Chapter 04

와이어샤크 개요 및 설치와 실행

1. 패킷 분석기

- 패킷 분석기(packet analyser)는 네트워크를 통해 전달되는 패킷을 캡처하여 그 내용을 화면에 나타내 주는 소프트웨어이다.
- 패킷 분석기에는 상용과 무료(오픈 또는 프리 소스)가 있으며, 그 기능도 여러 가지가 있다.
- 패킷 분석기는 대부분 공공기관, 금융기관, 일반회사, 학교 등에 있는 정보기기들을 케이블과 같은 전송 매체로 연결한 근거리 통신망(LAN; Local Area Network)에서 사용되는 분석 도구이다.
- 즉 네트워크 분석 도구라고도 한다.
- 패킷 분석기는 LAN 케이블을 따라 전달되는 전자기 신호를 데이터(패킷)로 캡처하여 패킷의 내용을 볼 수 있다.
- LAN 케이블을 따라 전송되는 전자기 신호를 데이터로 획득하는 것을 패킷 캡처(packet capture)라고 한다.
- 또한 획득한 패킷의 의미를 알아보는 것을 덤프 분석(dump analysis)이라고 한다.

1. 패킷 분석기

패킷 분석기의 종류

하드웨어 분석기

- 하드웨어 분석기는 들고 다닐 수 있는 휴대형으로 액정화면과 네트워크에 접속하기 위한 연결구(connector, 커넥터)가 달려 있다.
- 이 연결구를 조사하고자 하는 네트워크에 직접 연결하여 패킷을 살펴보거나 네트워크의 안전성을 확인한다.
- 하드웨어 분석기는 주로 네트워크에 트러블이 발생할 때 직접 현장에 가지고 가서 트러블을 해결하기 위해 사용한다.
- 하드웨어 분석기의 이점은 소프트웨어 분석기에서는 어려운 케이블의 품질 조사라든가 오류 프레임 등을 정확히 측정할 수 있다는 점이다.
- 실제로 대부분이 규모가 큰 기관의 네트워크 시스템 관리에서 이용되고 있다.

소프트웨어 분석기

- 소프트웨어 분석기는 노트북이나 서버에 설치하여 컴퓨터의 네트워크 인터페이스 카드를 이용하여 네트워크에 접속한다.
- 소프트웨어 분석기에는 상용과 무료(오픈 소스)가 있다.

2. 와이어샤크 개요

- 와이어샤크(Wireshark)는 근거리 통신망 상에서 전달되는 패킷을 분석하는 도구이다.
- 와이어샤크는 미국의 미주리대학에서 전산학을 공부한 제럴드 콤즈(Gerald Combs)가 개발한 LAN 분석기이다.
- 와이어샤크는 GPL이라는 라이센스 형태로 배포하고 있다.
- 콤즈는 당초 1988 년에 “Ethereal"이라는 이름으로 LAN 분석기를 개발하여 GPL로 공개하였다.
- 그는 당시 근무하고 있던 회사에서 개발팀의 핵심 멤버로서 일하고 있었는데, 8 년 후에 다른 직장으로 옮기게 되었다.
- 그 결과 Ethereal 프로젝트는 개발을 계속할 수 없게 되었고, 원래 회사가 저작권을 양도해주지 않아서 개발팀은 와이어샤크라는 새로운 상표로 개발을 계속하게 되었다.
- 현재, 와이어샤크는 엄청난 규모로 성장하였다.

2. 와이어샤크 개요

와이어샤크의 용도

- **와이어샤크는 다음과 같은 목적으로 이용할 수 있다.**
  - 컴퓨터 네트워크 프로토콜을 배우기 위해 사용한다.
  - 네트워크 관리자가 네트워크의 트러블을 해결하기 위해 사용한다.
  - 보안 기술자가 보안 문제를 시험하거나 확인/해결하기 위하여 사용한다.
  - 개발자가 프로토콜을 구현할 때 디버그(오류 확인)하기 위하여 사용한다.
  - 품질 관리 엔지니어가 네트워크 애플리케이션을 확인하는데 사용된다.

- **이 중에서 우리에게 필요한 와이어샤크의 최대 이용 목적은 네트워크 프로토콜을 배우는 것이다.**

2. 와이어샤크 개요

와이어샤크의 주요 기능

- **와이어샤크는 다음과 같은 주요 기능을 갖는다.**
  - 현재 대부분의 OS(유닉스, 리눅스, 윈도우 등)를 지원한다.
  - 네트워크 인터페이스로부터 실시간으로 패킷 데이터를 캡처할 수 있다.
  - 패킷에 대한 프로토콜 정보를 자세하게 보여준다 .
  - 캡처된 패킷 데이터를 열거나 저장할 수 있다.
  - 다른 패킷 분석기가 획득한 패킷 캡처 데이터를 변환하여 읽거나 출력할 수 있다 .
  - 여러 조건으로 패킷을 제한해서 검색할 수 있다 .
  - 필터링된 패킷을 원하는 색으로 나타낼 수 있다 .
  - 캡처한 데이터를 다양한 형식으로 출력할 뿐만 아니라 여러 가지 통계를 만들 수 있다.
  - 여러 가지 암호화 프로토콜의 복호를 지원한다.

- **서로 다른 네트워크 매체의 실시간 캡처**
  - 와이어샤크는 이더넷, 무선 LAN, Bluetooth, USB 등 다양한 네트워크 유형의 트래픽을 캡처할 수 있다.
  - 지원되는 특정 네트워크 유형은 하드웨어와 운영체제를 포함한 여러 요인에 의해 제한될 수 있다.

2. 와이어샤크 개요

와이어샤크의 장점

- 와이어샤크의 가장 큰 장점은 패킷의 내용을 자세하게 보여주는 것과 패킷 해석이다.
- 또한 버전업이 지주 이루어지는 것도 강점이다.
- 와이어샤크는 패킷의 내용을 자세하게 보여주고, 상용 패킷 분석기보다 훨씬 쉽게 패킷을 해석할 수 있다.
- 또한 새로운 프로토콜이 나오면 바로 이에 대응하는 버전으로 업그레이드 된다.
- 패킷 변환도 와이어샤크가 장점으로 삼는 부분이다.
- 와이어샤크는 상용 패킷 분석기가 캡처한 패킷이 저장된 파일을 읽어 들여 다른 파일 형식으로 출력하거나 복수의 캡처 파일을 결합하고, 이것을 바탕으로 분석할 수 있다.

2. 와이어샤크 개요

와이어샤크의 취약 분야

- 와이어샤크는 상용 LAN 분석기에 비해 통계 기능이나 보고 기능, 임계치 기능이 비교적 약하다고 할 수 있다.
- 다만 통계 기능과 보고 기능에 대해서는 현재 버전 업이 계속 진행되고 있으며 패킷 캡처의 내용을 표 형식으로 이해하기 쉽게 보여주거나 통신량의 꺾은 선 그래프나 막대그래프를 작성할 수 있게 되어 있다.
- 또한, 와이어샤크는 침입탐지시스템(IDS; Intrusion detection system) 로서 개발된 것이 아니어서 네트워크의 변화를 감지하고 화면에 경고 메시지를 나타내거나 관리자에게 메일을 보낼 수는 없다.
- 하지만 패킷을 캡처해서 네트워크의 이상을 파악할 수 있다.
- 나아가 와이어샤크는 네트워크를 직접 조작할 수도 없다.
- 상용 LAN 분석기에는 「패킷 생성기」라는 패킷 생성 도구가 포함되어 실제로 특정 패킷을 생성하여 네트워크를 통해 송신할 수 있다.
- 이에 비해 와이어샤크는 어디까지나 네트워크를 측정하는 기능만 가지고 있다.

3. 와이어샤크에서 패킷을 캡처/처리하는 방법

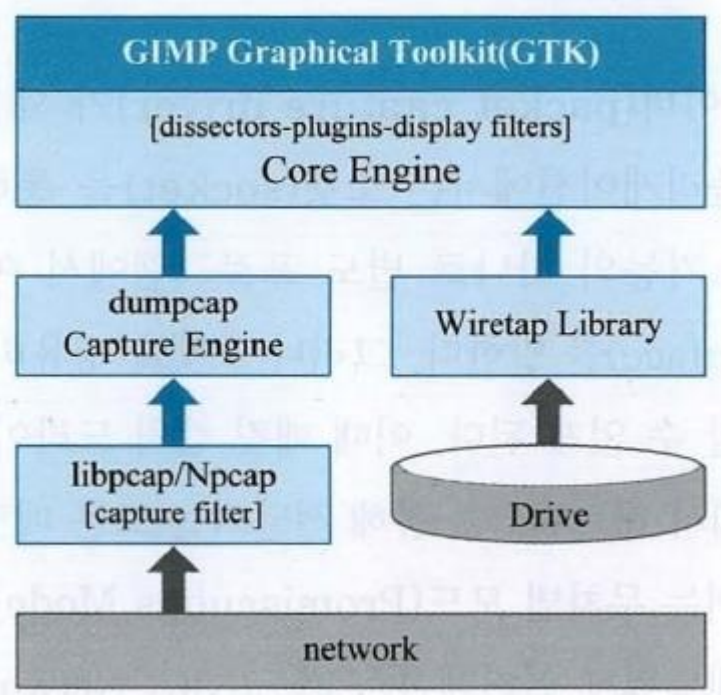
- 와이어샤크는 유용한 패킷 분석기이지만 와이어샤크 하나만으로 패킷을 쉽게 획득(캡처)할 수 없다.
- 네트워크를 통하여 전달되는 패킷을 캡처하기 위해서는 패킷 캡처 드라이버가 필요하다.
- 여기서 패킷 캡처 드라이버(packet capture driver)가 왜 필요한지 간단하게 살펴보자.
- 원래 일반적인 애플리케이션에서는 소켓 (socket)을 통하여 데이터를 송/수신한다.
- 소켓이란 OS가 가진 기능의 하나로 별도 프로그램에서 이용하기 위한 함수(API; Application Program Interface)를 말한다.
- 그러나 소켓을 경유하면 네트워크를 통해 전달되는 데이터를 직접 캡처할 수 없게 된다.
- 이때 패킷 캡처 드라이버를 이용하면 소켓을 건너뛰고 직접 패킷 분석기에서 네트워크를 통해 전달되는 모든 패킷을 조작할 수 있게 된다.

3. 와이어샤크에서 패킷을 캡처/처리하는 방법

- 또한 패킷 캡처 드라이버는 무차별 모드(Promiscuous Mode) 라는 특수한 설정으로 동작할 수 있다.
- 통상적인 네트워크 인터페이스 카드(NIC; Network Interface Card))는 기본적으로 자신과 관계가 있는 패킷만 캡처한다.
- 즉, 다른 컴퓨터의 통신은 캡처할 수 없다.
- 그러나, 패킷 캡처 드라이버는 목적지가 자신이 아닌 패킷일지라도 모두 캡처할 수 있는 상태(무차별 모드)로 NIC를 설정할 수 있다.
- 와이어샤크에서 사용되는 패킷 캡처 드라이버는 다음 세 가지가 있다.
  - Npcap(Windows용 패킷 캡처 드라이버)
  - libPcap(UNIX/Linux용 패킷 캡처 드라이버)
  - AirPcap(무선용 패킷 캡처 드라이버)

3. 와이어샤크에서 패킷을 캡처/처리하는 방법

- 따라서, 와이어샤크가 유선과 무선 네트워크에 연결되어 있다면, 와이어샤크가 트래픽 캡처 처리 과정은 그림과 같이 Npcap, AirPcap 및 libpcap 링크-계층 인터페이스 중 하나의 인터페이스에 의해 처리된다.

