CS 6043/5143: Computer Networking

FALL 2019

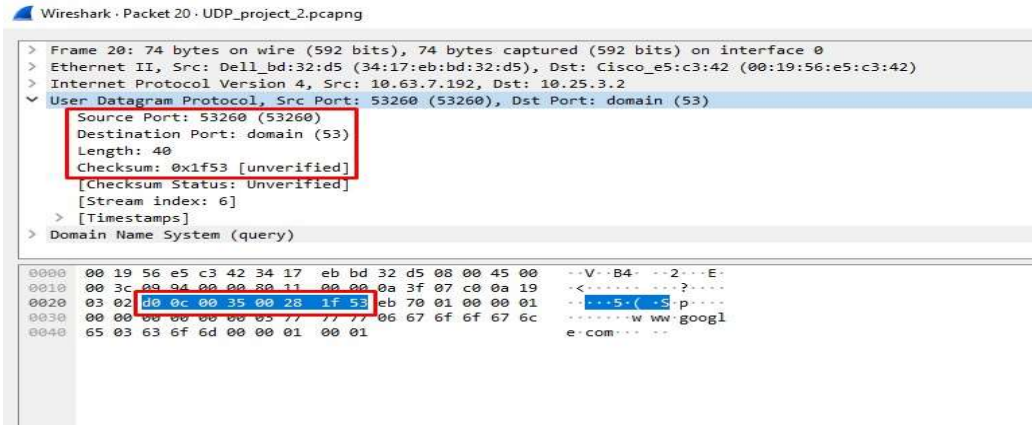
PROJECT

Part I: UDP

Open the file 'UDP_project_2.pcapng' in Wireshark and answer the following questions. Provide screenshots with necessary annotations in each case.

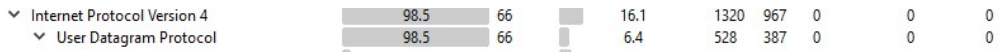
1. Find a UDP packet in the trace file and determine the name and length (in bytes) of each of the UDP header fields.

Ans: UDP header has length of 8 bytes. Header length is 2 bytes long.



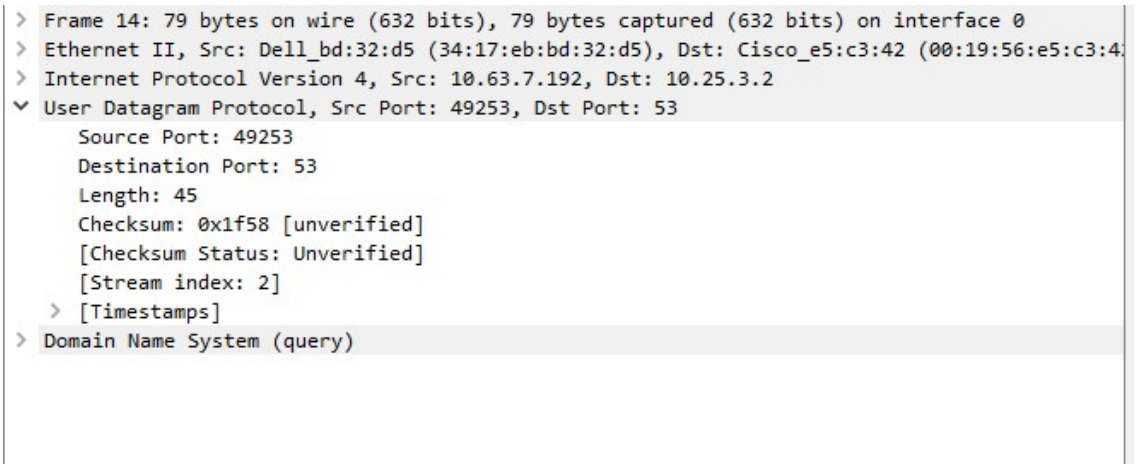
2. Using statistics feature of Wireshark, determine the percentage of IPv4 UDP packets in the capture.

