Wireshark 기초

Wireshark란?

- **Wireshark**는 네트워크 트래픽을 실시간으로 캡처하고 분석하는 데 사용되는 강력한 **오픈 소스 네트워크 프로토콜 분석기**입니다.
- 네트워크의 "귀"라고 생각하시면 됩니다. 네트워크를 오가는 모든 데이터를 엿듣고, 그 내용을 상세하게 보여줍니다.
- **주요 기능:**
  - 실시간 네트워크 데이터 캡처
  - 수백 가지 프로토콜 지원 및 상세 분석
  - 필터링 기능을 통한 특정 패킷 검색
  - 다양한 파일 형식으로 캡처된 데이터 저장 및 로드
  - 그래프 및 통계 분석

Wireshark이 활용

- **네트워크 문제 해결:** 연결 지연, 패킷 손실 등 네트워크 문제를 진단합니다.
- **네트워크 보안 분석:** 의심스러운 활동이나 악성 트래픽을 탐지합니다.
- **프로토콜 개발 및 디버깅:** 새로운 프로토콜 개발 시 통신 흐름을 검증합니다.
- **네트워크 성능 분석:** 대역폭 사용량, 트래픽 패턴 등을 파악하여 성능을 최적화합니다.
- **네트워크 교육:** 실제 네트워크 통신 과정을 시각적으로 이해하는 데 도움을 줍니다.

Wireshark 설치하기 1 (다운로드)

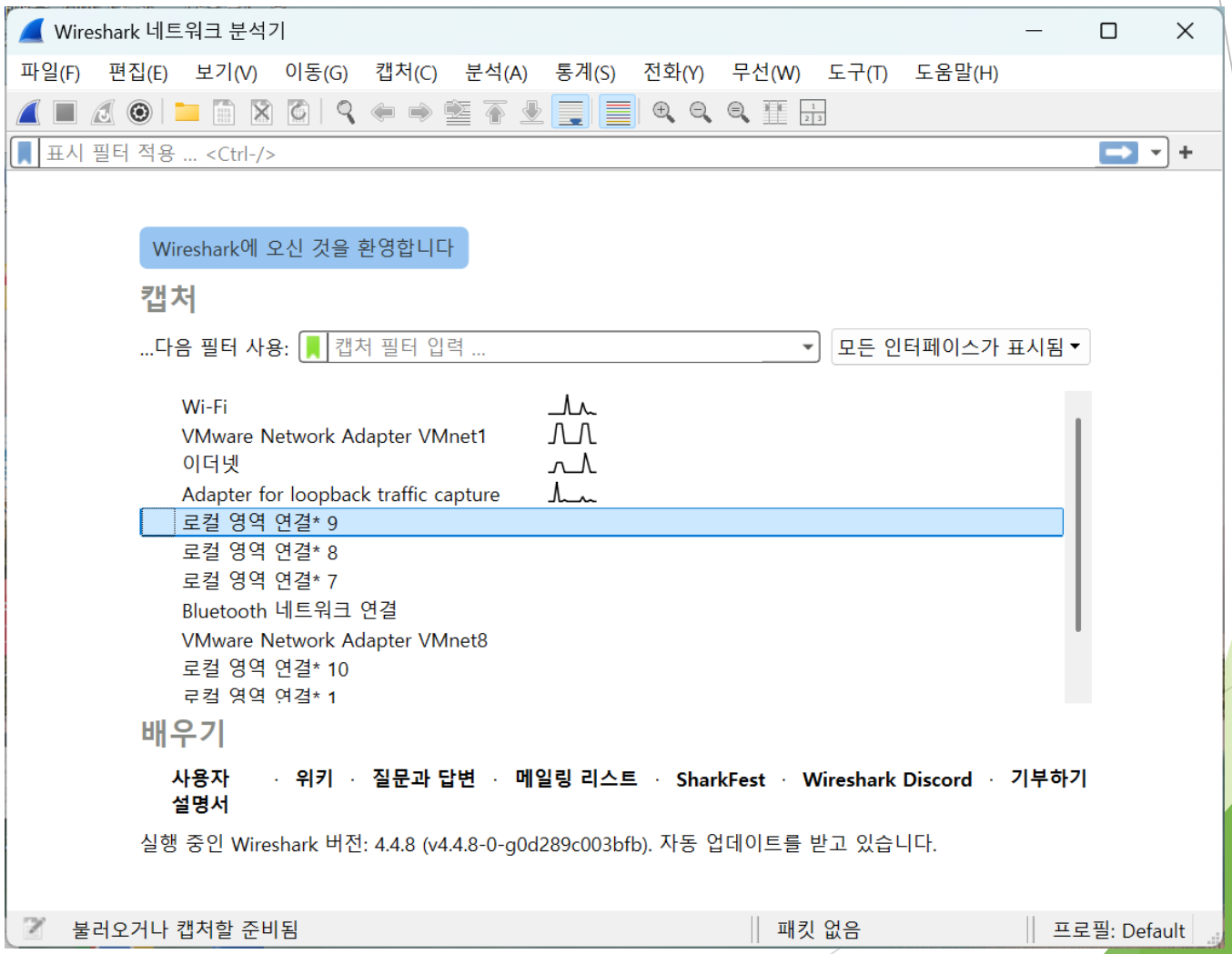
- Wireshark 공식 웹사이트에 접속합니다: https://www.wireshark.org/download.html
- 사용 중인 운영체제(Windows, macOS, Linux 등)에 맞는 설치 파일을 다운로드합니다.

