Laura Chappell presents…™

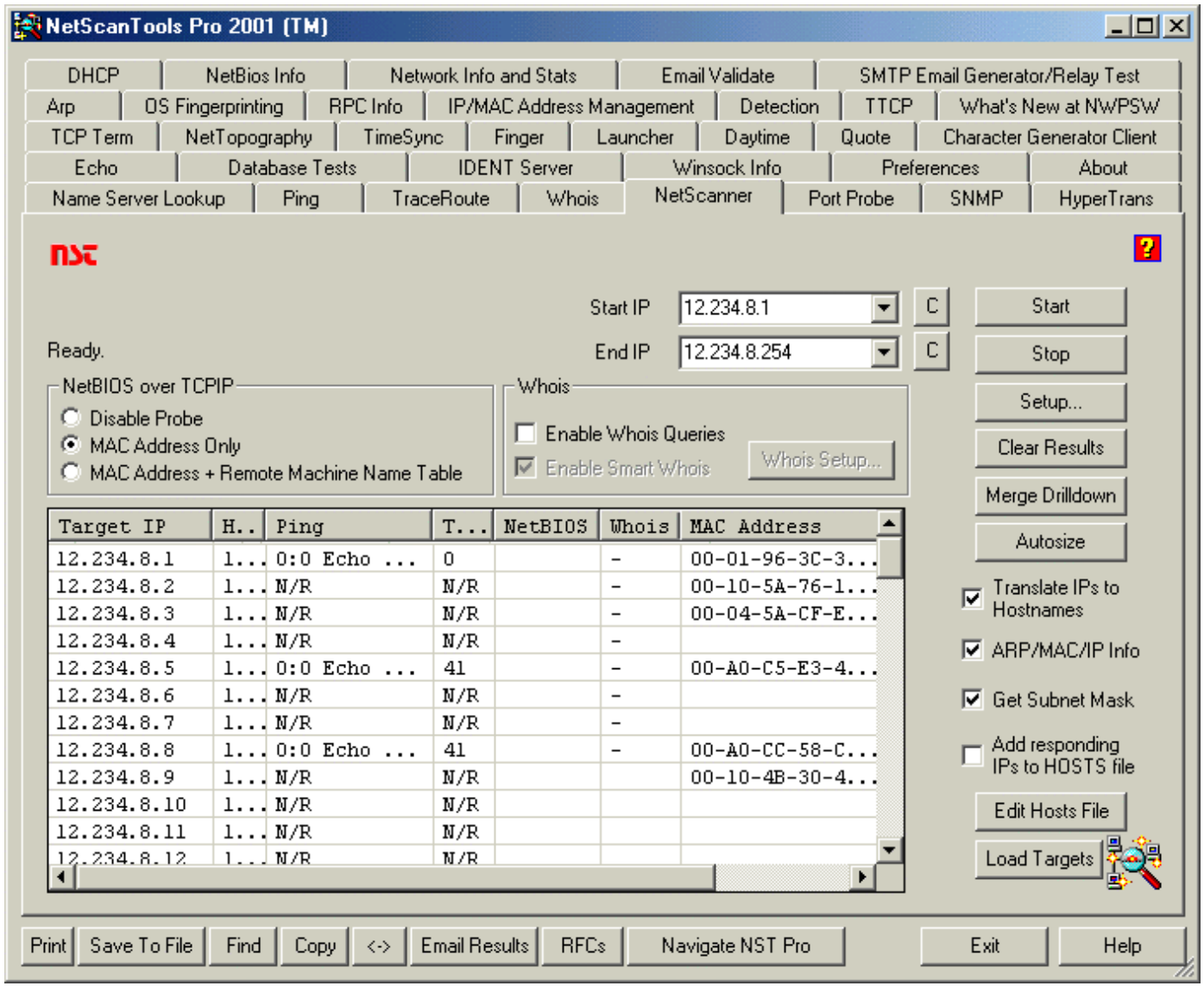
Hacker Tools and Tricks

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

2003 Hot Tools List

- NetScanTools Pro[$]
- Ethereal
- Sam Spade
- Snort + IDScenter
- nMap
- Ettercap
- Dsniff et al
- Specter (Honeypot)[$]
- 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[$]

