22100011015

Nursena Taşköprü

1.   Paket yakalama işleminizin toplam süresi ne kadardır? Bu bilgiyi nasıl elde ettiniz? Ekran görüntüsü ile gösteriniz.

Dosyadaki time sütunundan toplam süreyi ölçebiliriz

Toplam süre yaklaşık 10.41 saniye oluyor.

2.   Paket yakalama işleminin gerçek başlangıç ve bitiş zamanını (günün tarihi ve işlem zamanı) ekran görüntüsü ile belirtiniz. Bu bilgiyi görebilmek için Wireshark programında hangi işlem yapılmalıdır?

 Görebilmek için Görünüm> Zaman Görüntüleme Biçimi > Günün tarihi ve saati ayarı seçilmeli.

İlki başlangıç ikincisi bitiş

No.	Time	Source	Destination
297	2025-02-23 01:31:21,315424	20.189.173.10	192.168.52.35
298	2025-02-23 01:31:21,362001	192.168.52.35	128.119.245.12
299	2025-02-23 01:31:21,362001	192.168.52.35	20.189.173.10
300	2025-02-23 01:31:21,362001	192.168.52.35	13.107.21.239
301	2025-02-23 01:31:21,402138	13.107.21.239	192.168.52.35
302	2025-02-23 01:31:21,989720	20.189.173.10	192.168.52.35
303	2025-02-23 01:31:21,990738	192.168.52.35	20.189.173.10
304	2025-02-23 01:31:21,995719	192.168.52.35	20.189.173.10
305	2025-02-23 01:31:21,995766	192.168.52.35	20.189.173.10
306	2025-02-23 01:31:22,221626	192.168.52.35	224.0.0.251
307	2025-02-23 01:31:22,221869	fe80::9057:87b:45ae…	ff02::fb
308	2025-02-23 01:31:22,228658	20.189.173.10	192.168.52.35
309	2025-02-23 01:31:22,433675	20.189.173.10	192.168.52.35
310	2025-02-23 01:31:22,949481	20.189.173.10	192.168.52.35
311	2025-02-23 01:31:22,999046	192.168.52.35	20.189.173.10
312	2025-02-23 01:31:23,961446	192.168.52.35	20.189.173.10
313	2025-02-23 01:31:23,961499	192.168.52.35	20.189.173.10
314	2025-02-23 01:31:24,229946	20.189.173.10	192.168.52.35
315	2025-02-23 01:31:24,911160	20.189.173.10	192.168.52.35

No.	Time	Source	Destination	Protocol	Length	Info
1	2025-02-23 01:31:14,493592	192.168.52.35	20.42.73.30	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
2	2025-02-23 01:31:14,575702	20.42.73.30	192.168.52.35	TLSv1.2	174	Change Cipher Spec, Encrypted Handshake Message, Application
3	2025-02-23 01:31:14,580334	192.168.52.35	20.42.73.30	TLSv1.2	141	Application Data
4	2025-02-23 01:31:14,580395	192.168.52.35	20.42.73.30	TCP	1393	51801 → 443 [ACK] Seq=246 Ack=121 Win=255 Len=1339 [TCP PDU
5	2025-02-23 01:31:14,580395	192.168.52.35	20.42.73.30	TLSv1.2	248	Application Data
6	2025-02-23 01:31:14,580487	192.168.52.35	20.42.73.30	TLSv1.2	92	Application Data
7	2025-02-23 01:31:14,580550	192.168.52.35	20.42.73.30	TCP	1393	51801 → 443 [ACK] Seq=1817 Ack=121 Win=255 Len=1339 [TCP PDU
8	2025-02-23 01:31:14,580550	192.168.52.35	20.42.73.30	TCP	1393	51801 → 443 [ACK] Seq=3156 Ack=121 Win=255 Len=1339 [TCP PDU
9	2025-02-23 01:31:14,580550	192.168.52.35	20.42.73.30	TCP	1393	51801 → 443 [ACK] Seq=4495 Ack=121 Win=255 Len=1339 [TCP PDU
10	2025-02-23 01:31:14,580550	192.168.52.35	20.42.73.30	TLSv1.2	1232	Application Data
11	2025-02-23 01:31:14,881397	20.42.73.30	192.168.52.35	TLSv1.2	92	Application Data
12	2025-02-23 01:31:14,881468	20.42.73.30	192.168.52.35	TCP	54	443 → 51801 [ACK] Seq=159 Ack=1817 Win=16387 Len=0
13	2025-02-23 01:31:14,881481	20.42.73.30	192.168.52.35	TCP	54	443 → 51801 [ACK] Seq=159 Ack=3156 Win=16387 Len=0
14	2025-02-23 01:31:14,881490	20.42.73.30	192.168.52.35	TCP	54	443 → 51801 [ACK] Seq=159 Ack=4495 Win=16387 Len=0
15	2025-02-23 01:31:14,881498	20.42.73.30	192.168.52.35	TCP	54	443 → 51801 [ACK] Seq=159 Ack=5834 Win=16387 Len=0

