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

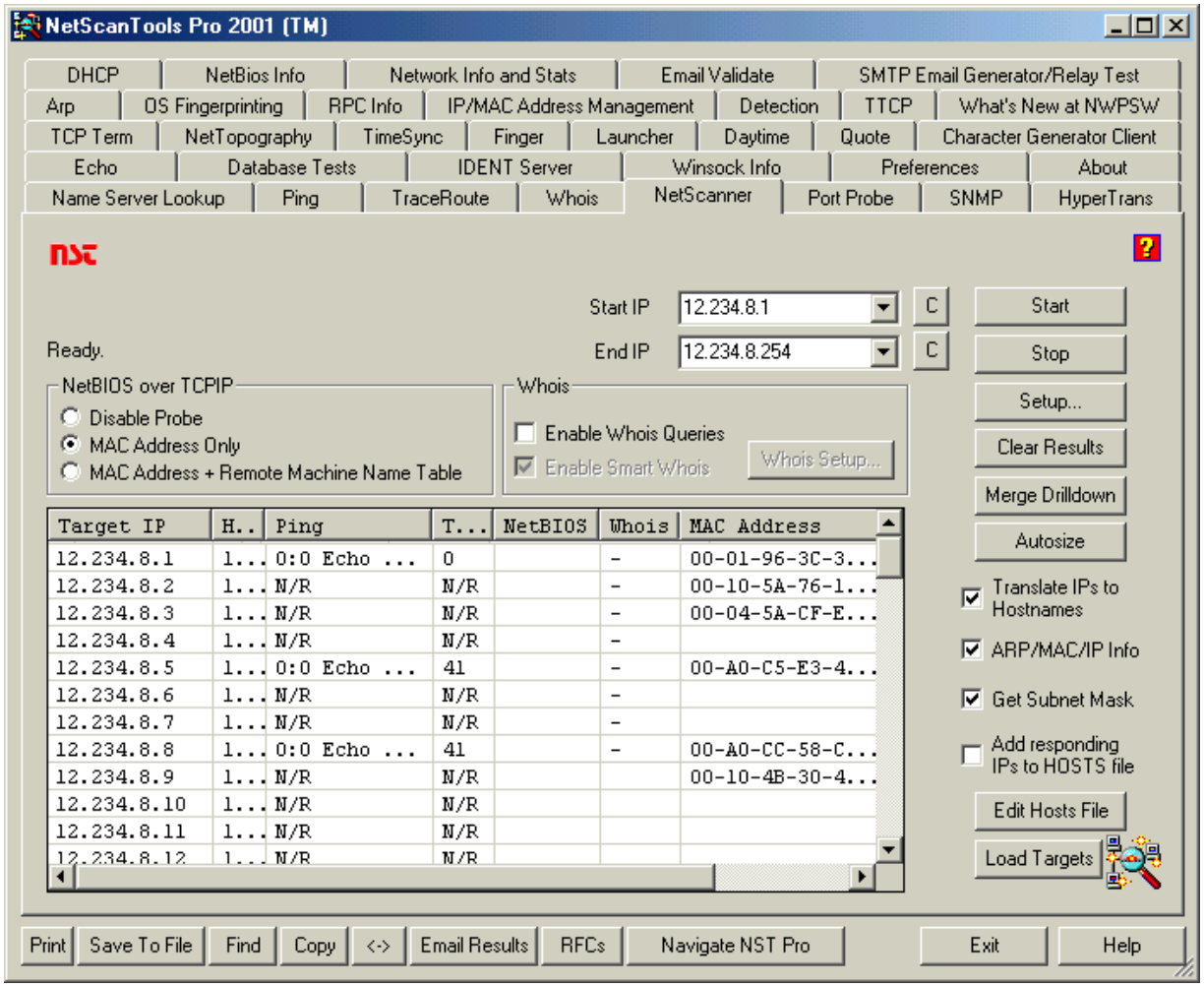
Laura Chappell
Sr. Protocol Analyst, Founder
Protocol Analysis Institute
www.packet-level.com

Novell

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 (L0phtCrack)$
LANGuard$
NetStumbler/MiniStumbler
Invisible Secrets$
HexWorkshop$
EtherPeek$
Sniffer$
Iris$
Brutus
Camera Shy
Ping Plotter$
KeyGhost Keylogger$
Spycop$

