VOSTROM

Download Buy Now Get Help

PATH ANALYZER PRO
illuminate your path.

path discovery, whois, firewall detection, geolocation, network testing
traceroute finally makes sense

Path Analyzer Pro Manual

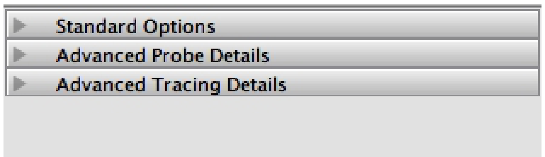
Introduction

Hello and welcome to the Path Analyzer Pro manual. You may begin your first trace immediately with the default settings installed.

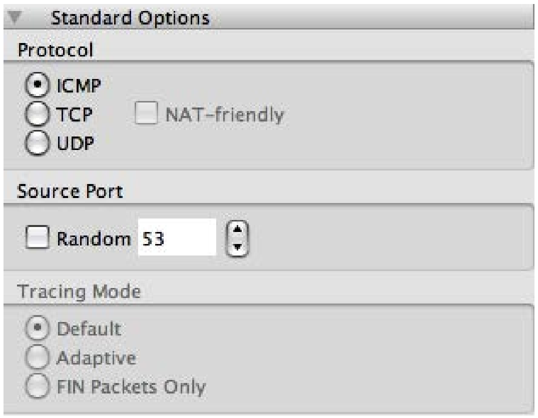
Software Customization

The Path Analyzer Pro manual will help you better understand the unique features of the software and how to change the default settings to customize the software for your specific needs.

Path Analyzer Pro has three main levels of options: Standard Options, Advanced Probe Details and Advanced Tracing Details.



Standard Options


Standard Options

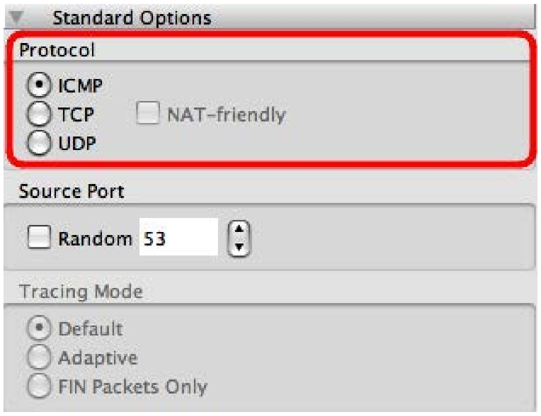
Protocol
● ICMP
○ TCP □ NAT-friendly
○ UDP

Source Port
□ Random 53

Tracing Mode
● Default
○ Adaptive
○ FIN Packets Only

The Standard Options section provides the user with customizable features that can affect your traceroute results. You will find that changing one or all of the features changes the amount of data received between the source and target. The three subsections include: Protocol, Source Port, and Tracing Mode.

Protocol



Standard Options

Protocol

● ICMP
○ TCP □ NAT-friendly
○ UDP

Source Port

□ Random 53

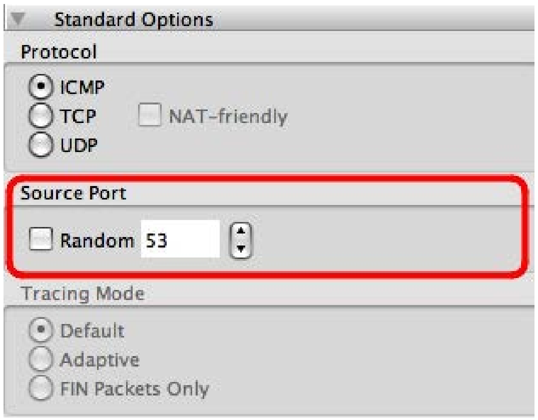
Tracing Mode

● Default
○ Adaptive
○ FIN Packets Only

Some traditional traceroute programs use the User Datagram Protocol (UDP) and others use the Internet Control Message Protocol (ICMP) to perform traces. Path Analyzer Pro is superior to traditional traceroute as you are given the option to choose which protocol you would like to use to perform a trace including ICMP,TCP or UDP. The following information may help you to determine which protocol to use for your trace:

ICMP- used generally for network debugging such as slow internet connectivity
TCP- used for web traffic, file transfers, and most common application protocols.
*NAT-friendly- only applies to TCP traces
UDP- used for Voice over IP (VoIP), streaming music and video, etc.

Source Port



Standard Options

Protocol

● ICMP
○ TCP □ NAT-friendly
○ UDP

Source Port

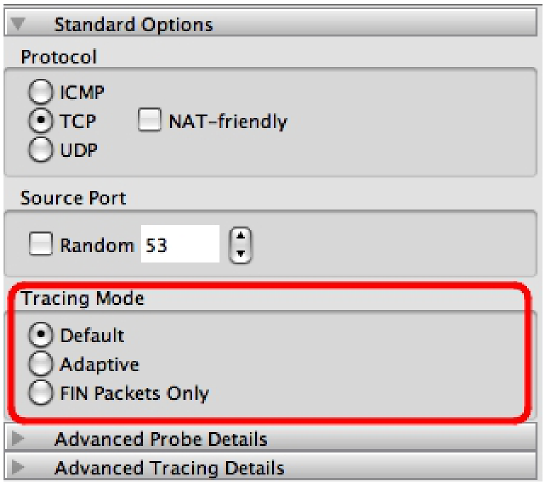
□ Random 53

Tracing Mode

● Default
○ Adaptive
○ FIN Packets Only

Path Analyzer Pro uses the default source port of 53 for all TCP and UDP traces. For a listing of other source port numbers you can visit www.iana.org. Source port numbers range from zero to 65,535. If youÕre not sure which source port to use, itÕs a safe choice to check the ÔrandomÕ checkbox instead, allowing Path Analyzer Pro to select one for you. Please Note: You may need to change the source port if there is a firewall at the target address. Whatever you enter will be remembered from trace to trace, but if you want to change the softwareÕs default settings to always use a certain source and destination port automatically with each different protocol, you may specify them in the Preferences section under the Ports tab. The preferences section will be detailed later in this manual.

Tracing Mode



▼ Standard Options

Protocol

○ ICMP
● TCP □ NAT-friendly
○ UDP

Source Port

□ Random 53

Tracing Mode

● Default
○ Adaptive
○ FIN Packets Only

▶ Advanced Probe Details

▶ Advanced Tracing Details

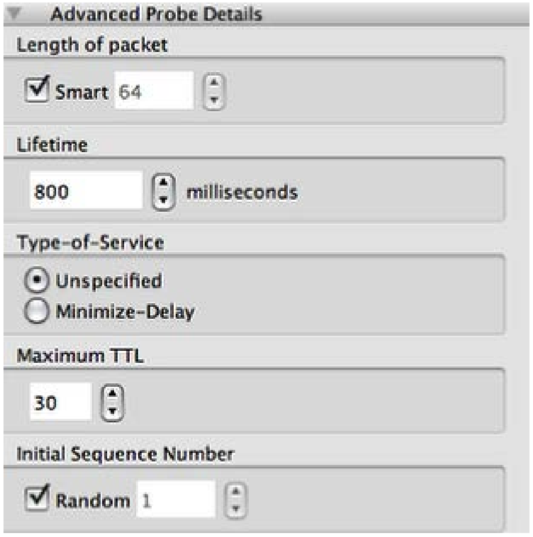
The Tracing Mode options are only available to the user when performing a TCP protocol trace. To activate and change the Tracing Mode options first choose TCP as your protocol under the Standard Options tab.

Default- The Tracing Mode is already set to Default which generates probes that appear to the target as a regular application.

Adaptive- generates probes that fool the target, possibly revealing more information, such as firewalls, in the path. Please Note: Your ability to successfully complete traces while using Adaptive mode depends not only on the target, but also on the security features of your local network. The sophisticated set of adaptive probes generated by Path Analyzer Pro when set to Adaptive mode may be discarded by your local network security equipment.

FIN Packets Only-generates only TCP packets with the FIN flag set in order to solicit an RST or TCP reset packet as a response from the target. This option may get beyond a firewall at the target thus giving the user more trace data but could be misconstrued as a malicious attack. Please Note: Path Analyzer Pro is not designed to be used as an attack tool.

