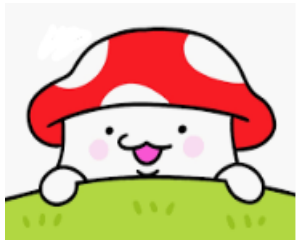


Traffic Monitor

(웹 사이트 어디 방문했니 ?)

정보보안융합S/W

이슬기 정재훈

2020.01.10.

지도 교수 : 이경문 이병천

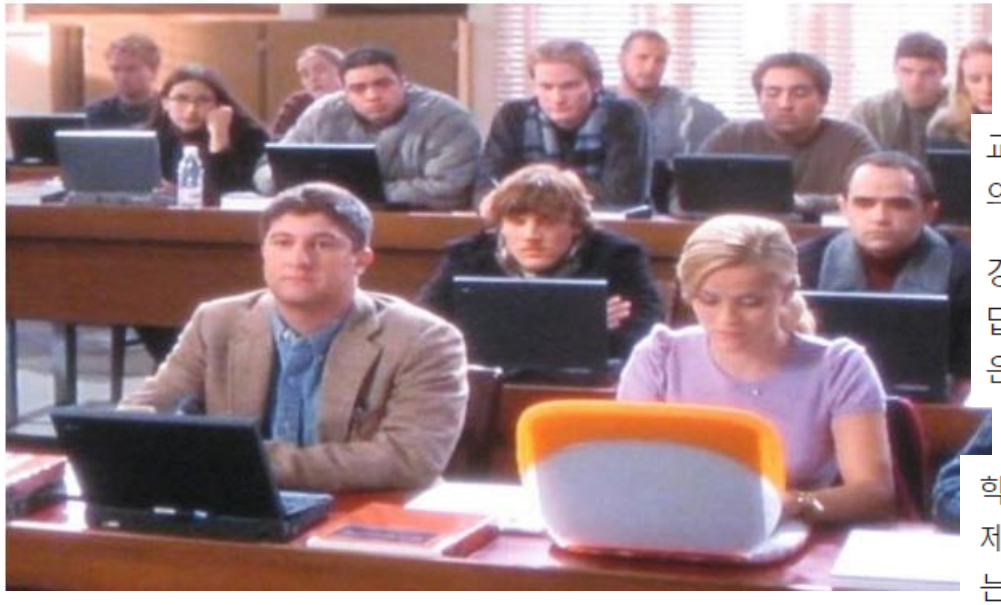
CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

