Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Networking 2

Lab : 5

Chapter : 8

**Exercise : 8. 01**

**Step 1 :**
TCP is very popular and reliable protocol uses handshake and acknowledgements to ensure the reliablity of the communcation and ensures the packets delivery from Point A to Point B.

* TCP lies at the level 4 of OSI model which is transporation layer. And it is responsible for the end to end communcation of the devices with enhanced reliablilty.

* TCP handles the flow of the data very well and sends packets to reciever based on the receivers acknowledgement, so no worry about the data overflow or Underflow.

Application protocols like HTTP, SSH, FTP, Telnet and SMTP etc. These protocols completely depend the TCP protocol.

These are the features of the TCP and it is properly established protocol for reliable communcation.

**Step 2 :**
UDP which is User Datagram Protocol is another main protocol in Internet Protocol and it sends data without any proper establishment like TCP.

* This protocol is connection less protocol, It never uses any preshared connection or anything, and treats easch datagrams as independent packets.

* This protocol has does not guarantee the delivery of the packets and packets flow independently, so it depends on the application it recieves, but UDP used in application where missing of individual packets don't affect the quality of message delivery, like streaming services, DNS, DHCP etc.

* It has less overhead and latency as there is no complex procedure to establish the connection and packets will not wait for any response therefore less latency.

* The main thing is UDP supports broadcast and multicast, can send the message to others invidually at the same time.

**Step 3 :**
ICMP is a kind of error reporting and managing protocol for delivery and status of the packets. ICMP messages are so crucial on networking particularly while sniffing.

* ICMP comes under layer 3 which routing and packet forwarding.

* Two types of messages that ICMP offers are : error messages and Query messages.
Error messages like :
1. Destination unreachable
2. Source quench
3. Time exceeded
4. Parameter problem
5. Redirection

Query Messages :
1. Echo (request/reply)
2. Timestamp(req,reply)
3. Address mask
4. Router advertisement.

These are the two types of message ICMP offers.

* ICMP offers troubleshooting options to keep the system updated about the information of the system.

**Step 4 :**
IGMP is a Internet Group Management Protocol is like managing the group protocol I would say, helps

to handle the multicast group memberships for example netflix subscribtion, Streaming on Television and subscription based Content etc are handled by IGMP and it is Layer 3 protocol also IGMP is broadly used.

**Exercise : 8. 02 :**

So My understanding is port is primary source for differentiating FTP or web server as like apartment number in the buildings.

**Step 1 :**

I think logical ports are necessary for the applications and servers to interact better because in networking delivering and receiving is the main part, so to send and receive we need proper entity. Ports are very important I think they determine, which purpose the communication is happening, for example, file transfer to the same device web request to the same device, authentication to the same device, and everything happens simultaneously, so to differentiate the services the ports are very important.
While in use ports will be open and after the session ports will be closed, also we can control the logical ports on the machine only, not on the server.

**Step 2 :**

| **Ports** | **Services** |
|---|---|
| **21** | **File transfer protocol** |
| **22** | **Secure shell protocol** |
| **25** | **SMTP** |
| **53** | **DNS** |
| **67/68** | **DHCP / DHCP Client** |
| **80** | **HTTP** |
| **88** | **Kerberos (Secure authentication for users)** |
| **143** | **IMAP** |
| **389** | **LDAP (Lightweight Directory access protocol)** |
| **443** | **HTTPS** |
| **3389** | **RDP (Remote Desktop Protocol)** |

**Step 3 :**
Netstat a : It is used display the network and port details and -a, means all the active ports can displayed when we run this command.
Netstat -b : Shows the executable program responsible for creating each connection.
Netstat - n : Show numerical address instead of showing the host names.
Netstat -o : It shows the process ID extra with each connection.

**Step 4 :**
Its an intersting question, By using netstat we will be displaying all the network details and statistics, but to find the origin of the malware or to root it, we need to run “netstat -b” which is used to showcase the executable program as malware is an executable program. So we can use this command to analyse the network.

**Step 5 :**

```
dinokp@Dinokps-MBP ~ % netstat
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  dinokps-mbp.lan.52366  ec2-34-230-249-1.https ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.52360 fe80::aede:48ff:.49188 ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.52357  ecs-121-36-83-10.http  CLOSE_WAIT
tcp6       0      0  2603-7081-13f0-8.52356 2606:4700::6811:.http  CLOSE_WAIT
tcp6       0      0  2603-7081-13f0-8.52354 2606:4700::6811:.http  CLOSE_WAIT
tcp6       0      0  2603-7081-13f0-8.52337 bh-in-f109.1e100.imaps ESTABLISHED
tcp6       0      0  2603-7081-13f0-8.52336 bh-in-f109.1e100.imaps ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.52191 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.52188 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.52186 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.52176 fe80::aede:48ff:.49188 ESTABLISHED
tcp4      31      0  dinokps-mbp.lan.52173  s3-r-w.ap-south-.https CLOSE_WAIT
tcp6       0      0  fe80::aede:48ff:.52095 fe80::aede:48ff:.49190 ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.52072  91.108.56.148.https    ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.52071 fe80::aede:48ff:.49186 ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.52049  wv-in-f109.1e100.imaps CLOSE_WAIT
tcp4       0      0  dinokps-mbp.lan.52021  149.154.167.41.https   ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.51909  110.43.67.241.http     CLOSE_WAIT
tcp6       0      0  fe80::aede:48ff:.51868 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.51829 fe80::aede:48ff:.49202 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.51279 fe80::aede:48ff:.49200 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.51220 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.51055 fe80::aede:48ff:.49190 ESTABLISHED
tcp4       0      0  localhost.50990        localhost.51024        ESTABLISHED
tcp4       0      0  localhost.51024        localhost.50990        ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.50975 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.50952 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  2603-7081-13f0-8.50951 bi-in-f109.1e100.imaps ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49955 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49954 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49950 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49949 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49947 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49945 fe80::aede:48ff:.49195 ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.49890  52.109.13.95.https     ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.49885  52.109.12.76.https     ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49827 fe80::aede:48ff:.49190 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49683 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49659 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49658 fe80::aede:48ff:.49188 ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49657 fe80::aede:48ff:.49188 ESTABLISHED
tcp4       0      0  dinokps-mbp.lan.49654  52.109.13.18.https     ESTABLISHED
tcp6       0      0  fe80::aede:48ff:.49645 fe80::aede:48ff:.49188 ESTABLISHED
```

**Step 6 :**

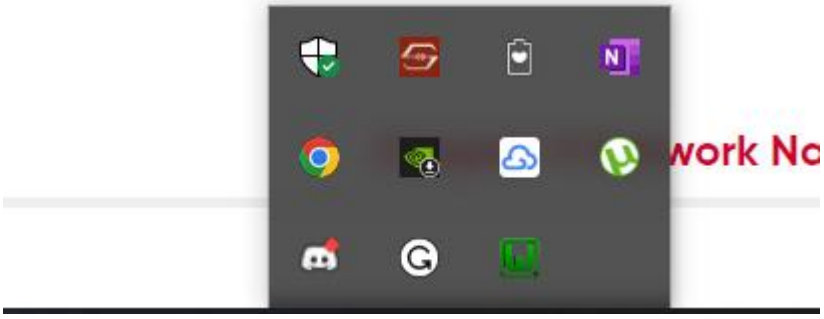
```
[chrome.exe]
 TCP    192.168.1.34:54462     192.156.234.2:443      ESTABLISHED     15840
[chrome.exe]
```

Connection established at port 443 which is HTTPS

**Step 7 :**

```
C:\WINDOWS\system32>netstat 15 -bano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1288
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4936
 [vmware-authd.exe]
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4936
 [vmware-authd.exe]
```

**Exercise : 8. 03 :**
**Step 1 :**



**Step 2 :**

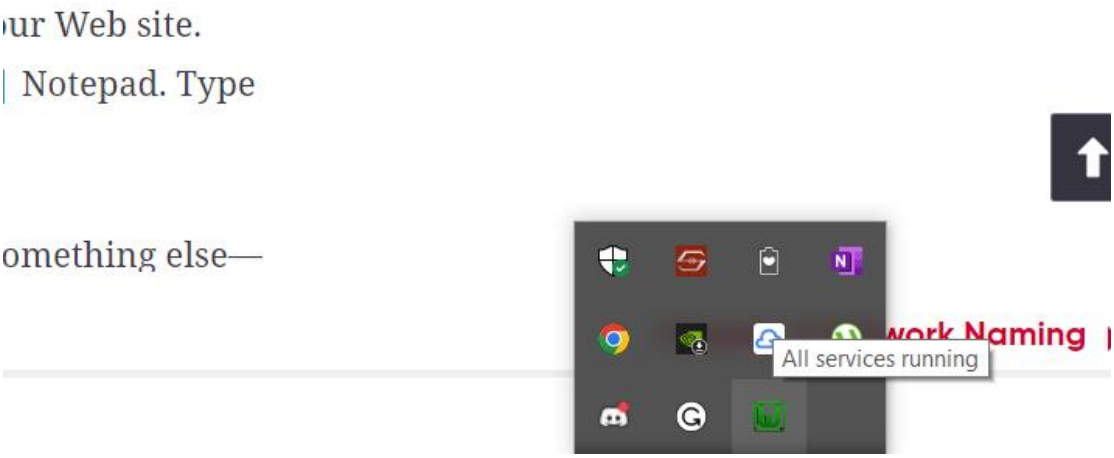
```
C:\Users\dinot>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
```

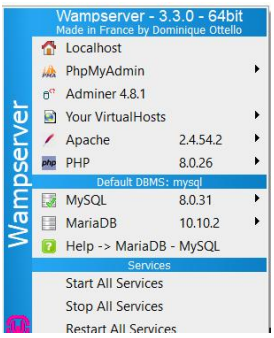
It means the tcp server is running on port 80 which is http server is running in backround.

**Step 3 :**
127.0.0.1 is a loopback address used in local machine only for testing the services and applications without sending data to other network or out of the system.
Whereas 0.0.0.0 means this service is bound to all the IPs in the system and can be used with all the application inside the system.

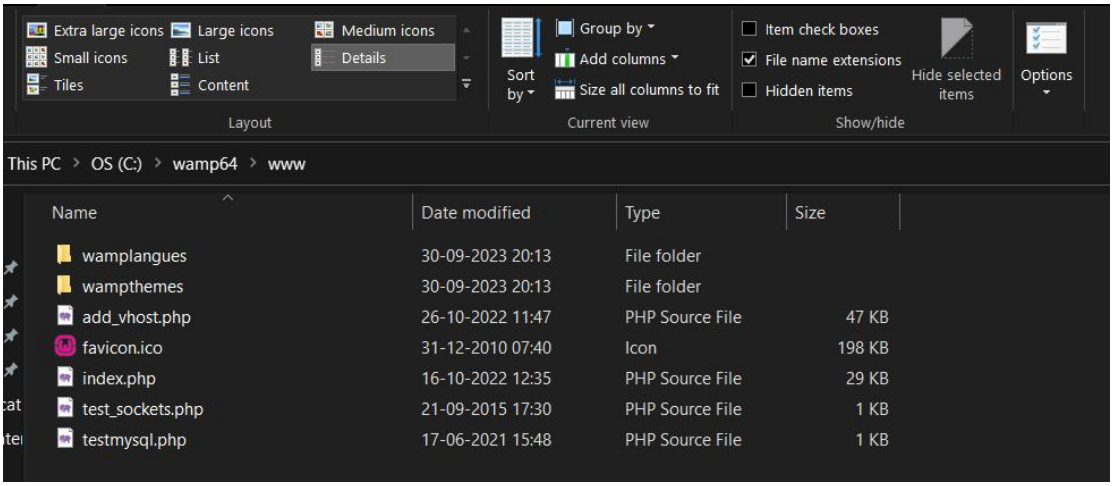
**Step 4 :**
It simply means UDP sockets are in listening mode, as they are connectionless "*" means UDP sockets are active to listen to the packets or catch the packets thrown at it.

**Step 5 :**
A.




Wampserver - 3.3.0 - 64bit
Made in France by Dominique Ottello
Localhost
PhpMyAdmin
Adminer 4.8.1
Your VirtualHosts
Apache 2.4.54.2
PHP 8.0.26
Default DBMS: mysql
MySQL 8.0.31
MariaDB 10.10.2
Help -> MariaDB - MySQL
Services
Start All Services
Stop All Services
Restart All Services
Wampserver

B.

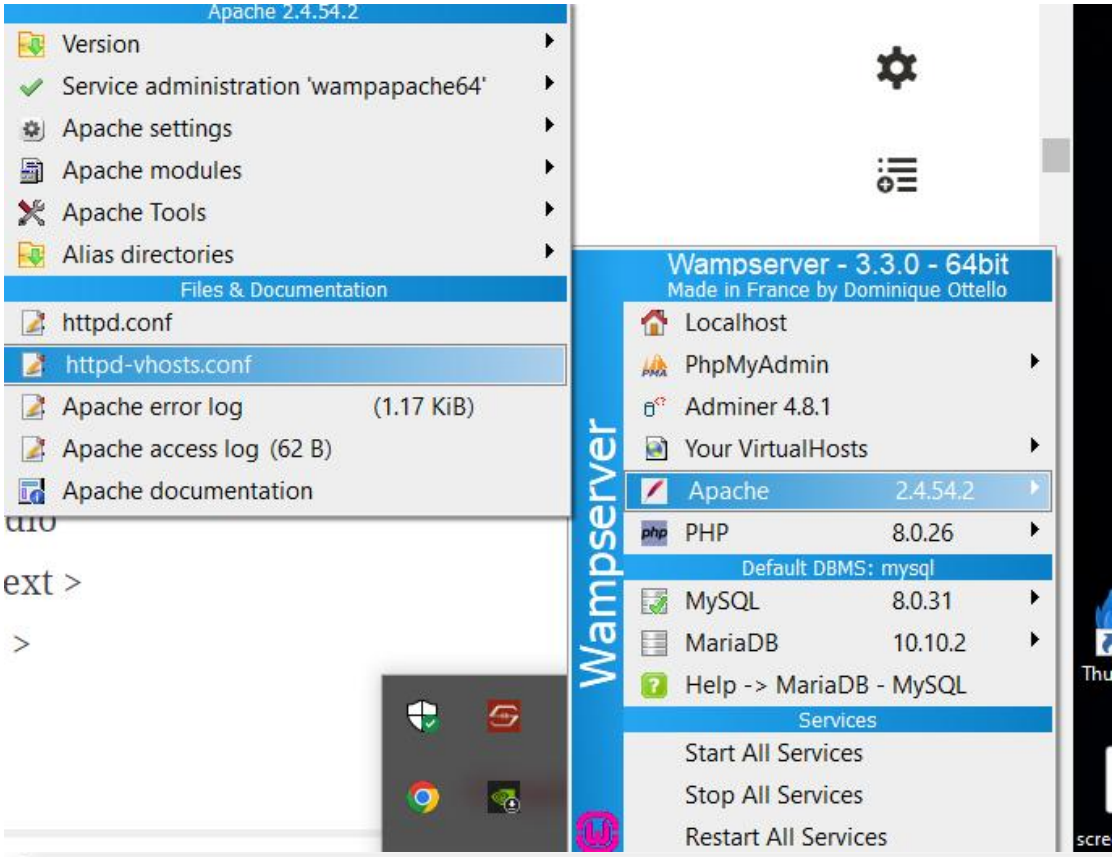

Extra large icons
Large icons
Medium icons
Small icons
List
Details
Tiles
Content
Layout
Sort by
Group by
Add columns
Size all columns to fit
Current view
Item check boxes
File name extensions
Hidden items
Hide selected items
Options
Show/hide
This PC › OS (C:) › wamp64 › www
Name
Date modified
Type
Size
wamplangues 30-09-2023 20:13 File folder
wampthemes 30-09-2023 20:13 File folder
add_vhost.php 26-10-2022 11:47 PHP Source File 47 KB
favicon.ico 31-12-2010 07:40 Icon 198 KB
index.php 16-10-2022 12:35 PHP Source File 29 KB
test_sockets.php 21-09-2015 17:30 PHP Source File 1 KB
testmysql.php 17-06-2021 15:48 PHP Source File 1 KB

