

4차 산업혁명과 함께하는 네트워크

네트워크 개론 3판

진혜진 지음



Chapter 01. 네트워크의 이해

목차

1. 네트워크 이해
2. 네트워크 분석 도구 설치
3. 네트워크 설정

01. 네트워크 이해

1. 네트워크의 개념

■ 네트워크의 사전적 의미

- 모뎀이나 LAN, 케이블, 무선매체 등 통신설비를 갖춘 컴퓨터로 서로 연결하는 조직이나 체계, 통신망이다.
- 즉, 통신설비들로 두 대 이상의 컴퓨터를 서로 연결한 것을 말한다. 컴퓨터 두 대로 연결했든, 그 이상으로 연결했든 간에 필요에 따라 여러 대를 서로 연결한 것이 바로 네트워크인 셈이다.

■ 데이터 공유

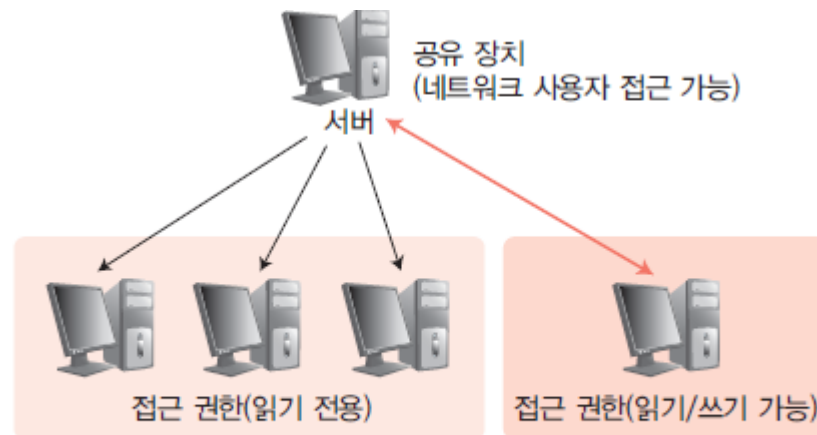


그림 1-1 데이터의 동시 접근

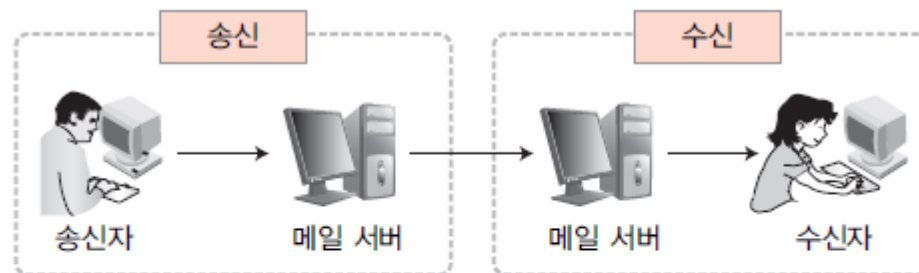
01. 네트워크 이해

■ 주변장치 공유



그림 1-2 프린터 공유

■ 능률적인 통신



- 1 송신자가 이메일을 보낸다.
- 2 메시지가 서버에 저장된다.
- 3 서버가 수신자에게 메시지가 있음을 알린다.
- 4 수신자가 서버에서 메시지를 검색하여 이메일을 읽는다.

그림 1-3 이메일 송수신 과정

01. 네트워크 이해

■ 손쉬운 백업



그림 1-4 구글 드라이브 백업

01. 네트워크 이해

2. 데이터 전송 규칙

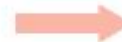
- 컴퓨터 한 대는 네트워크라고 할 수 없지만 컴퓨터가 두 대 이상 연결되어 있으면 컴퓨터 네트워크가 되고 컴퓨터간에 데이터를 주고받을 수 있다.
- 웹 사이트에 접속하는 것은 물론이고 네트워크나 인터넷에서 데이터를 주고 받는 데에는 규칙이 필요하다.

(1) 패킷

- 패킷은 컴퓨터 간에 데이터를 주고받을 때 네트워크를 통해 전송되는 데이터 전송단위(작은 조각)이다. 용량이 큰 데이터를 전송할 때는 작게 나누어서 보내는 것이 규칙.



패킷으로 분할한다.



모두 패킷으로 만든다.

용량이 큰 데이터는 패킷으로 분할해서 전송한다.

그림 1-5 용량이 큰 데이터의 패킷 분할

01. 네트워크 이해

- 분할된 패킷을 수신지로 전송할 때 네트워크 상황에 따라 전송한 순서대로 도착하지 않을 수도 있기 때문에 수신지에서는 분할된 패킷을 원래대로 재결합하는 작업을 해야 한다. 또한 패킷이 전송될 때 네트워크가 지연되면 패킷이 늦게 도착하거나 손실될 수도 있다.
- 다음 그림과 같이 패킷은 순서 없이 랜덤으로 수신지에 도착한다. 그러나 송신 측에서 각 패킷에 순서대로 번호를 붙여서 전송하고 수신 측에서는 번호에 맞춰 재조립함으로써 각 패킷이 원래 위치에 자리 잡을 수 있다. 마지막 패킷이 도착한 후 사진 전체의 패킷을 번호 순서로 정렬하면 송신 측에서 보낸 원래의 사진이 되는 것이다.

01. 네트워크 이해



그림 1-6 패킷 재조립

(2) 패킷 전송 과정

- 패킷은 헤더, 페이로드 payload, 제어 요소 등을 포함하는 데이터 세그먼트이다. 헤더는 데이터의 형태와 데이터의 송수신지, 일련번호 등으로 구성되고, 페이로드는 실제 전송 데이터를 포함하는 부분이다.
- 영문 성 Jin을 메신저로 전송할 때 패킷이 전송되는 과정을 간단히 살펴보자. 각 문자에 해당하는 이진 값은 다음과 같다.

01. 네트워크 이해

J: 1001010
i: 1101001
n: 1101110

❶ Jin이라는 데이터를 전송할 때 다음과 같이 패킷으로 분할해서 전송한다. 헤더의 일련번호는 이해하기 쉽게 간단한 숫자로 가정한다. 홀수 패리티 방식을 적용한다(3장 참고).

1	01001010	
2	11101001	
3	01101110	

❷ 전송된 데이터는 네트워크 상황에 따라 랜덤으로 도착한다. 다음은 inJ 형태로 도착한 경우이다.

2	11101001	
3	01101110	
1	01001010	

❸ 수신 측에 도착한 패킷은 헤더의 일련번호가 재조립되어 원래의 데이터인 Jin이 된다.

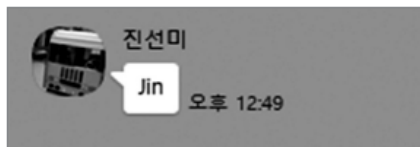


그림 1-7 SNS 전송 데이터

01. 네트워크 이해

3. 비트와 바이트

- 모든 컴퓨터는 2진수 0과 1을 다루며, 0과 1의 집합을 디지털 데이터라고 한다. [그림 1-5]의 사진도 0과 1만으로는 나타낼 수 없지만 0과 1이 많이 모이면 나타낼 수 있다. 0과 1의 정보를 나타내는 최소 단위를 비트 bit라고 한다. 비트는 0 또는 1을 모아서 나타낼 수 있으며, 8비트를 1바이트 byte라고 한다. 컴퓨터는 이러한 바이트 단위로 데이터를 읽고 쓰는 작업을 한다.



그림 1-8 비트와 바이트

- 컴퓨터는 0과 1의 집합으로만 다루며, 키보드로 문자를 입력할 수 있는 것은 숫자와 문자의 대응 표인 문자 코드가 정해져 있기 때문이다. 웹 사이트에 접속했을 때 간혹 문자가 깨져 보이기도 하는데 이는 해당 문자 코드가 원인인 경우가 많다. 아스키코드 ASCII code는 숫자, 기호, 알파벳을 다룰 수 있는 기본적인 문자 코드이다. 예를 들어 키보드의 A를 누르면 컴퓨터로 문자 코드가 전달되고, 컴퓨터는 A에 대응하는 문자 코드인 65를 확인하고 화면에 A를 표시한다. 사진과 마찬가지로 문자도 수신 측으로 문자에 해당하는 이진 값을 패킷으로 나누어 보내면 수신 측에서 패킷을 원래의 값으로 되돌린다.

02. 네트워크 분석도구 설치

1. 네트워크 분석 도구의 필요성

- 네트워크 분석 도구는 크게 하드웨어 분석 도구와 소프트웨어 분석 도구로 구분할 수 있다.
- 하드웨어 분석 도구는 들고 다닐 수 있는 휴대 형태로, 네트워크에 직접 연결하여 패킷을 확인하거나 네트워크의 상태를 확인할 수 있다. 가격이 비싼편이어서 주로 기업에서 사용하며 사내 네트워크 시스템 관리 등에 이용한다.
- 소프트웨어 분석 도구는 컴퓨터나 서버에 설치하여 네트워크 인터페이스 카드를 통해 네트워크에 접속한다. 오픈 소스 소프트웨어 분석 도구는 무료이므로 개인이나 학교뿐만 아니라 기업도 자유롭게 이용할 수 있다.
- 네트워크 분석 도구가 필요한 장에서는 와이어샹크를 이용하여 직접 패킷을 캡처하는 방법을 확인할 수 있다. 네트워크의 기본 통신 내용을 와이어샹크를 이용한 분석으로 시작한다면 흥미롭게 네트워크에 다가갈 수 있을 것이다.

02. 네트워크 분석도구 설치

1) 와이어샤크 홈페이지(<https://www.wireshark.org/>)에 접속한다.

