



CPIT-201

Networking Group Project (15%)

Packet Sniffing

H1 - Dr Mohammed AL Haddad - CPIT201

Group Members:

- **Faisal Bin Hassan - 2136143**
- **Mahmued Alardawi - 2135209**

- Submission Date: 10/26/2021

Table of Contents

Introduction	3
Computer Network	4
▪ Network Architecture	4
▪ Types Of Internet Protocols	6
▪ Internet Protocol (IP)	6
▪ PROTOCOLS	12
Wireshark Installation	13
Project Implementation	14
1) Captring TCP & HTTP Traffic To/From KAU Website	14
2) Capturing All Traffic To / From a YouTube Video	15
3) Capturing Group And Layers Information.	17
4) Packets That Are Transmitted To The KAU Website	19
5) Analyze The YouTube Packets Size	21
6) Random Packet That Is Transmitted From/To Your Computer	23
7) TCP Flags In The KAU Data Group	25
Conclusion	28
Appendix	29
References	29

Introduction

We'd like to welcome you on a journey filled with networking. While this time, we're going to face the computer's part of the network. In this booklet, you will find the following: -

- **Computer Networks (Discrete explanation)**
- **Protocol types**
- **Finding your own IP address**
- **Installing Wireshark**
- **Solving the Network Project**

By then, you'd be familiar with certain topics of network and the implementation of it in Wireshark.

**Best regards and wish you the best,
Faisal & Mahmued**

Computer Network

Network Architecture

Before we talk about types of internet protocols, let us talk about the primary layers of **Network Architecture**.

OSI model:

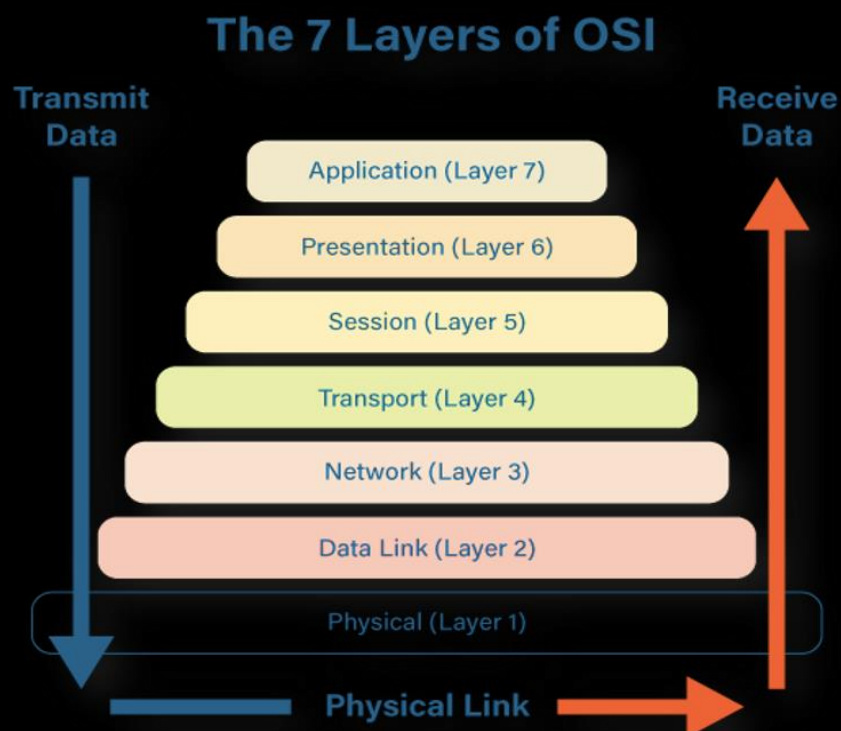
The **OSI** model stands for **Open System Interconnection Model**. **OSI** is a universal conceptual framework used to describe the functions of a networking system in 7-layers. This model published in 1984 by the **International Organization for Standardization (IOS)**.

OSI layers: -

1. **Physical Layer:** As its name says this layer is concerned with the physical matters like electricity or transmitting raw data. Its specifications such as voltages, cabling, etc.
2. **Data Link Layer:** this layer has two sub-layers of its own and they are: -
 - **Media access control layer (MAC):** provides flow control and multiplexing for device transmissions over a network.
 - **logical link control layer (LLC):** provides flow and error control over the physical medium as well as identifies line protocols.
3. **Network Layer:** This layer is responsible for receiving frames from the data link layer and delivering them to their intended destinations. The network layer finds the destination by using logical addresses, such as **internet protocol (IP)**.

4. **Transport Layer:** This layer manages the delivery and error checking of data packets. One of the most common examples of this layer is the **transmission control protocol (TCP)**.
5. **Session Layer:** This layer controls the conversations between different computers. also include authentication and reconnections.
6. **Presentation Layer (Syntax Layer):** this layer translates data for the application layer based on the syntax that the application accepts.
7. **Application Layer:** The application layer identifies communication partners, resource availability, and synchronizes communication. It is the application you use, such as the web browser, WhatsApp, etc.

In the following figure you will find it easy to understand the network 7-layers:



Types Of Internet Protocols

There is a substantial number of internet protocols. In this project we will only mention a bunch of them. For more information about this mater simply search on a web browser “types of internet protocols”.

Internet Protocol (IP): -

An **IP** address, or Internet Protocol address, is a series of numbers that identifies any device on a network. Computers use **IP** addresses to communicate with each other both over the internet as well as on other networks.

Extra information about **IP** addresses: -

1. There are two versions of **IP** addresses **IPv4** and **IPv6**. They summarized in the following figure:

IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses	7.9×10^{28} addresses
Addresses must be reused and masked	Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

2. **IP** address changeability: -

- **Static IP addresses:** A static IP address is simply an address that does not change. They used for servers or important equipment. They assigned by your **Internet Service Provider (ISP)**.
- **Dynamic IP Addresses:** As the name suggests, dynamic IP addresses are subject to change, sometimes at a moment's notice. They assigned by **Dynamic Host Configuration Protocol (DHCP)** servers.

3. **IP** address types: -

- **Private (local) IP address:** A private **IP** address is the address your network router assigns to your device. Each device within the same network is assigned a unique private **IP** address.
- **Private IP address ranges: -**
 - **Class A:** 10.0.0.0 – 10.255.255.255
 - **Class B:** 172.16.0.0 – 172.31.255.255
 - **Class C:** 192.168.0.0 – 192.168.255.255
- **Public (external) IP address:** Is an **IP** address that can be accessed directly over the internet and is assigned to your network router by your **Internet Service Provider (ISP)**.

