Docker & Packet Capture

컴퓨터네트워크 1주차

공과대학 5호관 633호
데이터 네트워크 연구실

조교 : 황동준

실습

1. 설치 및 환경 설정
2. Wireshark에서 http.server를 통해 HTTP Protocol의 packet capture
3. Docker 사용법 정리

과제

1. Virtualbox 설치 및 Ubuntu에 Docker 설치 (2점)
2. 질문에 대한 답을 보고서에 작성 (8점)
   - 질문 7개 (1점 or 2점)에 대해 답하기

실습1 : 설치 및 환경 설정

virtualbox, ubuntu 설치

- 운영체제 가상화 툴 (vmware와 유사)
- 윈도우, 리눅스, 맥에서 지원되는 멀티플랫폼 툴

- vitrualbox 및 ubuntu 설치 방법 : https://blog.dalso.org/linux/ubuntu-20-04-lts/8883
  - virtualbox version : 6.1.12
  - ubuntu version : 20.04 LTS
- 설치에 관련한 질문은 받지 않으며, 원활한 실습 진행을 위해 동일한 버전으로 설치를 하시기 바랍니다.

- 텍스트 에디터 설치
  - sudo apt install vim → 설정해둔 비밀번호 입력

wireshark 설치

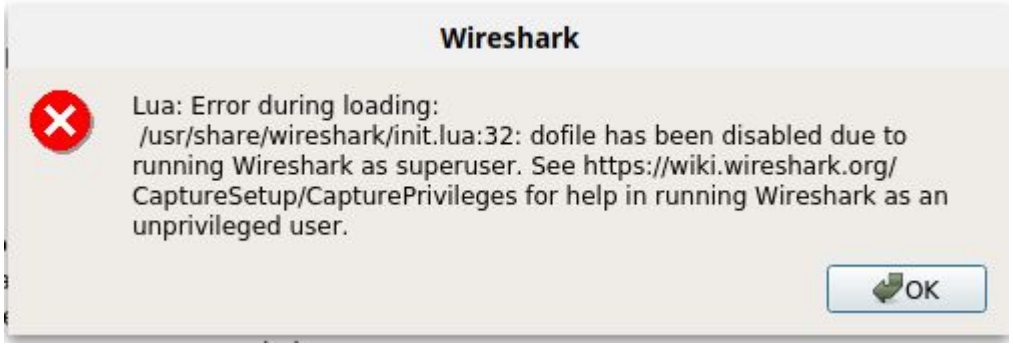
- 설치되어 있는경우에는 할필요 없음
- sudo add-apt-repository ppa:wireshark-dev/stable → [Enter]
- sudo apt update
- sudo apt install wireshark → [무조건 yes]
- 실행 : sudo wireshark

(참고) wireshark 삭제 :

