Jargons

2016314786 김호진

Vocabularies and Acronyms

Find meanings of following words in network context.

1. **ISP -** Internet Service Provider의 약어로, 기업체나 개인들에게 인터넷에 접속하는 수단을 제공하는 주체를 말합니다.

2. **NAT –** Network Address Translation의 약어로, IP 패킷의 TCP/UDP 포트 숫자와 소스 및 목적지의 IP 주소 등을 기록하면서 Router를 통해 네트워크 트래픽을 주고받는 기술을 말합니다. 전역적으로 고유한 IP 주소의 필요성을 줄이기 위한 메커니즘으로 NAT를 이용하면 전역적으로 고유하지 않은 주소를 가진 조직체가 그 주소를 전역적으로 Routing할 수 있는 주소 공간으로 변환해 인터넷에 연결할 수 있습니다.

3. **DHCP** – Dynamic Host Configuration Protocol의 약어로, 호스트 IP 구성 관리를 단순화하는 IP 표준입니다. 동적 호스트 구성 프로토콜 표준에서는 DHCP 서버를 이용하여 IP 주소 및 관련된 기타 구성 세부 정보를 네트워크의 DHCP 사용 클라이언트에게 동적으로 할당하는 메커니즘을 제공합니다.

4. **Congestion** – 매우 높은 부하상태에서 발생하게 되며, 네트워크 또는 장비가 처리할 용량이 초과했음을 의미합니다. 이러한 상태는 급속히 지연(latency)을 증가시키고 그 상태가 지속될 경우에는 데이터의 손실을 야기합니다.

5. **DNS** - Domain Name System의 약어로, 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 하기 위해 개발되었습니다. 특정 컴퓨터(또는 네트워크로 연결된 임의의 장치)의 주소를 찾기 위해, 사람이 이해하기 쉬운 도메인 이름을 숫자로 된 식별 번호(IP 주소)로 변환해 주는 네트워킹 시스템입니다.

6. **HTTP** - Hypertext Transfer Protocol의 약어로, 클라이언트와 서버 사이에 이루어지는 TCP/IP 기반 요청/응답 프로토콜입니다. 웹에서만 사용하는 프로토콜로써 데이터가 전송 중 파괴되거나 중복되거나 왜곡되는 것을 방지할 수 있습니다.

   HTTPS - Hyper Text Transfer Protocol over Secure socket layer의 약어로, HTTP의 보안이 강화된 버전입니다. HTTPS는 소켓 통신에서 일반 텍스트를 이용하는 대신 SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화하여 데이터의 적절한 보호를 보장합니다.

7. **NIC -** Network Interface Card의 약어로, PC나 서버 등의 컴퓨터를 네트워크에 연결시키기 위한 장치를 말합니다. PC와 NIC 사이에서 논리적으로 연결하는 소프트웨어가 있어 PC에서 NIC로 정보를 보내면 버퍼에 저장한 다음 네트워크에 맞는 시리얼 형태로 보내는 역할을 합니다. 네트워크 별로 이더넷, 토큰링, 고속 이더넷, 기가비트 이더넷, 비동기 전송 방식(ATM) 등 다양한 카드가 사용됩니다.

8. **MAC -** Media Access Control의 약어로, 자료 전송 프로토콜의 하부 계층이며 일곱 계층의 OSI 모델에 규정된 데이터 링크 계층의 일부입니다. MAC 서브 레이어는 공유 미디어 액세스 문제를 처리합니다.

9. **LAN -** Local Area Network의 약어로, 네트워크 매체를 이용하여 집, 사무실, 학교 등의 가까운 지역을 한데 묶는 컴퓨터 네트워크입니다.

   MAN – Metropolitan-Area Network의 약어로, 한 대도시 지역 전체 또는 캠퍼스에 구축되어 있는 네트워크를 말합니다. 일반적으로 MAN의 가동 영역은 지리적으로 LAN보다는 크지만, WAN보다는 작습니다.

