General Information about CyberKit

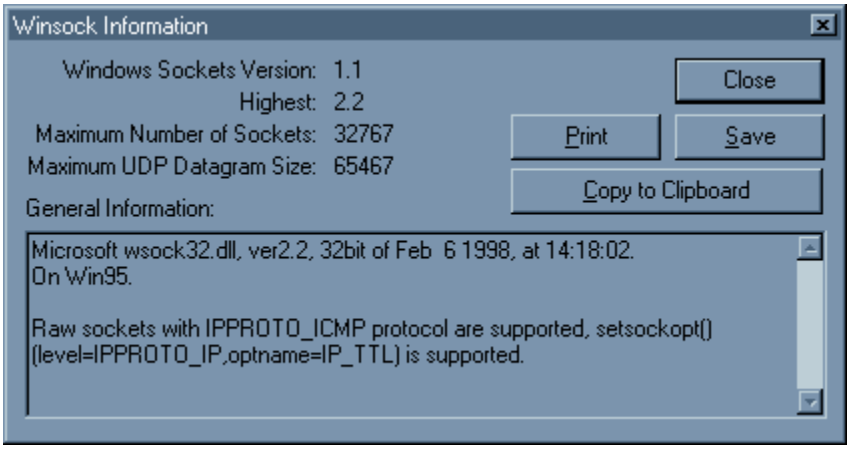
CyberKit requires Windows 95/98 or Windows NT.

CyberKit also requires a working TCP/IP connection to a LAN or the Internet.

To use ping and traceroute, you will need Microsoft winsock 2.0 or higher installed. It is possible to use a non-Microsoft winsock stack if this stack supports raw sockets. Windows 98 and Windows NT already ship with the winsock 2 stack, as will all future versions of Windows. Windows 95 users can download an upgrade from the Microsoft site. A link to this site can be found on the CyberKit homepage (http://www.cyberkit.net). To this date, Microsoft has no upgrade available for Windows NT 3.51.

Windows NT 4.0 requires administrator privileges to use raw sockets. However since service pack 4 there is a fix for this. See the trouble shooting section for more information.

You can use the Winsock Information item on the View menu to verify whether your winsock stack is compatible with CyberKit. You will need support for raw sockets and setsockopt() as you can see on the 2 bottom lines in the picture below.



Copyright Information and Disclaimer

CyberKit is **NOT** Public Domain software.

CyberKit is postcardware. Postcardware is almost freeware. If you try out a postcardware program, and decide that you'd like to use it on a regular basis, you then just send a postcard to the development team or programmer.

Please send the postcard (preferably one that has something to do with where you live) to the following address:

Luc Neijens
Berkenlaan 8
3960 BREE
Belgium

Distribution and Restrictions
You are free to distribute CyberKit. Any such distribution must be free of charge and limited to the original and unchanged archive.
You are not allowed to make any changes to CyberKit. This includes translating help files or any other part of the package to other languages.
You may not reverse engineer, decompile, or disassemble CyberKit.
You are not allowed to include CyberKit on a freeware/shareware CD-ROM collection, unless this CD-ROM collection is distributed free of charge.
You are allowed to include CyberKit on a cover CD-ROM for a book or magazine. However, in return, I request a copy of the book or magazine (send it to the above address).
In case of doubt, check with the author first.

DISCLAIMER
THE INFORMATION AND CODE PROVIDED IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL LUC NEIJENS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
PLEASE DO NOT USE CYBERKIT UNLESS YOU CAN FULLY AGREE WITH THIS DISCLAIMER.

Installing/Un-Installing CyberKit

Installing CyberKit
- Unzip the archive in a temporary directory.
- Click on the Start button on the Taskbar.
- Click on the Start menu's "Run" selection.
- Type the path to the unzipped files followed by "\SETUP.EXE".
- Click on the "OK" button.
- Follow the on-screen prompts to complete the installation.

Or if you're using WinZip: Just open the archive and select 'Install'.

CyberKit copies all its files to the CyberKit directory. It does not copy any files to other directories like the windows or system directory.

Registry Settings:
Disclaimer: With the registry editor (Windows 95 uses regedit.exe and Windows NT uses regedt32.exe) you can do devastating damage to your operating system. Use with EXTREME care!
CyberKit keeps user setting in the windows registry under the following key:
HKEY_CURRENT_USER/Software/Luc Neijens/CyberKit
The key CyberKit and its contents will be removed when you un-install CyberKit.
If at any time these settings are corrupted, you can safely delete the complete CyberKit key. CyberKit will create this key at startup if not present. However, you will lose your personal settings if you do this!

Un-installing CyberKit
- Open the control panel.
- Double click on the 'Add/Remove Programs' icon.
- You will see a list of installed software, select CyberKit on the list.
- Click on the "Add/Remove" button.
- Follow the on-screen prompts to complete the un-installation.

Getting Started with CyberKit

First, you need to understand the difference between a hostname and a host address:
A host address or TCP/IP address consists of 4 numbers between 0 and 255 separated by a period. For example, 120.56.98.45 would be a valid TCP/IP address. Every computer on the Internet (or any other TCP/IP network), including your PC, has a unique TCP/IP address. So, in order for your computer to be able to connect to any other computer on the Internet, it has to find out the TCP/IP address of that computer.

Now, how does my computer find the TCP/IP address of that FTP server, or that site I'm surfing to on the world wide web?
Well you are giving it to your computer! Of course you rarely enter a TCP/IP address, usually you just enter something like www.host.com, also known as a hostname. Your computer then uses this hostname to find out the TCP/IP address. This process is called 'resolving' a hostname.
How does this work?
First, your computer will look in your hosts file. The hosts file is located on your computer and it is a simple text file that looks something like this:
127.0.0.1 localhost
120.56.98.45 www.host.com
etc.

If this hosts file is not present, or it does not contain the hostname we are looking for, your computer will connect to a DNS (Domain Name Server) server and try to resolve the hostname there. Which DNS server your computer will connect to is specified in the TCP/IP settings of your computer.
The DNS server is in fact nothing more but a list of hostnames and the matching TCP/IP addresses.

So what does al this have to do with CyberKit?
Most functions in CyberKit will require a TCP/IP address or a hostname. If you enter a hostname, CyberKit will find out the TCP/IP address if needed and vice versa.
There are basically two ways to resolve a hostname into a TCP/IP address using CyberKit:
- You can use the standard DNS resolve functions. These functions are also used by other applications, like your e-mail client or web browser. Except for the NSLookUp client, all clients in CyberKit use the standard DNS functions.
  The standard DNS resolve functions use your computers network settings to locate your DNS server.
- You can use the specialized DNS functions that are provided by the NSLookUp client. Using NSLookUp you can freely choose the DNS server and record types that you want to query.

NSLookUp is certainly the most active client inside CyberKit. Even if you don't use it intentionally, CyberKit is using it all the time, quietly in the background.

What other clients does CyberKit offer you?
ping, traceroute, finger, whois, nslookup, time synchronizer, quote of the day, netscanner, dbscanner, check for mail, keep alive.

Related topics: sample hosts file, sample services file, sample protocol file

New Releases

The latest release can always be downloaded from the CyberKit homepage (http://www.cyberkit.net).

Beta releases
Beta releases are intermediate releases. They have not been fully tested and are likely to contain bugs. If you're not entirely at ease with beta releases, please **do not use them**! If, however, you don't mind a bug now and then, you can help me greatly by using the beta release and reporting any problems you may encounter.

New features
I need your input to keep CyberKit alive. Any bright ideas to make CyberKit better? Let me know! I promise I will consider all suggestions, however I reserve the right for the final decision. You can send new feature suggestions to Luc.Neijens@cyberkit.net.

How to report a problem
Read the problem reports section.

FAQ (Frequently Asked Questions)

Does CyberKit support proxy servers/firewalls?
WhoIs and Finger have support for firewalls.
If you just want to use Ping and TraceRoute on the LAN behind the firewall there is no problem. When you want to use them through the firewall you're firewall has to be configured to let ICMP messages pass through. Your network administrator should be able to do this for you.

How can I configure CyberKit to use Microsoft Internet Mail as my e-mail reader?
Go to the mail options dialog and specify the following as your e-mail program: "C:\WINDOWS\EXPLORER.EXE" /root,C:\WINDOWS\Internet Mail.{89292102-4755-11cf-9DC2-00AA006C2B84}

How can I ping myself?
You can always ping your own computer by using the address 127.0.0.1. As a shortcut you can use 'me' or 'myself' as hostname. You might also consider adding the line '127.0.0.1 localhost' to your hosts file.

How can I start CyberKit minimized in the tray?
Use the "Minimize To Tray" command line parameter, and set the 'Minimize To Tray' option in the general options dialog.

How do I install CyberKit?
Refer to the install/un-install section for instructions.

How do I uninstall CyberKit?
Refer to the install/un-install section for instructions.

How do I know if a host supports finger, whois or any other service?
Most of the time will Winsock return a specific error if a host does not support a service. If you try to connect to a host and you get the Winsock error 10061 (Connection refused), you can safely assume that that host does not support the service.
In the whois section is explained how you can get a list of recent whois servers.

How do I report a problem?
See the problem reports section for instructions.

What do I need to use CyberKit?
See the discussion in the about section

What is the difference between finger and whois?
Whois tends to give you more in-depth data. With whois you are connecting to a NIC server. Whois will only provide the information that is registered at the NIC server. The most common use is to obtain information about the owner of a domain.
With finger most of the time you are connecting to the provider of the user you are fingering. Finger can provide you with the log in information of users that are currently logged on to the system.

What programming language did you use to write CyberKit?
Visual C++ with Microsoft foundation classes (MFC).

Where can I find more 'Quote of the Day' servers?
Most NT servers support the Quote service, so this might be a place to start your search. Feel free to report other servers, so I can include them in the default bookmarks.

Where can I get the Winsock 2 stack?
There is an upgrade available for Windows 95 on the Microsoft site. You can find a link to this site on the

CyberKit homepage (http://www.cyberkit.net). Windows NT 4.0 and Windows 98 already ship with the new winsock stack. Microsoft did not release an update for Windows NT 3.51.

Where can I get the latest release of CyberKit?
You can download the latest release of CyberKit from the CyberKit homepage: http://www.cyberkit.net.

Why are the ping and the traceroute pages ‘grayed’ out?
See the trouble shooting section.

Why is it impossible to enter the '@' character?
It's not a bug, it's a feature!
See the 'Smart Address Splitting' option in the tips and tricks section.

Related topics: tips and tricks, trouble shooting, problem reports

Tips and Tricks

Adding an address to the bookmarks
Just used a query and want to enter it in the bookmarks? Select the "Add to bookmarks" menu item on the edit menu and CyberKit will do it for you! All you have to do is name the new bookmark and you are done.

Adding CyberKit to the startup menu
If you want to start CyberKit every time you start your computer, here's how you do it:
- Click on the Start button on the Taskbar
- Select 'Settings' and next 'Taskbar'
- Select 'Start Menu Programs'
- Select 'Add'
- Select 'Browse' and locate CyberKit.exe, next select 'Open'
- You will see something like 'C:\CyberKit\CyberKit.exe' (this can differ depending on the directory you installed CyberKit in). Add "Minimized To Tray" to the end of the line. You will have something like "C:\CyberKit\CyberKit.exe" "Minimized To Tray". This will make sure CyberKit starts minimized in the Tray.
- Select 'Next'
- Locate and select the 'startup' folder
- Select 'Next'
- Change the name for the shortcut to 'CyberKit'
- Select 'Finish'

Context sensitive help
CyberKit has context sensitive help. This means that if you press F1 from within for example traceroute, you'll get help about 'TraceRoute'.

Entering query and hostname
If you have the option 'Smart Address Splitting' selected, you don't have to enter query and hostname separately. Just enter (or paste from the clipboard) an e-mail address and let CyberKit do the splitting for you. 'Smart Address Splitting' can also filter the hostname out of an URL (http://…) or ftp (ftp://…) address.

Help function for whois servers
Most whois servers have a help function. Just enter help as query and the server will return help information.

Getting a list of users that are logged on to a system
Most finger servers return a list of users that are logged on if you leave the query field blank.

Obtaining a recent list of whois servers
To get a recent list of whois servers, use 'sipb.mit.edu' for hostname and 'whois-servers' as query. You will also find this address in the bookmarks that come with CyberKit.

Remember Last Function
You can let CyberKit remember the last used function by checking the 'Remember Last Function' field in the general options dialog. If you now start CyberKit, it will automatically switch to the last used function (ping, finger, whatever).

Remember Last Window Position
You can let CyberKit remember its window size and position by checking the 'Remember Window Position' field in the general options dialog. If you now start CyberKit, it will start at its last screen location (minimized, maximized, whatever).

Smart address splitting

Make your life easy and let CyberKit split the addresses for you. CyberKit will automatically filter the hostname out of an URL or e-mail address. When used in the Finger client this will split the e-mail address into the query and hostname. Try it, you'll like it!
You can set the 'Smart address splitting' option in the general options dialog.

Using non-proportional fonts
The query output will look nicer if you use a non-proportional font like courier or terminal. You can change the font from the options menu.

Related topics: trouble shooting, FAQ (Frequently Asked Questions), problem reports

Trouble Shooting

10061 (Connection refused) messages
These messages usually indicate that the server does not support the requested service.

Other Winsock error messages
I have tried to make the Winsock error messages as comprehensive as possible. The most common error messages include some information about the possible reason for the error. Most common errors are: using an invalid hostname, host address, a host that is down, etc.

Firewall/Proxy issues
See the FAQ(Frequently Asked Questions) section for more information.

