Computer Networks Lab 3

Goutam Halder
ID: M24CS005

Q1

Find all the active TCP ports on your system. Identify the ports and PIDs of your web browser. Can you identify the port number and PID of a specific TAB in your browser? Find out if any of the services running in your system use the standard ports of HTTP, DHCP, DNS, SMTP, and FTP.

Answer:
First I used the command "**netstat -an | findstr "TCP"**" in windows cmd. Where

- "-a": Displays all active connections and listening ports.
- "-n": Displays addresses and port numbers in numerical form.
- "findstr": To filter only TCP connections.

Now I used this command "**netstat -ano**" in windows cmd and also opened the Task Manger and opened the details page inside it.
I located a chrome task in the Task Manager with PID of 15400 and port number 5353.

Unfortunately, I'm unable to identify the PID for specific tab in chrome browser. Browsers typically run all tabs under the same process or share a pool of processes. So it is very hard to identify a specific tab.

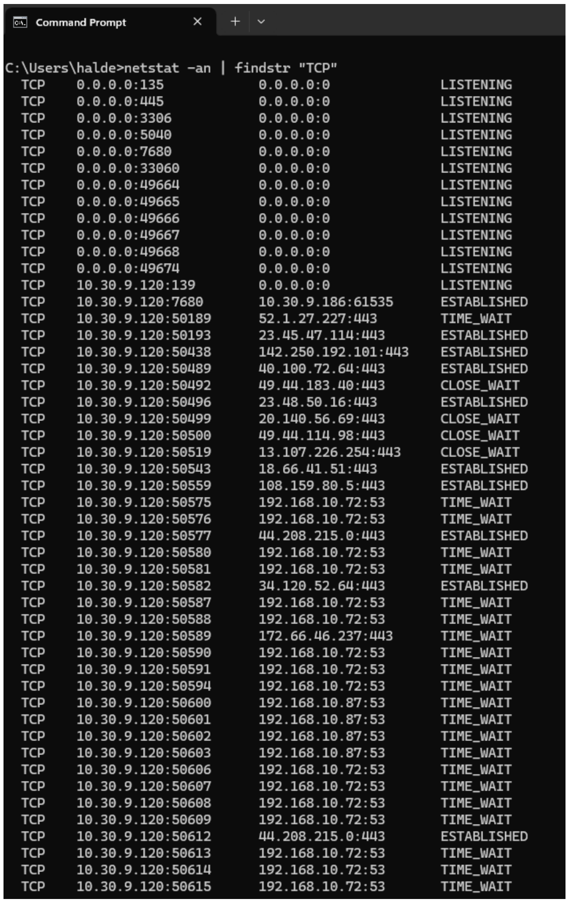
To check if any of the services running in my system use the standard ports of HTTP, DHCP, DNS, SMTP, and FTP, I used following commands.

```
netstat -an | findstr :80
netstat -an | findstr :443
netstat -an | findstr :67
netstat -an | findstr :68
netstat -an | findstr :53
netstat -an | findstr :25
```

netstat -an | findstr :21

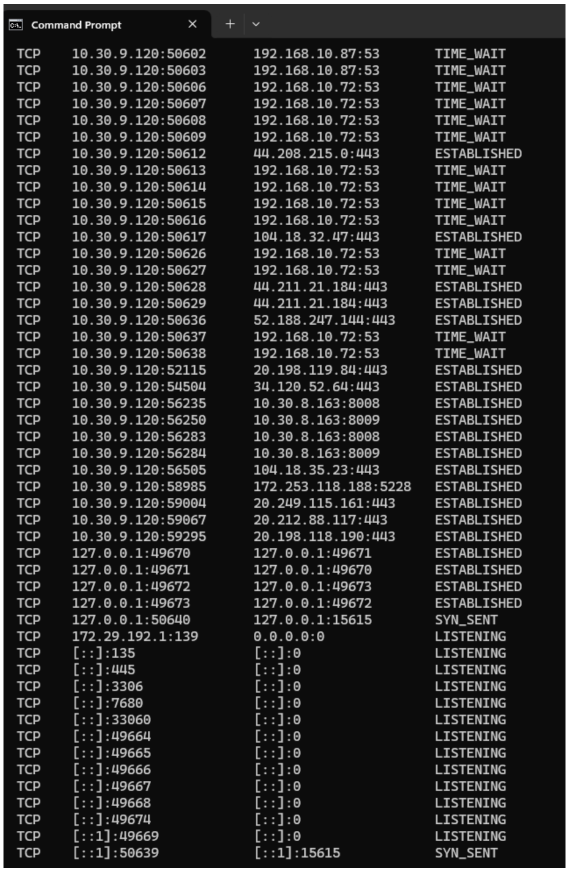
where

- Port 80: HTTP
- Port 443: HTTPS
- Port 67/68: DHCP
- Port 53: DNS
- Port 25: SMTP
- Port 21: FTP



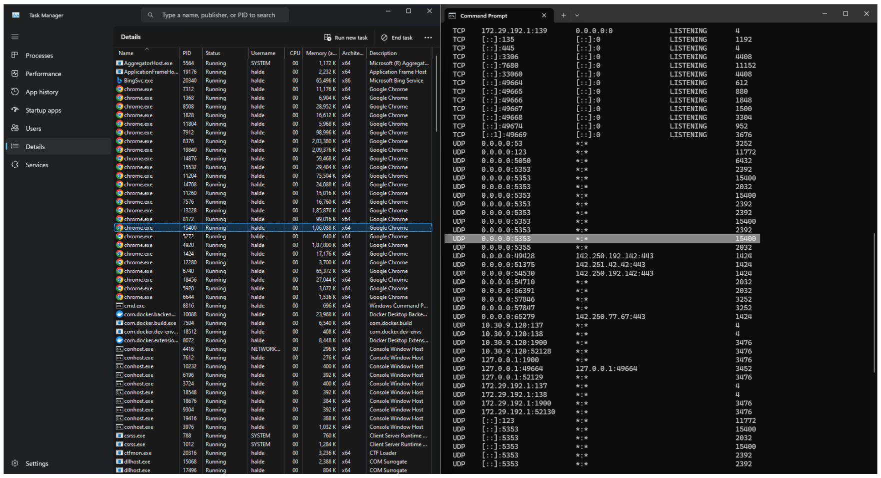
```
C:\Users\halde>netstat -an | findstr "TCP"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:33060          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    10.30.9.120:139        0.0.0.0:0              LISTENING
  TCP    10.30.9.120:7680       10.30.9.186:61535      ESTABLISHED
  TCP    10.30.9.120:50189      52.1.27.227:443        TIME_WAIT
  TCP    10.30.9.120:50193      23.45.47.114:443       ESTABLISHED
  TCP    10.30.9.120:50438      142.250.192.101:443    ESTABLISHED
  TCP    10.30.9.120:50489      40.100.72.64:443       ESTABLISHED
  TCP    10.30.9.120:50492      49.44.183.40:443       CLOSE_WAIT
  TCP    10.30.9.120:50496      23.48.50.16:443        ESTABLISHED
  TCP    10.30.9.120:50499      20.140.56.69:443       CLOSE_WAIT
  TCP    10.30.9.120:50500      49.44.114.98:443       CLOSE_WAIT
  TCP    10.30.9.120:50519      13.107.226.254:443     CLOSE_WAIT
  TCP    10.30.9.120:50543      18.66.41.51:443        ESTABLISHED
  TCP    10.30.9.120:50559      108.159.80.5:443       ESTABLISHED
  TCP    10.30.9.120:50575      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50576      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50577      44.208.215.0:443       ESTABLISHED
  TCP    10.30.9.120:50580      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50581      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50582      34.120.52.64:443       ESTABLISHED
  TCP    10.30.9.120:50587      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50588      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50589      172.66.46.237:443      TIME_WAIT
  TCP    10.30.9.120:50590      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50591      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50594      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50600      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50601      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50602      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50603      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50606      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50607      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50608      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50609      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50612      44.208.215.0:443       ESTABLISHED
  TCP    10.30.9.120:50613      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50614      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50615      192.168.10.72:53       TIME_WAIT
```

Figure 1: All TCP ports



```
  TCP    10.30.9.120:50602      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50603      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50606      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50607      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50608      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50609      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50612      44.208.215.0:443       ESTABLISHED
  TCP    10.30.9.120:50613      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50614      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50615      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50616      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50617      104.18.32.47:443       ESTABLISHED
  TCP    10.30.9.120:50626      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50627      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50628      44.211.21.184:443      ESTABLISHED
  TCP    10.30.9.120:50629      44.211.21.184:443      ESTABLISHED
  TCP    10.30.9.120:50636      52.188.247.144:443     ESTABLISHED
  TCP    10.30.9.120:50637      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50638      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:52115      20.198.119.84:443      ESTABLISHED
  TCP    10.30.9.120:54504      34.120.52.64:443       ESTABLISHED
  TCP    10.30.9.120:56235      10.30.8.163:8008       ESTABLISHED
  TCP    10.30.9.120:56250      10.30.8.163:8009       ESTABLISHED
  TCP    10.30.9.120:56283      10.30.8.163:8008       ESTABLISHED
  TCP    10.30.9.120:56284      10.30.8.163:8009       ESTABLISHED
  TCP    10.30.9.120:56505      104.18.35.23:443       ESTABLISHED
  TCP    10.30.9.120:58985      172.253.118.188:5228   ESTABLISHED
  TCP    10.30.9.120:59004      20.249.115.161:443     ESTABLISHED
  TCP    10.30.9.120:59067      20.212.88.117:443      ESTABLISHED
  TCP    10.30.9.120:59295      20.198.118.190:443     ESTABLISHED
  TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED
  TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED
  TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED
  TCP    127.0.0.1:49673        127.0.0.1:49672        ESTABLISHED
  TCP    127.0.0.1:50640        127.0.0.1:15615        SYN_SENT
  TCP    172.29.192.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:3306              [::]:0                 LISTENING
  TCP    [::]:7680              [::]:0                 LISTENING
  TCP    [::]:33060             [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49674             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  TCP    [::1]:50639            [::1]:15615            SYN_SENT
```

