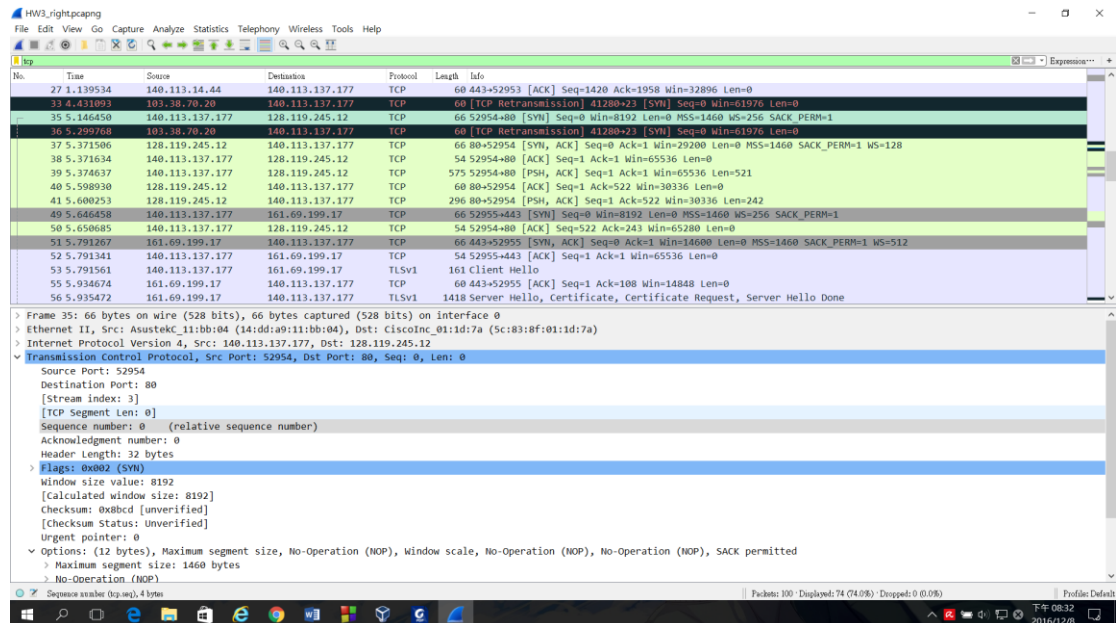


1. IP address : 140.113.137.177

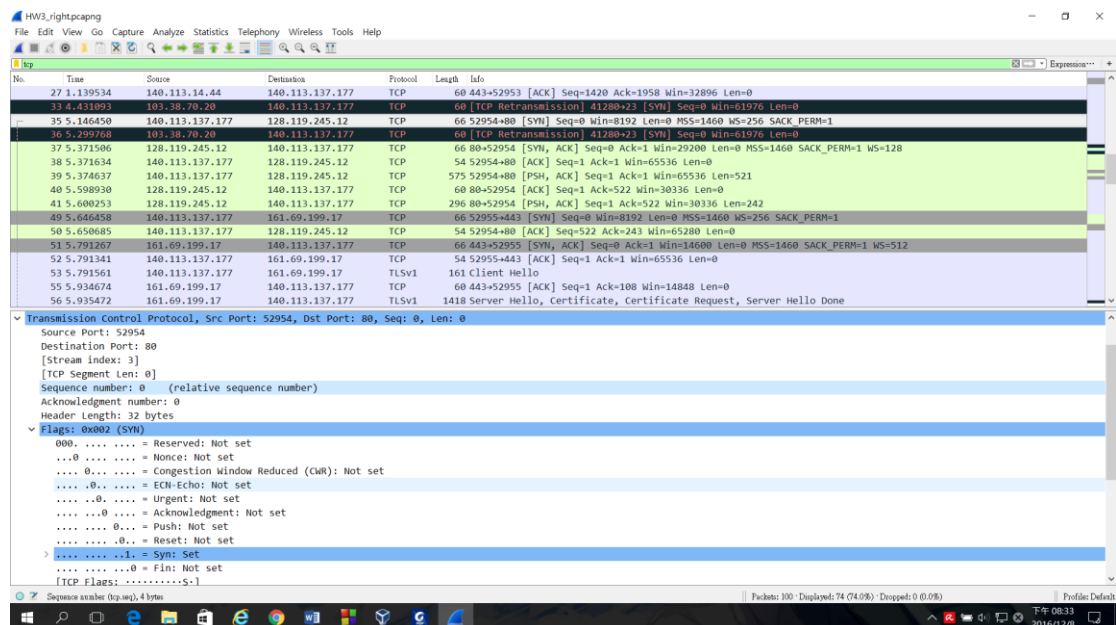
IP port : 52954

2. IP address : 128.119.245.12

