

EEM-413 Bilgisayar Ağları Lab3 (TCP)

*İlk olarak gerekli işlemleri yapıp yaptığımız trace işleminden sonra TCP araması yaparak ilk screenshotumuzu alıyoruz.

1)

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (Frame 4), which is a TCP SYN packet. The third pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
4	1.58751300	192.168.2.2	128.119.245.12	TCP	62	54852 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
5	1.72970200	128.119.245.12	192.168.2.2	TCP	62	http > 54852 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1
6	1.73976200	192.168.2.2	128.119.245.12	TCP	54	54852 > http [ACK] Seq=1 Ack=1 Win=63360 Len=0
7	1.74447000	192.168.2.2	128.119.245.12	TCP	602	[TCP segment of a reassembled PDU]
8	1.74633900	192.168.2.2	128.119.245.12	TCP	1506	[TCP segment of a reassembled PDU]
9	1.89339700	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=639 Win=7018 Len=0
10	1.89343300	192.168.2.2	128.119.245.12	TCP	1506	[TCP segment of a reassembled PDU]
11	1.91149500	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=2091 Win=8712 Len=0
12	1.91153600	192.168.2.2	128.119.245.12	TCP	2958	[TCP segment of a reassembled PDU]
13	2.05168200	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=3543 Win=11616 Len=0
14	2.05171400	192.168.2.2	128.119.245.12	TCP	2958	[TCP segment of a reassembled PDU]
15	2.07063400	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=4995 Win=14520 Len=0
16	2.07065600	192.168.2.2	128.119.245.12	TCP	2958	[TCP segment of a reassembled PDU]

Frame 4 Details:

- Frame 4: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
- Ethernet II, Src: wistronit_bb:06:cb (F0:de:f1:bb:06:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)
- Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol, Src Port: 54852 (54852), Dst Port: http (80), Seq: 0, Len: 0
- Source port: 54852 (54852)
- Destination port: http (80)
- Stream index: 0
- Sequence number: 0 (relative sequence number)
- Header length: 28 bytes
- Flags: 0x002 (SYN)
- Window size value: 8192
- [calculated window size: 8192]
- Checksum: 0x3851 (validation disabled)
- Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted

Raw Data:

```
0000 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 00 45 00 ..*.K... ..f...E.
0010 00 30 65 59 40 00 80 06 00 00 c0 a8 02 02 80 77 .0eY8... ..w
0020 f5 0c 00 00 50 1e 07 8b 63 00 00 00 70 02 .B.P.. ..C....p.
0030 20 00 38 51 00 00 02 04 05 b4 01 01 04 02 ..BQ.... ..
```

Yukarıda da görüldüğü gibi source IP 192.168.2.2 olan benim adresim ve TCP port numarasıda Source port : 54852 dir.

2)

gaia.cs.umass.edu adresinin yani destination ın IP Adresi : 128.119.245.12 ve

TCP port numarası yukarıda da görüldüğü gibi ;

TCP port numarası : 80 dir.

EEM-413 Bilgisayar Ağları Lab3 (TCP)

3)

