

컴퓨터네트워크 Task1

학과: 소프트웨어학과

학번: 2022125057

이름: 조재현

이메일: [cjh030808@kau.kr](mailto:cjh030808@kau.kr)

팀원:

2021125049 이은학

2022125041 이석진

**1. 개요**

이 과제에서는 서로 다른 네트워크를 사용하는 사람이 클라이언트와 서버 역할을 번갈아 수행하고 Wireshark를 이용해서 UDP와 TCP 패킷 분석이 목적이다.

**2. 이론적 배경**

포트포워딩: 컴퓨터 네트워크에서 라우터를 거쳐 하나의 IP주소와 포트번호의 결합으로 통신요청을 다른곳으로 넘겨주는 역할을 한다. 즉 공유기에 공인 IP가 설정되어 있고 각 기계(컴퓨터, 핸드폰, TV 등등)은 사설 IP를 사용하고 있는데 포트 번호를 보고 공유기가 사설 IP로 연결해주는 방식이다.

공인 IP: 인터넷 서비스 제공업체(ISP)로부터 할당받은, 외부에서 접근 가능한 IP 주소

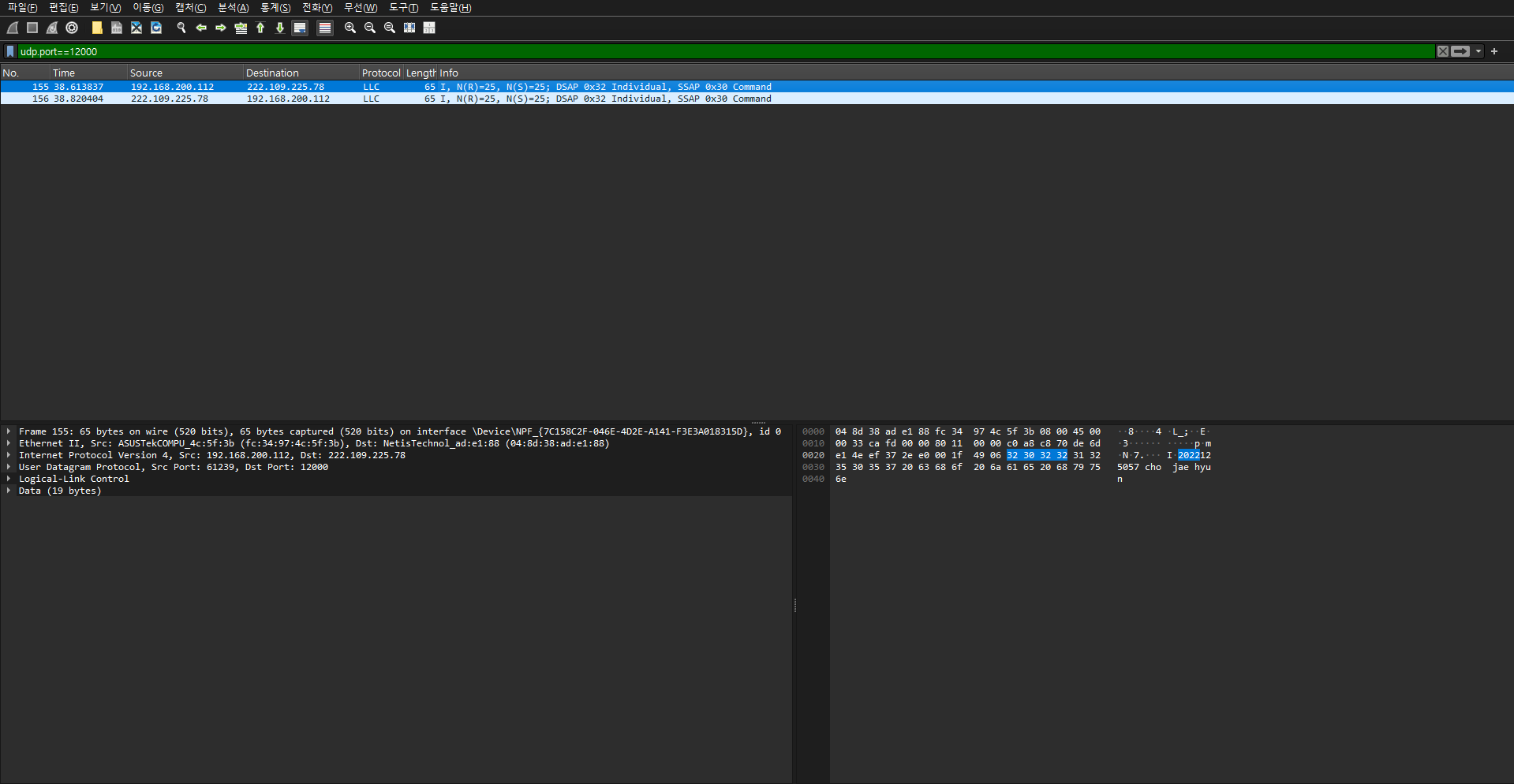
사설 IP: 내부 네트워크에서만 사용되는 IP 주소(예: 192.168.x.x, 10.x.x.x)

**3. Client 역할 패킷 분석**

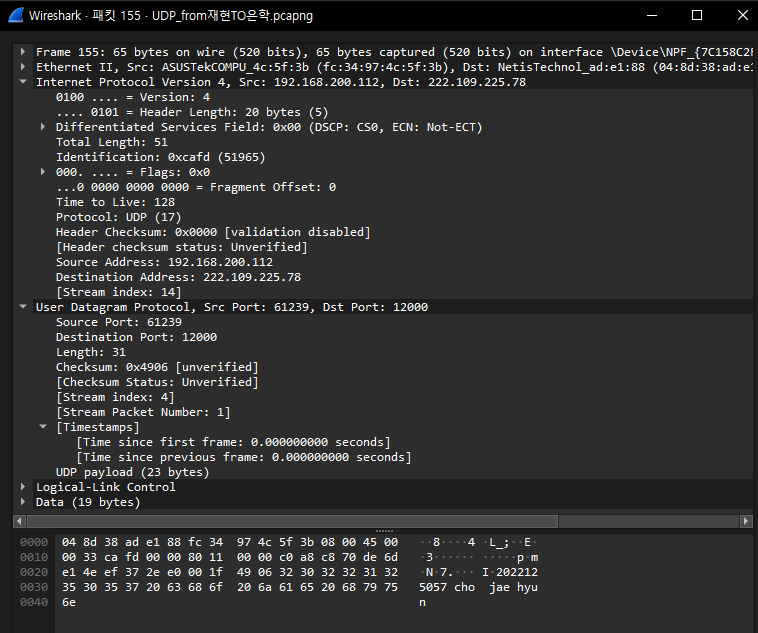
네트워크 인터페이스: Ethernet, 서버 포트: 12000

3-1. UDP

1. 조재현(client) <-> 이은학(server)



클라이언트 -> 서버 (UDP Request)



