

TCP ATÖLYESİ

ATÖLYENİN HEDEFİ:

Bu atölyede TCP paketinin nasıl alındığını öğreneceksiniz.

ATÖLYENİN AMACI:

Transmission Control Protocol (TCP), TCP/IP'nin ilk kısmıdır. Telnet, FTP ve BGP gibi bazı yönlendirme protokolleri gibi bağlantı odaklı hizmetlerin ve protokollerin ağlar üzerinden çalışmasını sağlar

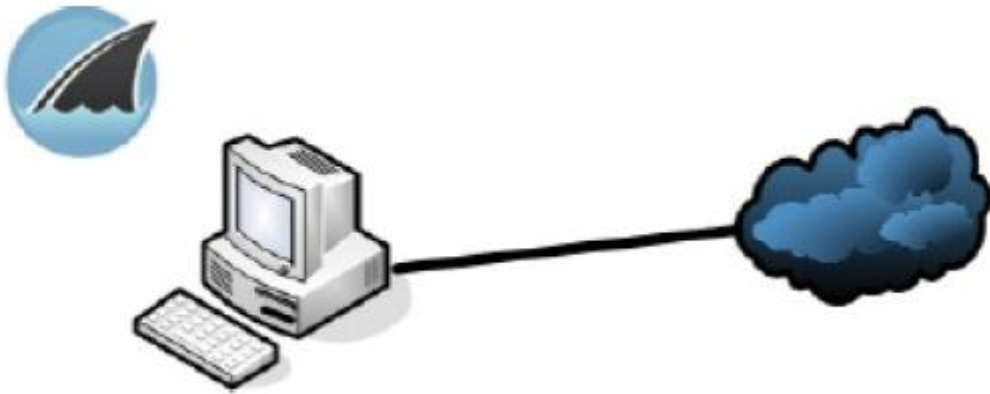
ATÖLYE ARACI:

Wireshark'ı ev bilgisayarınızda da aynı kolaylıkla çalıştırabilirsiniz.

Bir Telnet/SSH istemcisi olan Putty'yi kurun. Putty'yi <https://putty.org/> adresinden indirebilirsiniz. Putty, Telnet'i kullanmayı çok daha kolay hale getirir çünkü çoğu istemci yazılımı Telnet'i varsayılan olarak devre dışı bırakıyor.

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.

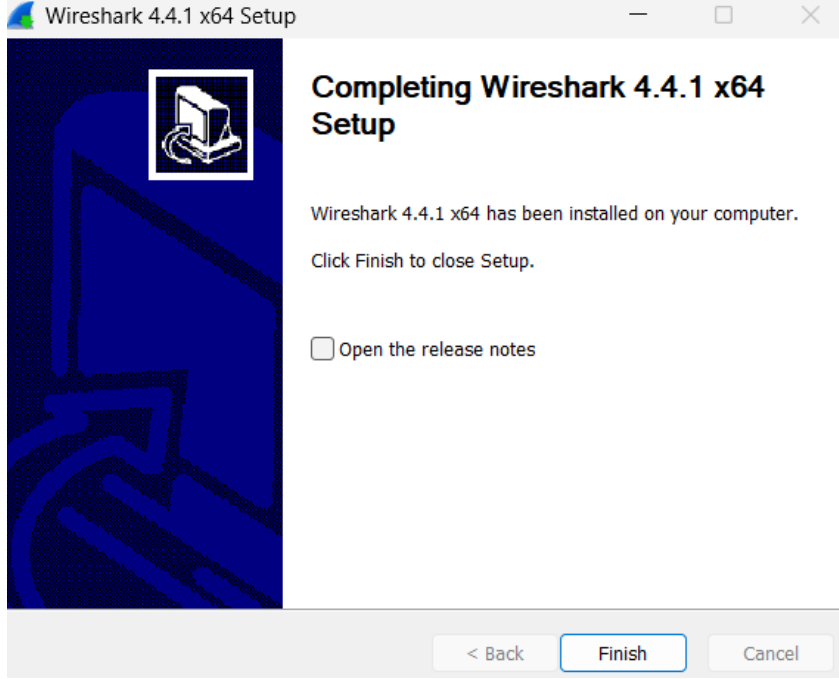


ATÖLYE ANLATIMI:

Adım 1:

<https://www.wireshark.org/download.html> Adresine giderek sisteminize uygun wireshark'ı indirin ve bilgisayarınıza kurun.

