Use the Power of the Mainframe to Turn Packet Traces into English

Nalini Elkins

Inside Products, Inc.

Inside Products, Inc.

sales@insidethestack.com

(831) 659-8360

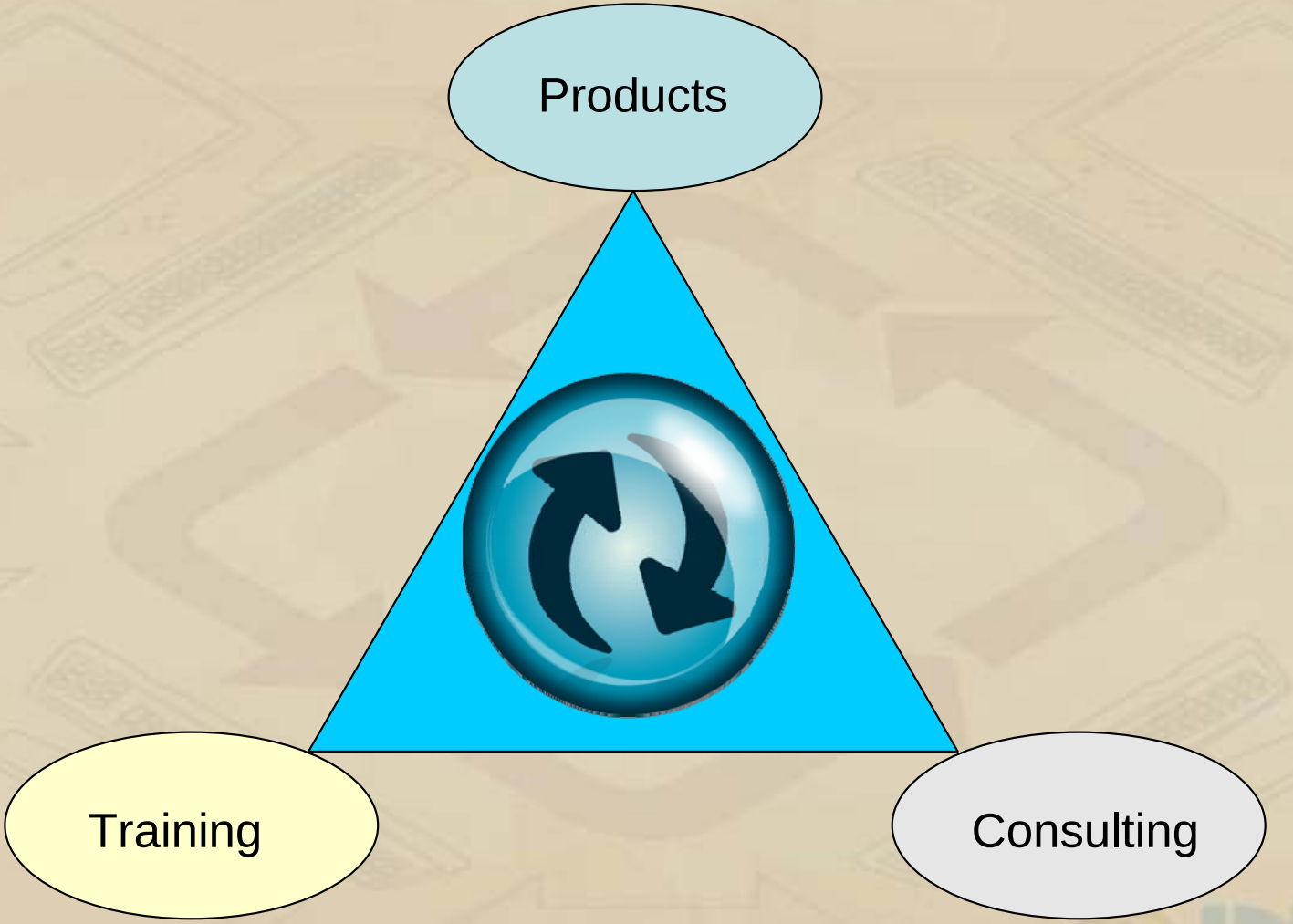
Inside Products

- z/OS Monitoring Products:
  - Inside the Stack
  - Early Warning System
  - Availability Checker
  - Application Checker
  - Connection Log
  - Trace Agent
- Analysis products:
  - IP Problem Finder DB2
  - IPv6 Problem Finder
  - TCP Response Time Monitor
  - SSL Problem Finder
  - EE Problem Finder

