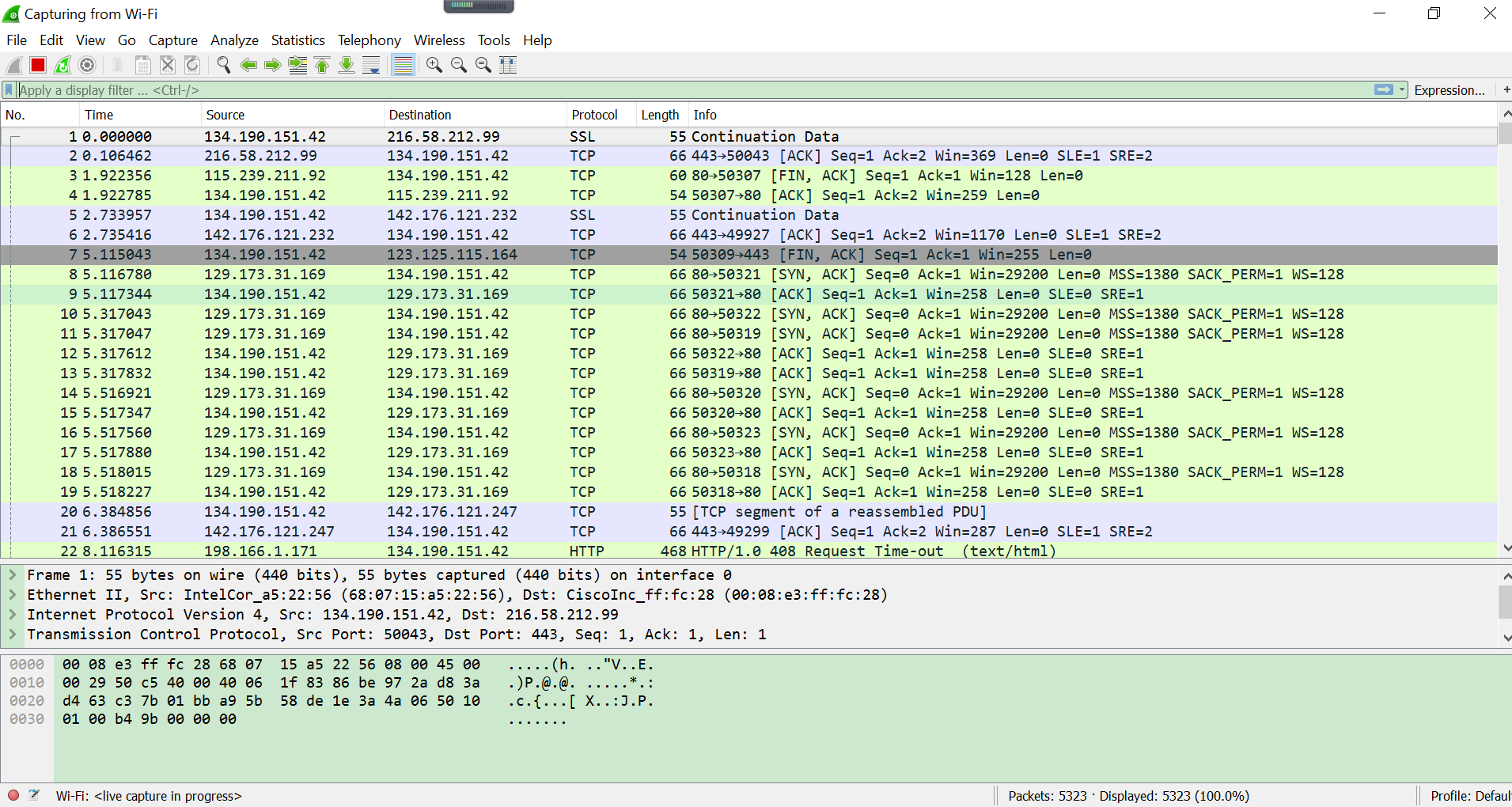
