McAfee VisualTrace

User Guide

Visual Trace Basics

Requirements

Your computer must meet all of the following requirements in order for you to be able to install and use Visual Trace:

- **A computer running a 32-bit version of Windows.** This includes all versions of Windows 95, 98, 98SE and 2000. It also includes Windows ME and NT 4.0. Windows 3.11 with Win32s *cannot* support Visual Trace. Windows 95 users need to have installed the Winsock 2 update. If you receive an error message when trying to run Visual Trace please search our online FAQ system for 'winsock 2'.
- **A non-proxy connection to the Internet.** This can be through a dial-up connection, cable or DSL connection or an office LAN. If your connection to the Internet is only through a proxy server, you will not be able to use Visual Trace. If you are behind a firewall and it is not configured to allow traceroute and ping, you will not be able to use Visual Trace. Firewalls can be reconfigured to allow Visual Trace to operate. Proxies can be replaced by or supplemented by a true NAT (network address translator). Talk to your network administrator for more information, direct them to this document and our online FAQ system.
- **Internet Explorer 4.01 or greater.** Visual Trace makes use of several updates to the Windows operating system. Some of these updates are available separately but the simplest way to ensure you have all the updates is to install IE 4.01 or greater. IE does not need to be your default or main browser; it simply needs to be installed.
- Visual Trace performs a great deal of data correlation in order to create the trace map as accurately as possible, in order to do this it must communicate with special application servers at McAfee.com headquarters. Any circumstance on your computer or local network, such as a firewall with too restrictive a configuration, may limit the ability of Visual Trace to perform all functions.

Note: If your only connection to the Internet is through a proxy server *you will not be able to use Visual Trace*.

What Is Visual Trace?

Visual Trace is a multi-purpose Internet tool used for finding information and trouble-shooting connection problems.

At the simplest level Visual Trace shows you how packets (data) get from your computer to another computer on the Internet. You see all the nodes (equipment of various types on the Internet that is passing traffic) between your computer and the trace target.

There are many situations where you need this information. Visual Trace is a useful tool when troubleshooting connections or just verifying that everything is working OK. There is also a wealth of information presented by Visual Trace, including the domain owners, relative locations, and in many cases geographical location of nodes.

Internet professionals, home users, law enforcement and many others use Visual Trace.
Besides using Visual Trace to look for weak spots in a connection, you can use it to:

- Discover if you can't reach a site due to a failure at your ISP or further into the Internet.
- Determine the point of a network failure that is preventing you from reaching a Web site.
- Determine the geographic location of sites and their users.
- Help track down the origin of unwanted e-mails ('spam').
- Monitor performance.
- Uncover the owners of a site.
- Determine the type and quality of connection a site has to the net.

- Get detailed contact information on sites all over the world (where available).

First Use

Set Home Location

The first time you run Visual Trace it will notice that you have not yet set your 'home' location.

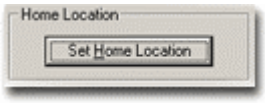

Figure 1

You set this value by choosing your country and then entering your home city or postal code. Setting your home location is not vital, and you may cancel this dialog and continue without setting it. You can set it or change it at any time through the Options dialog. More detailed information on setting your home location and the implications of it are explained elsewhere in the documentation.

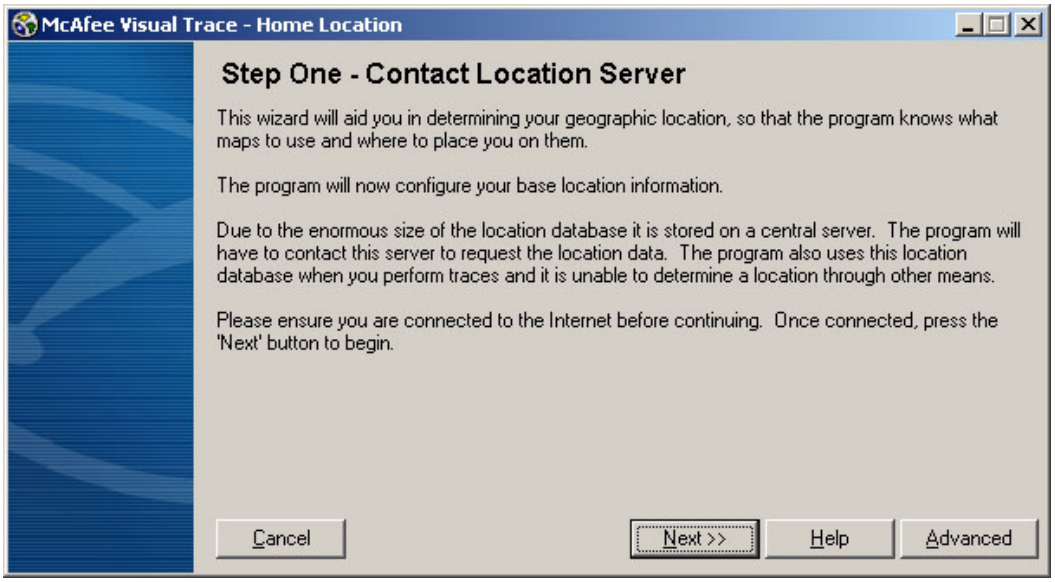

Figure 2

Orientation

When you first start Visual Trace it will display a welcome screen. From this screen, you can choose a variety of options for information related to Visual Trace. Advanced users will want to configure Visual Trace to update this page periodically as explained elsewhere in the documentation.

The Target bar is where the trace-to target is entered. Pressing the arrow on the drop-down control will show a list of past targets. When the program is first run the target list is filled with four test sites at random. The target bar always shows the last site traced when the program is first started. On the very first run, this site will be artificially from the random list. The trace history can be cleared from the options dialog.

To start a trace you can either:

- Type in an address or host name and press enter.
- Press the 'GO' button
- Drag a URL from another program onto the toolbar or target bar and drop it, then press 'GO'
- Use the trace button in the IE browser toolbar, or the right-click menu on a link in the browser.

When a trace is in progress, you can stop it by pressing the stop button or the ESC key.

If you enter an invalid target, you will get an error message. If you are not connected to the Internet when you start a trace then any target will be invalid and unreachable.

During the trace, a progress bar at the bottom of the window indicates the overall progress. An animated logo at the top right of the window indicates the program is busy or waiting for responses from remote servers. Sounds are played for different events during the trace, including requests being made and results returning from remote information servers and targets. A tone is sounded at the completion of the trace. If continuous pinging is turned on, a sound is played at the completion of each pass. Sounds can be turned on or off through the options dialog.

As the trace progresses, details are filled into the list view, info pane and map as they become available.
The main view shows the trace result as either a map or a list/graph. Initially docked at the right is the info pane. This sub-window can be 'floated' off the main window or left 'docked'.

Step By Step - Feature Tour

In this section, we will take you through all the major features of Visual Trace. Do not worry if you don't understand everything you see here at first. Some features will take time to understand, and depending upon your level of knowledge of the Internet, you may be unfamiliar with some of the concepts discussed here.

Visual Trace pulls in data from many different sources in order to show you the most complete information possible about the trace and the servers and networks on that trace. This requires a great deal of interaction between Visual Trace and various servers on the Web. McAfee.com operates some of these servers, and some of these servers are operated by public or quasi-public entities. Server availability is not perfect, and it will vary with network conditions, your connection status, and planned or unplanned server outages.

The heart of Visual Trace is a trace performed with ICMP packets. It is technically impossible for ICMP packets to travel through a proxy server. You must have either a direct connection to the Internet, or a true NAT connection to use Visual Trace.

The Startup Screen

When Visual Trace starts, it will show you a 'splash' screen. This screen is a quick link to useful information related to Visual Trace, including software and data updates. In normal operation, this screen is loaded dynamically with fresh content from a McAfee.com server. This allows us to notify you of updates and news that may affect your use of Visual Trace.

