

모바일 샌드박스

MobSF

- 앱(Android/iOS/Windows) 정적/동적 분석 도구
 - APK, IPA, APPX 등

MobSF 장점

- API 지원
- On-Premise
- 오픈소스
- Slack 커뮤니티 운영

MobSF 단점

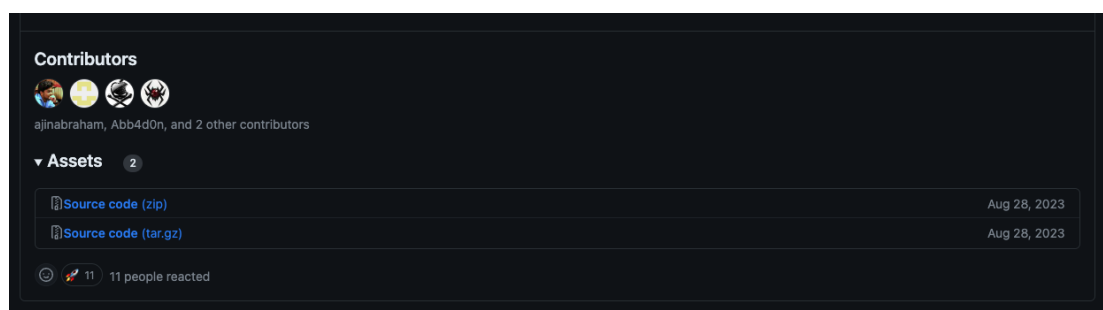
- Androguard 기반 → 앱 파일 크기 증가에 따라 퍼포먼스가 급격히 저하
- Frida 이슈

Prerequisite(windows10, build 19045 기준)

→ build 22621 테스트 완료

1. MobSF 설치

- <https://github.com/MobSF/Mobile-Security-Framework-MobSF>



2. Android studio & app tools 설치

- <https://developer.android.com/studio>

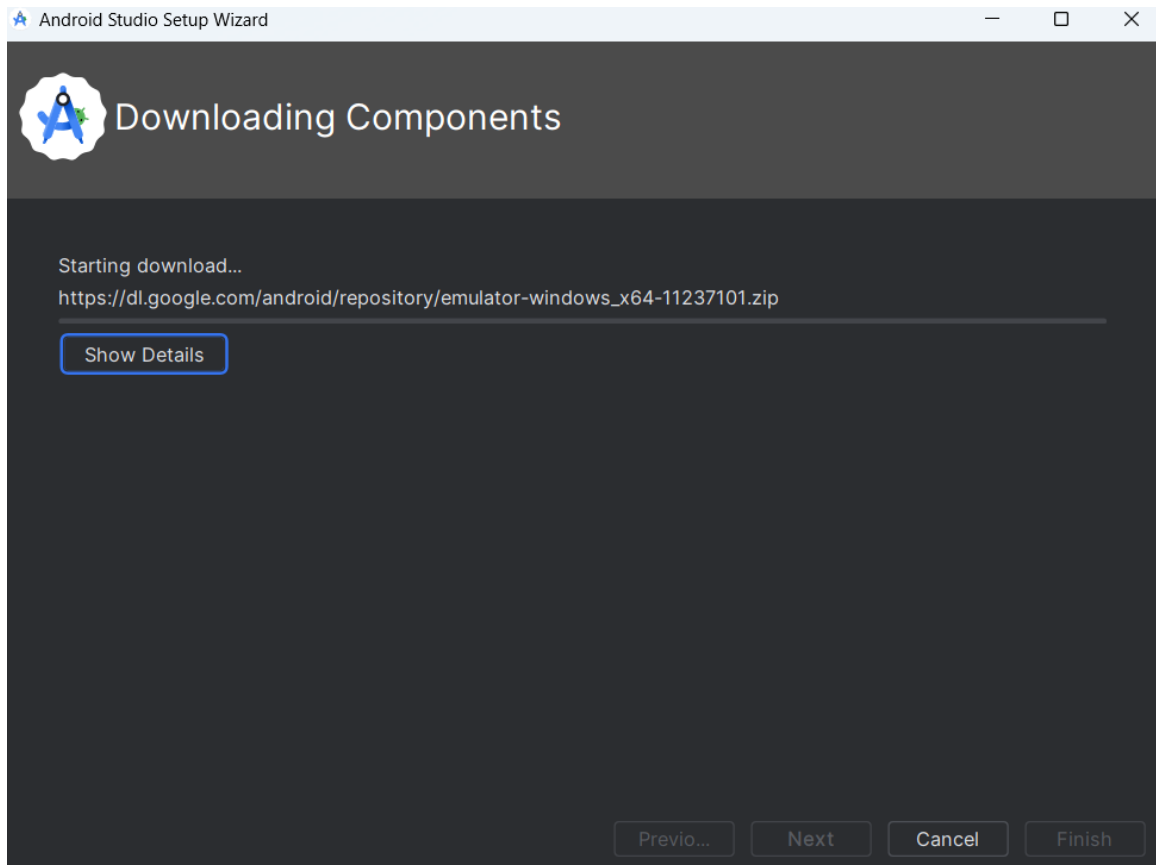
Android Studio downloads

Download the latest version of Android Studio. For more information, see the [Android Studio release notes](#).

Platform	Android Studio package	Size	SHA-256 checksum
Windows (64-bit)	android-studio-2022.3.1.20-windows.exe Recommended	1.1 GB	495d55bdd8bc1b8c6a41fcc5a31f8db0fbc3199a82fc4b0847d32f99fbe11b6
Windows (64-bit)	android-studio-2022.3.1.20-windows.zip No .exe installer	1.1 GB	c3ff4df64b1714867ee4301e5cbd9ea73a15b4385127f16bd530066b587cb5c9
Mac (64-bit)	android-studio-2022.3.1.20-mac.dmg	1.2 GB	2c3c4f44b015ff43ab350ed6218d24755835967bd3e3f1be6984d5334d0250f8
Mac (64-bit, ARM)	android-studio-2022.3.1.20-mac_arm.dmg	1.2 GB	62fcdeece46b0e816925a437dea7cbfd2921a943cc0fdeccf42c0346822ef9
Linux (64-bit)	android-studio-2022.3.1.20-linux.tar.gz	1.2 GB	224c4eb7a0c8e1c04f50eced1013495740c71abb898d5749d2c93172e7beadd8
ChromeOS	android-studio-2022.3.1.20-cros.deb	933.9 MB	af35214dd66ab946ecbf9865e8c8e8537219c8e3b166fb1cc435e35be6de4768

More downloads are available in the [download archives](#). For Android Emulator downloads, see the [Emulator download archives](#).

- SDK 컴포넌트 설치



- aapt.exe 환경변수 등록(windows)
 - C:\Users\{user_name}\AppData\Local\Android\Sdk\build-tools\34.0.0

3. Emulator

- Not available nested VM
 - 로컬 작업 권장(●'ㅂ'●)

1. android studio emulator

2. genemotion

- <https://www.genymotion.com/>

4. Python3

- 최신버전 권장
- <https://www.python.org/downloads/>

5. openssl

- <https://slproweb.com/products/Win32OpenSSL.html>

6. visual studio build-tools

- <https://visualstudio.microsoft.com/thank-you-downloading-visual-studio/?sku=BuildTools&rel=16>

7. JDK(11)

- <https://www.oracle.com/kr/java/technologies/javase/jdk11-archive-downloads.html>
- JDK 8 이상 필요
- JAVA_HOME 또는 JAVA_DIRECTORY 환경변수 등록
- 회원가입 필요
- https://drive.google.com/file/d/1SWysYSksmsjgyx2TIVi_7kTNQuJCix2o/view?usp=sharing





8. APK Sample

- https://drive.google.com/file/d/1_yg2Sp6Wru1w1eZJ4yw__HyeZINRwh0N/view?usp=sharing
- zip pw: infected

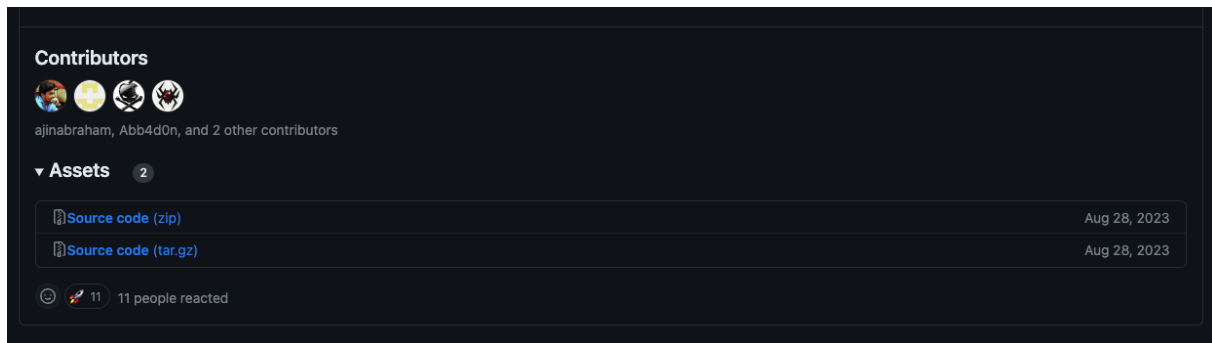
MobSF 설치 과정

1. android studio 설치
2. python3 설치
 - a. 3.12 미만
 - b. 테스트 환경: v3.11.7
3. openssl 설치
4. visual studio build-tools 설치

데스크톱 및 모바일 (4)

 C++를 사용한 데스크톱 개발 <input checked="" type="checkbox"/> MSVC, Clang, CMake 또는 MSBuild 등 선택한 도구를 사용하여 Windows용 최신 C++ 앱을 빌드합니다.	 .NET을 사용한 모바일 개발 <input type="checkbox"/> C# 및 F#를 사용하여 iOS, Android 및 Windows용 플랫폼 간 애플리케이션을 빌드하기 위한 도구입니다.
 .NET 데스크톱 빌드 도구 <input type="checkbox"/> C#, Visual Basic 및 F#를 사용하여 WPF, Windows Forms 및 콘솔 애플리케이션을 빌드하기 위한 도구입니다.	 유니버설 Windows 플랫폼 빌드 도구 <input type="checkbox"/> 유니버설 Windows 플랫폼 애플리케이션을 빌드하는 데 필요한 도구를 제공합니다.

5. MobSF 릴리즈 파일 다운로드

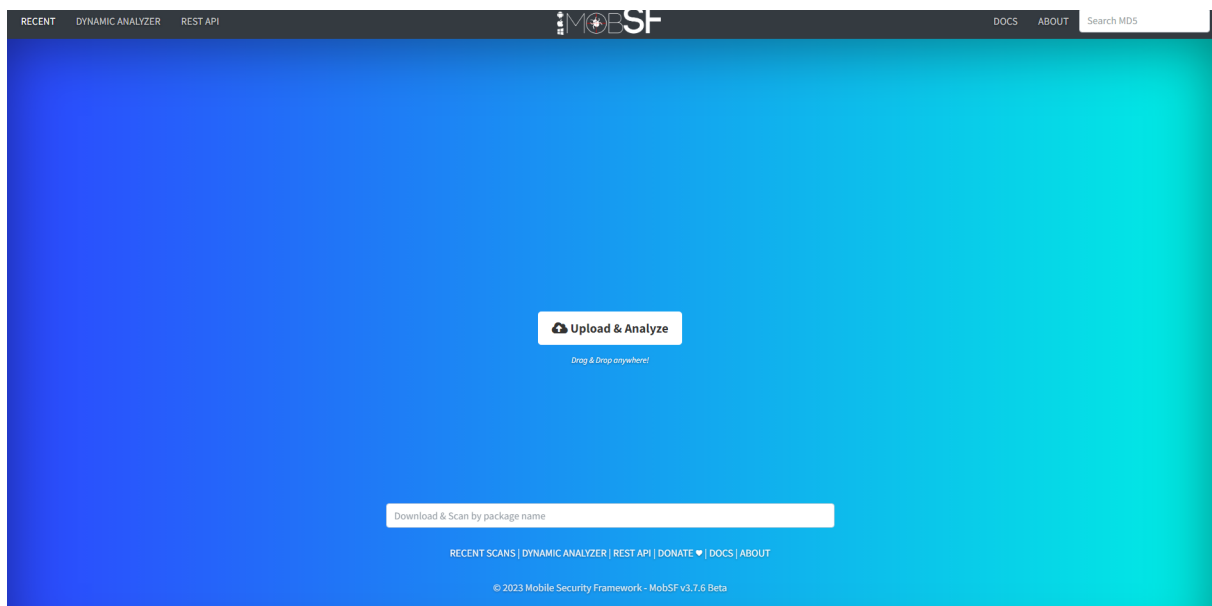


6. setup.bat 실행

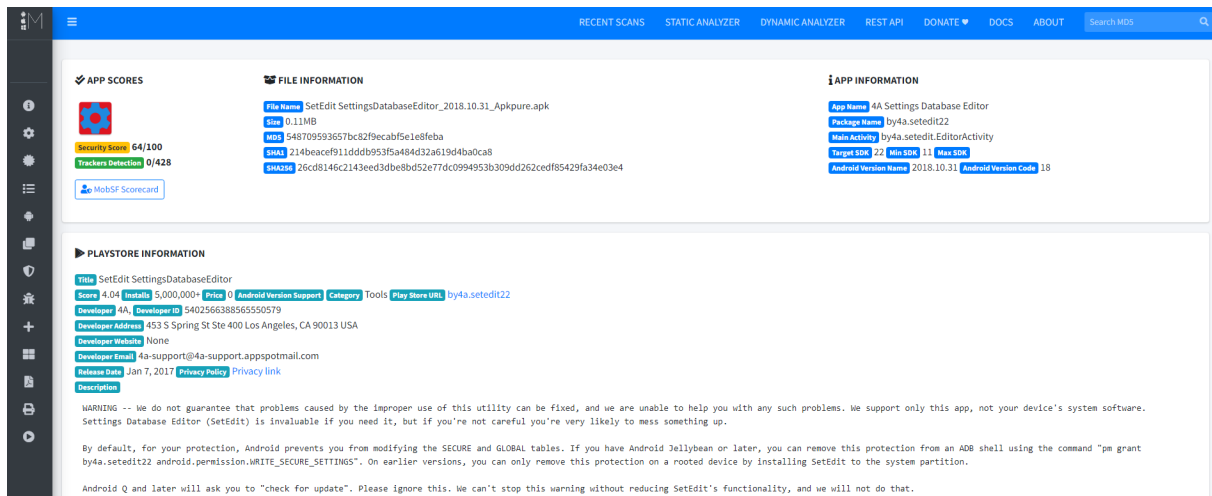
```
[INSTALL] Checking for Python version 3.9+
[INSTALL] Found Python 3.11.6
[INSTALL] Found pip
Requirement already satisfied: pip in c:\users\i\appdata\local\programs\python\python311\lib\site-packages (23.2.1)
Collecting pip
  Obtaining dependency information for pip from https://files.pythonhosted.org/packages/47/6a/453160888fab7c6a432a6e
afe6256d0d9f2cbd25971021da6491d899/pip-23.3.1-py3-none-any.whl.metadata
  Downloading pip-23.3.1-py3-none-any.whl.metadata (3.5 kB)
Downloading pip-23.3.1-py3-none-any.whl (2.1 MB)
----- 2.1/2.1 MB 12.2 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.2.1
    Uninstalling pip-23.2.1:
      Successfully uninstalled pip-23.2.1
```

7. run.bat 실행

4. 브라우저 실행 → localhost:8000 접속



9. apk 파일 drop 후 결과 보기



Project Goal

1. MobSF 구조 이해 하기

- 설정 파일
- 소스코드 / 메타데이터 저장소 분리
- 정적 / 동적 분석 모듈 구조 / 호출 관계 파악
- API 구조 및 사용법 이해
- 에뮬레이터 연동

2. 암호화된 DEX 파일이 포함된 APK 분석 시, 대시보드에 해당 DEX에 대한 정보 제공

- 앱 리패키징 → apktool(Open Source)
- 메모리 내 복호화 로드 → bytesIO(Python)
- 파일 복호화 방법
 - 알고리즘: AES-128/ECB
 - KEY: dbcdcfghijklmaop
 - CyberChef

1.

3. MobSF 내 Nested APK 지원

- 내부 APK에 대한 분석 자동화

4. 에뮬레이터 연동 및 탐지 우회(option)

- 설정 파일 내 에뮬레이터 정보 기입
- MobSF로 에뮬레이터/앱 컨트롤
- 에뮬레이터 탐지 우회(frida/non-frida)

5. MobSF를 이용한 앱 정적/동적 분석 결과 확인

- 앱 업로드 → 정적 분석 결과
- 에뮬레이터 실행 → 동적 분석 결과

6. API 커스터마이징을 통한 분석 자동화(python)

- API: https://mobsf.live/api_docs
- API 사용 예시:
<https://gist.github.com/ajinabraham/0f5de3b0c7b7d3665e54740b9f536d81>
- 커스텀 API 개발
- API로 MobSF 컨트롤
 - APK ↔ API(python) ↔ MobSF ↔ Emulator
 - File upload 이후, User Interaction 없어야함
- 커스텀 정적/동적 분석 기능 만들어보기(option)
 - 기존 기능 활용 / 새로운 기능 개발 무관

그 외 분석 도구

1. apktools

- <https://github.com/iBotPeaches/Apktool>
- 앱 리패키징

2. jadx

- <https://github.com/skylot/jadx>
- 소스코드 분석

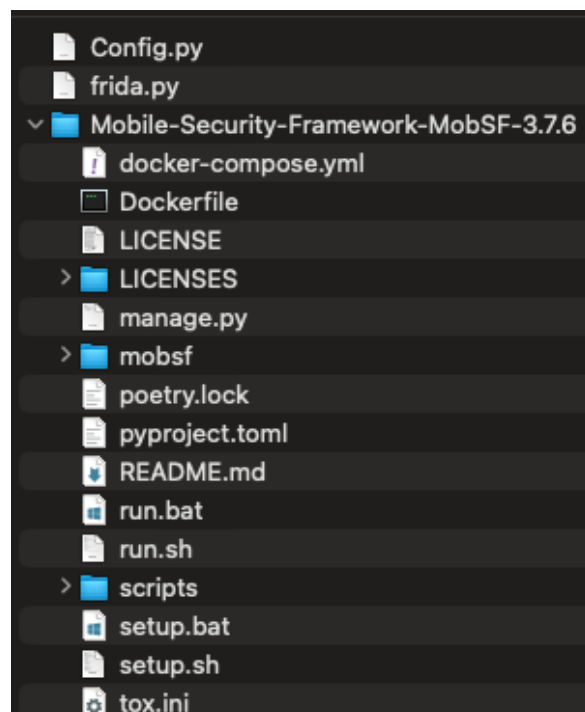
3. frida

- <https://github.com/frida/frida/releases>
- 탐지 우회

제출물

1. 소스코드 압축 파일(Google Drive)

- a. Mobsf + 설정파일 + Frida 스크립트 + 일원화 스크립트
- b. 2024_mma_{차수}_{조}_{이름}.zip



2. 커스텀 코드에 대한 Documentation

- a. Config / API / 분석 모듈
 - 암호화된 DEX 대시보드 출력 과정 필수
- b. 노션 추천(링크 공유)

3. mobsf 실행 → API를 사용한 정적/동적 분석 → 결과 import의 과정이 담긴 동영상(1분 내외)

- sample.apk

채점 기준

1. 압축 파일

2. Documentation

3. 동영상

- 예시

https://prod-files-secure.s3.us-west-2.amazonaws.com/9b314010-b882-45bd-adcd-4ab378aaca74/89a7aa90-8f4f-41bd-872b-9f1c3acff4c1/%E1%84%87%E1%85%AE%E1%86%AB%E1%84%89%E1%85%A5%E1%86%A8_%E1%84%80%E1%85%A7%E1%86%AF%E1%84%80%E1%85%AA_%E1%84%89%E1%85%B5%E1%84%8B%E1%85%A7%E1%86%AB.mp4

- 정적/동적 분석 일원화 여부
 - e.g.) 파일 업로드 → 정적 분석 → 동적 분석 → Report

4. 가산점

- 악성코드 패밀리 식별

궁금한 점은 오피스아워 신청하기