안드로이드 루팅해서 서버 만들기

Feat. Galaxy S8+ | Nextcloud

SCA 2학년 지윤찬

안드로이드 **루팅**해서 **서버 만들기**

목차

0 - 서론
- 프로젝트의 계기 & 구상

1 - 루팅이란?
- 구형 폰 비밀번호 크랙해보기

2 - S8+ 서버 세팅
- postmarketOS 설치
- 나만의 구글드라이브

3 - 마무리
- 소감

SCA 2학년 지윤찬

제 0장

서론 - 계기

프로젝트 계기

취미 : 전자기기 모으기

안드로이드 루팅해서 서버 만들기

프로젝트 계기

갤럭시 S2, 갤럭시 S3 버라이즌, 갤럭시 S4 LTE-A, 갤럭시 S8, 갤럭시 S8+ 스페셜에디션 ,갤럭시 S9+ , 갤럭시 S20 5g, 갤럭시 Z 플립4, 갤럭시 노트3 , 갤럭시 노트5, 갤럭시 노트9, 갤럭시 노트 10.1, 갤럭시노트 10.1 2014에디션, 갤럭시 그랜드, 갤럭시 그랜드맥스, 갤럭시 코어 어드밴스, 삼성노트북 5, 아이폰 6s, 아이폰 8+, 아이폰 X, 아이폰 SE 2020, 아이폰 12미니, 아이폰15프로, 아이패드 4, 아이패드 에어3, 맥북프로 2011 early, 맥북에어 mid2012, LG V20, LG X6, LG 울트라PC, DELL inspiron 15 3525, DELL Optiplex 7050, HP envy 360x, Lenovo ideapad 330s, Lenovo ideapad 330, HTC EVO 4G+, 외 노트북 10, 스마트폰 20, 조립 데스크탑 8, 음향기기 3 등등...

취미 : 전자기기 모으기

프로젝트 계기

이런 **남아도는 H/W 활용**
하고싶었음

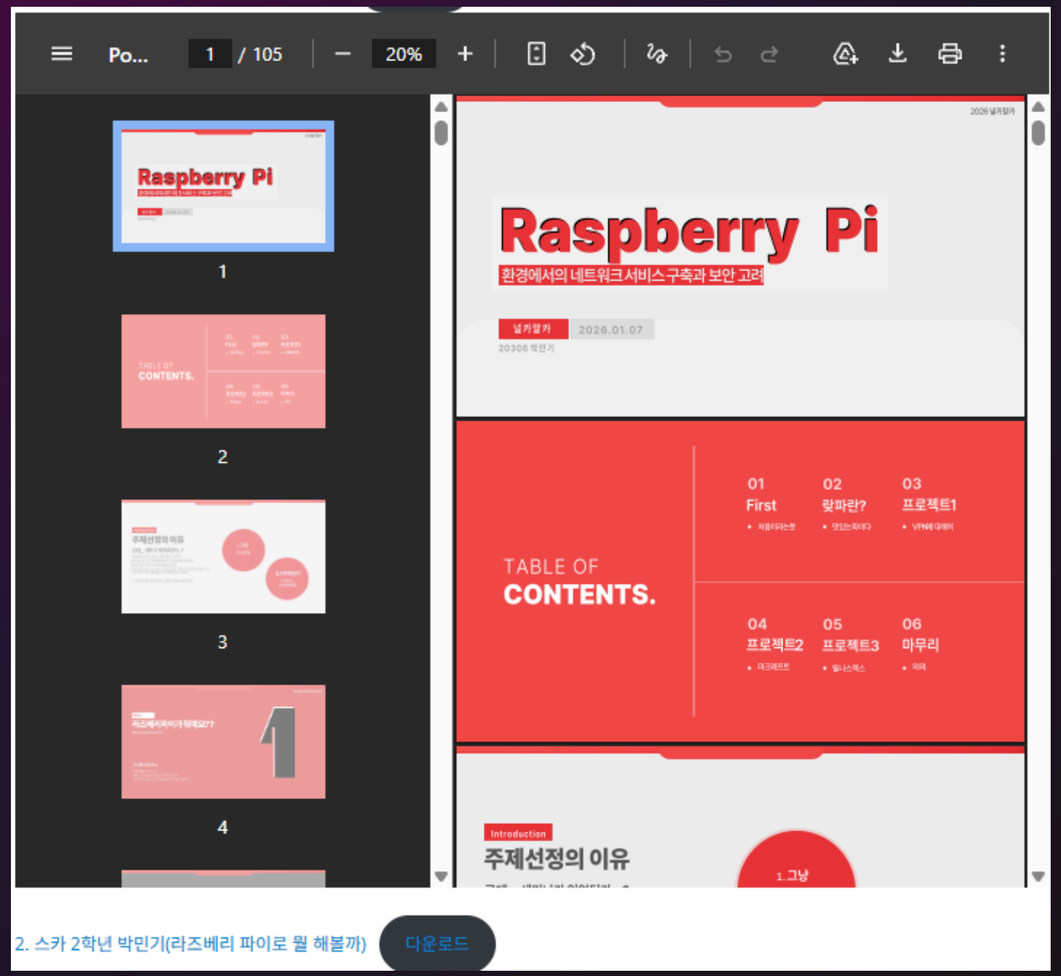
프로젝트 계기

이전까진 **묘책이X**

프로젝트 계기

그런데 **이걸** 보고
묘책이 떠오름

안드로이드 루팅해서 서버 만들기



출처 : 2025하반기 발표자료 - 민기선배

프로젝트 계기

시스템 구축

프로젝트 계기

남아도는 H/W 활용

제 0-1장

서론 - 구상

프로젝트 구상

전체적인 형태 : 저전력 서버 만들기

프로젝트 구상

처음 : iPhone 6s 탈옥해서 서버 만들기

프로젝트 구상

막상 **시작**하니 iPhone iOS 탈옥해서

처음 : 개발 제한 많음

제한사항이 **너무 많음**

안드로이드 루팅해서 서버 만들기

프로젝트 구상

2. 사양

칩	Apple A9 APL0898[2] & APL1022[3] SoC [구성 내용 확인] + 퀄컴 스냅드래곤 X7 LTE 모뎀[6]
메모리	2 GB LPDDR4 SDRAM

6s 탈옥해서

들기

메모리 2GB

프로젝트 구상

처음엔 iPhone 6s 탈옥해서 서버 만들기

에뮬/가상머신 X

프로젝트 구상

처음 iPhone 6s 탈옥해서 서버 만들기

iOS 위에서 돌리면 성능 ↓

프로젝트 구상

처음 : iPhone 6s 탈옥해서 서버 만들기

24시간

돌리기에도 부적합

안드로이드 루팅해서 서버 만들기

프로젝트 구상

Features	
Flashing	Broken
USB Networking	Works
Battery	Broken
Screen	Works
Touchscreen	Broken
Multimedia	
3D Acceleration	Broken
Audio	Broken
Camera	Broken
Connectivity	
WiFi	Broken
Bluetooth	Broken
GPS	Broken
Modem	
Calls	Broken
SMS	Broken
Mobile data	Broken
Miscellaneous	
FDE	*Untested*
USB OTG	Partial
Sensors	
Accelerometer	Broken

막 제한 없음

가장 중요한
네트워크 안됨!

프로젝트 구상

비교적 **자유로운**

Android 기반

프로젝트 구상

S8+ (6GB / 128GB)

프로젝트 구상

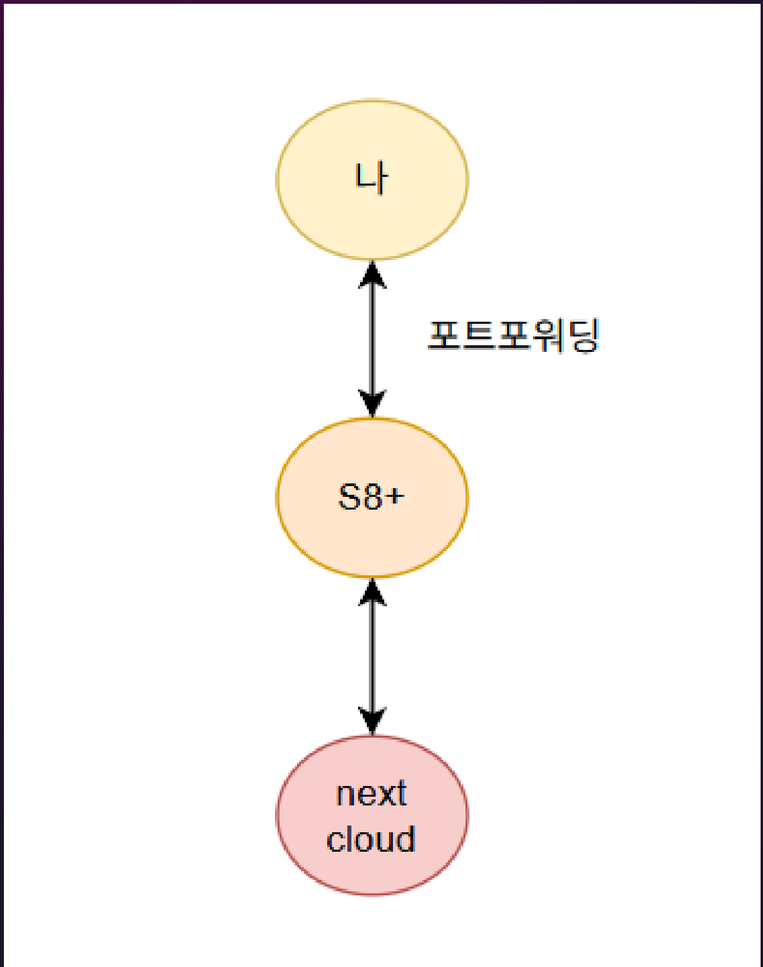
S8+ (6GB / 128GB)

프로젝트 구상

Features	
Flashing	Works
USB Networking	Works
Internal storage	*Untested*
SD card	*Untested*
Battery	Works
Screen	Works
Touchscreen	Works
Multimedia	
3D Acceleration	Broken
Audio	Broken
Camera	Broken
Camera Flash	*Untested*
Connectivity	
WiFi	Works
Bluetooth	Broken
GPS	Broken
NFC	*Untested*
Modem	
Calls	Broken
SMS	Broken
Mobile data	Broken
Miscellaneous	
FDE	Partial
USB OTG	Works

조건에 부합함

프로젝트 구상



프로젝트 구상

Step1 :
S8+ 루팅, 리눅스 설치

제 1장

루팅이란?

이름이 상당히 익숙함

이름(

```
# whoami
root
```

녹함

안드로이드 **루팅**해서 **서버 만들기** - 루팅이란?



Android 리눅스 커널기반

샤오미 갤럭시 ~~LG~~



Android 에서 Root 권한 얻는게 루팅

~~샤오미~~ ~~갤럭시~~ ~~LG~~

근데 이거 왜 함?

일반사용자보다높은권한을가
져,/data/system폴더에접근가능하고커
널까지갈아끼울수가있어져서오버클럭언
더볼팅등등많은걸할수있다.

일반사용자보다높은권한을가
ystem폴더에접근가능하고커
끼을수가있어서오버클럭언
팅등등많은걸할수있다.