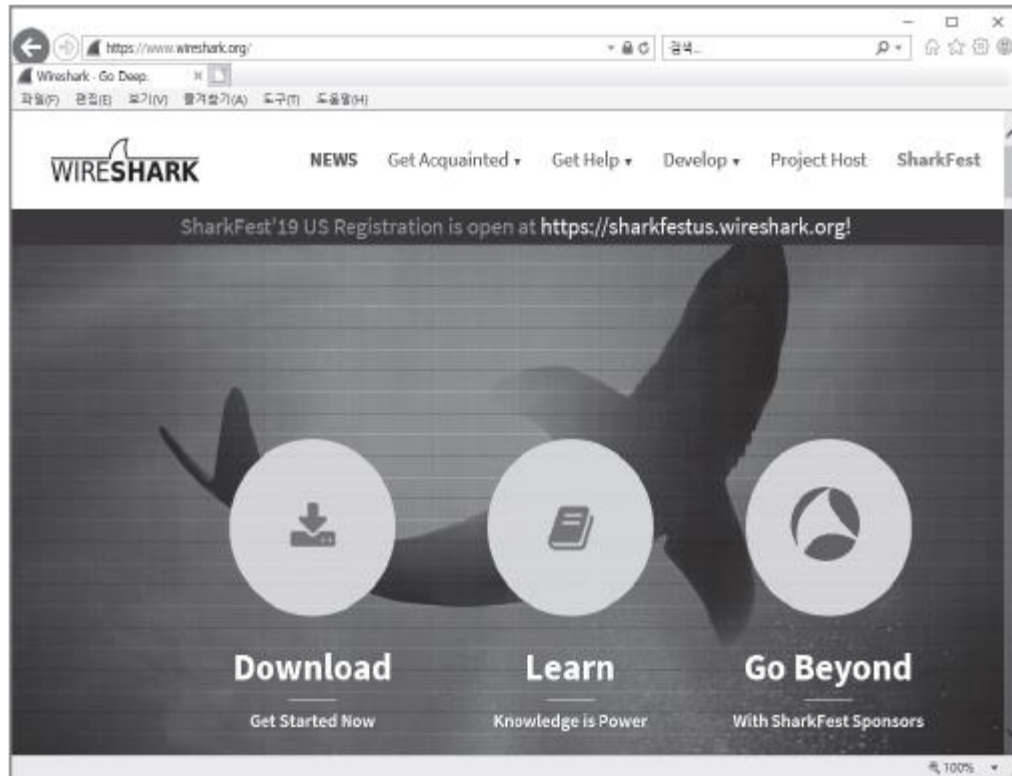


그림 1-9 와이어샤크 홈페이지 접속

02. 네트워크 분석도구 설치

2) <Download>를 클릭한 후 'Windows Installer(64-bit)'를 선택한다. 만약 32비트 윈도우 운영체제를 사용하고 있다면 'Windows Installer(32-bit)'를 선택한다.

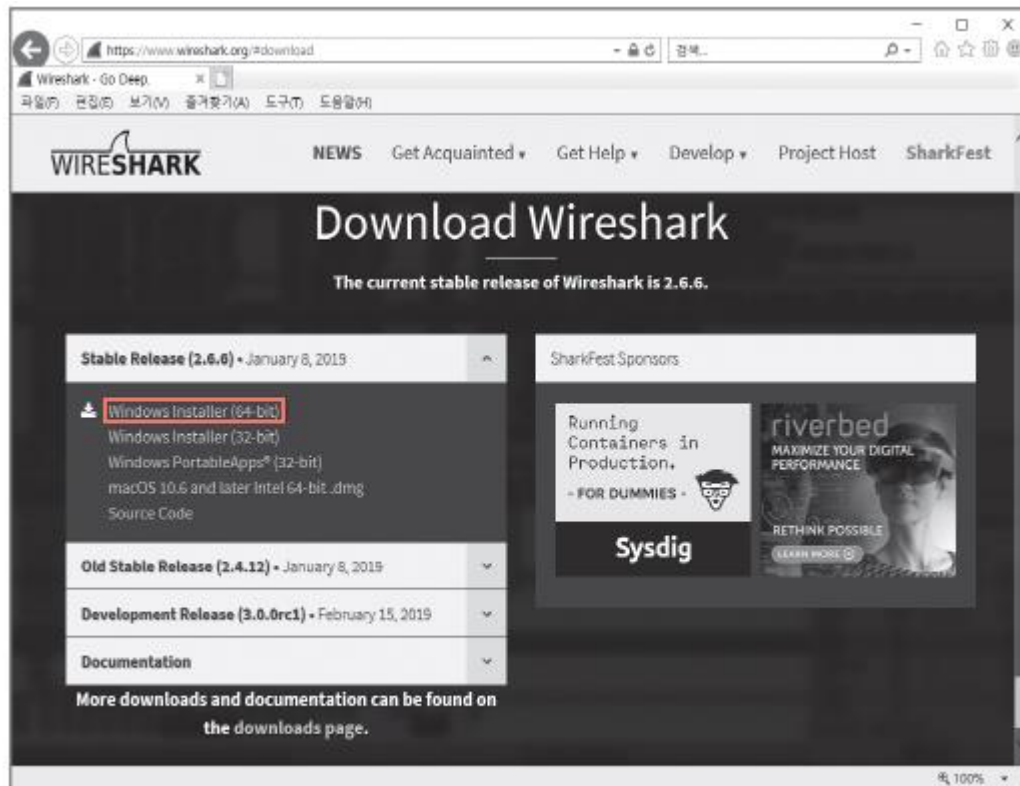


그림 1-10 'Windows Installer(64-bit)' 선택

02. 네트워크 분석도구 설치

NOTE 와이어샤크 버전이 계속 업데이트되고 있기 때문에 설치 시점에 이 책과 버전이 다를 수도 있다. 이 책에서는 패킷 분석의 기본적인 내용을 다루기 때문에 버전이 달라도 상관없다.

컴퓨터에 설치하지 않고 USB에 설치하는 경우 'Windows PortableApps®(32-bit)'를 다운로드하면 된다.

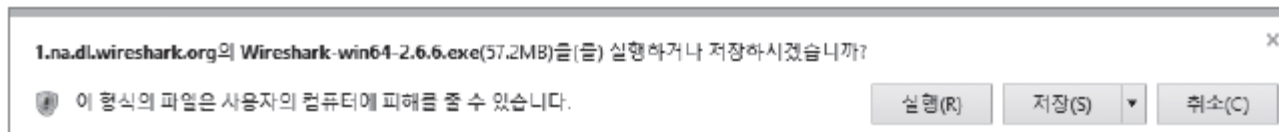


그림 1-11 실행 파일

컴퓨터 시스템 종류는 [제어판]-[시스템 및 보안]-[시스템]에서 확인할 수 있다.

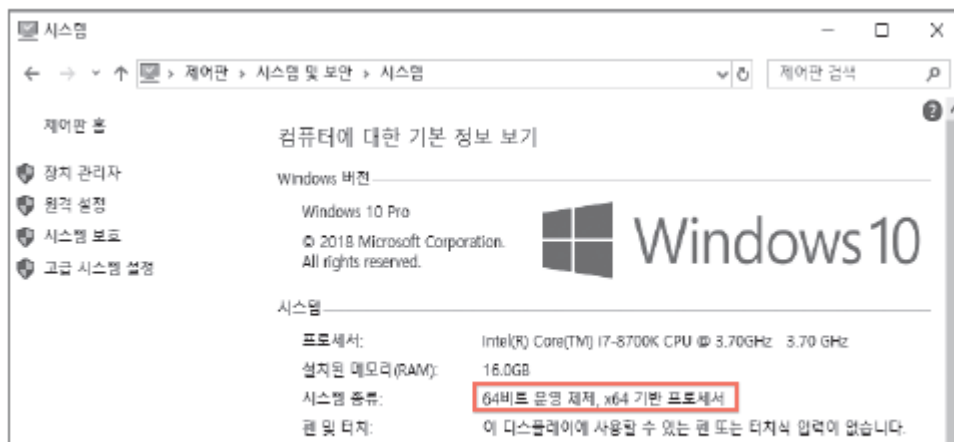


그림 1-12 시스템 종류

02. 네트워크 분석도구 설치

3) 와이어 샤크 설치 화면에서 <NEXT>를 클릭한다.

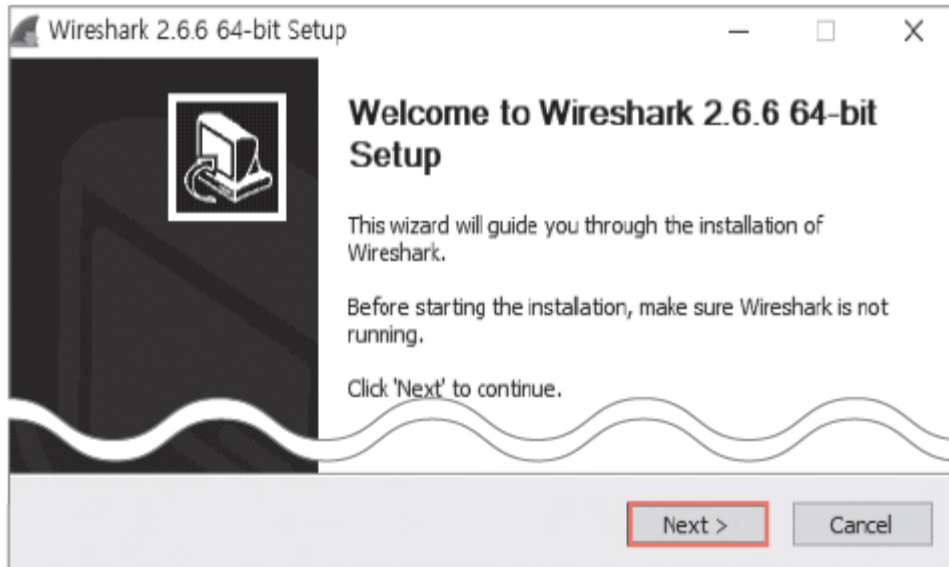


그림 1-13 와이어샤크 설치 화면

02. 네트워크 분석도구 설치

4) 라이선스 동의 화면에서 <I Agree>를 클릭한다.

