# **Assignment 1:**

# **Logo, company name Description automatically generated**

***Name:*** *Muhammad Rafay Malik , Shehryar Ahmed*

***Roll no:*** *221511 ,221589*

***Course:*** *Digital forensics*

***Course Instructor:*** *Ms. Mehmoona*

***AIR UNIVERSITY***

***DEPARTMENT OF CYBER SECURITY***

**1. Case Overview**

This report presents a comprehensive forensic analysis of email traffic captured via network sniffing tools, focusing on the Simple Mail Transfer Protocol (SMTP). The captured data, provided in .pcap format, was examined using Wireshark to identify potential security risks and trace email transmission details. The goal was to reconstruct email contents, analyze protocol behavior, and identify any security weaknesses such as exposed credentials or unauthorized access.

**2. Objective**

* Analyze and interpret SMTP traffic from the provided .pcap file.
* Reconstruct email content from fragmented packets.
* Decode Base64-encoded credentials.
* Identify key technical details such as ports, IP addresses, MAC addresses, and email clients.
* Highlight vulnerabilities and provide security recommendations.

**3. Protocol Under Investigation: SMTP**

SMTP is an application-layer protocol used to send email messages between servers and clients. By default, it operates on **port 25**, though ports **465** (SMTPS) and **587** (with STARTTLS) are also commonly used.

**Key Characteristics:**

* Operates in plaintext by default.
* Vulnerable to interception without encryption (SSL/TLS).
* Credentials often encoded in Base64 (not encrypted).

**4. Methodology**

**Tools and Techniques Used:**

* **Wireshark:** For capturing and analyzing packet data.
* **Base64 Decoder:** To decode user credentials from SMTP authentication exchanges.
* **TCP Stream Analysis:** For reassembling fragmented email data.
* **Header Inspection:** For extracting metadata including timestamps, source/destination IPs, and MAC addresses.

**Email Traffic Forensics**

Overview

• Simple Mail Transfer Protocol

• Hands-on lab

• A .pcap file contains MS Outlook email traffic

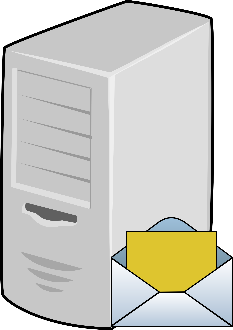
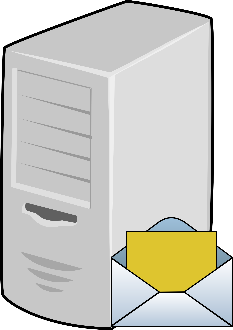
• Assume the traffic is decrease

**Simple Mail Transfer Protocol**

**Simple Mail Transfer Protocol (SMTP)**

• It is a protocol used for sending and receiving email messages over the Internet.

SMTP SMTP IMAP



SMTP (Simple Mail Transfer Protocol): sending emails

IMAP (Internet Access Message Protocol): **download** emails

**Simple Mail Transfer Protocol**

• SMTP operates on port 25 by default, but other ports such as 587 and 465 may also be used.

• SMTP uses a set of commands and responses to transfer email messages between clients and servers.

• SMTP is a plain text protocol

• data transmitted between clients and servers is not encrypted by default.

• SMTPS for secure email transmissions • SMTP over SSL/TLS

• STARTTLS

**SSL/TLS**

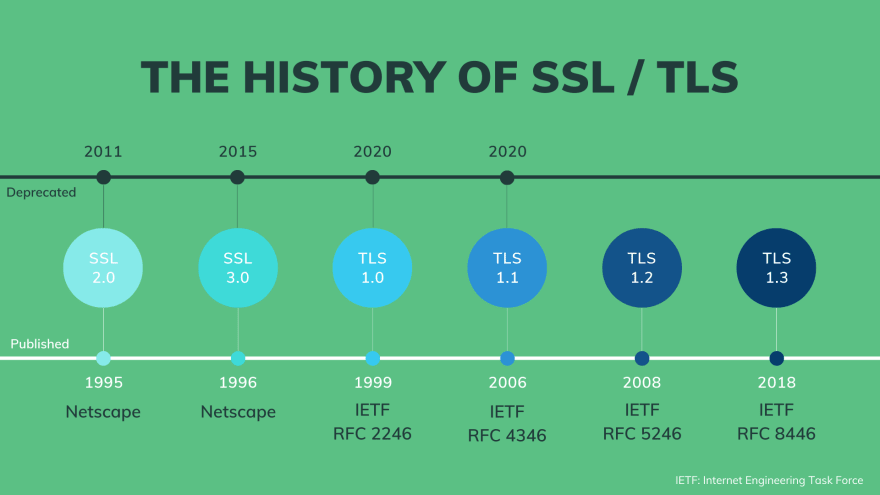
• SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that provide secure communication over the internet.

• SSL is the predecessor to TLS, and is no longer considered secure. • Key security features

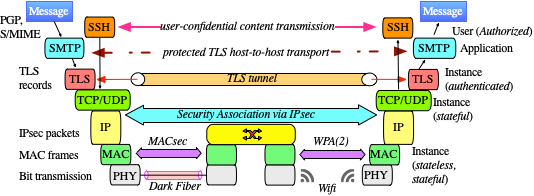
• Authentication: SSL and TLS provide mechanisms for authenticating the identity of the client and server, so that both parties can be sure they are communicating with the intended party.

• Data encryption: SSL and TLS encrypt data transmitted over the internet, so that it cannot be intercepted and read by unauthorized parties.

• Data integrity: SSL and TLS ensure the integrity of data transmitted over the internet, so that it cannot be modified in transit without detection.



https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd

SMTP is an application layer protocol

https://www.fehcom.de/qmail/smtptls.html

**:Forensics:**

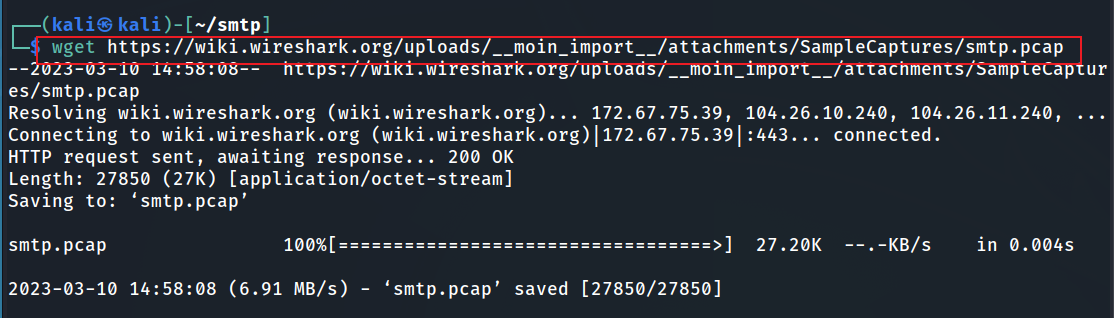
**Time to hunt**

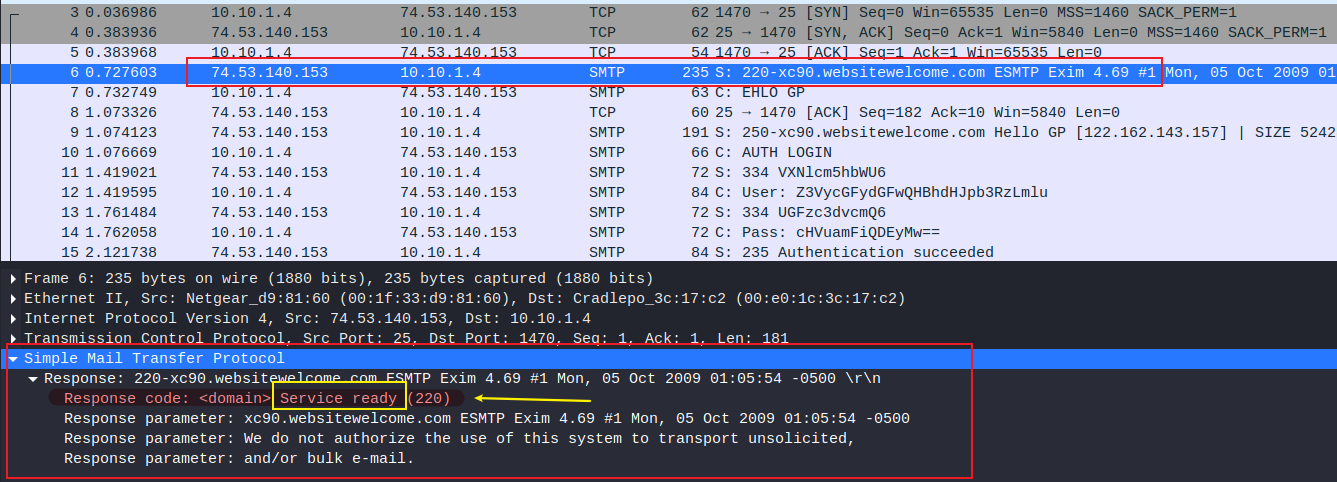
Capture Emails traffic With Wireshark

Lab Files

https://wiki.wireshark.org/SampleCaptures

Download smtp.pcap



SMTP first response “service ready”

indicates that

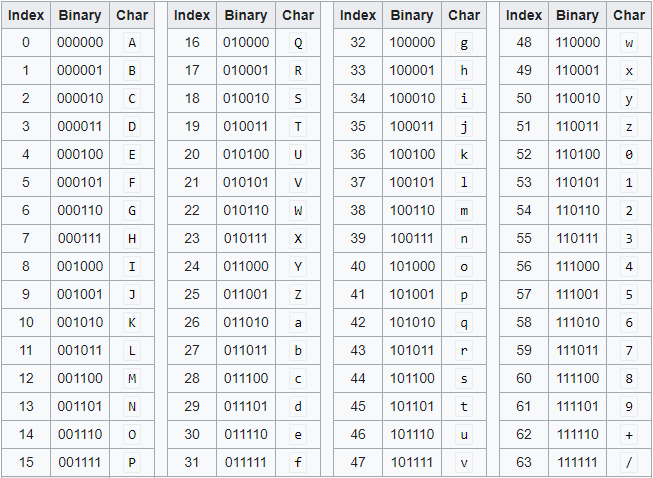
• the device is running an SMTP server and is ready to receive email messages.

• additional information about the server and a warning that the server does not authorize the use of its system to send unsolicited or bulk emails.

Username and password are base64 encoded



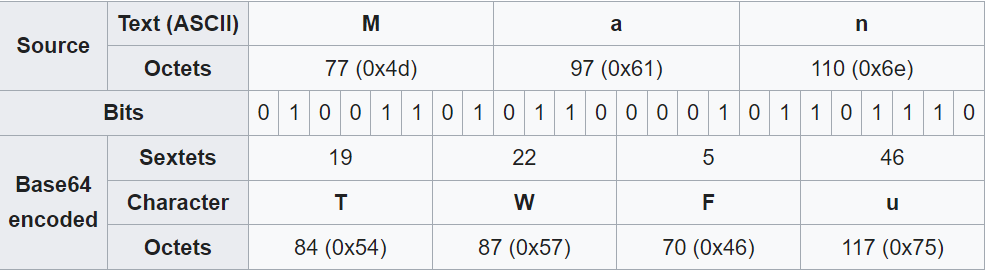
**What is Base64 encoding**

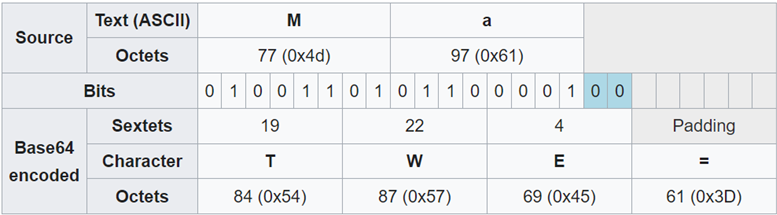
• Base64 encoding is a way to represent binary data in a text format.

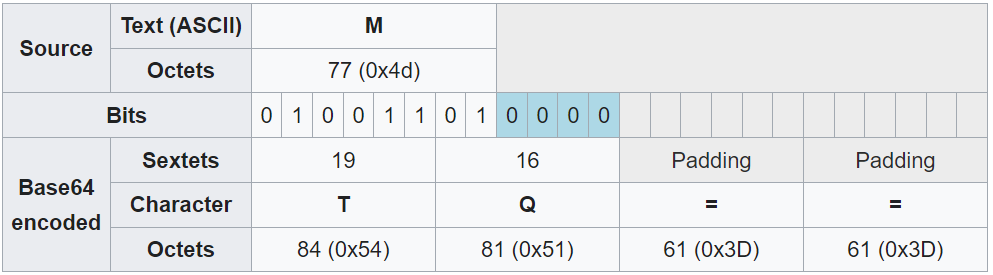
• It is often used in email messages, HTML pages, and other types of text-based communication to transfer binary data such as images, audio files, or other types of non-text data.