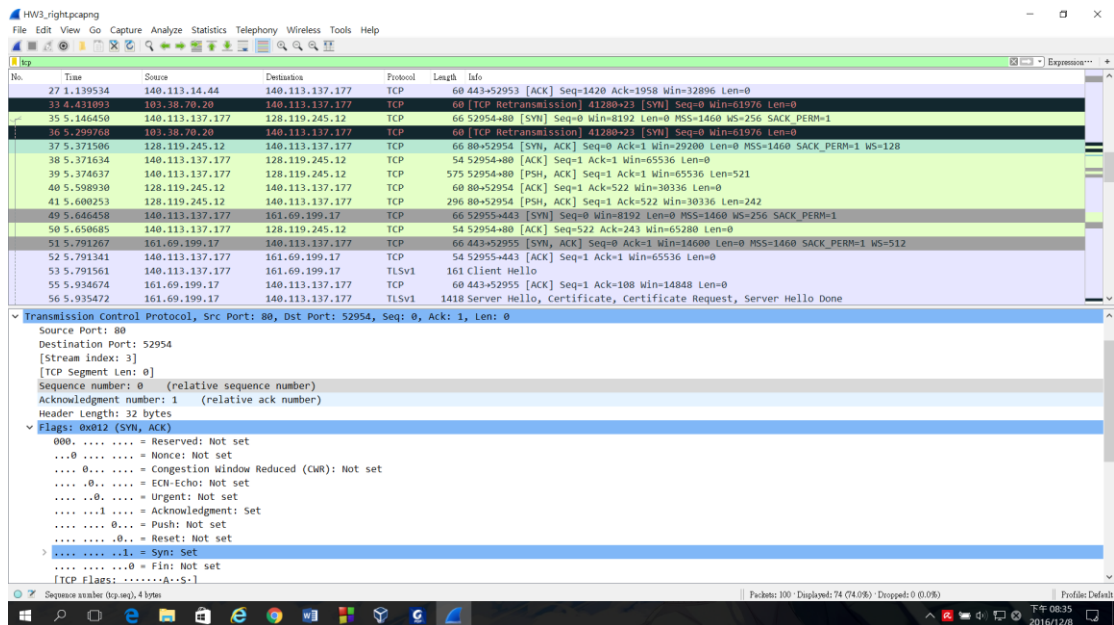
IP port : 80



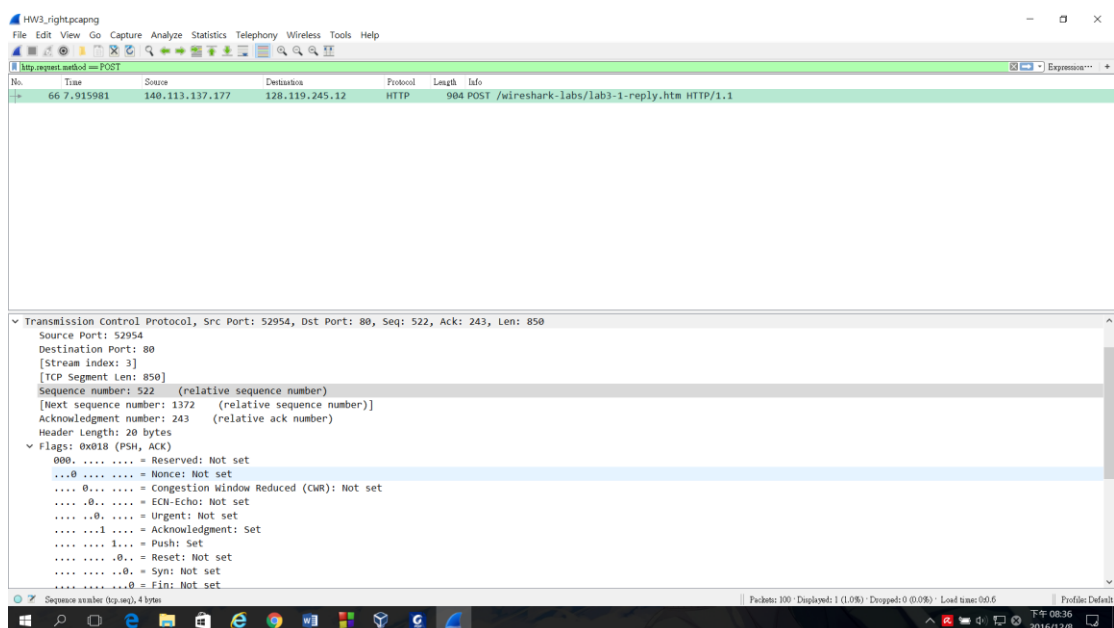
3. 0 , the Syn flag is set to 1 and this identifies the segment as a Syn segment.



