Logcat APP/Tool

2025.01.08

모바일시스템공학과 조민혁
소프트웨어학과 이승민, 정성원

INDEX

01 Logcat App/Tool

❖Logcat의 문제점

✓ Logcat은 로그 데이터를 명령어를 통해 간편하게 볼 수 있다는 장점이 있지만,
버퍼 용량이 다 차거나 전원 OFF 시 로그 데이터가 삭제된다는 특성이 있음

❖목적

✓ **휘발성 로그**를 **비휘발성 영역**으로 안전하게 옮겨 버퍼 용량이 다 차거나 전원이 OFF되어도 **로그가 삭제되지 않도록한다.**

✓ **포렌식 수사 관점**에서 개발

✓ 효율적인 포렌식 수사가 될 수 있도록 기여하는 측면에서 개발

Logcat App/Tool

❖기존에 생각했던 로직

✓ APP/Tool 내에서 시스템 명령어인 ‘adb logcat’이 작동하여 로그를 가져오도록 한다.

➔ 불가능 ..

✓ APP/Tool 내에서 시스템 로그가 존재하는 버퍼를 모니터링 하여 로그를 가져온다.

➔ 이것 역시 .. 불가능

✓ 이벤트가 발생할 때 호출되는 함수를 후킹하여 원하는 로직이 먼저 실행되도록 한다.

➔ 이것마저 .. 불가능

=> “안드로이드는 버전이 업데이트 될 수록 보안 정책 및 권한에 대하여 매우 정교해지고 있음”

❖해결 아이디어

✓ 어차피 **각 이벤트에 대해 어떤 로그가 발생**되는 지는 실험을 통해 분석 및 파악 가능

✓ 그러면 **기기가 이벤트가 인지**할 수 있다면 **로그를 흉내내어 비휘발성 영역에 로그 작성 가능**

=> “기기가 이벤트를 인지하도록 설계하자 !”

❖최종 로직

STEP 1) 기기에서 발생하는 여러 이벤트에 대해 **어떤 로그들이 생성되는 지 분석**한다.

STEP 2) 기기에서 발생하는 여러 이벤트들이 발생할 때 어떤 **브로드캐스트**가 발생하는 지 파악한다.

STEP 3) 만약, 브로드캐스트가 존재하지 않는 이벤트라면 **모니터링**을 하도록한다.

➔ Ex) ‘adb logcat -c’ ; 버퍼를 비우는 명령어

STEP 4) 해당 정보를 바탕으로 **코드를 작성**한다.

- 브로드캐스트 인지 부분
- 모니터링 부분
- 로그 작성 부분

Logcat App/Tool

❖ Logcat App/Tool 개발 계획서

✓ 참여 인원

- 포렌식 팀: 조민혁, 이승민
- 머신러닝 팀: 정성원

* 추후 인원 추가적으로 더 필요할 걸로 예상 ..

✓ 개발 환경

- 프로그래밍 언어: JAVA
- IDE: Android Studio
- 대상 OS: Android 14, Galaxy S21
- 기능 집중, 이에 따라 UI없음

Logcat App/Tool

❖무엇을 해야하는가?

① Anti-Forensic 행위 인지 및 로그 생성 - OK

- Timestamp 조작, logcat -c, 전원 끄기 및 재부팅, File 메타데이터 조작

② APP 관련 로그 생성 - 진행중 (전화 앱, 문자 앱 완료)

- 전화 앱, SMS 앱, 블루투스 앱, 차량 진단 앱, 내비게이션 앱, Android Auto 관련 앱들 ..

③ 서버로 보내기 - Next Level

- NAS? ICT관 3층 서버? 클라우드?

④ 자동차에도 적용

- 스마트폰과 자동차와의 통신을 중심으로 .. + 자동차에서 발생하는 로그

⑤ 커널 level에서 작동시키기

- eBPF .. APP을 명시적으로 실행하는 것이 아닌 디폴트로 시작되도록 작동시키는 것이 최종 목표

Logcat App/Tool

❖ 완성된 후 (단기 ~ 장기)

① 보험 회사와 논의

② 경찰청과 논의

③ 특허

④ 논문?

