Effective Network Trace Analysis

David J Cheng

Applied Expert Systems, Inc.
davec@aesclever.com

August 8, 2017, 10:00AM
Session 21116

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Agenda

- TCP/IP revisited
- Sample Cases
  - DHCP
  - DNS
  - FTP – Flow analysis, brute force attack
  - OSA - Excessive / Dropped packets, addressing errors
  - AT-TLS – Flow analysis
  - Performance issue
  - IDS trace
- Appendix – how to take traces

Note: trace analysis screen shots are from ***CleverView® for cTrace Analysis.***

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Using Traces

- Know your protocols!
  - Network stack
  - Application flow
  - Check for “errors”
  - Mismatched capabilities
  - Did someone change the TCP header option (e.g., SACK)?
  - Lost packets (congestions?)
- Establish baseline – capture normal traffic flow
- Network Time vs. Host (Server) Time
- Trace comparison
- Trace inventory with annotations
- Multiple trace points – multiple platforms
- Automate/schedule tracing

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

How to Take a Packet Trace? See Appendix

z/OS CTRACE:

- ***SYSTCPDA***
  - **Packet Trace**
    - Scope: TCP/IP stack
    - Packets entering or leaving the TCP/IP stack
  - **Data Trace**
    - scope: TCP/IP stack
    - Socket data into and out of the Physical File System (PFS)
    - Application data (unencrypted)
- ***SYSTCPOT***
  - **OSAENTA**
    - Scope: LPAR or CHPID
    - Frames entering or leaving an OSA adapter for a connected host
- ***STSTCPIS***
  - Intrusion Detection Services (IDS)
  - Packets are traced based on IDS policies

Data in the CTRACE Header is important! e.g., Packet Discard Code, IDS Probe ID, Correlator, IDS Policy, etc.

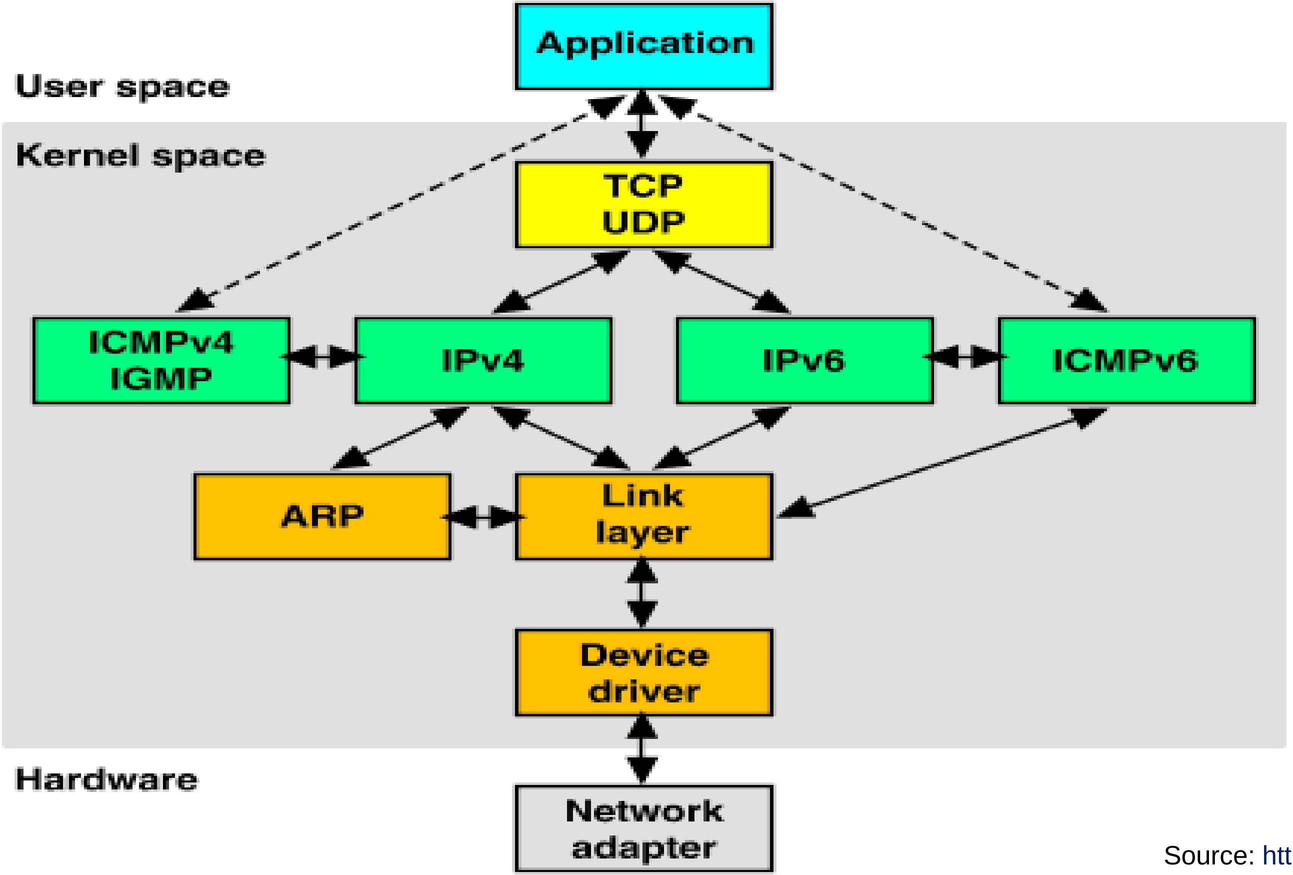
Linux, UNIX, AIX: tcpdump
Android*, iOS*: *tcpdump*
Windows: *windump*

* Requires root or jail break.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Networking Stack Support for TCP/IP

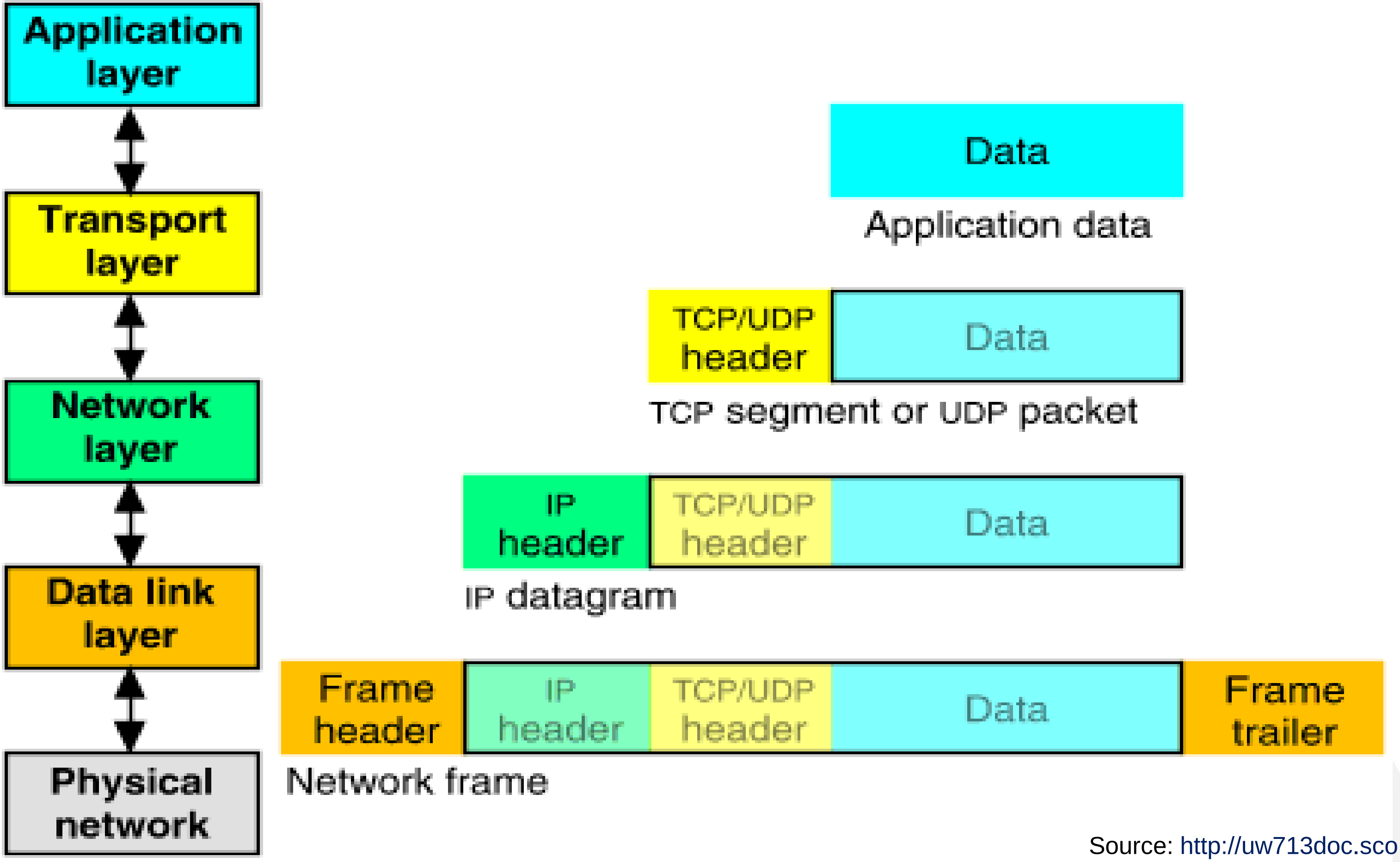


Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Encapsulation of Application Data within a Network Stack

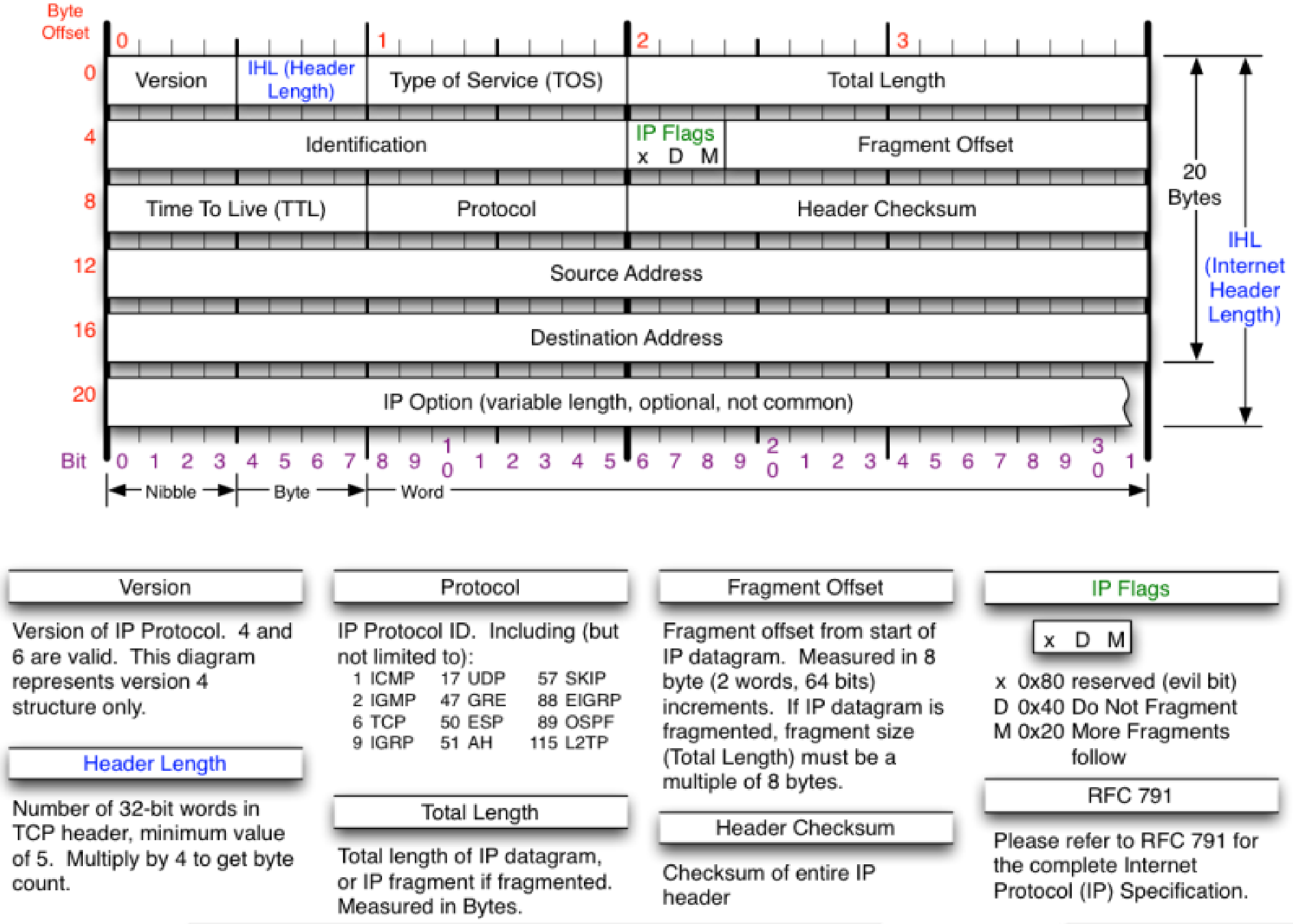


Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

IP Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

ID – Unique ID within “maximum datagram lifetime”

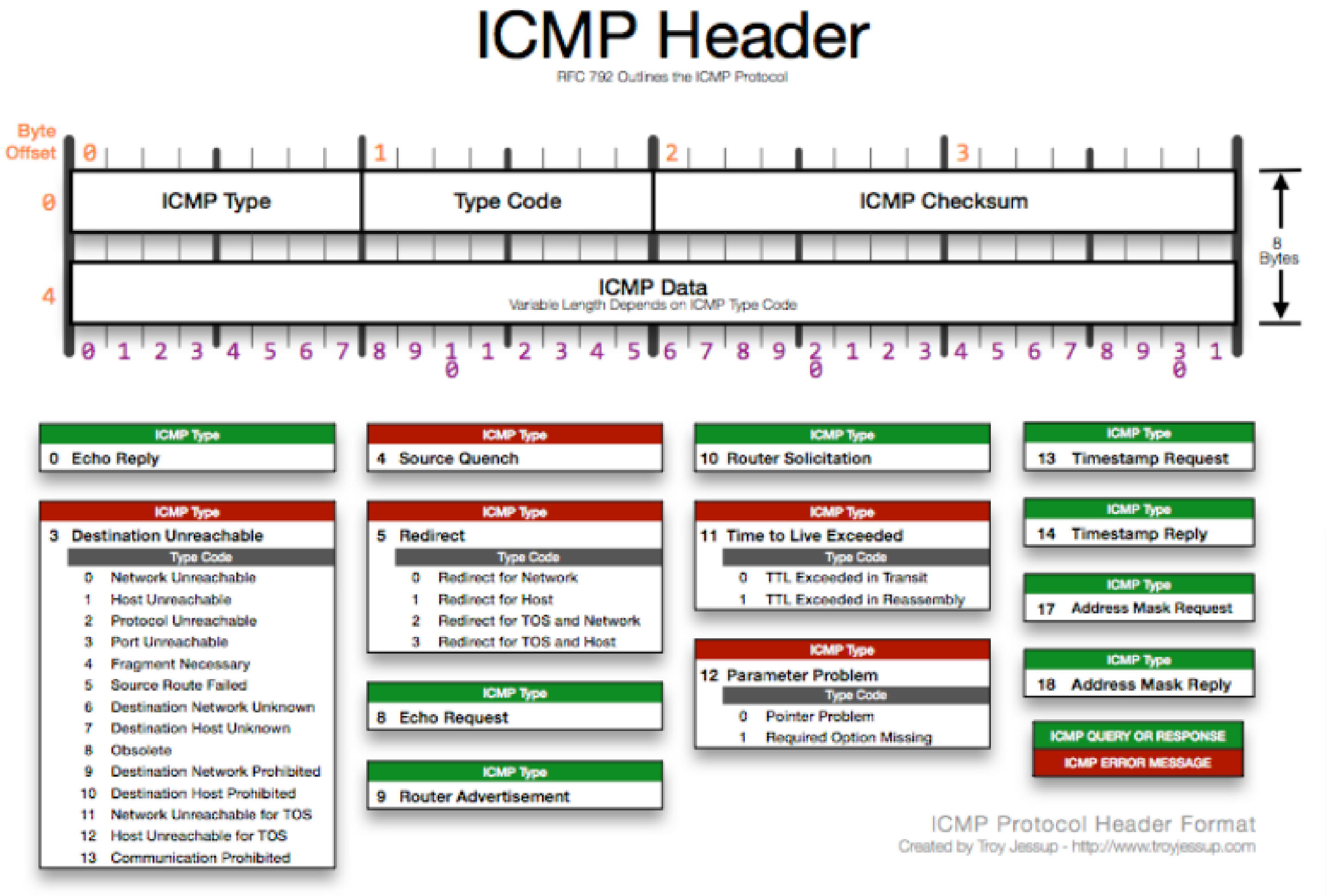
TTL – Time To Live, max value: 255. Decremented by 1 by each router. If it becomes 0 before reaching destination, then the packet is discarded by the router.

Source: http://nmap.org/book/images/hdr/MJB-IP-Header-800x576.png

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

ICMP Header



Used by network devices (e.g., routers) to send error or informational messages.

ping, traceroute, path MTU discovery, etc.

Source http://www.troyjessup.com/headers/ICMP_Header.png

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Fragmentation – split up large packets and reassemble fragments by routers (dated method)

Different networks have different maximum packet sizes (MTU: Maximum Transmission Unit); e.g., Ethernet 1.5K, WiFi 2.3K

To split up:

- Break up packet into smaller pieces (fragments)
- Copy IP header to pieces
- Adjust length, set offsets
- Set MF (More Fragments) on all pieces except the last one

Receiver:

- Use ID field to reassemble the pieces back together

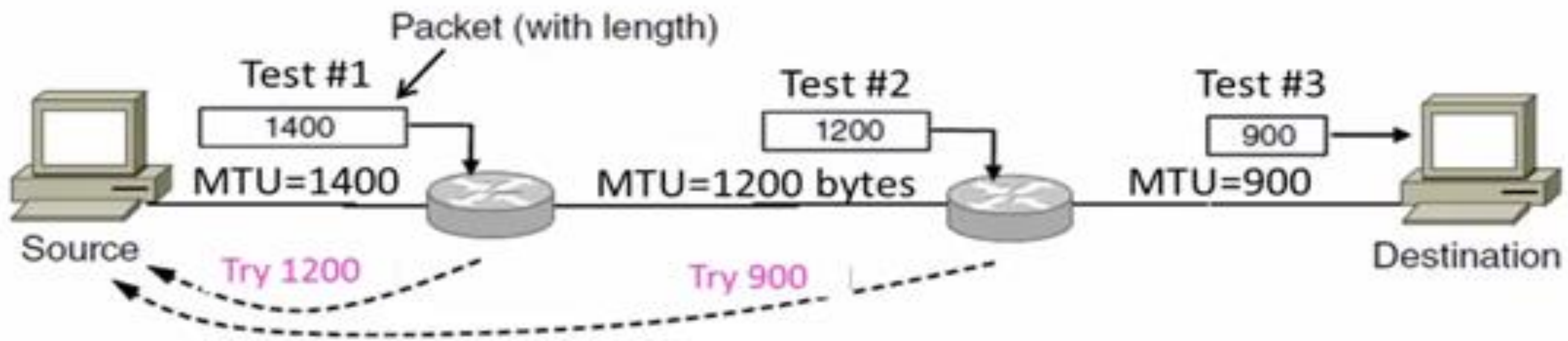
Fragmentation is undesirable: more work for routers/hosts, tends to magnify loss rate – if you lose a fragment you have to retransmit the entire packet

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Path MTU Discovery - avoids fragmentation (a better method)
Finds the smallest MTU of all links in the path

Implemented with DF (Don't Fragment) bit in IP Header and ICMP Type 3, Code 4: Destination Unreachable; Fragment Necessary, and link MTU (RFC 1191) to get feedback messages from routers



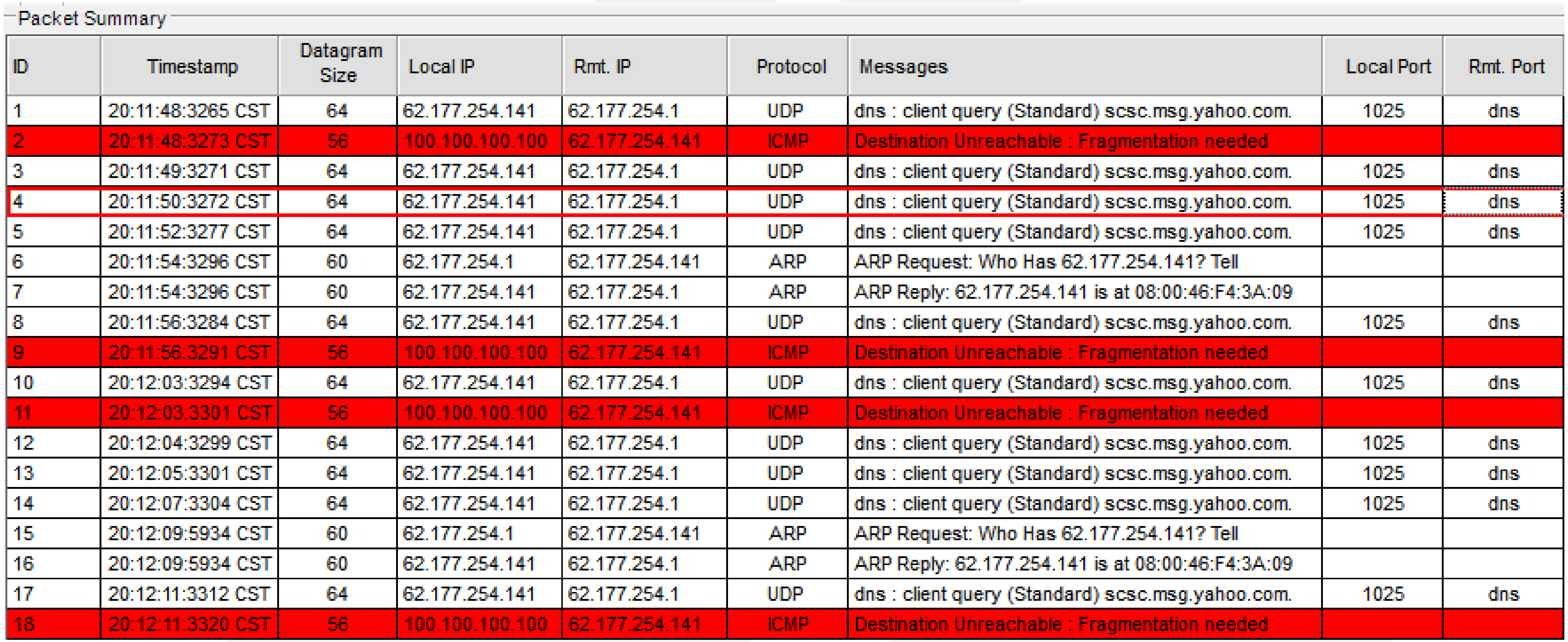
Source: Computer Networks lecture Professor David Wetherall, University of Washington

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

ICMP Type 3: *Destination Unreachable*
Code 4: *Fragmentation needed*

packet size > MTU but Don’t Fragment bit is set



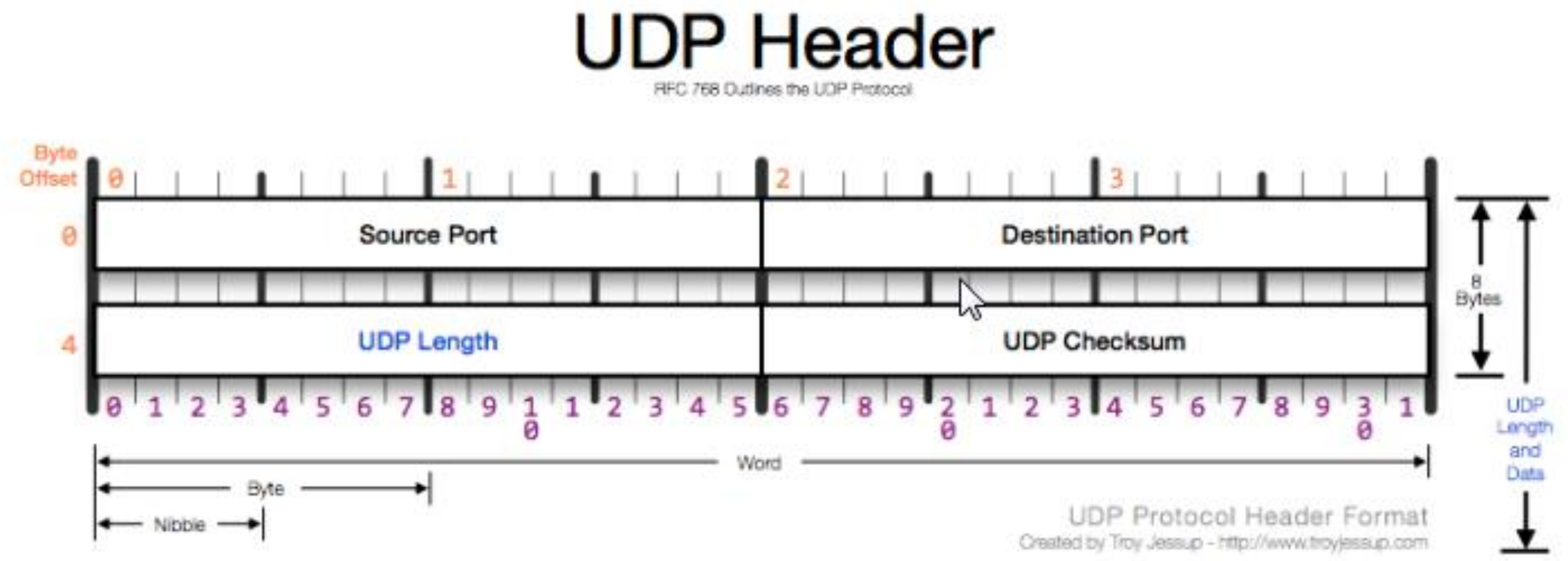
Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port
1	20:11:48:3265 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
2	20:11:48:3273 CST	56	100.100.100.100	62.177.254.141	ICMP	Destination Unreachable : Fragmentation needed		
3	20:11:49:3271 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
4	20:11:50:3272 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
5	20:11:52:3277 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
6	20:11:54:3296 CST	60	62.177.254.1	62.177.254.141	ARP	ARP Request: Who Has 62.177.254.141? Tell		
7	20:11:54:3296 CST	60	62.177.254.141	62.177.254.1	ARP	ARP Reply: 62.177.254.141 is at 08:00:46:F4:3A:09		
8	20:11:56:3284 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
9	20:11:56:3291 CST	56	100.100.100.100	62.177.254.141	ICMP	Destination Unreachable : Fragmentation needed		
10	20:12:03:3294 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
11	20:12:03:3301 CST	56	100.100.100.100	62.177.254.141	ICMP	Destination Unreachable : Fragmentation needed		
12	20:12:04:3299 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
13	20:12:05:3301 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
14	20:12:07:3304 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
15	20:12:09:5934 CST	60	62.177.254.1	62.177.254.141	ARP	ARP Request: Who Has 62.177.254.141? Tell		
16	20:12:09:5934 CST	60	62.177.254.141	62.177.254.1	ARP	ARP Reply: 62.177.254.141 is at 08:00:46:F4:3A:09		
17	20:12:11:3312 CST	64	62.177.254.141	62.177.254.1	UDP	dns : client query (Standard) scsc.msg.yahoo.com.	1025	dns
18	20:12:11:3320 CST	56	100.100.100.100	62.177.254.141	ICMP	Destination Unreachable : Fragmentation needed		

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

UDP Header Format

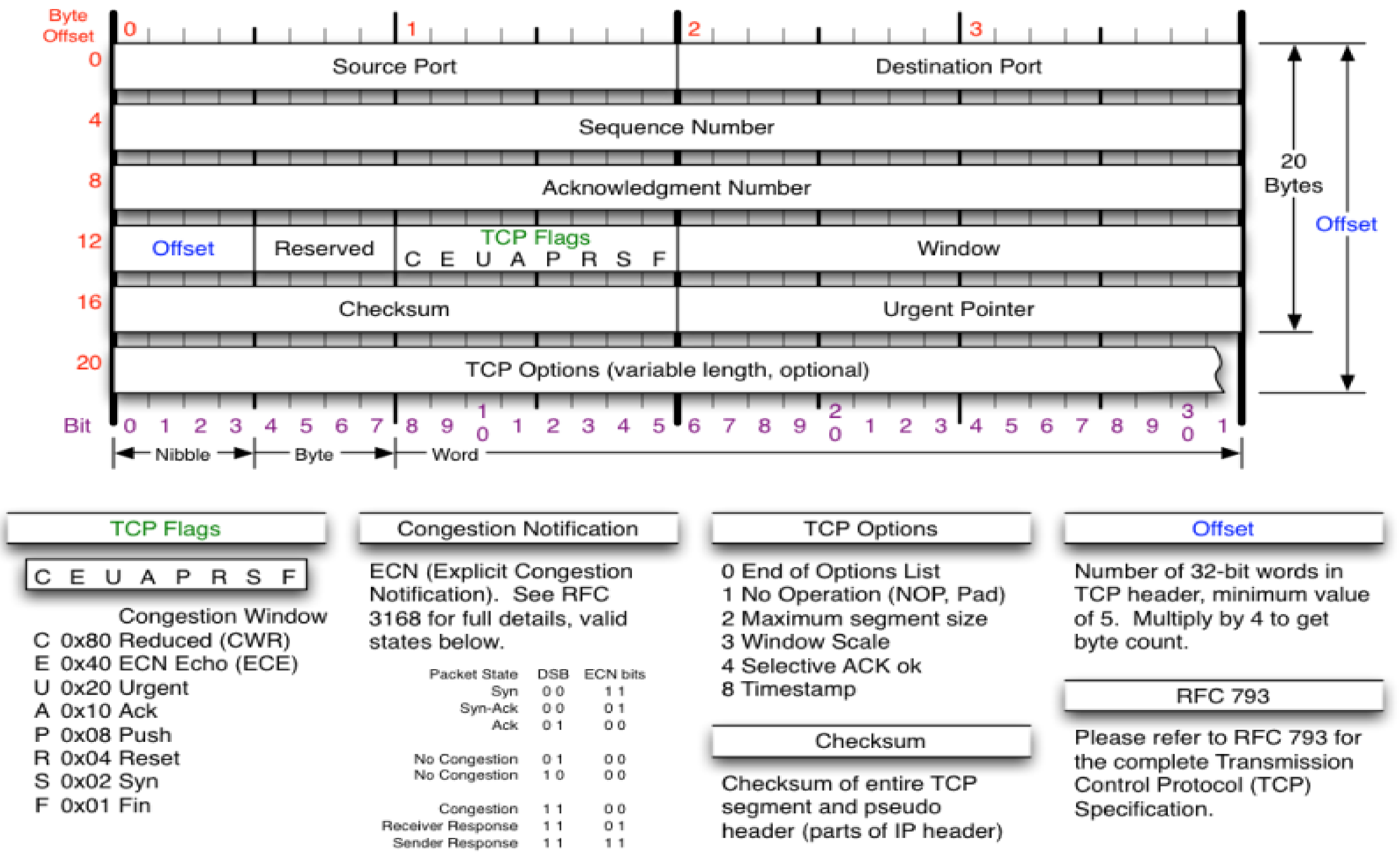


Source http://www.troyjessup.com/headers/UDP_Header.png

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TCP Header Format



Byte Offset	0	1	2	3
0	Source Port		Destination Port	
4	Sequence Number			
8	Acknowledgment Number			
12	Offset Reserved	TCP Flags C E U A P R S F	Window	
16	Checksum		Urgent Pointer	
20	TCP Options (variable length, optional)			

TCP Flags

C E U A P R S F

		Congestion Window
C	0x80	Reduced (CWR)
E	0x40	ECN Echo (ECE)
U	0x20	Urgent
A	0x10	Ack
P	0x08	Push
R	0x04	Reset
S	0x02	Syn
F	0x01	Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Source http://nmap.org/book/images/hdr/MJB-TCP-Header-800x564.png

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TCP Header

- **Source Port**
- **Destination Port**
- **Sequence Number**
- **Acknowledgment Number**

ACK Number = Incoming Sequence Number + Bytes Received

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP Header - Flags

- **URG** (Urgent) – Rarely used; indicates the Urgent Pointer field should be examined.
- **ACK** (Acknowledgement) - Segment contains an acknowledgment. Every segment should have ACK except for SYN or RST segments.
- **PSH** (Push) – Bypass buffering and send/receive the data immediately.
- **RST** (Reset) – Abnormal session termination, close the connection explicitly
- **SYN** (Synchronize) - Synchronize Sequence Numbers to establish a connection
- **FIN** (Finish) – Transaction finished, no more data from sender (but doesn’t close connection explicitly)

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TCP Options

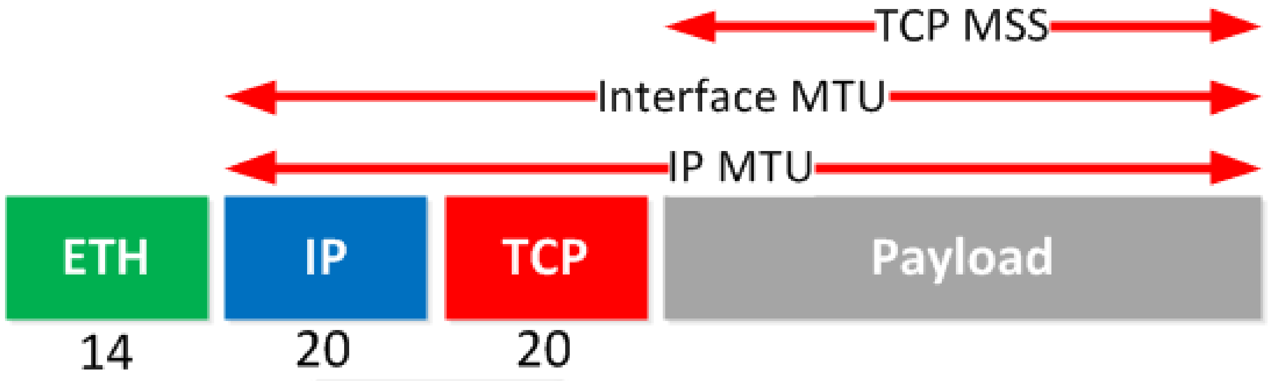
- Options are at the end of the standard TCP header and are a multiple of 8 bits in length.
    - 1 Byte Option Kind
        - Kind = 0: End of option list
        - Kind = 1: No Op (used for padding to make the header an even multiple of 32 bits)
    - 1 Byte Option Kind, 1 Byte Option Length, Option Data

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP Option – Maximum Segment Size (MSS)
Kind=2, Length=4

- Defines the Maximum Segment Size (MSS) to be used during a connection between 2 hosts – max number of bytes that can be received in a single TCP segment (not counting headers)
- Appears only in SYN, SYN/ACK.
- Both sides use the lower of the two advertised MSS values.
- MSS vs. MTU; e.g, if MTU=1500, what's the largest possible MSS?
- If MSS is omitted by one or both ends, default=536 bytes



Source: *https://networklessons.com/cisco/ccie-routing-switching/pppoe-mtu-troubleshooting-cisco-ios/*

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TCP Option – Window Scaling (RFC 1323)
Kind=3, Length=3

- Window Size (16 bits) – max amount of received data that can be buffered at one time on the receiving side. Max = 65,535 bytes.
- To take advantage of a network with high bandwidth and high delay. E.g, 10 Mbps with RTT=200ms.

