Wireshark

데이터 통신 1주차

조교 : 김수현
shkim950921@cs-cnu.org
데이터 네트워크 연구실(633호)

튜터 : 황동준

목표

1. virtualbox, raspberry pi 에서 Linux사용 방법을 안다.
2. Linux에서 Wireshark 설치 및 사용 법을 안다.
3. Wireshark에서 패킷 구조를 파악할 수 있다.

1. Linux 사용하기

1. Why Linux?
   - 터미널로 사용이 용이: 프로그램 설치나 실행시 따로 인터넷을 켜거나 클릭해서 실행시키지 않고도 터미널에서 바로 실행시킬 수 있음
   - 안드로이드등 다양한 기기는 리눅스 기반으로 만들어짐
2. 리눅스 사용방법 2가지(실습동안 리눅스를 사용할 예정, 더 편한 방식선택)
   a. virtual box
   b. raspberry pi

1. Linux 사용하기 - virtualbox

- 운영체제 가상화 툴(vmware와 유사)
- 오픈소스 프로그램
- 윈도우, 리눅스, 맥에서 지원되는 멀티플랫폼 툴
- virtual box 세팅하기 : https://docs.google.com/presentation/d/1edr8ZRSFqyfjoRij-ouiUGG6uDTRjGCAimHSF-Tskqk/edit?usp=sharing

1. Linux 사용하기 - raspberry pi

- 영국 라즈베리 파이 재단에서 만든 Linux 기반 초소형/초저가 PC
- 교육용 프로젝트 일환으로 개발
- 실습에 사용하는 모델은 Raspberry Pi 3 model B
- 참고 사이트 : https://www.raspberrypi.org/
- 라즈베리파이 세팅하기 : https://docs.google.com/presentation/d/1gdJu2hDBFKLUm5qLtlIvmiGHRsrZ_FqJQozomfM4Qco/edit?usp=sharing

2. wireshark 사용하기 - wireshark란

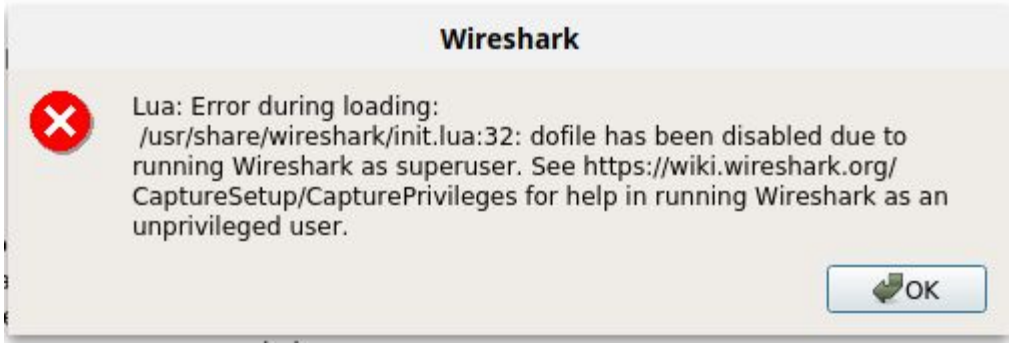
- 널리사용되는 네트워크 분석 프로그램
- Open-Source(GPL v2)
- 멀티 플랫폼(Windows, Linux, Mac, ….) 어떤 os에서도 사용 가능
- 이더넷, 토큰링, ATM등의 네트워크 하드웨어로부터 패킷 캡처가능
- Live Capture및 Offline 분석 가능
- 암호화된 패킷 분석 가능
- 필터링 가능 - 원하는 패킷만 캡처가능

2. wireshark 사용하기 - wireshark install in Linux

- 설치되어 있는경우에는 할필요 없음
- sudo apt-get-repository ppa:wireshark-dev/stable
- sudo apt-get update
- sudo apt-get install wireshark
- 실행 - sudo wireshark

