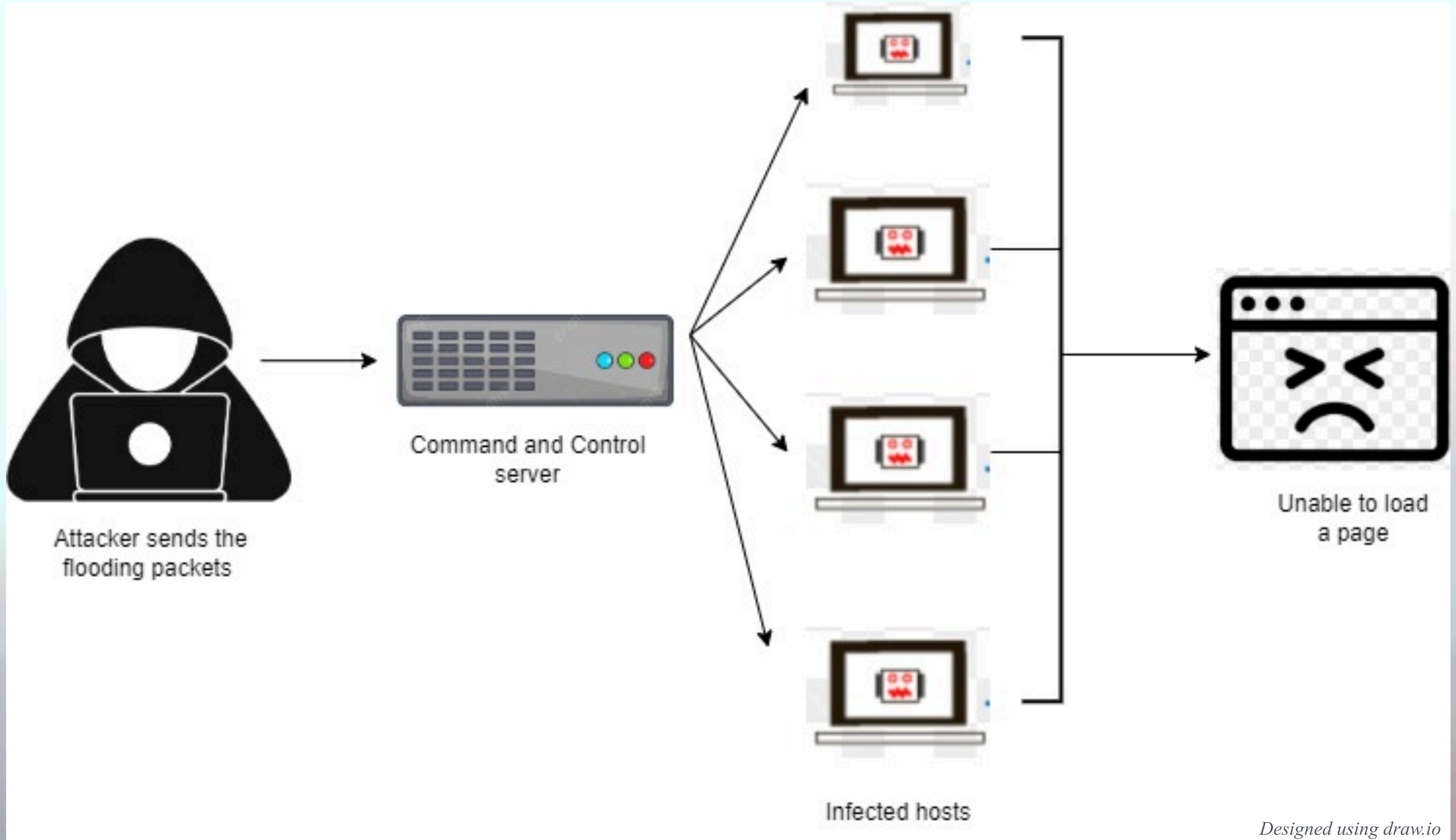
AI Threat Analysis System: Safeguarding businesses through dynamic cybersecurity insights.

