

● ● ● Laura Chappell presents...™



**Make sure you have
appropriate authorization
to run these tools
on your network.**

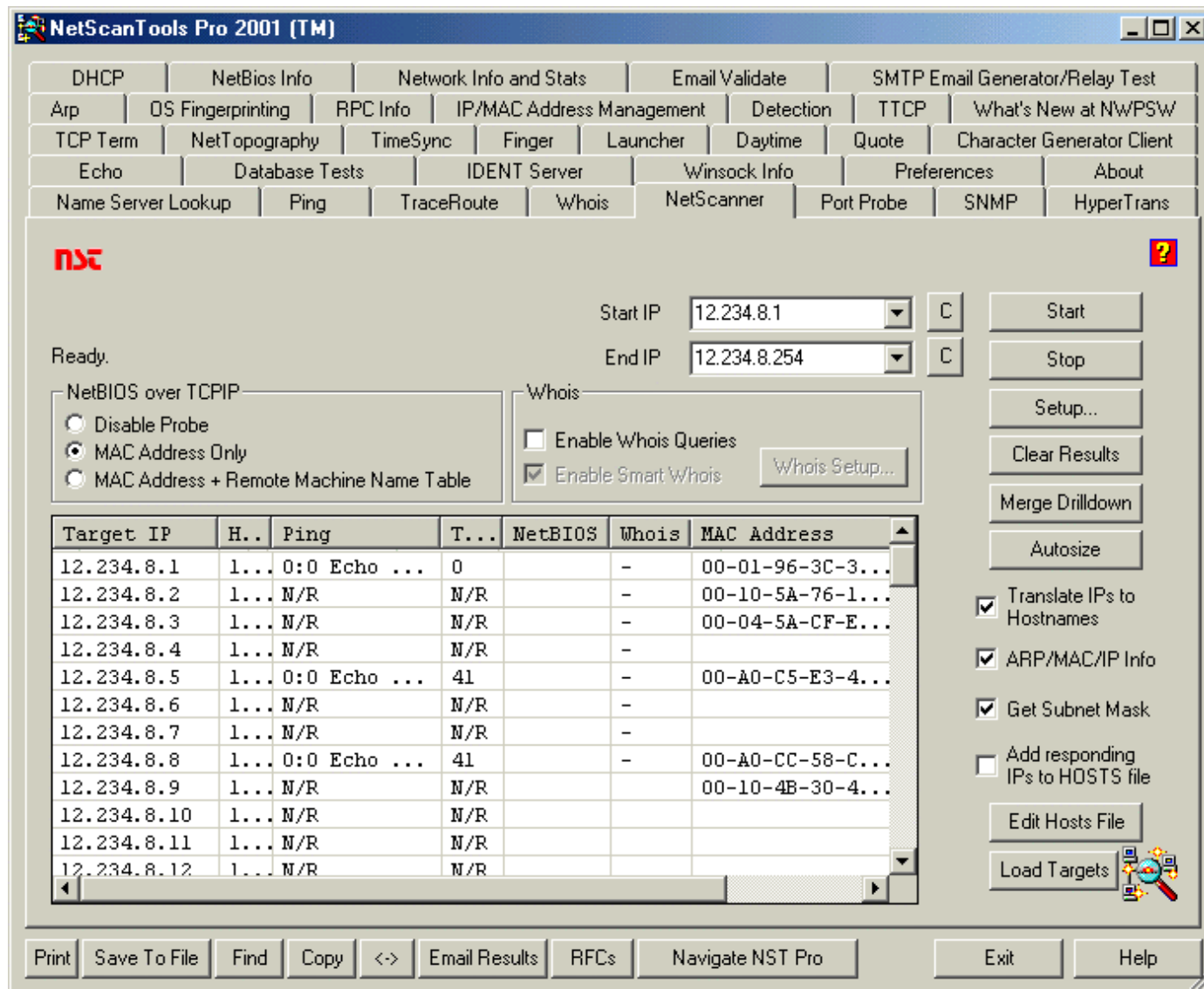
Hacker Tools and Tricks

A look at some of the hottest network troubleshooting, analysis and security tools/tricks around.

2003 Hot Tools List

- NetScanTools Pro\$
- Ethereal
- Sam Spade
- Snort + IDScenter
- onMap
- Ettercap
- Dsniff et al
- Specter (Honeypot)\$
- White Glove/Deception Toolkit\$
- AirMagnet\$
- GPS + Antennas\$
- LC4 (L0phtCrack)\$
- LANGuard\$
- NetStumbler/MiniStumbler
- Invisible Secrets\$
- HexWorkshop\$
- EtherPeek\$
- Sniffer\$
- Iris\$
- Brutus
- Camera Shy
- Ping Plotter\$
- KeyGhost Keylogger\$
- Spycop\$

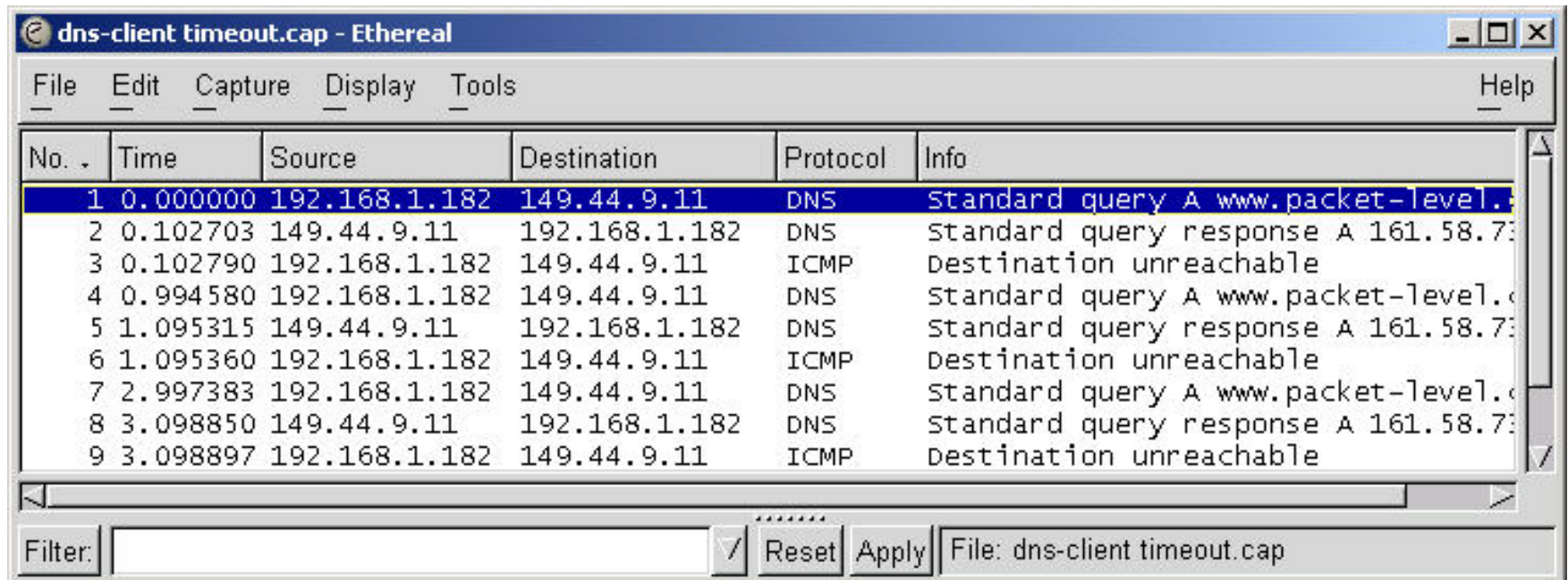
NetScanTools Pro\$ www.netscantools.com



Ethereal

www.ethereal.com

Opens a variety of trace file formats
Filtering (capture, display)
TCP stream reconstruction and analysis
Sortable trace files



Sam Spade

www.samspade.org

The screenshot displays the Sam Spade application window titled "Spade - Fast traceroute novell.com, finished". The interface includes a menu bar (File, Edit, View, Window, Basics, Tools, Help) and a toolbar with icons for Log, Copy, Paste, Ping, DNS, Whois, IPBlock, Dig, Trace, and Finger. The main workspace contains three overlapping windows:

- whois novell.com, finished**: Shows the command "03/01/02 01:15:51 whois novell.com" and the result ".com is a domain of USA & International Co".
- dns novell.com, finished**: Shows the command "03/01/02 01:16:05 dns novell.com" and the result "Canonical name: novell.com".
- Fast traceroute novell.com, finished**: Displays a traceroute visualization with a blue line graph and a table of hop data.

