Computer Network

AmirReza Azari
99101087

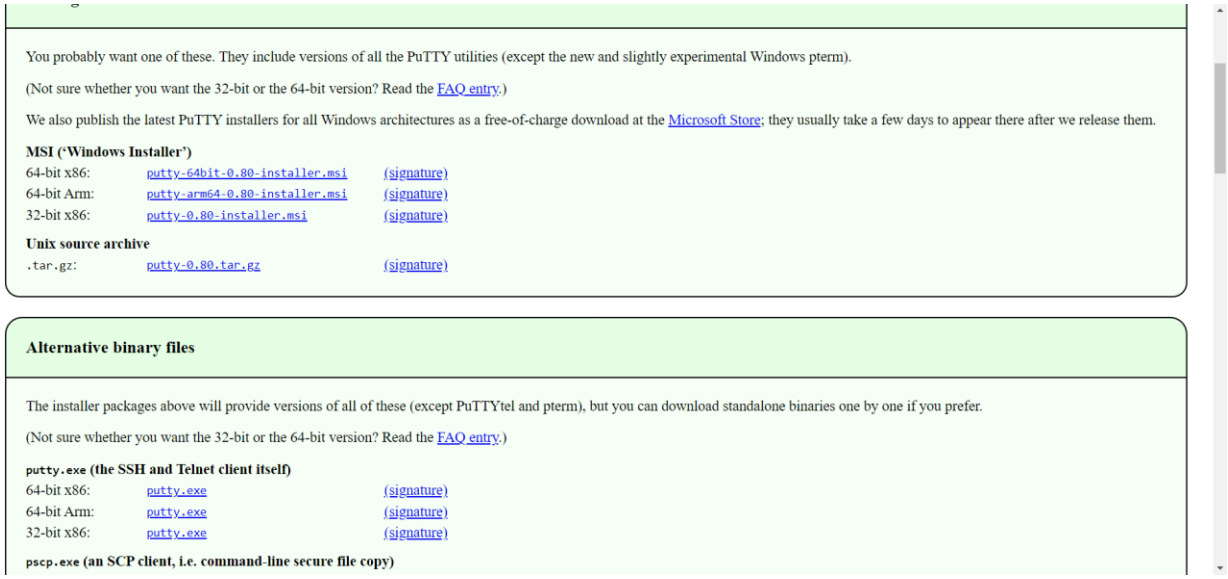
تمرین عملی اول

1. Telnet

1.1. اتصال از طریق Telnet

1.1.1. نصب و اجرا:

ابتدا putty را نصب و اجرا می‌نماییم. برای نصب از همان سایت ذکر شده کمک می‌گیریم. دقت نمایید روی سیستم عامل ویندوز این تمرین را انجام می‌دهیم.



You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the Microsoft Store; they usually take a few days to appear there after we release them.

MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.80-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.80-installer.msi	(signature)
32-bit x86:	putty-0.80-installer.msi	(signature)

Unix source archive

.tar.gz:	putty-0.80.tar.gz	(signature)

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you can download standalone binaries one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

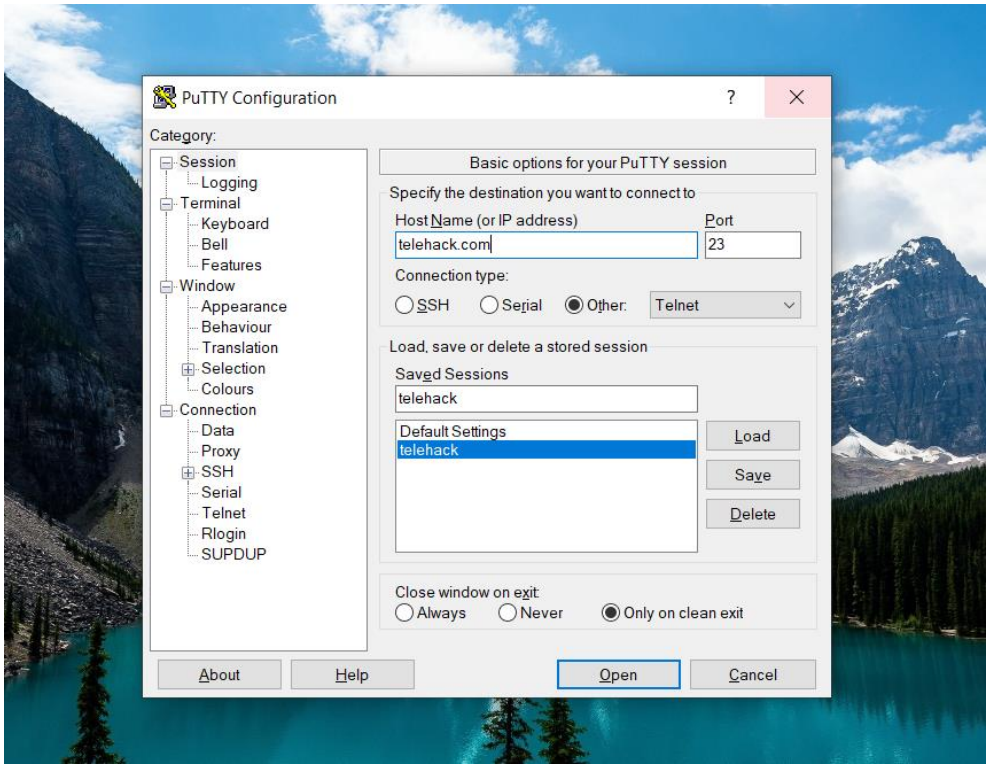
putty.exe (the SSH and Telnet client itself)

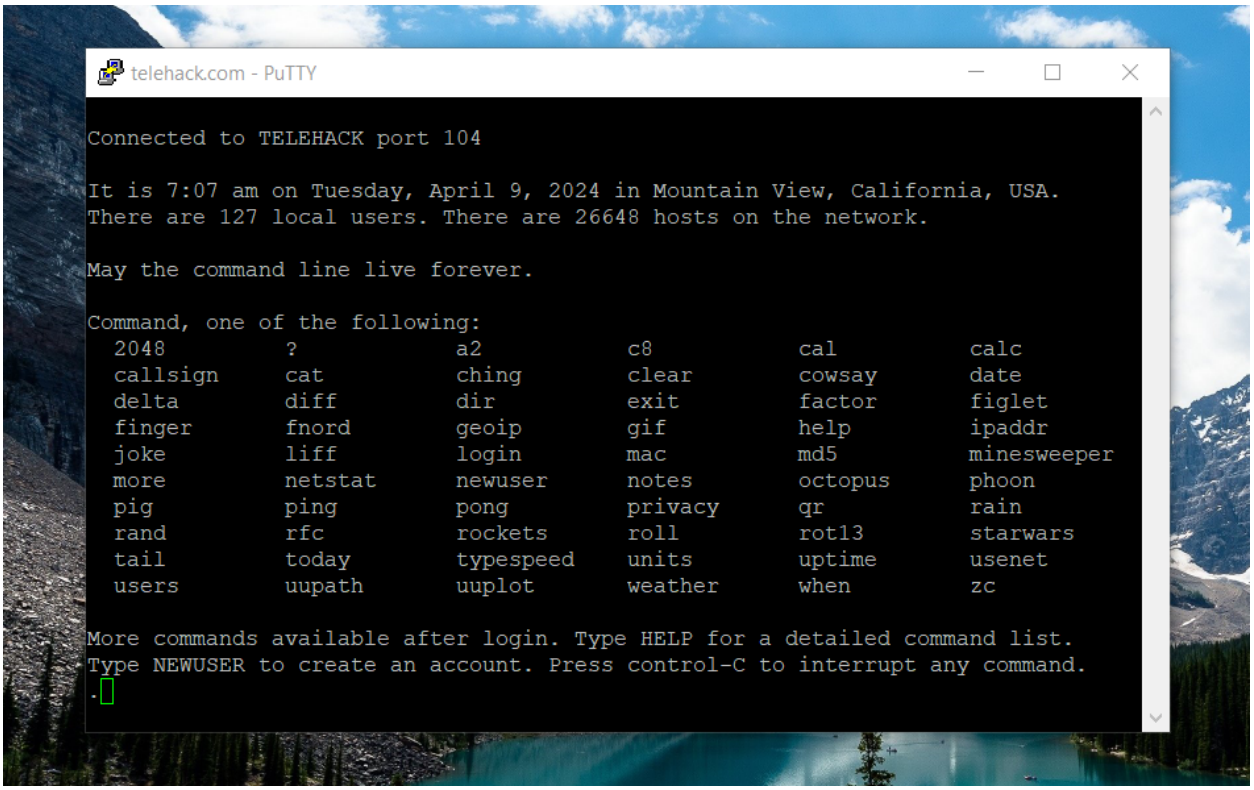
64-bit x86:	putty.exe	(signature)
64-bit Arm:	putty.exe	(signature)
32-bit x86:	putty.exe	(signature)

pscp.exe (an SCP client, i.e. command-line secure file copy)

1.1.2. اتصال به telehack.com روی پورت 23

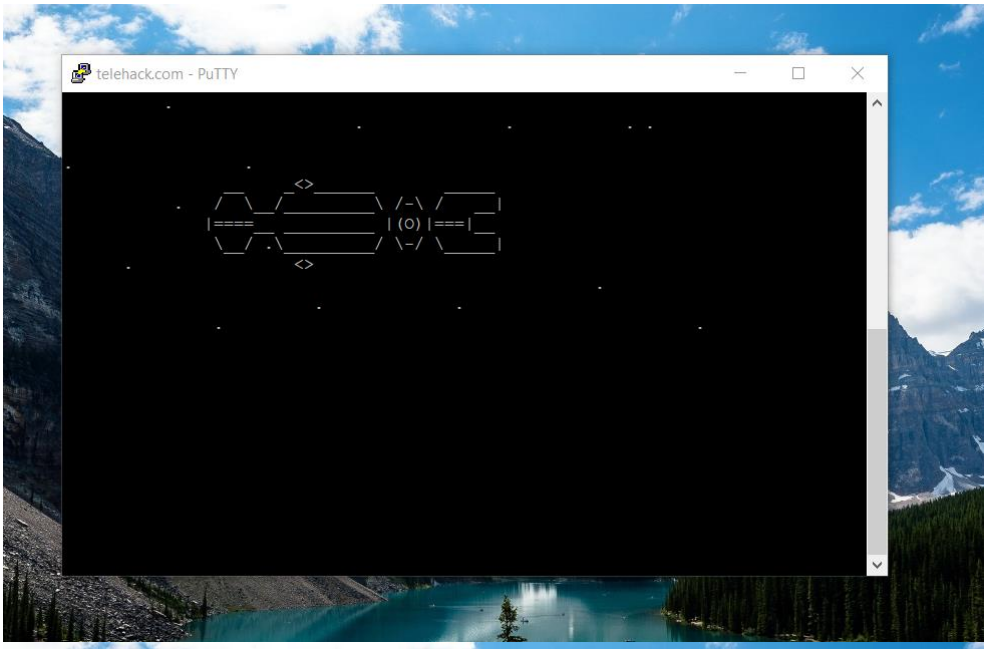
مانند تصویر زیر عمل می‌نماییم:

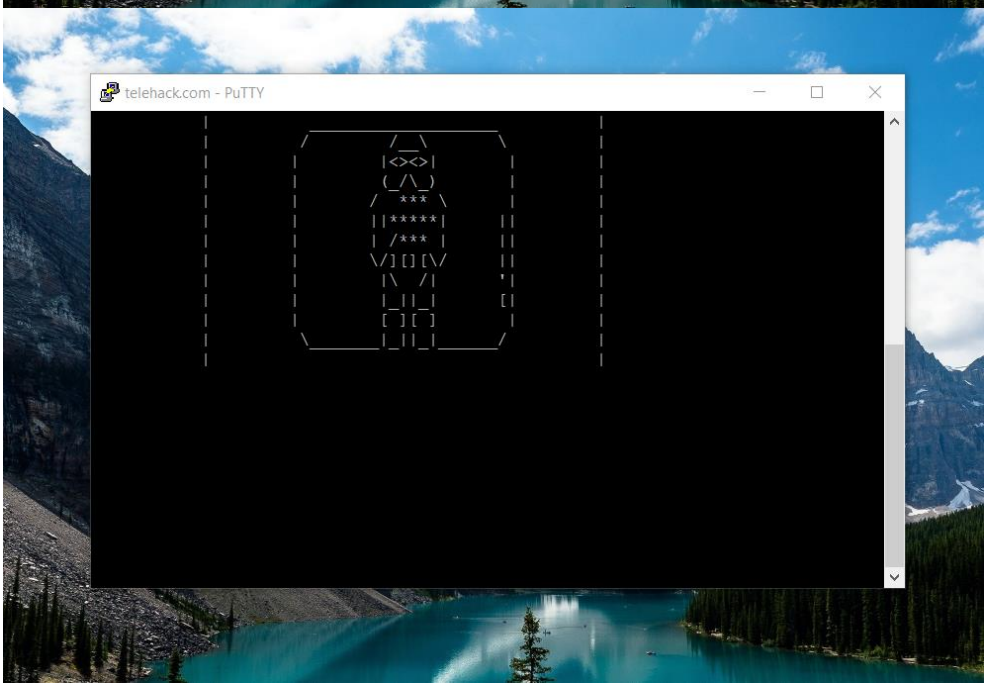

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
telehack.com
23
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
telehack
Default Settings
telehack
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

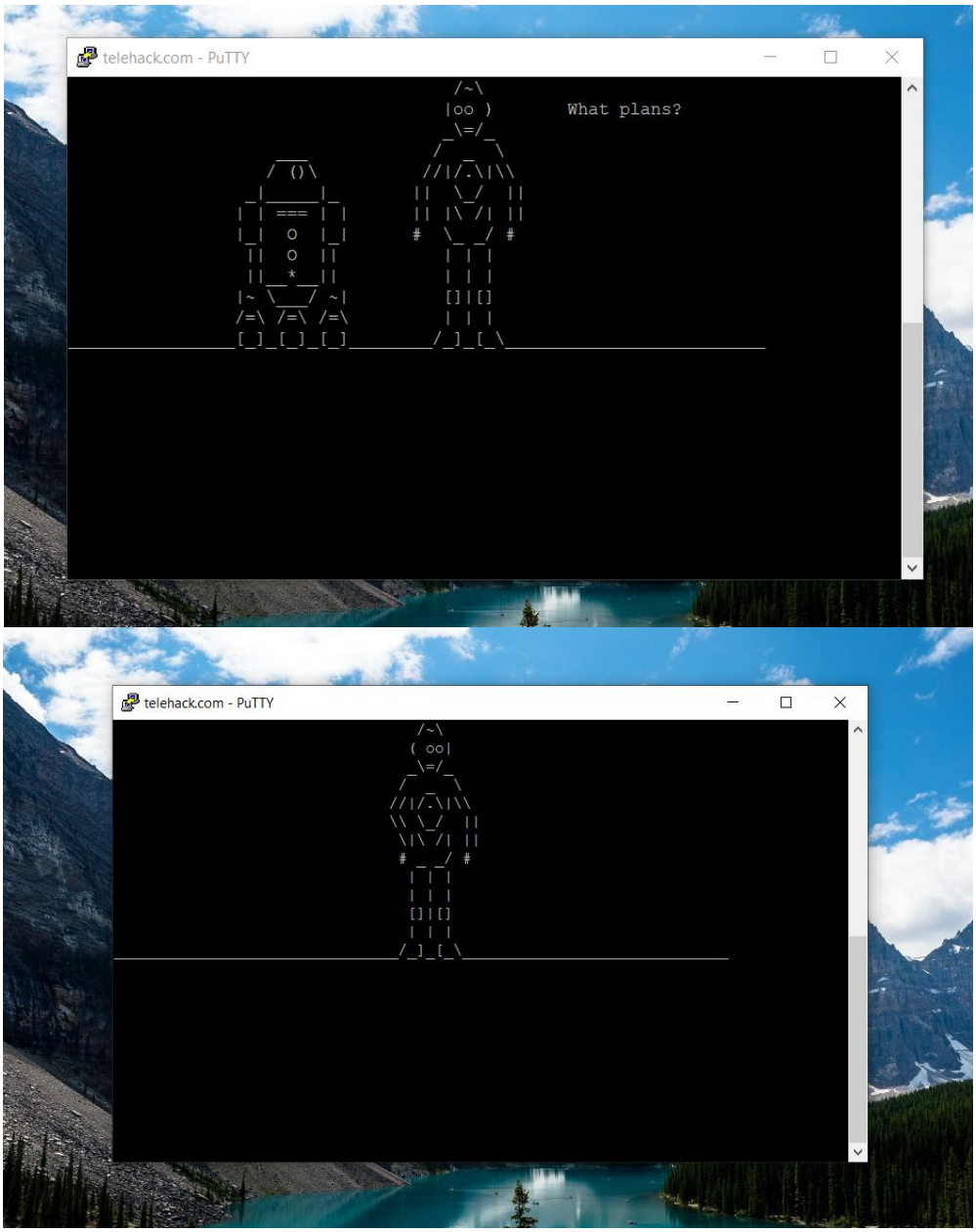

telehack.com - PuTTY
Connected to TELEHACK port 104
It is 7:07 am on Tuesday, April 9, 2024 in Mountain View, California, USA.
There are 127 local users. There are 26648 hosts on the network.
May the command line live forever.
Command, one of the following:
2048 ? a2 c8 cal calc
callsign cat ching clear cowsay date
delta diff dir exit factor figlet
finger fnord geoip gif help ipaddr
joke liff login mac md5 minesweeper
more netstat newuser notes octopus phoon
pig ping pong privacy qr rain
rand rfc rockets roll rot13 starwars
tail today typespeed units uptime usenet
users uupath uuplot weather when zc
More commands available after login. Type HELP for a detailed command list.
Type NEWUSER to create an account. Press control-C to interrupt any command.