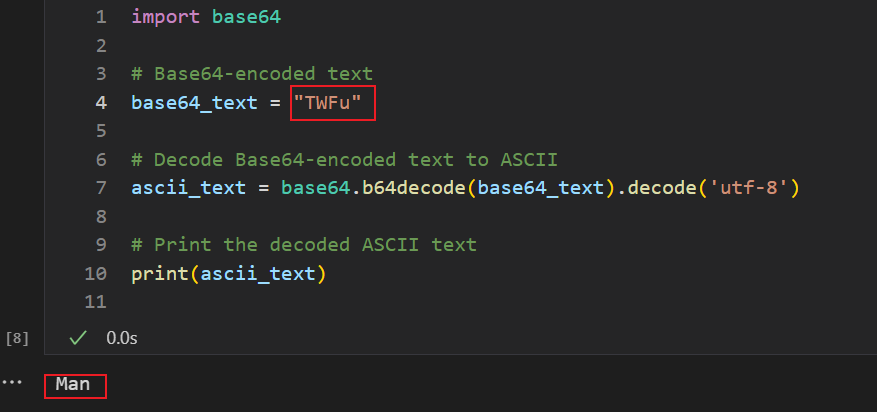
**Conversion**

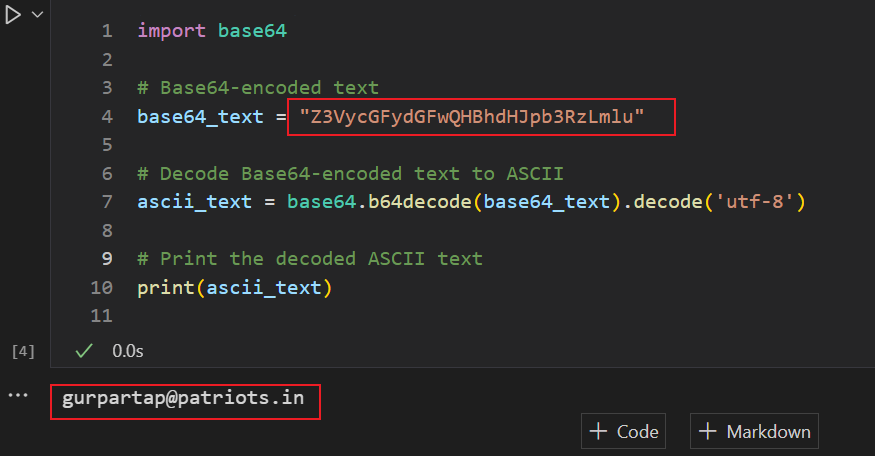


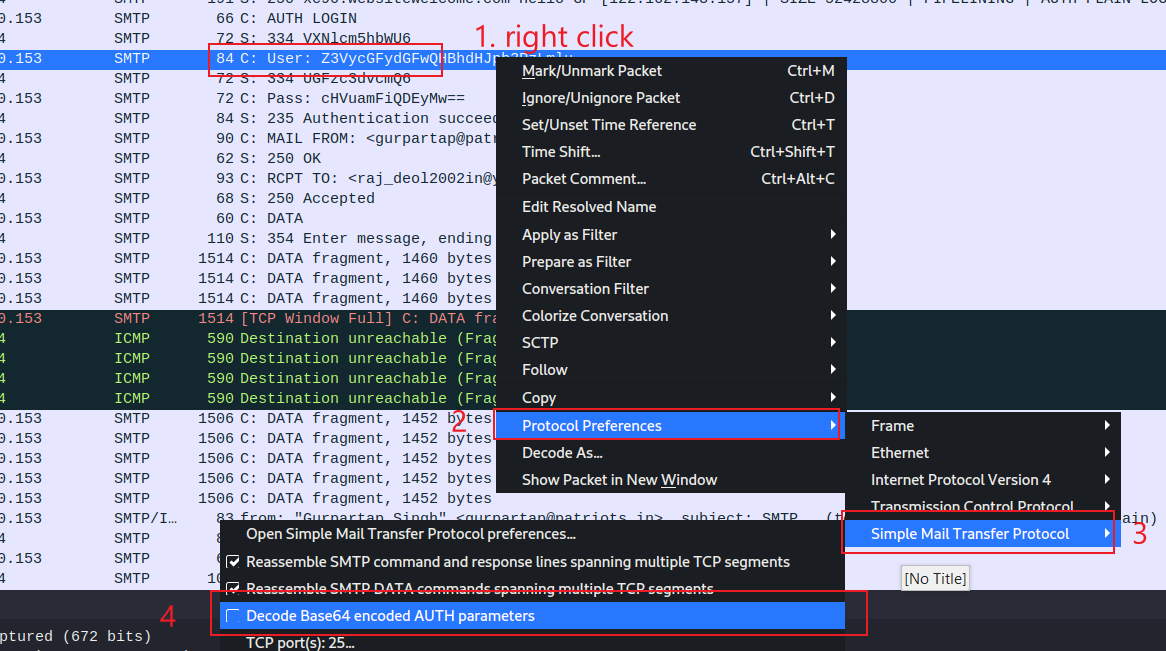


