2025 컴퓨터 네트워크

Task 2

Task 2: HTTP와 TCP 패킷 분석하기

- Web Server를 하나 선정하여 Browser로 접속할 때 오가는 패킷을 Wireshark으로 캡처
- Application Layer - HTTP, Transport Layer – TCP 패킷 분석

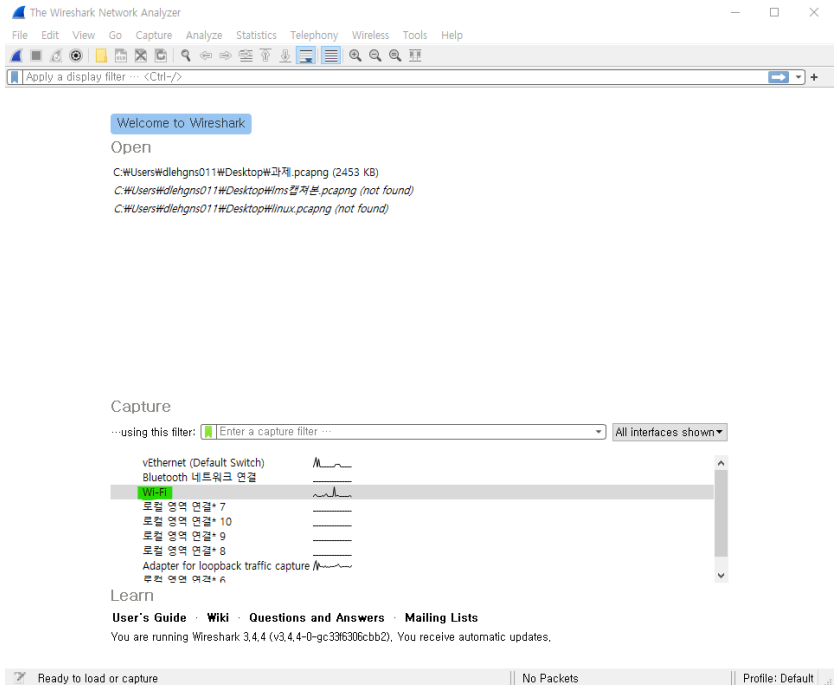
제출기한: 5/8 23:00

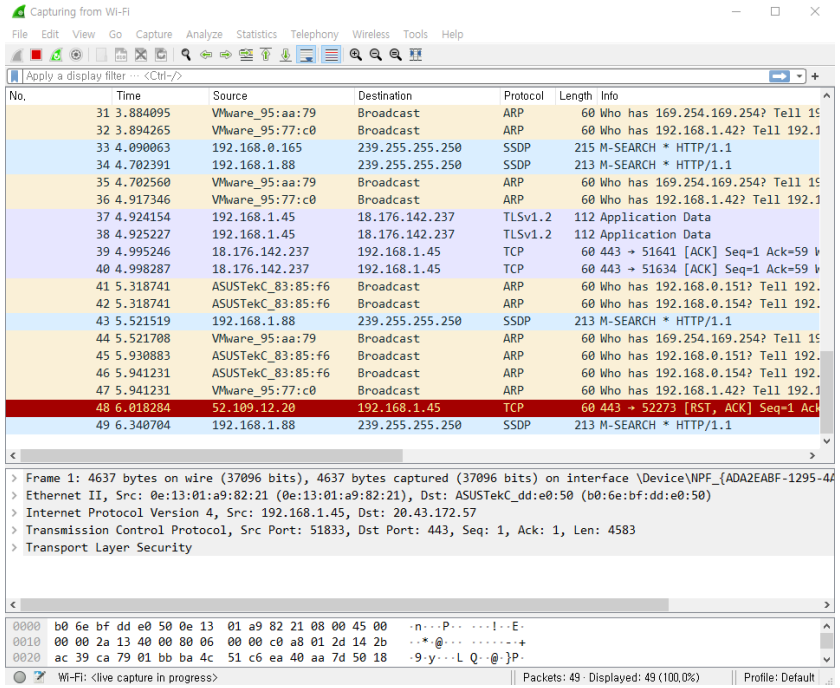
<진행 방법>

1. Wireshark를 실행, 캡처를 시작
2. Browser로 Web Server를 접속, 정보검색, 종료
3. 캡처 종료 및 캡처 내용을 저장 (확장자: *.pcapng).. 추후에도 사용되므로 저장 필수!
4. 캡처 내용에는 많은 패킷이 함께 들어 있으므로
   서버와 관련된 패킷만 필터링하여 분석한다.

