# Writing Wireshark filter expressions for packet capture

Group Members:
Zafran Ullah, Ihsan Ali,
Babar Naseer

# Wireshark

- **Wireshark** is a free and open-source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.

# Wireshark

- Two types of filter expressions are used in wireshark
  - Capture filter
  - Display filter

# Tasks

- Task1: Capturing and analyzing TCP packets
- Task2: Capturing and analyzing http packets
- Task3: Capturing and analyzing packets from PLAYIT.PK

# Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

- Facebook ip = **31.13.86.8**
- User ip =**10.110.161.147**
- Capture Filter: **tcp and host 31.13.86.8**
- Packets Captured: **643 over 25 seconds**
- Packets sent to facebook: **252**

  Display Filter: **ip.dst==31.13.86.8**
- Packets received from facebook: **391**

  Display Filter: **ip.dst==10.110.161.147**

# SYN Flag

- The SYN flag synchronizes sequence numbers to initiate a TCP connection

# Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

- **SYN Flag:**

For packets with SYN flag set

Display filter: **tcp.flags.syn==1 ,** Packets: **5**

For packets with SYN flag not set

Display filter: **tcp.flags.syn==0 ,** Packets: **638**

Number of packets with SYN set & sent to host:

Display filter :**tcp.flags.syn==1 && ip.dst==10.110.161.147 ,**

Packets:**1**

Number of TCP packets with SYN flag set and sent to Facebook:

Display filter: **tcp.flags.syn==1 && ip.dst== 31.13.86.8 ,**
Packets:**4**

# PUSH

- PSH- Push forces data delivery without waiting for buffers to fill. This is used for interactive traffic. The data will also be delivered to the application on the receiving end with out buffering.

# Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

- **PSH Flag:**

For packets with PUSH flag set

Display filter: **tcp.flags.push==1 ,** Packets: **250**

For packets with PUSH flag not set

Display filter: **tcp.flags.push==0 ,** Packets:**393**

Number of packets with PUSH set & sent to host:

Display filter :**tcp.flags.push==1 && ip.dst==10.110.164.135 ,**

Packets:**156**

Number of TCP packets with PUSH flag set and sent to Facebook:

Display filter: **tcp.flags.push==1 && ip.dst== 31.13.67.1 ,**
Packets:**94**

# Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

- **PSH & SYN Flag:**

For packets with PUSH & SYN flag set

Display filter: **(tcp.flags.push==1&&tcp.flags.syn==1) ,**

Packets: **0**

For packets with PUSH & SYN flag not set

Display filter: **(tcp.flags.push==0&&tcp.flags.syn==0) ,**
Packets: **388**

Number of packets with PUSH & SYN set & sent to host:

Display filter : **(tcp.flags.push==1&&tcp.flags.syn==1) &&ip.dst==10.110.161.147,**

Packets:**0**

Number of TCP packets with PUSH & SYN flag set and sent to Facebook:

Display filter **(tcp.flags.push==1&&tcp.flags.syn==1) &&ip.dst==31.13.86.8 ,** Packets:**0**

# RST Flag

- RST- Reset is an instantaneous abort in both directions or shows abnormal session disconnection

# Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

- **Reset Flag:**

For packets with RESET flag set

Display filter: **tcp.flags.reset==1 ,** Packets: **0**

For packets with RESET flag not set

Display filter: **tcp.flags. reset==0 ,** Packets: **625**

## Captured TCP Packets Statistics

Task: Capture all TCP traffic to/from Facebook

| | |
|---|---|
| Total Captured Packets | 643 |
| Packets Sent to Facebook | 252 |
| Packets Received from Facebook | 391 |
| Packets Sent to Facebook with SYN flag set | 4 |
| Packets Sent to Facebook with PSH flag set | 94 |
| Packets Received from Facebook with SYN flag set | 1 |
| Packets Received from Facebook with PSH flag set | 156 |
| Packets Sent to Facebook with SYN & PSH flags set | 0 |
| Packets Received from Facebook with SYN & PSH flags set | 0 |
| Total Packets With SYN flag set | 5 |
| Total Packets With PSH flag set | 250 |
| Total Packets With RST flag set | 0 |

# Task 2: Capture all HTTP traffic to and from Facebook while logging

- Display Filter:

**Tcp port 80 and host 31.13.86.8**

- Packets received from Facebook

**ip.dst==10.110.161.147**

- Packets sent to Facebook

Display Filter:

**ip.dst==3l.13.86.8**

# Task 3:capture all traffic to and from Playit.pk while playing a Popular video



Playit.pk :ip address **162.159.241.198)**

No capture filters were utilized as Playit.pk servers may change during streaming.

# Task 3:capture all traffic to and from Playit.pk while playing a Popular video

- Total Packets :**223**
- For packets with SYN flag set

Display filter: **tcp.flags.syn==1 ,** Packets: **42**

For packets PSH flag set

Display filter: **tcp.flags.push==1,** Packets: **47**

Number of packets with RST flag set :

Display filter: **tcp.flags.reset==1,** Packets: **1**

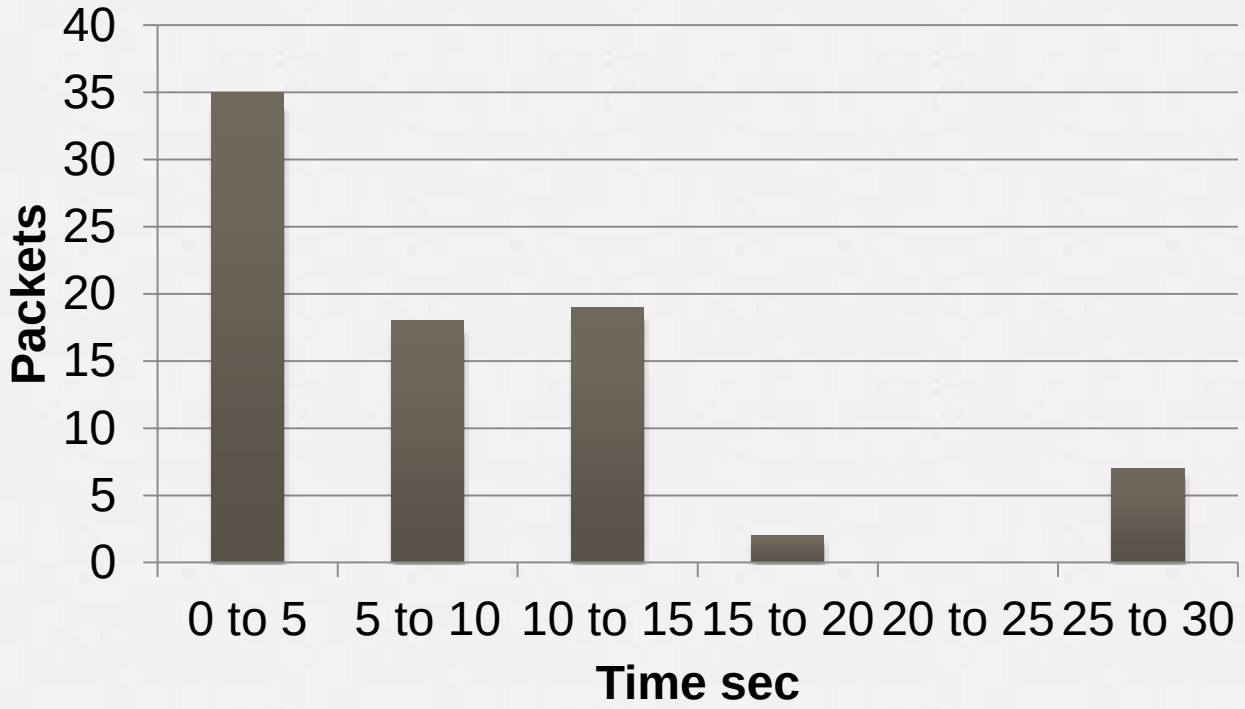
Number of TCP packets sent by host and received by Facebook:

Display filter **(ip.src== 10.110.164.135 and ip.dst==162.159.241.198),** Packets:**117**

Number of TCP packets sent by host and received by Facebook:

Display filter **(ip.src== 162.159.241.198 and ip.dst== 10.110.164.135),** Packets:**115**

# When Psh Flag==1



# Histogram of Packets size

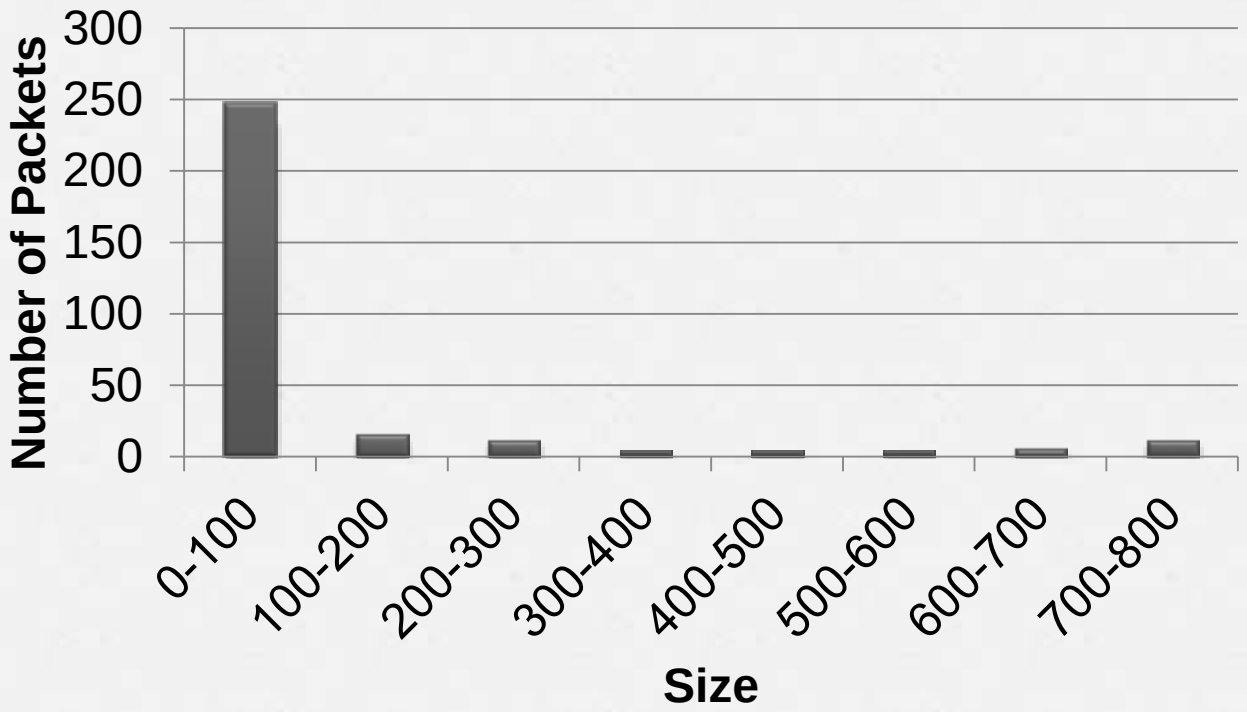
- Filter used:

frame.cap_len >= x && frame.cap_len <y

- From x to y

frame.cap_len >= 0 && frame.cap_len <100

# Histogram of Packets size




THANK YOU