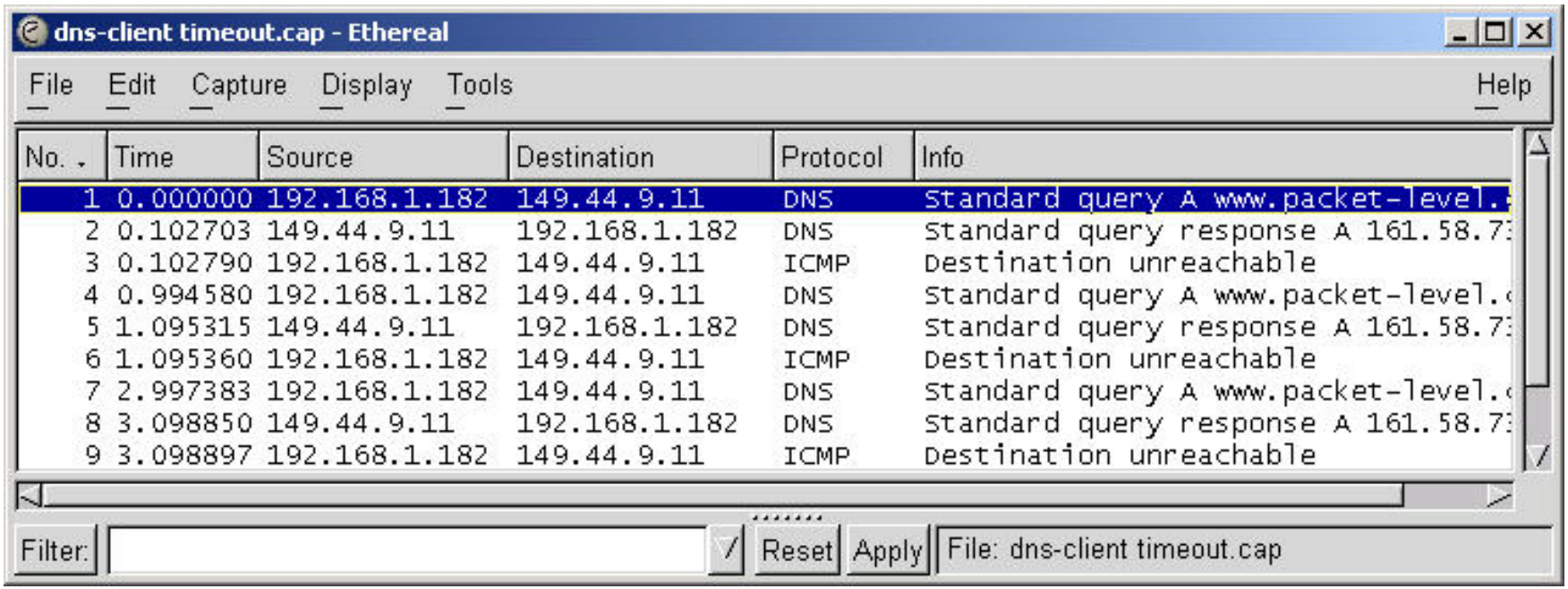
NetScanTools Pro$ www.netscantools.com



Ethereal

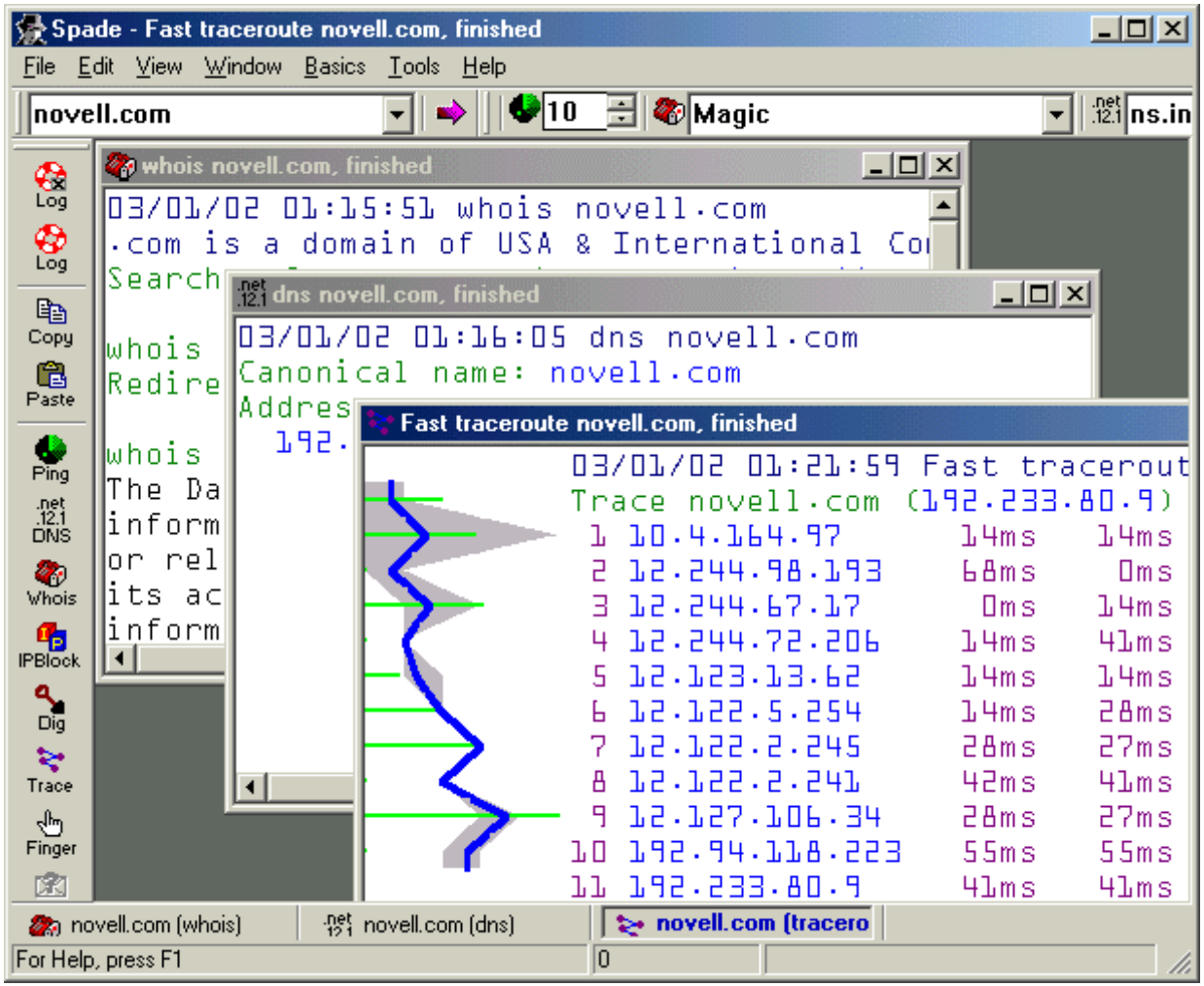
www.ethereal.com

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

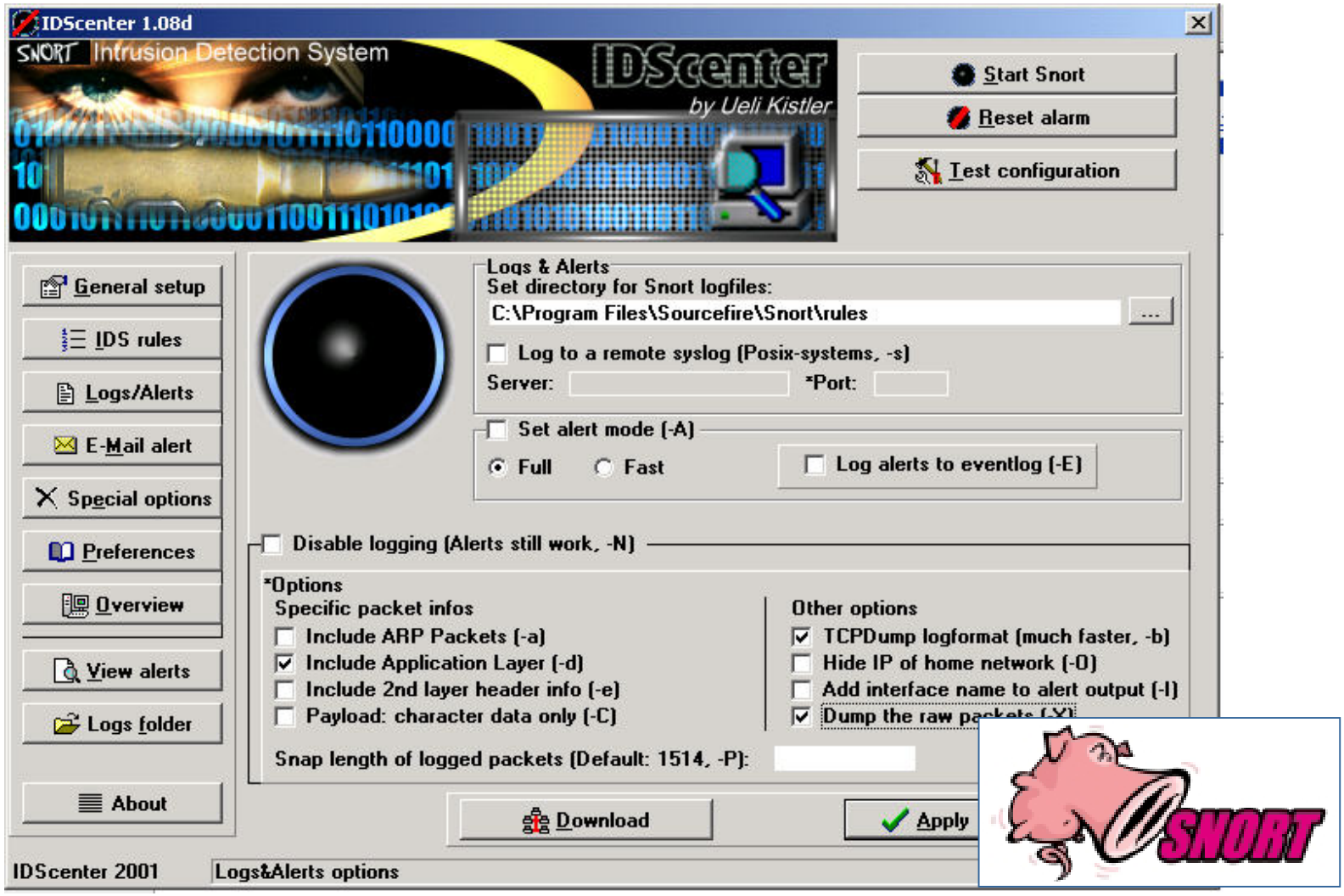


Sam Spade

www.samspade.org

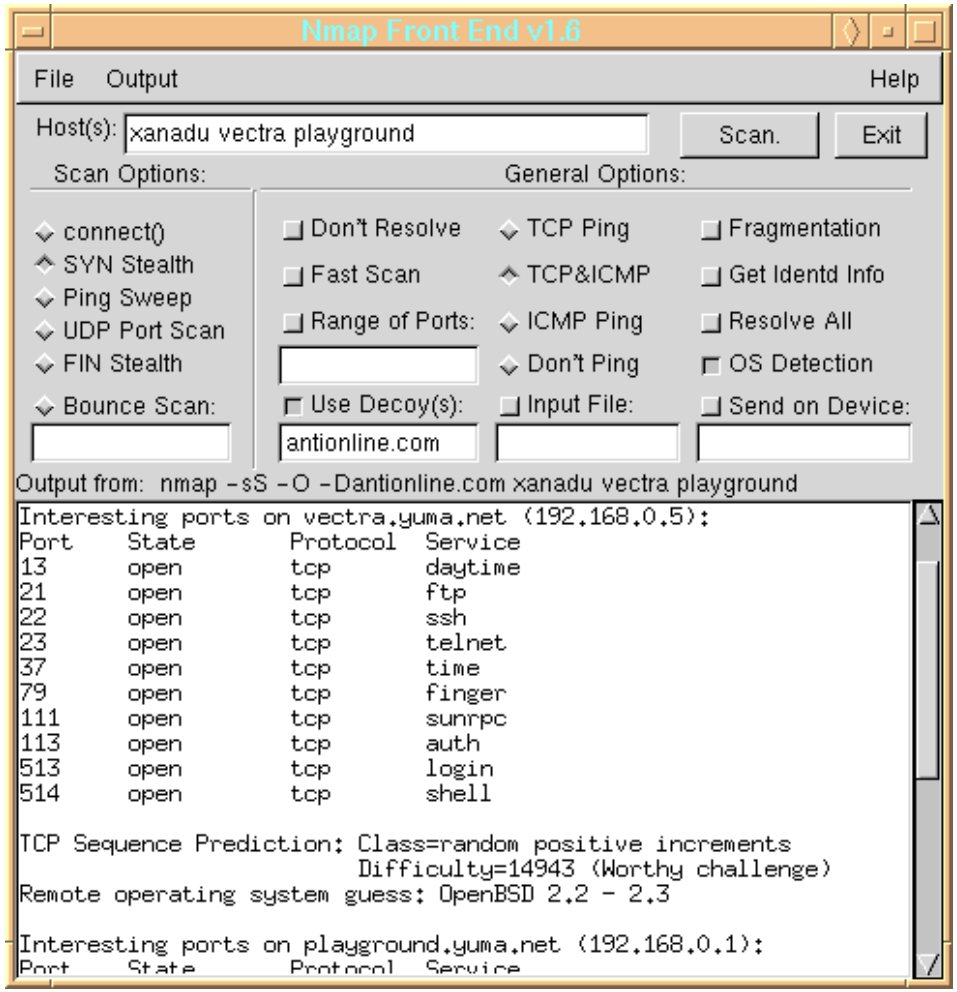


Snort + IDSCenter www.snort.org



nMap

