



Zachodniopomorski
Uniwersytet Technologiczny
w Szczecinie

Network Systems Administration

Report 4 - Analysis of TCP packages with Wireshark

dr inż. Piotr Lech

Abdurrahman Karaoluk

ka46312

Method : "www.zut.edu.pl" address was visited on the virtual machine. The packet traffic generated was analyzed with Wireshark.

Q1- What are IP address and TCP port number used by the client computer (source) and destination address with visit to “www.zut.edu.pl” ?

A1-

	Source	Destination
IP	192.168.127.136	212.14.18.124
Port Number	49074	80

Ss1-

The screenshot displays a Fedora 18 virtual machine environment. On the left, a web browser window shows the homepage of Zachodniopomorski Uniwersytet Techniczny w Szczecinie. Below the browser, a terminal window shows the output of the 'ifconfig' command for the 'eth0' interface, indicating it is up and running with IP 192.168.127.136. On the right, the Wireshark network traffic analyzer is open, showing a list of captured packets. The selected packet (No. 31) is a TCP segment from 192.168.127.136 to 212.14.18.124 on port 80. The packet details pane shows the source IP as 192.168.127.136 and the destination IP as 212.14.18.124. The packet bytes pane shows the raw data of the TCP segment.

Q2-What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

A2- The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and “www.zut.edu.pl”. According to the screenshot below, in the Flags section, the SYN flag is set to 1 which indicates that this segment is a SYN segment.

Ss2-

The screenshot displays a network security toolkit interface with three main windows:

- Browser Window:** Shows the website of Zachodniopomorski Uniwersytet Techniczny w Szczecinie.
- Terminal Window:** Shows the output of the `ifconfig` command for the `eth0` interface, indicating it is up and running with IP `192.168.127.136`.
- Network Security Toolkit Window:** Displays a list of network packets. The selected packet is a TCP SYN segment from `192.168.127.136` to `192.168.127.136` (localhost) with sequence number `0` and the SYN flag set.

The detailed view of the selected packet shows the following information:

- Source:** 192.168.127.136
- Destination:** 192.168.127.136
- Protocol:** TCP
- Flags:** SYN
- Sequence number:** 0
- Window size:** 64240
- Checksum:** 0x26ea (incorrect, should be 0x08f0)

Q3- What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did “www.zut.edu.pl” determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

A3- The sequence number of the SYN_ACK segment sent by “www.zut.edu.pl” to the client computer in reply to the SYN is 0. The value of the acknowledgement field in the SYN_ACK segment is determined by the server “www.zut.edu.pl” The server adds 1 to the initial sequence number of the SYN segment from the client computer. For this case, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the acknowledgement field in the SYN_ACK segment is 1. A segment will be identified as a SYN_ACK segment if both SYN flag and ACKnowledgement flag in the segment are set to 1.

Ss3-

The screenshot displays a network security toolkit interface with three main windows:

- Packet List:** Shows a list of captured packets. Packet 25 is highlighted, showing it is a TCP segment from 192.168.127.136 to 192.168.127.136, with sequence number 49074 and acknowledgment number 0.
- Packet Details:** Provides a detailed view of the selected packet. It shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The TCP header fields are expanded, showing the sequence number (49074), acknowledgment number (0), and the SYN and ACK flags set to 1.
- Terminal:** Displays the output of the `ifconfig` command for the client machine, showing the IP address 192.168.127.136 and the network configuration.

The packet details window shows the following information:

- Frame 25: 68 bytes on wire (488 bits), 68 bytes captured (488 bits)
- Ethernet II, Src: Vmware, F7:8e:62 (00:50:56:f7:8e:62), Dst: Vmware, bd:9e:2f (08:0c:29:bd:9e:2f)
- Internet Protocol Version 4, Src: www.zut.edu.pl (212.14.18.126), Dst: 192.168.127.136 (192.168.127.136)
- Transmission Control Protocol, Src Port: 80, Dst Port: 49074, Seq: 0, Ack: 1, Len: 0
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Flags: SYN, ACK
- Options: (4 bytes), Maximum segment size
- Timestamps

Q4- What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

A4- The sequence number of the TCP segment containing the HTTP Post command is 2.