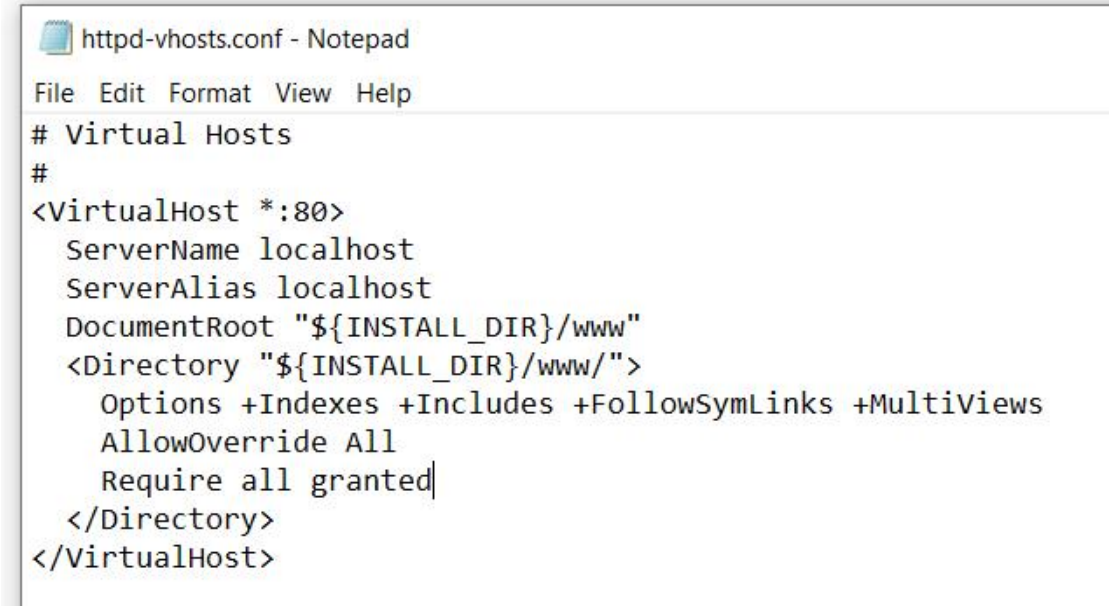
C.


*index.html - Notepad
File Edit Format View Help
Hello World
noindex.php 16-10-2022 12:35 PHP Source File 29 KB

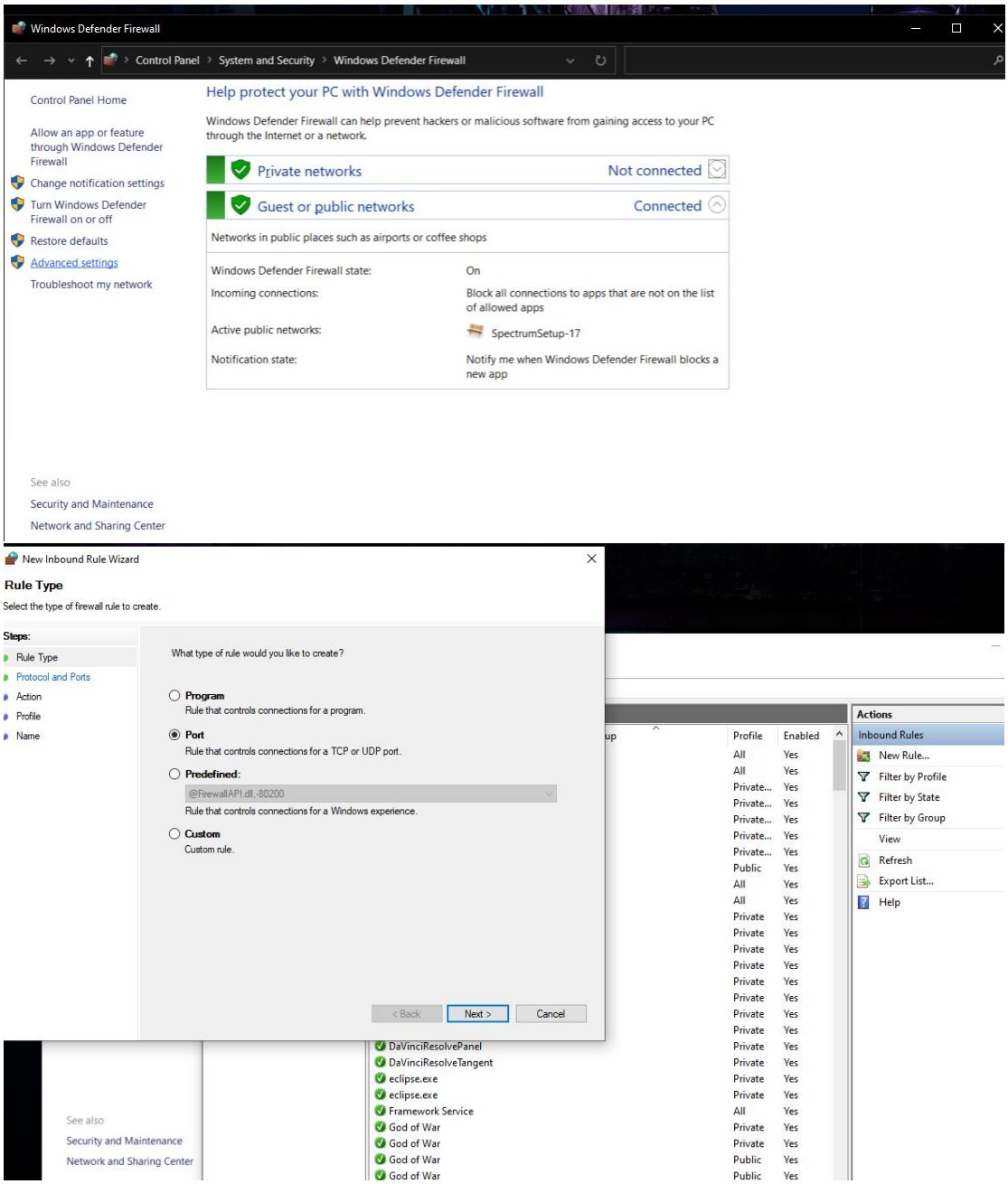
**Step 6 :**

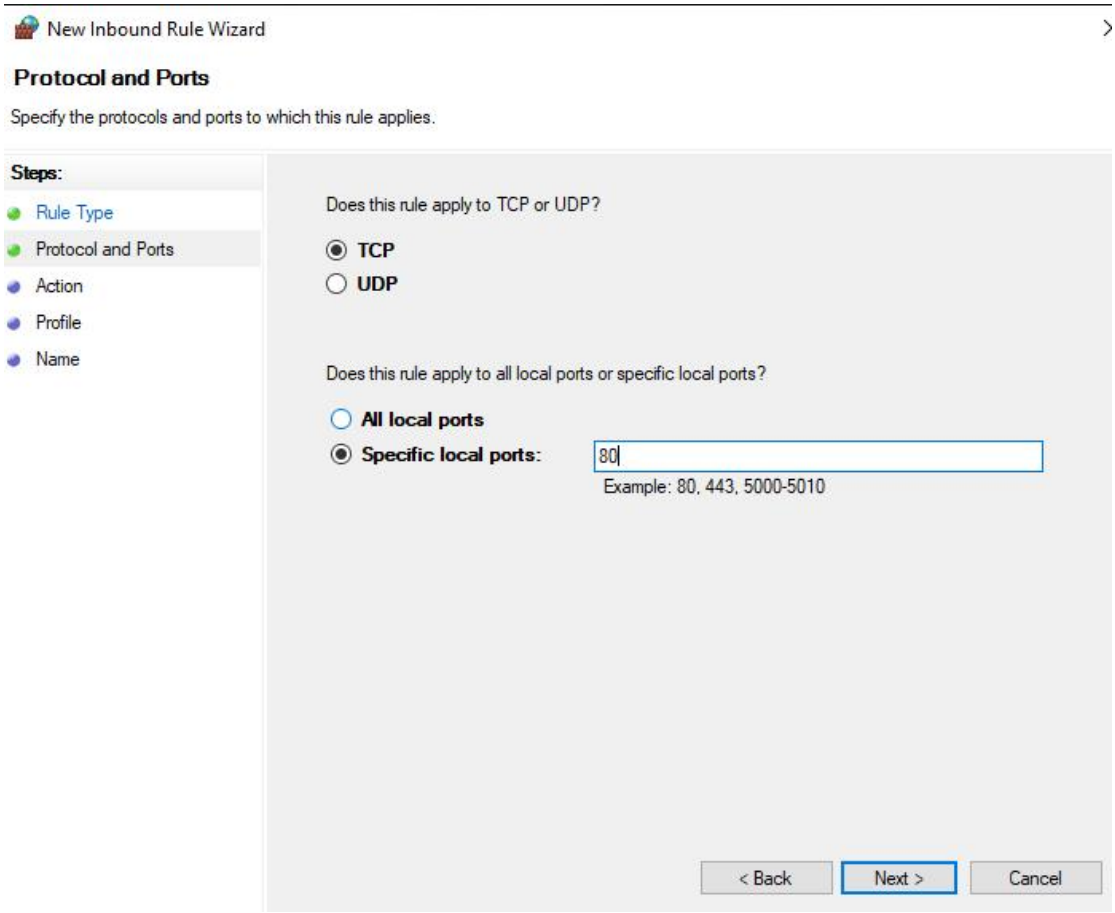
A.

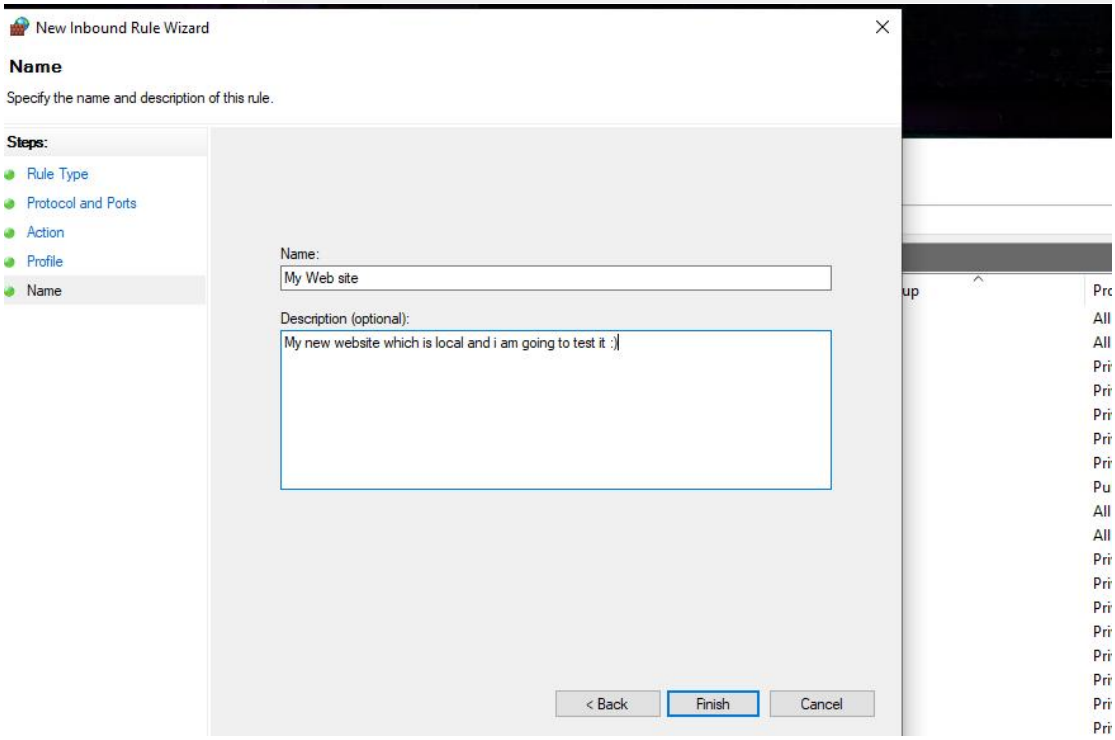

Apache 2.4.54.2
Version
Service administration 'wampapache64'
Apache settings
Apache modules
Apache Tools
Alias directories
Files & Documentation
httpd.conf
httpd-vhosts.conf
Apache error log (1.17 KiB)
Apache access log (62 B)
Apache documentation
Wampserver - 3.3.0 - 64bit
Made in France by Dominique Ottello
Localhost
PhpMyAdmin
Adminer 4.8.1
Your VirtualHosts
Apache 2.4.54.2
PHP 8.0.26
Default DBMS: mysql
MySQL 8.0.31
MariaDB 10.10.2
Help -> MariaDB - MySQL
Services
Start All Services
Stop All Services
Restart All Services
Wampserver


httpd-vhosts.conf - Notepad
File Edit Format View Help
# Virtual Hosts
#
<VirtualHost *:80>
ServerName localhost
ServerAlias localhost
DocumentRoot "${INSTALL_DIR}/www"
<Directory "${INSTALL_DIR}/www/">
Options +Indexes +Includes +FollowSymLinks +MultiViews
AllowOverride All
Require all granted
</Directory>
</VirtualHost>

B.