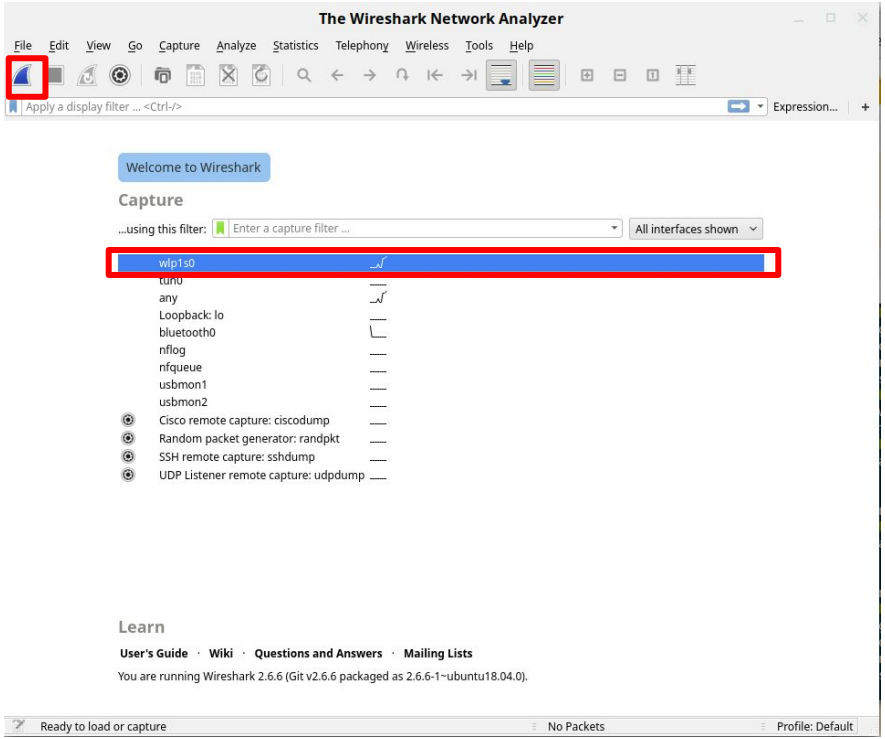
2. wireshark 사용하기 - wireshark install in Linux

- 실행중 다음화면나와도 관계없이 실행됨(root권한으로 실행했기 때문)



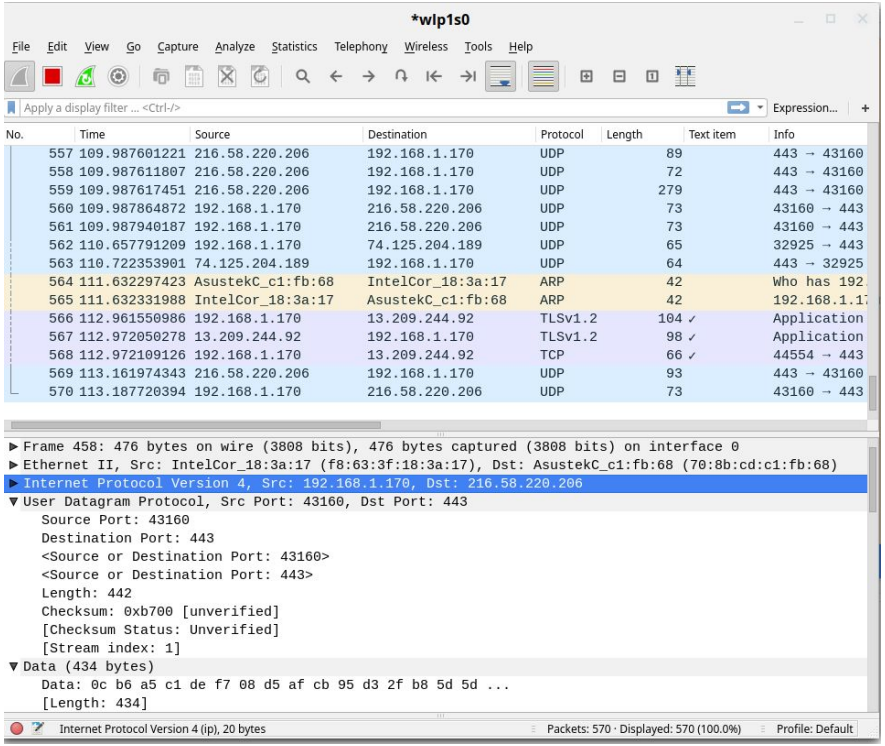
- 다음 에러를 없애고 싶은경우
  - sudo setcap 'CAP_NET_RAW+eip CAP_NET_ADMIN+eip' /usr/bin/dumpcap
  - sudo usermod -aG wireshark $USER
  - 후 컴퓨터 껐다킨 후,
  - 터미널창에 wireshark만 치면됨