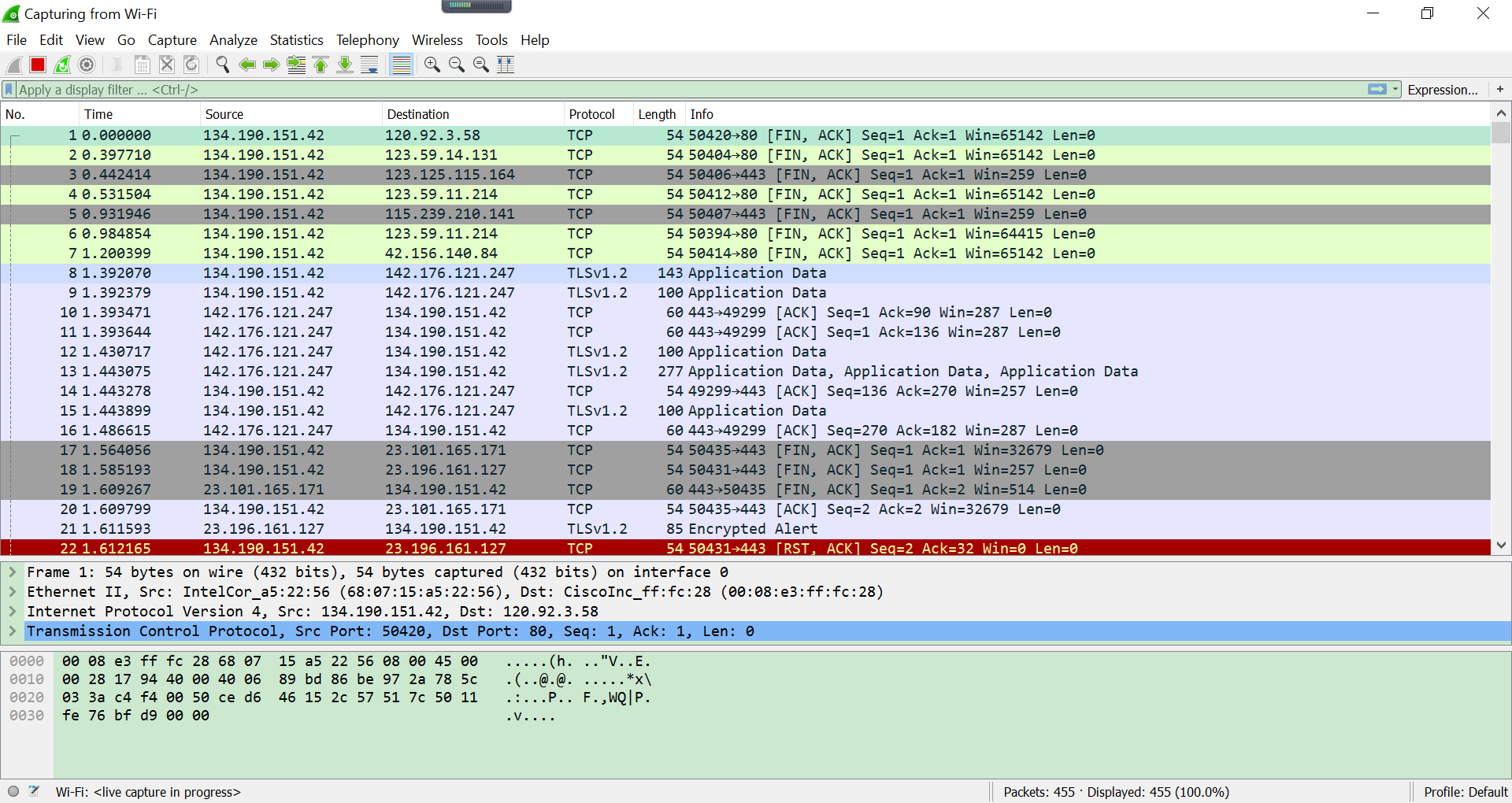
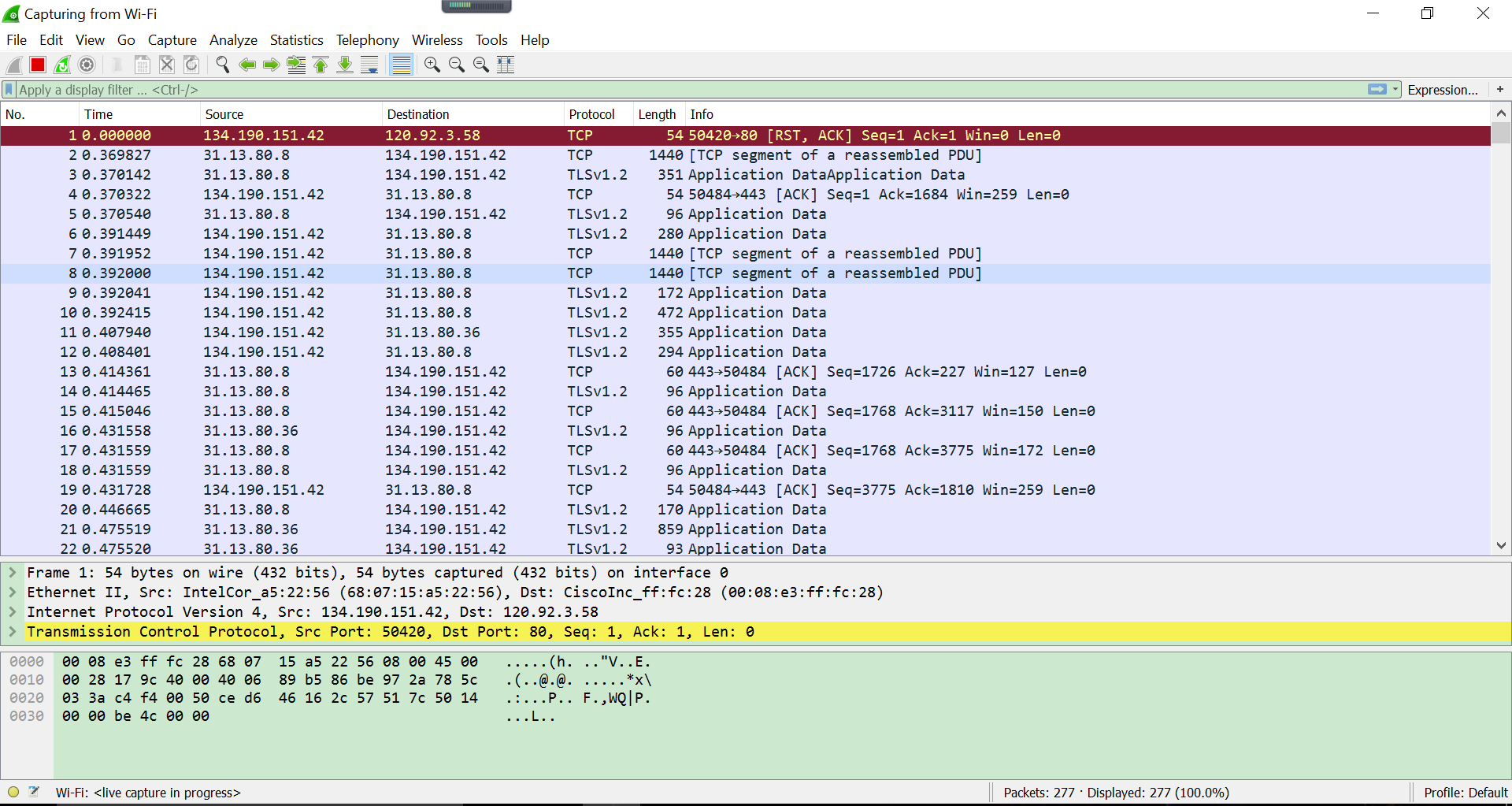
Assignment 2 Zehao Ba (B00732676)

