



Hot Tools 2004

Laura Chappell
Protocol Analysis Institute, Inc.
lchappell@packet-level.com
www.packet-level.com
www.podbooks.com

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



WARNING!

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

These Tools Allow You To:

1. **Sniff network passwords and unencrypted data**
2. **Open suspect files**
3. **Locate rogue servers on the network**
4. **Test blocked ports**
5. **Test for SMTP relaying**
6. **Perform reconnaissance on an attacker**
7. **Test for UDP and TCP flood vulnerabilities**
8. **Find evidence on a hard drive**
9. **Set up a decoy system**
10. **Log active connections/endpoints**
11. **Keylog a suspect system**
12. **Sniff wireless network communications**
13. **Hide information in graphics, audio files, etc.**

These Tools Allow You To:

14. **Test password integrity**
15. **Perform a brute force password crack**
16. **Audit a suspect system in stealth mode**
17. **Locate auditing software on the network**
18. **Intercept traffic and alter data**
19. **Locate M-i-M devices**
20. **Locate open shares on network drives**
21. **Identify unpatched systems**
22. **Traceback suspicious email**
23. **View HTTP graphic transfers**
24. **Locate rogue wireless access points**
25. **Surf the Internet anonymously**
26. **Hide surfing activity**

The White Hat/Black Hat Toolkit

- ❑ **Ethereal❖**
- ❑ **Hex Workshop ❖**
- ❑ **NetScanTools Pro ❖**
- ❑ **Nmap Network Scanner ❖**
- ❑ **Packet Builder**
- ❑ **Hurricane Search ❖**
- ❑ **Specter Honeypot ❖**
- ❑ **TCPView ❖**
- ❑ **Cain and Abel ❖**
- ❑ **White Glove/Deception Toolkit**
- ❑ **Snort and IDS Center**
- ❑ **Dsniff**
- ❑ **Keyghost Keylogger**
- ❑ **Brutus Password Cracker ❖**
- ❑ **Aida32 Auditor ❖**
- ❑ **Camera Shy**
- ❑ **Invisible Secrets ❖**
- ❑ **Ettercap Interceptor ❖**
- ❑ **LANguard Network Scanner ❖**
- ❑ **VisualRoute ❖**
- ❑ **HTTP Sniffer ❖**
- ❑ **NetStumbler/MiniStumbler ❖**
- ❑ **Stealth Surfer**
- ❑ **Various antennas and GPS**

❖ **LLK v5.0**

DEMO TIME!

Ethereal

Price: Free; distributed under the GNU license

Link: www.ethereal.com

General: Protocol analyzer; requires winpcap to run over W32 platform (available at winpcap.polito.it).

Sniff Passwords and Unencrypted Data

Virtual Office Password change in clear.enc - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.200.55	192.168.200.201	TCP	1360 > http [SYN] Seq=1
2	0.000016	192.168.200.201	192.168.200.55	TCP	http > 1360 [SYN, ACK]
3	0.000103	192.168.200.55	192.168.200.201	TCP	1360 > http [ACK] Seq=1
4	0.000337	192.168.200.55	192.168.200.201	HTTP	POST /nps/servlet/porta
5	0.001208	192.168.200.201	192.168.200.55	TCP	http > 1360 [ACK] Seq=2

Frame 4 (894 bytes on wire, 894 bytes captured)

```

0230 05 08 03 00 0a 43 01 01 00 09 03 3a 20 4a 35 43  CHE...CUU KIE. JSE
0260 53 53 49 4f 4e 49 44 3d 31 37 39 34 32 32 46 33  SSIONID= 179422F3
0270 35 38 42 45 39 36 33 38 37 41 37 38 32 37 31 32  58BE9638 7A782712
0280 45 43 39 37 37 43 42 38 3b 20 76 69 73 69 74 73  EC977CB8 ; visits
0290 3d 31 3b 20 75 73 65 72 49 64 3d 32 38 32 32 3b  =1; user Id=2822;
02a0 20 6e 6f 76 65 6c 6c 73 65 73 73 69 6f 6e 31 3d  novells ession1=
02b0 78 47 66 51 35 53 30 36 77 77 45 42 41 41 45 42  xGfQ5S06 wwEBAAEB
02c0 41 51 41 42 41 77 3d 3d 0d 0a 0d 0a 47 49 5f 49  AQABAW== ....GI_I
02d0 44 3d 25 37 42 42 30 38 44 39 36 33 39 2d 30 30  D=%7BB08 D9639-00
02e0 30 30 2d 30 30 46 35 2d 46 38 46 31 2d 37 44 37  00-00F5- F8F1-7D7
02f0 35 43 30 41 38 43 38 43 39 25 37 44 25 33 41 31  5C0A8C8C 9%7D%3A1
0300 33 36 39 38 31 32 31 31 34 25 33 41 36 38 30 32  36981211 4%3A6802
0310 34 32 34 33 34 26 61 63 74 69 6f 6e 3d 63 68 61  42434&ac tion=cha
0320 6e 67 65 50 61 73 73 77 6f 72 64 26 6f 6c 64 50  ngePassw ord&oldP
0330 61 73 73 77 6f 72 64 3d 6e 6f 76 65 6c 6c 31 26  assword= novell1&
0340 6e 65 77 50 61 73 73 77 6f 72 64 31 3d 6e 6f 76  newPassw ord1=nov
0350 65 6c 6c 26 6e 65 77 50 61 73 73 77 6f 72 64 32  ell&newP assword2
0360 3d 6e 6f 76 65 6c 6c 26 63 68 61 6e 67 65 2e 78  =novell& change.x
0370 3d 34 36 26 63 68 61 6e 67 65 2e 79 3d 33  =46&chan ge.y=3
  
```

Filter: / Reset Apply File: Virtual Office Password change in clear.enc

Hex Workshop

Price: US \$49.95

Link: www.bpsoft.com

General: General hex editor; includes Base Converter applet.





NetScanTools Pro

Price: US \$199.00

Link: www.netscantools.com

General: Multifunction tool that includes Wizard tool to help trace back and identify a device.

NetScanTools Pro 2004

File View Help

NetScanTools Pro. Because you need to know what's out there. (tm)

Welcome

Automated

Tools

Tools (alpha order)

- ARP
- Connection Detection
- Database Tests
- DHCP Server Discovery
- Discovery - Passive
- Email Validate
- Finger
- HyperTrans/DNS Verify/ASN-IRR
- IP Address/Country Mapping
- IP Packet Viewer
- IP/MAC Address Management
- Launcher
- Name Server Lookup
- Net Topography
- NetBIOS Info-Shares/System Basics
- NetBIOS Info-Advanced
- NetScanner
- Network Statistics**
- OS Fingerprinting
- Ping
- Port Scanner
- RBL Check
- RFC Reference
- Rp. RPC Info

Online

Program Info

For Help, press F1

Network Statistics This feature is similar to the 'netstat' command line function.

☐ Display Trojan Port Labels

☐ Display Full Process Paths

☒ Enable Double Click TCP Disconnects

Disconnect All TCP

Ready.

Refresh All

☐ Auto-Refresh Endpoint List

Refresh Interval

1 sec 10 sec

Network Info For This Computer

Statistics by Protocol

- IP
- ICMP
- TCP
- UDP

Network Interface List

TCP/UDP Connection Endpoint List

Process:PID	Protocol	Local IP:Port
svchost.exe:396	TCP	0.0.0.0:135(epmap)
System:8	TCP	0.0.0.0:445(micros...
MSTask.exe:672	TCP	0.0.0.0:1025(unknown)
System:8	TCP	0.0.0.0:1026(unknown)
spamkiller.exe:1228	TCP	0.0.0.0:1027(unknown)
spamkiller.exe:1228	TCP	0.0.0.0:1029(unknown)
spamkiller.exe:1228	TCP	0.0.0.0:1035(unknown)
spamkiller.exe:1228	TCP	0.0.0.0:1041(unknown)
spamkiller.exe:1228	TCP	0.0.0.0:1047(unknown)

Nmap

Price: Free

Link: www.insecure.org

General: Well-recognized network mapping tool includes timing mechanism, Xmas mapping and idle mapping

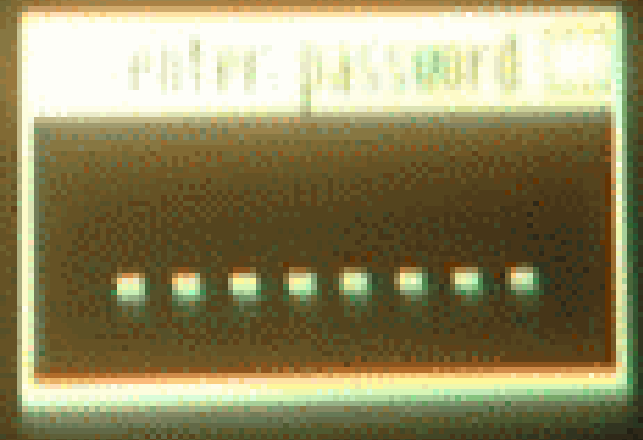
The Matrix Reloaded

**What is
Trinity
using?**

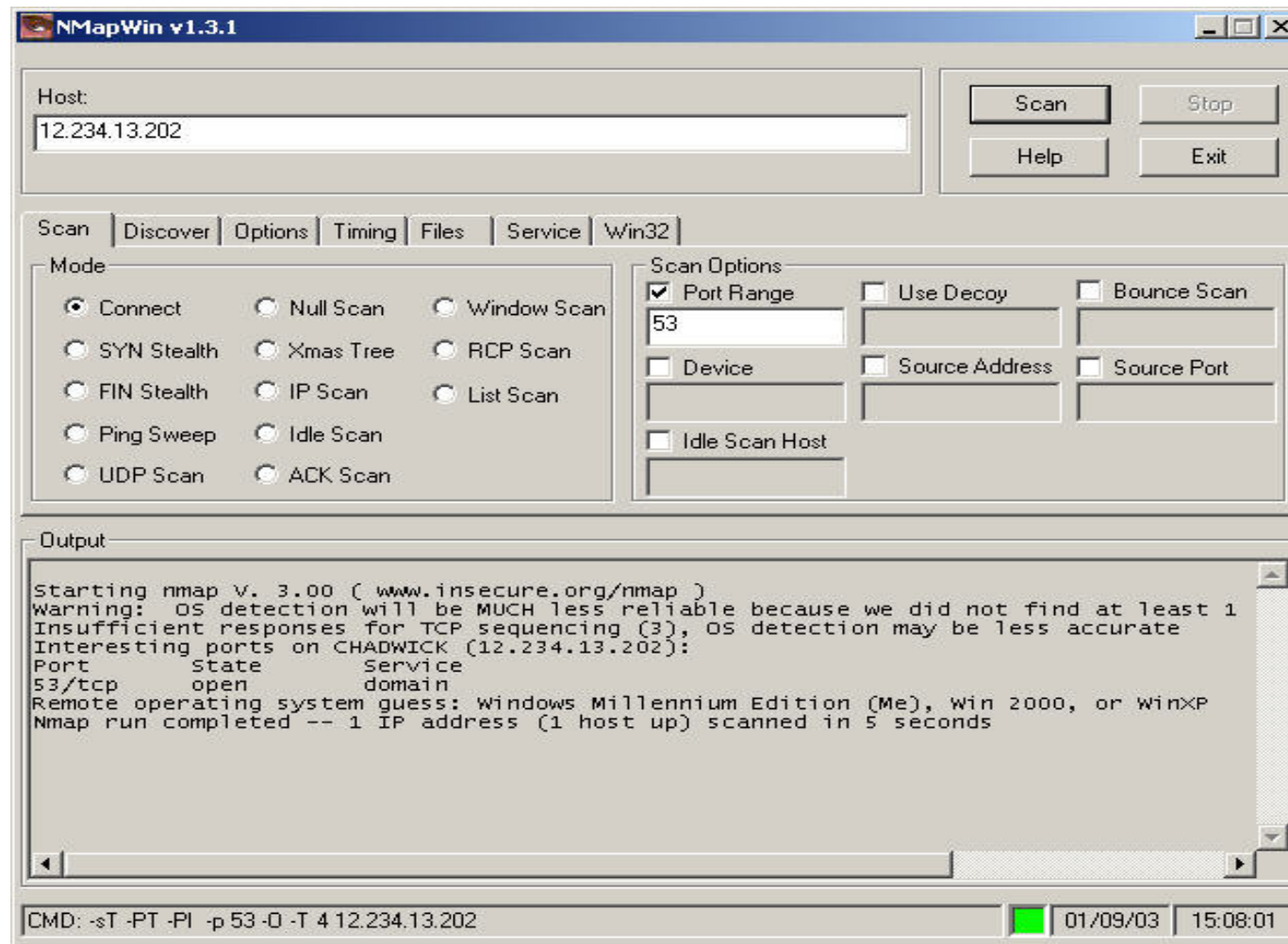


The Matrix Reloaded: Nmap!

```
Nmap run completed -- 1 IP address (1 host up) scanned
# sshoke 10.2.2.2 -rootpw="210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "210N0101".
System open: Access Level (9)
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: |
```