   WAN - Wide Area Network의 약어로, 국가나 대륙과 같이 넓은 지리적 거리/장소를 넘나드는 네트워크입니다. 넓은 지역에 설치된 컴퓨터들 간의 정보와 자원을 공유하기에 적합합니다.

10. **SSL –** Secure Socket Layer의 약어로, 컴퓨터 네트워크에 통신 보안을 제공하기 위해 설계된 암호 규약입니다. 인터넷과 같이 TCP/IP 네트워크를 사용하는 통신에 적용되며, 통신 과정에서 전송계층 종단간 보안과 데이터 무결성을 확보해줍니다. 웹 브라우징, 전자 메일, VoIP 같은 응용 부분에서 적용되고 있습니다.

    TLS - Transport Layer Security의 약어로, SSL이 발전 및 표준화되면서 바뀐 이름입니다. TLS는 클라이언트/서버 응용 프로그램이 네트워크로 통신을 하는 과정에서 도청, 간섭, 위조를 방지하기 위해서 설계되었습니다. 암호화를 통해서 최종단의 인증, 통신 기밀성을 유지시켜줍니다.

11. **Stream-oriented –** 클라이언트가 데이터를 연속 스트림 형태로 보낼 수 있는 전송 서비스의 한 유형으로, 이 방식의 전송 서비스에서는 모든 데이터가 보낸 순서대로 수신 측에 전달되며 복제되는 부분은 존재하지 않습니다.

    Chunk-oriented - 일반적으로 대용량 데이터를 처리하는 배치 프로세스의 특성상 대상 데이터들을 하나의 transaction으로 처리하기에는 어려움이 있기 때문에 대상 데이터를 임의의 Chunk 단위로 동작을 수행하는 것을 말합니다.

12. **E2E communication -** 일련의 메시지를 Unreliable한 communication을 통해 하나의 processor(sender)로부터 또 다른 processor(receiver)로 보내는 것을 말합니다.

***E2E principle –** 일반 네트워크에서 응용프로그램에 특화된 기능은 중앙 노드가 아닌 종단에 있어야 한다는 원칙입니다. 이 원칙에 따라 설계된 네트워크에서 응용 프로그램 별 기능은 네트워크를 설정하기 위해 존재하는 Gateway 및 Router 등의 중간 노드가 아닌 네트워크의 통신 끝 노드에 있어야 합니다. 이를 통해 부가적인 기능이 네트워크의 핵심 활동을 방해하거나 그 활동에 필요한 자원을 끌어가지 않으며, 네트워크 전반을 유지 및 보수하거나 업데이트 하는 과정이 복잡해지지 않습니다.

13. **AS -** Autonomous System의 약어로, 동일한 Routing 정책으로 하나의 관리자에 의하여 운용 및 관리되는 Router와 부분 통신망의 집합체를 말합니다. 인터넷은 이러한 자율 시스템들의 집합체라고 볼 수 있습니다.

14. **Gateway –** 2개 이상의 다른 종류 또는 같은 종류의 통신망을 상호 접속하여 통신망 간 정보를 주고받을 수 있게 하는 기능 단위 또는 장치를 말합니다. 통신망에는 근거리 통신망(LAN), 공중 데이터망(PDN), 공중 교환 전화망(PSTN) 등이 포함됩니다. Gateway는 프로토콜이 다른 복수의 통신망 간의 프로토콜을 변환하여 정보를 주고받습니다.

    Router – 네트워크 간의 연결점에서 패킷에 담긴 정보를 분석하여 적절한 통신 경로를 선택하고 전달해 주는 장치를 말합니다. Router는 서로 다른 네트워크를 인식하고, 가장 효율적인 경로를 선택하며, 흐름을 제어하고, 네트워크 내부에 여러 보조 네트워크를 구성하는 등의 다양한 네트워크 관리 기능을 수행합니다.