Figure 3

Note: If you have a slow Internet connection, or are very distant from the McAfee.com server, you can turn off the dynamic loading of this screen by un-checking the 'Load Visual Trace Today' item on the General tab of the Options Dialog.

You can return to this dynamic screen any time, or load it if you have it turned off, by clicking on the logo in the top right corner of the screen.

The Target

The primary purpose of Visual Trace is to run trace routes to other computers connected to the Internet. You can type targets into the Target field in the Visual Trace toolbar. You can also drag and drop links from browsers onto the Target field. When you drop a link onto Visual Trace, the link will be checked for a valid target and if one is found it will be placed into the Target field.

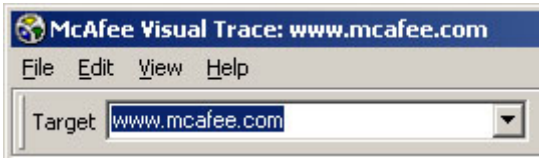

Figure 4

The Target field is also a drop-down list containing a history of previous targets. If you wish to clear this history list, you can do so in the Options Dialog using the 'Clear Trace History' button.
Once your selected target is ready in the Target field press 'Go'. You can also start a trace by pressing F5 or Ctrl+T. If you enter an IP address, the trace will begin immediately. If you enter a computer name, this name must be looked up through the DNS system and the corresponding IP address determined. This lookup process is normally very quick but in some cases may take several seconds or longer in the case of poor DNS response time. Visual Trace indicates that it is busy by spinning the logo in the top right of the window.
If the target cannot be resolved to an IP address, an error is displayed. There are several reasons why a target cannot be resolved to an IP address.

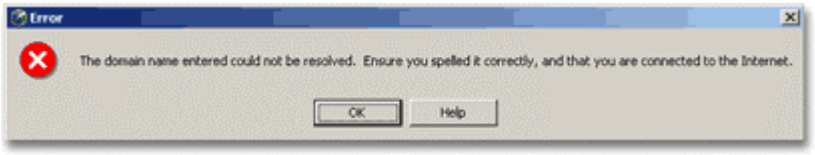

Figure 5

These include:
Unresponsive DNS server, either locally or responsible for the target domain
No active connection to the Internet, DNS server is therefore unreachable for query
Target name is not in use or invalid in some other way
Once the target has been resolved, the trace begins.

The Trace

Because Visual Trace makes an immediate attempt to place information for the target it may display information that is later revised to a different result. The most obvious behavior is an end location that changes positions on the map. The initially indicated position may be a guess based on partial results. This end location could change either if the true location is determined to be different, or if the location cannot be determined accurately enough to display as a result. Visual Trace is conservative in how it places locations on the map and will generally not use a guess as a result.

The complete trace and results involve dozens, sometimes several hundred individual queries. As information comes back, it is displayed within the program. Some individual items may take a long time to return and can hold up the overall trace result for some minutes. The response time of public server information is beyond your control and the control of McAfee.com. Response time will vary with time of day, server condition, and your distance from the server in question.

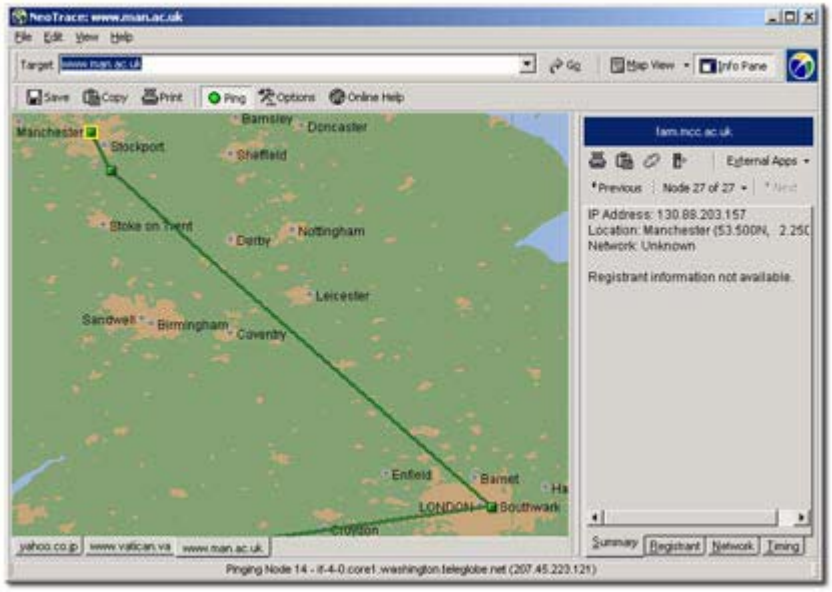

Figure 6

The actual trace consists of sending out a series of ICMP packets directed at the target. These packets are deliberately limited in how 'far' they can travel across the Internet. This limited life span causes the packets to expire prematurely and to be returned to Visual Trace before reaching the target. Visual Trace then examines these packets and assembles the route that a good packet would travel to the target.

At this point Visual Trace has a list of IP addresses that indicate the nodes from which the packets were returned when they expired, and the total round-trip time of each packet. From there, it begins making queries to determine the names of these nodes, their locations, and the registrants for the domain and network of each node.

While the queries are in progress the login in the top right corner of the window will spin, and a progress bar will be displayed at the bottom of the window. Even while results are still being collected, you can begin viewing them. When the results collection is complete the animation will stop and a completion sound will play.

The Results

The major details of the trace results are shown in the main displays. The list view shows you the IP addresses, names and response times. The map displays any geographical information that was found. Details specific to each node are also shown in the Info Pane at the right side of the window.

If all of your traces consist of only two nodes, this indicates a problem. Most likely, you are behind an overly restrictive firewall that is failing to allow the ICMP packets back to you. For more information see firewall related FAQ topics in the online documentation.

Note: Many users are confused about ping time. The ping time shown for each node is the round-trip time to that node. The times are ***not*** cumulative and it is not at all unusual to see higher times in the middle of the trace than the response time from the target. High times in the middle of the trace, or even unresponsive nodes, are not by themselves indication of a problem.

The Toolbar

Across the top of the window is the toolbar. It contains the Target entry as well as other functions that Visual Trace can perform on the entire trace. The Map View and List View buttons toggle the main view area between these modes. The Info Pane button toggles the display of this panel on and off.

Figure 7

When trace results are being displayed the Save, Copy and Print buttons become active. Results can be saved into any one of several text and image formats. When you press the Save button you will get a Save As… dialog that will allow you to choose your format.

The Copy button will bring up a choice of text or bitmap formats. The text or bitmap version of the trace will be placed in the clipboard. From there, it can be pasted into a document or e-mail.
The Print button does not directly print the trace results. It displays the results in your default Web browser for preview. From there, you can use the browser features to print.

The Ping button toggles continuous ping. This is a re-trace that occurs after the initial trace is completed. This is used to obtain a clearer timing sample or to monitor response times over a long period. More detail on this feature is available elsewhere in this documentation.

The List View

This view has the highest concentration of information. It shows all the nodes along the trace path as well as their names, IP addresses, timing details and more. The list also includes a graph column that indicates timing results.

