Project 1-Packet Size Distribution and Protocol Breakdown

1

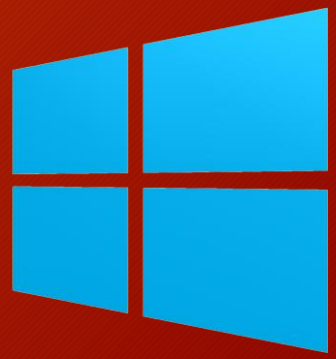
SCICOMP202 Networks and Communications

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.

Joanikij Chulev

Info and Platforms

- Processor: Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz 1.50 GHz
- Installed RAM: 8.00 GB (7.80 GB usable)
- System type: 64-bit operating system, x64-based processor
- OS: Windows
- Edition: Windows 10 Pro
- Version num: 21H1



Tracing was done in Wireshark.
Wireshark version: 3.6.2 (v3.6.2-0-g626020d9b3c3)

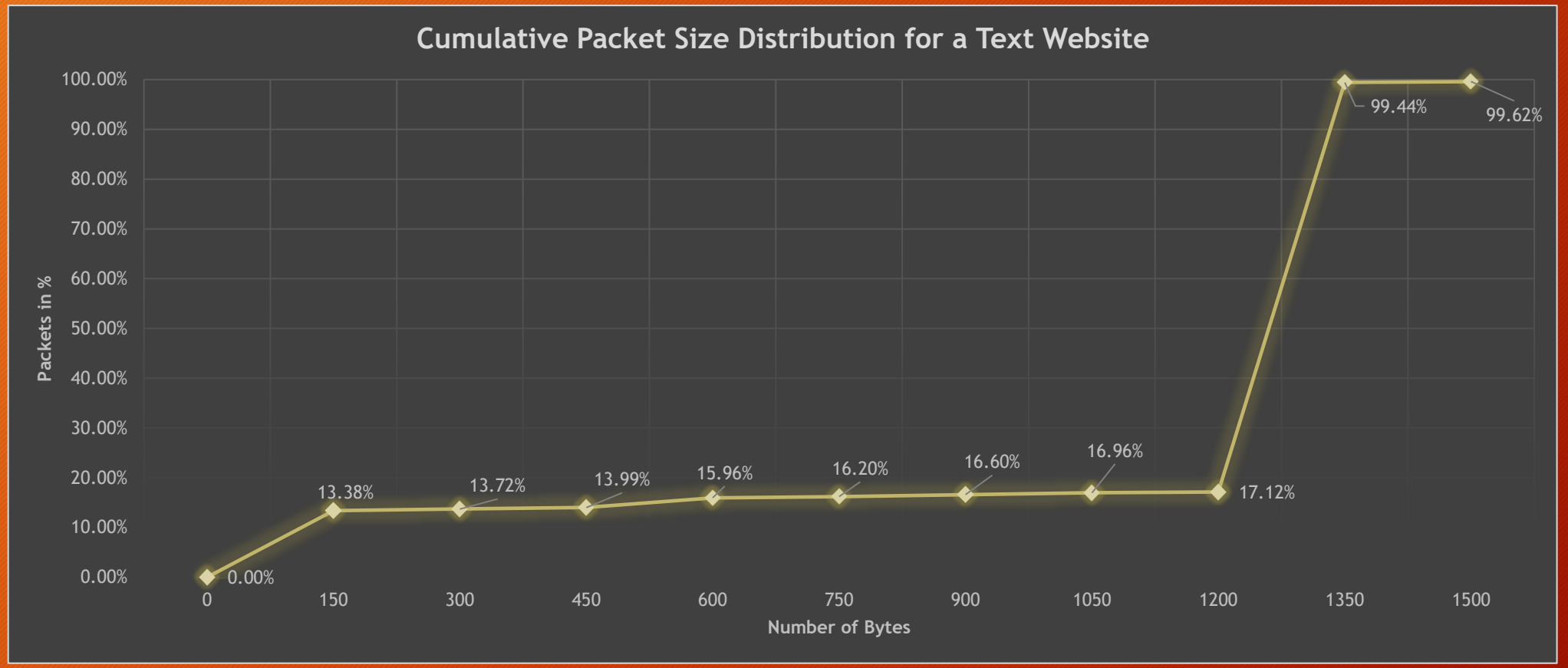
Connection type: Wireless(Wi-fi)
SSID: eduroam

Network adapter(NIC): Intel® wireless-AC 9462

Browsers used: Chrome [Version 98.0.4758.102 (64-bit)] and EDGE [Version 98.0.1108.62 (64-bit)]

