WIRESHARK

Res. Asst. Melek ŞENTÜRK

TELNET

Telnet (Teletype Network) is a network protocol used to connect to a remote server or device.

It allows users to access a server through the command line and perform operations on that server.

TELNET FEATURES

Provides Remote Access → The user can connect to a remote computer and execute commands via the terminal.

Works Over TCP/IP → Telnet communicates by default on port 23 using the TCP protocol.

Text-Based → All operations are performed through the command-line interface (CLI).

TELNET INSTALLATION

Check if Telnet is installed. Open CMD and run the "telnet" command. If the Telnet interface appears, it means it is installed. If it is not installed,

For Windows -> Open CMD or PowerShell as Administrator and enter the following command.

```
PS C:\WINDOWS\system32> dism /online /Enable-Feature /FeatureName:TelnetClient

Deployment Image Servicing and Management tool
Version: 10.0.19041.3636

Image Version: 10.0.19045.5487

Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.
PS C:\WINDOWS\system32>
```

TELNET INSTALLATION

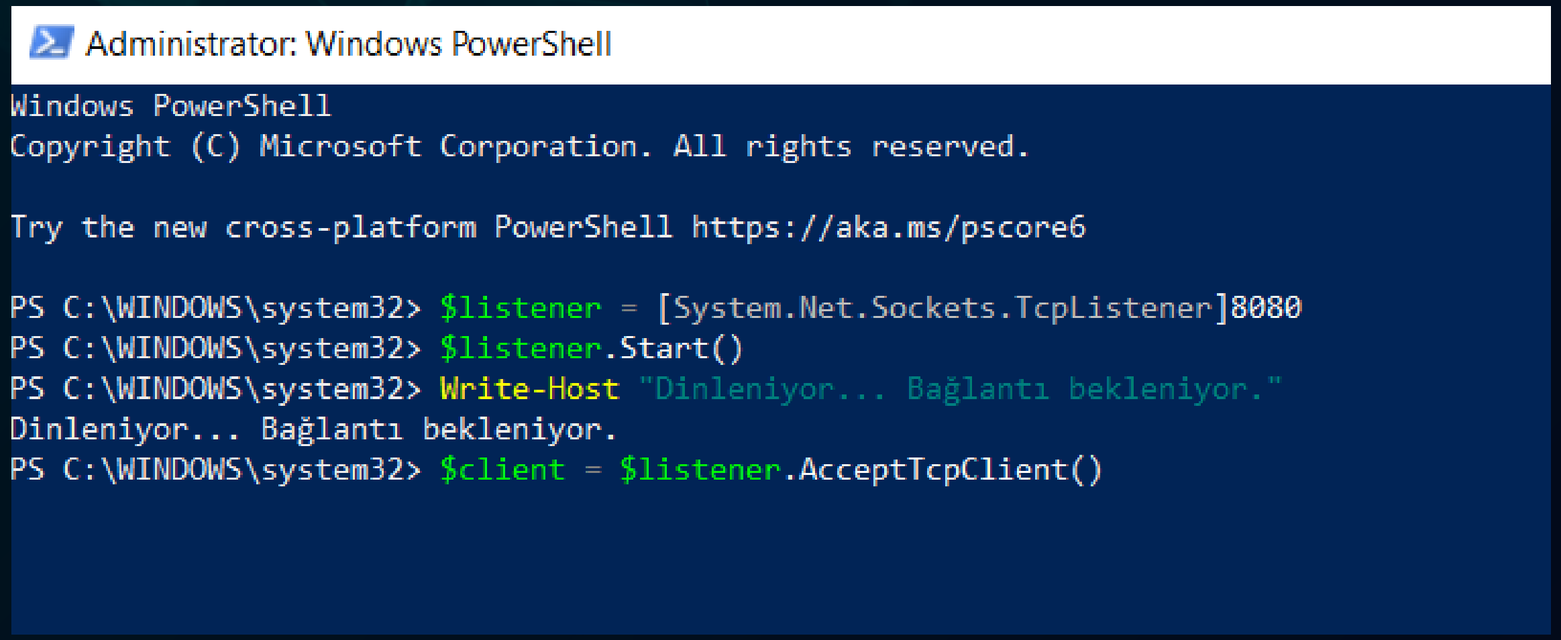
Check if Telnet is installed. If it is not installed,

For LINUX;

