

# 네트워크 인터페이스 계층 & 네트워크 패킷 분석

# 목차

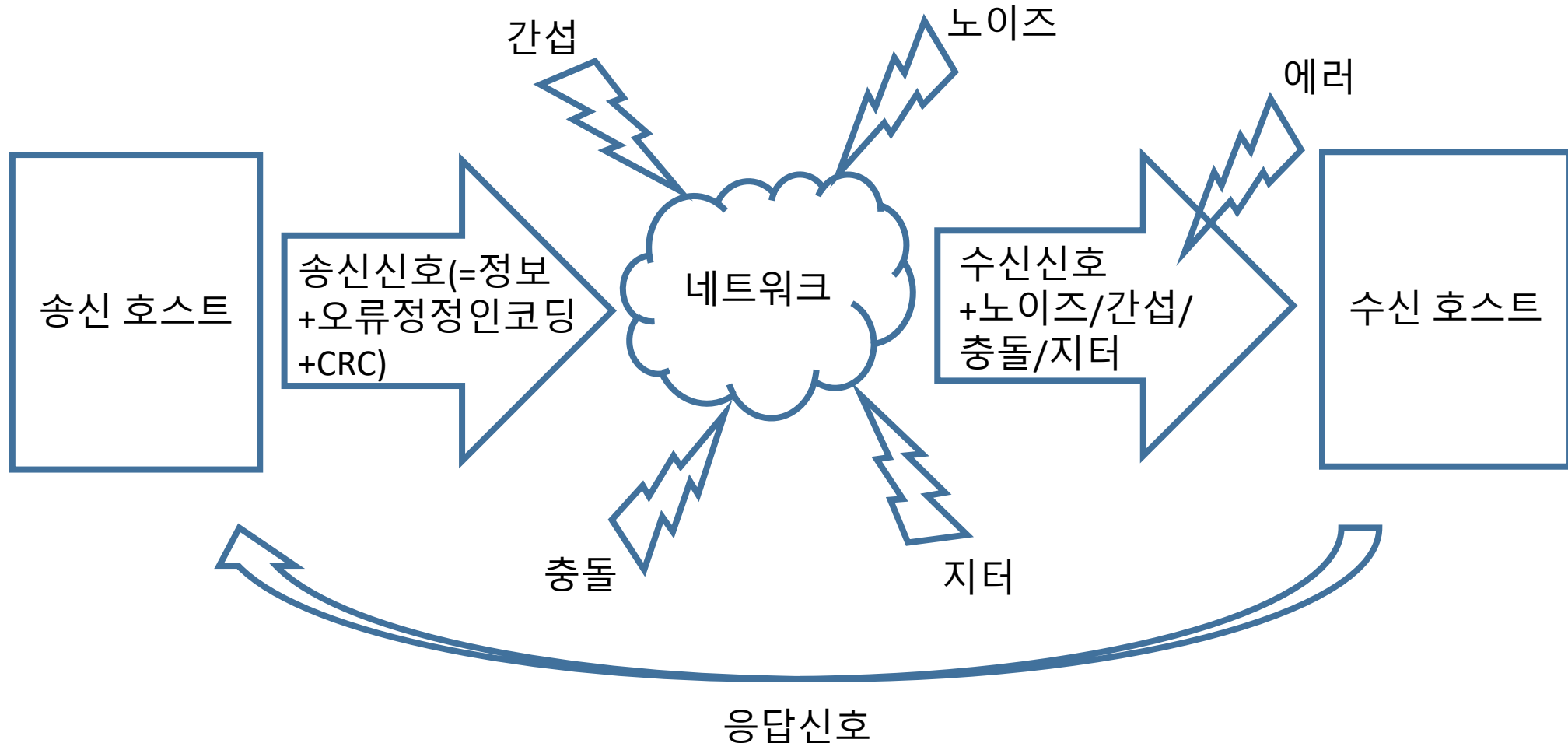
---

- 네트워크 인터페이스 계층의 프레임 전송
- 네트워크 인터페이스 계층 주소
- 네트워크 인터페이스 계층 전송 데이터
- 네트워크 패킷 분석
- 와이어샤크 고급 기능

# 네트워크 인터페이스 계층의 프레임 전송

- 네트워크의 신뢰 통신 방법

- 순방향 에러 정정 (Forward Error Correction, FEC) + 역방향 에러 정정 (Backward Error Correction, BEC) + 재전송 기법

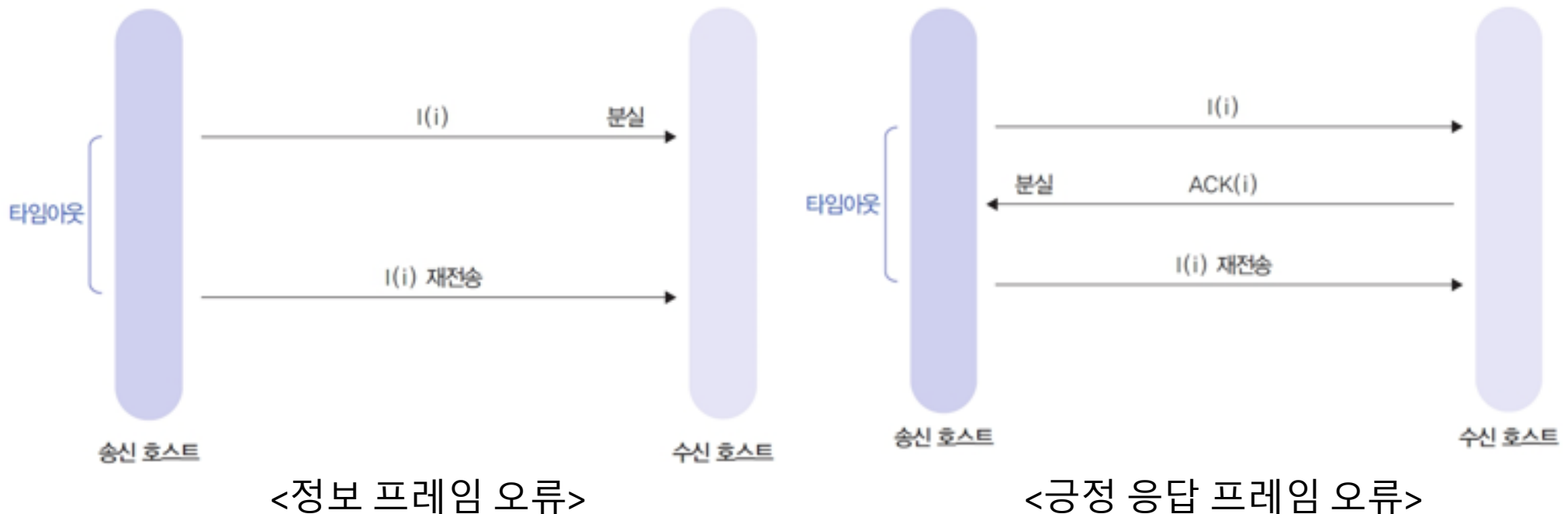


# 네트워크 인터페이스 계층의 프레임 전송

- 역방향 에러 정정 방식

- 긍정 응답 프레임

- ✓ 수신한 정보 프레임 오류가 발생하지 않았으면 (=정상적으로 수신했으면) 송신 호스트에 해당 프레임을 올바르게 수신했다는 의미로 ACK 프레임 (=긍정 응답 프레임)을 회신
    - ✓ 수신한 정보 프레임 오류가 발생하면, 송신 호스트에게 긍정 응답 프레임을 회신하지 않고, 송신 호스트는 일정 시간 동안 긍정 응답 프레임이 회신 받지 못하면 재전송함

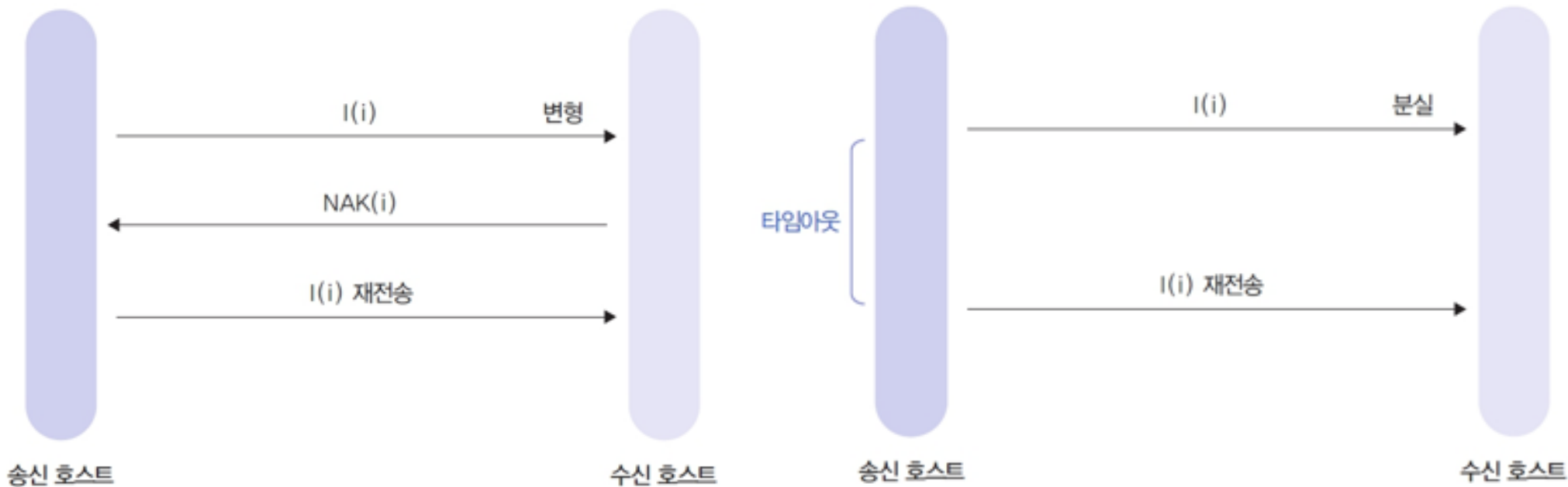


# 네트워크 인터페이스 계층의 프레임 전송

- 역방향 에러 정정 방식

- 부정 응답 프레임

- ✓ 정보 프레임에 오류가 발생하면 수신 호스트는 부정 응답을 송신 호스트에게 회신하여 오류 발생을 인지하고 원래의 정보 프레임을 재전송하도록 요청
    - ✓ 송신 호스트는 부정 응답 프레임을 수신하면 재전송함



