**Module Title: Network and Security**

**Module Code: COS7055-B**

**UB number - 24010283**

**1.Provide a screenshot for your machine IP Address by using ipconfg, or ifconfig  
commands**

A screenshot of a computer

Description automatically generated

**2. List 5 different protocols that appear in the protocol column. What port number is  
being used by your computer for this connection? How was this port number chosen?  
(Marks 15%)**

1. List of 5 Protocols Observed in the Protocol Column:

TCP (Transmission Control Protocol)

UDP (User Datagram Protocol)

ARP (Address Resolution Protocol)

MDNS (Multicast DNS)

DNS (Domain Name System)

2. Port Number Used by Your Computer for the Connection:

Port Number: 21

3. How Was This Port Number Chosen?

The reason that port 21 was chosen was because this is a well-known port reserved for ftp connections. It’s mainly predefined for servers and clients as per the internet assigned Number authority standards. The computer connects to the ftp server using port 21 as the destination port. However, the source port is assigned by the operating system

**3. Identify the packets detail that show the username and the password (Marks 10%)**

Packet Analysis for the username:

1. Packet Number:
   * 6946
2. Protocol:
   * FTP (File Transfer Protocol)
3. Source and Destination:
   * Source IP: 192.168.0.242
   * Destination IP: 130.14.250.13
4. Command and Credentials:
   * Command: USER
   * Username: anonymous
5. Details:
   * This packet is an FTP request in which the FTP server (130.14.250.13) receives the USER command from the client (192.168.0.242). For anonymous login attempts on FTP servers, the command specifies the username anonymous.
6. Significance:

* The user command is a part of the ftp authentication process.it analyses the PASS command and the which processed to provide us with the password. As the FTP command transmits the credentials in plain text the username can easily be intercepted.

A screenshot of a computer

Description automatically generated

Packet Analysis for the Password:

1. Packet Number:
   * 7426
2. Protocol:
   * FTP (File Transfer Protocol)
3. Source and Destination:
   * Source IP: 192.168.0.242
   * Destination IP: 130.14.250.13
4. Command and Credentials:
   * Command: PASS
   * Password: mmahmo51@bradford.ac.uk
5. Details:
   * This packet is an FTP request where the client (192.168.0.242) sends the PASS command to the FTP server (130.14.250.13). The PASS command provides the password associated with the previously sent username (anonymous in Packet #6946).
   * The password mmahmo51@bradford.ac.uk was transmitted in plaintext, highlighting the lack of encryption in FTP communication.
6. Significance:
   * Combined with the username (anonymous), this packet completes the FTP authentication process. Since the credentials are sent in plaintext, they can be easily intercepted and misused by attackers monitoring the network.

A screenshot of a computer

Description automatically generated

**4. 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 PC/Laptop to ftp.ncbi.nih.gov server, (only the SYN bit is set to 1):**

Packet number 6956 Time - 68.113144 source -192.168.0.242 Destination -130.14.250.13

Protocol TCP, Length 54 packet info 51959 → 21 [ACK] Seq=1888387770 Ack=1216610188 Win=7207 Len=0

Source IP Address: 192.168.0.242  
Destination IP Address: 130.14.250  
Source port number: 51959  
Destination port number: 21  
Sequence number: 1888387770  
Acknowledgement number: 1216610188  
Header length:20 bytes  
Window size:7207

A screenshot of a computer

Description automatically generated

**5. What is the sequence number of the TCP SYN segment that is used to initiate the  
TCP connection between your computer and ftp.ncbi.nih.gov? Why was this  
sequence number chosen?**

**Sequence Number of the TCP SYN Segment:**

* **Sequence Number:** 1888387770

**Why Was This Sequence Number Chosen?**

The sequence number in the Syn segment as displayed in my response is a randomly chosen initial sequence numbers and the reasoning why it is unique and random are highlighted below, By randomizing the ISN, TCP ensures that each session has its own unique starting point for sequencing packets.

* + **Prevent sequence number prediction attacks –** This is where an attack such as TCP spoofing could take place, this is where an attacker predicts the sequence number to inject malicious packets
  + **Ensure uniqueness-** so another reason would be to ensure uniqueness so that for each connection it ensures that the sequence numbers do not overlap with those sequence numbers that had been used in previous sessions.
  + **Another reason would be the assistance in tracking the order of the packets –** this would be assisting the communication between your computer and the server.

A screenshot of a computer

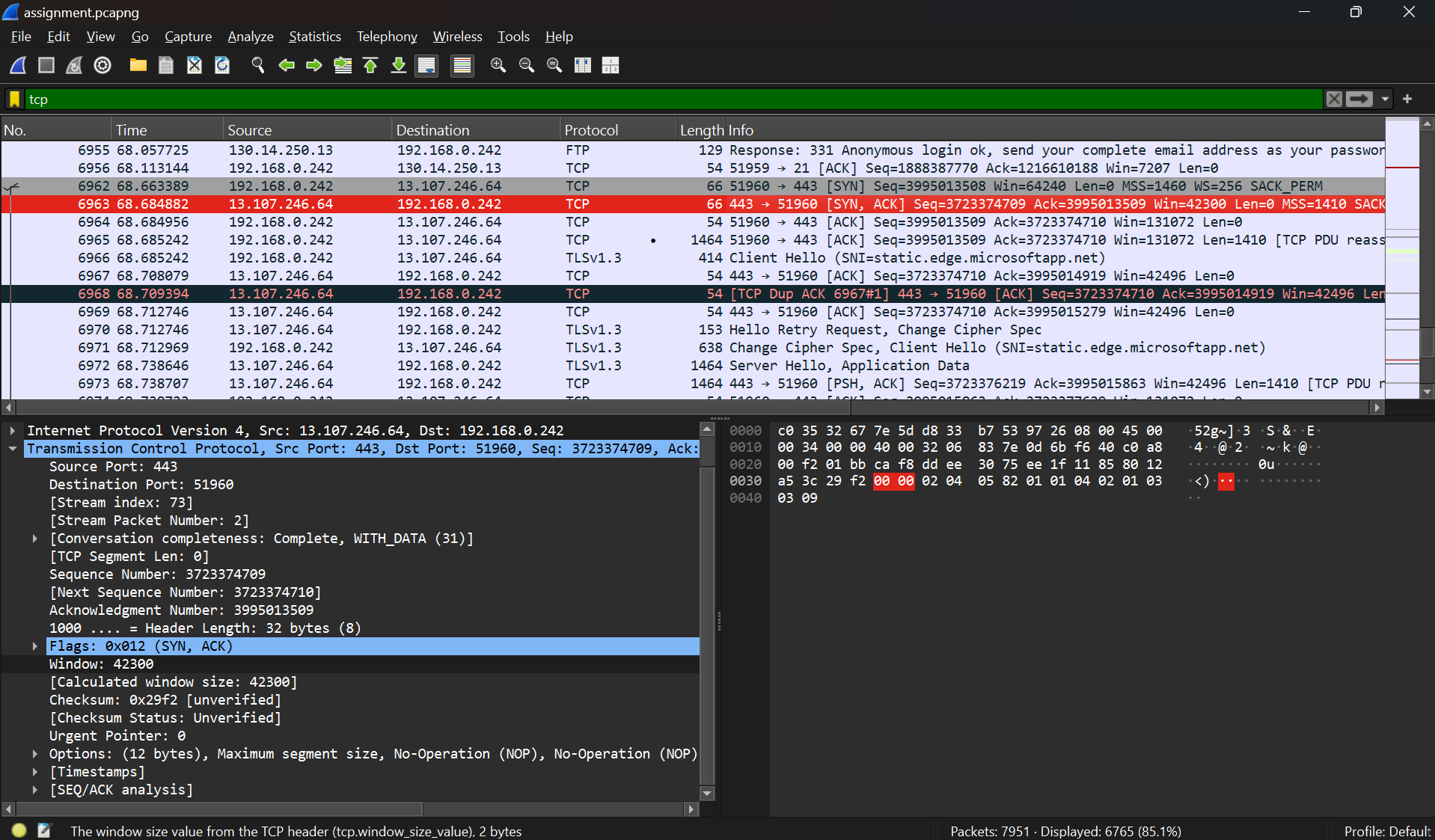
Description automatically generated

**6) In the second Wireshark filtered capture, the ftp.ncbi.nih.gov server  
acknowledges the request from the PC. Note the values of the SYN and ACK bits.**  
**SYN-ACK Packet Details:**