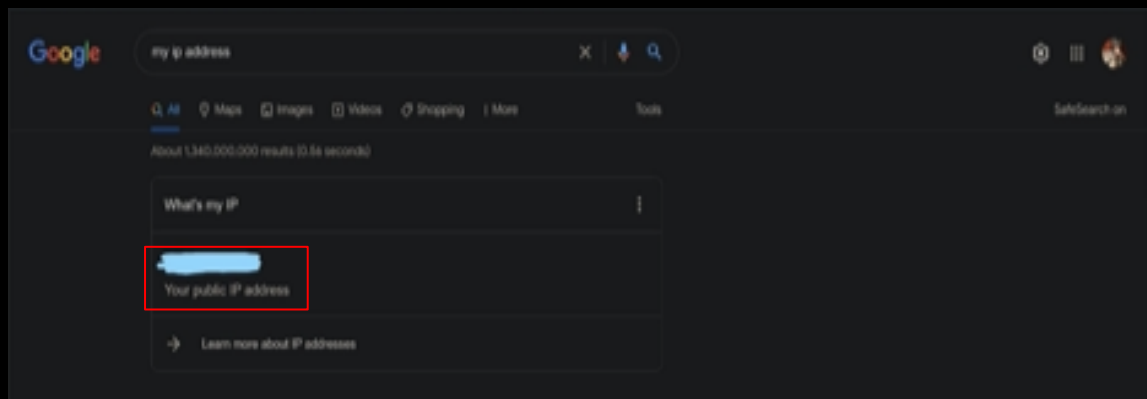
▪ **Public IP address vs Private IP address: -**



Public IP address	Private IP address
External (global) reach	Internal (local) reach
Used for communicating outside your private network, over the internet	Used for communicating within your private network, with other devices in your home or office
A unique numeric code never reused by other devices	A non-unique numeric code that may be reused by other devices in other private networks
Found by Googling: "What is my IP address?"	Found via your device's internal settings
Assigned and controlled by your internet service provider	Assigned to your specific device within a private network
Not free	Free
Any number not included in the reserved private IP address range Example: 8.8.8.8.	10.0.0.0 — 10.255.255.255; 172.16.0.0 — 172.31.255.255; 192.168.0.0 — 192.168.255.255 Example: 10.11.12.13

4. How to Find Your Public **IP** address: -

Simply type “what is my **IP** address” in the google search bar.



My public **IP** address is hidden for security reasons.

5. How to Find Your Private **IP** address: -

There is two ways to find your private **IP** address: -

- The first way is by the **Command Prompt (cmd)**. Just write “ipconfig” in the cmd.

```
Command Prompt

C:\Users\M7MQS>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

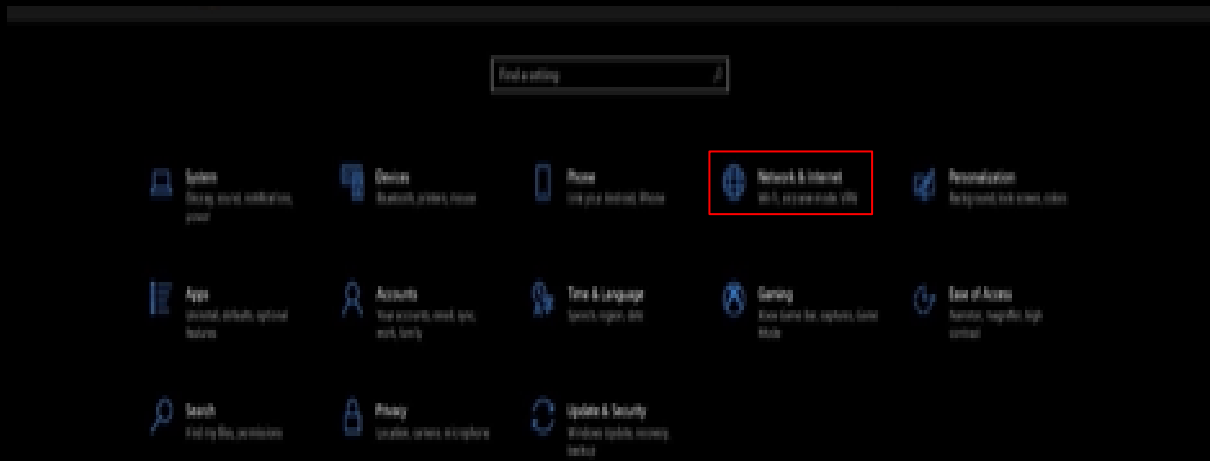
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::89d6:4aa3:2afa:8be9%8
    IPv4 Address. . . . . : 192.168.3.187
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.3.1

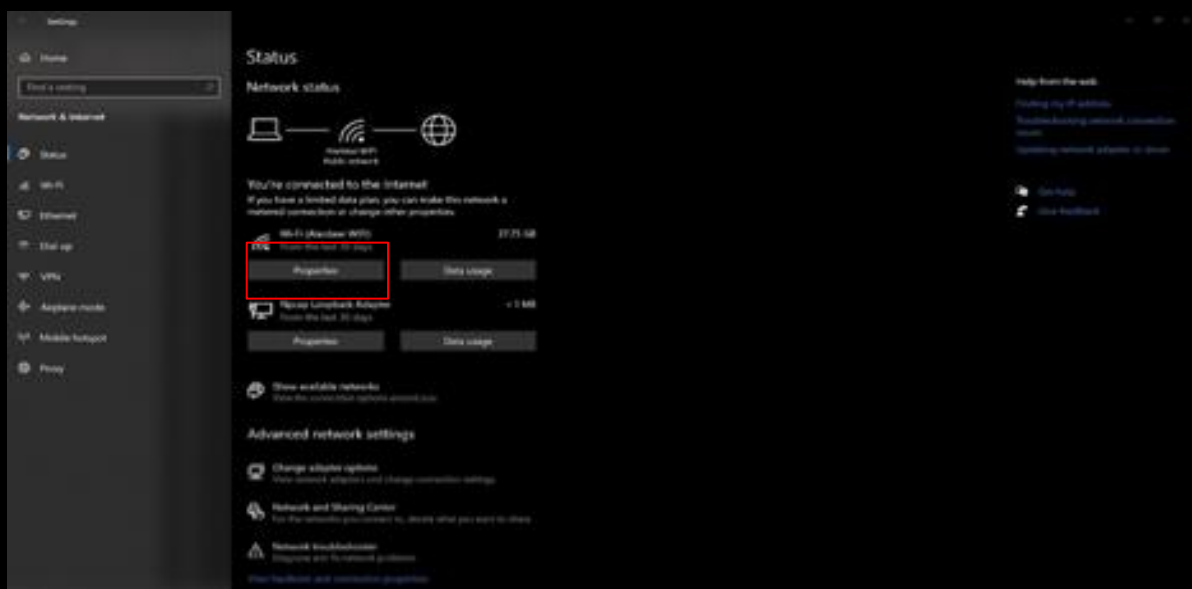
C:\Users\M7MQS>
```

- The second way is just for windows users: -

Enter on the network & internet settings.



From the “Status” menu Enter on the Wi-Fi or LAN proprieties.



Scroll down and you will Find your **IP** addresses.

The screenshot shows the Windows Settings application with the 'Alardawi WIFI' network selected. The 'IP settings' section shows 'Automatic (DHCP)' is selected. The 'Properties' section lists various network details. A red box highlights the 'Link-local IPv6 address' and 'IPv4 address' fields.

Settings

Alardawi WIFI

Set as metered connection
Off

If you set a data limit, Windows will set the metered connection setting for you to help you stay under your limit.

