



Laboratuvar Raporu 4

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Şevval Ayça Çerence

152120211128

Dr. Öğr. Üyesi İlker Özçelik

2024-2025

1. İçindekiler	2
2. Giriş	3
3. Sorular	
3.1	3
3.2	3
3.3	4
3.4	4
3.5	5
3.6	5
3.7	6
3.8	7
3.9.	7
3.10	7
3.11	8
3.12	8
3.13	9
3.14	9
4.Kaynakça	9

2. Giriş

TCP (İletim Kontrol Protokolü), internet üzerindeki cihazlar arasında güvenilir veri aktarımını sağlamak için geliştirilmiş bir iletişim protokolüdür. Uygulama katmanı ile ağ katmanı arasında köprü görevi görerek, veri paketlerinin doğru ve sıralı bir şekilde iletilmesini garanti eder. Bu protokol, veri bütünlüğünü sağlamak amacıyla hata tespiti ve düzeltme, akış kontrolü ve bağlantı yönetimi gibi mekanizmalar kullanır.

TCP, bağlantı odaklı bir protokoldür; yani veri aktarımı başlamadan önce, gönderici ve alıcı arasında güvenilir bir bağlantı kurulması gerekir. Bu süreç "üçlü el sıkışma" (Three-Way Handshake) yöntemiyle gerçekleşir. Ayrıca, TCP'nin akış kontrolü mekanizması sayesinde, alıcının kapasitesini aşmayacak şekilde veri iletimi sağlanır. Böylece, veri kaybı ve tıkanıklık gibi olası sorunlar minimize edilir.

Wireshark gibi analiz araçları, TCP trafiğini detaylı bir şekilde inceleyerek ağ performansını değerlendirmeye ve olası sorunları tespit etmeye yardımcı olur. Bu dokümanda, TCP'nin temel yapısı, çalışma prensipleri ve Wireshark kullanılarak nasıl analiz edileceği ele alınacaktır.

3.Sorular

3.1

5003	59.740594	199.232.190.172	172.20.10.5	HTTP	1360	HTTP/1.1 206 Partial Content
5374	60.578885	172.20.10.5	128.119.245.12	HTTP	1175	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
5445	60.769371	128.119.245.12	172.20.10.5	HTTP	831	HTTP/1.1 200 OK (text/html)
5548	61.037838	2a04:4e42:6f::684	2a00:1880:a100:7d4b...	HTTP	524	HTTP/1.1 206 Partial Content

Frame 5374: 1175 bytes on wire (9400 bits), 1175 bytes captured (9400 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0
Ethernet II, Src: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29), Dst: 0e:51:7e:db:db:64 (0e:51:7e:db:db:64)
Internet Protocol Version 4, Src: 172.20.10.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51777, Dst Port: 80, Seq: 151929, Ack: 1, Len: 1121
Source Port: 51777
Destination Port: 80
[Stream index: 75]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1121]
Sequence Number: 151929 (relative sequence number)
Sequence Number (raw): 3349148833
[Next Sequence Number: 153050 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)

İstemci bilgisayarın IP adresi 172.20.10.5 olarak belirlenmiş, TCP bağlantısı için kullanılan port numarası ise 51777 olarak tespit edilmiştir.

3.2

5003	59.740594	199.232.190.172	172.20.10.5	HTTP	1360	HTTP/1.1 206 Partial Content
5374	60.578885	172.20.10.5	128.119.245.12	HTTP	1175	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
5445	60.769371	128.119.245.12	172.20.10.5	HTTP	831	HTTP/1.1 200 OK (text/html)
5548	61.037838	2a04:4e42:6f::684	2a00:1880:a100:7d4b...	HTTP	524	HTTP/1.1 206 Partial Content

Frame 5445: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0
Ethernet II, Src: 0e:51:7e:db:db:64 (0e:51:7e:db:db:64), Dst: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.5
Transmission Control Protocol, Src Port: 80, Dst Port: 51777, Seq: 1, Ack: 153050, Len: 777
Source Port: 80
Destination Port: 51777
[Stream index: 75]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 777]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 546015755
[Next Sequence Number: 778 (relative sequence number)]

Gaia.cs.umass.edu sunucusunun IP adresi **128.119.245.12** olarak tespit edilmiş, TCP bağlantısı için kullanılan port numarası ise **80** olarak belirlenmiştir.

