Wireshark 설치 및 기본 사용법

2020년 7월

경북대학교 사물인터넷표준연구실

김경식 (kyungsik850@gmail.com)

요 약

Wireshark(와이어샤크)는 네트워크 패킷을 캡쳐하고 분석하는 오픈소스 도구이다. 네트워크의 문제, 분석, 소프트웨어 및 통신 프로토콜 개발 등에 쓰인다. 네트워크 프로그래밍에서 패킷의 흐름을 파악하기 유용한 프로그램이며 그 사용법에 대해서 알아본다.

목 차

1. 서론

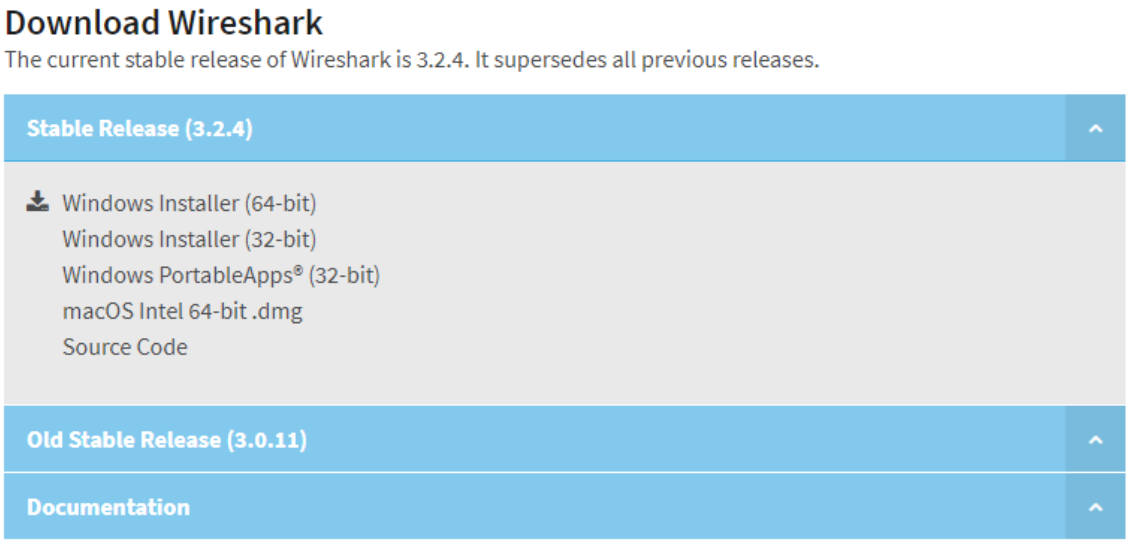
본 고에서는 패킷 분석 도구인 Wireshark의 설치 방법과 간단한 실행 방법을 설명할 것이며, Windows 운영체제 환경에서 구현한다.

2. Wireshark [1]

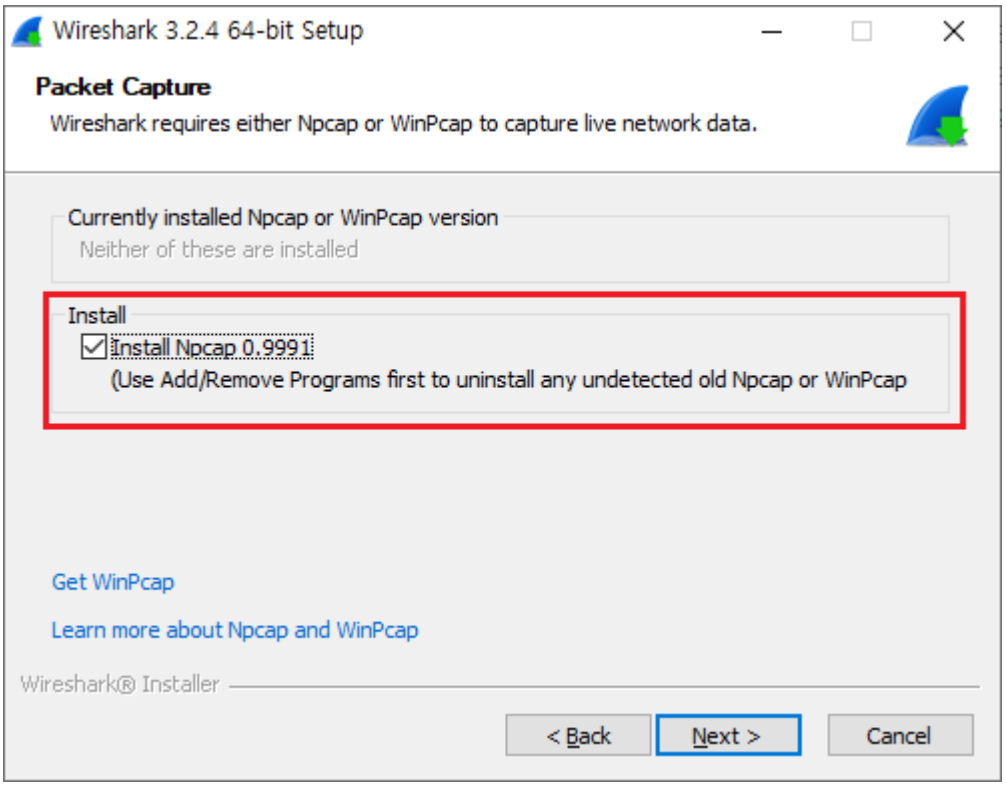
2.1 Wireshark 설치 [2]

