

Cyber Security Education Consortium (CSEC)

Nashville, TN: May 25, 2010

Jerry K. Sherrod, Ph.D., CCP
Networking and Communications Systems
Computer Science and Information Technology
Pellissippi State Community College
Knoxville, TN 37932
JSHERROD@PSTCC.EDU



FREE TOOLS FOR SYSTEM AND SECURITY ADMINISTRATORS

* Warning only use any of these tools with permission of your network administrator and not for malicious use

COMMAND LINE TOOLS

Selected Tools

WPSweep

WPSweep is a simple ping sweeper, that is, it pings a range of IP addresses and lists the ones that reply.

```
D:\>wpsweep 192.168.50.2 192.168.50.254
```

Got ping reply from the following hosts:

- 192.168.50.2
- 192.168.50.101
- 192.168.50.102
- 192.168.50.142
- 192.168.50.148
- 192.168.50.114
- 192.168.50.117
- 192.168.50.141
- 192.168.50.137
- 192.168.50.157

PStoreView

PStoreView lists the contents of the Protected Storage. It usually contains things like Internet Explorer username and password autocomplete, and Outlook account names and passwords.

```
D:\>pstoreview
```

The contents of the Protected Storage:

```
*** InfoDelivery
```

```
  * Subscriptions
```

```
*** IdentityMgr
```

```
  * Identities
```

```
    IdentitiesPass
```

PromiscDetect

PromiscDetect checks locally if your network adapter(s) is running in promiscuous mode, which may be a sign that you have a sniffer running on your computer. The first tool able to do this.

```
D:\>promiscdetect
```

Adapter name:

- Broadcom NetXtreme Gigabit Ethernet

Active filter for the adapter:

- Directed (capture packets directed to this computer)
- Multicast (capture multicast packets for groups the computer is a member of)
- Broadcast (capture broadcast packets)

PMDump

PMDump is a tool that lets you dump the memory contents of a process to a file without stopping the process.

```
D:\>PMDUMP -list
```

```
0 - System idle process
```

```
4 - System
```

```
776 - smss.exe
```

```
824 - csrss.exe
```

```
856 - winlogon.exe
```

```
900 - services.exe
```

```
912 - lsass.exe
```

```
1092 - ati2evxx.exe
```

```
1112 - svchost.exe
```

PEriscopes

PEriscopes is a PE file inspection tool. It works on ordinary 32-bit files as well as 64-bit and .NET ones.

```
D:\>periscopes snitch.exe
```

Valid PE file

File header information:

- Machine type: IA32 (x86)
- Executable image (not Object file or Library)
- Do not trim the working set aggressively
- Do not run from swap if on a removable medium
- Do not run from swap if on a network drive
- Can run on a multiprocessor system
- Contains no base relocations
- Cannot handle addresses beyond 2 Gb
- This file is not a DLL
- Link/compile date and time (UTC): Tue Dec 11 19:34:54 2

MACMatch

MACMatch lets you search for files by their last write, last access or creation time without changing any of these times.

```
D:\>macmatch . -a 2010-05-19:00.00 2010-5-19:12.00  
.\pstools\psservice.exe
```

- M: 2008-1-9:16.36
- A: 2010-5-19:8.49
- C: 2010-5-19:8.49

```
.\pstools\psshutdown.exe
```

- M: 2006-12-4:17.53
- A: 2010-5-19:8.49
- C: 2010-5-19:8.49

IPEye

IPEye is a TCP port scanner that can do SYN, FIN, Null and Xmas scans.

```
D:\>ipeye 192.168.50.2 -syn -p 20 100  
1-19 [not scanned]  
20-100 [drop]  
101-65535 [not scanned]
```

EtherChange

D:\>etherchange

0. Exit

1. 3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)
 2. 3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)
 3. Broadcom NetXtreme Gigabit Ethernet
 4. Broadcom NetXtreme 57xx Gigabit Controller
- Pick a network adapter: 1

EtherChange, continued

0. Exit

1. Specify a new Ethernet address

2. Go back to the built-in Ethernet address of the network adapter

Pick an action: 1

Specify a new Ethernet address (in hex without separators): 123456789001

The new Ethernet address has been set.

You need to disable and re-enable the network adapter (or reboot) to activate this new setting!

EFSView

EFSView lists the users who have ordinary decryption keys or recovery keys for an EFS encrypted file.

```
D:\>efsview .\abc.exe
```

Users with decryption keys:

- HACKER08\Administrator

Users with recovery keys:

DumpUsers

DumpUsers is able to dump account names and information even though RestrictAnonymous has been set to 1.

```
D:\>dumpusers -target hacker08 -type notdc  
-start 1 -stop 2000 -mode verbose
```

DumpUsers, continued

Account name: HACKER08\Administrator

- Password age: 21 days
- Privilege level: Administrator
- Home directory:
- Home directory mapped as:
- Comment: Built-in account for administering the computer/domain
- Account is: Enabled
- User can change password: Yes
- Account is locked out: No
- Password never expires: Yes
- The account is: Normal user
- Logon script path:
- Full name:
- User comment:

DumpUsers, continued 2

- Can log in from workstations: All
- Last logon to this DC / computer: Wed May 19 08:46:49 2010
- Last logon to this DC / computer: None
- Account expires: Never
- Max disk space: Unlimited
- Failed logins in a row to this DC / computer: 0
- Path to user profile:
- Password has expired: No

ClearLogs

ClearLogs clears the event log (Security, System or Application) that you specify. You run it from the Command Prompt, and it can also clear logs on a remote computer.

```
D:\>clearlogs -sec
```

Success: The log has been cleared

LIST ALTERNATE DATA STREAMS

```
D:\>lads
```

LADS - Freeware version 4.10

This program lists files with alternate data streams (ADS)

Use LADS on your own risk!

Scanning directory D:\

```
size  ADS in file
```

```
-----
```

```
0 bytes in 0 ADS listed
```

GPList

GPList lists information about the applied Group Policies.

```
D:\>gplist
```

Listing the applied Group Policies...

- * Group Policy Extension: Wireless

- * Policy Type: Computer

GPList, continued

- No Policy Applied
 - * Policy Type: User
 - No Policy Applied
- * Group Policy Extension: Folder Redirection
 - * Policy Type: Computer
 - No Policy Applied
 - * Policy Type: User
 - No Policy Applied

LNS - List NTFS Streams

LNS is a tool that searches for NTFS streams (aka alternate data streams or multiple data streams).

```
D:\FreeTools\PINK03\Downloads>lns .
```

Winfo

Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP. It also identifies the built-in Administrator and Guest accounts, even if their names have been changed.

```
D:\>winfo 192.168.50.100 -v
```

SYSTEM INFORMATION:

Warning: Unable to retrieve system information.
Reason : Unknown.

Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP. It also identifies the built-in Administrator and Guest accounts, even if their names have been changed.

```
D:\>wininfo 192.168.50.100 -v
```

SYSTEM INFORMATION:

Warning: Unable to retrieve system information.
Reason : Unknown.

Filestat

```
C:\Documents and Settings\MC131\Desktop>FileStat.exe FileStat.exe
```

```
Dumping FileStat.exe...
```

```
SD is valid.
```

```
SD is 164 bytes long.
```

```
SD revision is 1 == SECURITY_DESCRIPTOR_REVISION1
```

```
SD's Owner is Not NULL
```

```
SD's Owner-Defaulted flag is FALSE
```

```
  SID = PINK08/MC131 S-1-5-21--987176174-1510140708-1200401492-1019
```

```
SD's Group-Defaulted flag is FALSE
```

```
  SID = PINK08/None S-1-5-21--987176174-1510140708-1200401492-513
```

```
SD's DACL is Present
```

```
SD's DACL-Defaulted flag is FALSE
```

```
  ACL has 3 ACE(s), 88 bytes used, 0 bytes free
```

```
  ACL revision is 2 == ACL_REVISION2
```


Filestat, continued

```
SID = PINK08/MC131 S-1-5-21--
987176174-1510140708-1200401492-1019
  ACE 0 is an
ACCESS_ALLOWED_ACE_TYPE
  ACE 0 size = 36
  ACE 0 flags = 0x00
  ACE 0 mask = 0x001f01ff -R -W -X -D -
DEL_CHILD -CHANGE_PERMS -
TAKE_O
  SID = NT AUTHORITY/SYSTEM S-1-5-
18
  ACE 1 is an
ACCESS_ALLOWED_ACE_TYPE
  ACE 1 size = 20
  ACE 1 flags = 0x00
  ACE 1 mask = 0x001f01ff -R -W -X -D -
```

Hunt

```
C:\> Hunt.exe \\pink08
share = IPC$ - Remote IPC
share = D$ - Default share
share = ADMIN$ - Remote Admin
share = C$ - Default share
User = Administrator, , , Built-in account for administering the
computer/domain
```

Admin is PINK08\Administrator

User = Guest, , , Built-in account for guest access to the computer/domain

User = HelpAssistant, Remote Desktop Help Assistant Account, , Account
for Providing Remote Assistance

User = MC131, MC131, ,

User = Student, Student, ,

User = SUPPORT_388945a0, CN=Microsoft
Corporation,L=Redmond,S=Washington,C=US, ,

Hfind

```
C:\Documents and Settings\MC131\Desktop>HFind.exe
```

```
HFind v3.0 - Copyright(c) 2000, Foundstone, Inc.
```

```
Hidden file finder with last access times
```

```
Usage - hfind [path] /ns
```

```
[dirpath]    Directory to search - none equals current
```

```
-ns          Skip sub-directories
```

```
- or /       Either switch statement can be used
```

```
-?          Help
```

```
COMMAND PROMPT MUST HAVE A MINIMUM WIDTH OF 80  
CHARACTERS
```

GRAPHICAL TOOLS

WUPS

WUPS 1.4 - Copyright 1998-99, Arne Vidstrom
WUPS - Windows UDP Port Scanner
<http://www.ntsecurity.nu/toolbox/wups/>

IP to scan:

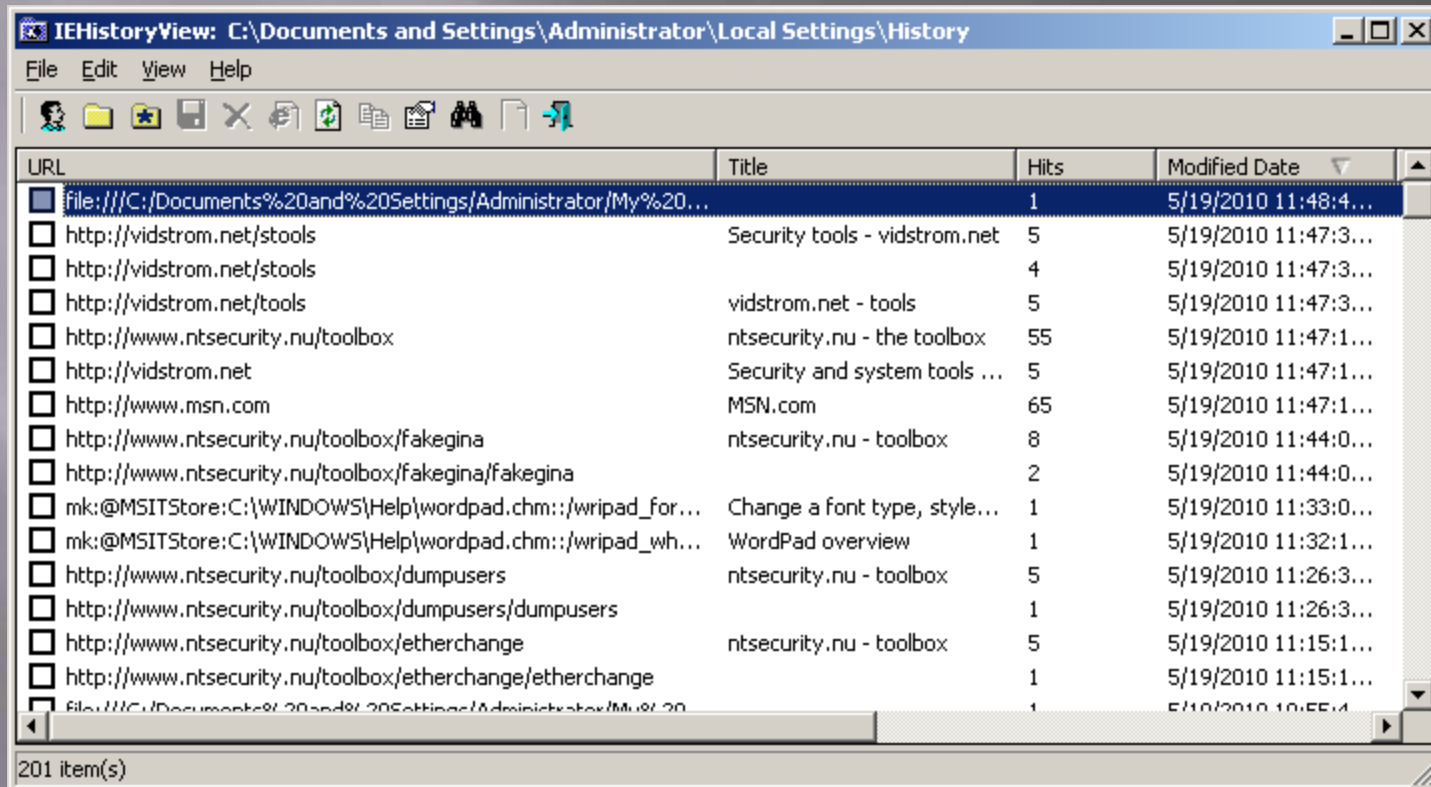
Start port: Stop port:

Delay, ms:

Status:

Open UDP ports:

IEHistoryView



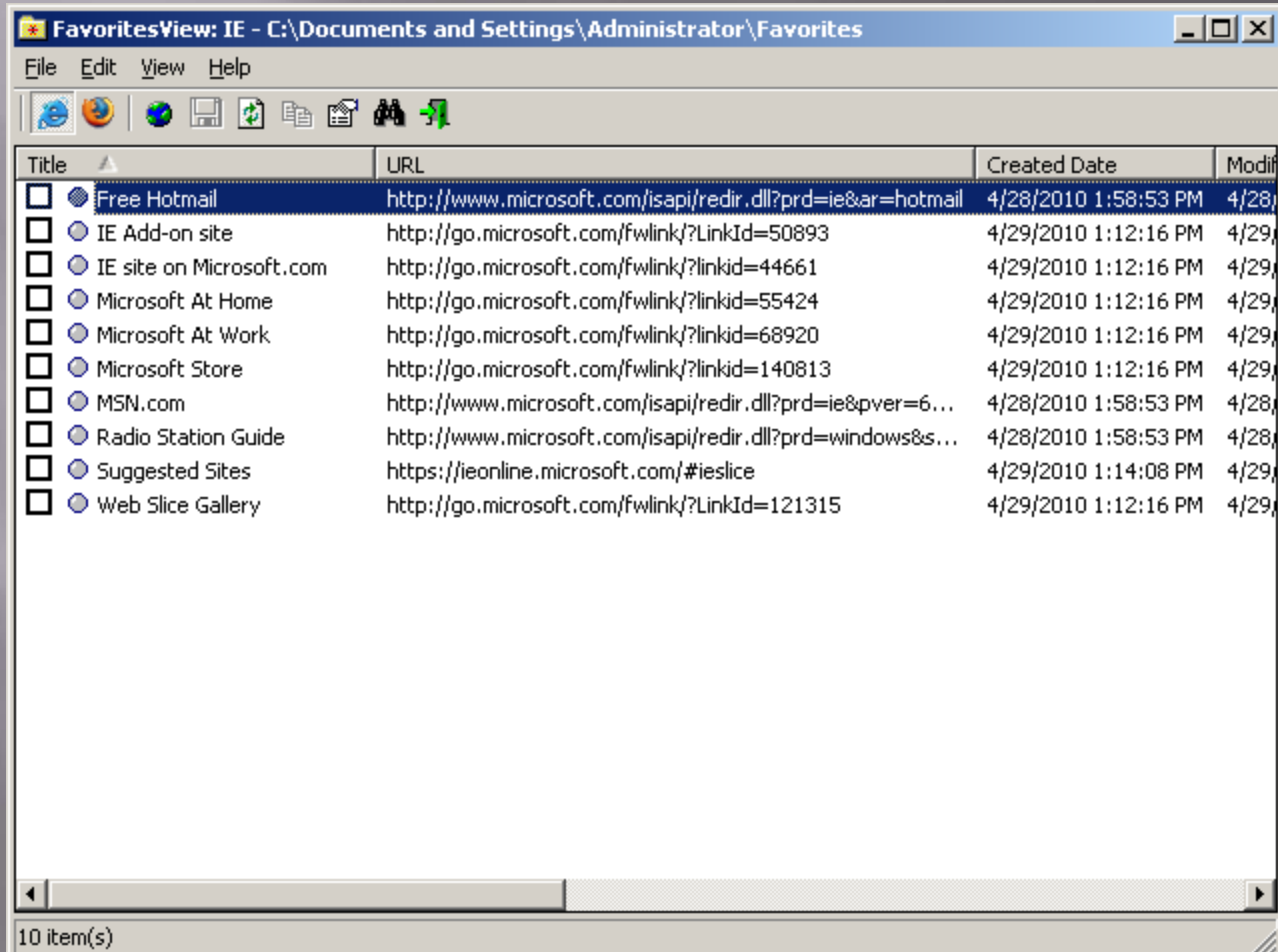
IEHistoryView: C:\Documents and Settings\Administrator\Local Settings\History

File Edit View Help

URL	Title	Hits	Modified Date
<input checked="" type="checkbox"/> file:///C:/Documents%20and%20Settings/Administrator/My%20...		1	5/19/2010 11:48:4...
<input type="checkbox"/> http://vidstrom.net/stools	Security tools - vidstrom.net	5	5/19/2010 11:47:3...
<input type="checkbox"/> http://vidstrom.net/stools		4	5/19/2010 11:47:3...
<input type="checkbox"/> http://vidstrom.net/tools	vidstrom.net - tools	5	5/19/2010 11:47:3...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox	ntsecurity.nu - the toolbox	55	5/19/2010 11:47:1...
<input type="checkbox"/> http://vidstrom.net	Security and system tools ...	5	5/19/2010 11:47:1...
<input type="checkbox"/> http://www.msn.com	MSN.com	65	5/19/2010 11:47:1...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox/fakegina	ntsecurity.nu - toolbox	8	5/19/2010 11:44:0...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox/fakegina/fakegina		2	5/19/2010 11:44:0...
<input type="checkbox"/> mk:@MSITStore:C:\WINDOWS\Help\wordpad.chm::wripad_for...	Change a font type, style...	1	5/19/2010 11:33:0...
<input type="checkbox"/> mk:@MSITStore:C:\WINDOWS\Help\wordpad.chm::wripad_wh...	WordPad overview	1	5/19/2010 11:32:1...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox/dumpusers	ntsecurity.nu - toolbox	5	5/19/2010 11:26:3...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox/dumpusers/dumpusers		1	5/19/2010 11:26:3...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox/etherchange	ntsecurity.nu - toolbox	5	5/19/2010 11:15:1...
<input type="checkbox"/> http://www.ntsecurity.nu/toolbox/etherchange/etherchange		1	5/19/2010 11:15:1...
<input type="checkbox"/> file:///C:/Documents%20and%20Settings/Administrator/My%20...		1	5/19/2010 10:55:4...

