

# 달콤 씹싸름한 ADB

KAIST PLRG 이성호, 황성재, 김용대, 류석영

# ADB?

- **A**ndroid **D**ebug **B**ridge
- 서버 - 클라이언트 모델로 동작



# 강력한 ADB

- 기기 및 유심의 정보 확인
- 어플리케이션 삭제 / 설치
- 어플리케이션 프로파일링
- 어플리케이션 메모리 상태 확인
- 화면 터치 이벤트 발생

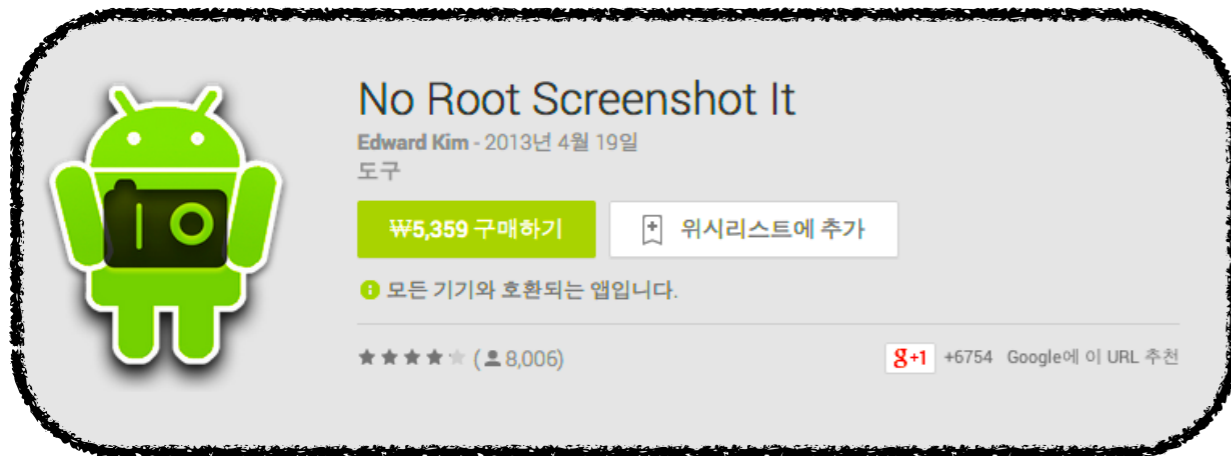
...


# ADB는 양날의 검


- 어플리케이션에서 ADB 서버에 접속(로컬 커넥션)
  - 일반적인 어플리케이션 권한 외의 작업 수행
- ADB 이용 시, 오직 '인터넷 권한' 만을 요구
  - 안드로이드의 '권한 기반 보안 정책' 이 흔들림


# 달콤한 ADB


- 루트 권한 없이는 불가능했던 일들을 척척!