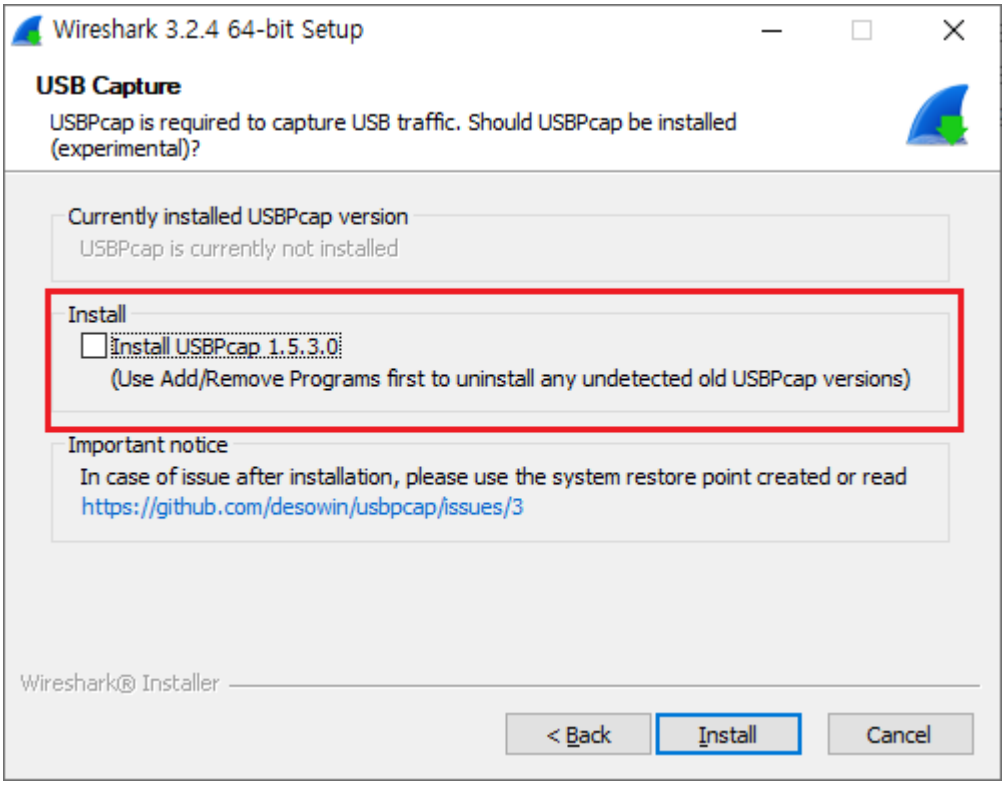
(1) Wireshark 홈페이지에 접속하여 본인 환경에 적합한 파일 다운로드