-> sudo apt update
-> sudo apt install telnet -y

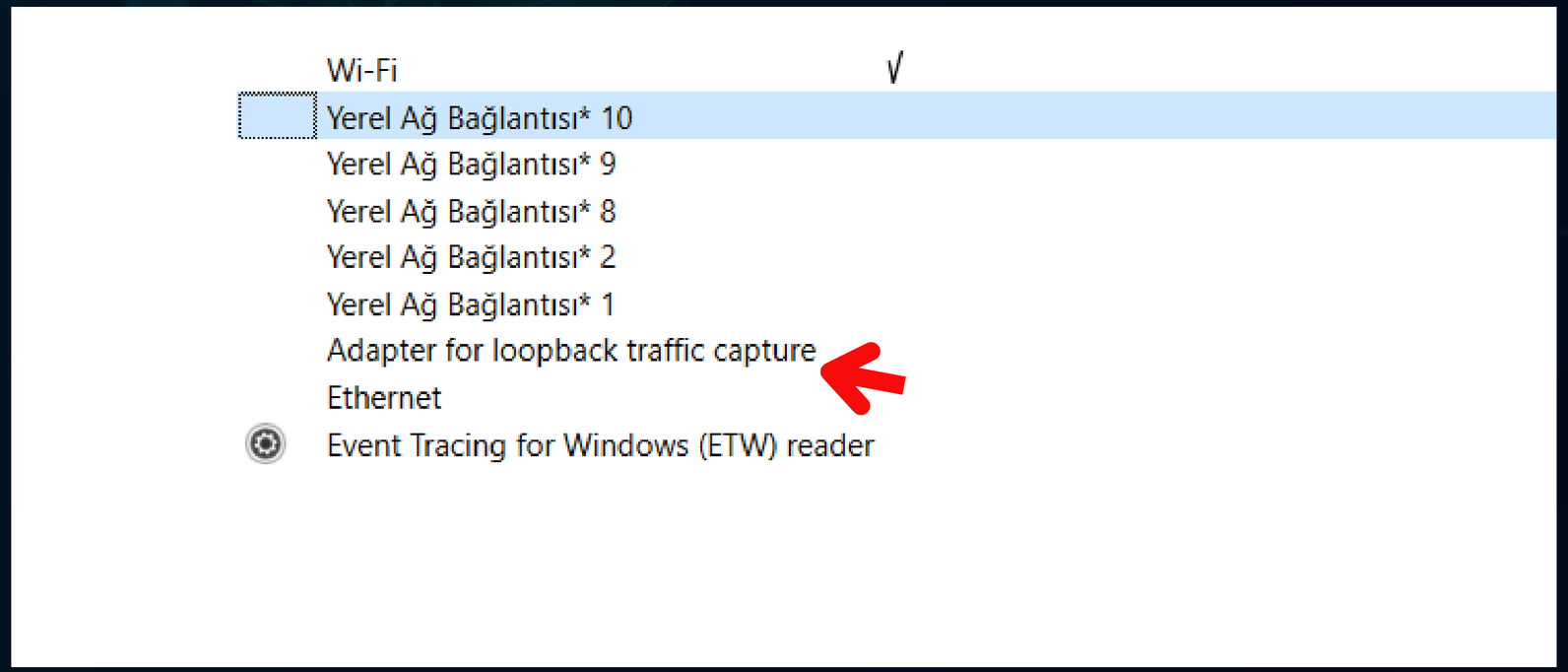
A SERVER ON LOCALHOST

We are creating a listener on port 8080 on localhost.



