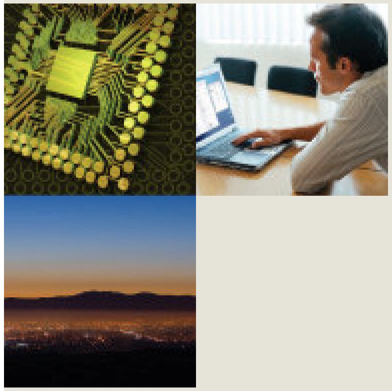
SHARE
Technology · Connections · Results

Diagnosing Mainframe Network Problems with Packet Trace



David Cheng

Applied Expert Systems (AES)

March 5, 2009 @ 1:30pm
Session # 3744
davec@aesclever.com

Agenda

- A Few Things to Consider
- How to Take a Packet Trace
- Know Your Protocols and Applications
  - TCP*
  - UDP*
  - IP*
  - ICMP*
  - DHCP
  - FTP
- Working Our Way Through Some Traces
- Concluding Remarks

A Few Things To Consider

- Know your Network
  - What does a performing network look like?
  - Do you have a good benchmark trace?
  - Network Map?
  - Is It Documented?
  - Is There a Change Log?
- What's the problem?
  - During development, debugging may be needed
  - Did it even hit z/OS, z/VM or zLinux TCP/IP?
  - Why is the SYN failing?
  - Is the response time reasonable?
  - TCP retransmission packets
  - Dropped TCP packets
- What Protocols Are Involved?
  - TCP/IP?
  - UDP?
  - ICMP?

How to Take a Packet Trace?

- z/OS CTRACE: SYSTCPDA, SYSTCPOT
  - Set up an External Writer Proc

```
E.g., SYS1.PROCLIB(AESWRT):

//IEFPROC EXEC PGM=ITTTRCWR,REGION=0K,TIME=1440,DPRTY=15
//TRCOUT01 DD DISP=SHR,DSN=trace.dataset
```

  - Set up tracing parameters

```
E.g., SYS1.PARMLIB(CTAESPRM):

TRACEOPTS ON WTR(AESWRT)
```

z/OS CTRACE: SYSTCPDA

- To Start Tracing:

```
TRACE CT,WTRSTART=AESWRT
V TCPIP,,PKT,CLEAR
V TCPIP,,PKT,LINKN=<link>,ON,FULL,PROT=TCP,IP=<ip addr>
TRACE CT,ON,COMP=SYSTCPDA,SUB=(TCPIP),PARM=CTAESPRM
```

- To Stop Tracing:

```
V TCPIP,,PKT,OFF
TRACE CT,OFF,COMP=SYSTCPDA,SUB=(TCPIP)
TRACE CT,WTRSTOP=AESWRT,FLUSH
```

- To View Tracing Status:

```
D TRACE,WTR=AESWRT
```

Verify that the external writer is active

```
D TCPIP,,NETSTAT,DE
```

Verify that **TrRecCnt** is non-zero and incrementing

z/OS CTRACE: SYSTCPOT

- OSA-Express2 Network Traffic Analyzer (OSAENTA)
  - Trace packets to a host attached to an OSA-Express2.
  - The host can be an LPAR with **z/OS, z/VM** or **Linux**.
  - The trace function is controlled by z/OS Communication Server, while the data is collected in the OSA at the network port.

- Pre-Reqs:
  - Install the required PTFs for z/OS V1R8 (APAR PK36947).
  - Install the microcode for the OSA (2094DEVICE PSP and the 2096DEVICE PSP).
  - Update the OSA using the Hardware Management Console (HMC) to:

    Define more data devices to systems that will use the trace function.

    Set the security for the OSA:

    LOGICAL PARTITION - Only packets from the LPAR

    CHPID - All packets using this CHPID
  - Verify the TRLE definitions for the OSA that it has one DATAPATH address available for tracing. Note that **two** DATAPATH addresses are required – one for data transfers and the other for trace data.

z/OS CTRACE: SYSTCPOT

- To Start Tracing:

```
TRACE CT,WTRSTART=AESWRT
V TCPIP,,OSAENTA,PORTNAME=<port>,CLEAR
V TCPIP,,OSAENTA,PORTNAME=<port>,ON,NOFILTER=ALL
TRACE CT,ON,COMP=SYSTCPOT,SUB=(TCPIP),PARM=CTAESPRM
```

- To Stop Tracing:

```
V TCPIP,,OSAENTA,PORTNAME=<port>,OFF
TRACE CT,OFF,COMP=SYSTCPOT,SUB=(TCPIP)
TRACE CT,WTRSTOP=AESWRT,FLUSH
```

- To View Tracing Status:

```
D TRACE,WTR=AESWRT
```

Verify that the external writer is active

z/OS CTRACE: SYSTCPOT

- To View Tracing Status (continued):

```
D TCPIP,,NETSTAT,DE
```

```
OSA-EXPRESS NETWORK TRAFFIC ANALYZER INFORMATION:
 OSA PORTNAME: DR281920          OSA DEVSTATUS:      READY
   OSA INTFNAME: EZANTADR281920  OSA INTFSTATUS:     READY
   OSA SPEED:    1000            OSA AUTHORIZATION:  LOGICAL PARTITION
   OSAENTA CUMULATIVE TRACE STATISTICS:
     DATAMEGS:    1                    FRAMES:           3625
     DATABYTES:   1641283              FRAMESDISCARDED:  0
     FRAMESLOST:  0
   OSAENTA ACTIVE TRACE STATISTICS:
     DATAMEGS:    0                    FRAMES:           23
     DATABYTES:   6148                 FRAMESDISCARDED:  0
     FRAMESLOST:  0                    TIMEACTIVE:       2
   OSAENTA TRACE SETTINGS:           STATUS: ON
     DATAMEGSLIMIT: 2147483647         FRAMESLIMIT:      2147483647
     ABBREV:        480                TIMELIMIT:        10080
     DISCARD:       NONE
   OSAENTA TRACE FILTERS:            NOFILTER: ALL
     DEVICEID: *
     MAC:      *
     VLANID:   *
     ETHTYPE:  *
     IPADDR:   *
     PROTOCOL: *
     PORTNUM:  *
```

z/VM:

- To enable the trace:
  - NETSTAT OBEY PACKETTRACESIZE 256
  - NETSTAT OBEY TRACEONLY ETH0 ENDTRACEONLY
- To start data collection:
  - TRSOURCE ID TCP TYPE GT BLOCK FOR USER tcpip_userid
  - TRSOURCE ENABLE ID TCP
- To stop data collection:
  - NETSTAT OBEY PACKETTRACESIZE 0
  - NETSTAT OBEY TRACEONLY ENDTRACEONLY
  - TRSOURCE DISABLE ID TCP
- To analyze a TRF trace file:
  - IPFORMAT command
  - Use the TRF2TCPD utility to convert the TRF file to pcap (tcpdump) format

Know Your Protocols and Applications - TCP

- TCP Functions
  - Establish Connections
  - Manage Connections
  - Terminate Connections
  - Handling and Packaging Data
  - Transferring Data
  - Providing Reliability
  - Flow Control and Congestion Avoidance

TCP Fundamentals

- It Started as NCP – Network Control Protocol and Then Became Transmission Control Program
  - Sorta like TCP and IP combined – RFC 675
- Improved and split into TCP (Transmission Control Protocol) and IP (Internet Protocol) – RFC 793
- Reliable Transportation of Data Over a Network
- Sliding Window Acknowledgement – A method used by TCP to manage the reliability and the rate of the data transmission
- Control bits – ACK, PSH, SYN, FIN, RST, URG
- Nagel Algorithm to prevent "send-side silly window syndrome”
  - Datagrams with small amounts of data - where the header is larger than the payload

TCP Codes Explained

- ACK – Acknowledge receipt of the packet
- PSH – Push – Send the data immediately
- SYN – Synchronize – Establish a connection
- FIN – Finish – Terminate the connection
- RST – Reset – See a Lot of These There Is a PROBLEM!
- URG – Urgent – Send It in a Hurry!

Sliding Window Acknowledgement

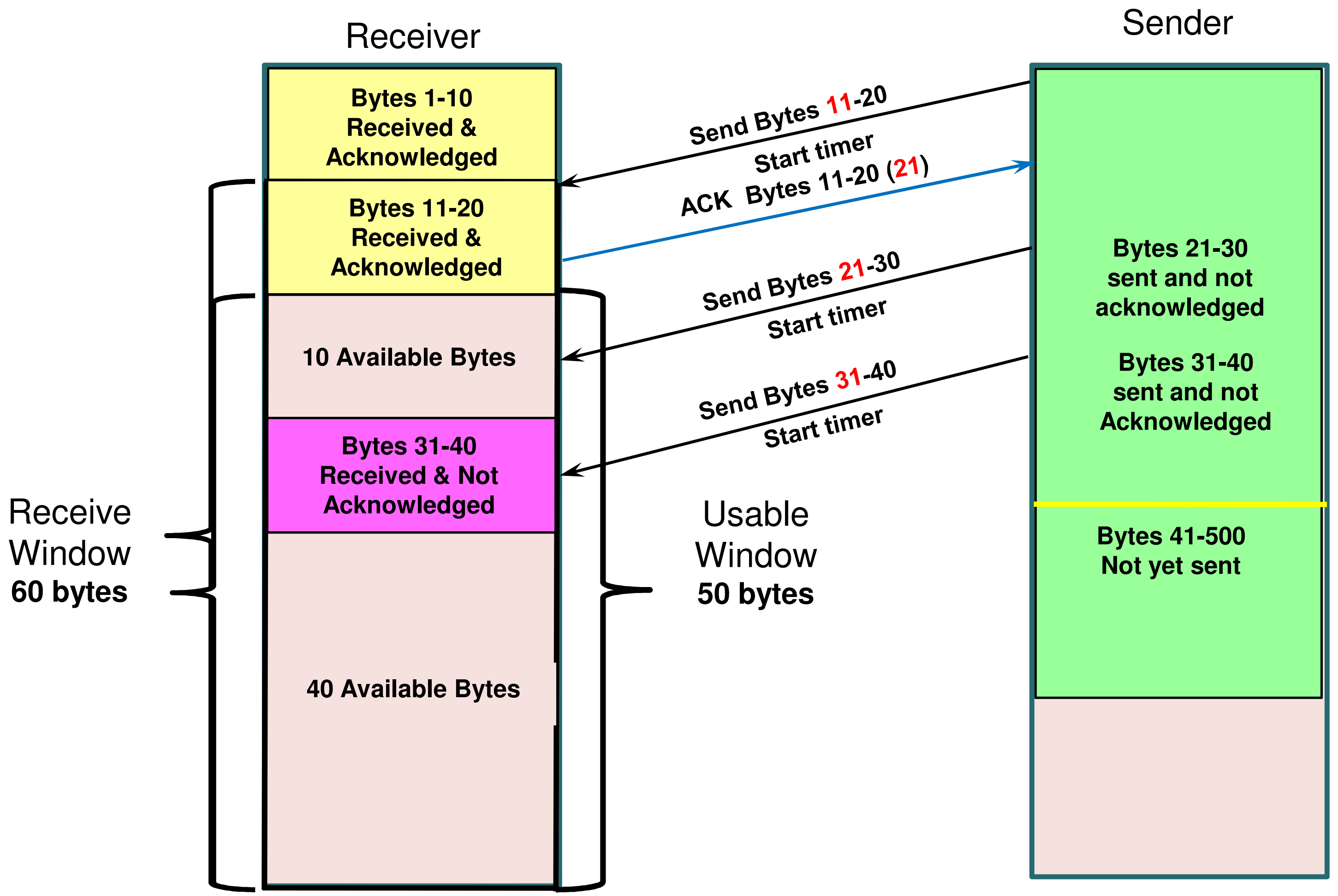
- **Advertised window size -** This field contains the amount of data that may be transmitted into the buffer.
- **Sequence number** – Identifies the first byte of data in this segment.
- **Acknowledgment number** – Identifies the next byte of data that a recipient is expecting to receive.
- With this information, a sliding-window protocol is implemented.

Sliding Window Acknowledgement

- Transmit categories
  1. Bytes Sent And Acknowledged
  2. Bytes Sent But Not Yet Acknowledged
  3. Bytes Not Yet Sent For Which Recipient Is Ready
  4. Bytes Not Yet Sent For Which Recipient Is Not Ready

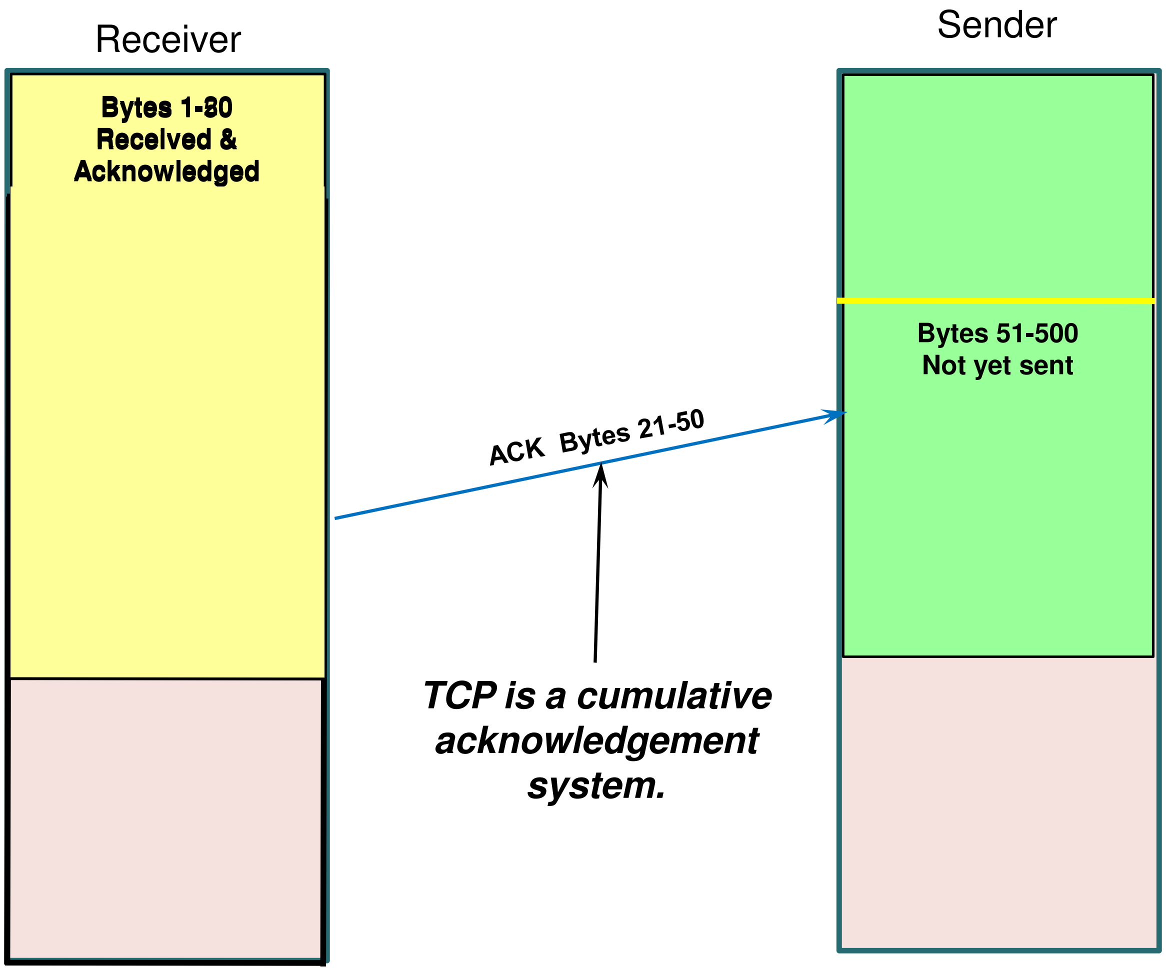
- Receive categories
  1. Bytes Received And Acknowledged. This is the receiver’s complement to Transmit Categories #1 and #2.
  2. Bytes Not Yet Received For Which Recipient Is Ready. This is the receiver’s complement to Transmit Category #3.
  3. Bytes Not Yet Received For Which Recipient Is Not Ready. This is the receiver’s complement to Transmit Category #4.

Sliding Window Acknowledgement



Receiver
Sender
Bytes 1-10 Received & Acknowledged
Bytes 11-20 Received & Acknowledged
10 Available Bytes
Bytes 31-40 Received & Not Acknowledged
40 Available Bytes
Send Bytes 11-20
Start timer
ACK Bytes 11-20 (21)
Send Bytes 21-30
Start timer
Send Bytes 31-40
Start timer
Bytes 21-30 sent and not acknowledged
Bytes 31-40 sent and not Acknowledged
Bytes 41-500 Not yet sent
Receive Window 60 bytes
Usable Window 50 bytes

Sliding Window Acknowledgement



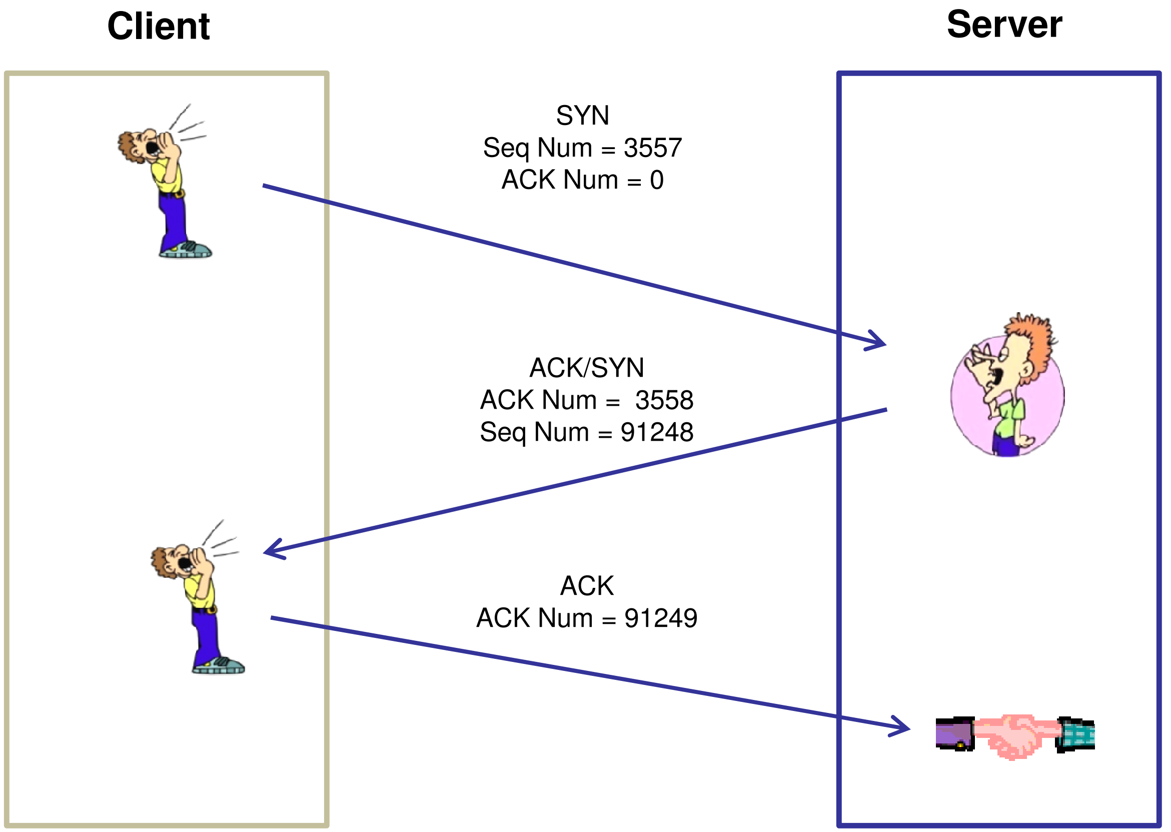
TCP is a cumulative acknowledgement system.

