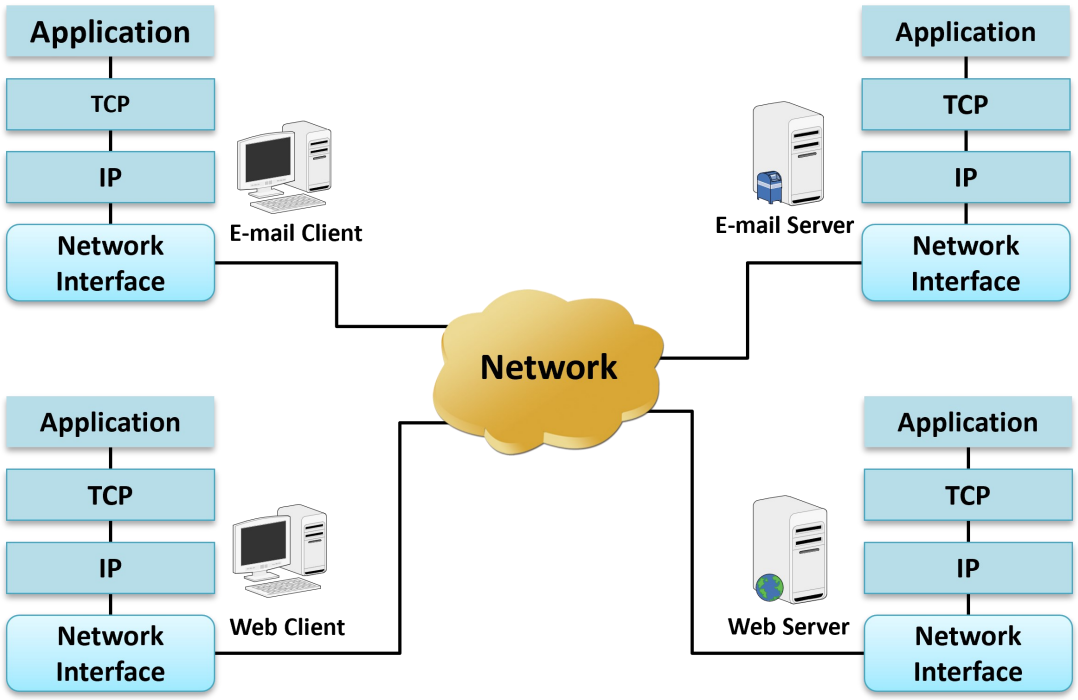
TCP Analytics

(Optimized TCP Record Processing)



Overview

GL's TCP Analytics application analyzes TCP connections between both internal Local Area Network (LAN) and external Wide Area Network (WAN) computers including servers and clients. The application helps troubleshoot large bandwidth consumption, failed TCP sessions, packet loss, poor TCP throughput and more. TCP Analytics (PKV400) is an optional application that is included in the PacketScan™ All IP protocol analysis software.

The core functionality is based on the data structures created by sequential processing of the TCP segments in the offline trace file of the PacketScan™. Due to the requirement to process huge trace files with billions of records the TCP Analytics is not based on the protocol decode functions but rather on the optimized fast TCP record processing.

These data structures need to be created once when the offline trace file is opened and are used to produce derivatives analytics. When offline file is closed the data structures are destroyed releasing memory resources.

PacketScan™ offline user interface is used to create base data structures for TCP connection analysis from an offline trace file containing captured frames or importing Wireshark packet captures. These data structures could be huge if the captured data files are hundreds of gigabytes or even many terabytes (1OE+12) in size. The proper configuration of computer's virtual memory is required to handle this data and is accomplished with the TCP Analytics program.

For more details, refer to TCP Analytics webpage.

GL Communications Inc.

818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878, U.S.A

(Web) www.gl.com - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) info@gl.com

Main Features

- Analyze TCP connections between internal company LAN connected computers and outside computers on the WAN
- Analyze TCP connections of a particular client server pair
- Analyze TCP connections on a subset of a LAN
- Display top level statistics
- Use PacketScan™ to display packets that belong to a selected TCP connection
- Export information to CSV files for subsequent Excel or a database import
- Sort tabular information by column values

TCP Analytics GUI (TAG) IPv4 Dashboard

The TAG dashboard includes a menu to invoke detailed TCP IPv4 connection information and summary overview of TCP connections in the currently opened and processed trace file. The window is resizable to adjust column width. Columns can be sorted by clicking on the column header.