Team Name: Access Denied
Team Code:HFC03
College : GSSSIETW, Mysuru

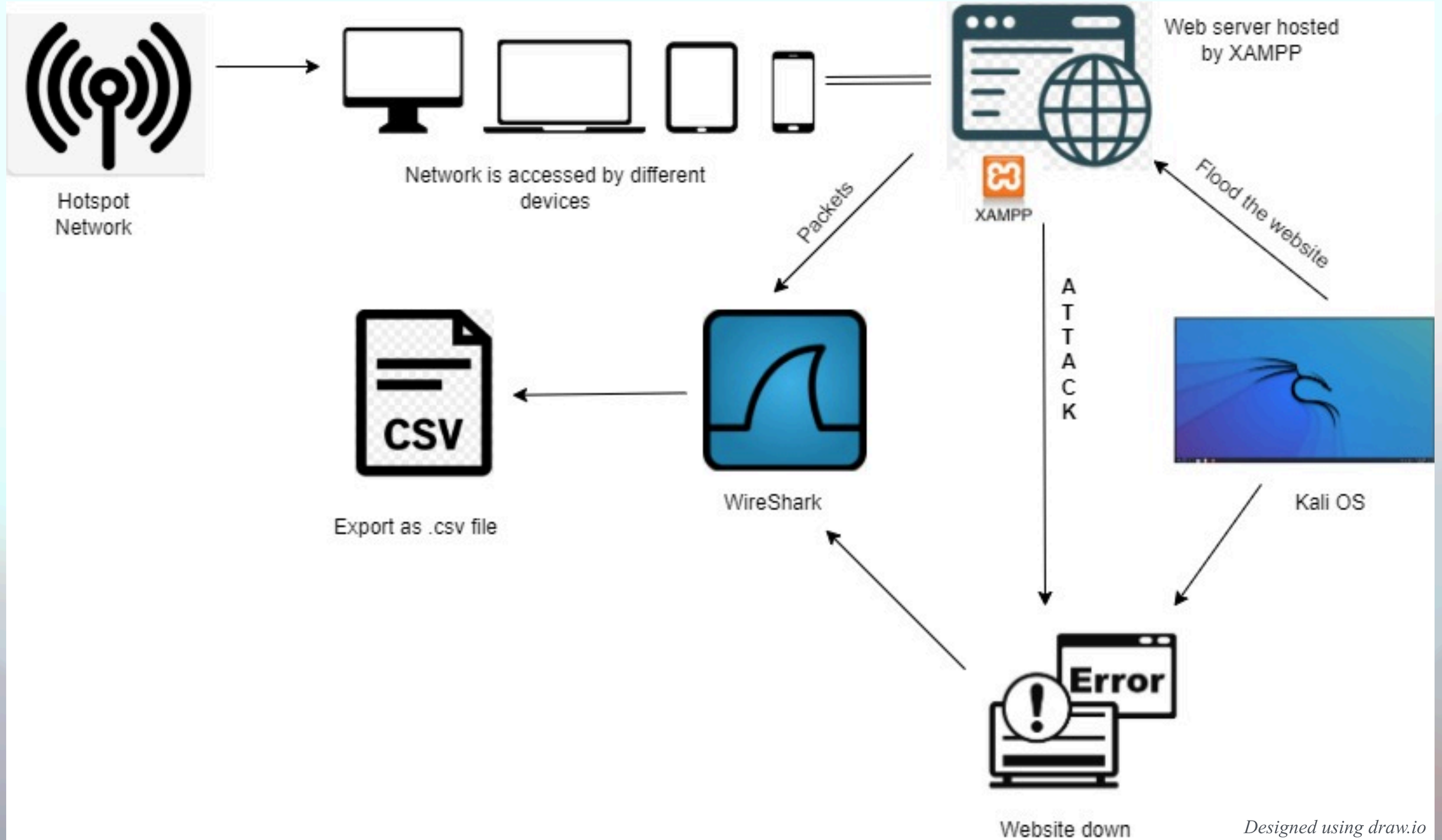
21 February,2024

Working Procedure of Attack



