

Hot Tools for TCP/IP Troubleshooting and Security (2003)

Laura Chappell
Sr. Protocol Analyst, Founder
Protocol Analysis Institute
www.packet-level.com



Novell®

N

2003 Hot Tools List



NetScanTools Pro^{\$}

Ethereal

Sam Spade

Snort + IDScenter

nMap

Ettercap

GRC's tools

Dsniff et al

Specter (Honeypot)^{\$}

White Glove/Deception Toolkit^{\$}

AirMagnet^{\$}

GPS + Antennas^{\$}

LC4 (LOphtCrack)^{\$}

LANGuard^{\$}

NetStumbler/MiniStumbler

Invisible Secrets^{\$}

HexWorkshop^{\$}

EtherPeek^{\$}

Sniffer^{\$}

Iris^{\$}

Brutus

Camera Shy

Ping Plotter^{\$}

KeyGhost Keylogger^{\$}

Spycop^{\$}



NetScanTools Pro\$

www.netscantools.com

NetScanTools Pro 2001 (TM)

Menu: DHCP, NetBios Info, Network Info and Stats, Email Validate, SMTP Email Generator/Relay Test, Arp, OS Fingerprinting, RPC Info, IP/MAC Address Management, Detection, TTCP, What's New at NWPSW, TCP Term, NetTopography, TimeSync, Finger, Launcher, Daytime, Quote, Character Generator Client, Echo, Database Tests, IDENT Server, Winsock Info, Preferences, About, Name Server Lookup, Ping, TraceRoute, Whois, NetScanner, Port Probe, SNMP, HyperTrans

Start IP: 12.234.8.1, End IP: 12.234.8.254

Ready.

NetBIOS over TCPIP: Disable Probe, MAC Address Only, MAC Address + Remote Machine Name Table

Whois: Enable Whois Queries, Enable Smart Whois

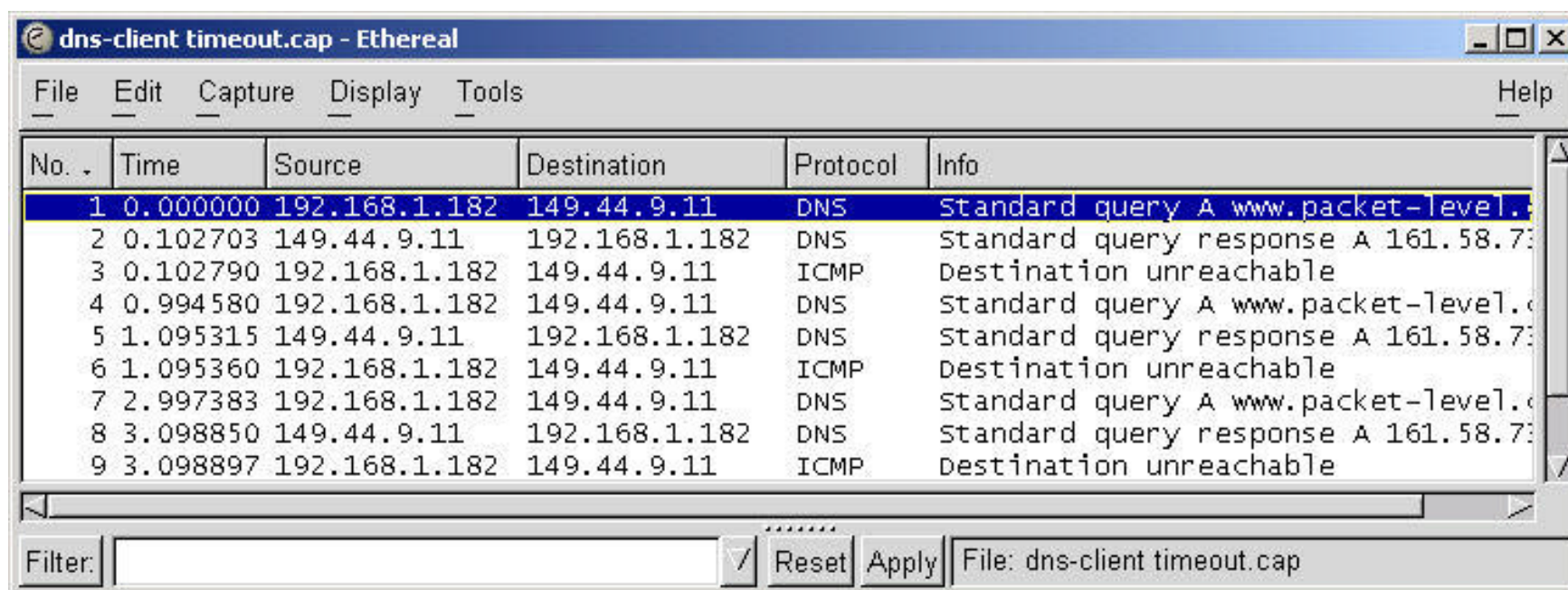
Target IP	H..	Ping	T...	NetBIOS	Whois	MAC Address
12.234.8.1	1...	0:0 Echo ...	0		-	00-01-96-3C-3...
12.234.8.2	1...	N/R	N/R		-	00-10-5A-76-1...
12.234.8.3	1...	N/R	N/R		-	00-04-5A-CF-E...
12.234.8.4	1...	N/R	N/R		-	
12.234.8.5	1...	0:0 Echo ...	41		-	00-A0-C5-E3-4...
12.234.8.6	1...	N/R	N/R		-	
12.234.8.7	1...	N/R	N/R		-	
12.234.8.8	1...	0:0 Echo ...	41		-	00-A0-CC-58-C...
12.234.8.9	1...	N/R	N/R		-	00-10-4B-30-4...
12.234.8.10	1...	N/R	N/R		-	
12.234.8.11	1...	N/R	N/R		-	
12.234.8.12	1...	N/R	N/R		-	

Buttons: Start, Stop, Setup..., Clear Results, Merge Drilldown, Autosize, Translate IPs to Hostnames, ARP/MAC/IP Info, Get Subnet Mask, Add responding IPs to HOSTS file, Edit Hosts File, Load Targets, Print, Save To File, Find, Copy, Email Results, RFCs, Navigate NST Pro, Exit, Help

Ethereal

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

www.ethereal.com



The screenshot shows the Ethereal interface with a packet capture window titled "dns-client timeout.cap". The main display area contains a table of captured packets. The table has columns for "No.", "Time", "Source", "Destination", "Protocol", and "Info". The data is as follows:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.182	149.44.9.11	DNS	standard query A www.packet-level.
2	0.102703	149.44.9.11	192.168.1.182	DNS	standard query response A 161.58.73
3	0.102790	192.168.1.182	149.44.9.11	ICMP	Destination unreachable
4	0.994580	192.168.1.182	149.44.9.11	DNS	standard query A www.packet-level.
5	1.095315	149.44.9.11	192.168.1.182	DNS	standard query response A 161.58.73
6	1.095360	192.168.1.182	149.44.9.11	ICMP	Destination unreachable
7	2.997383	192.168.1.182	149.44.9.11	DNS	standard query A www.packet-level.
8	3.098850	149.44.9.11	192.168.1.182	DNS	standard query response A 161.58.73
9	3.098897	192.168.1.182	149.44.9.11	ICMP	Destination unreachable

At the bottom of the window, there is a "Filter:" field, a "Reset" button, an "Apply" button, and a "File: dns-client timeout.cap" label.



