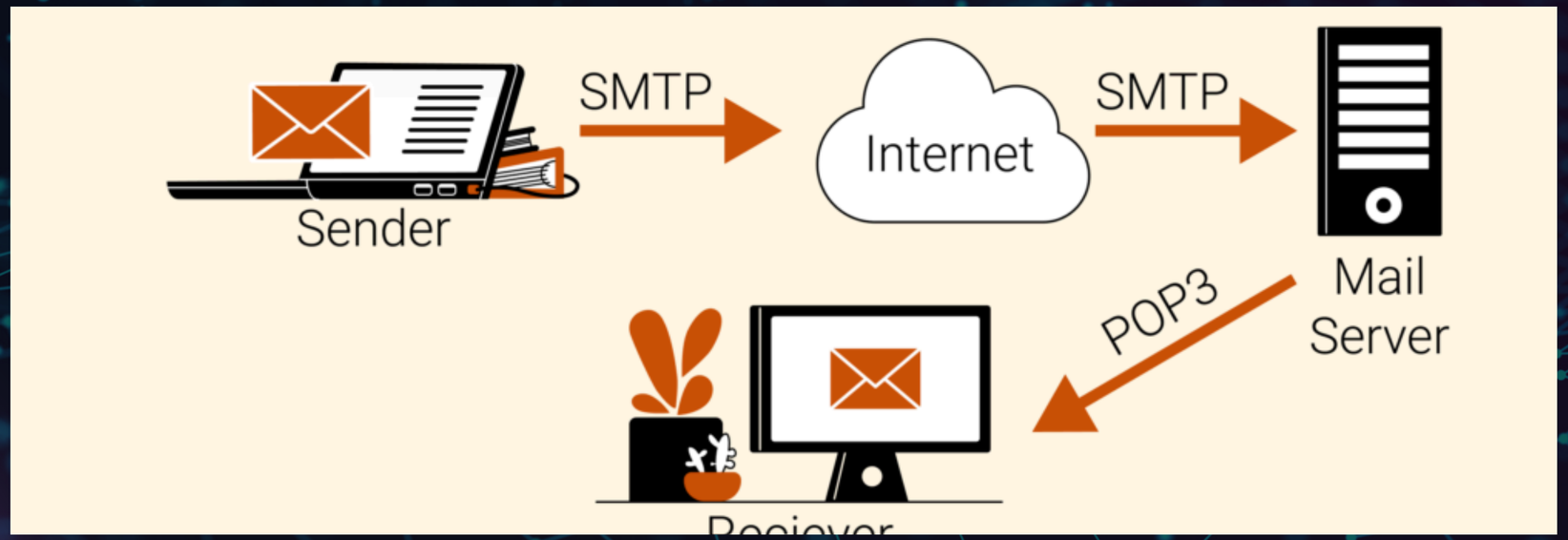
WIRESHARK

Res. Asst. Melek ŞENTÜRK

HOW DOES EMAIL WORK?

- The email system works between the sender, the server, and the receiver.
  - There are two main processes:
    - Send email
    - Receiving email



- For SMTP sending
- To get POP

SMTP (Simple Mail Transfer Protocol) – Sender Protocol

- Purpose: To send email.
  - From User → To Sender Mail Server
  - From Server → To Recipient's mail server
- How Does It Work?
  - The user writes an email and presses the "Send" button.
  - SMTP sends this email to the sending mail server.
  - If the recipient's mail server is different, SMTP transfers the message to that server.
- **Port Numbers:**
  - 25 (default)
  - 587 (encrypted transmission)

POP (Post Office Protocol) – Recipient Protocol

- **Purpose:** Downloads emails from the server to the recipient's device.
  - Most used version: POP3
- **How Does It Work?**
  - The user opens the email client (Outlook, Thunderbird, etc.).
  - POP3 connects to the server and downloads all emails.
  - By default, emails are deleted from the server (but this can be adjusted).
- **Port Numbers:**
  - 110 (default)
  - 995 (with SSL)

SMTP-POP COMPARISON

Özellik	SMTP	POP
Görev	E-posta **göndermek**	E-posta **almak**
Yönü	İstemci → Sunucu	Sunucu → İstemci
Port	25 / 587 / 465	110 / 995
Erişim	Sadece iletim	İndirme ve saklama
Sunucu Durumu	Giden kutusu	Gelen kutusu

An Email Journey

- The sender writes an e-mail and presses the Send button. (SMTP is enabled)
- Mail is forwarded from the Sender's server to the Receiver's server.
- The recipient turns on her computer, her email client connects via POP protocol.
- The mail from the server is downloaded to the Recipient's device.

