# SuperScan

SuperScan is a TCP port scanner, pinger and hostname resolver

It can:-

- perform simple ping tests to tell whether a remote computer is alive
- resolve hostnames into IP addresses and reverse lookup IP addresses into hostnames
- attempt to connect to other computers on a TCP network to see what services they are running
- read responses from connected hosts
- scan from a range of addresses and ports
- scan from a list of ports
- scan from selected ports from a list
- scan a list of hostnames contained in a text file

# Release History

### Version 2.06

Cosmetic changes to the scan results window; the banner tree icon (shown when data is read from a host) has been changed to make it a little easier to spot.

The port list format has changed again, sorry. I've done away with the label since it was rather redundant having both the label and a description.

In the port list configuartion window I've added a Merge button to allow you to merge port lists together.

### Version 2.05

Many additions and changes including:

- Resizable window. The window's controls resize and reposition to fit the window.
- The program will now fit (just) into an 800x600 screen using large fonts.
- Can choose to read response data from scanned hosts.
- Selectable probe data per port to force a response from a host.
- Selectable read timeout.
- Ignore IP 255 option.
- Load and save selectable port lists.
- Quickly select from previous 4 port lists.
- All main program options and settings saved on exit and restored on startup.
- Cosmetic user interface changes.
- Several bug fixes

### Version 2.04

Added a transmission speed slider. Some people have reported adverse effects of the program running at full speed, most probably due to the unmetered and unrestricted ICMP ping packet sending and also due to problems with Microsoft's async DNS lookup functions.

### Version 2.03

The program now has a proper help file (you're looking at it now) rather than the simple *readme.txt* text file. I debated whether it was worth while since I like to keep the program package size to a minimum but it does look much nicer.

The program now requires Winsock 2 to operate. Version 2.01 was meant to work with Winsock 1.1 but due to a bug (oops :-) it still required Winsock 2.

The hostname lookup code has been made more robust. Have hopefully fixed the *64* limit problem when resolving hostnames extracted from a text file.

Resolving hostnames after extracting addresses from a text file will now be considerably faster for numeric addresses.

### Version 2.02

Never publicly released

### Version 2.01

Added the Interfaces button. This feature requires Winsock 2.

### Version 2.00

Big rewrite. All options totally asynchronous and the pinger class rewritten (properly ;-). Lots of new features.

### Version 1.00

First version. Crude scanner. Slow.

# Requirements

This program will run on computers with Windows 95, Windows 98, Windows NT 4.0 and Windows 2000 with the TCP protocol installed.

For Windows 95 users, if the program claims that a required DLL, WS2_32.DLL was not found then you will need to install the Windows Sockets 2 update. This can be found on Microsoft's web site at

http://www.microsoft.com/windows/downloads/bin/W95ws2setup.exe

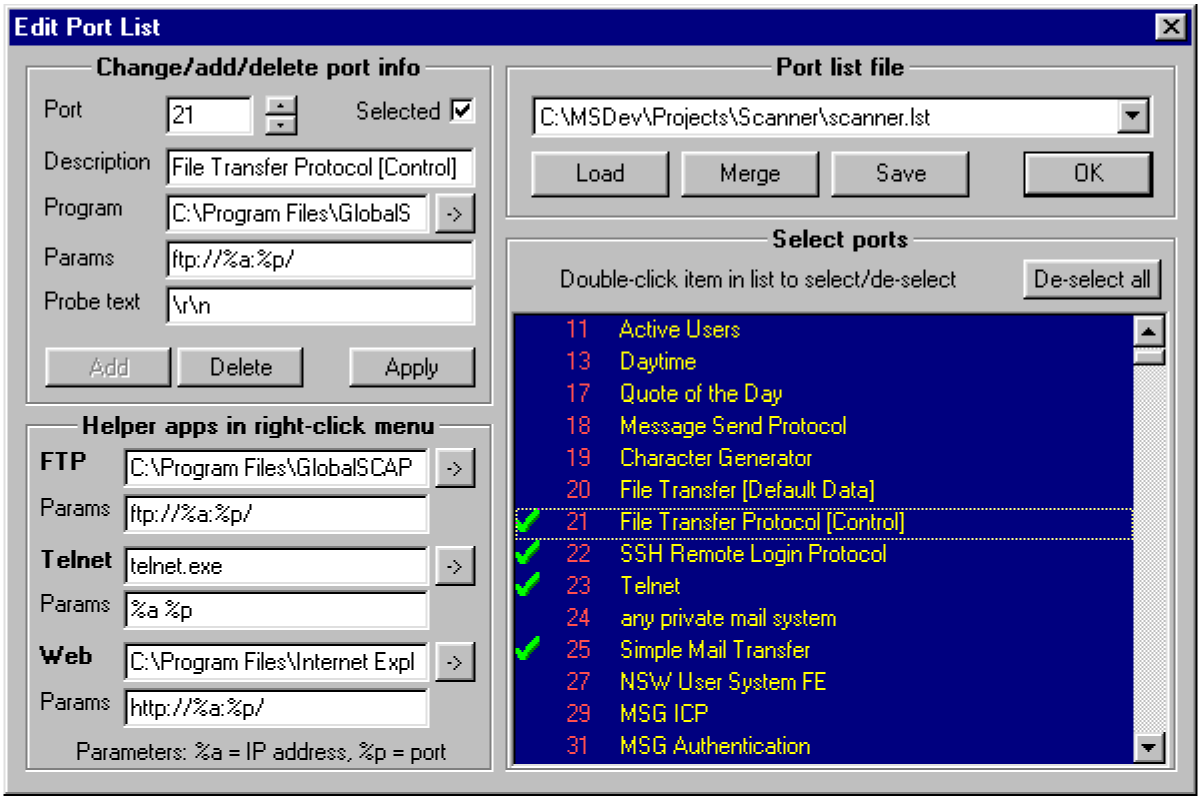
(986K) or by searching for Winsock 2 update for Windows 95 from their web site.

For all operating systems you will require the ICMP.DLL file although all Windows versions should ship with it.

# Quick Start

To perform a port scan of selected ports in a given IP range:

- Click the Port list setup button.
- Select/deselect the ports you want to scan from the scrolling list.
- Click OK to get back to the main window.
- Enter a hostname/IP in the Hostname Lookup box and click Lookup
- Adjust the IP range, e.g. click the 1..255 button for a class C range.
- Adjust the ping and connect timeouts and transmission speed if necessary.
- Make sure Only scan/show responding ping hosts is checked.
- Make sure All selected ports in list is selected.
- Click Start.
- Wait for the scan to end (all lights turn red, icon stops animating).
- Click the Prune button to remove IPs with no open ports.
- Click Expand all to show all open ports discovered.
- Right-click on open ports in the list to view with the given application.