Designed using draw.io

Collection of dataset



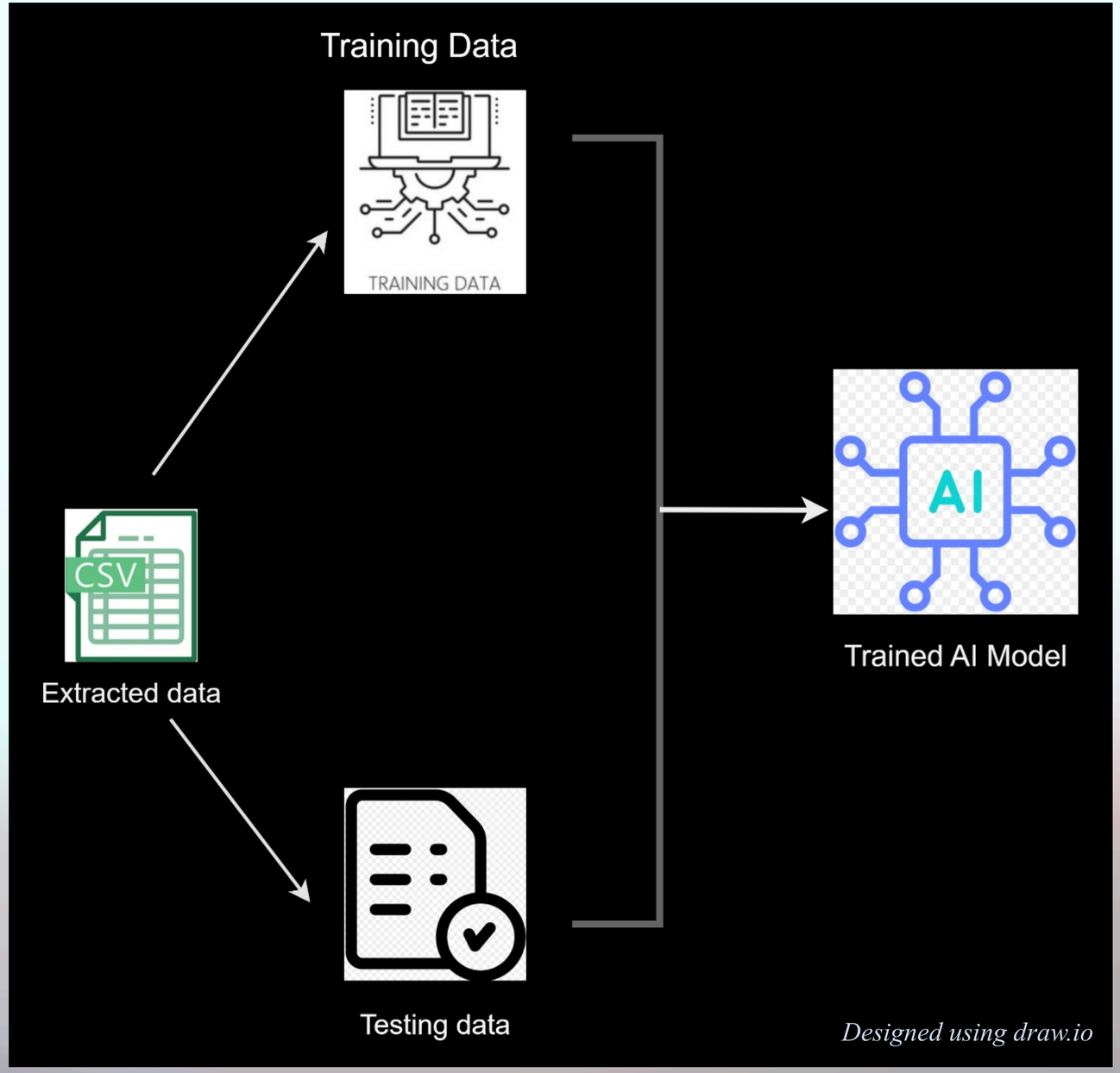
Designed using draw.io

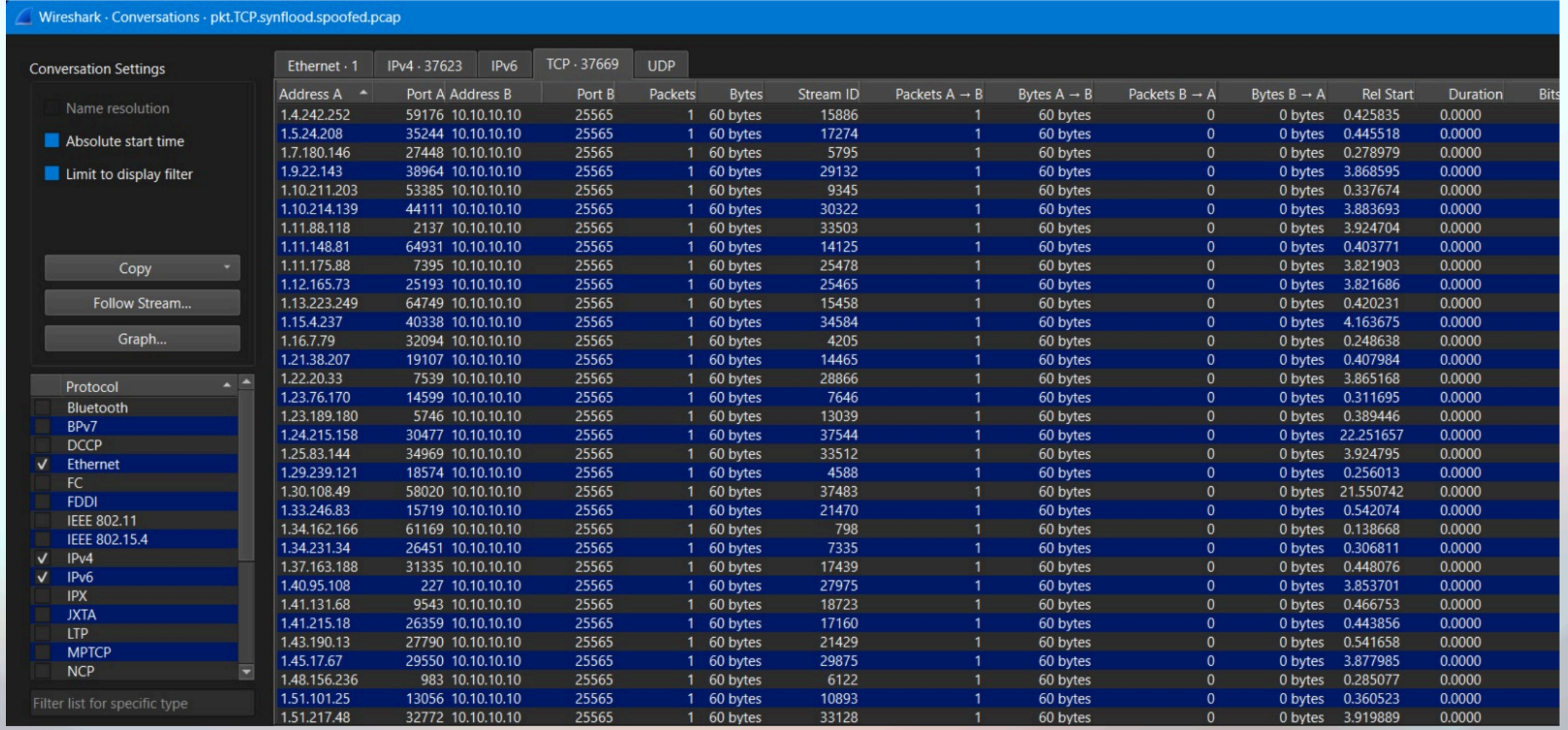