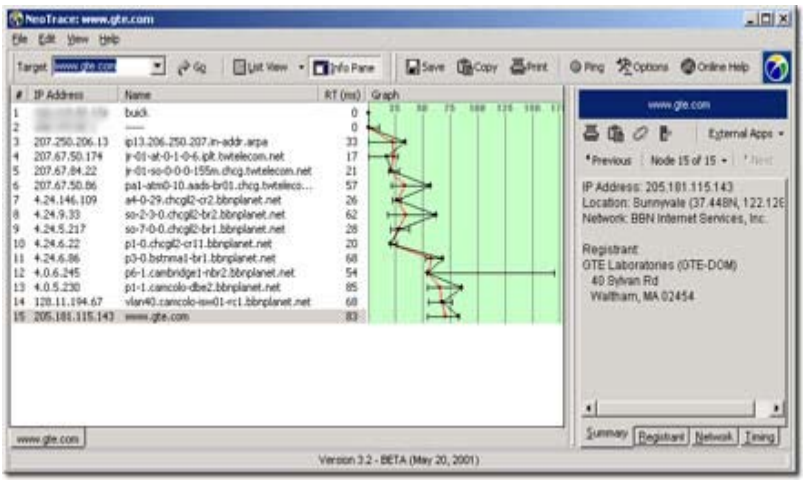

Figure 8

You can alter what items are shown in the List view through the Options dialog. Here you can choose what columns to display. These settings will be remembered between sessions.

Detailed information on the Graph portion of the display is elsewhere in this documentation.

The Node View

The Node view is an abstract representation of the trace path. This view is most meaningful while the trace is in progress and when you want to see the logical relationship between nodes.

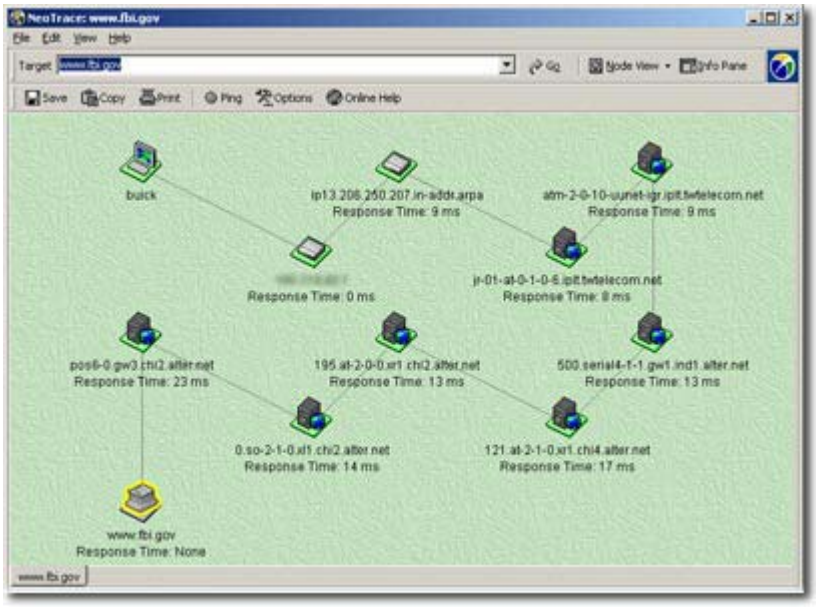

Figure 9

This is the clearest representation of the trace path itself.

The Map

The map display shows the approximate geographical route of the trace. Only nodes that have reliable location information available are placed on the map. All others are shown as unspecified points between the others, or are displayed on top of the last node with location information.

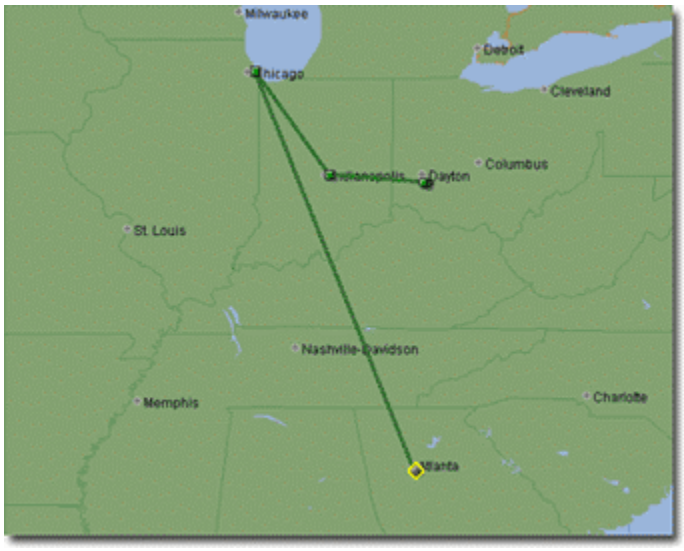

Figure 10

The accuracy of node placement on the map ranges from several hundred miles to less than one mile. Typically, a node is located by city, and the placement on the map indicates the city that the node is known to be near, but not the precise location of the node. In general the *most* accurate the placement can be is within one kilometer.

The detail of the map itself will vary depending on your level of zoom and where you are looking. Some areas of the world have good detail sub-maps that ship with the program. Additional maps may be made available from time to time through the Visual Trace Today update pages.

Figure 11

City labels are placed on the map as reference points. They do not necessarily label the precise cities or towns that the trace is passing through, but priority will be given to labeling cities near to the trace. Second priority in which cities to label is based on the population size of the city. Cities that are national capitols are labeled in all capital letters.

While the trace is in progress, the map display will automatically be zoomed to fit the current results. Once the trace is complete, you can scroll and zoom the map as you like. Scroll the map by clicking on it and dragging it. To zoom the map in and out you can click the left and right mouse buttons (without dragging), use the up and down arrows on the keyboard, or use the scroll wheel on a mouse equipped with one.

The Info Pane

At the right side of the window is the Info Pane. This panel displays information specific to each node of the trace. You choose which node to display information for by selecting it. The currently selected node is highlighted in the Map View with a yellow outline. In the List View, it is the row with a shaded background. You can click a node to select it.

Nodes can be 'navigated' with the keyboard as well. Pressing the PgUp and PgDn keys will cause the selected node to increment or decrement. You can move the selection to the beginning or end of the trace with the Home and End keys. If your mouse or keyboard has forward and back buttons for navigating Web pages, you can use these as well to navigate the nodes.

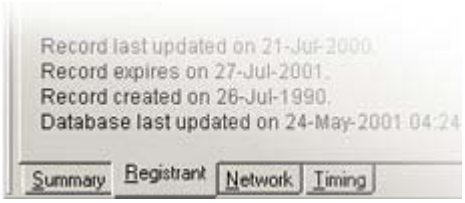

Figure 12

At the bottom of the Info Pane are several tabs. These tabs select the specific information you would like to view about the selected node. The text area in the Info Pane can be highlighted and text copied to the clipboard. Use Ctrl+C or Ctrl+Insert to copy text to the clipboard. The entire contents of the Info Pane can be copied to the clipboard using the copy button in the Info Pane.

The Info Pane can be kept 'docked' at the right edge of the window or it can be floated off as a separate window. To float the window, press the dock button in the Info Pane.

To re-dock the window, press the button again.

An individual node can be 'refreshed' with button in the Info Pane. A refresh consists of pinging the node again and performing all queries related to the node again.

Figure 13

Ping Updates

After a trace is complete, there is an option to continue pinging the nodes of the trace. This is toggled using the Ping button on the toolbar.

Performing several passes of the trace is always important if you are specifically looking at route performance. The initial pass timing results may be significantly different from average results, and average results are much more important than the worst and best case.

Specific settings for the ping looping can be set in the Options dialog.

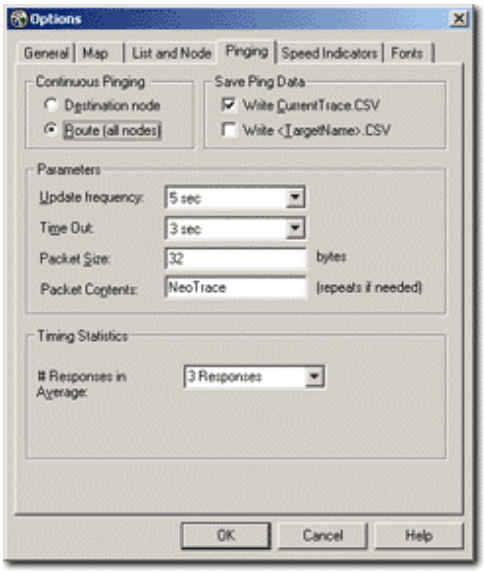

Figure 14

The Details

Keyboard Shortcuts

Nearly all features of Visual Trace allow use of the keyboard for access.

