COMP2322 Computer Networking

Lab 6 Report: TCP

Author
Wang Yuqi
[redacted]

Lecturer
Dr. LOU Wei

BsC in Computer Science
Academic year: 2024/2025 Sem 2

Tracefiles

Answer: The trace file for this lab report is:

File Name	Questions
`lab6_tracefile.pcapng`	`2, 4, 8, 10, 12`

DISCLAIMER To protect my **personal privacy**, only a selected subset of the original trace file is included. This partial trace retains lab-relevant traffic while scrubbing other sensitive data.

Sensitive Info The full trace contained these info that I do not wish to disclose:

- Public IPs of my private GPU compute nodes
- Public IPs of my private VPN network
- TLS handshake and key exchange messages
- Network activity that reveals my software usage and browsing habits

Questions

Question 2

Q: What is the IP address of `gaia.cs.umass.edu`? On what port number is it sending and receiving TCP segments for this connection?

```
Frame 10: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on
interface en0, id 0
Ethernet II, Src: [redacted], Dst: 9e:05:d6:68:17:27
(9e:05:d6:68:17:27)
Internet Protocol Version 4, Src: 10.0.0.128, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49358, Dst Port: 80, Seq: 4947, Ack: 1,
Len: 1440
    Source Port: 49358
    Destination Port: 80
    [Stream index: 28]
    [Stream Packet Number: 8]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 1440]
    Sequence Number: 4947    (relative sequence number)
    Sequence Number (raw): 1902326224
    [Next Sequence Number: 6387    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 664180307
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x010 (ACK)
    Window: 2070
    [Calculated window size: 132480]
    [Window size scaling factor: 64]
    Checksum: 0x895a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (1440 bytes)
    [Reassembled PDU in frame: 3652]
    TCP segment data (1440 bytes)
```

Answer:

- IP Address: `128.119.245.12`
- Port Number: `80`

Question 4

Q 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? What is it in the segment that identifies the segment as a SYN segment?

```
Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface
en0, id 0
Ethernet II, Src: [redacted], Dst: 9e:05:d6:68:17:27
(9e:05:d6:68:17:27)
Internet Protocol Version 4, Src: 10.0.0.128, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49358, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 49358
    Destination Port: 80
    [Stream index: 28]
    [Stream Packet Number: 1]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1902321277
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1011 .... = Header Length: 44 bytes (11)
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xf893 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale,
No-Operation (NOP), No-Operation (NOP), Timestamps, SACK permitted, End of
Option List (EOL), End of Option List (EOL)
    [Timestamps]
```

Answer:

- The (relative) sequence number: `0`
- The (raw) sequence number: `1902321277`
- The SYN flag (0x002) identifies the segment as a SYN segment.

Question 8

Q: What is the length of each of the first six TCP segments?

```
No.     Time        Source      Destination     Prot  Length    Info
2   3.319912    10.0.0.128  128.119.245.12  TCP   78
49358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2691615990 TSecr=0
SACK_PERM

3   3.378557    10.0.0.128  128.119.245.12  TCP   78
49359 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4270574587 TSecr=0
SACK_PERM

4   3.546212    128.119.245.12  10.0.0.128  TCP   74
80 → 49358 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM
TSval=541127697 TSecr=2691615990 WS=128

5   3.546499    10.0.0.128  128.119.245.12  TCP   66
49358 → 80 [ACK] Seq=1 Ack=1 Win=132480 Len=0 TSval=2691616216 TSecr=541127697

6   3.546947    10.0.0.128  128.119.245.12  TCP   692
49358 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132480 Len=626 TSval=2691616217
TSecr=541127697 [TCP PDU reassembled in 3652]

7   3.547069    10.0.0.128  128.119.245.12  TCP   1506
49358 → 80 [ACK] Seq=627 Ack=1 Win=132480 Len=1440 TSval=2691616217
TSecr=541127697 [TCP PDU reassembled in 3652]
```

Answer:

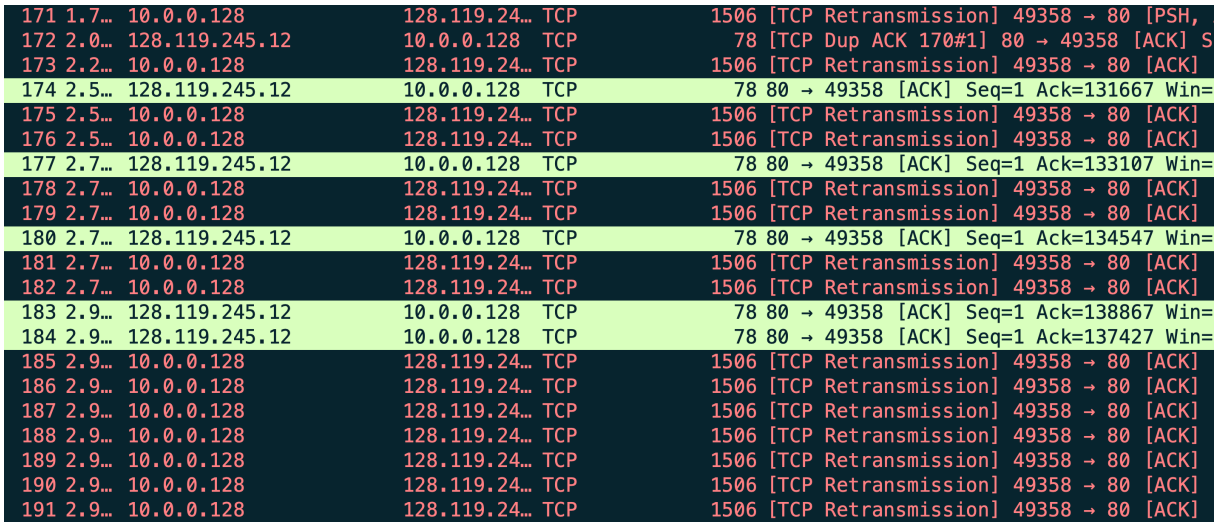
The length of the first six TCP segments (not packet) are:

1. `0 bytes` (total size = `78 bytes`)
2. `0 bytes` (total size = `78 bytes`)
3. `0 bytes` (total size = `74 bytes`)
4. `0 bytes` (total size = `66 bytes`)
5. `626 bytes` (total size = `692 bytes`)
6. `1440 bytes` (total size = `1506 bytes`)

Note: The packet number start from 2 instead of 1, because the first packet captured is a [RST, ACK]. Please refer to `lab6_tracefile.pcapng` for details.

Question 10

Q: Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?



171 1.7…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [PSH,
172 2.0…	128.119.245.12	10.0.0.128	TCP	78 [TCP Dup ACK 170#1] 80 → 49358 [ACK] S
173 2.2…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
174 2.5…	128.119.245.12	10.0.0.128	TCP	78 80 → 49358 [ACK] Seq=1 Ack=131667 Win=
175 2.5…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
176 2.5…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
177 2.7…	128.119.245.12	10.0.0.128	TCP	78 80 → 49358 [ACK] Seq=1 Ack=133107 Win=
178 2.7…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
179 2.7…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
180 2.7…	128.119.245.12	10.0.0.128	TCP	78 80 → 49358 [ACK] Seq=1 Ack=134547 Win=
181 2.7…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
182 2.7…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
183 2.9…	128.119.245.12	10.0.0.128	TCP	78 80 → 49358 [ACK] Seq=1 Ack=138867 Win=
184 2.9…	128.119.245.12	10.0.0.128	TCP	78 80 → 49358 [ACK] Seq=1 Ack=137427 Win=
185 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
186 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
187 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
188 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
189 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
190 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]
191 2.9…	10.0.0.128	128.119.24…	TCP	1506 [TCP Retransmission] 49358 → 80 [ACK]

Figure 1: Examples of retransmitted segments in the Wireshark tracefile

Answer:

- Yes, there are retransmitted segments in the trace file.
- I checked for segments with:
  - "`[TCP Retransmission]`" text in the Info column of the tracefile.
  - rows with `black shading` in the Wireshark GUI (see Figure 1).
  - `Seq` value much smaller than prior segments' `Seq` or `Ack` numbers.

Question 12

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

The throughput of the TCP connection can be calculated as:

$$\text{Throughput} = \frac{\text{Total Bytes Transferred}}{\text{Total Time Elapsed}}$$

- For *Total Bytes Transferred*: we need to determine the `Seq` number of the first and last non-`SYN` segments. The difference between these two numbers gives us the total number of bytes transferred.
- For *Total Time Elapsed*: we need to determine the time of the first and last non-`SYN` segment and the time of the last segment. The difference between these two times gives us the total time elapsed.

The First vs. Last Non-SYN Segment:

```
No.     Time        Source      Destination     Prot  Length    Info
5       0.673847    10.0.0.128  128.119.245.12  TCP   66        49358 → 80 [ACK]
Seq=1 Ack=1 Win=132480 Len=0 TSval=2691616216 TSecr=541127697

...

382   4.018635  128.119.245.12  10.0.0.128  TCP 66  80 → 49359 [ACK] Seq=1
Ack=152948 Win=232320 Len=0 TSval=541131036 TSecr=4270577865
```

Therefore,

- The first non-SYN segment is `No. 5` with `Seq=1` and `Time=0.673847`
- The last non-SYN segment is `No. 382` with `Ack=152948` and `Time=4.018635`

$$\begin{aligned}\text{Throughput} &= \frac{\text{Total Bytes Transferred}}{\text{Total Time Elapsed}} \\ &= \frac{152948 - 1}{4.018635 - 0.673847} \\ &\approx 45726.96 \text{ B/s} \\ &\approx 45.73 \text{ KB/s}\end{aligned}$$

Answer:

- The throughput of the TCP connection is approximately `45.73 KB/s`.
- I calculated this value by determining the total bytes transferred and the total time elapsed, as described above.