- sudo apt remove --purge wireshark
- sudo apt autoremove

wireshark 설치 오류 해결

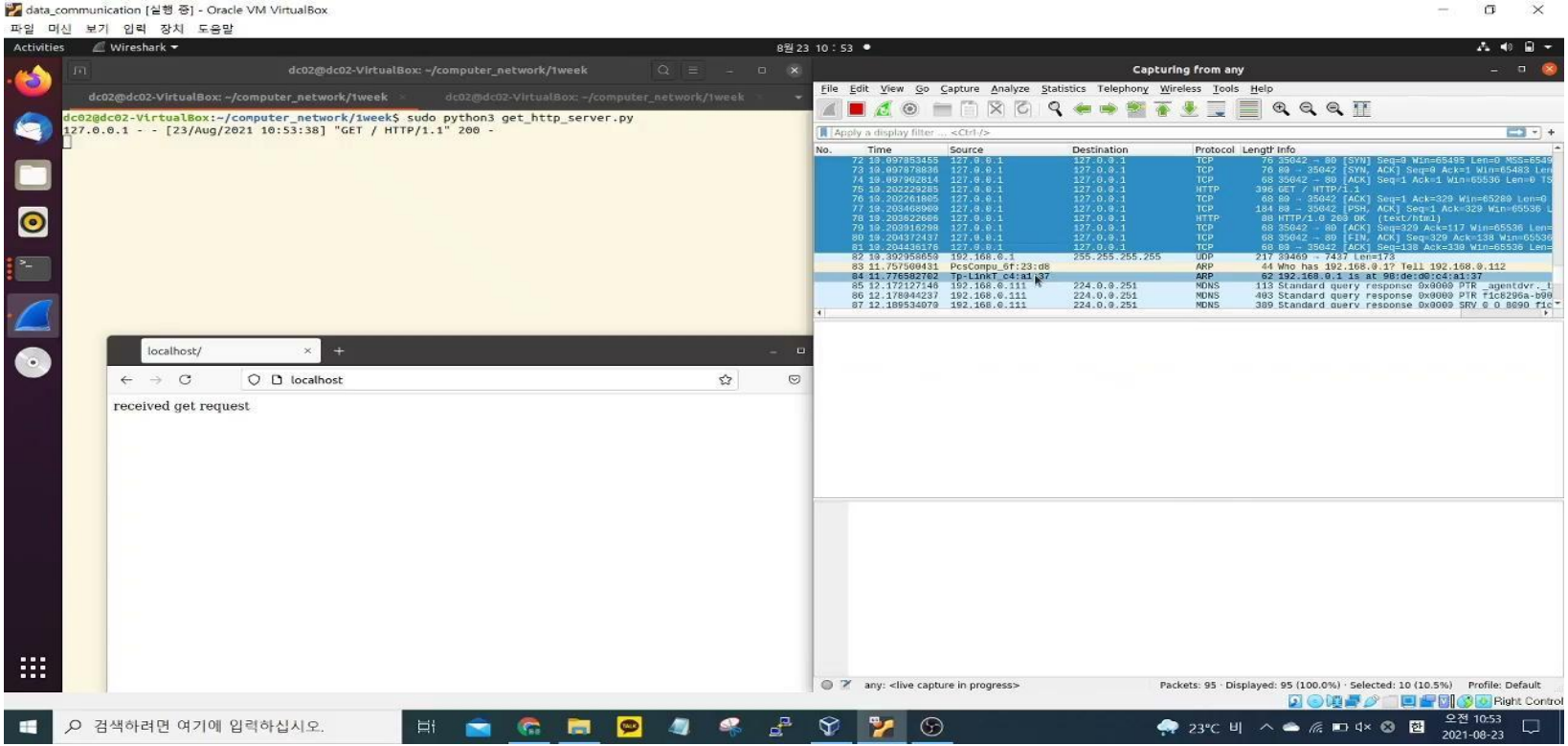
- 실행중 다음화면나와도 관계없이 실행됨(root권한으로 실행했기 때문)



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

https://drive.google.com/file/d/1doFkHSNiqmHvVtOuyPGUpYMlbwP8dfm_/view?usp=sharing

결과 영상



실습2 : Wireshark에서 http.server를 통해 HTTP Protocol의 packet capture

Python의 http.server (GET method)

- HTTP 메소드
  - 클라이언트와 서버 사이에 이루어지는 요청과 응답 데이터를 전송하는 방식

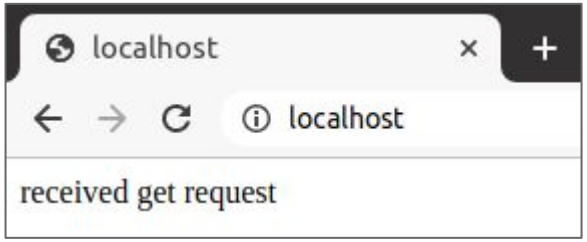
- GET 메소드
  - URI 형식으로 웹 서버측 리소스(데이터)를 요청

  - URI : 통합 자원 식별자
    - 인터넷에 있는 자원을 나타내는 유일한 주소

```python
from http.server import BaseHTTPRequestHandler, HTTPServer

class HandleRequests(BaseHTTPRequestHandler):
    def _set_headers(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/html')
        self.end_headers()

    def do_GET(self):
        self._set_headers()
        self.wfile.write('received get request'.encode('utf-8'))

host = ''
port = 80
HTTPServer((host, port), HandleRequests).serve_forever()
```

결과 화면 - 실행 및 접속

```
datanetwork@datanetwork-VirtualBox:~/ubuntu20/python_practice$ sudo python3 get
_http_server.py
127.0.0.1 - - [28/Aug/2020 13:59:10] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [28/Aug/2020 13:59:10] "GET /favicon.ico HTTP/1.1" 200 -
```

