**컴퓨터네트워킹 과제**

**PRG#1**

**강좌 명: 컴퓨터네트워킹**

**교수님: 안종석 교수님**

**학과: 컴퓨터공학과**

**학번: 2017112138**

**이름: 정여준**

**실습 수행**

1. wireshark 설치

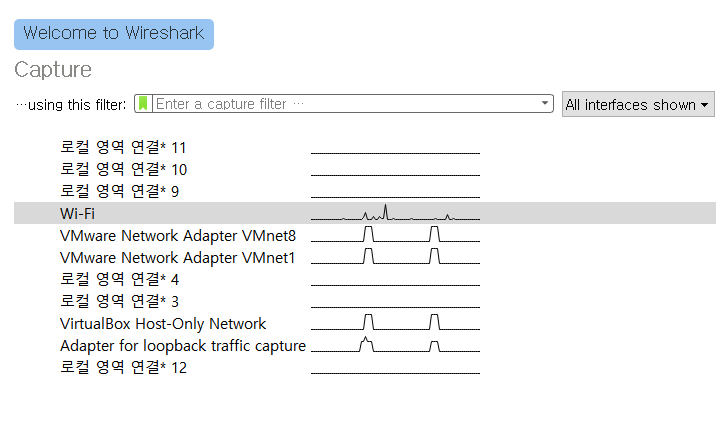
2. 패킷 통신

동국대학교 이클래스의 IP 주소를 찾는다.

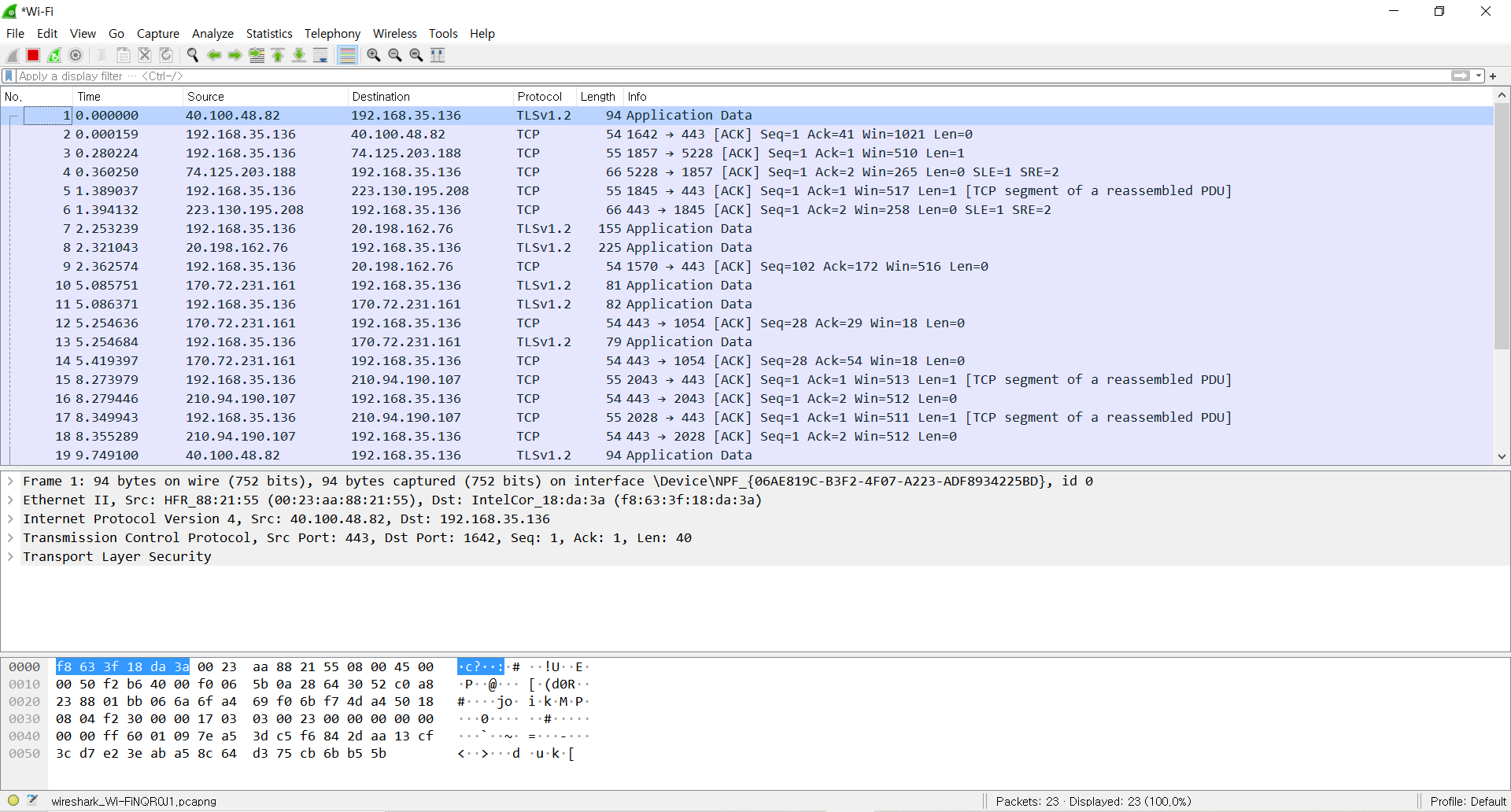
cmd창에 nslookup <https://eclass.dongguk.edu/> 명령어를 통해서 동국대학교 이클래스의 IP주소를 찾는다.