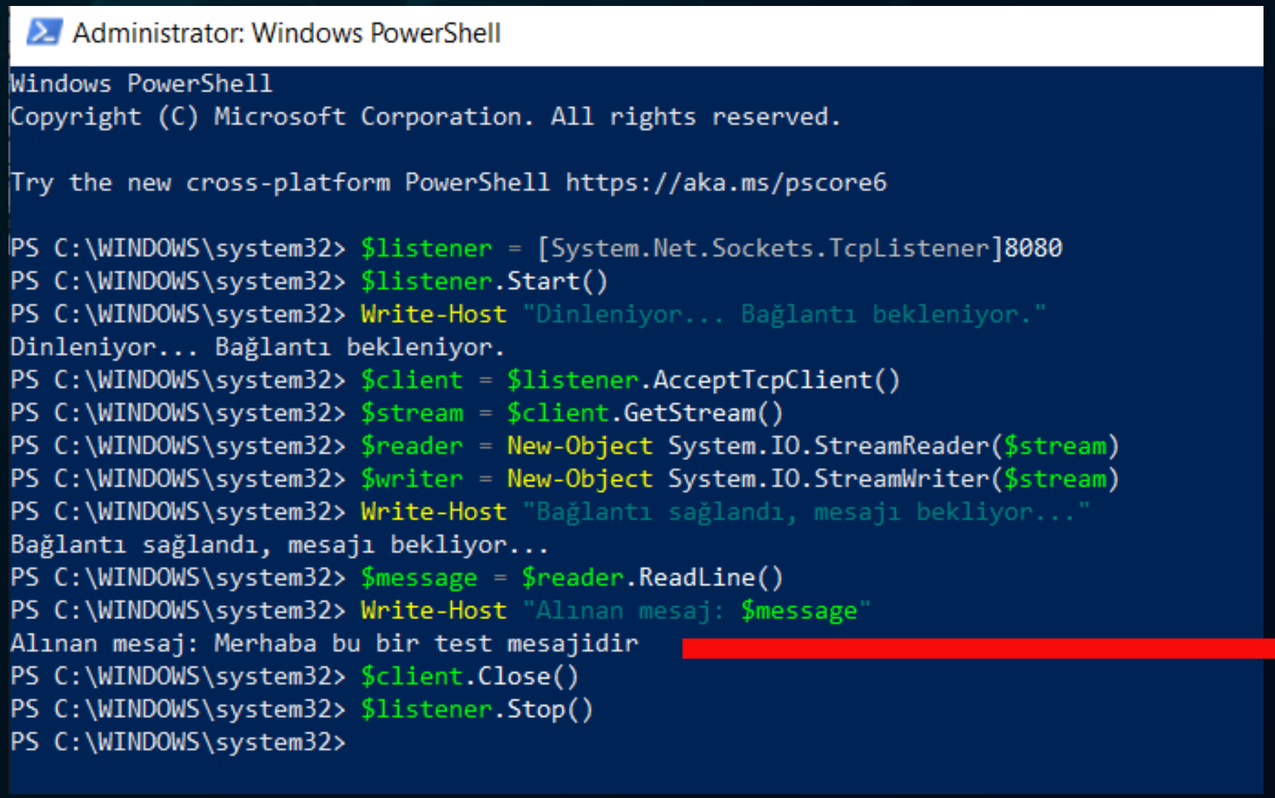
WIRESHARK SIDE

After starting the server, we activate Wireshark before connecting via Telnet and sending a message. Since packets will be transmitted on the local localhost, we select "loopback traffic."



CONNECTING TO THE SERVER WITH TELNET

To connect to the server with Telnet, open a CMD and enter the command "telnet 127.0.0.1 8080". Then, type a message in the same CMD window and press Enter.



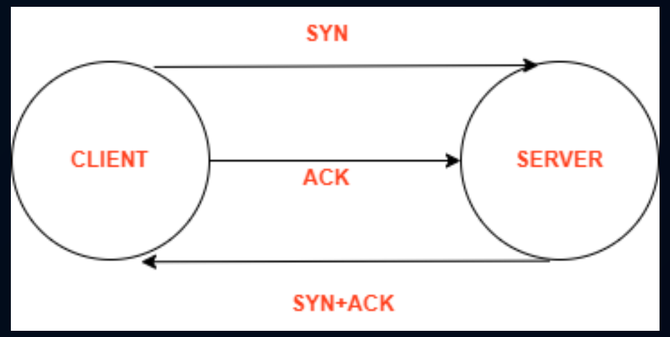
After sending the message, we can see the message received on the server side.

PACKET ANALYSIS (WIRESHARK)

On Wireshark, we can filter by using "tcp.port == 8080". (We specified port 8080 when creating the server initially, but we could have used any available port.)

127.0.0.1	127.0.0.1	TCP	56 50419 → 8080 [SYN] Seq=0 Win=6
127.0.0.1	127.0.0.1	TCP	56 8080 → 50419 [SYN, ACK] Seq=0
127.0.0.1	127.0.0.1	TCP	44 50419 → 8080 [ACK] Seq=1 Ack=1

Since we started a TCP server on localhost, we can see that a TCP connection is established before any data exchange occurs.



PACKET ANALYSIS (WIRESHARK)

127.0.0.1	127.0.0.1	TCP	45 50419 → 8080 [PSH, ACK] Se
127.0.0.1	127.0.0.1	TCP	44 8080 → 50419 [ACK] Seq=1 A
127.0.0.1	127.0.0.1	TCP	45 50419 → 8080 [PSH, ACK] Se
127.0.0.1	127.0.0.1	TCP	44 8080 → 50419 [ACK] Seq=1 A
127.0.0.1	127.0.0.1	TCP	45 50419 → 8080 [PSH, ACK] Se
127.0.0.1	127.0.0.1	TCP	44 8080 → 50419 [ACK] Seq=1 A
127.0.0.1	127.0.0.1	TCP	45 50419 → 8080 [PSH, ACK] Se

As seen, the client sends a TCP packet containing PSH+ACK to the server. PSH is a flag that tells the server to deliver the data immediately to the application layer. ACK indicates that the previous data has been received and that the system is ready for the next data.