2. wireshark사용하기 - wireshark 실행화면



- 상단에 파란색 버튼을 누르거나
- 자신의 네트워크 인터페이스 이름더블 클릭

2. wireshark사용하기 - wireshark 캡처화면

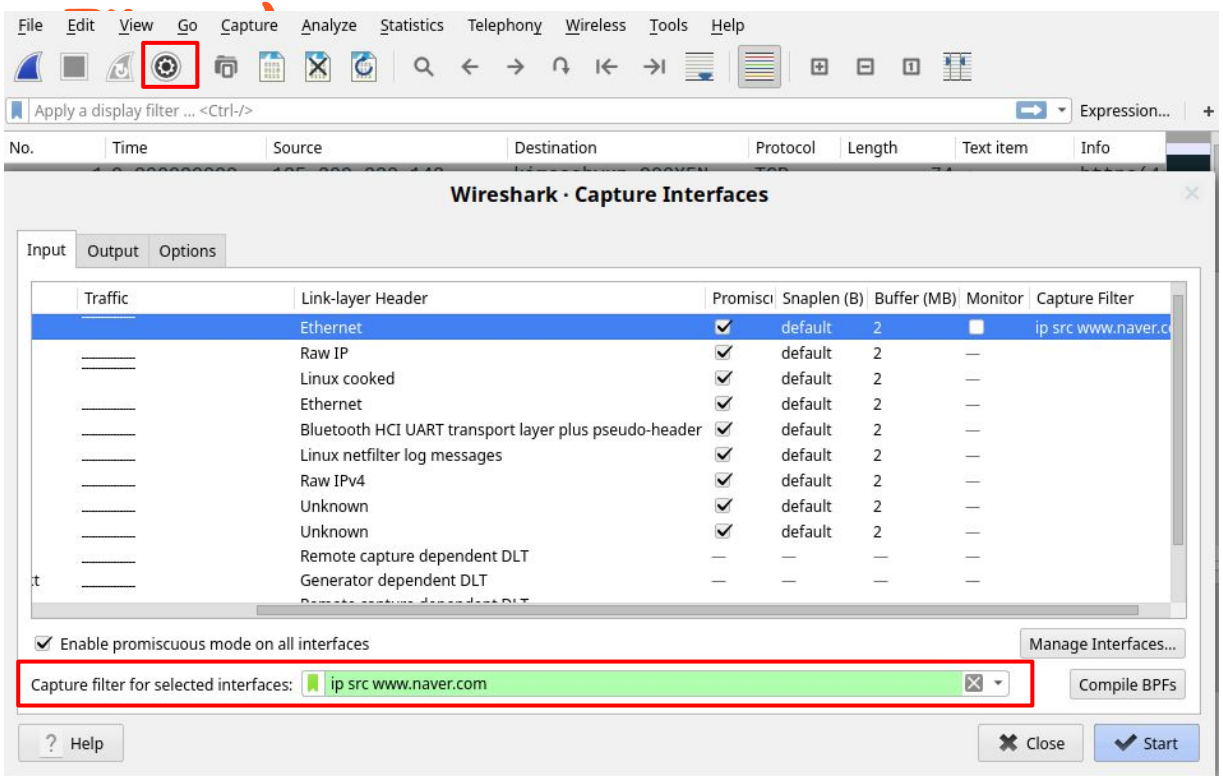


- tool bar
- menubar
- filterbar

- packet list pane

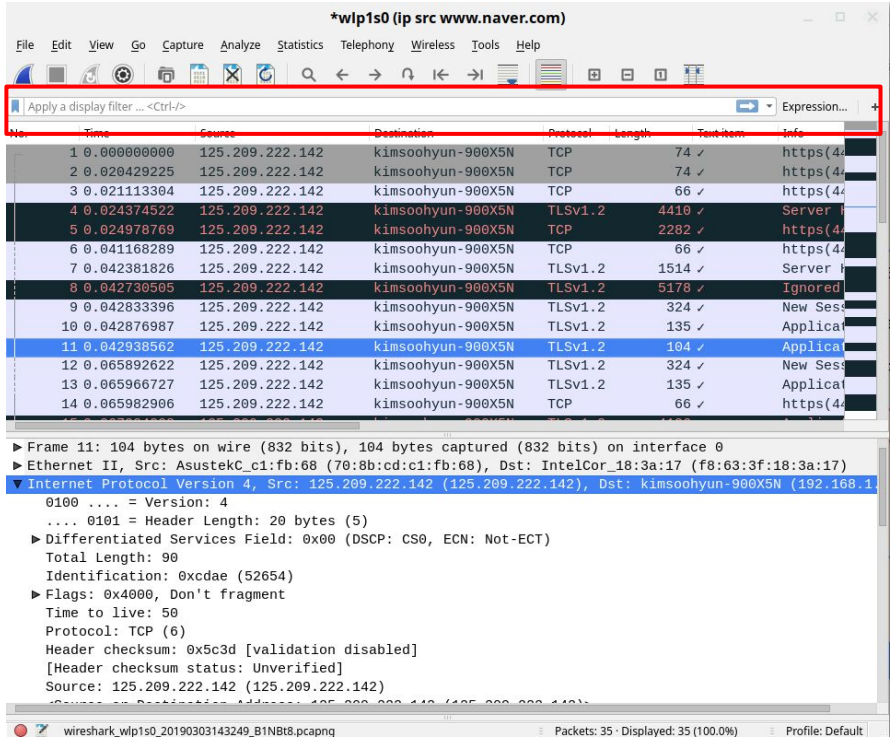
- Packet detail byte

3. wireshark 활용하기 - BPF(Berkeley Packet



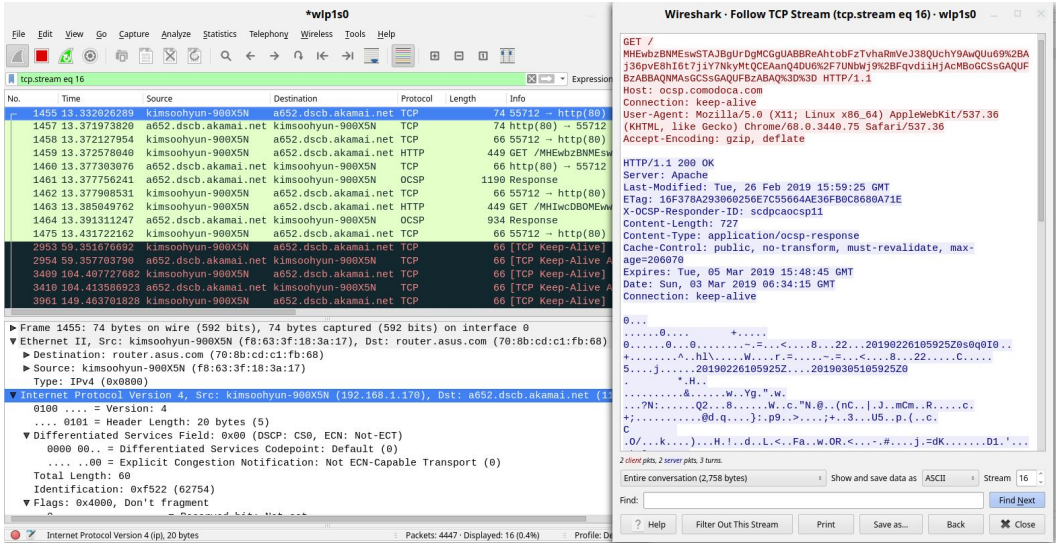
- 처음 패킷을 캡처하면 자신이 인터넷 접속하는 모든것을 캡처함
- 특정 패킷만 보이게 필터링 할 수 있음
- **BPF문법 :** http://biot.com/capstats/bpf.html

3. wireshark 활용하기 - Display Filter



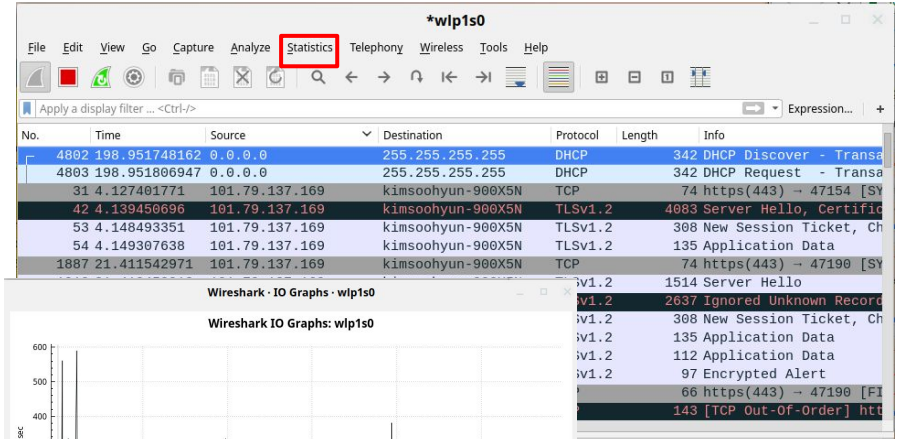
- BPF와는 다름!
  - BPF는 wireshark캡처전에 필터링하는것
- 캡처중인것을 대상으로 필터링함
- Filter bar 이용
- display filter 문법 : http://www.thegeekstuff.com/2012/07/wireshark-filter/