1.1.3. کاوش کردن *BBC* تعاملی

چند دستور را وارد می‌نماییم. ابتدا starwars:

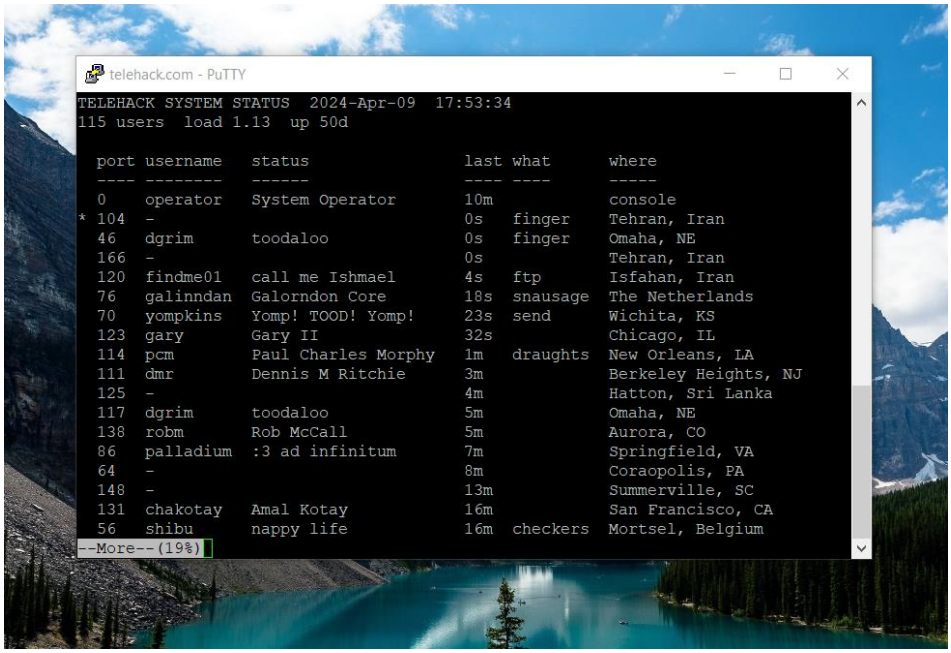




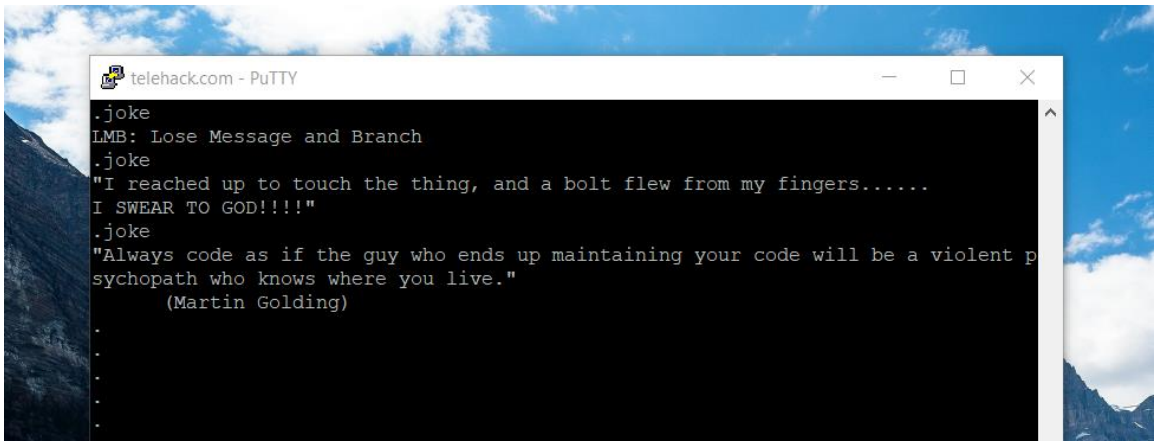


تصاویر زیبای بالا را به حالت فیلم گونه مشاهده می‌کنیم :)))))).

دستور finger:



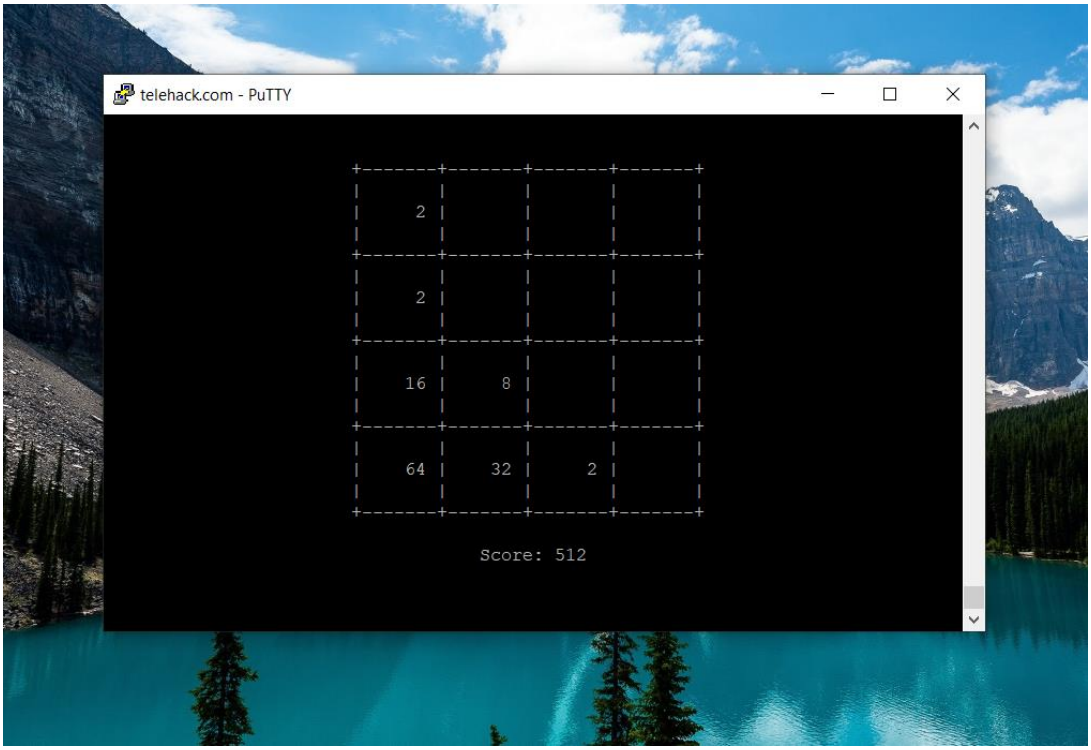
دستور joke:



:(((((

دستور weather:

بازی 2048:

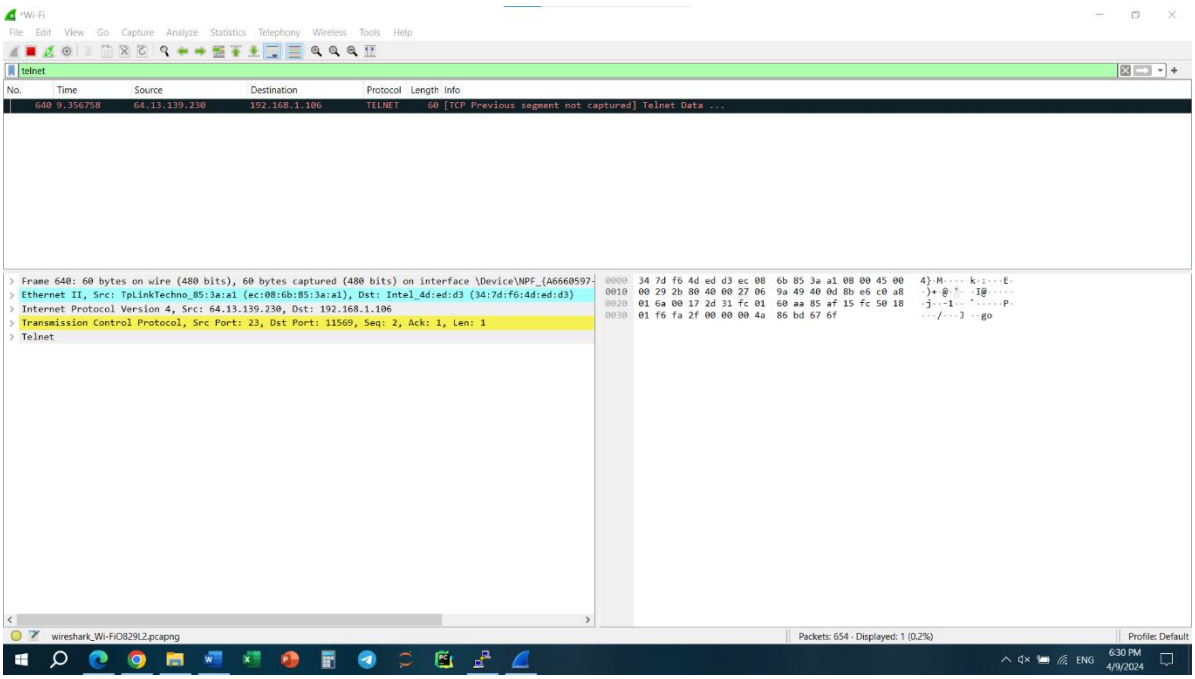


1.2. بررسی پکت‌ها

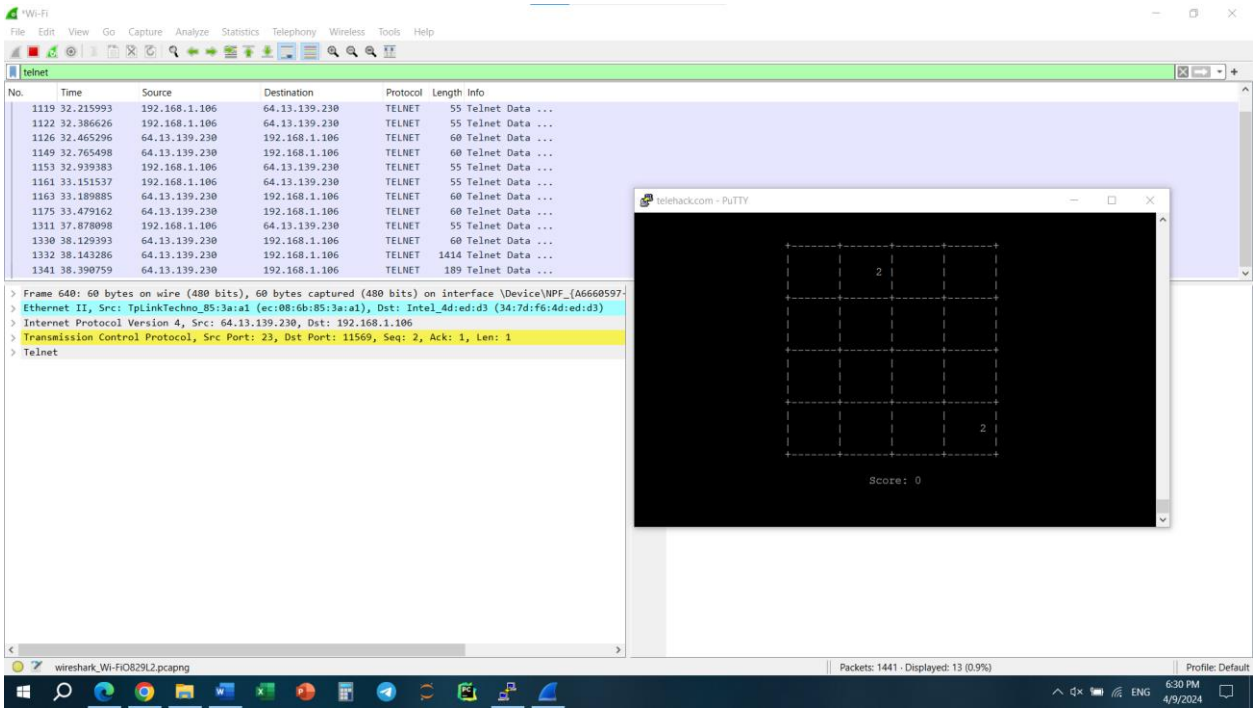
1.2.1. راه‌اندازی Wireshark:

در این بخش ابتدا وایرشارک رو روی Wi-Fi در حالت کپچر قرار می‌دهیم. سپس بازی 2048 را در تلنت انجام داده، پکت‌های telnet را بررسی و فیلتر می‌کنیم.

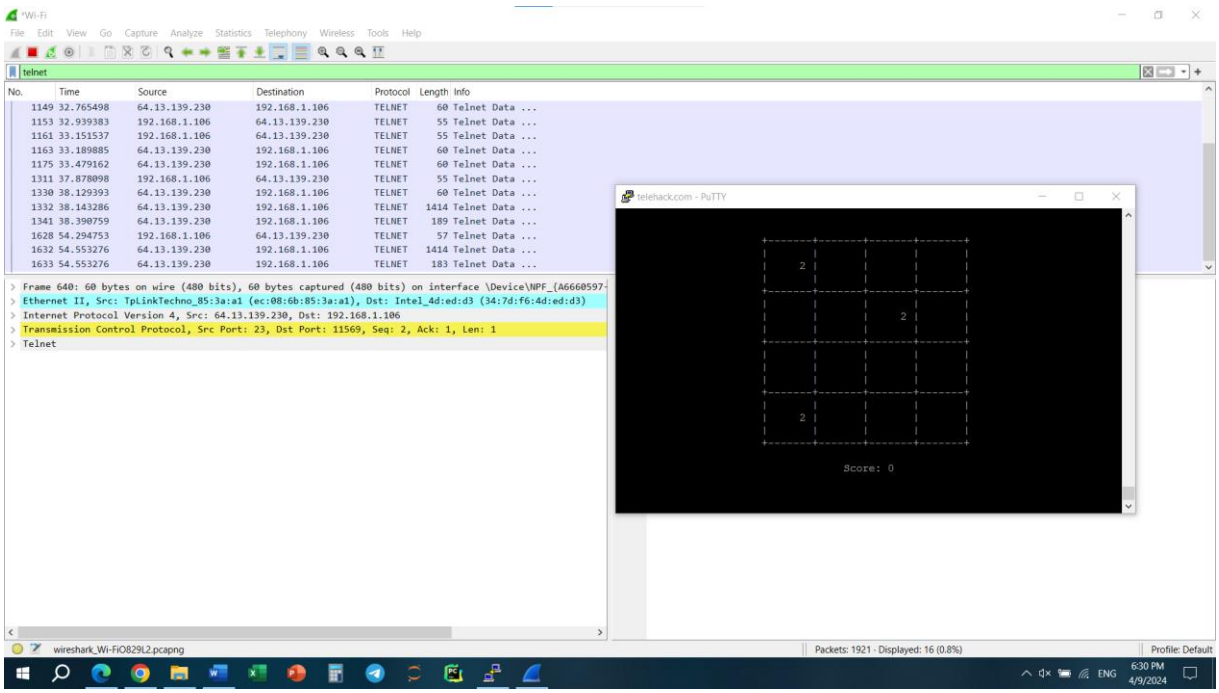
قبل انجام بازی 2048:



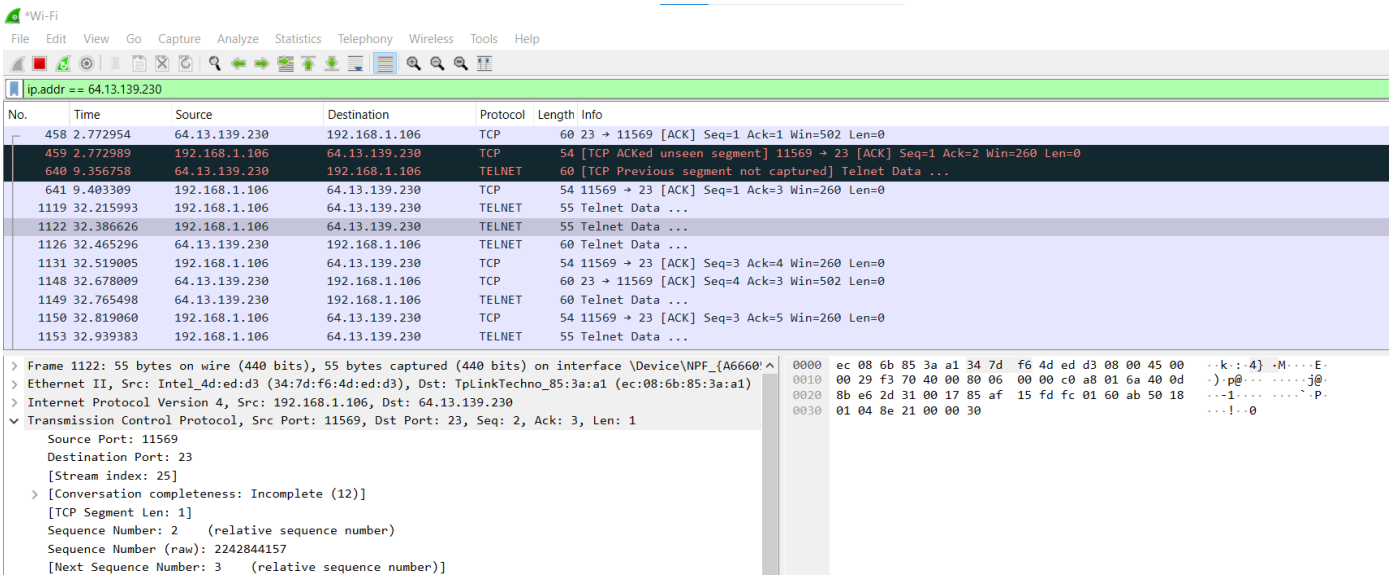
بعد اجرای 2048:



بعد انجام یک حرکت:

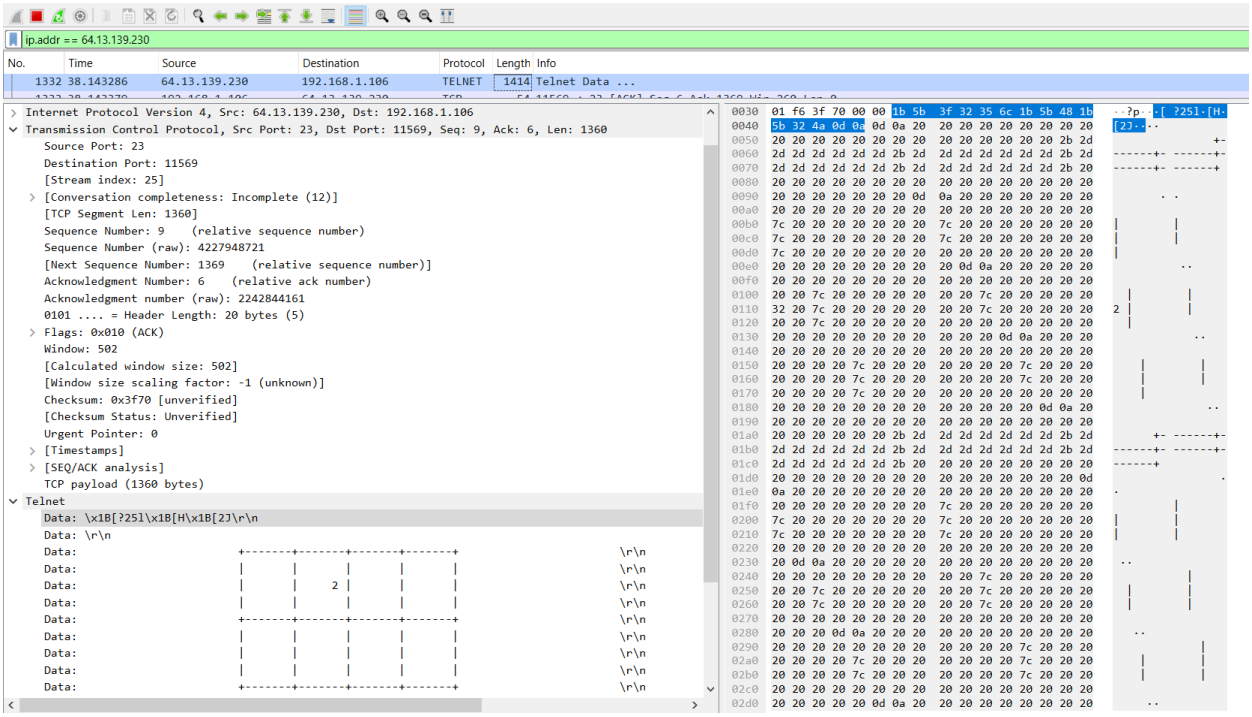


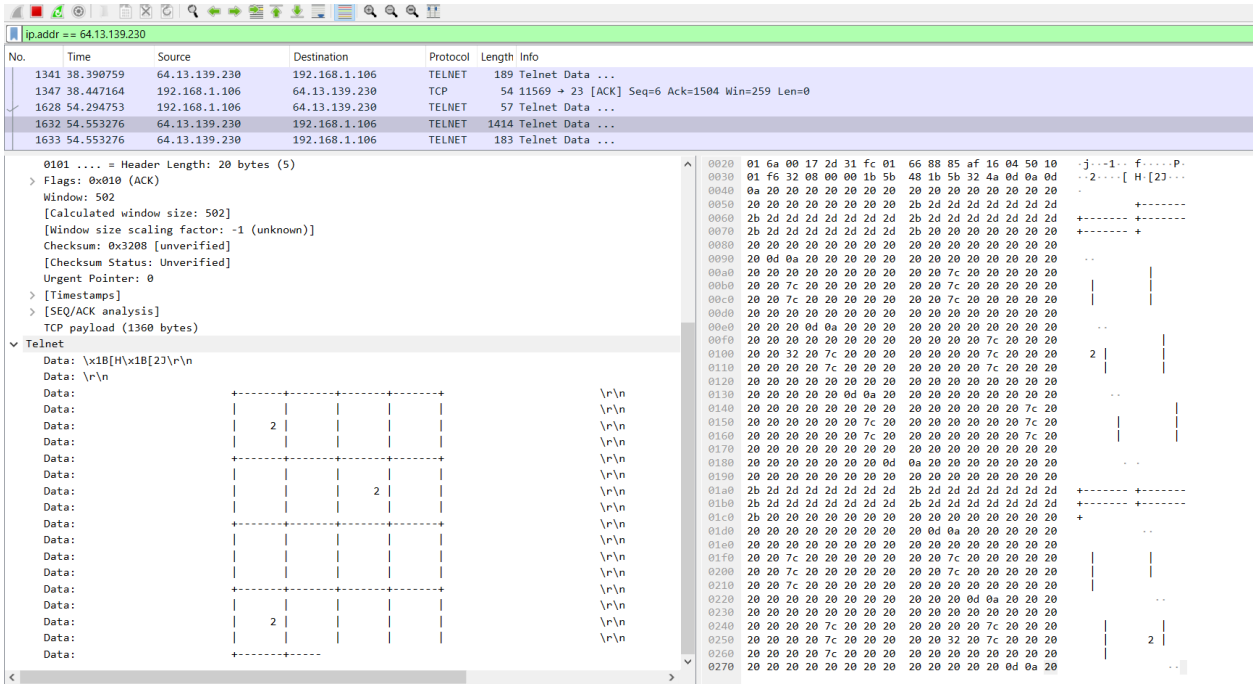
همچنین پکت‌ها را می‌توان با ip address نیز فیلتر نمود.

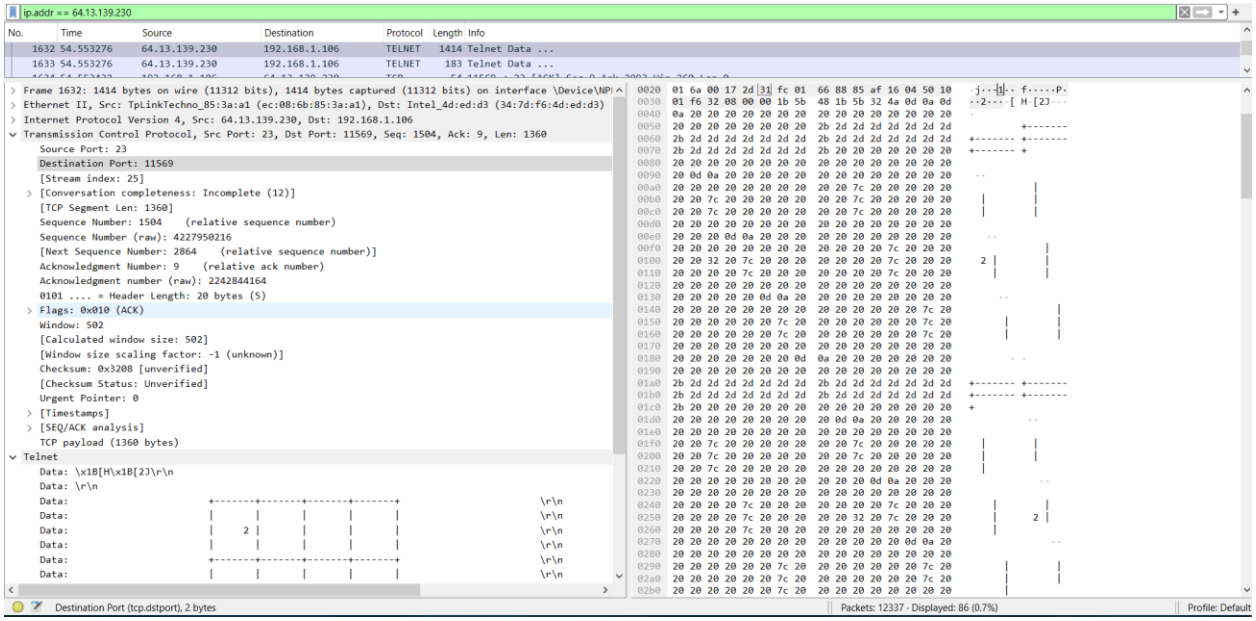


1.2.2. بررسی پکت‌ها:

در این بخش پکت‌ها را بررسی کرده و محتوا و هدرها را می‌توانید در عکس‌ها مشاهده نمایید.

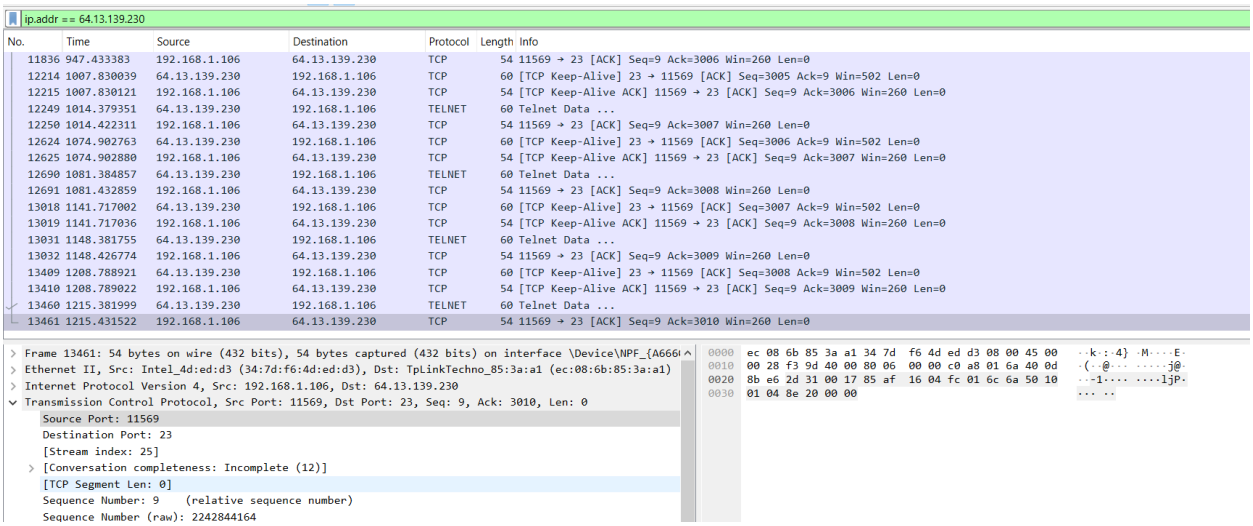


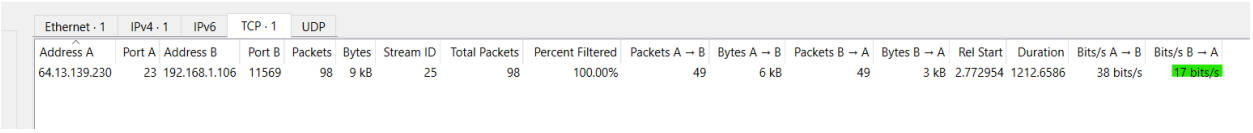




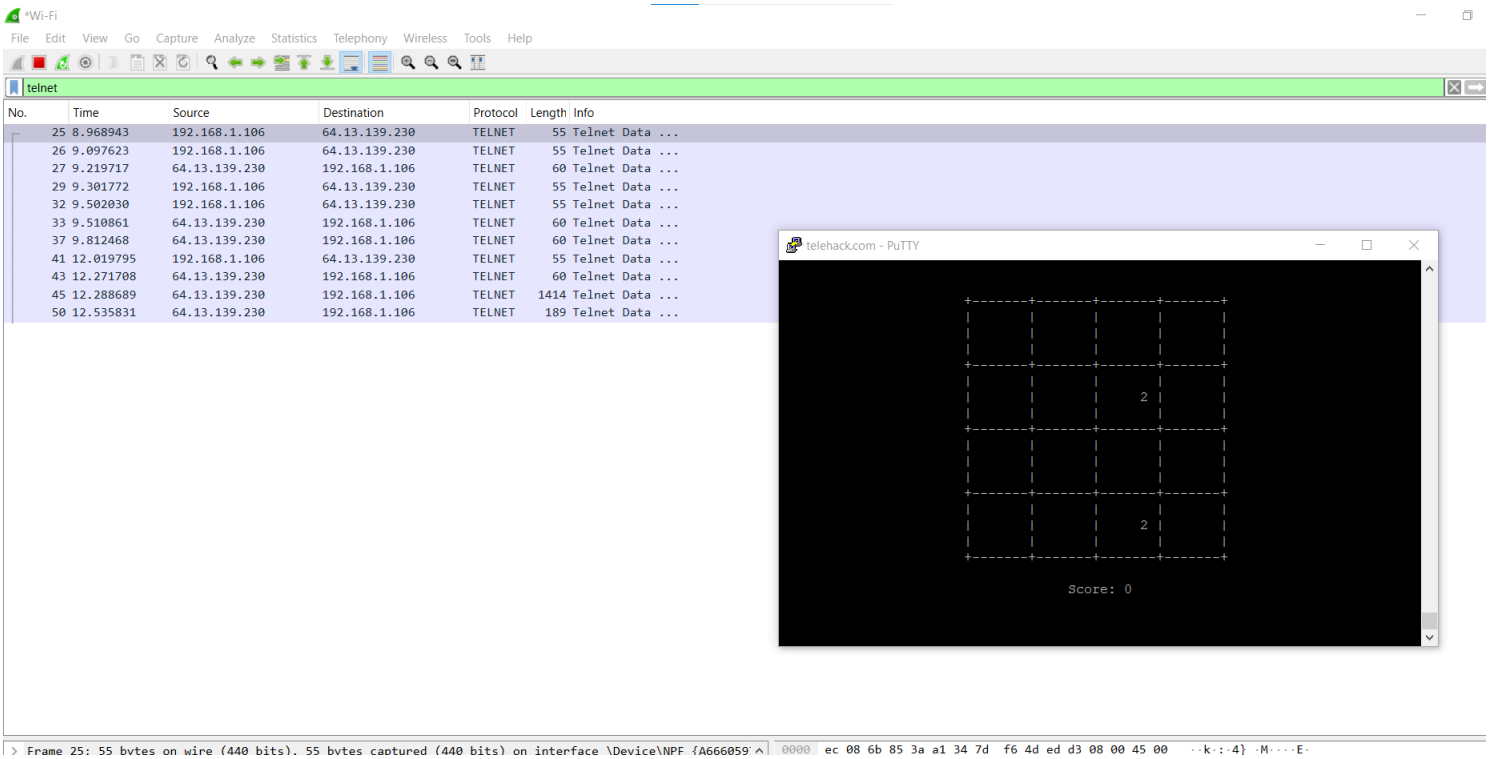
1.2.3. مقدار throughput:

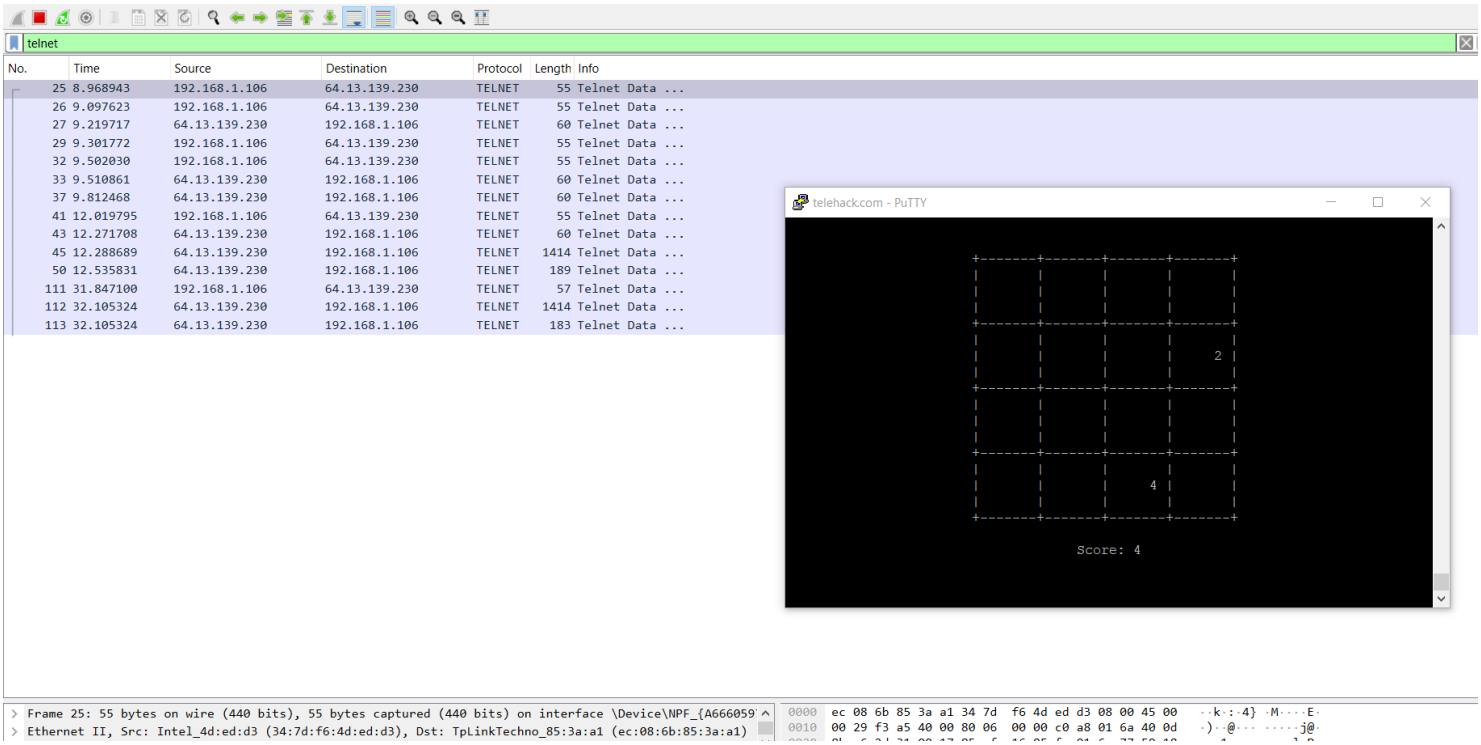
برای این کار دو نوع بررسی می‌توان داشت. یکی در بخش statistics و بخش conversation است که در 2 عکس زیر مشخص است.





که 17 بیت بر ثانیه نوشته شده است. اما این مقدار پس از انجام حرکت و گذشت زمان طولانی است. پس یک بار دیگر وایرشارک را در حالت کپچر قرار می‌دهیم، بازی 2048 را ری‌استارت می‌کنیم، و یک حرکت را انجام می‌دهیم. تصاویر زیر نشان‌دهنده این مراحل می‌باشند.

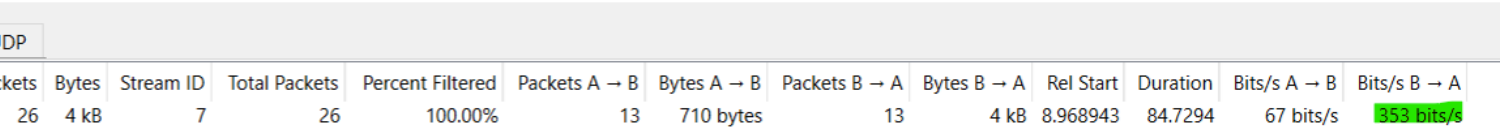




File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 64.13.139.230

No.	Time	Source	Destination	Protocol	Length	Info
25	8.968943	192.168.1.106	64.13.139.230	TELNET	55	Telnet Data ...
26	9.097623	192.168.1.106	64.13.139.230	TELNET	55	Telnet Data ...
27	9.219717	64.13.139.230	192.168.1.106	TELNET	60	Telnet Data ...
28	9.264443	192.168.1.106	64.13.139.230	TCP	54	11569 → 23 [ACK] Seq=3 Ack=2 Win=260 Len=0
29	9.301772	192.168.1.106	64.13.139.230	TELNET	55	Telnet Data ...
31	9.393650	64.13.139.230	192.168.1.106	TCP	60	23 → 11569 [ACK] Seq=2 Ack=3 Win=502 Len=0
32	9.502030	192.168.1.106	64.13.139.230	TELNET	55	Telnet Data ...
33	9.510861	64.13.139.230	192.168.1.106	TELNET	60	Telnet Data ...
34	9.548757	64.13.139.230	192.168.1.106	TCP	60	23 → 11569 [ACK] Seq=3 Ack=4 Win=502 Len=0
35	9.565064	192.168.1.106	64.13.139.230	TCP	54	11569 → 23 [ACK] Seq=5 Ack=3 Win=260 Len=0
36	9.750046	64.13.139.230	192.168.1.106	TCP	60	23 → 11569 [ACK] Seq=3 Ack=5 Win=502 Len=0
37	9.812468	64.13.139.230	192.168.1.106	TELNET	60	Telnet Data ...
38	9.864925	192.168.1.106	64.13.139.230	TCP	54	11569 → 23 [ACK] Seq=5 Ack=5 Win=260 Len=0
41	12.019795	192.168.1.106	64.13.139.230	TELNET	55	Telnet Data ...
42	12.269266	64.13.139.230	192.168.1.106	TCP	60	23 → 11569 [ACK] Seq=5 Ack=6 Win=502 Len=0
43	12.271708	64.13.139.230	192.168.1.106	TELNET	60	Telnet Data ...
45	12.288689	64.13.139.230	192.168.1.106	TELNET	1414	Telnet Data ...
46	12.288794	192.168.1.106	64.13.139.230	TCP	54	11569 → 23 [ACK] Seq=6 Ack=1367 Win=260 Len=0
50	12.535831	64.13.139.230	192.168.1.106	TELNET	189	Telnet Data ...
51	12.576923	192.168.1.106	64.13.139.230	TCP	54	11569 → 23 [ACK] Seq=6 Ack=1502 Win=259 Len=0
111	31.847100	192.168.1.106	64.13.139.230	TELNET	57	Telnet Data ...
112	32.105324	64.13.139.230	192.168.1.106	TELNET	1414	Telnet Data ...
113	32.105324	64.13.139.230	192.168.1.106	TELNET	183	Telnet Data ...
114	32.105389	192.168.1.106	64.13.139.230	TCP	54	11569 → 23 [ACK] Seq=9 Ack=2991 Win=260 Len=0
221	93.698265	64.13.139.230	192.168.1.106	TCP	60	[TCP Keep-Alive] 23 → 11569 [ACK] Seq=2990 Ack=9 Win=502 Len=0
222	93.698357	192.168.1.106	64.13.139.230	TCP	54	[TCP Keep-Alive ACK] 11569 → 23 [ACK] Seq=9 Ack=2991 Win=260 Len=0



DP												
kets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
26	4 kB	7	26	100.00%	13	710 bytes	13	4 kB	8.968943	84.7294	67 bits/s	353 bits/s

که در اینجا مقدار گذردهی 353 بیت بر ثانیه را داریم(برای TCP). راه دیگر این است که از اعداد و زمان 2 عکس قبلی بهره ببریم. می‌توانیم 2 مقدار را به دست بیاوریم. یکی مقدار گذردهی بر اساس 3 بسته اضافه شده بعد از انجام حرکت است، و یکی دیگر مقدار گذردهی بسته‌ها قبل انجام حرکت(طبیعتا برای کل را هم می‌شود به دست آورد). داریم:

$$Throughput_1 = \frac{data}{time}$$
$$= \frac{55+55+60+55+55+60+60+55+60+1414+189}{12.53-8.97}$$
$$= \frac{2118}{3.56} = 594.94$$

$$Throughput_2 = \frac{data}{time} = \frac{57+1414+183}{32.10-31.84} = 6{,}361.53$$

1.2.4. رمزنگاری:

همانطور که در تصاویر این سوال مشاهده می‌کنید. داده ها بدون رمزنگاری جا به جا می‌شوند و محتوای بازگشتی دستور HOST را می‌توانید درون packet به راحتی مشاهده کنید.

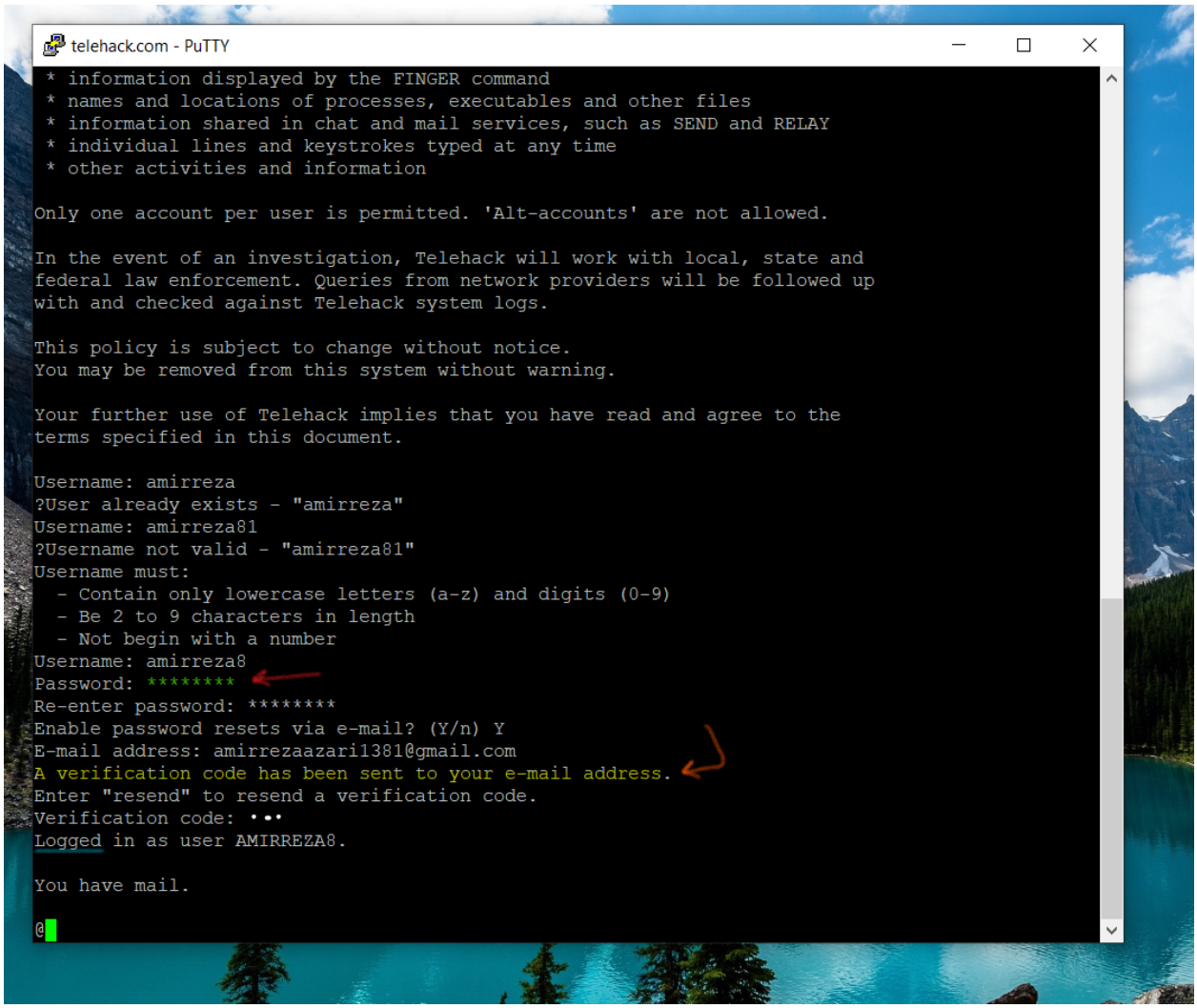
بنابراین برای کارهایی که امنیت در آنها زیاد مهم نیست، استفاده از telnet ایده خوبی است. همچنین برای کار در شبکه‌های لوکال هم ایده خوبی می‌باشد. اما بالعکس، هنگامی‌که امنیت داده‌ها مهم است و نمی‌خواهیم دستخوش تغییر بیرونی یا هر عامل ناشناخته بیرونی بشود، استفاده از telnet خیلی جالب نیست.

1.2.5. فرق اصلی SSH و Telnet

تفاوت اصلی این دو پروتکل در امنیت آنها است . telnet داده را به صورت text plain و بدون هیچ رمزنگاری ارسال می‌کند .در صورتی که ssh داده‌ها را با رمزنگاری ارسال می‌کند. همچنین مکانیزم قوی هم برای احراز هویت دارد.

1.2.6. نکات جالب:

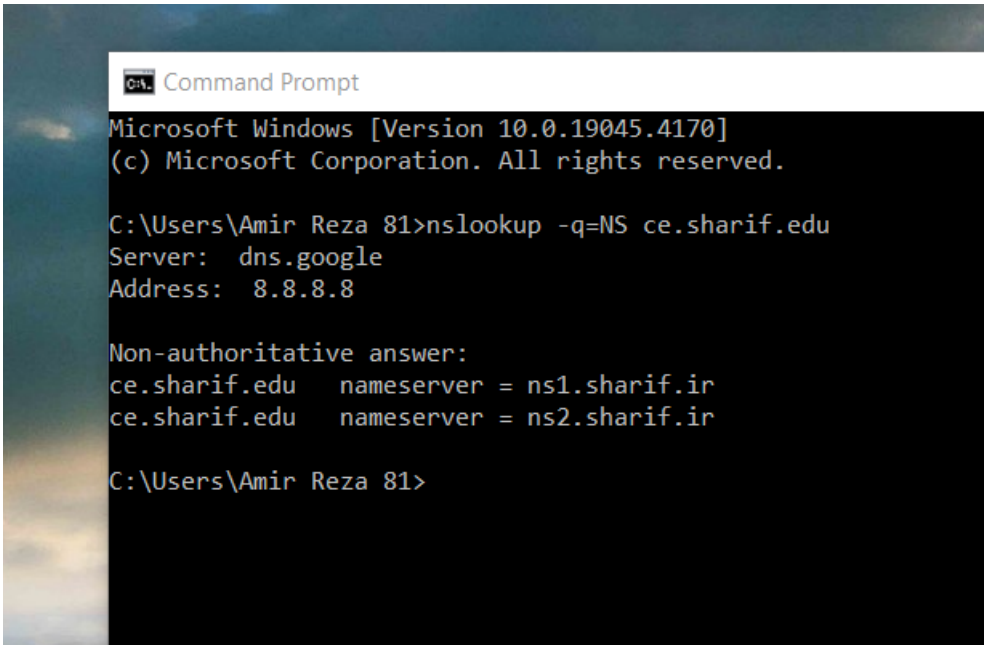
من در telehack ثبت نام کردم تا از قابلیت‌های آن استفاده کنم. و قسمت جالب ماجرا این بود که حتی در ارسال password هم از پروتکل telnet استفاده می‌شد. و پسورد من کامل در پکت‌ها قابل رویت بود. در کل فرآیند ثبت نام جالبی داشت.



DNS .2

NS .2.1:

در این تمرین از سیستم عامل ویندوز استفاده کرده‌ایم. اما برای این بخش هم از ویندوز و هم با کمک گرفتن از VMware از لینوکس بهره خواهیم برد.

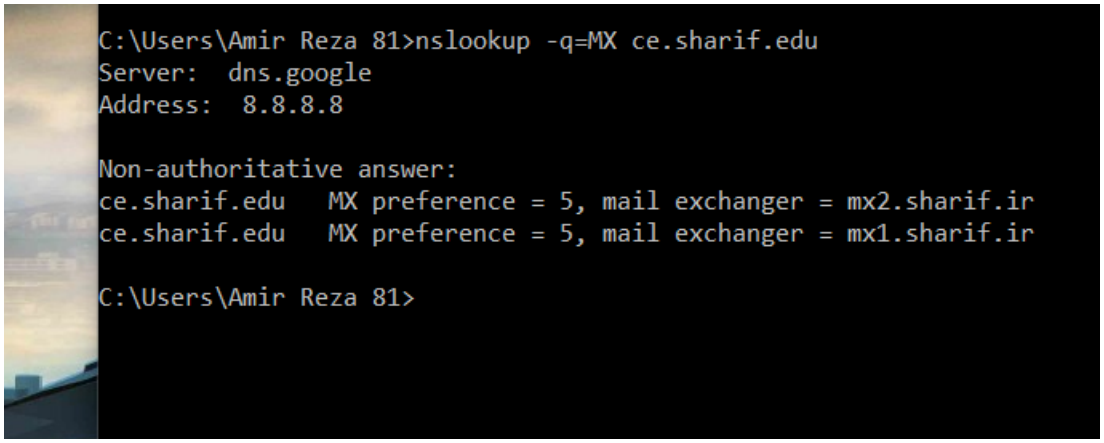


در این بخش، نام DNS server که به آن درخواست خود را ارسال کرده‌ایم و همچنین ip آدرس آن به ما داده شده است. برای بخش non-authoritative توضیح زیر را داریم:

> Sometimes, nslookup will return a **non-authoritative answer** after entering a query. This occurs when nslookup fetches information from your local DNS server cache, not the domain's authoritative server.