목차

주제선정 이유

주제선정 이유

내 이름은 !
Traffic Monitor



[현장] 대학들, 수업시간 '노트북 사용' 골치 아프다

학교 차원 지침 공론화 시급...미국도 골칫거리로 지침 마련

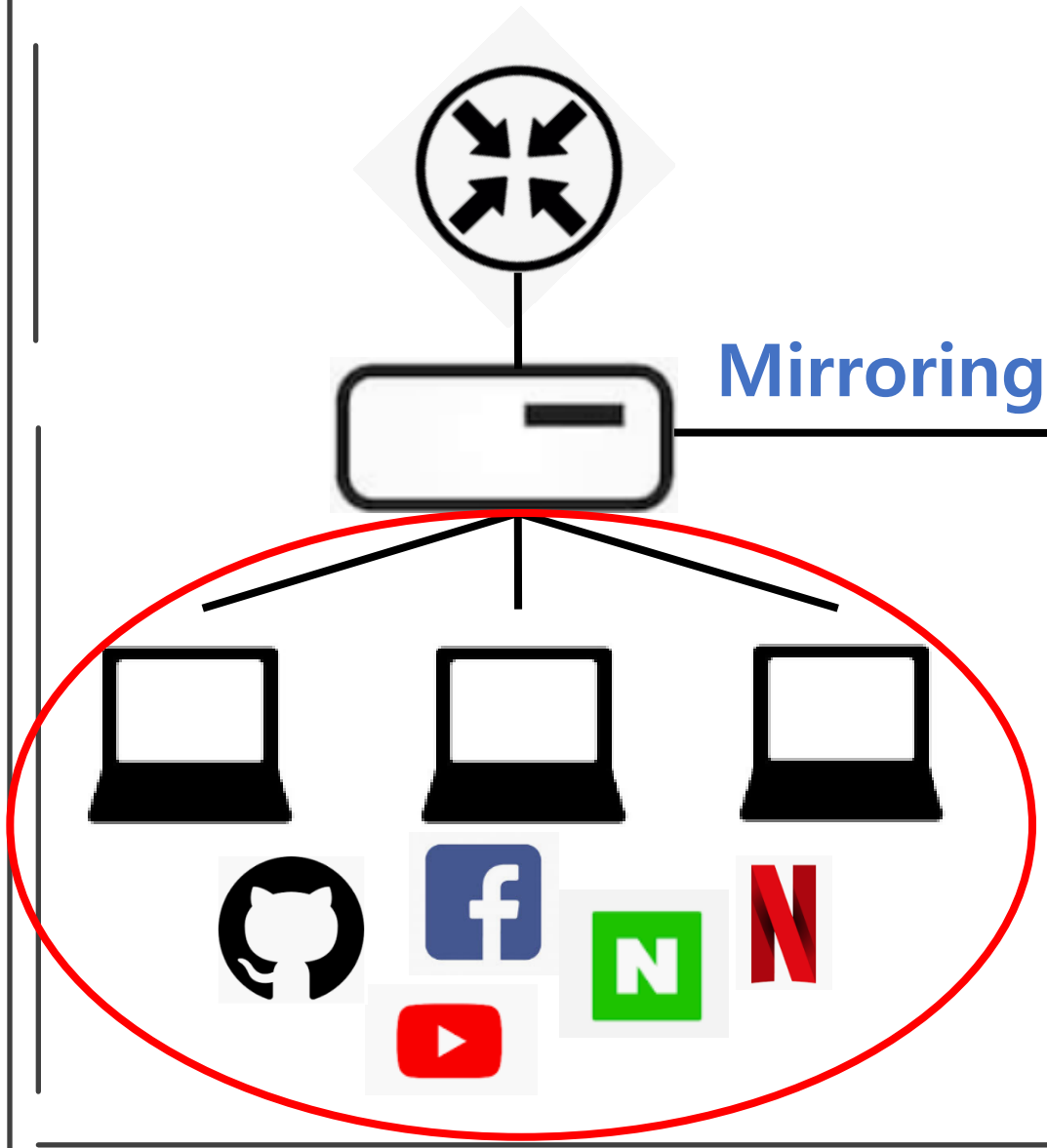
U's Line 사회팀 | 승인 2013.03.14 22:59

교수들의 불만은 학생들의 수업 집중도다. 노트북이나, 태블릿 PC, 스마트 폰 사용 등이 늘면서 강의시간 질문은 거의 없다는 것이 교수들의 한결같은 이야기다.

경기대 행정학과 김 모 교수는 "뭔가 치기는 치는데 칠판은 안보고 자판만 보고 무엇을 치는데 답답하다"며 "수업은 교수의 말과 눈을 바라보며 중요한 부분을 메모를 하기도 하는 것인데 지금 같은 분위기로 계속 수업을 하기가 어려울 것 같아 지침을 고민 중"이라고 토로했다.

학생들 간 불만도 있다. 전체 학생이 노트북을 하고, 태블릿 PC를 하는 것은 아니다. 성균관대 경제학과 민 모 군(22)은 "자판 두들기는 소리에 수업 집중에 방해를 받는다. 그서도 교수님 강의하는 내용을 받아 치냐고 하면 조금이라도 이해를 하겠지만 정작 치는 건 개인적인 내용이다. 좀 무례하기도 하다는 생각과 이렇게 비싼 등록금을 내고 다니는데 수업시간에 저렇게 한다는 것이 이해가 가지도 않는다"고 불평했다.

주제선정 이유



When ?

Who??

시간대별 호스트의
웹사이트 이용빈도를
체크할수 있는 시스템

How much ?

개발 환경

개발 환경

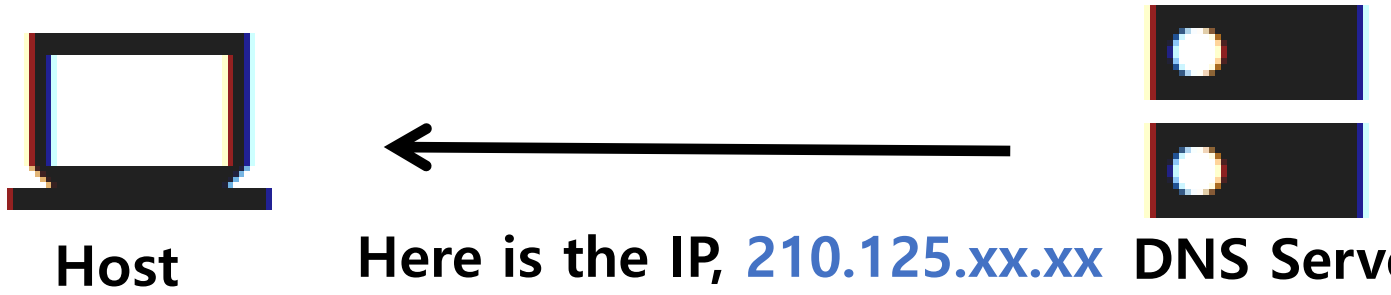
OS	개발 언어	웹 서버	Database
			
Kali Linux	C++	Apache2	MariaDB

동작 방식

DNS 란?