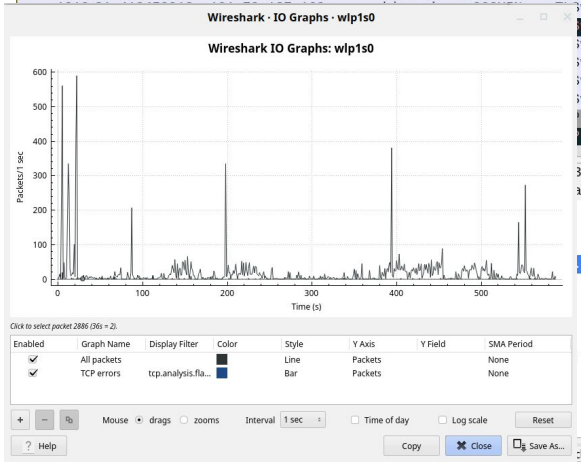
3. wireshark 활용하기 - Follow Stream

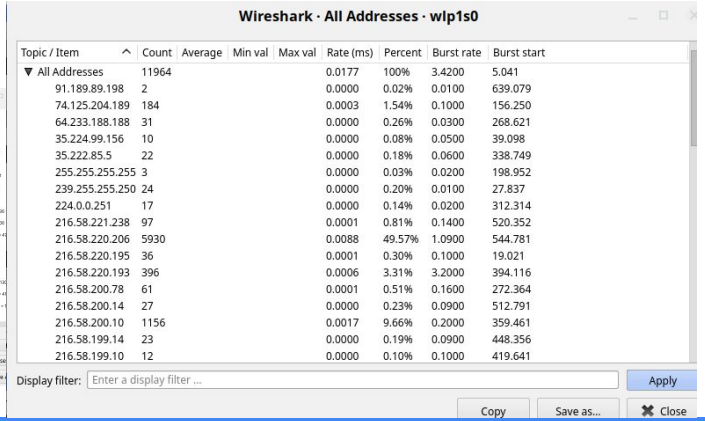


- 두 호스트가 주고받은 패킷을 한번에 모아 확인하고 싶은 경우 사용
- 패킷 선택후 오른쪽 버튼 Follow->(TCP|UDP|HTTP…)Stream
- 혹은 Analyze - Follow - (TCP|UDP|HTTP…)Stream