Website 1 (mainly plain text download)

Wireshark User's Guide



https://www.wireshark.org/docs/wsug_html/

Website 1 (mainly plain text download)

Wireshark User's Guide

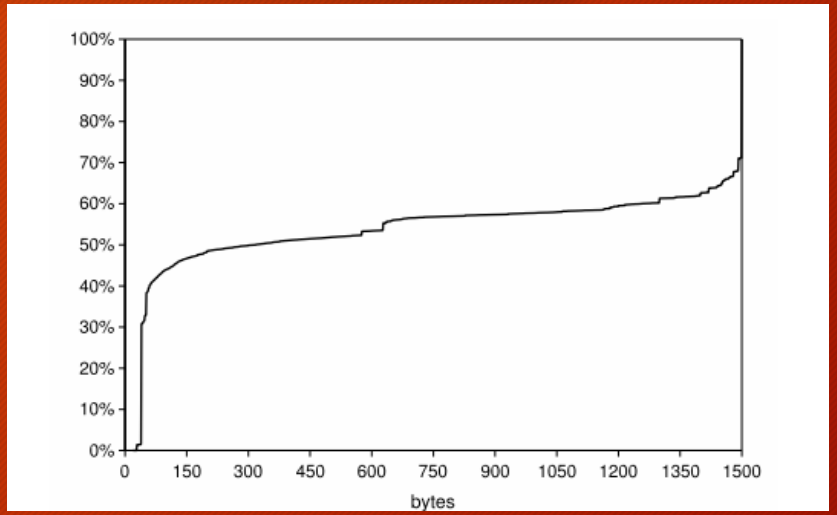
Protocol	Percent Packets %	Percent Bytes %
User Datagram Protocol(UDP)	98.86037063	0.735360242
Simple Service Discovery Protocol(SSDP)	0.39639283	0.006413025
QUIC IETF	98.81082152	94.15744825
Transmission Control Protocol(TCP)	1.139629373	1.962450262
Transport Layer Security(TLS)	0.663957982	2.133104922

https://www.wireshark.org/docs/wsug_html/

Website 1 (mainly plain text download)

Wireshark User's Guide

*Wolfgang John and Sven Tafvelin graph: The distribution is bimodal, with the major portion of lengths between 40 and 100 bytes and between 1400 and 1500 bytes. Mine graph: We can clearly identify that the graph is Bimodal, peaking at 13,38% and 99,94%. We must note that the second peak is much larger. The major portions of the lengths are between 0-150 (13,38%) and between 1200-1350 (82,32%) bytes. It is quite extreme in this regard, reaching its important peak towards the end.