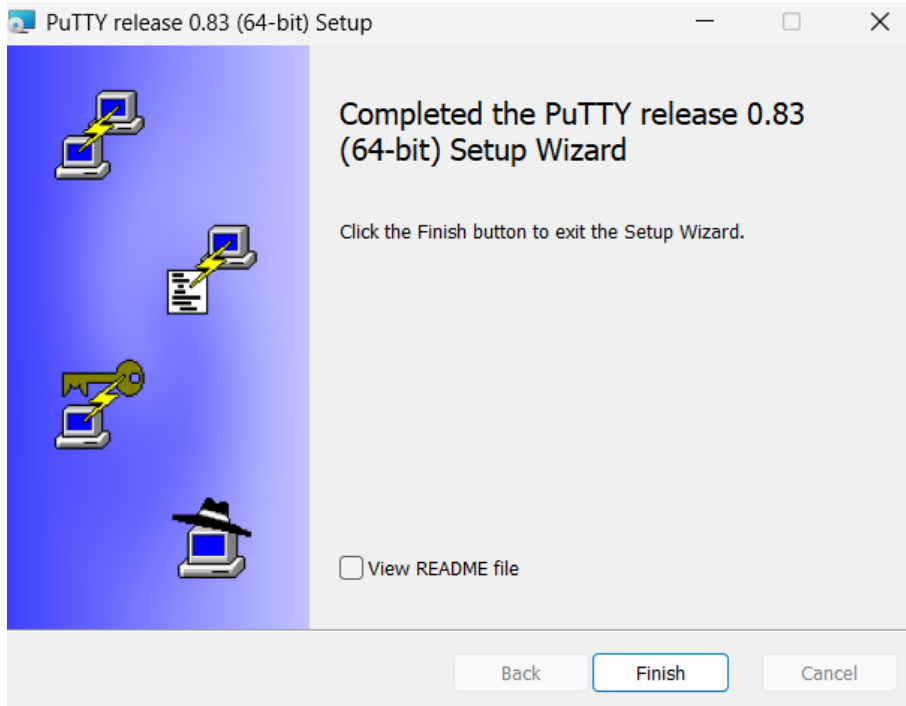
Wireshark kurulduğunda aşağıdaki ekranı göreceğiz:



Adım 2:

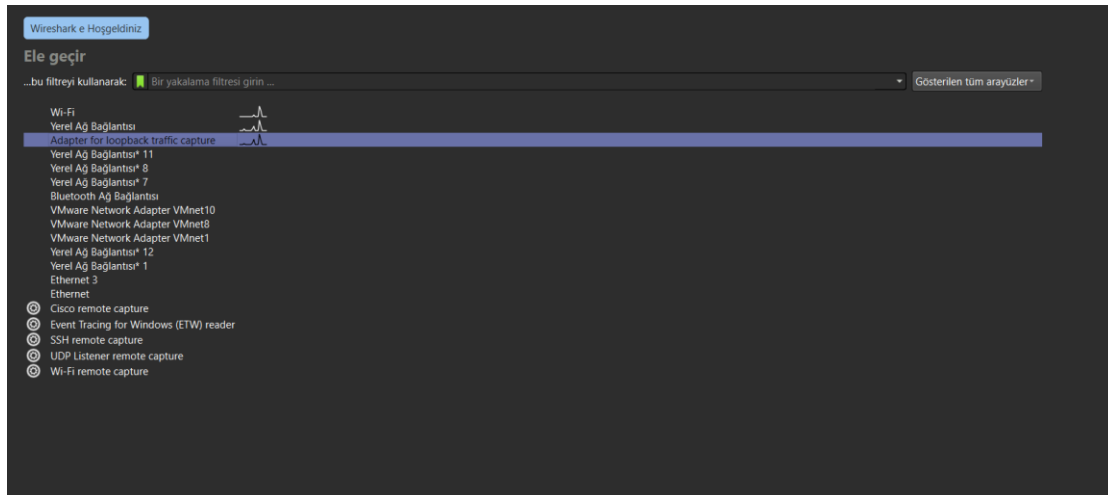
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html> Adresinden bilgisayarımıza uygun olan kurulum dosyasını indirelim.