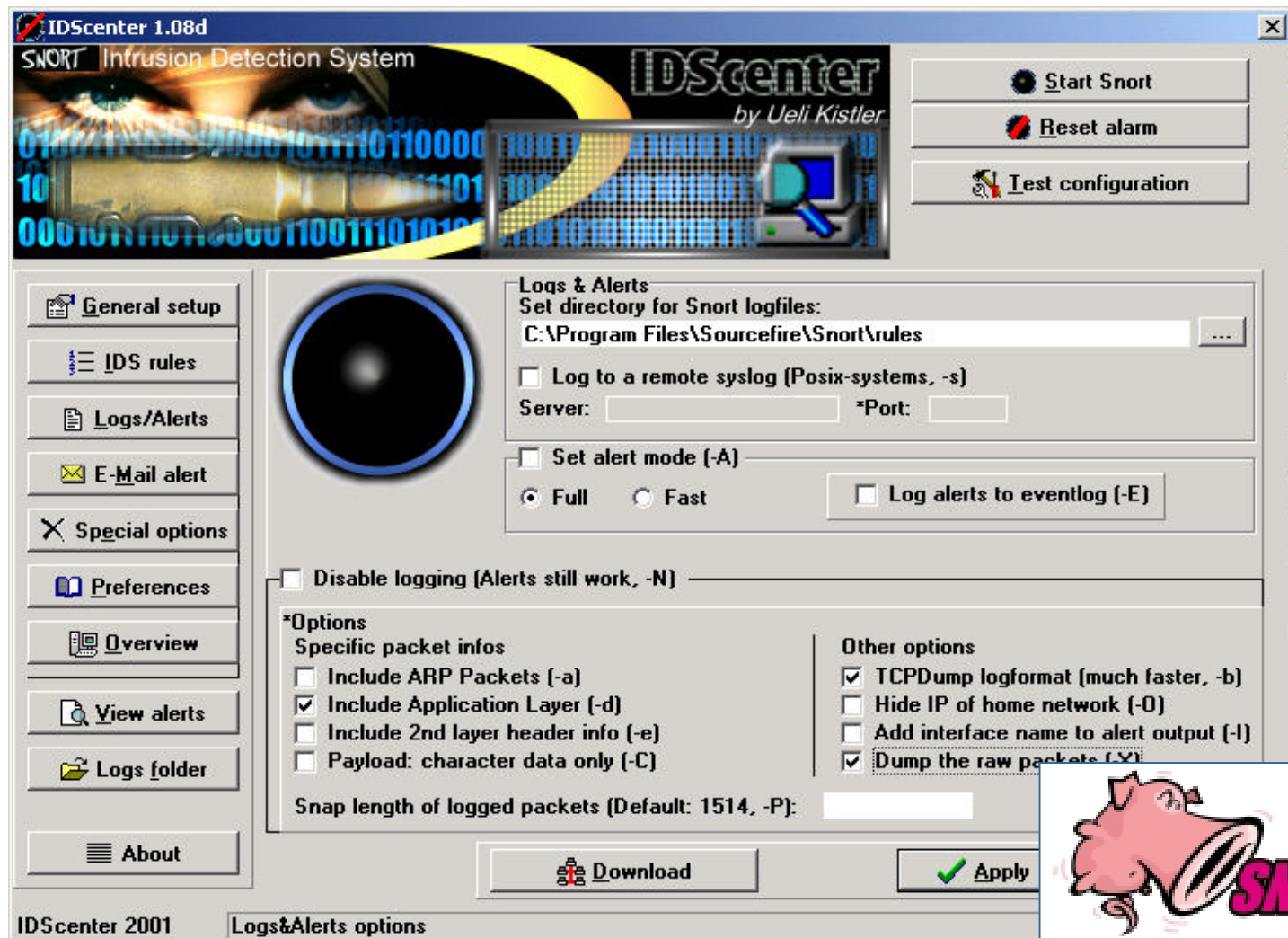
The traceroute table shows the path from the source to the destination (192.233.80.9):

Hop	IP Address	Time to Next Hop (ms)	Time to Destination (ms)
1	10.4.164.97	14ms	14ms
2	12.244.98.193	68ms	0ms
3	12.244.67.17	0ms	14ms
4	12.244.72.206	14ms	41ms
5	12.123.13.62	14ms	14ms
6	12.122.5.254	14ms	28ms
7	12.122.2.245	28ms	27ms
8	12.122.2.241	42ms	41ms
9	12.127.106.34	28ms	27ms
10	192.94.118.223	55ms	55ms
11	192.233.80.9	41ms	41ms

The status bar at the bottom shows the current active window as "novell.com (tracero)" and includes a "For Help, press F1" prompt.