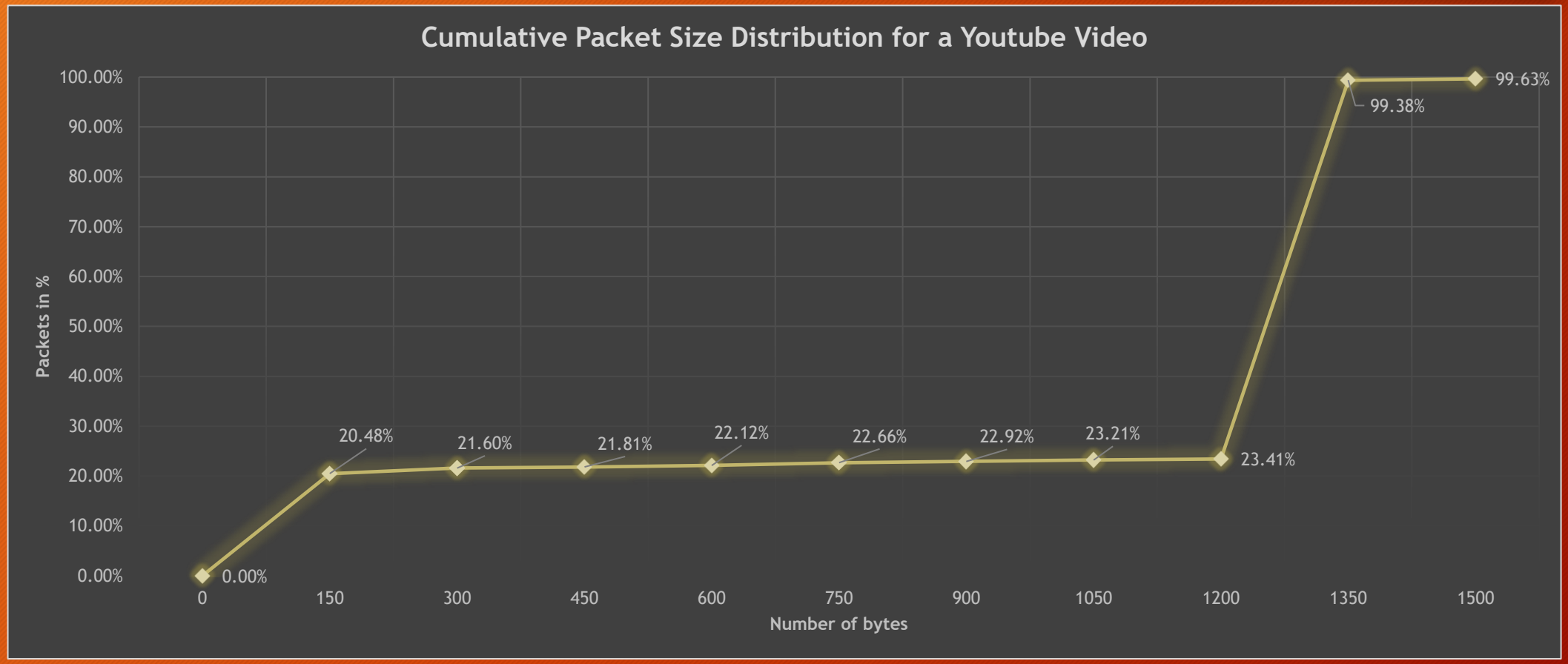


*Most packets in the study by Wolfgang John and Sven Tafvelin seem to be TCP packets - 91.3%, with UDP taking up 8,5%. Contrary, my table shows the exact opposite with TCP taking up 1,1% and UDP packets taking up 98,8%.

	2AM	
	Pkts	Data
TCP	91.3	97.6
UDP	8.5	2.3
ICMP	0.2	0.02
ESP	0.01	0.00
GRE	0.01	0.01

Website 2 (YouTube video)

What Does a Router Do



https://www.youtube.com/watch?v=CVrYEPHexB4

Website 2 (YouTube video)

What Does a Router Do

Protocol	Percent Packets%	Percent Bytes%
User Datagram Protocol(UDP)	94.3941354	0.734712039
QUIC IETF	94.27708988	93.91224212
Domain Name System(DNS)	0.197129305	0.013023961
Transmission Control Protocol(TCP)	5.605864597	2.068921868
Transport Layer Security(TLS)	1.952812173	2.209620206

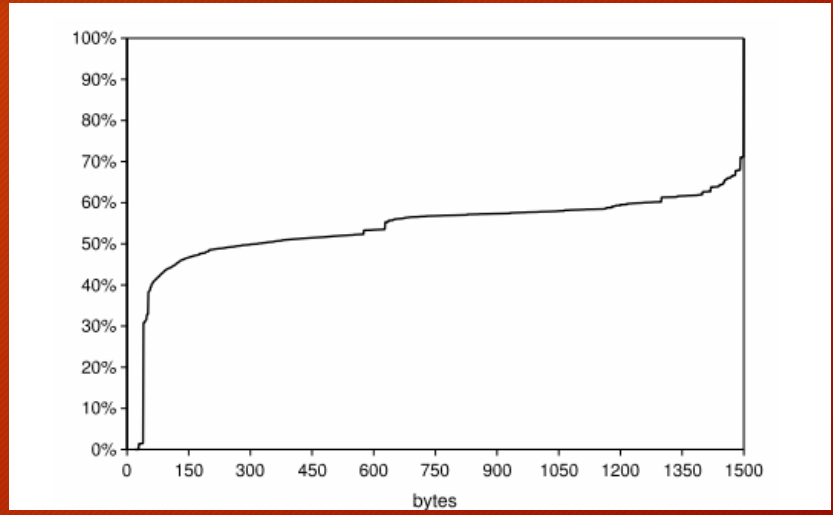
https://www.youtube.com/watch?v=CVrYEPHexB4

DNS data was used instead of SSDP, due to SSDP packets not reaching 0.1%.

Website 2 (YouTube video)

What Does a Router Do

*Wolfgang John and Sven Tafvelin graph: The distribution is bimodal, with the major portion of lengths between 40 and 100 bytes and between 1400 and 1500 bytes. Mine graph: We can clearly identify that the graph is Bimodal, peaking at 20,48% and 99,38%. We must note that the second peak is much larger. The major portions of the lengths are between 0-150 (20,48%) and between 1200-1350 (75,97%) bytes. It is quite extreme in this regard, reaching its important peak towards the end.