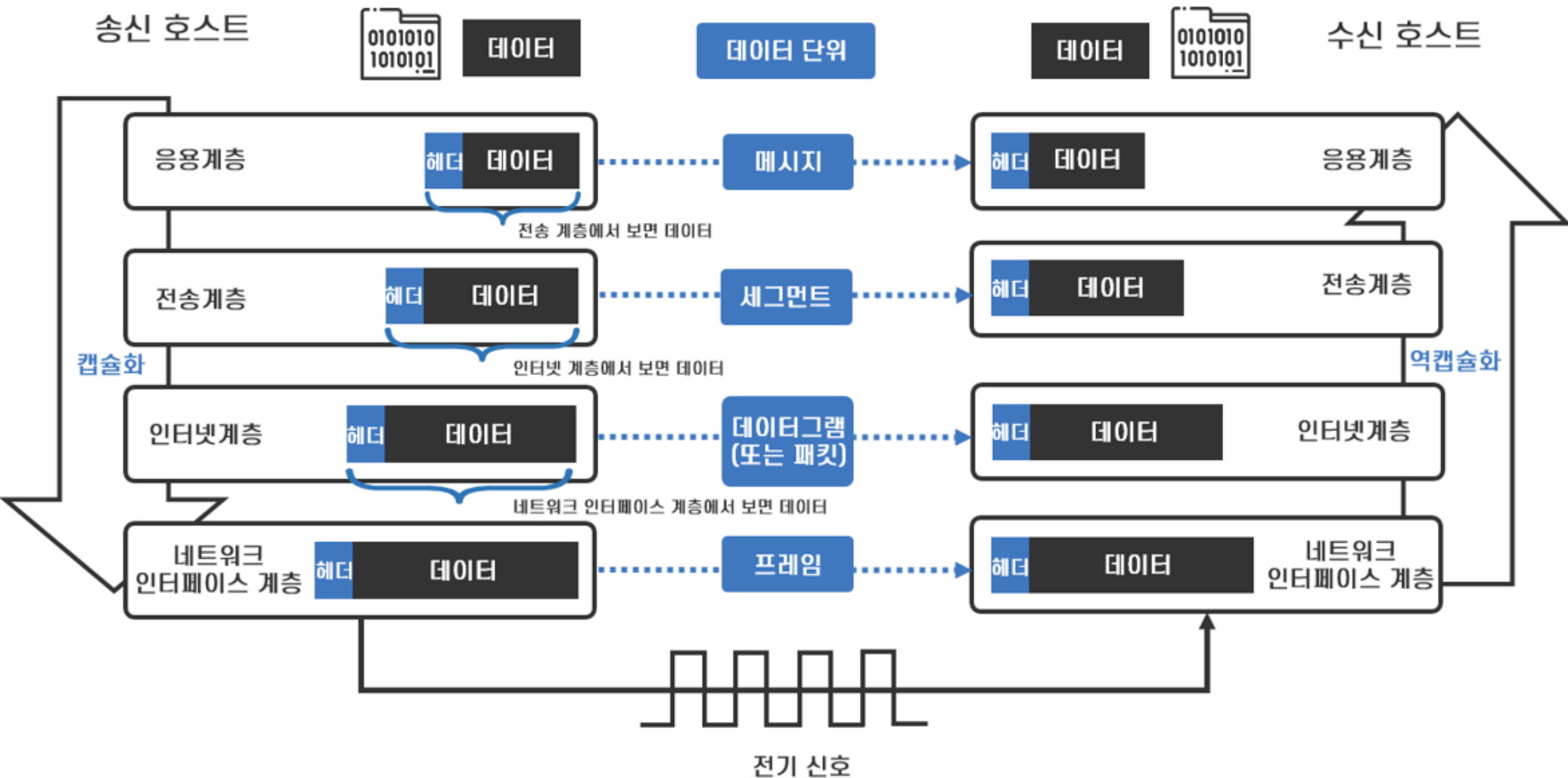
<정보 프레임 변형 오류>

<긍정 응답 프레임 분실 오류>

# 네트워크 인터페이스 계층의 프레임 전송

- 계층별 데이터 타입

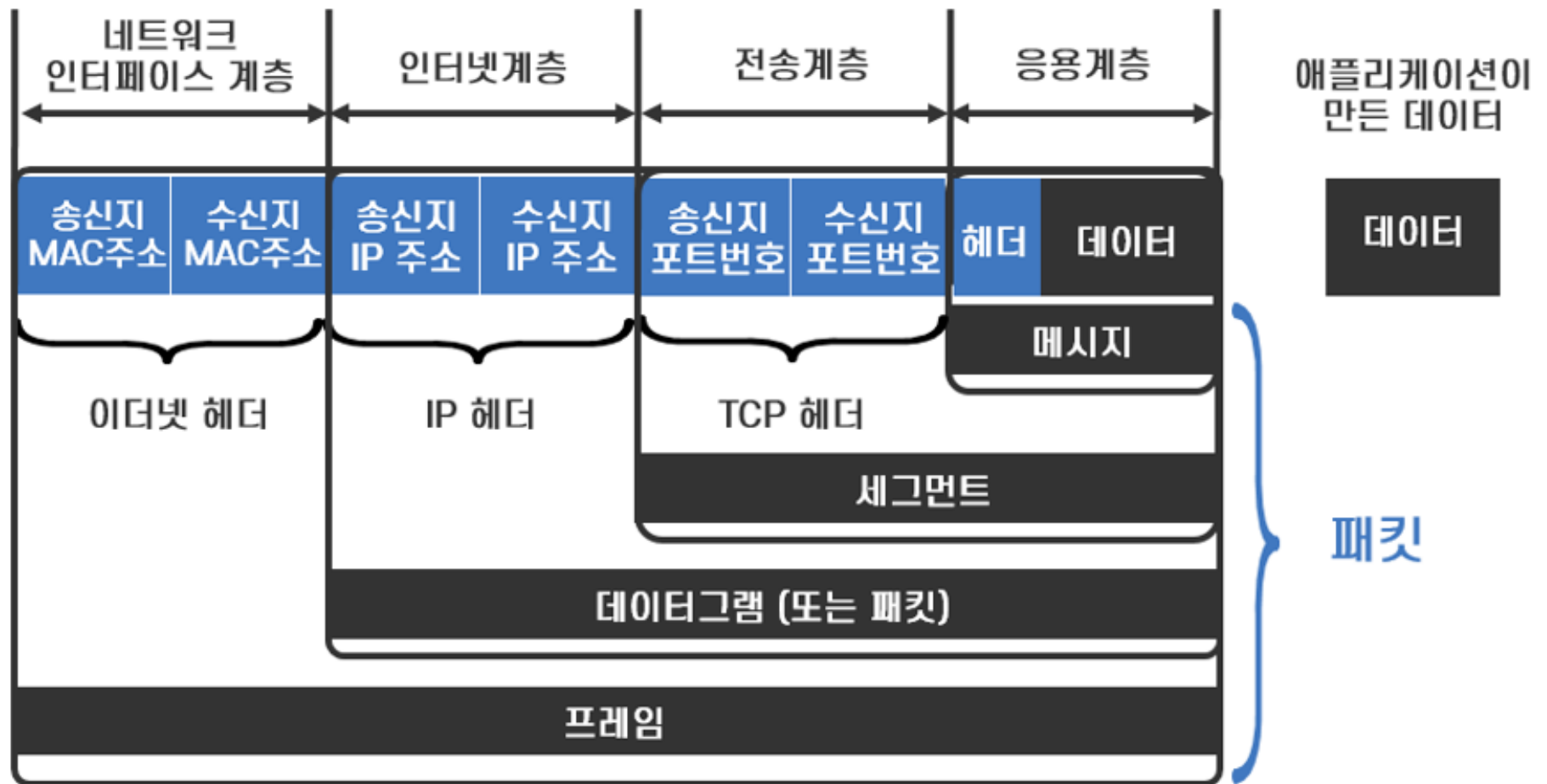
- 송신 노드, 수신 노드, 중간 노드 각각이 계층별로 데이터 처리



# 네트워크 인터페이스 계층의 프레임 전송

- 프레임 헤더 구조

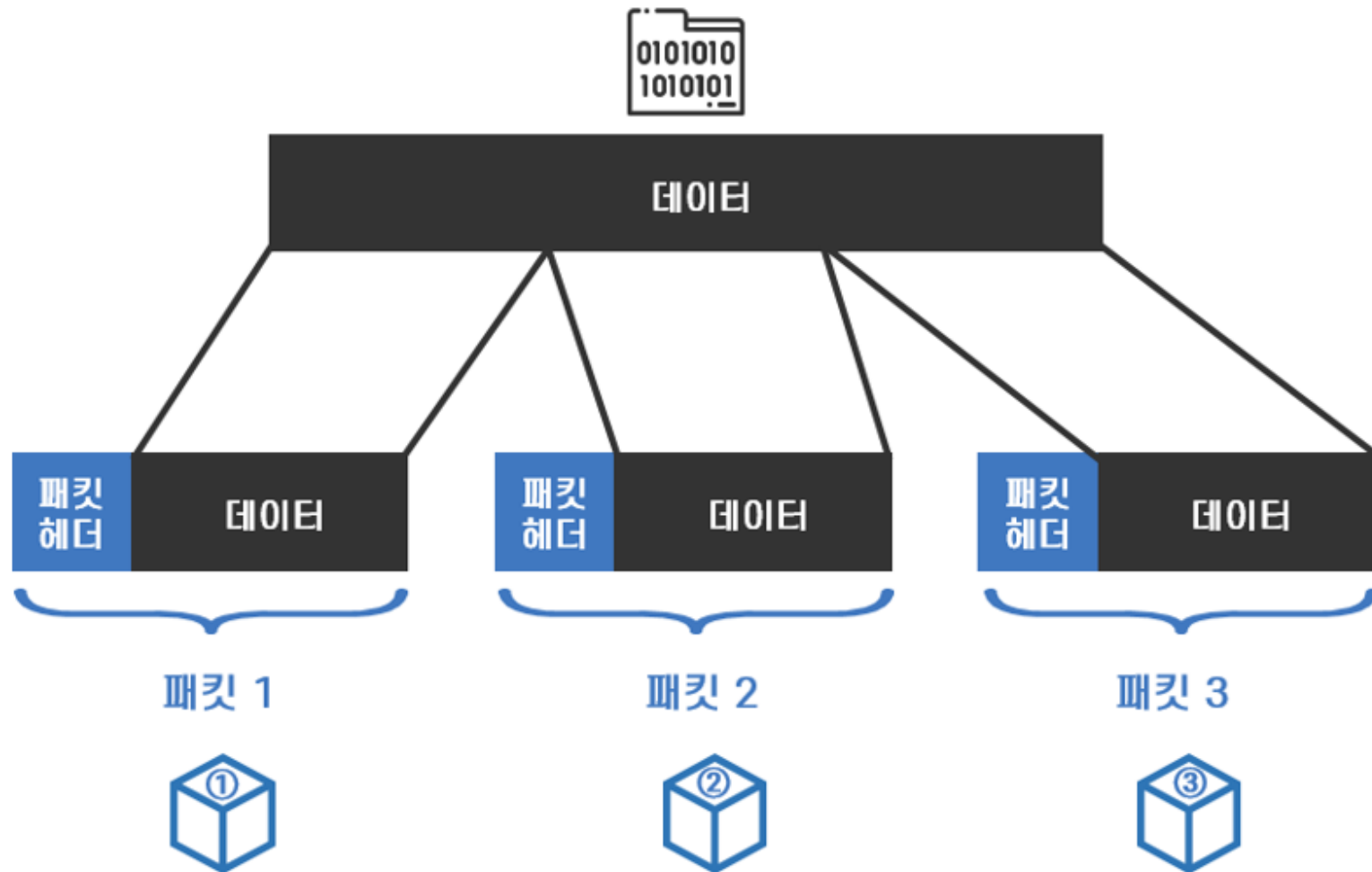
- 프레임 = 이더넷 헤더 + IP 헤더 + TCP 헤더 + 메시지(헤더+데이터)



# 네트워크 인터페이스 계층의 프레임 전송

- 데이터와 패킷

- 빅데이터가 여러 개의 데이터로 분할되어 패킷 헤더를 붙여서 네트워크로 전송됨.





# 네트워크 인터페이스 계층의 프레임 전송

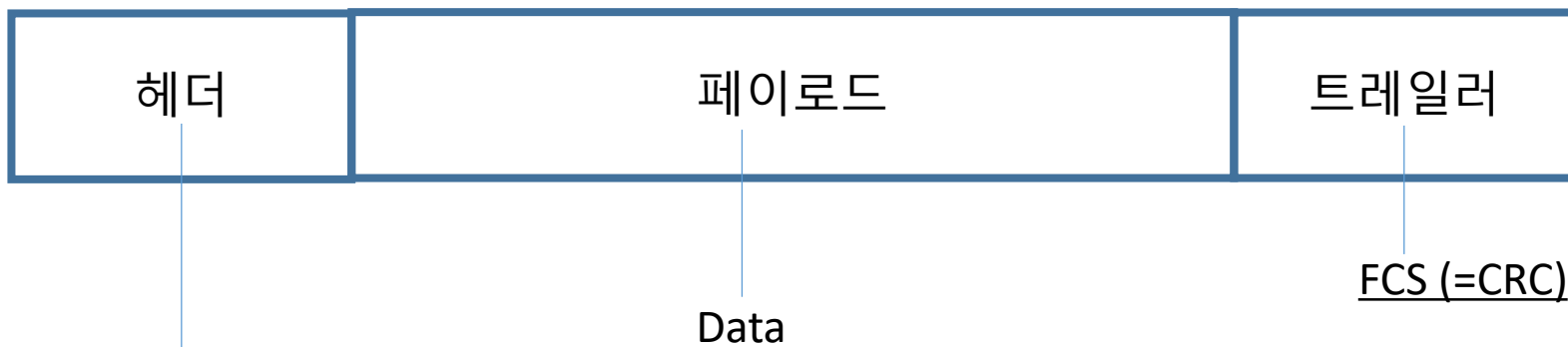
- 네트워크 전송 데이터 구조

- 패킷 = 헤더 + 데이터 + 트레일러

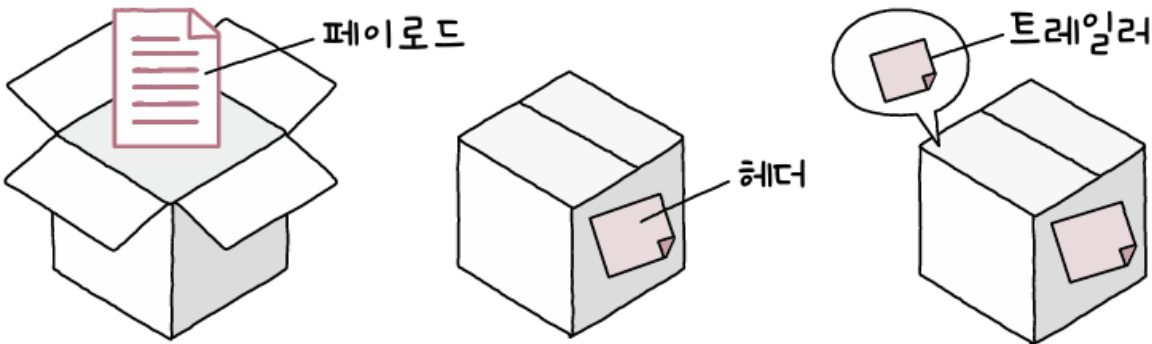
- ✓ 헤더: 데이터 종류, 데이터 길이, 페이로드를 수신하는 방법 (=전송 기법)에 관한 정보 (헤더 데이터도 자체적인 CRC 로 오류 검사)

- ✓ 페이로드: 송신 호스트가 전송하는 데이터 (오류 정정 인코딩 된 데이터)

- ✓ 트레일러: 페이로드 오류 확인하기 위한 체크섬 (FCS)



Preamble, Dest. Address, Source Address, Type/Length



패킷은 페이로드와 헤더로 구성되고, 때로는 트레일러도 포함됩니다.



# 네트워크 인터페이스 계층의 프레임 전송

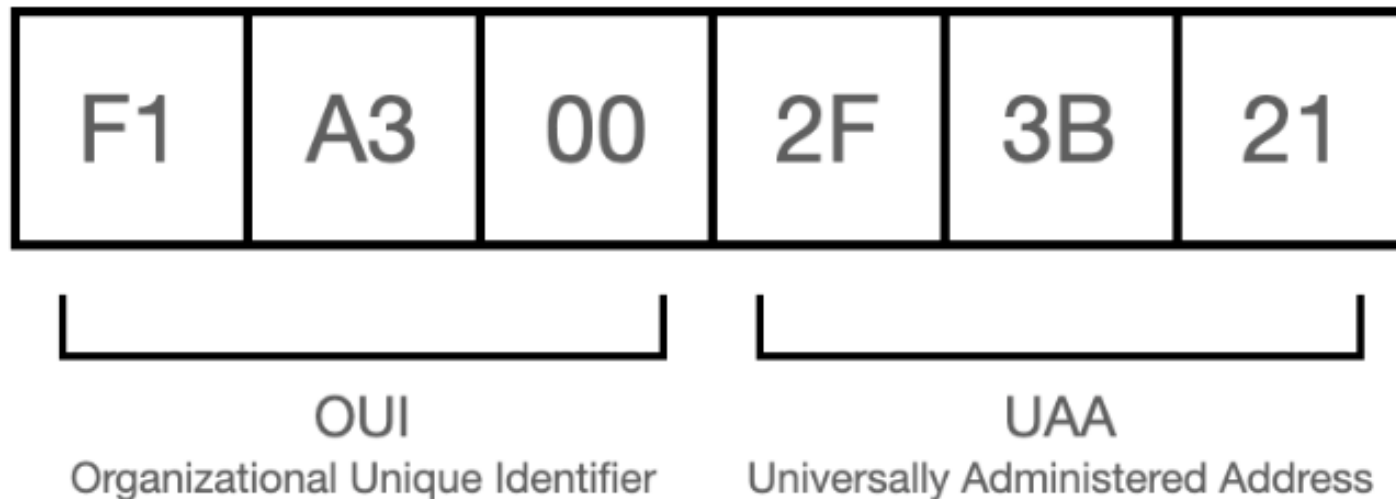
---

- 네트워크 전송: TCP/IP와 패킷 교환
  - OSI 7계층의 3계층 IP 프로토콜과 4계층 TCP 프로토콜을 활용하여 월드 와이드웹의 LAN과 WAN을 연결하여 인터넷 서비스를 실현시키는 네트워크 표준
  - TCP/IP 프로토콜은 엄청난 양의 데이터를 효율적이고 안정적으로 전송하기 위해 “패킷 교환 방식”으로 전송함
  - 패킷 교환 (Packet Switching) 방식은 미리 고정된 이동 경로를 설정하지 않는 대신 데이터를 패킷 단위로 나누고, 각 패킷에 고유 번호를 붙여서 네트워크에 흩뿌려서 전송하며, 각 패킷은 전송 당시 가장 효율적인 경로를 따라 최종 수신지로 각각 보내며, 최종 수신지에서 원래의 데이터로 재결합함
  - 패킷을 수신한 중간 노드는 패킷의 수신지 호스트 주소를 확인하고, 수신지 호스트까지 가는 다양한 경로 중 가장 좋은 경로를 선택하여 다음 중간 노드로 패킷을 전송하는 라우팅 수행

# 네트워크 인터페이스 계층 주소

- MAC 주소

- 랜 카드 (NIC)에 할당된 값이며, 전 세계에서 하나만 존재하는 고유한 값
- 48 비트로 표현 = 상위 24비트는 랜카드 제조사에서 부여한 OUI (Organizational Unique Identifier) 코드 + 하위 24비트는 제조사가 랜 카드에 고유하게 부여한 UAA (Universally Administered Address) 번호



- 콜론 (:) 이나 하이픈 (-)을 이용해서 16진수로 표기함 → F1-A3-00-2F-3B-21

# 네트워크 인터페이스 계층 주소



- 네트워크 인터페이스의 MAC 주소

- 송신 호스트의 네트워크 인터페이스 카드가 수신 호스트의 네트워크 인터페이스 카드의 MAC 주소를 아는 방법 → ARP 프로토콜 (3계층 프로토콜)