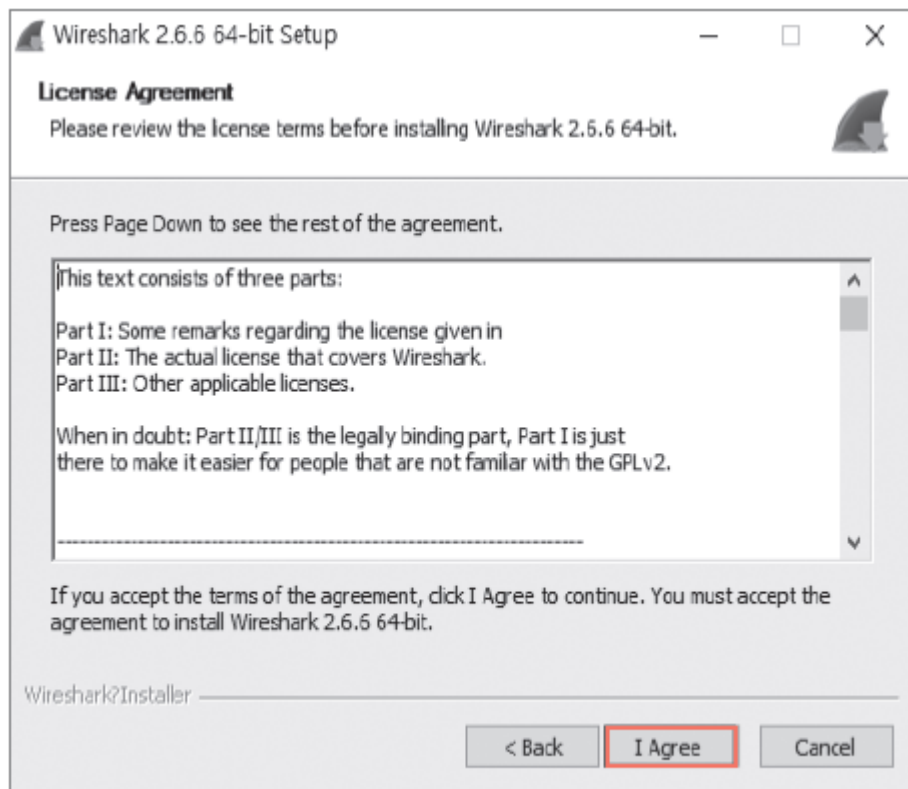


그림 1-14 라이선스 동의

02. 네트워크 분석도구 설치

5) 설치할 컴포넌트를 선택한 후 <Next>를 클릭한다. 기본적으로 선택된 컴포넌트대로 진행하면 된다.

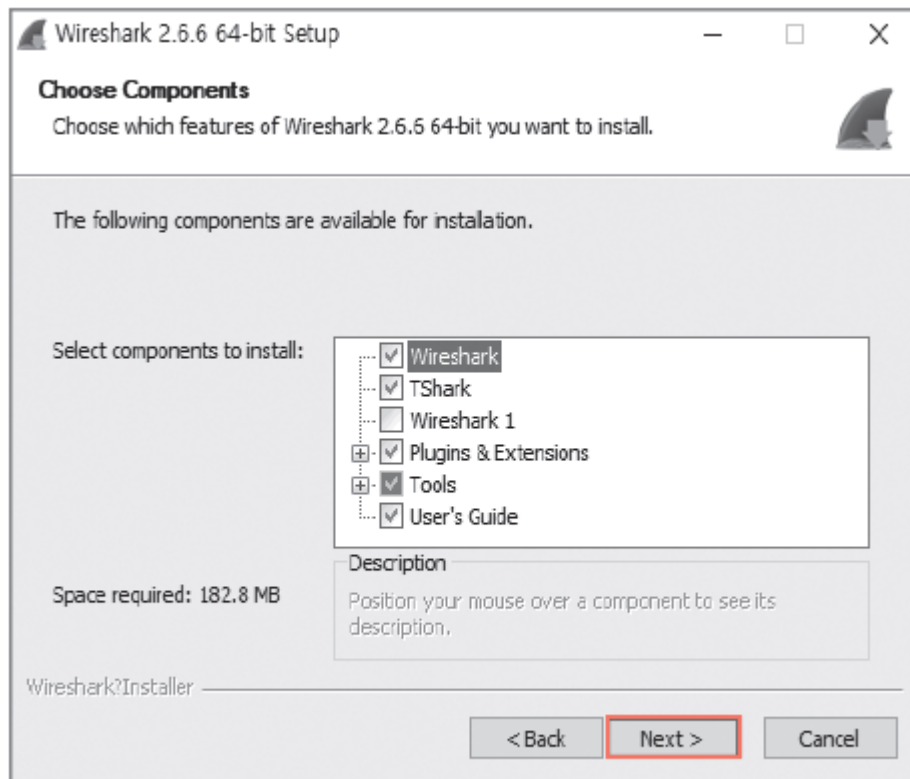


그림 1-15 설치할 컴포넌트 선택

02. 네트워크 분석도구 설치

6) 추가할 태스크가 있으면 선택하고 <Next>를 클릭한다.

- Wireshark Start Menu Item은 시작 메뉴 항목으로 shortcut을 생성한다.
- Wireshark Desktop Icon은 데스크톱에 아이콘으로 shortcut을 생성한다.
- Wireshark Quick Launch Icon은 시작 메뉴 옆에 빠른 실행 아이콘으로 shortcut을 생성한다.
- File Extensions에서는 와이어샤크와 연관된 파일의 확장자를 선택할 수 있다. File Extensions를 선택하면 다양한 확장자가 설정된다.

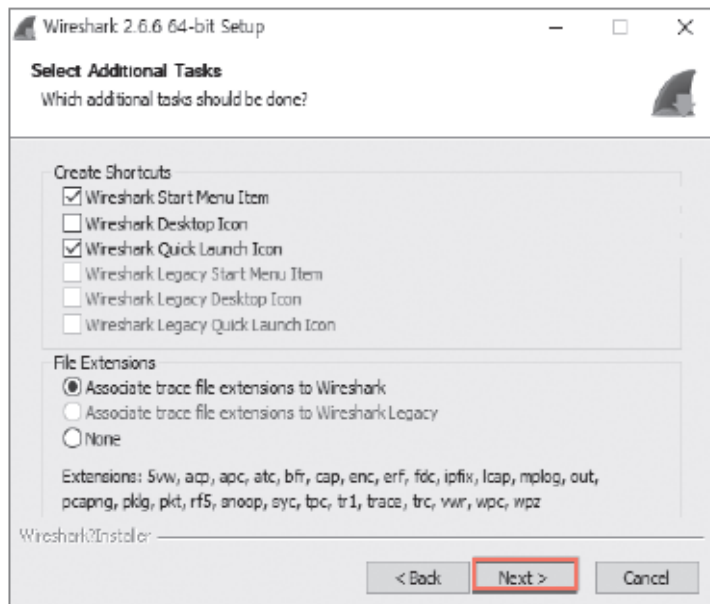


그림 1-16 추가할 태스크 선택

02. 네트워크 분석도구 설치

7) 인스톨할 경로를 선택한다. 'Destination Folder'에 설치할 위치 경로를 입력하거나 <Browse...>를 클릭하여 설치 위치를 선택한다.

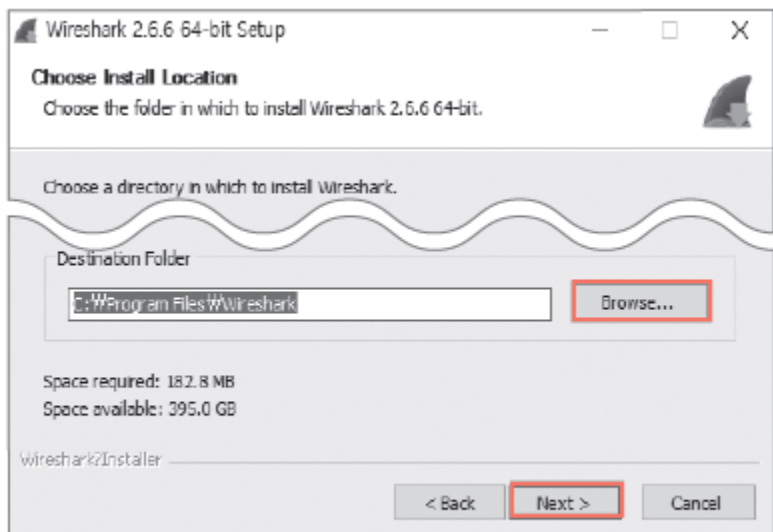


그림 1-17 인스톨할 경로 선택

02. 네트워크 분석도구 설치

8) WinPcap을 설치할지 여부를 확인하는 화면이 나타난다. 'Install WinPcap 4.1.3'에 체크한 뒤 <Next>를 클릭하면 와이어샤크 설치가 진행된다

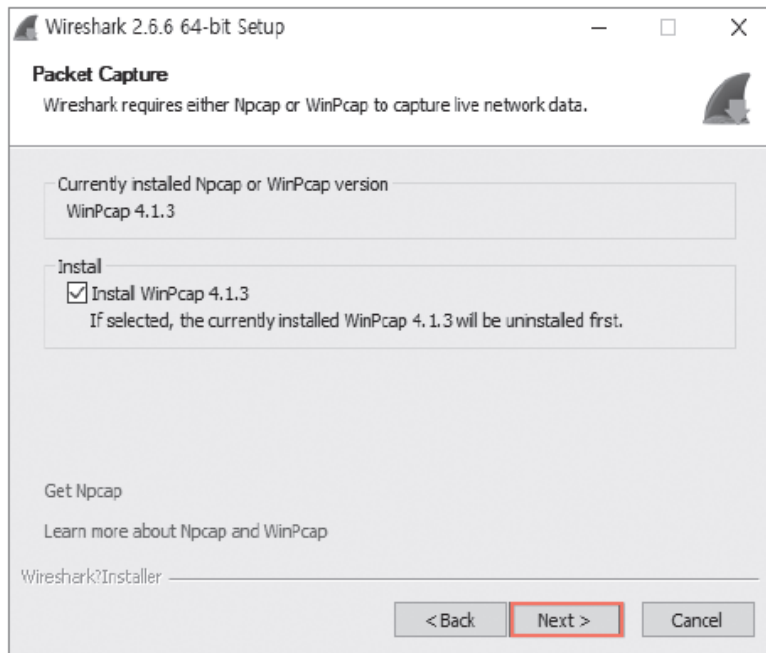


그림 1-18 WinPcap 설치 여부 확인

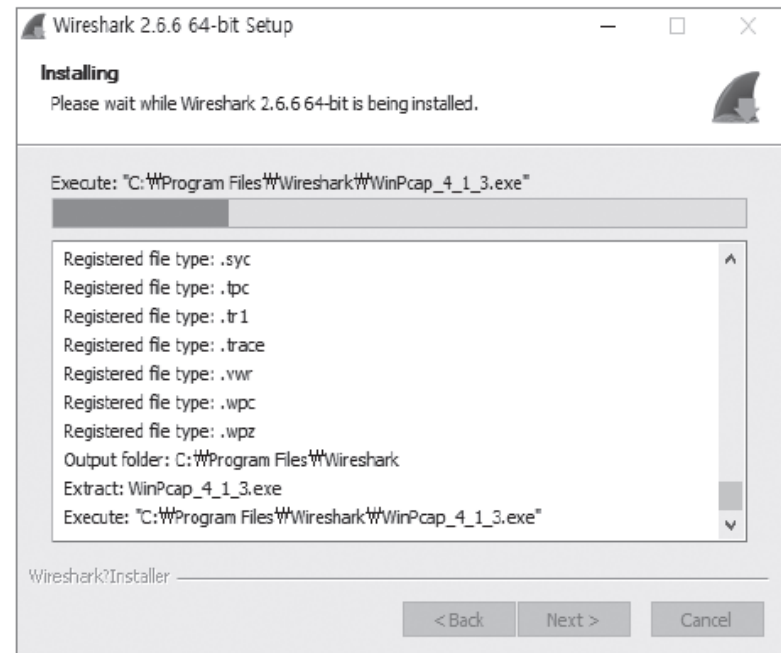


그림 1-19 와이어샤크 설치 진행

02. 네트워크 분석도구 설치

9) 와이어샤크를 설치하는 도중에 WinPcap 설치 화면이 나오면 <Next>를 클릭한다.