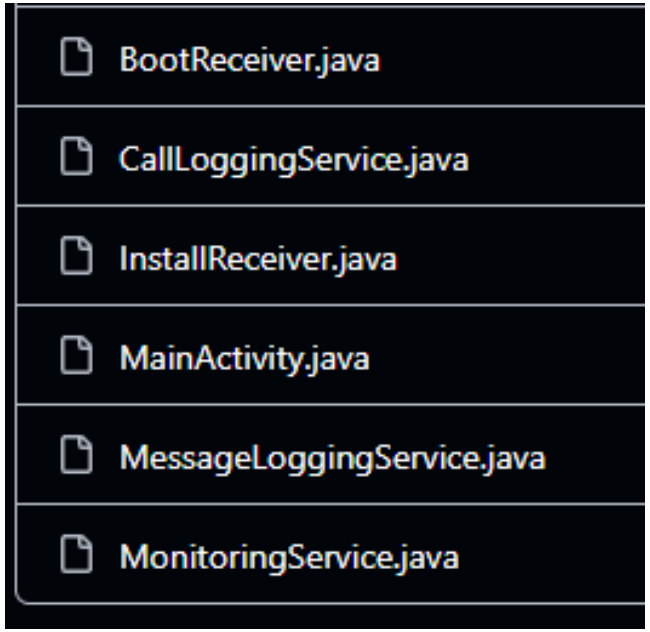
⑤ AOSP 제보 .. 또는 취약점 제보 (첫 번째 개인적인 희망 목표)

⑥ 언젠가 Android 버전이 올라가면 해당 기능 채택 (두 번째 개인적인 희망 목표)

02 작동 화면 및 시연

작동 화면 및 시연

❖ 코드 구성



BootReceiver: 부팅 시 앱 실행되도록 하는 Class

CallLoggingService: 전화 이벤트 및 로그 처리 Class

InstallReceiver: 패키지 설치 Class

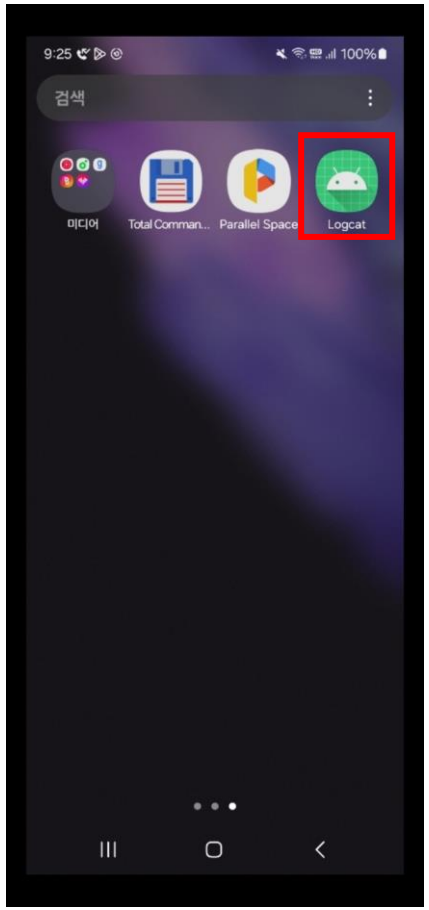
MainActivity: 프로그램의 첫 시작 부분

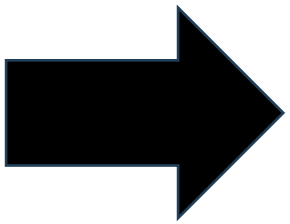
MessageLoggingService: 메시지 이벤트 및 로그 처리 Class

