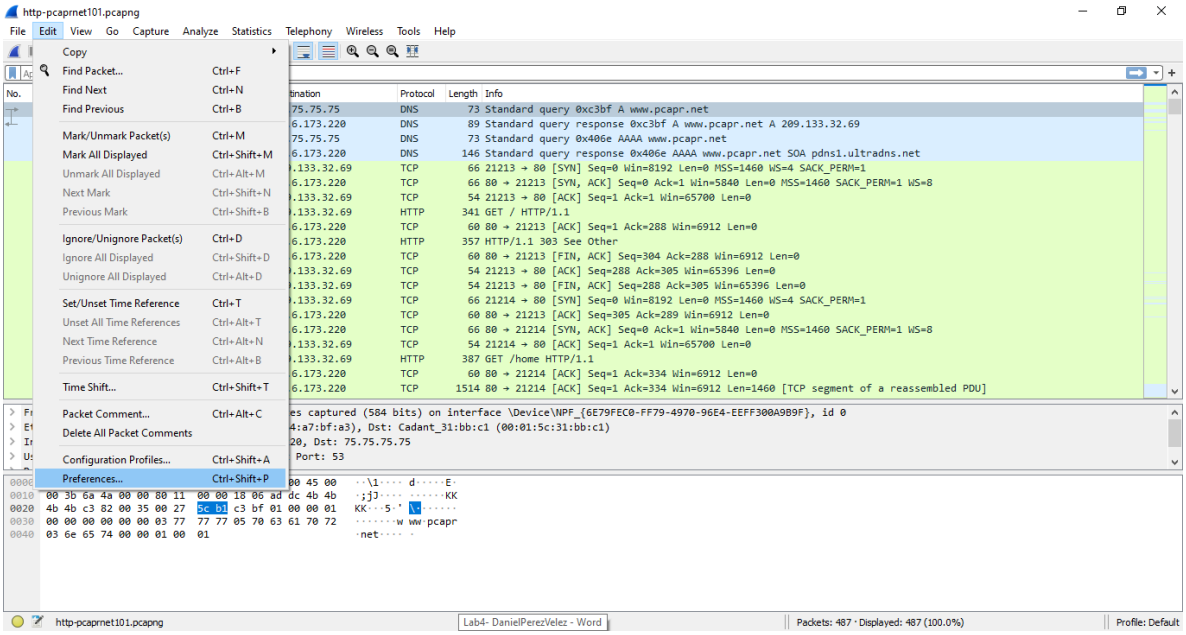
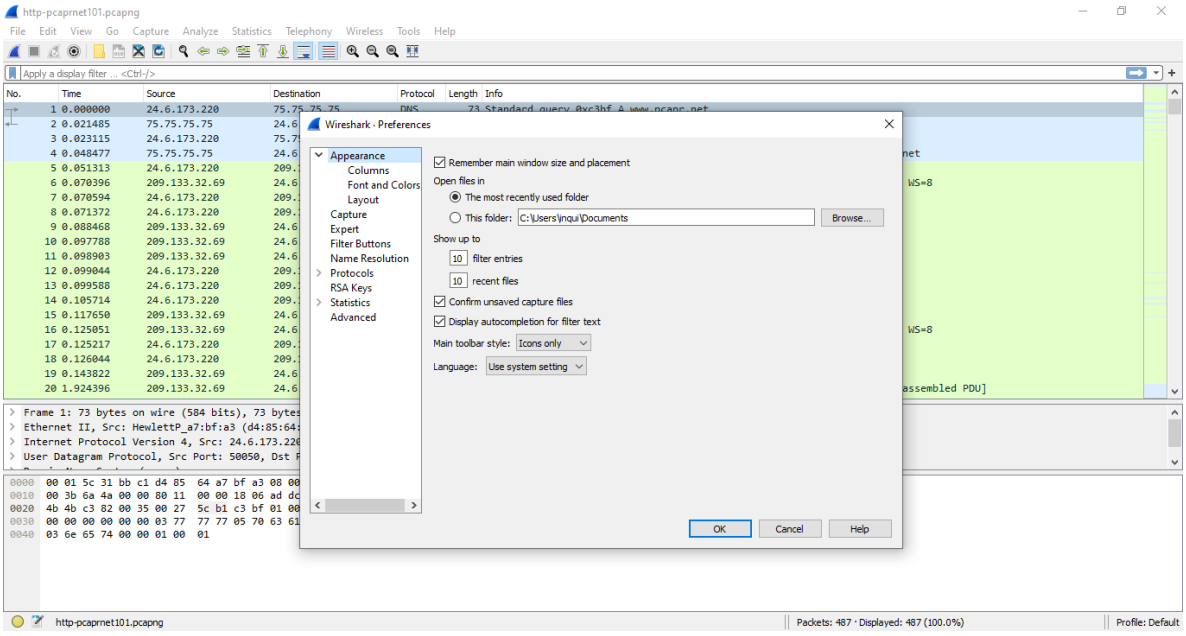
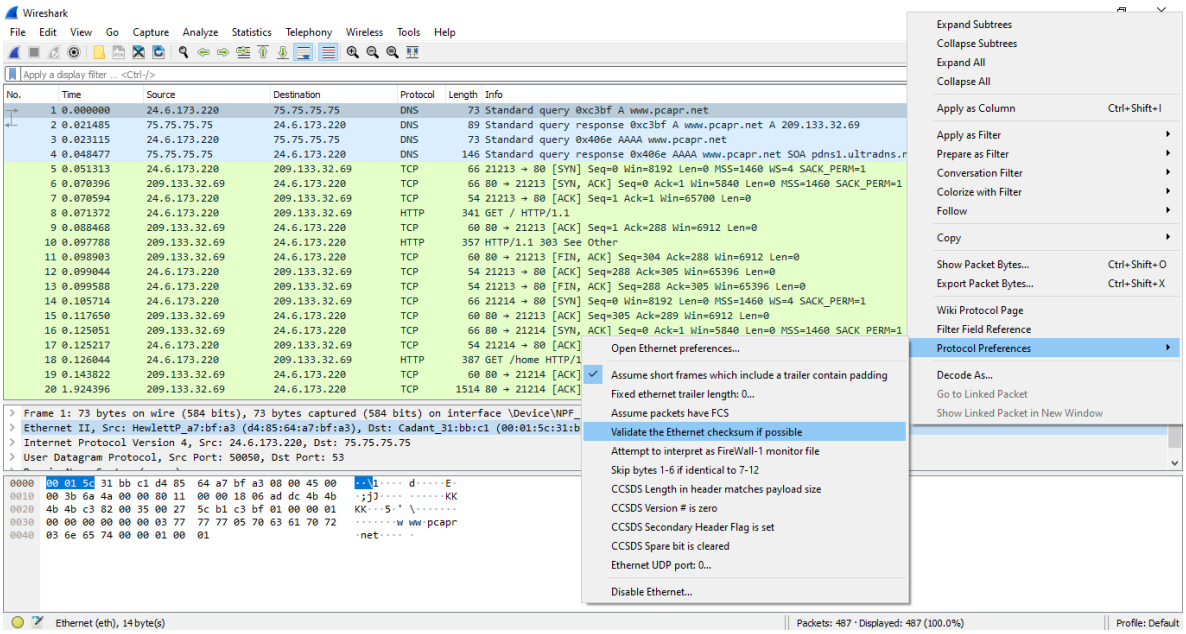
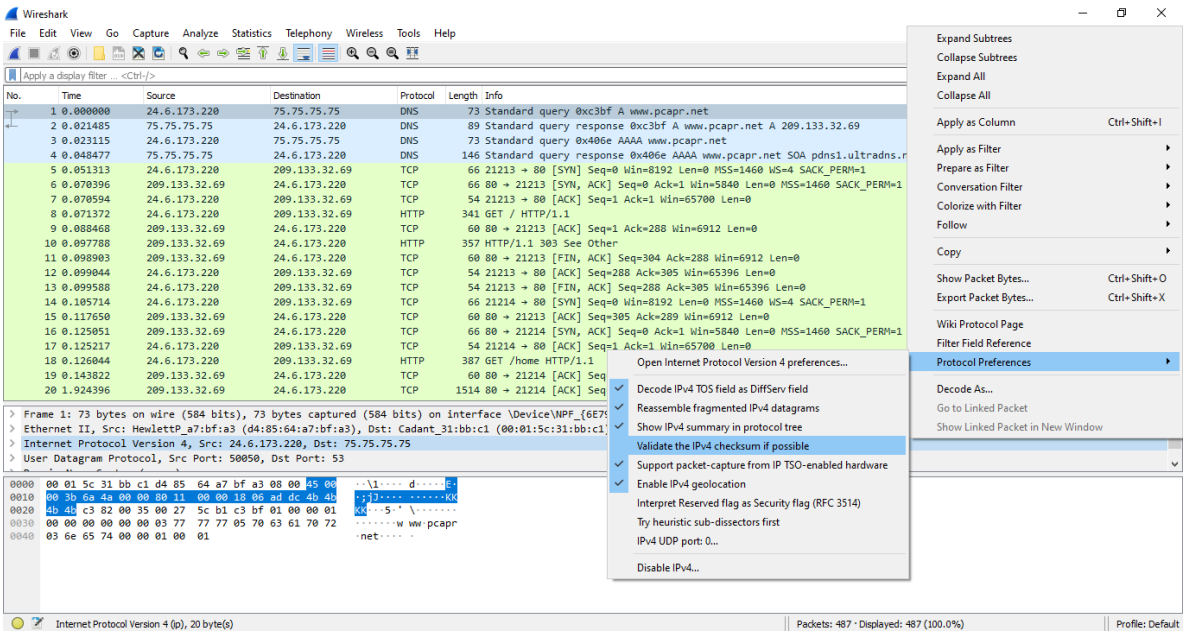
Laboratorio 5
Wireshark

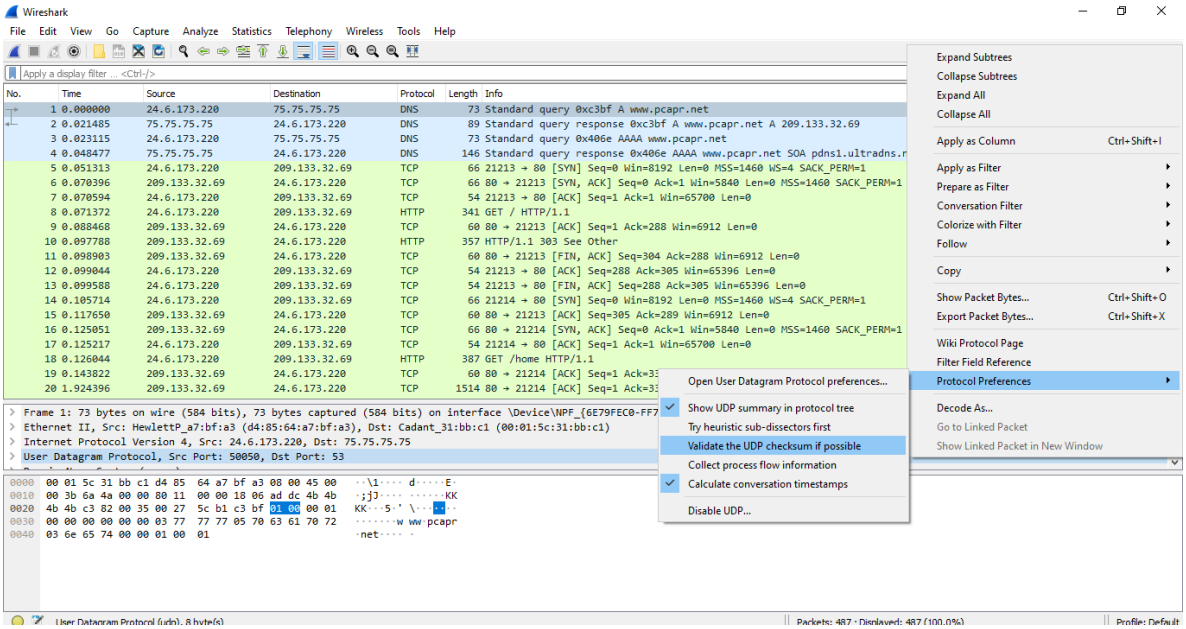
Wilmer Rodríguez Jiménez
Fundamentos de telecomunicaciones
Prof: Ismael Jimenez Sanchez
Periodo Ago – Dic

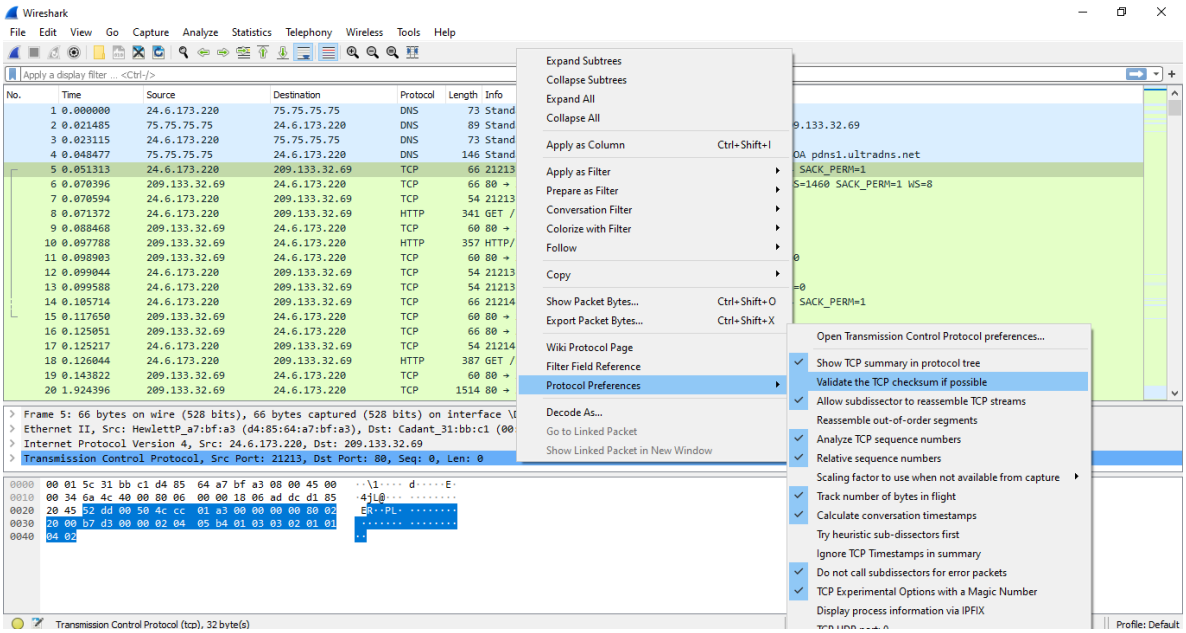

http-pcaprnet101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet(s) Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet(s) Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
Lab4- DanielPerezVelez - Word
Packets: 487 · Displayed: 487 (100.0%)
Profile: Default

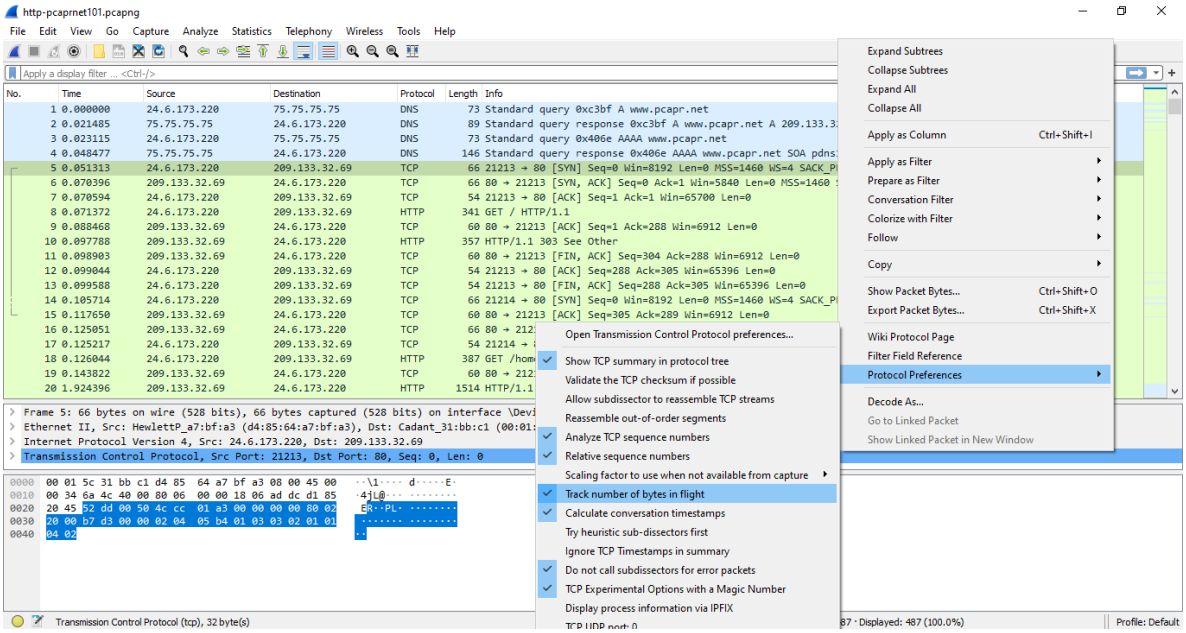

http-pcaprnet101.pcapng
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Remember main window size and placement
Open files in
The most recently used folder
This folder: C:\Users\inqui\Documents
Browse...
Show up to
10 filter entries
10 recent files
Confirm unsaved capture files
Display autocompletion for filter text
Main toolbar style: Icons only
Language: Use system setting
OK
Cancel
Help
Packets: 487 · Displayed: 487 (100.0%)
Profile: Default


Wireshark