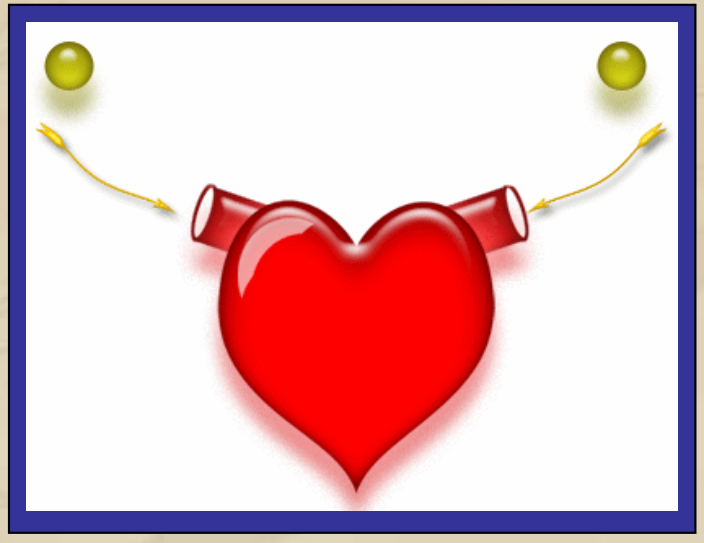
- Consulting Services
  - Network Health Check
  - Network Performance Check
  - System and Network Tuning
  - EE Health Check
  - IPv6 Migration Services

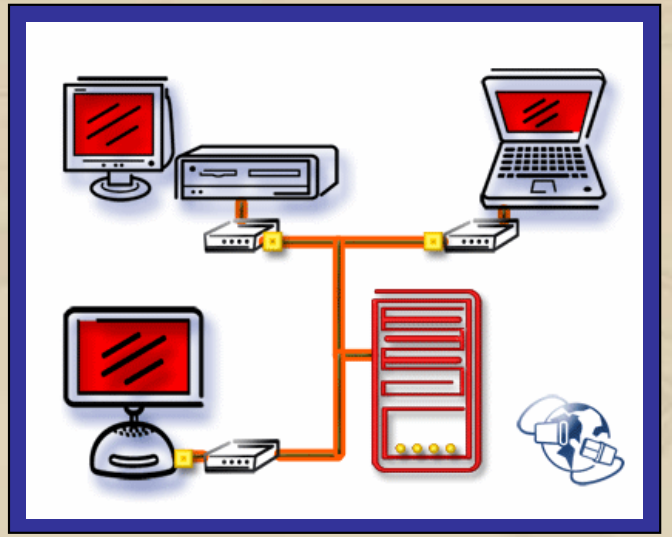
- Classes
  - TCP Tuning and Performance
  - Trace Analysis and Diagnostics (TCP; IPv6: SSL; EE)
  - Security (IPSec, SSL)
  - IPv6 (Addressing, Migration)

Our Philosophy



Tuning and Troubleshooting





- Just as the arteries of the heart can become clogged, so can the network.
- **Inside Products** points you to the areas of TCP/IP which need tuning.
- Problems such as: low throughput, poor response time, network overhead, excessive server CPU usage

What happens today…

Some typical situations:

- FTPs are slow
- An application has poor throughput
- A connection to a needed service keeps dropping

Then…

- The affected department calls meetings.
- Everyone says “It's not my fault!”
- Your manager says, “Joe, take a trace and have the answer back to me by tomorrow.”

You…

- Make arrangements for testing
- And end up with a million packet trace

- Which you have to read and decode.
- Everyone is looking over your shoulder asking you if you have the answer yet.

TCP Problem Finder to the Rescue

- Let us help you.

- How?

- Feed the trace into the TCP Problem Finder.
- Let it pinpoint the possible sections and devices which may have problems.
- TCP PF has years and years of network expertise built in. We add to it every day.

- Diagnostics on TCP networks is what we do.
- Diagnostics on TCP networks is all we do.

How to do this?