Advanced Probe Details



▼ Advanced Probe Details

Length of packet

☑ Smart 64

Lifetime

800 milliseconds

Type-of-Service

● Unspecified
○ Minimize-Delay

Maximum TTL

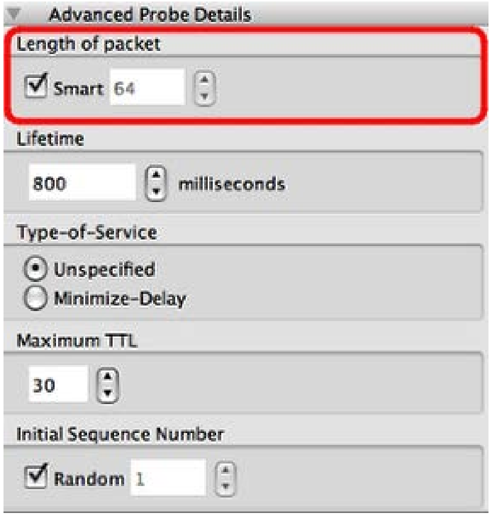
30

Initial Sequence Number

☑ Random 1

The Advanced Probe Details settings determine how probes are generated to perform the trace. This includes the Length of packet, Lifetime, Type of Service, Maximum TTL, and Initial Sequence Number.

Length of packet



Advanced Probe Details

Length of packet

☑ Smart 64

Lifetime

800 milliseconds

Type-of-Service

● Unspecified

○ Minimize-Delay

Maximum TTL

30

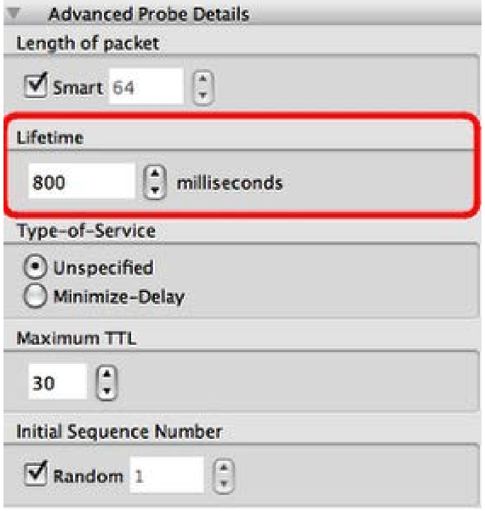
Initial Sequence Number

☑ Random 1

This option allows you to set the length of the packet for a trace. The minimum size of a packet, as a general rule, is approximately 64 bytes,depending on the protocol used. The maximum size of a packet depends on the physical network, but is generally 1500 bytes for a regular Ethernet network or 9000 bytes using Gigabit Ethernet networking with jumbo frames.

*Smart- Path Analyzer Pro uses Smart as the default Length of packet. When the Smart Option is checked the software will automatically select the minimum size of packets based on the protocol selected under Standard Options.

Lifetime



Advanced Probe Details

Length of packet

☑ Smart 64

Lifetime

800 milliseconds

Type-of-Service

● Unspecified

○ Minimize-Delay

Maximum TTL

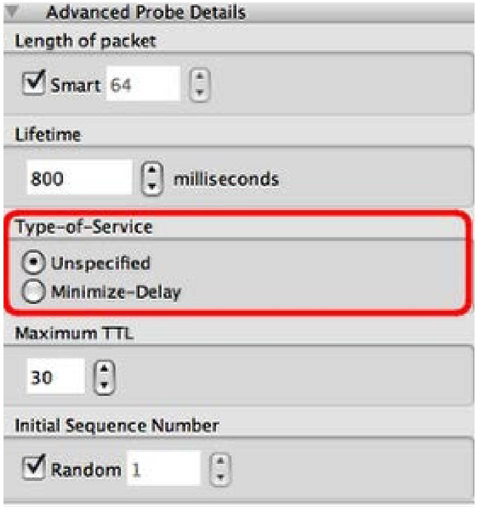
30

Initial Sequence Number

☑ Random 1

The amount of time the software waits for a response from the target before determining the packet was dropped. The default is set to 800 milliseconds.

Type-of-Service



Advanced Probe Details

Length of packet

☑ Smart 64

Lifetime

800 milliseconds

Type-of-Service

● Unspecified
○ Minimize-Delay

Maximum TTL

30

Initial Sequence Number

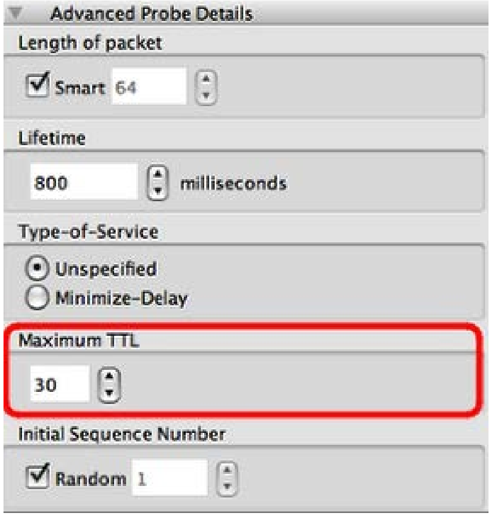
☑ Random 1

This field determines if the Type-of-Service (ToS) field within the packet is filled-in or not. In the IP Datagram, 8 bits are reserved for the service type. Some routers use this field to determine the priority of the packet.

Unspecified- the field is not filled-in within the packet when sent.

Minimize-Delay-the ToS field of the packet is filled-in with the ÒMinimize-DelayÓ option. The Minimize-Delay Type of Service may give priority to the packet sent, thus giving faster results when used in networks that support this field.

Maximum TTL



Advanced Probe Details

Length of packet

☑ Smart 64

Lifetime

800 milliseconds

Type-of-Service

● Unspecified
○ Minimize-Delay

Maximum TTL

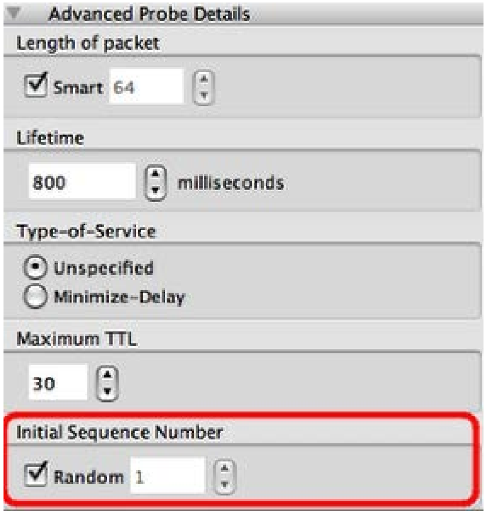
30

Initial Sequence Number

☑ Random 1

The maximum Time To Live (TTL) is the maximum number of hops to probe in an attempt to reach the target. The default number of hops is set to 30. The Maximum TTL that can be used is 255.

Initial Sequence Number



▼ Advanced Probe Details

Length of packet

☑ Smart 64

Lifetime

800 milliseconds

Type-of-Service

● Unspecified

○ Minimize-Delay

Maximum TTL

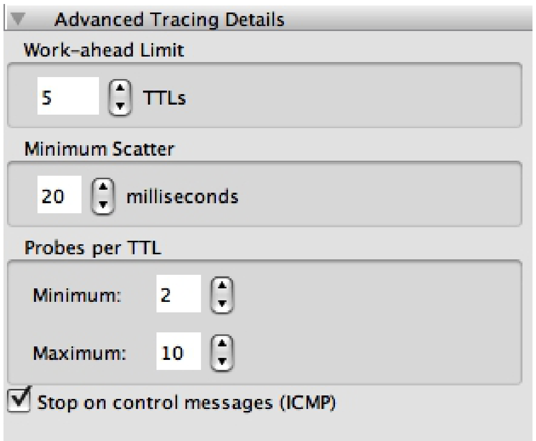
30

Initial Sequence Number

☑ Random 1

The Initial Sequence Number is set as a counting mechanism within the packet between the source and target. It is set to Random as the default but you may choose another starting number by unchecking the Random button and filling-in a different number. Please Note: The Initial Sequence Number only applies to TCP connections.

Advanced Tracing Details



▼ Advanced Tracing Details

Work-ahead Limit

5 TTLs

Minimum Scatter

20 milliseconds

Probes per TTL

Minimum: 2

Maximum: 10

☑ Stop on control messages (ICMP)

The Advanced Tracing Details affect the speed and thoroughness of your trace.

