BÀI TẬP THỰC HÀNH 1

BÀI TẬP THỰC HÀNH 1

Họ và tên: Nguyễn Đình Mạnh

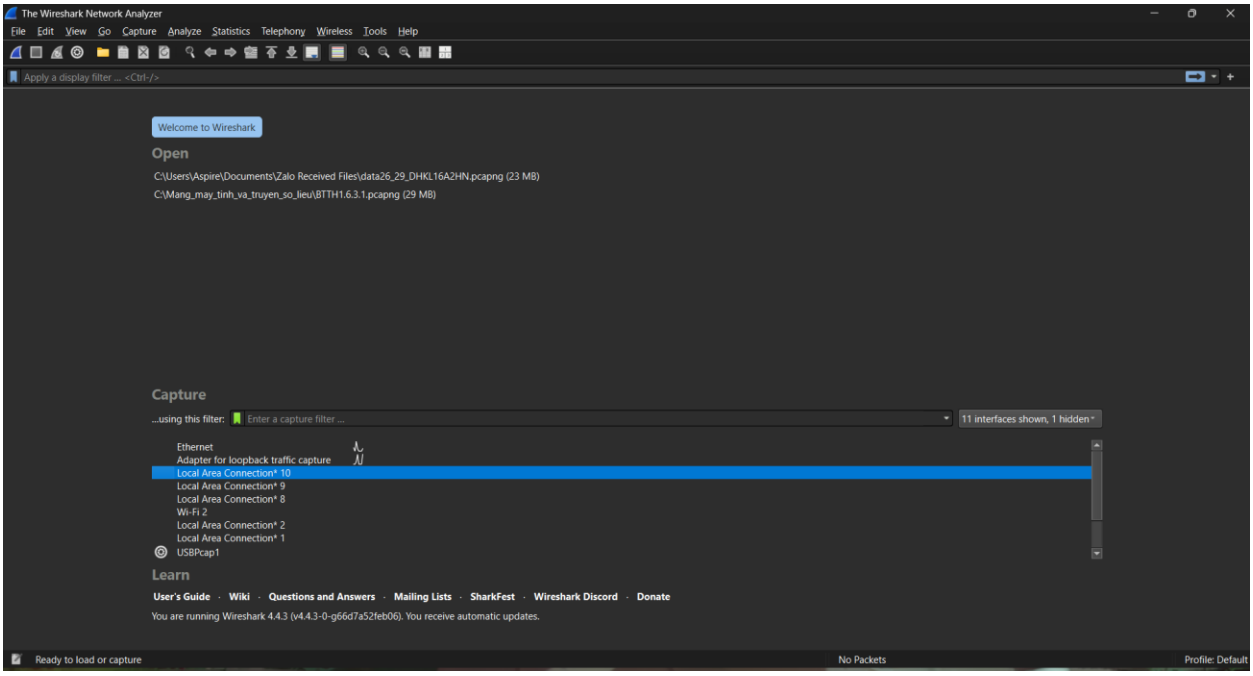
Mã sinh viên: 22174600037

Lớp:DHKL16A2HN

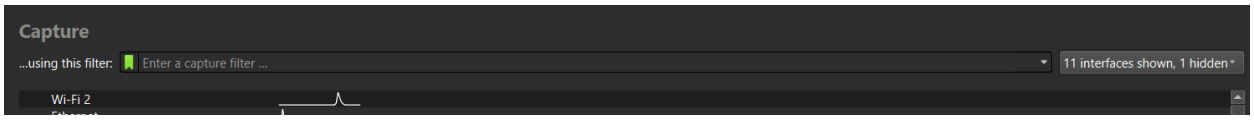
THỰC HÀNH: Hướng dẫn bắt quá trình bắt tay 3 bước TCP bằng Wireshark. Mục tiêu của bài thực hành này là bắt và phân tích quá trình bắt tay 3 bước TCP bằng Wireshark, giúp thấy trực tiếp các gói SYN, SYN-ACK, ACK.