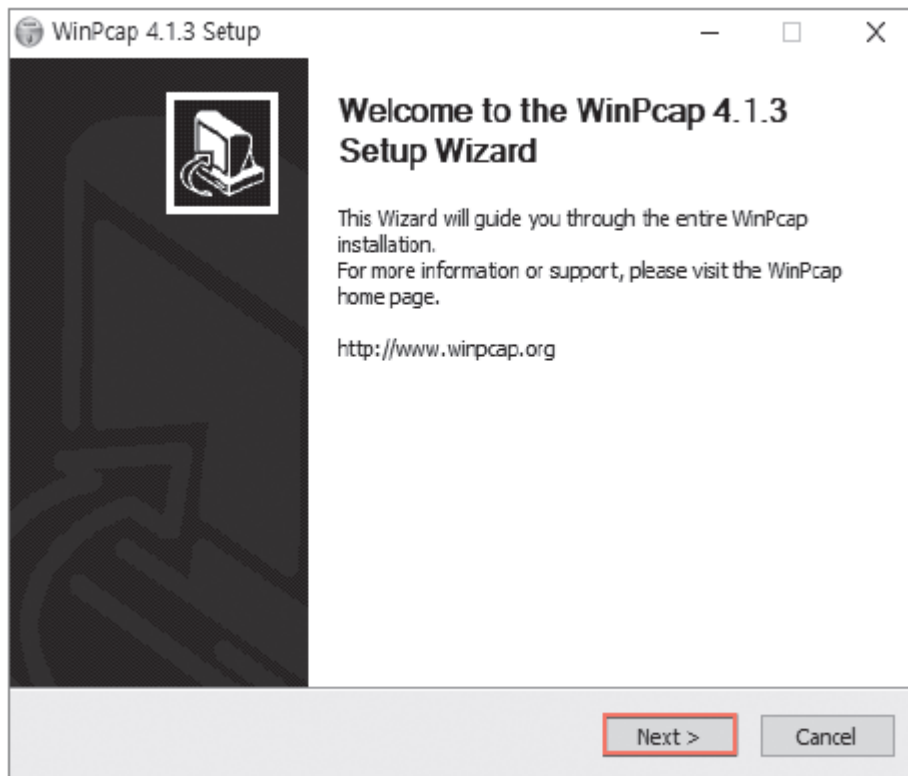


그림 1-20 WinPcap 설치 화면

02. 네트워크 분석도구 설치

10) 라이선스 동의 화면이 나타나면 <I Agree>를 클릭한다.

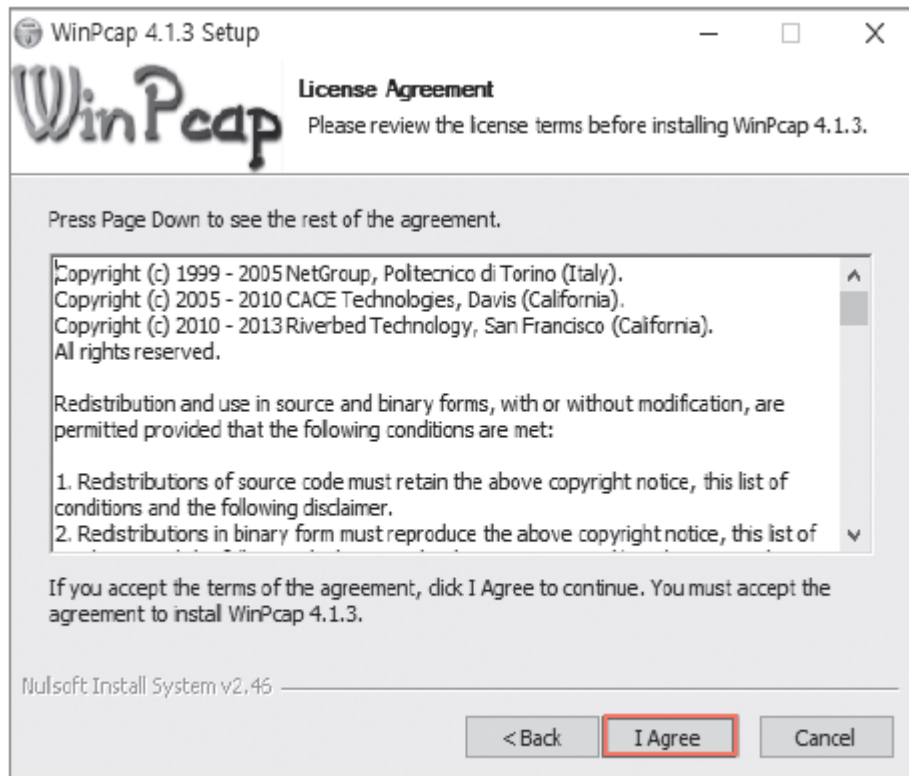


그림 1-21 라이선스 동의

02. 네트워크 분석도구 설치

11) WinPcap 설치 옵션을 설정한다. 컴퓨터가 부팅될 때 WinPcap도 자동으로 시작하도록 기본적으로 체크가 되어 있다. <Install>을 클릭하면 WinPcap 설치가 시작된다.

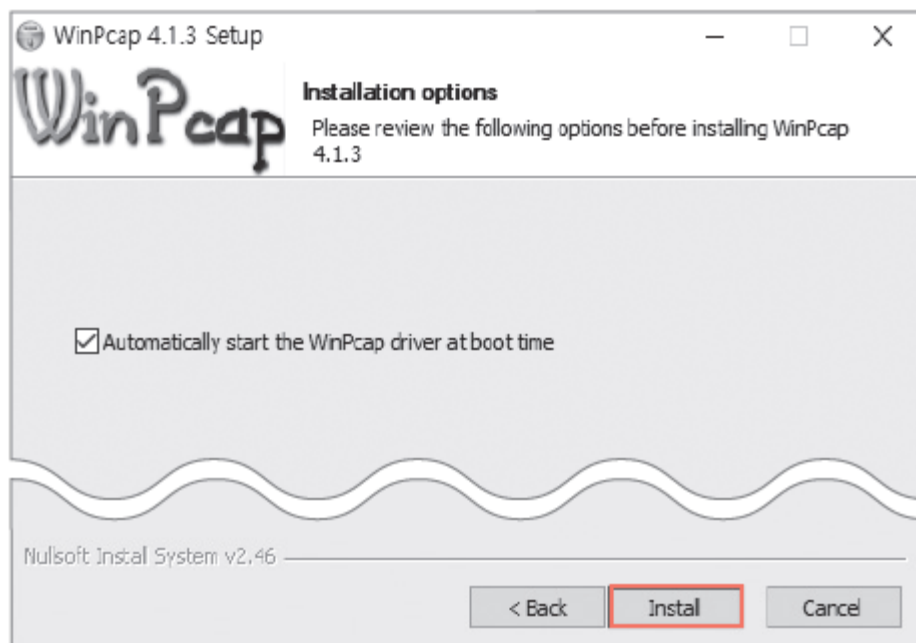


그림 1-22 WinPcap 설치 옵션

02. 네트워크 분석도구 설치

12) WinPcap 설치가 끝나면 <Finish>를 클릭한다.



그림 1-23 WinPcap 설치 종료

02. 네트워크 분석도구 설치

13) WinPcap 설치가 끝나면 와이어샤크 설치 진행 화면으로 돌아간다. 와이어샤크 설치가 완료되면 <Completed>가 표시되고, <Next>를 클릭하면 와이어샤크 설치 완료 화면이 나타난다

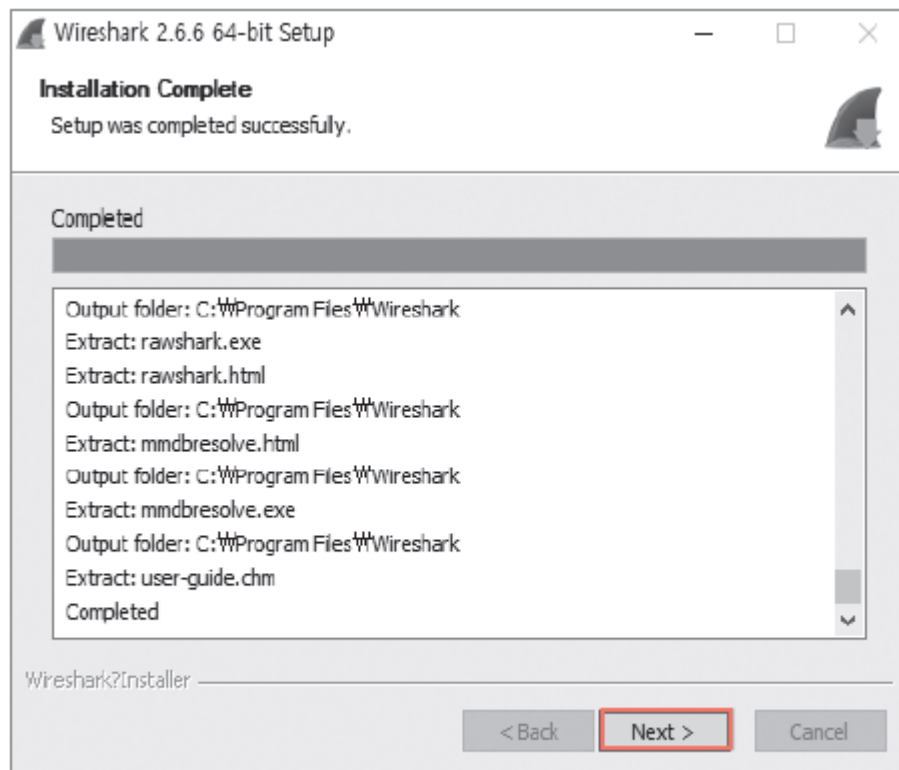


그림 1-24 와이어샤크 설치 화면

02. 네트워크 분석도구 설치

14) 와이어샤크 설치 완료 화면이 나타나면 <Finish>를 클릭한다.

