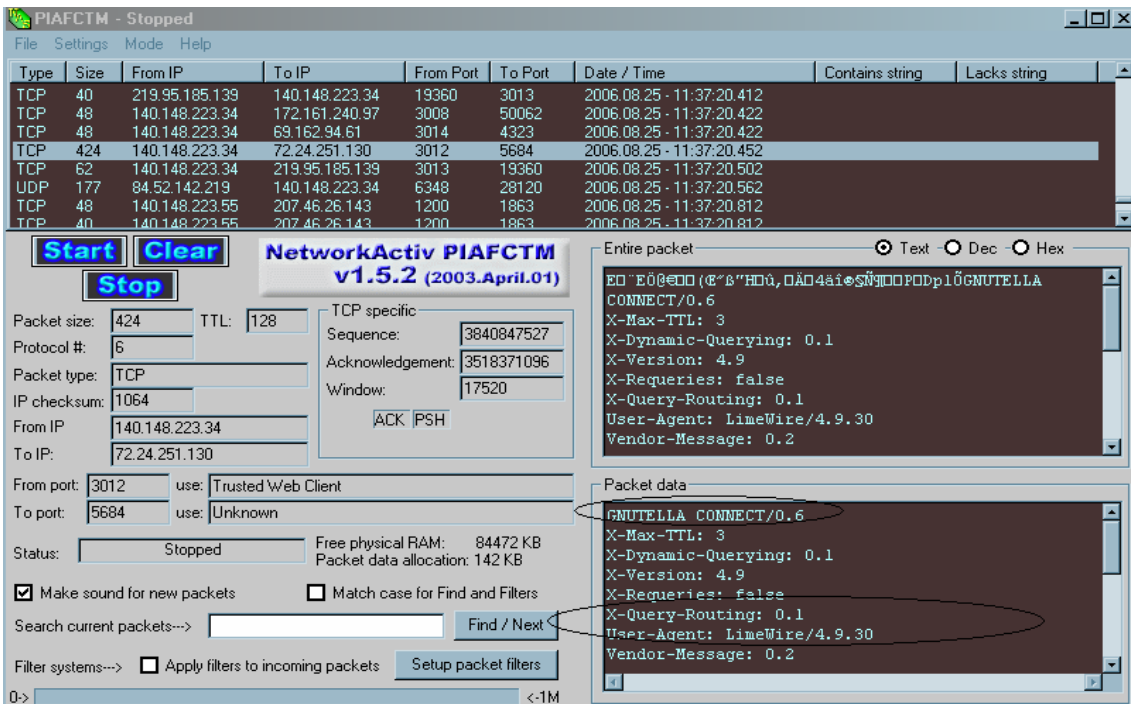
En la **Figura 4.3.7** podemos ver como podemos interceptar los paquetes que son mandados vía Messenger. Otro aspecto importante es que podemos ver que en un determinado puerto que tipo de protocolo se esta corriendo, en este caso el MSNP es un protocolo de conexión de Microsoft para el uso del Messenger.



[NetworkActive, 2005]

Figura 4.3.7 Obtención del mensaje

En este caso algo que es importante que se comente es que los procesos de aplicaciones P2P, se pueden llegar a interceptar también. Se puede ver cualquier tipo de tráfico que este cruzando por la red. **Figura 4.3.8**

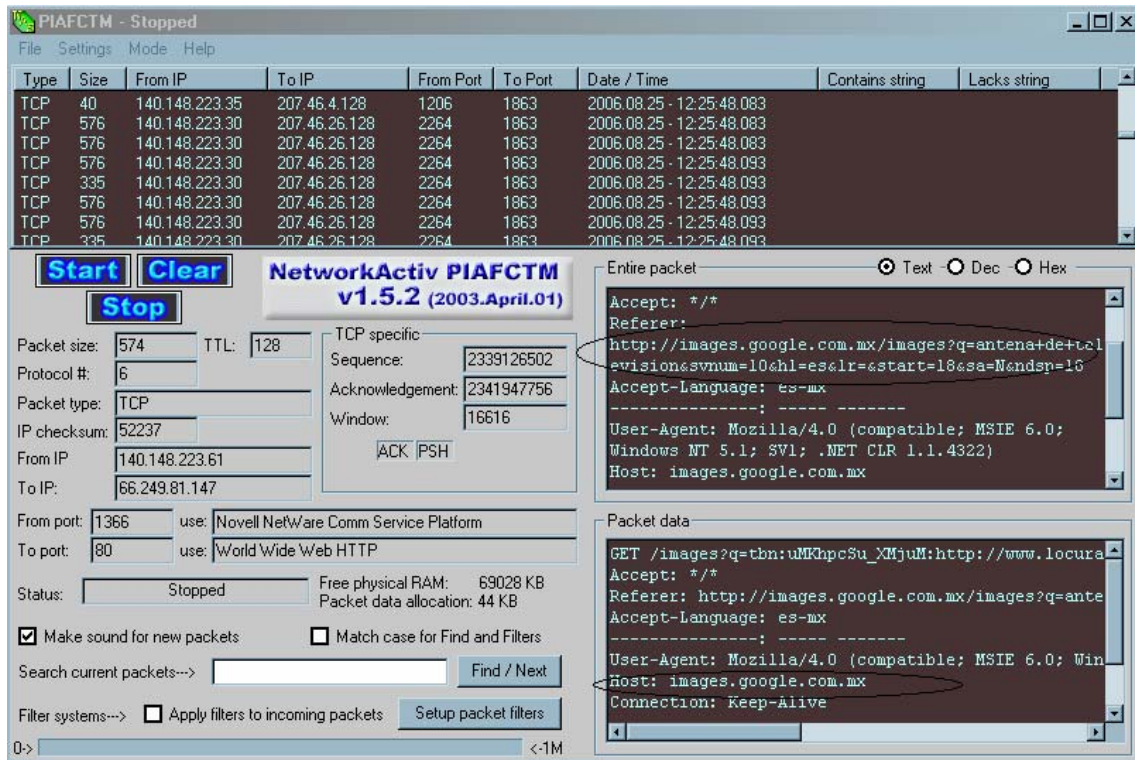


[NetworkActive, 2005]