4. 1, the Syn flag and the Acknowledgment flag are both set to 1 and this identifies the segment as a Syn-Ack segment.



5. 522



6. 1460 bytes

The screenshot shows a Wireshark packet capture of a network traffic. The packet list on the left shows a SYN packet (No. 35) from 140.113.137.177 to 140.113.137.177, protocol TCP, length 60 bytes. The packet details pane on the right shows the following information:

- Destination Port: 80
- [Stream index: 3]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 0
- Header Length: 32 bytes
- Flags: 0x002 (SYN)
- Window size value: 8192
- [calculated window size: 8192]
- Checksum: 0x8bdc [unverified]
- [checksum status: unverified]
- Urgent pointer: 0
- Options: (12 bytes), Maximum segment size, No-operation (NOP), Window scale, No-operation (NOP), No-operation (NOP), SACK permitted
 - > Maximum segment size: 1460 bytes
 - > No-operation (NOP)
 - > Window scale: 8 (multiply by 256)
 - > No-operation (NOP)
 - > No-operation (NOP)
 - > TCP SACK Permitted option: True

The packet bytes pane at the bottom shows the raw data of the packet.

7. 29200 bytes

The screenshot shows a Wireshark packet capture of a network traffic. The packet list on the left shows a SYN packet (No. 35) from 140.113.137.177 to 140.113.137.177, protocol TCP, length 60 bytes. The packet details pane on the right shows the following information:

- Source Port: 80
- Destination Port: 52954
- [Stream index: 3]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- Acknowledgment number: 1 (relative ack number)
- Header Length: 32 bytes
- Flags: 0x002 (SYN, ACK)
- Window size value: 29200
- [calculated window size: 29200]
- Checksum: 0x11b2 [unverified]
- [checksum status: unverified]
- Urgent pointer: 0
- Options: (12 bytes), Maximum segment size, No-operation (NOP), No-operation (NOP), SACK permitted, No-operation (NOP), Window scale
 - > Maximum segment size: 1460 bytes
 - > No-operation (NOP)
 - > No-operation (NOP)
 - > TCP SACK Permitted option: True
 - > No-operation (NOP)

The packet bytes pane at the bottom shows the raw data of the packet.

8. Total amount data transmitted :

the acknowledgment number of the last segment – the sequence number of the first segment = 1021 – 1 = 1020 bytes

Total transmission time :

$$8.191373 - 5.374637 = 2.816736$$

$$1020 / 2.816736 = 362.121264 \text{ bytes/sec}$$

The top screenshot shows a list of packets in Wireshark. The detailed view pane displays the following information for a selected packet:

- Transmission Control Protocol, Src Port: 52954, Dst Port: 80, Seq: 1, Ack: 1, Len: 521
- Source Port: 52954
- Destination Port: 80
- [Stream index: 3]
- [TCP Segment Len: 521]
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 522 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Header Length: 20 bytes
- Flags: 0x018 (PSH, ACK)
- Window size value: 256
- [calculated window size: 65536]
- [Window size scaling factor: 256]
- Checksum: 0x8dca [unverified]
- [checksum status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [RTT: 0.225184000 seconds]
- [Bytes in flight: 521]
- [Bytes sent since last PSH flag: 521]

The bottom screenshot shows a list of packets in Wireshark. The detailed view pane displays the following information for a selected packet:

- Transmission Control Protocol, Src Port: 52954, Dst Port: 80, Seq: 1372, Ack: 1021, Len: 0
- Source Port: 52954
- Destination Port: 80
- [Stream index: 3]
- [TCP Segment Len: 0]
- Sequence number: 1372 (relative sequence number)
- Acknowledgment number: 1021 (relative ack number)
- Header Length: 20 bytes
- Flags: 0x010 (ACK)
- Window size value: 252
- [calculated window size: 64512]
- [Window size scaling factor: 256]
- Checksum: 0x8bc1 [unverified]
- [checksum status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [This is an ACK to the segment in frame: 68]
- [The RTT to ACK the segment was: 0.050414000 seconds]
- [RTT: 0.225184000 seconds]

加分題：1.因為 data 大於 MMS 的大小，故 TCP 要分段送出去

2. the host uses two tuple (destination id and destination port) and sequence number to identify the TCP segments which belong to same application message.

心得：這次的實驗主要是在了解 TCP 的運作方式，透過這次的實驗我對上課所教的東西更有實感，不會只有抽象的觀念而已，有種我在運用上課所學的感覺。網路這種東西比想像中還要複雜，簡單的上傳資料就需要透過多次的來回聯絡，之前可能只是覺得：喔這樣啊。做完這次作業，對於這種東西的複雜度更加了解，也對於創立 protocol 的人更感佩服了。