Ss4-

The screenshot shows a Fedora NET system with a terminal window and a Wireshark packet capture. The terminal window displays the output of the `ifconfig` command for the `ss4` VM, showing network configuration details such as IP address, netmask, and broadcast address. The Wireshark window shows a packet capture of an HTTP POST request. The packet list pane highlights a packet with sequence number 381. The packet details pane shows the TCP segment with sequence number 381 and the HTTP request body containing the word "POST".

```
ifconfig
3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
   inet 192.168.127.136 netmask 255.255.255.0 broadcast 192.168.127.255
   inet6 fe80::31b:7b09:ea78:fcdb prefixlen 64 scopeid 0x20<ll>
   ether 08:0c:29:bd:9e:2f txqueuelen 1000 (Ethernet)
   RX packets 5620 bytes 6922402 (6.6 MiB)
   RX errors 0 dropped 0 overruns 0 frame 0
   TX packets 1935 bytes 194964 (190.4 KiB)
   TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

flags=73<UP,LOOPBACK,RUNNING> mtu 65536
   inet 127.0.0.1 netmask 255.0.0.0
   inet6 ::1 prefixlen 128 scopeid 0x10<host>
   loop txqueuelen 1000 (local loopback)
   RX packets 32 bytes 2020 (1.9 KiB)
   RX errors 0 dropped 0 overruns 0 frame 0
   TX packets 20 bytes 2020 (1.9 KiB)
   TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

localhost ~#
```

Wireshark packet capture details:

```
Sequence number (tcp.seq), 4 bytes
Packets: 933 · Displayed: 1 (0.1%) · Dropped: 0 (0.0%) · Profile: Default
```

Q5- Consider the TCP connection.

Q1- What are the sequence numbers of two segments in the TCP connection?

A1- Sequence number for segment 1 is 1, sequence number for segment 2 is 399.

Q2- At what time was each segment sent?

A2- 9.608997 s for segment 1 and 8.625840 s for segment 2.

Q3- When was the ACK for each segment received?

A3- ACK for segment 1 was received at 9.608997 s and ACK for segment 2 is received at 8.625840 s.

Ss5-

The image shows a Wireshark network packet capture of a TCP connection. The packet list at the top shows several packets, including a GET request (Seq=399) and a 307 Temporary Redirect response (Seq=527). The packet details for the response show the sequence number 399 and acknowledgment number 527. The packet bytes show the raw data of the response.

No.	Time	Source	Destination	Protocol	Info
19	8.190540	192.168.127.136	server-143-204-89-5...	TCP	47774 → 443 [ACK] Seq=1 Ack=1 Win=62780 [TCP CHECKSUM INCORRECT] L...
20	8.191054	server-143-204-89-5...	192.168.127.136	TCP	[TCP ACKed unseen segment] 443 → 47774 [ACK] Seq=1 Ack=2 Win=64240...
25	8.605323	192.168.127.136	www.zut.edu.pl	TCP	49074 → 80 [SYN] Seq=0 Win=64240 [TCP CHECKSUM INCORRECT] Len=0 MS...
26	8.608823	www.zut.edu.pl	192.168.127.136	TCP	80 → 49074 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
27	8.608997	192.168.127.136	www.zut.edu.pl	TCP	49074 → 80 [ACK] Seq=1 Ack=1 Win=64240 [TCP CHECKSUM INCORRECT] Le...
28	8.609904	192.168.127.136	www.zut.edu.pl	HTTP	GET / HTTP/1.1
29	8.610282	www.zut.edu.pl	192.168.127.136	TCP	80 → 49074 [ACK] Seq=1 Ack=399 Win=64240 Len=0
30	8.625799	www.zut.edu.pl	192.168.127.136	HTTP	HTTP/1.1 307 Temporary Redirect (text/html)
31	8.625840	192.168.127.136	www.zut.edu.pl	TCP	49074 → 80 [ACK] Seq=399 Ack=527 Win=63784 [TCP CHECKSUM INCORRECT]...
32	8.658066	192.168.127.136	www.zut.edu.pl	TCP	58866 → 443 [SYN] Seq=0 Win=64240 [TCP CHECKSUM INCORRECT] Len=0 M...