링크: https://www.wireshark.org/download.html

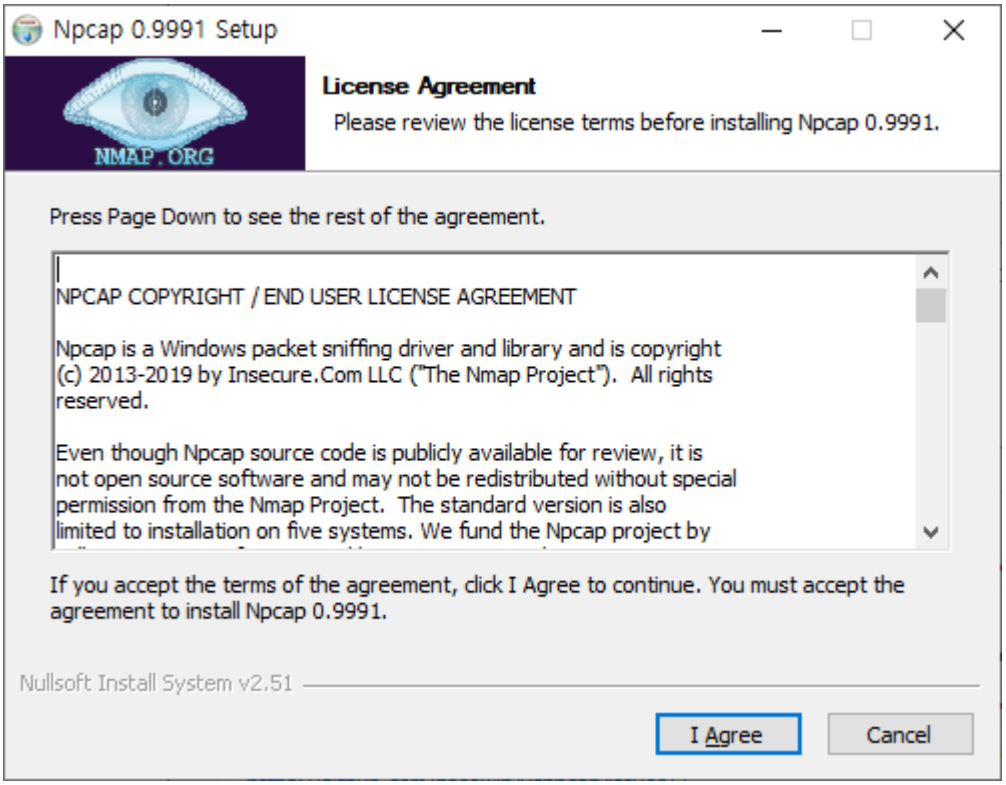


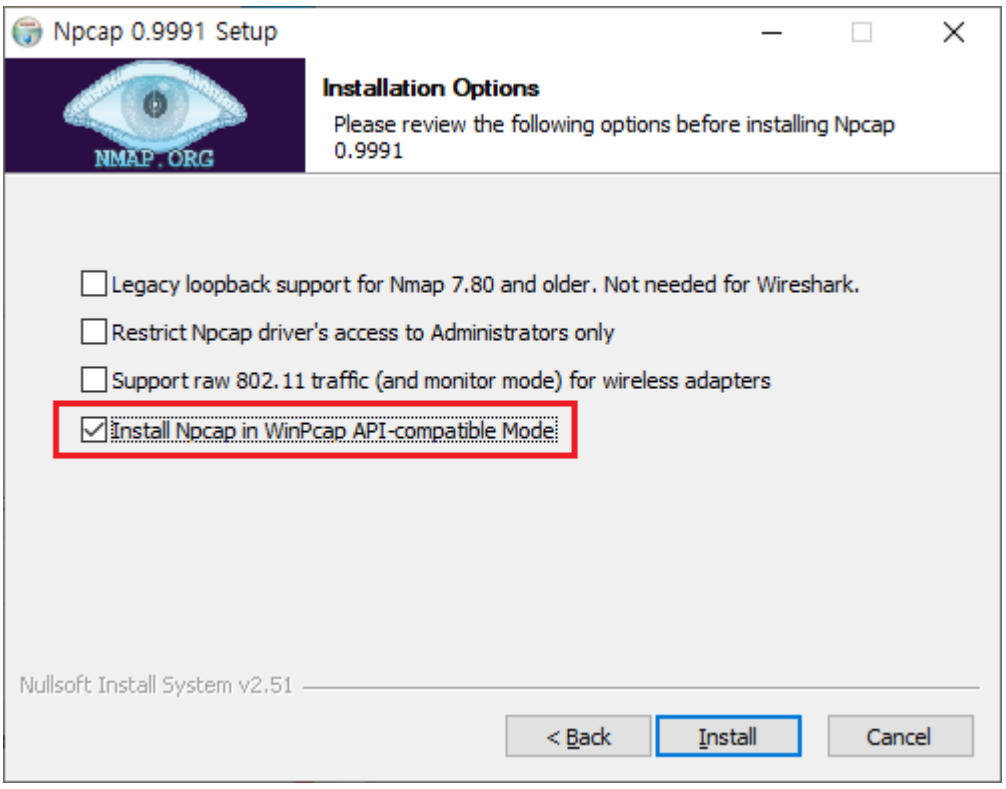
(2) 설치 중 Npcap 체크(필요), USBPcap은 체크 해제(불필요) [3]