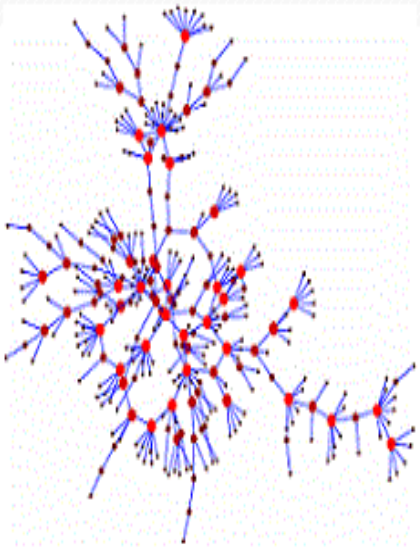
- First, let’s see what packet ranges and devices may have problems.
- TCP Problem Finder will guide you through the analysis.
- In network issues, problems tend to cluster -- either to a time frame or to a set of devices.
- Let’s find them. First, the overview:

IP PROBLEM FINDER

Show Trace Analysis
Trace File: sample17

INSIDE PRODUCTS
Thinking Inside the Box

»Trace Analysis



The trace you have selected has been imported into the product. The packets have been sorted according to the protocol (TCP, UDP, ICMP, SSL, IPv4 or IPv6.).
The import has also looked for any errors or problems in the traffic. Here you will see the packets and devices where there are most likely to be problems. If you wish, you may drill down and analyze these in more detail.

The total number of trace packets loaded in is: 500,223.

»Packet ranges with problems

It is quite likely that the problems in the trace are in the packet ranges below:

Trace ID : 3
Starting Packet ID : 500
Ending Packet ID : 749
*
Total Resets: 0
Total Out Of Order: 6
Total Delayed ACK: 0
Total Retransmit: 5
Total Zero Window: 0
Total Small Window: 0
Total Window Update Low : 0
Total Window Update High: 0
*

Trace ID : 3
Starting Packet ID : 750
Ending Packet ID : 999
*
Total Resets: 0
Total Out Of Order: 3
Total Delayed ACK: 1
Total Retransmit: 3
Total Zero Window: 0
Total Small Window: 0
Total Window Update Low : 3
Total Window Update High: 0
*

DoDetailedAnalysis

»Connections with problems

It is quite likely that the problems in the trace are with the connections below:

TraceID : 3
From Address: 10.173.12.5
To Address : 67.217.66.244
From Port : 4750
To Port : 443
Protocol : 2
BytesIntF#1 : 0
BytesIntF#2 : 0
Total Resets: 0
Total Out Of Order: 0
Total Delayed ACK: 0
Total Retransmit: 0
Total Zero Window: 1
Total Small Window: 1
Total Window Update Low : 0
Total Window Update High: 0
*

TraceID : 3
From Address: 10.197.4.1
To Address : 10.173.12.5
From Port : 58315
To Port : 4726
Protocol : 2
BytesIntF#1 : 287872
BytesIntF#2 : 0
Total Resets: 0
Total Out Of Order: 9
Total Delayed ACK: 0

Then, do a detailed analysis

- Now, is the fun part!
- TCP Problem Finder provides detailed analysis, recommendations, and guidance, guidance, guidance.

What Happened?

Drill Down	Total Occurrences by Error Code	Error Code	Error Code Decoded
	124	100	This is most likely an unrecoverable error. No data was received from partner. Data traffic was received from the source IP address and source port but not the destination IP address and port. The destination server may not have a listening port at the port indicated, there may be a firewall issue or the data traffic from the source IP and port may be inappropriate overhead.
	2	101	This is an unrecoverable error. Bad TCP Open (RST). A TCP Open (SYN) packet was sent from the source IP address and source port to start a session with the application at the destination port. The destination IP address and port responded with a RESET packet rather than the SYN-ACK packet which was expected. Reasons for this include: • The destination server may not have a listening port at the port indicated. • The destination server may have capacity issues or

- TCP Problem Finder will tell you what kind of errors were found in the trace and how many time.

Where Did It Happen?

Error Code : 121

This error is a performance warning. Small window sizes were found in the data traffic. Receive congestion window sizes which are less than 10,000 were found. This may cause performance degradation. Data traffic is transferred but it may be slower than desired or possible.