  Max amount of data in *one-way* transit = B x D

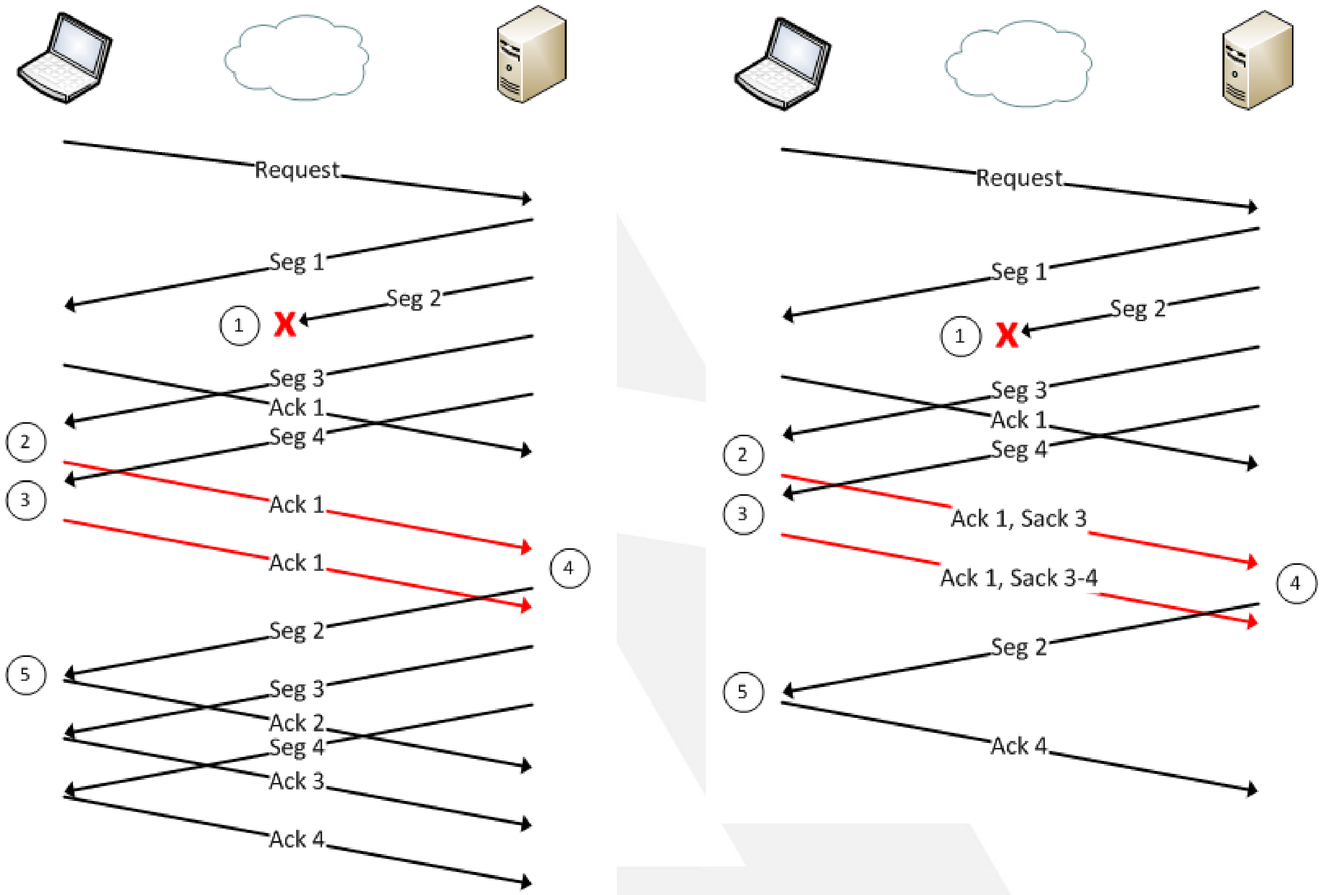
  10 Mbps x 0.1 s = 1 Mb = 125,000 bytes vs. 65,535 (52% utilization)
- Use the *Window Scaling* option to increase the TCP Receive Window Size above its max value of 65,535 bytes.
- It specifies an 8-byte shift count; max = 14. So the effective max window size is 2^{16+14} = 1 GB
- This option is sent only in a SYN segment. The scale multiplier remains static for the duration of the TCP connection.
- Window Scaling is only in effect if both sides include the option. The shift count may be 0: offering to scale, while applying a scale factor of 1 to its own receive window.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP Option – Selective ACK (RFC 2018)
Kind=5,Length=variable

- Cumulative ACK vs. Selective ACK (SACK)
- Cut down # of retransmissions
- Check both sides are supporting SACK

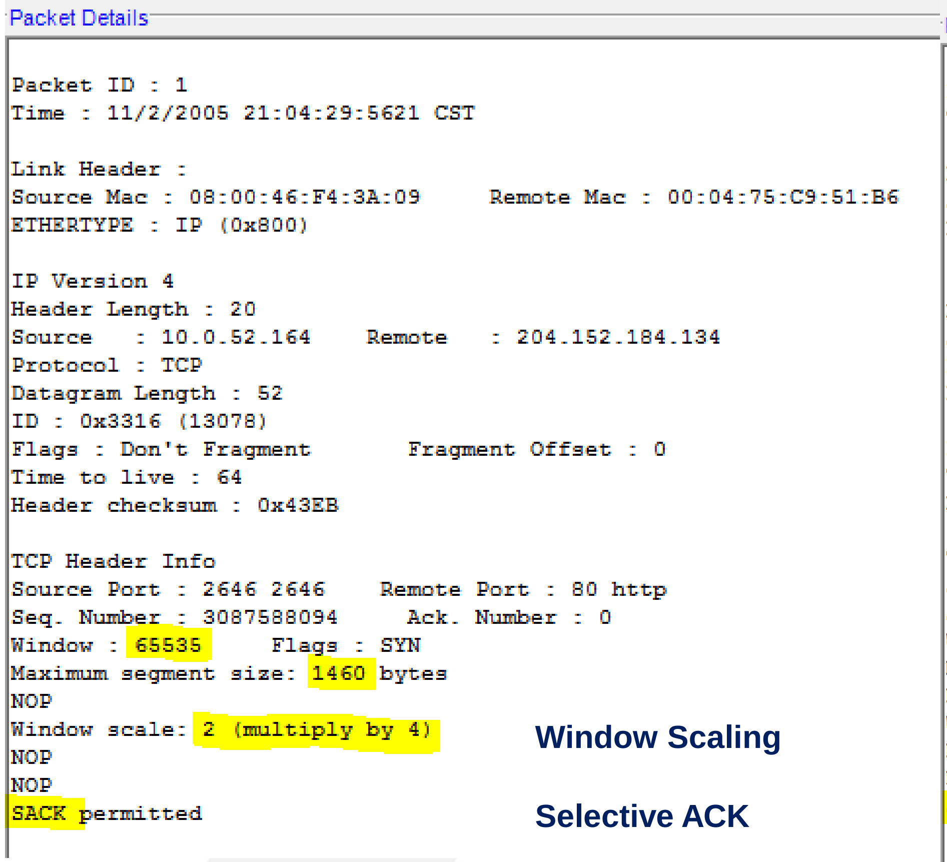


Source: *http://packetlife.net/blog/2010/jun/17/tcp-selective-acknowledgments-sack/*

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP Options – MSS, Window Scaling, SACK

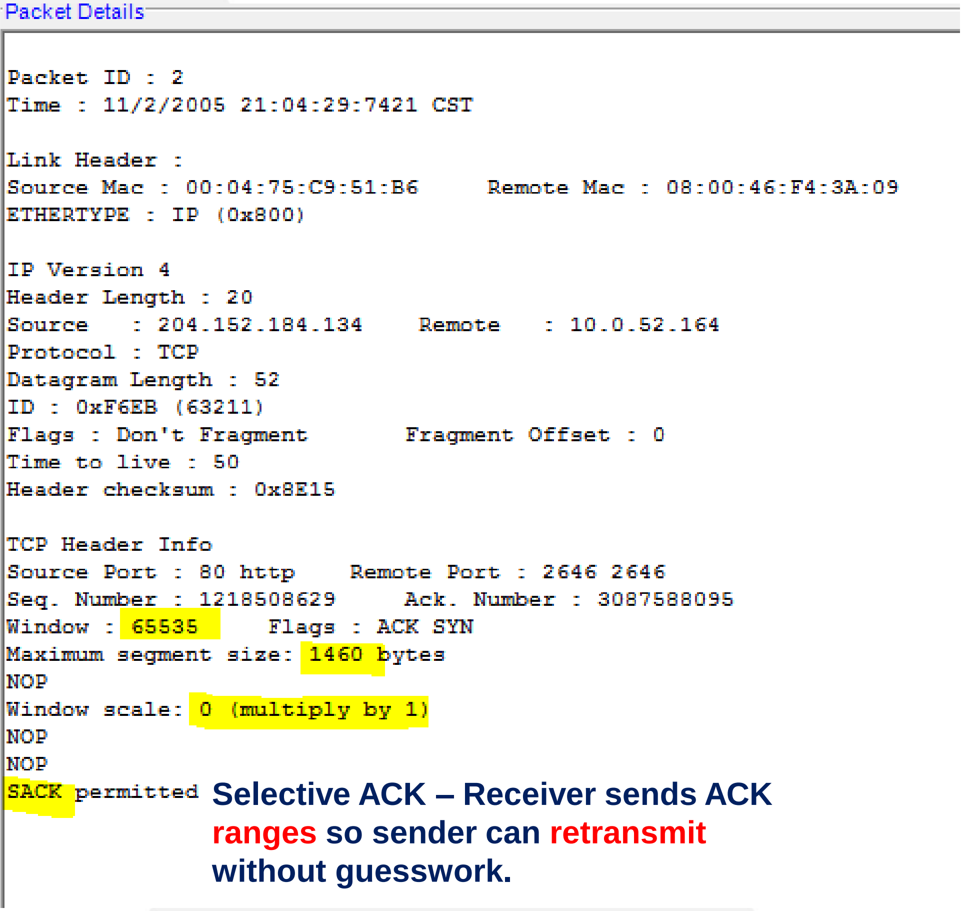


Packet Details

```
Packet ID : 1
Time : 11/2/2005 21:04:29:5621 CST

Link Header :
Source Mac : 08:00:46:F4:3A:09     Remote Mac : 00:04:75:C9:51:B6
ETHERTYPE : IP (0x800)

IP Version 4
Header Length : 20
Source    : 10.0.52.164    Remote    : 204.152.184.134
Protocol : TCP
Datagram Length : 52
ID : 0x3316 (13078)
Flags : Don't Fragment       Fragment Offset : 0
Time to live : 64
Header checksum : 0x43EB

TCP Header Info
Source Port : 2646 2646    Remote Port : 80 http
Seq. Number : 3087588094     Ack. Number : 0
Window : 65535      Flags : SYN
Maximum segment size: 1460 bytes
NOP
Window scale: 2 (multiply by 4)
NOP
NOP
SACK permitted
```

Window Scaling

Selective ACK



Packet Details

```
Packet ID : 2
Time : 11/2/2005 21:04:29:7421 CST

Link Header :
Source Mac : 00:04:75:C9:51:B6     Remote Mac : 08:00:46:F4:3A:09
ETHERTYPE : IP (0x800)

IP Version 4
Header Length : 20
Source    : 204.152.184.134    Remote    : 10.0.52.164
Protocol : TCP
Datagram Length : 52
ID : 0xF6EB (63211)
Flags : Don't Fragment       Fragment Offset : 0
Time to live : 50
Header checksum : 0x8E15

TCP Header Info
Source Port : 80 http    Remote Port : 2646 2646
Seq. Number : 1218508629     Ack. Number : 3087588095
Window : 65535      Flags : ACK SYN
Maximum segment size: 1460 bytes
NOP
Window scale: 0 (multiply by 1)
NOP
NOP
SACK permitted
```

Selective ACK – Receiver sends ACK ranges so sender can retransmit without guesswork.

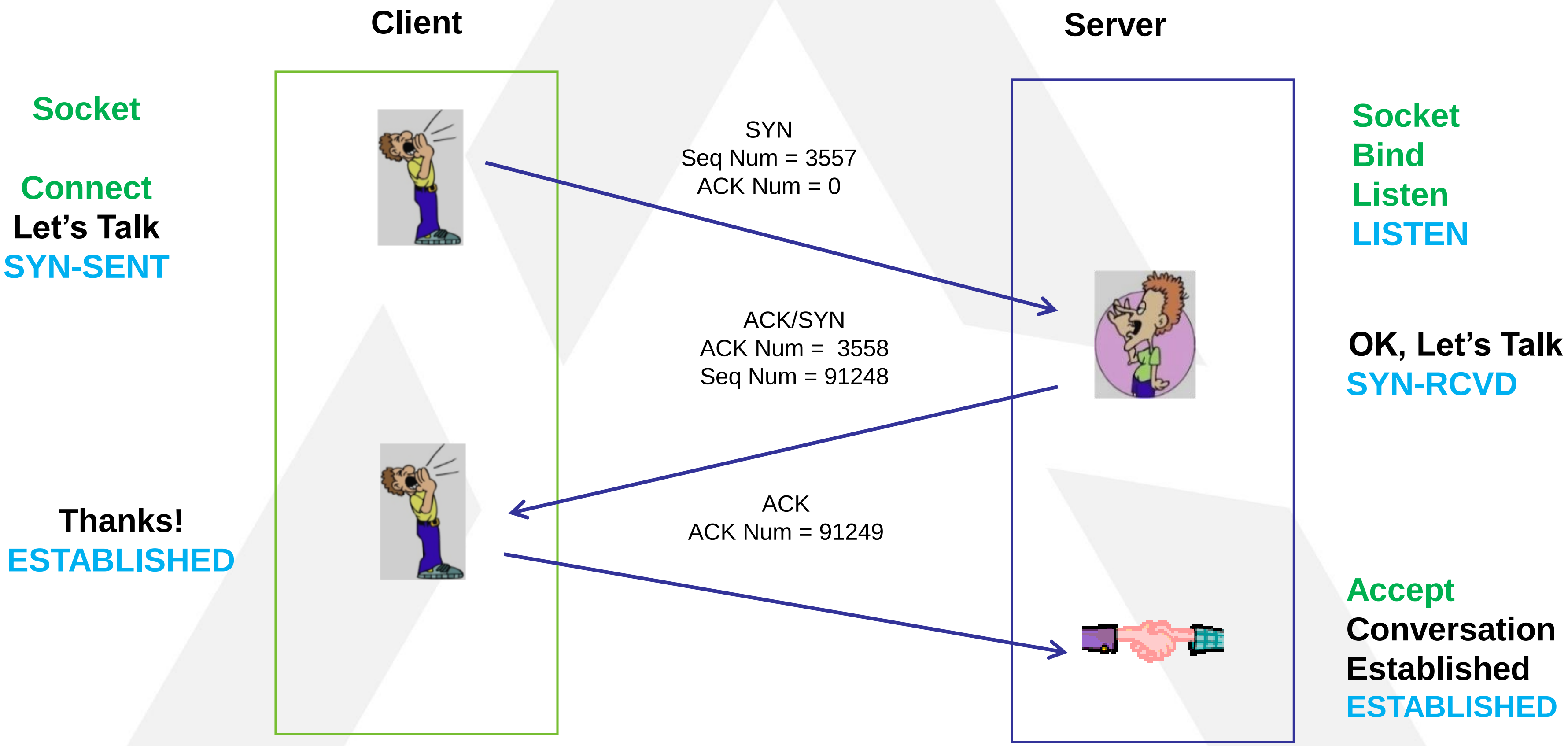
- ***What's the actual Window size?***
- ***What's the MTU?***

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP - Establishing a Connection

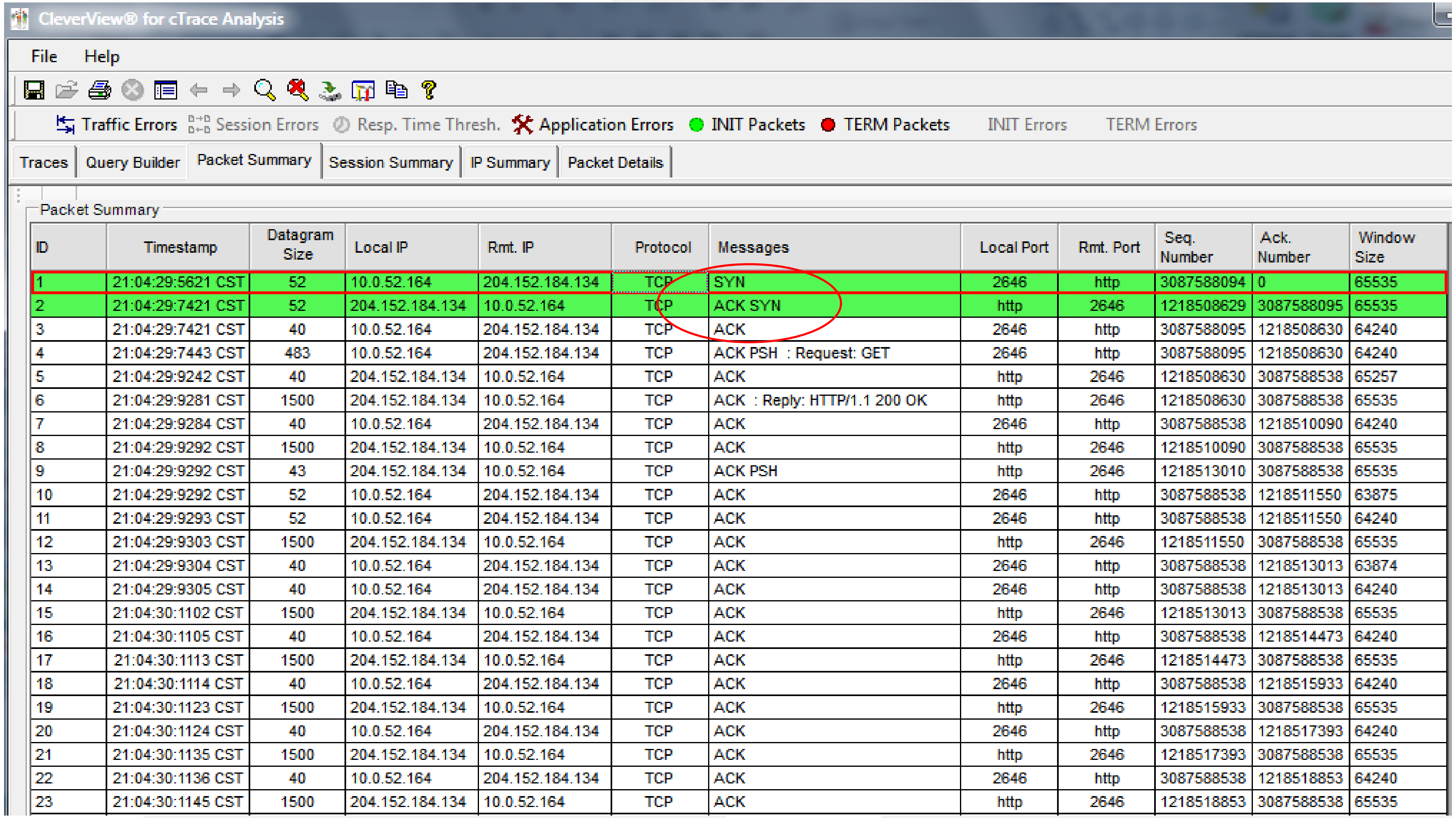
The 3 Way Handshake (3 segments)



Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP - Establishing a Connection



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	21:04:29:5621 CST	52	10.0.52.164	204.152.184.134	TCP	SYN	2646	http	3087588094	0	65535
2	21:04:29:7421 CST	52	204.152.184.134	10.0.52.164	TCP	ACK SYN	http	2646	1218508629	3087588095	65535
3	21:04:29:7421 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588095	1218508630	64240
4	21:04:29:7443 CST	483	10.0.52.164	204.152.184.134	TCP	ACK PSH : Request: GET	2646	http	3087588095	1218508630	64240
5	21:04:29:9242 CST	40	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218508630	3087588538	65257
6	21:04:29:9281 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK : Reply: HTTP/1.1 200 OK	http	2646	1218508630	3087588538	65535
7	21:04:29:9284 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218510090	64240
8	21:04:29:9292 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218510090	3087588538	65535
9	21:04:29:9292 CST	43	204.152.184.134	10.0.52.164	TCP	ACK PSH	http	2646	1218513010	3087588538	65535
10	21:04:29:9292 CST	52	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218511550	63875
11	21:04:29:9293 CST	52	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218511550	64240
12	21:04:29:9303 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218511550	3087588538	65535
13	21:04:29:9304 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218513013	63874
14	21:04:29:9305 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218513013	64240
15	21:04:30:1102 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218513013	3087588538	65535
16	21:04:30:1105 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218514473	64240
17	21:04:30:1113 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218514473	3087588538	65535
18	21:04:30:1114 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218515933	64240
19	21:04:30:1123 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218515933	3087588538	65535
20	21:04:30:1124 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218517393	64240
21	21:04:30:1135 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218517393	3087588538	65535
22	21:04:30:1136 CST	40	10.0.52.164	204.152.184.134	TCP	ACK	2646	http	3087588538	1218518853	64240
23	21:04:30:1145 CST	1500	204.152.184.134	10.0.52.164	TCP	ACK	http	2646	1218518853	3087588538	65535

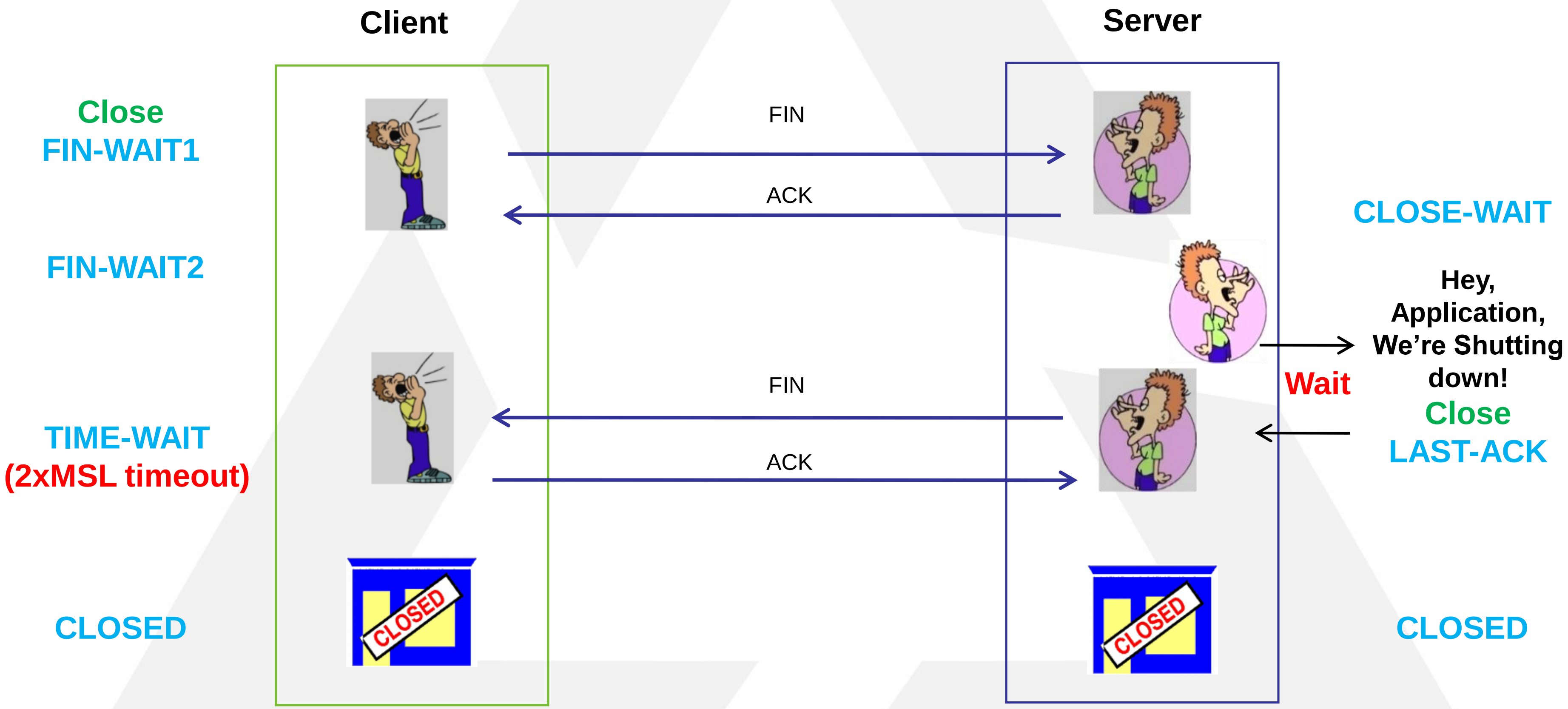
Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP - Connection Termination

4 segments to terminate.

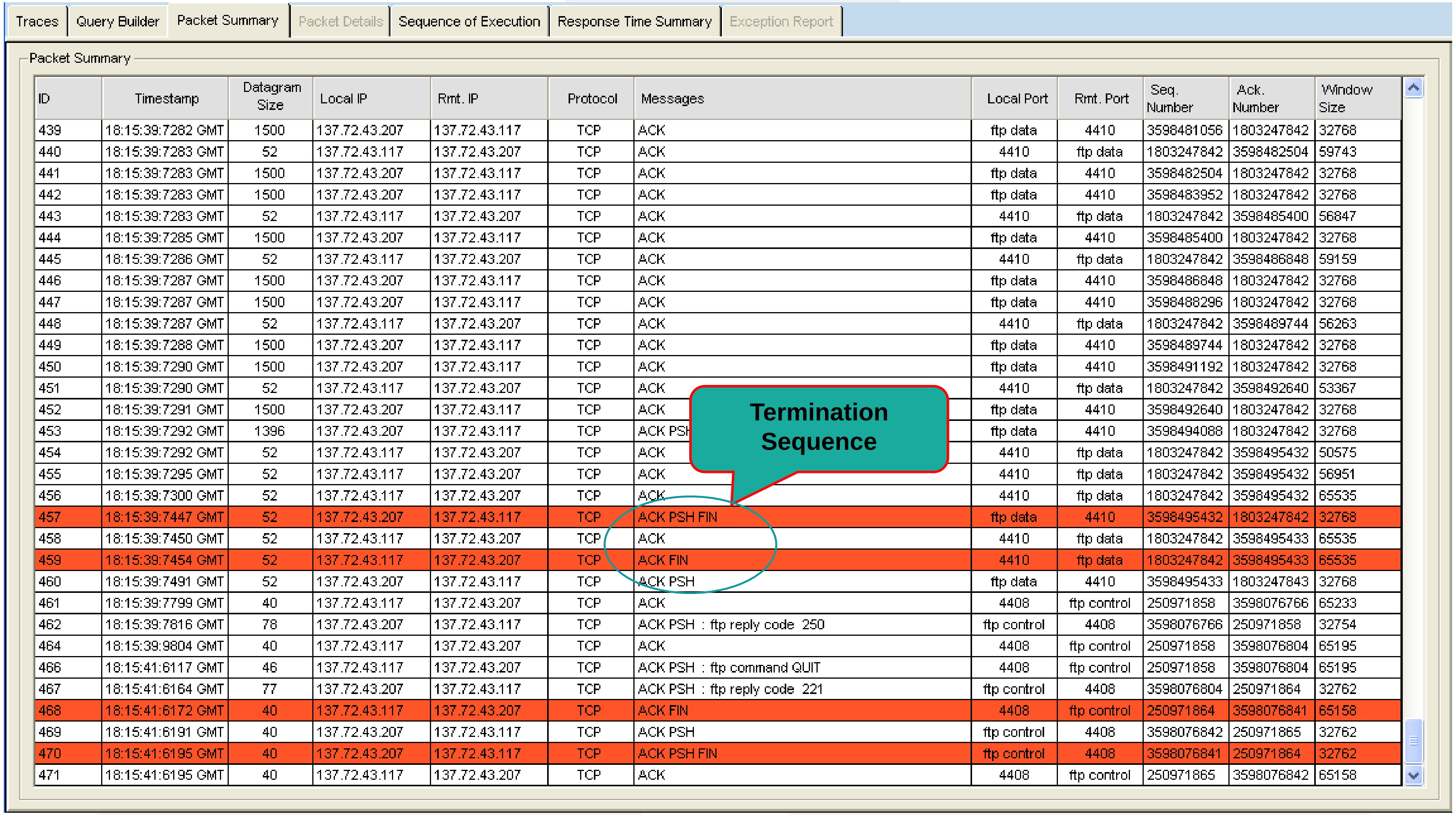
TCP half-close: allows one end to terminate its output, while still receiving data from the other end)



Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TCP - Connection Termination

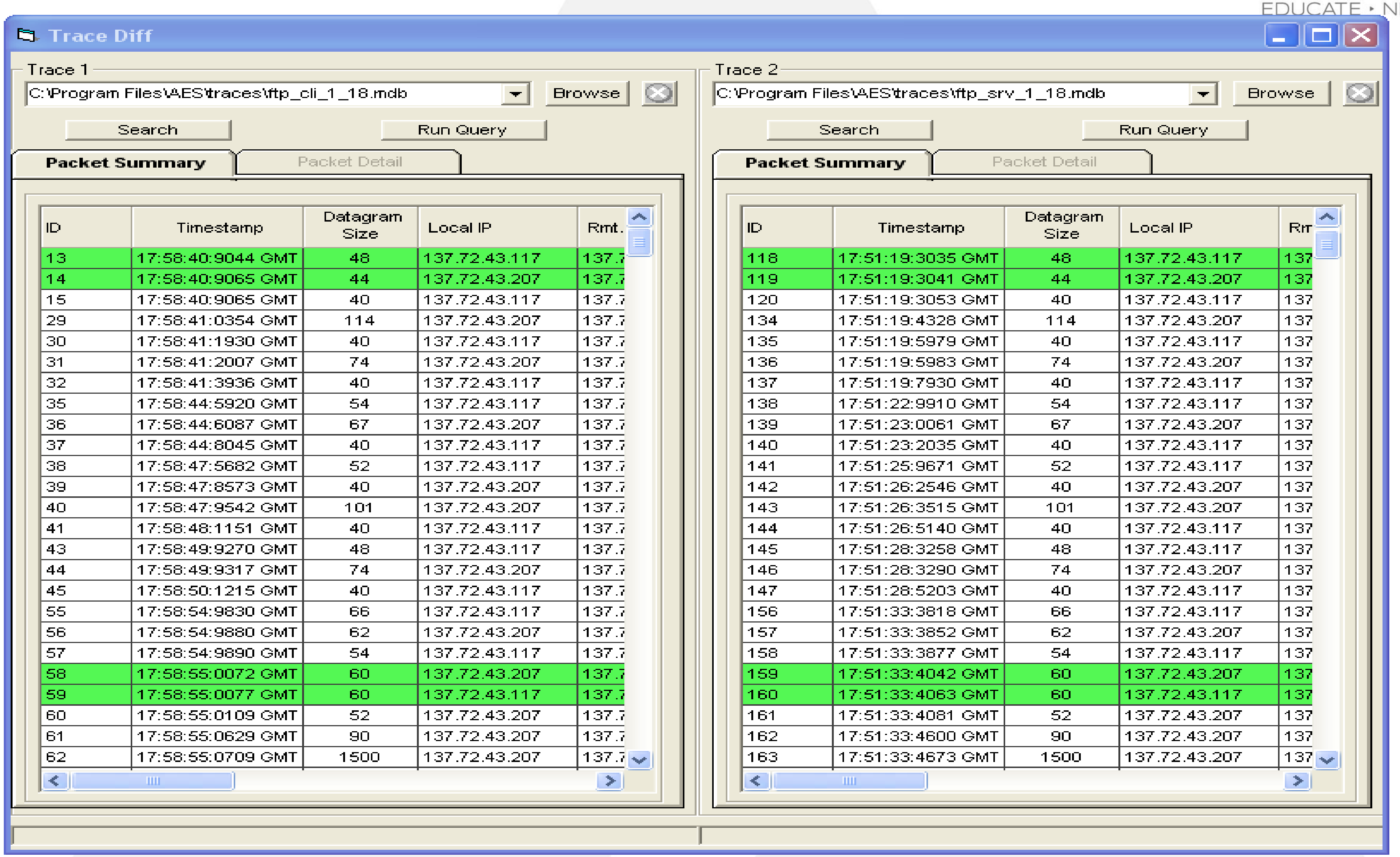


ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
439	18:15:39:7282 GMT	1500	137.72.43.207	137.72.43.117	TCP	ACK	ftp data	4410	3598481056	1803247842	32768
440	18:15:39:7283 GMT	52	137.72.43.117	137.72.43.207	TCP	ACK	4410	ftp data	1803247842	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 PSH	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

Termination Sequence

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Comparing Traces – Baselining; Multiple Trace Points



Trace 1: C:\Program Files\AES\traces\ftp_cli_1_18.mdb

ID	Timestamp	Datagram Size	Local IP	Rmt.
13	17:58:40:9044 GMT	48	137.72.43.117	137.7
14	17:58:40:9065 GMT	44	137.72.43.207	137.7
15	17:58:40:9065 GMT	40	137.72.43.117	137.7
29	17:58:41:0354 GMT	114	137.72.43.207	137.7
30	17:58:41:1930 GMT	40	137.72.43.117	137.7
31	17:58:41:2007 GMT	74	137.72.43.207	137.7
32	17:58:41:3936 GMT	40	137.72.43.117	137.7
35	17:58:44:5920 GMT	54	137.72.43.117	137.7
36	17:58:44:6087 GMT	67	137.72.43.207	137.7
37	17:58:44:8045 GMT	40	137.72.43.117	137.7
38	17:58:47:5682 GMT	52	137.72.43.117	137.7
39	17:58:47:8573 GMT	40	137.72.43.207	137.7
40	17:58:47:9542 GMT	101	137.72.43.207	137.7
41	17:58:48:1151 GMT	40	137.72.43.117	137.7
43	17:58:49:9270 GMT	48	137.72.43.117	137.7
44	17:58:49:9317 GMT	74	137.72.43.207	137.7
45	17:58:50:1215 GMT	40	137.72.43.117	137.7
55	17:58:54:9830 GMT	66	137.72.43.117	137.7
56	17:58:54:9880 GMT	62	137.72.43.207	137.7
57	17:58:54:9890 GMT	54	137.72.43.117	137.7
58	17:58:55:0072 GMT	60	137.72.43.207	137.7
59	17:58:55:0077 GMT	60	137.72.43.117	137.7
60	17:58:55:0109 GMT	52	137.72.43.207	137.7
61	17:58:55:0629 GMT	90	137.72.43.207	137.7
62	17:58:55:0709 GMT	1500	137.72.43.207	137.7

Trace 2: C:\Program Files\AES\traces\ftp_srv_1_18.mdb

ID	Timestamp	Datagram Size	Local IP	Rm
118	17:51:19:3035 GMT	48	137.72.43.117	137
119	17:51:19:3041 GMT	44	137.72.43.207	137
120	17:51:19:3053 GMT	40	137.72.43.117	137
134	17:51:19:4328 GMT	114	137.72.43.207	137
135	17:51:19:5979 GMT	40	137.72.43.117	137
136	17:51:19:5983 GMT	74	137.72.43.207	137
137	17:51:19:7930 GMT	40	137.72.43.117	137
138	17:51:22:9910 GMT	54	137.72.43.117	137
139	17:51:23:0061 GMT	67	137.72.43.207	137
140	17:51:23:2035 GMT	40	137.72.43.117	137
141	17:51:25:9671 GMT	52	137.72.43.117	137
142	17:51:26:2546 GMT	40	137.72.43.207	137
143	17:51:26:3515 GMT	101	137.72.43.207	137
144	17:51:26:5140 GMT	40	137.72.43.117	137
145	17:51:28:3258 GMT	48	137.72.43.117	137
146	17:51:28:3290 GMT	74	137.72.43.207	137
147	17:51:28:5203 GMT	40	137.72.43.117	137
156	17:51:33:3818 GMT	66	137.72.43.117	137
157	17:51:33:3852 GMT	62	137.72.43.207	137
158	17:51:33:3877 GMT	54	137.72.43.117	137
159	17:51:33:4042 GMT	60	137.72.43.207	137
160	17:51:33:4063 GMT	60	137.72.43.117	137
161	17:51:33:4081 GMT	52	137.72.43.207	137
162	17:51:33:4600 GMT	90	137.72.43.207	137
163	17:51:33:4673 GMT	1500	137.72.43.207	137

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Inferring Packet Loss from Duplicate ACKs

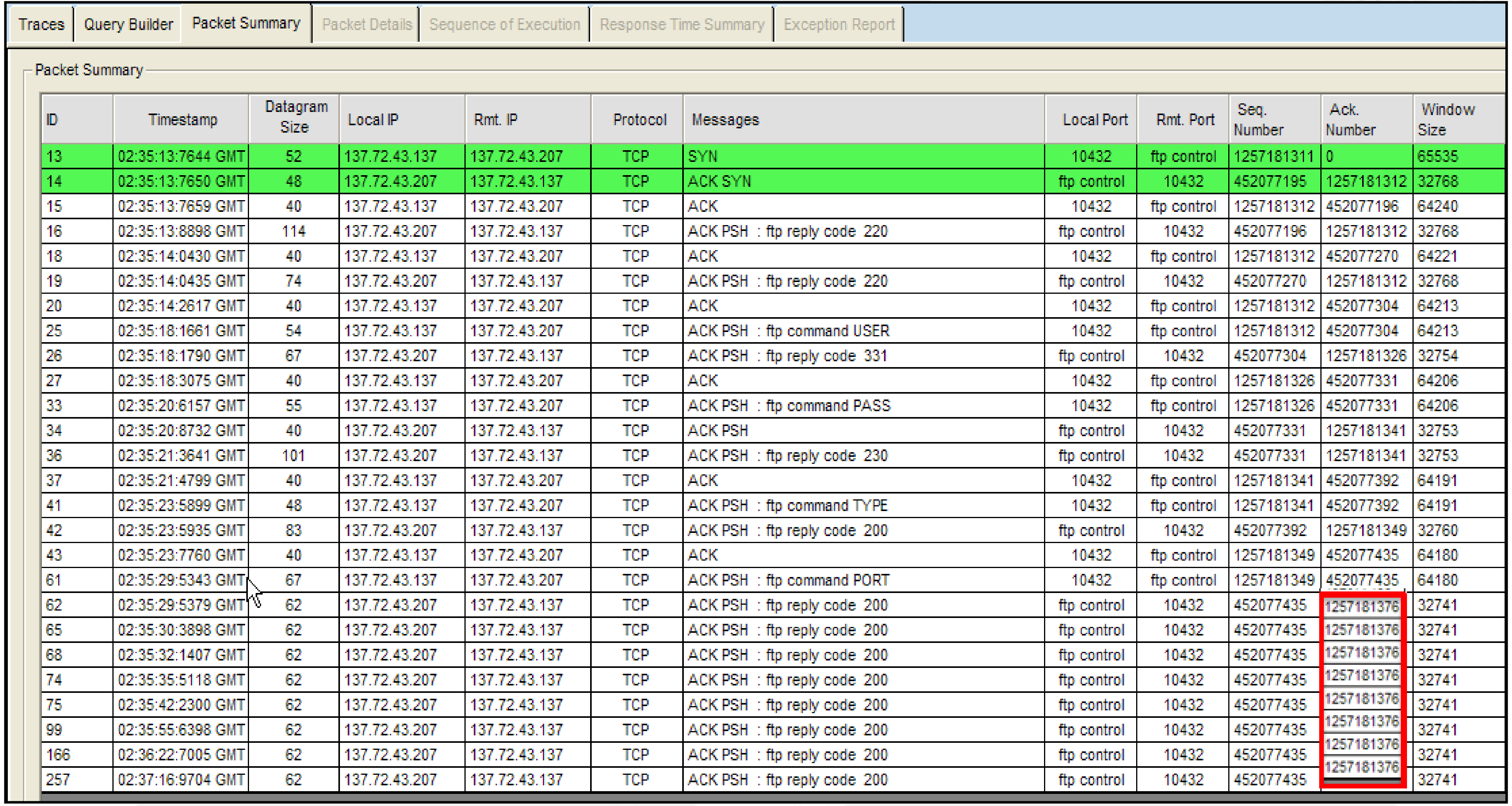
- Duplicate ACKs tells us:
  - Some new data did arrive but it was not next segment
  - The next segment might be lost

- Treat 3 (usually) Duplicate ACKs as a loss
  - Retransmit next expected segment before Retransmission Timeout (RTO) - Fast Retransmit

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Inferring Packet Loss from Duplicate ACKs



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

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TCP Zero Window Size

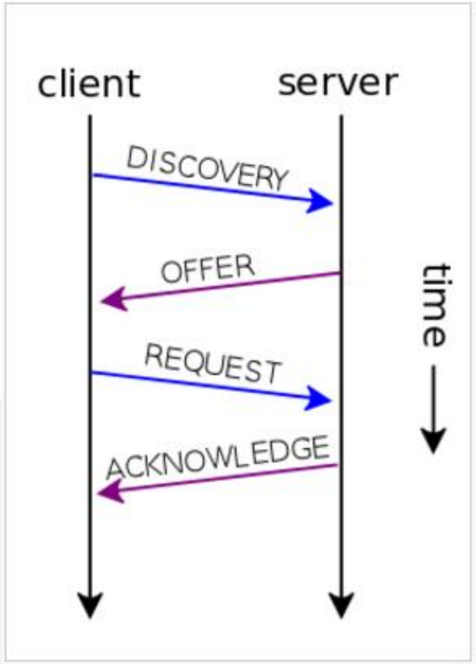
- The receiver is not able to receive any data at the moment because the receive buffer is “full”.
- The sender will wait for a while and retry. If this goes on long enough, the sender will reset the connection.
- NOT a network problem