Bước 1: Mở Wireshark và bắt đầu thu thập gói tin

1. Mở Wireshark



2. Chọn card mạng đang sử dụng kết nối Internet (Wi-Fi hoặc Ethernet).

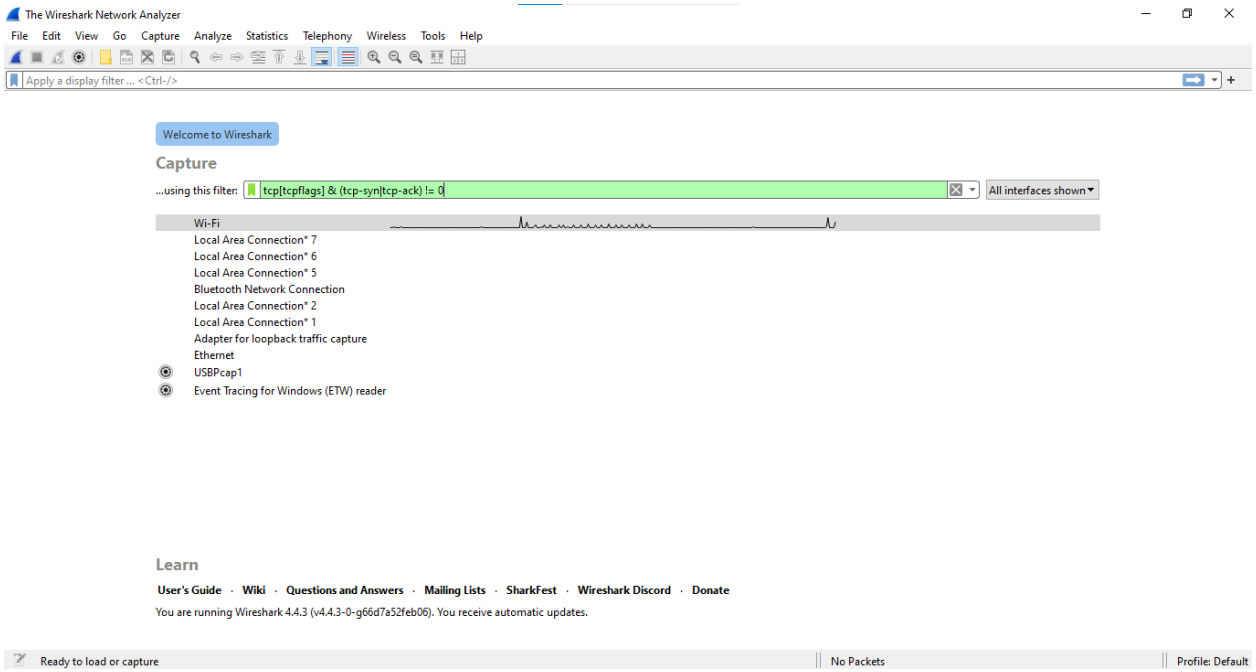


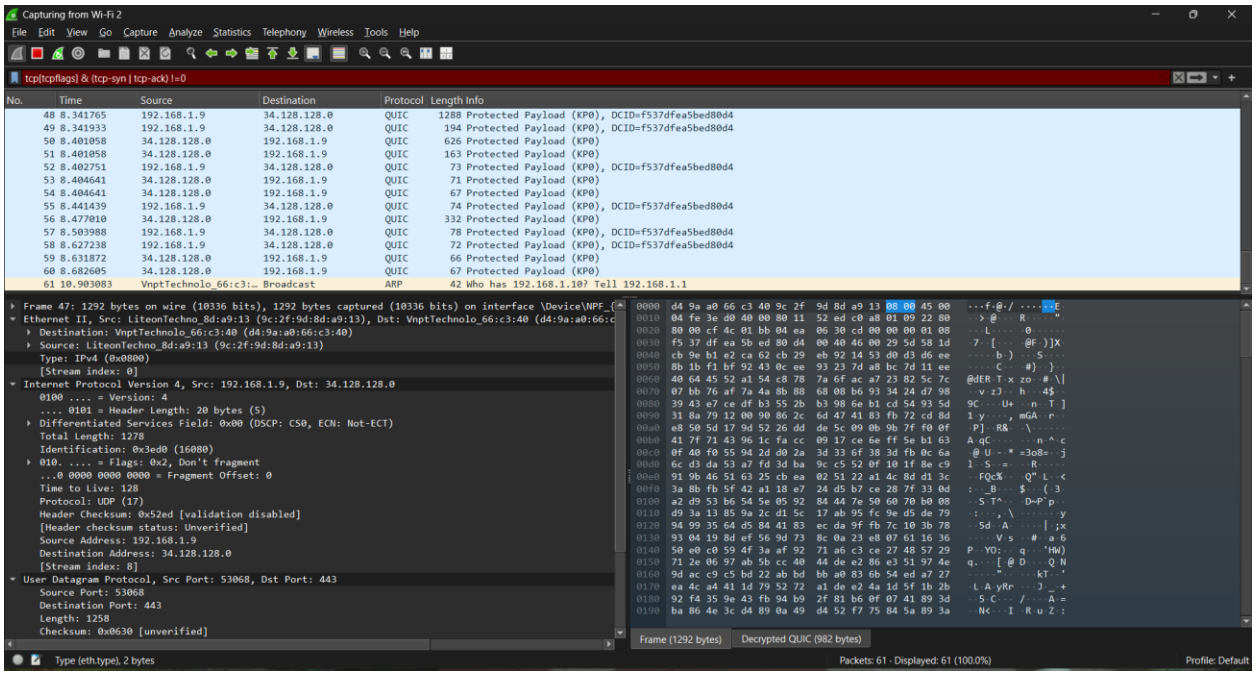
&

3. Nhập bộ lọc để chỉ hiển thị gói tin TCP liên quan đến quá trình bắt tay:

3.1. Nếu muốn lọc gói SYN hoặc ACK trong Capture Filter (ô nhập đ/k lọc), dùng cú pháp sau:

```
tcp[tcpflags] & (tcp-syn|tcp-ack) != 0
```

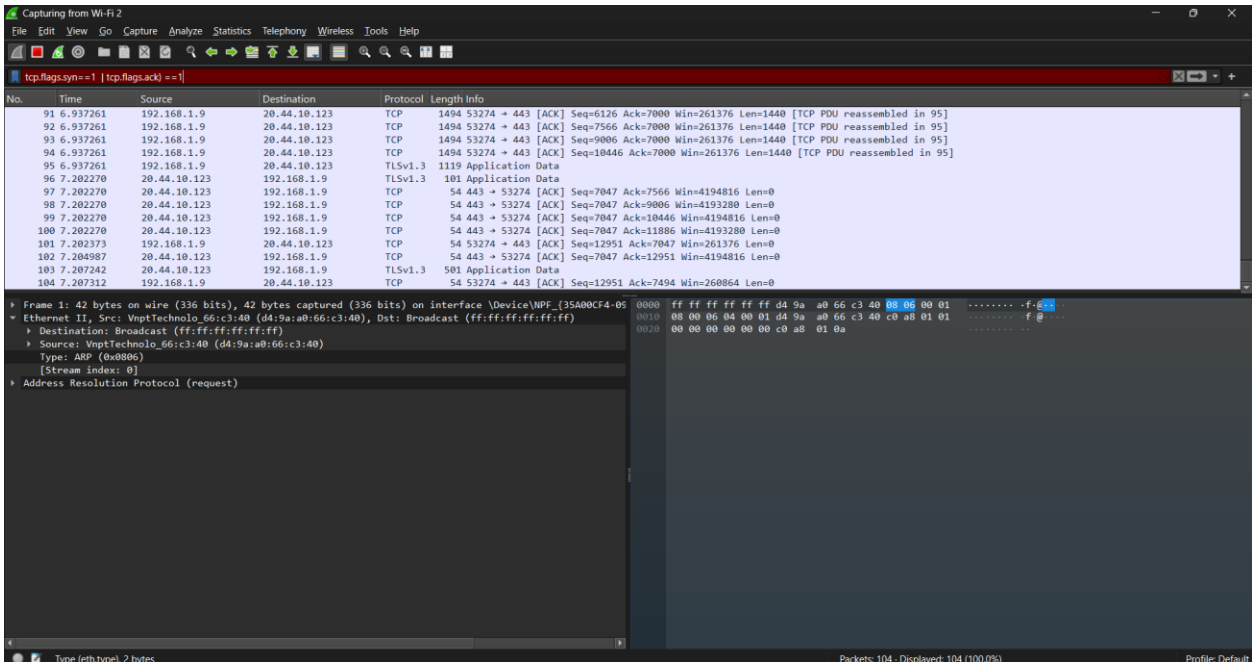




3.2. Nếu muốn lọc sau khi đã bắt gói tin (Display Filter), dùng cú pháp:

```
tcp.flags.syn == 1 || tcp.flags.ack == 1
```

Lưu ý: Display Filter chỉ hoạt động sau khi đã bắt gói tin xong

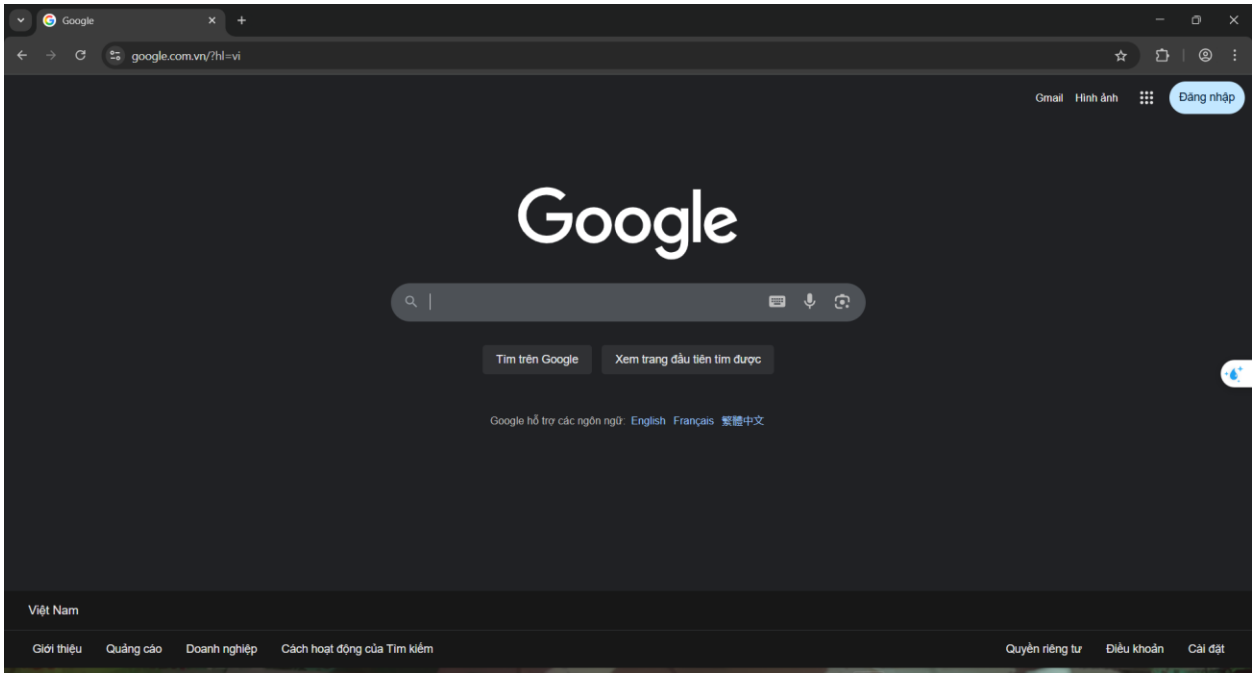


Bước 2: Khởi tạo kết nối TCP

Cách 1: Truy cập một trang web bằng trình duyệt

• Mở trình duyệt và nhập một URL (ví dụ: http://www.example.com).

• Khi nhấn Enter, trình duyệt sẽ thực hiện kết nối TCP đến máy chủ web.



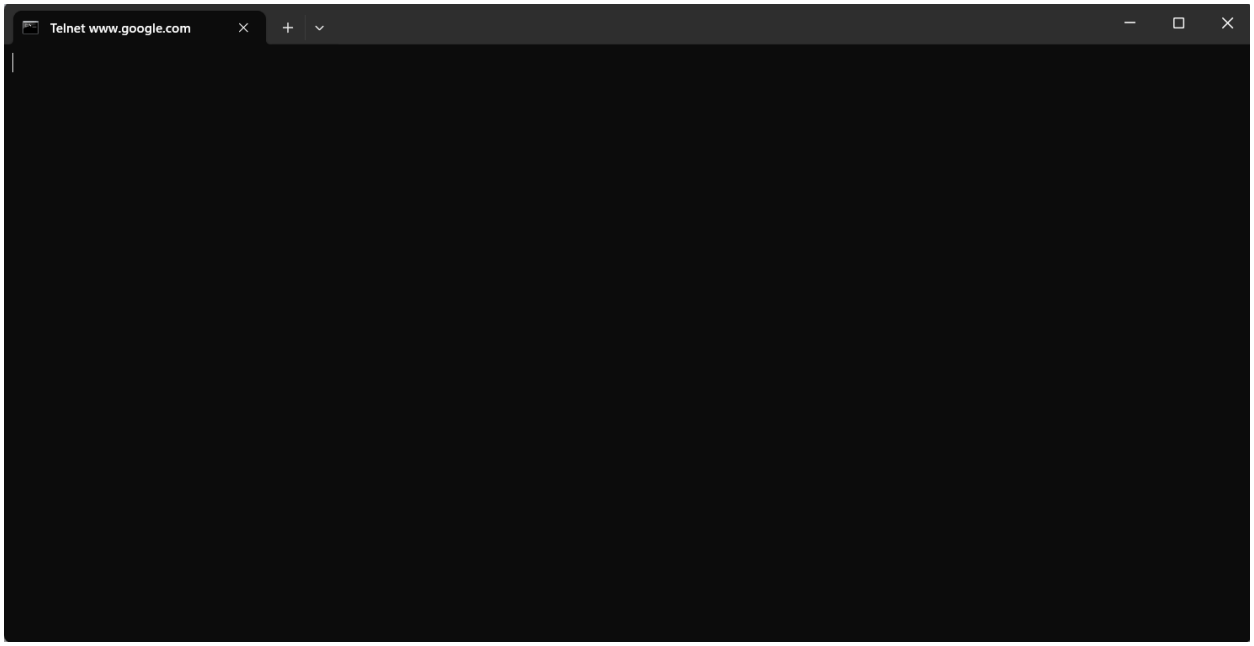
Cách 2: Sử dụng telnet để kết nối đến một máy chủ

Mở Command Prompt (Windows) hoặc Terminal (Linux/macOS)

Nhập lệnh sau để mở kết nối TCP đến cổng 80 (HTTP) của Google

```
telnet www.google.com 80
```

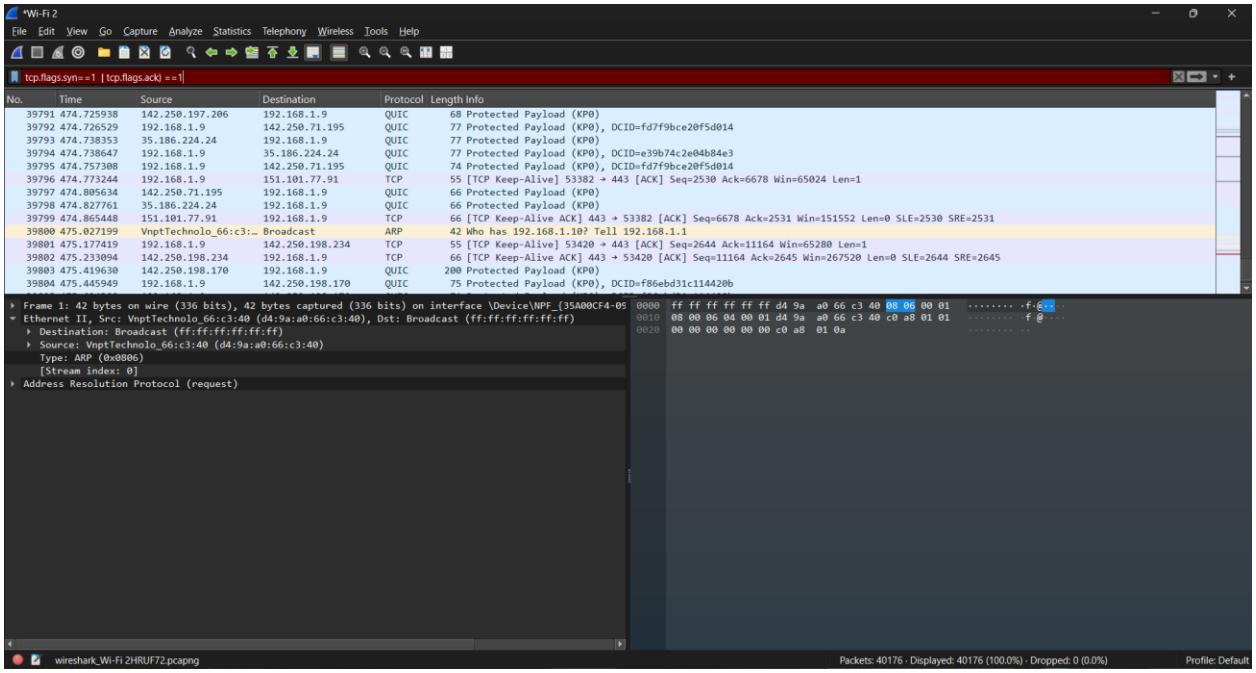
Nếu telnet hiển thị Connected to www.google.com, nghĩa là kết nối TCP đã được thiết lập.



