

# Management, Troubleshooting and Security Tools That Every IT Professional Should Own

**Laura Chappell**

**Sr. Protocol/Security Analyst**  
**Protocol Analysis Institute, LLC**  
**[www.packet-level.com](http://www.packet-level.com)**

# Warning!



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

## Tools Covered in this Session

- **Ethereal**
- **Hex Workshop**
- **NetScanTools Pro**
- **Packet Builder**
- **Visual Route**
- **Secure USB Drive**

- **TCPView**
- **Cain and Abel**
- **Hurricane Search**
- **Aida32 Auditor  
(Everest)**
- **LANGuard Network  
Scanner**

# Ethereal



**Price:** Free; distributed under the GNU license



**Link:** [www.ethereal.com](http://www.ethereal.com)



**General:** Protocol analyzer; requires winpcap to run over W32 platform (available at [winpcap.polito.it](http://winpcap.polito.it))

# Locate Network Faults, Clear Text 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 05 00 0a 43 01 01 00 09 03 5a 20 4a 33 43  che..Coo 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 session=
02b0  78 47 66 51 35 53 30 36 77 77 45 42 41 41 45 42  xGFQ5S06 wwEBAEB
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  =novell1& 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**

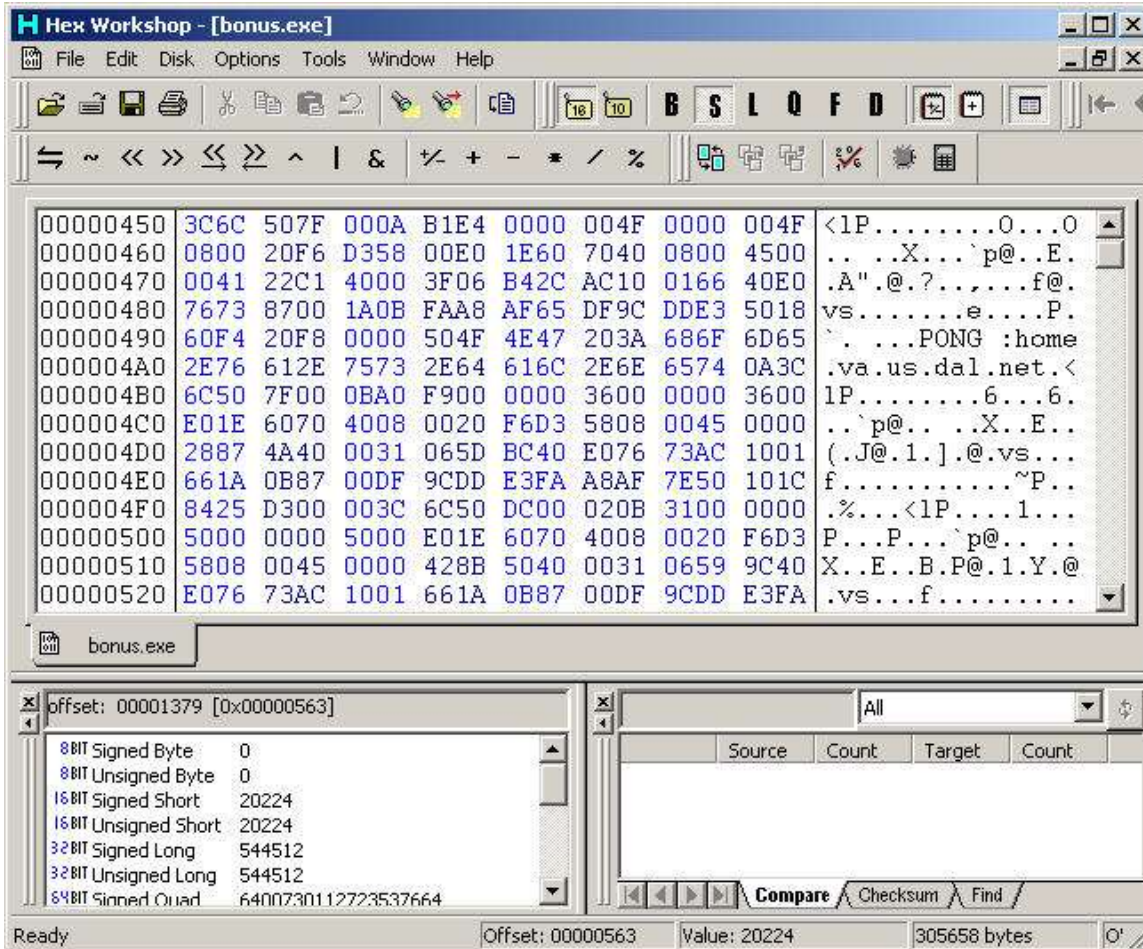


**Link: [www.bpsoft.com](http://www.bpsoft.com)**



**General: General hex editor; includes Base Converter applet**

# Open Suspect Files



Hex Workshop - [bonus.exe]