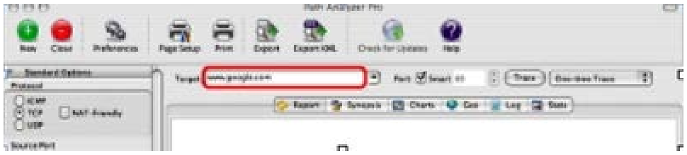
Work-ahead Limit- this option allows you to set a limit of the number of TTLÕs(hops ahead) the software will probe before awaiting replies. The default is set to 5 hops ahead.

Minimum Scatter-used to set the minimum amount of time to pause between sending probes. The default is set to 20 milliseconds.

Probes per TTL-used to set the minimum and maximum amount of probes sent to each hop. The more probes you send the more thorough the resulting statistics, the less probes you send the faster your trace will complete.

Stop on control messages (ICMP)- tells the software to stop if ICMP messages are received from the target. This option is automatically checked as its default.

Now that your options have been set letÕs begin your first trace!



Target www.google.com

Performing Your First Trace

Enter a Target

A target is the only mandatory parameter for a trace session. Simply click inside the Target field and enter one of either a Hostname, IP Address, URL, or E-mail address.

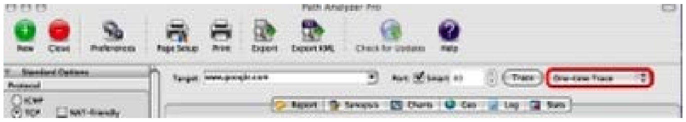
Hostnames may be entered using regular notation such as www.google.com. If a hostname is entered and Smart destination port selection is enabled, Path Analyzer will try to determine what kind of server processes the hostname you provided may be running. For example, a server beginning with www would be identified as a web server, and Path Analyer would set the destination port to 80 automatically. If you don't want Path Analyzer to automatically set the destination port, simple uncheck the Smart checkbox and set the destination port manually or accept the default.

IP addresses may be entered in quad-dotted notation, like 4.2.2.1. If an IP address is entered, Path Analyzer uses the default settings for source and destination ports (or the last settings if you customized them).

E-mail addresses must be in the form someone@example.com. If an e-mail address is entered, Path Analyzer will automatically perform a DNS MX (Mail Exchanger) lookup to determine the primary mail exchange for this e-mail address and auto-configure itself to trace to that server, destination port 25. Extra information related to the target e-mail system will also be revealed under the Synopsis tab if e-mail tracing is used.

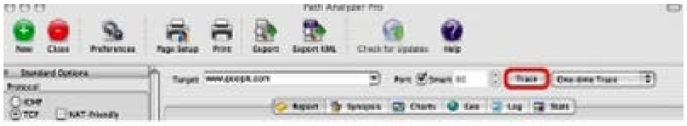
URLs may be entered in their complete form such as ftp://ftp.example.com:21/. If a URL is entered with the port attribute omitted, Path Analyzer will automatically check the URL against the local system's services database to find the appropriate destination port for the service referenced in the URL. For example, http would yield destination port 80. If a port is included in the URL, Path Analyzer pro will auto-configure itself to use the destination port referenced inside the URL you provided.

Select a Duration



By clicking on the duration selector, you can configure Path Analyzer to perform a One-time Trace, a Timed Trace, or a Continuous Trace. Just as their names suggest, a One-time trace will perform the trace just once, a Timed Trace will ask you to select a duration in Hours:Minutes:Seconds format, and a Continuous Trace will continue forever until it is interrupted by pressing the Stop button.

Begin your trace



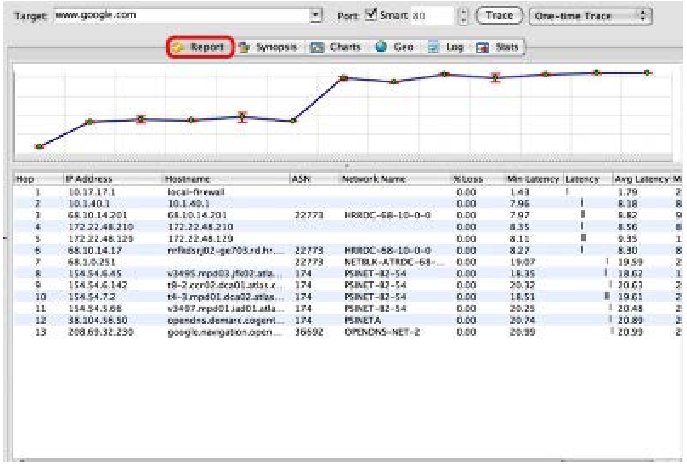
By clicking on the Trace button or simply by pressing Return while your cursor is still in the Target entry field, Path Analyzer will begin the trace.

While Path Analyzer is performing the trace, the Trace button will change to a Stop button which allows you to terminate the trace prematurely at any time.

LetÕs take a look at the trace results obtained by Path Analyzer Pro!

Path Analyzer Pro comes fully-equipped with automatic Report generation, a one-page Synopsis of your trace results, impressive charts used to Chart your trace results, Geo location of your trace with export to Google Earth, a traceroute Log and traceroute Statistics. All of the information within each window is exportable making it a must-have tool for any network-engineer or systems professional.

REPORTS



Hop	IP Address	Hostname	ASN	Network Name	%Loss	Min Latency	Latency	Avg Latency	M
1	10.17.17.1	local-firewall			0.00	1.43		1.79	2
2	10.1.40.1	10.1.40.1			0.00	7.96		8.18	8
3	68.10.14.201	68.10.14.201	22773	HRRDC-68-10-0-0	0.00	7.97		8.82	9
4	172.22.48.210	172.22.48.210			0.00	8.35		8.56	8
5	172.22.48.129	172.22.48.129			0.00	8.11		9.35	1
6	68.10.14.17	rcfldsrj02-ge703.rd.hr...	22773	HRRDC-68-10-0-0	0.00	8.27		8.30	8
7	68.1.0.251		22773	NETBLK-ATRDC-68-...	0.00	19.07		19.59	2
8	154.54.6.45	v3495.mpd03.jfk02.atla...	174	PSINET-82-54	0.00	18.35		18.62	1
9	154.54.6.142	t8-2.ccr02.dca01.atlas.c...	174	PSINET-82-54	0.00	20.32		20.63	2
10	154.54.7.2	t4-3.mpd01.dca02.atlas...	174	PSINET-82-54	0.00	18.51		19.61	2
11	154.54.3.66	v3497.mpd01.iad01.atla...	174	PSINET-82-54	0.00	20.25		20.48	2
12	38.104.36.50	opendns.demarc.cogent...	174	PSINETA	0.00	20.74		20.89	2
13	208.69.32.230	google.navigation.open...	36692	OPENDNS-NET-2	0.00	20.99		20.99	2

The Report tab in the main window shows a linear chart depicting the number of hops between you and the target. The line connects each hop at a point whose vertical position is determined by its latency. The higher the point, the higher that hopÕs latency. This gives you an instant visual of whether a network connectivity problem may be occurring. Below the linear chart is a list columns giving the specific results for your trace.

Hop-When performing a trace, data is sent from you to the target. Your results will show all of the devices, routers, servers, etc., that your data packets passed-through to get to the target. Each device is called a hop in the path, starting at hop 1 and incrementing until it reaches the target. Please note: If Path Analyzer Pro informs you that no replies were received from a specific hop in the path, a device is likely receiving it, but is intentionally not responding. This is common behavior amongst network security devices such as firewalls.

IP Address- Every device has a corresponding IP address listed for each hop.

Hostname- Each IP address may have a corresponding hostname listed in the global domain name system (DNS).

ASN- Autonomous System Numbers identify the network responsible for the IP address at the time of this trace. These numbers are important because the ASN uniquely identifies each network on the Internet. This number is used to identify who is the responsible Internet Service Provider (ISP) for each IP address or hop.

Network Name- The network name is the name given to the allocation of IP addresses by its registrant. This is customarily the name of the ISP. This data is based on the AS number and/or network registry information attained via whois, whichever is more specific at the time of your trace.

% Loss- The percentage of probe packets Path Analyzer Pro sent to each hop that did not result in any perceivable reply.

Min Latency-The minimum amount of latency for a given hop. (the valley) Please note: Latency is the time it takes for Path Analyzer ProÕs probe packets to reach the hop and the time it takes the hopÕs reply to be received, or the total round trip time of packets.

Latency- Depicts the same information as the linear chart above to associate latency with a particular hop in a column view. Latency is the roundtrip time from you to the target.

Avg Latency-The average amount of latency for a given hop.