Following steps to collect data:

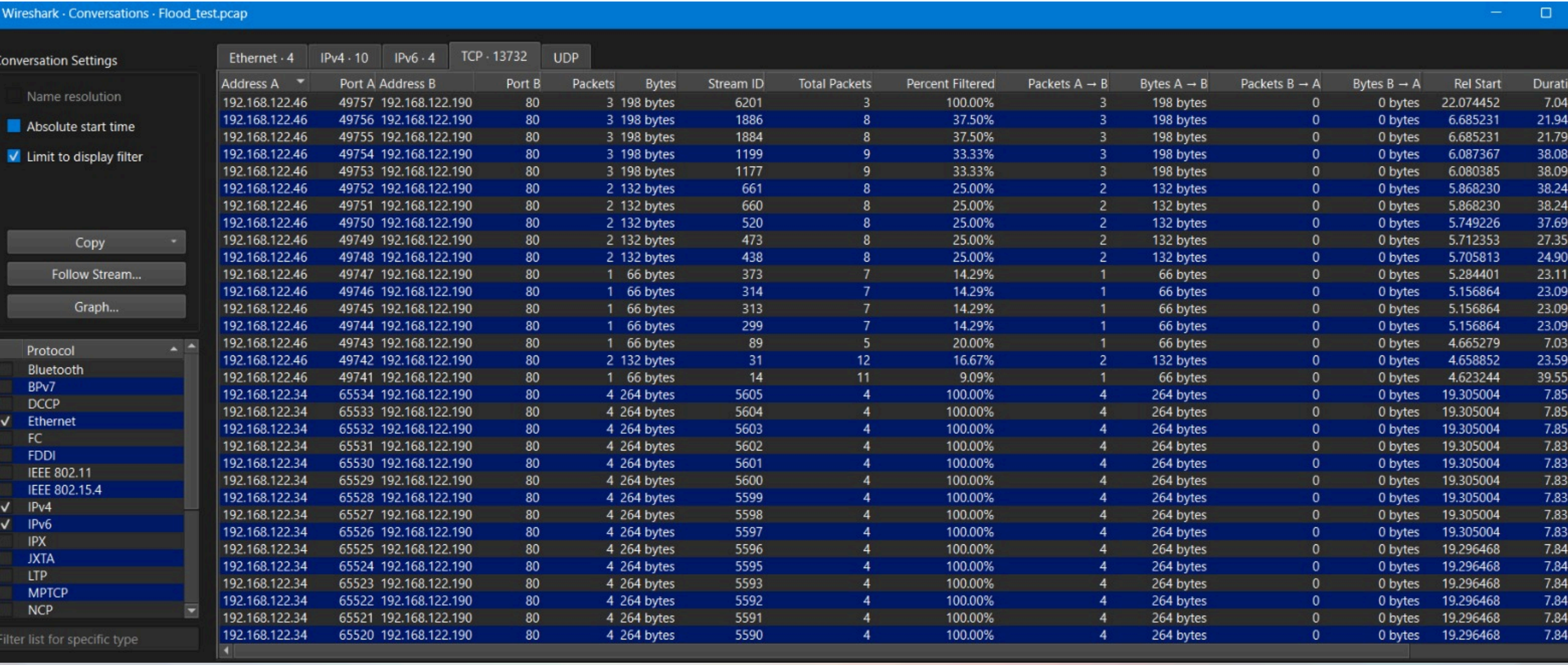
(This data is collected based on the requirements for the project.)

