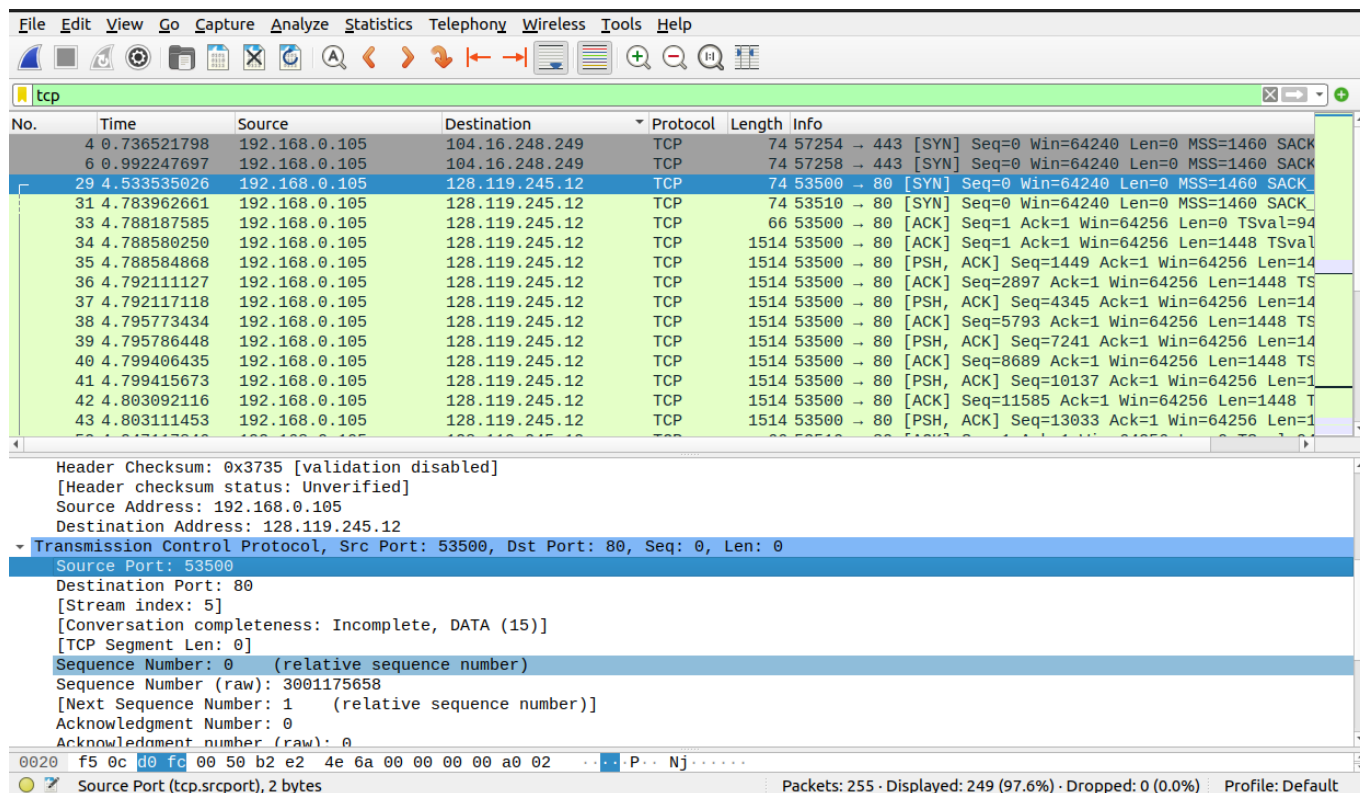


Практика 7. Транспортный уровень

1. Wireshark: TCP

Перехват TCP-передачи данных от вашего компьютера удаленному серверу.



1. Какой IP-адрес и номер порта TCP использует ваш компьютер (отправитель), передающий файл серверу gaia.cs.umass.edu?

Мой компьютер:

IP: 192.168.0.105

PORT: 53500

2. Каков IP-адрес у сервера gaia.cs.umass.edu? Каковы номера портов для отправки и приема TCP-сегментов этого соединения?