201 item(s)

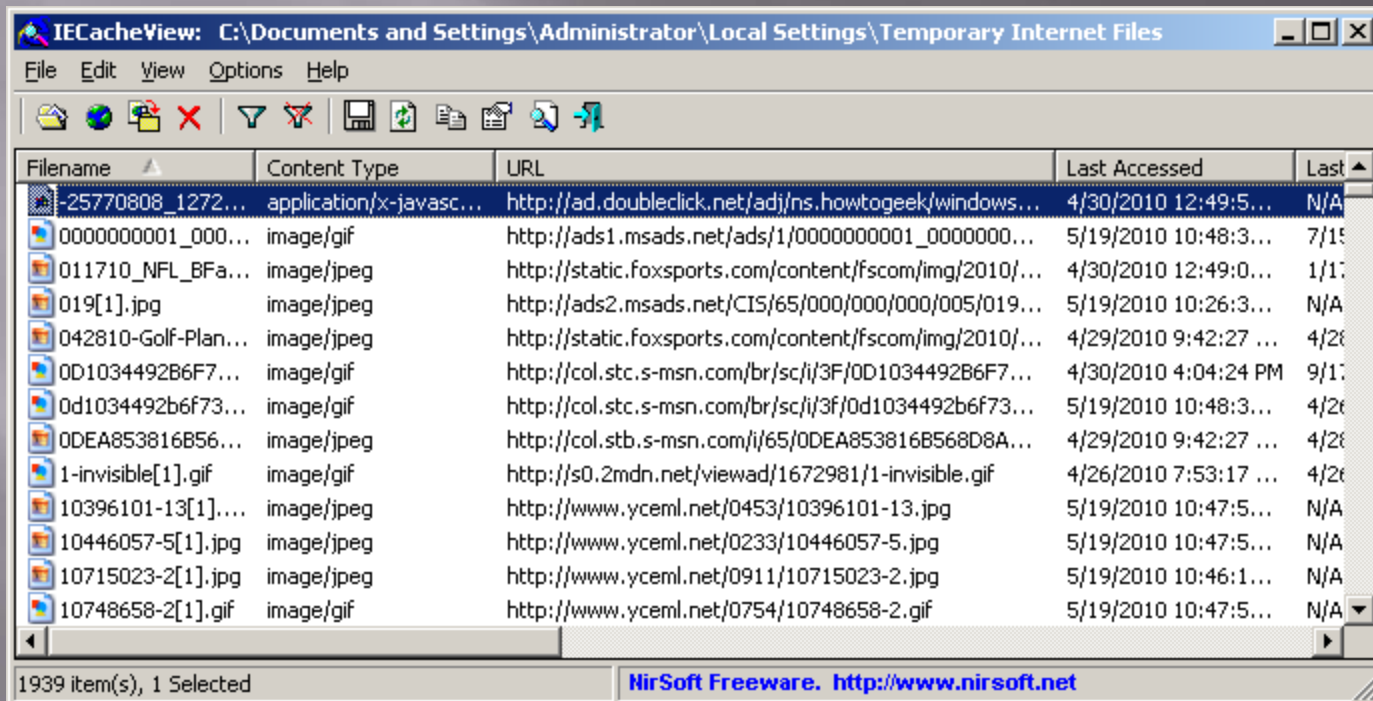
FavoritesView:IE



The screenshot shows a window titled "FavoritesView: IE - C:\Documents and Settings\Administrator\Favorites". The window contains a menu bar with "File", "Edit", "View", and "Help". Below the menu bar is a toolbar with icons for Internet Explorer, a globe, a folder, a document, a printer, and a search icon. The main area is a table with four columns: "Title", "URL", "Created Date", and "Modified". The table lists 10 items, with "Free Hotmail" selected. The status bar at the bottom indicates "10 item(s)".

Title	URL	Created Date	Modified
<input checked="" type="checkbox"/> Free Hotmail	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail	4/28/2010 1:58:53 PM	4/28/2010 1:58:53 PM
<input type="checkbox"/> IE Add-on site	http://go.microsoft.com/fwlink/?LinkId=50893	4/29/2010 1:12:16 PM	4/29/2010 1:12:16 PM
<input type="checkbox"/> IE site on Microsoft.com	http://go.microsoft.com/fwlink/?linkid=44661	4/29/2010 1:12:16 PM	4/29/2010 1:12:16 PM
<input type="checkbox"/> Microsoft At Home	http://go.microsoft.com/fwlink/?linkid=55424	4/29/2010 1:12:16 PM	4/29/2010 1:12:16 PM
<input type="checkbox"/> Microsoft At Work	http://go.microsoft.com/fwlink/?linkid=68920	4/29/2010 1:12:16 PM	4/29/2010 1:12:16 PM
<input type="checkbox"/> Microsoft Store	http://go.microsoft.com/fwlink/?linkid=140813	4/29/2010 1:12:16 PM	4/29/2010 1:12:16 PM
<input type="checkbox"/> MSN.com	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6...	4/28/2010 1:58:53 PM	4/28/2010 1:58:53 PM
<input type="checkbox"/> Radio Station Guide	http://www.microsoft.com/isapi/redir.dll?prd=windows&s...	4/28/2010 1:58:53 PM	4/28/2010 1:58:53 PM
<input type="checkbox"/> Suggested Sites	https://ieonline.microsoft.com/#ieslice	4/29/2010 1:14:08 PM	4/29/2010 1:14:08 PM
<input type="checkbox"/> Web Slice Gallery	http://go.microsoft.com/fwlink/?LinkId=121315	4/29/2010 1:12:16 PM	4/29/2010 1:12:16 PM

IECacheView



The screenshot shows the IECacheView application window. The title bar reads "IECacheView: C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations and navigation. The main area is a table with the following columns: "Filename", "Content Type", "URL", "Last Accessed", and "Last".

Filename	Content Type	URL	Last Accessed	Last
-25770808_1272...	application/x-javasc...	http://ad.doubleclick.net/adj/ns.howtogeek/windows...	4/30/2010 12:49:5...	N/A
0000000001_000...	image/gif	http://ads1.msads.net/ads/1/0000000001_0000000...	5/19/2010 10:48:3...	7/15
011710_NFL_BFa...	image/jpeg	http://static.foxsports.com/content/fscom/img/2010/...	4/30/2010 12:49:0...	1/10
019[1].jpg	image/jpeg	http://ads2.msads.net/CIS/65/000/000/000/005/019...	5/19/2010 10:26:3...	N/A
042810-Golf-Plan...	image/jpeg	http://static.foxsports.com/content/fscom/img/2010/...	4/29/2010 9:42:27 ...	4/26
0D1034492B6F7...	image/gif	http://col.stc.s-msn.com/br/sc/i/3f/0D1034492B6F7...	4/30/2010 4:04:24 PM	9/10
0d1034492b6f73...	image/gif	http://col.stc.s-msn.com/br/sc/i/3f/0d1034492b6f73...	5/19/2010 10:48:3...	4/26
0DEA853816B56...	image/jpeg	http://col.stb.s-msn.com/i/65/0DEA853816B568D8A...	4/29/2010 9:42:27 ...	4/26
1-invisible[1].gif	image/gif	http://s0.2mdn.net/viewad/1672981/1-invisible.gif	4/26/2010 7:53:17 ...	4/26
10396101-13[1]...	image/jpeg	http://www.ycml.net/0453/10396101-13.jpg	5/19/2010 10:47:5...	N/A
10446057-5[1].jpg	image/jpeg	http://www.ycml.net/0233/10446057-5.jpg	5/19/2010 10:47:5...	N/A
10715023-2[1].jpg	image/jpeg	http://www.ycml.net/0911/10715023-2.jpg	5/19/2010 10:46:1...	N/A
10748658-2[1].gif	image/gif	http://www.ycml.net/0754/10748658-2.gif	5/19/2010 10:47:5...	N/A

At the bottom of the window, it displays "1939 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

IECookiesView

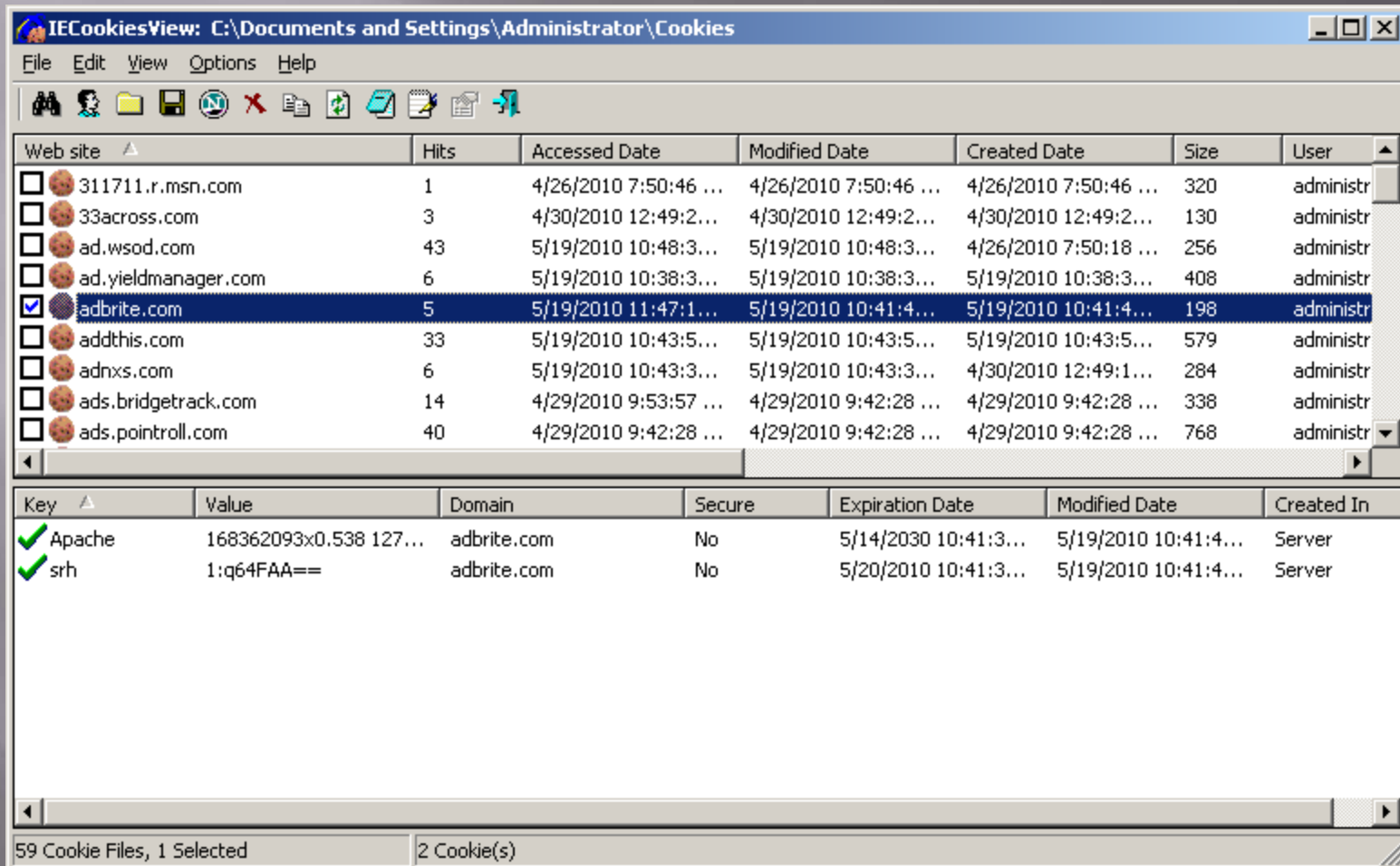
The screenshot shows the IECookiesView application window. The title bar reads "IECookiesView: C:\Documents and Settings\Administrator\Cookies". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains various icons for file operations. The main window is divided into two panes. The top pane displays a list of cookies with columns for "Web site", "Hits", "Accessed Date", "Modified Date", and "Created Date". The bottom pane displays a table with columns for "Key", "Value", "Domain", "Secure", "Expiration Date", and "Modified Date". The status bar at the bottom indicates "59 Cookie Files".

Web site	Hits	Accessed Date	Modified Date	Created Date
<input type="checkbox"/> 311711.r.msn.com	1	4/26/2010 7:50:46 ...	4/26/2010 7:50:46 ...	4/26/2010 7:50:46 ...
<input type="checkbox"/> 33across.com	3	4/30/2010 12:49:2...	4/30/2010 12:49:2...	4/30/2010 12:49:2...
<input type="checkbox"/> ad.wsod.com	43	5/19/2010 10:48:3...	5/19/2010 10:48:3...	4/26/2010 7:50:18 ...
<input type="checkbox"/> ad.yieldmanager.com	6	5/19/2010 10:38:3...	5/19/2010 10:38:3...	5/19/2010 10:38:3...
<input type="checkbox"/> adbrite.com	5	5/19/2010 11:47:1...	5/19/2010 10:41:4...	5/19/2010 10:41:4...
<input type="checkbox"/> addthis.com	33	5/19/2010 10:43:5...	5/19/2010 10:43:5...	5/19/2010 10:43:5...
<input type="checkbox"/> adnxs.com	6	5/19/2010 10:43:3...	5/19/2010 10:43:3...	4/30/2010 12:49:1...
<input type="checkbox"/> ads.bridgetrack.com	14	4/29/2010 9:53:57 ...	4/29/2010 9:42:28 ...	4/29/2010 9:42:28 ...
<input type="checkbox"/> ads.pointroll.com	40	4/29/2010 9:42:28 ...	4/29/2010 9:42:28 ...	4/29/2010 9:42:28 ...

Key	Value	Domain	Secure	Expiration Date	Modified Date
-----	-------	--------	--------	-----------------	---------------

59 Cookie Files

IECookiesView (with details)



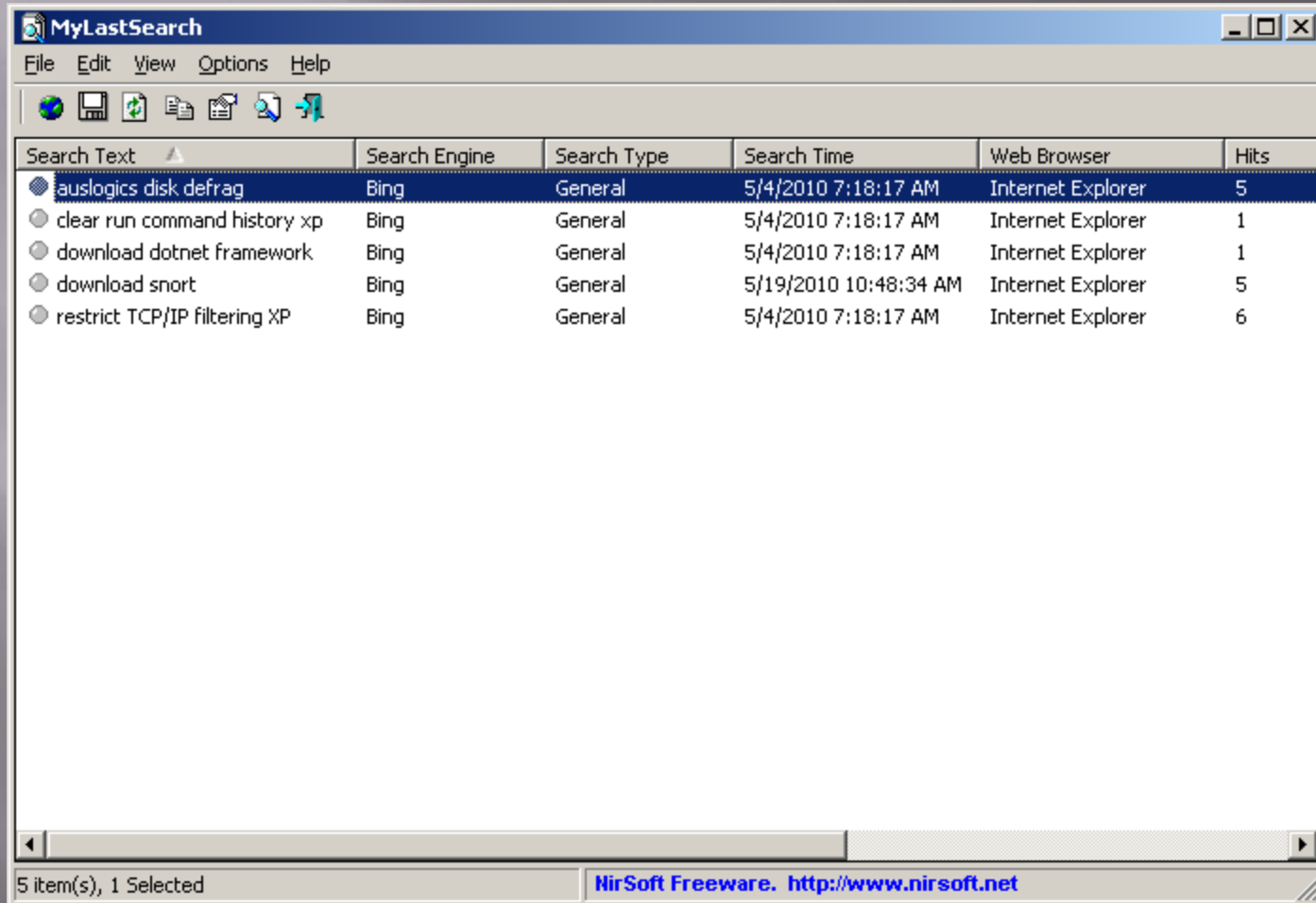
The screenshot shows the IECookiesView application window. The title bar reads "IECookiesView: C:\Documents and Settings\Administrator\Cookies". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for navigation and file operations. The main window is divided into two panes. The top pane is a table listing cookies from various websites. The bottom pane shows the details of the selected cookie.