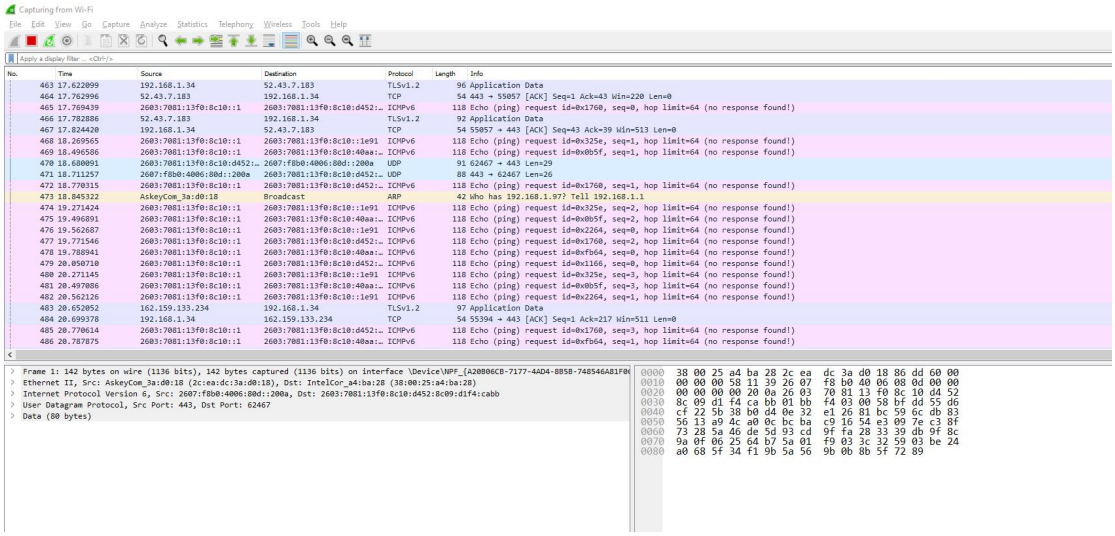

Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
SpectrumSetup-17
Notification state:
Notify me when Windows Defender Firewall blocks a new app
See also
Security and Maintenance
Network and Sharing Center
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Profile
Enabled
DaVinciResolvePanel
DaVinciResolveTangent
eclipse.exe
eclipse.exe
Framework Service
God of War
God of War
God of War
God of War
See also
Security and Maintenance
Network and Sharing Center


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
80
Example: 80, 443, 5000-5010
< Back
Next >
Cancel

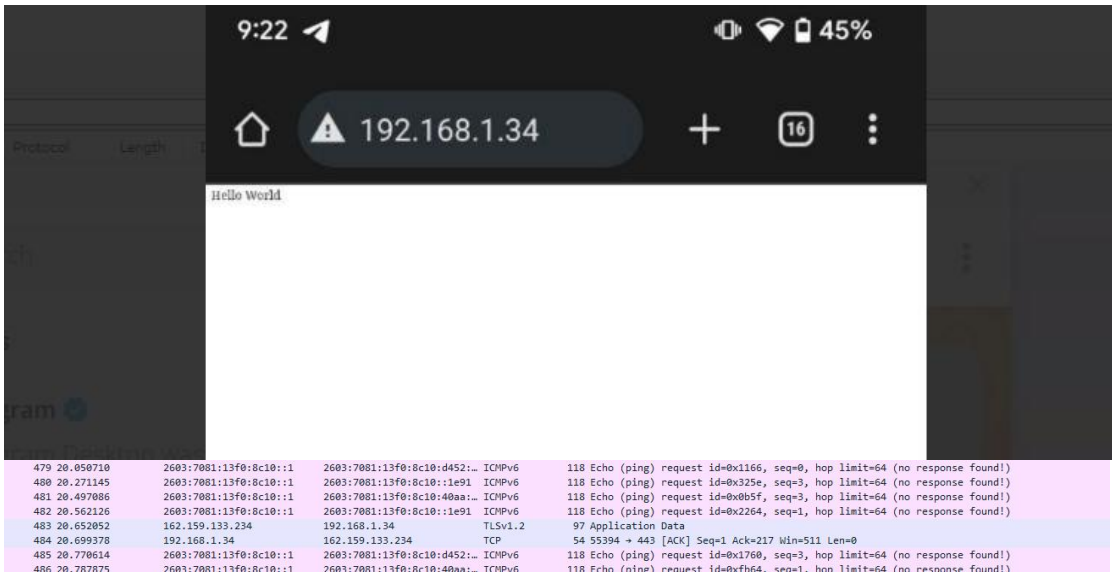

New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
My Web site
Description (optional):
My new website which is local and i am going to test it :)
< Back
Finish
Cancel

## Step 7 :

A.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
463 17.622099 192.168.1.34 52.43.7.183 TLSv1.2 96 Application Data
464 17.762996 52.43.7.183 192.168.1.34 TCP 54 443 → 55057 [ACK] Seq=1 Ack=43 Win=220 Len=0
465 17.769439 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1760, seq=0, hop limit=64 (no response found!)
466 17.782886 52.43.7.183 192.168.1.34 TLSv1.2 92 Application Data
467 17.824420 192.168.1.34 52.43.7.183 TCP 54 55057 → 443 [ACK] Seq=43 Ack=39 Win=513 Len=0
468 18.269565 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x325e, seq=1, hop limit=64 (no response found!)
469 18.496586 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:… ICMPv6 118 Echo (ping) request id=0x0b5f, seq=1, hop limit=64 (no response found!)
470 18.680091 2603:7081:13f0:8c10:d452:… 2607:f8b0:4006:80d::200a UDP 91 62467 → 443 Len=29
471 18.711257 2607:f8b0:4006:80d::200a 2603:7081:13f0:8c10:d452:… UDP 88 443 → 62467 Len=26
472 18.770315 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1760, seq=1, hop limit=64 (no response found!)
473 18.845322 AskeyCom_3a:d0:18 Broadcast ARP 42 Who has 192.168.1.97? Tell 192.168.1.1
474 19.271424 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x325e, seq=2, hop limit=64 (no response found!)
475 19.496891 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:… ICMPv6 118 Echo (ping) request id=0x0b5f, seq=2, hop limit=64 (no response found!)
476 19.562687 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x2264, seq=0, hop limit=64 (no response found!)
477 19.771546 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1760, seq=2, hop limit=64 (no response found!)
478 19.788941 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:… ICMPv6 118 Echo (ping) request id=0xfb64, seq=0, hop limit=64 (no response found!)
479 20.050710 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1166, seq=0, hop limit=64 (no response found!)
480 20.271145 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x325e, seq=3, hop limit=64 (no response found!)
481 20.497086 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:… ICMPv6 118 Echo (ping) request id=0x0b5f, seq=3, hop limit=64 (no response found!)
482 20.562126 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x2264, seq=1, hop limit=64 (no response found!)
483 20.652052 162.159.133.234 192.168.1.34 TLSv1.2 97 Application Data
484 20.699378 192.168.1.34 162.159.133.234 TCP 54 55394 → 443 [ACK] Seq=1 Ack=217 Win=511 Len=0
485 20.770614 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1760, seq=3, hop limit=64 (no response found!)
486 20.787875 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:… ICMPv6 118 Echo (ping) request id=0xfb64, seq=1, hop limit=64 (no response found!)
Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{A20B06CB-7177-44D4-8B58-748546A81F0
Ethernet II, Src: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18), Dst: IntelCor_a4:ba:28 (38:00:25:a4:ba:28)
Internet Protocol Version 6, Src: 2607:f8b0:4006:80d::200a, Dst: 2603:7081:13f0:8c10:d452:8c09:d1f4:cabb
User Datagram Protocol, Src Port: 443, Dst Port: 62467
Data (80 bytes)
0000 38 00 25 a4 ba 28 2c ea dc 3a d0 18 86 dd 60 00
0010 00 00 00 58 11 39 26 07 f8 b0 40 06 08 0d 00 00
0020 00 00 00 00 20 0a 26 03 70 81 13 f0 8c 10 d4 52
0030 8c 09 d1 f4 ca bb 01 bb f4 03 00 58 bf dd 55 d6
0040 cf 22 5b 38 b0 d4 0e 32 e1 26 81 bc 59 6c db 83
0050 56 13 a9 4c a0 0c bc ba c9 16 54 e3 09 7e c3 8f
0060 73 28 5a 46 de 5d 93 cd 9f fa 28 33 39 db 9f 8c
0070 9a 0f 06 25 64 b7 5a 01 f9 03 3c 32 59 03 be 24
0080 a0 68 5f 34 f1 9b 5a 56 9b 0b 8b 5f 72 89

B.


9:22
45%
192.168.1.34
16
Hello World
479 20.050710 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1166, seq=0, hop limit=64 (no response found!)
480 20.271145 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x325e, seq=3, hop limit=64 (no response found!)
481 20.497086 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:… ICMPv6 118 Echo (ping) request id=0x0b5f, seq=3, hop limit=64 (no response found!)
482 20.562126 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x2264, seq=1, hop limit=64 (no response found!)
483 20.652052 162.159.133.234 192.168.1.34 TLSv1.2 97 Application Data
484 20.699378 192.168.1.34 162.159.133.234 TCP 54 55394 → 443 [ACK] Seq=1 Ack=217 Win=511 Len=0
485 20.770614 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:… ICMPv6 118 Echo (ping) request id=0x1760, seq=3, hop limit=64 (no response found!)

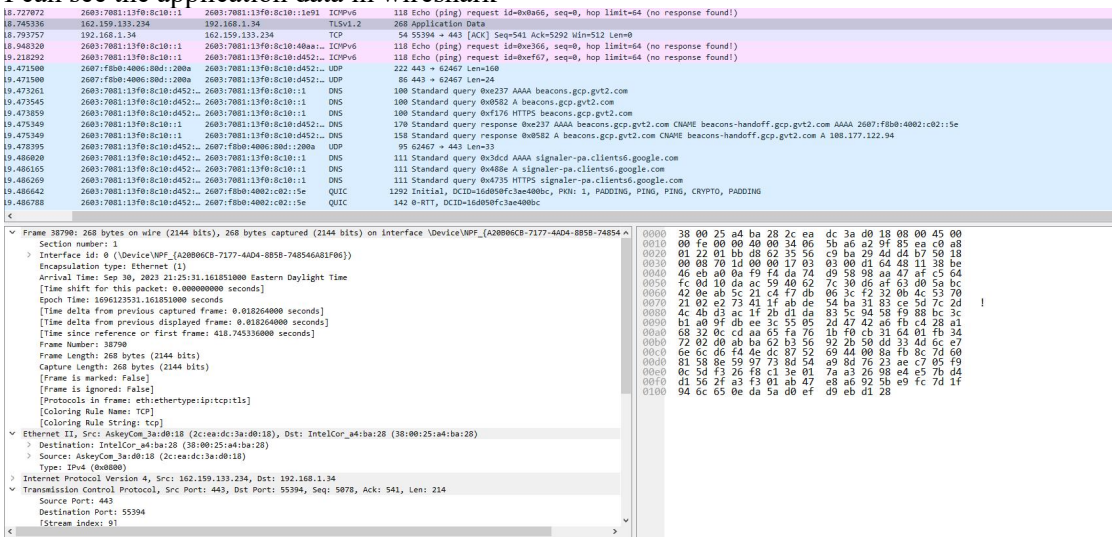
C.

I captured the Ip of my wifi in netstat through which I ran the webserver :

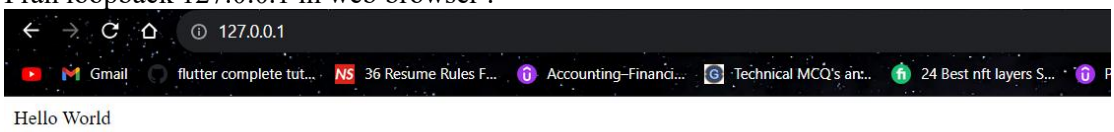
```
TCP    192.168.1.34:80        192.168.1.120:38966    TIME_WAIT
TCP    192.168.1.34:80        192.168.1.120:38976    ESTABLISHED
TCP    192.168.1.34:80        192.168.1.120:47344    ESTABLISHED
TCP    192.168.1.34:80        192.168.1.120:56978    TIME_WAIT
TCP    192.168.1.34:80        192.168.1.120:56988    TIME_WAIT
TCP    192.168.1.34:53281     52.159.126.152:443     ESTABLISHED
TCP    192.168.1.34:53662     52.159.126.152:443     ESTABLISHED
TCP    192.168.1.34:55057     52.43.7.183:443        ESTABLISHED
TCP    192.168.1.34:55375     54.196.227.84:443      ESTABLISHED
TCP    192.168.1.34:55394     162.159.133.234:443    ESTABLISHED
TCP    192.168.1.34:55510     204.79.197.222:443     TIME_WAIT
TCP    192.168.1.34:55512     51.132.193.104:443     TIME_WAIT
TCP    192.168.1.34:55513     108.138.106.51:443     ESTABLISHED
TCP    192.168.1.34:55519     13.107.18.254:443      ESTABLISHED
TCP    192.168.1.34:55520     13.107.6.254:443       ESTABLISHED
TCP    192.168.1.34:55522     204.79.197.222:443     TIME_WAIT
TCP    192.168.1.34:55523     91.108.56.148:443      ESTABLISHED
TCP    192.168.1.34:55524     91.108.56.148:80       TIME_WAIT
TCP    192.168.1.34:55526     91.108.56.148:443      TIME_WAIT
TCP    192.168.1.34:55527     149.154.167.92:443     TIME_WAIT
TCP    192.168.1.34:55528     91.108.56.148:80       TIME_WAIT
TCP    192.168.1.34:55529     149.154.167.92:80      TIME_WAIT
TCP    192.168.1.34:55531     91.108.56.148:443      TIME_WAIT
TCP    192.168.1.34:55532     149.154.167.41:443     TIME_WAIT
TCP    192.168.1.34:55533     91.108.56.148:80       TIME_WAIT
TCP    192.168.1.34:55536     54.152.26.34:443       ESTABLISHED
TCP    192.168.1.34:55537     3.211.92.239:443       CLOSE_WAIT
TCP    192.168.1.34:55538     3.229.227.245:443      CLOSE_WAIT
```

D :

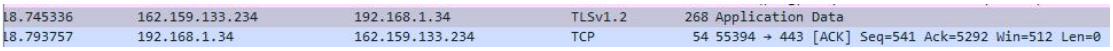
I can see the application data in wireshark



I ran loopback 127.0.0.1 in web browser :

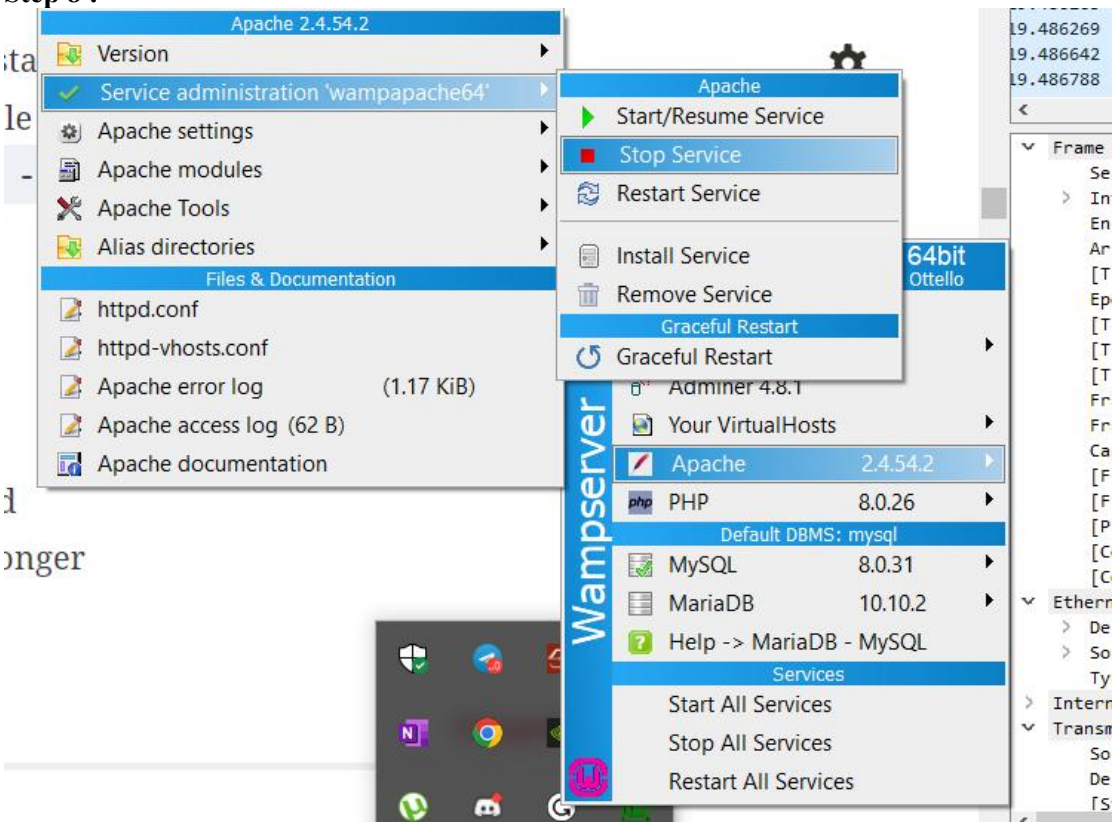


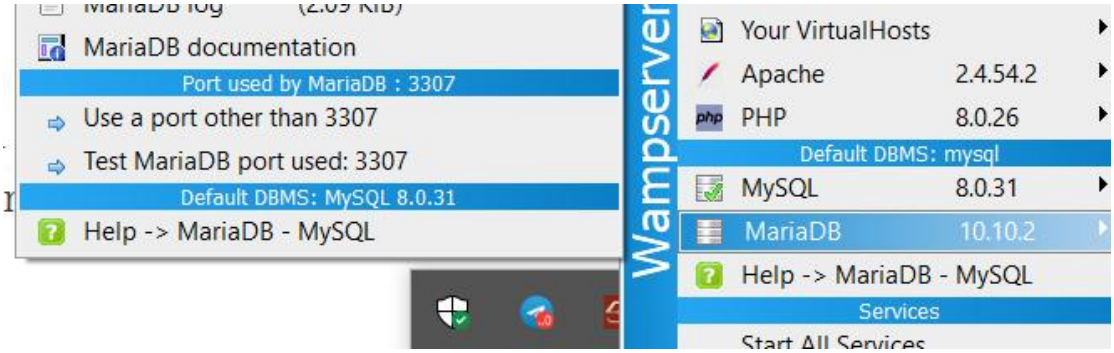

E.