3. wireshark 활용하기 - statistics



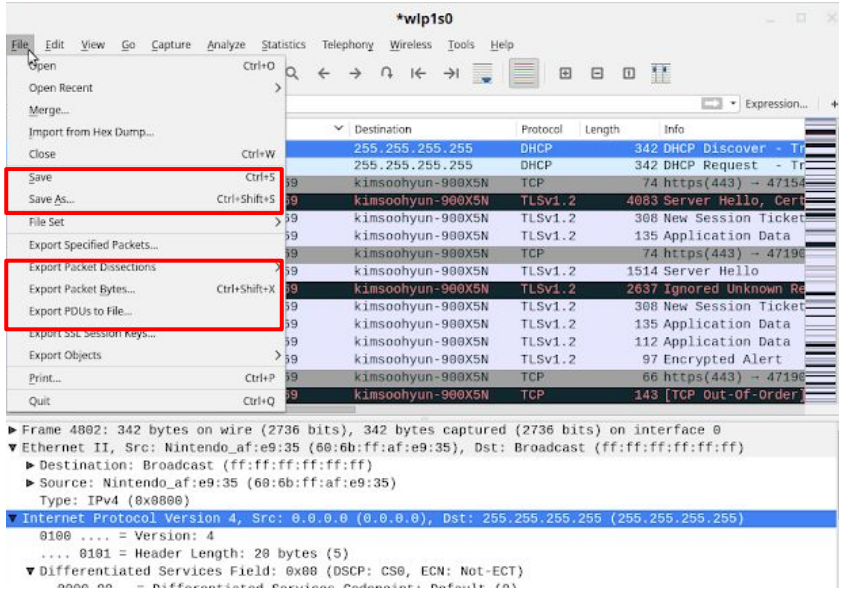


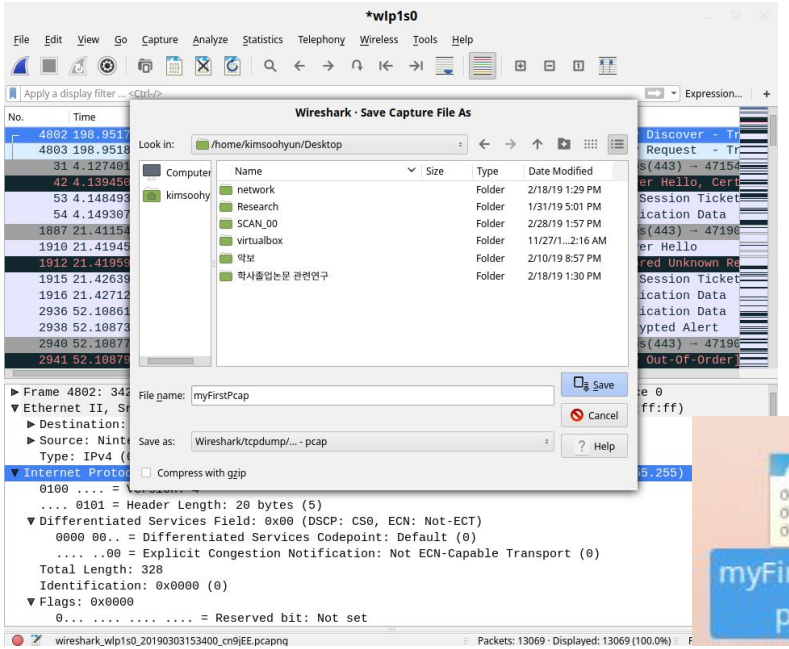


- 패킷의 전체 흐름,
- 패킷 분석할때 많이 쓰이는 목록

- Input/Ouput그래프, 포트별 flowGraph, 연결에서 각 프로토콜 통계등 다양하게 확인 가능