Web site	Hits	Accessed Date	Modified Date	Created Date	Size	User
<input type="checkbox"/> 311711.r.msn.com	1	4/26/2010 7:50:46 ...	4/26/2010 7:50:46 ...	4/26/2010 7:50:46 ...	320	administr
<input type="checkbox"/> 33across.com	3	4/30/2010 12:49:2...	4/30/2010 12:49:2...	4/30/2010 12:49:2...	130	administr
<input type="checkbox"/> ad.wsod.com	43	5/19/2010 10:48:3...	5/19/2010 10:48:3...	4/26/2010 7:50:18 ...	256	administr
<input type="checkbox"/> ad.yieldmanager.com	6	5/19/2010 10:38:3...	5/19/2010 10:38:3...	5/19/2010 10:38:3...	408	administr
<input checked="" type="checkbox"/> adbrite.com	5	5/19/2010 11:47:1...	5/19/2010 10:41:4...	5/19/2010 10:41:4...	198	administr
<input type="checkbox"/> addthis.com	33	5/19/2010 10:43:5...	5/19/2010 10:43:5...	5/19/2010 10:43:5...	579	administr
<input type="checkbox"/> adnxs.com	6	5/19/2010 10:43:3...	5/19/2010 10:43:3...	4/30/2010 12:49:1...	284	administr
<input type="checkbox"/> ads.bridgetrack.com	14	4/29/2010 9:53:57 ...	4/29/2010 9:42:28 ...	4/29/2010 9:42:28 ...	338	administr
<input type="checkbox"/> ads.pointroll.com	40	4/29/2010 9:42:28 ...	4/29/2010 9:42:28 ...	4/29/2010 9:42:28 ...	768	administr

Key	Value	Domain	Secure	Expiration Date	Modified Date	Created In
<input checked="" type="checkbox"/> Apache	168362093x0.538 127...	adbrite.com	No	5/14/2030 10:41:3...	5/19/2010 10:41:4...	Server
<input checked="" type="checkbox"/> srh	1:q64FAA==	adbrite.com	No	5/20/2010 10:41:3...	5/19/2010 10:41:4...	Server

59 Cookie Files, 1 Selected | 2 Cookie(s)

MyLastSearch



The screenshot shows the MyLastSearch application window. The title bar reads "MyLastSearch". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for file operations and search. The main area contains a table with the following data:

Search Text	Search Engine	Search Type	Search Time	Web Browser	Hits
● auslogics disk defrag	Bing	General	5/4/2010 7:18:17 AM	Internet Explorer	5
○ clear run command history xp	Bing	General	5/4/2010 7:18:17 AM	Internet Explorer	1
○ download dotnet framework	Bing	General	5/4/2010 7:18:17 AM	Internet Explorer	1
○ download snort	Bing	General	5/19/2010 10:48:34 AM	Internet Explorer	5
○ restrict TCP/IP filtering XP	Bing	General	5/4/2010 7:18:17 AM	Internet Explorer	6

At the bottom of the window, the status bar shows "5 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

SiteShoter

SiteShoter [minimize] [maximize] [close]

Single URL/File:

URLs File:

Filename:

Web Browser Options

Width: Height:

Automatically extend browser size according to Web page

Maximum Width: Maximum Height:

Cut the Web page in the following location:

Left: Top: Width: Height:

Disable main scrollbars Disable JavaScript Disable Flash

Save Options

JPEG Quality (0 - 100):

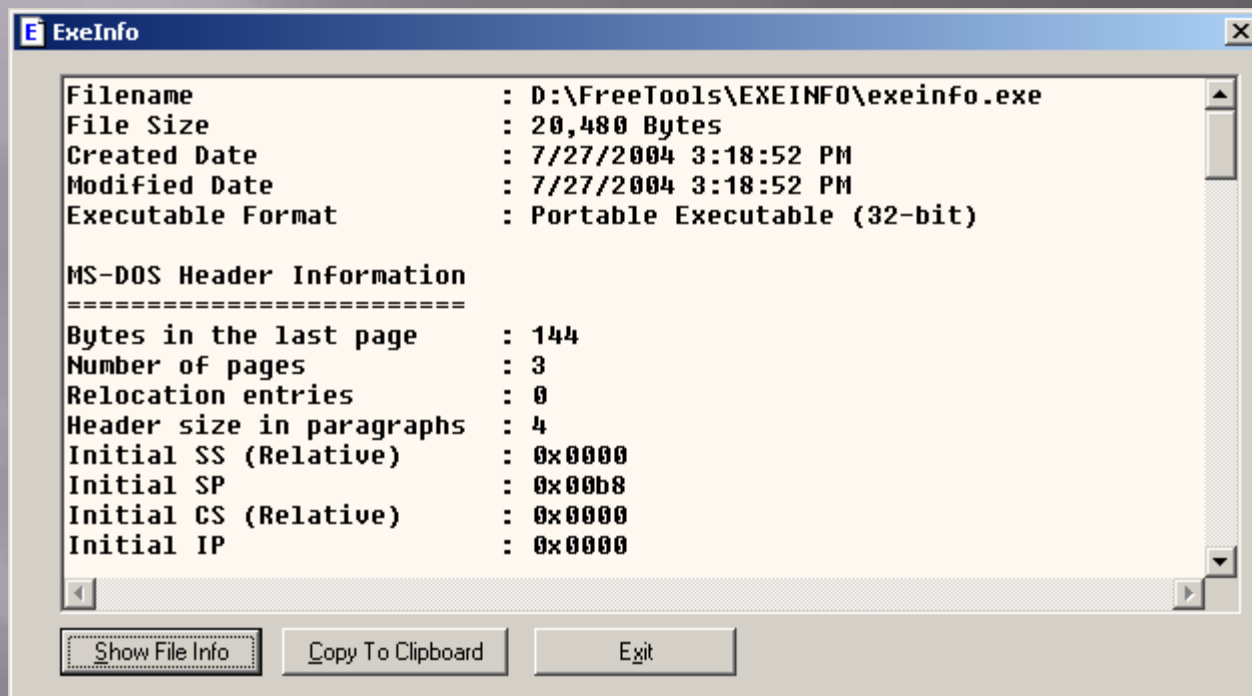
Image Size (In %):

Timeout (In milliseconds):

Open the screenshot file after save

Take a screenshot of this Web page every

ExeInfo



AdapterWatch (TCP/UDP Tab)

The screenshot shows the AdapterWatch application window with the TCP/UDP Statistics tab selected. The window title is "AdapterWatch" and it has a menu bar with "File", "Edit", "View", "Options", and "Help". Below the menu bar are several icons. The main area is a table with two columns: "Entry Name" and "Value". The table is divided into sections for TCP and UDP statistics. At the bottom of the window, it indicates "2 Adapter(s)".

Entry Name	Value
TCP Statistics	
Retransmission time-out (RTO) algorithm	Van Jacobson's Algorithm
Minimum retransmission time-out value (In Milliseconds)	300
Maximum retransmission time-out value (In Milliseconds)	120,000
Maximum number of connections	4,294,967,295
Number of active opens	579
Number of passive opens	4
Number of failed connection attempts	22
Number of established connections that have been reset	401
Number of currently established connections	1
Number of segments received	14,770
Number of segments transmitted	10,338
Number of segments retransmitted	968
Number of errors received	0
Number of segments transmitted with the reset flag set	371
Cumulative number of connections	10
UDP Statistics	
Number of datagrams received	9,745
Number of datagrams transmitted	77,132
number of received datagrams that were discarded because of invalid port	25,027
Number of erroneous datagrams that were received	0
Number of entries in the UDP listener table	13

2 Adapter(s)

AdapterWatch (IP Tab)

AdapterWatch

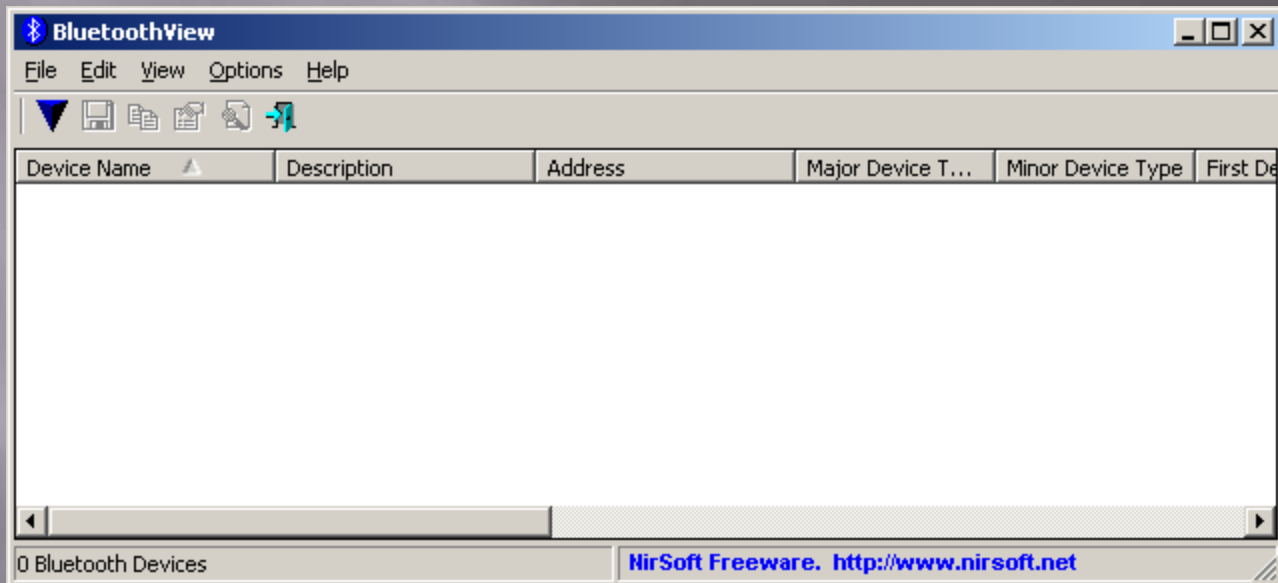
File Edit View Options Help

Network Adapters TCP/UDP Statistics IP Statistics ICMP Statistics General

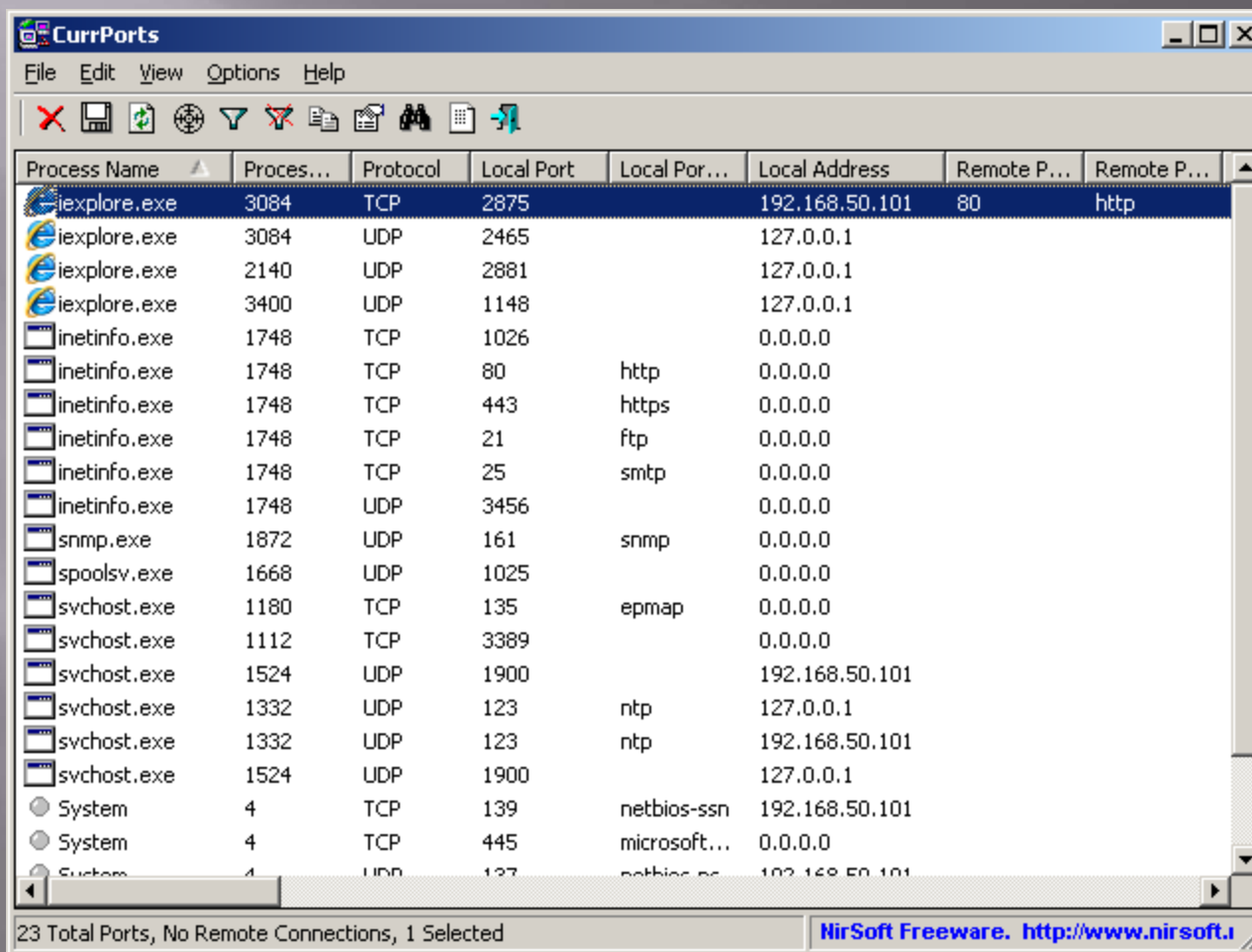
Entry Name	Value
IP Forwarding	Enabled
Default initial time to live (TTL) value	128
Number of datagrams received	65,005
Number of datagrams received with header error	0
number of datagrams received with address error	3
Number of datagrams received with unknown protocol	0
Number of datagrams forwarded	0
Number of received datagrams discarded	17,825
Number of received datagrams delivered	46,716
Number of outgoing datagrams that IP is requested to transmit	89,734
Number of outgoing datagrams discarded	0
Number of transmitted datagrams discarded	628
number of datagrams with no route to the destination IP address	0
Amount of time allowed for all pieces of a fragmented datagram to arrive	60
Number of datagrams that were required re-assembly	0
Number of datagrams that were successfully reassembled	0
Number of datagrams that failed to reassembled	0
Number of datagrams that were fragmented successfully	0
Datagrams that have not been fragmented because the IP header specifies no...	0
Number of fragments created	0
Number of interfaces	3
Number of IP addresses associated with this computer	3
Number of routes in the IP routing table	8

2 Adapter(s)

BlueToothView



CurrPorts



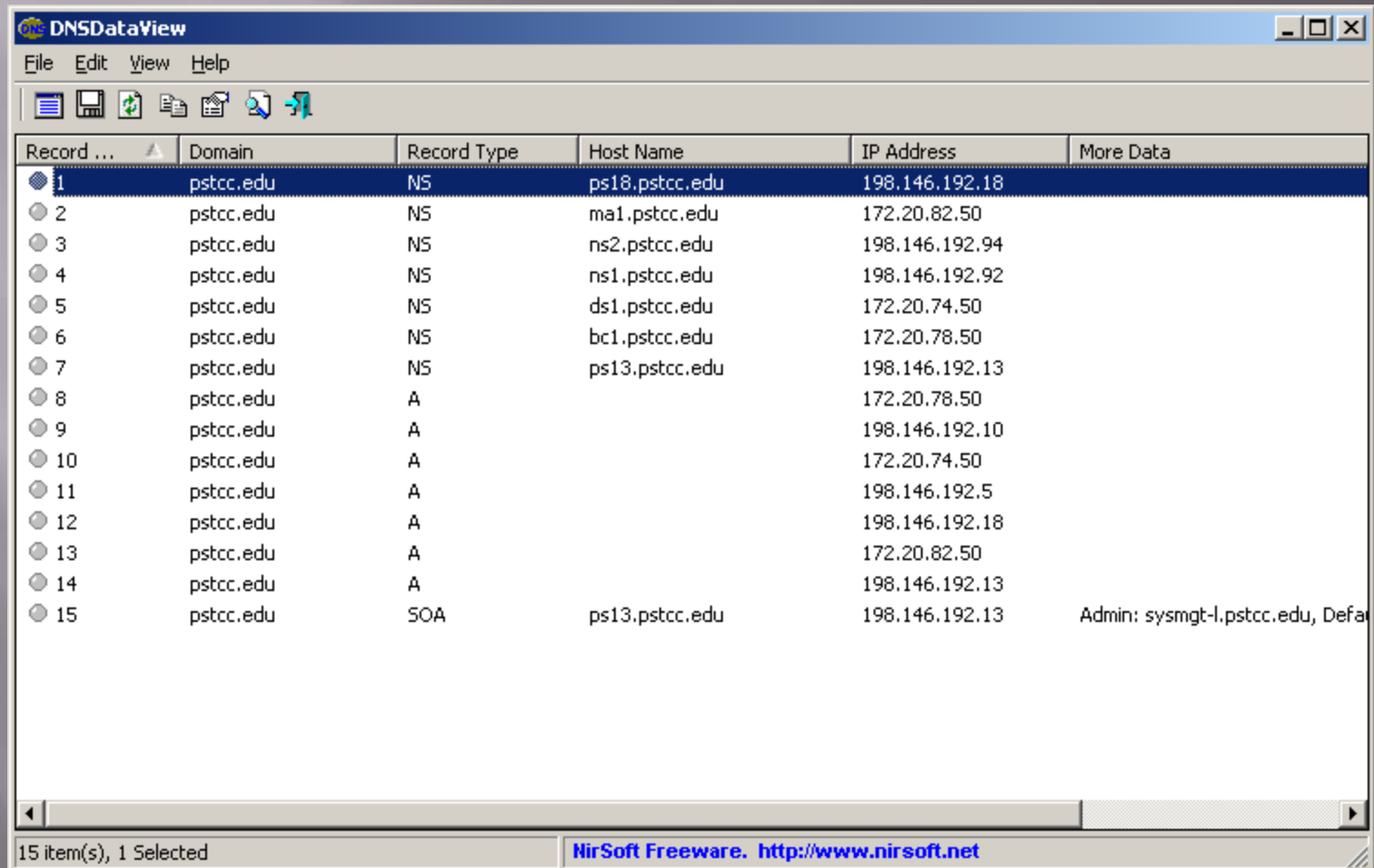
The screenshot shows the CurrPorts application window. The title bar reads "CurrPorts". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations and network-related functions. The main area is a table with the following columns: Process Name, Process ID, Protocol, Local Port, Local Port Name, Local Address, Remote Port, and Remote Port Name. The table lists several processes, including Internet Explorer (iexplore.exe), Internet Information Services (inetinfo.exe), Simple Network Management Protocol (snmp.exe), Spooling Service (spoolsv.exe), and Service Host (svchost.exe). The status bar at the bottom indicates "23 Total Ports, No Remote Connections, 1 Selected" and includes the NirSoft Freeware logo and website URL.