wireshark를 실행한다.



Wi-Fi를 눌러서 패킷들의 캡쳐를 시작한다.



와이파이 인터페이스에서 오고 가는 패킷들을 찾아주는 것이다.

위에서 나오는 정보들은 다음과 같은 정보들이다.

No.: 패킷을 수집한 순서

Time: 패킷이 수집된 시간

Source: 패킷을 보낸 주소

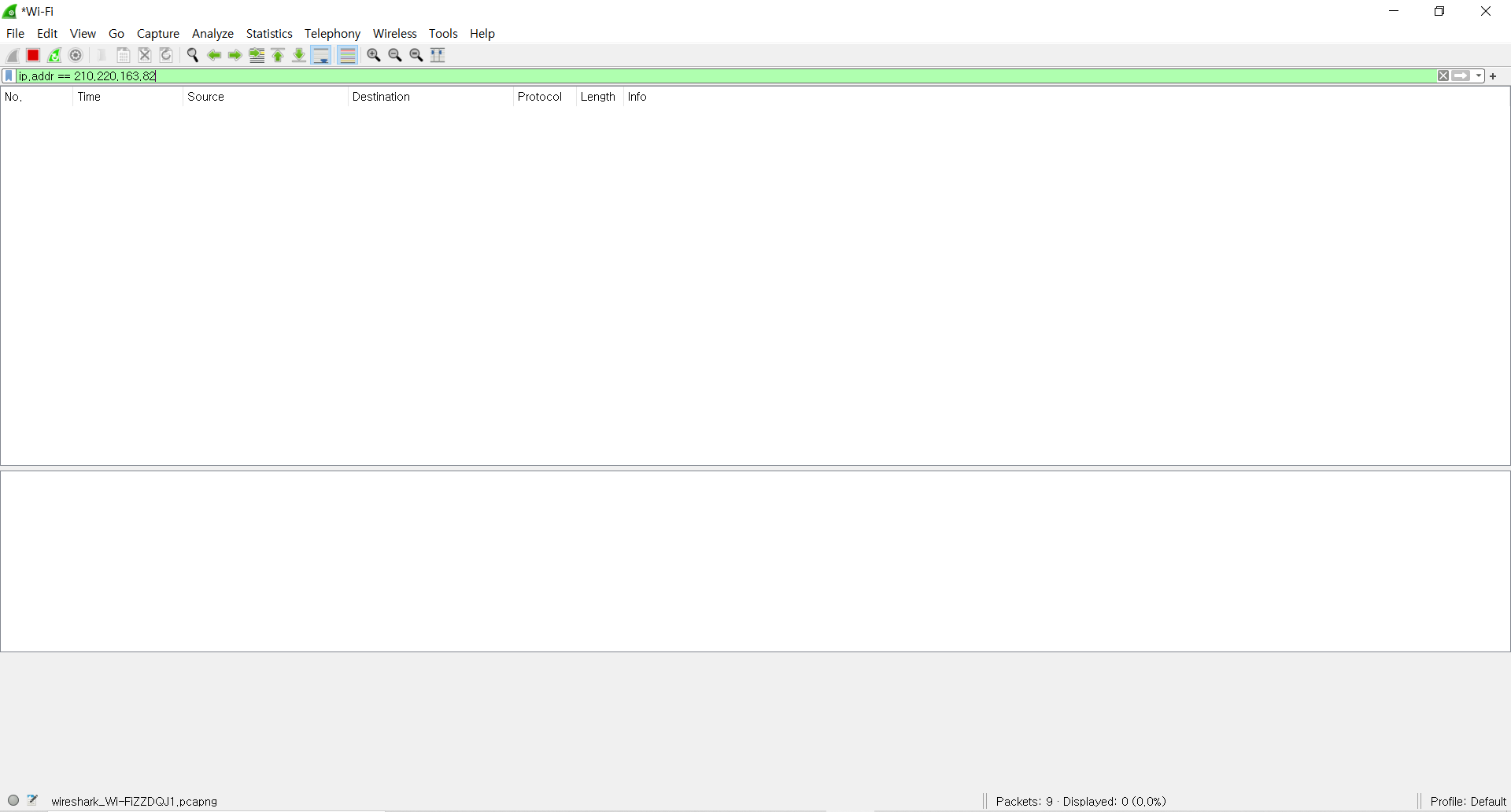
Destination: 패킷 도착 주소

Protocol: 프로토콜 정보

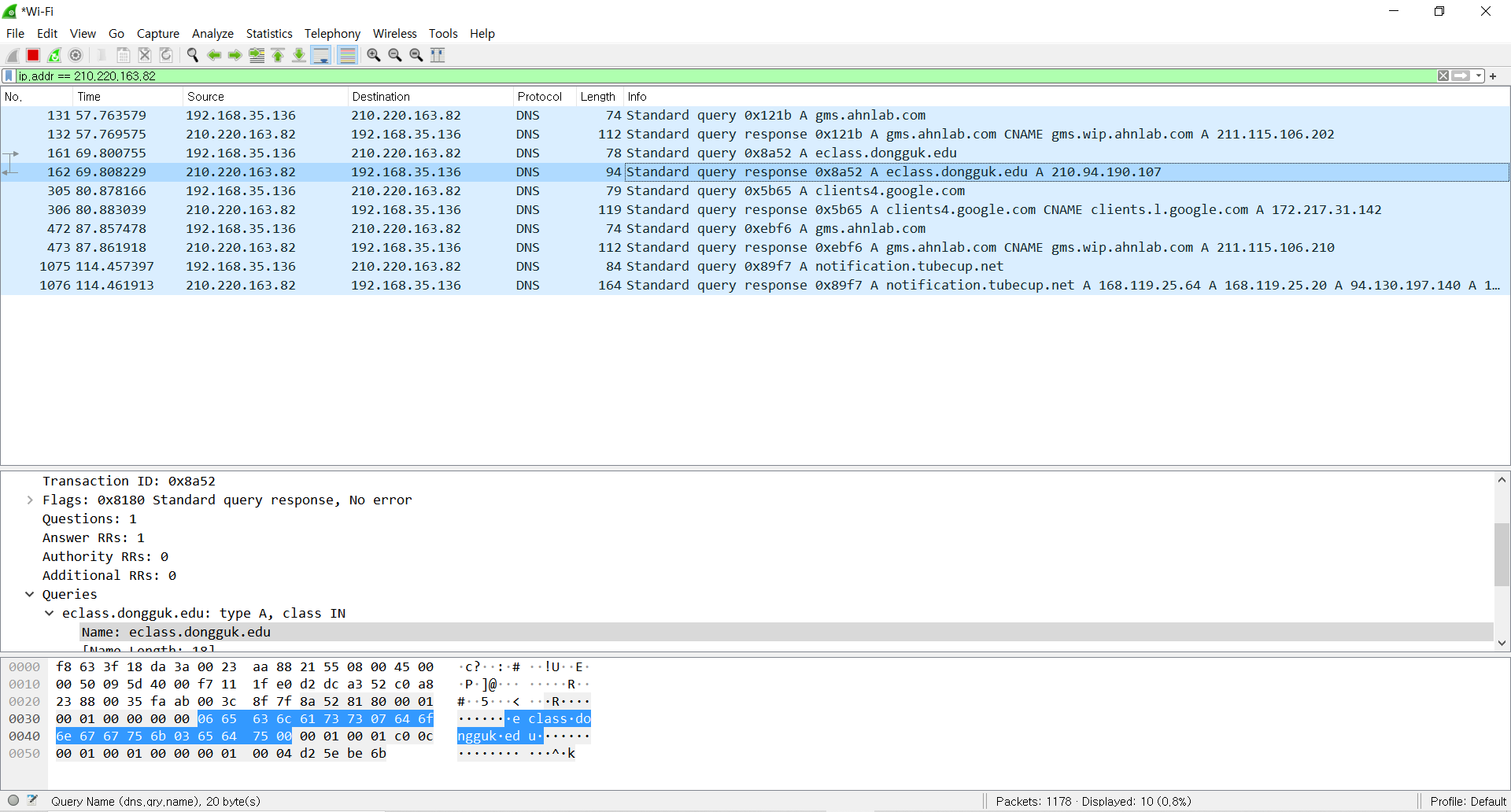
Length: 패킷의 길이

info: 패킷 정보

이제 필터링을 통해서 동국대학교 이클래스와 연관된 IP 주소만 나올 수 있도록 지정해준다. 지정하는 명령어는 ip.addr == 주소로 하면 된다.



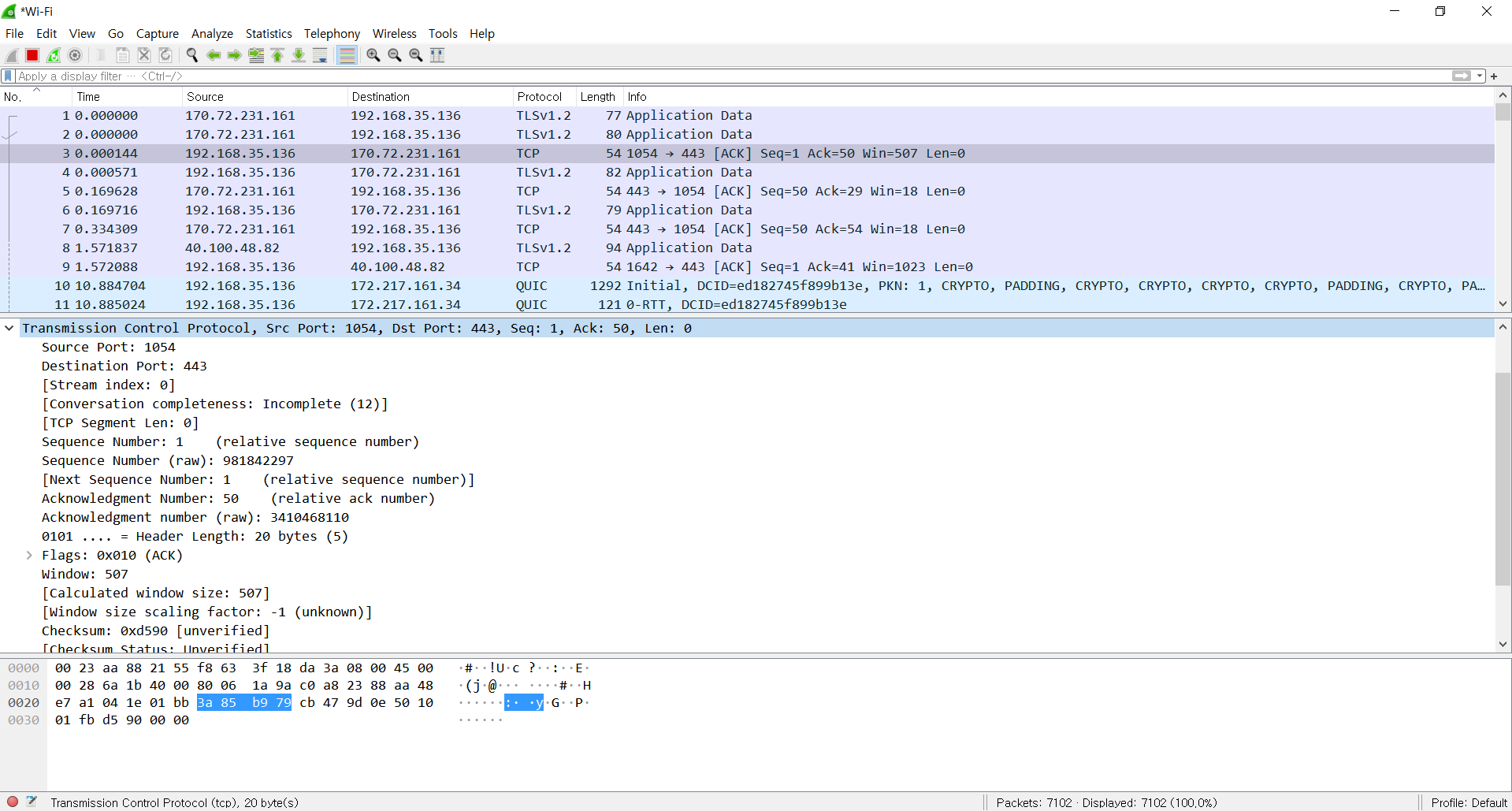
현재 이클래스 웹사이트에 접속하지 않았기 때문에 아무것도 뜨지 않는 것을 볼 수 있다. 그럼 이제 이클래스에 접속한다.



나의 노트북 주소인 192.168.35.136과 동국대학교 이클래스의 주소인 210.220.163.82 사이의 패킷이 통신하는 것을 확인할 수 있다.

3. 표시되는 결과 분석

Protocol이 TCP인 것을 선택하면 TCP에 관한 정보가 나오는 것을 확인할 수 있다.



위의 패킷에서 표시되는 결과를 분석해본다.

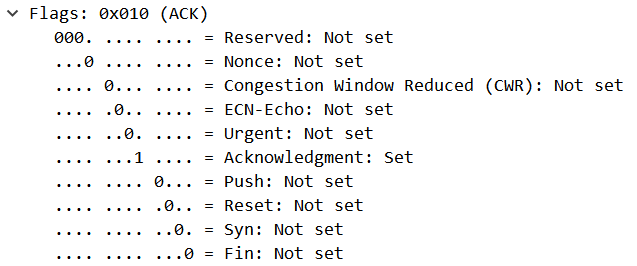
일단 Source Port는 발신지 포트이다. 즉 위의 패킷의 발진지 포트는 1054인 것을 확인할 수 있다.

Destination Port는 도착지 포트로 위의 패킷의 도착지 포트는 443인 것을 확인할 수 있다.

Sequence number는 순차번호필드로 고유한 번호를 가지며 이 값으로 TCP 세그먼트에 대한 식별 값을 제공하며, 통신 스트림 일부가 분실되면 확인을 위해 수신자를 사용 가능하게 한다. 이 순차번호는 패킷에 포함되어 있는 데이터만큼 증가하게 된다.

Acknowledgment Number는 확인 응답 번호 필드로 다음번에 기대되는 순차번호를 표시한다.

Header Length는 데이터 오프셋 필드로 TCP 헤더의 길이를 정의한다. 길이는 4byte씩 증가된다. TCP 헤더의 길이가 다양하게 변화시킬 필요가 있으므로 이 필드가 필요하게 된다.



플래그에 대한 설명

Urgent는 긴급 비트로 만약 이 비트가 1로 설정된 경우 긴급 포인터 필드로 정의되는 특정 위치에서 시작하는 패킷의 데이터를 알기 위해 발신자가 원하는 수신자를 나타낸다.

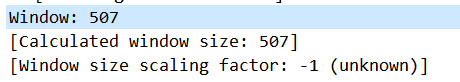
Acknowledgment는 확인 응답 비트로 이 비트가 설정되어 있으면 이 패킷은 확인 응답이라는 것을 나타내는 플래그이다.

Push는 TCP 세그먼트가 발신자나 수신자의 측면에서 버퍼에 유지되면 안된다는 것을 표시한다.