Bahsedildiği üzere analyse kısmından http işareti kaldırıldığında sadece TCP connectionları görülebilmekteyiz. Screenshotu aşağıdadır.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, filtered by 'tcp'. The middle pane shows the details of the selected packet (No. 32), which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4	1.59751300	192.168.2.2	128.119.245.12	TCP	62	54852 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
5	1.73970300	128.119.245.12	192.168.2.2	TCP	62	http > 54852 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1
6	1.73976300	192.168.2.2	128.119.245.12	TCP	54	54852 > http [ACK] Seq=1 Ack=1 Win=65340 Len=0
7	1.74447000	192.168.2.2	128.119.245.12	TCP	692	54852 > http [PSH, ACK] Seq=1 Ack=1 Win=65340 Len=638
8	1.74633900	192.168.2.2	128.119.245.12	ICP	1506	54852 > http [ACK] Seq=639 Ack=1 Win=65340 Len=1452
9	1.89339700	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=639 Win=7018 Len=0
10	1.89343300	192.168.2.2	128.119.245.12	TCP	1506	54852 > http [ACK] Seq=2091 Ack=1 Win=85340 Len=1452
11	1.91149500	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=2091 Win=8712 Len=0
12	1.91153000	192.168.2.2	128.119.245.12	TCP	2958	54852 > http [ACK] Seq=1 Ack=6447 Win=59340 Len=2904
13	2.05168200	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=6447 Win=11616 Len=0
14	2.05171400	192.168.2.2	128.119.245.12	TCP	2958	54852 > http [ACK] Seq=1 Ack=6447 Win=59340 Len=2904
15	2.07063400	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=4995 Win=14520 Len=0
16	2.07066000	192.168.2.2	128.119.245.12	ICP	2958	54852 > http [ACK] Seq=9331 Ack=1 Win=59340 Len=2904
17	2.08664500	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=6447 Win=17424 Len=0
18	2.08667200	192.168.2.2	128.119.245.12	TCP	2958	54852 > http [ACK] Seq=12255 Ack=1 Win=65340 Len=2904
19	2.21061300	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=7699 Win=20328 Len=0
20	2.21064400	192.168.2.2	128.119.245.12	TCP	2958	54852 > http [PSH, ACK] Seq=15159 Ack=1 Win=65340 Len=2904
21	2.22638500	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=9331 Win=23232 Len=0
22	2.22642500	192.168.2.2	128.119.245.12	TCP	2958	54852 > http [ACK] Seq=18063 Ack=1 Win=65340 Len=2904
23	2.24450100	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=10803 Win=26136 Len=0
24	2.24457000	192.168.2.2	128.119.245.12	ICP	2958	54852 > http [ACK] Seq=20967 Ack=1 Win=65340 Len=2904
25	2.26052200	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=12255 Win=29040 Len=0
26	2.26059200	192.168.2.2	128.119.245.12	ICP	2958	54852 > http [ACK] Seq=23871 Ack=1 Win=65340 Len=2904
27	2.27459300	192.168.2.2	173.194.70.94	SSL	55	continuation data
28	2.27850500	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=13707 Win=33396 Len=0
29	2.27856000	192.168.2.2	128.119.245.12	ICP	2958	54852 > http [ACK] Seq=26727 Ack=1 Win=65340 Len=2904
30	2.29449000	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=15159 Win=36300 Len=0
31	2.29453000	192.168.2.2	128.119.245.12	ICP	2958	54852 > http [ACK] Seq=29879 Ack=1 Win=65340 Len=2904
32	2.37011800	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=16611 Win=39204 Len=0

Frame 4: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Winbond [8:00:0E:14:66:14], Dst: Arcadyan [02:43:14:00:1A:2A:02:14:AD]
...K... ..f...E.
...0ey8... ..w
...D.P... ..c...p.
...8Q... ..

EEM-413 Bilgisayar Ağları Lab3 (TCP)

4) TCP SYN segmenti aşağıda da gösterildiği gibi 0 değerine sahiptir. Flag kısmı ile birlikte gösterilmektedir.

Wireshark capture of a TCP SYN segment. The packet list shows a SYN segment from 192.168.2.2 to 128.119.245.12. The packet details show the TCP header with Seq=0, Win=0, and the SYN flag set. The packet bytes show the raw TCP header and data.

No.	Time	Source	Destination	Protocol	Length	Info
4	1.59751300	192.168.2.2	128.119.245.12	TCP	62	54852 > http [SYN] Seq=0 Win=0 MSS=1460 SACK_PERM=1
5	1.73970300	128.119.245.12	192.168.2.2	TCP	62	http > 54852 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1
6	1.73976300	192.168.2.2	128.119.245.12	TCP	54	54852 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
7	1.74447000	192.168.2.2	128.119.245.12	TCP	62	54852 > http [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=638
8	1.74633900	192.168.2.2	128.119.245.12	TCP	1506	54852 > http [ACK] Seq=639 Ack=1 Win=65536 Len=1452
9	1.89339700	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=639 Win=7018 Len=0
10	1.89343300	192.168.2.2	128.119.245.12	TCP	1506	54852 > http [ACK] Seq=2091 Ack=1 Win=65536 Len=1452
11	1.91149500	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=2091 Win=8712 Len=0
12	1.91157800	192.168.2.2	128.119.245.12	TCP	2058	54852 > http [ACK] Seq=1347 Ack=1 Win=65536 Len=2004
13	2.05168200	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=3543 Win=11616 Len=0