Ping and traceroute tabs are grayed out / Winsock issues
Ping and traceroute require some of the Winsock 2 features. Winsock 2 already ships with Windows NT 4.0 and Windows 98. You can download an upgrade for Windows 95 from the Microsoft site. Microsoft has no upgrade for Windows NT 3.51. If you are running a lower version (Windows 95 comes with the 1.1 release) or a non-Microsoft winsock stack that does not support raw sockets, these two pages will be 'grayed' out. See also general information about CyberKit.
This problem might also occur when running under a non-administrator account on Windows NT. Ping and traceroute require RAW socket support. By design, Windows NT requires administrator privileges to access RAW sockets.
Gary L Peskin has provided me with a solution for this problem (thanks Gary!)
The workaround is described in the Microsoft Knowledge Base article Q195445. It applies to service pack 4:
... "To work around this problem in Windows NT 4.0, you can disable the security check on RAW sockets by creating the following registry variable and setting its value to DWORD 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Afd\Parameters\DisableRawSecurity After you change the registry, you need to restart your computer." ...

Ping and traceroute tabs are grayed out / Microsoft Proxy issues
It seams there is a problem with RASIFace.dll (located in the CyberKit directory) combined with Microsoft Proxy server. RASIFace.dll handles all RAS functions for CyberKit (dialing connections, checking which connections are active, etc.). For some reason RASIFace.dll sometimes fails to load properly, causing ping and traceroute to be disabled. As a workaround you can rename RASIFace.dll to some other name. You will not be able to use CheckForMail or use CyberKit to dial your RAS connections, but all other functions should be functional.

Time is displaying incorrect 'Local Time' / Synchronize Time is not working correctly
You must ensure your Control Panel's Date/Time applet accurately reflects both your timezone and your daylight savings time. CyberKit relies on these settings to retrieve the current system clock in GMT adjusted format.
If you have a TZ variable set in your autoexec.bat file make sure it is defined accurately. In fact, unless there is a clear need for this variable, it is best to remove it outright and let the Control Panel settings handle the timezone.

Other problem?
Most questions/problems can be solved by reading the help file first. I've put a lot of effort in it, so please use it! I can assure you that answering the same questions day in day out, while I know the answer is in the help file, is pretty frustrating. Read the tips and tricks and the FAQ (Frequently Asked Questions) sections first, next try to do a find on a keyword.
Ask yourself whether I'm the right person to answer your question. If your question is not specifically linked to using CyberKit, use the Internet! There are plenty information sources out there about programming, networking, sockets, TCP/IP, etc. with more information than I can possible provide.
If you cannot find the answer in the help file, you can reach me by e-mail at the following address:

Luc.Neijens@cyberkit.net.

Related topics: tips and tricks, FAQ (Frequently Asked Questions), problem reports

Problem Reports

Before reporting a problem
- If you have a problem with a beta, make sure you're running the latest beta.
- Read the help file, especially the tips and tricks, the FAQ (Frequently Asked Questions) and the trouble shooting sections.
- Visit the CyberKit homepage (http://www.cyberkit.net) and make sure your problem is not already reported.

The information I need
- What OS are your running and what version: Windows 95/98/NT 3.51/NT 4.0?
- What winsock stack are you using? You can use the Winsock Information item on the view menu and copy the results in your message.
- Describe in detail what you did, what function you were using, what input you provided (addresses, hostname, options).
- Note down in detail any messages (statusbar, dialog, etc.) you got from CyberKit.
- Provide a detailed description on how to reproduce the problem.
- Are you willing to provide additional information if needed?
- Any other information you think may be relevant.

Please **do not** send me large attachments unless I specifically ask for them!

Send this information by e-mail to: Luc.Neijens@cyberkit.net.

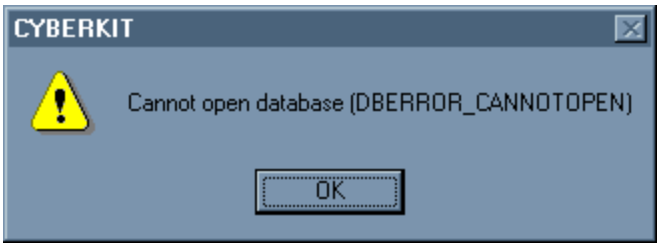
Related topics: trouble shooting, tips and tricks, FAQ (Frequently Asked Questions)

The CyberKit Database

The CyberKit Database consists of a single file, CyberKit.db, located in the CyberKit directory. It contains the CyberKit bookmarks and the mail accounts.
It is only installed by the CyberKit installation procedure when there is no other database present in the CyberKit directory. This will ensure you keep your personalized settings when installing a new release of CyberKit.

Compacting the CyberKit database
As you change data in a database, the database file can become fragmented and use more disk space than is necessary. Periodically, you can use the 'Compact Database' item from the Option menu to defragment the CyberKit database. The compacted database is usually smaller and often runs faster. Before compacting the database, CyberKit creates a backup. The backup is called CyberKit.db1 and is located in the CyberKit directory. If another CyberKit.db1 exists, it is overwritten.

Running multiple instances of CyberKit
Only one instance of CyberKit can have the database in use. If you start an extra copy of CyberKit, CyberKit will display the following dialog:



After you click on the ‘OK’ button, CyberKit will continu to run. However certain functions that require the database in order to work, will be disabled. These functions are:
- Check for new mail and consequently the new mail dialog. Also the mail options tabs will not appear in the settings dialog.
- All features that depend on the bookmark dialog, adding bookmarks, importing bookmarks, etc.

It is possible to suppress this dialog by using the “Don’t open DB” command line parameter. In this case CyberKit will not try to open the database and the functions mentioned above will not be available. See the command line parameters for more information on how to use command line parameters.

More Information (RFC's)

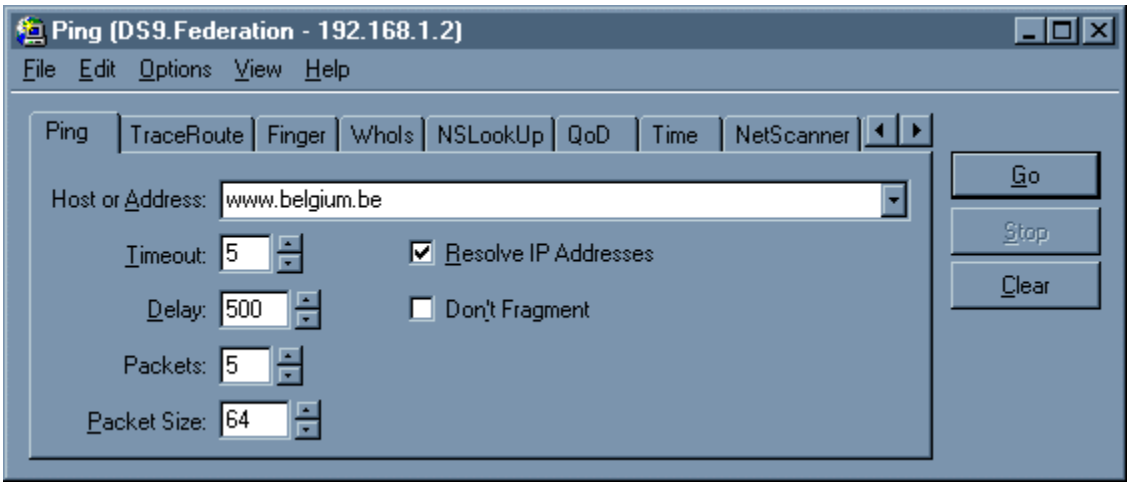
This help file is a user guide for CyberKit. If you need more specific information about TCP/IP or one of the services (e.g. ping, finger, …) you will need to find some other resources. Probable the best resource out there is the Internet. With the help of a search engine you'll be able to find all the information you will ever need! You can use the following information as a starting point.

The RFC's (Request For Comments) contain the specifications for Internet services like finger, whois, etc. They are ideal for those who want to program their own services or those who want to know the finer details. A search for 'RFC' in a search engine will provide you with lots of sites where you can read the RFC's text files. Here are a few to start with:

- RFC 865: The Quote of Day Protocol
- RFC 867: The Daytime Protocol
- RFC 868: The Time Protocol
- RFC 954: The WhoIs Protocol
- RFC 1034: Domain Names: Concepts and facilities (NS LookUp)
- RFC 1035: Domain Names: Implementation and specification (NS LookUp)
- RFC 1288: The Finger User Information Protocol
- RFC 1305: The Network Time Protocol (NTP)
- RFC 1885: The Internet Control Message Protocol (ICMP)
- RFC 1939: The Post Office Protocol Version 3 (POP3)
- RFC 2030: The Simple Network Time Protocol (SNTP)

Ping

What is ping?
Ping verifies a connection to a remote host by sending an ICMP (Internet Control Message Protocol) ECHO packet to the host and listening for an ECHO REPLY packet. The type of the ECHO REPLY packet can be one of the following: 0 = normal echo reply, 3 = destination unreachable, 11 = TTL expired.
A message is always sent to an IP **address**. If you do not specify an address but a hostname, this hostname is resolved to an IP address using your default DNS server. In this case you're vulnerable to a possible invalid entry on your DNS (Domain Name Server) server. You can simulate this resolving by using nslookup and a search type of 'Use Winsock Function GetHostByX'.
The hostname that is displayed is obtained by resolving the originating IP address using your default DNS server.



To ping a host, do one of the following and press <enter> or select the Go button:
- Enter an address in the 'Host or Address' field. You can also copy the address from somewhere else and paste it in the 'Host or Address' field.
- Select an address from the drop down menu.
- Open the bookmarks dialog with F12 and select the address to use.

To ping yourself, enter 'me' or 'myself' as hostname.

You can set any of the following options:
- Timeout: the time, in seconds, CyberKit will wait for a response.
- Delay: the interval, in milliseconds, between pings.
- Packet Size: the size, in bytes, of the ICMP message.
- Number of Pings: the number of times you want to ping the host.
- Resolve IP Addresses: whether you want CyberKit to resolve the IP addresses for you. Unlike with traceroute this will not save you a lot of time, but it is there if you want to use it. If you choose to use it, you can always resolve the IP addresses later by double clicking on the sequence number for the host.
- Don't Fragment: uses a feature in winsock that tells the IP layer not to fragment messages.

For each reply, you will see the following information:
- Number: The sequence number of the ping.
- Address: The IP address of the host that sent the ICMP echo reply.
- Host Name: The name of the host (only if you check 'Resolve IP Addresses').
- Msg Type: The type of the ICMP echo reply message.
- TTL: The value of the TTL field in the IP header of the ICMP echo reply.
- Time: The time in ms between the moment CyberKit sends the echo message to the remote host and

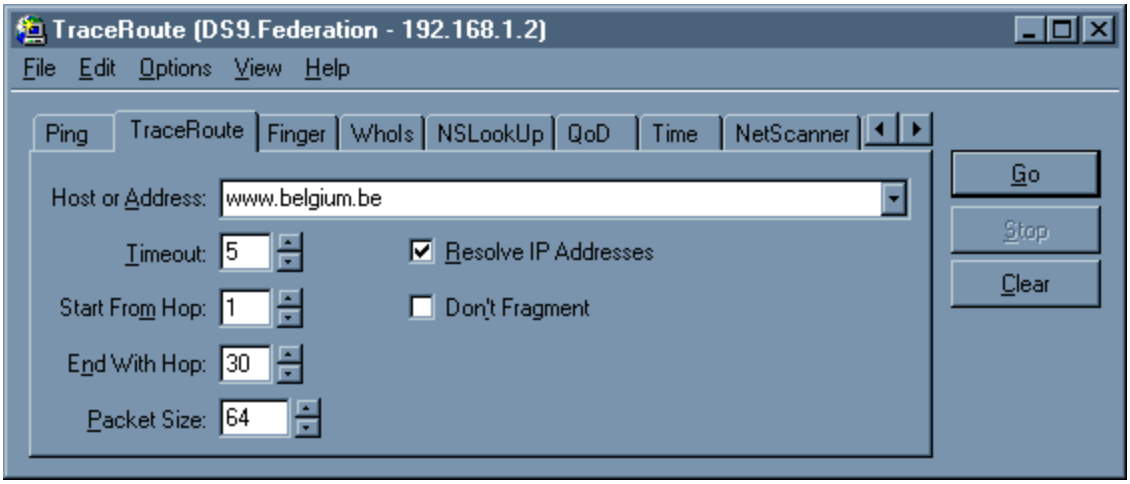
the moment CyberKit receives the response.

Related topics: traceroute, nslookup, netscanner

Traceroute

What is traceroute?
Traceroute determines the route taken to a destination by sending ICMP (Internet Control Message Protocol) ECHO packets with varying TTL (Time To Live) values to the destination and listen for an ECHO REPLY packet.
The type of the ECHO REPLY packet can be one of the following:
0 = normal echo reply
3 = destination unreachable
11 = TTL expired.

Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to traceroute (type of the ICMP echo reply = 11). Traceroute determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until a ICMP echo reply with type 0 is received, or the maximum TTL (=Maximum Hops) is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired time-to-live (TTL's) and will be invisible to traceroute (you will get a 'No response from this host' entry).
The hostname that is displayed is obtained by resolving the originating IP address for the ICMP echo reply message using your default DNS (Domain Name Server) server.



To trace the route to a host, do one of the following and press <enter> or select to Go button:
- Enter an address in the 'Host or Address' field. You can also copy the address from somewhere else and paste it in the 'Host or Address' field.
- Select an address from the drop down menu.
- Open the bookmarks with F12 and select the address to use.

You can set any of the following options:
- Timeout: the time, in seconds, CyberKit will wait for a response.
- Start From Hop: set this to '1' if you want to start with the first hop. **TIP:** if for your ISP (Internet Service Provider) the first hop never responds, set this to '2'.
- Maximum Hops: the maximum number of hops to trace. In fact, this is the maximum value for TTL.
- Packet Size: the size, in bytes, of the ICMP message.
- Resolve IP Addresses: whether you want CyberKit to resolve the IP addresses for you. Unlike with ping this can speed things up considerably. If you choose to use this option, you can always resolve the IP addresses later by double clicking on the sequence number for the host.