** 서버의 주소를 알기 위해서는 nslookup을 사용

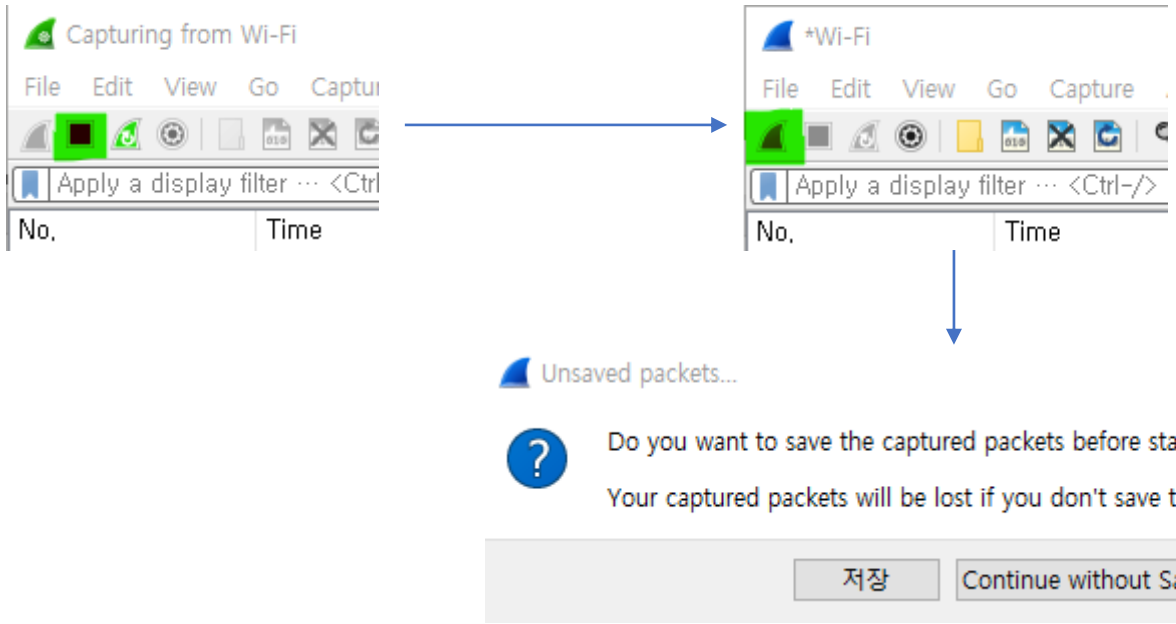
Wireshark 사용법





Wireshark를 실행 후 wi-fi(사용자의 네트워크 연결에 따라 다름, 여기서는 와이파이로 네트워크를 실행)를 선택하게 되면 오른쪽 화면으로 넘어가면서 캡처를 실행하게 됩니다.

Wireshark 사용법



1. MAC ID 필터링
- Source & DST 둘다 : eth.addr == 00:12:34:56:78:9A

2. IP 필터링
- Source & DST 둘다 : ip.addr == 13.107.4.50

3. 포트 필터링 (TCP, UDP 동일)
- Source & DST 둘다 : tcp.port == 80

명령어 : and, or

좌측 상단에 중지버튼을 누르게 되면 패킷의 캡처를 멈추게 됩니다. 다시 캡처를 하고 싶다면 우측 상단에 실행 버튼을 누르면 기존 캡처를 저장하는 창이 나오게 됩니다.

