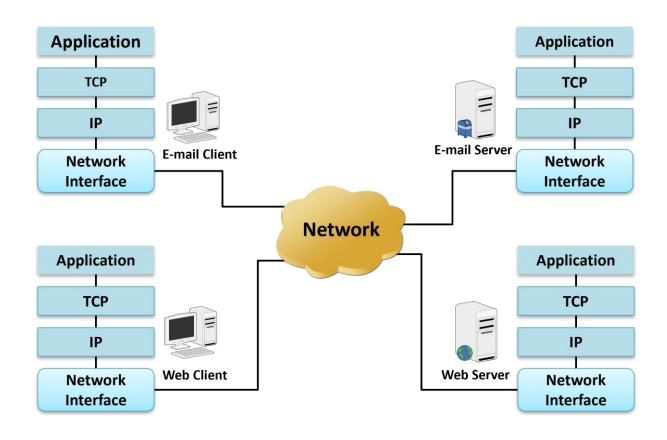# TCP Analytics

Optimized Fast TCP Record Processing

TCP Analytics Network

- The TCP Analytics application analyzes TCP connections between both internal Local Area Network (LAN) and external Wide Area Network (WAN) computers including servers and clients
- Helps troubleshoot large bandwidth consumption, failed TCP sessions, packet loss, poor TCP throughput and more
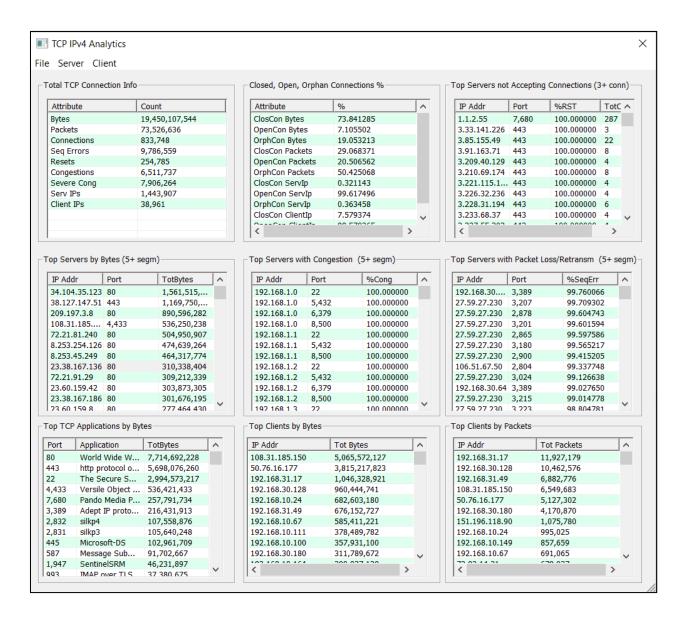
Main Features

- 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
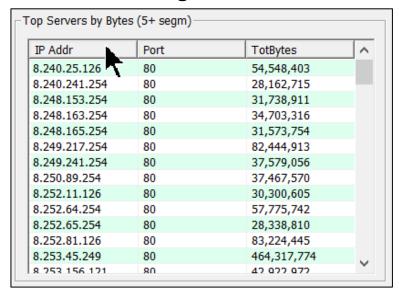
TCP Analytics GUI (TAG) IPv4 Dashboard

- 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

Sorting Columns and TCP Connection Information

Sorting Columns

Top Servers by Bytes (5+ segm)

IP Addr	Port	TotBytes
8.240.25.126	80	54,548,403
8.240.241.254	80	28,162,715
8.248.153.254	80	31,738,911
8.248.163.254	80	34,703,316
8.248.165.254	80	31,573,754
8.249.217.254	80	82,444,913
8.249.241.254	80	37,579,056
8.250.89.254	80	37,467,570
8.252.11.126	80	30,300,605
8.252.64.254	80	57,775,742
8.252.65.254	80	28,338,810
8.252.81.126	80	83,224,445
8.253.45.249	80	464,317,774
8.253.156.121	80	42,922,972

Total TCP Connection Information

Total TCP Connection Info

Attribute	Count
Bytes	19,450,107,544
Packets	73,526,636
Connections	833,748
Seq Errors	9,786,559
Resets	254,785
Congestions	6,511,737
Severe Cong	7,906,264
Serv IPs	1,443,907
Client IPs	38,961