Perform Reconnaissance on an Attacker



Packet Builder

Price: Free

Link: www.engagesecurity.com

General: Built by Gregory Wilmes; runs on winpcap; download .rsb scripts (Packet Builder was formerly called "Rafale")

Test Flood Vulnerabilities

Engage Packet builder

File Modules Managers Options Language Help

Network interface : **1 : Intel 8255x-based Integrated Fast Ethernet** **Inf**

☐ Set as source IP ☐ Set as destination IP

[Ethernet]

Specify destination (MAC) ☐

Specify source (MAC) ☐ **00D05944AF80**

[IP]

Source IP : **10.4.2.1** Port : **1024**

Destination IP : **10.7.1.1** Port : **53**

Specify header size ☐ **5** x 4 (bytes)

Type of service : **Routine**

Specify total length ☐ **28**

Specify identification ☐ **0**

Fragmentation : DF : **0 : May Fragment**

MF : **0 : Last Fragment**

Offset : **0** x 8 TTL : **128**

Protocol : **17 : UDP**

Specify checksum ☐ **0**

TCP UDP ICMP

0 ☐ Specify UDP checksum

[Data]

From file ☐

Test UDP packet stream:

[Commands]

Nb of packets : **1000** Packet type : **UDP** **SEND**

[Script]

RUN SCRIPT

Status : Ready.

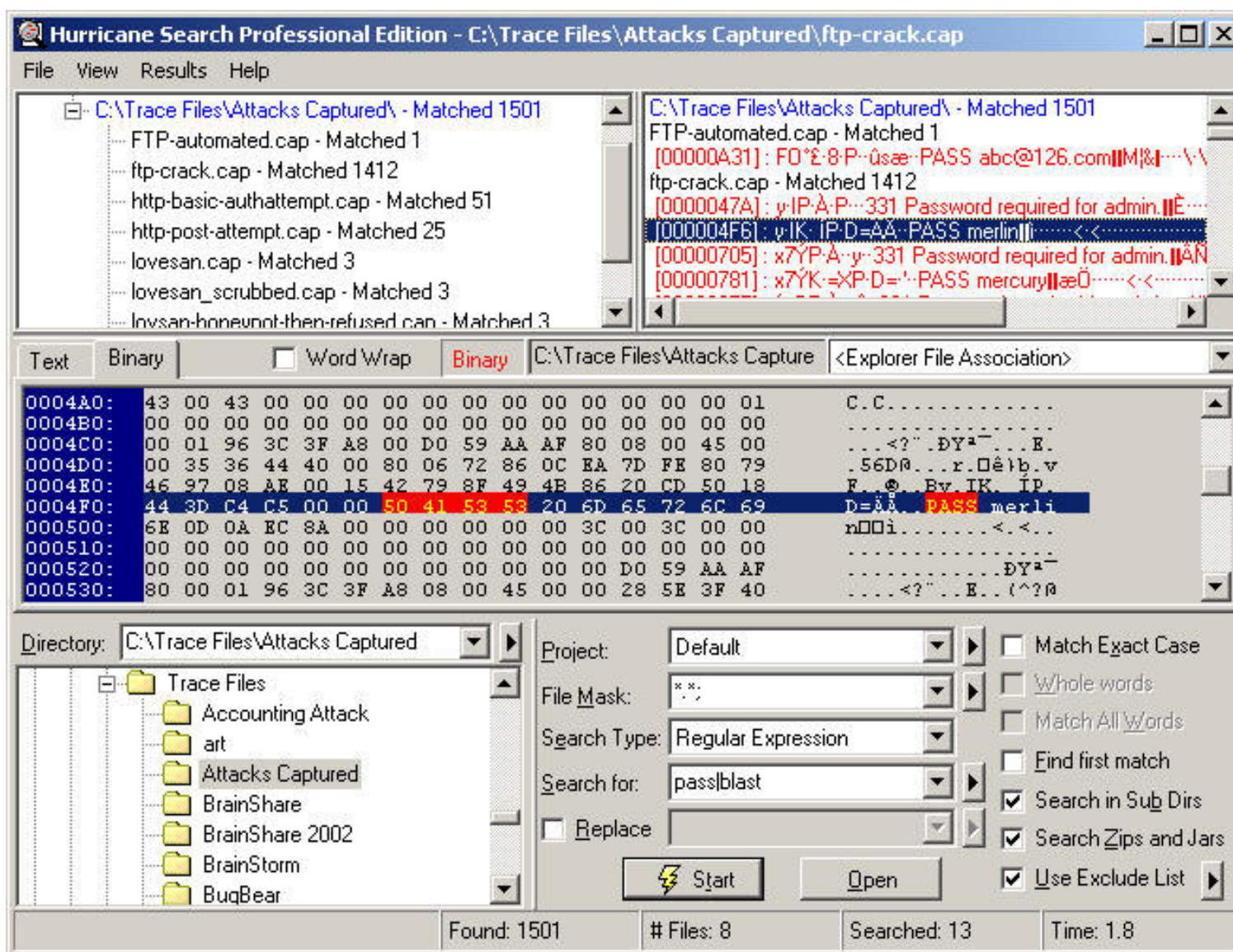
Hurricane Search

Price: US \$149

Link: www.hurricanesoft.com

General: Grep-like tool; can search through zipped files; use “|” to search for multiple terms.

Find Evidence on a Hard Drive



Hurricane Search Professional Edition - C:\Trace Files\Attacks Captured\ftp-crack.cap

File View Results Help

C:\Trace Files\Attacks Captured\ - Matched 1501

- FTP-automated.cap - Matched 1
- ftp-crack.cap - Matched 1412
- http-basic-authattempt.cap - Matched 51
- http-post-attempt.cap - Matched 25
- lovesan.cap - Matched 3
- lovesan_scrubbed.cap - Matched 3
- lovesan-honeypot-then-refused.cap - Matched 3

C:\Trace Files\Attacks Captured\ - Matched 1501

FTP-automated.cap - Matched 1

[00000431]: F0*E-8-P-0sae-PASS abc@126.com||M|&|...\\

ftp-crack.cap - Matched 1412

[0000047A]: y-IP-A-P-331 Password required for admin.||E....

[000004F6]: v|K-IP-D-AA-PASS merlin||<<.....

[00000705]: x7YP-A-y-331 Password required for admin.||AN

[00000781]: x7YK-X-P-D-AA-PASS mercury||æ0.....<<.....

Text Binary ☐ Word Wrap **Binary** C:\Trace Files\Attacks Capture <Explorer File Association>

0004A0:	43	00	43	00	00	00	00	00	00	00	00	00	00	00	00	01	C.C.....
0004B0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0004C0:	00	01	96	3C	3F	A8	00	D0	59	AA	AF	80	08	00	45	00	...<?"..DY^~...E.
0004D0:	00	35	36	44	40	00	80	06	72	86	0C	EA	7D	FE	80	79	.56D0...r.0ê)b.v
0004E0:	46	97	08	AE	00	15	42	79	8F	49	4B	86	20	CD	50	18	F..@..Bv.IK..IP.
0004F0:	44	3D	C4	C5	00	00	50	41	53	53	20	6D	65	72	6C	69	D=AA..PASS merli
000500:	6E	0D	0A	EC	8A	00	00	00	00	00	00	00	3C	00	00	00	n00i.....<.<..
000510:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000520:	00	00	00	00	00	00	00	00	00	00	00	00	D0	59	AA	AFDY^~
000530:	80	00	01	96	3C	3F	A8	08	00	45	00	00	28	5E	3F	40	...<?"..E..(^?0

Directory: C:\Trace Files\Attacks Captured

- Trace Files
 - Accounting Attack
 - art
 - Attacks Captured
 - BrainShare
 - BrainShare 2002
 - BrainStorm
 - BugBear

Project: Default

File Mask: *.*

Search Type: Regular Expression

Search for: passblast

☐ Replace

☐ Match Exact Case

☐ Whole words

☐ Match All Words

☐ Find first match

☒ Search in Sub Dirs

☒ Search Zips and Jars

☒ Use Exclude List

Start **Open**

Found: 1501 # Files: 8 Searched: 13 Time: 1.8



Specter Honeypot

Price: \$400-\$899 depending on OS spoofing abilities

Link: www.specter.com

General: Slick interface; spoofs numerous OS types; silencer option addresses DoS possibility; use markers to correlate hard drive with an attack.

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
- ☐ FreeBSD

Services

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

Traps

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

Generic Trap Name
Slammer

Generic Trap Port
1434

Notification

- ☒ Incident DB
- ☐ Alert mail
- ☐ Short mail
- ☐ Status mail
- ☒ Event log
- ☐ Syslog
- ☒ Silencer
- ☐ Markers
- ☐ Legal message
- ☐ Online updates
- ☐ Use HTTP Proxy

Configure Syslog

Silencer Configuration

Check for updates

Proxy IP Address
?

Proxy Port
8080

Intelligence

- ☒ Finger
- ☒ Trace Finger
- ☒ Port Scan
- ☒ DNS Lookup
- ☒ Whois
- ☒ Telnet Banner
- ☒ Ftp Banner
- ☒ Smtt Banner
- ☒ Http Header
- ☒ Http Document
- ☒ Trace Route

Max. Hops
60

Character

- ☐ Random
- ☐ Failing
- ☐ Secure
- ☐ Open
- ☒ Aggressive
- ☐ Strange

Password Type

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

☒ Send Pw file

Start Engine

Stop Engine

Reconfigure

Log Analyzer

Load

Save

About

License

Engine Messages

☒ Errors
☒ Connections

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

Host Name :

SVR045A

User Configuration

System Name :

ACCT

Network Configuration

Configuration Version :

1.0

Web Service Configuration

Mail Server IP Address :

Mail Address :

☐ Include settings in mails

Short Mail Address :

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

Hello Fred - good to have you back again.