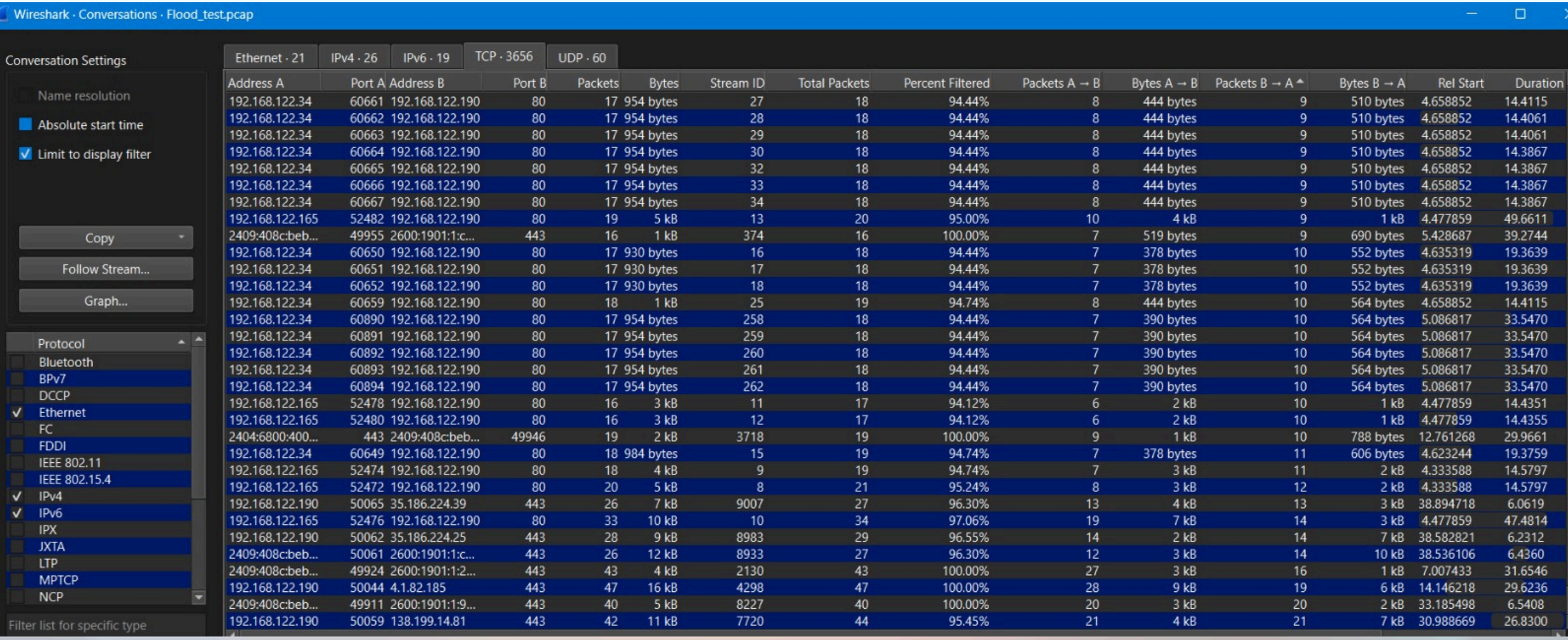
- **Wireshark:** To trace connections, view the contents of suspect network transactions and identify bursts of network traffic.
- **Kali OS:**Kali includes hacking tools that can be used to carry out and defend against brute-force attacks, wireless attacks, IP spoofing attacks.
- **hping3:** It is a tool ,we can use for DDOS attack and can use it for scanning like Nmap. It is the packet count that we want to send it to the victim.
- **Nmap:**It is used to discover hosts and services on a computer network by sending packets and analysing the responses.
- **XAMPP:** It is an open source software package which provides a local web server environment for testing and development.
- **Flooding(DDOS Attack):**In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic.