3.3

Wireshark analizine göre, istemci bilgisayarın IP adresi 172.20.10.5 olarak tespit edilmiş, TCP bağlantısı için kullanılan port numarası ise 51777 olarak belirlenmiştir.

3.4

```
987 34.335146 2a00:1880:a100:7d4b... 2a00:1880:ffff::b90... TCP 86 51752 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1390 WS=256 SACK_PERM
988 34.372677 2a00:1880:ffff::b90... 2a00:1880:a100:7d4b... TCP 86 80 → 51752 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1410 SACK_PERM WS=128
989 34.372774 2a00:1880:a100:7d4b... 2a00:1880:ffff::b90... TCP 74 51752 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3969454598
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
 000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: 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
[TCP Flags: .....S.]
Window: 65535
[Calculated window size: 65535]
Checksum: 0xc52c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]
[SEQ/ACK analysis]
```

Wireshark ortamında yapılan üçlü el sıkışma (three-way handshake) sürecinde, ilk adımda SYN segmenti gönderildiğinde, sequence number değeri genellikle 0 olarak görülür. Bu durumda SYN bayrağı (SYN flag) 1'e set edilmiştir. Bu, bağlantı kurulum sürecinin başladığını gösteren bir işarettir. İlgili ekran görüntüsünde, bu SYN segmentinin doğru şekilde iletildiği ve sequence number değerinin 0 olarak ayarlandığı açıkça gözlemlenebilir. Bu, bağlantı kurulumunun ilk aşamasıdır ve TCP iletişimi için temel bir adımdır.

3.5

22	3.650149	2a04:4e42:70::347	2a00:1880:a100:7d4b...	TCP	74	443 → 51609 [ACK] Seq=1 Ack=49 Win=314 Len=0
23	3.655657	128.119.245.12	172.20.10.5	TCP	66	80 → 51725 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
24	3.655801	172.20.10.5	128.119.245.12	TCP	54	51725 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
25	3.655919	2a04:4e42:70::347	2a00:1880:a100:7d4b...	TCP	74	443 → 51609 [ACK] Seq=1 Ack=88 Win=314 Len=0
26	3.655919	2a04:4e42:70::347	2a00:1880:a100:7d4b...	TLSv1.2	113	Application Data
27	3.655919	2a04:4e42:70::347	2a00:1880:a100:7d4b...	TCP	74	443 → 51609 [ACK] Seq=40 Ack=425 Win=320 Len=0
35	3.669876	128.119.245.12	172.20.10.5	TCP	66	80 → 51726 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
36	3.669997	172.20.10.5	128.119.245.12	TCP	54	51726 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
37	3.693170	2a04:4e42:70::347	2a00:1880:a100:7d4b...	TLSv1.2	275	Application Data
38	3.693285	2a00:1880:a100:7d4b...	2a04:4e42:70::347	TCP	74	51609 → 443 [ACK] Seq=425 Ack=241 Win=255 Len=0
39	3.694383	2a00:1880:a100:7d4b...	2a04:4e42:70::347	TLSv1.2	109	Application Data
41	3.761739	2a04:4e42:70::347	2a00:1880:a100:7d4b...	TCP	74	443 → 51609 [ACK] Seq=241 Ack=460 Win=320 Len=0
43	5.908386	2a00:1880:a100:7d4b...	2600:1901:0:47fc::	TCP	75	51512 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
44	6.009630	2600:1901:0:47fc::	2a00:1880:a100:7d4b...	TCP	86	443 → 51512 [ACK] Seq=1 Ack=2 Win=1050 Len=0 SLE=1 SRE=2
46	8.400019	2a00:1450:0017:816::	2a00:1880:a100:7d4b...	TLSv1.2	147	Application Data

Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{0FC459ED-E4DD-4993-A33A-3A2168C6AE4C}, id 0
Ethernet II, Src: 0e:51:7e:db:db:64 (0e:51:7e:db:db:64), Dst: LiteonTechno_a4:48:29 (9c:2f:9d:a4:48:29)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.5
Transmission Control Protocol, Src Port: 80, Dst Port: 51725, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 51725
[Stream index: 4]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2354418486
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3709717695
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x012 (SYN, ACK)
000. = Reserved: Not set
...0 = Accurate ECN: Not set
.... 0... = Congestion Window Reduced: Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1. = Acknowledgment: Set
....0.. = Push: Not set
....0.. = Reset: Not set
►1. = Syn: Set
....0 = Fin: Not set