Sam Spade

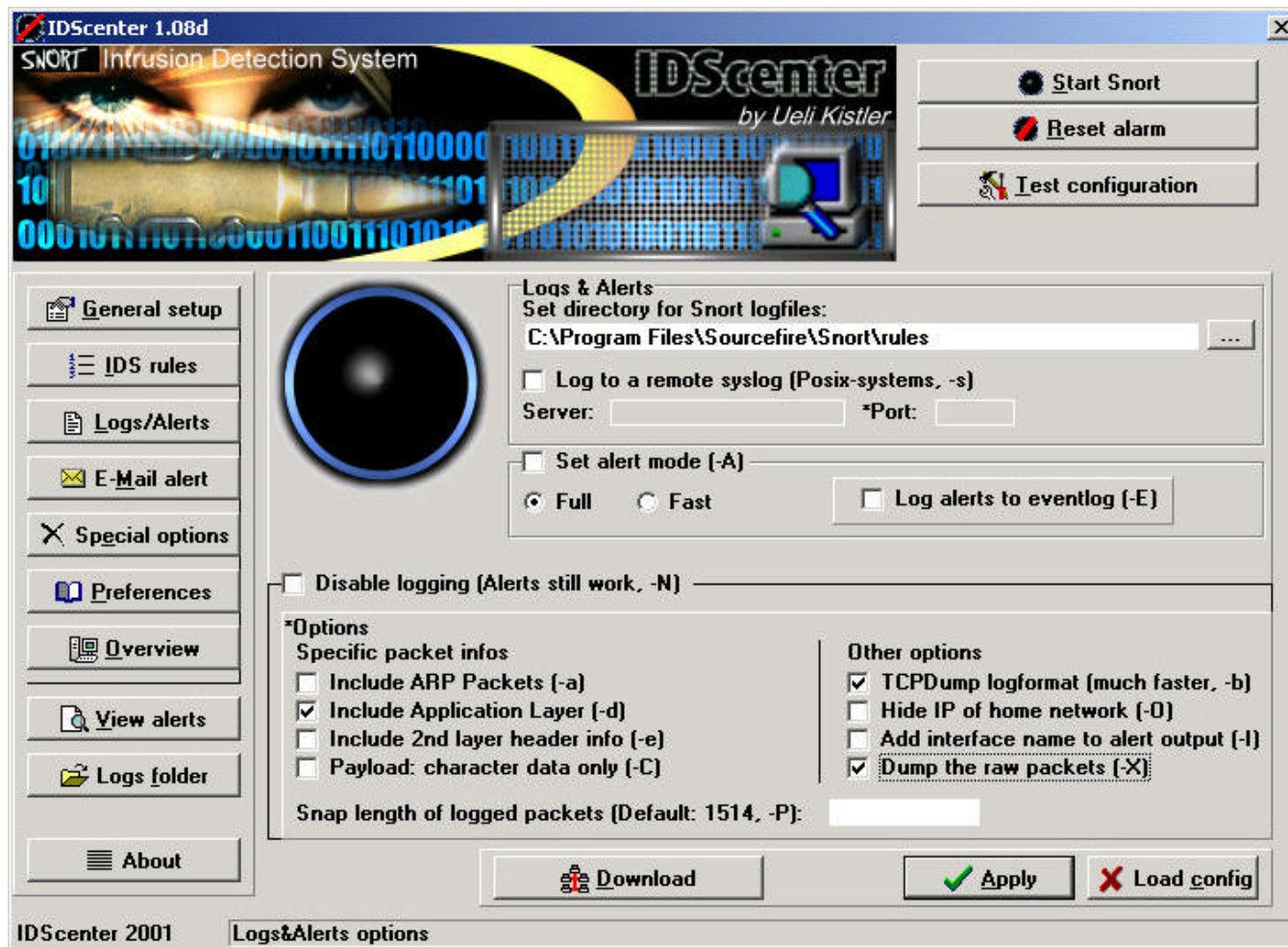
www.samspade.org

The screenshot shows the Sam Spade application interface with three overlapping windows:

- whois novell.com, finished:** Shows the command 'whois novell.com' and the result: '.com is a domain of USA & International Co'. It also shows a search for 'novell.com' with results for 'The Da' and 'inform'.
- dns novell.com, finished:** Shows the command 'dns novell.com' and the result: 'Canonical name: novell.com'.
- Fast traceroute novell.com, finished:** Shows a traceroute for 'novell.com (192.233.80.9)'. The results are as follows:

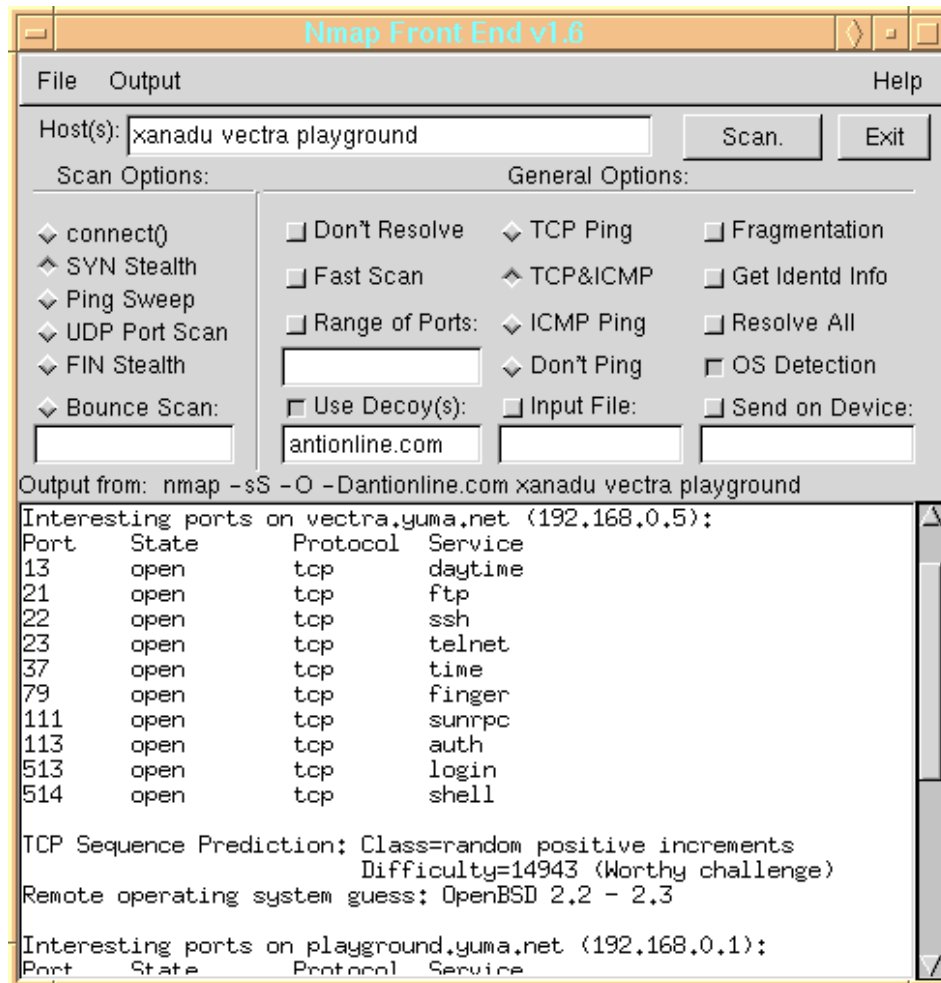
Hop	IP Address	RTT (ms)	Source RTT (ms)
1	10.4.164.97	14ms	14ms
2	12.244.98.193	68ms	0ms
3	12.244.67.17	0ms	14ms
4	12.244.72.206	14ms	41ms
5	12.123.13.62	14ms	14ms
6	12.122.5.254	14ms	28ms
7	12.122.2.245	28ms	27ms
8	12.122.2.241	42ms	41ms
9	12.127.106.34	28ms	27ms
10	192.94.118.223	55ms	55ms
11	192.233.80.9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

Snort + IDSCenter



N nMap

www.insecure.org



N

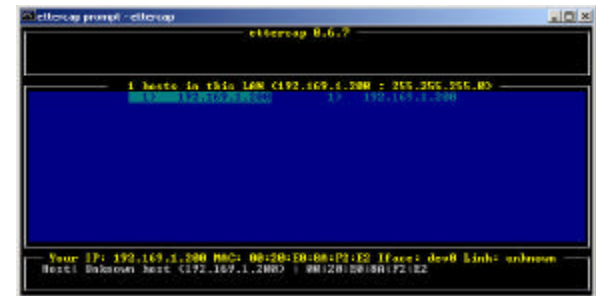
Ettercap

ettercap.sourceforge.net/download



Dangerous! Warning!

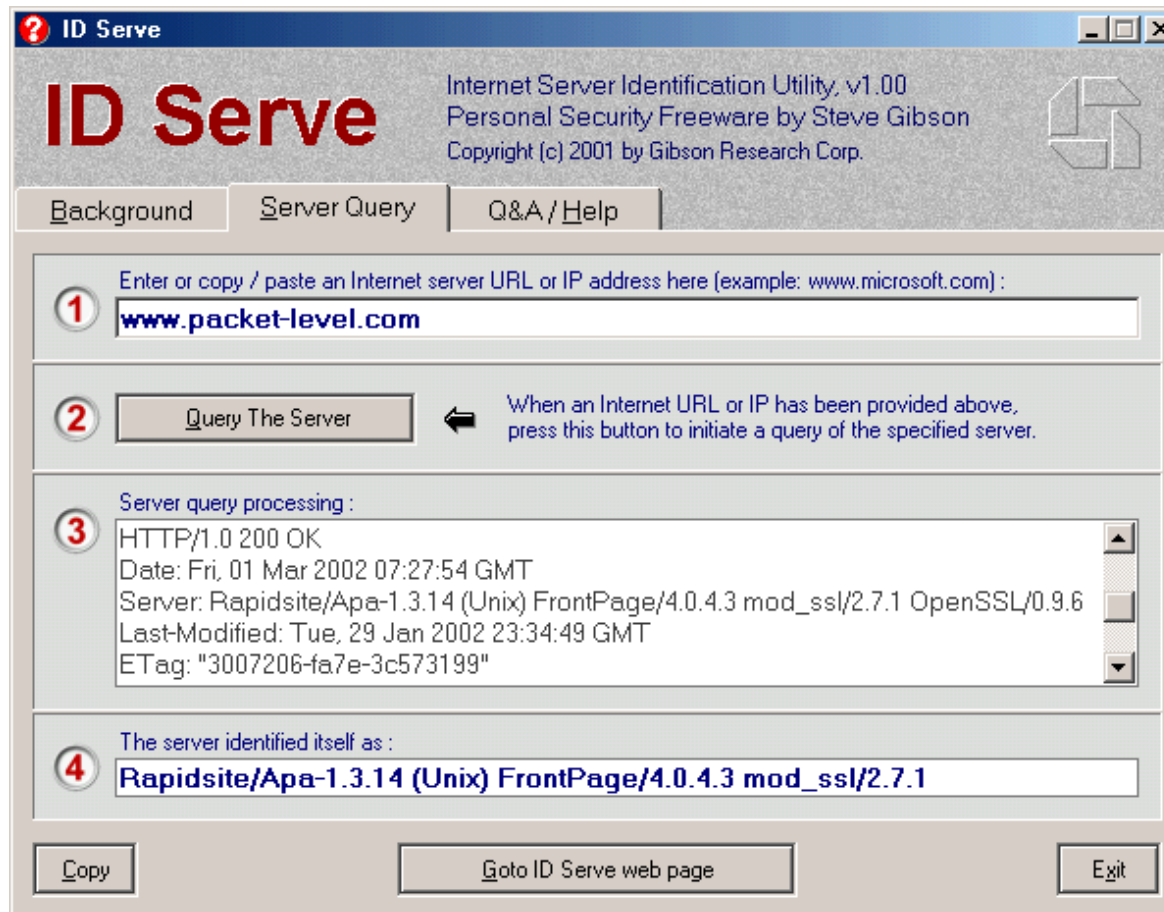
- Uses ARP Poisoning to perform M-i-M attacks
- Character injection in data stream
- Sniffs USER, PASS and data of SSH connections
- Sniffs up SSL data (HTTPS)
- Remote sniffing through GRE tunnel
- Password collector
- Passive/active OS fingerprinting
- Kills connections
- Packet factory