İndirme işlemi sonunda aşağıdaki ekranla karşılaşacağız:



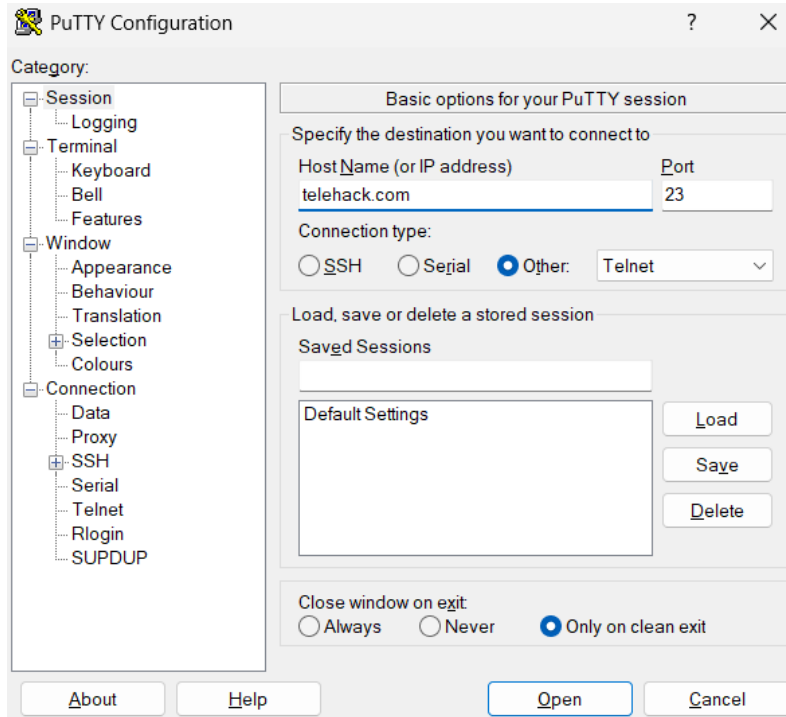
Adım 3:

wireshark'ı açalım ve sniff etmek istediğimiz bağlantıyı seçelim. Ben “yerel ağ bağlantısı”'nı seçtim.



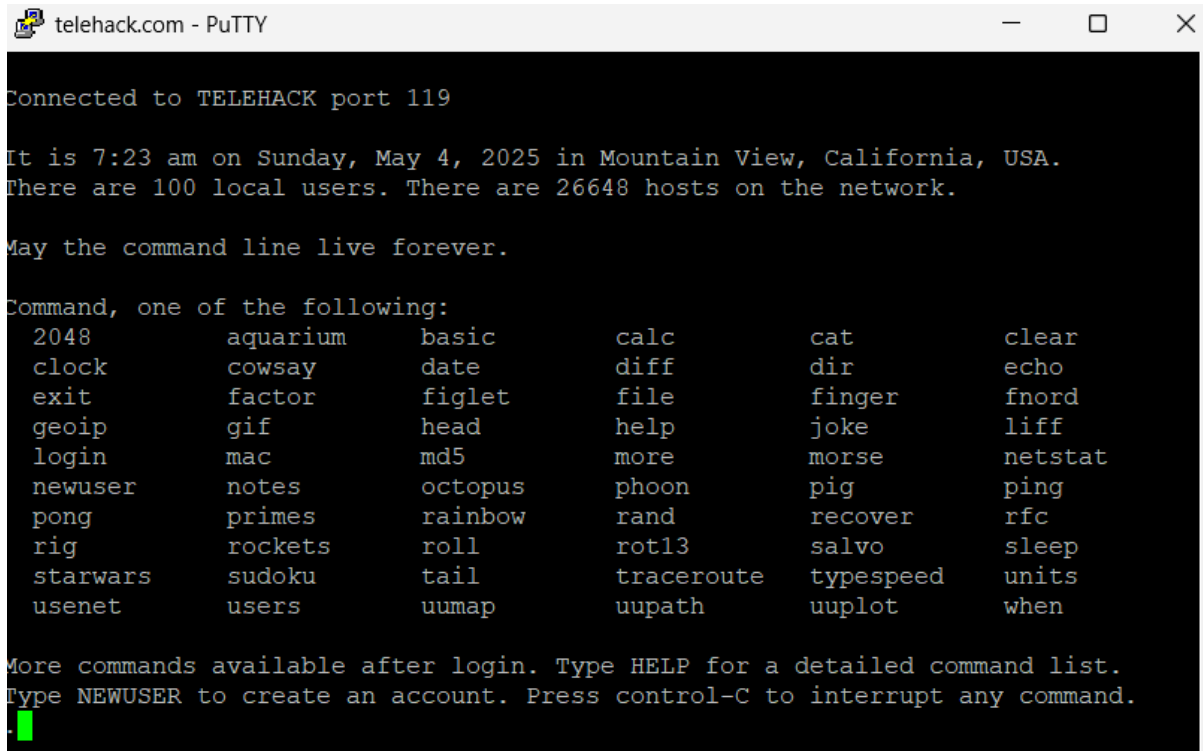
Adım 4:

Putty'yi açarak host name kısmına telehack.com yazıp 23 portunu seçip Other diyerek Telnet'i seçelim.



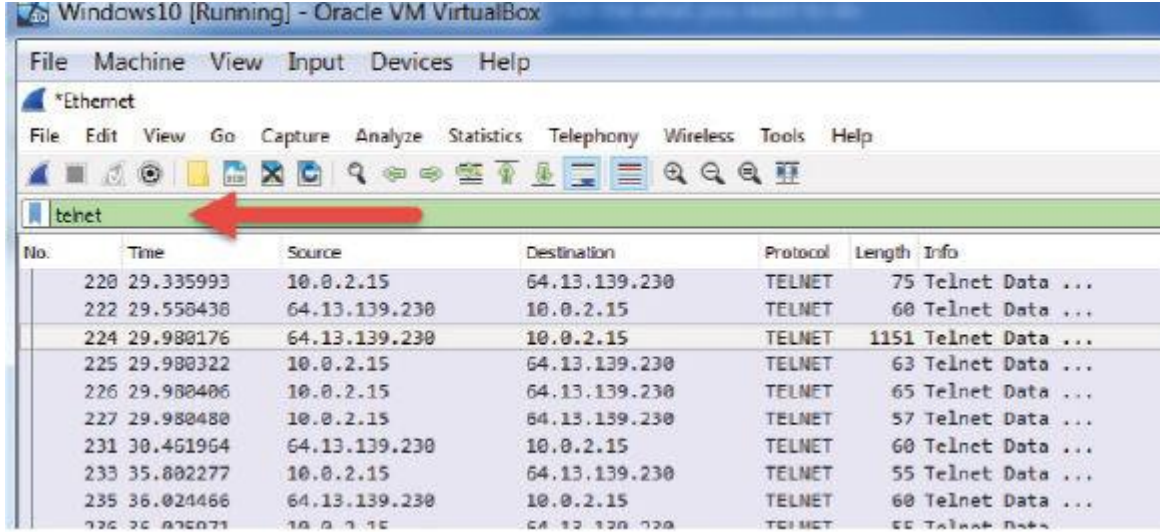
Adım 5:

Open yazısına basalım. Eğer aşağıdaki ekran çıkarsa başarılı olmuşuz demektir.



Adım 6:

Wiresharka geri dönerek filtre kısmına telnet yazalım. Ok işaretine basarak telnet paketlerini filtrelemiş oluruz.