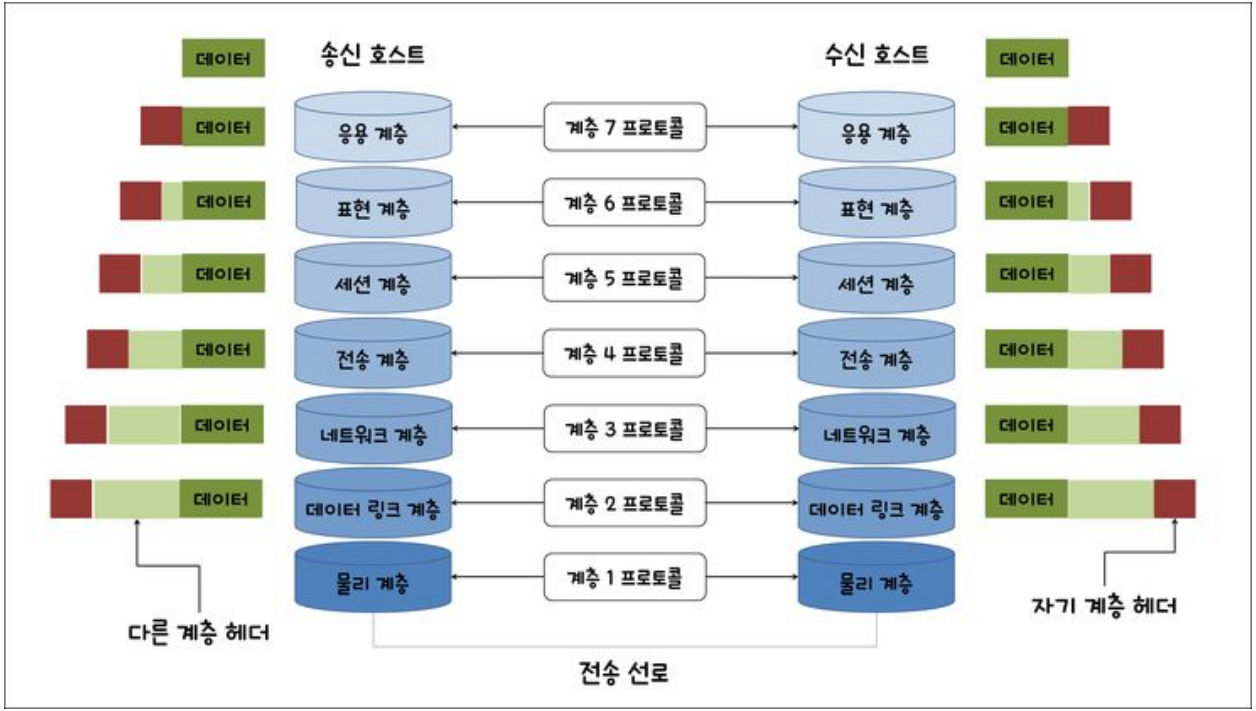
3. wireshark 활용하기 - 패킷저장





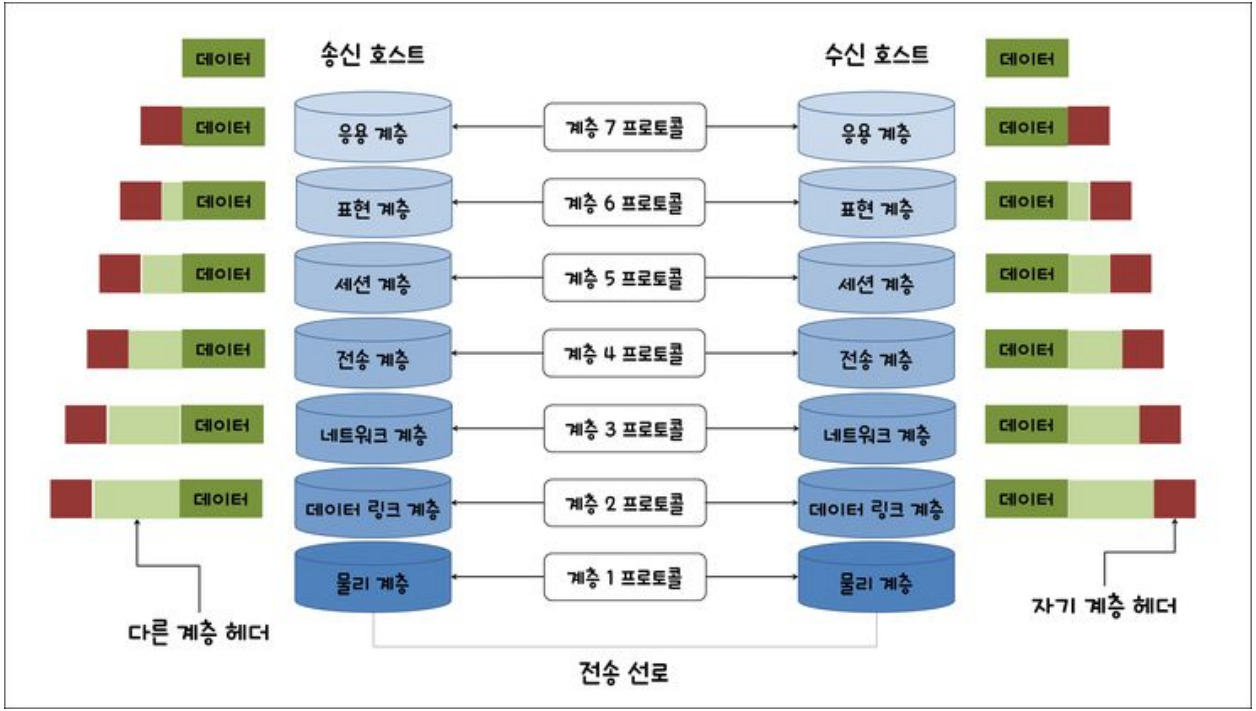
- 캡처중인것을 중지하고 저장
- save : .pcap형태로 저장
- export:CSV,CArraays Plain Text다양한 형태로 저장