Connection Distribution in Percentage and Rejection of Client Connections

Distribution in Percentage Among Closed, Open and Orphan Connections

Closed, Open, Orphan Connections %
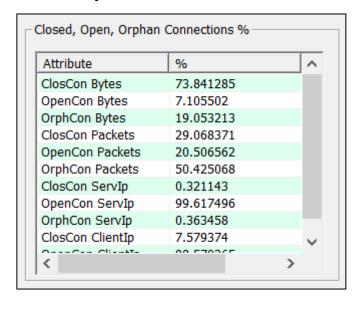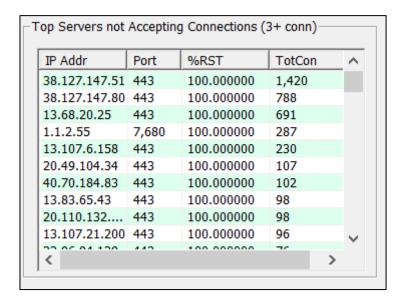
Attribute	%
ClosCon Bytes	73.841285
OpenCon Bytes	7.105502
OrphCon Bytes	19.053213
ClosCon Packets	29.068371
OpenCon Packets	20.506562
OrphCon Packets	50.425068
ClosCon ServIp	0.321143
OpenCon ServIp	99.617496
OrphCon ServIp	0.363458
ClosCon ClientIp	7.579374
OpenCon ClientIp	98.570265

Top Servers Rejecting Client Connections

Top Servers not Accepting Connections (3+ conn)

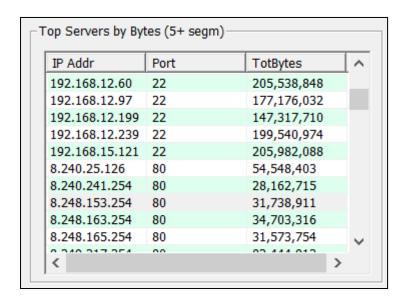| IP Addr	Port	%RST	TotCon
38.127.147.51	443	100.000000	1,420
38.127.147.80	443	100.000000	788
13.68.20.25	443	100.000000	691
1.1.2.55	7,680	100.000000	287
13.107.6.158	443	100.000000	230
20.49.104.34	443	100.000000	107
40.70.184.83	443	100.000000	102
13.83.65.43	443	100.000000	98
20.110.132....	443	100.000000	98
13.107.21.200	443	100.000000	96
	443	100.000000	76

GL Communications

Top Servers by Bytes Transferred and with Reduced Windows Size

Top Servers by Bytes Transferred

Top Servers by Bytes (5+ segm)

IP Addr	Port	TotBytes
192.168.12.60	22	205,538,848
192.168.12.97	22	177,176,032
192.168.12.199	22	147,317,710
192.168.12.239	22	199,540,974
192.168.15.121	22	205,982,088
8.240.25.126	80	54,548,403
8.240.241.254	80	28,162,715
8.248.153.254	80	31,738,911
8.248.163.254	80	34,703,316
8.248.165.254	80	31,573,754

Top Servers with Reduced Windows Size (Congested)

Top Servers with Congestion (5+ segm)

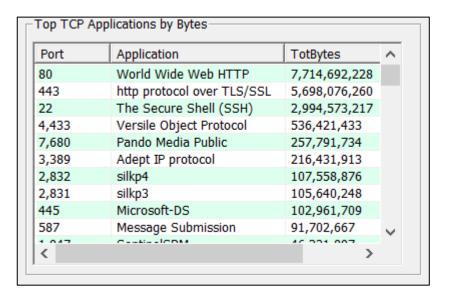| IP Addr	Port	%Cong
192.168.1.0	22	100.000000
192.168.1.0	5,432	100.000000
192.168.1.0	6,379	100.000000
192.168.1.0	8,500	100.000000
192.168.1.1	22	100.000000
192.168.1.1	5,432	100.000000
192.168.1.1	8,500	100.000000
192.168.1.2	22	100.000000
192.168.1.2	5,432	100.000000
192.168.1.2	6,379	100.000000

Top Servers with Packet Loss and Top TCP Applications by Bytes

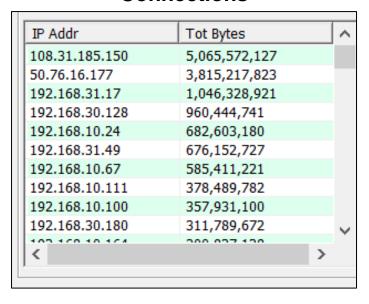**Top Servers with Percentage of Sequence Errors
(Packet Loss/Retransmission)**
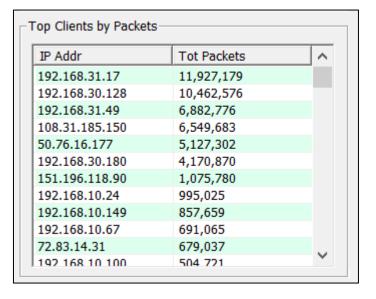
Top TCP Applications by Received Bytes