TCP üçlü el sıkışma (three-way handshake) sürecinin ikinci adımında, SYN+ACK segmenti gönderildiğinde sequence number değeri genellikle 0 olarak görülür. Bu durumda Acknowledgement (ACK) alanı ise 1 olarak ayarlanmış, yani bu segment, ilk SYN segmentinin alındığını ve onaylandığını belirten bir yanıt içerir.

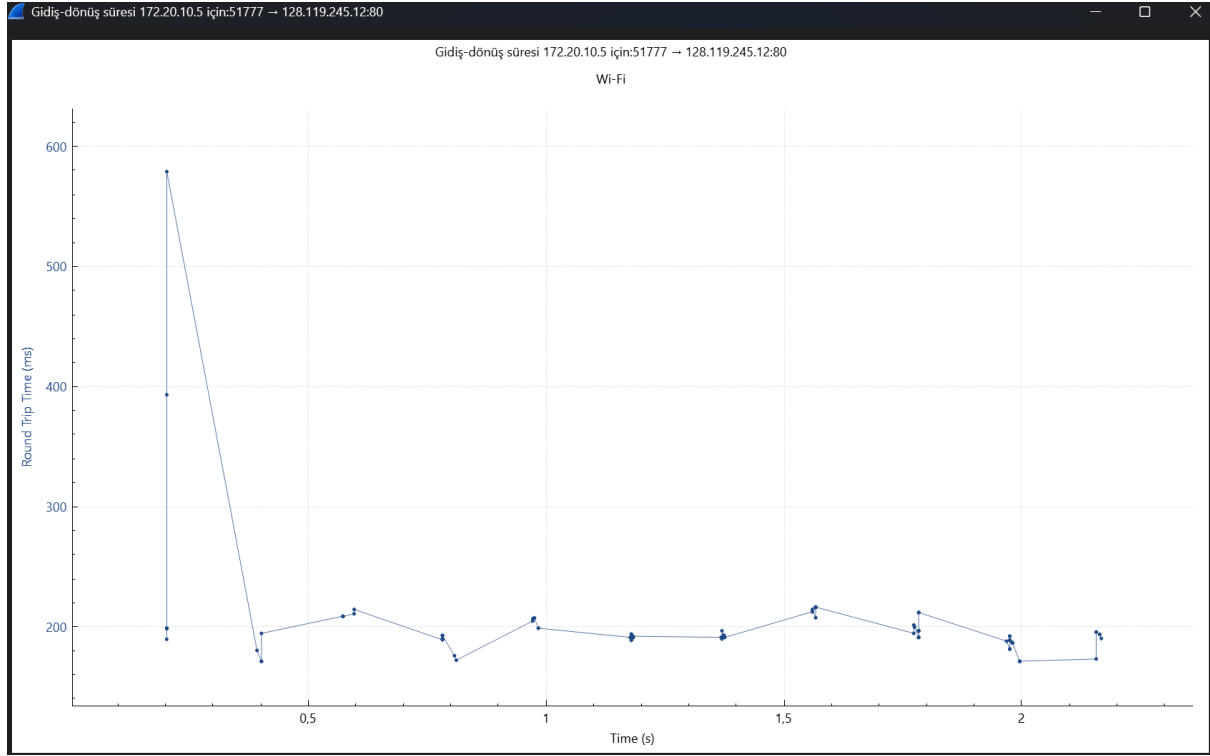
SYN+ACK segmentinin içerisinde hem SYN bayrağı hem de ACK bayrağı 1'e set edilmiştir. SYN bayrağı, bu segmentin bağlantı kurulumunun bir parçası olduğunu belirtirken, ACK bayrağı ise önceki SYN segmentinin başarılı bir şekilde alındığını ve bununla birlikte bir sonraki adım için bağlantı kurulumunun devam edeceğini gösterir.

Ayrıca, ACK değeri, bir sonraki segmentin sequence number'ına eşittir. Bu, alıcı cihazın, gönderilen SYN segmentini aldığını ve iletişim kurulumunun devam etmesi için gerekli yanıtı verdiğini ifade eder.

