# TCS2351 NETWORK SECURITY

## Trimester 1, 2023/2024

## Lecture: FCI

## Lecturer: Dr. Chan Wai Kok


| No | Student Name | Student ID |
|---|---|---|
| 1 | Kristina Geetha Menon a/p Christopher Menon | 1201201474 |

# Question 10

Output file = xyz.pcap

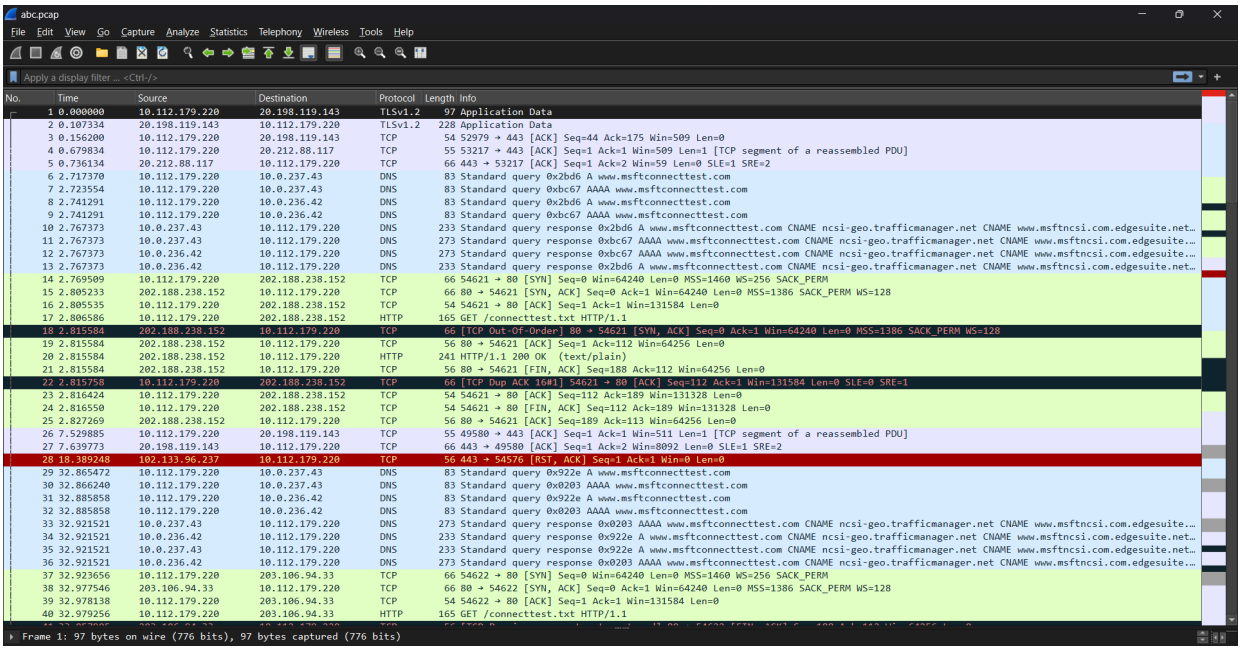
Change all source ip addresses to 18.X.X.X.

And rewrite the output into a file called xyz.pcap. (tcpdump format)

Other packets remain unchanged and are written to file xyz.pcap as well.

Bear in mind you have to recalculate the IP checksum for that packet.

1) **Capture the packet in Wireshark and save as abc.pcap**.