Top Servers with Packet Loss/Retransm (5+ segm)

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

Top TCP Applications by Bytes

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

Top Client IP Addresses by Bytes and Packets for all Client TCP Connections

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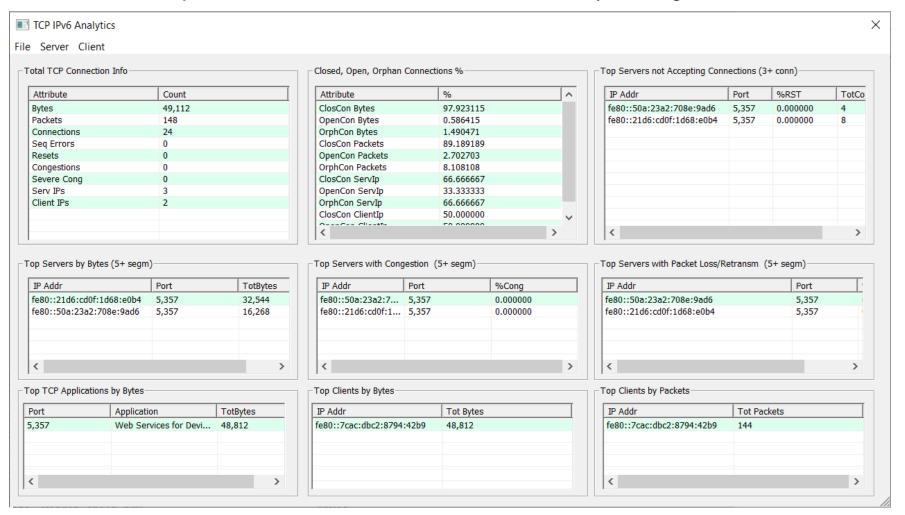
IP Addr	Tot Bytes
108.31.185.150	5,065,572,127
50.76.16.177	3,815,217,823
192.168.31.17	1,046,328,921
192.168.30.128	960,444,741
192.168.10.24	682,603,180
192.168.31.49	676,152,727
192.168.10.67	585,411,221
192.168.10.111	378,489,782
192.168.10.100	357,931,100
192.168.30.180	311,789,672

Top Client IP Addresses by Packets for all Client TCP Connections

Top Clients by Packets

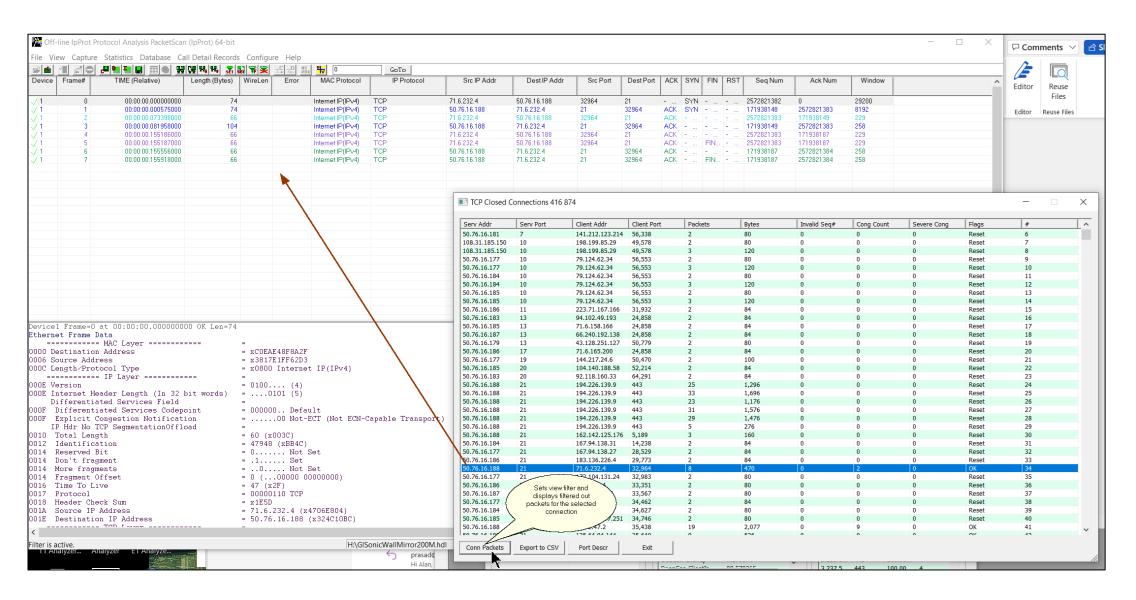| IP Addr	Tot Packets
192.168.31.17	11,927,179
192.168.30.128	10,462,576
192.168.31.49	6,882,776
108.31.185.150	6,549,683
50.76.16.177	5,127,302
192.168.30.180	4,170,870
151.196.118.90	1,075,780
192.168.10.24	995,025
192.168.10.149	857,659
192.168.10.67	691,065
72.83.14.31	679,037
192.168.10.100	504,721

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.