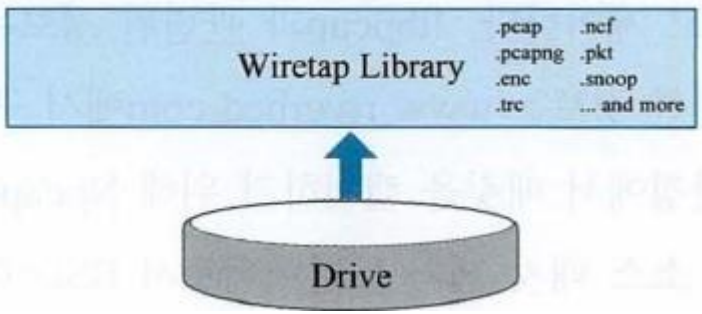


3. 와이어샤크에서 패킷을 캡처/처리하는 방법

- 와이어샤크로 트래픽을 수집할 때 dumpcap이라는 도구가 실제 패킷 캡처를 시작하게 한다.
- 네트워크를 통해 수집된 프레임들은 특수 목적 링크-계층 드라이버 중 하나를 통하여 바로 와이어샤크의 캡처 엔진(Capture Engine)으로 전달된다. 캡처 필터를 적용하면 캡처 필터를 경유하여 통과한 프레임은 코어엔진으로 전달된다.
- 캡처 필터는 버클리 패킷 필터링 (BPF; Berkeley Packet Filtering) 문법을 준수한다.
- 캡처/추적 파일을 읽어들일 때는, Npcap. AirPcap 및 libpcap 인터페이스는 사용되지 않는다.
- Wiretap 라이브러리는 저장된 추적 파일에 대한 입력/출력 기능을 위해서 사용된다.
- 추적 파일을 읽을 때 Wiretap 라이브러리는 프레임을 코어 엔진(Core Engine)으로 전달한다.

3. 와이어샤크에서 패킷을 캡처/처리하는 방법

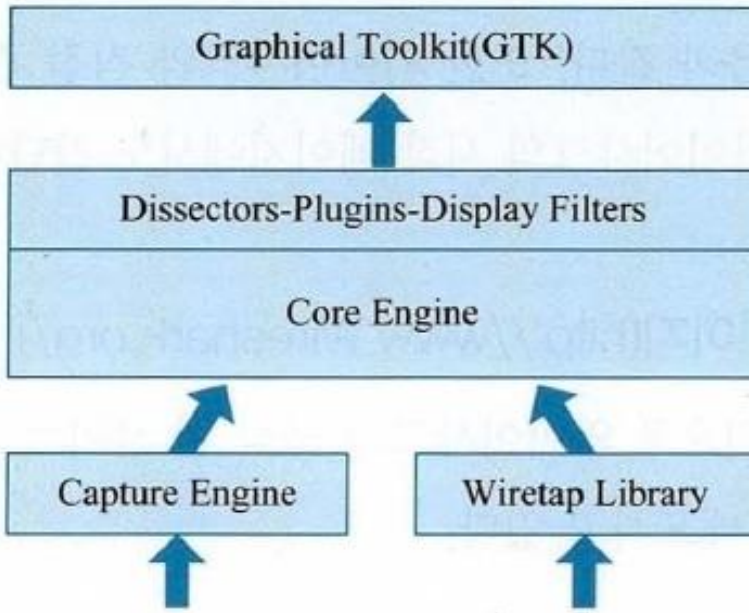
- 공개된 추적 파일은 그림에 나타난 것과같이 와이어샤크 wiretap 라이브러리를 통해 처리된다.



- 와이어샤크 wiretap 라이브러리에 있는 추적 파일 유형의 전체 목록을 보려면, 와이어샤크를 실행하고 File | Open을 선택한 다음 드롭다운 목록에서 File of Type을 클릭하면 된다.

3. 와이어샤크에서 패킷을 캡처/처리하는 방법

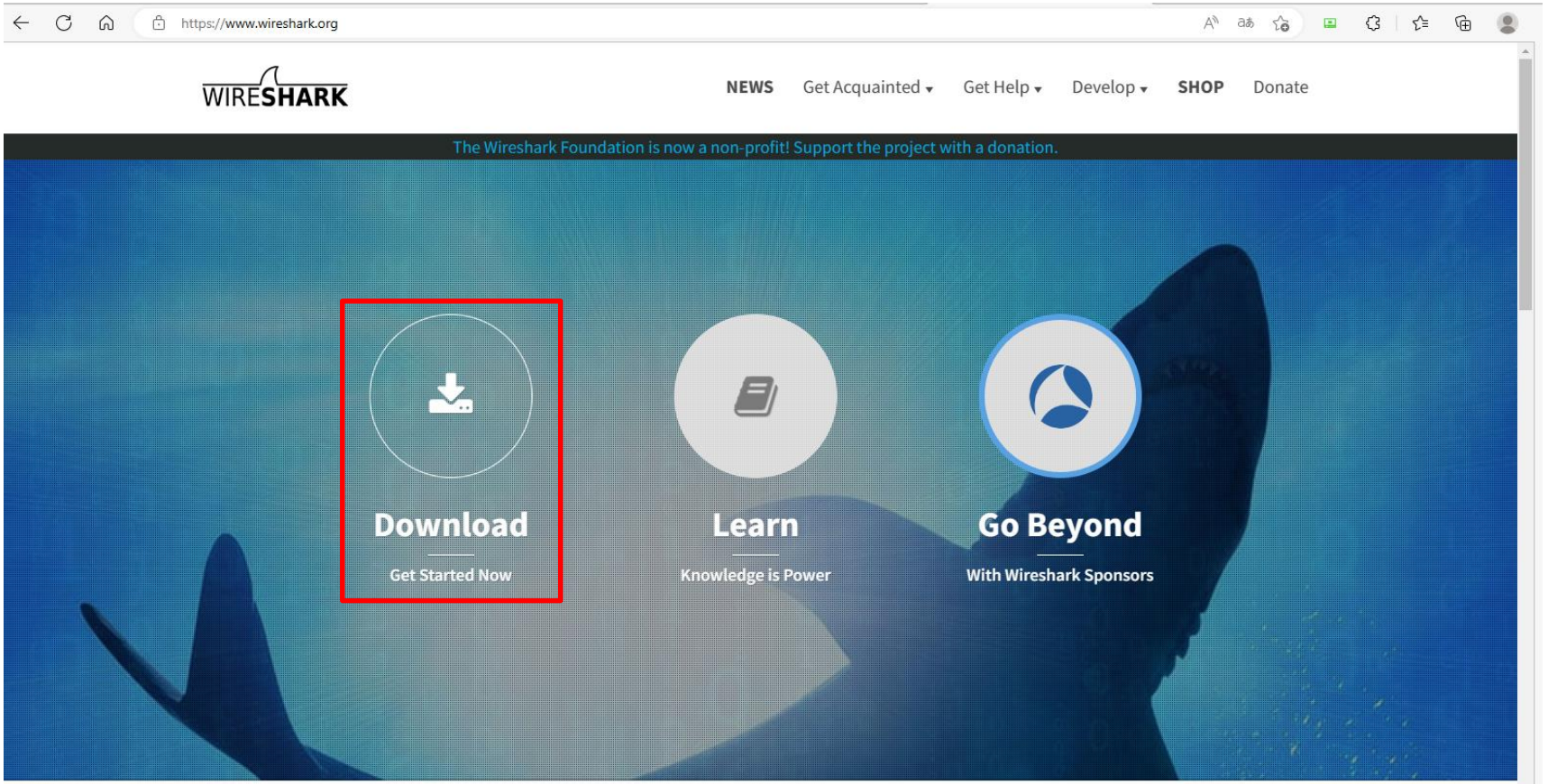
- 와이어샤크에서 패킷을 처리하는 방법은 그림에 sk타난 바와 같이 libpcap, Npcap 및 AirPcap에 의해 처리되거나 wiretap 라이브러리에 의해 공개된 추적 파일은 코어 엔진(core engine) 에서 처리된다.
- 캡처 엔진은 프레임을 코어 엔진(Core Engine)으로 전달한다.
- 이것은 와이어샤크의 주요 핵심 기능이다.



4. 와이어샤크 설치와 실행

와이어샤크 다운로드

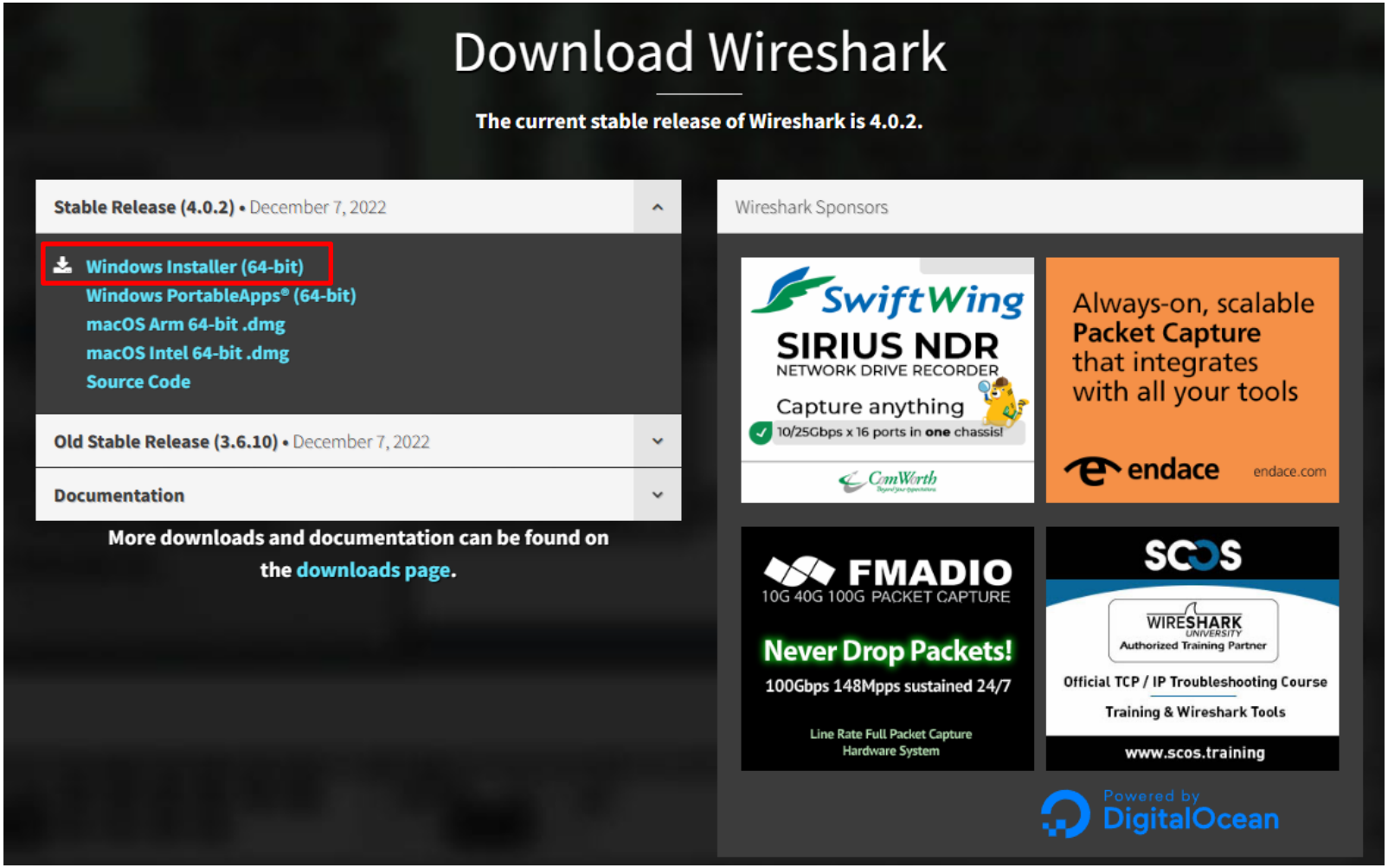
- 와이어샤크와 Npcap은 와이어샤크의 공식 홈페이지에서 무료로 다운받을 수 있다.
- 웹 브라우저에서 와이어샤크의 홈페이지(http://www.wireshark.org)에 접속하여 Download(Get Started Now)를 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 다운로드