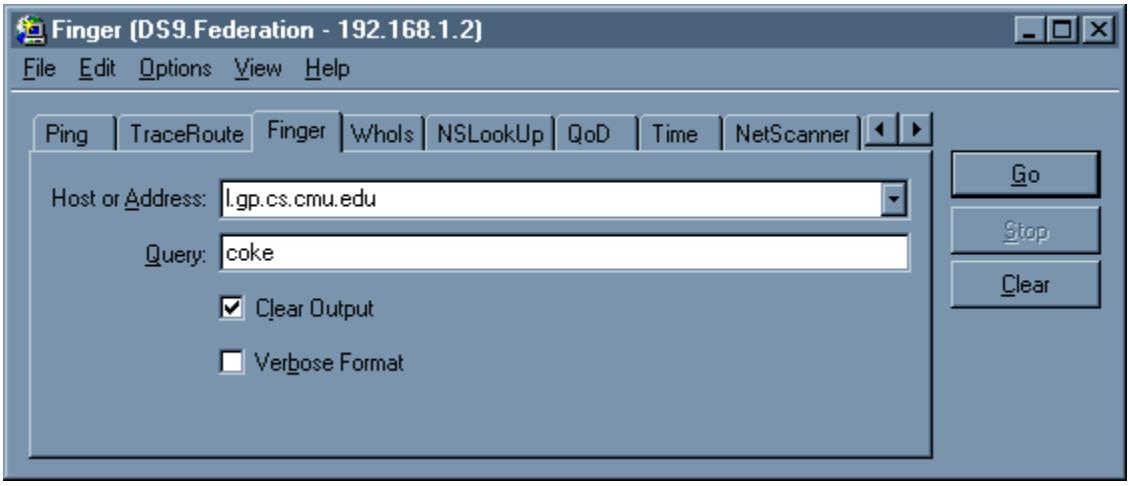
- Don't Fragment: uses a feature in winsock that tells the IP layer not to fragment messages.

For each host along the route, you will receive the following information:
- Number: The sequence number of the host in the Route.
- Address: The IP address of the host.
- Host Name: The name of the host.
- Msg Type: The type of the ICMP echo reply message.
- Time: The time between the moment CyberKit sends the echo message to the remote host and the moment CyberKit receives the response.

Related topics: ping, nslookup, netscanner

Finger

What is finger?
Finger allows you to obtain information about a user based upon his or her email address. Finger is typically supported by unix hosts.
The default port number for finger is 79. To use another port number, separate the host name from the port number by a ‘:’. For example: Entering a host name like ‘www.host.com:18’ will use port 18 instead of the default port.



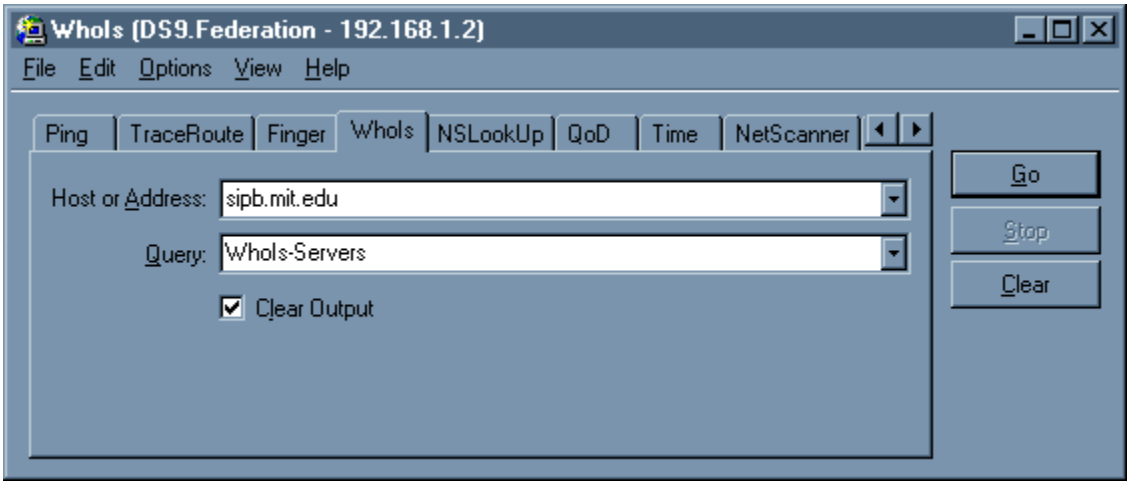
To finger a person, or host, do one of the following and press <enter> or select the Go button:
- Enter an e-mail address in the ‘Host or Address’ or ‘Query’ field. You can also copy the address from somewhere else and paste it in one of the above fields.
- Enter a hostname in the ‘Host or Address’ field.
- Select a hostname or e-mail address from the drop down menu.
- Open the bookmarks with F12 and select on the address to use.

You can set any of the following options:
- Clear Output: if you check this, the output will be cleared for each request.
- Verbose Format: some hosts will return more information if you check this field. A host that does not support this option is supposed to ignore it. Some hosts, however, will interpret this option as part of the user name and return an error message like "Illegal character in user name". If you encounter this problem, uncheck this field and try again.

To change the font select ‘Output Font’ from the Options Menu.
You can use CTRL-F (or the ‘Find’ menu item on the Edit menu) to search the received data.

Whois

What is whois?
You can use whois to query a whois server (e.g. the InterNIC database) for names of companies, people, domain names, and IP address assignments. If you are querying an IP address you should limit your query to the first 3 parts for best results (use 125.58.65 and not 125.58.65.125).
There are many different parameters and keywords, that you can use in a whois query. Most servers will return a detailed description of the different types of query when you enter a '?' or 'HELP' in the query field.
To obtain a recent list of whois servers use 'Whols-Servers' as query and 'sipb.mit.edu' as host.
The default port number for whois is 43. To use another port number, separate the host name from the port number by a ':'. For example: Entering a host name like 'www.host.com:18' will use port 18 instead of the default port.



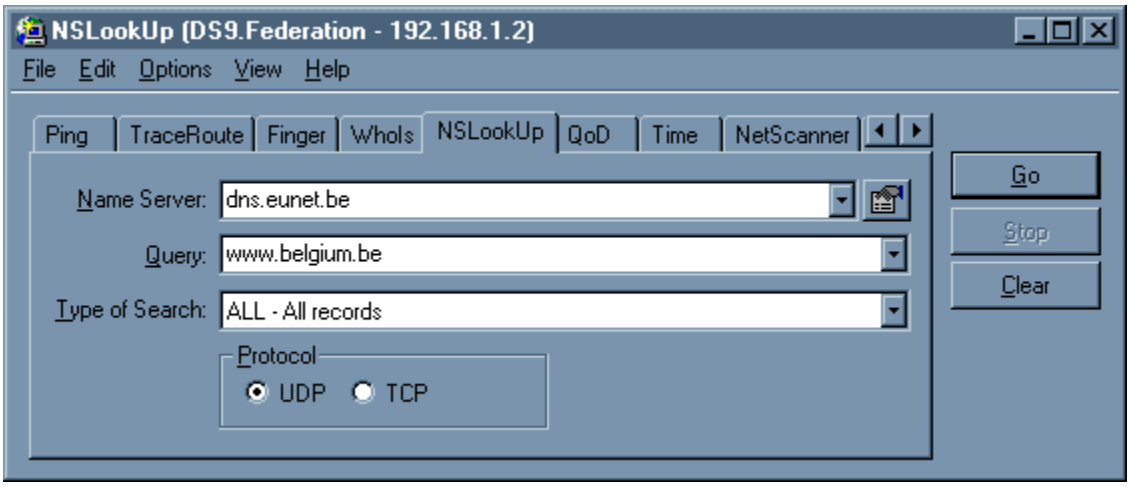
To use whois, do one of the following and press <enter> or select the Go button:
- Enter an hostname in the 'Host or Address' and a query in the 'Query' field. You can also copy the information from somewhere else and paste it in one of the above fields.
- Enter a hostname in the 'Host or Address' field.
- Select a hostname and/or query from the drop down menu.
- Open the bookmarks with F12 and select the address to use.

You can set any of the following options:
- Clear Output: if you check this, the output will be cleared for each request.

To change the font select 'Output Font' from the Options Menu.
You can use CTRL-F (or the 'Find' menu item on the Edit menu) to search the received data.

Name Server Lookup

What is nslookup?
One of the main features of nslookup is resolving a hostname into its TCP/IP addresses and vice versa. Any available aliases will also be reported.
Also you can query any DNS server on the network for specific RR (resource records).



To see additional nslookup options, click on  .

To resolve a hostname or TCP/IP address, do one of the following and press <enter> or select the Go button:
- Enter the address you want to resolve. You can use one of the following methods for this:
  - Enter an address in the 'Host or Address' field. You can also copy the address from somewhere else and paste it in the 'Host or Address' field.
  - Select an address from the drop down menu.
  - Open the bookmarks with F12 and select the address to use.
- Specify the 'Type of Search':
  - Specify 'Use Winsock Function GetHostByX' to use the standard resolve function (this function is used by most applications, like your browser, email program etc. and the other client functions in CyberKit). This function always uses the default DNS server as specified in the network settings of your computer.
  - You can also interrogate any other DNS server on the net for specific resource records. Just select the resource record in the 'Type of Search' field and enter the address or hostname of the DNS server in the 'Name Server' field.

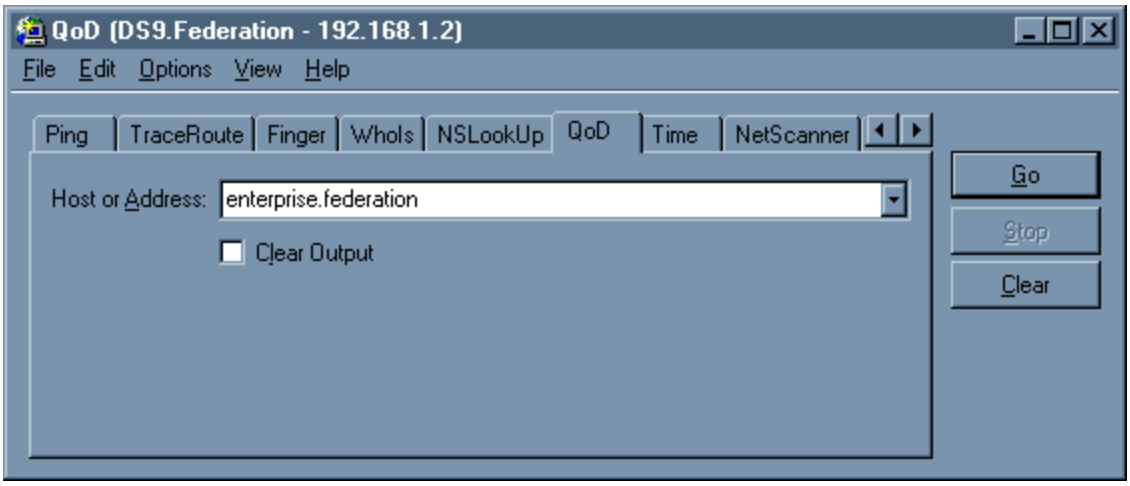
You can set any of the following options:
- Clear Output: if you check this, the output will be cleared for each request.
- Verbose Format: if you check this field, you will get a more detailed output.
- Protocol: You can choose between the UDP (faster but less reliable) or the TCP (slower but more reliable) protocol. This option is not available when you select 'Use Winsock Function GetHostByX' or the 'AXFR - Transfer of an entire zone'. This is because the first requires the UDP protocol and the latter requires the TCP protocol.

To change the font select 'Output Font' from the Options Menu.
You can use CTRL-F (or the 'Find' menu item on the Edit menu) to search the received data.

Related topics: ping, traceroute, netscanner

Quote Of The Day

What is quote of the day?
Quote of the day will connect to a quote server and return a random quote (also known as cookie). NT servers typically support quote of the day. The default port number for Quote of the day is 17. To use another port number, separate the host name from the port number by a ‘:’. For example: Entering a host name like ‘www.host.com:18’ will use port 18 instead of the default port.



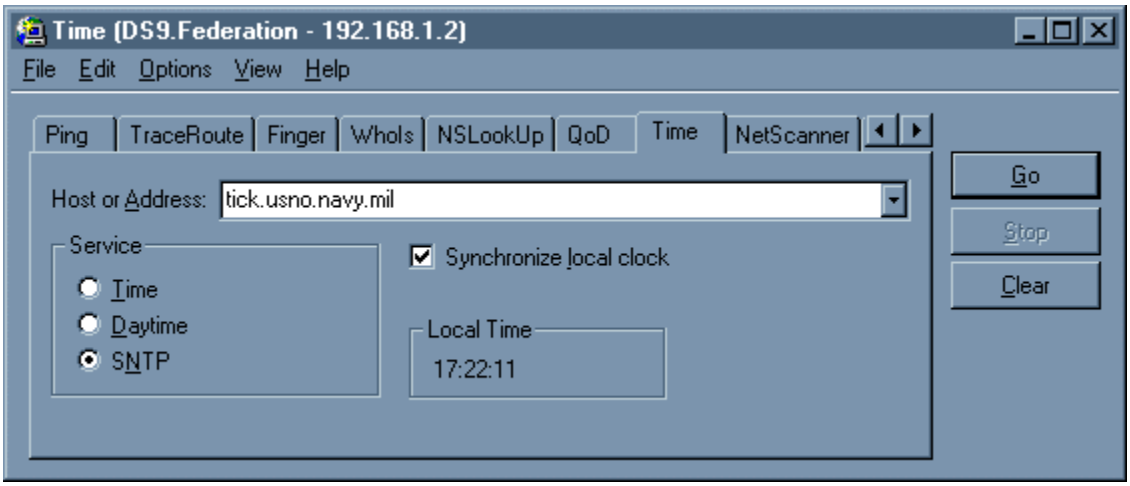
To get the quote of the day, do one of the following and press <enter> or select the Go button:
- Enter an address in the ‘Host or Address’ field. You can also copy the address from somewhere else and paste it in the ‘Host or Address’ field.
- Select an address from the drop down menu.
- Open the bookmarks with F12 and select the address to use.