TCP Sequence of Events

- Establishing a connection
- Data transfer
- Termination

Establishing a Connection

The 3 Way Handshake



Client

Server

Socket

Connect
Let’s Talk
SYN-SENT

SYN
Seq Num = 3557
ACK Num = 0

Socket
Bind
Listen
LISTEN

OK, Let’s Talk
SYN-RCVD

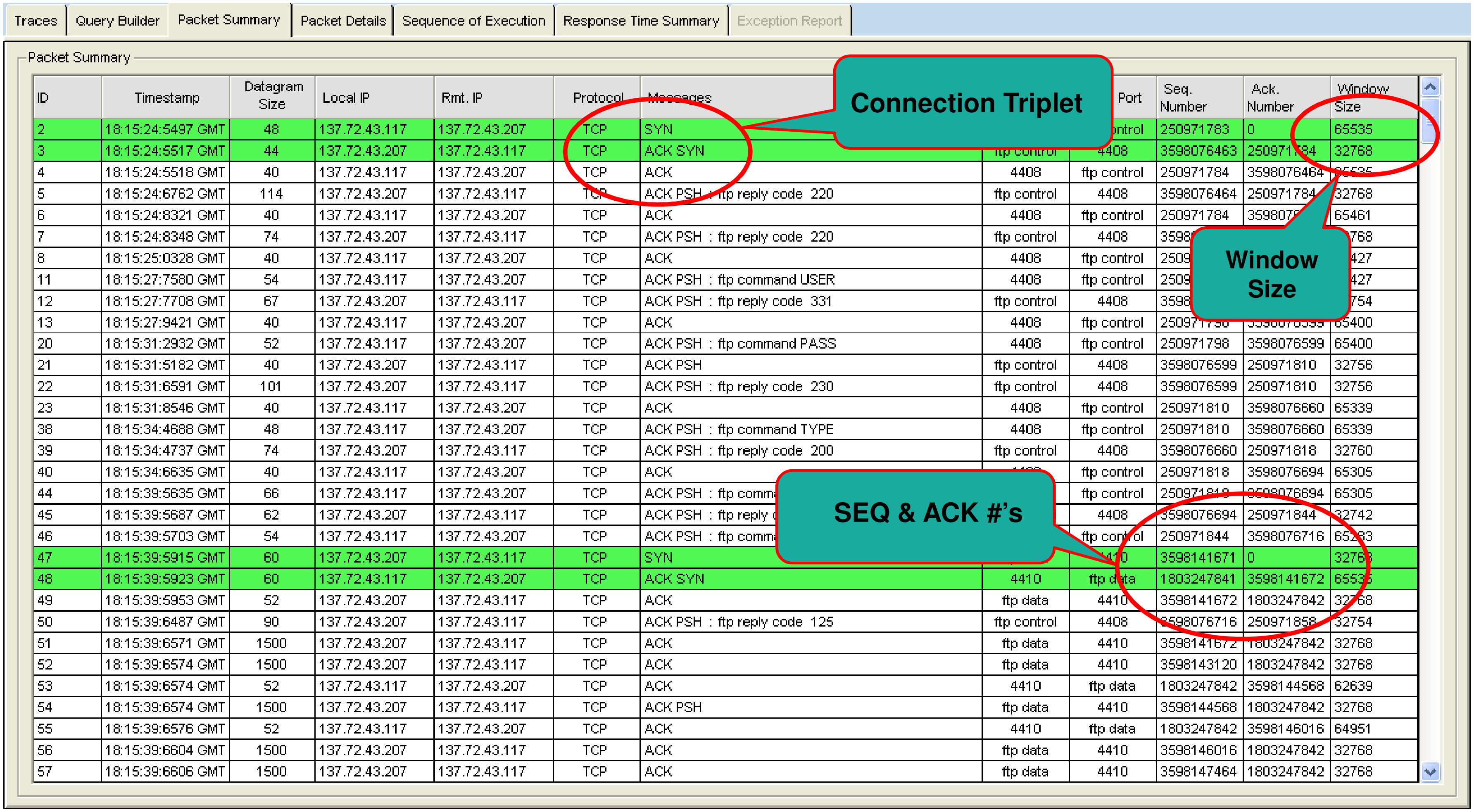
ACK/SYN
ACK Num = 3558
Seq Num = 91248

Thanks!
ESTABLISHED

ACK
ACK Num = 91249

Accept
Conversation
Established
ESTABLISHED

Establishing a Connection
The 3 Way Handshake

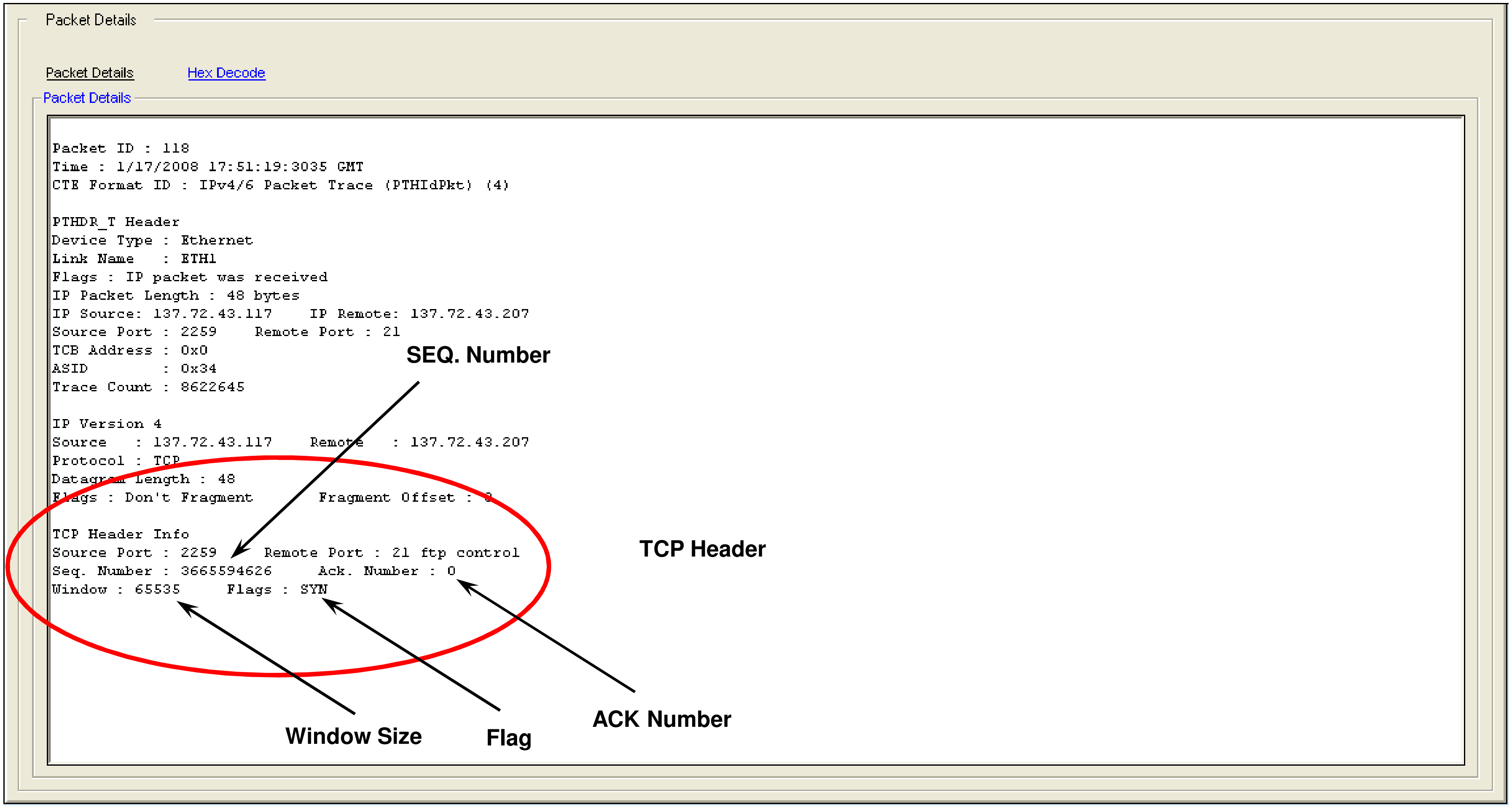


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages		Port	Seq. Number	Ack. Number	Window Size
2	18:15:24:5497 GMT	48	137.72.43.117	137.72.43.207	TCP	SYN	[illegible]	ntrol	250971783	0	65535
3	18:15:24:5517 GMT	44	137.72.43.207	137.72.43.117	TCP	ACK SYN	ftp control	4408	3598076463	250971784	32768
4	18:15:24:5518 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971784	3598076464	65535
5	18:15:24:6762 GMT	114	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 220	ftp control	4408	3598076464	250971784	32768
6	18:15:24:8321 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971784	359807	65461
7	18:15:24:8348 GMT	74	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 220	ftp control	4408	3598	[illegible]	768
8	18:15:25:0328 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	2509	[illegible]	427
11	18:15:27:7580 GMT	54	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp command USER	4408	ftp control	2509	[illegible]	427
12	18:15:27:7708 GMT	67	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 331	ftp control	4408	3598	[illegible]	754
13	18:15:27:9421 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971798	3598076599	65400
20	18:15:31:2932 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp command PASS	4408	ftp control	250971798	3598076599	65400
21	18:15:31:5182 GMT	40	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp control	4408	3598076599	250971810	32756
22	18:15:31:6591 GMT	101	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 230	ftp control	4408	3598076599	250971810	32756
23	18:15:31:8546 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971810	3598076660	65339
38	18:15:34:4688 GMT	48	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp command TYPE	4408	ftp control	250971810	3598076660	65339
39	18:15:34:4737 GMT	74	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 200	ftp control	4408	3598076660	250971818	32760
40	18:15:34:6635 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971818	3598076694	65305
44	18:15:39:5635 GMT	66	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp comma	[illegible]	ftp control	250971818	3598076694	65305
45	18:15:39:5687 GMT	62	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply c	[illegible]	4408	3598076694	250971844	32742
46	18:15:39:5703 GMT	54	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp comma	[illegible]	ftp control	250971844	3598076716	65283
47	18:15:39:5915 GMT	60	137.72.43.207	137.72.43.117	TCP	SYN	[illegible]	4410	3598141671	0	32768
48	18:15:39:5923 GMT	60	137.72.43.117	137.72.43.207	TCP	ACK SYN	4410	ftp data	1803247841	3598141672	65535
49	18:15:39:5953 GMT	52	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598141672	1803247842	32768
50	18:15:39:6487 GMT	90	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 125	ftp control	4408	3598076716	250971858	32754
51	18:15:39:6571 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598141672	1803247842	32768
52	18:15:39:6574 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598143120	1803247842	32768
53	18:15:39:6574 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598144568	62639
54	18:15:39:6574 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp data	4410	3598144568	1803247842	32768
55	18:15:39:6576 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598146016	64951
56	18:15:39:6604 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598146016	1803247842	32768
57	18:15:39:6606 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598147464	1803247842	32768

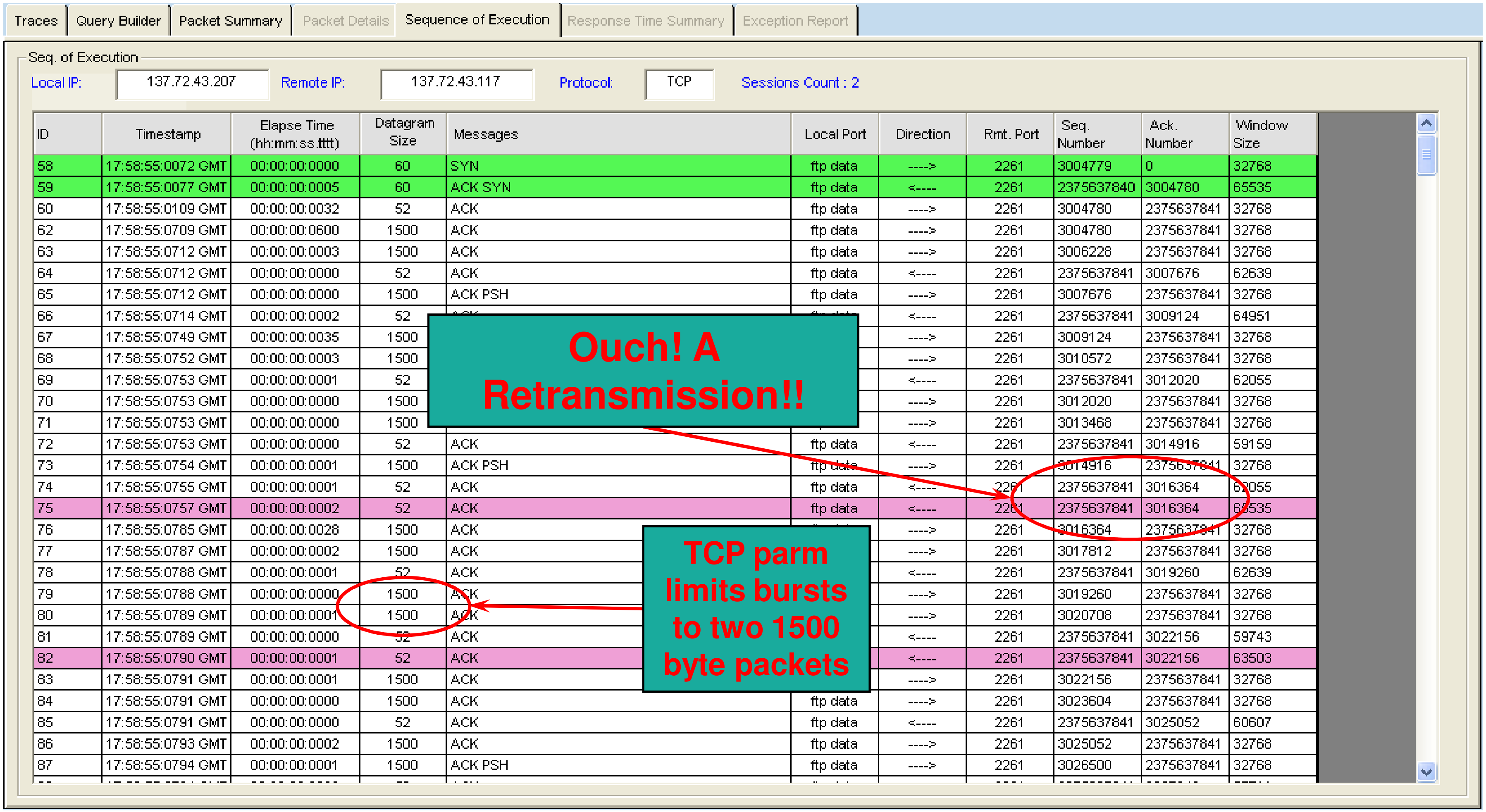
Establishing a Connection

Packet Details



```
Packet ID : 118
Time : 1/17/2008 17:51:19:3035 GMT
CTE Format ID : IPv4/6 Packet Trace (PTHIdPkt) (4)

PTHDR_T Header
Device Type : Ethernet
Link Name   : ETH1
Flags : IP packet was received
IP Packet Length : 48 bytes
IP Source: 137.72.43.117    IP Remote: 137.72.43.207
Source Port : 2259    Remote Port : 21
TCB Address : 0x0
ASID        : 0x34
Trace Count : 8622645

IP Version 4
Source   : 137.72.43.117    Remote   : 137.72.43.207
Protocol : TCP
Datagram Length : 48
Flags : Don't Fragment      Fragment Offset : 0

TCP Header Info
Source Port : 2259    Remote Port : 21 ftp control
Seq. Number : 3665594626     Ack. Number : 0
Window : 65535     Flags : SYN
```

Data Transfer



Seq. of Execution

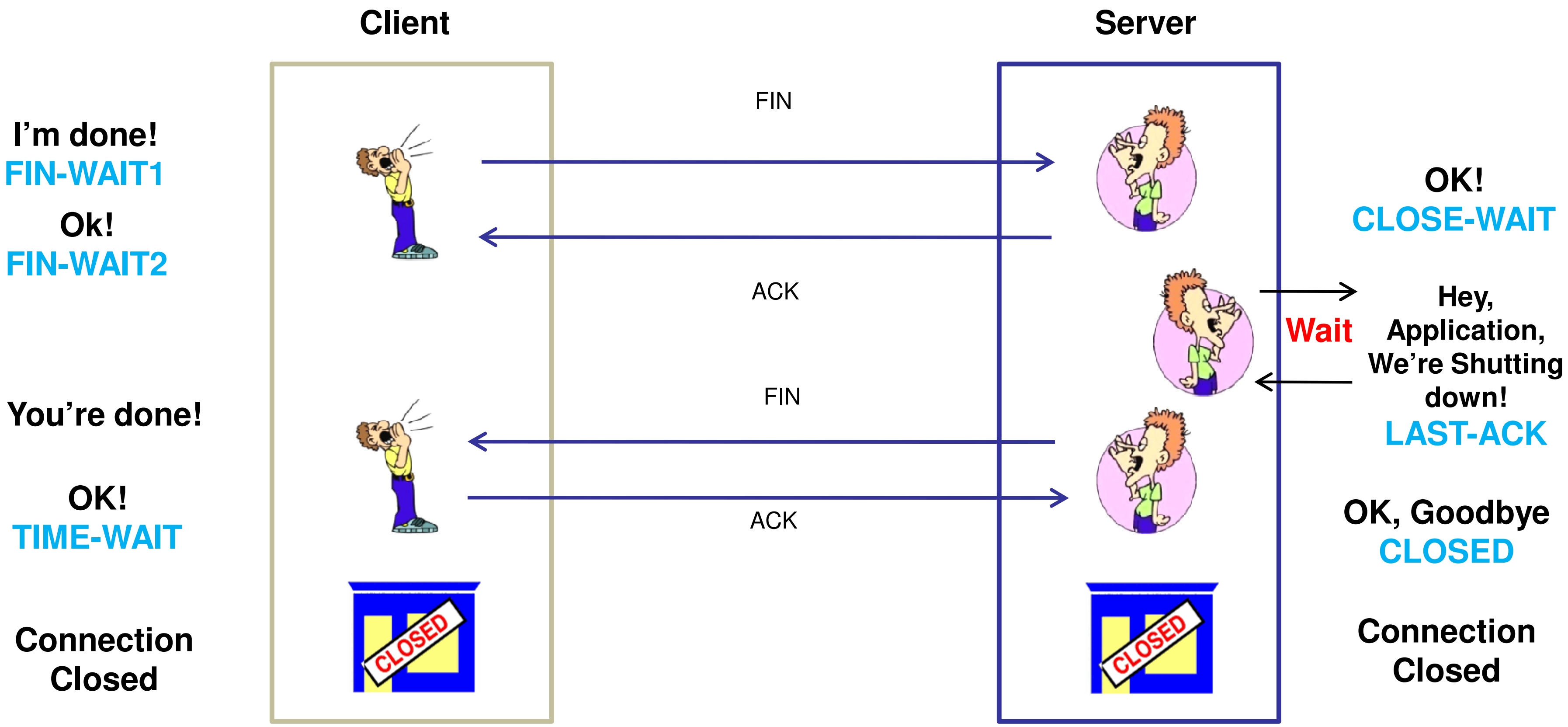
Local IP: 137.72.43.207 Remote IP: 137.72.43.117 Protocol: TCP Sessions Count : 2

ID	Timestamp	Elapse Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
58	17:58:55:0072 GMT	00:00:00:0000	60	SYN	ftp data	---->	2261	3004779	0	32768
59	17:58:55:0077 GMT	00:00:00:0005	60	ACK SYN	ftp data	<----	2261	2375637840	3004780	65535
60	17:58:55:0109 GMT	00:00:00:0032	52	ACK	ftp data	---->	2261	3004780	2375637841	32768
62	17:58:55:0709 GMT	00:00:00:0600	1500	ACK	ftp data	---->	2261	3004780	2375637841	32768
63	17:58:55:0712 GMT	00:00:00:0003	1500	ACK	ftp data	---->	2261	3006228	2375637841	32768
64	17:58:55:0712 GMT	00:00:00:0000	52	ACK	ftp data	<----	2261	2375637841	3007676	62639
65	17:58:55:0712 GMT	00:00:00:0000	1500	ACK PSH	ftp data	---->	2261	3007676	2375637841	32768
66	17:58:55:0714 GMT	00:00:00:0002	52			<----	2261	2375637841	3009124	64951
67	17:58:55:0749 GMT	00:00:00:0035	1500			---->	2261	3009124	2375637841	32768
68	17:58:55:0752 GMT	00:00:00:0003	1500			---->	2261	3010572	2375637841	32768
69	17:58:55:0753 GMT	00:00:00:0001	52			<----	2261	2375637841	3012020	62055
70	17:58:55:0753 GMT	00:00:00:0000	1500			---->	2261	3012020	2375637841	32768
71	17:58:55:0753 GMT	00:00:00:0000	1500			---->	2261	3013468	2375637841	32768
72	17:58:55:0753 GMT	00:00:00:0000	52	ACK	ftp data	<----	2261	2375637841	3014916	59159
73	17:58:55:0754 GMT	00:00:00:0001	1500	ACK PSH	ftp data	---->	2261	3014916	2375637841	32768
74	17:58:55:0755 GMT	00:00:00:0001	52	ACK	ftp data	<----	2261	2375637841	3016364	62055
75	17:58:55:0757 GMT	00:00:00:0002	52	ACK	ftp data	<----	2261	2375637841	3016364	65535
76	17:58:55:0785 GMT	00:00:00:0028	1500	ACK		---->	2261	3016364	2375637841	32768
77	17:58:55:0787 GMT	00:00:00:0002	1500	ACK		---->	2261	3017812	2375637841	32768
78	17:58:55:0788 GMT	00:00:00:0001	52	ACK		<----	2261	2375637841	3019260	62639
79	17:58:55:0788 GMT	00:00:00:0000	1500	ACK		---->	2261	3019260	2375637841	32768
80	17:58:55:0789 GMT	00:00:00:0001	1500	ACK		---->	2261	3020708	2375637841	32768
81	17:58:55:0789 GMT	00:00:00:0000	52	ACK		<----	2261	2375637841	3022156	59743
82	17:58:55:0790 GMT	00:00:00:0001	52	ACK		<----	2261	2375637841	3022156	63503
83	17:58:55:0791 GMT	00:00:00:0001	1500	ACK		---->	2261	3022156	2375637841	32768
84	17:58:55:0791 GMT	00:00:00:0000	1500	ACK	ftp data	---->	2261	3023604	2375637841	32768
85	17:58:55:0791 GMT	00:00:00:0000	52	ACK	ftp data	<----	2261	2375637841	3025052	60607
86	17:58:55:0793 GMT	00:00:00:0002	1500	ACK	ftp data	---->	2261	3025052	2375637841	32768
87	17:58:55:0794 GMT	00:00:00:0001	1500	ACK PSH	ftp data	---->	2261	3026500	2375637841	32768

Ouch! A Retransmission!!

TCP parm limits bursts to two 1500 byte packets

Connection Termination



Client

Server

I'm done!
FIN-WAIT1

FIN

OK!
CLOSE-WAIT

Ok!
FIN-WAIT2

ACK

Wait

Hey, Application, We're Shutting down!
LAST-ACK

You're done!