C:\ 명령 프롬프트

```
Microsoft Windows [Version 10.0.19045.4894]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\USER>arp -a
```

```
인터페이스: 192.168.0.37 --- 0x7  
인터네트 주소      물리적 주소      유형  
192.168.0.1        90-9f-33-71-ef-50  동적  
192.168.0.33       04-0e-3c-e9-f9-65  동적  
192.168.0.255      ff-ff-ff-ff-ff-ff  정적  
224.0.0.2          01-00-5e-00-00-02  정적  
224.0.0.22         01-00-5e-00-00-16  정적  
224.0.0.113        01-00-5e-00-00-71  정적  
224.0.0.251        01-00-5e-00-00-fb  정적  
224.0.0.252        01-00-5e-00-00-fc  정적  
239.192.152.143    01-00-5e-40-98-8f  정적  
239.255.255.250    01-00-5e-7f-ff-fa  정적  
255.255.255.255    ff-ff-ff-ff-ff-ff  정적
```

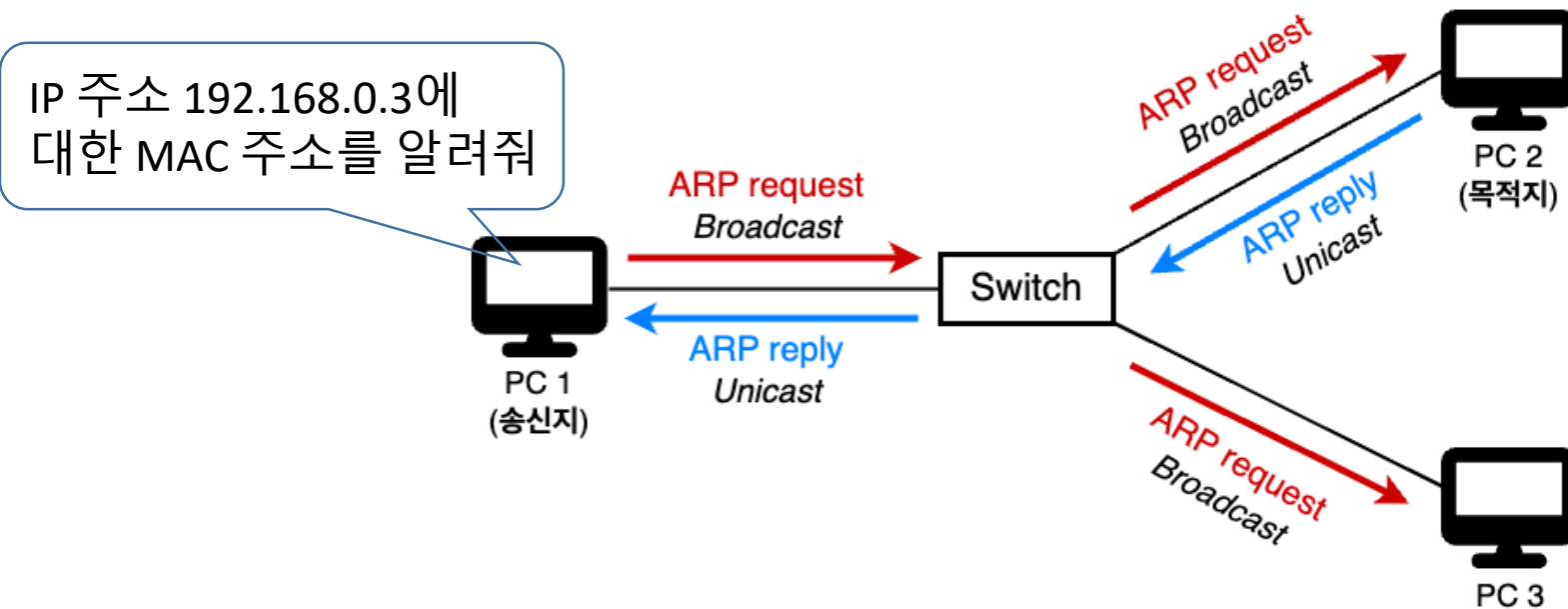
```
C:\Users\USER>
```

# 네트워크 인터페이스 계층 주소

- ARP를 이용해서 MAC 주소를 알아내는 과정

목표: 송신 PC 1 (IP 주소: 192.168.0.2)가 수신 PC 2 (IP 주소: 192.168.0.3)에게 데이터 전송

- 송신 PC 1은 자신의 메모리 (ARP 테이블)에 192.168.0.3 IP 주소의 MAC 주소 정보가 있는지 확인함
- 자신의 메모리에 정보가 없다면 PC 1은 네트워크의 주변 컴퓨터들에게 192.168.0.3이라는 IP 주소의 MAC 주소 컴퓨터가 있는지 ARP 요청 프레임을 브로드캐스팅함

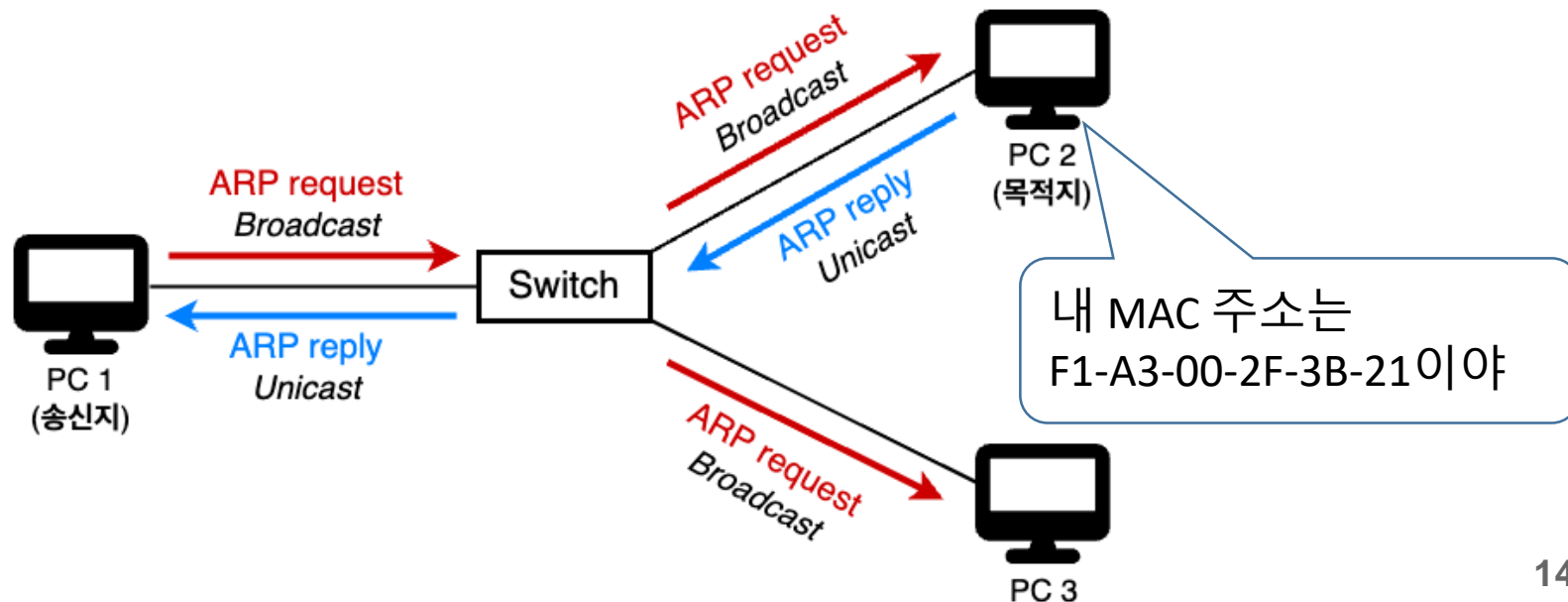


# 네트워크 인터페이스 계층 주소

- ARP를 이용해서 MAC 주소를 알아내는 과정

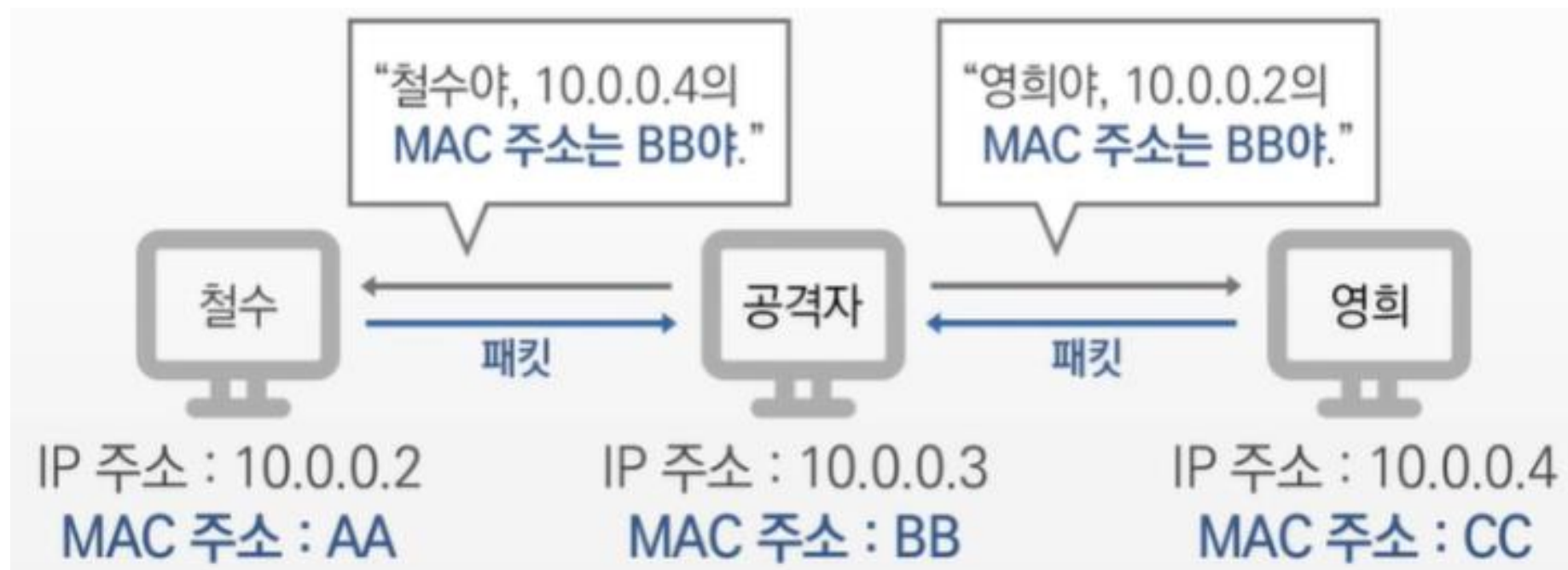
목표: 송신 PC 1 (IP 주소: 192.168.0.2)가 수신 PC 2 (IP 주소: 192.168.0.3)에게 데이터 전송

- ARP 요청 프레임을 수신한 컴퓨터는 자신의 IP를 192.168.0.3과 비교함
- 192.168.0.3 IP 컴퓨터 B가 컴퓨터 A에게 ARP 응답함
- 컴퓨터 A는 컴퓨터 B의 IP 주소와 MAC 주소의 매핑 정보 값을 메모리 (ARP 테이블)에 저장함
- 그 이후부터 컴퓨터 A는 컴퓨터 B와 통신할 때, ARP 테이블을 참조하여 통신



# 네트워크 인터페이스 계층 주소

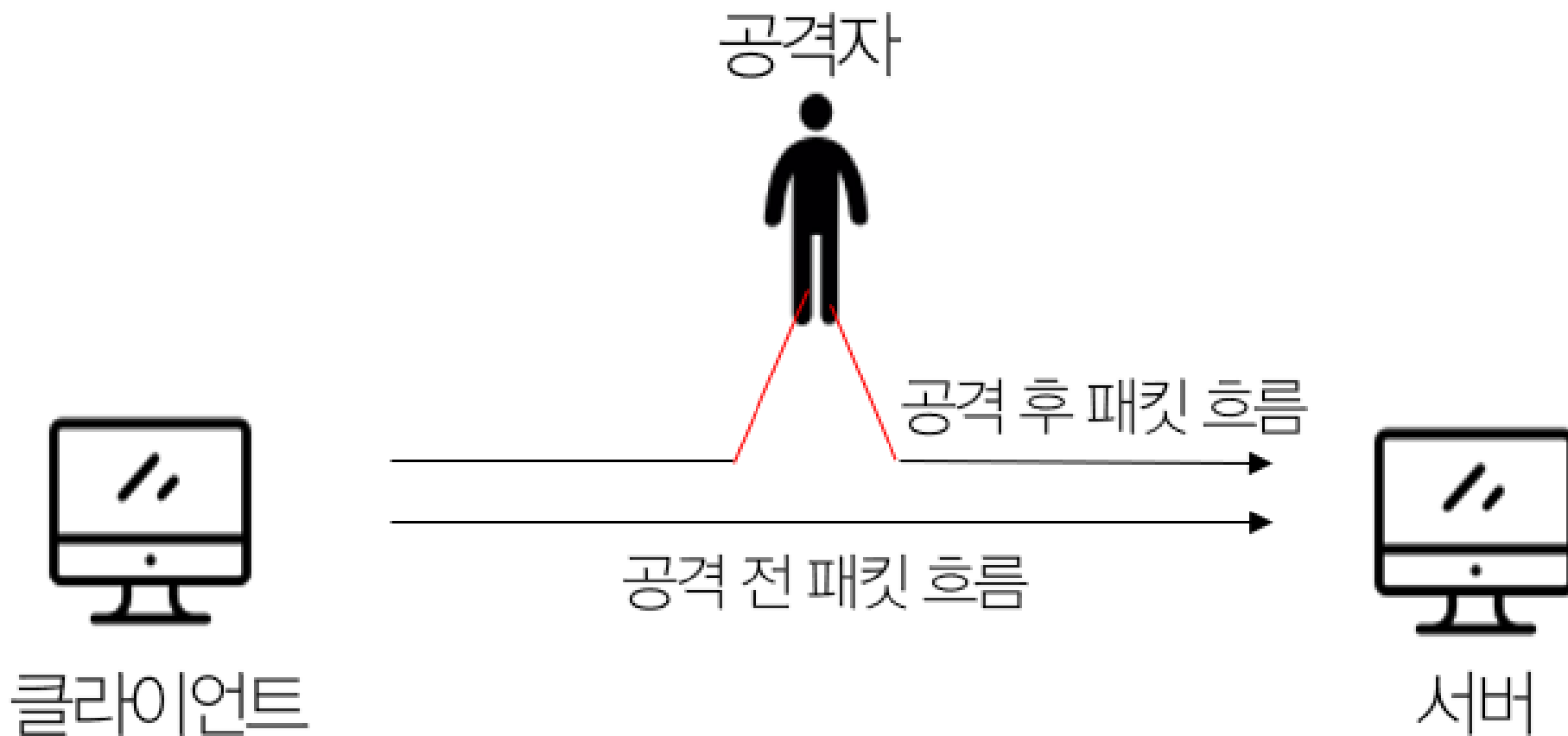
- ARP 프로토콜의 취약점을 활용한 공격 (=ARP 스푸핑 공격)
  - ARP 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법
  - 데이터 링크 프로토콜인 ARP 프로토콜을 이용하므로 근거리 네트워크 (=LAN)에서만 사용할 수 있는 공격