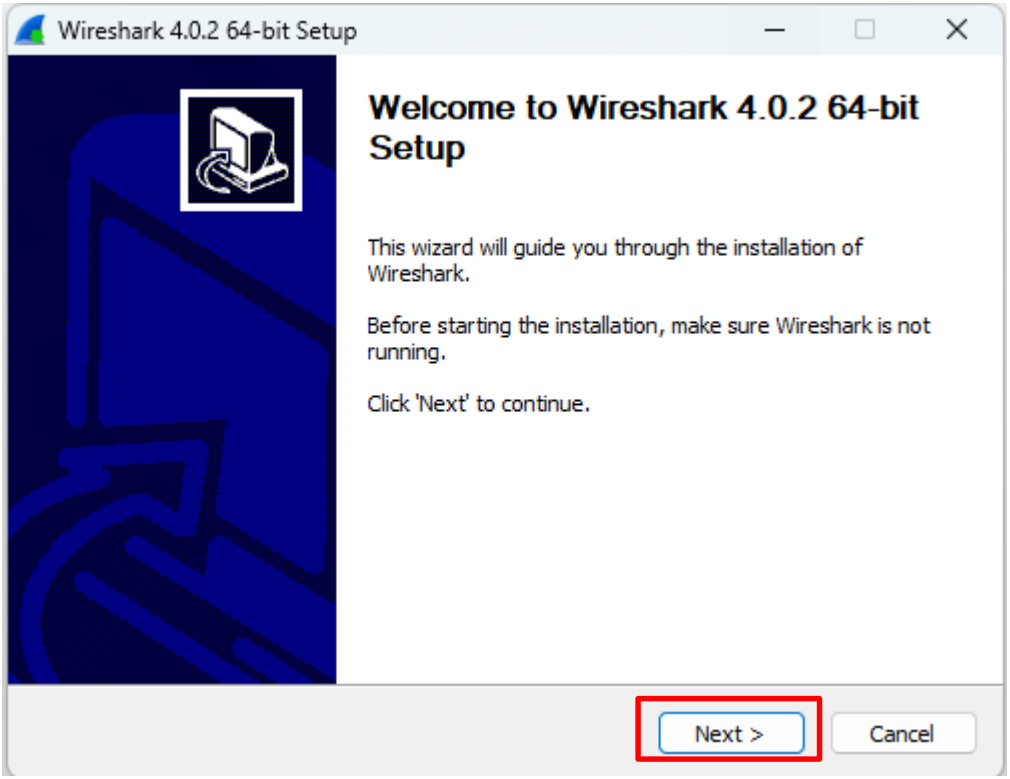
- 다운로드 페이지(https://www.wireshark.org/#download)에서 안정판(Stable Release)에 있는 항목 중 사용자의 OS에 맞는 설치 파일을 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

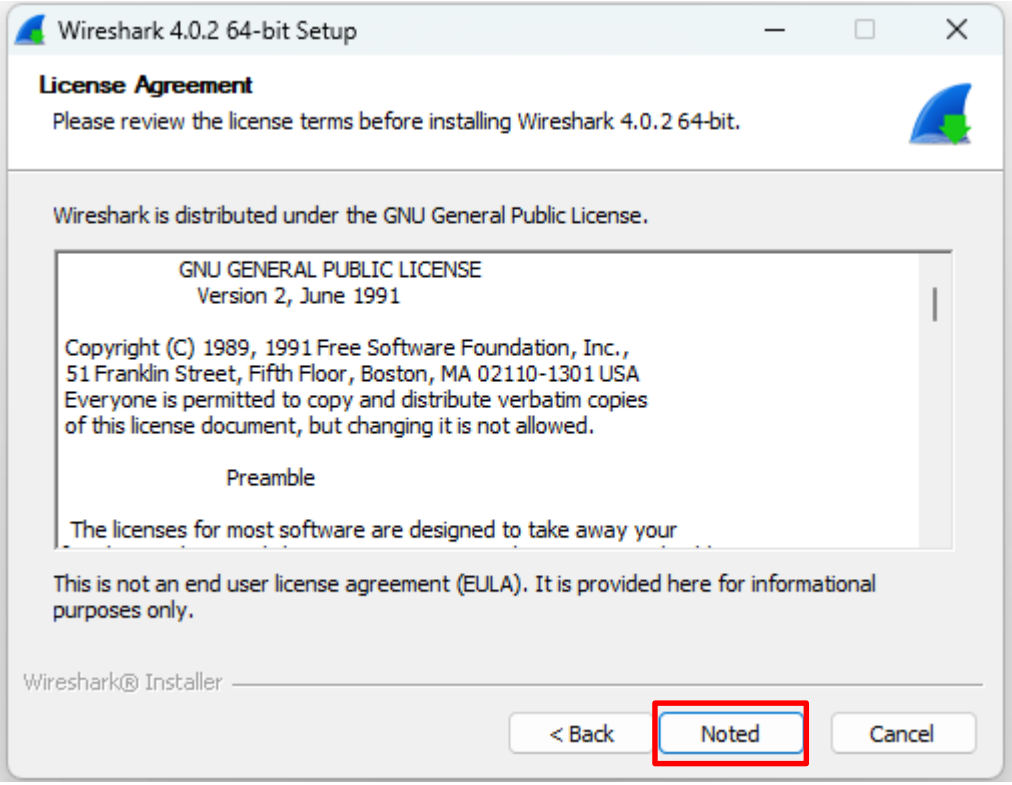
- 파일 탐색기에서 다운로드 폴더로 들어가서 폴더 안에 있는 와이어샤크 설치 파일을 실행한다.
- Wireshark Setup Wizard 화면이 나타나면 [Next] 버튼을 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

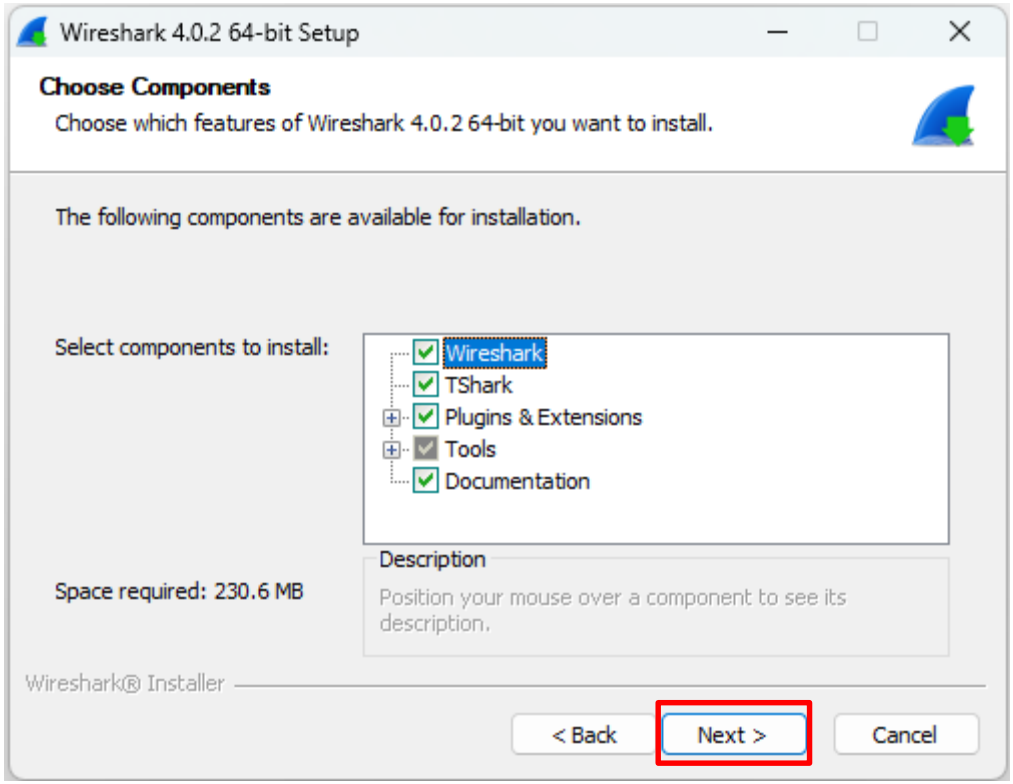
- 그러면 License Agreement(라이센스 동의) 화면이 나타나면 [Noted] 버튼을 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

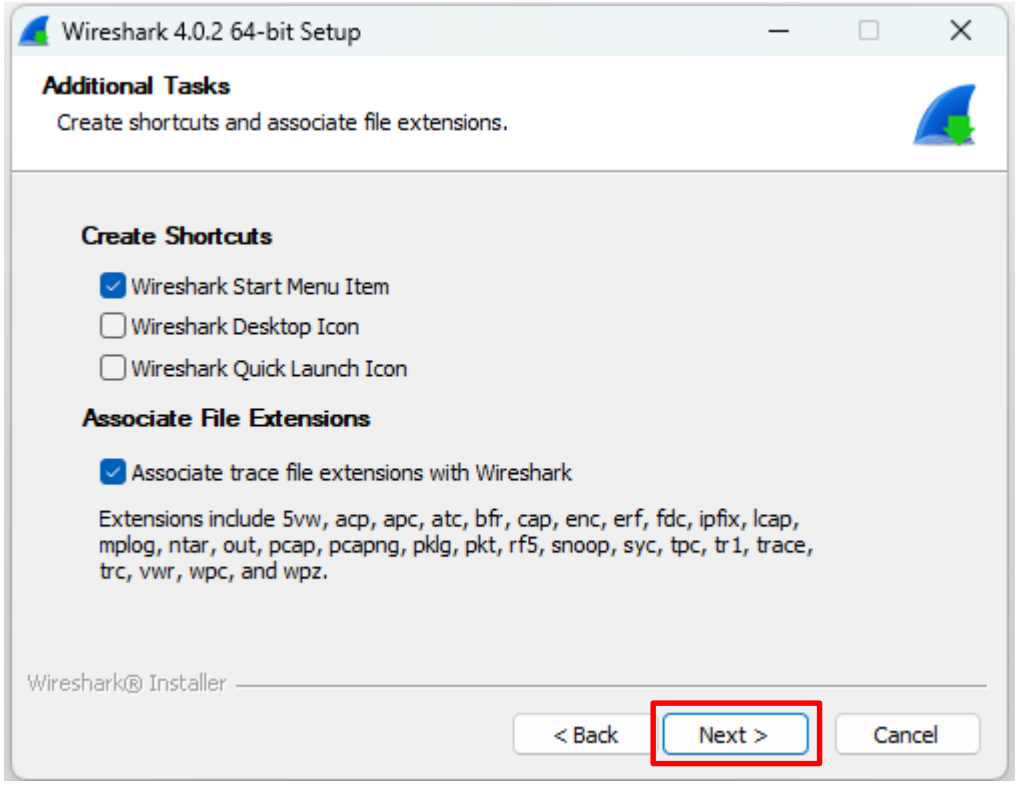
- 그러면 Choose Components(컴포넌트 선택) 화면이 나타난다.
- 여기서 설치할 컴포넌트를 선택한다.
- 그냥 디폴트대로 하면 된다.
- 그런 다음 [Next] 버튼을 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