- **Destination Port**
  - **Destination port 515 is responsible for 73.33% of the total errors.**
- **Source IP**
  - **10.120.10.216 is responsible for 73.33% of the total errors.**
- **Source Network (Octet1 - Octet3)**
  - **10.120.10 is responsible for 86.66% of the total errors.**
- **Source Network (Octet1)**
  - **10 is responsible for 100.0% of the total errors.**
- **Destination Network (Octet1)**
  - **10 is responsible for 100.0% of the total errors.**

- Next, you probably want to know where exactly the problems were.

Session Details

10.120.10.200:23 10.236.78.103:1119	• No small window sizes from 10.236.78.103:1119 were found in the data flow. • No zero window sizes from 10.120.10.200:23 were found in the data flow. • No zero window sizes from 10.236.78.103:1119 were found in the data flow. **Duplicate Segments** • No duplicate segments from 10.120.10.200:23 were found in the data flow. • Duplicate segments were found on this session from 10.236.78.103:1119. • The number of duplicate segments received is: 1. The total packets received is: 5. The percent of packets which are duplicate segments is:20.0%. • The number of bytes received in duplicate segments is: 14. The total bytes received is: 28. The percent of bytes received in duplicate segments is:50.0%. • Packet 1318992 was duplicated 1 times.

- You may want to analyze exactly what happened in the session.
- From the TCP open to data transmission to the close is analyzed for problems.

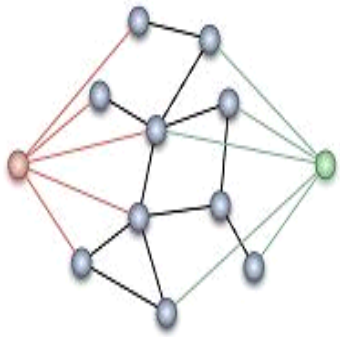
IP PROBLEM FINDER

TCP Analysis Reports
Trace File: sample17

INSIDE PRODUCTS
Thinking Inside the Box

»Expert Trace Analysis

You may wish to start with the Main Reports first.



- Show TCP Trace Narrative
- Show TCP Visual Trace
- Create TCP Packets Graphs

- Show TCP Packets
- Show TCP Packets - Diagnostics
- Show TCP Window Sizes
- Show All TCP Window Updates

- Show TCP Segmentation Offload

- Show TCP Duplicate ACKs
- Show TCP Duplicate Segments
- Show TCP Selective ACKs
- Show TCP Delayed Acks
- Show TCP Out Of Order
- Show TCP Retransmits
- Show TCP Resets
- Show TCP Resets And Cause
- Show TCP Session Start
- Show TCP Session Start Failures
- Show TCP Session End
- Show TCP Session End With Reset

»Main Reports

You may use the links here to view the analysis of this trace.

- Show TCP Traffic Analysis
- Show TCP Error Analysis
- Show TCP Good Events
- Show TCP Traffic Summary
- Show TCP Address List

- Show Major TCP Problem Sources
- Show Complete TCP Problem Sources
- Show Detailed TCP Analysis

Many reports to analyze TCP, UDP, IPv4, IPv6, DNS, SSL

»Other Reports

You may go to other reports from here. Click below to change to other menus.

- Go to Main Report Menu

To analyze IP reassembly or fragmentation in IPv6 or IPv4 go to:

- Go to IPv4 / IPv6 Report Menu

For statistics on tunneling (IPv6 packets in IPv4) go to:

- Go to IPv6 Tunnel Report Menu

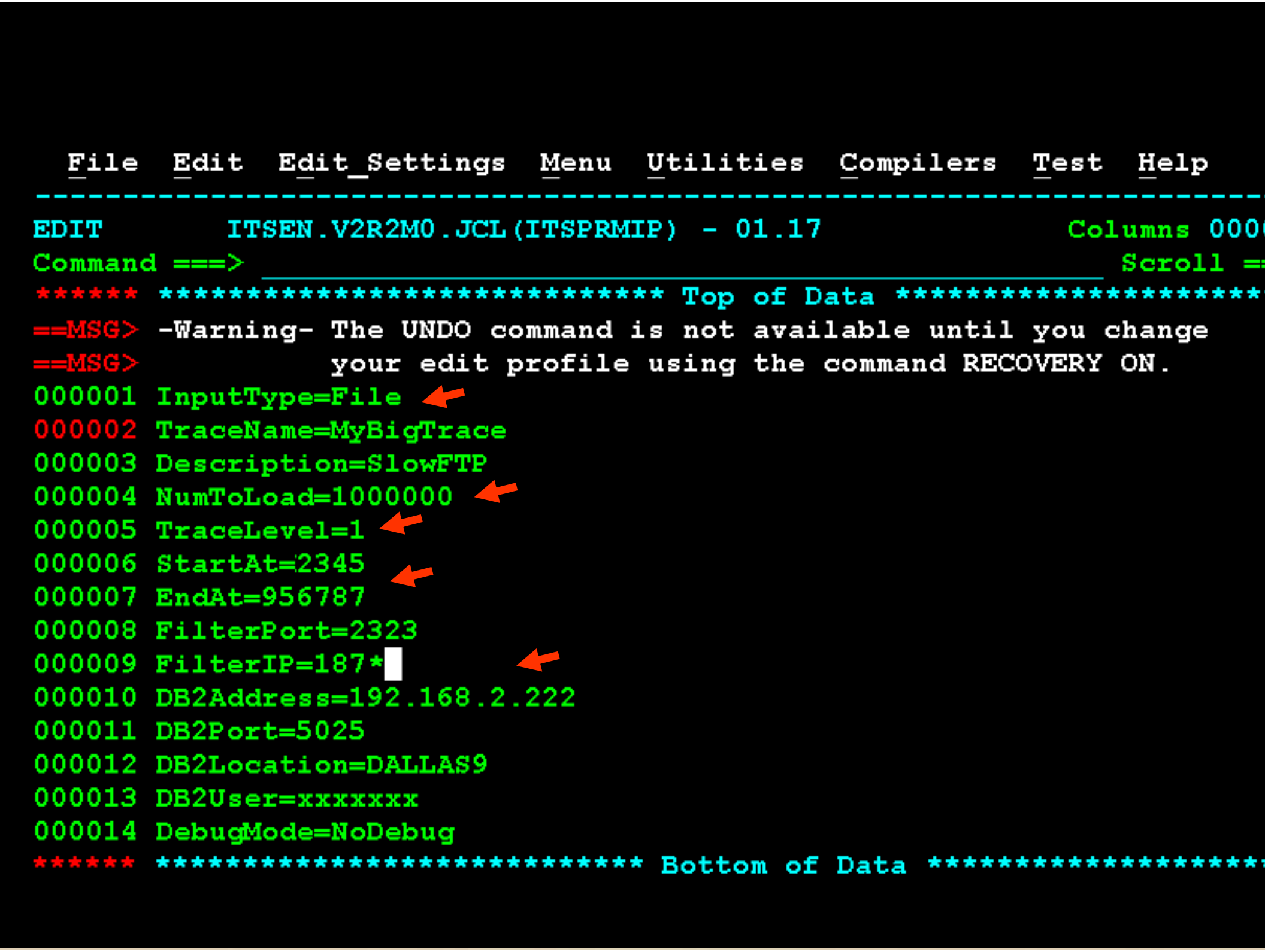
For detailed analysis on higher level protocols including packets sent natively in IPv4, IPv6 or tunneled (IPv6 packets in IPv4) go to:

- Go to UDP Report Menu
- Go to ICMP / ICMPv6 Report Menu

- Go to DNS Report Menu
- Go to SSL Report Menu

But, what about the mainframe?

- So far, what you have been seeing is the PC GUI.
- Analyzing packets is a lot of work.
- Why not use the power of the mainframe?


File Edit Edit_Settings Menu Utilities Compilers Test Help
EDIT ITSEN.V2R2M0.JCL(ITSPRMIP) - 01.17 Columns 000
Command ===> Scroll =
****** ********** Top of Data **********
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 InputType=File
000002 TraceName=MyBigTrace
000003 Description=SlowFTP
000004 NumToLoad=1000000
000005 TraceLevel=1
000006 StartAt=2345
000007 EndAt=956787
000008 FilterPort=2323
000009 FilterIP=187*
000010 DB2Address=192.168.2.222
000011 DB2Port=5025
000012 DB2Location=DALLAS9
000013 DB2User=xxxxxxx
000014 DebugMode=NoDebug
****** ********** Bottom of Data **********

How do we do the analysis?