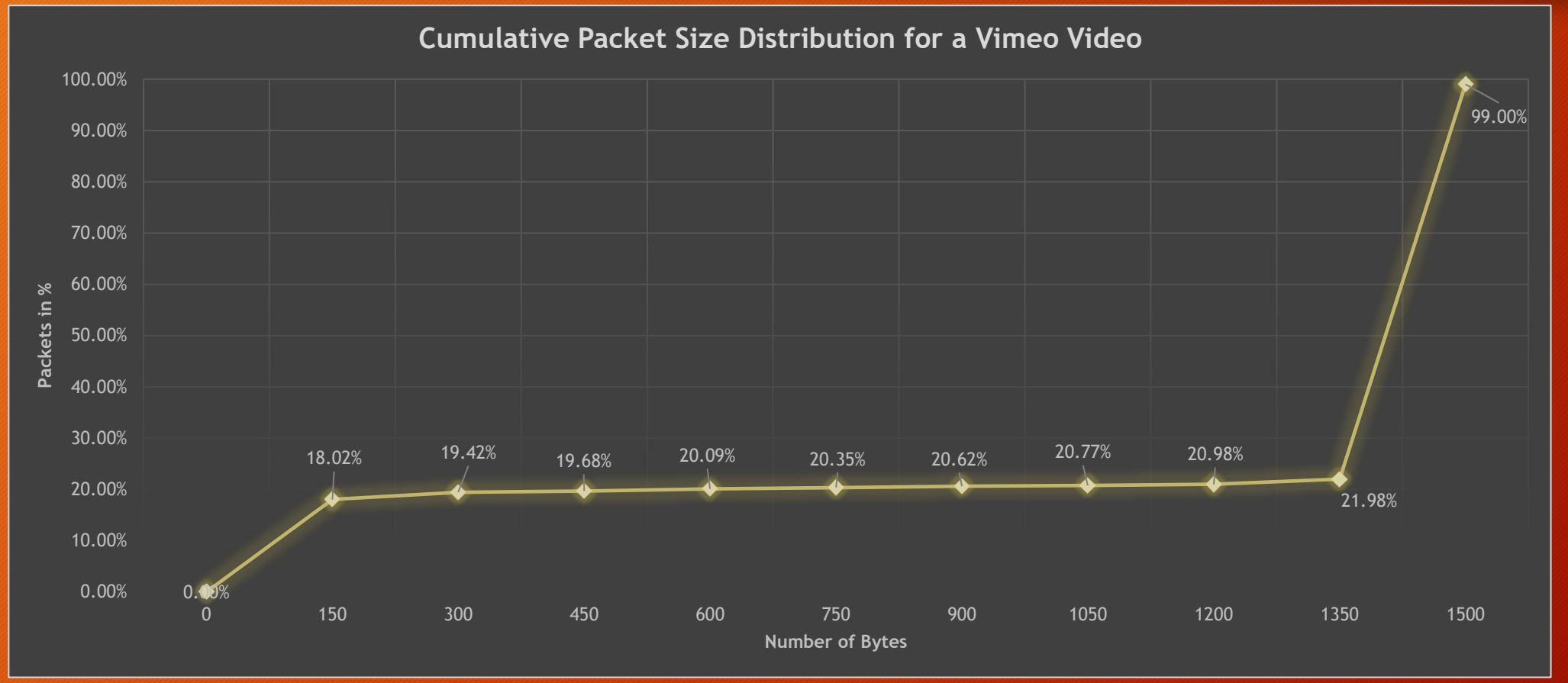


*Most packets in the study by Wolfgang John and Sven Tafvelin seem to be TCP packets - 91.3%, with UDP taking up 8,5%. Contrary, my table shows the exact opposite with TCP taking up 5,6% and UDP packets taking up 94,4%.

