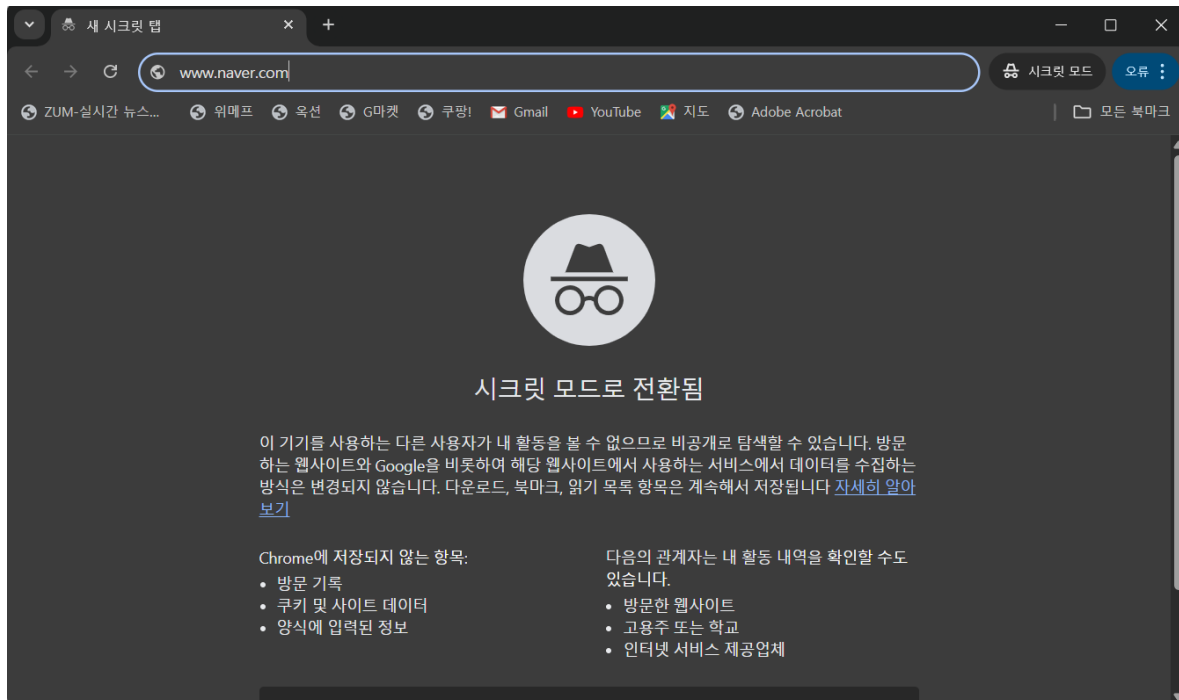


보안프로토콜 6주차 과제

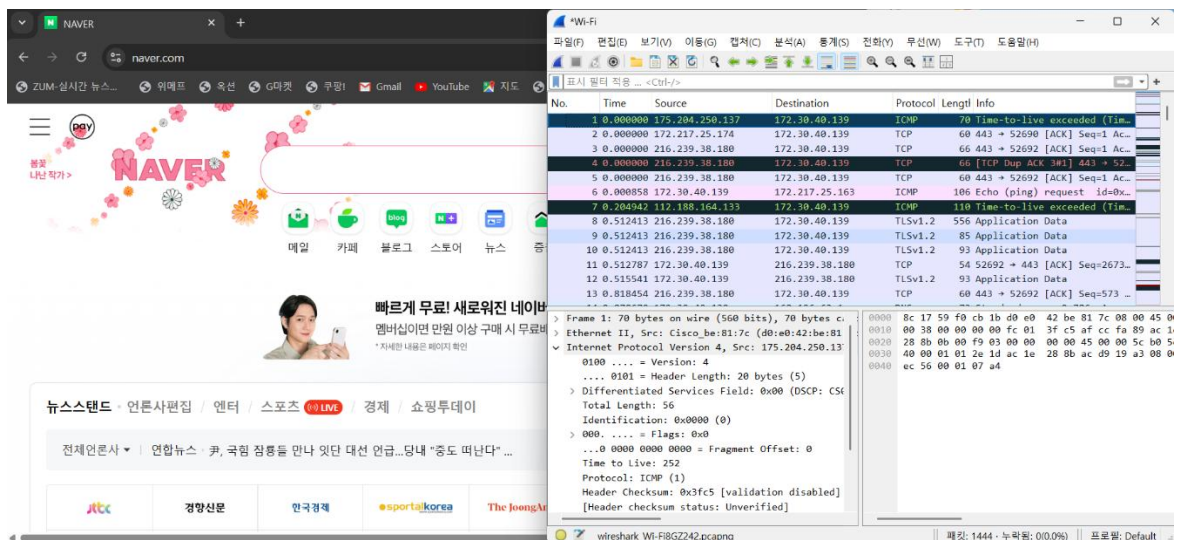
202121556 곽지현

크롬 브라우저 창을 시크릿 모드로 열고 주소 창에 naver.com 입력



WIRESHARK 캡처버튼을 클릭 후, 네이버 페이지에 접속한다.

네이버 홈페이지 로딩이 끝나면 WIRESHARK 정지 버튼 클릭



캡처된 데이터에서 DNS 쿼리 부분을 찾는다.

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list on the left shows a series of packets. Packet 14 is selected, showing a DNS Standard query from 172.30.40.139 to 168.126.63.1. The packet details pane on the right shows the structure of the DNS query, including Transaction ID, Flags, Questions, Answer RRs, Authority RRs, Additional RRs, and Queries. The packet bytes pane on the right shows the raw data of the packet, with the DNS query data highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.512413	216.239.38.180	172.30.40.139	TLSv1.2	93	Application Data
11	0.512787	172.30.40.139	216.239.38.180	TCP	54	52692 → 443 [ACK] Seq=2673 Ack=534 Win=...
12	0.515541	172.30.40.139	216.239.38.180	TLSv1.2	93	Application Data
13	0.818454	216.239.38.180	172.30.40.139	TCP	60	443 → 52692 [ACK] Seq=573 Ack=2712 Win=...
14	0.878670	172.30.40.139	168.126.63.1	DNS	73	Standard query 0x786c A www.naver.com
15	0.879469	172.30.40.139	168.126.63.1	DNS	73	Standard query 0x4f0b HTTPS www.naver.c...
16	0.979632	168.126.63.1	172.30.40.139	DNS	174	Standard query response 0x786c A www.na...
17	0.979632	168.126.63.1	172.30.40.139	DNS	171	Standard query response 0x4f0b HTTPS ww...
18	0.981181	172.30.40.139	223.130.192.248	TCP	66	52702 → 443 [SYN] Seq=0 Win=65535 Len=0...
19	0.987708	172.30.41.80	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
20	1.071683	223.130.192.248	172.30.40.139	TCP	66	443 → 52702 [SYN, ACK] Seq=0 Ack=1 Win=...
21	1.071795	172.30.40.139	223.130.192.248	TCP	54	52702 → 443 [ACK] Seq=1 Ack=1 Win=65280...
