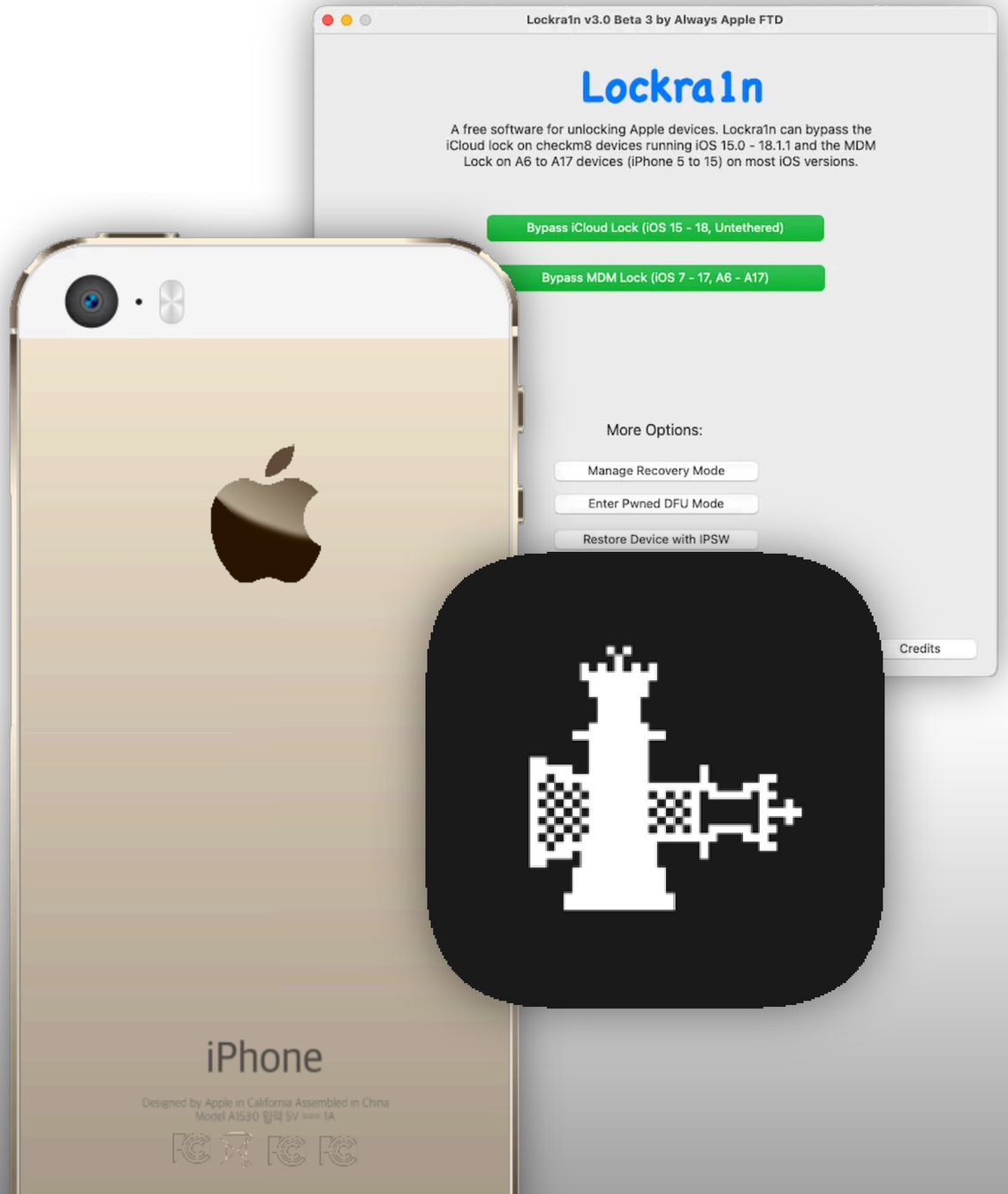



# 구형 아이폰,

# iCloudLock 우회하기.

Checkm8 취약점과 Lockra1n 툴을 이용하여
iPhone의 Activation Lock 우회 해보기

20210지윤찬

# index




1 ---------- 어쩌다가 이 주제를 고르게 되었는가
2 ---------- Apple 인증 동작 원리
3 ---------- 취약점 분석 및 JailBreak
4---------- Lockra1n 및 분석
5 ---------- 마무리

