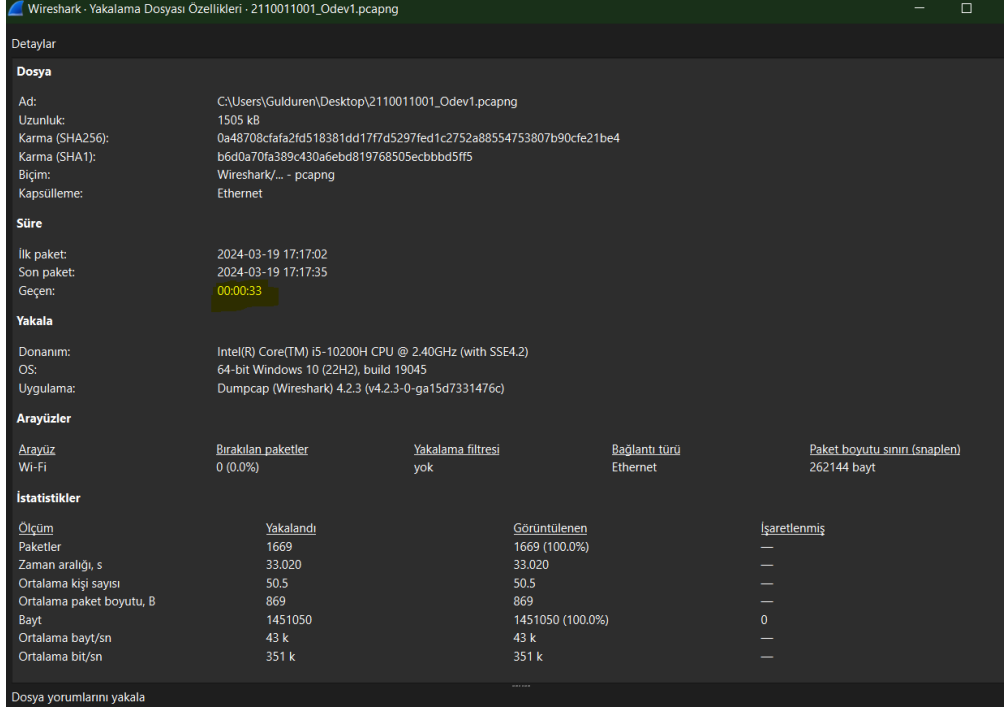


DERYA NAİLİYE KIMIRTI – 21100011001

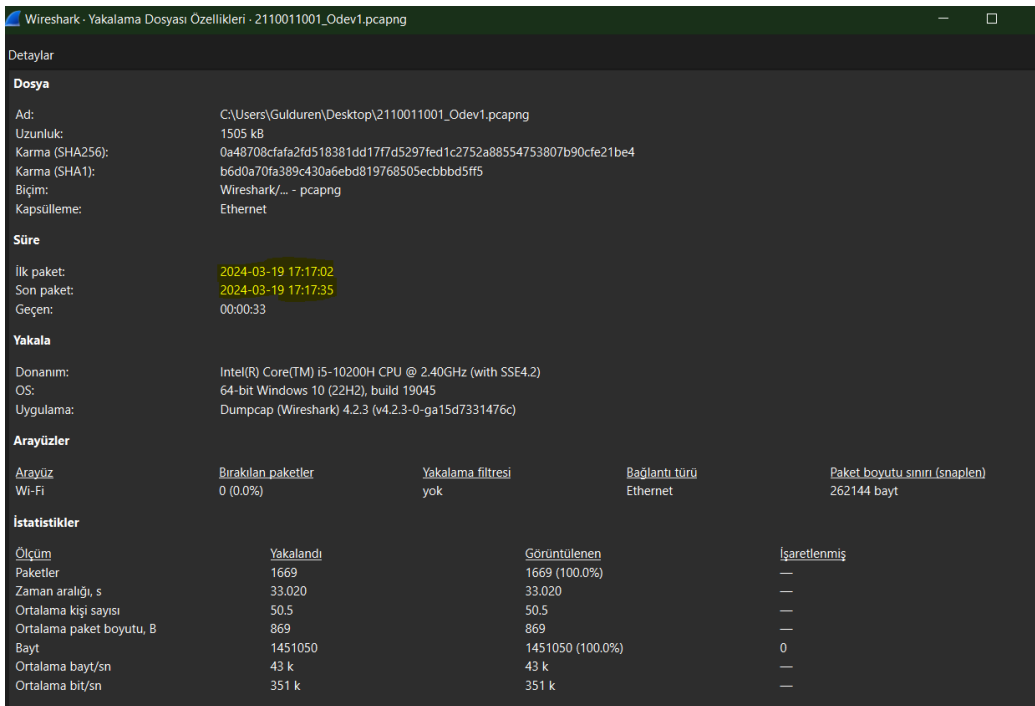
1- Paket yakalama işleminizin toplam süresi ne kadardır? Bu bilgiyi nasıl elde ettiniz?