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

DHCP

- UDP Port 67 – Server daemon
- UDP Port 68 – Client process
- Transaction ID – keeping track of responses and requests
- DHCP Message Types:
  1. DHCP Discover
  2. DHCP Offer
  3. DHCP Request
  4. DHCP Decline
  5. DHCP Acknowledgement
  6. DHCP Negative Acknowledgement (NACK)
  7. DHCP Release
  8. DHCP Informational

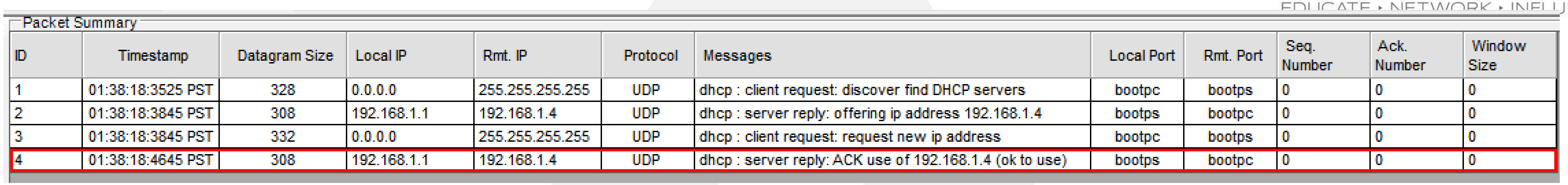


https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

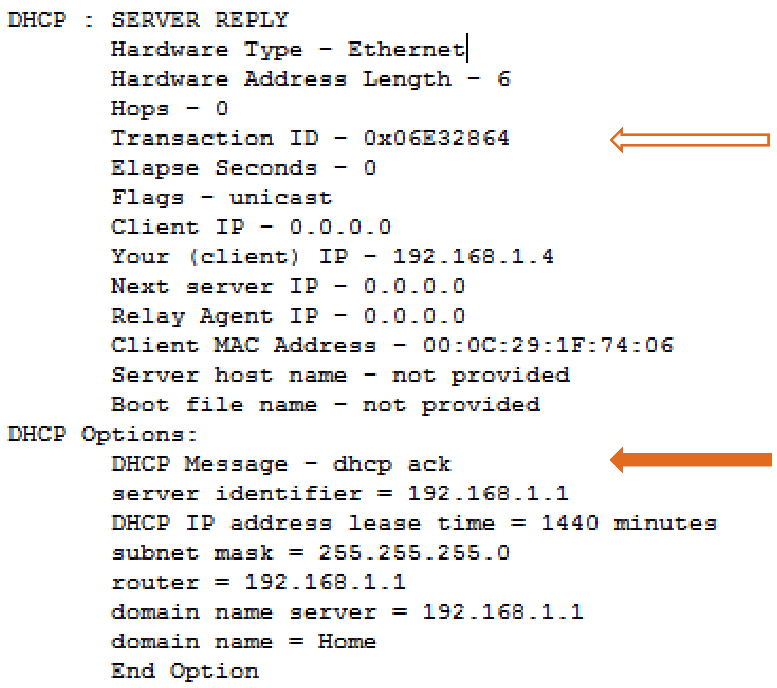
DHCP Normal Sequence



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	01:38:18:3525 PST	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: discover find DHCP servers	bootpc	bootps	0	0	0
2	01:38:18:3845 PST	308	192.168.1.1	192.168.1.4	UDP	dhcp : server reply: offering ip address 192.168.1.4	bootps	bootpc	0	0	0
3	01:38:18:3845 PST	332	0.0.0.0	255.255.255.255	UDP	dhcp : client request: request new ip address	bootpc	bootps	0	0	0
4	01:38:18:4645 PST	308	192.168.1.1	192.168.1.4	UDP	dhcp : server reply: ACK use of 192.168.1.4 (ok to use)	bootps	bootpc	0	0	0

DHCP Discover (Msg Type 1) -> Offer (2) -> Request (3) -> Ack (5)



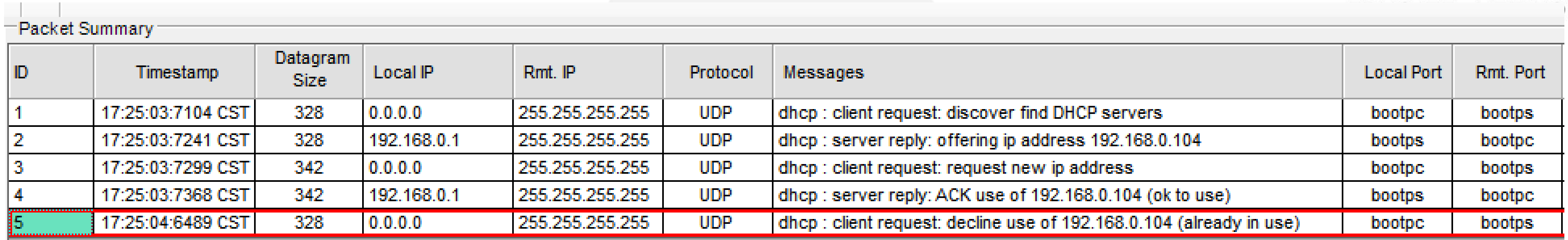
```
DHCP : SERVER REPLY
       Hardware Type - Ethernet
       Hardware Address Length - 6
       Hops - 0
       Transaction ID - 0x06E32864
       Elapse Seconds - 0
       Flags - unicast
       Client IP - 0.0.0.0
       Your (client) IP - 192.168.1.4
       Next server IP - 0.0.0.0
       Relay Agent IP - 0.0.0.0
       Client MAC Address - 00:0C:29:1F:74:06
       Server host name - not provided
       Boot file name - not provided
DHCP Options:
       DHCP Message - dhcp ack
       server identifier = 192.168.1.1
       DHCP IP address lease time = 1440 minutes
       subnet mask = 255.255.255.0
       router = 192.168.1.1
       domain name server = 192.168.1.1
       domain name = Home
       End Option
```

All 4 packets have the same Transaction ID

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

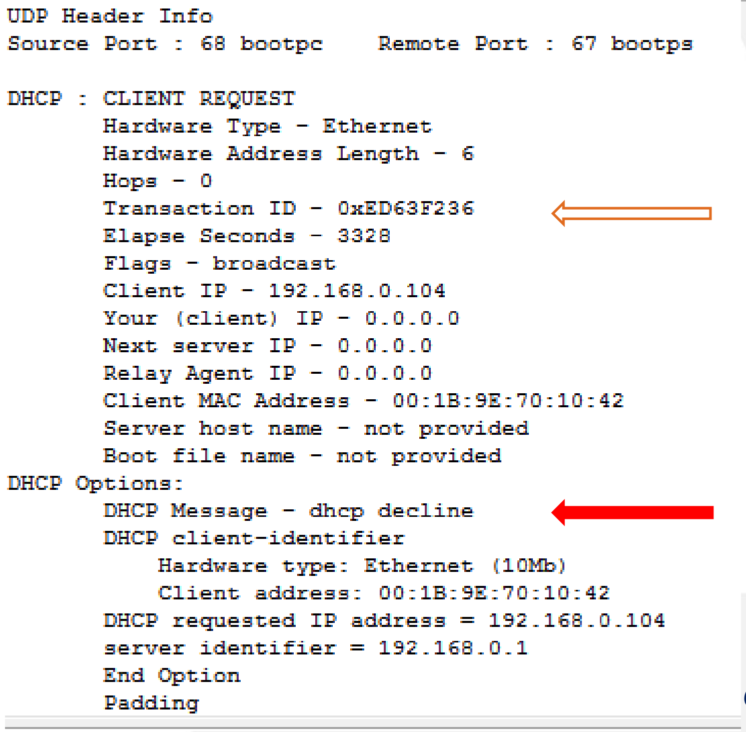
DHCP Decline sequence



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port
1	17:25:03:7104 CST	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: discover find DHCP servers	bootpc	bootps
2	17:25:03:7241 CST	328	192.168.0.1	255.255.255.255	UDP	dhcp : server reply: offering ip address 192.168.0.104	bootps	bootpc
3	17:25:03:7299 CST	342	0.0.0.0	255.255.255.255	UDP	dhcp : client request: request new ip address	bootpc	bootps
4	17:25:03:7368 CST	342	192.168.0.1	255.255.255.255	UDP	dhcp : server reply: ACK use of 192.168.0.104 (ok to use)	bootps	bootpc
5	17:25:04:6489 CST	328	0.0.0.0	255.255.255.255	UDP	dhcp : client request: decline use of 192.168.0.104 (already in use)	bootpc	bootps

DHCP Discover (Msg Type 1) -> Offer (2) -> Request (3) -> Ack (5) -> Decline (4)



```
UDP Header Info
Source Port : 68 bootpc    Remote Port : 67 bootps

DHCP : CLIENT REQUEST
       Hardware Type - Ethernet
       Hardware Address Length - 6
       Hops - 0
       Transaction ID - 0xED63F236
       Elapse Seconds - 3328
       Flags - broadcast
       Client IP - 192.168.0.104
       Your (client) IP - 0.0.0.0
       Next server IP - 0.0.0.0
       Relay Agent IP - 0.0.0.0
       Client MAC Address - 00:1B:9E:70:10:42
       Server host name - not provided
       Boot file name - not provided
DHCP Options:
       DHCP Message - dhcp decline
       DHCP client-identifier
           Hardware type: Ethernet (10Mb)
           Client address: 00:1B:9E:70:10:42
       DHCP requested IP address = 192.168.0.104
       server identifier = 192.168.0.1
       End Option
       Padding
```

All 5 packets have the same Transaction ID

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

DNS

- UDP/TCP Port **53**
  - Message ID – Transaction ID that associates DNS queries with responses
  - Some of the flags in DNS header
    - Request/Response
    - Recursion Desired (RD) – ask other DNS servers on behalf of the clients
    - Truncation Occurred (> 512 bytes) **
    - Response Code
      - 0 – No Error
      - 1 – Format Error
      - 2 – Server Failure
      - 3 – Name Error
      - 4 – Not Implemented
      - 5 – Refused

** should be using the TCP protocol

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

DNS commands

nslookup and **dig**

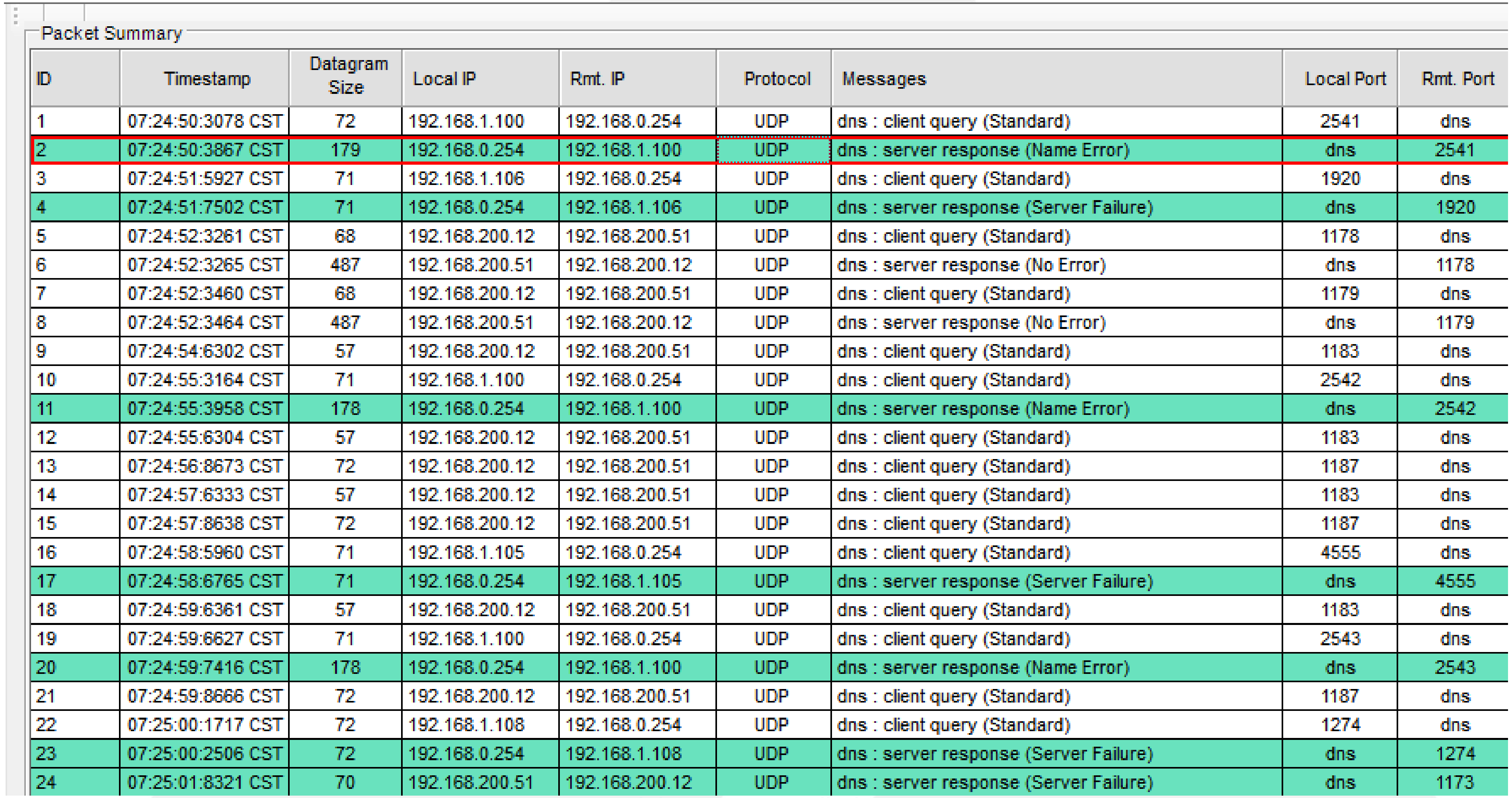
```
nslookup  share.org  8.8.8.8
nslookup  162.209.40.65  8.8.4.4
nslookup –type=mx  share.org  8.8.8.8
```

```
dig @8.8.8.8  share.org  a +short
dig @8.8.4.4 -x  162.209.40.65  +short
dig @8.8.8.8  share.org  mx +short
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

DNS Queries



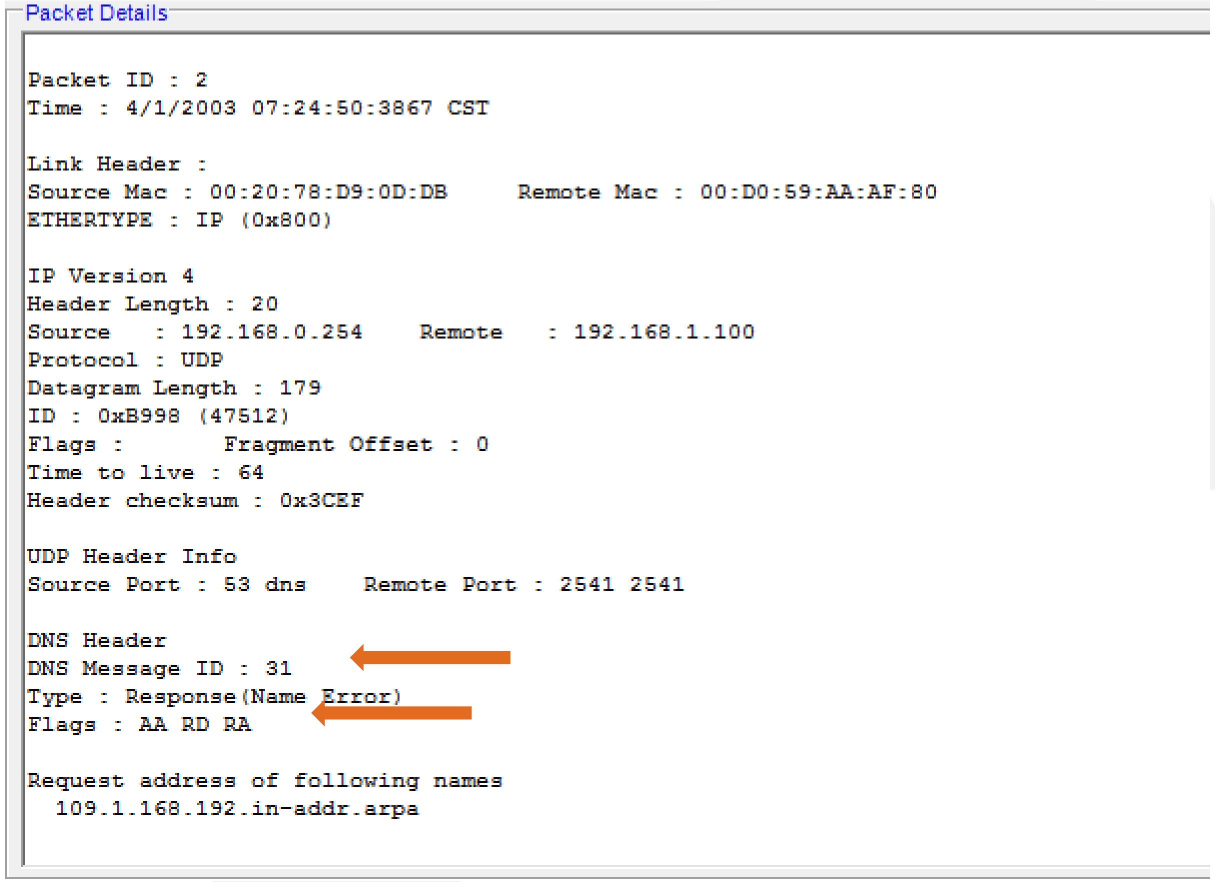
Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port
1	07:24:50:3078 CST	72	192.168.1.100	192.168.0.254	UDP	dns : client query (Standard)	2541	dns
2	07:24:50:3867 CST	179	192.168.0.254	192.168.1.100	UDP	dns : server response (Name Error)	dns	2541
3	07:24:51:5927 CST	71	192.168.1.106	192.168.0.254	UDP	dns : client query (Standard)	1920	dns
4	07:24:51:7502 CST	71	192.168.0.254	192.168.1.106	UDP	dns : server response (Server Failure)	dns	1920
5	07:24:52:3261 CST	68	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1178	dns
6	07:24:52:3265 CST	487	192.168.200.51	192.168.200.12	UDP	dns : server response (No Error)	dns	1178
7	07:24:52:3460 CST	68	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1179	dns
8	07:24:52:3464 CST	487	192.168.200.51	192.168.200.12	UDP	dns : server response (No Error)	dns	1179
9	07:24:54:6302 CST	57	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1183	dns
10	07:24:55:3164 CST	71	192.168.1.100	192.168.0.254	UDP	dns : client query (Standard)	2542	dns
11	07:24:55:3958 CST	178	192.168.0.254	192.168.1.100	UDP	dns : server response (Name Error)	dns	2542
12	07:24:55:6304 CST	57	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1183	dns
13	07:24:56:8673 CST	72	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1187	dns
14	07:24:57:6333 CST	57	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1183	dns
15	07:24:57:8638 CST	72	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1187	dns
16	07:24:58:5960 CST	71	192.168.1.105	192.168.0.254	UDP	dns : client query (Standard)	4555	dns
17	07:24:58:6765 CST	71	192.168.0.254	192.168.1.105	UDP	dns : server response (Server Failure)	dns	4555
18	07:24:59:6361 CST	57	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1183	dns
19	07:24:59:6627 CST	71	192.168.1.100	192.168.0.254	UDP	dns : client query (Standard)	2543	dns
20	07:24:59:7416 CST	178	192.168.0.254	192.168.1.100	UDP	dns : server response (Name Error)	dns	2543
21	07:24:59:8666 CST	72	192.168.200.12	192.168.200.51	UDP	dns : client query (Standard)	1187	dns
22	07:25:00:1717 CST	72	192.168.1.108	192.168.0.254	UDP	dns : client query (Standard)	1274	dns
23	07:25:00:2506 CST	72	192.168.0.254	192.168.1.108	UDP	dns : server response (Server Failure)	dns	1274
24	07:25:01:8321 CST	70	192.168.200.51	192.168.200.12	UDP	dns : server response (Server Failure)	dns	1173

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

DNS Response: Name Error



Packet Details

```
Packet ID : 2
Time : 4/1/2003 07:24:50:3867 CST

Link Header :
Source Mac : 00:20:78:D9:0D:DB     Remote Mac : 00:D0:59:AA:AF:80
ETHERTYPE : IP (0x800)

IP Version 4
Header Length : 20
Source    : 192.168.0.254    Remote    : 192.168.1.100
Protocol : UDP
Datagram Length : 179
ID : 0xB998 (47512)
Flags :        Fragment Offset : 0
Time to live : 64
Header checksum : 0x3CEF

UDP Header Info
Source Port : 53 dns    Remote Port : 2541 2541

DNS Header
DNS Message ID : 31
Type : Response(Name Error)
Flags : AA RD RA

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

Flags:

AA Authoritative Answer – response came from an authoritative server for the domain name

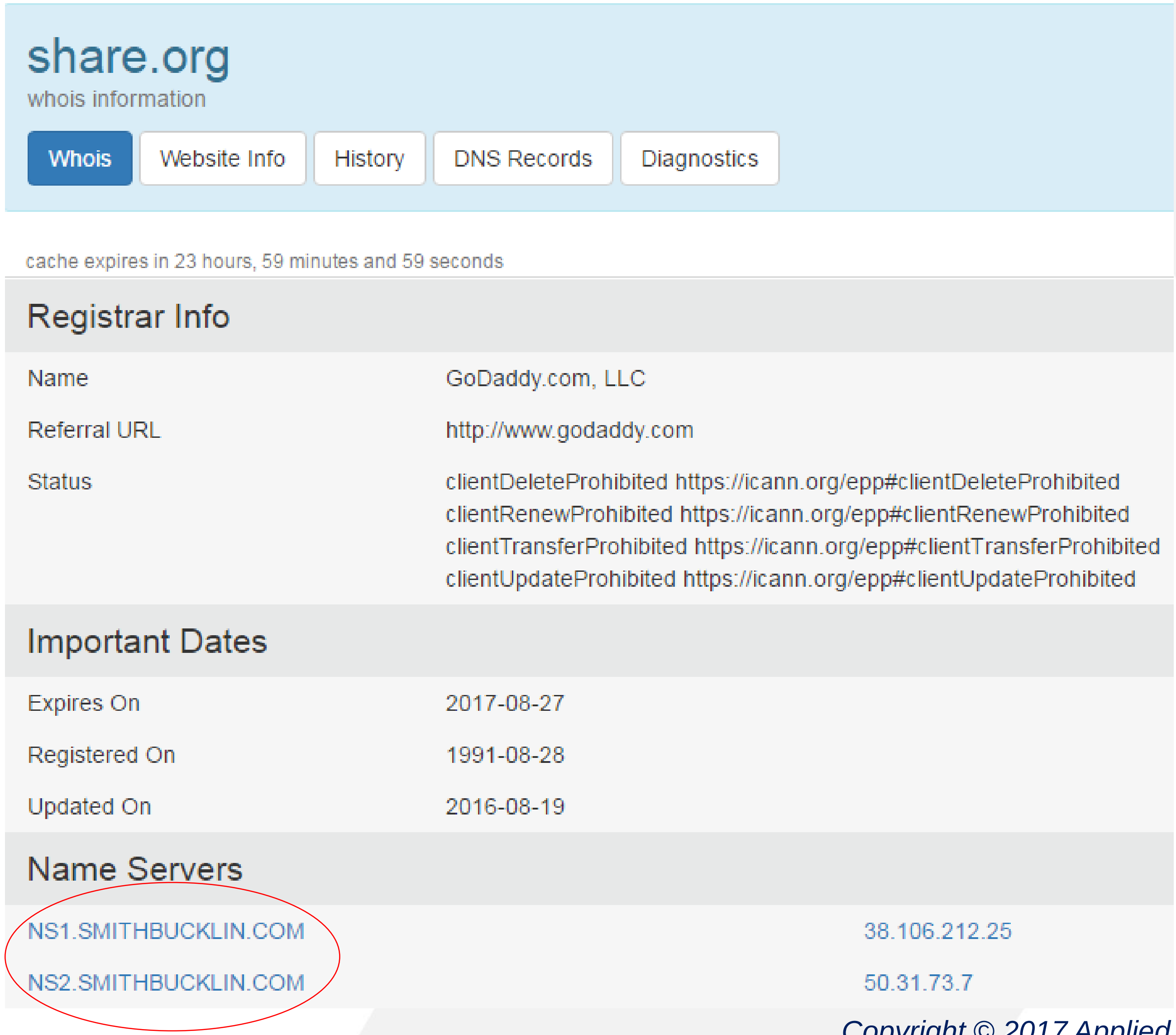
RD Recursion Desired (Root servers > Top Level Domains > Second Level Domains…..)

RA Recursion Available on this server

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

DNS Response: Authoritative vs. Non-Authoritative



share.org

whois information

cache expires in 23 hours, 59 minutes and 59 seconds

Registrar Info

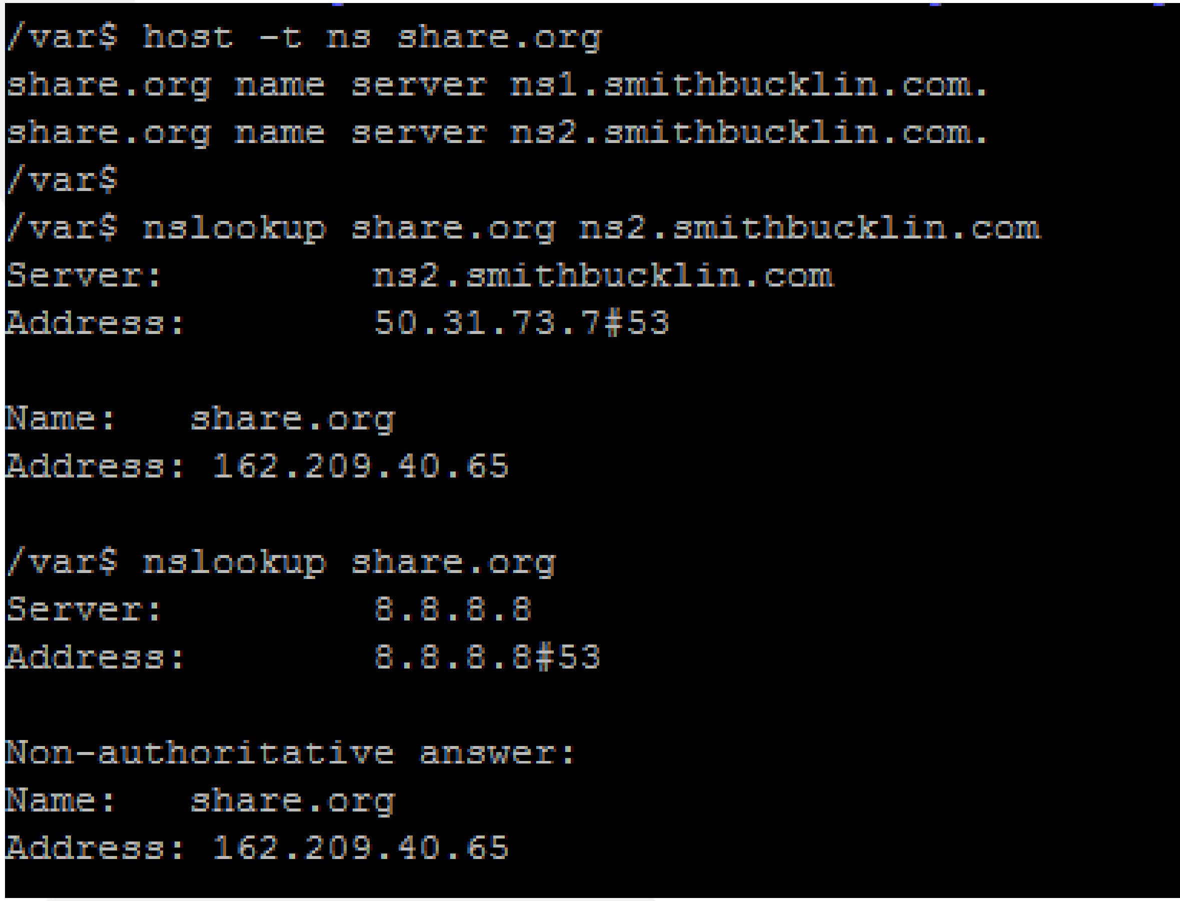
Name	GoDaddy.com, LLC
Referral URL	http://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates

Expires On	2017-08-27
Registered On	1991-08-28
Updated On	2016-08-19

Name Servers

NS1.SMITHBUCKLIN.COM	38.106.212.25
NS2.SMITHBUCKLIN.COM	50.31.73.7

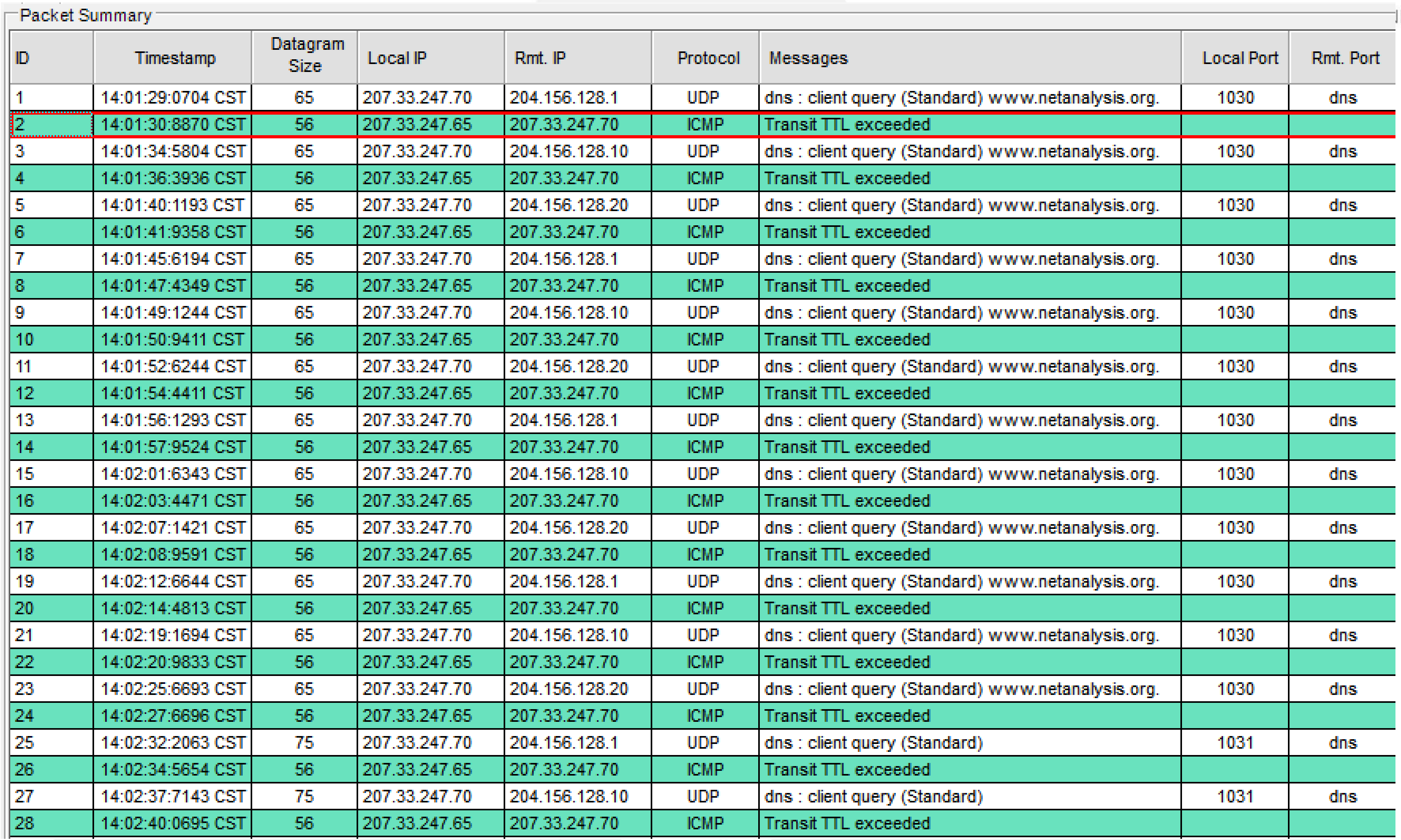


```
/var$ host -t ns share.org
share.org name server ns1.smithbucklin.com.
share.org name server ns2.smithbucklin.com.
/var$
/var$ nslookup share.org ns2.smithbucklin.com
Server:         ns2.smithbucklin.com
Address:        50.31.73.7#53

Name:   share.org
Address: 162.209.40.65

/var$ nslookup share.org
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   share.org
Address: 162.209.40.65
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

DNS Queries – routing problem



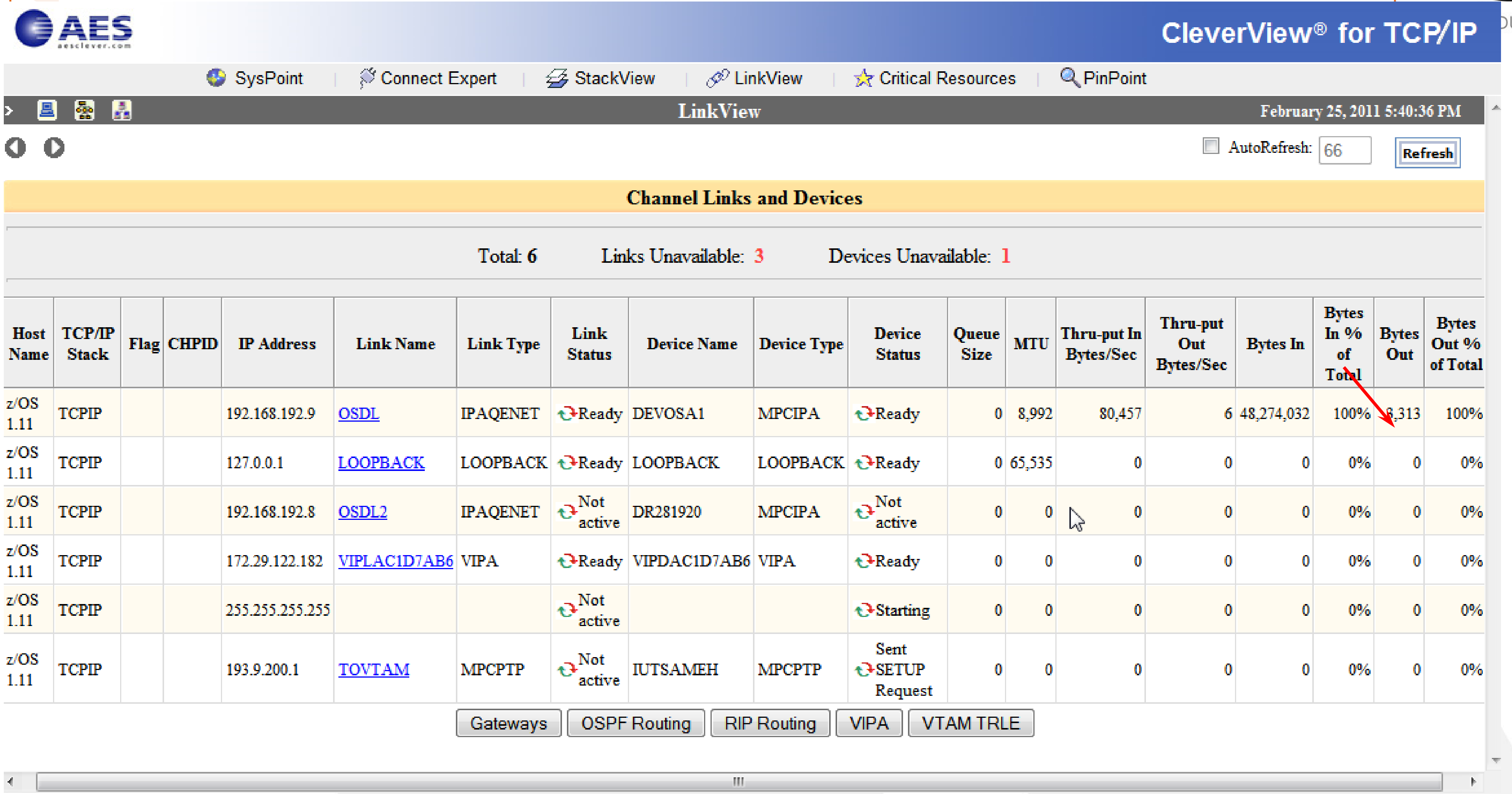
Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port
1	14:01:29:0704 CST	65	207.33.247.70	204.156.128.1	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
2	14:01:30:8870 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
3	14:01:34:5804 CST	65	207.33.247.70	204.156.128.10	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
4	14:01:36:3936 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
5	14:01:40:1193 CST	65	207.33.247.70	204.156.128.20	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
6	14:01:41:9358 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
7	14:01:45:6194 CST	65	207.33.247.70	204.156.128.1	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
8	14:01:47:4349 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
9	14:01:49:1244 CST	65	207.33.247.70	204.156.128.10	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
10	14:01:50:9411 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
11	14:01:52:6244 CST	65	207.33.247.70	204.156.128.20	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
12	14:01:54:4411 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
13	14:01:56:1293 CST	65	207.33.247.70	204.156.128.1	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
14	14:01:57:9524 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
15	14:02:01:6343 CST	65	207.33.247.70	204.156.128.10	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
16	14:02:03:4471 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
17	14:02:07:1421 CST	65	207.33.247.70	204.156.128.20	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
18	14:02:08:9591 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
19	14:02:12:6644 CST	65	207.33.247.70	204.156.128.1	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
20	14:02:14:4813 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
21	14:02:19:1694 CST	65	207.33.247.70	204.156.128.10	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
22	14:02:20:9833 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
23	14:02:25:6693 CST	65	207.33.247.70	204.156.128.20	UDP	dns : client query (Standard) www.netanalysis.org.	1030	dns
24	14:02:27:6696 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
25	14:02:32:2063 CST	75	207.33.247.70	204.156.128.1	UDP	dns : client query (Standard)	1031	dns
26	14:02:34:5654 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		
27	14:02:37:7143 CST	75	207.33.247.70	204.156.128.10	UDP	dns : client query (Standard)	1031	dns
28	14:02:40:0695 CST	56	207.33.247.65	207.33.247.70	ICMP	Transit TTL exceeded		

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

OSA –Excessive Inbound Packets in Real-Time Monitoring



Channel Links and Devices

Total: 6   Links Unavailable: 3   Devices Unavailable: 1

Host Name	TCP/IP Stack	Flag	CHPID	IP Address	Link Name	Link Type	Link Status	Device Name	Device Type	Device Status	Queue Size	MTU	Thru-put In Bytes/Sec	Thru-put Out Bytes/Sec	Bytes In	Bytes In % of Total	Bytes Out	Bytes Out % of Total
z/OS 1.11	TCPIP			192.168.192.9	OSDL	IPAQENET	Ready	DEVOSA1	MPCIPA	Ready	0	8,992	80,457	6	48,274,032	100%	8,313	100%
z/OS 1.11	TCPIP			127.0.0.1	LOOPBACK	LOOPBACK	Ready	LOOPBACK	LOOPBACK	Ready	0	65,535	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			192.168.192.8	OSDL2	IPAQENET	Not active	DR281920	MPCIPA	Not active	0	0	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			172.29.122.182	VIPLAC1D7AB6	VIPA	Ready	VIPDAC1D7AB6	VIPA	Ready	0	0	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			255.255.255.255			Not active			Starting	0	0	0	0	0	0%	0	0%
z/OS 1.11	TCPIP			193.9.200.1	TOVTAM	MPCPTP	Not active	IUTSAMEH	MPCPTP	Sent SETUP Request	0	0	0	0	0	0%	0	0%

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Check OSA Links Statistics: *Netstat Devlinks*