- We read the trace file using batch Java programs (JzOS).
- Load the trace into DB2 for analysis.
- Create recommendations.
- Use the PC GUI to view.
- Add the power of the mainframe to the beauty of the PC GUI.

A sample problem from earlier this month.

- There were connection drops for a major critical application used by law enforcement.
- They use cell phones & connect via a VPN.
- Problem has been going on for weeks.
- Mainframe pointed at VPN, VPN guys said ‘No way it is us’.
- Application was third party. Very cooperative.
- We took a trace at both ends.

Show TCP Packets - Diagnostics
Sort Order : Packet Number
End At Packet 341
Destination Address : 10.217.102.108
Showing Entries : 1 -100
Using: Trace File:333

-	-	Packet Number	Packet Date	Source Address	Source Port	Destination Address	Destination Port	IP ID	Time To Live	Data Length	Sequence	ACK	Expected ACK	Delta (ss.milli.micro)
1		51	2012-03-08 10:20:23.823253		2323		2323	D2A2	60	3	2230183829	3868022489	2230183832	0.000.160
2		66	2012-03-08 10:20:23.829106		2323		2323	D2AD	60	3	2230183832	3868022492	2230183835	0.005.694
3		194	2012-03-08 10:24:25.790071		2323		2323	642F	60	3	2230183835	3868022492	2230183838	241.761.259
4		209	2012-03-08 10:24:25.795070		2323		2323	6439	60	3	2230183838	3868022495	2230183841	0.004.779
5		292	2012-03-08 10:25:44.799960		2323		2323	89CB	60	0	2230183841	3868022530	0	0.272.602
6		293	2012-03-08 10:25:45.009777		2323		2323	8A0C	60	211	2230183841	3868022530	2230184052	0.209.817
7		295	2012-03-08 10:25:45.301115		2323		2323	8A1C	60	0	2230184052	3868022538	0	0.290.840
8		340	2012-03-08 10:26:57.286306		2323		2323	FB19	255	This is the TCP Reset 0	2230184052	3868022573	0	0.001.558

What is with the TTL?

- Mainframe had been sending packets with TTL of 60.
- All of a sudden we get one with a TTL of 255.
- It is a RESET.