Bước 3: Phân tích gói tin trong Wireshark

Sau khi thực hiện một trong các bước trên, quay lại Wireshark và dừng thu thập gói tin.

nhấn Stop Capture (nút vuông đỏ) sau khi lệnh Telnet thực hiện xong.

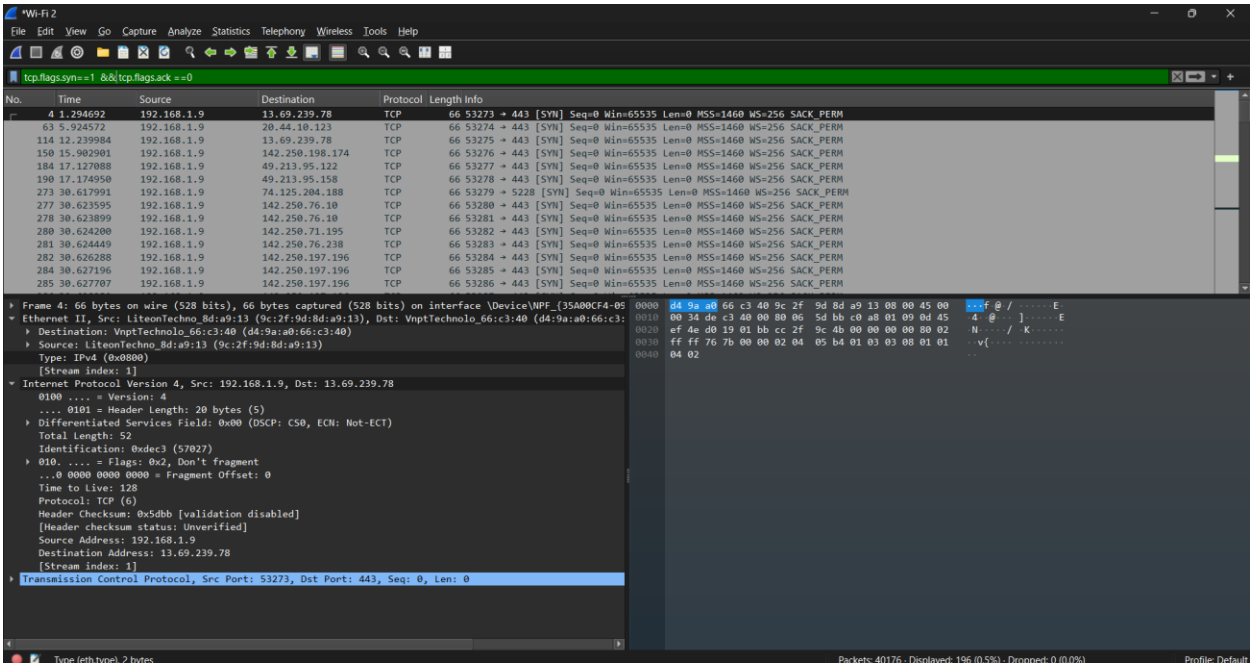


Chúng ta sẽ thấy một loạt gói TCP.

Trong ô Display Filter, nhập bộ lọc sau để chỉ hiển thị gói SYN:

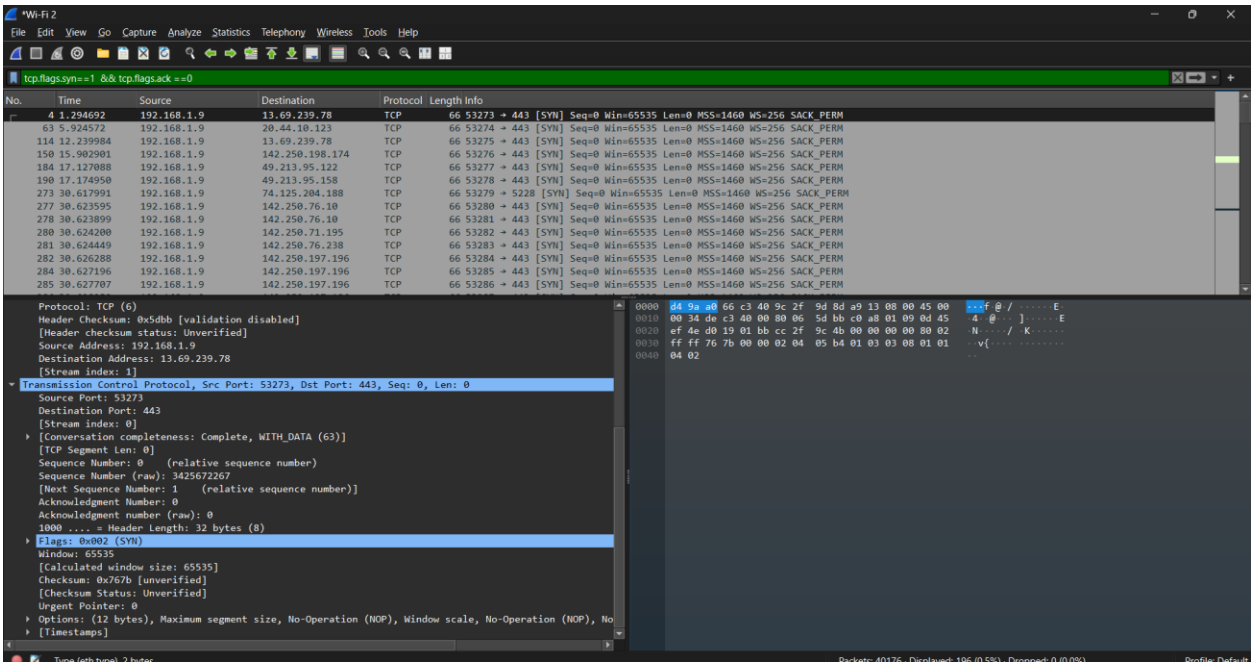
```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

Nhấn Enter sẽ thấy gói SYN đầu tiên được gửi từ máy của mình đến www.google.com



Bước 4: Phân tích gói SYN

Nhấp vào gói SYN để xem chi tiết. Trong phần Transmission Control Protocol (TCP), kiểm tra các thông tin:



Xác nhận đây là gói SYN khởi tạo kết nối TCP.

Bước 5: Tìm gói SYN-ACK và ACK để quan sát toàn bộ bắt tay 3 bước

❑ Tìm gói SYN-ACK từ Google:

Nhập bộ lọc:

tcp.flags.syn == 1 && tcp.flags.ack == 1

Kiểm tra:

- Flags: SYN = 1, ACK = 1
- Acknowledgment Number: x + 1 (phản hồi từ Google).

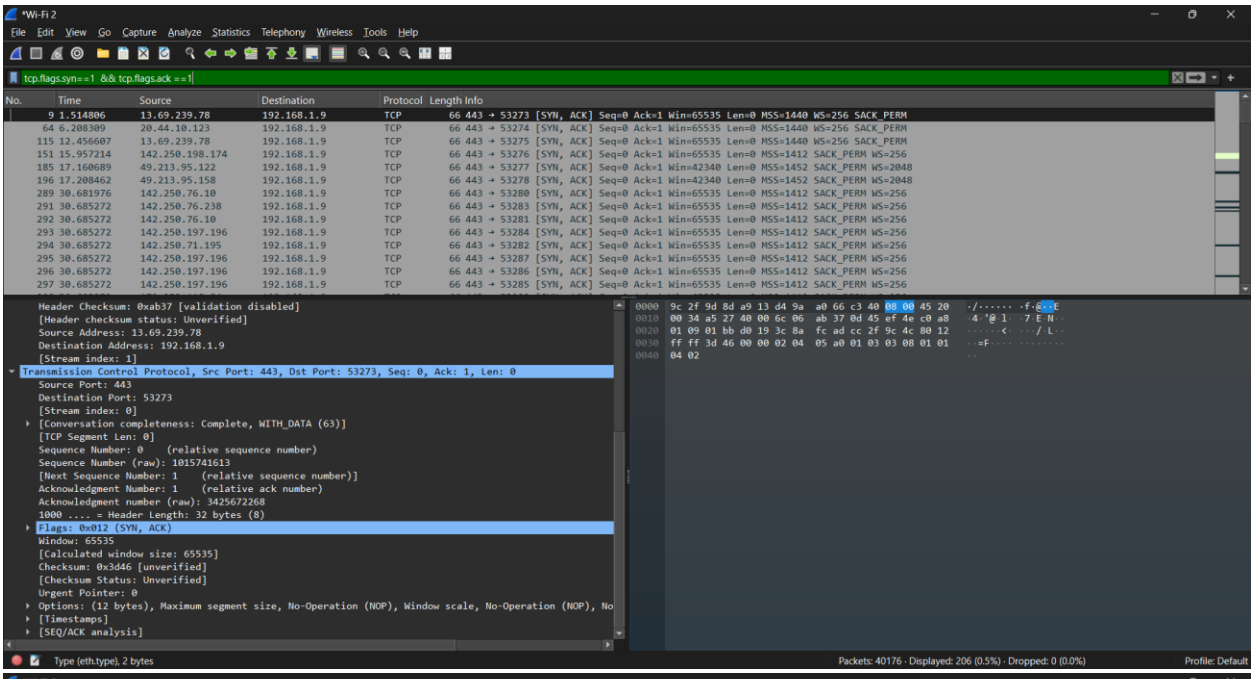
Tìm gói ACK từ máy người dùng:

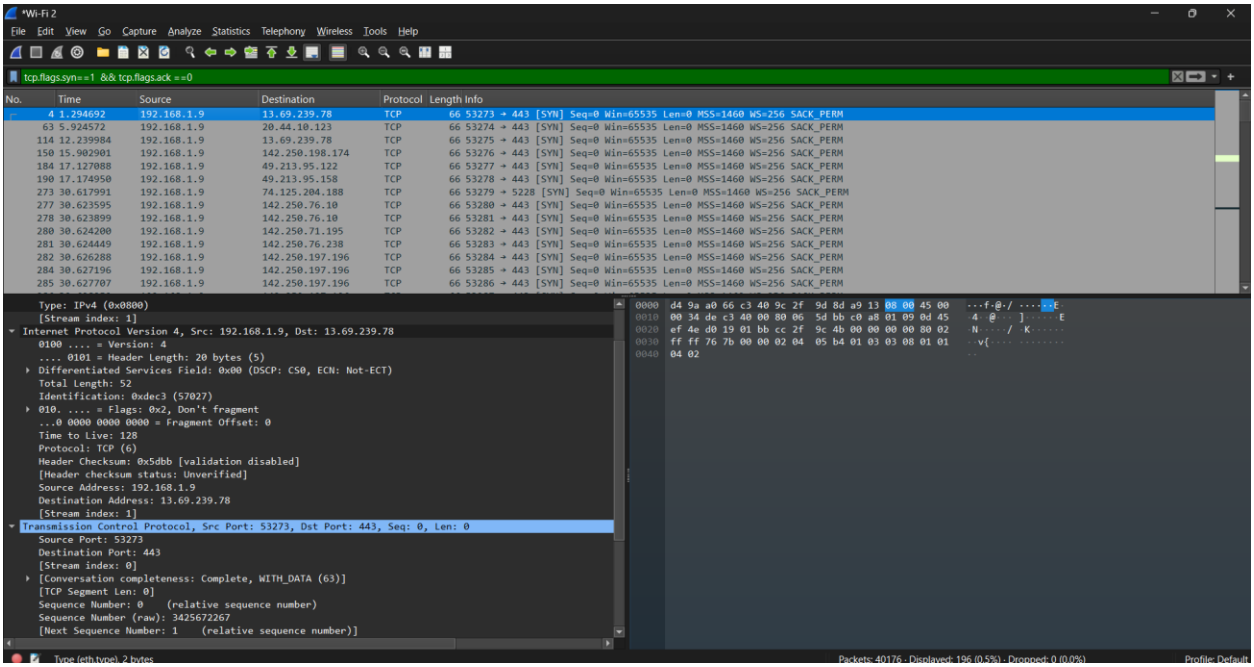
```
tcp.flags.ack == 1 && tcp.flags.syn == 0
```

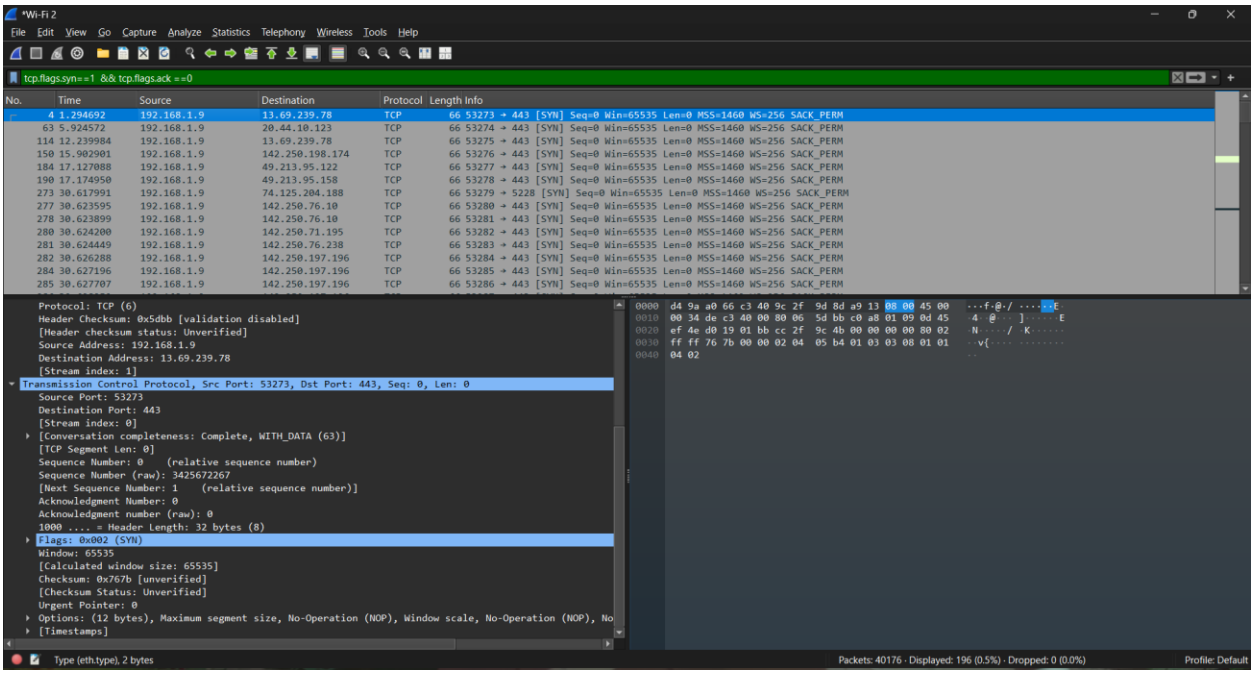
Kiểm tra

Flags: ACK = 1

Acknowledgment Number: y + 1 (phản hồi từ máy người dùng).


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1 && tcp.flags.ack ==1
No. Time Source Destination Protocol Length Info
9 1.514806 13.69.239.78 192.168.1.9 TCP 66 443 → 53273 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
64 6.208309 20.44.10.123 192.168.1.9 TCP 66 443 → 53274 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
115 12.456607 13.69.239.78 192.168.1.9 TCP 66 443 → 53275 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
151 15.957214 142.250.198.174 192.168.1.9 TCP 66 443 → 53276 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
185 17.160689 49.213.95.122 192.168.1.9 TCP 66 443 → 53277 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1452 SACK_PERM WS=2048
196 17.208462 49.213.95.158 192.168.1.9 TCP 66 443 → 53278 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1452 SACK_PERM WS=2048
289 30.681976 142.250.76.10 192.168.1.9 TCP 66 443 → 53280 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
291 30.685272 142.250.76.238 192.168.1.9 TCP 66 443 → 53283 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
292 30.685272 142.250.76.10 192.168.1.9 TCP 66 443 → 53281 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
293 30.685272 142.250.197.196 192.168.1.9 TCP 66 443 → 53284 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
294 30.685272 142.250.71.195 192.168.1.9 TCP 66 443 → 53282 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
295 30.685272 142.250.197.196 192.168.1.9 TCP 66 443 → 53287 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
296 30.685272 142.250.197.196 192.168.1.9 TCP 66 443 → 53286 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
297 30.685272 142.250.197.196 192.168.1.9 TCP 66 443 → 53285 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
Header Checksum: 0xab37 [validation disabled]
[Header checksum status: Unverified]
Source Address: 13.69.239.78
Destination Address: 192.168.1.9
[Stream index: 1]