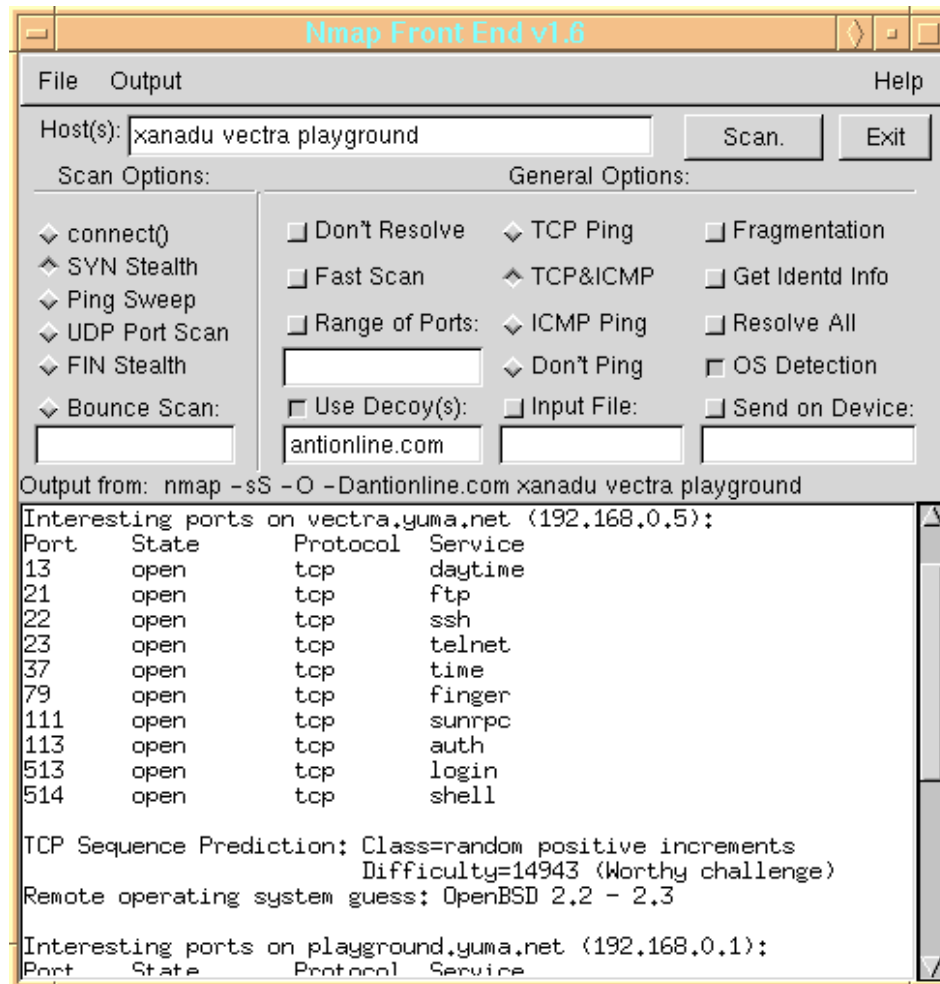
Snort + IDScenter

www.snort.org



nMap

www.insecure.org

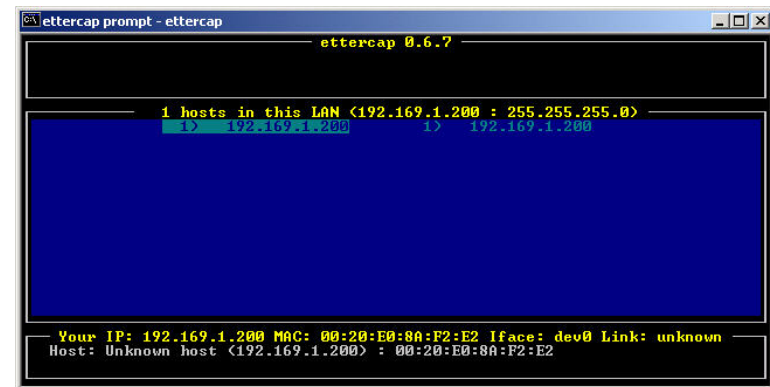


Ettercap

ettercap.sourceforge.net/download

o Dangerous! Warning!

- Uses ARP Poisoning to perform M-i-M attacks
- Character injection in data stream
- Sniffs USER, PASS and data of SSH connections
- Sniffs up SSL data (HTTPS)
- Remote sniffing through GRE tunnel
- Password collector
- Passive/active OS fingerprinting
- Kills connections
- Packet factory

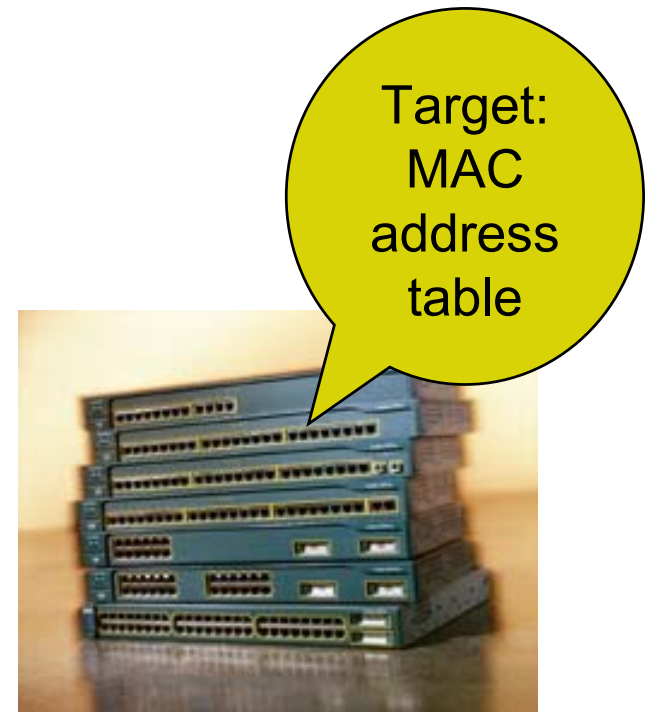


oPassive tools

- Dsniff
- Filesnarf
- Mailsnarf
- Msgsnarf
- Urlsnarf
- Webspy

oActive attack tools

- Arpspoof
- Dnsspoof
- Macof (fail open/duplicate MACs)



Specter Honeypot \$ www.specter.com

Specter Control

S P E C T E R

Engine Version : **S** ?
Threads : ?
Connections so far : ?

Operating System

- ☐ Random
- ☐ Windows 98 ?
- ☐ Windows NT ?
- ☐ Windows 2000 ?
- ☐ Windows XP ?
- ☒ MacOS ?
- ☐ MacOS X ?
- ☐ Linux ?
- ☐ Solaris ?
- ☐ NeXTStep ?
- ☐ Tru64 ?
- ☐ Irix ?
- ☐ Unisys Unix ?
- ☐ AIX ?

Services

- ☒ FTP ?
- ☒ TELNET ?
- ☐ SMTP ?
- ☐ FINGER ?
- ☒ HTTP ?
- ☐ NETBUS ?
- ☒ POP3 ?
- ☒ Provide mails

Intelligence

- ☒ Finger ?
- ☒ Trace Finger ?
- ☒ Port Scan ?
- ☒ DNS Lookup ?
- ☒ Whois ?
- ☒ Telnet Banner ?
- ☒ Ftp Banner ?
- ☒ SmtP Banner ?
- ☒ Http Header ?
- ☒ Http Doc. ?
- ☒ Trace Route ?

Max. Hops **60**

Traps

- ☒ DNS ?
- ☒ IMAP4 ?
- ☒ SUN-RPC ?
- ☒ SSH ?
- ☒ SUB-7 ?
- ☒ BO2K ?
- ☐ GENERIC ?

Generic Trap Name
MYTRAP

Generic Trap Port
5544

Password Type

- ☐ Easy ?
- ☐ Normal ?
- ☐ Hard ?
- ☐ Mean ?
- ☐ Fun ?
- ☒ Cheswick ?
- ☐ Warning ?

- ☐ Send PW file ?

Notification

- ☒ Incident DB ?
- ☐ Alert mail ?
- ☐ Short mail ?
- ☐ Status mail ?
- ☒ Event log ?
- ☐ Syslog ?

Priority

- ☒ Emergency
- ☐ Alert
- ☐ Critical
- ☐ Error
- ☐ Warning
- ☐ Notice
- ☐ Informational

Facility

- ☒ Kernel
- ☐ User
- ☐ Security

Syslog Server IP Address
?

Engine Messages

FTP : 192.168.1.113 on Fri Feb 21 11:53:23 2003

Services Status

- FTP **stopped**
- TELNET **stopped**
- SMTP **stopped**
- FINGER **stopped**
- HTTP **stopped**
- NETBUS **stopped**
- DNS **stopped**
- SUB-7 **stopped**
- SUN-RPC **stopped**
- POP3 **stopped**
- IMAP4 **stopped**
- BO2K **stopped**
- SSH **stopped**
- GENERIC **stopped**

Start Engine **Reconfigure** **Load** **About**

Stop Engine **Log Analyzer** **Save** **License**

Host Name : **bill-the-bloodsucking-tic** ?

System Name : **imac4me** ?

Configuration Version : **1.0** ?

Mail Server IP Address : ?

Mail Address : ?

Short Mail Address : ?

☐ Include settings in mails ?

Status Mail Period [h] : **24** ?

☐ Remote Management Port : **28** **Set Password** ?

☐ Expect friendly connections **IP Addresses** ?

☐ Use custom mail message for POP3 **Edit Message** ?