File Edit Disk Options Tools Window Help

B S L Q F D

```
00000450 3C6C 507F 000A B1E4 0000 004F 0000 004F <1P.....0...0
00000460 0800 20F6 D358 00E0 1E60 7040 0800 4500 .. .X...`p@..E.
00000470 0041 22C1 4000 3F06 B42C AC10 0166 40E0 .A".@.?.....f@.
00000480 7673 8700 1A0B FAA8 AF65 DF9C DDE3 5018 vs.....e....P.
00000490 60F4 20F8 0000 504F 4E47 203A 686F 6D65 ` . ...PONG :home
000004A0 2E76 612E 7573 2E64 616C 2E6E 6574 0A3C .va.us.dal.net.<
000004B0 6C50 7F00 0BA0 F900 0000 3600 0000 3600 1P.....6...6.
000004C0 E01E 6070 4008 0020 F6D3 5808 0045 0000 ..`p@.. .X..E..
000004D0 2887 4A40 0031 065D BC40 E076 73AC 1001 (.J@.1.]@.vs...
000004E0 661A 0B87 00DF 9CDD E3FA A8AF 7E50 101C f.....~P..
000004F0 8425 D300 003C 6C50 DC00 020B 3100 0000 .%...<1P....1...
00000500 5000 0000 5000 E01E 6070 4008 0020 F6D3 P...P...`p@.. .
00000510 5808 0045 0000 428B 5040 0031 0659 9C40 X..E..B.P@.1.Y.@
00000520 E076 73AC 1001 661A 0B87 00DF 9CDD E3FA .vs...f.....
```

bonus.exe

offset: 00001379 [0x00000563]

8BIT Signed Byte	0
8BIT Unsigned Byte	0
16BIT Signed Short	20224
16BIT Unsigned Short	20224
32BIT Signed Long	544512
32BIT Unsigned Long	544512
64BIT Signed Quad	6400730112723537664

Source	Count	Target	Count
--------	-------	--------	-------

Compare Checksum Find

Ready Offset: 00000563 Value: 20224 305658 bytes

# NetScanTools Pro



**Price: US \$199.00**



**Link: [www.netscantools.com](http://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
  - RFC RFC 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

Ready.

Auto-Refresh Endpoint List

Refresh Interval: 1 sec ————— 10 sec

Enable Double Click TCP Disconnects

**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)
spankiller.exe:1228	TCP	0.0.0.0:1027 (unknown)
spankiller.exe:1228	TCP	0.0.0.0:1029 (unknown)
spankiller.exe:1228	TCP	0.0.0.0:1035 (unknown)
spankiller.exe:1228	TCP	0.0.0.0:1041 (unknown)
spankiller.exe:1228	TCP	0.0.0.0:1047 (unknown)