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name
iexplore.exe	3084	TCP	2875		192.168.50.101	80	http
iexplore.exe	3084	UDP	2465		127.0.0.1		
iexplore.exe	2140	UDP	2881		127.0.0.1		
iexplore.exe	3400	UDP	1148		127.0.0.1		
inetinfo.exe	1748	TCP	1026		0.0.0.0		
inetinfo.exe	1748	TCP	80	http	0.0.0.0		
inetinfo.exe	1748	TCP	443	https	0.0.0.0		
inetinfo.exe	1748	TCP	21	ftp	0.0.0.0		
inetinfo.exe	1748	TCP	25	smtp	0.0.0.0		
inetinfo.exe	1748	UDP	3456		0.0.0.0		
snmp.exe	1872	UDP	161	snmp	0.0.0.0		
spoolsv.exe	1668	UDP	1025		0.0.0.0		
svchost.exe	1180	TCP	135	epmap	0.0.0.0		
svchost.exe	1112	TCP	3389		0.0.0.0		
svchost.exe	1524	UDP	1900		192.168.50.101		
svchost.exe	1332	UDP	123	ntp	127.0.0.1		
svchost.exe	1332	UDP	123	ntp	192.168.50.101		
svchost.exe	1524	UDP	1900		127.0.0.1		
System	4	TCP	139	netbios-ssn	192.168.50.101		
System	4	TCP	445	microsoft...	0.0.0.0		
System	4	UDP	137	netbios-ns	192.168.50.101		

23 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.it>

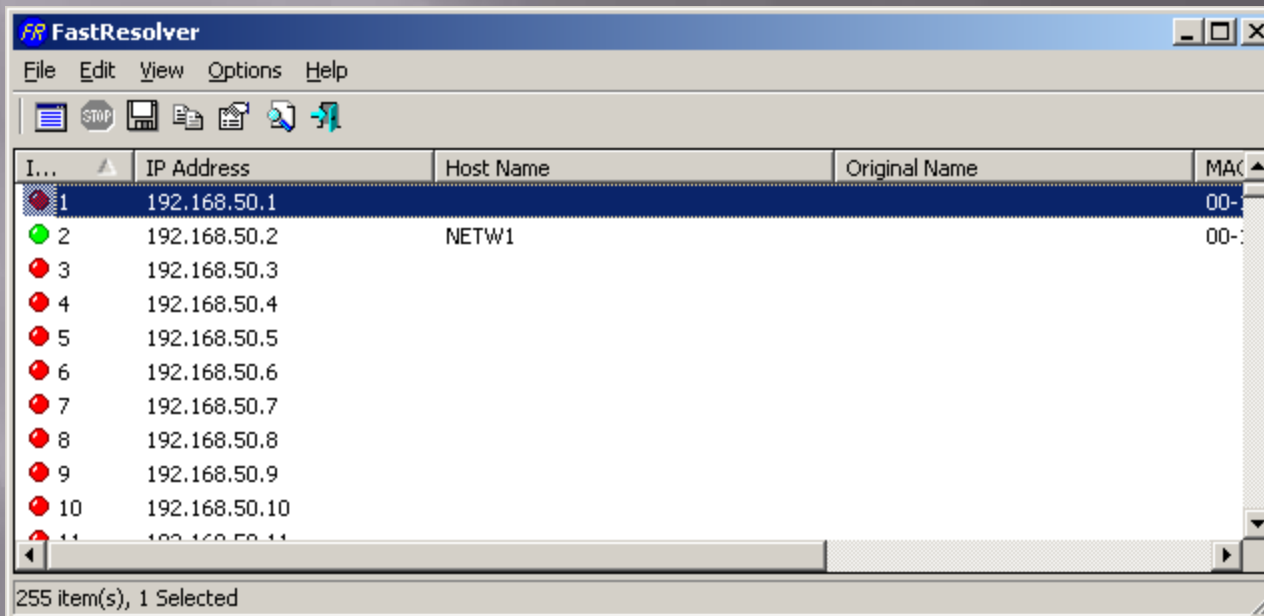
DNSDataView



The screenshot shows the DNSDataView application window. The title bar reads "DNSDataView". The menu bar includes "File", "Edit", "View", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area is a table with the following columns: "Record ...", "Domain", "Record Type", "Host Name", "IP Address", and "More Data". The table contains 15 records. Record 1 is selected. The status bar at the bottom indicates "15 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

Record ...	Domain	Record Type	Host Name	IP Address	More Data
1	pstcc.edu	NS	ps18.pstcc.edu	198.146.192.18	
2	pstcc.edu	NS	ma1.pstcc.edu	172.20.82.50	
3	pstcc.edu	NS	ns2.pstcc.edu	198.146.192.94	
4	pstcc.edu	NS	ns1.pstcc.edu	198.146.192.92	
5	pstcc.edu	NS	ds1.pstcc.edu	172.20.74.50	
6	pstcc.edu	NS	bc1.pstcc.edu	172.20.78.50	
7	pstcc.edu	NS	ps13.pstcc.edu	198.146.192.13	
8	pstcc.edu	A		172.20.78.50	
9	pstcc.edu	A		198.146.192.10	
10	pstcc.edu	A		172.20.74.50	
11	pstcc.edu	A		198.146.192.5	
12	pstcc.edu	A		198.146.192.18	
13	pstcc.edu	A		172.20.82.50	
14	pstcc.edu	A		198.146.192.13	
15	pstcc.edu	SOA	ps13.pstcc.edu	198.146.192.13	Admin: sysmgt-l.pstcc.edu, Defa

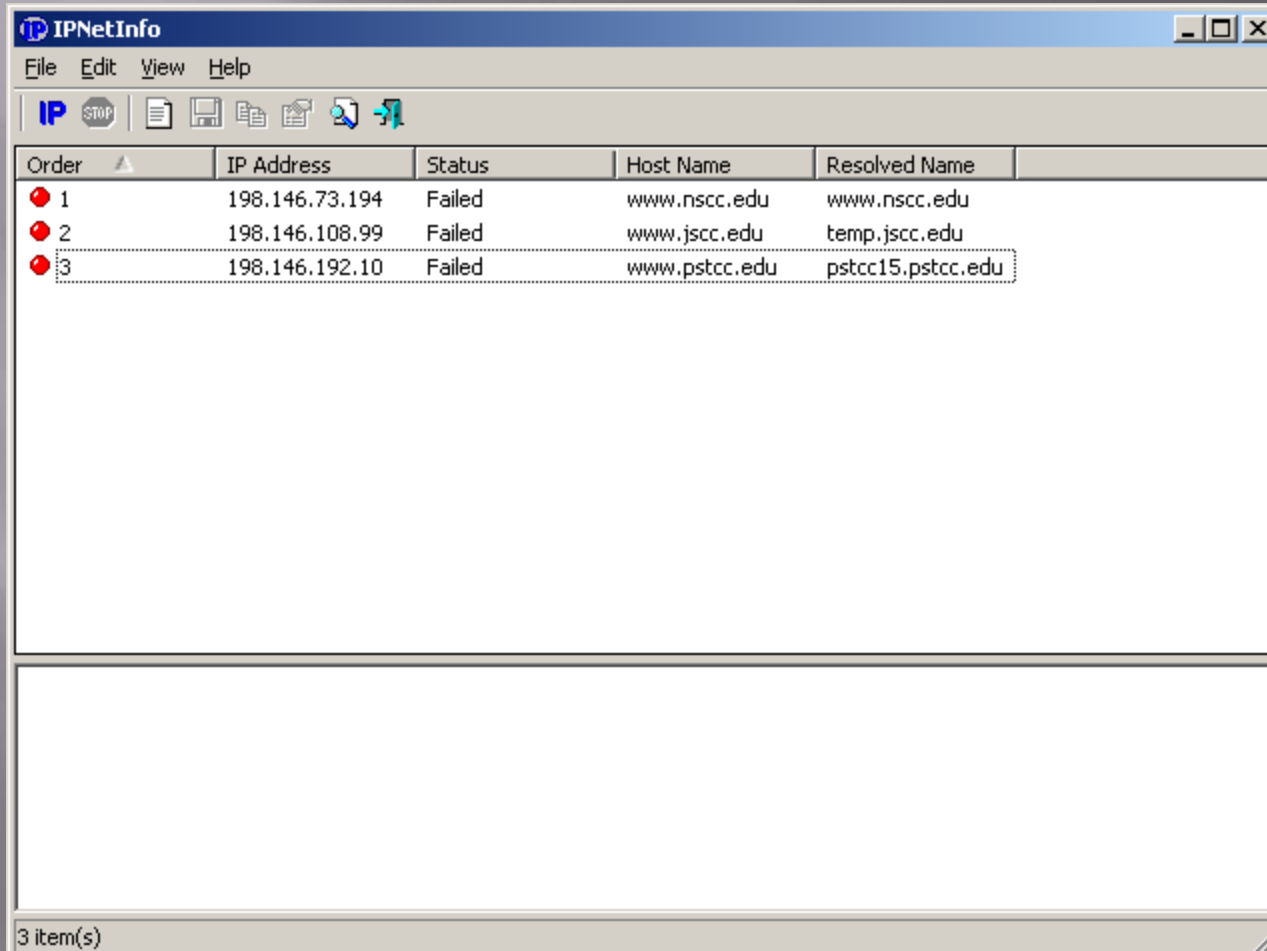
FastResolver



The screenshot shows the FastResolver application window. The title bar reads "FastResolver". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for file operations and a "STOP" button. The main area is a table with the following columns: "I...", "IP Address", "Host Name", "Original Name", and "MAC". The table contains 11 rows of data, with the first row selected. The status bar at the bottom indicates "255 item(s), 1 Selected".

I...	IP Address	Host Name	Original Name	MAC
1	192.168.50.1			00-
2	192.168.50.2	NETW1		00-
3	192.168.50.3			
4	192.168.50.4			
5	192.168.50.5			
6	192.168.50.6			
7	192.168.50.7			
8	192.168.50.8			
9	192.168.50.9			
10	192.168.50.10			
11	192.168.50.11			

IPNetInfo

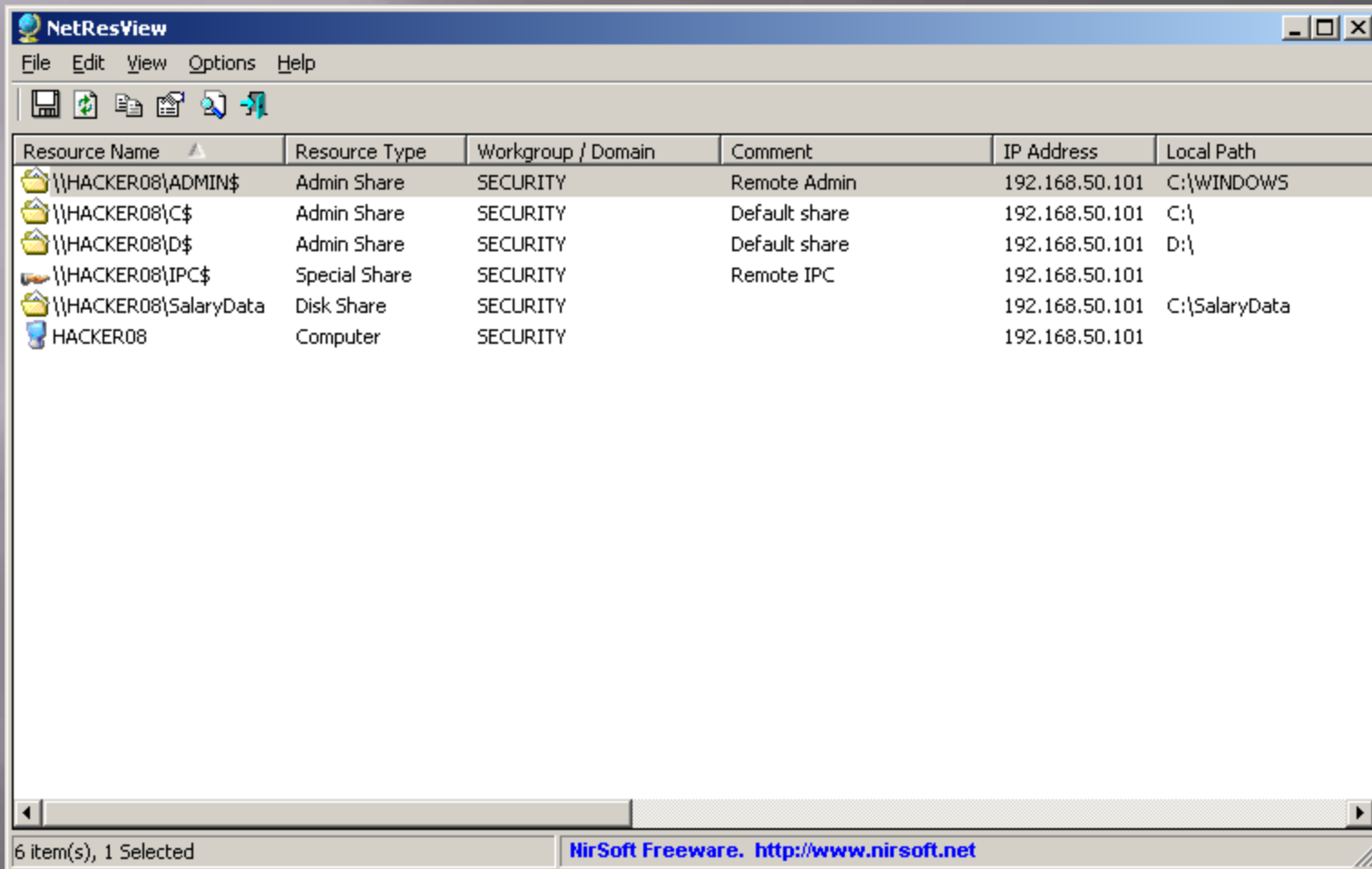


The screenshot shows a window titled "IPNetInfo" with a menu bar (File, Edit, View, Help) and a toolbar. The main area contains a table with the following data:

Order	IP Address	Status	Host Name	Resolved Name
1	198.146.73.194	Failed	www.nsccl.edu	www.nsccl.edu
2	198.146.108.99	Failed	www.jsccl.edu	temp.jsccl.edu
3	198.146.192.10	Failed	www.pstcc.edu	pstcc15.pstcc.edu

At the bottom of the window, it displays "3 item(s)".

NetResView

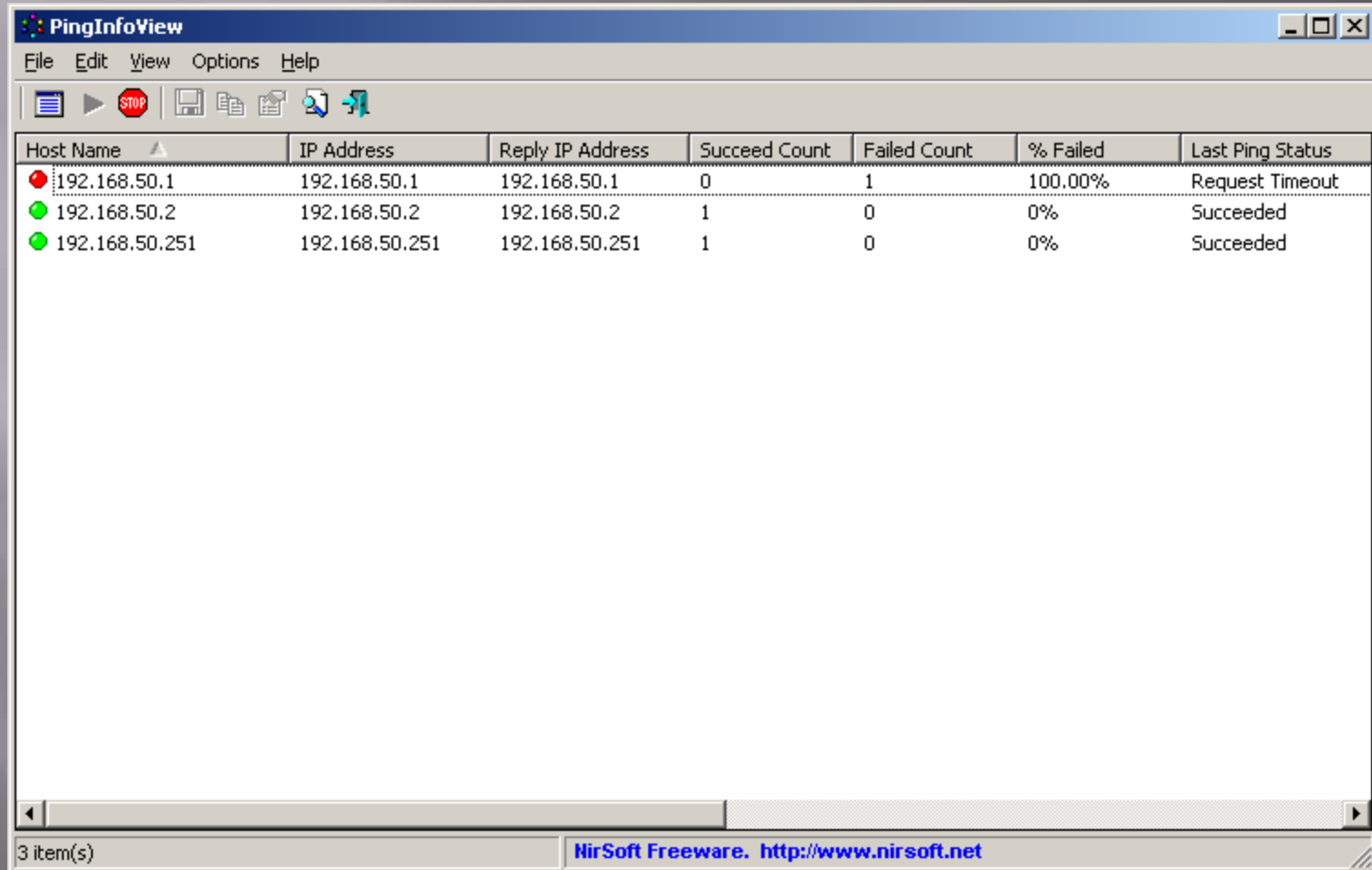


The screenshot shows the NetResView application window. The title bar reads "NetResView". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for refresh, print, save, and other functions. The main area displays a table with the following data:

Resource Name	Resource Type	Workgroup / Domain	Comment	IP Address	Local Path
\\HACKER08\ADMIN\$	Admin Share	SECURITY	Remote Admin	192.168.50.101	C:\WINDOWS
\\HACKER08\C\$	Admin Share	SECURITY	Default share	192.168.50.101	C:\
\\HACKER08\D\$	Admin Share	SECURITY	Default share	192.168.50.101	D:\
\\HACKER08\IPC\$	Special Share	SECURITY	Remote IPC	192.168.50.101	
\\HACKER08\SalaryData	Disk Share	SECURITY		192.168.50.101	C:\SalaryData
HACKER08	Computer	SECURITY		192.168.50.101	

At the bottom of the window, the status bar shows "6 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

PingInfoView

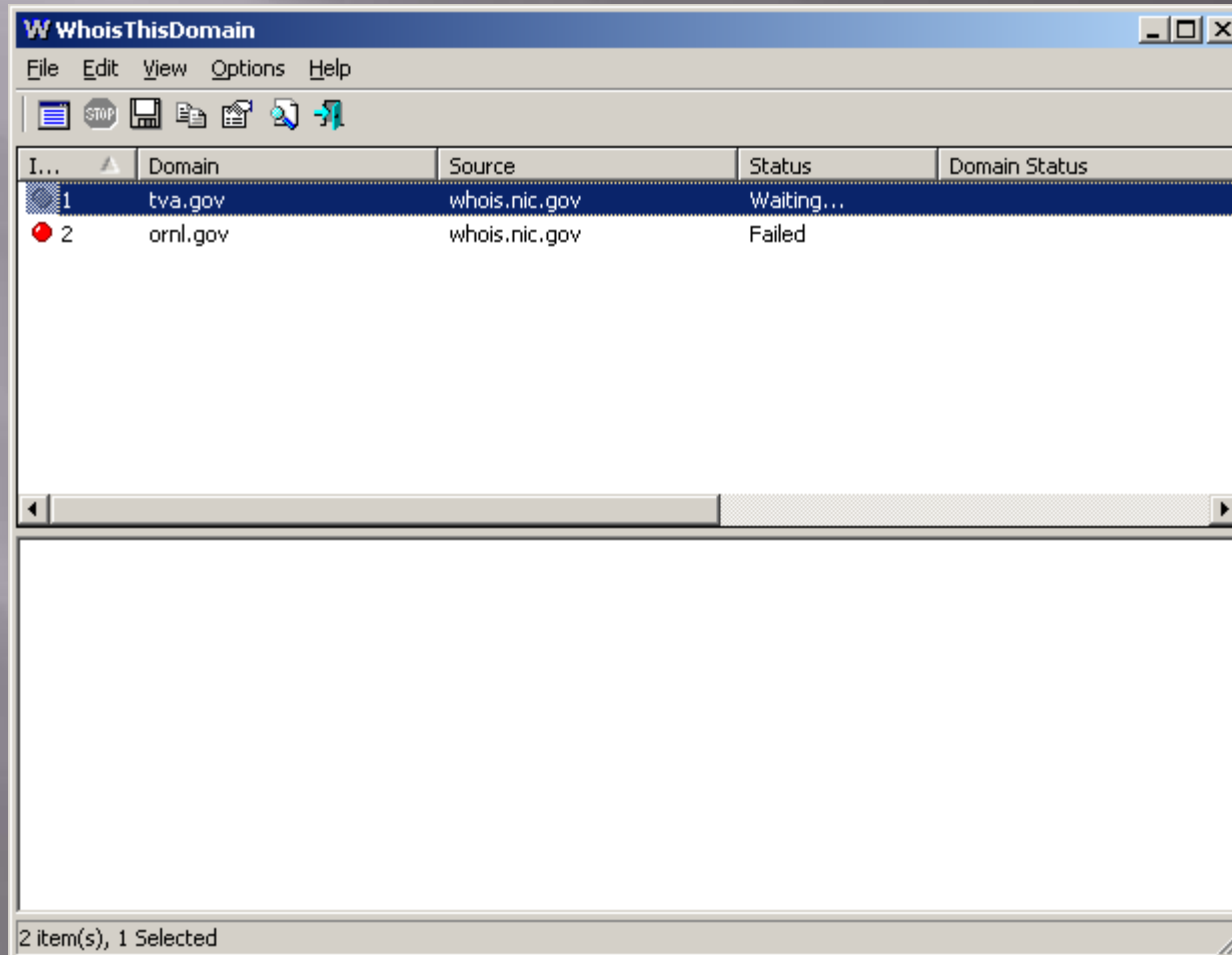


The screenshot shows the PingInfoView application window. The title bar reads "PingInfoView". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for list view, play, stop, save, print, copy, paste, and refresh. The main area contains a table with the following data:

Host Name	IP Address	Reply IP Address	Succeed Count	Failed Count	% Failed	Last Ping Status
192.168.50.1	192.168.50.1	192.168.50.1	0	1	100.00%	Request Timeout
192.168.50.2	192.168.50.2	192.168.50.2	1	0	0%	Succeeded
192.168.50.251	192.168.50.251	192.168.50.251	1	0	0%	Succeeded

At the bottom left of the window, it says "3 item(s)". At the bottom right, there is a footer: "NirSoft Freeware. <http://www.nirsoft.net>".