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Open Ethernet preferences...
Assume short frames which include a trailer contain padding
Fixed ethernet trailer length: 0...
Assume packets have FCS
Validate the Ethernet checksum if possible
Attempt to interpret as FireWall-1 monitor file
Skip bytes 1-6 if identical to 7-12
CCSDS Length in header matches payload size
CCSDS Version # is zero
CCSDS Secondary Header Flag is set
CCSDS Spare bit is cleared
Ethernet UDP port: 0...
Disable Ethernet...
Ethernet (eth), 14 byte(s)
Packets: 487 · Displayed: 487 (100.0%)
Profile: Default


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 24.6.173.220 75.75.75.75 DNS 73 Standard query 0xc3bf A www.pcapr.net
2 0.021485 75.75.75.75 24.6.173.220 DNS 89 Standard query response 0xc3bf A www.pcapr.net A 209.133.32.69
3 0.023115 24.6.173.220 75.75.75.75 DNS 73 Standard query 0x406e AAAA www.pcapr.net
4 0.048477 75.75.75.75 24.6.173.220 DNS 146 Standard query response 0x406e AAAA www.pcapr.net SOA pdns1.ultradns.r
5 0.051313 24.6.173.220 209.133.32.69 TCP 66 21213 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6 0.070396 209.133.32.69 24.6.173.220 TCP 66 80 → 21213 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