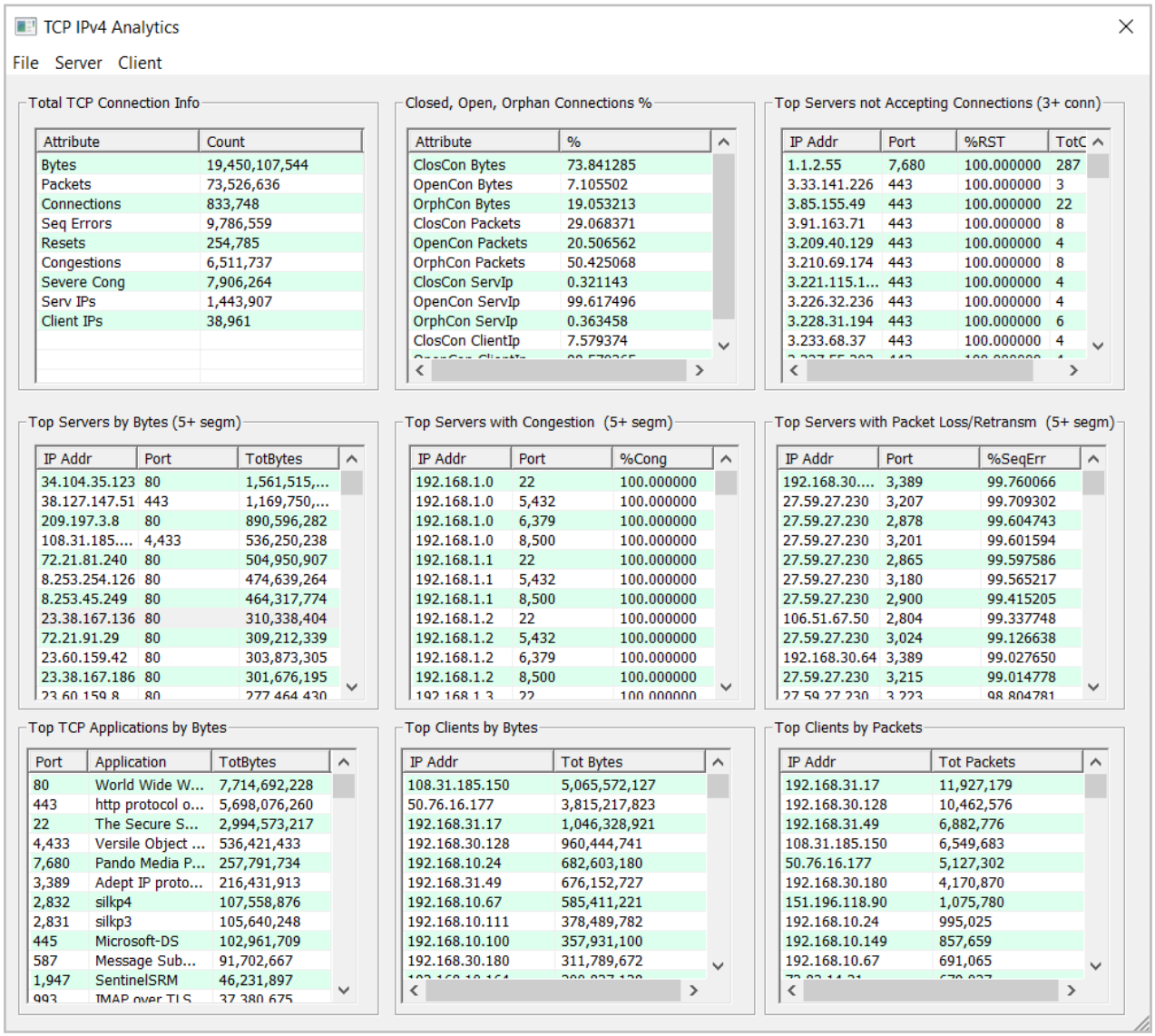


Figure: TAG IPv4 Dashboard

Sorting Columns

Sort columns in an ascending or descending order.

