

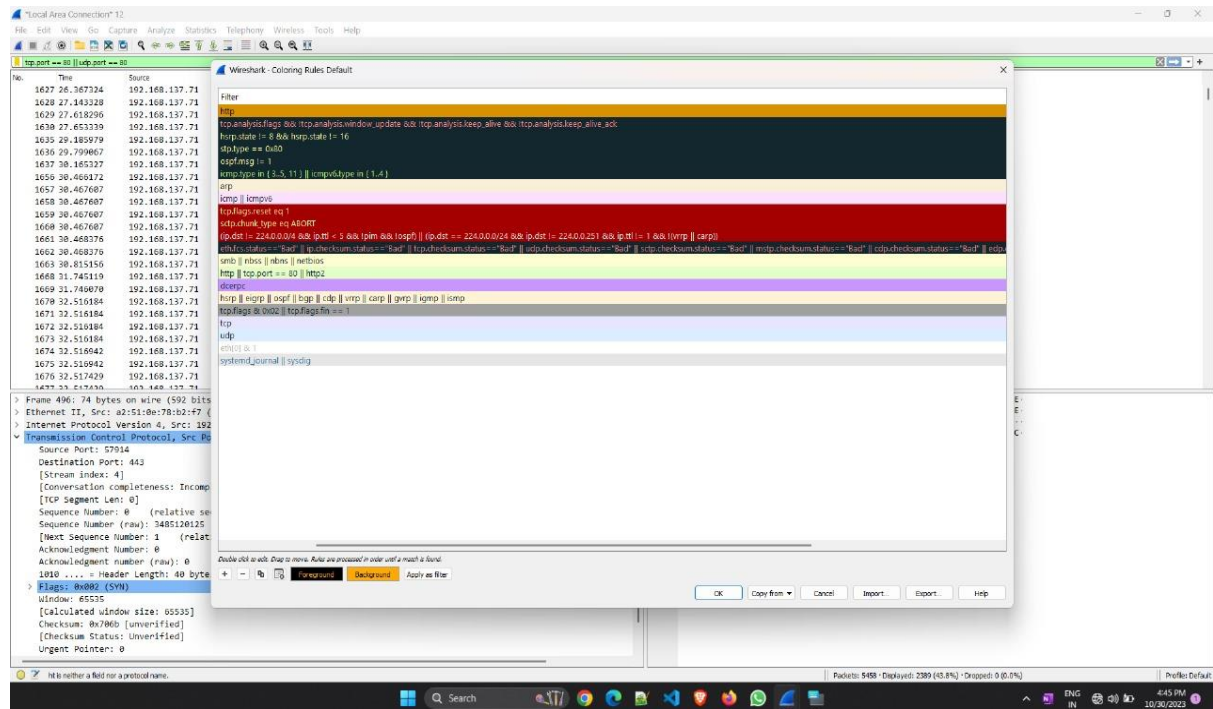
## PRACTICAL 7

\*packet sniffing (juno log in details)

Wireshark packet capture showing a login attempt. The selected packet is a POST request to /login.xml with application/x-www-form-urlencoded data. The packet details pane shows the form items: mode=191, username=chacherkards, password=Dhananjay@123, a=169847314779, and producttype=0. The packet bytes pane shows the raw data in hexadecimal and ASCII.