GRC's Tools

www.grc.com



N

Dsniff et al



Passive tools

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

www.monkey.org/~dugsong/dsniff/



Active attack tools

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



Target:
MAC
address
table



Specter Honeypot\$

The screenshot displays the Specter Control web interface. At the top, the title bar reads "Specter Control". Below the title bar, the word "SPECTER" is displayed in a stylized, purple, blocky font. To the right of the title bar, there are fields for "Engine Version" (set to 'S'), "Threads", and "Connections so far".

The main interface is divided into several sections:

- Operating System:** Radio buttons for Random, Windows 98, Windows NT, Windows 2000, Windows XP, MacOS (selected), MacOS X, Linux, Solaris, NeXTStep, Tru64, Irix, Unisys Unix, and AIX.
- Services:** Checkboxes for FTP, TELNET, SMTP, FINGER, HTTP, NETBUS, POP3, and "Provide mails".
- Traps:** Checkboxes for DNS, IMAP4, SUN-RPC, SSH, SUB-7, BO2K, and GENERIC.
- Notification:** Checkboxes for Incident DB, Alert mail, Short mail, Status mail, Event log, and Syslog.
- Intelligence:** Checkboxes for Finger, Trace Finger, Port Scan, DNS Lookup, Whois, Telnet Banner, Ftp Banner, Sntp Banner, Http Header, Http Doc, and Trace Route.
- Character:** Radio buttons for Random, Failing (selected), Secure, Open, Aggressive, and Strange.
- Password Type:** Radio buttons for Easy, Normal, Hard, Mean, Fun, Cheswick, and Warning.
- Generic Trap Name:** Text field containing "MYTRAP".
- Generic Trap Port:** Text field containing "5544".
- Priority:** Radio buttons for Emergency (selected), Alert, Critical, Error, Warning, Notice, and Informational.
- Facility:** Radio buttons for Kernel (selected), User, and Security.
- Syslog Server IP Address:** Text field containing "?".
- Send PW file:** Checkbox.
- Max. Hops:** Text field containing "60".

On the right side of the interface, there is a status panel showing the engine's current state. It displays "FTP : 192.168.1.113 on Fri Feb 21 11:53:23 2003" and a large black box with a red dashed border containing the text "www.specter.com". Below this, a list of services and their status is shown:

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

Below the status panel, there are several buttons: "Start Engine", "Reconfigure", "Load", "About", "Stop Engine", "Log Analyzer", "Save", and "License".

The bottom section of the interface contains various configuration fields and checkboxes:

- Host Name:** Text field containing "bill-the-bloodsucking-tic".
- System Name:** Text field containing "imac4me".
- Configuration Version:** Text field containing "1.0".
- Mail Server IP Address:** Text field.
- Mail Address:** Text field.
- Short Mail Address:** Text field.
- Status Mail Period [h]:** Text field containing "24".
- Remote Management:** Checkbox.
- Port:** Text field containing "28".
- Expect friendly connections:** Checkbox.
- Use custom mail message for POP3:** Checkbox.
- Use custom warning message:** Checked checkbox.
- Include settings in mails:** Checkbox.
- IP Addresses:** Text field.
- Edit Message:** Text field containing "good to see you again fred".



AirMagnet\$

The screenshot displays the AirMagnet software interface. The top window is titled "LiveCapture [My Profile]" and shows a signal level graph for 802.11b. Below it is another graph for 802.11a. A tree view on the left shows "802.11 Information" with sub-items: SSID (1), Ad-Hoc, Infrastructure, AP, and STA (1). A statistics table at the bottom left shows:

Broadcast	179	Multicast	0
Unicast	9	Total Frames	188

The main packet capture window on the right shows a list of captured packets. The first packet is highlighted with a red dashed box and contains the text "www.airmagnet.com". The interface includes a menu bar with "File", "View", "Tools", and "Help". The bottom status bar shows "Scan 64" and various tool icons: Start, Channel, Infrastructure, AirWISE, Charts, and Decodes.

N

GPS\$ + Antennas\$

pigtails



amplifiers



www.fab-corp.com



antennas



N

LC4 (L0phtCrack)\$



- Password cracking tool - excellent!

