

# 10/08(화) 78 Research Lab Meeting

2024.09.27

모바일시스템공학과 조민혁

# INDEX

01

Logcat 도구

02

논문 관련

**01**

# Logcat 도구 개발

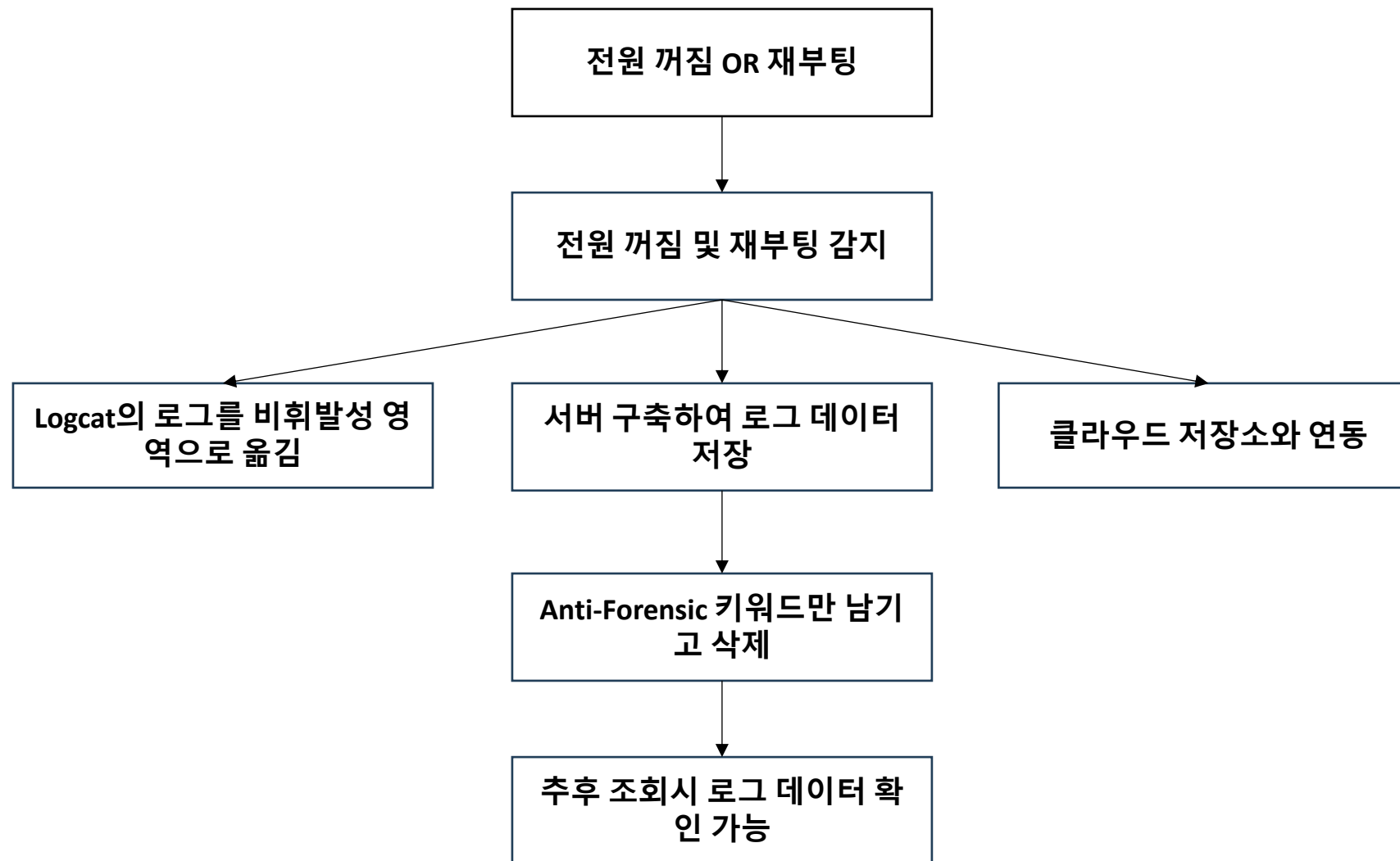
## ❖ Logcat의 문제점

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

## ❖ 목적

- ✓ 휘발성 로그가 재부팅 또는 전원 꺼짐 감지 시 비휘발성 영역으로 옮겨져서 “안티-포렌식” 키워드만 남기고, 삭제한다.
- ✓ 포렌식 수사 관점에서 개발
- ✓ 효율적인 포렌식 수사가 될 수 있도록 기여하는 측면에서 개발