- HTTP와 TCP 말고도 Application layer와 transport layer에서 속한 패킷이 있다면 추가적으로 분석해주세요.

- 최대한 다양한 상황과 수업시간에 배운 개념들을 확인할 수 있도록 패킷들을 찾고 보고서에 이런 내용들을 넣어주세요.

Ex. HTTP : method, version, 상태 코드 등등

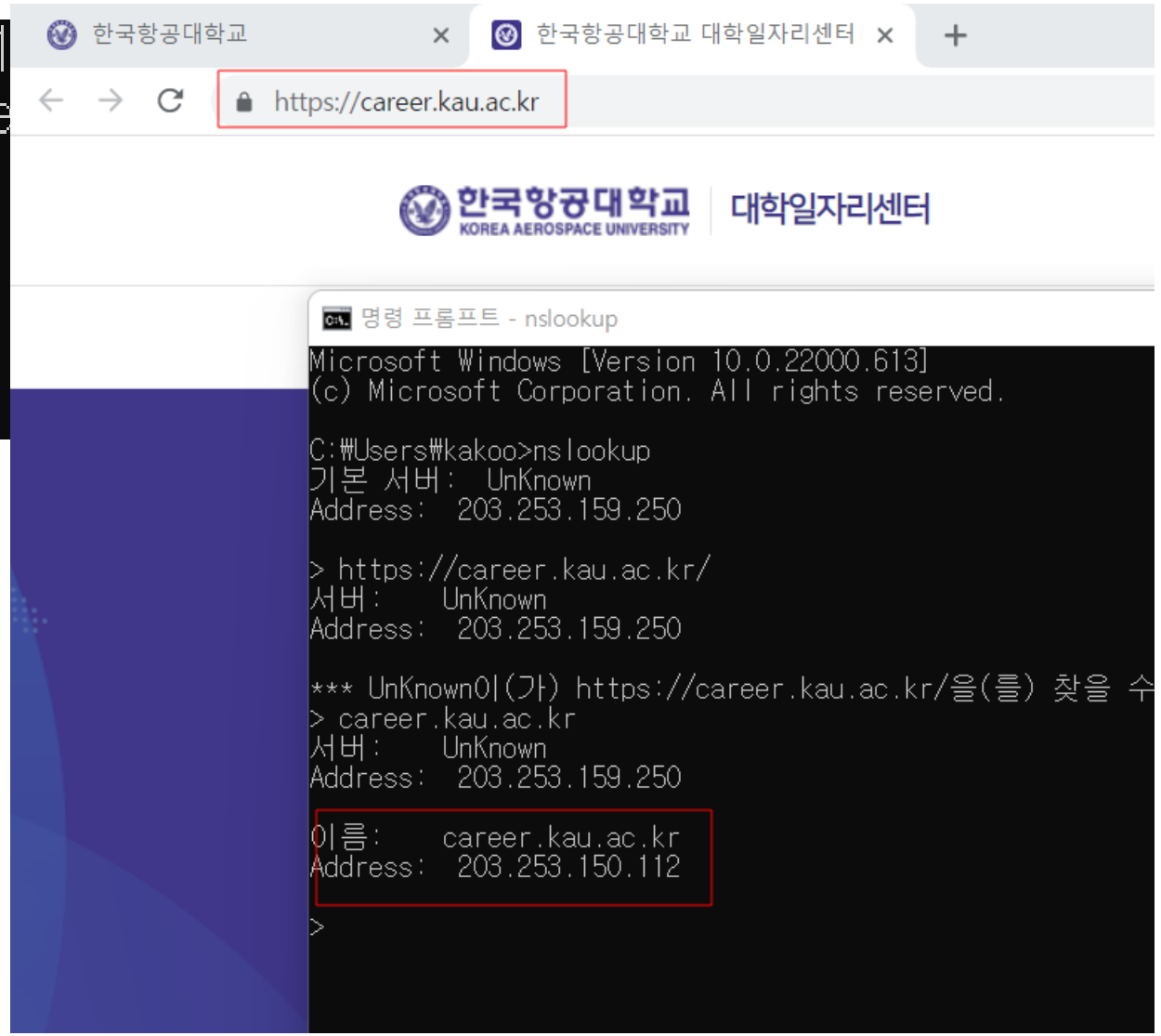
Ex. TCP : Duplicate Ack, 3-way or 4-way handshaking, flow control 등등