[Stream index: 0]
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 = Nonce: Not set
....0. = Congestion Window Reduced (CWR): Not set
....0. = ECN-Echo: Not set
....0. = Urgent: Not set
....0. = acknowledgment: Not set
....0. = Push: Not set
....0. = Reset: Not set
...1. = Syn: set
....0. = Fin: Not set
window size value: 8192
[calculated window size: 8192]
Checksum: 0x3851 [validation disabled]
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
Maximum segment size: 1460 bytes
No-Operation (NOP)

0000 00 1a 2a 02 48 ed f0 de f1 bb 66 c5 08 00 45 00 ...K...F...E..
0010 00 30 65 59 40 00 00 06 03 00 c0 a8 02 02 80 77 ...0...W..
0020 f5 0c d6 44 00 30 1e 07 8b 63 00 00 00 70 02 ...D.P...P..
0030 20 00 38 91 00 00 02 04 03 b4 01 01 01 01 02 ...8q.....

5)

SYN ACK nın sequence numarası tracelerdeki 2. Sırada belirtildiği gibi Seq=0 dır.

SYN ACK kısmındaki ACK =1 kısmı acknowlegde değerinin 1 olduğunu göstermektedir.

Gaia.cs.umass.edu adresi bu değeri SYN ve ack flaglarının set olma durumuna göre tanımlamıştır.

Syn flagının set olma durumu ve diğer flagların durumu yukarıdaki screenshotta belirtilmektedir.

EEM-413 Bilgisayar Ağları Lab3 (TCP)

6)

Aşağıdaki screenshottada görüldüğü gibi SYN ve ACK set olmuş durumda ve push flagi set edilmiş durumdadır. Bundan dolayı HTTP POST command kısmında mavi ile belirtilen kısımdır.

Wireshark network traffic capture showing a successful HTTP POST request. The packet list shows a SYN-ACK (Seq=639, Ack=1) and a PUSH-ACK (Seq=639, Ack=1, Push=1). The packet details pane shows the TCP flags: SYN, ACK, and PUSH are set. The packet bytes pane shows the raw data of the packet.

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
4	1.59751300	192.168.2.2	128.119.245.12	TCP	62	54852 > http [SYN, Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
5	1.73970300	128.119.245.12	192.168.2.2	TCP	62	http > 54852 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1
6	1.73976300	192.168.2.2	128.119.245.12	TCP	54	54852 > http [ACK] Seq=1 Ack=1 win=65340 Len=0
7	1.74447000	192.168.2.2	128.119.245.12	TCP	692	54852 > http [PSH, ACK] Seq=1 Ack=1 win=65340 Len=618
8	1.74633900	192.168.2.2	128.119.245.12	TCP	1506	54852 > http [ACK] Seq=639 Ack=1 win=65340 Len=1452
9	1.89339700	128.119.245.12	192.168.2.2	TCP	60	http > 54852 [ACK] Seq=1 Ack=639 win=7018 Len=0

Frame 7: 692 bytes on wire (5536 bits), 692 bytes captured (5536 bits) on interface 0

Ethernet II, Src: Wistroni_bb:66:cb (f0:de:f1:bb:66:cb), Dst: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed)

Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 54852 (54852), Dst Port: http (80), Seq: 1, Ack: 1, Len: 638

Source port: 54852 (54852)

Destination port: http (80)

[Stream index: 0]

Sequence number: 1 (relative sequence number)

[Next sequence number: 639 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header length: 20 bytes

Flags: 0x018 (PSH, ACK)

000. = 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

....1. = Push: Set

....0. = Reset: Not set

....0. = Syn: Not set

....0. = Fin: Not set

Window size value: 65340

[calculated window size: 65340]

0000 00 1a 2a 02 4b ed f0 de f1 bb 66 cb 08 00 45 00 ..K... ..f...E.

