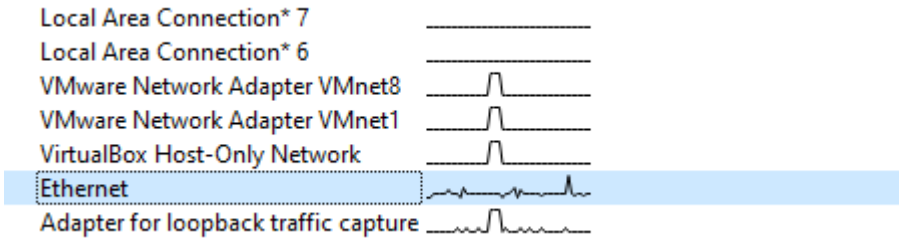
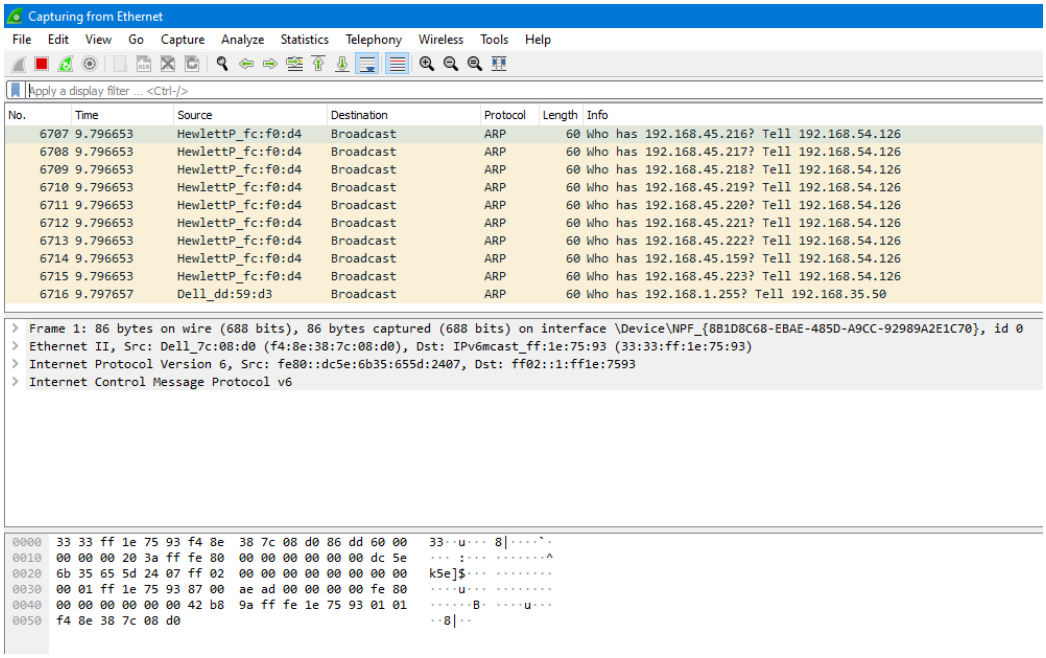
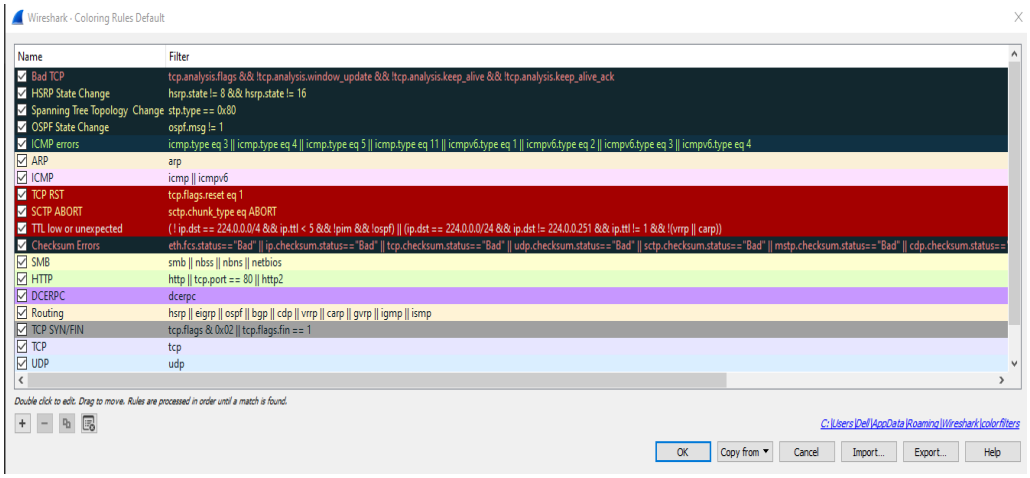
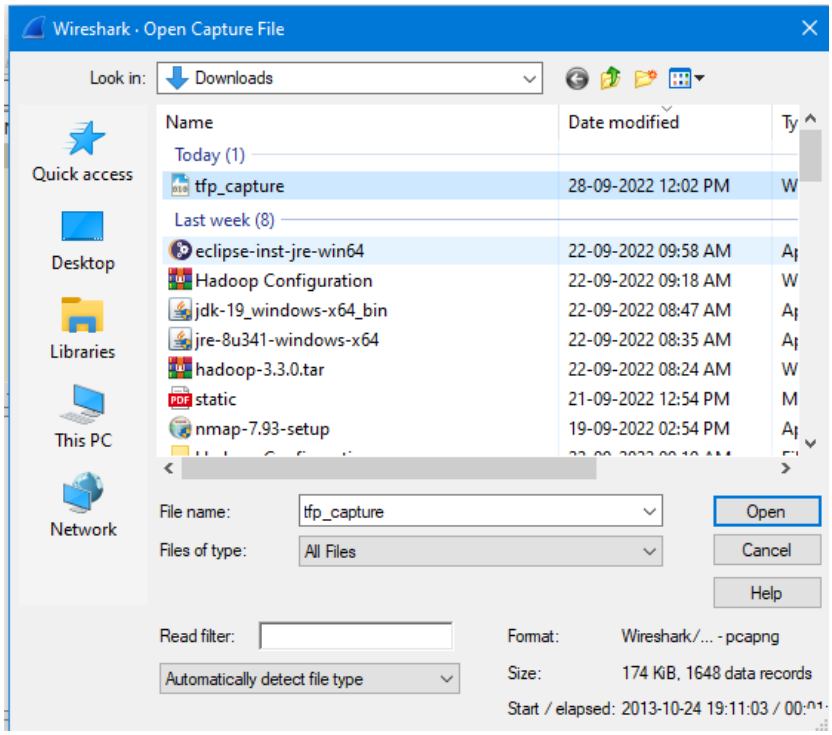
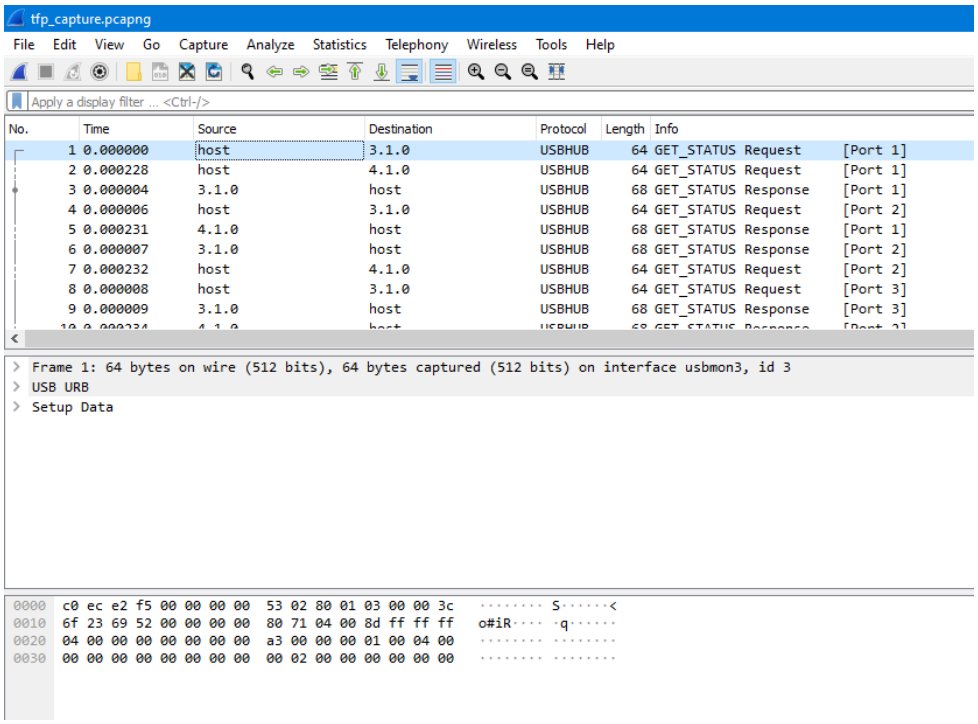
EXPERIMENT NO.6

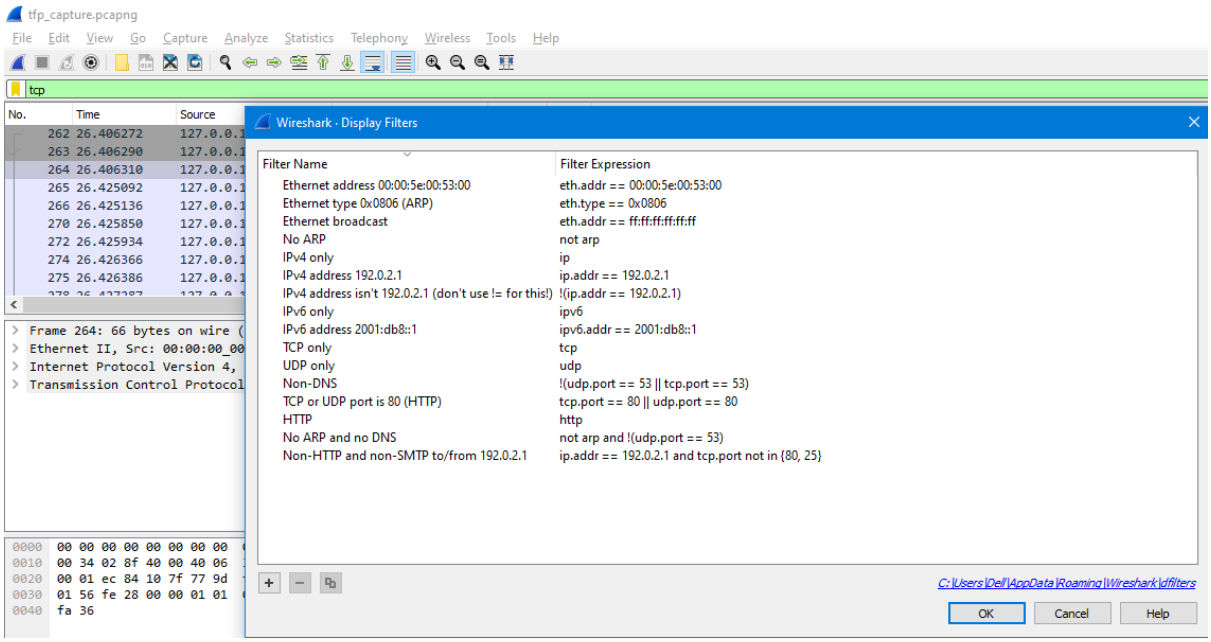


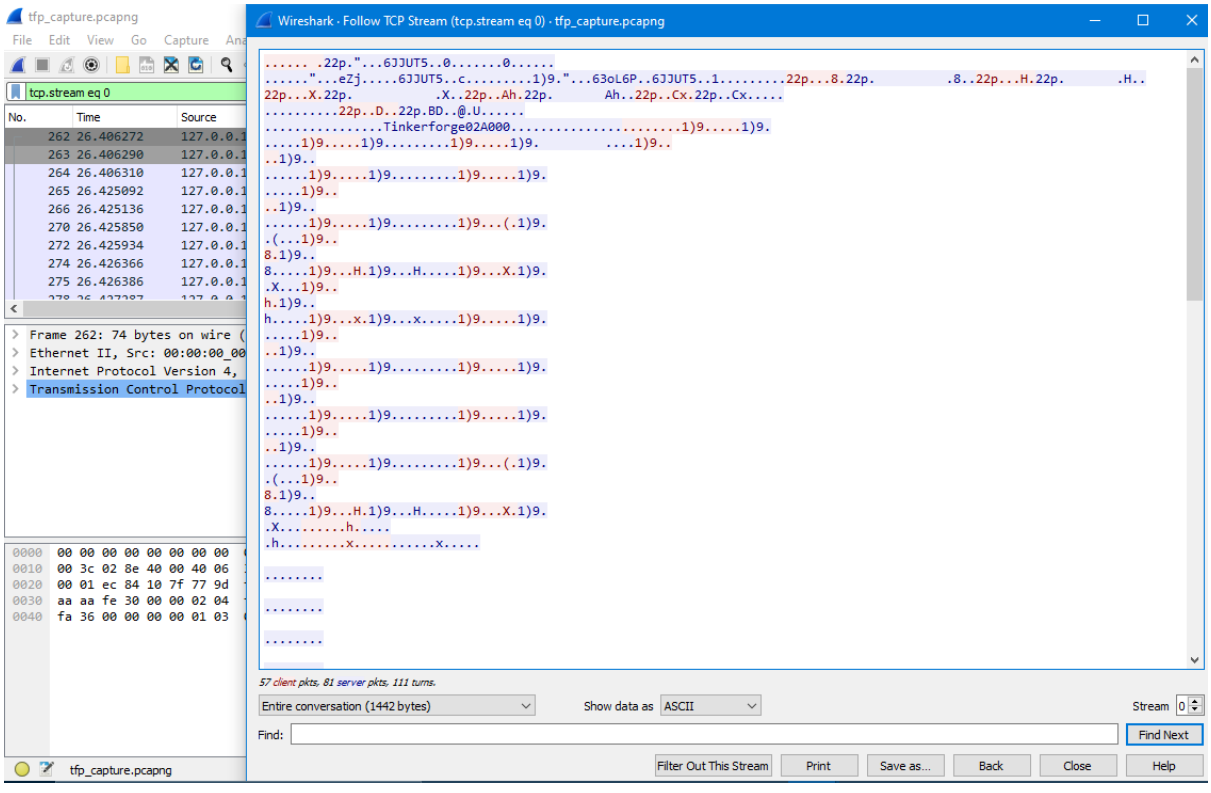


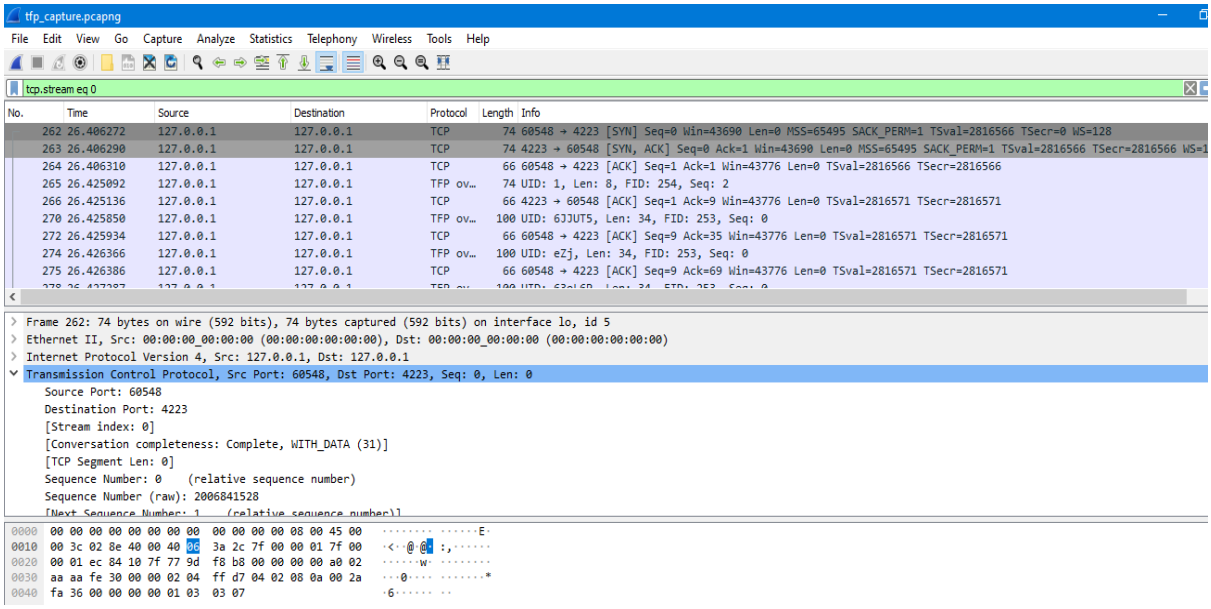



Wireshark · Open Capture File
Look in:
Downloads
Quick access
Desktop
Libraries
This PC
Network
Name
Date modified
Today (1)
tfp_capture
28-09-2022 12:02 PM
Last week (8)
eclipse-inst-jre-win64
22-09-2022 09:58 AM
Hadoop Configuration
22-09-2022 09:18 AM
jdk-19_windows-x64_bin
22-09-2022 08:47 AM
jre-8u341-windows-x64
22-09-2022 08:35 AM
hadoop-3.3.0.tar
22-09-2022 08:24 AM
static
21-09-2022 12:54 PM