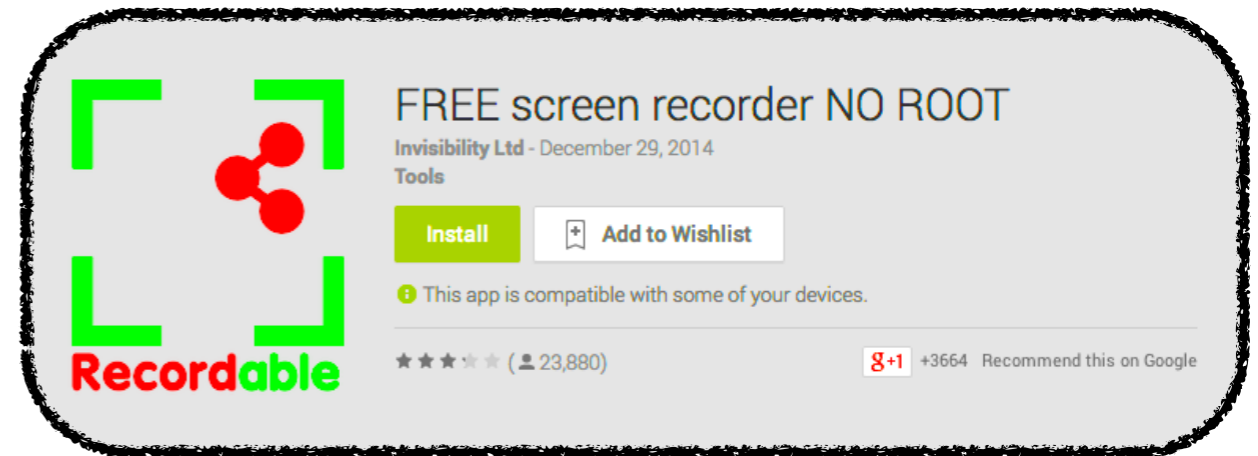



 **No Root Screenshot It**  
Edward Kim - 2013년 4월 19일  
도구


₩5,359 구매하기     위시리스트에 추가


 모든 기기와 호환되는 앱입니다.


★★★★☆ ( 8,006)     +6754 Google에 이 URL 추천



 **FREE screen recorder NO ROOT**  
Invisibility Ltd - December 29, 2014  
Tools

Install     Add to Wishlist

 This app is compatible with some of your devices.