Figura 4.3.8 Procesos P2P

Podemos observar como al interceptar este paquete obtuvimos exactamente la página que estaba siendo visitada por cierto usuario, en la parte que dice:

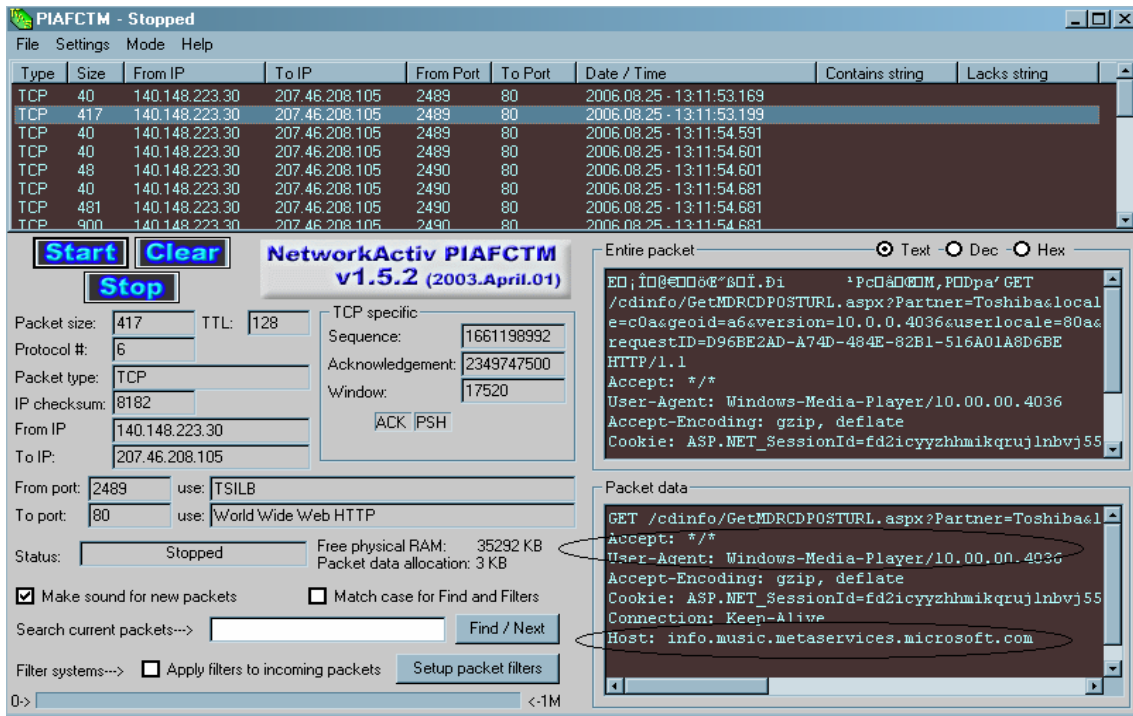
“Referer:http//images.google.com.mx”, **Figura 4.3.9**



[NetworkActive, 2005]

**Figura 4.3.9** Obtención del host

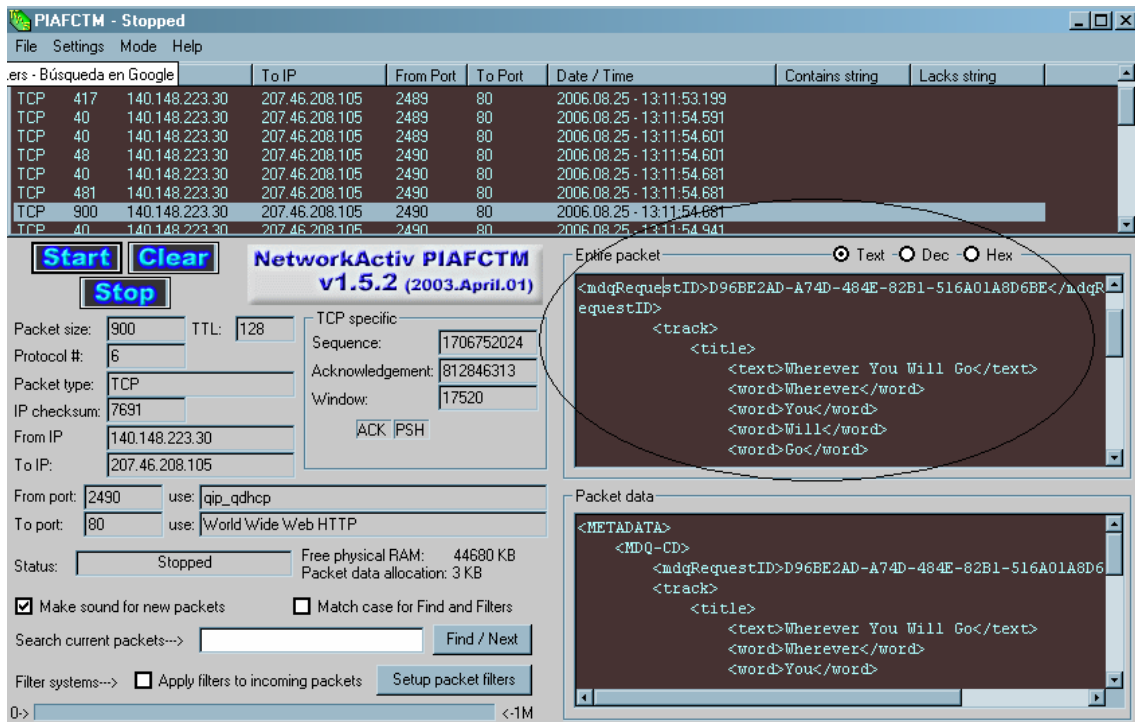
Podemos examinar detalladamente como es además de la información del host también se te da la información acerca de que tipo de reproductor se está usando para reproducir la música. **Figura 4.3.10**



[NetworkActive, 2005]

**Figura 4.3.10 Windows Media Player**

En este caso, **Figura 4.3.11**, se puede observar como es que lo que se manda comprimido por el Windows Media Player puede verse a manera de texto. Se extrae la información que viene empaquetada.