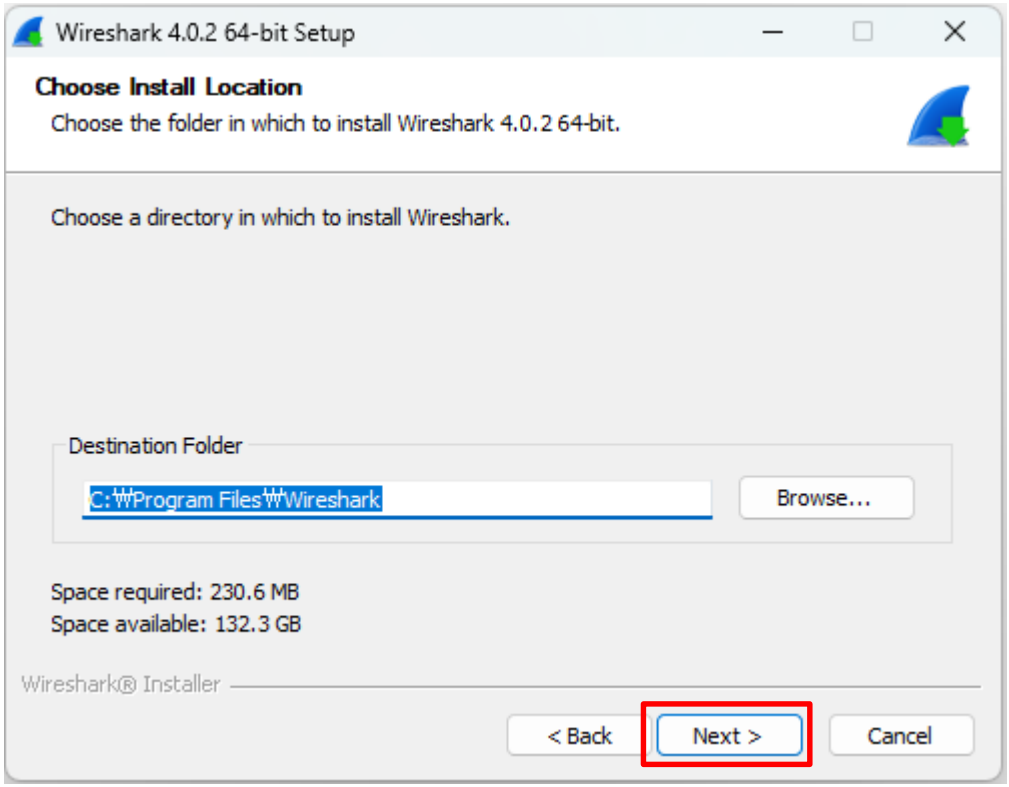
- 추가 태스크 선택 화면(Select Additional Tasks)이 나타난다.
- 추가할 태스크를 선택한다.
- 이 화면에서도 [Next] 버튼을 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

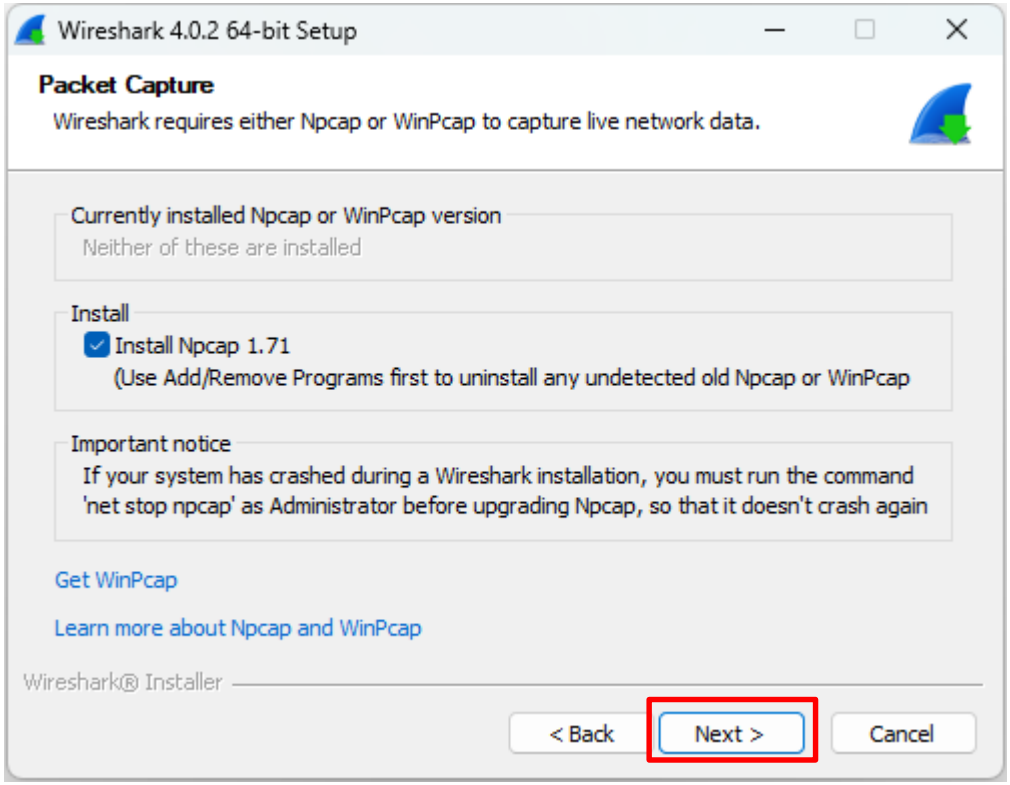
- 그러면 설치 장소 선택 화면이 나타난다.
- 여기서 [Destination Folder]란의 텍스트 박스에 설치할 장소의 경로를 지정하려면 [Browse ...] 버튼을 클릭하여 설치할 곳을 입력하면 된다.
- 디폴트는 [C:₩Program Files₩Wireshark]이다.
- 그냥 [Next] 버튼을 클릭하면 된다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

- 'Npcap을 설치할 것인지?' 를 묻는 화면이 나타난다.
- [Install] 란의 [Install Npcap 1.10]에 체크가 되어있음을 확인하고 [Next] 버튼을 클릭한다.



4. 와이어샤크 설치와 실행

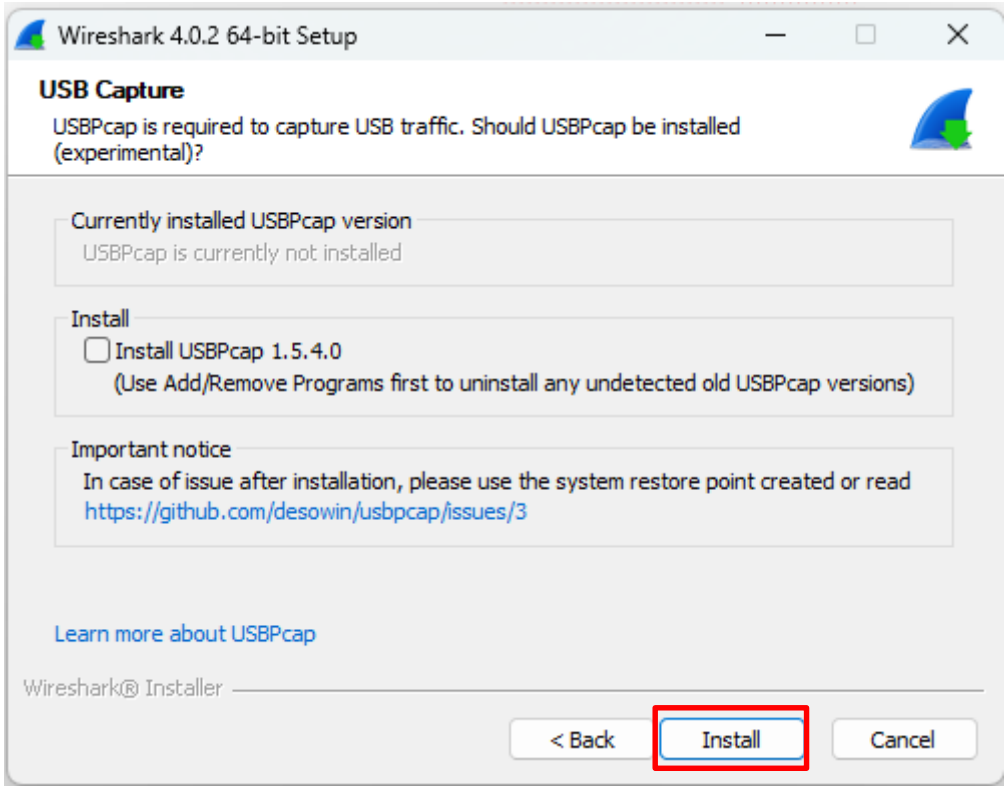
와이어샤크 설치

- 이때에 Npcap이 이미 설치되어 있으면 [Currently installed Npcap or WinPcap version]란에 현재 Npcap의 버전이 나타난다.
- 여기서 Npcap의 버전이 최신 것이 아니면 설치 화면이 나타나고 최신 버전의 설치 화면이 열린다.
- 또한 이전에 Ethereal 이나 와이어샤크를 사용하고 있어서 이전 버전의 Npcap이 설치되어 있으면 설치할 때에 트러블의 원인이 될 수 있다.
- 따라서 윈도우즈의 [프로그램 추가와 삭제] 화면에서 이전 버전의 와이어샤크나 Npcap을 미리 삭제해 놓는 것이 좋다.