General Shortcuts

F5	Start Trace
Esc	Stop Trace
Ctrl + Enter	Complete address with www. - .com and start trace
Ctrl + D	Delete current trace
Ctrl + G	Go Online (Open Visual Trace Home Page)
Ctrl + N	Toggle Ping
Ctrl + O	View Option Dialog
Ctrl + P	Print
Ctrl + S	Save
Ctrl + T	Start/Stop Trace
Alt + L	Change to List/Graph View
Alt + M	Change to Map View
Alt + Left	View Previous Trace Tab
Alt + Right	View Next Trace Tab
Alt + 1	View Trace Tab 1
Alt + 2	View Trace Tab 2
Alt + 3	View Trace Tab 3
Alt + 4	View Trace Tab 4
Alt + 5	View Trace Tab 5

Node Navigation

To move through the trace nodes use the following keys:

Home	Move to first (local) node of trace
End	Move to last (target) node of trace
PgUp	Move forward one node
PgDn	Move back one node

Changing the selected node in this manner will cause the Info Pane to show the results for that node. If 'auto-center to selected node' is turned on in the Map Options, the map will center itself on each node

Map Mode
Up and Down Arrows Zoom map

The Back and Next buttons on 'Internet' keyboards can navigate the nodes in the same manner as using PgUp and PgDn.

Mouse Shortcuts

In the map, users with a scroll wheel mouse can zoom the map in and out using it. If your mouse has next and back buttons for Web navigation, you can use these to navigate the nodes of the trace.

Reading the Graph

The graph is an important tool in trace analysis. It helps you to spot potential areas of trouble, changes in network conditions, international links, modem-connected nodes, and more.

Whenever you consider the ping times and graph to be an important factor be certain to run the ping loop for at least 10 iterations. This will ensure you have a good solid average time. It may also be important to minimize any other network traffic while performing the trace and the ping loops; simultaneous traffic can block free passage of the packets and cause artificially high response times.

Spikes
It is very common to see a single node in the midst of a trace that has a very high response time. It would be easy to jump to the conclusion that this node is responsible for poor traffic performance, but it would be completely wrong.

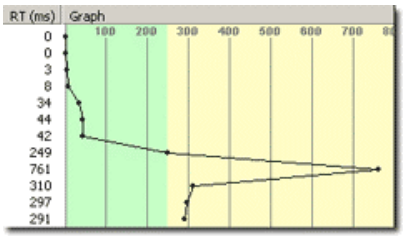

Figure 15

Remember that ping times in Visual Trace are not cumulative. If node 8 has a ping time of 400 ms (milliseconds) and node 10 has a ping time of 200 ms, then packets are going all the way from your computer to node 10 and back again in only 200 ms.

This may seem counterintuitive at first. How could it possibly be coming back faster from a node that is farther away? Especially since it had to go through that slow node to get there and back. The answer has to do with how the Internet works, so allow a brief lesson in routing.

All traffic on the Internet consists of packets. A packet is a small piece of data, anywhere from a few bytes to a couple thousand bytes. The packet has an address on it that tells nodes handling the packet where it is going. Your computer sends the packet out to the LAN or modem. The packet is handed to the next node in line, which routes it according to a routing table. The routing table tells it which other node to hand a packet to based on what the destination address is. This is similar to how real packages travel through the postal system, being handed off from one section of the postal system to another.

At each node, the packet is inspected and passed along. Nodes in the middle of a trace are by definition routers, their most important job is to take packets, inspect them, and pass them along. This gets priority over all other things, including responding to requests. Requests include pinging. Therefore, in our example when a packet bound for node 10 hits node 8, it handles it as efficiently as possible by passing it on. However, when it receives a packet asking it to respond back it pushes it off as being a lower priority.

In some extreme cases, routers are instructed to ignore ping requests completely. This can result in an unresponsive node right in the middle of an otherwise normal trace.

Trends
We know spikes don't tell us much about traffic, but what about trends? In general, ping times should get higher as the trace gets farther from your computer. This is only logical; more nodes have had to handle the packet.

On homogenous network segments, the trends will be very steady. Similar equipment connected through similar network segments will tend to introduce the same amount of additional delay at each hop. Once you know this, it is easy to spot changes between networks and hardware types.

Two changes in segment types are obvious: modems and international. International connections are typically undersea cables, but there are some limited uses of satellite as well. If you are a modem user, your own modem is right at the start of every trace. You can see the ping time go from 0 up to several hundred milliseconds on the very first hop. This delay, or latency, is unavoidable in acoustic modems.

The time involved in converting the signal, and other overhead involved in the hardware mean that there is always that amount of latency in your connection.

When a target node is also connected through a modem, another similar jump will be visible at that end of the graph.

International connections can be obvious, especially when crossing the Atlantic or Pacific. These jumps in total response time are not nearly as great today as they were just two years ago, but they are still frequently obvious.

High Local Response Time

In general, the trend will always be higher ping times farther away. In a few circumstances, they will be higher on the two or three nodes closest to you for brief periods. This indicates heavy local traffic at your ISP, or more likely traffic to your computer. Compare a trace done with no other network activity to one performed while you are downloading a large file.

Recognize Typical Patterns

If you use Visual Trace to monitor response times at sites important to you be sure you establish a 'baseline' trace. At a time when responses from the remote site are clearly normal, and there is minimal local traffic, run a trace with at least ten ping loops afterward. Save or print a copy of these results for future reference when comparing ping times.

External Application Use

External Application Configuration files allow Visual Trace to start another program, while optionally passing to it information gathered from the trace or from a particular node on the trace.

External application configuration files must be located in the ExternalApps directory, located in the Visual Trace installation directory, and must have the extension ".config". The file consists of five lines with each line as follows:

1. Menu name
2. Description
3. Command Path
4. Command Name
5. Command Parameters

The first line the Menu name is the name that the external application will have in the external application submenu.

The second line is a description of the configuration file. This line is ignored and can be treated as comment line.

The third line contains the command path and is the absolute path of the command. If nothing is present then the PATH environment variable will be used to try to find the executable.

The fourth line contains the name of the executable.

The fifth line contains the parameters passed to the executable, i.e., command line arguments.

Variables

The command name and command parameters can contain variables. The list of allowable variables is

%X	Hostname, if available, else the IP address
%H	Hostname
%I	IP address
%D	Domain Name
%N	Netname
%T	Round Trip Time
%A	Latitude
%G	Longitude

Variables present on the first three lines in the configuration file will not be interpreted as variables. In addition, the letter corresponding to a variable can be either upper- or lower-case, i.e., %X == %x.

As an example, the configuration file for ftp is (the line numbers are added for clarity):

```
1: Ftp
2: # Description
3:
4: ftp
5: %X
```

Command Line Options

The ability to run Visual Trace from the command line has been expanded in version 3.0. The new options available at the command line greatly extend the capabilities of Visual Trace. The following are the possible options:

Visual Trace [target] -p -t -x -o [filename] -min –max

[target]	The target destination.
-p	Specifies the number of ping loops to undertake. < positive a be should>
-t	Specifies the time delay between loops, in milliseconds. Should be a non-negative value.
-x	Have Visual Trace exit after all ping loops are completed.
-o [filename]	The name of the file to save the data in.
-min	Run Visual Trace minimized.
-max	Run Visual Trace maximized.

The option flags are case insensitive and the order they are listed on the command line is irrelevant.

