# What is Wireshark?

와이어샤크는 네트워크 패킷 분석기입니다. 네트워크 패킷 분석기는 네트워크 패킷을 캡처하려고 시도하고 가능하면 자세하게 패킷 데이터를 표시합니다. 와이어 샤크는 무료로 제공되고, 오픈 소스이며, 현재 사용할 수 있는 최고의 패킷 분석기 중 하나입니다.

오픈 소스 소프트웨어 프로젝트이므로 GNU General Public License에 따라 배포됩니다.

와이어샤크는 아래와 같은 특징들을 가집니다.

* UNIX 및 Windows에서 사용 가능합니다.
* 네트워크 인터페이스에서 라이브 패킷 데이터를 캡처합니다.
* Tcpdump/WinDump, Wireshark 및 기타 여러 패킷 캡처 프로그램으로 캡처한 패킷 데이터가 들어있는 파일을 엽니다.
* 매우 상세한 프로토콜 정보로 패킷을 표시합니다.
* 캡처된 패킷 데이터를 저장합니다.
* 일부 또는 모든 패킷을 여러 캡처 파일 형식으로 내보냅니다.
* 많은 기준으로 패킷을 필터링할 수 있습니다.
* 필터를 기반으로 패킷 표시를 색상화합니다.
* 와이어샤크는 침입 탐지 시스템이 아니므로 누군가가 네트워크에서 이상한 일을 할 때 경고하지 않습니다.
* 네트워크상의 모든 것을 조작하지 않으며 단지 측정할 뿐입니다.

주로 서버, 클라이언트 통신을 하는 프로그램을 개발할 때 정보 교환이 제대로 이루어지고 있는지 확인하는 과정에서 많이 사용되는 도구입니다.

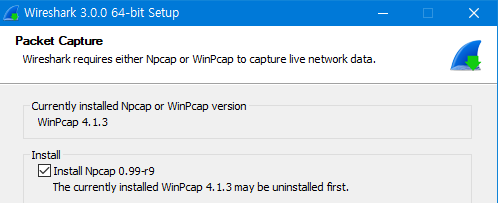
# Library

**pcap**

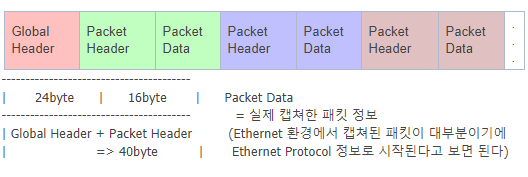
packet capture로 컴퓨터 네트워크 관리 분야에서 네트워크 트래픽 포착용 API를 구성하고 있습니다. Pcap 라이브러리를 사용하면 내 호스트에서 demultiplexing 과정을 거치기 전의 패킷을 열어 분석할 수 있습니다.

유닉스 계열 운영 체제들은 Libpcap, 윈도우 계열 운영 체제들은 Winpcap이 있습니다.

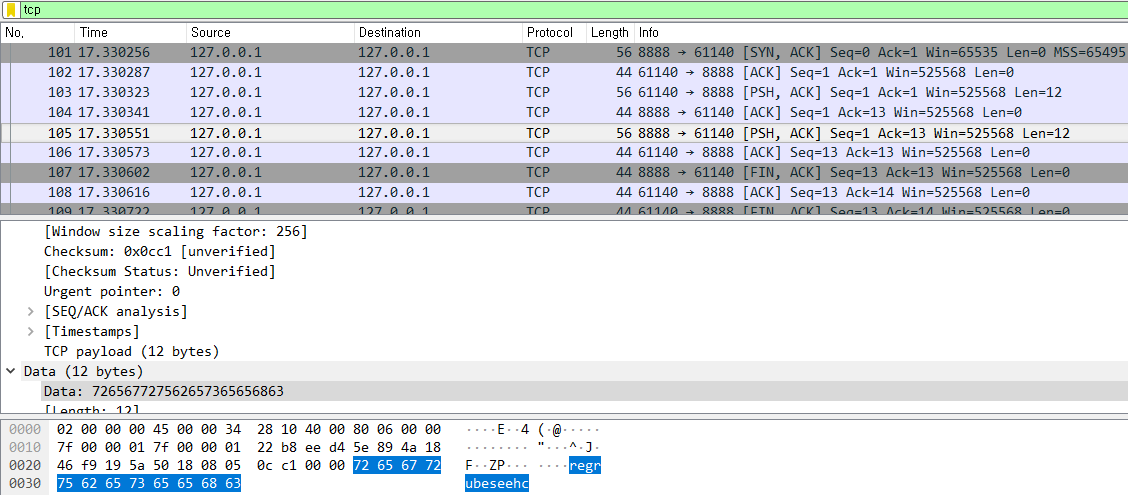
와이어샤크의 경우 기본적으로 Libpcap을 사용하며 설치 과정에서 Winpcap을 선택해 설치할 수 있습니다. 그런데 WinPcap 프로그램은 2013년 3월 8일 업데이트된 WinPcap 4.1.3 버전 이후로 업데이트가 더 이상 제공되지 않고 있어 Wireshark 3.0.0 버전부터는 WinPcap 대신 Npcap 드라이버로 전환하게 됐습니다.



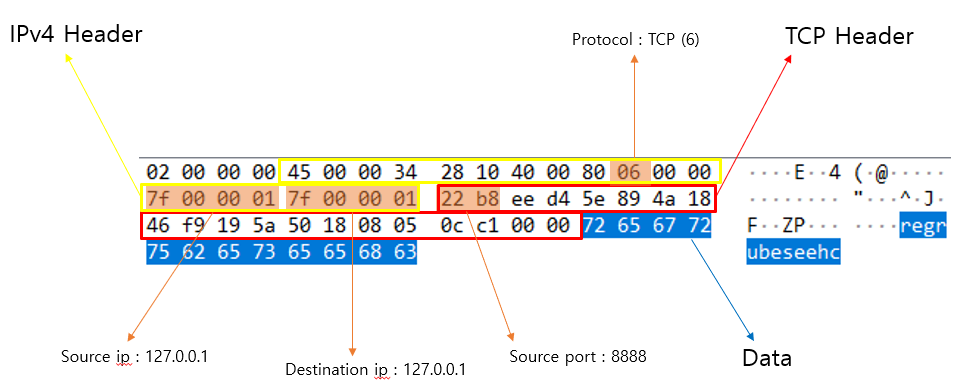
이 라이브러리를 사용해 패킷을 캡처하면 .PCAP라는 하일 포맷으로 저장됩니다. pcap의 파일 포맷은 아래와 같습니다.



# Wireshark TCP packet capture



Npcap Loopback Adapter에서 tcp로 필터링해 캡처한 패킷입니다. 나중에 안 사실인데, 여기서 캡처하는 패킷은 Npcap이 Winsock Kernel 기술을 사용해 루프백 패킷만 캡처한다고 합니다. 즉 로컬 내에서의 패킷을 캡처하는 것 같습니다. 이더넷에서는 루프백으로 보낸 패킷이 잡히지 않았습니다.



메시지는 cheeseburger를 보냈습니다.

앞의 헤더 부분들을 빼면 12바이트의 Data 부분이 나옵니다. 보니까 위에서 찾아본 pcap파일 포맷이랑 좀 달랐습니다. 루프백으로 보낸 패킷이라 그런지 아니면 다른 이유에서 인지는 아직 잘 모르겠습니다.