    Switch – 네트워크 스위치(network switch)는 처리 가능한 패킷의 숫자가 큰 것으로, 네트워크 단위들을 연결하는 통신 장비입니다. Hub처럼 각 컴퓨터에서 주고받는 데이터가 다른 모든 컴퓨터에 전송되는 것이 아니라, 데이터를 필요로 하는 컴퓨터에만 전송되기 때문에 Switch의 사용 목적은 Hub와 유사하지만, 훨씬 향상된 네트워크 속도를 제공합니다. 또한 Hub와 다르게 병목 현상이 쉽게 발생하지 않습니다. 하지만 Switch의 처리용량을 초과하는 데이터 흐름에 대해서는 취약하므로 커다란 네트워크의 경우 VLAN Switch나 Router 등을 사용해야 합니다.

    Hub - 구내 정보 통신망(LAN) 전송 선로의 중심에 위치하여, 바퀴살 모양으로 단말 장치를 접속하는 형태의 중계 장치를 말합니다. 한 대의 Hub를 중심으로 여러 대의 컴퓨터와 네트워크 장비가 서로 연결되며, 같은 Hub에 연결된 컴퓨터와 네트워크 장비는 상호 간의 통신을 할 수 있습니다.

15. **Ethernet –** 컴퓨터 네트워크 기술의 하나로, 일반적으로 LAN, MAN 및 WAN에서 가장 많이 활용되는 기술 규격입니다. Ethernet Network는 CSMA/CD를 사용하며 10Mbps의 속도로 다양한 종류의 케이블을 통해서 가동됩니다. 대부분 IEEE 802.3 규약으로 표준화되었으며, 현재 가장 널리 사용되고 있습니다.

CSMA-CD - Carrier Sense Multiple Access/Collision Detect의 약어로, 컴퓨터 네트워크 분야에서 성능개선을 위해 CSMA를 일정 부분 수정한 방식입니다. 각 노드는 데이터 송신 전에 반송파를 이용해 다른 노드가 채널을 사용하고 있는지 감지하고 만약 채널이 비어 있으면 데이터를 전송합니다. 전송 시점과 동시에 다른 노드에서 데이터를 전송하게 되면 충돌이 탐지되며 해당 노드는 즉시 전송을 중단하고 임의 시간 동안 대기한 후 데이터를 재전송합니다. 전송 선로를 분할하지 않고 각 단말을 공동으로 사용하며, 언제 어느 단말이 해당하는 전송 선로를 사용하는지는 각 단말이 정해진 규칙에 따라 송신권의 확보를 자발적으로 판정합니다. CSMA/CD 액세스는 Ethernet과 IEEE 802.3에 의해 사용됩니다.