NetScanTools Pro$



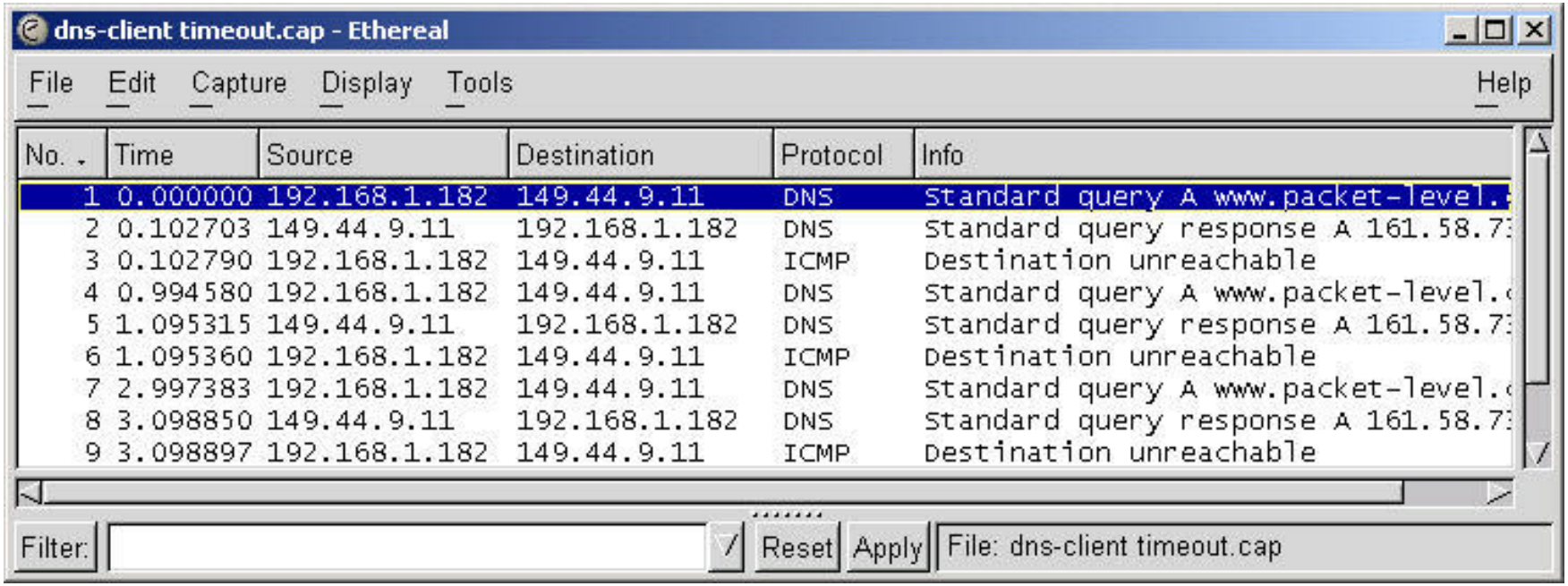
www.netscantools.com

Novell

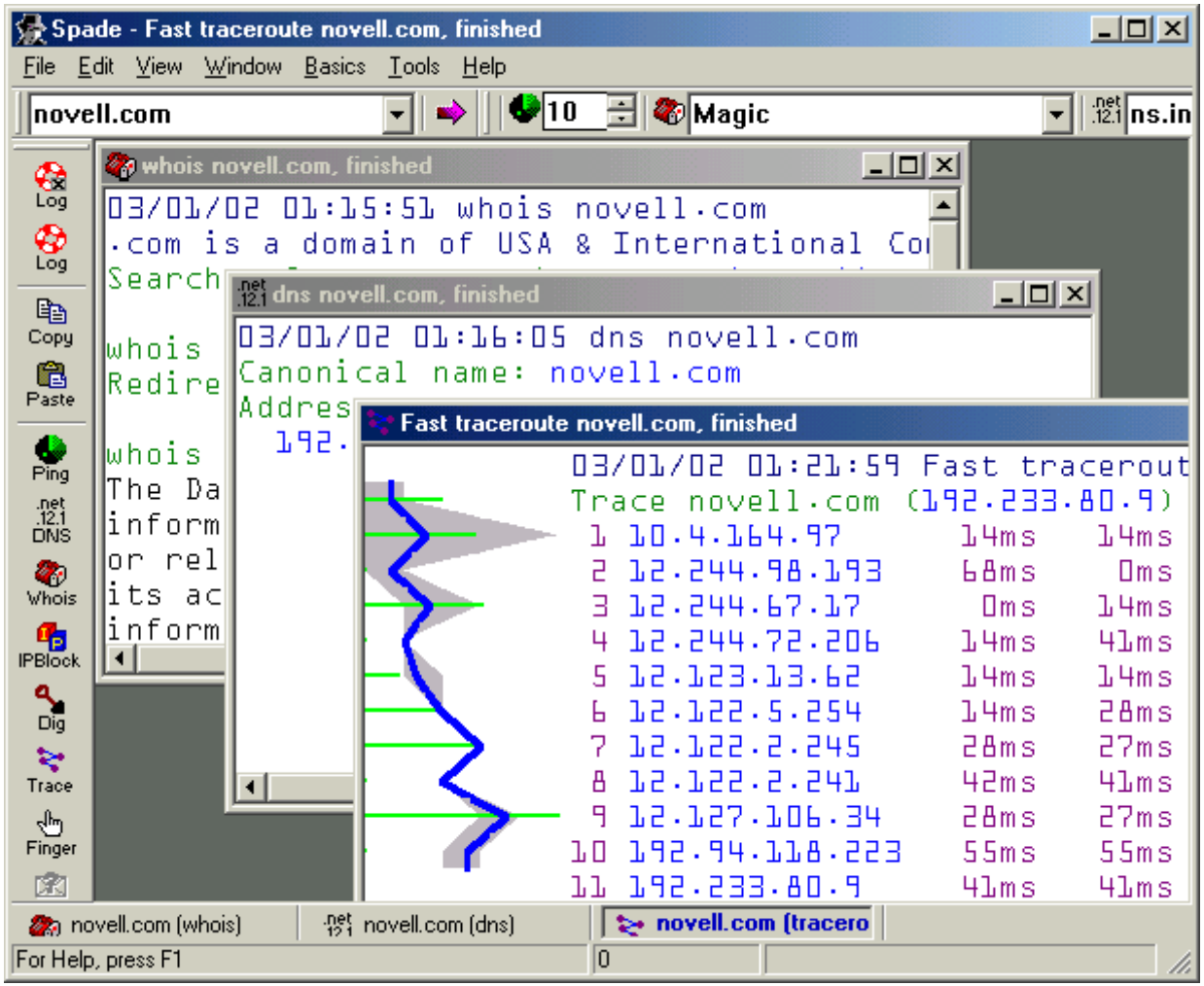
Ethereal

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

www.ethereal.com



Sam Spade



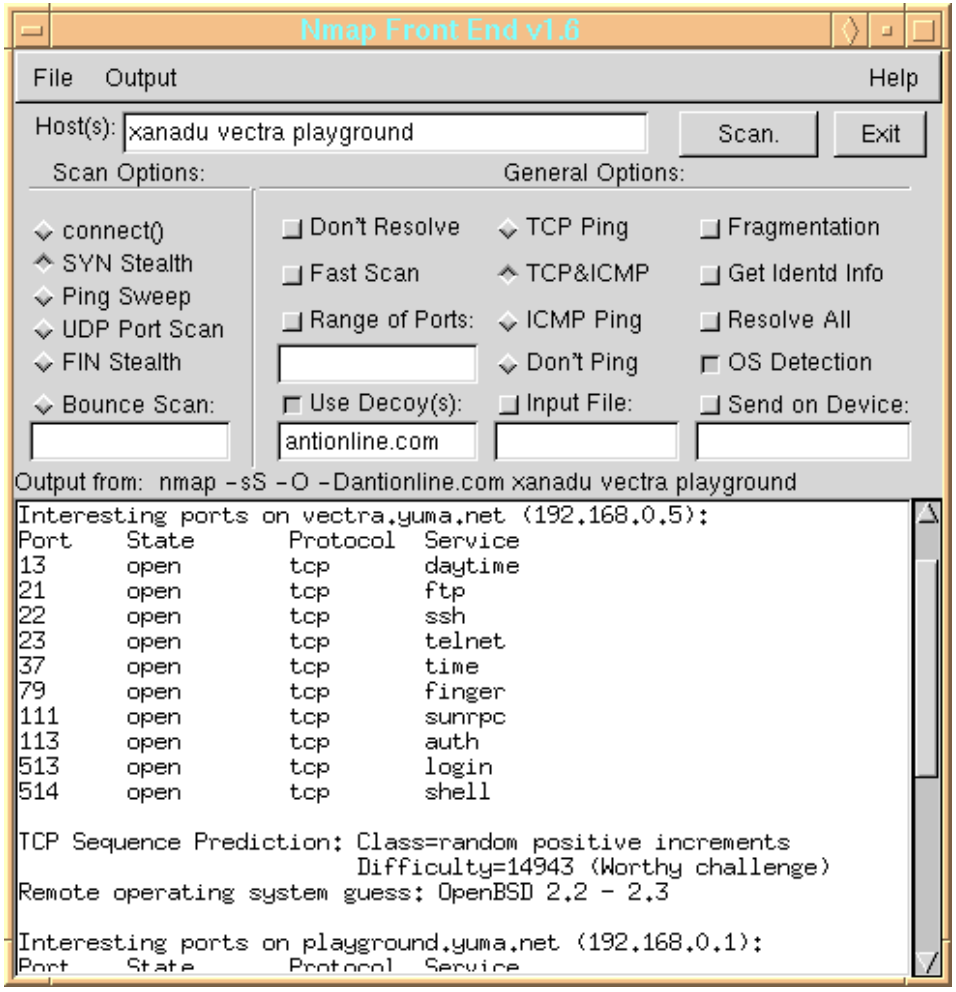
www.samspade.org

Novell

Snort + IDSCenter

www.snort.org

nMap



www.insecure.org

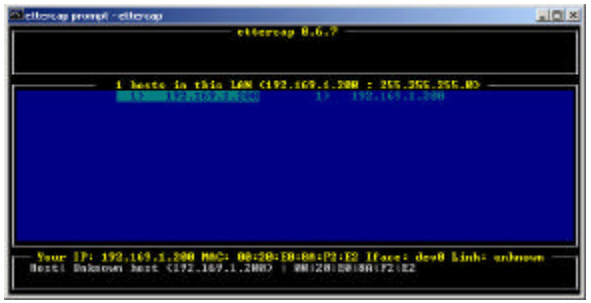
Novell

Ettercap

ettercap.sourceforge.net/download

Dangerous! Warning!

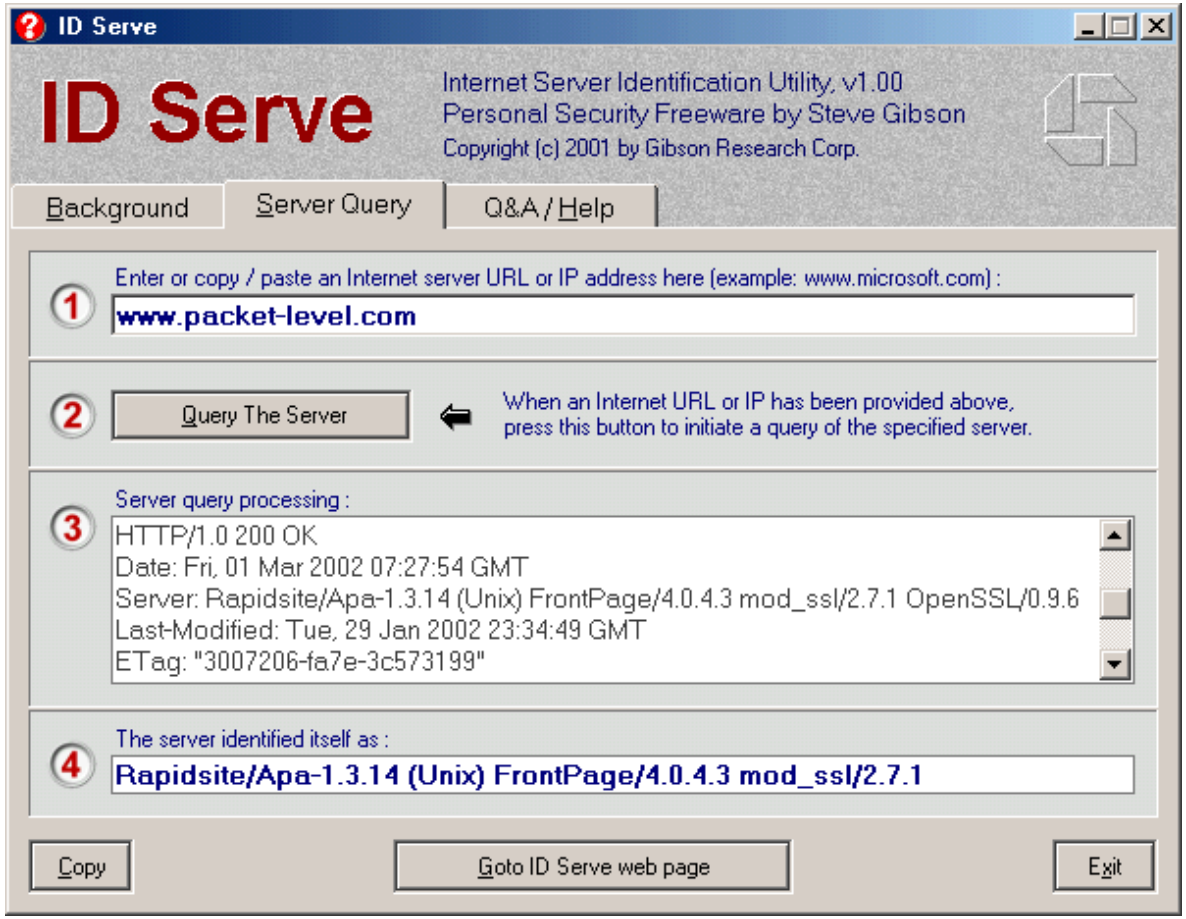
- Uses ARP Poisoning to perform M-i-M attacks
- Character injection in data stream
- Sniffs USER, PASS and data of SSH connections
- Sniffs up SSL data (HTTPS)
- Remote sniffing through GRE tunnel
- Password collector
- Passive/active OS fingerprinting
- Kills connections
- Packet factory