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

- Also check out John the Ripper

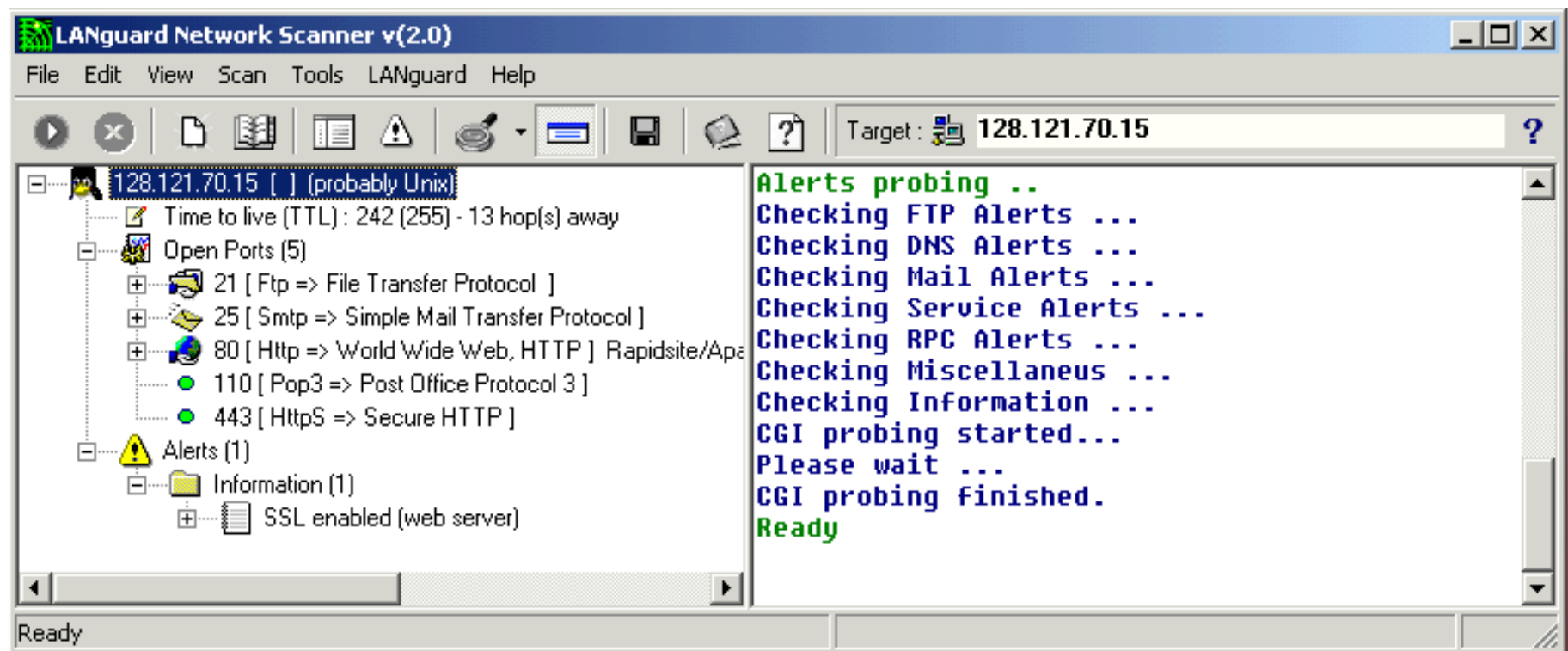
- www.openwall.com/john/

www.@stake.com



LANGuard\$

www.gfi.com



NetStumbler/MiniStumbler

www.netstumbler.com

The image displays two overlapping windows from the NetStumbler suite. The background window is 'City 2.ns1', showing a tree view of channels (1-11) and SSIDs, and a table of detected networks. The foreground window is 'MiniStumbler', showing a similar table of detected networks. The MiniStumbler window also includes a status bar at the bottom with indicators for 'Ready', 'Not scanning', 'GPS Off', and the number '94'.

MAC	SSID	Name	Ch
00022D05BD...	Network		7
00045AFA7F...	mitsui		6
00045A0E98...	linksys		6
00045A0F0D...	iannucci		6
00601D218A...	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		11

MAC	SSID
0030AB0C2D77	Harmless
004096427E53	c6228t
00022D03FF1F	Micha[REDACTED]
0090D100BFB9	WLAN
00045A0E006D	linksys
00022D2977C8	CUSD
00601D218EF5	iBook Network: pass
00E00304B094	sbwipop
00022D29FC5C	WaveLAN Network
0030AB12A38D	Wireless
0060B366CF8D	COMPAQ
003065013BAF	NetThang
00E00304B958	shwinon1

N

Invisible Secrets^{\$}

LSB Steganography

Data injection or data replacement

www.neobytesolutions.com

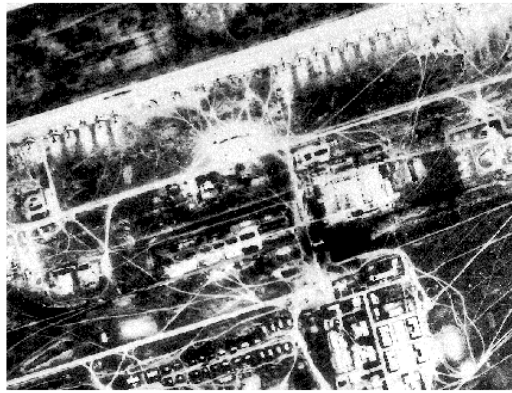


Figure 4: Long-Range Aviation Airfield⁵



Carrier

+

Secret

=

Stego Image



EtherPeek\$

The screenshot shows the EtherPeek NX application window. The main window displays a list of captured packets in a table:

Packet	Source	Source ...	Destination	Dest. Port	Flags	Size	Protoc..
1	IP-0.0.0.0	bootpc	IP Broadcast	bootps		346	UDP...
2	IP-10.0.0.1	bootps	IP-10.0.99.2	bootpc		308	UDP...

Below the table, the details for Packet 2 are shown:

- Flags: 0x00
- Status: 0x00
- Packet Length: 308
- Timestamp: 14:15:37.716675 11/18/1999
- Ethernet Header
 - Destination: 00:A0:CC:30:C8:DB
 - Source: 00:10:4B:30:C4:4A

The raw packet data is displayed in hexadecimal and ASCII format:

```
0000: 00 A0 CC 30 C8 DB 00 10 4B 30 C4 4A 08 00 45 0
0016: 01 22 3D DB 00 00 80 11 84 ED 0A 00 00 01 0A 0
0032: 63 02 00 43 00 44 01 0E 96 36 02 01 06 00 DE 0
0048: DE 03 00 00 00 00 00 00 00 00 0A 00 63 02 00 0
0064: 00 00 00 00 00 00 00 A0 CC 30 C8 DB 00 00 00 0
0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0096: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
```