IMAP (Internet Message Access Protocol)

- IMAP has evolved as an alternative to POP and offers more features.
- How Does It Work?
  - **Connect to email server:** User opens email client (Outlook, Apple Mail, etc.).
  - **Emails remain on the server:** IMAP ensures that emails remain on the server. This means that emails cannot be downloaded, only read.
  - **Synchronization:** If a user performs an action on one device (for example, reads or deletes an email), this action is synchronized across the other devices.
  - **More control:** User can create email folders and move messages into these folders.

SMTP and POP Server Setup and Email Sending with Python

- SMTP Server allows us to send emails. We create an SMTP server using Python. We run the python file we created for the SMTP server.

```
PS C:\Users\Melek\Desktop> python smtp.py
```

- POP Server provides email receiving operations. We create a POP server using Python. We start the python file we created for the POP server in a separate Powershell.

```
PS C:\Users\Melek\Desktop> python pop.py
[+] POP3 server listening on port 110...
```

SMTP and POP Server Setup and Email Sending with Python

- Then, we run the Python file we created for sending e-mails on a separate Powershell.

```
PS C:\Users\Melek\Desktop> python mail.py
E-posta başarıyla gönderildi.
```

- Finally, we connect to the POP server to receive the e-mail. To do this, we run the Python file we created via a separate Powershell. And we see the e-mail lists on the server.

```
PS C:\Users\Melek\Desktop> python pop-client.py
STAT sonucu: (3, 882)
LIST sonucu: (b'+OK 3 messages', [b'1 294', b'2 294', b'3 294'], 21)
RETR sonucu: (b'+OK 283 octets', [b'From: melek@example.com', b"To: ['gizem@example.com']", b'Message:', b'From: melek@
xample.com', b'', b'To: gizem@example.com', b'', b'Subject: Selam', b'', b'Content-Type: text/plain; charset="utf-8"',
'', b'Content-Transfer-Encoding: 8bit', b'', b'MIME-Version: 1.0', b'', b'', b'', b'Bu bir test mesaj\xc4\xb1d\xc4\xb1r
 T\xc3\xbcrk\xc3\xa7e karakter i\xc3\xa7erir: \xc4\xb1, \xc3\xa7, \xc5\x9f, \xc3\xbc, \xc3\xb6, \xc4\xb0'], 296)
PS C:\Users\Melek\Desktop>
```

WIRESHARK SIDE

- Since the transactions occur locally, we choose Loopback traffic.