1. Experimental study with Wireshark

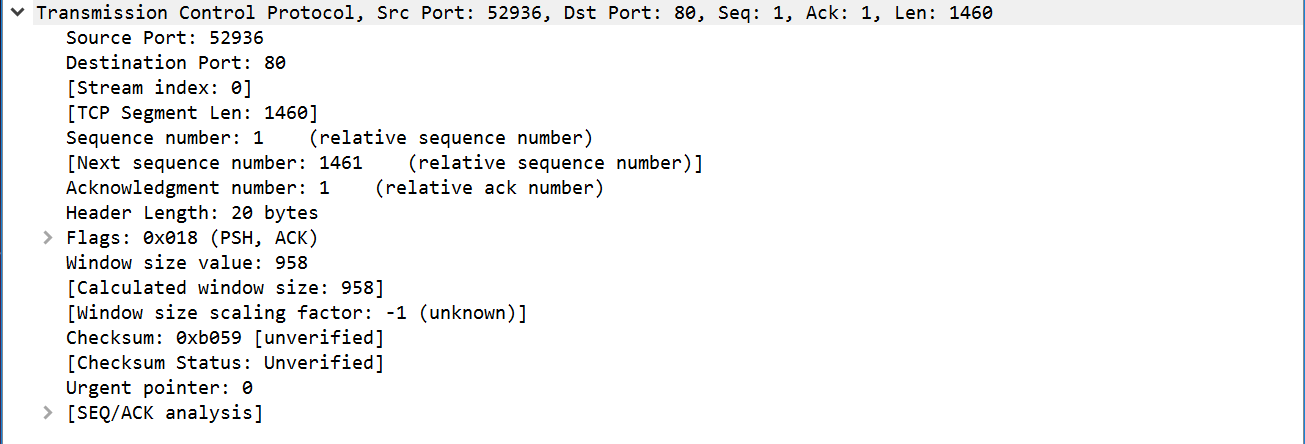
b) www.cisco.com



www.google.ca

 www.facebook.com

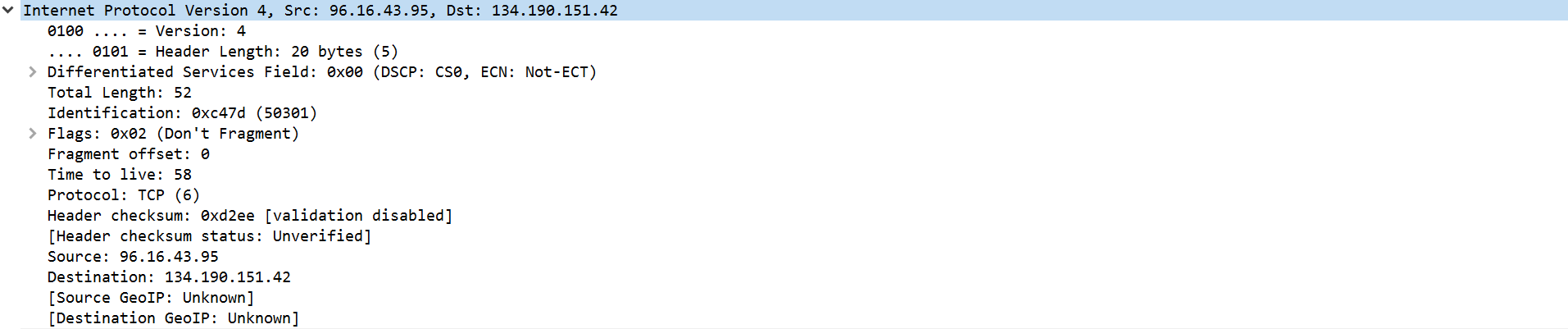
c) www.cisco.com-TCP segment



0 15 16 31

|  |  |  |  |
| --- | --- | --- | --- |
| Source port number:52936 | | | Destination port number:80 |
| Sequence number:1 | | | |
| Acknowledgement Number:1 | | | |
| Header length :20 | Reserved: Not set | Flags: 0x018 (PSH, ACK) | Window size: 958 |
| TCP checksum = 0xb059 | | | Urgent pointer: 0 |
| TCP Segment data = 1386 bytes | | | |