```
DevName: DEVOSA1           DevType: MPCIPA
   DevStatus: Ready
   LnkName: OSDL              LnkType: IPAQENET   LnkStatus: Ready
     Speed: 0000001000
     IpBroadcastCapability: No
     CfgRouter: Non                   ActRouter: Non
     ArpOffload: Yes                  ArpOffloadInfo: Yes
     ActMtu: 8992
     VLANid: None                     VLANpriority: Disabled
. . .
Link Statistics:
     BytesIn                           = 25081576230
     Inbound Packets                   = 194853959
     Inbound Packets In Error          = 194353459
     Inbound Packets Discarded         = 194352011
     Inbound Packets With No Protocol  = 0
     BytesOut                          = 103520236
     Outbound Packets                  = 387012
     Outbound Packets In Error         = 0
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

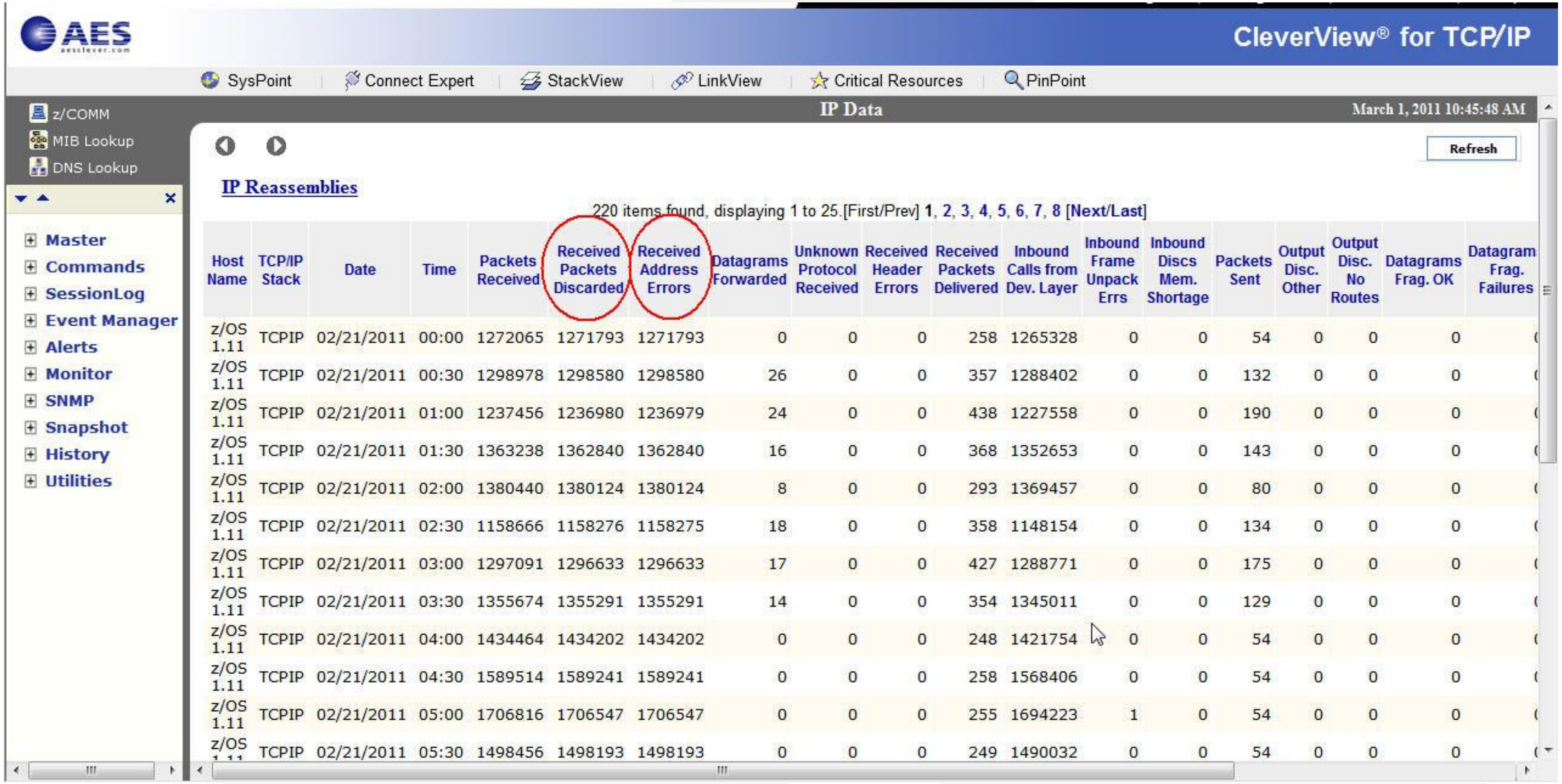
Check IP Statistics: *Netstat Stats Proto IP*

```
MVS TCP/IP NETSTAT CS V1R11       TCPIP Name: TCPIP           02:22:49
IP Statistics (IPv4)
  Packets Received                  = 194959223
  Received Header Errors            = 194429115      (discarded due to IP header errors)
  Received Address Errors           = 194431079      (invalid destination IP address)
  Datagrams Forwarded               = 4680
  Unknown Protocols Received        = 0
  Received Packets Discarded        = 0
  Received Packets Delivered        = 523425
  Output Requests                   = 409928
  Output Discards No Route          = 0
  Output Discards (other)           = 0
  Reassembly Timeouts               = 0
  Reassembly Required               = 0
  Reassembly Successful             = 0
  Reassembly Failures               = 0
  Datagrams Successfully Fragmented = 0
  Datagrams Failing Fragmentation   = 0
  Fragments Created                 = 0
  Inbound Packets handled by zIIP   = 0
  Outbound Packets handled by zIIP  = 0
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Check Historical IP Interface Data



IP Data

March 1, 2011 10:45:48 AM

IP Reassemblies

220 items found, displaying 1 to 25.[First/Prev] 1, 2, 3, 4, 5, 6, 7, 8 [Next/Last]

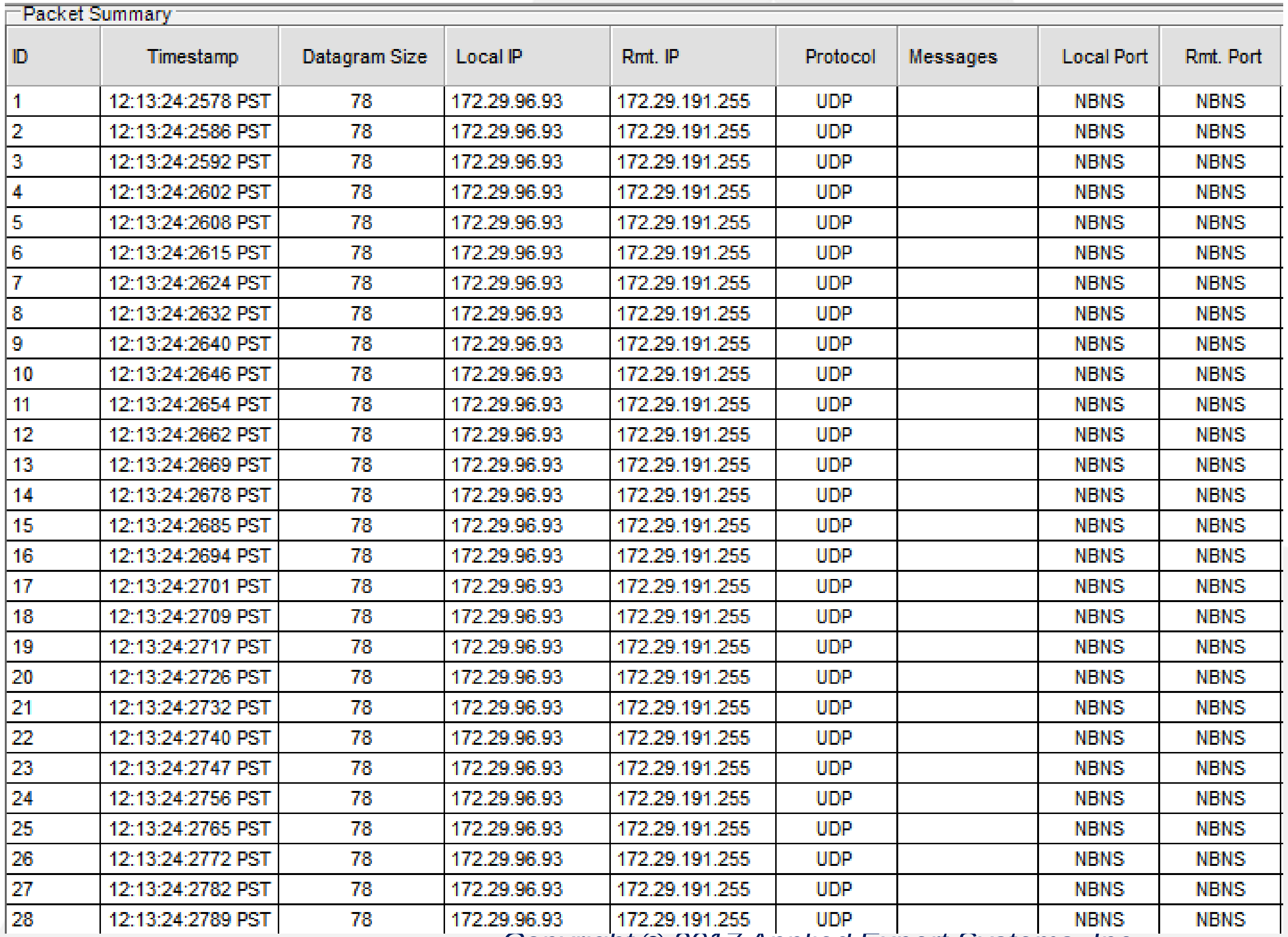
Host Name	TCP/IP Stack	Date	Time	Packets Received	Received Packets Discarded	Received Address Errors	Datagrams Forwarded	Unknown Protocol Received	Received Header Errors	Received Packets Delivered	Inbound Calls from Dev. Layer	Inbound Frame Unpack Errs	Inbound Discs Mem. Shortage	Packets Sent	Output Disc. Other	Output Disc. No Routes	Datagrams Frag. OK	Datagram Frag. Failures
z/OS 1.11	TCPIP	02/21/2011	00:00	1272065	1271793	1271793	0	0	0	258	1265328	0	0	54	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	00:30	1298978	1298580	1298580	26	0	0	357	1288402	0	0	132	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	01:00	1237456	1236980	1236979	24	0	0	438	1227558	0	0	190	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	01:30	1363238	1362840	1362840	16	0	0	368	1352653	0	0	143	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	02:00	1380440	1380124	1380124	8	0	0	293	1369457	0	0	80	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	02:30	1158666	1158276	1158275	18	0	0	358	1148154	0	0	134	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	03:00	1297091	1296633	1296633	17	0	0	427	1288771	0	0	175	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	03:30	1355674	1355291	1355291	14	0	0	354	1345011	0	0	129	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	04:00	1434464	1434202	1434202	0	0	0	248	1421754	0	0	54	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	04:30	1589514	1589241	1589241	0	0	0	258	1568406	0	0	54	0	0	0	(
z/OS 1.11	TCPIP	02/21/2011	05:00	1706816	1706547	1706547	0	0	0	255	1694223	1	0	54	0	0	0	(
z/OS	TCPIP	02/21/2011	05:30	1498456	1498193	1498193	0	0	0	249	1490032	0	0	54	0	0	0	(

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Capture Discarded Packets

VARY TCPIP*tcpipproc*,PKT,ON,DISCard=ALL



Packet Summary

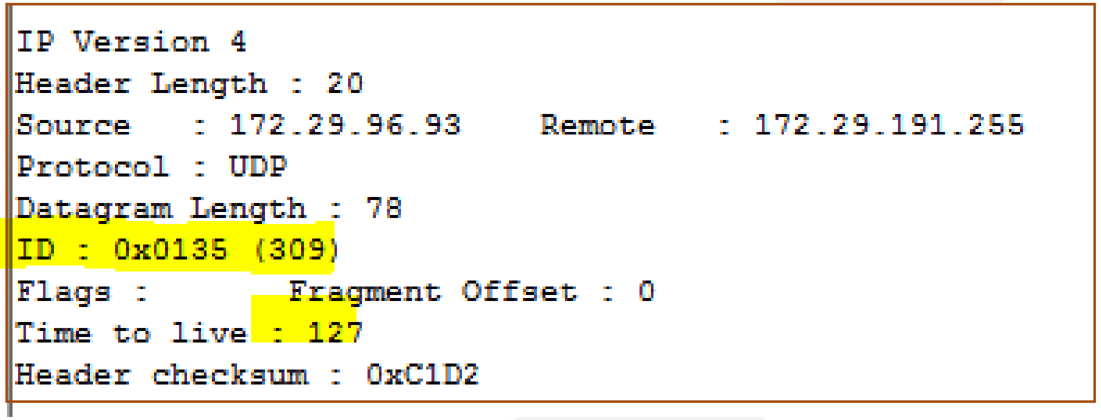
ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port
1	12:13:24:2578 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
2	12:13:24:2586 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
3	12:13:24:2592 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
4	12:13:24:2602 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
5	12:13:24:2608 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
6	12:13:24:2615 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
7	12:13:24:2624 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
8	12:13:24:2632 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
9	12:13:24:2640 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
10	12:13:24:2646 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
11	12:13:24:2654 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
12	12:13:24:2662 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
13	12:13:24:2669 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
14	12:13:24:2678 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
15	12:13:24:2685 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
16	12:13:24:2694 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
17	12:13:24:2701 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
18	12:13:24:2709 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
19	12:13:24:2717 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
20	12:13:24:2726 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
21	12:13:24:2732 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
22	12:13:24:2740 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
23	12:13:24:2747 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
24	12:13:24:2756 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
25	12:13:24:2765 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
26	12:13:24:2772 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
27	12:13:24:2782 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS
28	12:13:24:2789 PST	78	172.29.96.93	172.29.191.255	UDP		NBNS	NBNS

Copyright © 2017 Applied Expert Systems, Inc.

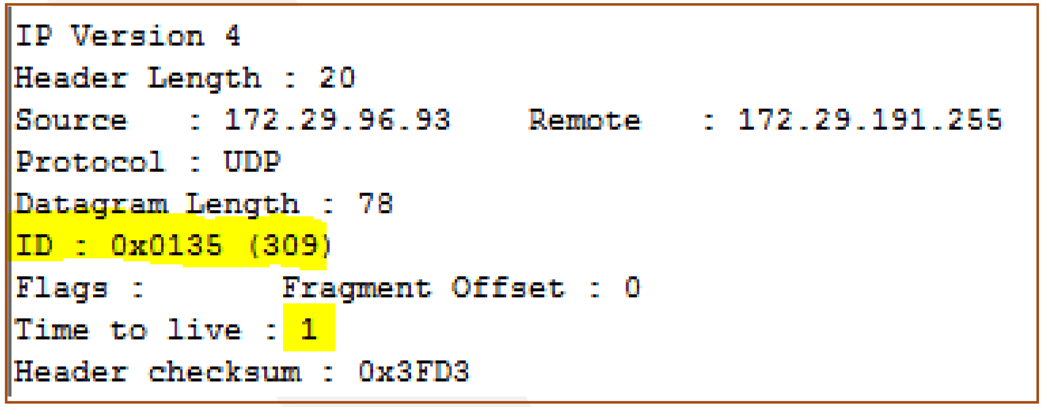
Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Check the Offending Packets

The same packet was repeated 127 times – How do we know they are the same?
starting with TTL=127, then TTL=126, TTL=125, … … and ending with TTL=1



```
IP Version 4
Header Length : 20
Source    : 172.29.96.93    Remote    : 172.29.191.255
Protocol : UDP
Datagram Length : 78
ID : 0x0135 (309)
Flags :        Fragment Offset : 0
Time to live : 127
Header checksum : 0xC1D2
```



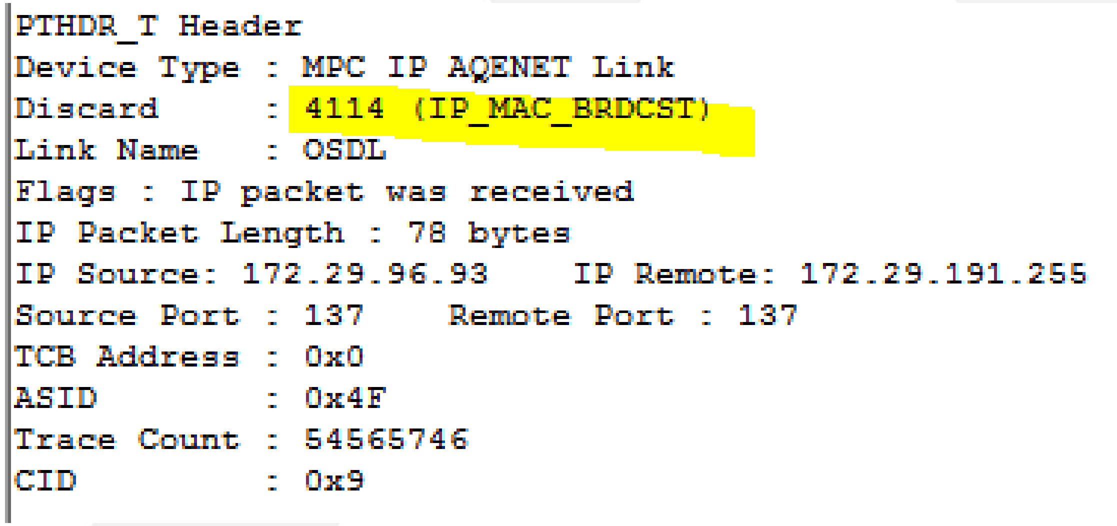
```
IP Version 4
Header Length : 20
Source    : 172.29.96.93    Remote    : 172.29.191.255
Protocol : UDP
Datagram Length : 78
ID : 0x0135 (309)
Flags :        Fragment Offset : 0
Time to live : 1
Header checksum : 0x3FD3
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Why were these packets discarded?

Check the Discard Code.



```
PTHDR_T Header
Device Type : MPC IP AQENET Link
Discard     : 4114 (IP_MAC_BRDCST)
Link Name   : OSDL
Flags : IP packet was received
IP Packet Length : 78 bytes
IP Source: 172.29.96.93    IP Remote: 172.29.191.255
Source Port : 137    Remote Port : 137
TCB Address : 0x0
ASID        : 0x4F
Trace Count : 54565746
CID         : 0x9
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Comm Server IP & SNA Codes

- Discard Reason Code

Discard Reason Code	Category
1 – 4095	OSA
4096 – 8191	Interface and IP layer
8192 – 12287	TCP layer
12288 – 20479	Reserved

  - 4114 (IP_MAC_BRDCST): The MAC broadcast packet not accepted.
- Destination IP = 172.29.191.255 ?

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

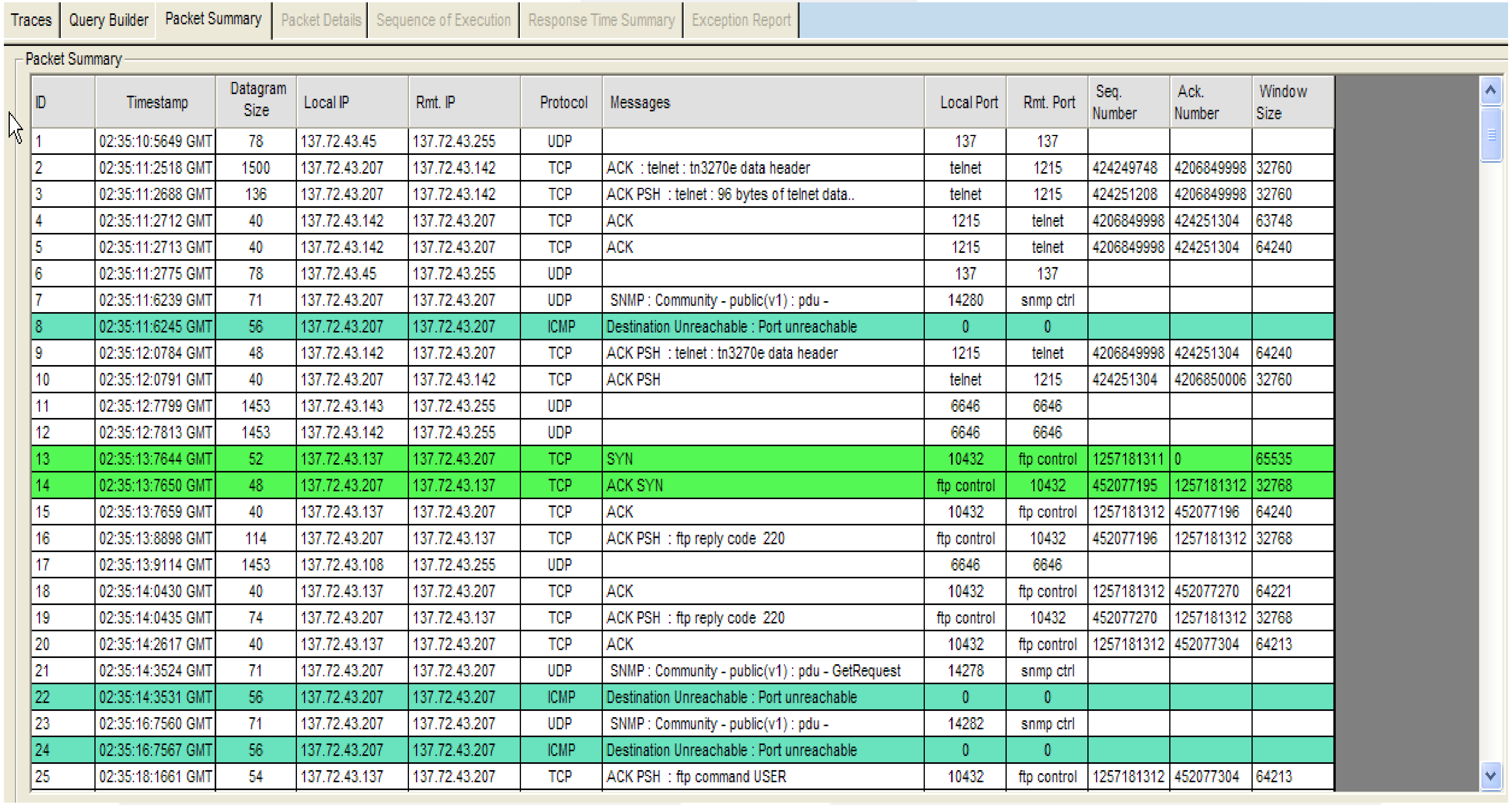
Discarded Packets - continued

- The drop reason code 4114 usually indicates that the packet has a non-broadcast destination IP address and a broadcast media header (the broadcast indicator is on in the media header). This is likely to be caused by an invalid locally administered MAC address.
- **netbios-ns**
  - NetBIOS Name Service (over UDP port 137)
  - Similar to DNS
  - Name Query request

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

FTP – Lost SYN Packet



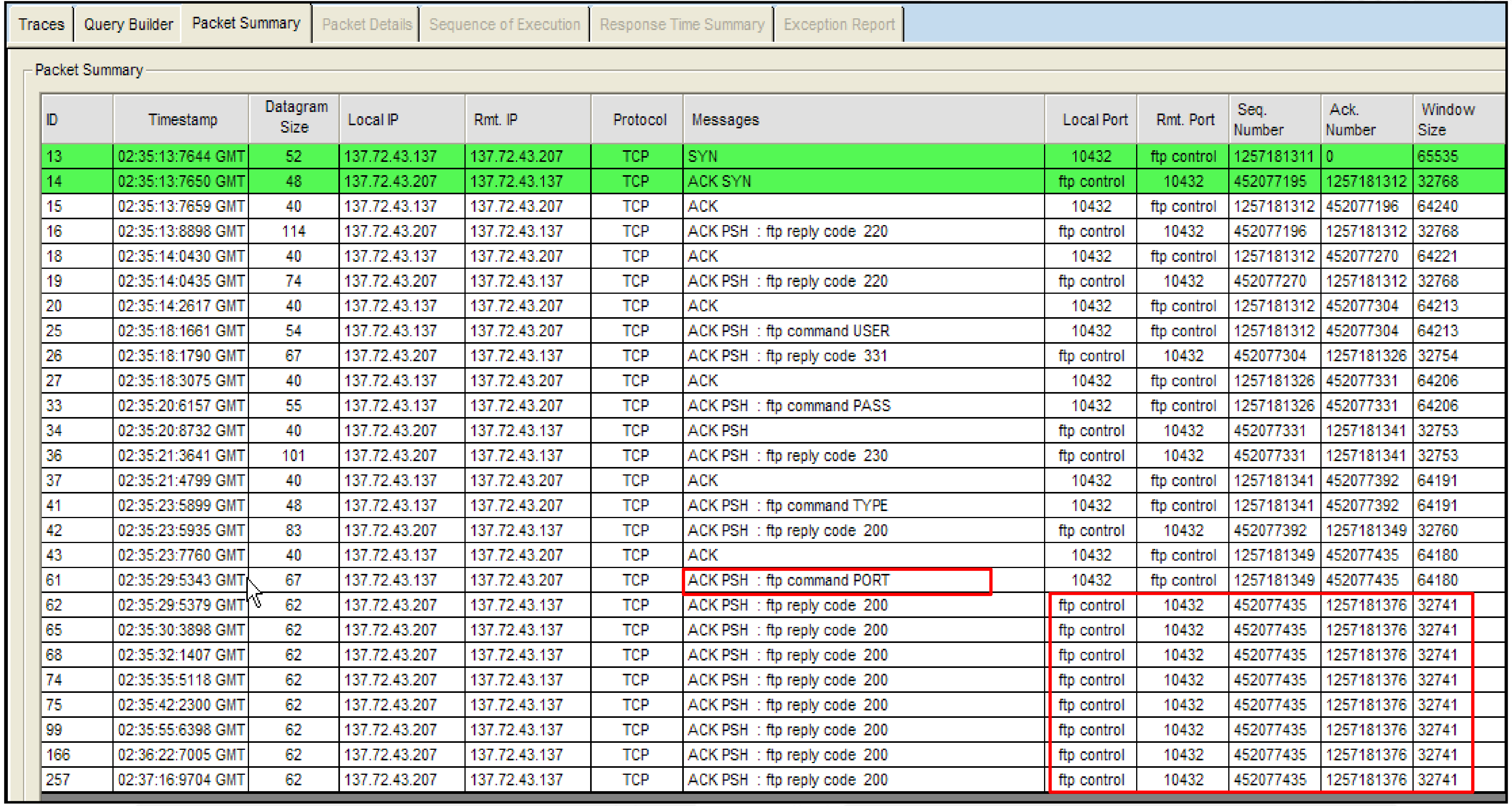
Packet Summary

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

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

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

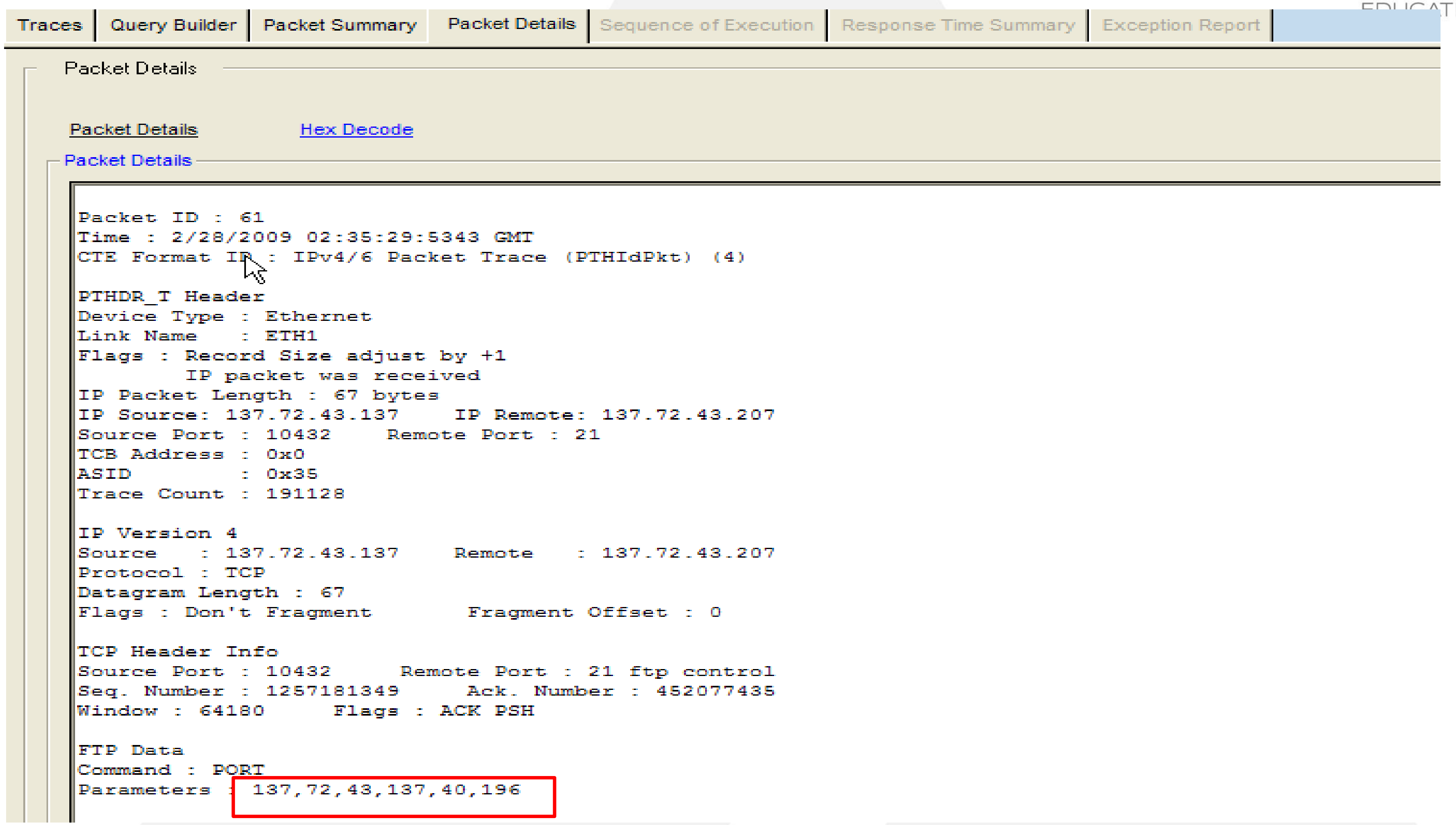


ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
13	02:35:13:7644 GMT	52	137.72.43.137	137.72.43.207	TCP	SYN	10432	ftp control	1257181311	0	65535
14	02:35:13:7650 GMT	48	137.72.43.207	137.72.43.137	TCP	ACK SYN	ftp control	10432	452077195	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

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Analysis - 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
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Analysis – PORT command continued

Active FTP

- Server initiates the data connection
- PORT command contains the data connection listening port

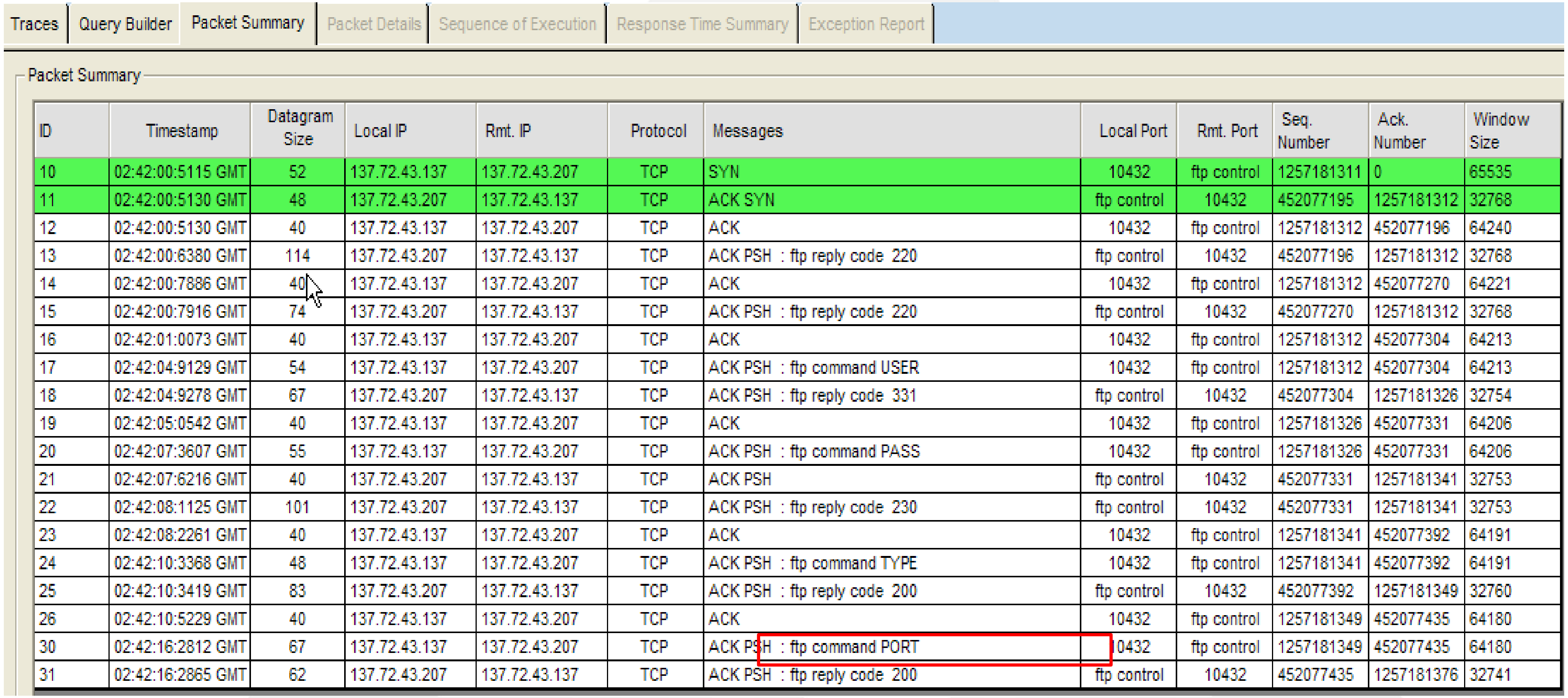
PORT 137,72,43,137,40,196

- 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, port 20)
  - to client (137.72.43.137, port 10436)

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Analysis – check the corresponding Sniffer trace



Packet Summary

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

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

FTP Analysis

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.

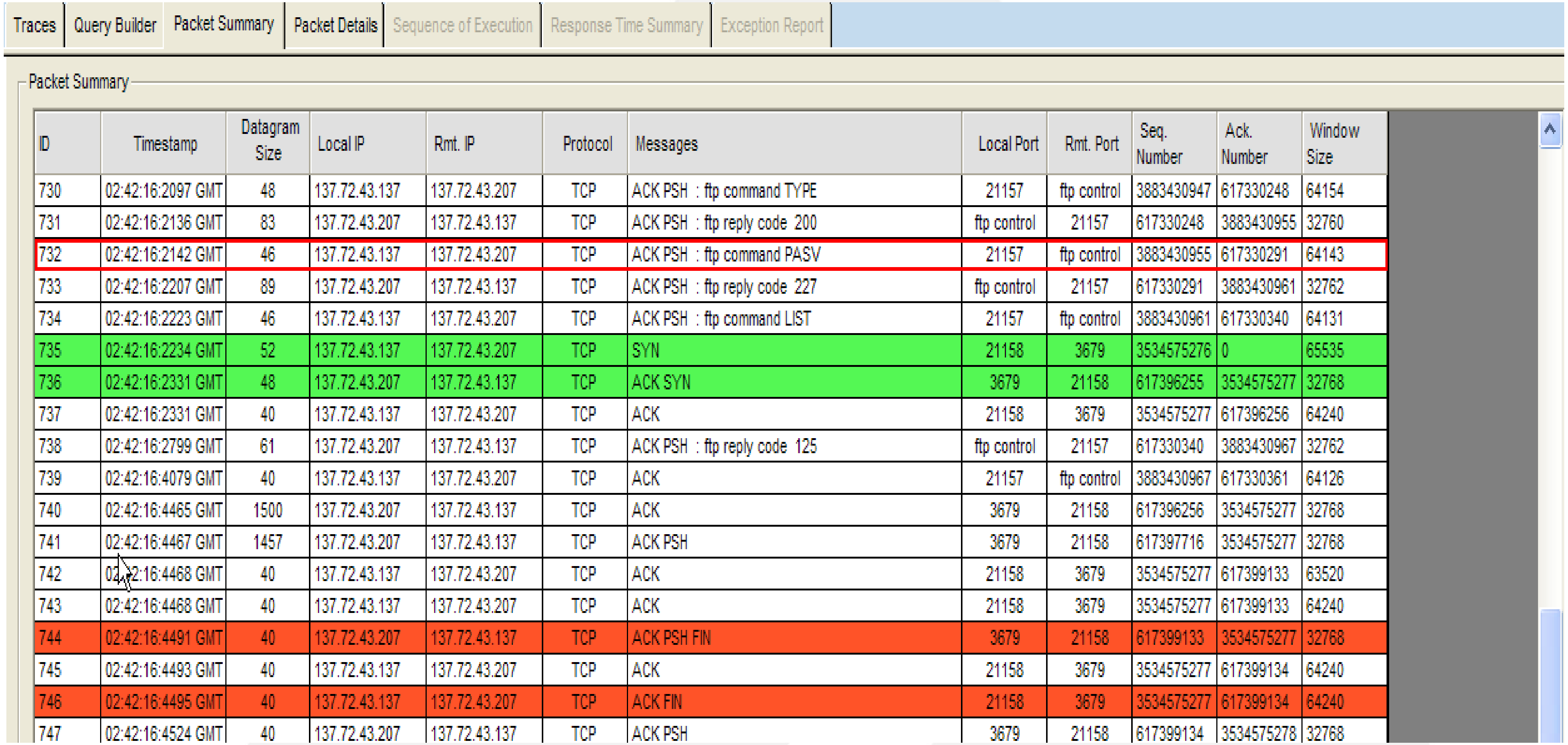
Passive FTP:

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

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

FTP Analysis – a Good PASV

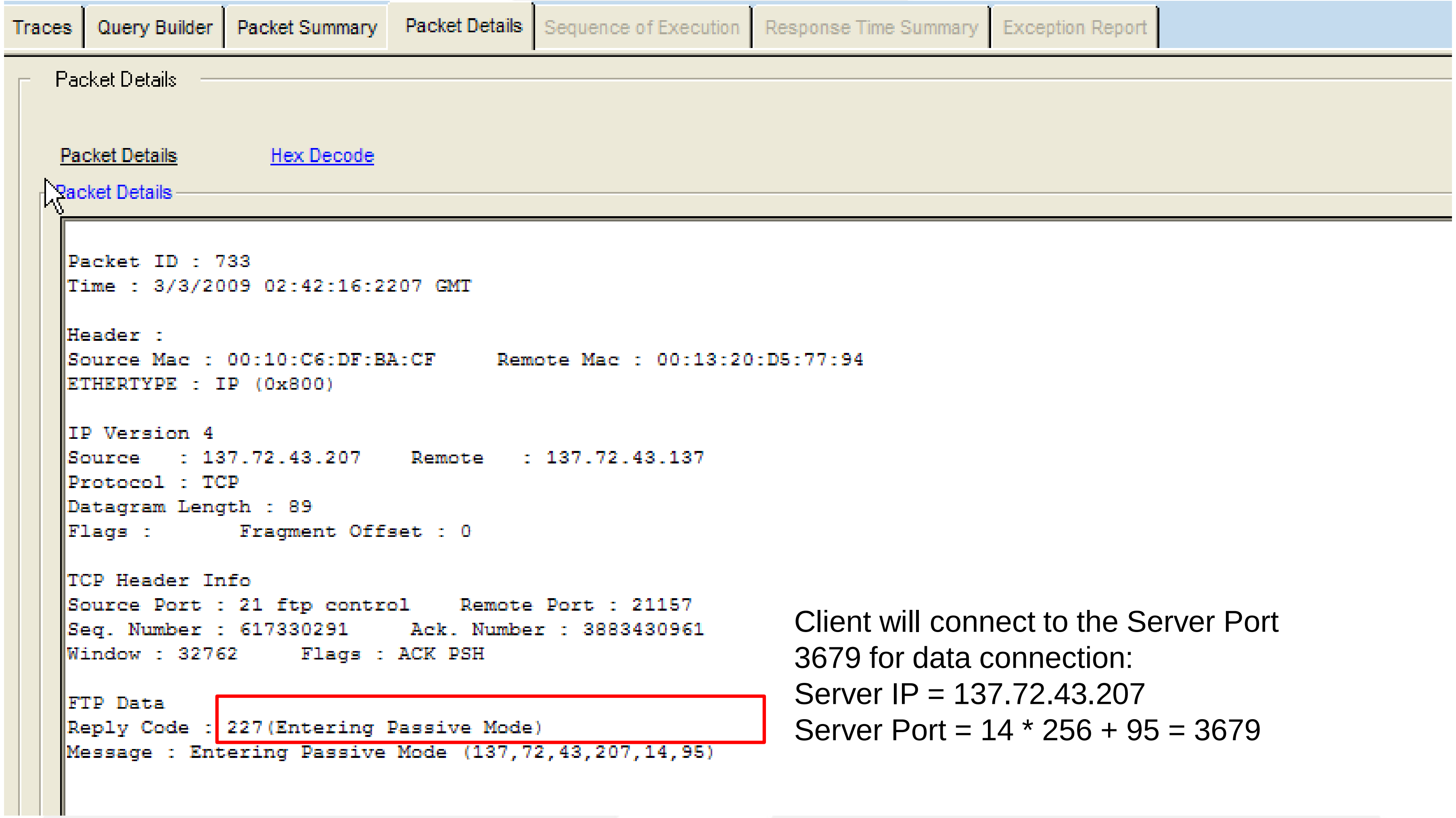


ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
730	02:42:16:2097 GMT	48	137.72.43.137	137.72.43.207	TCP	ACK PSH : ftp command TYPE	21157	ftp control	3883430947	617330248	64154
731	02:42:16:2136 GMT	83	137.72.43.207	137.72.43.137	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

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Analysis – PASV Reply

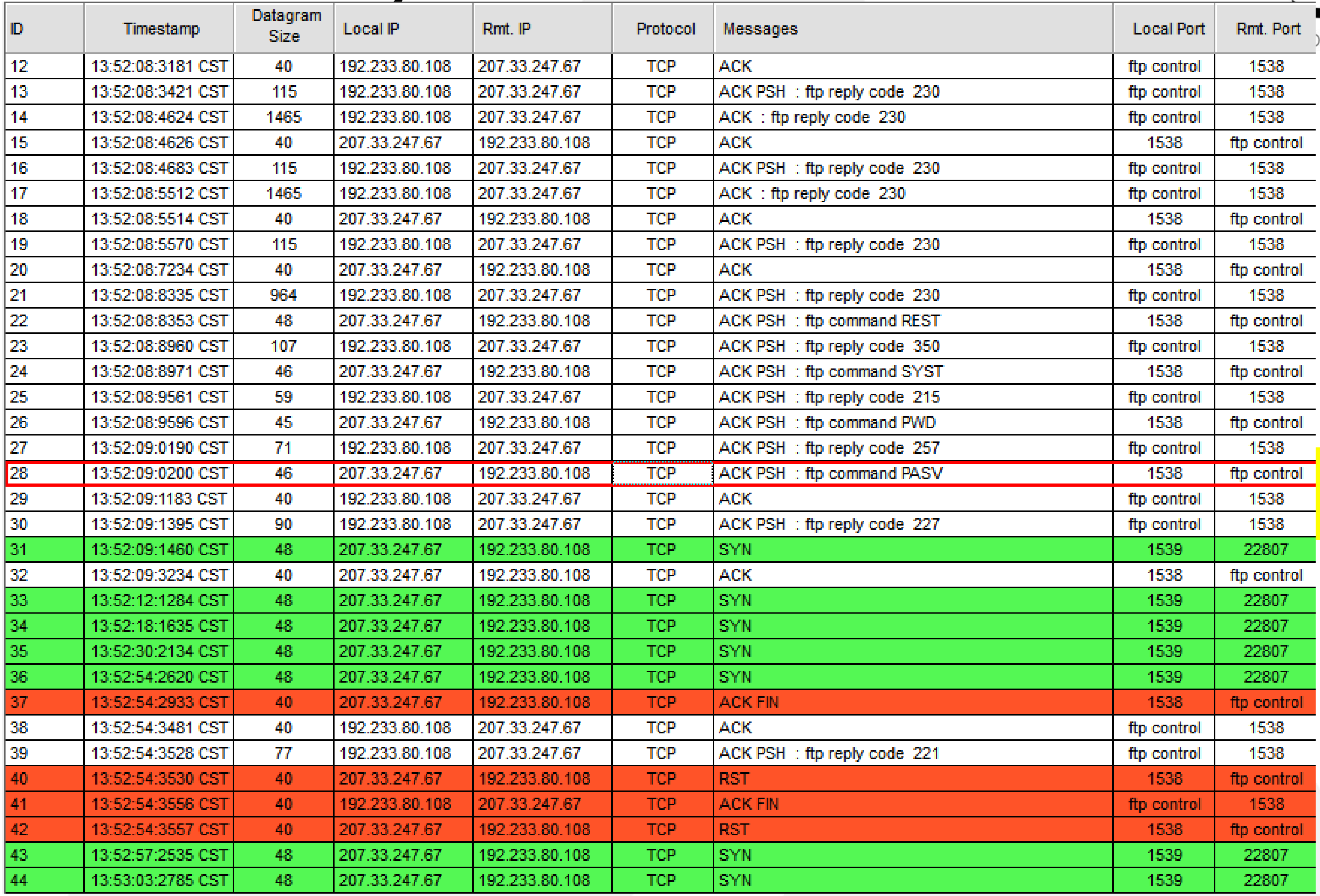