Ans:



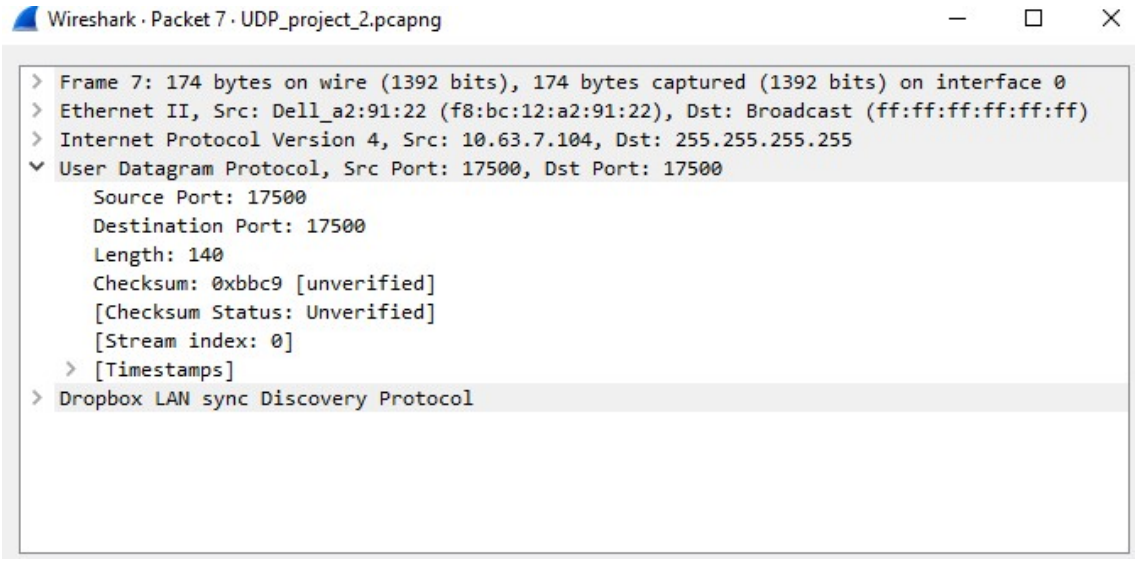
3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

Ans: The length is the number of bytes in the UDP segment.An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.The length of UDP payload for selected packet is 45-8=37bytes



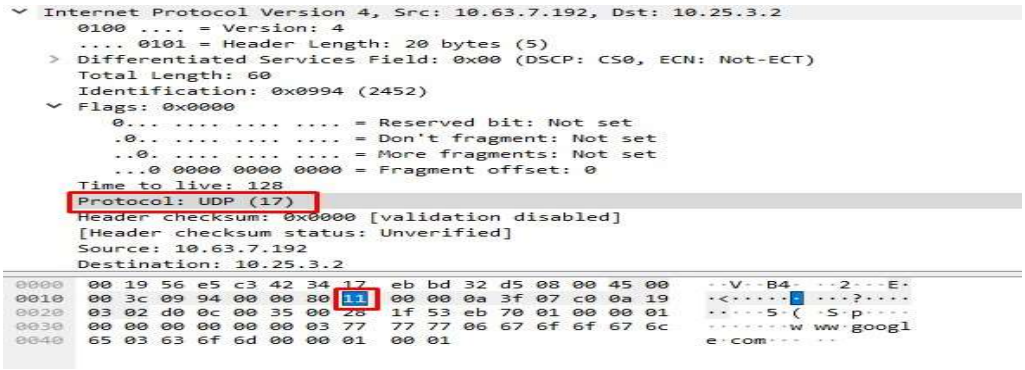
4. What are the source port and length of the first UDP packet in the trace file? What is the largest possible source port number?

Ans: The source port is 17500 and length is 140 bytes. This is a Dropbox LAN sync discovery protocol packet.The largest possible port number is 2^{16}-1= 65535



5. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notations along with a screenshot of Wireshark showing those values.