Getting familiar with Wireshark

1. Preparation

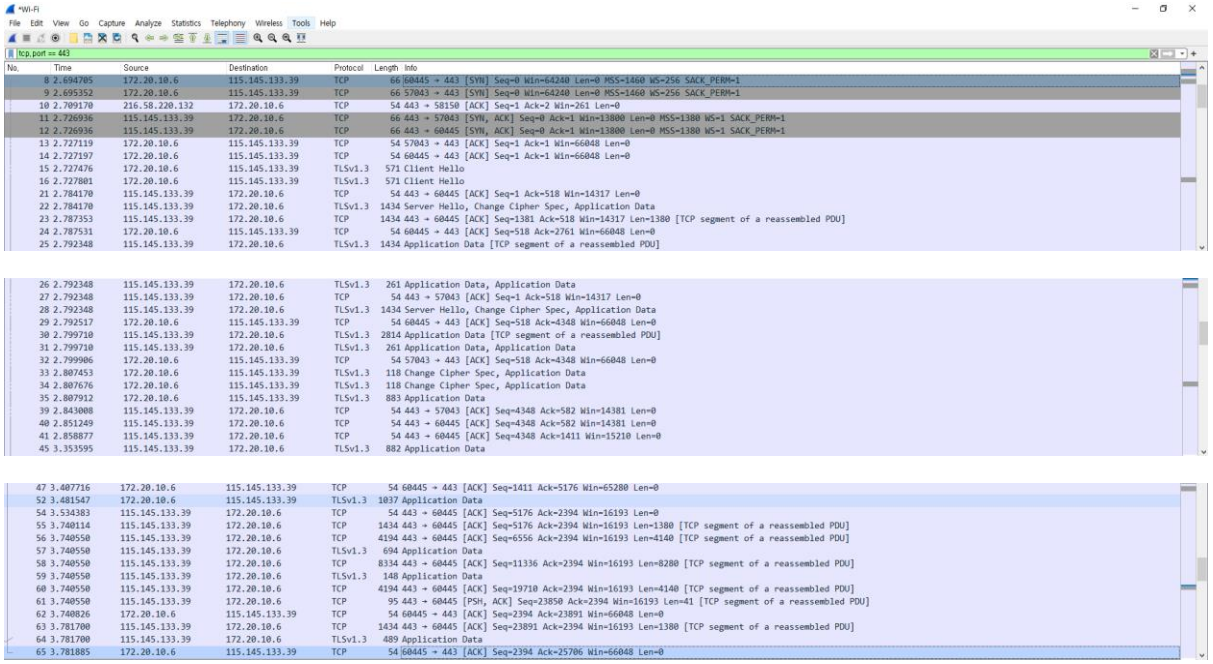
- **Wireshark is the most popular network protocol analyzer. It helps you to see what data is inside of packets in the network.**
- **Download and install Wireshark at `http://www.wireshark.org`.**
- **Learn how to use the tool by watching .**

- `https://www.youtube.com/watch?v=jvuiI1Leg6w&t=802s`
- `https://www.youtube.com/watch?v=0ELCdQaHELs`

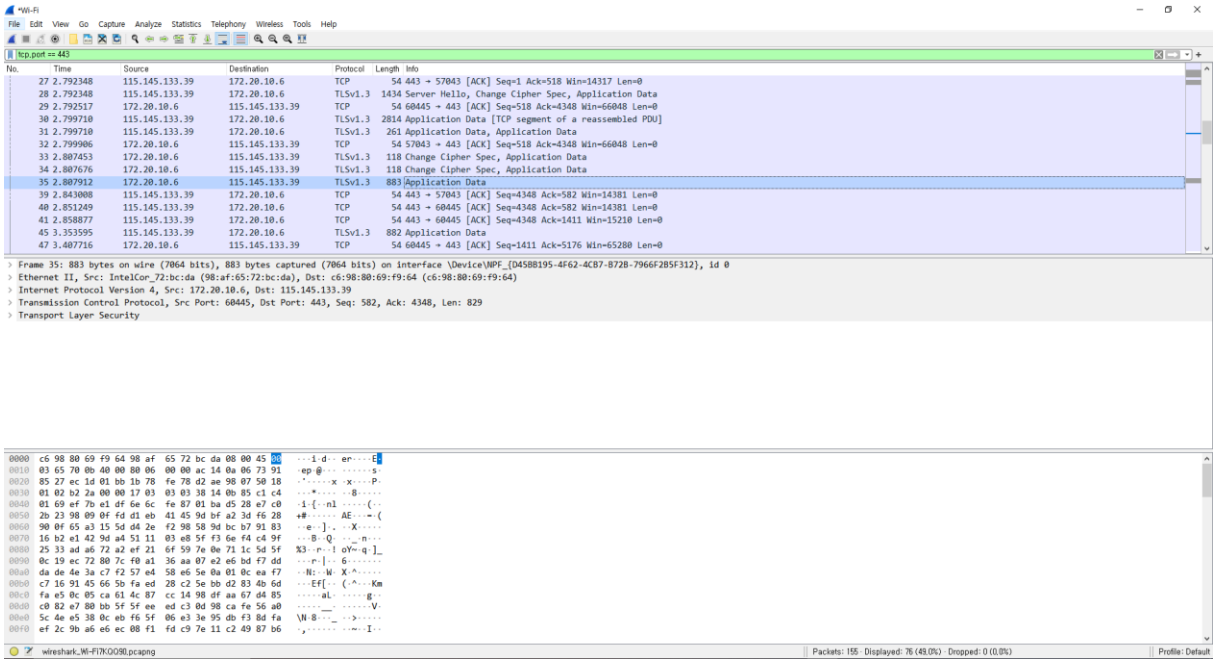
- **Read a tutorial at https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/**
- **Close all opened running applications**
- **Browsers, email program and other applications that typically send data to the Internet**
- **This will minimize the amount of traffic you**