4. 와이어샤크 설치와 실행

와이어샤크 설치

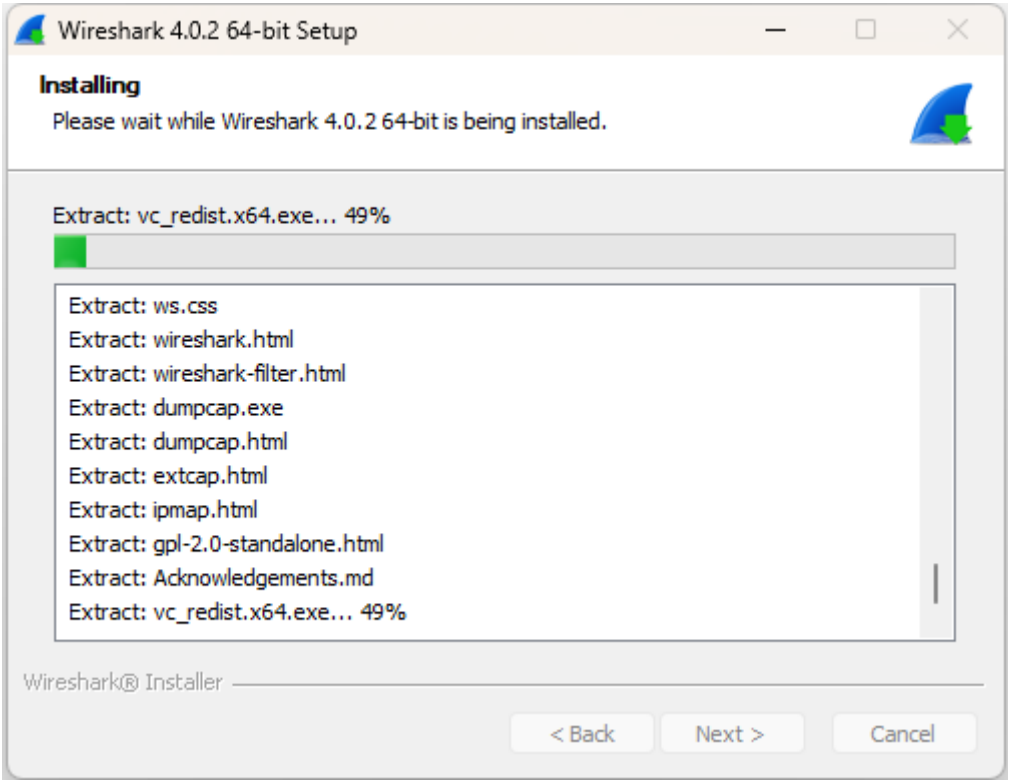
- 그런 다음 USB 트래픽을 캡처하기 위한 USBPcap 설치를 묻는 화면이 나타난다.
- 이것은 USB 트래픽을 캡처하기 위한 캡처 드라이버이다.
- 설치를 계속하려면 [Install] 버튼을 클릭한다.
- 그러면 와이어샤크 설치가 계속된다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

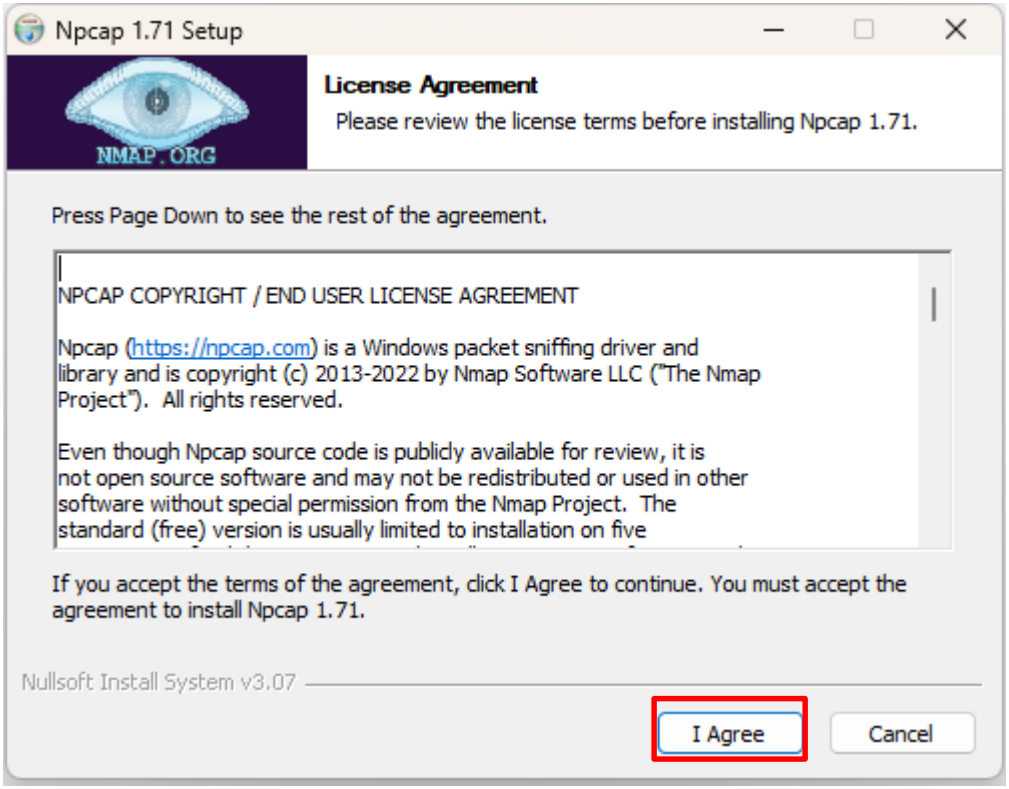
- 그런 다음 설치 진척 상황 화면에서 progress bar(녹색)가 진행되고 있음을 확인한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

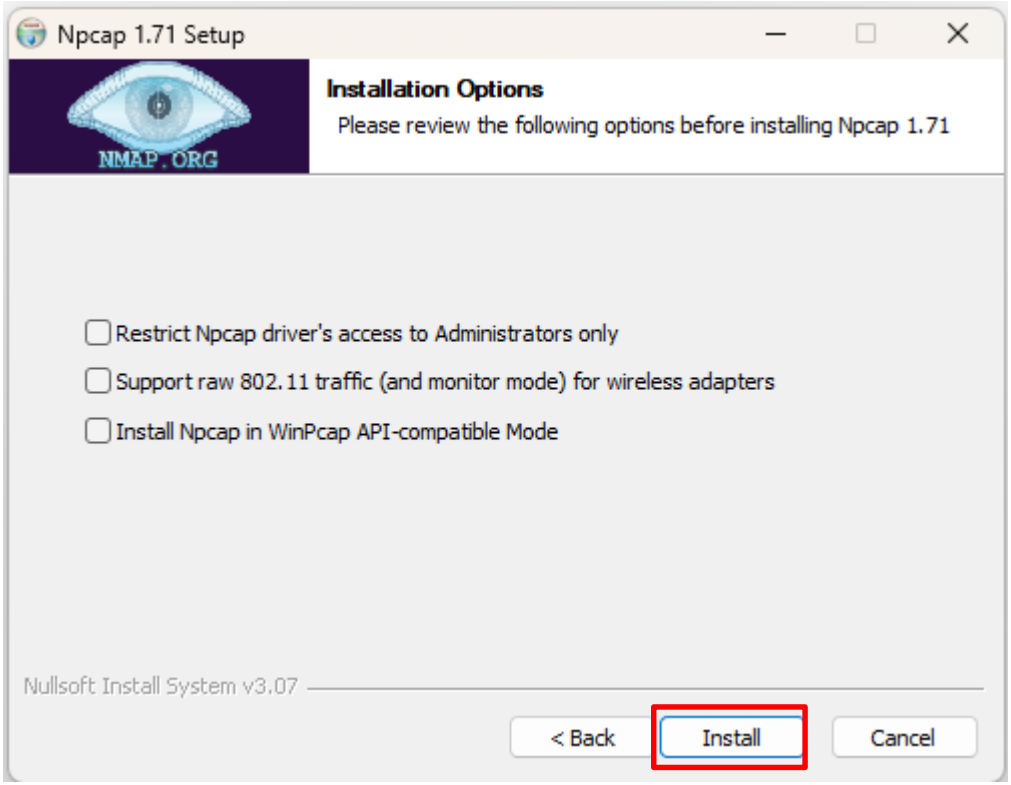
- 와이어샤크가 설치되는 과정에 Npcap의 License Agreement(라이센스 동의) 화면이 나타난다.
- 여기서 [I Agree]를 누르면 Installation Options(설치 옵션) 화면이 나타난다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

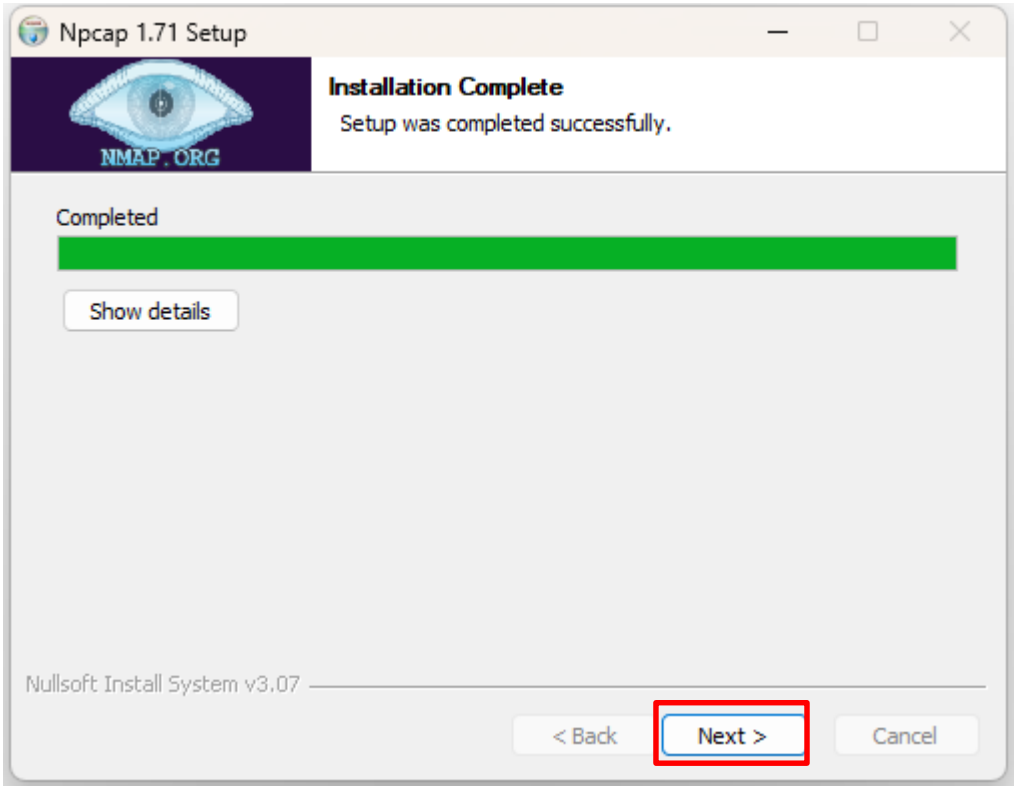
- 필요한 경우 옵션을 선택할 수 있다.
- 그리고 여기서 [Install] 버튼을 클릭한다.
- 만약 최신 Npcap이 이미 설치되어 있는 경우에는 이 화면은 나타나지 않는다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

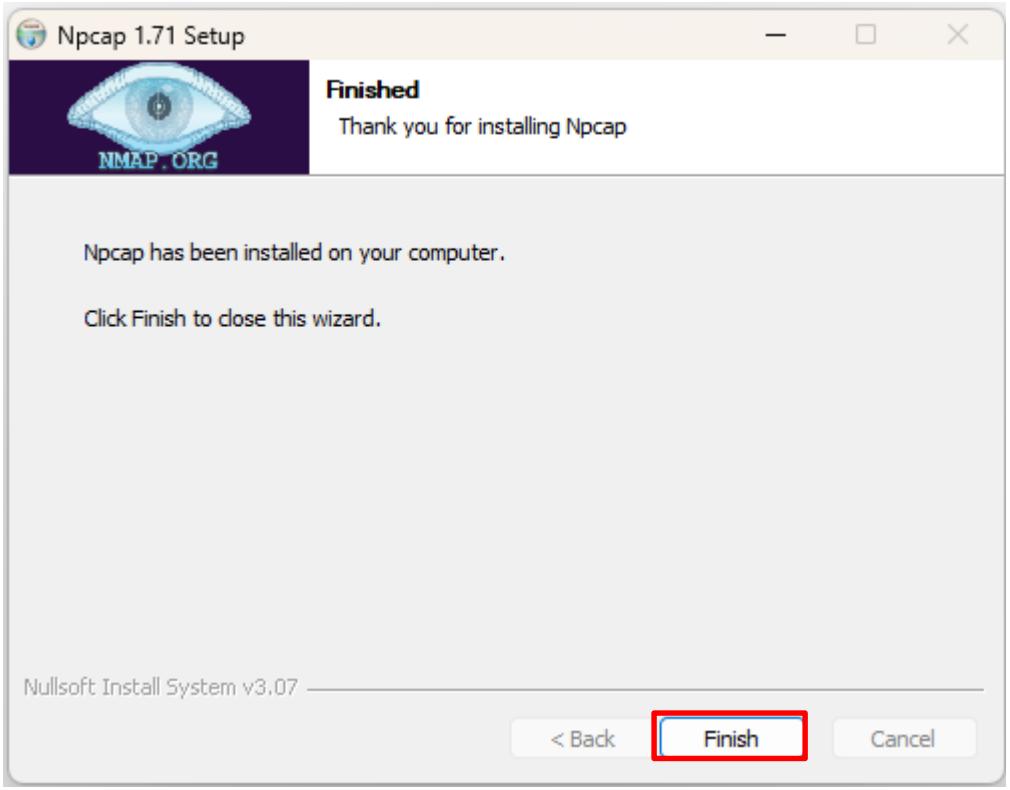
- 그러면 Npcap의 설치가 시작된다.
- 설치가 완료(Installation Complete)되면 [Next] 버튼을 클릭한다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

