Institute of Information Technology

University of Dhaka

Assignment on TCP protocol observation

Submitted to:

Professor Md. Shariful Islam

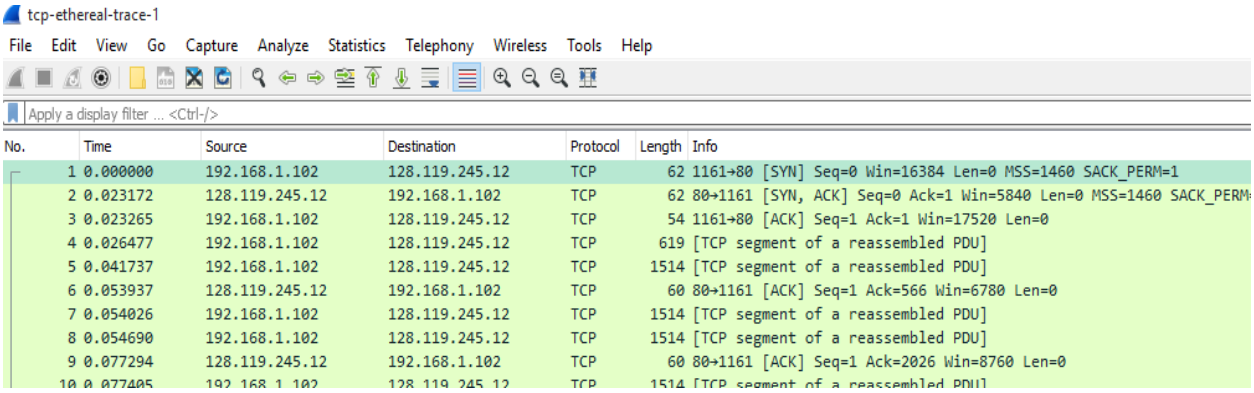
IIT,DU

Submitted by:

Tulshi Chandra Das

Roll:811

1.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161→80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80→1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161→80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	[TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80→1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80→1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]

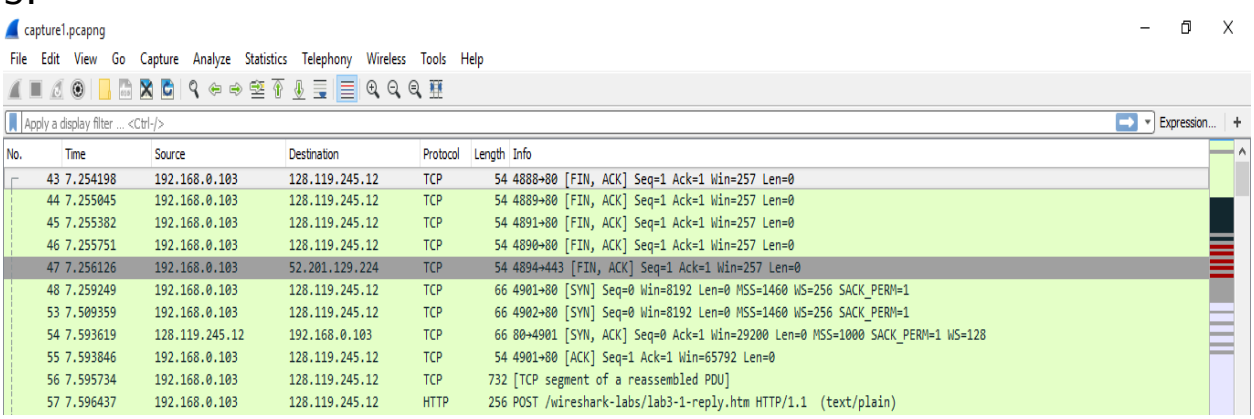
IP address and TCP port number used by the client computer:

192.168.1.102 and 1161

2.

gaia.cs.umass.edu's IP address is *128.119.245.12*, port number is *80*

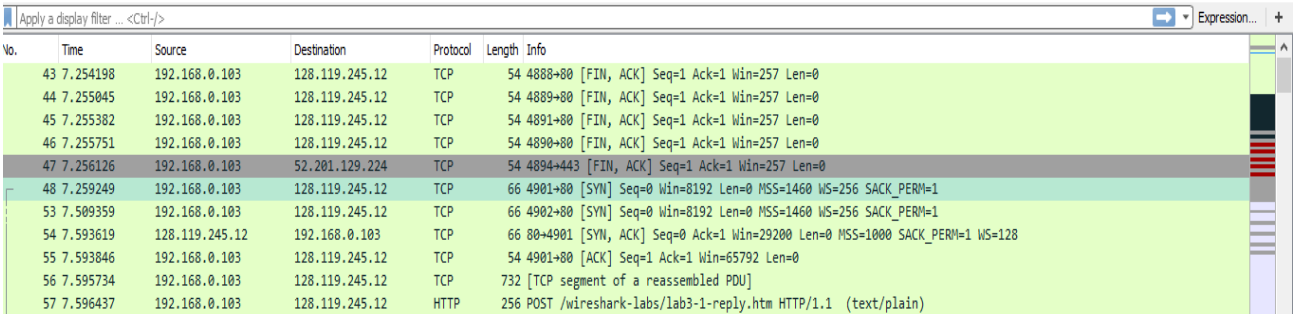
3.



No.	Time	Source	Destination	Protocol	Length	Info
43	7.254198	192.168.0.103	128.119.245.12	TCP	54	4888→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
44	7.255045	192.168.0.103	128.119.245.12	TCP	54	4889→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
45	7.255382	192.168.0.103	128.119.245.12	TCP	54	4891→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
46	7.255751	192.168.0.103	128.119.245.12	TCP	54	4890→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
47	7.256126	192.168.0.103	52.201.129.224	TCP	54	4894→443 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
48	7.259249	192.168.0.103	128.119.245.12	TCP	66	4901→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
53	7.509359	192.168.0.103	128.119.245.12	TCP	66	4902→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
54	7.593619	128.119.245.12	192.168.0.103	TCP	66	80→4901 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1000 SACK_PERM=1 WS=128
55	7.593846	192.168.0.103	128.119.245.12	TCP	54	4901→80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
56	7.595734	192.168.0.103	128.119.245.12	TCP	732	[TCP segment of a reassembled PDU]
57	7.596437	192.168.0.103	128.119.245.12	HTTP	256	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)

Sorce ip: 192.168.0.103; source port: 4894

4.

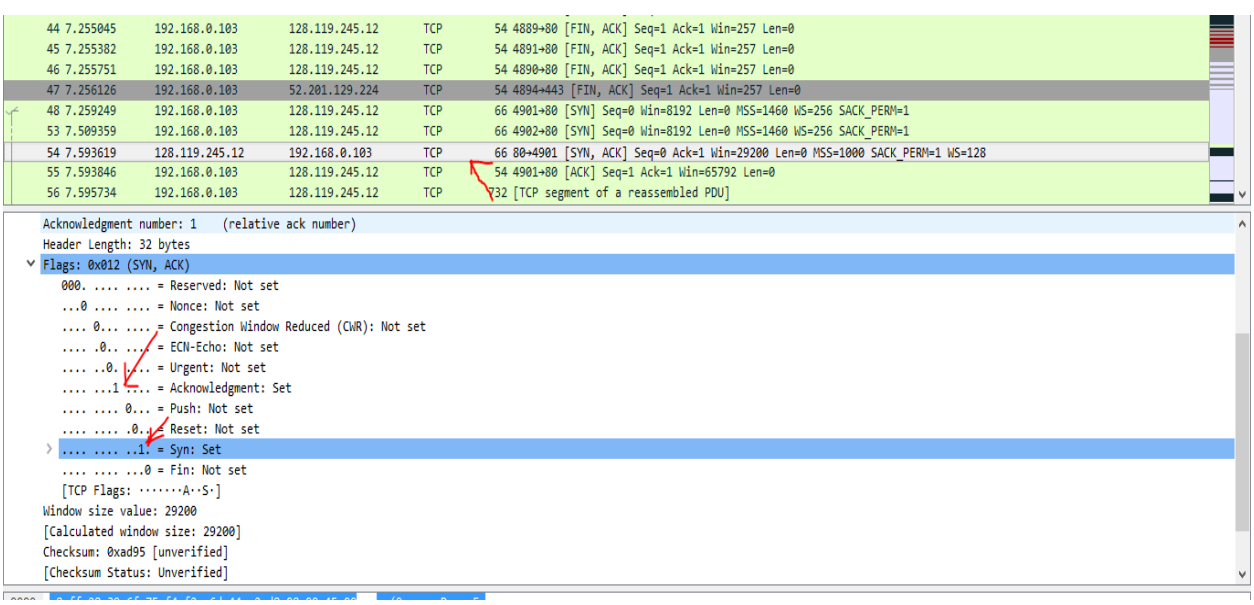


No.	Time	Source	Destination	Protocol	Length	Info
43	7.254198	192.168.0.103	128.119.245.12	TCP	54	4888→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
44	7.255045	192.168.0.103	128.119.245.12	TCP	54	4889→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
45	7.255382	192.168.0.103	128.119.245.12	TCP	54	4891→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