WhoisThisDomain

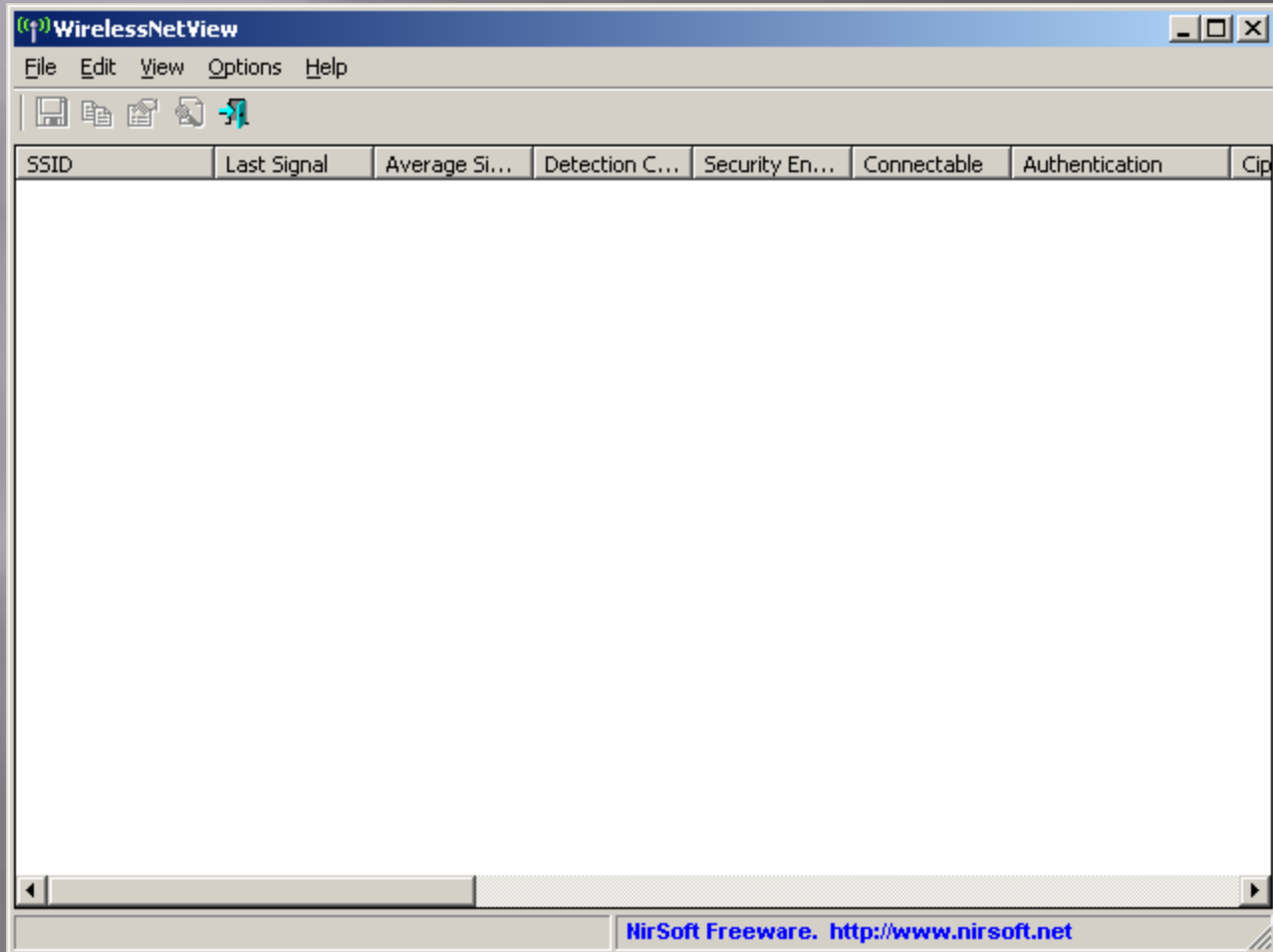


The screenshot shows a window titled "WhoisThisDomain" with a menu bar (File, Edit, View, Options, Help) and a toolbar. Below the toolbar is a table with the following data:

I...	Domain	Source	Status	Domain Status
1	tva.gov	whois.nic.gov	Waiting...	
2	ornl.gov	whois.nic.gov	Failed	

The status bar at the bottom indicates "2 item(s), 1 Selected".

WirelessNetView



AlternateStreamView

The screenshot shows the AlternateStreamView application window. The main window has a menu bar (File, Edit, View, Options, Help) and a toolbar with various icons. Below the toolbar is a table listing streams. The table has three columns: Stream Name, Filename, and Full S. The table contains 8 rows of data. The last row is selected. A Properties dialog box is open over the table, showing the details for the selected stream.

Stream Name	Filename	Full S
:Zone.Identifier:\$DATA	D:\Widstrom\cpuid.exe	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\crashprocess.exe	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\explorelibs.exe	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\findidt.exe	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\lddtroj.tar.gz	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\listobj.exe	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\taft.exe	D:\Wi
:Zone.Identifier:\$DATA	D:\Widstrom\wkml.exe	D:\Wi

Properties

Stream Name: :Zone.Identifier:\$DATA

Filename: D:\Widstrom\wkml.exe

Full Stream Name: D:\Widstrom\wkml.exe:Zone.Identifier

Stream Size: 26

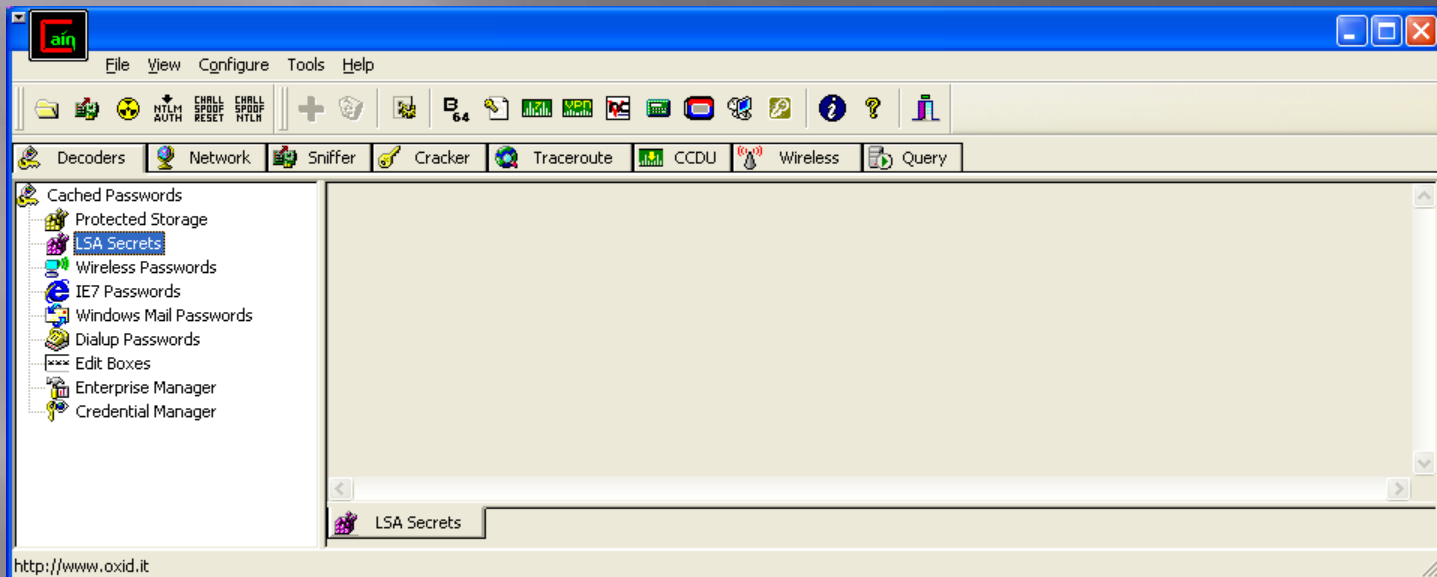
Stream Allocated Size: 32

OK

8 item(s), 1 Selected

NirSoft Freeware. h

Cain (Decoders Tab)

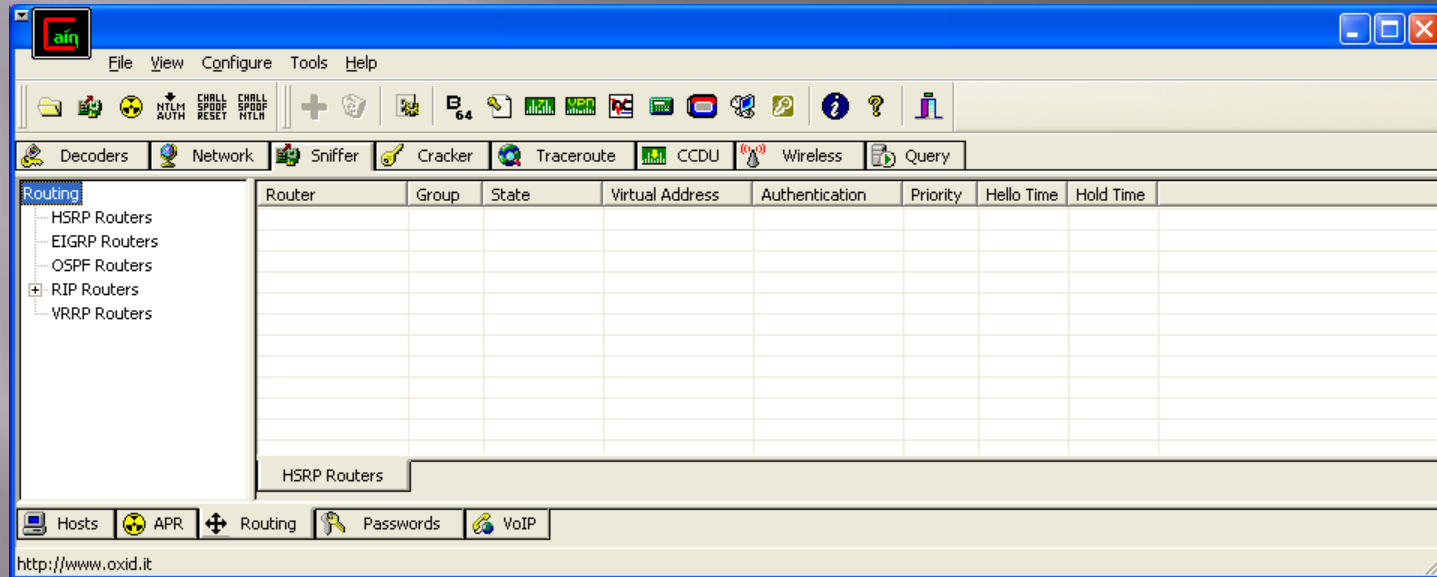


Cain (Network Tab)

The screenshot shows the 'Network' tab of the Cain software. The interface is divided into several sections:

- Menu Bar:** File, View, Configure, Tools, Help
- Toolbar:** Contains various icons for file operations, network tools, and help.
- Tabbed Interface:** Includes 'Decoders', 'Network' (selected), 'Sniffer', 'Cracker', 'Traceroute', 'CCDU', 'Wireless', and 'Query'.
- Tree View (Left):** Shows a hierarchical view of the network:
 - Entire Network
 - Microsoft Windows Network
 - Quick List
- Main Table:** A table with the following columns: Name, Type, Version, Comment. The table is currently empty.
- Bottom Panel:** A 'Computers' section with a laptop icon.
- Status Bar:** Displays the URL <http://www.oxid.it>.

Cain (Sniffer Tab)



Cain (Cracker Tab)

The screenshot displays the 'Cracker' tab in the Cain & Abel application. The interface includes a menu bar (File, View, Configure, Tools, Help), a toolbar with icons for file operations and network tools, and a main window divided into a tree view and a table.

Tree View (Left):

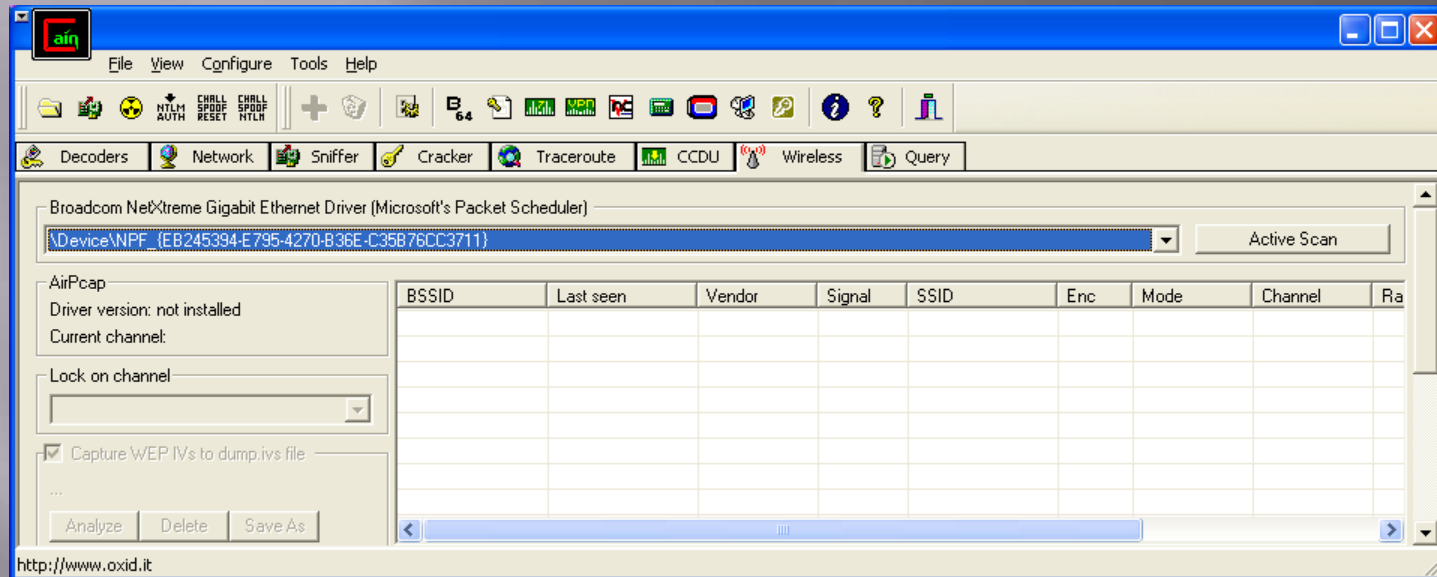
- Cracker
 - LM & NTLM Hashes (0)
 - NTLMv2 Hashes (0)
 - MS-Cache Hashes (0)
 - PWL files (0)
 - Cisco IOS-MD5 Hashes (0)
 - Cisco PIX-MD5 Hashes (0)
 - APOP-MD5 Hashes (0)
 - CRAM-MD5 Hashes (0)
 - OSPF-MD5 Hashes (0)
 - RIPv2-MD5 Hashes (0)
 - RRRP-HMAC Hashes (0)
 - VNC-3DES (0)
 - MD2 Hashes (0)
 - MD4 Hashes (0)

Table (Right):

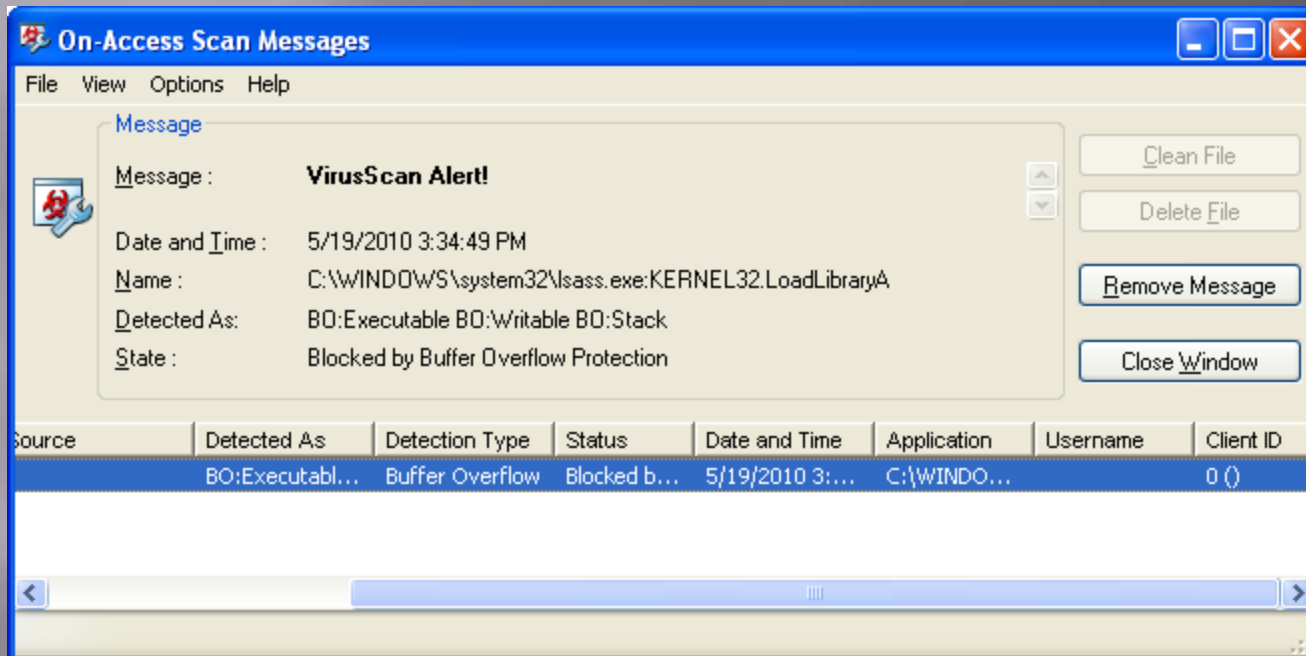
User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type

At the bottom left of the window, the URL <http://www.oxid.it> is displayed.