FIN

OK!
TIME-WAIT

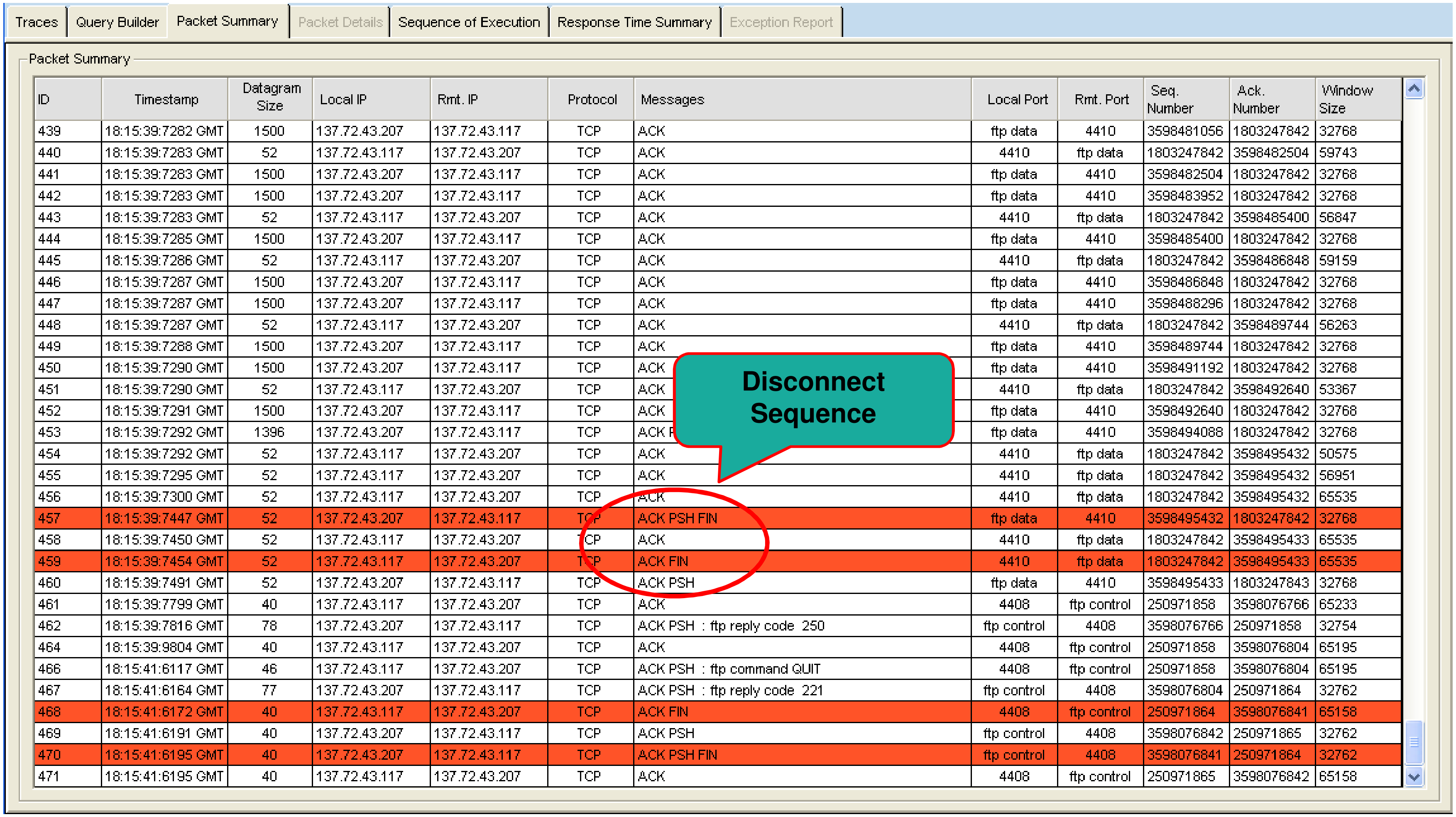
ACK

OK, Goodbye
CLOSED

Connection Closed

Connection Closed

Connection Termination

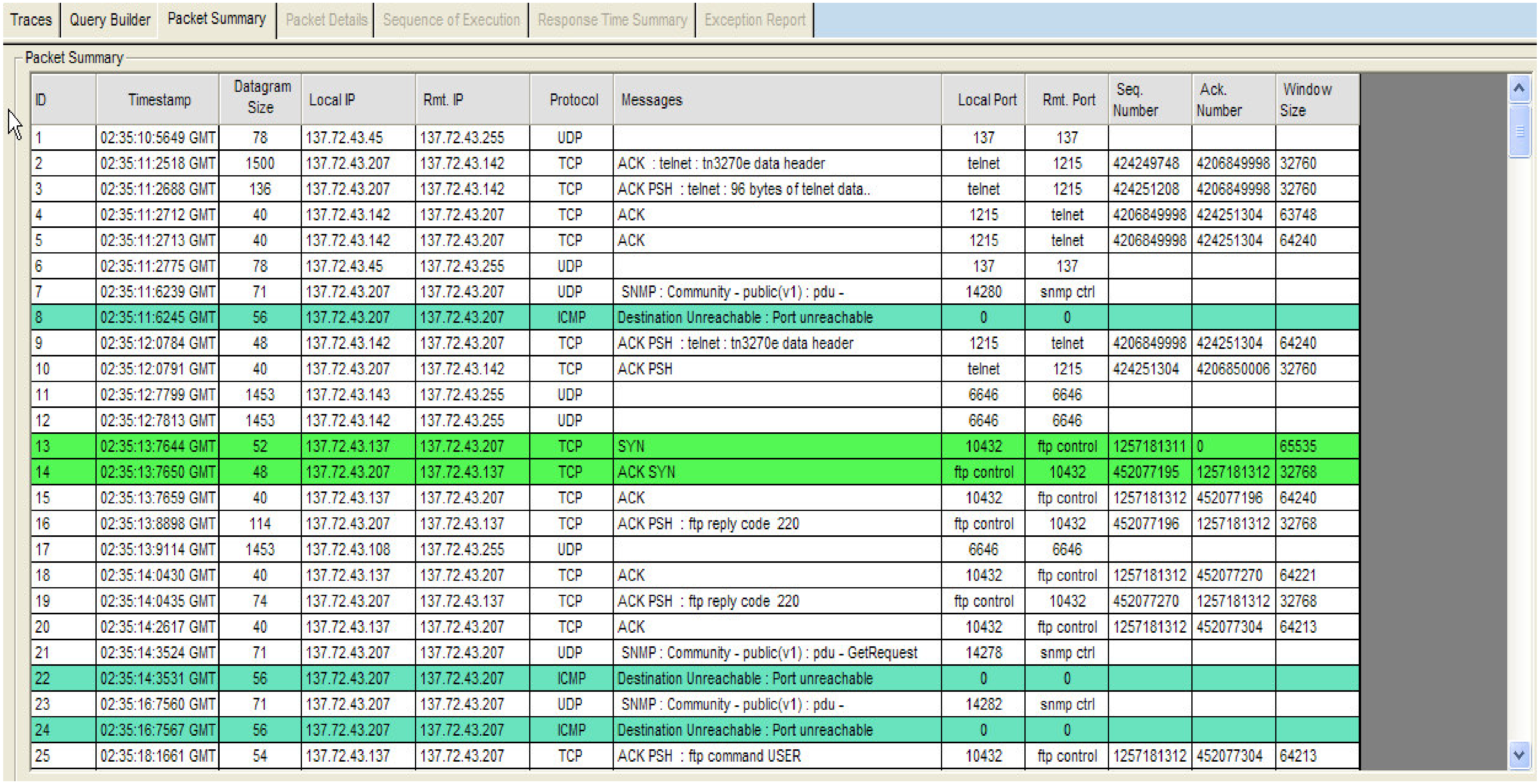


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
439	18:15:39:7282 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598481056	1803247842	32768
440	18:15:39:7283 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598482504	59743
441	18:15:39:7283 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598482504	1803247842	32768
442	18:15:39:7283 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598483952	1803247842	32768
443	18:15:39:7283 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598485400	56847
444	18:15:39:7285 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598485400	1803247842	32768
445	18:15:39:7286 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598486848	59159
446	18:15:39:7287 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598486848	1803247842	32768
447	18:15:39:7287 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598488296	1803247842	32768
448	18:15:39:7287 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598489744	56263
449	18:15:39:7288 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598489744	1803247842	32768
450	18:15:39:7290 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598491192	1803247842	32768
451	18:15:39:7290 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598492640	53367
452	18:15:39:7291 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598492640	1803247842	32768
453	18:15:39:7292 GMT	1396	137.72.43.207	137.72.43.117	TCP	ACK P	ftp data	4410	3598494088	1803247842	32768
454	18:15:39:7292 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495432	50575
455	18:15:39:7295 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495432	56951
456	18:15:39:7300 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495432	65535
457	18:15:39:7447 GMT	52	137.72.43.207	137.72.43.117	TCP	ACK PSH FIN	ftp data	4410	3598495432	1803247842	32768
458	18:15:39:7450 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	3598495433	65535
459	18:15:39:7454 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK FIN	4410	ftp data	1803247842	3598495433	65535
460	18:15:39:7491 GMT	52	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp data	4410	3598495433	1803247843	32768
461	18:15:39:7799 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971858	3598076766	65233
462	18:15:39:7816 GMT	78	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 250	ftp control	4408	3598076766	250971858	32754
464	18:15:39:9804 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971858	3598076804	65195
466	18:15:41:6117 GMT	46	137.72.43.117	137.72.43.207	TCP	ACK PSH : ftp command QUIT	4408	ftp control	250971858	3598076804	65195
467	18:15:41:6164 GMT	77	137.72.43.207	137.72.43.117	TCP	ACK PSH : ftp reply code 221	ftp control	4408	3598076804	250971864	32762
468	18:15:41:6172 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK FIN	4408	ftp control	250971864	3598076841	65158
469	18:15:41:6191 GMT	40	137.72.43.207	137.72.43.117	TCP	ACK PSH	ftp control	4408	3598076842	250971865	32762
470	18:15:41:6195 GMT	40	137.72.43.207	137.72.43.117	TCP	ACK PSH FIN	ftp control	4408	3598076841	250971864	32762
471	18:15:41:6195 GMT	40	137.72.43.117	137.72.43.207	TCP	ACK	4408	ftp control	250971865	3598076842	65158

Disconnect Sequence

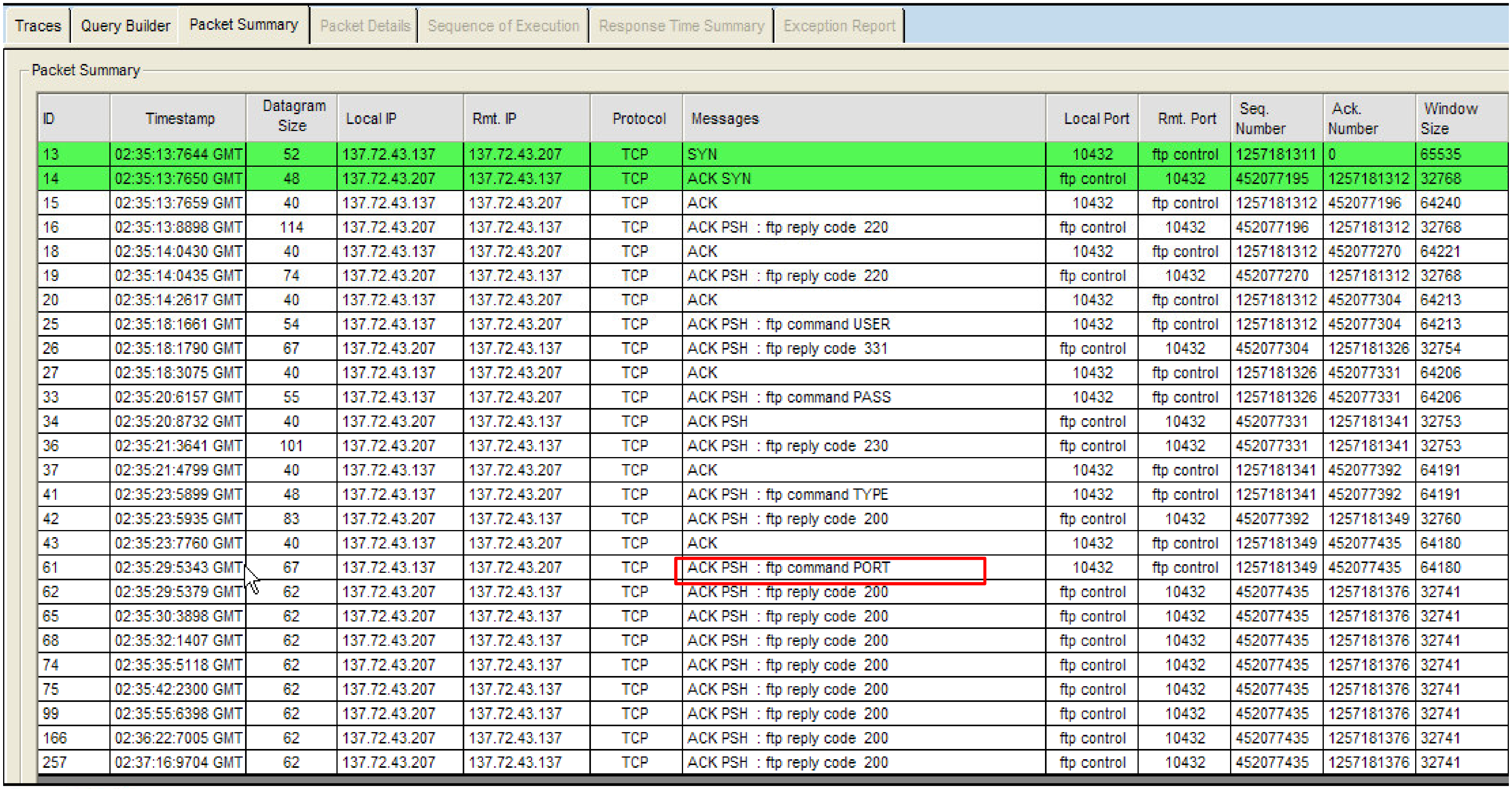
FTP Diagnosis



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	02:35:10:5649 GMT	78	137.72.43.45	137.72.43.255	UDP		137	137			
2	02:35:11:2518 GMT	1500	137.72.43.207	137.72.43.142	TCP	ACK : telnet : tn3270e data header	telnet	1215	424249748	4206849998	32760
3	02:35:11:2688 GMT	136	137.72.43.207	137.72.43.142	TCP	ACK PSH : telnet : 96 bytes of telnet data..	telnet	1215	424251208	4206849998	32760
4	02:35:11:2712 GMT	40	137.72.43.142	137.72.43.207	TCP	ACK	1215	telnet	4206849998	424251304	63748
5	02:35:11:2713 GMT	40	137.72.43.142	137.72.43.207	TCP	ACK	1215	telnet	4206849998	424251304	64240
6	02:35:11:2775 GMT	78	137.72.43.45	137.72.43.255	UDP		137	137			
7	02:35:11:6239 GMT	71	137.72.43.207	137.72.43.207	UDP	SNMP : Community - public(v1) : pdu -	14280	snmp ctrl			
8	02:35:11:6245 GMT	56	137.72.43.207	137.72.43.207	ICMP	Destination Unreachable : Port unreachable	0	0			
9	02:35:12:0784 GMT	48	137.72.43.142	137.72.43.207	TCP	ACK PSH : telnet : tn3270e data header	1215	telnet	4206849998	424251304	64240
10	02:35:12:0791 GMT	40	137.72.43.207	137.72.43.142	TCP	ACK PSH	telnet	1215	424251304	4206850006	32760
11	02:35:12:7799 GMT	1453	137.72.43.143	137.72.43.255	UDP		6646	6646			
12	02:35:12:7813 GMT	1453	137.72.43.142	137.72.43.255	UDP		6646	6646			
13	02:35:13:7644 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
14	02:35:13:7650 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	1257181312	32768
15	02:35:13:7659 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077196	64240
16	02:35:13:8898 GMT	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077196	1257181312	32768
17	02:35:13:9114 GMT	1453	137.72.43.108	137.72.43.255	UDP		6646	6646			
18	02:35:14:0430 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077270	64221
19	02:35:14:0435 GMT	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077270	1257181312	32768
20	02:35:14:2617 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077304	64213
21	02:35:14:3524 GMT	71	137.72.43.207	137.72.43.207	UDP	SNMP : Community - public(v1) : pdu - GetRequest	14278	snmp ctrl			
22	02:35:14:3531 GMT	56	137.72.43.207	137.72.43.207	ICMP	Destination Unreachable : Port unreachable	0	0			
23	02:35:16:7560 GMT	71	137.72.43.207	137.72.43.207	UDP	SNMP : Community - public(v1) : pdu -	14282	snmp ctrl			
24	02:35:16:7567 GMT	56	137.72.43.207	137.72.43.207	ICMP	Destination Unreachable : Port unreachable	0	0			
25	02:35:18:1661 GMT	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	10432	ftp control	1257181312	452077304	64213

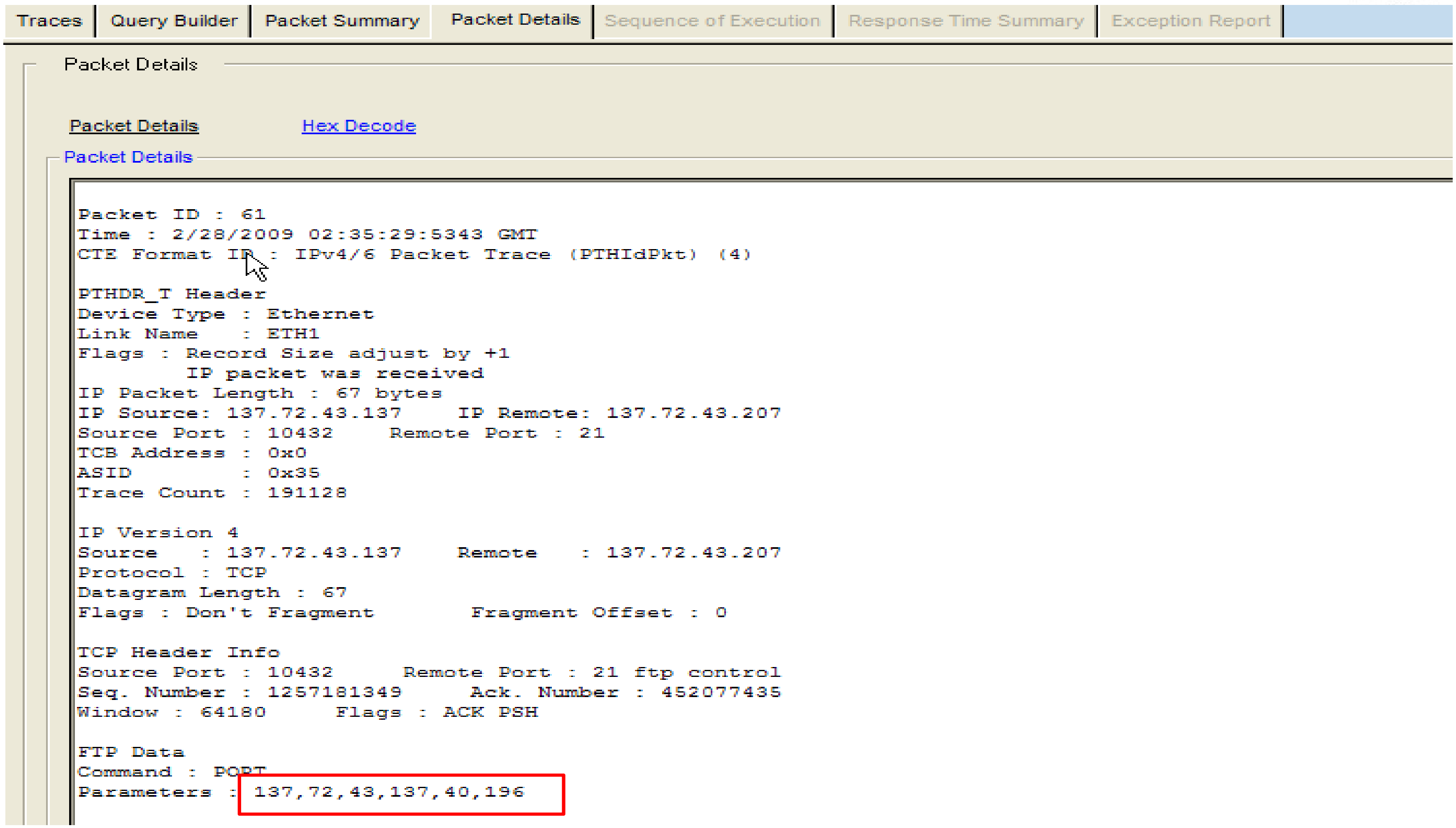
FTP Diagnosis – zoom in on FTP ports: Control connection vs. Data connection



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
13	02:35:13:7644 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
14	02:35:13:7650 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	1257181312	32768
15	02:35:13:7659 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077196	64240
16	02:35:13:8898 GMT	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077196	1257181312	32768
18	02:35:14:0430 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077270	64221
19	02:35:14:0435 GMT	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077270	1257181312	32768
20	02:35:14:2617 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077304	64213
25	02:35:18:1661 GMT	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	10432	ftp control	1257181312	452077304	64213
26	02:35:18:1790 GMT	67	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 331	ftp control	10432	452077304	1257181326	32754
27	02:35:18:3075 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181326	452077331	64206
33	02:35:20:6157 GMT	55	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PASS	10432	ftp control	1257181326	452077331	64206
34	02:35:20:8732 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH	ftp control	10432	452077331	1257181341	32753
36	02:35:21:3641 GMT	101	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 230	ftp control	10432	452077331	1257181341	32753
37	02:35:21:4799 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181341	452077392	64191
41	02:35:23:5899 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	10432	ftp control	1257181341	452077392	64191
42	02:35:23:5935 GMT	83	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077392	1257181349	32760
43	02:35:23:7760 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181349	452077435	64180
61	02:35:29:5343 GMT	67	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PORT	10432	ftp control	1257181349	452077435	64180
62	02:35:29:5379 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
65	02:35:30:3898 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
68	02:35:32:1407 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
74	02:35:35:5118 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
75	02:35:42:2300 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
99	02:35:55:6398 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
166	02:36:22:7005 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741
257	02:37:16:9704 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741

FTP Diagnosis – Analyze the PORT command



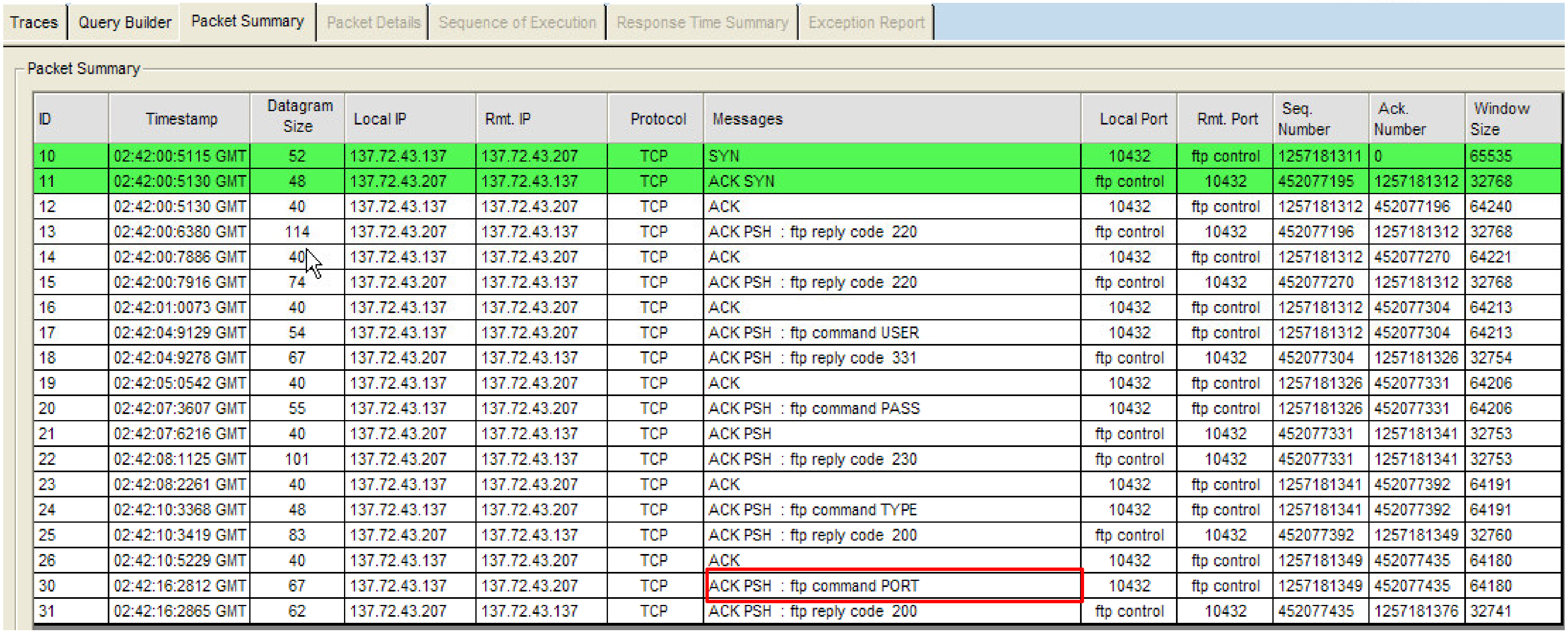
```
Packet ID : 61
Time : 2/28/2009 02:35:29:5343 GMT
CTE Format ID : IPv4/6 Packet Trace (PTHIdPkt) (4)

PTHDR_T Header
Device Type : Ethernet
Link Name   : ETH1
Flags : Record Size adjust by +1
        IP packet was received
IP Packet Length : 67 bytes
IP Source: 137.72.43.137    IP Remote: 137.72.43.207
Source Port : 10432     Remote Port : 21
TCB Address : 0x0
ASID        : 0x35
Trace Count : 191128

IP Version 4
Source    : 137.72.43.137    Remote    : 137.72.43.207
Protocol : TCP
Datagram Length : 67
Flags : Don't Fragment        Fragment Offset : 0

TCP Header Info
Source Port : 10432      Remote Port : 21 ftp control
Seq. Number : 1257181349      Ack. Number : 452077435
Window : 64180      Flags : ACK PSH

FTP Data
Command : PORT
Parameters : 137,72,43,137,40,196
```

FTP Diagnosis – Analyze the PORT command continued

PORT 137,72,43,137,40,196

- Specifies that the FTP Server will initiate the data connection
- Client's IP Address: 137.72.43.137
- Client's Port: 40 * 256 + 196 = 10436
- Expect to see a SYN packet:
  - from server (137.72.43.207)
  - to client (137.72.43.137)

FTP Diagnosis – check the equivalent Sniffer trace



ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
10	02:42:00:5115 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
11	02:42:00:5130 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	1257181312	32768
12	02:42:00:5130 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077196	64240
13	02:42:00:6380 GMT	114	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077196	1257181312	32768
14	02:42:00:7886 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077270	64221
15	02:42:00:7916 GMT	74	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 220	ftp control	10432	452077270	1257181312	32768
16	02:42:01:0073 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181312	452077304	64213
17	02:42:04:9129 GMT	54	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command USER	10432	ftp control	1257181312	452077304	64213
18	02:42:04:9278 GMT	67	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 331	ftp control	10432	452077304	1257181326	32754
19	02:42:05:0542 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181326	452077331	64206
20	02:42:07:3607 GMT	55	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PASS	10432	ftp control	1257181326	452077331	64206
21	02:42:07:6216 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH	ftp control	10432	452077331	1257181341	32753
22	02:42:08:1125 GMT	101	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 230	ftp control	10432	452077331	1257181341	32753
23	02:42:08:2261 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181341	452077392	64191
24	02:42:10:3368 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	10432	ftp control	1257181341	452077392	64191
25	02:42:10:3419 GMT	83	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077392	1257181349	32760
26	02:42:10:5229 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	10432	ftp control	1257181349	452077435	64180
30	02:42:16:2812 GMT	67	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PORT	10432	ftp control	1257181349	452077435	64180
31	02:42:16:2865 GMT	62	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	10432	452077435	1257181376	32741

FTP Diagnosis

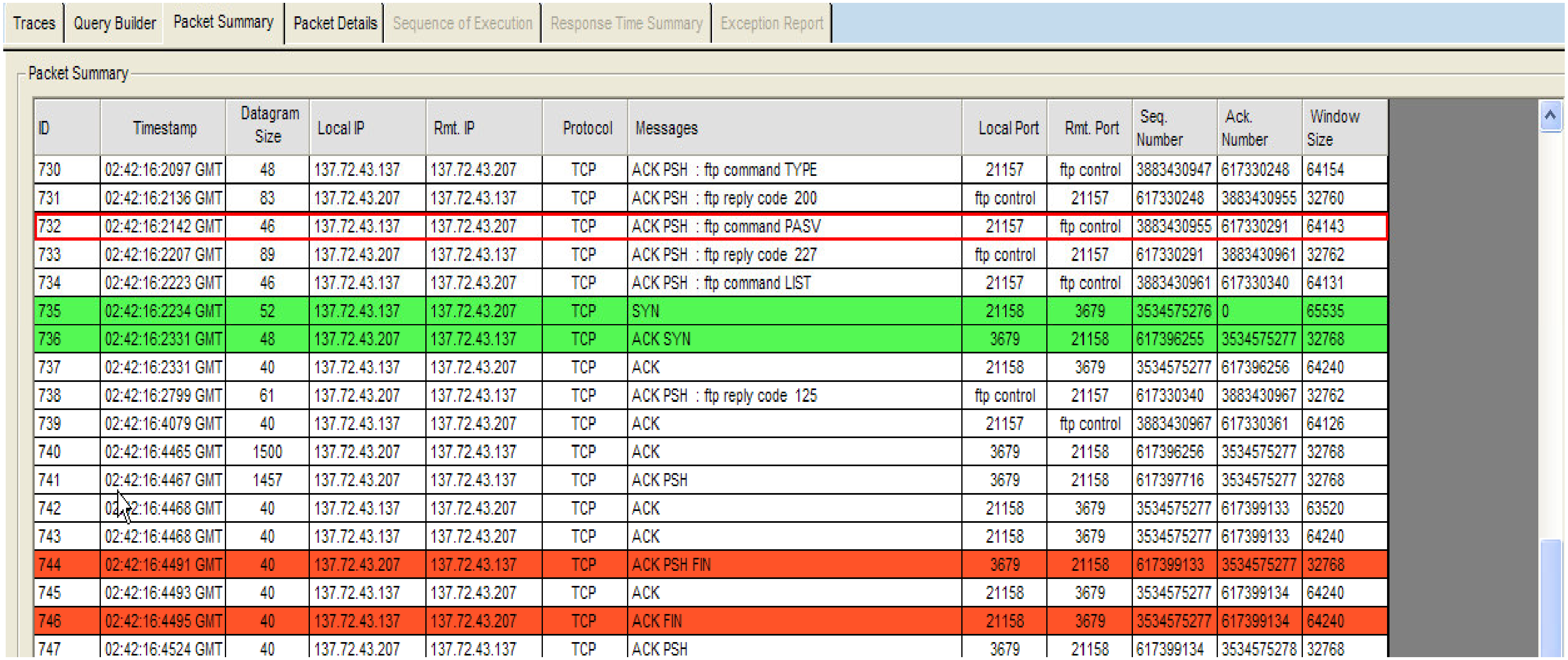
Sniffer trace shows the PORT command was sent to the server but there was no SYN packet coming in – SYN packet was “lost”

Might be related to firewall issues - check firewall setting, FTP.DATA and TCP PROFILE settings.