2. Execution 1

- **Open Wireshark program and open web browser**
- **Capture packets to record HTTP traffics into a file using Wireshark while you are browsing `www.skku.edu` using filter "tcp port 443".**
- **Once the page download finishes stop the record. Make sure that you filter out packets only for carrying HTTPS traffic.**
- **Answer to the following questions.**



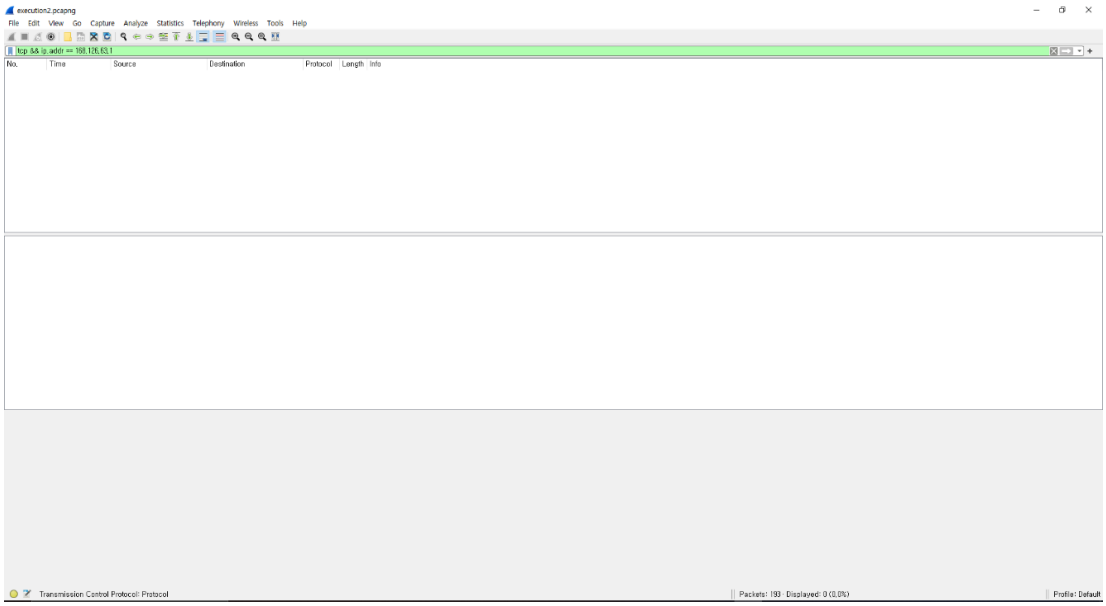
- **How long does it take to download the page?**
  첫번째 packet 이 기록된 시간이 2.694705s 이고 마지막 packet 이 기록된 시간이 3.781885s 이므로 페이지가 다운로드 되는데 1.08718s 가 소요되었음을 알 수 있습니다.
- **How many packets in the record?**
  기록을 살펴보면 8~9, 11~16, 21~35, 39~41, 45, 47, 52, 54~65 번 packet 이 Laptop(172.20.10.6)과 www.skku.edu(115.145.133.39) 사이에서 통신을 하고 있으므로 총 41 개의 packets 이 존재함을 알 수 있습니다.