출발지 IP: 192.168.200.112

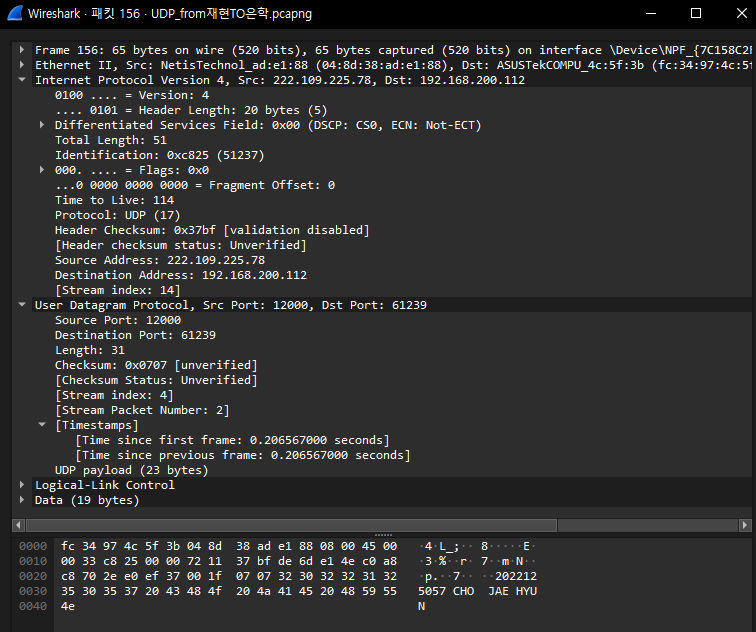
목적지 IP: 222.109.225.78

출발지 포트: 61239

목적지 포트: 12000

전송된 데이터 내용: 2022125057 cho jae hyun

서버 -> 클라이언트 (UDP Response)



출발지 IP: 222.109.225.78

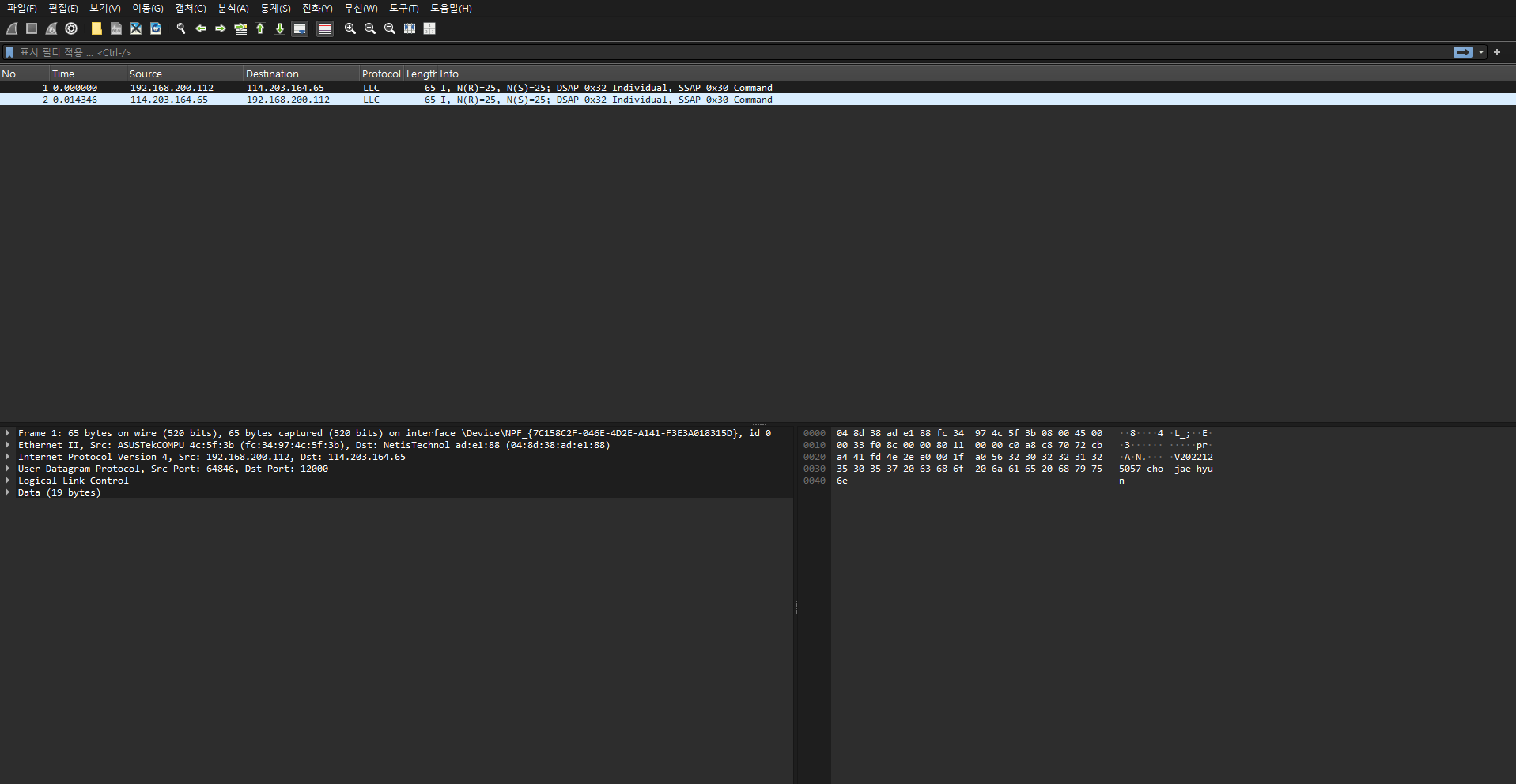
목적지 IP: 192.168.200.112

출발지 포트: 12000

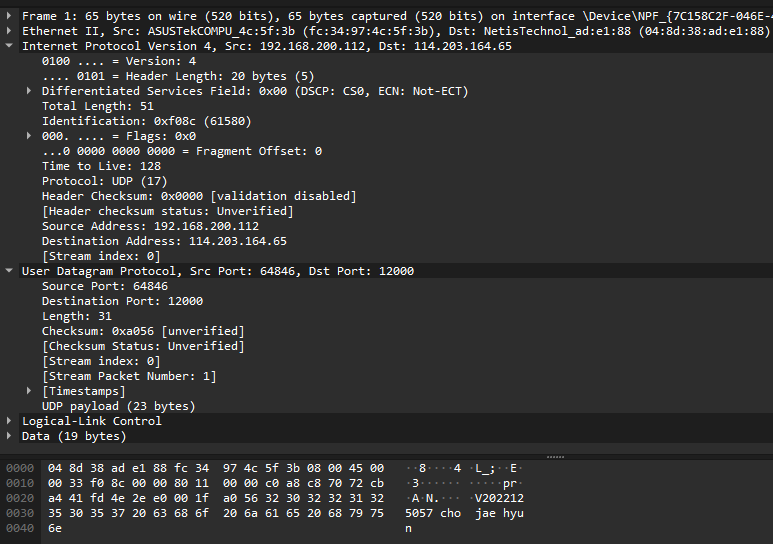
목적지 포트: 61239

응답 데이터: 2022125057 CHO JAE HYUN

2. 조재현(client) <-> 이석진(server)



클라이언트 -> 서버 (UDP Request)