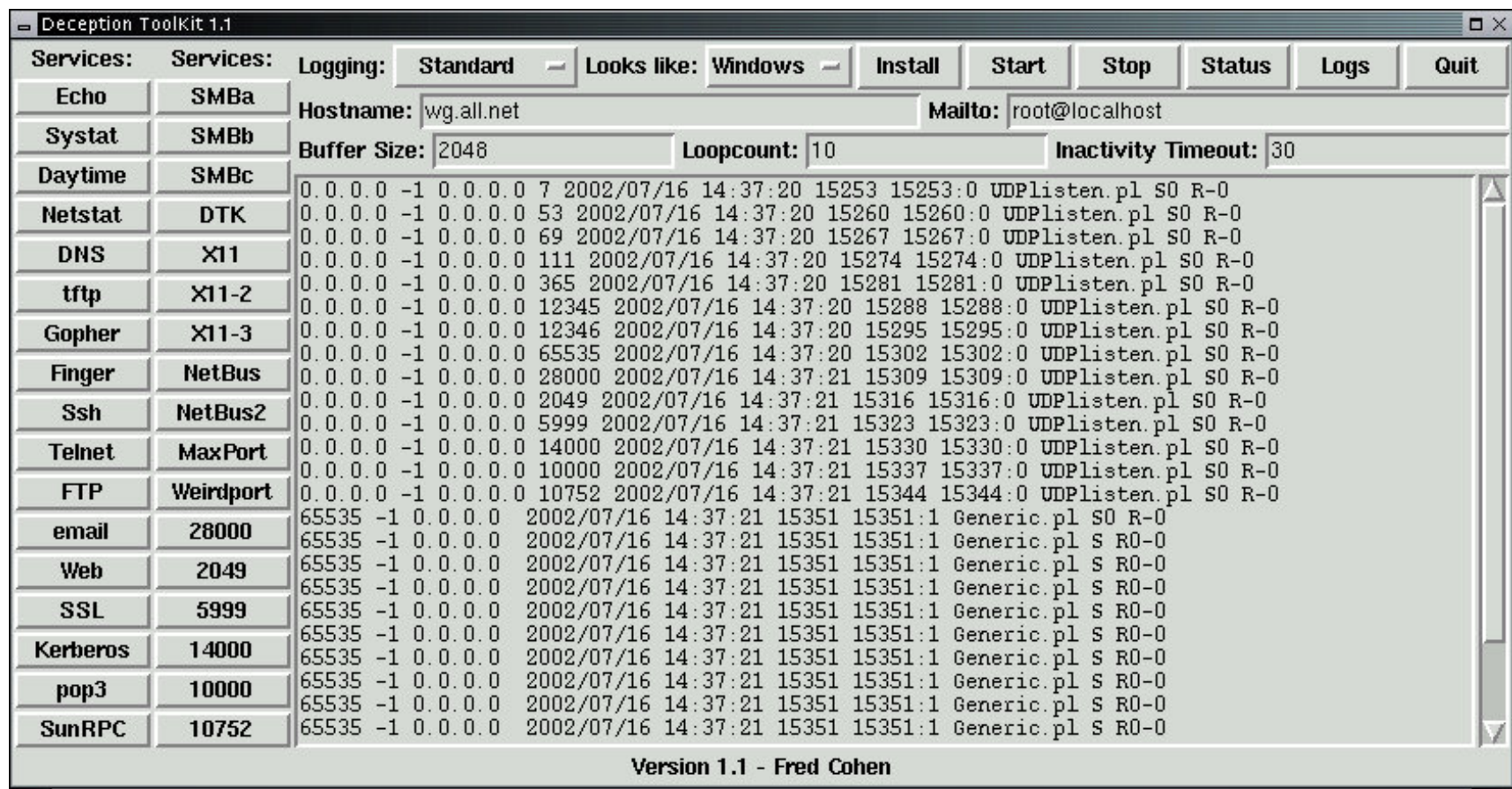
☒ Use custom warning message ?

good to see you again fred

White Glove \$/Deception Toolkit

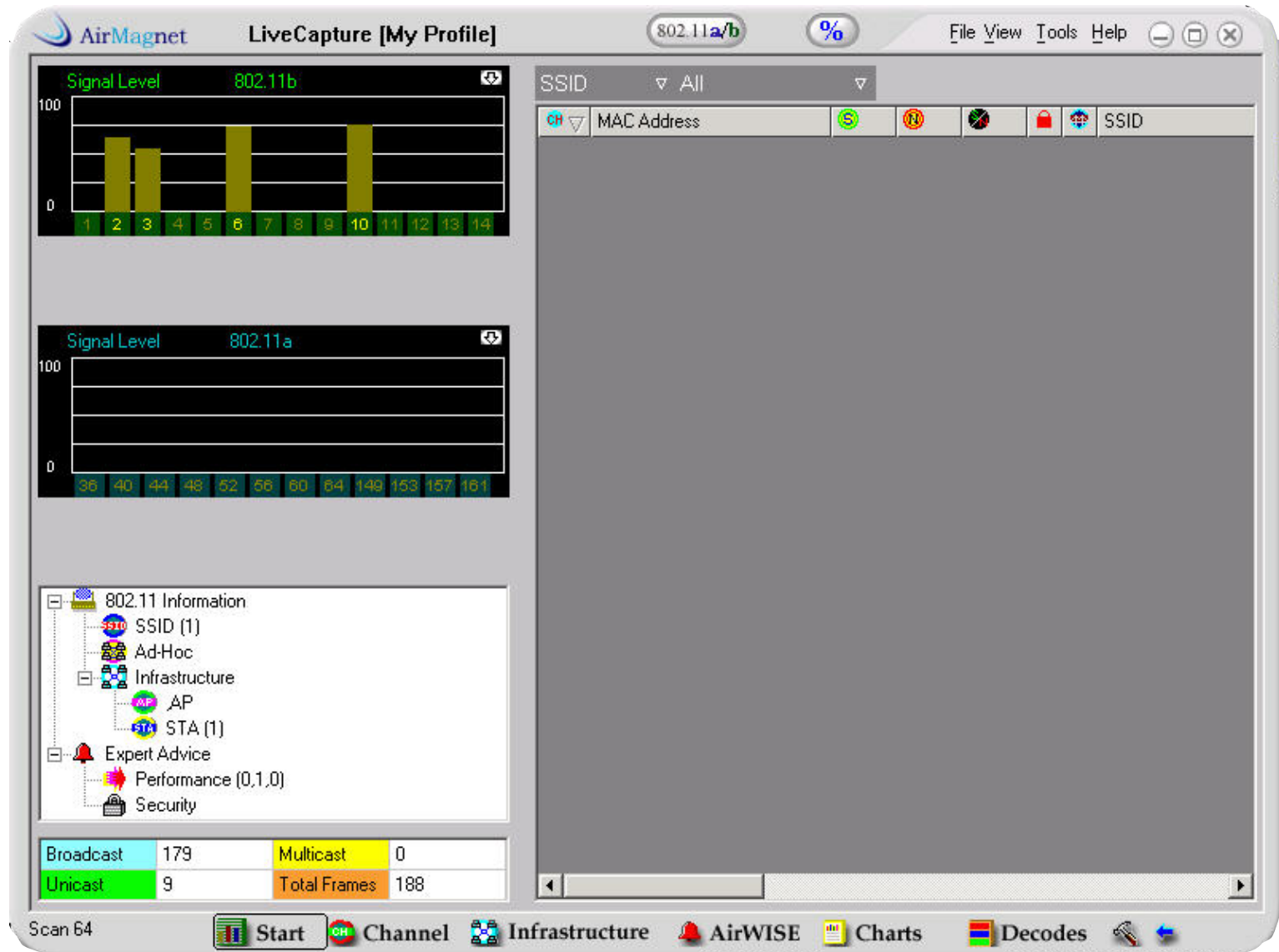
www.all.net

Deception Toolkit (DTK) on White Glove



AirMagnet \$

www.airmagnet.com



GPS\$ + Antennas \$

www.fab-corp.com

pigtails



amplifiers



antennas



LC4 \$ (L0phtCrack)

www.@stake.com

- Password cracking tool
– excellent!

- Uh... er... I mean
Password auditing and
recovery tool!