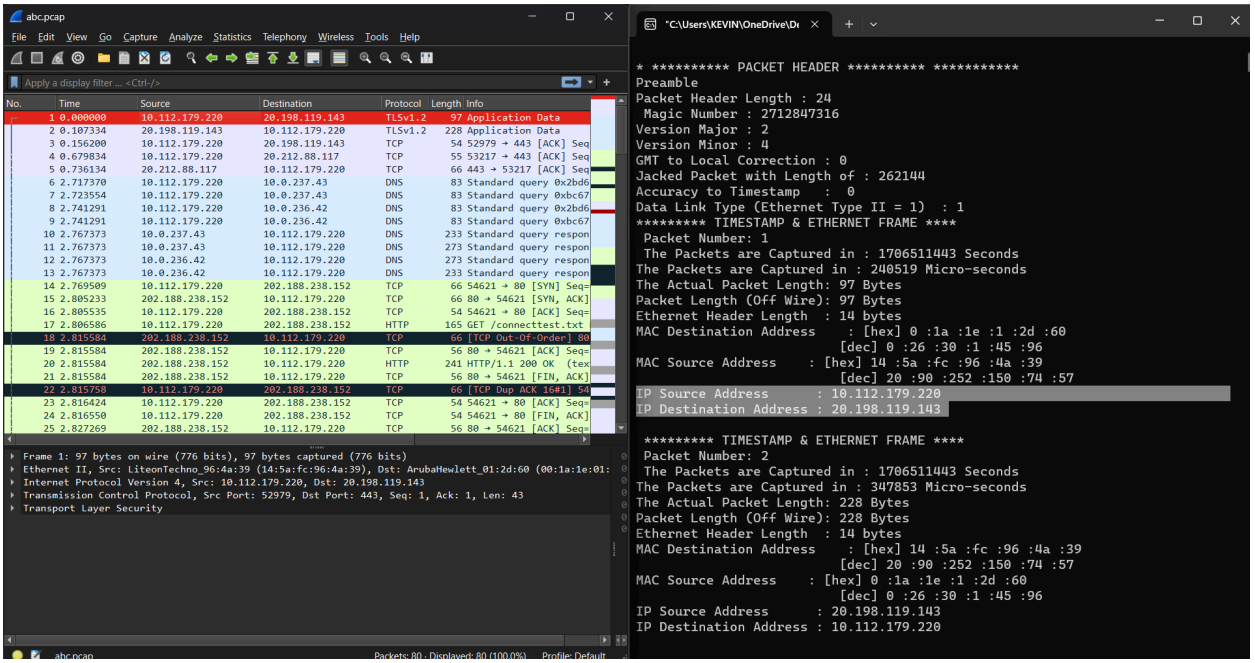



2) **Modify the code (1201201474_net1.cpp) to capture the IP source address and IP Destination address.**

```
// IP Header to capture IP Source address and Destination address
typedef struct ip_header
{
    unsigned char version_ihl;        // Version (4 bits) + Internet header length (4 bits)
    unsigned char dscp_ecn;           // DSCP (6 bits) + ECN (2 bits)
    unsigned short total_length;      // Total length
    unsigned short identification;    // Identification
    unsigned short flags_fragoffset; // Flags (3 bits) + Fragment offset (13 bits)
    unsigned char ttl;                // Time to Live
    unsigned char protocol;           // Protocol
    unsigned short checksum;          // Header checksum
    unsigned int src_ip;              // Source IP address
    unsigned int dest_ip;             // Destination IP address
} ip_hdr;
```

```
// Read and display IP header information
fread((char *)&ip, sizeof(ip), 1, input);
cout << "IP Source Address      : " << ((ip.src_ip >> 0) & 0xFF) << "." << ((ip.src_ip >> 8) & 0xFF)
     << "." << ((ip.src_ip >> 16) & 0xFF) << "." << ((ip.src_ip >> 24) & 0xFF) << endl;

cout << "IP Destination Address : " << ((ip.dest_ip >> 0) & 0xFF) << "." << ((ip.dest_ip >> 8) & 0xFF)
     << "." << ((ip.dest_ip >> 16) & 0xFF) << "." << ((ip.dest_ip >> 24) & 0xFF) << endl;
```

3) Run the 1201201474_net1.cpp file to compare the IP Source and Destination address with Wireshark.




**Note**: The IP source and destination address is similar compared to Wireshark. Hence, it is successful to locate all the IP packets.