출발지 IP: 192.168.200.112

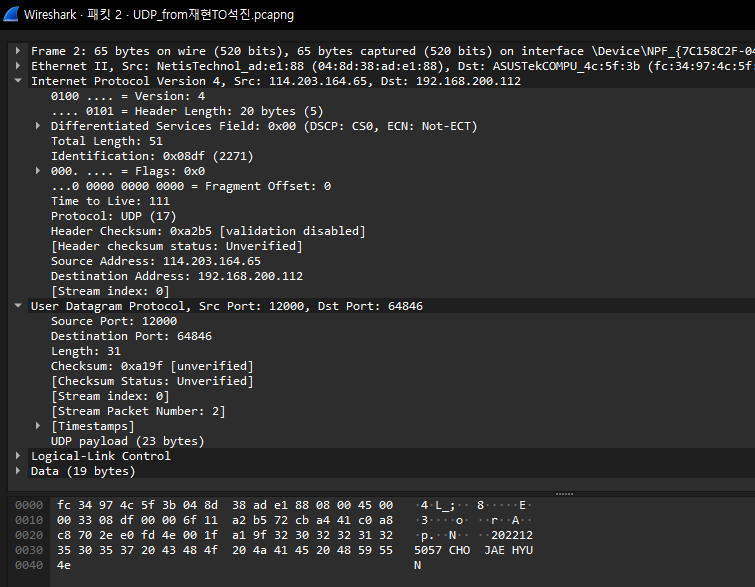
목적지 IP: 114.203.164.65

출발지 포트: 64846

목적지 포트: 12000

전송된 데이터 내용: 2022125057 cho jae hyun

서버-> 클라이언트 (UDP Response)



출발지 IP: 114.203.164.65

목적지 IP: 192.168.200.112

출발지 포트: 12000

목적지 포트: 64846

응답 데이터: 2022125057 CHO JAE HYUN

3-2. TCP

TCP는 UDP와 다르게 3-way handshake 과정을 포함됨.

Wireshark에서 캡처한 TCP 패킷을 분석한 결과, 클라이언트와 서버 간의 TCP 연결이 정상적으로 설정됨을 확인할 수 있었다.

- SYN→ 클라이언트가 서버에 연결 요청

- SYN-ACK→ 서버가 응답

- ACK→ 클라이언트가 확인 응답

TCP 4-way Handshake (연결 종료)

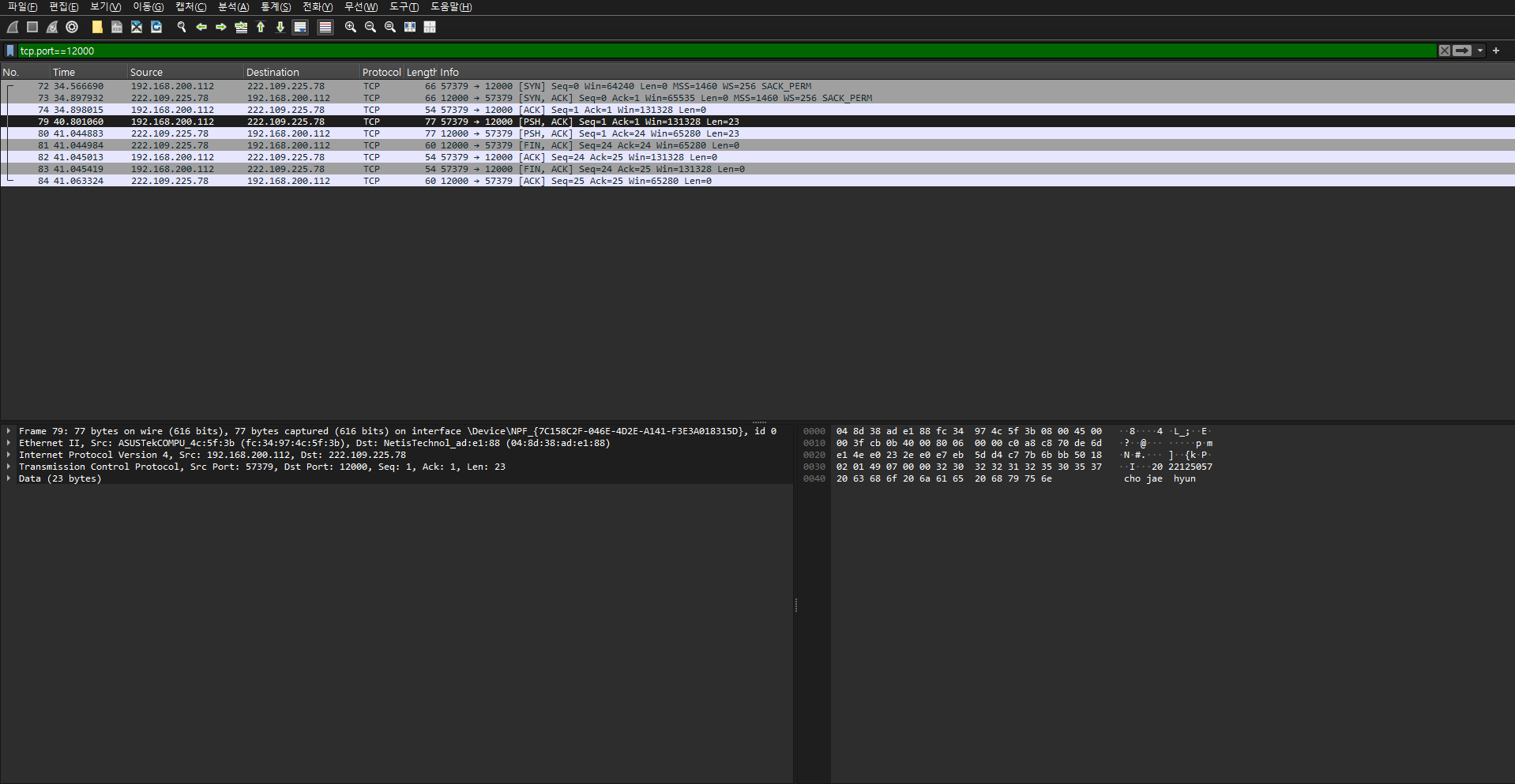
- FIN→ 클라이언트 또는 서버가 연결 종료 요청

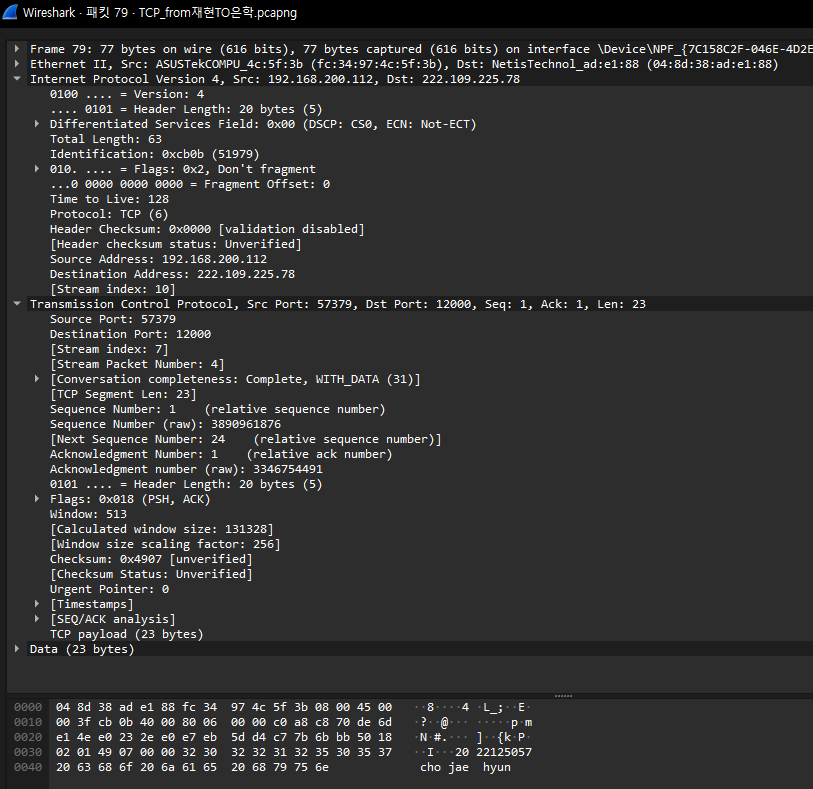
- ACK→ 상대방이 확인 응답

- FIN→ 반대쪽에서 연결 종료 요청

- ACK→ 최종 확인 후 연결 종료

1. 조재현(client) <-> 이은학(server)