Port: 21 Selected ☑

Description: File Transfer Protocol [Control]

Program: C:\Program Files\GlobalS

Params: ftp://%a:%p/

Probe text: \r\n

**FTP**: C:\Program Files\GlobalSCAP

Params: ftp://%a:%p/

**Telnet**: telnet.exe

Params: %a %p

**Web**: C:\Program Files\Internet Expl

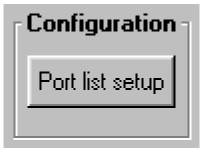
Params: http://%a:%p/

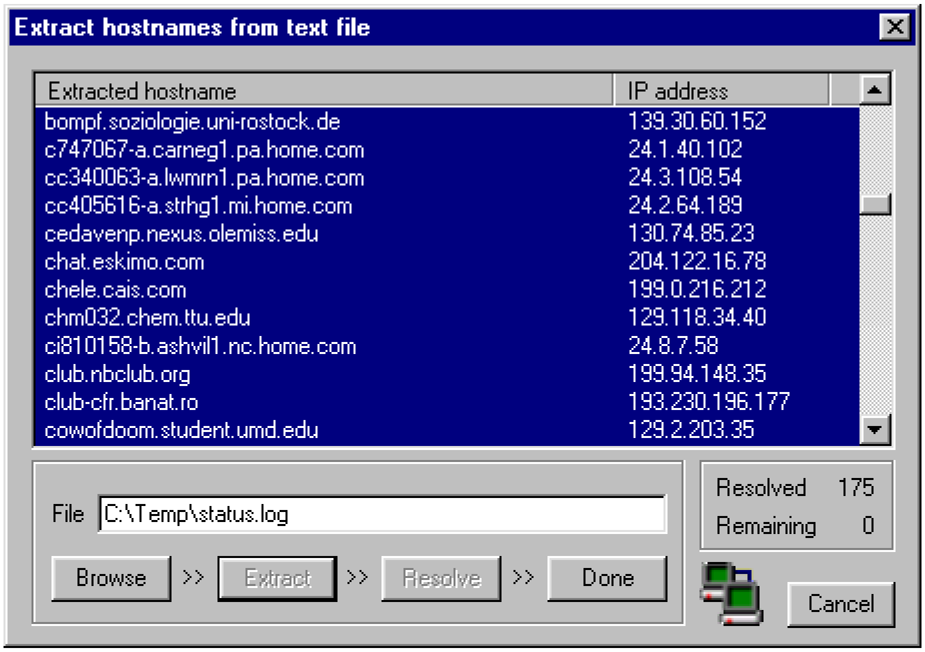
Parameters: %a = IP address, %p = port

C:\MSDev\Projects\Scanner\scanner.lst

Double-click item in list to select/de-select

| | | |
|---|---|---|
| | 11 | Active Users |
| | 13 | Daytime |
| | 17 | Quote of the Day |
| | 18 | Message Send Protocol |
| | 19 | Character Generator |
| | 20 | File Transfer [Default Data] |
| ✓ | 21 | File Transfer Protocol [Control] |
| ✓ | 22 | SSH Remote Login Protocol |
| ✓ | 23 | Telnet |
| | 24 | any private mail system |
| ✓ | 25 | Simple Mail Transfer |
| | 27 | NSW User System FE |
| | 29 | MSG ICP |
| | 31 | MSG Authentication |


Configuration
Port list setup



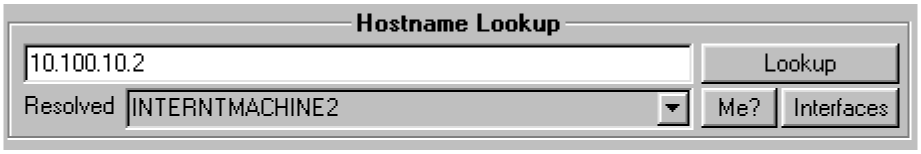
| Extracted hostname | IP address |
|---|---|
| bompf.soziologie.uni-rostock.de | 139.30.60.152 |
| c747067-a.carneg1.pa.home.com | 24.1.40.102 |
| cc340063-a.lwmrn1.pa.home.com | 24.3.108.54 |
| cc405616-a.strhg1.mi.home.com | 24.2.64.189 |
| cedavenp.nexus.olemiss.edu | 130.74.85.23 |
| chat.eskimo.com | 204.122.16.78 |
| chele.cais.com | 199.0.216.212 |
| chm032.chem.ttu.edu | 129.118.34.40 |
| ci810158-b.ashvil1.nc.home.com | 24.8.7.58 |
| club.nbclub.org | 199.94.148.35 |
| club-cfr.banat.ro | 193.230.196.177 |
| cowofdoom.student.umd.edu | 129.2.203.35 |

File C:\Temp\status.log

Resolved 175

Remaining 0

# Hostname lookup section



10.100.10.2

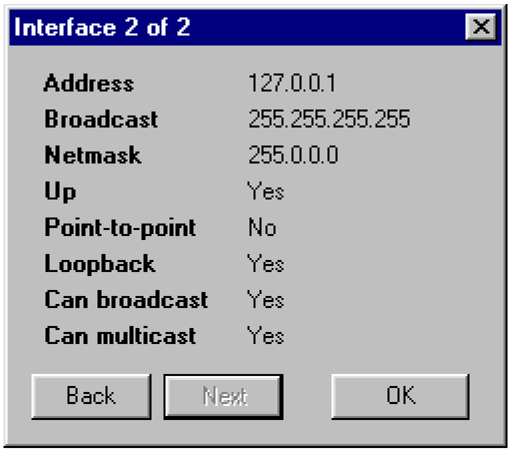
Resolved INTERNTMACHINE2

Enter a hostname/IP in the Hostname Lookup box and click Lookup.

To find your own current IP, click the Me? button.

If the hostname/IP can be resolved the Start and Stop IP boxes in the IP section will contain the resolved IP address and the Resolved box will show the hostname or [Unknown] if not found. The drop-down box on the Resolved section will contain any additional aliases for the hostname.