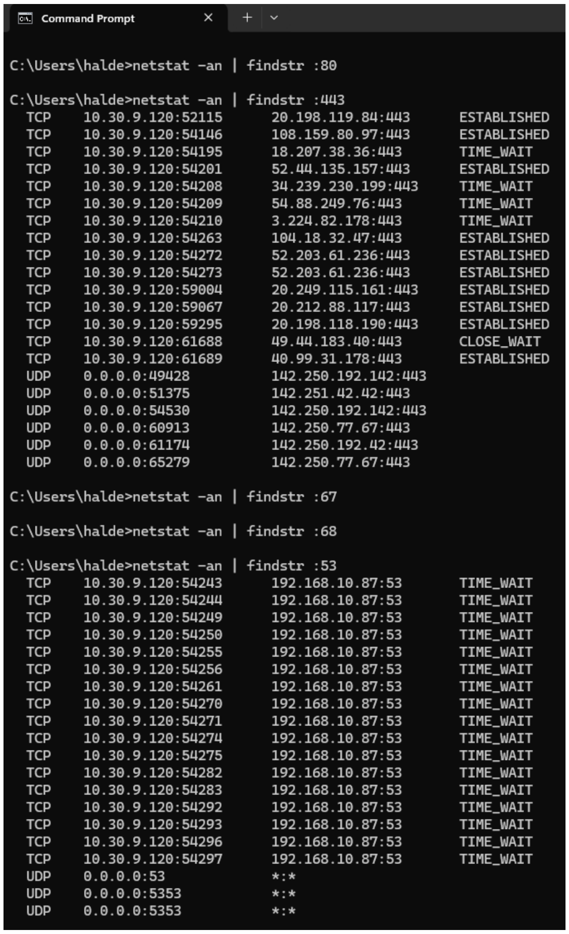
Figure 2: All TCP ports



Name	PID	Status	Username	CPU	Memory (a...	Archite...	Description
AggregatorHost.exe	5564	Running	SYSTEM	00	1,172 K	x64	Microsoft (R) Aggregat...
ApplicationFrameHo...	19176	Running	halde	00	2,232 K	x64	Application Frame Host
BingSvc.exe	20340	Running	halde	00	65,496 K	x86	Microsoft Bing Service
chrome.exe	7312	Running	halde	00	11,176 K	x64	Google Chrome
chrome.exe	1368	Running	halde	00	6,904 K	x64	Google Chrome
chrome.exe	8508	Running	halde	00	28,952 K	x64	Google Chrome
chrome.exe	1828	Running	halde	00	16,612 K	x64	Google Chrome
chrome.exe	11804	Running	halde	00	5,968 K	x64	Google Chrome
chrome.exe	7912	Running	halde	00	98,996 K	x64	Google Chrome
chrome.exe	8376	Running	halde	00	2,03,380 K	x64	Google Chrome
chrome.exe	19840	Running	halde	00	2,09,376 K	x64	Google Chrome
chrome.exe	14876	Running	halde	00	59,468 K	x64	Google Chrome
chrome.exe	15532	Running	halde	00	29,404 K	x64	Google Chrome
chrome.exe	11204	Running	halde	00	75,504 K	x64	Google Chrome
chrome.exe	14708	Running	halde	00	24,088 K	x64	Google Chrome
chrome.exe	11260	Running	halde	00	15,016 K	x64	Google Chrome
chrome.exe	7576	Running	halde	00	16,760 K	x64	Google Chrome
chrome.exe	13228	Running	halde	00	1,85,876 K	x64	Google Chrome
chrome.exe	8172	Running	halde	00	99,016 K	x64	Google Chrome
chrome.exe	15400	Running	halde	00	1,06,088 K	x64	Google Chrome
chrome.exe	5272	Running	halde	00	640 K	x64	Google Chrome
chrome.exe	4920	Running	halde	00	1,87,800 K	x64	Google Chrome
chrome.exe	1424	Running	halde	00	17,176 K	x64	Google Chrome
chrome.exe	12280	Running	halde	00	3,700 K	x64	Google Chrome
chrome.exe	6740	Running	halde	00	65,372 K	x64	Google Chrome
chrome.exe	18456	Running	halde	00	27,044 K	x64	Google Chrome
chrome.exe	5920	Running	halde	00	3,072 K	x64	Google Chrome
chrome.exe	6644	Running	halde	00	1,536 K	x64	Google Chrome
cmd.exe	8316	Running	halde	00	696 K	x64	Windows Command P...
com.docker.backen...	10088	Running	halde	00	23,968 K	x64	Docker Desktop Backe...
com.docker.build.exe	7504	Running	halde	00	6,540 K	x64	com.docker.build
com.docker.dev-env...	18512	Running	halde	00	408 K	x64	com.docker.dev-envs
com.docker.extensio...	8072	Running	halde	00	8,448 K	x64	Docker Desktop Extens...
conhost.exe	4416	Running	NETWORK...	00	296 K	x64	Console Window Host
conhost.exe	7612	Running	halde	00	276 K	x64	Console Window Host
conhost.exe	10232	Running	halde	00	400 K	x64	Console Window Host
conhost.exe	6196	Running	halde	00	392 K	x64	Console Window Host
conhost.exe	3724	Running	halde	00	400 K	x64	Console Window Host
conhost.exe	18548	Running	halde	00	392 K	x64	Console Window Host
conhost.exe	18676	Running	halde	00	384 K	x64	Console Window Host
conhost.exe	9304	Running	halde	00	392 K	x64	Console Window Host
conhost.exe	19416	Running	halde	00	388 K	x64	Console Window Host
conhost.exe	3976	Running	halde	00	1,032 K	x64	Console Window Host
csrss.exe	788	Running	SYSTEM	00	760 K		Client Server Runtime ...
csrss.exe	1012	Running	SYSTEM	00	1,284 K		Client Server Runtime ...
ctfmon.exe	20316	Running	halde	00	3,236 K	x64	CTF Loader
dllhost.exe	15068	Running	halde	00	2,388 K	x64	COM Surrogate
dllhost.exe	17496	Running	halde	00	804 K	x64	COM Surrogate

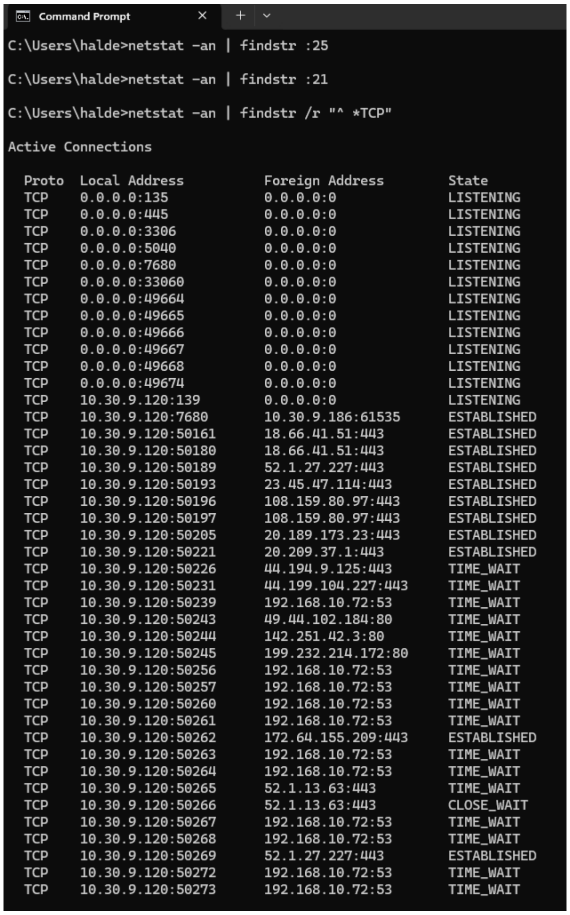
```
  TCP    172.29.192.1:139       0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       1192
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3306              [::]:0                 LISTENING       4408
  TCP    [::]:7680              [::]:0                 LISTENING       11152
  TCP    [::]:33060             [::]:0                 LISTENING       4408
  TCP    [::]:49664             [::]:0                 LISTENING       612
  TCP    [::]:49665             [::]:0                 LISTENING       880
  TCP    [::]:49666             [::]:0                 LISTENING       1848
  TCP    [::]:49667             [::]:0                 LISTENING       1500
  TCP    [::]:49668             [::]:0                 LISTENING       3304
  TCP    [::]:49674             [::]:0                 LISTENING       952
  TCP    [::1]:49669            [::]:0                 LISTENING       3676
  UDP    0.0.0.0:53             *:*                                    3252
  UDP    0.0.0.0:123            *:*                                    11772
  UDP    0.0.0.0:5050           *:*                                    6432
  UDP    0.0.0.0:5353           *:*                                    2392
  UDP    0.0.0.0:5353           *:*                                    15400
  UDP    0.0.0.0:5353           *:*                                    2032
  UDP    0.0.0.0:5353           *:*                                    15400
  UDP    0.0.0.0:5353           *:*                                    2392
  UDP    0.0.0.0:5353           *:*                                    2392
  UDP    0.0.0.0:5353           *:*                                    15400
  UDP    0.0.0.0:5353           *:*                                    2392
  UDP    0.0.0.0:5353           *:*                                    15400
  UDP    0.0.0.0:5355           *:*                                    2032
  UDP    0.0.0.0:49428          142.250.192.142:443                    1424
  UDP    0.0.0.0:51375          142.251.42.42:443                      1424
  UDP    0.0.0.0:54530          142.250.192.142:443                    1424
  UDP    0.0.0.0:54710          *:*                                    2032
  UDP    0.0.0.0:56391          *:*                                    2032
  UDP    0.0.0.0:57846          *:*                                    3252
  UDP    0.0.0.0:57847          *:*                                    3252
  UDP    0.0.0.0:65279          142.250.77.67:443                      1424
  UDP    10.30.9.120:137        *:*                                    4
  UDP    10.30.9.120:138        *:*                                    4
  UDP    10.30.9.120:1900       *:*                                    3476
  UDP    10.30.9.120:52128      *:*                                    3476
  UDP    127.0.0.1:1900         *:*                                    3476
  UDP    127.0.0.1:49664        127.0.0.1:49664                        3452
  UDP    127.0.0.1:52129        *:*                                    3476
  UDP    172.29.192.1:137       *:*                                    4
  UDP    172.29.192.1:138       *:*                                    4
  UDP    172.29.192.1:1900      *:*                                    3476
  UDP    172.29.192.1:52130     *:*                                    3476
  UDP    [::]:123               *:*                                    11772
  UDP    [::]:5353              *:*                                    15400
  UDP    [::]:5353              *:*                                    2032
  UDP    [::]:5353              *:*                                    15400
  UDP    [::]:5353              *:*                                    2392
  UDP    [::]:5353              *:*                                    2392
```

Figure 3: Found port and PID of chrome.