DNS란 **Domain Name System** 을 일컫는다.
인터넷을 이용할땐 **IP** 와 **Port** 를 이용해 통신을 한다.
숫자로 이루어진 **IP 주소 체계**를 사용자가 기억하기 쉬운
언어체계(Domain)로 변환해주는 시스템이다.

DNS Query Response 란 ?



DNS Query 응답 패킷으로
해당 Domain의 IP 정보를
알 수 있습니다.

```
Answers
  www.joongbu.ac.kr: type A, class IN, addr 210.125.239.51
    Name: www.joongbu.ac.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 6382
    Data length: 4
    Address: 210.125.239.51
```

No.	Time	Source	Destination	Protocol	Len	Info
99	1.826161	210.220.163.82	192.168.0.11	DNS	93	Standard query response 0xdb7f A www.joongbu.ac.kr A 210.125.239.51

DNS Query 란 ?

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

DNS Record Type 종류

```
Answers
▼ www.joongbu.ac.kr: type A, class IN, addr 210.125.239.51
    Name: www.joongbu.ac.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 6382
    Data length: 4
    Address: 210.125.239.51
```

서버의 IPv4정보를 획득하기 위해서 Type Hex 값이 0x0001 일때만 정보를 저장.

Problem 1

```
C:₩Users₩JBU_Lee>nslookup
기본 서버:  cellspot.router
Address:  192.168.29.1

> www.youtube.com
서버:    cellspot.router
Address:  192.168.29.1

권한 없는 응답:
이름:    youtube-ui.l.google.com
Addresses:  2404:6800:4004:806::200e
          172.217.25.110
          172.217.25.78
          172.217.24.142
          172.217.26.14
          172.217.25.206
          172.217.25.238
          172.217.31.142
          172.217.26.46
          172.217.161.78
          172.217.31.174
          172.217.161.46
          216.58.197.206
          216.58.197.174
Aliases:  www.youtube.com
```

IF(IP 응답이 여러개면?)

{

}

Solution 1

```
▾ Domain Name System (response)
    Transaction ID: 0xce8a
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Addit▾ Domain Name System (response)
  ▸ Queri      Transaction ID: 0x8e08
  ▾ Answe    ▸ Flags: 0x8180 Standard query response, No error
             Questions: 1
             Answer RRs: 14
             Authority RRs: 0
             Additional RRs: 0
           ▸ Queries
           ▾ Answers
```

www.joongbu.ac.kr

www.youtube.com

Answer RRs Filed 를 통해서
응답 쿼리 개수를 파악하고,
Type 이 0x0001(A) 일때를 모두 저장!

동작 방식

1.1 사용자 정보 저장

웹과 통신하기전에 발생하는 DNS Query Response Packet을 이용해 사용자와 서버의 정보를 DB에 저장한다.

Client_MAC Client_IP

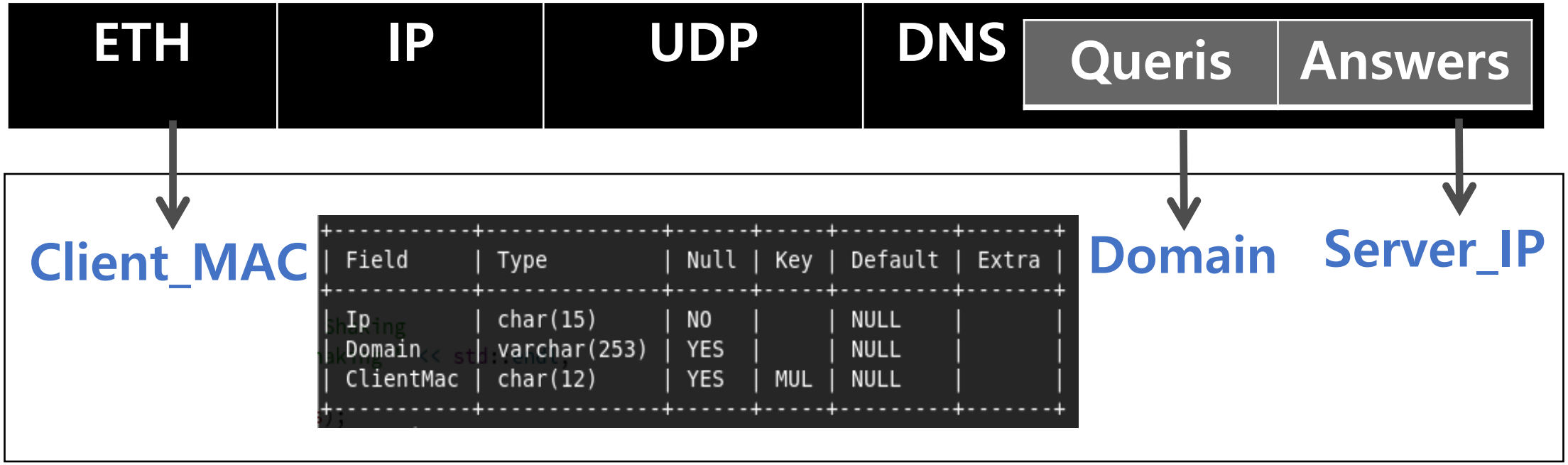
```
+-------+----------+------+-----+---------+-------+
| Field | Type     | Null | Key | Default | Extra |
+-------+----------+------+-----+---------+-------+
| Mac   | char(12) | NO   | PRI | NULL    |       |
| IP    | char(15) | YES  |     | NULL    |       |
| log   | int(11)  | YES  |     | NULL    |       |
+-------+----------+------+-----+---------+-------+
```

