**The University of Bradford**

**Faculty of Engineering and Informatics**

**Department of Computer Science**

**Coursework (100%)**

**Module Title:** Network and Protocols

**Module Code:** COS7024-B

**Module Credit:** 20

**Academic Level:** 7

**Coursework Title:** Network Traffic Analysis using Wireshark

This coursework introduces students to a free network analyser. Network analysers are very useful tools for understanding data communication strategies in computer networks. They scan the data packets in any network and provide a visual view of packets as they flow past the computer. We use Wireshark, a sniffer which may be downloaded for free off the Internet. Further details about Wireshark as well as downloads are available at www.wireshark.org

In this coursework, you will be examining several aspects of TCP, SMTP and HTTP application layer protocols. Follow the steps below to complete this coursework:

**Step 1: Start a Wireshark capture.**

1. Close all unnecessary network traffic, such as the web browser, to limit the amount traffic during the Wireshark capture.
2. Start the Wireshark capture.

**Step 2: telnet to the** [**SMTP.brad.ac.uk**](ftp://ftp.ed.ac.uk) **25 server.**

* 1. You should receive output similar to the following:  
     **220 radon.cen.brad.ac.uk ESMTP Postfix**  
     NOTE: Once the telnet session is established, the Backspace and Delete keys do not work. If a typo is made, press Enter and retry the command. In some cases, it may be necessary to close the telnet session and reconnect.
  2. If you receive an error similar to **Could not open connection to the host, on port 25: Connect failed**, this indicates that your machine could not establish a telnet session with the destination server using port 25. If you initially attempted to connect using the destination server's name, try to connect using its IP address instead. If this is successful, you likely have a DNS issue. If you are unable to connect using the destination server's name or IP address, port 25 is being blocked somewhere between your machine and the destination server. The issue is probably due to a firewall on the destination server's end, but it can also be caused by a network misconfiguration or firewall on your end.

**Step 3:** Type: **EHLO  *bradford.ac.uk***

**Step 4:** Type: **mail from:** *<your\_ email\_address>* and press Enter

**Step 5:** Type: **rcpt to:** *<asadik@bradford.ac.uk>* and press Enter

**Step 6:** Type: **rcpt to:** *<your\_ email\_address >* and press Enter

**Step 7:** Type: **data** and press Enter.

**Step 8:** Type: **Subject:** *<a subject of your email>* and press Enter

**Step 9:** Type: ***This is a test message sent from telnet*.** and press Enter.

**Step 10:** Type: **.**   and press Enter

**Step 11:** Type: **quit**

**Step 12:** Stop capturing and save the captured file as ***coursework2022-23.pcapng***

**NOTE: - If you are unable to run Wireshark on a live connection, you can download a packet trace file *coursework2022-23.pcapng* that was captured.**

**I am using the Wireshark file provided on canvas as I couldn’t get the telnet to work on my laptop.**

Answer the following questions (all questions are weighted):

1. Change the **Time** column in Wireshark from seconds to Date and Time of the Day

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated (**Marks 2%)**

1. Add two columns to Wireshark interface one called **SrcPort** and another called **DesPort**.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

(**Marks 3%)**

1. List 5 different protocols from each the network layers that appear in the protocol column. What port number is being used by your or client computer for this connection? How was this port number chosen?

UDP

Port number: 54915

Port numbers of the user data protocol are dynamically assigned for clients between the range of 4096-65535. The port number that was assigned in the file for the packet chosen was 54915, however this could have been any in the range.

Graphical user interface, text, application, email

Description automatically generated

TCP

Port number 445

Port 445 is used for server message block protocol (SMB), which is used for file sharing. This is used on top of the TCP stack allowing for SMB to work over the internet.

Graphical user interface, application, Word

Description automatically generated

DNS

Port number: 53

DNS uses the port 53 to maintain the coherence between the DNS database and the server. It either uses the TCP or UDP port 53 to do this.

Graphical user interface, text, application

Description automatically generated

SMTP:

Port number: 25

SMTP default port number is 25 and is used to relay emails on the internet. As this is an email message SMTP needs to use this port or another port like 587.

Graphical user interface, text, application

Description automatically generated

HTTP

Port number: 80

Port 80 is the default network port used to send and receive unencrypted web pages. Port 80 is not secure resulting in the contents being sent unencrypted. It is a port that listens to a server and expects to receive web client traffic. HTTPS would use port 443 which is encrypted.

Graphical user interface, application

Description automatically generated

(**Marks 10%)**

1. What was the message, and what was the subject of the email from Wireshark?

Graphical user interface, application

Description automatically generated

Subject = Wireshark coursework

Message = This is a test message sent from telnet

**(Marks 10%)**

1. What protocol does SMTP run on top of?

SMTP can be found running on top of TCP. TCP is ideal for this protocol as TCP checks to see if every packet is received and if it isn’t it is resent, ensuring that the entire message is delivered. As SMTP it only makes sense to use TCP as every single packet is important; The recipient may only receive half a message which is useless if SMTP was run on top of UDP for example. Screenshot below shows SMTP protocol being used on top of TCP.

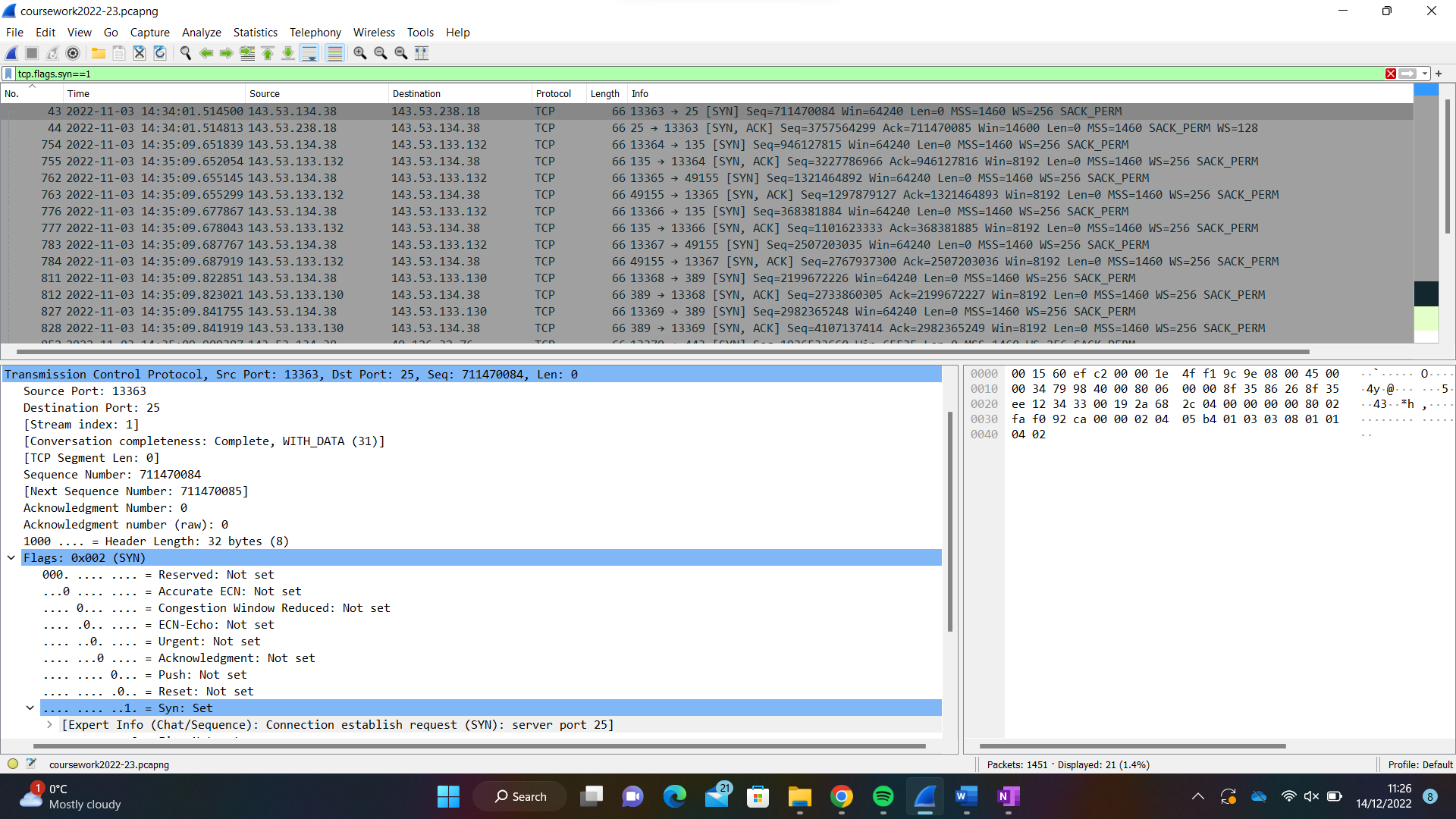
Graphical user interface, text, application