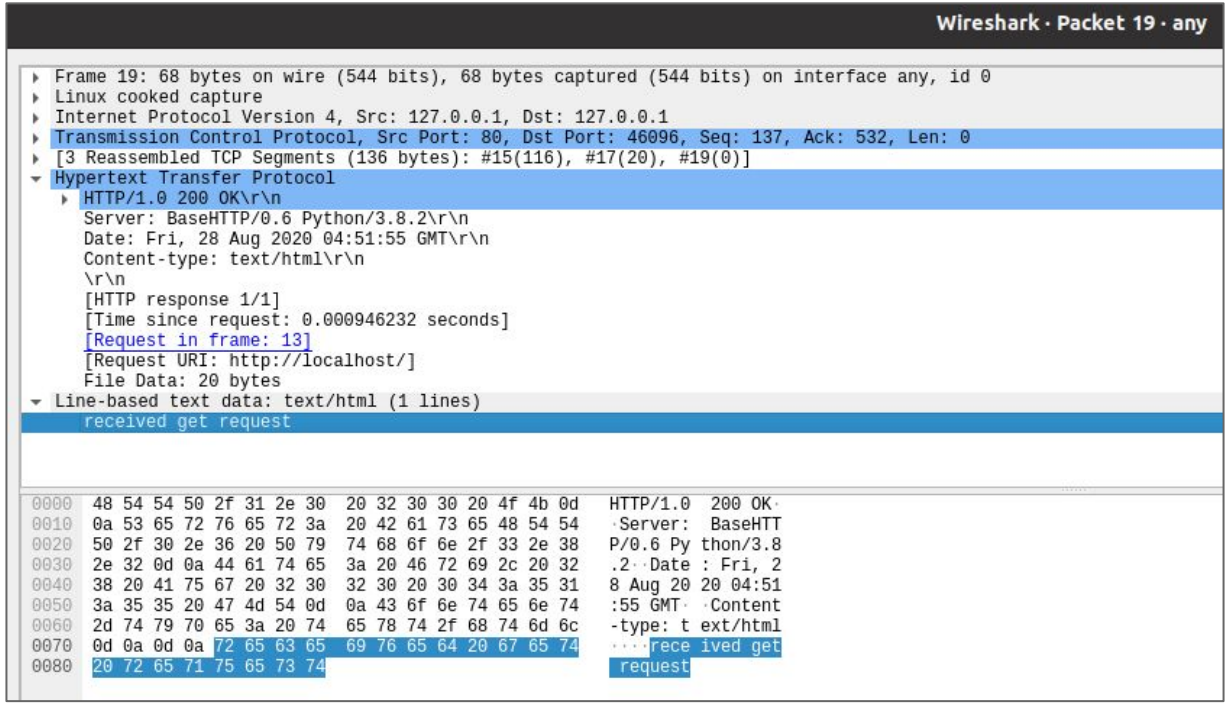


1. python3 [file_name].py 로 파일을 실행 (Permission 오류가 발생하면 sudo를 붙여 실행)
2. Wireshark 실행 ⇒ $ sudo wireshark
3. 파일 실행 후, 브라우저 접속하여 localhost:80 으로 접속하게 되면 오른쪽과 같은 이미지가 보임