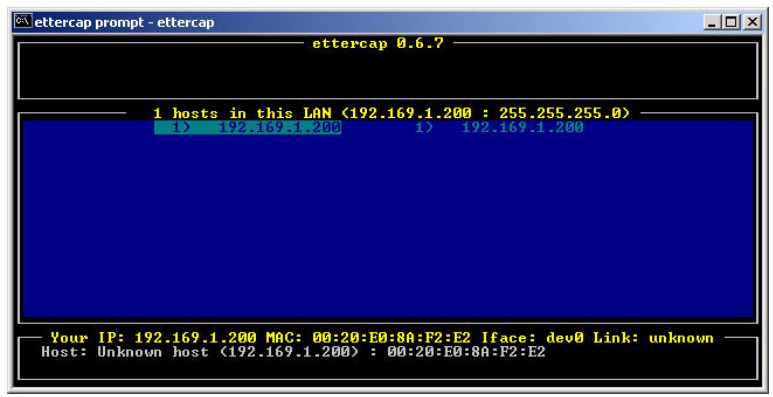
www.insecure.org



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

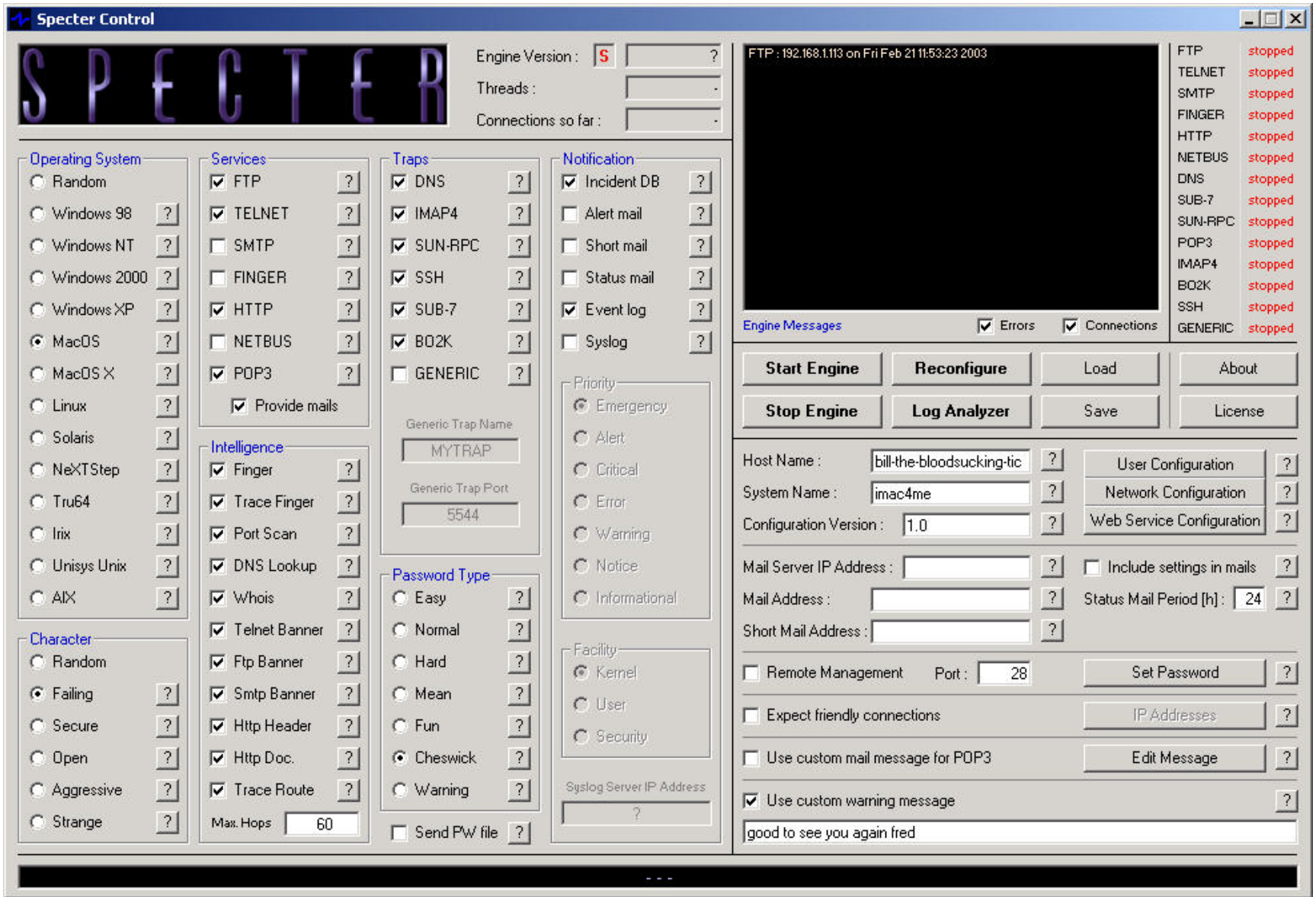


Dsniff et al

www.monkey.org/~dugsong/dsniff/

- Passive tools
  - Dsniff
  - Filesnarf
  - Mailsnarf
  - Msgsnarf
  - Urlsnarf
  - Webspy
- Active attack tools
  - Arpspoof
  - Dnsspoof
  - Macof (fail open/duplicate MACs)

