MEHRAD HAGHSHENAS

SCICOMP202
NETWORKS & COMMUNICATIONS

Project 1 Packet Size Distribution and Protocol Breakdown

"This is all my own work. I have not knowingly allowed others to copy my work. This work has not been submitted for assessment in any other context."

- Hardware: macOS Monterey. (version 12.2.1)
- Software: Wireshark. (version 3.6.1)
- Network Connection: wireless. (Wifi)
- Physical Network Interface Card: en0
- mac address: d4:57:63:cc:7a:45
- Web Browser: Google Chrome.

Website 1: http://www.gutenberg.org/ebooks/2701

My IP address: 192.168.1.104 (ip.addr == 192.168.1.104)

Total number of frames: 163291

Time: around 20:00

Duration: 20 minutes.

Total number of frames with the source or destination IP address 192.168.1.104: 159798

Total number of frames with destination my IP address: 127884

Total number of frames with source my IP address: 31927

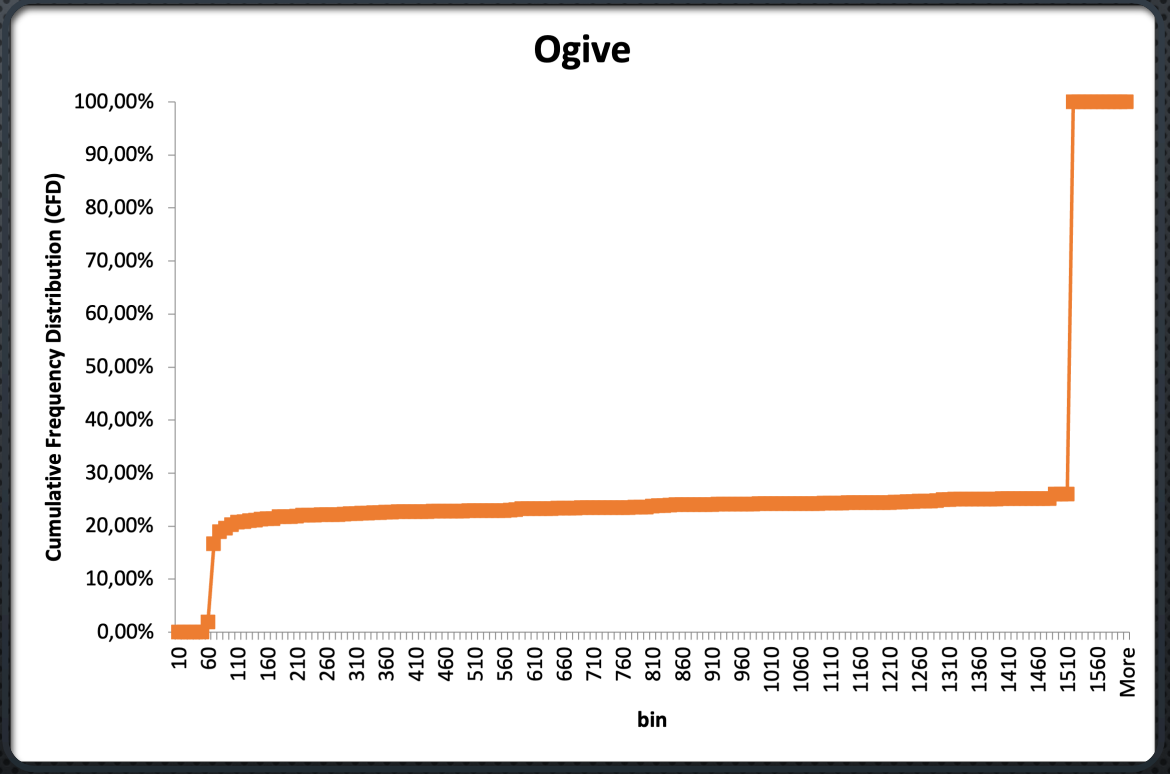
percentage of packets:

IPv6: 0.8%.

IPv4: 98.4%.