The number of ping loops specified on the command line should be a positive integer. If a negative integer, a zero, or no number is specified then the default value is used. The default value is one.

The time delay should be expressed as a non-negative value. If a negative value or no value is specified then the default value is used. The default value for the time delay is the time delay stored in the options dialog.

If a file is specified on the command line, this file will be saved in the Results directory. The type of file that is saved is dependent on the filename extension. The recognized extensions are "txt" which saves the trace results in a text format; "png", "bmp", and "jpg" which saves only the Map display; and, "rtf", "mht", and "htm" or "html" for saving the trace results with an embedded copy of the Map. If the extension is not one of these, it defaults to saving the trace results in a text format. Note that the argument immediately following the -o flag is taken as the filename. If no filename is specified and the -o flag is the last item in the argument list then no output of the trace results is undertaken, i.e., there is no default filename used. Likewise, if an option flag immediately follows -o, again without a filename given then there is no outputting of the trace results. Note that all this is independent of the ping results being written to the csv files. See the section on CSV Format.

To have unattended pinging enacted, a target must be specified. In addition, the -p option must be included on the command line. If only the target is specified on the command line or if other option flags are given but -p is not one of them, then the program starts and performs a single trace to the target. The other option flags are ignored. If no target is specified on the command line then the program starts and waits for user input, again, the other options are ignored.

The -min option takes precedence over the -max option, if for some strange reason both are specified. Either of these flags can be specified independent of whether unattended pinging is enabled.

The ordering of the options doesn't matter.

Some examples will help clarify the use of the command line options.

Examples:

1. **Visual Trace www.McAfee.com**
   Visual Trace is started and a trace is initiated to www.McAfee.com. The state of the program after the initial trace is dependent on the options the user has saved in the options dialog.

2. **Visual Trace –min**
   Visual Trace is started minimized. A trace is obviously not started since a target is not specified. If the target is absent, and other options are specified on the command line, they are ignored. Recall also, the -min flag has precedence over the -max flag. Also note, that when Visual Trace is started in minimized mode all sounds are turned off. They can be turned back on using the options dialog.

3. **Visual Trace www.McAfee.com.com -p 10 -t 3000 -min -x -o McAfee.com.log**
   Ten ping loops to www.McAfee.com.com is undertaken with a time delay of three seconds. The window is minimized, the trace results are written in text format to the file McAfee.com.log and after the ten loops are completed, Visual Trace is exited.

4. **Visual Trace www.McAfee.com.com -p –max**
   A single ping loop is done to www.McAfee.com.com in a maximized window. Visual Trace is not exited when completed.

5. **Visual Trace**
   Visual Trace is started in normal mode.

6. **Visual Trace -x -o McAfee.com.htm -t 10000 www.McAfee.com.com**
   A trace is performed to www.McAfee.com.com using the default ping time delay as defined in the options dialog. All the options on the command line are ignored except the target since the -p option was not specified. There is no html output file created nor does the program terminate upon completion. This command is, in effect, identical to 1).

7. **Visual Trace -x -o McAfee.com.htm -t 10000 www.McAfee.com.com -p 4**
   A trace is performed to www.McAfee.com. Four ping loops are done with a time delay of ten seconds. The trace results are written in html format to the file McAfee.com.htm in the Results directory and the program is terminated when this is completed.

8. **Visual Trace -P 2 -T 3500 -mAX www.McAfee.com.com**
   A trace is initiated to www.McAfee.com.com performing two loops with a delay of 3.5 seconds and the window is maximized. This is just to show that the options are case insensitive.

9. **Visual Trace -p 2 -t 3500 -o www.McAfee.com.com**
   Start up Visual Trace and no trace is initiated. This is because the target is specified immediately following the output flag so the program takes the target as being the output filename. Therefore, no target is specified and all the options are ignored.

10. **Visual Trace -p 2 -t 3500 www.McAfee.com.com -o**
    A trace is initiated to www.McAfee.com.com using the number of ping loops and time delay as given in the arguments, however, there is no outputting of the trace results to a command-line-specified file.

11. **Visual Trace -p 2 -t 3500 www.McAfee.com.com -o –x**
    Same as above except the program is terminated after completion.

CSV Format

Visual Trace can store trace results to CSV files (Comma Separated Value). CSV files are easy to parse if you want to write custom programs to manipulate trace results. By combining this feature with the ability to run Visual Trace from a command line, you can combine Visual Trace with your own custom scripting or application to create specialized solutions.

If you have Excel installed on your computer it will already have CSV files associated with it.

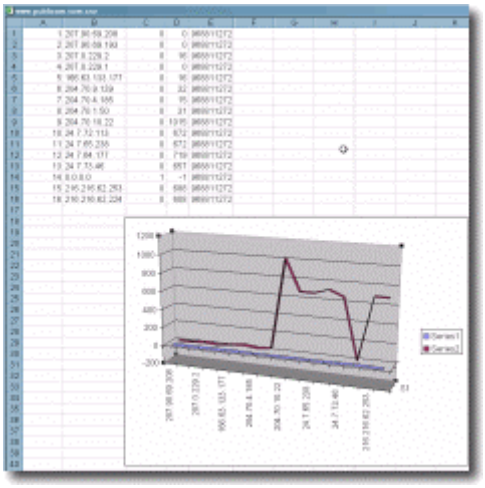

Figure 16

The Files

Every time a trace is initiated, a file called CurrentTrace.csv is created. Optional files that are named for the trace target can also be created.

The CurrentTrace.csv file is overwritten with new results each time a new trace is started. The optional target-specific files are never overwritten. Instead, they are continually appended to with new results. Tools making use of the CSV files can choose which results from the file to consider by looking at the time/date stamp.

The target-specific CSV file will be named for the destination node name, such as Visual Trace.com.csv, or if the host name cannot be resolved, it will use the IP address such as 207.90.69.201.csv. If the target is unreachable, the target name that was given will be used.

The CSV files are stored in the Results folder.

File Format

Each line of the file contains the result for one ping pass of one node. Within each line are five values, separated by commas. These values are:

1. Node Number
2. IP Address
3. Error Code
4. Round-Trip (Ping) Time
5. Time/Date Stamp

The error code is 0 for normal operation, 1 for unreachable (non-responsive) nodes, 2 for other errors on the node. Lines with a non-zero error code will have the value -1 entered in the Round-Trip Time column.

Round-Trip Time is in milliseconds.

The Time/Date Stamp is given as the number of seconds since Jan 1 1970. This is a standard time format, which is easily converted to the natural date/time.

Performance

Due to the progressive growth of cached data, you will find that the time required for gathering all trace data decreases as you execute more traces.

The tracing in Visual Trace is extremely fast due to parallel processing of requests. However, if it is busy doing other things at the same time this will slow down the display. Updating the map display takes longer than refreshing the list view; so for the fastest display of results (especially on older machines) perform traces in list view.

The trace results themselves are not affected by what mode you view while the trace is progressing, just the speed with which the results are shown.

The difference in the results display mainly affects users on low-latency connections; on high-latency connections such as a modem, there is more time between results returning to the program so there is more time available to update the display.

Submitting Location Information

Please read this entire topic before attempting to use the location submission feature.

There are nearly a dozen ways that Visual Trace gets information on where nodes are located. The quality of this information ranges from extremely precise (within a few feet) to very vague (in the right country only).

There is no substitute for the quality of directly observed information. If you have direct knowledge of the location of any number of computers, you can help contribute to the overall quality of the information available. Thanks to changes made to Visual Trace Pro, which allow new information to be rapidly approved and introduced back into the location server system, it is possible for new contributions to be integrated very quickly.

Even if you do not have specific information, you can still contribute simply through your own knowledge of where you are.