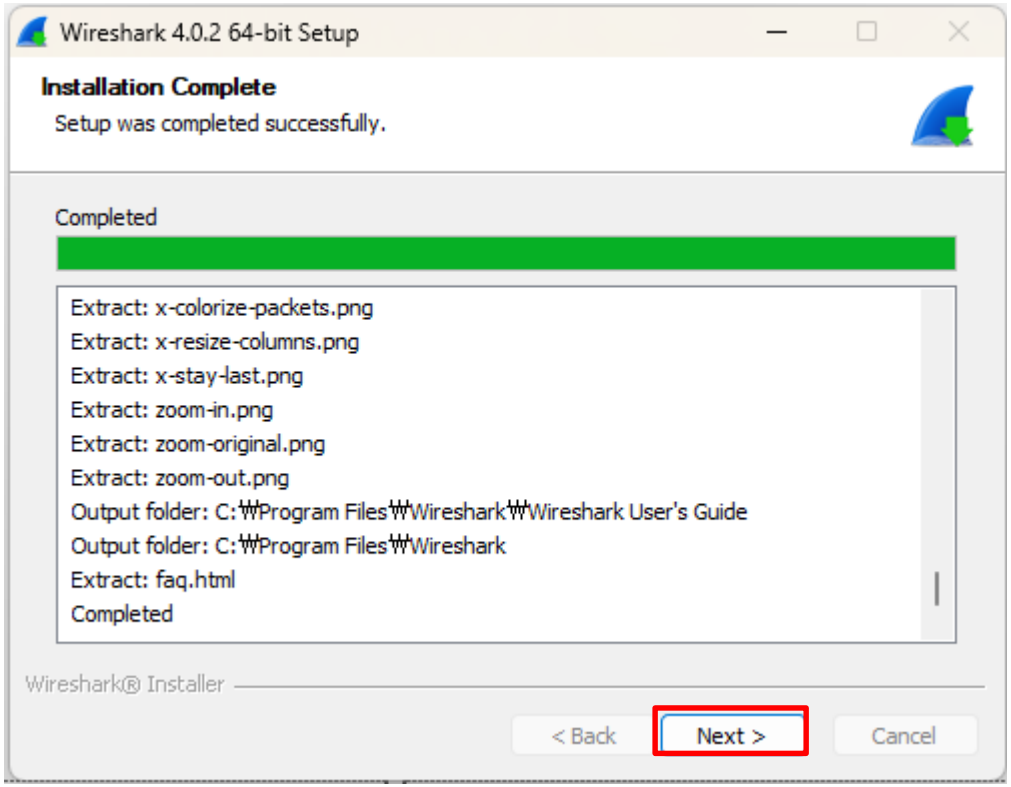
- Npcap의 설치가 종료되면 화면에 [Finished]라고 나타난다.
- 내용을 확인하고 [Finish] 버튼을 클릭한다.
- 이제 Npcap의 설치가 완료된 것이다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

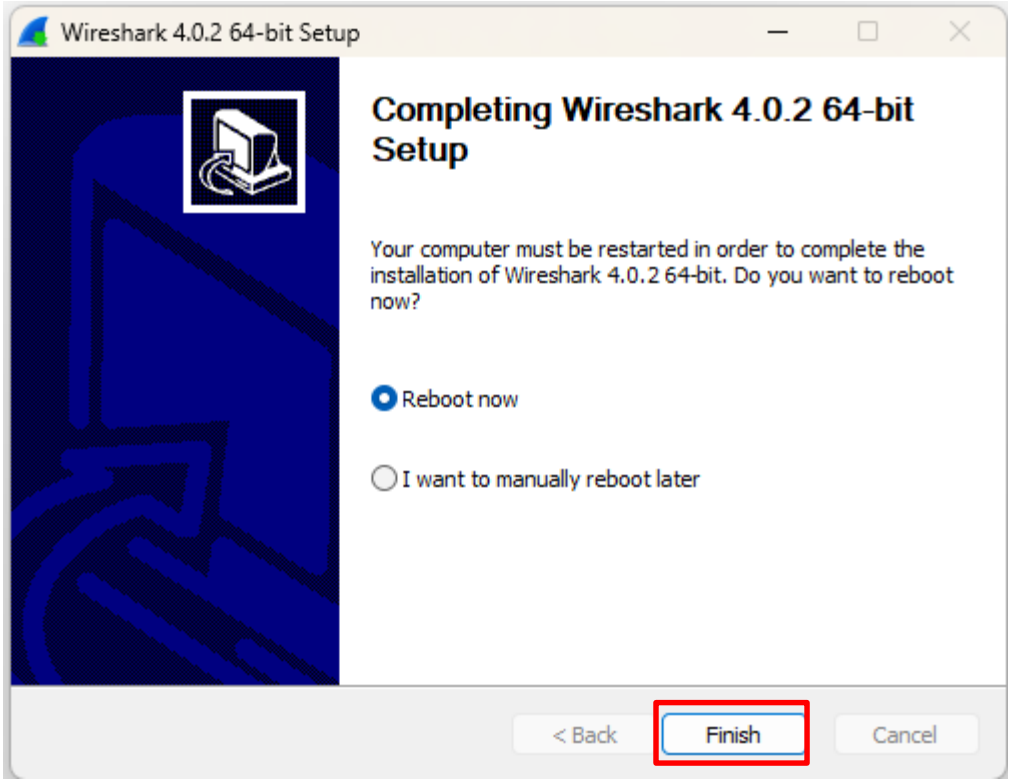
- Npcap의 설치가 완료된 후에도 와이어샤크의 설치는 계속된다.
- Progress Bar가 진행되고 있으므로 내용을 확인하기 바란다.
- Progress Bar가 끝까지 진행되면 화면상에 [Installation Complete], Progress Bar에 [Completed]라고 나타난다.
- 이제 [Next] 버튼을 클릭하면 Wireshark Setup 화면이 나타난다.



4. 와이어샤크 설치와 실행

와이어샤크 설치

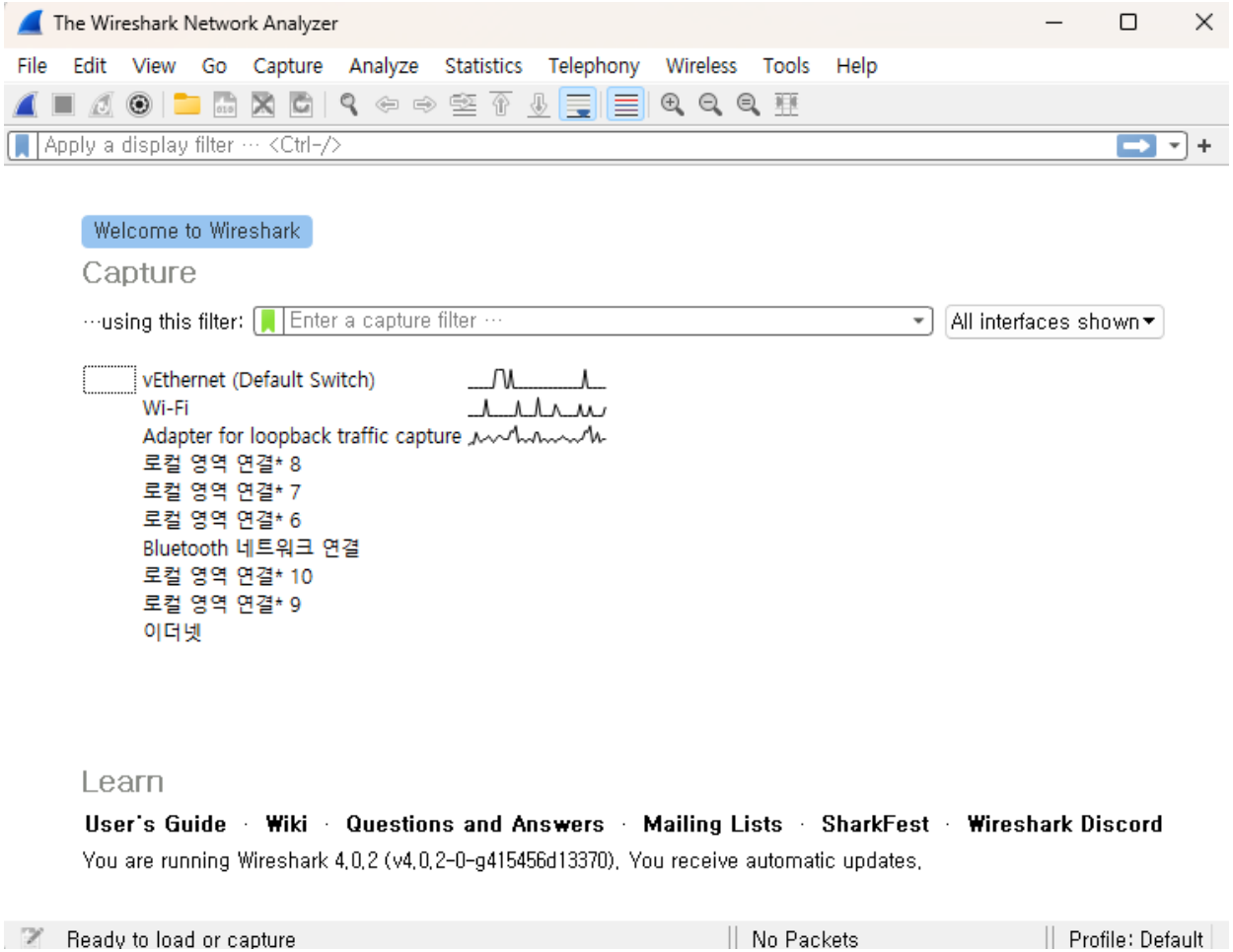
- 이것으로 와이어샤크의 설치가 완료된 것이다.
- 여기서 [Reboot now]를 선택하면 와이어샤크의 완전한 설치를 위해 재부팅을 하게 된다.
- 또한 [I want to manually reboot later]를 체크하면 나중에 재부팅을 한다.
- 하지만 USBPcap을 설치했을 경우에는 반드시 재실행이 필요하다.



4. 와이어샤크 설치와 실행

설치 확인과 시작

- 와이어샤크의 설치가 종료되면 윈도우즈의 「시작」 메뉴에서 와이어샤크를 실행할 수 있다.
- 그러면 그림과 같이 시작 화면이 나타난다.

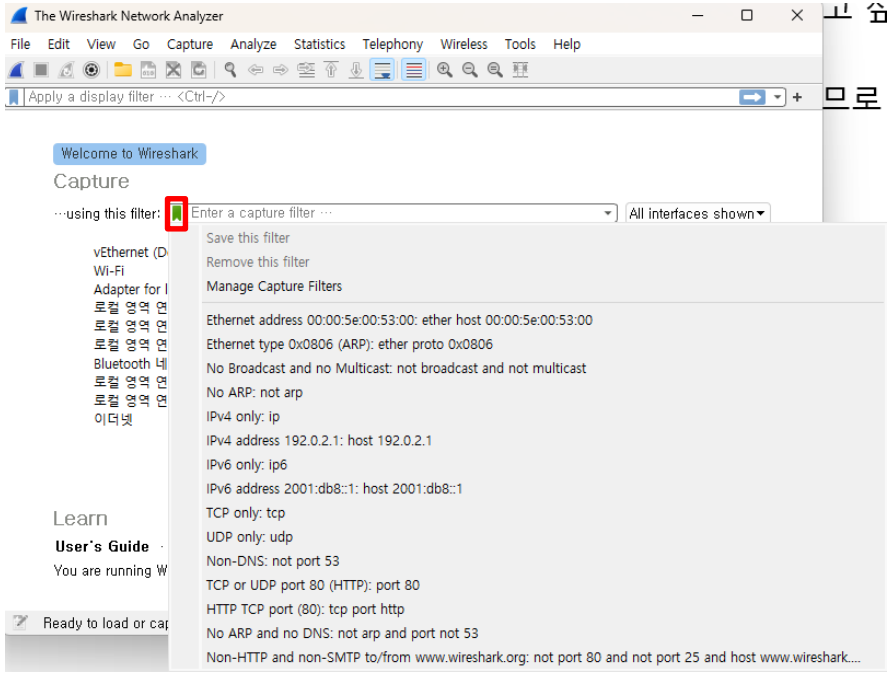


4. 와이어샤크 설치와 실행

와이어샤크 시작 화면

- 시작 화면은 와이어샤크 주요 작업을 시작할 수 있게 되어있다.
- 화면은 크게 [Capture(캡처), [Learn(학습)] 영역으로 구분되어 있다.

- **Capture(캡처)란?**
  - 맨 먼저 " ... using this filter: "란이 있는데, 여기는 패킷을 캡처할 때 적용하고 싶은 필터를 "Enter a capture filter ... "란에 직접 입력하면 된다.
  - 이때 화면의 녹색 부분을 마우스로 클릭하면 선택할 수 있는 목록이 나타나므로 원하는 것을 선택하면 된다.

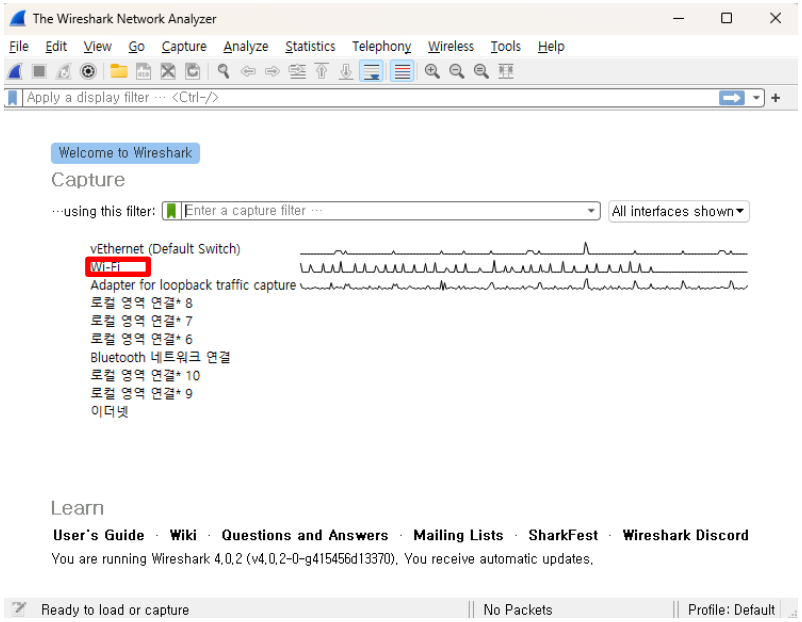


4. 와이어샤크 설치와 실행

와이어샤크 시작 화면

- 시작 화면은 와이어샤크 주요 작업을 시작할 수 있게 되어있다.
- 화면은 크게 [Capture(캡처), [Learn(학습)] 영역으로 구분되어 있다.

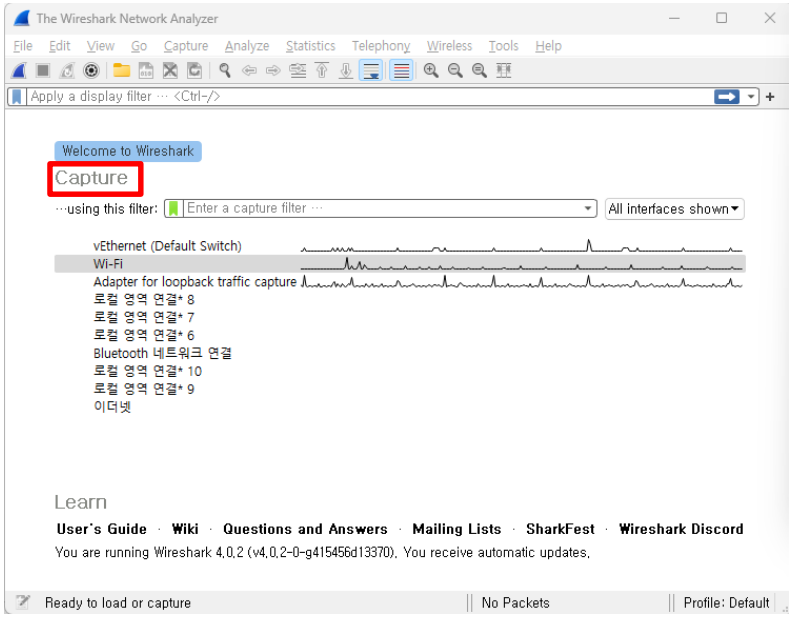
- **Capture(캡처)란?**
  - 그 밑에는 [Interface List]가 나타나는데, 이는 이더넷, 로컬 영역 연결, Wi-Fi, Adapter for Loopback traffic capture, USBPcap 등이다.
  - 여기서 그래프 모양이 나타나고 있는 이더넷을 선택하면 바로 무차별 모드로 캡처가 시작된다.

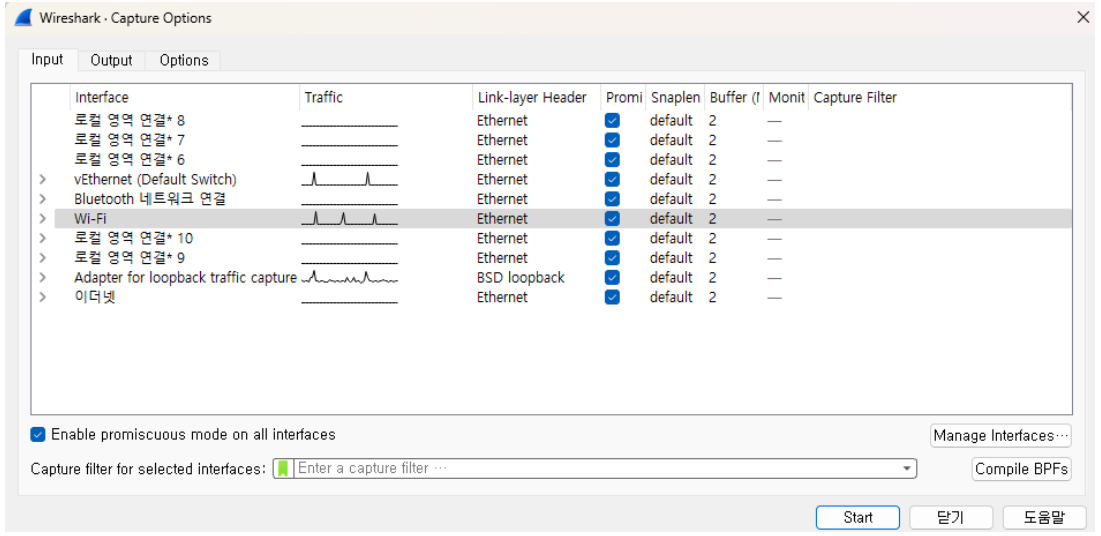


4. 와이어샤크 설치와 실행

와이어샤크 시작 화면

- **Capture(캡처)란?**
  - 그리고 우측 끝에 있는 [All interfaces shown]의 아래 화살표를 선택하면 디스플레이하고 있는 인터페이스를 알려준다.
  - 그리고 [Capture]를 클릭하면 와이어샤크(및 캡처 드라이버)에서 인식된 캡처 인터페이스 목록이 나타난다.
  - 윈도우 환경일 경우에는 IPv6 링크 로컬 인터페이스나 터널 인터페이스 가상 환경에 대해서도 캡처 드라이버에서 인식된다고 나타나므로 주의하기 바란다.





4. 와이어샤크 설치와 실행

와이어샤크 시작 화면

Capture(캡처)란?

- 각 인터페이스의 오른쪽에는 꺾은선 그래프로 패킷의 캡처 상태가 나타난다.
- 이 인터페이스에서 패킷을 캡처하고 있으면 꺾은선 그래프 상태로 나타나고 이를 통해 트래픽 양을 확인할 수 있다.
- 또한 인터페이스에 마우스를 맞추면 그 인터페이스의 주소 정보도 확인할 수 있다.
- 각 인터페이스는 클릭하면 선택된 상태가 되며 캡처 필터를 지정하거나 더블클릭하여 캡처를 시작할 수 있다.
- 또한 [Ctrl + 클릭]으로 복수의 인터페이스를 개별적으로 선택하거나 [Shift + 클릭]으로 복수의 인터페이스를 한 번에 지정할 수 있다.

4. 와이어샤크 설치와 실행

와이어샤크 시작 화면

- **Learn란?**
  - 와이어샤크를 배우기 위한 링크가 나타난다.
  - 이 영역에는 User's Guide, WiKi, Questions and Answers, Mailing Lists가 나타나는데, 이 시점에서 원하는 항목을 선택하면 해당 홈페이지가 나타난다.
  - 이렇게 시작 화면이 잘 나타나면 와이어샤크의 설치가 완료된 것이다.
  - 와이어샤크를 종료하고자 할 때는 화면 우측 상단 맨 끝에 있는 [x]를 클릭하면 된다.

4. 와이어샤크 설치와 실행

와이어샤크 커맨드 라인 인터페이스

커맨드 라인 도구설치 확인

- 먼저 커맨드 라인 도구가 정상적으로 설치되어 있는지 확인한다.
- 윈도우즈의「시작」메뉴에서「모든 프로그램」-「보조 프로그램」-「명령 프롬프트」를 선택한다.
- 그리고 명령 프롬프트가 나타나면 [cd "c:₩Program Files₩Wireshark"]라고 입력하고 엔터키를 누른다.
- 그러면 해당 디렉토리로 이동한다.
- 다음에 [dir *.exe]라고 입력하고 엔터키를 누른다.
- 그러면 이 디렉토리에 있는 실행 프로그램이 나타난다.
- 모든 도구가 설치되면 같이 다음 파일이 나타난다.

• editcap.exe	• text2pcap.exe	• reordercao.exe	• mergecap.exe
• capinfos.exe	• tshark.exe	• rawshark.exe	• dumpcap.exe

4. 와이어샤크 설치와 실행

와이어샤크 커맨드 라인 인터페이스

커맨드 라인 도구설치 확인

- 그림은 윈도우즈에서 명령 프롬프트를 이용하여 화면에 나타난 예이다.