Novell

GRC's Tools

www.grc.com



Novell

Dsniff et al

www.monkey.org/~dugsong/dsniff/

Passive tools

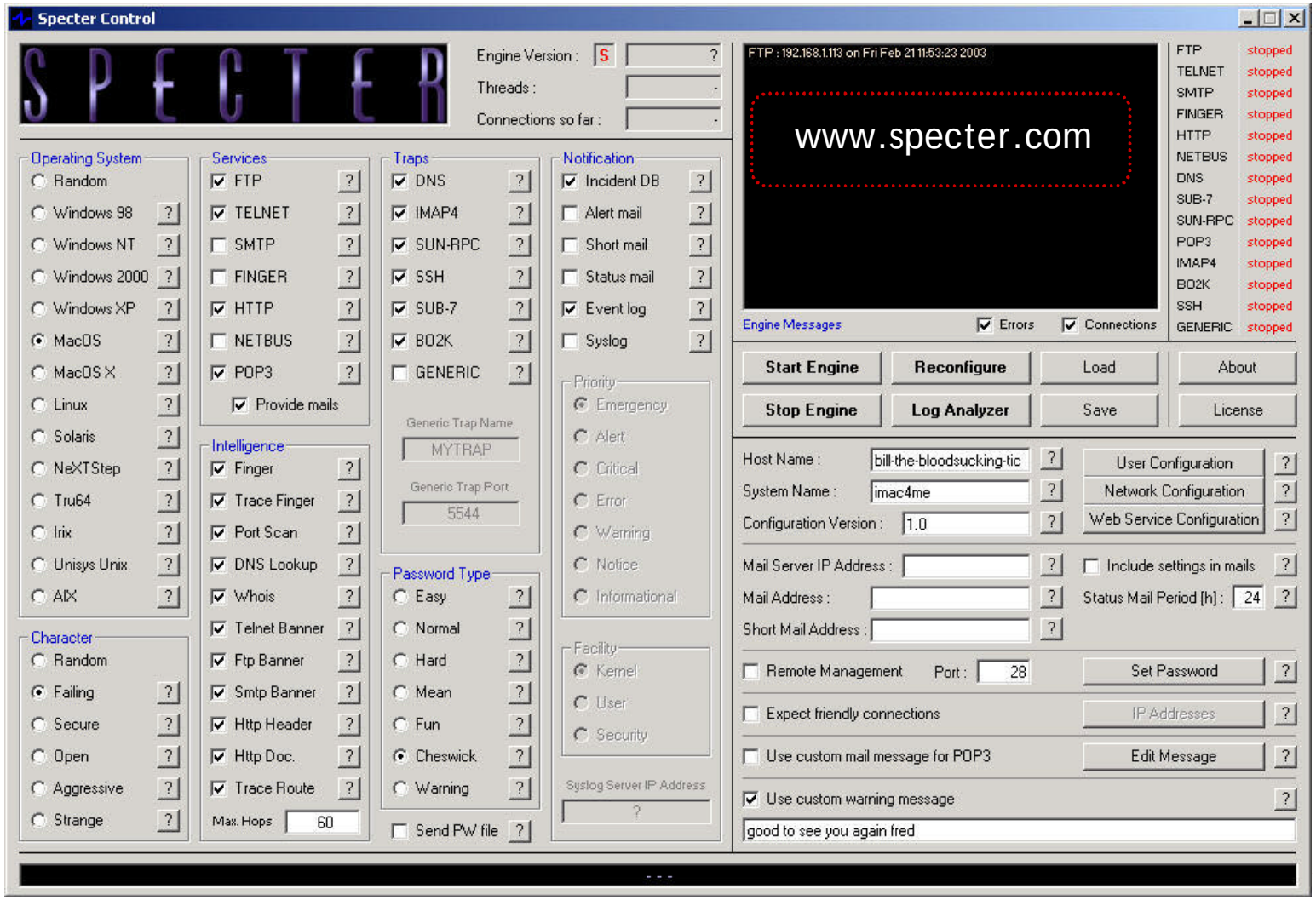
- Dsniff
- Filesnarf
- Mailsnarf
- Msgsnarf
- Urlsnarf
- Webspy