You can set any of the following options:
- Clear Output: if you check this, the output will be cleared for each request.

To change the font select ‘Output Font’ from the Options Menu.
You can use CTRL-F (or the ‘Find’ menu item on the Edit menu) to search the received data.

Time

What is 'time'?
With 'time' you can connect to a time server and see the difference in time between your PC's clock and the time server. With the Time and SNTP service you can let CyberKit synchronize your PC clock.



To get the time from a time server, do one of the following and press <enter> or select the Go button:
- Enter an address in the 'Host or Address' field. You can also copy the address from somewhere else and paste it in the 'Host or Address' field.
- Select an address from the drop down menu.
- Open the bookmarks with F12 and select the address to use.

You can set any of the following options:
- Service: select the service that CyberKit should use for this request. You can select Time, Daytime or SNTP.
- Synchronize local clock: if you check this, CyberKit will synchronize your local PC clock with the time server when you press the Go button. This option is only available for the Time and SNTP service.

To change the font select 'Output Font' from the Options Menu.

Is time displaying an incorrect local time or is the synchronize feature setting your system clock to an incorrect time? Have a look at the trouble shooting section for more help!

SNTP field descriptions (extracted from RFC2030)
Leap Indicator (LI): This is a two-bit code warning of an impending leap second to be inserted/deleted in the last minute of the current day, with bit 0 and bit 1, respectively, coded as follows:

LI Meaning
---
0 no warning
1 last minute has 61 seconds
2 last minute has 59 seconds)
3 alarm condition (clock not synchronized)

Version Number (VN): This is a three-bit integer indicating the NTP/SNTP version number. The version number is 3 for Version 3 (IPv4 only) and 4 for Version 4 (IPv4, IPv6 and OSI). If necessary to distinguish between IPv4, IPv6 and OSI, the encapsulating context must be inspected.

Mode: This is a three-bit integer indicating the mode, with values defined as follows:

Mode	Meaning
0	reserved
1	symmetric active
2	symmetric passive
3	client
4	server
5	broadcast
6	reserved for NTP control message
7	reserved for private use

In unicast and anycast modes, the client sets this field to 3 (client) in the request and the server sets it to 4 (server) in the reply. In multicast mode, the server sets this field to 5 (broadcast).

Stratum: This is a eight-bit unsigned integer indicating the stratum level of the local clock, with values defined as follows:

Stratum	Meaning
0	unspecified or unavailable
1	primary reference (e.g., radio clock)
2-15	secondary reference (via NTP or SNTP)
16-255	reserved

Poll Interval: This is an eight-bit signed integer indicating the maximum interval between successive messages, in seconds to the nearest power of two. The values that can appear in this field presently range from 4 (16 s) to 14 (16284 s); however, most applications use only the sub-range 6 (64 s) to 10 (1024 s).

Precision: This is an eight-bit signed integer indicating the precision of the local clock, in seconds to the nearest power of two. The values that normally appear in this field range from -6 for mains-frequency clocks to -20 for microsecond clocks found in some workstations.

Root Delay: This is a 32-bit signed fixed-point number indicating the total roundtrip delay to the primary reference source, in seconds with fraction point between bits 15 and 16. Note that this variable can take on both positive and negative values, depending on the relative time and frequency offsets. The values that normally appear in this field range from negative values of a few milliseconds to positive values of several hundred milliseconds.

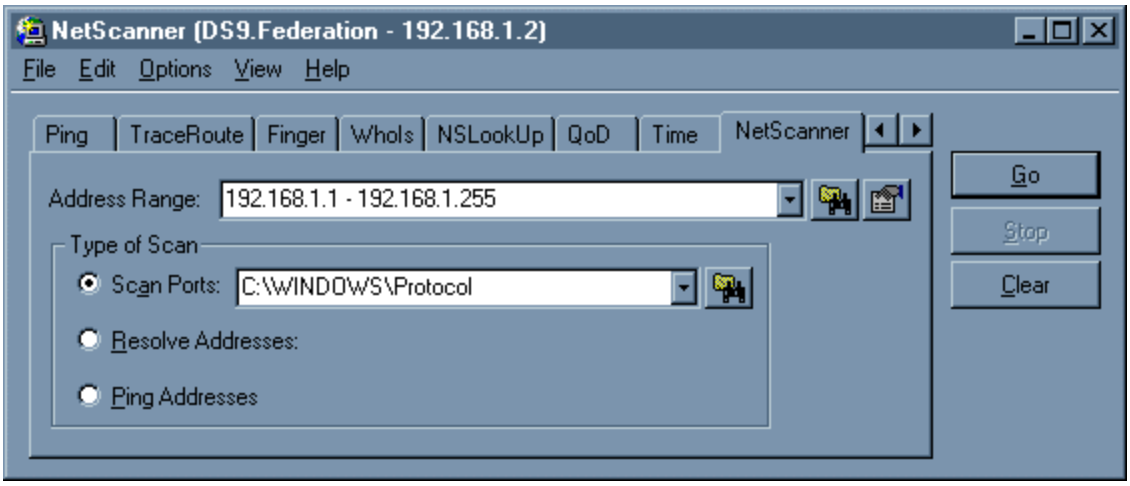
Root Dispersion: This is a 32-bit unsigned fixed-point number indicating the nominal error relative to the primary reference source, in seconds with fraction point between bits 15 and 16. The values that normally appear in this field range from 0 to several hundred milliseconds.

Reference Identifier: This is a 32-bit bitstring identifying the particular reference source. In the case of NTP Version 3 or Version 4 stratum-0 (unspecified) or stratum-1 (primary) servers, this is a four-character ASCII string, left justified and zero padded to 32 bits. In NTP Version 3 secondary servers, this is the 32-bit IPv4 address of the reference source. In NTP Version 4 secondary servers, this is the low order 32 bits of the latest transmit timestamp of the reference source. NTP primary (stratum 1) servers should set this field to a code identifying the external reference source according to the following list. If the external reference is one of those listed, the associated code should be used. Codes for sources not listed can be contrived as propriate.

Code	External Reference Source
LOCL	Uncalibrated local clock used as a primary reference for a subnet without external means of synchronization
PPS	Atomic clock or other pulse-per-second source individually calibrated to national standards
ACTS	NIST dialup modem service
USNO	USNO modem service
PTB	PTB (Germany) modem service
TDF	Allouis (France) Radio 164 kHz
DCF	Mainflingen (Germany) Radio 77.5 kHz
MSF	Rugby (UK) Radio 60 kHz
WWV	Ft. Collins (US) Radio 2.5, 5, 10, 15, 20 MHz
WWVB	Boulder (US) Radio 60 kHz
WWVH	Kaui Hawaii (US) Radio 2.5, 5, 10, 15 MHz
CHU	Ottawa (Canada) Radio 3330, 7335, 14670 kHz
LORC	LORAN-C radionavigation system
OMEG	OMEGA radionavigation system
GPS	Global Positioning Service
GOES	Geostationary Orbit Environment Satellite

NetScanner

What is ‘netscanner’?
With ‘netscanner' you can scan a range of TCP/IP addresses. For each TCP/IP address you can:
- Scan a range of ports to see what services are provided & active on that address.
- Resolve the address into a hostname.
- Ping the address to see whether it is active.



To see additional netscanner options, click on  .

Enter the address range in the ‘Address Range’ field. You can use the address range dialog to help you entering the range. Click on  to display the address range dialog.

The portscanner function
Enter the port range in the 'Scan Ports' field. You can use the port range dialog to help you enter the range. Click on  to display the port range dialog.
To retrieve the service name, Cyberkit uses the winsock database on your computer.

The resolver function
If you select the ‘name server’ setting of the netscanner client, netscanner will use this name server to resolve the range of addresses. Otherwise, netscanner will use the name server as configured in your network settings.
Select the ‘generate hosts file’ setting of the netscanner client, to generate a hosts file. This hosts file will contain the addresses that were resolved successfully.

The ping function
Select the ‘generate hosts file’ setting of the netscanner client, to generate a hosts file. The hosts file will contain the addresses that responded to ping.

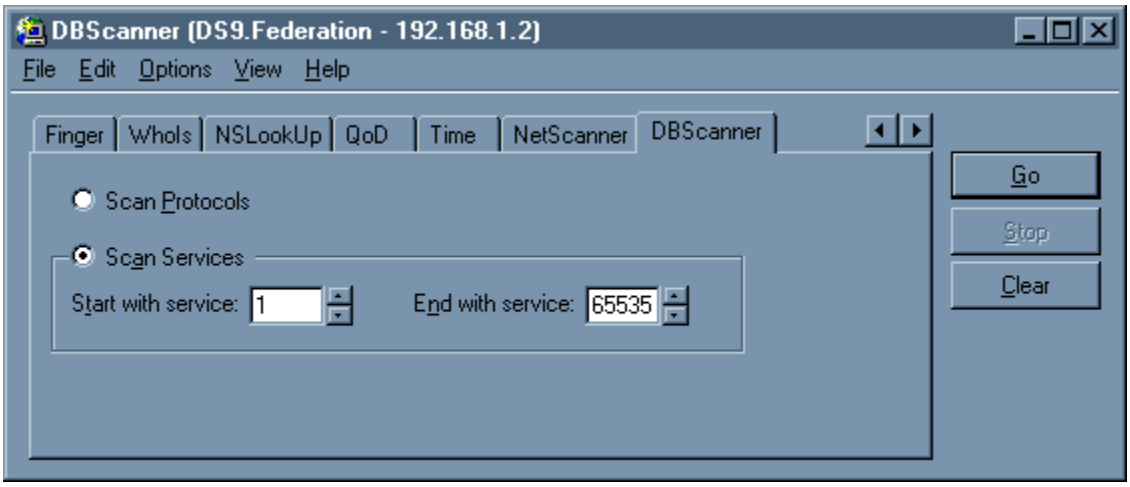
Some syntax rules for 'custom' input files:
If you want to create a 'custom' input file you need to follow some basic syntax rules. Basically you need to use the same syntax as is used in a standard HOSTS or SERVICES files:
- Lines containing only spaces are ignored.
- Lines where the first non-blank character is a '#' are ignored.
- Only the first valid TCP/IP address or port number on each line is processed.
- At the moment only the tcp protocol is supported in netscanner. If you use the SERVICES syntax to

enter port numbers (e.g. 20/tcp, 42/udp), only the ports with the tcp protocol are processed.
- The TCP/IP address and any text following it must be separated by at least one space.
- Unless you use the SERVICES syntax, a port number and any text following it must be separated by at least one space.

Related topics: sample hosts file, sample lmhosts file, sample services file, sample protocol file, ping, traceroute, dbscanner

Winsock Database Scanner

What is dbscanner?
DBscanner will scan your winsock database for available services and protocols. Absence of this database can cause problems with winsock programs. You can use this function to verify whether it is available and working properly.
Don't confuse dbscanner with netscanner. Netscanner scans a computer for **active** services, dbscanner simply displays the contents of the winsock database. This does not mean these services are actually active on your computer.
The winsock database consist of 2 text files on your computer. The names of these files are SERVICES and PROTOCOL.
Netscanner also uses this database to retrieve the name of a service.



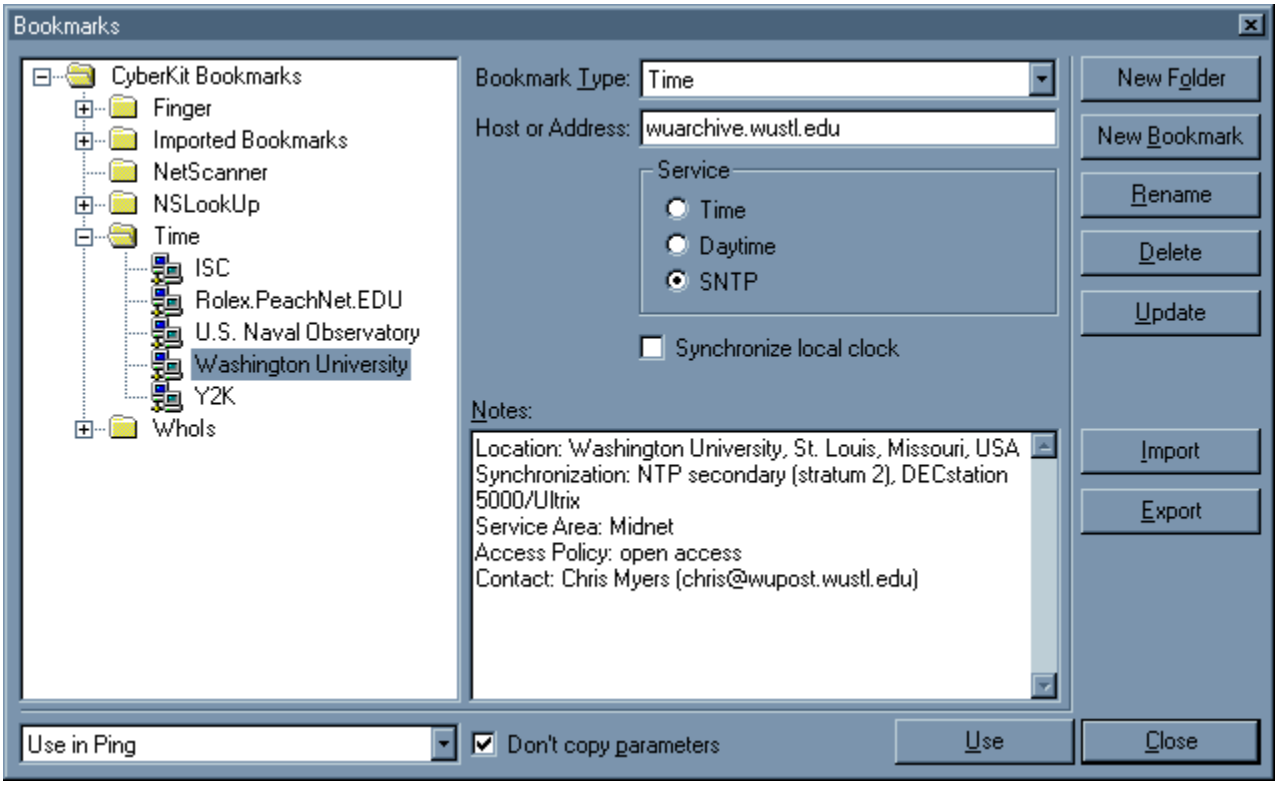
You can set any of the following options:
- Scan Protocols: Scan the winsock database for all available protocols. The scan ranges from protocol number 1 through 255.
- Scan Services: Scan the winsock database for all available services. The scan can range from port (service) 1 through 65535. If you don't want to scan this complete range (time consuming) you can specify a different range.