nslookup 사용법과, 캡쳐한 패킷 시나리오들

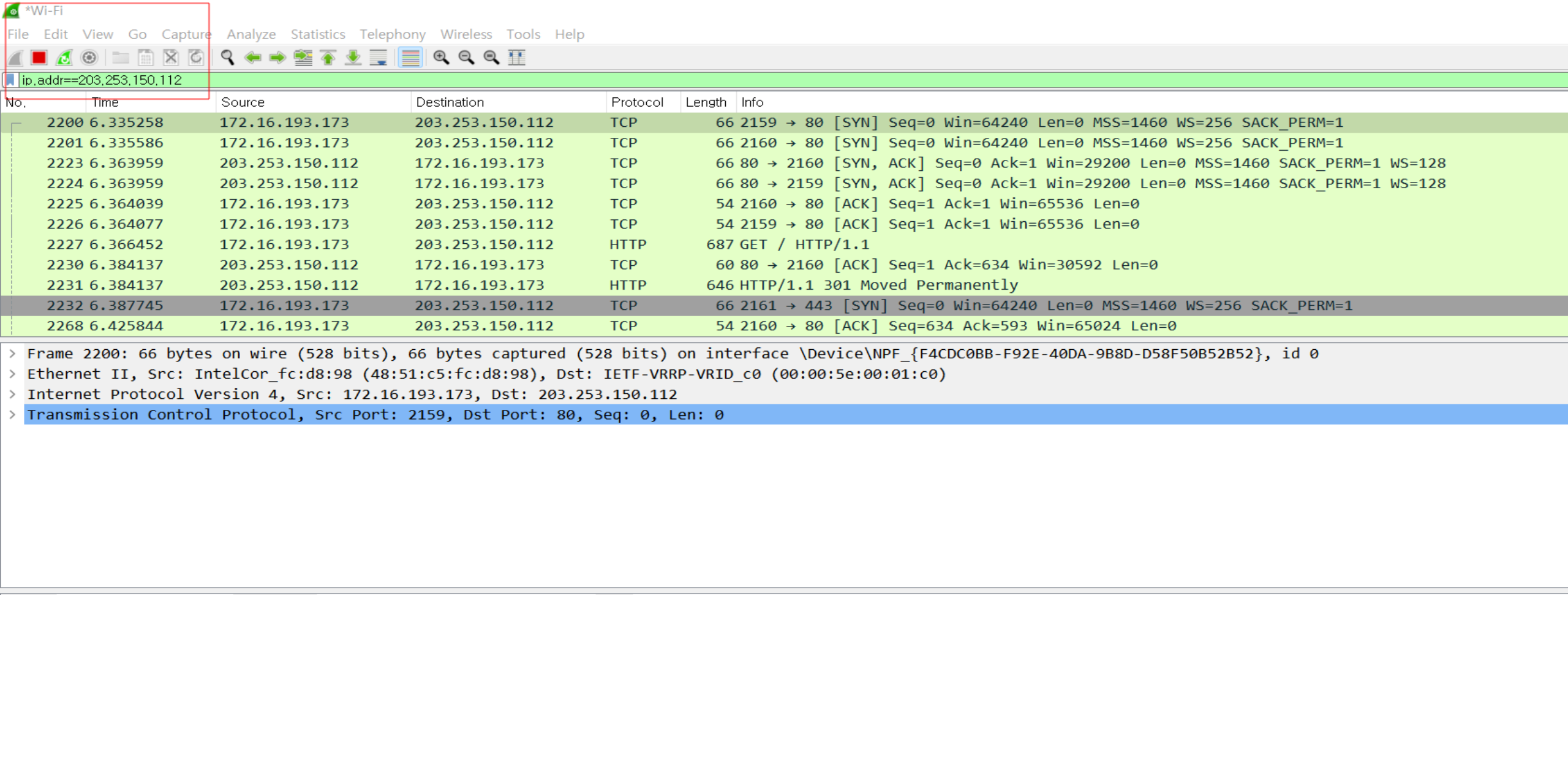
명령 프롬프트 - nslookup

```
Microsoft Windows [Version 10.0.22000.61
(c) Microsoft Corporation. All rights re

C:₩Users₩kakoo>nslookup
기본 서버:  UnKnown
Address:  203.253.159.250
```