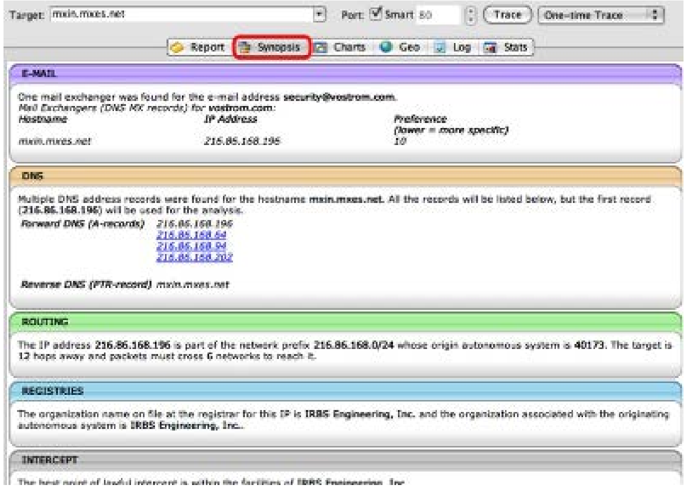
Max Latency- The maximum amount of latency for a given hop. (the peak)

Std Dev- Standard Deviation, also known as jitter, shows you where network anomalies may be occurring. Standard deviation is a mathematical equation used to calculate the variance, an average of the squared differences between data points and the mean. The standard deviation is the most common measure of how widely spread the values in a data set are. Standard deviation is an important factor in telecommunications. Technically, it is a characterization of the aggregate random and deterministic (predictable) jitter. Jitter is essentially a variation in the communications signal. In this case, jitter is the variation in the total round trip time (latency) between the source and the destination of a probe. Understanding jitter is important because depending on the protocol or application being communicated, transporting data back and forth more slowly may actually be optimal compared to having some information arrive early and some late. This is especially important for such applications and voice over IP (VoIP). Therefore, a network with less jitter should be considered more stable/reliable than a network with more jitter. Or, to put it another way, the lower the jitter, the better.

Please note:

You may cut-and-paste any information attribute from the Report page by right-clicking on it (which will reveal a context-sensitive menu). Alternatively, the entire report grid may be exported to an comma-separated values (CSV) document using the Export feature. The CSV export format is perfect for importing into your favorite spreadsheet application.

Synopsis



Target: mxin.mxes.net

Port: ☑ Smart 80

One-time Trace

E-MAIL

One mail exchanger was found for the e-mail address **security@vostrom.com**.

Mail Exchangers (DNS MX records) for ***vostrom.com:***

Hostname	*IP Address*	*Preference (lower = more specific)*
mxin.mxes.net	*216.86.168.196*	*10*

DNS

Multiple DNS address records were found for the hostname **mxin.mxes.net**. All the records will be listed below, but the first record (**216.86.168.196**) will be used for the analysis.

Forward DNS (A-records) *216.86.168.196*
216.86.168.64
216.86.168.94
216.86.168.202

Reverse DNS (PTR-record) *mxin.mxes.net*

ROUTING

The IP address **216.86.168.196** is part of the network prefix **216.86.168.0/24** whose origin autonomous system is **40173**. The target is **12** hops away and packets must cross **6** networks to reach it.

REGISTRIES

The organization name on file at the registrar for this IP is **IRBS Engineering, Inc.** and the organization associated with the originating autonomous system is **IRBS Engineering, Inc.**.

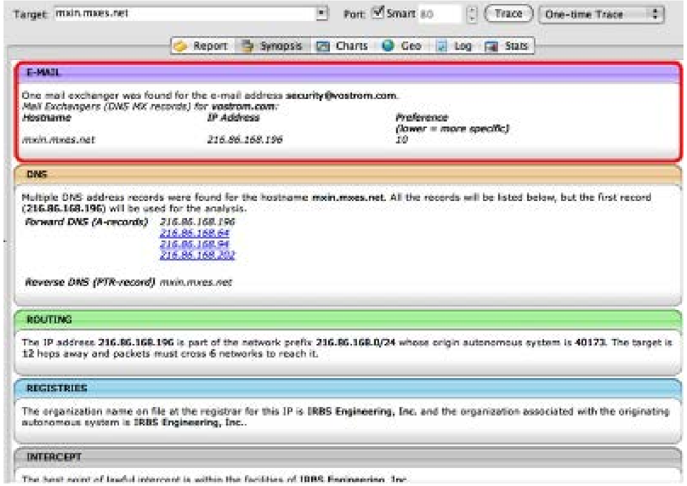
INTERCEPT

The best point of lawful intercept is within the facilities of **IRBS Engineering, Inc**

The Synopsis tab is Path Analyzer ProÕs #1 customer-ranked feature. It gives you a one-page summary containing the most important high-level details of your trace. The Synopsis page can be used to explain the details of the path between you and a target in plain language, or to determine the best point of lawful intercept to name just a few examples. You may cut-and-paste information from the Synopsis page, or the entire page may be exported to an HTML document using the Export feature. The HTML document may be inserted into an e-mail or opened using any standard web browser.

The Synopsis is divided into several sections explained below.

Email



Target: mxin.mxes.net

Port: ☑ Smart 80

E-MAIL

One mail exchanger was found for the e-mail address **security@vostrom.com**.
Mail Exchangers (DNS MX records) for ***vostrom.com:***

Hostname	***IP Address***	***Preference*** ***(lower = more specific)***
mxin.mxes.net	*216.86.168.196*	*10*

DNS

Multiple DNS address records were found for the hostname **mxin.mxes.net**. All the records will be listed below, but the first record (**216.86.168.196**) will be used for the analysis.

Forward DNS (A-records) *216.86.168.196*
216.86.168.64
216.86.168.94
216.86.168.202

Reverse DNS (PTR-record) *mxin.mxes.net*

ROUTING

The IP address **216.86.168.196** is part of the network prefix **216.86.168.0/24** whose origin autonomous system is **40173**. The target is **12** hops away and packets must cross **6** networks to reach it.

REGISTRIES

The organization name on file at the registrar for this IP is **IRBS Engineering, Inc.** and the organization associated with the originating autonomous system is **IRBS Engineering, Inc.**.

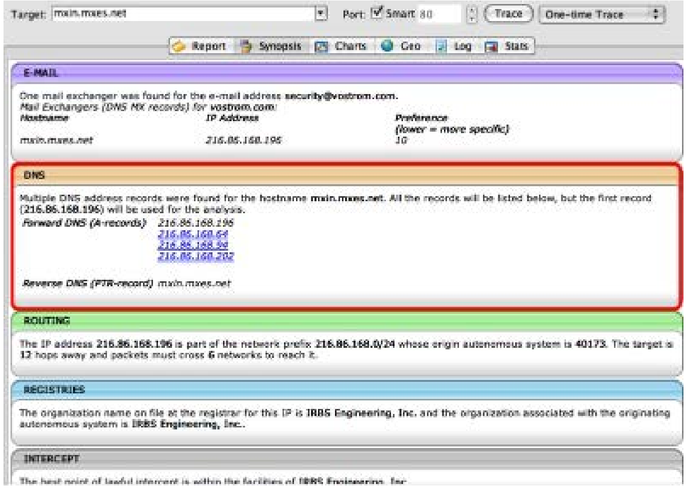
INTERCEPT

The best point of lawful intercept is within the facilities of **IRBS Engineering, Inc.**

The e-mail section of the Synopsis appears when you enter an e-mail address as a target. Path Analyzer Pro automatically search DNS to find all the mail servers on the Internet responsible for handling mail for e-mail address you entered. All the mail servers (referred to as mail exchangers) the software discovered are listed by their hostname, IP address and preference/priority.

The mail server with the lowest priority number is the one chiefly responsible for handling the userÕs e-mail. Mail servers with a higher priority number are usually back-up mail servers. If multiple servers are found with the same lowest-priority number, they are both equally responsible for the userÕs e-mail service and either may be used. Path Analyzer Pro automatically selects the most specific e-mail server for the basis of its trace, but clicking on any other mail server listed in the Synopsis will completely refresh the Synopsis page to display the most specific information for the IP you clicked.

DNS



Target: mxin.mxes.net

Port: ☑ Smart 80

E-MAIL

One mail exchanger was found for the e-mail address **security@vostrom.com**.
Mail Exchangers (DNS MX records) for ***vostrom.com:***

Hostname	***IP Address***	***Preference*** ***(lower = more specific)***
mxin.mxes.net	*216.86.168.196*	*10*

DNS

Multiple DNS address records were found for the hostname **mxin.mxes.net**. All the records will be listed below, but the first record (**216.86.168.196**) will be used for the analysis.