nmap-7.93-setup
19-09-2022 02:54 PM
File name:
tfp_capture
Files of type:
All Files
Open
Cancel
Help
Read filter:
Automatically detect file type
Format:
Wireshark/... - pcapng
Size:
174 KiB, 1648 data records
Start / elapsed:
2013-10-24 19:11:03 / 00:


tfp_capture.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 host 3.1.0 USBHUB 64 GET_STATUS Request [Port 1]
2 0.000228 host 4.1.0 USBHUB 64 GET_STATUS Request [Port 1]
3 0.000004 3.1.0 host USBHUB 68 GET_STATUS Response [Port 1]
4 0.000006 host 3.1.0 USBHUB 64 GET_STATUS Request [Port 2]
5 0.000231 4.1.0 host USBHUB 68 GET_STATUS Response [Port 1]
6 0.000007 3.1.0 host USBHUB 68 GET_STATUS Response [Port 2]
7 0.000232 host 4.1.0 USBHUB 64 GET_STATUS Request [Port 2]
8 0.000008 host 3.1.0 USBHUB 64 GET_STATUS Request [Port 3]
9 0.000009 3.1.0 host USBHUB 68 GET_STATUS Response [Port 3]
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface usbmon3, id 3
USB URB
Setup Data
0000 c0 ec e2 f5 00 00 00 00 53 02 80 01 03 00 00 3c
0010 6f 23 69 52 00 00 00 00 80 71 04 00 8d ff ff ff
0020 04 00 00 00 00 00 00 00 a3 00 00 00 01 00 04 00
0030 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00


tfp_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source
262 26.406272 127.0.0.1
263 26.406290 127.0.0.1
264 26.406310 127.0.0.1
265 26.425092 127.0.0.1
266 26.425136 127.0.0.1
270 26.425850 127.0.0.1
272 26.425934 127.0.0.1
274 26.426366 127.0.0.1
275 26.426386 127.0.0.1
Frame 264: 66 bytes on wire (
Ethernet II, Src: 00:00:00_00
Internet Protocol Version 4,
