PACKET CAPTURE ANALYSIS

Team Members:

Astha Rani

Chetan Surya D

Deekshitha

Sarthak Mishra

Shivaneeth P

Mentor:

Mr. Prabodh CP

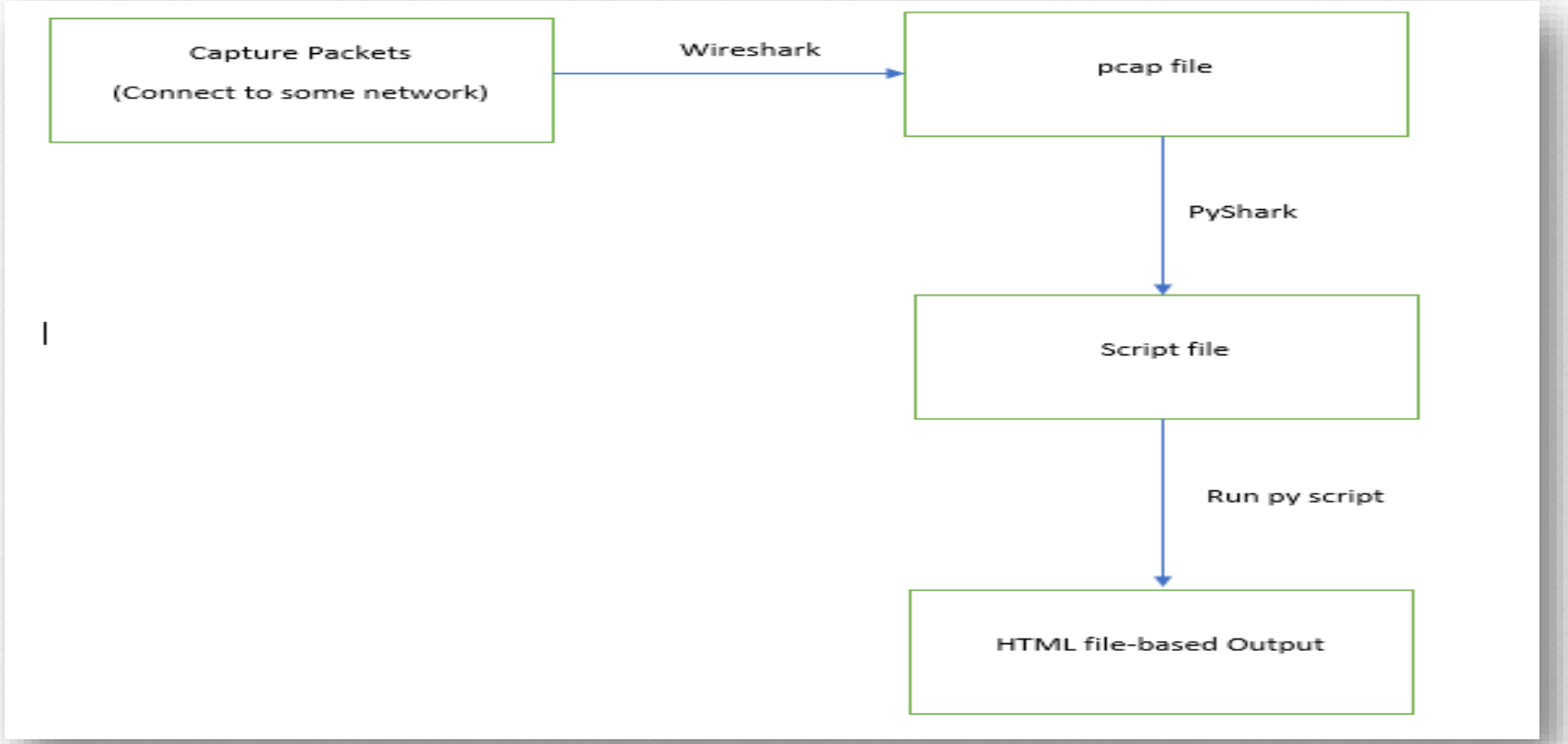
OVERVIEW

This project aims at capturing packets and generating analysis using specific fields namely Length(bytes), Protocol used, Time of capturing and No. of packets captured.

Furthermore, analyzing the packets captured by establishing the connection between two systems.

To aid us in analyzing the packets, we will be dealing with pyshark and tshark(command line version of wireshark).

DEVELOPMENT FLOW



CAPTURED PACKETS SUMMARY

Ref: https://github.com/sarthaksarm/Packet_Capture_CISCO/blob/master/Packet_Capture/Scripts/print_script.py

Captured Packets

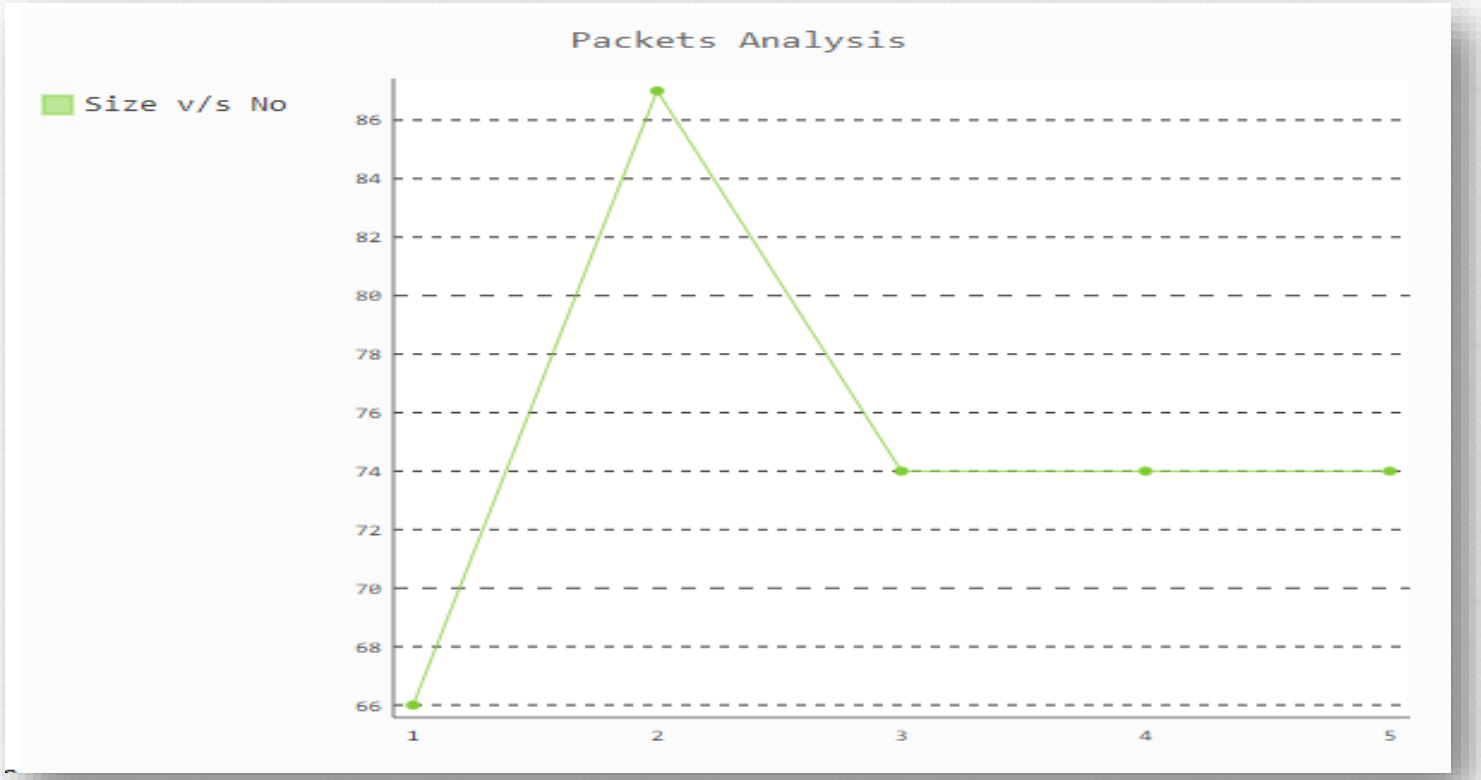
Packet Summary

No	Time	Source IP	Dest. IP	Protoc.	Len	Port	Info
2	0.049502	2404:6800:4007:809::2002	2401:4900:4bc2:d73:25d9:5a63:1eec:6678	UDP	87	443	\xe2\x86\x92 54643 Len=25
3	0.159692	2001:4de0:ac19::1:b:1a	2401:4900:4bc2:d73:25d9:5a63:1eec:6678	TCP	74	443	\xe2\x86\x92 49617 [FIN, ACK] Seq=1 Ack=1 Win=53 Len=0
4	0.186285	2001:4de0:ac19::1:b:1a	2401:4900:4bc2:d73:25d9:5a63:1eec:6678	TCP	74	443	\xe2\x86\x92 49620 [FIN, ACK] Seq=1 Ack=1 Win=53 Len=0
5	0.346351	2001:4de0:ac19::1:b:1a	2401:4900:4bc2:d73:25d9:5a63:1eec:6678	TCP	74	443	\xe2\x86\x92 49622 [FIN, ACK] Seq=1 Ack=1 Win=53 Len=0

ANALYSIS

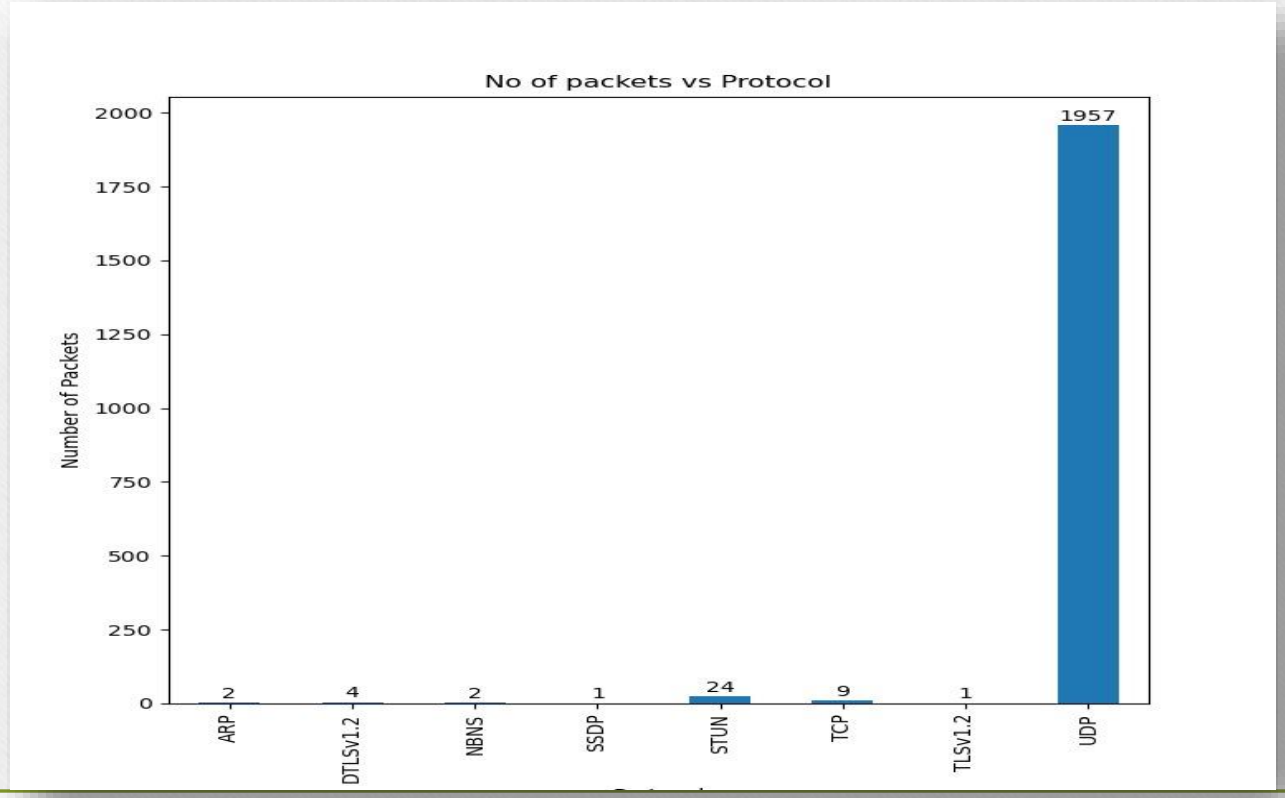
PACKET SIZE vs PACKET NO.

Ref: https://github.com/sarthaksarm/Packet_Capture_CISCO/blob/master/Packet_Capture/Scripts/Len_No_script.py



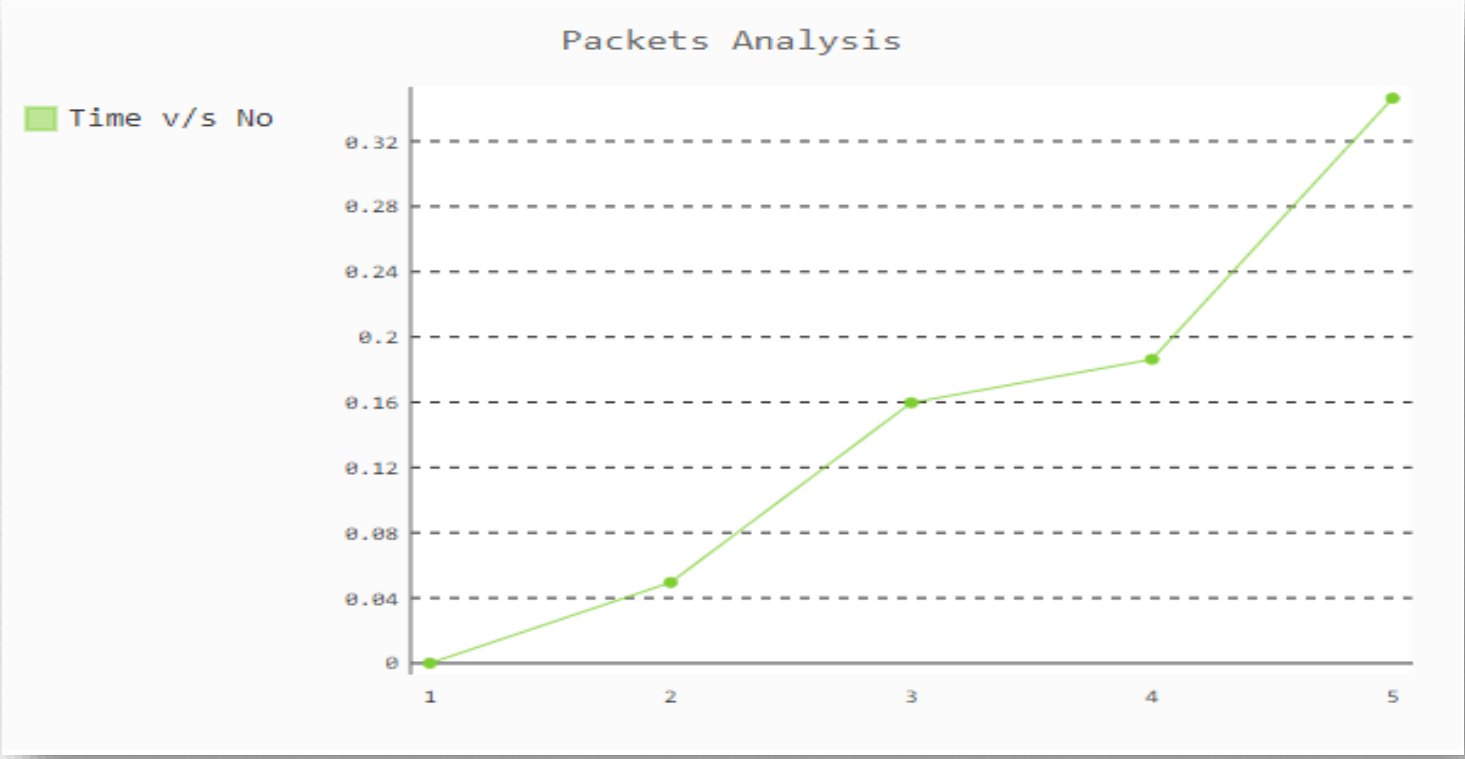
NO. OF PACKETS vs PROTOCOL USED

Ref:
https://github.com/sarthaksarm/Packet_Capture_CISCO/blob/master/Packet_Capture/Scripts/Protocol_PacketNo_script.py



CAPTURED TIME vs PACKET NO.

Ref: https://github.com/sarthaksarm/Packet_Capture_CISCO/blob/master/Packet_Capture/Scripts/Time_No_script.py



ESTABLISHING CONNECTION

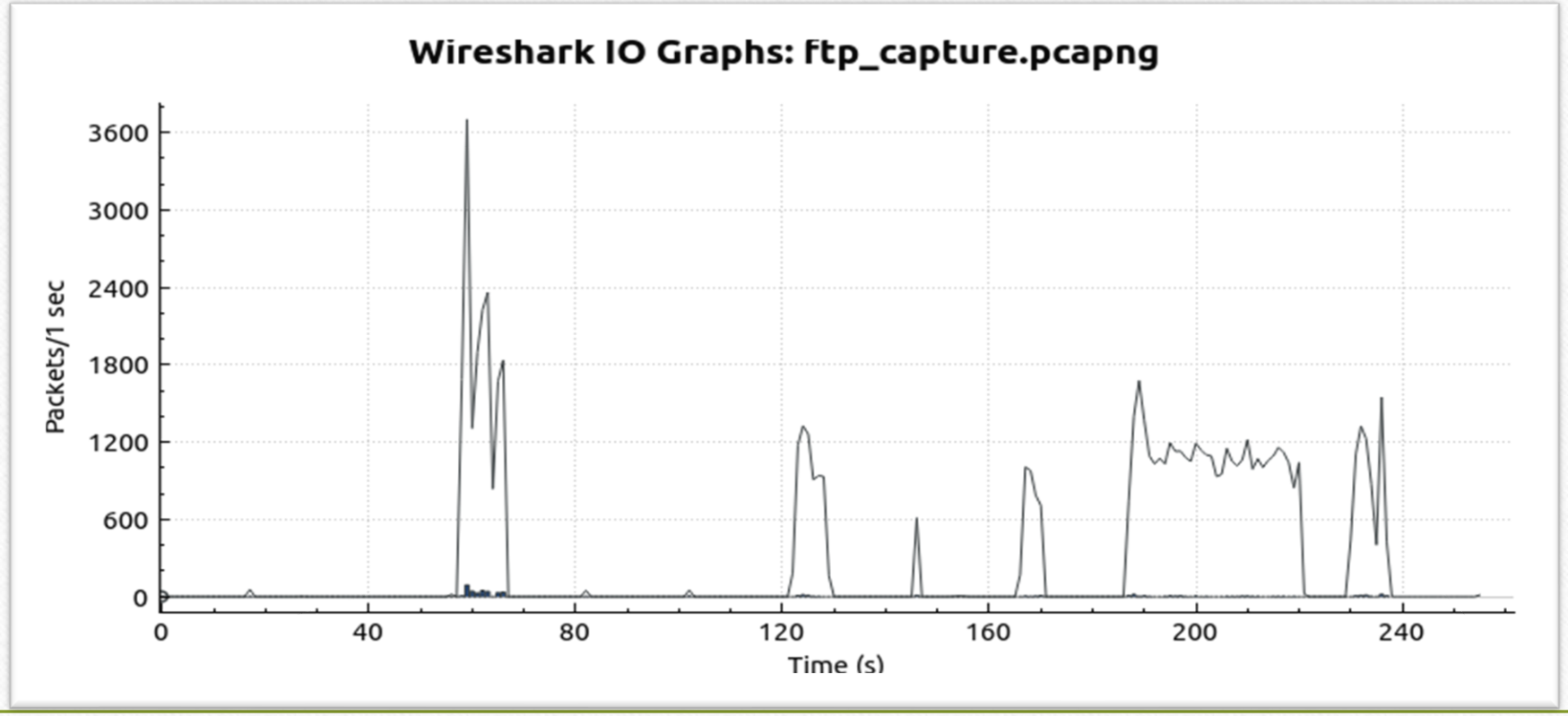
How did we really do it?

Ref: https://github.com/sarthaksarm/Packet_Capture_CISCO/tree/master/Packet_Capture/Scripts

- Using FTP as the application layer protocol and establishing the connection between two systems by making one as client and other as server.
- Filezilla is the application used to make one machine serve as server listening for connection requests.
- Transferred multiple files between the two, and captured the packets.

IO GRAPH

Ref: https://github.com/sarthaksarm/Packet_Capture_CISCO/blob/master/Packet_Capture/Output/IO_Graph.PNG



CONVERSATIONS

Ref: https://github.com/sarthaksarm/Packet_Capture_CISCO/blob/master/Packet_Capture/Output/Conversations.PNG

Ethernet · 3 | IPv4 · 5 | IPv6 · 1 | TCP · 3737 | UDP · 3

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A →
10.0.2.15	36694	74.125.200.188	5228	1	60	0	0	1	60	0.000000	0.0000	
10.0.2.15	40092	192.168.43.152	21	1,833	154 k	663	42 k	1,170	112 k	17.677728	64.9107	
10.0.2.15	53099	192.168.43.152	51976	8	1,905	4	236	4	1,669	56.846135	1.1569	
10.0.2.15	40094	192.168.43.152	21	14,790	1,381 k	5,600	389 k	9,190	991 k	58.031044	197.2332	
10.0.2.15	40096	192.168.43.152	21	14,806	1,385 k	5,596	389 k	9,210	996 k	58.038724	197.2262	
10.0.2.15	59841	192.168.43.152	58602	8	634	4	236	4	398	59.083267	0.0020	
10.0.2.15	59235	192.168.43.152	56381	8	552	4	236	4	316	59.122274	0.0013	
10.0.2.15	56585	192.168.43.152	49941	11	10 k	6	344	5	9,959	59.309367	0.0855	
10.0.2.15	60775	192.168.43.152	53783	8	638	4	236	4	402	59.416166	0.0039	
10.0.2.15	60813	192.168.43.152	52748	8	479	4	236	4	243	59.693415	0.0520	
10.0.2.15	53891	192.168.43.152	52244	8	637	4	236	4	401	59.938319	0.0081	
10.0.2.15	56247	192.168.43.152	50467	8	551	4	236	4	315	59.973743	0.0020	
10.0.2.15	58483	192.168.43.152	53764	8	555	4	236	4	319	60.101680	0.0017	
10.0.2.15	60427	192.168.43.152	51172	8	554	4	236	4	318	60.609768	0.0052	
10.0.2.15	49935	192.168.43.152	49834	8	620	4	236	4	384	60.726696	0.0079	
10.0.2.15	53319	192.168.43.152	49446	8	866	4	236	4	630	61.015297	0.0155	
10.0.2.15	57437	192.168.43.152	53385	8	639	4	236	4	403	61.029714	0.0222	
10.0.2.15	59197	192.168.43.152	53091	8	551	4	236	4	315	61.162007	0.0047	
10.0.2.15	60173	192.168.43.152	50142	8	561	4	236	4	325	61.360435	0.0335	
10.0.2.15	57233	192.168.43.152	55930	358	2,899 k	148	8,012	210	2,890 k	61.604636	0.1592	
10.0.2.15	59703	192.168.43.152	54406	8	823	4	236	4	587	61.702644	0.0911	
10.0.2.15	57049	192.168.43.152	52123	755	6,426 k	283	15 k	472	6,410 k	61.899011	0.2732	
10.0.2.15	54739	192.168.43.152	49517	8	551	4	236	4	315	61.935976	0.0015	
10.0.2.15	56591	192.168.43.152	53743	8	633	4	236	4	397	61.970887	0.0067	
10.0.2.15	55095	192.168.43.152	49953	16	25 k	8	452	8	24 k	62.481493	0.0453	
10.0.2.15	51563	192.168.43.152	50308	7	416	4	236	3	180	62.495848	20.0921	
10.0.2.15	57125	192.168.43.152	52414	9	2,912	5	290	4	2,622	62.802799	0.0794	

THANK YOU