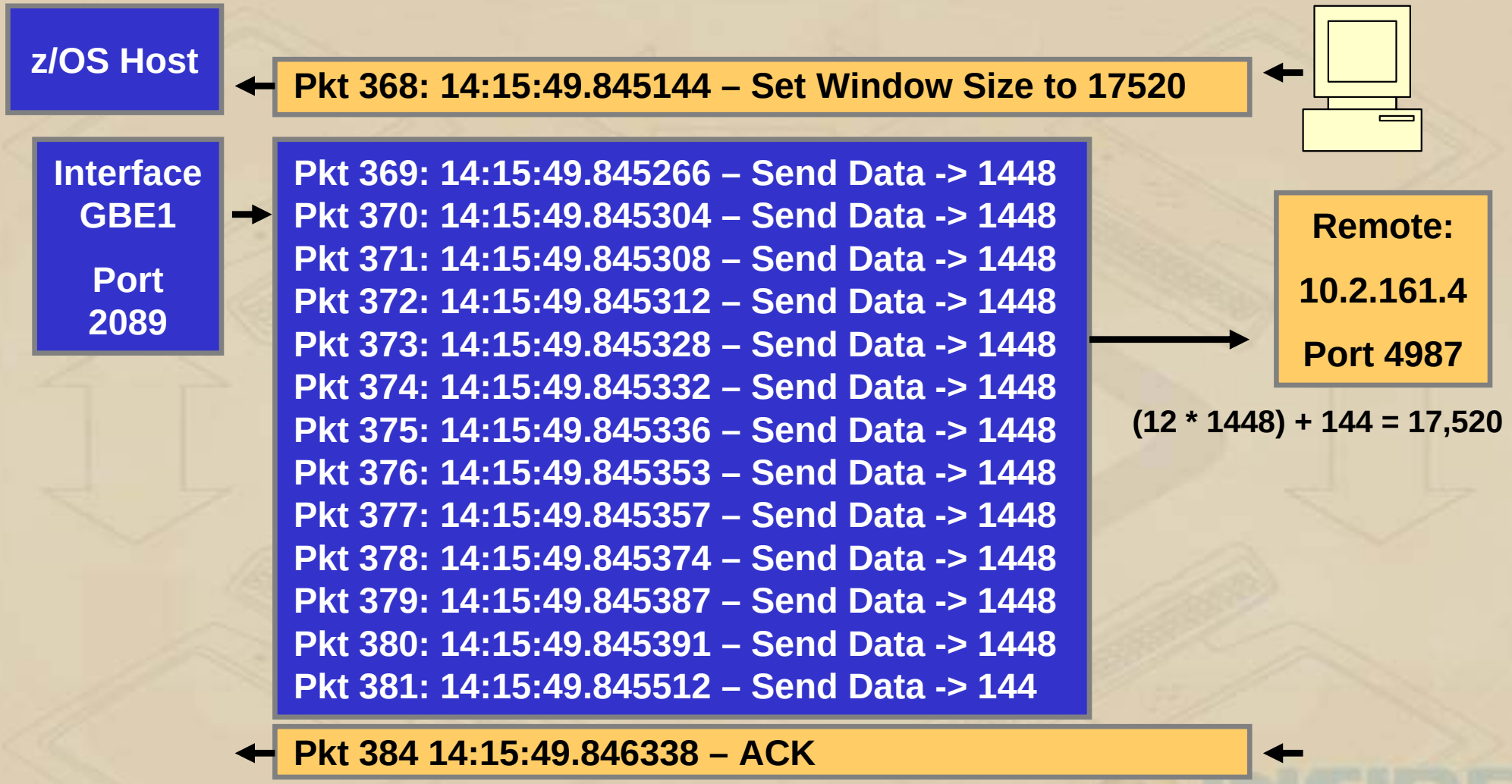
- Hmm.
- Don’t think the mainframe sent that one!

- This kind of report changes the conversation. Finger pointing levels tend to drop.

Segmentation Offload

- The TCP/IP stack can offload most IPv4 outbound TCP segmentation processing to an OSA-Express feature in QDIO mode using TCP segmentation offload support.
- You can configure this function by specifying the SEGMENTATIONOFFLOAD parameter on the GLOBALCONFIG profile statement.
- Analyze Segmentation Offload with TCP Problem Finder.

Window Scaling Congestion Window



Compare IPv6 and IPv4

Destination Address	IP Protocol	Connection Time (ss.milli.micro)	Total Packets	Throughput Packets Per Second	Total Data Bytes	Throughput Data Bytes Per Second	Minimum Bytes In Flight	Average Bytes In Flight	Maximum Bytes In Flight
208.111.39.67	IPv4	35.327.127	2K (52.01%)	65	11K (0.57%)	324	0	7	28
208.111.39.67	IPv4	0.020.015	5 (0.11%)	5	480 (0.02%)	480	0	96	480
208.111.39.67	IPv4	0.019.998	5 (0.11%)	5	480 (0.02%)	480	0	96	480
208.111.39.67	IPv4	5.371.834	8 (0.18%)	1	6K (0.31%)	1,218	0	761	1K
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	20.940.750	11 (0.25%)	< 0	9K (0.5%)	495	0	908	8K
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	20.792.770	8 (0.18%)	< 0	9K (0.48%)	474	0	1K	8K
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	20.797.733	9 (0.2%)	< 0	1K (0.06%)	60	0	139	579
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	20.795.714	8 (0.18%)	< 0	1K (0.09%)	90	0	234	1K
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	20.793.697	8 (0.18%)	< 0	1K (0.06%)	60	0	156	579
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	20.741.833	8 (0.18%)	< 0	9K (0.5%)	497	0	1K	8K
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	6.440.179	76 (1.73%)	12	42K (2.15%)	7,026	0	1K	7K
2607:F740::3F:216:3EFF:FE68:72C0	IPv6	6.108.390	69 (1.57%)	11	2K (0.12%)	419	0	47	1K

- As integration of IPv6 happens, it is interesting to compare both protocols in terms of throughput and bytes in flight.