Wireshark 설치하기 2 (설치 과정-Windows 기준)

- 다운로드한 .exe 설치 파일을 더블 클릭하여 실행합니다.
- Next를 클릭하여 설치를 시작합니다.
- 구성 요소 선택 화면에서는 기본 설정을 유지하고 Next를 클릭합니다. (특별한 경우가 아니라면 변경할 필요 없습니다.)
- 바로가기 생성 및 파일 연결 설정 화면도 기본 설정을 유지하고 Next를 클릭합니다.
- **NPcap 설치:** Wireshark는 네트워크 인터페이스에서 패킷을 캡처하기 위해 **NPcap**이라는 드라이버가 필요합니다.
  - Install Npcap을 반드시 **체크**하고 Next를 클릭합니다.
  - NPcap 설치 마법사가 시작되면 I Agree를 클릭하여 동의하고 설치를 진행합니다.
  - NPcap 설치가 완료되면 Finish를 클릭합니다.
- Wireshark 설치 위치를 지정합니다. 기본 경로를 권장하며 Next를 클릭합니다.
- Install을 클릭하여 Wireshark 설치를 시작합니다.
- 설치가 완료되면 Finish를 클릭하여 마법사를 종료합니다.

Wireshark 기본 화면

- Wireshark를 실행하면 다음과 같은 기본 화면을 볼 수 있습니다.



Wireshark 화면 주요 영역 1

- **캡처 인터페이스 목록:** 패킷을 캡처할 수 있는 네트워크 인터페이스 목록을 보여줍니다. (예: 이더넷, Wi-Fi 등)
- **캡처 필터 입력창:** 특정 조건을 만족하는 패킷만 캡처하도록 필터를 설정합니다.
- **표시 필터 입력창:** 이미 캡처된 패킷 중 특정 조건을 만족하는 패킷만 화면에 표시하도록 필터를 설정합니다.
- **패킷 목록 창 (Packet List Pane):** 캡처된 패킷들의 요약 정보를 보여줍니다.
  - **No.:** 패킷 번호
  - **Time:** 캡처된 시간
  - **Source:** 출발지 IP 주소
  - **Destination:** 목적지 IP 주소
  - **Protocol:** 사용된 프로토콜 (HTTP, TCP, UDP 등)
  - **Length:** 패킷 길이
  - **Info:** 패킷에 대한 간략한 정보

첫 패킷 캡처하기

1. **캡처할 인터페이스 선택:** Wireshark 초기 화면에서 패킷을 캡처할 네트워크 인터페이스(예: 유선 LAN을 사용한다면 Ethernet, Wi-Fi를 사용한다면 Wi-Fi)를 클릭하여 선택합니다.