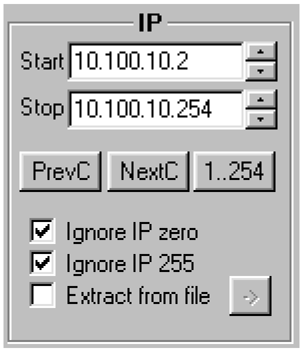
To show the currently active interfaces (IP addresses) assigned to your computer you can click on the Interfaces button to bring up this window.



| | |
|---|---|
| **Address** | 127.0.0.1 |
| **Broadcast** | 255.255.255.255 |
| **Netmask** | 255.0.0.0 |
| **Up** | Yes |
| **Point-to-point** | No |
| **Loopback** | Yes |
| **Can broadcast** | Yes |
| **Can multicast** | Yes |

Click the Next and Back buttons to move through the list. The currently showing IP address will be transferred into the IP section of the main window. Click OK to close the window.

# IP section



IP

Start 10.100.10.2

Stop 10.100.10.254

☑ Ignore IP zero

☑ Ignore IP 255

☐ Extract from file

Either use the hostname lookup feature (see previous entry) or manually enter a start and stop IP address in the Start and Stop boxes. The up/down buttons to the right of the IP boxes will add/subtract one from the shown IP.

Clicking the Prev C button will set the start and stop IPs to the previous Class C network range.

Clicking the Next C button will set the start and stop IPs to the next Class C network range.

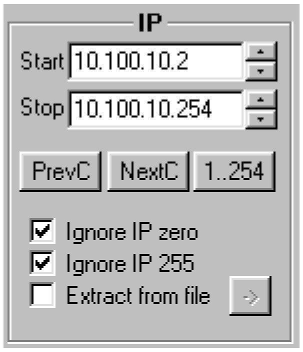
Clicking 0 -- 255 (or 1 -- 255, 1..254 or 1..255 depending on the setting of the buttons mentioned below) will set the start and end IP address ranges appropriately, ignoring either address that end with .0 or .255.

Selecting the Ignore IP zero box will cause any scans to ignore any generated IP addresses that end with .0.

Selecting the Ignore IP 255 box will cause any scans to ignore any generated IP addresses that end with .255.

If you want to perform a scan using IP addresses from a text file, select Use IPs from text file. When this is selected the manual entry IP boxes will be grayed out and you can then click on the Load button to get to the file scan dialog window. See the next section on how to scan the text file for IP addresses.

# Use IPs from text file



Start 10.100.10.2

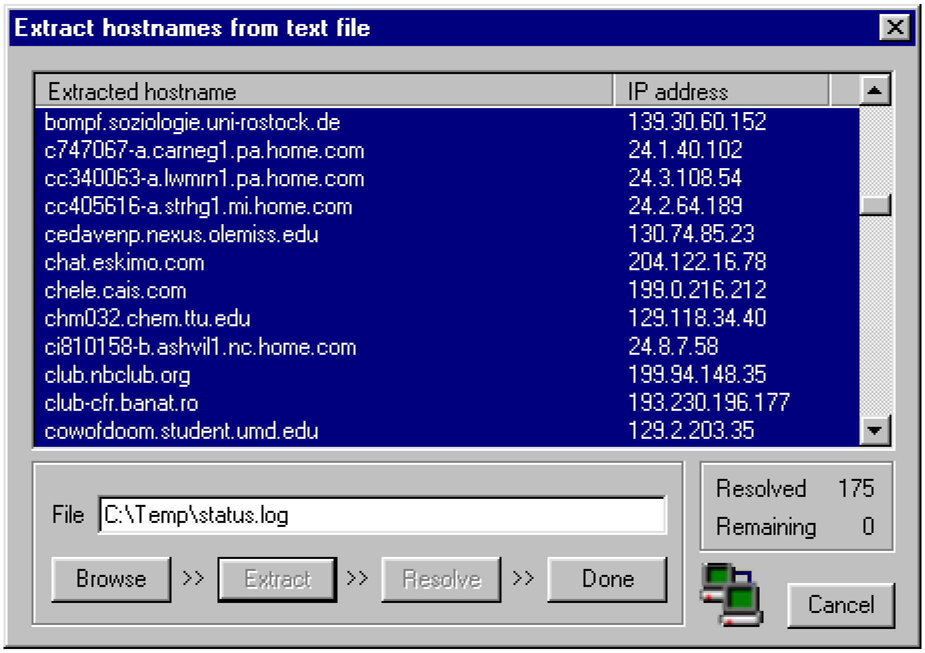
Stop 10.100.10.254

☑ Ignore IP zero

☑ Ignore IP 255

□ Extract from file

Selecting Use IPs from text file and clicking on the Load -> button will take you to the Extract hostnames from text file section.



| Extracted hostname | IP address |
|---|---|
| bompf.soziologie.uni-rostock.de | 139.30.60.152 |
| c747067-a.carneg1.pa.home.com | 24.1.40.102 |
| cc340063-a.lwmrn1.pa.home.com | 24.3.108.54 |
| cc405616-a.strhg1.mi.home.com | 24.2.64.189 |
| cedavenp.nexus.olemiss.edu | 130.74.85.23 |
| chat.eskimo.com | 204.122.16.78 |
| chele.cais.com | 199.0.216.212 |
| chm032.chem.ttu.edu | 129.118.34.40 |
| ci810158-b.ashvil1.nc.home.com | 24.8.7.58 |
| club.nbclub.org | 199.94.148.35 |
| club-cfr.banat.ro | 193.230.196.177 |
| cowofdoom.student.umd.edu | 129.2.203.35 |

File C:\Temp\status.log

Resolved 175

Remaining 0

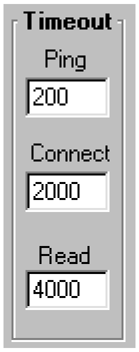
The first thing to do is browse for a text file (or type in the name in the edit box).

Next click on Extract to have the program scan through the text file and extract valid IP addresses and hostnames. The program is quite intelligent when finding valid hostnames from the text but it might be required to remove potential confusing text using an external editor beforehand. You can click Browse and Extract as many times as you like using different files and the program will add the new hostnames to the list. Any duplicate items will automatically be removed.

When all hostnames have been found you can click on the Resolve button to convert all hostnames into numeric IP addresses in
preparation for the port scan. This can take some time if you have many hundreds of addresses to resolve. Once this has completed (the Remaining count becomes zero and the icon stops animating) you can click on the Done button to transfer you back to the main window and perform a scan by clicking on Start.

At any time in this window you can click Cancel to abort the operation and return you to the main window.