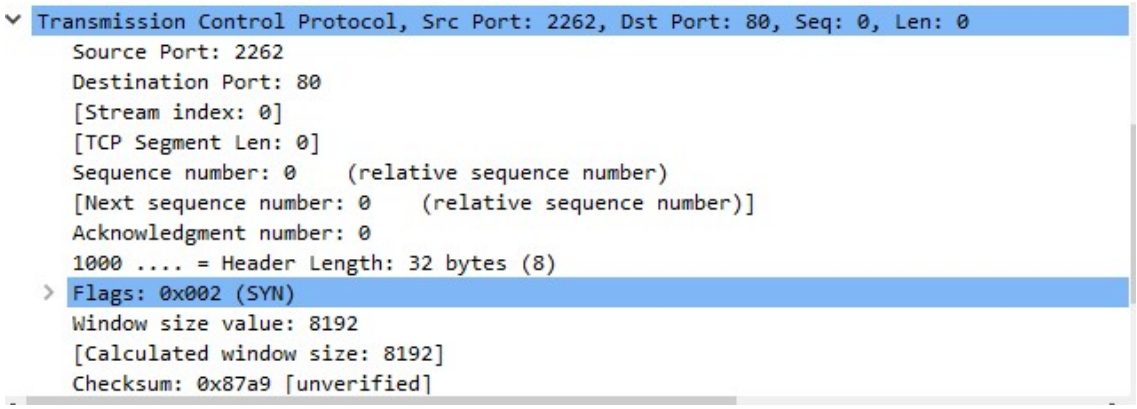
Ans: The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

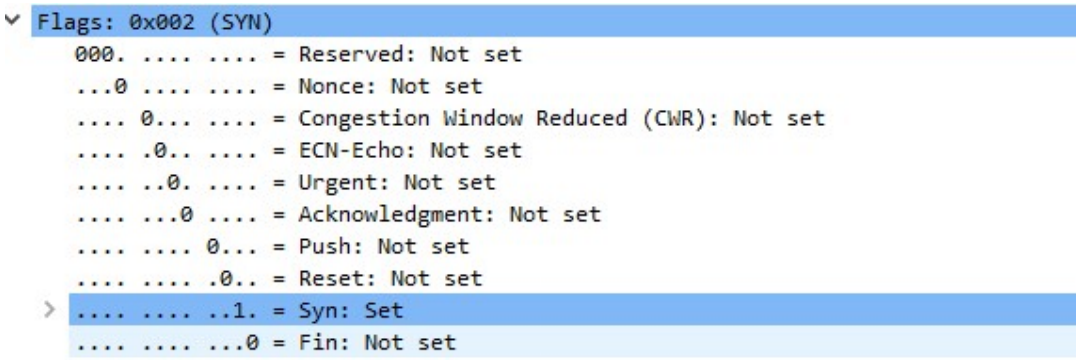


Part II: TCP

1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and *gaia.cs.umass.edu*?

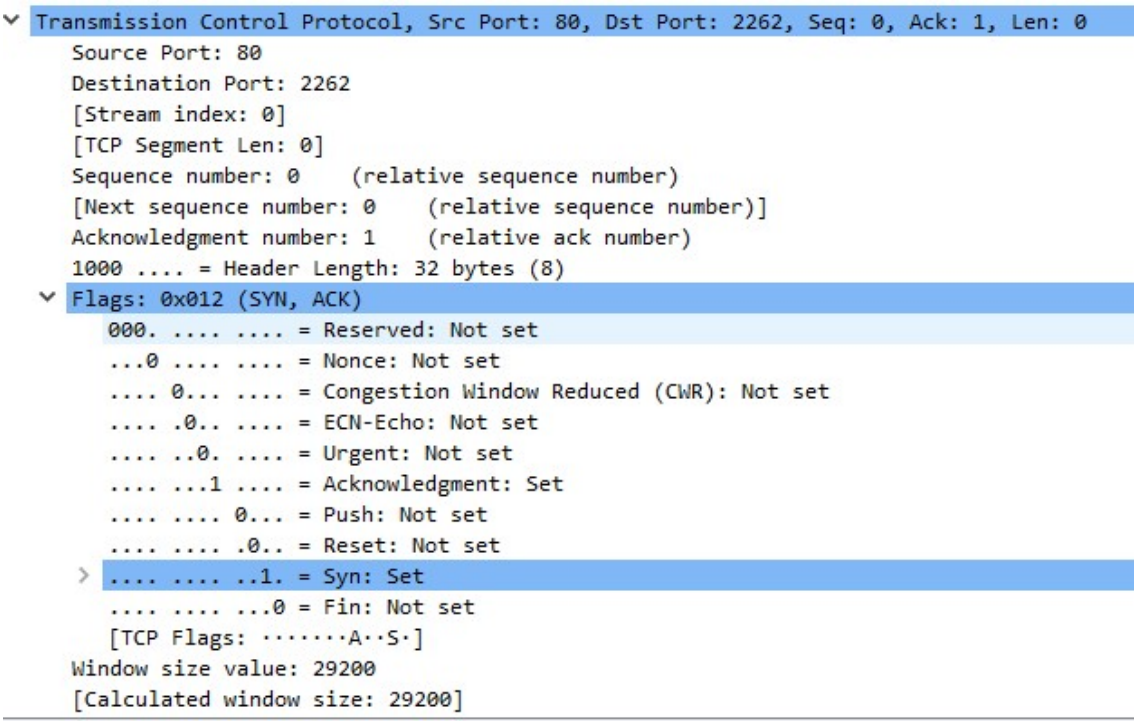
Ans: The sequence number of the TCP SYN segment is 0 since it is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu.





