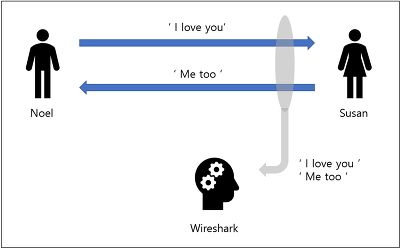
**컴퓨터네트워크 Assignment #7**

* **wireshark 프로그램이란?**

와이어샤크는 네트워크 \*패킷을 캡처하고 분석하는 데 사용되는 공개된 \*패킷 스니핑 프로그램이다. 강력하고 쉬운 사용법으로 해킹, 보안 취약점 분석, 보안 컨설팅, 개인정보 영향평가 등 여러 분야에서 폭 넓게 사용된다.

와이어샤크의 기본 작동 개념은 다음과 같다.



Noel과 Susan이 같은 네트워크 구간에서 메신저 등을 통해 대화를 주고받는 경우 와이어샤크를 사용하여 제3자가 이 둘 사이의 네트워크로 돌아다니는 패킷(네트워크상의 데이터)을 수신하여 \*PCAP(Packet Capture)라는 파일 포맷으로 저장된다. 이때, 와이어샤크는 자체 프로그램으로 네트워크 트래픽을 캡처하는 것이 아닌, 운영체제에서 지원하는 캡처 라이브러리를 이용하여 수집한다.

\*패킷 : OSI 7계층 중에서 네트워크 계층의 기본전송 단위

\*패킷 스니핑(=프로토콜 분석, 패킷 분석) : 네트워크상에서 발생하는 일을 잘 이해하기 위해 네트워크를 통해 전달되는 실제 데이터를 수집하고 해석하는 과정. 3가지 단계로 나뉜다.

- 수집 : 패킷을 수집하기 위해 선택된 네트워크 인터페이스를 무차별 모드로 변경 후 회선에서 원본 바이너리 데이터를 수집한다.

- 변환 : 수집된 바이너리 데이터를 읽을 수 있는 형태로 변환시킨다.

- 분석 : 스니퍼 프로그램 내부에 존재하는 정보를 이용해 수집된 네트워크 데이터의 프로토콜을 검증하고, 프로토콜의 특징과 내용을 분석한다.

\*PCAP : 네트워크 트래픽을 캡처하는 API 구성을 말한다.