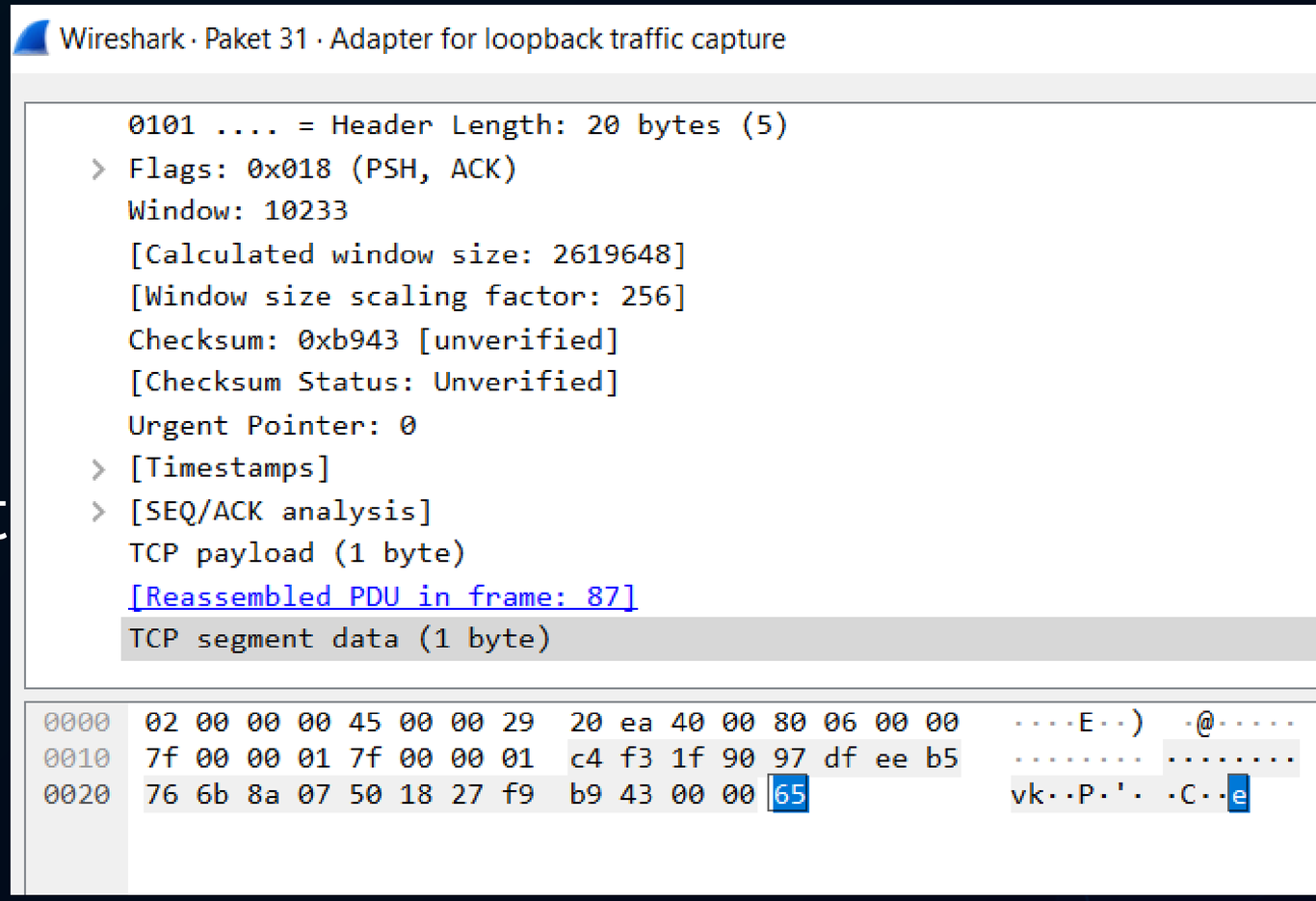
The server sends an ACK packet to indicate that it has received the data. The process continues until all the content is transmitted.

PACKET ANALYSIS (WIRESHARK)

127.0.0.1	127.0.0.1	TCP	45	50419 → 8080 [PSH, ACK] Se

When we look at the content of the second packet, we can see that the transmitted data is the letter "e".

The reason the sent text is transmitted letter by letter is that Telnet operates on a character-based system. This means user inputs are sent to the server in real-time.



PACKET ANALYSIS (WIRESHARK)

TCP	44 8080 → 50419 [FIN, ACK] Seq=1 Ack=32 Win=2619648 Len=0
TCP	44 50419 → 8080 [ACK] Seq=32 Ack=2 Win=2619648 Len=0
TCP	44 50419 → 8080 [FIN, ACK] Seq=32 Ack=2 Win=2619648 Len=0
TCP	44 8080 → 50419 [ACK] Seq=2 Ack=33 Win=2619648 Len=0

After all the data is transmitted, the server sends a FIN+ACK packet to the client to close the connection.

The client confirms receiving the server's FIN+ACK packet with an ACK packet and then sends its own FIN+ACK packet to terminate the connection.

Finally, the server sends an ACK packet to indicate that it has received the client's packet, and the TCP connection is terminated.

To observe the progression of packets over time, I/O graphs can be analyzed.