Related topics: sample hosts file, sample lmhosts file, sample services file, sample protocol file, netscanner

The Bookmarks

The bookmarks are stored in the CyberKit database.

What are the bookmarks?
The bookmarks are a collection of client addresses (and their parameters). This enables you to enter all the different parameters for a specific query with one mouse click. If you are using a certain query over and over again, you should enter it in the bookmarks.



The bookmark dialog is divided into 2 parts:
- On the left side you see the tree view that contains all your bookmarks.
- On the right side, you see all the parameters that belong to the bookmark that is selected in the tree view.

Each bookmark is of a specific type. The type of the bookmark links it to a CyberKit client and determines the parameters you can store along with it. You can choose between the following types: Ping, TraceRoute, Finger, WhoIs, NSLookUp, Quote Of The Day, Time and NetScanner.

When you open the bookmarks dialog, CyberKit will automatically open the relevant folder in the tree view. The folder that is opened depends on the client that is active at the time you open the bookmarks dialog. This will only work if you **don't rename the first set of folders in the tree view.**
The names of the first set of folders should be: Ping, TraceRoute, Finger, WhoIs, NSLookUp, Quote Of The Day, Time and NetScanner. The names are case sensitive so make sure you enter them exactly as shown here.
Since this feature significantly improves the use of the bookmarks dialog, I strongly suggest you do not rename the first set of folders. Inside these folders, you can, ofcourse, organize your bookmarks in any way you see fit.

Adding a folder

Select the folder where you want to add a new subfolder and click on the ‘‘New Folder’’ button. A folder with the name ‘‘New Folder’’ is added to the tree view. The cursor will be positioned on the folder name so you can directly edit the name for the new folder. When you are finished, press ‘‘enter’’ to store the new folder.

Renaming a folder
Select the folder in the tree view and press the ‘‘Rename’’ button. Enter the new name and press ‘‘enter’’ to store it.

Deleting a folder
Select the folder in the tree view and press the ‘‘Delete’’ button. You can also use the delete key on your keyboard.

Moving a folder
Select the folder in the tree view. While keeping the left mouse button down, drag the folder to its new destination in the tree view. Moving a folder will also move all the bookmarks and subfolders that are contained in the folder.

Adding a bookmark
First you need to add an entry to the tree view. Select the folder where you want to add the bookmark and click on the ‘‘New Bookmark’’ button. A bookmark with the name ‘‘New Bookmark’’ is added to the tree view. The cursor will be positioned on the bookmark name so you can directly edit the name for the new bookmark. When you are finished, press ‘‘enter’’ to store the new bookmark.
Next, while the bookmark is still selected in the tree view, select the bookmark type and enter the parameters you want to store along with the bookmark. When you are finished entering the parameters, click on the ‘‘Update’’ button to store the bookmark settings.

Tip: If you have just done a query in one of the CyberKit clients and want to store it in the bookmarks, select the ‘‘Add to Bookmarks’’ from the edit menu. The query, along with all its parameters are added to the bookmarks. All you have to do is enter a name for the new bookmark and you are done.
If you have not renamed the first set of folders (see the discussion above), CyberKit will add the bookmark to the folder that corresponds with the active client.

Renaming a bookmark
Select the bookmark in the tree view and press the ‘‘Rename’’ button. Enter the new name and press ‘‘enter’’ to store it.

Deleting a bookmark
Select the bookmark in the tree view and press the ‘‘Delete’’ button. You can also use the delete key on your keyboard.

Moving a bookmark
Select the bookmark in the tree view. While keeping the left mouse button down, drag the bookmark to its new destination in the tree view.

Changing the parameters of a bookmark
Select the bookmark in the tree view. Next enter the new parameters. When you are finished entering the paramerters, click on the ‘‘Update’’ button to store the new settings.

Changing the type of a bookmark
Select the bookmark in the tree view. Next select the new bookmark type. Since each bookmark type has different parameters, you will lose the previous parameters when you change the bookmark type.

Importing bookmarks
Press the ‘‘Import’’ button to import bookmarks.

You can use this function to import the address book from release 2.4. A new folder “Imported Bookmarks” will be created and all the imported bookmarks will reside in this folder. Since the address book from release 2.4 did not store any parameters along with the bookmarks, you will need to do some editing after importing it.
CyberKit comes with a collection of sample bookmarks that you can import if you like. The file is called Bookmark.cbm and is located in the CyberKit directory.

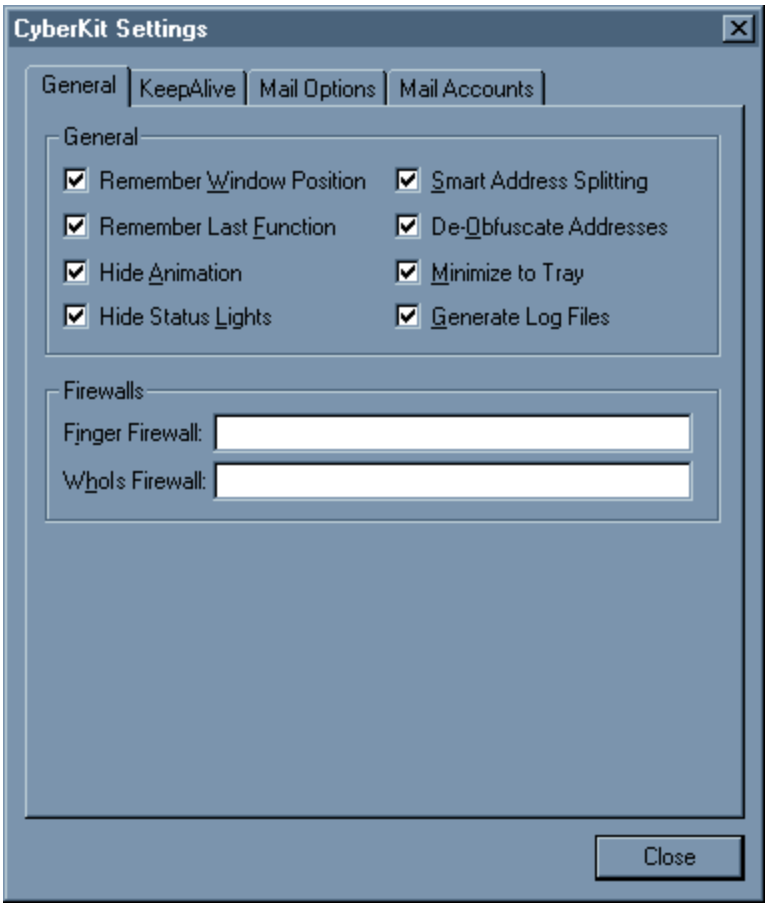
Exporting bookmarks
Press the “Export” button to export bookmarks.
You can use this function to exchange bookmarks with versions of CyberKit that are located on another computer.

Using a bookmark
This is what the bookmarks are all about. You want to copy the information from the bookmarks dialog to your client inside CyberKit.
- Select the bookmark in the tree view.
- Use the list box, located in the lower left corner of the bookmarks dialog, to select the client where you want to use the bookmark.
- If you don’t want to copy the parameters, check the ‘Don’t copy parameters’ box.
- Press the “Use” button.

Tip: Double clicking on a bookmark in the tree view has the same effect as clicking on the “Use” button.

As a shortcut for the bookmarks dialog, you can use F12.

The General Options Dialog



Remember Window Position
Check this if you want CyberKit to remember its window position. This way CyberKit will start where you last left it.

Remember Last Function
Check this if you want CyberKit to remember the last used function. This way CyberKit will start with the last used function.

Hide animation
Check this if you don't want to see the little animation when CyberKit is active.

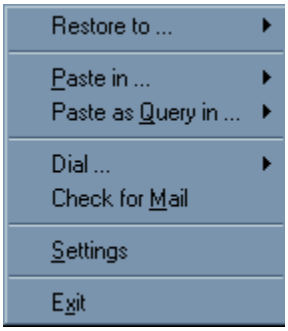
Hide Status Lights
Check this if you don't want to see the CyberKit status lights (located above the Go button).

Smart Address Splitting
Check this if you want CyberKit to automatically split addresses at the @ sign when entered in the finger or whois client. This is very useful when you paste email addresses in the host or query field.
If you check this option, CyberKit will also filter the hostname out of an url (http://…) or ftp (ftp://…) address when you enter them in address fields.

De-Obfuscate Addresses
Check this if you want CyberKit to automatically de-obfuscate addresses when you paste or enter them in address fields.

Minimize To Tray (not available on Windows NT 3.51 and lower)
Check this if you want CyberKit to minimize to the tray. CyberKit will add an icon to the tray and when you minimize CyberKit, it will remove itself from the task bar. The icon will show a little lightning flash whenever CyberKit is doing something. The color of this lightning flash indicates what is happening:
- Yellow: A client function is active (ping, traceroute, etc.)
- Green: CyberKit is checking for new mail.
- Blue: CyberKit is keeping your connection alive.
- Red: CyberKit is dialing your connection.

If you left click on the CyberKit tray icon, CyberKit will restore itself to its last position.



If you right click on the CyberKit tray icon, you will get a popup menu. See the CyberKit contextmenus for more information.

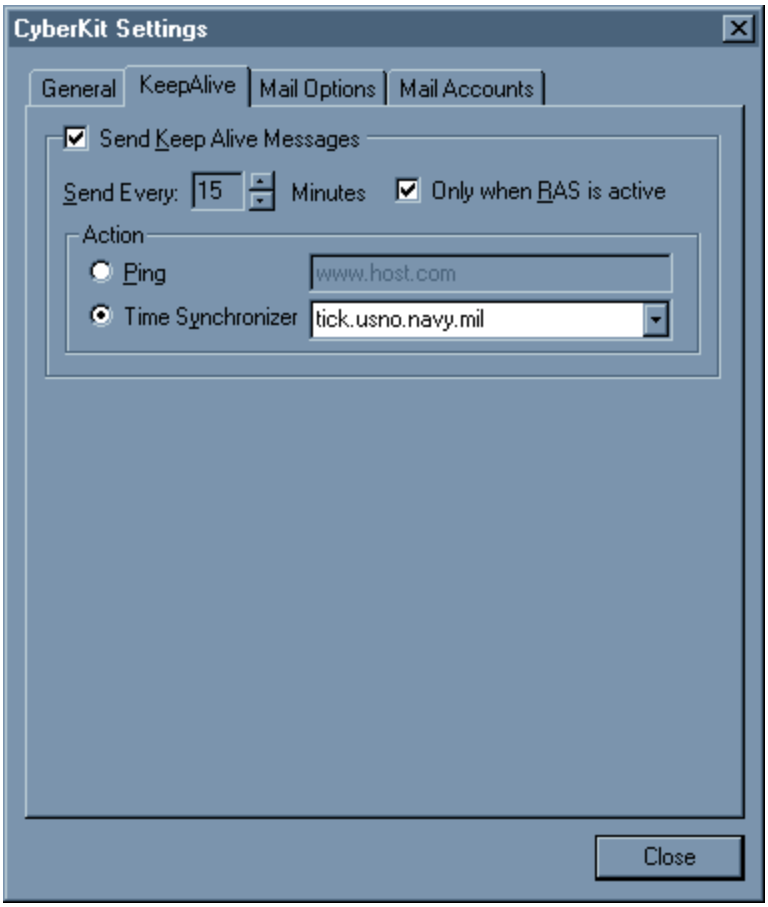
Generate Log Files
If you check this option, all the CyberKit clients (like ping, finger, etc.) will create log files in the CyberKit directory.
Each client has a separate log file. You can use these log files for diagnostic purposes. This is especially usefull for the clients that work in the background, like keepalive and checkformail. Therefor, I recommend you leave this option on. You don't need to worry about disk space, the files are small and there is only one log file for each client.

Finger Firewall
If you have to use a firewall for finger, enter it here.

Whois Firewall
If you have to use a firewall for whois, enter it here.

Related topics: the keepalive options dialog, the mail options dialog, the mail accounts dialog

The KeepAlive Options Dialog



Send KeepAlive Messages
Check this if you want CyberKit to keep your connection alive. The second light above the 'Go' button indicates the status of this function.

Send every x minutes
Specify the interval between keep alive messages. Keep Alive only becomes active if there is an active dialup connection.