Forward DNS (A-records) *216.86.168.196*
216.86.168.64
216.86.168.94
216.86.168.202

Reverse DNS (PTR-record) *mxin.mxes.net*

ROUTING

The IP address **216.86.168.196** is part of the network prefix **216.86.168.0/24** whose origin autonomous system is **40173**. The target is **12** hops away and packets must cross **6** networks to reach it.

REGISTRIES

The organization name on file at the registrar for this IP is **IRBS Engineering, Inc.** and the organization associated with the originating autonomous system is **IRBS Engineering, Inc.**.

INTERCEPT

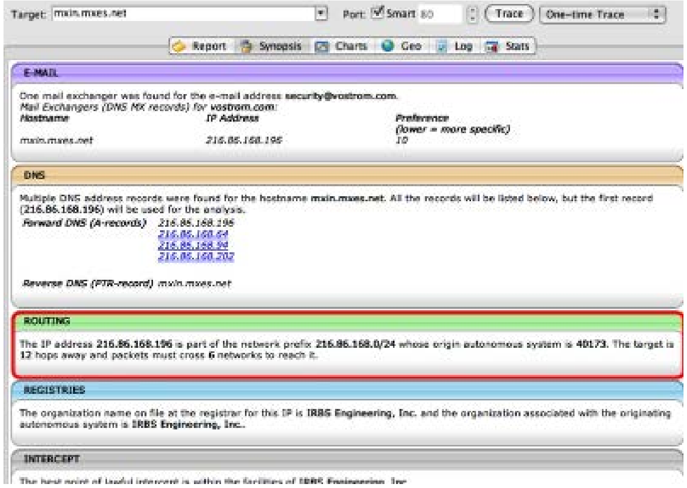
The best point of lawful intercept is within the facilities of **IRBS Engineering, Inc.**

The DNS section of the Synopsis provides all the important DNS information about your target. This section will change to include the most relevant information based on the target you enter, including DNS address (A) records, in-addr pointer (PTR) records, canonical names (CNAME) records, etc.

DNS makes it possible to use multiple IP addresses for a single hostname. So, if youÕre tracing by hostname, you should always check the Synopsis as it will reveal all DNS address (A) records associated with the hostname you type. Plus, these other IP addresses are clickable, and one click on each will completely refresh the Synopsis page to display the most specific information for the IP you clicked.

Similarly, if you type an IP address as your trace target, the Synopsis DNS section with show you the DNS in-addr (reverse) name associated with the IP.

Routing



E-MAIL

One mail exchanger was found for the e-mail address **security@vostrom.com.**
Mail Exchangers (DNS MX records) for **vostrom.com:**

Hostname	*IP Address*	*Preference (lower = more specific)*
mxin.mxes.net	*216.86.168.196*	*10*

DNS

Multiple DNS address records were found for the hostname **mxin.mxes.net**. All the records will be listed below, but the first record (216.86.168.196) will be used for the analysis.

Forward DNS (A-records) *216.86.168.196*
216.86.168.64
216.86.168.94
216.86.168.202

Reverse DNS (PTR-record) mxin.mxes.net

ROUTING

The IP address **216.86.168.196** is part of the network prefix **216.86.168.0/24** whose origin autonomous system is **40173**. The target is **12** hops away and packets must cross **6** networks to reach it.

REGISTRIES

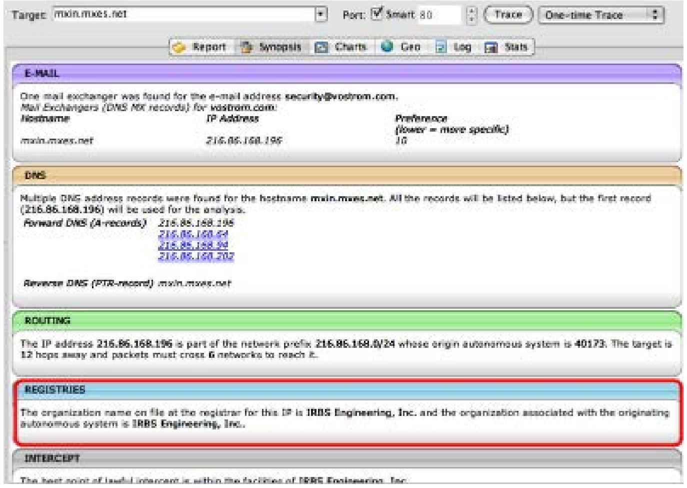
The organization name on file at the registrar for this IP is **IRBS Engineering, Inc.** and the organization associated with the originating autonomous system is **IRBS Engineering, Inc.**.

INTERCEPT

The best point of lawful intercept is within the facilities of **IRBS Engineering, Inc.**

The Routing section of the Synopsis gives you a clear summary of the target IP address, the most specific global network prefix to which it belongs, and the Autonomous System Number (ASN) of the ISP or organization responsible for announcing this prefix on the Internet. In addition, we see that the trace results from the Report Tab is summarized by stating that the target is 12 hops away and packets must cross 6 networks to reach it. Because Path Analyzer Pro determined which ISPs were responsible for every IP address involved in the trace, it determined how many different network jurisdictions were involved in the path between you and the target.

Registries - (Whois)



E-MAIL

One mail exchanger was found for the e-mail address **security@vostrom.com.**
Mail Exchangers (DNS MX records) for **vostrom.com:**

Hostname	*IP Address*	*Preference (lower = more specific)*
mxin.mxes.net	*216.86.168.196*	*10*

DNS

Multiple DNS address records were found for the hostname **mxin.mxes.net**. All the records will be listed below, but the first record (216.86.168.196) will be used for the analysis.

Forward DNS (A-records) *216.86.168.196*
216.86.168.64
216.86.168.94
216.86.168.202

Reverse DNS (PTR-record) mxin.mxes.net

ROUTING

The IP address **216.86.168.196** is part of the network prefix **216.86.168.0/24** whose origin autonomous system is **40173**. The target is **12** hops away and packets must cross **6** networks to reach it.

REGISTRIES

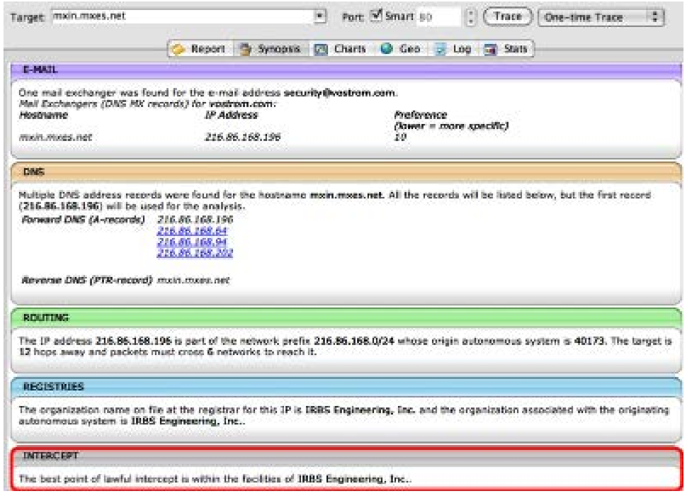
The organization name on file at the registrar for this IP is **IRBS Engineering, Inc.** and the organization associated with the originating autonomous system is **IRBS Engineering, Inc.**.

INTERCEPT

The best point of lawful intercept is within the facilities of **IRBS Engineering, Inc.**

The Registries section gives you a summary of the information currently on file with the Regional Internet Registries with regard to the IP address of the target.. Before, in the Routing section, Path Analyzer Pro automatically determined the AS number 40173 for the IP address 216.86.168.196 which tells you who is responsible for routing the target IP address. Now, in the Registries section, Path Analyzer Pro automatically determined the organization name associated with the target IP address at the Regional Internet Registry, which in the sample here is IRBS Engineering, Inc., the target Ôs ISP. It is important not only to find out who is responsible for the assignment of this target IP address, but also who is the party currently responsible for its routing on the Internet. This is is referred to as the organization associated with the originating autonomous system, also disclosed by Path Analyzer Pro.