Transmission Control Protocol
0000 00 00 00 00 00 00 00 00
0010 00 34 02 8f 40 00 40 06
0020 00 01 ec 84 10 7f 77 9d
0030 01 56 fe 28 00 00 01 01
0040 fa 36
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00 eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP) eth.type == 0x0806
Ethernet broadcast eth.addr == ff:ff:ff:ff:ff:ff
No ARP not arp
IPv4 only ip
IPv4 address 192.0.2.1 ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!) !(ip.addr == 192.0.2.1)
IPv6 only ipv6
IPv6 address 2001:db8::1 ipv6.addr == 2001:db8::1
TCP only tcp
UDP only udp
Non-DNS !(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP) tcp.port == 80 || udp.port == 80
HTTP http
No ARP and no DNS not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1 ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
C:\Users\Dell\AppData\Roaming\Wireshark\dfilters
OK Cancel Help


tfp_capture.pcapng
tcp.stream eq 0
No. Time Source
262 26.406272 127.0.0.1
263 26.406290 127.0.0.1
264 26.406310 127.0.0.1
265 26.425092 127.0.0.1
266 26.425136 127.0.0.1
270 26.425850 127.0.0.1
272 26.425934 127.0.0.1
274 26.426366 127.0.0.1
275 26.426386 127.0.0.1
Frame 262: 74 bytes on wire (
Ethernet II, Src: 00:00:00_00
Internet Protocol Version 4,
Transmission Control Protocol
0000 00 00 00 00 00 00 00 00
0010 00 3c 02 8e 40 00 40 06
0020 00 01 ec 84 10 7f 77 9d
0030 aa aa fe 30 00 00 02 04
0040 fa 36 00 00 00 00 01 03
tfp_capture.pcapng
Wireshark · Follow TCP Stream (tcp.stream eq 0) · tfp_capture.pcapng
..... .22p."...6JJUT5..0.....0.....