[DB Name: Client]

동작 방식

1.2 웹 서버 정보 저장

웹과 통신하기전에 발생하는 DNS Query Response Packet을 이용해 사용자와 서버의 정보를 DB에 저장한다.



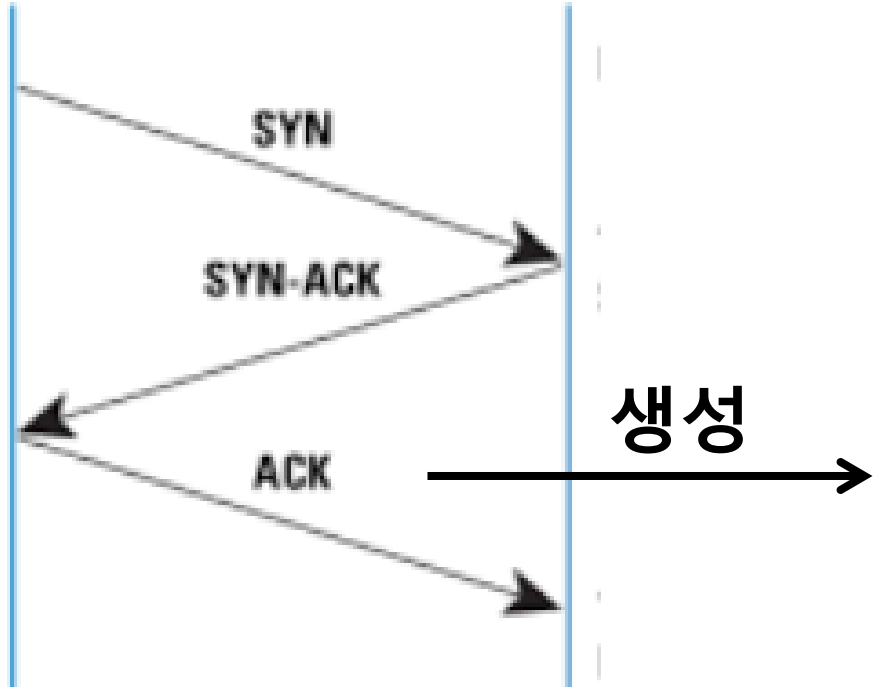
[DB Name: Server]

동작 방식

2.1 Flow 관리의 생성

TCP 세션이 맺어지면 Flow 관리를 시작하며, 암호화된 통신이라도 주소정보는 보이기 때문에 트래픽을 확인, 관리 할 수 있다.

TCP 3-way Handshake



생성

Key	Value
Client_IP	Client_Mac
Client_Port	Start time
Server IP	bps
Server Port	pps

메모리에 저장되는 map

동작 방식

2.2 로그 정보 저장

TCP 세션이 끊어지면 해당 Flow를 삭제하며 DB에 Insert 를 진행,
아래의 경우를 모니터링 한다.