Transmission Control Protocol, Src Port: 443, Dst Port: 53273, Seq: 0, Ack: 1, Len: 0
Source Port: 443
Destination Port: 53273
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1015741613
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3425672268
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
Window: 65535
[Calculated window size: 65535]
Checksum: 0x3d46 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No
[Timestamps]
[SEQ/ACK analysis]
0000 9c 2f 9d 8d a9 13 d4 9a a0 66 c3 40 08 00 45 20
0010 00 34 a5 27 40 00 6c 06 ab 37 0d 45 ef 4e c0 a8
0020 01 09 01 bb d0 19 3c 8a fc ad cc 2f 9c 4c 80 12
0030 ff ff 3d 46 00 00 02 04 05 a0 01 03 03 08 01 01
0040 04 02
Type (eth.type), 2 bytes
Packets: 40176 · Displayed: 206 (0.5%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1 && tcp.flags.ack ==0
No. Time Source Destination Protocol Length Info
4 1.294692 192.168.1.9 13.69.239.78 TCP 66 53273 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
63 5.924572 192.168.1.9 20.44.10.123 TCP 66 53274 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
114 12.239984 192.168.1.9 13.69.239.78 TCP 66 53275 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
150 15.902901 192.168.1.9 142.250.198.174 TCP 66 53276 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
184 17.127088 192.168.1.9 49.213.95.122 TCP 66 53277 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
190 17.174950 192.168.1.9 49.213.95.158 TCP 66 53278 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
273 30.617991 192.168.1.9 74.125.204.188 TCP 66 53279 → 5228 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
277 30.623595 192.168.1.9 142.250.76.10 TCP 66 53280 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
278 30.623899 192.168.1.9 142.250.76.10 TCP 66 53281 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
280 30.624200 192.168.1.9 142.250.71.195 TCP 66 53282 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
281 30.624449 192.168.1.9 142.250.76.238 TCP 66 53283 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
282 30.626288 192.168.1.9 142.250.197.196 TCP 66 53284 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
284 30.627196 192.168.1.9 142.250.197.196 TCP 66 53285 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
285 30.627707 192.168.1.9 142.250.197.196 TCP 66 53286 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Type: IPv4 (0x0800)
[Stream index: 1]
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 13.69.239.78
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xdec3 (57027)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x5dbb [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.9
Destination Address: 13.69.239.78
[Stream index: 1]
Transmission Control Protocol, Src Port: 53273, Dst Port: 443, Seq: 0, Len: 0
Source Port: 53273