클라이언트 -> 서버 (TCP Request) 

출발지 IP: 192.168.200.112

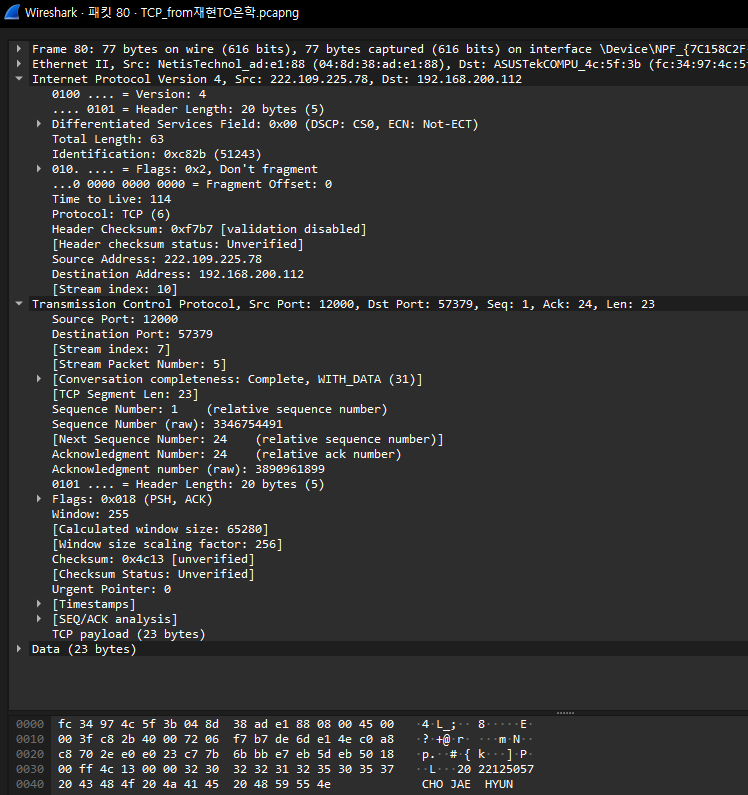
목적지 IP: 222.109.225.78

출발지 포트: 57379

목적지 포트: 12000

전송된 데이터 내용: 2022125057 cho jae hyun

서버 -> 클라이언트 (TCP Response)



출발지 IP: 222.109.225.78

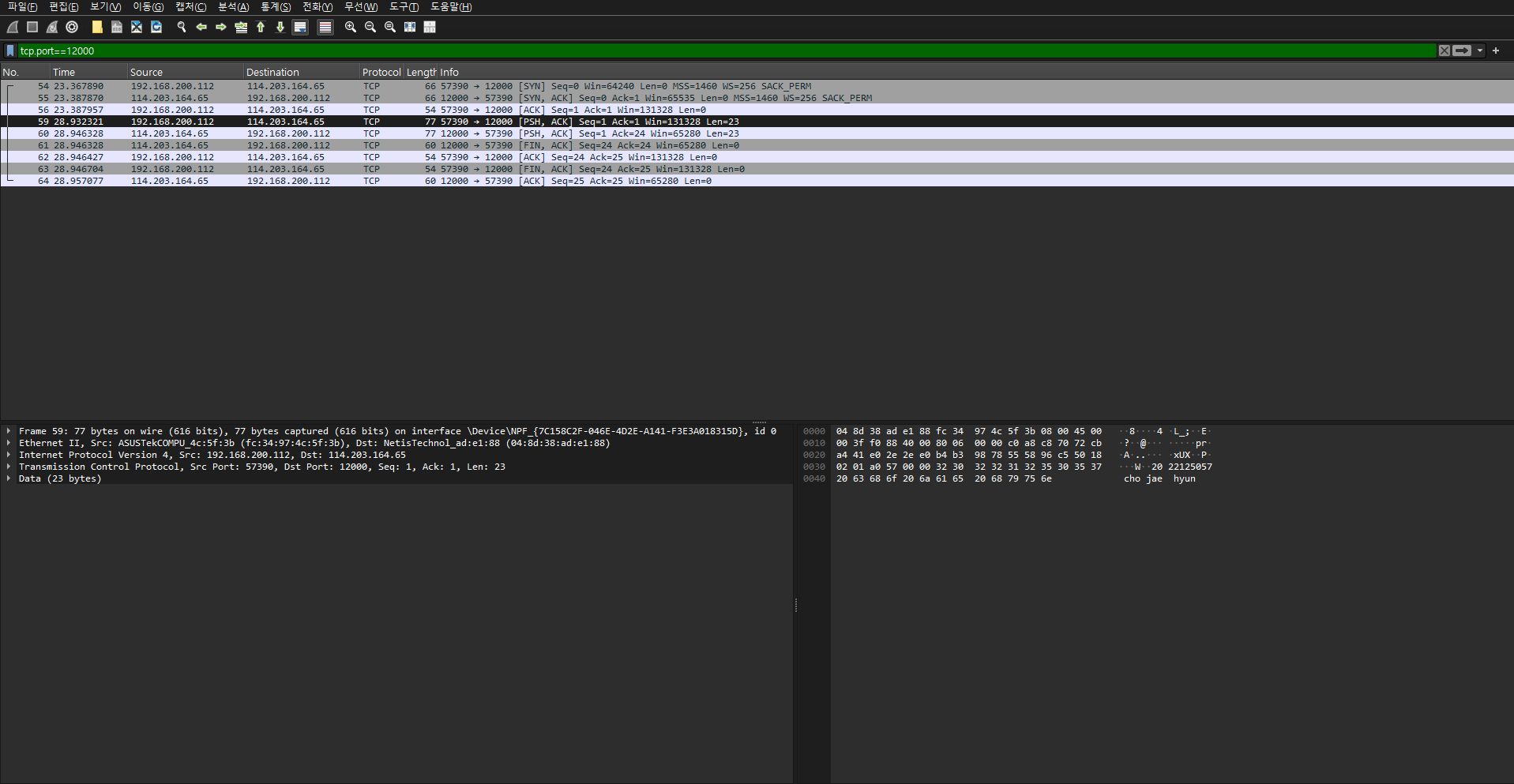
목적지 IP: 192.168.200.112

출발지 포트: 12000

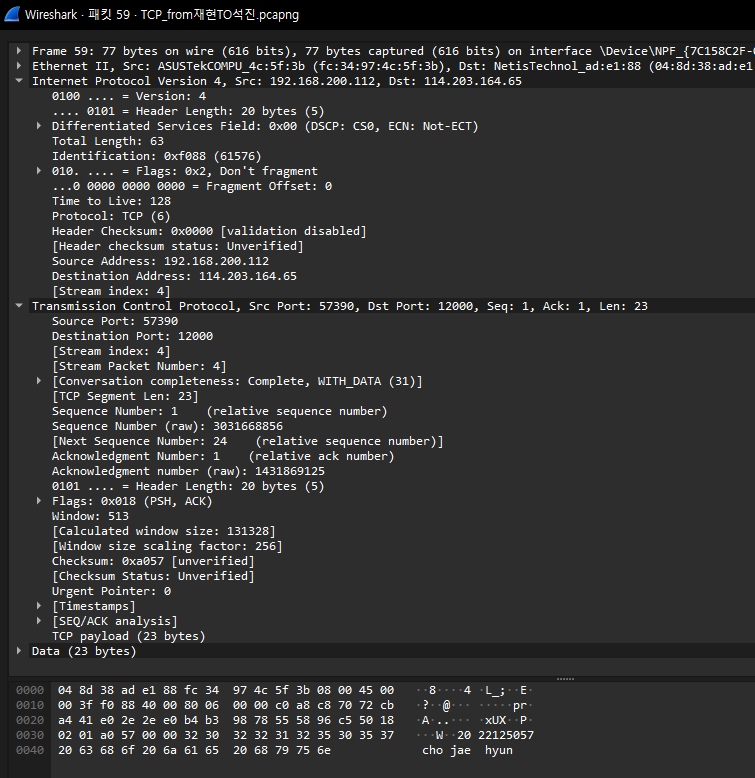
목적지 포트: 57379

응답 데이터: 2022125057 CHO JAE HYUN

2. 조재현(client) <-> 이석진(server)



클라이언트 -> 서버 (TCP Request)



출발지 IP: 192.168.200.112

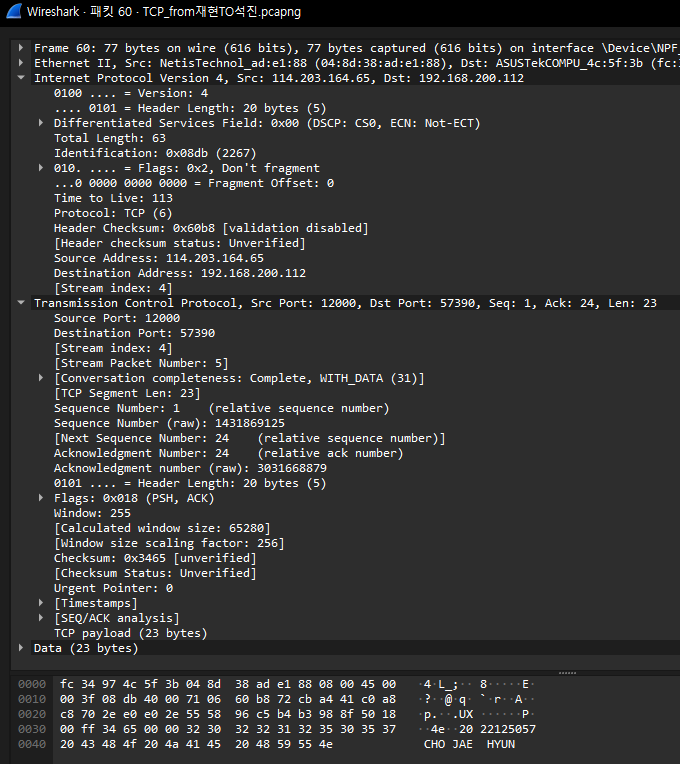
목적지 IP: 114.203.164.65

출발지 포트: 57390

목적지 포트: 12000

전송된 데이터 내용: 2022125057 cho jae hyun

서버 -> 클라이언트 (TCP Response)