지루하고 현학적



일반적으로 **못하는 거**
다 **할 수 있다**

for 리눅스 설치

예를들면
비밀번호 크랙하기

제 1-1장

구형 폰 루팅해서 비밀번호 크랙하기

대상



갤럭시 그랜드

안드로이드 4.1.2(취약함)

password.key(40자 sha-1)

대상



갤럭시 그랜드

/data/system/locksettings.db

password.key

대상



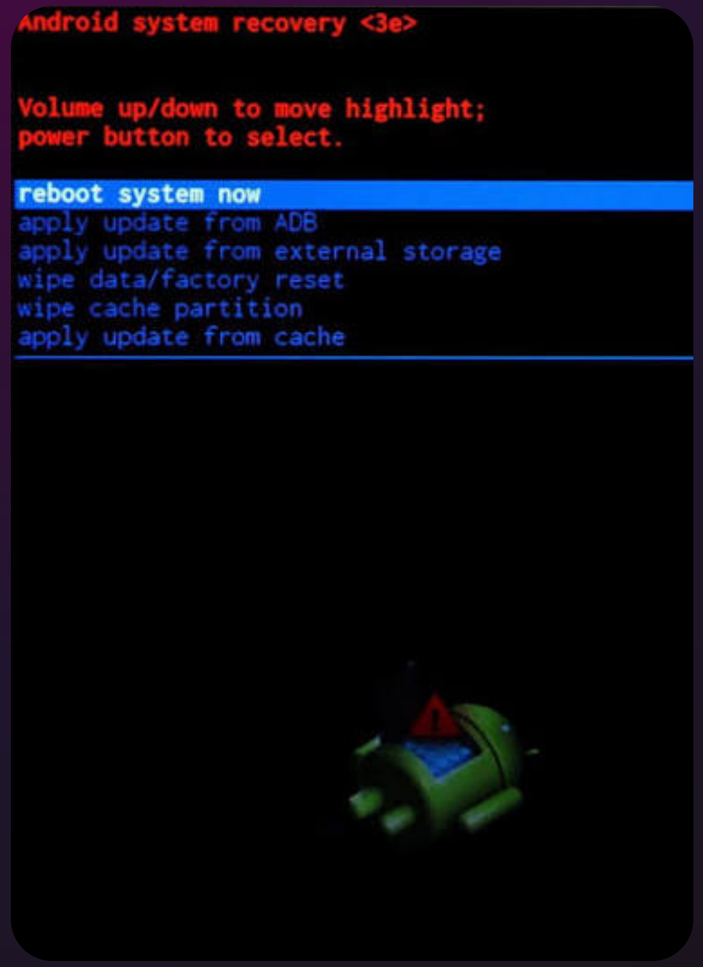
갤럭시 그랜드

/../locksettings.db **(salt 값)**

password.key **(sha-1 값)**

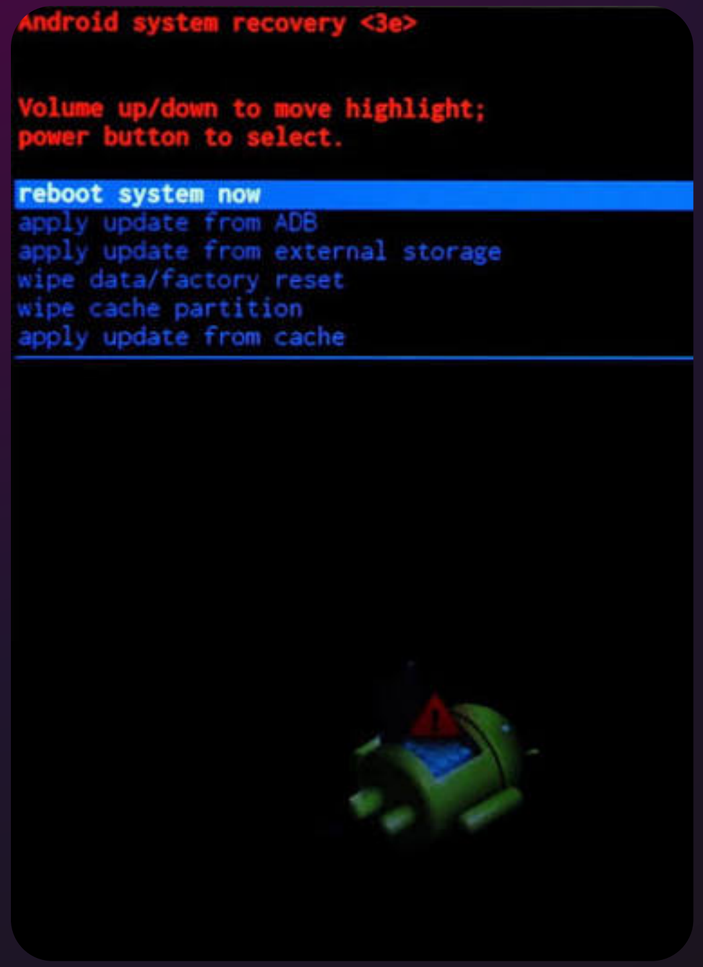
두 값으로 원본 비밀번호 크랙 가능

리커버리 모드



리커버리모드

원래는 초기화, 시스템 복구용



리커버리모드 (부팅이전)

일반사용자 < 리커버리 권한

안드로이드 **루팅**해서 **서버 만들기** - 루팅해서 비밀번호 크랙하기



리커버리모드

바꿀 수 있음!

Custom Recovery

Custom Recovery

(말그대로 커스텀 리커버리라는 뜻)

Custom Recovery

(말그대로 커스텀 리커버리라는 뜻)

순정 리커버리보다 기능 다양,
root 권한 파일 접근 가능

Custom Recovery

(말그대로 커스텀 리커버리라는 뜻)



TWRP 리커버리



CWM 리커버리

Custom Recovery
(말그대로 커스텀 리커버리라는 뜻)

편의를 위해
리커버리 내장 루팅툴 사용



TWRP 리커버리

CWM 리커버리

ADB
(Android Debug Bridge)

=디버깅하려고 쓰는 거

ADB
(Android Debug Bridge)

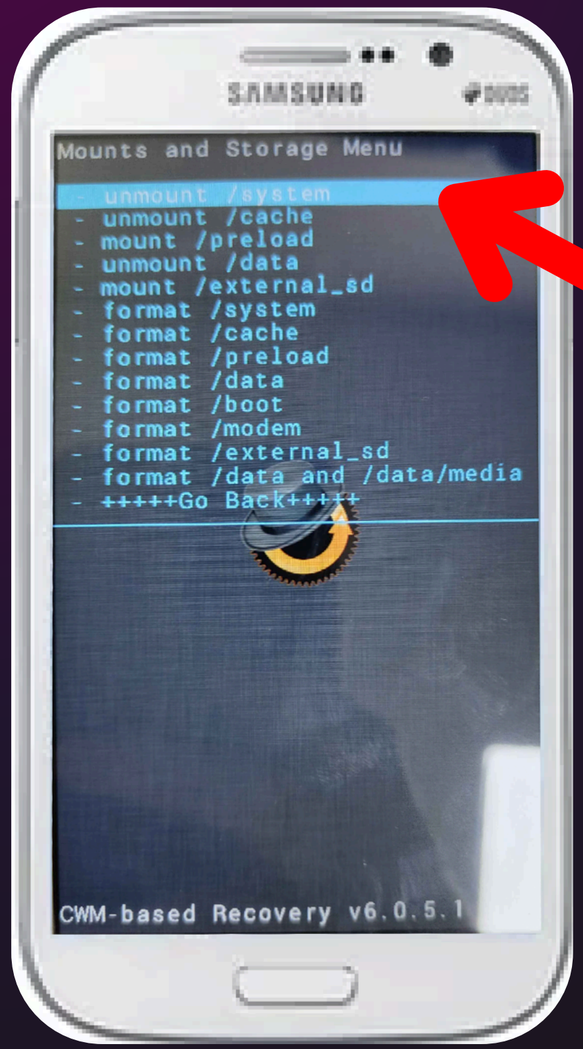
adb shell : 안드로이드 기기 CLI 로 쓰기

adb push/pull : 안드로이드 기기 파일 옮기기

.

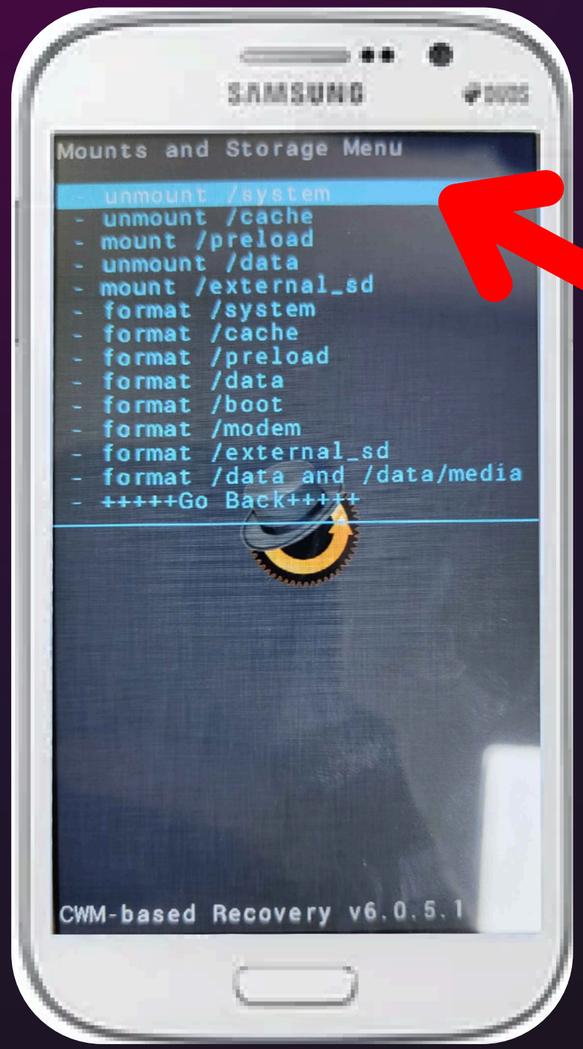
.

안드로이드 **루팅**해서 **서버 만들기** - 루팅해서 비밀번호 크랙하기



/system , /data 마운트

안드로이드 루팅해서 서버 만들기 - 루팅해서 비밀번호 크랙하기



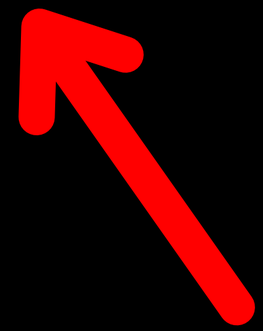
locksettings.db (salt 값)
password.key (sha-1 값)

/system , /data
마운트

Adb pull /data/system

F:\down\platform-tools\system>cat password.key

1DE2EE8A0D46E0C5B658FCC781A3091EB643D992



sha-1 해시

안드로이드 루팅해서 서버 만들기 - 루팅해서 비밀번호 크랙하기

```
F:\down\platform-tools\system>sqlite3.exe locksettings.db

sqlite> select * from locksettings;

1|lockscreen.disabled|0|0
.
.
5|migrated_user_specific|0|true
6|lockscreen.password_salt|0|-3049710941163274 4
.
.
20|lockscreen.password_type|0|131072
```

솔트값

안드로이드 루팅해서 서버 만들기 - 루팅해서 비밀번호 크랙하기

파이썬 코드

```
import hashlib
import itertools
import time

TARGET = "1DE2EE8A0D46E0C5B658FCC781A3091EB643D992"
SALT = "ff93a70a62d7e998"

def android_old_hash(pin: str) -> str:
    return hashlib.sha1((pin + SALT).encode()).hexdigest().upper()

start = time.time()
count = 0

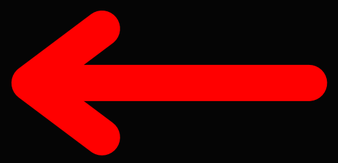
for length in range(4, 9):
    print(f"[*] trying {length}-digit PIN")

    for nums in itertools.product("0123456789", repeat=length):
        pin = "".join(nums)
        count += 1

        if android_old_hash(pin) == TARGET:
            print(f"[+] FOUND: {pin}")
            print(f"[*] checked: {count}")
            print(f"[*] elapsed: {time.time() - start:.2f}s")
            exit()

        if count % 100000 == 0:
            elapsed = time.time() - start
            print(f"[*] checked={count}, speed={count / elapsed:.0f}/s")

print("not found")
```



써보실 분들은
복사해서 써보시고요

안드로이드 루팅해서 서버 만들기 - 루팅해서 비밀번호 크랙하기

```
import hashlib
import itertools
import time

TARGET = "1DE2EE8A0D46E0C5B658FCC781A3091EB643D992"
SALT = "ff93a70a62d7e998"

def android_old_hash(pin: str) -> str:
    return hashlib.sha1((pin + SALT).encode()).hexdigest().upper()

start = time.time()
count = 0

for length in range(4, 9):
    print(f"[*] trying length {length}")

    for nums in itertools.product("123456789", repeat=length):
        pin = "".join(nums)
        count += 1

        if android_old_hash(pin) == TARGET:
            print(f"[+] FOUND: {pin}")
            print(f"[*] checked: {count}")
            print(f"[*] elapsed: {time.time() - start:.2f}s")
            exit()

        if count % 100000 == 0:
            elapsed = time.time() - start
            print(f"[*] checked={count}, speed={count / elapsed:.0f}/s")

print("not found")
```

결과 : 123




```
Administrator\AppData\Loc
latform-tools/exploit.py
-digit PIN
234
  1235
  0.00s
```

해서 써보시고요

예전 기기들 :