TCPView

Price: Free

Link: www.sysinternals.com

General: TCP connection and UDP endpoint tracking; tear down connections.

Log Active Connections/Endpoints

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

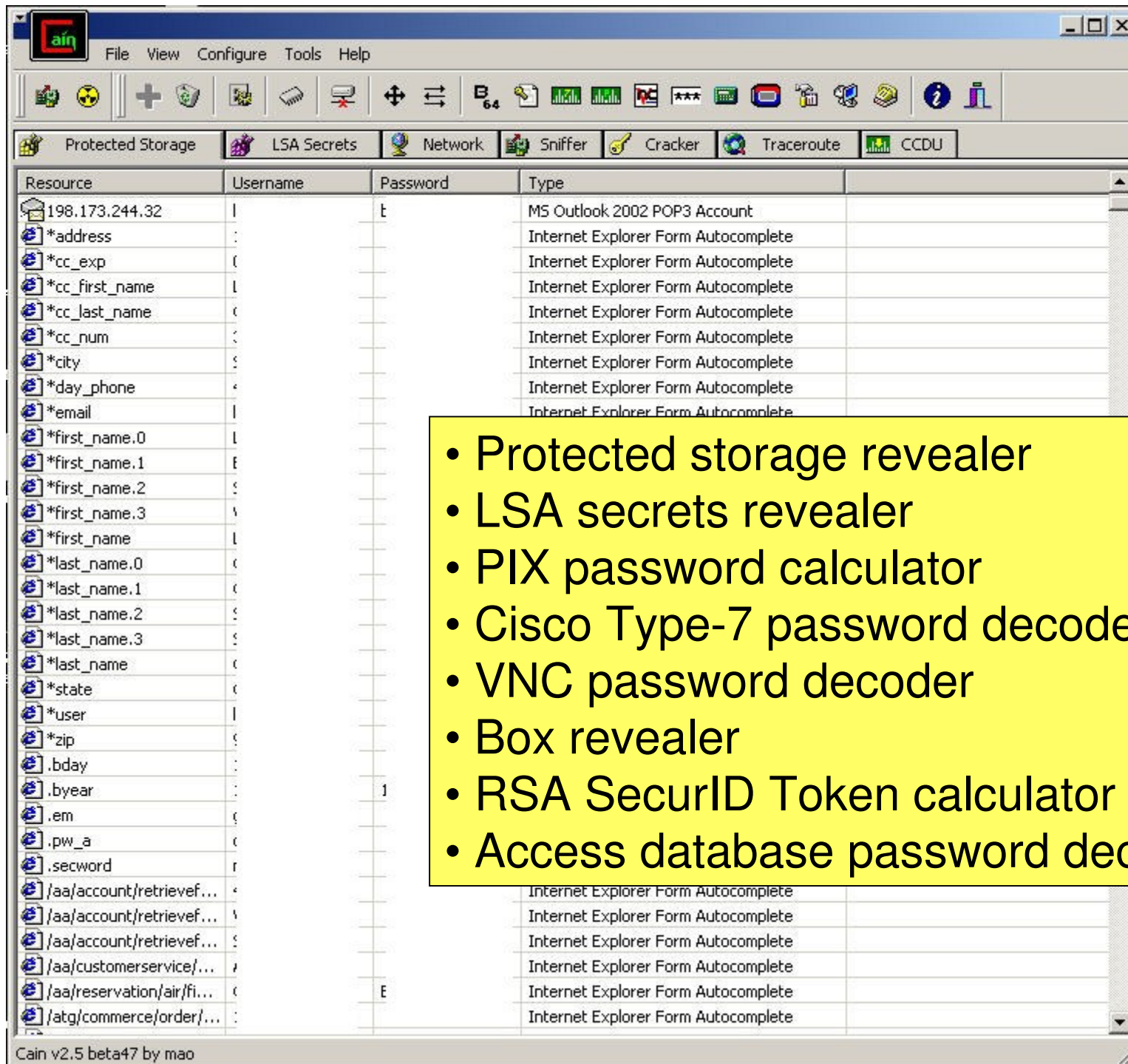
Process	Protocol	Local Address	Remote Address	State
IEXPLORE.EXE:1340	UDP	CHADWICK:1192	...	
IEXPLORE.EXE:1492	UDP	CHADWICK:1082	...	
IEXPLORE.EXE:1752	UDP	CHADWICK:1338	...	
IEXPLORE.EXE:1752	TCP	CHADWICK:1342	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	chadwick:1342	www.packet-level.c...	ESTABLISHE
IEXPLORE.EXE:1752	TCP	CHADWICK:1343	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	CHADWICK:1344	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	CHADWICK:1345	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	CHADWICK:1346	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	chadwick:1343	www.packet-level.c...	ESTABLISHE
IEXPLORE.EXE:1752	TCP	chadwick:1344	www.packet-level.c...	ESTABLISHE
IEXPLORE.EXE:1752	TCP	chadwick:1345	www.packet-level.c...	ESTABLISHE
IEXPLORE.EXE:1752	TCP	chadwick:1346	www.packet-level.c...	ESTABLISHE
IEXPLORE.EXE:1752	TCP	CHADWICK:1359	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	CHADWICK:1360	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	CHADWICK:1361	CHADWICK:0	LISTENING
IEXPLORE.EXE:1752	TCP	CHADWICK:1362	CHADWICK:0	LISTENING
IEXPLORE.EXE:520	UDP	CHADWICK:1133	...	
IEXPLORE.EXE:520	TCP	CHADWICK:1333	CHADWICK:0	LISTENING
IEXPLORE.EXE:520	TCP	chadwick:1333	216.142.16.242:http	ESTABLISHE
lsass.exe:236	UDP	chadwick:isakmp	...	
MSTask.exe:656	TCP	CHADWICK:1025	CHADWICK:0	LISTENING
services.exe:216	UDP	CHADWICK:1026	...	

Cain and Abel

Price: Password cracker; local forensic tool

Link: www.oxid.it

General: All-in-all a very dangerous tool in the wrong hands.



The screenshot shows the main window of Cain v2.5 beta47 by mao. The interface includes a menu bar (File, View, Configure, Tools, Help), a toolbar with various icons, and a tabbed interface. The 'Protected Storage' and 'LSA Secrets' tabs are active. The 'Protected Storage' tab displays a table with columns: Resource, Username, Password, and Type. The table lists various system resources and their associated usernames and passwords, including Outlook accounts, Internet Explorer form autocomplete data, and various system files. The 'LSA Secrets' tab is also visible, showing a similar table structure.

Resource	Username	Password	Type
198.173.244.32			MS Outlook 2002 POP3 Account
*address	:		Internet Explorer Form Autocomplete
*cc_exp	:		Internet Explorer Form Autocomplete
*cc_first_name	:		Internet Explorer Form Autocomplete
*cc_last_name	:		Internet Explorer Form Autocomplete
*cc_num	:		Internet Explorer Form Autocomplete
*city	:		Internet Explorer Form Autocomplete
*day_phone	:		Internet Explorer Form Autocomplete
*email	:		Internet Explorer Form Autocomplete
*first_name.0	:		Internet Explorer Form Autocomplete
*first_name.1	:		Internet Explorer Form Autocomplete
*first_name.2	:		Internet Explorer Form Autocomplete
*first_name.3	:		Internet Explorer Form Autocomplete
*first_name	:		Internet Explorer Form Autocomplete
*last_name.0	:		Internet Explorer Form Autocomplete
*last_name.1	:		Internet Explorer Form Autocomplete
*last_name.2	:		Internet Explorer Form Autocomplete
*last_name.3	:		Internet Explorer Form Autocomplete
*last_name	:		Internet Explorer Form Autocomplete
*state	:		Internet Explorer Form Autocomplete
*user	:		Internet Explorer Form Autocomplete
*zip	:		Internet Explorer Form Autocomplete
.bday	:		Internet Explorer Form Autocomplete
.byear	:		Internet Explorer Form Autocomplete
.em	:		Internet Explorer Form Autocomplete
.pw_a	:		Internet Explorer Form Autocomplete
.secword	:		Internet Explorer Form Autocomplete
/aa/account/retrievef...	:		Internet Explorer Form Autocomplete
/aa/account/retrievef...	:		Internet Explorer Form Autocomplete
/aa/account/retrievef...	:		Internet Explorer Form Autocomplete
/aa/customerservice/...	:		Internet Explorer Form Autocomplete
/aa/reservation/air/fi...	:		Internet Explorer Form Autocomplete
/atg/commerce/order/...	:		Internet Explorer Form Autocomplete

- Protected storage revealer
- LSA secrets revealer
- PIX password calculator
- Cisco Type-7 password decoder
- VNC password decoder
- Box revealer
- RSA SecurID Token calculator
- Access database password decoder

White Glove/Deception Toolkit

Price: White Glove \$100
 Deception Toolkit - Free

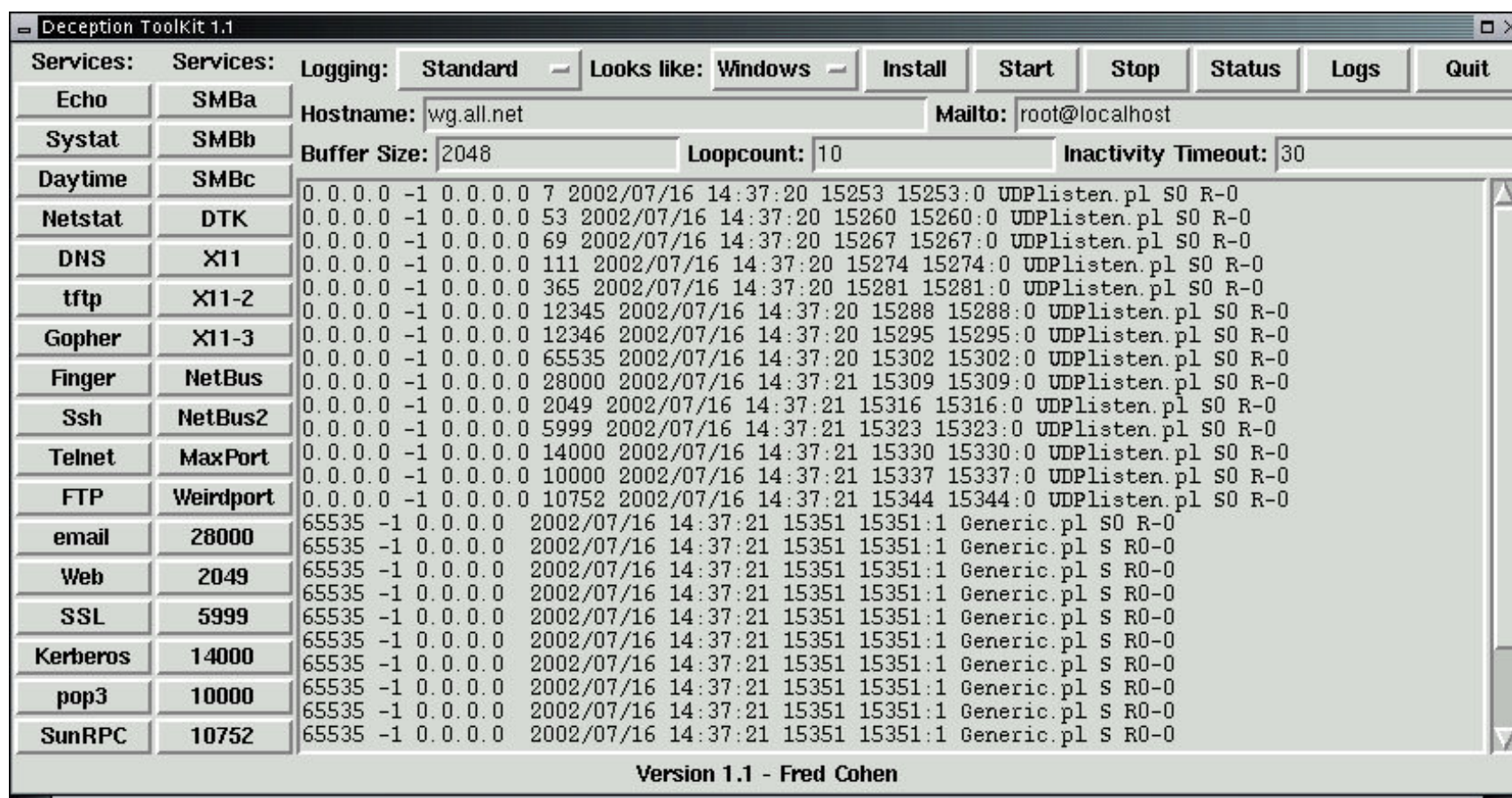
Link: www.all.net

General: Honeypot; interface included if run
 over White Glove (bootable Linux).