Reset은 RST 비트 설정에 대한 TCP 패킷은 TCP 연결을 종료, 즉 접속을 강제로 종료한다. 이 패킷은 이상 종료 시 사용된다.

SYN는 동기화 비트로 송신측과 수신측의 일련번호를 확인할 때 사용되고 이 비트가 1이면 이 패킷은 TCP 핸드셰이크 프로세스의 SYN 단계라는 뜻이다.

FIN은 Finish 비트로 프로세스가 완료됐고 데이터 스트림이 전송됐다는 것을 의미한다.

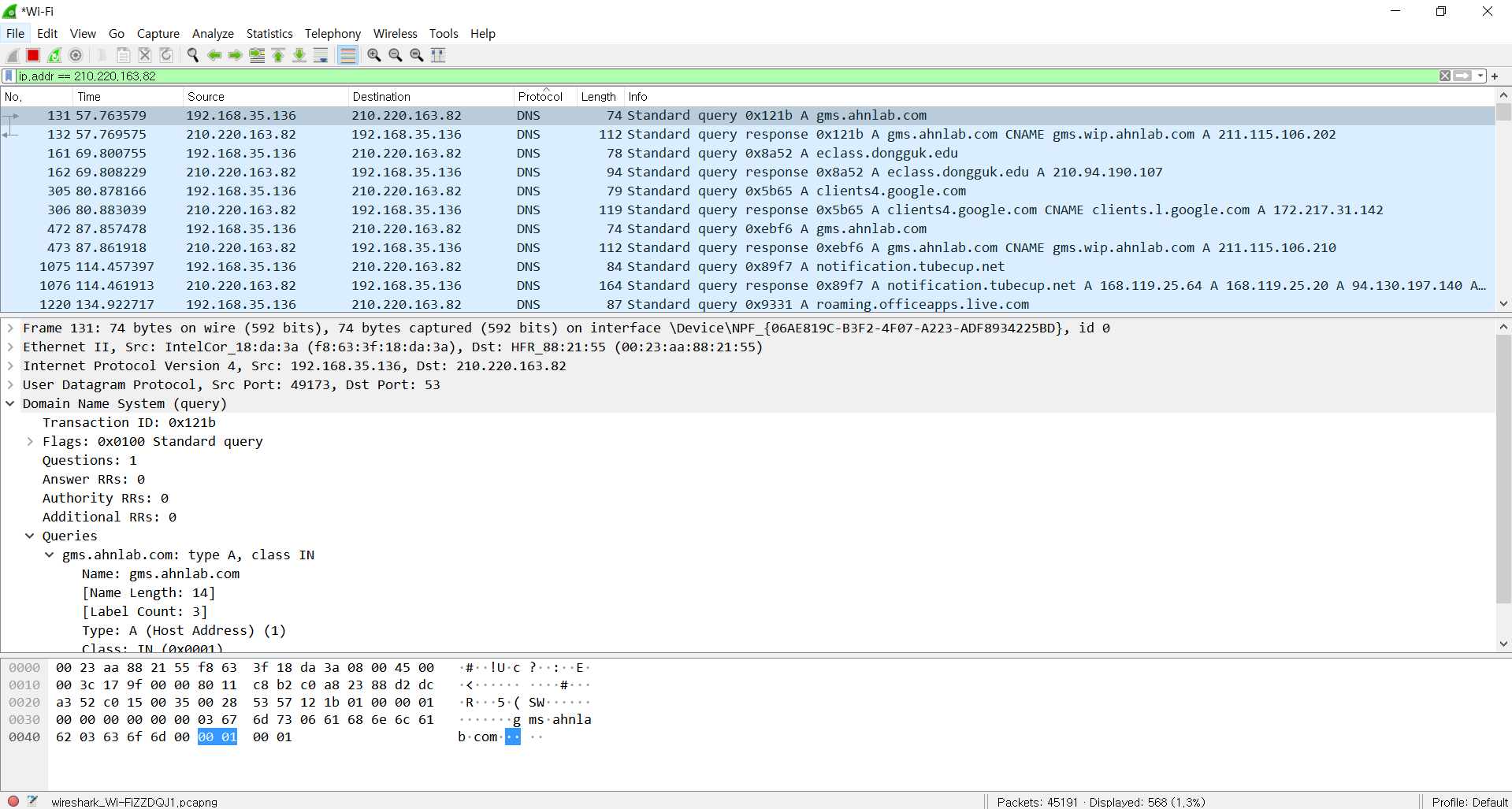


window 필드는 TCP 수신 버퍼를 바이트 크기로 표시한다.



checksum 필드는 TCP 헤더와 데이터의 내용 뿐만 아니라 IP 헤더로부터 파생된 의사 헤더에 대한 내용을 수행한다.