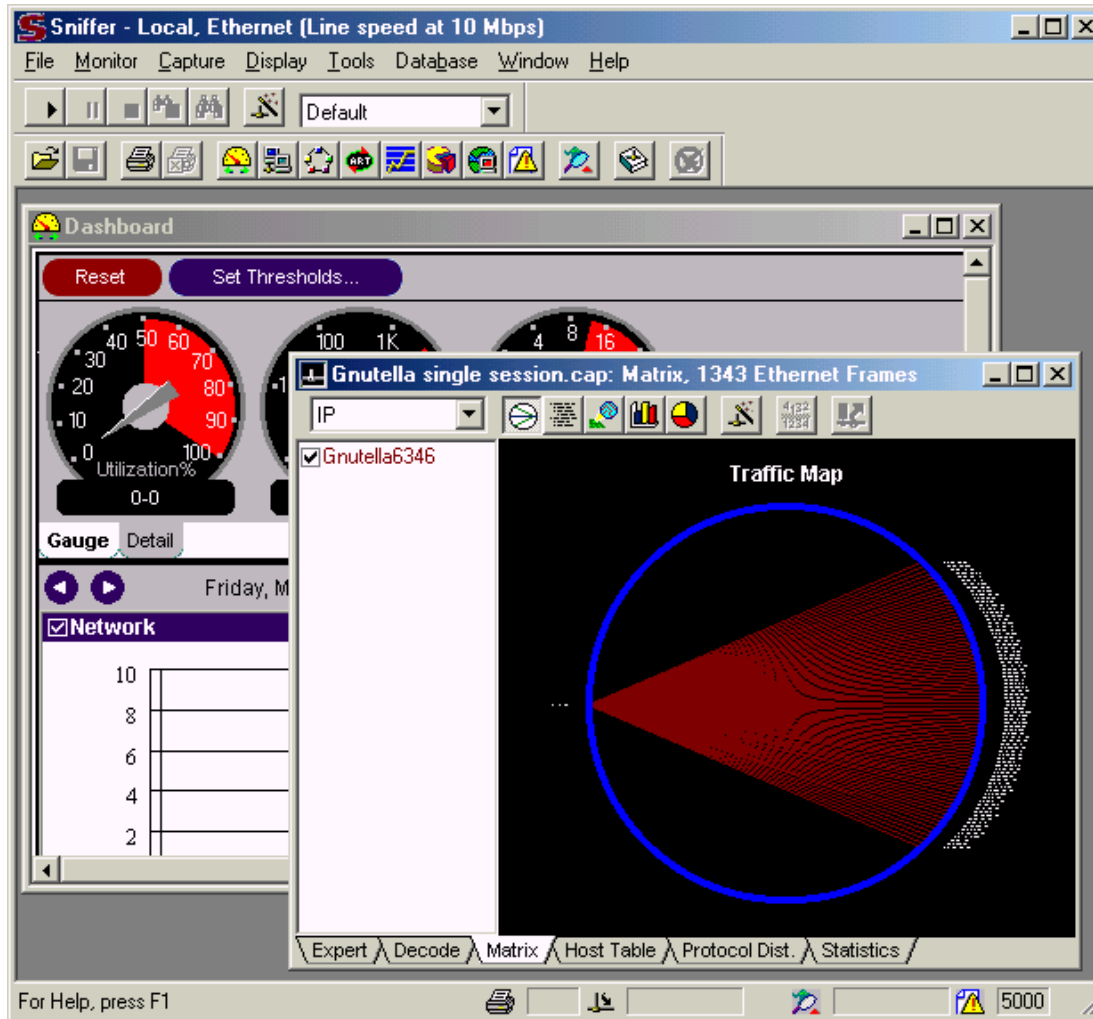
An inset window titled "Size Statistics" shows a "Packet Size Distribution" pie chart. The chart is dominated by a large green slice representing sizes less than or equal to 64 bytes, which accounts for 97.56% of the total. A much smaller blue slice represents sizes between 65 and 127 bytes, accounting for 2.44%. The legend on the right lists size ranges: <= 64 (green), 65-127 (blue), 128-255 (red), 256-511 (magenta), 512-1023 (yellow), 1024-1517 (cyan), and >= 1518 (pink).

A red dashed box on the right side of the screenshot contains the URL www.wildpackets.com.

N

Sniffer\$

www.sniffer.com



N

Iris\$

www.eeye.com

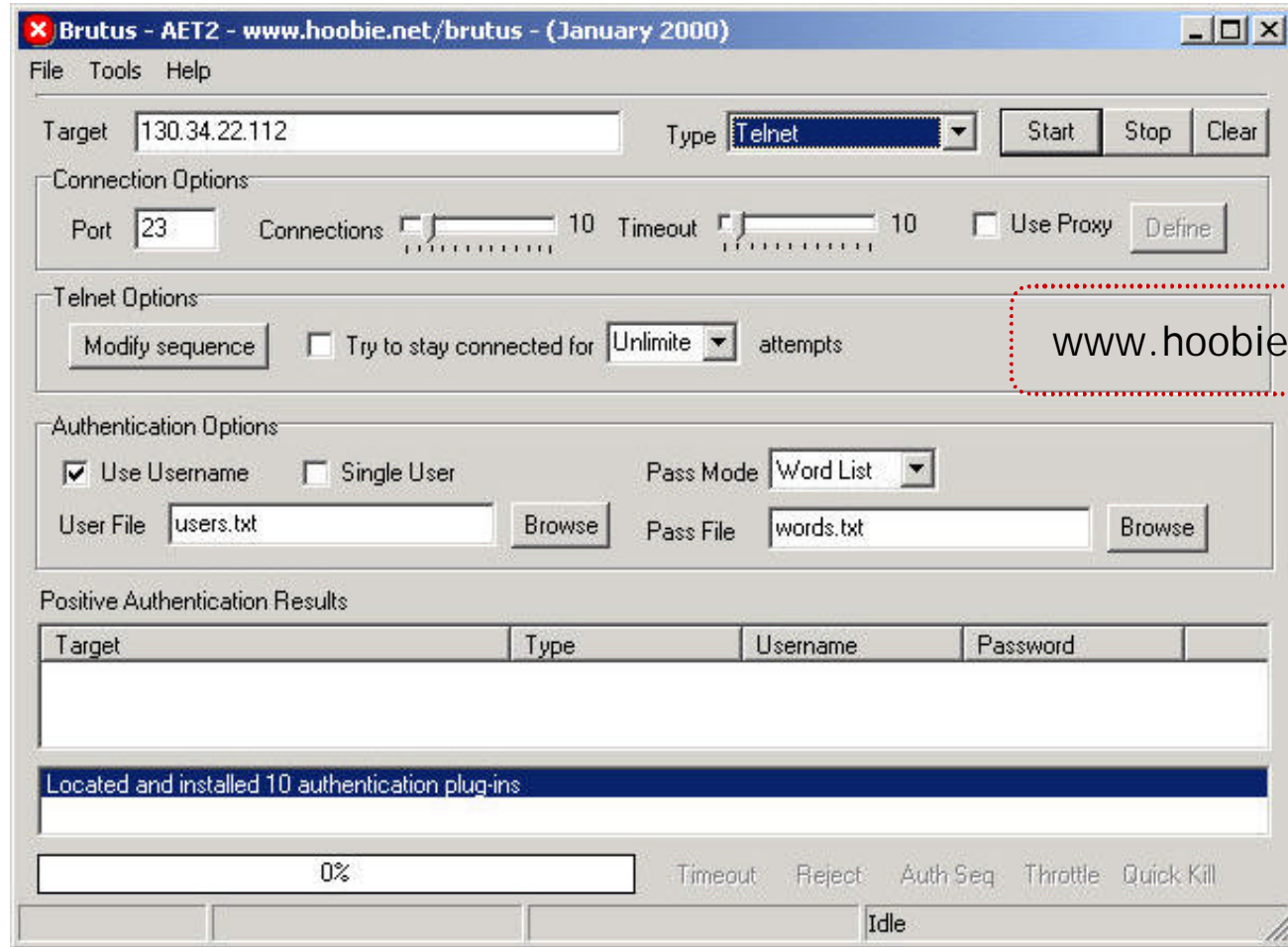
No.	MAC source addr	MAC dest. addr	Frame	Protocol
113	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
114	SONY-0d53e9	IBM-cfa677	IP	TCP-> NETBIOS-SSN
115	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
116	SONY-0d53e9	IBM-cfa677	IP	TCP-> NETBIOS-SSN
117	IBM-cfa677	SONY-0d53e9	IP	TCP-> NETBIOS-SSN
118	SONY-0d53e9	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 .(ei@
0020 01 07 09 7F 00 8B F0 45 64 BD 2A F9 6A F0 50 11 ..D..
0030 3F F9 F6 C3 00 00 00 00 00 00 00 00 00 00 00 ?ùöÄ.