White Glove \$/Deception Toolkit

www.all.net

Deception Toolkit (DTK) on White Glove



Snort and IDS Center (Windows)

Price: Free; distributed under the GNU license

Link: www.snort.org and
www.engagesecurity.com

General: IDS and front end. Well-respected; numerous contributors; newly documented.

Snort + IDScenter

www.snort.org



Keyghost Keylogger

Price: US \$89 (home edition)

Link: www.keyghost.com

General: Hardware keylogging device; formats include plug style and full keyboard style.

Keylog a Suspect System



```

Untitled - Notepad
File Edit Format Help
Keyghosts

[C] safe mode

***
KeyGhost II Standard v8.0.0
www.keyghost.com

Menu >
1) Entire log download
2) Section log download
3) wipe log
4) Format memory
5) Options
6) Optimize speed
7) Password change
8) Diagnostics
9) exit

select > 1

- key to stop -

keys so far is 1088 out of 524000 ...

Test
<alt-'F4><alt-'F4><alt-'F4><alt-'F4<ON><PWR><'F7>
<bks><KS><bks>krueg<ON>|Mic
hael...

It really depends on the amount that you buy - you can get a
good deal if you purchase in quantity

```

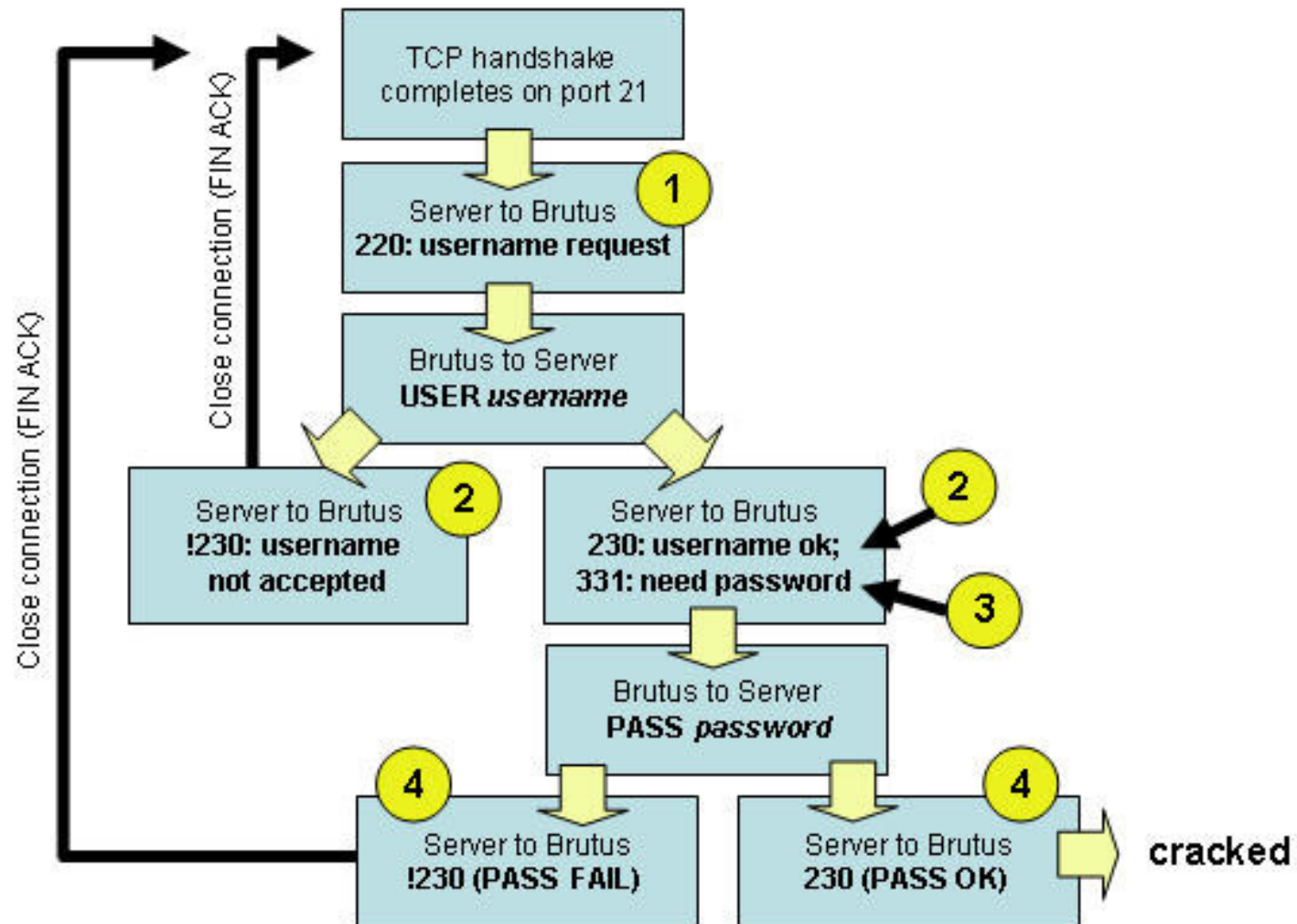

Brutus

Price: Free

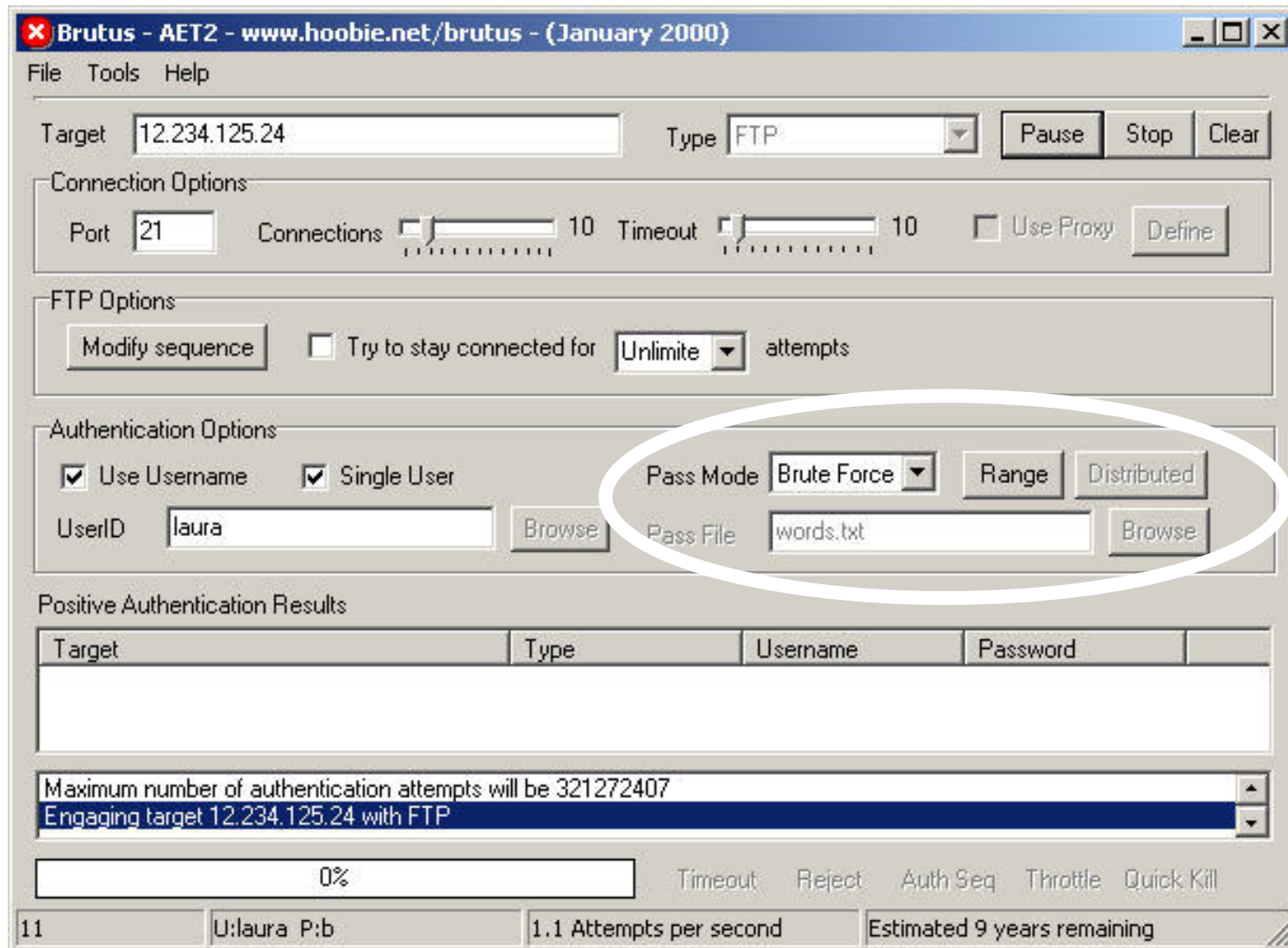
Link: www.hoobie.net

General: Specialized and brute force password cracking tool; contains 800 word password list; username and password process can be customized.

Password Cracking Technique



Perform a Brute Force Password Crack



The screenshot shows the Brutus application window titled "Brutus - AET2 - www.hoobie.net/brutus - (January 2000)". The interface includes a menu bar (File, Tools, Help) and several configuration sections. The "Target" field is set to "12.234.125.24" and the "Type" is set to "FTP". The "Connection Options" section shows "Port" as 21, "Connections" as 10, and "Timeout" as 10. The "FTP Options" section has a "Modify sequence" button and a checkbox for "Try to stay connected for" set to "Unlimited" attempts. The "Authentication Options" section is highlighted with a white oval and contains the following settings: "Use Username" and "Single User" are checked; "Pass Mode" is set to "Brute Force" (a dropdown menu); "Range" and "Distributed" are buttons; "UserID" is set to "laura" with a "Browse" button; and "Pass File" is set to "words.txt" with a "Browse" button. Below these options is a "Positive Authentication Results" table with columns for Target, Type, Username, and Password. At the bottom, a status bar shows "11" in the first column, "U:laura P:b" in the second, "1.1 Attempts per second" in the third, and "Estimated 9 years remaining" in the fourth. A progress bar above the status bar shows "0%".

