백엔드 팀 실습

2주차

16 김성민

ARGOS

INDEX

백엔드 팀 2주차

도메인 설정

- 도메인
- 무료 도메인 설정

ARGOS

도메인

도메인 네임 (Domain Name)

컴퓨터를 식별하는 데 사용되는 호스트 명.

도메인 레지스트리 (도메인 네임 데이터베이스)에 저장되어 있음.

숫자의 집합으로 된 IP 주소보다 외우기 쉬우며, 반드시 IP 주소와 1:1로 대응되지 않음.

(1:다, 다:1의 경우도 가능.)

대부분 유료로 대여를 해 주지만, 다행스럽게도 잘 쓰이지 않는 최상위 도메인을

무료로 대여 해 주는 곳이 있음. 실습을 위해서는 이러한 곳을 이용할 예정.

정식 서비스를 등록하기 위해, 사람들이 외우기 쉬운 도메인이 필요하다면

유료로 제공하는 호스팅 업체를 찾아보는 것이 좋음. (argos.or.kr도 유료 호스팅)

무료 도메인 설정

freenom

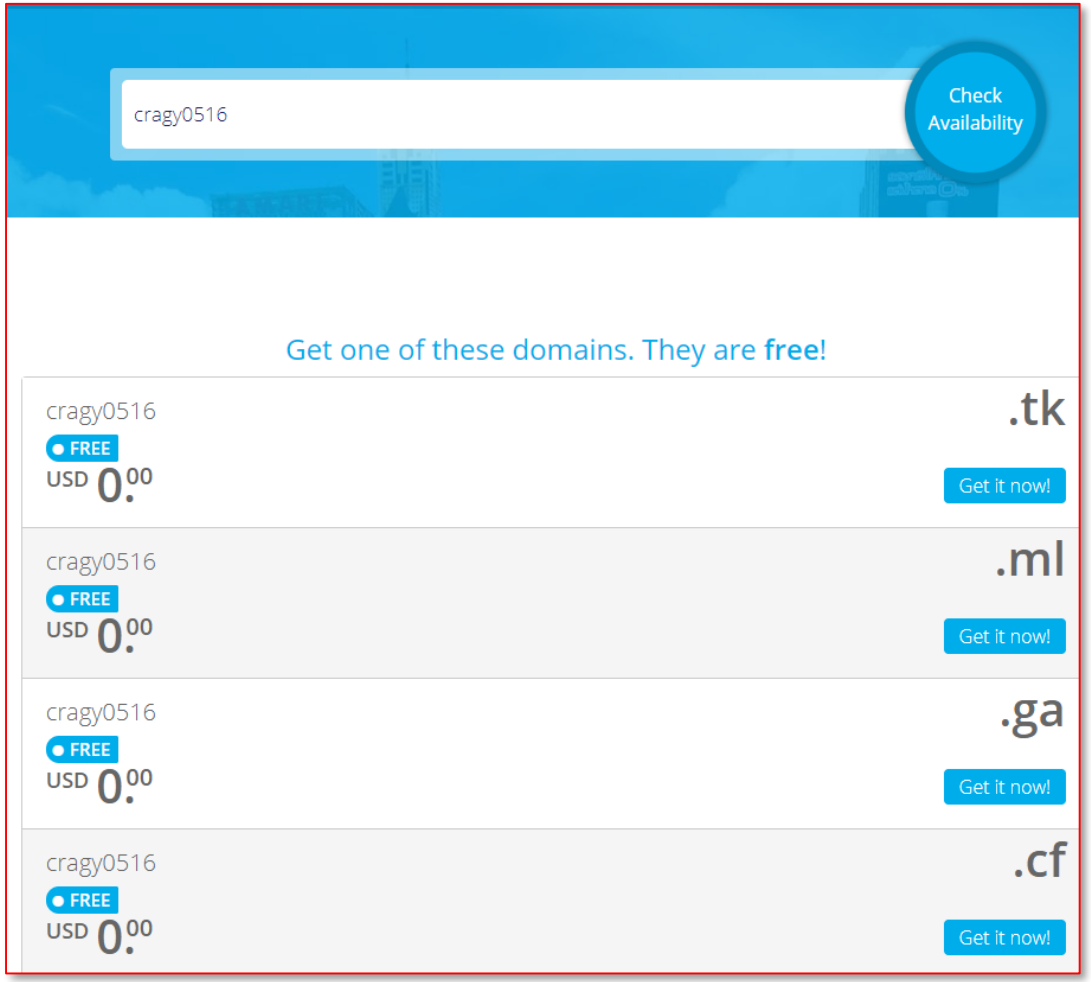
https://my.freenom.com/

Services -> Register a New Domain

사용하고 싶은 도메인 입력.

무료로 이용 가능한 도메인 확인.

(회원가입은 나중에 함)



사용 날짜 선택 (3 ~ 12개월 무료)

12개월 초과 사용하려면 일정 금액을 지불해야 함.

실습을 위해서 원하는 기간 자유롭게 선택.

Expire되기 14일 전 부터 갱신 가능하며, 무제한 갱신 가능.

하지만 갱신하지 못하면 해당 도메인은 일정 기간 동안 유료로 전환.

회원가입

진행 하다 보면 이메일이나 소셜 로그인으로 가입해야 함.

다른 건 괜찮은데 주소 쓰는게 조금 걸릴 수 있어서 가져옴.

복사 편하게 하기 위한 링크

한글주소	영문주소	우편번호
도로명 대전광역시 유성구 대학로 99 (궁동, 충남대학교)	99, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea	34134