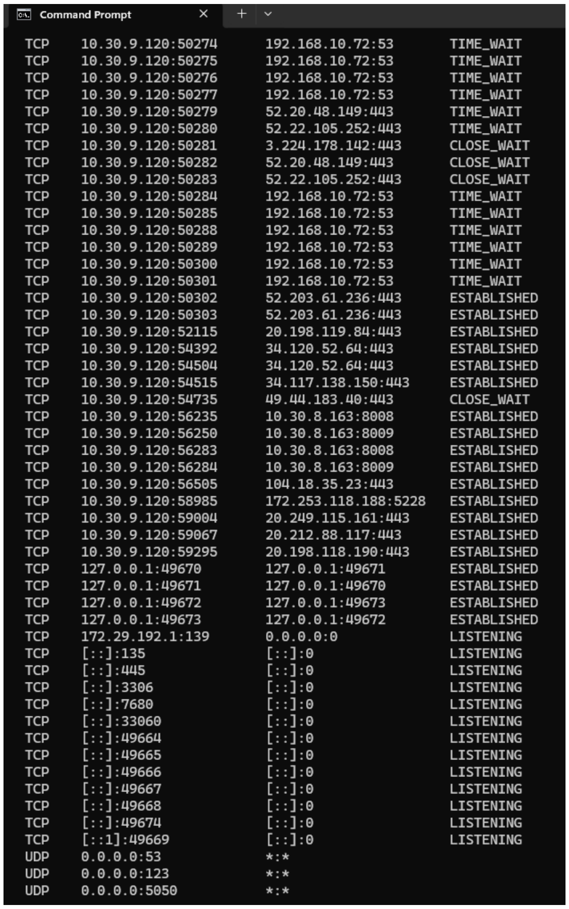
```
C:\Users\halde>netstat -an | findstr :80

C:\Users\halde>netstat -an | findstr :443
  TCP    10.30.9.120:52115      20.198.119.84:443      ESTABLISHED
  TCP    10.30.9.120:54146      108.159.80.97:443      ESTABLISHED
  TCP    10.30.9.120:54195      18.207.38.36:443       TIME_WAIT
  TCP    10.30.9.120:54201      52.44.135.157:443      ESTABLISHED
  TCP    10.30.9.120:54208      34.239.230.199:443     TIME_WAIT
  TCP    10.30.9.120:54209      54.88.249.76:443       TIME_WAIT
  TCP    10.30.9.120:54210      3.224.82.178:443       TIME_WAIT
  TCP    10.30.9.120:54263      104.18.32.47:443       ESTABLISHED
  TCP    10.30.9.120:54272      52.203.61.236:443      ESTABLISHED
  TCP    10.30.9.120:54273      52.203.61.236:443      ESTABLISHED
  TCP    10.30.9.120:59004      20.249.115.161:443     ESTABLISHED
  TCP    10.30.9.120:59067      20.212.88.117:443      ESTABLISHED
  TCP    10.30.9.120:59295      20.198.118.190:443     ESTABLISHED
  TCP    10.30.9.120:61688      49.44.183.40:443       CLOSE_WAIT
  TCP    10.30.9.120:61689      40.99.31.178:443       ESTABLISHED
  UDP    0.0.0.0:49428          142.250.192.142:443
  UDP    0.0.0.0:51375          142.251.42.42:443
  UDP    0.0.0.0:54530          142.250.192.142:443
  UDP    0.0.0.0:60913          142.250.77.67:443
  UDP    0.0.0.0:61174          142.250.192.42:443
  UDP    0.0.0.0:65279          142.250.77.67:443

C:\Users\halde>netstat -an | findstr :67

C:\Users\halde>netstat -an | findstr :68

C:\Users\halde>netstat -an | findstr :53
  TCP    10.30.9.120:54243      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54244      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54249      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54250      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54255      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54256      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54261      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54270      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54271      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54274      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54275      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54282      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54283      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54292      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54293      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54296      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:54297      192.168.10.87:53       TIME_WAIT
  UDP    0.0.0.0:53             *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
```

Figure 4:



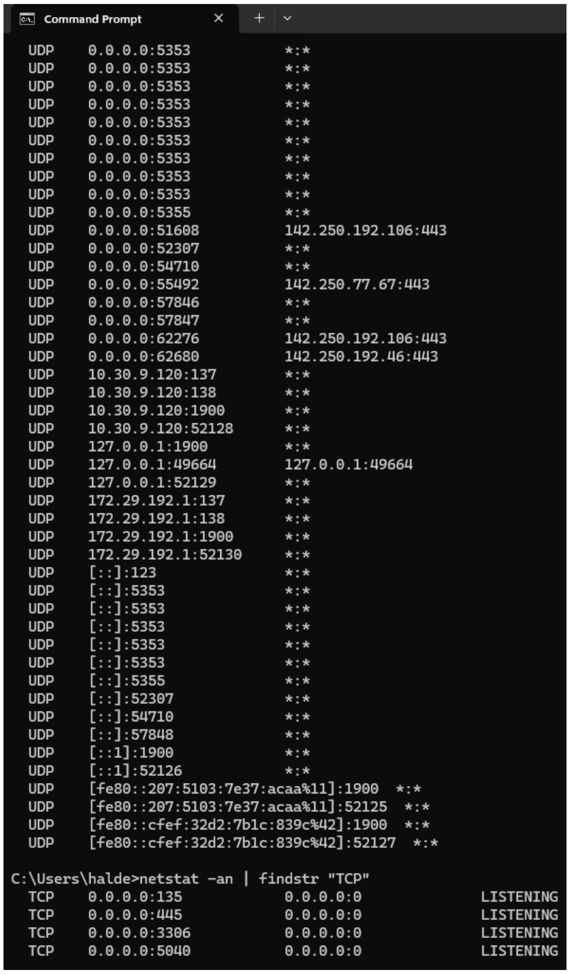
```
C:\Users\halde>netstat -an | findstr :25

C:\Users\halde>netstat -an | findstr :21

C:\Users\halde>netstat -an | findstr /r "^ *TCP"

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:33060          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    10.30.9.120:139        0.0.0.0:0              LISTENING
  TCP    10.30.9.120:7680       10.30.9.186:61535      ESTABLISHED
  TCP    10.30.9.120:50161      18.66.41.51:443        ESTABLISHED
  TCP    10.30.9.120:50180      18.66.41.51:443        ESTABLISHED
  TCP    10.30.9.120:50189      52.1.27.227:443        ESTABLISHED
  TCP    10.30.9.120:50193      23.45.47.114:443       ESTABLISHED
  TCP    10.30.9.120:50196      108.159.80.97:443      ESTABLISHED
  TCP    10.30.9.120:50197      108.159.80.97:443      ESTABLISHED
  TCP    10.30.9.120:50205      20.189.173.23:443      ESTABLISHED
  TCP    10.30.9.120:50221      20.209.37.1:443        ESTABLISHED
  TCP    10.30.9.120:50226      44.194.9.125:443       TIME_WAIT
  TCP    10.30.9.120:50231      44.199.104.227:443     TIME_WAIT
  TCP    10.30.9.120:50239      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50243      49.44.102.184:80       TIME_WAIT
  TCP    10.30.9.120:50244      142.251.42.3:80        TIME_WAIT
  TCP    10.30.9.120:50245      199.232.214.172:80     TIME_WAIT
  TCP    10.30.9.120:50256      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50257      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50260      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50261      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50262      172.64.155.209:443     ESTABLISHED
  TCP    10.30.9.120:50263      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50264      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50265      52.1.13.63:443         TIME_WAIT
  TCP    10.30.9.120:50266      52.1.13.63:443         CLOSE_WAIT
  TCP    10.30.9.120:50267      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50268      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50269      52.1.27.227:443        ESTABLISHED
  TCP    10.30.9.120:50272      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50273      192.168.10.72:53       TIME_WAIT
```

Figure 5:



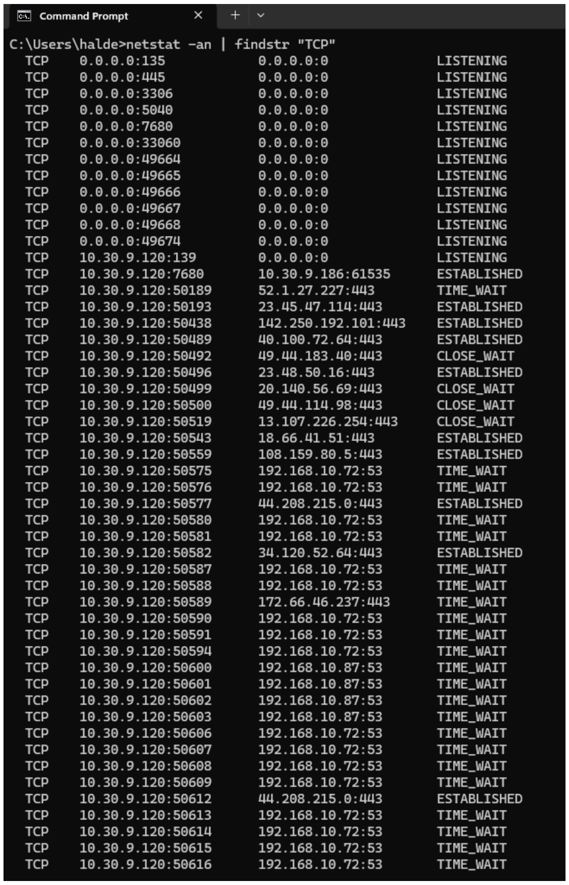
```
  TCP    10.30.9.120:50274      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50275      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50276      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50277      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50279      52.20.48.149:443       TIME_WAIT
  TCP    10.30.9.120:50280      52.22.105.252:443      TIME_WAIT
  TCP    10.30.9.120:50281      3.224.178.142:443      CLOSE_WAIT
  TCP    10.30.9.120:50282      52.20.48.149:443       CLOSE_WAIT
  TCP    10.30.9.120:50283      52.22.105.252:443      CLOSE_WAIT
  TCP    10.30.9.120:50284      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50285      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50288      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50289      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50300      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50301      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50302      52.203.61.236:443      ESTABLISHED
  TCP    10.30.9.120:50303      52.203.61.236:443      ESTABLISHED
  TCP    10.30.9.120:52115      20.198.119.84:443      ESTABLISHED
  TCP    10.30.9.120:54392      34.120.52.64:443       ESTABLISHED
  TCP    10.30.9.120:54504      34.120.52.64:443       ESTABLISHED
  TCP    10.30.9.120:54515      34.117.138.150:443     ESTABLISHED
  TCP    10.30.9.120:54735      49.44.183.40:443       CLOSE_WAIT
  TCP    10.30.9.120:56235      10.30.8.163:8008       ESTABLISHED
  TCP    10.30.9.120:56250      10.30.8.163:8009       ESTABLISHED
  TCP    10.30.9.120:56283      10.30.8.163:8008       ESTABLISHED
  TCP    10.30.9.120:56284      10.30.8.163:8009       ESTABLISHED
  TCP    10.30.9.120:56505      104.18.35.23:443       ESTABLISHED
  TCP    10.30.9.120:58985      172.253.118.188:5228   ESTABLISHED
  TCP    10.30.9.120:59004      20.249.115.161:443     ESTABLISHED
  TCP    10.30.9.120:59067      20.212.88.117:443      ESTABLISHED
  TCP    10.30.9.120:59295      20.198.118.190:443     ESTABLISHED
  TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED
  TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED
  TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED
  TCP    127.0.0.1:49673        127.0.0.1:49672        ESTABLISHED
  TCP    172.29.192.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:3306              [::]:0                 LISTENING
  TCP    [::]:7680              [::]:0                 LISTENING
  TCP    [::]:33060             [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49674             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  UDP    0.0.0.0:53             *:*
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:5050           *:*
```

Figure 6:



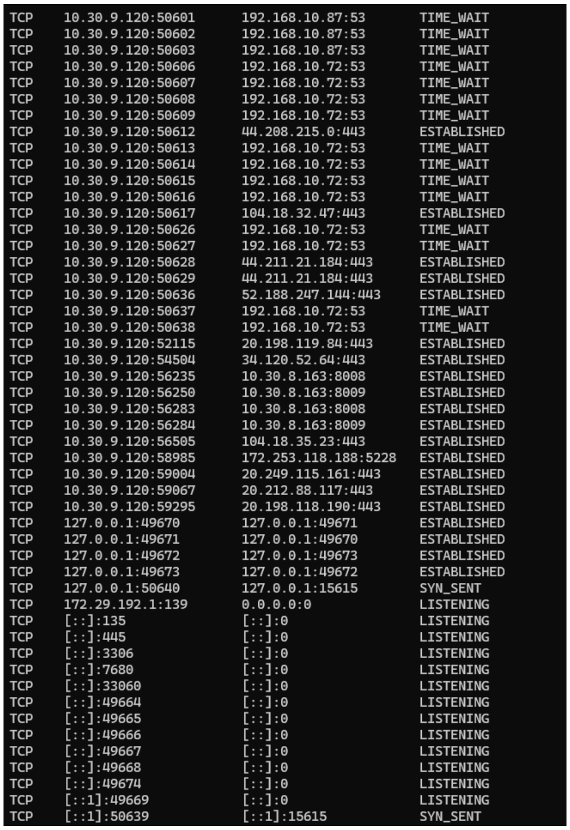
```
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:51608          142.250.192.106:443
  UDP    0.0.0.0:52307          *:*
  UDP    0.0.0.0:54710          *:*
  UDP    0.0.0.0:55492          142.250.77.67:443
  UDP    0.0.0.0:57846          *:*
  UDP    0.0.0.0:57847          *:*
  UDP    0.0.0.0:62276          142.250.192.106:443
  UDP    0.0.0.0:62680          142.250.192.46:443
  UDP    10.30.9.120:137        *:*
  UDP    10.30.9.120:138        *:*
  UDP    10.30.9.120:1900       *:*
  UDP    10.30.9.120:52128      *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:49664        127.0.0.1:49664
  UDP    127.0.0.1:52129        *:*
  UDP    172.29.192.1:137       *:*
  UDP    172.29.192.1:138       *:*
  UDP    172.29.192.1:1900      *:*
  UDP    172.29.192.1:52130     *:*
  UDP    [::]:123               *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:52307             *:*
  UDP    [::]:54710             *:*
  UDP    [::]:57848             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:52126            *:*
  UDP    [fe80::207:5103:7e37:acaa%11]:1900  *:*
  UDP    [fe80::207:5103:7e37:acaa%11]:52125  *:*
  UDP    [fe80::cfef:32d2:7b1c:839c%42]:1900  *:*
  UDP    [fe80::cfef:32d2:7b1c:839c%42]:52127  *:*

C:\Users\halde>netstat -an | findstr "TCP"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
```

Figure 7:



```
C:\Users\halde>netstat -an | findstr "TCP"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:33060          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    10.30.9.120:139        0.0.0.0:0              LISTENING
  TCP    10.30.9.120:7680       10.30.9.186:61535      ESTABLISHED
  TCP    10.30.9.120:50189      52.1.27.227:443        TIME_WAIT
  TCP    10.30.9.120:50193      23.45.47.114:443       ESTABLISHED
  TCP    10.30.9.120:50438      142.250.192.101:443    ESTABLISHED
  TCP    10.30.9.120:50489      40.100.72.64:443       ESTABLISHED
  TCP    10.30.9.120:50492      49.44.183.40:443       CLOSE_WAIT
  TCP    10.30.9.120:50496      23.48.50.16:443        ESTABLISHED
  TCP    10.30.9.120:50499      20.140.56.69:443       CLOSE_WAIT
  TCP    10.30.9.120:50500      49.44.114.98:443       CLOSE_WAIT
  TCP    10.30.9.120:50519      13.107.226.254:443     CLOSE_WAIT
  TCP    10.30.9.120:50543      18.66.41.51:443        ESTABLISHED
  TCP    10.30.9.120:50559      108.159.80.5:443       ESTABLISHED
  TCP    10.30.9.120:50575      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50576      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50577      44.208.215.0:443       ESTABLISHED
  TCP    10.30.9.120:50580      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50581      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50582      34.120.52.64:443       ESTABLISHED
  TCP    10.30.9.120:50587      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50588      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50589      172.66.46.237:443      TIME_WAIT
  TCP    10.30.9.120:50590      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50591      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50594      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50600      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50601      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50602      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50603      192.168.10.87:53       TIME_WAIT
  TCP    10.30.9.120:50606      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50607      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50608      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50609      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50612      44.208.215.0:443       ESTABLISHED
  TCP    10.30.9.120:50613      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50614      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50615      192.168.10.72:53       TIME_WAIT
  TCP    10.30.9.120:50616      192.168.10.72:53       TIME_WAIT
```

Figure 8:



```
TCP    10.30.9.120:50601      192.168.10.87:53       TIME_WAIT
TCP    10.30.9.120:50602      192.168.10.87:53       TIME_WAIT
TCP    10.30.9.120:50603      192.168.10.87:53       TIME_WAIT
TCP    10.30.9.120:50606      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50607      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50608      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50609      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50612      44.208.215.0:443       ESTABLISHED
TCP    10.30.9.120:50613      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50614      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50615      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50616      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50617      104.18.32.47:443       ESTABLISHED
TCP    10.30.9.120:50626      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50627      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50628      44.211.21.184:443      ESTABLISHED
TCP    10.30.9.120:50629      44.211.21.184:443      ESTABLISHED
TCP    10.30.9.120:50636      52.188.247.144:443     ESTABLISHED
TCP    10.30.9.120:50637      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:50638      192.168.10.72:53       TIME_WAIT
TCP    10.30.9.120:52115      20.198.119.84:443      ESTABLISHED
TCP    10.30.9.120:54504      34.120.52.64:443       ESTABLISHED
TCP    10.30.9.120:56235      10.30.8.163:8008       ESTABLISHED
TCP    10.30.9.120:56250      10.30.8.163:8009       ESTABLISHED
TCP    10.30.9.120:56283      10.30.8.163:8008       ESTABLISHED
TCP    10.30.9.120:56284      10.30.8.163:8009       ESTABLISHED
TCP    10.30.9.120:56505      104.18.35.23:443       ESTABLISHED
TCP    10.30.9.120:58985      172.253.118.188:5228   ESTABLISHED
TCP    10.30.9.120:59004      20.249.115.161:443     ESTABLISHED
TCP    10.30.9.120:59067      20.212.88.117:443      ESTABLISHED
TCP    10.30.9.120:59295      20.198.118.190:443     ESTABLISHED
TCP    127.0.0.1:49670        127.0.0.1:49671        ESTABLISHED
TCP    127.0.0.1:49671        127.0.0.1:49670        ESTABLISHED
TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED
TCP    127.0.0.1:49673        127.0.0.1:49672        ESTABLISHED
TCP    127.0.0.1:50640        127.0.0.1:15615        SYN_SENT
TCP    172.29.192.1:139       0.0.0.0:0              LISTENING
TCP    [::]:135               [::]:0                 LISTENING
TCP    [::]:445               [::]:0                 LISTENING
TCP    [::]:3306              [::]:0                 LISTENING
TCP    [::]:7680              [::]:0                 LISTENING
TCP    [::]:33060             [::]:0                 LISTENING
TCP    [::]:49664             [::]:0                 LISTENING
TCP    [::]:49665             [::]:0                 LISTENING
TCP    [::]:49666             [::]:0                 LISTENING
TCP    [::]:49667             [::]:0                 LISTENING
TCP    [::]:49668             [::]:0                 LISTENING
TCP    [::]:49674             [::]:0                 LISTENING
TCP    [::1]:49669            [::]:0                 LISTENING
TCP    [::1]:50639            [::1]:15615            SYN_SENT
```

Figure 9:

Q2

1. When you browse the IIT Bhilai main page, how many GET requests are sent(How many of these GET requests are for embedded content, and how many are for the text)? Plot the IO graph for packets sent to iitbhilai.ac.in and packets received from iitbhilai.ac.in

2. For the response to your HTTP GET request, reconstruct the image using a hex editor.

3. Find the interpacket interval between multiple GET requests.

4. Find the throughput observed while browsing the IIT Bhilai site under two cases:

   (a) When no other traffic is in the background.