3.6

Wireshark'ta 5374 numaralı TCP segmenti, HTTP POST komutunu içeriyor ve sequence number'ı 1 olarak görünüyor. Bu, üçlü el sıkışma (three-way handshake) tamamlandıktan sonra veri iletiminin başladığını gösterir.

Sequence number + len değeri kadar artarak devam etmiştir, ilk sequence numarası 1, İkinci için 699, üçüncü için 1438156, dördüncü için 1439534, beşinci için 1440912,altıncı için 1442290 olarak bulunmuştur. Len değeri=1378 değerine eşittir.



3.8

5287	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=125329 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5288	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=126729 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5289	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=128129 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5290	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=129529 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5291	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[PSH, ACK] Seq=130929 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5292	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=132329 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]

Hepsinin len değeri 1400'dür ve eşittir.

3.9

5287	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=125329 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5288	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=126729 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5289	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=128129 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5290	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=129529 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5291	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[PSH, ACK] Seq=130929 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]
5292	60.386419	172.20.10.5	128.119.245.12	TCP	1454	51777 → 80	[ACK] Seq=132329 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 5374]

TCP, güvenilir veri iletimi sağlamak için ACK numaralarını kullanır. Her veri segmenti alıcı tarafından onaylanır ve gönderici, her bir segmentin alındığını doğrulayan bir ACK alır. Burada, alıcı pencere boyutu (Win=65280) göndericinin veri gönderme hızını sınırlamaktadır. Segment uzunluğu (1454 bayt) pencere boyutundan küçük olduğu için veri iletimi düzgün şekilde gerçekleşir. Ancak, alıcı tamponu dolarsa, alıcı pencere boyutunu sıfıra ayarlayarak göndericiyi durdurur ve veri akışını kontrol eder.

3.10

Yeniden gönderim yaşanmamıştır; paketlerdeki ACK numaralarına bakıldığında, her ACK numarası artış göstermekte ve tekrarlama olmadığı görülmektedir. Bu durum, veri iletiminin sorunsuz bir şekilde gerçekleştiğini ve her bir segmentin başarıyla alındığını gösterir.

3.11

Receiver'ın 1400 byte uzunluğunda olan ACK segmentlerinde gözlemlenebilecek bazı durumlar bulunmaktadır. Özellikle, bir satırda birden fazla ACK paketi yer aldığında, her bir ACK numarasının artış gösterdiği ve her bir segmentin başarıyla alındığı gözlemlenebilir. Bu, veri iletiminde alıcı tarafından gelen ACK paketlerinin, gönderilen segmentlerin sırasıyla alındığını ve onaylandığını gösterir. Bu tür durumlar, veri akışının düzgün ve kesintisiz bir şekilde gerçekleştiğini, herhangi bir yeniden gönderim (retransmission) gerekliliği olmadığını gösterir. ACK numaralarındaki artış, her bir yeni segmentin başarıyla iletilmesini ve alıcı tarafından kabul edildiğini doğrular.

3.12

5375 60.578947	128.119.245.12	172.20.10.5	TCP	54 80 → 51777 [ACK] Seq=1 Ack=144929 Win=252416 Len=0
5376 60.619485	2a00:1880:a100:7d4b...	2a04:4e42:6f::684	TCP	86 51770 → 80 [ACK] Seq=699 Ack=1438156 Win=37376 Len=0 TSval=781606201 TSecr=562810028
5444 60.769371	128.119.245.12	172.20.10.5	TCP	54 80 → 51777 [ACK] Seq=1 Ack=153050 Win=252416 Len=0
5445 60.769371	128.119.245.12	172.20.10.5	HTTP	831 HTTP/1.1 200 OK (text/html)

1. Byte Farkı:

- İlk TCP segmenti (ACK numarası) = 144929
- Son TCP segmenti (ACK numarası) = 153050
- Byte Farkı = 153050 - 144929 = 8121 bayt

2. İletim Zamanı Farkı:

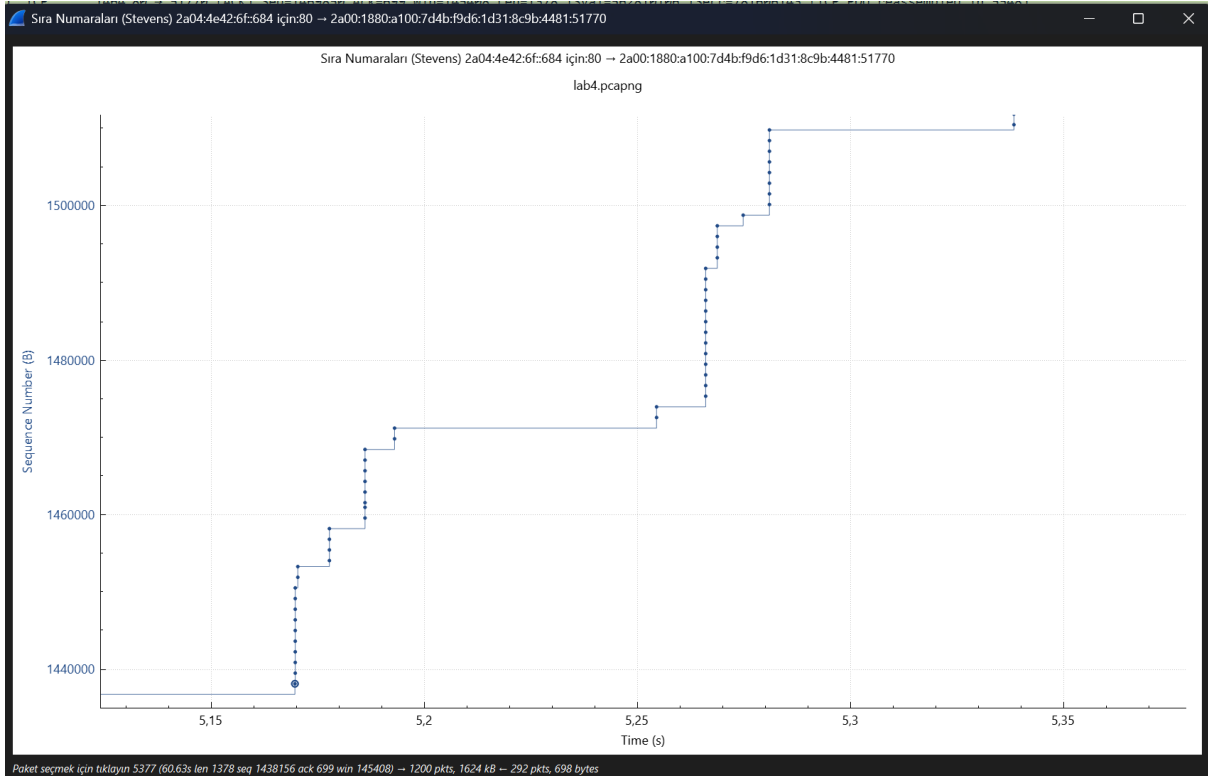
- İlk zaman = 0.706926 saniye
- Son zaman = 0.136435 saniye
- Zaman Farkı = 0.706926 - 0.136435 = 0.570491 saniye

3. Throughput Hesaplama:

- Throughput = Byte Farkı / Zaman Farkı
- Throughput = 8121 bayt / 0.570491 saniye = 14235.11 bayt/saniye

Bu durumda, TCP bağlantısının throughput değeri yaklaşık olarak 14235.11 bayt/saniye olarak hesaplanır.

3.13



TCP slow start aşaması, 60.578947 s zaman damgasında başlayıp 60.769371 s civarında sona ermiştir ve yaklaşık 190 ms sürmüştür. Bu sürecin beklenenden kısa olması, erken tıkanıklık kontrolüne geçiş ve ACK gecikmeleri nedeniyle meydana gelmiş olabilir. Ölçülen veriler, TCP'nin ideal davranışından sapmalar göstererek pencere boyutunun tam kullanılmadığını, alıcı tarafında gecikmeler yaşandığını ve ağ trafiğinin değişkenlik gösterdiğini ortaya koymaktadır. Bu durum, paket kaybı, gecikmeli ACK mekanizması veya ağdaki tıkanıklık seviyelerinin artmasıyla açıklanabilir.

3.14

Sorular cevaplanmıştır.

4.Kaynakça

Wireshark Lab: TCP v8.0 Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross