# WIRESHARK

Res. Asst. Melek ŞENTÜRK

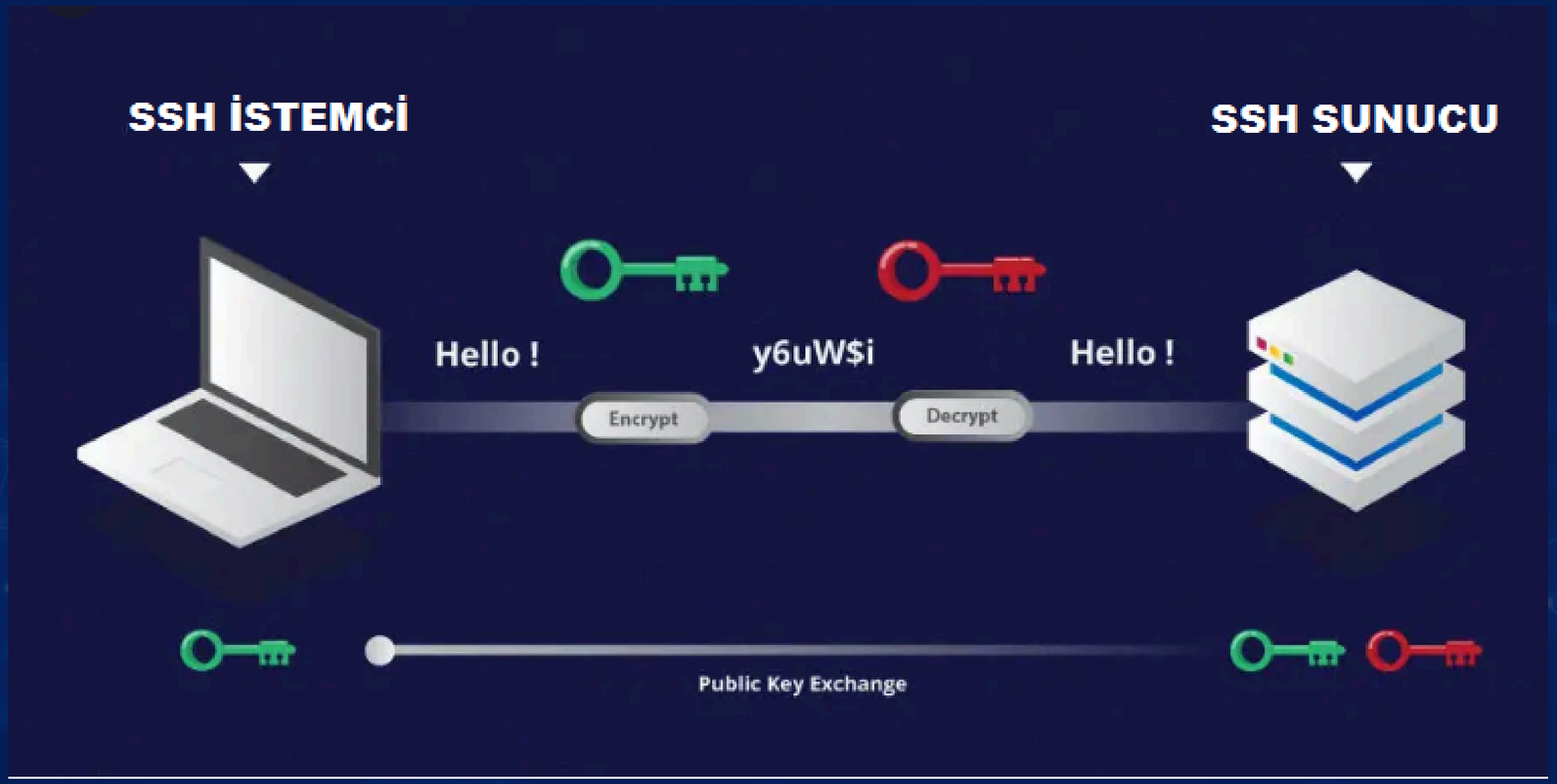
# SSH (SECURE SHELL)

SSH is a protocol used to securely connect to and manage a remote device (server) over a secure network.