3. Toplam yakalanan paket sayısı kaçtır?

315 paket yakalanmış

4. 1 ve 3. sorularda elde ettiğiniz bilgilere göre trafik hızınızı (paket/ms) hesaplayınız.

ms olması için 10.41 sn * 1000 deriz = 10410ms

paket sayısı = 315

trafik hızı = 315 / 10410 ms = 0,03025936599942363 paket/ms

5. Yakalanan paketlerden 3 farklı protokole ait paketlerin paket no, protokol ve bilgi kısımlarını yazınız.

Sadece istenen sütunlar gözüksün diye seçtim sonra arama kısmından protokolleri aradım

TCP

DNS

HTTP

6. HTTP protokolüne ait paket bilgilerini görüntülemek için hangi ifade ile filtreleme yapılmadır? İlgili filtrelemeyi yaparak ekran görüntüsü ile gösteriniz

Aşağıdaki kısıma http yazarak filtrelenmesini sağlayabiliriz.
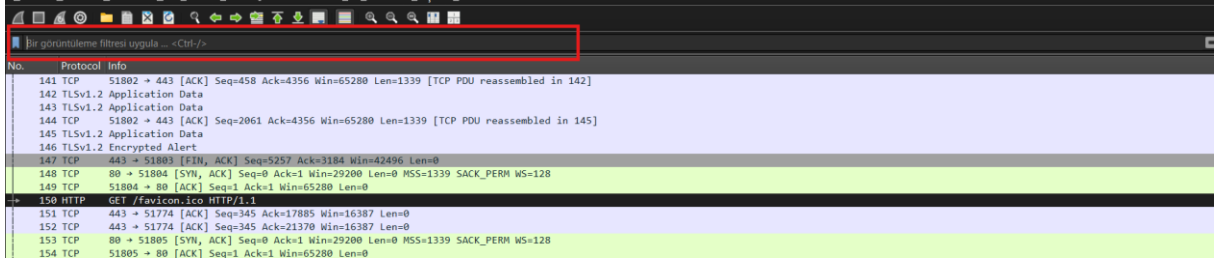
Sonuç
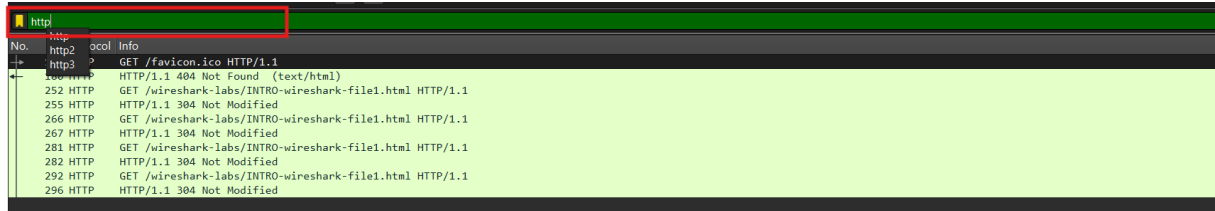
7. HTTP paketlerinin gönderilip alınması adımları arasında dinlenen ağda başka paket alışverişi olmuş mudur? Ekran görüntüsü ile gösteriniz.