From this we can see TCP is Client and TLSv1.2 is server which say 268 Application Data.

**Step 8 :**






It seems like Maria DB runs on port 3307 even though we stopped apache web server, Now lets check with netstat -an to capture it.

```
  TCP    [::]:3307              [::]:0                 LISTENING
```

We can see port 3307 is still listening.

**Step 9 :**

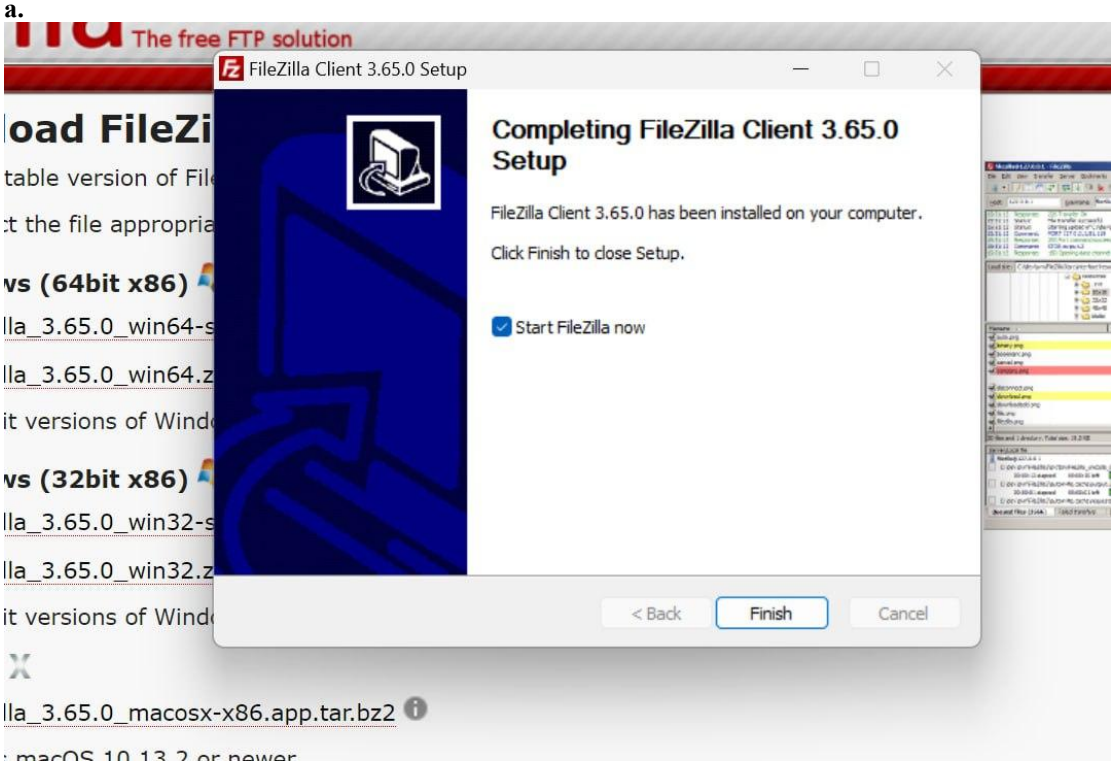
```
Active Connections

  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    0.0.0.0:902            0.0.0.0:0              LISTENING
```

It simply means there is no port 80 is running as we stopped the apache service. So it is no more like it showed in step 2.

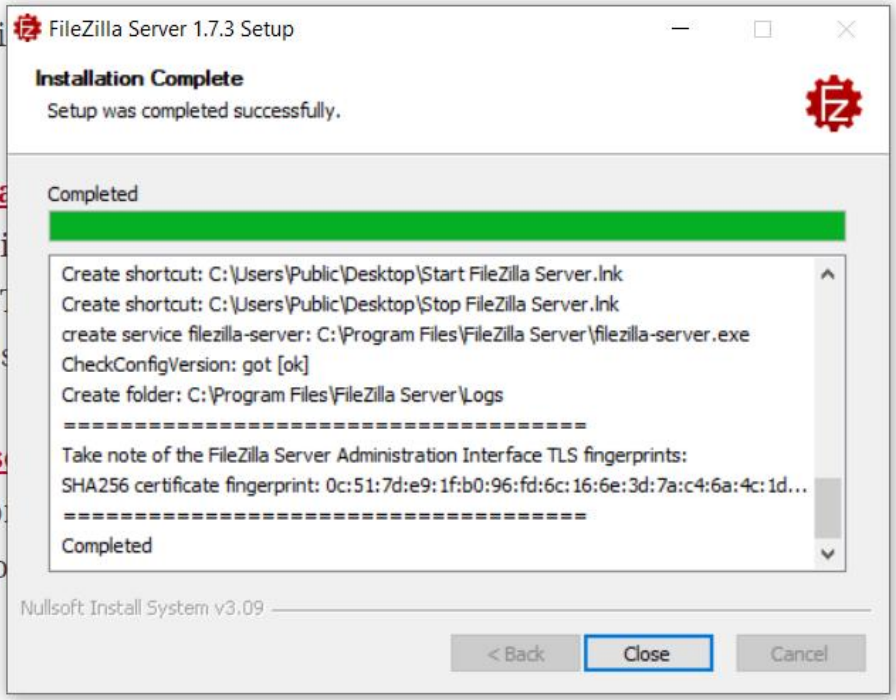
**Exercise : 8. 04 :**

**Step 1 :**

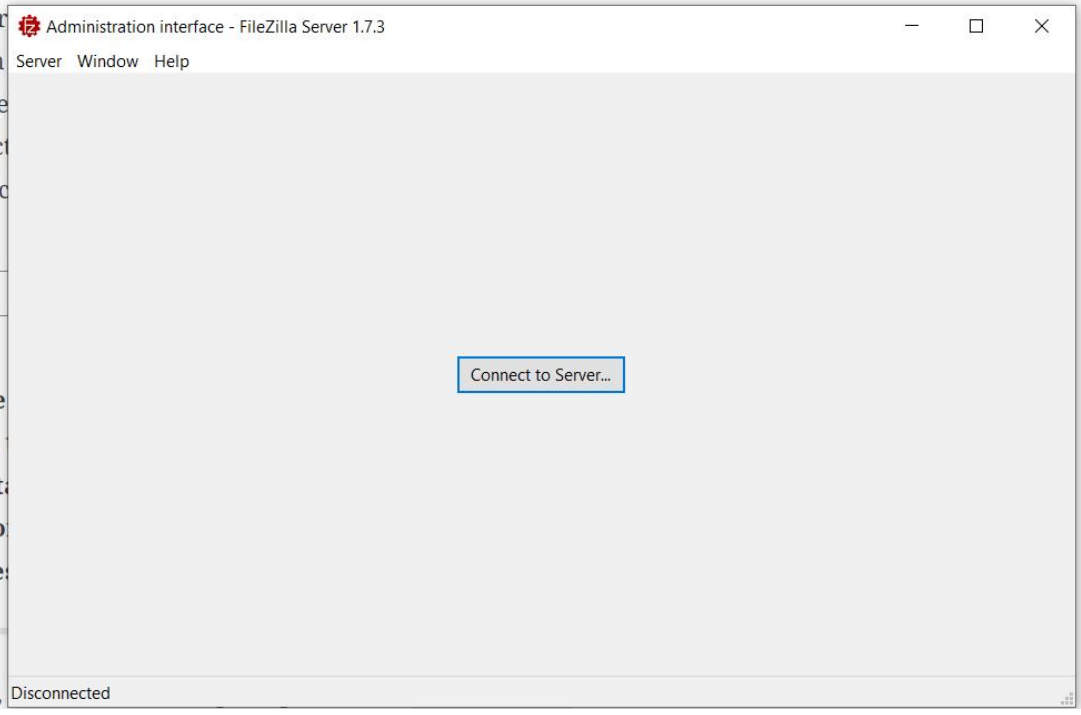
**a.**

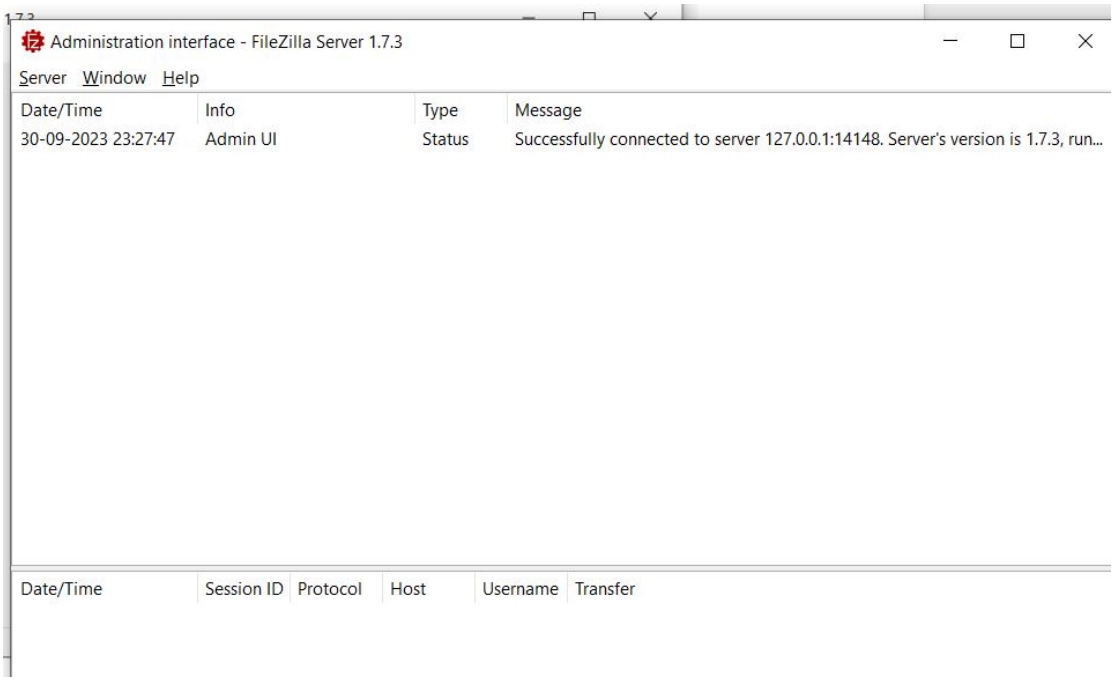


**B.**

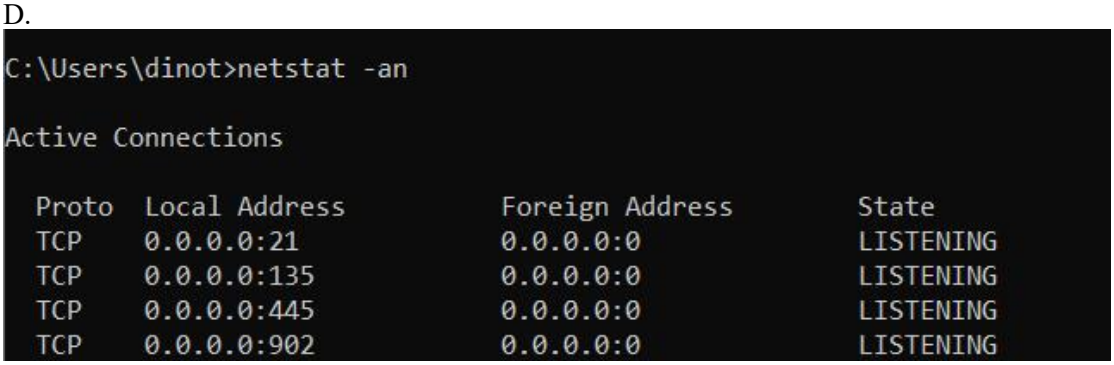

FileZilla Server 1.7.3 Setup
Installation Complete
Setup was completed successfully.
Completed
Create shortcut: C:\Users\Public\Desktop\Start FileZilla Server.lnk
Create shortcut: C:\Users\Public\Desktop\Stop FileZilla Server.lnk
create service filezilla-server: C:\Program Files\FileZilla Server\filezilla-server.exe
CheckConfigVersion: got [ok]
Create folder: C:\Program Files\FileZilla Server\Logs
Take note of the FileZilla Server Administration Interface TLS fingerprints:
SHA256 certificate fingerprint: 0c:51:7d:e9:1f:b0:96:fd:6c:16:6e:3d:7a:c4:6a:4c:1d...
Completed
Nullsoft Install System v3.09
< Back
Close
Cancel

**C.**


Administration interface - FileZilla Server 1.7.3
Server Window Help
Connect to Server...
Disconnected



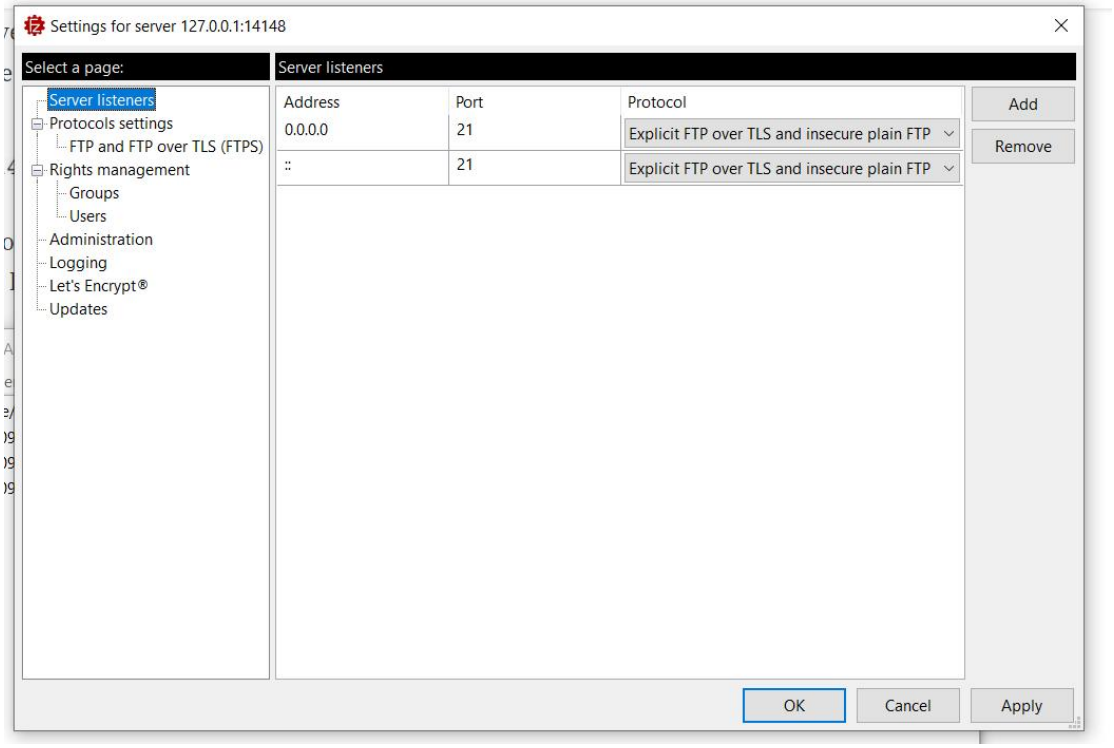

D.