	2AM	
	Pkts	Data
TCP	91.3	97.6
UDP	8.5	2.3
ICMP	0.2	0.02
ESP	0.01	0.00
GRE	0.01	0.01

Website 3 (Vimeo video)

Catchpoint Traceroute Demo



https://vimeo.com/366765726

Website 3 (Vimeo video)

Catchpoint Traceroute Demo

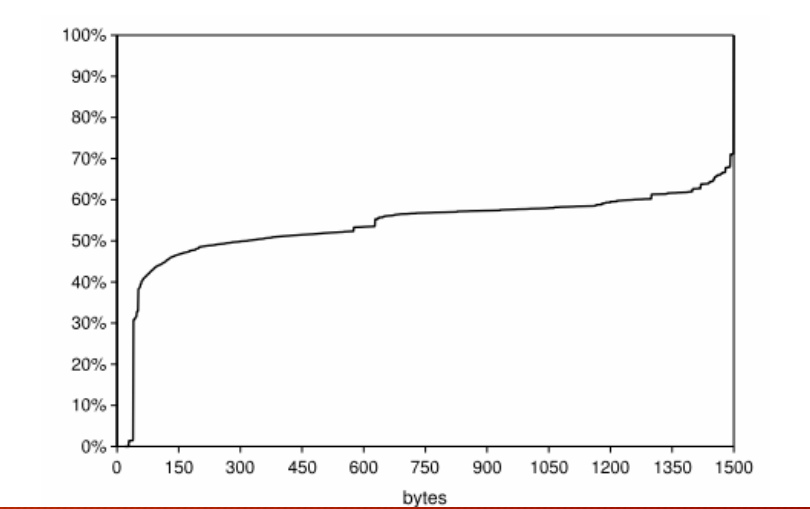
Protocol	Percent Packets%	Percent Bytes%
User Datagram Protocol(UDP)	90.73472745	0.547233433
QUIC IETF	90.61349959	85.6789158
Domain Name System(DNS)	0.129886998	0.007226552
Transmission Control Protocol(TCP)	9.265272546	11.20291182
Transport Layer Security(TLS)	4.242975278	12.47645944

https://vimeo.com/366765726

Website 3 (Vimeo video)

Catchpoint Traceroute Demo

*Wolfgang John and Sven Tafvelin graph: The distribution is bimodal, with the major portion of lengths between 40 and 100 bytes and between 1400 and 1500 bytes. Mine graph: We can clearly identify that the graph is Bimodal, peaking at 18,02% and 99%. We must note that the second peak is much larger. The major portions of the lengths are between 0-150 (18,02%) and between 1350-1500 (77%) bytes. The majority is in the 1350-1500 byte segment unlike the previous website downloads. It is quite extreme in this regard, reaching its important peak towards the end.



*Most packets in the study by Wolfgang John and Sven Tafvelin seem to be TCP packets - 91.3%, with UDP taking up 8,5%. Contrary, my table shows the exact opposite with TCP taking up 9,3% and UDP packets taking up 90,7%.

	2AM	
	Pkts	Data
TCP	91.3	97.6
UDP	8.5	2.3
ICMP	0.2	0.02
ESP	0.01	0.00
GRE	0.01	0.01

*TLS packet seem to take a large portion of the data in this analysis! (12,5%).
*5Xtimes more than the other website downloads!