0010 02 a6 65 5b 40 00 80 06 00 00 c0 a8 02 02 80 77 ..e[8... ..W

0020 f5 0c d6 44 00 50 1e 07 8b 64 56 df a8 0b 50 18 ...D.P... ..dv..kp.

0030 ff 3c 3a c7 00 00 50 4f 93 54 20 2f 7f 09 72 65 <... ..PO ST /wire

0040 73 68 61 72 6d 2d 6c 61 62 73 2f 6c 61 62 33 2d shark-la bs/lab3-

0050 21 2d 73 68 70 6c 70 7a 68 74 6d 70 48 64 64 50 1 control bps wire

EEM-413 Bilgisayar Ağları Lab3 (TCP)

shottada kırmızı ile belirtilmiş olan 6 paket veriyi göstermektayım.

The first screenshot shows a list of 26 packets. The selected packet (No. 122) is highlighted in red. The packet details pane shows the following information:

- Frame 122: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Aradyan_02:4b:ed (00:1a:2a:02:4b:ed), Dst: Wistron_Lb66:cb (f0:de:f1:bb:66:cb)
- Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.2 (192.168.2.2)
- Transmission Control Protocol, Src Port: http (80), Dst Port: http (80), Seq: 1, Ack: 3543, Len: 0

The second screenshot shows a zoomed-in view of the packet details for the selected packet (No. 122). The packet details pane shows the following information:

- Frame 122: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Aradyan_02:4b:ed (00:1a:2a:02:4b:ed), Dst: Wistron_Lb66:cb (f0:de:f1:bb:66:cb)
- Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.2 (192.168.2.2)
- Transmission Control Protocol, Src Port: http (80), Dst Port: http (80), Seq: 1, Ack: 3543, Len: 0

EEM-413 Bilgisayar Ağları Lab3 (TCP)

Yukarıda kırmızı ile gösterilen her ikili için gelen ACK mesajları bu ikililerin altlarında bulunmaktadır.

****Hocam tüm değerleri kendi traceimden hesaplıyorum ancak hepsinin ACK sürelerini veya normal sürelerini yukarıdaki iki screenshoot da görebilirsiniz. Segment numaralarını göstermedim ama içlerini açıp yazdım .**

Segment Numarası	Gönderme Süresi(sn)	ACK süresi(sn)	Uzunluk(byte)	RTT(sn)
1	0,143234	0.144592	692	0.001358
639	0,148036	0.297894	1506	0.149858
125511	2.219200	2.195250	1506	0.000325
126963	2.219205	2.219524	1506	0.000474
129867	2.445199	2.592395	1506	0.147196
131319	2.445204	2.611942	1506	0.166738

EstimatedRTT leri her segment için aşağıya yazıcam ancak 1 tanesinin çözümünü göstericem.