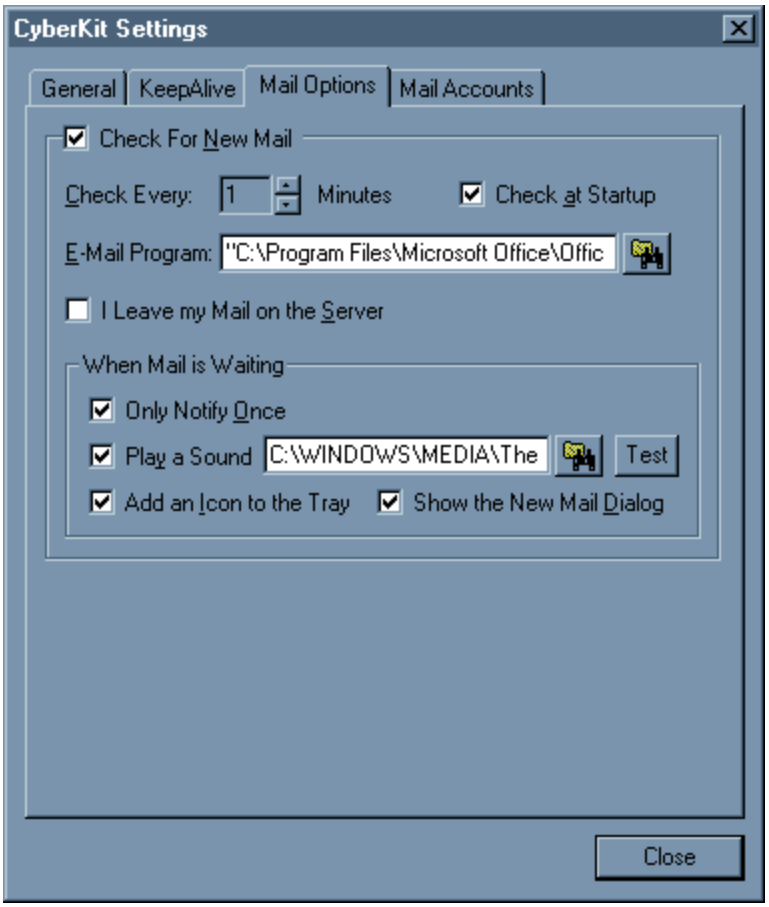
Only when RAS is active
Check this option when you only want KeepAlive to function when there is a RAS connection active. If, however, you don't use RAS, you can disable this option and KeepAlive will function all the time.

Ping
If you want KeepAlive to use the ping client to keep your connection alive, specify a host in this field. CyberKit will ping this host periodically.

Time Synchronizer
If you want KeepAlive to use the time client to keep your connection alive, enter a timeserver in this field. CyberKit will synchronize your PC clock with this timeserver periodically.

Related topics: the general options dialog, the mail options dialog, the mail accounts dialog

The Mail Options Dialog



Check For New Mail
Check this if you want CyberKit to check for new mail. You can configure you mail accounts in the mail accounts dialog. At this time only the POP3 protocol is supported. Check with your system administrator for more information about the POP3 protocol. The third light above the 'Go' button indicates the status of this function.

Check Every x Minutes
Specify how often CyberKit has to check for new mail.

Check at startup
Check this if you want CyberKit to check for new mail when you start it.

E-Mail Reader
If you enter the full path and filename for your E-mail reader here, a left click on the new mail icon in the tray will launch your E-mail reader. If the path or filename of your E-mail reader contains spaces, you'll have to enclose it with double quotes. Any command line parameters must be separated by a space and located outside the quotes.
If you're an Internet Mail user, try this: "C:\WINDOWS\EXPLORER.EXE" /root,C:\WINDOWS\Internet Mail.{89292102-4755-11cf-9DC2-00AA006C2B84}

I Leave my Mail on the Server
Check this option if your mail client does not remove your mail from the server after you've read it.

Only Notify Once
If you enable this option, CyberKit will only notify you once of new mail. The number of messages in the new mail dialog will still be updated.

Play a sound
Enter any .wav file you want. If you don't specify any .wav file, CyberKit will use the default PC-speaker beep.

Add an icon to the tray (not available on Windows NT 3.51 and lower)
CyberKit will add an icon to the Tray when there is mail waiting for you. A left click on this icon will launch the new mail dialog, a right click will show the new mail menu. If you let your mouse cursor hover above this icon, a message will appear with the number of new mail messages.

Show the new mail dialog box
CyberKit will pop up the new mail dialog whenever there is new mail waiting for you.

Remarks:
CyberKit will **NOT** notify you of new mail in the following cases:

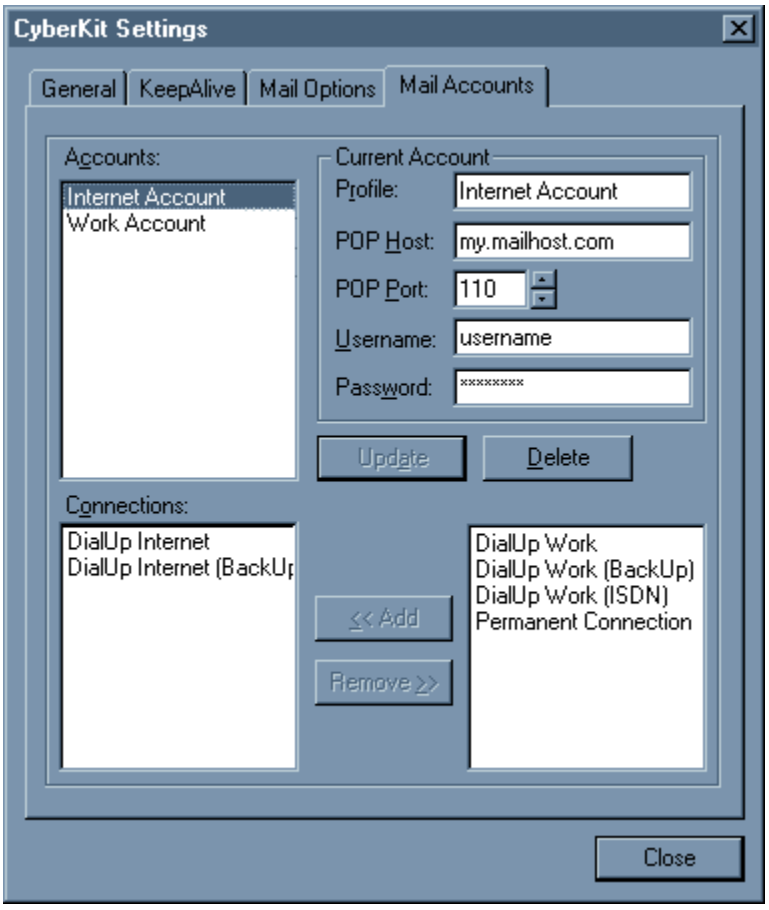
1) The number of messages has not changed since the last check.
2) The number of messages has grown since the last check and you have the 'Only Notify Once' option enabled (this does not apply if the number of messages in the last check was zero). In this case the number of messages in the new mail dialog will still be updated.

Related topics: the general options dialog, the keepalive options dialog, the mail accounts dialog, the new mail dialog

The Mail Accounts Options Dialog

The mail accounts are stored in the CyberKit database.

What is the mail accounts dialog?
In this dialog you can configure your mail accounts. Each mail accounts consists of: a profile name, POP host, POP port number (defaults to the standard POP port number 110), user name, password and a list of dialup connections.
The profile name is what you will see in the new mail dialog, you can choose it freely.
The list of dialup connections contains all dialup connections through which the selected mail account is accessible. Each mail account can have a different list of dialup connections. CyberKit will only check those mail accounts for which at least one of the dialup connections is active.
The 'Permanent Connection' is a special dialup connection that you can select when for example you have a permanent LAN connection through which you can access your mail account. In this case CyberKit will always check this mail account, no matter which dialup connections are active.
In order for CyberKit to check your mail account you must specify either 'Permanent Connection' or at least one dialup connection.



To enter a new account
Enter the profile name and the new account information in the 'Current Account' area and select the Add button.
You cannot enter 2 accounts with the same profile name.

To delete an existing account
Select the profile name for the account you want to delete in the 'Accounts' list and select the Delete

button.

To modify an existing account
Select the profile name for the account you want to change in the ‘Accounts’ list. The account information will appear in the ‘Current Account’ area. Make the desired changes and select the Modify button.
If you change the profile name for an existing account, the Add button will appear instead of the Modify button. Select the Add button to add the new account and then delete the account with the incorrect profile name.

To add or remove dialup connections from an account
If the account does not exist, create it first.
Select the account in the ‘Accounts’ list. The account information will appear in the ‘Current Account’ area. Any dialup connections that are currently associated with this account will appear in the ‘Connections’ list.
To add a connection, select it in the lower right list and press the Add button. The connection will appear in the ‘Connections’ list.
To remove a connection, select it in the ‘Connections’ list and press the Remove button. The connection will disappear from the ‘Connections’ list.
The ‘Permanent Connection’ cannot be combined with any other dialup connection. If you want to add this connection, you’ll have to remove all other dialup connections first.

Related topics: the general options dialog, the keepalive options dialog, the mail options dialog, the new mail dialog

The Command Line Parameters

Using command line parameters you can customize the way CyberKit starts. For example: you could start CyberKit minimized in the tray, or you can create a shortcut that will synchronize your PC clock with a time server when you double click on it.
Different command line parameters are separated by a '?'.
There are 3 types of command line parameters:

Client selection
You can use these command line parameters when you want to activate a specific client function, like Ping or Time, when you start CyberKit.

To activate the Ping client you can use the following command line parameter:
"Client=Ping"

Most of the time you will also want to specify an IP address or a hostname:
"Client=Ping?Address=www.belgium.be"

A better syntax for combining the "Client" and "Address" parameters is:
"Ping://www.belgium.be"

Client settings
Each client function has a number of settings that can be specified on the command line. You could specify a timeout value for Ping, a time server for Time, etc. Most of these settings are client specific, for example the "Packet Size" parameter has no meaning for the Time client.

Ping client parameters
"Timeout=5": The timeout in seconds.
"Delay=500": The delay in miliseconds.
"Packets=5": The number of ICMP packets to send.
"Packet Size=128": The size of the ICMP packet in bytes.

Examples:
"Client=Ping?Address=www.belgium.be?Packets=3?Timeout=3"
"Ping://www.belgium.be?Packets=5?Packet Size=64"
"Ping://www.belgium.be?Timeout=5?Delay=300?Packets=3?Packet Size=128?Activate"

You can find more information about these settings in the ping section of this help file.

Traceroute client parameters
"Timeout=5": The timeout in seconds.
"Start From Hop=1": The starting hop number.
"End With Hop=30": The ending hop number.
"Packet Size=128": The size of the ICMP packet in bytes.

Examples:
"TraceRoute://www.belgium.be?Timeout=5"
"TraceRoute://www.belgium.be?Timeout=5?Start From Hop=2?End With Hop=30?Activate"

You can find more information about these settings in the traceroute section of this help file.

Finger client parameters
"Query=my.email@address": The finger query.

Examples:
"Finger://l.gp.cs.cmu.edu?Query=coke"
"Finger://l.gp.cs.cmu.edu?Query=coke?Activate"

You can find more information about these settings in the finger section of this help file.

Whois client parameters
"Query=WhoIs-Servers": The whois query.

Examples:
"WhoIs://sipb.mit.edu?Query=WhoIs-Servers"
"WhoIs://sipb.mit.edu?Query=WhoIs-Servers?Activate"

You can find more information about these settings in the whois section of this help file.

NSLookup client parameters
"Query=www.belgium.be": The nslookup query.
"Type Of Search=GetHostByX": The type of search.
"Protocol=UDP":The protocol to use. Can be any of the following: 'TCP', 'UDP'.

Examples:
"NSLookUp://ns.internic.net?Query=www.belgium.be?Type Of Search=MX?Protocol=UDP"
"NSLookUp://ns.internic.net?Query=www.belgium.be?Type Of Search=GetHostByX?Protocol=TCP?Activate"

You can find more information about these settings in the nslookup section of this help file.

Quote of the day client parameters
There are no quote of the day parameters.

Example:
“Quote Of The Day://www.quote.com?Activate”

You can find more information about these settings in the quote of the day section of this help file.

Time client parameters
"Service=SNTP": The service you want to use. Can be any of the following: 'Time', 'Daytime', 'SNTP'
"Synchronize Local Clock": If you want to synchronize your PC clock.

Examples:
"Time://norad.arc.nasa.gov?Service=SNTP"
"Time://norad.arc.nasa.gov?Service=SNTP?Synchronize Local Clock?Minimize To Tray?Activate?Quit"

You can find more information about these settings in the time section of this help file.

Netscanner client parameters
"Port Range=1-65535": The range of ports to scan. This can also be a file, "Port Range=d:\folder\file.txt".
"Type Of Scan=Scan Ports": The type of scan you want to perform. Can be any of the following: 'Scan Ports', 'Resolve Addresses', 'Ping Addresses'

Examples:
"NetScanner://192.168.0.0 - 192.168.0.255?Port Range=1 - 500?Type Of Scan=Scan Ports"
"NetScanner://c:\inputfile.txt?Type Of Scan=Resolve Addresses?Activate"

You can find more information about these settings in the netscanner section of this help file.

General Settings
These settings are not related to a specific client function.

“Don’t Open DB”: CyberKit will not try to open the database. Read the discussion in the CyberKit database section for more information.
"Minimize To Tray": If you want to minimize CyberKit to the tray when you start it.
"Dial=RAS connection": When you want to dial a RAS connection when you start CyberKit.
"Activate": When you want the client function to start without having to press the 'GO' button.
"Quit": When you want CyberKit to quit as soon as the requested action is finished.

Examples:
"Time://norad.arc.nasa.gov?Service=SNTP?Synchronize Local Clock?Minimize To Tray?Dial=My Provider?Activate?Quit"

How to enter command line parameters
- Right click on the CyberKit icon
- Select properties
- Append the command line parameters to the target field.