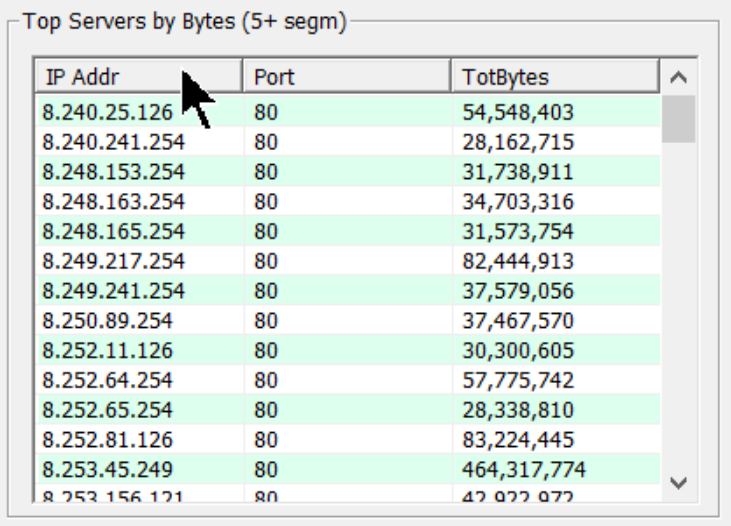


Figure: Sorting Columns

Total TCP Connection Information

- Seq Errors for TCP Sequence Number field errors indicate missing, duplicate or out of order packets
- Resets are connections with RST flags usually indicates refused connections by servers etc.
- Congestions indicate reduced window size due to congestions (indication of the receiving side to slow down transmission on the other end)
- Severe Cong indicates 0 window size in the TCP header when receiving size cannot accept ANY TCP packets for the connection
- Serv IPs, Client IPs just counts the unique IPv4 addresses for servers and clients

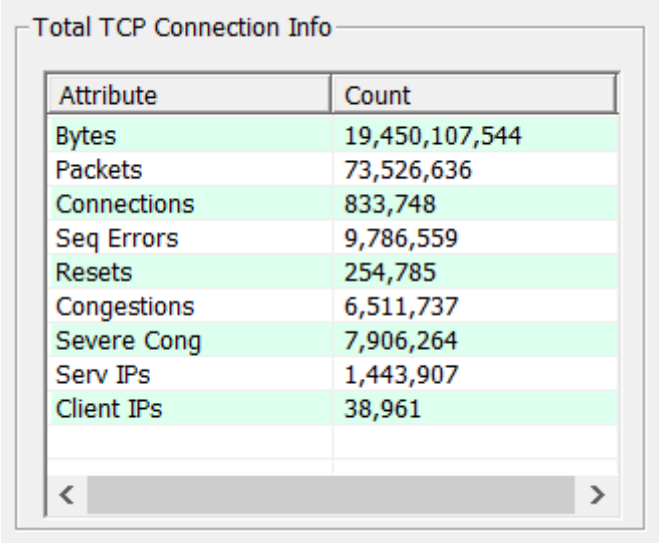


Figure: Total TCP Connection Information

Distribution in Percentage Among Closed, Open and Orphan Connections

Display Closed, Open, and Orphan connections in percentage.

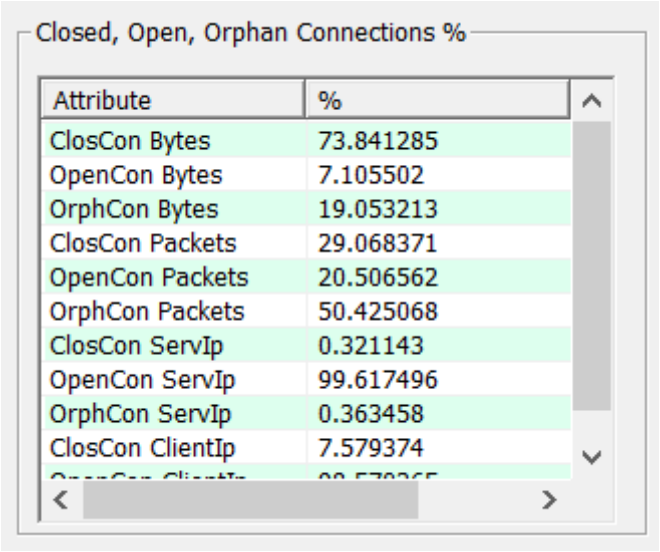


Figure: Closed, Open, and Orphan Connections

Top Servers Rejecting Client Connections

- IP Addr and Port columns display server IP address and TCP port number
- %RST (resets) is the percentage of connections being rejected. This list includes only servers with total of 3 or more connections to avoid noise
- TotCon is the total number of connections to the server addr/port pair