Summary and conclusions

The study findings

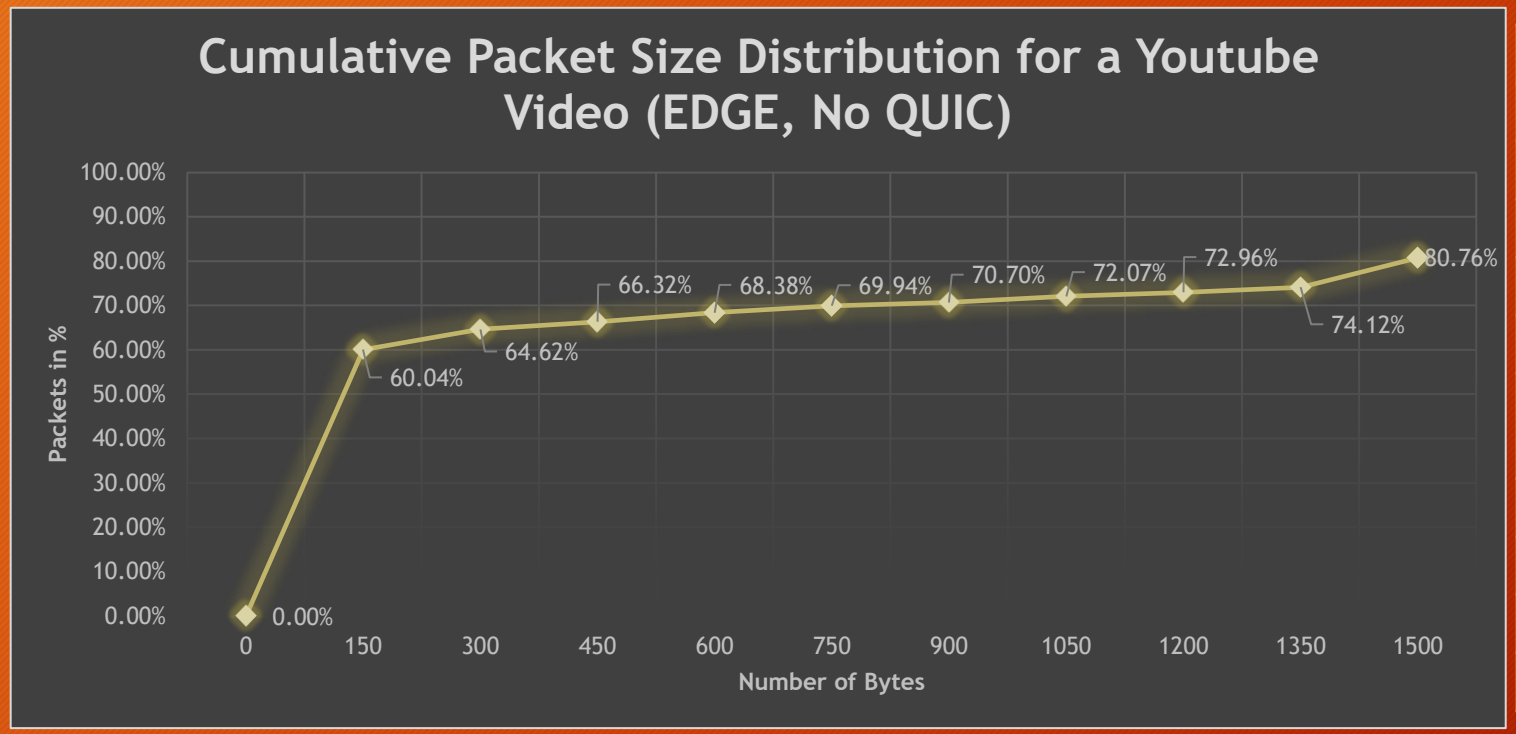
- Regarding packet size distribution, two findings should be noted. First, IP packet lengths of 628 bytes have become even more common than the default datagram size, with P2P traffic identified as likely source. Second, except for router traffic, jumbo packets are used for a single custom application only and are not seen otherwise.
- (http://conferences.sigcomm.org/imc/2007/papers/imc91.pdf)

My findings

- With the invention of the QUIC protocol (Quick UDP internet connection) used for low-latency transportation often used for apps and services that require speedy online service, the majority of the packets are UDP packets containing the majority of the data. IP packet lengths of 1242 bytes(~70%) are the most common by far, as well as 54-88 bytes (~15%).

Extra credit: Browser differences – using EDGE

- For this part I used edge for the Youtube video, as well as disabling the QUIC protocol. Results:
- Instead of UDP (2,4%), most packets were TCP (94,9%).



Now the IPV6 header is used in combination with the IPV4.

Protocol	Percent Packets	Percent Bytes
Internet Protocol Version 6	0.078719496	0.00073282
User Datagram Protocol	0.078719496	0.000146564
Multicast Domain Name System	0.078719496	0.00073282
Internet Protocol Version 4	97.27105747	0.452760843
User Datagram Protocol	2.335345054	0.004348067
Simple Service Discovery Protocol	0.314877985	0.012751074
Multicast Domain Name System	0.078719496	0.00073282
Domain Name System	1.941747573	0.035273086
Transmission Control Protocol	94.93571241	99.13228574
Transport Layer Security	53.1094201	112.1155296

Extra credit: IP Flags

- The study: The analysis of the IP flags (fragment bits) revealed that 91.3% of all observed IP packets have the don't fragment bit (DF) set, as proposed by Path MTU Discovery (RFC 1191). 8.65% use neither DF nor MF (more fragments) and 0.04% set solely the MF bit.
- *Using the ip.flags filters I found the following results in the Website 1 (mainly plain text download) trace file.*
- In my analysis almost all packets 10078 (99.9%) have the don't fragment bit (DF) set. Also a very high percentile, corresponding to the study. Only 13(0.1%) of the packets have the don't fragment bit (DF): not set. (as well as having a value of Flags: 0x00). Although, unlike the study none of the packets seemed to have the More Fragments (MF) bit to set/use it. Meaning, all 10091 (100.0%) of the packets had this bit to not set.

Most of the IP flag fields(~99%) were resembled like this. With these given values.