Olmuş. 150 nolu ve 180 nolu paketler arasında http dışı paket alışverişi olmuş

```
148 TCP       80 → 51804 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1339 SACK_PERM WS=128
149 TCP       51804 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
150 HTTP      GET /favicon.ico HTTP/1.1
151 TCP       443 → 51774 [ACK] Seq=345 Ack=17885 Win=16387 Len=0
152 TCP       443 → 51774 [ACK] Seq=345 Ack=21370 Win=16387 Len=0
153 TCP       80 → 51805 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1339 SACK_PERM WS=128
154 TCP       51805 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
155 TCP       443 → 51774 [ACK] Seq=345 Ack=28429 Win=16387 Len=0
156 TCP       443 → 51774 [ACK] Seq=345 Ack=33253 Win=16387 Len=0
157 TCP       443 → 51774 [ACK] Seq=345 Ack=34592 Win=16387 Len=0
158 TCP       443 → 51774 [ACK] Seq=345 Ack=37270 Win=16387 Len=0
159 TCP       443 → 51774 [ACK] Seq=345 Ack=39948 Win=16387 Len=0
160 TCP       443 → 51774 [ACK] Seq=345 Ack=42073 Win=16387 Len=0
161 TCP       443 → 51774 [ACK] Seq=345 Ack=44751 Win=16387 Len=0
162 TCP       443 → 51774 [ACK] Seq=345 Ack=46898 Win=16387 Len=0
163 TCP       443 → 51774 [ACK] Seq=345 Ack=49576 Win=16387 Len=0
164 TCP       443 → 51774 [ACK] Seq=345 Ack=52254 Win=16387 Len=0
165 TCP       443 → 51774 [ACK] Seq=345 Ack=57202 Win=16373 Len=0
166 TCP       [TCP Window Update] 443 → 51774 [ACK] Seq=345 Ack=57202 Win=16387 Len=0
167 TLSv1.2   Application Data
168 TLSv1.2   Application Data, Application Data, Application Data
169 TCP       51774 → 443 [ACK] Seq=70655 Ack=1046 Win=255 Len=0
170 TCP       443 → 51774 [ACK] Seq=1046 Ack=62026 Win=16387 Len=0
171 TCP       443 → 51774 [ACK] Seq=1046 Ack=63365 Win=16387 Len=0
172 TCP       443 → 51774 [ACK] Seq=1046 Ack=66043 Win=16387 Len=0
173 TCP       443 → 51774 [ACK] Seq=1046 Ack=68721 Win=16387 Len=0
174 TCP       443 → 51774 [ACK] Seq=1046 Ack=70655 Win=16387 Len=0
175 TLSv1.2   Application Data
176 TCP       443 → 51802 [ACK] Seq=4394 Ack=3400 Win=4195072 Len=0
177 TCP       51802 → 443 [ACK] Seq=4722 Ack=4394 Win=65280 Len=0
178 TCP       443 → 51802 [ACK] Seq=4394 Ack=4722 Win=4193536 Len=0
179 TCP       80 → 51804 [ACK] Seq=1 Ack=455 Win=30336 Len=0
180 HTTP      HTTP/1.1 404 Not Found  (text/html)
181 TLSv1.2   Application Data
```