Target: MAC address table

Active attack tools

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

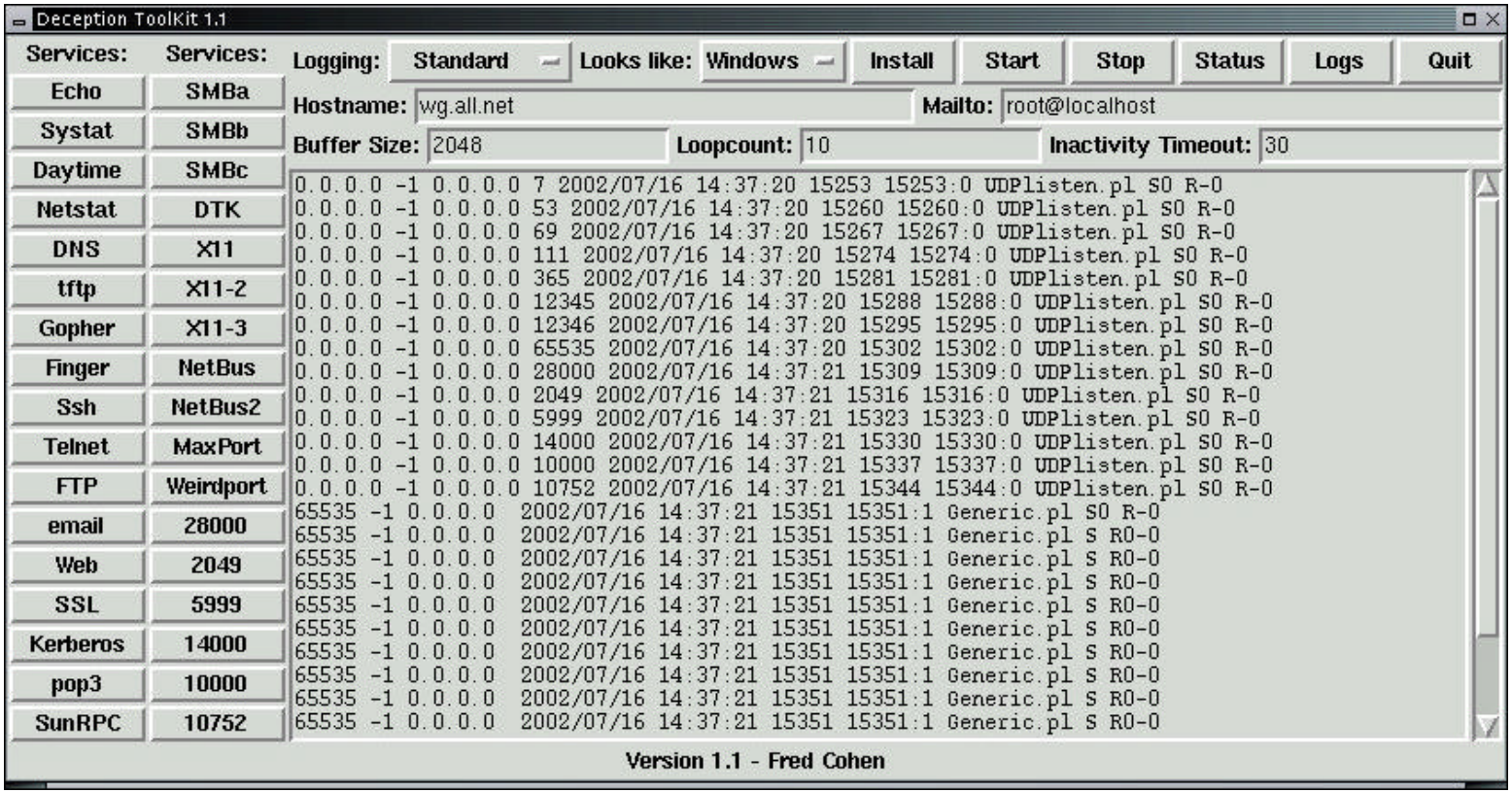
Specter Honeypot$



White Glove$/Deception Toolkit

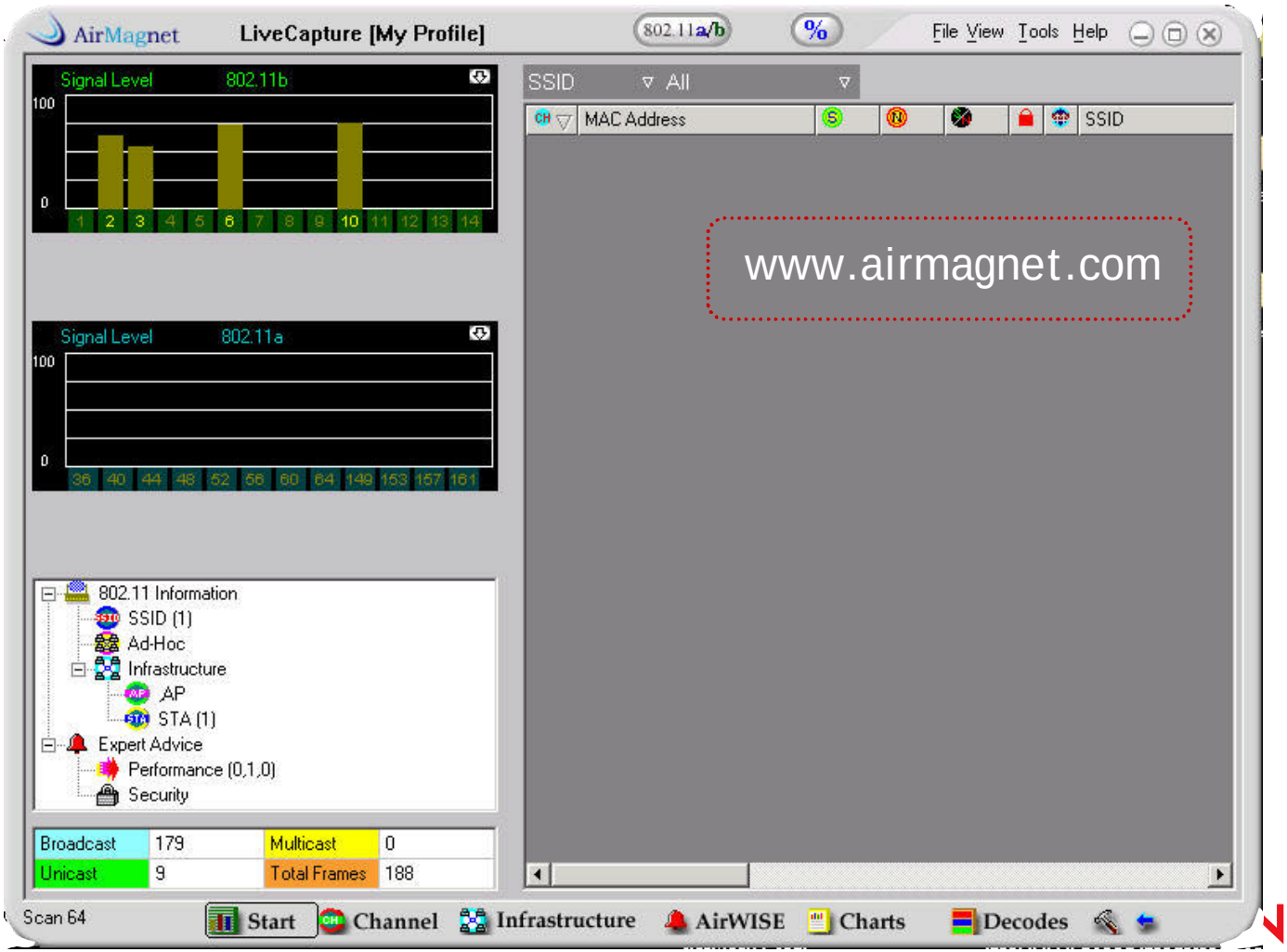
Deception Toolkit (DTK) on White Glove

www.all.net



Novell

AirMagnet$



Novell

GPS$ + Antennas$

pigtails

amplifiers

www.fab-corp.com

antennas

Novell

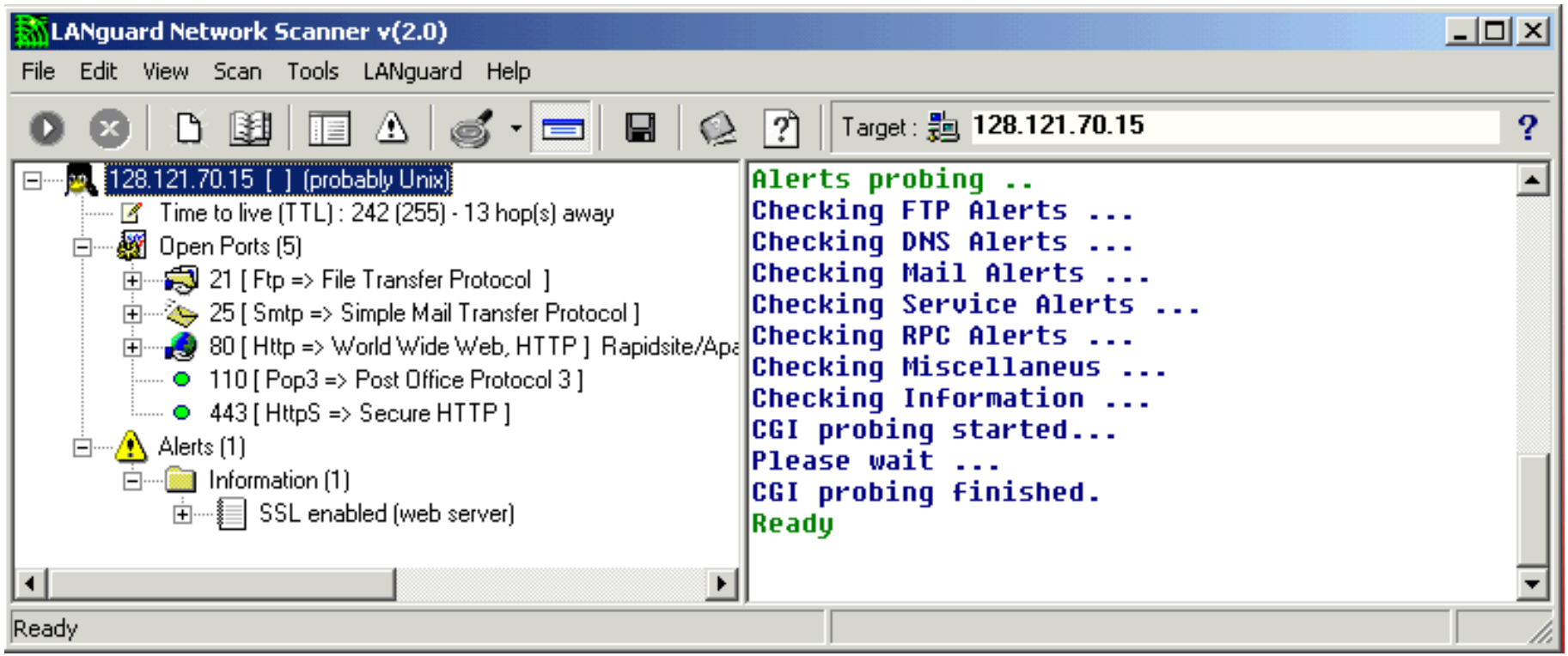
LC4 (L0phtCrack)$

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/

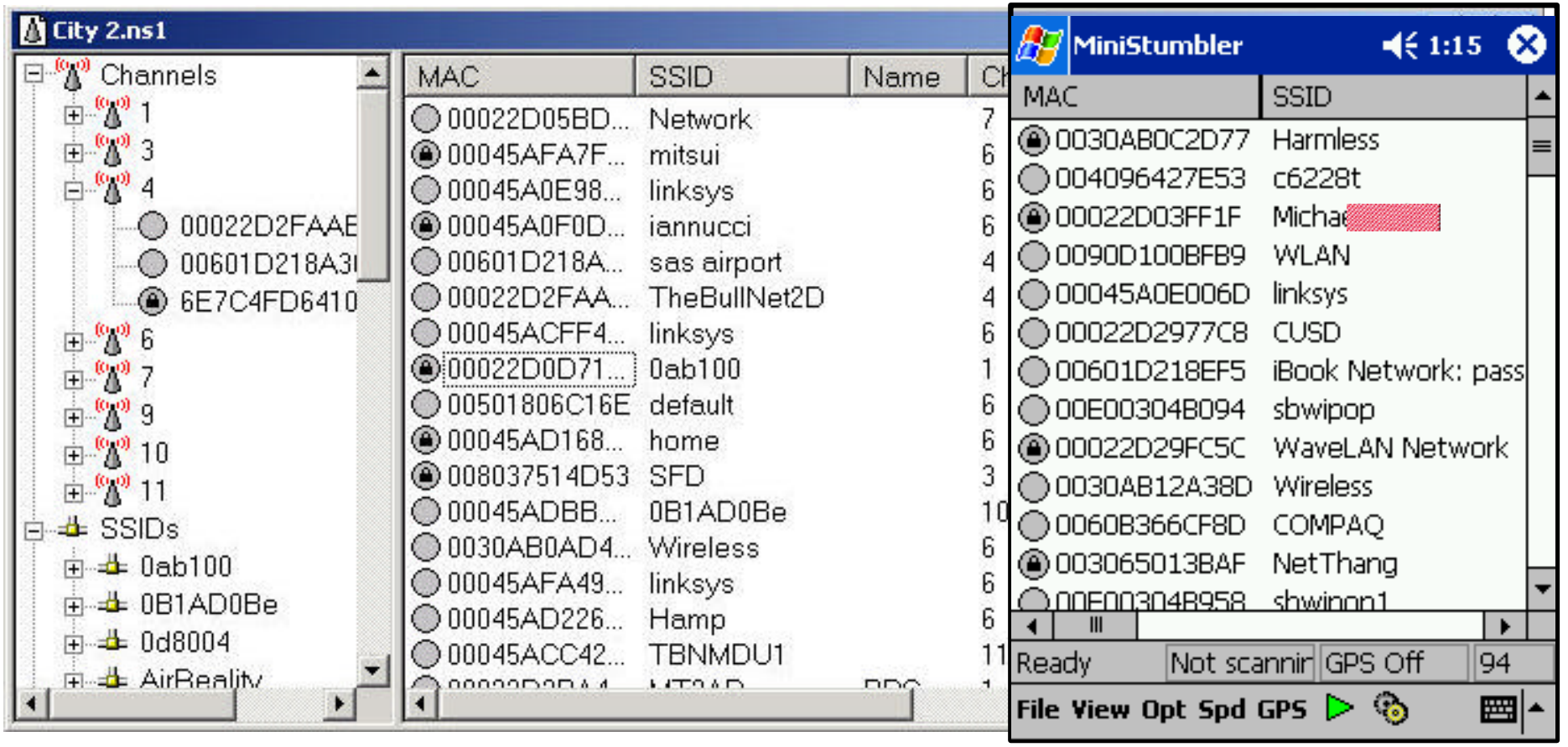
LANGuard$

www.gfi.com



NetStumbler / MiniStumbler

www.netstumbler.com



Invisible Secrets$

www.neobytesolutions.com

LSB Steganography

Data injection or data replacement

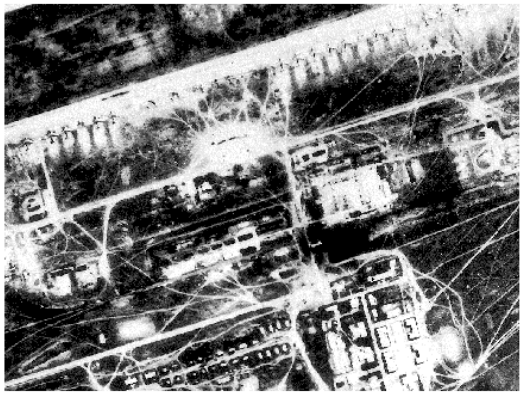
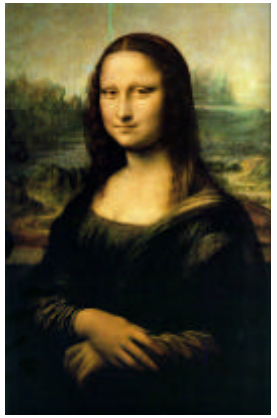


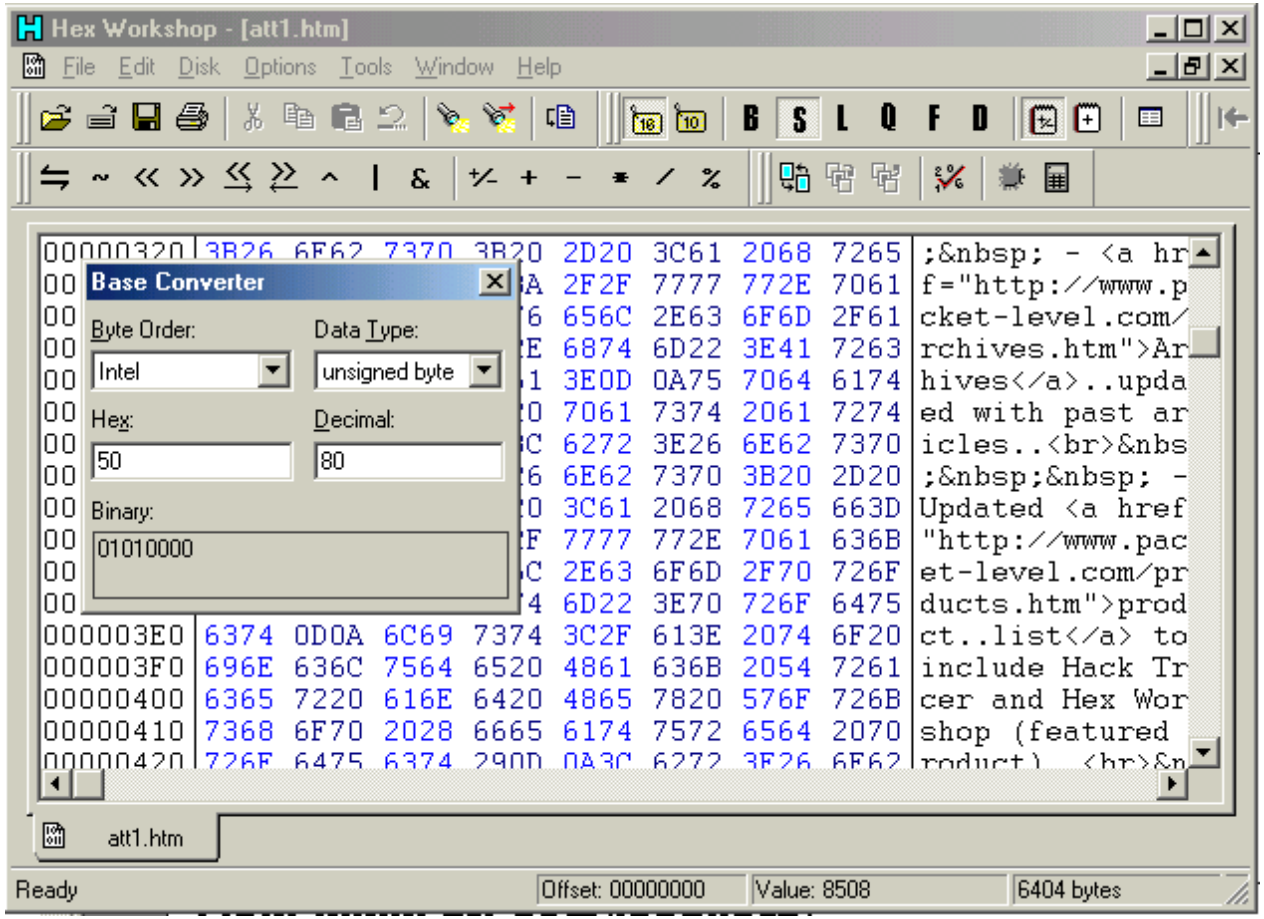
Figure 4: Long-Range Aviation Airfield[5]