# Timeouts section



Timeout

Ping

200

Connect

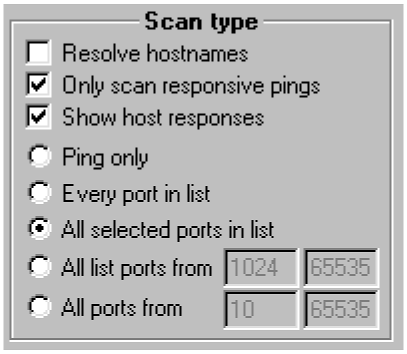
2000

Read

4000

Set the timeout for pings and connection attempts and read timeouts using these three boxes. Times are represented in milliseconds (thousandths of a second). i.e. 1000 = 1 second.

# Scan type section



Scan type

□ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1024 65535
○ All ports from 10 65535

Checking Resolve hostnames will attempt to resolve the hostname of each machine encountered during the scan.

Checking Only scan/show responding ping hosts will result in only responding machines being shown during a ping scan, and only responding machines being scanned and shown during a port scan.

Checking Show host responses will make the program listen for any data coming back from the scanned host on the respective port. You must also have set the probe text entry in the port list section for the port in order to illicit a response from the host.

Selecting a scan type of Ping only will only ping the machines in the provided IP range. No port scanning will take place.

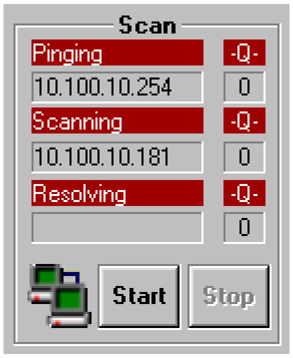
Selecting a scan type of Every port in list will perform a port scan in the provided IP range, trying to connect to every port listed in
the port list.

Selecting a scan type of All selected ports in list (default at startup) will perform a port scan in the provided IP range, trying to connect to every port in the port list that has a checkmark next to it.

Selecting a scan type of All list ports from .. to .. will perform a port scan in the provided IP range, trying to connect to every port in the port list within the given port range.

Selecting a scan type of All ports from .. to .. will perform a port scan in the provided IP range, trying to connect to every port in the given port range, regardless of whether the port is in the port list.

# Scan section

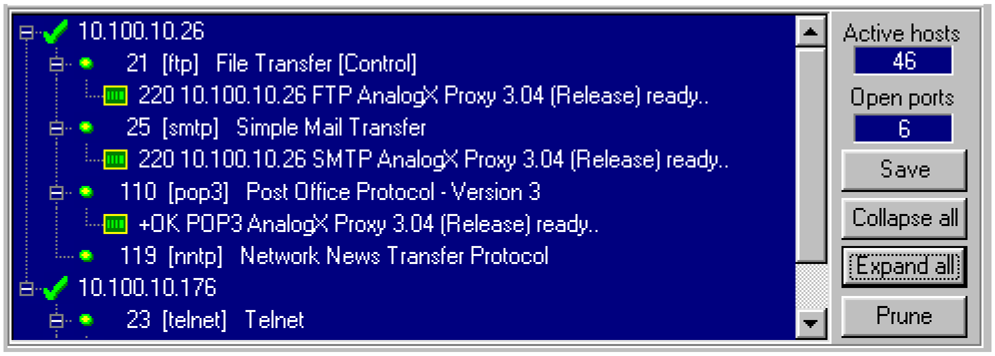


Pinging: 10.100.10.254 — 0
Scanning: 10.100.10.181 — 0
Resolving: — 0

This shows any current activity during a scan. The three sections, Pinging, Scanning and Resolving each show the current IP address that is being considered for each operation. The -Q- fields show how many IP addresses are still awaiting responses.

Start will start the scan and Stop will terminate a scan in progress.

# Results list section



```
10.100.10.26
    21  [ftp]  File Transfer [Control]
        220 10.100.10.26 FTP AnalogX Proxy 3.04 (Release) ready..
    25  [smtp]  Simple Mail Transfer
        220 10.100.10.26 SMTP AnalogX Proxy 3.04 (Release) ready..
    110  [pop3]  Post Office Protocol - Version 3
        +OK POP3 AnalogX Proxy 3.04 (Release) ready..
    119  [nntp]  Network News Transfer Protocol
10.100.10.176
    23  [telnet]  Telnet
```

Active hosts 46

Open ports 6

The main window here shows the results of the scan in a tree form. The tree comprises a sorted list of IP addresses (with resolved hostnames next to them if Resolve hostnames was selected) that represent replies from the current scan. A green check mark next to a tree node signifies a positive ping response from a machine. A red cross signifies no ping response (only shown when Only scan/show responding ping hosts is not selected).

If a port scan has been selected (as opposed to just a simple ping scan) then any responding ports for each address will be shown as child items indented in from the IP address tree leaf. Also, if you have opted to show host responses the text response from that machine's port will be shown underneath and indented from the port leaf. Characters in the response data that are not displayable will be shown as a dot character.

Click Save to save the current scan results list to a text file on disk.

Click Collapse all to close up all open leaves in the tree list.

Click Expand all to open up all open leaves in the tree list.

Click Prune to remove any IP addresses that have no open ports shown.