```
Packet ID : 733
Time : 3/3/2009 02:42:16:2207 GMT

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

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Analysis – a Failed PASV

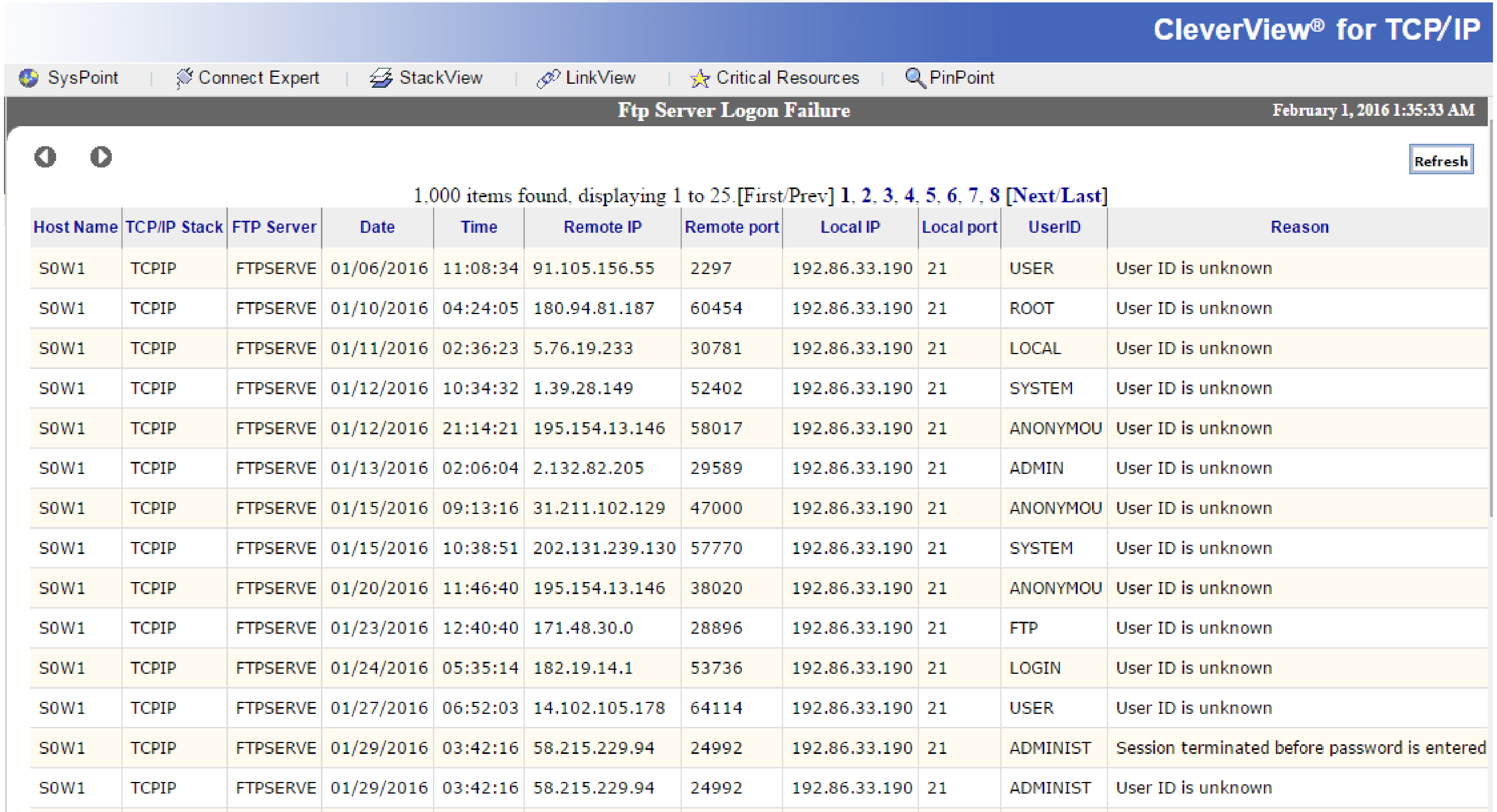


ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port
12	13:52:08:3181 CST	40	192.233.80.108	207.33.247.67	TCP	ACK	ftp control	1538
13	13:52:08:3421 CST	115	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 230	ftp control	1538
14	13:52:08:4624 CST	1465	192.233.80.108	207.33.247.67	TCP	ACK : ftp reply code 230	ftp control	1538
15	13:52:08:4626 CST	40	207.33.247.67	192.233.80.108	TCP	ACK	1538	ftp control
16	13:52:08:4683 CST	115	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 230	ftp control	1538
17	13:52:08:5512 CST	1465	192.233.80.108	207.33.247.67	TCP	ACK : ftp reply code 230	ftp control	1538
18	13:52:08:5514 CST	40	207.33.247.67	192.233.80.108	TCP	ACK	1538	ftp control
19	13:52:08:5570 CST	115	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 230	ftp control	1538
20	13:52:08:7234 CST	40	207.33.247.67	192.233.80.108	TCP	ACK	1538	ftp control
21	13:52:08:8335 CST	964	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 230	ftp control	1538
22	13:52:08:8353 CST	48	207.33.247.67	192.233.80.108	TCP	ACK PSH : ftp command REST	1538	ftp control
23	13:52:08:8960 CST	107	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 350	ftp control	1538
24	13:52:08:8971 CST	46	207.33.247.67	192.233.80.108	TCP	ACK PSH : ftp command SYST	1538	ftp control
25	13:52:08:9561 CST	59	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 215	ftp control	1538
26	13:52:08:9596 CST	45	207.33.247.67	192.233.80.108	TCP	ACK PSH : ftp command PWD	1538	ftp control
27	13:52:09:0190 CST	71	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 257	ftp control	1538
28	13:52:09:0200 CST	46	207.33.247.67	192.233.80.108	TCP	ACK PSH : ftp command PASV	1538	ftp control
29	13:52:09:1183 CST	40	192.233.80.108	207.33.247.67	TCP	ACK	ftp control	1538
30	13:52:09:1395 CST	90	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 227	ftp control	1538
31	13:52:09:1460 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807
32	13:52:09:3234 CST	40	207.33.247.67	192.233.80.108	TCP	ACK	1538	ftp control
33	13:52:12:1284 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807
34	13:52:18:1635 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807
35	13:52:30:2134 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807
36	13:52:54:2620 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807
37	13:52:54:2933 CST	40	207.33.247.67	192.233.80.108	TCP	ACK FIN	1538	ftp control
38	13:52:54:3481 CST	40	192.233.80.108	207.33.247.67	TCP	ACK	ftp control	1538
39	13:52:54:3528 CST	77	192.233.80.108	207.33.247.67	TCP	ACK PSH : ftp reply code 221	ftp control	1538
40	13:52:54:3530 CST	40	207.33.247.67	192.233.80.108	TCP	RST	1538	ftp control
41	13:52:54:3556 CST	40	192.233.80.108	207.33.247.67	TCP	ACK FIN	ftp control	1538
42	13:52:54:3557 CST	40	207.33.247.67	192.233.80.108	TCP	RST	1538	ftp control
43	13:52:57:2535 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807
44	13:53:03:2785 CST	48	207.33.247.67	192.233.80.108	TCP	SYN	1539	22807

Message : Entering Passive Mode (**192,233,80,108,89,23**).
89x256 + 23 = **22807**

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Proactively Monitoring for FTP Server Logon Failures



Ftp Server Logon Failure

February 1, 2016 1:35:33 AM

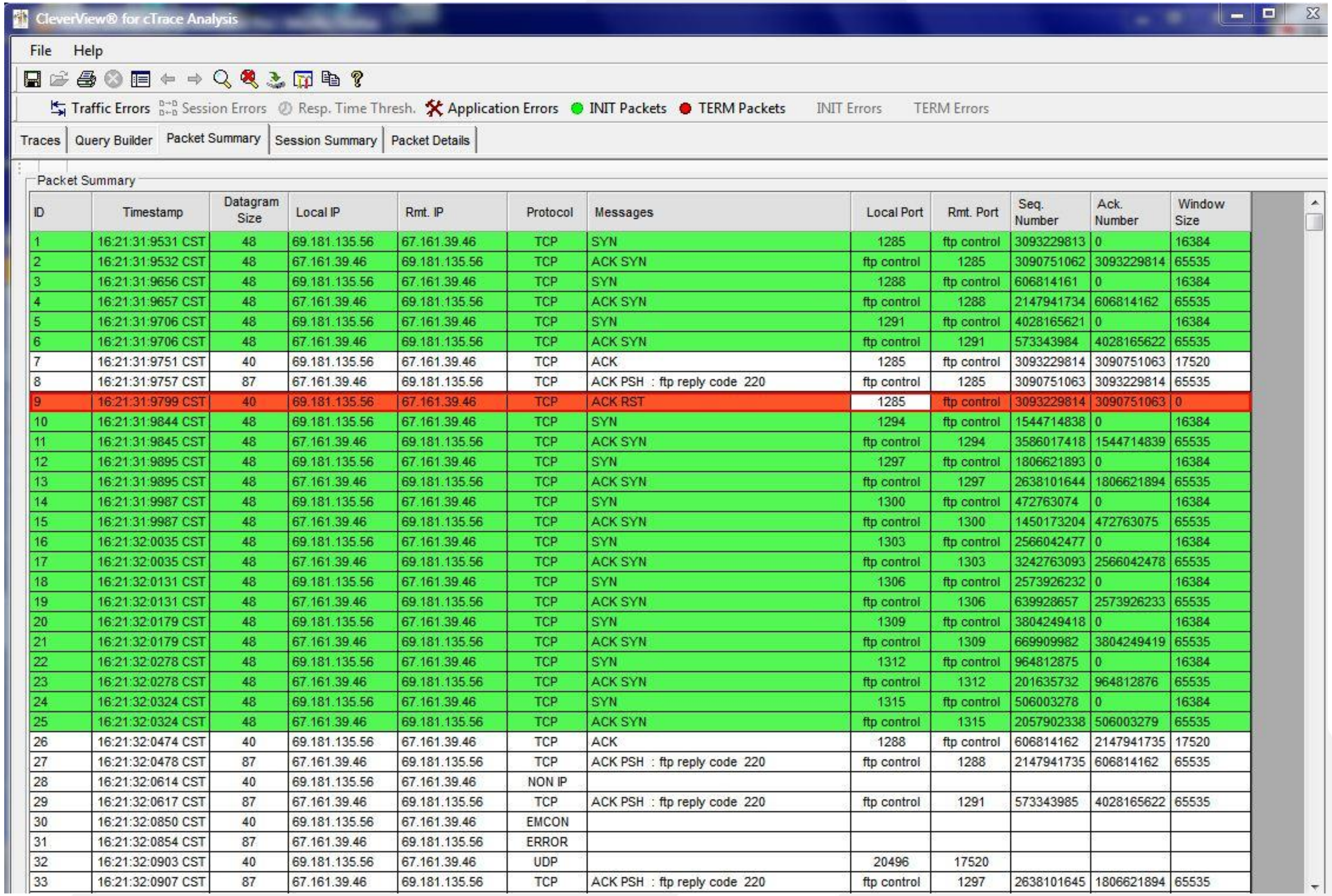
1,000 items found, displaying 1 to 25.[First/Prev] 1, 2, 3, 4, 5, 6, 7, 8 [Next/Last]

Host Name	TCP/IP Stack	FTP Server	Date	Time	Remote IP	Remote port	Local IP	Local port	UserID	Reason
S0W1	TCPIP	FTPSERVE	01/06/2016	11:08:34	91.105.156.55	2297	192.86.33.190	21	USER	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/10/2016	04:24:05	180.94.81.187	60454	192.86.33.190	21	ROOT	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/11/2016	02:36:23	5.76.19.233	30781	192.86.33.190	21	LOCAL	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/12/2016	10:34:32	1.39.28.149	52402	192.86.33.190	21	SYSTEM	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/12/2016	21:14:21	195.154.13.146	58017	192.86.33.190	21	ANONYMOU	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/13/2016	02:06:04	2.132.82.205	29589	192.86.33.190	21	ADMIN	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/15/2016	09:13:16	31.211.102.129	47000	192.86.33.190	21	ANONYMOU	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/15/2016	10:38:51	202.131.239.130	57770	192.86.33.190	21	SYSTEM	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/20/2016	11:46:40	195.154.13.146	38020	192.86.33.190	21	ANONYMOU	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/23/2016	12:40:40	171.48.30.0	28896	192.86.33.190	21	FTP	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/24/2016	05:35:14	182.19.14.1	53736	192.86.33.190	21	LOGIN	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/27/2016	06:52:03	14.102.105.178	64114	192.86.33.190	21	USER	User ID is unknown
S0W1	TCPIP	FTPSERVE	01/29/2016	03:42:16	58.215.229.94	24992	192.86.33.190	21	ADMINIST	Session terminated before password is entered
S0W1	TCPIP	FTPSERVE	01/29/2016	03:42:16	58.215.229.94	24992	192.86.33.190	21	ADMINIST	User ID is unknown

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Brute Force Attack

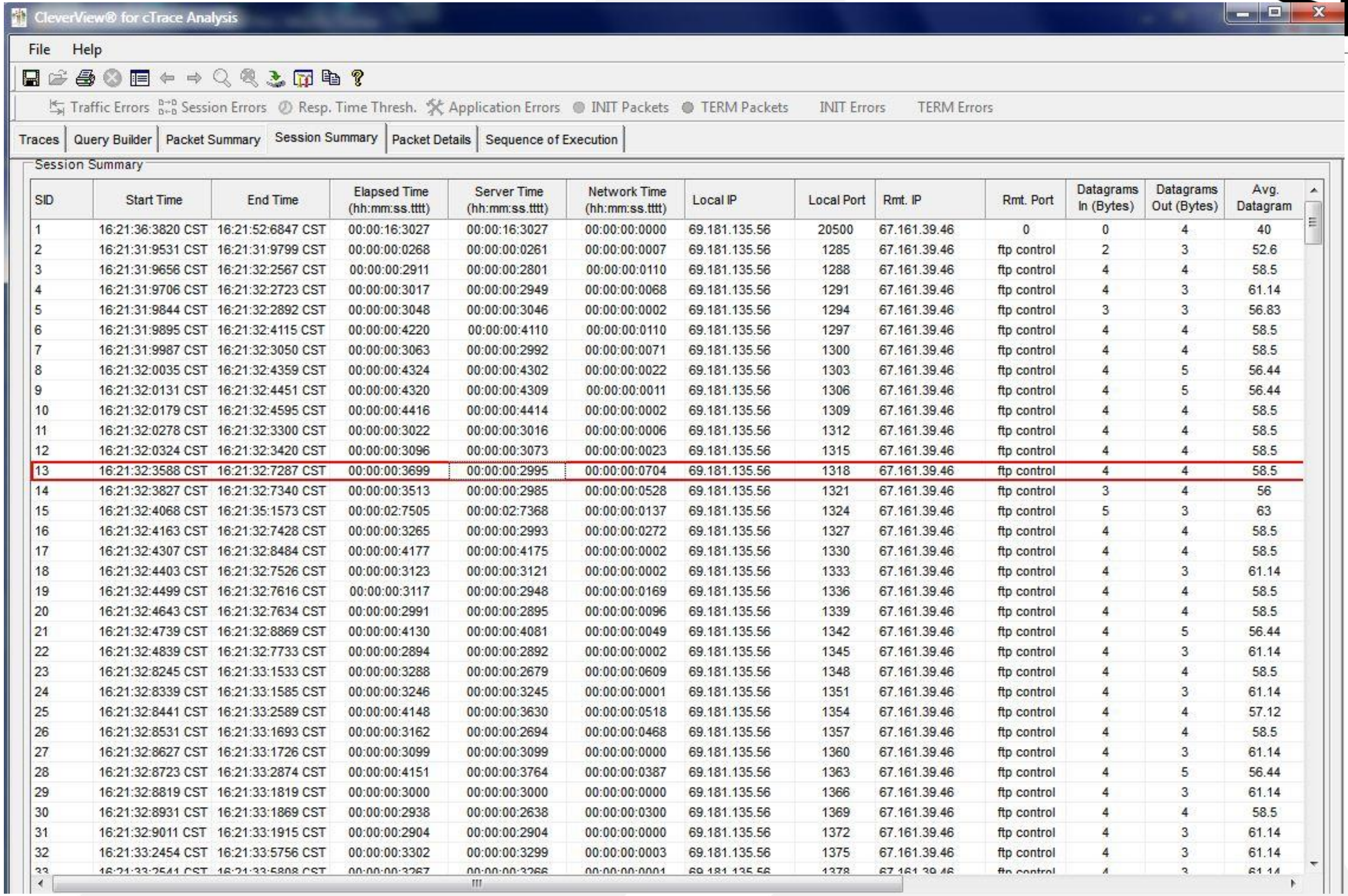


ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	16:21:31:9531 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1285	ftp control	3093229813	0	16384
2	16:21:31:9532 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1285	3090751062	3093229814	65535
3	16:21:31:9656 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1288	ftp control	606814161	0	16384
4	16:21:31:9657 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1288	2147941734	606814162	65535
5	16:21:31:9706 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1291	ftp control	4028165621	0	16384
6	16:21:31:9706 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1291	573343984	4028165622	65535
7	16:21:31:9751 CST	40	69.181.135.56	67.161.39.46	TCP	ACK	1285	ftp control	3093229814	3090751063	17520
8	16:21:31:9757 CST	87	67.161.39.46	69.181.135.56	TCP	ACK PSH : ftp reply code 220	ftp control	1285	3090751063	3093229814	65535
9	16:21:31:9799 CST	40	69.181.135.56	67.161.39.46	TCP	ACK RST	1285	ftp control	3093229814	3090751063	0
10	16:21:31:9844 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1294	ftp control	1544714838	0	16384
11	16:21:31:9845 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1294	3586017418	1544714839	65535
12	16:21:31:9895 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1297	ftp control	1806621893	0	16384
13	16:21:31:9895 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1297	2638101644	1806621894	65535
14	16:21:31:9987 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1300	ftp control	472763074	0	16384
15	16:21:31:9987 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1300	1450173204	472763075	65535
16	16:21:32:0035 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1303	ftp control	2566042477	0	16384
17	16:21:32:0035 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1303	3242763093	2566042478	65535
18	16:21:32:0131 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1306	ftp control	2573926232	0	16384
19	16:21:32:0131 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1306	639928657	2573926233	65535
20	16:21:32:0179 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1309	ftp control	3804249418	0	16384
21	16:21:32:0179 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1309	669909982	3804249419	65535
22	16:21:32:0278 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1312	ftp control	964812875	0	16384
23	16:21:32:0278 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1312	201635732	964812876	65535
24	16:21:32:0324 CST	48	69.181.135.56	67.161.39.46	TCP	SYN	1315	ftp control	506003278	0	16384
25	16:21:32:0324 CST	48	67.161.39.46	69.181.135.56	TCP	ACK SYN	ftp control	1315	2057902338	506003279	65535
26	16:21:32:0474 CST	40	69.181.135.56	67.161.39.46	TCP	ACK	1288	ftp control	606814162	2147941735	17520
27	16:21:32:0478 CST	87	67.161.39.46	69.181.135.56	TCP	ACK PSH : ftp reply code 220	ftp control	1288	2147941735	606814162	65535
28	16:21:32:0614 CST	40	69.181.135.56	67.161.39.46	NON IP						
29	16:21:32:0617 CST	87	67.161.39.46	69.181.135.56	TCP	ACK PSH : ftp reply code 220	ftp control	1291	573343985	4028165622	65535
30	16:21:32:0850 CST	40	69.181.135.56	67.161.39.46	EMCON						
31	16:21:32:0854 CST	87	67.161.39.46	69.181.135.56	ERROR						
32	16:21:32:0903 CST	40	69.181.135.56	67.161.39.46	UDP		20496	17520			
33	16:21:32:0907 CST	87	67.161.39.46	69.181.135.56	TCP	ACK PSH : ftp reply code 220	ftp control	1297	2638101645	1806621894	65535

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Brute Force Attack – Zoom in on FTP Control Sessions

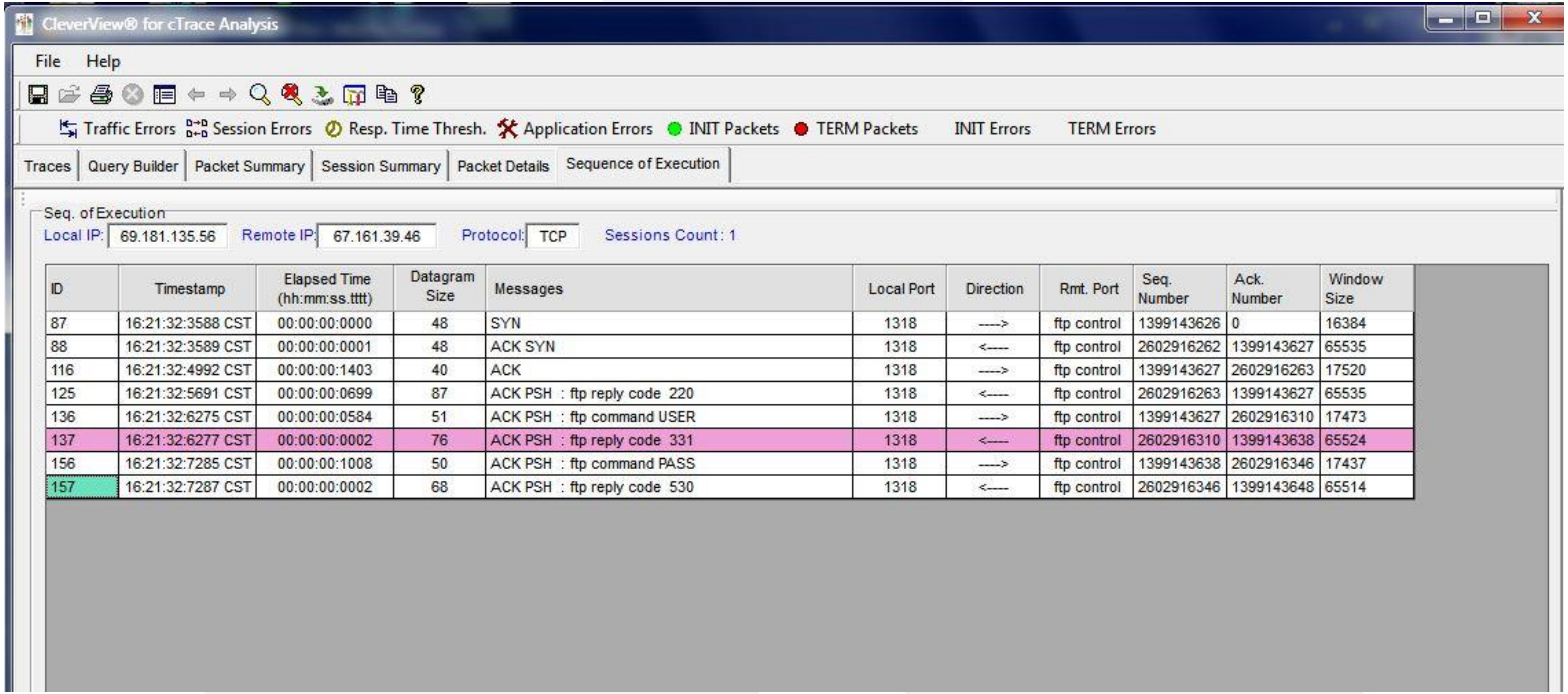


Session Summary

SID	Start Time	End Time	Elapsed Time (hh:mm:ss.tttt)	Server Time (hh:mm:ss.tttt)	Network Time (hh:mm:ss.tttt)	Local IP	Local Port	Rmt. IP	Rmt. Port	Datagrams In (Bytes)	Datagrams Out (Bytes)	Avg. Datagram
1	16:21:36:3820 CST	16:21:52:6847 CST	00:00:16:3027	00:00:16:3027	00:00:00:0000	69.181.135.56	20500	67.161.39.46	0	0	4	40
2	16:21:31:9531 CST	16:21:31:9799 CST	00:00:00:0268	00:00:00:0261	00:00:00:0007	69.181.135.56	1285	67.161.39.46	ftp control	2	3	52.6
3	16:21:31:9656 CST	16:21:32:2567 CST	00:00:00:2911	00:00:00:2801	00:00:00:0110	69.181.135.56	1288	67.161.39.46	ftp control	4	4	58.5
4	16:21:31:9706 CST	16:21:32:2723 CST	00:00:00:3017	00:00:00:2949	00:00:00:0068	69.181.135.56	1291	67.161.39.46	ftp control	4	3	61.14
5	16:21:31:9844 CST	16:21:32:2892 CST	00:00:00:3048	00:00:00:3046	00:00:00:0002	69.181.135.56	1294	67.161.39.46	ftp control	3	3	56.83
6	16:21:31:9895 CST	16:21:32:4115 CST	00:00:00:4220	00:00:00:4110	00:00:00:0110	69.181.135.56	1297	67.161.39.46	ftp control	4	4	58.5
7	16:21:31:9987 CST	16:21:32:3050 CST	00:00:00:3063	00:00:00:2992	00:00:00:0071	69.181.135.56	1300	67.161.39.46	ftp control	4	4	58.5
8	16:21:32:0035 CST	16:21:32:4359 CST	00:00:00:4324	00:00:00:4302	00:00:00:0022	69.181.135.56	1303	67.161.39.46	ftp control	4	5	56.44
9	16:21:32:0131 CST	16:21:32:4451 CST	00:00:00:4320	00:00:00:4309	00:00:00:0011	69.181.135.56	1306	67.161.39.46	ftp control	4	5	56.44
10	16:21:32:0179 CST	16:21:32:4595 CST	00:00:00:4416	00:00:00:4414	00:00:00:0002	69.181.135.56	1309	67.161.39.46	ftp control	4	4	58.5
11	16:21:32:0278 CST	16:21:32:3300 CST	00:00:00:3022	00:00:00:3016	00:00:00:0006	69.181.135.56	1312	67.161.39.46	ftp control	4	4	58.5
12	16:21:32:0324 CST	16:21:32:3420 CST	00:00:00:3096	00:00:00:3073	00:00:00:0023	69.181.135.56	1315	67.161.39.46	ftp control	4	4	58.5
13	16:21:32:3588 CST	16:21:32:7287 CST	00:00:00:3699	00:00:00:2995	00:00:00:0704	69.181.135.56	1318	67.161.39.46	ftp control	4	4	58.5
14	16:21:32:3827 CST	16:21:32:7340 CST	00:00:00:3513	00:00:00:2985	00:00:00:0528	69.181.135.56	1321	67.161.39.46	ftp control	3	4	56
15	16:21:32:4068 CST	16:21:35:1573 CST	00:00:02:7505	00:00:02:7368	00:00:00:0137	69.181.135.56	1324	67.161.39.46	ftp control	5	3	63
16	16:21:32:4163 CST	16:21:32:7428 CST	00:00:00:3265	00:00:00:2993	00:00:00:0272	69.181.135.56	1327	67.161.39.46	ftp control	4	4	58.5
17	16:21:32:4307 CST	16:21:32:8484 CST	00:00:00:4177	00:00:00:4175	00:00:00:0002	69.181.135.56	1330	67.161.39.46	ftp control	4	4	58.5
18	16:21:32:4403 CST	16:21:32:7526 CST	00:00:00:3123	00:00:00:3121	00:00:00:0002	69.181.135.56	1333	67.161.39.46	ftp control	4	3	61.14
19	16:21:32:4499 CST	16:21:32:7616 CST	00:00:00:3117	00:00:00:2948	00:00:00:0169	69.181.135.56	1336	67.161.39.46	ftp control	4	4	58.5
20	16:21:32:4643 CST	16:21:32:7634 CST	00:00:00:2991	00:00:00:2895	00:00:00:0096	69.181.135.56	1339	67.161.39.46	ftp control	4	4	58.5
21	16:21:32:4739 CST	16:21:32:8869 CST	00:00:00:4130	00:00:00:4081	00:00:00:0049	69.181.135.56	1342	67.161.39.46	ftp control	4	5	56.44
22	16:21:32:4839 CST	16:21:32:7733 CST	00:00:00:2894	00:00:00:2892	00:00:00:0002	69.181.135.56	1345	67.161.39.46	ftp control	4	3	61.14
23	16:21:32:8245 CST	16:21:33:1533 CST	00:00:00:3288	00:00:00:2679	00:00:00:0609	69.181.135.56	1348	67.161.39.46	ftp control	4	4	58.5
24	16:21:32:8339 CST	16:21:33:1585 CST	00:00:00:3246	00:00:00:3245	00:00:00:0001	69.181.135.56	1351	67.161.39.46	ftp control	4	3	61.14
25	16:21:32:8441 CST	16:21:33:2589 CST	00:00:00:4148	00:00:00:3630	00:00:00:0518	69.181.135.56	1354	67.161.39.46	ftp control	4	4	57.12
26	16:21:32:8531 CST	16:21:33:1693 CST	00:00:00:3162	00:00:00:2694	00:00:00:0468	69.181.135.56	1357	67.161.39.46	ftp control	4	4	58.5
27	16:21:32:8627 CST	16:21:33:1726 CST	00:00:00:3099	00:00:00:3099	00:00:00:0000	69.181.135.56	1360	67.161.39.46	ftp control	4	3	61.14
28	16:21:32:8723 CST	16:21:33:2874 CST	00:00:00:4151	00:00:00:3764	00:00:00:0387	69.181.135.56	1363	67.161.39.46	ftp control	4	5	56.44
29	16:21:32:8819 CST	16:21:33:1819 CST	00:00:00:3000	00:00:00:3000	00:00:00:0000	69.181.135.56	1366	67.161.39.46	ftp control	4	3	61.14
30	16:21:32:8931 CST	16:21:33:1869 CST	00:00:00:2938	00:00:00:2638	00:00:00:0300	69.181.135.56	1369	67.161.39.46	ftp control	4	4	58.5
31	16:21:32:9011 CST	16:21:33:1915 CST	00:00:00:2904	00:00:00:2904	00:00:00:0000	69.181.135.56	1372	67.161.39.46	ftp control	4	3	61.14
32	16:21:33:2454 CST	16:21:33:5756 CST	00:00:00:3302	00:00:00:3299	00:00:00:0003	69.181.135.56	1375	67.161.39.46	ftp control	4	3	61.14
33	16:21:33:2541 CST	16:21:33:5808 CST	00:00:00:3267	00:00:00:3266	00:00:00:0001	69.181.135.56	1378	67.161.39.46	ftp control	4	3	61.14