* Source IP Address: 13.107.246.64  
  The server ([ftp.ncbi.nih.gov](ftp://ftp.ncbi.nih.gov)) is responding to us by indicating that it is reachable and that it is ready to establish a communication line.
* Destination IP Address: 192.168.0.242 – This destination address shows that the server has acknowledged the request that the client had sent from the client which is our machine with this specific Ip address. This confirms that the server would know where it should send the acknowledgement of the session.
* Source Port Number: 443 – this HTTPS port is a well-known port that is used by the server. This tells us that the connection is secure and that it may involve encrypted data exchange.
* Destination Port Number: 51960 – This Destination port was specifically chosen by the computer for this session. This is done to ensure that the response can be matched to the initial SYN packet, especially when multiple connections are active.
* Sequence Number: 3723374709 – This sequence number has been randomly chosen by the server. The reason this has been done is to ensure uniqueness for the session and it enables the reliable tracking of data, and it also prevents over lapping with other communications.
* Acknowledgment Number: 3995013509 – so this is basically an increment of the initial sequence number, by acknowledging the clients sequence number (3995013508) incremented by 1 the server then confirms the clients SYN request and that its then ready for the next step.
* **Header Length**: 32 bytes  
  (This indicates the size of the TCP header, which includes the SYN and ACK flags along with other fields.)
* Window Size: 42300 The window size tells the client how much data can be received by the server before it requires an acknowledgment this ensures efficient and smooth data flow.

Why is the SYN-ACK Significant for the Connection?

* Reliable Communication: The reason why the SYN-ACK is so significant is since without it the client would not know if the server had received its connection request.
* Security: The implementation and use of random sequence numbers for the SYN and SYN-ACK packets helps increase security by protecting against tcp spoofing attacks.
* Synchronization: The reason synchronization is crucial for security is that it ensures that both devices can agree on sequence numbers which prevents data corruption during transmission.



**6) 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**

With regards to the tcp session termination process, the connection is close down in a complete manner meaning that each direction of the communication are terminated independently and the following 4 packets below are exchanges during the session termination.

1. **Packet 1 (Client to Server):**
   * **Source IP Address**: 192.168.0.242
   * **Destination IP Address**: 104.168.0.242
   * **Source Port Number**: 51892
   * **Destination Port Number**: 443
   * **Flags**: 0 x 010 ACK
   * **Sequence Number**: 1049332910
   * **Acknowledgment Number**: 2008339082

This packet indicates that the client is requesting to terminate the connection from its side, while acknowledging the server’s data.

A computer screen shot of a number

Description automatically generated

1. **Packet 2 (Server to Client):**
   * **Source IP Address**: 192.168.0.242
   * **Destination IP Address**: 20.190.160.22
   * **Source Port Number**: 51850
   * **Destination Port Number**: 443
   * **Flags**: FIN, ACK
   * **Sequence Number**: 85596039
   * **Acknowledgment Number**: 4062415557
   * The server acknowledges the client's FIN and requests to close the connection from its side.

A computer screen shot of a program

Description automatically generated

1. **Packet 3 (Client to Server):**
   * **Source IP Address**: 20.190.160.22
   * **Destination IP Address**: 192.168.0.242
   * **Source Port Number**: 443
   * **Destination Port Number**: 51850
   * **Flags**: FIN, ACK
   * **Sequence Number**: 4062415557
   * **Acknowledgment Number**: 85596040

The client acknowledges the server’s FIN and completes the termination process from the client side.