Passive FTP:

- Client initiates the data connection.
- Check to reply to the PASV command to determine the IP address and Port number of the server for the data connection.

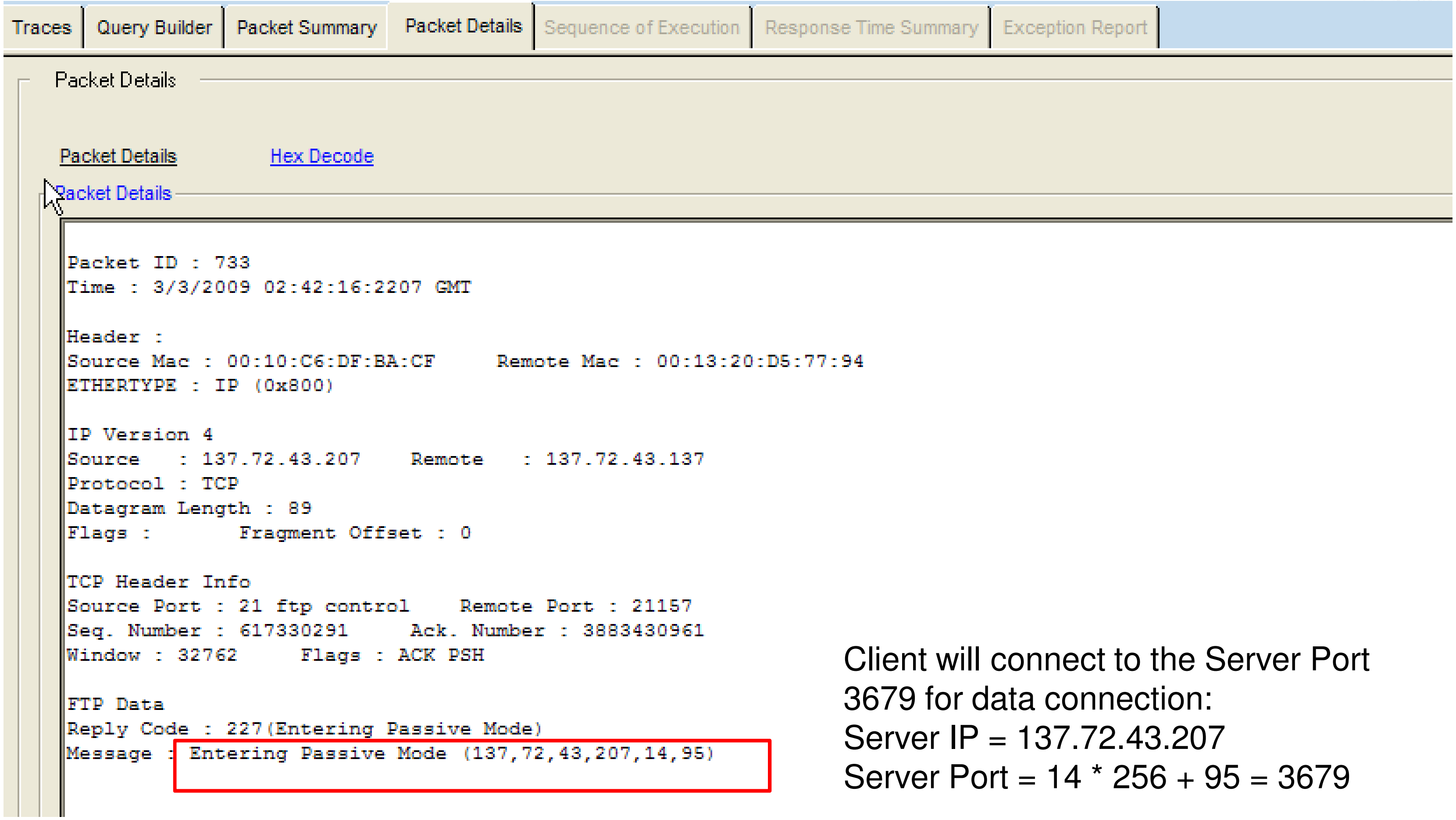
FTP Diagnosis – Passive FTP



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
730	02:42:16:2097 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	21157	ftp control	3883430947	617330248	64154
731	02:42:16:2136 GMT	83	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 200	ftp control	21157	617330248	3883430955	32760
732	02:42:16:2142 GMT	46	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command PASV	21157	ftp control	3883430955	617330291	64143
733	02:42:16:2207 GMT	89	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 227	ftp control	21157	617330291	3883430961	32762
734	02:42:16:2223 GMT	46	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command LIST	21157	ftp control	3883430961	617330340	64131
735	02:42:16:2234 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	21158	3679	3534575276	0	65535
736	02:42:16:2331 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	3679	21158	617396255	3534575277	32768
737	02:42:16:2331 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617396256	64240
738	02:42:16:2799 GMT	61	137.72.43.207	137.72.43.137	TCP	ACK PSH : ftp reply code 125	ftp control	21157	617330340	3883430967	32762
739	02:42:16:4079 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21157	ftp control	3883430967	617330361	64126
740	02:42:16:4465 GMT	1500	137.72.43.207	137.72.43.137	TCP	ACK	3679	21158	617396256	3534575277	32768
741	02:42:16:4467 GMT	1457	137.72.43.207	137.72.43.137	TCP	ACK PSH	3679	21158	617397716	3534575277	32768
742	02:42:16:4468 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617399133	63520
743	02:42:16:4468 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617399133	64240
744	02:42:16:4491 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH FIN	3679	21158	617399133	3534575277	32768
745	02:42:16:4493 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK	21158	3679	3534575277	617399134	64240
746	02:42:16:4495 GMT	40	137.72.43.137	137.72.43.207	TCP	ACK FIN	21158	3679	3534575277	617399134	64240
747	02:42:16:4524 GMT	40	137.72.43.207	137.72.43.137	TCP	ACK PSH	3679	21158	617399134	3534575278	32768

FTP Diagnosis – Analyze the PASV Reply



```
Packet ID : 733
Time : 3/3/2009 02:42:16:2207 GMT

Header :
Source Mac : 00:10:C6:DF:BA:CF     Remote Mac : 00:13:20:D5:77:94
ETHERTYPE : IP (0x800)

IP Version 4
Source    : 137.72.43.207    Remote    : 137.72.43.137
Protocol : TCP
Datagram Length : 89
Flags :        Fragment Offset : 0

TCP Header Info
Source Port : 21 ftp control    Remote Port : 21157
Seq. Number : 617330291     Ack. Number : 3883430961
Window : 32762     Flags : ACK PSH

FTP Data
Reply Code : 227(Entering Passive Mode)
Message : Entering Passive Mode (137,72,43,207,14,95)
```

Client will connect to the Server Port 3679 for data connection:
Server IP = 137.72.43.207
Server Port = 14 * 256 + 95 = 3679

Know Your Protocols and Applications - IP

IP is an unreliable, connectionless, unacknowledged protocol

- IP Functions
- IP Fundamentals
- IP Sequence of Events

IP Functions

- Delivery of datagrams across a network of connected networks
- Addressing – Classful, Subnetting
- Data Encapsulation and Packaging
- Fragmentation and Reassembly
- Direct and Indirect Delivery

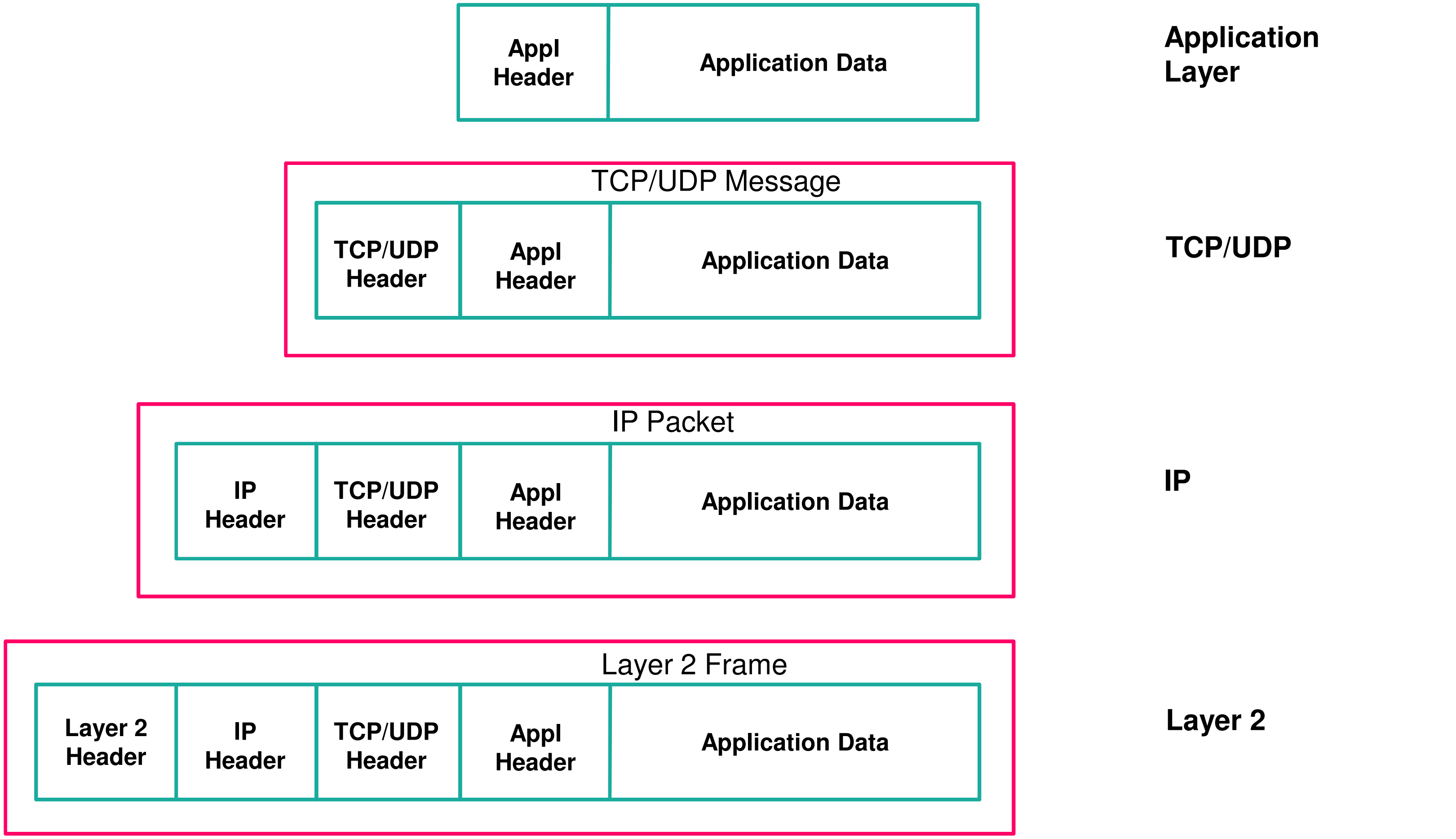
IP Fundamentals

- RFC 791 – IPv4 – There was no 1, 2 or 3!
- Addressing
  - Classful - Network Bits & Host Bits
    - A - 8 Network, 24 Host **1**.0.0.0 to **126.** 255.255.255
    - B - 16 Network, 16 Host **128.0**.0.0 to **191.255**.255.255
    - C - 28 Network, 8 Host **192.0.0**.0 to **223. 255.255.255**
    - D - n/a – multicasting 224.0.0.0 to 239. 255.255.255
    - E - n/a – experimental 240.0.0.0 to 255. 255.255.255
  - IP Addresses with special connotations
    - 0.0.0.0 – refers to this device (When it does not know its address)
    - 255.255.255.255 – broadcast address – to all hosts on <u>this</u> network
  - Reserved, Private and Loopback Addresses
    - Reserved – blocks of addresses set aside with no defined purpose at this time
    - Private – Allows the creation of private internets – RFC 1918 – Unroutable addresses to the public internet
      - *10.0.0.0 – 10.255.255.255*
      - *172.16.0.0 – 172.31.255.255*
      - *192.168.0.0 – 192.168.255.255*
    - Loopback - 127.0.0.0. to 127.255.255.255 - used for testing purposes

IP Fundamentals

- Addressing – continued
  - Subnetting – RFC 950 adds subnetworks to a network
  - Host is broken into Subnet and Host
  - Facilitates breaking a large network into groups of smaller networks
- Encapsulation and Formatting
  - Interprotocol Operation
  - Data is passed down to the lower layers of the OSI Model
  - Each Lower Layer Encapsulates the message with it’s own format
  - IP Receives messages from TCP and UDP
  - IP adds its header information to the message

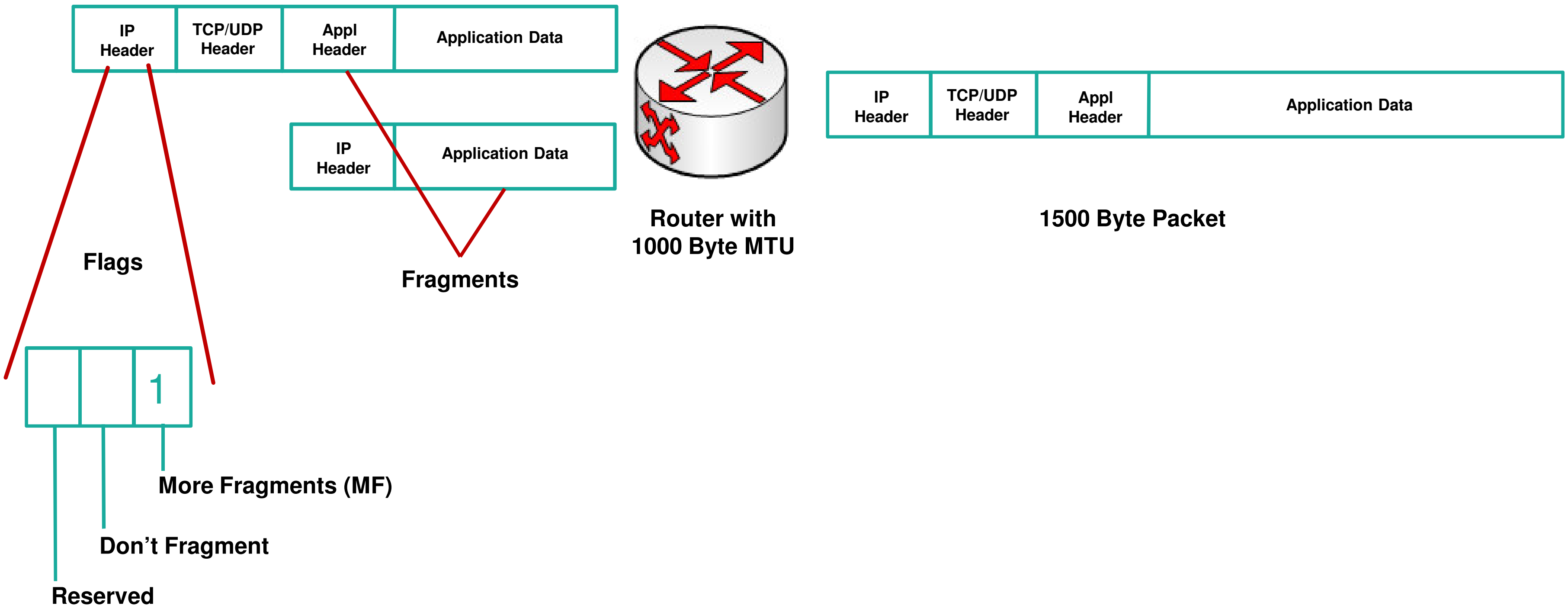
Encapsulation & Packaging



IP Fragmentation and Reassembly

- Fragmentation and Reassembly
  - MTU – The Maximum Transmission Unit of a Device is Smaller than the Incoming Packet Size
  - Reassembly is done at the destination device
  - Try to Avoid – Causes More Work for the Network Devices
    - More packets to route
    - More data is routed (additional bytes due to headers on the fragments)
    - Reassembly uses CPU at the destination device
  - Fragments may also be fragmented if they go through a device with a smaller MTU!

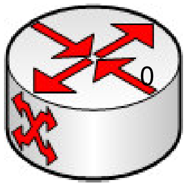
IP Fragmentation and Reassembly



IP Fragmentation and Reassembly

MF	Offset	Data – 8980 Bytes
0	0	

9000 byte packet – 8980 data + 20 byte IP Header



3300 byte MTU Device

MF	Offset	Data – 3280 Bytes
1	0	

3300 byte packet – 3280 data + 20 byte IP Header

MF	Offset	Data – 3280 Bytes
1	410	

3300 byte packet – 3280 data + 20 byte IP Header

MF	Offset	Data – 2420 Bytes
0	820	

2440 byte packet – 2420 data + 20 byte IP Header

IP Reassembly

- Fragment Recognition
  - The MF flag is set and the Fragment Offset has a value other than 0
  - Fragmented message is identified by:
    - Source and Destination IP address
    - Protocol in the header
    - Identification field
- Buffer Initialization
  - Created to store fragments as they arrive
  - Keeps track of which portions are filled (Offset determine where in the buffer the fragment will be)

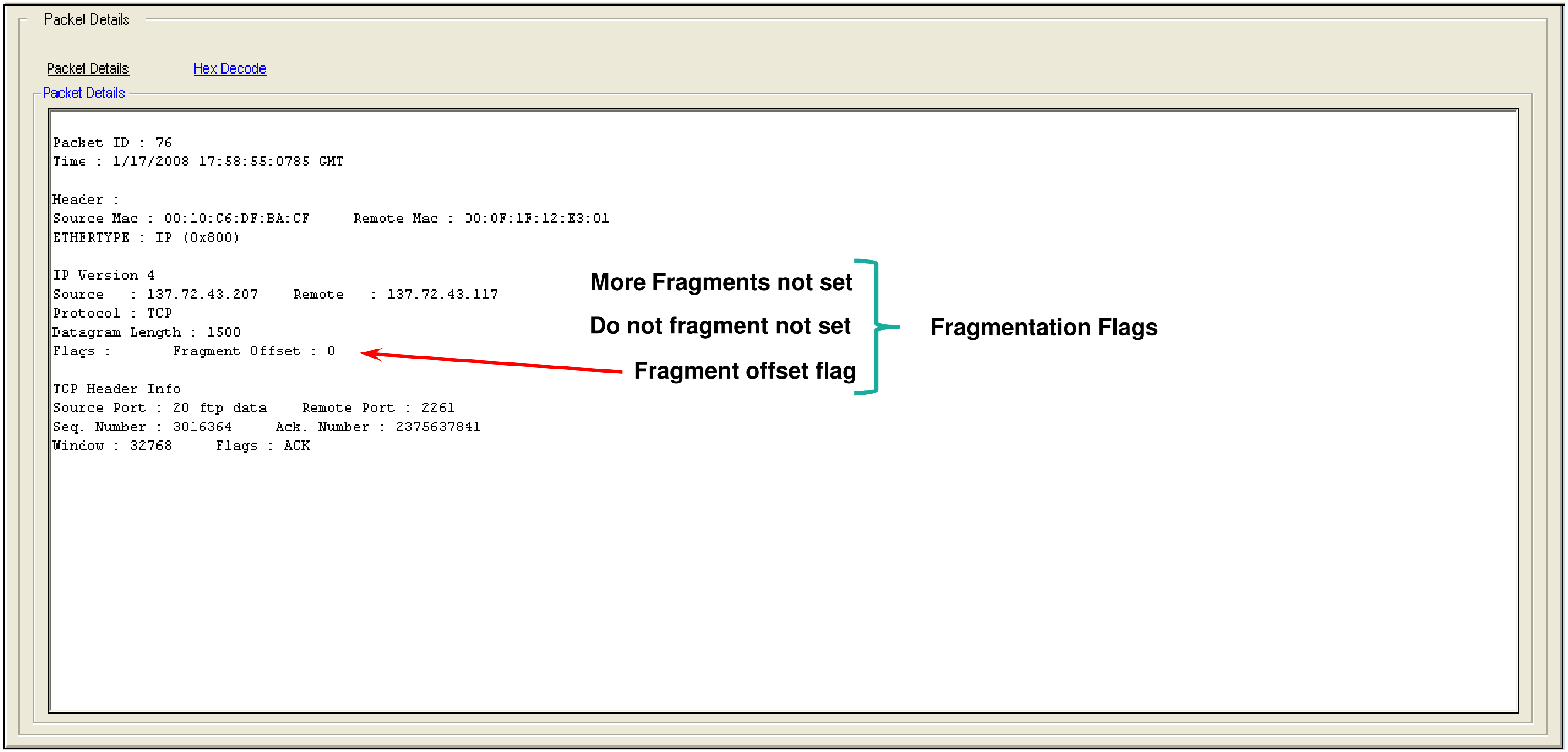
IP Reassembly

- Timer Initialization
  - Timer ensures that the receiving device doesn't wait forever for IP fragments to arrive
  - IP relies in the upper layer to notify the sender the packet was not received
- Fragment Receipt and Processing
  - When a fragment arrives, it is placed in the buffer
  - When the packet is completely reassembled, it is processed as an unfragmented packet

Direct and Indirect Delivery

- Direct Delivery
  - Packets are sent between two devices on the same physical network
- Indirect Delivery (Routing)
  - Packets are sent between two devices on a different physical network
  - Packets go through routers to get to the final destination

IP Header



```
Packet ID : 76
Time : 1/17/2008 17:58:55:0785 GMT

Header :
Source Mac : 00:10:C6:DF:BA:CF     Remote Mac : 00:0F:1F:12:E3:01
ETHERTYPE : IP (0x800)

IP Version 4
Source   : 137.72.43.207    Remote   : 137.72.43.117
Protocol : TCP
Datagram Length : 1500
Flags :        Fragment Offset : 0

TCP Header Info
Source Port : 20 ftp data    Remote Port : 2261
Seq. Number : 3016364     Ack. Number : 2375637841
Window : 32768     Flags : ACK
```