결과 화면 - Wireshark

- wireshark에서 IP주소가 127.0.0.1로 되어있는 패킷 중 HTTP Protocol 패킷 확인

- “received get request” 문구를 확인 가능
  - 오른쪽 이미지는 패킷을 더블클릭하여 자세한 정보 확인

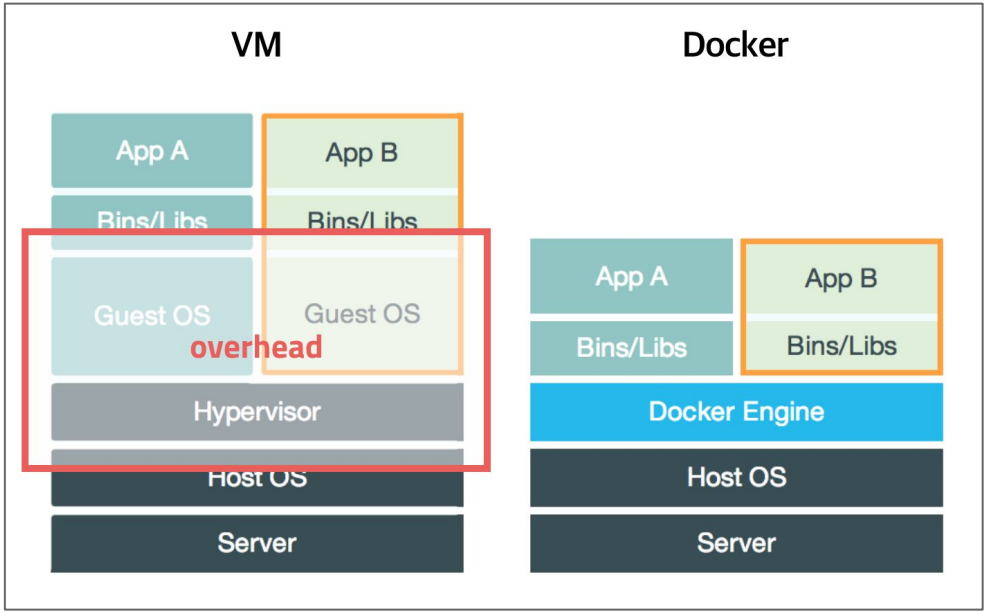


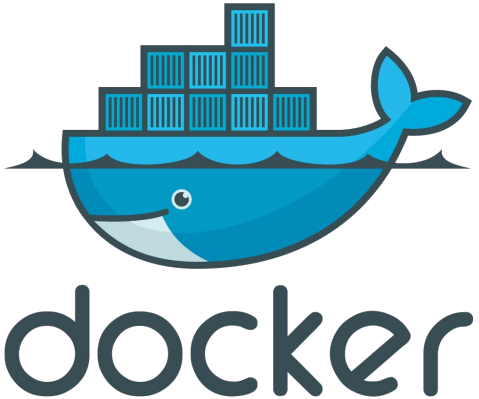
실습3 : Docker 사용법 정리

https://subicura.com/2017/01/19/docker-guide-for-beginners-1.html

Docker

- 컨테이너 기반의 오픈소스 가상화 플랫폼
  - 컨테이너 : 격리된 공간에서 프로세스가 동작하는 기술





https://subicura.com/2017/01/19/docker-guide-for-beginners-2.html

Docker 설치 및 Docker Hub 소개

- Docker의 경우 리눅스 컨테이너 기술로 macOS나 Windows에 직접 설치하거나, 가상머신에 설치하기 바람
- 우리는 이전 슬라이드에서 설치한 ubuntu 20.04LTS에서 Docker를 설치
  - curl -fsSL https://get.docker.com/ | sudo sh
    (Docker 설치 명령어)
- Docker에는 이미 다른 사용자들이 컨테이너를 쌓아 만든 이미지가 모인 Hub이 있음 → Docker Hub이라 부름
  - https://hub.docker.com/

Docker 컨테이너 및 네트워크 명령어

- docker ps -a
- docker images
- docker run -it (-i -t) --name hello ubuntu:latest /bin/bash
  - apt update
  - apt install net-tools
  - apt install iputils-ping
  - apt install traceroute
  - ifconfig

- docker network ls
- docker network inspect [bridge/host]

https://subicura.com/2017/01/19/docker-guide-for-beginners-1.html

https://iamreo.tistory.com/entry/Docker-%EB%AA%85%EB%A0%B9%EC%96%B4-%EC%A0%95%EB%A6%AC

과제 질문

1. Docker Image를 확인하는 명령어는? (1점)
2. Docker Container를 제거하는 명령어는? (1점)
3. Docker Container를 모두 확인하는 명령어는? (start, stop 포함) (1점)
4. Container ID가 ce1e418584c3일때, Container의 log를 보는 명령어는? (1점)
5. Docker Container를 실행하는 명령어는? (옵션 모두 제외, 기본 명령어만) (1점)
    a. 옵션이 들어가있어도 점수에는 영향 주지 않음
6. 5번의 답과 docker run 명령어와의 차이점은? (1점)
7. Docker와 VM의 차이점은? (2점)
    a. 관련 자료 읽어본 후, 이해한 그대로 작성할 것

과제 제출

- 과제 제출 기한
  - 2021년 9월 16일 17:59 까지 사이버 캠퍼스에 제출

- 제출 파일 (.pdf)
  - 보고서
    - 질문에 대한 답

- 딜레이 1일당 20%감점
  - ex) 10점 만점 기준, 1일 딜레이인 경우 8점

- 과제 카피 적발시 보여준사람 본사람 모두 0점처리
  - 카피 적발기준 : 과제 유사도 80%이상

유의사항

- 파일명 : CN02_01_학번_이름.pdf
  - 보고서 제출
  - 보고서 : PDF로 제출할것
    - 과제 목표 (도출해야할 결과)
    - 코드 설명과 과제 해결 방법 (질문에 대한 답)
    - 과제 느낀점 및 하고싶은 말 (선택사항)
  - 형식 지켜지지 않을시 채점대상에서 제외 (보고서도 HWP, DOC은 채점대상에서 제외)

- 질문
  - 질문은 디스코드에서 받음 (과목 공지사항에 공지된 디스코드 링크로 접속)

부 록

Ubuntu란?

1. Why Ubuntu?
    - Linux의 특징을 모두 물려받은 자유 소프트웨어
    - 터미널 사용을 통한 편리성
    - 안드로이드등 다양한 기기는 리눅스 기반으로 만들어짐

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