It is widely used, especially on Linux and Unix-based systems, and ensures secure data transmission through encryption.

It creates an encrypted communication channel, preventing plaintext data from being intercepted by malicious actors.

# SSH (SECURE SHELL)



# USE CASES

SSH allows the client computer to connect to an SSH server. Through this connection, the user can send commands to the server and manage it.

It supports protocols such as SCP (Secure Copy Protocol) and SFTP (SSH File Transfer Protocol) for file transfer.

It has the ability to route data through a secure tunnel. This is used to establish secure connections over untrusted networks or to run specific services through an encrypted channel.

# USE CASES

It supports both password-based authentication and key-based authentication methods.

SSH is used not only for computers but also for network devices (such as routers, switches, and firewalls).

# HOW DOES IT WORK?

SSH operates on a client-server architecture and establishes a secure connection between the client and the server.

**Connection Initiation:** The SSH client sends a request to connect to the server.

**Authentication:** The user is authenticated with a password or SSH keys.

**Selection of Encryption Algorithms:** The SSH client and server determine the encryption algorithm to be used during the connection.

**Secure Channel Setup:** A secure connection is established between the client and server using the selected encryption method.

**Authentication:** The user is authenticated with a password or SSH keys.

**Communication:** The user can execute commands on the server or transfer files.

# SSH SERVER CHECK

To check if OpenSSH Server is installed, open PowerShell as an administrator;

```
PS C:\WINDOWS\system32> Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*'


Name  : OpenSSH.Client~~~~0.0.1.0
State : Installed

Name  : OpenSSH.Server~~~~0.0.1.0
State : Installed



PS C:\WINDOWS\system32>
```

# SSH SERVER CHECK

If OpenSSH Server is not installed, go to Start Menu → Settings → Apps → Optional Features → Add a feature → OpenSSH Server.

Start → Services (services.msc) → OpenSSH SSH Server → Start.

To verify that it is working;

```
PS C:\WINDOWS\system32> Get-Service sshd

Status   Name               DisplayName
------   ----               -----------
Running  sshd               OpenSSH SSH Server


PS C:\WINDOWS\system32>
```

# CONNECTING WITH SSH

Open CMD or PowerShell;

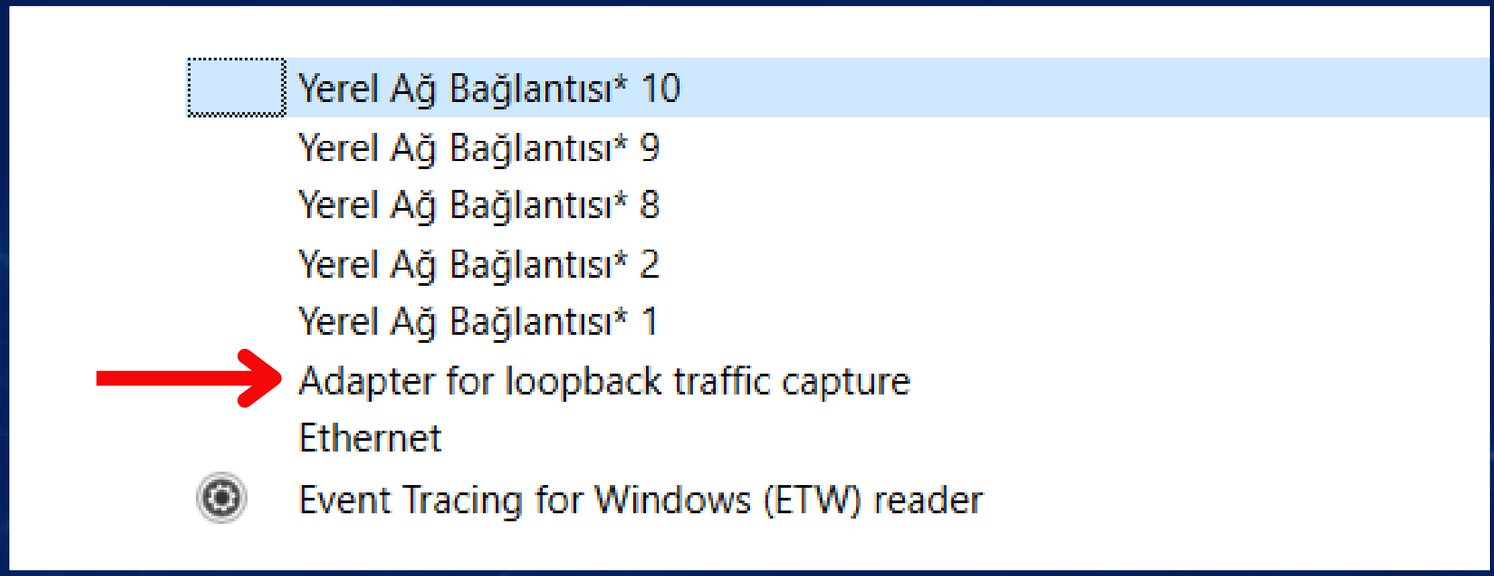
```
C:\Users\Melek>ssh melek@127.0.0.1
melek@127.0.0.1's password:
```