# 네트워크 인터페이스 계층 주소

- ARP 스푸핑 공격의 원리

- ARP 공격을 통해 공격자가 클라이언트와 서버의 패킷 전송 흐름을 변경하여 공격자가 패킷을 도청하거나 위변조할 수 있도록 함

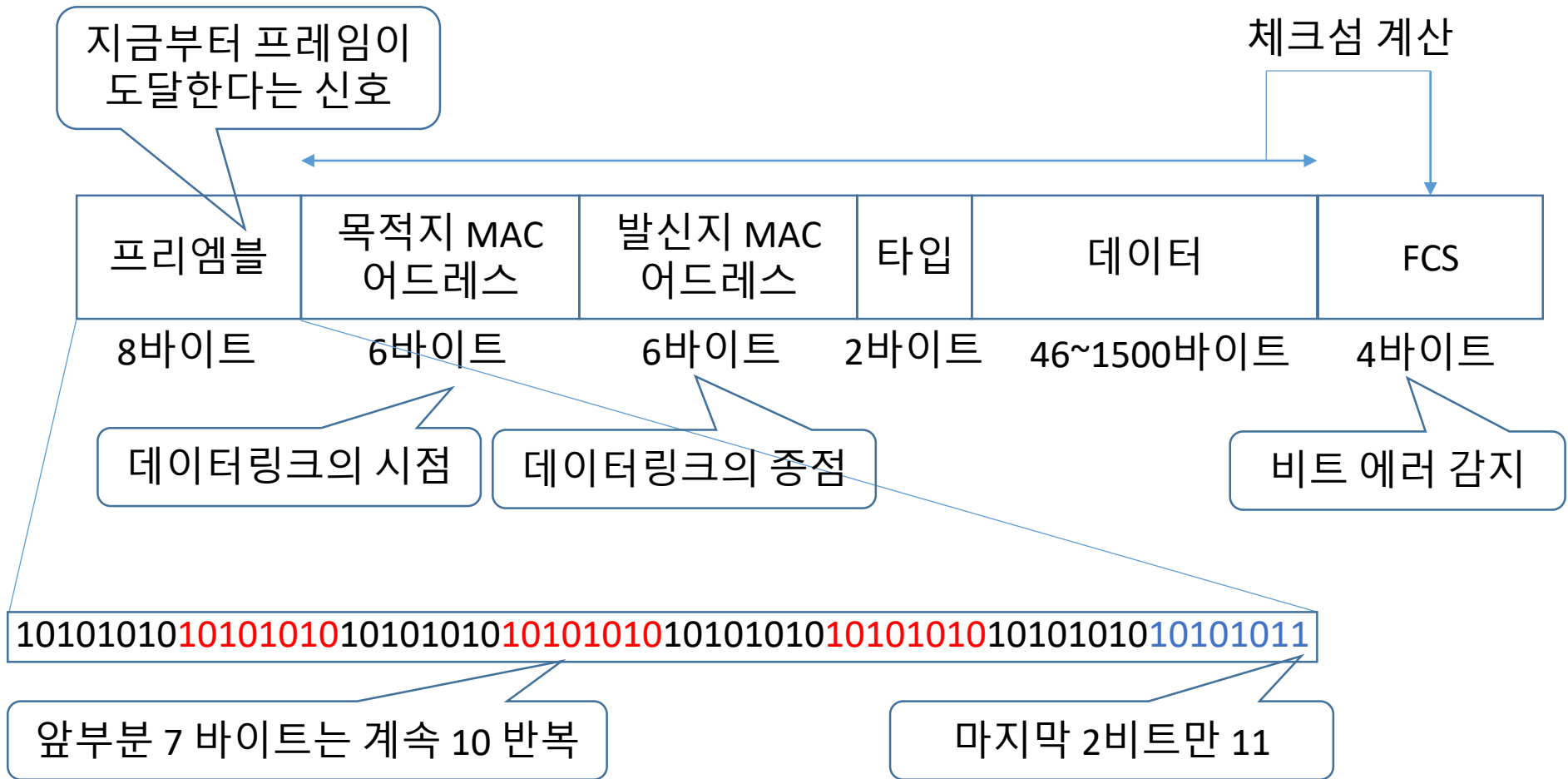




# 네트워크 인터페이스 계층 전송 데이터

- Ethernet 프레임

- 프리엠블 + 헤더 (주소 + 타입) + 데이터 + FCS 구조
- 데이터: 46~1500 바이트 길이
- FCS: 데이터를 CRC (Cyclic Redundancy Check, 순환 중복 검사)하여 FCS에 추가



# 네트워크 인터페이스 계층 전송 데이터

---

- Ethernet 헤더

- Preamble (프리앰블)

- ✓ Ethernet 프로토콜이 시작되는 지점을 알려주는 기능
    - ✓ 총 8byte인데, 1010 1010 이 일곱 번 반복하면서 (7byte) 전기 신호를 보내는 쪽과 받는 쪽을 동기화하고 마지막 1 byte로 1010 1011을 전송하여 Ethernet 헤더의 시작을 알려줌.
    - ✓ 마지막 1 byte는 시작을 알려주는 SFD (Start Frame Delimiter) 라고 함.

- Destination/Source Address (주소)

- ✓ 목적지 MAC 주소 6byte, 출발지 MAC 주소 6byte
    - ✓ A 컴퓨터가 공유기를 통해 B 컴퓨터에 데이터를 전달한다면, A 컴퓨터가 보내는 프레임의 목적지 주소는 공유기의 MAC 주소가 되고, 출발지 주소는 A 컴퓨터의 MAC 주소가 됨

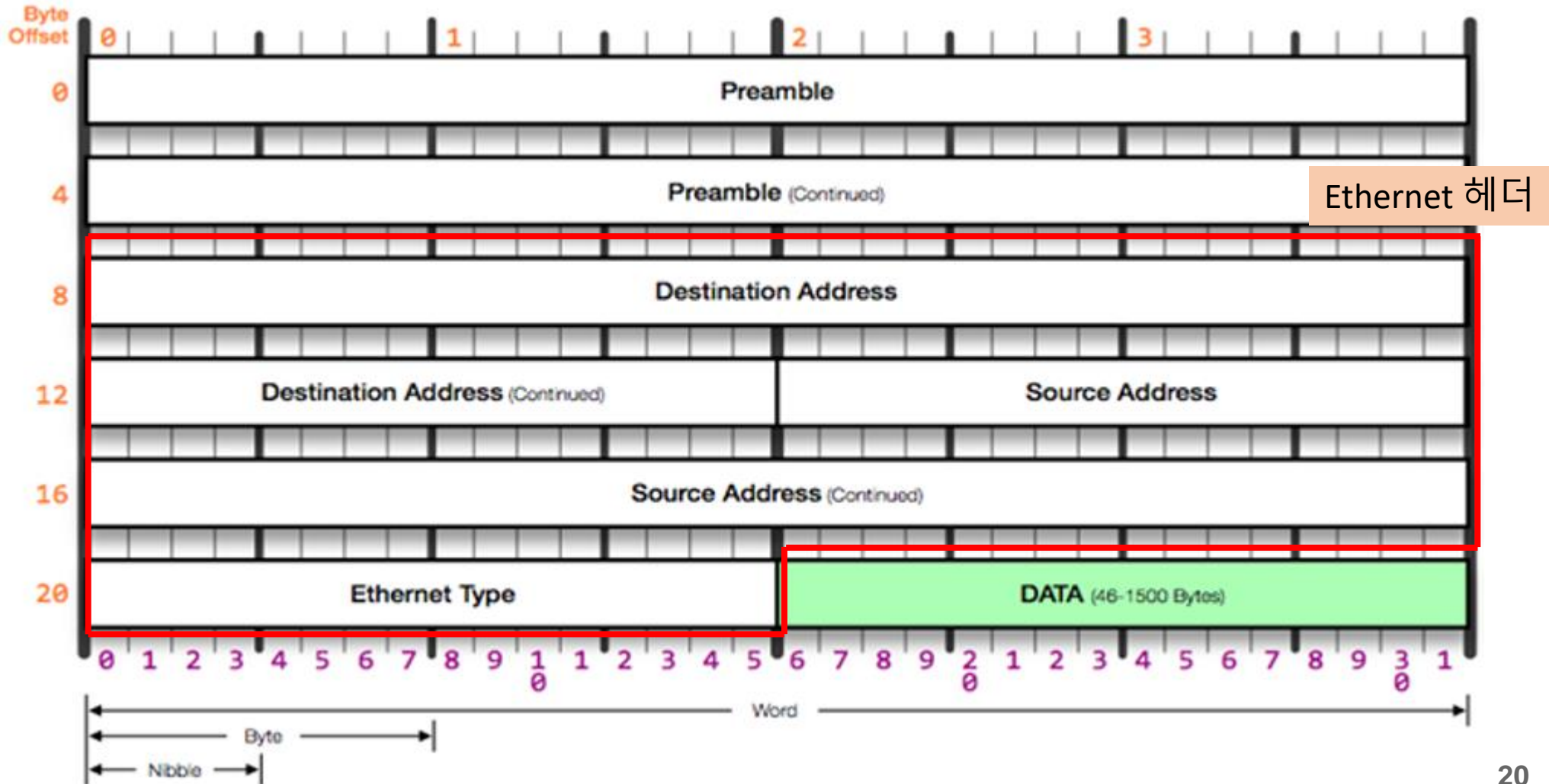
- Ethernet Type (상위 프로토콜의 유형)

- ✓ 데이터를 캡슐화할 때 사용한 3계층 프로토콜이 무엇인지 알려주는 기능
    - ✓ 3계층 프로토콜은 ARP 나 IPv4 인 경우가 많음; ARP는 0x0806, IPv4는 0x0800 으로 표시



# 네트워크 인터페이스 계층 전송 데이터

- Ethernet 프로토콜
  - Ethernet 2 헤더



# 네트워크 패킷 분석

---

- 패킷 분석기 (Packet analyzer) | 패킷 스니퍼 (Packet sniffer)
  - 네트워크 분석: 네트워크 통신 과정에서 패킷을 스니핑 (Sniffing)하여 수집 (=Capture, 캡처)하고, 분석하는 것
    - ✓ 패킷 캡처 (Packet capture): 네트워크 케이블로 전송되는 전기 신호를 데이터 형태로 획득하는 것
    - ✓ 덤프 분석 (dump analysis): 획득한 패킷의 의미를 분석하는 것
  - 네트워크 분석가의 기본 요건
    - ✓ TCP/IP 통신 프로토콜에 대한 이해
    - ✓ 패킷 분석기 사용법
    - ✓ 패킷 구조와 패킷 흐름 이해
  - 패킷 분석기: 네트워크를 통해 전달되는 패킷을 캡처하여 패킷의 내용을 화면에 나타내 주는 소프트웨어
  - 패킷 분석기 종류
    - ✓ 하드웨어 분석기
    - ✓ 소프트웨어 분석기

# 네트워크 패킷 분석

---

- 와이어샹크

- 근거리 네트워크 상에서 전달되는 패킷을 분석하는 네트워크 패킷 분석 소프트웨어 도구 (무료 오픈소스)
- 1988년 미국의 제럴드 콤즈 (Gerald Combs)가 첫 버전인 Ethereal 개발하여 오픈소스로 공개
- 유닉스, 리눅스 등 다양한 운영체제에서 사용할 수 있음
- Npcap 이란 소프트웨어를 사용하여 윈도우에서 패킷 분석할 수 있음

- 와이어샹크 용도

- 컴퓨터 네트워크 프로토콜을 배우기 위해 사용
- 네트워크 관리자가 네트워크 트러블을 해결하기 위해 사용
- 보안 기술자가 보안 문제를 시험하거나 확인/해결하기 위해 사용
- 개발자 프로토콜을 구현할 때 디버그(오류 확인)하기 위해 사용
- 품질 관리 엔지니어가 네트워크 애플리케이션을 확인하는데 사용

# 네트워크 패킷 분석

---

- 와이어샤크 주요 기능

- 대부분의 OS (유닉스, 리눅스, 윈도우 등)를 지원
- 네트워크 인터페이스로부터 실시간으로 패킷 데이터를 캡처할 수 있음
- 패킷에 대한 프로토콜 정보를 자세하게 보여줌
- 캡처된 패킷 데이터를 열거나 저장할 수 있음
- 다른 패킷 분석기가 획득한 패킷 캡처 데이터를 변환하여 열거나 출력할 수 있음
- 여러 조건으로 패킷을 제한하여 검색할 수 있음
- 필터링된 패킷을 원하는 색으로 나타낼 수 있음
- 캡처한 데이터를 다양한 형식으로 출력할 뿐만 아니라 여러가지 통계를 만들 수 있음
- 여러가지 암호 프로토콜 복호를 지원함



# 네트워크 패킷 분석

---

- 와이어샤크 장점

- 패킷 내용을 자세하게 보여줌
- 패킷 내용을 분석해 줌
- 상용 패킷 분석기 보다 훨씬 쉽게 패킷을 해석할 수 있음
- 캡처 파일 (capture file), 추적 파일 (trace file)로 캡처 패킷을 저장하여 다른 파일 형식으로 출력하거나 복수의 캡처 파일을 결합하고 분석할 수 있음

- 와이어샤크 한계점

- 상용 분석기에 비해 통계 기능이나 보고 기능, 임계치 기능이 비교적 약함
- 침입탐지시스템 (IDS, intrusion detection system)으로 개발된 것이 아니므로 네트워크 변화를 감지하고 대응할 수 없음
- 네트워크를 직접 조작할 수 없음 (단순 스니핑/분석 장치); 상용 분석기에는 패킷 생성 도구가 포함되어서 특정 조건의 패킷을 생성해서 송신할 수 있음