For example, suppose you want to start CyberKit with the ping tab and minimized to the tray:
If CyberKit is located in the C:\Program Files\CyberKit folder you should enter the following in the target field:
“C:\Program Files\CyberKit\CyberKit.exe” "Ping://www.host.com?Minimized To Tray"

Shortcut Keys in CyberKit

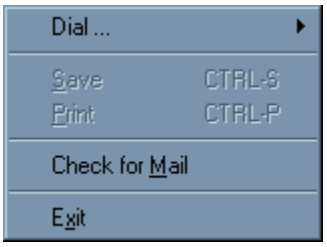
You can use the ENTER key as a shortcut for the GO button, and the ESC key as a shortcut for the STOP button. CTRL-TAB switches to the next tab, CTRL-SHIFT-TAB switches to the previous tab. Whenever there is a button or text field with a underlined letter, you can press ALT-<underlined letter> as a shortcut key for that button or for selecting that text field.
Some examples:
- ALT-g is a shortcut for the GO button
- ALT-a, in most functions, is a shortcut for jumping to the 'host or address' field.
- ALT-v (shortcut for the view menu) followed by ALT-w (shortcut for the winsock information item in the view menu) shows you the winsock information dialog.
- ALT-F4 terminates CyberKit
- CTRL-M shows the new mail dialog
- CTRL-F shows the find dialog
- CTRL-P print client results
- CTRL-S save client results to a file
- F3 finds the next occurrence of the search string
- F1 shows the help file
- F9 shows the options dialog
- F10 shows the output font dialog
- F11 shows the Winsock Information dialog
- F12 shows the bookmarks dialog

Cyberkit also supports the standard shortcut keys of the edit boxes:
Use CTRL-C to copy text to the clipboard, CTRL-V to paste text from the clipboard, CTRL-X to cut text to the clipboard. CTRL-Z will undo your last action in the edit box.

The Menus

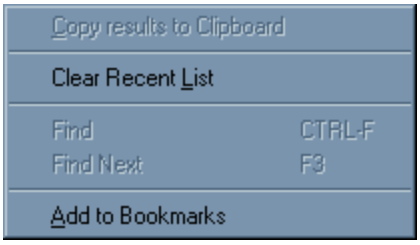
There are five available menus in CyberKit.

The file menu



Dial …: This will bring up a list of your RAS dialup connections. If you select any of these dialup connections, CyberKit will dial the connection for you. If you have more than 10 dial-up connections, a dialog box will open, containing all your dial-up connections.
Save: Saves the results of the active client to a file.
Print: Prints the results of the active client.
Check for Mail: CyberKit will check your mail accounts for new mail. Whether CyberKit checks a specific mail account for new mail is determined by the mail account configuration.
Exit: Quit CyberKit.

The edit menu



Copy results to Clipboard: Copies the results of the active client to the windows clipboard.
Clear Recent List: Clears the recent list boxes of the active client.
Find: This will bring up the find dialog. This menu item is only available in the finger, whois, nslookup, time and quote of day client.
Find Next: Searches for the next occurrence of the search string. The search string is entered by using the find dialog. This menu item is only available in the finger, whois, nslookup, time and quote of day tab.
Add to Bookmarks: This will bring up the bookmarks dialog and initialize a new entry with data from the active client.

The options menu

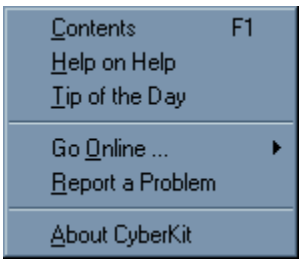
Settings: This will bring up the options dialog.
Compact Database: This will compact the CyberKit database.
Output Font: This will bring up the font selection dialog. This menu item is only available in the finger, whois, nslookup, time and quote of the day client. The selected font will be used to display the results of

the active client.

The view menu

Winsock Information: This will bring up the winsock information dialog.
New Mail Dialog: This will bring up the new mail dialog.
Bookmarks: This will bring up the bookmarks dialog.

The help menu



Contents: Activate the help file and switch to the help contents page.
Help on Help: Activate the standard windows help on help file. This help file contains usefull information about how to effectively use the windows help files.
Tip of the Day: This will bring up the tip of the day dialog.
Go Online and …:

- **Visit CyberKit Homepage:** This will start your Web Browser and point it to the CyberKit HomePage. Use this to go online and check for new releases, bug reports, etc.
- **Give Feedback:** This will start your e-mail program so you can send me a message with your feedback information.

Report a Problem: Shows the help file section about reporting problems.
About CyberKit: Select this menu item to see the about box.

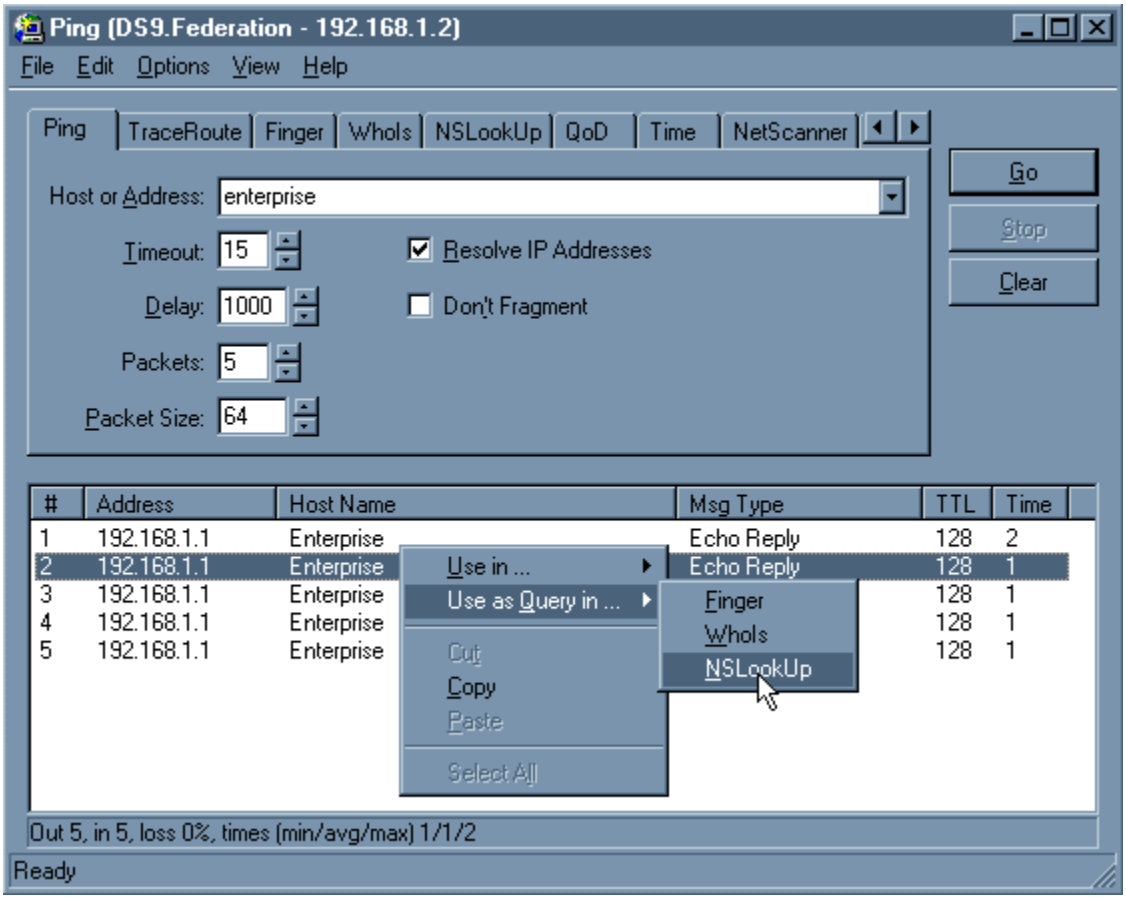
Related topics: the context menus

The Context Menus

There are 2 different context menus in CyberKit.

The edit context menu

This menu is supported by most of the CyberKit input and output fields. Activate the menu by clicking the right mouse button above the field.

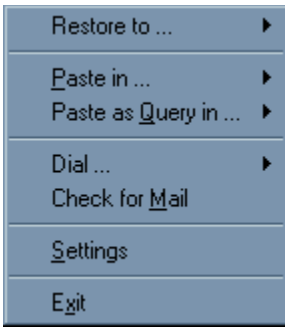


Use in …: This will bring up a list of CyberKit clients. If you select any of these clients, CyberKit will switch to this client and copy the selected text into the host field of this client.
Use as Query in …: This will bring up a list of CyberKit clients. If you select any of these clients, CyberKit will switch to this client and copy the selected text into the query field of this client.

Cut: Remove the selected text from the field under the mouse cursor and copy it to the windows clipboard.
Copy: Copy the selected text from the field under the mouse cursor to the windows clipboard.
Paste: Copy the text from the windows clipboard into the field under the mouse cursor.
Select All: Select all the text in the field under the mouse cursor.

The tray context menu

Activate this menu by right clicking the right mouse button above the CyberKit tray icon.



Restore to …: This will bring up a list of CyberKit clients. If you select any of these clients, CyberKit will switch to this client. If CyberKit was minimized to the tray it will restore itself first.
Paste in …: This will bring up a list of CyberKit clients. If you select any of these clients, CyberKit will switch to this client and copy the text from the windows clipboard into the host field of this client.

Paste as Query in …: This will bring up a list of CyberKit clients. If you select any of these clients, CyberKit will switch to this client and copy the text from the windows clipboard into the query field of this client.

Dial …: This will bring up a list of your RAS dialup connections. If you select any of these dialup connections, CyberKit will dial the connection for you. If you have more than 10 dial-up connections, a dialog box will open, containing all your dial-up connections.

Check for Mail: CyberKit will check your mail accounts for new mail. Whether CyberKit checks a specific mail account for new mail is determined by the mail account configuration.

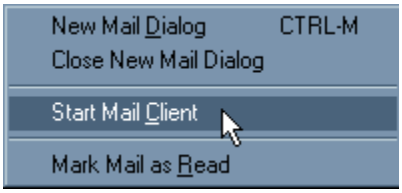
Settings: This will bring up the options dialog.

Exit: Quit CyberKit.

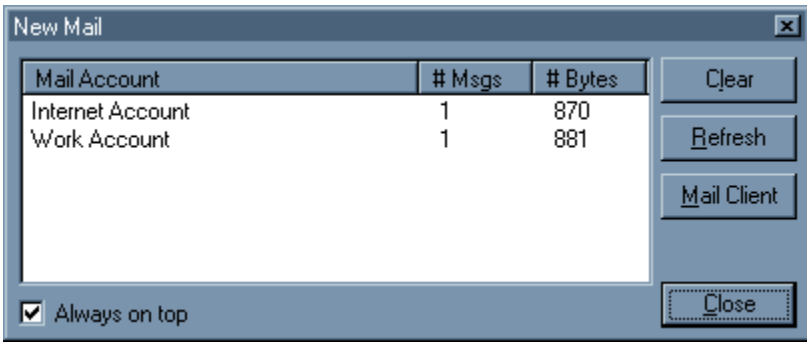
Related topics: the menus

The New Mail Dialog

What is the new mail dialog?
The new mail dialog shows you a list of mail accounts that have received new mail since you last checked. You can configure this dialog to be displayed automatically when CyberKit detects there is new mail for you, or you can activate this dialog from the view menu.
This dialog will also appear if you left click the new mail icon in the tray. A right click on this icon will show the following menu:



You can open/close the new mail dialog and start your mail reader from this menu.
The 'Mark Mail as Read' option will cause CyberKit to consider your mail as read (see the remarks section below for more information).



Use the 'Clear' button to clear the accounts in the dialog.
Use the 'Refresh' button to make CyberKit check for new mail. If new mail is detected the numbers in the dialog will be updated to reflect the current status.
Use the 'Mail Client' button to launch you mail reader. You can configure your mail reader in the mail options dialog.
Use the 'Close' button to close this dialog.
Select 'Always on top' if you don't want the new mail dialog to disapear behind other windows.

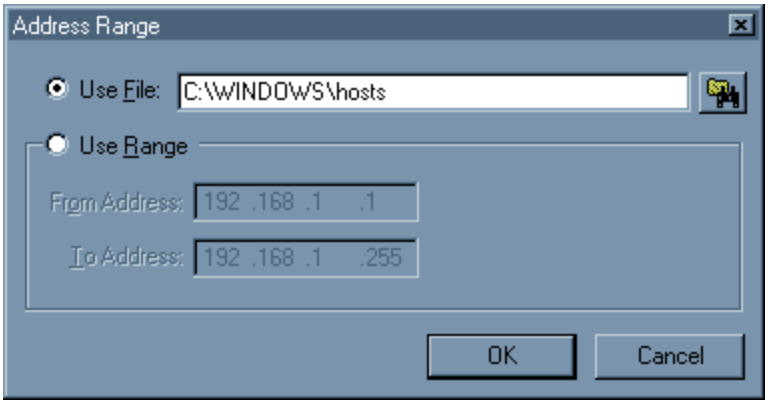
Remarks:
If you don't leave you mail on the server, detecting new mail is pretty straight forward. CyberKit will simply check your mail account and any mail present is considered new mail. Whenever you read this mail with your mail reader, it will be deleted from the server. The next time CyberKit checks for new mail, your account will be empty, and that's it!
If you leave your mail on the server, there is no easy way for CyberKit to determine which mail you've already read and which mail is new. Therefor, CyberKit keeps track of the number of messages in your mail account. New mail is detected when this number increases. Whenever you use the 'Mail Client' or the 'Close' button on the new mail dialog, CyberKit considers your mail as read and will only notify you again when the number of messages increases. The same applies for the 'Mark Mail as Read' option on the new mail menu.

As a shortcut for the New Mail Dialog item on the View menu, you can use CTRL-M.

Related topics: the mail options dialog, the mail accounts dialog

The Address Range Dialog

The address range dialog is used by the netscanner client of CyberKit. You use it to enter the range of addresses you want to scan.