출발지 IP: 114.203.164.65

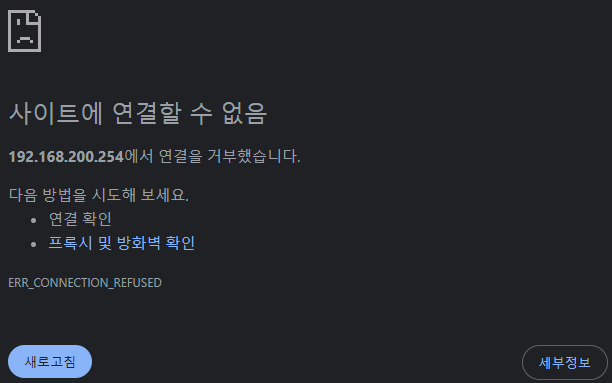
목적지 IP: 192.168.200.112

출발지 포트: 12000

목적지 포트: 57390

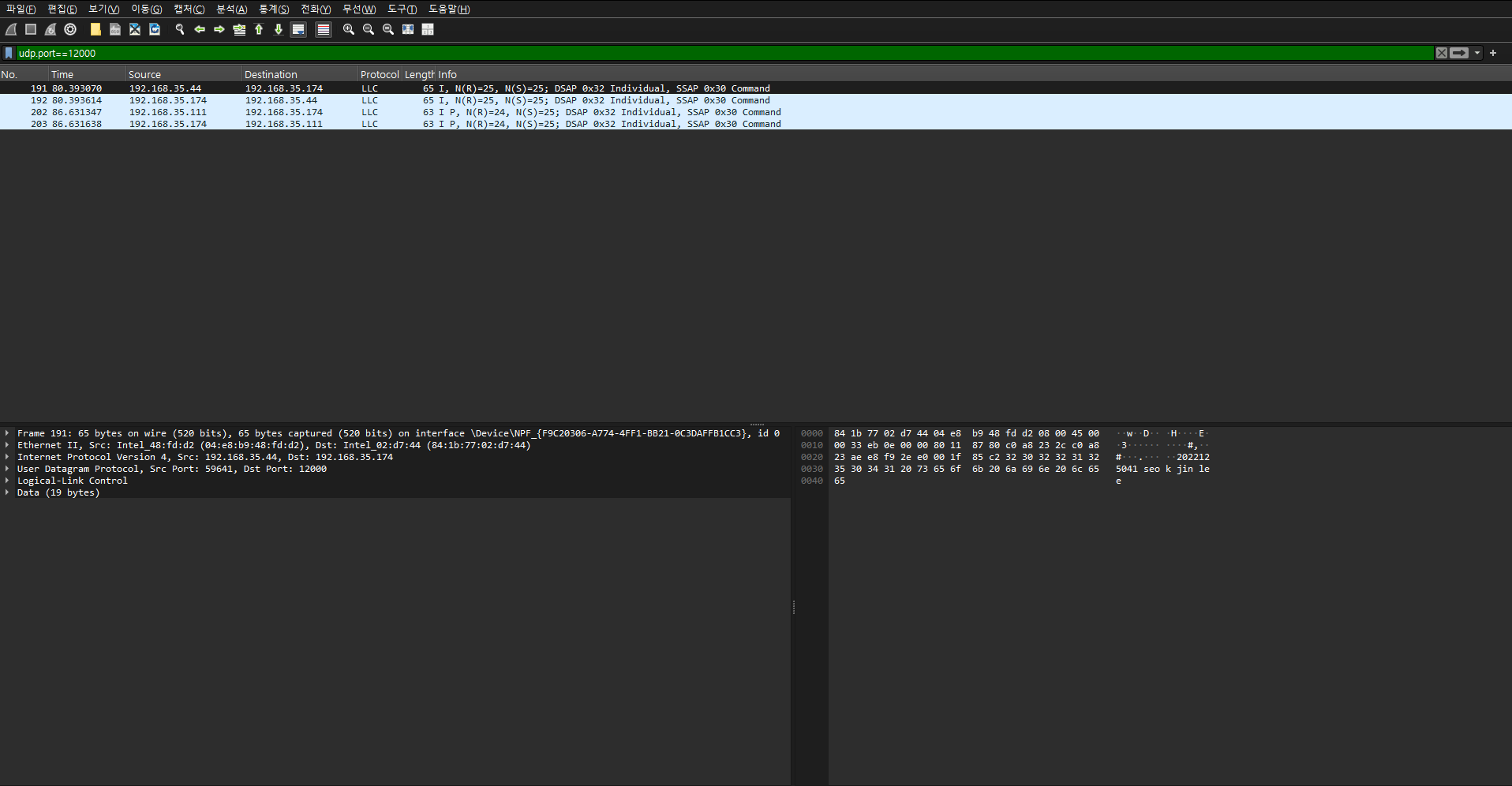
응답 데이터: 2022125057 CHO JAE HYUN

**4. Server 역할 패킷 분석**

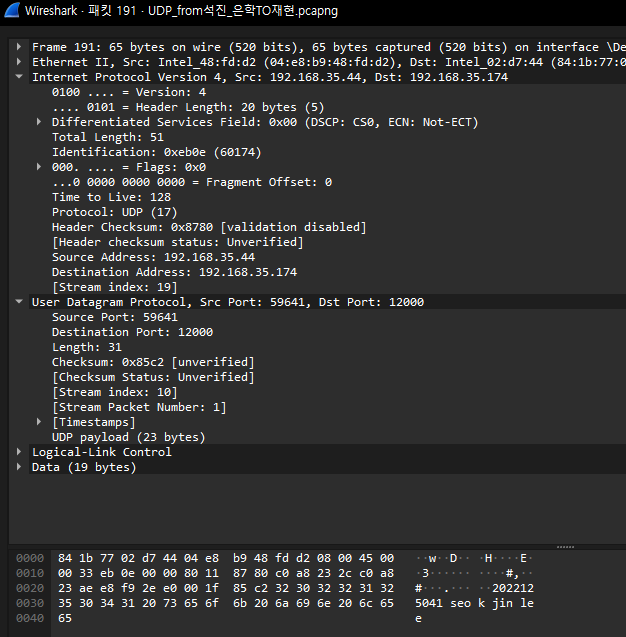


내 집에서는 네트워크 관리 웹사이트가 차단되어 있어 포트포워딩을 진행할 수 없었다. 이에 팀원 모두가 이석진의 집에 모여 내가 서버 역할을 맡고 팀원들이 클라이언트 역할을 수행하였다.

1. UDP, 클라이언트(이은학, 이석진) <-> 서버(조재현)



클라이언트(이석진) -> 서버(조재현) (UDP Resquest)



출발지 IP: 192.168.35.44

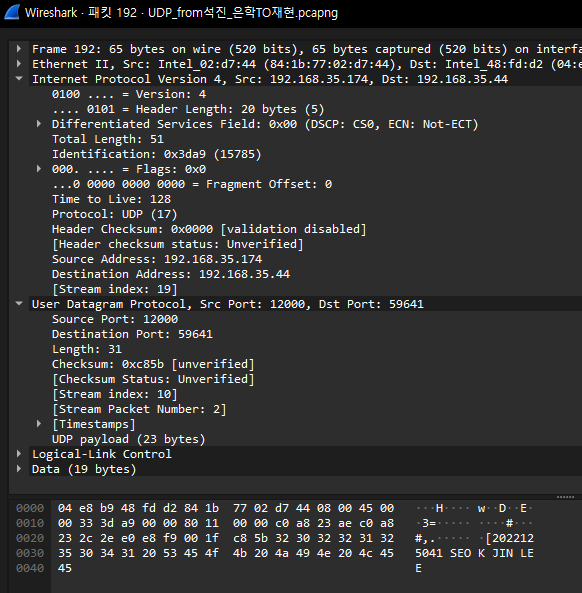
목적지 IP: 192.168.35.174

출발지 포트: 59641

목적지 포트: 12000

전송된 데이터 내용: 2022125041 seok jin lee

서버(조재현) -> 클라이언트(이석진)(UDP Response)



출발지 IP: 192.168.35.174

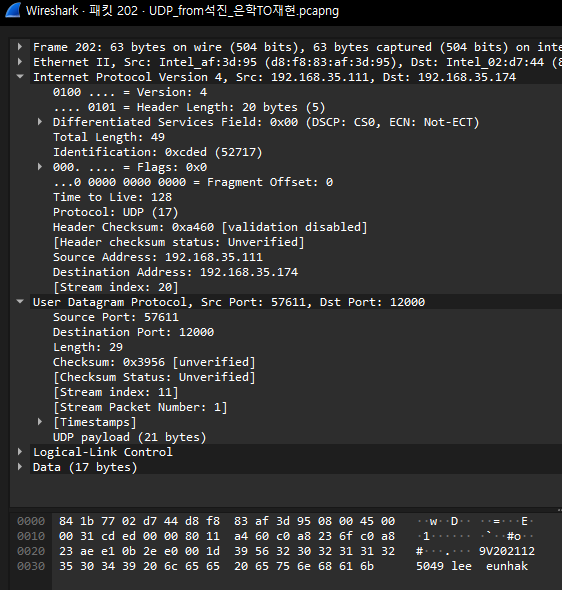
목적지 IP: 192.168.35.44

출발지 포트: 12000

목적지 포트: 59641

응답 데이터: 2022125041 SEOK JIN LEE

클라이언트(이은학) -> 서버(조재현) (UDP Request)



출발지 IP: 192.168.35.111

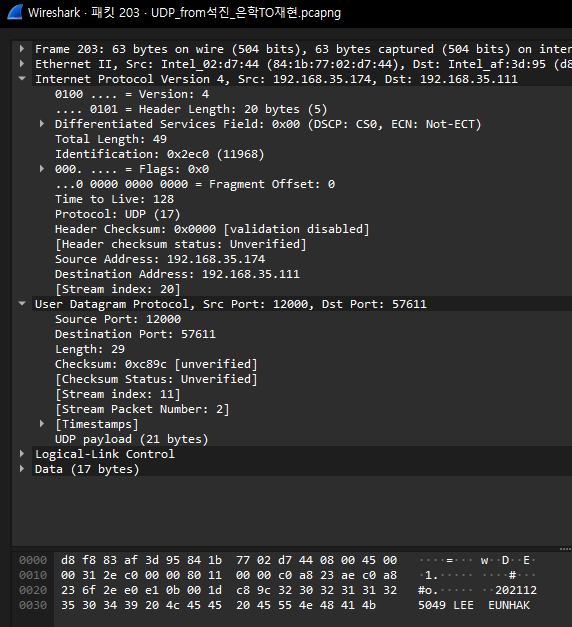
목적지 IP: 192.168.35.174

출발지 포트: 57611

목적지 포트: 12000

전송된 데이터 내용: 2021125049 lee eunhak

서버(조재현) -> 클라이언트(이은학)(UDP Response)