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTP Brute Force Attack – Check FTP Commands and Replies



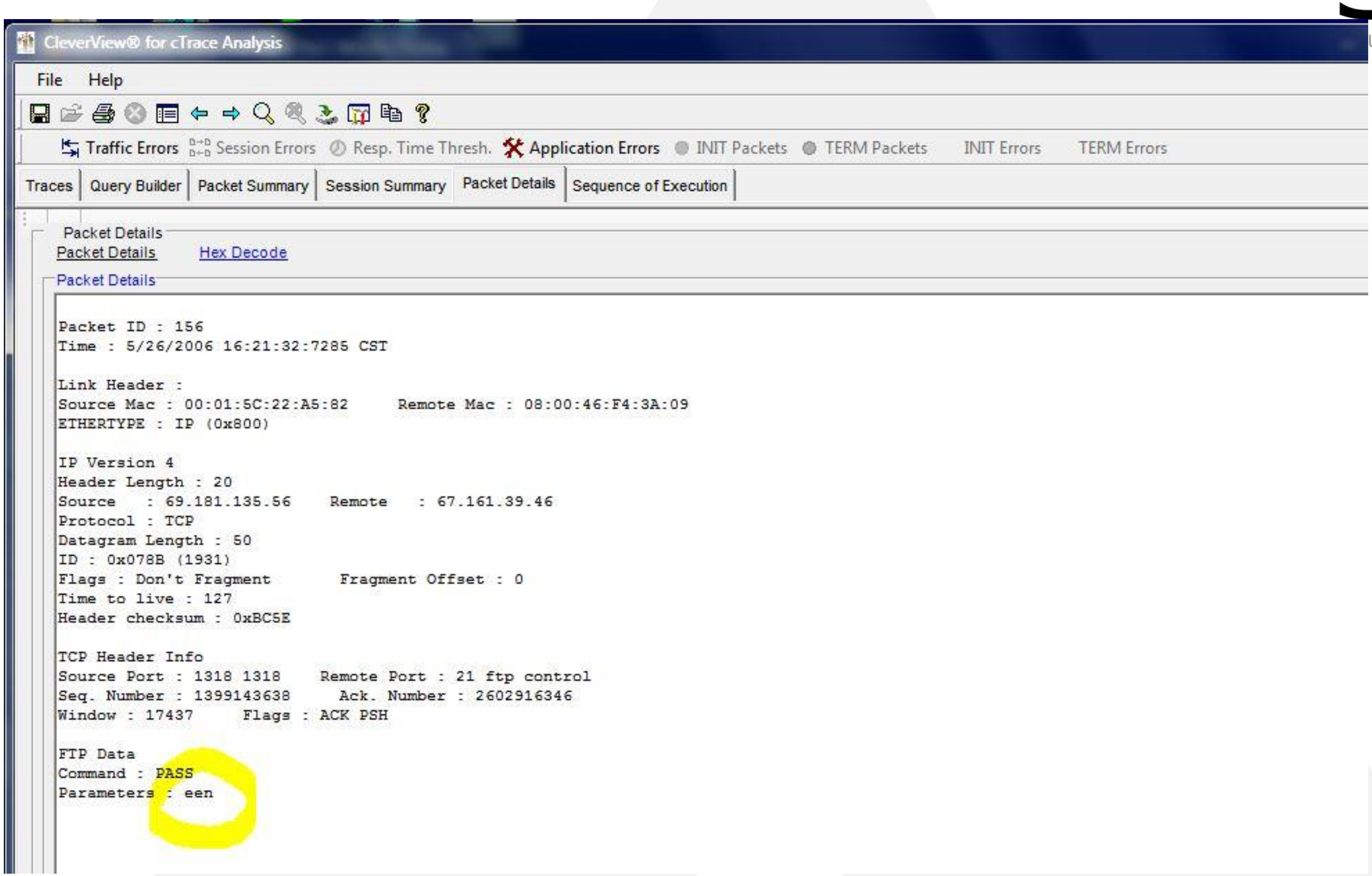
Local IP: 69.181.135.56 Remote IP: 67.161.39.46 Protocol: TCP Sessions Count: 1

ID	Timestamp	Elapsed Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
87	16:21:32:3588 CST	00:00:00:0000	48	SYN	1318	---->	ftp control	1399143626	0	16384
88	16:21:32:3589 CST	00:00:00:0001	48	ACK SYN	1318	<----	ftp control	2602916262	1399143627	65535
116	16:21:32:4992 CST	00:00:00:1403	40	ACK	1318	---->	ftp control	1399143627	2602916263	17520
125	16:21:32:5691 CST	00:00:00:0699	87	ACK PSH : ftp reply code 220	1318	<----	ftp control	2602916263	1399143627	65535
136	16:21:32:6275 CST	00:00:00:0584	51	ACK PSH : ftp command USER	1318	---->	ftp control	1399143627	2602916310	17473
137	16:21:32:6277 CST	00:00:00:0002	76	ACK PSH : ftp reply code 331	1318	<----	ftp control	2602916310	1399143638	65524
156	16:21:32:7285 CST	00:00:00:1008	50	ACK PSH : ftp command PASS	1318	---->	ftp control	1399143638	2602916346	17437
157	16:21:32:7287 CST	00:00:00:0002	68	ACK PSH : ftp reply code 530	1318	<----	ftp control	2602916346	1399143648	65514

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

FTP Brute Force Attack – Check PASS Command Packet Details



```
Packet ID : 156
Time : 5/26/2006 16:21:32:7285 CST

Link Header :
Source Mac : 00:01:5C:22:A5:82     Remote Mac : 08:00:46:F4:3A:09
ETHERTYPE : IP (0x800)

IP Version 4
Header Length : 20
Source   : 69.181.135.56    Remote   : 67.161.39.46
Protocol : TCP
Datagram Length : 50
ID : 0x078B (1931)
Flags : Don't Fragment       Fragment Offset : 0
Time to live : 127
Header checksum : 0xBC5E

TCP Header Info
Source Port : 1318 1318    Remote Port : 21 ftp control
Seq. Number : 1399143638     Ack. Number : 2602916346
Window : 17437     Flags : ACK PSH

FTP Data
Command : PASS
Parameters : een
```

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TLS/SSL
https (Port 443), AT-TLS (appl. port)

- Transport Layer Security provides security for communications over networks by encrypting the segments at the transport layer end to end.

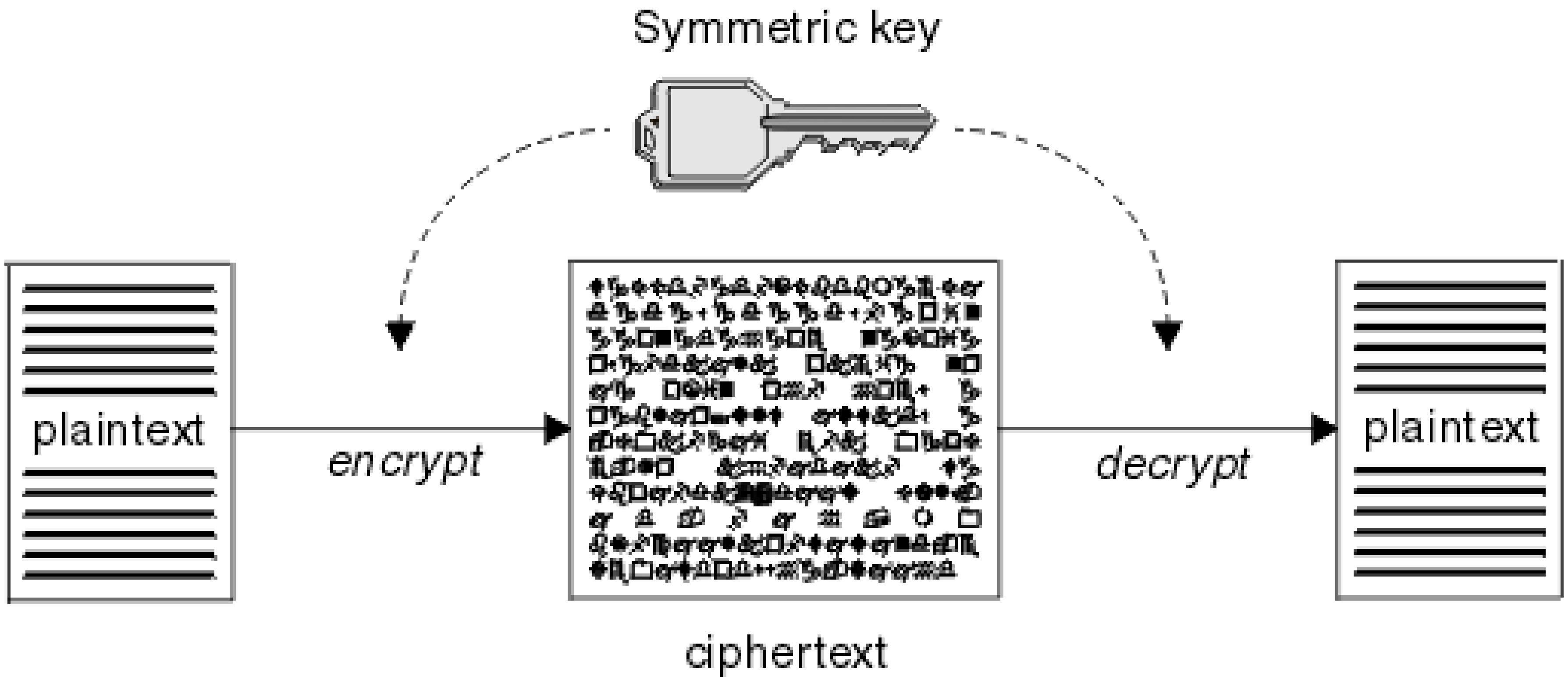
- TLS V1.0 (RFC 2246) is based on SSL V3.0.

- It does not require the client and the server to arrange for a secret key to be exchanged *before* the transaction.
  - Asymmetric keys (public/private) for handshaking and secret key exchange.
  - Secret key (symmetric) mechanism for subsequent communication.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TLS/SSL, AT-TLS – Secret Key (Symmetric)

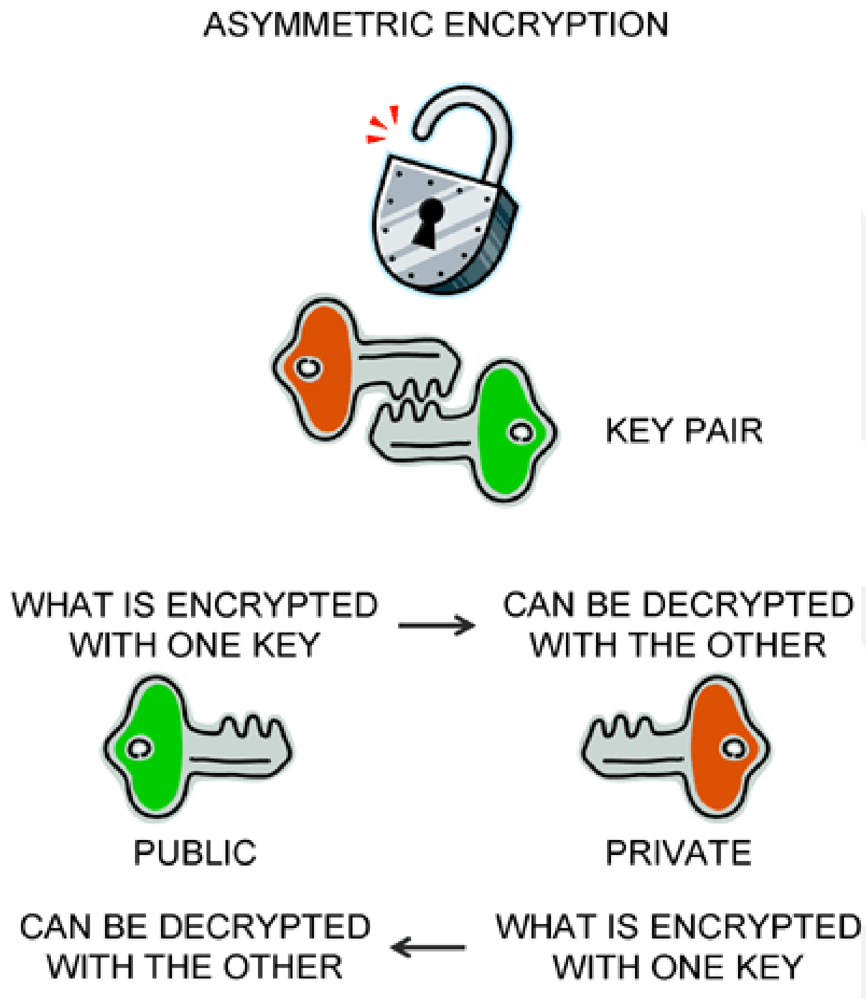


Source: http://middleware.its.state.nc.us/middleware/Documentation/en_US/htm/csqzas00/csq01skc.gif

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

TLS/SSL, AT-TLS – Public/Private Keys


ASYMMETRIC ENCRYPTION
KEY PAIR
WHAT IS ENCRYPTED WITH ONE KEY
CAN BE DECRYPTED WITH THE OTHER
PUBLIC
PRIVATE
CAN BE DECRYPTED WITH THE OTHER
WHAT IS ENCRYPTED WITH ONE KEY

Source:
http://www.teracomtraining.com/tutorials/teracom-tutorial-asymmetric-encryption.gif

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TLS/SSL Basic Flow

- Negotiate cipher suites and compression algorithms.

- Authenticate the server (and optionally the client) through certificates and public/private keys.

- **Server -> Client:** The server uses its private key to encrypt and the client uses the public key to decrypt.

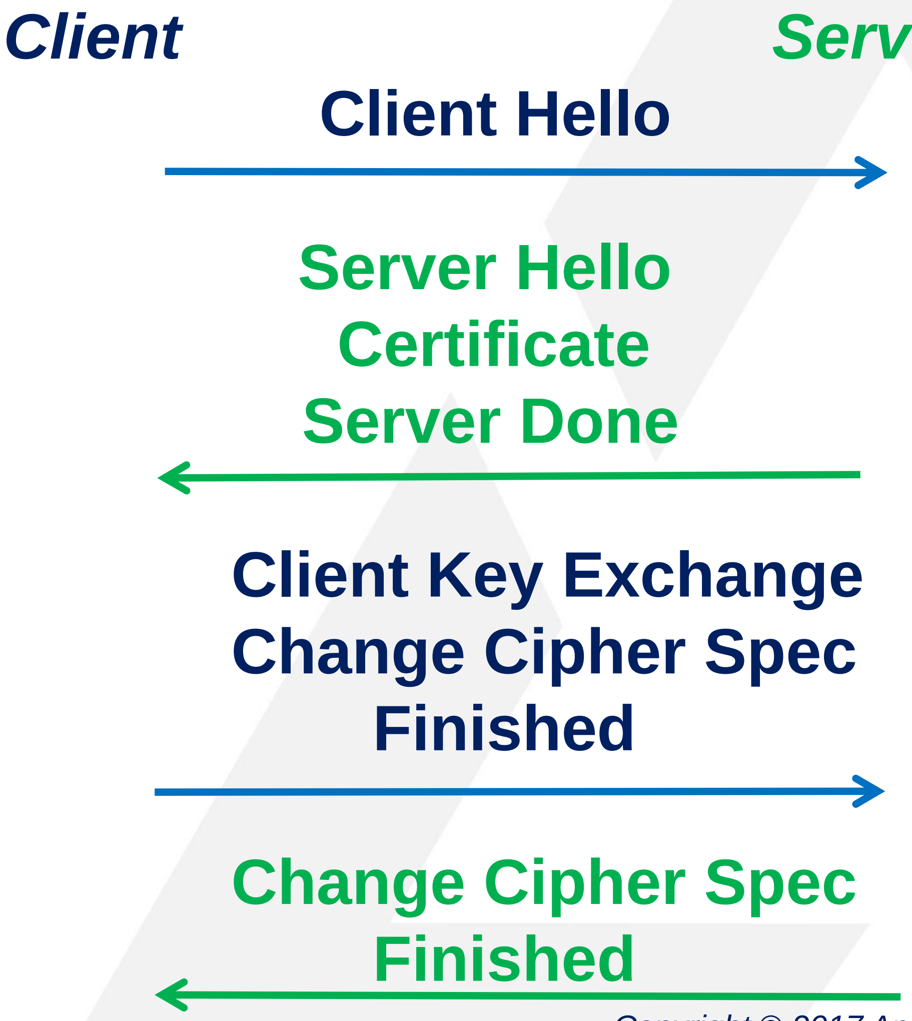
- **Client -> Server:** the client uses the public key to encrypt and the server uses its private key to decrypt.

- Exchange random numbers and a pre-master secret (all encrypted), which is used with other data to create a shared secret key – the **Master Secret** is used to encrypt/decrypt the data.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TLS/SSL Handshake – Server Authentication



Hello
Highest SSL/TLS version supported
Ciphers and Compression Method
Session ID
Random data for key generation

Certificate:
Server Certificate – contains server's public key.

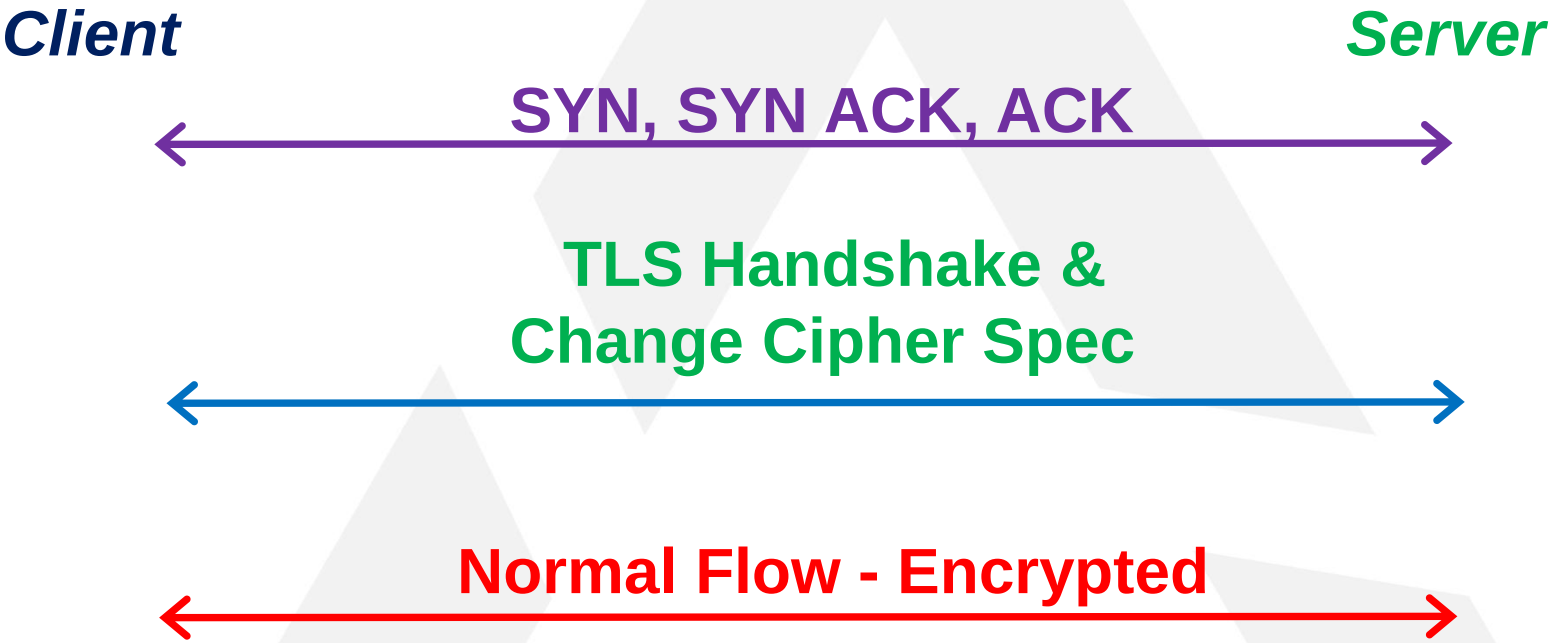
Client Key Exchange
Client generates the pre-master secret and encrypt it with server's public key. Both the client and the server generate the Master Secret key (**symmetric**) on their own using the pre-master secret and the random data that is generated from the SERVER_HELLO and CLIENT_HELLO commands.

Change Cipher Spec
Indicates that all subsequent data will be encrypted.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

AT-TLS Flow



Client

Server

SYN, SYN ACK, ACK

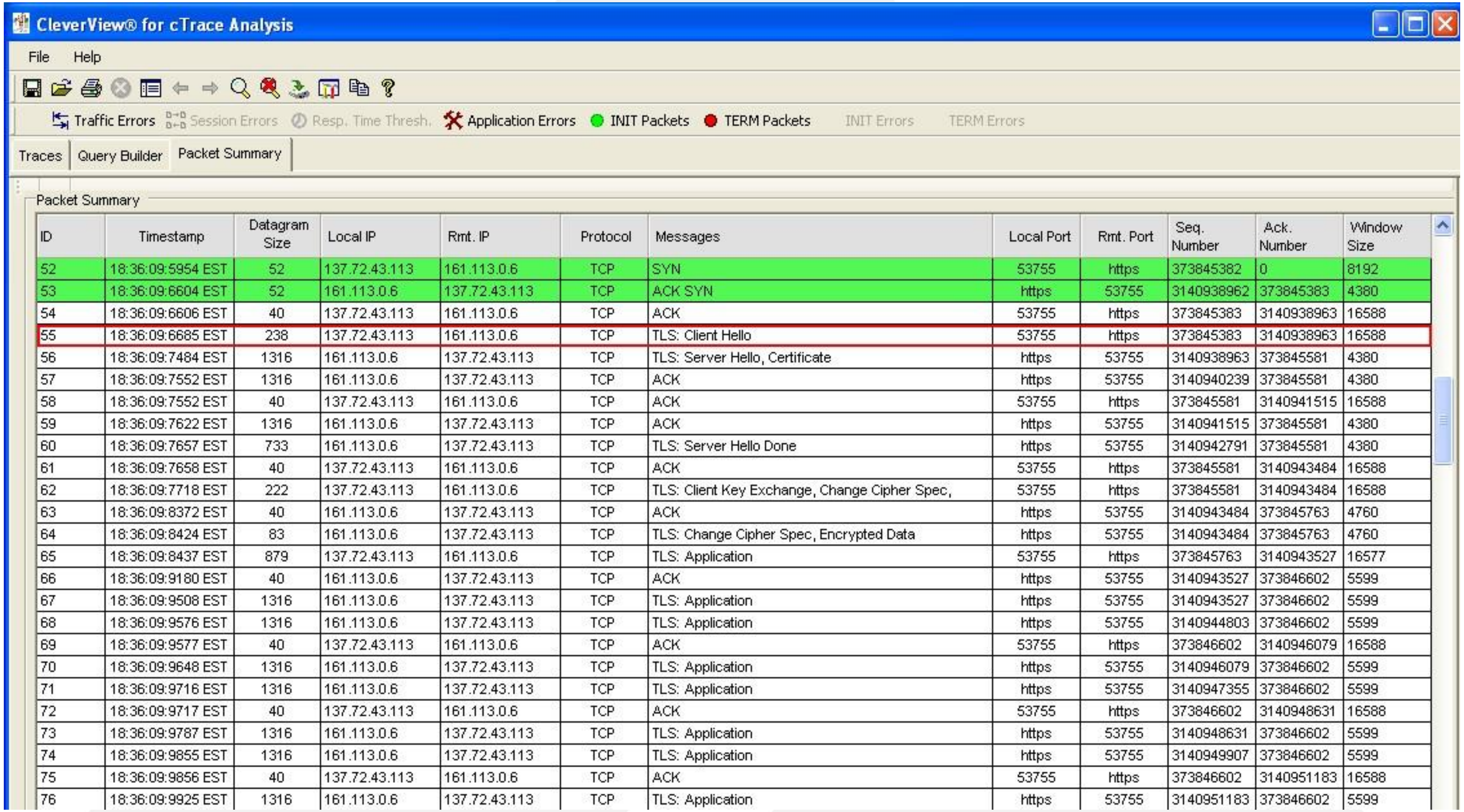
TLS Handshake &
Change Cipher Spec

Normal Flow - Encrypted

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

HTTPS (Port 443)

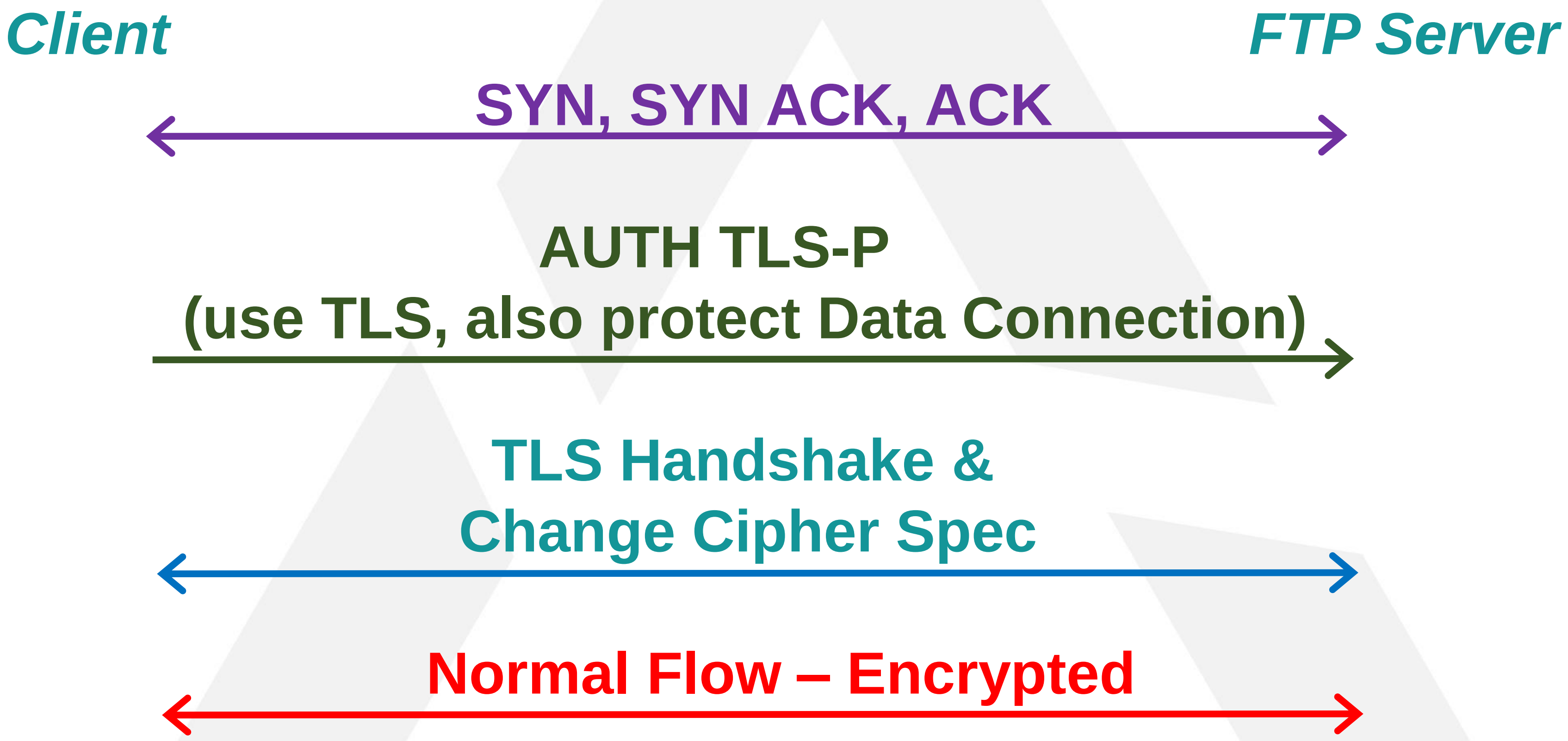


Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
52	18:36:09:5954 EST	52	137.72.43.113	161.113.0.6	TCP	SYN	53755	https	373845382	0	8192
53	18:36:09:6604 EST	52	161.113.0.6	137.72.43.113	TCP	ACK SYN	https	53755	3140938962	373845383	4380
54	18:36:09:6606 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373845383	3140938963	16588
55	18:36:09:6685 EST	238	137.72.43.113	161.113.0.6	TCP	TLS: Client Hello	53755	https	373845383	3140938963	16588
56	18:36:09:7484 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Server Hello, Certificate	https	53755	3140938963	373845581	4380
57	18:36:09:7552 EST	1316	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140940239	373845581	4380
58	18:36:09:7552 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373845581	3140941515	16588
59	18:36:09:7622 EST	1316	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140941515	373845581	4380
60	18:36:09:7657 EST	733	161.113.0.6	137.72.43.113	TCP	TLS: Server Hello Done	https	53755	3140942791	373845581	4380
61	18:36:09:7658 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373845581	3140943484	16588
62	18:36:09:7718 EST	222	137.72.43.113	161.113.0.6	TCP	TLS: Client Key Exchange, Change Cipher Spec,	53755	https	373845581	3140943484	16588
63	18:36:09:8372 EST	40	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140943484	373845763	4760
64	18:36:09:8424 EST	83	161.113.0.6	137.72.43.113	TCP	TLS: Change Cipher Spec, Encrypted Data	https	53755	3140943484	373845763	4760
65	18:36:09:8437 EST	879	137.72.43.113	161.113.0.6	TCP	TLS: Application	53755	https	373845763	3140943527	16577
66	18:36:09:9180 EST	40	161.113.0.6	137.72.43.113	TCP	ACK	https	53755	3140943527	373846602	5599
67	18:36:09:9508 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140943527	373846602	5599
68	18:36:09:9576 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140944803	373846602	5599
69	18:36:09:9577 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373846602	3140946079	16588
70	18:36:09:9648 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140946079	373846602	5599
71	18:36:09:9716 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140947355	373846602	5599
72	18:36:09:9717 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373846602	3140948631	16588
73	18:36:09:9787 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140948631	373846602	5599
74	18:36:09:9855 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140949907	373846602	5599
75	18:36:09:9856 EST	40	137.72.43.113	161.113.0.6	TCP	ACK	53755	https	373846602	3140951183	16588
76	18:36:09:9925 EST	1316	161.113.0.6	137.72.43.113	TCP	TLS: Application	https	53755	3140951183	373846602	5599

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

FTPS – FTP w/SSL Control Connection



Client

FTP Server

SYN, SYN ACK, ACK

AUTH TLS-P
(use TLS, also protect Data Connection)

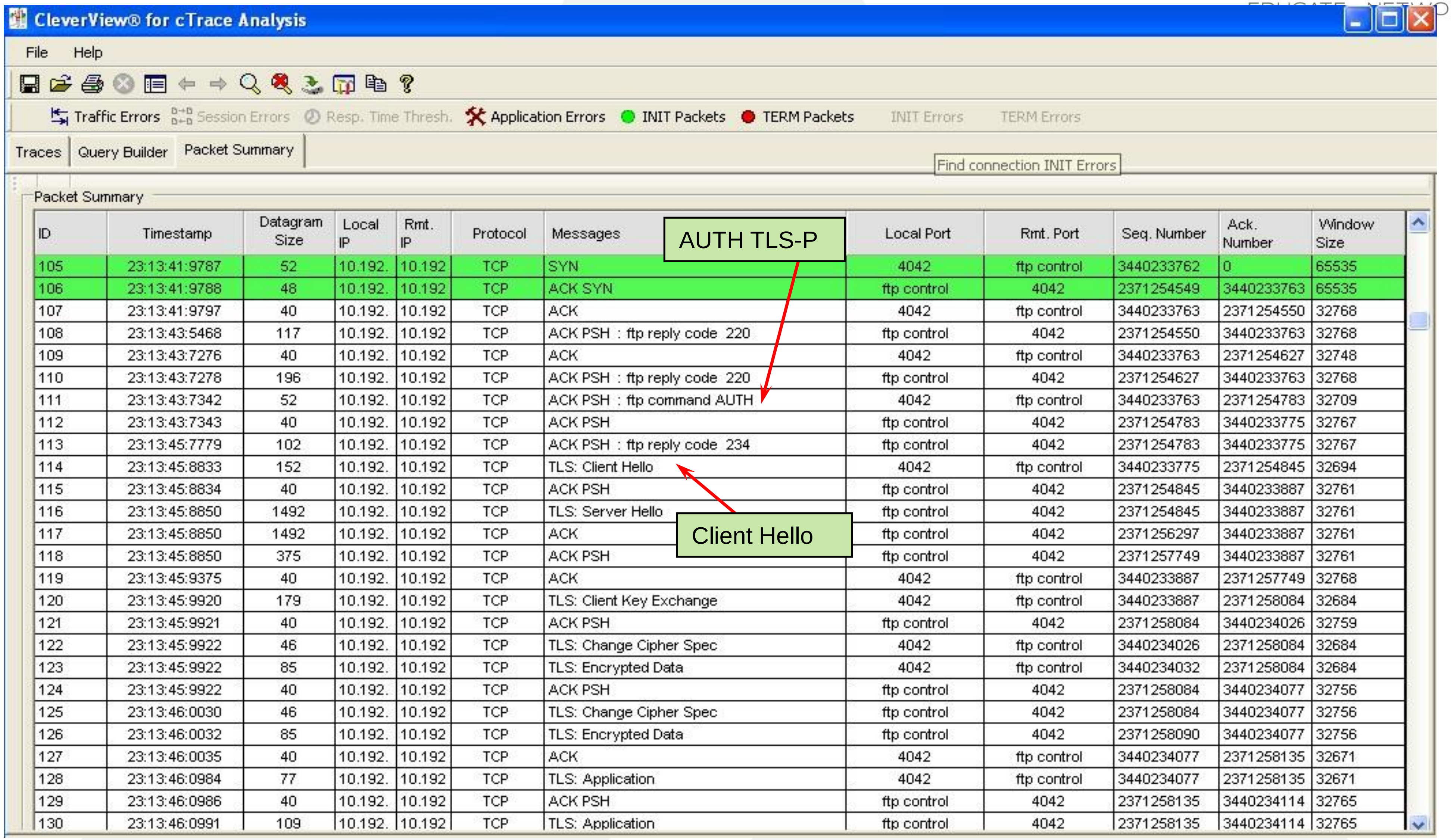
TLS Handshake &
Change Cipher Spec

Normal Flow – Encrypted

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

AT-TLS - FTP w/SSL



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
105	23:13:41:9787	52	10.192.	10.192	TCP	SYN	4042	ftp control	3440233762	0	65535
106	23:13:41:9788	48	10.192.	10.192	TCP	ACK SYN	ftp control	4042	2371254549	3440233763	65535
107	23:13:41:9797	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440233763	2371254550	32768
108	23:13:43:5468	117	10.192.	10.192	TCP	ACK PSH : ftp reply code 220	ftp control	4042	2371254550	3440233763	32768
109	23:13:43:7276	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440233763	2371254627	32748
110	23:13:43:7278	196	10.192.	10.192	TCP	ACK PSH : ftp reply code 220	ftp control	4042	2371254627	3440233763	32768
111	23:13:43:7342	52	10.192.	10.192	TCP	ACK PSH : ftp command AUTH	4042	ftp control	3440233763	2371254783	32709
112	23:13:43:7343	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371254783	3440233775	32767
113	23:13:45:7779	102	10.192.	10.192	TCP	ACK PSH : ftp reply code 234	ftp control	4042	2371254783	3440233775	32767
114	23:13:45:8833	152	10.192.	10.192	TCP	TLS: Client Hello	4042	ftp control	3440233775	2371254845	32694
115	23:13:45:8834	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371254845	3440233887	32761
116	23:13:45:8850	1492	10.192.	10.192	TCP	TLS: Server Hello	ftp control	4042	2371254845	3440233887	32761
117	23:13:45:8850	1492	10.192.	10.192	TCP	ACK	ftp control	4042	2371256297	3440233887	32761
118	23:13:45:8850	375	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371257749	3440233887	32761
119	23:13:45:9375	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440233887	2371257749	32768
120	23:13:45:9920	179	10.192.	10.192	TCP	TLS: Client Key Exchange	4042	ftp control	3440233887	2371258084	32684
121	23:13:45:9921	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371258084	3440234026	32759
122	23:13:45:9922	46	10.192.	10.192	TCP	TLS: Change Cipher Spec	4042	ftp control	3440234026	2371258084	32684
123	23:13:45:9922	85	10.192.	10.192	TCP	TLS: Encrypted Data	4042	ftp control	3440234032	2371258084	32684
124	23:13:45:9922	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371258084	3440234077	32756
125	23:13:46:0030	46	10.192.	10.192	TCP	TLS: Change Cipher Spec	ftp control	4042	2371258084	3440234077	32756
126	23:13:46:0032	85	10.192.	10.192	TCP	TLS: Encrypted Data	ftp control	4042	2371258090	3440234077	32756
127	23:13:46:0035	40	10.192.	10.192	TCP	ACK	4042	ftp control	3440234077	2371258135	32671
128	23:13:46:0984	77	10.192.	10.192	TCP	TLS: Application	4042	ftp control	3440234077	2371258135	32671
129	23:13:46:0986	40	10.192.	10.192	TCP	ACK PSH	ftp control	4042	2371258135	3440234114	32765
130	23:13:46:0991	109	10.192.	10.192	TCP	TLS: Application	ftp control	4042	2371258135	3440234114	32765

AUTH TLS-P

Client Hello

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TLS Header

Offset	Length	Description	Decimal Value	Meaning
0	1	Content Type	20 (0x14)	Change Cipher Spec
			21 (0x15)	**Alert**
			22 (0x16)	Handshake
			23 (0x17)	Application
1	2	Version		
1	1	Major Version	3	
2	1	Minor Version	0	SSLv3
			1	TLS 1.0
			2	TLS 1.1
			3	TLS 1.2
3	2	Length	N	The length of the Protocol Message
5	N	Protocol Message		

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TLS Alert Protocol (Content Type = 21)

Offset	Length	Description	Decimal Value	Meaning
5	1	Level of alert	1	Warning – connection or security may be unstable
			2	Fatal – connection or security may be compromised, or an unrecoverable error has occurred.
			Others	Encrypted alert
6	1	Alert Description Type	0	Close notify
			10	Unexpected message
			20	Bad record MAC
			21	Decryption failed
			22	Record overflow
			30	Decompression failure
			40	Handshake fail
			41	No certificate
			42	Bad certificate
			43	Unsupported certificate
			44	Certificate revoked
			45	Certificate expired
			46	Certificate unknown
			47	Illegal parameter
			48	Unknown CA (Certificate Authority)
			49	Access denied
			50	Decode error
			51	Decrypt error
			60	Export restriction
			70	Protocol version not supported
			71	Insufficient security
			80	Internal error
			90	User cancelled
			100	No renegotiation
			110	Unsupported extension

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Sample TLS/SSL Decoding

```
Hex Data:
16 03 01 00 C1 01 00 00 BD 03 01 4B 71 F1 69 DA 10 ….

Secure Socket Layer
   TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 193
      Handshake Protocol: Client Hello
         Handshake Type: Client Hello (1)
         Length: 189
         Version: TLS 1.0 (0x0301)
         Random
            GMT Unix Time: Feb 9, 2010 15:36:09.0000000000
            Random Bytes: DA10 …..
         Session ID Length: 32
         Session ID: 2D585DAEF198D9BB951DD9F58D7766465B88A493B98ACC3C...
         Cipher Suites Length: 70
         Cipher Suites (35 suites)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
            Cipher Suite: …….
```

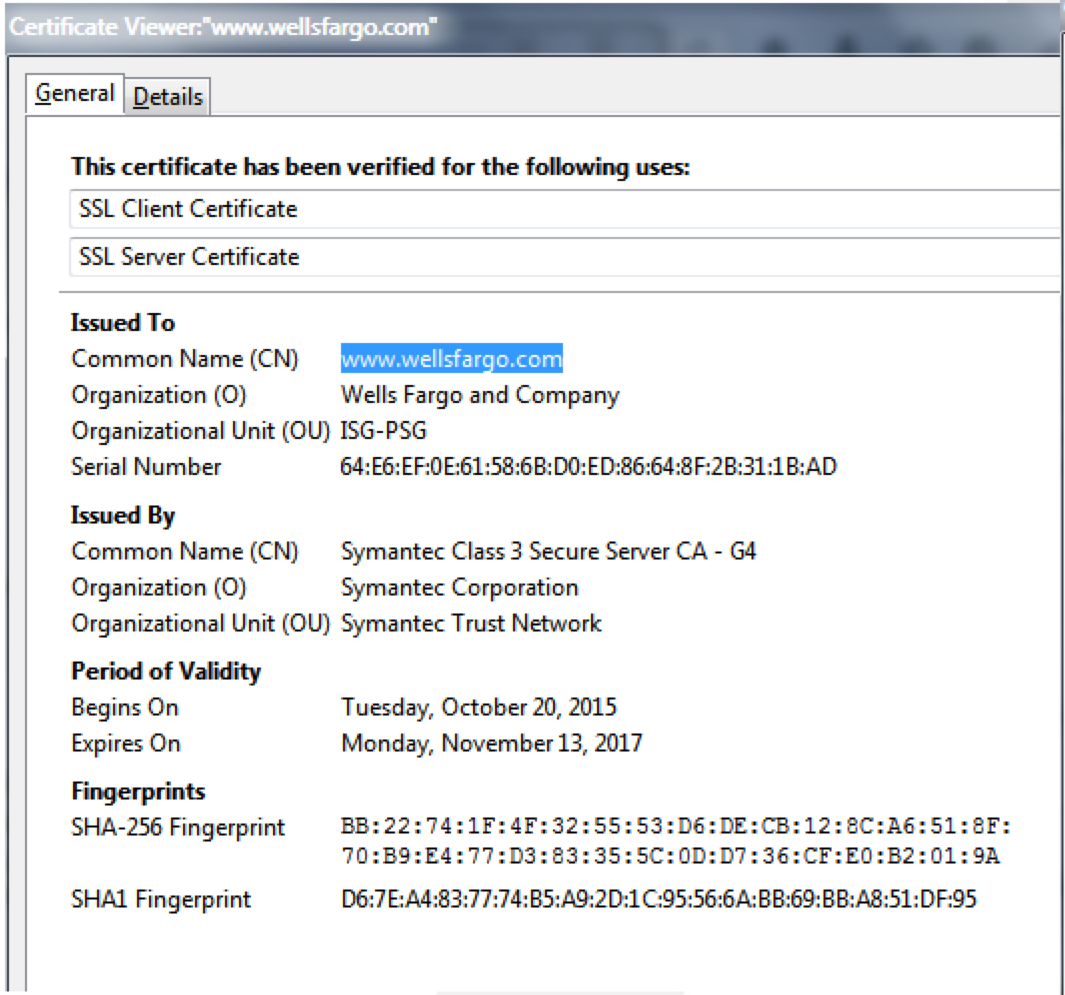
28 Random Bytes - to be used with the premaster secret to generate the symmetric key.