이번에는 Protocol이 DNS인 것을 확인해본다.



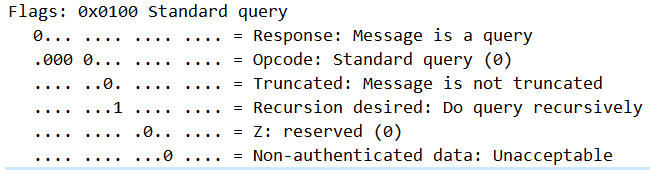
위의 그림을 보면 DNS가 4개의 기본 section으로 구성되어 있는 것을 볼 수 있다.

1. Question 2. Answer 3. Authority 4. Additional

이제 DNS 패킷을 분석해본다.

Transaction ID는 DNS 쿼리와 응답에 연관되는데 사용자는 이 필드에서 DNS에 관련된 모든 것을 보기 위한 값을 필터링 할 수 있다.

Flags는 쿼리 특성을 정의하는 수많은 필드로 구성되어 있다.

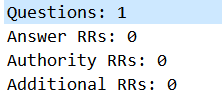


Response는 응답비트로 요청(0)인지 응답(1)인지 표시한다. 위의 패킷은 0이므로 패킷이 요청한 것임을 알 수 있다.

Opcode는 쿼리의 유형을 지정하고 일반적으로 일반적인 요청에 대해 0000을 포함한다.

Truncation은 응답이 길어서 잘렸는지에 대해서 알려주고 위의 패킷을 보면 잘리지 않았다 라고 나오는 것을 볼 수 있다.

Z는 0으로 설정된다. Non-authenticated data는 데이터에 권한이 있는지를 보는 필드로 위 패킷에서는 0으로 설정되어 받아들일 수 없다고 나온다.

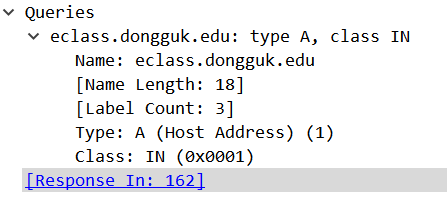


Questions는 질문의 숫자를 표시하고 일반적으로 한 패킷당 1개의 질문을 볼 수 있다.

Answer RRs는 Answer RRs의 수를 표시한다.

Authority RRs는 Authority RRs 응답 수를 표시한다.

Additional RRs는 Additional RRs 응답 수를 표시한다.



Name은 결정중인 이름을 포함한다. 형식은 이름에서 영문자 바이트의 숫자를 표시하기 위해 숫자 구분문자를 이용하는 가변길이다.