   (b) When a large file download is in progress.

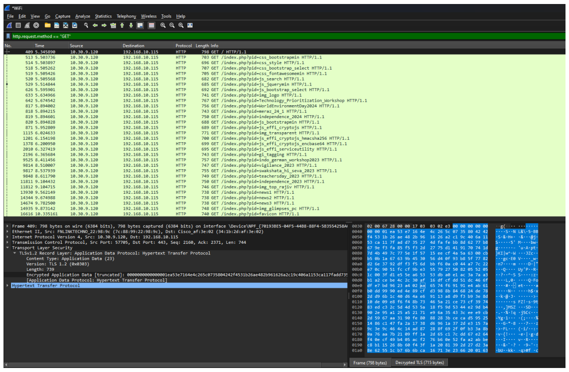
   The throughput calculation needs filtering only IIT Bhilai pages (from the GET request originated from your browser until the last response arrives at the end of the web page).

Answer:

1) In Windows cmd, I typed this command `set SSLKEYLOGFILE=C:\Users\halde\SSLKEYS\sslkeys.log` to create the environment variable file. Then in the TLS option of Wireshark's protocol under the preference tab, I gave the file path to (Pre)Master-Secret log file name. So it can decrypt and show HTTP packets.

Now I started wireshark for capturing and serf to IIT Bhilai's site and after some times stoped the capturing.

Now I added this filter **http.request.method == "GET"** in wireshark to see the GET requests. There are total 31 GET requests out of it total 23 are of embedded content and 8 are text content.



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

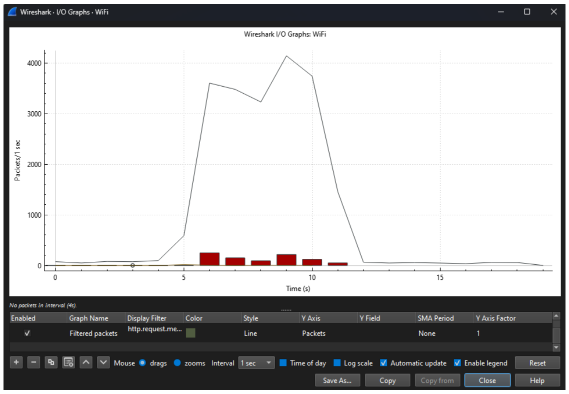
http.request.method == "GET"

```
No.    Time       Source        Destination     Protocol Length Info
  409 5.345890    10.30.9.120   192.168.10.115  HTTP     798 GET / HTTP/1.1
  513 5.503736    10.30.9.120   192.168.10.115  HTTP     703 GET /index.php?pid=css_bootstrapmin HTTP/1.1
  514 5.503897    10.30.9.120   192.168.10.115  HTTP     696 GET /index.php?pid=css_style HTTP/1.1
  518 5.505262    10.30.9.120   192.168.10.115  HTTP     707 GET /index.php?pid=css_bootstrap_select HTTP/1.1
  519 5.505426    10.30.9.120   192.168.10.115  HTTP     705 GET /index.php?pid=css_fontawesomemin HTTP/1.1
  520 5.505568    10.30.9.120   192.168.10.115  HTTP     682 GET /index.php?pid=js_search HTTP/1.1
  529 5.514844    10.30.9.120   192.168.10.115  HTTP     685 GET /index.php?pid=js_jquerymin HTTP/1.1
  626 5.595901    10.30.9.120   192.168.10.115  HTTP     692 GET /index.php?pid=js_bootstrap_select HTTP/1.1
  633 5.634966    10.30.9.120   192.168.10.115  HTTP     741 GET /index.php?pid=img_logo HTTP/1.1
  642 5.674542    10.30.9.120   192.168.10.115  HTTP     767 GET /index.php?pid=Technology_Prioritization_Workshop HTTP/1.1
  817 5.894002    10.30.9.120   192.168.10.115  HTTP     756 GET /index.php?pid=WorldEnvironmentDay2024 HTTP/1.1
  818 5.894215    10.30.9.120   192.168.10.115  HTTP     743 GET /index.php?pid=meraz_24_1 HTTP/1.1
  819 5.894601    10.30.9.120   192.168.10.115  HTTP     750 GET /index.php?pid=independence_2024 HTTP/1.1
  820 5.894828    10.30.9.120   192.168.10.115  HTTP     688 GET /index.php?pid=js_bootstrapmin HTTP/1.1
  871 5.952809    10.30.9.120   192.168.10.115  HTTP     689 GET /index.php?pid=js_effi_cryptojs HTTP/1.1
 1115 6.024633    10.30.9.120   192.168.10.115  HTTP     771 GET /index.php?pid=img_transparent HTTP/1.1
 1201 6.154198    10.30.9.120   192.168.10.115  HTTP     700 GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1
 1378 6.200950    10.30.9.120   192.168.10.115  HTTP     699 GET /index.php?pid=js_effi_cryptojs_encbase64 HTTP/1.1
 2010 6.327419    10.30.9.120   192.168.10.115  HTTP     695 GET /index.php?pid=js_effi_serviceutility HTTP/1.1
 2196 6.365684    10.30.9.120   192.168.10.115  HTTP     743 GET /index.php?pid=gi_tagging HTTP/1.1
 9525 8.411456    10.30.9.120   192.168.10.115  HTTP     757 GET /index.php?pid=indo_german_workshop2023 HTTP/1.1
 9814 8.510007    10.30.9.120   192.168.10.115  HTTP     747 GET /index.php?pid=vigilance_2023 HTTP/1.1
 9817 8.537939    10.30.9.120   192.168.10.115  HTTP     755 GET /index.php?pid=swakshata_hi_seva_2023 HTTP/1.1
 9848 8.611790    10.30.9.120   192.168.10.115  HTTP     749 GET /index.php?pid=teachersday_2023 HTTP/1.1
11811 9.104432    10.30.9.120   192.168.10.115  HTTP     750 GET /index.php?pid=independence_2023 HTTP/1.1
11812 9.104715    10.30.9.120   192.168.10.115  HTTP     746 GET /index.php?pid=img_top_rajiv HTTP/1.1
13930 9.562149    10.30.9.120   192.168.10.115  HTTP     738 GET /index.php?pid=news1 HTTP/1.1
14344 9.674988    10.30.9.120   192.168.10.115  HTTP     738 GET /index.php?pid=news2 HTTP/1.1
14674 9.782500    10.30.9.120   192.168.10.115  HTTP     738 GET /index.php?pid=news3 HTTP/1.1
14935 9.873142    10.30.9.120   192.168.10.115  HTTP     748 GET /index.php?pid=img_glimpses_pc HTTP/1.1
16616 10.335161   10.30.9.120   192.168.10.115  HTTP     740 GET /index.php?pid=favicon HTTP/1.1
```

```
> Frame 409: 798 bytes on wire (6384 bits), 798 bytes captured (6384 bits) on interface \Device\NPF_{70193BE5-04F5-4488-88F4-5B3554258A
> Ethernet II, Src: FNLINKTECHNO_22:98:9c (7c:88:99:22:98:9c), Dst: Cisco_af:3e:02 (34:1b:2d:af:3e:02)
> Internet Protocol Version 4, Src: 10.30.9.120, Dst: 192.168.10.115
> Transmission Control Protocol, Src Port: 57705, Dst Port: 443, Seq: 2160, Ack: 2371, Len: 744
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 739
      Encrypted Application Data [truncated]: 0000000000000001ea53e7164e4c265c0735804242f4531b26ae482b961626a2c19c406a1153ca117fadd735
      [Application Data Protocol: Hypertext Transfer Protocol]
> Hypertext Transfer Protocol
```

```
0030  02 00 67 28 00 00 17 03  03 02 e3 00 00 00 00 00
0040  00 00 01 ea 53 e7 16 4e  4c 26 5c 07 35 80 42 42
0050  f4 53 1b 26 ae 48 2b 96  16 26 a2 c1 9c 40 6a 11
0060  53 ca 11 7f ad d7 35 27  4d fa fe bb 8d 62 77 b8
0070  67 9e f3 fa 85 f5 f3 2d  27 75 d1 41 91 70 74 1d
0080  7d 4b 49 7c 77 5e 1f 57  15 ee cf 4a 5a 63 00 cb
0090  b5 0b 1a 67 63 9b 45 30  56 d4 0f 93 b8 5f 77 82
00a0  d2 6e 37 92 df f3 f5 6d  bb f6 0a c0 44 a7 7c 22
00b0  e7 0c 90 51 fc cf 9b e3  55 79 27 50 82 05 52 05
00c0  1c 00 3f d1 e5 5e a6 53  53 db a0 e1 ac 3a 7a a3
00d0  b1 a2 ce be 4c 2c 30 af  16 df cf dd 51 dc 46 6f
00e0  df e7 bd 96 23 a4 02 aa  65 74 f6 91 91 e4 ab 61
00f0  b0 dd 99 90 ed 4e 89 cf  d3 98 8b 84 68 24 de 78
0100  2d d9 6b 1c 40 d6 4a e6  91 13 a8 d9 f3 b9 3e 8d
0110  10 de 09 e8 f6 f4 8b 73  46 5a 21 ce 73 cf 39 74
0120  83 ed c3 2c 5d 4d 53 5a  18 f5 9d 53 44 e2 9d b4
0130  90 2e 95 a1 25 a5 21 71  e9 6a 35 43 3c ee e9 cb
0140  2d 59 67 aa 31 90 fe 80  88 28 3b ce ca d5 95 25
0150  14 86 c1 47 fa 2a 17 38  d6 96 1a 37 2d e3 15 7a
0160  9c 3e 9c 46 4c 14 ad 87  28 8f 69 2f 0f b3 3a 8b
0170  0a 76 aa 7b 21 09 ff 1a  2d 65 c1 7c dd 67 e2 64
0180  f4 0e cf 49 b4 05 ac f2  76 b6 0e 52 fa a2 ab be
0190  c8 b1 15 26 8b 60 f4 3f  1a 20 81 39 2d 27 d2 3a
01a0  8e 62 55 1c b7 6b 6b ca  16 71 3e 23 66 20 01 63
```