Set a data limit to help control data usage on this network

IP settings

IP assignment: Automatic (DHCP)
Edit

Properties

SSID: Alardawi WIFI
Protocol: Wi-Fi 5 (802.11ac)
Security type: WPA2-Personal
Network band: 5 GHz
Network channel: 36
Link speed (Receive/Transmit): 585/585 (Mbps)





Link-local IPv6 address: fe80:89d6:4aa3:2afa:8be9%9
IPv4 address: 192.168.3.187

IPv4 DNS servers: 192.168.3.1

Manufacturer: Realtek Semiconductor Corp.
Description: TP-Link Wireless USB Adapter
Driver version: 1030.38.712.2019
Physical address (MAC): 7C:C2:C6-0E-5C:80
Copy

Taskbar: Type here to search, Task View, File Explorer, Microsoft Edge, Google Chrome, Word, PowerPoint, Settings, Weather (32°C Sunny), Volume, Network, Date/Time (ENG 3:07 PM 10/25/2021).

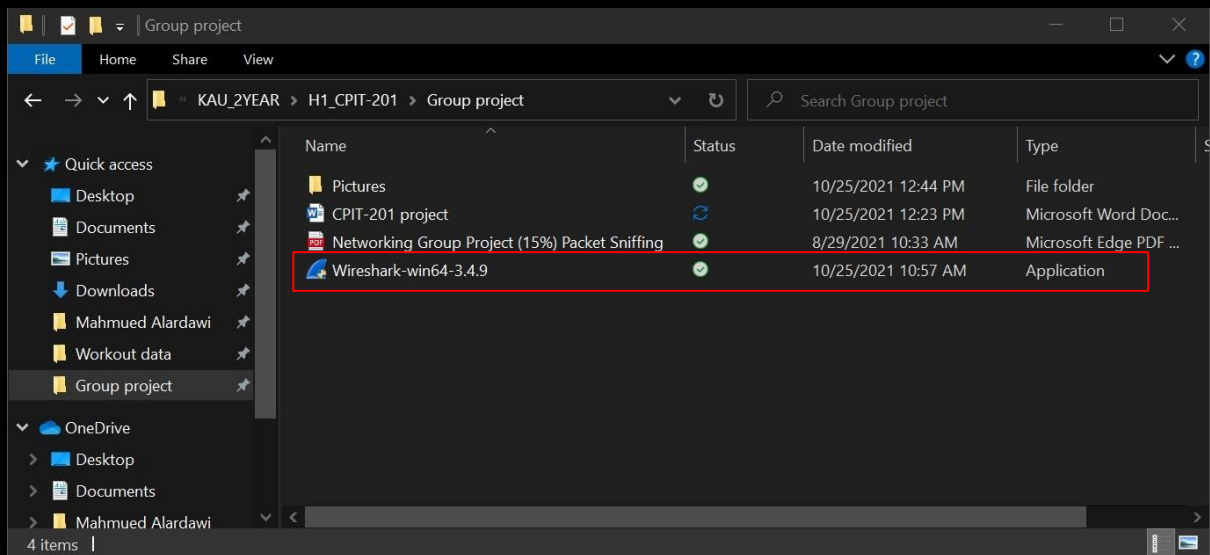
PROTOCOLS

-  **Transmission Control Protocol (TCP):** TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
-  **User Datagram Protocol (UDP):** UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
-  **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
-  **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems.

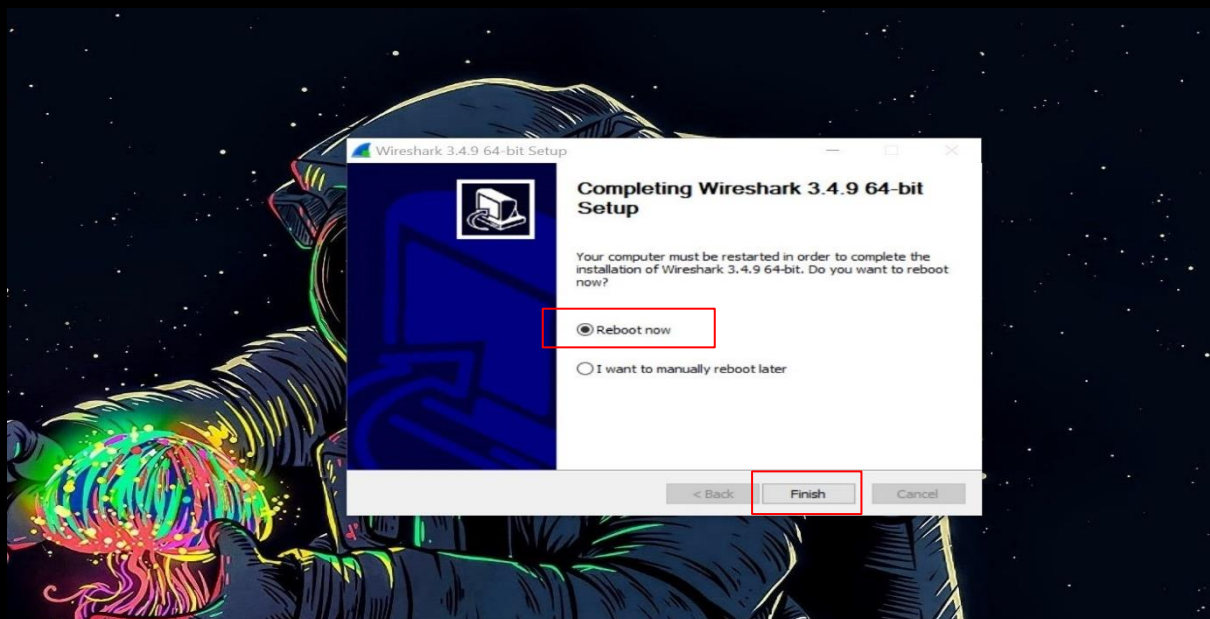
Wireshark Installation

Download Wireshark from (<http://www.wireshark.org/download.html>) and choose which download is suitable for your device.

Press on the downloaded application set-up.



Follow the given instruction until you get this reboot window. Then Press on reboot now and press finish after that.



After you rebooted you will find the Wireshark application installed.

2. Find a popular YouTube video and play it while capturing all traffic to/from YouTube and write the exact packet capture filter expressions.

- **Note:** Capture and save each traffic separately for easy analysis. For example, visit **KAU** website and capture the traffic then stop capturing and save the work. Then, visit **YouTube** and do the same.
- **Note:** By this step you will have two traffic capturing groups of **KAU** website, and **YouTube** video.

(2 - solution)

(YOUTUBE CAPTURED DATA. pcap)