Ciphers are listed in order of preference – from the strongest to the weakest

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Sample Digital Certificate



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	www.wellsfargo.com
Organization (O)	Wells Fargo and Company
Organizational Unit (OU)	ISG-PSG
Serial Number	64:E6:EF:0E:61:58:6B:D0:ED:86:64:8F:2B:31:1B:AD

Issued By

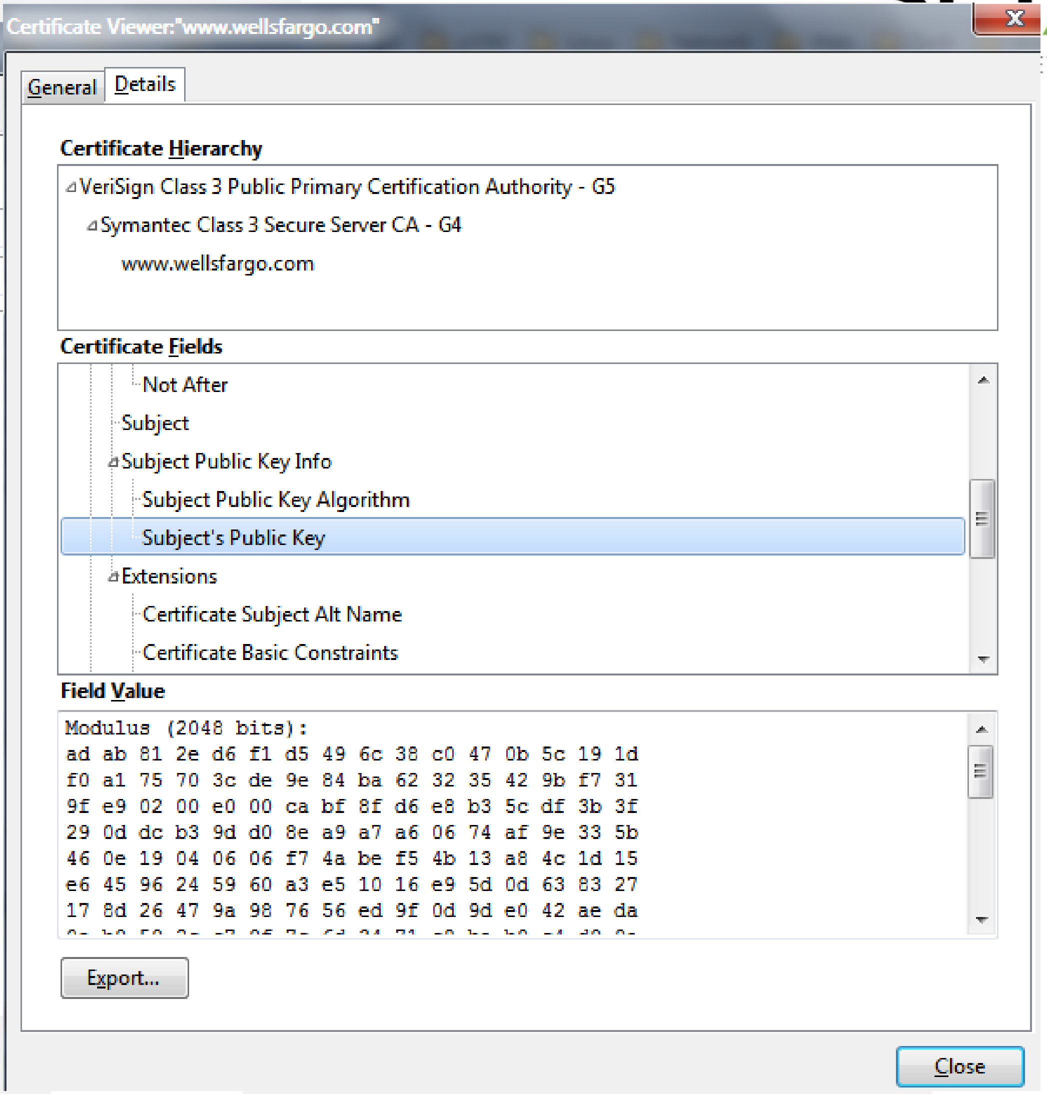
Common Name (CN)	Symantec Class 3 Secure Server CA - G4
Organization (O)	Symantec Corporation
Organizational Unit (OU)	Symantec Trust Network

Period of Validity

Begins On	Tuesday, October 20, 2015
Expires On	Monday, November 13, 2017

Fingerprints

SHA-256 Fingerprint	BB:22:74:1F:4F:32:55:53:D6:DE:CB:12:8C:A6:51:8F: 70:B9:E4:77:D3:83:35:5C:0D:D7:36:CF:E0:B2:01:9A
SHA1 Fingerprint	D6:7E:A4:83:77:74:B5:A9:2D:1C:95:56:6A:BB:69:BB:A8:51:DF:95



Certificate Hierarchy

- VeriSign Class 3 Public Primary Certification Authority - G5
  - Symantec Class 3 Secure Server CA - G4
    - www.wellsfargo.com

Certificate Fields

- Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensions
  - Certificate Subject Alt Name
  - Certificate Basic Constraints

Field Value

```
Modulus (2048 bits):
ad ab 81 2e d6 f1 d5 49 6c 38 c0 47 0b 5c 19 1d
f0 a1 75 70 3c de 9e 84 ba 62 32 35 42 9b f7 31
9f e9 02 00 e0 00 ca bf 8f d6 e8 b3 5c df 3b 3f
29 0d dc b3 9d d0 8e a9 a7 a6 06 74 af 9e 33 5b
46 0e 19 04 06 06 f7 4a be f5 4b 13 a8 4c 1d 15
e6 45 96 24 59 60 a3 e5 10 16 e9 5d 0d 63 83 27
17 8d 26 47 9a 98 76 56 ed 9f 0d 9d e0 42 ae da
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

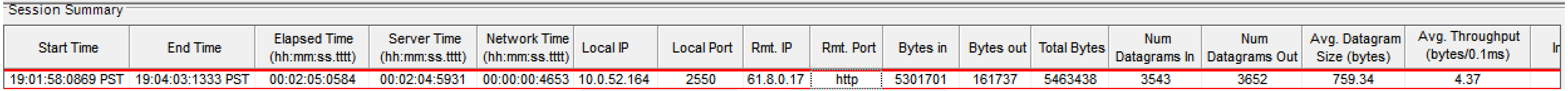
AT-TLS Data Decryption

- AT-TLS data is always encrypted in the packet trace. By default, Data Trace does not show unencrypted AT-TLS data either for security reason.
- However, user can configure AT-TLS policy to turn on the CtraceClearText parameter to trace the unencrypted application data.

Copyright © 2017 Applied Expert Systems, Inc.

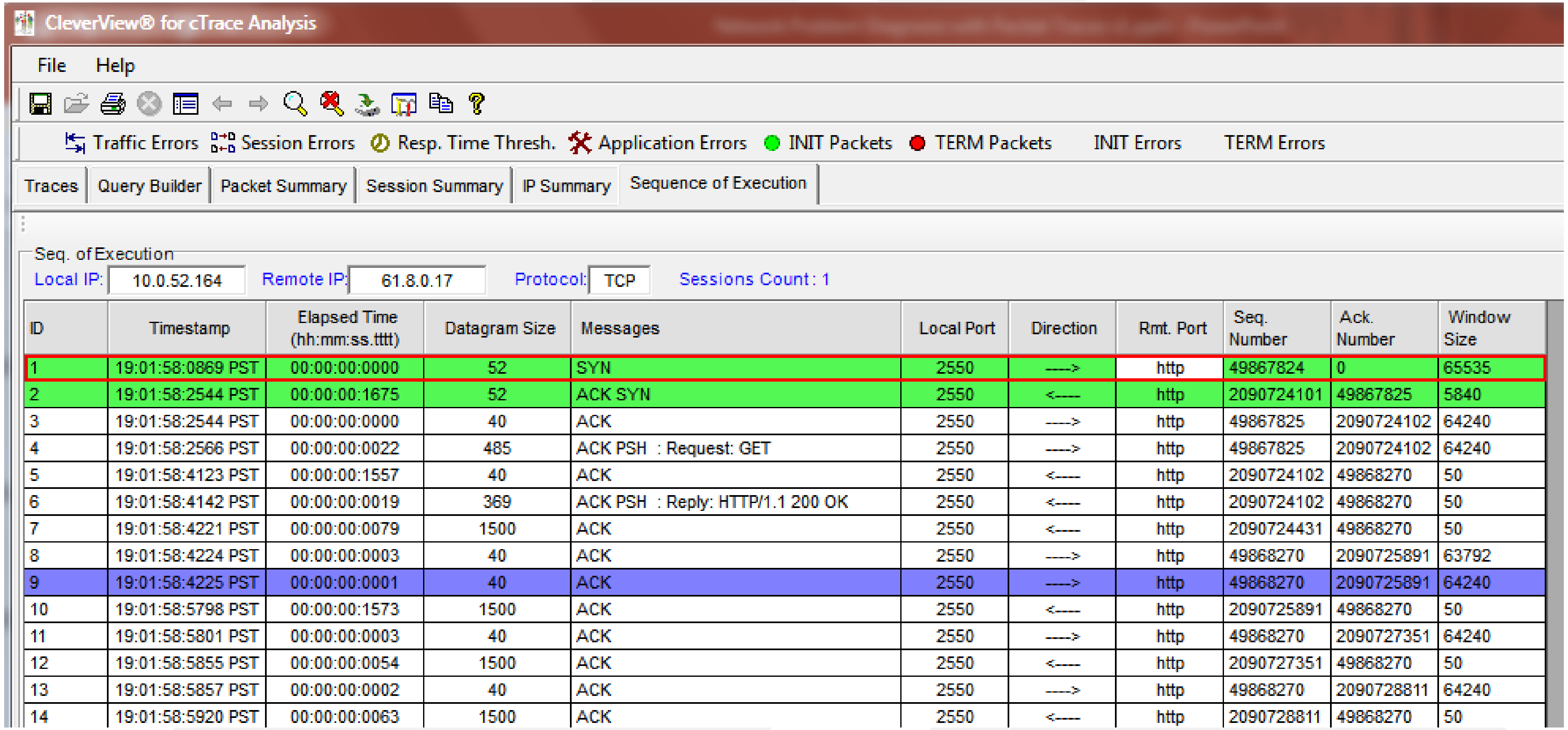
Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Performance Problem



Session Summary

Start Time	End Time	Elapsed Time (hh:mm:ss.tttt)	Server Time (hh:mm:ss.tttt)	Network Time (hh:mm:ss.tttt)	Local IP	Local Port	Rmt. IP	Rmt. Port	Bytes in	Bytes out	Total Bytes	Num Datagrams In	Num Datagrams Out	Avg. Datagram Size (bytes)	Avg. Throughput (bytes/0.1ms)	Ir
19:01:58:0869 PST	19:04:03:1333 PST	00:02:05:0584	00:02:04:5931	00:00:00:4653	10.0.52.164	2550	61.8.0.17	http	5301701	161737	5463438	3543	3652	759.34	4.37	



Seq. of Execution

Local IP: 10.0.52.164 Remote IP: 61.8.0.17 Protocol: TCP Sessions Count : 1

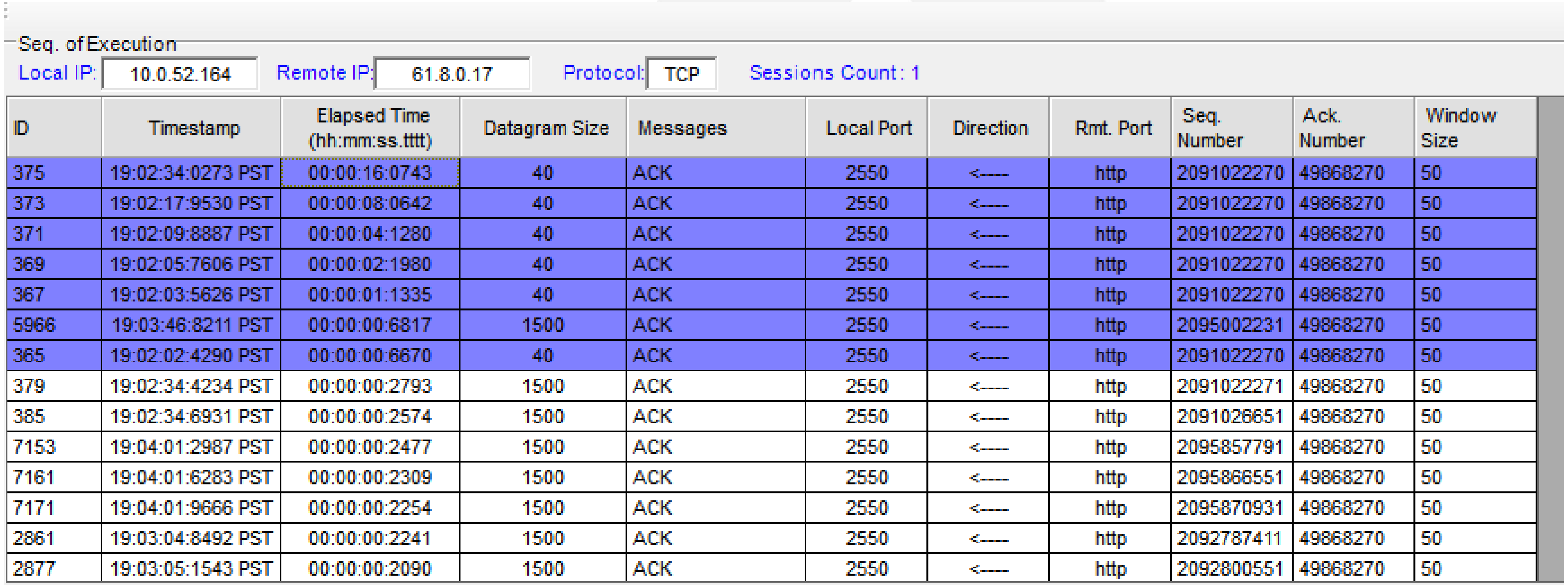
ID	Timestamp	Elapsed Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
1	19:01:58:0869 PST	00:00:00:0000	52	SYN	2550	---->	http	49867824	0	65535
2	19:01:58:2544 PST	00:00:00:1675	52	ACK SYN	2550	<----	http	2090724101	49867825	5840
3	19:01:58:2544 PST	00:00:00:0000	40	ACK	2550	---->	http	49867825	2090724102	64240
4	19:01:58:2566 PST	00:00:00:0022	485	ACK PSH : Request: GET	2550	---->	http	49867825	2090724102	64240
5	19:01:58:4123 PST	00:00:00:1557	40	ACK	2550	<----	http	2090724102	49868270	50
6	19:01:58:4142 PST	00:00:00:0019	369	ACK PSH : Reply: HTTP/1.1 200 OK	2550	<----	http	2090724102	49868270	50
7	19:01:58:4221 PST	00:00:00:0079	1500	ACK	2550	<----	http	2090724431	49868270	50
8	19:01:58:4224 PST	00:00:00:0003	40	ACK	2550	---->	http	49868270	2090725891	63792
9	19:01:58:4225 PST	00:00:00:0001	40	ACK	2550	---->	http	49868270	2090725891	64240
10	19:01:58:5798 PST	00:00:00:1573	1500	ACK	2550	<----	http	2090725891	49868270	50
11	19:01:58:5801 PST	00:00:00:0003	40	ACK	2550	---->	http	49868270	2090727351	64240
12	19:01:58:5855 PST	00:00:00:0054	1500	ACK	2550	<----	http	2090727351	49868270	50
13	19:01:58:5857 PST	00:00:00:0002	40	ACK	2550	---->	http	49868270	2090728811	64240
14	19:01:58:5920 PST	00:00:00:0063	1500	ACK	2550	<----	http	2090728811	49868270	50

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Performance Problem - continued

- Between which packets is the most time spent?



Seq. of Execution

Local IP: 10.0.52.164 Remote IP: 61.8.0.17 Protocol: TCP Sessions Count : 1

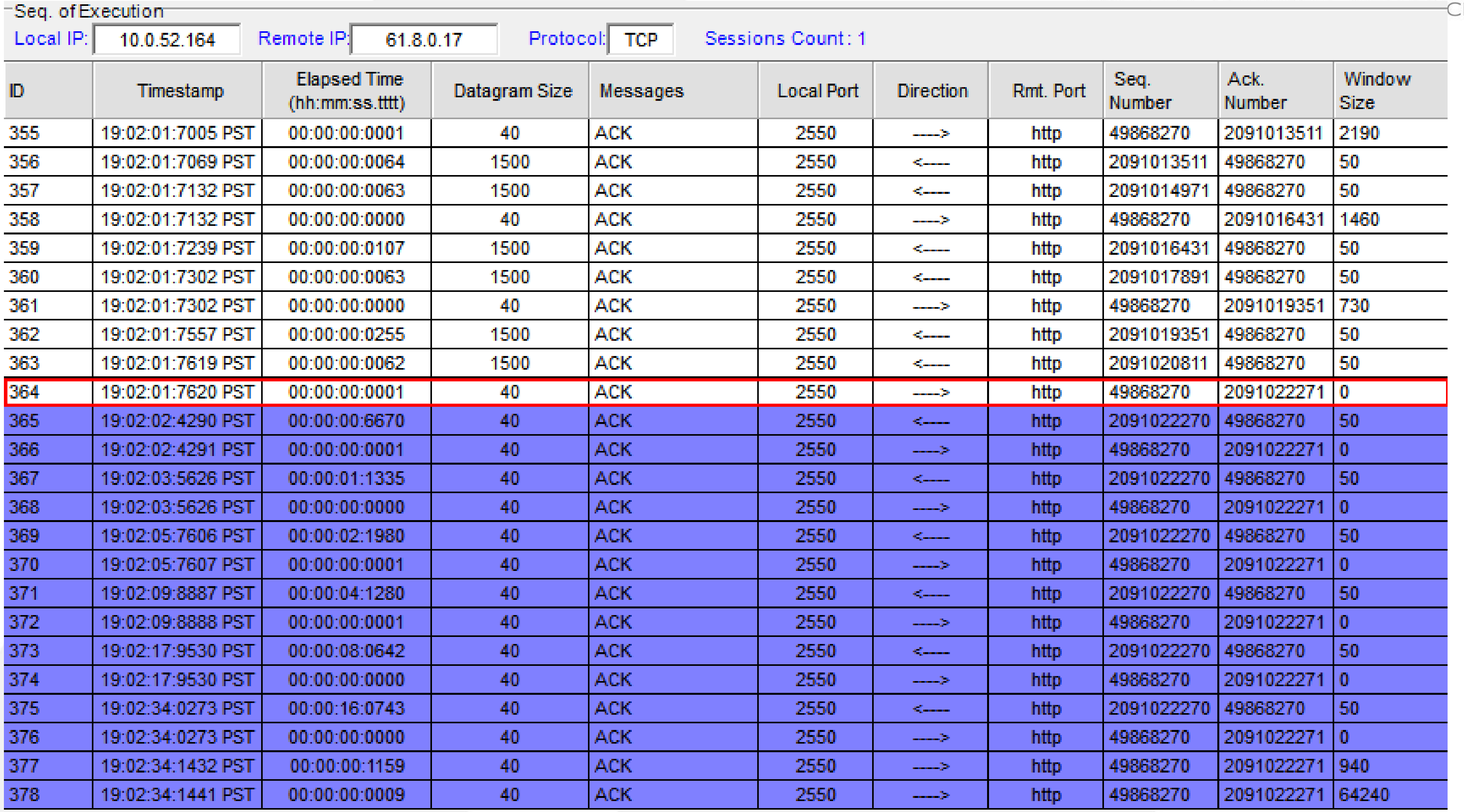
ID	Timestamp	Elapsed Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
375	19:02:34:0273 PST	00:00:16:0743	40	ACK	2550	<----	http	2091022270	49868270	50
373	19:02:17:9530 PST	00:00:08:0642	40	ACK	2550	<----	http	2091022270	49868270	50
371	19:02:09:8887 PST	00:00:04:1280	40	ACK	2550	<----	http	2091022270	49868270	50
369	19:02:05:7606 PST	00:00:02:1980	40	ACK	2550	<----	http	2091022270	49868270	50
367	19:02:03:5626 PST	00:00:01:1335	40	ACK	2550	<----	http	2091022270	49868270	50
5966	19:03:46:8211 PST	00:00:00:6817	1500	ACK	2550	<----	http	2095002231	49868270	50
365	19:02:02:4290 PST	00:00:00:6670	40	ACK	2550	<----	http	2091022270	49868270	50
379	19:02:34:4234 PST	00:00:00:2793	1500	ACK	2550	<----	http	2091022271	49868270	50
385	19:02:34:6931 PST	00:00:00:2574	1500	ACK	2550	<----	http	2091026651	49868270	50
7153	19:04:01:2987 PST	00:00:00:2477	1500	ACK	2550	<----	http	2095857791	49868270	50
7161	19:04:01:6283 PST	00:00:00:2309	1500	ACK	2550	<----	http	2095866551	49868270	50
7171	19:04:01:9666 PST	00:00:00:2254	1500	ACK	2550	<----	http	2095870931	49868270	50
2861	19:03:04:8492 PST	00:00:00:2241	1500	ACK	2550	<----	http	2092787411	49868270	50
2877	19:03:05:1543 PST	00:00:00:2090	1500	ACK	2550	<----	http	2092800551	49868270	50

Duplicate ACKs

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

Performance Problem - continued



Seq. of Execution

Local IP: 10.0.52.164 Remote IP: 61.8.0.17 Protocol: TCP Sessions Count: 1

ID	Timestamp	Elapsed Time (hh:mm:ss.tttt)	Datagram Size	Messages	Local Port	Direction	Rmt. Port	Seq. Number	Ack. Number	Window Size
355	19:02:01:7005 PST	00:00:00:0001	40	ACK	2550	---->	http	49868270	2091013511	2190
356	19:02:01:7069 PST	00:00:00:0064	1500	ACK	2550	<----	http	2091013511	49868270	50
357	19:02:01:7132 PST	00:00:00:0063	1500	ACK	2550	<----	http	2091014971	49868270	50
358	19:02:01:7132 PST	00:00:00:0000	40	ACK	2550	---->	http	49868270	2091016431	1460
359	19:02:01:7239 PST	00:00:00:0107	1500	ACK	2550	<----	http	2091016431	49868270	50
360	19:02:01:7302 PST	00:00:00:0063	1500	ACK	2550	<----	http	2091017891	49868270	50
361	19:02:01:7302 PST	00:00:00:0000	40	ACK	2550	---->	http	49868270	2091019351	730
362	19:02:01:7557 PST	00:00:00:0255	1500	ACK	2550	<----	http	2091019351	49868270	50
363	19:02:01:7619 PST	00:00:00:0062	1500	ACK	2550	<----	http	2091020811	49868270	50
364	19:02:01:7620 PST	00:00:00:0001	40	ACK	2550	---->	http	49868270	2091022271	0
365	19:02:02:4290 PST	00:00:00:6670	40	ACK	2550	<----	http	2091022270	49868270	50
366	19:02:02:4291 PST	00:00:00:0001	40	ACK	2550	---->	http	49868270	2091022271	0
367	19:02:03:5626 PST	00:00:01:1335	40	ACK	2550	<----	http	2091022270	49868270	50
368	19:02:03:5626 PST	00:00:00:0000	40	ACK	2550	---->	http	49868270	2091022271	0
369	19:02:05:7606 PST	00:00:02:1980	40	ACK	2550	<----	http	2091022270	49868270	50
370	19:02:05:7607 PST	00:00:00:0001	40	ACK	2550	---->	http	49868270	2091022271	0
371	19:02:09:8887 PST	00:00:04:1280	40	ACK	2550	<----	http	2091022270	49868270	50
372	19:02:09:8888 PST	00:00:00:0001	40	ACK	2550	---->	http	49868270	2091022271	0
373	19:02:17:9530 PST	00:00:08:0642	40	ACK	2550	<----	http	2091022270	49868270	50
374	19:02:17:9530 PST	00:00:00:0000	40	ACK	2550	---->	http	49868270	2091022271	0
375	19:02:34:0273 PST	00:00:16:0743	40	ACK	2550	<----	http	2091022270	49868270	50
376	19:02:34:0273 PST	00:00:00:0000	40	ACK	2550	---->	http	49868270	2091022271	0
377	19:02:34:1432 PST	00:00:00:1159	40	ACK	2550	---->	http	49868270	2091022271	940
378	19:02:34:1441 PST	00:00:00:0009	40	ACK	2550	---->	http	49868270	2091022271	64240

Zero Window Size

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

z/OS CTRACE: IDS Trace (SYSTCPIS)

- **CTIIDS*xx*** PARMLIB member:

```
TRACEOPTS
           WTRSTART(AESWRT)
           ON
           WTR(AESWRT)
           BUFSIZE(32M)
```

- S TCPIP,PARM=‘IDS=*xx*’
- IDS Policy Definition:

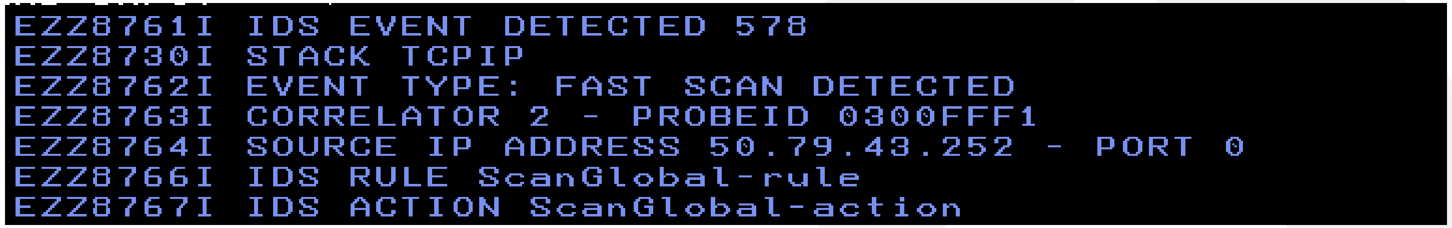
```
IDSAction                  ScanGlobal-action
{
  ActionType               ScanGlobal
  IDSReportSet             ScanGlobalReportSet
  {
    TypeActions            CONSOLE
    MaxEventMessage        15
    TypeActions            LOG
    LogDetail              Yes
    TypeActions            STATISTICS
    TypeActions            TRACE
    TraceData              FULL
  }
}
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

IDS Trace Analysis

- IDS Messages



```
EZZ8761I IDS EVENT DETECTED 578
EZZ8730I STACK TCPIP
EZZ8762I EVENT TYPE: FAST SCAN DETECTED
EZZ8763I CORRELATOR 2 - PROBEID 0300FFF1
EZZ8764I SOURCE IP ADDRESS 50.79.43.252 - PORT 0
EZZ8766I IDS RULE ScanGlobal-rule
EZZ8767I IDS ACTION ScanGlobal-action
```

- PROBEID – Identifies and describes the type of IDS event
  - Attacks
  - Intrusions
  - Traffic Regulations

- Correlator – Correlates to the offending packets in the trace

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

IDS Trace Analysis

IDS **PROBEIDs** are four bytes in length.

Byte 1 - indicates the IDS type:

- X'01' TCP ***Traffic Regulation*** event
- X'02' UDP ***Traffic Regulation*** event
- X'03' ***Scan*** detection event
- X'04' ***Attack*** detection event

Byte 2:

- ***Scan*** - Suspicious level
- X'01' for very suspicious packet.
- X'02' for possibly suspicious packet.
- X'03' for normal packet.
- X'00' is used to report a scan detected event or other unusual situation that
- might affect scan processing. These conditions are not written to the IDS trace
- but are written to the syslogd or the console if requested by the policy.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

IDS Trace Analysis

PROBEID Byte 2:

- ***Attack*** - Type of attack
  - X'01' MALFORMED_PACKET
  - X'02' OUTBOUND_RAW
  - X'03' IP_FRAGMENT
  - X'04' ICMP_REDIRECT
  - X'05' RESTRICTED_IP_OPTIONS
  - X'06' RESTRICTED_IP_PROTOCOL
  - X'07' FLOOD
  - X'08' PERPETUAL_ECHO
  - X'09' DATA_HIDING
  - X'0A' TCP_QUEUE_SIZE
  - X'0B' GLOBAL_TCP_STALL
  - X'0C' OUTBOUND_RAW_IPV6
  - X'0D' RESTRICTED_IPV6_NEXT_HDR
  - X'0E' RESTRICTED_IPV6_DST_OPTIONS
  - X'0F' RESTRICTED_IPV6_HOP_OPTIONS
  - X'10' EE_LDLC_CHECK
  - X'11' EE_MALFORMED_PACKET
  - X'12' EE_PORT_CHECK
  - X'13' EE_XID_FLOOD

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

IDS Trace Analysis - PROBEID

X'01000001' TCP TR, enter constrained for receive queue.

X'01000002' TCP TR, exit constrained for receive queue.

X'01000003' TCP TR, enter constrained for send queue.

X'01000004' TCP TR, exit constrained for send queue.

X'01002200' TCP TR, enter or leave constrained during close processing.

X'01002400' TCP TR, enter or leave constrained during close processing.

…….

X'04130001' Attack, type=EE_XID_FLOOD, A non-responsive XID was logged.

X'04130002' Attack, type=EE_XID_FLOOD, An XID flood start was detected.

X'04130003' Attack, type=EE_XID_FLOOD, An XID flood end was detected.

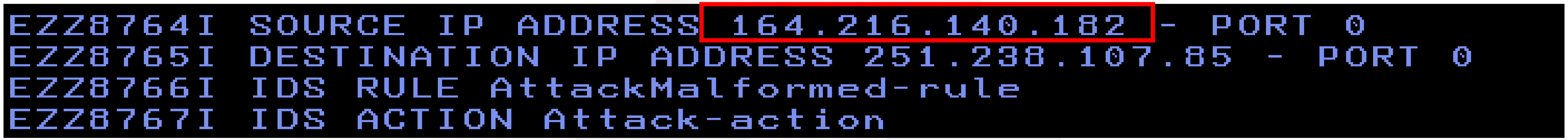
X'0413FFF0' Attack, type=EE_XID_FLOOD, Log records suppressed for EE XID flood attacks

Reference: z/OS Communications Server IP and SNA Codes

Copyright © 2017 Applied Expert Systems, Inc.

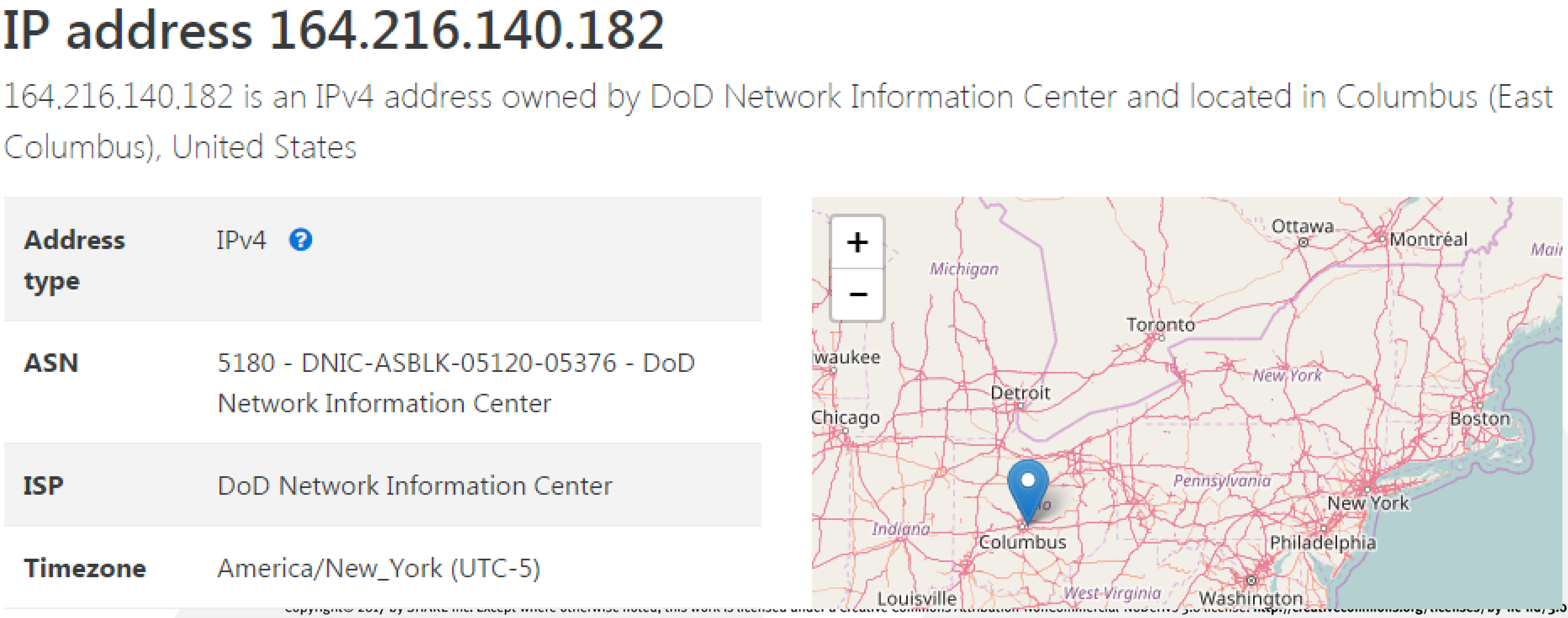
Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

IDS Trace Analysis – PROBEID example



```
EZZ8764I SOURCE IP ADDRESS 164.216.140.182 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 251.238.107.85 - PORT 0
EZZ8766I IDS RULE AttackMalformed-rule
EZZ8767I IDS ACTION Attack-action
```

PROBEID 04010006 - Attack, type=MALFORMED_PACKET, IPv4 header error, source IP address/destination IP address error.