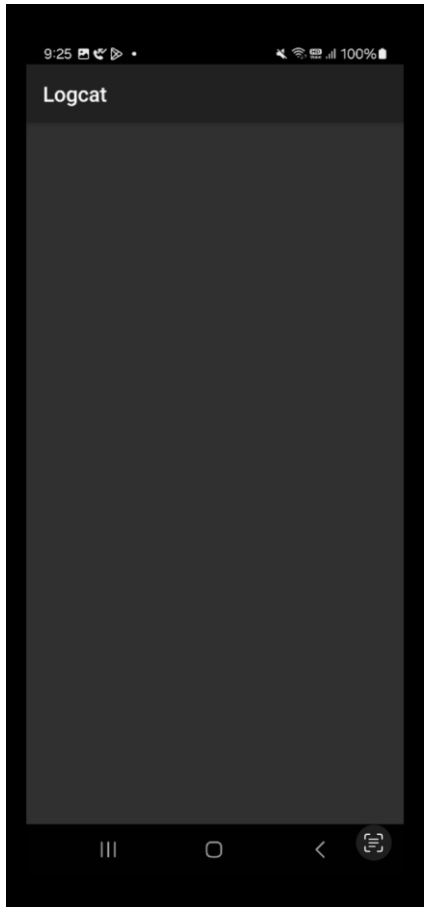
MonitoringService: Anti-Forensic 이벤트 및 로그 처리 Class

작동 화면 및 시연

❖ 작동 화면







작동 화면 및 시연

❖ 시연: Anti-Forensic 관련 부분

- Timestamp 조작, logcat -c, 전원 끄기 및 재부팅, File 메타데이터 조작

1.
```
2025-01-16 20:01:30 Anti-forensic event detected: android.intent.action.TIME_SET
2025-01-16 20:01:30 SystemClockTime: Setting time of day to sec=1737025290764
2025-01-16 20:01:30 Auto time setting enabled: false
2025-01-16 20:01:30 Before System Time : 2025-01-16 20:01:30
```

2.
```
Logcat buffer cleared (logcat -c detected).
```

3.
```
Device shutdown detected
```

4.
```
2025-01-07 20:08:08 MediaStore changed: content://media/external/images/media/1000000856
File Name (DISPLAY_NAME): 20250103_171245.jpg
Relative Path: DCIM/Camera/
Modifed After Date: 2031-12-14 17:12:00
```

작동 화면 및 시연

❖ 시연: APP 관련 부분

- 전화 앱, SMS 앱, 블루투스 앱, 차량 진단 앱, 내비게이션 앱, Android Auto 관련 앱들

```
2025-01-07 19:59:40 Call Type: 발신 통화 시작 Number: 01049232198 Start Time: 2025-01-07 19:59:40 End Time: N/A Duration: 0 seconds
2025-01-07 19:59:47 Call Type: 발신 통화 종료 Number: 01049232198 Start Time: 2025-01-07 19:59:40 End Time: 2025-01-07 19:59:47 Duration: 6 seconds
2025-01-07 20:00:04 Call Type: 수신 전화 울림 Number: 01049232198 Start Time: N/A End Time: N/A Duration: 0 seconds
2025-01-07 20:00:07 Call Type: 수신 통화 시작 Number: 01049232198 Start Time: 2025-01-07 20:00:07 End Time: N/A Duration: 0 seconds
2025-01-07 20:00:09 Call Type: 발신 통화 종료 Number: 01049232198 Start Time: 2025-01-07 20:00:07 End Time: 2025-01-07 20:00:09 Duration: 1 seconds
2025-01-07 20:00:39 Call Type: 수신 전화 울림 Number: 01049232198 Start Time: N/A End Time: N/A Duration: 0 seconds
2025-01-07 20:00:42 Call Type: 수신 전화 거절 또는 받지 않음 Number: 01049232198 Start Time: N/A End Time: N/A Duration: 0 seconds
```

```
2025-01-07 19:59:03 SMS Sent to/from: 01065749080 Message: TEST
2025-01-07 19:59:03 SMS Received to/from: 01065749080 Message: TEST
2025-01-07 19:59:03 SMS Sent to/from: 01065749080 Message: TEST
2025-01-07 19:59:19 SMS Received to/from: 01065749080 Message: TEST
```

03 방학 후 계획

방학 후 계획

❖ 2025년 ~ 2026년 개강 후 계획

- 2025 상반기 화이트햇 스쿨 희망 (학교 수업 병행)
  - 조민혁, 이승민
- 2025 하반기 자격증 및 여러 프로젝트 수행 (휴학)
- 2026 상반기 인턴 희망
- 2026 하반기 BOB 희망
  - 조민혁, 이승민

감사합니다