7 0.070594 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8 0.071372 24.6.173.220 209.133.32.69 HTTP 341 GET / HTTP/1.1
9 0.088468 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [ACK] Seq=1 Ack=288 Win=6912 Len=0
10 0.097788 209.133.32.69 24.6.173.220 HTTP 357 HTTP/1.1 303 See Other
11 0.098903 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [FIN, ACK] Seq=304 Ack=288 Win=6912 Len=0
12 0.099044 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [ACK] Seq=288 Ack=305 Win=65396 Len=0
13 0.099588 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [FIN, ACK] Seq=288 Ack=305 Win=65396 Len=0
14 0.105714 24.6.173.220 209.133.32.69 TCP 66 21214 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15 0.117650 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [ACK] Seq=305 Ack=289 Win=6912 Len=0
16 0.125051 209.133.32.69 24.6.173.220 TCP 66 80 → 21214 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17 0.125217 24.6.173.220 209.133.32.69 TCP 54 21214 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
18 0.126044 24.6.173.220 209.133.32.69 HTTP 387 GET /home HTTP/1.1
19 0.143822 209.133.32.69 24.6.173.220 TCP 60 80 → 21214 [ACK] Seq
20 1.924396 209.133.32.69 24.6.173.220 TCP 1514 80 → 21214 [ACK] Seq
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{6E7
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 50050, Dst Port: 53
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 3b 6a 4a 00 00 80 11 00 00 18 06 ad dc 4b 4b
0020 4b 4b c3 82 00 35 00 27 5c b1 c3 bf 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 05 70 63 61 70 72
0040 03 6e 65 74 00 00 01 00 01
Internet Protocol Version 4 (ip), 20 byte(s)
Packets: 487 · Displayed: 487 (100.0%)
Profile: Default
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Open Internet Protocol Version 4 preferences...
Decode IPv4 TOS field as DiffServ field
Reassemble fragmented IPv4 datagrams
Show IPv4 summary in protocol tree
Validate the IPv4 checksum if possible
Support packet-capture from IP TSO-enabled hardware
Enable IPv4 geolocation
Interpret Reserved flag as Security flag (RFC 3514)
Try heuristic sub-dissectors first
IPv4 UDP port: 0...
Disable IPv4...


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 24.6.173.220 75.75.75.75 DNS 73 Standard query 0xc3bf A www.pcapr.net