출발지 IP: 192.168.35.174

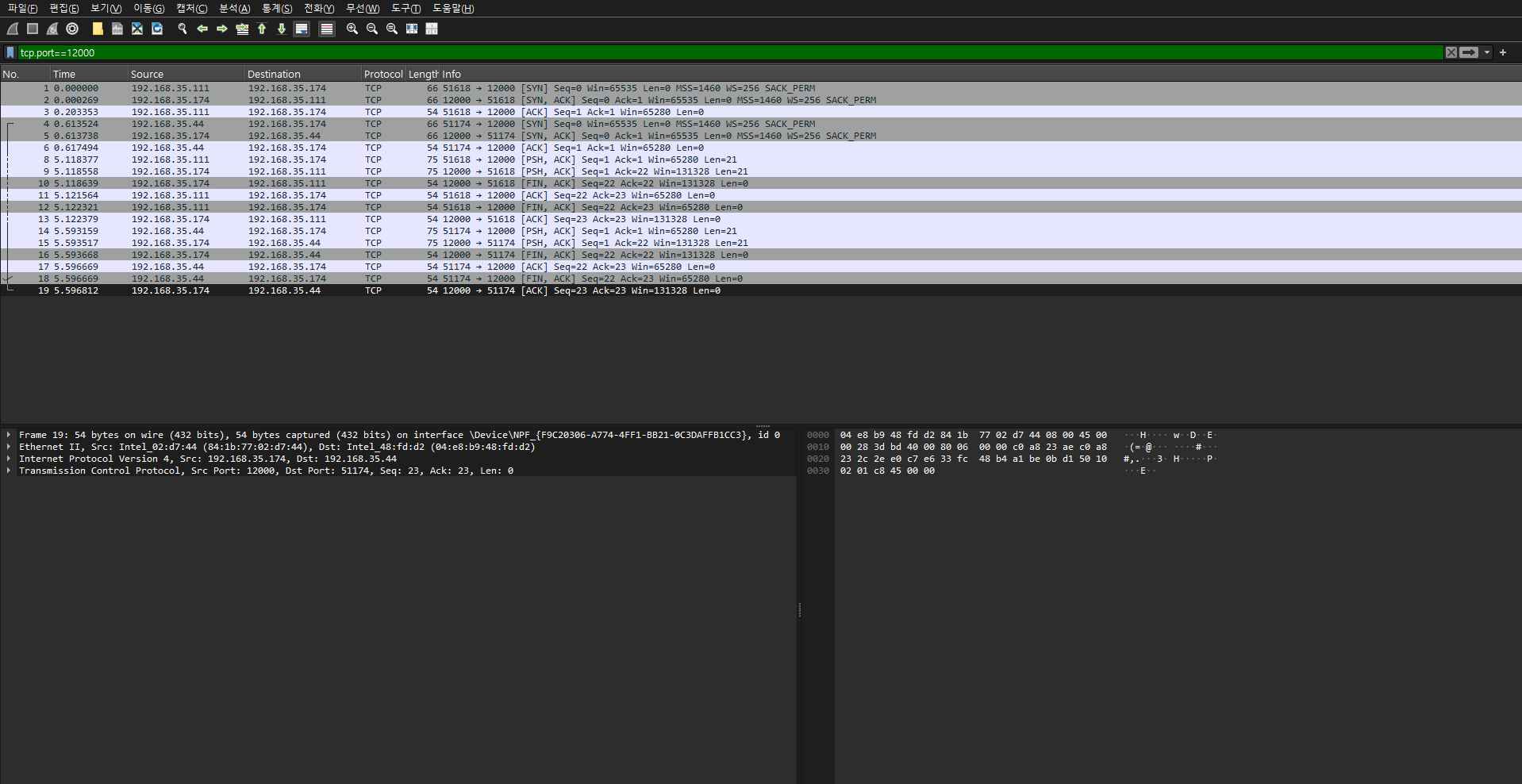
목적지 IP: 192.168.35.111

출발지 포트: 12000

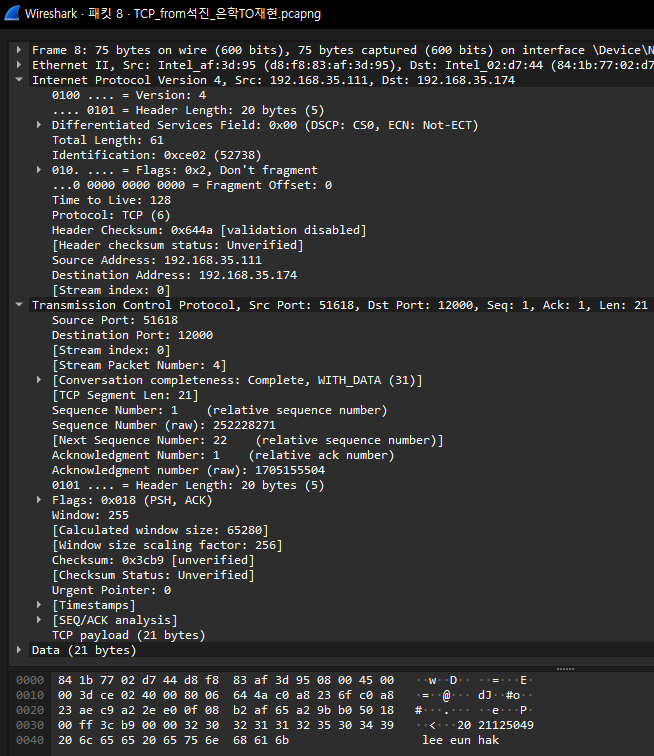
목적지 포트: 57611

응답 데이터: 2021125049 LEE EUNHAK

2. TCP, 클라이언트(이은학, 이석진) <-> 서버(조재현)



클라이언트(이은학) -> 서버(조재현) (TCP Resquest)



출발지 IP: 192.168.35.111

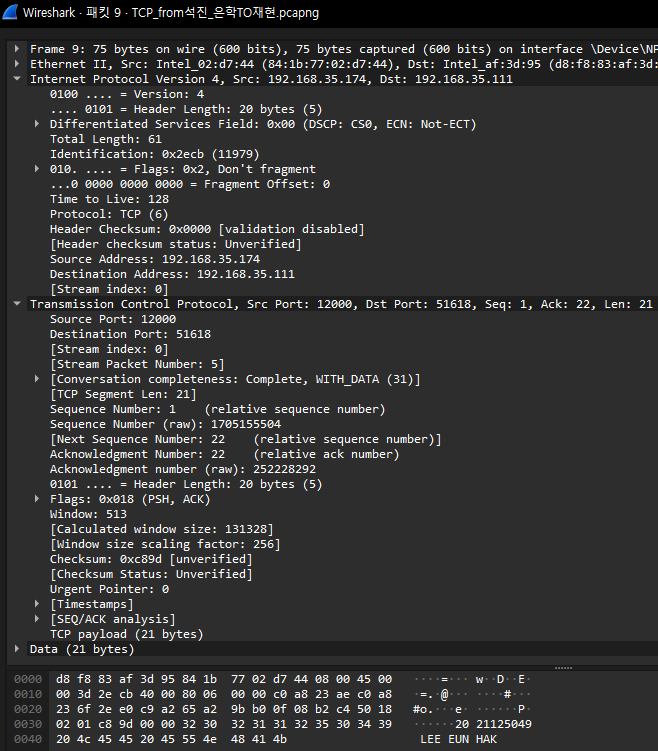
목적지 IP: 192.168.35.174

출발지 포트: 51618

목적지 포트: 12000

전송 데이터 내용: 2021125049 lee eun hak

서버(조재현) -> 클라이언트(이은학) (TCP Response)