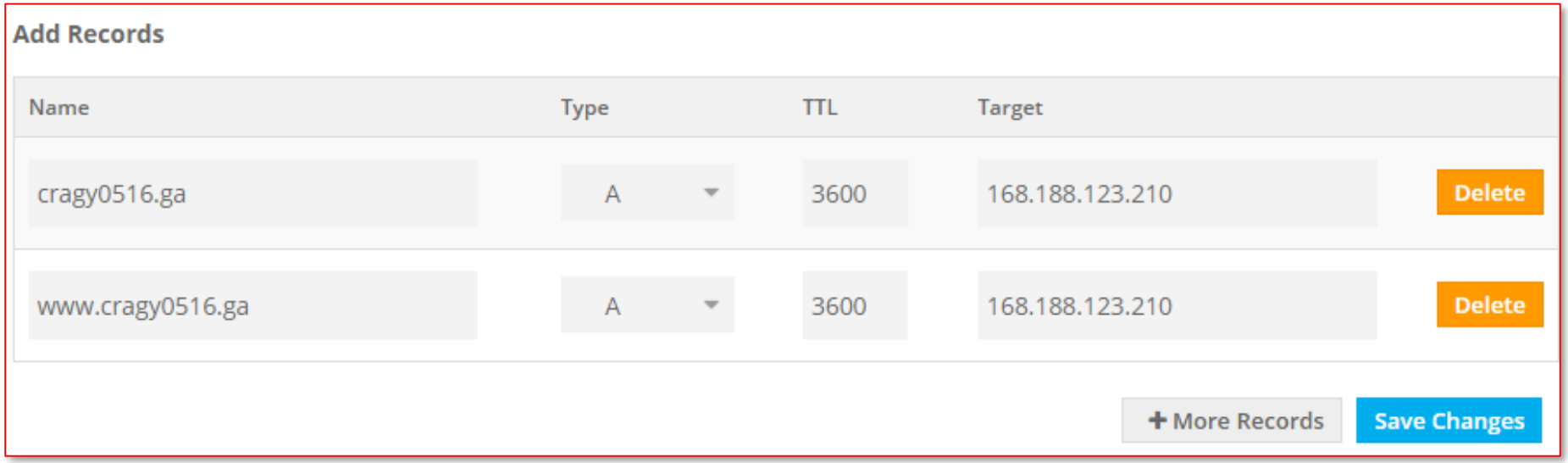
Record 등록

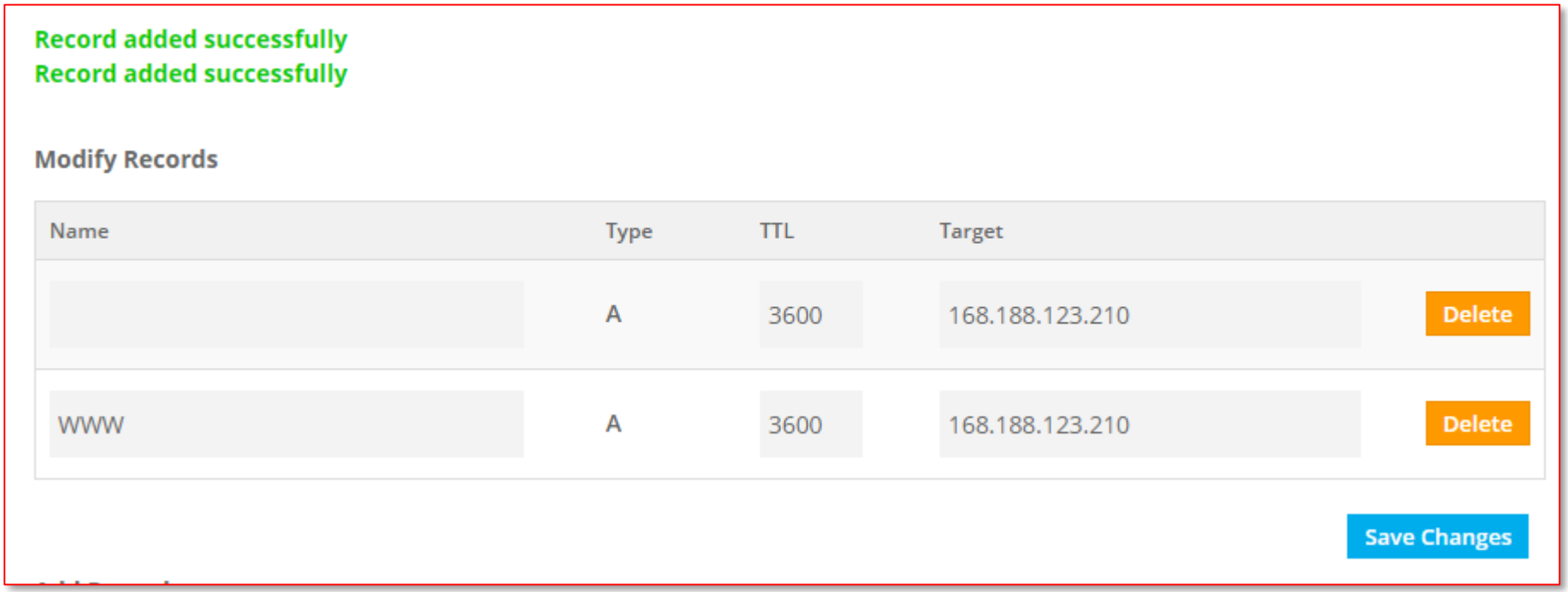
로그인한 뒤,

Services -> My Domains -> Manage Domain -> Manage Freenom DNS

아래 그림과 같이 입력

(결과에 도메인 이름이 사라져서 나오는데, 원래 그렇습니다.)





등록 결과

(적용되기 까지 시간은 좀 걸린다.)