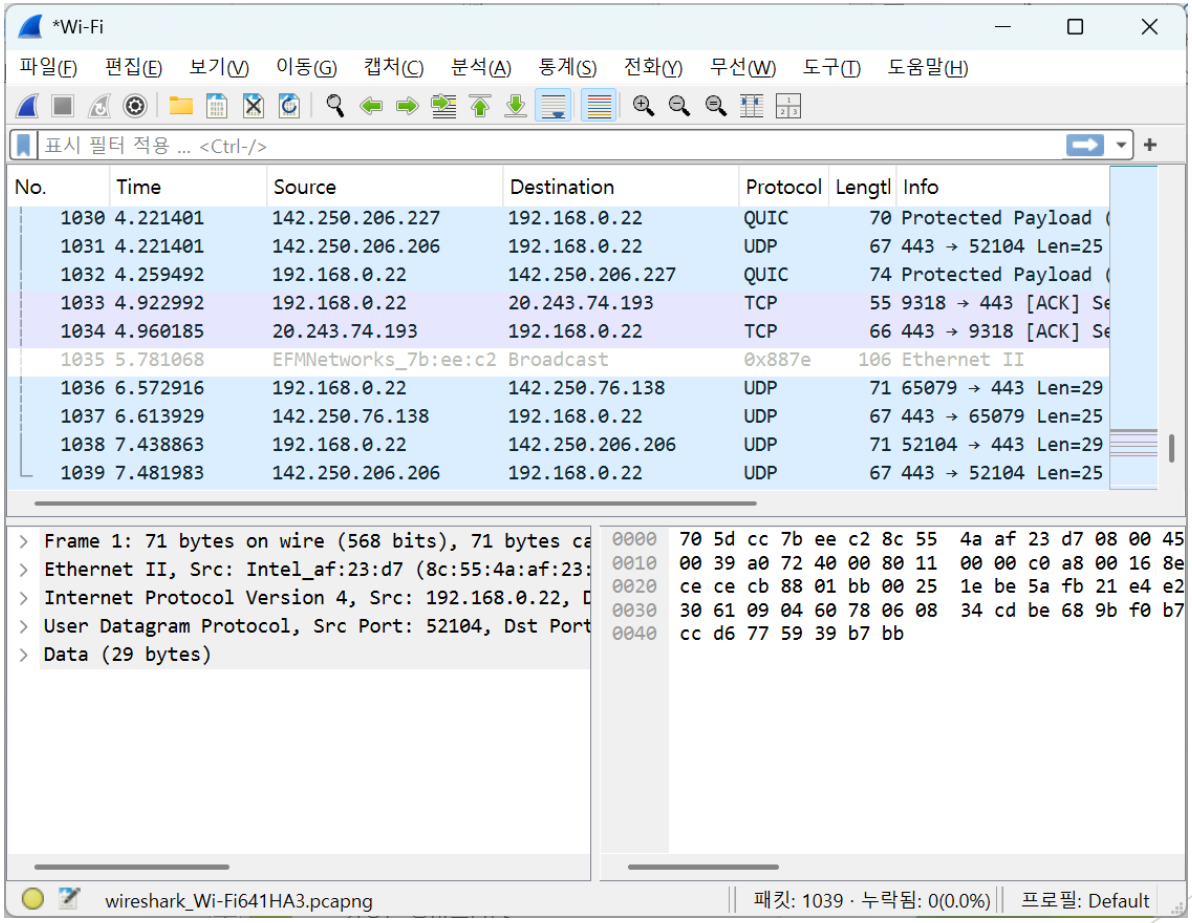
   - 인터페이스 옆에 그래프가 활발하게 움직이는 것이 현재 트래픽이 있는 인터페이스입니다.

2. **캡처 시작:** 선택한 인터페이스를 더블 클릭하거나, 상단 도구 모음에서 **파란색 지느러미 아이콘** (Start capturing packets)을 클릭합니다.

3. **패킷 확인:** 캡처가 시작되면 네트워크를 오가는 패킷들이 패킷 목록 창에 실시간으로 나타납니다.

4. **캡처 중지:** 상단 도구 모음에서 **빨간색 사각형 아이콘** (Stop capturing packets)을 클릭하여 캡처를 중지합니다.

Wireshark 화면 주요 영역 2



- **패킷 상세 정보 창 (Packet Details Pane):** 선택된 패킷의 계층별 상세 정보를 보여줍니다. (이더넷, IP, TCP/UDP, 애플리케이션 계층 등)
- **패킷 바이트 창 (Packet Bytes Pane):** 선택된 패킷의 원본 데이터를 16진수 및 ASCII 값으로 보여줍니다.

기본 필터 사용법

- Wireshark의 필터는 크게 두 가지로 나뉩니다.
- **캡처 필터 (Capture Filters):** 패킷을 **캡처하기 전**에 특정 조건을 만족하는 패킷만 네트워크로부터 받아들이도록 설정합니다. 불필요한 패킷을 미리 걸러내어 파일 크기를 줄이고 분석 효율을 높입니다.
  - 캡처 인터페이스 목록 화면의 Capture filter for selected interface(s) 입력창에 입력합니다.
- **표시 필터 (Display Filters):** 이미 **캡처된 패킷들 중에서** 특정 조건을 만족하는 패킷만 화면에 표시하도록 설정합니다. 원본 캡처 파일은 그대로 유지됩니다.
- Wireshark 실행 후 상단 표시 필터 입력창에 입력합니다.