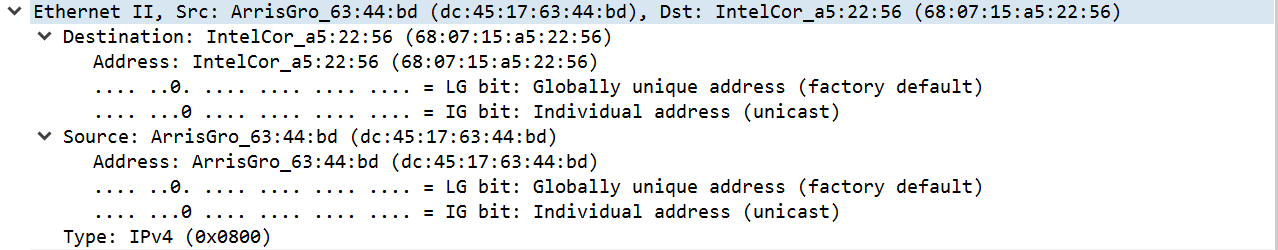
www.cisco.com-IP datagram



0 16 31

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP version:4 | Header  Length: 20 bytes | Differentiated Services Field: 0x00 (DSCP CS0: ECN: NOT-ECT) | Total length: 52 | |
| Identification: 0Xc47d (50301) | | | Flags: 0x02 (Don't Fragment) | Fragment Offset: 0 |
| Time-to-live:58 | | Protocol: TCP(6) | Header Checksum: 0xd2ee | |
| Source IP Address: 96.16.43.95 | | | | |
| Destination IP Address: 134.190.151.42 | | | | |

www.cisco.com-data link layer frame

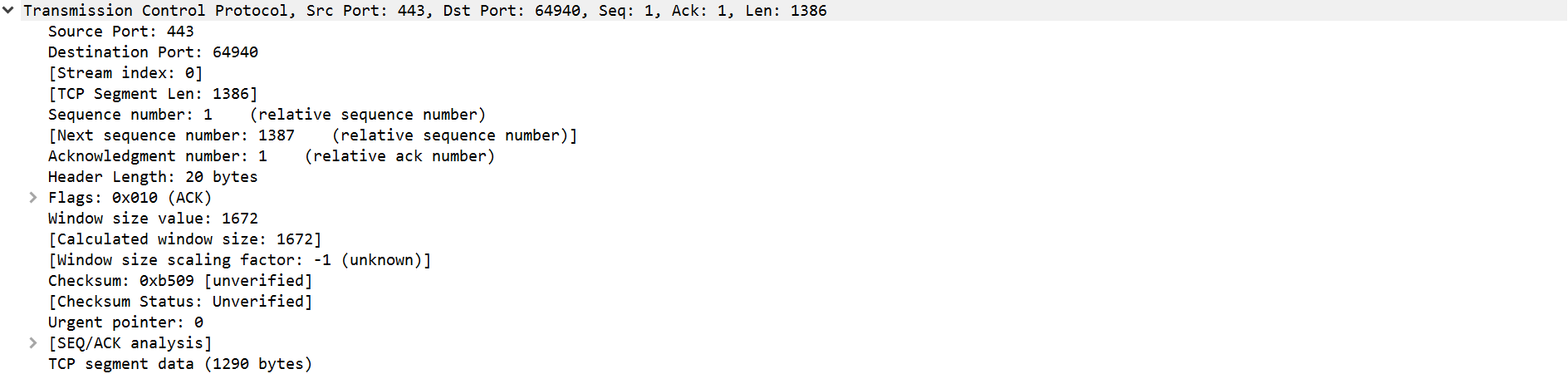


Ethernet Header:

|  |  |  |
| --- | --- | --- |
| Destination Address:  68:07:15:a5:22:56 | Source Address:  45:17:63:44:bd | Type: IP v4(0x0800) |