예전 기기들 : 취약함

요즘 기기들 : **OEM Lock등**

커스텀 리커버리를 그냥은 **설치하지 못함**

요즘은 얻는것 <<<< 잃는것

ex. 삼성페이, 서비스센터

루팅은 적절하게해야함

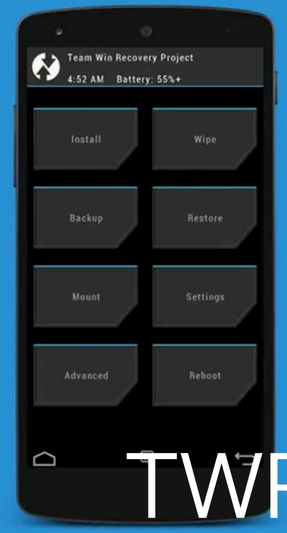
→ 이 프로젝트는 특수한 경우임

ex. 삼성페이, 저비즈센터

제 2-1장

PostmarketOS 설치

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



TeamWin

TWRP Recovery

TWRP 리커버리

THEANDROIDSOUL

postmarketOS

포스트마켓 OS

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



알파인 리눅스 for 스마트폰

postmarketOS

포스트마켓 OS

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



TWRP 리커버리



포스트마켓 OS

자원 낭비 최소화 + 24시간 운영

이 부분에서 **3-4 일** 소요

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



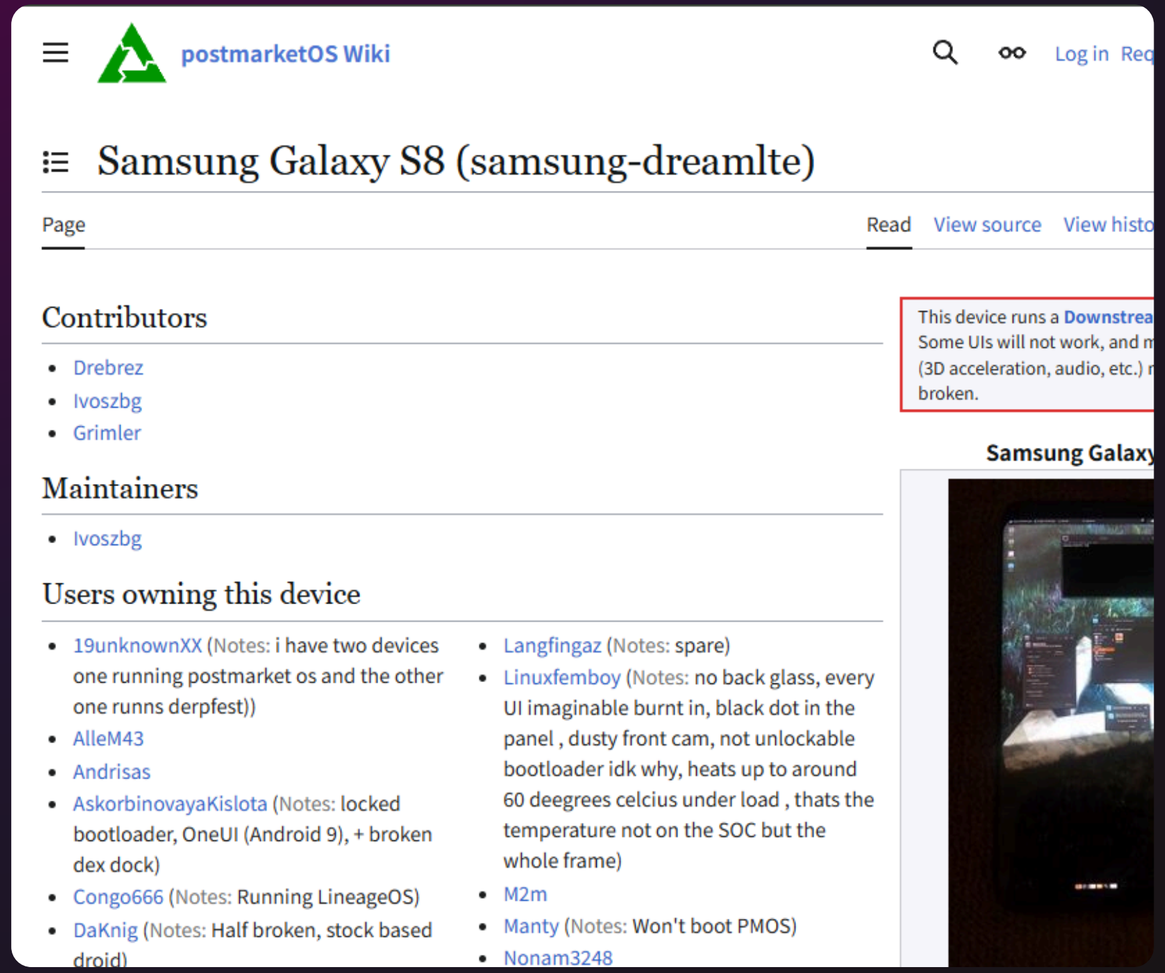
구글에도 자료가 거의X

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



가장 먼저 커스텀 리커버리 설치

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



하위기종인 S8 자료 탐색

상위호환

기대하며 **부팅 이미지 제작**

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



결과?

대 실패...

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



결과?

삼성로고 멈춤

내 실패...

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



결과?

내 실패...

삼성로고 멈춤

OS 실행시 생성되는 로그 X

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



결과?

= 리눅스 진입도 못했다

삼성 로고 멈춤

OS 실행시 생성되는 로그 X

갤럭시 부팅과정

S-Boot → boot.img → kernel/initramfs → rootfs

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. kernel/initramfs
4. rootfs

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. kernel/initramfs
4. rootfs

순정 부트로더

ex. GRUB

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. kernel/initramfs
4. rootfs

순정 부트로더

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. kernel/initramfs
4. rootfs

순정 부트로더

boot.img

갤럭시 부팅과정

1. S-Boot
2. **boot.img**
3. kernel/initramfs
4. rootfs

커널/initramfs
들어있는 img 파일

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. **kernel/initramfs**
4. rootfs

커널 다들 알고 계시니까 skip

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. **kernel/initramfs**
4. rootfs

initramfs?

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. **kernel/initramfs**
4. rootfs

= initial ram file system

initramfs?

rootfs 마운트

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. **kernel/initramfs**
4. rootfs

= initial ram file system

" / "디렉터리 마운트

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. **kernel/initramfs**
4. rootfs

initramfs?

=임시 OS
for rootfs

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. kernel/initramfs
4. **rootfs**

rootfs

갤럭시 부팅과정

1. S-Boot
2. boot.img
3. kernel/initramfs
4. **rootfs**

= root file system

= 실제 사용 OS

그래서 찾아낸 문제점

순정 부트로더 : android 전용

포스트마켓 OS(알파인 리눅스)는 일반 리눅스 형태...

부트로더 처음부터 만들기???

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치

README GPL-2.0 license

uniLoader

uniLoader is a minimalistic loader, capable of booting Linux kernels. It can be used as an intermediate bootloader, providing a clean booting environment in case of a forced and buggy bootloader.

uniLoader : 폰 전용 리눅스 부트로더

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치

README GPL-2.0 license

uniLoader

uniLoader is a minimalistic loader, capable of booting Linux kernels. It can be used as an intermediate bootloader, providing a clean booting environment in case of a forced and buggy bootloader.

S8은 있는데 S8+ 부트로더가 없음 🤯

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치

README GPL-2.0 license

uniLoader

둘 다 **Exynos8895** 기반,
다만 **메모리, 낸드의 종류**가 달라 boot.img 에 로딩된 kernel, initramfs 의 위치가 다를 수 있음

S8은 있는데 S8+ 부트로더가 없음 🤯

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치

README GPL-2.0 license

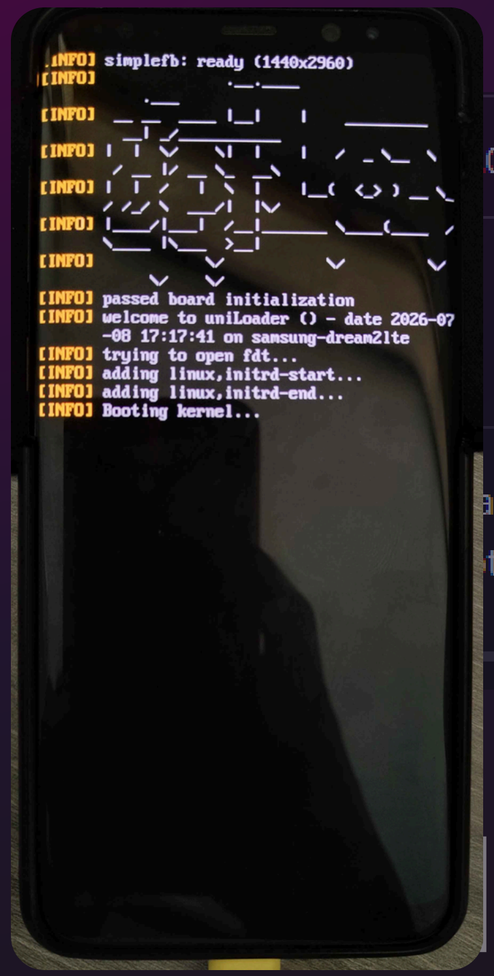
uniLoader

uniLoader is a minimalistic loader, capable of booting Linux kernels. It can be used as a.
providing a clean booting environment in case of a forced and buggy bootloader.



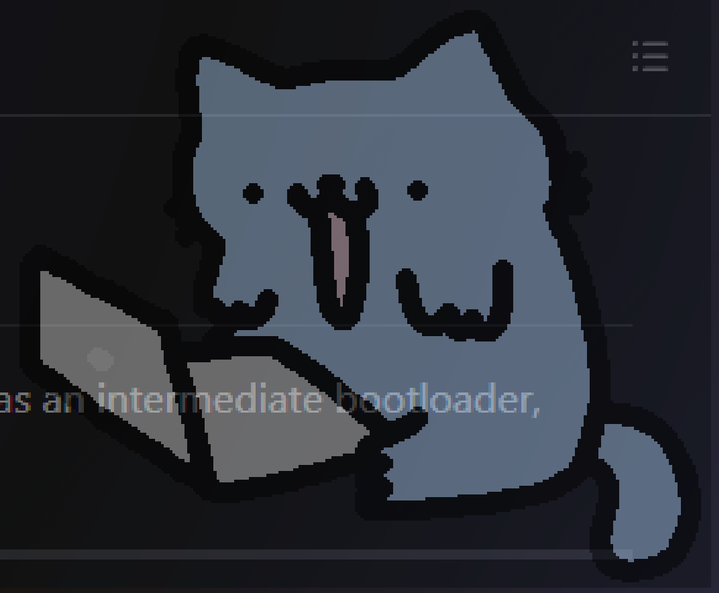
부트로더부터 **포팅(기기 맞춤화)** 해야함 😇

안드로이드 루팅해서 **서버 만들기** - PostmarketOS 설치



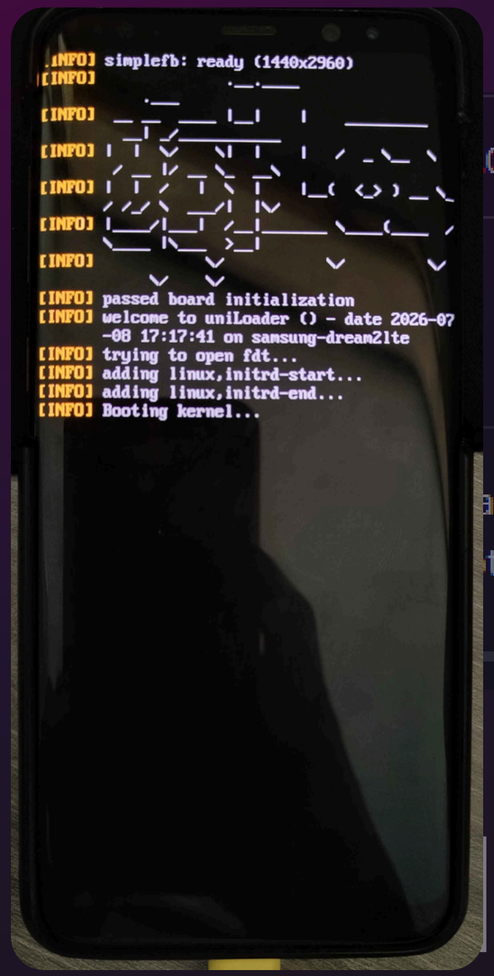
0 license

alistic loader, capable of booting Linux kernels. It can be used as an intermediate bootloader,
ting environment in case of a forced and buggy bootloader.