More Fragments not set

Do not fragment not set

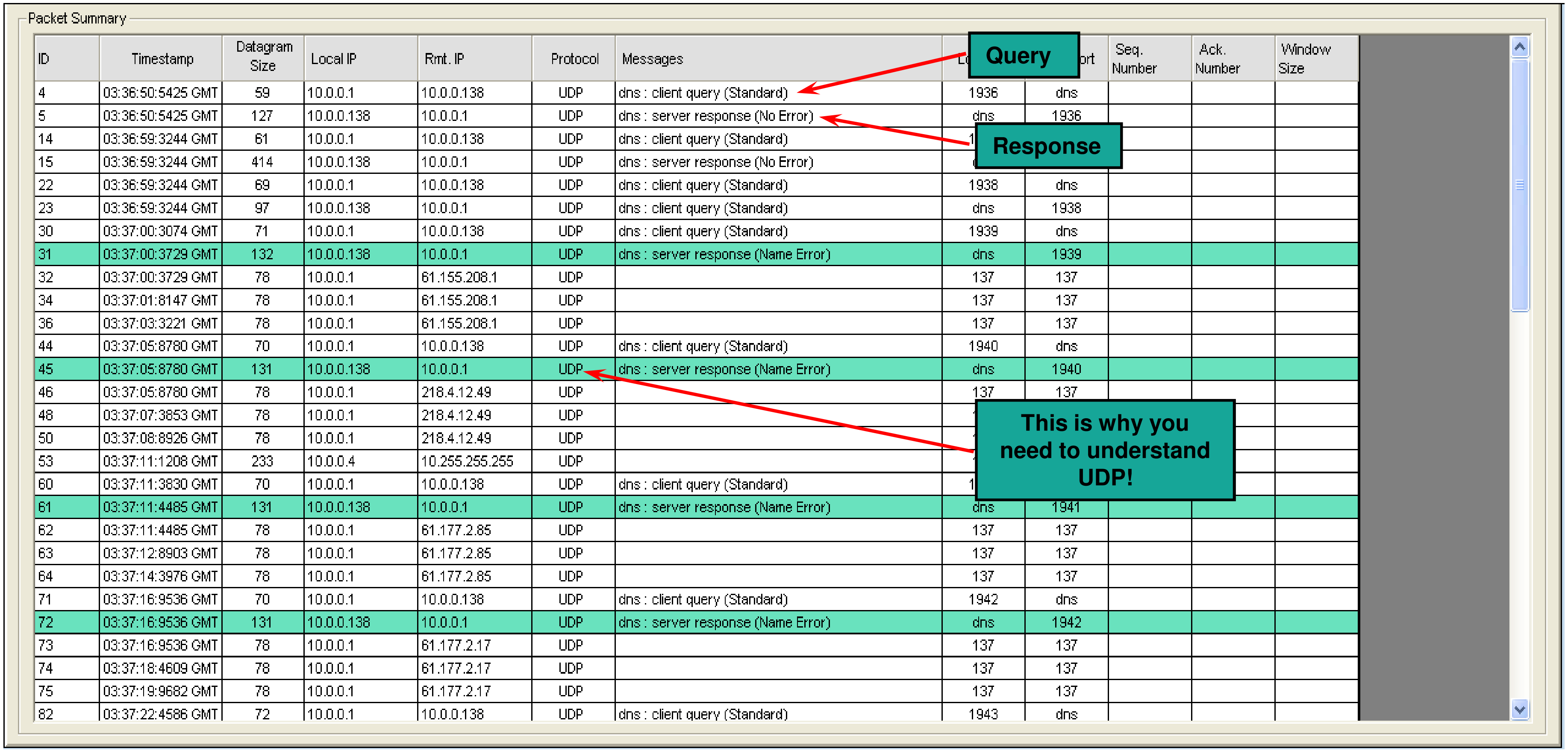
Fragment offset flag

Fragmentation Flags

Working Our Way Through a DNS Trace

- Case #1 – A successful DNS query
  - Submit a name for an IP Address Request
- Case #2 – A failed DNS query
  - Name does not exist

DNS Query Packets



Packet Summary

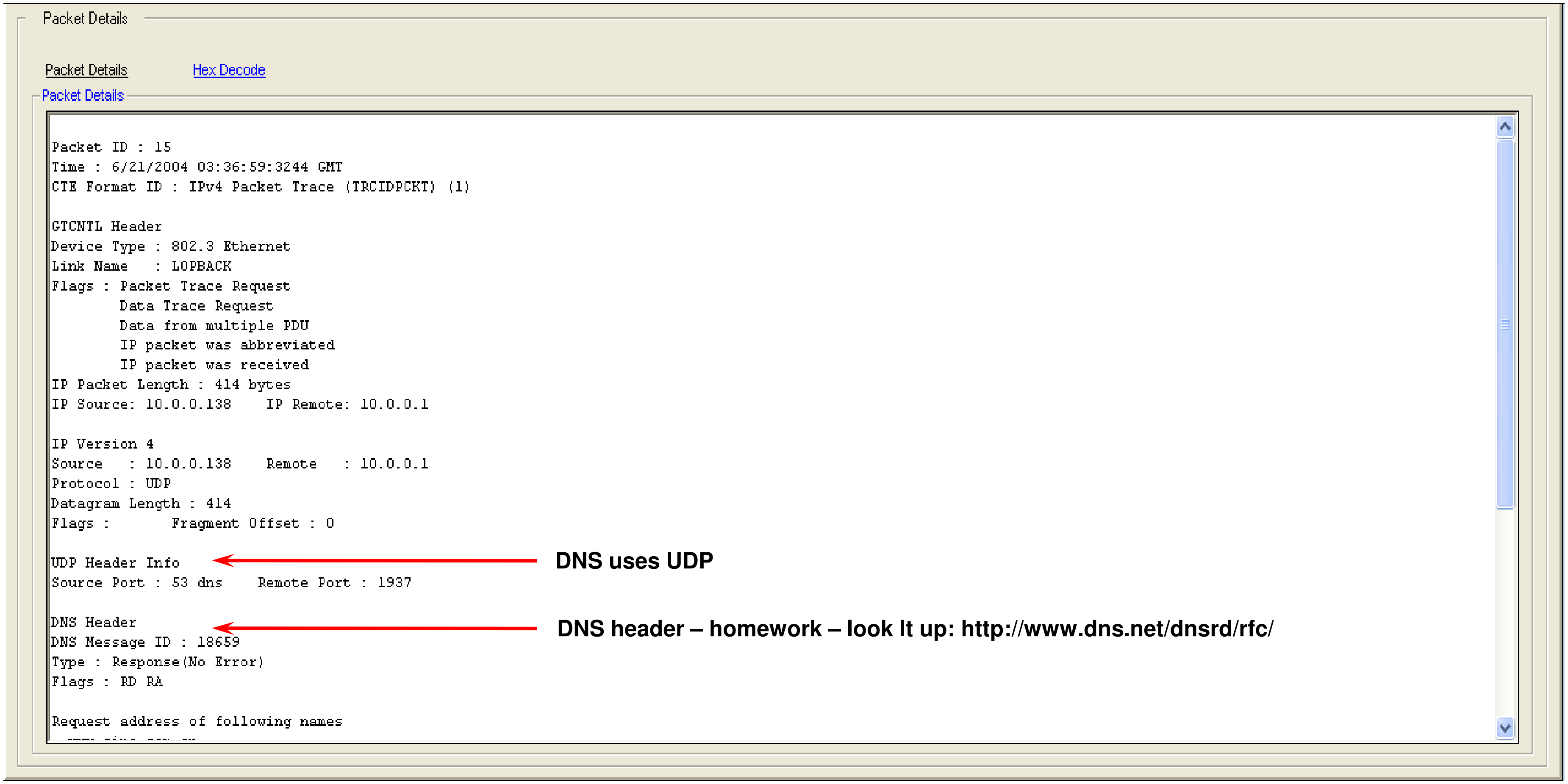
ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Lo	ort	Seq. Number	Ack. Number	Window Size
4	03:36:50:5425 GMT	59	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1936	dns			
5	03:36:50:5425 GMT	127	10.0.0.138	10.0.0.1	UDP	dns : server response (No Error)	dns	1936			
14	03:36:59:3244 GMT	61	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1	[illegible]			
15	03:36:59:3244 GMT	414	10.0.0.138	10.0.0.1	UDP	dns : server response (No Error)	[illegible]	[illegible]			
22	03:36:59:3244 GMT	69	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1938	dns			
23	03:36:59:3244 GMT	97	10.0.0.138	10.0.0.1	UDP	dns : client query (Standard)	dns	1938			
30	03:37:00:3074 GMT	71	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1939	dns			
31	03:37:00:3729 GMT	132	10.0.0.138	10.0.0.1	UDP	dns : server response (Name Error)	dns	1939			
32	03:37:00:3729 GMT	78	10.0.0.1	61.155.208.1	UDP		137	137			
34	03:37:01:8147 GMT	78	10.0.0.1	61.155.208.1	UDP		137	137			
36	03:37:03:3221 GMT	78	10.0.0.1	61.155.208.1	UDP		137	137			
44	03:37:05:8780 GMT	70	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1940	dns			
45	03:37:05:8780 GMT	131	10.0.0.138	10.0.0.1	UDP	dns : server response (Name Error)	dns	1940			
46	03:37:05:8780 GMT	78	10.0.0.1	218.4.12.49	UDP		137	137			
48	03:37:07:3853 GMT	78	10.0.0.1	218.4.12.49	UDP		[illegible]	[illegible]			
50	03:37:08:8926 GMT	78	10.0.0.1	218.4.12.49	UDP		[illegible]	[illegible]			
53	03:37:11:1208 GMT	233	10.0.0.4	10.255.255.255	UDP		[illegible]	[illegible]			
60	03:37:11:3830 GMT	70	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1	[illegible]			
61	03:37:11:4485 GMT	131	10.0.0.138	10.0.0.1	UDP	dns : server response (Name Error)	dns	1941			
62	03:37:11:4485 GMT	78	10.0.0.1	61.177.2.85	UDP		137	137			
63	03:37:12:8903 GMT	78	10.0.0.1	61.177.2.85	UDP		137	137			
64	03:37:14:3976 GMT	78	10.0.0.1	61.177.2.85	UDP		137	137			
71	03:37:16:9536 GMT	70	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1942	dns			
72	03:37:16:9536 GMT	131	10.0.0.138	10.0.0.1	UDP	dns : server response (Name Error)	dns	1942			
73	03:37:16:9536 GMT	78	10.0.0.1	61.177.2.17	UDP		137	137			
74	03:37:18:4609 GMT	78	10.0.0.1	61.177.2.17	UDP		137	137			
75	03:37:19:9682 GMT	78	10.0.0.1	61.177.2.17	UDP		137	137			
82	03:37:22:4586 GMT	72	10.0.0.1	10.0.0.138	UDP	dns : client query (Standard)	1943	dns			

Query

Response

This is why you need to understand UDP!

A successful DNS query

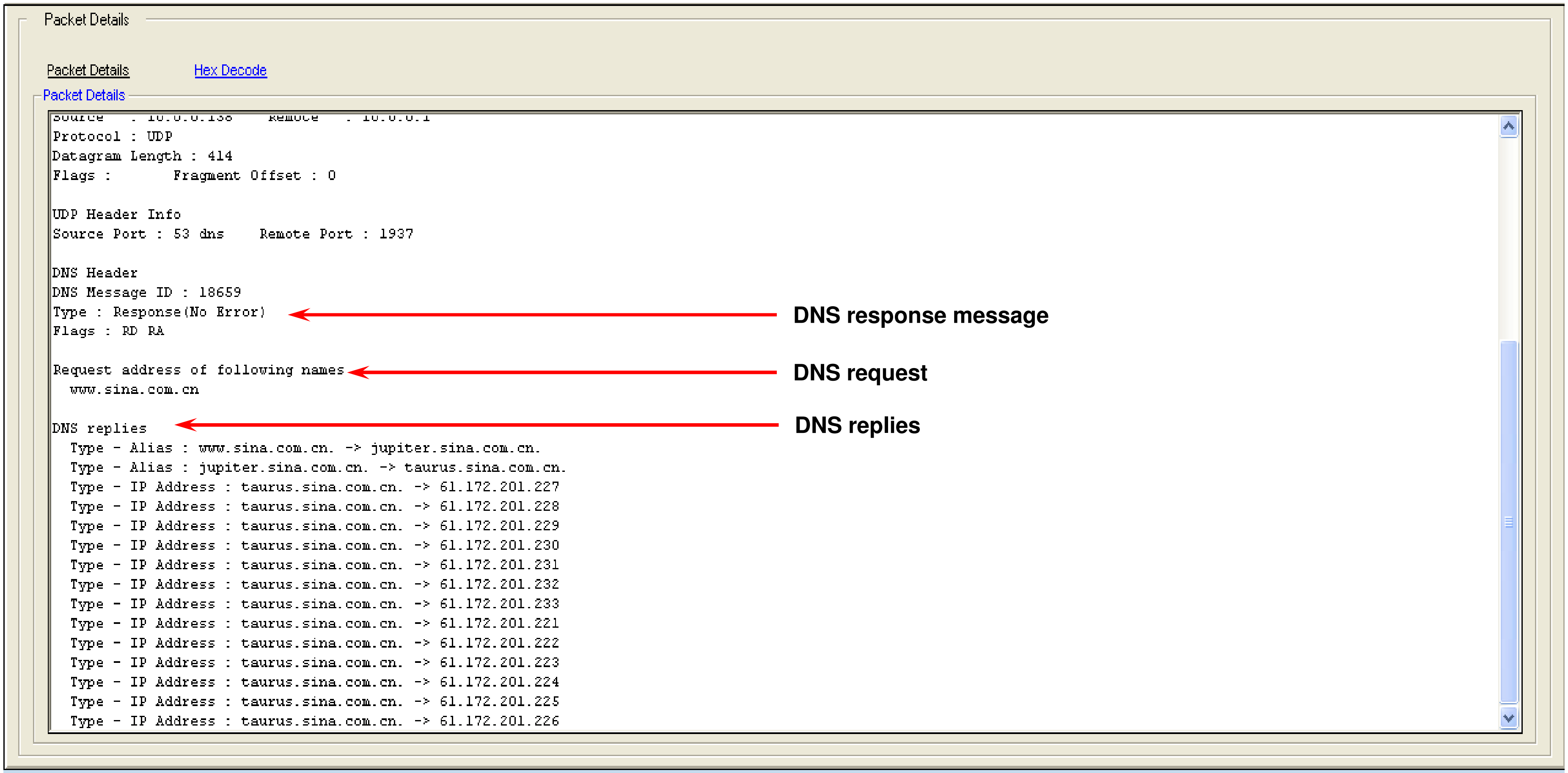


```
Packet ID : 15
Time : 6/21/2004 03:36:59:3244 GMT
CTE Format ID : IPv4 Packet Trace (TRCIDPCKT) (1)

GTCNTL Header
Device Type : 802.3 Ethernet
Link Name   : LOPBACK
Flags : Packet Trace Request
        Data Trace Request
        Data from multiple PDU
        IP packet was abbreviated
        IP packet was received
IP Packet Length : 414 bytes
IP Source: 10.0.0.138    IP Remote: 10.0.0.1

IP Version 4
Source   : 10.0.0.138    Remote   : 10.0.0.1
Protocol : UDP
Datagram Length : 414
Flags :       Fragment Offset : 0

UDP Header Info
Source Port : 53 dns    Remote Port : 1937

DNS Header
DNS Message ID : 18659
Type : Response(No Error)
Flags : RD RA

Request address of following names
```

DNS uses UDP

DNS header – homework – look It up: http://www.dns.net/dnsrd/rfc/

A successful DNS query



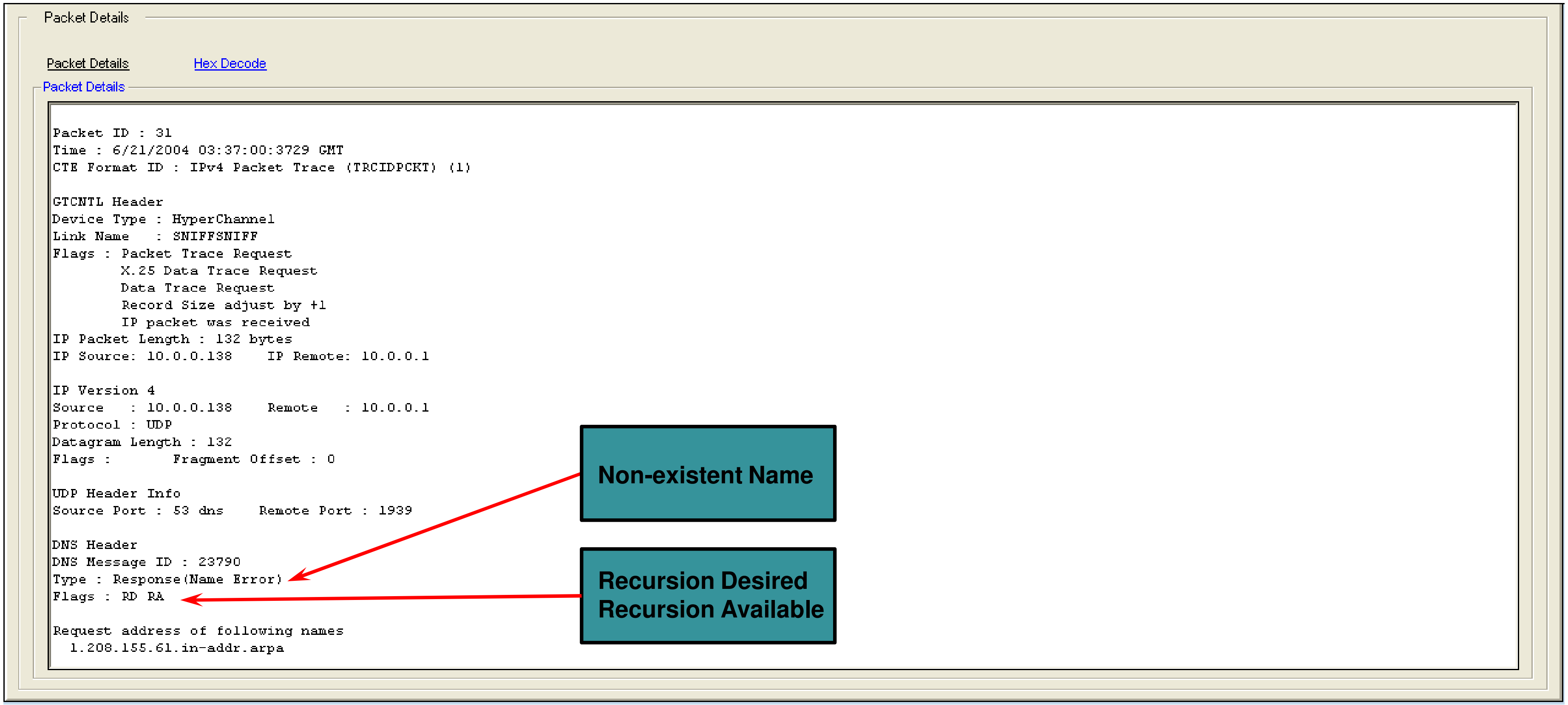
```
Source   : 10.0.0.138    Remote   : 10.0.0.1
Protocol : UDP
Datagram Length : 414
Flags :       Fragment Offset : 0

UDP Header Info
Source Port : 53 dns    Remote Port : 1937

DNS Header
DNS Message ID : 18659
Type : Response(No Error)
Flags : RD RA

Request address of following names
  www.sina.com.cn

DNS replies
  Type - Alias : www.sina.com.cn. -> jupiter.sina.com.cn.
  Type - Alias : jupiter.sina.com.cn. -> taurus.sina.com.cn.
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.227
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.228
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.229
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.230
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.231
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.232
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.233
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.221
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.222
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.223
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.224
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.225
  Type - IP Address : taurus.sina.com.cn. -> 61.172.201.226
```

DNS response message

DNS request

DNS replies

A failed DNS query



```
Packet ID : 31
Time : 6/21/2004 03:37:00:3729 GMT
CTE Format ID : IPv4 Packet Trace (TRCIDPCKT) (1)

GTCNTL Header
Device Type : HyperChannel
Link Name   : SNIFFSNIFF
Flags : Packet Trace Request
        X.25 Data Trace Request
        Data Trace Request
        Record Size adjust by +1
        IP packet was received
IP Packet Length : 132 bytes
IP Source: 10.0.0.138    IP Remote: 10.0.0.1

IP Version 4
Source   : 10.0.0.138    Remote   : 10.0.0.1
Protocol : UDP
Datagram Length : 132
Flags :      Fragment Offset : 0

UDP Header Info
Source Port : 53 dns    Remote Port : 1939

DNS Header
DNS Message ID : 23790
Type : Response(Name Error)
Flags : RD RA

Request address of following names
  1.208.155.61.in-addr.arpa
```

Non-existent Name

Recursion Desired
Recursion Available

Know Your Protocols and Applications - UDP

User Datagram Protocol

- RFC 768 – 3 Pages long!
- Simple and Fast
- Applications do not require Acknowledgement, Reliability or Message Flow Control
- Messages can be lost with no consequence

Know Your Protocols and Applications – UDP Message Format

- Pseudo Header (Prepended to the UDP Datagram 12 bytes)
  - IP Source Address
  - IP Destination Address
  - IP Protocol Field
  - UDP Length Field
- UDP Header (8 Bytes)
  - Source Port
  - Destination Port
  - Length
  - Checksum (Pseudo Header and Header only)
- Data – Variable Length

Know Your Protocols and Applications – UDP

UDP Applications

- Bootstrap Protocol - BOOTP
- Dynamic Host Configuration Protocol – DHCP
- Domain Name Services – DNS
- Enterprise Extender - EE
- Router Information Protocol – RIP-1, RIP-2
- Simple Network Management Protocol – SNMP
- Trivial File Transfer Protocol – TFTP

Enterprise Extender

- SNA Transport over UDP ‘Pipelines’ through IP cloud
- No changes to SNA applications, just Comm. Server
- Requires correlated VTAM – TCP/IP definitions and priorities