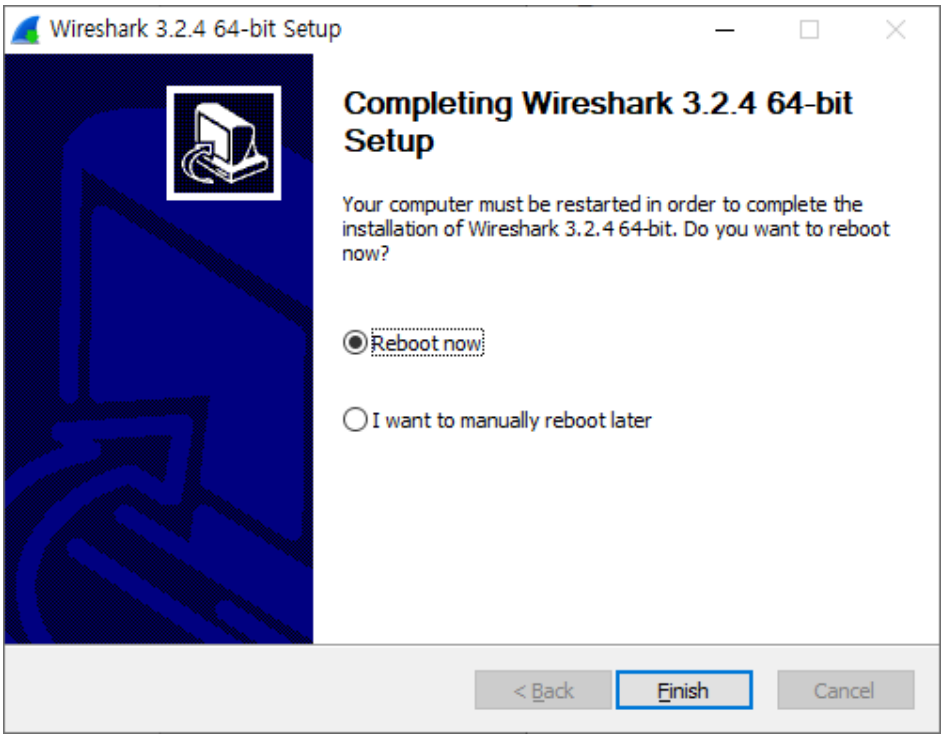


(3) Npcap 설치 시 Install Npcap in WinPcap API-compatible Mode 체크

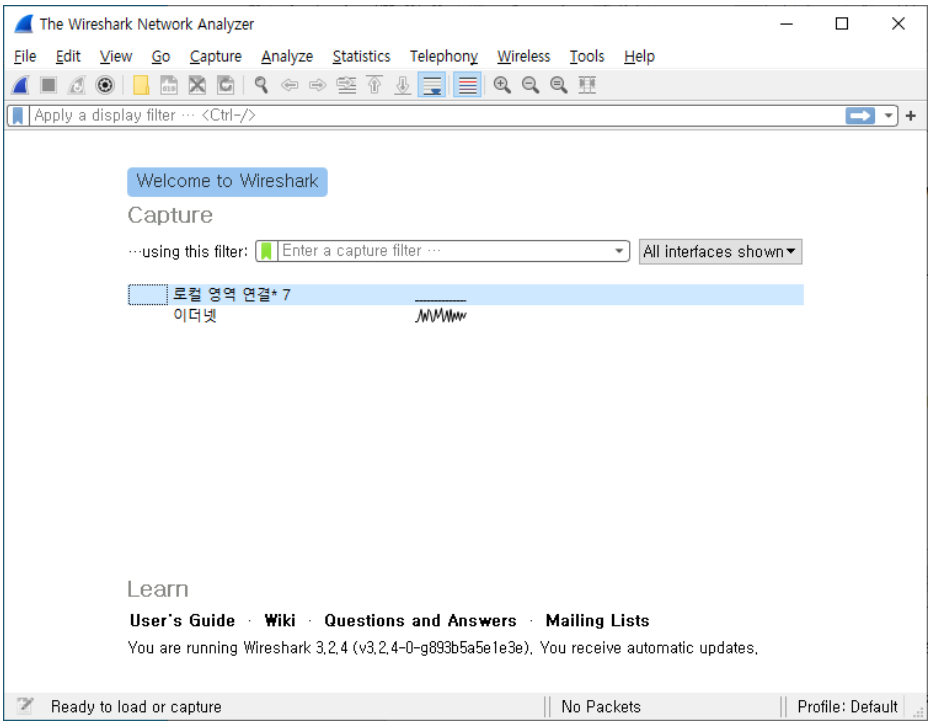




(4) 설치 완료 후 재부팅

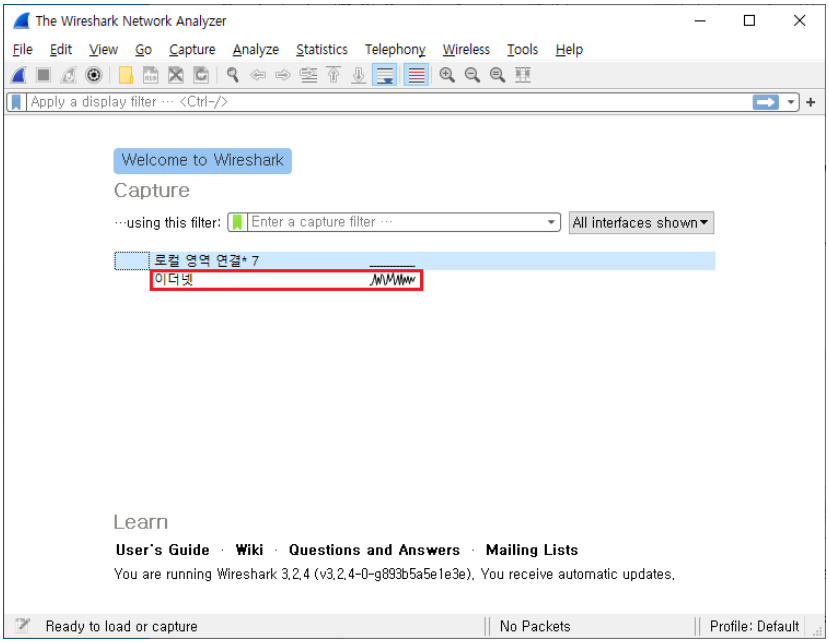


(5) 설치 완료 후 실행

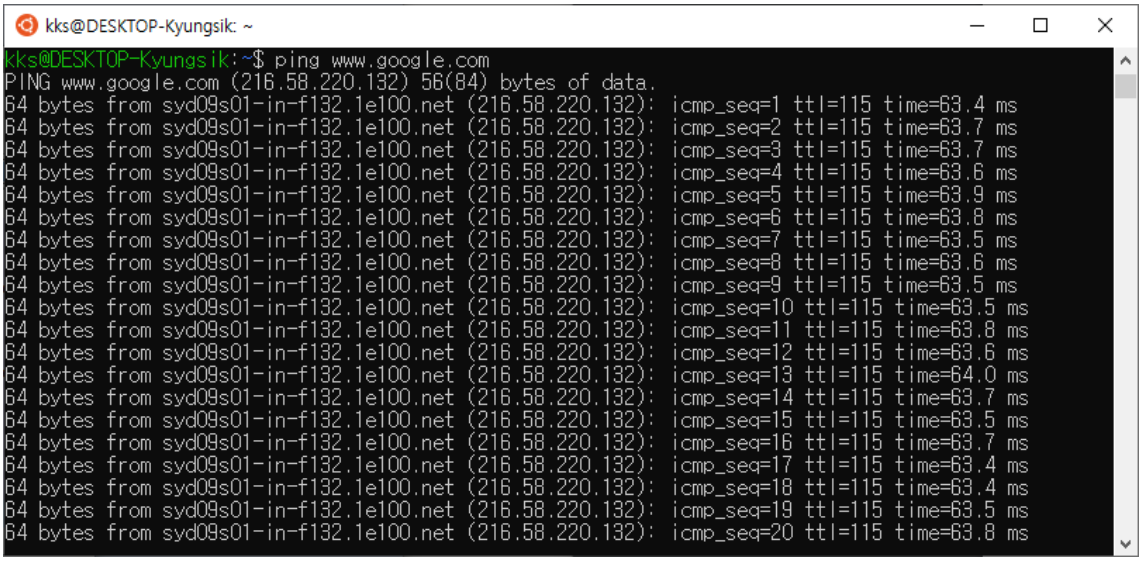