Frame 31: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Vmware_bd:9e:2f (00:0c:29:bd:9e:2f), Dst: Vmware_f7:8e:62 (00:50:56:f7:8e:62)

Internet Protocol Version 4, Src: 192.168.127.136 (192.168.127.136), Dst: www.zut.edu.pl (212.14.18.124)

Transmission Control Protocol, Src Port: 49074, Dst Port: 80, Seq: 399, Ack: 527, Len: 0

Source Port: 49074

Destination Port: 80

[Stream index: 9]

TCP Segment Len: 0

Sequence number: 399 (relative sequence number)

Next sequence number: 399 (relative sequence number)

Acknowledgment number: 527 (relative ack number)

0101 ... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

0000 ... = Reserved: Not set

...0 ... = Nonce: Not set

...0 ... = Congestion Window Reduced (CWR): Not set

...0 ... = ECN-Echo: Not set

...0 ... = Urgent: Not set

...1 ... = Acknowledgment: Set

...0 ... = Push: Not set

0000 00 50 56 f7 8e 62 00 0c 29 bd 9e 2f 08 00 45 00 PV...b...).../...E...

0010 00 28 ca f5 40 00 40 06 49 1f c0 a8 7f 88 d4 0e (...@... I... ..

0020 12 7c bf b2 00 50 5b e9 9a fb 39 db 13 85 50 10 |...P[...9...P...

0030 f9 28 26 d6 00 00 (&...

Sequence number (tcp.seq), 4 bytes

Packets: 933 · Displayed: 917 (98.3%) · Dropped: 0 (0.0%) · Profile: Default

Q6- What is the length of any TCP segment?

A6- The length of TCP segment is 1316 bytes.

Ss6-

The screenshot displays the NetworkMiner interface with the following details:

- Filter:** tcp
- Table:** A list of network packets. The selected packet (No. 43) is a TCP segment from 192.168.127.136 to 192.168.127.136, Seq=5557, Ack=518, Win=64240, Len=1316.
- Details:**
 - Source Port: 443
 - Destination Port: 58866
 - [Stream index: 10]
 - [TCP Segment Len: 1316]
 - Sequence number: 5557 (relative sequence number)
 - [Next sequence number: 6873 (relative sequence number)]
 - Acknowledgment number: 518 (relative ack number)
 - 0101 ... = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 64240
 - [Calculated window size: 64240]
 - [Window size scaling factor: -2 (no window scaling used)]
 - Checksum: 0xdd41 [correct]
 - [Checksum Status: Good]
 - [Calculated Checksum: 0xdd41]
 - Urgent pointer: 0
 - [SEQ/ACK analysis]
 - [Timestamps]
 - TCP payload (1316 bytes)
 - TCP segment data (1316 bytes)
- Payload:** A hex dump of the TCP segment data, starting with 0030 fa f9 dd 41 00 00 3a 02 82 01 01 00 c5 76 0f 0f.
- Status Bar:** A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1316 bytes. Packets: 933 · Displayed: 917 (98.3%) · Dropped: 0 (0.0%) · Profile: Default

Q7- What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

A7- The minimum amount of available buffer space advertised at the received is 6440 bytes.