Figure 10: GET requests



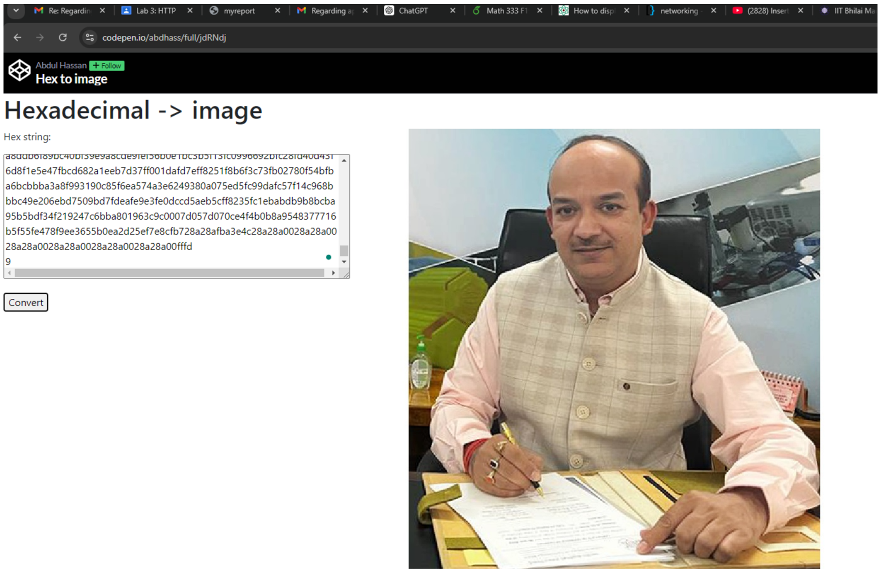
No packets in interval (4s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
✓	Filtered packets	http.request.me...	🟩	Line	Packets		None	1

Mouse ● drags ● zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

Figure 11: I/O graph

2)



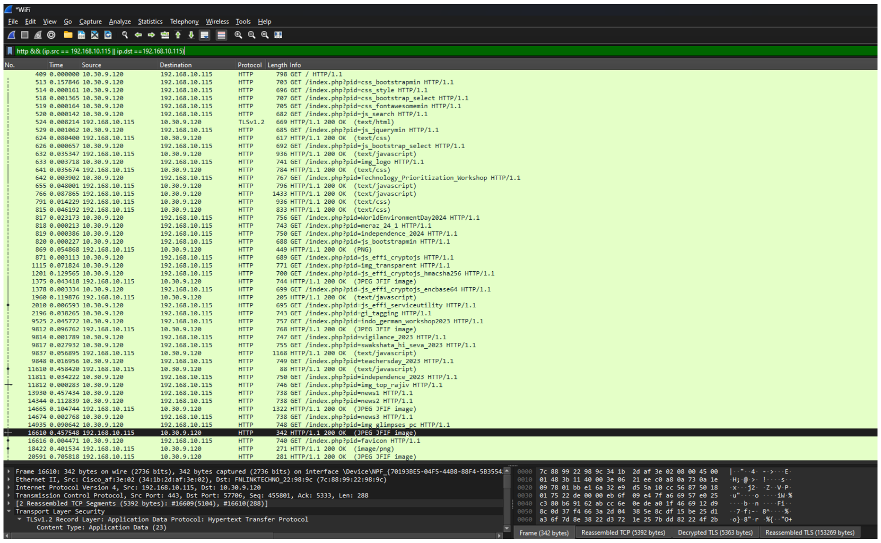
Hexadecimal -> image

Hex string:

```
a8ddb6f89bc40bf39e9a8cde9fef56b0e1bc3b5f13fc0996692bfc28fd40d43f
6d8f1e5e47fbcd682a1eeb7d37ff001dafd7eff8251f8b6f3c73fb02780f54bfb
a6bcbbba3a8f993190c85f6ea574a3e6249380a075ed5fc99dafc57f14c968b
bbc49e206ebd7509bd7fdeafe9e3fe0dccd5aeb5cff8235fc1ebabdb9b8bcba
95b5bdf34f219247c6bba801963c9c0007d057d070ce4f4b0b8a9548377716
b5f55fe478f9ee3655b0ea2d25ef7e8cfb728a28afba3e4c28a28a0028a28a00
28a28a0028a28a0028a28a0028a28a00fffd
9
```

Figure 12: Image reconstructed using hex editor.

3)


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && (ip.src == 192.168.10.115 || ip.dst ==192.168.10.115)

```
No.   Time     Source          Destination     Protocol Length Info
  409 0.000000 10.30.9.120     192.168.10.115  HTTP      798 GET / HTTP/1.1
  513 0.157846 10.30.9.120     192.168.10.115  HTTP      703 GET /index.php?pid=css_bootstrapmin HTTP/1.1
  514 0.000161 10.30.9.120     192.168.10.115  HTTP      696 GET /index.php?pid=css_style HTTP/1.1
  518 0.001365 10.30.9.120     192.168.10.115  HTTP      707 GET /index.php?pid=css_bootstrap_select HTTP/1.1
  519 0.000164 10.30.9.120     192.168.10.115  HTTP      705 GET /index.php?pid=css_fontawesomemin HTTP/1.1
  520 0.000142 10.30.9.120     192.168.10.115  HTTP      682 GET /index.php?pid=js_search HTTP/1.1
  524 0.008214 192.168.10.115  10.30.9.120     TLSv1.2   669 HTTP/1.1 200 OK  (text/html)
  529 0.001062 10.30.9.120     192.168.10.115  HTTP      685 GET /index.php?pid=js_jquerymin HTTP/1.1
  624 0.080400 192.168.10.115  10.30.9.120     HTTP      617 HTTP/1.1 200 OK  (text/css)
  626 0.000657 10.30.9.120     192.168.10.115  HTTP      692 GET /index.php?pid=js_bootstrap_select HTTP/1.1
  632 0.035347 192.168.10.115  10.30.9.120     HTTP      936 HTTP/1.1 200 OK  (text/javascript)
  633 0.003718 10.30.9.120     192.168.10.115  HTTP      741 GET /index.php?pid=img_logo HTTP/1.1
  641 0.035674 192.168.10.115  10.30.9.120     HTTP      784 HTTP/1.1 200 OK  (text/css)
  642 0.003902 10.30.9.120     192.168.10.115  HTTP      767 GET /index.php?pid=Technology_Prioritization_Workshop HTTP/1.1
  655 0.048001 192.168.10.115  10.30.9.120     HTTP      796 HTTP/1.1 200 OK  (text/javascript)
  766 0.087865 192.168.10.115  10.30.9.120     HTTP     1433 HTTP/1.1 200 OK  (text/javascript)
  791 0.014229 192.168.10.115  10.30.9.120     HTTP      936 HTTP/1.1 200 OK  (text/css)
  815 0.046192 192.168.10.115  10.30.9.120     HTTP      833 HTTP/1.1 200 OK  (text/css)
  817 0.023173 10.30.9.120     192.168.10.115  HTTP      756 GET /index.php?pid=WorldEnvironmentDay2024 HTTP/1.1
  818 0.000213 10.30.9.120     192.168.10.115  HTTP      743 GET /index.php?pid=meraz_24_1 HTTP/1.1
  819 0.000386 10.30.9.120     192.168.10.115  HTTP      750 GET /index.php?pid=independence_2024 HTTP/1.1
  820 0.000227 10.30.9.120     192.168.10.115  HTTP      688 GET /index.php?pid=js_bootstrapmin HTTP/1.1
  869 0.054868 192.168.10.115  10.30.9.120     HTTP      449 HTTP/1.1 200 OK  (PNG)
  871 0.003113 10.30.9.120     192.168.10.115  HTTP      689 GET /index.php?pid=js_effi_cryptojs HTTP/1.1
 1115 0.071824 10.30.9.120     192.168.10.115  HTTP      771 GET /index.php?pid=img_transparent HTTP/1.1
 1201 0.129565 10.30.9.120     192.168.10.115  HTTP      700 GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1
 1375 0.043418 192.168.10.115  10.30.9.120     HTTP      744 HTTP/1.1 200 OK  (JPEG JFIF image)
 1378 0.003334 10.30.9.120     192.168.10.115  HTTP      699 GET /index.php?pid=js_effi_cryptojs_encbase64 HTTP/1.1
 1960 0.119876 192.168.10.115  10.30.9.120     HTTP      205 HTTP/1.1 200 OK  (text/javascript)
 2010 0.006593 10.30.9.120     192.168.10.115  HTTP      695 GET /index.php?pid=js_effi_serviceutility HTTP/1.1
 2196 0.038265 10.30.9.120     192.168.10.115  HTTP      743 GET /index.php?pid=gi_tagging HTTP/1.1
 9525 2.045772 10.30.9.120     192.168.10.115  HTTP      757 GET /index.php?pid=indo_german_workshop2023 HTTP/1.1
 9812 0.096762 192.168.10.115  10.30.9.120     HTTP      768 HTTP/1.1 200 OK  (JPEG JFIF image)
 9814 0.001789 10.30.9.120     192.168.10.115  HTTP      747 GET /index.php?pid=vigilance_2023 HTTP/1.1
 9817 0.027932 10.30.9.120     192.168.10.115  HTTP      755 GET /index.php?pid=swakshata_hi_seva_2023 HTTP/1.1
 9837 0.056895 192.168.10.115  10.30.9.120     HTTP     1168 HTTP/1.1 200 OK  (text/javascript)
 9848 0.016956 10.30.9.120     192.168.10.115  HTTP      749 GET /index.php?pid=teachersday_2023 HTTP/1.1
11610 0.458420 192.168.10.115  10.30.9.120     HTTP       88 HTTP/1.1 200 OK  (text/javascript)
11811 0.034222 10.30.9.120     192.168.10.115  HTTP      750 GET /index.php?pid=independence_2023 HTTP/1.1
11812 0.000283 10.30.9.120     192.168.10.115  HTTP      746 GET /index.php?pid=img_top_rajiv HTTP/1.1
13930 0.457434 10.30.9.120     192.168.10.115  HTTP      738 GET /index.php?pid=news1 HTTP/1.1
14344 0.112839 10.30.9.120     192.168.10.115  HTTP      738 GET /index.php?pid=news2 HTTP/1.1
14665 0.104744 192.168.10.115  10.30.9.120     HTTP     1322 HTTP/1.1 200 OK  (JPEG JFIF image)
14674 0.002768 10.30.9.120     192.168.10.115  HTTP      738 GET /index.php?pid=news3 HTTP/1.1
14935 0.090642 10.30.9.120     192.168.10.115  HTTP      748 GET /index.php?pid=img_glimpses_pc HTTP/1.1
16610 0.457548 192.168.10.115  10.30.9.120     HTTP      342 HTTP/1.1 200 OK  (JPEG JFIF image)
16616 0.004471 10.30.9.120     192.168.10.115  HTTP      740 GET /index.php?pid=favicon HTTP/1.1
18422 0.401534 192.168.10.115  10.30.9.120     HTTP      271 HTTP/1.1 200 OK  (image/png)
20591 0.705818 192.168.10.115  10.30.9.120     HTTP      281 HTTP/1.1 200 OK  (JPEG JFIF image)
```