2. OSI 7계층



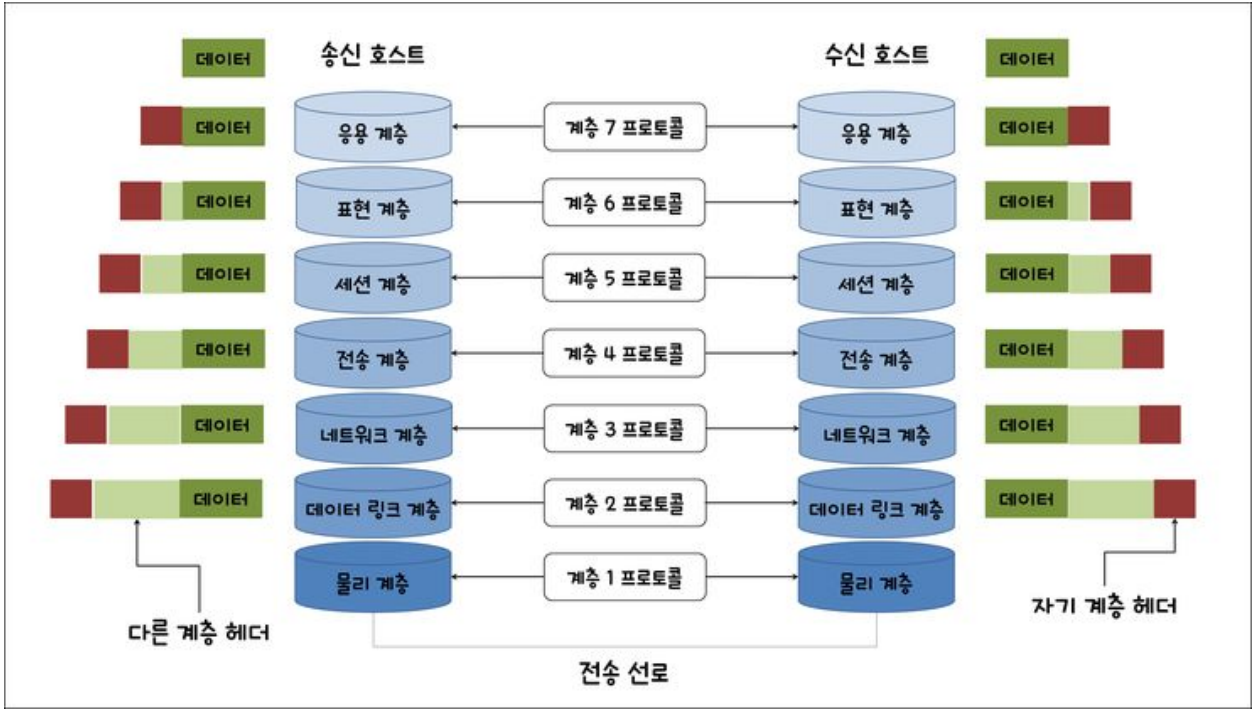
- 네트워크에서 통신이 일어나는 과정을 7단계로 나눈것
- 통신이 일어나는 과정을 단계별로 파악가능
- 송신시 위계층에서 헤더를 붙여 아래계층으로 내려오고, 수신시 헤더를 떼어 위의 계층으로 올라간다.
- 각 계층의 헤더에는 각계층에서 필요한 정보들이 들어가 있음