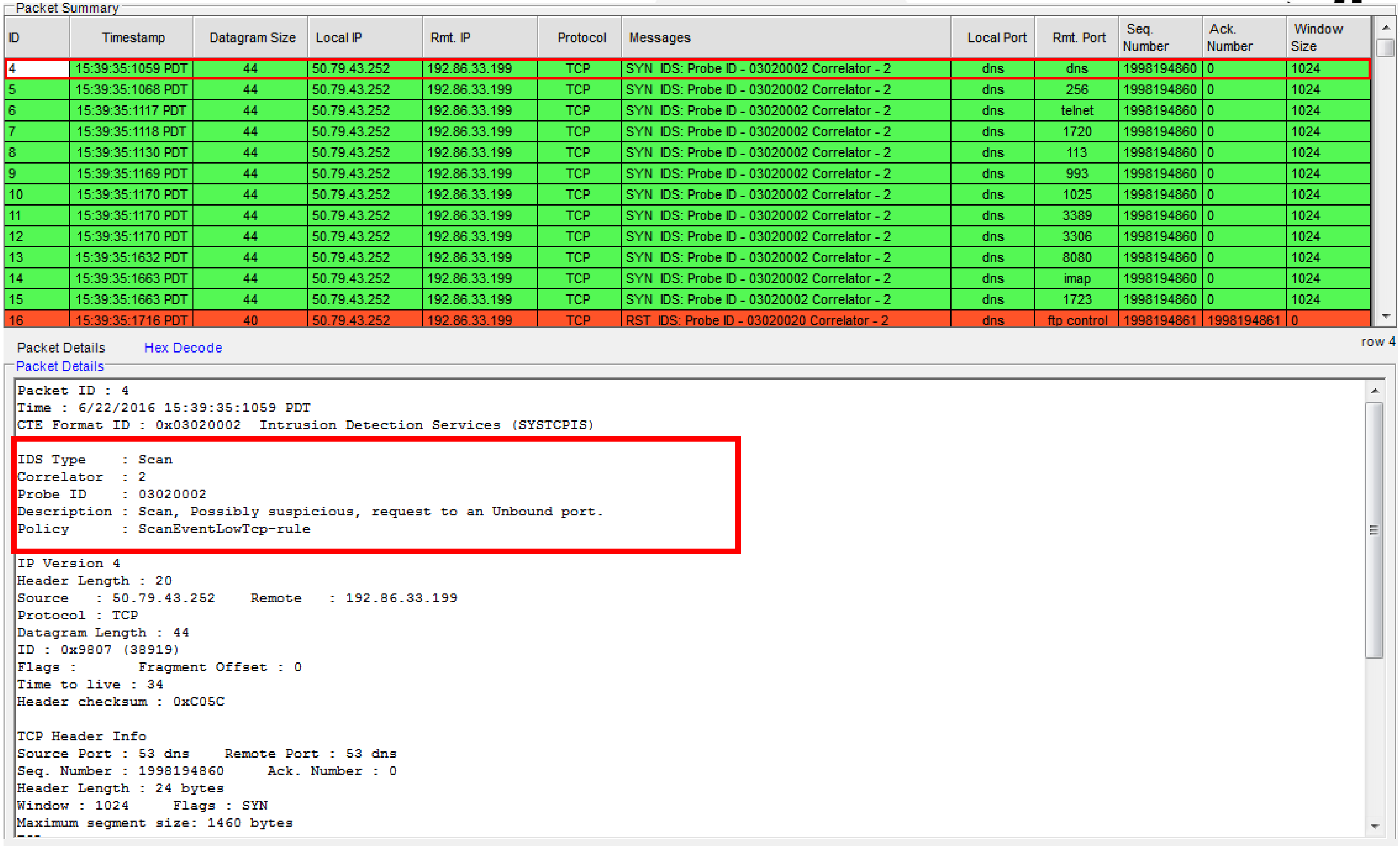
IP address 164.216.140.182

164.216.140.182 is an IPv4 address owned by DoD Network Information Center and located in Columbus (East Columbus), United States

Address type	IPv4 ?
ASN	5180 - DNIC-ASBLK-05120-05376 - DoD Network Information Center
ISP	DoD Network Information Center
Timezone	America/New_York (UTC-5)

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

IDS Trace Analysis



Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
4	15:39:35:1059 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	dns	1998194860	0	1024
5	15:39:35:1068 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	256	1998194860	0	1024
6	15:39:35:1117 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	telnet	1998194860	0	1024
7	15:39:35:1118 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	1720	1998194860	0	1024
8	15:39:35:1130 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	113	1998194860	0	1024
9	15:39:35:1169 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	993	1998194860	0	1024
10	15:39:35:1170 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	1025	1998194860	0	1024
11	15:39:35:1170 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	3389	1998194860	0	1024
12	15:39:35:1170 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	3306	1998194860	0	1024
13	15:39:35:1632 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	8080	1998194860	0	1024
14	15:39:35:1663 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	imap	1998194860	0	1024
15	15:39:35:1663 PDT	44	50.79.43.252	192.86.33.199	TCP	SYN IDS: Probe ID - 03020002 Correlator - 2	dns	1723	1998194860	0	1024
16	15:39:35:1716 PDT	40	50.79.43.252	192.86.33.199	TCP	RST IDS: Probe ID - 03020020 Correlator - 2	dns	ftp control	1998194861	1998194861	0

```
Packet ID : 4
Time : 6/22/2016 15:39:35:1059 PDT
CTE Format ID : 0x03020002  Intrusion Detection Services (SYSTCPIS)

IDS Type     : Scan
Correlator   : 2
Probe ID     : 03020002
Description  : Scan, Possibly suspicious, request to an Unbound port.
Policy       : ScanEventLowTcp-rule

IP Version 4
Header Length : 20
Source    : 50.79.43.252     Remote    : 192.86.33.199
Protocol : TCP
Datagram Length : 44
ID : 0x9807 (38919)
Flags :         Fragment Offset : 0
Time to live : 34
Header checksum : 0xC05C

TCP Header Info
Source Port : 53 dns    Remote Port : 53 dns
Seq. Number : 1998194860      Ack. Number : 0
Header Length : 24 bytes
Window : 1024     Flags : SYN
Maximum segment size: 1460 bytes
```

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Summary

- Establish baselines
- Use IP ID to track a packet across networks
- Host time vs. Network time
- Negotiate “down” (e.g., MSS, Window Scaling, SSL/TLS Handshake)
- Duplicate ACKs
- Zero-window size
- Ack Num = Incoming Seq Num + Bytes Received
- May need to trace “discarded packets”
- CTRACE Header has Discard Code
- Monitor network for anomalies and investigate the cause

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Appendix

How to Take a Packet Trace?

z/OS CTRACE:

- SYSTCPDA
  - Packet Trace
    - Scope: TCP/IP stack
    - Packets entering or leaving the TCP/IP stack
  - Data Trace
    - scope: TCP/IP stack
    - Socket data into and out of the Physical File System (PFS)
    - Application data (unencrypted)

- SYSTCPOT
  - OSAENTA
    - Scope: LPAR or CHPID
    - Frames entering or leaving an OSA adapter for a connected host
- STSTCPIS
  - Intrusion Detection Services (IDS)
  - Packets are traced based on IDS policies

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

z/OS CTRACE: SYSTCPDA – Packet Trace

- 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)
… other trace options …
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

z/OS CTRACE: SYSTCPDA – Packet Trace

- *To Start Tracing:*

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

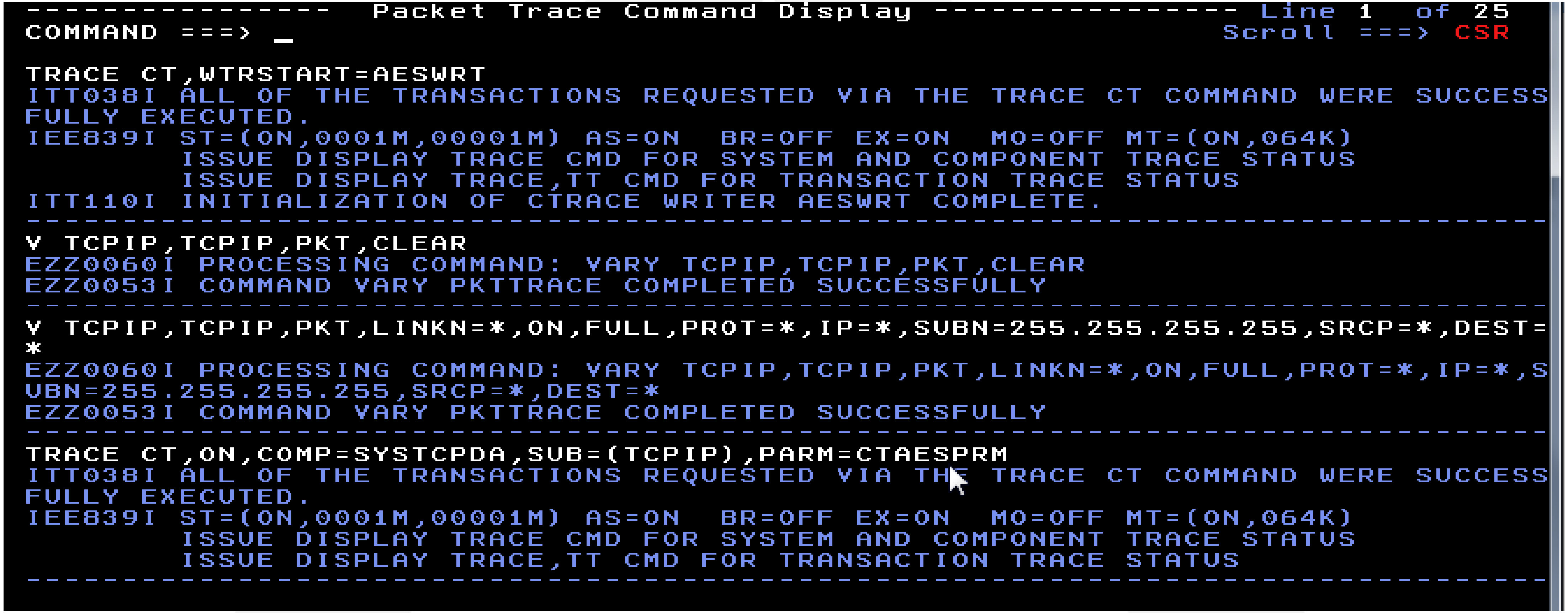
- *To View Tracing Status:*

D TRACE,WTR=AESWRT	Verify that the external writer is active
D TCPIP,tcpip,NETSTAT,DE	Verify that **TrRecCnt** is non-zero and incrementing

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

z/OS CTRACE: SYSTCPDA - Starting a Trace

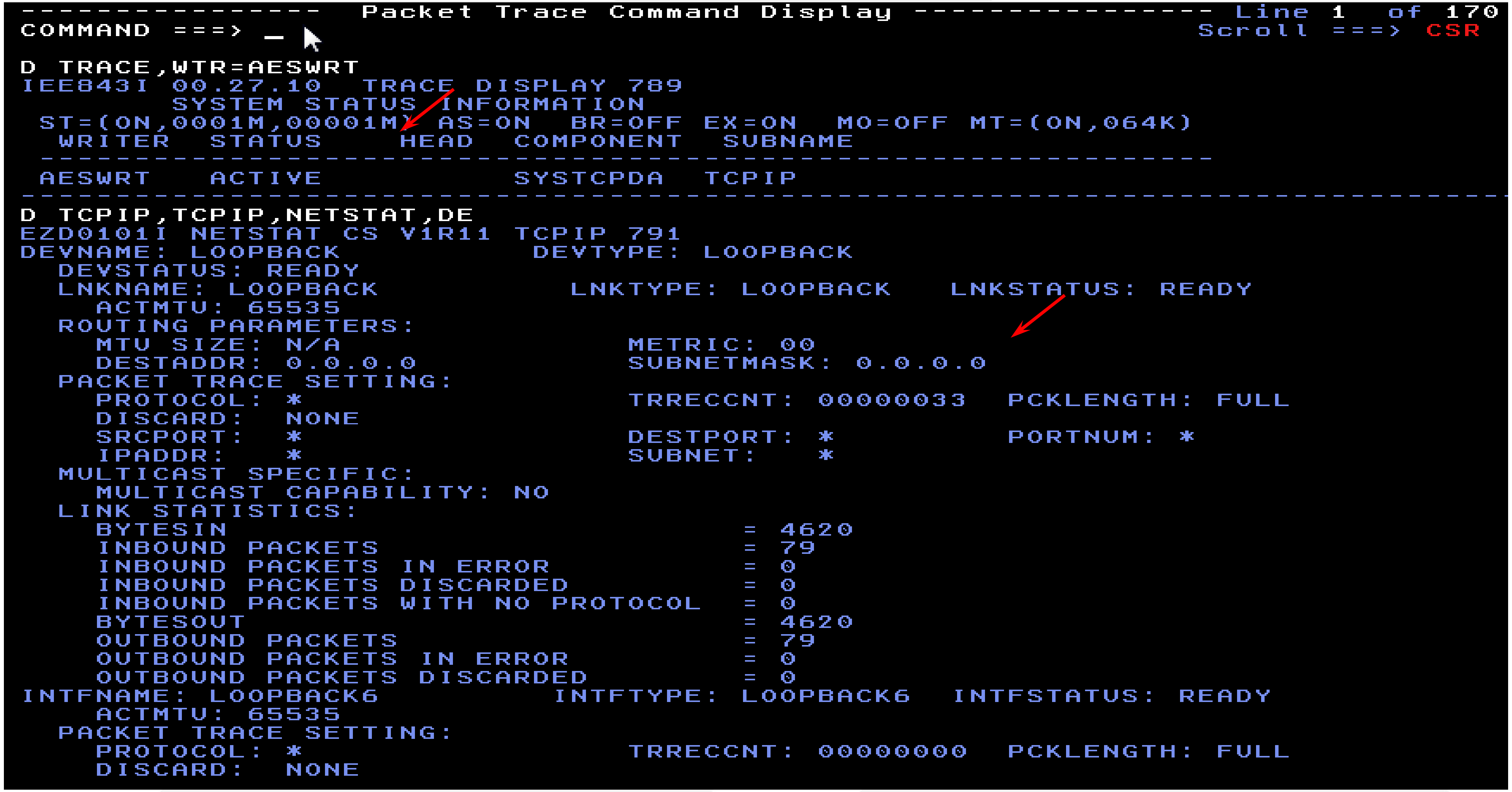


```
----------------  Packet Trace Command Display ----------------  Line 1  of 25
COMMAND ===> _                                                  Scroll ===> CSR

TRACE CT,WTRSTART=AESWRT
ITT038I ALL OF THE TRANSACTIONS REQUESTED VIA THE TRACE CT COMMAND WERE SUCCESS
FULLY EXECUTED.
IEE839I ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
        ISSUE DISPLAY TRACE CMD FOR SYSTEM AND COMPONENT TRACE STATUS
        ISSUE DISPLAY TRACE,TT CMD FOR TRANSACTION TRACE STATUS
ITT110I INITIALIZATION OF CTRACE WRITER AESWRT COMPLETE.
-------------------------------------------------------------------------------
V TCPIP,TCPIP,PKT,CLEAR
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,PKT,CLEAR
EZZ0053I COMMAND VARY PKTTRACE COMPLETED SUCCESSFULLY
-------------------------------------------------------------------------------
V TCPIP,TCPIP,PKT,LINKN=*,ON,FULL,PROT=*,IP=*,SUBN=255.255.255.255,SRCP=*,DEST=
*
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,PKT,LINKN=*,ON,FULL,PROT=*,IP=*,S
UBN=255.255.255.255,SRCP=*,DEST=*
EZZ0053I COMMAND VARY PKTTRACE COMPLETED SUCCESSFULLY
-------------------------------------------------------------------------------
TRACE CT,ON,COMP=SYSTCPDA,SUB=(TCPIP),PARM=CTAESPRM
ITT038I ALL OF THE TRANSACTIONS REQUESTED VIA THE TRACE CT COMMAND WERE SUCCESS
FULLY EXECUTED.
IEE839I ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
        ISSUE DISPLAY TRACE CMD FOR SYSTEM AND COMPONENT TRACE STATUS
        ISSUE DISPLAY TRACE,TT CMD FOR TRANSACTION TRACE STATUS
-------------------------------------------------------------------------------
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

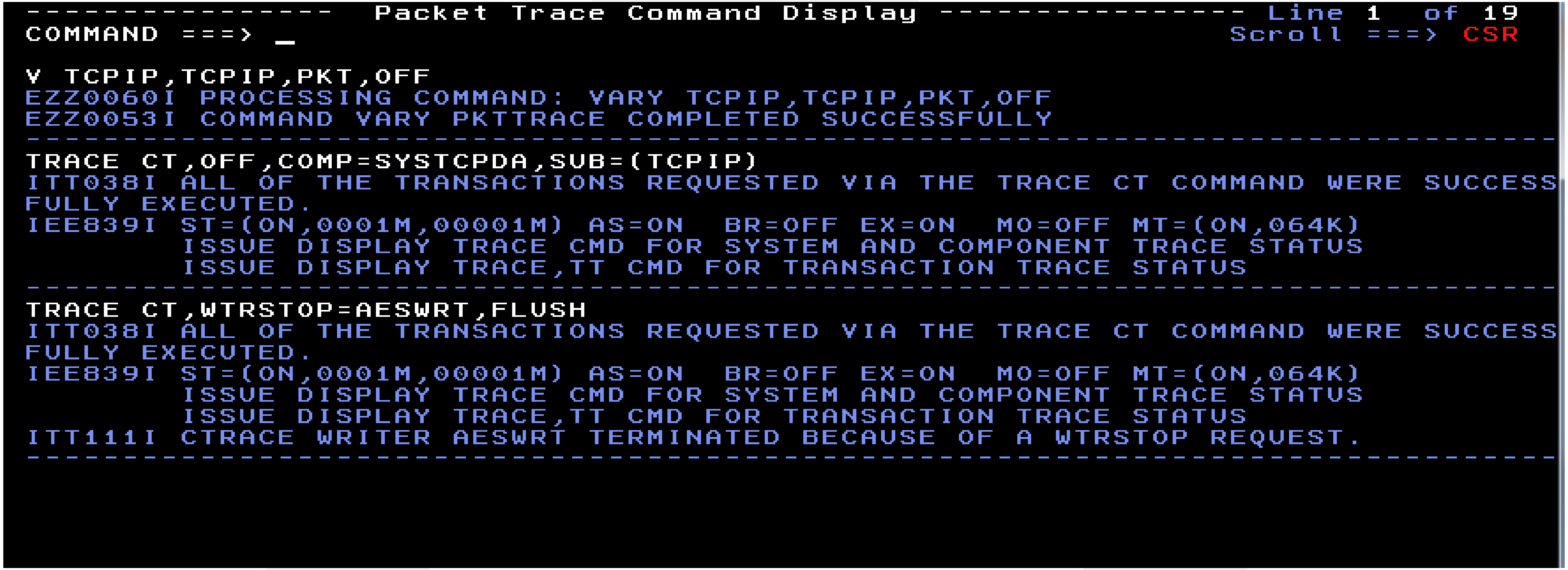
z/OS CTRACE: SYSTCPDA - Checking Trace Status



```
----------------  Packet Trace Command Display ---------------- Line 1  of 170
COMMAND ===> _                                                Scroll ===> CSR

D TRACE,WTR=AESWRT
IEE843I 00.27.10  TRACE DISPLAY  789
        SYSTEM STATUS INFORMATION
 ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
  WRITER  STATUS    HEAD  COMPONENT  SUBNAME
 ---------------------------------------------------------------
 AESWRT   ACTIVE          SYSTCPDA  TCPIP
-------------------------------------------------------------------------------
D TCPIP,TCPIP,NETSTAT,DE
EZD0101I NETSTAT CS V1R11 TCPIP  791
DEVNAME: LOOPBACK          DEVTYPE: LOOPBACK
  DEVSTATUS: READY
  LNKNAME: LOOPBACK          LNKTYPE: LOOPBACK   LNKSTATUS: READY
    ACTMTU: 65535
  ROUTING PARAMETERS:
    MTU SIZE: N/A               METRIC: 00
    DESTADDR: 0.0.0.0           SUBNETMASK: 0.0.0.0
  PACKET TRACE SETTING:
    PROTOCOL: *                 TRRECCNT: 00000033  PCKLENGTH: FULL
    DISCARD:  NONE
    SRCPORT:  *                 DESTPORT: *         PORTNUM: *
    IPADDR:   *                 SUBNET:   *
  MULTICAST SPECIFIC:
    MULTICAST CAPABILITY: NO
  LINK STATISTICS:
    BYTESIN                           = 4620
    INBOUND PACKETS                   = 79
    INBOUND PACKETS IN ERROR          = 0
    INBOUND PACKETS DISCARDED         = 0
    INBOUND PACKETS WITH NO PROTOCOL  = 0
    BYTESOUT                          = 4620
    OUTBOUND PACKETS                  = 79
    OUTBOUND PACKETS IN ERROR         = 0
    OUTBOUND PACKETS DISCARDED        = 0
INTFNAME: LOOPBACK6         INTFTYPE: LOOPBACK6  INTFSTATUS: READY
    ACTMTU: 65535
  PACKET TRACE SETTING:
    PROTOCOL: *                 TRRECCNT: 00000000  PCKLENGTH: FULL
    DISCARD:  NONE
```

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

z/OS CTRACE: SYSTCPDA - Stopping a Trace



```
----------------  Packet Trace Command Display ---------------- Line 1  of 19
COMMAND ===> _                                                Scroll ===> CSR

V TCPIP,TCPIP,PKT,OFF
EZZ0060I PROCESSING COMMAND: VARY TCPIP,TCPIP,PKT,OFF
EZZ0053I COMMAND VARY PKTTRACE COMPLETED SUCCESSFULLY
-------------------------------------------------------------------------------
TRACE CT,OFF,COMP=SYSTCPDA,SUB=(TCPIP)
ITT038I ALL OF THE TRANSACTIONS REQUESTED VIA THE TRACE CT COMMAND WERE SUCCESS
FULLY EXECUTED.
IEE839I ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
        ISSUE DISPLAY TRACE CMD FOR SYSTEM AND COMPONENT TRACE STATUS
        ISSUE DISPLAY TRACE,TT CMD FOR TRANSACTION TRACE STATUS
-------------------------------------------------------------------------------
TRACE CT,WTRSTOP=AESWRT,FLUSH
ITT038I ALL OF THE TRANSACTIONS REQUESTED VIA THE TRACE CT COMMAND WERE SUCCESS
FULLY EXECUTED.
IEE839I ST=(ON,0001M,00001M) AS=ON  BR=OFF EX=ON  MO=OFF MT=(ON,064K)
        ISSUE DISPLAY TRACE CMD FOR SYSTEM AND COMPONENT TRACE STATUS
        ISSUE DISPLAY TRACE,TT CMD FOR TRANSACTION TRACE STATUS
ITT111I CTRACE WRITER AESWRT TERMINATED BECAUSE OF A WTRSTOP REQUEST.
-------------------------------------------------------------------------------
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

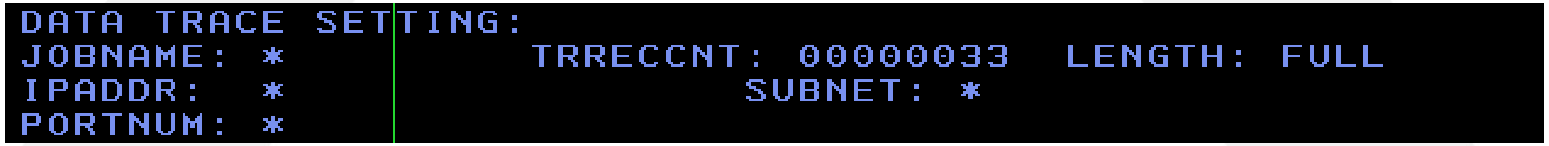
z/OS CTRACE: SYSTCPDA – Data Trace

- *To Start/Stop Data Trace:*

```
V TCPIP,tcpip,DAT,ON,<trace options>

V TCPIP,tcpip,DAT,OFF
```

- *To View Tracing Status:*

```
D TCPIP,tcpip,NETSTAT,CONFIG
```



```
DATA TRACE SETTING:
JOBNAME: *          TRRECCNT: 00000033  LENGTH: FULL
IPADDR:  *                  SUBNET: *
PORTNUM: *
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

z/OS CTRACE: SYSTCPOT – OSAENTA Trace

- OSA-Express Network Traffic Analyzer (OSAENTA)
  - Trace data is collected (by the device drivers of OSA) as frames enter or leave an OSA adapter for a connected host
  - The host can be an LPAR with **z/OS, z/VM** or **Linux**
  - ARP packets, MAC headers (w/VLAN tags)
  - The trace function is controlled by z/OS Communication Server, while the data is collected in the OSA at the network port

- Pre-Reqs:
  - Require 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

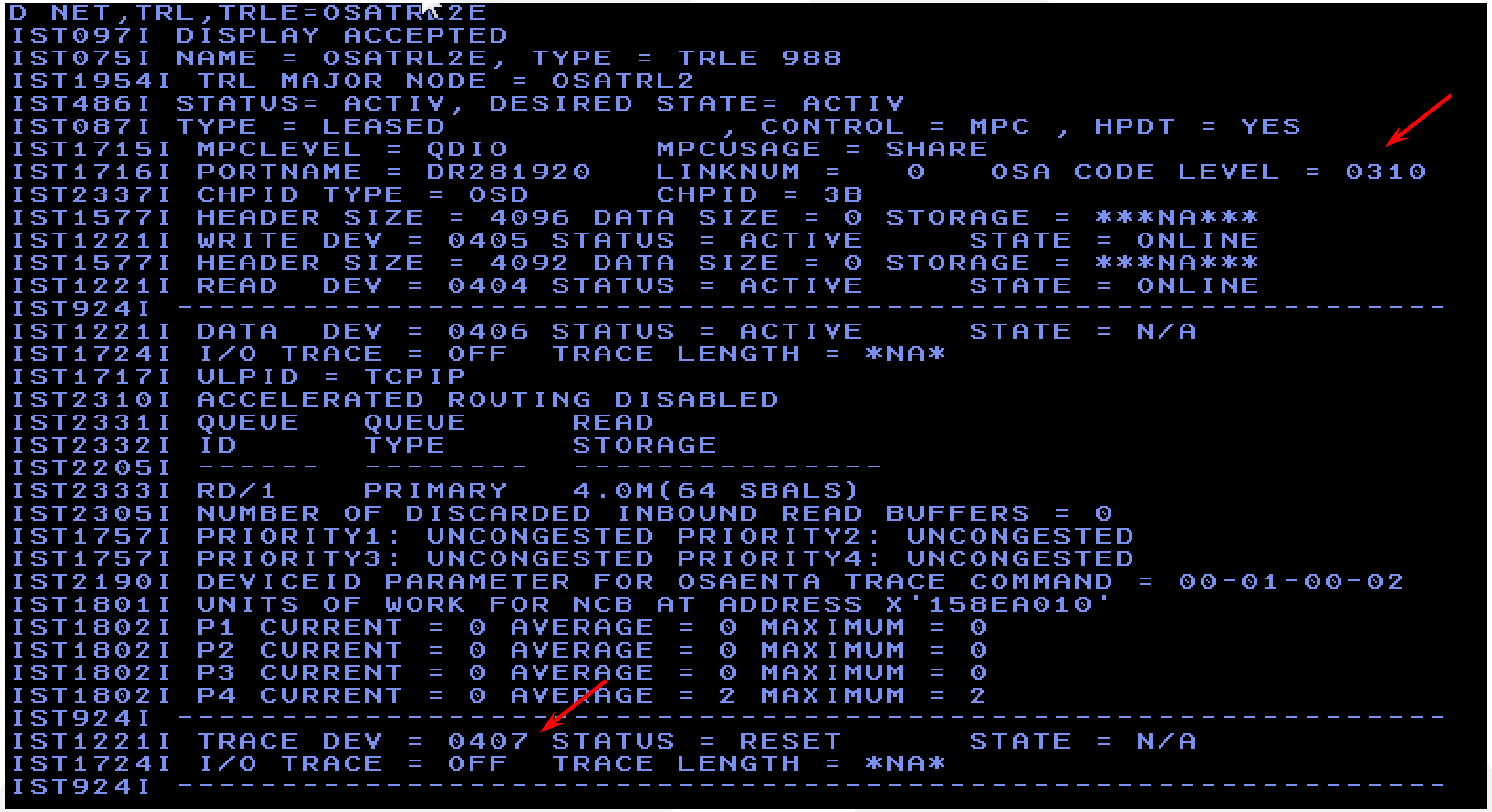
    CHPID - All packets using this CHPID
  - Verify the TRLE definitions for the OSA that it has one DATAPATH address available for tracing. Note that **two** DATAPATH addresses are required – one for data transfers and the other for trace data.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

TRLE Definition and D NET,TRL,TRLE=

```
OSATRL2  VBUILD TYPE=TRL
OSATRL2E TRLE LNCTL=MPC,READ=(0404),WRITE=(0405),DATAPATH=(0406,0407), X
               PORTNAME=DR281920,                                      X
```



```
D NET,TRL,TRLE=OSATRL2E
IST097I DISPLAY ACCEPTED
IST075I NAME = OSATRL2E, TYPE = TRLE 988
IST1954I TRL MAJOR NODE = OSATRL2
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST087I TYPE = LEASED             , CONTROL = MPC , HPDT = YES
IST1715I MPCLEVEL = QDIO       MPCUSAGE = SHARE
IST1716I PORTNAME = DR281920   LINKNUM =   0   OSA CODE LEVEL = 0310
IST2337I CHPID TYPE = OSD      CHPID = 3B
IST1577I HEADER SIZE = 4096 DATA SIZE = 0 STORAGE = ***NA***
IST1221I WRITE DEV = 0405 STATUS = ACTIVE     STATE = ONLINE
IST1577I HEADER SIZE = 4092 DATA SIZE = 0 STORAGE = ***NA***
IST1221I READ  DEV = 0404 STATUS = ACTIVE     STATE = ONLINE
IST924I -------------------------------------------------------------
IST1221I DATA  DEV = 0406 STATUS = ACTIVE     STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST1717I ULPID = TCPIP
IST2310I ACCELERATED ROUTING DISABLED
IST2331I QUEUE   QUEUE     READ
IST2332I ID      TYPE      STORAGE
IST2205I ------  --------  ---------------
IST2333I RD/1    PRIMARY   4.0M(64 SBALS)
IST2305I NUMBER OF DISCARDED INBOUND READ BUFFERS = 0
IST1757I PRIORITY1: UNCONGESTED PRIORITY2: UNCONGESTED
IST1757I PRIORITY3: UNCONGESTED PRIORITY4: UNCONGESTED
IST2190I DEVICEID PARAMETER FOR OSAENTA TRACE COMMAND = 00-01-00-02
IST1801I UNITS OF WORK FOR NCB AT ADDRESS X'158EA010'
IST1802I P1 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P2 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P3 CURRENT = 0 AVERAGE = 0 MAXIMUM = 0
IST1802I P4 CURRENT = 0 AVERAGE = 2 MAXIMUM = 2
IST924I -------------------------------------------------------------
IST1221I TRACE DEV = 0407 STATUS = RESET       STATE = N/A
IST1724I I/O TRACE = OFF  TRACE LENGTH = *NA*
IST924I -------------------------------------------------------------
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

z/OS CTRACE: OSAENTA

- *To Start Tracing*:

```
TRACE CT,WTRSTART=AESWRT
V TCPIP,tcpip,OSAENTA,PORTNAME=<port>,CLEAR
V TCPIP,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
  D TCPIP,tcpip,NETSTAT,DE
```

to verify that the external writer is active

to check status

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

z/OS CTRACE: OSAENTA

- To View Tracing Status (continued):

```
D TCPIP,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:  *
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

z/OS CTRACE: OSAENTA ABBREV Parm

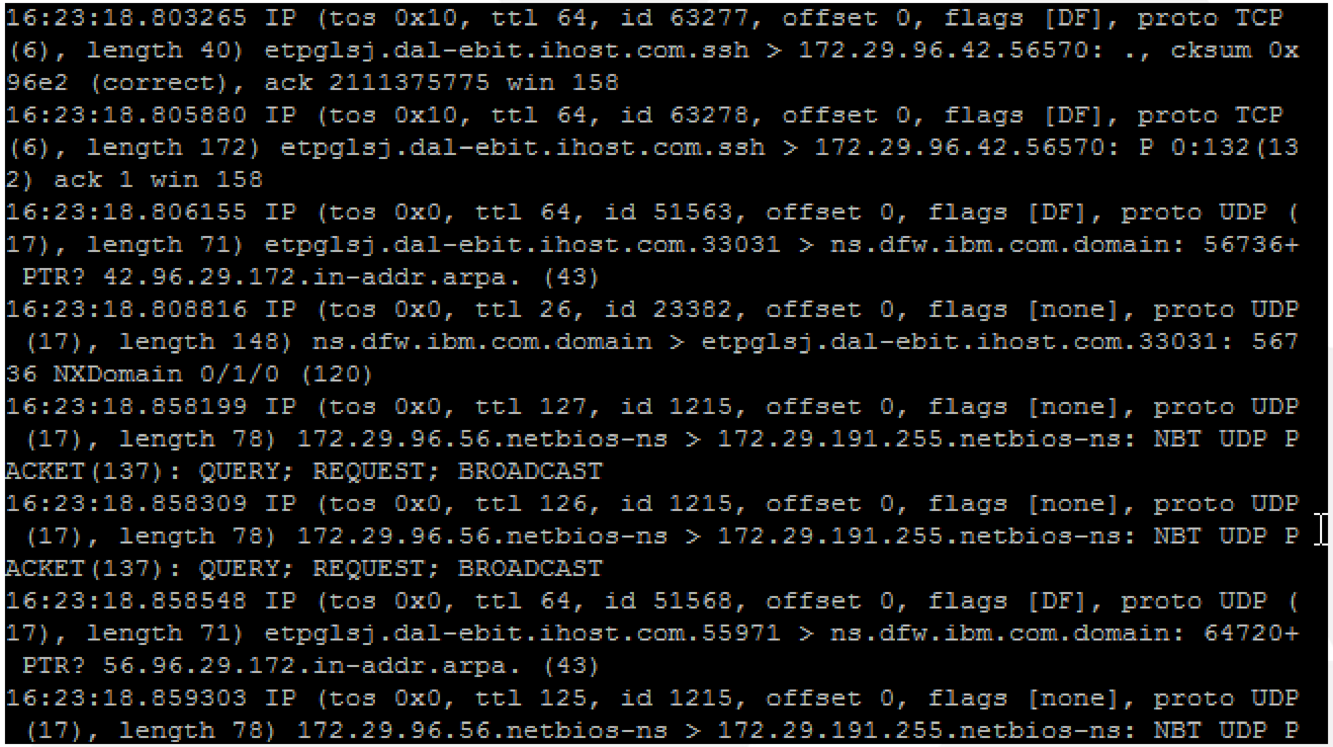
- Specify FULL or ABBREV={length | 224 } for the amount of data to be traced.
- ABBREV allows a value up to 64K, why the maximum value is reset to 480?
- “An OSA might limit the amount of data that is actually traced.”
  - To conserve the OSA trace buffer space
  - ABBREV value is rounded up to the next 32-byte multiple with a maximum of 480
- To circumvent this limitation, start Packet Trace at the same time.

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Linux, Unix and AIX: tcpdump (Windows: windump)

- Requires root authority; use the “su” command first
- Output is formatted trace (default) or written to a pcap file
- tcpdump -w *xyz.pcap* -s 0 [-i any …]
- tcpdump –D : shows a list of available interfaces
- tcpdump -v (sample output from SLES 11 on System z)



```
16:23:18.803265 IP (tos 0x10, ttl 64, id 63277, offset 0, flags [DF], proto TCP
(6), length 40) etpglsj.dal-ebit.ihost.com.ssh > 172.29.96.42.56570: ., cksum 0x
96e2 (correct), ack 2111375775 win 158
16:23:18.805880 IP (tos 0x10, ttl 64, id 63278, offset 0, flags [DF], proto TCP
(6), length 172) etpglsj.dal-ebit.ihost.com.ssh > 172.29.96.42.56570: P 0:132(13
2) ack 1 win 158
16:23:18.806155 IP (tos 0x0, ttl 64, id 51563, offset 0, flags [DF], proto UDP (
17), length 71) etpglsj.dal-ebit.ihost.com.33031 > ns.dfw.ibm.com.domain: 56736+
 PTR? 42.96.29.172.in-addr.arpa. (43)
16:23:18.808816 IP (tos 0x0, ttl 26, id 23382, offset 0, flags [none], proto UDP
 (17), length 148) ns.dfw.ibm.com.domain > etpglsj.dal-ebit.ihost.com.33031: 567
36 NXDomain 0/1/0 (120)
16:23:18.858199 IP (tos 0x0, ttl 127, id 1215, offset 0, flags [none], proto UDP
 (17), length 78) 172.29.96.56.netbios-ns > 172.29.191.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
16:23:18.858309 IP (tos 0x0, ttl 126, id 1215, offset 0, flags [none], proto UDP
 (17), length 78) 172.29.96.56.netbios-ns > 172.29.191.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
16:23:18.858548 IP (tos 0x0, ttl 64, id 51568, offset 0, flags [DF], proto UDP (
17), length 71) etpglsj.dal-ebit.ihost.com.55971 > ns.dfw.ibm.com.domain: 64720+
 PTR? 56.96.29.172.in-addr.arpa. (43)
16:23:18.859303 IP (tos 0x0, ttl 125, id 1215, offset 0, flags [none], proto UDP
 (17), length 78) 172.29.96.56.netbios-ns > 172.29.191.255.netbios-ns: NBT UDP P
```

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**

References

http://www.tcpipguide.com/index.htm
http://www.firewall.cx/networking-topics/65-tcp-protocol-analysis/138-tcp-options.html
http://packetlife.net/captures/
https://wiki.wireshark.org/Presentations

Copyright © 2017 Applied Expert Systems, Inc.

Copyright© 2017 by SHARE Inc. Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. **http://creativecommons.org/licenses/by-nc-nd/3.0/**