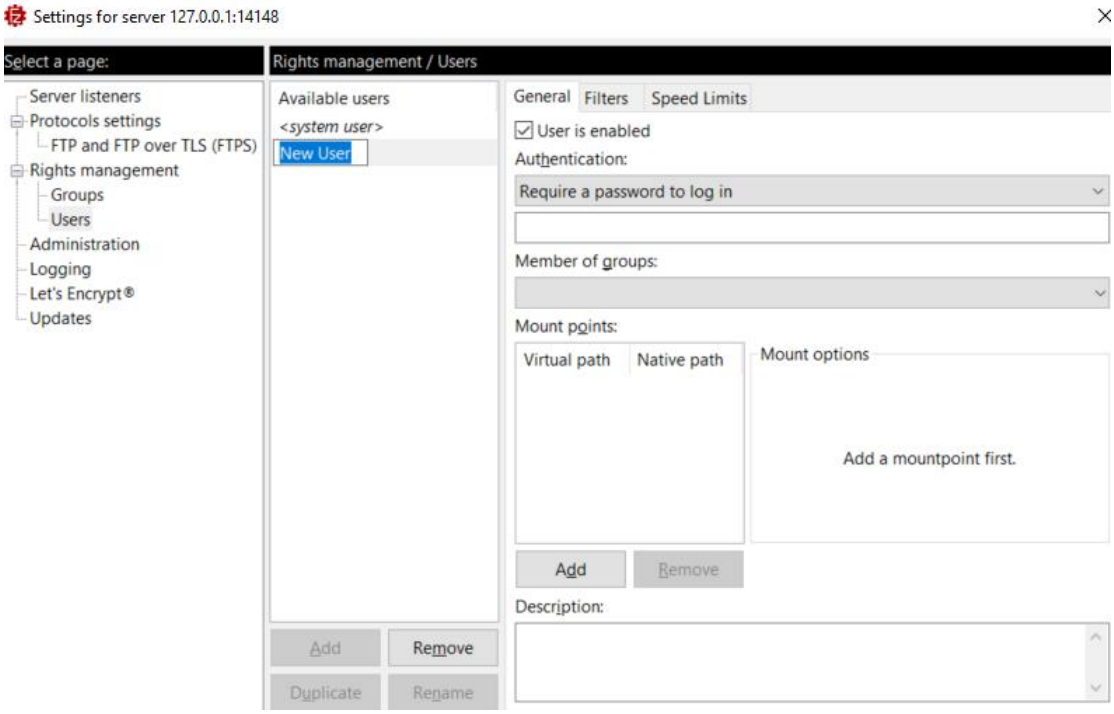

As FTP server is started in this system and it will work with any IP bound with this system. And Loop back server is started too for listening back to the server for testing purposes.

**Step 2 :**

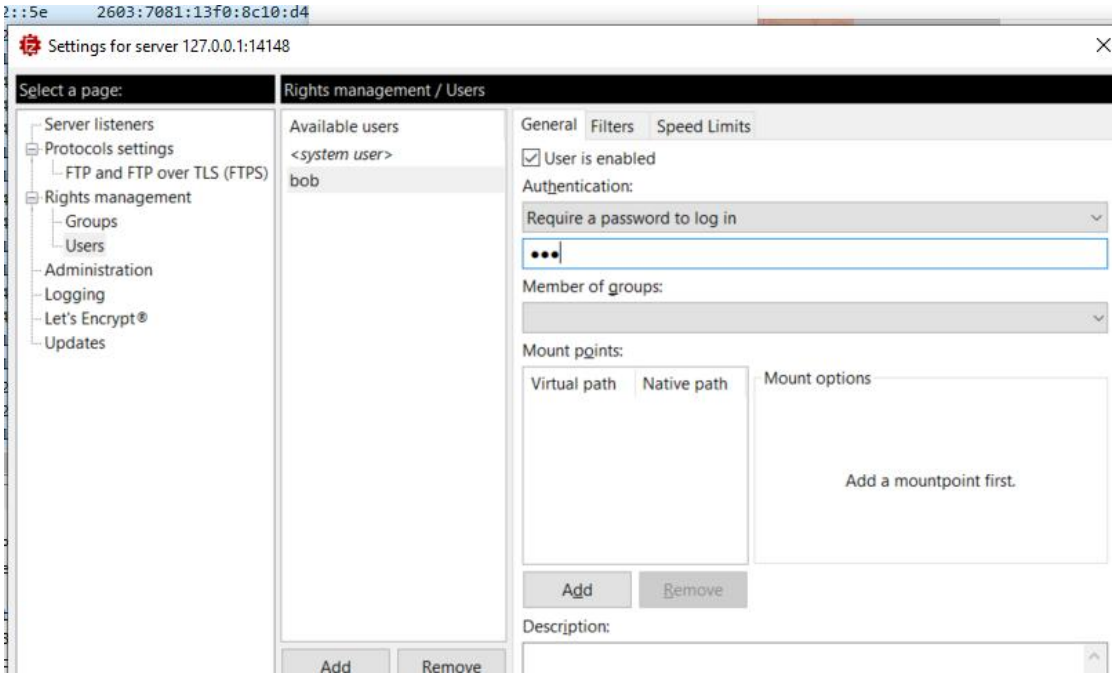
A.


Settings for server 127.0.0.1:14148
Select a page:
Server listeners
Protocols settings
FTP and FTP over TLS (FTPS)
Rights management
Groups
Users
Administration
Logging
Let's Encrypt®
Updates
Server listeners
Address
Port
Protocol
0.0.0.0
21
Explicit FTP over TLS and insecure plain FTP
::
21
Explicit FTP over TLS and insecure plain FTP
Add
Remove
OK
Cancel
Apply

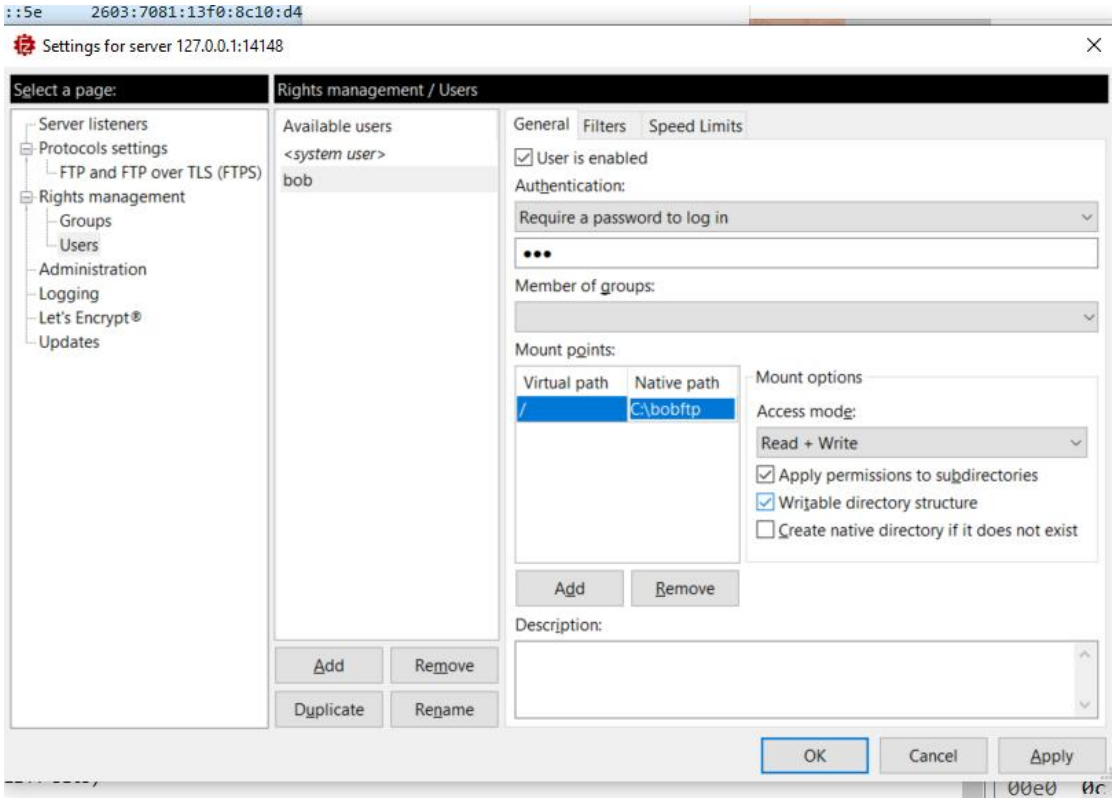
B.


Settings for server 127.0.0.1:14148
Select a page:
Server listeners
Protocols settings
FTP and FTP over TLS (FTPS)
Rights management
Groups
Users
Administration
Logging
Let's Encrypt®
Updates
Rights management / Users
Available users
<system user>
New User
Add
Remove
Duplicate
Rename
General
Filters
Speed Limits
User is enabled
Authentication:
Require a password to log in
Member of groups:
Mount points:
Virtual path
Native path
Mount options
Add a mountpoint first.
Add
Remove
Description:

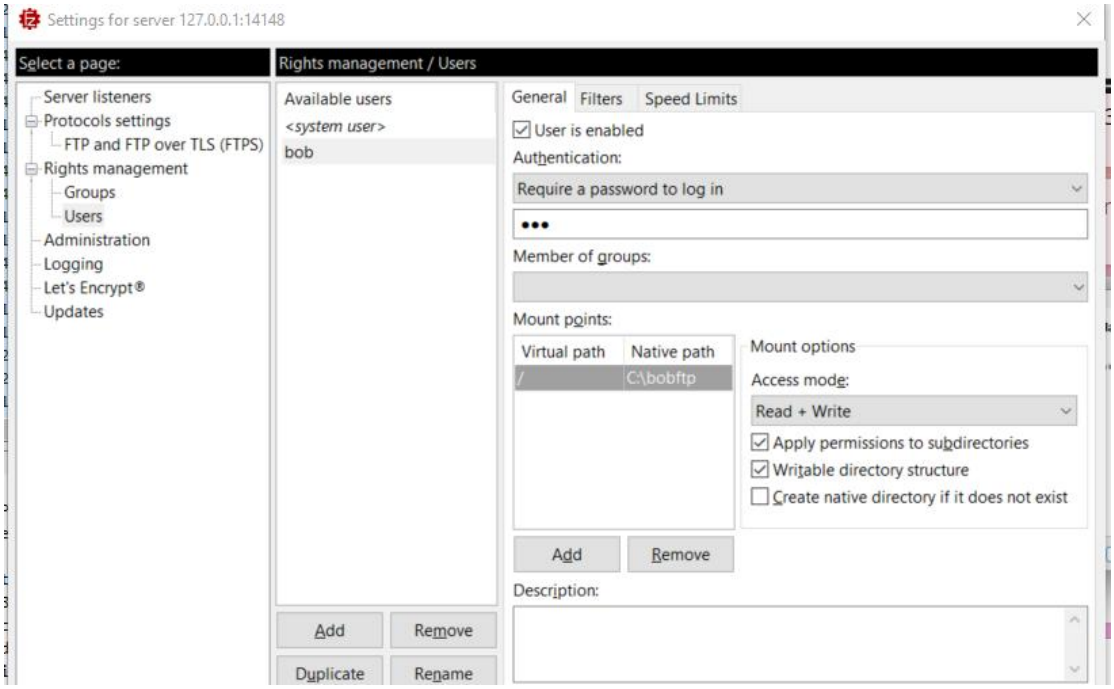
C.


2::5e 2603:7081:13f0:8c10:d4
Settings for server 127.0.0.1:14148
Select a page:
Server listeners
Protocols settings
FTP and FTP over TLS (FTPS)
Rights management
Groups
Users
Administration
Logging
Let's Encrypt®
Updates
Rights management / Users
Available users
<system user>
bob
Add
Remove
General
Filters
Speed Limits
User is enabled
Authentication:
Require a password to log in
Member of groups:
Mount points:
Virtual path
Native path
Mount options
Add a mountpoint first.
Add
Remove
Description:

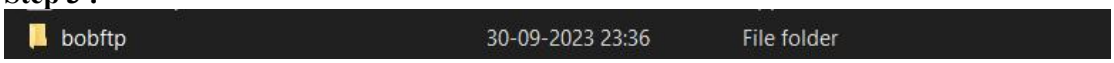
E.