Ss7-

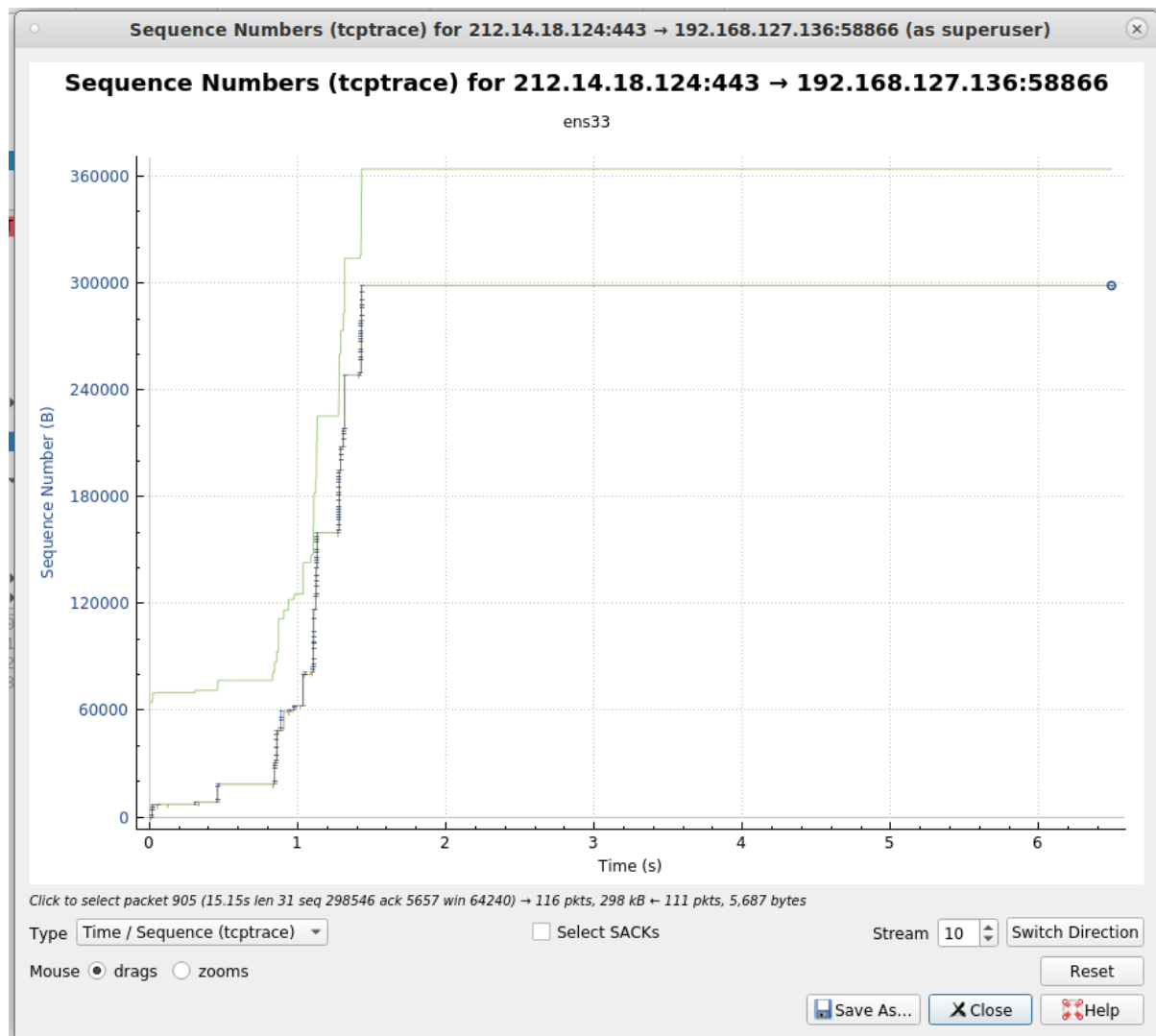
The screenshot displays the NetworkMiner interface with the following details:

- Packet List:** Shows a series of TCP packets. Packet 43 is selected, showing a PSH, ACK segment with Seq=5557, Ack=518, Win=64240, and Len=1316.
- Packet Details:** Provides a breakdown of the selected packet, including source/destination ports, sequence numbers, acknowledgment numbers, and flags. It highlights the "Calculated window size: 64240" and "Window size value: 64240".
- Packet Data:** Displays the raw hex and ASCII data of the packet, which is a GET request for the OCSP response for the certificate igicert.com.
- Status Bar:** Indicates that the scaled window size (if scaling has been used) is 2 bytes, and shows statistics: Packets: 933, Displayed: 917 (98.3%), Dropped: 0 (0.0%), Profile: Default.

Q8- Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

A8- Yes there are retransmitted segments in the trace file. This can be explained by packets with same sequence number at different time is found.

Ss8-



FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Q10- What is the throughput (bytes transferred per unit time) for the TCP connection?
Explain how you calculated this value.

A10-

Throughput = (Amount of data transmitted) / (Time incurred)

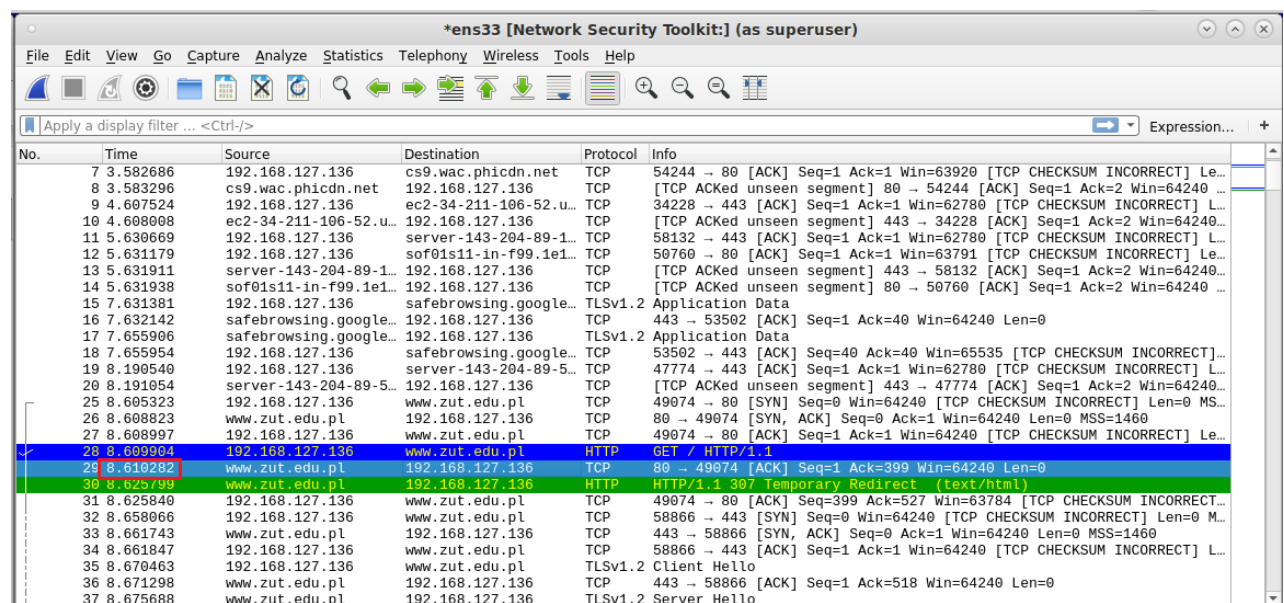
Amount of data transmitted = 326,646 bytes

