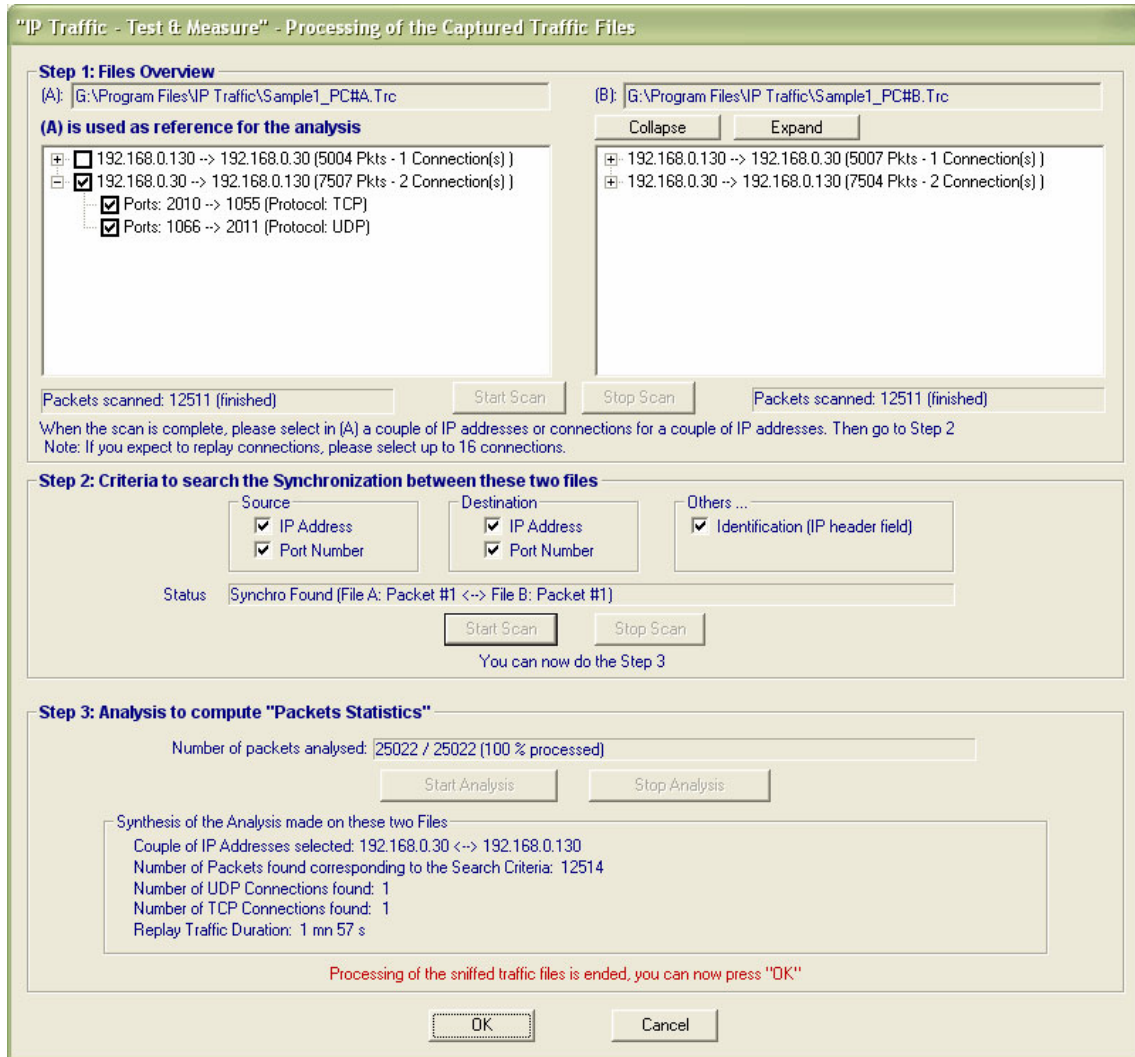


IP Traffic Test & Measure

Analysis of a Captured File



"IP Traffic - Test & Measure" - Processing of the Captured Traffic Files

Step 1: Files Overview

(A): G:\Program Files\IP Traffic\Sample1_PC#A.Trc
 (B): G:\Program Files\IP Traffic\Sample1_PC#B.Trc

(A) is used as reference for the analysis

192.168.0.130 -> 192.168.0.30 (5004 Pkts - 1 Connection(s))
 192.168.0.30 -> 192.168.0.130 (7507 Pkts - 2 Connection(s))
 Ports: 2010 -> 1055 (Protocol: TCP)
 Ports: 1066 -> 2011 (Protocol: UDP)

Packets scanned: 12511 (finished) Start Scan Stop Scan Packets scanned: 12511 (finished)

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2
 Note: If you expect to replay connections, please select up to 16 connections.