2 0.021485 75.75.75.75 24.6.173.220 DNS 89 Standard query response 0xc3bf A www.pcapr.net A 209.133.32.69
3 0.023115 24.6.173.220 75.75.75.75 DNS 73 Standard query 0x406e AAAA www.pcapr.net
4 0.048477 75.75.75.75 24.6.173.220 DNS 146 Standard query response 0x406e AAAA www.pcapr.net SOA pdns1.ultradns.r
5 0.051313 24.6.173.220 209.133.32.69 TCP 66 21213 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6 0.070396 209.133.32.69 24.6.173.220 TCP 66 80 → 21213 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
7 0.070594 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8 0.071372 24.6.173.220 209.133.32.69 HTTP 341 GET / HTTP/1.1
9 0.088468 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [ACK] Seq=1 Ack=288 Win=6912 Len=0
10 0.097788 209.133.32.69 24.6.173.220 HTTP 357 HTTP/1.1 303 See Other
11 0.098903 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [FIN, ACK] Seq=304 Ack=288 Win=6912 Len=0
12 0.099044 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [ACK] Seq=288 Ack=305 Win=65396 Len=0
13 0.099588 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [FIN, ACK] Seq=288 Ack=305 Win=65396 Len=0
14 0.105714 24.6.173.220 209.133.32.69 TCP 66 21214 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15 0.117650 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [ACK] Seq=305 Ack=289 Win=6912 Len=0
16 0.125051 209.133.32.69 24.6.173.220 TCP 66 80 → 21214 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
17 0.125217 24.6.173.220 209.133.32.69 TCP 54 21214 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
18 0.126044 24.6.173.220 209.133.32.69 HTTP 387 GET /home HTTP/1.1
19 0.143822 209.133.32.69 24.6.173.220 TCP 60 80 → 21214 [ACK] Seq=1 Ack=33
20 1.924396 209.133.32.69 24.6.173.220 TCP 1514 80 → 21214 [ACK] Seq=1 Ack=33
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{6E79FEC0-FF7
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 50050, Dst Port: 53
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 3b 6a 4a 00 00 80 11 00 00 18 06 ad dc 4b 4b
0020 4b 4b c3 82 00 35 00 27 5c b1 c3 bf 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 05 70 63 61 70 72
0040 03 6e 65 74 00 00 01 00 01
User Datagram Protocol (udp), 8 byte(s)
Packets: 487 · Displayed: 487 (100.0%)
Profile: Default
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Open User Datagram Protocol preferences...