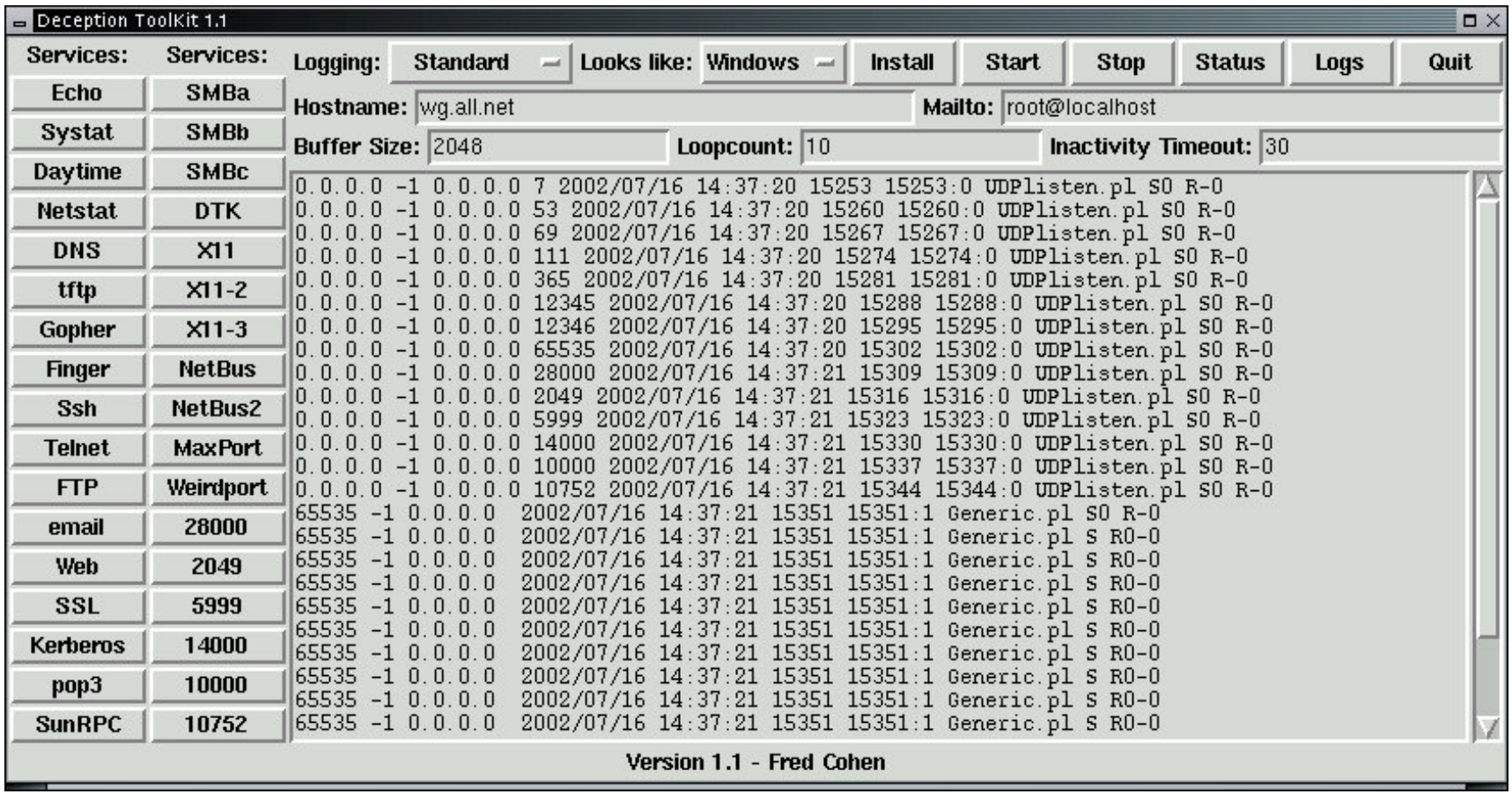
Specter Honeypot $ www.specter.com



White Glove $/Deception Toolkit

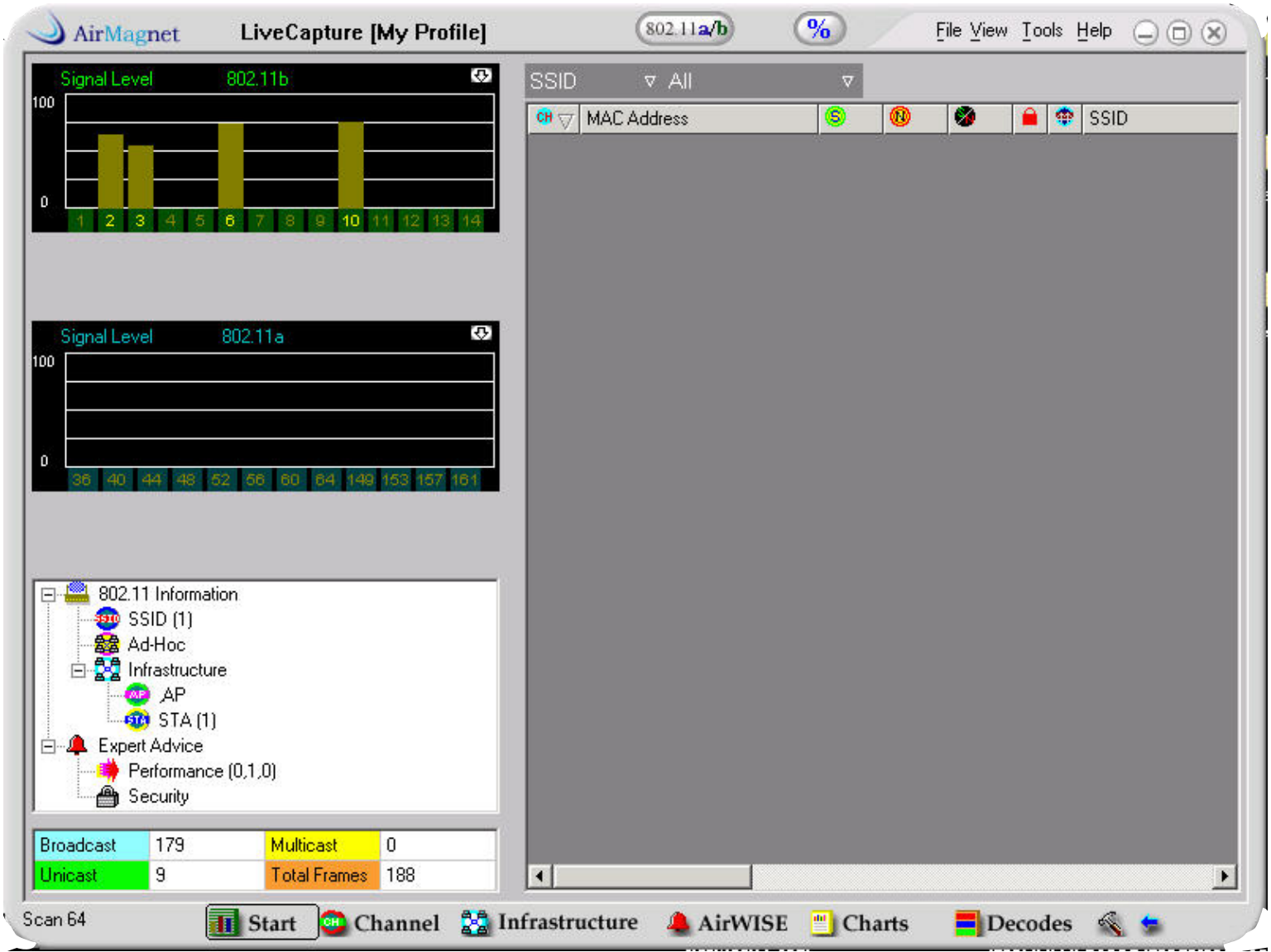
www.all.net

Deception Toolkit (DTK) on White Glove



AirMagnet $

www.airmagnet.com



GPS$ + Antennas $

www.fab-corp.com

pigtails

amplifiers

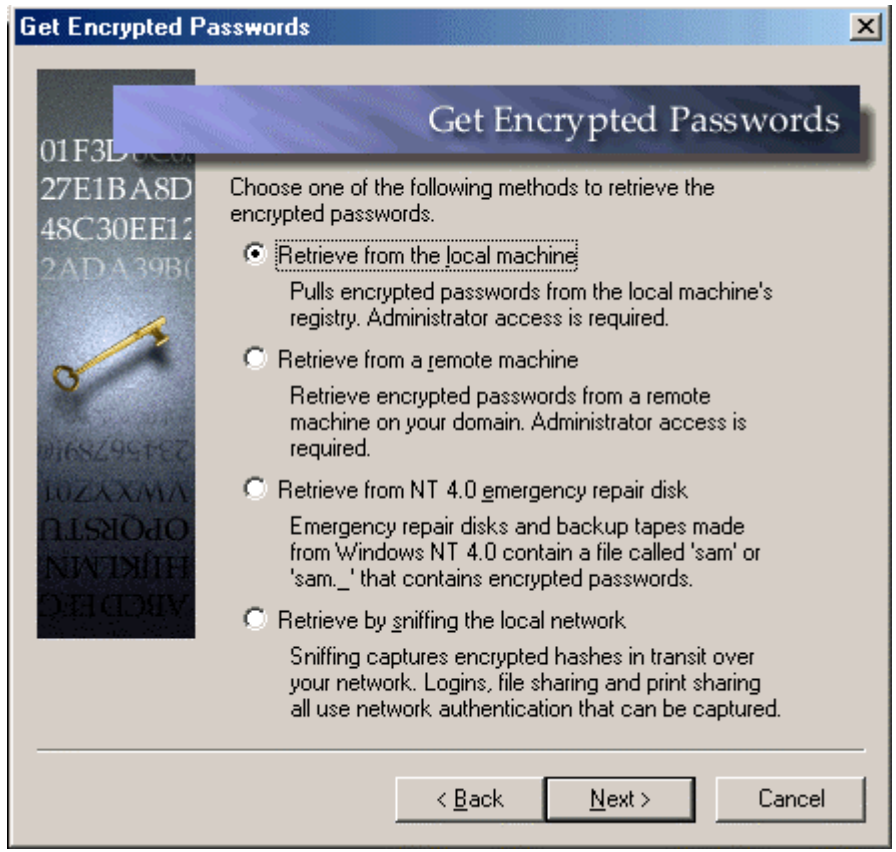
antennas

LC4 $ (L0phtCrack)

www.@stake.com

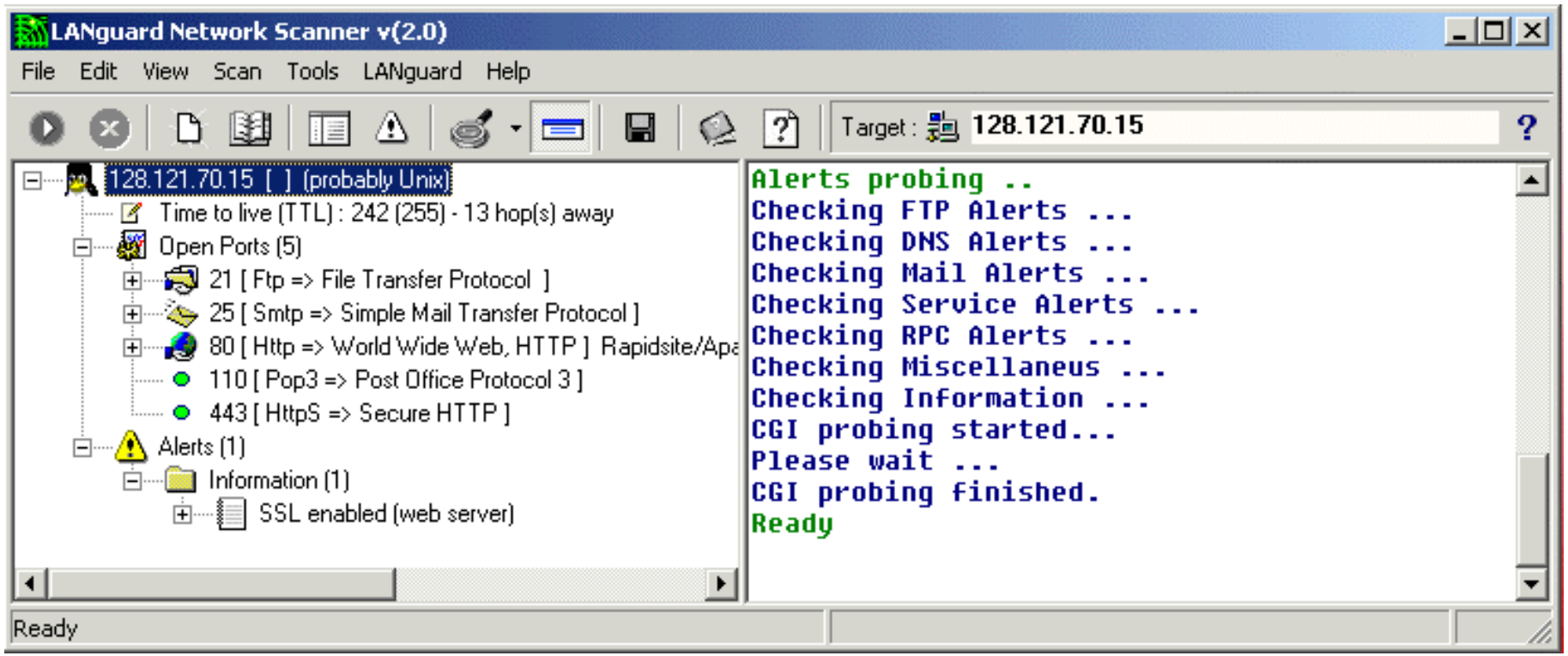
- Password cracking tool – excellent!
- Uh… er… I mean Password auditing and recovery tool!
- Also check out John the Ripper