★★★★☆ ( 23,880)     +3664 Recommend this on Google



 **ClockworkMod Tether (no root)**  
ClockworkMod - 2013년 12월 20일  
도구

설치     위시리스트에 추가

 모든 기기와 호환되는 앱입니다. 인앱 구매 제공

★★★★☆ ( 23,308)     +15705 Google에 이 URL 추천



 **Remote ADB Shell**  
Cameron Gutman - November 14, 2013  
Tools

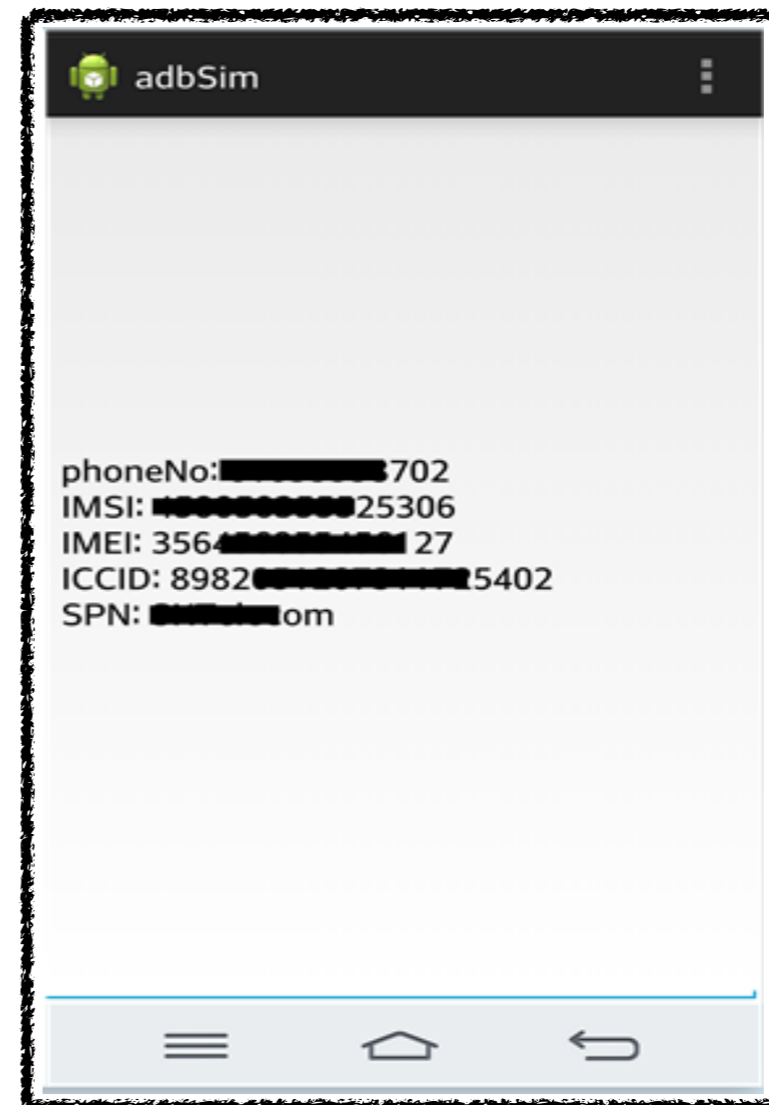
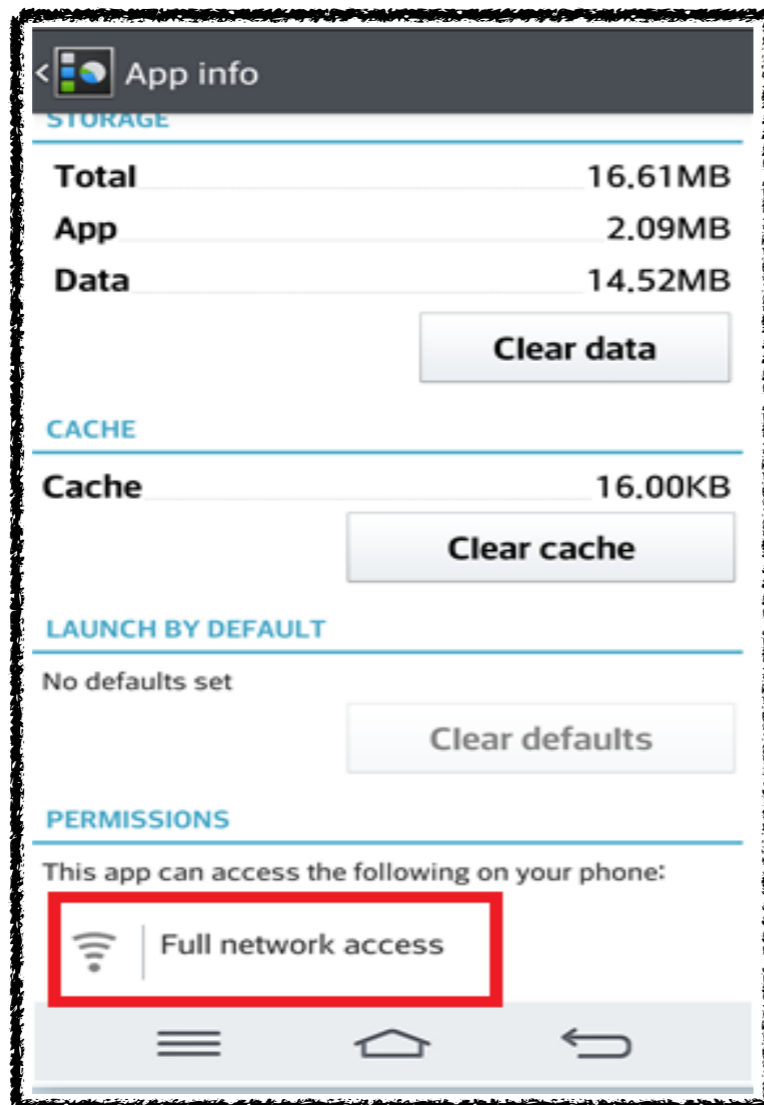
Installed

 This app is compatible with all of your devices.