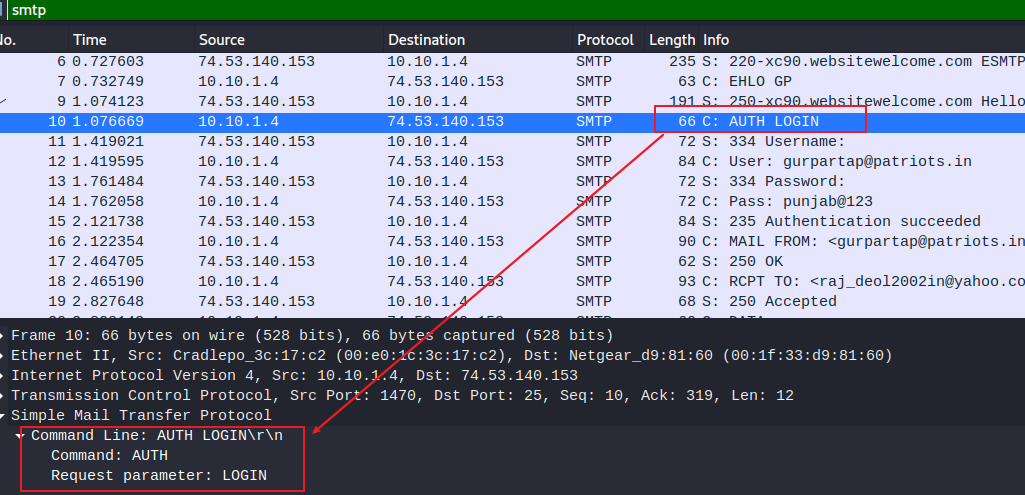


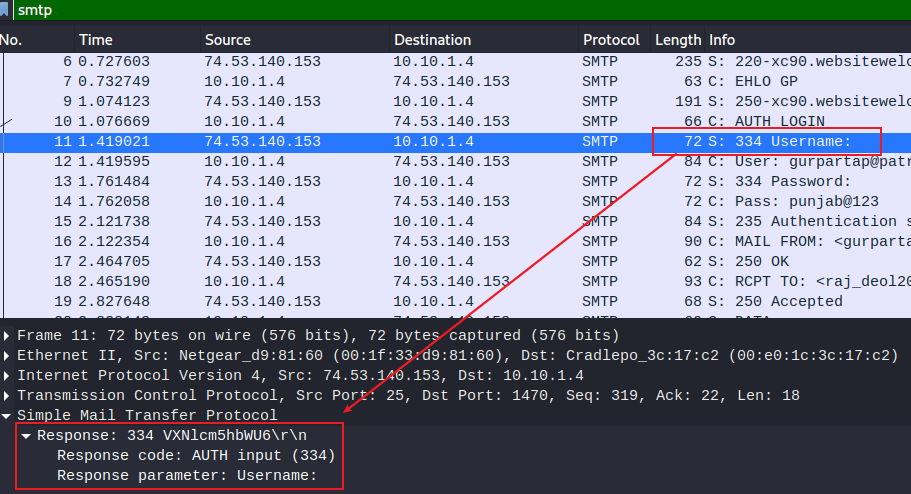


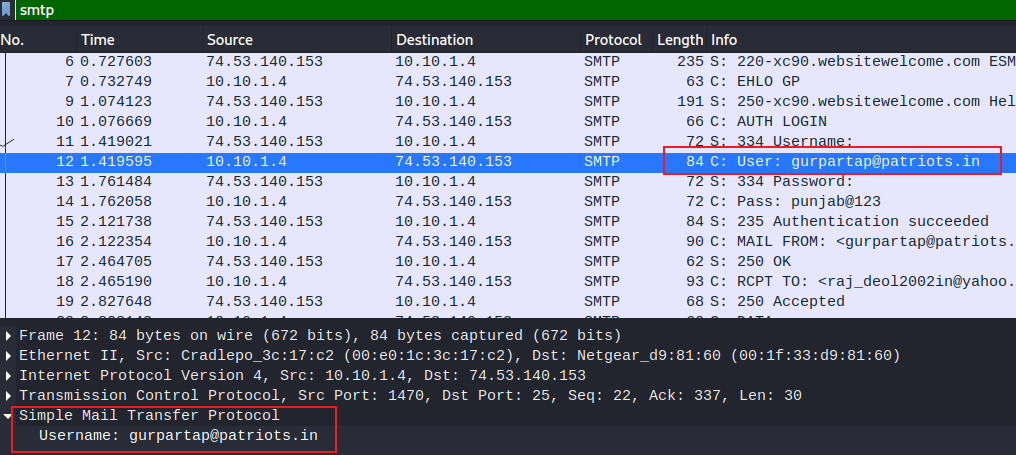
**Decoding Based64 to text**

**Decoding username**