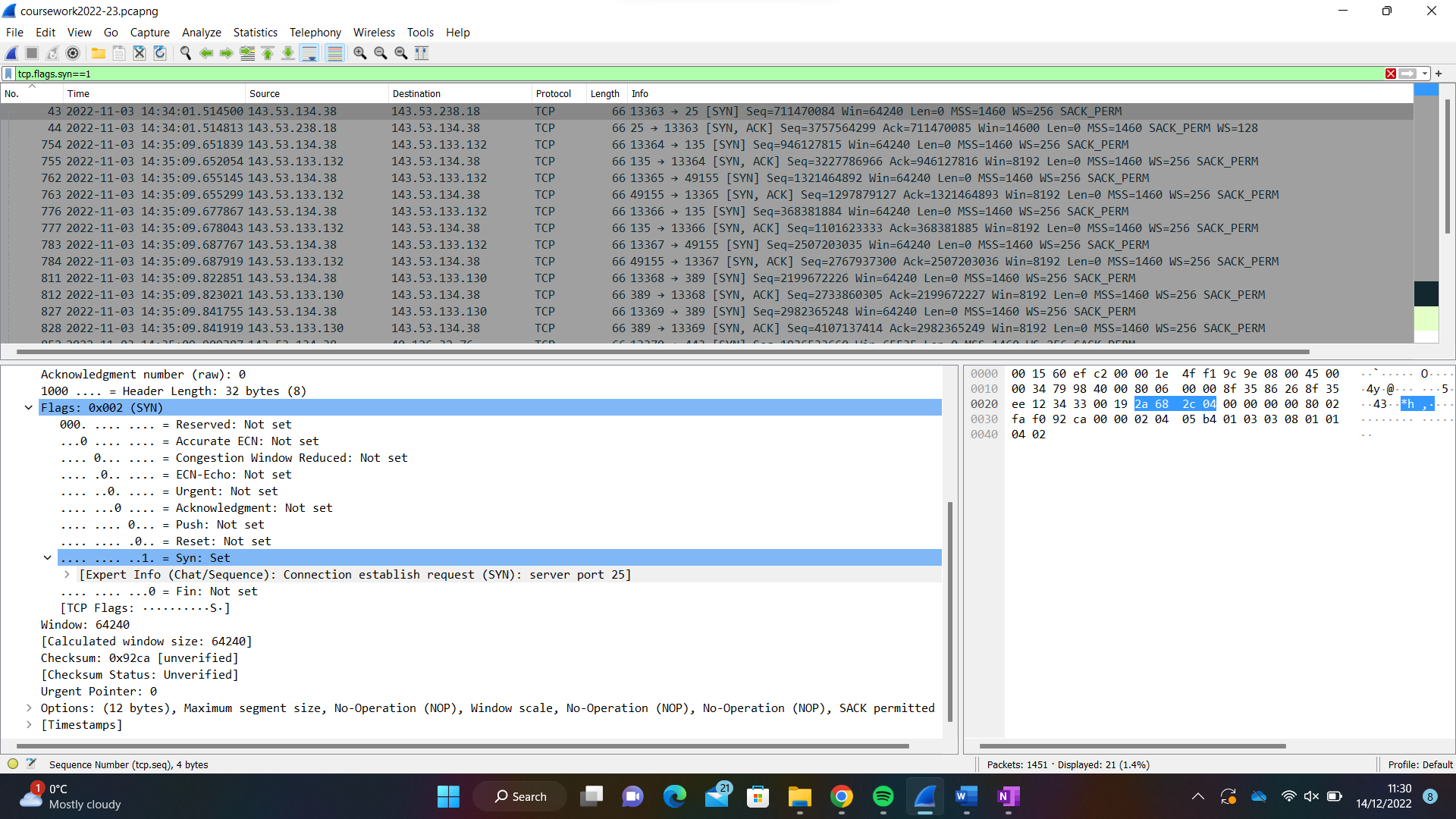
Description automatically generated

(**Marks 5%)**

1. Using the Wireshark capture of the first TCP session start up (SYN bit set to 1), fill in information about the TCP header:

From your or client PC/Laptop to **SMTP.brad.ac.uk** server, (only the SYN bit is set to 1):





|  |  |
| --- | --- |
| Source IP Address: | 143.53.134.38 |
| Destination IP Address: | 143.53.238.18 |
| Source port number: | 13363 |
| Destination ort number: | 13371 |