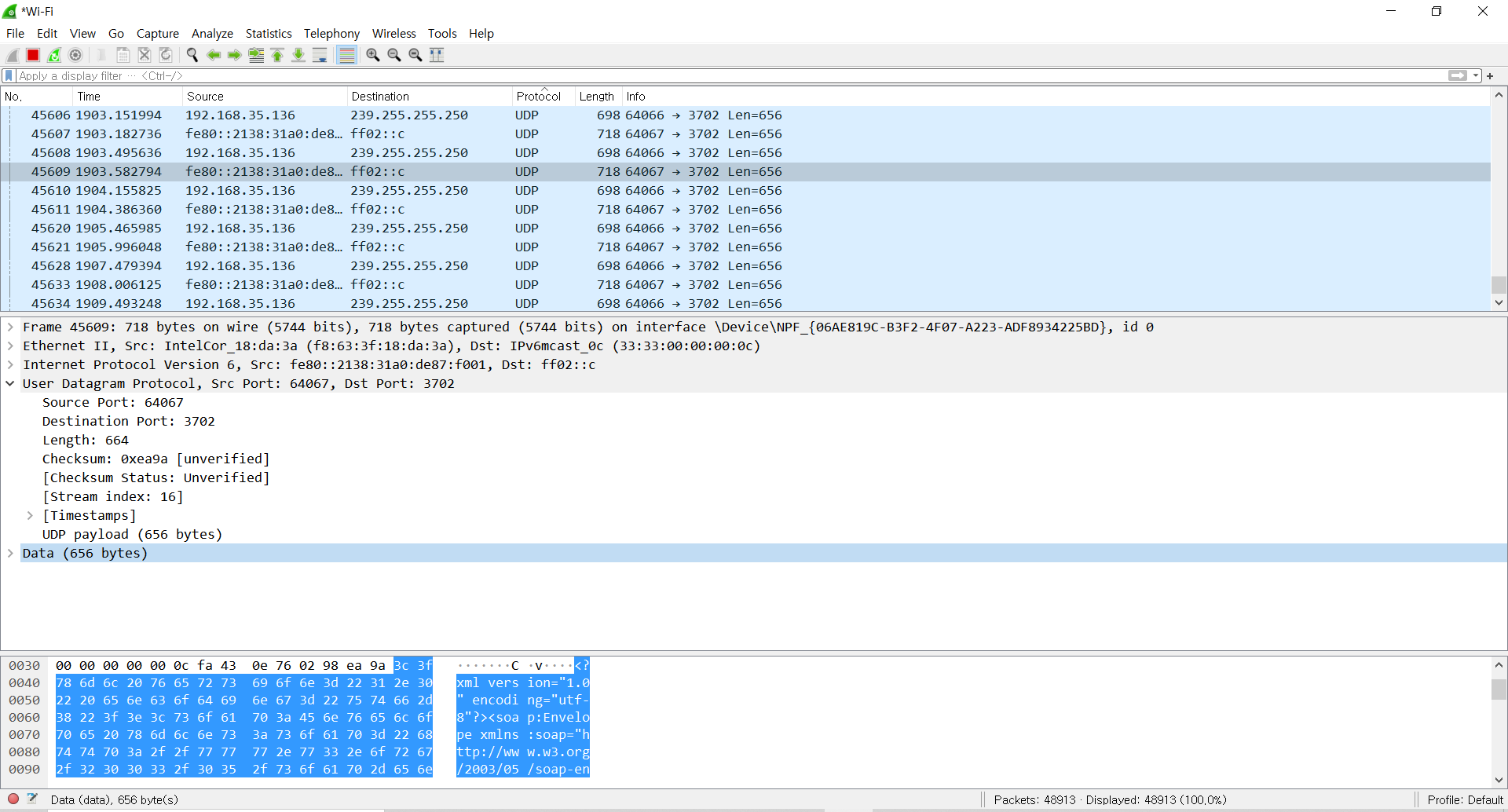
Type은 쿼리의 유형을 나타내는 필드로 현재는 A로 호스트 주소를 나타내게 된다.

유형은 다음과 같다.



Class는 TCP/IP 통신에 대한 인터넷 클래스 주소를 표시하기 위해 1(0x0001)로 설정된다.

다음으로는 Protocol이 UDP인 것에 대해서 알아본다.



Source Port는 목적지 포트 빌드로 응답 패킷에서 수신중인 포트를 열기 위해서 주로 사용되며 프로토콜을 정의하기 위한 목적으로 사용되며 현재는 64067 포트를 사용한다.

Destination Port는 발신지 포트 빌드로 이 필드는 목적지 애플리케이션이나 프로세스를 정의하고 일부 경우 발신지와 목적지 포트 번호들은 클라이언트나 서버 프로세스와 같다. 현재는 목적지 포트와 다른 3702를 사용한다.

Length는 길이 필드로 UDP 헤더에서 유효한 데이터의 끝까지 패킷의 길이를 정의하며, 현재 화면에서 664를 표시한다.

Checksum은 checksum에 대한 정보를 나타내며 가끔 사용자는 checksum 필드가 모두 0으로 설정된 것을 볼 수 있는데 이는 checksum이 인증되지 않았다는 의미이다.