  www.openwall.com/john/



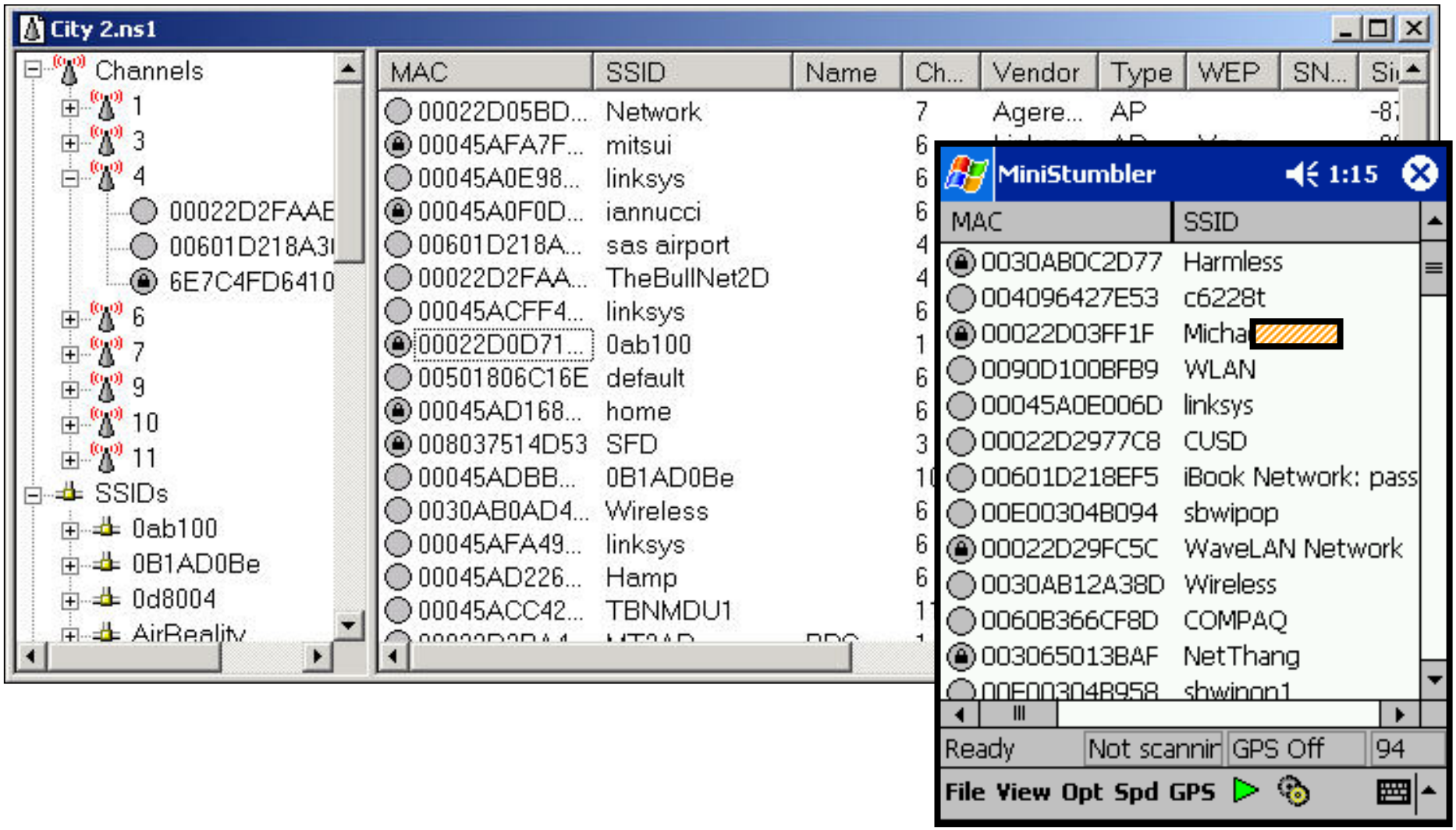
LANGuard$

www.gfi.com



NetStumbler/MiniStumbler

www.netstumbler.com



Invisible Secrets$

www.neobytesolutions.com

LSB Steganography
Data injection or data replacement

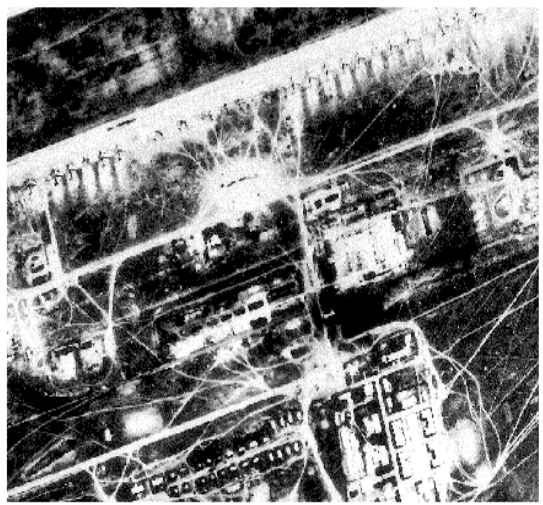
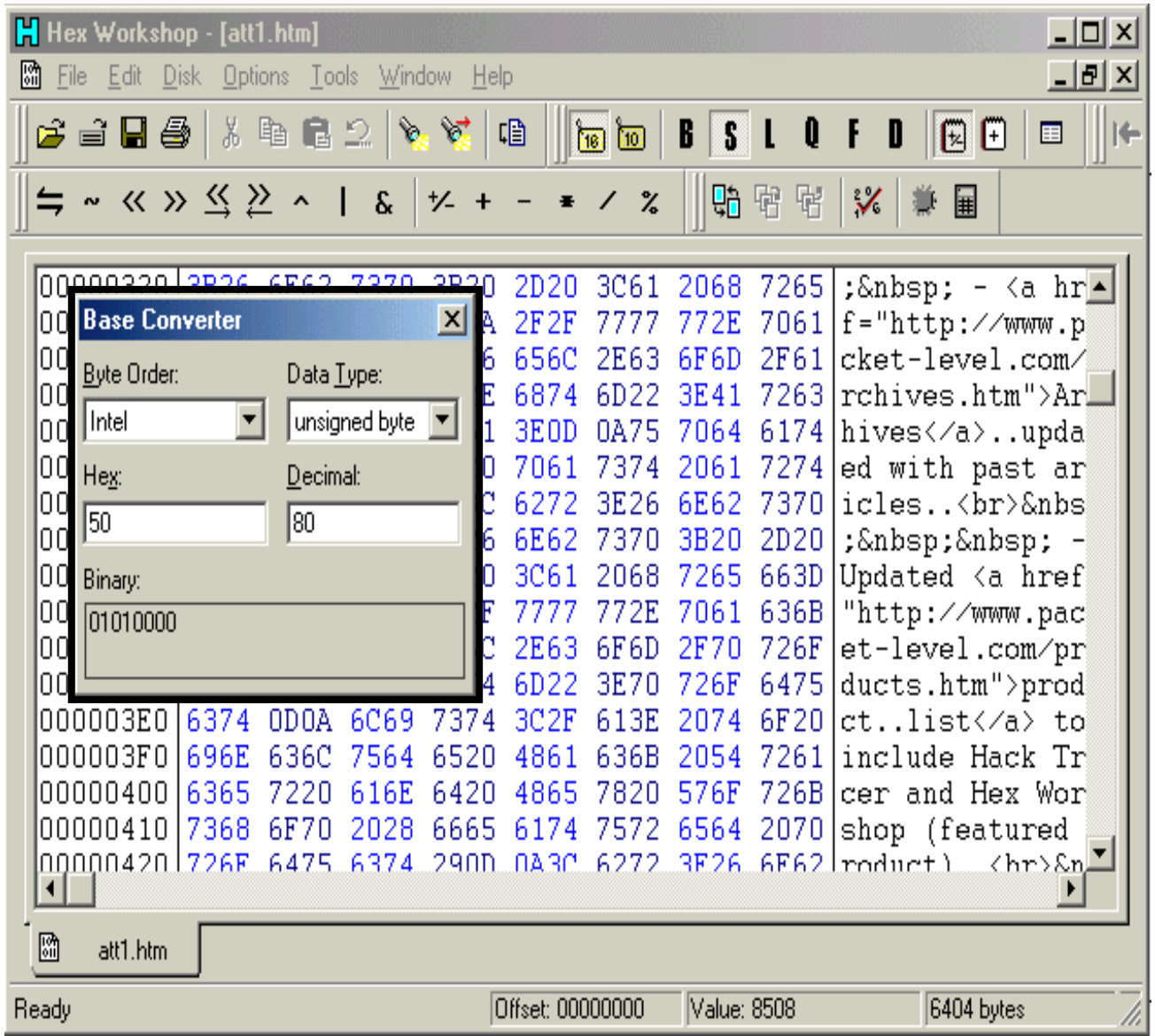