A new way..

- So. You can continue to operate in the current mode.
- Take hours, days or even weeks to resolve problems.

- Or you can try something different.

Let us help you!

- When you buy a product, always buy:
  - Quality
  - Dedication
  - Innovation.
- Never be afraid to support Independent Software.
- Inside Products, in business since 2001.

TCP, EE, SSL, IPv6 Problem Finders

The products for the serious diagnostician :

the Problem Finders allow you to:

- Quickly find problems in diagnostic traces - which can consist of thousands or hundreds of thousands of packets!
- Get automatic recommendations and analysis
- **TCP Problem Finder** turns a trace into English!

- We expect that the amount of time saved is a factor of 8. That is, a trace which might take 8 hours to do manually, can be done in 1 hour with our **Problem Finders.**

- Packet loss,
- Retransmits,
- An error indicator, for example from a printer which is out of paper, or
- A keep-alive indicator.

- Too many duplicate acknowledgments may indicate a situation which needs to be further investigated.
- No duplicate acknowledgements from 10.197.4.1 port:58315 were found in tl

Delayed Acknowledgements

- No delayed acknowledgements from 10.173.12.5 port:4726 were found in th
- No delayed acknowledgements from 10.197.4.1 port:58315 were found in th

Out of Order Segments

- No out of order packets from 10.173.12.5 port:4726 were found in the data fl
- Out of order packets were found on this session from 10.197.4.1 port:58315.
- The number of out of order packets received is: 9. The total packets received i packets which are out of order is:3.87%.
- The number of bytes received in out of order packets is: 9,452. The total byte The percent of bytes received in out of order packets is:3.28%.
- Packet 464 was out of order.
- Packet 474 was out of order.
- Packet 507 was out of order.
- Packet 515 was out of order.
- Packet 519 was out of order.
- Packet 537 was out of order.
- Packet 552 was out of order.
- Packet 556 was out of order.
- Packet 928 was out of order.

Selective ACKs

- Selective ACKs were found on this session from 10.173.12.5 port:4726.
- The number of selective ACK packets received is: 200. The total packets received is: 220. The percent of packets which are selective ACKs is:90.9%.
- Packet 465 was a selective ACK.
- Packet 467 was a selective ACK.
- Packet 469 was a selective ACK.
- Packet 471 was a selective ACK

IP Problem Finder will tell you of problems with SACK, out of order, dup ACKs, and much more!

SHARKFEST '12

Wireshark Developer and User Conference

June 24th - 27th, 2012 • UC Berkeley

REGISTER NOW »

Home Register Agenda Lodging Sponsors

Get Connected with Sharkfest:

Join Inside Products at SharkFest.

We will be speaking and helping to sponsor the event.

Sharkfest '12 • June 24th – 27th

5th annual meeting of Wireshark gurus, newbi

Join the global Wireshark developer and user communit
transfer and networking.

This year, our growing event features two fabulous keynote presenters – Cliff Stoll and Steve Riley, more session choices, and a separate hands-on lab track to accommodate more participants than ever before.

Register now and bring your A-game for this info-packed event to be held, for the first time, at UC Berkeley, Clark Kerr Campus, Berkeley, CA.

Download the Sharkfest Agenda and get a sneak peak at the full lineup.

Keynote Speakers

Clifford Stoll

Few embody the kind of erratic intellectuality like Cliff Stoll. He is a speaker (his 2006 TED Talk registered nearly three quarters of a million views), an astronomer, and author best known for his pursuit of hacker Markus Hess in 1986 and the subsequent 1989 book detailing his investigation. Stoll taught college-level physics to eighth graders and home-schooled teenagers and now builds and sells Klein bottles in his spare time.

UC Berkeley, Clark Kerr Campus
2601 Warring Street
Berkeley, CA 94720
See map »

Registration Information

Sharkfest Agenda

Early Bird Attendee Registration $695.00

Contact Us!

- For more information:
  - Products,
  - Consulting,
  - TCP/IP classes

1-831-659-8360

sales@insidethestack.com

- Pricing for IP Problem Finders:
  - $25K per site per year.
  - Like buying a router!

Australia: Blueline Software

UK : FitzSoftware

BENELUX: Adinsec BvBa

Israel : NESS

France : Query Informatique