46	7.255751	192.168.0.103	128.119.245.12	TCP	54	4890→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
47	7.256126	192.168.0.103	52.201.129.224	TCP	54	4894→443 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
48	7.259249	192.168.0.103	128.119.245.12	TCP	66	4901→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
53	7.509359	192.168.0.103	128.119.245.12	TCP	66	4902→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
54	7.593619	128.119.245.12	192.168.0.103	TCP	66	80→4901 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1000 SACK_PERM=1 WS=128
55	7.593846	192.168.0.103	128.119.245.12	TCP	54	4901→80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
56	7.595734	192.168.0.103	128.119.245.12	TCP	732	[TCP segment of a reassembled PDU]
57	7.596437	192.168.0.103	128.119.245.12	HTTP	256	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)

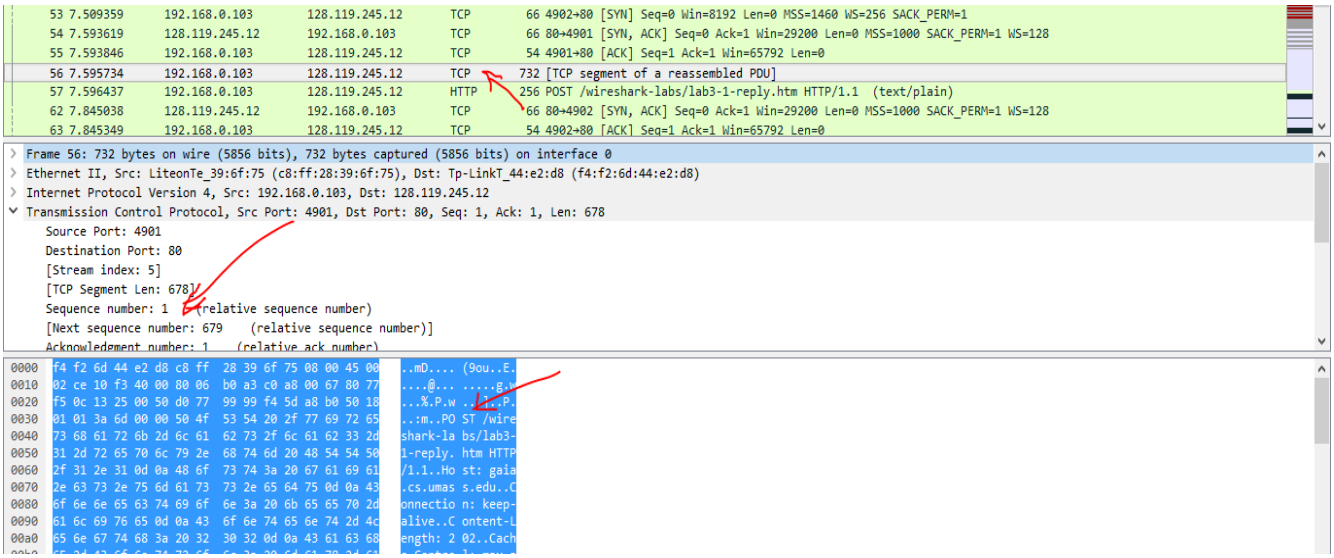
Seq number: 0. At flag part SYN in set to 1, so it is SYN segment.

5.

According to the screenshot below, the sequence number of the SYN_ACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0. The value of the acknowledgement field in the SYN_ACK segment is determined by the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of the SYN segment from the client computer. For this case, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the acknowledgement field in the SYN_ACK segment is 1. A segment will be identified as a SYN_ACK segment if both SYN flag and ACKnowledgement flag in the segment are set to 1.



6.



Seq number: 1

7.

Sequence number for segment 1 is 1,

Sequence number for segment 2 is 881.

Sequence number of segment 3 is 0.

Sequence number of segment 4 is 1.

Sequence number of segment 5 is 1.

Sequence number of segment 6 is 1.