* **wireshark는 어떠한 라이브러리를 사용하는가?(Linux, Windows)**

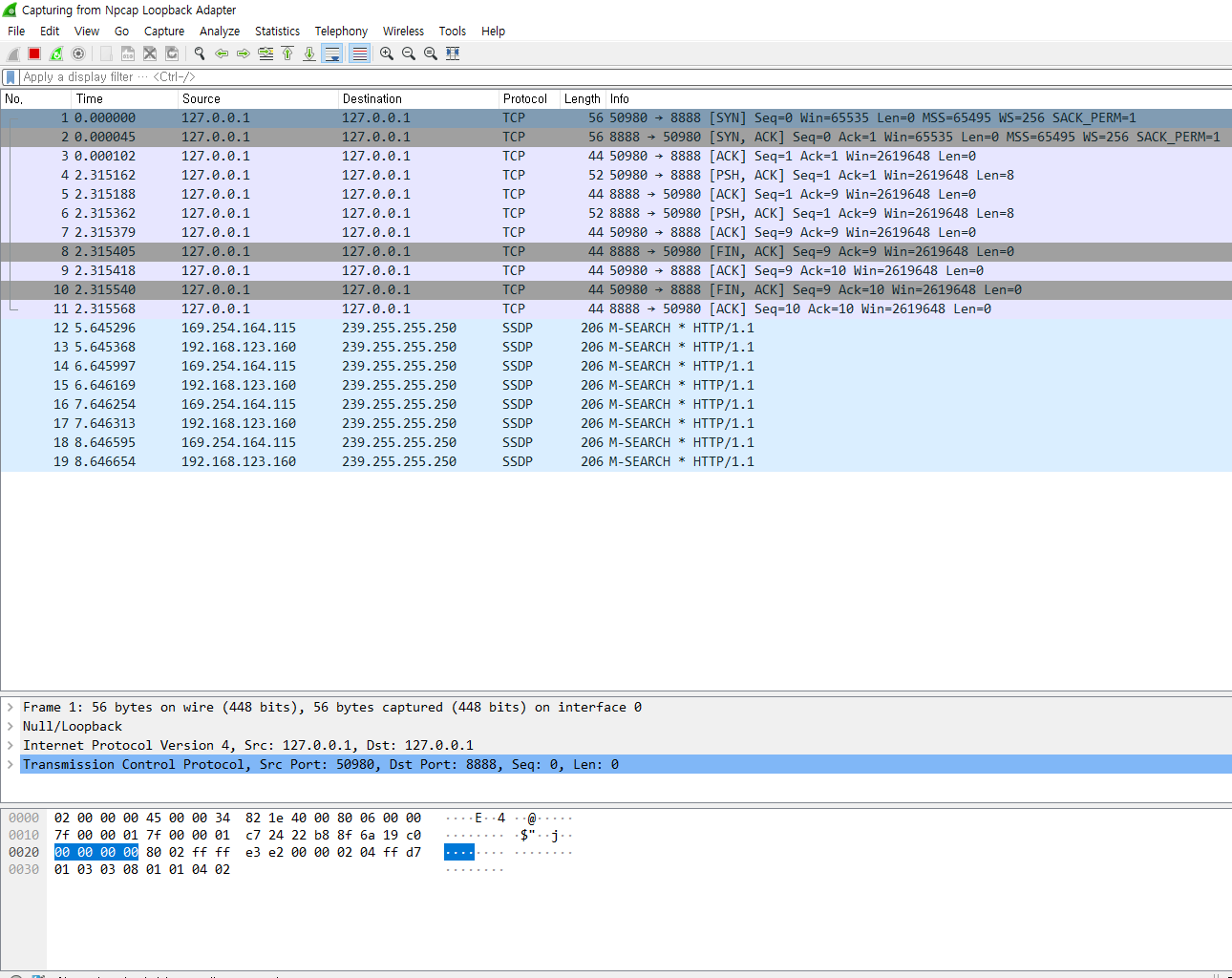
Linux -> LibPcap

LibPcap(Portable Packet Capturing Library) : LAN상의 패킷을 시스템과 독립적인 사용자 레벨에서 캡쳐하는 라이브러리로 BSD 기반의 패킷 캡쳐 구조를 가진다. Promiscuous 모드로 동작하고, 이더넷과 PPP 등 다양한 네트워크 모드에서 사용 가능하며 개발자 API도 제공한다.

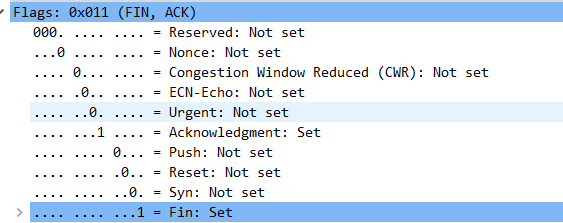
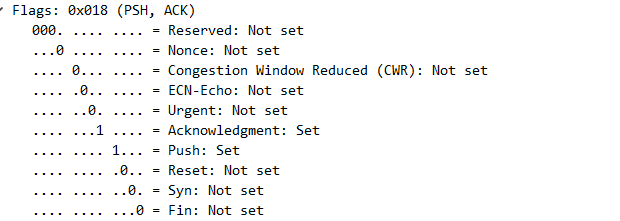
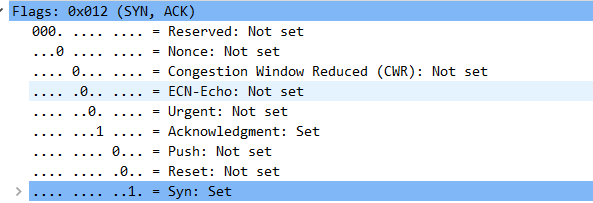
Windows -> WinPcap

WinPcap(Packet Capture Architecture for Windows: 윈도우용 패킷 캡쳐 아키텍쳐) : 패킷 캡쳐 라이브러리를 기반으로 한 자유 및 오픈 소스 패킷 분석 프로그램으로, NIC(Network Interface Card)를 통해 송/수신되는 패킷을 분석하는데 유용한 프로그램. LibPcape의 Win32 포트이며 크게 두가지 요소로 구성되어 있다.

* 대부분의 유닉스 커널에서 제공하는 BPF 기능에 기반한 커널 수준 패킷 필터 드라이브
* 윈도우용 고수준 프로그래밍 라이브러리
* **wireshark로 Assignment #2(문자열 거꾸로 전송)가 실행되면서 서버-클라이언트간 주고받은 TCP 패킷을 캡쳐해서 사진 첨부**

****

위에 사진을 보면 초반에 클라이언트와 서버는 SYN과 ACK를 이용해 3핸드셰이킹을 통해 서로 간에 연결을 이루고 있다. 이후 PSH를 통해 서로 간에 데이터를 보내고 난 뒤 FIN을 통해 서로 간의 연결을 종료하고 있다. 용어를 설명하자면 다음과 같다.

* SYN : 연결 요청 플래그(초기에 시퀀스 번호를 보내 세션을 연결하는 데 사용된다.)
* ACK : 응답(패킷을 받았다는 것을 알려주는 패킷이다.)
* PSH : 밀어넣기(받은 데이터를 즉시 Application 계층으로 전송하도록 하는 신호이다.)
* FIN : 연결 종료 요청(전송할 데이터가 더 이상 없어 세션 연결을 종료시킨다.)

패킷들을 순서대로 눌러 상태를 살펴보면 SYN, ACK가 선언된 패킷은 Acknowledgment와 Syn부분이 set으로 변해 있는 것을 알 수 있고 다른 경우 또한 선언된 패킷이 활성화 되는 것을 알 수 있다.