Target: 12.234.125.24 Type: FTP [Pause] [Stop] [Clear]

Connection Options
Port: 21 Connections: 10 Timeout: 10 [Use Proxy] [Define]

FTP Options
[Modify sequence] [Try to stay connected for] Unlimited attempts

Authentication Options
[x] Use Username [x] Single User
UserID: laura [Browse] Pass Mode: Brute Force [Range] [Distributed]
Pass File: words.txt [Browse]

Positive Authentication Results

Target	Type	Username	Password
Maximum number of authentication attempts will be 321272407 Engaging target 12.234.125.24 with FTP			

0% [Timeout] [Reject] [Auth Seq] [Throttle] [Quick Kill]

11 U:laura P:b 1.1 Attempts per second Estimated 9 years remaining

Aida32

Price: Free

Link: www.aida32.hu

General: System auditing tool; excellent reporting abilities; can be set in stealth mode for remote auditing (not completely undetectable).

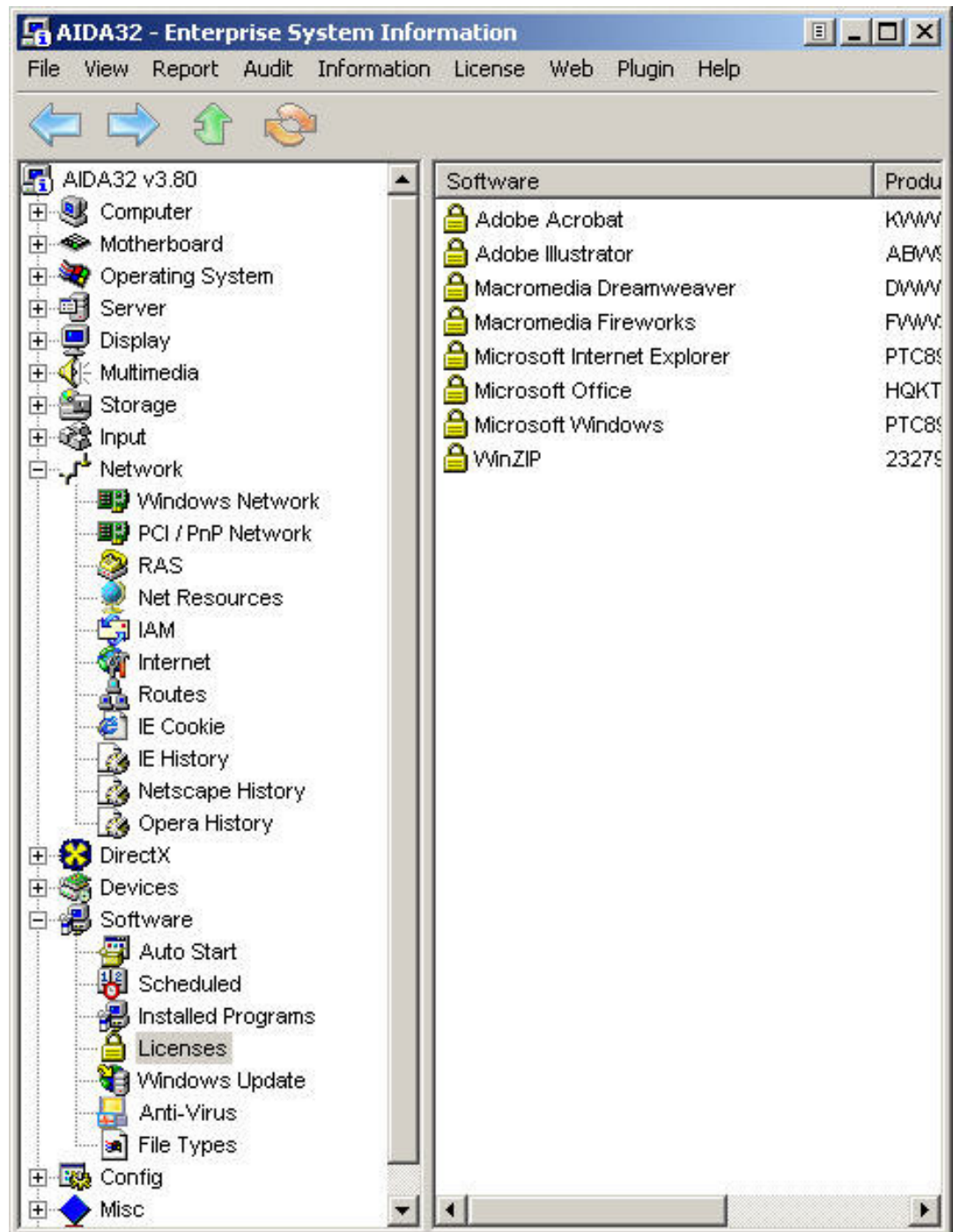
Note: On March 23, 2004, Tamas Miklos announced discontinuation of further development/updates/licensing of Aida32. It still works great, however.

Audit a Suspect System in Stealth Mode

C:\aida32 /hiddenserver /silent

I recommend you set Aida up to audit on a schedule and upload the results instead of leaving the server process running all the time (security issue). See www.aida32.hu for details.

25 August 2004



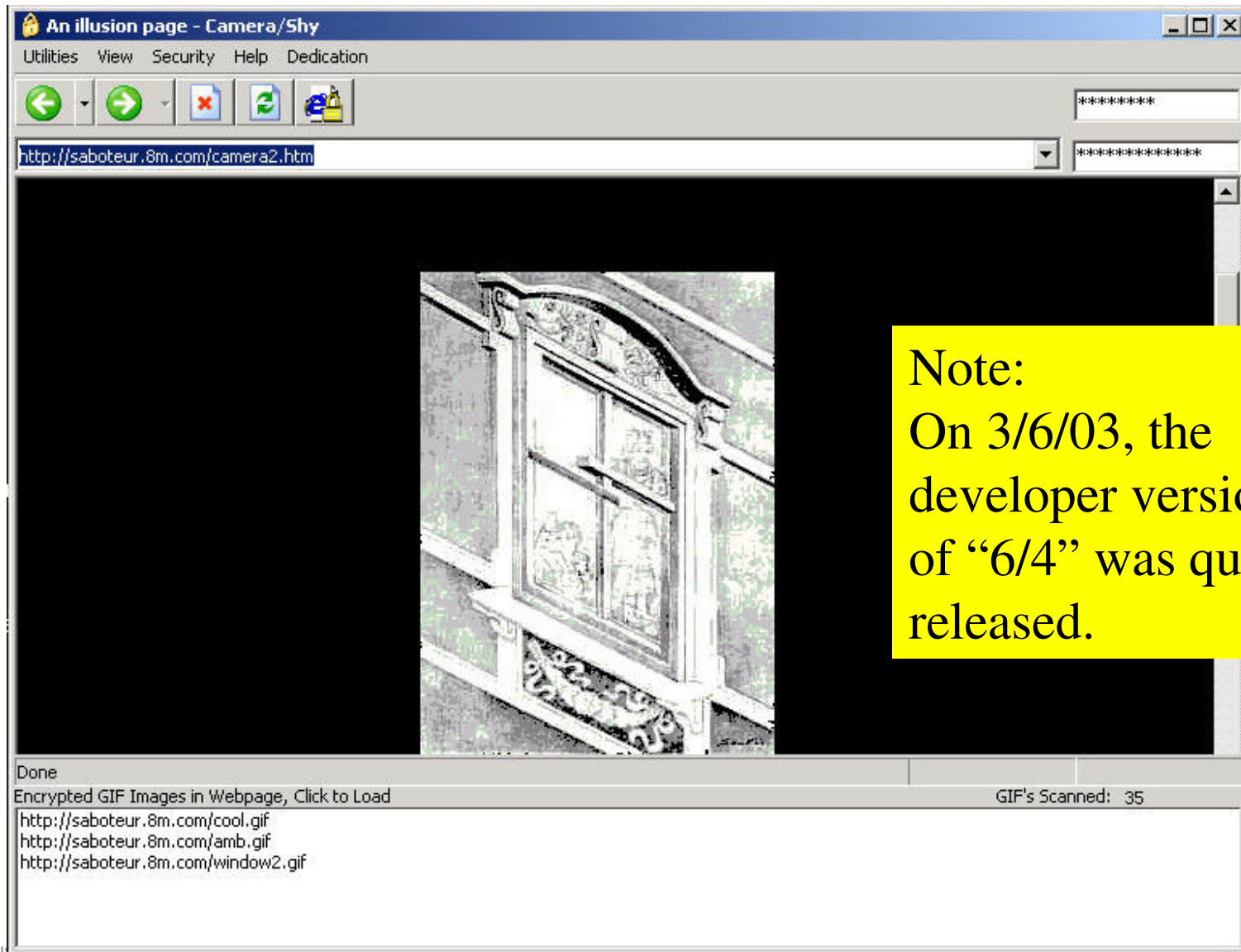
Camera Shy

Price: Free.

Link: hactivismo.com

General: Steganography site browser.

Camera Shy



Invisible Secrets

Price: \$49

Link: www.neobytesolutions.com

General: Steganography tool – includes ability to shred files and remote Internet footprints.

Invisible Secrets

LSB Steganography
Data injection or data replacement

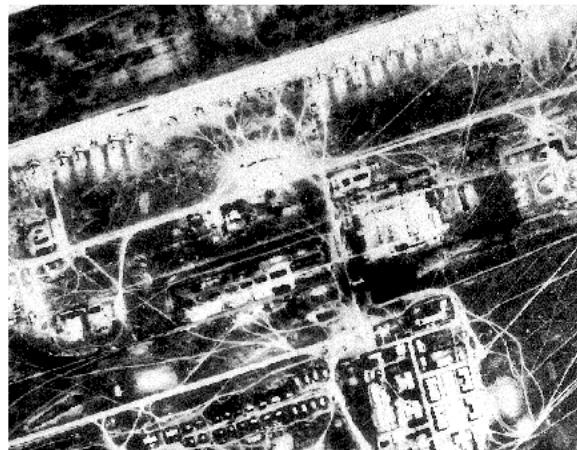
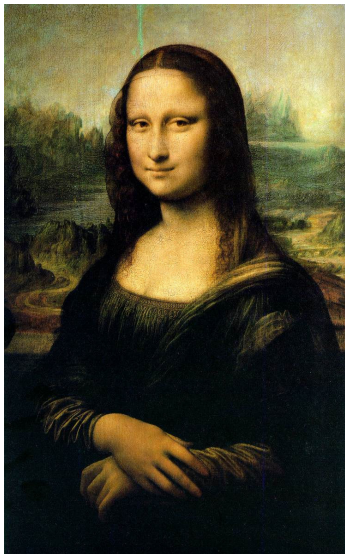
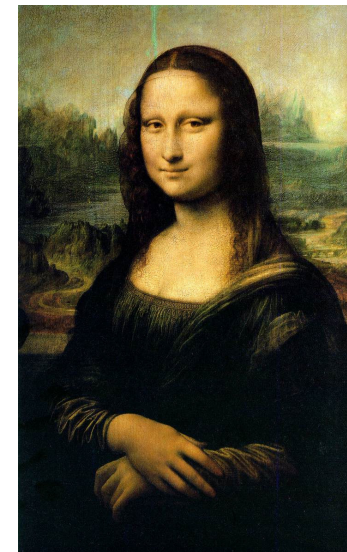