백엔드 팀 2주차

웹 서버 설치

- nginx 설치
- HTTPS 설정
- 인증서 자동 갱신

ARGOS

nginx 설치

ARGOS

패키지 업그레이드 / 업데이트

sudo apt-get upgrade

sudo apt-get update

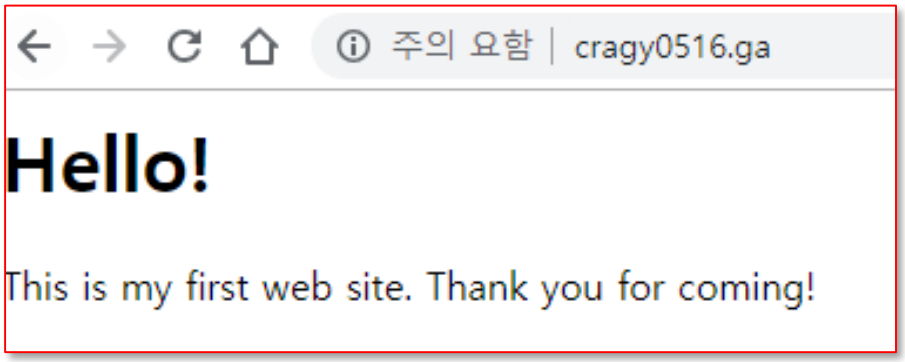
nginx 설치

sudo apt-get install nginx

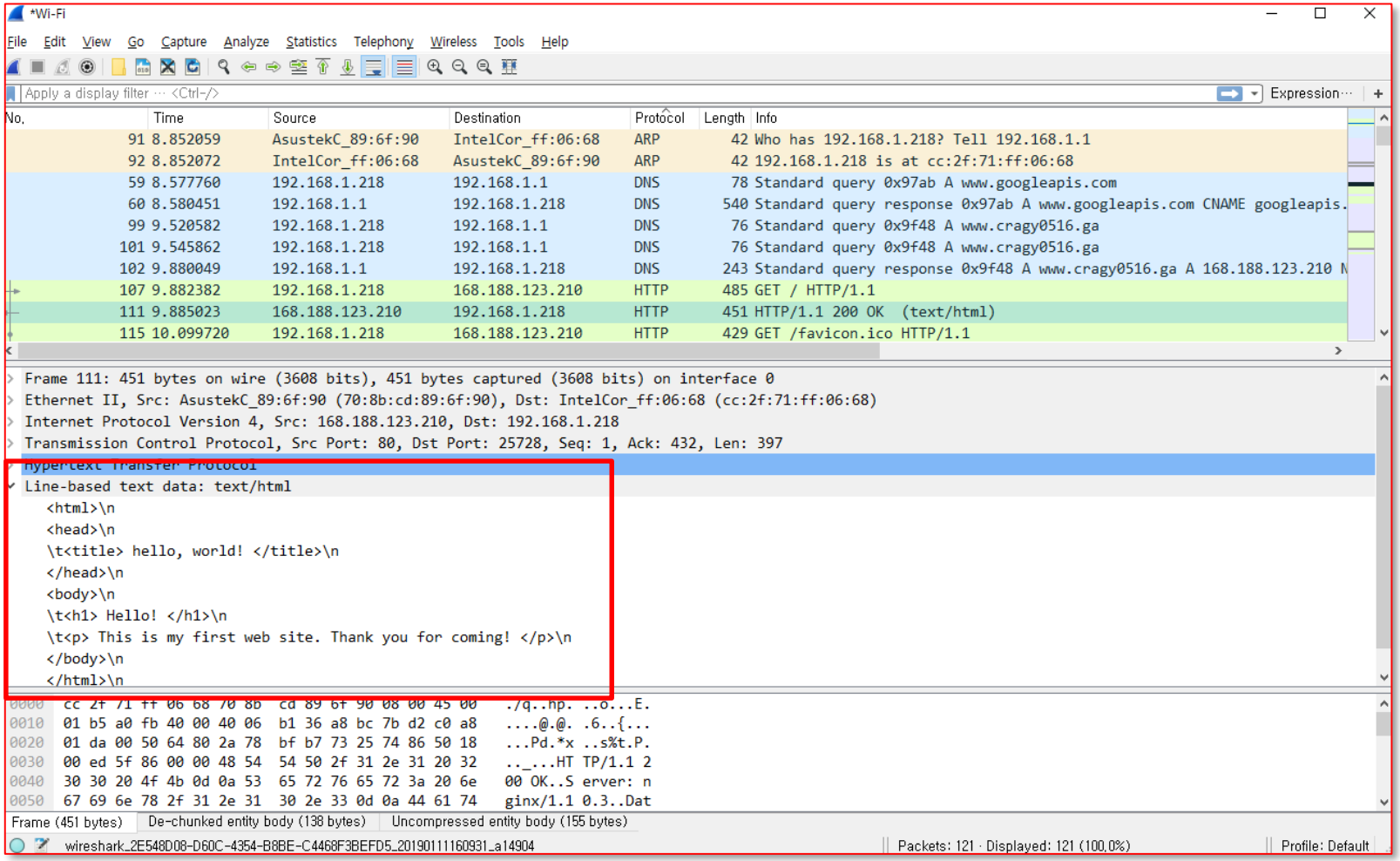
```
pi@raspberrypi:/var/www/html $ pwd
/var/www/html
pi@raspberrypi:/var/www/html $ sudo vi index.html
```