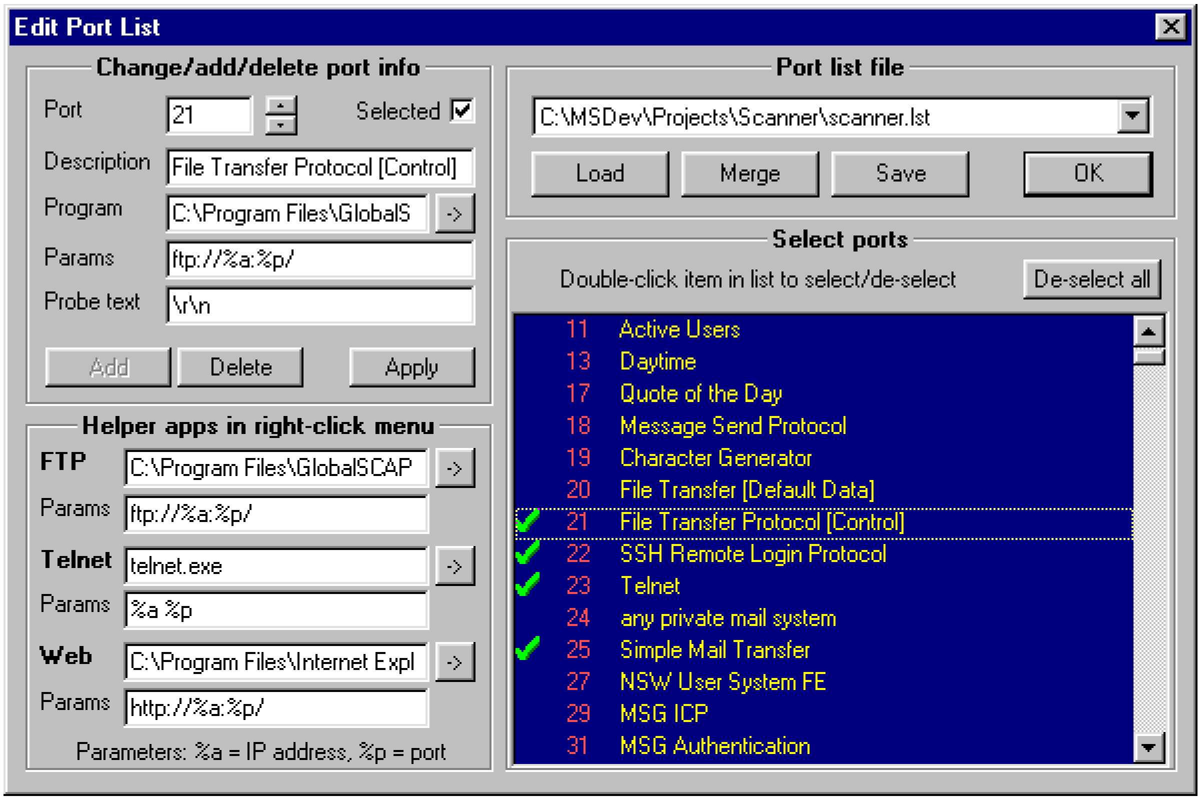
Double clicking on a port item in the list will transfer the selected IP address into the hostname lookup box.

Right-clicking on a port item in the list brings up a popup menu for connecting to the given IP address on the selected port using a specific helper application. Three standard connection helper applications are defined: FTP, Telnet and Web browse. These are set up in the Configuration section. Selecting any of these three items will launch the associated helper application and try to connect to the selected IP on the selected port (provided you can specify command-line parameters that the application understands). An example might be to Telnet to an open port 79 (Finger) to view Finger information or simply open up your web browser when you select an open port 80.

The Custom menu item will activate a custom application (if one has been specified) that is linked with this particular port. For example you may wish to set up a SSH client application to be associated with the port for SSH. Then right-clicking on an open SSH port and selecting the custom item will launch your SSH client.

# Configuration section

Clicking on Port list setup will take you to the port list configuration section.



Port: 21  Selected ☑

Description: File Transfer Protocol [Control]

Program: C:\Program Files\GlobalS

Params: ftp://%a:%p/

Probe text: \r\n

FTP: C:\Program Files\GlobalSCAP

Params: ftp://%a:%p/

Telnet: telnet.exe

Params: %a %p

Web: C:\Program Files\Internet Expl

Params: http://%a:%p/

Parameters: %a = IP address, %p = port

C:\MSDev\Projects\Scanner\scanner.lst

Double-click item in list to select/de-select

| | | |
|---|---|---|
| | 11 | Active Users |
| | 13 | Daytime |
| | 17 | Quote of the Day |
| | 18 | Message Send Protocol |
| | 19 | Character Generator |
| | 20 | File Transfer [Default Data] |
| ✓ | 21 | File Transfer Protocol [Control] |
| ✓ | 22 | SSH Remote Login Protocol |
| ✓ | 23 | Telnet |
| | 24 | any private mail system |
| ✓ | 25 | Simple Mail Transfer |
| | 27 | NSW User System FE |
| | 29 | MSG ICP |
| | 31 | MSG Authentication |

Here you can add, change and delete ports from the port list, select or de-select ports to be scanned and select helper applications that will be shown when you right-click on the port tree list for connecting to the specified port.

The most frequently used part of this dialog will be selecting and de-selecting ports to be scanned. Use the scrolling port list and double-click a port item to select/de-select it. To de-select all ports click on the Deselect all button.

You can change the ports in the list, together with their description and helper application (for the right-click popup menu on the main screen list) using the Add, Delete and Apply buttons at the top left of this window.

Here is a description of each entry field in the Change/add/delete port info section:

- **Port**
  The TCP port number you want to add/change/delete, 1 - 65535.

- **Selected**
  Specifies whether the port is selected for scanning. A check mark will appear/disappear for the port in the list when you change this.

- **Description**
  A more informative description of the TCP port.

- **Program**
  When you right-click on a discovered port after a scan has been performed a popup menu will appear. The Custom menu item in this menu refers to this application and will be launched when you select it. If no helper program has been associated with this port then the Custom menu item will not be selectable.

- **Params**
  These are optional parameters that will be passed to the program selected in the Program box. Use %a to specify the IP address that this port was found on and %p as a substitute for the port number.

- **Probe text**
  This is a text prompt that will be sent to the IP address and port if a successful TCP connection is made and you have selected the Show host responses box. You can use the text \r to specify a carriage return value (hex 0D) and \n to represent a line-feed character (hex 0A).

**Remember to hit *Apply* to make your changes permanent and save the list to disk when done.**

To change the three standard helper applications for the right-click popup menu on the main screen list use the bottom section of this window.

To load a pre-created port list file from disk click on the Load button and select a .lst file to load. You can also quickly select from one of the last 4 loaded port lists by clicking on the drop-down list.

If you want to merge one or more lists together then click on the Merge button. THis will prompt you to select a port list file on disk and will merge the two lists together. Duplicate items in the currently displayed list will not be replaced by the new file merged from disk. You can click Merge as many files as you like to merge several files.

Saving the current port list is accomplished by clicking the Save button and choosing a filename to save it under.

The program comes as standard with three port lists:

- **scanner.lst**
  is derived from the RFC document describing common ports for the entire 65536 port range with additions and modifications.
- **hensss.lst**
  is derived from the list in the book Hacking Exposed, Network Security Secrets and Solutions and contains commonly exploited application and trojan ports.
- **trojans.lst**
  is derived from a list kindly provided to me by Int_13h of tlsecurity.com

## Comments/suggestions/bugs

Comments/suggestions/bugs to: lazypig@hotmail.com

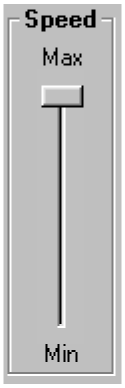
Visit my home page to see some of the other utilities I've written

http://members.home.com/rkeir/software.html

This software is distributed as freeware. I take no responsibility for any damage or problems caused by using it but I do welcome comments and suggestions.