If you have direct knowledge of the location of a computer or group of computers, we encourage you to submit this data. First, determine if we already have location information for this computer by tracing it. If the node location is shown as unknown or if the information that is given is not entirely accurate, then you should submit new data.

To submit data for a single computer simply fill in as much information as you know.

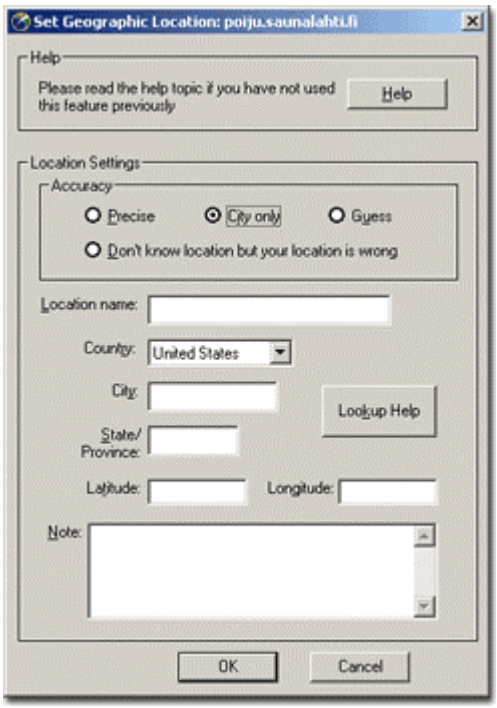

Figure 17

Information on groups of computers is much more effective. This further information should be included in the Note field of the dialog. Useful information falls into two categories: ranges of IP addresses, and patterns of machine names.

For example, if your network contains IP addresses between 207.90.69.192 and 207.90.69.222 and they are all located in the same place you should include that information in the note. If you can give an approximate or exact address, we can use this in determining the latitude and longitude if you do not have another means of determining it. This is the most commonly available type of information to individuals.

If you are a network administrator, or you work for an ISP, NOC or other network infrastructure related position, please contact us for information on how you can submit block data to us conveniently.
If the information you are submitting is for a **specific location**, for example an office building or a school campus, please include this information as part of the note and as the name for the location.

If you are entering exact Latitude and Longitude, you must enter them as **signed decimal** values. Information entered into this dialog is not stored locally unless you enter *precise* information. When precise information is entered, it will be stored in the location file locally in addition to being submitted to the central database. For more information on the local file and creating location data for it, see the topic Creating Private Location Data.

Creating Private Location Data

In addition to submitting data to the master database, you can create LOC data for your own private use. This is very useful for private network space and networks which are not attached to the Internet at all but use TCP/IP. Private LOC data is stored in the file NeoLoc.ini.

You can edit the file with any text editor. Be sure you use a simple text editor that will save in plain ASCII format, such as notepad.

The NeoLoc.ini file consists of single-line entries with a pattern, a latitude/longitude value, and a confidence value. The first line of the file indicates the total number of entries in the file. Be sure to increment this value if you edit the file by hand.

Example:

```
Count=2
www.McAfee.com.com=-39.55,84.22,200
*.McAfee.com.com=-35.28,82.43,200
```

The confidence is an integer value in the range [0-255]. The higher the value the "more confident" you are of the location data being entered. For reference, if you enter private location information via the edit node location dialog the value 200 is used.

Entries can contain a simple machine name or have * wildcards at the beginning or in the middle. The precision (number of decimal places) of the lat/lon values can be as high or low as you like.

In addition to the basics, this example demonstrates another principle of this file. Visual Trace will search through this file from top to bottom and return as soon as it finds a match, so items should be listed from the specific to the general. In this example, most machines in the McAfee.com.com domain are located in the location indicated by the wildcard, but the Web server is located in a different place.

Configuration

The Options Dialog allows you to set a variety of behaviors within Visual Trace. To view the options simply press the Options button on the toolbar or press Ctrl + O.

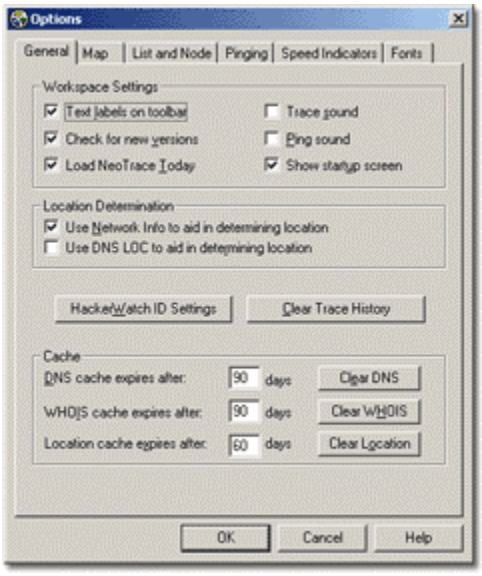

Figure 18

General

The 'Clear Trace History' button will delete the history list that appears in the drop-down list attached to the Target entry on the toolbar.

If 'Load Visual Trace Today' is checked, the initial screen shown when Visual Trace loads will be taken from a remote server. Using this remote page allows you to be sure to see any dynamic changes that may be made to the page. If you experience performance problems due to slow load time of this page, you may want to turn it off. You can view the dynamic page at any time by clicking on the logo in the top right corner of the window.

If 'Check for new versions' is checked Visual Trace will periodically (approximately once a month) query a remote server to see if there are any updates available for Visual Trace. Updates include new data files, maps and updates to the program itself. The update check is made when Visual Trace started.

In the Location Determination section of the dialog, you can turn on use of Network and DNS LOC information. If the Network information is used it applies only to the target node and will only be used if all other methods of determining the location fail. The Network information used will be the country, city and postal code that appear in the Network information for that node.

DNS LOC is a specialized type of DNS entry that contains information about the location of a node. Very few nodes have this information available and this combined with the performance cost of using it result in it being a feature not used by default. If you are certain you will get better results by using DNS LOC then you should enable it. If you are not familiar with it, we recommend you leave it disabled.

If you use Visual Trace to trace hits you receive on your firewall, you may want to turn on HackerWatch support. This enables you to report specific event information to HackerWatch.org for analysis and possible further action. To sign up for HackerWatch press the 'Sign Up For HackerWatch' button. Visit www.hackerwatch.org for more information.

Visual Trace caches a lot of information that it receives from the many queries it makes on each trace. Having this information cached locally improves the performance time and reduces the number of queries made by Visual Trace. The trade off is that information does go out of date. The default expiration times for the local caches are reasonable, but you may wish to adjust them to suit your particular usage of Visual Trace. Most users will not want to change these values.

Map

The map display properties can be adjusted to suit your personal taste and computer performance. Turning off detailed items may improve the draw speed of the map on older computers.

The color scheme used to display the map can be altered. Visual Trace ships with several color schemes from which you may choose. If you are interested in creating a custom color scheme of your own, search the McAfee.com knowledge base for information on obtaining a utility that will allow you to create new schema.

By default, Visual Trace will zoom the map in and re-size it to fit the trace in progress. You may choose to turn off these behaviors with the 'Zoom Settings' options.

The 'Save Image Format' determines the file format used for the map portion of trace results saved at HTML.

By default, Visual Trace will display the map while you scroll it. If you do not like this feature or if it does not perform well on your computer, you may turn it off by clearing the check box next to the 'Active Drag Map' item.

To change your 'Home Location,' click the button to display the wizard.