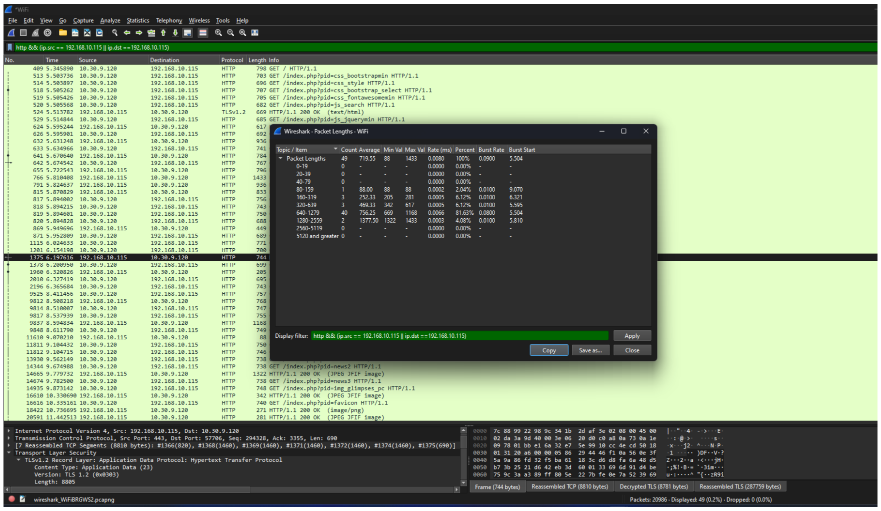
```
> Frame 16610: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{70193BE5-04F5-44B8-88F4-5B3554
> Ethernet II, Src: Cisco_af:3e:02 (34:1b:2d:af:3e:02), Dst: FNLINKTECHNO_22:98:9c (7c:88:99:22:98:9c)
> Internet Protocol Version 4, Src: 192.168.10.115, Dst: 10.30.9.120
> Transmission Control Protocol, Src Port: 443, Dst Port: 57706, Seq: 455801, Ack: 5333, Len: 288
> [2 Reassembled TCP Segments (5392 bytes): #16609(5104), #16610(288)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
```

```
0000  7c 88 99 22 98 9c 34 1b  2d af 3e 02 08 00 45 00
0010  01 48 3b 11 40 00 3e 06  21 ee c0 a8 0a 73 0a 1e
0020  09 78 01 bb e1 6a 32 e9  d5 5a 10 cc 56 87 50 18
0030  01 75 22 de 00 00 eb 6f  09 e4 7f a6 69 57 e0 25
0040  c3 80 b6 91 62 ab cc 6e  0e de a0 1f 46 69 12 d9
0050  8c 0d 37 f4 66 3a 2d 04  38 5e 8c df 15 be 25 d1
0060  a3 6f 7d 8e 38 22 d3 72  1e 25 7b dd 82 22 4f 2b
```

Frame (342 bytes) | Reassembled TCP (5392 bytes) | Decrypted TLS (5363 bytes) | Reassembled TLS (153269 bytes)

Figure 13: Interpacket interval between multiple GET requests.

4)
a)


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && (ip.src == 192.168.10.115 || ip.dst ==192.168.10.115)

```
No.   Time      Source          Destination     Protocol Length Info
  409 5.345890  10.30.9.120     192.168.10.115  HTTP      798 GET / HTTP/1.1
  513 5.503736  10.30.9.120     192.168.10.115  HTTP      703 GET /index.php?pid=css_bootstrapmin HTTP/1.1
  514 5.503897  10.30.9.120     192.168.10.115  HTTP      696 GET /index.php?pid=css_style HTTP/1.1
  518 5.505262  10.30.9.120     192.168.10.115  HTTP      707 GET /index.php?pid=css_bootstrap_select HTTP/1.1
  519 5.505426  10.30.9.120     192.168.10.115  HTTP      705 GET /index.php?pid=css_fontawesomemin HTTP/1.1
  520 5.505568  10.30.9.120     192.168.10.115  HTTP      682 GET /index.php?pid=js_search HTTP/1.1
  524 5.513782  192.168.10.115  10.30.9.120     TLSv1.2   669 HTTP/1.1 200 OK  (text/html)
  529 5.514844  10.30.9.120     192.168.10.115  HTTP      685 GET /index.php?pid=js_jquerymin HTTP/1.1
  624 5.595244  192.168.10.115  10.30.9.120     HTTP      617
  626 5.595901  10.30.9.120     192.168.10.115  HTTP      692
  632 5.631248  192.168.10.115  10.30.9.120     HTTP      936
  633 5.634966  10.30.9.120     192.168.10.115  HTTP      741
  641 5.670640  192.168.10.115  10.30.9.120     HTTP      784
  642 5.674542  10.30.9.120     192.168.10.115  HTTP      767
  655 5.722543  192.168.10.115  10.30.9.120     HTTP      796
  766 5.810408  192.168.10.115  10.30.9.120     HTTP     1433
  791 5.824637  192.168.10.115  10.30.9.120     HTTP      936
  815 5.870829  192.168.10.115  10.30.9.120     HTTP      833
  817 5.894002  10.30.9.120     192.168.10.115  HTTP      756
  818 5.894215  10.30.9.120     192.168.10.115  HTTP      743
  819 5.894601  10.30.9.120     192.168.10.115  HTTP      750
  820 5.894828  10.30.9.120     192.168.10.115  HTTP      688
  869 5.949696  192.168.10.115  10.30.9.120     HTTP      449
  871 5.952809  10.30.9.120     192.168.10.115  HTTP      689
 1115 6.024633  10.30.9.120     192.168.10.115  HTTP      771
 1201 6.154198  10.30.9.120     192.168.10.115  HTTP      700
 1375 6.197616  192.168.10.115  10.30.9.120     HTTP      744
 1378 6.200950  10.30.9.120     192.168.10.115  HTTP      699
 1960 6.320826  192.168.10.115  10.30.9.120     HTTP      205
 2010 6.327419  10.30.9.120     192.168.10.115  HTTP      695
 2196 6.365684  10.30.9.120     192.168.10.115  HTTP      743
 9525 8.411456  10.30.9.120     192.168.10.115  HTTP      757
 9812 8.508218  192.168.10.115  10.30.9.120     HTTP      768
 9814 8.510007  10.30.9.120     192.168.10.115  HTTP      747
 9817 8.537939  10.30.9.120     192.168.10.115  HTTP      755
 9837 8.594834  192.168.10.115  10.30.9.120     HTTP     1168
 9848 8.611790  10.30.9.120     192.168.10.115  HTTP      749
11610 9.070210  192.168.10.115  10.30.9.120     HTTP       88
11811 9.104432  10.30.9.120     192.168.10.115  HTTP      750
11812 9.104715  10.30.9.120     192.168.10.115  HTTP      746
13930 9.562149  10.30.9.120     192.168.10.115  HTTP      738
14344 9.674988  10.30.9.120     192.168.10.115  HTTP      738 GET /index.php?pid=news2 HTTP/1.1
14665 9.779732  192.168.10.115  10.30.9.120     HTTP     1322 HTTP/1.1 200 OK  (JPEG JFIF image)
14674 9.782500  10.30.9.120     192.168.10.115  HTTP      738 GET /index.php?pid=news3 HTTP/1.1
14935 9.873142  10.30.9.120     192.168.10.115  HTTP      748 GET /index.php?pid=img_glimpses_pc HTTP/1.1
16610 10.330690 192.168.10.115  10.30.9.120     HTTP      342 HTTP/1.1 200 OK  (JPEG JFIF image)
16616 10.335161 10.30.9.120     192.168.10.115  HTTP      740 GET /index.php?pid=favicon HTTP/1.1
18422 10.736695 192.168.10.115  10.30.9.120     HTTP      271 HTTP/1.1 200 OK  (image/png)
20591 11.442513 192.168.10.115  10.30.9.120     HTTP      281 HTTP/1.1 200 OK  (JPEG JFIF image)
```

Wireshark · Packet Lengths · WiFi

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	49	719.55	88	1433	0.0080	100%	0.0900	5.504
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	0	-	-	-	0.0000	0.00%	-	-
80-159	1	88.00	88	88	0.0002	2.04%	0.0100	9.070
160-319	3	252.33	205	281	0.0005	6.12%	0.0100	6.321
320-639	3	469.33	342	617	0.0005	6.12%	0.0100	5.595
640-1279	40	756.25	669	1168	0.0066	81.63%	0.0800	5.504
1280-2559	2	1377.50	1322	1433	0.0003	4.08%	0.0100	5.810
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: http && (ip.src == 192.168.10.115 || ip.dst ==192.168.10.115)

```
> Internet Protocol Version 4, Src: 192.168.10.115, Dst: 10.30.9.120
> Transmission Control Protocol, Src Port: 443, Dst Port: 57706, Seq: 294328, Ack: 3355, Len: 690
> [7 Reassembled TCP Segments (8810 bytes): #1366(820), #1368(1460), #1369(1460), #1371(1460), #1372(1460), #1374(1460), #1375(690)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 8805
```

```
0000  7c 88 99 22 98 9c 34 1b  2d af 3e 02 08 00 45 00
0010  02 da 3a 9d 40 00 3e 06  20 d0 c0 a8 0a 73 0a 1e
0020  09 78 01 bb e1 6a 32 e7  5e 99 10 cc 4e cd 50 18
0030  01 31 20 a6 00 00 05 86  29 44 46 f1 0a 56 0e 3f
0040  5a 9a 86 fd 32 f5 ba 61  18 3c d6 d8 fa 6a 48 d5
0050  b7 3b 25 21 d6 42 eb 3d  60 01 33 69 6d 91 d4 be
0060  75 9c 3a a3 89 ff 80 5e  22 7b fe 0e 7a 52 39 69
```