4) **Task: I will need to modify my code in which:**
   a) Change all source ip captured in abc.pcap to 18.X.X.X. The code below represents the implementation on modifying the captured ip source address.

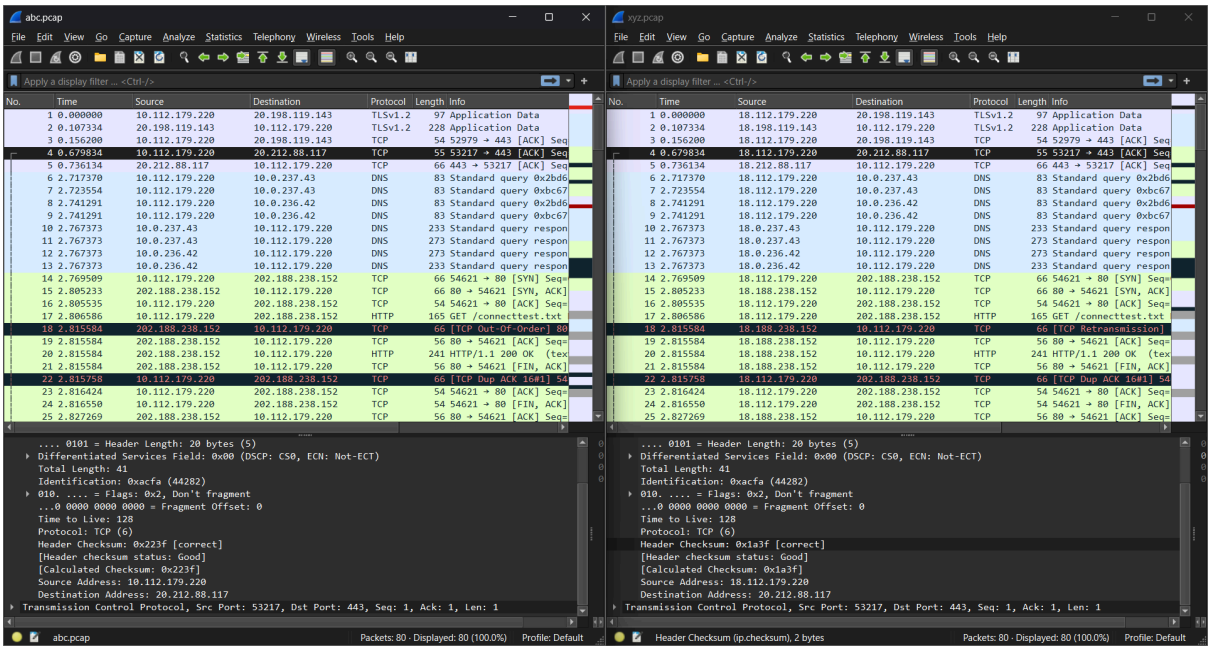
```
// Modify the source IP address -> 18.X.X.X
unsigned char *src_ip_bytes = reinterpret_cast<unsigned char*>(&ip.src_ip);

src_ip_bytes[0] = 18;
```

   b) Recalculate the IP checksum.