- **Pick a packet carrying a payload (data). In the middle window of Wireshark, how many protocols do you see and what are they?**
  임의로 35 번 packet 을 선택한 뒤 확인해보면, 총 4 개의 Protocol (Ethernet Protocol, Internet Protocol, Transmission Control Protocol, Transport Layer Security Protocol)을 볼 수 있습니다.
- **What is the version of TLS?**
  TLS 의 버전은 1.3 입니다.
- **In the IP protocol, what are source and destination addresses?**
  Source address - 172.20.10.6
  Destination address - 115.145.133.39
- **In the TCP protocol, what are source and destination ports?**
  Source port - 60445
  Destination port - 443
- **In the second layer protocol, what are source and destination MAC addresses?**
  Source MAC address - IntelCor_72:bc:da (98:af:65:72:bc:da)
  Destination MAC address - c6:98:80:69:f9:64 (c6:98:80:69:f9:64)
- **What is the application protocol? It should be HTTPS. How come does Wireshark not display HTTPS? Why can't you see the data carried in the TLS?**
  HTTPS 는 소켓 통신에서 일반 텍스트를 이용하는 대신 SSL 이나 TLS 를 통해 세션 데이터를 암호화하여 데이터를 보호하기 때문에 Wireshark 를 통해 application protocol 인 HTTPS 를 볼 수 없는 것입니다. 위 사진의 35 번 packet 을 살펴보면, Transport Layer Security 가 암호화하고 있음을 확인할 수 있습니다.

3. Execution 2

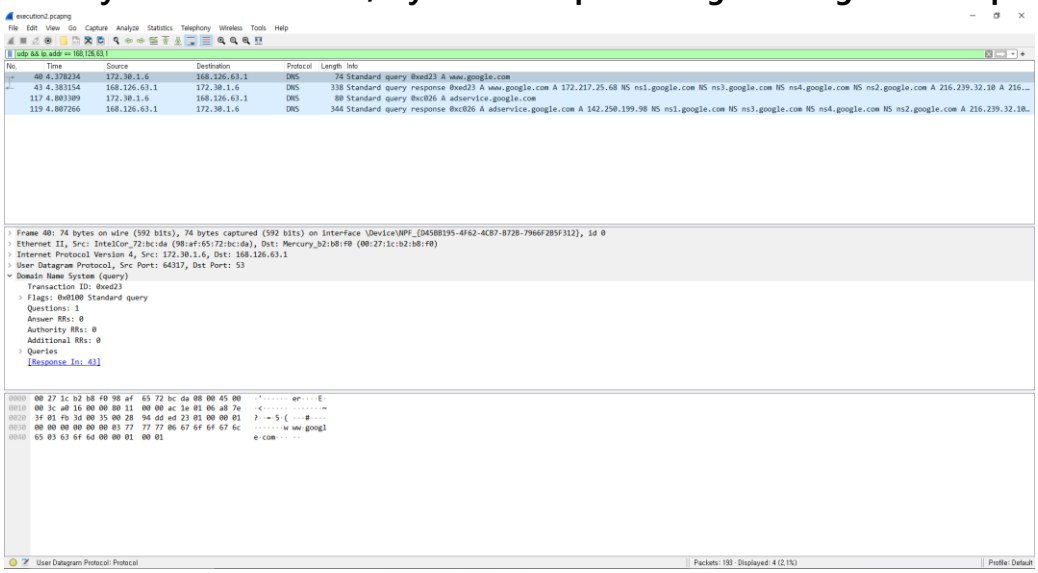
- **Open Wireshark program and open web browser**
- **Capture packets to record HTTP traffics into a file using Wireshark while you are browsing `www.google.com`. using filter "tcp".**
- **Answer to the following questions**