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. Tüm hakları saklıdır.

melek@DESKTOP-KN9BFE4 C:\Users\Melek>
```

# WIRESHARK SIDE

Start Wireshark and proceed with "Loopback".



# SENDING MESSAGES WITH SSH

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. Tüm hakları saklıdır.

melek@DESKTOP-KN9BFE4 C:\Users\Melek>echo "Merhaba, bu bir test mesajıdır!"
"Merhaba, bu bir test mesajıdır!"

melek@DESKTOP-KN9BFE4 C:\Users\Melek>
```

# ANALYSIS THROUGH WIRESHARK

| Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 127.0.0.1 | 127.0.0.1 | SSH | 88 | Client: Encrypted packet (len=44) |
| 127.0.0.1 | 127.0.0.1 | TCP | 44 | 22 → 50448 [ACK] Seq=1 Ack=45 Win=10225 Len=0 |
| 127.0.0.1 | 127.0.0.1 | SSH | 88 | Server: Encrypted packet (len=44) |
| 127.0.0.1 | 127.0.0.1 | TCP | 44 | 50448 → 22 [ACK] Seq=45 Ack=45 Win=10221 Len=0 |
| 127.0.0.1 | 127.0.0.1 | SSH | 292 | Client: Encrypted packet (len=248) |
| 127.0.0.1 | 127.0.0.1 | TCP | 44 | 22 → 50448 [ACK] Seq=45 Ack=293 Win=10224 Len=0 |
| 127.0.0.1 | 127.0.0.1 | SSH | 80 | Server: Encrypted packet (len=36) |
| 127.0.0.1 | 127.0.0.1 | TCP | 44 | 50448 → 22 [ACK] Seq=293 Ack=81 Win=10221 Len=0 |
| 127.0.0.1 | 127.0.0.1 | SSH | 120 | Server: Encrypted packet (len=76) |
| 127.0.0.1 | 127.0.0.1 | TCP | 44 | 50448 → 22 [ACK] Seq=293 Ack=157 Win=10220 Len=0 |
| 127.0.0.1 | 127.0.0.1 | SSH | 168 | Server: Encrypted packet (len=124) |
| 127.0.0.1 | 127.0.0.1 | TCP | 44 | 50448 → 22 [ACK] Seq=293 Ack=281 Win=10220 Len=0 |
| 127.0.0.1 | 127.0.0.1 | SSH | 80 | Client: Encrypted packet (len=36) |

# ANALYSIS THROUGH WIRESHARK