Nslookup으로 알아낸 서버의 주소를 이용해 필터링한다



Protocol	Length	Info
TCP	1514	443 → 2163 [ACK] Seq=40597 Ack=7844 Win=22272 Len=1460 [TCP segment of a reassembled PDU]
TCP	1514	443 → 2163 [ACK] Seq=42057 Ack=7844 Win=22272 Len=1460 [TCP segment of a reassembled PDU]
TCP	1514	443 → 2163 [ACK] Seq=43517 Ack=7844 Win=22272 Len=1460 [TCP segment of a reassembled PDU]
TCP	1514	443 → 2163 [ACK] Seq=44977 Ack=7844 Win=22272 Len=1460 [TCP segment of a reassembled PDU]
TCP	1514	443 → 2167 [ACK] Seq=16434 Ack=5173 Win=16896 Len=1460 [TCP segment of a reassembled PDU]
TCP	1514	[TCP Retransmission] 443 → 2161 [ACK] Seq=40934 Ack=8697 Win=24064 Len=1460
TCP	66	[TCP Previous segment not captured] 443 → 2167 [ACK] Seq=19831 Ack=5173 Win=16896 Len=0 S
TCP	54	2161 → 443 [ACK] Seq=8697 Ack=42571 Win=65536 Len=0
TCP	54	2166 → 443 [ACK] Seq=6074 Ack=33243 Win=131328 Len=0
TCP	54	2165 → 443 [ACK] Seq=4320 Ack=63281 Win=131328 Len=0
TCP	54	2164 → 443 [ACK] Seq=6927 Ack=46758 Win=131328 Len=0

34616	181.291788	172.16.193.173	203.253.150.112	TCP	54	2165 → 443 [FIN, ACK] Seq=18102 Ack=364307 Win=131328 Len=0
34617	181.291851	172.16.193.173	203.253.150.112	TCP	54	2165 → 443 [RST, ACK] Seq=18103 Ack=364307 Win=0 Len=0
34618	181.291980	172.16.193.173	203.253.150.112	TCP	54	2164 → 443 [FIN, ACK] Seq=13762 Ack=168824 Win=130560 Len=0
34619	181.292014	172.16.193.173	203.253.150.112	TCP	54	2164 → 443 [RST, ACK] Seq=13763 Ack=168824 Win=0 Len=0
34620	181.292111	172.16.193.173	203.253.150.112	TCP	54	2167 → 443 [FIN, ACK] Seq=13053 Ack=407155 Win=131328 Len=0
34621	181.292139	172.16.193.173	203.253.150.112	TCP	54	2167 → 443 [RST, ACK] Seq=13054 Ack=407155 Win=0 Len=0
34622	181.292236	172.16.193.173	203.253.150.112	TCP	54	2161 → 443 [FIN, ACK] Seq=19184 Ack=486587 Win=65536 Len=0
34623	181.292269	172.16.193.173	203.253.150.112	TCP	54	2161 → 443 [RST, ACK] Seq=19185 Ack=486587 Win=0 Len=0
34638	181.293388	172.16.193.173	203.253.150.112	TCP	54	2168 → 443 [FIN, ACK] Seq=2854 Ack=6222 Win=131328 Len=0
34639	181.293467	172.16.193.173	203.253.150.112	TCP	54	2168 → 443 [RST, ACK] Seq=2855 Ack=6222 Win=0 Len=0