출발지 IP: 192.168.35.174

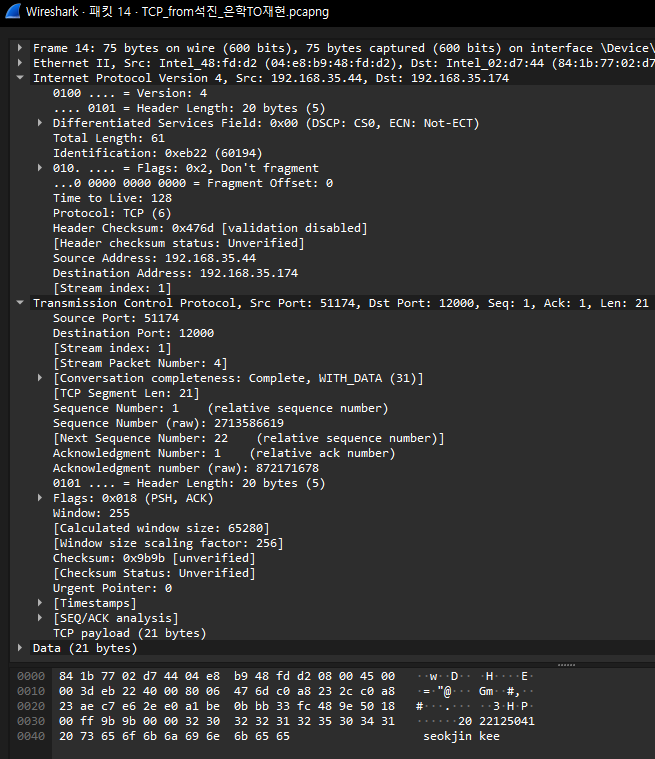
목적지 IP: 192.168.35.111

출발지 포트: 12000

목적지 포트: 51618

응답 데이터: 2021125049 LEE EUN HAK

클라이언트(이석진) -> 서버(조재현) (TCP Resquest)



출발지 IP: 192.168.35.44

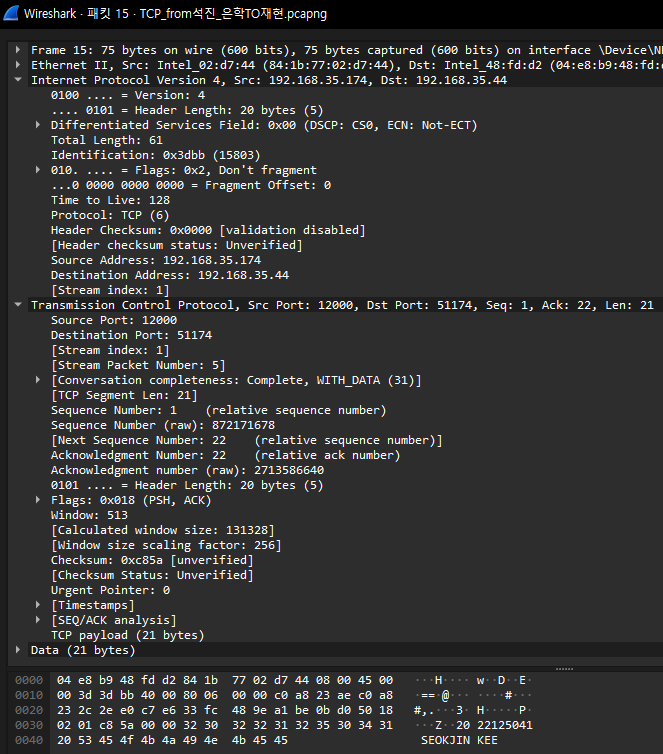
목적지 IP: 192.168.35.174

출발지 포트: 51174

목적지 포트: 12000

전송 데이터 내용: 2022125041 seokjin kee

서버(조재현) -> 클라이언트(이석진) (TCP Response)



출발지 IP: 192.168.35.44

목적지 IP: 192.168.35.111

출발지 포트: 12000

목적지 포트: 51174

응답 데이터: 2022125041 SEOKJIN KEE

**5. 동일 PC에서 server/client 실행 시 캡처 안 되는 이유**

Wireshark는 기본적으로 물리적 네트워크 인터페이스(Wi-Fi, Ethernet 등)를 통해 송수신되는 패킷을 캡처하는 도구이다. 그러나 동일한 PC에서 서버와 클라이언트를 실행할 경우, 데이터는 네트워크 인터페이스를 거치지 않고 OS 내부의 네트워크 스택을 통해 루프백 인터페이스에서 처리 된다. 그러므로 다른 사람과 통신 할 때 패킷을 캡쳐하는 Wi-Fi 혹은 Ethernet 인터페이스에서는 캡쳐가 되지 않는다.

**6. 정리**

UDP와 TCP 프로토콜을 이용한 클라이언트 <-> 서버 통신을 분석하고, Wireshark를 활용하여 패킷을 분석 할 수 있었다. UDP는 연결 지향이 아니고 비교적 빠른 전송이 가능하지만 신뢰성이 보장되지 않는 반면, TCP는 3-way handshake 과정을 통해 신뢰성을 보장하며 데이터가 순서대로 전달됨을 확인하였다.

또한, 포트 포워딩을 설정함으로써 서로 다른 네트워크에 위치한 클라이언트와 서버 간의 통신을 가능하게 만들었으며, 이를 통해 공인 IP와 사설 IP 간의 매핑 과정도 이해할 수 있었다. 동일한 PC에서 서버와 클라이언트를 실행할 경우, 네트워크 인터페이스를 거치지 않는 로컬 루프백 인터페이스를 통해 데이터가 전달되므로 Wireshark에서 패킷이 캡처되지 않는다는 점도 실제로 확인할 수 있었다.

**7. 느낀 점**

초기에는 IP, 포트, 포트 포워딩, 패킷과 같은 개념을 이론적으로만 알고 있어 실제 사용과의 연결이 어려웠다. 하지만 이번 실습을 통해 직접 설정하고 활용하면서 개념들이 점차 명확해졌고, 퍼즐처럼 맞춰지는 경험을 했다.

포트 포워딩의 경우, 참고 자료를 활용하여 비교적 쉽게 설정할 수 있었으나, 서로 다른 네트워크에서 서버에 접속할 때 어떤 IP 주소를 사용해야 하는지 혼란스러웠다. 하지만 공인 IP를 사용해야 한다는 점을 깨닫고 문제를 해결하면서 네트워크 주소 체계에 대한 이해가 더욱 깊어졌다.

수업 시간에 배운 "IP 주소는 집 주소, 포트 번호는 수취인과 비슷한 개념"이라는 비유가 실습을 통해 더욱 실감 나게 다가왔다. 이번 실험을 통해 네트워크 개념을 실제 환경에서 적용해 보고, 이론과 실습의 연관성을 깊이 이해할 수 있는 의미 있는 경험이었다.