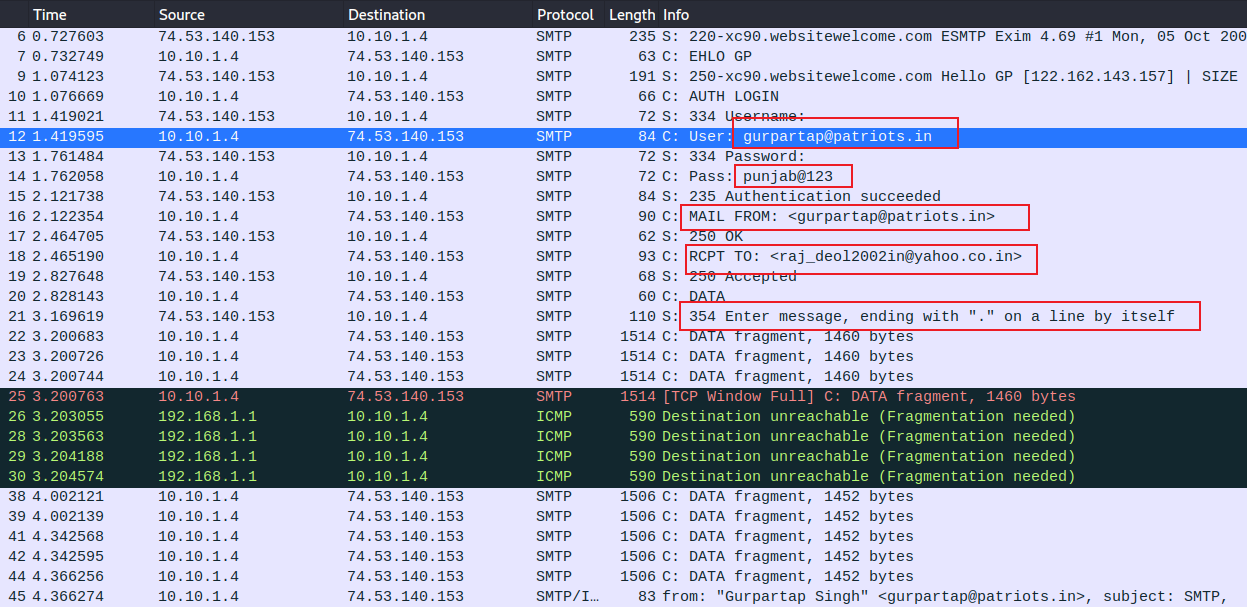




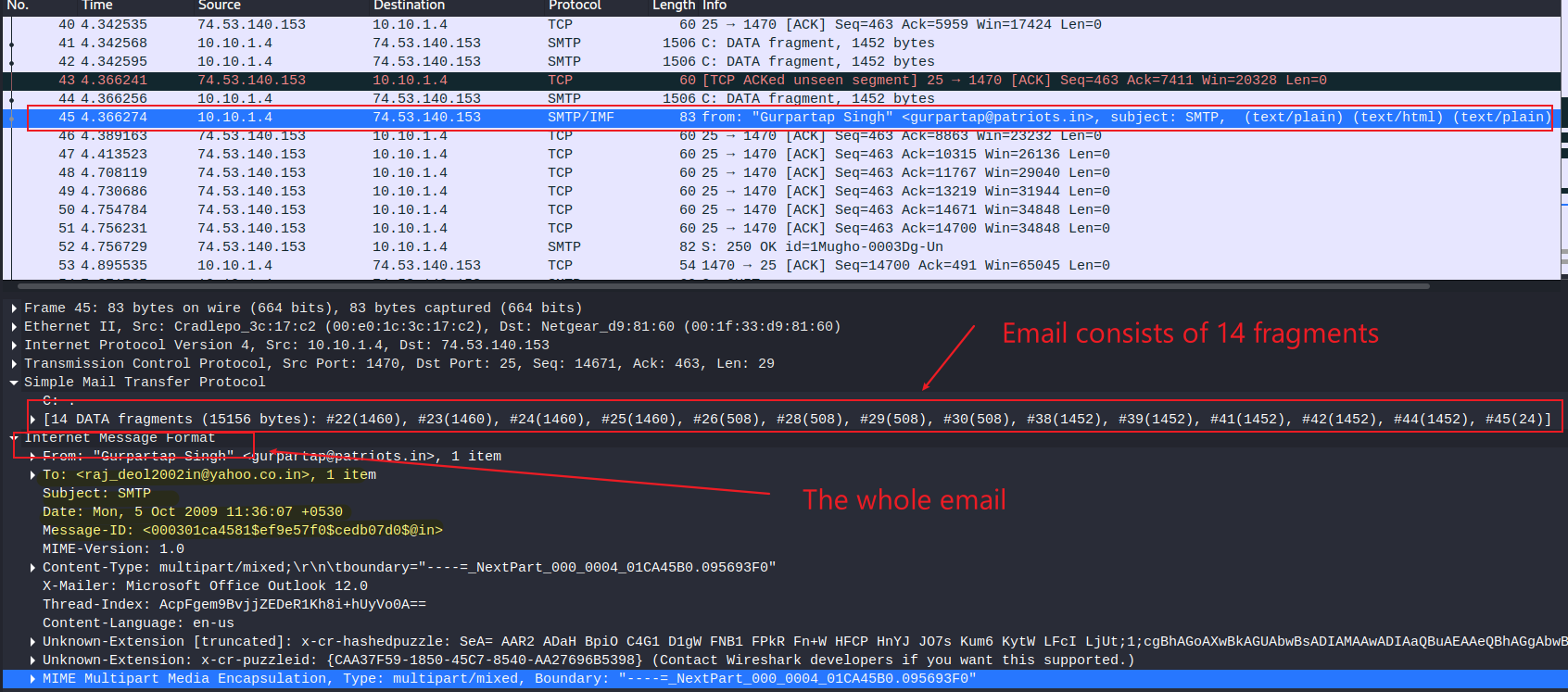




ignore them

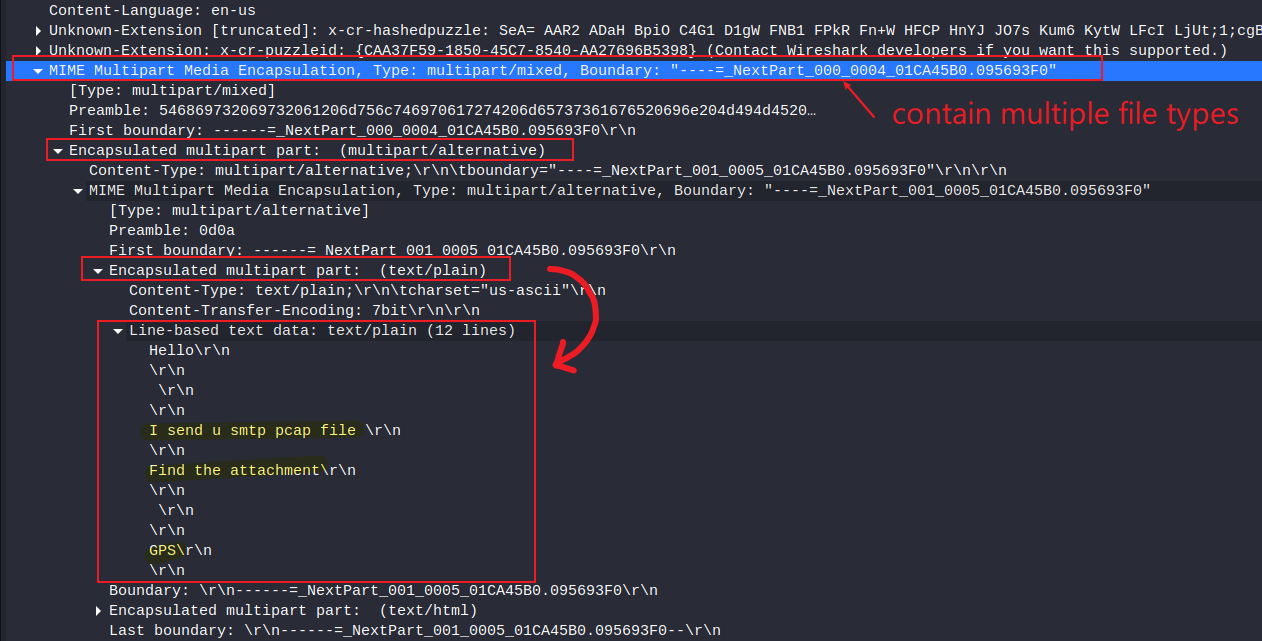