# Packet Builder



**Price:** Free

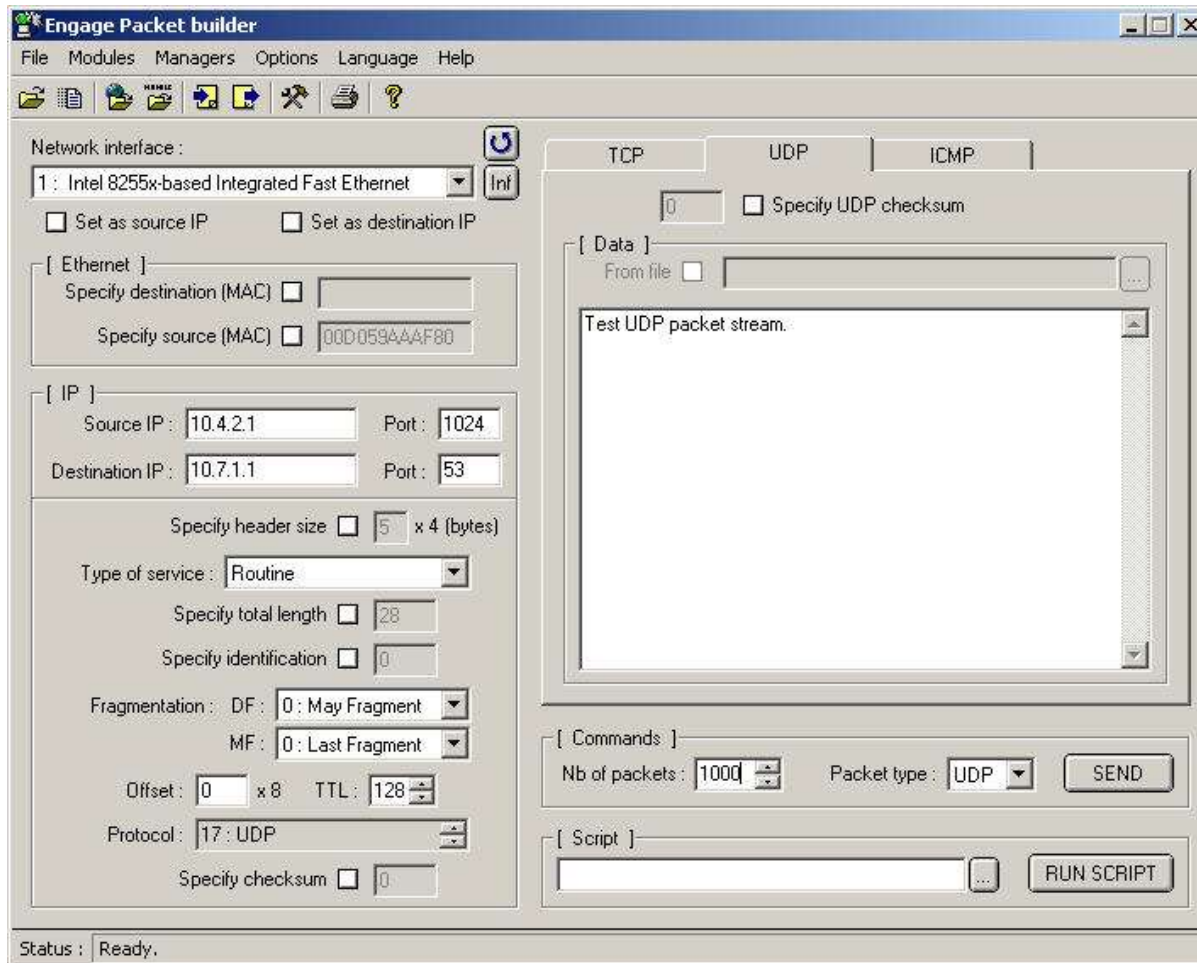


**Link:** [www.engagesecurity.com](http://www.engagesecurity.com)



**General:** Runs on winpcap; download .rsb scripts (Packet Builder was formerly called "Rafale")

# Test Flood Vulnerabilities



# Packet Builder



**Price:** Free



**Link:** [www.engagesecurity.com](http://www.engagesecurity.com)



**General:** Runs on winpcap; download .rsb scripts (Packet Builder was formerly called "Rafale")

# Secure USB Drive



**Price: US \$89-749**



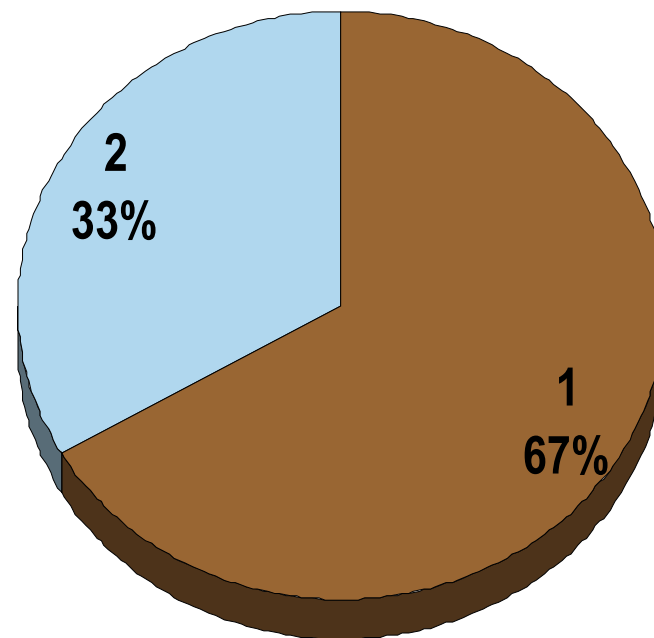
**Link: Various**



# Do you own a USB drive?

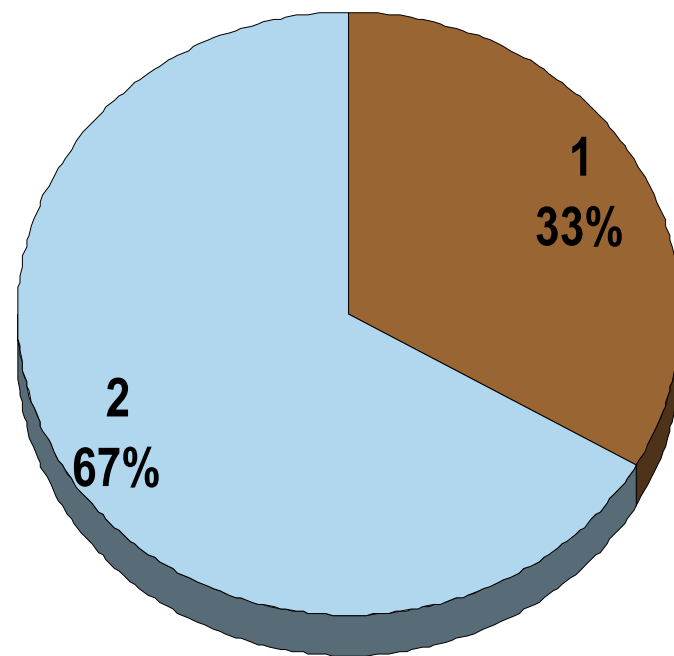
**1. Yes**

**2. No**

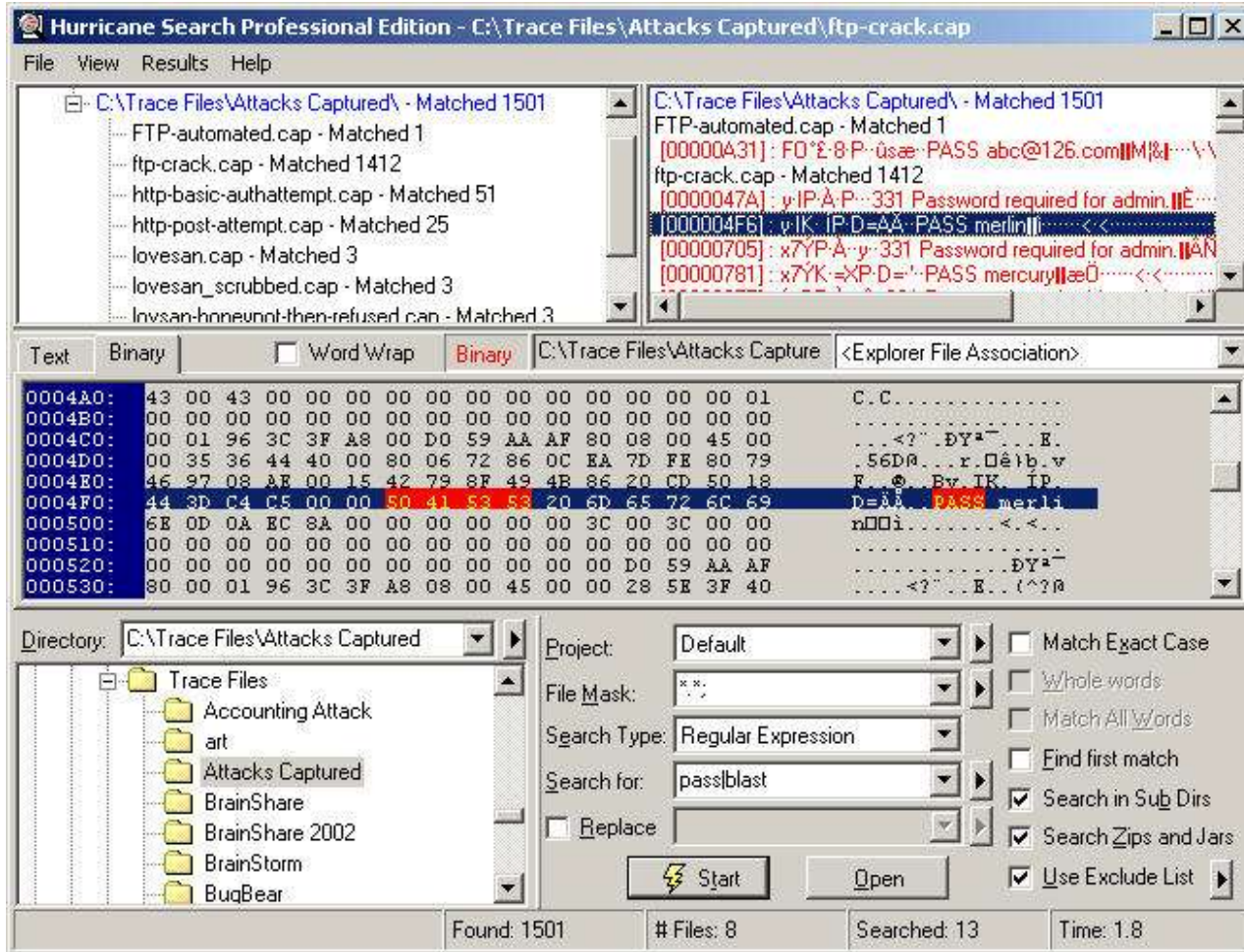


# Have you ever stored confidential information on that drive?

1. Yes
2. No



## Find Evidence on a Hard Drive



The screenshot displays the Hurricane Search Professional Edition interface. The main window shows search results for the file 'ftp-crack.cap' located in 'C:\Trace Files\Attacks Captured\'. The search criteria are 'passblast' using a Regular Expression search type. The results pane shows a list of files with their match counts, and the main text area displays the raw data from the selected file. A specific line of data is highlighted in blue, showing a password attempt: 'D=AA PASS merli'. The status bar at the bottom indicates that 1501 files were found, 8 files were searched, and the search took 1.8 seconds.