- Run Wireshark 2.6.6 64-bit에 체크하면 설치 완료 후 와이어샤크가 자동으로 실행된다.
- Show News에 체크하면 와이어샤크 릴리스 노트를 참조할 수 있다.

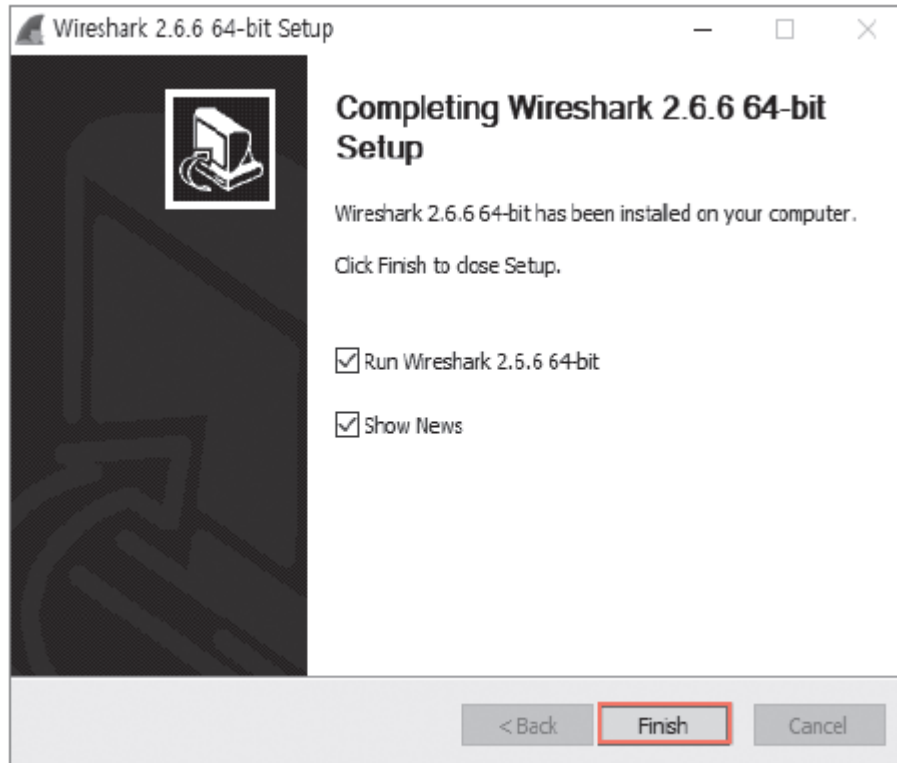


그림 1-25 와이어샤크 설치 완료

02. 네트워크 분석도구 설치

- 만약 와이어샤크와 WinPcap을 제거하고 싶다면 [제어판]-[프로그램]-[프로그램 및 기능]-[프로그램 제거 또는 변경]에서 제거할 수 있다.

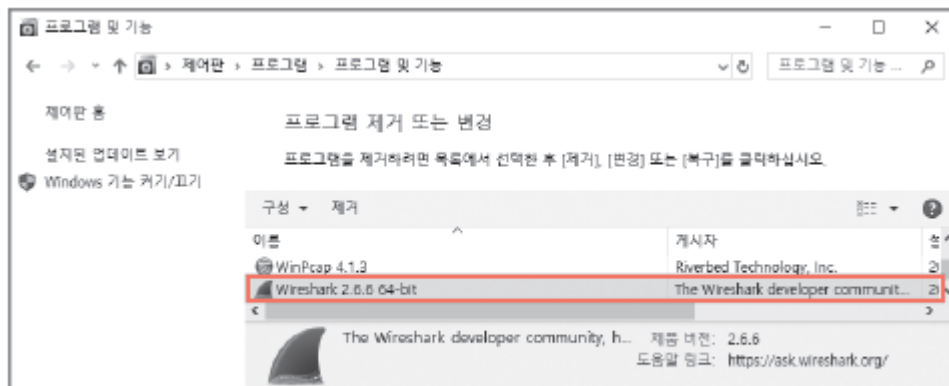


그림 1-26 와이어샤크와 WinPcap 제거

02. 네트워크 분석도구 설치

3. 와이어샤크 실행

- 1) 와이어샤크가 설치되면 [시작] 메뉴에서 와이어샤크를 실행할 수 있다. 설치 완료 창에서 'Run Wireshark 2.6.6 64-bit'에 체크했다면 자동으로 와이어샤크가 실행된다
- 2) 와이어샤크가 실행되면 와이어샤크에서 인식된 LAN 카드가 목록에 나타나며, 그중에서 캡처하려는 이더넷(네트워크 인터페이스)을 클릭하면 패킷 캡처가 시작된다(상어 등지느러미 아이콘을 클릭해도 바로 캡처를 시작할 수 있다). 또한 'Capture' 영역을 클릭하면 캡처 인터페이스 창이 나타나고 패킷을 캡처할 수 있는 LAN 카드가 표시된다.
캡처하려는 인터페이스를 선택한 후 <Start>를 클릭해도 패킷 캡처가 시작된다.

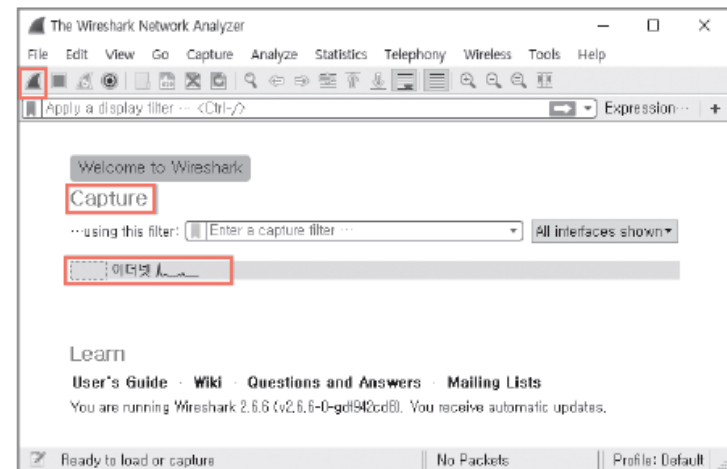


그림 1-27 와이어샤크 실행

02. 네트워크 분석도구 설치

- 패킷을 캡처하려면 윈도우의 관리자 권한으로 와이어샤크를 실행하고, 네트워크 통신을 하고있는 올바른 인터페이스를 선택해야 한다. 통신하지 않는 인터페이스를 선택하면 패킷이 캡처되지 않는다.

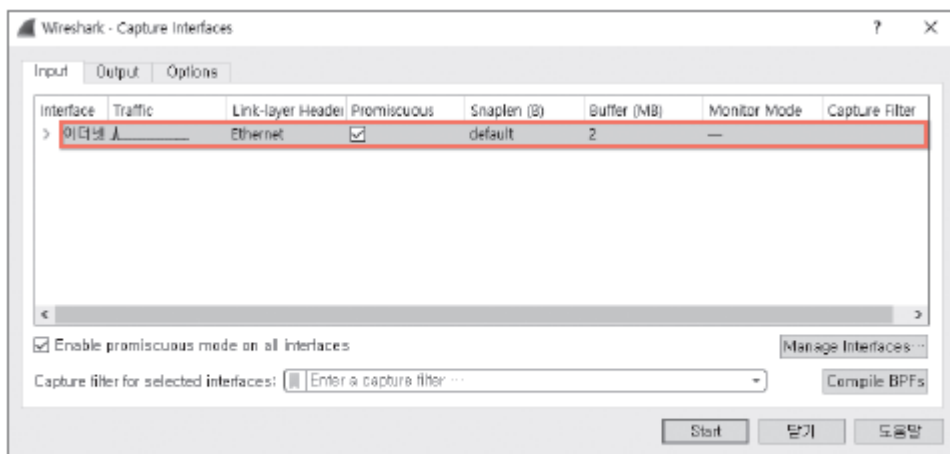


그림 1-28 캡처 인터페이스

02. 네트워크 분석도구 설치

- 3) 와이어샤크가 실행되고 통신을 시작하지 않아도 많은 패킷이 화면에 표시된다. 크롬 등의 웹 브라우저나 지메일과 같은 이메일 프로그램 애플리케이션을 실행하지 않아도 그 뒤에서 운영체제나 상주 프로그램 등이 통신을 하고 있기 때문이다
- 4) 자주 접속하는 웹 사이트의 패킷을 캡처해보자. 웹 브라우저를 실행하여 웹 사이트에 접속한다.