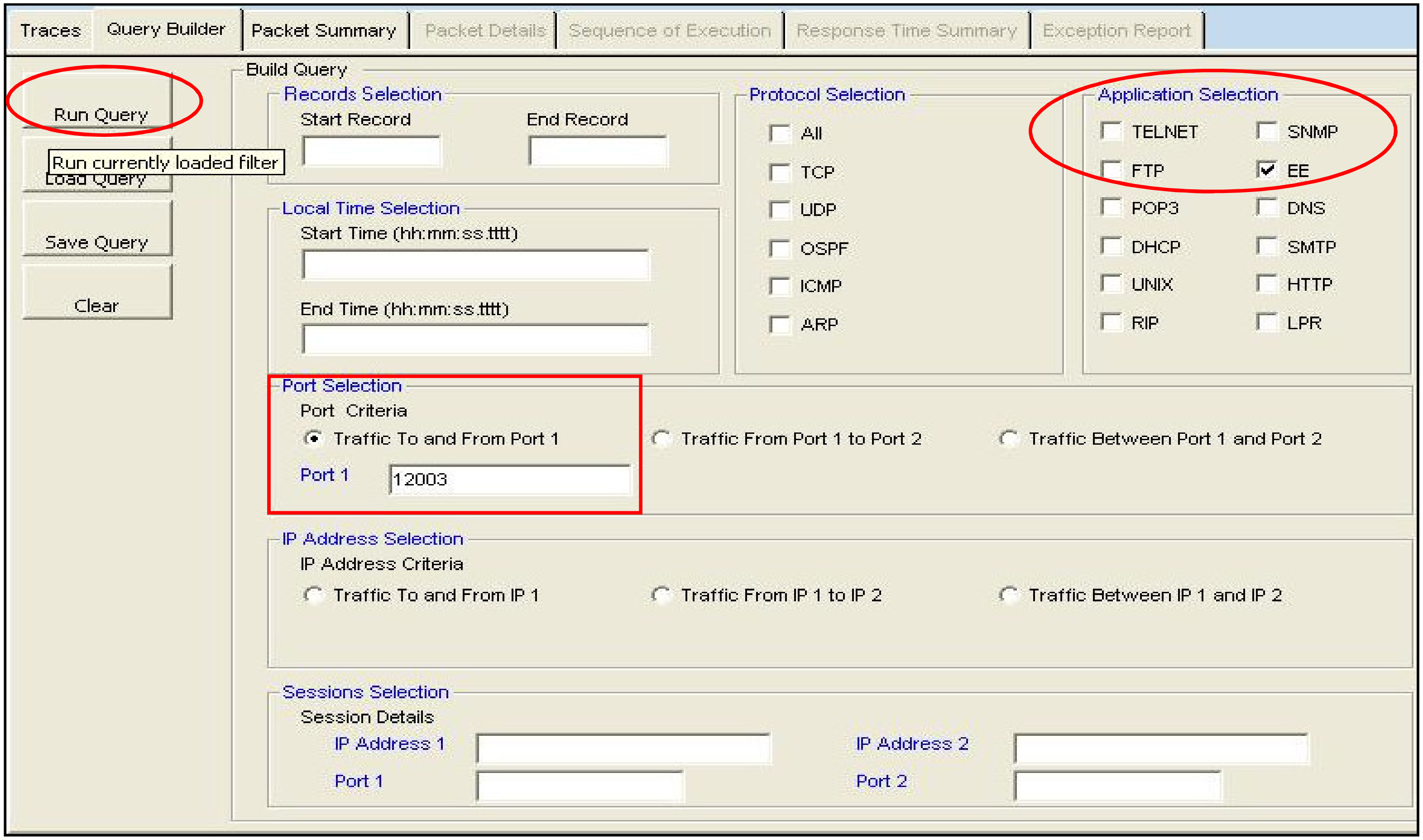
  - VTAM XCA Node & Switched Node - COS match w/ Remote CP
  - IP Link = IUTSAMEH, UDP Ports based on TOS priorities
  - 12000 (C0 = net/control TOS) up to 12004 (20 = low TOS)

Enterprise Extender

- SNA “handshaking” still happens at “lowest level”
  (Preserves SNA error checking/handling)

- With 3 packet header additions for routing flow control…
  1) Rapid Transport Protocol (RTP)
     “Hybrid” routing layer between IP/UDP packets & SNA
  2) Automatic Network Routing (ANR)
     Correlation between IP-style priorities (TOS) and…
     SNA-style session and path priorities (COS and TG’s)
  3) First, Adaptive Rate-Based Flow (ARB), now ARB2
     Provides algorithm to better handle performance
     Avoids potential “lost data” issues since connectionless

Enterprise Extender Packet Filtering



Build Query

Records Selection

Start Record

End Record

Local Time Selection

Start Time (hh:mm:ss.tttt)

End Time (hh:mm:ss.tttt)

Protocol Selection

□ All
□ TCP
□ UDP
□ OSPF
□ ICMP
□ ARP

Application Selection

□ TELNET	□ SNMP
□ FTP	☑ EE
□ POP3	□ DNS
□ DHCP	□ SMTP
□ UNIX	□ HTTP
□ RIP	□ LPR

Port Selection

Port Criteria

● Traffic To and From Port 1 ○ Traffic From Port 1 to Port 2 ○ Traffic Between Port 1 and Port 2

Port 1: 12003

IP Address Selection

IP Address Criteria

○ Traffic To and From IP 1 ○ Traffic From IP 1 to IP 2 ○ Traffic Between IP 1 and IP 2

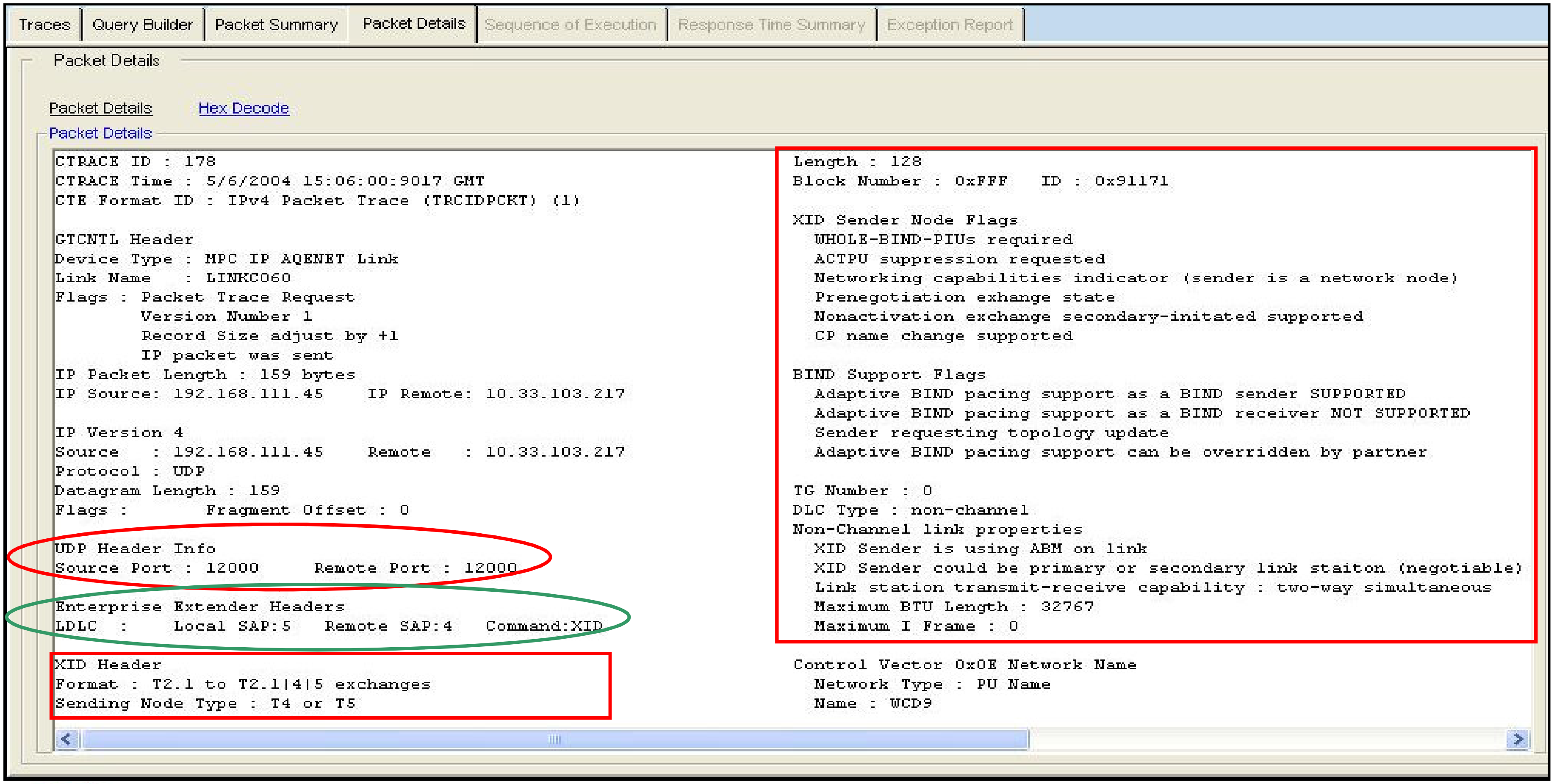
Sessions Selection

Session Details

IP Address 1 IP Address 2

Port 1 Port 2

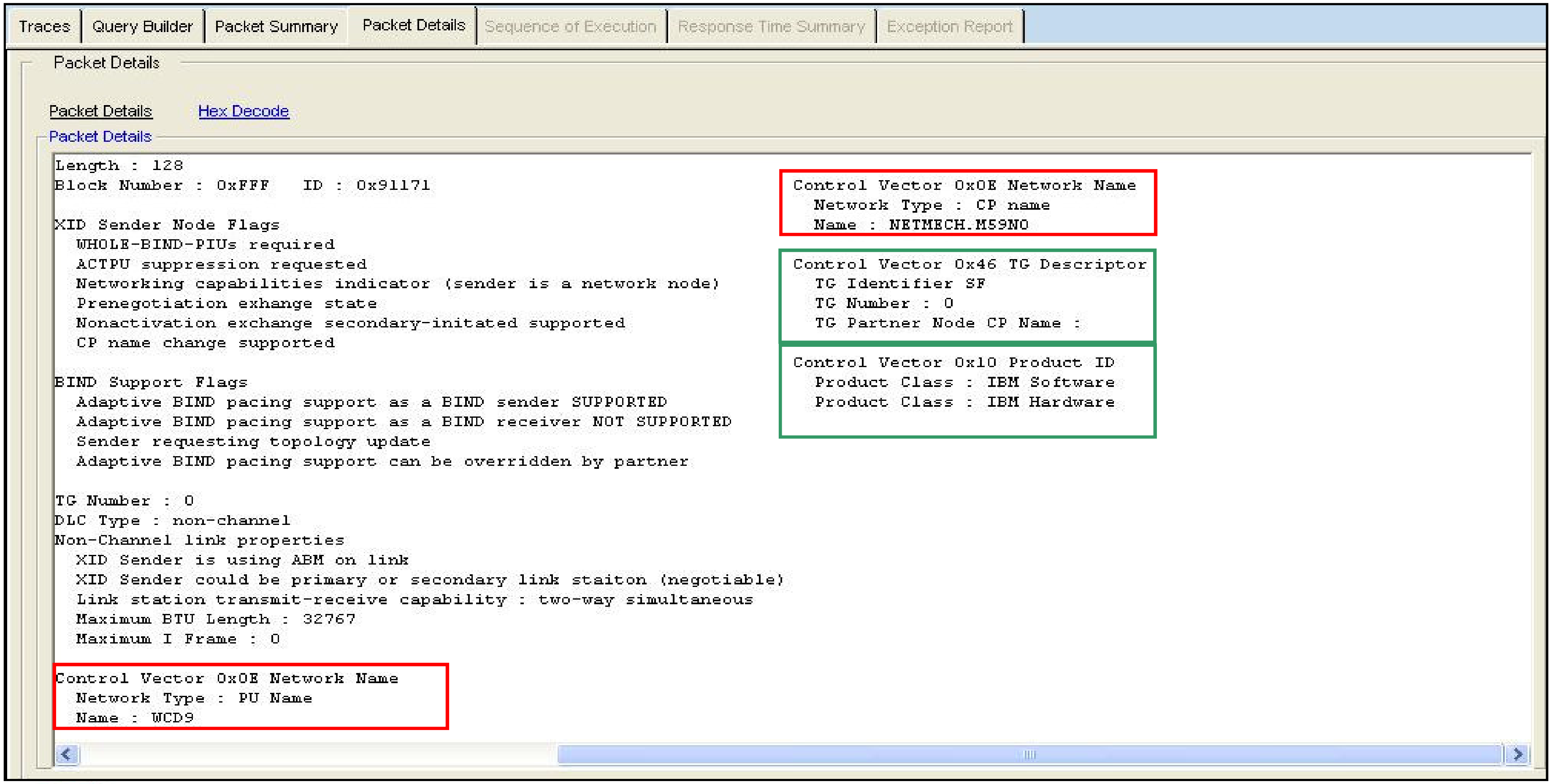
EE XID Init Packet: ‘Packet Details’ (Record #178 - Part 1)



```
CTRACE ID : 178
CTRACE Time : 5/6/2004 15:06:00:9017 GMT
CTE Format ID : IPv4 Packet Trace (TRCIDPCKT) (1)

GTCNTL Header
Device Type : MPC IP AQENET Link
Link Name    : LINKC060
Flags : Packet Trace Request
        Version Number 1
        Record Size adjust by +1
        IP packet was sent
IP Packet Length : 159 bytes
IP Source: 192.168.111.45    IP Remote: 10.33.103.217

IP Version 4
Source    : 192.168.111.45    Remote    : 10.33.103.217
Protocol : UDP
Datagram Length : 159
Flags :       Fragment Offset : 0

UDP Header Info
Source Port : 12000     Remote Port : 12000

Enterprise Extender Headers
LDLC   :    Local SAP:5    Remote SAP:4    Command:XID

XID Header
Format : T2.1 to T2.1|4|5 exchanges
Sending Node Type : T4 or T5
```

```
Length : 128
Block Number : 0xFFF    ID : 0x91171

XID Sender Node Flags
  WHOLE-BIND-PIUs required
  ACTPU suppression requested
  Networking capabilities indicator (sender is a network node)
  Prenegotiation exhange state
  Nonactivation exchange secondary-initated supported
  CP name change supported

BIND Support Flags
  Adaptive BIND pacing support as a BIND sender SUPPORTED
  Adaptive BIND pacing support as a BIND receiver NOT SUPPORTED
  Sender requesting topology update
  Adaptive BIND pacing support can be overridden by partner

TG Number : 0
DLC Type : non-channel
Non-Channel link properties
  XID Sender is using ABM on link
  XID Sender could be primary or secondary link staiton (negotiable)
  Link station transmit-receive capability : two-way simultaneous
  Maximum BTU Length : 32767
  Maximum I Frame : 0

Control Vector 0x0E Network Name
  Network Type : PU Name
  Name : WCD9
```

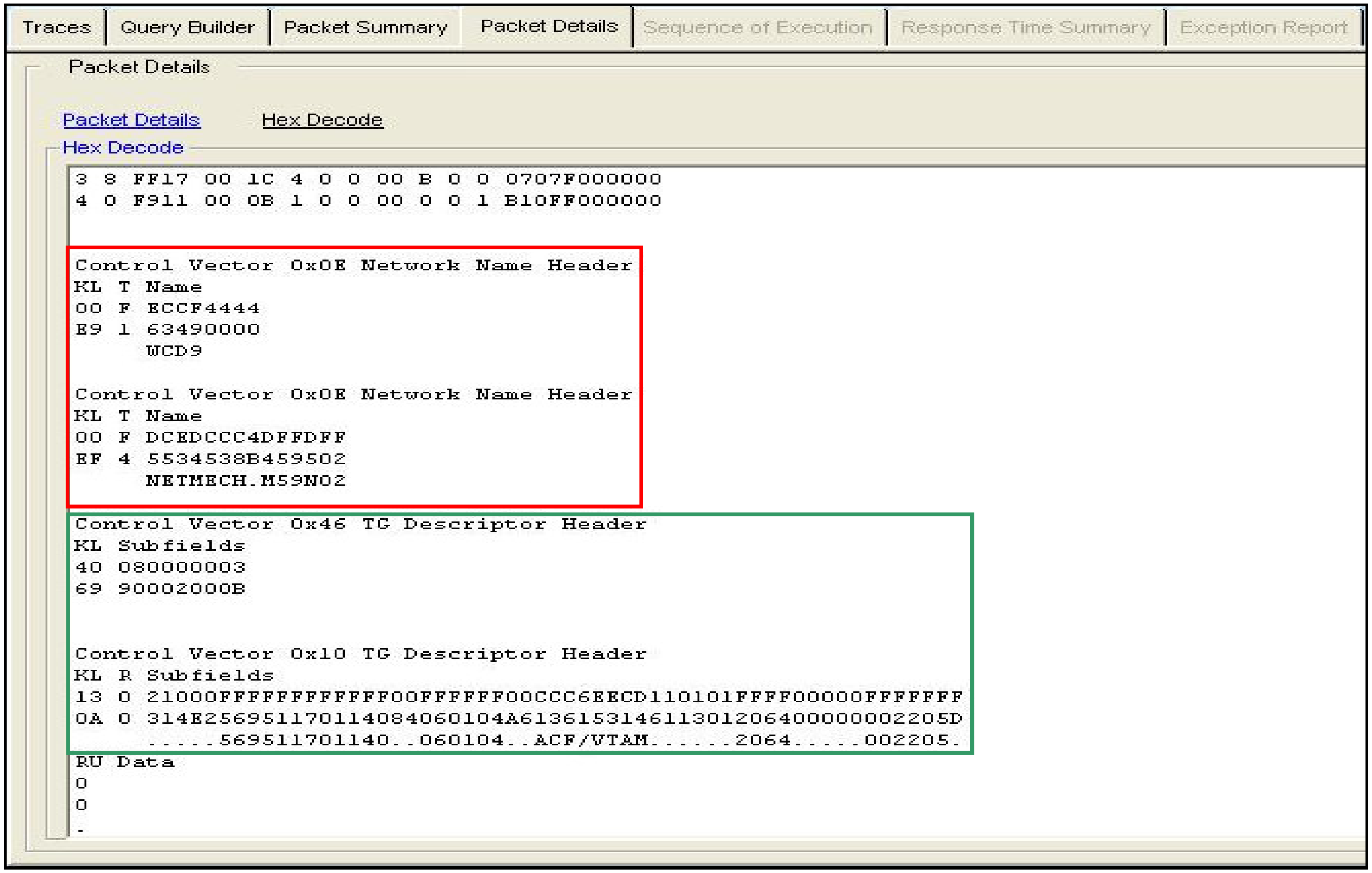
EE XID Init Packet: ‘Packet Details’ (Record #178 - Part 2)



```
Length : 128
Block Number : 0xFFF   ID : 0x91171

XID Sender Node Flags
  WHOLE-BIND-PIUs required
  ACTPU suppression requested
  Networking capabilities indicator (sender is a network node)
  Prenegotiation exhange state
  Nonactivation exchange secondary-initated supported
  CP name change supported

BIND Support Flags
  Adaptive BIND pacing support as a BIND sender SUPPORTED
  Adaptive BIND pacing support as a BIND receiver NOT SUPPORTED
  Sender requesting topology update
  Adaptive BIND pacing support can be overridden by partner

TG Number : 0
DLC Type : non-channel
Non-Channel link properties
  XID Sender is using ABM on link
  XID Sender could be primary or secondary link staiton (negotiable)
  Link station transmit-receive capability : two-way simultaneous
  Maximum BTU Length : 32767
  Maximum I Frame : 0

Control Vector 0x0E Network Name
  Network Type : PU Name
  Name : WCD9
```

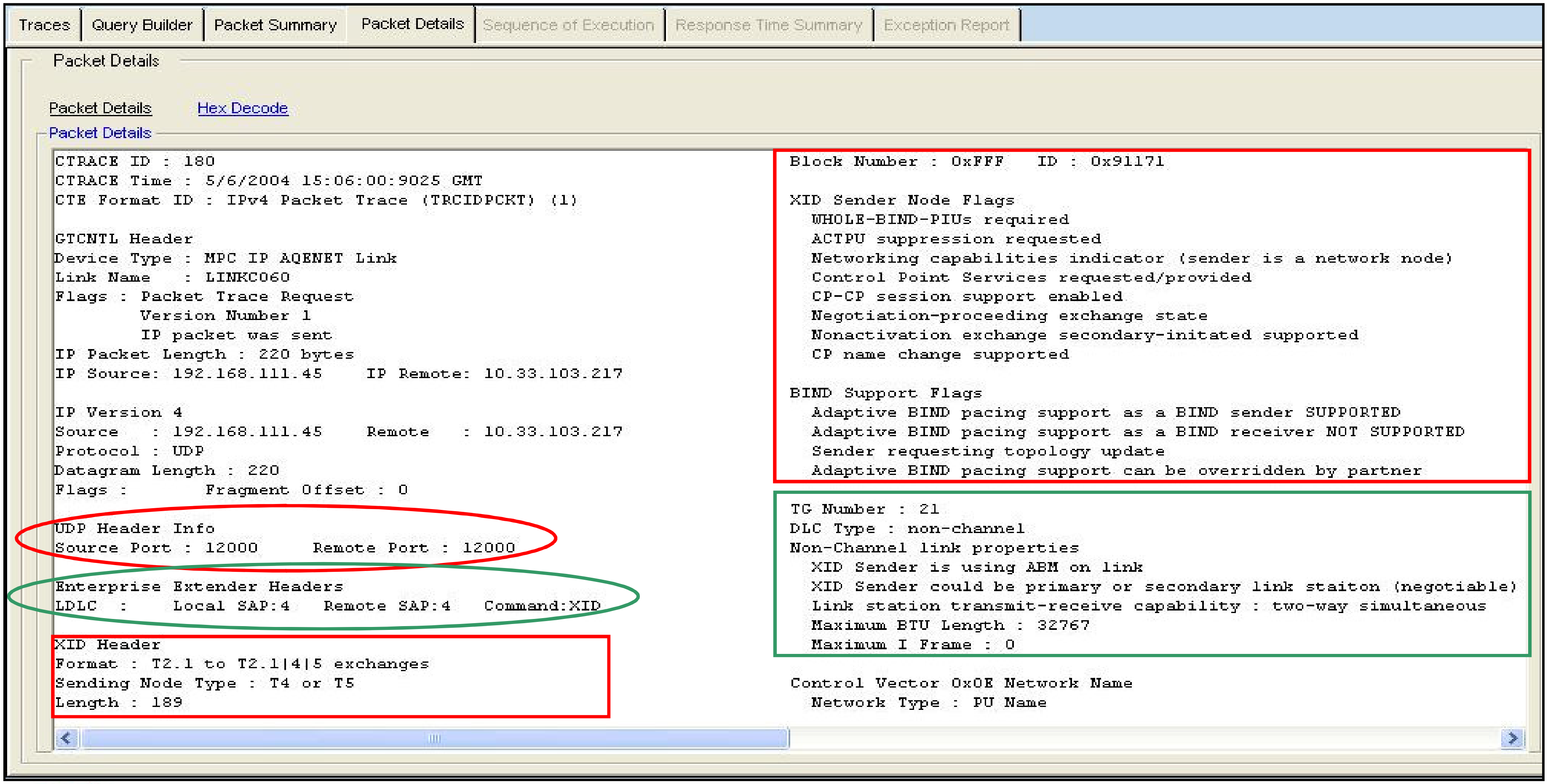
```
Control Vector 0x0E Network Name
  Network Type : CP name
  Name : NETMECH.M59NO

Control Vector 0x46 TG Descriptor
  TG Identifier SF
  TG Number : 0
  TG Partner Node CP Name :

Control Vector 0x10 Product ID
  Product Class : IBM Software
  Product Class : IBM Hardware
```

EE XID Init Packet: ‘Hex Decode’ (Record #178 - Part 2 – skipped Part 1)



```
3 8 FF17 00 1C 4 0 0 00 B 0 0 0707F000000
4 0 F911 00 0B 1 0 0 00 0 0 1 B10FF000000

Control Vector 0x0E Network Name Header
KL T Name
00 F ECCF4444
E9 1 63490000
     WCD9

Control Vector 0x0E Network Name Header
KL T Name
00 F DCEDCCC4DFFDFF
EF 4 5534538B459502
     NETMECH.M59N02
Control Vector 0x46 TG Descriptor Header
KL Subfields
40 080000003
69 90002000B


Control Vector 0x10 TG Descriptor Header
KL R Subfields
13 0 21000FFFFFFFFFFFF00FFFFFF00CCC6EECD110101FFFF00000FFFFFFF
0A 0 314E256951170114084060104A613615314611301206400000002205D
     .....569511701140..060104..ACF/VTAM......2064.....002205.
RU Data
0
0
-
```