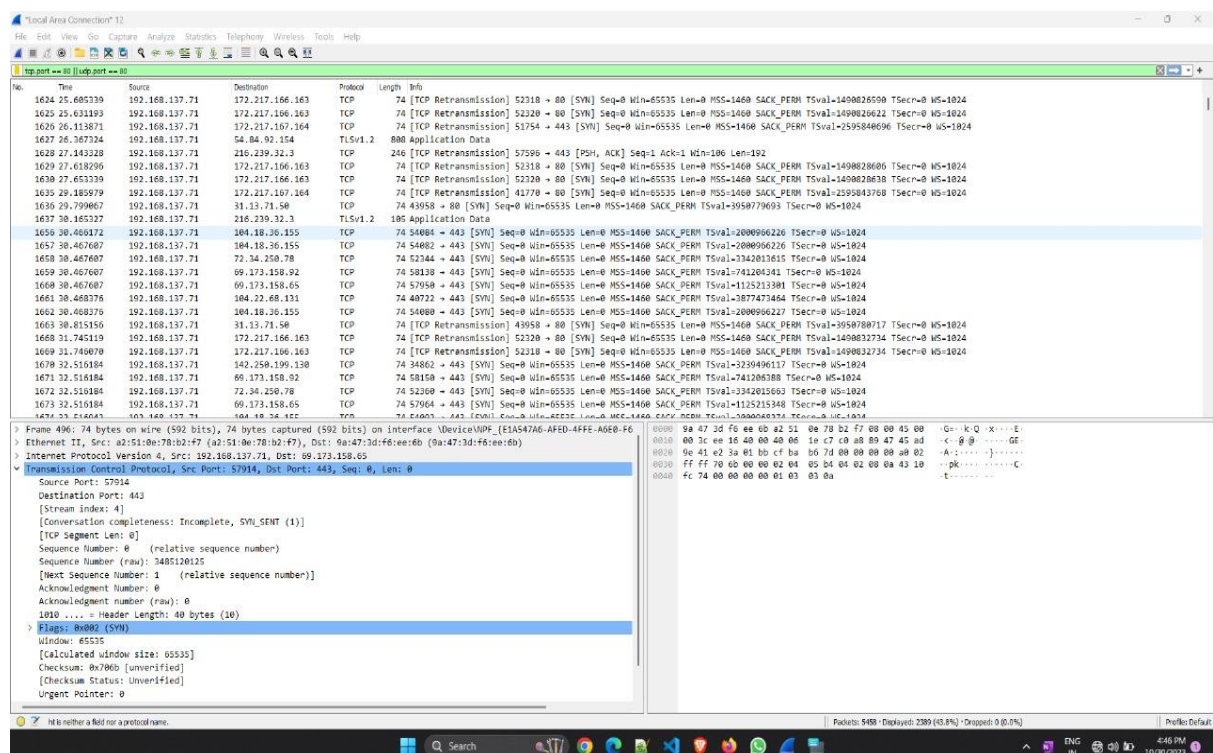
```
Sequence Number (raw): 2978542606
[Next Sequence Number: 825 (relative sequence number)]
Acknowledgment Number: 26421 (relative ack number)
Acknowledgment number (raw): 2638817644
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x990a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (473 bytes)
> Hypertext Transfer Protocol
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "mode" = "191"
    > Form item: "username" = "chacherkards"
    > Form item: "password" = "Dhananjay@123"
    > Form item: "a" = "169847314779"
    > Form item: "producttype" = "0"
```

## \*Color coding



## \*filters

1.tcp.port==80|udp.port==80



2.ip.addr==172.16.177.5

The image shows a Wireshark packet capture of a network traffic. The main pane displays a list of packets, with packet 2655 selected. The packet details pane shows the structure of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet is a reassembled TCP segment from 172.16.177.5 to 172.16.190.154. The packet is a JavaScript file named 'cyberowm.js'.

Packet 2655: Ethernet II, Src: D-Link(DC:81:40:04:80), Dst: ChongChin\_Fei(10:47:3d:fe:10:00:00), Protocol: TCP, Length: 1460. The packet is a reassembled TCP segment from 172.16.177.5 to 172.16.190.154. The packet is a JavaScript file named 'cyberowm.js'.

3.http

The image shows a Wireshark packet capture of a network traffic. The main pane displays a list of packets, with packet 2655 selected. The packet details pane shows the structure of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header. The packet is an HTTP GET request from 172.16.190.154 to 172.16.177.5. The request is for a file named 'cyberowm.js'.

Packet 2655: Ethernet II, Src: D-Link(DC:81:40:04:80), Dst: ChongChin\_Fei(10:47:3d:fe:10:00:00), Protocol: HTTP, Length: 1460. The packet is an HTTP GET request from 172.16.190.154 to 172.16.177.5. The request is for a file named 'cyberowm.js'.