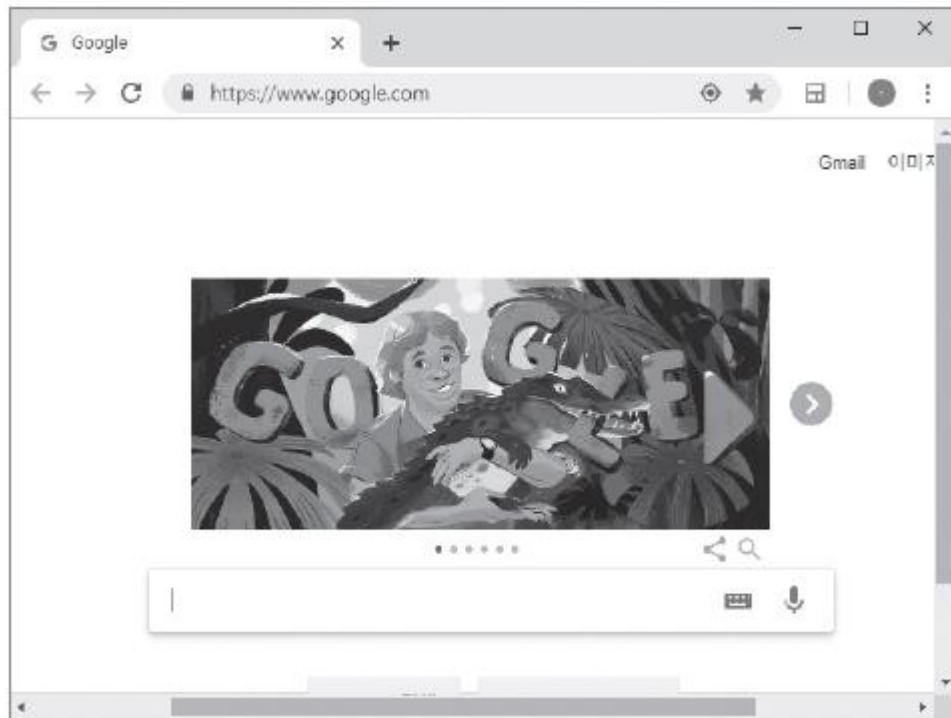
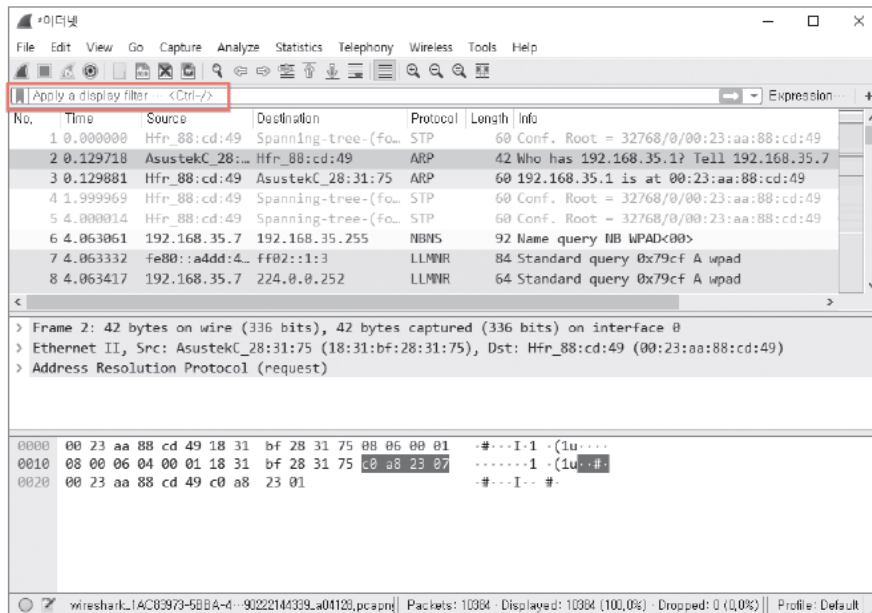


그림 1-29 웹 사이트 접속

02. 네트워크 분석도구 설치

- 웹 사이트의 패킷을 캡처할 때는 주의할 사항이 있다. 웹 브라우저는 한 번 접속한 웹 사이트의 내용을 저장하는 캐시 기능이 있기 때문에 한 번 접속한 웹 사이트의 경우 통신이 이루어지지 않고 디스크에 저장된 캐시를 사용하여 웹 사이트를 표시하므로 패킷을 제대로 캡처할 수 없다. 동일한 웹 사이트를 다시 읽어들이 때는 슈퍼 리로드(Ctrl) 을 누른 채 웹 브라우저의 새로 고침 버튼 클릭)를 하면 디스크에 캐시가 있더라도 서버로부터 모든 데이터를 다시 읽어들이 수 있다. 웹 사이트의 패킷을 캡처할 때는 슈퍼 리로드 기능을 사용하면 편리하다.
- 다음은 구글에 접속했을 때의 패킷 캡처 화면으로 많은 정보가 표시되고 있음을 확인할 수 있다. 툴바의 멈춤 아이콘을 클릭하면 패킷 캡처가 정지된다.

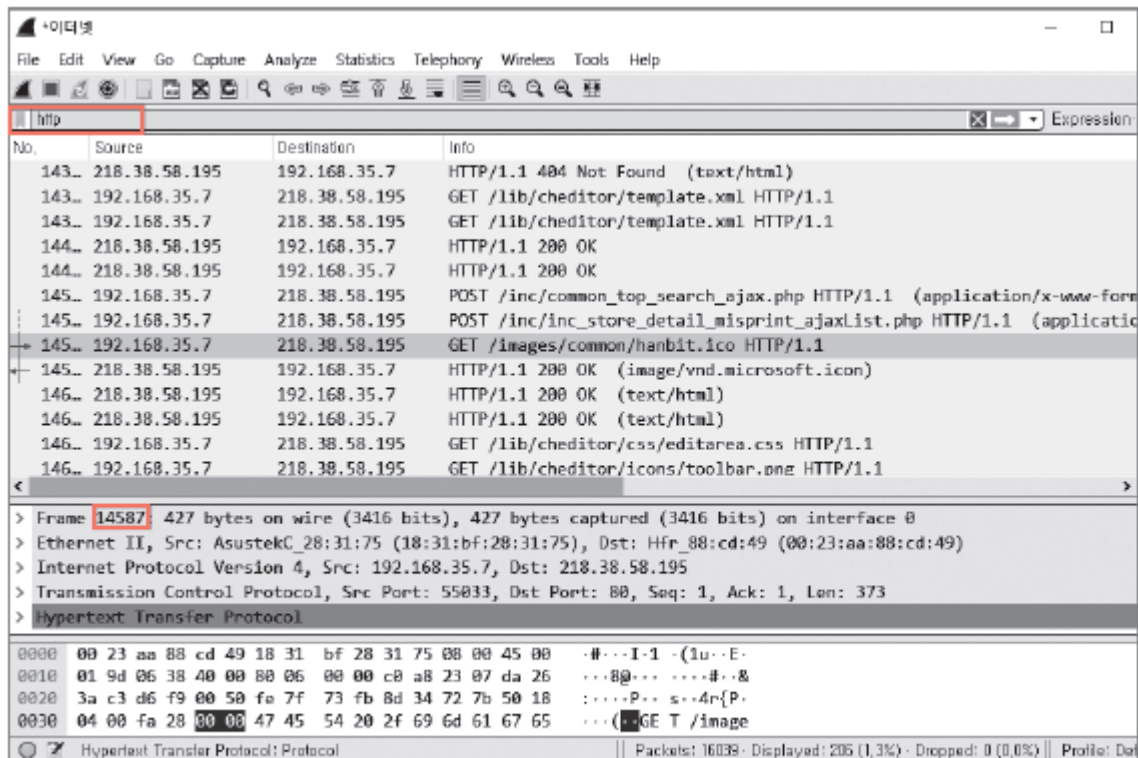


Ctrl+f5

그림 1-30 패킷 캡처 화면

02. 네트워크 분석도구 설치

5) 웹 사이트에 접속할 때 송수신되는 HTTPHyperText Transfer Protocol 패킷을 확인해보자. 한빛출판네트워크 웹 사이트에 접속하여 '네트워크 개론'을 검색했더니 화면에 많은 패킷이 나타났다. 이 중에서 HTTP 패킷만 나타나도록 화면 상단의 [Apply a display filter]에 'http'를 입력하고 를 클릭한다.



패킷리스트 영역

패킷 상세 영역

패킷 데이터 영역

그림 1-31 HTTP 패킷

02. 네트워크 분석도구 설치

- 화면 상단의 패킷 리스트 영역에는 캡처된 패킷이 한 행에 하나씩 표시된다. 여기서 패킷 분석을 하기 위해 선택한 패킷([그림 1-31]의 14587번 패킷)은 진한 색으로 표시되고, 그 내용을 패킷 상세 영역과 패킷 데이터 영역에서 확인할 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
9...	57.544726	218.38.58.195	192.168.35.7	HTTP	1266	HTTP/1.1 200 OK (PNG)
9...	57.547399	218.38.58.195	192.168.35.7	HTTP	75	HTTP/1.1 200 OK (PNG)
9...	57.548603	218.38.58.195	192.168.35.7	HTTP	1290	HTTP/1.1 200 OK (PNG)
9...	57.551319	192.168.35.7	218.38.58.195	HTTP	585	GET /images/common/cate_b12.png HTTP/1.1
9...	57.557331	218.38.58.195	192.168.35.7	HTTP	1290	HTTP/1.1 200 OK (PNG)
1...	57.609687	218.38.58.195	192.168.35.7	HTTP	415	HTTP/1.1 200 OK (text/plain)
→ 1...	57.673607	192.168.35.7	218.38.58.195	HTTP	638	GET /images/common/hanbit.ico HTTP/1.1
← 1...	57.675670	218.38.58.195	192.168.35.7	HTTP	215	HTTP/1.1 200 OK (image/vnd.microsoft.ic

그림 1-32 패킷 리스트 영역

- Source는 현재 컴퓨터의 IP 주소를, Destination은 접속한 웹 사이트의 IP 주소를 나타낸다. 자신이 사용하고 있는 컴퓨터의 IP 주소(192.168.35.7)는 명령 프롬프트(cmd) 창에서 ipconfig 명령어로 확인할 수 있고, 접속한 웹 사이트(한빛출판네트워크)의 IP 주소(218.38.58.195)는 'tracert 도메인명' 또는 'ping 도메인명'으로 확인할 수 있다