[NetworkActive, 2005]

**Figura 4.3.11 Letra de la canción**



**Daño:** El daño que puede causar este tipo de información la cual se obtiene de manera ilegal puede ocasionar que se violen los derechos de las personas de privacidad. Cualquiera puede correr este tipo de programas y puede andar escaneando a las demás personas sin su autorización. La información podría ser mal intencionada y hasta puede causar problemas con otras personas.

Para saber más acerca de cómo usar este programa, ver el **Apéndice C: NetworkActive**

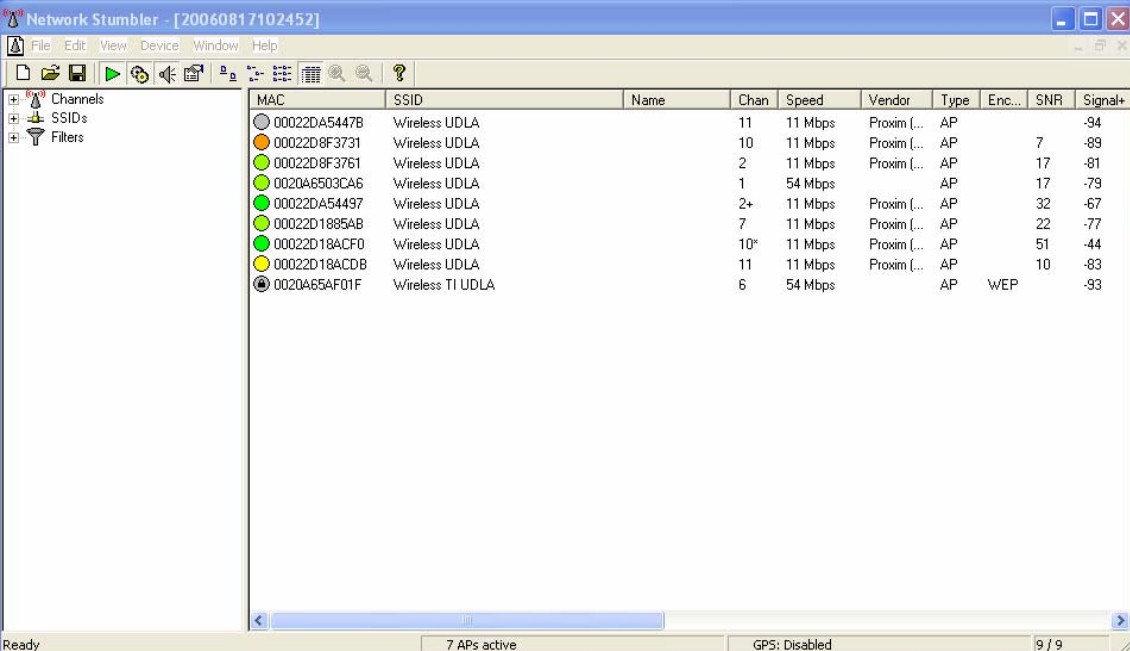
## 4.4 Análisis de seguridad con Netstumbler

**NetStumbler:** es una herramienta que nos sirve para poder ver cuales son los AP que están disponibles en un área en particular.

### Caso

**Situación:** Usuarios están navegando por la red en la sala HU.

**Vulnerabilidad:** Se puede observar a continuación como es que el programa pone en una lista junto con su dirección MAC, el canal en el que se encuentra y otros datos importantes. **Figura 4.4.1**



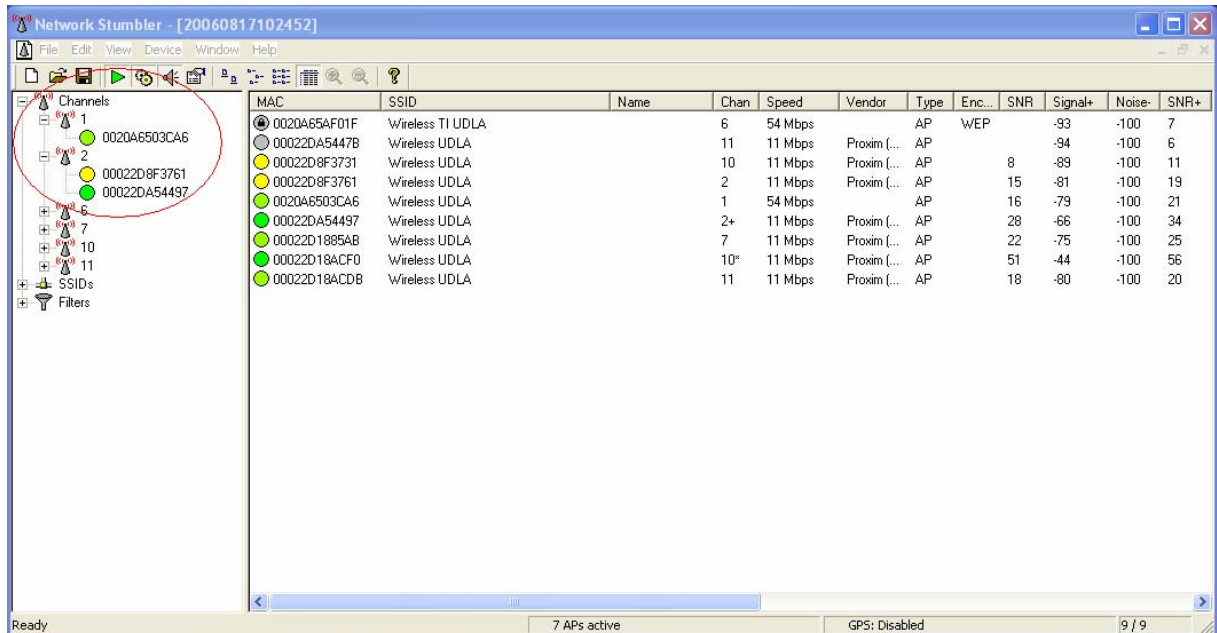
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00022DA5447B	Wireless UDLA		11	11 Mbps	Proxim [...]	AP			-94
00022D8F3731	Wireless UDLA		10	11 Mbps	Proxim [...]	AP		7	-89
00022D8F3761	Wireless UDLA		2	11 Mbps	Proxim [...]	AP		17	-81
0020A6503CA6	Wireless UDLA		1	54 Mbps		AP		17	-79
00022DA54497	Wireless UDLA		2+	11 Mbps	Proxim [...]	AP		32	-67
00022D1895AB	Wireless UDLA		7	11 Mbps	Proxim [...]	AP		22	-77
00022D18ACF0	Wireless UDLA		10*	11 Mbps	Proxim [...]	AP		51	-44
00022D18ACDB	Wireless UDLA		11	11 Mbps	Proxim [...]	AP		10	-83
0020A65AF01F	Wireless TI UDLA		6	54 Mbps		AP	WEP		-93