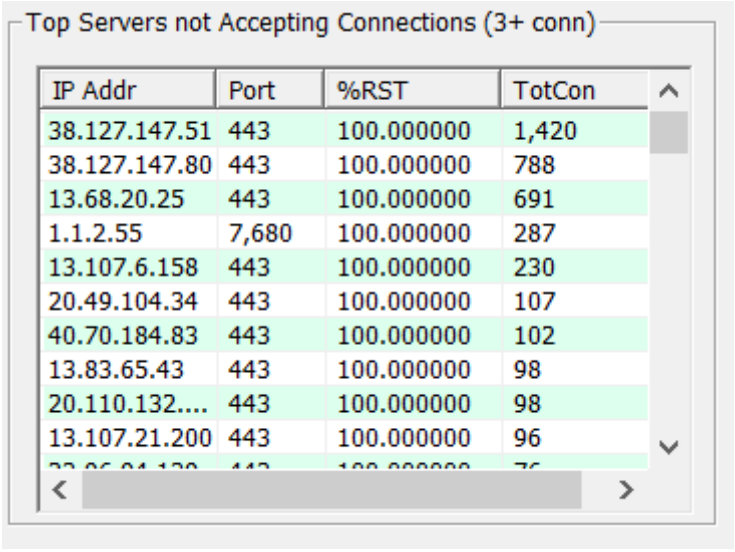


Figure: Top Servers Rejecting Client Connections

Top Servers by Bytes Transferred

Information is collected only for connections with 5 or more segments for a connection. Each line is a total for all connections for a particular server TCP application with unique IP address and TCP port.

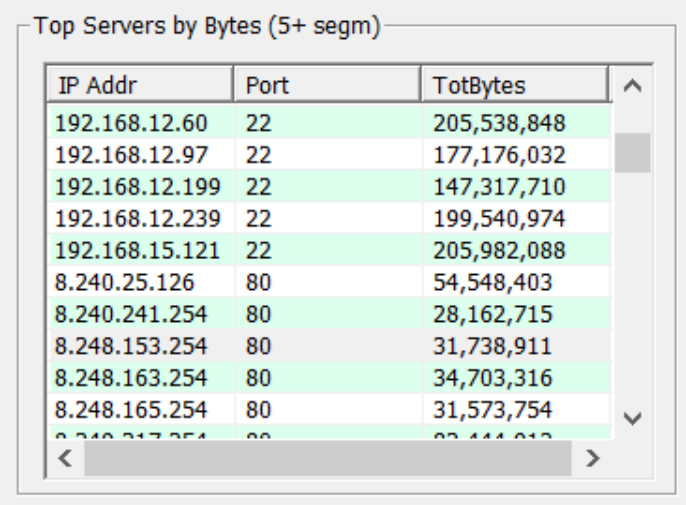


Figure: Top Servers by Bytes Transferred

Top Servers with Reduced Windows Size (Congested)

Includes connection with at least 5 segments (packets) and is showing servers with the largest percentage of packets with reduced window size.