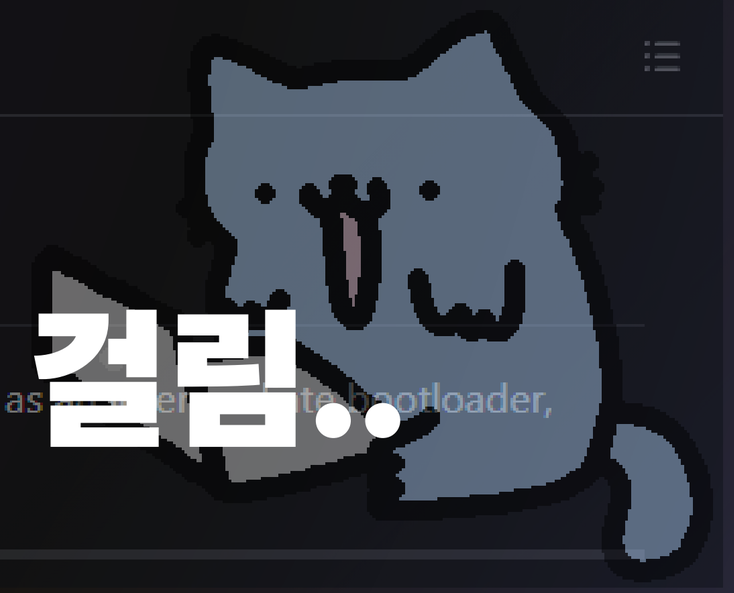
부터 **포팅(기기 맞춤화)** 해야함 😇

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



0 license

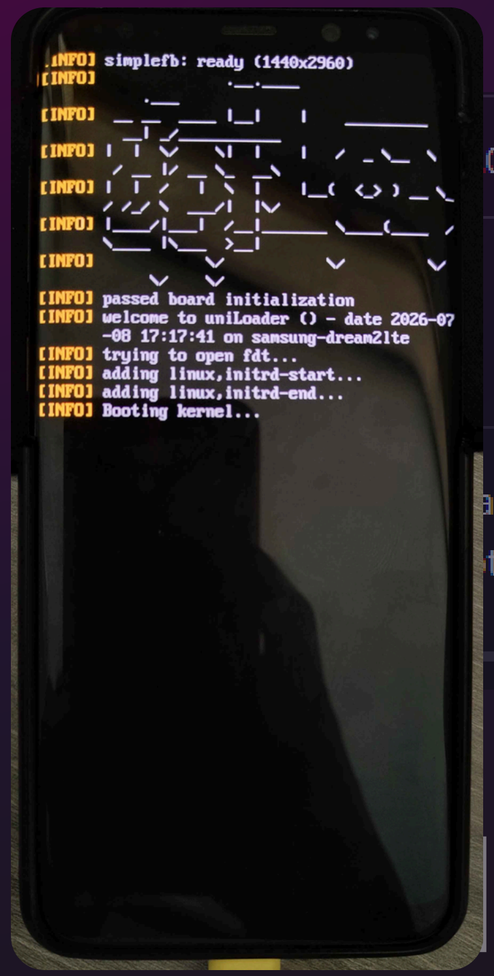
alistic loader, capab f k nels. It can be sed as
ting environment in case of a forced and buggy bootloader.



10시간 정도 걸림..

부터 **포팅(기기 맞춤화)** 해야함 😇

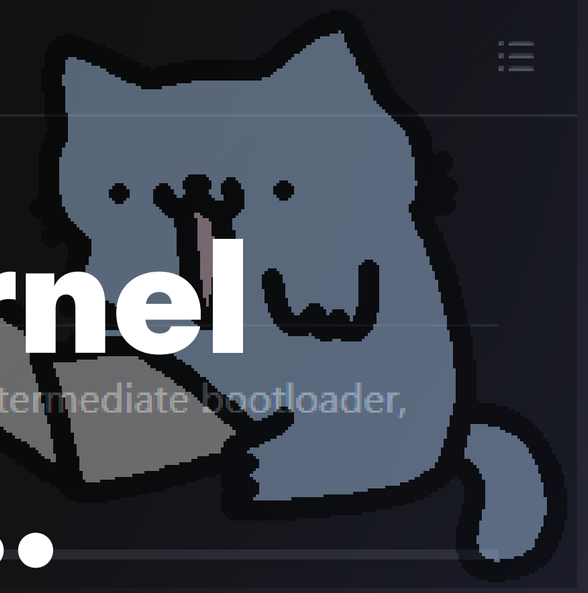
안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



0 license

listic loader, capable of booting Linux kernels. It can be used as an intermediate bootloader,

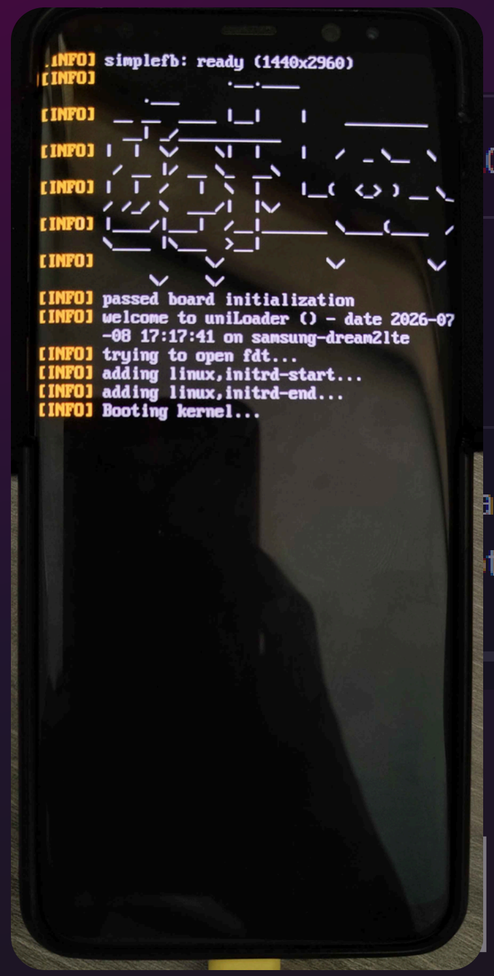
ting environment in case of a fo



Booting Kernel 에서 멈춤...

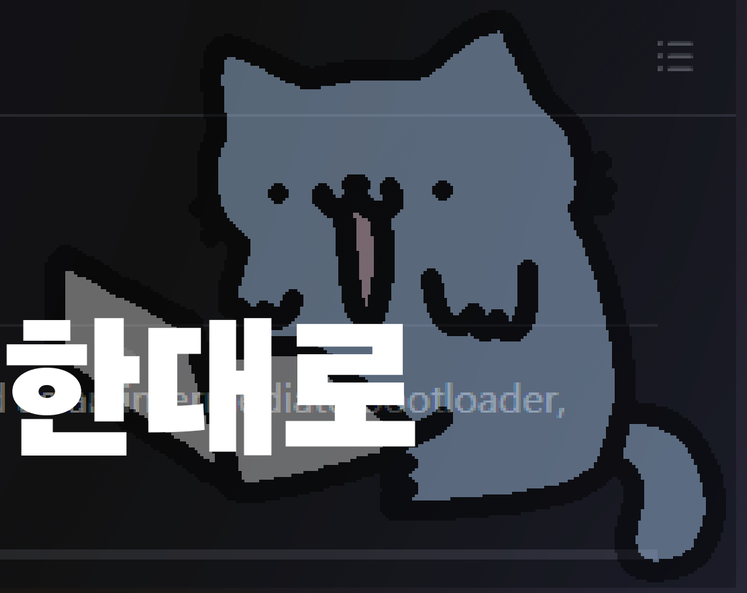
부터 **포팅(기기 맞춤화)** 해야함 😇

안드로이드 루팅해서 **서버 만들기** - PostmarketOS 설치



0 license

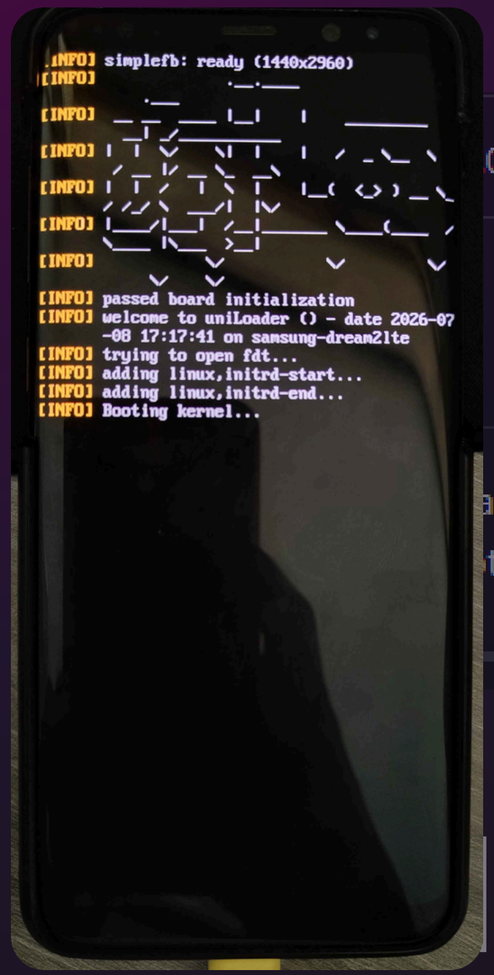
alistic loader, capable of boo
ting environment in case of a forced and buggy bootloader.



= 앞서 우려한대로

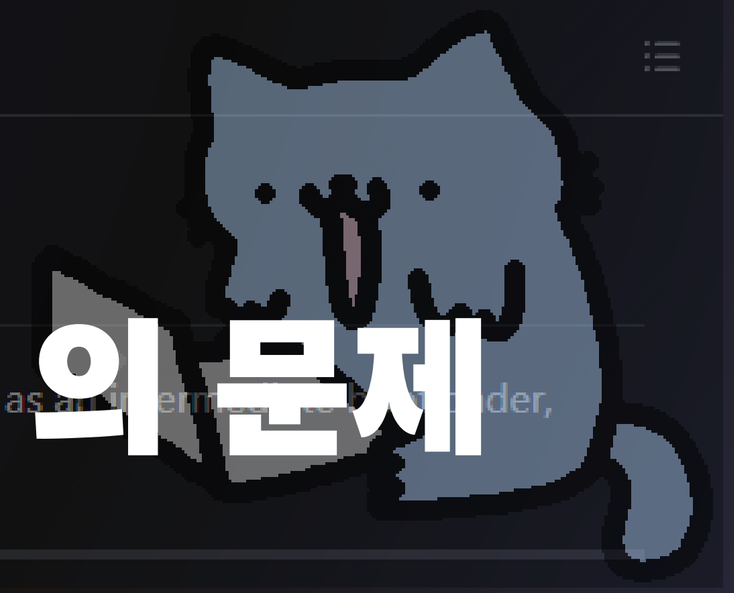
부터 **포팅(기기 맞춤화)** 해야함 😇

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



0 license

alistic loader, ca e o ernels t as a ader,
ting environment in case of a forced and buggy bootloa