[NetStumbler, v 0.4.0]

**Figura 4.4.1 Información de AP**

**Daño:** Como se puede observar en el círculo tenemos los canales en las que está disponible una red WIFI, más aparte la información de la MAC etc.

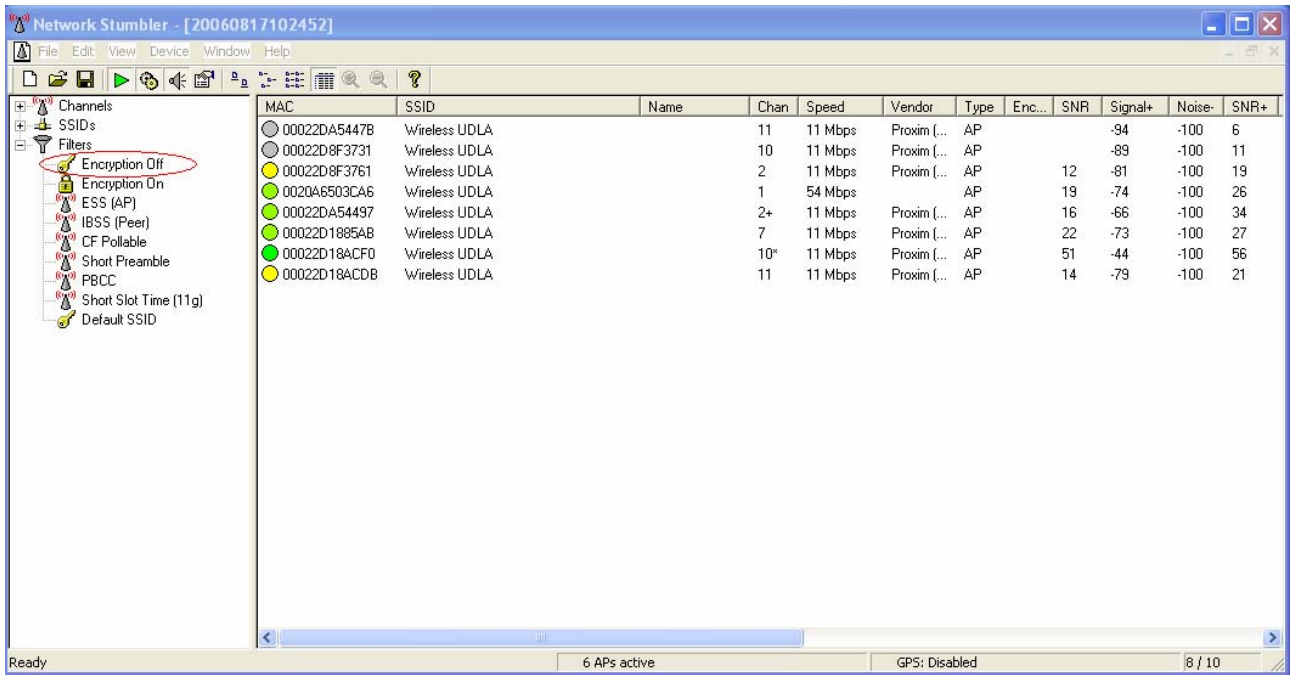
Con esto ya sabríamos a que canal conectarnos para tener acceso a Internet.



[NetStumbler, v 0.4.0]

**Figura 4.4.2 Información sobre MAC**

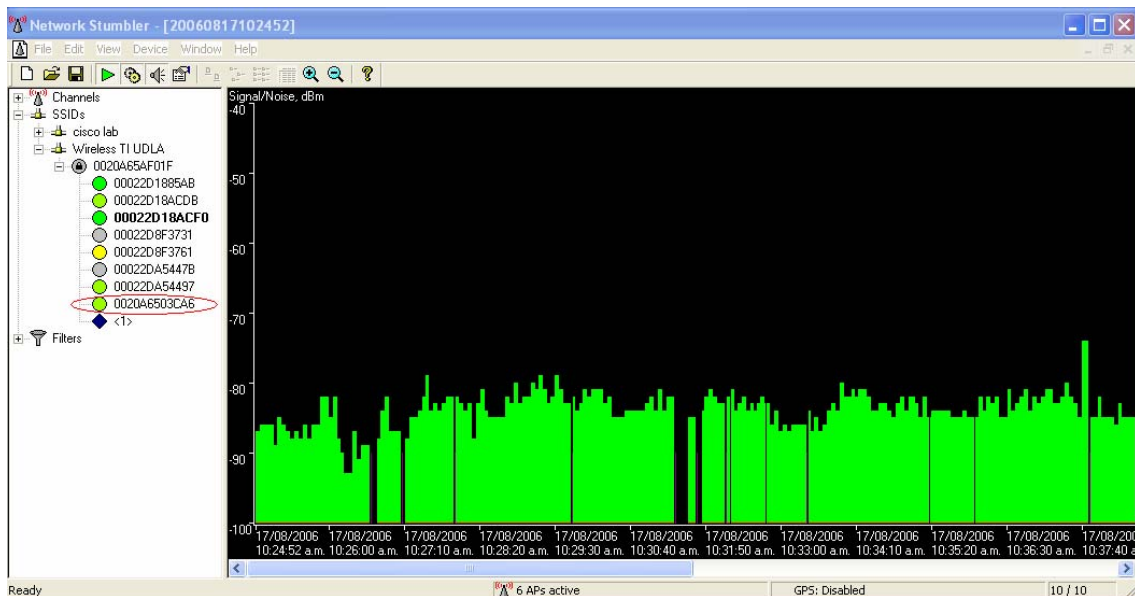
A continuación podemos observar como es que tenemos la opción de que se nos desplieguen los AP que tienen encriptación así como los que no la tienen. **Figura 4.4.3**