- ***Through wireshark, we extracted 7 different attributes in which, we are adding one extra attribute and name it as "Target ".***

Data Training




Wireshark · Conversations · pkt.TCP.synflood.spoofed.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
Filter list for specific type
Ethernet · 1
IPv4 · 37623
IPv6
TCP · 37669
UDP
Address A Port A Address B Port B Packets Bytes Stream ID Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits
1.4.242.252 59176 10.10.10.10 25565 1 60 bytes 15886 1 60 bytes 0 0 bytes 0.425835 0.0000
1.5.24.208 35244 10.10.10.10 25565 1 60 bytes 17274 1 60 bytes 0 0 bytes 0.445518 0.0000
1.7.180.146 27448 10.10.10.10 25565 1 60 bytes 5795 1 60 bytes 0 0 bytes 0.278979 0.0000
1.9.22.143 38964 10.10.10.10 25565 1 60 bytes 29132 1 60 bytes 0 0 bytes 3.868595 0.0000
1.10.211.203 53385 10.10.10.10 25565 1 60 bytes 9345 1 60 bytes 0 0 bytes 0.337674 0.0000
1.10.214.139 44111 10.10.10.10 25565 1 60 bytes 30322 1 60 bytes 0 0 bytes 3.883693 0.0000
1.11.88.118 2137 10.10.10.10 25565 1 60 bytes 33503 1 60 bytes 0 0 bytes 3.924704 0.0000
1.11.148.81 64931 10.10.10.10 25565 1 60 bytes 14125 1 60 bytes 0 0 bytes 0.403771 0.0000
1.11.175.88 7395 10.10.10.10 25565 1 60 bytes 25478 1 60 bytes 0 0 bytes 3.821903 0.0000
1.12.165.73 25193 10.10.10.10 25565 1 60 bytes 25465 1 60 bytes 0 0 bytes 3.821686 0.0000
1.13.223.249 64749 10.10.10.10 25565 1 60 bytes 15458 1 60 bytes 0 0 bytes 0.420231 0.0000
1.15.4.237 40338 10.10.10.10 25565 1 60 bytes 34584 1 60 bytes 0 0 bytes 4.163675 0.0000
1.16.7.79 32094 10.10.10.10 25565 1 60 bytes 4205 1 60 bytes 0 0 bytes 0.248638 0.0000
1.21.38.207 19107 10.10.10.10 25565 1 60 bytes 14465 1 60 bytes 0 0 bytes 0.407984 0.0000
1.22.20.33 7539 10.10.10.10 25565 1 60 bytes 28866 1 60 bytes 0 0 bytes 3.865168 0.0000
1.23.76.170 14599 10.10.10.10 25565 1 60 bytes 7646 1 60 bytes 0 0 bytes 0.311695 0.0000
1.23.189.180 5746 10.10.10.10 25565 1 60 bytes 13039 1 60 bytes 0 0 bytes 0.389446 0.0000
1.24.215.158 30477 10.10.10.10 25565 1 60 bytes 37544 1 60 bytes 0 0 bytes 22.251657 0.0000
1.25.83.144 34969 10.10.10.10 25565 1 60 bytes 33512 1 60 bytes 0 0 bytes 3.924795 0.0000
1.29.239.121 18574 10.10.10.10 25565 1 60 bytes 4588 1 60 bytes 0 0 bytes 0.256013 0.0000
1.30.108.49 58020 10.10.10.10 25565 1 60 bytes 37483 1 60 bytes 0 0 bytes 21.550742 0.0000
1.33.246.83 15719 10.10.10.10 25565 1 60 bytes 21470 1 60 bytes 0 0 bytes 0.542074 0.0000
1.34.162.166 61169 10.10.10.10 25565 1 60 bytes 798 1 60 bytes 0 0 bytes 0.138668 0.0000
1.34.231.34 26451 10.10.10.10 25565 1 60 bytes 7335 1 60 bytes 0 0 bytes 0.306811 0.0000
1.37.163.188 31335 10.10.10.10 25565 1 60 bytes 17439 1 60 bytes 0 0 bytes 0.448076 0.0000
1.40.95.108 227 10.10.10.10 25565 1 60 bytes 27975 1 60 bytes 0 0 bytes 3.853701 0.0000
1.41.131.68 9543 10.10.10.10 25565 1 60 bytes 18723 1 60 bytes 0 0 bytes 0.466753 0.0000
1.41.215.18 26359 10.10.10.10 25565 1 60 bytes 17160 1 60 bytes 0 0 bytes 0.443856 0.0000
1.43.190.13 27790 10.10.10.10 25565 1 60 bytes 21429 1 60 bytes 0 0 bytes 0.541658 0.0000
1.45.17.67 29550 10.10.10.10 25565 1 60 bytes 29875 1 60 bytes 0 0 bytes 3.877985 0.0000
1.48.156.236 983 10.10.10.10 25565 1 60 bytes 6122 1 60 bytes 0 0 bytes 0.285077 0.0000
1.51.101.25 13056 10.10.10.10 25565 1 60 bytes 10893 1 60 bytes 0 0 bytes 0.360523 0.0000
1.51.217.48 32772 10.10.10.10 25565 1 60 bytes 33128 1 60 bytes 0 0 bytes 3.919889 0.0000


Wireshark · Conversations · Flood_test.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