Show email content (14 fragments, Wireshark reassemble them at 45)



email client: office outlook 12.0

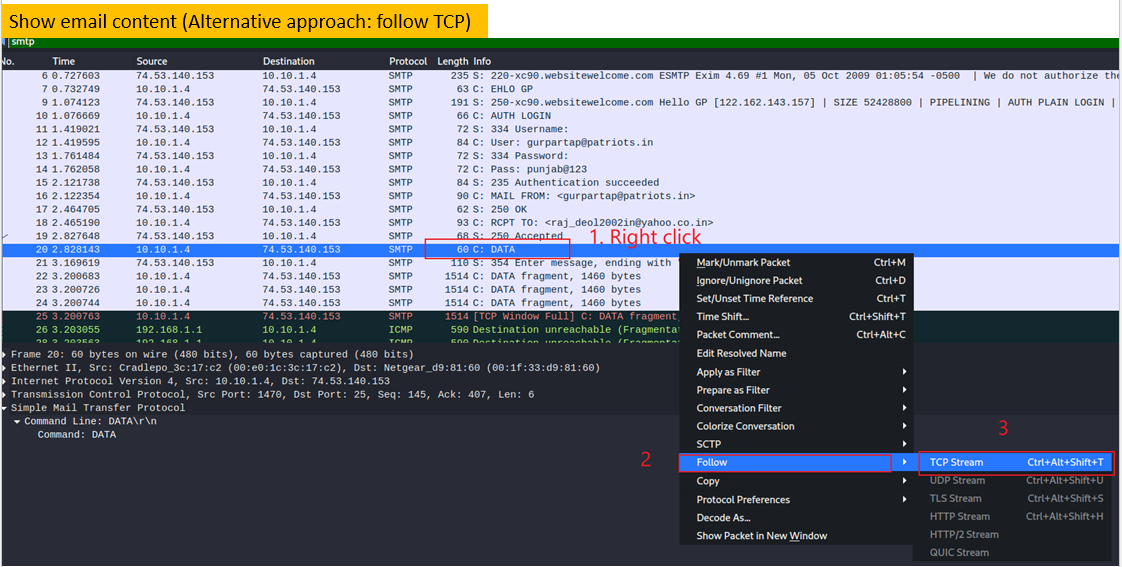
Show email content (text content)