★★★★☆ ( 78)     +81 Recommend this on Google

# 쌩쌩쌩 ADB

- 사용자 기기 정보 훔치기

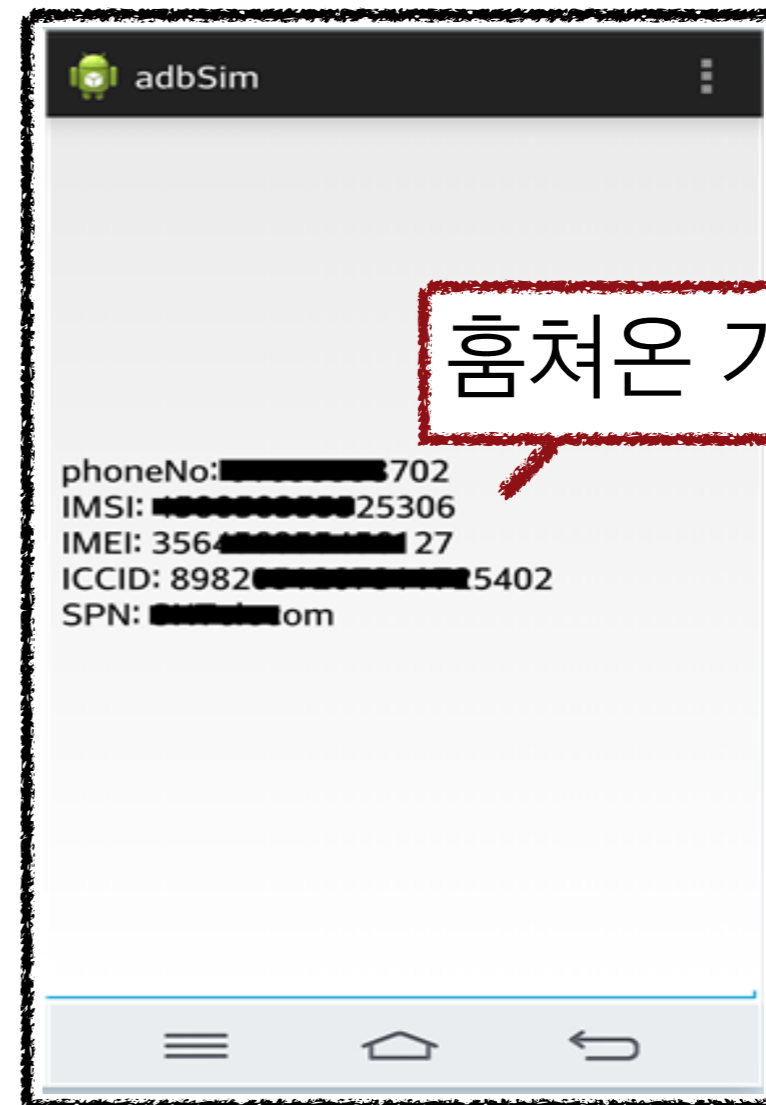


# 쌩쌩쌩 ADB

- 사용자 기기 정보 훔치기



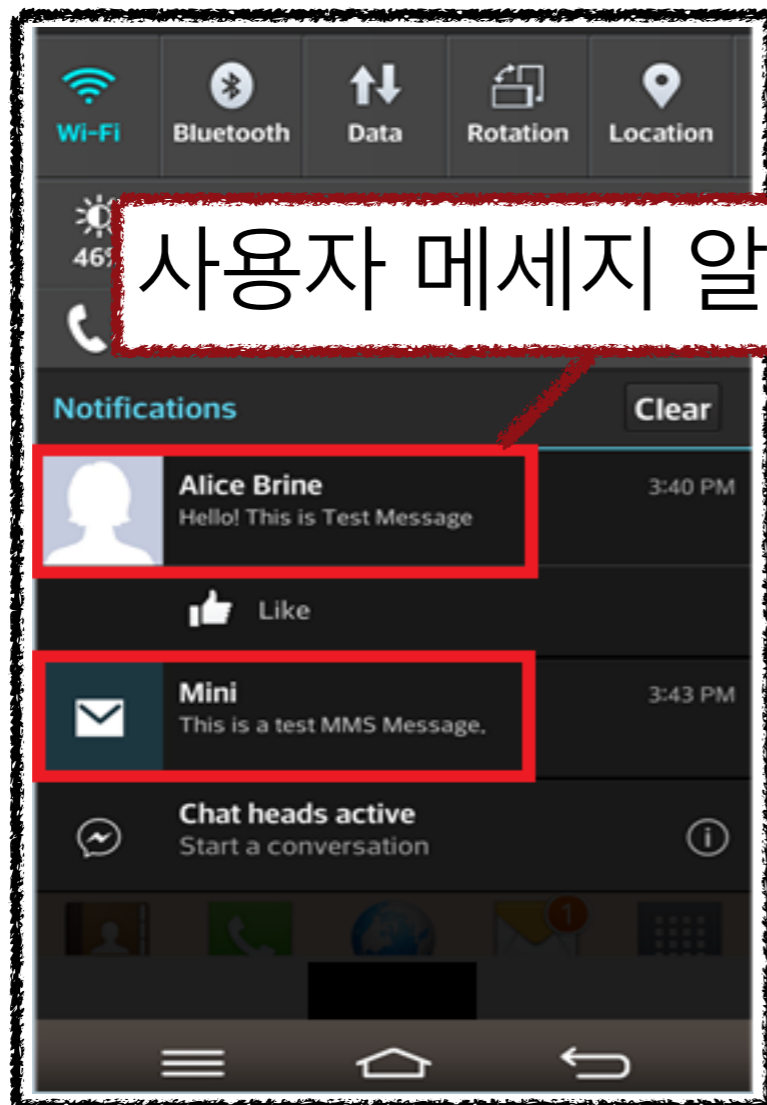
어플리케이션이 요구한 권한



훔쳐온 기기 정보