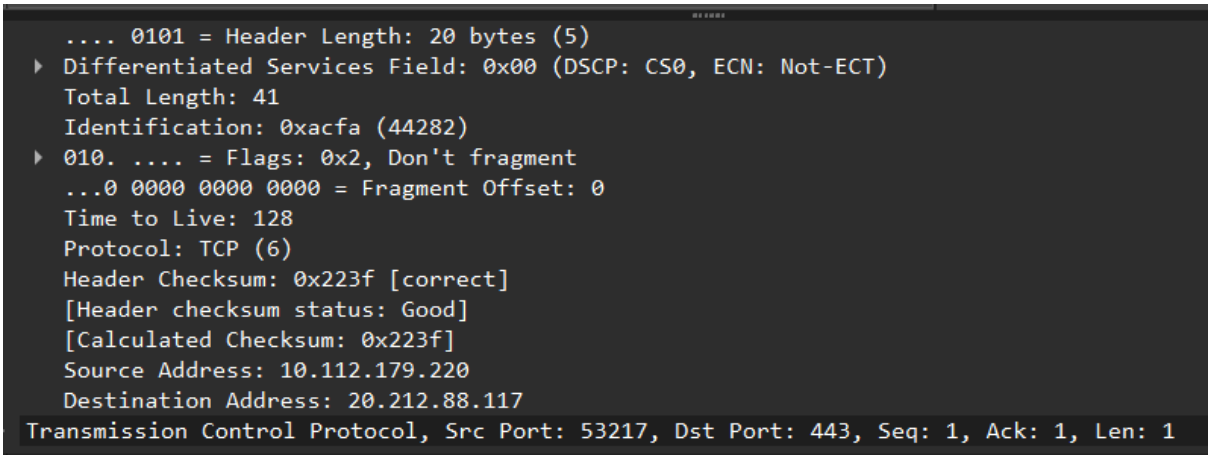
```
// Recalculate the IP checksum - call function
ip.checksum = calculateIPChecksum(&ip);
```

```c
// Function to recalculate IP checksum
unsigned short calculateIPChecksum(ip_header *ip_hdr)
{
    unsigned long sum = 0;
    unsigned short *ip_header_ptr = (unsigned short *)ip_hdr;
    int header_length = sizeof(ip_header) / 2; // Divide by 2 to get the number of 16-bit words

    ip_hdr->checksum = 0; // Clear the checksum field before calculation

    // Calculate the sum of all 16-bit words in the IP header
    for (int i = 0; i < header_length; i++)
    {
        sum += *ip_header_ptr++;
    }

    // Fold carry bits back into the sum
    while (sum >> 16)
    {
        sum = (sum & 0xFFFF) + (sum >> 16);
    }

    // Take the one's complement
    sum = ~sum;

    return (unsigned short)sum;
}
```

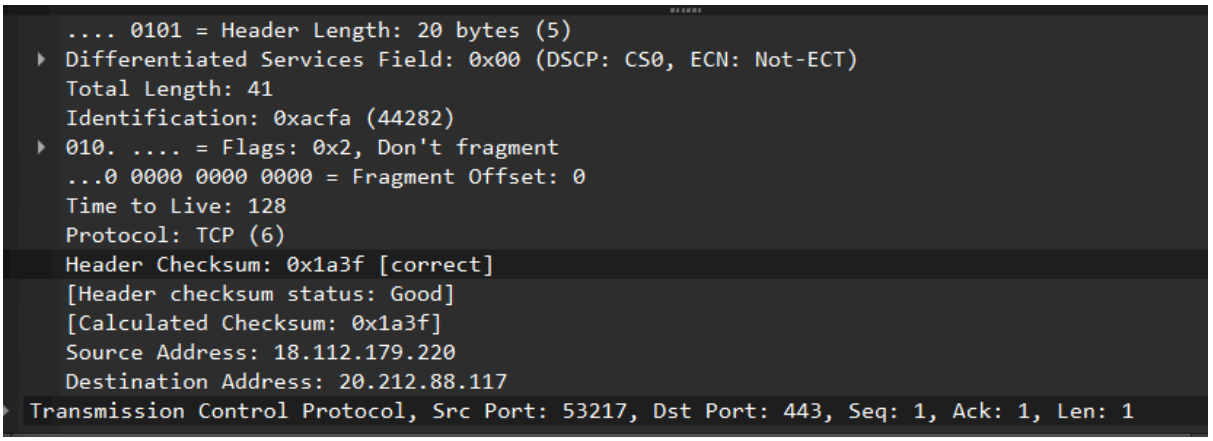
The IP checksum has been validated at the xyz.pcap (output file) indicating that it has been calculated correctly and ensures the integrity of the packets. The output of the checksum is as per screenshot below.