/var/www/html

새로운 index.html 작성



index.html 표시 확인



Wireshark로 캡처한 패킷

HTTP 통신이 암호화되지 않음. 스니핑 공격에 취약. -> 암호화 필요

HTTPS 설정

Letsencrypt

참고 : https://kr.minibrary.com/353/

https://certbot.eff.org/lets-encrypt/pip-nginx

설치

wget https://dl.eff.org/certbot-auto

chmod a+x certbot-auto

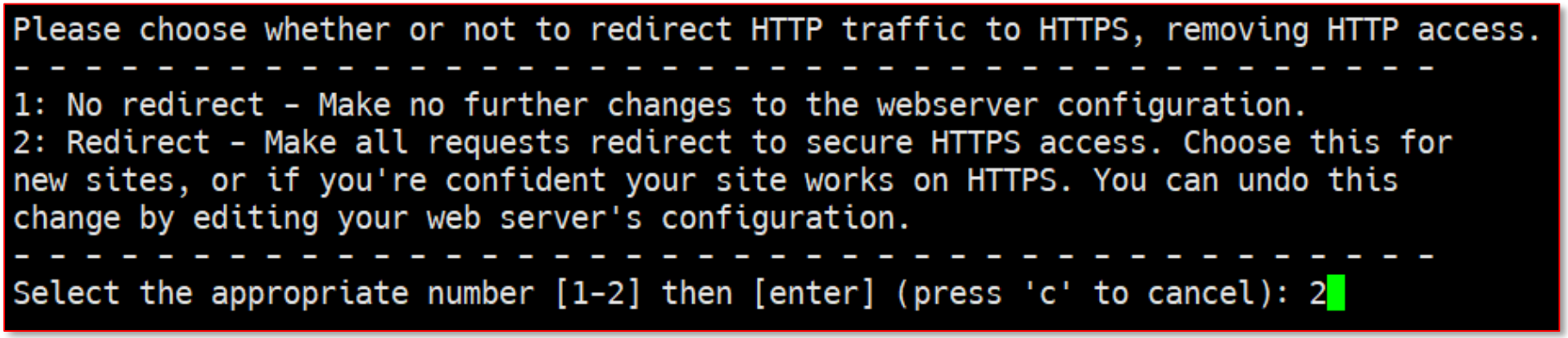
sudo ./path/to/certbot-auto --nginx


```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): cragy0516@gmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated)  (Enter 'c' to cancel): cragy0516.ga
Obtaining a new certificate
```

설치 시 이메일, 약관 동의, 도메인 이름 설정 등 진행.



2번을 선택.

HTTP 요청을 HTTPS로 리다이렉션 하여 HTTP 접근 차단.

