Submission - LAB 2: TCP

Please submit during this lab session or else at next week's lab session.

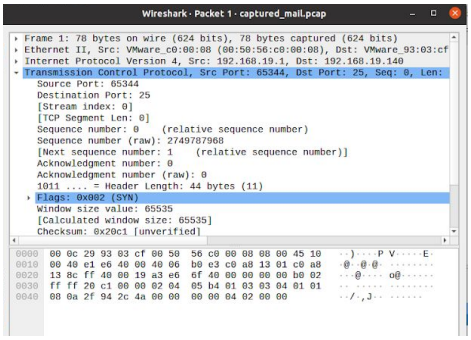
Student name: Nathan Crowley Student ID: 118429092
Submission date: 11/11/20

1. TCP - Email trace

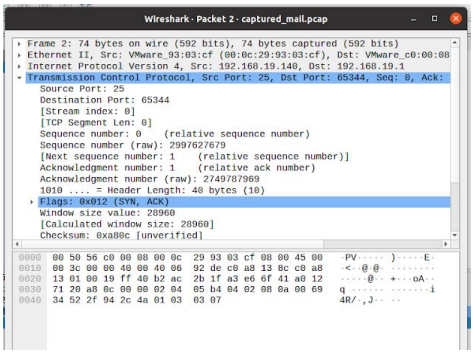
1 What are the pairs of IP addresses and TCP ports found in the email communication? Which IP and port belong to the email server and which to the client?

- TCP handshake = client sends SYN to establish connection with server and informs the server about the client should start communication. So from wireshark I can see that the SYN has source:192.168.19.1 and destination:192.168.19.140. Also if I inspect the TCP section in wireshark I can see that the source Port=65344 and destination Port=25.
- Client = **IP:**192.168.19.1**, Port:**65344
- Server = **IP:**192.168.19.140, **Port:25**

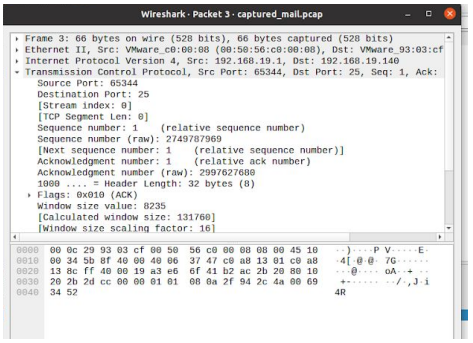
SYN:



SYN-ACK:



ACK:

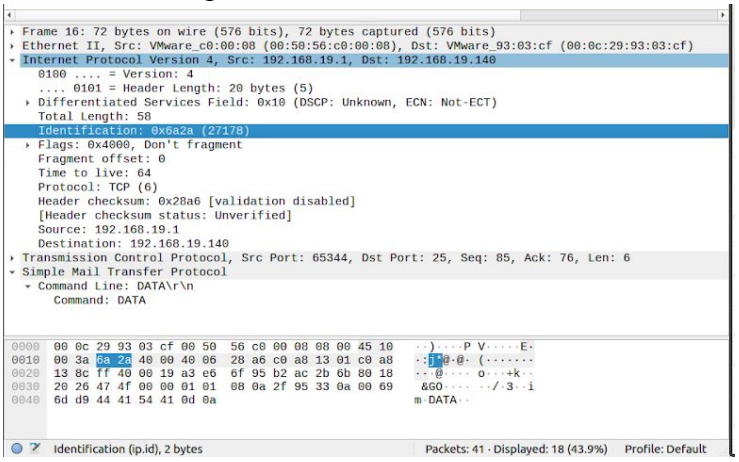


2 From the packet trace, find four different commands for SMTP. Write down packet ID containing those commands.

- SMTP = Simple Mail Transfer Protocol, an application used to send, receive, and relay outgoing emails between senders and receivers. When an email is sent it is transferred over the internet from one server to another using SMTP. SMTP email is just an email sent using the SMTP server.
- All commands from sent from client to sever.

1) Command = “HELO”, PacketID: 0xe239
2) Command = “MAIL”, PacketID: 0xe929
3) Command = “RCPT”, PacketID: 0xc067
4) Command = “DATA”, PacketID: 0xa62a

Identification = packetID.



3 Write down four response codes for SMTP and their corresponding meaning and the packets containing them in the trace.

- SMTP Response Codes = consists of three digits.
  - **The error code class:**
    First digit indicates **whether or not the server accepted** the command. This is a digit ranging from 1-5.
  - **Subject**:
    Middle digit gives **more information**, stating whether there was a syntactic problem, connection trouble, etc.
  - **Detail**:
    Last digit provides even more information about the **mail transfer status**.
- Example: 220 = SMTP Service ready.

All responses sent from server to client:

1) **Response Code: 220 Service ready**. Packet = indicates that the SMTP server is ready to continue forward the next command.

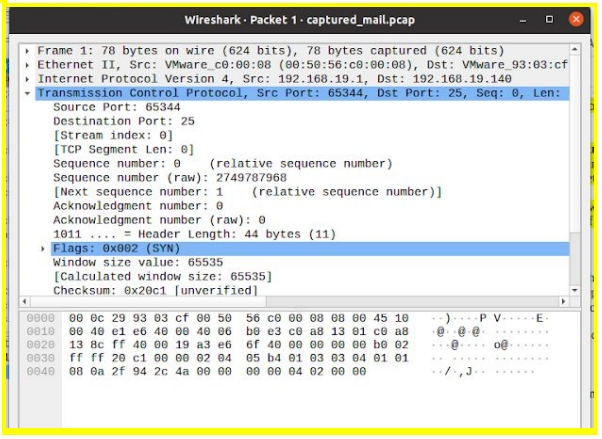
2) **Response Code: 250 Requested mail action okay, completed.** Packet = indicates that the SMTP communication was successful. It is issued in response to every accepted command.

3) **Response Code: 354 Start mail input; end with <CRLF>.<CRLF>**. Packet = indicates that the server is ready to accept the message itself.

4) **Response Code: 221 Service closing transmission channel.** Packet = states that the session or connection to mail server is ending and all processes are complete.

4 What are the TCP flags of the first three packets of the TCP connection? What is the name of this mechanism?

- TCP flags: are used to indicate a particular state of connection to provide useful information like troubleshooting purposes or to handle a control of a particular connection. Each flag corresponds to a 1 bit information.
- First three flags in TCP connection.
    1) **SYN**: used in the first step of connection establishment. Only the first packet from sender and receiver should have this flag set. **Used for synchronizing sequence number** (to tell the other end which sequence number they should accept).

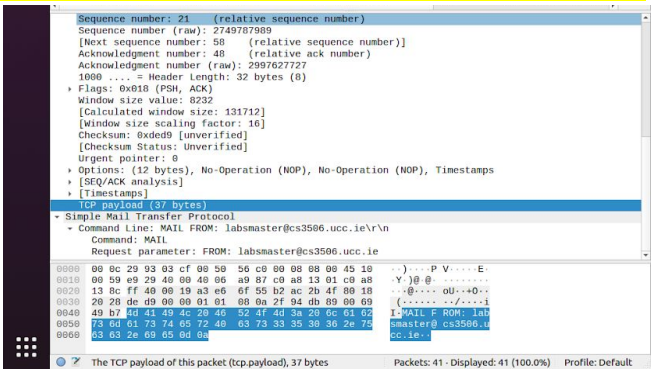


    2) **SYN, ACK:** The a**cknowledgement number is set** to 1 more than the received sequence number (A+1) and the **sequence number** that the server chooses for the packet is another random number (B).

    3) **ACK:** used to acknowledge packets which are **successfully received** by the host. The flag is set if the acknowledgement number field contains a valid ack number.

5 What is the sequence number of the TCP segment containing the mail FROM address? Note that in order to find a specific payload, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with "FROM" within its DATA field.
How many bytes of TCP payload does this packet contain? What is the FROM email address?

- Sequence number of FROM:
  - Relative sequence number = **21**
  - Raw sequence number = 2749787989
- TCP payload packet bytes: **37 bytes**.
- FROM email address: **labsmaster@cs3506.ucc.ie**



6 Packets No. 9 and 10 have the same sequence numbers. How do you explain this?

- Sequence number = the byte number of the first byte of data in the TCP packet sent(also called TCP segment).
- The Acknowledgement number = the sequence number of the next byte the receiver expects.
- Same sequence numbers: both frames point to the same payload data at sequence number x.

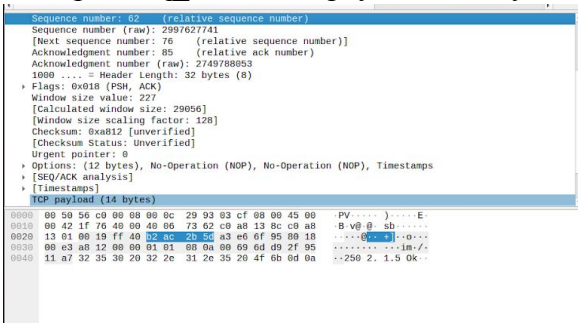
7 Select frame 14. What is its ACK number?
It acknowledges frame 13. Use the ACK number and segment information to explain why. How does Wireshark compute "next Seq number"?

- Frame 14 ACK number:
  - **ACK number = 85**.
  - **Sequence number = 62.**
- Why does is acknowledge frame 13:

  Frame 13 is a RCPT to establish a receipt of the message to itsomp@loaclhost. So frame 14 is the SMTP code (250) to acknowledge that frame 13 action is okay and completed.

- How to compute “next Seq number”:
  next sequence number = sequence number + payload.
  Since sequence number indicates the start of the payload the next sequence number must start just after the payload.

Example: seq_num = 62. payload = 14bytes. Next seq_num = 62+14 = 76.

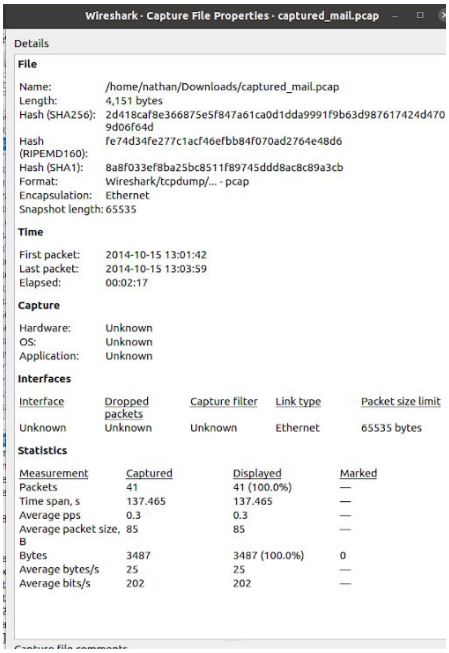


8 View Statistics – Capture File Properties. What is the throughput (bytes transferred per time unit) for the TCP connection? Explain how Wireshark calculates this value.

- Throughput = rate that data is successfully delivered over a TCP connection. Its an important metric to measure the quality of a network connection.
- **Throughput (in bits) = size of file / transmission time.**
- time span = 137.465 seconds.
- size of file = 27896 bits (3487 bytes).
- **Throughput = 27896 bits / 137.465 seconds = 202.9 bits/second.**

9 How many bytes of TCP payload were transferred in this transmission in total? How did you compute this?

- **Total payload transferred = bits/s * time span = 202 * 137.465 = 27,767.93 btis = 3470.99125 bytes with average bits/second.**

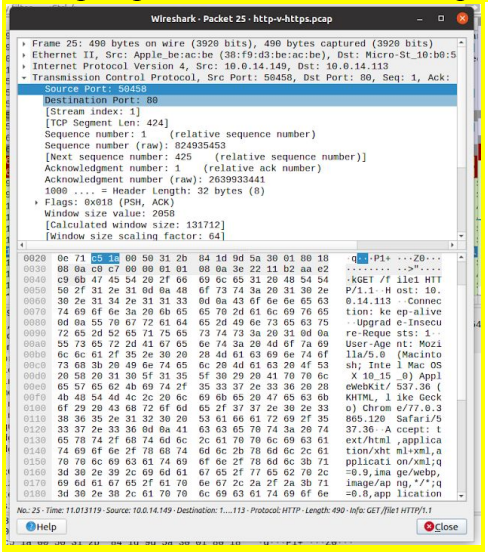


2. TCP - HTTP trace

1 What are the client and server TCP ports used for downloading over HTTP and HTTPS?

- Client:
  HTTP: port 50458
  HTTPS: port 50457.
- Server:
  HTTP: port 80.
  HTTPS: port 443.