$$\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRT}$$

Birinci için RTT = 0.001358 sn

$$\text{İkinci için RTT} = 0.875 * 0.001358 + 0.125 * 0.149858 = 0.0199205$$

$$\text{Üçüncü için RTT} = 0.0174710$$

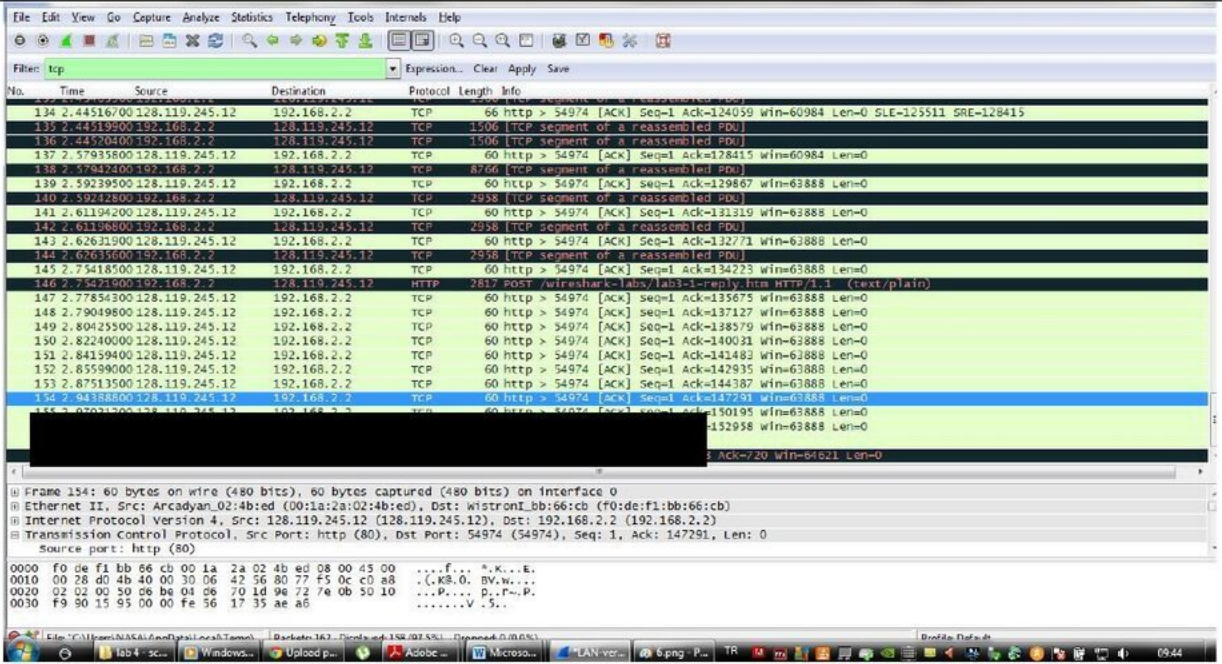
$$\text{Dördüncü için RTT} = 0.0153463$$

$$\text{Beşinci RTT} = 0.0318275$$

$$\text{Altıncı için RTT} = 0.0486913$$

9)

gaia.cs.umass.edu bu adres için ilk serverdan gelen ack 5840 byte ve son Ack geldiğinde windows size en çok 64621 olabiliyor. Aşağıdaki screenshoot daka win : kısmında belirtilmiştir. Bu trace de receiver buffer kapasitesiyle ilgili bir sıkıntı çekmemiştir.



10) Benim traceimde retransmission var ancak bu birden fazla kere denediğim için olduğunu düşünüyorum çünkü ilkinde yoktu .

11)

ACK isim	Ack seq. numarası	Ack data
ACK1	639	60byte
ACK2	2091	1460byte
ACK3	3543	1460byte

*Daha çok uzun bi şekilde devam etsede örnek olarak 3 tane gösterdim.