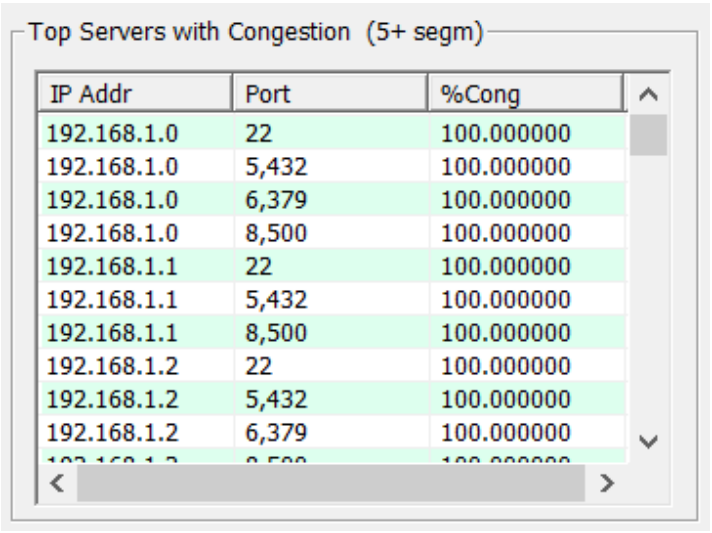
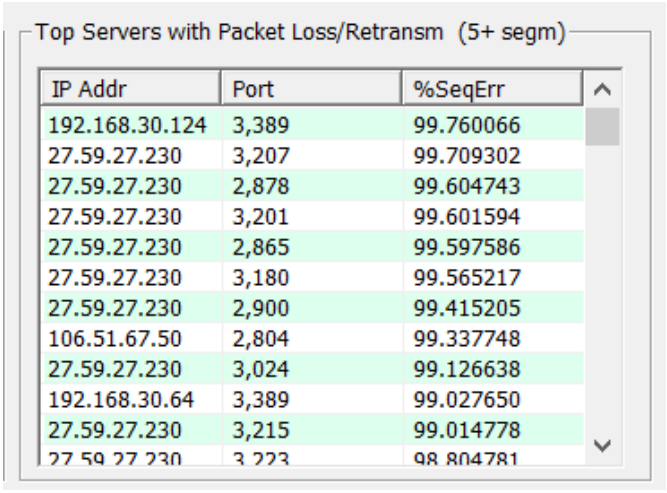


Figure: Top Servers with Reduced Window Size

Top Servers with Largest Percentage of Sequence Errors (Packet Loss/Retransmission)

Indicates the most affected servers by percentage of TCP segments with sequence number errors caused by missed packets, packets retransmission and reordering etc.

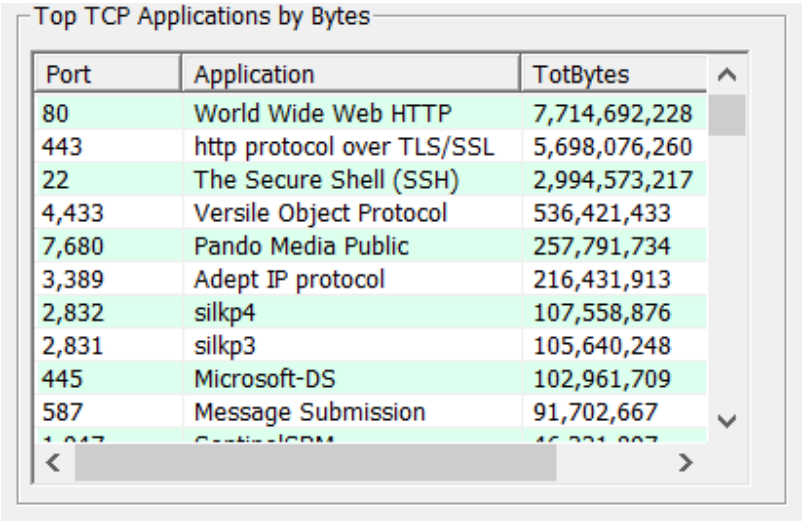


IP Addr	Port	%SeqErr
192.168.30.124	3,389	99.760066
27.59.27.230	3,207	99.709302
27.59.27.230	2,878	99.604743
27.59.27.230	3,201	99.601594
27.59.27.230	2,865	99.597586
27.59.27.230	3,180	99.565217
27.59.27.230	2,900	99.415205
106.51.67.50	2,804	99.337748
27.59.27.230	3,024	99.126638
192.168.30.64	3,389	99.027650
27.59.27.230	3,215	99.014778
27.59.27.230	3,223	98.804781

Figure: Top Servers with Packet Loss or Retransmission

Top TCP Applications by Received Bytes

Total bytes are the sum of all bytes for all connections to all IP addresses with particular TCP port number.

