GETTING CSV FROM WIRESHARK

## 1. Changing Column Preferences

For the ML algorithms in the Analyser tool, the datasets have to be of a specific format. The column headers of the test dataset must consist of :

['Version', 'Protocol', 'TTL', 'SrcAddress', 'DestAddress', 'SrcPort', 'DestPort', 'SeqNum', 'AckNum', 'Flag', 'DataSize', 'Service'] in the same order.

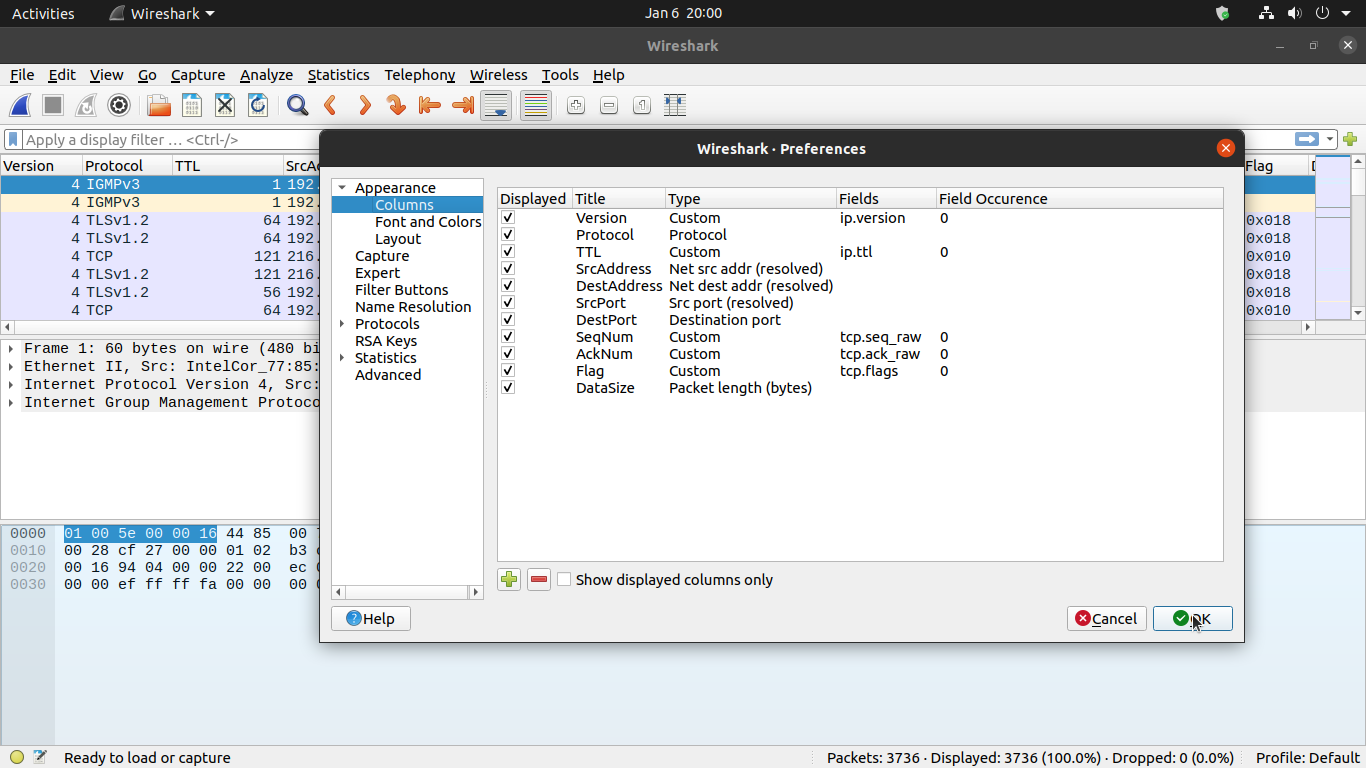
By default, Wireshark doesn’t display these columns.

To make Wireshark display these columns and save the capture file as csv follow the steps:

### 1.1 Right click on a column and choose “Column Preferences”

### 

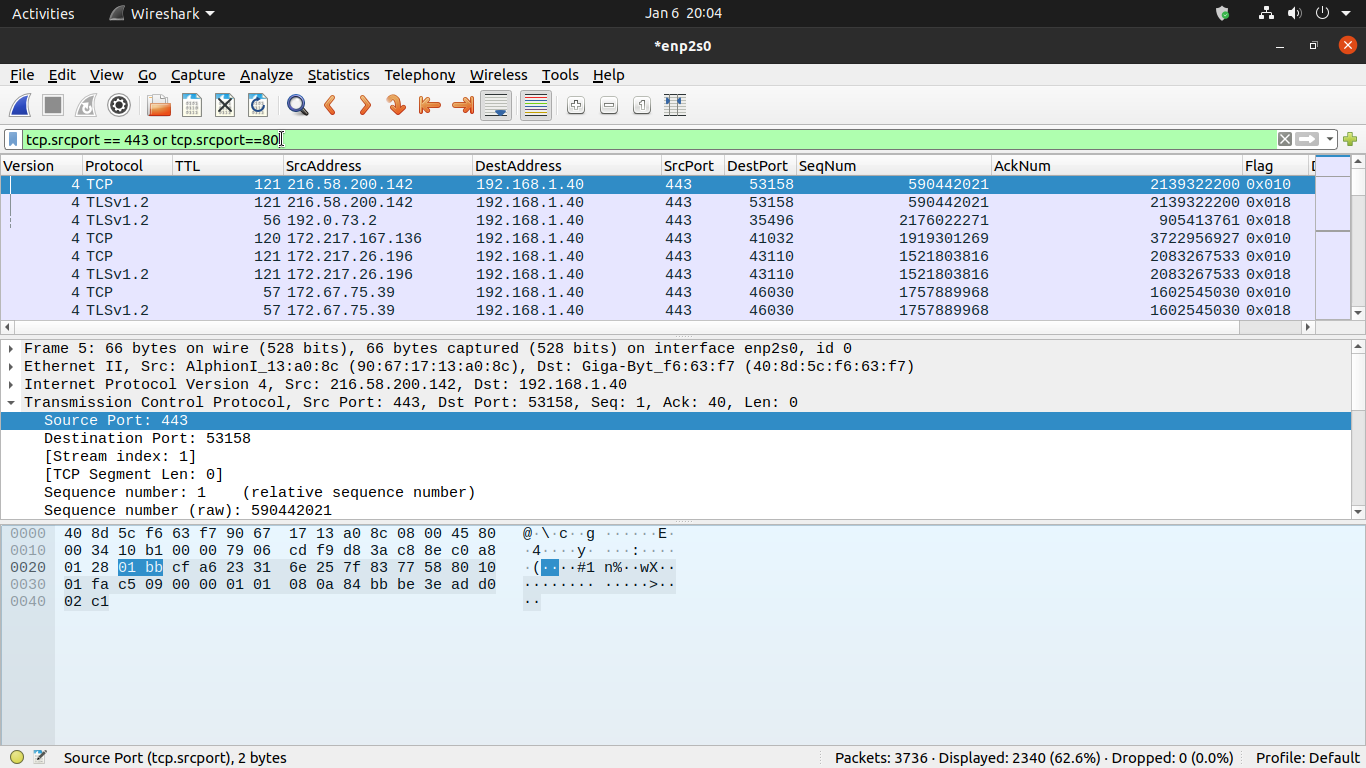
Edit the column preferences to this:



### 1.2 Filter HTTP and HTTPS packets

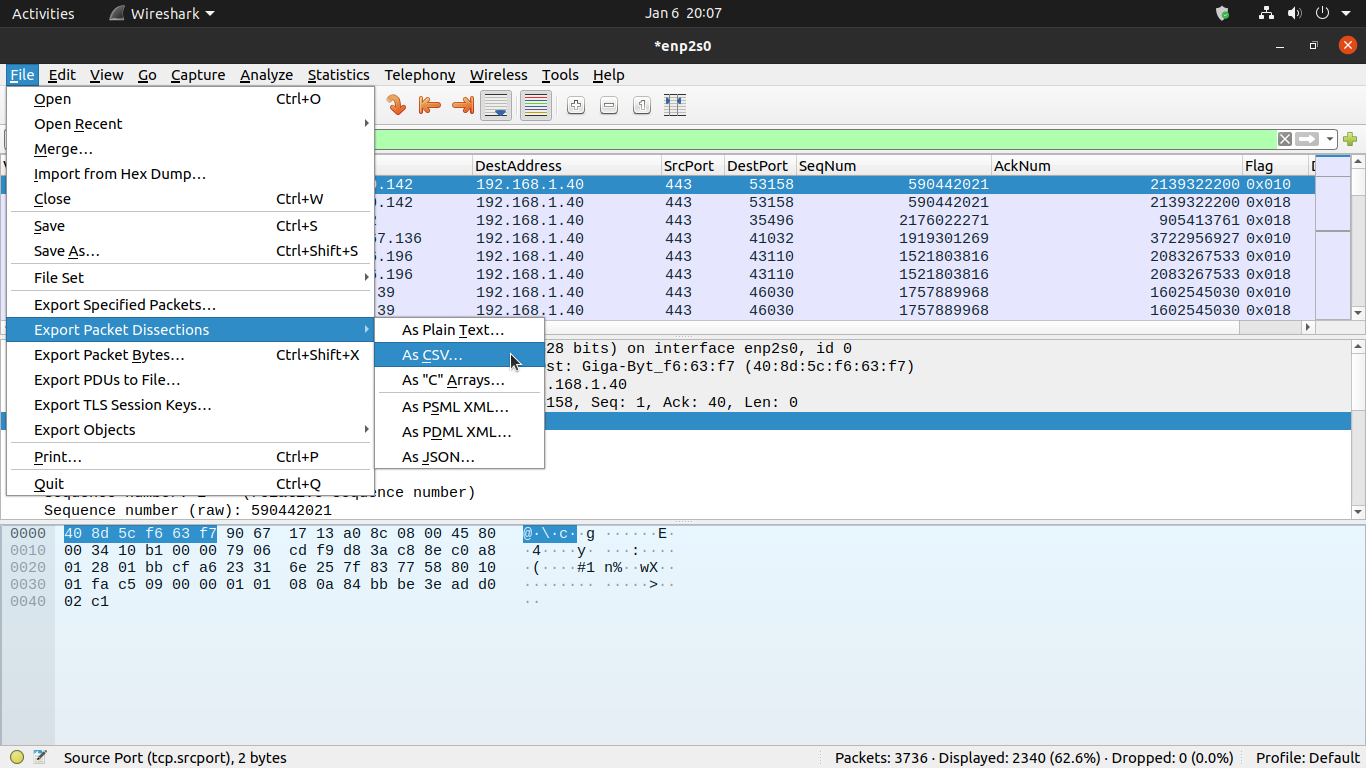
The tool is trained on HTTP and HTTPS packets. So filtering only HTTP and HTTPS packets would yield better accuracy.

Enter “tcp.srcport == 443 or tcp.srcport==80” in the display filter to filter the packets



## 2. Exporting to CSV

The tool needs the packets to be stored in .csv format. To export the Wireshark capture to CSV file click on File -> Export Packet Dissections -> As CSV



Enter the filename and click on save.