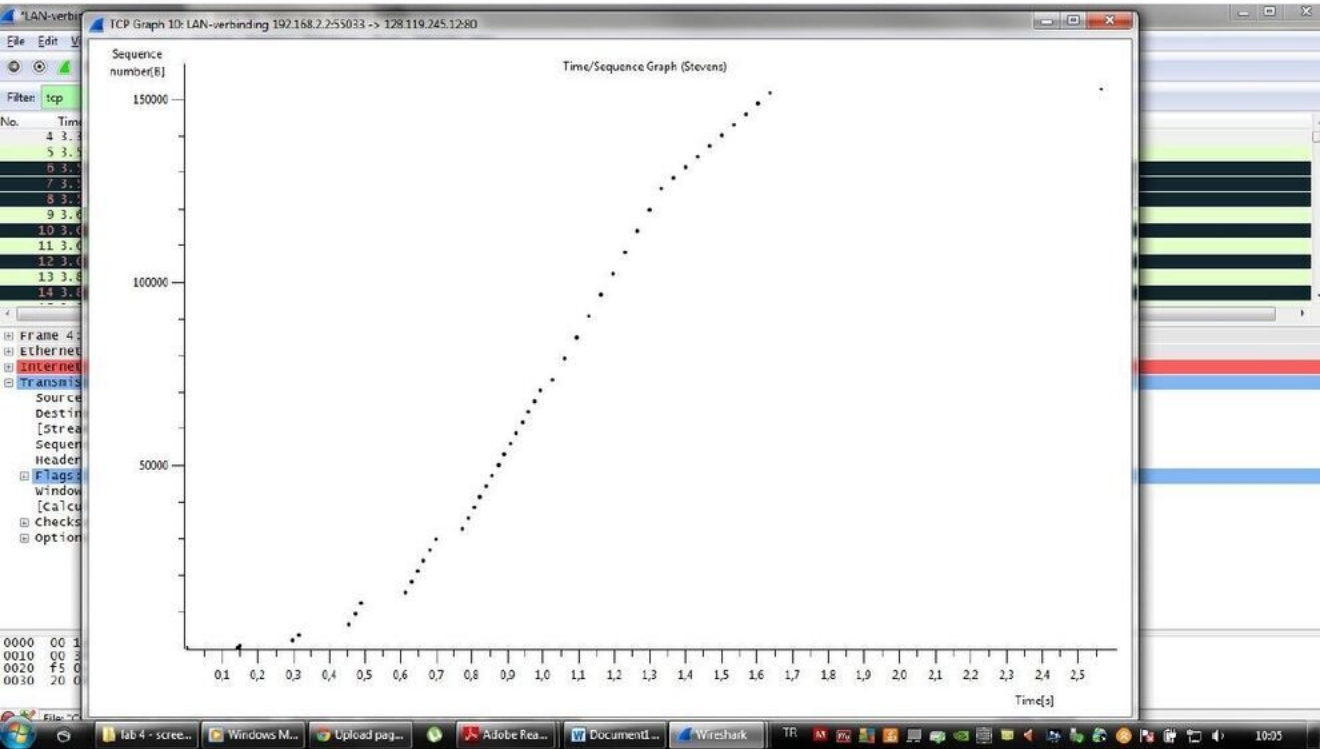
Cumlatif ACK receiverın her aldığında geliyor.

12) Throughput nedir nasıl hesaplanır sorusunun cevabı :

As a common throughput computation, in this question, we select the average time period as the whole connection time. Then, the average throughput for this TCP connection is computed as the ratio between the total amount data and the total transmission time. The total amount data transmitted can be computed by the difference between the sequence number of the first TCP segment (i.e. 1 byte for No. 4 segment) and the acknowledged sequence number of the last ACK (164091 bytes for No. 202 segment). Therefore, the total data are $164091 - 1 = 164090$ bytes. The whole transmission time is the difference of the time instant of the first TCP segment (i.e., 0.026477 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 202 segment). Therefore, the total transmission time is $5.455830 - 0.026477 = 5.4294$ seconds. Hence, the throughput for the TCP connection is computed

EEM-413 Bilgisayar Ağları Lab3 (TCP)

as $164090/5.4294 = 30.222$ KByte/sec.



13) ** Benim grafiğim örnek gösterilenden biraz farklı çıktı ama trace den almak istemediğim için kendiminkini koydum .

*Slow startı baktığımızda tanımlayabiliriz. HTTP POST gönderisi ve grafiğin eğiminde bu sonuca varılabileceğini düşünüyorum.

*Tcp göndericisi bu yapıda daha agresif ve ağ çok yoğun olduğunda karışabileceğini düşünüyorum ayrıca ACK lar bazen düzenli gelemeyebiliyor.TCP nin slow start fazında küçük web objelerinin gönderilmesi ciddi bi zaman kaybı olabilir.Ayrıca TCP nin davranışı direk kullandığı uygulamaya bağlıdır.