Address	Hex Data	ASCII Data
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	..56D...r.Dé)b.v
0004E0:	46 97 08 AF 00 15 42 79 8F 49 4B 86 20 CD 50 18	E. @. By 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 3C 00 3C 00 00	n00i.....<.<..
000510:	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 D0 59 AA AF	.....DY*~
000530:	80 00 01 96 3C 3F A8 08 00 45 00 00 28 5E 3F 40	....<? .E. (^?@



# TCPView



**Price: Free**

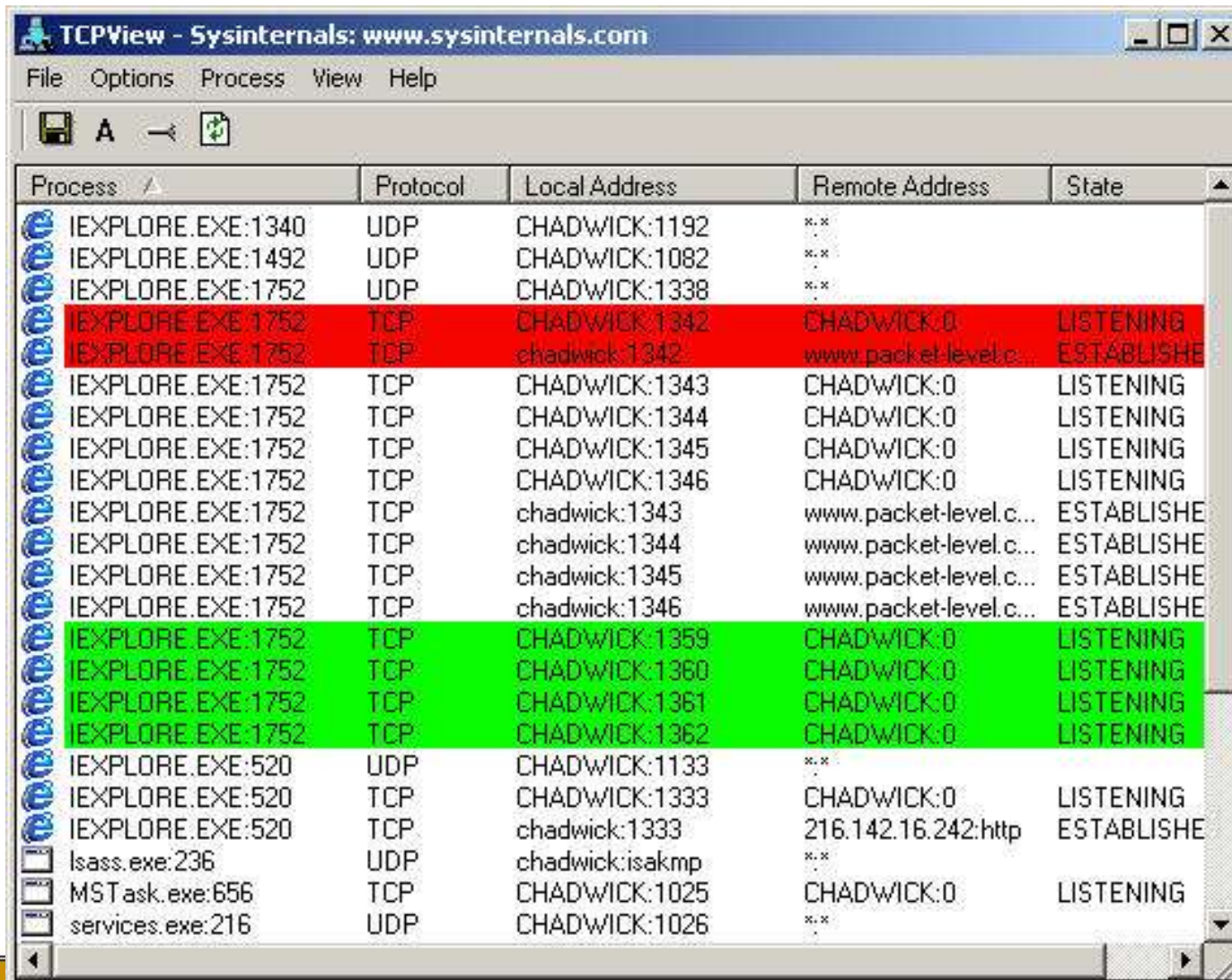


**Link: [www.sysinternals.com](http://www.sysinternals.com)**



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

# Log Active Connections/Endpoints



The screenshot shows the TCPView application window from Sysinternals. The window title is "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Options", "Process", "View", and "Help". The toolbar contains icons for file operations and a search icon. The main display is a table with the following columns: "Process", "Protocol", "Local Address", "Remote Address", and "State".