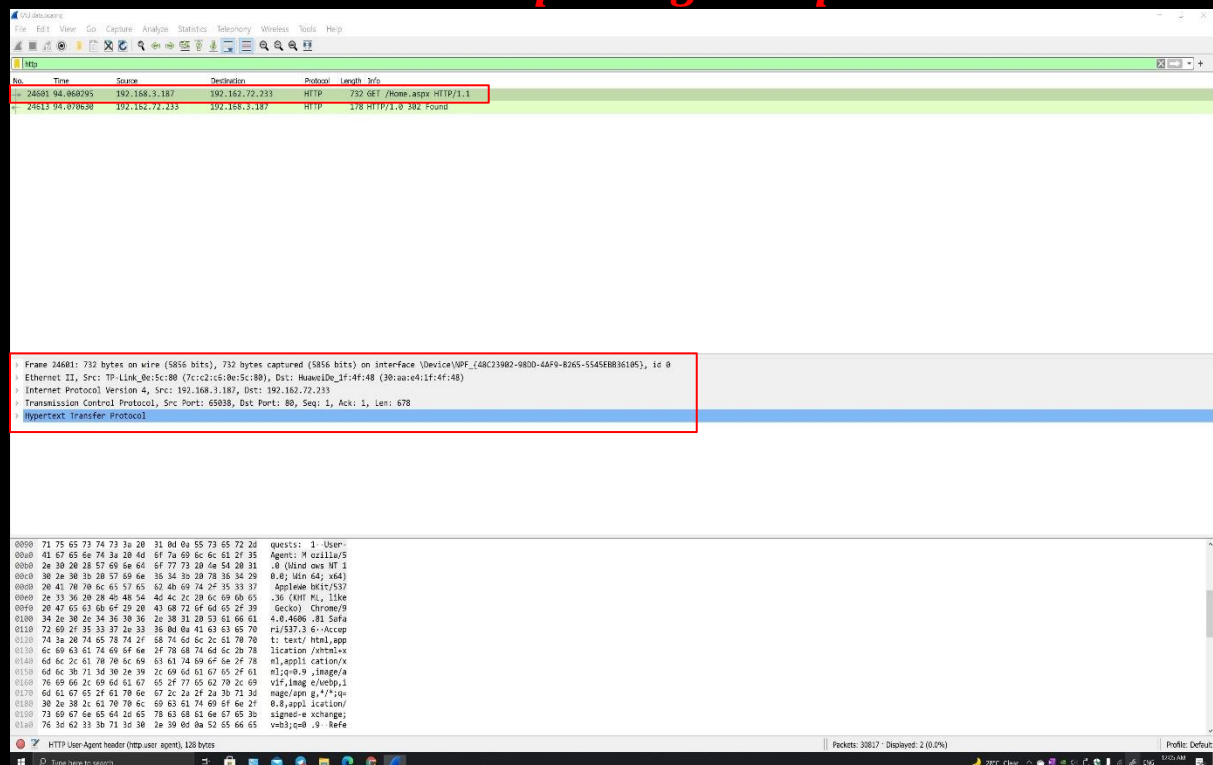
(DATA IN FILE!)

3. From each capturing group, click on the traffic line (pick only one that has all the 5 layers information i.e., physical, data link, network, transport, and application layer) to view the following information, **mark the answers on the screen shots, then write them down on Table1: -**

- **Layer 1:** Physical shows bits on the wire (i.e., Record the frame length)
- **Layer 2:** Data Link shows an Ethernet frame with MAC addresses (i.e., Record the source and destination MAC address)
- **Layer 3:** Network shows an IP packet with IP addresses (i.e., Record the IP address of the source and destination)
- **Layer 4:** Transport shows TCP/UDP segments with port numbers (i.e., Record the source and destination ports)
- **Layer 5:** Application layer shows used application (i.e., Record the protocol's name that have been used in this layer)

(3 - solution)

KAU Capturing Group



YouTube Capturing Group

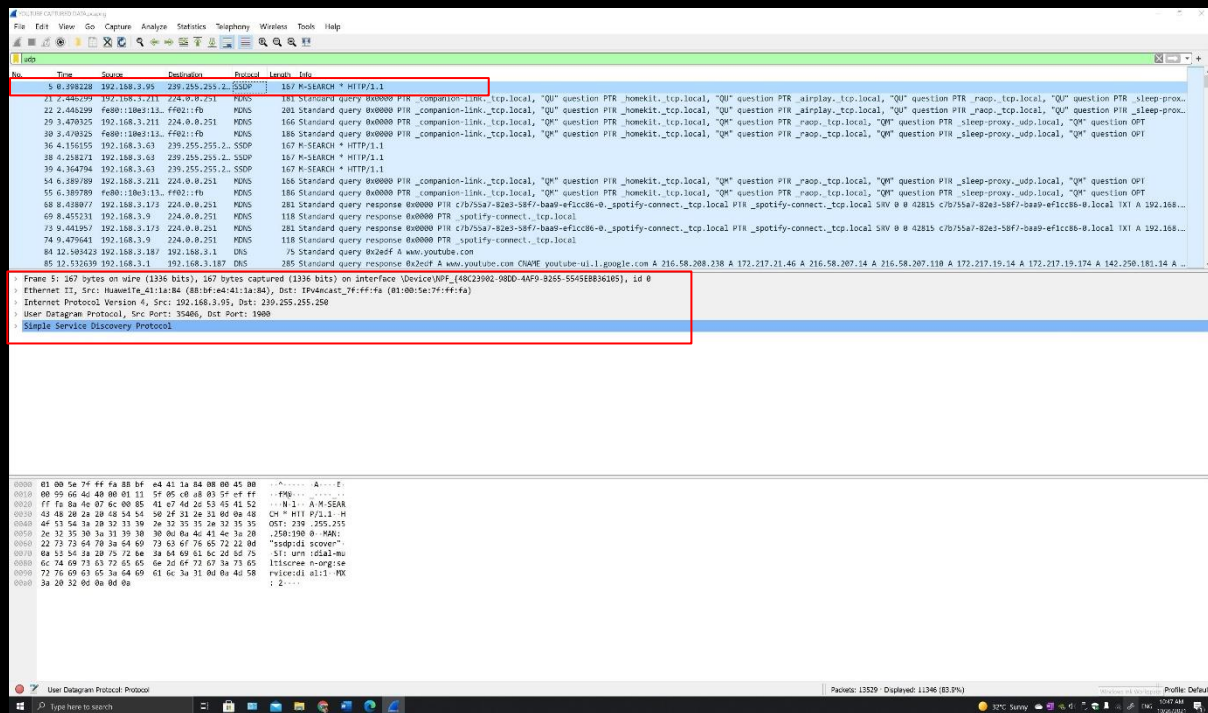


Table1

Layers	KAU Group	YouTube Group
Layer1: Physical	Frame length = 732 bytes on wire (5856 bits)	Frame length = 167 bytes on wire (1336 bits)
Layer2: Data Link	Src MAC address = 7c:c2:c6:02:5c:80 Dst MAC address = 30:aa:e4:1f:4f:48	Src MAC address = 88:bf:e4:41:1a:84 Dst MAC address = 01:00:5e:7f:ff:fa
Layer3: Network	Src IPv4 address = 192.168.3.187 Dst IPv4 address = 192.162.72.233	Src IPv4 address = 192.168.3.95 Dst IPv4 address = 239.255.255.250
Layer4: Transport	TCP Src port number = 65038 TCP Dst port number = 80	UDP Src port number = 35406 UDP Dst port number = 1900
Layer5: Application	Hyper Text Transfer Protocol (HTTP)	Simple Service Discovery Protocol (SSDP)