| Sequence number: | 711470084 |
| Acknowledgement number: | 0 |
| Header length: | 32 bytes |
| Window size: | 64240 |

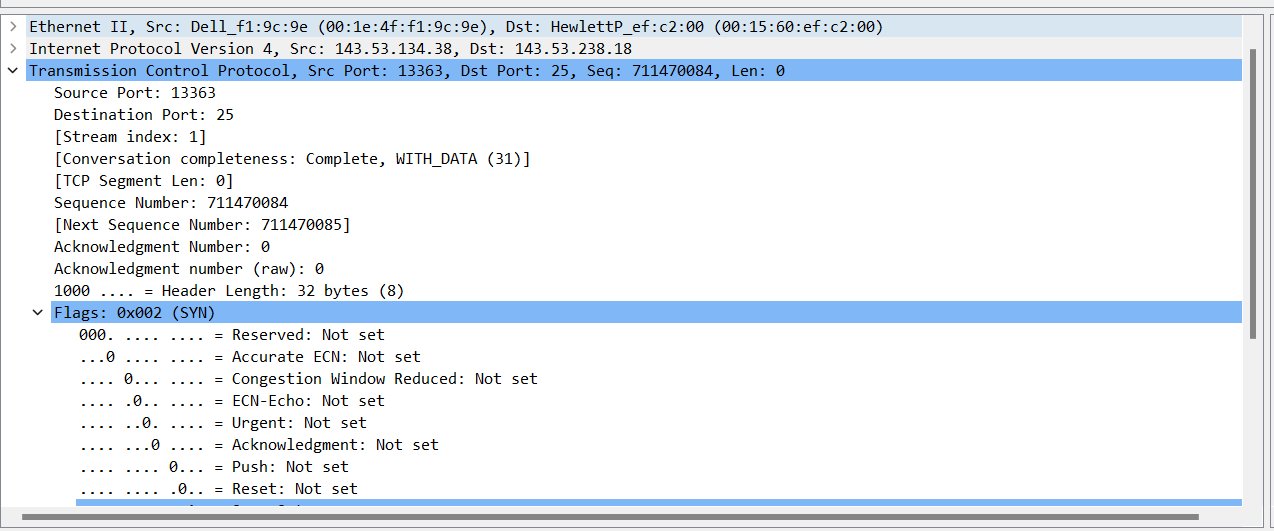
(**Marks 15%)**

1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and **SMTP.brad.ac.uk**? Why was this sequence number chosen? (Note that Wireshark does not by default show you real sequence numbers, it shows you relative sequence numbers. You should disable this function in Wireshark's TCP preferences.)