---------------------------------------------------------------------------------------------------------------------

www.google.com-TCP segment



0 15 16 31

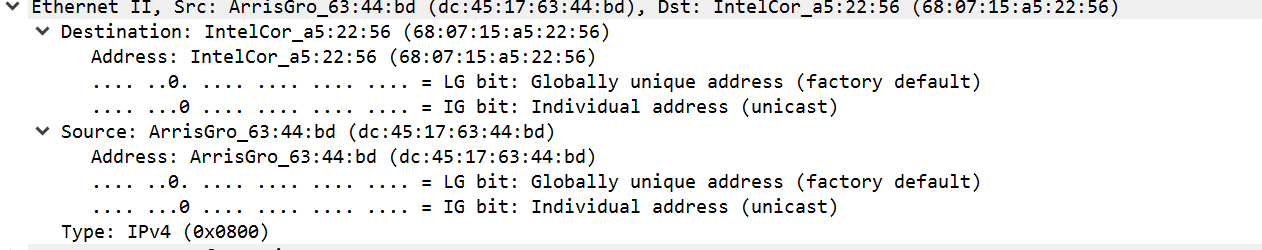
|  |  |  |  |
| --- | --- | --- | --- |
| Source port number:443 | | | Destination port number:64940 |
| Sequence number:1 | | | |
| Acknowledgement Number:1 | | | |
| Header length :20 | Reserved: Not set | Flags: 0x010 (ACK) | Window size: 1672 |
| TCP checksum = 0xb509 | | | Urgent pointer: 0 |
| TCP Segment data = 1290 bytes | | | |

www.google.com-IP datagram

0 16 31

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP version:4 | Header  Length: 20 bytes | Differentiated Services Field: 0x00 (DSCP CS0: ECN: NOT-ECT) | Total length: 1426 | |
| Identification: 0x6622 (26146) | | | Flags: 0x00 (Don't Fragment) | Fragment Offset: 0 |
| Time-to-live:59 | | Protocol: TCP(6) | Header Checksum: 0xedbe | |
| Source IP Address: 142.176.121.236 | | | | |
| Destination IP Address: 134.190.151.42 | | | | |

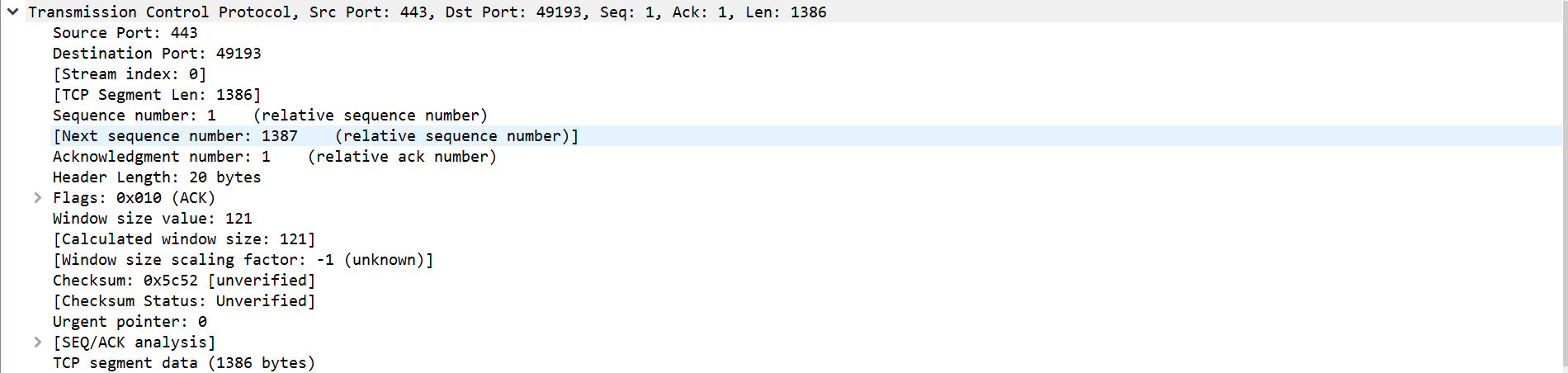
www.google.com-data link layer frame



|  |  |  |
| --- | --- | --- |
| Destination Address:  68:07:15:a5:22:56 | Source Address:  45:17:63:44:bd | Type: IP v4(0x0800) |

---------------------------------------------------------------------------------------------------------------------