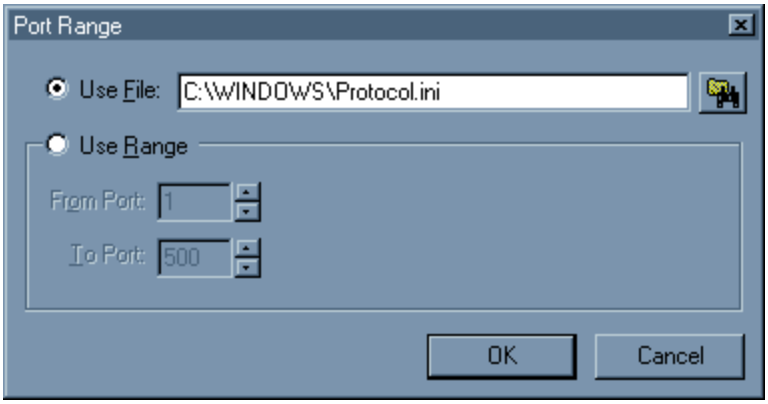


This address range can be any of the following:
- A singe TCP/IP address.
- Two TCP/IP addresses separated by a '-'.
- A file name that contains a number of TCP/IP addresses. CyberKit can handle standard hosts and lmhosts files.

Related topics: the port range dialog, netscanner, sample hosts file, sample lmhosts file

The Port Range Dialog

The port range dialog is used by the netscanner client of CyberKit. You use it to enter the range of ports you want to scan.

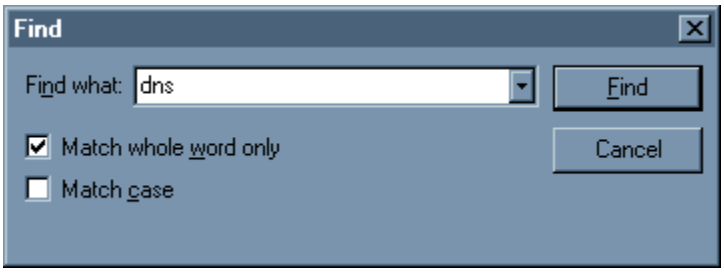


This port range can be any of the following:
- A single port number.
- Two port numbers separated by a '-'.
- A file name that contains a list of port numbers. CyberKit can handle standard PROTOCOL and SERVICES files.

Related topics: the address range dialog, netscanner, sample services file, sample protocol file

The Find Dialog

What is the find dialog?
You can use the find dialog to search for a specific text string in the CyberKit results. This option is only available in the client functions that contain a text output field. These are: finger, whois, nslookup, time and quote of the day.



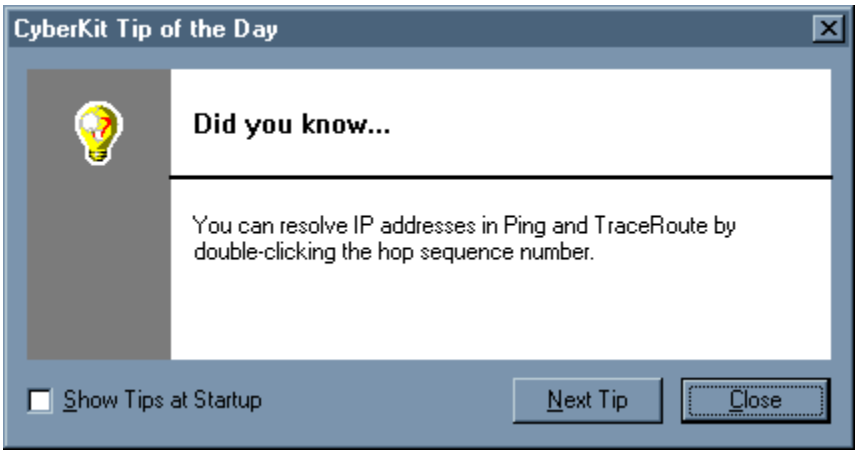
To search for a word or string, do one of the following and press <enter> or select the Find button:
Enter a search string in the 'Find what' field. You can also copy the string from somewhere else and paste it in the 'Find what' field.

You can set any of the following options:
- Match whole word only: if you check this, a search string 'out' will find the word 'out' but not the word 'output'.
- Match case: if you check this, a search string 'output' will find the word 'output' but not the word 'Output'.

As a shortcut for the Find item on the Edit menu, you can use CTRL-F. F3 will search for the next occurrence of the search string you entered in the Find Dialog.

The Tip of the Day Dialog

What is the tip of the day dialog?
This dialog will display a random tip each time it is displayed. The tips are read from the tips.dat file in the CyberKit directory.



If you no longer want to see this dialog when you start CyberKit, clear the 'Show Tips at Startup' field in the tips of the day dialog. If, at a later time, you want to reactivate the tips of the day dialog, you can re-activate it from the help menu.

Privacy Issues

With the Internet and the growing interconnectivity between computers, privacy has become a hot issue. Rumors about applications taking a snapshot of what is installed on your computer and then sending that information over the net to the manufacturer (without your knowledge) are at the least disturbing.

I can assure you CyberKit does not send any information whatsoever over the line except for what is absolutely necessary to perform the requested function.
For example, when CyberKit is checking for new mail, it has to log on to your POP account. This includes sending user id and password over the line. I think it is clear that this can not be avoided. Your e-mail client will have to do the same. Just be aware that this is happening and change your password frequently! CyberKit does encrypt the password, but I'm not a cryptographer, so I can assure you that if someone with bad intentions has access to it, he will be able to decipher your password (even if I was a cryptographer, given enough time and computer power, any code can be broken!).

The Status Lights

 3 lights

Just above the ‘Go’ button you can see 3 status lights:
- The first indicates that one of the functions: ping, traceroute, finger, whois, nslookup or quote of the day is active.
- The second is used by the Keep Alive function.
- The third is used by the Check For New Mail function.

The color of the lights changes when the funciton is active or if some error occurred:
- A green light indicates the function is active.
- A red light indicates something went wrong. In this case, you can use the generate log files option to track down the problem.

Note: It is possible to hide the status lights. See the general options for more information.

Sample Hosts File

Depending on your windows version, the hosts file is located in different folders. Usually there is also a hosts.sam file. This is just a sample file and is not used by Windows.
On windows 95 you can find it in the windows folder.
On windows NT you can find it in the winnt/system32/drivers/etc folder.
Because you can choose the name of your windows folder when you install windows, the name of the windows folder can be different on your computer. The folders above are the default values.

```
# Copyright (c) 1994 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Chicago
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1   localhost
192.168.1.1 Enterprise
192.168.1.2 DS9
```

Related topics: sample lmhosts file, sample services file, sample protocol file, netscanner

Sample Lmhosts File

Depending on your windows version, the lmhosts file is located in different folders. Usually there is also a lmhosts.sam file. This is just a sample file and is not used by Windows.
On windows 95 you can find it in the windows folder.
On windows NT you can find it in the winnt/system32/drivers/etc folder.
Because you can choose the name of your windows folder when you install windows, the name of the windows folder can be different on your computer. The folders above are the default values.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows
# NT.
#
# This file contains the mappings of IP addresses to NT computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the comptername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#      #PRE
#      #DOM:<domain>
#      #INCLUDE <filename>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addtion the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
#
\machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessio
nshares
# in the registry. Simply add "public" to the list found there.
```

```
#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino         #PRE #DOM:networking  #net group's DC
# 102.54.94.102    "appname  \0x14"                     #special app server
# 102.54.94.123    popular            #PRE             #source server
# 102.54.94.117    localsrv           #PRE             #needed for the
include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.
```

Related topics: sample hosts file, sample lmhosts file, sample services file, sample protocol file, netscanner

Sample Services File

Depending on your windows version, the services file is located in different folders.
On windows 95 you can find it in the windows folder.
On windows NT you can find it in the winnt/system32/drivers/etc folder.
Because you can choose the name of your windows folder when you install windows, the name of the windows folder can be different on your computer. The folders above are the default values.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This file contains port numbers for well-known services as defined by
# RFC 1060 (Assigned Numbers).
#
# Format:
#
# <service name>  <port number>/<protocol>  [aliases...]   [#<comment>]
#
echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat             11/tcp
systat             11/tcp    users
daytime            13/tcp
daytime            13/udp
netstat            15/tcp
qotd               17/tcp    quote
qotd               17/udp    quote
chargen            19/tcp    ttytst source
chargen            19/udp    ttytst source
ftp-data           20/tcp
ftp                21/tcp
telnet             23/tcp
smtp               25/tcp    mail
time               37/tcp    timserver
time               37/udp    timserver
rlp                39/udp    resource      # resource location
name               42/tcp    nameserver
name               42/udp    nameserver
whois              43/tcp    nicname       # usually to sri-nic
domain             53/tcp    nameserver    # name-domain server
domain             53/udp    nameserver
nameserver         53/tcp    domain        # name-domain server
nameserver         53/udp    domain
mtp                57/tcp                  # deprecated
bootp              67/udp                  # boot program server
tftp               69/udp
rje                77/tcp    netrjs
finger             79/tcp
link               87/tcp    ttylink
supdup             95/tcp
hostnames         101/tcp    hostname      # usually from sri-nic
iso-tsap          102/tcp
dictionary        103/tcp    webster
x400              103/tcp                  # ISO Mail
x400-snd          104/tcp
```

```
csnet-ns          105/tcp
pop               109/tcp    postoffice
pop2              109/tcp                    # Post Office
pop3              110/tcp    postoffice
portmap           111/tcp
portmap           111/udp
sunrpc            111/tcp
sunrpc            111/udp
auth              113/tcp    authentication
sftp              115/tcp
path              117/tcp
uucp-path         117/tcp
nntp              119/tcp    usenet         # Network News Transfer
ntp               123/udp    ntpd ntp       # network time protocol (exp)
nbname            137/udp
nbdatagram        138/udp
nbsession         139/tcp
NeWS              144/tcp    news
sgmp              153/udp    sgmp
tcprepo           158/tcp    repository     # PCMAIL
snmp              161/udp    snmp
snmp-trap         162/udp    snmp
print-srv         170/tcp                   # network PostScript
vmnet             175/tcp
load              315/udp
vmnet0            400/tcp
sytek             500/udp
biff              512/udp    comsat
exec              512/tcp
login             513/tcp
who               513/udp    whod
shell             514/tcp    cmd            # no passwords used
syslog            514/udp
printer           515/tcp    spooler        # line printer spooler
talk              517/udp
ntalk             518/udp
efs               520/tcp                   # for LucasFilm
route             520/udp    router routed
timed             525/udp    timeserver
tempo             526/tcp    newdate
courier           530/tcp    rpc
conference        531/tcp    chat
rvd-control       531/udp    MIT disk
netnews           532/tcp    readnews
netwall           533/udp                   # -for emergency broadcasts
uucp              540/tcp    uucpd          # uucp daemon
klogin            543/tcp                   # Kerberos authenticated rlogin
kshell            544/tcp    cmd            # and remote shell
new-rwho          550/udp    new-who        # experimental
remotefs          556/tcp    rfs_server rfs# Brunhoff remote filesystem
rmonitor          560/udp    rmonitord      # experimental
monitor           561/udp                   # experimental
garcon            600/tcp
maitrd            601/tcp
busboy            602/tcp
acctmaster        700/udp
acctslave         701/udp
```

```
acct              702/udp
acctlogin         703/udp
acctprinter       704/udp
elcsd             704/udp                 # errlog
acctinfo          705/udp
acctslave2        706/udp
acctdisk          707/udp
kerberos          750/tcp    kdc          # Kerberos authentication--tcp
kerberos          750/udp    kdc          # Kerberos authentication--udp
kerberos_master   751/tcp                 # Kerberos authentication
kerberos_master   751/udp                 # Kerberos authentication
passwd_server     752/udp                 # Kerberos passwd server
userreg_server    753/udp                 # Kerberos userreg server
krb_prop          754/tcp                 # Kerberos slave propagation
erlogin           888/tcp                 # Login and environment passing
kpop             1109/tcp                 # Pop with Kerberos
phone            1167/udp
ingreslock       1524/tcp
maze             1666/udp
nfs              2049/udp                 # sun nfs
knetd            2053/tcp                 # Kerberos de-multiplexor
eklogin          2105/tcp                 # Kerberos encrypted rlogin
rmt              5555/tcp    rmtd
mtb              5556/tcp    mtbd         # mtb backup
man              9535/tcp                 # remote man server
w                9536/tcp
mantst           9537/tcp                 # remote man server, testing
bnews           10000/tcp
rscs0           10000/udp
queue           10001/tcp
rscs1           10001/udp
poker           10002/tcp
rscs2           10002/udp
gateway         10003/tcp
rscs3           10003/udp
remp            10004/tcp
rscs4           10004/udp
rscs5           10005/udp
rscs6           10006/udp
rscs7           10007/udp
rscs8           10008/udp
rscs9           10009/udp
rscsa           10010/udp
rscsb           10011/udp
qmaster         10012/tcp
qmaster         10012/udp
```

Related topics: sample hosts file, sample lmhosts file, sample protocol file, netscanner

Sample Protocol File

Depending on your windows version, the protocol file is located in different folders.
On windows 95 you can find it in the windows folder.
On windows NT you can find it in the winnt/system32/drivers/etc folder.
Because you can choose the name of your windows folder when you install windows, the name of the windows folder can be different on your computer. The folders above are the default values.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This file contains the Internet protocols as defined by RFC 1060
# (Assigned Numbers).
#
# Format:
#
# <protocol name>  <assigned number>  [aliases...]   [#<comment>]
ip       0     IP       # Internet protocol
icmp     1     ICMP     # Internet control message protocol
ggp      3     GGP      # Gateway-gateway protocol
tcp      6     TCP      # Transmission control protocol
egp      8     EGP      # Exterior gateway protocol
pup      12    PUP      # PARC universal packet protocol
udp      17    UDP      # User datagram protocol
hmp      20    HMP      # Host monitoring protocol
xns-idp  22    XNS-IDP  # Xerox NS IDP
rdp      27    RDP      # "reliable datagram" protocol
rvd      66    RVD      # MIT remote virtual disk
```

Related topics: sample hosts file, sample lmhosts file, sample services file, netscanner