# Logcat 개발 순서도



# 개발 계획

---


## ❖도구 Ver.

- ✓ 프로그래밍 언어: C++
- ✓ 프레임워크: Native C++

## ❖어플 Ver.

- ✓ 프로그래밍 언어: Java
- ✓ 프레임워크: Android SDK, Android Jetpack

\* 추후 공부하면서 수정될 수 있음



**02**

## 논문 확장

## ❖ 논문 주제 :

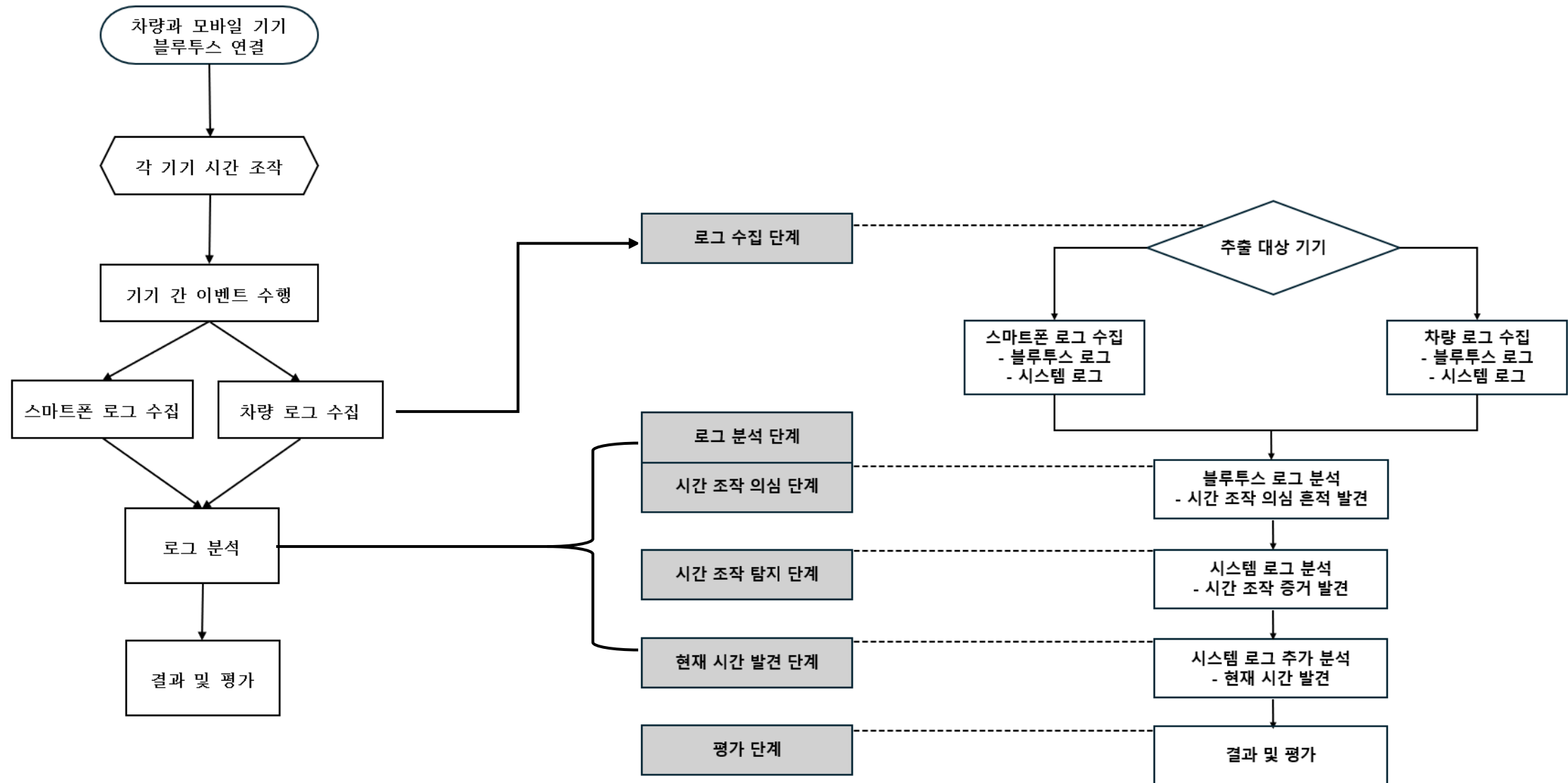
“블루투스로 연결된 스마트폰과 자동차 인포테인먼트 시스템에서의 시간 조작 탐지”

## ❖ 실험 방법 :

- 네트워크 시간 동기화 OFF
- 두 기기 모두 시간 조작
- 로그 수집 및 분석
- 결론 도출



# 해당 논문에서 사용한 프로세스



## ❖ 실험 결과

- 프로세스 절차를 따르면 블루투스 로그에서 이벤트에서의 타임스탬프 변경을 통한 시간 조작 확인 가능
- 시스템 로그에서 **시간 조작 증거 발견 가능**
- 시스템 로그 추가 분석 시 **시간 조작 당시 시간 발견 가능**

## ❖ 한계점

- 블루투스 HCI 스냅 로그 기능이 꺼져 있으면 블루투스 로그 추출 불가

# 논문 확장 관련 궁금한 점

---

Q1) 한계점에 언급된 것 처럼 블루투스 HCI 스냅 로그가 비활성화된 상태에서도 블루투스 로그를 추출할 수 있는 방법이 있는지?

Q2) 만약 스마트폰이나 차량이 파손되면 로그를 추출할 수 있는 방법이 있는지?

Q3) 앞서 제시한 프로세스에 대해 프로그램으로 개발하는 것에 대해 어떻게 생각하시는지?

- 구체적으로는 개발 가능성, 개발 후 해당 프로그램에 대한 가치가 궁금

감사합니다

---