[NetStumbler, v 0.4.0]

**Figura 4.4.3 Información sobre seguridad**

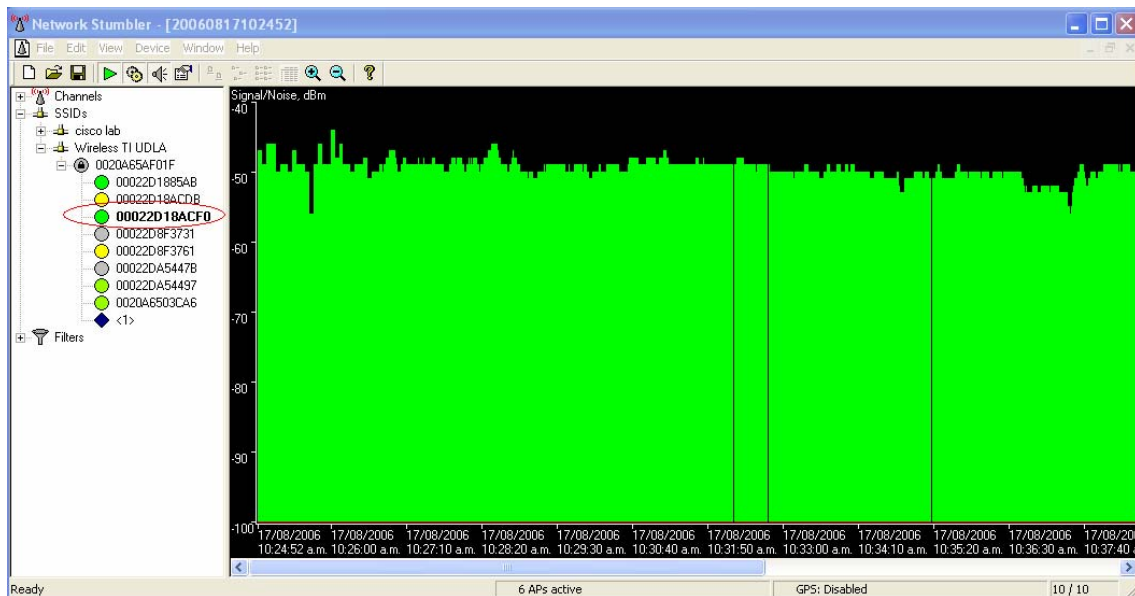
Otro recurso con el que contamos es que podemos observar que tan buena es la señal del AP y esto nos da la facilidad para poder conectarnos al que tenga mejor señal. En este caso esta figura nos muestra un AP con señal muy baja. **Figura 4.4.4**



[NetStumbler, v 0.4.0]

**Figura 4.4.4 Intensidad de señal**

Al contrario de esta **Figura 4.4.5**, la cual nos muestra que existe un AP que tiene muy buena señal al cual nos podemos conectar.



[NetStumbler, v 0.4.0]