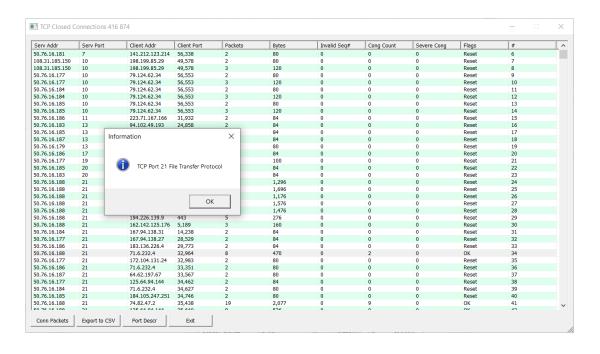- The window is resizable to adjust column width. Columns can be sorted by clicking on the column header.
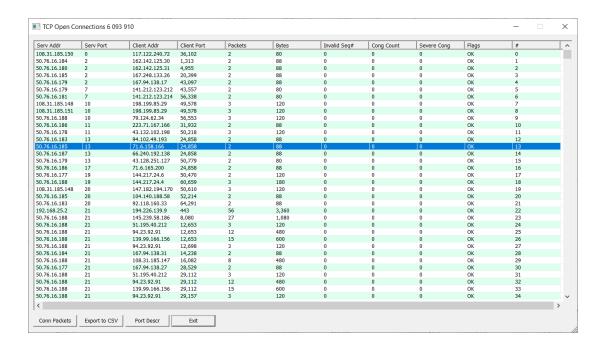
TCP Connections Information

TCP Closed and Open Connections

TCP Closed Connections

TCP Open Connections

TCP Orphan Connections

Serv Addr	Serv Port	Client Addr	Client Port	Packets	#
108.31.185.150	10	198.199.85.29	49,578	2	0
50.76.16.177	10	79.124.62.34	56,553	2	1
50.76.16.184	10	79.124.62.34	56,553	2	2
50.76.16.185	10	79.124.62.34	56,553	2	3
50.76.16.188	21	71.6.232.4	32,964	1	4
50.76.16.188	21	74.82.47.2	35,438	3	5
50.76.16.188	21	125.64.94.144	35,640	2	6
50.76.16.188	21	192.241.212.117	38,958	1	7
50.76.16.188	21	167.248.133.44	38,960	1	8
50.76.16.188	21	172.104.131.24	41,352	7	9
50.76.16.186	21	221.2.163.231	46,378	2	10
108.31.185.150	21	221.2.163.231	46,378	2	11
50.76.16.188	21	130.211.54.158	55,070	1	12
50.76.16.188	21	130.211.54.158	55,334	1	13
50.76.16.179	21	34.116.115.71	56,015	2	14
50.76.16.180	21	34.116.115.71	56,015	2	15
50.76.16.181	21	34.116.115.71	56,015	2	16
50.76.16.183	21	34.116.115.71	56,015	2	17
50.76.16.184	21	34.116.115.71	56,015	2	18
50.76.16.185	21	34.116.115.71	56,015	2	19
50.76.16.188	21	34.116.115.71	56,015	3	20
50.76.16.177	21	156.232.7.218	57,603	2	21
50.76.16.179	21	156.232.7.218	57,603	2	22
50.76.16.180	21	156.232.7.218	57,603	2	23
50.76.16.181	21	156.232.7.218	57,603	2	24
50.76.16.182	21	156.232.7.218	57,603	2	25
50.76.16.183	21	156.232.7.218	57,603	2	26
50.76.16.184	21	156.232.7.218	57,603	2	27
50.76.16.185	21	156.232.7.218	57,603	2	28
50.76.16.186	21	156.232.7.218	57,603	2	29
50.76.16.187	21	156.232.7.218	57,603	2	30
50.76.16.188	21	156.232.7.218	57,603	3	31
138.99.6.173	22	50.76.16.179	8,415	4	32
23.227.146.106	22	108.31.185.150	9,107	3	33
50.76.16.188	22	185.220.102.253	12,152	1	34

TCP Orphan Connections 1 128 096

Conn Packets   Export to CSV   Port Descr   Exit

Thank You