A computer screen shot of a black screen

Description automatically generated

1. **Packet 4 (Server to Client):**
   * **Source IP Address**: 192.168.0.242
   * **Destination IP Address**: 20.190.160.22
   * **Source Port Number**: 51850
   * **Destination Port Number**: 443
   * **Flags**: ACK
   * **Sequence Number**: 85596040
   * **Acknowledgment Number**: 4062415558

The server acknowledges the client's FIN and completes the termination process from the server side."

A computer screen shot of a black screen

Description automatically generated

The TCP connection is then analysed in the packet exchange it is a structured sequence ensuing an orderly closure of the communication. The process includes 4 packets with it starting of with an ACK and then FIN, ACK which signals a message to terminate and then the server follows up a response by responding with FIN, ACK and then the client concluded it with an ACK. This sequence that is using Fin and Ack flags has done so to maintain session integrity while the synchronization of sequence and acknowledgment numbers ensure that no data is lost. The source and the destination Ip and ports highlight the endpoints. However, the clients on the other hand would use a dynamic port and they would use the port 433 that we had earlier addressed to ensure secure HTTPS Communication. The next sections such as the timing, sequence numbers and window size reflect that the conditions are favourable and that the network is in a secure and healthy position and that we can close the process down without any data loss. If we look at this from a security perspective, we can see that this termination would provide us with insightful information with regards to possible vulnerabilities such a sequence numbers being different or mismatched flags or irregular timing and this may possibly suggest issues such as spoofing, session hijacking or denial of service attacks. This set up and layout of the TCP termination packets ensures that there is a level of traceability and reliability against closures, and it also safeguards session integrity which makes it a critical process for secure communication and effective network monitoring

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?  
   (Marks 10%)

Packet 1: Source 51893 → Destination 443 ACK

This is the first packet I have included since it acknowledges the previously received data. This confirms to us that the client has processed everything sent by the server sent up until that point. This shows us that this serves as the initial step in the termination process ensuring that no data is left unacknowledged. Without this packet there would be level of ambiguity regarding the state of the connection, the acknowledgement number in this packet shows me that there is data integrity and that the state for colure is ready to be initiated

A screenshot of a computer

Description automatically generated

Packet 2: Source 443 → Destination 51893

This next packet is now selected as this is the servers’ first active step towards terminating the session. This is because there is a FIN flag included, which indicates to us that this is the server signaling its intention to close the connection from its side. The following ACK flag then acknowledges the client's previous data. This 2-way purpose packet does align with the tcp termination procedure, and it represents the server's half of the closure procedure that is taking place

A computer screen shot of a computer program

Description automatically generated

Packet 3: Source 51893 → Destination 443

So, in this sequence the client responds with the following packet FIN, ACK and this is an indication of the process to terminate the connection. The FIN flag indicates that the client is closing the session from their side. While the ACK flag indicates to us an acknowledgment of the servers FIN from packet 2. This step here is quite important for completing the client termination and demonstrates the correct procedure for the tcp handshake connection ending.

A computer screen with white text

Description automatically generated

Packet 4: Source 51893 → Destination 443

A computer screen shot of a number

Description automatically generated

The server acknowledges the client's FIN and completes the termination process from the server side."

In the TCP connection sequence, the client uses an ephemeral port and in our example that would be port 51893 which would be referring to the first SYN packet. The Server then responds using a 443 port for HTTPS.

The Next ACK packet then keeps the same source and destination port numbers as the previous session. This is done to ensure that the connection is identified and is accurately tracked on both sides.

The usage of different port numbers does indeed help to identify the TCP connection. The reason as to why this is important is because a client can hive multiple different connections to the same server. And that the combination of source and destination ip addresses and port numbers would allow the network to manage the data flow for each connection.Even If the port

Even though the port numbers are not the same, they follow a consistent pattern where the client uses an ephemeral port, and the server uses a well-known service port. This is a fundamental aspect of how TCP connections are established and maintained.

A screenshot of a computer

Description automatically generated

Destination

(104.208.16.89)

Client (192.168.0.242)

FIN ACK – Source: 51850, Dest: 443

ACK Source: 51893, Dest 443

FIN ACK – Source: 443, Dest: 51850

Ack Source: 51850 – Dest: 443

Destination

(104.208.16.89)

Client (192.168.0.242)