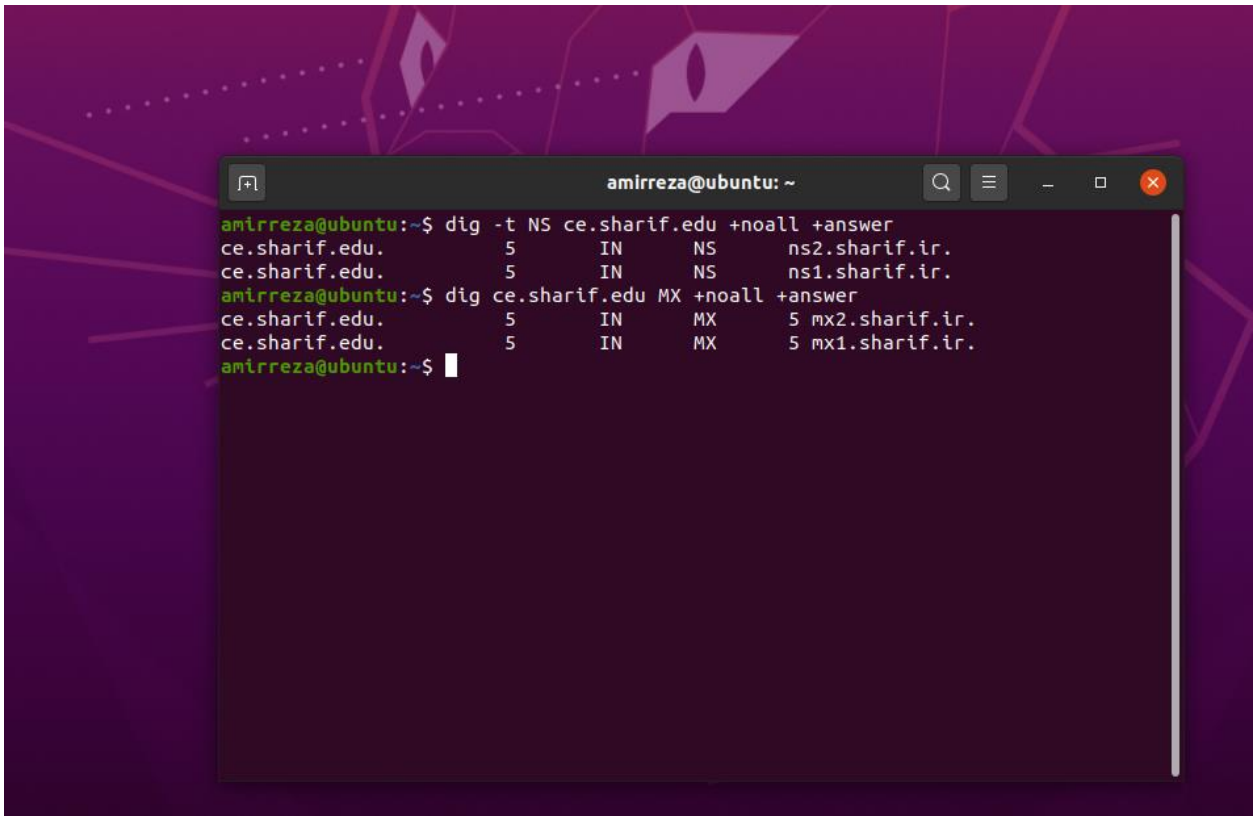
MX .2.2:

مشابه بخش قبل، این بار برای رکوردهای MX درخواست زده‌ایم.



بخش سرور و آدرس ما مانند بخش قبل است.

در قسمت دیگر، دو mail server برای ce.sharif.edu با ترجیحات یکسان (preference) داریم. تصویر زیر این دستورات در لینوکس را نشان می‌دهد.



دستور dig یک دستور ارتباط با dns سرور ها است. در این دستور با t- مشخص کرده ایم که recordهای نوع NS را نیاز داریم .همچنین با دستور های noall+ و awnser+ قسمت دلخواه پاسخ را دریافت کرده‌ایم. در پاسخ ذکر شده‌است که name server مربوط به ce،sharif.edu، دو سرور با آدرس‌های ns1.sharif.edu و ns2.sharif.edu می‌باشند.

مشابه دستور قبلی این‌بار record های MX را دریافت می‌کنیم. این record ها مربوط به server mailها می‌باشد. همانطور که در تصویر مشخص است. دو آدرس برای دریافت و ارسال ایمیل ها به عنوان record ثبت شده است. عدد ۵ که قبل از هر کدام آمده است مربوط به اولویت آنها است که در اینجا اولویت هر دو سرور برای دریافت ایمیل‌ها یکسان است.

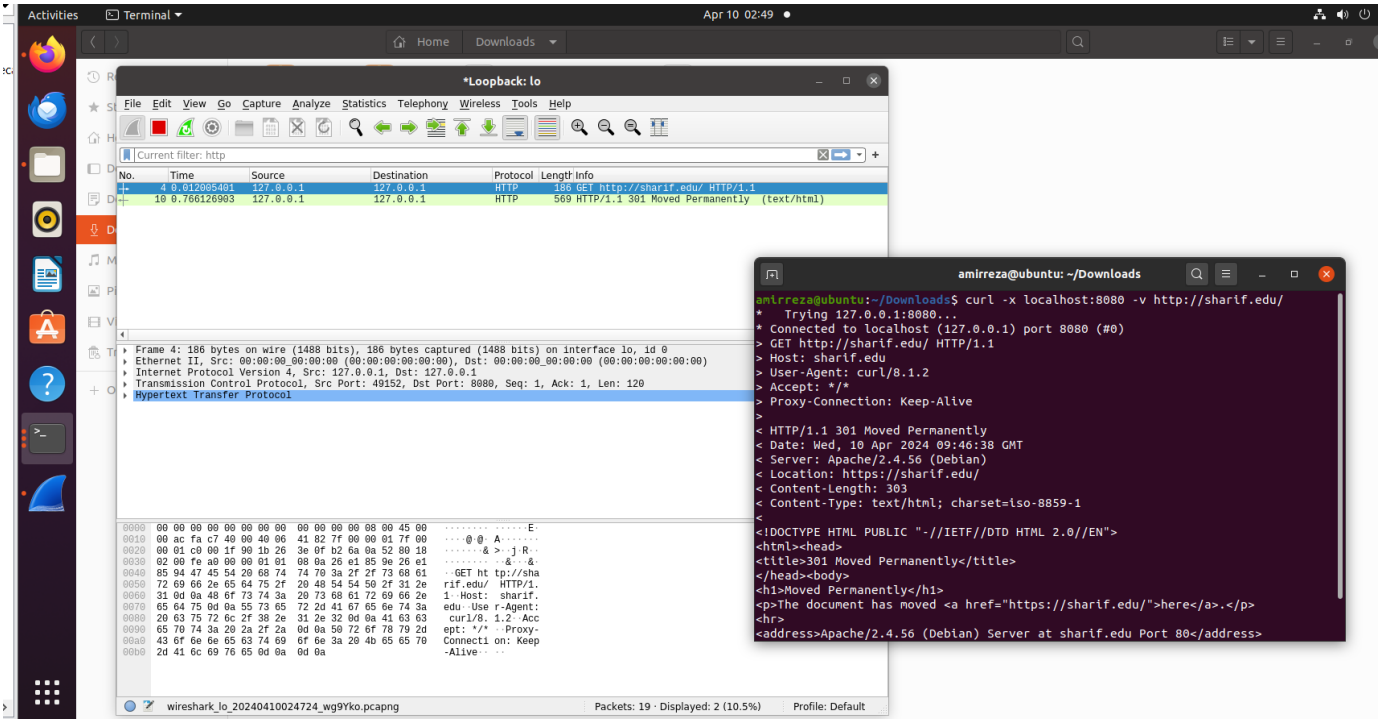
3. HTTP Proxy

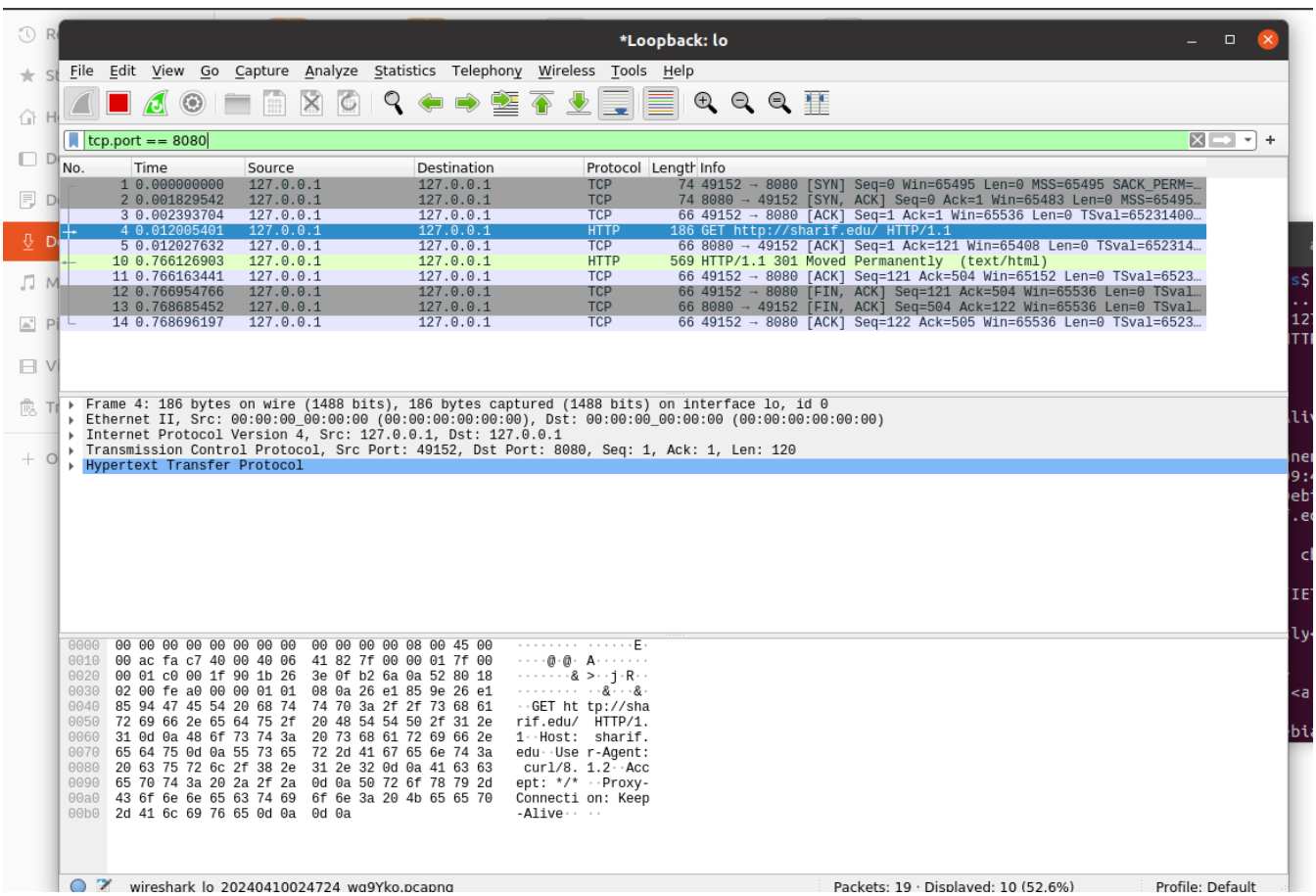
3.1. راه‌اندازی gost:

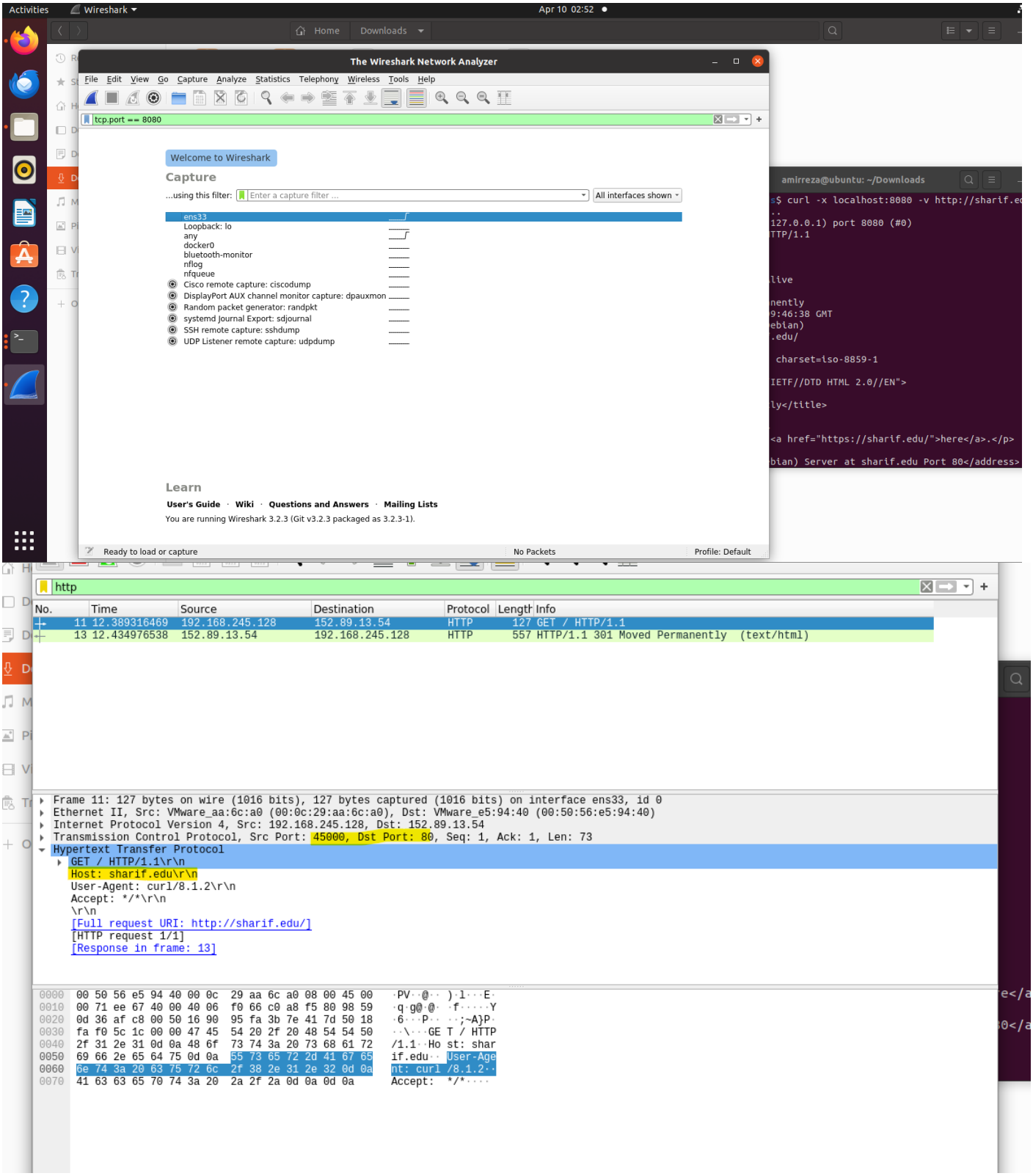
در این بخش به دلیل اینکه از سیستم عامل ویندوز استفاده می‌کنیم، کار کمی سخت می‌شد. به همین دلیل از VMware و Ubuntu کمک گرفته‌ایم. ابتدا gost و wireshark را نصب می‌نماییم. سپس wireshark را هم در حالت loopback و هم ens کپچر می‌کنیم. سپس با دستور زیر ادامه می‌دهیم. بسته‌ها، پورت‌ها، آدرس مبدا و مقصد و لاگ‌های gost در تصاویر بعدی قابل ملاحظه می‌باشند.