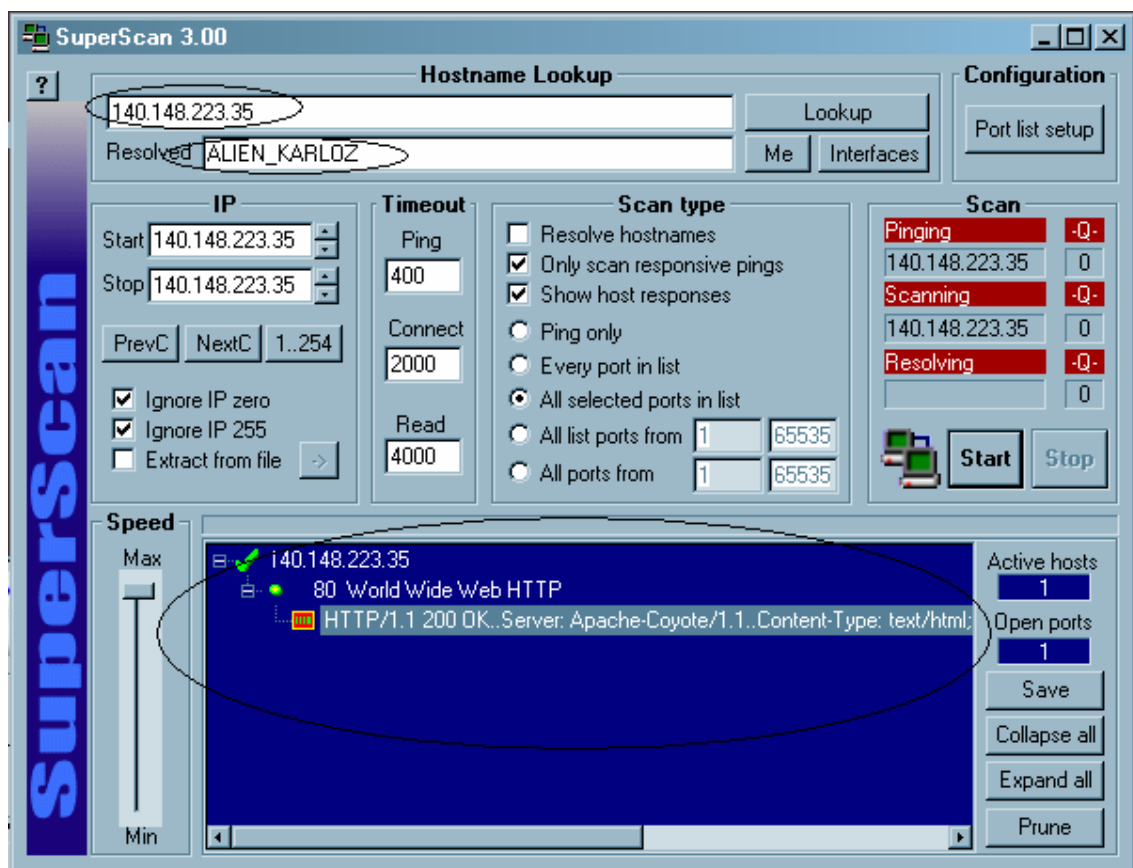
**Figura 4.4.5 Intensidad de señal**

Para saber más acerca de cómo usar este programa, ver el **Apéndice B: NetStumbler**

## 4.5 Pruebas de seguridad con SuperScan

Esta herramienta lo que hacer es escanear todos los puertos de algún IP determinado que se encuentre dentro de la red de donde se corre el SuperScan.

Aquí podemos observar como es que el programa nos muestra el número de IP del usuario al que se le esta haciendo el escaneo al igual que aparece su nombre de usuario y el tipo de protocolos que está ejecutando. **Figura 4.5.1**

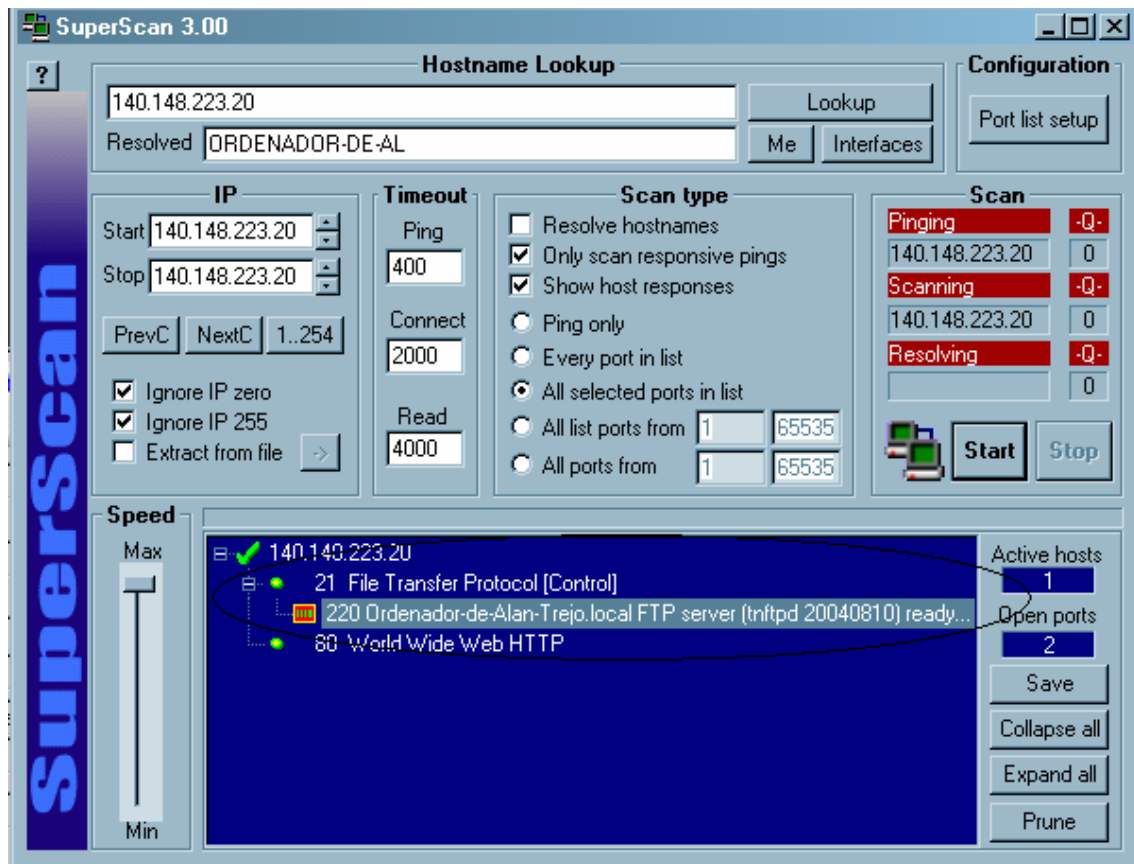


[SuperScan, v3.00]

**Figura 4.5.1** Información de puertos

## Caso

**Situación:** Varios usuarios estaban en sala 4 haciendo sus tareas



[SuperScan, v3.00]

**Figura 4.5.2 Información de FTP**

**Vulnerabilidad:** Se pone a correr el programa y encuentra diversos puertos indicando los servicios que se están usando

**Daño:** Que pasaría si la persona que está escaneando la red se pone a pasar archivos a través de un FTP, como lo indica la **Figura 4.5.2**, la persona podría a llegar a corromper los archivos o a verlos, lo cual sería algo malo para el usuario.