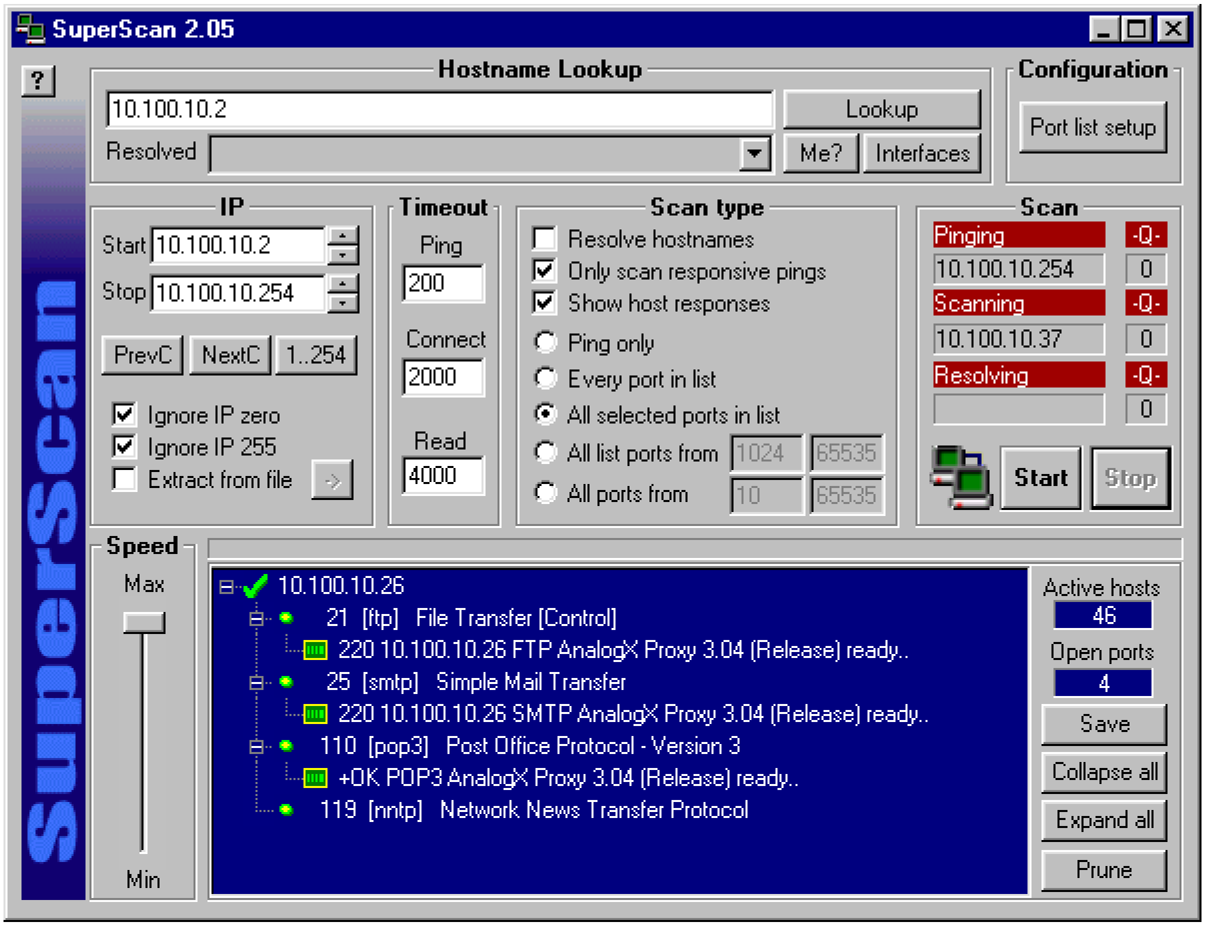
***Rob Keir***

# Speed section



Using this slider you can take control over how fast the program transmits data. At the maximum setting with the slider at the topmost position the program will try to run at the fastest safe rate. The slowest speed setting should let even the slowest modem cope with the amount of output data.

# Main Window



Hostname Lookup: 10.100.10.2

Resolved:

IP

Start 10.100.10.2

Stop 10.100.10.254

☑ Ignore IP zero

☑ Ignore IP 255

☐ Extract from file

Timeout

Ping 200

Connect 2000

Read 4000

Scan type

☐ Resolve hostnames

☑ Only scan responsive pings

☑ Show host responses

○ Ping only

○ Every port in list

● All selected ports in list

○ All list ports from 1024 65535

○ All ports from 10 65535

Scan

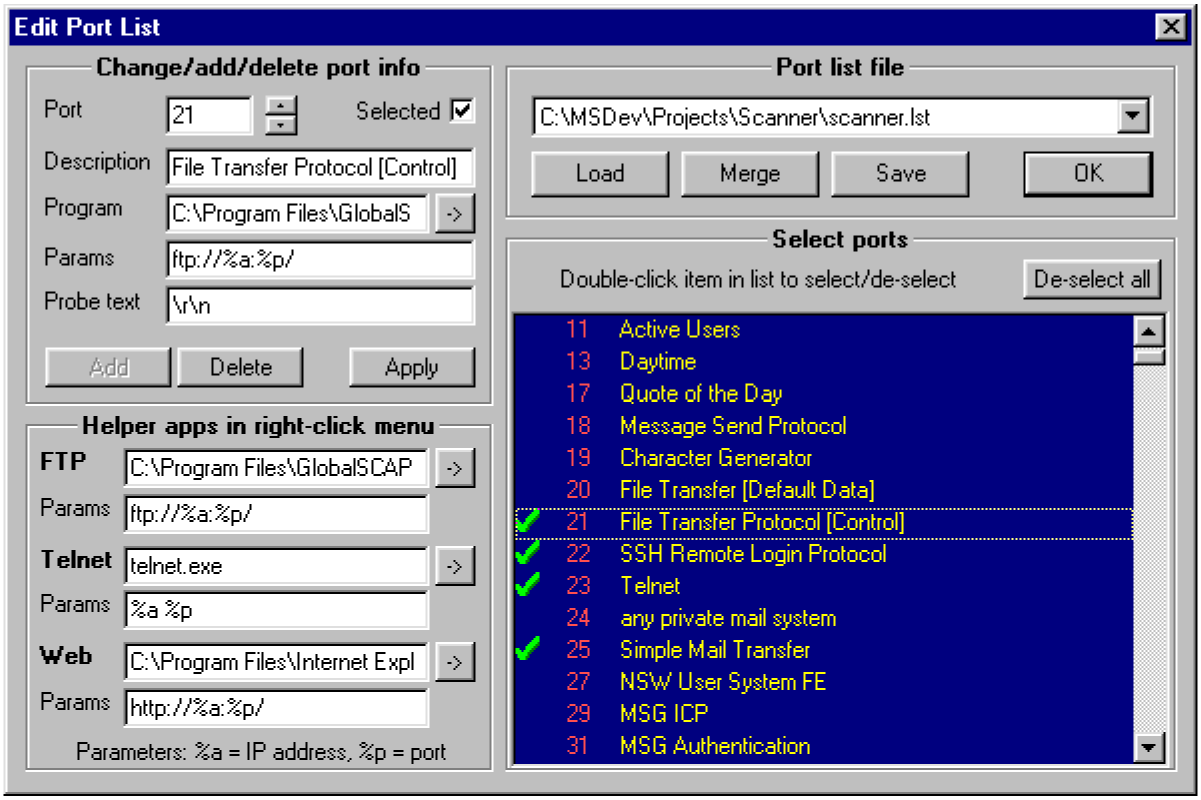
| | |
|---|---|
| Pinging | -Q- |
| 10.100.10.254 | 0 |
| Scanning | -Q- |
| 10.100.10.37 | 0 |
| Resolving | -Q- |
| | 0 |

```
⊟ ✓ 10.100.10.26
   ⊟ ● 21  [ftp]  File Transfer [Control]
        └ 220 10.100.10.26 FTP AnalogX Proxy 3.04 (Release) ready..
   ⊟ ● 25  [smtp]  Simple Mail Transfer
        └ 220 10.100.10.26 SMTP AnalogX Proxy 3.04 (Release) ready..
   ⊟ ● 110  [pop3]  Post Office Protocol - Version 3
        └ +OK POP3 AnalogX Proxy 3.04 (Release) ready..
     ● 119  [nntp]  Network News Transfer Protocol
```

