

Network Protocol Analysis Guide

How to use it?

Step1:

Install Wireshark

[Wireshark • Go Deep](#)

Step2:

Run the program directly

Select TShark program (TShark is the command-line equivalent of the network protocol analyzer Wireshark)

Select the network trace file for which needs to be analyzed

Network Trace Analyzer

File

Help

Select Tshark

C:/Program Files/Wireshark/tshark.exe

tshark

Select Mode

☒ single trace

☐ concurrent traces

Select 1st Trace File

C:/temp/tcpdump.pcap

trace

Select 2nd Trace File

trace

Load/Unload/Analyze

load

unload

analyze

Select IP Addresses

1st trace

2nd trace

IP List

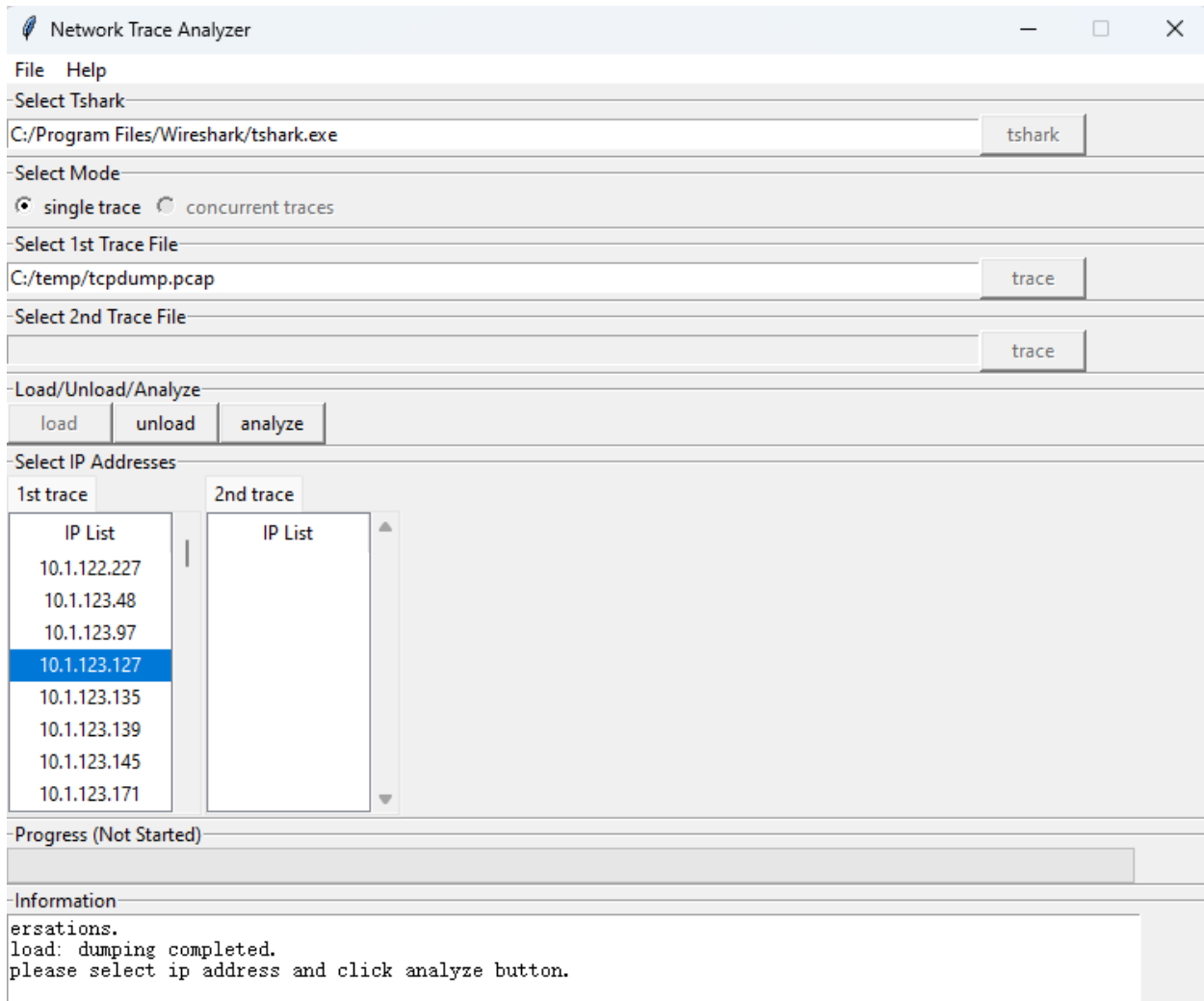
IP List

Progress (Not Started)

Information

Step3:

Click the load button and wait for a while. Loading time may range from several minutes to more than ten minutes. If the network packet file is very large and there are huge number of IP addresses, it may take longer.



Step4:

Select the IP address you want to analyze then click analyze button.

You can select maximum 3 IP addresses (ctrl+select).

Network Trace Analyzer

File

Help

Select Tshark

C:/Program Files/Wireshark/tshark.exe

tshark

Select Mode

☒ single trace
☐ concurrent traces

Select 1st Trace File

C:/temp/tcpdump.pcap

trace

Select 2nd Trace File

trace

Load/Unload/Analyze

load

unload

analyze

Select IP Addresses

1st trace

2nd trace

IP List

10.1.122.227
10.1.123.48
10.1.123.97
10.1.123.127
10.1.123.135
10.1.123.139
10.1.123.145
10.1.123.171

IP List

Progress (Not Started)

Information

versations.

load: dumping completed.

please select ip address and click analyze button.

Step5:

The analysis report file will be generated in the same directory as the network trace file.

<input type="checkbox"/> Name	Date modified	Type	Size
trace_inside_analysis_html_report_175...	2025/9/25 13:01	Microsoft Edge H...	77 KB
tcpdump.pcap	2019/9/6 13:51	Wireshark capture...	195,314 KB