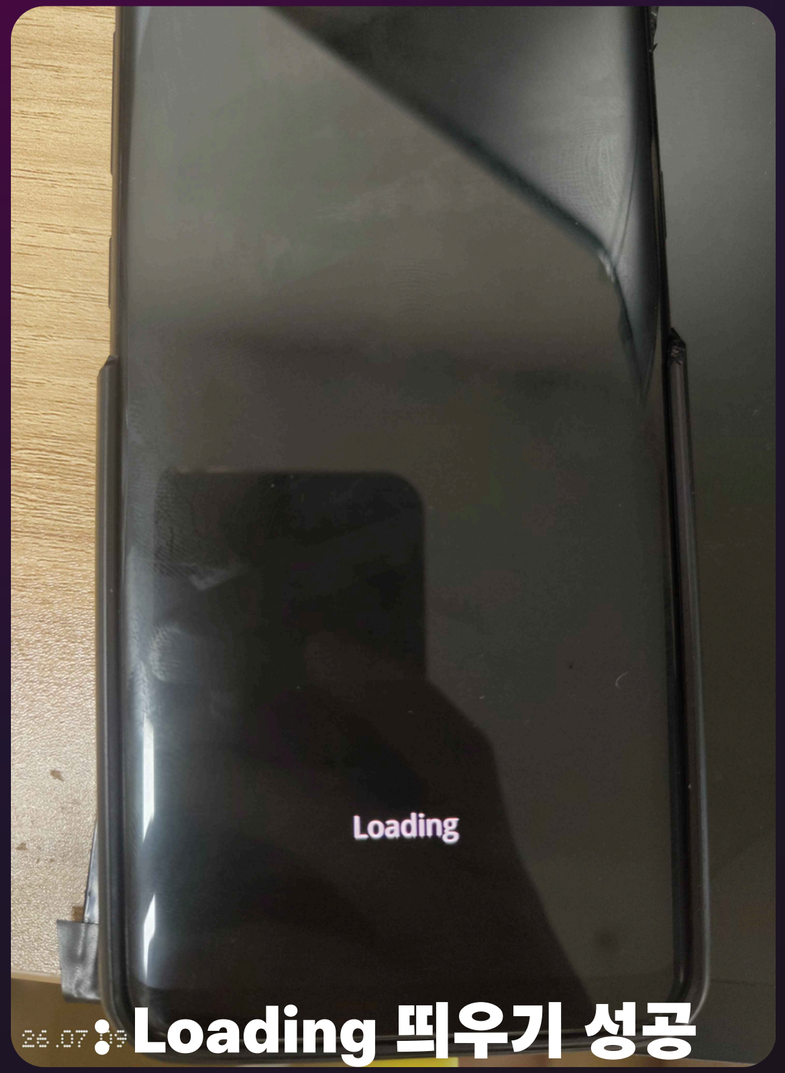


= boot.img 의 문제

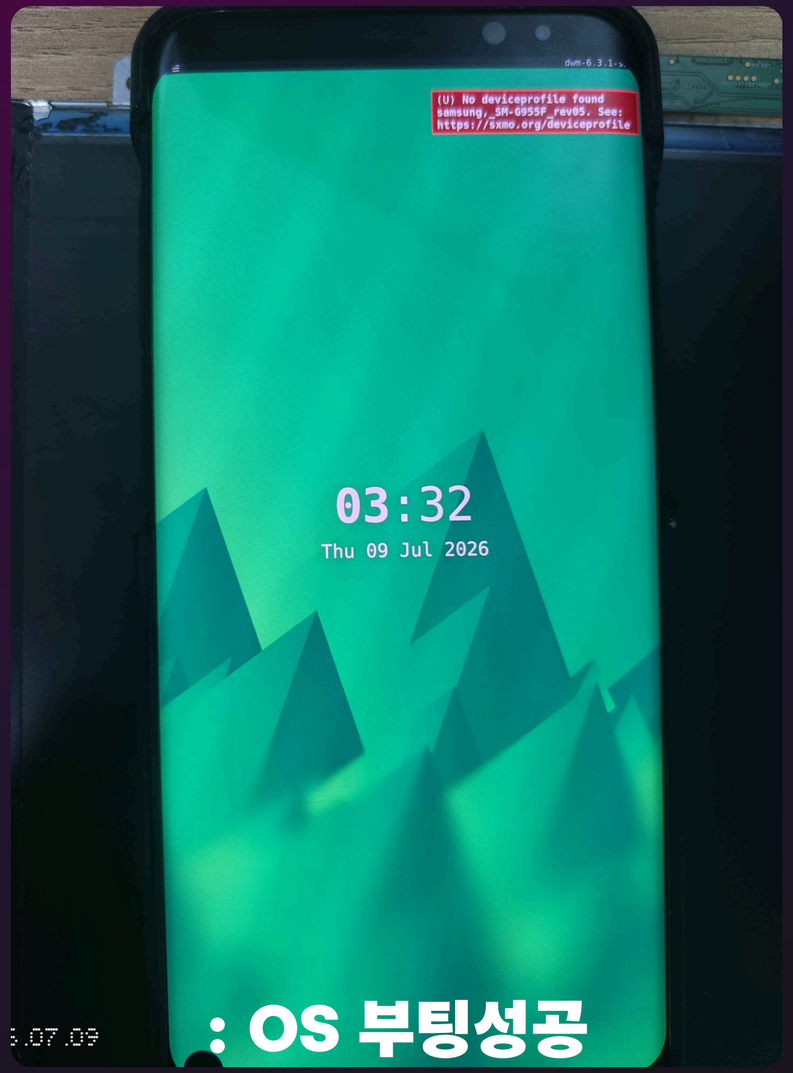
부터 **포팅(기기 맞춤화)** 해야함 😇

Codex 와 Boot.img 수정
17시간 즈음...

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



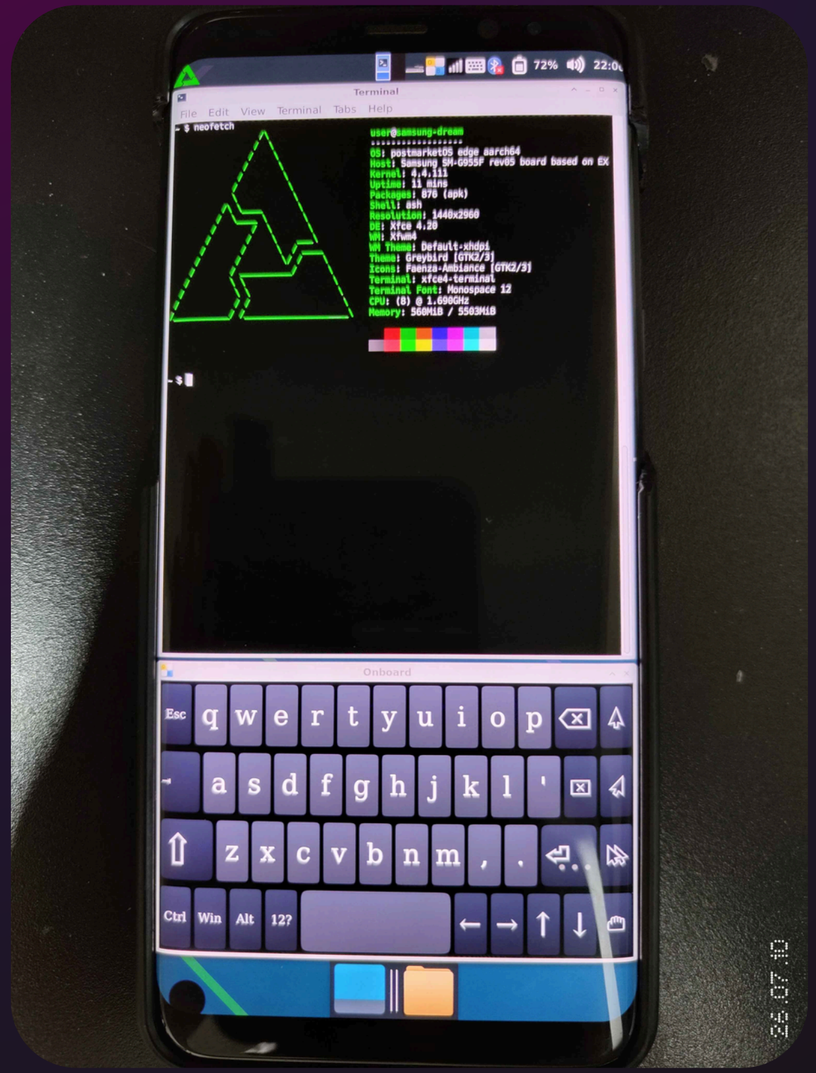
안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



: OS 부팅성공

추가 설정
이후..