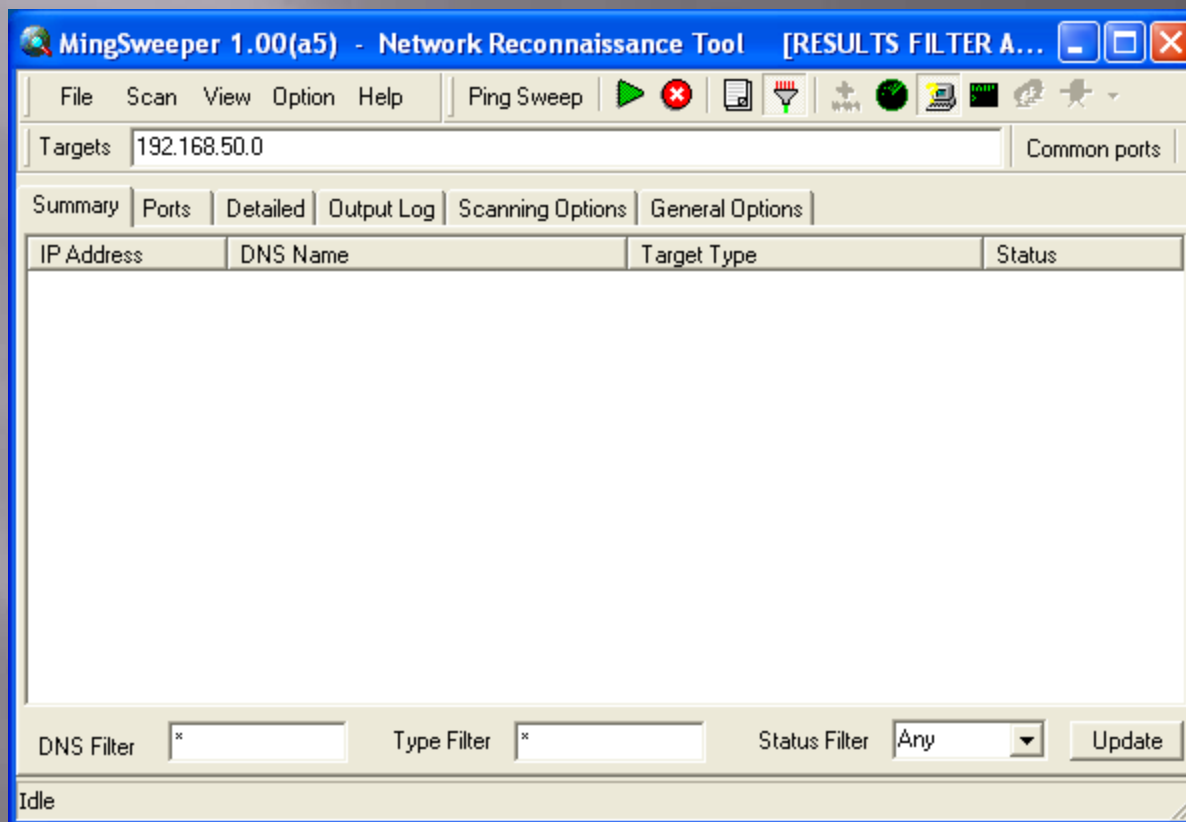
Cain (Wireless Tab)



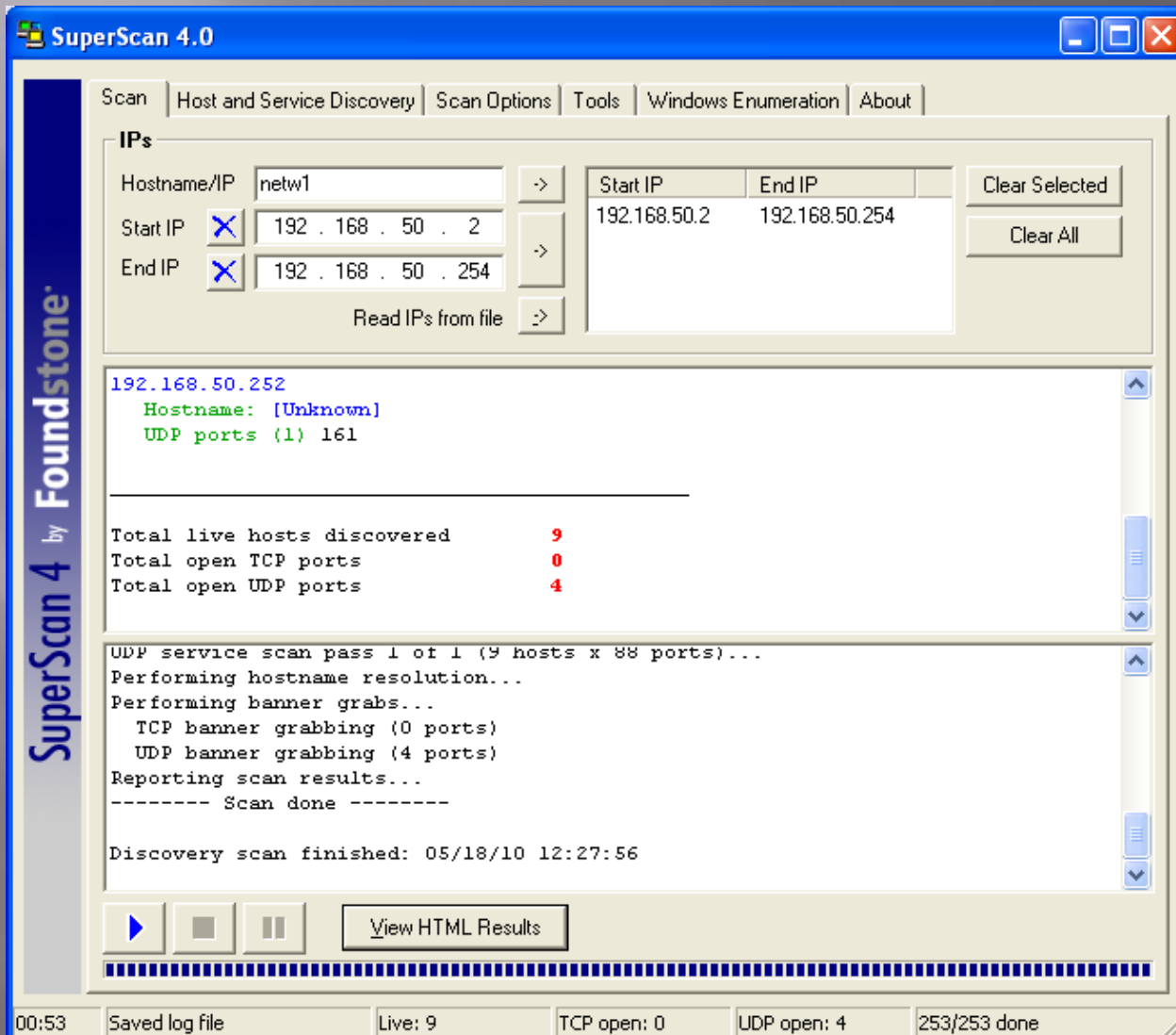
Cain (WARNING!!!!!!!!!!!!!!)



MingSweeper



SuperScan (Scan Tab)



The screenshot shows the SuperScan 4.0 application window with the 'Scan' tab selected. The interface includes a menu bar, a sidebar with the 'Foundstone' logo, and a main control area. The 'IPs' section contains input fields for Hostname/IP (netw1), Start IP (192.168.50.2), and End IP (192.168.50.254), along with a table of selected IP ranges. The main display area shows scan results for 192.168.50.252, including hostname resolution and open UDP ports. A summary table at the bottom of the main display shows 9 live hosts discovered, 0 open TCP ports, and 4 open UDP ports. The status bar at the bottom provides a progress overview: 00:53, Saved log file, Live: 9, TCP open: 0, UDP open: 4, 253/253 done.

SuperScan 4 by Foundstone

Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About

IPs

Hostname/IP: netw1 → Start IP: 192.168.50.2 End IP: 192.168.50.254

Start IP	End IP
192.168.50.2	192.168.50.254

Clear Selected
Clear All

Read IPs from file →

192.168.50.252
Hostname: [Unknown]
UDP ports (1) 161

Total live hosts discovered	9
Total open TCP ports	0
Total open UDP ports	4

UDP service scan pass 1 of 1 (9 hosts x 88 ports)...

Performing hostname resolution...

Performing banner grabs...

- TCP banner grabbing (0 ports)
- UDP banner grabbing (4 ports)

Reporting scan results...

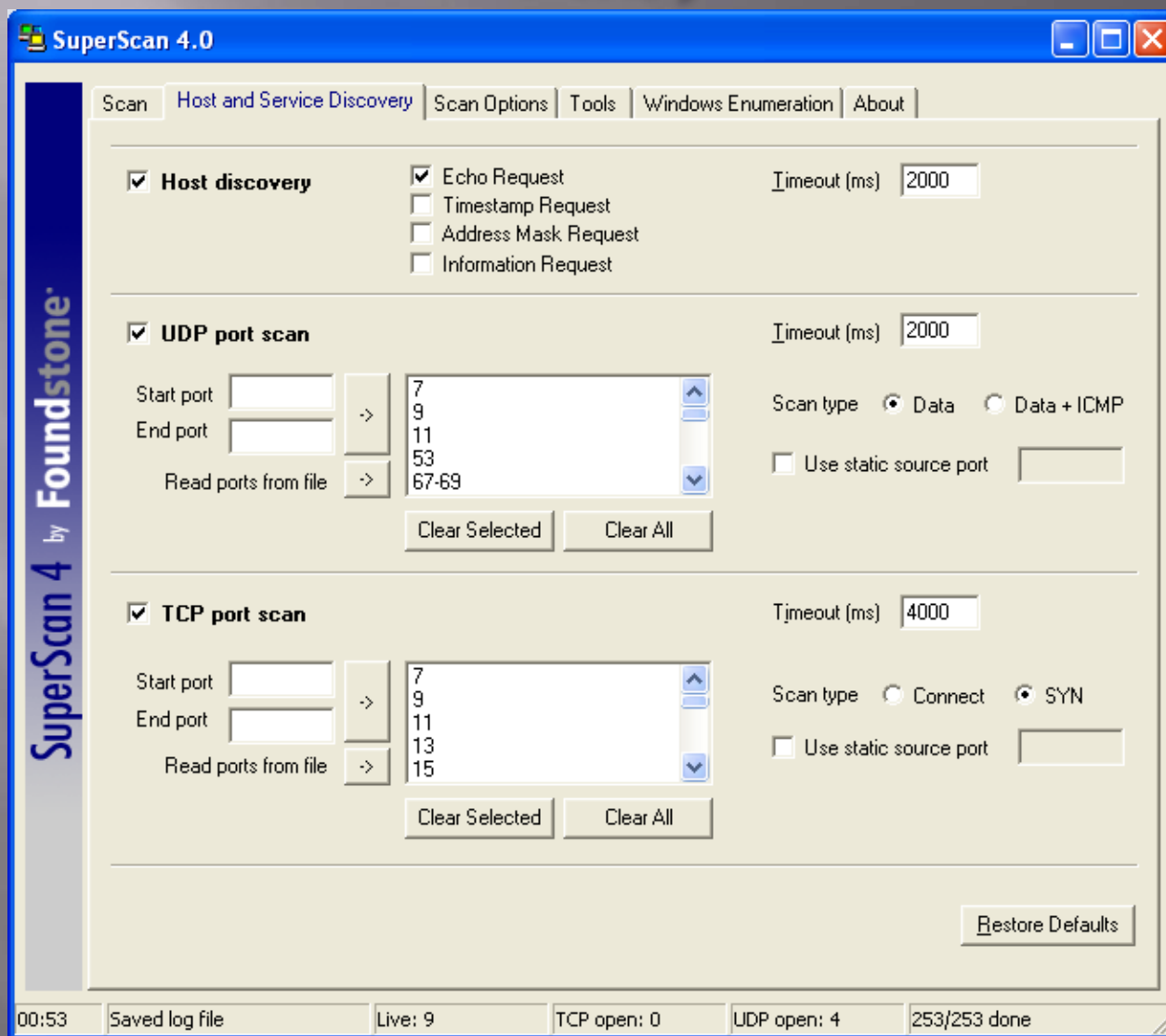
----- Scan done -----

Discovery scan finished: 05/18/10 12:27:56

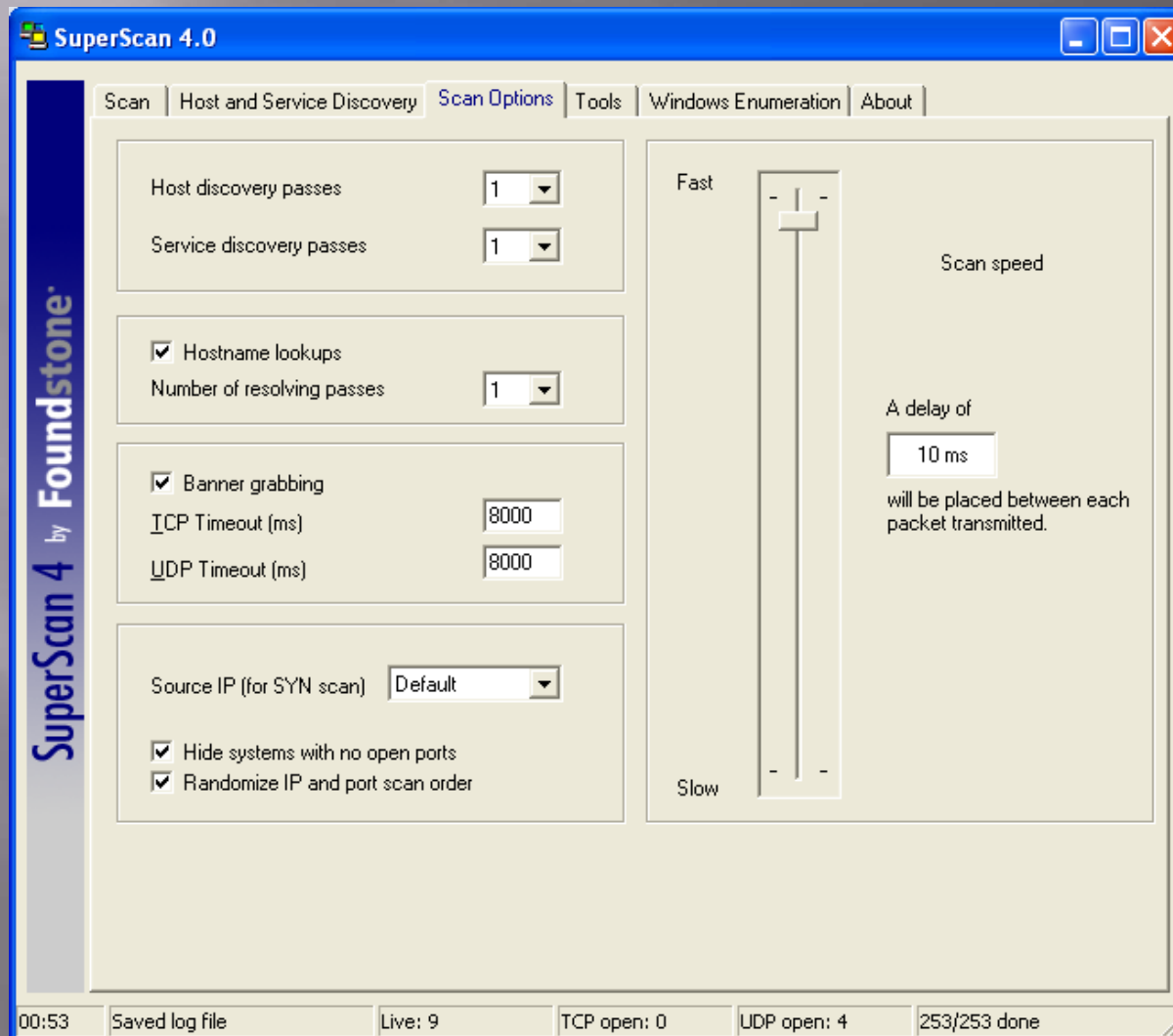
▶ ■ || View HTML Results

00:53 | Saved log file | Live: 9 | TCP open: 0 | UDP open: 4 | 253/253 done

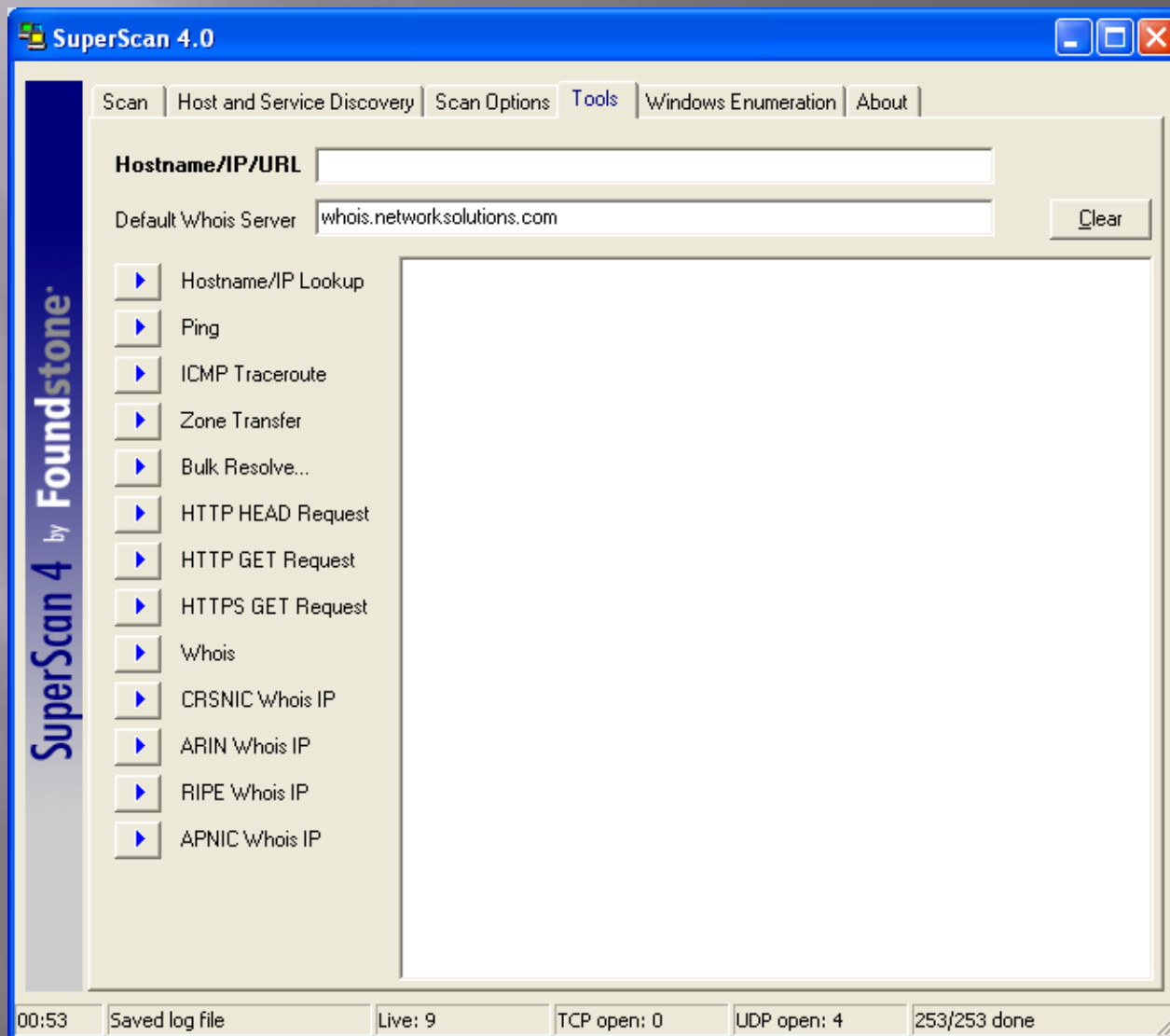
SuperScan (Host and Discovery Tab)