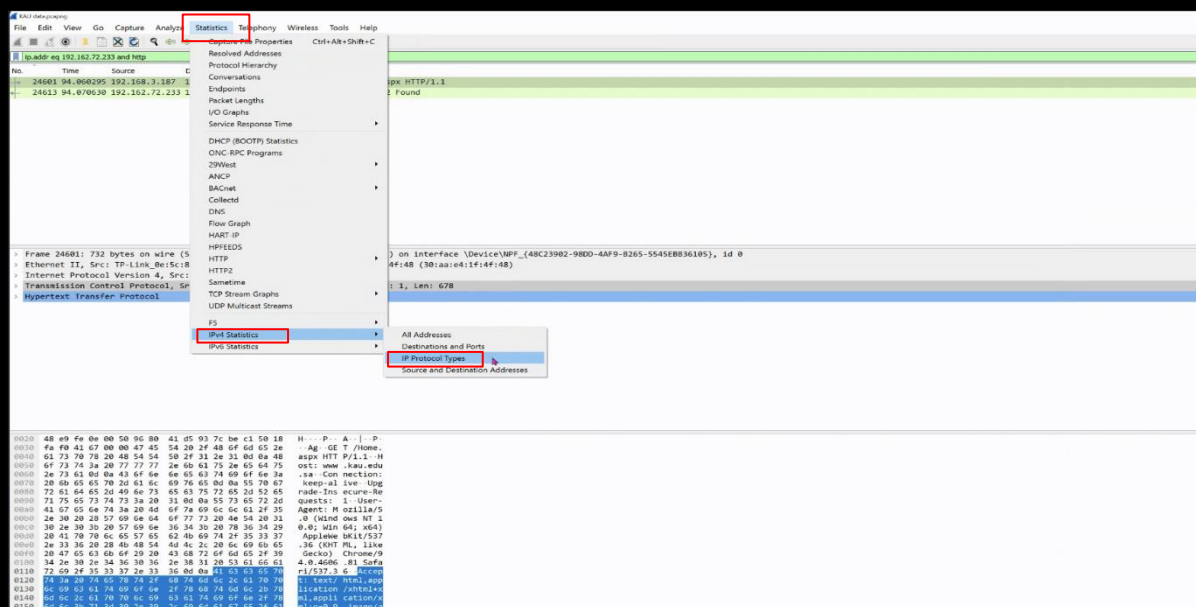
4. Find the following packets that are transmitted to the KAU website (Hint: KAU IP address is 192.162.72) by using the proper display filter expression; **Report the answers with screen shot that show how you figure them out?**

4.1 Number of packets with all transmission control protocol (TCP).

Step1: Do as shown in the image then a window will pop.

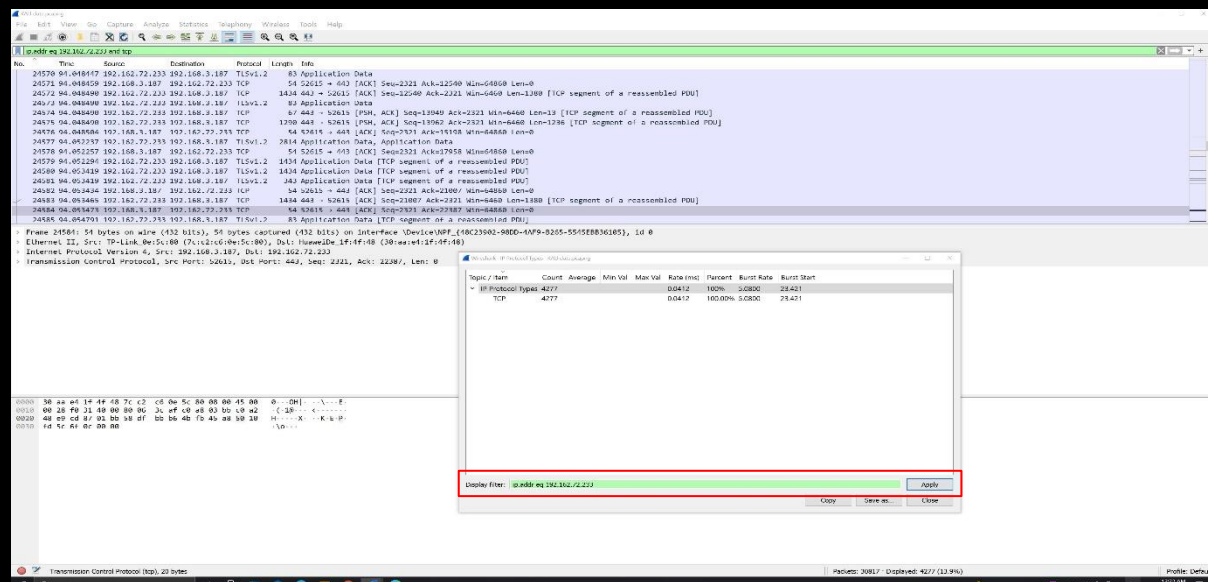
(4.1 - solution)

Step1: Do as shown in the following image.



Step2: Use filters expressions in to solve (4.1).

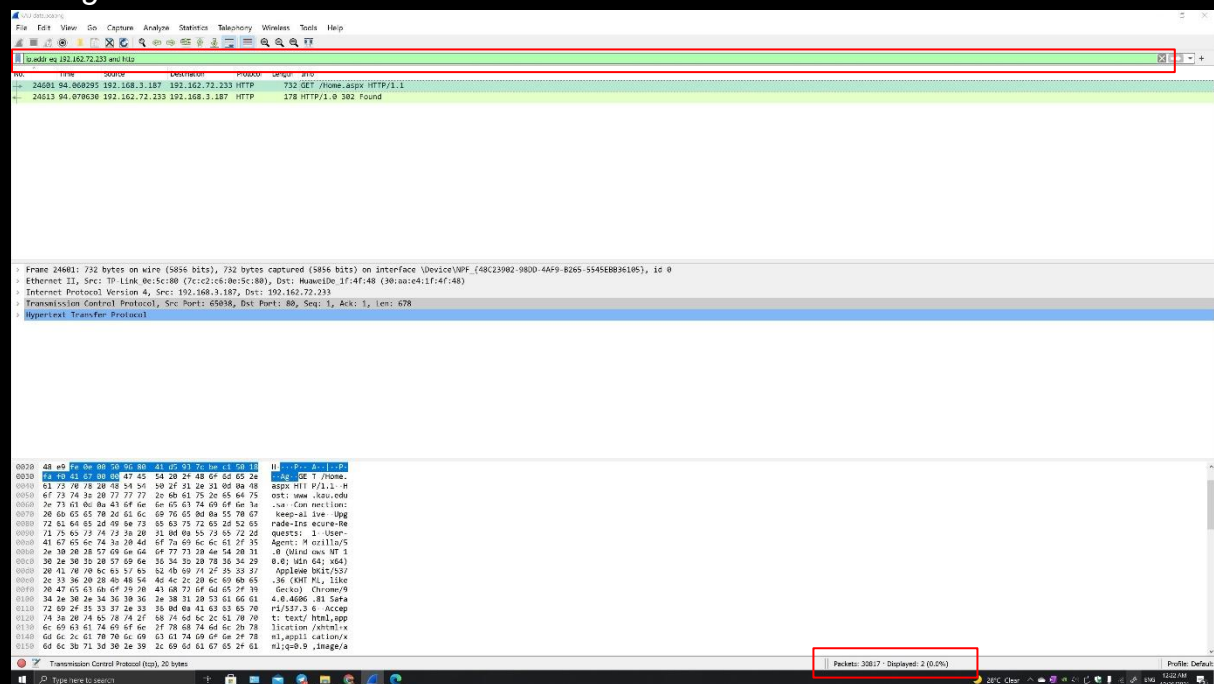
The filter is "ip.addr eq 192.162.72.233" the last number (233) is changeable.



