18 Nisan 2021

Engin Karataş

16008118040

Bilgisayar ağları

TCP FÖY RAPORU

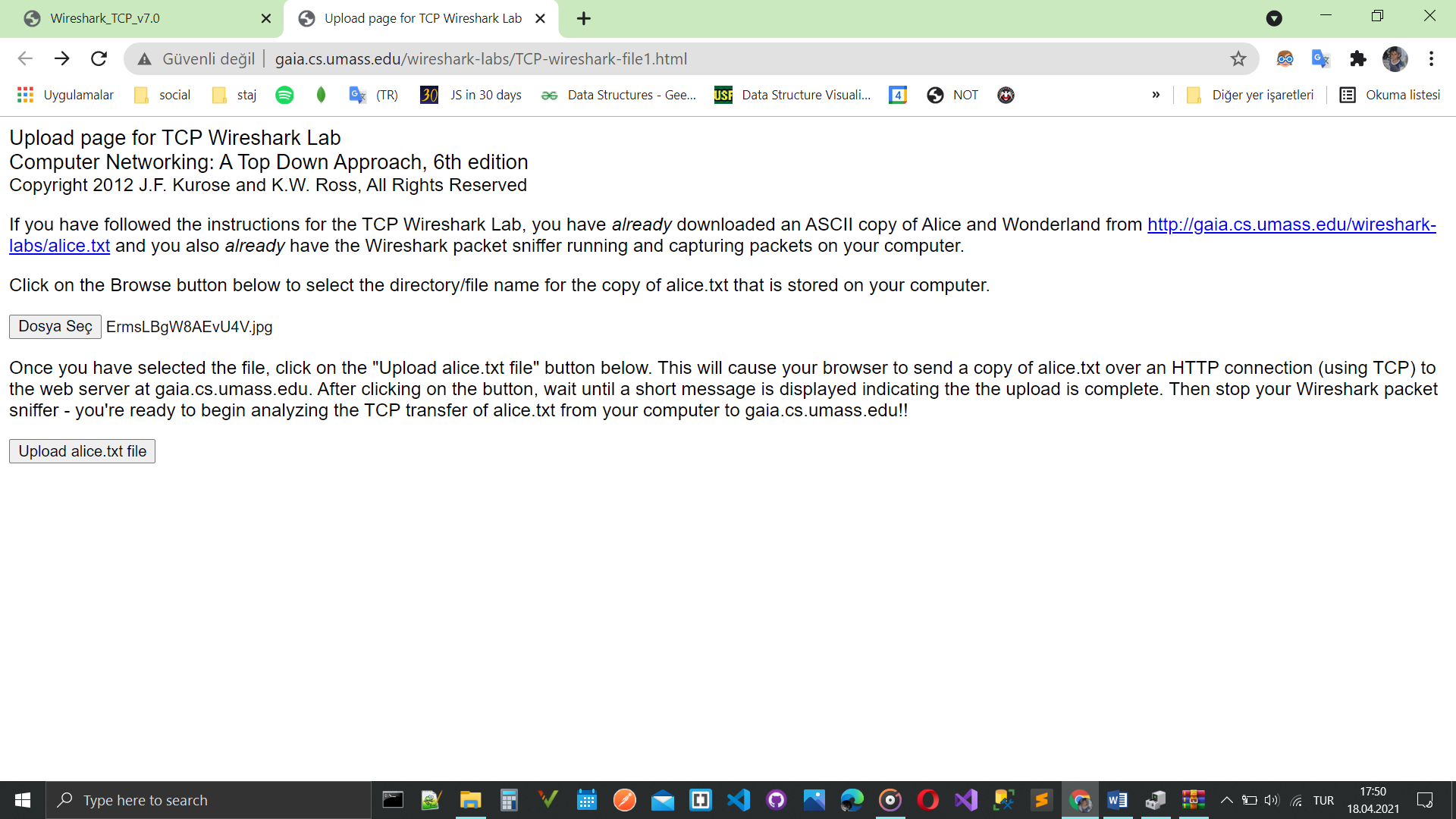
BİLGİSAYAR AĞLARI TCP FÖY RAPORU

# Föy Wireshark\_TCP\_v7.0

TCP veri iletimini sağlayan bir protokoldür. http, tcp ile birlikte kullanılır. Wireshark\_TCP\_v7.0 adlı dökümanımızda da, bilgisayar ortamında tcp protokolü paketlerinin nasıl capture ediliği, nasıl analiz edildiği, ve giden dataların grafiksel olarak nasıl analiz edildiği hususunda temel bilgiler içermektedir. TCP congestion control algorithm yani TCP tıkanıklık kontrol algoritmasını incelenmiştir. Yine TCP nin slow start and cogestion avoidance yani yavaş başlangıç ve tıkanıklıktan kaçınma konusunda bilgiler verilmiştir. Wireshark uygulamasında nasıl capture işlemi yapılabileceğini, filteleme metodlarının nasıl çalıştırılacağını ve istenmeyen protokollerin(örneğin http) nasıl gizleneceği anlatılmıştır.