Filter list for specific type
Ethernet · 4
IPv4 · 10
IPv6 · 4
TCP · 13732
UDP
Address A Port A Address B Port B Packets Bytes Stream ID Total Packets Percent Filtered Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Durati
192.168.122.46 49757 192.168.122.190 80 3 198 bytes 6201 3 100.00% 3 198 bytes 0 0 bytes 22.074452 7.04
192.168.122.46 49756 192.168.122.190 80 3 198 bytes 1886 8 37.50% 3 198 bytes 0 0 bytes 6.685231 21.94
192.168.122.46 49755 192.168.122.190 80 3 198 bytes 1884 8 37.50% 3 198 bytes 0 0 bytes 6.685231 21.79
192.168.122.46 49754 192.168.122.190 80 3 198 bytes 1199 9 33.33% 3 198 bytes 0 0 bytes 6.087367 38.08
192.168.122.46 49753 192.168.122.190 80 3 198 bytes 1177 9 33.33% 3 198 bytes 0 0 bytes 6.080385 38.09
192.168.122.46 49752 192.168.122.190 80 2 132 bytes 661 8 25.00% 2 132 bytes 0 0 bytes 5.868230 38.24
192.168.122.46 49751 192.168.122.190 80 2 132 bytes 660 8 25.00% 2 132 bytes 0 0 bytes 5.868230 38.24
192.168.122.46 49750 192.168.122.190 80 2 132 bytes 520 8 25.00% 2 132 bytes 0 0 bytes 5.749226 37.69
192.168.122.46 49749 192.168.122.190 80 2 132 bytes 473 8 25.00% 2 132 bytes 0 0 bytes 5.712353 27.35
192.168.122.46 49748 192.168.122.190 80 2 132 bytes 438 8 25.00% 2 132 bytes 0 0 bytes 5.705813 24.90
192.168.122.46 49747 192.168.122.190 80 1 66 bytes 373 7 14.29% 1 66 bytes 0 0 bytes 5.284401 23.11
192.168.122.46 49746 192.168.122.190 80 1 66 bytes 314 7 14.29% 1 66 bytes 0 0 bytes 5.156864 23.09
192.168.122.46 49745 192.168.122.190 80 1 66 bytes 313 7 14.29% 1 66 bytes 0 0 bytes 5.156864 23.09
192.168.122.46 49744 192.168.122.190 80 1 66 bytes 299 7 14.29% 1 66 bytes 0 0 bytes 5.156864 23.09
192.168.122.46 49743 192.168.122.190 80 1 66 bytes 89 5 20.00% 1 66 bytes 0 0 bytes 4.665279 7.03
192.168.122.46 49742 192.168.122.190 80 2 132 bytes 31 12 16.67% 2 132 bytes 0 0 bytes 4.658852 23.59
192.168.122.46 49741 192.168.122.190 80 1 66 bytes 14 11 9.09% 1 66 bytes 0 0 bytes 4.623244 39.55
192.168.122.34 65534 192.168.122.190 80 4 264 bytes 5605 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.85
192.168.122.34 65533 192.168.122.190 80 4 264 bytes 5604 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.85
192.168.122.34 65532 192.168.122.190 80 4 264 bytes 5603 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.85
192.168.122.34 65531 192.168.122.190 80 4 264 bytes 5602 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.83
192.168.122.34 65530 192.168.122.190 80 4 264 bytes 5601 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.83
192.168.122.34 65529 192.168.122.190 80 4 264 bytes 5600 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.83
192.168.122.34 65528 192.168.122.190 80 4 264 bytes 5599 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.83
192.168.122.34 65527 192.168.122.190 80 4 264 bytes 5598 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.83
192.168.122.34 65526 192.168.122.190 80 4 264 bytes 5597 4 100.00% 4 264 bytes 0 0 bytes 19.305004 7.83
192.168.122.34 65525 192.168.122.190 80 4 264 bytes 5596 4 100.00% 4 264 bytes 0 0 bytes 19.296468 7.84
192.168.122.34 65524 192.168.122.190 80 4 264 bytes 5595 4 100.00% 4 264 bytes 0 0 bytes 19.296468 7.84
192.168.122.34 65523 192.168.122.190 80 4 264 bytes 5593 4 100.00% 4 264 bytes 0 0 bytes 19.296468 7.84
192.168.122.34 65522 192.168.122.190 80 4 264 bytes 5592 4 100.00% 4 264 bytes 0 0 bytes 19.296468 7.84
192.168.122.34 65521 192.168.122.190 80 4 264 bytes 5591 4 100.00% 4 264 bytes 0 0 bytes 19.296468 7.84