- ➔ İstatistikler menüsünden “Yakalama Dosyası Özellikleri”ni seçtiğimizde yakaladığımız paketlerin detaylı açıklaması ekran görüntüsünde yer almaktadır. Sarı renkle belirtilen süre paket yakalama işlem süremizi göstermektedir.
- ➔ Paket yakalama işleminizin toplam süresi: 00:00:33



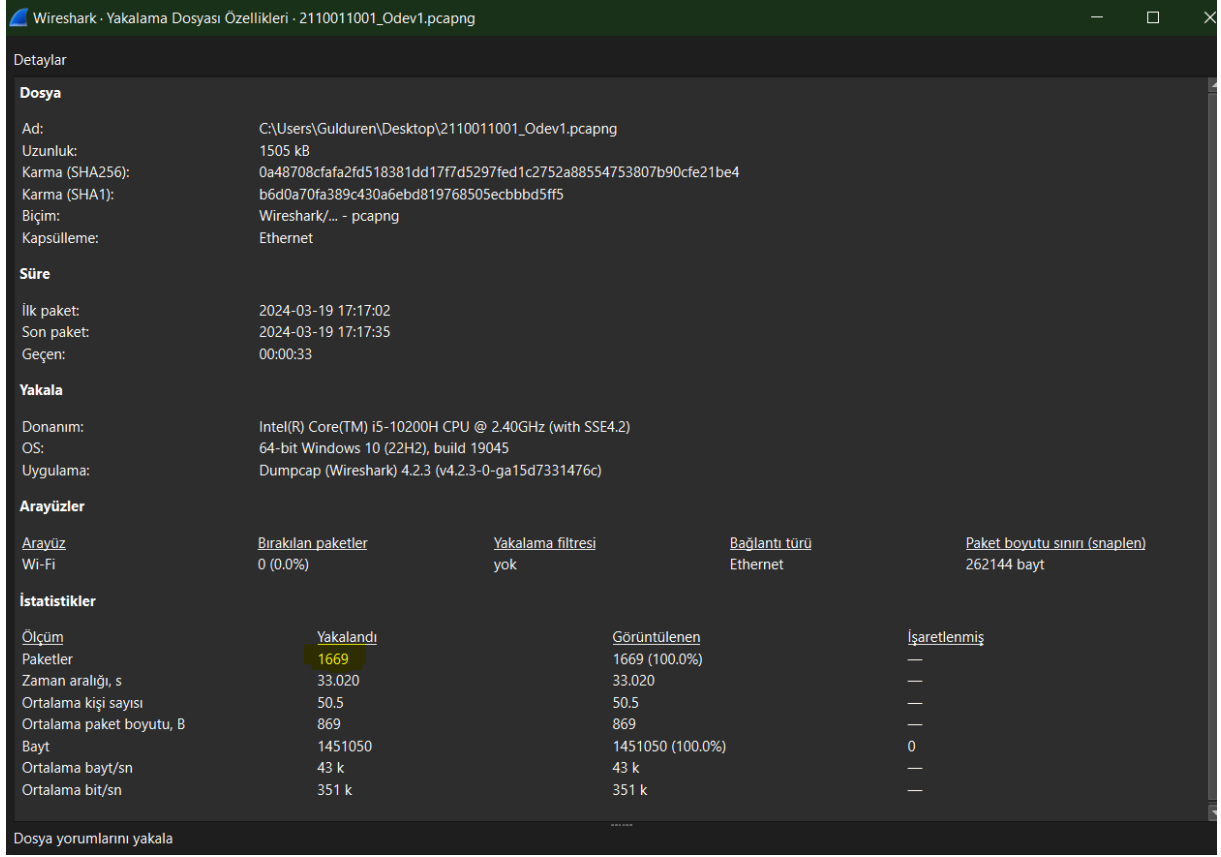
2- Paket yakalama işleminin gerçek başlangıç ve bitiş zamanını (günün tarihi ve işlem zamanı) ekran görüntüsü ile belirtiniz. Bu bilgiyi görebilmek için Wireshark programında hangi işlem yapılmalıdır?

- ➔ İstatistikler menüsünden “Yakalama Dosyası Özellikleri”ni seçtiğimizde yakaladığımız paketlerin detaylı açıklaması ekran görüntüsünde yer almaktadır.
- ➔ Sarı renkle belirtilen “ilk paket: 2024-03-19 17:17:02” ve “son paket: 2024-03-19 17:17:35” bilgileri paket yakalama işleminin gerçek başlangıç ve bitiş zamanını göstermektedir.