The header checksum of Frame 4 from abc.pcap (original).



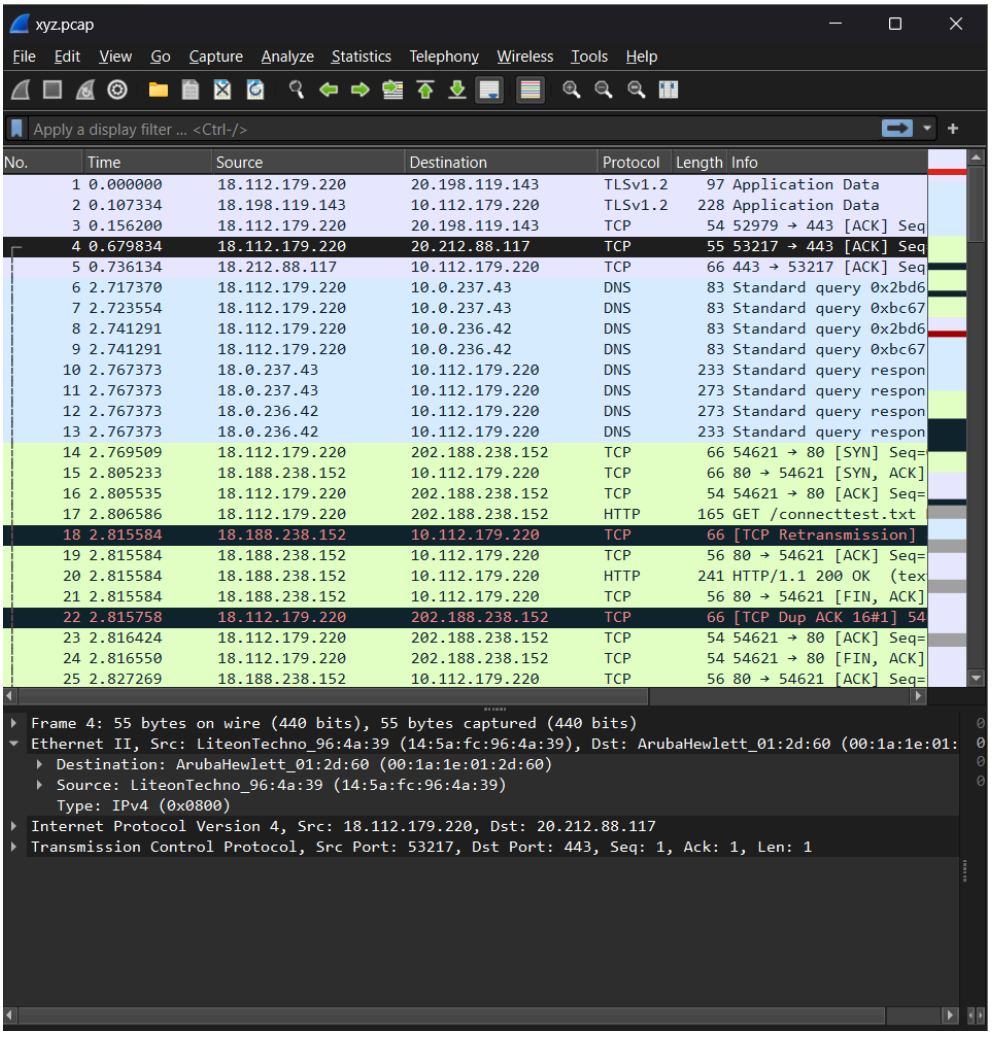

The header checksum of Frame 4 from xyz.pcap (modified IP source address).