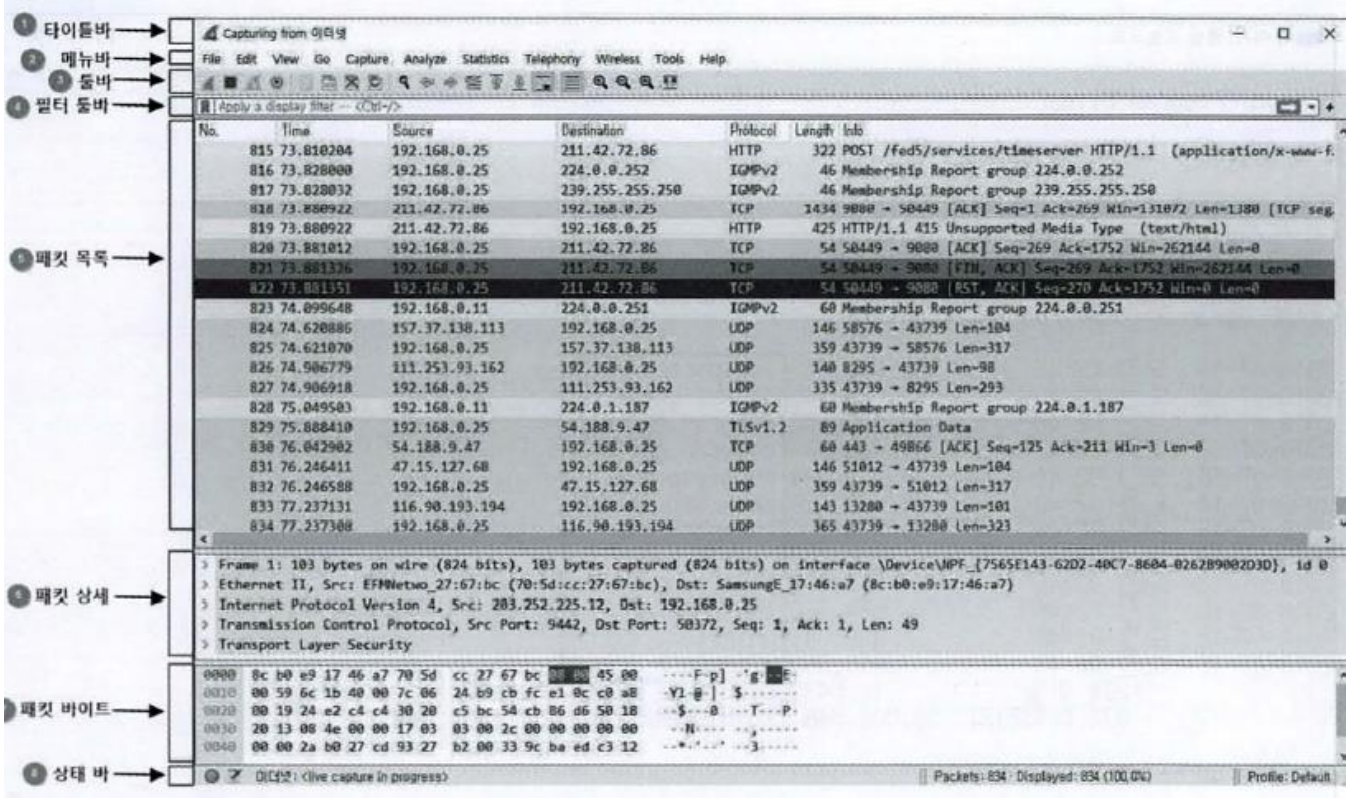
```
C:\Users\jinu>cd \

C:\>cd "Program Files"

C:\Program Files>cd Wireshark

C:\Program Files\Wireshark>dir *.exe
 C 드라이브의 볼륨에는 이름이 없습니다.
 볼륨 일련 번호: 460E-597A

 C:\Program Files\Wireshark 디렉터리

2022-12-08  오전 03:39           348,640 capinfos.exe
2022-12-08  오전 03:39           329,184 captype.exe
2022-12-08  오전 03:39           326,624 dftest.exe
2022-12-08  오전 03:39           435,680 dumpcap.exe
2022-12-08  오전 03:39           362,464 editcap.exe
2022-12-08  오전 03:39           335,328 mergecap.exe
2022-12-08  오전 03:39           338,400 mmdbresolve.exe
2022-11-10  오전 12:45         1,149,544 npcap-1.71.exe
2022-12-08  오전 03:39           387,040 rawshark.exe
2022-12-08  오전 03:39           331,232 reordercap.exe
2022-12-08  오전 03:39           370,656 text2pcap.exe
2022-12-08  오전 03:39           604,640 tshark.exe
2022-12-08  오전 03:39           445,136 uninstall-wireshark.exe
2022-12-08  오전 03:39         9,010,144 Wireshark.exe
              14개 파일          14,774,712 바이트
               0개 디렉터리  141,586,358,272 바이트 남음
```

4. 와이어샤크 설치와 실행

■ 와이어샤크 사용자 인터페이스

▪ 와이어샤크의 메인 화면 구성

- 먼저 실제로 패킷 캡처를 하기 전에 화면의 구성을 살펴본다.
- 와이어샤크의 화면은 대부분의 윈도우즈 애플리케이션 화면과 비슷하다.

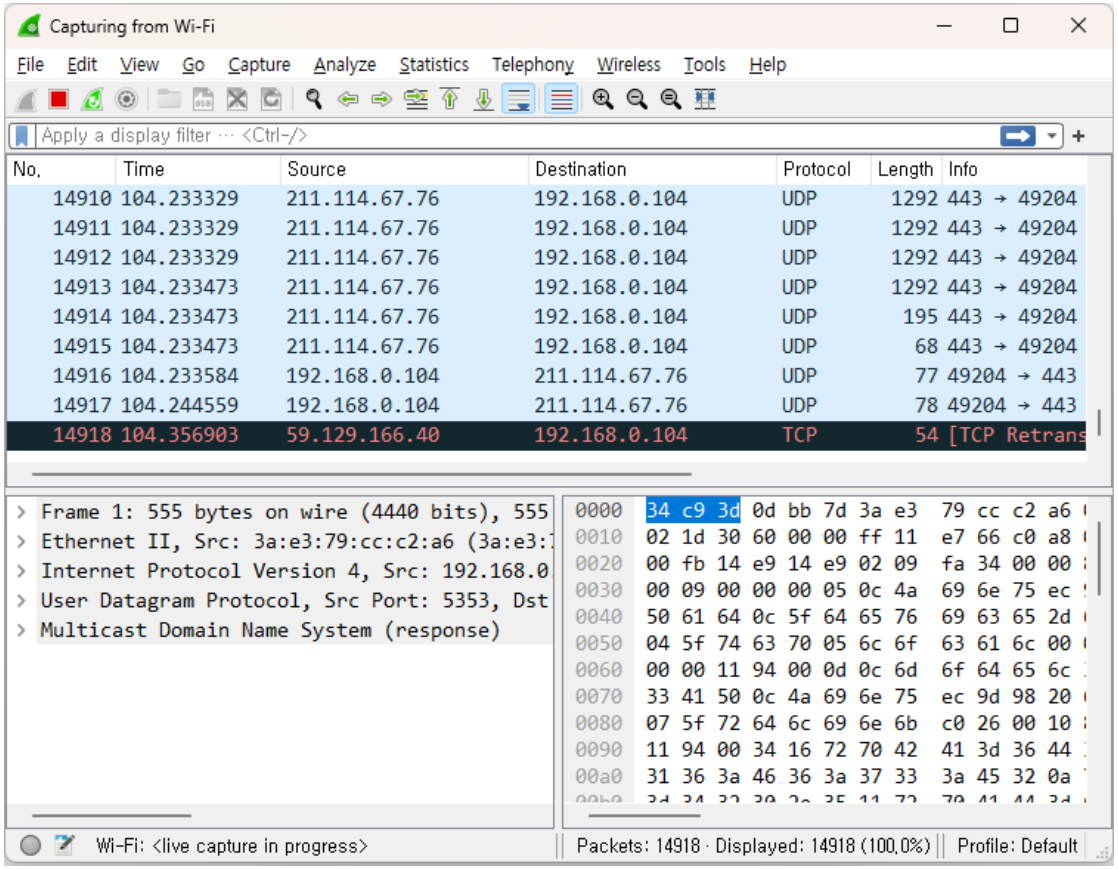


4. 와이어샤크 설치와 실행

와이어샤크 사용자 인터페이스

와이어샤크 화면을 자세히 살펴보자

- 먼저 실제로 패킷 캡처를 하기 전에 화면의 구성을 살펴본다.
- 와이어샤크의 화면은 대부분의 윈도우즈 애플리케이션 화면과 비슷하다.

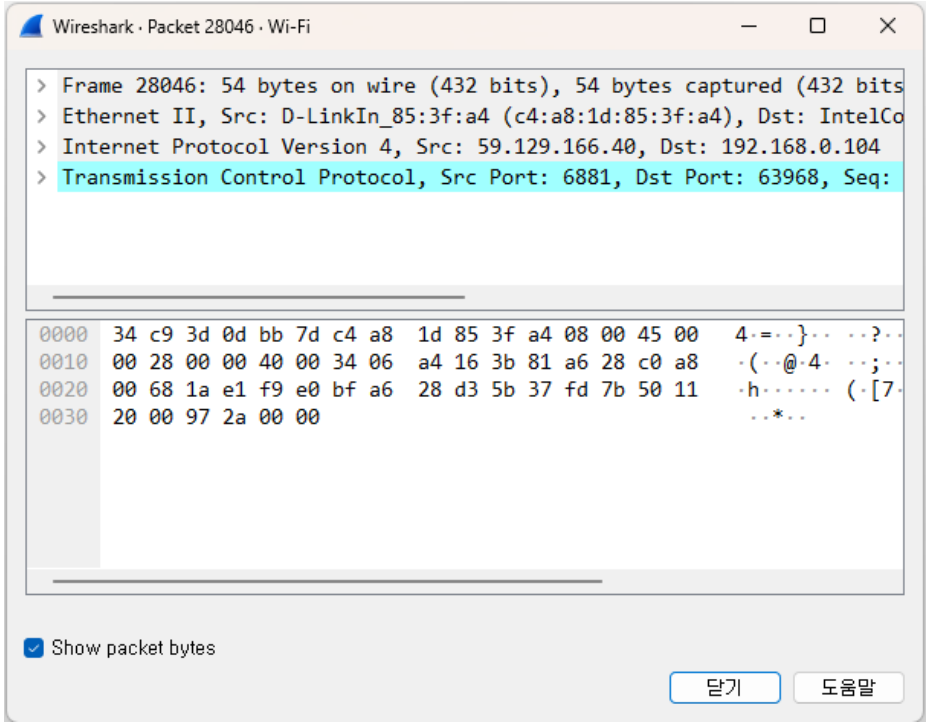


4. 와이어샤크 설치와 실행

와이어샤크 사용자 인터페이스

와이어샤크 화면을 자세히 살펴보자

- 패킷 목록 정보는 캡처한 패킷의 개요를 보여준다.
- 한 줄에 하나의 패킷(Ethernet 프레임)씩 보여주며 간단한 설명이 들어있다.
- 이 중에 하나의 패킷을 더블클릭하면 그 패킷의 상세 내용이 패킷 상세 정보와 패킷 바이트 정보에 나타난다.



Thank You