TCP protokolünün, kaynağa giderken ve acknowladgement döndürürkenki süresi hakkında bilgiler verilmiş, bu süreninin verimi ile ilgili bahsedilmiştir. İlgili paketlerin capturingi hakkında örneklemeler yapılmış, verilen link üzerinden post işlemi gerçekleştirilmiş, paketler incelenmiştir. İncelenen paketlerin makaleyi okuyan öğrencilerin kavramasına bırakılmıştır. Paketlerin içeriğinin ne olduğu hakkında bilgi verilmemiştir.

Statics->TCP Stream Graph->TimeSequenceGraph tab yolu üzerinde bulunun TCP nin giden ve gelen paketlerin görsel bir şekilde gösterilebileceği, izlenebileceği TCP-Graph grafiği gösterilmiştir. Bu grafikte zamana göre sıra numarasının(sequence number) değerleri bulunmaktadır.



Yukarıda doküman tarafından linki verilen dosya seç butonuyla alice.txt dosyası sisteme yüklenir ve TCP protokolü, dökümanın verdiği adımlar sayesinde capture edilir.

Dökümanda verilen http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip yolu indirilmeli, içerisindeki tcp-ethereal-trace-1 dosyası wireshark tarafından açıldıktan sorna, filtre kısmına tcp yazıp enter`a basılmalıdır. Böyelce protokolü tcp olan paketleri görmüş oluruz. Örneğin buradaki soruları cevaplayalım:

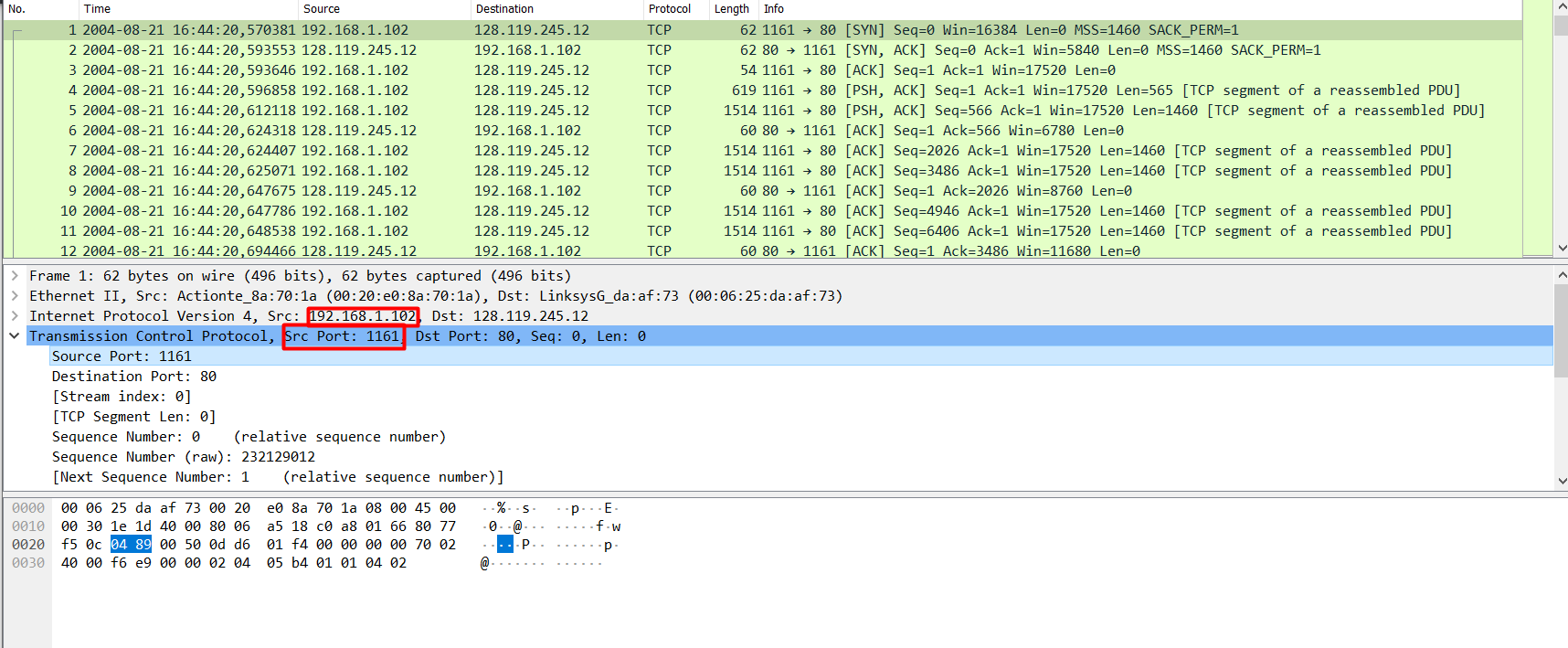
Başlamadan önce

**SYN - (Senkronize et) Bir bağlantı başlatır**

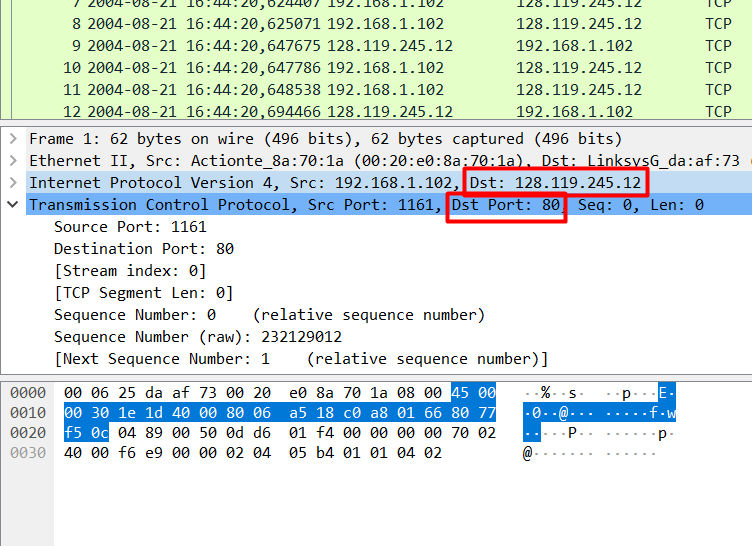
**FIN - (Son) Bir bağlantıyı temiz bir şekilde sonlandırır**