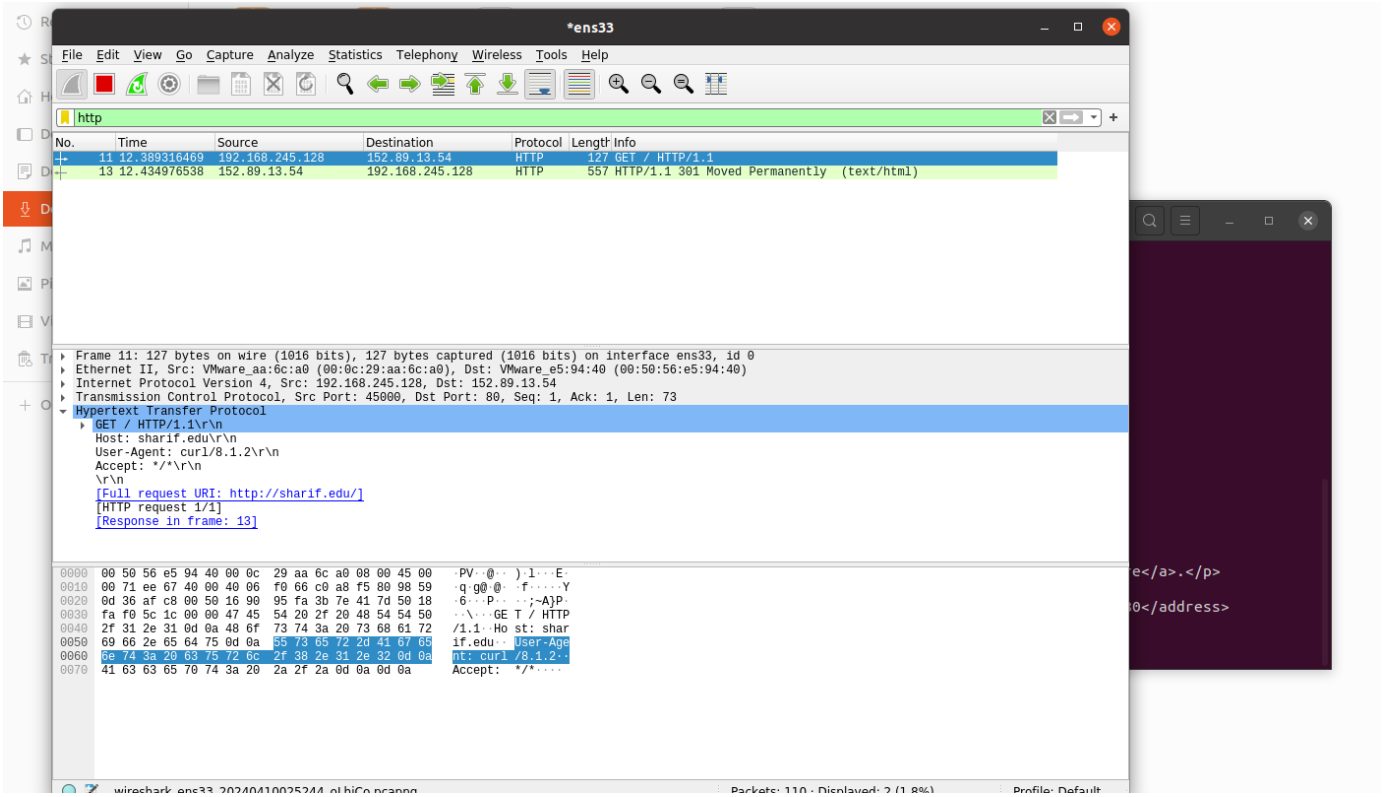
curl -x localhost:8080 -v http://sharif.edu

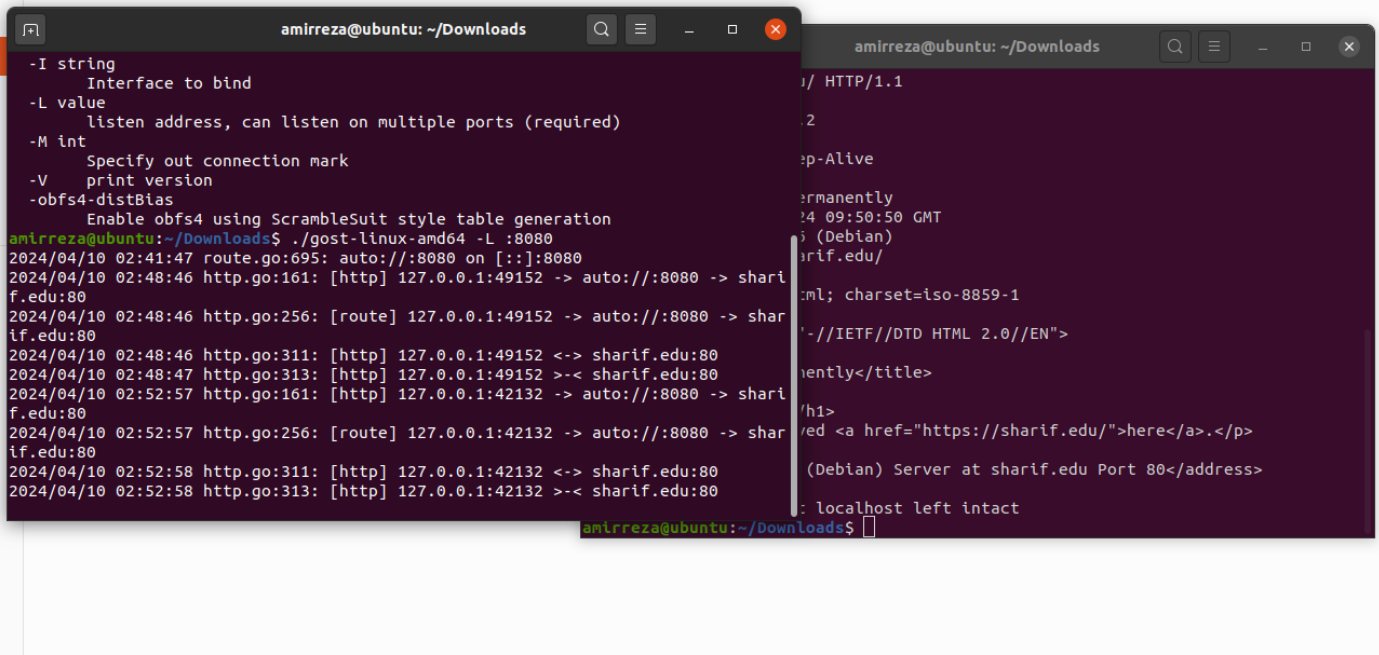
3.2. Curl:

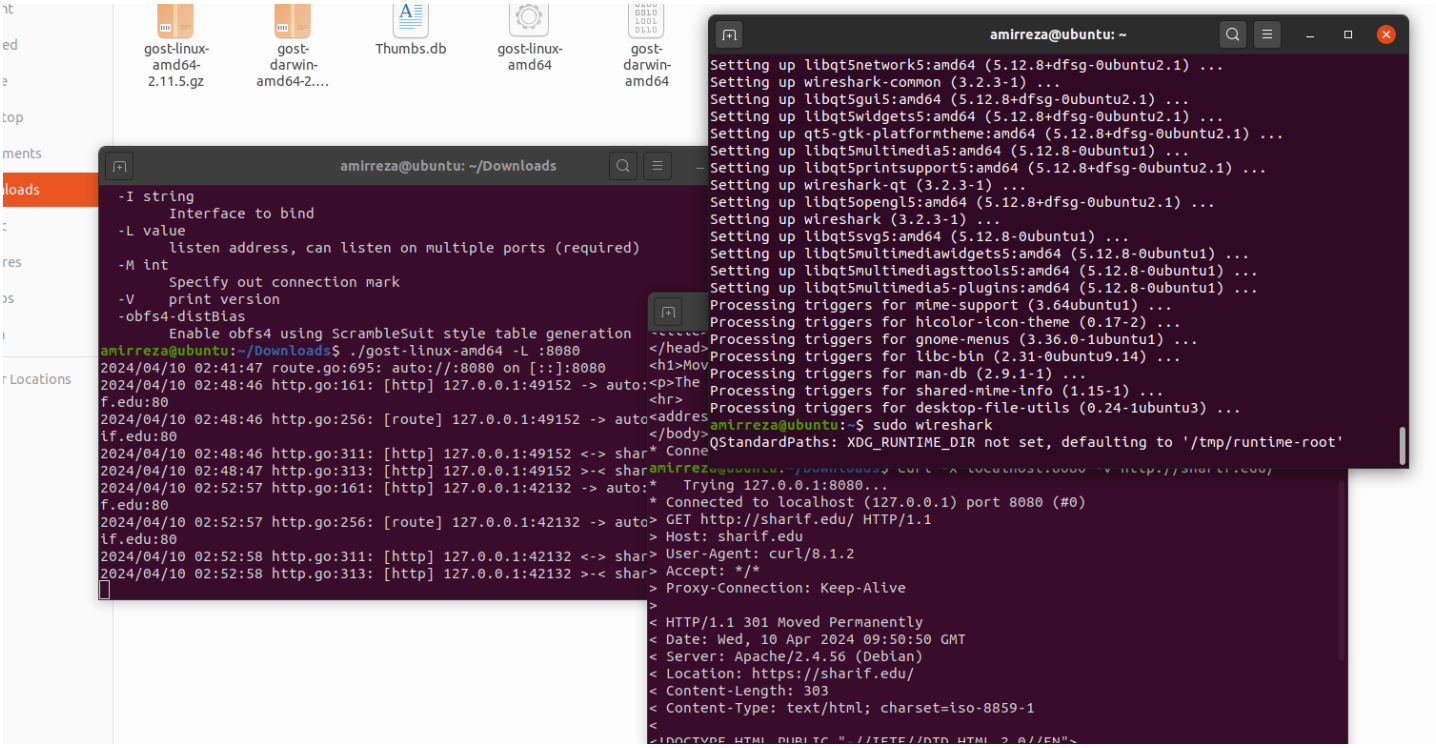

Activities
Terminal
Apr 10 02:49
Home
Downloads
*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
No. Time Source Destination Protocol Length Info
4 0.012005401 127.0.0.1 127.0.0.1 HTTP 186 GET http://sharif.edu/ HTTP/1.1
10 0.766126903 127.0.0.1 127.0.0.1 HTTP 569 HTTP/1.1 301 Moved Permanently (text/html)
Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49152, Dst Port: 8080, Seq: 1, Ack: 1, Len: 120
Hypertext Transfer Protocol
wireshark_lo_20240410024724_wg9Yko.pcapng
Packets: 19 · Displayed: 2 (10.5%)
Profile: Default
amirreza@ubuntu: ~/Downloads
amirreza@ubuntu:~/Downloads$ curl -x localhost:8080 -v http://sharif.edu/
* Trying 127.0.0.1:8080...
* Connected to localhost (127.0.0.1) port 8080 (#0)
> GET http://sharif.edu/ HTTP/1.1
> Host: sharif.edu
> User-Agent: curl/8.1.2
> Accept: */*
> Proxy-Connection: Keep-Alive
>
< HTTP/1.1 301 Moved Permanently
< Date: Wed, 10 Apr 2024 09:46:38 GMT
< Server: Apache/2.4.56 (Debian)
< Location: https://sharif.edu/
< Content-Length: 303
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
<hr>
<address>Apache/2.4.56 (Debian) Server at sharif.edu Port 80</address>


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 8080
No. Time Source Destination Protocol Length Info
1 0.000000000 127.0.0.1 127.0.0.1 TCP 74 49152 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=…
2 0.001829542 127.0.0.1 127.0.0.1 TCP 74 8080 → 49152 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495…
3 0.002393704 127.0.0.1 127.0.0.1 TCP 66 49152 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=65231400…
4 0.012005401 127.0.0.1 127.0.0.1 HTTP 186 GET http://sharif.edu/ HTTP/1.1
5 0.012027632 127.0.0.1 127.0.0.1 TCP 66 8080 → 49152 [ACK] Seq=1 Ack=121 Win=65408 Len=0 TSval=652314…
10 0.766126903 127.0.0.1 127.0.0.1 HTTP 569 HTTP/1.1 301 Moved Permanently (text/html)
11 0.766163441 127.0.0.1 127.0.0.1 TCP 66 49152 → 8080 [ACK] Seq=121 Ack=504 Win=65152 Len=0 TSval=6523…
12 0.766954766 127.0.0.1 127.0.0.1 TCP 66 49152 → 8080 [FIN, ACK] Seq=121 Ack=504 Win=65536 Len=0 TSval…
13 0.768685452 127.0.0.1 127.0.0.1 TCP 66 8080 → 49152 [FIN, ACK] Seq=504 Ack=122 Win=65536 Len=0 TSval…
14 0.768696197 127.0.0.1 127.0.0.1 TCP 66 49152 → 8080 [ACK] Seq=122 Ack=505 Win=65536 Len=0 TSval=6523…
Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49152, Dst Port: 8080, Seq: 1, Ack: 1, Len: 120
Hypertext Transfer Protocol
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ....E.
0010 00 ac fa c7 40 00 40 06 41 82 7f 00 00 01 7f 00 ....@.@. A.....
0020 00 01 c0 00 1f 90 1b 26 3e 0f b2 6a 0a 52 80 18 .....& >..j.R..
0030 02 00 fe a0 00 00 01 01 08 0a 26 e1 85 9e 26 e1 ....&...&.
0040 85 94 47 45 54 20 68 74 74 70 3a 2f 2f 73 68 61 ..GET ht tp://sha
0050 72 69 66 2e 65 64 75 2f 20 48 54 54 50 2f 31 2e rif.edu/ HTTP/1.
0060 31 0d 0a 48 6f 73 74 3a 20 73 68 61 72 69 66 2e 1..Host: sharif.
0070 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a edu..Use r-Agent:
0080 20 63 75 72 6c 2f 38 2e 31 2e 32 0d 0a 41 63 63 curl/8. 1.2..Acc
0090 65 70 74 3a 20 2a 2f 2a 0d 0a 50 72 6f 78 79 2d ept: */* ..Proxy-
00a0 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 Connecti on: Keep
00b0 2d 41 6c 69 76 65 0d 0a 0d 0a -Alive.. ..
wireshark_lo_20240410024724_wg9Yko.pcapng
Packets: 19 · Displayed: 10 (52.6%)
Profile: Default


Activities
Wireshark
Apr 10 02:52
Home
Downloads
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 8080
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
ens33
Loopback: lo
any
docker0
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).
Ready to load or capture
No Packets
Profile: Default
amirreza@ubuntu: ~/Downloads
http
No. Time Source Destination Protocol Length Info
11 12.389316469 192.168.245.128 152.89.13.54 HTTP 127 GET / HTTP/1.1
13 12.434976538 152.89.13.54 192.168.245.128 HTTP 557 HTTP/1.1 301 Moved Permanently (text/html)
Frame 11: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface ens33, id 0
Ethernet II, Src: VMware_aa:6c:a0 (00:0c:29:aa:6c:a0), Dst: VMware_e5:94:40 (00:50:56:e5:94:40)
Internet Protocol Version 4, Src: 192.168.245.128, Dst: 152.89.13.54
Transmission Control Protocol, Src Port: 45000, Dst Port: 80, Seq: 1, Ack: 1, Len: 73
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: sharif.edu\r\n
User-Agent: curl/8.1.2\r\n
Accept: */*\r\n
\r\n
[Full request URI: http://sharif.edu/]
[HTTP request 1/1]
[Response in frame: 13]
0000 00 50 56 e5 94 40 00 0c 29 aa 6c a0 08 00 45 00 ·PV··@··)·l···E·
0010 00 71 ee 67 40 00 40 06 f0 66 c0 a8 f5 80 98 59 ·q·g@·@· ·f·····Y
0020 0d 36 af c8 00 50 16 90 95 fa 3b 7e 41 7d 50 18 ·6···P·· ··;~A}P·
0030 fa f0 5c 1c 00 00 47 45 54 20 2f 20 48 54 54 50 ··\···GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 68 61 72 /1.1··Ho st: shar
0050 69 66 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 if.edu·· User-Age
0060 6e 74 3a 20 63 75 72 6c 2f 38 2e 31 2e 32 0d 0a nt: curl /8.1.2··
0070 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a Accept: */*····