Frame (744 bytes) | Reassembled TCP (8810 bytes) | Decrypted TLS (8781 bytes) | Reassembled TLS (287759 bytes)

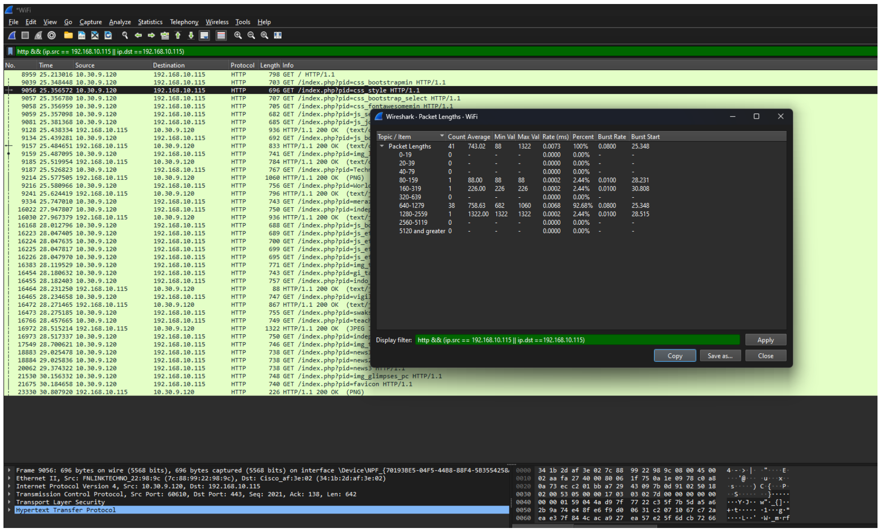
wireshark_WiFiBRGWS2.pcapng

Packets: 20986 · Displayed: 49 (0.2%) · Dropped: 0 (0.0%)

Figure 14: When no traffic is in the background

Now for throughput(without any traffic in the background) we have to find the total size of the packets,
which is = 719.55 * 49 = 35257.95 bytes.
Throughput = 35257.95/(11.442-5.346) = 35257.95/6.096 = 5783.784 bytes/sec.

b)


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && (ip.src == 192.168.10.115 || ip.dst ==192.168.10.115)

```
No.   Time      Source         Destination    Protocol Length Info
 8959 25.213016 10.30.9.120    192.168.10.115 HTTP      798 GET / HTTP/1.1
 9039 25.348448 10.30.9.120    192.168.10.115 HTTP      703 GET /index.php?pid=css_bootstrapmin HTTP/1.1
 9056 25.356572 10.30.9.120    192.168.10.115 HTTP      696 GET /index.php?pid=css_style HTTP/1.1
 9057 25.356780 10.30.9.120    192.168.10.115 HTTP      707 GET /index.php?pid=css_bootstrap_select HTTP/1.1
 9058 25.356959 10.30.9.120    192.168.10.115 HTTP      705 GET /index.php?pid=css_fontawesomemin HTTP/1.1
 9059 25.357098 10.30.9.120    192.168.10.115 HTTP      682 GET /index.php?pid=js_se
 9081 25.381368 10.30.9.120    192.168.10.115 HTTP      685 GET /index.php?pid=js_jq
 9128 25.438334 192.168.10.115 10.30.9.120    HTTP      936 HTTP/1.1 200 OK  (text/c
 9134 25.439281 10.30.9.120    192.168.10.115 HTTP      692 GET /index.php?pid=js_bo
 9157 25.484651 192.168.10.115 10.30.9.120    HTTP      833 HTTP/1.1 200 OK  (text/c
 9159 25.487095 10.30.9.120    192.168.10.115 HTTP      741 GET /index.php?pid=img_l
 9185 25.519954 192.168.10.115 10.30.9.120    HTTP      784 HTTP/1.1 200 OK  (text/c
 9187 25.526823 10.30.9.120    192.168.10.115 HTTP      767 GET /index.php?pid=Techn
 9214 25.577505 192.168.10.115 10.30.9.120    HTTP     1060 HTTP/1.1 200 OK  (PNG)
 9216 25.580966 10.30.9.120    192.168.10.115 HTTP      756 GET /index.php?pid=World
 9241 25.624419 192.168.10.115 10.30.9.120    HTTP      796 HTTP/1.1 200 OK  (text/j
 9334 25.747010 10.30.9.120    192.168.10.115 HTTP      743 GET /index.php?pid=meraz
16022 27.947807 10.30.9.120    192.168.10.115 HTTP      750 GET /index.php?pid=indep
16030 27.967379 192.168.10.115 10.30.9.120    HTTP      936 HTTP/1.1 200 OK  (text/j
16168 28.012796 10.30.9.120    192.168.10.115 HTTP      688 GET /index.php?pid=js_bo
16223 28.047405 10.30.9.120    192.168.10.115 HTTP      689 GET /index.php?pid=js_ef
16224 28.047635 10.30.9.120    192.168.10.115 HTTP      700 GET /index.php?pid=js_ef
16225 28.047817 10.30.9.120    192.168.10.115 HTTP      699 GET /index.php?pid=js_ef
16226 28.047970 10.30.9.120    192.168.10.115 HTTP      695 GET /index.php?pid=js_ef
16383 28.119529 10.30.9.120    192.168.10.115 HTTP      771 GET /index.php?pid=img_t
16454 28.180632 10.30.9.120    192.168.10.115 HTTP      743 GET /index.php?pid=gi_ta
16455 28.182403 10.30.9.120    192.168.10.115 HTTP      757 GET /index.php?pid=indo_
16464 28.231250 192.168.10.115 10.30.9.120    HTTP       88 HTTP/1.1 200 OK  (text/j
16465 28.234658 10.30.9.120    192.168.10.115 HTTP      747 GET /index.php?pid=vigil
16472 28.271465 192.168.10.115 10.30.9.120    HTTP      867 HTTP/1.1 200 OK  (text/j
16473 28.275185 10.30.9.120    192.168.10.115 HTTP      755 GET /index.php?pid=swaks
16766 28.457665 10.30.9.120    192.168.10.115 HTTP      749 GET /index.php?pid=teach
16972 28.515214 192.168.10.115 10.30.9.120    HTTP     1322 HTTP/1.1 200 OK  (JPEG J
16973 28.517337 10.30.9.120    192.168.10.115 HTTP      750 GET /index.php?pid=indep
17549 28.700621 10.30.9.120    192.168.10.115 HTTP      746 GET /index.php?pid=img_t
18883 29.025478 10.30.9.120    192.168.10.115 HTTP      738 GET /index.php?pid=news1
18884 29.025836 10.30.9.120    192.168.10.115 HTTP      738 GET /index.php?pid=news2
20062 29.374322 10.30.9.120    192.168.10.115 HTTP      738 GET /index.php?pid=news3 HTTP/1.1
21530 30.156332 10.30.9.120    192.168.10.115 HTTP      748 GET /index.php?pid=img_glimpses_pc HTTP/1.1
21675 30.184658 10.30.9.120    192.168.10.115 HTTP      740 GET /index.php?pid=favicon HTTP/1.1
23330 30.807920 192.168.10.115 10.30.9.120    HTTP      226 HTTP/1.1 200 OK  (PNG)
```

Wireshark · Packet Lengths · WiFi

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	41	743.02	88	1322	0.0073	100%	0.0800	25.348
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	0	-	-	-	0.0000	0.00%	-	-
80-159	1	88.00	88	88	0.0002	2.44%	0.0100	28.231
160-319	1	226.00	226	226	0.0002	2.44%	0.0100	30.808
320-639	0	-	-	-	0.0000	0.00%	-	-
640-1279	38	758.63	682	1060	0.0068	92.68%	0.0800	25.348
1280-2559	1	1322.00	1322	1322	0.0002	2.44%	0.0100	28.515
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: http && (ip.src == 192.168.10.115 || ip.dst ==192.168.10.115)

```
Frame 9056: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits) on interface \Device\NPF_{70193BE5-04F5-44B8-88F4-5B3554258
Ethernet II, Src: FNLINKTECHNO_22:98:9c (7c:88:99:22:98:9c), Dst: Cisco_af:3e:02 (34:1b:2d:af:3e:02)
Internet Protocol Version 4, Src: 10.30.9.120, Dst: 192.168.10.115
Transmission Control Protocol, Src Port: 60610, Dst Port: 443, Seq: 2021, Ack: 138, Len: 642
Transport Layer Security
Hypertext Transfer Protocol
```

```
0000  34 1b 2d af 3e 02 7c 88  99 22 98 9c 08 00 45 00
0010  02 aa fa 27 40 00 80 06  1f 75 0a 1e 09 78 c0 a8
0020  0a 73 ec c2 01 bb a7 29  43 09 7b 0d 91 02 50 18
0030  02 00 53 05 00 00 17 03  03 02 7d 00 00 00 00 00
0040  00 00 01 59 04 4a d9 7f  77 22 c3 5f 7b 5d a5 a6
0050  2b 9a 74 e4 8f e6 f9 d0  06 31 c2 07 10 67 c7 2a
0060  ea e3 7f 84 4c ac a9 27  ea 57 e2 5f 6d cb 72 66
```

Figure 15: When there is traffic in the background

Now for throughput(with traffic in the background) we have to find the total size of the packets,
which is = 743.02 * 41 = 30463.82 bytes.
Throughput = 30463.82/(30.808-25.213) = 30463.82/5.595 = 5444.829 bytes/sec.