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3425672267
[Next Sequence Number: 1 (relative sequence number)]
0000 d4 9a a0 66 c3 40 9c 2f 9d 8d a9 13 08 00 45 00
0010 00 34 de c3 40 00 80 06 5d bb c0 a8 01 09 0d 45
0020 ef 4e d0 19 01 bb cc 2f 9c 4b 00 00 00 00 80 02
0030 ff ff 76 7b 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Type (eth.type), 2 bytes
Packets: 40176 · Displayed: 196 (0.5%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1 && tcp.flags.ack ==0
No. Time Source Destination Protocol Length Info
4 1.294692 192.168.1.9 13.69.239.78 TCP 66 53273 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
63 5.924572 192.168.1.9 20.44.10.123 TCP 66 53274 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
114 12.239984 192.168.1.9 13.69.239.78 TCP 66 53275 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
150 15.902901 192.168.1.9 142.250.198.174 TCP 66 53276 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
184 17.127088 192.168.1.9 49.213.95.122 TCP 66 53277 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
190 17.174950 192.168.1.9 49.213.95.158 TCP 66 53278 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
273 30.617991 192.168.1.9 74.125.204.188 TCP 66 53279 → 5228 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
277 30.623595 192.168.1.9 142.250.76.10 TCP 66 53280 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
278 30.623899 192.168.1.9 142.250.76.10 TCP 66 53281 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
280 30.624200 192.168.1.9 142.250.71.195 TCP 66 53282 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
281 30.624449 192.168.1.9 142.250.76.238 TCP 66 53283 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
282 30.626288 192.168.1.9 142.250.197.196 TCP 66 53284 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
284 30.627196 192.168.1.9 142.250.197.196 TCP 66 53285 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
285 30.627707 192.168.1.9 142.250.197.196 TCP 66 53286 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Protocol: TCP (6)
Header Checksum: 0x5dbb [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.9
Destination Address: 13.69.239.78
[Stream index: 1]
Transmission Control Protocol, Src Port: 53273, Dst Port: 443, Seq: 0, Len: 0
Source Port: 53273
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3425672267
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 65535
[Calculated window size: 65535]
Checksum: 0x767b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No
[Timestamps]
0000 d4 9a a0 66 c3 40 9c 2f 9d 8d a9 13 08 00 45 00
0010 00 34 de c3 40 00 80 06 5d bb c0 a8 01 09 0d 45
0020 ef 4e d0 19 01 bb cc 2f 9c 4b 00 00 00 00 80 02
0030 ff ff 76 7b 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Type (eth.type), 2 bytes
Packets: 40176 · Displayed: 196 (0.5%) · Dropped: 0 (0.0%)
Profile: Default