Figure 4: Long-Range Aviation Airfield[5]

Carrier + Secret = Stego Image

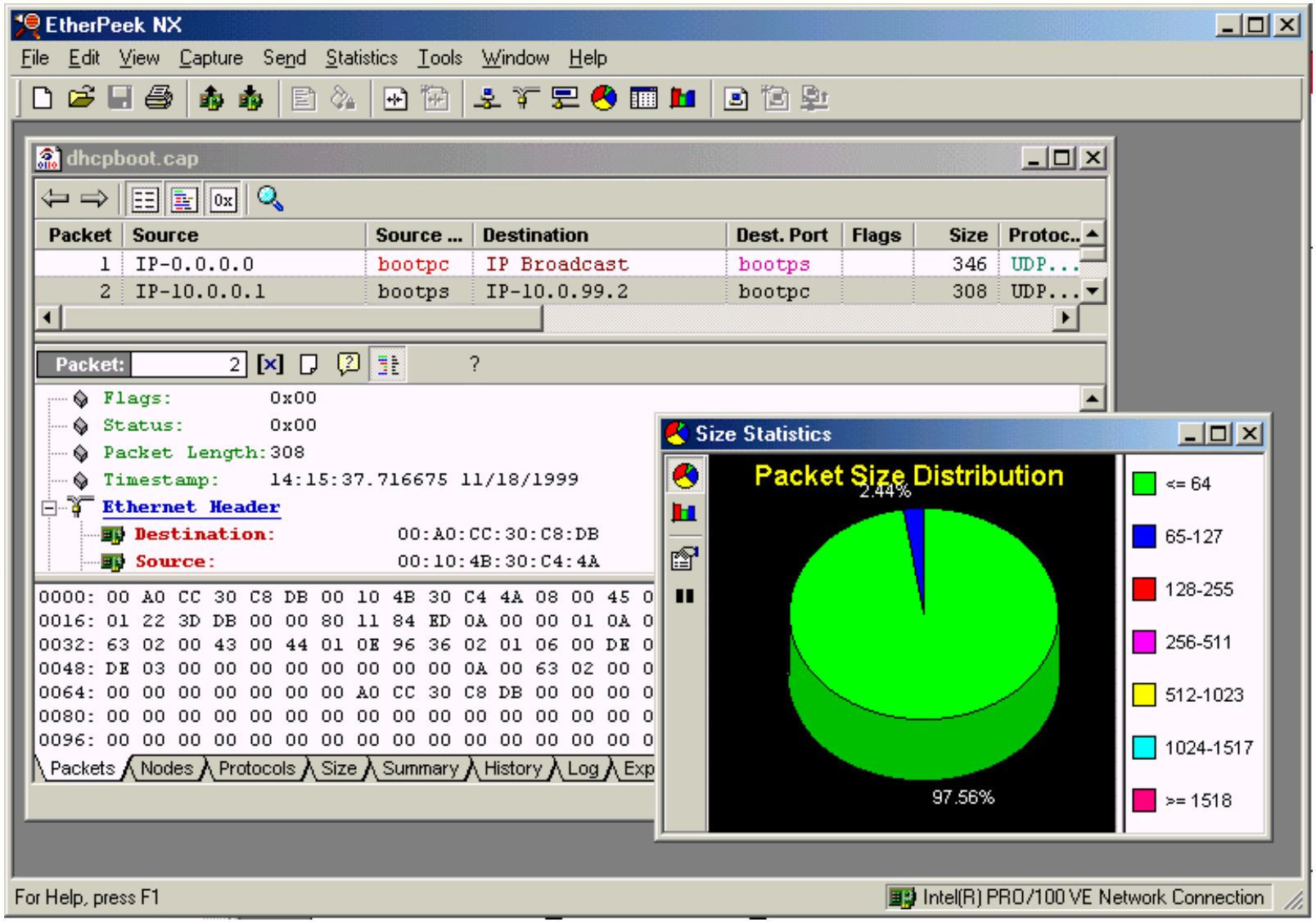
HexWorkshop$

www.bpsoft.com



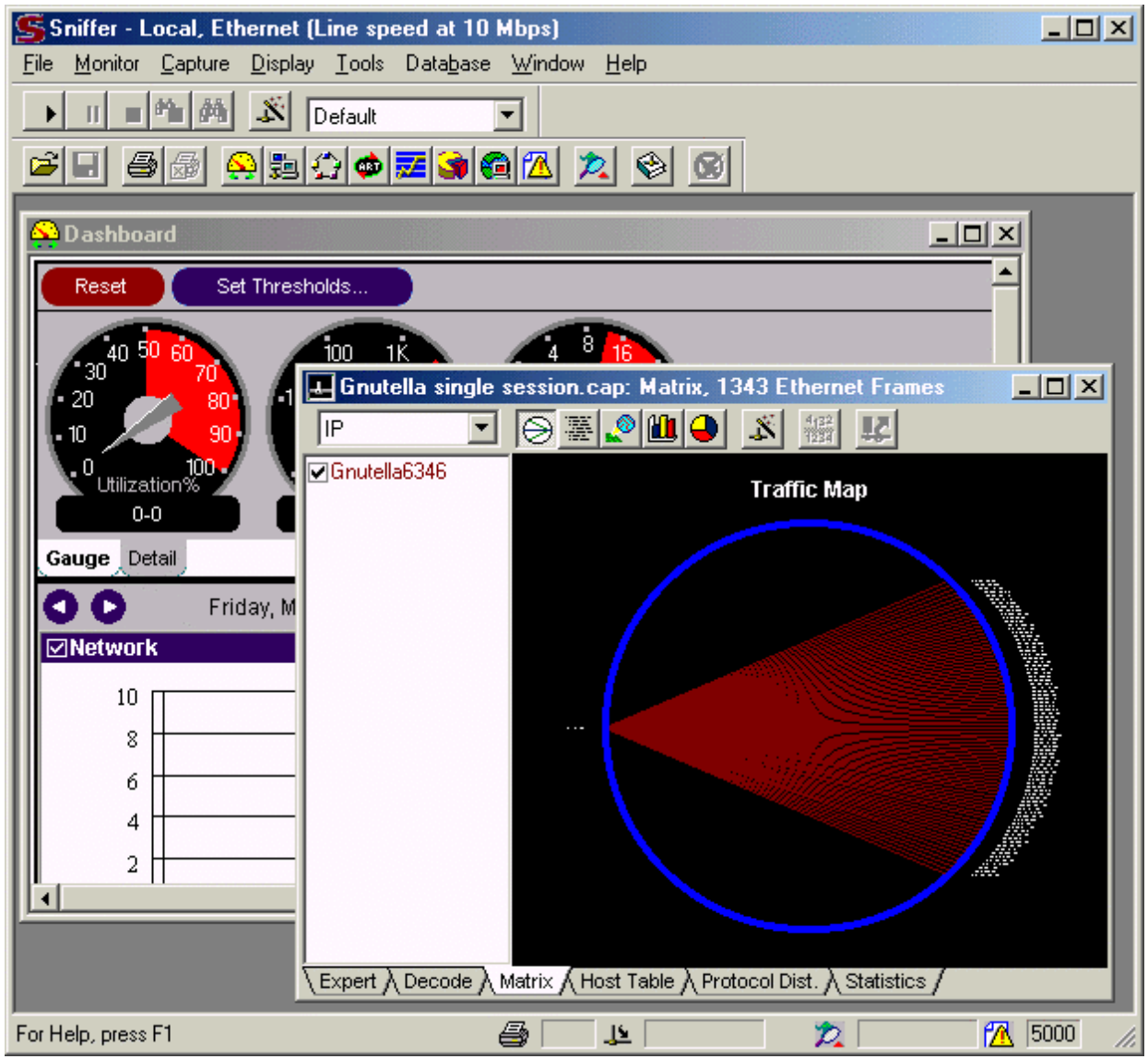
EtherPeek$

www.wildpackets.com