No.	Time	Source	Destination	Protocol	Length	Info
52	7.410138	172.168.121.130	224.0.0.252	LLMNR	66	Standard query 0xcc50 A isatap
53	7.509359	192.168.0.103	128.119.245.12	TCP	66	4902→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
54	7.593619	128.119.245.12	192.168.0.103	TCP	66	80→4901 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1000 SACK_PERM=1 WS=128
55	7.593846	192.168.0.103	128.119.245.12	TCP	54	4901→80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
56	7.595734	192.168.0.103	128.119.245.12	TCP	732	[TCP segment of a reassembled PDU]
57	7.596437	192.168.0.103	128.119.245.12	HTTP	256	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
58	7.678586	fe80::f512:3651:5d1…	ff02::1:3	LLMNR	84	Standard query 0xc576 A wpad
59	7.679470	192.168.0.103	224.0.0.252	LLMNR	64	Standard query 0xc576 A wpad
60	7.752517	172.168.121.130	224.0.0.252	LLMNR	66	Standard query 0xdf4b A isatap
61	7.845037	172.168.121.130	224.0.0.252	LLMNR	66	Standard query 0xcc50 A isatap
62	7.845038	128.119.245.12	192.168.0.103	TCP	66	80→4902 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1000 SACK_PERM=1 WS=128
63	7.845349	192.168.0.103	128.119.245.12	TCP	54	4902→80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
64	7.917434	128.119.245.12	192.168.0.103	TCP	54	80→4901 [ACK] Seq=1 Ack=679 Win=30592 Len=0
65	7.936156	128.119.245.12	192.168.0.103	TCP	54	80→4901 [ACK] Seq=1 Ack=881 Win=32000 Len=0
66	7.936302	128.119.245.12	192.168.0.103	HTTP	831	HTTP/1.1 200 OK (text/html)
67	7.987162	192.168.0.103	128.119.245.12	TCP	54	4901→80 [ACK] Seq=881 Ack=778 Win=65024 Len=0
68	8.015434	192.168.0.103	192.168.0.255	NBNS	92	Name query NB WPAD<00>
69	8.111527	192.168.0.103	128.119.245.12	TCP	54	[TCP Retransmission] 4890→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0

b.

Time for segment 1: 7.595734

Time for segment 2: 7.5964377

Time for segment 3: 7.845038

Time for segment 4: 7.845349

Time for segment 5: 7.917434

Time for segment 6: 7.936156

8.

Length for segment 1: 732

Length for segment 1: 256

Length for segment 1: 66

Length for segment 1: 54

Length for segment 1: 54

Length for segment 1: 54

9.

Available Buffer Space for segment 1:65792

Available Buffer Space for segment 2:65792

Available Buffer Space for segment 3:29200

Available Buffer Space for segment 4:65792

Available Buffer Space for segment 5:30592

Available Buffer Space for segment 6:32000

10.

Yes, there are some retransmitted segments in the trace file. This can be explained by packets with same sequence number at different time is not found.

No.	Time	Source	Destination	Protocol	Length	Info
64	7.917434	128.119.245.12	192.168.0.103	TCP	54	80→4901 [ACK] Seq=1 Ack=679 Win=30592 Len=0
65	7.936156	128.119.245.12	192.168.0.103	TCP	54	80→4901 [ACK] Seq=1 Ack=881 Win=32000 Len=0
66	7.936302	128.119.245.12	192.168.0.103	HTTP	831	HTTP/1.1 200 OK (text/html)
67	7.987162	192.168.0.103	128.119.245.12	TCP	54	4901→80 [ACK] Seq=881 Ack=778 Win=65024 Len=0
68	8.015434	192.168.0.103	192.168.0.255	NBNS	92	Name query NB WPAD<00>
69	8.111527	192.168.0.103	128.119.245.12	TCP	54	[TCP Retransmission] 4890→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
70	8.157714	192.168.0.103	52.201.129.224	TCP	54	[TCP Retransmission] 4894→443 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
71	8.174905	172.168.121.130	224.0.0.252	LLMNR	66	Standard query 0xdf4b A isatap
72	8.283484	192.168.0.103	128.119.245.12	TCP	54	[TCP Retransmission] 4888→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
73	8.370414	192.168.0.103	128.119.245.12	TCP	54	[TCP Retransmission] 4891→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
74	8.373187	192.168.0.103	128.119.245.12	TCP	54	[TCP Retransmission] 4889→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
75	8.705529	LiteonTe_39:6f:75	IntelCor_36:6b:36	ARP	42	Who has 192.168.0.110? Tell 192.168.0.103
76	8.710297	IntelCor_36:6b:36	LiteonTe_39:6f:75	ARP	42	192.168.0.110 is at 00:db:df:36:6b:36
77	8.766452	192.168.0.103	192.168.0.255	NBNS	92	Name query NB WPAD<00>
78	9.721325	192.168.0.103	128.119.245.12	TCP	54	[TCP Retransmission] 4890→80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
79	9.754381	172.168.121.130	224.0.0.252	LLMNR	66	Standard query 0x78f8 A isatap
80	9.861640	192.168.0.103	52.201.129.224	TCP	54	[TCP Retransmission] 4894→443 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
81	10.158761	172.168.121.130	224.0.0.252	LLMNR	66	Standard query 0x78f8 A isatap

11.

According to the screenshot below, we can see that the ACK numbers increase in the sequence of 679, 881 and so on.