Carrier + Secret = Stego Image

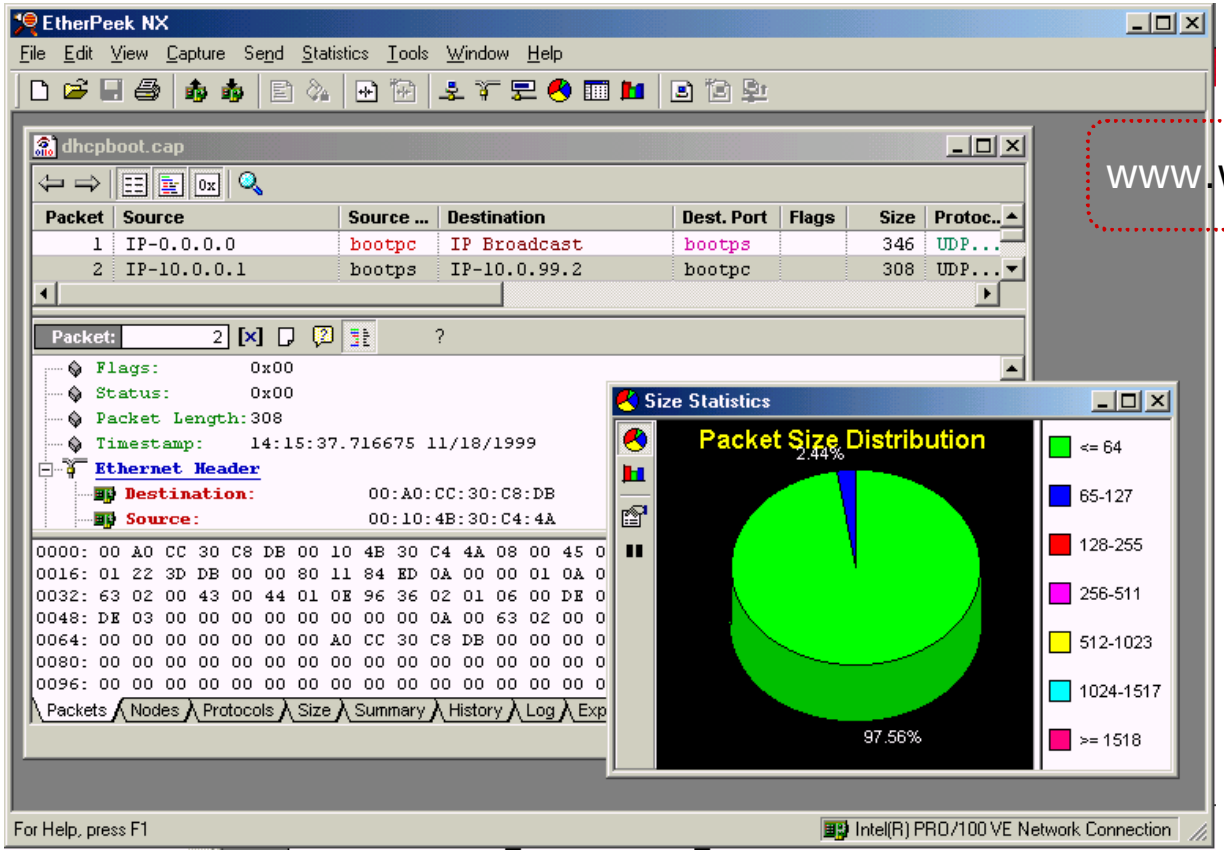
HexWorkshop$

www.bpsoft.com



Novell

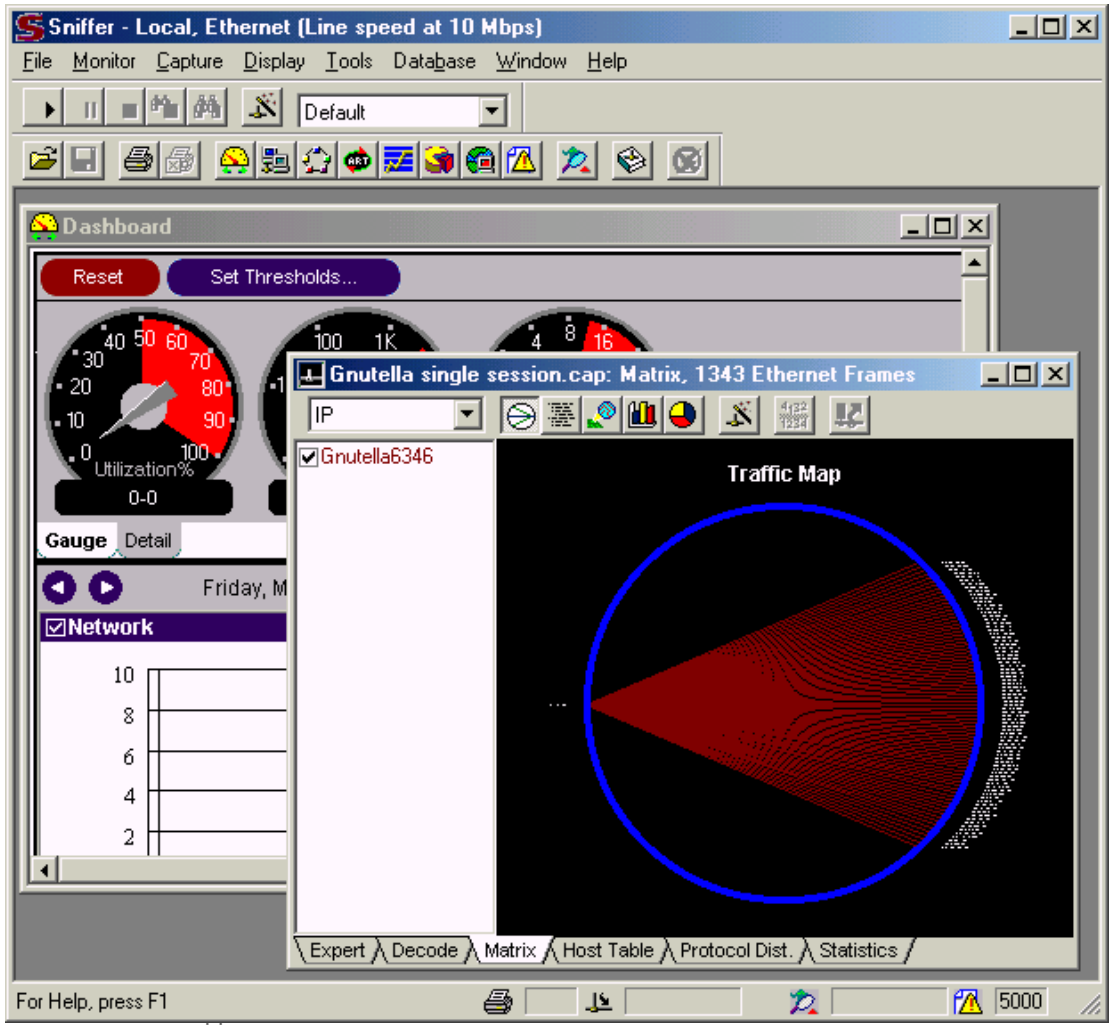
EtherPeek$



www.wildpackets.com

Novell

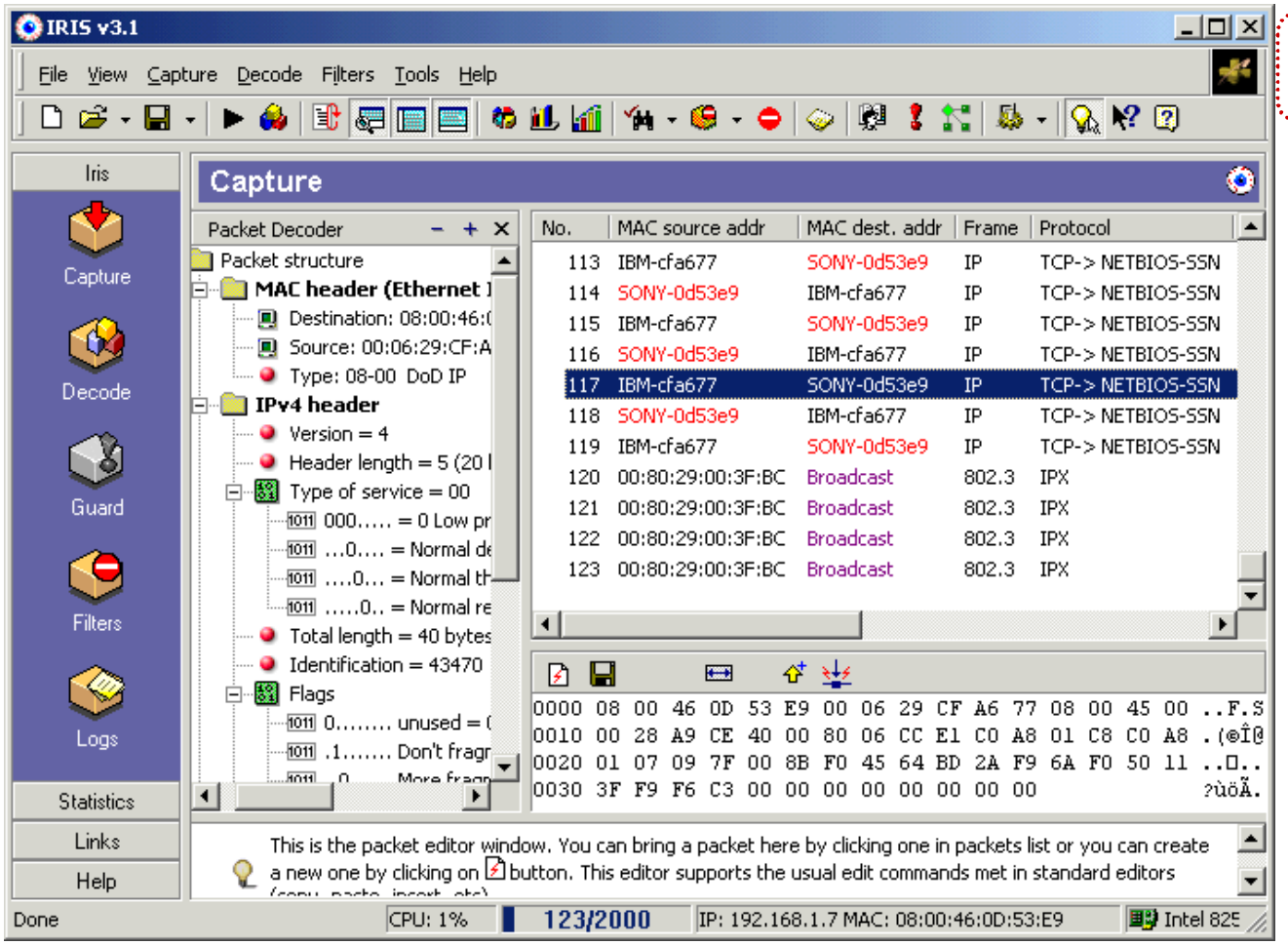
Sniffer$



www.sniffer.com

Novell