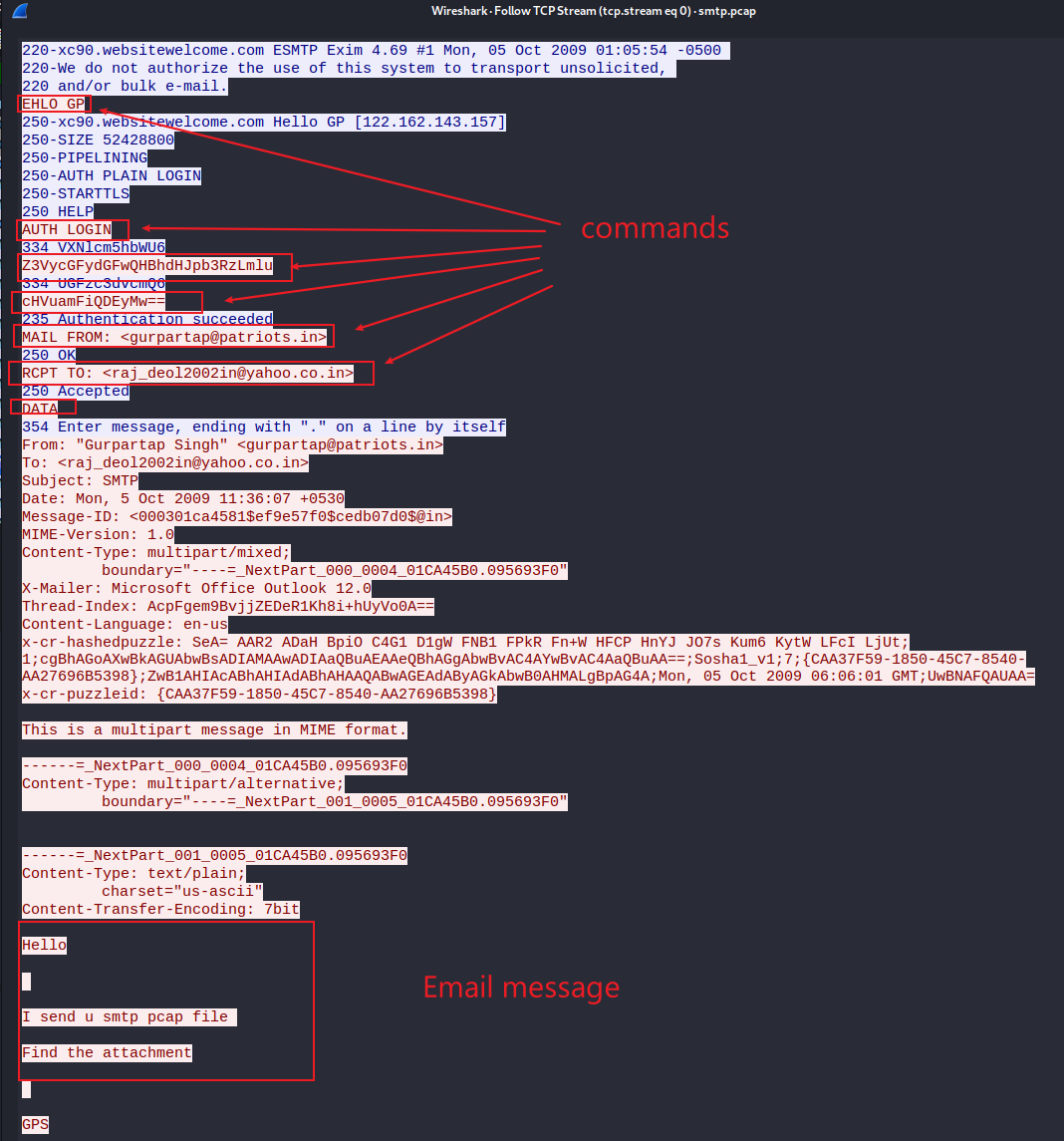


first part



Show email content (Alternative approach: follow TCP)





**5. Forensic Findings**

| **Aspect** | **Details** |
| --- | --- |
| **Email Client** | Microsoft Outlook 12.0 |
| **Timestamps** | Extracted from email headers and packet metadata |
| **SMTP Server Response** | 220 Service Ready indicating server is accepting connections |
| **Authentication** | Base64-encoded username and password captured and decoded |
| **Email Content** | Email reconstructed from 14 TCP fragments; included plain text and HTML |
| **IP Addresses** | Identified for both sender and receiver |
| **MAC Addresses** | Obtained from Ethernet headers |
| **Ports Used** | Port 25 (SMTP), others observed: 465 (SMTPS), 143/993 (IMAP) |

**6. Security Observations**

* **Unencrypted SMTP Traffic:** Credentials were captured in plaintext, enabling easy decoding.
* **Base64 Obfuscation:** Credentials were merely encoded, not encrypted—posing a risk of unauthorized access.
* **Lack of SSL/TLS:** No evidence of secure SMTP channels such as SMTPS or STARTTLS being used.
* **Server Disclosure:** SMTP banner disclosed information about server capabilities and limitations.

**7. Recommendations**

1. **Implement Secure SMTP (SMTPS or STARTTLS):** Ensure email servers enforce encrypted communication to protect against interception.
2. **Use Stronger Authentication Mechanisms:** Replace Base64 encoding with secure authentication methods and consider MFA.
3. **Disable Plaintext Logins:** Configure mail servers to reject authentication over unsecured channels.
4. **Monitor SMTP Logs for Abnormal Activity:** Detect and respond to unusual login attempts or bulk message transmissions.
5. **Educate Users:** Raise awareness about the dangers of unsecured email communications and phishing risks.

**8.Conclusion**

1. The analysis revealed several significant security flaws in the email transmission process, particularly due to the lack of encryption and the exposure of sensitive credentials. The SMTP traffic was susceptible to interception, enabling potential attackers to reconstruct emails and access confidential information.
2. This highlights the critical need for encryption protocols and secure configurations when transmitting email over the internet.

**Questions you need to answer**

• When did it happen?

• the timestamps email

• The email client

• outlook

• The content of the email

• multiple parts

• What was the approach?

• ports (sender and receiver)

• IP addresses (sender and receiver)

• Mac addresses (sender and receive