02. 네트워크 분석도구 설치

```
관리자: 명령 프롬프트
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert www.hanbit.co.kr

최대 30홉 이상의
www.hanbit.co.kr [218.38.58.195]으로 가는 경로 추적:

  1  <1 ms    <1 ms    <1 ms    192.168.35.1
  2  <1 ms    <1 ms    <1 ms    192.168.55.1
  3  *        *        *        요청 시간 초과
  4  *        *        *        요청 시간 초과
  5  *        *        *        요청 시간 초과
  6  *        *        *        요청 시간 초과
  7  *        *        *        요청 시간 초과
  8  *        *        *        요청 시간 초과
  9  *        *        *        요청 시간 초과
 10  *        *        *        요청 시간 초과
 11  3 ms     3 ms     1 ms     218.38.58.195

추적을 완료했습니다.
```

```
관리자: 명령 프롬프트
C:\Windows\system32>ipconfig

Windows IP 구성

이더넷 어댑터 이더넷:

    연결별 DNS 접미사. . . . . : 
    링크-로컬 IPv6 주소. . . . . : fe80::1a4d:f1:4884:6d1b:e97%4
    IPv4 주소. . . . . : 192.168.35.7
    서브넷 마스크. . . . . : 255.255.255.0
    기본 게이트웨이. . . . . : 192.168.35.1

C:\Windows\system32>ping www.hanbit.co.kr

Ping www.hanbit.co.kr [218.38.58.195] 32바이트 데이터 사용:
218.38.58.195의 응답: 바이트=32 시간=1ms TTL=54
218.38.58.195의 응답: 바이트=32 시간=1ms TTL=54
218.38.58.195의 응답: 바이트=32 시간=1ms TTL=54
218.38.58.195의 응답: 바이트=32 시간=1ms TTL=54

218.38.58.195에 대한 Ping 통계:
    패킷: 보낸 = 4, 받은 = 4, 손실 = 0 (0% 손실),
    왕복 시간(밀리초):
        최소 = 1ms, 최대 = 1ms, 평균 = 1ms
```

그림 1-33 IP 주소 확인

02. 네트워크 분석도구 설치

- 화면 중앙의 패킷 상세 영역에는 패킷의 의미가 통신 계층에 따라 트리 형태로 표시된다.

```
> Transmission Control Protocol, Src Port: 54746, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
▼ Hypertext Transfer Protocol
  > GET /images/common/hanbit.ico HTTP/1.1\r\n
    Host: www.hanbit.co.kr\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\n
    Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://www.hanbit.co.kr/store/books/look.php?p_code=88069473976\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,k;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  > Cookie: PHPSESSID=9oi911q6he10ktdioviomdvc17; _ga-GA1.3.241080138.1550814278; _gid-GA1.3.1271486862.1550814278
```

그림 1-34 패킷 상세 영역

- 화면 하단의 패킷 데이터 영역에는 송수신한 데이터의 내용이나 통신 데이터로 전송된 요청(HTTP Request) 문자가 표시된다.

0110	63 63 65 70 74 3a 20 69 6d 61 67 65 2f 77 65 62	Accept: image/webp,image/apng,image/*,*/*;q=0.8
0120	70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 69 6d 61	Referer: http://www.hanbit.co.kr/store/books/look.php?p_code=88069473976
0130	67 65 2f 2a 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a	Accept-Encoding: gzip, deflate
0140	52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f	Accept-Language: ko-KR,k;q=0.9,en-US;q=0.8,en;q=0.7
0150	77 77 77 2e 68 61 6e 62 69 74 2e 63 6f 2e 6b 72	
0160	2f 73 74 6f 72 65 2f 62 6f 6f 6b 73 2f 6c 6f 6f	
0170	6b 2e 70 68 70 3f 70 5f 63 6f 64 65 3d 42 38 38	
0180	36 39 34 37 33 39 37 36 0d 0a 41 63 63 65 70 74	
0190	2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c	
01a0	20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74	
01b0	2d 4c 61 6e 67 75 61 67 65 3a 20 6b 6f 2d 4b 52	

그림 1-35 패킷 데이터 영역

02. 네트워크 분석도구 설치

4. 캡처 파일 저장

1) [File]-[Save]를 선택한 후 캡처 파일의 이름을 입력한다. 기본적으로 파일 형식은 확장자가 .pcapng로 설정되어 있다.

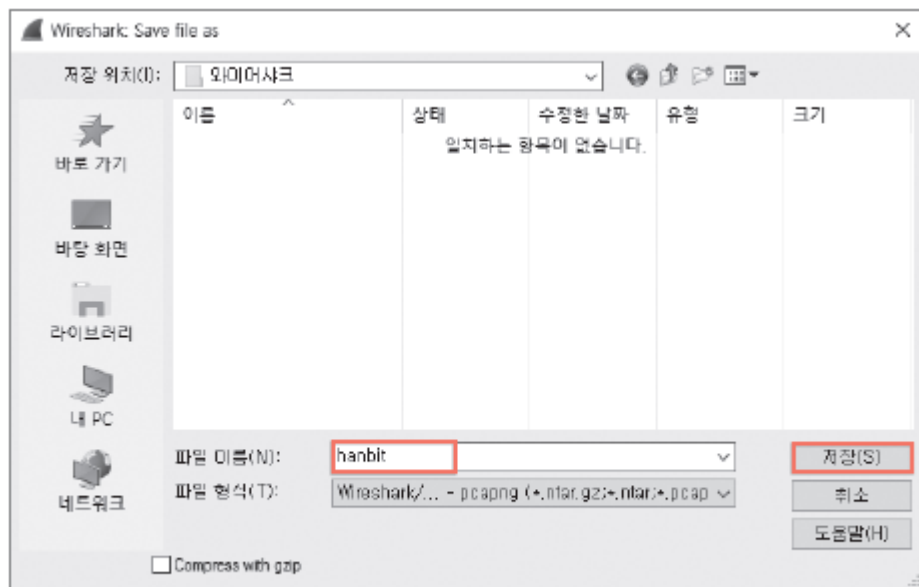


그림 1-36 캡처 파일 저장

02. 네트워크 분석도구 설치

- 2) 캡처 파일을 저장한 폴더를 열어 보면 와이어샤크 모양의 'hanbit.pcapng' 파일이 생성된것을 확인할 수 있다. 이 파일을 더블클릭하면 와이어샤크가 실행되면서 캡처 파일 내용이 화면에 나타난다.

- 와이어샤크는 패킷에서 데이터를 복원해서 추출할 수 있다. 캡처 파일 저장 경로를 탐색기에서 확인하면 HTTP 통신에서 이미지 파일이 출력되는 것을 확인할 수 있다.

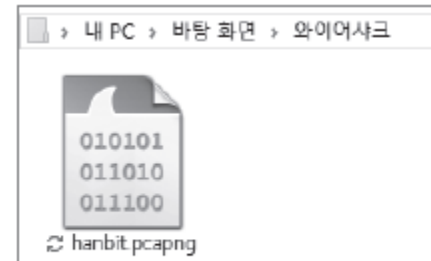


그림 1-37 캡처 파일 확인

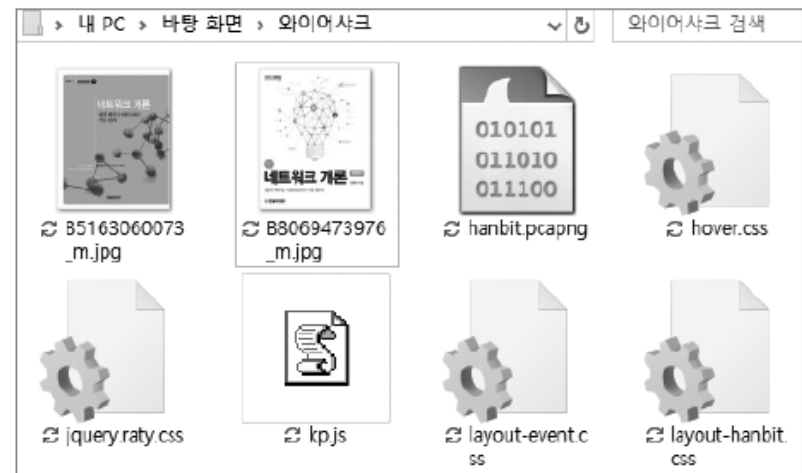


그림 1-38 데이터 복원 추출

03. 네트워크 설정

3. 네트워크 명령어

명령 프롬프트에서 명령어를 입력하면 네트워크 설정 정보를 확인할 수 있다.

■ hostname 명령어

컴퓨터 이름을 확인할 수 있다

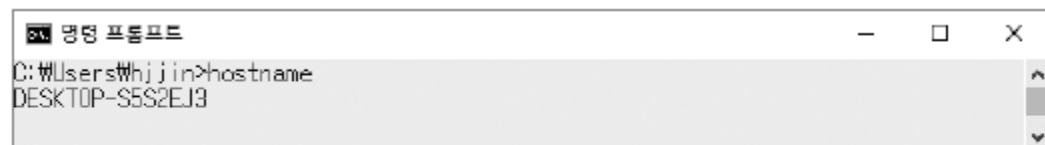


그림 1-59 hostname 명령어

■ net user 명령어

컴퓨터 사용자 계정을 확인할 수 있다.