Time incurred = 17,491128 – 8.610282 = 8.880846

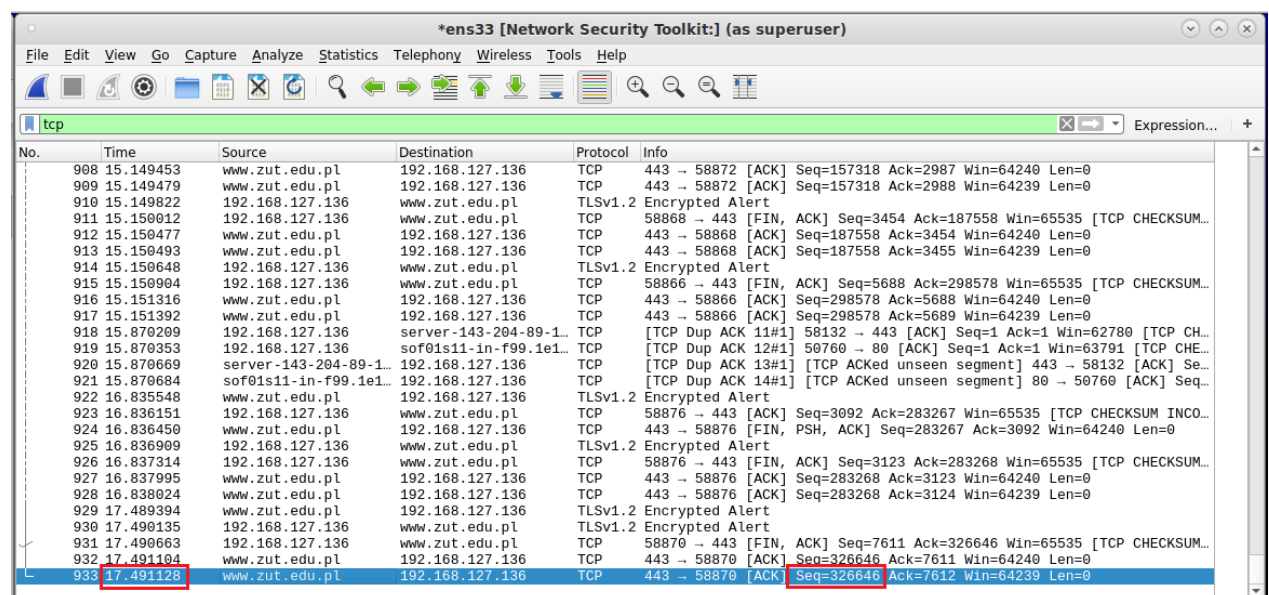
Throughput = 326646 / 8,880846

Throughput = 36.780,9553

Ss10-



No.	Time	Source	Destination	Protocol	Info
7	3.582686	192.168.127.136	cs9.wac.phicdn.net	TCP	54244 → 80 [ACK] Seq=1 Ack=1 Win=63920 [TCP CHECKSUM INCORRECT] Le...
8	3.583296	cs9.wac.phicdn.net	192.168.127.136	TCP	[TCP ACKed unseen segment] 80 → 54244 [ACK] Seq=1 Ack=2 Win=64240 ...
9	4.607524	192.168.127.136	ec2-34-211-106-52.u...	TCP	34228 → 443 [ACK] Seq=1 Ack=1 Win=62780 [TCP CHECKSUM INCORRECT] L...
10	4.608008	ec2-34-211-106-52.u...	192.168.127.136	TCP	[TCP ACKed unseen segment] 443 → 34228 [ACK] Seq=1 Ack=2 Win=64240...
11	5.630669	192.168.127.136	server-143-204-89-1...	TCP	58132 → 443 [ACK] Seq=1 Ack=1 Win=62780 [TCP CHECKSUM INCORRECT] L...
12	5.631179	192.168.127.136	sof01s11-in-f99.1e1...	TCP	50760 → 80 [ACK] Seq=1 Ack=1 Win=63791 [TCP CHECKSUM INCORRECT] Le...
13	5.631911	server-143-204-89-1...	192.168.127.136	TCP	[TCP ACKed unseen segment] 443 → 58132 [ACK] Seq=1 Ack=2 Win=64240 ...
14	5.631938	sof01s11-in-f99.1e1...	192.168.127.136	TCP	[TCP ACKed unseen segment] 80 → 50760 [ACK] Seq=1 Ack=2 Win=64240 ...
15	7.631381	192.168.127.136	safebrowsing.google...	TLSv1.2	Application Data
16	7.632142	safebrowsing.google...	192.168.127.136	TCP	443 → 53502 [ACK] Seq=1 Ack=40 Win=64240 Len=0
17	7.655906	safebrowsing.google...	192.168.127.136	TLSv1.2	Application Data
18	7.655954	192.168.127.136	safebrowsing.google...	TCP	53502 → 443 [ACK] Seq=40 Ack=40 Win=65535 [TCP CHECKSUM INCORRECT]...