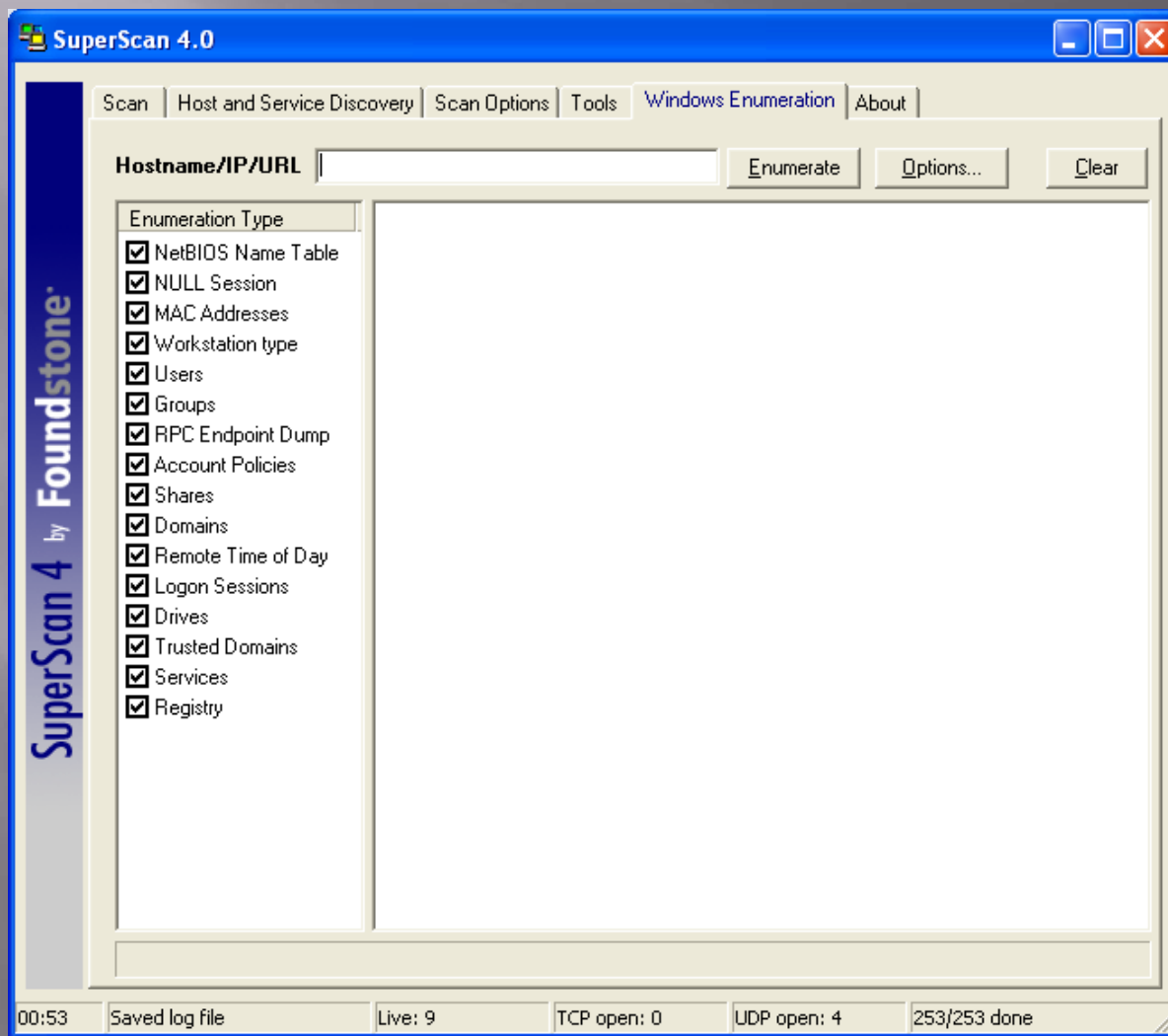
SuperScan (Scan Options Tab)



SuperScan (Tools Tab)



SuperScan (Windows Enumeration Tab)



Brutus

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target Type

Connection Options

Port Connections Timeout Use Proxy

HTTP (Basic) Options

Method KeepAlive

Authentication Options

Use Username Single User Pass Mode

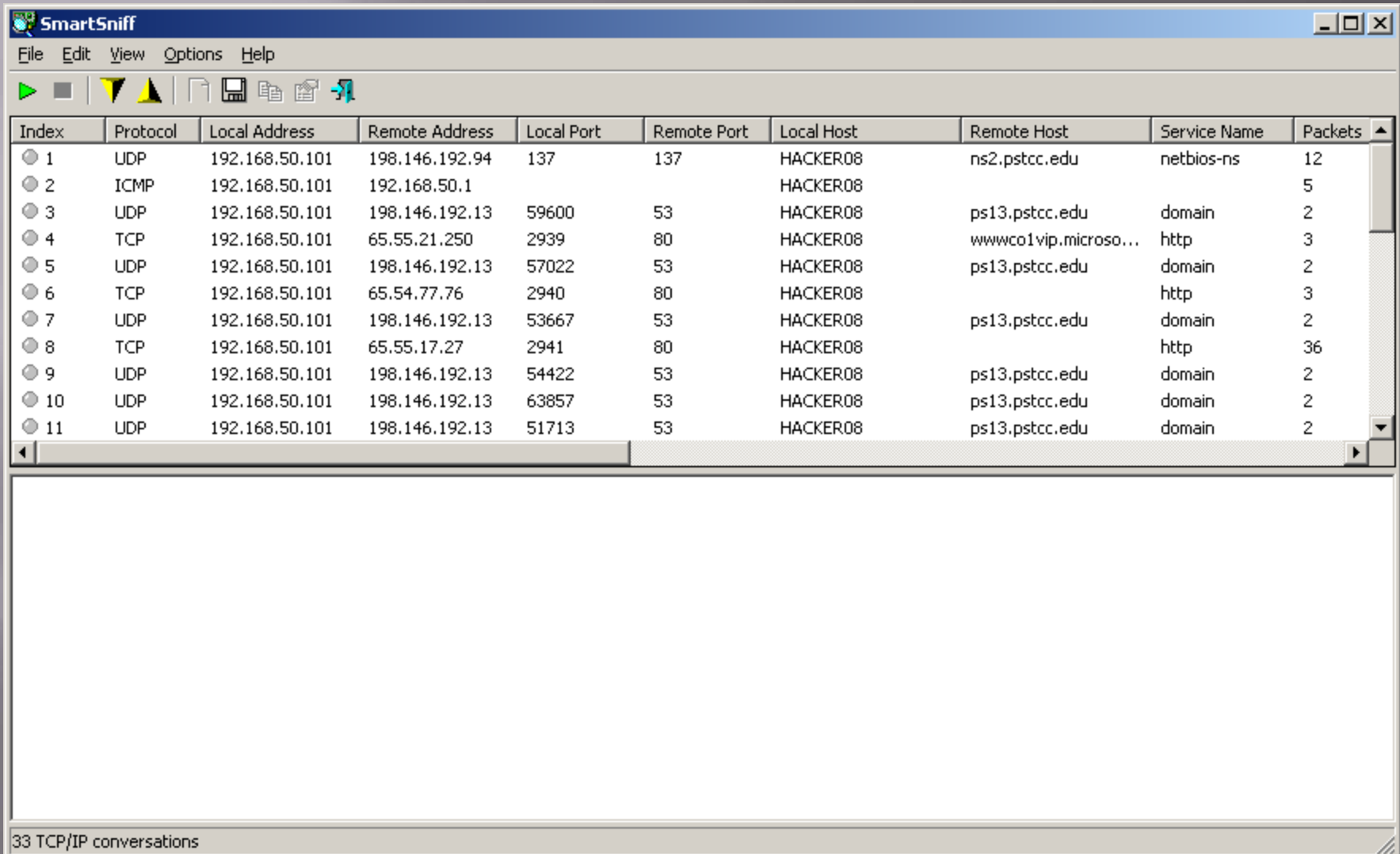
User File Pass File

Positive Authentication Results

Target	Type	Username	Password
Target www.pstcc.edu verified			
Password file words.txt is not valid!			

Idle

SmartSniff



The image shows a screenshot of the SmartSniff application window. The window title is "SmartSniff" and it has a menu bar with "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for play, stop, refresh, save, print, and help. The main area contains a table with 11 rows of network traffic data. The table has columns for Index, Protocol, Local Address, Remote Address, Local Port, Remote Port, Local Host, Remote Host, Service Name, and Packets. The data shows various protocols including UDP, ICMP, and TCP, with destinations like HACKER08, ns2.pstcc.edu, and ps13.pstcc.edu. A status bar at the bottom indicates "33 TCP/IP conversations".

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host	Service Name	Packets
1	UDP	192.168.50.101	198.146.192.94	137	137	HACKER08	ns2.pstcc.edu	netbios-ns	12
2	ICMP	192.168.50.101	192.168.50.1			HACKER08			5
3	UDP	192.168.50.101	198.146.192.13	59600	53	HACKER08	ps13.pstcc.edu	domain	2
4	TCP	192.168.50.101	65.55.21.250	2939	80	HACKER08	wwwco1vip.microso...	http	3
5	UDP	192.168.50.101	198.146.192.13	57022	53	HACKER08	ps13.pstcc.edu	domain	2
6	TCP	192.168.50.101	65.54.77.76	2940	80	HACKER08		http	3
7	UDP	192.168.50.101	198.146.192.13	53667	53	HACKER08	ps13.pstcc.edu	domain	2
8	TCP	192.168.50.101	65.55.17.27	2941	80	HACKER08		http	36
9	UDP	192.168.50.101	198.146.192.13	54422	53	HACKER08	ps13.pstcc.edu	domain	2
10	UDP	192.168.50.101	198.146.192.13	63857	53	HACKER08	ps13.pstcc.edu	domain	2
11	UDP	192.168.50.101	198.146.192.13	51713	53	HACKER08	ps13.pstcc.edu	domain	2

33 TCP/IP conversations

Zenmap

The screenshot shows the Zenmap application window. At the top, there are menu options: Scan, Tools, Profile, and Help. Below the menu, the Target field is set to 192.168.50.251 and the Profile is Intense scan plus UDP. A Scan button and a Cancel button are visible. The Command field contains the following text: `nmap -sS -sU -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.50.251`.

On the left side, there are tabs for Hosts and Services. Under the Hosts tab, a list of hosts is shown: 192.168.50.101 and 192.168.50.251. At the bottom left, there is a Filter Hosts button.

The main area displays the Nmap Output. The output text is as follows:

```
nmap -sS -sU -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.50.251

Starting Nmap 5.10BETA1 ( http://nmap.org ) at
2010-05-20 11:39 Eastern Daylight Time
NSE: Loaded 35 scripts for scanning.
Initiating ARP Ping Scan at 11:39
Scanning 192.168.50.251 [1 port]
Completed ARP Ping Scan at 11:39, 0.06s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:39
Completed Parallel DNS resolution of 1 host. at 11:39,
0.00s elapsed
Initiating SYN Stealth Scan at 11:39
Scanning 192.168.50.251 [1000 ports]
Discovered open port 23/tcp on 192.168.50.251
Discovered open port 443/tcp on 192.168.50.251
Discovered open port 80/tcp on 192.168.50.251
Discovered open port 14000/tcp on 192.168.50.251
Discovered open port 7627/tcp on 192.168.50.251
Discovered open port 280/tcp on 192.168.50.251
Discovered open port 631/tcp on 192.168.50.251
Discovered open port 9100/tcp on 192.168.50.251
Discovered open port 515/tcp on 192.168.50.251
Completed SYN Stealth Scan at 11:39, 1.27s elapsed
(1000 total ports)
Initiating UDP Scan at 11:39
Scanning 192.168.50.251 [1000 ports]
Discovered open port 5353/udp on 192.168.50.251
Discovered open port 111/udp on 192.168.50.251
Discovered open port 2049/udp on 192.168.50.251
Completed UDP Scan at 11:39, 1.48s elapsed (1000 total
ports)
Initiating Service scan at 11:39
Scanning 16 services on 192.168.50.251
Discovered open port 161/udp on 192.168.50.251
Discovered open/filtered port 161/udp on 192.168.50.251
```

Zenmap, continued

The screenshot shows the Zenmap application window. The title bar reads "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The "Target:" field contains "192.168.50.251" and the "Profile:" dropdown is set to "Intense scan plus UDP". The "Command:" field displays the command: `nmap -sS -sU -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.50.251`. Below the command field are tabs for "Hosts" and "Services". The "Services" tab is active, showing a list of services on the left: ftp, printer, http, tcpwrapped, unknown, jetdirect, telnet, mdns, snmp, svrloc, rpcbind, and netbios-ns (highlighted). A "Filter Hosts" button is at the bottom left. The main area shows the "Nmap Output" tab with a table of results:

Hostname	Port	Protocol	State	Version
192.168.50.251	137	udp	open filtered	

Zenmap, continued #2

The screenshot shows the Zenmap application window. The title bar reads "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The "Target" field contains "192.168.50.251" and the "Profile" dropdown is set to "Intense scan plus UDP". The "Command" field displays the full nmap command: `nmap -sS -sU -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.50.251`. Below the command field are tabs for "Hosts" and "Services". A list of services is shown on the left, including ftp, printer, http, tcpwrapped, unknown, jetdirect, telnet, mdns, snmp, svrloc, rpcbind, and netbios-ns. The main area shows the "Nmap Output" for the target IP. It includes sections for "Comments", "Host Status", and "Addresses".

Target: 192.168.50.251 Profile: Intense scan plus UDP Scan Cancel

Command: nmap -sS -sU -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.50.251

Hosts Services

Service

- ftp
- printer
- http
- tcpwrapped
- unknown
- jetdirect
- telnet
- mdns
- snmp
- svrloc
- rpcbind
- netbios-ns

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

192.168.50.251

- Comments**
- Host Status**
 - State: up
 - Open ports: 17
 - Filtered ports: 3
 - Closed ports: 1982
 - Scanned ports: 2000
 - Up time: Not available
 - Last boot: Not available
- Addresses**
 - IPv4: 192.168.50.251
 - IPv6: Not available
 - MAC: 00:1A:4B:1B:EE:82

Metasploit

```
bash
[*] Configuring multi-user permissions for first run...
[*] Configuring the initial user environment...

      ##          ###      ##      ##
## ##  #### #####  ####  #####  ##     ###  ##
##### ##  ##  ##   ##   ##  ##  ##  ##  ##  ##  ##
##### #####  ##  #####  ####  ##  ##  ##  ##  ##
## # ##   ##  ##  ##  ##  #####  ##  ##  ##  ##  ##
##  ##  #### ##   #####  #####  ##  ####  ####  ####

                    #
= [ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --- [ 481 exploits - 220 auxiliary
+ -- --- [ 192 payloads - 22 encoders - 8 nops
= [ svn r7957 updated 148 days ago (2009.12.23)

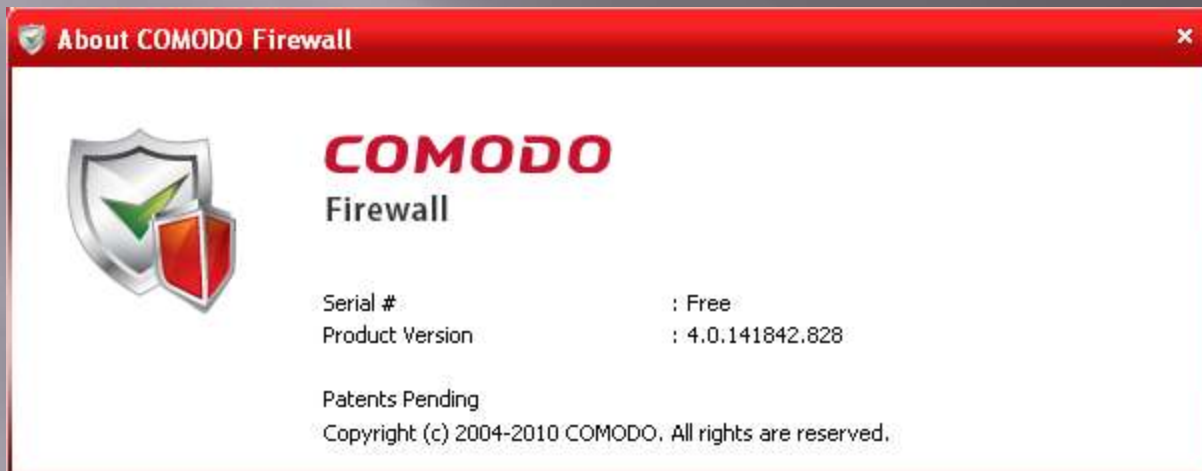
Warning: This copy of the Metasploit Framework was last updated 148 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
      http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
msf > ?

Core Commands
=====

  Command      Description
  -----
  ?             Help menu
  back          Move back from the current context
  banner        Display an awesome metasploit banner
  cd            Change the current working directory
  color         Toggle color
  connect       Communicate with a host
  exit          Exit the console
  help          Help menu
  info          Displays information about one or more module
```

Comodo



Comodo

COMODO Firewall

[Summary](#) Firewall Defense+ More...

Summary

System Status
All systems are active and running.
You do not need to perform any actions at this time.

Network Defense
The Firewall has blocked [0](#) intrusion attempt(s) so far.
The Firewall security level is set to [Block All Mode](#)
 [0](#) inbound connection(s)
 [0](#) outbound connection(s)
[Restore All Activities](#)

Proactive Defense
The Defense+ has blocked [108](#) suspicious attempt(s) so far.
The Defense+ security level is set to [Paranoid Mode](#)
 [53](#) application(s) are active and running in the memory.
 [5](#) file(s) are [waiting for your review](#)

Highlights

Upgrade your Security Today! Try FREE for 30 days! Get Full Protection Against Viruses and Improve your PC Speed!

[Learn More](#)

Subscription Information

Subscription Status: [Activate Now](#)
Guarantee Status: [Not Activated](#)

[Live Support](#)

Traffic

All systems are active and running.

Comodo

Active Process List

Application	PID	Company	User Name
Windows Operating System	0		NT AUTHORITY\SY...
System	4		NT AUTHORITY\SY...
smss.exe	788	Microsoft Corporation	NT AUTHORITY\SY...
csrss.exe	864	Microsoft Corporation	NT AUTHORITY\SY...
winlogon.exe	1256	Microsoft Corporation	NT AUTHORITY\SY...
services.exe	1300	Microsoft Corporation	NT AUTHORITY\SY...
CLPSLS.exe	1484	COMODO	NT AUTHORITY\SY...
ati2evxx.exe	1512	ATI Technologies Inc.	NT AUTHORITY\SY...
svchost.exe	1532	Microsoft Corporation	NT AUTHORITY\SY...
naPrdMgr.exe	3536	McAfee, Inc.	NT AUTHORITY\SY...
wmiprvse.exe	3212	Microsoft Corporation	NT AUTHORITY\SY...
svchost.exe	1592	Microsoft Corporation	NT AUTHORITY\SY...
cmdagent.exe	612		NT AUTHORITY\SY...
svchost.exe	640	Microsoft Corporation	NT AUTHORITY\SY...
MsMpEng.exe	652	Microsoft Corporation	NT AUTHORITY\SY...
svchost.exe	976	Microsoft Corporation	NT AUTHORITY\SY...
svchost.exe	1660	Microsoft Corporation	NT AUTHORITY\SY...