....."...eZj.....6JJUT5..c.....1)9."...63oL6P..6JJUT5..1.....22p...8.22p. .8..22p...H.22p. .H..
22p...X.22p. .X..22p..Ah.22p. Ah..22p..Cx.22p..Cx.....
.....22p..D..22p.BD..@.U.....
.....Tinkerforge02A000.....1)9....1)9.
.....1)9.....1)9.....1)9.....1)9. ....1)9..
..1)9..
.....1)9.....1)9.....1)9.....1)9.
.....1)9..
..1)9..
.....1)9.....1)9.....1)9...(.1)9.
.(...1)9..
8.1)9..
8.....1)9...H.1)9...H.....1)9...X.1)9.
.X...1)9..
h.1)9..
h.....1)9...x.1)9...x.....1)9.....1)9.
.....1)9..
..1)9..
.....1)9.....1)9.....1)9.....1)9.
.....1)9..
..1)9..
.....1)9.....1)9.....1)9.....1)9.
.....1)9..
..1)9..
.....1)9.....1)9.....1)9...(.1)9.
.(...1)9..
8.1)9..
8.....1)9...H.1)9...H.....1)9...X.1)9.
.X.....h.....
.h.....x.....x.....
.....
.....
.....
57 client pkts, 81 server pkts, 111 turns.
Entire conversation (1442 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream Print Save as... Back Close Help


tfp_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
262 26.406272 127.0.0.1 127.0.0.1 TCP 74 60548 → 4223 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=2816566 TSecr=0 WS=128
263 26.406290 127.0.0.1 127.0.0.1 TCP 74 4223 → 60548 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=2816566 TSecr=2816566 WS=1
264 26.406310 127.0.0.1 127.0.0.1 TCP 66 60548 → 4223 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=2816566 TSecr=2816566
265 26.425092 127.0.0.1 127.0.0.1 TFP ov… 74 UID: 1, Len: 8, FID: 254, Seq: 2
266 26.425136 127.0.0.1 127.0.0.1 TCP 66 4223 → 60548 [ACK] Seq=1 Ack=9 Win=43776 Len=0 TSval=2816571 TSecr=2816571
270 26.425850 127.0.0.1 127.0.0.1 TFP ov… 100 UID: 6JJUT5, Len: 34, FID: 253, Seq: 0
272 26.425934 127.0.0.1 127.0.0.1 TCP 66 60548 → 4223 [ACK] Seq=9 Ack=35 Win=43776 Len=0 TSval=2816571 TSecr=2816571
274 26.426366 127.0.0.1 127.0.0.1 TFP ov… 100 UID: eZj, Len: 34, FID: 253, Seq: 0
275 26.426386 127.0.0.1 127.0.0.1 TCP 66 60548 → 4223 [ACK] Seq=9 Ack=69 Win=43776 Len=0 TSval=2816571 TSecr=2816571
Frame 262: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 5
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 60548, Dst Port: 4223, Seq: 0, Len: 0
Source Port: 60548
Destination Port: 4223
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2006841528
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 3c 02 8e 40 00 40 06 3a 2c 7f 00 00 01 7f 00
0020 00 01 ec 84 10 7f 77 9d f8 b8 00 00 00 00 a0 02
0030 aa aa fe 30 00 00 02 04 ff d7 04 02 08 0a 00 2a
0040 fa 36 00 00 00 00 01 03 03 07