1) FIN Flag

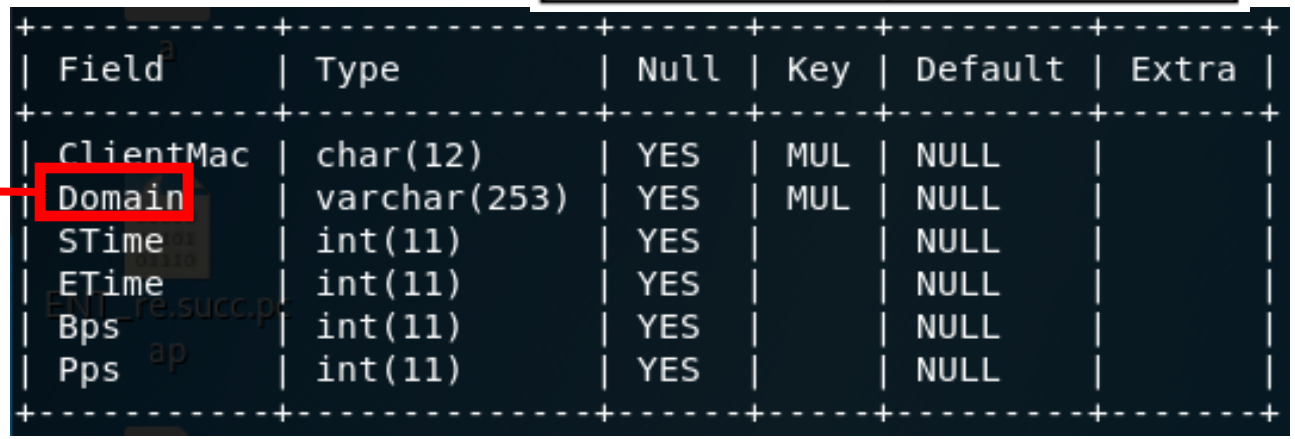
2) RST Flag

3) ESTABLISHED
   장시간 대기 상태

4) SYN SENT 상태

How do you know?

Key	Value
Client_IP	Client_Mac
Client_Port	Start time
Server IP	bps
Server Port	pps



Field	Type	Null	Key	Default	Extra
ClientMac	char(12)	YES	MUL	NULL	
Domain	varchar(253)	YES	MUL	NULL	
STime	int(11)	YES		NULL	
ETime	int(11)	YES		NULL	
Bps	int(11)	YES		NULL	
Pps	int(11)	YES		NULL	

[DB Name: Log]

동작 방식

Key	Value
Client_IP	Client_Mac
Client_Port	Start time
Server IP	bps
Server Port	pps

SELECT Domain FROM Server
WHERE Ip="175.35.XX.XX"

```
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| Ip        | char(15)     | NO   |     | NULL    |       |
| Domain    | varchar(253) | YES  |     | NULL    |       |
| ClientMac | char(12)     | YES  | MUL | NULL    |       |
+-----------+--------------+------+-----+---------+-------+
```

[DB Name: Server]