- 와이어샤크 정보

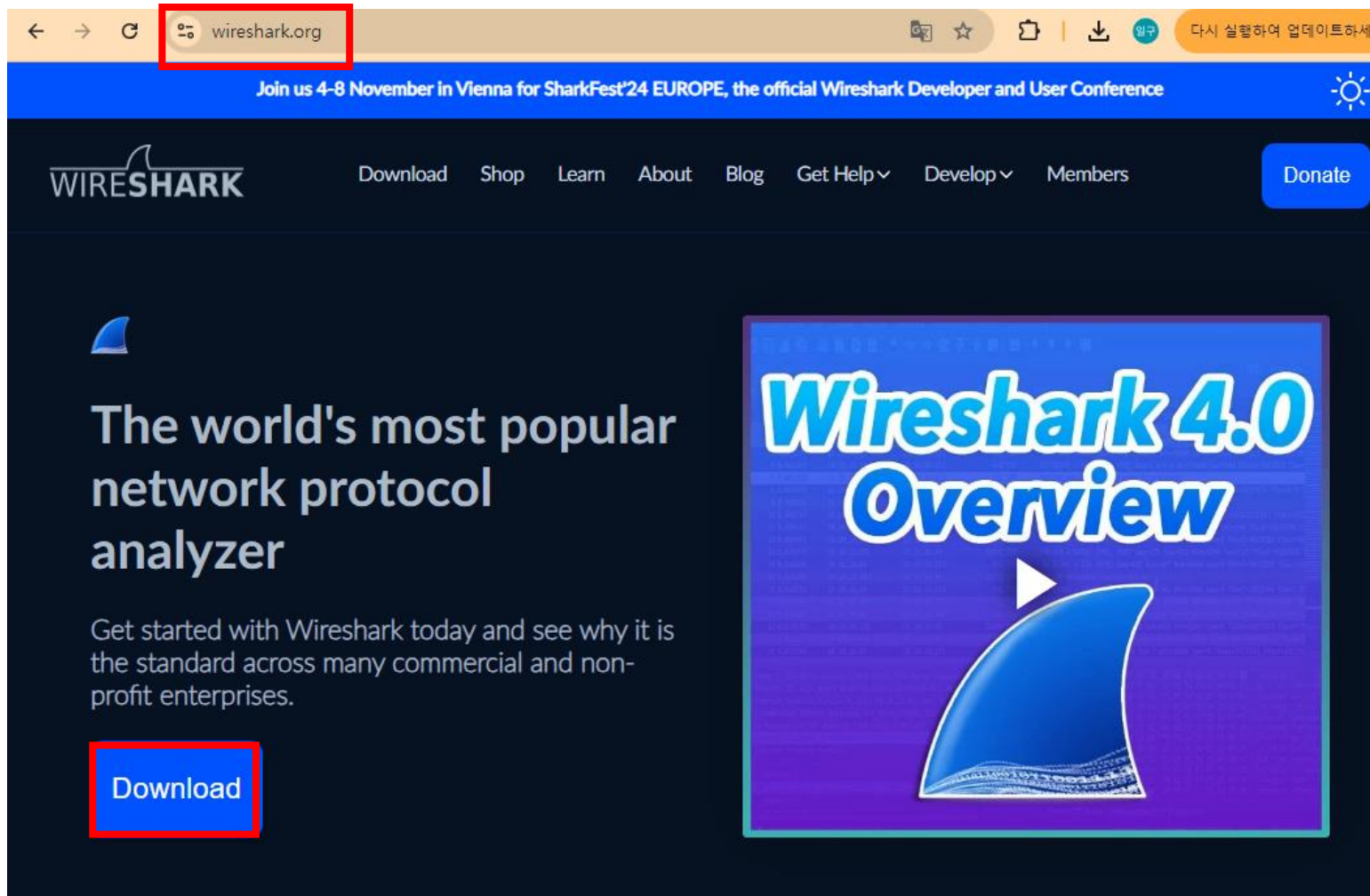
- <https://wiki.wireshark.org/>



# 네트워크 패킷 분석

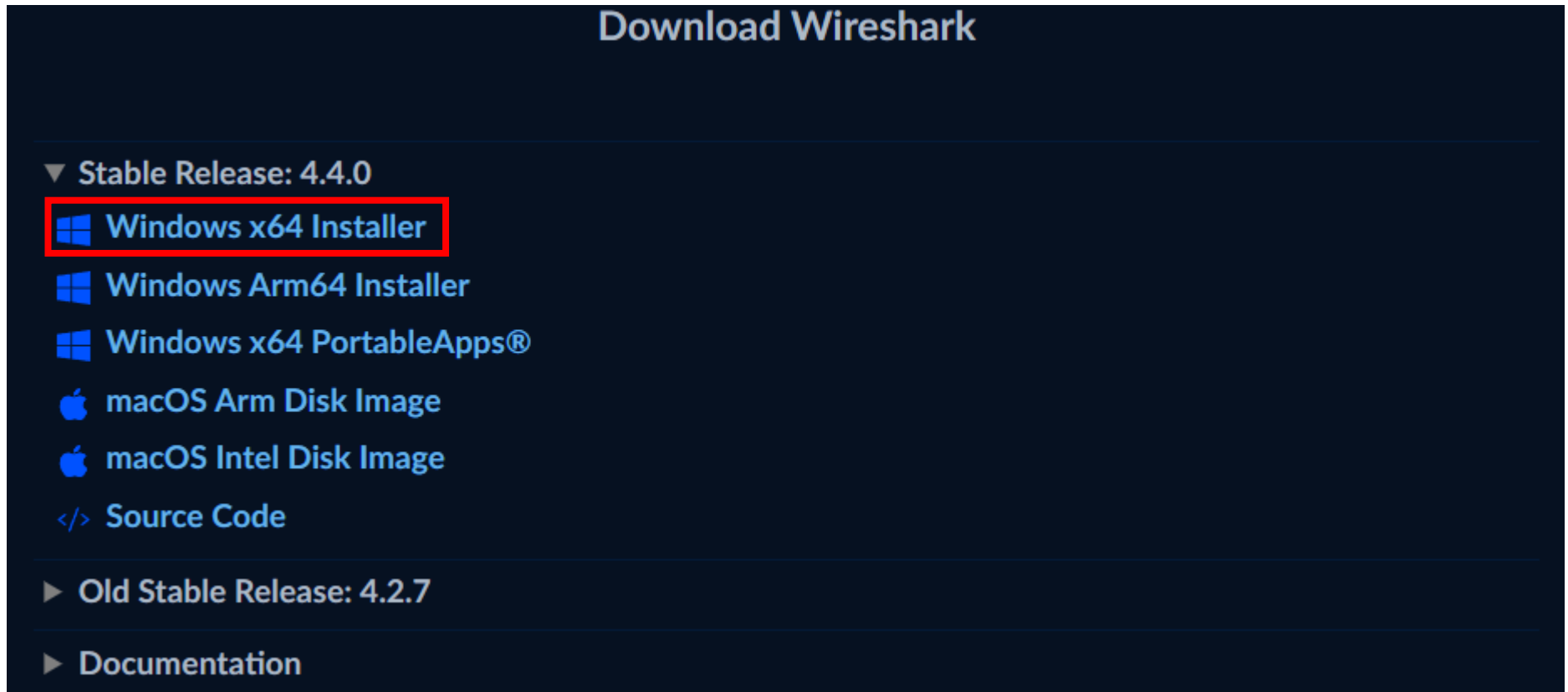
- 와이어샤크

- <https://www.wireshark.org/>



# 네트워크 패킷 분석

- 와이어샤크 다운로드
  - <https://www.wireshark.org/#downloadLink>



# 네트워크 패킷 분석

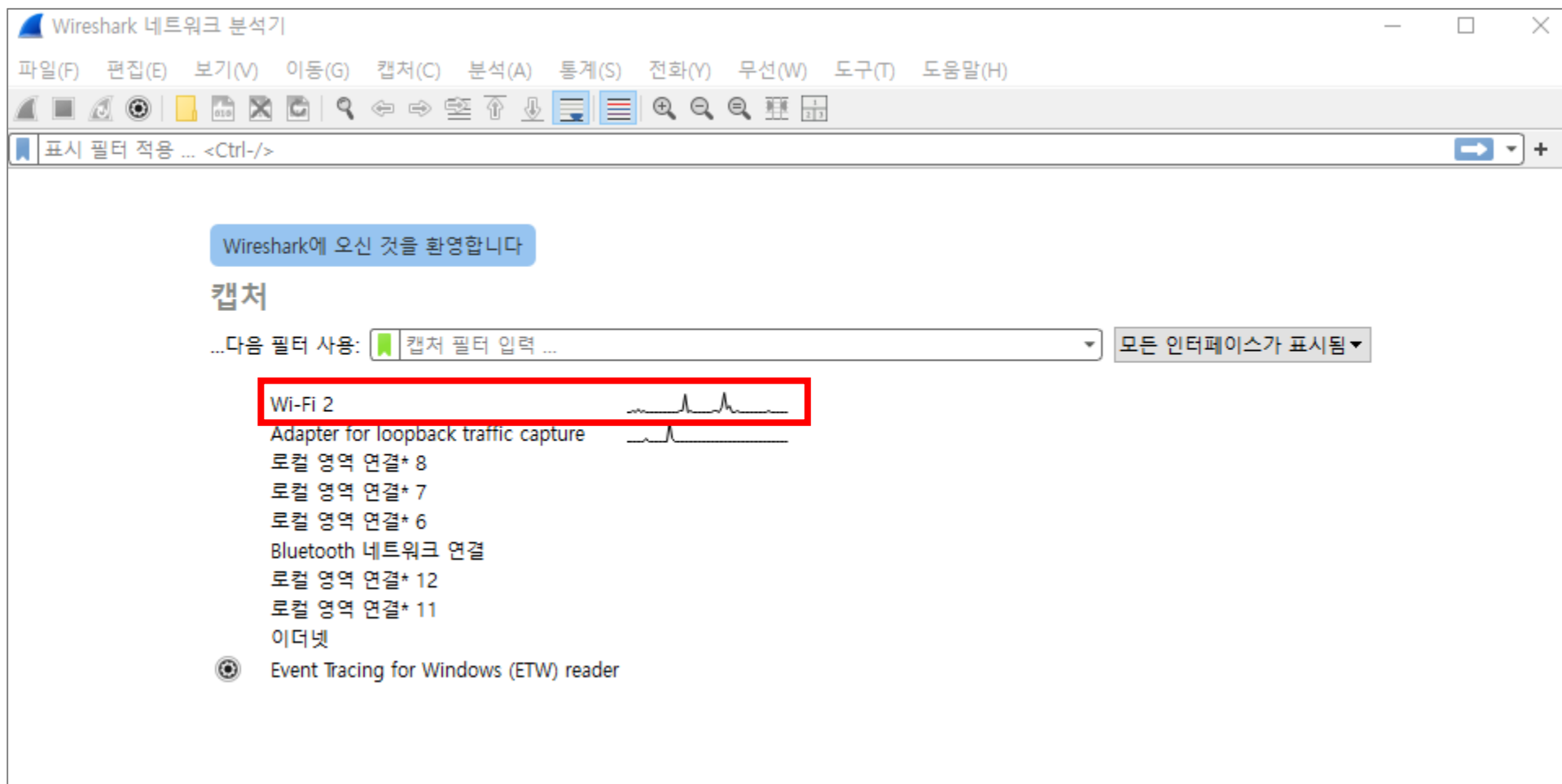
- 와이어샤크 설치
  - 기본 설정으로 모두 ok, next 선택하여 설치

The image displays a sequence of six screenshots from the Wireshark 4.4.0 x64 Setup and Npcap 1.79 Setup installers, illustrating the installation process. Red boxes highlight the 'Next >', 'Noted', and 'Install' buttons.

- Welcome to Wireshark 4.4.0 x64 Setup:** The first screen of the installer, showing a welcome message and a 'Next >' button.
- License Agreement:** The second screen, displaying the GNU General Public License (Version 2, June 1991) and a 'Noted' button.
- Choose Components:** The third screen, allowing the user to select components to install. The 'Wireshark' and 'TShark' components are selected, and the 'Next >' button is highlighted.
- Packet Capture:** The fourth screen, showing the 'Currently installed Npcap version' (Npcap 1.55) and the 'Install' button.
- Installing:** The fifth screen, showing the progress of the installation and the 'Next >' button.
- Installation Options:** The sixth screen, showing the 'Installation Options' for Npcap 1.79, including options to restrict access to Administrators only, support raw 802.11 traffic, and install Npcap in WinPcap API-compatible Mode. The 'Install' button is highlighted.

# 네트워크 패킷 분석

- 와이어샤크 실행하기



# 네트워크 패킷 분석

- 와이어샤크 시작하기
  - 시작화면: 캡처 자동 시작

Wi-Fi 2에서 캡처 중

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

표시 필터 적용 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	0.593788	192.168.0.37	172.217.174.110	UDP	75	62803 → 443 Len=33
9	0.701135	172.217.174.110	192.168.0.37	UDP	141	443 → 62803 Len=99
10	0.701135	172.217.174.110	192.168.0.37	UDP	291	443 → 62803 Len=249
11	0.701709	192.168.0.37	172.217.174.110	UDP	78	62803 → 443 Len=36
12	0.760365	172.217.174.110	192.168.0.37	UDP	66	443 → 62803 Len=24
13	1.241495	172.217.26.234	192.168.0.37	UDP	200	443 → 64650 Len=158
14	1.267897	211.115.106.207	192.168.0.37	TCP	54	80 → 53605 [FIN, ACK] Seq=1 Ack=1 Win=30 Len=0
15	1.268012	192.168.0.37	211.115.106.207	TCP	54	53605 → 80 [ACK] Seq=1 Ack=2 Win=511 Len=0
16	1.275610	192.168.0.37	172.217.26.234	UDP	74	64650 → 443 Len=32
17	2.036432	172.217.31.170	192.168.0.37	UDP	74	443 → 54031 Len=32
18	2.047939	192.168.0.37	172.217.31.170	UDP	75	54031 → 443 Len=33
19	2.214453	192.168.0.37	20.167.82.148	TLSv1.2	105	Application Data
20	2.341501	20.167.82.148	192.168.0.37	TLSv1.2	94	Application Data

< Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on 0  
> Ethernet II, Src: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4), Dst: EFMNet  
> Internet Protocol Version 4, Src: 192.168.0.37, Dst: 34.117.59.81  
> Transmission Control Protocol, Src Port: 53594, Dst Port: 80, Seq: 600000000

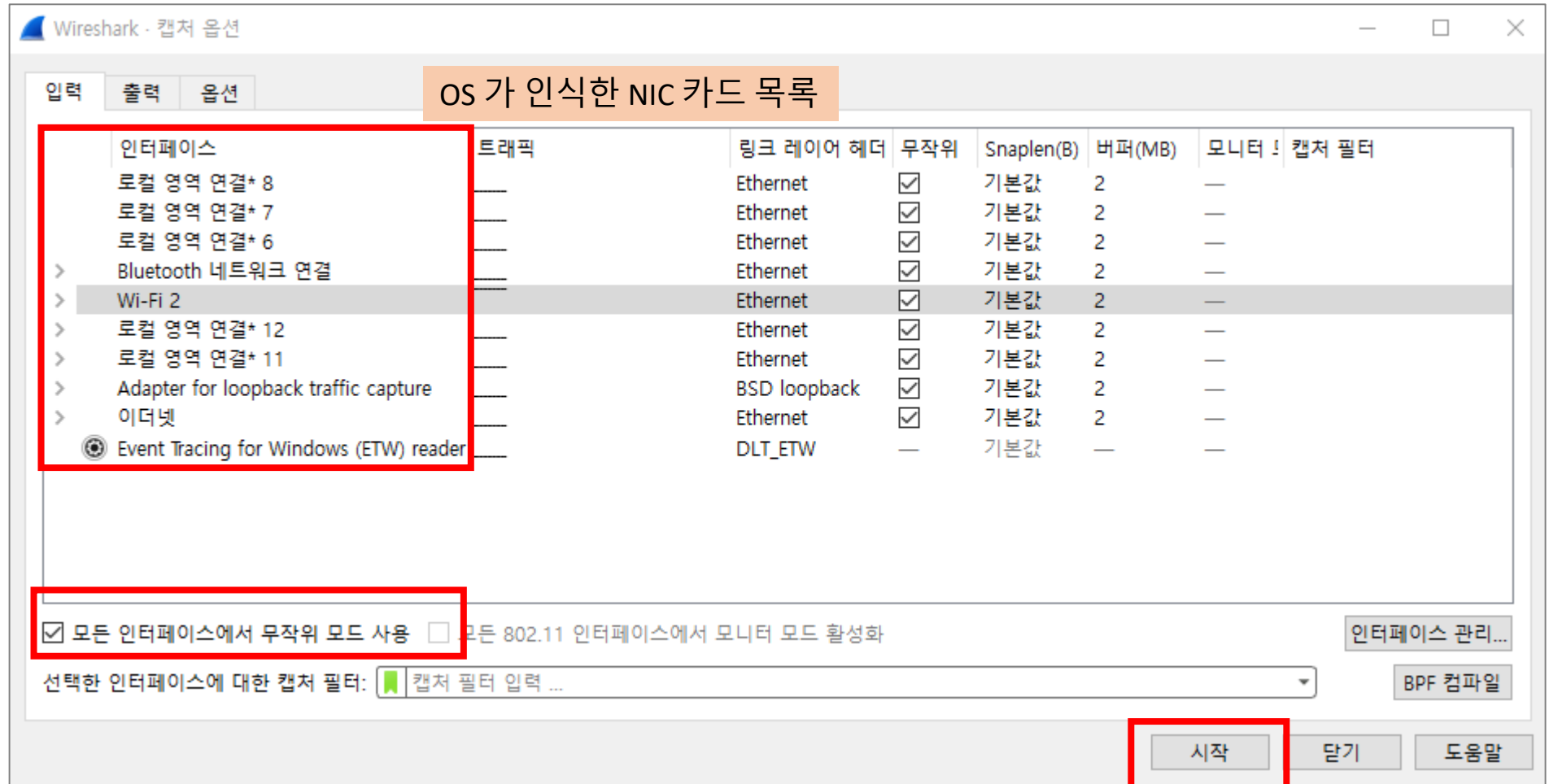
0000 90 9f 33 71 ef 50 20 0b d0 39 85 f4 08 00 45 00 ..3q·P · ·9···E·  
0010 00 34 57 67 40 00 80 06 84 c9 c0 a8 00 25 22 75 ·4wg@·· ····%u  
0020 3b 51 d1 5a 00 50 79 24 19 6e 00 00 00 00 80 02 ;Q·Z·Py\$ ·n·····  
0030 fa f0 f1 4e 00 00 02 04 05 b4 01 03 03 08 01 01 ···N··········  
0040 04 02 ..

Wi-Fi 2: <live capture in progress> 패킷: 20 프로파일: Default

# 네트워크 패킷 분석

- 와이어샤크 캡처 옵션

- 캡처 -> 옵션 메뉴 선택 -> 스니핑할 인터페이스 선택 -> 시작



# 네트워크 패킷 분석

- 와이어샤크를 이용한 프레임 캡처
  - 패킷 캡처 결과가 실시간 업데이트 됨.
  - 패킷 캡처 정지하려면 "캡처" -> "정지"

Wi-Fi 2에서 캡처 중

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

표시 필터 적용 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
120	6.837981	50.16.195.84	192.168.0.37	TCP	1514	443 → 53533 [ACK] Seq=10026 Ack=4755 Win=81920 Len=1460 [TCP PDU r
121	6.837981	50.16.195.84	192.168.0.37	TCP	1514	443 → 53533 [ACK] Seq=11486 Ack=4755 Win=81920 Len=1460 [TCP PDU r
122	6.837981	50.16.195.84	192.168.0.37	TCP	1514	443 → 53533 [ACK] Seq=12946 Ack=4755 Win=81920 Len=1460 [TCP PDU r
123	6.838026	192.168.0.37	50.16.195.84	TCP	54	53533 → 443 [ACK] Seq=4755 Ack=14406 Win=131328 Len=0
124	6.838061	50.16.195.84	192.168.0.37	TCP	1514	443 → 53533 [ACK] Seq=14406 Ack=4755 Win=81920 Len=1460 [TCP PDU r
125	6.838061	50.16.195.84	192.168.0.37	TCP	1514	443 → 53533 [ACK] Seq=15866 Ack=4755 Win=81920 Len=1460 [TCP PDU r
126	6.838061	50.16.195.84	192.168.0.37	TCP	1514	443 → 53533 [ACK] Seq=17326 Ack=4755 Win=81920 Len=1460 [TCP PDU r
127	6.838061	50.16.195.84	192.168.0.37	TLSv1.2	124	Application Data, Application Data
128	6.838103	192.168.0.37	50.16.195.84	TCP	54	53533 → 443 [ACK] Seq=4755 Ack=18856 Win=131328 Len=0
129	6.841314	192.168.0.37	210.125.88.1	DNS	79	Standard query 0xb3af A gates.grammarly.com
130	6.844795	210.125.88.1	192.168.0.37	DNS	175	Standard query response 0xb3af A gates.grammarly.com A 34.225.165.
131	6.845492	192.168.0.37	34.225.165.184	TCP	66	53534 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
132	7.040439	34.225.165.184	192.168.0.37	TCP	66	443 → 53534 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_P

Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0  
Ethernet II, Src: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4), Dst: EFMNet  
Internet Protocol Version 4, Src: 192.168.0.37, Dst: 52.123.254.201  
User Datagram Protocol, Src Port: 62564, Dst Port: 443  
Data (38 bytes)

0000 90 9f 33 71 ef 50 20 0b d0 39 85 f4 08 00 45 00 ..3q.P . .9...E.  
0010 00 42 fe 60 40 00 80 11 08 38 c0 a8 00 25 34 7b .B..@... .8...%4{  
0020 fe c9 f4 64 01 bb 00 2e 9b 2a 50 b4 34 7b fe c9 ...d... .\*P.4{..  
0030 4e be ea ad 6a 26 98 54 30 a2 9e d7 5b d3 83 d0 N...j&.T 0...[...  
0040 80 05 5e 91 c1 49 6f 2b a5 6d 44 09 7b 33 97 80 ...^..Io+ .mD.{3..

Wi-Fi 2: <live capture in progress> 패킷: 132 프로파일: Default

패킷 선택

패킷 데이터

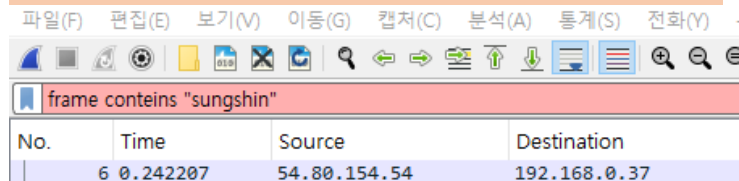
각 계층별 정보

# 네트워크 패킷 분석

- 와이어샤크를 이용한 프레임 캡처
  - Packet filtering: sungshin 이 포함된 frame 만 캡처

✓ Filter 입력란에 조건식 입력: frame contains "sungshin"

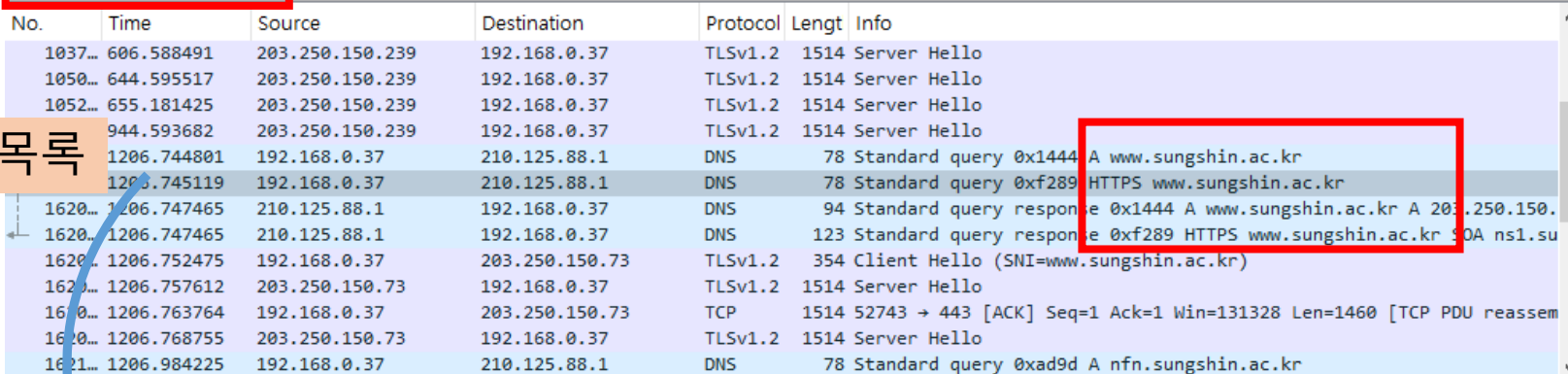
필터 입력 조건식이 틀리면 녹색



No.	Time	Source	Destination
6	0.242207	54.80.154.54	192.168.0.37

필터 입력 조건식이 형식에 맞다면 녹색

패킷 목록



No.	Time	Source	Destination	Protocol	Length	Info
1037...	606.588491	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
1050...	644.595517	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
1052...	655.181425	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
1094...	944.593682	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
1206...	1206.744801	192.168.0.37	210.125.88.1	DNS	78	Standard query 0x1444 A www.sungshin.ac.kr
1206...	1206.745119	192.168.0.37	210.125.88.1	DNS	78	Standard query 0xf289 HTTPS www.sungshin.ac.kr
1620...	1206.747465	210.125.88.1	192.168.0.37	DNS	94	Standard query response 0x1444 A www.sungshin.ac.kr A 203.250.150.239
1620...	1206.747465	210.125.88.1	192.168.0.37	DNS	123	Standard query response 0xf289 HTTPS www.sungshin.ac.kr 50A ns1.sungshin.ac.kr
1620...	1206.752475	192.168.0.37	203.250.150.73	TLSv1.2	354	Client Hello (SNI=www.sungshin.ac.kr)
1620...	1206.757612	203.250.150.73	192.168.0.37	TLSv1.2	1514	Server Hello
1620...	1206.763764	192.168.0.37	203.250.150.73	TCP	1514	52743 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembly completed]
1620...	1206.768755	203.250.150.73	192.168.0.37	TLSv1.2	1514	Server Hello
1621...	1206.984225	192.168.0.37	210.125.88.1	DNS	78	Standard query 0xad9d A nfn.sungshin.ac.kr

패킷 상세 정보

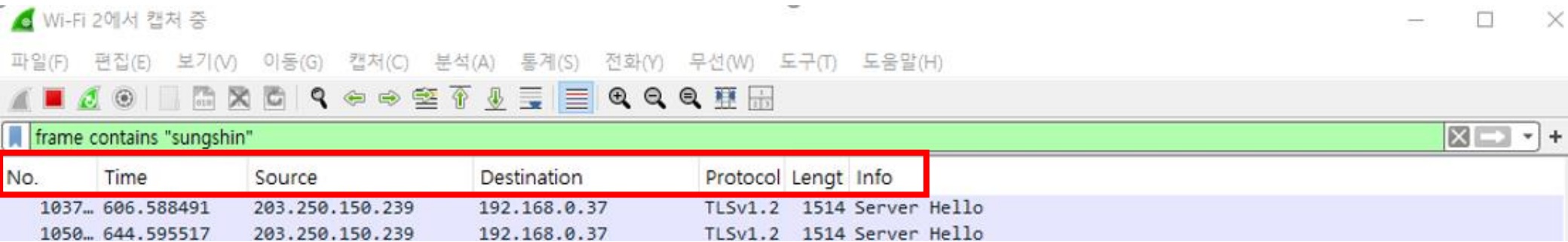
패킷 바이트

패킷 데이터



# 네트워크 패킷 분석

- 패킷 목록 정보에서 각 열의 디스플레이 내용



No.	Time	Source	Destination	Protocol	Lengt	Info
1037...	606.588491	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
1050...	644.595517	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello

열 이름	디스플레이 내용
No.	패킷의 일련 번호를 나타냄
Time	패킷을 캡처한 시간 정보
Source	패킷 발신지 상위층 주소
Destination	패킷 목적지 상위층 주소
Protocol	상위층 프로토콜 이름
Length	패킷 길이
Info	패킷 개요

# 네트워크 패킷 분석

## • 패킷 개요 정보와 상세 정보

> 상태 화면에서 패킷 개요 확인

```
> Frame 978: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on i
> Ethernet II, Src: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4), Dst: EFMNetworks_71:ef:5
> Internet Protocol Version 4, Src: 192.168.0.37, Dst: 3.208.85.212
> Transmission Control Protocol, Src Port: 52062, Dst Port: 443, Seq: 8609, Ack: 50
```

> 클릭하면 v로 바뀌고 상세 정보가 나타남

```
> Frame 978: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on i
> Ethernet II, Src: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4), Dst: EFMNetworks_71:ef:5
v Internet Protocol Version 4, Src: 192.168.0.37, Dst: 3.208.85.212
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 1500
        Identification: 0xb033 (45107)
    > 010. .... = Flags: 0x2, Don't fragment
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: TCP (6)
        Header Checksum: 0x2a77 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.37
        Destination Address: 3.208.85.212
        [Stream index: 19]
    > Transmission Control Protocol, Src Port: 52062, Dst Port: 443, Seq: 8609, Ack: 50
```

# 네트워크 패킷 분석

- 패킷 바이트 정보

주소  
(패킷의 위치)

16진수 덤프 (실제 데이터 내용)

ASCII 표시  
(데이터 내용을 문자로 표현)

0000	90 9f 33 71 ef 50 20 0b d0 39 85 f4 08 00 45 00	..3q.P . .9...E.
0010	05 dc b0 33 40 00 80 06 2a 77 c0 a8 00 25 03 d0	...3@... *w...%..
0020	55 d4 cb 5e 01 bb 16 7b 6b 4f 8d 93 d1 1f 50 10	U..^...{ k0...P.
0030	01 fc e6 f7 00 00 17 03 03 0f 73 00 00 00 00 00	.....s.....
0040	00 00 b6 85 1d ca bd 70 16 7c a2 5d df ac f4 46	.....p  .]...F
0050	9c ef 96 c3 9e ac 8c 22 8e fb ad cb e6 79 0b 3c	....." .....y.<
0060	aa 0d d5 83 ad 2c b5 69 11 38 26 ca 45 53 60 9f	....., .i .8&.ES`.
0070	08 c0 05 06 07 aa 3f e3 d1 51 2e aa 75 20 aa a5	.....? . Q. .u ..
0080	63 c2 df cb a9 c7 ff 3d f7 84 2c 8f 66 b0 03 30	c.....= .., .f..0
0090	49 9e 6a ea a2 13 dc c8 9e fd 3c 1e 40 dc e6 63	I.j..... <.@..c
00a0	56 e2 5d 52 99 47 55 4f 1e 3c a7 7e 52 3d fe db	V.]R.GUO <~R=...
00b0	7c af 03 9c 80 8e bc ba 93 36 b3 6c c3 be 46 78	..... .6.l..Fx
00c0	e3 de 7e 38 64 50 ed 81 82 68 6a 37 ac 87 c1 5b	..~8dP... .hj7...[
00d0	35 1b d0 fd db 65 b9 8e 97 b2 4e e5 b5 b5 e1 b4	5....e... .N.....
00e0	66 81 de 6b 40 94 45 4e b8 d7 df 57 c6 dd aa 62	f..k@.EN ...W...b
00f0	8b b7 39 d6 cd 39 fb 8d c4 8a 11 3c e4 11 1f cf	..9..9... <....