Сервер:

IP: 128.119.245.12

PORT: 80

3. Какой порядковый номер у SYN TCP-сегмента, который используется для установления TCP-соединения между компьютером клиента и сервером gaia.cs.umass.edu? Как определяется, что это именно SYN-сегмент?

Sequence Number: 0

Чтобы определить, что это именно SYN-сегмент, нужно обратить внимание на флаги в заголовке TCP.

4. Какой порядковый номер у SYN ACK-сегмента, отправленного сервером gaia.cs.umass.edu на компьютер клиента в ответ на SYN-сегмент? Какое значение хранится в поле подтверждения в SYNACK-сегменте? Как сервер gaia.cs.umass.edu определил это значение? Как определяется, что это именно SYNACK-сегмент?

Sequence Number: 0

Acknowledgment Number: 1

Значение подтверждения в SYN ACK-сегменте определяется путем увеличения порядкового номера из SYN-сегмента на единицу.

Опять же смотрим на флаги в заголовке TCP. В SYN ACK-сегменте устанавливаются два флага: SYN и ACK.

5. Какой порядковый номер у TCP-сегмента, содержащего команду POST протокола HTTP? (для нахождения команды POST вам потребуется проникнуть внутрь поля содержимого пакета в нижней части окна Wireshark, чтобы найти сегмент, в поле DATA которого хранится значение POST)

Wireshark - Packet 34 - wlp2s0

[Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 1448]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 3001175659
 [Next Sequence Number: 1449 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 2770151727
 1000 = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
 Window: 502
 [Calculated window size: 64256]
 [Window size scaling factor: 128]
 Checksum: 0x6c41 (unverified)
 0040 d5 2d 50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 --POST / wireshar
 0050 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65 k-labs/l ab3-1-re
 0060 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f 31 2e 31 ply.htm HTTP/1.1
 0070 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e .Host: gaia.cs.
 0080 75 6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d umass.ed u-User-
 0090 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5
 00a0 2e 30 28 58 31 31 3b 20 55 62 75 6e 74 75 3b .0 (X11; Ubuntu;
 00b0 20 4c 69 6e 75 78 20 78 38 36 5f 36 3a 3b 20 72 Linux x 86_64; r
 00c0 76 3a 31 30 39 2e 30 29 20 47 65 63 6b 6f 2f 32 v:109.0) Gecko/2
 00d0 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
 00e0 31 31 32 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 112.0.0 A ccept: t
 00f0 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 ext/html , applica
 0100 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 tion/xht ml+xml,a
 0110 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 pplicati on/xml;q
 0120 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c =0.9, ima ge/avif,

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1,448 bytes: Packets: 255 - Displayed: 249 (97.6%) - Dropped: 0 (0.0%) Profile: Default

Sequence Number: 1

6. Рассмотрите TCP-сегмент, содержащий команду POST протокола HTTP, как первый TCP сегмент соединения. Какие порядковые номера у первых шести сегментов TCP соединения (включая сегмент, содержащий команду POST протокола HTTP)? Когда был отправлен каждый сегмент? Когда был получен ACK-пакет для каждого сегмента? Покажите разницу между тем, когда каждый TCP-сегмент был отправлен и когда было получено каждое подтверждение, чему равно значение RTT для каждого из 6 сегментов?