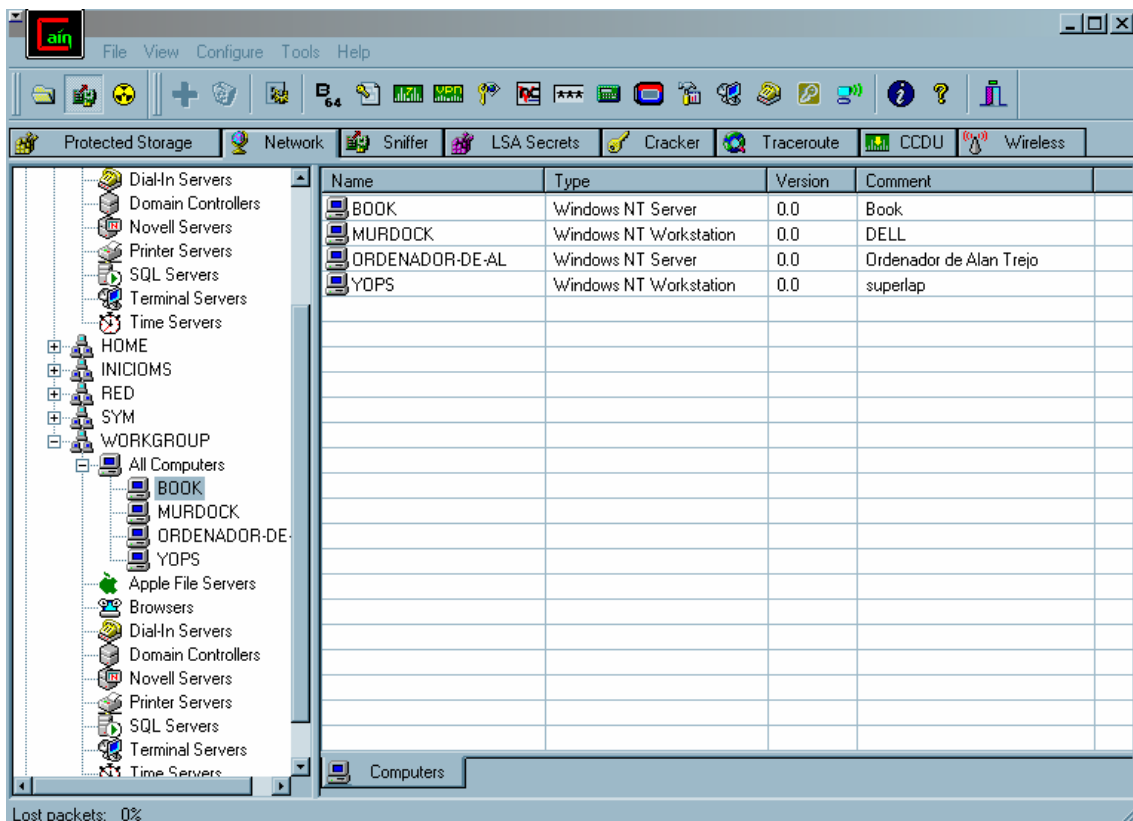
Para saber más acerca de cómo usar este programa, ver el **Apéndice D: SuperScan**

## 4.6 Pruebas de seguridad con Cain & Abel

Cain y Abel es una herramienta que permite recuperar passwords de sistemas operativos tipo Windows. La herramienta es un sniffer la cual como su nombre lo indica, está olfatea la red y recupera todo tipo de passwords que se encuentran en el sistema, así como también recupera los passwords que se encuentran en la memoria caché de la computadora. Recupera todo tipo de credenciales de varias fuentes.

**Situación:** Imaginémonos que existe una empresa muy importante de TI la cual tiene guardados en sus servidores cosas muy importantes. ¿Qué pasaría si alguien supiera cuales son las computadoras donde se guarda la información?

**Vulnerabilidad:** En este caso vemos como el programa dada una red determinada va a sacar información de las computadoras que están conectadas a ese red, se abstrae el nombre de la máquina, SO que se esta usando y cuales de esas computadoras están sirviendo como simple estaciones de trabajo y cuales como servidores. **Figura 4.6.1**



[Massimiliano, 2001]