# 네트워크 패킷 분석

- 와이어샤크로 캡슐화된 패킷 분석하기

- 패킷 정보 창에서 Ethernet II 선택 → 우측에 Ethernet 정보

Wi-Fi 2에서 캡처 중

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

frame contains "sungshin"

No.	Time	Source	Destination	Protocol	Length	Info
511	14.188212	168.126.63.1	192.168.0.37	DNS	95	Standard query response 0xebb5 A ipsi.sungshin.ac.kr A 203.250.150.87
512	14.189556	168.126.63.1	192.168.0.37	DNS	124	Standard query response 0x9618 HTTPS ipsi.sungshin.ac.kr SOA ns1.sungshin
518	14.327915	192.168.0.37	168.126.63.1	DNS	79	Standard query 0x79c1 A ipsi.sungshin.ac.kr
519	14.328233	192.168.0.37	168.126.63.1	DNS	79	Standard query 0xb54a HTTPS ipsi.sungshin.ac.kr
520	14.331359	168.126.63.1	192.168.0.37	DNS	95	Standard query response 0x79c1 A ipsi.sungshin.ac.kr A 203.250.150.87
521	14.331359	168.126.63.1	192.168.0.37	DNS	124	Standard query response 0xb54a HTTPS ipsi.sungshin.ac.kr SOA ns1.sungshin
529	14.342870	192.168.0.37	203.250.150.87	TLSv1.2	323	Client Hello (SNI=ipsi.sungshin.ac.kr)
537	14.348366	203.250.150.87	192.168.0.37	TLSv1.2	1514	Server Hello
585	14.461537	192.168.0.37	203.250.150.87	TCP	1514	55450 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
688	14.558182	192.168.0.37	203.250.150.87	TCP	1514	55451 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
690	14.558750	192.168.0.37	203.250.150.87	TCP	1514	55452 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
37301	77.810945	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
37594	118.495010	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello

< Frame 537: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112) on interface 0

Ethernet II, Src: EFMNetworks\_71:ef:50 (90:9f:33:71:ef:50), Dst: 20:0b:00:00:00:00

Internet Protocol Version 4, Src: 203.250.150.87, Dst: 192.168.0.37

Transmission Control Protocol, Src Port: 443, Dst Port: 55448, Seq: 1, Len: 1514

Transport Layer Security

0000 20 0b d0 39 85 f4 90 9f 33 71 ef 50 08 00 45 00 ...9... 3q·P··E·  
0010 05 dc fd 6a 40 00 fb 06 59 91 cb fa 96 57 c0 a8 ...j@... Y...W·  
0020 00 25 01 bb d8 98 f1 11 6c 5c 51 eb 56 62 50 10 ·%····· l\Q·VbP·  
0030 3f c9 71 9d 00 00 16 03 03 00 5b 02 00 00 57 03 ?·q····· ·[...W·  
0040 03 ae d6 4f eb f6 90 07 52 d2 ab 34 f6 38 03 f4 ...O····· R·4·8·  
0050 ed d f1 6f df b6 eb ae ed 76 56 df b5 42 de 88 ...o····· vV··B·  
0060 0c 20 32 e8 34 02 86 2c a8 e6 1b b0 dc bd ef 75 ·2·4··, ······u  
0070 50 6f b0 9b 46 2d 61 a2 e6 c9 6d 55 ad 7c be 05 Po··F-a··mU·|·  
0080 f 00 00 0f ff 01 00 01 00 00 0b 00 02 .../·····  
0090 7 00 00 16 03 03 0e b2 0b 00 0e ae 00 .....  
00a0 6 81 30 82 06 7d 30 82 05 65 a0 03 02 .....0·· }0·e·  
00b0 01 02 02 10 0d 92 17 d1 f8 c1 1e dc 63 af f8 a2 .....c··  
00c0 68 47 0a 7b 30 0d 06 09 2a 86 48 86 f7 0d 01 01 hG·{0·· ·\*·H··  
00d0 0b 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02 ...0^1·0··U··  
00e0 55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 US1·0·· U···Dig  
00f0 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 iCert In c1·0··U  
0100 04 0b 13 10 77 77 72 2e 64 69 67 69 63 65 72 74 ...www. digicert  
0110 2e 63 6f 6d 31 1d 30 1b 06 03 55 04 03 13 14 54 .com1·0··U···T  
0120 68 61 77 74 65 20 54 4c 53 20 52 53 41 20 43 41 hawte TL S RSA CA

프레임데이터

# 네트워크 패킷 분석

- 와이어샤크로 캡슐화된 패킷 분석하기

- 프레임 정보 창에서 Internet Protocol Version 4 선택 → 우측에 IPv4 정보 됨

Wi-Fi 2에서 캡처 중

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

frame contains "sungshin"

No.	Time	Source	Destination	Protocol	Length	Info
511	14.188212	168.126.63.1	192.168.0.37	DNS	95	Standard query response 0xebb5 A ipsi.sungshin.ac.kr A 203.250.150.87
512	14.189556	168.126.63.1	192.168.0.37	DNS	124	Standard query response 0x9618 HTTPS ipsi.sungshin.ac.kr SOA ns1.sungshin
518	14.327915	192.168.0.37	168.126.63.1	DNS	79	Standard query 0x79c1 A ipsi.sungshin.ac.kr
519	14.328233	192.168.0.37	168.126.63.1	DNS	79	Standard query 0xb54a HTTPS ipsi.sungshin.ac.kr
520	14.331359	168.126.63.1	192.168.0.37	DNS	95	Standard query response 0x79c1 A ipsi.sungshin.ac.kr A 203.250.150.87
521	14.331359	168.126.63.1	192.168.0.37	DNS	124	Standard query response 0xb54a HTTPS ipsi.sungshin.ac.kr SOA ns1.sungshin
529	14.342870	192.168.0.37	203.250.150.87	TLSv1.2	323	Client Hello (SNI=ipsi.sungshin.ac.kr)
537	14.348366	203.250.150.87	192.168.0.37	TLSv1.2	1514	Server Hello
585	14.461537	192.168.0.37	203.250.150.87	TCP	1514	55450 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
688	14.558182	192.168.0.37	203.250.150.87	TCP	1514	55451 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
690	14.558750	192.168.0.37	203.250.150.87	TCP	1514	55452 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
37301	77.810945	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
37594	118.495010	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello

< >

> Frame 537: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
> Ethernet II, Src: EEMNetworks 71:ef:50 (90:9f:33:71:ef:50), Dst: 20:0b:00:00:00:00  
> Internet Protocol Version 4, Src: 203.250.150.87, Dst: 192.168.0.37  
> Transmission Control Protocol, Src Port: 443, Dst Port: 55448, Seq: 1, Len: 0  
> Transport Layer Security

0000 20 0b d0 39 85 f4 90 9f 33 71 ef 50 08 00 45 00 ...9... 3q·P·E·  
0010 05 dc fd 6a 40 00 fb 06 59 91 cb fa 96 57 c0 a8 ...j@... Y...W·  
0020 00 25 01 bb d8 98 f1 11 6c 5c 51 eb 56 62 50 10 ...%... l\Q·VbP·  
0030 31 c9 71 9d 00 00 16 03 03 00 5b 02 00 00 57 03 ...?·q... [·W·  
0040 03 ae d6 4f eb f6 90 07 52 d2 ab 34 f6 38 03 f4 ...·0... R·4·8·  
0050 0a 9d f1 6f df b6 eb ae ed 76 56 df b5 42 de 88 ...·o... vV·B·  
0060 fc 20 32 e8 34 02 86 2c a8 e6 1b b0 dc bd ef 75 ...·2·4·, ...u  
0070 5a 6f b0 9b 46 2d 61 a2 e6 c9 6d 55 ad 7c be 05 Po·F·a· ·mU·|·  
0080 2f 00 00 0f ff 01 00 01 00 00 0b 00 02 .../...  
0090 17 00 00 16 03 03 0e b2 0b 00 0e ae 00 ...  
00a0 06 81 30 82 06 7d 30 82 05 65 a0 03 02 ...·0... }0·e·  
00b0 01 02 02 10 0d 92 17 d1 f8 c1 1e dc 63 af f8 a2 ...·c·  
00c0 68 47 0a 7b 30 0d 06 09 2a 86 48 86 f7 0d 01 01 hG·{0... \*·H·  
00d0 0b 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02 ...0^1·0 ...U·  
00e0 55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 US1·0... U...Dig  
00f0 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 iCert In c1·0...U  
0100 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74 ...www. digicert  
0110 2e 63 6f 6d 31 1d 30 1b 06 03 55 04 03 13 14 54 .com1·0· ·U...T  
0120 68 61 77 74 65 20 54 4c 53 20 52 53 41 20 43 41 hawte TL S RSA CA

프레임데이터

# 네트워크 패킷 분석

- 와이어샤크로 캡슐화된 패킷 분석하기

- 프레임 정보 창에서 Transmission Control Protocol 선택 -> 우측에 TCP 정보

Wi-Fi 2에서 캡처 중

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

frame contains "sungshin"

No.	Time	Source	Destination	Protocol	Length	Info
511	14.188212	168.126.63.1	192.168.0.37	DNS	95	Standard query response 0xebb5 A ipsi.sungshin.ac.kr A 203.250.150.87
512	14.189556	168.126.63.1	192.168.0.37	DNS	124	Standard query response 0x9618 HTTPS ipsi.sungshin.ac.kr SOA ns1.sungshin
518	14.327915	192.168.0.37	168.126.63.1	DNS	79	Standard query 0x79c1 A ipsi.sungshin.ac.kr
519	14.328233	192.168.0.37	168.126.63.1	DNS	79	Standard query 0xb54a HTTPS ipsi.sungshin.ac.kr
520	14.331359	168.126.63.1	192.168.0.37	DNS	95	Standard query response 0x79c1 A ipsi.sungshin.ac.kr A 203.250.150.87
521	14.331359	168.126.63.1	192.168.0.37	DNS	124	Standard query response 0xb54a HTTPS ipsi.sungshin.ac.kr SOA ns1.sungshin
529	14.342870	192.168.0.37	203.250.150.87	TLSv1.2	323	Client Hello (SNI=ipsi.sungshin.ac.kr)
537	14.348366	203.250.150.87	192.168.0.37	TLSv1.2	1514	Server Hello
585	14.461537	192.168.0.37	203.250.150.87	TCP	1514	55450 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
688	14.558182	192.168.0.37	203.250.150.87	TCP	1514	55451 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
690	14.558750	192.168.0.37	203.250.150.87	TCP	1514	55452 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in
37301	77.810945	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello
37594	118.495010	203.250.150.239	192.168.0.37	TLSv1.2	1514	Server Hello

< >

> Frame 537: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112) on interface 0

> Ethernet II, Src: EFMNetworks\_71:ef:50 (90:9f:33:71:ef:50), Dst: 20:0b:0d:00:00:00

> Internet Protocol Version 4, Src: 203.250.150.87, Dst: 192.168.0.37

> **Transmission Control Protocol, Src Port: 443, Dst Port: 55448, Seq: 1**

> Transport Layer Security

프레임데이터

0000 20 0b d0 39 85 f4 90 9f 33 71 ef 50 08 00 45 00 ...9... 3q·P·E·

0010 05 dc fd 6a 40 00 fb 06 59 91 cb fa 96 57 c0 a8 ...j@... Y...W·

0020 00 25 01 bb d8 98 f1 11 6c 5c 51 eb 56 62 50 10 ...%..... 1\Q·VbP·

0030 3f c9 71 9d 00 00 16 03 03 00 5b 02 00 00 57 03 ...?·q..... [·W·

0040 03 ae d6 4f eb f6 90 07 52 d2 ab 34 f6 38 03 f4 ...·O..... R·4·8·

0050 ed 9d f1 6f df b6 eb ae ed 76 56 df b5 42 de 88 ...·o..... vV·B·

0060 fc 20 02 e8 34 02 86 2c a8 e6 1b b0 dc bd ef 75 ...·2·4·, .....u

0070 50 6f b0 9b 46 2d 61 a2 e6 c9 6d 55 ad 7c be 05 ...Po·F·a· ·mU·|·

0080 00 7f c0 2f 00 00 0f ff 01 00 01 00 00 0b 00 02 ...·/.....

0090 00 00 16 03 03 0e b2 0b 00 0e ae 00 ..... .....

00a0 31 30 82 06 7d 30 82 05 65 a0 03 02 .....0· }0·e·

00b0 0d 92 17 d1 f8 c1 1e dc 63 af f8 a2 ..... .....

00c0 68 47 0a 7b 30 0d 06 09 2a 86 48 86 f7 0d 01 01 ...hG·{0· ·\*·H·

00d0 0b 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02 ...·0^1·0 ··U·

00e0 55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 ...US1·0· ·U·Dig

00f0 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 ...iCert In c1·0·U

0100 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74 ...·www. digicert

0110 2e 63 6f 6d 31 1d 30 1b 06 03 55 04 03 13 14 54 ...·com1·0· ·U·T

0120 68 61 77 74 65 20 54 4c 53 20 52 53 41 20 43 41 ...hawte TL S RSA CA

- 와이어샹크로 캡슐화된 패킷 분석하기

Offset	Hex	ASCII
0000	20 0b d0 39 85 f4 90 9f 33 71 ef 50 08 00 45 00	· · 9 · · · · 3q · P · · E ·
0010	05 dc fd 6a 40 00 fb 06 59 91 cb fa 96 57 c0 a8	· · · j@ · · · Y · · · · W · ·
0020	00 25 01 bb d8 98 f1 11 6c 5c 51 eb 56 62 50 10	· % · · · · · 1 \ Q · VbP ·
0030	3f c9 71 9d 00 00 16 03 03 00 5b 02 00 00 57 03	? · q · · · · · · [ · · · W ·
0040	03 ae d6 4f eb f6 90 07 52 d2 ab 34 f6 38 03 f4	· · · O · · · · R · · 4 · 8 · ·
0050	ed 9d f1 6f df b6 eb ae ed 76 56 df b5 42 de 88	· · · o · · · · · · vV · · B · ·
0060	fc 20 32 e8 34 02 86 2c a8 e6 1b b0 dc bd ef 75	· 2 · 4 · · , · · · · · · · u
0070	50 6f b0 9b 46 2d 61 a2 e6 c9 6d 55 ad 7c be 05	Po · · F - a · · · mU ·   · ·
0080	a0 7f c0 2f 00 00 0f ff 01 00 01 00 00 0b 00 02	· · · / · · · · · · · · · ·
0090	01 00 00 17 00 00 16 03 03 0e b2 0b 00 0e ae 00	· · · · · · · · · · · · · ·
00a0	0e ab 00 06 81 30 82 06 7d 30 82 05 65 a0 03 02	· · · · · 0 · · } 0 · · e · ·
00b0	01 02 02 10 0d 92 17 d1 f8 c1 1e dc 63 af f8 a2	· · · · · · · · · · · · c · ·
00c0	68 47 0a 7b 30 0d 06 09 2a 86 48 86 f7 0d 01 01	hG · { 0 · · · * · H · · · ·
00d0	0b 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02	· · · 0 ^ 1 · 0 · · · U · · ·
00e0	55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67	US1 · 0 · · · U · · · · Dig
00f0	69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55	iCert In c1 · 0 · · · U
0100	04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74	· · · · www · digicert
0110	2e 63 6f 6d 31 1d 30 1b 06 03 55 04 03 13 14 54	· com1 · 0 · · · U · · · · T
0120	68 61 77 74 65 20 54 4c 53 20 52 53 41 20 43 41	hawte TL S RSA CA