2. OSI 7계층



- 네트워크에서 통신이 일어나는 과정을 7단계로 나눈것
- 통신이 일어나는 과정을 단계별로 파악가능
- 송신시 위계층에서 헤더를 붙여 아래계층으로 내려오고, 수신시 헤더를 떼어 위의 계층으로 올라간다.
- 각 계층의 헤더에는 각계층에서 필요한 정보들이 들어가 있음

2. OSI 7계층



- 네트워크에서 통신이 일어나는 과정을 7단계로 나눈것
- 통신이 일어나는 과정을 단계별로 파악가능
- 송신시 위계층에서 헤더를 붙여 아래계층으로 내려오고, 수신시 헤더를 떼어 위의 계층으로 올라간다.
- 각 계층의 헤더에는 각계층에서 필요한 정보들이 들어가 있음

Homework

- 다음 사이트에서 웹사이트 5개를 선택하여 아래의 질문에 대한 답을 보고서로 작성하여 .pcap파일과 함께 제출
- 질문의 대답에대한 wireshark 캡처 사진 및 질문의 대답에 대한 이유 서술 필수

- https://www.alexa.com/topsites/countries/KR

- 각 사이트별로 하나의 패킷을 선정한 후 질문에 대답

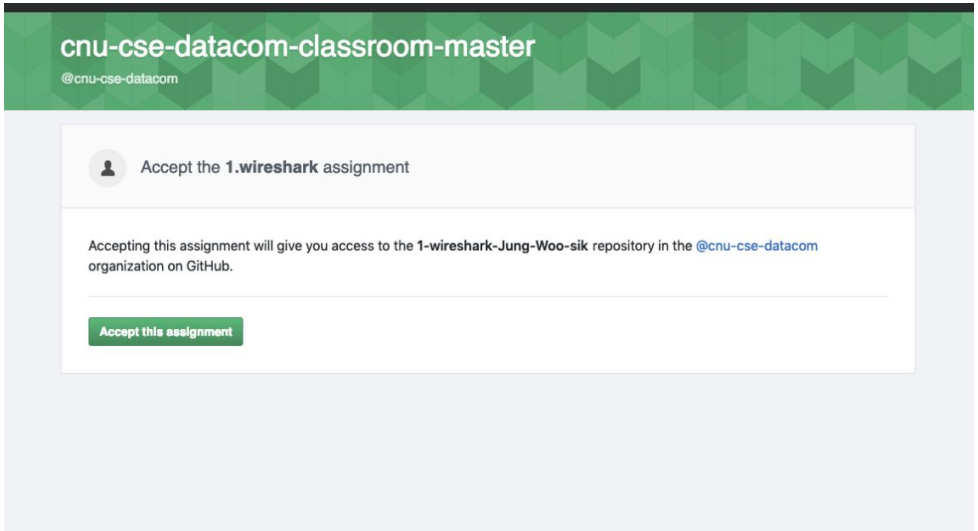
- 제출일 : 3월11일
- Github Classroom URL : https://classroom.github.com/a/jYwu1R6o

Homework -Questions

- Is the frame an outgoing or an incoming frame?
- What is the source IP address of the network-layer header in the frame?
- What is the destination IP address of the network-layer header in the frame?
- What is the total number of bytes in the whole frame?
- What is the number of bytes in the Ethernet (data-link layer) header?
- What is the number of bytes in the IP header?
- What is the number of bytes in the TCP header?
- What is the total bytes in the message (at the application layer)?

과제 제출 방법-1

- Github Classroom URL : https://classroom.github.com/a/jYwu1R6o
- 다음URL



유의사항

- Github Classroom에 제출, 제출기한 반드시 확인할것
- 파일명 : **DC02_01(과제번호)_학번_이름.zip**
  - **.pcap파일**과 **보고서**를 함께 압축하여 제출
  - ex)DC02_01_20170000_김수현.zip
  - 형식 지켜지지 않을시 채점안함
  - 보고서:PDF로 작성할것(HWP, DOC은 채점안함)
    - 과제 목표(도출해야할 결과)
    - 질문에 대한 답변 (사진 및 대답에 대한 이유 서술)
    - 과제후기(느낀점 및 조교에게 하고싶은말, 선택사항)

유의사항(Cont'd)

- 실습조교:김수현
- 메일:shkim950921@cs-cnu.org
- 연구실 633호(데이터 네트워크 연구실)
  - 방문전 사전 메일 필수
  - 가능하면 18시 이후 방문 요망, 18시 이전 방문은 못받을 수 있음
- 메일 보낼시 지켜야할 사항
  - 제목 : [데이터통신] 학번_이름
    - 지키지 않을시 질문 메일을 못볼 수 있음
  - OS환경 사전명시(예 - ubuntu 14.04.3 LTS 64bit)