2.2 Wireshark를 사용하여 패킷 분석

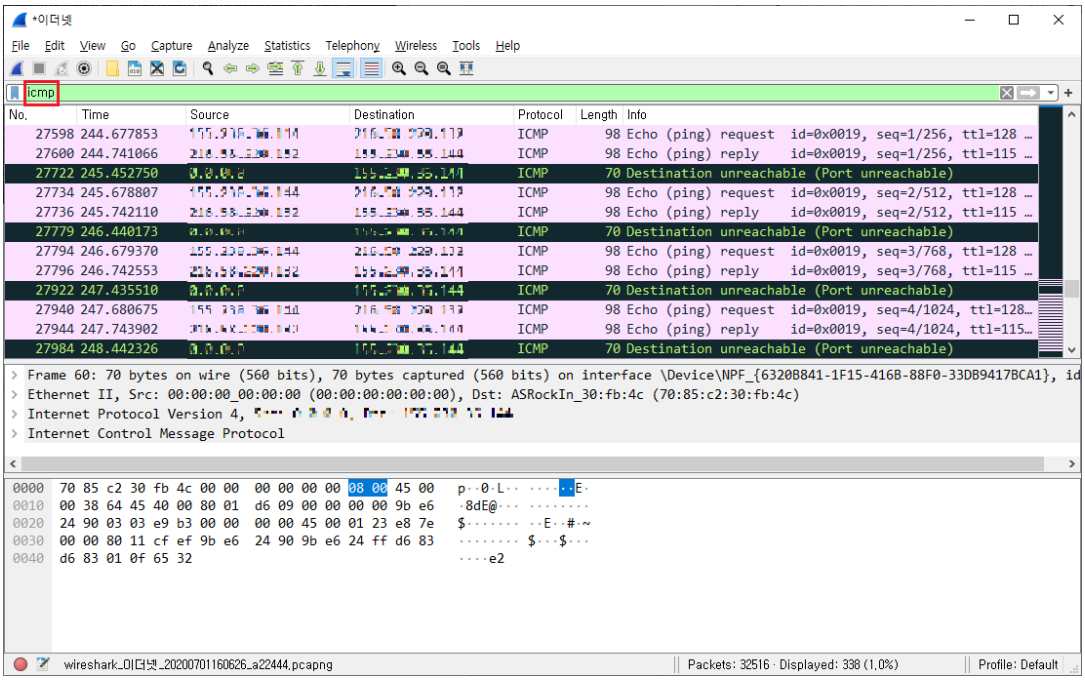
(1) Wireshark 실행 후 이더넷 클릭



(2) Ubuntu에서 “ping www.google.com” 입력



(3) 패킷 처리를 확인하기 위해 필터에 “icmp” 입력 후 패킷 정보 확인[4]



3. 결론

지금까지 본 고에서 Wireshark의 설치 방법과 간단한 사용 방법에 대해서 알아보았다. Wireshark는 네트워크 공부에 있어서 중요한 프로그램이기 때문에 사용법을 제대로 익힌다면 많은 도움이 될 것이다.

참고 문헌

[1] Wireshark, https://www.wireshark.org/

[2] Wireshark 설치, https://www.wireshark.org/download.html

[3] 설치 방법, http://blog.naver.com/PostView.nhn?blogId=cds0915&logNo=220591516229

[4] Wireshark 필터, https://byeong9935.tistory.com/100