4.2 Number of packets with all hypertext transmission protocol (HTTP).

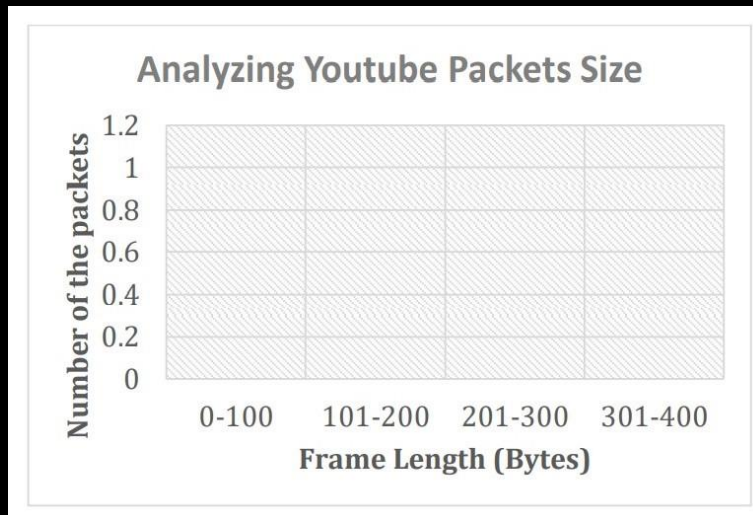
(4.2 - solution)

The filter is "ip.addr eq 192.162.72.233 and http" the last number (233) is changeable.



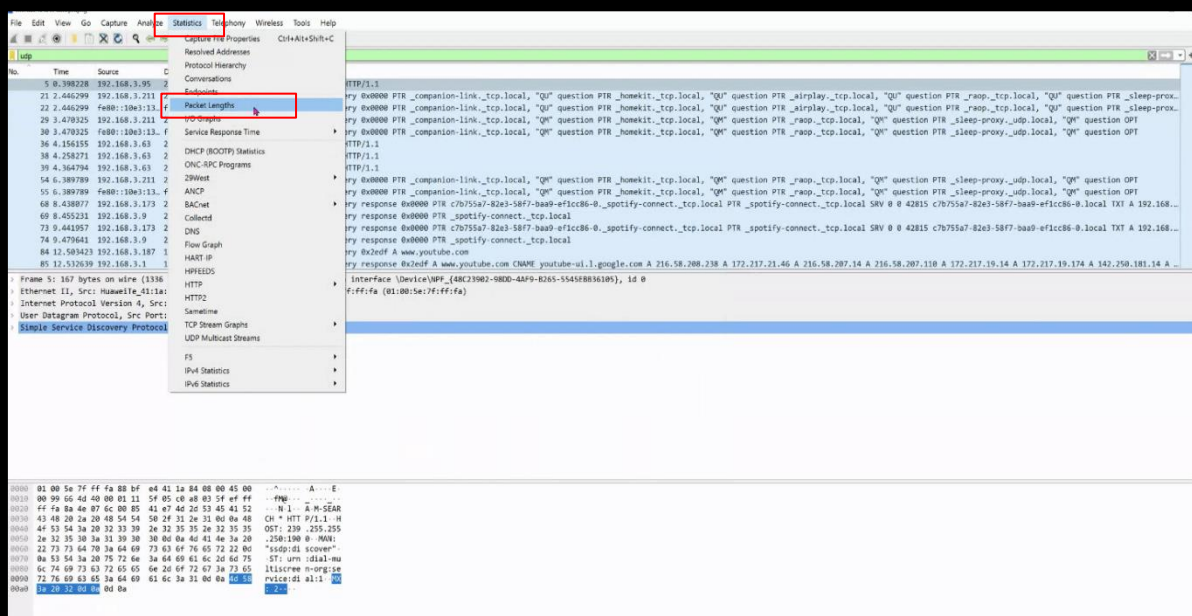
5. Analyse the YouTube packets size. Draw a chart that shows how many packets are fallen within different range of sizes. For example, packet with size 50 bytes belongs to a frame length group (0-100); packet with 120 bytes belongs to frame length group (101-200). **Please use the following chart to represent your answer.**

Chart example

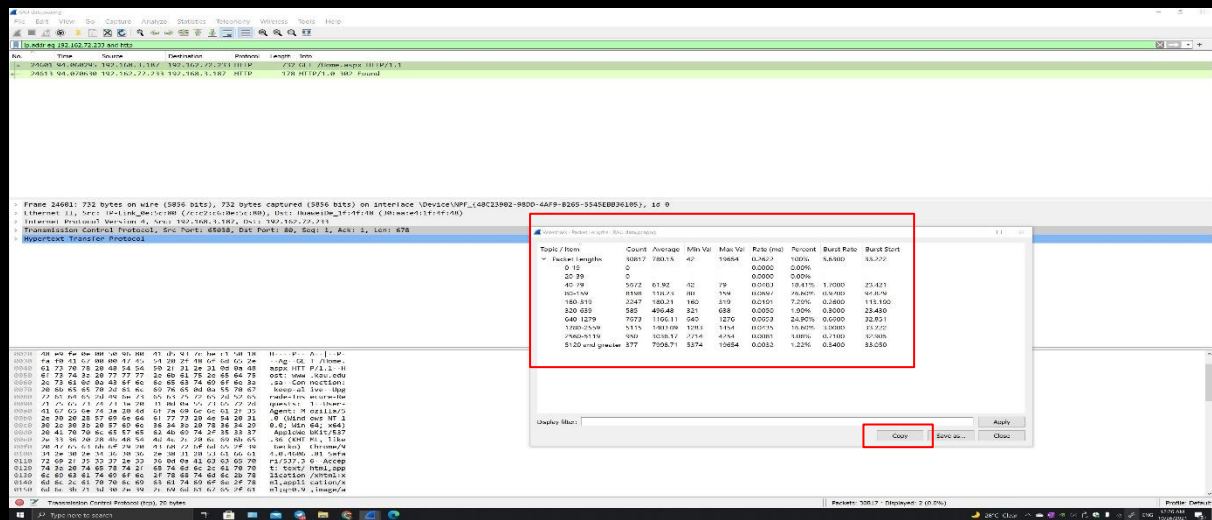


(5 - solution)

Step1: Do as shown in the following image.



Step2: Take the shown Data from **Wireshark** and analyse them in **Excel**.