Intercept



Target: mxin.mxes.net Port: ☑ Smart 80

E-MAIL

One mail exchanger was found for the e-mail address **security@vostrom.com**.
Mail Exchangers (DNS MX records) for **vostrom.com**:

Hostname	*IP Address*	*Preference (lower = more specific)*
mxin.mxes.net	*216.86.168.196*	*10*

DNS

Multiple DNS address records were found for the hostname **mxin.mxes.net**. All the records will be listed below, but the first record (**216.86.168.196**) will be used for the analysis.

Forward DNS (A-records) *216.86.168.196*
216.86.168.64
216.86.168.94
216.86.168.202

Reverse DNS (PTR-record) *mxin.mxes.net*

ROUTING

The IP address **216.86.168.196** is part of the network prefix **216.86.168.0/24** whose origin autonomous system is **40173**. The target is **12** hops away and packets must cross **6** networks to reach it.

REGISTRIES

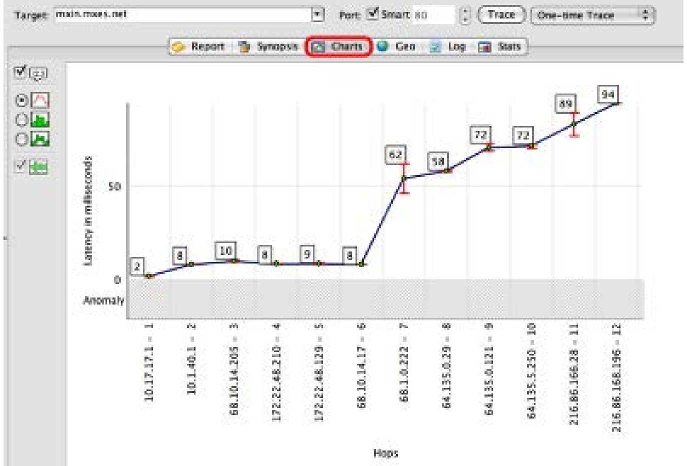
The organization name on file at the registrar for this IP is **IRBS Engineering, Inc.** and the organization associated with the originating autonomous system is **IRBS Engineering, Inc.**.

INTERCEPT

The best point of lawful intercept is within the facilities of **IRBS Engineering, Inc.**.

The Intercept section is particularly important to law enforcement professionals tracking down sources of on-line fraud and for other reasons. This section finds the point in the global network where all possible routes to a target IP address converge. In the network recommended by Path Analyzer Pro as the best point of lawful intercept, it is possible to intercept all communications between the target IP address and the Internet at large.

CHARTS



The Charts tab gives you a variety of impressive charts used to display the results of your trace. You pick which chart to use and your data is automatically showcased without the hassle of using additional software. Each chart depicts the latency in milliseconds (y-axis) between you and each corresponding IP address or hop (x-axis) between you (left-most) and the target of your trace (right-most). This visual representation can make it easier to see where network anomalies are occurring.

Chart options include:

*Show Labels - Check this box to show on your chart the maximum number in milliseconds of latency for a given IP address (hop).

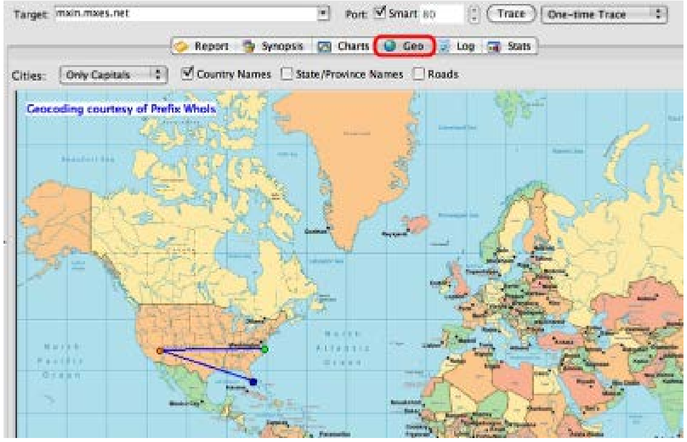
Linear Chart - Select this option to view your results as a Linear Chart. In a linear chart, a horizontal line connects the average latency value of each hop while a vertical line is drawn between the minimum and maximum latency values of each hop.

Bar Chart - Select this option to view your results as a Bar Chart in which each IP address/hop is measured by a vertical bar depicting its average latency value. Traffic-light-type colorization is applied to the bar chart to indicate areas of reasonable (green), sub-optimal (yellow) and problematic (red) average latency.

Mirrored Chart -To create a Mirrored Chart select the Bar Chart icon and then check the Mirrored Chart checkbox. Some people find the mirrored bar chart easier to read at-a-glance.

Candles Chart- Select this option to view your results as a Candles Chart. In a candles-type chart, a bar is drawn between the minimum and maximum latency values of each hop, and a horizontal line is drawn inside the bar at the average latency value.

GEO



Target: main.mxes.net Port: ☑ Smart 80 One-time Trace

Cities: Only Capitals ☑ Country Names □ State/Province Names □ Roads

Path Analyzer Pro uses map imagery to highlight the location of each IP address in the path between you and your target. The map included in Path Analyzer Pro is a layered, zoom-able Mercator projection of the whole Earth.

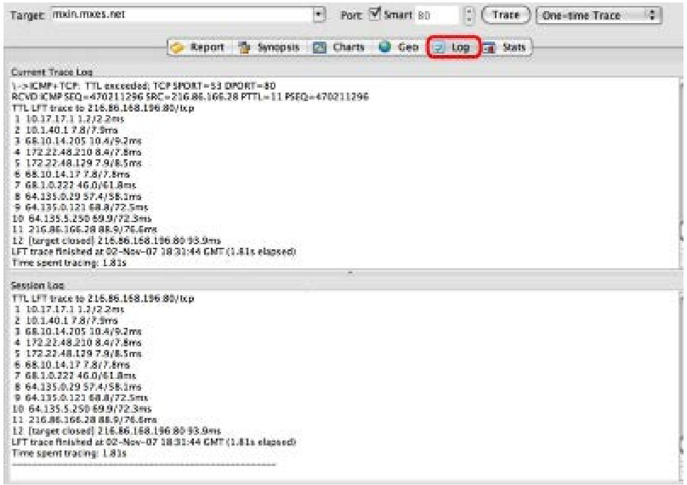
For an even more detailed and immersive view of the path, you may use the Export feature to save a Keyhole Markup Language (KML) file that can be opened by Google Earth. You may also click the Export KML button to immediately launch Google Earth to view the trace without saving the KML file.

After selecting the Geo tab, your mapped results can be viewed in a variety of ways. LetÕs first take a look at Cities. Select the drop-down box to select cities of what minimum population-size you would like to display on your map. As you can see in our example your options include: None (or no cities shown), Only Capitals, 3,000,000 + population , 900,000 + population, 250,000 + population, 75,000 + population, or All cities. You may choose to add the Country Names, State/Province Names and Roads to your map by selecting their corresponding checkboxes.

By hovering your mouse over any point on the path, a popup window will appear in which you are able to view its Longitude, Latitude, Country, State, and City. In addition, you can view the hop number (HOPNO), IP address, hostname, and ASN as displayed in your trace results.

After exploring the map features you can Export your map to Google Earth by clicking on the Export KML icon in the toolbar at the top of the Path Analyzer Pro main window. You can manipulate your mapped results in Google Earth to further zoom in on your target or path. Alternatively, you may use the Export feature to save the geographic information in a keyhole markup language (KML) format file to be opened with Google Earth or another compatible software program later on.