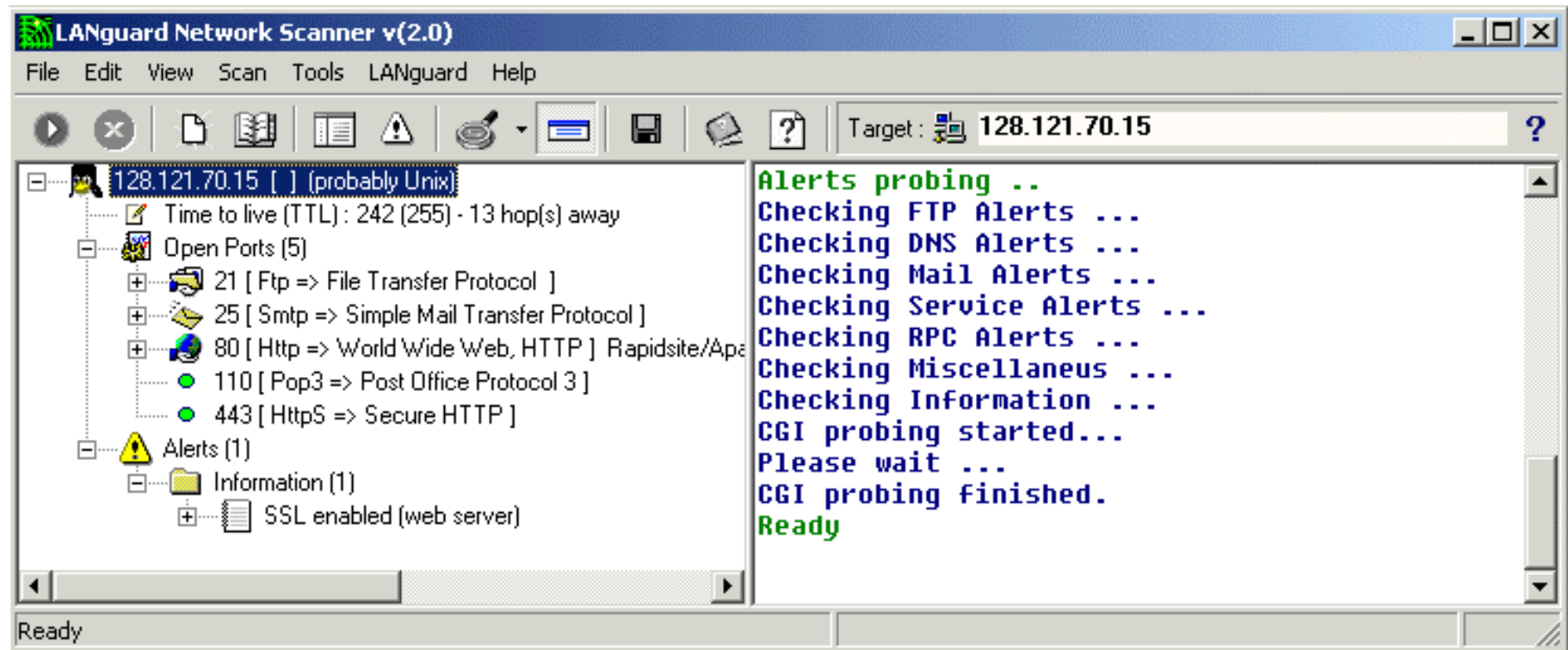
- Also check out John the
Ripper

www.openwall.com/john/



LANGuard\$

www.gfi.com



NetStumbler/MiniStumbler

www.netstumbler.com

The image shows two windows from the NetStumbler suite. The main window, titled 'City 2.ns1', displays a list of detected wireless networks. It has a sidebar on the left with 'Channels' (1-11) and 'SSIDs' (0ab100, 0B1AD0Be, 0d8004, AirReality). The main table lists networks with columns for MAC, SSID, Name, Channel, Vendor, Type, WEP, SN, and Signal. The entry '00022D0D71...' with SSID '0ab100' is highlighted.

MAC	SSID	Name	Ch...	Vendor	Type	WEP	SN...	Si...
00022D05BD...	Network		7	Agere...	AP			-8...
00045AFA7F...	mitsui		6	Linksys	AP			86...
00045A0E98...	linksys		6					
00045A0F0D...	iannucci		6					
00601D218A31	sas airport		4					
00022D2FAA...	TheBullNet2D		4					
00045ACFF4...	linksys		6					
00022D0D71...	0ab100		1					
00501806C16E	default		6					
00045AD168...	home		6					
008037514D53	SFD		3					
00045ADBB...	0B1AD0Be		10					
0030AB0AD4...	Wireless		6					
00045AFA49...	linksys		6					
00045AD226...	Hamp		6					
00045ACC42...	TBNMDU1		1					

Overlaid on the bottom right is the 'MiniStumbler' window, which shows a similar list of networks. The entry '00022D03FF1F' with SSID 'Michael' is highlighted with a yellow box. The status bar at the bottom of the MiniStumbler window shows 'Ready', 'Not scanning', 'GPS Off', and a signal strength of '94'.