No.	Time	Source	Destination	* Protocol	Length	Info
33	4.788187585	192.168.0.105	128.119.245.12	TCP	60	53590 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=94625022 TSecr=1992938797 [TCP segment of a reassembled PDU]
34	4.788187585	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=1448 TSval=94625022 TSecr=1992938797 [TCP segment of a reassembled PDU]
35	0.00004618	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [PSH, ACK] Seq=1449 Ack=1 Win=64256 Len=1448 TSval=94625022 TSecr=1992938797 [TCP segment of a reassembled PDU]
36	0.003538877	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [ACK] Seq=2897 Ack=1 Win=64256 Len=1448 TSval=94625026 TSecr=1992938797 [TCP segment of a reassembled PDU]
37	0.003538868	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [PSH, ACK] Seq=4345 Ack=1 Win=64256 Len=1448 TSval=94625026 TSecr=1992938797 [TCP segment of a reassembled PDU]
38	0.007193184	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [ACK] Seq=5793 Ack=1 Win=64256 Len=1448 TSval=94625029 TSecr=1992938797 [TCP segment of a reassembled PDU]
39	0.007269198	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [PSH, ACK] Seq=7241 Ack=1 Win=64256 Len=1448 TSval=94625029 TSecr=1992938797 [TCP segment of a reassembled PDU]
40	0.010826185	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [ACK] Seq=8889 Ack=1 Win=64256 Len=1448 TSval=94625033 TSecr=1992938797 [TCP segment of a reassembled PDU]
41	0.010835423	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [PSH, ACK] Seq=10137 Ack=1 Win=64256 Len=1448 TSval=94625033 TSecr=1992938797 [TCP segment of a reassembled PDU]
42	0.014511866	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [ACK] Seq=11585 Ack=1 Win=64256 Len=1448 TSval=94625036 TSecr=1992938797 [TCP segment of a reassembled PDU]
43	0.014531203	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [PSH, ACK] Seq=13033 Ack=1 Win=64256 Len=1448 TSval=94625036 TSecr=1992938797 [TCP segment of a reassembled PDU]
44	0.150477032	128.119.245.12	192.168.0.105	TCP	74	80 -> 53590 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 TSval=1992939048 TSecr=94625017 WS=128
45	0.150477983	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=1449 Win=31872 Len=0 TSval=1992939053 TSecr=94625022
46	0.150478023	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=2897 Win=34816 Len=0 TSval=1992939053 TSecr=94625022
47	0.150478063	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=4345 Win=37760 Len=0 TSval=1992939055 TSecr=94625026
48	0.150478103	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=5793 Win=40576 Len=0 TSval=1992939056 TSecr=94625026
49	0.150478153	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=7241 Win=43520 Len=0 TSval=1992939059 TSecr=94625029
50	0.150478193	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=8889 Win=46336 Len=0 TSval=1992939059 TSecr=94625029
51	0.150478233	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=10137 Win=49280 Len=0 TSval=1992939068 TSecr=94625033
52	0.150537596	192.168.0.105	128.119.245.12	TCP	66	53510 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=94625181 TSecr=1992939048
53	0.150571811	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [ACK] Seq=14481 Ack=1 Win=64256 Len=1448 TSval=94625181 TSecr=1992939053 [TCP segment of a reassembled PDU]
54	0.150572425	192.168.0.105	128.119.245.12	TCP	1514	53590 -> 80 [PSH, ACK] Seq=15929 Ack=1 Win=64256 Len=1448 TSval=94625181 TSecr=1992939053 [TCP segment of a reassembled PDU]
55	0.150825291	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=11585 Win=52224 Len=0 TSval=1992939063 TSecr=94625033
56	0.150825422	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=13033 Win=55040 Len=0 TSval=1992939068 TSecr=94625036
57	0.150825482	128.119.245.12	192.168.0.105	TCP	60	80 -> 53590 [ACK] Seq=1 Ack=14481 Win=57984 Len=0 TSval=1992939068 TSecr=94625036

Номер	-	Время отправления TCP пакета	-	Время получения ACK	-	разница
1	-	4.788580250	-	4.947057882	-	0.1584776323
1449	-	4.788584868	-	4.947058233	-	0.1584733649
2897	-	4.792111127	-	4.947058273	-	0.1549471459
4345	-	4.792117118	-	4.947058313	-	0.1549411950
5793	-	4.795773434	-	4.947058353	-	0.1512849190
7241	-	4.795786448	-	4.947058403	-	0.1512719549

7. Чему равна пропускная способность (количество байтов, передаваемых в единицу времени) для этого TCP-соединения? Объясните, как вы получили это значение.

Делим длину каждого пакета на его RTT и берём среднее. Получается **9553**