Data acquired

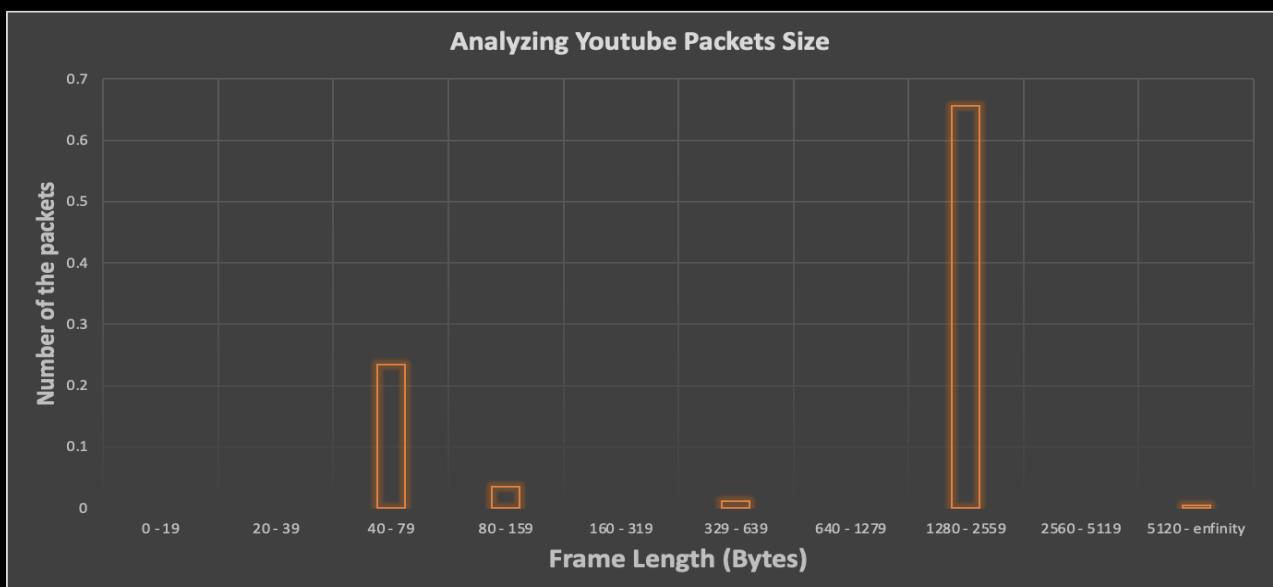
Packets Length - Youtube - Notepad

File Edit Format View Help

Packet Lengths:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	13529	1064.32	42	47654	0.0794	100%	6.1700	52.306
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	3164	67.57	42	79	0.0186	23.39%	1.2600	22.207
80-159	470	107.52	80	159	0.0028	3.47%	0.2000	14.196
160-319	364	196.05	160	313	0.0021	2.69%	0.5200	14.371
320-639	165	504.85	320	635	0.0010	1.22%	0.1200	13.344
640-1279	231	841.47	641	1275	0.0014	1.71%	0.1400	22.456
1280-2559	8882	1394.04	1289	1454	0.0521	65.65%	5.4700	52.306
2560-5119	184	3059.43	2854	4254	0.0011	1.36%	0.4000	13.087
5120 and greater	69	12187.33	5654	47654	0.0004	0.51%	0.4100	13.243

Wanted Chart



6. Select random packet that is transmitted from/to your computer and record the following information: - **(Please take a screenshot and show your work on it).**

- 6.1 **What the exact filter that have been used?**
- 6.2 **No:** Packet Number
- 6.3 **Time:** Time in seconds that the frame was captured
- 6.4 **Source:** Source address of the frame
- 6.5 **Destination:** Destination address of the frame
- 6.6 **Protocol:** Protocol of the frame

(6.1 - solution)

Step1: find your **IP** address and your **Gateway** address from the **cmd**.

The filter is “ip.addr eq 192.168.3.187 and ip.addr eq 192.168.3.1”, this filter is my

The screenshot displays two windows. The top window is Wireshark, showing a packet capture filter: `ip.addr eq 192.168.3.187 and ip.addr eq 192.168.3.1`. The packet list shows several DNS queries and responses. The bottom window is a Windows Command Prompt showing the output of the `ipconfig` command, which displays the network configuration for the Ethernet adapter. The IP address is `192.168.3.187` and the Default Gateway is `192.168.3.1`.

```

Microsoft Windows [Version 10.0.19042.1200]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HMK>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 
   Ethernet adapter Realtek USB Ethernet:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 
   Link-local IPv6 address . . . . : fe80::a8b1:5060:4238:9439d
   IPv4 Address. . . . . : 192.168.3.187
   Subnet Mask . . . . . : 255.255.0.0
   Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 
   Wireless LAN adapter Local Area Connection* 12:

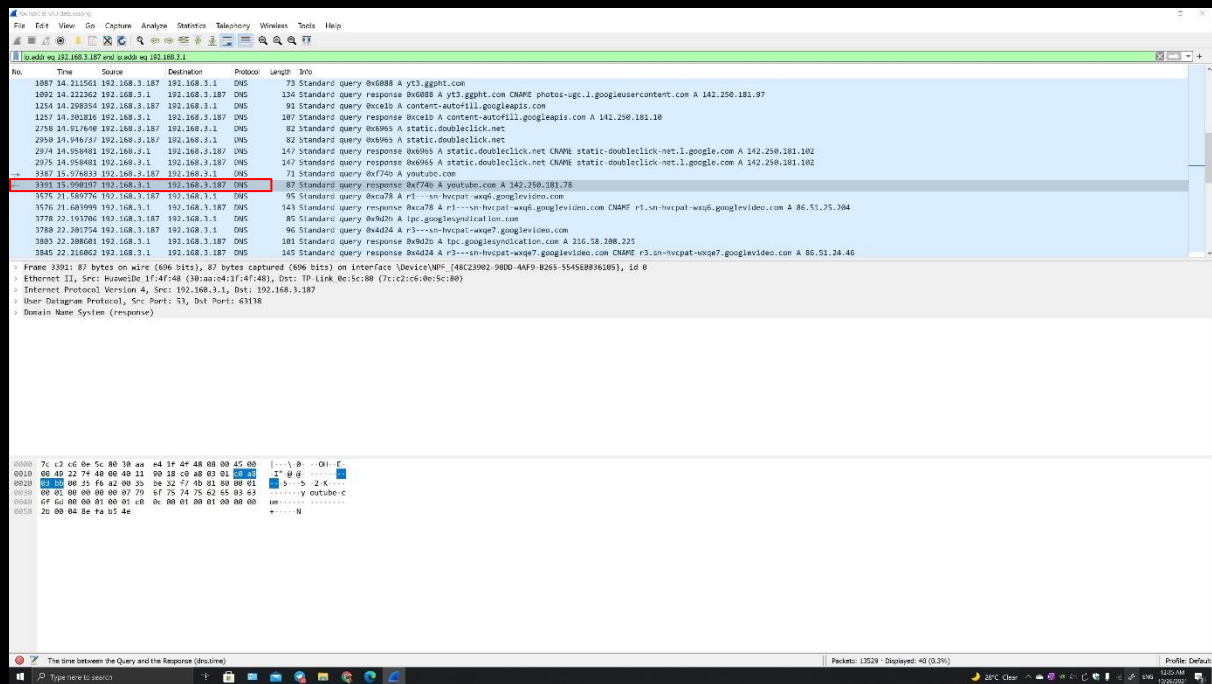
   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 
   Wireless LAN adapter Wi-Fi:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 
   Link-local IPv6 address . . . . : fe80::8381:aaaf:1afa:8a750
   IPv4 Address. . . . . : 192.168.3.187
   Subnet Mask . . . . . : 255.255.0.0
   Default Gateway . . . . . : 192.168.3.1

C:\Users\HMK>
  
```

IPv4 address and my Default Gateway address.