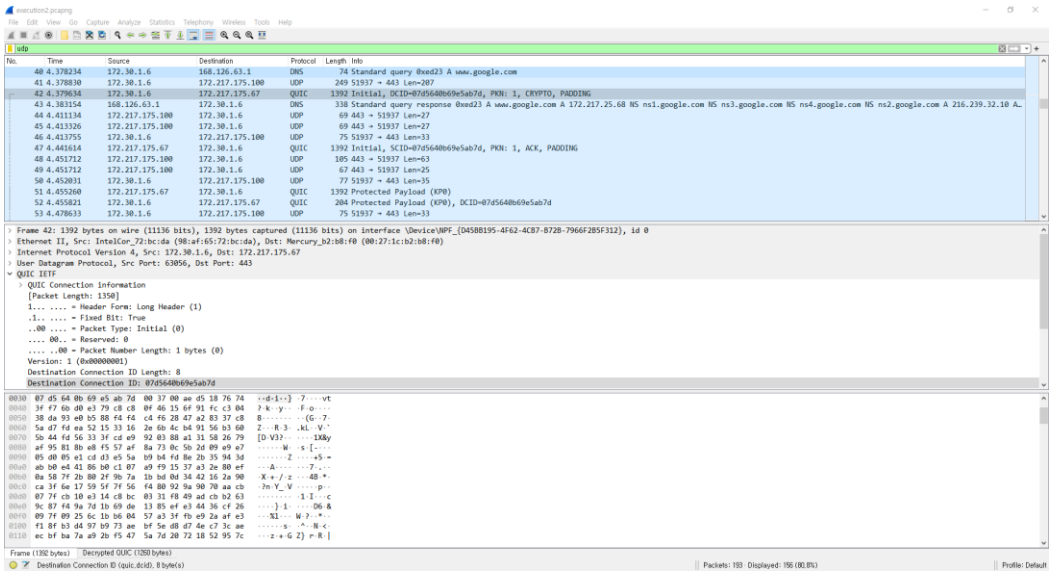
- **How many packets have you recorded?**

  크롬 브라우저에서 www.google.com 을 열었을 때, TCP 로 필터링하면 어떠한 packet 도 잡히지 않는 것을 확인할 수 있습니다.

  - **In case you recorded some packets what is the IP address of the google server? Compare this IP address with the IP address by DNS looking at `https://dns.google.com/`.**
- **In case you recorded none, try to record packets again using filter "udp"**



- **Pick a packet carrying a payload (data). In the middle window of Wireshark, how many protocols do you see and what are they?**
  다음의 packet 들 중에서 임의의 packet 을 선택하여 확인해보면, 총 4 개의 Protocol (Ethernet Protocol, Internet Protocol, User Datagram Protocol, Domain Name System Protocol)을 볼 수 있습니다.



  그런데 UDP 로만 필터링하면, 42 번과 같은 packet 도 존재합니다. 이러한 Packet 에서는 총 4 개의 Protocol (Ethernet Protocol, Internet Protocol, User Datagram Protocol, Quick UDP Internet Connections Protocol)을 확인할 수 있습니다.

- **Why are there UDP and TCP differences in between Execution 1 and 2**
  HTTP/3 는 HTTP 의 세 번째 메이저 버전으로, 기존의 HTTP/1, HTTP/2 와는 다르게 TCP 가 아닌 UDP 기반의 프로토콜인 QUIC 을 사용하여 통신하는 프로토콜입니다. TCP 는 연결형 서비스로 packet 교환이 virtual circuit 방식으로 이루어집니다. 이러한 TCP 의 경우, 신뢰성이 높지만 전송 속도가 느립니다. UDP 는 비연결형 서비스로 packet 교환이 datagram 방식으로 이루어집니다. UDP 의 경우, 신뢰성은 낮지만 전송 속도는 빠릅니다. 그런데, 구글은 TCP 를 대체하는 네트워크 프로토콜인 QUIC 을 크롬 브라우저와 구글 서버에 기본으로 적용하고 있습니다. 그렇기 때문에 Execution 1 에서는 TCP 로, Execution 2 에서는 UDP 로 필터링했을 때 packet 을 확인할 수 있는 것입니다.