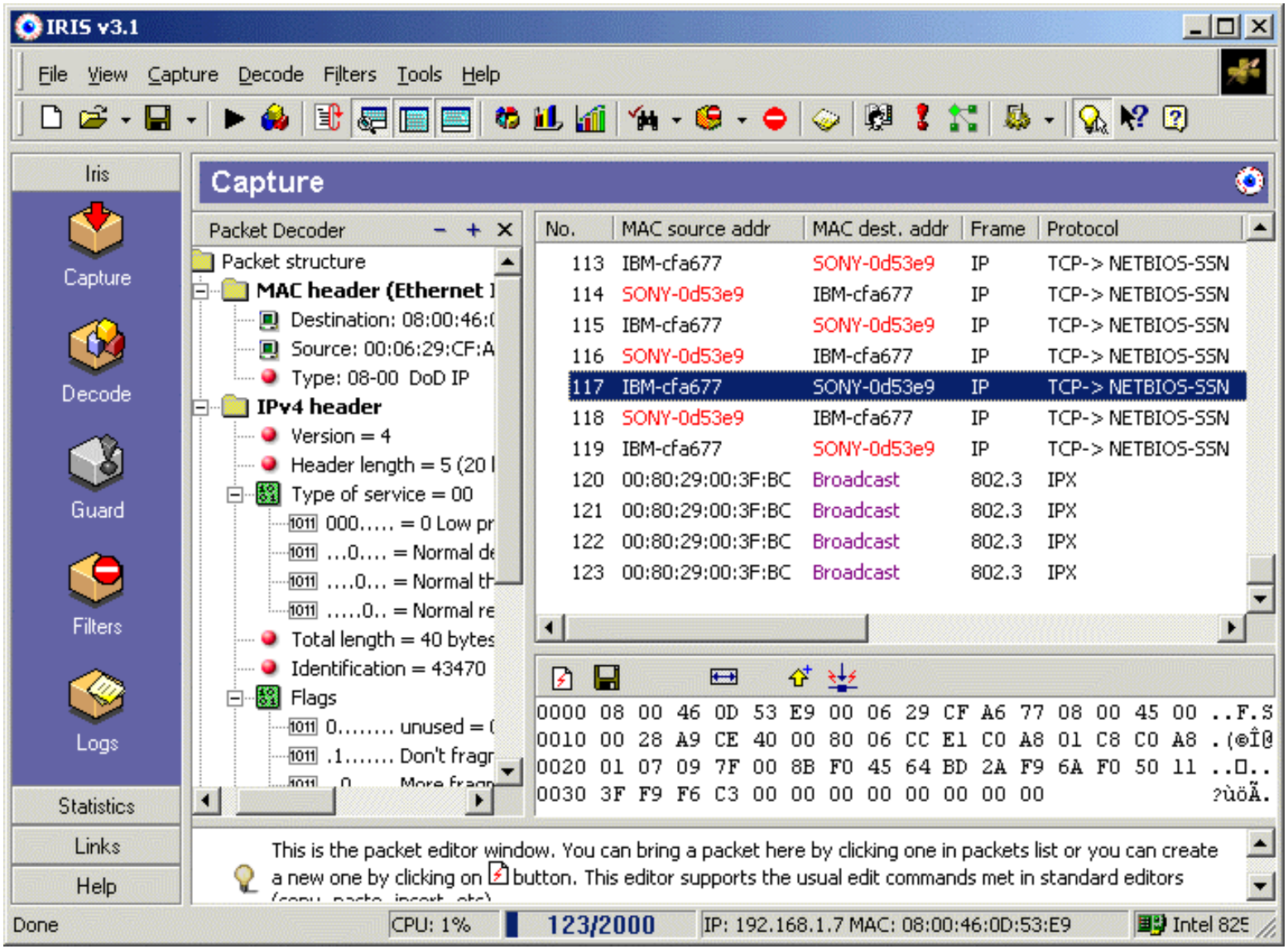
Sniffer$

www.sniffer.com



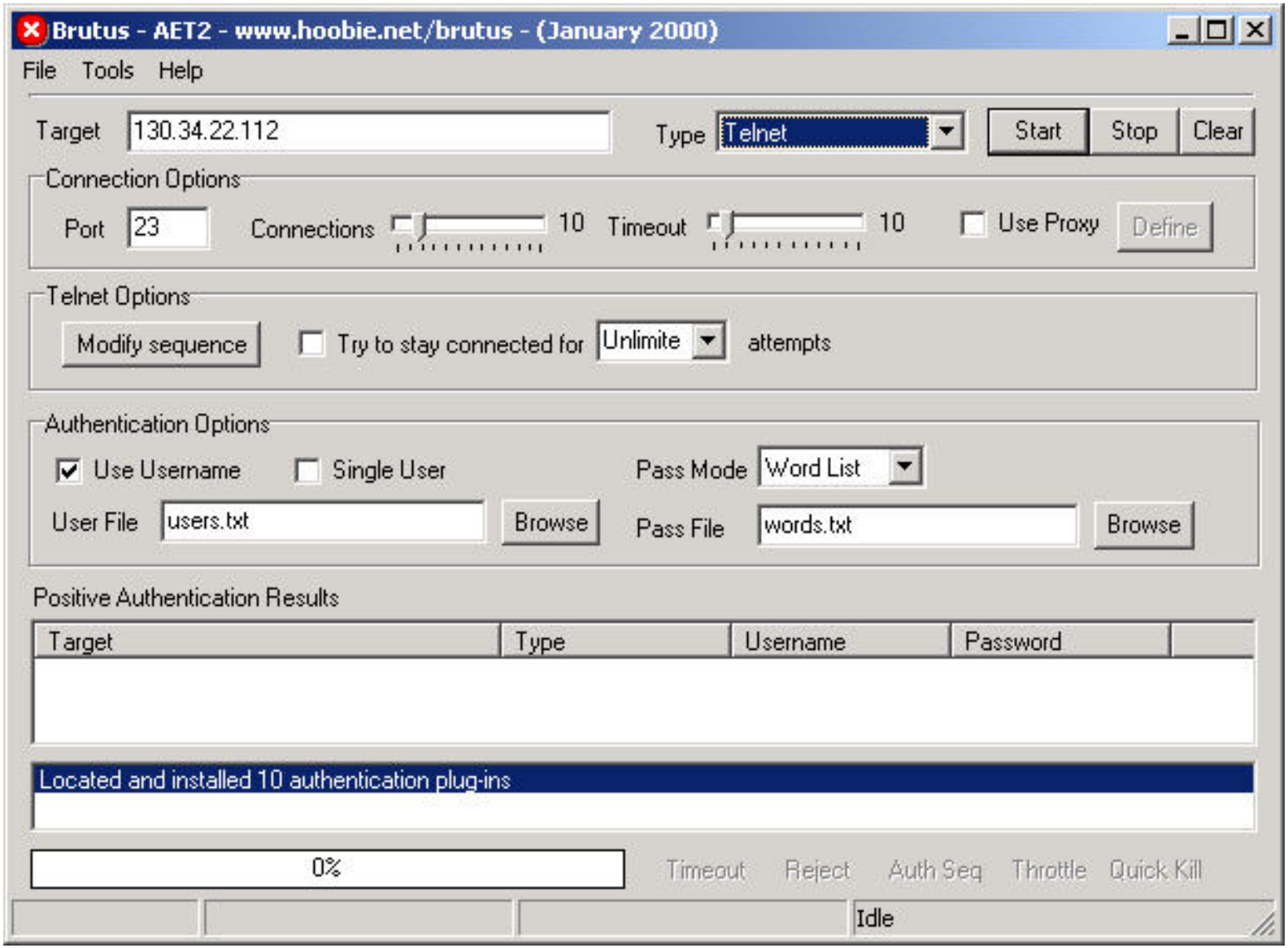
Iris$

www.eeye.com



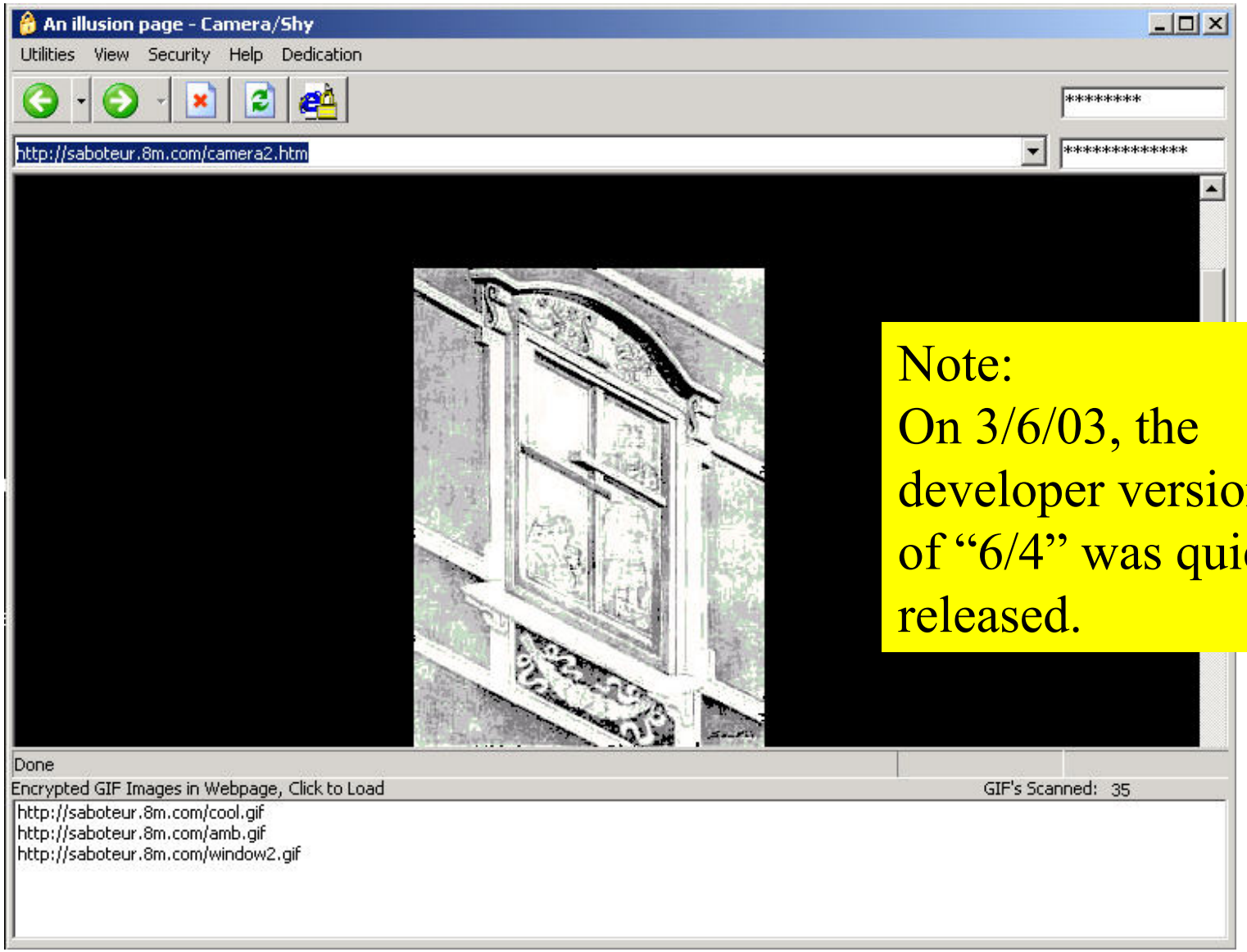
Brutus

www.hoobie.net/brutus



Camera Shy