안드로이드 루팅해서 서버 만들기 - PostmarketOS 설치



시스템 정보 잘 잡힘

환경구성 완료

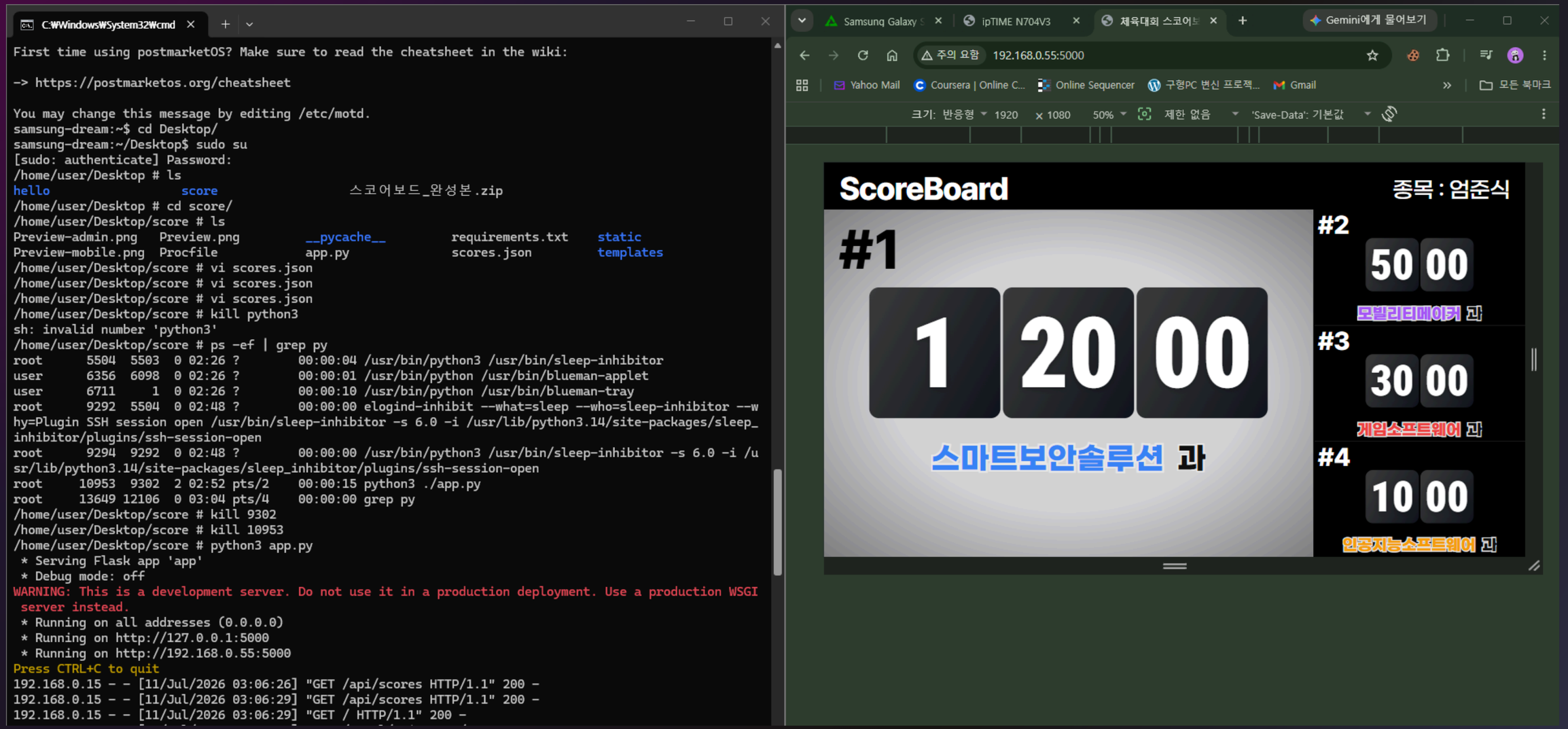
→ 본격적인 웹 서버 세팅

제 2-2장

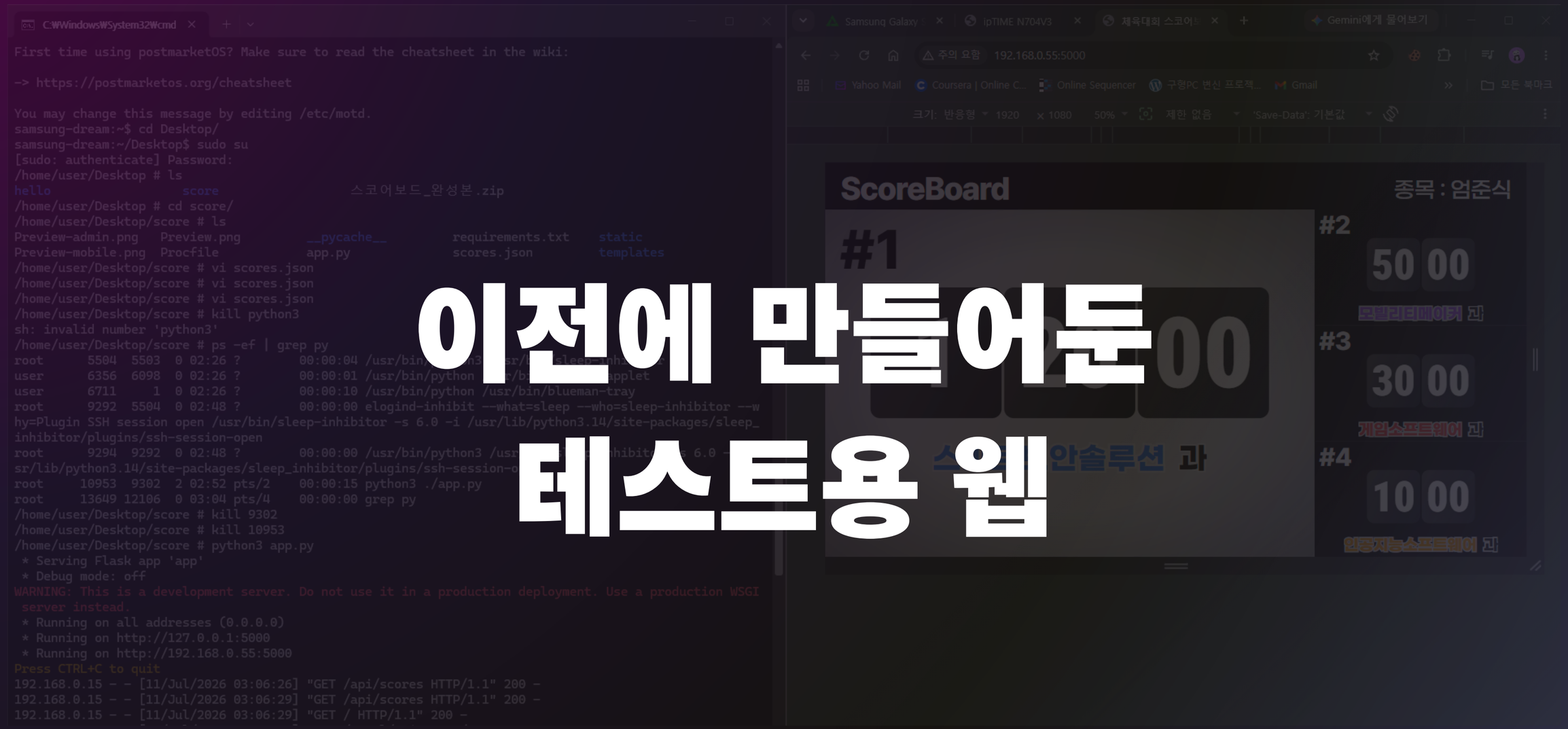
나만의 구글드라이브

테스트

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



이전에 만들어둔 테스트용 웹

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브

C:₩Windows₩System32₩cmd

```
First time using postmarketOS? Make sure to read the cheatsheet in the wiki:

-> https://postmarketos.org/cheatsheet

You may change this message by editing /etc/motd.
samsung-dream:~$ cd Desktop/
samsung-dream:~/Desktop$ sudo su
[sudo: authenticate] Password:
/home/user/Desktop # ls
hello                   score                   스코어보드_완성본.zip
/home/user/Desktop # cd score/
/home/user/Desktop/score # ls
Preview-admin.png   Preview.png         __pycache__         requirements.txt    static
Preview-mobile.png  Procfile            app.py              scores.json         templates
/home/user/Desktop/score # vi scores.json
/home/user/Desktop/score # vi scores.json
/home/user/Desktop/score # vi scores.json
/home/user/Desktop/score # kill python3
sh: invalid number 'python3'
/home/user/Desktop/score # ps -ef | grep py
root      5504  5503  0 02:26 ?        00:00:04 /usr/bin/python3 /usr/bin/sleep
user      6356  6098  0 02:26 ?        00:00:01 /usr/bin/python /usr/bin/blueman
user      6711     1  0 02:26 ?        00:00:10 /usr/bin/python /usr/bin/blueman-tray
root      9292  5504  0 02:48 ?        00:00:00 elogind-inhibit --what=sleep --who=sleep-inhibitor --w
hy=Plugin SSH session open /usr/bin/sleep-inhibitor -s 6.0 -i /usr/lib/python3.14/site-packages/sleep_
inhibitor/plugins/ssh-session-open
root      9294  9292  0 02:48 ?        00:00:00 /usr/bin/python3 /usr/bin/sleep-inhibitor -s 6.0 -i /u
sr/lib/python3.14/site-packages/sleep_inhibitor/plugins/ssh-session-open
root     10953  9302  2 02:52 pts/2    00:00:15 python3 ./app.py
root     13649 12106  0 03:04 pts/4    00:00:00 grep py
/home/user/Desktop/score # kill 9302
/home/user/Desktop/score # kill 10953
/home/user/Desktop/score # python3 app.py
 * Serving Flask app 'app'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI
 server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.0.55:5000
Press CTRL+C to quit
192.168.0.15 - - [11/Jul/2026 03:06:26] "GET /api/scores HTTP/1.1" 200 -
192.168.0.15 - - [11/Jul/2026 03:06:29] "GET /api/scores HTTP/1.1" 200 -
192.168.0.15 - - [11/Jul/2026 03:06:29] "GET / HTTP/1.1" 200 -
```

Samsung Galaxy | ipTIME N704V3 | 체육대회 스코어보 | Gemini에게 물어보기

주의 요함 192.168.0.55:5000

Yahoo Mail | Coursera | Online C... | Online Sequencer | 구형PC 변신 프로젝... | Gmail | 모든 북마크

크기: 반응형 1920 × 1080 50% 제한 없음 'Save-Data': 기본값

ScoreBoard

종목 : 엄준식

#1

20 00

스마트보안솔루션 과

#2

50 00

모빌리티메이커 과

#3

30 00

정상작동

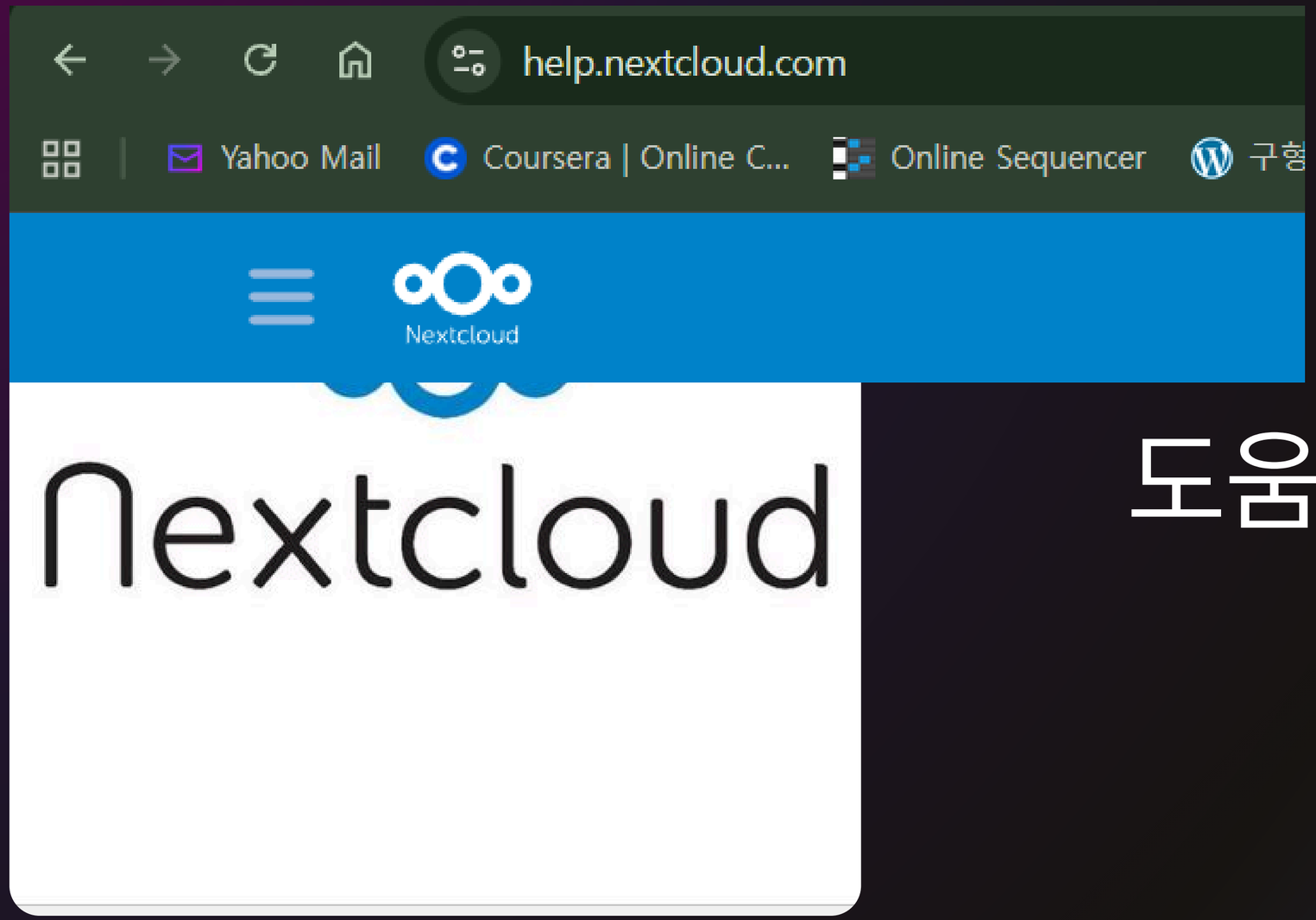


안드로이드 루팅해서 **서버 만들기** - 나만의 구글드라이브



구글 드라이브 대용 UI

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



도움말을 참고함

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브

ash

SSH 로 접속

ash

구성요소 설치

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브

ash

```
sudo apk update
sudo apk add nextcloud33 nextcloud33-mysql nextcloud33-occ nextcloud33-initscript
sudo apk add nginx nginx-openrc
sudo apk add mariadb mariadb-client mariadb-openrc
sudo apk add redis redis-openrc
sudo apk add php85-fpm php85-pecl-apcu php85-pecl-redis php85-exif php85-sodium
sudo apk add openssl curl
```

ash

DB 세팅

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브

ash

```
CREATE DATABASE nextcloud CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY '비밀번호';

GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';

FLUSH PRIVILEGES;

EXIT;
```

ash

ufw 로 방화벽 설정

ash

22번 포트 → 2222

2222 : 192.168.x.x 대역만 허용

443 허용

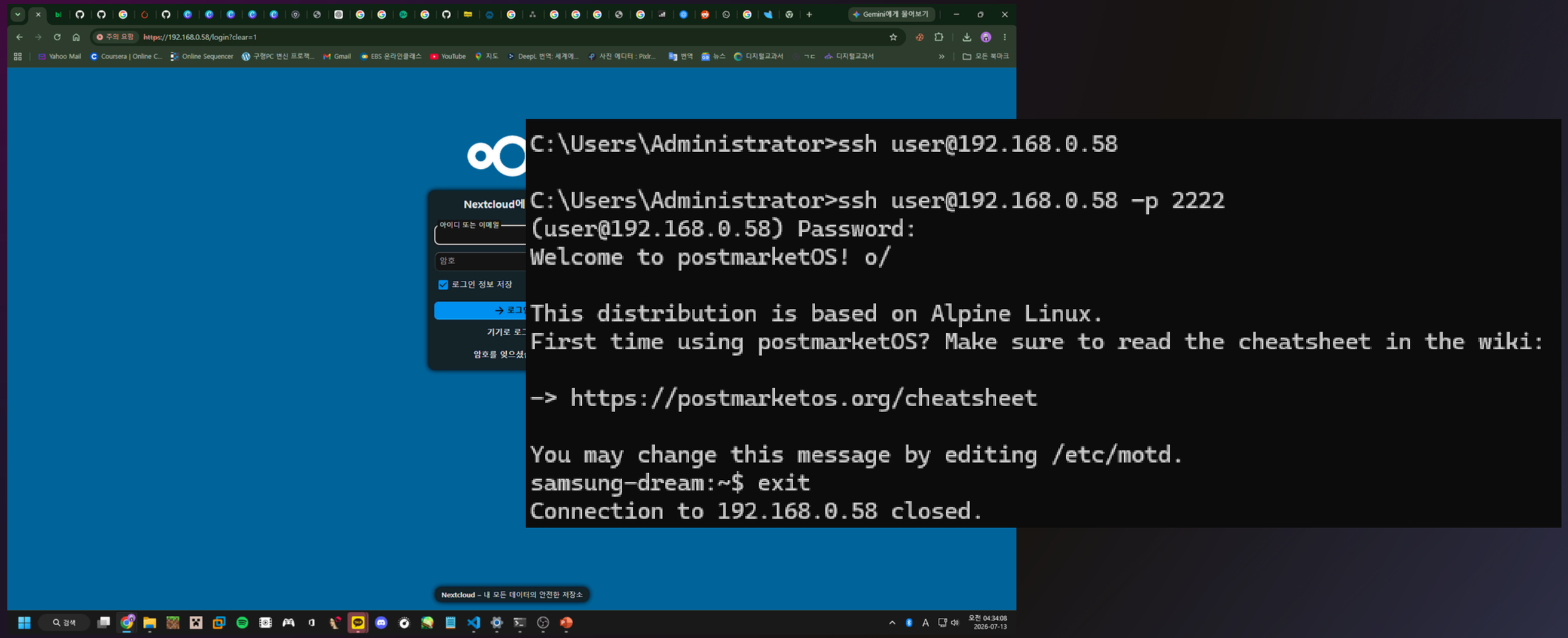
80 허용

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브

ash

```
sudo ufw default deny
sudo ufw allow from 192.168.0.0/16 to any port 2222/tcp
sudo ufw allow 80
sudo ufw allow 443
```