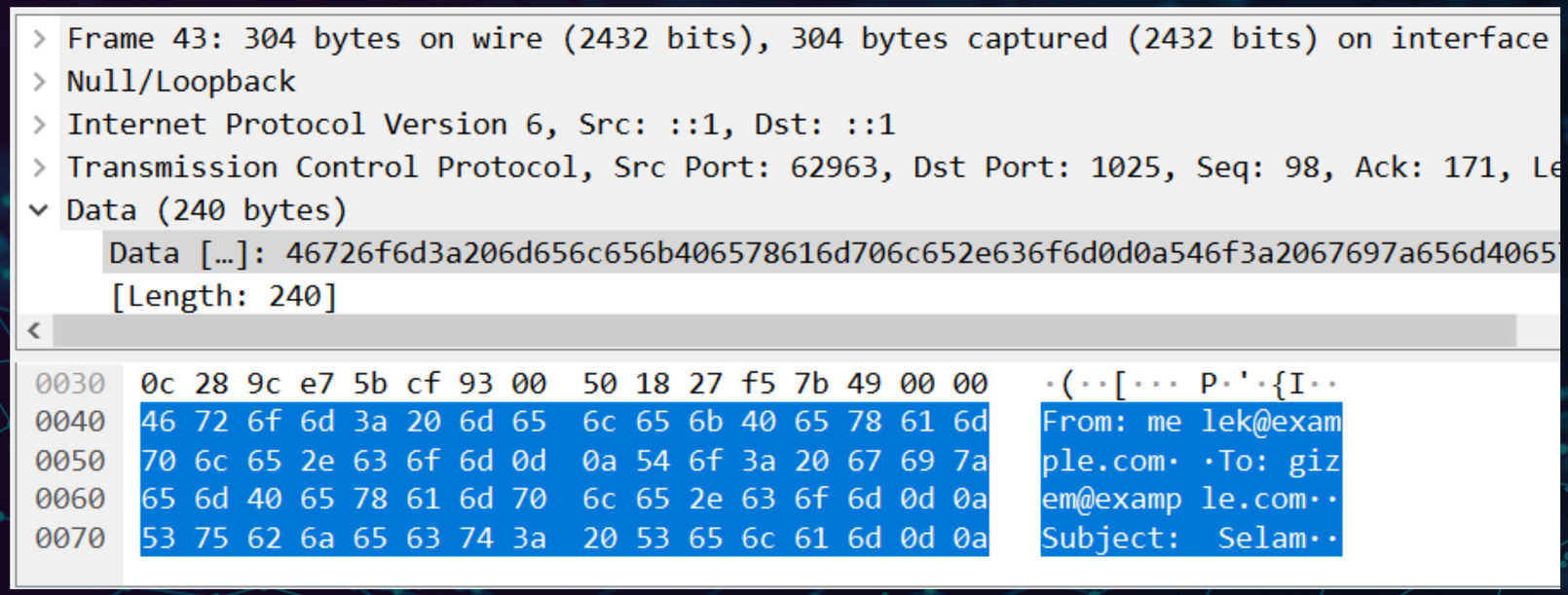
- SMTP requires reliable, sequential and error-free data transfer. Therefore, TCP is used in the transport layer. When we examine it on Wireshark, we see that a TCP connection is first established with the SMTP server.

TCP	76	62960 → 1025 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
TCP	76	1025 → 62960 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
TCP	64	62960 → 1025 [ACK] Seq=1 Ack=1 Win=327168 Len=0

- Data is transmitted in the [PSH+ACK] lines.

WIRESHARK SIDE

- SMTP is unencrypted by default. Additionally, since encryption options are not activated on the client, the mail content appears as follows on Wireshark.



WIRESHARK SIDE

Establishing a TCP connection to the POP server

TCP	56	62967 → 110 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SA
TCP	56	110 → 62967 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=654
TCP	44	62967 → 110 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
POP	67	S: +OK POP3 server ready
TCP	44	62967 → 110 [ACK] Seq=1 Ack=24 Win=2619648 Len=0
POP	55	C: USER test
TCP	44	110 → 62967 [ACK] Seq=24 Ack=12 Win=2619648 Len=0
POP	63	S: +OK User accepted
TCP	44	62967 → 110 [ACK] Seq=12 Ack=43 Win=2619648 Len=0
POP	55	C: PASS 1234
TCP	44	110 → 62967 [ACK] Seq=43 Ack=23 Win=2619648 Len=0
POP	67	S: +OK Password accepted
TCP	44	62967 → 110 [ACK] Seq=23 Ack=66 Win=2619648 Len=0
POP	50	C: STAT
TCP	44	110 → 62967 [ACK] Seq=66 Ack=29 Win=2619648 Len=0
POP	55	S: +OK 2 588
TCP	44	62967 → 110 [ACK] Seq=29 Ack=77 Win=2619648 Len=0
POP	50	C: LIST

He enters his username and password. We can see it because there is no encryption.

It tells you how many emails there are and their size.

WIRESHARK SIDE

- The client receives the mail from the POP server and the connection is terminated. We can see the mail content in the same way because we do not use encryption.