2::5e 2603:7081:13f0:8c10:d4
Settings for server 127.0.0.1:14148
Select a page:
Server listeners
Protocols settings
FTP and FTP over TLS (FTPS)
Rights management
Groups
Users
Administration
Logging
Let's Encrypt®
Updates
Rights management / Users
Available users
<system user>
bob
Add
Remove
Duplicate
Rename
General
Filters
Speed Limits
User is enabled
Authentication:
Require a password to log in
Member of groups:
Mount points:
Virtual path
Native path
/
C:\bobftp
Mount options
Access mode:
Read + Write
Apply permissions to subdirectories
Writable directory structure
Create native directory if it does not exist
Add
Remove
Description:
OK
Cancel
Apply

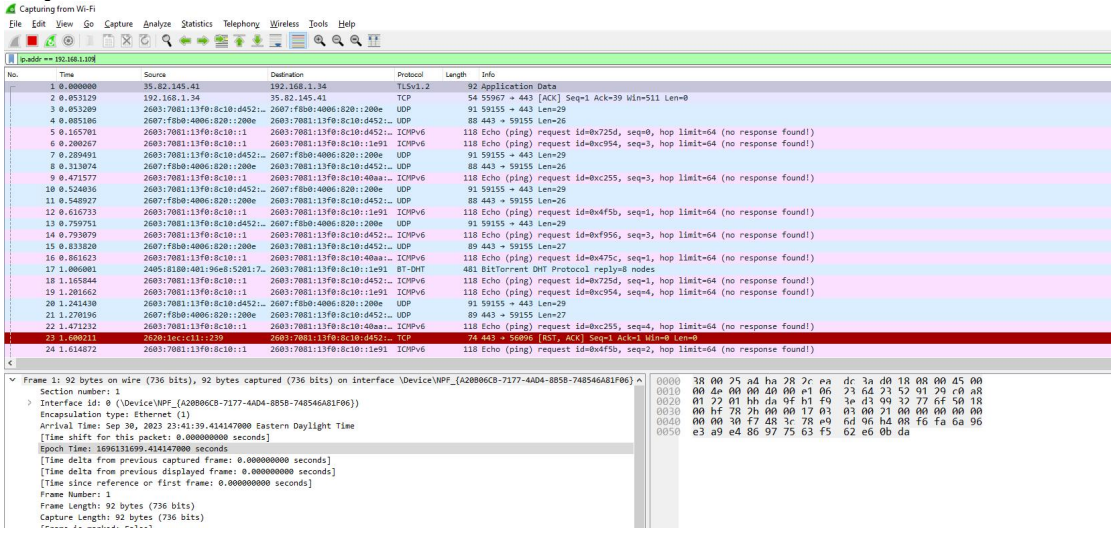
F.




## Step 3 :

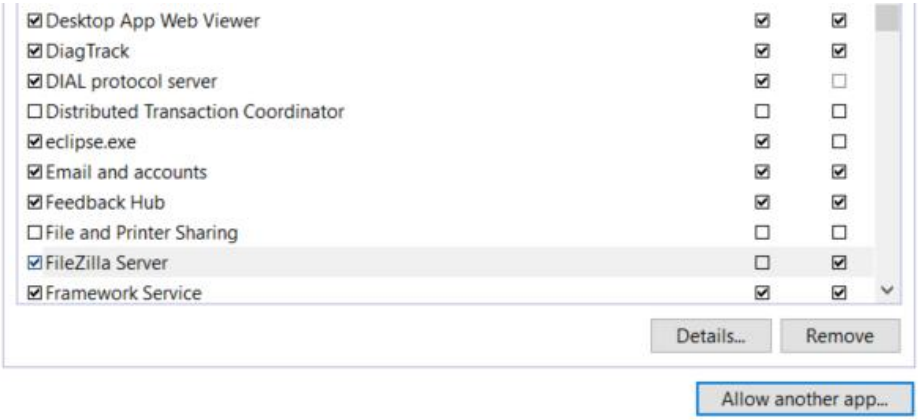



## Step 4 :



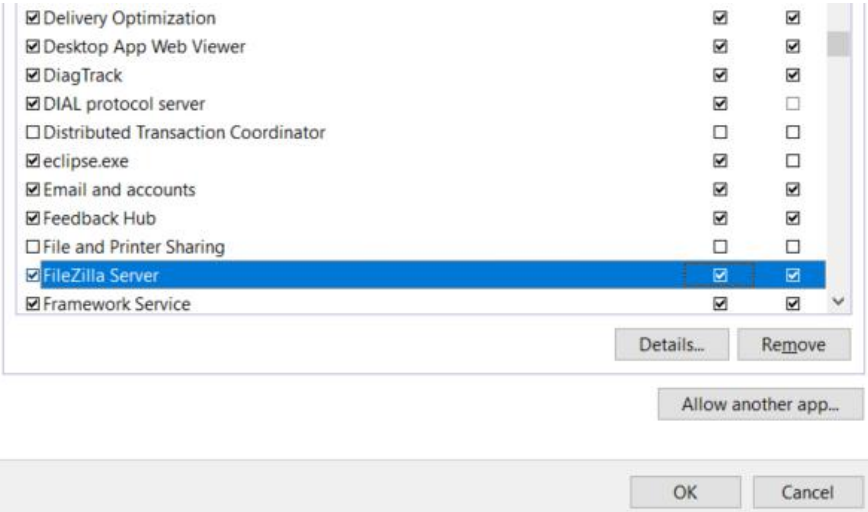
**Step 5 :**

I.

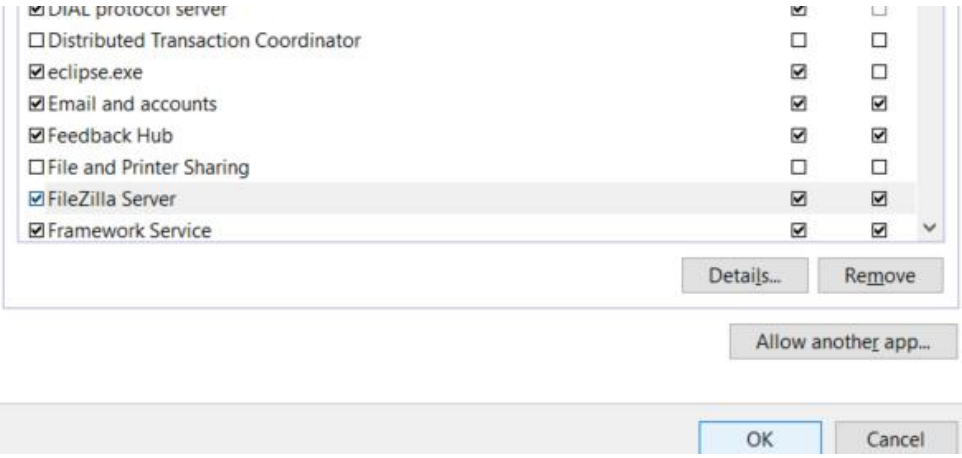



FileZilla added successfully

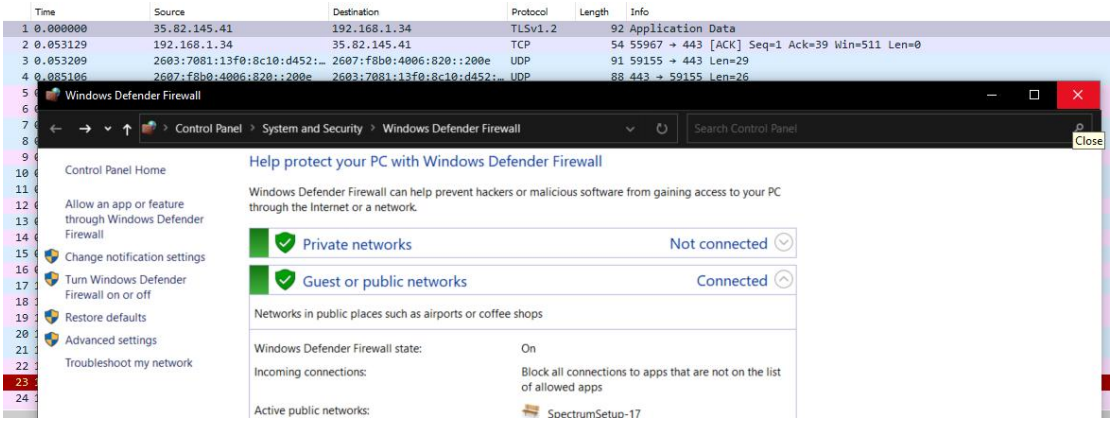
J.



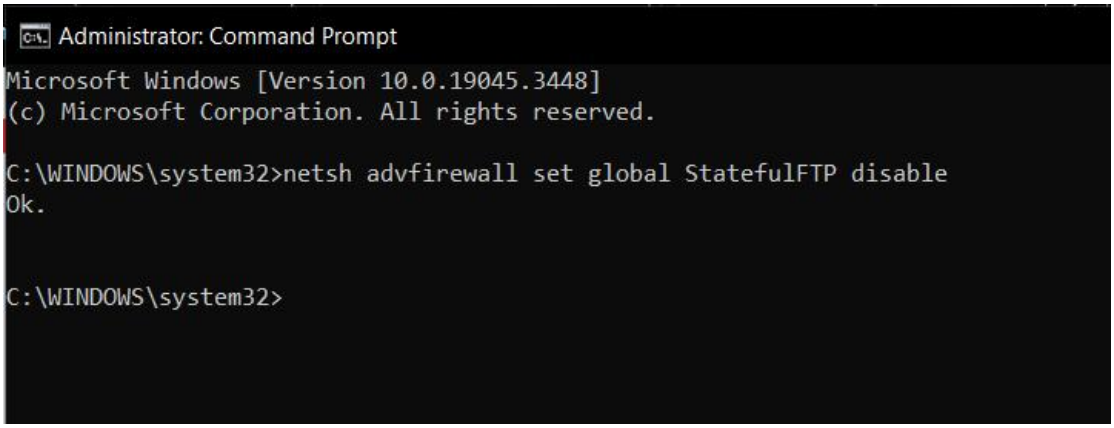

K.




L.

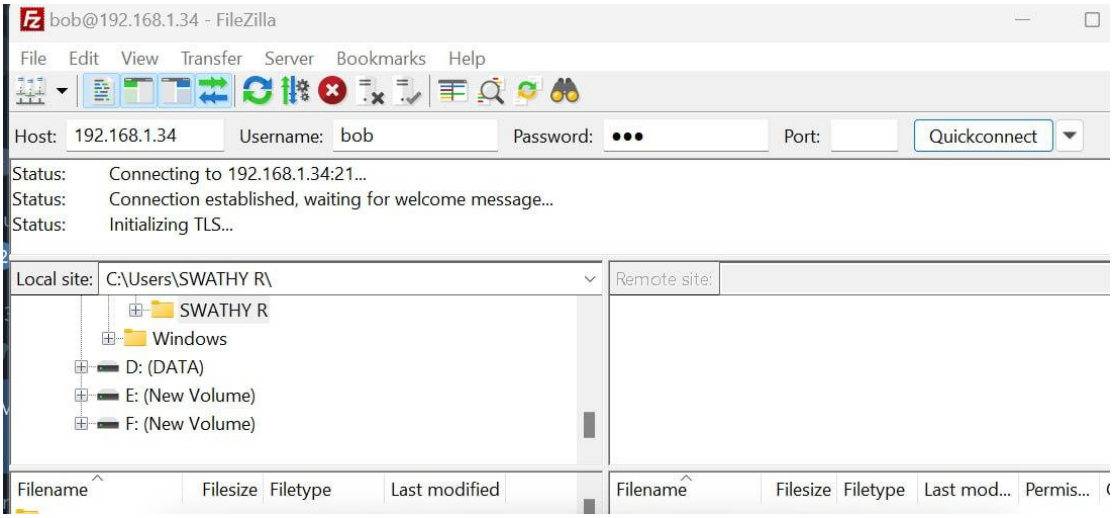

Time Source Destination Protocol Length Info
1 0.000000 35.82.145.41 192.168.1.34 TLSv1.2 92 Application Data
2 0.053129 192.168.1.34 35.82.145.41 TCP 54 55967 → 443 [ACK] Seq=1 Ack=39 Win=511 Len=0
3 0.053209 2603:7081:13f0:8c10:d452:… 2607:f8b0:4006:820::200e UDP 91 59155 → 443 Len=29
4 0.085106 2607:f8b0:4006:820::200e 2603:7081:13f0:8c10:d452:… UDP 88 443 → 59155 Len=26
Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Close
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
SpectrumSetup-17

M.


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>netsh advfirewall set global StatefulFTP disable
Ok.
C:\WINDOWS\system32>

**Step 6 :**

C.


bob@192.168.1.34 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: 192.168.1.34 Username: bob Password: ●●● Port: Quickconnect
Status: Connecting to 192.168.1.34:21...
Status: Connection established, waiting for welcome message...
Status: Initializing TLS...
Local site: C:\Users\SWATHY R\
Remote site:
SWATHY R
Windows
D: (DATA)
E: (New Volume)
F: (New Volume)
Filename Filesize Filetype Last modified
Filename Filesize Filetype Last mod... Permis...

D.


Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful

## Step 7 :

A.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.109
No. Time Source Destination Protocol Length Info
1 0.000000 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
2 0.031575 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
3 0.160825 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:... ICMPv6 118 Echo (ping) request id=0x3620, seq=4, hop limit=64 (no response found!)
4 0.234444 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
5 0.264061 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
6 0.297843 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x6524, seq=2, hop limit=64 (no response found!)
7 0.470057 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
8 0.500120 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
9 0.549204 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:... ICMPv6 118 Echo (ping) request id=0x6825, seq=2, hop limit=64 (no response found!)
10 0.702629 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
11 0.719117 Chongqin_40:2d:b7 Broadcast ARP 42 Who has 169.254.169.254? Tell 192.168.1.109
12 0.732832 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
13 0.843378 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:820::200e UDP 91 59155 → 443 Len=29
14 0.870016 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:... ICMPv6 118 Echo (ping) request id=0x9926, seq=2, hop limit=64 (no response found!)
15 0.873093 2607:f8b0:4006:820::200e 2603:7081:13f0:8c10:d452:... UDP 88 443 → 59155 Len=26
16 1.138033 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
17 1.168573 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
18 1.298739 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0x6524, seq=3, hop limit=64 (no response found!)
19 1.550070 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:40aa:... ICMPv6 118 Echo (ping) request id=0x6825, seq=3, hop limit=64 (no response found!)
20 1.743152 Chongqin_40:2d:b7 Broadcast ARP 42 Who has 169.254.169.254? Tell 192.168.1.109
21 1.870257 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:... ICMPv6 118 Echo (ping) request id=0x9926, seq=3, hop limit=64 (no response found!)
22 1.974337 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
23 2.005608 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
24 2.159733 54.196.227.84 192.168.1.34 TCP 54 443 → 55375 [ACK] Seq=1 Ack=1 Win=27 Len=0
Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A81F06}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A81F06})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 30, 2023 23:59:23.009216000 Eastern Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1696132763.009216000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 91 bytes (728 bits)
Capture Length: 91 bytes (728 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: IntelCor_a4:ba:28 (38:00:25:a4:ba:28), Dst: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18)
Destination: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18)
Source: IntelCor_a4:ba:28 (38:00:25:a4:ba:28)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2603:7081:13f0:8c10:d452:8c09:d1f4:cabb, Dst: 2607:f8b0:4006:81e::200a
User Datagram Protocol, Src Port: 56633, Dst Port: 443
Data (29 bytes)
0000 2c ea dc 3a d0 18 38 00 25 a4 ba 28 86 dd 60 0d
0010 60 d3 00 25 11 40 26 03 70 81 13 f0 8c 10 d4 52
0020 8c 09 d1 f4 ca bb 26 07 f8 b0 40 06 08 1e 00 00
0030 00 00 00 00 20 0a dd 39 01 bb 00 25 ba ae 5d f5
0040 de 12 32 3d 81 7f dc 67 ad c5 6c b8 7e af b9 58
0050 c4 f7 34 b6 1a 3a d0 fb 25 45 b6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10:d452:... ICMPv6 118 Echo (ping) request id=0x2162, seq=0, hop limit=64 (no response found!)
2 0.034630 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
3 0.064800 2607:f8b0:4006:81e::200a 2603:7081:13f0:8c10:d452:... UDP 87 443 → 56633 Len=25
4 0.416205 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 1292 Initial, DCID=e6661098267249c8, PKN: 1, PADDING, PING, PING, PADDING, CRYPTO, PADDING, PING, PING, PADDING
5 0.416396 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 141 0-RTT, DCID=e6661098267249c8
6 0.416593 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 887 0-RTT, DCID=e6661098267249c8
7 0.421106 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 188 0-RTT, DCID=e6661098267249c8
8 0.428721 2603:7081:13f0:8c10::1 2603:7081:13f0:8c10::1e91 ICMPv6 118 Echo (ping) request id=0xfe5f, seq=1, hop limit=64 (no response found!)
9 0.454209 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 1292 Protected Payload (KP0)
10 0.454209 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 840 Protected Payload (KP0)
11 0.454209 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 250 Protected Payload (KP0)
12 0.454209 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 86 Protected Payload (KP0)
13 0.454209 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 85 Protected Payload (KP0)
14 0.454597 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 140 Handshake, DCID=e6661098267249c8
15 0.454682 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 93 Protected Payload (KP0), DCID=e6661098267249c8
16 0.454766 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 93 Protected Payload (KP0), DCID=e6661098267249c8
17 0.464531 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 594 Protected Payload (KP0)
18 0.464531 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 149 Protected Payload (KP0)
19 0.464531 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 84 Protected Payload (KP0)
20 0.464777 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 97 Protected Payload (KP0), DCID=e6661098267249c8
21 0.464825 2607:f8b0:4006:81e::2003 2603:7081:13f0:8c10:d452:... QUIC 84 Protected Payload (KP0)
22 0.464864 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 97 Protected Payload (KP0), DCID=e6661098267249c8
23 0.464908 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::2003 QUIC 93 Protected Payload (KP0), DCID=e6661098267249c8
24 0.465470 2603:7081:13f0:8c10:d452:... 2607:f8b0:4006:81e::200a UDP 91 56633 → 443 Len=29
Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A81F06}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{A20B06CB-7177-4AD4-8B5B-748546A81F06})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 1, 2023 00:00:04.435575000 Eastern Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1696132804.435575000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 118 bytes (944 bits)
Capture Length: 118 bytes (944 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:icmpv6:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18), Dst: IntelCor_a4:ba:28 (38:00:25:a4:ba:28)
Destination: IntelCor_a4:ba:28 (38:00:25:a4:ba:28)
Source: AskeyCom_3a:d0:18 (2c:ea:dc:3a:d0:18)
Type: IPv6 (0x86dd)
0000 38 00 25 a4 ba 28 2c ea dc 3a d0 18 86 dd 60 0b
0010 af 4b 00 40 3a 40 26 03 70 81 13 f0 8c 10 00 00
0020 00 00 00 00 00 01 26 03 70 81 13 f0 8c 10 d4 52
0030 8c 09 d1 f4 ca bb 80 00 c8 ad 21 62 00 00 ab ab
0040 7f b1 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00