3- Toplam yakalanan paket sayısı kaçtır?

- İstatistikler menüsünden “Yakalama Dosyası Özellikleri”ni seçtiğimizde yakaladığımız paketlerin detaylı açıklaması ekran görüntüsünde yer almaktadır.
- Yakalanan toplam paket: 1669



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

- Yakalanan paket sayısı:1669
- Geçen süre: (33 sn) 33000 ms
- Trafik hızım: (paket/ms)= $1669/33000 = 0,05057$ paket/ms

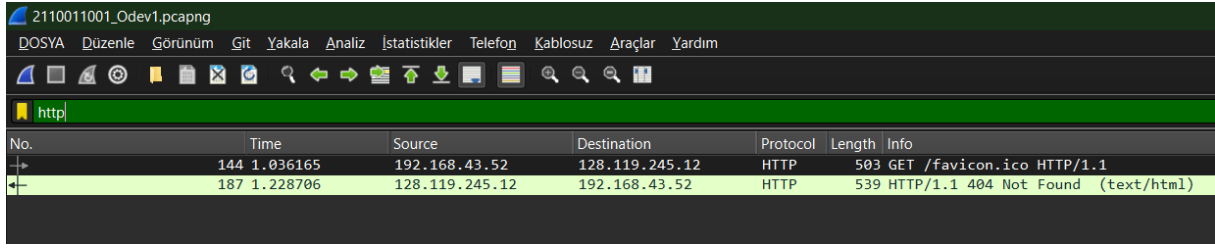
5- Yakalanan paketlerden 3 farklı protokole ait paketlerin paket no, protokol ve bilgi kısımlarını yazınız.

149	1.042280	192.168.43.52	142.250.187.138	TCP	66 49902 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
150	1.052031	216.58.213.99	192.168.43.52	QUIC	66 Protected Payload (KP0)
151	1.057993	142.251.140.74	192.168.43.52	TLSv1.3	1442 Server Hello, Change Cipher Spec

Paket no:	Protokol:	Bilgi:
149	TCP	49902 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
150	QUIC	Protected Payload (KP0)
151	TLSv1.3	Server Hello, Change Cipher Spec

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

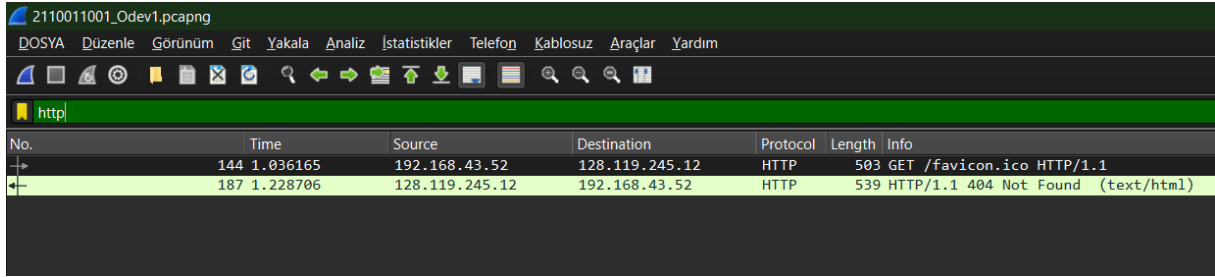
“Bir görüntüleme filtresi uygula” kısmından arama kısmına “http” diye arattığımızda http protokolüne ait bilgileri görüntülemek için filtreleme yapılır.



No.	Time	Source	Destination	Protocol	Length	Info
144	1.036165	192.168.43.52	128.119.245.12	HTTP	503	GET /favicon.ico HTTP/1.1
187	1.228706	128.119.245.12	192.168.43.52	HTTP	539	HTTP/1.1 404 Not Found (text/html)

7- HTTP paketleri arasında başka paket alışverişi olmuş mudur? Ekran görüntüsü ile gösteriniz.

- Evet olmuştur.
- “Bir görüntüleme filtresi uygula” kısmından arama kısmına “http” diye arattığımızda http protokolüne ait bilgileri görüntülemek için filtreleme yapılır.
- Yapılan filtrelemede “144” ve “187” paket nolu iki tane http paketleri yakalanmıştır.
- 144’ten 187’ye atlama gerçekleştiğine göre bu http paketleri arasında başka paket alışverişi gerçekleşmiştir.



No.	Time	Source	Destination	Protocol	Length	Info
144	1.036165	192.168.43.52	128.119.245.12	HTTP	503	GET /favicon.ico HTTP/1.1
187	1.228706	128.119.245.12	192.168.43.52	HTTP	539	HTTP/1.1 404 Not Found (text/html)