22	1.072446	172.30.40.139	223.130.192.248	TLSv1.3	1809	Client Hello (SNI=www.naver.com)

Frame 14: 73 bytes on wire (584 bits), 73 bytes captured
> Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst:
> Internet Protocol Version 4, Src: 172.30.40.139, Dst: 168
> User Datagram Protocol, Src Port: 56661, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x786c
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[\[Response In: 16\]](#)

0000 d0 e0 42 be 81 7c 8c 17 59 f0 cb 1b 08 00 45 00
0010 00 3b 8c 33 00 00 80 11 00 00 ac 1e 28 8b a8 7e
0020 3f 01 dd 55 00 35 00 27 bc 61 78 6c 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 05 6e 61 76 65 72
0040 03 63 6f 6d 00 00 01 00 01

wireshark_Wi-Fi8GZ242.pcapng | 패킷: 1444 · 누락됨: 0(0.0%) | 프로파일: Default

네이버 IP로 연결하는 과정 (3-Way Handshake) 을 찾는다.

[SYN]

[SYN, ACK]

[ACK]

174 Standard query response 0x786c
171 Standard query response 0x4f0b
66 52702 → 443 [SYN] Seq=0 Win=65535
179 M-SEARCH * HTTP/1.1
66 443 → 52702 [SYN, ACK] Seq=0 Ac
54 52702 → 443 [ACK] Seq=1 Ack=1 W
1809 Client Hello (SNI=www.naver.com)

첫번째 패킷(SYN)을 클릭 -> Frame 필드 부분 확인 (실제 데이터)

The screenshot shows the Wireshark interface with a packet capture of a SYN packet. The packet list on the left shows packet 18 selected, which is a TCP SYN packet from 172.30.40.139 to 223.130.192.248. The packet details pane on the right shows the following structure:

- Frame 18: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: Cisco_be:81:7c (d0:e0:42:be:81:7c)
- Internet Protocol Version 4, Src: 172.30.40.139, Dst: 223.130.192.248
- Transmission Control Protocol, Src Port: 52702, Dst Port: 443, Seq: 0, Len: 0

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The first few bytes are 0000, 0010, 0020, 0030, 0040, which correspond to the Ethernet II header fields.