**ACK - Alınan verileri onaylar**

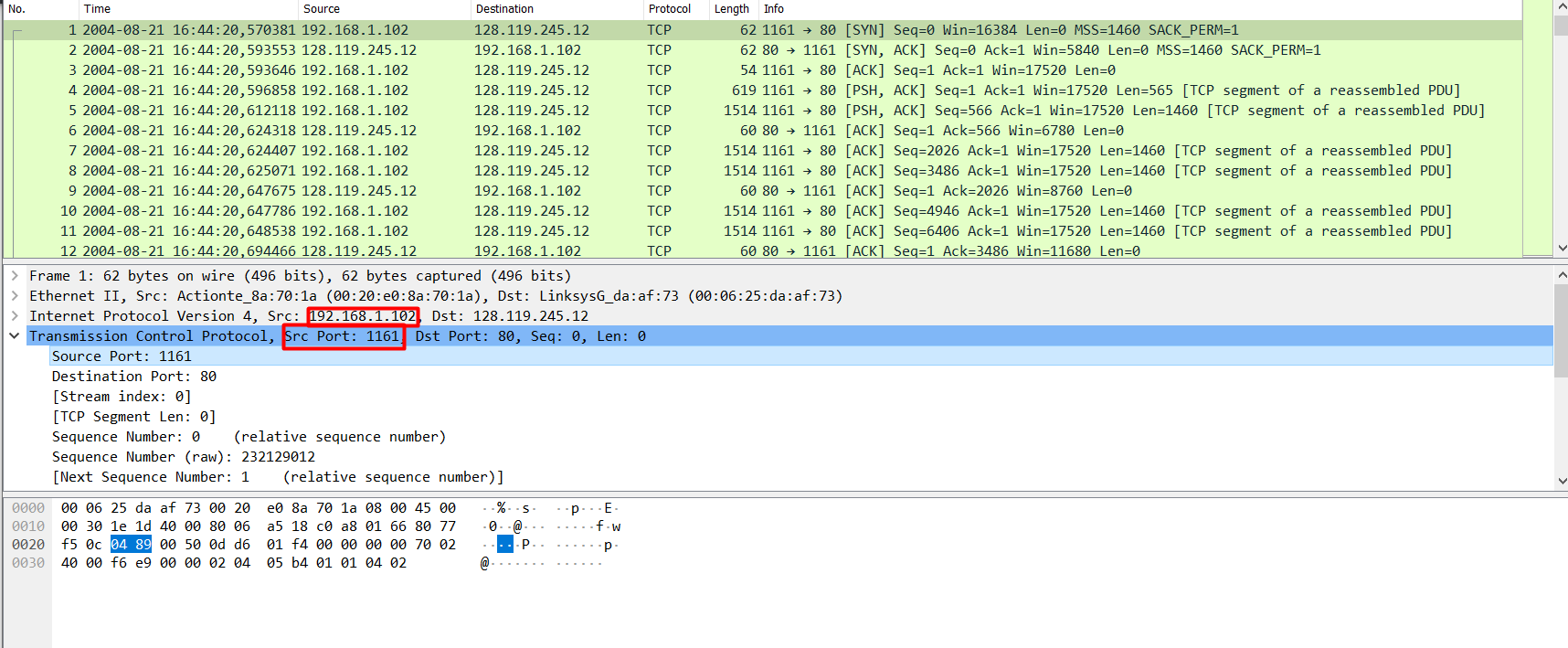
Dosyayı gaia.cs.umass.edu'ya aktaran istemci bilgisayar (kaynak) tarafından kullanılan IP adresi ve TCP bağlantı noktası numarası nedir?



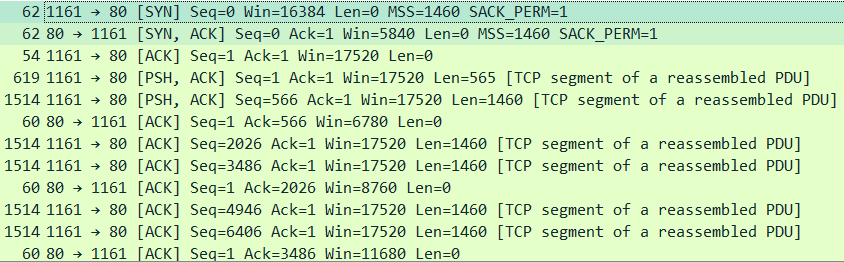
2. gaia.cs.umass.edu'nun IP adresi nedir? Bu bağlantı için hangi bağlantı noktası numarasında TCP segmentleri gönderiyor ve alıyor?