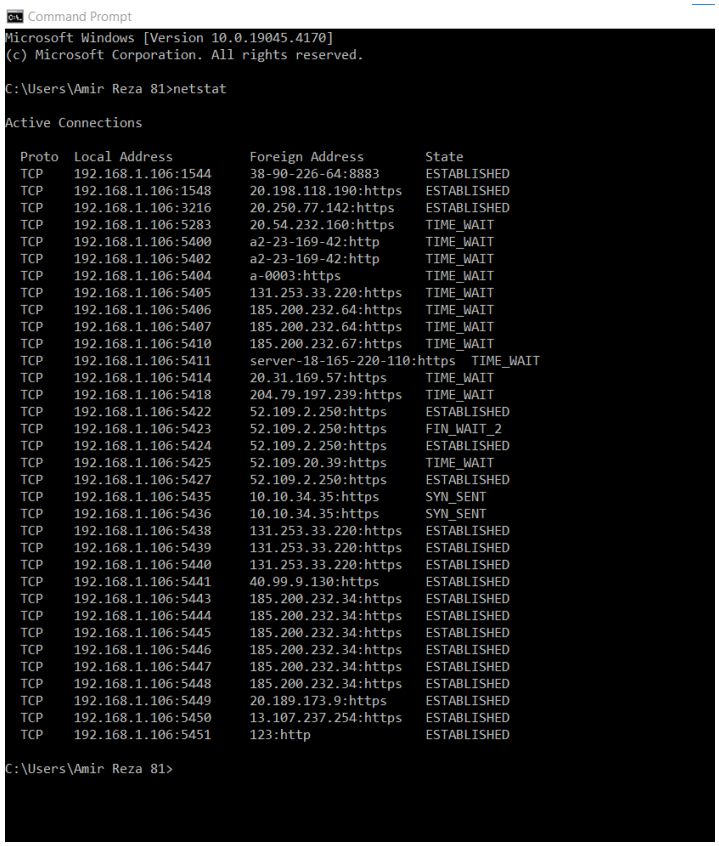

*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
11 12.389316469 192.168.245.128 152.89.13.54 HTTP 127 GET / HTTP/1.1
13 12.434976538 152.89.13.54 192.168.245.128 HTTP 557 HTTP/1.1 301 Moved Permanently (text/html)
Frame 11: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface ens33, id 0
Ethernet II, Src: VMware_aa:6c:a0 (00:0c:29:aa:6c:a0), Dst: VMware_e5:94:40 (00:50:56:e5:94:40)
Internet Protocol Version 4, Src: 192.168.245.128, Dst: 152.89.13.54
Transmission Control Protocol, Src Port: 45000, Dst Port: 80, Seq: 1, Ack: 1, Len: 73
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: sharif.edu\r\n
User-Agent: curl/8.1.2\r\n
Accept: */*\r\n
\r\n
[Full request URI: http://sharif.edu/]
[HTTP request 1/1]
[Response in frame: 13]
0000 00 50 56 e5 94 40 00 0c 29 aa 6c a0 08 00 45 00
0010 00 71 ee 67 40 00 40 06 f0 66 c0 a8 f5 80 98 59
0020 0d 36 af c8 00 50 16 90 95 fa 3b 7e 41 7d 50 18
0030 fa f0 5c 1c 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 68 61 72
0050 69 66 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65
0060 6e 74 3a 20 63 75 72 6c 2f 38 2e 31 2e 32 0d 0a
0070 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a
Accept: */*


amirreza@ubuntu: ~/Downloads
-I string
Interface to bind
-L value
listen address, can listen on multiple ports (required)
-M int
Specify out connection mark
-V print version
-obfs4-distBias
Enable obfs4 using ScrambleSuit style table generation
amirreza@ubuntu:~/Downloads$ ./gost-linux-amd64 -L :8080
2024/04/10 02:41:47 route.go:695: auto://:8080 on [::]:8080
2024/04/10 02:48:46 http.go:161: [http] 127.0.0.1:49152 -> auto://:8080 -> sharif.edu:80
2024/04/10 02:48:46 http.go:256: [route] 127.0.0.1:49152 -> auto://:8080 -> sharif.edu:80
2024/04/10 02:48:46 http.go:311: [http] 127.0.0.1:49152 <-> sharif.edu:80
2024/04/10 02:48:47 http.go:313: [http] 127.0.0.1:49152 >-< sharif.edu:80
2024/04/10 02:52:57 http.go:161: [http] 127.0.0.1:42132 -> auto://:8080 -> sharif.edu:80
2024/04/10 02:52:57 http.go:256: [route] 127.0.0.1:42132 -> auto://:8080 -> sharif.edu:80
2024/04/10 02:52:58 http.go:311: [http] 127.0.0.1:42132 <-> sharif.edu:80
2024/04/10 02:52:58 http.go:313: [http] 127.0.0.1:42132 >-< sharif.edu:80
amirreza@ubuntu: ~/Downloads
amirreza@ubuntu:~/Downloads$

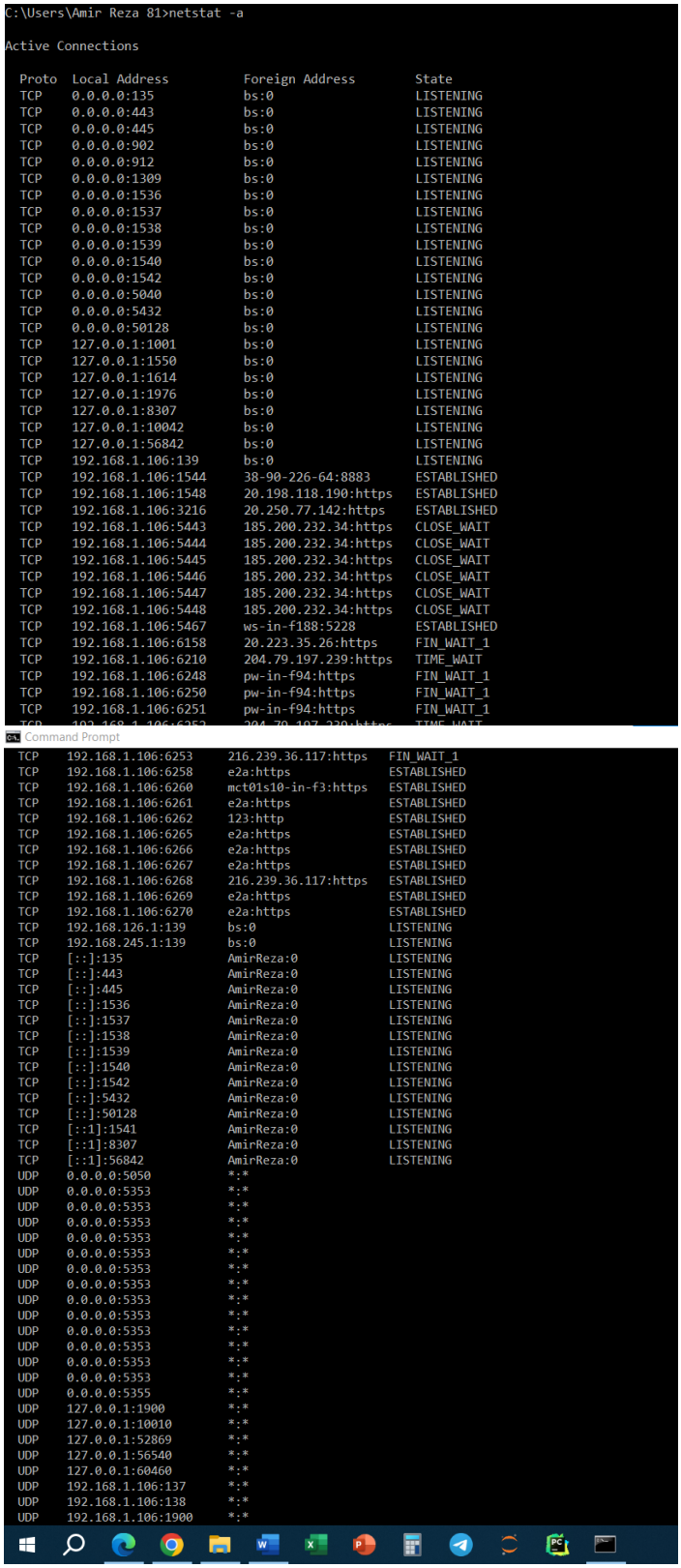


Netstat .4

:All connections .4.1


Command Prompt
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Amir Reza 81>netstat
Active Connections
Proto Local Address Foreign Address State
TCP 192.168.1.106:1544 38-90-226-64:8883 ESTABLISHED
TCP 192.168.1.106:1548 20.198.118.190:https ESTABLISHED
TCP 192.168.1.106:3216 20.250.77.142:https ESTABLISHED
TCP 192.168.1.106:5283 20.54.232.160:https TIME_WAIT
TCP 192.168.1.106:5400 a2-23-169-42:http TIME_WAIT
TCP 192.168.1.106:5402 a2-23-169-42:http TIME_WAIT
TCP 192.168.1.106:5404 a-0003:https TIME_WAIT
TCP 192.168.1.106:5405 131.253.33.220:https TIME_WAIT
TCP 192.168.1.106:5406 185.200.232.64:https TIME_WAIT
TCP 192.168.1.106:5407 185.200.232.64:https TIME_WAIT
TCP 192.168.1.106:5410 185.200.232.67:https TIME_WAIT
TCP 192.168.1.106:5411 server-18-165-220-110:https TIME_WAIT
TCP 192.168.1.106:5414 20.31.169.57:https TIME_WAIT
TCP 192.168.1.106:5418 204.79.197.239:https TIME_WAIT
TCP 192.168.1.106:5422 52.109.2.250:https ESTABLISHED
TCP 192.168.1.106:5423 52.109.2.250:https FIN_WAIT_2
TCP 192.168.1.106:5424 52.109.2.250:https ESTABLISHED
TCP 192.168.1.106:5425 52.109.20.39:https TIME_WAIT
TCP 192.168.1.106:5427 52.109.2.250:https ESTABLISHED
TCP 192.168.1.106:5435 10.10.34.35:https SYN_SENT
TCP 192.168.1.106:5436 10.10.34.35:https SYN_SENT
TCP 192.168.1.106:5438 131.253.33.220:https ESTABLISHED
TCP 192.168.1.106:5439 131.253.33.220:https ESTABLISHED
TCP 192.168.1.106:5440 131.253.33.220:https ESTABLISHED
TCP 192.168.1.106:5441 40.99.9.130:https ESTABLISHED
TCP 192.168.1.106:5443 185.200.232.34:https ESTABLISHED
TCP 192.168.1.106:5444 185.200.232.34:https ESTABLISHED
TCP 192.168.1.106:5445 185.200.232.34:https ESTABLISHED
TCP 192.168.1.106:5446 185.200.232.34:https ESTABLISHED
TCP 192.168.1.106:5447 185.200.232.34:https ESTABLISHED
TCP 192.168.1.106:5448 185.200.232.34:https ESTABLISHED
TCP 192.168.1.106:5449 20.189.173.9:https ESTABLISHED
TCP 192.168.1.106:5450 13.107.237.254:https ESTABLISHED
TCP 192.168.1.106:5451 123:http ESTABLISHED
C:\Users\Amir Reza 81>

در این بخش تمامی کانکشن‌ها را مشاهده می‌کنید. دقت نمایید از دستور netstat استفاده کردیم. می‌توانیم برای تمام کانکشن‌ها از a- بهره ببریم.



```
C:\Users\Amir Reza 81>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            bs:0                   LISTENING
  TCP    0.0.0.0:443            bs:0                   LISTENING
  TCP    0.0.0.0:445            bs:0                   LISTENING
  TCP    0.0.0.0:902            bs:0                   LISTENING
  TCP    0.0.0.0:912            bs:0                   LISTENING
  TCP    0.0.0.0:1309           bs:0                   LISTENING
  TCP    0.0.0.0:1536           bs:0                   LISTENING
  TCP    0.0.0.0:1537           bs:0                   LISTENING
  TCP    0.0.0.0:1538           bs:0                   LISTENING
  TCP    0.0.0.0:1539           bs:0                   LISTENING
  TCP    0.0.0.0:1540           bs:0                   LISTENING
  TCP    0.0.0.0:1542           bs:0                   LISTENING
  TCP    0.0.0.0:5040           bs:0                   LISTENING
  TCP    0.0.0.0:5432           bs:0                   LISTENING
  TCP    0.0.0.0:50128          bs:0                   LISTENING
  TCP    127.0.0.1:1001         bs:0                   LISTENING
  TCP    127.0.0.1:1550         bs:0                   LISTENING
  TCP    127.0.0.1:1614         bs:0                   LISTENING
  TCP    127.0.0.1:1976         bs:0                   LISTENING
  TCP    127.0.0.1:8307         bs:0                   LISTENING
  TCP    127.0.0.1:10042        bs:0                   LISTENING
  TCP    127.0.0.1:56842        bs:0                   LISTENING
  TCP    192.168.1.106:139      bs:0                   LISTENING
  TCP    192.168.1.106:1544     38-90-226-64:8883      ESTABLISHED
  TCP    192.168.1.106:1548     20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.106:3216     20.250.77.142:https    ESTABLISHED
  TCP    192.168.1.106:5443     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5444     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5445     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5446     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5447     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5448     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5467     ws-in-f188:5228        ESTABLISHED
  TCP    192.168.1.106:6158     20.223.35.26:https     FIN_WAIT_1
  TCP    192.168.1.106:6210     204.79.197.239:https   TIME_WAIT
  TCP    192.168.1.106:6248     pw-in-f94:https        FIN_WAIT_1
  TCP    192.168.1.106:6250     pw-in-f94:https        FIN_WAIT_1
  TCP    192.168.1.106:6251     pw-in-f94:https        FIN_WAIT_1
  TCP    192.168.1.106:6253     216.239.36.117:https   FIN_WAIT_1
  TCP    192.168.1.106:6258     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6260     mct01s10-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6261     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6262     123:http               ESTABLISHED
  TCP    192.168.1.106:6265     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6266     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6267     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6268     216.239.36.117:https   ESTABLISHED
  TCP    192.168.1.106:6269     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6270     e2a:https              ESTABLISHED
  TCP    192.168.126.1:139      bs:0                   LISTENING
  TCP    192.168.245.1:139      bs:0                   LISTENING
  TCP    [::]:135               AmirReza:0             LISTENING
  TCP    [::]:443               AmirReza:0             LISTENING
  TCP    [::]:445               AmirReza:0             LISTENING
  TCP    [::]:1536              AmirReza:0             LISTENING
  TCP    [::]:1537              AmirReza:0             LISTENING
  TCP    [::]:1538              AmirReza:0             LISTENING
  TCP    [::]:1539              AmirReza:0             LISTENING
  TCP    [::]:1540              AmirReza:0             LISTENING
  TCP    [::]:1542              AmirReza:0             LISTENING
  TCP    [::]:5432              AmirReza:0             LISTENING
  TCP    [::]:50128             AmirReza:0             LISTENING
  TCP    [::1]:1541             AmirReza:0             LISTENING
  TCP    [::1]:8307             AmirReza:0             LISTENING
  TCP    [::1]:56842            AmirReza:0             LISTENING
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:10010        *:*
  UDP    127.0.0.1:52869        *:*
  UDP    127.0.0.1:56540        *:*
  UDP    127.0.0.1:60460        *:*
  UDP    192.168.1.106:137      *:*
  UDP    192.168.1.106:138      *:*
  UDP    192.168.1.106:1900     *:*
```

```
  UDP    [::]:5353                  *:*
  UDP    [::]:5355                  *:*
  UDP    [::1]:1900                 *:*
  UDP    [::1]:52865                *:*
  UDP    [fe80::4fa2:aac0:e023:e45e%11]:1900  *:*
  UDP    [fe80::4fa2:aac0:e023:e45e%11]:52863  *:*
  UDP    [fe80::c80f:812b:885c:3a7e%14]:1900  *:*
  UDP    [fe80::c80f:812b:885c:3a7e%14]:52862  *:*
  UDP    [fe80::d124:abb5:1ba:a629%19]:1900  *:*
  UDP    [fe80::d124:abb5:1ba:a629%19]:52864  *:*

C:\Users\Amir Reza 81>
```

همچنین از n- می‌توان برای سرعت بیشتر بهره برد.

```
C:\Users\Amir Reza 81>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1309           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1536           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1539           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1540           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1542           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:50128          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1550         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1614         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1976         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:10042        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:56842        0.0.0.0:0              LISTENING
  TCP    192.168.1.106:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.106:1544     38.90.226.64:8883      ESTABLISHED
  TCP    192.168.1.106:1548     20.198.118.190:443     ESTABLISHED
  TCP    192.168.1.106:3216     20.250.77.142:443      ESTABLISHED
  TCP    192.168.1.106:5443     185.200.232.34:443     CLOSE_WAIT
  TCP    192.168.1.106:5444     185.200.232.34:443     CLOSE_WAIT
  TCP    192.168.1.106:5445     185.200.232.34:443     CLOSE_WAIT
  TCP    192.168.1.106:5446     185.200.232.34:443     CLOSE_WAIT
  TCP    192.168.1.106:5447     185.200.232.34:443     CLOSE_WAIT
  TCP    192.168.1.106:5448     185.200.232.34:443     CLOSE_WAIT
  TCP    192.168.1.106:5467     173.194.76.188:5228    ESTABLISHED
  TCP    192.168.1.106:6158     20.223.35.26:443       FIN_WAIT_1
  TCP    192.168.1.106:6210     204.79.197.239:443     TIME_WAIT
  TCP    192.168.1.106:6216     216.239.32.116:443     ESTABLISHED
  TCP    192.168.1.106:6217     130.211.17.170:443     ESTABLISHED
  TCP    192.168.1.106:6218     130.211.17.170:443     FIN_WAIT_1
  TCP    192.168.1.106:6219     172.217.18.99:443      ESTABLISHED
  TCP    192.168.1.106:6220     216.58.206.35:443      ESTABLISHED
  TCP    192.168.1.106:6221     34.104.35.123:80       ESTABLISHED
  TCP    192.168.1.106:6222     216.58.206.35:443      ESTABLISHED
  TCP    192.168.1.106:6223     216.239.36.117:443     ESTABLISHED
```

```
  TCP    192.168.1.106:6221     34.104.35.123:80       ESTABLISHED
  TCP    192.168.1.106:6222     216.58.206.35:443      ESTABLISHED
  TCP    192.168.1.106:6223     216.239.36.117:443     ESTABLISHED
  TCP    192.168.1.106:6224     172.217.18.99:443      ESTABLISHED
  TCP    192.168.1.106:6225     172.217.169.227:443    ESTABLISHED
  TCP    192.168.1.106:6226     216.239.36.117:443     ESTABLISHED
  TCP    192.168.126.1:139      0.0.0.0:0              LISTENING
  TCP    192.168.245.1:139      0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:443               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:1536              [::]:0                 LISTENING
  TCP    [::]:1537              [::]:0                 LISTENING
  TCP    [::]:1538              [::]:0                 LISTENING
  TCP    [::]:1539              [::]:0                 LISTENING
  TCP    [::]:1540              [::]:0                 LISTENING
  TCP    [::]:1542              [::]:0                 LISTENING
  TCP    [::]:5432              [::]:0                 LISTENING
  TCP    [::]:50128             [::]:0                 LISTENING
  TCP    [::1]:1541             [::]:0                 LISTENING
  TCP    [::1]:8307             [::]:0                 LISTENING
  TCP    [::1]:56842            [::]:0                 LISTENING
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:10010        *:*
  UDP    127.0.0.1:52869        *:*
  UDP    127.0.0.1:56540        *:*
  UDP    127.0.0.1:60460        *:*
  UDP    192.168.1.106:137      *:*
  UDP    192.168.1.106:138      *:*
  UDP    192.168.1.106:1900     *:*
  UDP    192.168.1.106:52868    *:*
  UDP    192.168.126.1:137      *:*
  UDP    192.168.126.1:138      *:*
  UDP    192.168.126.1:1900     *:*
```