LOG



Target: main.mxes.net Port: ☑ Smart 80 One-time Trace

Current Trace Log

```
\->ICMP+TCP: TTL exceeded; TCP SPORT=53 DPORT=80
RCVD ICMP SEQ=470211296 SRC=216.86.166.28 PTTL=11 PSEQ=470211296
TTL LFT trace to 216.86.168.196:80/tcp
 1  10.17.17.1 1.2/2.2ms
 2  10.1.40.1 7.8/7.9ms
 3  68.10.14.205 10.4/9.2ms
 4  172.22.48.210 8.4/7.8ms
 5  172.22.48.129 7.9/8.5ms
 6  68.10.14.17 7.8/7.8ms
 7  68.1.0.222 46.0/61.8ms
 8  64.135.0.29 57.4/58.1ms
 9  64.135.0.121 68.8/72.5ms
10  64.135.5.250 69.9/72.3ms
11  216.86.166.28 88.9/76.6ms
12  [target closed] 216.86.168.196:80 93.9ms
LFT trace finished at 02-Nov-07 18:31:44 GMT (1.81s elapsed)
Time spent tracing: 1.81s
```

Session Log

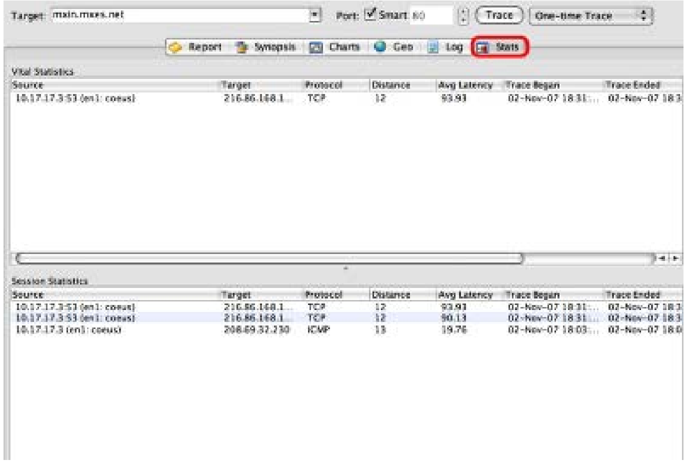
```
TTL LFT trace to 216.86.168.196:80/tcp
 1  10.17.17.1 1.2/2.2ms
 2  10.1.40.1 7.8/7.9ms
 3  68.10.14.205 10.4/9.2ms
 4  172.22.48.210 8.4/7.8ms
 5  172.22.48.129 7.9/8.5ms
 6  68.10.14.17 7.8/7.8ms
 7  68.1.0.222 46.0/61.8ms
 8  64.135.0.29 57.4/58.1ms
 9  64.135.0.121 68.8/72.5ms
10  64.135.5.250 69.9/72.3ms
11  216.86.166.28 88.9/76.6ms
12  [target closed] 216.86.168.196:80 93.9ms
LFT trace finished at 02-Nov-07 18:31:44 GMT (1.81s elapsed)
Time spent tracing: 1.81s
----------------------------------------------------------------
```

The Log tab details all data packets being sent and received by the program. The Log is specifically meant to be used by the experienced network engineer or system administrator.

The Current Trace Log shows you packet details based look at your current trace. Now, if you scroll down to the bottom of your Current Trace Log you should see your trace results as they would typically be displayed in a normal traceroute through a command line interface. Take a look at our example here. From the number 1, meaning our first hop, we can see the corresponding IP address and the latency in milliseconds. Also, you can easily highlight this information and Copy and Paste it into an email without having to export it.

The Session Log details all past traces performed by the software since last opened. Note: The past route traces will not be saved after closing Path Analyzer Pro. If you want to retain these logs, it is best to use the Export button to save your trace results before closing the program.

STATS



Target: main.mxes.net Port: ☑ Smart 80 One-time Trace

Vital Statistics

Source	Target	Protocol	Distance	Avg Latency	Trace Began	Trace Ended
10.17.17.3:53 (en1: coeus)	216.86.168.1...	TCP	12	93.93	02-Nov-07 18:31:...	02-Nov-07 18:3

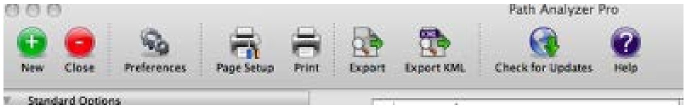
Session Statistics

Source	Target	Protocol	Distance	Avg Latency	Trace Began	Trace Ended
10.17.17.3:53 (en1: coeus)	216.86.168.1...	TCP	12	93.93	02-Nov-07 18:31:...	02-Nov-07 18:3
10.17.17.3:53 (en1: coeus)	216.86.168.1...	TCP	12	90.13	02-Nov-07 18:31:...	02-Nov-07 18:3
10.17.17.3 (en1: coeus)	208.69.32.230	ICMP	13	19.76	02-Nov-07 18:03:...	02-Nov-07 18:0

The Stats tab is similar to the Log feature. It details the current trace under Vital Statistics giving the Source IP address, the Target IP address, the Protocol used for the trace, the number of hops or Distance away the source is from the target, the Average Latency, when the Trace Began, when the Trace Ended and if there were any Filters detected in the path.

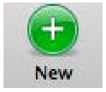
The Session Statistics window shows the past trace details for all traces performed since the program was last opened.

PATH ANALYZER PRO TOOLBAR



The Path Analyzer Pro Toolbar contains your basic features.

NEW

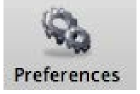


The New icon allows you to open multiple sessions to perform simultaneous traces. Your Operating System (OS) may only allow a certain amount based on your systems level of performance.

CLOSE

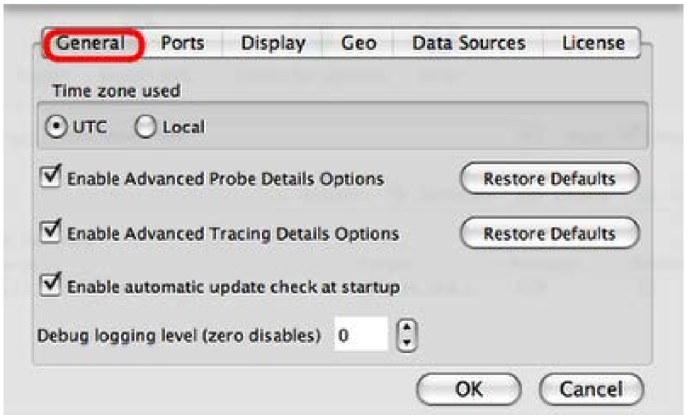
The Close icon closes the current window/session of Path Analyzer Pro.

PREFERENCES



The Preferences icon allows you to customize Path Analyzer Pro to fit your needs. There are six categories in the Preferences section: General, Ports, Display, Geo, Data Sources, and License. You can make changes to one or all of the sections by choosing an option other than the defaults already selected for you and clicking OK when completed.

General



Time zone used

● UTC ○ Local

☑ Enable Advanced Probe Details Options

☑ Enable Advanced Tracing Details Options

☑ Enable automatic update check at startup

Debug logging level (zero disables) 0

The General tab is used to change the Time zone for your trace results. You can choose either Coordinated Universal Time (UTC) or your Local time zone. The default is set to the UTC time zone. This is useful in coordinating information with network service providers or others around the world who may be in different time zones.

The General section allows you to change the left sidebar column that includes the drop-down menus: Standard Options, Advanced Probe Details, and Advanced Tracing Details. Path Analyzer Pro comes with all 3 drop-down menus viewable upon start up. If you are finding that you donÕt use the Advanced Probe Details Options or the Advanced Tracing Details Options then you can simply uncheck the box to hide them. If you decide later you want these options available to you again simply check the box to enable them or click the button Restore Defaults next to each option.

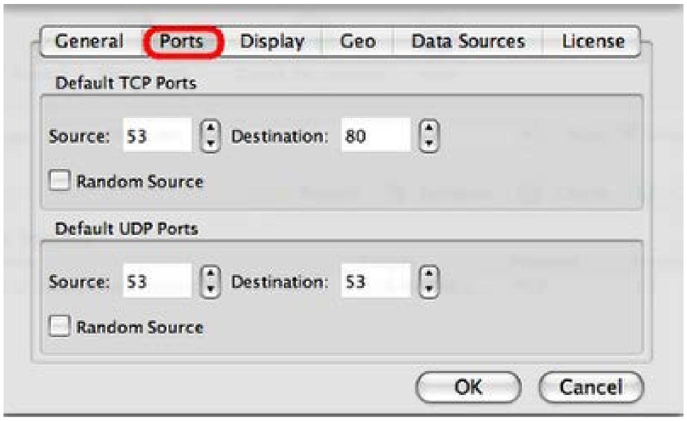
Enable automatic update check at startup- For your convenience, Path Analyzer Pro checks for new software updates each time it is started. If new updates are available you will be informed and given the option of installing them. To disable this feature, simply uncheck this option checkbox.

Debug logging Level (zero disables)- The debugging log level is disabled by default by setting it to zero. This feature is designed solely to support customers -- our technical support staff may ask a user to enable this feature if they are experiencing a problem. When the number is incremented, Path Analyzer Pro will create or append a log file containing detailed information about the programÕs activities.

In Mac OS X, the log will be created in the /Library/Logs directory and will be named ÒpaproyyyyMMdd.logÓ where yyyy is the current year, MM is the current month, and dd is the current day of the month.