(6.2 -> 6.6 - solution)



Q/A Table

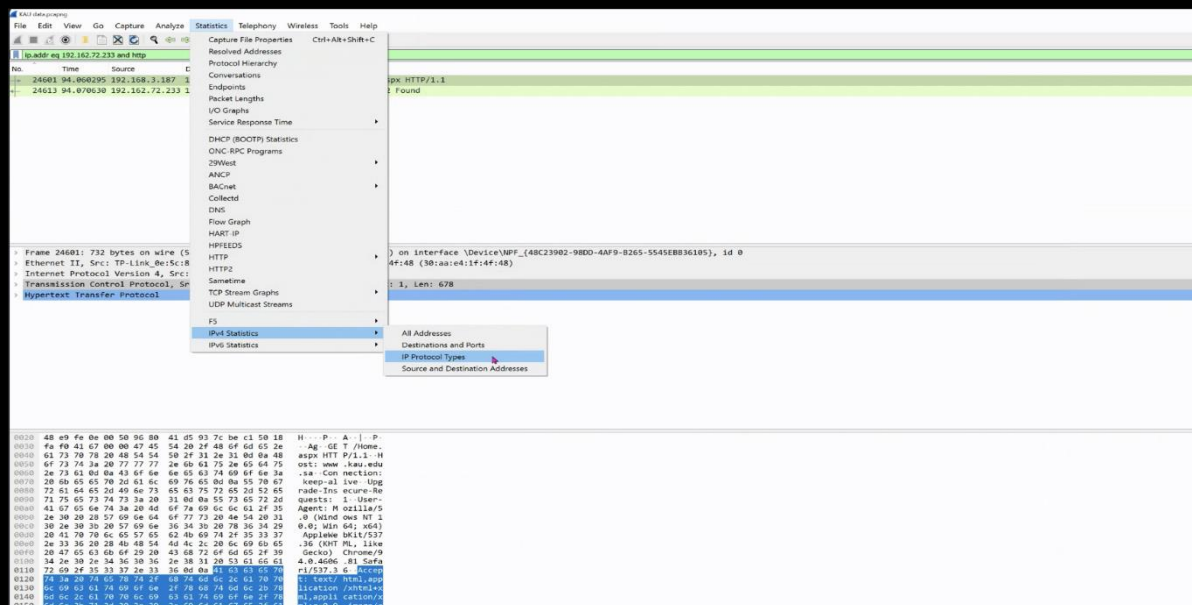
Questions	Answer
2. No	3391
3. Time	15.990197
4. Source	192.168.3.1
5. Destination	129.168.3.187
6. Protocol	IP, UDP, DNS

7. From the data that you collected from question B.1 (KAU group). Count all TCP packets that have the flags **SYN**, **PSH**, or **RST** set that were sent from your host by using the proper display filter expression. *(Please take a screenshot and show your work on it as well as report all three counts in a table)*

For more information visit this link: <https://www.keycdn.com/support/tcpflags>

(7 - solution)

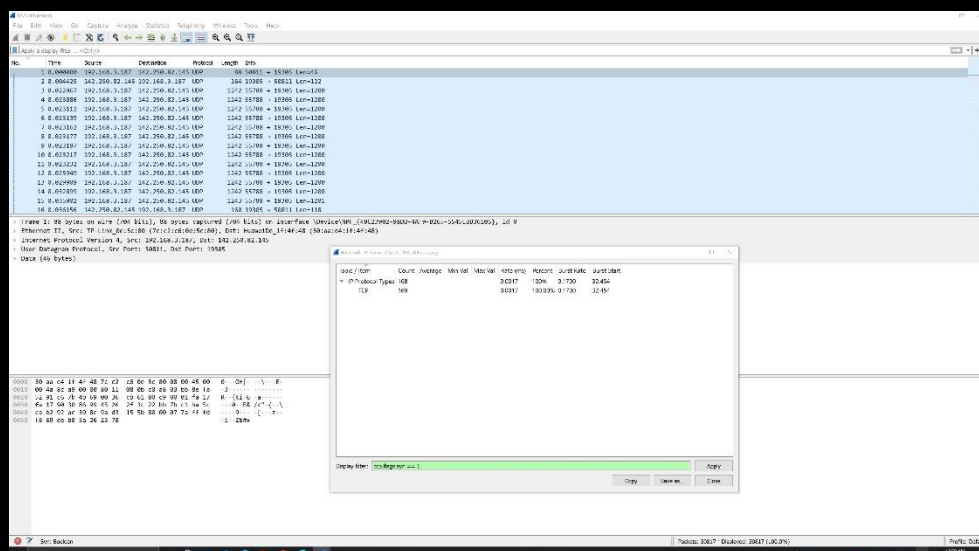
Step1: Do as shown in the image.



Step2: Use filtering expressions to find the **TCP flags.**

The images are using filters to find the wanted flags: -

SYN filtering expression is "tcp.flags.syn == 1".



PSH filtering expression is `"tcp.flags.push == 1"`.

The screenshot shows the Wireshark interface with a packet capture of 16 UDP packets. A display filter `tcp.flags.push == 1` is applied, resulting in 0 packets displayed. A packet details pane for packet 16 is visible, showing Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (46 bytes). A packet bytes pane shows the raw data in hexadecimal and ASCII. A statistics window is open, showing the protocol distribution: IP Protocol Types (2666) and TCP (2666).

RST filtering expression is `"tcp.flags.reset == 1"`.

The screenshot shows the Wireshark interface with a packet capture of 16 UDP packets. A display filter `tcp.flags.reset == 1` is applied, resulting in 0 packets displayed. A packet details pane for packet 16 is visible, showing Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (46 bytes). A packet bytes pane shows the raw data in hexadecimal and ASCII. A statistics window is open, showing the protocol distribution: IP Protocol Types (15) and TCP (15).

Count Table

TCP flags	Count	Filtering expression
ACK	9715	Tcp.flags.ack == 1
SWR	0	Tcp.flags.swr == 1
ECN	0	Tcp.flags.ecn == 1
FIN	72	Tcp.flags.fin == 1
NS	0	Tcp.flags.ns == 1
PUSH(PSH)	2666	Tcp.flags.push == 1
RES	0	Tcp.flags.res== 1
RESET(RST)	15	Tcp.flags.reset== 1
STR	0	Tcp.flags.str == 1
SYN	168	Tcp.flags.syn == 1
URG	0	Tcp.flags.urg == 1

CONCLUSION

With all thanks and regards to the coordinators of this course. We as a group, got to not only maintain a solid scheme of idea on TCP flags, protocol types and the different layers of it. We've got to implement it and get a closer look at the application parts of it. By using our universities website, we got to see the HTTP, on the other hand, we got to see different protocol types when capturing the YouTube video.

APPENDIX FILES

 (KAU CAPTURED DATA. pcap)

 (YouTube CAPTURED DATA. pcap)

(DATA IN FILES!)

REFERENCES

- <https://osqa-ask.wireshark.org/questions/20423/pshack-wireshark-capture/>
- <https://osqa-ask.wireshark.org/questions/24961/filter-for-syn-psh-and-rst-flags/>
- <https://www.keycdn.com/support/tcp-flags>
- <https://www.fieldengineer.com/blogs/what-is-a-computer-network>
- <https://www.geeksforgeeks.org/basics-computer-networking/>
- <https://www.javatpoint.com/computer-network-tcp-ip-model>
- <https://www.guru99.com/tcp-ip-model.html>
- <https://www.forcepoint.com/cyber-edu/osi-model>
- <https://www.youtube.com/watch?v=cNwEVYkx2Kk>
- <https://www.youtube.com/watch?v=AEaKrQ3SpW8>