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 & Abel



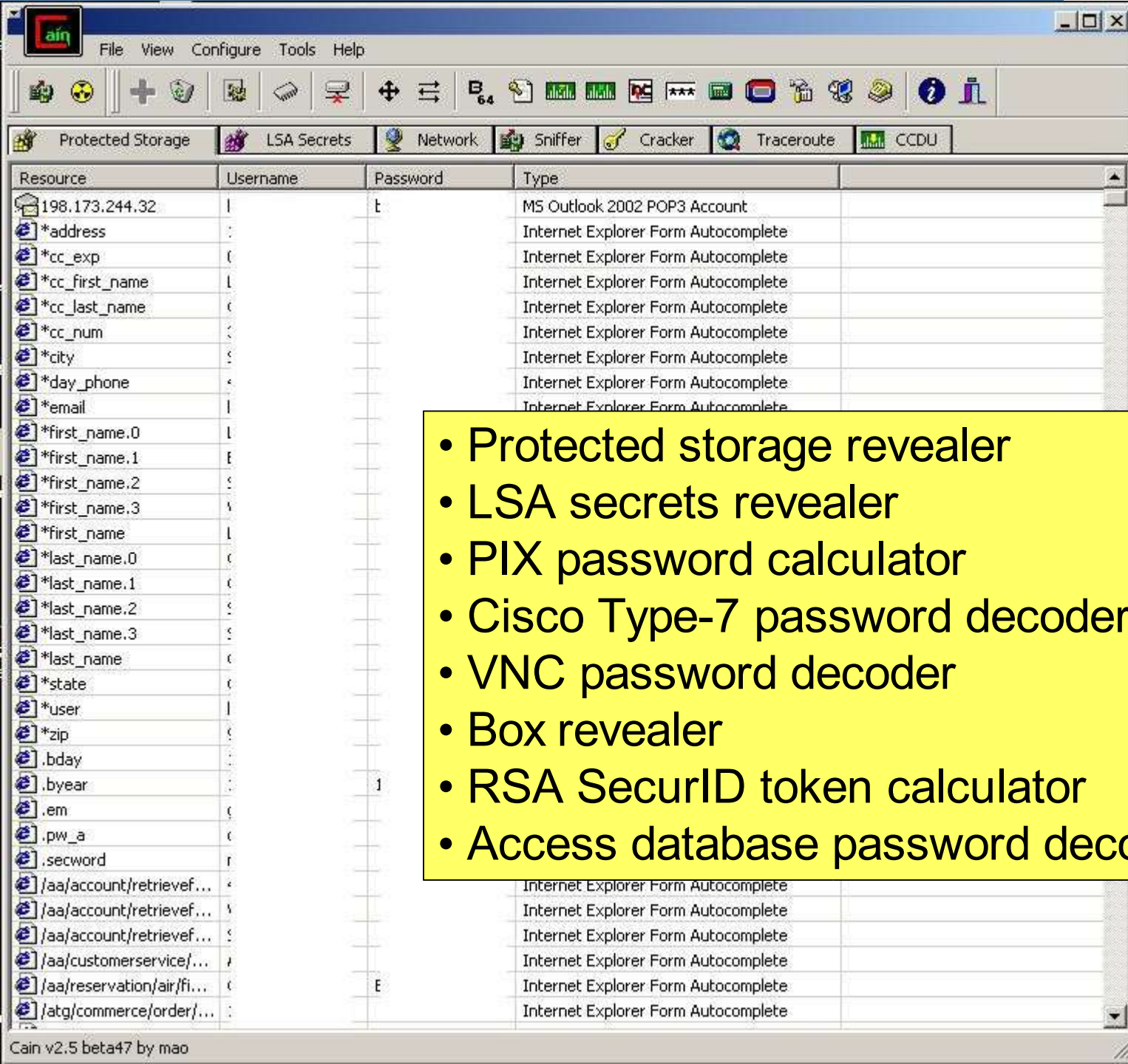
**Price: Free**



**Link: [www.oxid.id](http://www.oxid.id)**



**General: Read and clean protected storage – other wonderful tricks**



- 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

# Aida32/Everest



**Price: Free**



**Link: [www.lavalys.com](http://www.lavalys.com)**



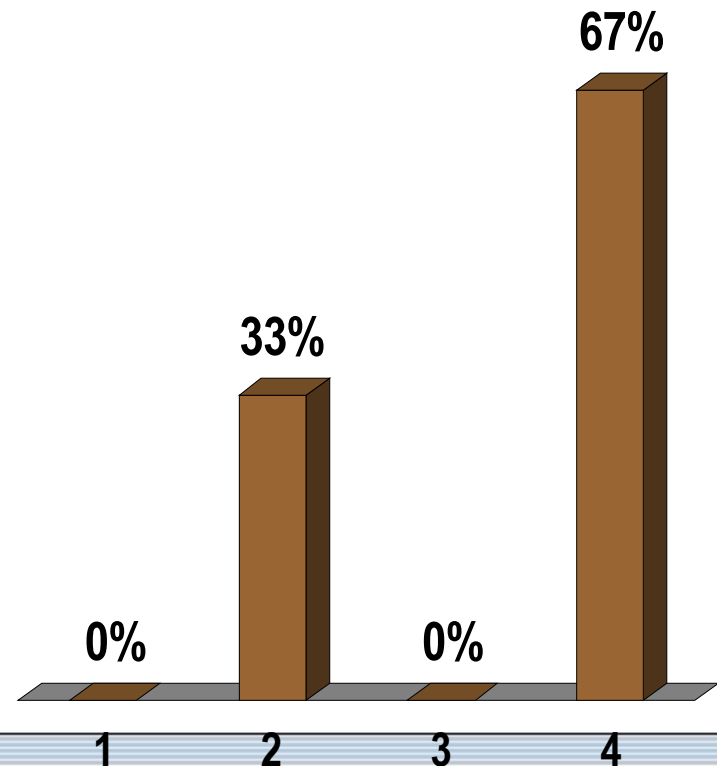
**General: Perform local and remote system audits (software and hardware)**