**Figura 4.6.1 Servidores**

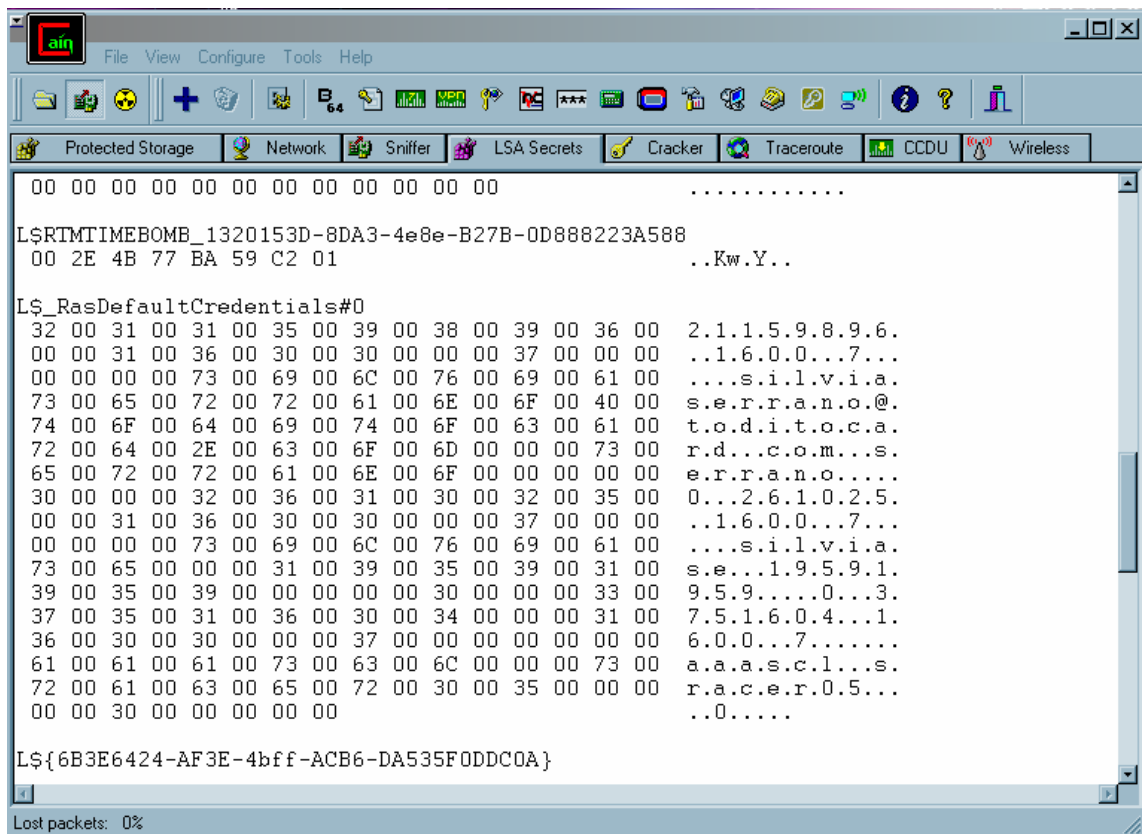


**Daño:** Podemos ver como esto puede ser muy peligroso porque si alguien conoce cual de nuestras computadoras sirve como servidor, personas que quieran dañar el sistema sabrían a cual computadora deben atacar para tirar el servidor y eso sería algo muy crítico para cualquier empresa. En tan sólo pensar en las pérdidas que puede ocasionar.

### Caso

**Situación:** Todo el mundo en las empresas tiene acceso a Internet. Aunque se trata de limitar a que los empleados no tengan un 100% de utilidad en la red, siempre existe una manera para pasar esos obstáculos que no nos dejan ejecutar un cierto servicio.

**Vulnerabilidad:** Existen unos registros que están guardados en ciertos archivos en Windows, esta herramienta puede abstraer cierto tipo de passwords. **Figura 4.6.2**



[Massimiliano, 2001]

**Figura 4.6.2 Credenciales**

**Daño:** Una vez que tenemos las credenciales para acceder al sistema, que pasaría si un trabajador de cierta empresa tiene las claves de acceso y sabe cual es la clave de cierta computadora. Que tal si se mete y encuentra información clasificada. Pueden llegar a ocurrir graves cosas como por ejemplo ver archivos que no le corresponden o la persona pudiera incurrir en el espionaje y vender documentos importantes.

## Caso

### Situación:

**Vulnerabilidad:** Como se puede observar aparte de que nos da la información sobre el IP nos viene ya sea el tipo de computadora que tiene el usuario o mejor aun te da la información de la marca del router. **Figura 4.6.3**

The screenshot shows a network analysis tool interface with a table of network data. The table has columns for IP address, MAC address, DUI fingerprint, Host name, and several other columns (B31, B16, B8, Gr). The data rows list various IP addresses and their corresponding MAC addresses and DUI fingerprints, along with host names like 'Soch\_System\_SYM', 'SARA', 'FRANZISKA', and 'MURDOCK'.

IP address	MAC address	DUI fingerprint	Host name	B31	B16	B8	Gr
140.148.223.61	0014BFEC49BE	Cisco-Linksys LLC	Soch_System_SYM				
140.148.223.56	00C09FA95A4B	QUANTA COMPUTER, INC.	SARA				
140.148.223.49	00904BF1DE49	GemTek Technology Co., Ltd.					
140.148.223.47	0014A53EA11F	Gemtek Technology Co., Ltd.	FRANZISKA				
140.148.223.45	0013CE47AE53	Intel Corporate					
140.148.223.43	00904B58A742	GemTek Technology Co., Ltd.					
140.148.223.36	0011248D4DEB	Apple Computer					
140.148.223.35	000FB002D1A1	Compal Electronics,INC.					
140.148.223.30	00904BF722A2	GemTek Technology Co., Ltd.					
140.148.223.27	0013022BF3FB	Intel Corporate					
140.148.223.24	000E9B850171	Ambit Microsystems Corporation					
140.148.223.21	0011F594887D	ASKEY COMPUTER CORP.	MURDOCK				
140.148.223.20	00112428CBA8	Apple Computer					
140.148.223.17	000D9385E573	Apple Computer					
140.148.223.4	0020A652A500	PROXIM, INC.					
140.148.223.3	0020A652A4FE	PROXIM, INC.					
140.148.223.1	000CDB6CB780	Foundry Networks					
140.148.223.22	0011F5B6A991	ASKEY COMPUTER CORP.					
140.148.223.34	0014A5C4AE2A	Gemtek Technology Co., Ltd.					

[Massimiliano, 2001]

**Figura 4.6.3 Routers**

**Daño:** Uno podría pensar que el saber la marca de un router no es gran cosa, sin embargo, sabemos muy bien que comúnmente al principio en cualquier tipo de equipos salen con algún tipo de hoyo el cual tiene que ser parchado con una actualización. Que tal si sabemos que el router que tiene una escuela es Foundry Networks. Pues en caso de que tenga muy mala suerte la escuela habrá comprado un router que de seguro necesita parches el cual si la persona quiere vulnerar el sistema de la escuela además de saber cual es el router, donde se encuentra, su dirección IP una opción sería checar si ese router que salió tiene algunas parches para así poder tomar ventaja de eso e infiltrarse en el router. Aparte de que ya que uno sabe que tipo de router se tiene es muy fácil meterse a una página y ver que tipos de comandos son los que tiene ese router y así hacerle aun más fácil el acceso al atacante.

Para saber más acerca de cómo usar este programa, ver el **Apéndice E: Cain**

## **Aspectos de Seguridad evaluados**

- Obtención de claves
- Observación puertos abiertos
- Snooping
- Infiltración a routers
- Análisis detalladamente los protocolos de transmisión de información TCP, UDP
- Intercepción de comunicaciones vía Chat.

Como conclusión pudimos observar como es que con las herramientas que analizamos e hicimos pruebas, vimos todo tipo de vulnerabilidades que se pueden presentar en las redes inalámbricas, vimos desde como se pueden interceptar cualquier tipo de protocolos, hasta como es que se pueden recuperar passwords y acceder al sistema de una manera muy sencilla.