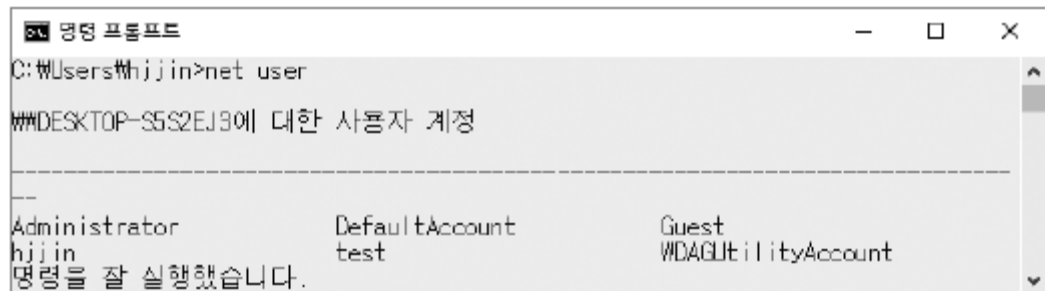
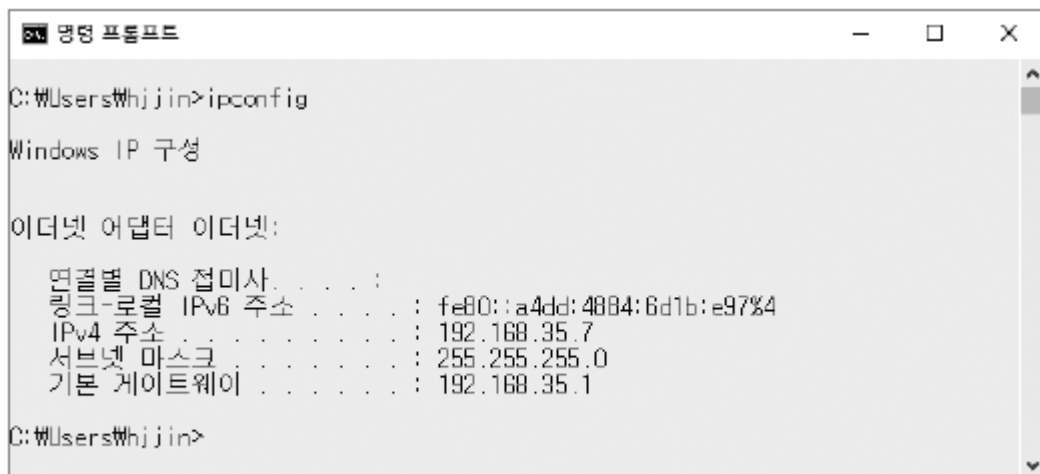


그림 1-60 net user 명령어

03. 네트워크 설정

■ ipconfig 명령어

컴퓨터의 네트워크 설정 정보(IP 주소, 게이트웨이 등)를 확인할 수 있다. IP 주소는 네트워크에 연결된 모든 장치에 있는 고유 주소이며, 이 IP 주소로 서로 통신할 수 있다



```
C:\Users\Whjjin>ipconfig

Windows IP 구성

이더넷 어댑터 이더넷:

    연결별 DNS 접미사. . . . . : 
    링크-로컬 IPv6 주소 . . . . : fe80::a4dd:4884:6d1b:e97%4
    IPv4 주소 . . . . . : 192.168.35.7
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 192.168.35.1

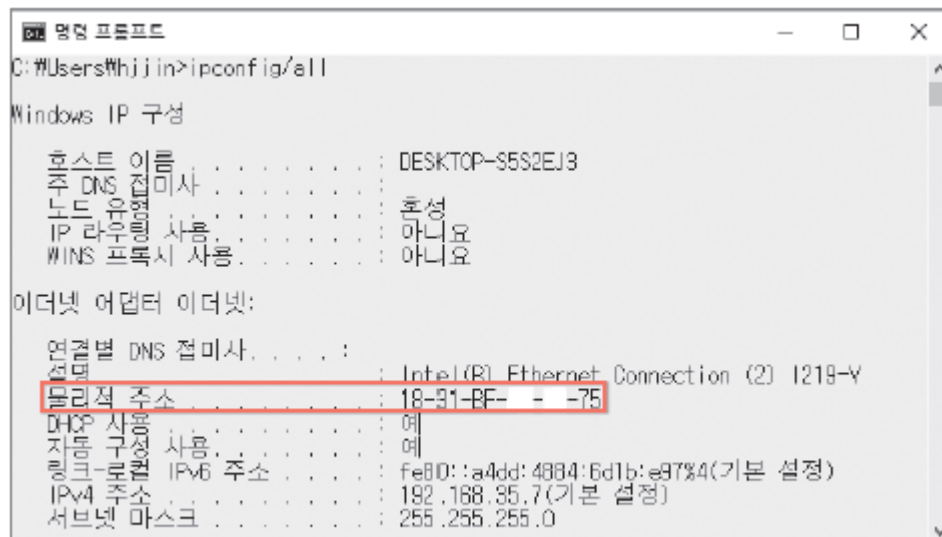
C:\Users\Whjjin>
```

그림 1-61 ipconfig 명령어

03. 네트워크 설정

■ ipconfig/all 명령어

컴퓨터의 실제 주소(MAC, 물리적 주소)를 확인할 수 있다.



```
명령 프롬프트
C:\Users\whjjin>ipconfig/all

Windows IP 구성

호스트 이름 . . . . . : DESKTOP-S5S2EJ3
주 DNS 접미사 . . . . . :
노드 유형 . . . . . : 혼성
IP 라우팅 사용 . . . . . : 아니요
WINS 프록시 사용 . . . . . : 아니요

이더넷 어댑터 이더넷:

연결별 DNS 접미사 . . . . :
설명 . . . . . : Intel(R) Ethernet Connection (2) I218-V
물리적 주소 . . . . . : 18-91-BF- - -75
DHCP 사용 . . . . . : 예
자동 구성 사용 . . . . . : 예
링크-로컬 IPv6 주소 . . . : fe80::a4dd:4884:6d1b:e97%4(기본 설정)
IPv4 주소 . . . . . : 192.168.35.7(기본 설정)
서브넷 마스크 . . . . . : 255.255.255.0
```

그림 1-62 ipconfig/all 명령어

03. 네트워크 설정

■ ipconfig/release 명령어

현재 IP 주소를 해제할 수 있다. 할당받은 IP 주소가 해제되면서 네트워크 연결이 끊긴다.

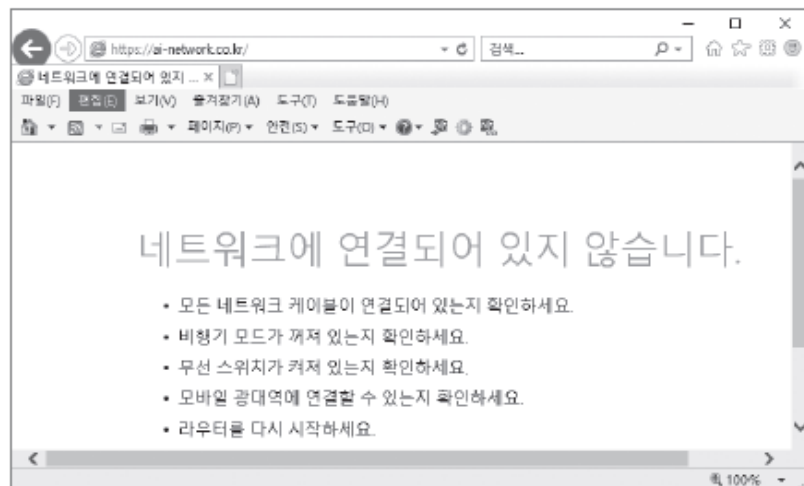
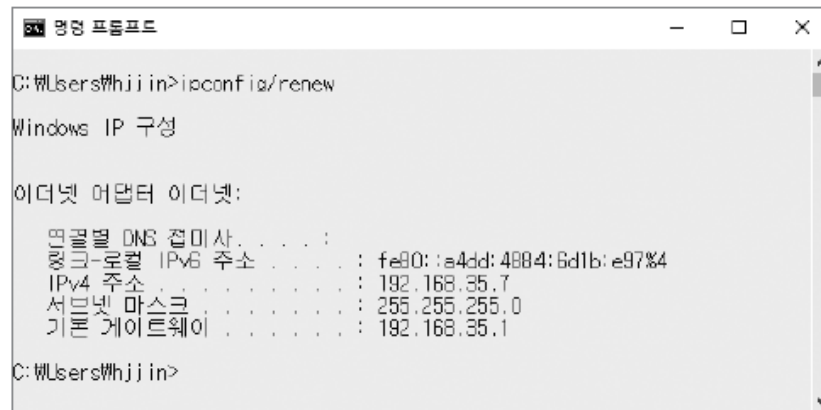


그림 1-63 ipconfig/release 명령어

03. 네트워크 설정

■ ipconfig/renew 명령어

네트워크에서 DHCP를 사용할 때 컴퓨터의 새로운 IP 주소를 얻을 수 있다. IP 주소를 생성함으로써 네트워크에 연결된다.



```
C:\Users\whjjin>ipconfig/renew

Windows IP 구성

이더넷 어댑터 이더넷:

    연결될 DNS 접미사 . . . . . :
    링크-로컬 IPv6 주소 . . . . . : fe80::a4dd:4884:6d1b:e97%4
    IPv4 주소 . . . . . : 192.168.35.7
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 192.168.35.1

C:\Users\whjjin>
```

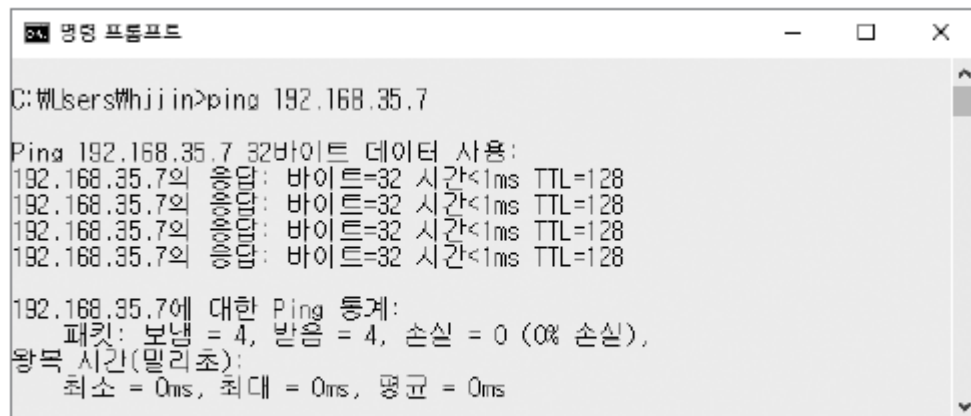


그림 1-64 ipconfig/renew 명령어

03. 네트워크 설정

■ ping 명령어

컴퓨터의 네트워크 상태를 점검하거나 진단하는 명령어(ping IP 주소)로, 컴퓨터가 네트워크에 제대로 연결되었는지 확인할 수 있다. 문제가 있을 때는 응답이 없거나 왕복 시간이 오래 걸린다.



```
명령 프롬프트
C:\Users\hijin>ping 192.168.35.7

Ping 192.168.35.7 32바이트 데이터 사용:
192.168.35.7의 응답: 바이트=32 시간<1ms TTL=128
192.168.35.7의 응답: 바이트=32 시간<1ms TTL=128
192.168.35.7의 응답: 바이트=32 시간<1ms TTL=128
192.168.35.7의 응답: 바이트=32 시간<1ms TTL=128

192.168.35.7에 대한 Ping 통계:
    패킷: 보낸 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

그림 1-65 ping 명령어