## Audit Local or Remote Systems



# Have you performed a vulnerability scan on your own network?

1. Yes
2. Yes, but it was lame
3. No
4. Not yet, but we're planning on it



# LANguard Network Scanner



**Price:** US \$295 and up



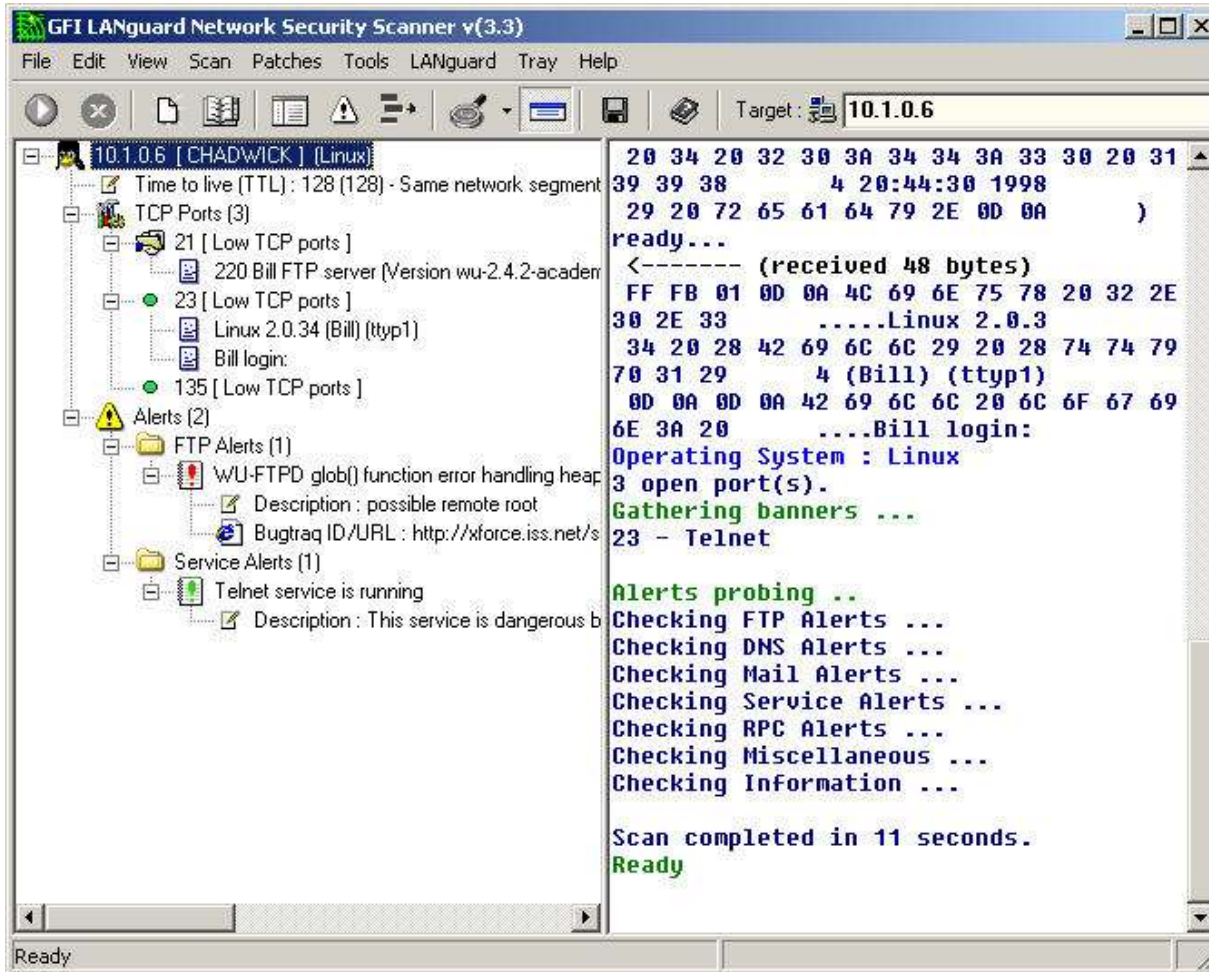
**Link:** [www.gfi.com](http://www.gfi.com)