19	8.190540	192.168.127.136	server-143-204-89-5...	TCP	47774 → 443 [ACK] Seq=1 Ack=1 Win=62780 [TCP CHECKSUM INCORRECT] L...
20	8.191054	server-143-204-89-5...	192.168.127.136	TCP	[TCP ACKed unseen segment] 443 → 47774 [ACK] Seq=1 Ack=2 Win=64240...
25	8.605323	192.168.127.136	www.zut.edu.pl	TCP	49074 → 80 [SYN] Seq=0 Win=64240 [TCP CHECKSUM INCORRECT] Len=0 MS...
26	8.608823	www.zut.edu.pl	192.168.127.136	TCP	80 → 49074 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
27	8.608997	192.168.127.136	www.zut.edu.pl	TCP	49074 → 80 [ACK] Seq=1 Ack=1 Win=64240 [TCP CHECKSUM INCORRECT] Le...
28	8.609904	192.168.127.136	www.zut.edu.pl	HTTP	GET / HTTP/1.1
29	8.610282	www.zut.edu.pl	192.168.127.136	TCP	80 → 49074 [ACK] Seq=1 Ack=399 Win=64240 Len=0
30	8.625799	www.zut.edu.pl	192.168.127.136	HTTP	HTTP/1.1 307 Temporary Redirect (text/html)
31	8.625840	192.168.127.136	www.zut.edu.pl	TCP	49074 → 80 [ACK] Seq=399 Ack=527 Win=63784 [TCP CHECKSUM INCORRECT]...
32	8.658066	192.168.127.136	www.zut.edu.pl	TCP	58866 → 443 [SYN] Seq=0 Win=64240 [TCP CHECKSUM INCORRECT] Len=0 M...
33	8.661743	www.zut.edu.pl	192.168.127.136	TCP	443 → 58866 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
34	8.661847	www.zut.edu.pl	192.168.127.136	TCP	58866 → 443 [ACK] Seq=1 Ack=1 Win=64240 [TCP CHECKSUM INCORRECT] L...
35	8.670463	192.168.127.136	www.zut.edu.pl	TLSv1.2	Client Hello
36	8.671298	www.zut.edu.pl	192.168.127.136	TCP	443 → 58866 [ACK] Seq=1 Ack=518 Win=64240 Len=0
37	8.675688	www.zut.edu.pl	192.168.127.136	TLSv1.2	Server Hello