캡처 필터 (Capture Filters) 예시

필터	설명	예시
host [IP 주소]	특정 IP 주소와 관련된 패킷만 캡처	host 192.168.1.100
src host [IP 주소]	특정 출발지 IP 주소의 패킷만 캡처	src host 10.0.0.5
dst host [IP 주소]	특정 목적지 IP 주소의 패킷만 캡처	dst host 8.8.8.8
port [포트 번호]	특정 포트 번호를 사용하는 패킷만 캡처	port 80 (HTTP)
src port [포트 번호]	특정 출발지 포트 번호를 사용하는 패킷만 캡처	src port 22 (SSH)
dst port [포트 번호]	특정 목적지 포트 번호를 사용하는 패킷만 캡처	dst port 443 (HTTPS)
tcp	TCP 프로토콜만 캡처	tcp
udp	UDP 프로토콜만 캡처	udp
icmp	ICMP 프로토콜만 캡처	icmp
http	HTTP 프로토콜만 캡처 (실제로는 tcp port 80 권장)	tcp port 80
not [필터]	해당 필터에 해당하지 않는 패킷 캡처	not arp (ARP 제외)
[필터1] and [필터2]	두 가지 조건을 모두 만족하는 패킷 캡처	host 192.168.1.1 and port 23
[필터1] or [필터2]	두 가지 조건 중 하나라도 만족하는 패킷 캡처	port 80 or port 443

표시 필터 (Display Filters) 예시

필터	설명	예시
ip.addr == [IP 주소]	특정 IP 주소와 관련된 패킷만 표시	ip.addr == 192.168.1.1
ip.src == [IP 주소]	특정 출발지 IP 주소의 패킷만 표시	ip.src == 10.0.0.10
ip.dst == [IP 주소]	특정 목적지 IP 주소의 패킷만 표시	ip.dst == 172.16.0.1
tcp.port == [포트 번호]	특정 TCP 포트를 사용하는 패킷만 표시	tcp.port == 80
udp.port == [포트 번호]	특정 UDP 포트를 사용하는 패킷만 표시	udp.port == 53 (DNS)
http	HTTP 프로토콜만 표시	http
dns	DNS 프로토콜만 표시	dns
arp	ARP 프로토콜만 표시	arp
protocol == [프로토콜 이름]	특정 프로토콜만 표시 (예: tcp, udp, icmp)	protocol == icmp
frame.len > [길이]	특정 길이보다 큰 패킷만 표시	frame.len > 1000
not [필터]	해당 필터에 해당하지 않는 패킷 표시	not arp
[필터1] && [필터2]	두 가지 조건을 모두 만족하는 패킷 표시	ip.src == 192.168.1.1 && tcp.port == 21

자주 사용하는 표시 필터 조합

- 특정 **IP** 주소의 **HTTP** 트래픽만 보고 싶을 때:
  - ip.addr == 192.168.1.100 && http
- **DNS** 쿼리 및 응답만 보고 싶을 때:
  - dns
- 특정 포트를 사용하는 **TCP** 연결 오류를 찾을 때:
  - tcp.port == 80 && tcp.flags.reset == 1 (TCP Reset 패킷 찾기)
- 네트워크 대역폭을 많이 사용하는 패킷을 찾을 때:
- frame.len > 1500 (큰 크기의 패킷 위주로 필터링)

실습 1

- 내 컴퓨터에서 특정 웹사이트 접속 패킷 캡처 및 필터링
  - Wireshark를 실행하고 인터넷에 연결된 인터페이스를 선택합니다.
  - **캡처 시작** 버튼을 클릭합니다.
  - 웹 브라우저를 열고 www.google.com에 접속합니다.
  - Wireshark에서 **캡처 중지** 버튼을 클릭합니다.
  - 표시 필터 입력창에 http.host == "www.google.com"을 입력하고 Enter를 누릅니다.
  - 구글 웹사이트와 관련된 HTTP 트래픽만 표시되는 것을 확인합니다.

실습 2

- **Ping 명령어 패킷 분석**
  - 명령 프롬프트(CMD) 또는 터미널을 엽니다.
  - Wireshark에서 캡처를 시작합니다.
  - 명령 프롬프트에서 **ping 8.8.8.8** (구글 DNS 서버)을 입력하고 **Enter**를 누릅니다.
  - Wireshark에서 캡처를 중지합니다.
  - 표시 필터 입력창에 **icmp**를 입력하고 **Enter**를 누릅니다.
- Echo (ping) request와 Echo (ping) reply 패킷들이 표시되는 것을 확인하고, 각 패킷을 클릭하여 상세 정보를 살펴봅니다.

저장 및 내보내기

- .pcapng 포맷으로 저장
- 필터 후 지정 패킷만 내보내기 가능

보안 및 윤리

- 본인 네트워크에서만 캡처
- 무단 캡처는 법적 책임 유의