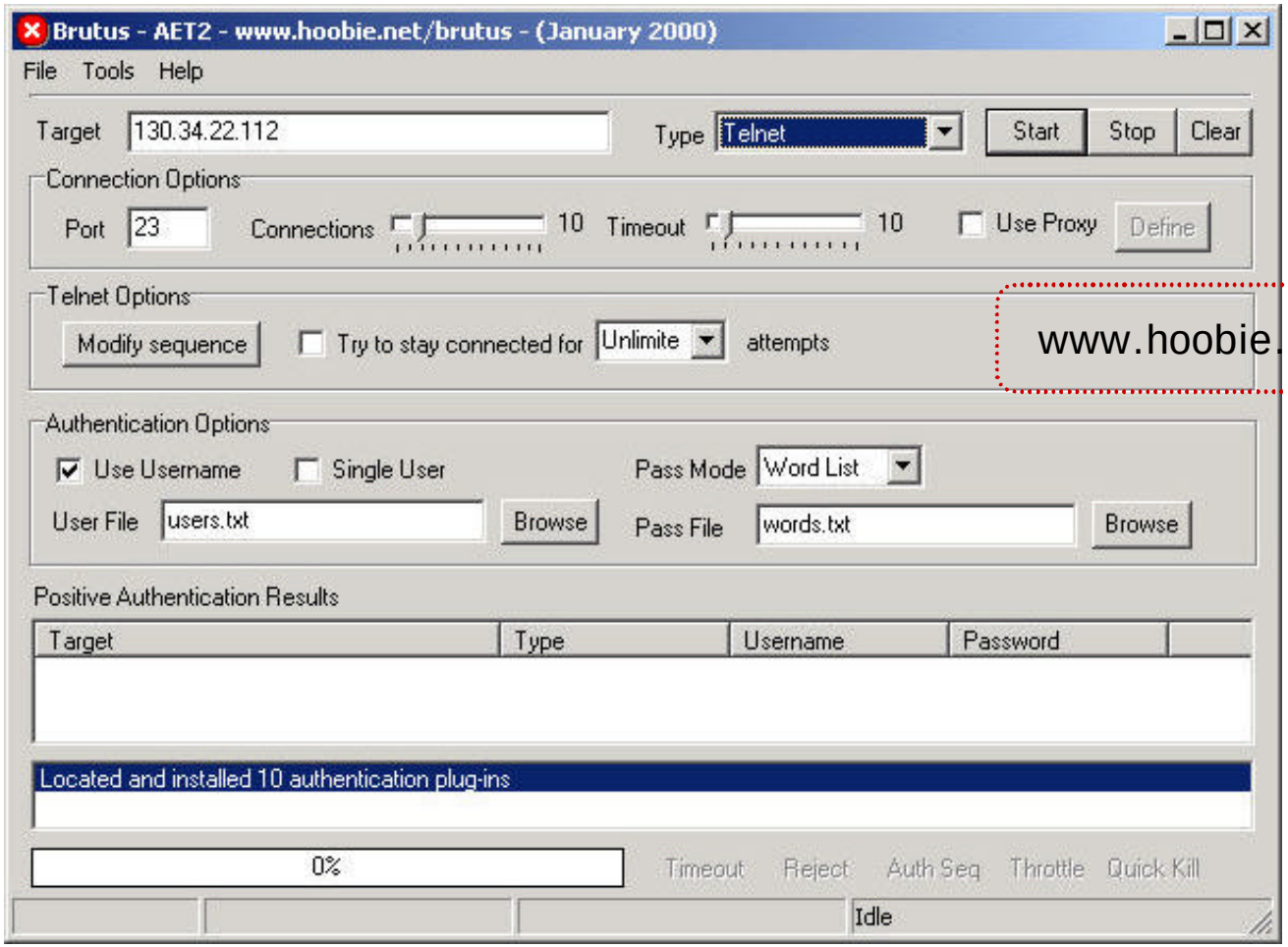
Iris$



www.eeye.com

Novell

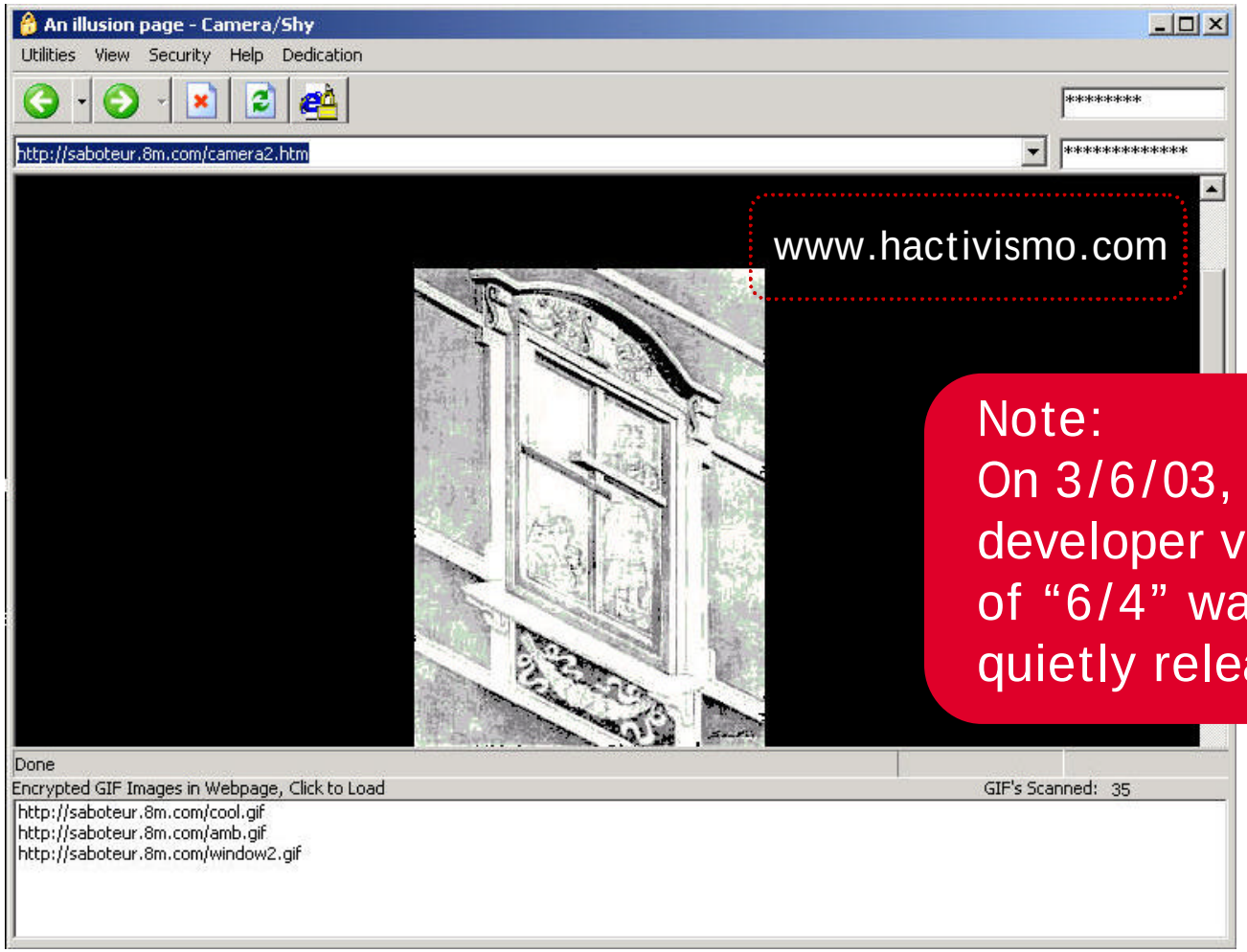
Brutus



www.hoobie.net/brutus

Novell

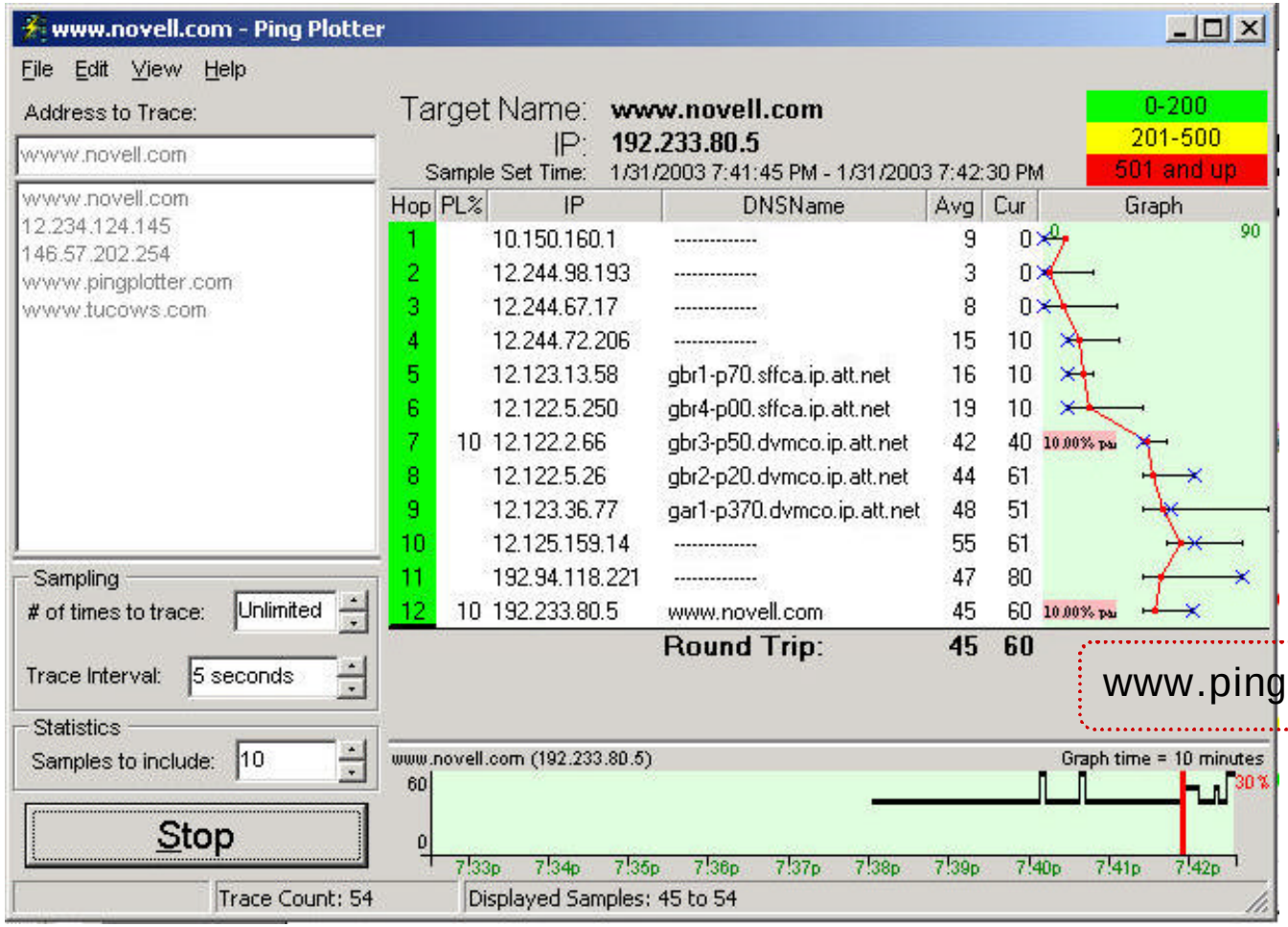
Camera Shy



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

Novell

Ping Plotter$