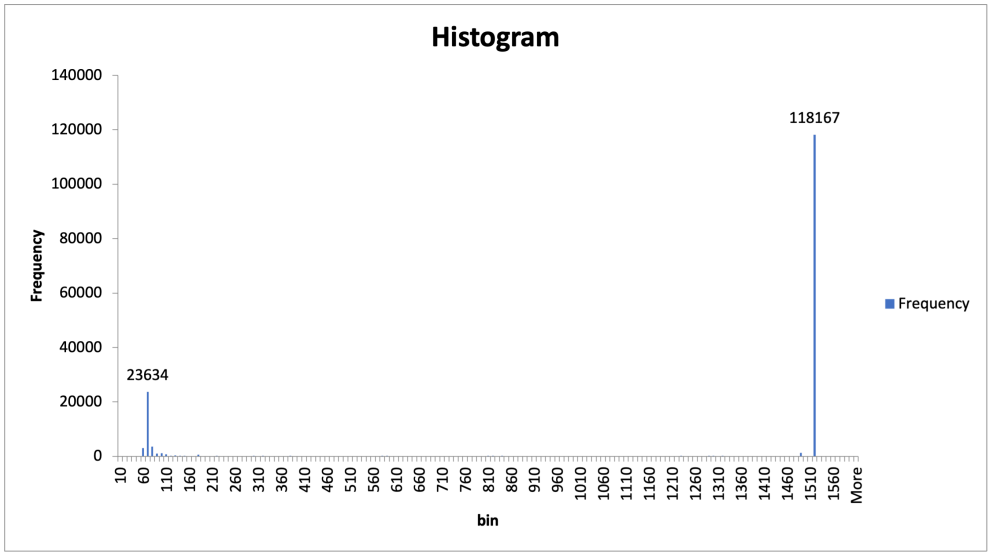
ARP:0.8%

- Website 1 URL: http://www.gutenberg.org/ebooks/2701



protocol length	count	percentage
1514	118166	73,94
66	22950	14,36
54	3009	1,88
78	2257	1,41
1484	1324	0,82
92	542	0,34
75	526	0,33
67	367	0,23
74	340	0,21

Graph is Bimodal.



- Protocal Breakdown:

protocol	percentage of packets	percentage of data
TCP	95.7%	91.1%
UDP	3.4%	0.1%
QUIC	2.5%	0.6%

Website2: https://www.youtube.com/watch?v=sLCC1Wu2Cmc

My IP address: 192.168.1.104 (ip.addr == 192.168.1.104)

Total number of frames: 39894

Time: around 20:00

Duration: 10 minutes.

Total number of frames with the source or destination IP address 192.168.1.104: 35309

Total number of frames with destination my IP address: 28288

Total number of frames with source my IP address: 7021

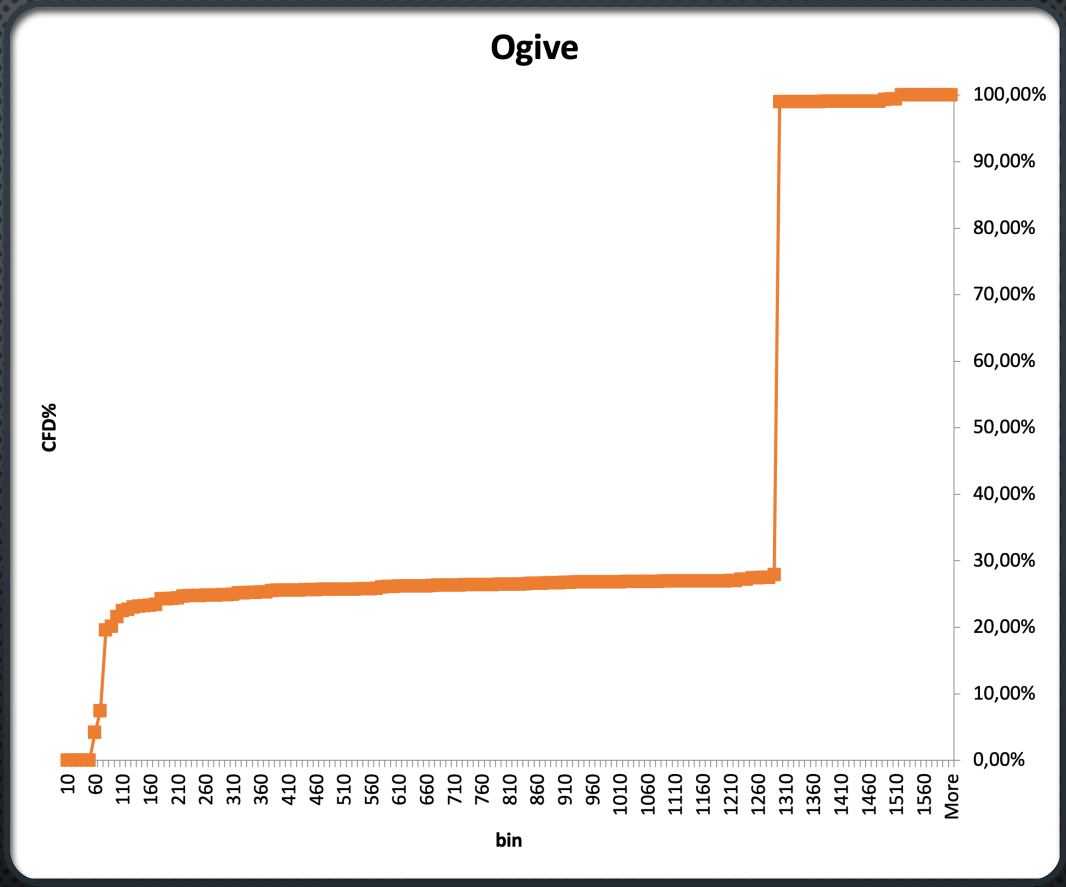
percentage of packets:

IPv6: 8.7%

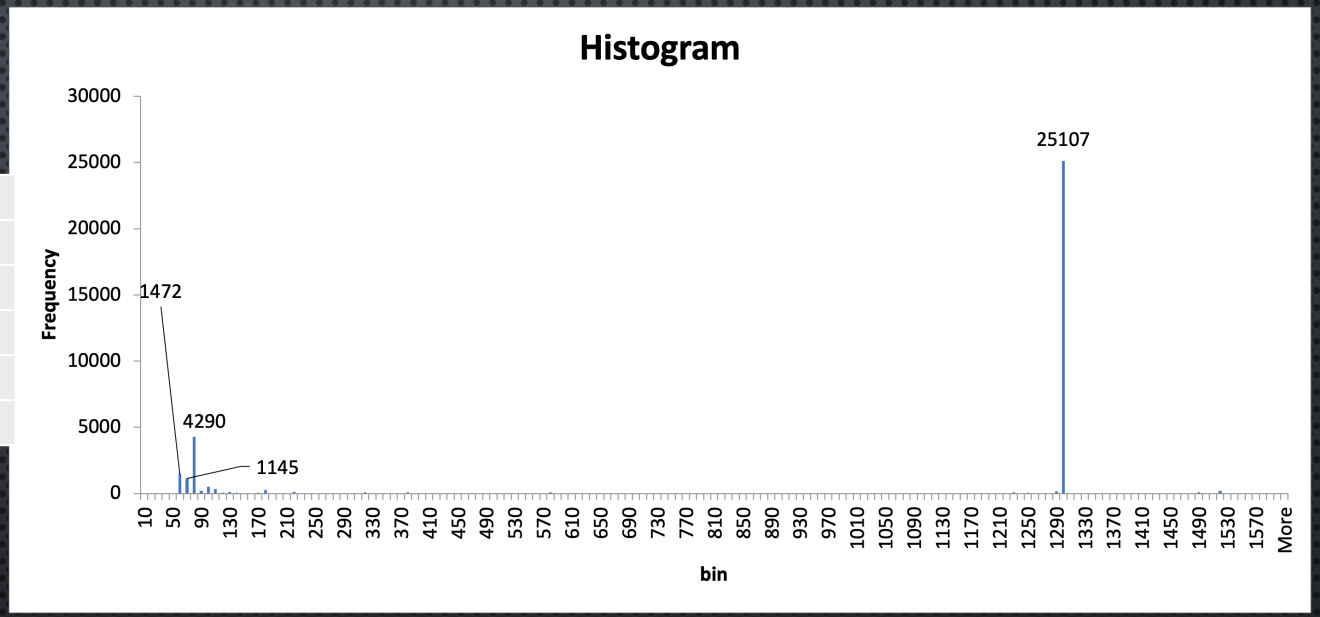
IPv4:89.7%

ARP:1.6%

- WEBSITE2: HTTPS://WWW.YOUTUBE.COM/WATCH?V=SLCC1WU2CMC



protocol length	count	percent
1292	25107	71,10
75	2385	6,75
54	1472	4,16
76	1224	3,46
66	739	2,09



Graph is again bimodal.