Invisible Secrets\$

www.neobytesolutions.com

LSB Steganography
Data injection or data replacement

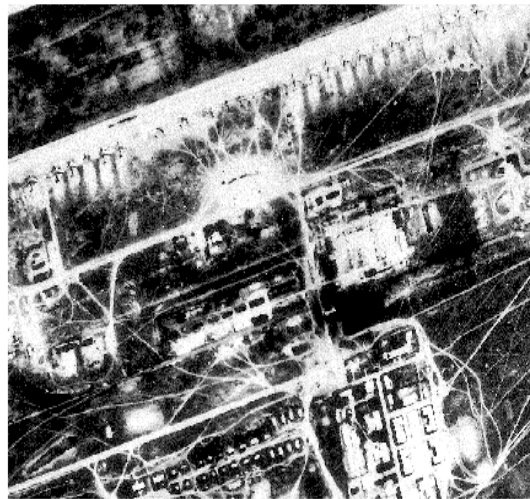


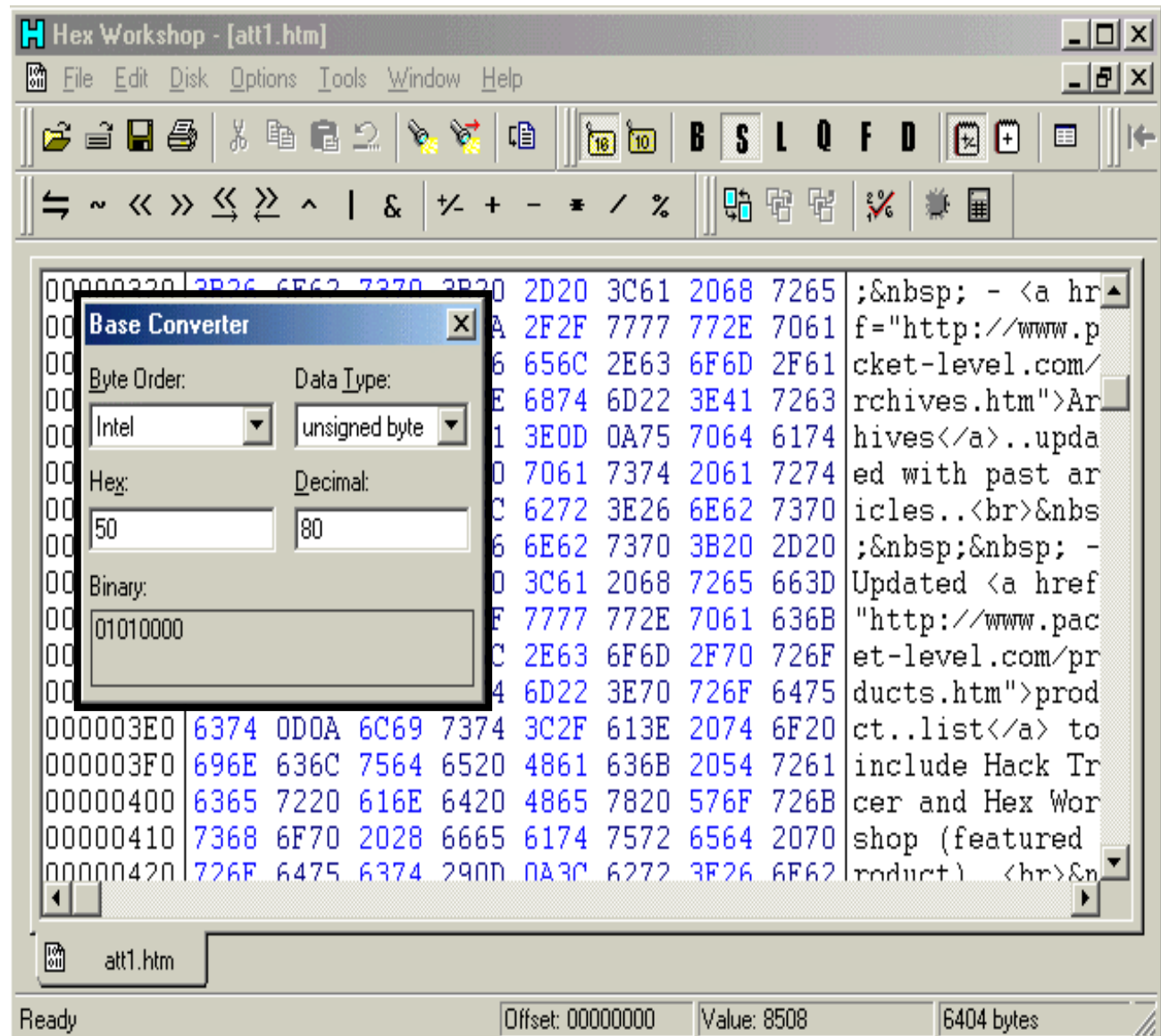
Figure 4: Long-Range Aviation Airfield⁵

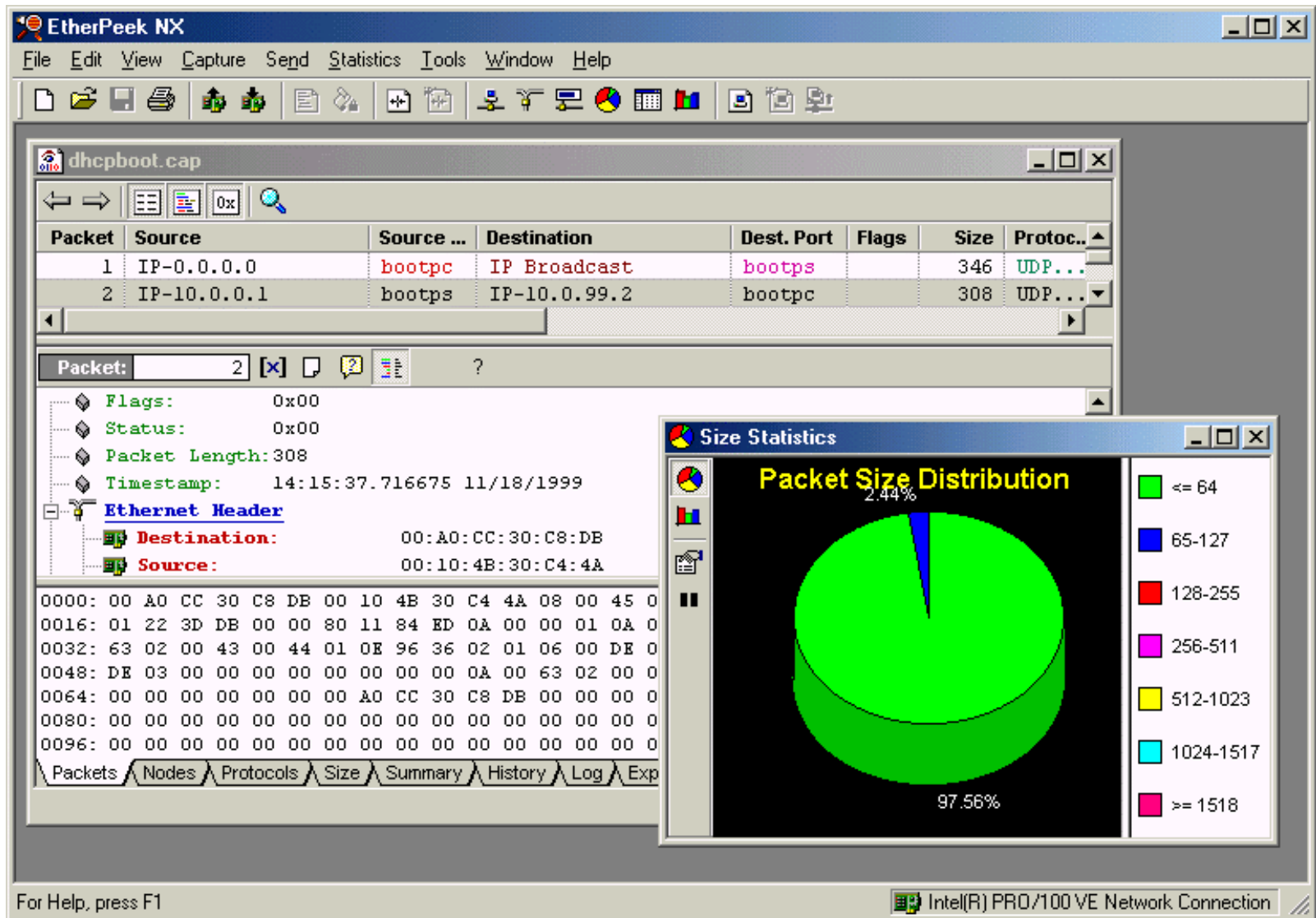


Carrier + Secret = Stego Image

HexWorkshop\$

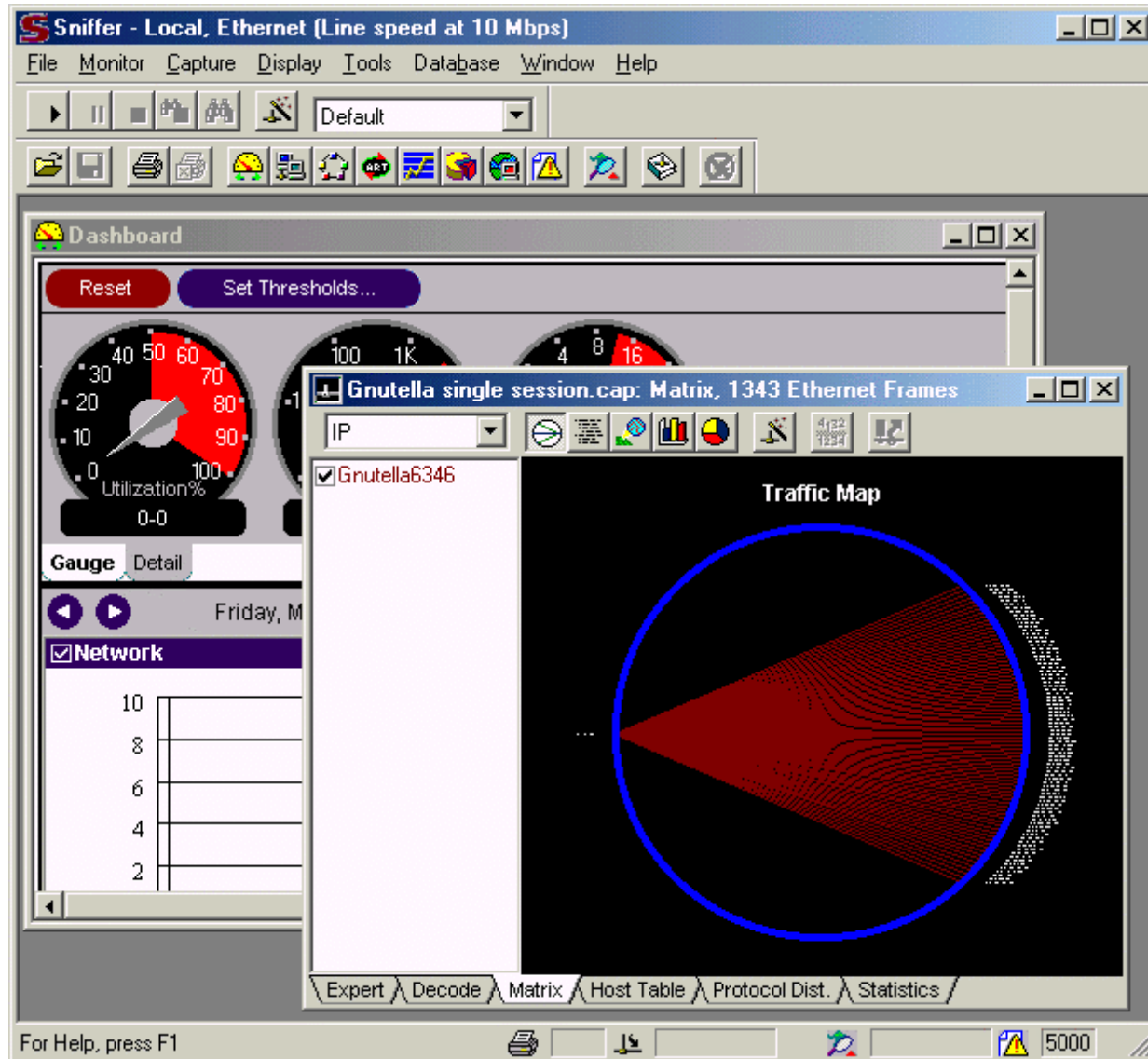
www.bpsoft.com





Sniffer\$

www.sniffer.com



IRIS v3.1

File View Capture Decode Filters Tools Help

Capture

Packet Decoder

Packet structure

- MAC header (Ethernet II)**
 - Destination: 08:00:46:0D:53:E9
 - Source: 00:06:29:CF:A6:77
 - Type: 08-00 DoD IP
- IPv4 header**
 - Version = 4
 - Header length = 5 (20 bytes)
 - Type of service = 00
 - 00000000 = 0 Low priority
 - 00000000 = Normal delay sensitive
 - 00000000 = Normal throughput sensitive
 - 00000000 = Normal reliability sensitive
 - Total length = 40 bytes
 - Identification = 43470
 - Flags
 - 00000000 unused = 0
 - 00000000 Don't fragment
 - 00000000 More fragments

No.	MAC source addr	MAC dest. addr	Frame	Protocol
113	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
114	SONY-0d53e9	IBM-cfa677	IP	TCP-> NETBIOS-SSN
115	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
116	SONY-0d53e9	IBM-cfa677	IP	TCP-> NETBIOS-SSN
117	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