Ethernet 부분 확인 (MAC 주소)

The screenshot shows the Wireshark interface with the same packet capture. The packet details pane on the right shows the Ethernet II details expanded, showing the source and destination MAC addresses:

- Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: Cisco_be:81:7c (d0:e0:42:be:81:7c)
- Source: Intel_f0:cb:1b (8c:17:59:f0:cb:1b)
- Type: IPv4 (0x0800)
- [Stream index: 0]

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The first few bytes are 0000, 0010, 0020, 0030, 0040, which correspond to the Ethernet II header fields.

IP 부분 확인 (IP 주소 - 172.30.40.139 / 223.130.192.248)

The screenshot shows the Wireshark interface with a packet list on the left and packet details on the right. The selected packet is a TCP SYN packet (No. 18) from 172.30.40.139 to 223.130.192.248. The packet details pane shows the following information:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 52
- Identification: 0xda6f (55919)
- 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 172.30.40.139
- Destination Address: 223.130.192.248
- [Stream index: 6]
- Transmission Control Protocol, Src Port: 52702, Dst Port: 443, Seq: 0

The packet bytes pane shows the raw data of the packet, including the IP header and the TCP header.

TCP 부분 확인 (포트 번호 - 52702 / 443)

The screenshot shows the Wireshark interface with a packet list on the left and packet details on the right. The selected packet is a TCP SYN packet (No. 18) from 172.30.40.139 to 223.130.192.248. The packet details pane shows the following information:

- Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: Cisco_be:81
- Internet Protocol Version 4, Src: 172.30.40.139, Dst: 223.130.192.248
- Transmission Control Protocol, Src Port: 52702, Dst Port: 443, Seq: 0
- Source Port: 52702
- Destination Port: 443
- [Stream index: 2]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 2278147414
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1000 = Header Length: 32 bytes (8)

The packet bytes pane shows the raw data of the packet, including the IP header and the TCP header.

18번에서 시작한 패킷은 103번 패킷에서 끝난다.

*Wi-Fi				
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S)				
표시 필터 적용 ... <Ctrl-/>				
No.	Time	Source	Destination	
16	0.979632	168.126.63.1	172.30.40.139	
17	0.979632	168.126.63.1	172.30.40.139	
18	0.981181	172.30.40.139	223.130.192.248	
19	0.987708	172.30.41.80	239.255.255.250	
20	1.071683	223.130.192.248	172.30.40.139	
21	1.071795	172.30.40.139	223.130.192.248	
22	1.072446	172.30.40.139	223.130.192.248	
23	1.165646	223.130.192.248	172.30.40.139	
24	1.165646	223.130.192.248	172.30.40.139	
25	1.165646	223.130.192.248	172.30.40.139	
26	1.165646	223.130.192.248	172.30.40.139	
27	1.165841	172.30.40.139	223.130.192.248	
28	1.169377	172.30.40.139	223.130.192.248	
*Wi-Fi				
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A)				
표시 필터 적용 ... <Ctrl-/>				
No.	Time	Source	Destination	
97	1.578343	172.30.40.139	223.130.192.248	
98	1.582028	223.130.192.248	172.30.40.139	
99	1.582028	223.130.192.248	172.30.40.139	
100	1.582028	223.130.192.248	172.30.40.139	
101	1.582142	172.30.40.139	223.130.192.248	
102	1.582182	172.30.40.139	223.130.192.248	
103	1.582205	172.30.40.139	223.130.192.248	
104	1.587208	172.30.40.139	168.126.63.1	
105	1.587921	172.30.40.139	168.126.63.1	
106	1.623748	43.250.152.63	172.30.40.139	
107	1.623889	172.30.40.139	43.250.152.63	
108	1.624682	172.30.40.139	43.250.152.63	
109	1.625112	43.250.152.63	172.30.40.139	