```





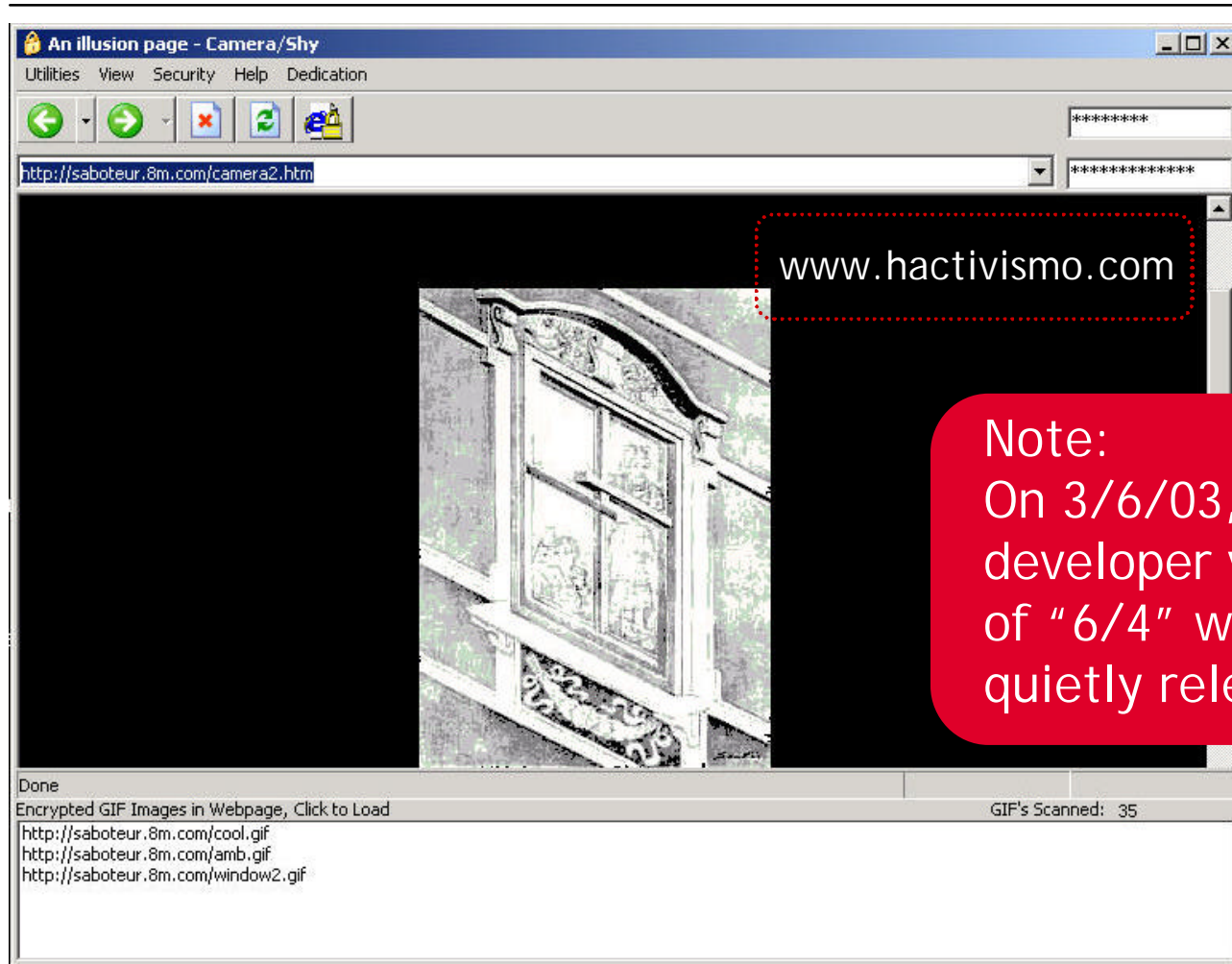
Brutus



www.hoobie.net/brutus

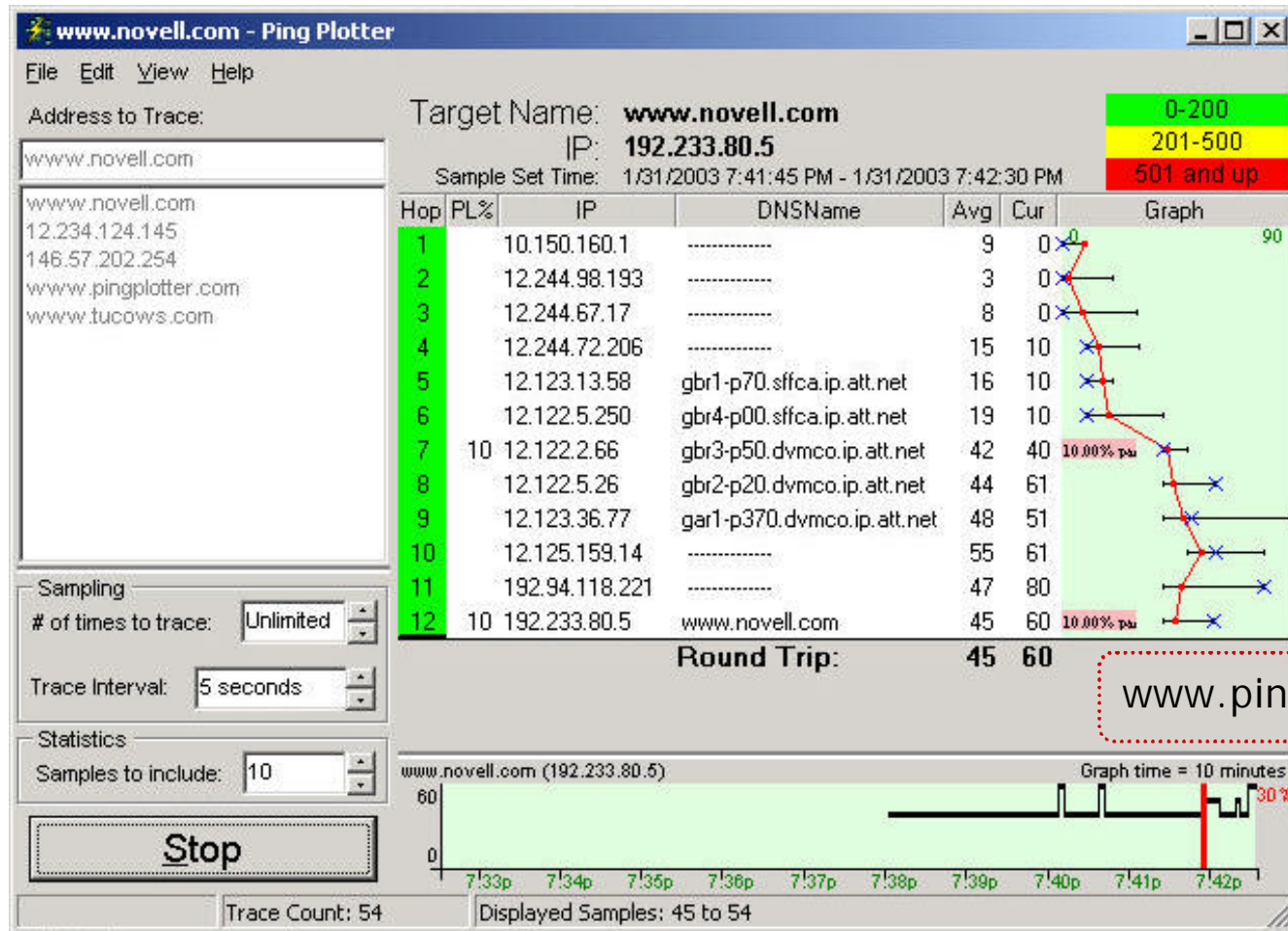
N

Camera Shy





Ping Plotter\$



N

KeyGhost Keylogger\$

Test out at the Packet-Level booth.

Password: **keyghost**

Instructions at booth

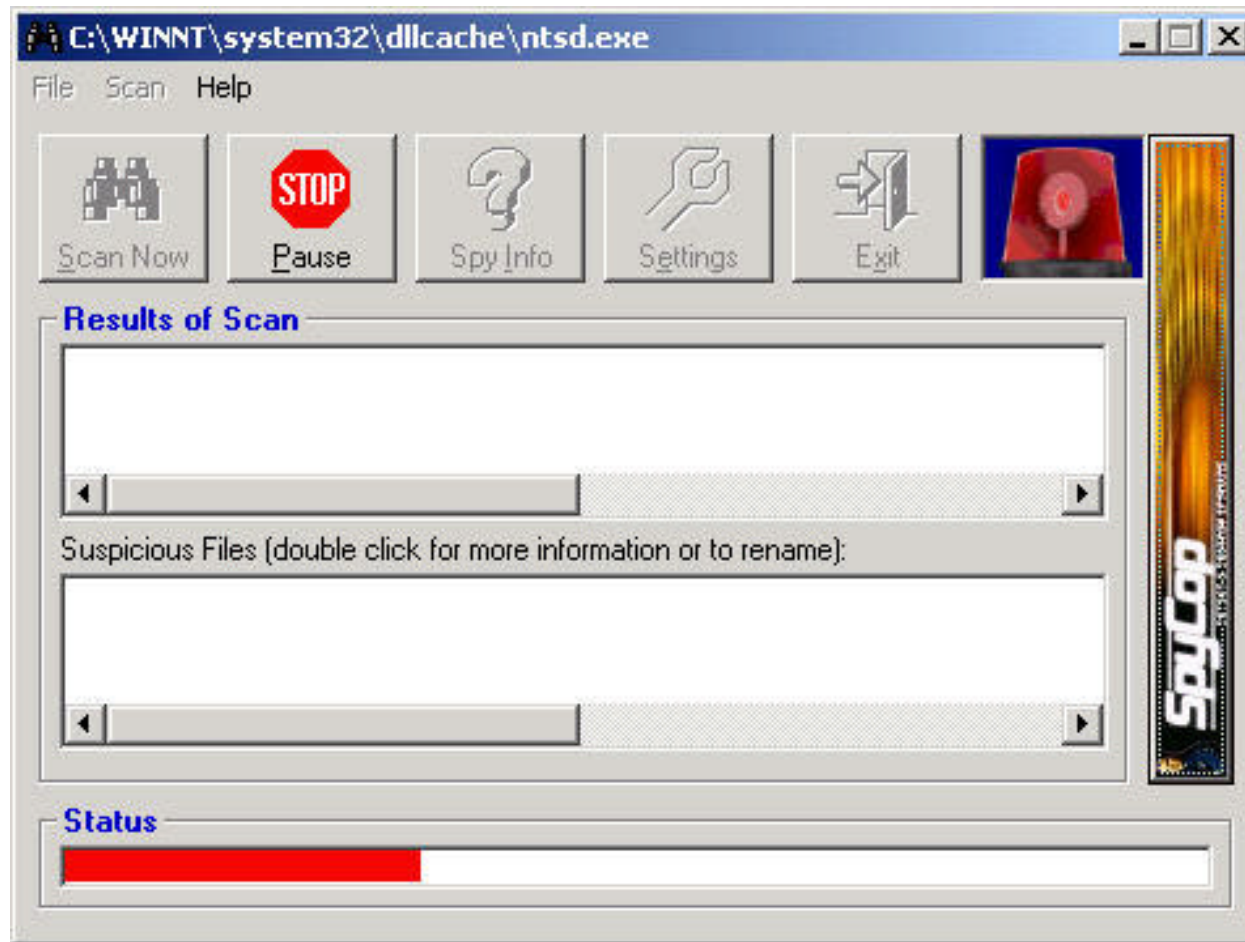


www.keyghost.com



N

Spycop\$



www.spycop.com

N

Laura's Lab Kit v4.0

Contains many of these tools and more

Video clips



Trace files

2003 Course Outlines

More...

Join the analysis/cybercrime roadshow in 2003!

**Check out the online courses at
www.packet-level.com**

Novell.®