- Protocol Breakdown:

protocol	percentage of packets	percentage of DATA
TCP	19.9%	4.1%
UDP	78.4%	0.7%
QUIC	76.5%	90.7%

Website 3: https://vimeo.com/366765726

My IP address: 192.168.1.104 (ip.addr == 192.168.1.104)

Total number of frames: 34098

Time: around 20:00

Duration: 10 minutes.

Total number of frames with the source or destination IP address 192.168.1.104: 31200

Total number of frames with destination my IP address: 23387

Total number of frames with source my IP address: 7813

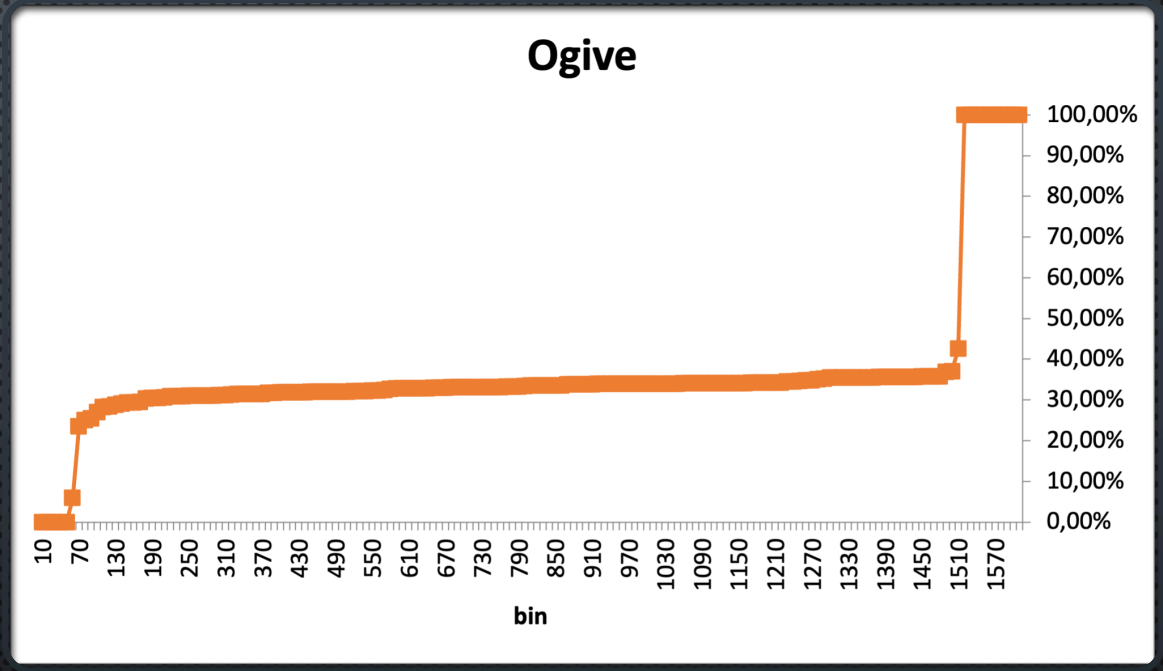
percentage of packets:

IPv6: 5.3%

IPv4:92.8%

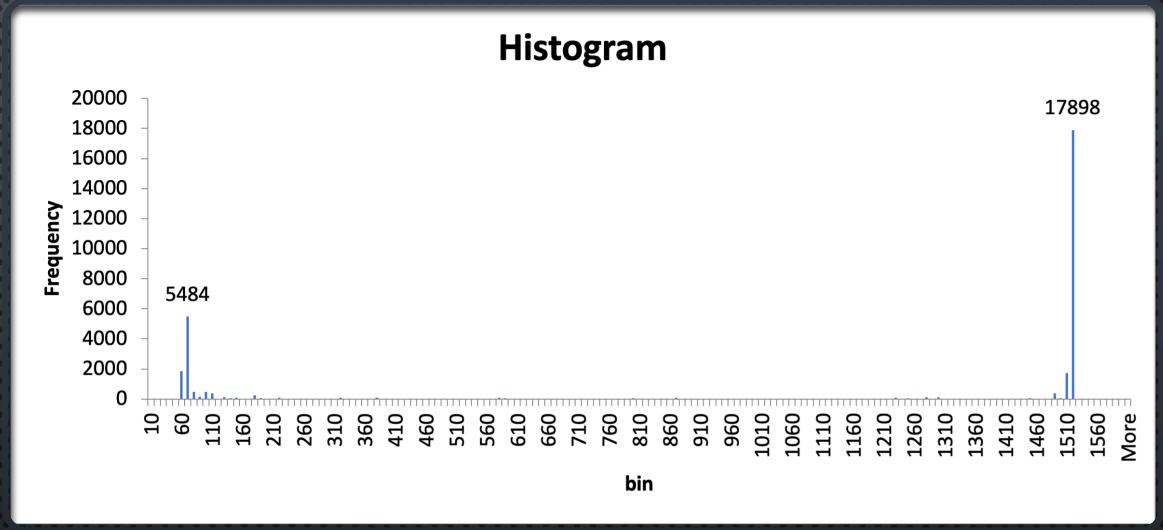
ARP:1.8%

- WEBSITE 3: HTTPS://VIMEO.COM/366765726



- AGAIN BIMODAL.

protocol length	count	percent
1514	17898	57,36
66	5430	17,40
54	1846	5,91
1510	1739	5,57



- PROTOCOL BREAKDOWN:

protocol	percentage of packets	percentage of DATA
TCP	94%	94.8%
UDP	4%	0.0%
QUIC	1.8%	1%

COMPARING

1. Both CFDs are bimodal.
2. 576 byte-lengthed protocols are only 2 in website 1 and 0 for the latter two websites. whereas Data collected between 1997 and 2002 reported about fractions of 576 sizes from 10% up to 40%. The usage of the default data- gram size of 576 byte was further decreased to a fraction of only 0.95% in the research paper. (reason: pre-dominance of PMTUD)
3. The article captured BGP, CLNP, CDP, but I did not.
4. The max length seen was 1514. Therefore, no jumbo packets were seen. But in the research they had 0.15% packets with size over 1560. the reason was BGP updates between backbone- or access routers.
5. 628 lengthed protocols cumulated to 1.76% of the protocols in the research (with P2P traffic identified as likely source). Whereas we only had 2 (in numbers!) for the first website.

For all three websites

Res+SYN+FIN	0
RES+SYN	0
SYN+FIN	0
Fin+Res	0

Research article

Anomaly	2AM	10AM	2PM	8PM
RST+SYN+FIN	8	35	11	15
RST+SYN	25	70	43	27
SYN+FIN	4	22	8	9
Zero Flags	32	78	86	90
RST+FIN	10200	10988	14320	16334

	Website 1	Website 2	Website 3	overall	Research
TCP anomalies or loss	5885 (3.68%) 159798	357 (1.01%) 35309	1648 (5.2%) 31200	7890 (3.48%) (226307)	Next page
ECN	687 (0.43%)	1 (0%)	0	688 (0.3%)	0.02%
Ack	154492 (96.67%)	4469 (12.65%)	30185 (96.74%)	189146 (83.57%)	98.6%
PSH	8197 (5.12%)	1942 (5.5%)	3764 (12.06%)	13903 (6.14%)	22.4%
URG	0	0	0	0	663 number
RES	0	0	0	0	
MF solely set	0	0	0	0	0.04%
DF solely set	156032 (97.64%)	30164 (85.42%)	29384 (94.17%)	215580 (95.25%)	91.3%
Neither set	3371 (2.10)	5145 (14.57%)	1816 (5.82%)	10332 (4.56%)	8.65%
Both set	0	0	0	0	NAN

We have not fragmentation in any study case.

8572/10770000000
Very low.

Anomaly	2AM	10AM	2PM	8PM
Undef.Kind	1062	507	413	388
Invalid OL	1200	399	915	3020
Invalid HL	71	528	130	119

Conclusion: The output is pretty much similar to the research output. However, the protocol breakdown in youtube is different and we have a burst of UDP. If we continue watching youtube for long time, we will have a starvation of TCP which will case security issues.
WE have new packets QUIC.
Still most packets are IPv4.