192.168.122.34 65520 192.168.122.190 80 4 264 bytes 5590 4 100.00% 4 264 bytes 0 0 bytes 19.296468 7.84



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.122.34	60661	192.168.122.190	80	17	954 bytes	27	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.4115
192.168.122.34	60662	192.168.122.190	80	17	954 bytes	28	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.4061
192.168.122.34	60663	192.168.122.190	80	17	954 bytes	29	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.4061
192.168.122.34	60664	192.168.122.190	80	17	954 bytes	30	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.3867
192.168.122.34	60665	192.168.122.190	80	17	954 bytes	32	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.3867
192.168.122.34	60666	192.168.122.190	80	17	954 bytes	33	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.3867
192.168.122.34	60667	192.168.122.190	80	17	954 bytes	34	18	94.44%	8	444 bytes	9	510 bytes	4.658852	14.3867
192.168.122.165	52482	192.168.122.190	80	19	5 kB	13	20	95.00%	10	4 kB	9	1 kB	4.477859	49.6611
2409:408c:beb...	49955	2600:1901:1:c...	443	16	1 kB	374	16	100.00%	7	519 bytes	9	690 bytes	5.428687	39.2744
192.168.122.34	60650	192.168.122.190	80	17	930 bytes	16	18	94.44%	7	378 bytes	10	552 bytes	4.635319	19.3639
192.168.122.34	60651	192.168.122.190	80	17	930 bytes	17	18	94.44%	7	378 bytes	10	552 bytes	4.635319	19.3639
192.168.122.34	60652	192.168.122.190	80	17	930 bytes	18	18	94.44%	7	378 bytes	10	552 bytes	4.635319	19.3639
192.168.122.34	60659	192.168.122.190	80	18	1 kB	25	19	94.74%	8	444 bytes	10	564 bytes	4.658852	14.4115
192.168.122.34	60890	192.168.122.190	80	17	954 bytes	258	18	94.44%	7	390 bytes	10	564 bytes	5.086817	33.5470
192.168.122.34	60891	192.168.122.190	80	17	954 bytes	259	18	94.44%	7	390 bytes	10	564 bytes	5.086817	33.5470
192.168.122.34	60892	192.168.122.190	80	17	954 bytes	260	18	94.44%	7	390 bytes	10	564 bytes	5.086817	33.5470
192.168.122.34	60893	192.168.122.190	80	17	954 bytes	261	18	94.44%	7	390 bytes	10	564 bytes	5.086817	33.5470
192.168.122.34	60894	192.168.122.190	80	17	954 bytes	262	18	94.44%	7	390 bytes	10	564 bytes	5.086817	33.5470
192.168.122.165	52478	192.168.122.190	80	16	3 kB	11	17	94.12%	6	2 kB	10	1 kB	4.477859	14.4351
192.168.122.165	52480	192.168.122.190	80	16	3 kB	12	17	94.12%	6	2 kB	10	1 kB	4.477859	14.4355
2404:6800:400...	443	2409:408c:beb...	49946	19	2 kB	3718	19	100.00%	9	1 kB	10	788 bytes	12.761268	29.9661
192.168.122.34	60649	192.168.122.190	80	18	984 bytes	15	19	94.74%	7	378 bytes	11	606 bytes	4.623244	19.3759
192.168.122.165	52474	192.168.122.190	80	18	4 kB	9	19	94.74%	7	3 kB	11	2 kB	4.333588	14.5797
192.168.122.165	52472	192.168.122.190	80	20	5 kB	8	21	95.24%	8	3 kB	12	2 kB	4.333588	14.5797
192.168.122.190	50065	35.186.224.39	443	26	7 kB	9007	27	96.30%	13	4 kB	13	3 kB	38.894718	6.0619
192.168.122.165	52476	192.168.122.190	80	33	10 kB	10	34	97.06%	19	7 kB	14	3 kB	4.477859	47.4814
192.168.122.190	50062	35.186.224.25	443	28	9 kB	8983	29	96.55%	14	2 kB	14	7 kB	38.582821	6.2312
2409:408c:beb...	50061	2600:1901:1:c...	443	26	12 kB	8933	27	96.30%	12	3 kB	14	10 kB	38.536106	6.4360
2409:408c:beb...	49924	2600:1901:1:2...	443	43	4 kB	2130	43	100.00%	27	3 kB	16	1 kB	7.007433	31.6546
192.168.122.190	50044	4.1.82.185	443	47	16 kB	4298	47	100.00%	28	9 kB	19	6 kB	14.146218	29.6236
2409:408c:beb...	49911	2600:1901:1:9...	443	40	5 kB	8227	40	100.00%	20	3 kB	20	2 kB	33.185498	6.5408
192.168.122.190	50059	138.199.14.81	443	42	11 kB	7720	44	95.45%	21	4 kB	21	7 kB	30.988669	26.8300