Active hosts 46

Open ports 4

# Port List window



Change/add/delete port info

Port 21 Selected ☑

Description File Transfer Protocol [Control]

Program C:\Program Files\GlobalS

Params ftp://%a:%p/

Probe text \r\n

Helper apps in right-click menu

FTP C:\Program Files\GlobalSCAP

Params ftp://%a:%p/

Telnet telnet.exe

Params %a %p

Web C:\Program Files\Internet Expl

Params http://%a:%p/

Parameters: %a = IP address, %p = port

Port list file

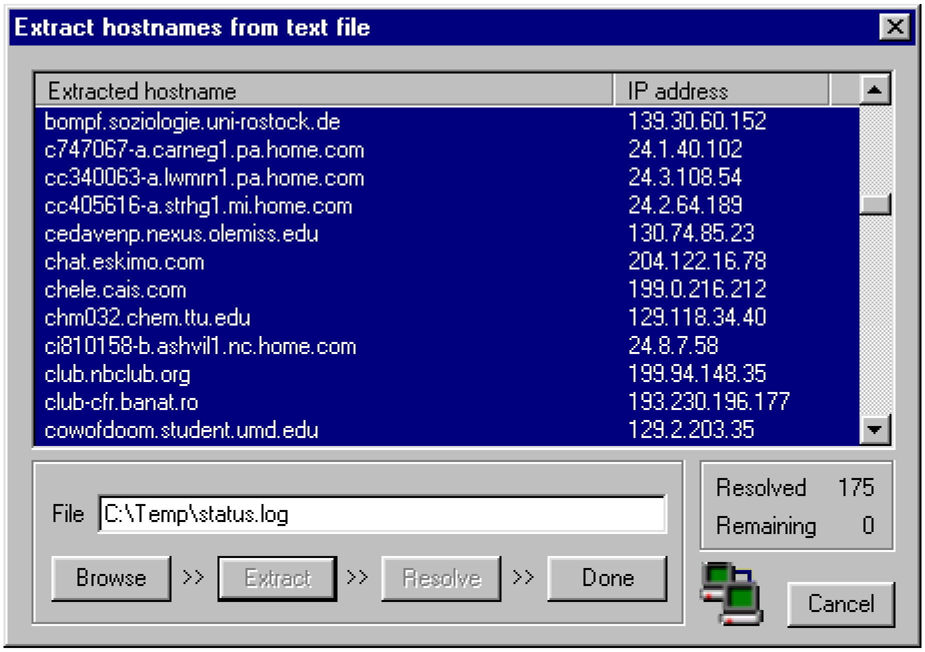
C:\MSDev\Projects\Scanner\scanner.lst

Select ports

Double-click item in list to select/de-select

| | | |
|---|---|---|
| | 11 | Active Users |
| | 13 | Daytime |
| | 17 | Quote of the Day |
| | 18 | Message Send Protocol |
| | 19 | Character Generator |
| | 20 | File Transfer [Default Data] |
| ✓ | 21 | File Transfer Protocol [Control] |
| ✓ | 22 | SSH Remote Login Protocol |
| ✓ | 23 | Telnet |
| | 24 | any private mail system |
| ✓ | 25 | Simple Mail Transfer |
| | 27 | NSW User System FE |
| | 29 | MSG ICP |
| | 31 | MSG Authentication |

# Extract From Text File window

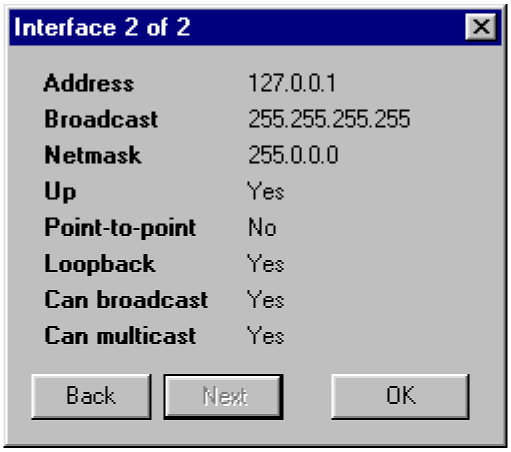


| Extracted hostname | IP address |
|---|---|
| bompf.soziologie.uni-rostock.de | 139.30.60.152 |
| c747067-a.carneg1.pa.home.com | 24.1.40.102 |
| cc340063-a.lwmrn1.pa.home.com | 24.3.108.54 |
| cc405616-a.strhg1.mi.home.com | 24.2.64.189 |
| cedavenp.nexus.olemiss.edu | 130.74.85.23 |
| chat.eskimo.com | 204.122.16.78 |
| chele.cais.com | 199.0.216.212 |
| chm032.chem.ttu.edu | 129.118.34.40 |
| ci810158-b.ashvil1.nc.home.com | 24.8.7.58 |
| club.nbclub.org | 199.94.148.35 |
| club-cfr.banat.ro | 193.230.196.177 |
| cowofdoom.student.umd.edu | 129.2.203.35 |