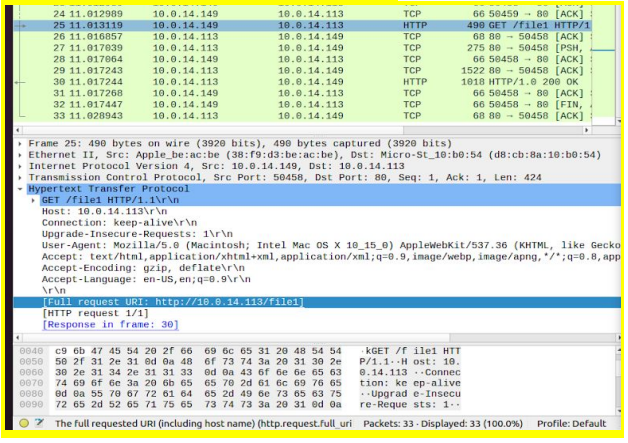
Example: packet 25 HTTP GET request to server at port 80.



2 Based on reviewing the trace provided what are the risks associated with HTTP traffic as opposed to the use of TLS based HTTPS.

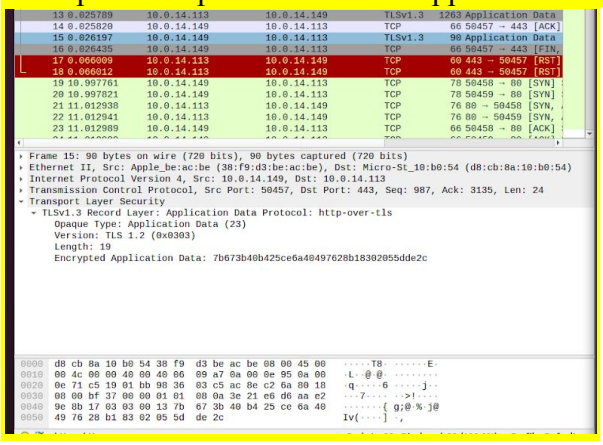
- **TLS:** encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit. Useful for private and sensitive information such as passwords,credit card numbers,etc.

- Risks of HTTP are that your data is not encrypted and is sent across as plain text and if intercepted can easily be interpreted.
  Example: HTTP GET file request packet 25 has the *"Full request URL"* in plain text in the HTTP section.



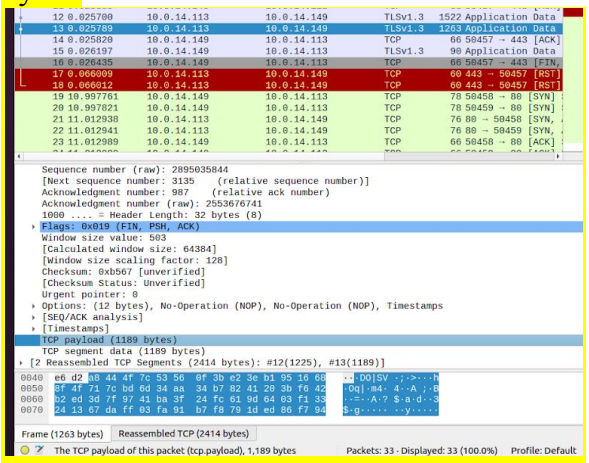
- Whereas HTTPS is secure as it sends the encrypted data as cipher text and anyone intercepting would not be able to understand this encrypted data. Making it much safer to use.

  Example: TLS packet 15 has its application data encrypted.



3 How much overhead does encryption incur (how many more Bytes are being transmitted) in the HTTPS case? How did you compute this?

- Data sent over HTTPS has much larger payload. For example, the largest HTTPS packet payload = 1448 bytes. Whereas the largest HTTP packet has payload = 944 bytes.



- As well as the large payloads there is a longer time to set up a HTTPS handshake whereas HTTP does not have this problem.