2. What are the sequence number and acknowledgement number of the first SYNACK packet sent from the server to the client computer? How were the values determined by the server? *(hint: relative seq and ack values displayed by Wireshark is fine, no need to show actual numbers)*

Ans: Sequence number of the SYNACK segment from gaia.cs.umass.edu to the client computer in reply to the SYN has the value of 0 in this trace. The value of the ACK in SYNACK segment is 1. The value of the ACK field in the SYNACK segment is determined by gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment.



3. What are the minimum and maximum amount of available buffer spaces advertised at the receiver for the entire trace?

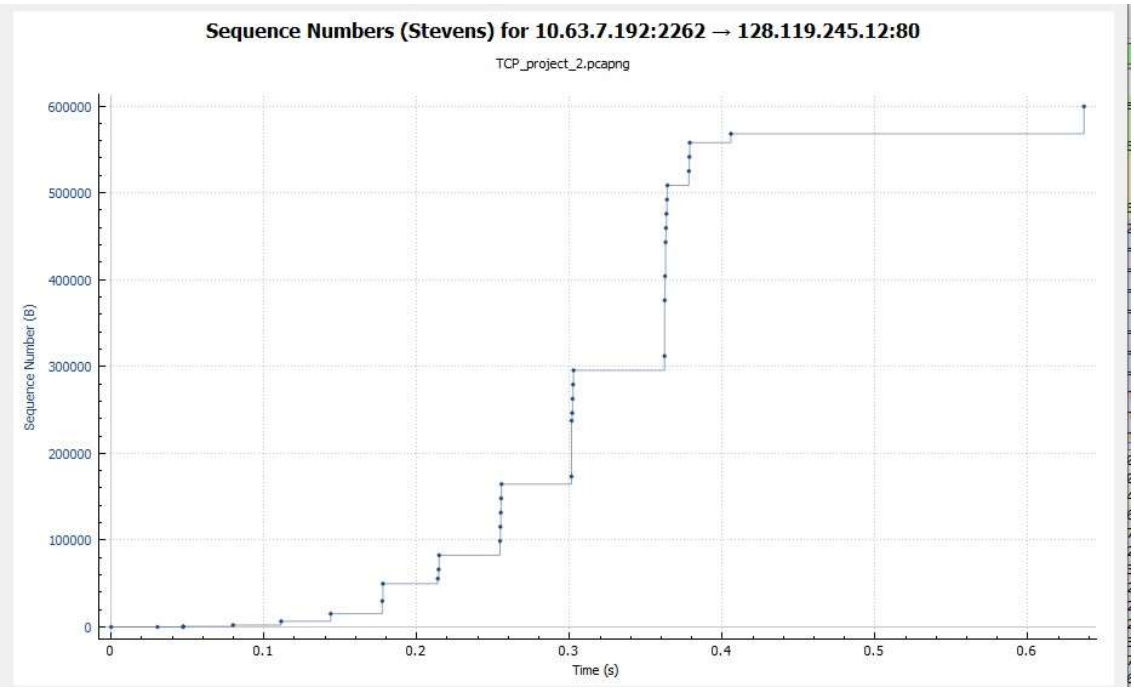
Ans:The minimum amount of buffer space (receiver window) advertised at gaia.cs.umass.edu for the entire trace is 29200 bytes, which is shown in the first acknowledgment from the server. This receiver window grows steadily until a maximum receiver buffer size of 843392 bytes.