118	SONY-0d53e9	IBM-cfa677	IP	TCP-> NETBIOS-SSN
119	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
120	00:80:29:00:3F:BC	Broadcast	802.3	IPX
121	00:80:29:00:3F:BC	Broadcast	802.3	IPX
122	00:80:29:00:3F:BC	Broadcast	802.3	IPX
123	00:80:29:00:3F:BC	Broadcast	802.3	IPX

0000 08 00 46 0D 53 E9 00 06 29 CF A6 77 08 00 45 00 ..F.S
 0010 00 28 A9 CE 40 00 80 06 CC E1 C0 A8 01 C8 C0 A8 .(@I@
 0020 01 07 09 7F 00 8B F0 45 64 BD 2A F9 6A F0 50 11 ..Q..
 0030 3F F9 F6 C3 00 00 00 00 00 00 00 00 00 00 00 00 ?ùöÃ.

This is the packet editor window. You can bring a packet here by clicking one in packets list or you can create a new one by clicking on [New] button. This editor supports the usual edit commands met in standard editors (copy, paste, insert, etc).

Done CPU: 1% 123/2000 IP: 192.168.1.7 MAC: 08:00:46:0D:53:E9 Intel 825

Brutus

www.hoobie.net/brutus

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target Type

Connection Options

Port Connections Timeout ☐ Use Proxy

Telnet Options

☐ Try to stay connected for attempts

Authentication Options

☒ Use Username ☐ Single User Pass Mode

User File Pass File

Positive Authentication Results

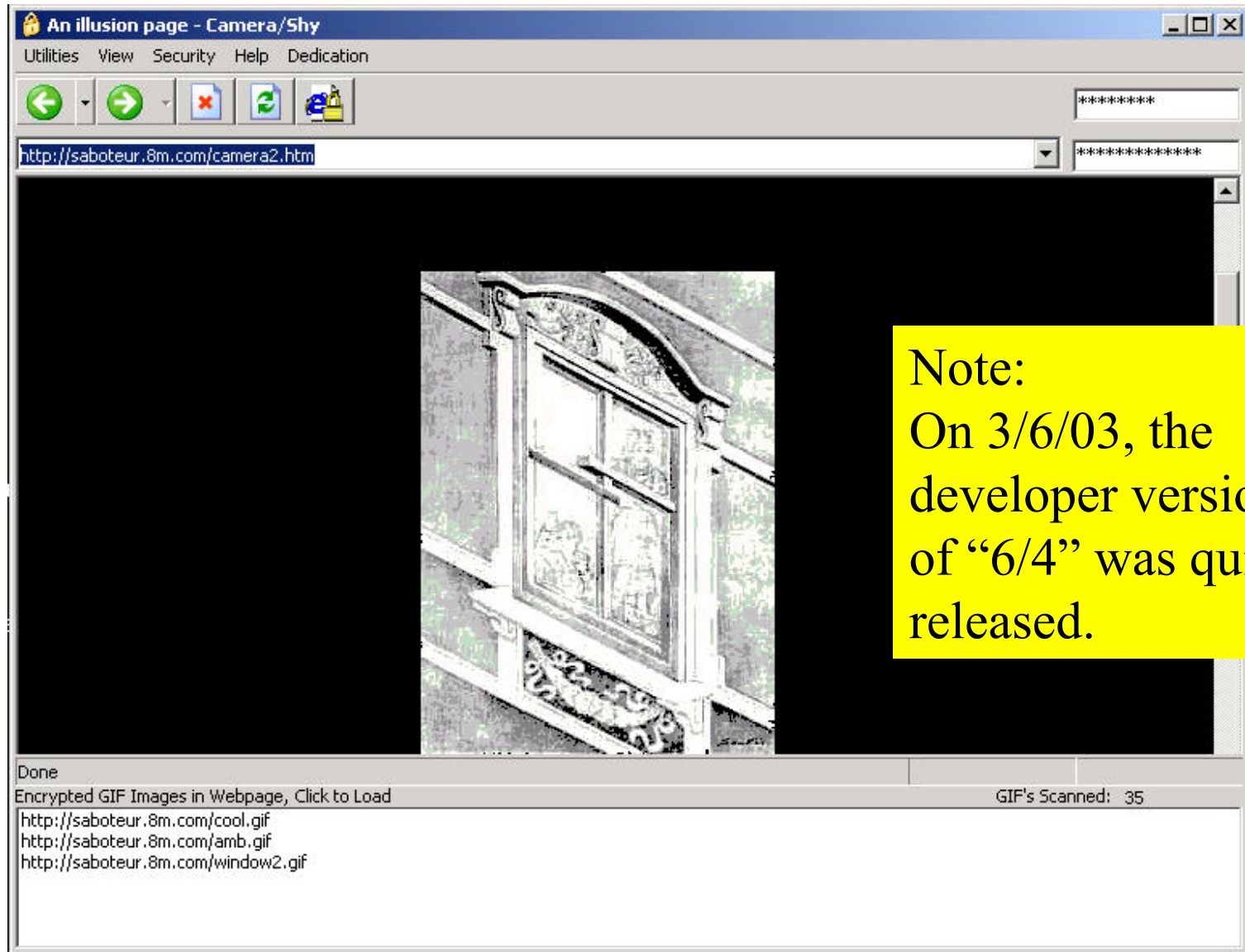
Target	Type	Username	Password
Located and installed 10 authentication plug-ins			