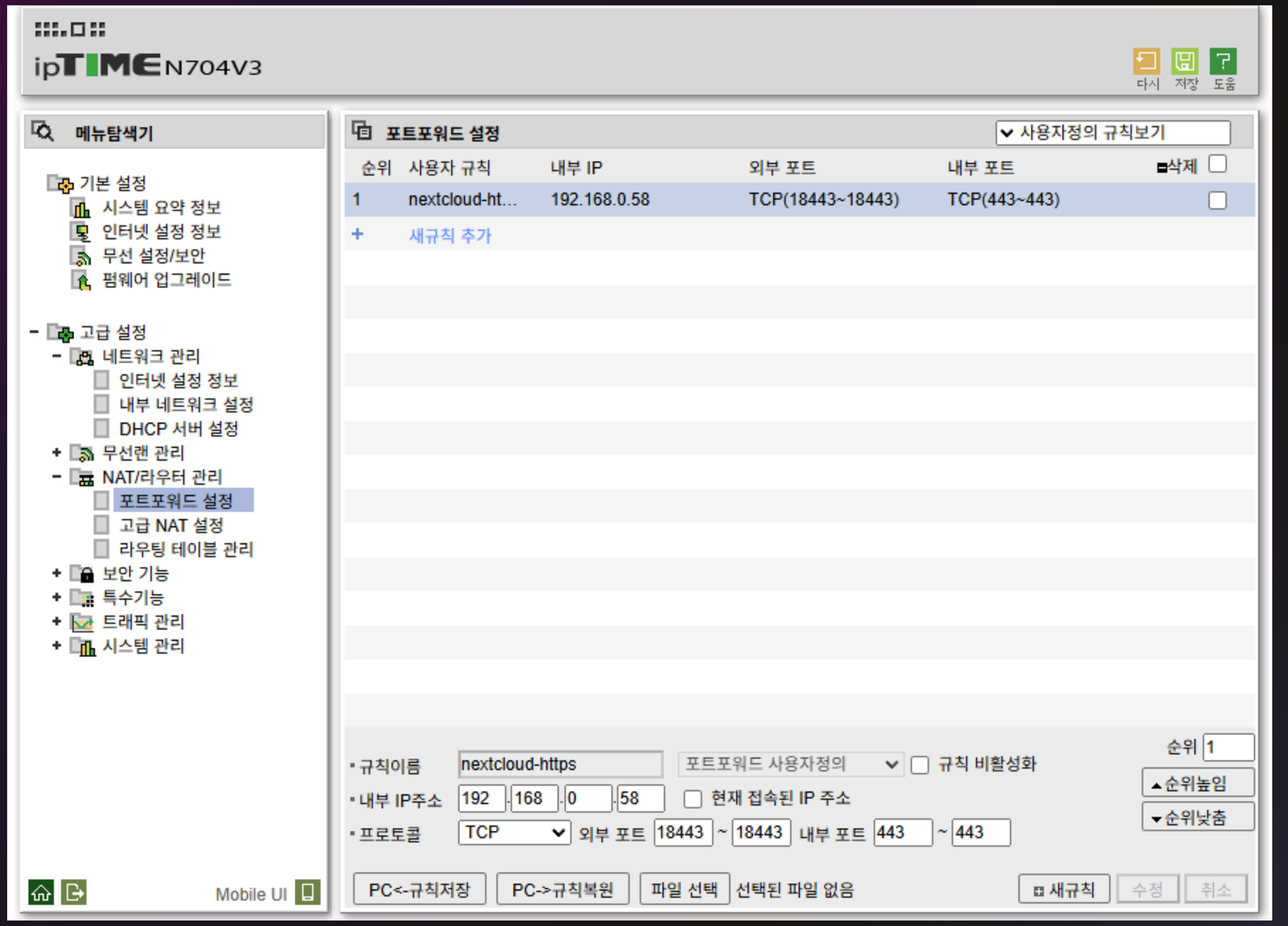
안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



ash

포트포워딩

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



NAT 설정

GAPD-7500 > 네트워크 설정 > NAT 설정

외부에서 내부 네트워크로의 접속이 가능하도록 설정할 수 있습니다.

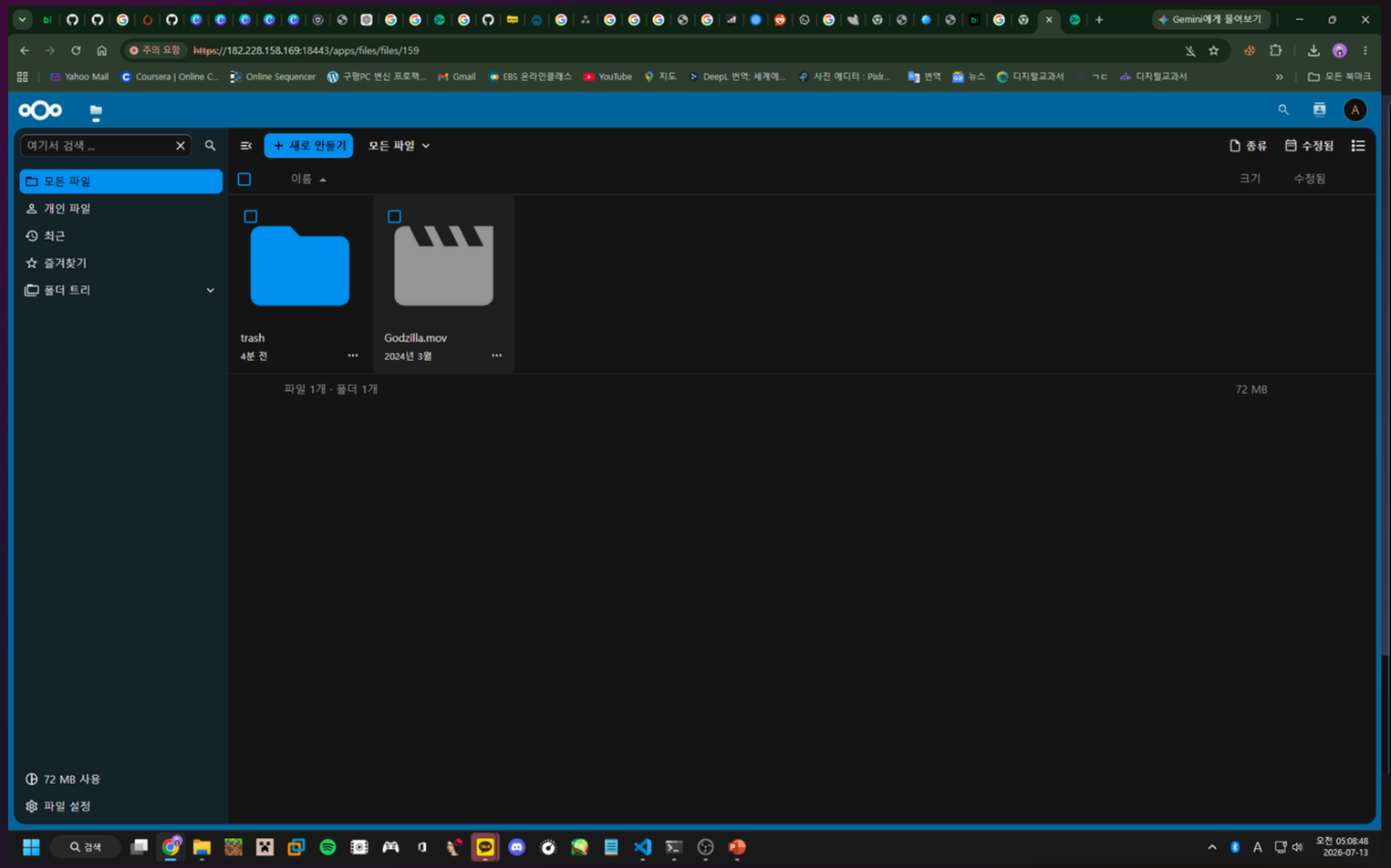
- 설정에 따라 보안상 이슈가 있을 수 있으므로 사용에 주의하세요.
- 최대 32개를 설정할 수 있습니다.

포트포워딩 | DMZ 서버 (포트포워딩) | NAT-T

포트포워딩 설정 [추가]

	No.	ON/OFF	서비스 포트	프로토콜	IP 주소	내부 포트
☐	1	◉ ON ○ OFF	18443~18443	TCP/IP	192.168.219.172	18443