Command Prompt

```
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:10010        *:*
  UDP    127.0.0.1:52869        *:*
  UDP    127.0.0.1:56540        *:*
  UDP    127.0.0.1:60460        *:*
  UDP    192.168.1.106:137      *:*
  UDP    192.168.1.106:138      *:*
  UDP    192.168.1.106:1900     *:*
  UDP    192.168.1.106:52868    *:*
  UDP    192.168.126.1:137      *:*
  UDP    192.168.126.1:138      *:*
  UDP    192.168.126.1:1900     *:*
  UDP    192.168.126.1:52866    *:*
  UDP    192.168.245.1:137      *:*
  UDP    192.168.245.1:138      *:*
  UDP    192.168.245.1:1900     *:*
  UDP    192.168.245.1:52867    *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:52865            *:*
  UDP    [fe80::4fa2:aac0:e023:e45e%11]:1900  *:*
  UDP    [fe80::4fa2:aac0:e023:e45e%11]:52863  *:*
  UDP    [fe80::c80f:812b:885c:3a7e%14]:1900  *:*
  UDP    [fe80::c80f:812b:885c:3a7e%14]:52862  *:*
  UDP    [fe80::d124:abb5:1ba:a629%19]:1900  *:*
  UDP    [fe80::d124:abb5:1ba:a629%19]:52864  *:*

C:\Users\Amir Reza 81>
```

4.2. TCP connections:

در این بخش هم از دستور netstat -p tcp و هم از دستور "netstat -a | find "TCP استفاده کرده‌ایم.

```
C:\Users\Amir Reza 81>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.106:1544     38-90-226-64:8883      ESTABLISHED
  TCP    192.168.1.106:1548     20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.106:3216     20.250.77.142:https    ESTABLISHED
  TCP    192.168.1.106:5443     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5444     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5445     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5446     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5447     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5448     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5467     ws-in-f188:5228        ESTABLISHED
  TCP    192.168.1.106:5886     20.54.232.160:https    TIME_WAIT
  TCP    192.168.1.106:5945     a-0003:https           TIME_WAIT
  TCP    192.168.1.106:5947     20.103.156.88:https    TIME_WAIT
  TCP    192.168.1.106:5950     i66:https              TIME_WAIT
  TCP    192.168.1.106:5951     i66:https              TIME_WAIT
  TCP    192.168.1.106:5953     server-18-165-220-57:https  TIME_WAIT
  TCP    192.168.1.106:5955     i66:https              TIME_WAIT
  TCP    192.168.1.106:5957     i66:https              TIME_WAIT
  TCP    192.168.1.106:5961     204.79.197.239:https   TIME_WAIT
  TCP    192.168.1.106:5967     mct01s10-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:5972     fra15s46-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:5973     e2a:https              FIN_WAIT_1
  TCP    192.168.1.106:5974     e2a:https              FIN_WAIT_1
  TCP    192.168.1.106:5978     a-0003:https           TIME_WAIT
  TCP    192.168.1.106:5982     i66:https              TIME_WAIT
  TCP    192.168.1.106:5983     i66:https              TIME_WAIT
  TCP    192.168.1.106:5986     server-18-165-220-57:https  TIME_WAIT
  TCP    192.168.1.106:5988     20.103.156.88:https    TIME_WAIT
  TCP    192.168.1.106:5993     mil07s07-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:5994     123:http               ESTABLISHED
  TCP    192.168.1.106:5995     a-0003:https           ESTABLISHED
  TCP    192.168.1.106:5996     mct01s20-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:5997     fra15s46-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:5998     jr-in-f94:https        ESTABLISHED
  TCP    192.168.1.106:5999     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6000     fra15s46-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6001     fra15s46-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6002     mct01s20-in-f14:https  FIN_WAIT_1

C:\Users\Amir Reza 81>
```

Command Prompt

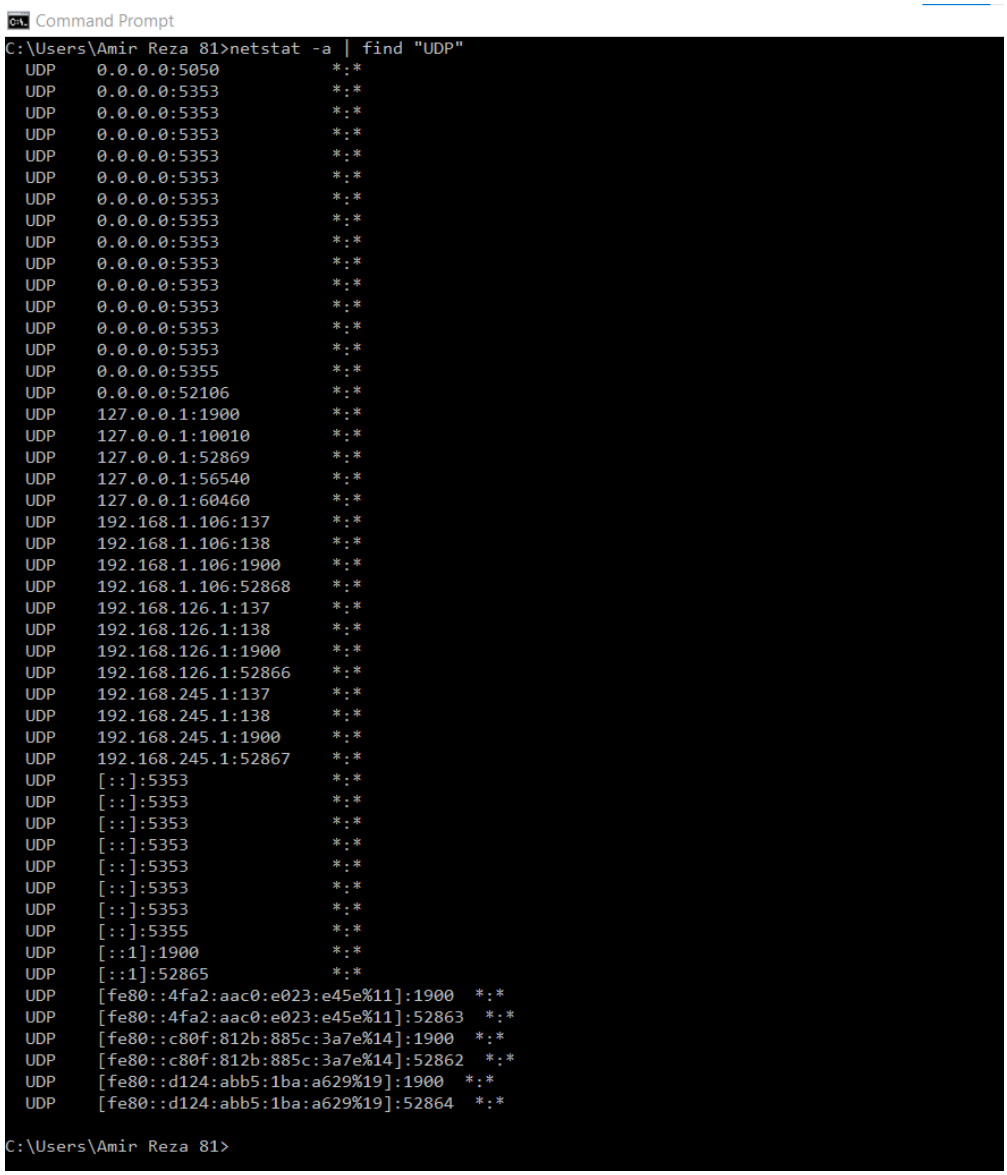
```
C:\Users\Amir Reza 81>netstat -a | find "TCP"
  TCP    0.0.0.0:135            bs:0                   LISTENING
  TCP    0.0.0.0:443            bs:0                   LISTENING
  TCP    0.0.0.0:445            bs:0                   LISTENING
  TCP    0.0.0.0:902            bs:0                   LISTENING
  TCP    0.0.0.0:912            bs:0                   LISTENING
  TCP    0.0.0.0:1309           bs:0                   LISTENING
  TCP    0.0.0.0:1536           bs:0                   LISTENING
  TCP    0.0.0.0:1537           bs:0                   LISTENING
  TCP    0.0.0.0:1538           bs:0                   LISTENING
  TCP    0.0.0.0:1539           bs:0                   LISTENING
  TCP    0.0.0.0:1540           bs:0                   LISTENING
  TCP    0.0.0.0:1542           bs:0                   LISTENING
  TCP    0.0.0.0:5040           bs:0                   LISTENING
  TCP    0.0.0.0:5432           bs:0                   LISTENING
  TCP    0.0.0.0:50128          bs:0                   LISTENING
  TCP    127.0.0.1:1001         bs:0                   LISTENING
  TCP    127.0.0.1:1550         bs:0                   LISTENING
  TCP    127.0.0.1:1614         bs:0                   LISTENING
  TCP    127.0.0.1:1976         bs:0                   LISTENING
  TCP    127.0.0.1:8307         bs:0                   LISTENING
  TCP    127.0.0.1:10042        bs:0                   LISTENING
  TCP    127.0.0.1:56842        bs:0                   LISTENING
  TCP    192.168.1.106:139      bs:0                   LISTENING
  TCP    192.168.1.106:1544     38-90-226-64:8883      ESTABLISHED
  TCP    192.168.1.106:1548     20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.106:3216     20.250.77.142:https    ESTABLISHED
  TCP    192.168.1.106:5443     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5444     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5445     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5446     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5447     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5448     185.200.232.34:https   CLOSE_WAIT
  TCP    192.168.1.106:5467     ws-in-f188:5228        ESTABLISHED
  TCP    192.168.1.106:6033     a-0003:https           FIN_WAIT_2
  TCP    192.168.1.106:6042     me-in-f94:https        FIN_WAIT_1
  TCP    192.168.1.106:6043     me-in-f94:https        FIN_WAIT_1
  TCP    192.168.1.106:6050     bingforbusiness:http   TIME_WAIT
  TCP    192.168.1.106:6053     204.79.197.237:https   FIN_WAIT_2
  TCP    192.168.1.106:6055     185.200.232.9:https    TIME_WAIT
  TCP    192.168.1.106:6056     185.200.232.9:https    TIME_WAIT
  TCP    192.168.1.106:6057     185.200.232.67:https   TIME_WAIT
  TCP    192.168.1.106:6058     server-18-165-220-106:https  TIME_WAIT
  TCP    192.168.1.106:6060     20.199.58.43:https     TIME_WAIT
  TCP    192.168.1.106:6063     a-0003:https           FIN_WAIT_2
  TCP    192.168.1.106:6067     204.79.197.239:https   FIN_WAIT_1
  TCP    192.168.1.106:6076     131.253.33.220:https   FIN_WAIT_2
  TCP    192.168.1.106:6080     fra15s46-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:6081     fra15s46-in-f3:https   FIN_WAIT_1
```

```
  TCP    192.168.1.106:6076     131.253.33.220:https   FIN_WAIT_2
  TCP    192.168.1.106:6080     fra15s46-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:6081     fra15s46-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:6084     mia09s02-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:6087     mia09s02-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:6090     mil07s07-in-f3:https   FIN_WAIT_1
  TCP    192.168.1.106:6105     e2a:https              FIN_WAIT_1
  TCP    192.168.1.106:6108     20.69.137.228:https    ESTABLISHED
  TCP    192.168.1.106:6109     131.253.33.220:https   ESTABLISHED
  TCP    192.168.1.106:6110     20.189.173.18:https    ESTABLISHED
  TCP    192.168.1.106:6111     mct01s10-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6113     mct04s04-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6114     123:http               ESTABLISHED
  TCP    192.168.1.106:6115     a-0003:https           ESTABLISHED
  TCP    192.168.1.106:6116     jr-in-f94:https        ESTABLISHED
  TCP    192.168.1.106:6117     jr-in-f94:https        ESTABLISHED
  TCP    192.168.1.106:6118     a-0003:https           SYN_SENT
  TCP    192.168.1.106:6119     20.85.30.134:https     ESTABLISHED
  TCP    192.168.1.106:6120     20.85.30.134:https     ESTABLISHED
  TCP    192.168.1.106:6121     fra15s46-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6122     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6123     e2a:https              ESTABLISHED
  TCP    192.168.1.106:6124     mil07s07-in-f3:https   ESTABLISHED
  TCP    192.168.1.106:6125     mil07s07-in-f3:https   ESTABLISHED
  TCP    192.168.126.1:139      bs:0                   LISTENING
  TCP    192.168.245.1:139      bs:0                   LISTENING
  TCP    [::]:135               AmirReza:0             LISTENING
  TCP    [::]:443               AmirReza:0             LISTENING
  TCP    [::]:445               AmirReza:0             LISTENING
  TCP    [::]:1536              AmirReza:0             LISTENING
  TCP    [::]:1537              AmirReza:0             LISTENING
  TCP    [::]:1538              AmirReza:0             LISTENING
  TCP    [::]:1539              AmirReza:0             LISTENING
  TCP    [::]:1540              AmirReza:0             LISTENING
  TCP    [::]:1542              AmirReza:0             LISTENING
  TCP    [::]:5432              AmirReza:0             LISTENING
  TCP    [::]:50128             AmirReza:0             LISTENING
  TCP    [::1]:1541             AmirReza:0             LISTENING
  TCP    [::1]:8307             AmirReza:0             LISTENING
  TCP    [::1]:56842            AmirReza:0             LISTENING

C:\Users\Amir Reza 81>
```

4.3. UDP connections:

در این تصویر تمام کانکشن‌های udp در حالت listen را مشاهده می‌کنید.



از netstat -ap udp هم می‌توان استفاده کرد.

```
C:\Users\Amir Reza 81>netstat -ap udp

Active Connections

  Proto  Local Address          Foreign Address        State
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:10010        *:*
  UDP    127.0.0.1:52869        *:*
  UDP    127.0.0.1:56540        *:*
  UDP    127.0.0.1:60460        *:*
  UDP    192.168.1.106:137      *:*
  UDP    192.168.1.106:138      *:*
  UDP    192.168.1.106:1900     *:*
  UDP    192.168.1.106:52868    *:*
  UDP    192.168.126.1:137      *:*
  UDP    192.168.126.1:138      *:*
  UDP    192.168.126.1:1900     *:*
  UDP    192.168.126.1:52866    *:*
  UDP    192.168.245.1:137      *:*
  UDP    192.168.245.1:138      *:*
  UDP    192.168.245.1:1900     *:*
  UDP    192.168.245.1:52867    *:*

C:\Users\Amir Reza 81>
```

۴.۴. IP packets:

```
C:\Users\Amir Reza 81>netstat -ps ip

IPv4 Statistics

  Packets Received                   = 166511
  Received Header Errors             = 2
  Received Address Errors            = 0
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 2201
  Received Packets Delivered         = 168446
  Output Requests                    = 146000
  Routing Discards                   = 0
  Discarded Output Packets           = 972
  Output Packet No Route             = 24
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

C:\Users\Amir Reza 81>
```

از s- برای گرفتن آمار استفاده می‌کنیم.

برای اطلاعات بیشتر از انواع flagها، این لینک مناسب است.

ویدیوهای مربوط به سوالات 2 تا 4 ، در فایل زیپِ آپلود شده موجود می‌باشند.