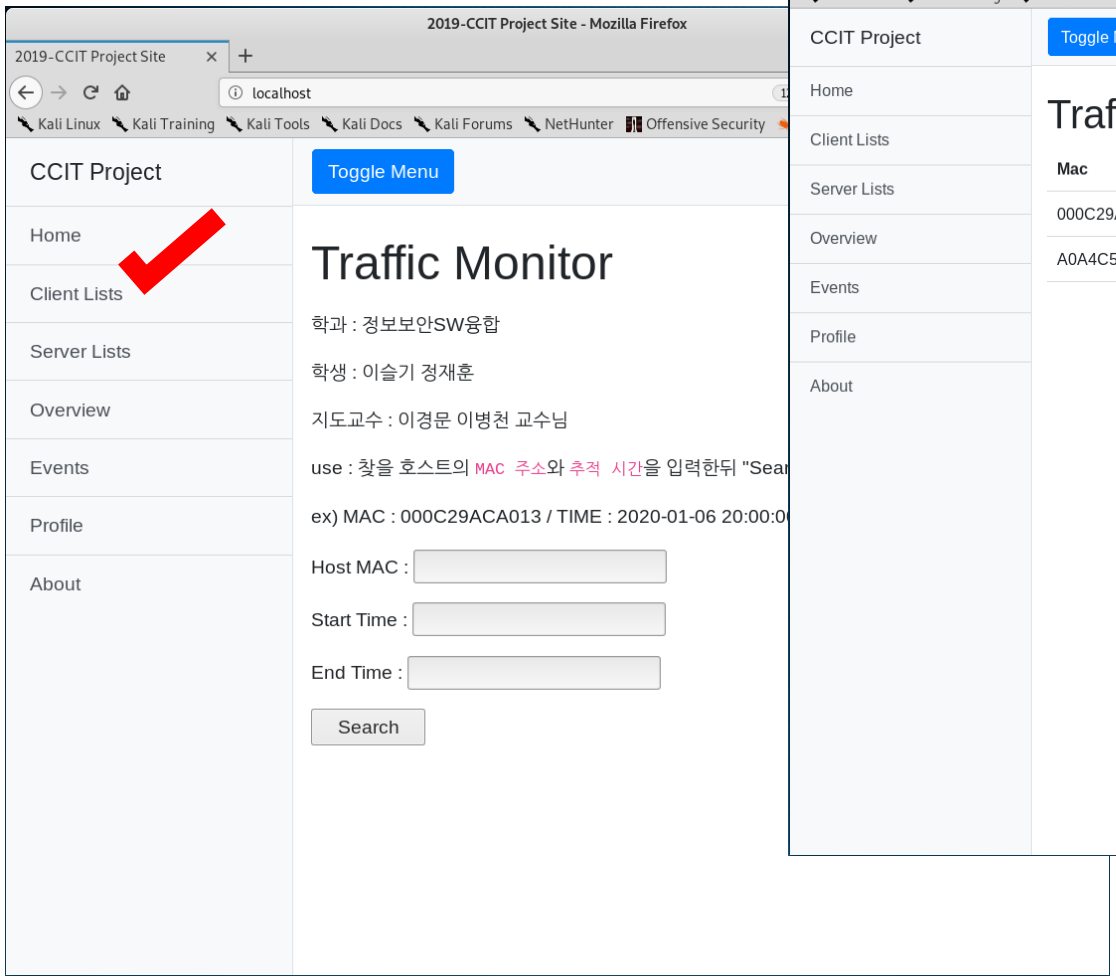
www.joongbu.ac.kr

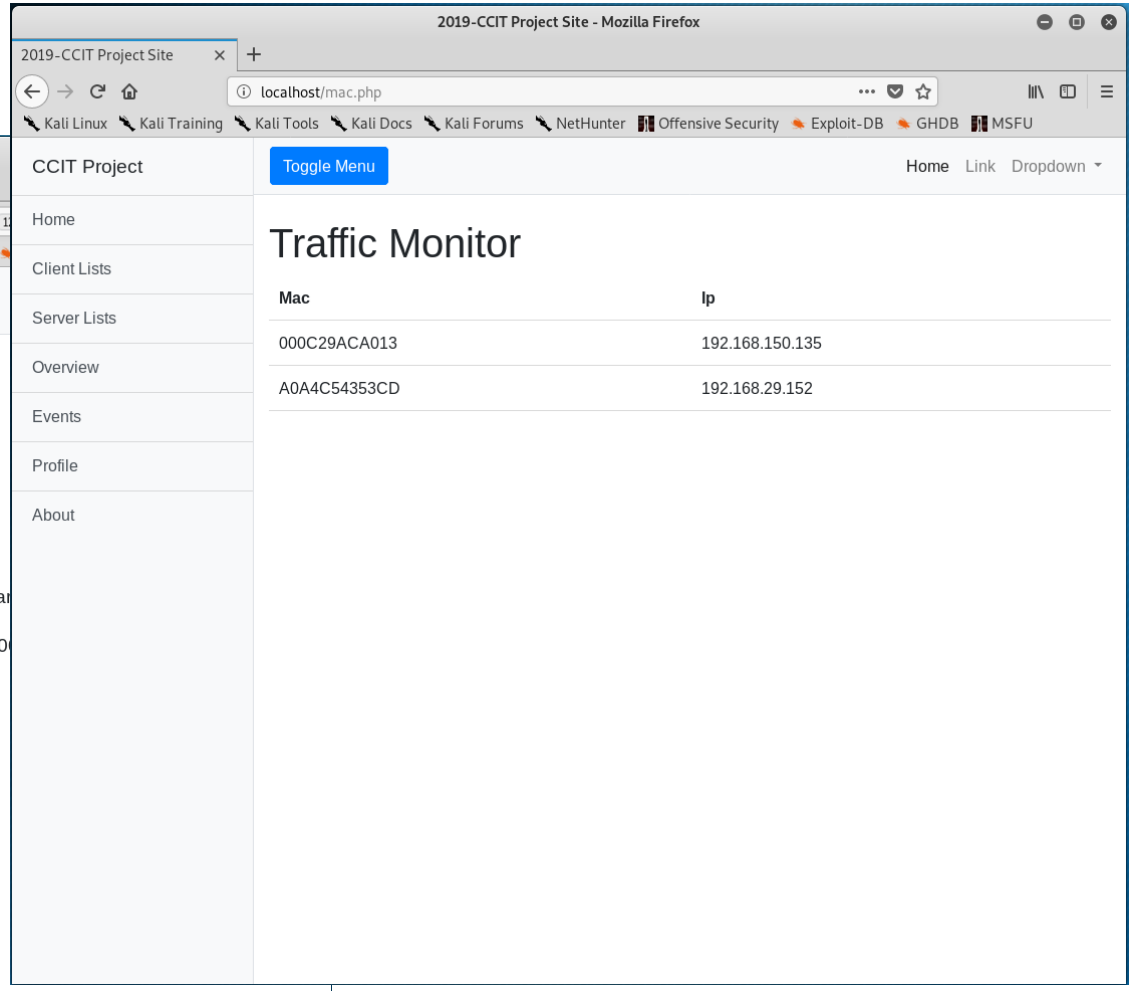
```
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| ClientMac | char(12)     | YES  | MUL | NULL    |       |
| Domain    | varchar(253) | YES  | MUL | NULL    |       |
| STime     | int(11)      | YES  |     | NULL    |       |
| ETime     | int(11)      | YES  |     | NULL    |       |
| Bps       | int(11)      | YES  |     | NULL    |       |
| Pps       | int(11)      | YES  |     | NULL    |       |
+-----------+--------------+------+-----+---------+-------+
```

[DB Name: Log]