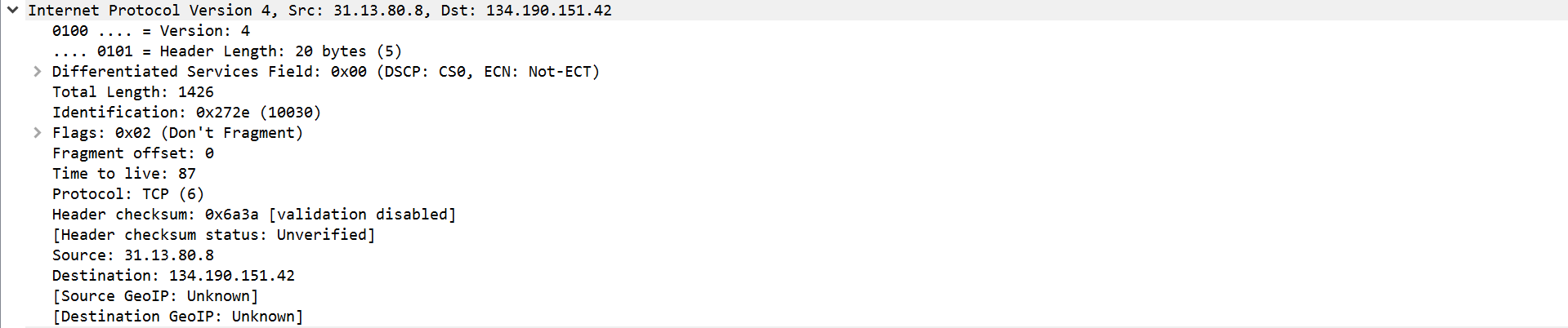
www.facebook.com-TCP segment



0 15 16 31

|  |  |  |  |
| --- | --- | --- | --- |
| Source port number:443 | | | Destination port number:49193 |
| Sequence number:1 | | | |
| Acknowledgement Number:1 | | | |
| Header length :20 bytes | Reserved: Not set | Flags: 0x010 (ACK) | Window size: 121 |
| TCP checksum = 0x5c52 | | | Urgent pointer: 0 |
| TCP Segment data = 1386 bytes | | | |

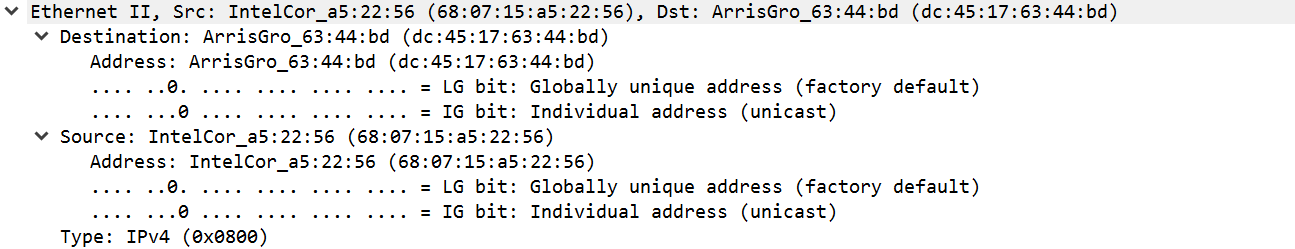
www.facebook.com-IP datagram



0 16 31

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP version:4 | Header  Length: 20 bytes | Differentiated Services Field: 0x00 (DSCP CS0: ECN: NOT-ECT) | Total length: 1426 | |
| Identification: 0x272e (10030) | | | Flags: 0x02 (Don't Fragment) | Fragment Offset: 0 |
| Time-to-live:87 | | Protocol: TCP(6) | Header Checksum: 0x6a3a | |
| Source IP Address: 31.13.80.8 | | | | |
| Destination IP Address: 134.190.151.42 | | | | |

www.facebook.com-data link layer frame



|  |  |  |
| --- | --- | --- |
| Destination Address:  45:17:63:44:bd | Source Address:  68:07:15:a5:22:56 | Type: IP v4(0x0800) |

d) According to the screen snapshot of the three websites, I found we can use Wireshark to know the packet, MAC/IP address, TCP/UDP port, protocol or the content of packet during the transmission and we can find the transmission process. The wireshark helps us to understand how the packet transmit in the different layer and what is the specific information of the transmission.

3.