ARGOS

HTTPS 적용 확인

ip.addr == 168.188.123.210

	Time	Source	Destination	Protocol	Length	Info
100	2.230148	192.168.1.218	168.188.123.210	TLSv1.2	588	Application Data
101	2.230802	168.188.123.210	192.168.1.218	TCP	60	443 → 26313 [ACK] Seq=2956 Ack=603 Win=30336 Len=0
102	2.231406	168.188.123.210	192.168.1.218	TCP	60	443 → 26313 [ACK] Seq=2956 Ack=1137 Win=31360 Len=0
103	2.285639	168.188.123.210	192.168.1.218	TLSv1.2	1514	Server Hello
104	2.285917	168.188.123.210	192.168.1.218	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]
105	2.285932	192.168.1.218	168.188.123.210	TCP	54	26312 → 443 [ACK] Seq=518 Ack=2921 Win=65536 Len=0
106	2.286031	168.188.123.210	192.168.1.218	TLSv1.2	89	Server Key Exchange, Server Hello Done
107	2.286220	192.168.1.218	168.188.123.210	TLSv1.2	139	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
108	2.287218	168.188.123.210	192.168.1.218	TCP	60	443 → 26312 [ACK] Seq=2956 Ack=603 Win=30336 Len=0
109	2.289594	168.188.123.210	192.168.1.218	TLSv1.2	304	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
110	2.290493	168.188.123.210	192.168.1.218	TLSv1.2	254	Application Data
111	2.290565	192.168.1.218	168.188.123.210	TCP	54	26313 → 443 [ACK] Seq=1137 Ack=3406 Win=65024 Len=0
112	2.296313	168.188.123.210	192.168.1.218	TLSv1.2	304	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
114	2.340492	192.168.1.218	168.188.123.210	TCP	54	26312 → 443 [ACK] Seq=603 Ack=3206 Win=65280 Len=0

암호화된 통신 수행

인증서 자동 갱신

ARGOS

인증서는 3개월마다 만료

이를 자동으로 갱신하기 위해 crontab 사용

sudo vi /etc/crontab

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
0 0,12 * * * python -c 'import random; import time; time.sleep(random.random( ) * 3600)' && ./home/pi/Desktop/certbot-auto renew
```

DB 설정

MySQL 설치

sudo apt-get install mysql-server mysql-client

MySQL 접속

sudo mysql -uroot

root 비밀번호 변경 (링크 참조)

use mysql

INSERT INTO user (host,user,authentication_string,ssl_cipher,

x509_issuer,x509_subject) VALUES ('localhost','root',password('my_password','','',''));

```
MariaDB [(none)]> SELECT host,user,authentication_string FROM mysql.user;
+-----------+------+-------------------------------------------+
| host      | user | authentication_string                     |
+-----------+------+-------------------------------------------+
| localhost | root | *34A[redacted]                            |
+-----------+------+-------------------------------------------+
1 row in set (0.00 sec)