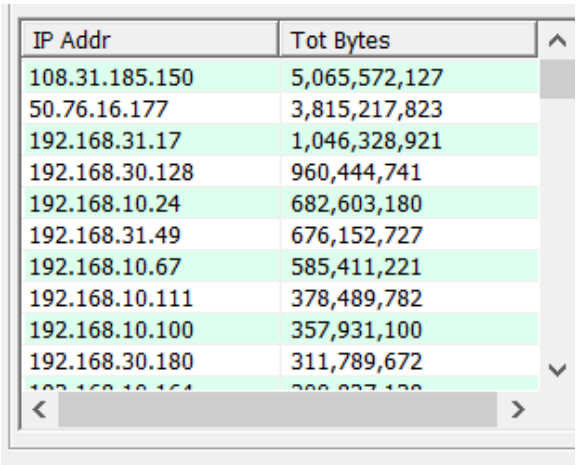


Port	Application	TotBytes
80	World Wide Web HTTP	7,714,692,228
443	http protocol over TLS/SSL	5,698,076,260
22	The Secure Shell (SSH)	2,994,573,217
4,433	Versile Object Protocol	536,421,433
7,680	Pando Media Public	257,791,734
3,389	Adept IP protocol	216,431,913
2,832	silkp4	107,558,876
2,831	silkp3	105,640,248
445	Microsoft-DS	102,961,709
587	Message Submission	91,702,667

Figure: Top TCP Applications by Received Bytes

Top Client IP Addresses by Bytes for all Client TCP Connections

- Used to diagnose computers that cause the network congestions
- These are the clients that transmit or receive largest amount of data
- This is a total for all connections and all TCP applications per client

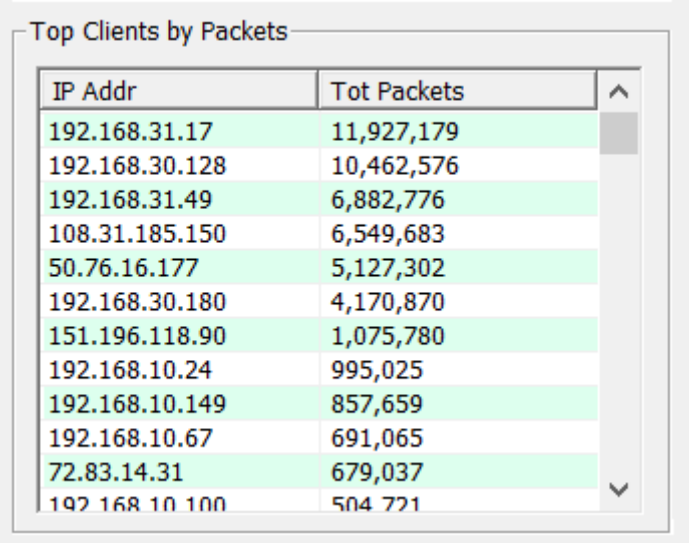


IP Addr	Tot Bytes
108.31.185.150	5,065,572,127
50.76.16.177	3,815,217,823
192.168.31.17	1,046,328,921
192.168.30.128	960,444,741
192.168.10.24	682,603,180
192.168.31.49	676,152,727
192.168.10.67	585,411,221
192.168.10.111	378,489,782
192.168.10.100	357,931,100
192.168.30.180	311,789,672

Figure: Top Client IP Address by Bytes for all Client TCP Connections

Top Client IP Addresses by Packets for all Client TCP Connections

- Total for all connections and all TCP applications per client
- Used to diagnose computers that cause the network congestions and potential viruses or wiring and Hardware malfunctions
- These are the clients that transmit or receive largest number of packets



Top Clients by Packets

IP Addr	Tot Packets
192.168.31.17	11,927,179
192.168.30.128	10,462,576
192.168.31.49	6,882,776
108.31.185.150	6,549,683
50.76.16.177	5,127,302
192.168.30.180	4,170,870
151.196.118.90	1,075,780
192.168.10.24	995,025
192.168.10.149	857,659
192.168.10.67	691,065
72.83.14.31	679,037

Figure: Top Client IP Address by Packets for all Client TCP Connections

TAG IPv6 Dashboard

The TAG dashboard includes a menu to invoke detailed TCP IPv6 connection information and summary overview of TCP connections in the currently opened and processed trace file. The window is resizable to adjust column width. Columns can be sorted by clicking on the column header .