Figure 4: Long-Range Aviation Airfield⁵



Carrier + Secret = Stego Image

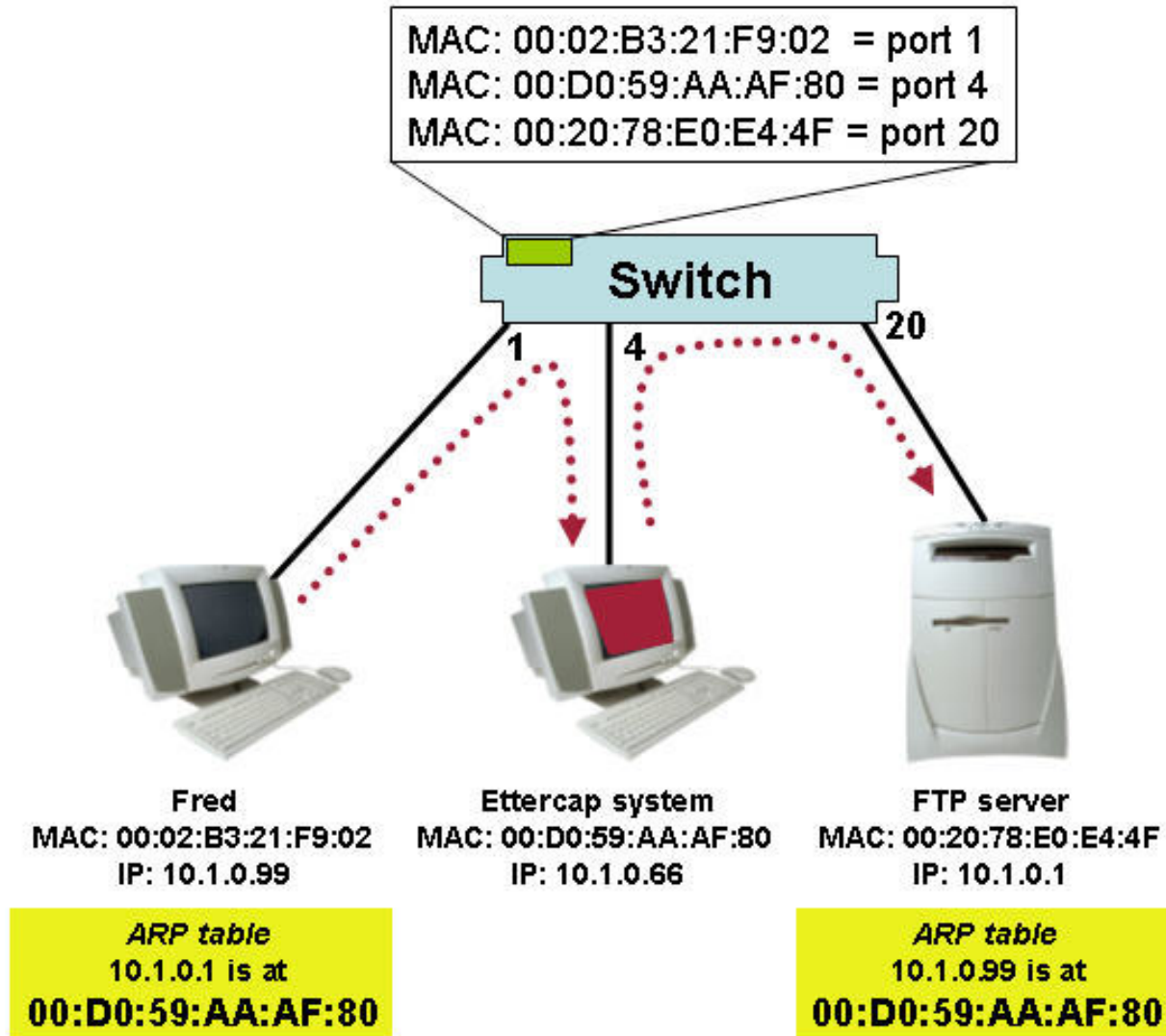
Ettercap

Price: Free

Link: www.sourceforge.net

General: Traffic interceptor using Man-in-the-Middle attack method; catches passwords; can inject data into traffic; can alter data in traffic path.

M-i-M Poisoning (Sniff Off an Unmanageable Switch)



Intercept Traffic and Capture Usernames/Passwords

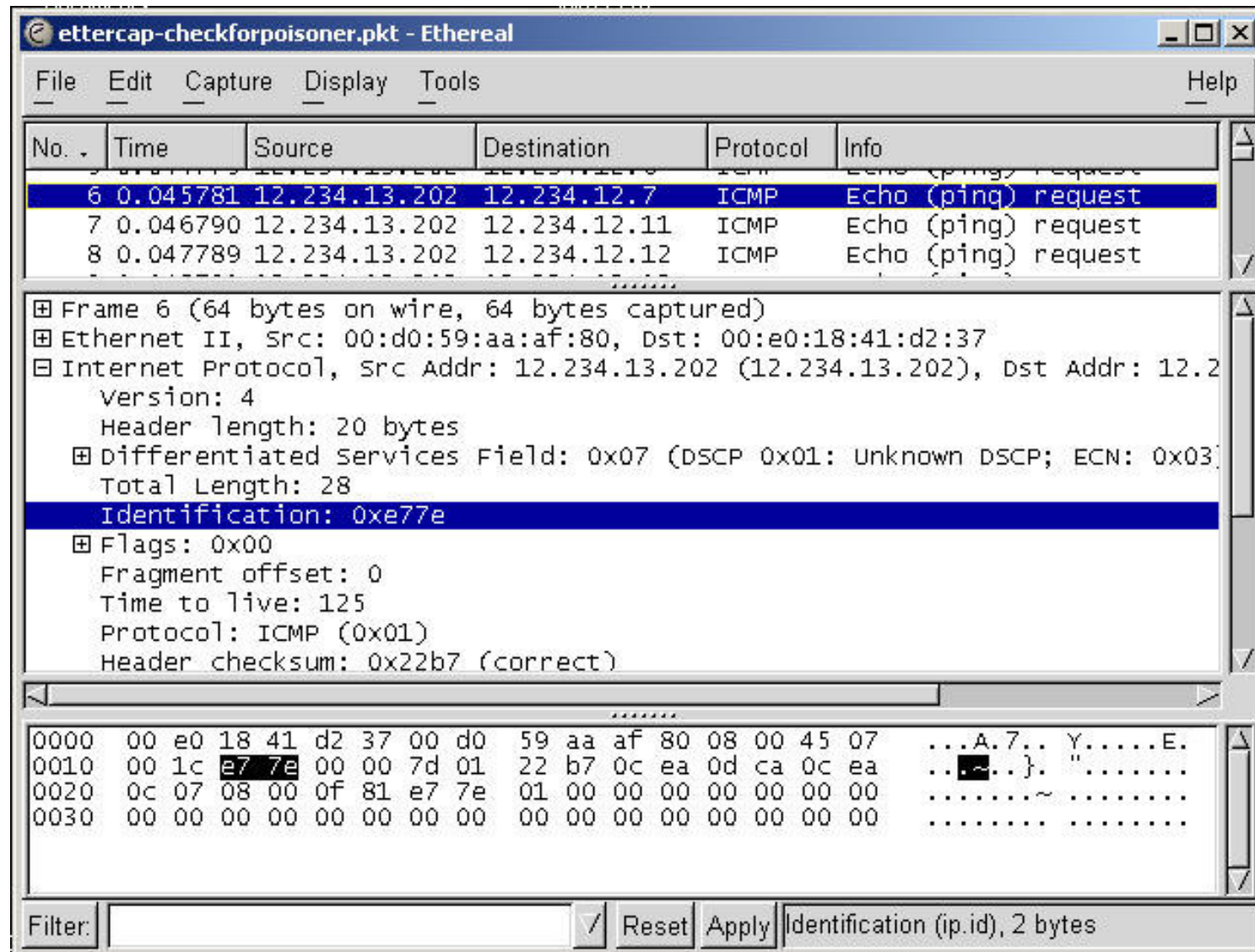


```
ettercap prompt - ettercap
ettercap 0.6.7

367 hosts in this LAN (12.234.13.202 : 255.255.254.0)
1> 12.234.13.202      1> 12.234.13.202
2> 12.234.12.1       2> 12.234.12.1
3> 12.234.12.4       3> 12.234.12.4
4> 12.234.12.6       4> 12.234.12.6
5> 12.234.12.7       5> 12.234.12.7
6> 12.234.12.9       6> 12.234.12.9
7> 12.234.12.10      7> 12.234.12.10
8> 12.234.12.11      8> 12.234.12.11
9> 12.234.12.12      9> 12.234.12.12
10> 12.234.12.13     10> 12.234.12.13
11> 12.234.12.14     11> 12.234.12.14
12> 12.234.12.15     12> 12.234.12.15
13> 12.234.12.16     13> 12.234.12.16
14> 12.234.12.18     14> 12.234.12.18
15> 12.234.12.20     15> 12.234.12.20
16> 12.234.12.21     16> 12.234.12.21
17> 12.234.12.22     17> 12.234.12.22
18> 12.234.12.23     18> 12.234.12.23
19> 12.234.12.24     19> 12.234.12.24
20> 12.234.12.25     20> 12.234.12.25
21> 12.234.12.26     21> 12.234.12.26
22> 12.234.12.27     22> 12.234.12.27
23> 12.234.12.28     23> 12.234.12.28
24> 12.234.12.29     24> 12.234.12.29
25> 12.234.12.30     25> 12.234.12.30
26> 12.234.12.31     26> 12.234.12.31
27> 12.234.12.34     27> 12.234.12.34
28> 12.234.12.35     28> 12.234.12.35
29> 12.234.12.36     29> 12.234.12.36

Your IP: 12.234.13.202 MAC: 00:D0:59:AA:AF:80 Iface: dev0 Link: SWITCH
Host: 12-234-12-14.client.attbi.com (12.234.12.14) : 00:50:18:06:F6:5D
```

Locate M-i-M Ettercap Devices



ettercap-checkforpoisoner.pkt - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
6	0.045781	12.234.13.202	12.234.12.7	ICMP	Echo (ping) request
7	0.046790	12.234.13.202	12.234.12.11	ICMP	Echo (ping) request
8	0.047789	12.234.13.202	12.234.12.12	ICMP	Echo (ping) request

Frame 6 (64 bytes on wire, 64 bytes captured)

Ethernet II, Src: 00:d0:59:aa:af:80, Dst: 00:e0:18:41:d2:37

Internet Protocol, Src Addr: 12.234.13.202 (12.234.13.202), Dst Addr: 12.234.12.7