With Ip address and without IP address

B.

```
C:\Windows\System32>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8089           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8191           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9999           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    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1290         127.0.0.1:8191         ESTABLISHED
  TCP    127.0.0.1:1291         127.0.0.1:8191         ESTABLISHED
  TCP    127.0.0.1:1293         127.0.0.1:8191         ESTABLISHED
  TCP    127.0.0.1:1294         127.0.0.1:8191         ESTABLISHED
  TCP    127.0.0.1:1303         127.0.0.1:8191         ESTABLISHED
  TCP    127.0.0.1:1304         127.0.0.1:8191         ESTABLISHED
```

C.

```
  TCP    192.168.1.34:21        192.168.1.109:3661     ESTABLISHED
  TCP    192.168.1.34:139       0.0.0.0:0              LISTENING
  TCP    192.168.1.34:53281     52.159.126.152:443     ESTABLISHED
  TCP    192.168.1.34:53662     52.159.126.152:443     ESTABLISHED
  TCP    192.168.1.34:55375     54.196.227.84:443      ESTABLISHED
  TCP    192.168.1.34:55523     91.108.56.148:443      ESTABLISHED
```

Port 21 is used as we can see in our first line.

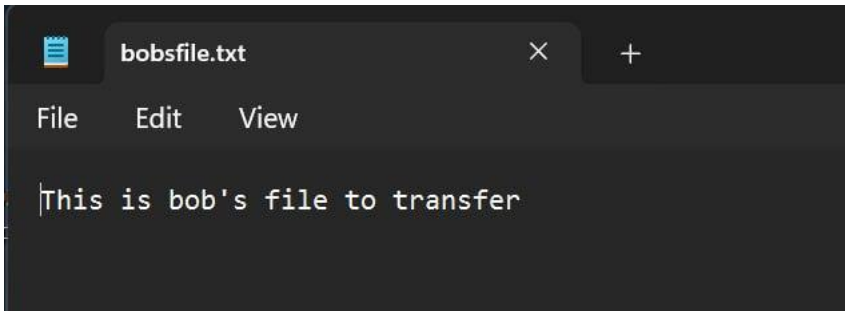
D.

Port 3661 is used for FTP Client as we can see in this IP address

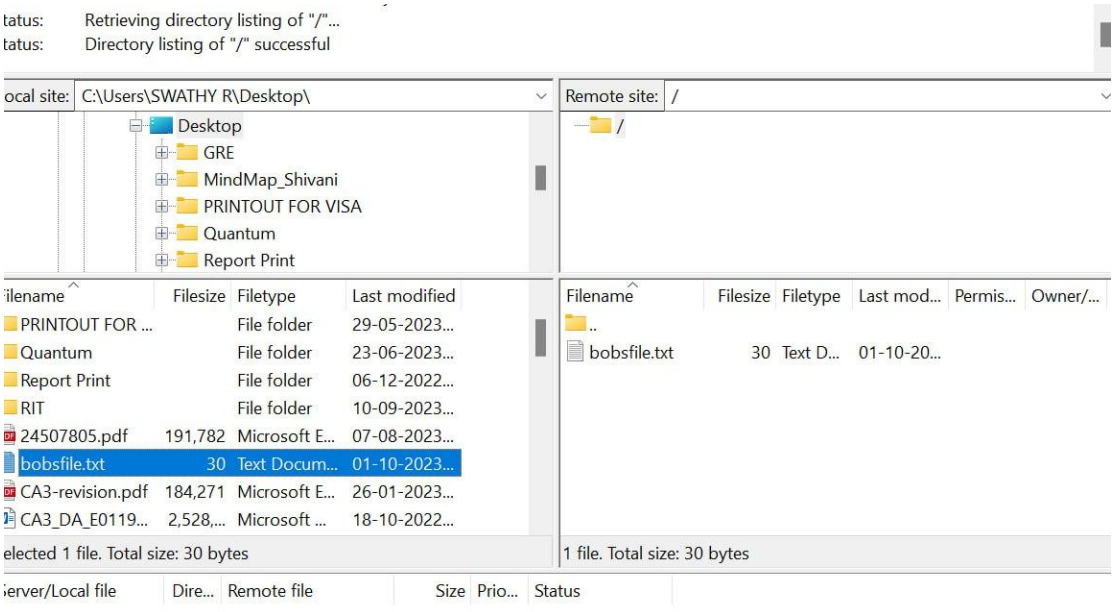
```
TCP    192.168.1.34:21        192.168.1.109:3661     ESTABLISHED
```

**Step 8 :**

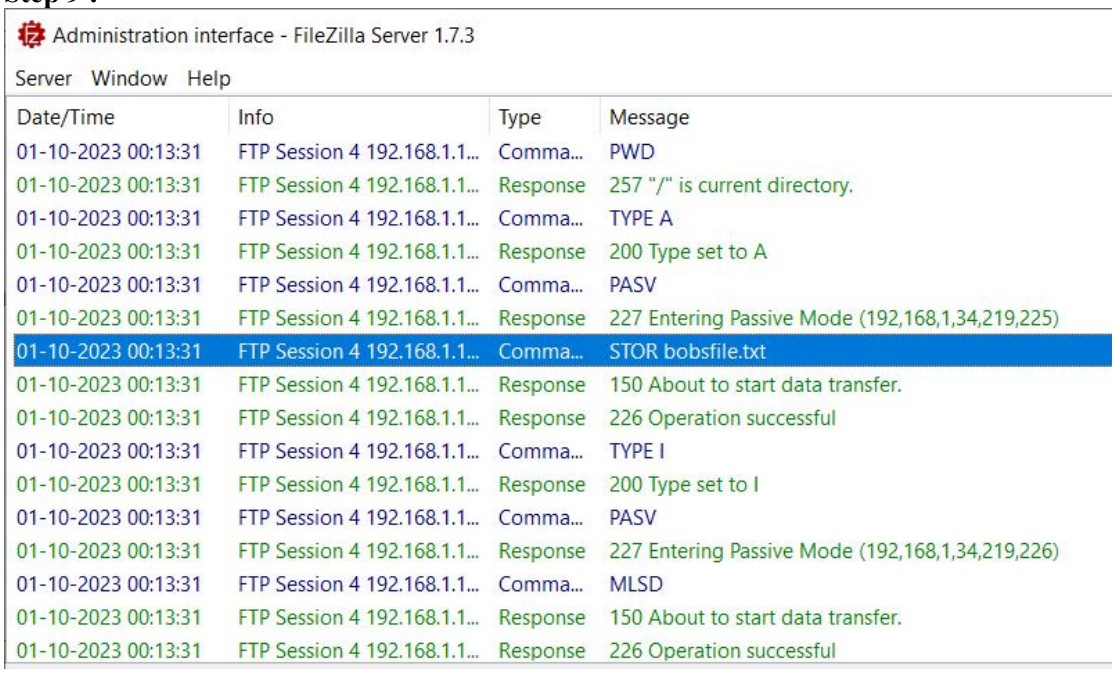
A.

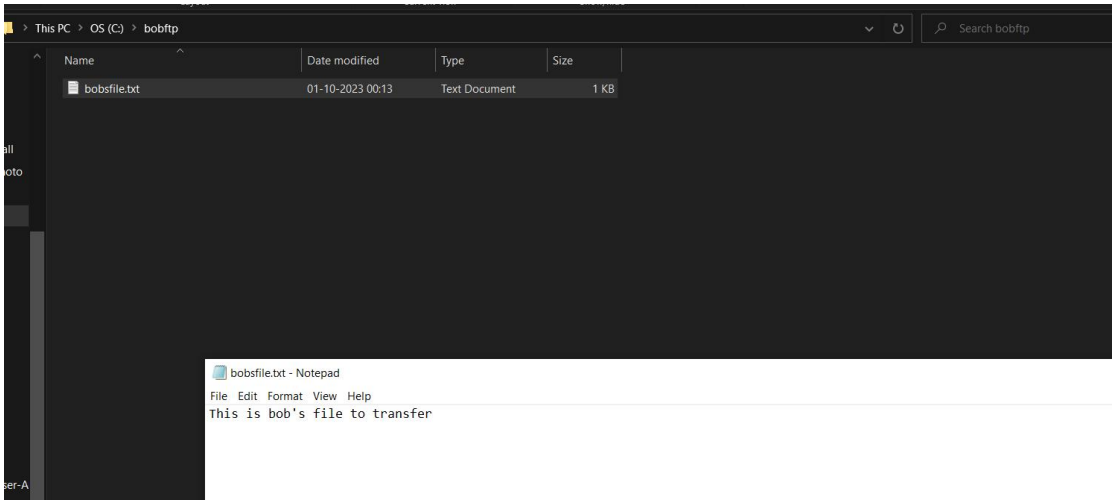


B.


tatus: Retrieving directory listing of "/"...
tatus: Directory listing of "/" successful
ocal site: C:\Users\SWATHY R\Desktop\
Desktop
GRE
MindMap_Shivani
PRINTOUT FOR VISA
Quantum
Report Print
Remote site: /
/
ilename Filesize Filetype Last modified
PRINTOUT FOR ... File folder 29-05-2023...
Quantum File folder 23-06-2023...
Report Print File folder 06-12-2022...
RIT File folder 10-09-2023...
24507805.pdf 191,782 Microsoft E... 07-08-2023...
bobsfile.txt 30 Text Docum... 01-10-2023...
CA3-revision.pdf 184,271 Microsoft E... 26-01-2023...
CA3_DA_E0119... 2,528,... Microsoft ... 18-10-2022...
elected 1 file. Total size: 30 bytes
Filename Filesize Filetype Last mod... Permis... Owner/...
..
bobsfile.txt 30 Text D... 01-10-20...
1 file. Total size: 30 bytes
erver/Local file Dire... Remote file Size Prio... Status

**Step 9 :**

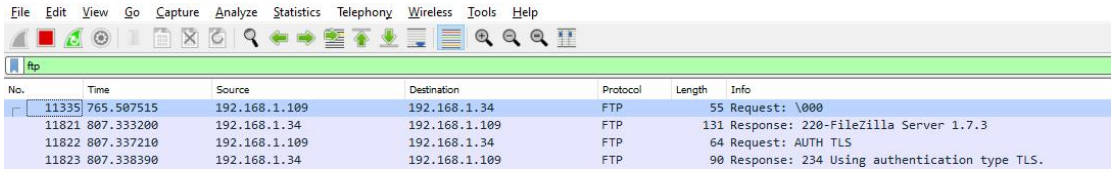

Administration interface - FileZilla Server 1.7.3
Server Window Help
Date/Time Info Type Message
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... PWD
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 257 "/" is current directory.
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... TYPE A
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 200 Type set to A
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... PASV
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 227 Entering Passive Mode (192,168,1,34,219,225)
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... STOR bobsfile.txt
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 150 About to start data transfer.
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 226 Operation successful
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... TYPE I
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 200 Type set to I
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... PASV
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 227 Entering Passive Mode (192,168,1,34,219,226)
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Comma... MLSD
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 150 About to start data transfer.
01-10-2023 00:13:31 FTP Session 4 192.168.1.1... Response 226 Operation successful




File is transferred successfully to the server.

**Step 10 :**

A.

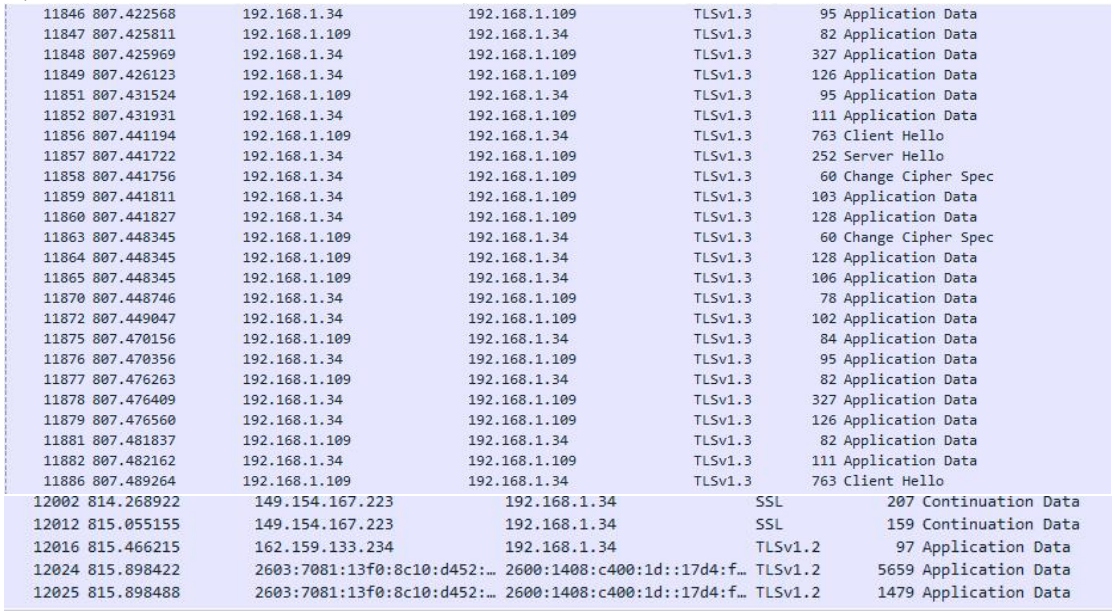



We can see here source is client and transferred to server through FTP protocol

B.