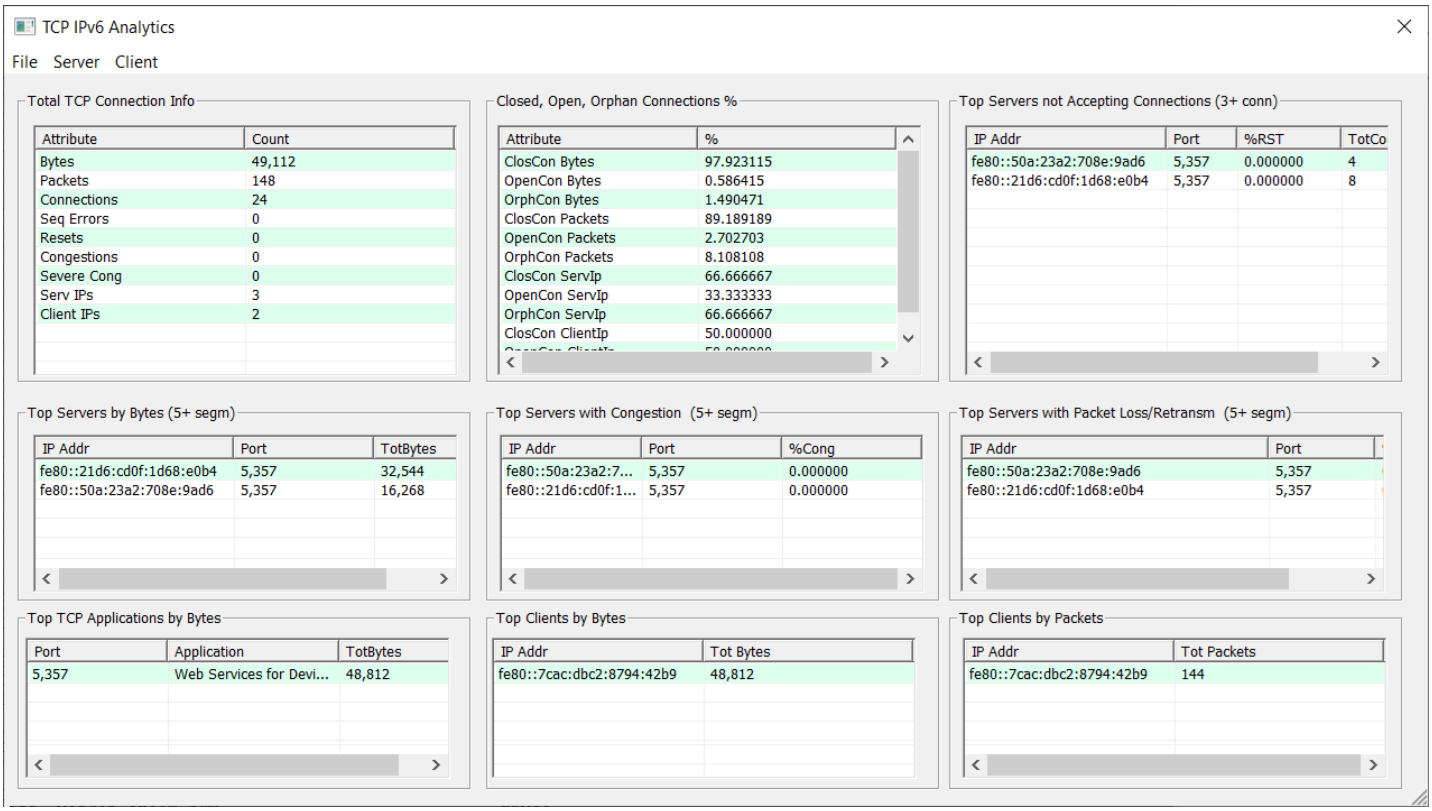


Figure: TAG IPv6 Dashboard

Buyer's Guide

Item No	Product Description
PKV400	TCP Analytics (Optional with PacketScan™)

Item No	Related Software
PKV100	PacketScan™ - (Online and Offline)
PKV101	Offline PacketScan™

Item No	Related Hardware
PKV120	PacketScan™ HD High Density IP Traffic Analyzer

For more details, refer to TCP Analytics webpage.

GL Communications Inc.
818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878, U.S.A
(Web) www.gl.com - (V) +1-301-670-4784 (F) +1-301-670-9187 - (E-Mail) info@gl.com