# 어쩌다가 이 주제를 고르게 되었는가...

# 어쩌다 이 주제?



당근

# 어쩌다 이 주제?



당근

iPhone 이나 전자기기
사모으는 **취미**

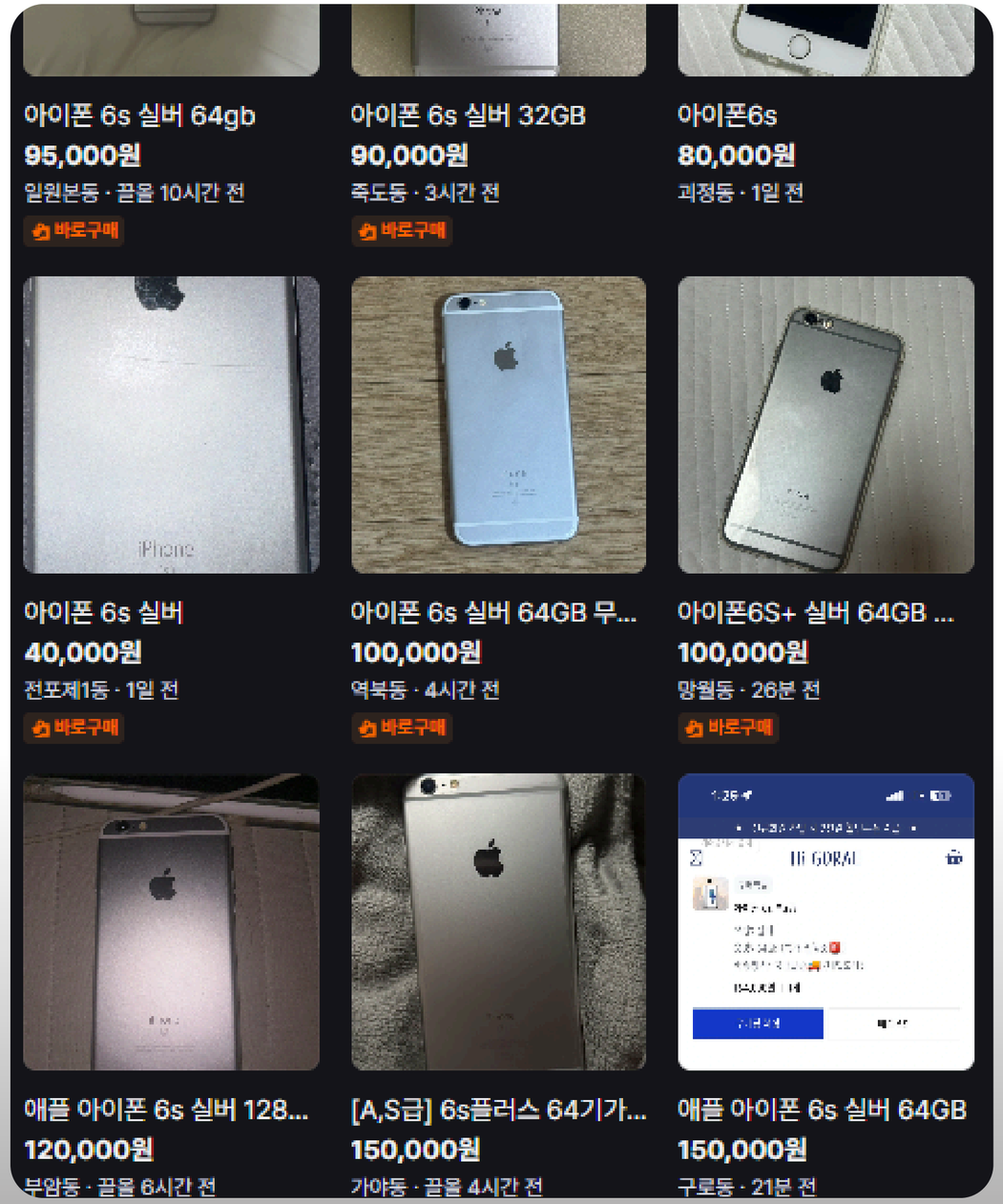
# 어쩌다 이 주제?