# 네트워크 패킷 분석

- Ethernet 프로토콜 프레임 캡처하고 분석하기
  - ipconfig /all 로 내 컴퓨터의 MAC주소 확인

 명령 프롬프트

무선 LAN 어댑터 Wi-Fi 2:

```
연결별 DNS 접미사. . . . . :
설명. . . . . : Realtek 8821CU Wireless LAN 802.11ac USB NIC
물리적 주소. . . . . : 20-0B-D0-39-85-F4
DHCP 사용. . . . . : 예
자동 구성 사용. . . . . : 예
링크-로컬 IPv6 주소. . . . . : fe80::ef7f:55f8:f98c:1e84%7(기본 설정)
IPv4 주소. . . . . : 192.168.0.37(기본 설정)
서브넷 마스크. . . . . : 255.255.255.0
임대 시작 날짜. . . . . : 2024년 10월 5일 토요일 오후 2:52:46
임대 만료 날짜. . . . . : 2024년 10월 5일 토요일 오후 8:52:48
기본 게이트웨이. . . . . : 192.168.0.1
DHCP 서버. . . . . : 192.168.0.1
DHCPv6 IAID. . . . . : 455085008
DHCPv6 클라이언트 DUID. . . . . : 00-01-00-01-27-F7-21-F9-3C-7C-3F-ED-3A-00
DNS 서버. . . . . : 210.125.88.1
                  168.126.63.1
Tcpip를 통한 NetBIOS. . . . . : 사용
```



# 네트워크 패킷 분석

- Ethernet 프로토콜 프레임 캡처하고 분석하기
  - 와이어샤크 필터에 다음의 조건식 입력: eth.src==컴퓨터의MAC주소

\*Wi-Fi 2

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

eth.src==20-0B-D0-39-85-F4

No.	Time	Source	Destination	Protocol	Length	Info
1557...	3086.481811	192.168.0.37	43.250.152.22	TLSv1.3	89	Application Data
1558...	3086.482873	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3416463 Win=1053952 Len=0
1558...	3086.482999	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3417923 Win=1053952 Len=0
1558...	3086.483726	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3420843 Win=1053952 Len=0
1558...	3086.483795	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3421764 Win=1053184 Len=0
1558...	3086.551099	192.168.0.37	172.217.175.3	QUIC	77	Protected Payload (KP0), DCID=f74bcbfda55670d2
1558...	3086.576915	192.168.0.37	172.217.175.3	QUIC	75	Protected Payload (KP0), DCID=f74bcbfda55670d2
1558...	3086.607876	192.168.0.37	20.194.180.207	TCP	55	[TCP Keep-Alive] 53117 → 443 [ACK] Seq=1717 Ack=1535 Win=513 Len=1
1558...	3086.965616	20:0b:d0:39:85:f4	EFMNetworks_71:ef:50	ARP	42	192.168.0.37 is at 20:0b:d0:39:85:f4
1558...	3087.678467	192.168.0.37	52.6.63.136	TCP	54	56703 → 443 [ACK] Seq=4141 Ack=33490 Win=131072 Len=0

> Frame 155796: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on 0

> Ethernet II, Src: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4), Dst: EFMNetworks\_71:ef:50

> Internet Protocol Version 4, Src: 192.168.0.37, Dst: 43.250.152.22

> Transmission Control Protocol, Src Port: 55841, Dst Port: 443, Seq: 200

> Transport Layer Security

```
0000  90 9f 33 71 ef 50 20 0b d0 39 85 f4 08 00 45 00  ..3q.P. .9...E.
0010  00 4b 4d 26 40 00 80 06 28 a9 c0 a8 00 25 2b fa  .KM&@... (....%+
0020  98 16 da 21 01 bb 4e 52 c8 ad 36 8e e9 ca 50 18  ...!...NR ..6...P.
0030  10 10 2e e4 00 00 17 03 03 00 1e d7 3d 14 9d 4e  ..,... ..==...N
0040  0c 14 da 20 a7 9b 79 89 42 96 7f c0 82 59 9a 96  ... .y. B....Y..
0050  fa b2 28 03 4d 5f 2d ae 41                        ..(·M_· A
```

# 네트워크 패킷 분석

- Ethernet 프로토콜 프레임 캡처하고 분석하기
  - Ethernet II 부분 더블클릭해서 확장하여 destination address, source address, type 정보 확인하기

\*Wi-Fi 2

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

eth.src==20-0B-D0-39-85-F4

No.	Time	Source	Destination	Protocol	Length	Info
1557...	3086.481811	192.168.0.37	43.250.152.22	TLSv1.3	89	Application Data
1558...	3086.482873	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3416463 Win=1053952 Len=0
1558...	3086.482999	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3417923 Win=1053952 Len=0
1558...	3086.483726	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3420843 Win=1053952 Len=0
1558...	3086.483795	192.168.0.37	43.250.152.22	TCP	54	55841 → 443 [ACK] Seq=20109 Ack=3421764 Win=1053184 Len=0
1558...	3086.551099	192.168.0.37	172.217.175.3	QUIC	77	Protected Payload (KP0), DCID=f74bcbfda55670d2
1558...	3086.576915	192.168.0.37	172.217.175.3	QUIC	75	Protected Payload (KP0), DCID=f74bcbfda55670d2
1558...	3086.607876	192.168.0.37	20.194.180.207	TCP	55	[TCP Keep-Alive] 53117 → 443 [ACK] Seq=1717 Ack=1535 Win=513 Len=1
1558...	3086.965616	20:0b:d0:39:85:f4	EFMNetworks_71:ef:50	ARP	42	192.168.0.37 is at 20:0b:d0:39:85:f4
1558...	3087.678467	192.168.0.37	52.6.63.136	TCP	54	56703 → 443 [ACK] Seq=4141 Ack=33490 Win=131072 Len=0

< >

> Frame 155796: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)

▼ Ethernet II, Src: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4), Dst: EFMNetworks\_71:ef:50 (90:9f:33:71:ef:50)

Destination: EFMNetworks\_71:ef:50 (90:9f:33:71:ef:50)

Source: 20:0b:d0:39:85:f4 (20:0b:d0:39:85:f4)

Type: IPv4 (0x0800)

[Stream index: 0]

> Internet Protocol Version 4, Src: 192.168.0.37, Dst: 43.250.152.22

> Transmission Control Protocol, Src Port: 55841, Dst Port: 443, Seq: 200

> Transport Layer Security

< >

0000 90 9f 33 71 ef 50 20 0b d0 39 85 f4 08 00 45 00 ...3q·P··9···E·

0010 00 4b 4d 26 40 00 80 06 28 a9 c0 a8 00 25 2b fa ·KM&@···(···%+·

0020 98 16 da 21 01 bb 4e 52 c8 ad 36 8e e9 ca 50 18 ···!··NR··6··P·

0030 10 10 2e e4 00 00 17 03 03 00 1e d7 3d 14 9d 4e ············=·N

0040 0c 14 da 20 a7 9b 79 89 42 96 7f c0 82 59 9a 96 ····y·B····Y·

0050 fa b2 28 03 4d 5f 2d ae 41 ··(·M\_··A

Ethernet (eth), 14바이트

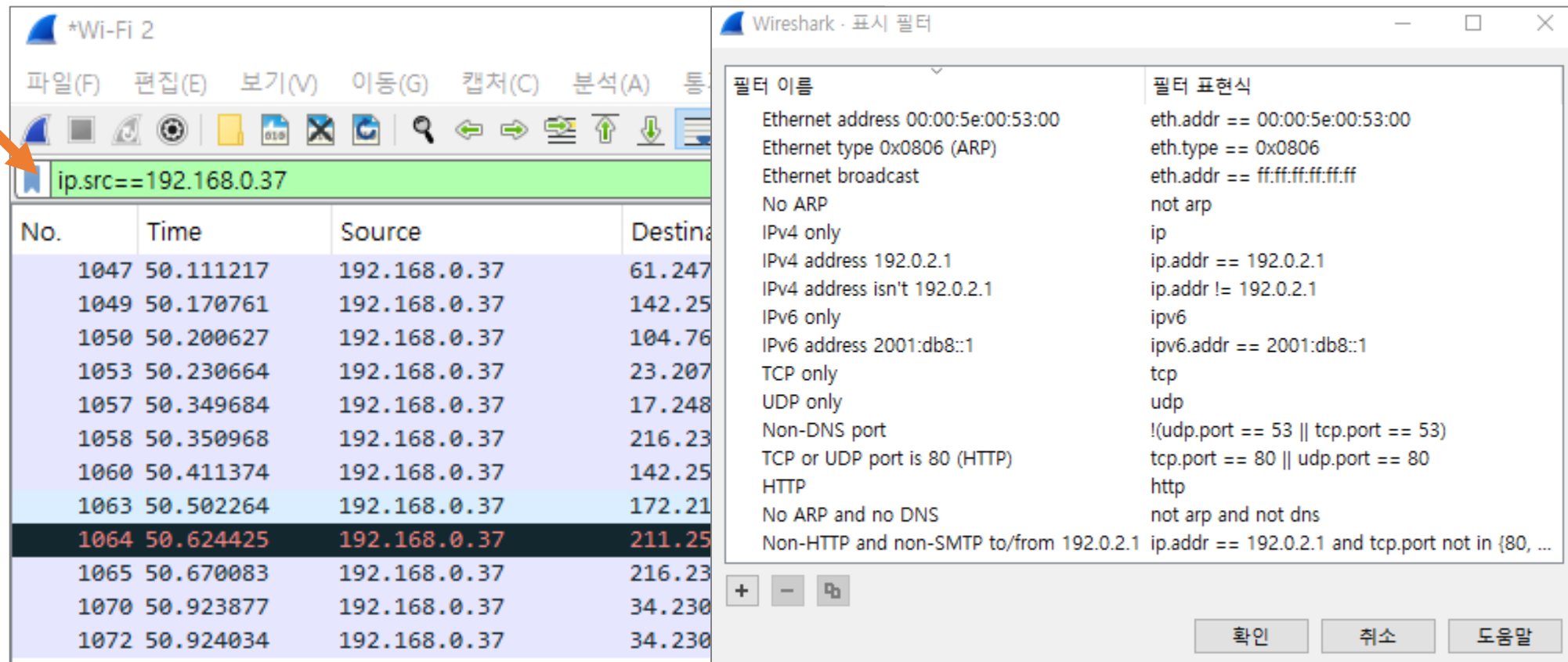
패킷: 155832 개 표시됨: 57381(36.8%) · 누락됨: 0(0.0%) | 프로파일: Default

# 네트워크 패킷 분석

- 와이어샤크 필터 고급 기능

- 필터 프로필: 디스플레이 필터의 입력란의 좌측 “Filter” 버튼 클릭

- ✓ 자주 사용하는 필터 정의 등록되어 있음.



The image shows the Wireshark network protocol analyzer interface. On the left, the packet list pane displays a table of captured packets. The filter bar at the top of this pane shows the active filter `ip.src==192.168.0.37`, with an orange arrow pointing to the 'Filter' button on its left. On the right, the 'Wireshark - 표시 필터' (Wireshark - Display Filter) dialog box is open, showing a list of predefined filters and their corresponding expressions.

필터 이름	필터 표현식
Ethernet address 00:00:5e:00:53:00	<code>eth.addr == 00:00:5e:00:53:00</code>
Ethernet type 0x0806 (ARP)	<code>eth.type == 0x0806</code>
Ethernet broadcast	<code>eth.addr == ff:ff:ff:ff:ff:ff</code>
No ARP	<code>not arp</code>
IPv4 only	<code>ip</code>
IPv4 address 192.0.2.1	<code>ip.addr == 192.0.2.1</code>
IPv4 address isn't 192.0.2.1	<code>ip.addr != 192.0.2.1</code>
IPv6 only	<code>ipv6</code>
IPv6 address 2001:db8::1	<code>ipv6.addr == 2001:db8::1</code>
TCP only	<code>tcp</code>
UDP only	<code>udp</code>
Non-DNS port	<code>!(udp.port == 53    tcp.port == 53)</code>
TCP or UDP port is 80 (HTTP)	<code>tcp.port == 80    udp.port == 80</code>
HTTP	<code>http</code>
No ARP and no DNS	<code>not arp and not dns</code>
Non-HTTP and non-SMTP to/from 192.0.2.1	<code>ip.addr == 192.0.2.1 and tcp.port not in {80, ...}</code>

# 네트워크 패킷 분석

## • 와이어샤크 필터 고급 기능

비교	==	<ul style="list-style-type: none"> <li>• 같다는 의미</li> <li>• ip.addr==192.168.1.1 // IP 주소가 192.168.1.1 의 패킷</li> </ul>
	!=	<ul style="list-style-type: none"> <li>• 같지 않다는 의미</li> <li>• ip.addr!=192.168.1.1 // IP 주소가 192.168.1.1 이 아닌 패킷</li> </ul>
	>,<,>=,<=	<ul style="list-style-type: none"> <li>• 비교의 뜻으로서, 각각 크다, 작다, 크거나 같다, 작거나 같다는 의미.</li> <li>• tcp.port &gt; 1024 // TCP 포트 번호가 1024 번 보다 큰 패킷.</li> </ul>
논리	&&	<ul style="list-style-type: none"> <li>• "그리고"의 의미</li> <li>• ip.src==192.168.2.5 &amp;&amp; tcp.scrport==80 // 송신 IP 주소 192.168.2.5 이면서 TCP 포트 80인 패킷.</li> </ul>
		<ul style="list-style-type: none"> <li>• "또는"의 의미</li> <li>• ip.dst==192.168.2.5    ip.dst==192.168.2.8 // 수신측 IP 주소가 192.168.2.5 또는 192.168.2.8 인 패킷.</li> </ul>
	^^	<ul style="list-style-type: none"> <li>• XOR 의 의미</li> <li>• ip.src==168.2.5 ^^ tcp.scrport==80 // "송신측 IP 주소가 192.168.2.5 이면서 송신측 TCP 포트 80번이 아닌 패킷" 과 "송신측 IP 주소가 192.168.2.5가 아니면서 송신측 TCP 포트 80번인 패킷"</li> </ul>
	!	<ul style="list-style-type: none"> <li>• 부정</li> <li>• !tcp // TCP 이외의 패킷</li> </ul>

# 네트워크 패킷 분석



- 와이어샤크 필터 고급 기능

필터	의미
ip.src == IP 주소	소스 IP 주소가 지정한 IP 주소인 패킷 표시
ip.dst == IP 주소	목적지 IP 주소가 지정한 IP 주소인 패킷 표시
ip.addr==IP주소	소스 혹은 목적지 IP 주소가 지정한 IP 주소인 패킷 표시.
ip.addr==IP주소1 && ip.addr==IP주소2	IP 주소1과 IP주소 2간 주고 받는 패킷 표시.
http or dns	HTTP 또는 DNS 패킷 표시
tcp.port==포트번호	지정한 포트 번호가 송신측 또는 수신측 패킷인 것 표시.
tcp contains <문자열>	지정한 문자열을 포함하는 TCP 패킷 표시
tcp.flags.syn==1	TCP 의 SYN 패킷만을 표시

# 네트워크 패킷 분석

## • 와이어샤크 필터 고급 기능: 패킷 마킹

The image shows the Wireshark interface with a packet capture running. The packet list pane shows several packets, including a TCP ACK packet (No. 978). The packet details pane shows the structure of the selected packet. The packet bytes pane shows the raw data. The 'Packet Marking' (패킷 마킹) menu is open, showing options like 'Select and mark packets (M)' (선택 항목 마크/해제(M)), 'Select and unmark packets (U)' (선택 항목 표시/해제(U)), 'Time-based filtering' (시간 기반 필터링), 'Tag packets' (패킷 주석), and 'Export selected packets' (해석된 이력 편집).

< 패킷 마킹 후 >

< 패킷 마킹 전 >

The image shows the Wireshark interface after packet marking. The packet list pane shows the same packets as before, but the selected packet (No. 978) is now highlighted in red. The packet details pane shows the structure of the selected packet. The packet bytes pane shows the raw data. The status bar at the bottom indicates that 1072 packets are displayed (482.05% of the total).

---

# Q&A