[Get Live Support](#) Close

Comodo

<input type="checkbox"/> All ?	File Path	Company	Created	Submit...
<input type="checkbox"/>	C:\Program Files\ATI Technologies\ATI Control Panel\... ATI Technol...	ATI Technol...	4/29/2...	4/29/2...
<input type="checkbox"/>	C:\Program Files\CyberLink\PowerDVD\DVDLauncher....	CyberLink C...	4/29/2...	4/29/2...
<input type="checkbox"/>	C:\Program Files\Common Files\InstallShield\UpdateS...	InstallShield ...	4/29/2...	4/29/2...
<input type="checkbox"/>	C:\Program Files\Common Files\InstallShield\UpdateS...	InstallShield ...	4/29/2...	4/29/2...
<input type="checkbox"/>	C:\WINDOWS\System32\DLA\DLACTRLW.EXE	Sonic Solutions	4/29/2...	4/29/2...

Buttons: Add, Move to, Remove, Lookup..., Submit..., Delete File, Purge

Bottom: [Get Live Support](#) / [Read the Privacy Statement](#) Close

Comodo

COMODO Firewall

Summary

Firewall

Defense+

More...

Firewall Tasks

Common Tasks

Advanced



View Firewall Events

This section allows you to view a record of the events and alerts triggered by possible attacks on your computer.



Define a New Trusted Application

This shortcut represents a convenient way to create an automatic Allow rule for applications that you trust.



Define a New Blocked Application

This shortcut represents a convenient way to create an automatic Deny rule for applications that you do not trust.



Stealth Ports Wizard

This wizard allows you to create a set of global firewall rules, which will affect your computer's visibility from other computers.



View Active Connections

View which applications are currently connecting to the Internet along with the IP, Port, Protocol and Traffic level of the connection.



My Blocked Network Zones

Allows you to define which addresses or network zones your computer should not communicate with. For example, spyware sites.

✓ All systems are active and running.

Comodo

COMODO Firewall

System is trying to **connect to the Internet**. What would you like to do?

Application: System
Remote: 198.146.192.92 - UDP
Port: nbname(137)

Security Considerations


System is a **safe** application. You can safely allow this request.

Allow this request [Fewer Options](#) ▲
 Block this request
 Treat this application as
 Remember my answer

[? Get Live Support](#)

COMODO Defense+

searchindexer.exe is trying to **execute** searchfilterhost.exe. What would you like to do?




Security Considerations

searchindexer.exe is a **safe** application. searchfilterhost.exe is **also a safe** application. You can safely allow this request.


Allow this request [Fewer Options](#) ▲
 Block this request
 Treat this application as
 Create a "Windows" system restore point
 Submit the files to COMODO for analysis
 Remember my answer

[? Get Live Support](#)

Comodo

**COMODO Defense+**


wordpad.exe is trying to **access a protected pseudo-COM interface**. What would you like to do?



wordpad.exe

Security Considerations


wordpad.exe is a **safe** application. It is **about to access the protected pseudo-COM interface \RPC Control\spoolss**. You can safely allow this request.

Create a "Windows" system restore point [More Options](#) 


Submit the files to COMODO for analysis

Remember my answer

[? Get Live Support](#)

**COMODO Defense+**


searchindexer.exe is trying to **execute** searchprotocolhost.exe. What would you like to do?



searchindexer.exe searchprotocolhost.exe

Security Considerations

searchindexer.exe is a **safe** application. searchprotocolhost.exe is **also a safe** application. You can safely allow this request.

Create a "Windows" system restore point [More Options](#) 

Submit the files to COMODO for analysis

Remember my answer!

[? Get Live Support](#)

Logs

- Logs per Module
 - Antivirus Events
 - Firewall Events
 - Defense+ Events**
 - Other Logs
 - Alerts Displayed
 - Tasks Launched
 - Configuration Changes

Date Filter

May, 2010						
M	T	W	T	F	S	S
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						
June, 2010						
M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

Firewall Events Defense+ Events

Date	Application	Flags	Target	Alert
5/17/2010 8:55:50 AM	C:\WINDOWS\system32\userinit.exe	Modify Key, Safe	HKUS\5-1-5-21-3307791122-1510140...	Related alert
5/17/2010 8:56:05 AM	C:\Program Files\ATI Technologies...	Sandboxed As	Limited	Related alert
5/17/2010 8:56:11 AM	C:\Program Files\CyberLink\Power...	Direct Keyboard Access		
5/17/2010 8:56:21 AM	C:\WINDOWS\system32\dla\DLAC...	Modify File	C:\WINDOWS\system32\dla\DLA.INI	
5/17/2010 8:56:25 AM	C:\Program Files\CyberLink\Power...	Sandboxed As	Limited	Related alert
5/17/2010 8:56:46 AM	C:\PROGRA~1\COMMON~1\INST...	Sandboxed As	Limited	Related alert
5/17/2010 8:56:51 AM	C:\Program Files\Common Files\Ins...	Sandboxed As	Limited	Related alert
5/17/2010 8:57:04 AM	C:\WINDOWS\System32\DLA\DLA...	Sandboxed As	Limited	Related alert
5/17/2010 8:57:21 AM	C:\WINDOWS\system32\searchind...	Modify Key	HKLM\SYSTEM\ControlSet001\Service...	
5/17/2010 8:57:27 AM	C:\WINDOWS\system32\searchind...	Modify Key	HKLM\SYSTEM\ControlSet001\Service...	
5/17/2010 8:57:30 AM	C:\Program Files\Network Associat...	Create Process, Safe	C:\Program Files\Network Associat...	Related alert
5/17/2010 8:57:33 AM	C:\WINDOWS\system32\searchind...	Modify Key	HKLM\SYSTEM\ControlSet001\Service...	
5/17/2010 8:57:33 AM	C:\WINDOWS\system32\userinit.exe	Modify Key	HKUS\5-1-5-21-3307791122-1510140...	
5/17/2010 8:57:33 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\WINDOWS\system32\CatRoot2...	
5/17/2010 8:57:37 AM	C:\Program Files\Java\jre6\bin\jqs...	Modify Key, Safe	HKLM\SYSTEM\ControlSet001\Service...	Related alert
5/17/2010 8:57:41 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:41 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:43 AM	C:\Program Files\McAfee\VirusSca...	Modify Key, Safe	HKLM\SYSTEM\ControlSet???\Services...	Related alert
5/17/2010 8:57:46 AM	C:\Program Files\McAfee\VirusSca...	Modify Key, Safe	HKLM\SYSTEM\ControlSet???\Services...	Related alert
5/17/2010 8:57:47 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:47 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:48 AM	C:\WINDOWS\system32\mfefvtps....	Modify Key, Safe	HKLM\SYSTEM\ControlSet???\Services...	Related alert
5/17/2010 8:57:49 AM	C:\WINDOWS\system32\ymnat.exe	Modify File	\Device\Afd\Endpoint	Related alert
5/17/2010 8:57:53 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:53 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:53 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	
5/17/2010 8:57:53 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\WINDOWS\SoftwareDistributio...	
5/17/2010 8:57:53 AM	C:\WINDOWS\system32\fxssvc.exe	Modify Key, Safe	HKLM\SYSTEM\ControlSet001\Service...	Related alert
5/17/2010 8:57:58 AM	C:\Program Files\VMware\VMware ...	Modify File	\Device\Afd\Endpoint	Related alert
5/17/2010 8:57:59 AM	C:\WINDOWS\system32\searchind...	Modify File	C:\Documents and Settings\All Use...	

Comodo

The screenshot shows the 'COMODO Firewall - Log Viewer' application window. The interface includes a menu bar with 'File' and 'View', a filter section for 'Today', 'Current Week', 'Current Month', and 'Entire Period', and a 'Logs' sidebar on the left. The sidebar lists various log categories, with 'Firewall Events' selected. Below the sidebar is a 'Date Filter' set to 'May, 2010'. The main area displays a table of firewall events with columns for Date, Application, Action, Direction, Protocol, Source IP, Source Port, Destination IP, Destination Port, and Alert. The table contains six records, all from the 'System' application, with the first record being 'Asked' and the others 'Blocked'.

Date	Application	Action	Direction	Protocol	Source IP	Sourc...	Destination IP	Destin...	Alert
5/17/2010 9:14:46 AM	System	Asked	Out	UDP	192.168.50.112	137	198.146.192.92	137	Related alert
5/17/2010 9:16:13 AM	System	Blocked	Out	UDP	192.168.50.112	137	198.146.192.92	137	
5/17/2010 9:16:51 AM	System	Blocked	Out	UDP	192.168.50.112	137	198.146.192.92	137	
5/17/2010 9:16:54 AM	System	Blocked	Out	UDP	192.168.50.112	137	198.146.192.92	137	
5/17/2010 9:17:00 AM	System	Blocked	Out	UDP	192.168.50.112	137	198.146.192.92	137	
5/17/2010 9:17:03 AM	System	Blocked	Out	UDP	192.168.50.112	137	198.146.192.92	137	

Records: 6

Wireshark

12 8.827605 192.168.50.127 192.168.50.255 BROWSER Local Master Announcement HACKER09, Wor...

Destination port: netbios-dgm (138)
Length: 209

- Checksum: 0x7da8 [validation disabled]
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)
- SMB Mailslot Protocol
- Microsoft windows Browser Protocol
 - Command: Local Master Announcement (0x0f)
 - Update Count: 0
 - Update Periodicity: 12 minutes
 - Host Name: HACKER09
 - OS Major Version: 5
 - OS Minor Version: 1
 - Server Type: 0x00051003
 - Browser Protocol Major Version: 15
 - Browser Protocol Minor Version: 1
 - Signature: 0xaa55
 - Host Comment:

0000	ff ff ff ff ff ff 00 1a a0 a9 35 c5 08 00 45 005...E.
0010	00 e5 b1 1e 00 00 80 11 a2 1a c0 a8 32 7f c0 a82...
0020	32 ff 00 8a 00 8a 00 d1 7d a8 11 0e b3 2a c0 a8	2..... }....*..
0030	32 7f 00 8a 00 bb 00 00 20 45 49 45 42 45 44 45	2..... EIEBEDE
0040	4c 45 46 46 43 44 41 44 4a 43 41 43 41 43 41 43	LEFFCDAD JCACACAC
0050	41 42 41 42 41 42 41 42 41 00 20 46 44 45 46 45	ACACACAC A EDEFF

Wireshark

The image shows a screenshot of the Wireshark network protocol analyzer. The main window, titled "Conversations: CSEC-1.pcap", displays a list of "Ethernet Conversations". Below this, a smaller window titled "CSEC-1.pcap - Wireshark" is open, showing the main interface with a menu bar, toolbar, and a packet list table.

Conversations: CSEC-1.pcap

Ethernet: 7 | Fibre Channel | FDDI | IPv4: 4 | IPX | JXTA | NCP | RSVP | SCTP | TCP | Token Ring | UDP: 1 | USB | WLAN

Ethernet Conversations

Address A	Address B	Packets -	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B
Cisco_21:d6:02	Cisco_21:d6:02	1	60	1	60	0	0	3.991857000	0.0000	N/A
Cisco_31:66:3f	IPv4mcast_00:00:01	1	60	1	60	0	0	5.326781000	0.0000	N/A
Dell_a9:35:c5	Broadcast	1	243	1	243	0	0	8.827605000	0.0000	N/A
Dell_a9:2f:20	IPv4mcast_7f:ff:fa	1	46	1	46	0	0	8.844760000	0.0000	N/A
Cisco_31:66:3f	IPv4mcast_00:00:0d	1	68	1	68	0	0	10.060650000	0.0000	N/A
Cisco_21:d6:02	Spanning tree (for bridge) 00:0...	6	260	6	260	0	0	0.000000000	10.0186	287.46
Cisco_31:66:3f	CGMP									

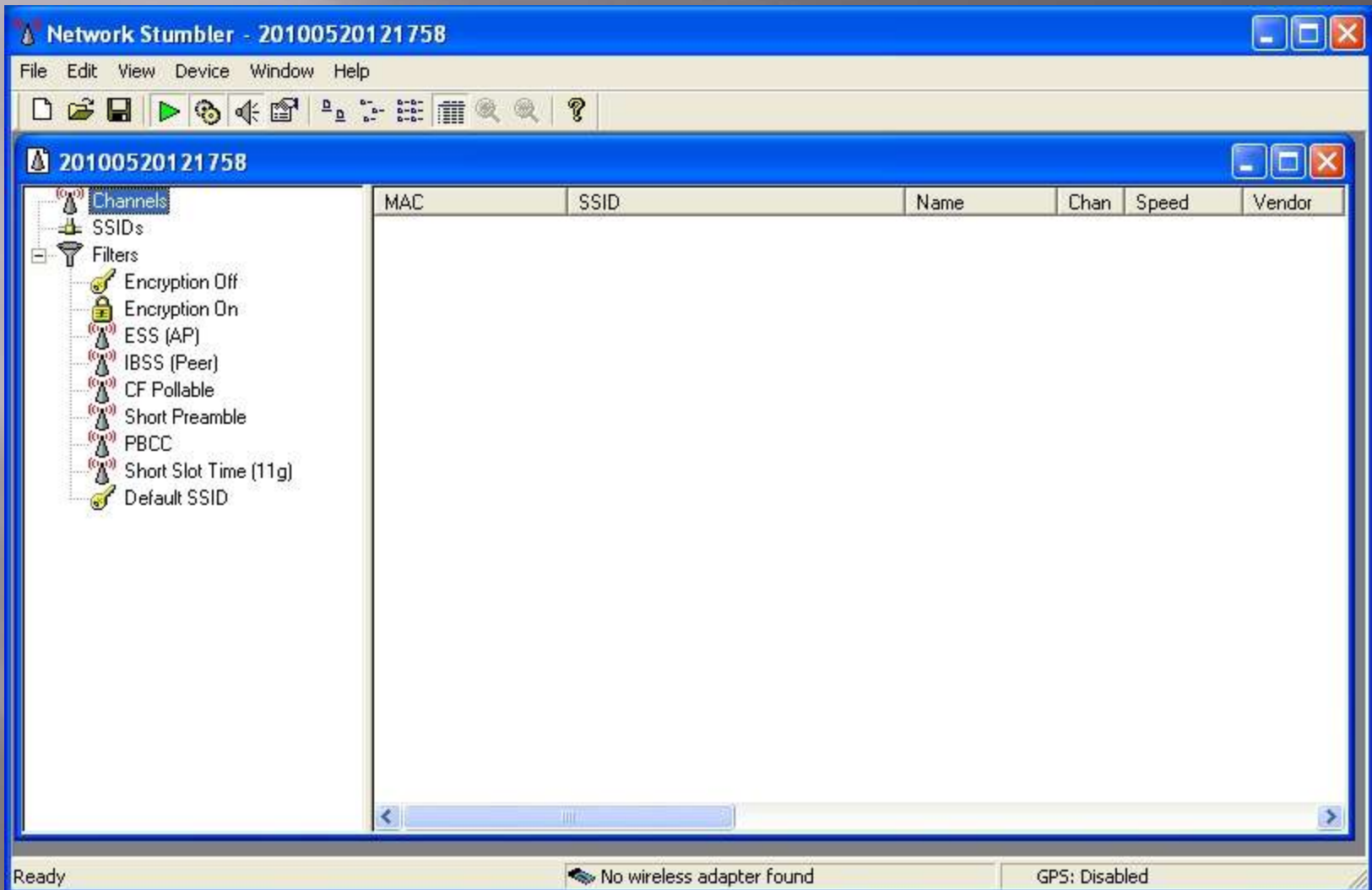
CSEC-1.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
-------	------	--------	-------------	----------	------

NetStumbler



Ettercap

ettercap NG-0.7.3

Start Targets Hosts View Mitm Filters Logging Plugins

Targets X Host List X

IP Address	MAC Address	Description
192.168.50.1	00:1C:58:31:66:3F	
192.168.50.2	00:19:B9:C9:F1:AF	
192.168.50.101	00:10:18:2E:72:E1	
192.168.50.102	00:04:75:F5:28:38	
192.168.50.104	00:1A:A0:A9:36:53	
192.168.50.112	00:1A:A0:C5:3C:FC	
192.168.50.114	00:1A:A0:A9:31:F5	
192.168.50.117	00:1A:A0:A9:2F:20	
192.168.50.127	00:1A:A0:A9:35:C5	
192.168.50.137	00:1A:A0:A9:2F:27	
192.168.50.141	00:1A:A0:A9:A7:26	
192.168.50.142	00:1A:A0:A9:2F:0B	
192.168.50.145	00:1A:A0:A9:36:22	
192.168.50.148	00:1A:A0:A9:38:20	

Delete Host Add to Target 1 Add to Target 2

{Device}\NPF_{1B93230B-0D10-495C-B89A-1F5E53B2D69E} -> 00:1A:A0:A9:2F:20 192.168.50.117
255 255 255 0

Angry IP Scanner

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.50.0 to 192.168.50.255 IP Range

Hostname: PINK08 IP /24 Start

IP	Ping	Hostname	Ports [0+]
192.168.50.1	[n/a]	[n/s]	[n/s]
192.168.50.2	0 ms	NETW1	[n/s]
192.168.50.3	[n/a]	[n/s]	[n/s]
192.168.50.4	[n/a]	[n/s]	[n/s]
192.168.50.5	[n/a]	[n/s]	[n/s]
192.168.50.6	[n/a]	[n/s]	[n/s]
192.168.50.7	[n/a]	[n/s]	[n/s]
192.168.50.8	[n/a]	[n/s]	[n/s]
192.168.50.9	[n/a]	[n/s]	[n/s]
192.168.50.10	[n/a]	[n/s]	[n/s]
192.168.50.11	[n/a]	[n/s]	[n/s]
192.168.50.12	[n/a]	[n/s]	[n/s]

Ready Display: All Threads: 0

Hackpack

The screenshot shows a window titled "Foundstone HackPack" with a blue title bar. The window content is divided into several sections:

- Header:** "Foundstone | HackPack v1.0" on the left and "About HackPack" on the right.
- Left Navigation Panel:** A list of tools and categories including "Foundstone", "Foundstone News and Events", "SSLDigger" (selected), "CookieDigger", "WSDigger", "SecureUML Template", "Validator NET", "NETMon", "NET Security Toolkit", "SiteScope", "Hacme Travel", "Hacme Bank", "SiteDigger", "Hacme Books", "Hacme Shipping", "Web", "Network", and "Passwords".
- Main Content Area:**
 - Tool Name:** SSLDigger
 - Current Version:** 1.02
 - Home Page:** <http://www.foundstone.com/resources/proddesc/sitedigger.htm>
 - Platform:** Windows
 - Description:** SSLDigger is a tool to assess the strength of SSL servers by testing the ciphers supported. Some of these ciphers are known to be insecure.
 - Buttons:** "Install Latest..."
 - Navigation:** "News" and "Articles" tabs.

Hackpack: WSDigger

The screenshot shows a window titled "Foundstone HackPack" with a blue title bar. The main content area is dark-themed and displays information for the "WSDigger" tool. On the left, there is a vertical list of tool categories and names, with "WSDigger" selected. The main area shows the tool's name, home page URL, platform, and a detailed description. A "News" section is partially visible at the bottom.

Foundstone HackPack v1.0 About HackPack

Foundstone News and Events
SSLDigger
CookieDigger
WSDigger
SecureUML Template
Validator NET
NETMon
NET Security Toolkit
SiteScope
Hacme Travel
Hacme Bank
SiteDigger
Hacme Books
Hacme Shipping

Tool Name: WSDigger Current Version: 1.0
Home Page: <http://www.foundstone.com/resources/proddesc/wsdigger.htm>
Platform: Windows

Description
WSDigger is a free open source tool designed by Foundstone to automate black-box web services security testing (also known as penetration testing). WSDigger is more than a tool, it is a web services testing framework. Version one of this framework contains sample attack plug-ins for SQL injection, cross site scripting and XPATH injection attacks. A web service vulnerable to XPATH injection is provided as an example with the tool. By releasing the framework as an open-source tool, users are

News
Articles

Web
Network
Passwords