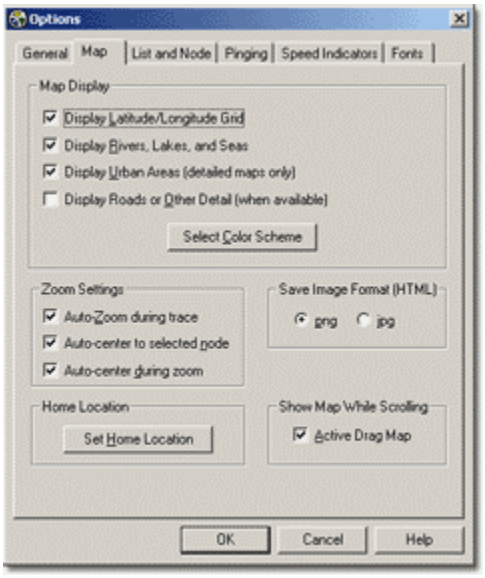

Figure 19

List Settings

The List Display settings allow you to choose which items to display as columns in the List View. Note that it is quite possible to have much more data than can easily fit on screen.

The order of columns displayed cannot be changed in this release of Visual Trace.

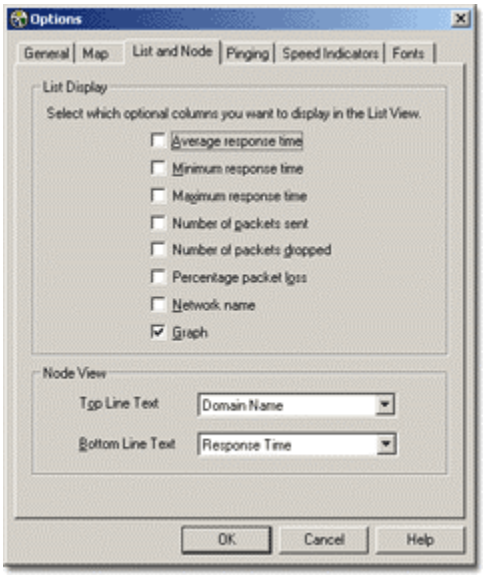

Figure 20

Pinging

For most purposes, the default settings are fine. If you have specific testing you need to perform, you may want to alter these settings.

By default, Visual Trace writes out the results of each ping to each node to a CSV file. There are two files involved, a CurrentTrace.CSV file that is re-created for each individual trace, and a file named for the target that is always appended to. Visual Trace never deletes the named file.

In addition to the frequency with which pings are performed, you can alter the specifications of the ping packet itself. You should normally leave the packet contents equal to 'Visual Trace' unless you have a specific reason to alter it.

Speed Indicators

Colors are used to divide sections of the graph and on the trace nodes displayed in the Map View. The color is determined by the ping time to that node, taken from a range determined in this section of the Options Dialog.

You may choose a default range of times by pressing the Default Fast or Default Slow buttons (low latency and high latency). If you are using a modem you should use the slow settings, most other users should use the fast settings. This has no effect on anything other than the colors used in the graph and on the map nodes.

Once you are familiar with the characteristics of your connection you may want to set your own custom color bands.

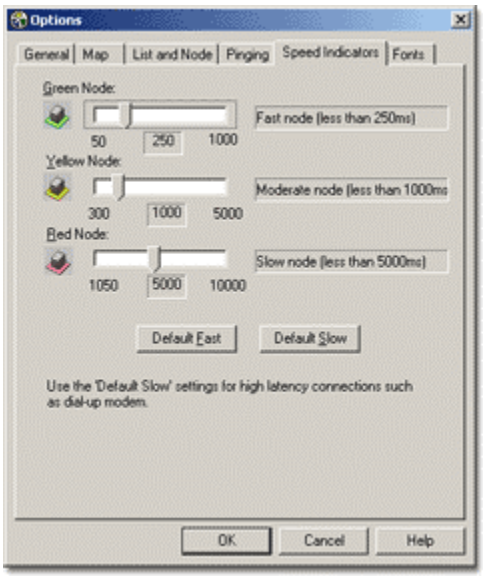

Figure 21

Glossary

BPS
(Bits-Per-Second) The speed at which data is transmitted in bits-per-second. A 28.8 modem can move 28,800 bits per second.

Browser
A program that is used to look at various kinds of Internet resources.

Cookie
A Cookie most commonly refers to a piece of information sent by a Web Server to a user's Web Browser. The Browser software sends it back to the Server whenever the browser makes additional requests from the Server. When you visit a previously visited site, and you are welcomed by name, thank (or blame) a cookie that told them who you are.

When a Web Server attempts to send a cookie to your computer, you may get an Intruder warning from Hack Tracer.

Country Codes
In the course of tracing intrusion attempts you will eventually encounter a country code. The country code is a two-letter tag at the end of a site URL that identifies the country where the site is located. See the on-line help for a detailed list of country codes.

Domain Name System/Server (DNS)
The Domain Name System simplifies Internet navigation. Computers on the Internet can only be found at their numerical IP address (e.g., 206.216.115.4). An address like "McAfee.com" makes sense to a human but a DNS server must match it up to its real IP address. The DNS server databases are updated regularly as new domain names are registered.

Domain Name
An Internet site's unique name that consists of two or more parts separated by dots. Example: McAfee.com, whitehouse.gov, www.chubu.ac.jp.

DSL
DSL or Digital Subscriber Line is an increasingly popular method of connecting to the Internet over regular phone lines. DSL offers the advantage of a relatively high-speed connection at prices substantially lower than ISDN connections. In theory, DSN has a download speed limit of 9 megabits per second and an upload limit of 640 kilobits per second. In reality, and dependent of your provider's equipment as well as your system equipment, you can expect anything from about 1.5 megabit download/128 kilobit upload (Asymmetric DSL) to 384 kilobits in both directions (Symmetric DSL).

E-mail
Electronic Mail, messages sent via the Internet or within a company LAN or WAN. E-mail attachments in the form of EXE (executable) files or VBS (Visual Basic script) files have become increasingly popular as a means of transmitting viruses and Trojans.

Finger
Software that allows you find out more information about an Internet user such as their real name and if they are logged on to a network or the Internet.

Firewall
Hardware and/or software designed to keep unauthorized outsiders from tampering with a computer system. That system may be a standalone computer, a small LAN or a company-wide network or WAN with thousands of users. Hack Tracer is a software firewall effective in protecting standalone computers and small networks.

FTP
FTP or File Transfer Protocol is used to move files between Internet sites. When you "download" a file from a site, e.g. a virus program update, you are using FTP. Public FTP sites from which you can download program or driver updates are usually anonymous FTP servers that permit anonymous logins.

Private FTP sites normally require a Login name as well as a password and those who use them regularly, usually make use of specialized FTP programs.

Hit
A "hit" is a single request from a Web browser for a single item from a Web server. A single Web page with text and graphics will require multiple hits in order to acquire the complete page. The number of hits required to get the entire page, the size of graphic files, the speed of your connection and the transfer speed of all the various nodes between your browser and the Web site all add up to a page that appears in seconds or one that comes in very slowly.

HTTP
Hypertext Transfer Protocol moves hypertext (HTML) files on the Internet from the server you are visiting to the browser you are viewing with.

Internet
The Internet consists of a huge number of inter-connected networks that use the TCP/IP protocols for the location and transfer of data. The Internet evolved from a linking of university and college computers (in the late 1960s and early 1970s) funded by the U.S. Department of Defense and called the ARPANET. The Internet today is a global network of almost 100,000 independent networks.

Intranet
A private network, usually inside an organization, that functions very much like the Internet. It has become common practice to permit access to such Intranets from standalone computers used by students or employees off-campus or off-site. Firewalls, login procedures and passwords are designed to provide security.

IP Number
The Internet Protocol Number or IP address is a unique number consisting of four parts separated by dots (e.g. 63.227.89.66). Every computer of the Internet from the largest server to a laptop communicating through a cell phone has a unique IP number. Not every computer has a domain name but everyone has an IP.

ISDN
Integrated Services Digital Network is yet another way of moving data at high speed over existing phone lines (see DSL). ISDN is widely available and with increasing pressure from DSL providers, cost is coming down. While a 128,000 Bps rate is theoretically possible, most users find that reality is in the 56,000 to 64,000 Bps range.