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x07 (DSCP 0x01: Unknown DSCP; ECN: 0x03)
Total Length: 28
Identification: 0xe77e
Flags: 0x00
Fragment offset: 0
Time to live: 125
Protocol: ICMP (0x01)
Header checksum: 0x22b7 (correct)

```

0000  00 e0 18 41 d2 37 00 d0 59 aa af 80 08 00 45 07  ...A.7..Y....E.
0010  00 1c e7 7e 00 00 7d 01 22 b7 0c ea 0d ca 0c ea  ..~}. ".....
0020  0c 07 08 00 0f 81 e7 7e 01 00 00 00 00 00 00 00  .....~.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```

Filter: [] Reset Apply Identification (ip.id), 2 bytes



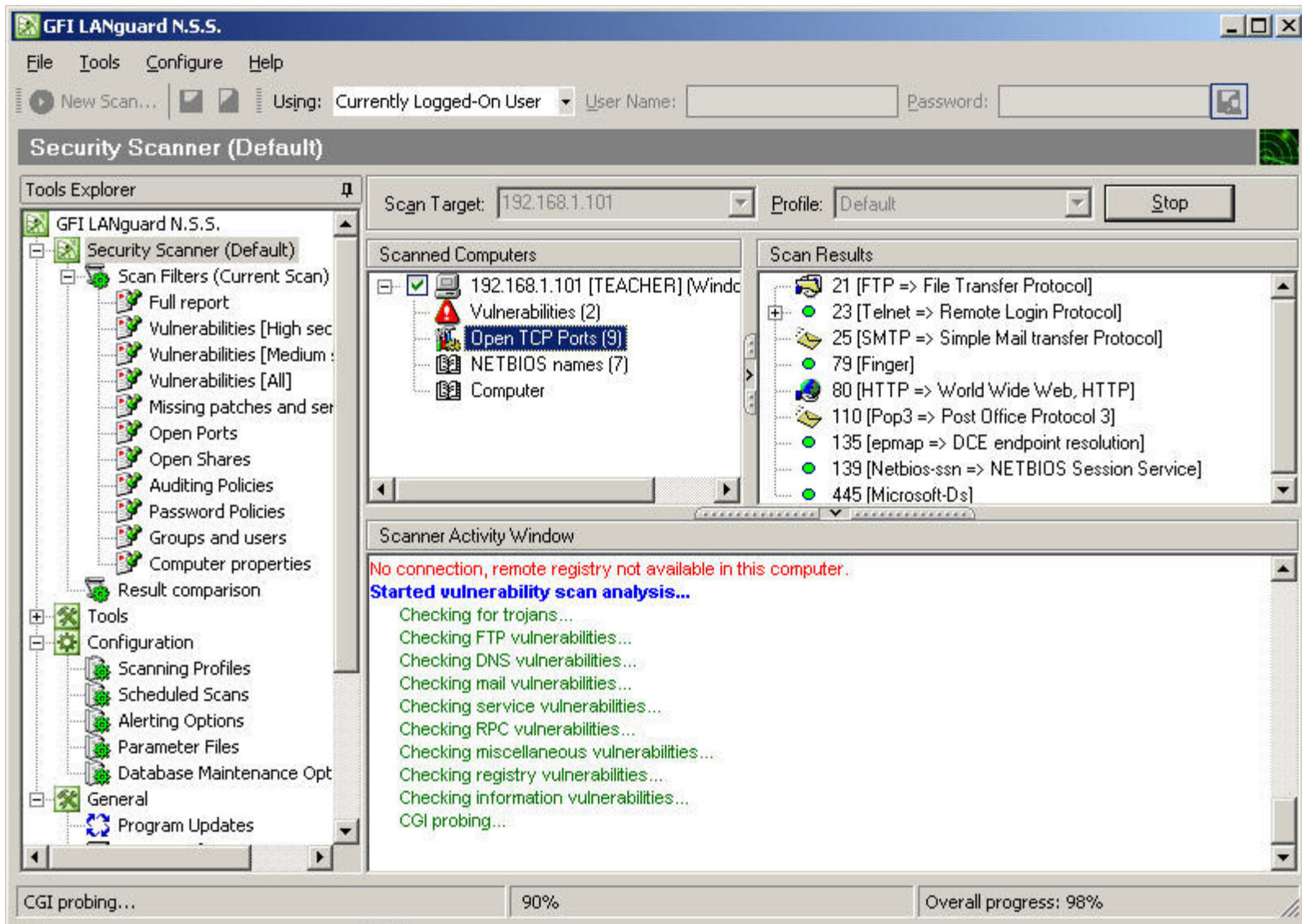
LANguard Network Scanner

Price: US \$295 and up

Link: www.gfi.com

General: Vulnerability scanner; OS fingerprinting; port scanning; locate open shares; locate cgi script vulnerabilities; patch/hotfix detection.

Locate Open Ports, Shares and Unpatched Systems on the Network



VisualRoute

Price: US \$49.95 and up

Link: www.visualware.com


General: Visual representation of traceroute operation; includes whois functionality.

Trace Back Suspicious Email

Microsoft

All Products | Support | Search | Microsoft.com Guide

Microsoft Home



Microsoft Customer

this is the latest version of security update, the "September 2003, Cumulative Patch" update which eliminates all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express. Install now to protect your computer from these vulnerabilities, the most serious of which could allow an malicious user to run executable on your system. This update includes the functionality of all previously released patches.

? System requirements	Windows 95/98/Me/2000/NT/XP
? This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
? Recommendation	Customers should install the patch at the earliest opportunity.
? How to install	Run attached file. Choose Yes on displayed dialog box.
? How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the [Microsoft Technical Support](#) web site. For security-related information about Microsoft products, please visit the [Microsoft Security Advisor](#) web site, or [Contact Us](#).

Thank you for using Microsoft products.

Please do not reply to this message. It was sent from an unmonitored e-mail address and we are unable to respond to any replies.

The names of the actual companies and products mentioned herein are the trademarks of their respective owners.

Contact Us | Legal | TRUSTe

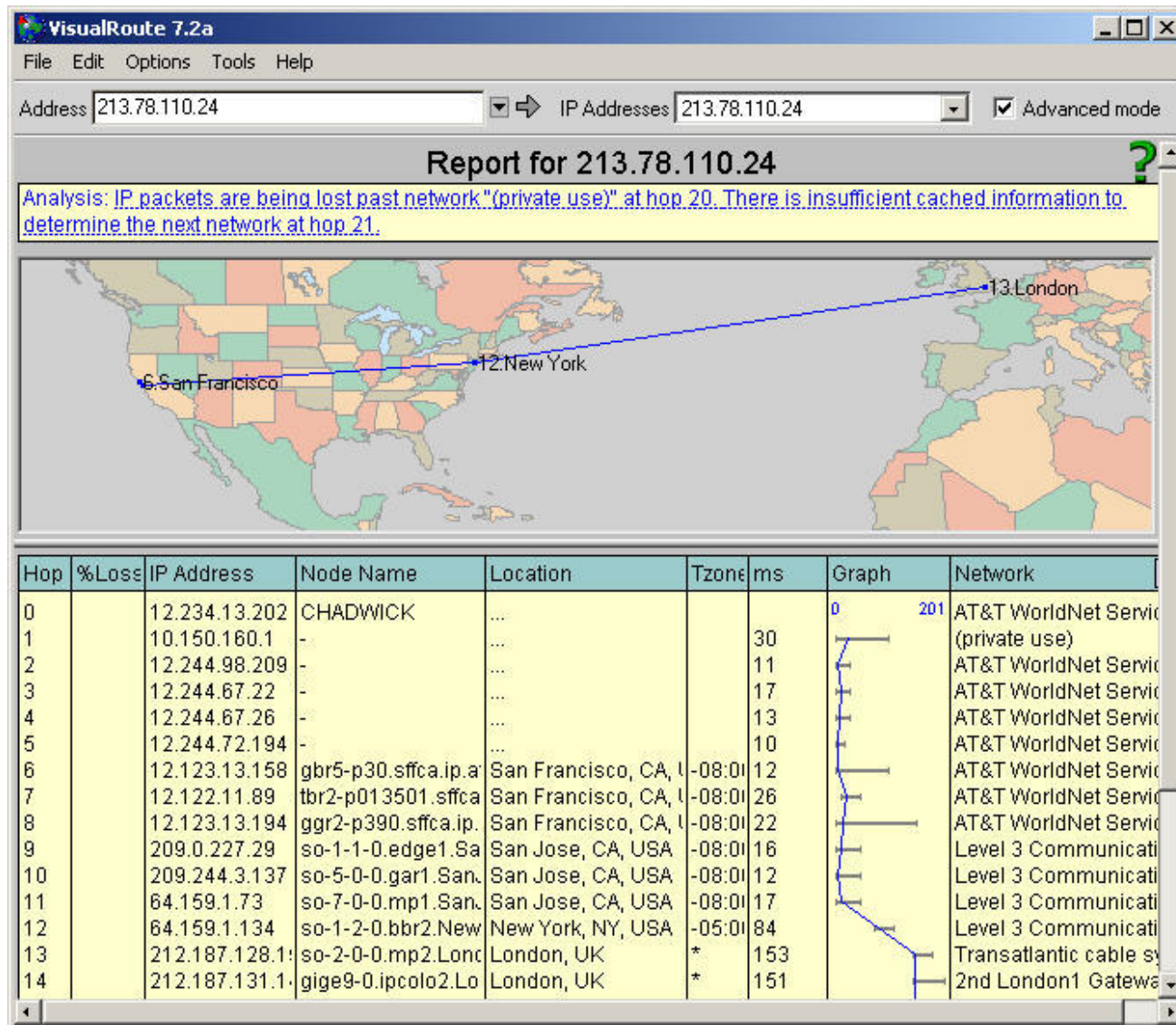
©2003 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Privacy Statement](#) | [Accessibility](#)

Examining the Email Header

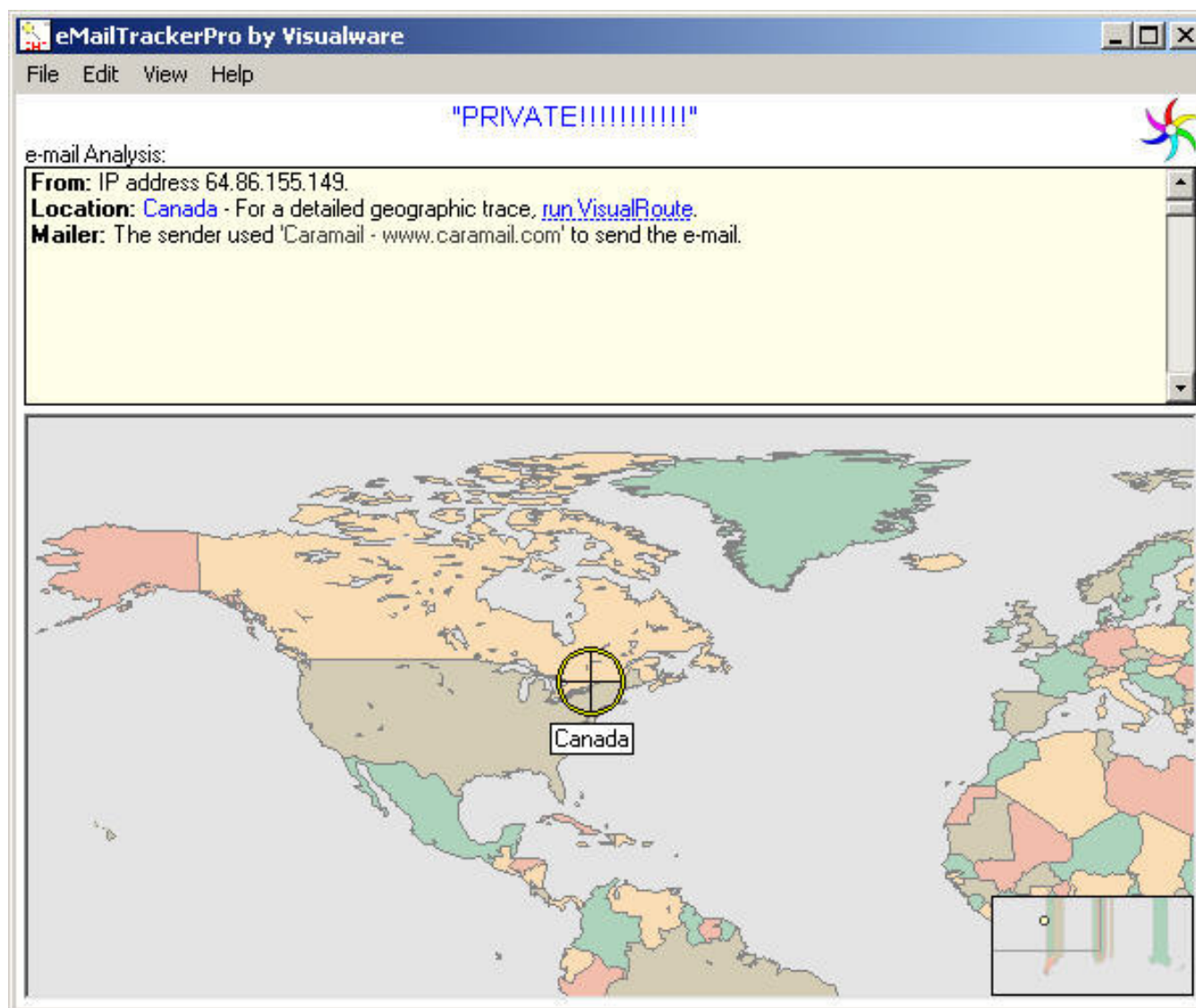
Last “Received” is closest to sender.