0%

Idle

Camera Shy

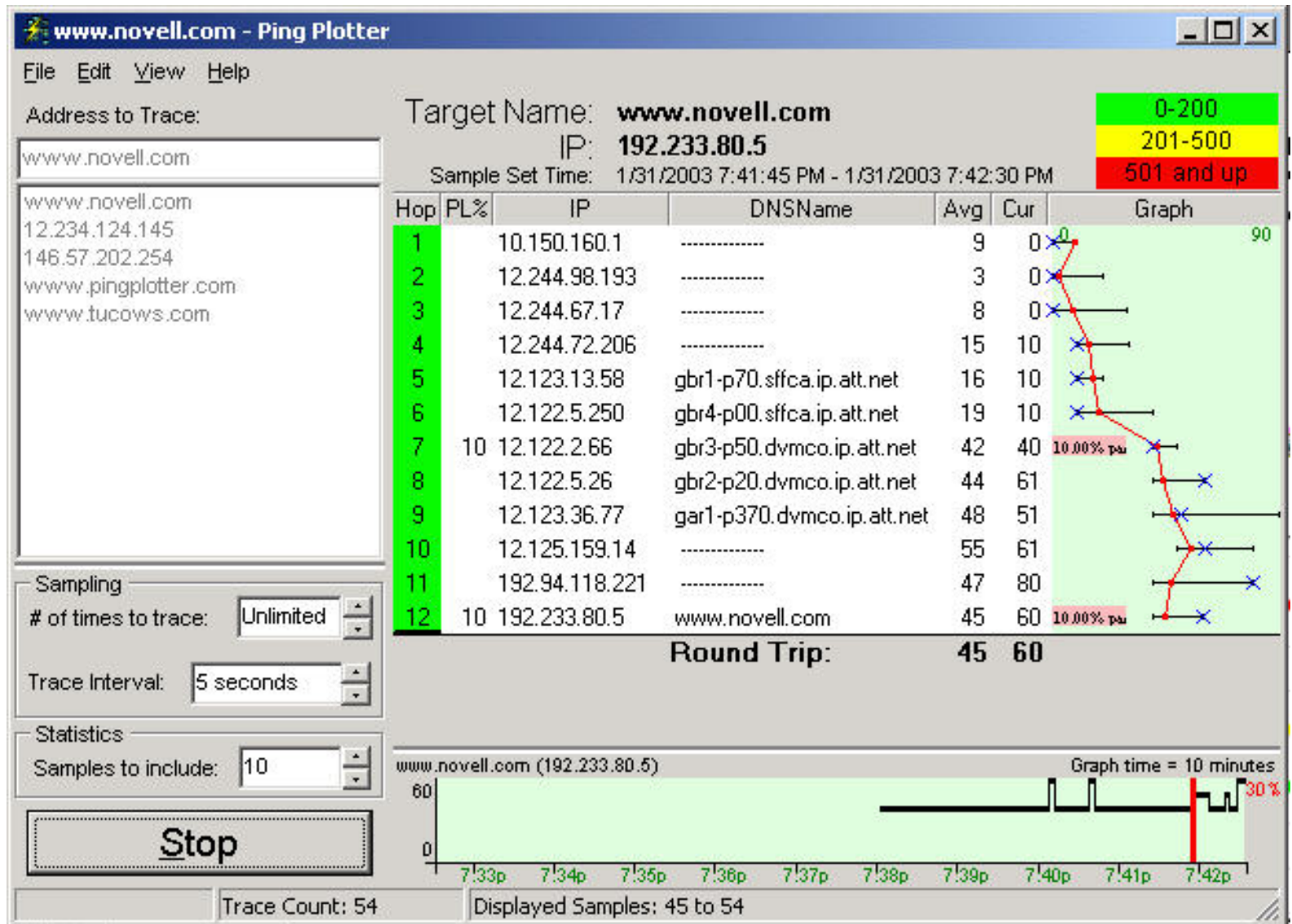
www.hactivismo.com



Note:
On 3/6/03, the
developer version
of "6/4" was quietly
released.

Ping Plotter\$

www.pingplotter.com

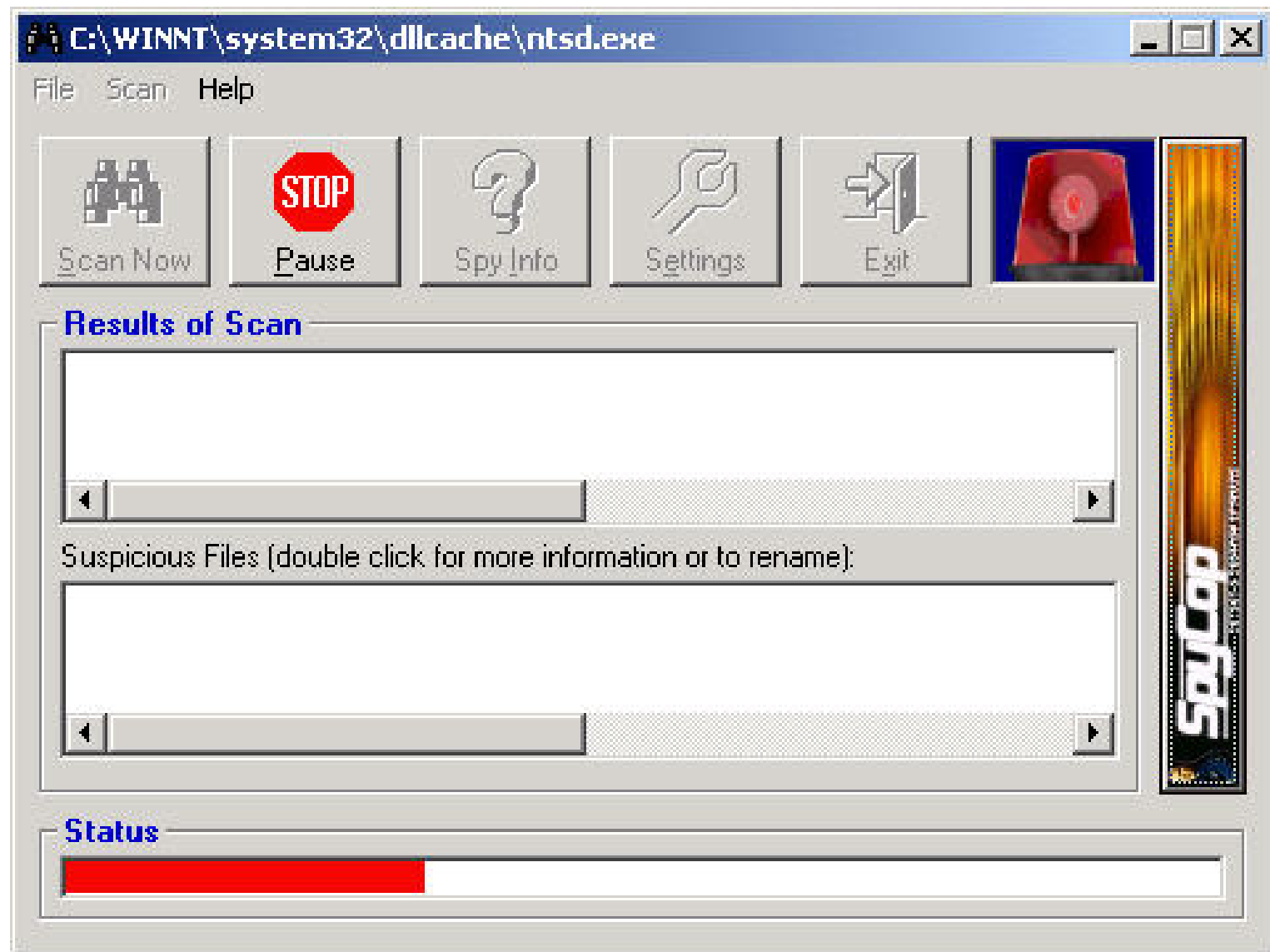


KeyGhost Keylogger\$ www.keyghost.com



Spycop\$

www.spycop.com



Laura's Lab Kit

- Available at www.podbooks.com
 - Contains many of these tools and more
 - Video clips
 - Trace files
 - 2003 Course Outlines
 - More...

Conclusion

- There are great tools out there for network administrators
 - Many of them are free
 - All of these are worth purchasing (if required)
- You need to take some time to work with these tools to get the most out of them
- Make sure you have appropriate authorization to run these tools on your network.
- Look for other “*Laura Chappell presents*” courses that cover many of these tools