Show UDP summary in protocol tree
Try heuristic sub-dissectors first
Validate the UDP checksum if possible
Collect process flow information
Calculate conversation timestamps
Disable UDP...


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \D
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69
Transmission Control Protocol, Src Port: 21213, Dst Port: 80, Seq: 0, Len: 0
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 34 6a 4c 40 00 80 06 00 00 18 06 ad dc d1 85
0020 20 45 52 dd 00 50 4c cc 01 a3 00 00 00 00 80 02
0030 20 00 b7 d3 00 00 02 04 05 b4 01 03 03 02 01 01
0040 04 02
Transmission Control Protocol (tcp), 32 byte(s)
Profile: Default
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Open Transmission Control Protocol preferences...
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
Analyze TCP sequence numbers
Relative sequence numbers
Scaling factor to use when not available from capture
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
TCP Experimental Options with a Magic Number
Display process information via IPFIX


http-pcaprnet101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 24.6.173.220 75.75.75.75 DNS 73 Standard query 0xc3bf A www.pcapr.net
2 0.021485 75.75.75.75 24.6.173.220 DNS 89 Standard query response 0xc3bf A www.pcapr.net A 209.133.3
3 0.023115 24.6.173.220 75.75.75.75 DNS 73 Standard query 0x406e AAAA www.pcapr.net
4 0.048477 75.75.75.75 24.6.173.220 DNS 146 Standard query response 0x406e AAAA www.pcapr.net SOA pdns
5 0.051313 24.6.173.220 209.133.32.69 TCP 66 21213 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_P
6 0.070396 209.133.32.69 24.6.173.220 TCP 66 80 → 21213 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
7 0.070594 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8 0.071372 24.6.173.220 209.133.32.69 HTTP 341 GET / HTTP/1.1
9 0.088468 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [ACK] Seq=1 Ack=288 Win=6912 Len=0
10 0.097788 209.133.32.69 24.6.173.220 HTTP 357 HTTP/1.1 303 See Other
11 0.098903 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [FIN, ACK] Seq=304 Ack=288 Win=6912 Len=0
12 0.099044 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [ACK] Seq=288 Ack=305 Win=65396 Len=0
13 0.099588 24.6.173.220 209.133.32.69 TCP 54 21213 → 80 [FIN, ACK] Seq=288 Ack=305 Win=65396 Len=0
14 0.105714 24.6.173.220 209.133.32.69 TCP 66 21214 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_P
15 0.117650 209.133.32.69 24.6.173.220 TCP 60 80 → 21213 [ACK] Seq=305 Ack=289 Win=6912 Len=0
16 0.125051 209.133.32.69 24.6.173.220 TCP 66 80 → 212
17 0.125217 24.6.173.220 209.133.32.69 TCP 54 21214 →
18 0.126044 24.6.173.220 209.133.32.69 HTTP 387 GET /hom
19 0.143822 209.133.32.69 24.6.173.220 TCP 60 80 → 212
20 1.924396 209.133.32.69 24.6.173.220 HTTP 1514 HTTP/1.1
Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devi
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.133.32.69
Transmission Control Protocol, Src Port: 21213, Dst Port: 80, Seq: 0, Len: 0
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 34 6a 4c 40 00 80 06 00 00 18 06 ad dc d1 85
0020 20 45 52 dd 00 50 4c cc 01 a3 00 00 00 00 80 02
0030 20 00 b7 d3 00 00 02 04 05 b4 01 03 03 02 01 01
0040 04 02
Transmission Control Protocol (tcp), 32 byte(s)
87 · Displayed: 487 (100.0%)
Profile: Default
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Open Transmission Control Protocol preferences...
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
Analyze TCP sequence numbers
Relative sequence numbers
Scaling factor to use when not available from capture
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
TCP Experimental Options with a Magic Number
Display process information via IPFIX