ISP
Internet Service Provider. This is the subscription service that provides you with Internet connectivity. It may be a small local company with a few thousand subscribers, a regional company (e.g. uswest.net) or a nationwide mega-provider like A.O.L. or AT&T WorldNet. Most ISPs sell you a connection, nothing more. They provide no security whatsoever and if your system is hacked and subsequently damaged or destroyed, they don't owe you the time of day. On the other hand, if you are a hacker or violate any of the fine print in your ISP service agreement, they can cut off your Internet access before you can say World Wide Web.

LAN
Local Area Network. Two or more computers that are linked together and able to share programs, data and/or peripherals.

MIME
Multipurpose Internet Mail Extensions, MIME, is the standard format used for transmitting files attached to E-mail messages (pictures, sound files, video files, executables, etc.). The attachment is encoded when it leaves your computer and is decoded and restored to its original form at the receiving end. The specific encoding/decoding format for a given file varies with the file type. Once in a great while, you may receive a MIME format attachment, essentially an attachment that was not properly encoded or decoded. If you open it and look at it, it will appear to be indecipherable gobbledygook.

Modem
MOdulator/DEModulator. Your modem takes data you are sending and modulates it so that it can be transmitted over an analog voice phone line. Your modem accepts incoming modulated data and demodulates it so that it is usable by your computer. The earliest modems required the user to place the telephone handset into a cradle with padded apertures for the two ends of the handset. Speeds were in the range of 300 to 1,200 Bps. With improvements in error correction, modems today under ideal conditions can transmit data at over 50,000 Bps. over a single phone line. DSL and ISDN connections offer even higher speeds. These days the term modem is frequently used to describe external network connection devices that don't actually perform any modulation or demodulation, such as DSL and Cable modems which are actually digital end-to-end.

NAT (Network Address Translator)
A NAT is logically similar to both a proxy and a gateway. The NAT hides the private addresses of the local network from the public address side attached to the Internet. The NAT takes packets from the private network and re-writes them using one of its public IP addresses and sends it onto the public network (Internet). When the response to the packet comes back, the NAT takes this inbound packet and redirects it to the private address that originated the traffic. NATs allow large groups of computers to access the Internet through a very small number of IP addresses. Without NAT technology, the supply of IP addresses would have run dry in the late 1990's. The Internet Connection Sharing built into Windows 98SE and later is a NAT.

Network
When you connect two or more computers, you create a network. When you connect two or more networks you create an internet (lower case "i").

Node
A single computer connected to a network. When you ask Hack Tracer to perform a trace, the Visual Trace Express trace list shows you all of the nodes between your computer and the source of your intrusion event. The nodes simply served as connection points in passing along the data.

Non-Routable IP
See 'Private IP Space'

Packet Switching
This is the method used to move data on the Internet. The data you are sending or receiving is broken up into pieces, each piece carrying the IP address of where it is going and where it is coming from. Billions of these pieces are passing through the Internet at any given time and the major node servers are sorting these pieces and routing them at incredible speeds. The E-mail you are reading or the Web page you are looking at has been reassembled and delivered to your monitor after traveling across town or around the world and, best of all, you don't have to give it a moments thought.

Password
A code (usually alphanumeric) you use to gain access to your computer, to a given program, or to a Web site.

PING
Packet Internet Groper is a program used to determine whether a specific IP address is accessible. A packet is sent to the specified address and the program waits for a reply. Programs like Visual Trace and Visual Trace Express use PING to identify and/or troubleshoot Internet connections. In addition to identifying the target site, these programs also note all of the nodes the data passed through between the two ends of the connection. The most popular shareware PING utility is the full-featured version of Visual Trace.

Port
A place where information goes into and/or out of a computer, e.g. a conventional analog modem is connected to a serial port. The port numbers in TCP/IP communications are virtual values used to separate traffic into application-specific streams. The ports (destination and source) captured in the Hack Tracer Event Log are significant because different applications listen and transmit on different ports. Ports are assigned to standard protocols like SMTP or HTTP so that programs know what port to try a connection on. The destination port for TCP packets indicates the application or server being looked for. In the case of UDP packets, the source port has more significance.

PPP
Point to Point Protocol allows a computer to use a regular phone line and modem to make TCP/IP connections to the Internet.

Private IP Space
Also known as non-routable IP address space. There are three blocks of IP addresses that are reserved for private networks. These IP addresses are used only on private networks, and cannot be connected directly to the public Internet. If a non-routable IP address is used on a computer connected to the Internet, it must gateway through a NAT. The private IP blocks are:
10.0.0.0 through 10.255.255.255 (Any IP Address starting with 10.)
172.16.0.0 through 172.31.255.255
192.168.0.0 through 192.168.255.255

Proxy Server
Proxies are used as intermediaries in connections to the Internet. They are generally only useful for common application uses such as Web browsing. Proxies offer several benefits. They are able to cache page content locally; reducing Internet bound traffic as well as local response time. They offer some security benefits by isolating the local network from direct contact with the Internet. They also offer local ability to restrict access to the Internet in general. Proxies do have many limitations, one of which is that they cannot handle ICMP traffic, the base traffic used for Ping and Traceroute. For small networks, a NAT is a superior solution to a proxy.

Server
A computer or software that provides specific services to software running on other computers. The "mail server" at your ISP is software that handles all of the incoming and outgoing mail for all of your ISP's users. A server on a LAN is hardware that constitutes the primary node on the network. It may also have software that provides specific services, data or other capabilities to all of the client computers attached to it.

SLIP
Serial Line Internet Protocol used to connect a computer to the Internet by way of a phone line. PPP is replacing SLIP because it is more efficient.

SMTP
Simple Mail Transfer Protocol is a set of rules governing the sending and receiving of E-mail on the Internet.

SNMP
Simple Network Management Protocol is a set of standards governing communication with devices connected to a TCP/IP network. This communication takes the form of Protocol Data Units or "PDU's."

SSL
Secure Sockets Layer, a protocol created by Netscape Communications to enable encrypted, secure communications across the Internet. Internet banking, securities and e-commerce sites commonly use SSL.

TCP/IP
Transmission Control Protocol/Internet Protocol, the protocols that make the Internet possible and that make it possible for your computer to be part of the Internet.

Top Level Domains
Top Level Domains (TLDs) are the most common domain name extensions. The most familiar of these is the ubiquitous "DOT COM" but there are others in common usage:
COM US Commercial
EDU US Educational
GOV US Government
INT International
MIL US Military
NET Network
ORG Non-Profit Organization

Trojan Horse
A type of computer worm or virus that comes to you disguised as a desirable program. The name is based on the famous Trojan horse that was left outside the walls of Troy by a departing army that appeared to have given up its plans of conquest. The horse, which concealed a band of soldiers, was brought into the walled city by its unwary inhabitants. The soldiers opened the gates of the city in the middle of the night and Troy was destroyed by the returning troops.

URL
Uniform Resource Locator, the standard format for Internet addresses.

USENET
More commonly called Newsgroups, USENET is a decentralized worldwide community made up of almost 20,000 discussion groups covering almost every conceivable area of interest. Rule of thumb: don't accept software from someone you meet in a newsgroup or chat room!

VPN
Virtual Private Network. A network that makes use of the Internet to connect computers that are in different locations. Communication is encrypted for security.

WAN
Wide Area Network, a network of computers that covers an area larger than a single building or campus. In the past WANs have been private networks connecting geographically separated offices of the same organization. WANs are rapidly being replaced by the Internet and the wide use of VPNs.

WWW
The World Wide Web or just "The Web." Many people think of this in terms of what is accessible to their browser but in reality the Web now encompasses all of the resources that make up the Internet including such things as FTP sites, USENET, and much more.