안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브





안드로이드 루팅해서 서버 만들기 - 나만의 구글드라이브



https://massy-ji.p-e.kr:18443

제 3장

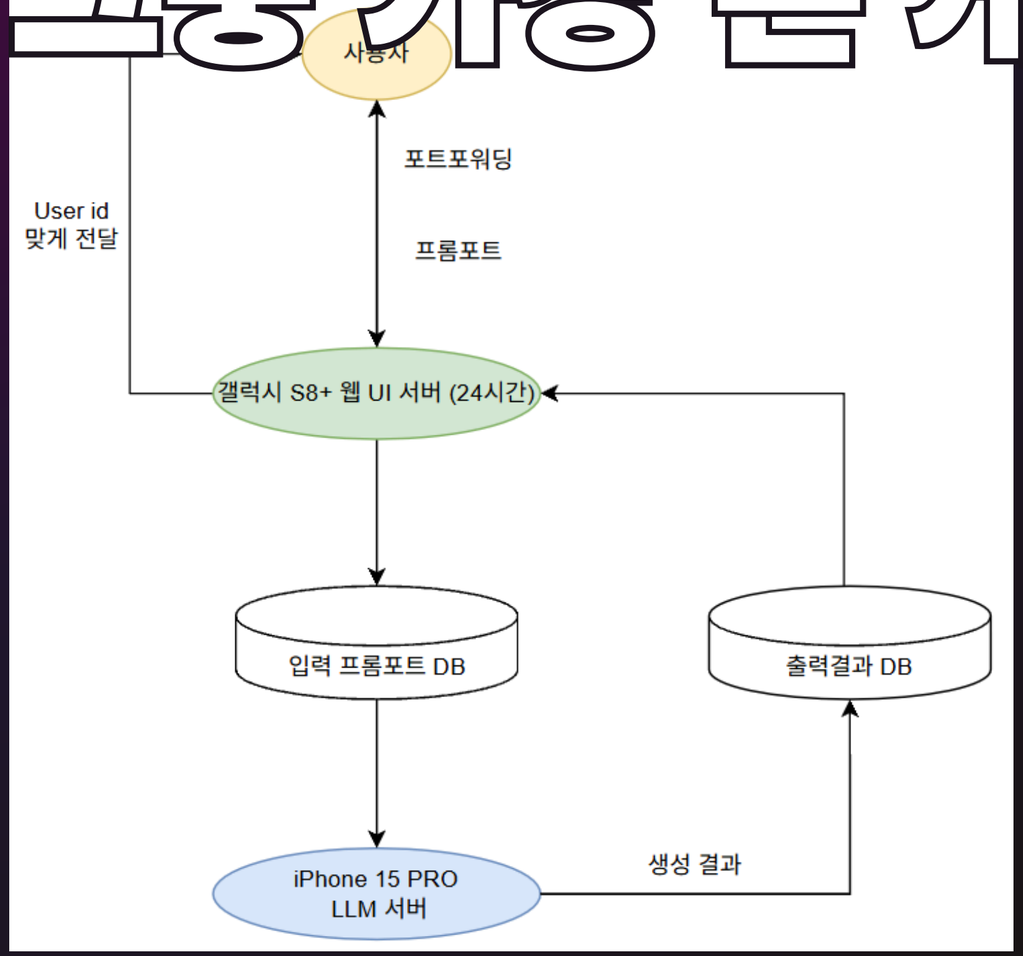
마무리

시간도 부족했고 여러모로 아쉬운게 많음

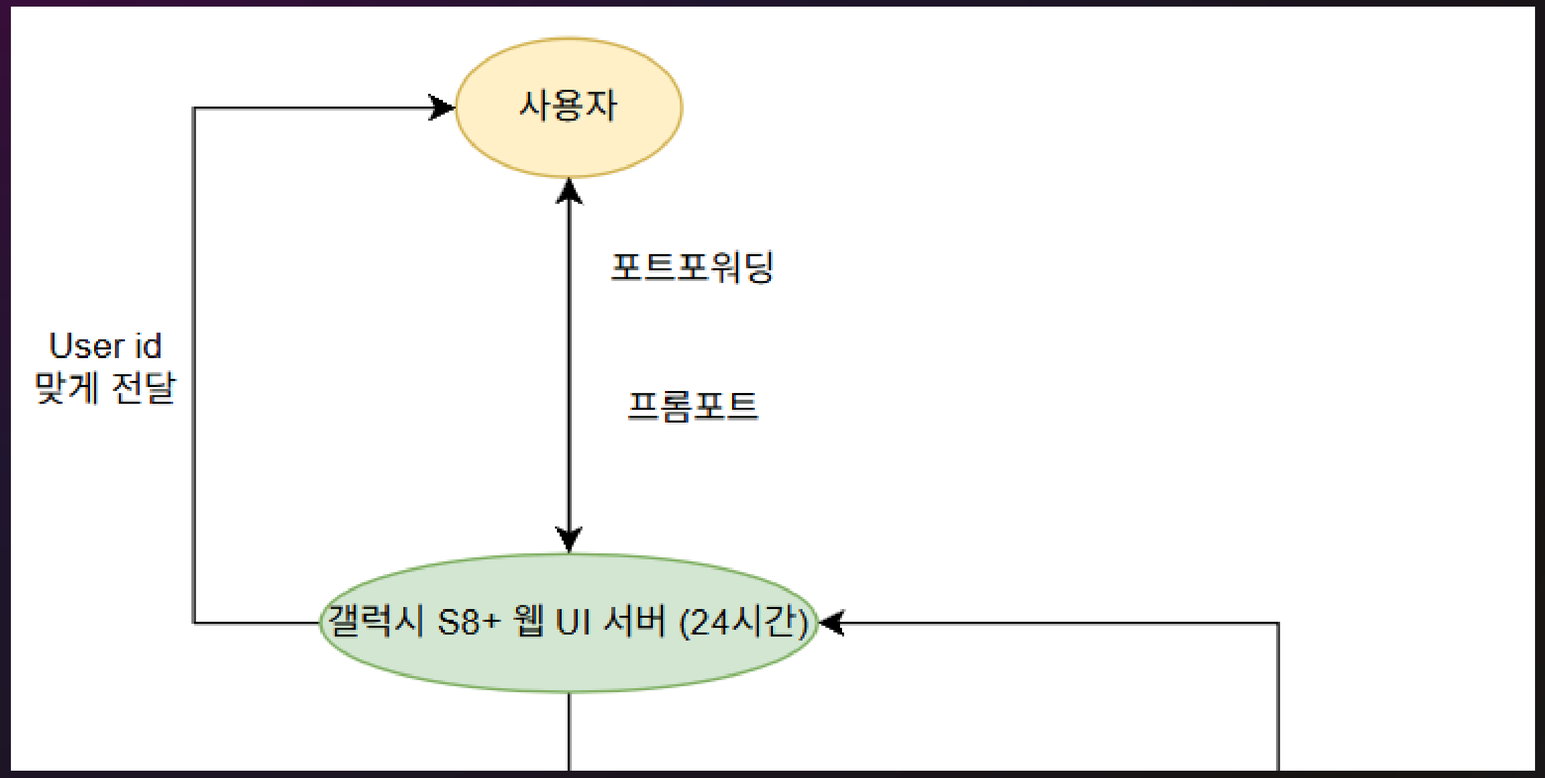
그래도 남아도는 H/W 활용한다는 목표는 달성...

안드로이드 루팅해서 서버 만들기 - 마무리

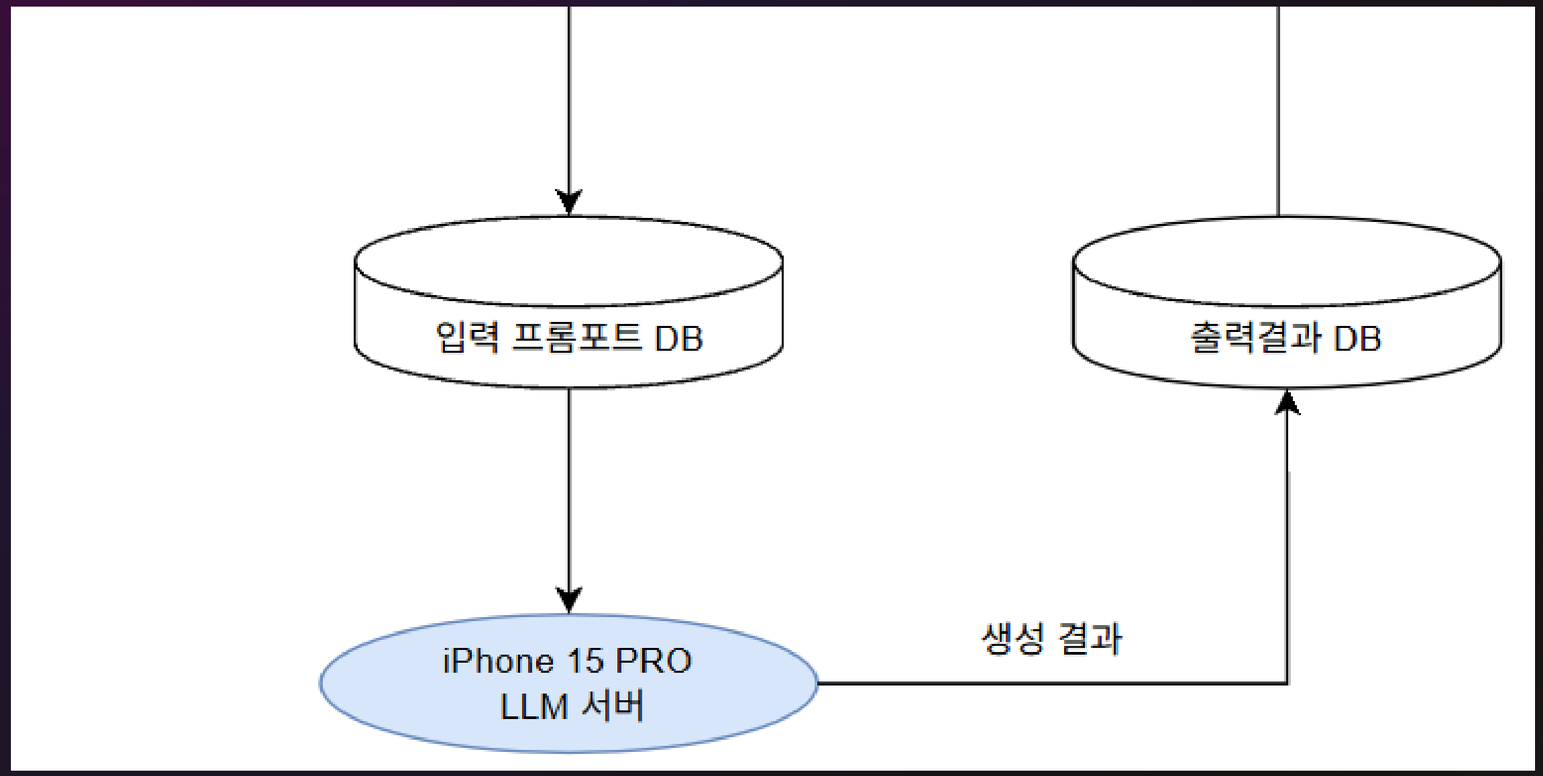
그중 가장 큰게 바로 원래계획



그중 가장 큰 게 바로 원래계획

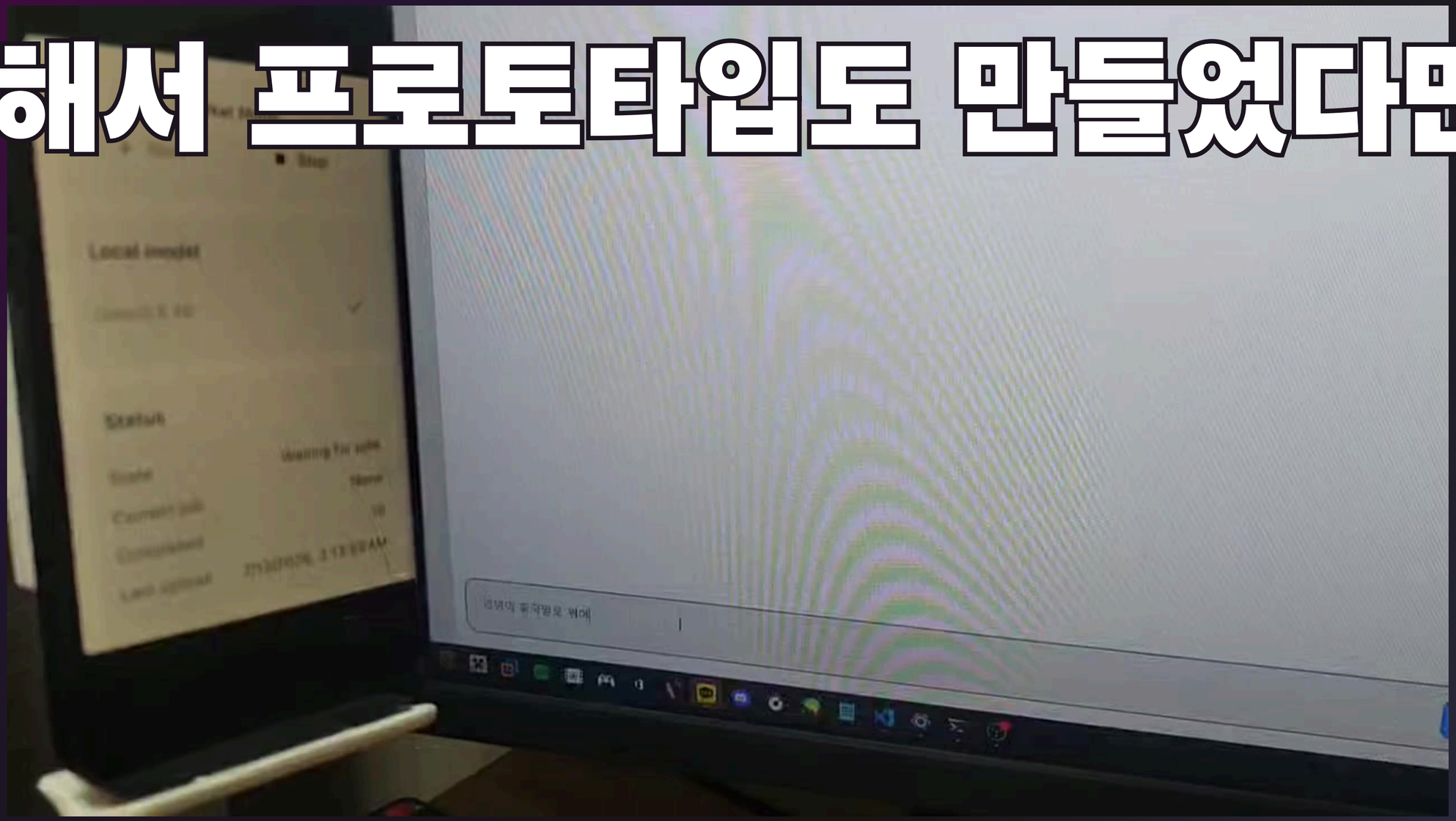


그중 가장 큰 게 바로 원래계획



안드로이드 루팅해서 서버 만들기 - 마무리

..해서 프로토타입도 만들었다만



만들다보니 구조가 너무 복잡해져서 기각

api 직접 불러오는게 안돼서 이렇게 구현

안드로이드 루팅해서 서버 만들기 - 마무리

포트포워딩 된
프론트엔드 채팅창
웹사이트

iPhone



http 로 내부망
데이터 통신용
웹사이트

S8+



안드로이드 루팅해서 서버 만들기 - 마무리

포트포워딩 된
프론트엔드 채팅창
웹사이트

iPhone



3초마다 polling

http 로 내부망
데이터 통신용
웹사이트

S8+



Android, Linux 부팅구조

포트포워딩,
실제 방화벽 구성

여러모로
부족한점을 많이 깨닳음

Q&A

Thank You!!