Step 2: Criteria to search the Synchronization between these two files

Source: IP Address, Port Number
 Destination: IP Address, Port Number
 Others ...: Identification (IP header field)

Status: Synchro Found (File A: Packet #1 <-> File B: Packet #1)

Start Scan Stop Scan

You can now do the Step 3

Step 3: Analysis to compute "Packets Statistics"

Number of packets analysed: 25022 / 25022 (100 % processed)

Start Analysis Stop Analysis

Synthesis of the Analysis made on these two Files:
 Couple of IP Addresses selected: 192.168.0.30 <-> 192.168.0.130
 Number of Packets found corresponding to the Search Criteria: 12514
 Number of UDP Connections found: 1
 Number of TCP Connections found: 1
 Replay Traffic Duration: 1 mn 57 s

Processing of the sniffed traffic files is ended, you can now press "OK"

OK Cancel

- In the Step 1, IP addresses 192.168.0.30 → 192.168.0.130 are selected.
- In step 2, the synchronization criteria are set.
- After running step 3, the synthesis is displayed showing 1 TCP and 1 UDP connection.
- By using the "Packet Statistics" option, the results shown overleaf are displayed.



IP Traffic Test & Measure

Analysis of a Captured File

Offline Packet Statistics

Computer A ==> Computer B Save ... Computer B ==> Computer A

IP address of A: 192.168.0.30 IP address of B: 192.168.0.130

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...	Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...
22:00:43.428	Sent	...	2010->1...	48 (TCP)	xD013	22:00:43.420	Sent	...	1055->2...	48 (TCP)	x6441
PC 22:00:43.451	Sent	0 (?)	2010->1...	40 (TCP)	xD014	PC 22:00:43.420	Sent	0 (?)	1055->2...	40 (TCP)	x6442
PC 22:00:43.490	Sent	0 (?)	2010->1...	40 (TCP)	xD015	PC 22:00:43.423	Sent	1 (?)	1055->2...	1500 (TCP)	x6443
PC 22:00:43.530	Sent	0 (?)	2010->1...	40 (TCP)	xD016	PC 22:00:43.442	Sent	1 (?)	1055->2...	1500 (TCP)	x6444
PC 22:00:43.570	Sent	0 (?)	2010->1...	40 (TCP)	xD017	PC 22:00:43.462	Sent	1 (?)	1055->2...	1500 (TCP)	x6445
PC 22:00:43.611	Sent	0 (?)	2010->1...	40 (TCP)	xD018	PC 22:00:43.481	Sent	1 (?)	1055->2...	1500 (TCP)	x6446
PC 22:00:43.651	Sent	0 (?)	2010->1...	40 (TCP)	xD019	PC 22:00:43.501	Sent	1 (?)	1055->2...	1500 (TCP)	x6447
PC 22:00:43.691	Sent	0 (?)	2010->1...	40 (TCP)	xD01A	PC 22:00:43.521	Sent	1 (?)	1055->2...	1500 (TCP)	x6448
PC 22:00:43.731	Sent	0 (?)	2010->1...	40 (TCP)	xD01B	PC 22:00:43.541	Sent	1 (?)	1055->2...	1500 (TCP)	x6449
PC 22:00:43.771	Sent	0 (?)	2010->1...	40 (TCP)	xD01C	PC 22:00:43.561	Sent	1 (?)	1055->2...	1500 (TCP)	x644A
PC 22:00:43.810	Sent	0 (?)	2010->1...	40 (TCP)	xD01D	PC 22:00:43.582	Sent	1 (?)	1055->2...	1500 (TCP)	x644B
PC 22:00:43.850	Sent	0 (?)	2010->1...	40 (TCP)	xD01E	PC 22:00:43.602	Sent	2 (?)	1055->2...	1500 (TCP)	x644C
PC 22:00:43.890	Sent	0 (?)	2010->1...	40 (TCP)	xD01F	PC 22:00:43.622	Sent	1 (?)	1055->2...	1500 (TCP)	x644D

Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter	Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer A	7507	3	0%	120 ms	1 ms	Total Computer B	5007	3	0%	8 ms	0 ms
1066 -> 2011 (UDP)	5000	3	0%	178 ms	1 ms	1055 -> 2010 (TCP)	5007	3	0%	8 ms	0 ms
2010 -> 1055 (TCP)	2507	0	0%	6 ms	0 ms						

In this example, 3 UDP packets have been lost and the transit delay has an average of 178 ms for the UDP connection. 3 TCP packets sent by PC #B have been lost and the average transit delay is 7 ms.