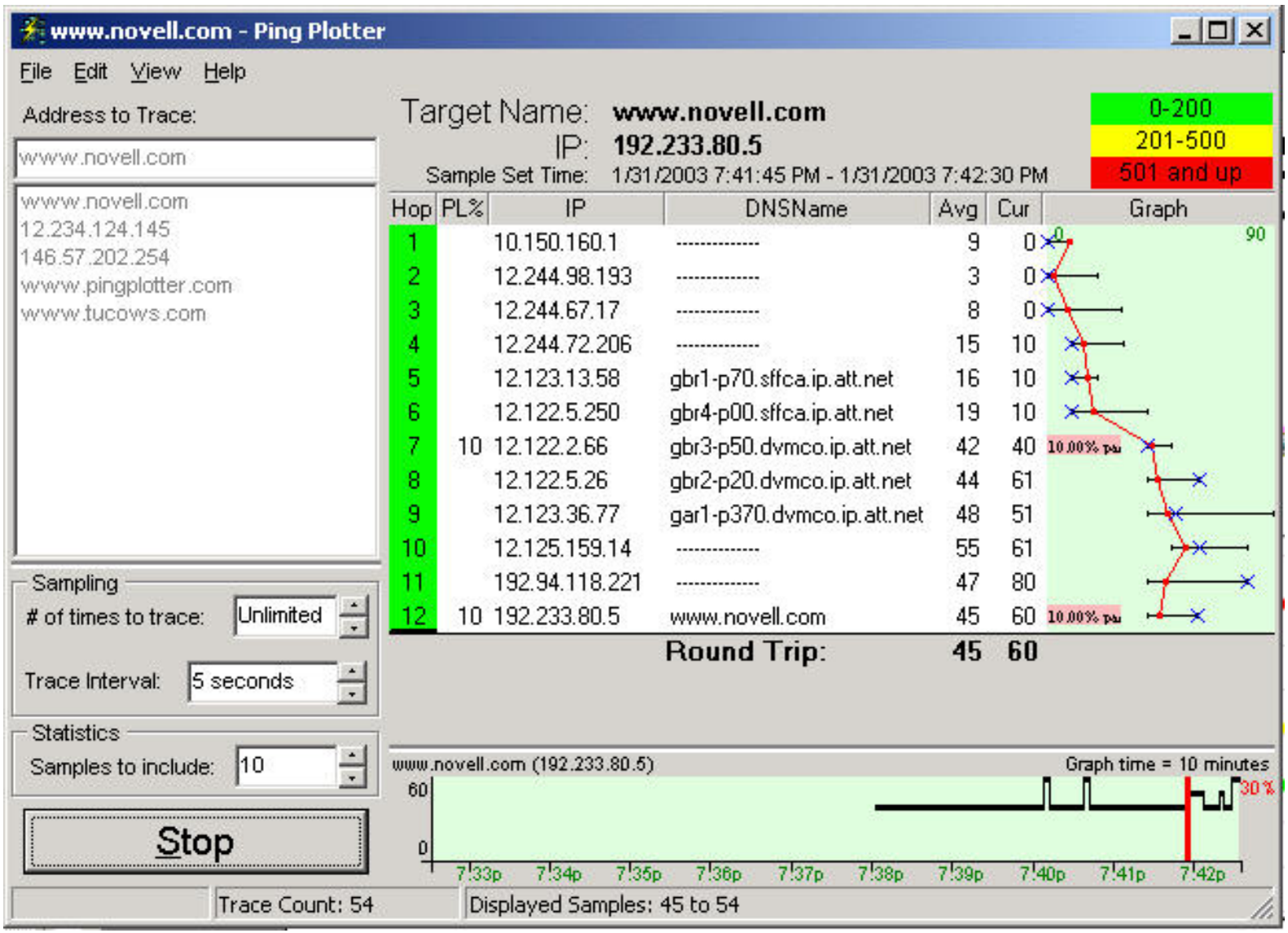
www.hactivismo.com



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

Ping Plotter$

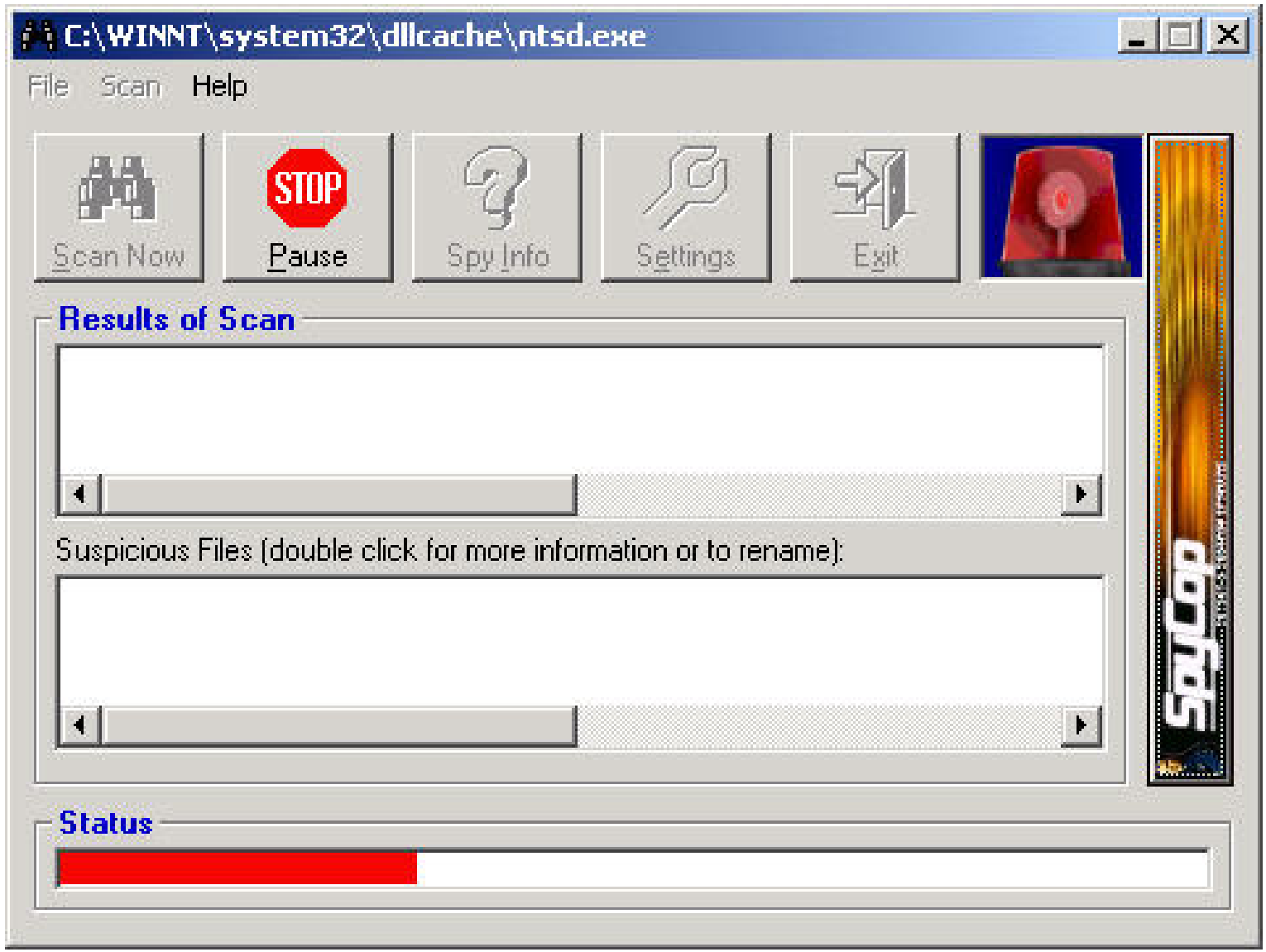
www.pingplotter.com



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