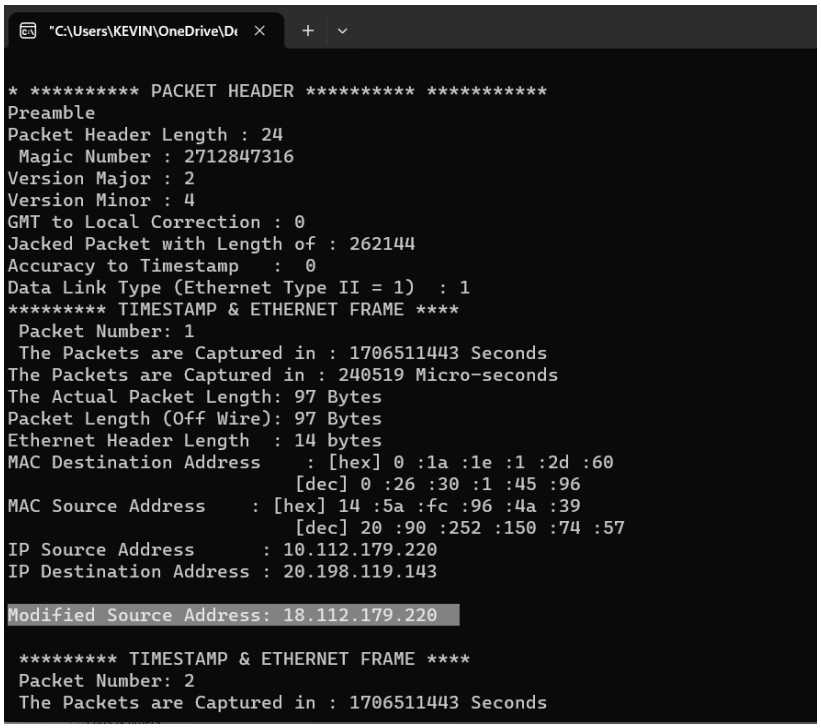

c) And rewrite the output into a file called xyz.pcap. (tcpdump format).

```
// Write the modified packet to the output file -> xyz.pcap
fwrite((char *)&tt, sizeof(tt), 1, output);
fwrite((char *)&eth, sizeof(eth), 1, output);
fwrite((char *)&ip, sizeof(ip), 1, output);

// Write the remaining data from the original packet
for (i = 0; i < tt.caplen - sizeof(eth) - sizeof(ip); i++)
{
    fread((char *)&buff, sizeof(buff), 1, input);
    fwrite((char *)&buff, sizeof(buff), 1, output);
}
```

The output of xyz.pcap file is as per below screenshot.

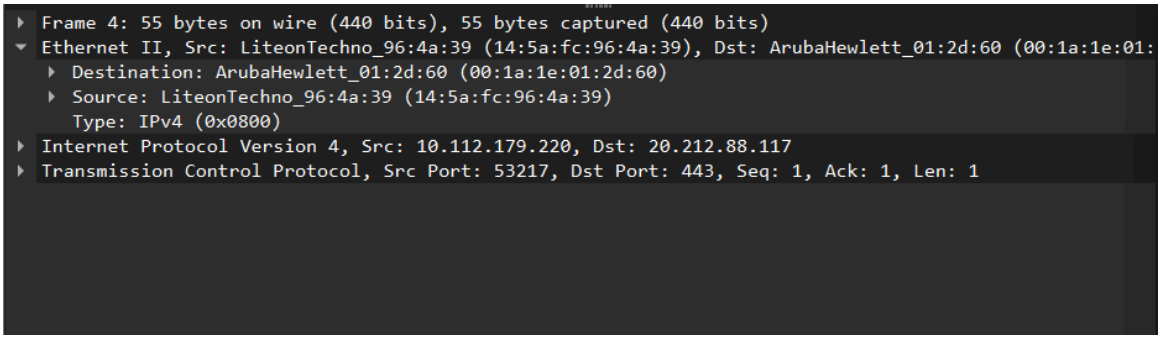



d) Display the modified IP source address to the console.



e) Additionally, the MAC address has been compared to make sure it is the same between the abc.pcap and xyz.pcap.

The MAC address of Frame 4 from abc.pcap.




The MAC address of Frame 4 from xyz.pcap.