Connection is established.

C,D :




As we can see application data, Cipher spec and client hello and other information has been shared successfully.

Port 21 and 3661 is used by server and client.

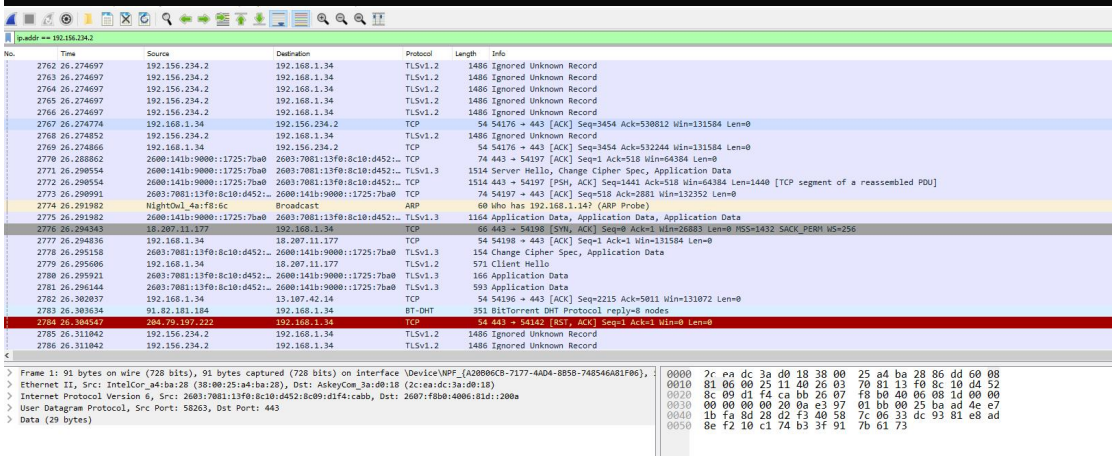
**Step 11 :**

Having port 20 specifically for transferring data raised the security concerns and change of

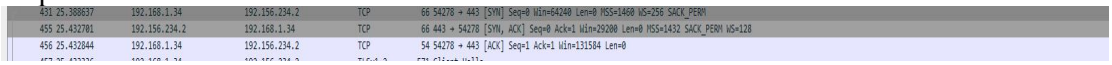
being attacked on that port was higher and the firewall tend to restrict the data and chances of blocking the connection is higher created issues for users to connect to server and data establishment.
Introduction of passive File transfer mode is broadly used now, server can establish a dynamic port in this case above we can see 3661 port file transfer by the client. So this dynamic establishment of port is far better and widely used.
Therefore port 20 is no longer used.

**Exercise : 8. 05 :**
**Step 1 :**

```
C:\Users\dinot>ping www.flcc.edu

Pinging www.flcc.edu [192.156.234.2] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.156.234.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\dinot>_
```

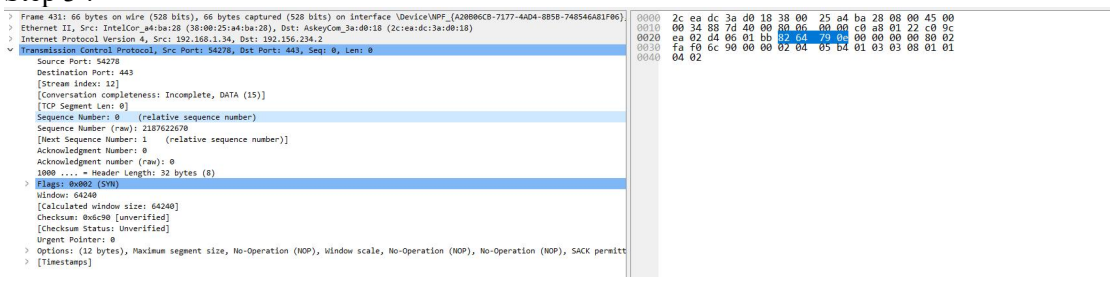



Step : 2




First step it is [SYN] flag and second step [SYN] flag with [ACK] acknowledgement, and final step is [ACK]
These are three flags for three way handshake

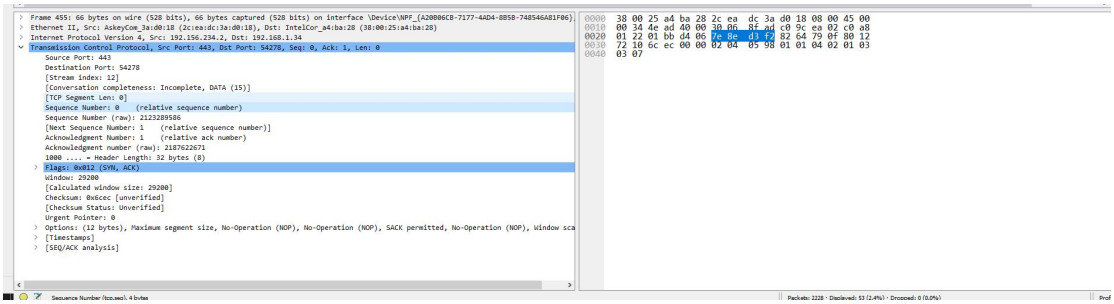
Step 3 :




Sequence is 0 and HEX values are 82 64 79 0e

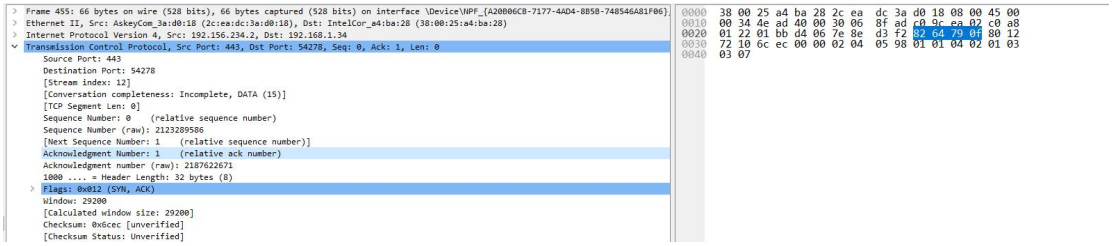
**Step 4 :**

A.



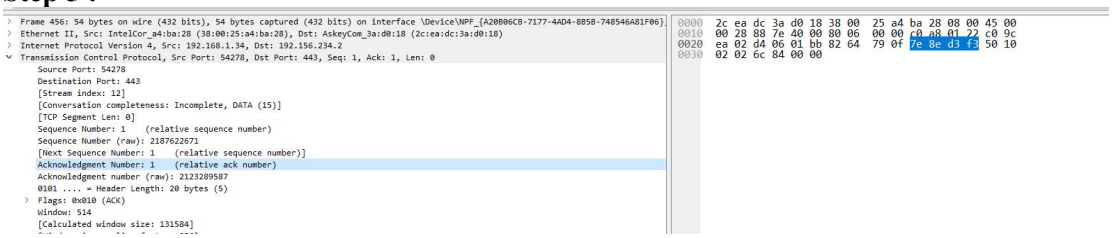

Hex value is 7e 8e d3 f2

B.




Acknoledgement number is 82 64 79 0f
Yes it is 0e + 1 = 0f from step 3.

**Step 5 :**




Acknowledgement hex value is 7e 8e d3 f3
F2 + 1 = f3

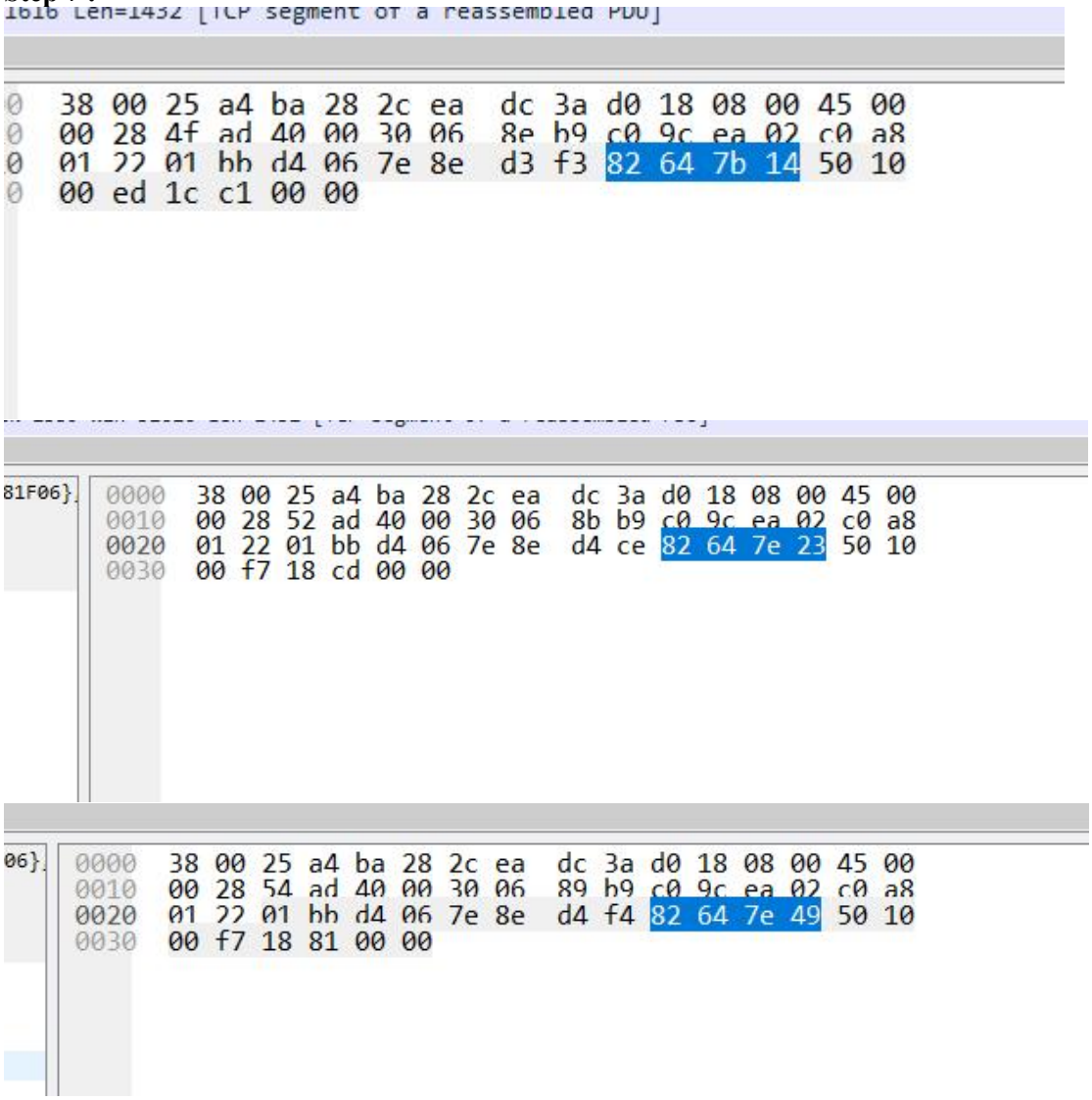
Step 6 :
Four number in Hex
SYN = 82 64 79 0e (Acknowledgment number ), 7e 8e d3 f2 (Sequence Number)
SYN, ACK = 82 64 79 0f
ACK = 7e 8e d3 f3 ( Acknowledgement number )

X = 82 64 79 0e
X+1 = 82 64 79 0f

Y = 7e 8e d3 f2
Y+1 = 7e 8e d3 f3

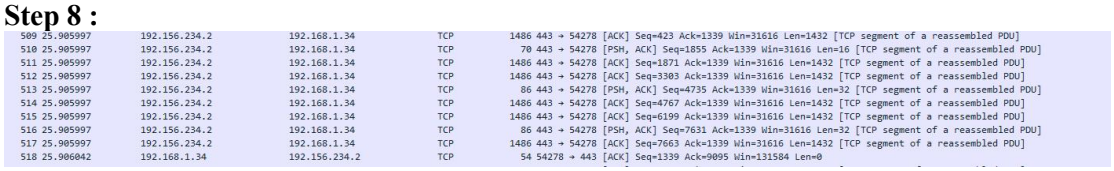
It show cases the three way handshake happened.

**Step 7 :**

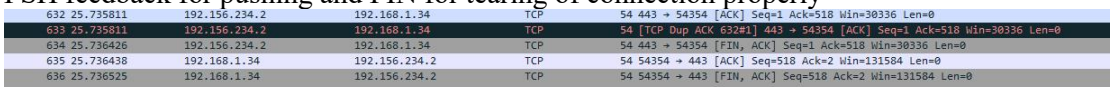



Series of acknowledgement from TCP handshakes.

**Step 8 :**




PSH feedback for pushing and FIN for tearing of connection properly




**Lab Analysis :**

1. I think both protocols has its pros and cons. TCP is like formal connection and UDP behaves informally but both serves their purpose based on the scenarios and they are used accordingly.

TCP establishes the Handshake three way before sending the packets to cross check, so that the frames won't go missing in the connection makes it reliable connection and ends with FIN acknowledgement.

Whereas UDP is connectionless, it works with independent frames they have less overhead and used for streaming services and DHCP and DNS etc. Frames may reach and some may not does not affect the application. This is ensure the safety of the service and UDP sometimes seems to be better for some applications.
So it depends on the application we are using which will determine the protocol accordingly.

2. Logical ports are like tap of water in house, we can lot of taps when we want particular tap to give water we will open so similarly when FTP server is tranferring data to client it uses port 21 and it opens it in client machine, whereas DNS will open 53 while it server communicate with client. This is how it works.
Whereas firewall can't be close or open they just filter the ports neither stop them or push them.

3. TCP handshake is main process for TCP to properly establish the connection between A and B. Three handshakes are :
I. SYN
II. SYN, ACK
III. ACK

First the client will send the request to server and server gives back as ack and client sends the request again and finally server sends the ack to establish the proper connection .
This is how the three way handshake starts in TCP protocol.

4. ICMP protocol which gives echos and waits for replies to give all the details through pinging the other system.

**Key Term Quiz :**
**1. Netstat -b**
**2. TCP and UDP , ICMP and IGMP**
**3. SMTP for sending and IMAP for receiving**
**4. Apache HTTP server**
**5. PORT 21**