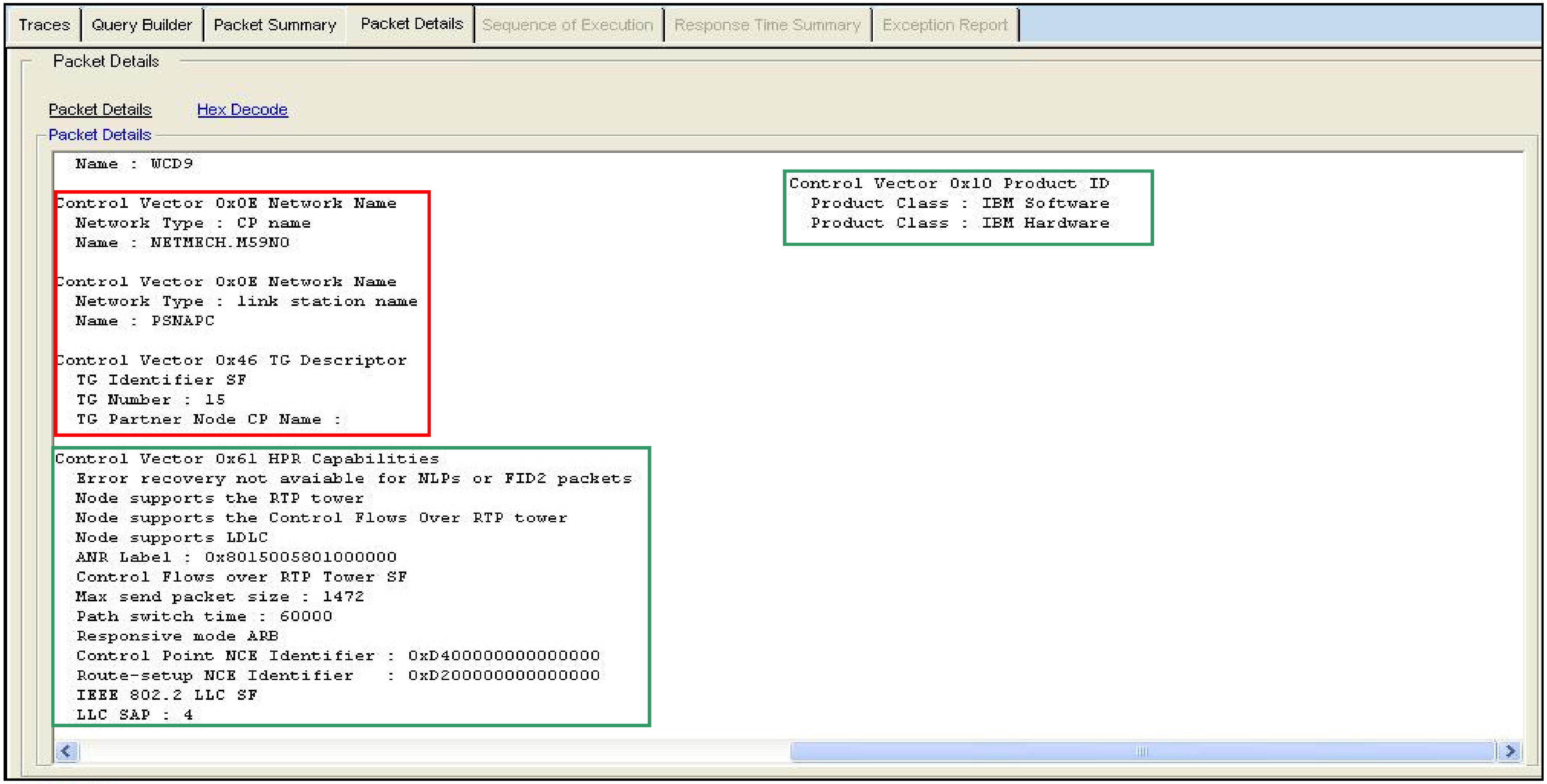
EE XID Init Packet: ‘Packet Details’ (Record #180 - Part 1)



```
CTRACE ID : 180
CTRACE Time : 5/6/2004 15:06:00:9025 GMT
CTE Format ID : IPv4 Packet Trace (TRCIDPCKT) (1)

GTCNTL Header
Device Type : MPC IP AQENET Link
Link Name   : LINKC060
Flags : Packet Trace Request
        Version Number 1
        IP packet was sent
IP Packet Length : 220 bytes
IP Source: 192.168.111.45    IP Remote: 10.33.103.217

IP Version 4
Source   : 192.168.111.45    Remote   : 10.33.103.217
Protocol : UDP
Datagram Length : 220
Flags :        Fragment Offset : 0

UDP Header Info
Source Port : 12000      Remote Port : 12000

Enterprise Extender Headers
LDLC  :    Local SAP:4    Remote SAP:4    Command:XID

XID Header
Format : T2.1 to T2.1|4|5 exchanges
Sending Node Type : T4 or T5
Length : 189
```

```
Block Number : 0xFFF    ID : 0x91171

XID Sender Node Flags
  WHOLE-BIND-PIUs required
  ACTPU suppression requested
  Networking capabilities indicator (sender is a network node)
  Control Point Services requested/provided
  CP-CP session support enabled
  Negotiation-proceeding exchange state
  Nonactivation exchange secondary-initated supported
  CP name change supported

BIND Support Flags
  Adaptive BIND pacing support as a BIND sender SUPPORTED
  Adaptive BIND pacing support as a BIND receiver NOT SUPPORTED
  Sender requesting topology update
  Adaptive BIND pacing support can be overridden by partner

TG Number : 21
DLC Type : non-channel
Non-Channel link properties
  XID Sender is using ABM on link
  XID Sender could be primary or secondary link staiton (negotiable)
  Link station transmit-receive capability : two-way simultaneous
  Maximum BTU Length : 32767
  Maximum I Frame : 0

Control Vector 0x0E Network Name
  Network Type : PU Name
```

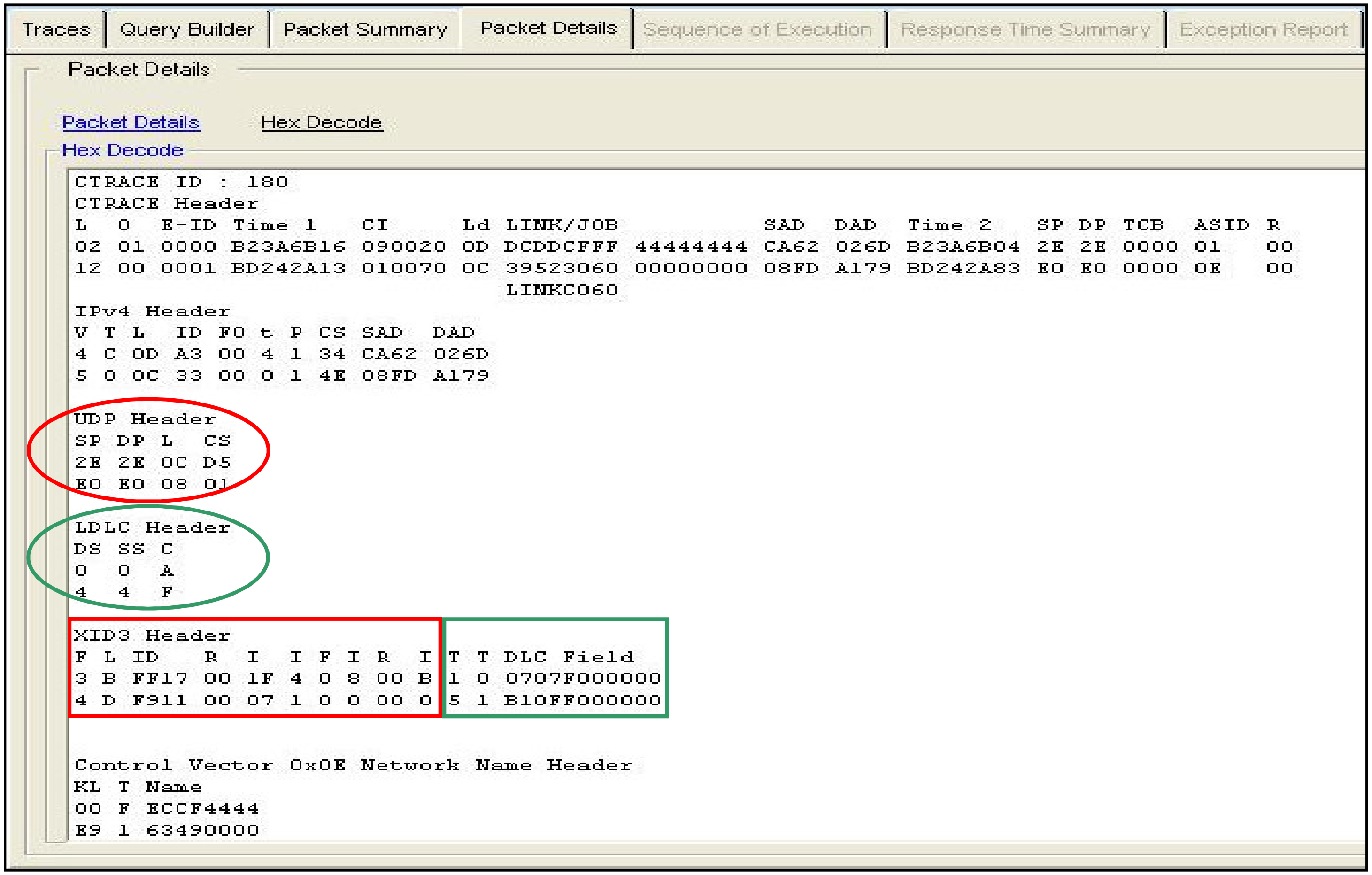
EE XID Init Packet: ‘Packet Details’ (Record #180 - Part 2)



```
  Name : WCD9

Control Vector 0x0E Network Name
  Network Type : CP name
  Name : NETMECH.M59NO

Control Vector 0x0E Network Name
  Network Type : link station name
  Name : PSNAPC

Control Vector 0x46 TG Descriptor
  TG Identifier SF
  TG Number : 15
  TG Partner Node CP Name :

Control Vector 0x61 HPR Capabilities
  Error recovery not avaiable for NLPs or FID2 packets
  Node supports the RTP tower
  Node supports the Control Flows Over RTP tower
  Node supports LDLC
  ANR Label : 0x8015005801000000
  Control Flows over RTP Tower SF
  Max send packet size : 1472
  Path switch time : 60000
  Responsive mode ARB
  Control Point NCE Identifier : 0xD400000000000000
  Route-setup NCE Identifier   : 0xD200000000000000
  IEEE 802.2 LLC SF
  LLC SAP : 4
```

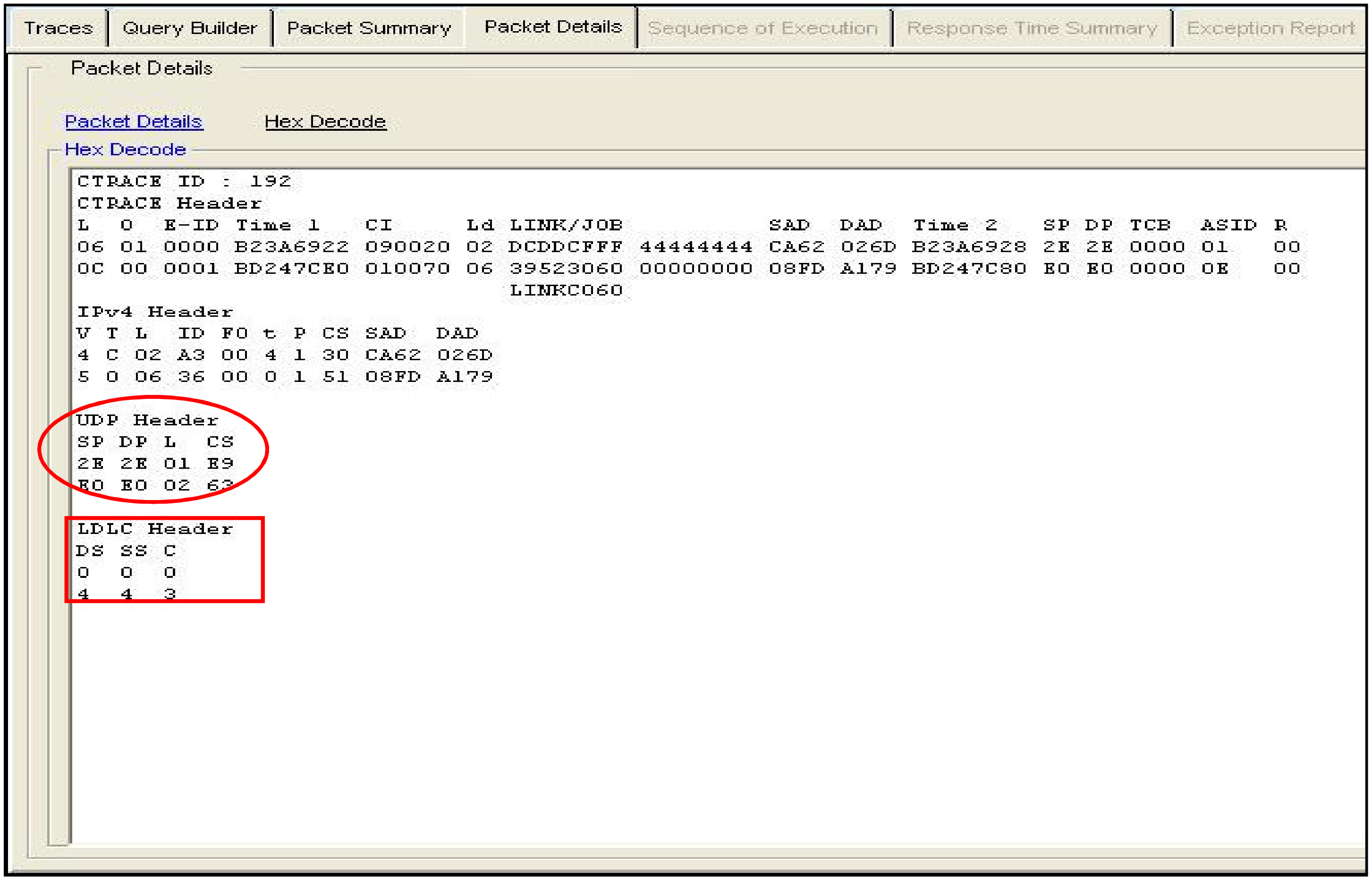
```
Control Vector 0x10 Product ID
  Product Class : IBM Software
  Product Class : IBM Hardware
```

EE XID Init Packet: ‘Hex Decode’ (Record #180 - Just Part 1)



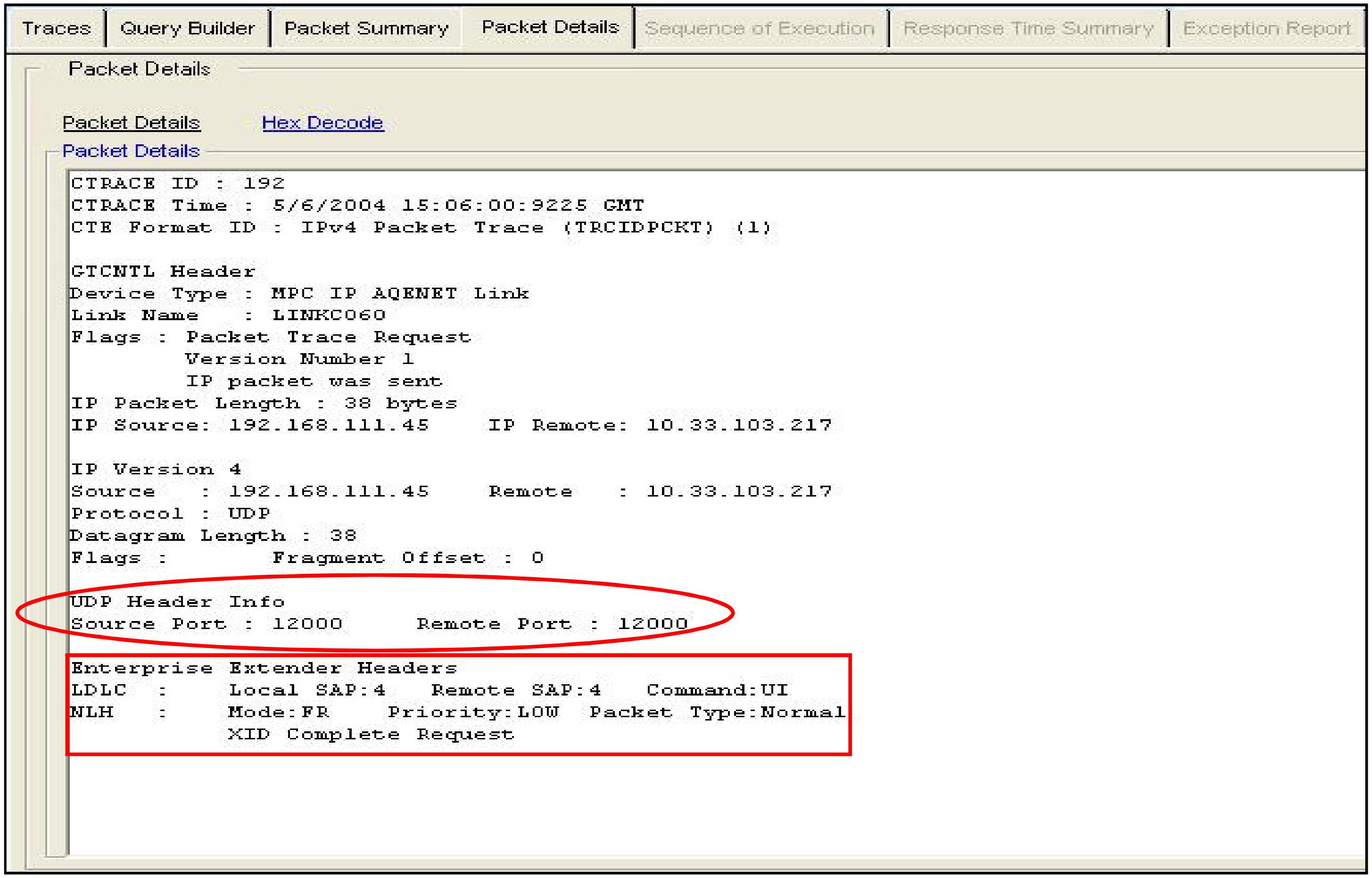
```
CTRACE ID : 180
CTRACE Header
L  O  E-ID Time 1   CI     Ld LINK/JOB          SAD  DAD  Time 2   SP DP TCB  ASID R
02 01 0000 B23A6B16 090020 0D DCDDCFFF 44444444 CA62 026D B23A6B04 2E 2E 0000 01   00
12 00 0001 BD242A13 010070 0C 39523060 00000000 08FD A179 BD242A83 E0 E0 0000 0E   00
                              LINKC060
IPv4 Header
V T L  ID FO t P CS SAD  DAD
4 C 0D A3 00 4 1 34 CA62 026D
5 0 0C 33 00 0 1 4E 08FD A179

UDP Header
SP DP L  CS
2E 2E 0C D5
E0 E0 08 01

LDLC Header
DS SS C
0  0  A
4  4  F

XID3 Header
F L ID   R  I  I F I R  I T T DLC Field
3 B FF17 00 1F 4 0 8 00 B 1 0 0707F000000
4 D F911 00 07 1 0 0 00 0 5 1 B10FF000000


Control Vector 0x0E Network Name Header
KL T Name
00 F ECCF4444
E9 1 63490000
```

EE XID Init Packet: ‘Packet Details’ (Record #192 - Only Part)



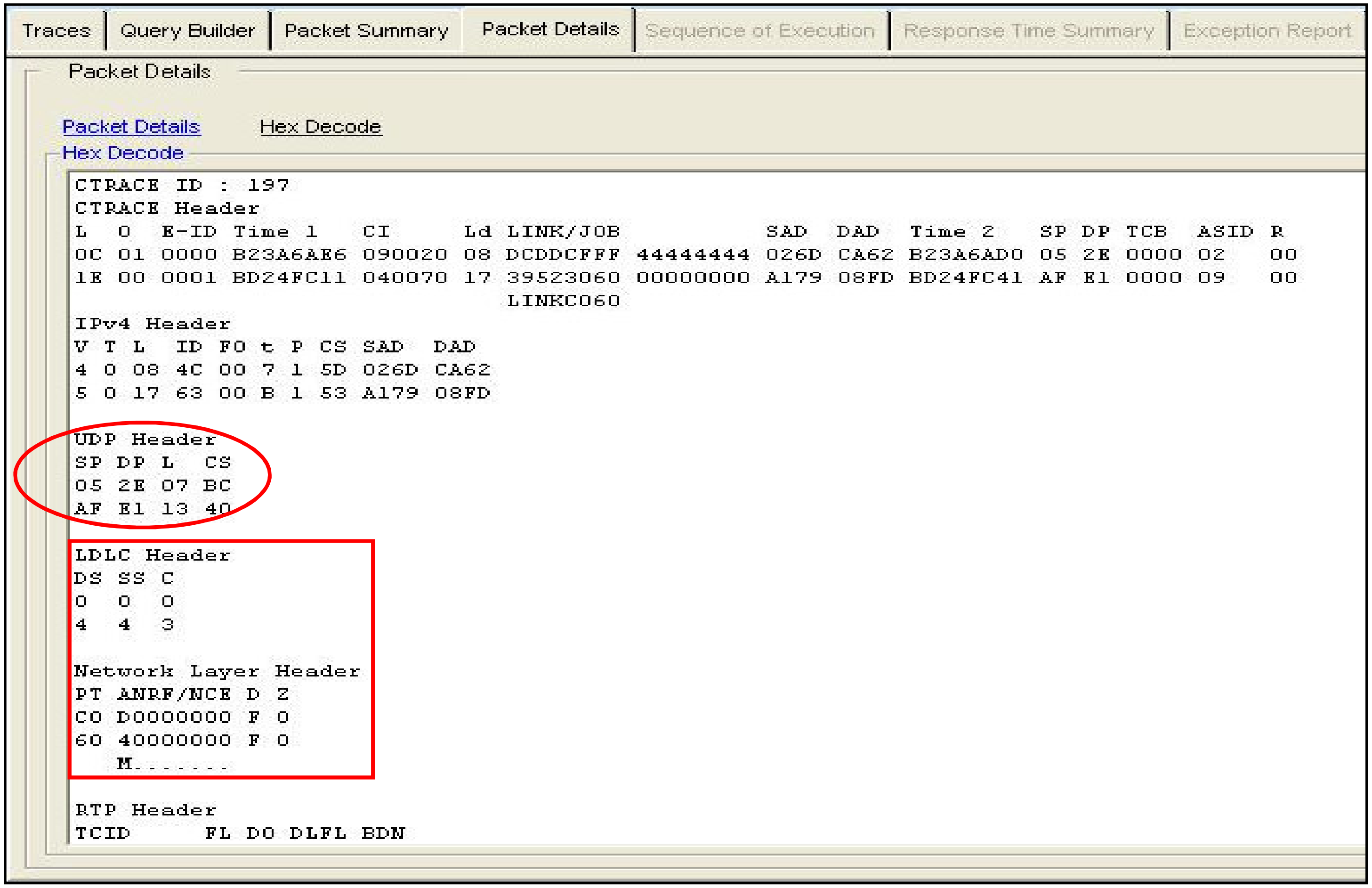
```
CTRACE ID : 192
CTRACE Header
L  O  E-ID Time 1   CI     Ld LINK/JOB          SAD  DAD  Time 2   SP DP TCB  ASID R
06 01 0000 B23A6922 090020 02 DCDDCFFF 44444444 CA62 026D B23A6928 2E 2E 0000 01   00
0C 00 0001 BD247CE0 010070 06 39523060 00000000 08FD A179 BD247C80 E0 E0 0000 0E   00
                              LINKC060
IPv4 Header
V T L  ID FO t P CS SAD  DAD
4 C 02 A3 00 4 1 30 CA62 026D
5 0 06 36 00 0 1 51 08FD A179

UDP Header
SP DP L  CS
2E 2E 01 E9
E0 E0 02 63

LDLC Header
DS SS C
0  0  0
4  4  3
```

EE XID Init Packet: ‘Packet Details’ (Record #192 - Only Part)