MariaDB [(none)]>
```

ARGOS

localhost에서 접속할 때, 그 외(%)에서 접속할 때 비밀번호를 다르게 설정 가능.

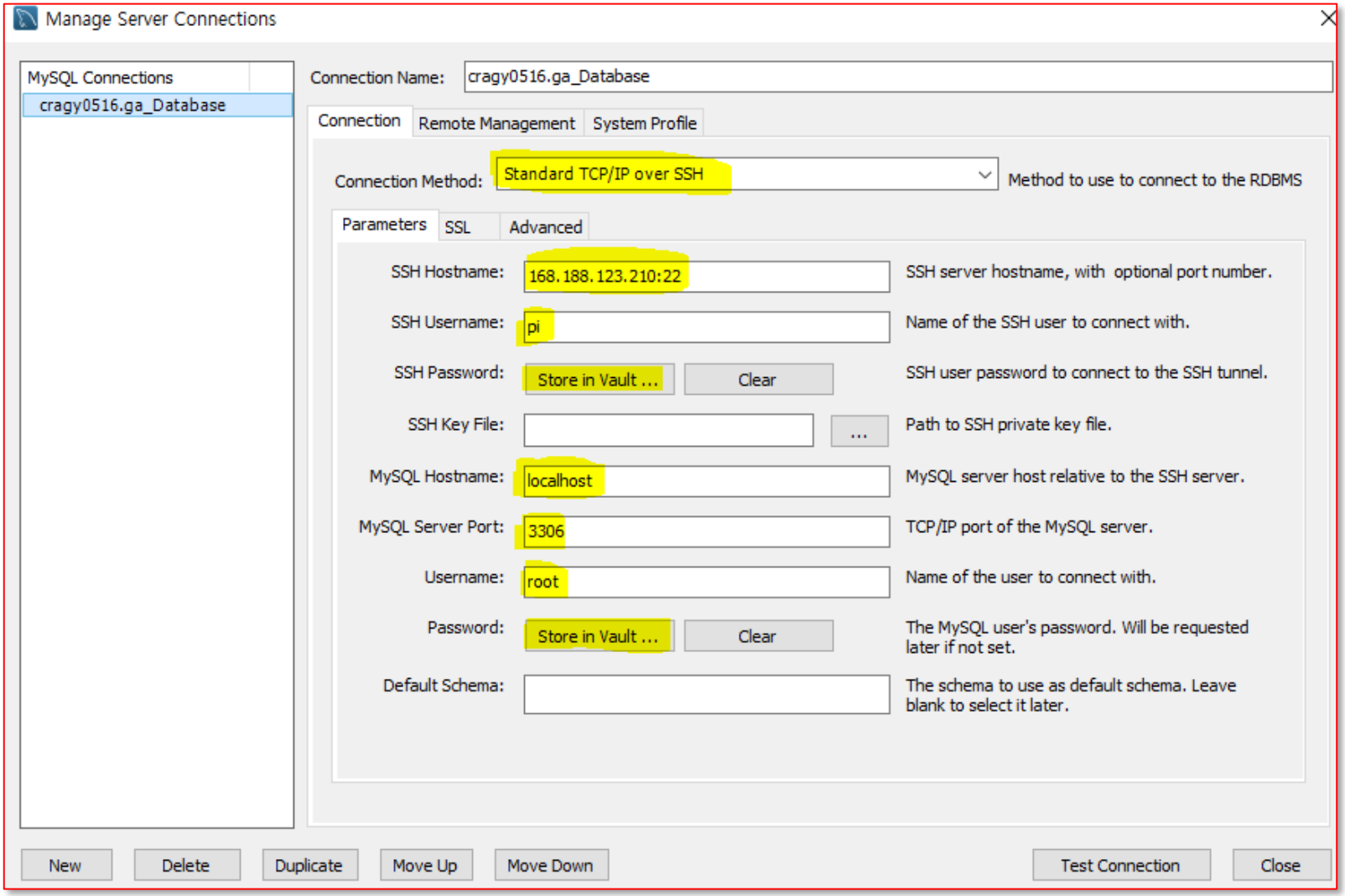
SSH 터널링을 통해 접속할 예정이므로 localhost의 경우만 허용.

MySQL Workbench 다운로드

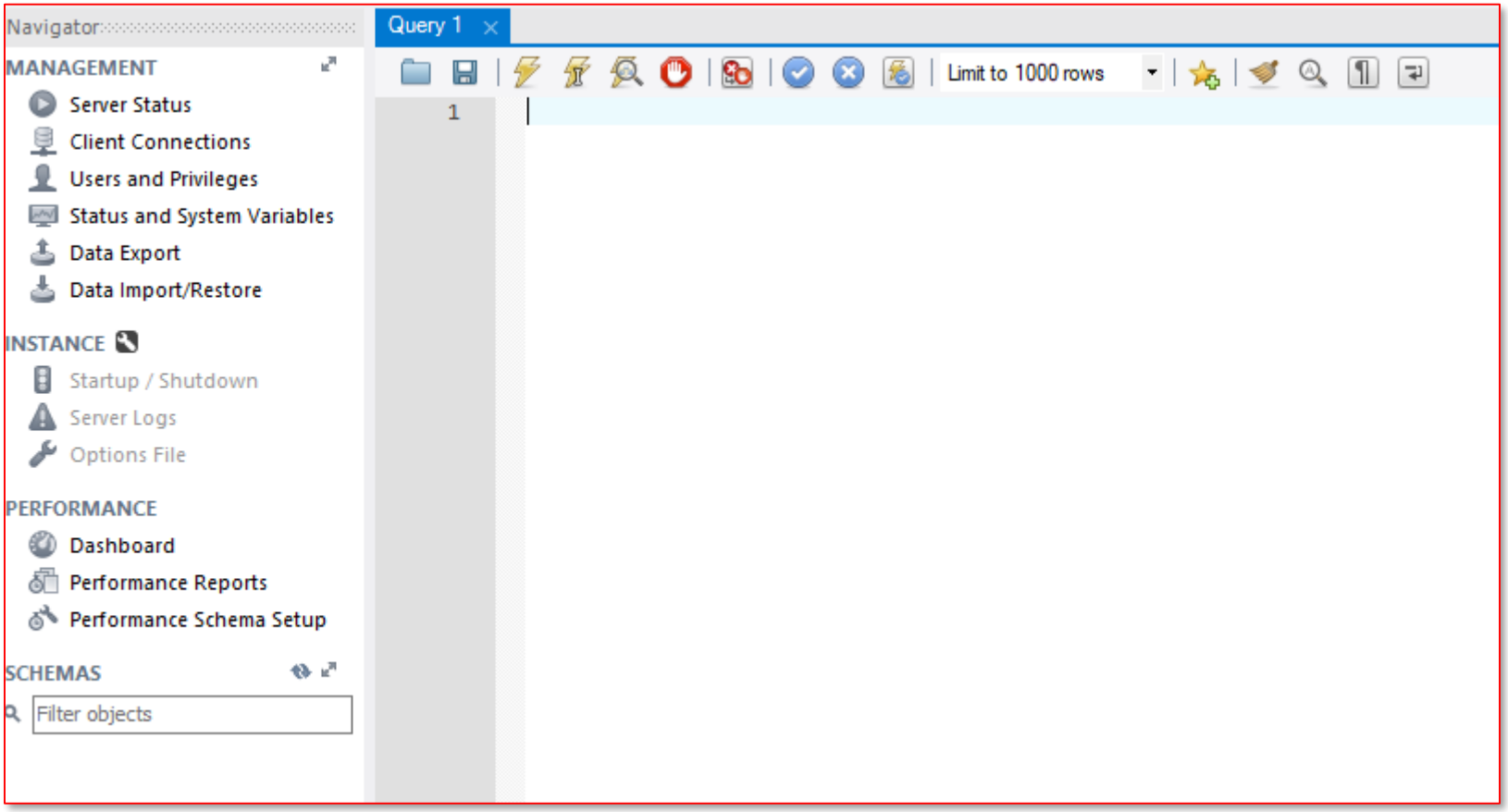
https://www.mysql.com/products/workbench/

SSH 터널링을 통해 Database 접속

Windows PC => SSH Remote Server (라즈베리 파이) => Database Server (localhost)


Manage Server Connections
MySQL Connections
cragy0516.ga_Database
Connection Name:
cragy0516.ga_Database
Connection
Remote Management
System Profile
Connection Method:
Standard TCP/IP over SSH
Method to use to connect to the RDBMS
Parameters
SSL
Advanced
SSH Hostname:
168.188.123.210:22
SSH server hostname, with optional port number.
SSH Username:
pi
Name of the SSH user to connect with.
SSH Password:
Store in Vault ...
Clear
SSH user password to connect to the SSH tunnel.
SSH Key File:
...
Path to SSH private key file.
MySQL Hostname:
localhost
MySQL server host relative to the SSH server.
MySQL Server Port:
3306
TCP/IP port of the MySQL server.
Username:
root
Name of the user to connect with.
Password:
Store in Vault ...
Clear
The MySQL user's password. Will be requested later if not set.
Default Schema:
The schema to use as default schema. Leave blank to select it later.
New
Delete
Duplicate
Move Up
Move Down
Test Connection
Close

접속 성공 확인


Navigator
MANAGEMENT
Server Status
Client Connections
Users and Privileges
Status and System Variables
Data Export
Data Import/Restore
INSTANCE
Startup / Shutdown
Server Logs
Options File
PERFORMANCE
Dashboard
Performance Reports
Performance Schema Setup
SCHEMAS
Filter objects
Query 1
Limit to 1000 rows
1

Q & A

Thank You for Listening

Created By cragy0516
Thanks To ccoma