In Windows, the log will be created in the current working directory (usually the directory in which the application is installed) and will be named ÒpaproyyyyMMdd.logÓ where yyyy is the current year, MM is the current month, and dd is the current day of the month.

Ports



Default TCP Ports

Source: 53 Destination: 80

□ Random Source

Default UDP Ports

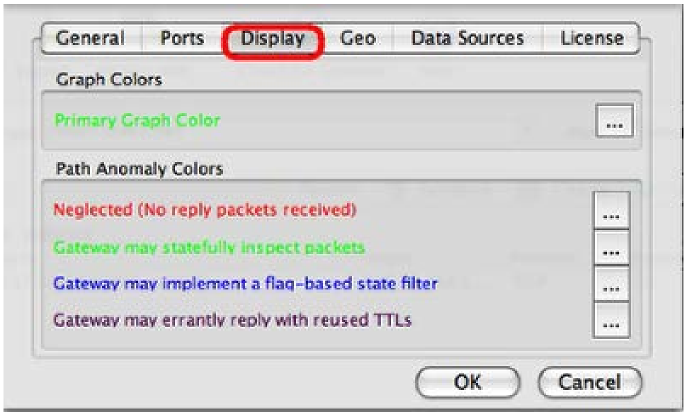
Source: 53 Destination: 53

□ Random Source

Path Analyzer Pro has the unique feature of allowing you to change both the source and destination ports for TCP and UDP traces. The Ports tab allows you to change the source and destination ports for both UDP and TCP traces (ICMP traces do not require a port number). Changing the source port and/or destination port may allow you to get through firewalls to achieve better trace results or to simulate a specific application. For a listing of possible port numbers and the services they commonly involve, please visit www.iana.org.

If you are unfamiliar with port numbers it is recommended that you check the Random Source box to enable the software to choose an appropriate port for you.

Display



Graph Colors

Primary Graph Color

Path Anomaly Colors

Neglected (No reply packets received)

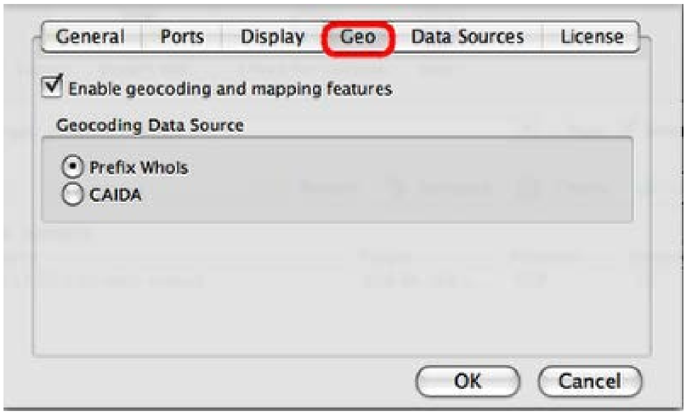
Gateway may statefully inspect packets

Gateway may implement a flag-based state filter

Gateway may errantly reply with reused TTLs

The Display tab allows to change what colors are used to display your chart and path anomaly trace results.

Geo



☑ Enable geocoding and mapping features

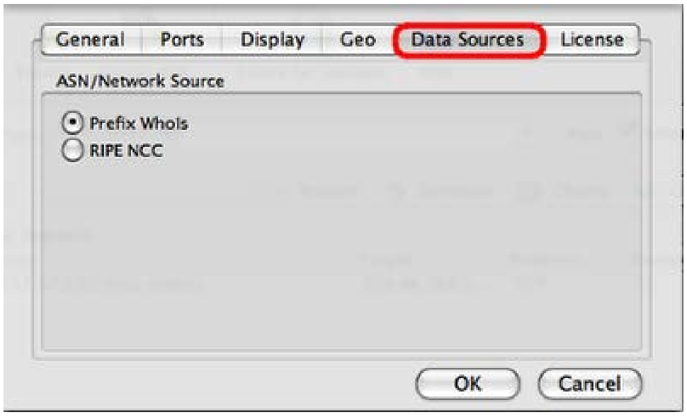
Geocoding Data Source

● Prefix WhoIs
○ CAIDA

The GEO tab allows you to change related to the geocoding and mapping features of the software. By default, geocoding and mapping features are enabled. If you would like to disable the Geocoding and mapping features all together, simply uncheck the box. Disabling these features will significantly reduce the programÕs memory usage and may also increase its overall speed.

Please note: Geocoding data is downloaded from the Internet and is not determined by Path Analyzer Pro. To change the preferred source of Geocoding Data, select either Prefix Whois or CAIDA. It is important to note that neither of these systems is infallible and that it is not possible to be 100% accurate in all cases when determining where an IP address is located. Different organizations providing this data have different algorithms and approaches to estimating geographical positions of IP addresses. We encourage you to research the alternatives and select the one whose processes you agree with the most.

Data Sources

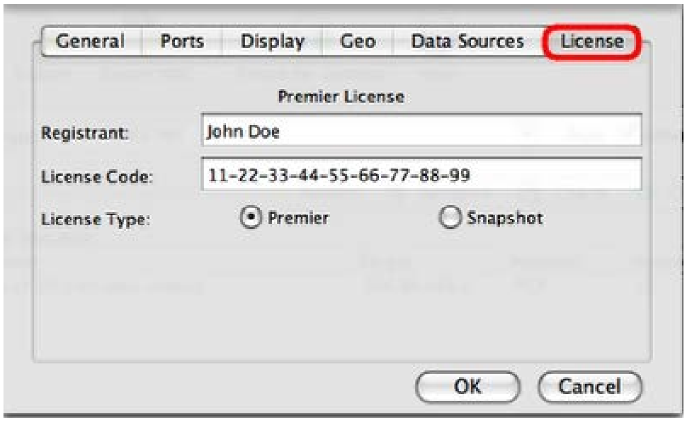


ASN/Network Source

● Prefix WhoIs
○ RIPE NCC

The Data Sources tab allows you to choose which ASN/Network Source or Regional Internet Registries (RIR) you use to obtain your trace data. The registries or whois data aids Path Analyzer Pro in determining who is the network service provider for each IP address along the path to a target. The default is set to obtain this information from Prefix Whois. To change your data source to RIPE (RŽseaux IP EuropŽens) NCC simply select it. We encourage you to research the alternatives and select the one whose processes you agree with the most.

License



Premier License

Registrant: John Doe

License Code: 11-22-33-44-55-66-77-88-99

License Type: ● Premier ○ Snapshot

The License tab holds your license information including: license type, to whom the license is registered, and the license code itself.

PAGE SETUP

Page Setup

The Page Setup button allows you to set up how your data will be printed and select several print options that may be available to you based on your operating system and printer.

PRINT

Print

The Print button allows you to print your trace data. The Print function is context-sensitive which means it is aware of the data/tab you are currently viewing and will perform its action based on your perspective, or on what youÕre currently looking at. Select the trace results from the Report, Synopsis, Charts, Geo, Log, or Stats tabs and then click the Print button to print the corresponding page. Note: You must select a tab to print the trace results within that window. Between the Print function and Page Setup function, you may your print options such as setting the print mode to portrait or landscape to better showcase your charts, etc.

EXPORT

Export

The Export button allows you to export trace results from each of the trace results tabs: Report, Synopsis, Charts, Geo, Log, Stats. The Export function is context-sensitive which means it is aware of the data/tab you are currently viewing and will perform its action based on your perspective, or on what youÕre currently looking at.

The trace results in the Report tab will automatically be exported as a comma-separated values (CSV) file which is great for importing data into your favorite spreadsheet program.

The Synopsis tab exports data as a HTML file viewable in any standard web browser.

The Charts tab exports data as a portable network graphic (PNG) file perfect for dropping into an e-mail or document.

The Geo tab exports data as either a portable network graphic (PNG) containing the map, or as a keyhole markup language (KML) file that can be opened by Google Earth.

The Log tab exports data as a HTML file viewable in any standard web browser.

The Stats tab exports data as a comma-separated values (CSV) file, great for importing data into your favorite spreadsheet program.

EXPORT KML

The Export KML button is a workflow shortcut that exports your trace results to KML and when possible, automatically opens Google Earth for you and imports your trace immediately.

This concludes the Path Analyzer Pro manual. Please visit our FAQ page for additional help using Path Analyzer Pro.

© VOSTROM – Privacy Notice – May 10th 2018, 12:54pm UTC