3. İstemci bilgisayarınız (kaynak) tarafından dosyayı gaia.cs.umass.edu'ya aktarmak için kullanılan IP adresi ve TCP bağlantı noktası numarası nedir?



4.İstemci bilgisayar ile gaia.cs.umass.edu arasındaki TCP bağlantısını başlatmak için kullanılan TCP SYN segmentinin sıra numarası nedir?



Burada sıra numarası :

Bir TCP oturumunun her iki tarafındaki istemci, ne kadar veri gönderdiğini takip etmek için kullandığı 32 bitlik bir sıra numarası tutar.



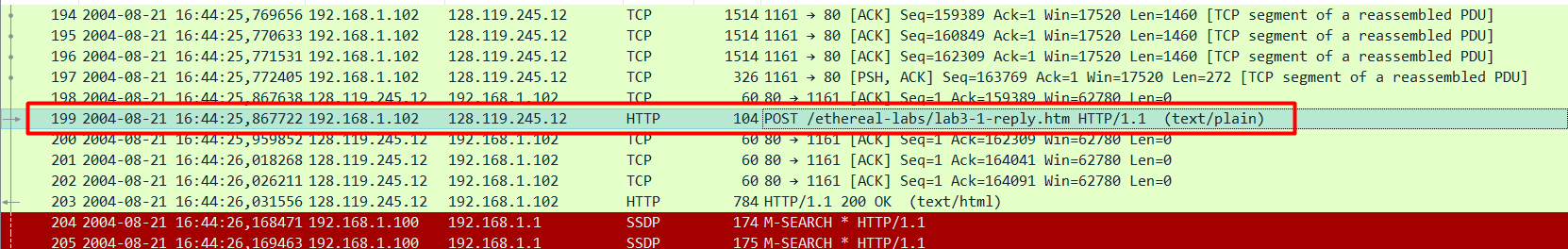
Segmenti bir SYN segmenti olarak tanımlayan segmente nedir?

SYN seqmenti

5. gaia.cs.umass.edu tarafından SYN'ye yanıt olarak istemci bilgisayara gönderilen SYNACK segmentinin sıra numarası nedir?

C:\Users\sona\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Screenshot_8.png

6. HTTP POST komutunu içeren TCP segmentinin sıra numarası nedir?



http.request.method == "POST" yazarak post işlemleri bulunabilir veya yukarıdaki gibi info kısmında post kelimesi aranmalıdır.

8. What is the length of each of the first six TCP segments?

1-0

2-0

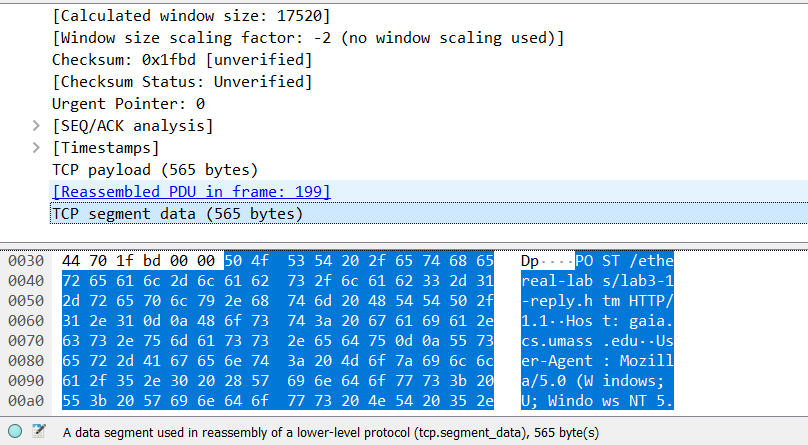
3-0

4-565

5-1460

6-0

8. İlk altı TCP kesiminin her birinin uzunluğu nedir?



565 byte olduğu görülür

10. Are there any retransmitted segments in the trace file? What did you check for (in

the trace) in order to answer this question?

Hayır yok. Ack ve sequance yi kontrol ettim . aynı kayıtlar yok