A screenshot of a computer

Description automatically generated

The SYN flag is set to 1 therefore indicates that this segment is a SYN segment.



The sequence number was 711470084

Sequence numbers show the order of the messages, this is important as it helps piece together the messages being sent. This sequence number was assigned to this packet as it was the next message being sent in the message sequence. This allows the TCP protocol ensure that every message is sent and each packet is rearranged in the correct order for the recipient to view.

(**Marks 10%)**

1. In the second Wireshark filtered capture, the **SMTP.brad.ac.uk** server acknowledges the request from the PC/Laptop. Note the values of the SYN and ACK bits. Fill in the following information regarding the SYN-ACK message.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

|  |  |
| --- | --- |
| Source IP Address: | 143.53.238.18 |
| Destination IP Address: | 143.53.134.38 |
| Source port number: | 25 |
| Destination port number: | 13363 |
| Sequence number: | 3757564299 |
| Acknowledgement number: | 711470085 |
| Header length: | 32 bytes |
| Window size: | 14600 |

(**Marks 15%)**

1. Apply the TCP filter again in Wireshark to examine the termination of the TCP session. Four packets are transmitted for the termination of the TCP session. Because TCP connection is full duplex, each direction must terminate independently. Examine the frames, source and destination addresses.

In frame 1432 it shows a segment with the FIN flag. This is server to PC. The PC then sends an ACK to acknowledge the receipt of the FIN to terminate the session from the server to the client in frame 1433.

In frame 1434 the PC sends a FIN to the FTP server to terminate the TCP session. The FTP server responds with an ACK to acknowledge the FIN from the PC in frame 1435. Now the TCP session is terminated between the FTP server and PC.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

(**Marks 10%)**

1. Draw a timing datagram illustrating the sequence of the first four-packet. For each packet, indicated the source and destination port numbers. Are the port numbers the same?

A screenshot of a computer

Description automatically generated with medium confidence

Frame 1432

Source port: 25

Destination port: 13363

Frame 1433

Source port: 13363

Destination port: 25

Frame 1434

Source port: 13363

Destination port: 25

Frame 1435

Source port: 25

Destination port: 13363

Client port number is 25.

Server port number is 13363.

Theses are the two port numbers being used as the client is terminating their session with the server.

(**Marks 10%)**

1. Some experts believe that sending an email message is like sending a postcard.

Why? How secure is SMTP email? How could security be improved?

SMTP does not send an email directly to the receiver instead it sends the message to the email server and then to everyone, however it is usually only the recipient who sees it in their emails. The email isn’t sent using any form of encryption is acceptable to a man in the middle and eaves dropping. It is to a postcard as a postcards message is not concealed and is available to view by anyone who can see it, as it is not in an envelope. To improve security TLS can be enabled when sending the messages. This ensures that the message is encrypted when being sent through the transport layer resulting in the SMTP to become SMTPs. SMTPs is a secure channel ensuring man in the middle attack and eaves dropping does not successfully obtain the contents of the email being sent unless the encryption is broken.

(**Marks 10%)**

**Deliverables**

In addition to provide answers, you should also include the ***coursework2022-23.pcapng*** file**,** and **SCREENSHOT** images (for each step and answer) taken from the Wireshark in your report file. Your assignment archive must be submitted to the Canvas by **Friday 16/12/2022 at 23:59**