No.	Time	Source	Destination	Protocol	Info
908	15.149453	www.zut.edu.pl	192.168.127.136	TCP	443 → 58872 [ACK] Seq=157318 Ack=2987 Win=64240 Len=0
909	15.149479	www.zut.edu.pl	192.168.127.136	TCP	443 → 58872 [ACK] Seq=157318 Ack=2988 Win=64239 Len=0
910	15.149822	192.168.127.136	www.zut.edu.pl	TLSv1.2	Encrypted Alert
911	15.150012	192.168.127.136	www.zut.edu.pl	TCP	58868 → 443 [FIN, ACK] Seq=3454 Ack=187558 Win=65535 [TCP CHECKSUM]...
912	15.150477	www.zut.edu.pl	192.168.127.136	TCP	443 → 58868 [ACK] Seq=187558 Ack=3454 Win=64240 Len=0
913	15.150493	www.zut.edu.pl	192.168.127.136	TCP	443 → 58868 [ACK] Seq=187558 Ack=3455 Win=64239 Len=0
914	15.150648	192.168.127.136	www.zut.edu.pl	TLSv1.2	Encrypted Alert
915	15.150904	192.168.127.136	www.zut.edu.pl	TCP	58866 → 443 [FIN, ACK] Seq=5688 Ack=298578 Win=65535 [TCP CHECKSUM]...
916	15.151316	www.zut.edu.pl	192.168.127.136	TCP	443 → 58866 [ACK] Seq=298578 Ack=5688 Win=64240 Len=0
917	15.151392	www.zut.edu.pl	192.168.127.136	TCP	443 → 58866 [ACK] Seq=298578 Ack=5689 Win=64239 Len=0
918	15.152029	192.168.127.136	server-143-204-89-1...	TCP	[TCP Dup ACK 11#1] 58132 → 443 [ACK] Seq=1 Ack=1 Win=62780 [TCP CH...
919	15.152033	192.168.127.136	sof01s11-in-f99.1e1...	TCP	[TCP Dup ACK 12#1] 50760 → 80 [ACK] Seq=1 Ack=1 Win=63791 [TCP CHE...
920	15.152069	server-143-204-89-1...	192.168.127.136	TCP	[TCP Dup ACK 13#1] [TCP ACKed unseen segment] 443 → 58132 [ACK] Se...
921	15.152069	sof01s11-in-f99.1e1...	192.168.127.136	TCP	[TCP Dup ACK 14#1] [TCP ACKed unseen segment] 80 → 50760 [ACK] Seq...
922	16.835548	www.zut.edu.pl	192.168.127.136	TLSv1.2	Encrypted Alert
923	16.836151	192.168.127.136	www.zut.edu.pl	TCP	58876 → 443 [ACK] Seq=3092 Ack=283267 Win=65535 [TCP CHECKSUM INCO...
924	16.836450	www.zut.edu.pl	192.168.127.136	TCP	443 → 58876 [FIN, PSH, ACK] Seq=283267 Ack=3092 Win=64240 Len=0
925	16.836909	192.168.127.136	www.zut.edu.pl	TLSv1.2	Encrypted Alert
926	16.837314	192.168.127.136	www.zut.edu.pl	TCP	58876 → 443 [FIN, ACK] Seq=3123 Ack=283268 Win=65535 [TCP CHECKSUM]...
927	16.837995	www.zut.edu.pl	192.168.127.136	TCP	443 → 58876 [ACK] Seq=283268 Ack=3123 Win=64240 Len=0
928	16.838024	www.zut.edu.pl	192.168.127.136	TCP	443 → 58876 [ACK] Seq=283268 Ack=3124 Win=64239 Len=0
929	17.489394	www.zut.edu.pl	192.168.127.136	TLSv1.2	Encrypted Alert
930	17.490135	192.168.127.136	www.zut.edu.pl	TLSv1.2	Encrypted Alert
931	17.490663	192.168.127.136	www.zut.edu.pl	TCP	58870 → 443 [FIN, ACK] Seq=7611 Ack=326646 Win=65535 [TCP CHECKSUM]...
932	17.491104	www.zut.edu.pl	192.168.127.136	TCP	443 → 58870 [ACK] Seq=326646 Ack=7611 Win=64240 Len=0
933	17.491128	www.zut.edu.pl	192.168.127.136	TCP	443 → 58870 [ACK] Seq=326646 Ack=7612 Win=64239 Len=0