당근



학생 → 돈 없음

→ 가능한 **저렴**하게



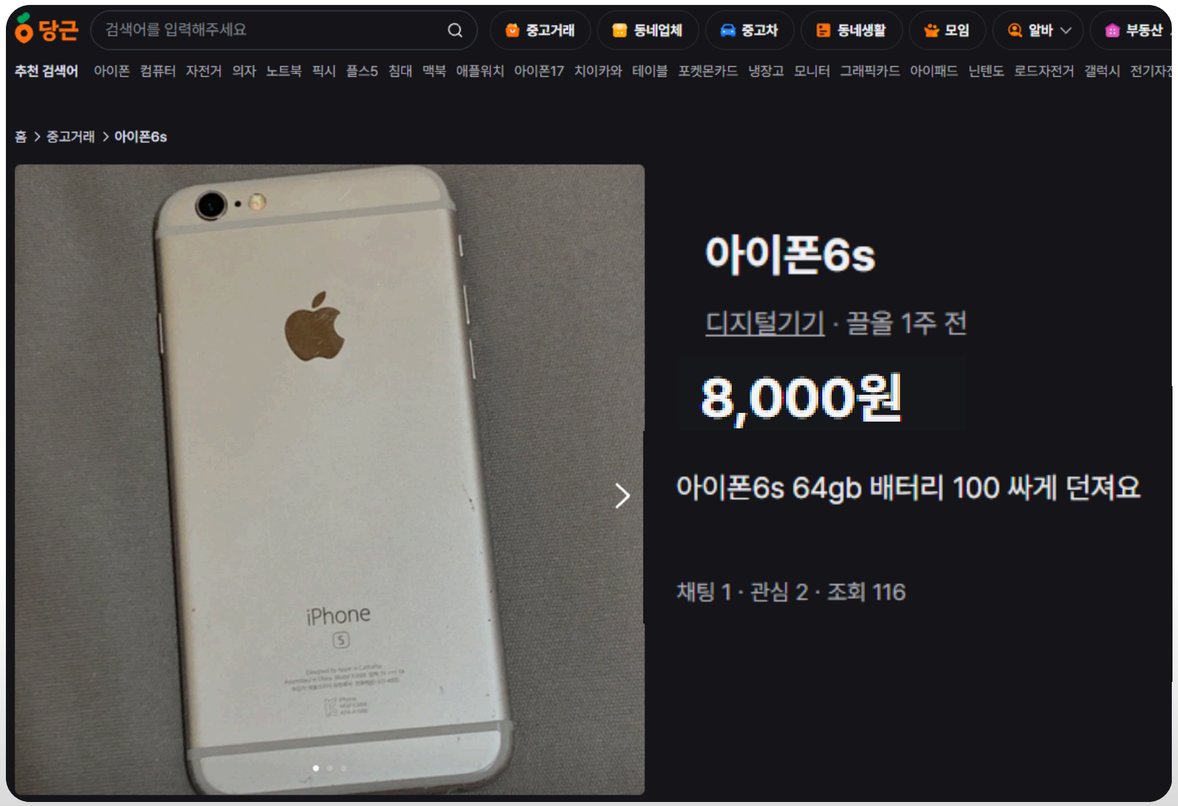

# 어쩌다 이 주제?

**(평균 8만원~)**

다른 글 대비 아주 저렴한

iPhone 6s 발견

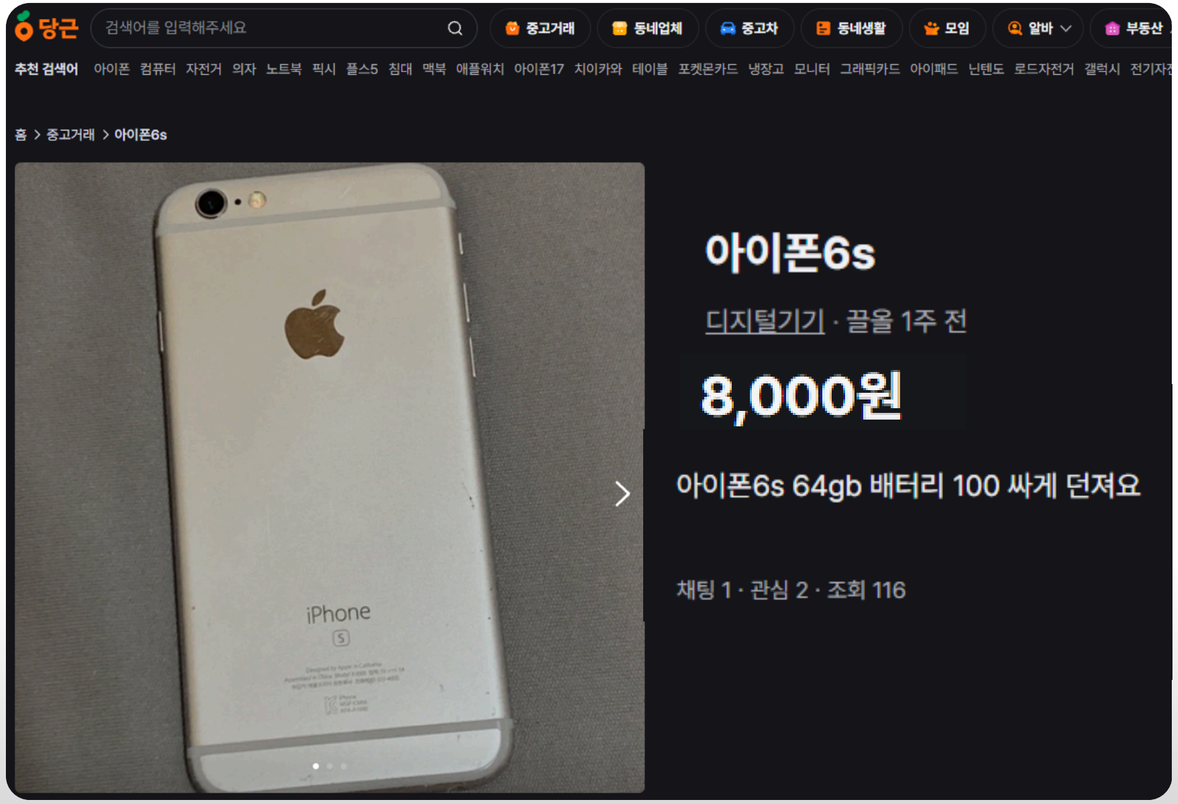
# 어쩌다 이 주제?




아주 저렴

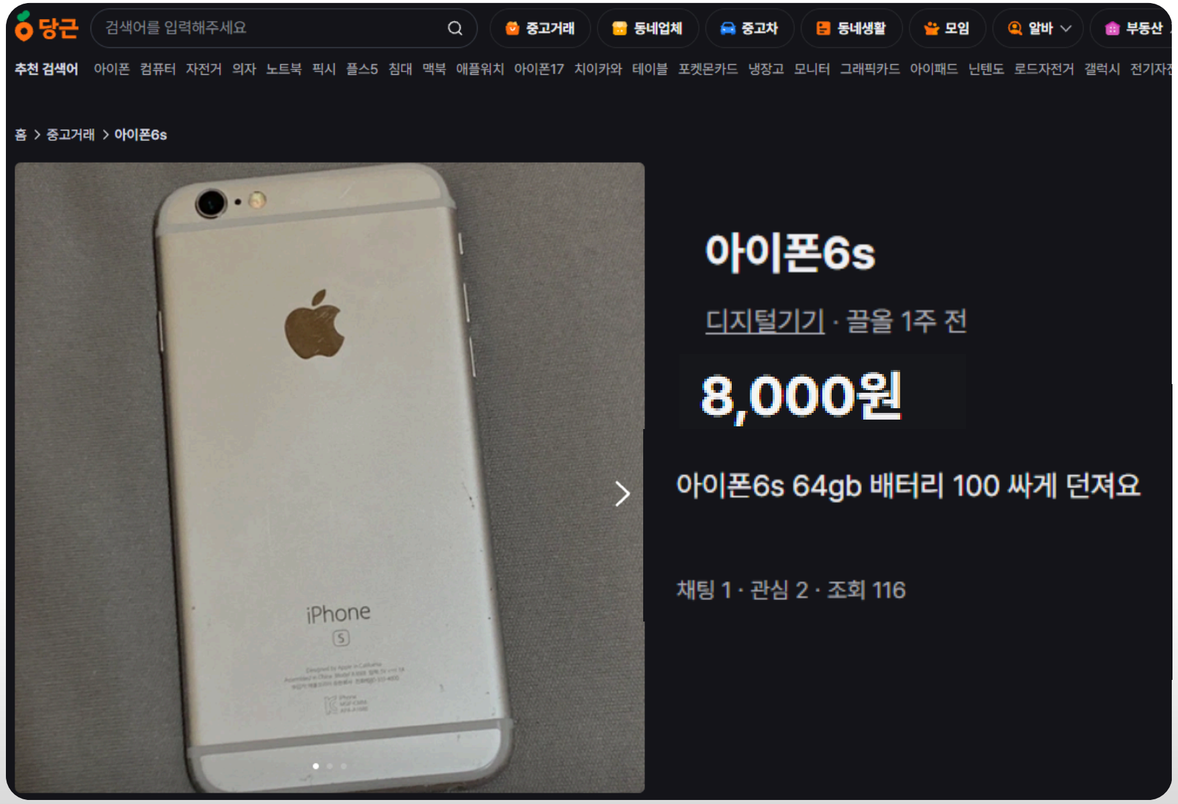
**→ 싼게 비지떡**

# 어쩌다 이 주제?




## Activation Lock

상태

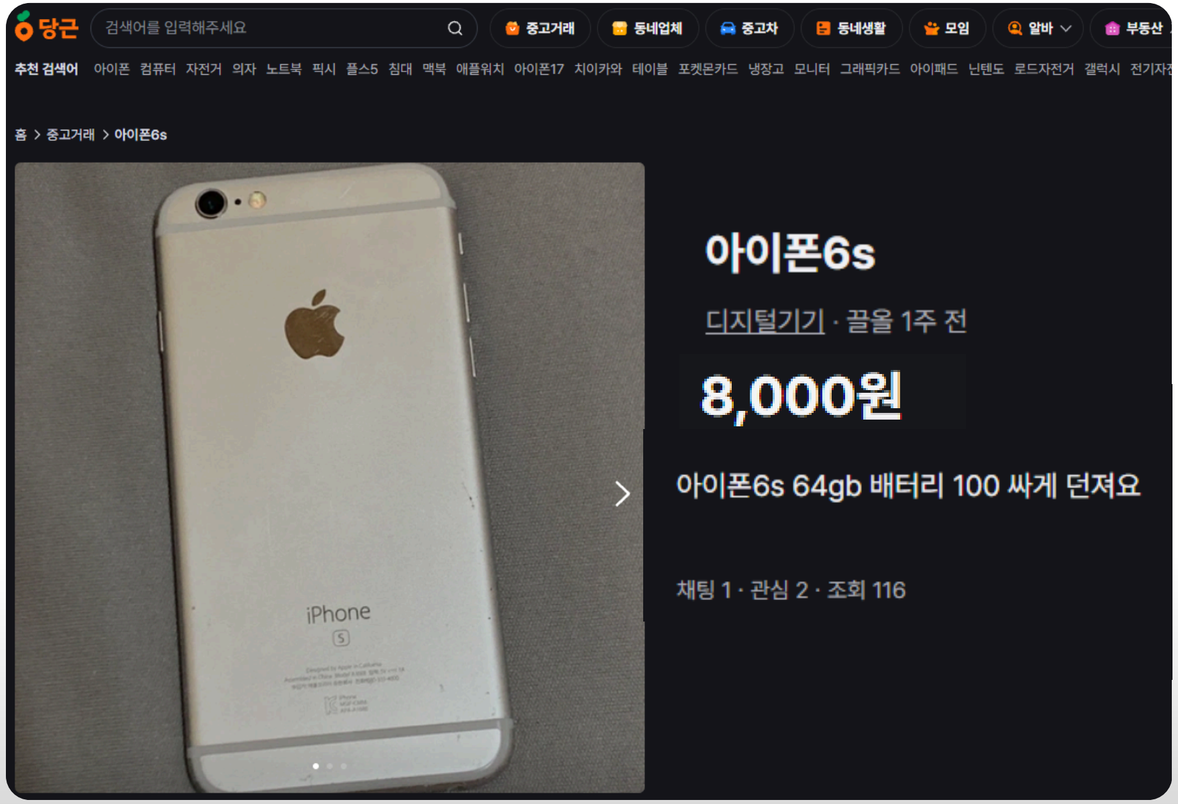



# 어쩌다 이 주제?

## Activation Lock

상태

→ 조금의 조사



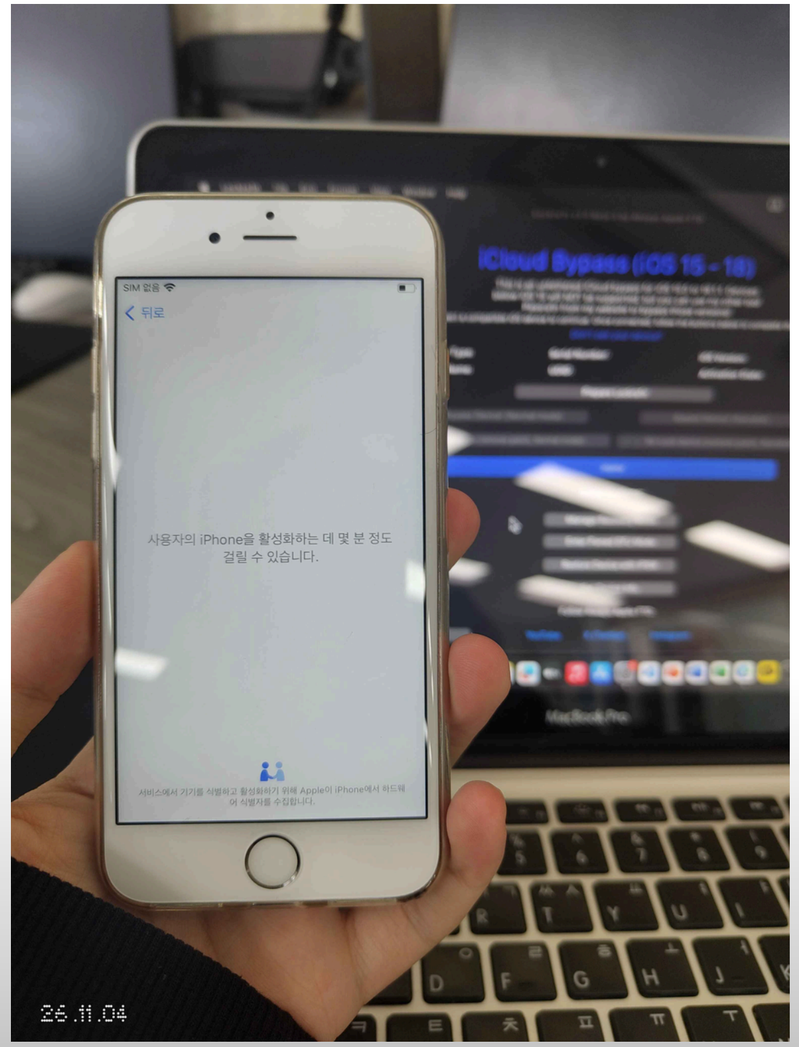

# 어쩌다 이 주제?

## Activation Lock

## 상태

**→ 조금의 조사**

**→ 상세한 건 다음 파트에...**



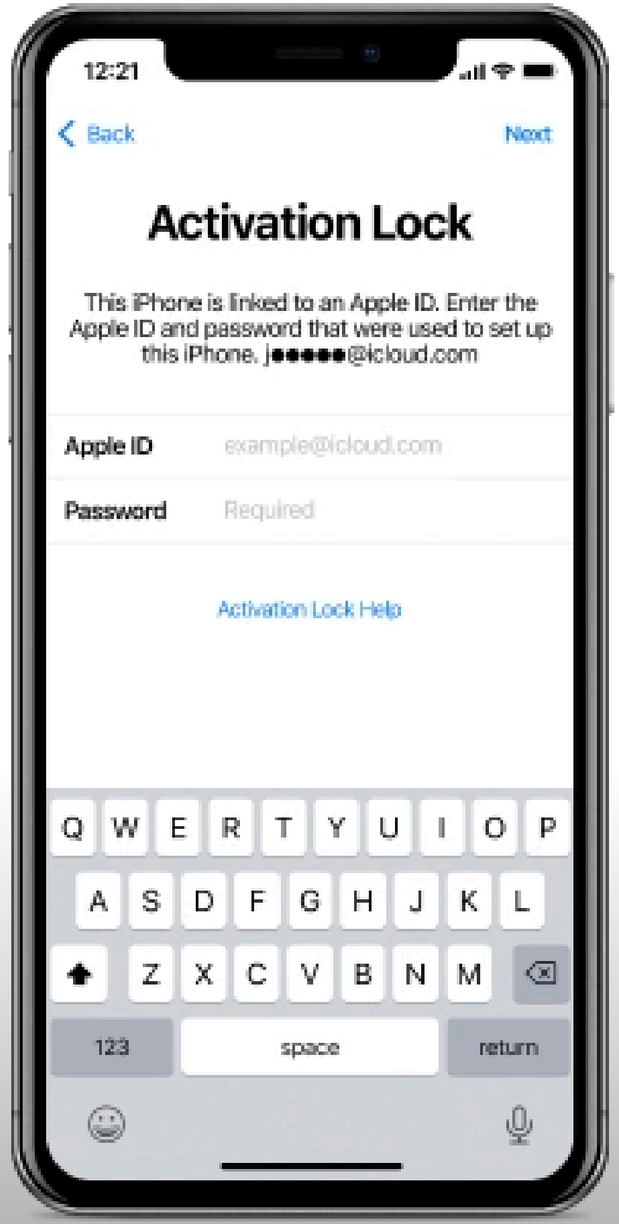

# Preview

Activation Lock
풀리는 영상



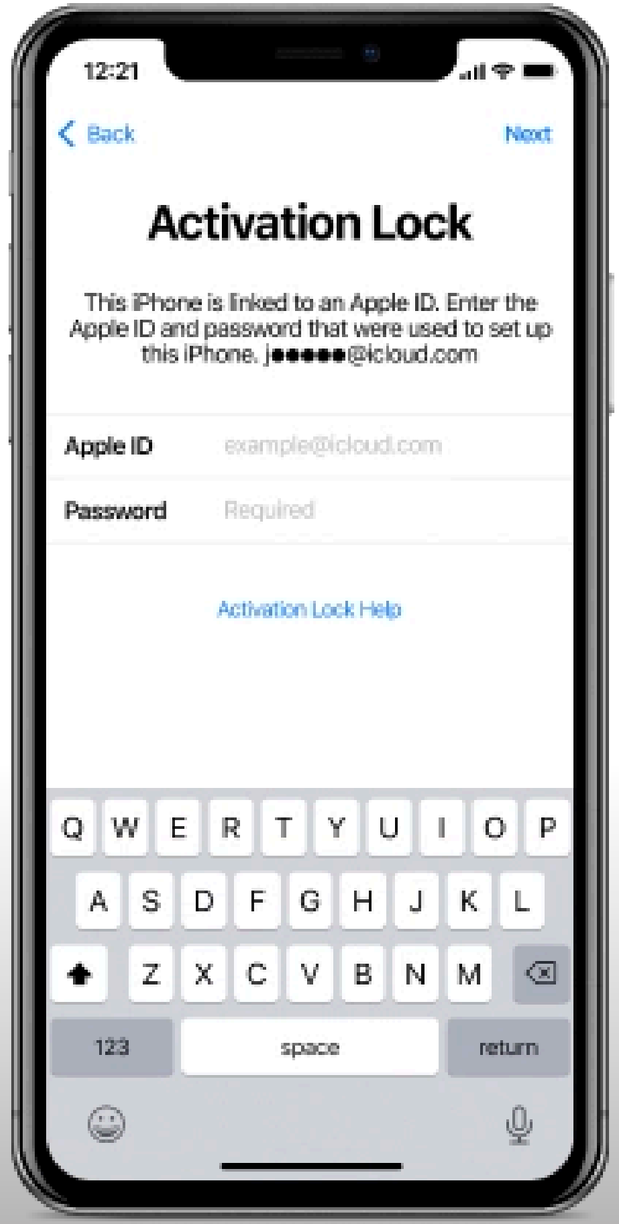
# What is Activation Lock?

& How it work




# Actvation Lock

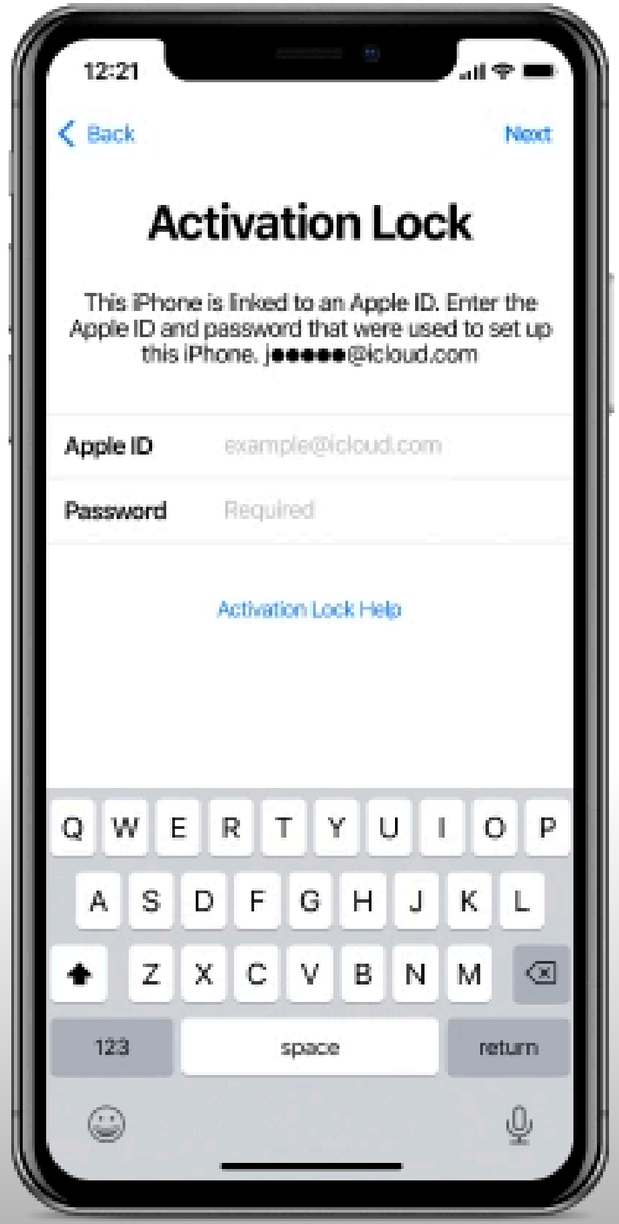
- iCloud Lock, Activation Lock 이라고도 불림
- Apple 의 분실 또는 도난당한 기기를 초기화하거나 재활성화하여 사용하는 것을 차단하는 보안장치
- Apple ID 자격 증명 없이는 홈화면으로 진입할 수 없음




# Actvation Lock

- iCloud Lock, Activation Lock 이라고도 불림
- Apple 의 분실 또는 도난당한 장치를 초기화하거나 재활성화하여 사용자 데이터를 보호하는 보안장치
- Apple ID 자격 증명 없이는 userspace 로 진입할 수 없음

**조금 복잡**




# Actvation Lock

로그아웃 안하고 초기화할 경우 생기고, 초기설정에서 못넘어가서 기기 사용 못함

**판매자가 이전 계정을 잃어버려서 싸게 구매**

# Actvation Lock




iPhone



Apple Server

# Actvation Lock




iPhone

활성화여부 확인요청



Apple Server

# Actvation Lock



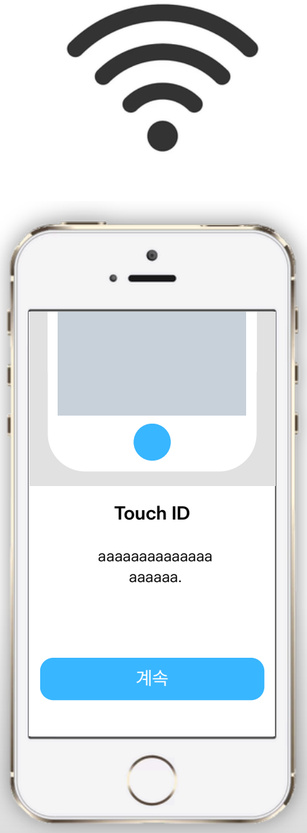

iPhone

IMEI + S/N + @



Apple Server

# Actvation Lock




iPhone

정상적이면

인증서 줌



Apple Server

# Actvation Lock




iPhone

아니면

이런 화면 뜨게됨



Apple Server

# Actvation Lock




iPhone

아니면

이런 화면 뜨게됨



Apple Server






# **Vuln** and **JailBreak**



# checkm8

## checkm8

- 수억 대의 iOS 기기에 적용 가능한 영구적이고 패치 불가능한 부트로롬 취약점
- 이것은 연구자들을 위한 것이며, 아직 Cydia를 이용한 탈옥 도구는 아닙니다.
- SecureROM 덤프, iOS 펌웨어용 키백 암호 해독, JTAG용 장치 등급 하향 조정이 가능합니다.
- 현재 지원되는 SoC: s5l8947x, s5l8950x, s5l8955x, s5l8960x, t8002, t8004, t8010, t8011, t8015
- 향후 지원 SoC: s5l8940x, s5l8942x, s5l8945x, s5l8747x, t7000, t7001, s7002, s8000, s8001, s8003, t8012
- 최신 iOS 버전에서 Cydia를 이용한 완전 탈옥은 가능하지만 추가 작업이 필요합니다.

## 체크메이트(Checkmate)가 무엇인가요?

체스에서 킹이 공격받은 경우를 우리는 체크라고 부릅니다. 체크메이트(줄여서 메이트라고도 부릅니다)는 공격받은 킹이 체크를 벗어날 수 없는 경우입니다. 이때, 경기는 상대 킹을 체크메이트한 선수의 승리로 끝납니다.

axi0mX 가 2019년에
발표한 취약점



# checkm8

JailBreak 가능한 코드실행
이후 ActivationLock 우회가능



# checkm8

하드웨어 BootROM 취약점

(Read Only Memory)

**업데이트로 패치** 불가능



# checkm8

## 하드웨어 BootROM 취약점

(Read Only Memory)

## **업데이트로 패치** 불가능

(A5-A11) iPhone 4s ~ iPhone X

수 억대 영향



# checkm8

## BootROM의 USB DFU 처리 과정중 UAF 일어남



# checkm8

DFU mode = 저수준 복구모드



# checkm8

DFU mode = 저수준 복구모드

iOS 재설치 초기화 등등...



checkm8

# UAF
# (Use After Free)



# checkm8

example.c

```c
char *ptr = malloc(16);
strcpy(ptr, "Hello");

free(ptr);          // 메모리 해제
printf("%s", ptr); // UAF: 해제된 메모리에 접근
```



checkm8

BootROM 에도 비슷한게 있음



checkm8

잘 활용하면 Control Flow Hijacking 가능




# JailBreak?

## 탈옥




# JailBreak?

## 탈옥

Appstore 아닌 스토어에서 앱 다운하기

tweak 설치하기

root 접근하기

etc...




# JailBreak?

## 탈옥

제조사가 사용 가능하게 풀어준 범위에서 탈출하기




# JailBreak?

## 정상부팅

## BootROM → iBoot → Kernel → iOS




# JailBreak?

## 탈옥시부팅

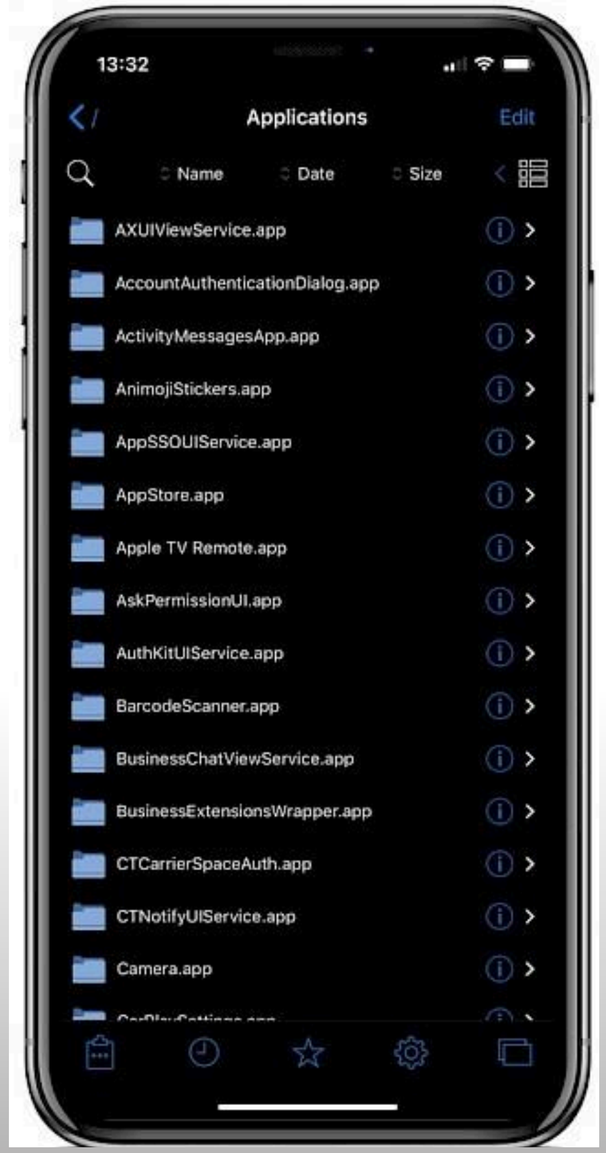
BootROM(취약점) → (페이로드로 변경된 부팅과정) → root 권한 있는 iOS




palera1n

# JailBreak?

- 구형기기에 iOS 26(테마) 설치




palera1n

# JailBreak?

- 구형기기에 iOS 26(테마 트윅) 설치
- 진짜 파일탐색기(Root 접근)




palera1n

# JailBreak?

- 구형기기에 iOS 26(테마 트윅) 설치
- 진짜 파일탐색기(Root 접근)
- **ActivationLock 우회조건 충족**



# Lockra1n

# Lockra1n



Target S/N 등 정보



User

DEV server

# Lockra1n




User

로컬 활성화용 데이터 제공



DEV server

# Lockra1n



탈옥으로 로컬 인증 루틴 조작




User

iPhone

Lockra1n

# 잠금해제 완료




iPhone



# Lockra1n

- MacBook
- Lockra1n
- iPhone(Target)

# Lockra1n

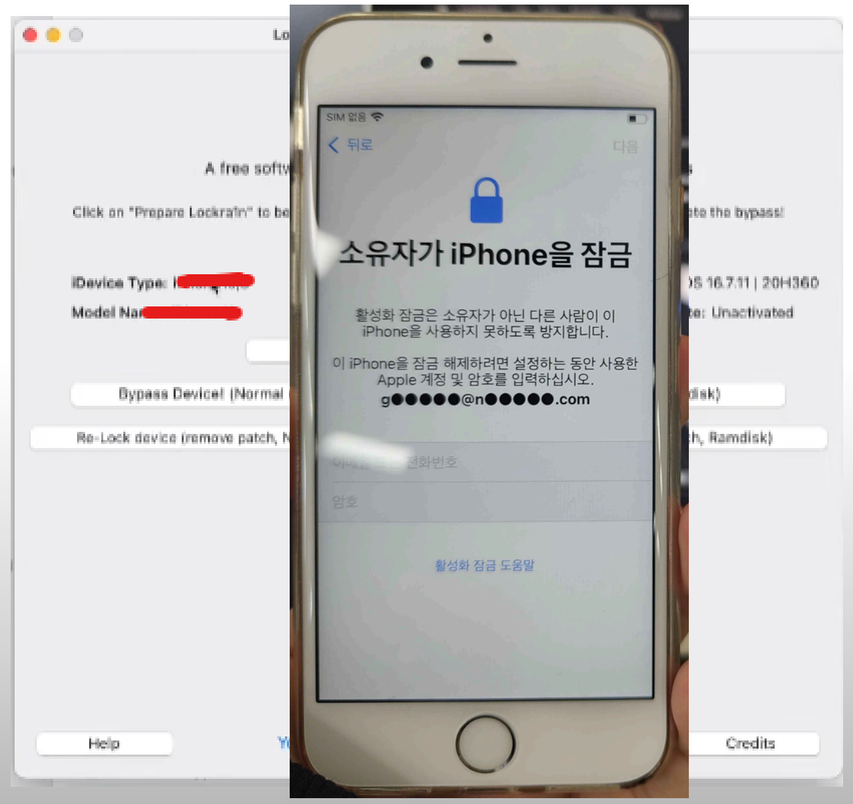
## 1. 장치연결




기기 S/N 등 정보 확인 가능

# Lockra1n

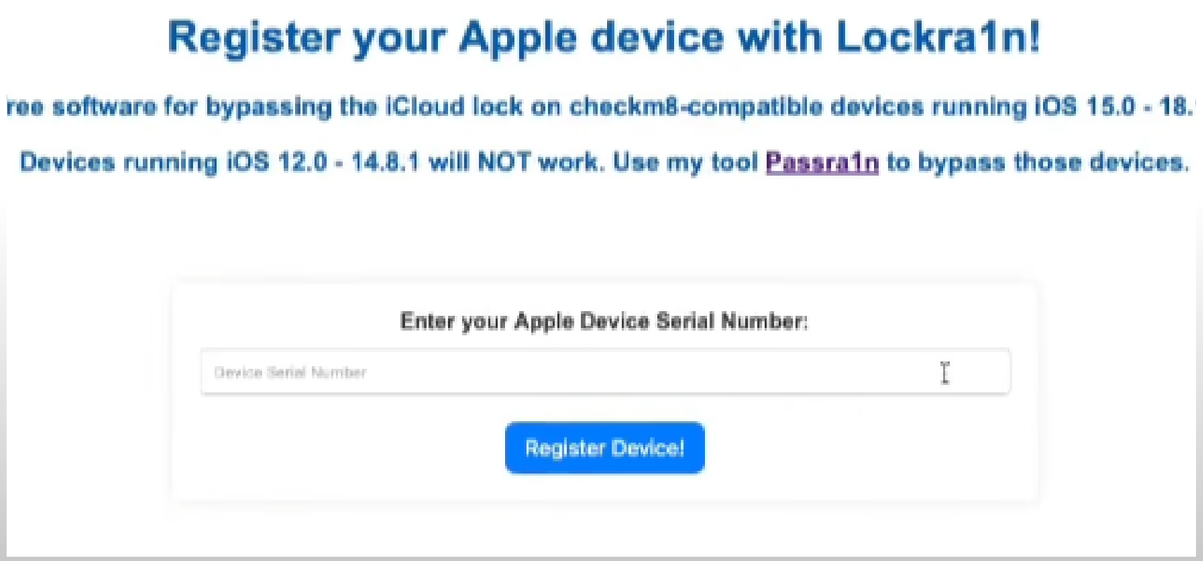
## 1. 장치연결




기기 S/N 등 정보 확인 가능

Lockra1n

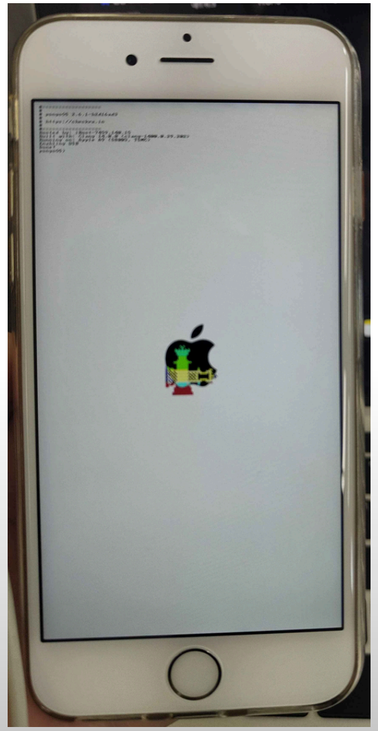
# 2. 장치등록

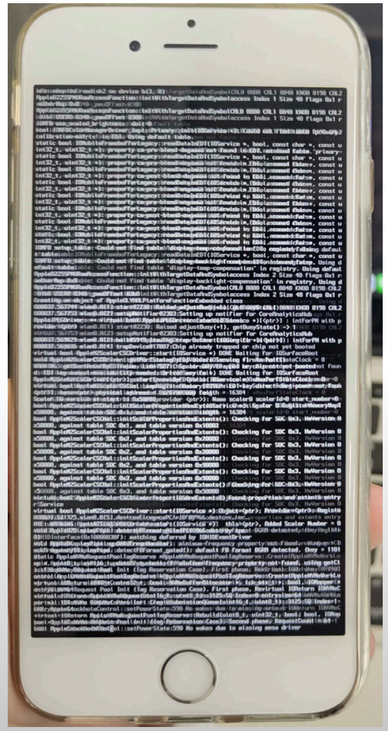



기기 S/N 서버 전달

# Lockra1n

## 3. DFU 모드 진입 + 탈옥



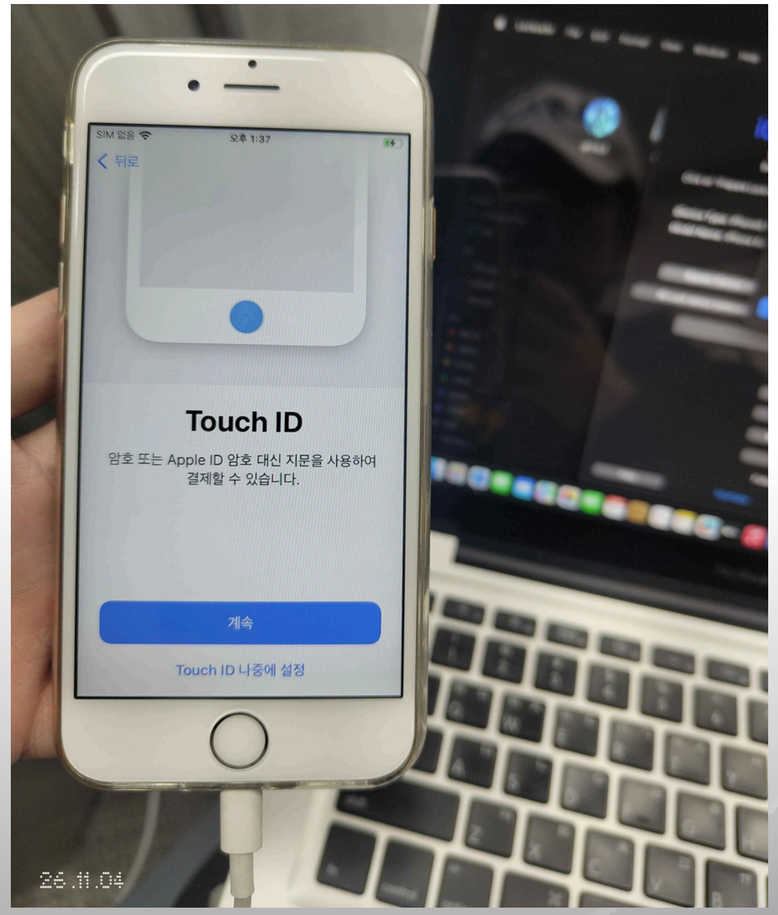


DFU 모드 진입 + 탈옥

# Lockra1n

## 4. bypass 패치 설치





# 결론

# 결론

Lockra1n 툴을 이용해
ActivationLock 해제와 원리에
대해 알아보았다.

# 결론

일부 기능(SIM,LTE)등이 제한됨

# 결론

만약에 비슷한 기회가 생기면
한번쯤 도전해봐도 좋을 실습

# 결론

시간만 충분했으면 더 자세히
분석하고 발표했을거 같다.

# 결론

마지막으로 말하고싶은 것

# 결론




iPhone Duo 출시 당일 시연한
취약점(비공개)

# 결론

## 대 딸깎 시대 이전(~2022)




## 대 딸깎 시대(2022~)



# 결론

## 대 딸깎 시대 이전(~2022)



- 사람이 직접 확인
- 분석에 오랜시간 걸림

## 대 딸깎 시대(2022~)

- AI 에이전트가 대신해줌
- 비교적 적은 시간 걸림
- 공격도 잘함

# 결론

## 대 딸깎 시대(2022~)

이제 AI 에이전트가 직접 취약점 찾고 공격하는
시대인데 계속 발전한다면 더 위험해지지않을까..



# Thank You

for listening