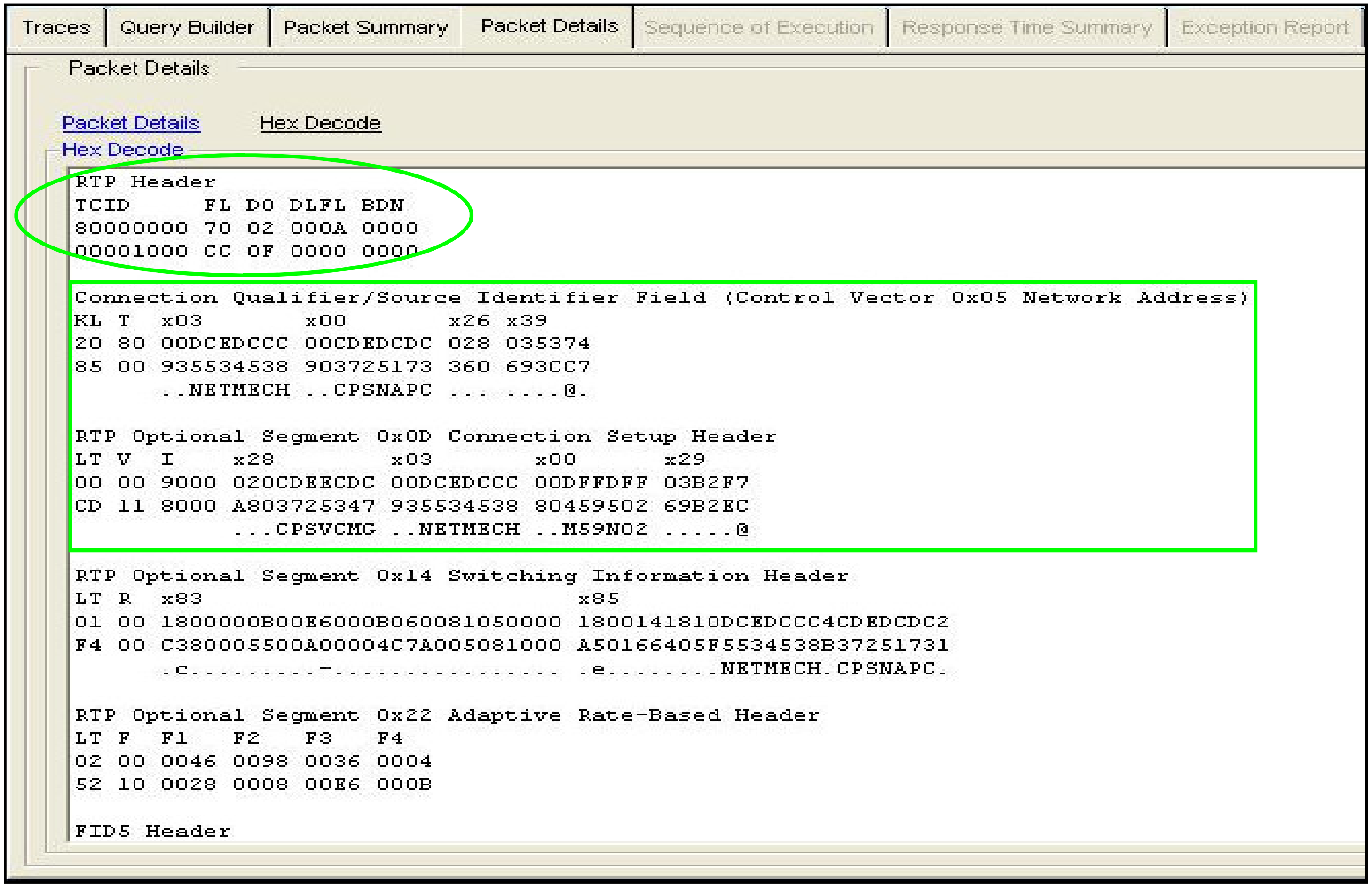
```
CTRACE ID : 192
CTRACE Time : 5/6/2004 15:06:00:9225 GMT
CTE Format ID : IPv4 Packet Trace (TRCIDPCKT) (1)

GTCNTL Header
Device Type : MPC IP AQENET Link
Link Name    : LINKC060
Flags : Packet Trace Request
        Version Number 1
        IP packet was sent
IP Packet Length : 38 bytes
IP Source: 192.168.111.45     IP Remote: 10.33.103.217

IP Version 4
Source    : 192.168.111.45     Remote    : 10.33.103.217
Protocol : UDP
Datagram Length : 38
Flags :        Fragment Offset : 0

UDP Header Info
Source Port : 12000      Remote Port : 12000

Enterprise Extender Headers
LDLC   :    Local SAP:4    Remote SAP:4    Command:UI
NLH    :    Mode:FR     Priority:LOW   Packet Type:Normal
            XID Complete Request
```

XID Complete ACK: ‘Hex Decode’ (Record #197 - Part 1)



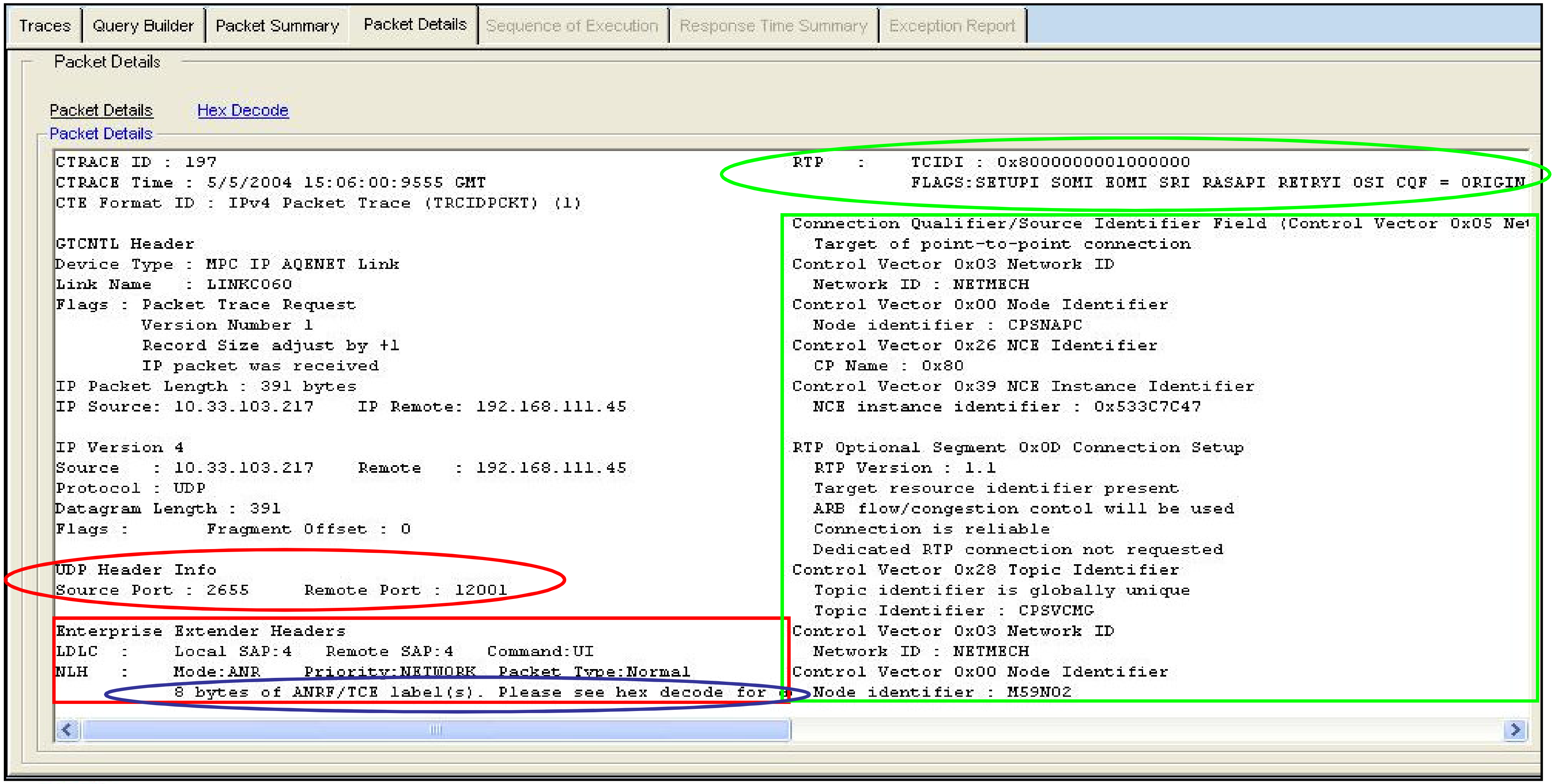
```
CTRACE ID : 197
CTRACE Header
L  O  E-ID Time 1   CI     Ld LINK/JOB          SAD  DAD  Time 2   SP DP TCB  ASID R
0C 01 0000 B23A6AE6 090020 08 DCDDCFFF 44444444 026D CA62 B23A6AD0 05 2E 0000 02   00
1E 00 0001 BD24FC11 040070 17 39523060 00000000 A179 08FD BD24FC41 AF E1 0000 09   00
                              LINKC060
IPv4 Header
V T L  ID FO t P CS SAD  DAD
4 0 08 4C 00 7 1 5D 026D CA62
5 0 17 63 00 B 1 53 A179 08FD

UDP Header
SP DP L  CS
05 2E 07 BC
AF E1 13 40

LDLC Header
DS SS C
0  0  0
4  4  3

Network Layer Header
PT ANRF/NCE D Z
C0 D0000000 F 0
60 40000000 F 0
   M.......

RTP Header
TCID     FL DO DLFL BDN
```

XID Complete ACK: ‘Hex Decode’ (Record #197 - Part 2)



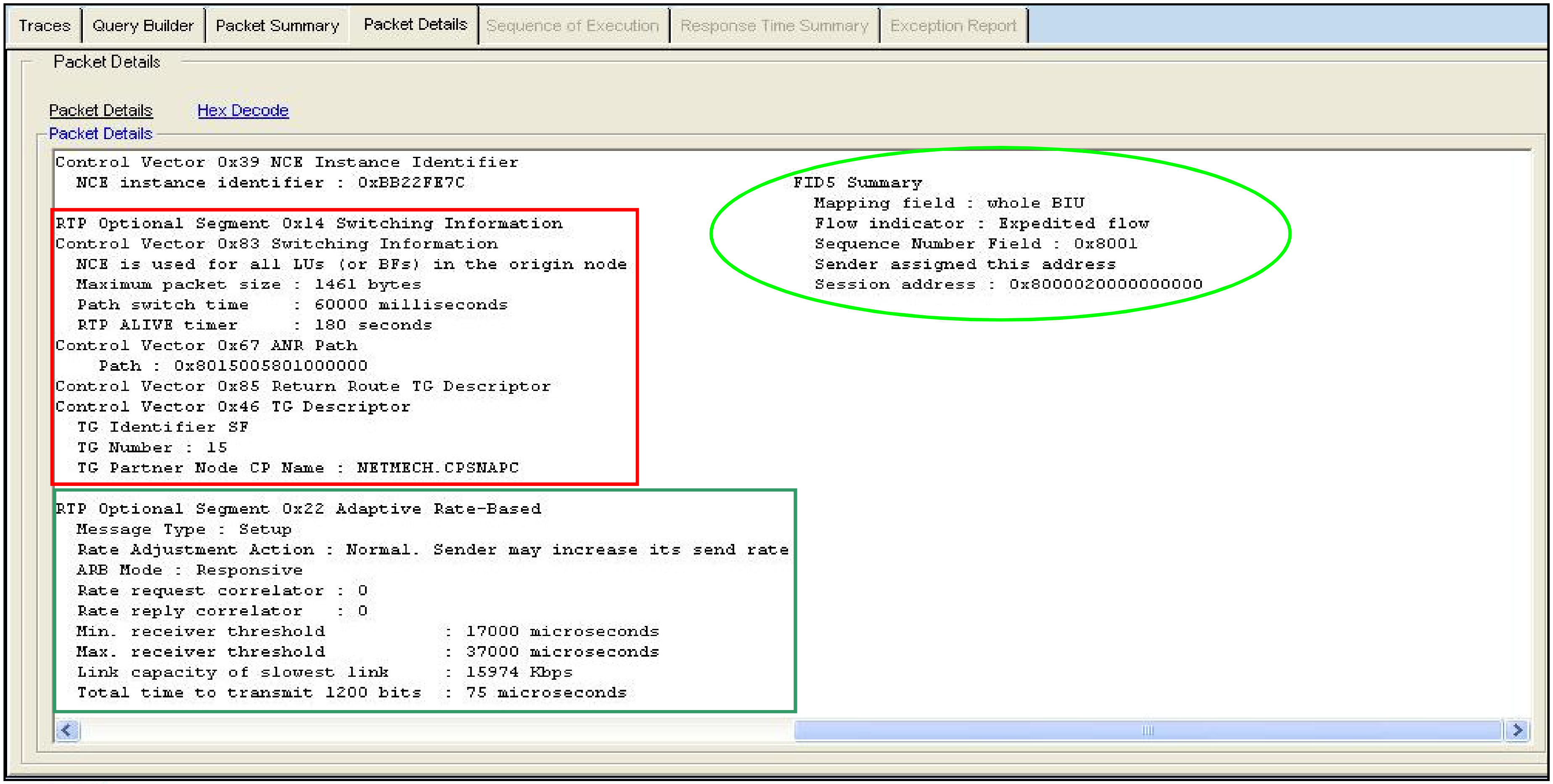
```
RTP Header
TCID     FL DO DLFL BDN
80000000 70 02 000A 0000
00001000 CC 0F 0000 0000

Connection Qualifier/Source Identifier Field (Control Vector 0x05 Network Address)
KL T  x03       x00       x26 x39
20 80 00DCEDCCC 00CDEDCDC 028 035374
85 00 935534538 903725173 360 693CC7
      ..NETMECH ..CPSNAPC ... ....@.

RTP Optional Segment 0x0D Connection Setup Header
LT V  I    x28       x03       x00      x29
00 00 9000 020CDEECDC 00DCEDCCC 00DFFDFF 03B2F7
CD 11 8000 A803725347 935534538 80459502 69B2EC
           ...CPSVCMG ..NETMECH ..M59N02 .....@

RTP Optional Segment 0x14 Switching Information Header
LT R  x83                          x85
01 00 1800000B00E6000B060081050000 1800141810DCEDCCC4CDEDCDC2
F4 00 C380005500A00004C7A005081000 A50166405F5534538B37251731
      .c.........-................. .e........NETMECH.CPSNAPC.

RTP Optional Segment 0x22 Adaptive Rate-Based Header
LT F  F1   F2   F3   F4
02 00 0046 0098 0036 0004
52 10 0028 0008 00E6 000B

FID5 Header
```

EE XID Init Packet: ‘Packet Details’ (Record #197- Part 1)



```
CTRACE ID : 197                                                     RTP   :    TCIDI : 0x8000000001000000
CTRACE Time : 5/5/2004 15:06:00:9555 GMT                                       FLAGS:SETUPI SOMI EOMI SRI RASAPI RETRYI OSI CQF = ORIGIN
CTE Format ID : IPv4 Packet Trace (TRCIDPCKT) (1)
                                                                    Connection Qualifier/Source Identifier Field (Control Vector 0x05 Ne
GTCNTL Header                                                         Target of point-to-point connection
Device Type : MPC IP AQENET Link                                    Control Vector 0x03 Network ID
Link Name   : LINKC060                                                Network ID : NETMECH
Flags : Packet Trace Request                                        Control Vector 0x00 Node Identifier
        Version Number 1                                              Node identifier : CPSNAPC
        Record Size adjust by +1                                    Control Vector 0x26 NCE Identifier
        IP packet was received                                        CP Name : 0x80
IP Packet Length : 391 bytes                                        Control Vector 0x39 NCE Instance Identifier
IP Source: 10.33.103.217    IP Remote: 192.168.111.45                 NCE instance identifier : 0x533C7C47

IP Version 4                                                        RTP Optional Segment 0x0D Connection Setup
Source   : 10.33.103.217    Remote   : 192.168.111.45                 RTP Version : 1.1
Protocol : UDP                                                        Target resource identifier present
Datagram Length : 391                                                 ARB flow/congestion contol will be used
Flags :       Fragment Offset : 0                                     Connection is reliable
                                                                      Dedicated RTP connection not requested
UDP Header Info                                                     Control Vector 0x28 Topic Identifier
Source Port : 2655     Remote Port : 12001                            Topic identifier is globally unique
                                                                      Topic Identifier : CPSVCMG
Enterprise Extender Headers                                         Control Vector 0x03 Network ID
LDLC  :    Local SAP:4   Remote SAP:4   Command:UI                    Network ID : NETMECH
NLH   :    Mode:ANR    Priority:NETWORK  Packet Type:Normal         Control Vector 0x00 Node Identifier
           8 bytes of ANRF/TCE label(s). Please see hex decode for    Node identifier : M59N02
```

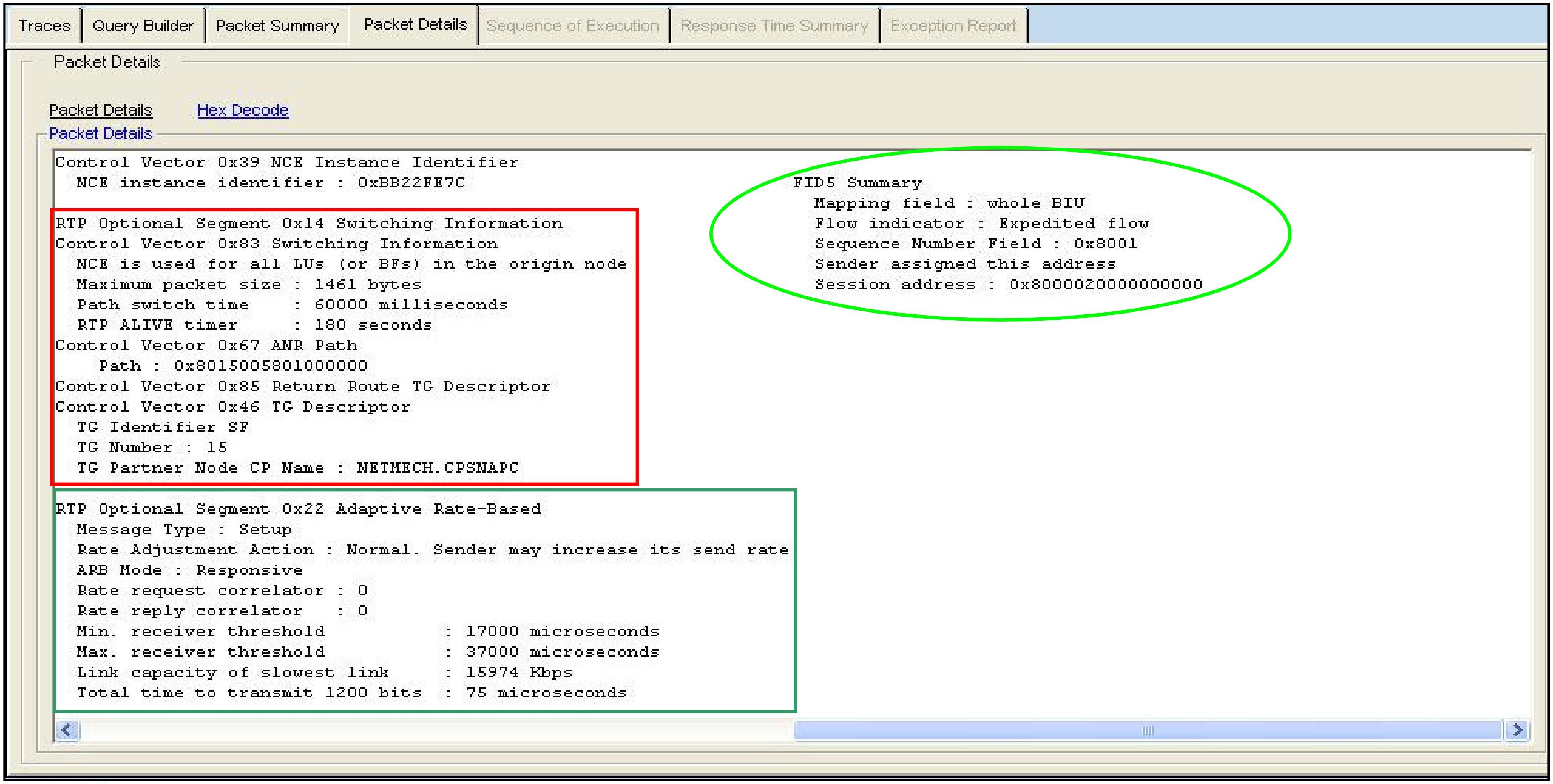
EE XID Init Packet: 'Packet Details' (Record #197- Part 2)



```
Control Vector 0x39 NCE Instance Identifier
  NCE instance identifier : 0xBB22FE7C

RTP Optional Segment 0x14 Switching Information
Control Vector 0x83 Switching Information
  NCE is used for all LUs (or BFs) in the origin node
  Maximum packet size : 1461 bytes
  Path switch time    : 60000 milliseconds
  RTP ALIVE timer     : 180 seconds
Control Vector 0x67 ANR Path
    Path : 0x8015005801000000
Control Vector 0x85 Return Route TG Descriptor
Control Vector 0x46 TG Descriptor
  TG Identifier SF
  TG Number : 15
  TG Partner Node CP Name : NETMECH.CPSNAPC

RTP Optional Segment 0x22 Adaptive Rate-Based
  Message Type : Setup
  Rate Adjustment Action : Normal. Sender may increase its send rate
  ARB Mode : Responsive
  Rate request correlator : 0
  Rate reply correlator   : 0
  Min. receiver threshold           : 17000 microseconds
  Max. receiver threshold           : 37000 microseconds
  Link capacity of slowest link     : 15974 Kbps
  Total time to transmit 1200 bits  : 75 microseconds
```

```
FID5 Summary
  Mapping field : whole BIU
  Flow indicator : Expedited flow
  Sequence Number Field : 0x8001
  Sender assigned this address
  Session address : 0x8000020000000000
```

EE XID Init Packet: ‘Packet Details’ (Record #197- Part 3)



```
Control Vector 0x39 NCE Instance Identifier
  NCE instance identifier : 0xBB22FE7C

RTP Optional Segment 0x14 Switching Information
Control Vector 0x83 Switching Information
  NCE is used for all LUs (or BFs) in the origin node
  Maximum packet size : 1461 bytes
  Path switch time     : 60000 milliseconds
  RTP ALIVE timer      : 180 seconds
Control Vector 0x67 ANR Path
    Path : 0x8015005801000000
Control Vector 0x85 Return Route TG Descriptor
Control Vector 0x46 TG Descriptor
  TG Identifier SF
  TG Number : 15
  TG Partner Node CP Name : NETMECH.CPSNAPC

RTP Optional Segment 0x22 Adaptive Rate-Based
  Message Type : Setup
  Rate Adjustment Action : Normal. Sender may increase its send rate
  ARB Mode : Responsive
  Rate request correlator : 0
  Rate reply correlator   : 0
  Min. receiver threshold           : 17000 microseconds
  Max. receiver threshold           : 37000 microseconds
  Link capacity of slowest link     : 15974 Kbps
  Total time to transmit 1200 bits  : 75 microseconds
```

```
FID5 Summary
  Mapping field : whole BIU
  Flow indicator : Expedited flow
  Sequence Number Field : 0x8001
  Sender assigned this address
  Session address : 0x8000020000000000
```

Know Your Protocols and Applications - ICMP

Internet Control Message Protocol

- Overview
- A Sampling of Messages

ICMP Overview

- RFC
  - 792 – Basic Operation
  - 1256 – Router Discovery Messages
  - 1393 – traceroute
  - 1812 – IPv4 Router Requirements
- Unreliable, Connectionless, Unacknowledged Delivery
- Administrative Assistant to IP
- Message Classes
  - Error Messages
  - Informational Messages
  - 8 Bit Field
    - 256 possible messages
    - Defined Sequentially on a First Come, First Served Basis

ICMP Overview

- Message Codes
  - Additional Information
  - 8 Bit Field
  - Sort of a Message Subtype
- ICMPv4
- ICMPv6

ICMP Message Samples (ICMPv4)

• Echo Request	– Type value 0
• Echo Reply	– Type Value 8
• Destination Unreachable	– Type Value 3
• Time Exceeded	– Type Value 11
• Traceroute	– Type Value 30
• Router Advertisement	– Type Value 9
• Router Solicitation	– Type Value 10

Concluding Remarks

- Know your network (response times, configuration, etc.)
- Know the protocols involved in the problem area
- Take traces at different points in the network to isolate the problem
- Find ways to eliminate excess traffic
  - OSPF Routing and Advertisements
  - M/S Netbios
  - SQL and DB Queries
  - ICMP
  - Others?
- Analyze, analyze, analyze