Ayrıca paket kısmına !http yazarak da http olmayan paketleri görebiliriz görebiliriz


```
!http

No.    Protocol Info
     1 TLSv1.2  Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
     2 TLSv1.2  Change Cipher Spec, Encrypted Handshake Message, Application Data
     3 TLSv1.2  Application Data
     4 TCP      51801 → 443 [ACK] Seq=246 Ack=121 Win=255 Len=1339 [TCP PDU reassembled in 5]
     5 TLSv1.2  Application Data
     6 TLSv1.2  Application Data
     7 TCP      51801 → 443 [ACK] Seq=1817 Ack=121 Win=255 Len=1339 [TCP PDU reassembled in 10]
     8 TCP      51801 → 443 [ACK] Seq=3156 Ack=121 Win=255 Len=1339 [TCP PDU reassembled in 10]
     9 HTTP     51801 → 443 [ACK] Seq=4495 Ack=121 Win=255 Len=1339 [TCP PDU reassembled in 10]
    10 TLSv1.2  Application Data
    11 TLSv1.2  Application Data
    12 TCP      443 → 51801 [ACK] Seq=159 Ack=1817 Win=16387 Len=0
    13 TCP      443 → 51801 [ACK] Seq=159 Ack=3156 Win=16387 Len=0
    14 TCP      443 → 51801 [ACK] Seq=159 Ack=4495 Win=16387 Len=0
    15 TCP      443 → 51801 [ACK] Seq=159 Ack=5834 Win=16387 Len=0
    16 TCP      51801 → 443 [ACK] Seq=7012 Ack=159 Win=255 Len=0
    17 TCP      443 → 51801 [ACK] Seq=159 Ack=7012 Win=16382 Len=0
    18 TCP      51774 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 21]
    19 TCP      51774 → 443 [ACK] Seq=1340 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 21]
    20 TCP      51774 → 443 [ACK] Seq=2679 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 21]
    21 TLSv1.2  Application Data
    22 TCP      51774 → 443 [ACK] Seq=4836 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    23 TCP      51774 → 443 [ACK] Seq=6175 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    24 TCP      51774 → 443 [ACK] Seq=7514 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    25 TCP      51774 → 443 [ACK] Seq=8853 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    26 TCP      51774 → 443 [ACK] Seq=10192 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    27 TCP      51774 → 443 [ACK] Seq=11531 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    28 TCP      51774 → 443 [ACK] Seq=12870 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in 29]
    29 TLSv1.2  Application Data
    30 TCP      51613 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
    31 TCP      443 → 51613 [ACK] Seq=1 Ack=2 Win=16385 Len=0 SLE=1 SRE=2
    32 TCP      443 → 51774 [ACK] Seq=1 Ack=4836 Win=16387 Len=0
    33 TCP      443 → 51774 [ACK] Seq=1 Ack=7514 Win=16387 Len=0
    34 TCP      [TCP Retransmission] 51774 → 443 [PSH, ACK] Seq=13833 Ack=1 Win=253 Len=1339 [TCP PDU reassembled in
    35 TLSv1.2  Application Data
    36 TLSv1.2  Application Data
```
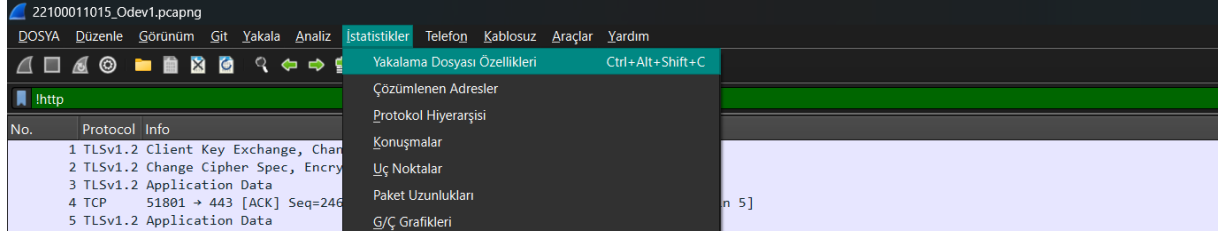
Ek Olarak:

Kısmından sorduğunuz birkaç soru dahil çoğu bilgiye ulaşabiliriz