2	0.628600	10.63.7.192	128.119.245.12	TCP	66	2262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	0.658848	128.119.245.12	10.63.7.192	TCP	66	80 → 2262 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
9	0.658917	10.63.7.192	128.119.245.12	TCP	54	2262 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
10	0.659350	10.63.7.192	10.52.5.208	SMB2	346	Create Request File: sadatms\desktop\1600.txt
11	0.659673	10.52.5.208	10.63.7.192	SMB2	354	Create Response File: sadatms\desktop\1600.txt
12	0.660541	10.63.7.192	10.52.5.208	SMB2	171	Read Request Len:32768 Off:0 File: sadatms\desktop\1600.txt
13	0.661587	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=301 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]
14	0.661588	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=1761 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]
15	0.661589	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=3221 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]
16	0.661590	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=4681 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]
17	0.661591	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=6141 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]
18	0.661618	10.63.7.192	10.52.5.208	TCP	54	64061 → 445 [ACK] Seq=410 Ack=7601 Win=256 Len=0
19	0.661915	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=7601 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]
20	0.661916	10.52.5.208	10.63.7.192	TCP	1514	445 → 64061 [ACK] Seq=9061 Ack=410 Win=251 Len=1460 [TCP segment of a reassembled PDU]

No.	Time	Source	Destination	Protocol	Length	Info
767	1.064754	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=572317 Win=824576 Len=0
768	1.064755	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=573777 Win=827520 Len=0
769	1.064755	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=575237 Win=830464 Len=0
770	1.064756	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=576697 Win=833280 Len=0
771	1.065471	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=578157 Win=836224 Len=0
772	1.065473	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=579617 Win=839168 Len=0
773	1.065474	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=581077 Win=842112 Len=0
774	1.065475	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=582537 Win=843392 Len=0
775	1.065476	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=585457 Win=843392 Len=0
776	1.066308	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=588377 Win=843392 Len=0
777	1.066310	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=591297 Win=843392 Len=0
778	1.066311	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=594217 Win=843392 Len=0
779	1.067085	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=597137 Win=843392 Len=0
780	1.067087	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=599394 Win=843392 Len=0
781	1.067088	128.119.245.12	10.63.7.192	HTTP	831	HTTP/1.1 200 OK (text/html)
789	2.002046	172.217.7.206	10.63.7.192	TCP	66	https(443) → mnp-exchange(2197) [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2

4. Are there any retransmitted segments in the trace file? What is the reasoning behind your answer?

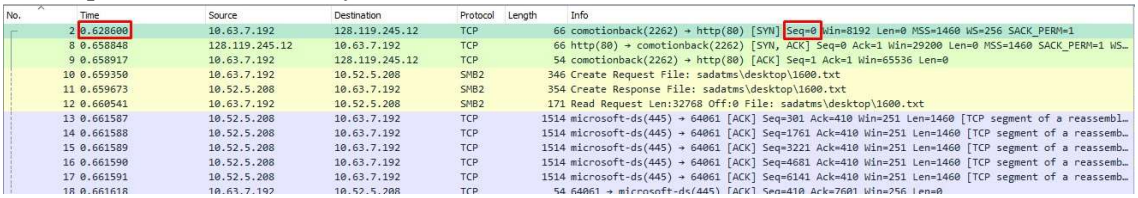
Ans: There are no retransmitted segments in the trace file. In the *Time-Sequence-Graph (Stevens)* of this trace, all the sequence numbers from source (10.63.7.192) to the destination (128.119.245.12) are increasing with respect to time. If there is a retransmitted segment, the sequence number of this retransmitted segment should be less than those of its neighboring segments.



5. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

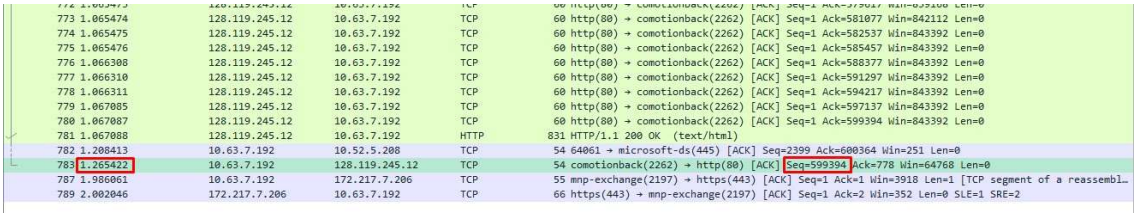
Ans: Throughput = Total amount of data / Total transmission time

In this packet trace, M = 0 bytes for frame #2 and t1 = 0.628600 seconds



No.	Time	Source	Destination	Protocol	Length	Info
2	0.628600	10.63.7.192	128.119.245.12	TCP	66	comotionback(2262) → http(80) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	0.658848	128.119.245.12	10.63.7.192	TCP	66	http(80) → comotionback(2262) [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS…
9	0.658917	10.63.7.192	128.119.245.12	TCP	54	comotionback(2262) → http(80) [ACK] Seq=1 Ack=1 Win=65536 Len=0
10	0.659350	10.63.7.192	10.52.5.208	SMB2	346	Create Request File: sadatms\desktop\1600.txt
11	0.659673	10.52.5.208	10.63.7.192	SMB2	354	Create Response File: sadatms\desktop\1600.txt
12	0.660541	10.63.7.192	10.52.5.208	SMB2	171	Read Request Len:32768 Off:0 File: sadatms\desktop\1600.txt
13	0.661587	10.52.5.208	10.63.7.192	TCP	1514	microsoft-ds(445) → 64061 [ACK] Seq=301 Ack=410 Win=251 Len=1460 [TCP segment of a reassembl…
14	0.661588	10.52.5.208	10.63.7.192	TCP	1514	microsoft-ds(445) → 64061 [ACK] Seq=1761 Ack=410 Win=251 Len=1460 [TCP segment of a reassemb…
15	0.661589	10.52.5.208	10.63.7.192	TCP	1514	microsoft-ds(445) → 64061 [ACK] Seq=3221 Ack=410 Win=251 Len=1460 [TCP segment of a reassemb…
16	0.661590	10.52.5.208	10.63.7.192	TCP	1514	microsoft-ds(445) → 64061 [ACK] Seq=4681 Ack=410 Win=251 Len=1460 [TCP segment of a reassemb…
17	0.661591	10.52.5.208	10.63.7.192	TCP	1514	microsoft-ds(445) → 64061 [ACK] Seq=6141 Ack=410 Win=251 Len=1460 [TCP segment of a reassemb…
18	0.661618	10.63.7.192	10.52.5.208	TCP	54	64061 → microsoft-ds(445) [ACK] Seq=410 Ack=7601 Win=256 Len=0

N = 599394 bytes for frame #783 and t2 = 1.265422 seconds



773	1.065474	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=581077 Win=842112 Len=0
774	1.065475	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=582537 Win=843392 Len=0
775	1.065476	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=585457 Win=843392 Len=0
776	1.066308	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=588377 Win=843392 Len=0
777	1.066310	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=591297 Win=843392 Len=0
778	1.066311	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=594217 Win=843392 Len=0
779	1.067085	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=597137 Win=843392 Len=0
780	1.067087	128.119.245.12	10.63.7.192	TCP	60	http(80) → comotionback(2262) [ACK] Seq=1 Ack=599394 Win=843392 Len=0
781	1.067088	128.119.245.12	10.63.7.192	HTTP	831	HTTP/1.1 200 OK (text/html)
782	1.208413	10.63.7.192	10.52.5.208	TCP	54	64061 → microsoft-ds(445) [ACK] Seq=2399 Ack=600364 Win=251 Len=0
783	1.265422	10.63.7.192	128.119.245.12	TCP	54	comotionback(2262) → http(80) [ACK] Seq=599394 Ack=778 Win=64768 Len=0
787	1.986061	10.63.7.192	172.217.7.206	TCP	55	mnp-exchange(2197) → https(443) [ACK] Seq=1 Ack=1 Win=3918 Len=1 [TCP segment of a reassembl…
789	2.002046	172.217.7.206	10.63.7.192	TCP	66	https(443) → mnp-exchange(2197) [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2

Throughput = (N-M)/ (t2-t1)

= (599394 – 0)/ (1.265422 – 0.6286)

= 599394/0.636822

= 941,226.9

= 941.2 K bytes per second.