**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



```
GFI LANguard Network Security Scanner v(3.3)
File Edit View Scan Patches Tools LANguard Tray Help
Target: 10.1.0.6
10.1.0.6 [CHADWICK] (Linux)
  Time to live (TTL) : 128 (128) - Same network segment
  TCP Ports (3)
    21 [ Low TCP ports ]
      220 Bill FTP server (Version wu-2.4.2-academ
    23 [ Low TCP ports ]
      Linux 2.0.34 (Bill) (ttyp1)
      Bill login:
    135 [ Low TCP ports ]
  Alerts (2)
    FTP Alerts (1)
      WU-FTPD glob() function error handling heap
        Description : possible remote root
        Bugtraq ID/URL : http://xforce.iss.net/s
    Service Alerts (1)
      Telnet service is running
        Description : This service is dangerous b
20 34 20 32 30 3A 34 34 3A 33 30 20 31
39 39 38      4 20:44:30 1998
29 20 72 65 61 64 79 2E 0D 0A      )
ready...
<----- (received 48 bytes)
FF FB 01 0D 0A 4C 69 6E 75 78 20 32 2E
30 2E 33      .....Linux 2.0.3
34 20 28 42 69 6C 6C 29 20 28 74 74 79
70 31 29      4 (Bill) (ttyp1)
0D 0A 0D 0A 42 69 6C 6C 20 6C 6F 67 69
6E 3A 20      ....Bill login:
Operating System : Linux
3 open port(s).
Gathering banners ...
23 - Telnet

Alerts probing ..
Checking FTP Alerts ...
Checking DNS Alerts ...
Checking Mail Alerts ...
Checking Service Alerts ...
Checking RPC Alerts ...
Checking Miscellaneous ...
Checking Information ...

Scan completed in 11 seconds.
Ready
```

# VisualRoute



**Price: US \$49.95 and up**

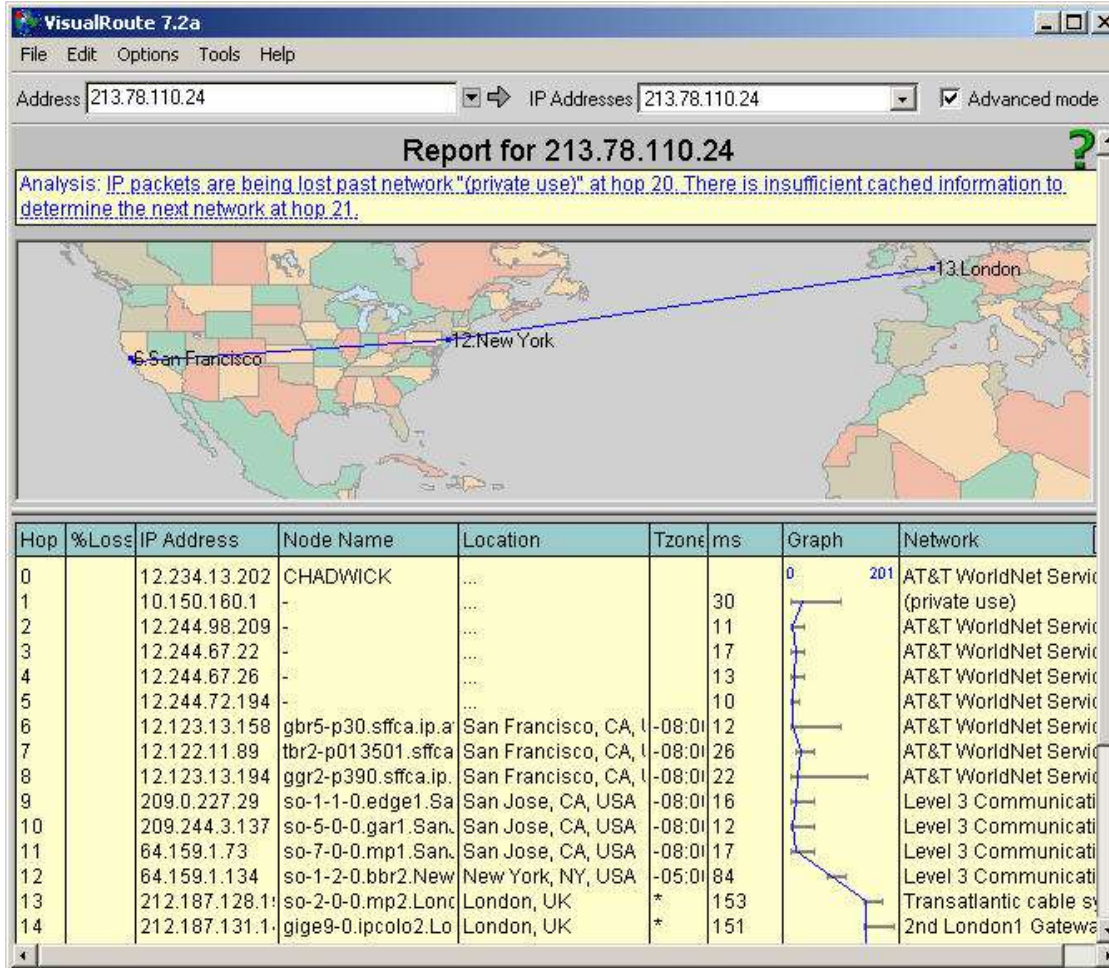


**Link: [www.visualware.com](http://www.visualware.com)**



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

## Visual Trace Back



## Conclusion

- **There are great inexpensive tools for IT professionals**
- **Ensure you have permission before using these tools on the company network**
- **Send me your tools list!**  
[Ichappell@packet-level.com](mailto:Ichappell@packet-level.com)