www.pingplotter.com

Novell

KeyGhost Keylogger$

Test out at the Packet-Level booth.

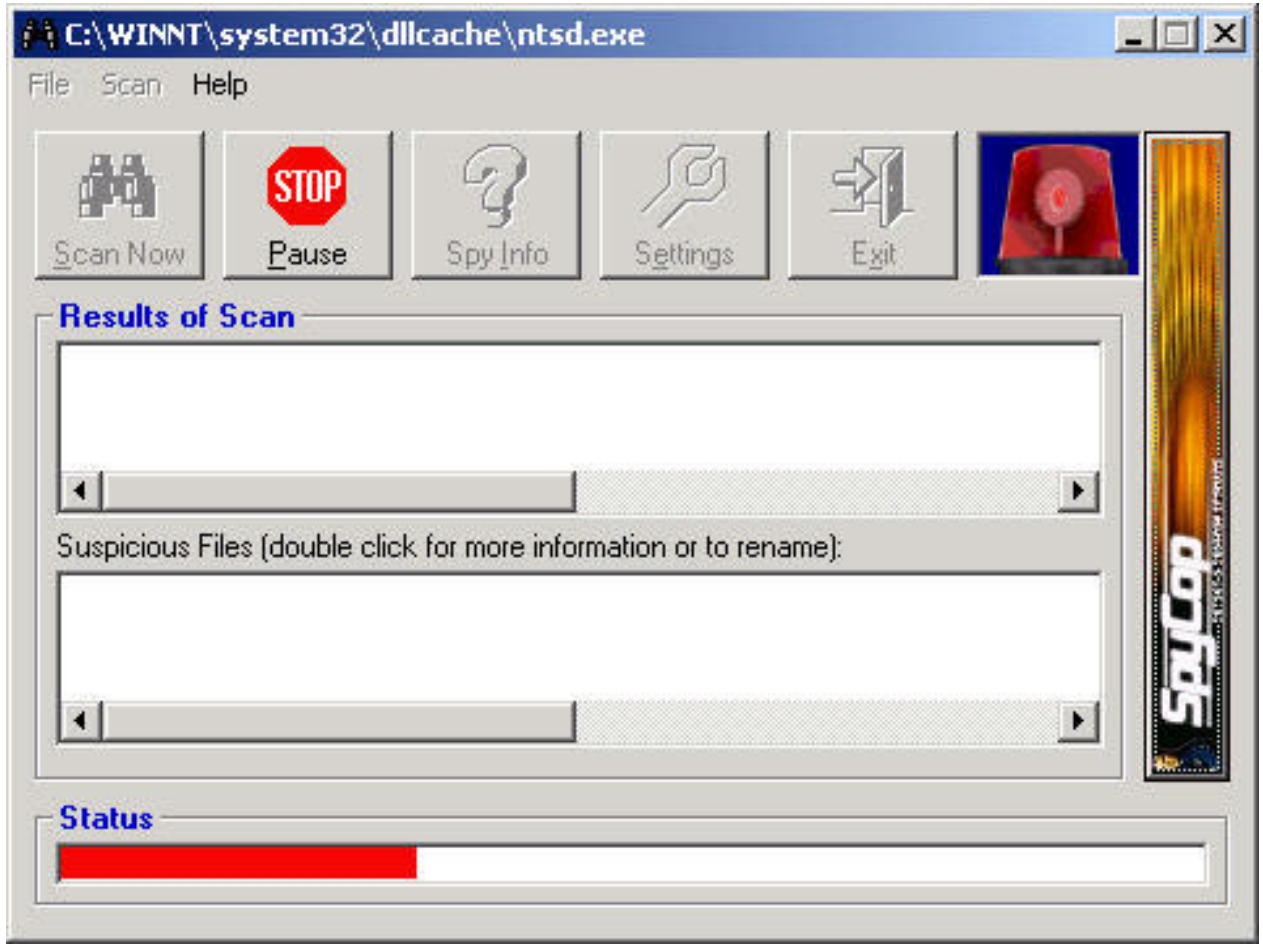
www.keyghost.com

Password: keyghost

Instructions at booth

Novell

Spycop$



www.spycop.com

Novell

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®