동작 방식

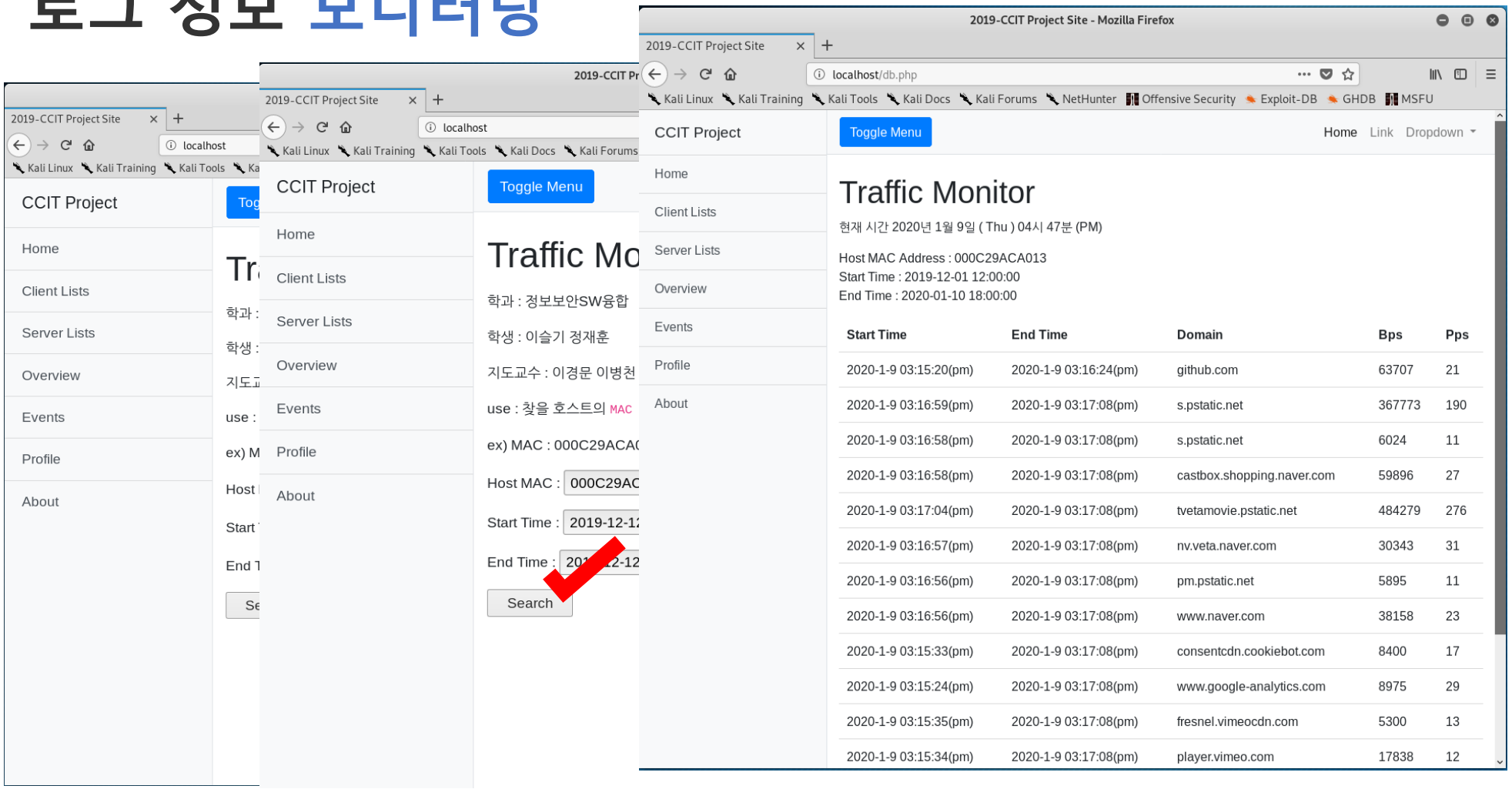
3.1 로그 정보 모니터링





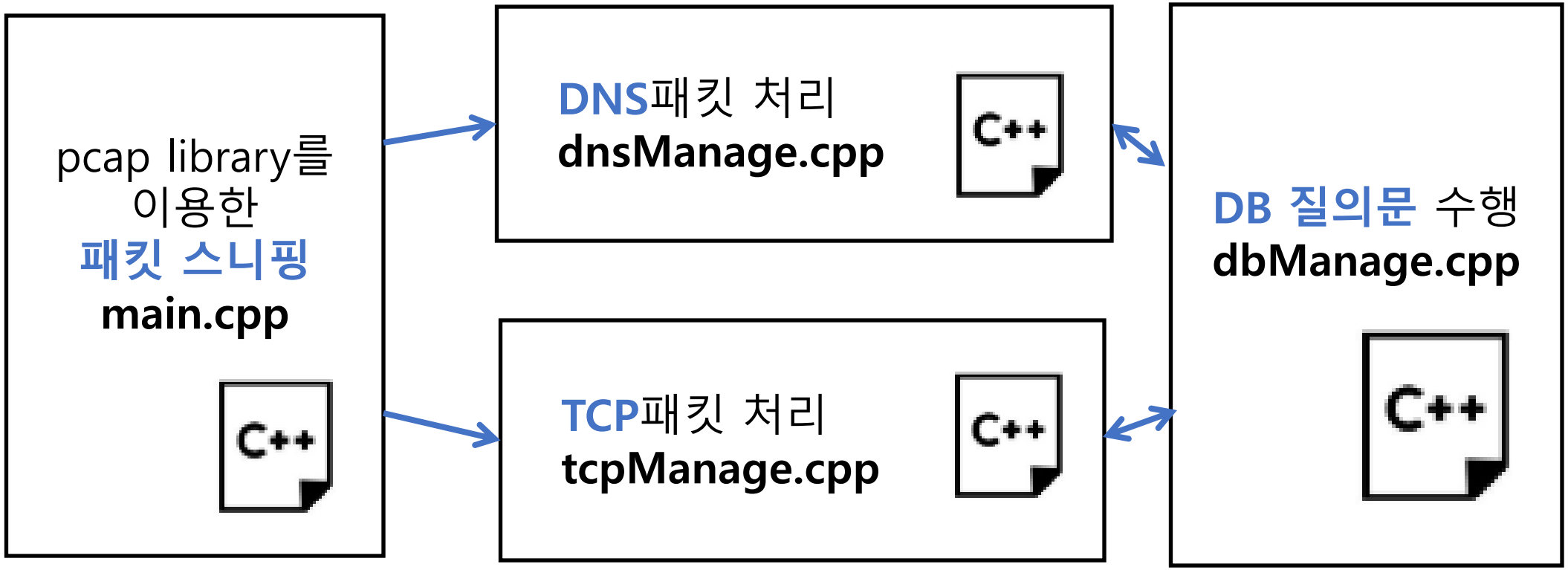
동작 방식

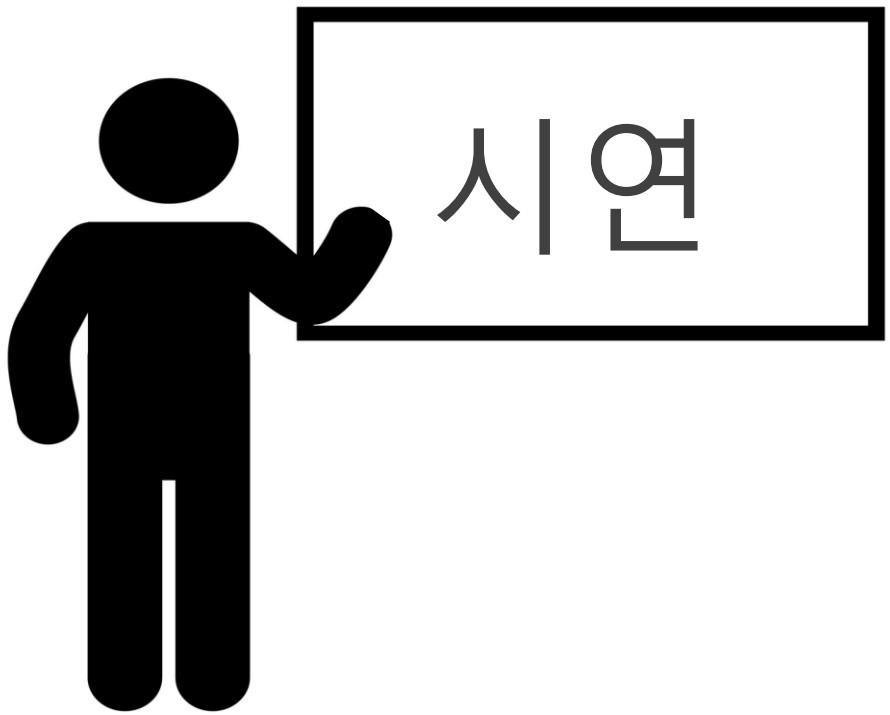
3.1 로그 정보 모니터링

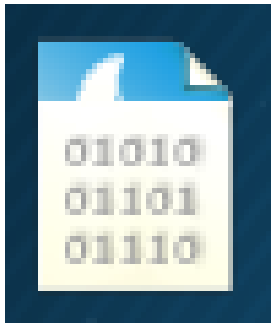


동작 방식

4.1 기능 모듈화



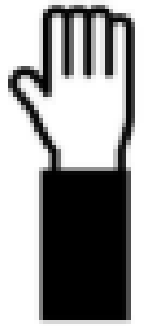




ccitproject.pcap

pcap_open_offline()

Q & A



HP : 010-2303-8619
E-mail : seolki100480@gmail.com
Git : github.com/JBU-seol/traffic_manager


감사합니다