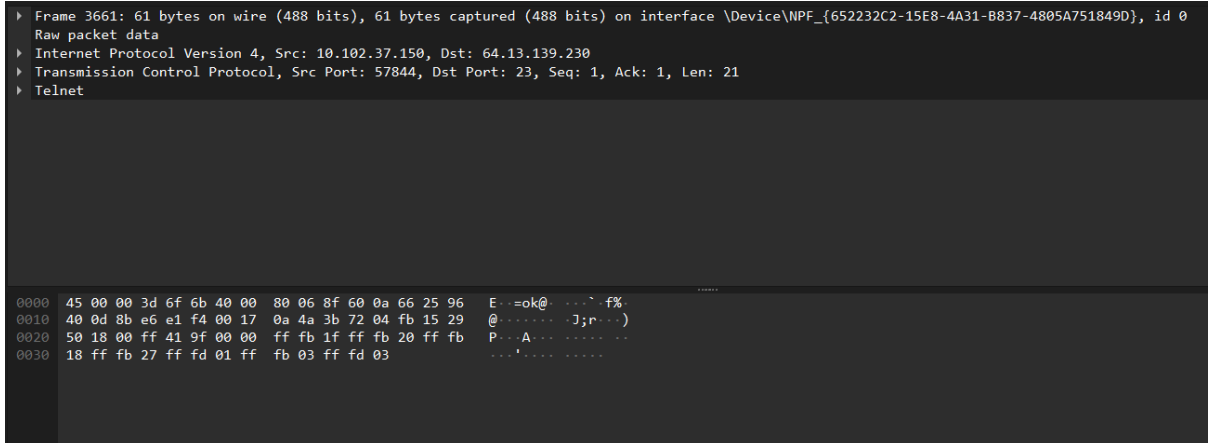


Adım 7:

Paketlerden birine tıklarsanız, daha fazla ayrıntıya inebilirsiniz. Lütfen

Telnet'in kullandığı 'TCP' yazdığına dikkat edin. Alanları aşağıdaki TCP paketinin görüntüsüyle karşılaştırın. Kaç alanı görebileceğinize bakın.

Kaynak portunun 23 olduğunu görebilirsiniz, ki bu elbette Telnet'tir.



Adım 8:

TCP paket formatı aşağıda görüldüğü gibidir.

TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags		Window Size			
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

Adım 9:

Son olarak, Telnet'in oturumun içeriklerini şifrelemediğini unutmayın, böylece veri akışında neyin gönderildiğini kolayca görebilirsiniz. Wireshark'ın alt penceresinde, Telnet üzerinden gönderilen gerçek verileri bulacaksınız.

```

PuTTY (inactive)
Connected to TELEHACK port 49

It is 5:49 pm on Sunday, September 9, 2018 in Mountain View, California, USA.
There are 30 local users. There are 26637 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
2048      ?      a2      ac      advent      basic
bf        c8      cal      calc      ching        clear
clock     cowsay   date      echo      eliza        factor
figlet    finger   fnord     geoip     help         hosts
ipaddr    joke      login     mac        md5          morse
newuser   notes     octopus   phoon     pig          ping
primes    privacy   qr        rain      rand         rfc
rig       roll      rot13     sleep     starwars     traceroute
units     uptime    usenet    users     uumap        uupath
uuplot    weather   when      zc        zork         zrun
  
```

```

02 0f 00 17 c2 9e 4a 07 2c 05 2e 3b 79 c3 50 10 .....J...y.P
ff ff e2 61 00 00 ff fb 01 ff fd 18 ff fd 1f 0d ...a.....
0a 43 6f 6e 6e 65 63 74 65 64 20 74 6f 20 54 45 ..Connect ed to TE
4c 45 48 41 43 4b 20 70 6f 72 74 20 34 39 0d 0a ..LEHACK p ort 49..
ff fe 20 ff fa 18 01 ff f0 ff fe 27 0d 0a 49 74 .. .. ..It
20 69 73 20 35 3a 34 39 20 70 6d 20 6f 6e 20 53 .. is 5:49 pm on S
75 6e 64 61 79 2c 20 53 65 70 74 65 6d 62 65 72 .. unday, S eptember
20 39 2c 20 32 30 31 38 20 69 6e 20 4d 6f 75 6e .. 9, 2018 in Moun
74 61 69 6e 20 56 69 65 77 2c 20 43 61 6c 69 66 .. tain Vie w, Calif
6f 72 6e 69 61 2c 20 55 53 41 2e 0d 0a 54 68 65 .. ornia, U SA..The
72 65 20 61 72 65 20 33 30 20 6c 6f 63 61 6c 20 .. re are 3 0 local
75 73 65 72 73 2e 20 54 68 65 72 65 20 61 72 65 .. users. T here are
20 32 36 36 33 37 20 68 6f 73 74 73 20 6f 6e 20 .. 26637 h osts on
  
```