```
Received: from msgdirector2.onetel.net.uk (212.67.96.149)
        by mail11a.verio-web.com (RS ver 1.0.86vs) with SMTP id 1-0875884261
        for <lchappell@packet-level.com>; Fri, 19 Sep 2003 02:51:01 -0400 (EDT)
Received: from cpcagpya (213-78-110-24.friaco.onetel.net.uk [213.78.110.24])
by msgdirector2.onetel.net.uk (Mirapoint Messaging Server MOS 3.3.6-GR)
with SMTP id AJC60345;
Fri, 19 Sep 2003 07:43:43 +0100 (BST)
Date: Fri, 19 Sep 2003 07:43:42 +0100 (BST)
Message-Id: <200309190643.AJC60345@msgdirector2.onetel.net.uk>
FROM: "Security Department" <vkrmgchc_selgh@cqqi.microsoft.com>
TO: "Commercial Customer" <customer@cqqi.microsoft.com>
SUBJECT: Net Security Upgrade
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="qqcfwvbvhdttrdf"
X-Loop-Detect:1
Status:
```

Visual Trace Back



eMailTracker Pro



HTTP Sniffer

Price: US \$29.95

Link: www.iffetech.com

General: HTTP traffic sniffer; graphic reassembler

View HTTP Graphic Transfers

HttpDetect (EffeTech HTTP Sniffer) - Unregistered Version

File View Sniffer Help

No.	Time	Client(IP:PORT)	Server(IP:PORT)	URL	File Length	Status
173	Sep 21...	12.234.13.202 :1526	images.godaddy.com :80	/assets/home/img_nav_grey.gif	103	FIN, 200
174	Sep 21...	12.234.13.202 :1528	images.godaddy.com :80	/assets/home/img_nav_grey_on.gif	102	FIN, 200
175	Sep 21...	12.234.13.202 :1525	images.godaddy.com :80	//assets/spc_trans.gif	43	FIN, 200
176	Sep 21...	12.234.13.202 :1527	images.godaddy.com :80	/assets/home/img_arrow_orange.gif	125	FIN, 200
177	Sep 21...	12.234.13.202 :1526	images.godaddy.com :80	/assets/spc_ff6600.gif	799	FIN, 200
178	Sep 21...	12.234.13.202 :1528	images.godaddy.com :80	/assets/home/img_hpgirl.gif	5842	FIN, 200
179	Sep 21...	12.234.13.202 :1525	images.godaddy.com :80	/assets/home		
180	Sep 21...	12.234.13.202 :1527	images.godaddy.com :80	/assets/home		
181	Sep 21...	12.234.13.202 :1526	images.godaddy.com :80	/assets/home		
182	Sep 21...	12.234.13.202 :1528	images.godaddy.com :80	/assets/home		
183	Sep 21...	12.234.13.202 :1525	images.godaddy.com :80	/assets/home		
184	Sep 21...	12.234.13.202 :1528	images.godaddy.com :80	/assets/home		
185	Sep 21...	12.234.13.202 :1526	images.godaddy.com :80	/assets/home		

HTTP Request Header

```
GET /assets/home/img_hpgirl_wedge.gif
HTTP/1.1
Accept: */*
Referer: http://www.godaddy.com/gdshop/default.asp?e=com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Host: images.godaddy.com
Connection: Keep-Alive
Cookie: SITESERVER=ID=cfe50c3a5cf993849edadbd420b32c3
```

HTTP Res

HTTP/1.1
Server: :
Date: Su
Content-
Accept-R
Last-Mod
ETag: "f
Content-


HTTP Communications Detail

Detail Content Text View Packets Commands

URL: 64.89.23.131/images/index_18.jpg

Local: C:\WINNT\temp\1064184763_750825_index_18.jpg

Refresh



OK Cancel Apply

Buffer: 9% URLs: 195 Packets: 1903

NetStumbler/MiniStumbler

Price: Free

Link: www.netstumbler.com

General: Wireless access point locator;
denotes whether WEP is enabled;
displays signal-to-noise ratio

Locate Rogue Wireless Access Points

City 2.ns1

Channels	MAC	SSID	Name	Ch...	Vendor	Type	WEP	SN...	Si...
1	00022D05BD...	Network		7	Agere...	AP			-87
3	00045AFA7F...	mitsui		6	Linksys	AP	Yes		-86
4	00045A0E98...	linksys		6	Linksys	AP			-90
	00022D2FAAE								
	00045A0F0D...	iannucci		6	Linksys	AP	Yes		-76
	00601D218A...	sas airport		4	Agere...	AP			-87
	00022D2FAA...	TheBullNet2D		4	Agere...	AP			-77
	00045ACFF4...	linksys		6	Linksys	AP			-84
	00022D0D71...	0ab100		1	Agere...	AP	Yes		-86
	00501806C16E	default		6	Advan...	AP			-87
	00045AD168...	home		6	Linksys	AP	Yes		-79
	008037514D53	SFD		3		AP	Yes		-66
	00045ADBB...	0B1AD0Be		10	Linksys	AP			-84
	0030AB0AD4...	Wireless		6	Delta (...)	AP			-87
	00045AFA49...	linksys		6	Linksys	AP			-87
	00045AD226...	Hamp		6	Linksys	AP			-89
	00045ACC42...	TBNMDU1		11	Linksys	AP			-97
	00022D2FAA...	UTSAD	DDC	1	Agere...	AP			-77

SSIDs

- 0ab100
- 0B1AD0Be
- 0d8004
- AirReality

Stealth Surfer

Price: US \$29.95

Link: www.stealthsurfer.biz

General: Anonymous surfing tool; also includes some added features such as cookie erasing and pop-up blocking.



AirMagnet

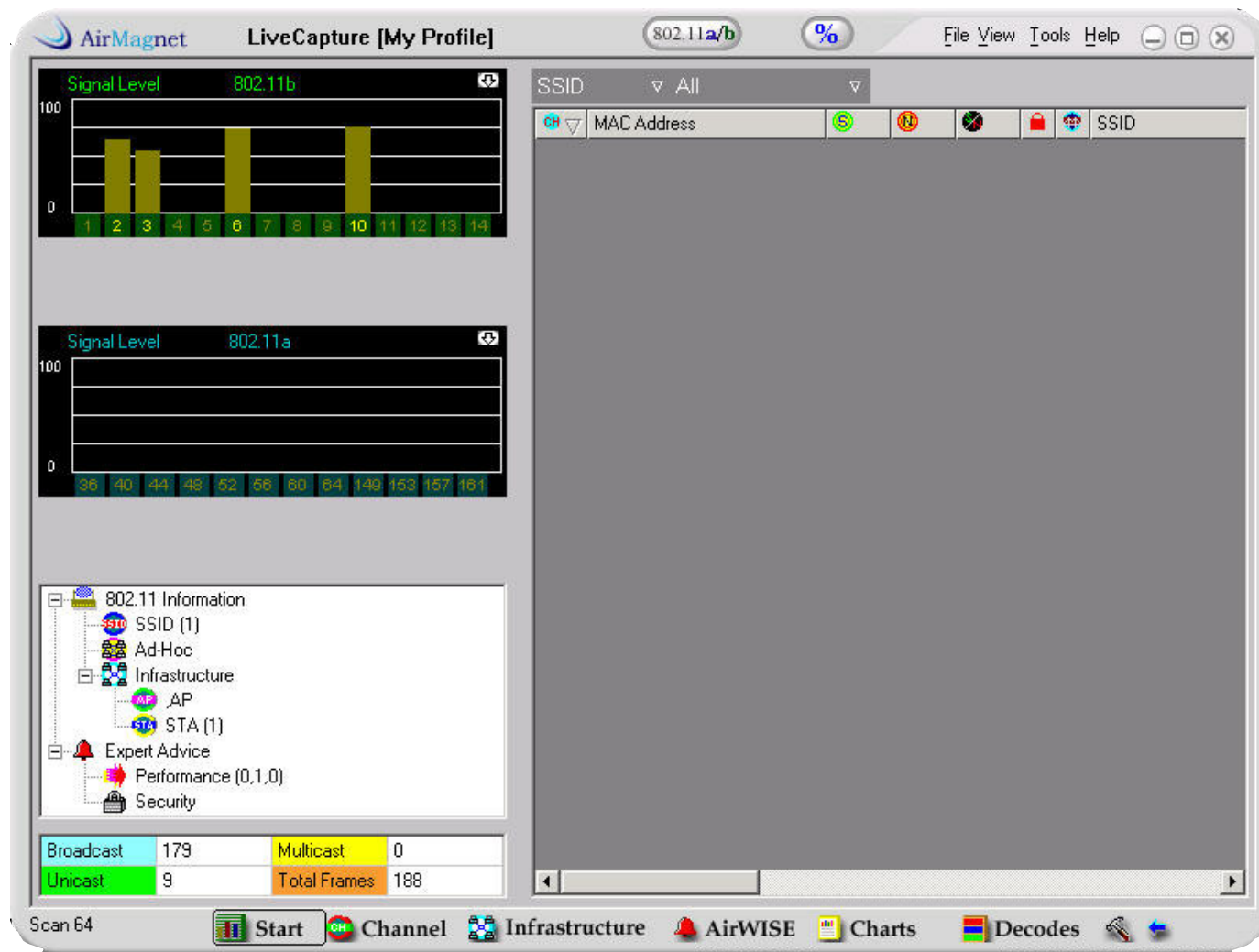
Price: Varies by product type

Link: www.airmagnet.com

General: Wireless network analyzer; site surveyor; security analyzer.

KEY TOOL FOR WIRELESS NETWORKS!

AirMagnet Wireless Analyzer



GPS + Antennas at www.fab-corp.com

pigtails



amplifiers



antennas



Conclusion

- Play with tools on the Laura's Lab Kit.
- Join the Protocol Analysis Institute mailing list online at www.packet-level.com.
- Work with the tools listed (with appropriate authorization, of course).
- Send me your tools list!