File C:\Temp\status.log

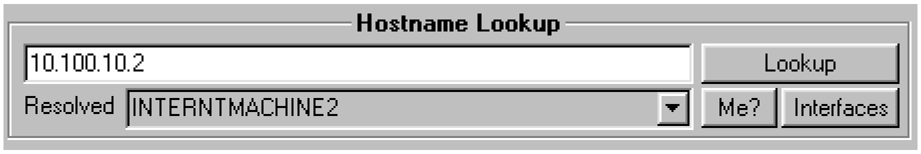
Resolved 175
Remaining 0

# Interfaces window



Interface 2 of 2

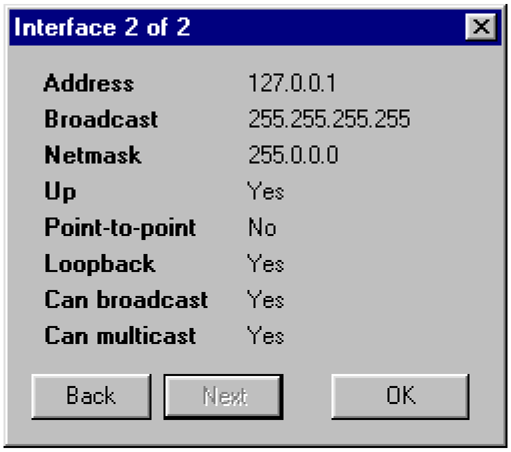
| | |
|---|---|
| **Address** | 127.0.0.1 |
| **Broadcast** | 255.255.255.255 |
| **Netmask** | 255.0.0.0 |
| **Up** | Yes |
| **Point-to-point** | No |
| **Loopback** | Yes |
| **Can broadcast** | Yes |
| **Can multicast** | Yes |



Hostname Lookup

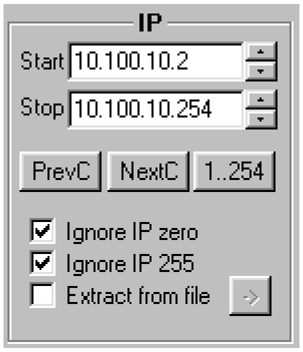
10.100.10.2

Resolved INTERNTMACHINE2



Interface 2 of 2

| | |
|---|---|
| **Address** | 127.0.0.1 |
| **Broadcast** | 255.255.255.255 |
| **Netmask** | 255.0.0.0 |
| **Up** | Yes |
| **Point-to-point** | No |
| **Loopback** | Yes |
| **Can broadcast** | Yes |
| **Can multicast** | Yes |



IP

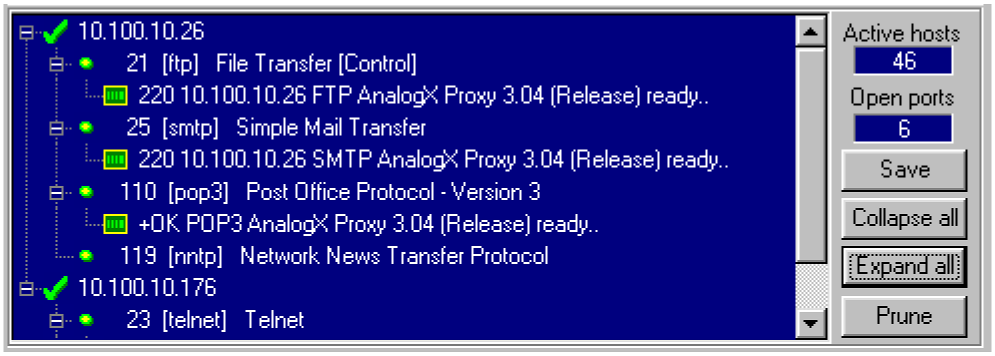
Start 10.100.10.2

Stop 10.100.10.254

☑ Ignore IP zero

☑ Ignore IP 255

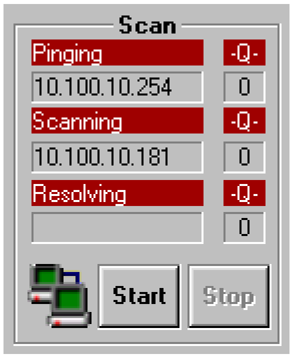
□ Extract from file



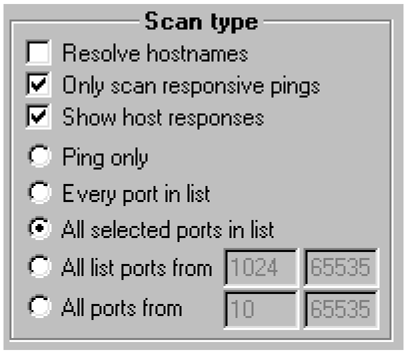
```
⊟ ✓ 10.100.10.26
    ⊟ ● 21  [ftp]   File Transfer [Control]
        └ 220 10.100.10.26 FTP AnalogX Proxy 3.04 (Release) ready..
    ⊟ ● 25  [smtp]   Simple Mail Transfer
        └ 220 10.100.10.26 SMTP AnalogX Proxy 3.04 (Release) ready..
    ⊟ ● 110  [pop3]   Post Office Protocol - Version 3
        └ +OK POP3 AnalogX Proxy 3.04 (Release) ready..
    └ ● 119  [nntp]   Network News Transfer Protocol
⊟ ✓ 10.100.10.176
    ⊟ ● 23  [telnet]   Telnet
```

Active hosts 46

Open ports 6



Pinging -Q-
10.100.10.254 0
Scanning -Q-
10.100.10.181 0
Resolving -Q-
0



Scan type

☐ Resolve hostnames

☑ Only scan responsive pings

☑ Show host responses

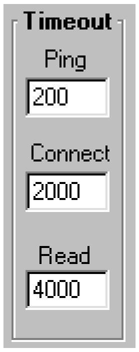
○ Ping only

○ Every port in list

● All selected ports in list

○ All list ports from 1024 65535

○ All ports from 10 65535



Timeout

Ping

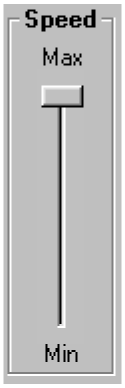
200

Connect

2000

Read

4000


Speed
Max
Min