# 쌉쌉름한 ADB

- 사용자 개인 정보 훔치기



사용자 메시지 알림

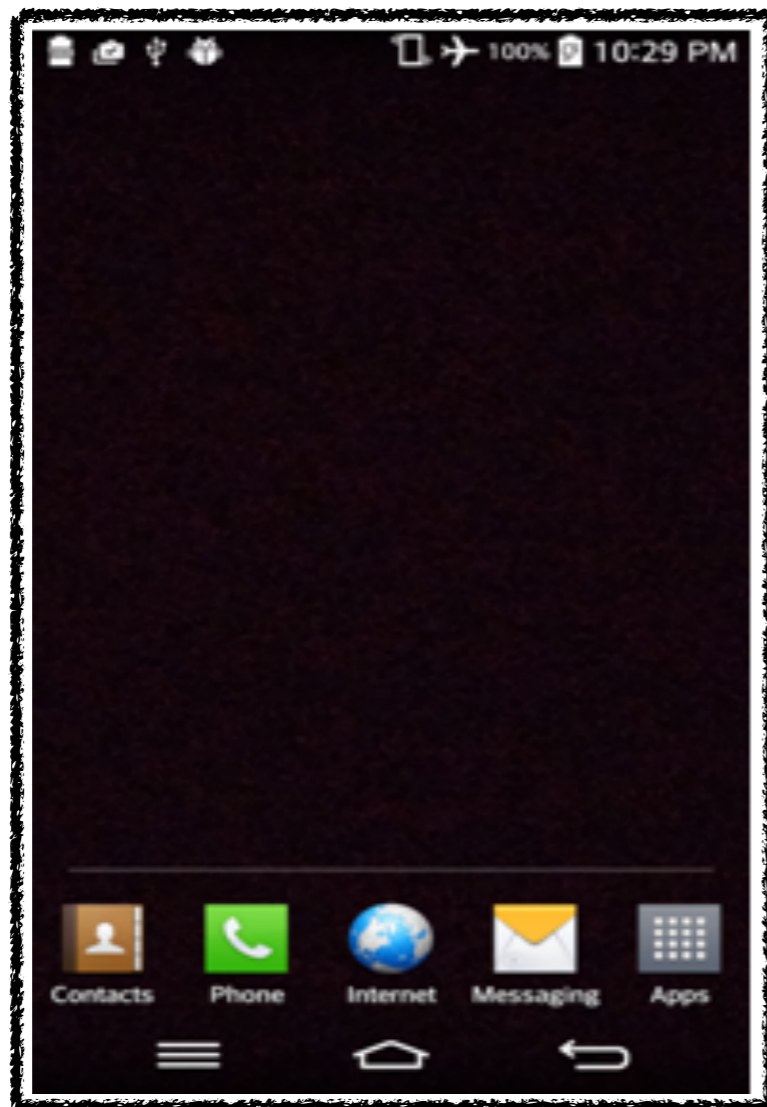


훔쳐온 사용자 메시지 정보



# 쌩쌩쌩 ADB

- 사용자 기기 못쓰게 하기



# 연구의 결과로

- ADB를 통한...
  - 다양한 공격 방법 제시
  - 악성 어플리케이션 탐지 도구 개발
  - 시스템 관점의 보안대책 제안

감사합니다.