

KSC 발표자료

자동차의 오디오 비디오 내비게이션 시스템에서 마스킹 된 주행 로그 데이터를 복원하는 방법

CSOS lab, Dankook University
김선재 석사연구원, 조성제 교수님
{rlatjswo0824, sjcho}@dankook.ac.kr
<http://securesw.dankook.ac.kr/>

INDEX

1 서론

- AVN 시스템의 로그 데이터 및 문제점
- 본 연구의 목표

2 관련 연구

- 관련 연구
- 관련 연구들과의 차별성

3 데이터 수집 및 분석 방법

- 데이터 수집
- 마스킹 된 데이터 분석 및 복원

4 결론

5 향후 연구 방향

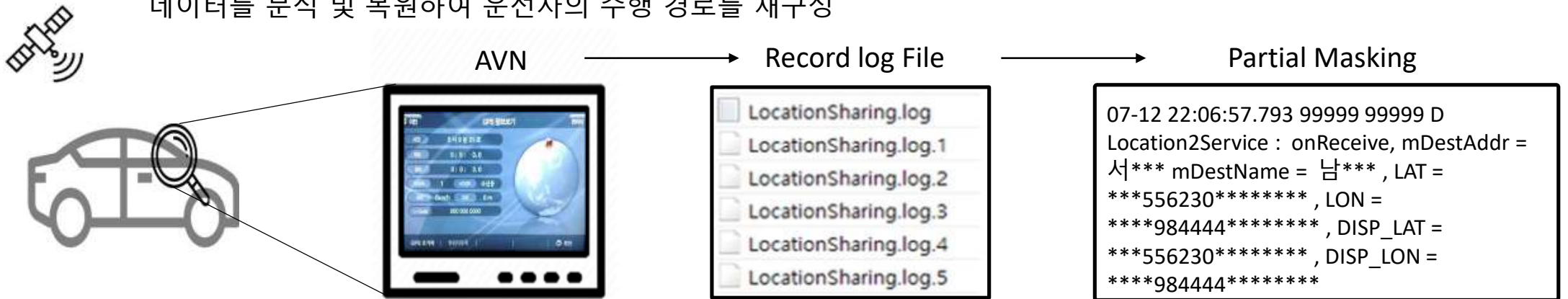
서론

✓ AVN 시스템의 로그 데이터 및 문제점

- 최신 자동차의 AVN(Audio Video Navigation) 시스템은 GPS(Global Positioning System)나 GNSS(Global Navigation Satellite System)를 기반으로 **운전자의 위치 데이터를 비휘발성 로그 파일로** 기록
 - AVN 기능: 경로 안내, 실시간 교통 정보 제공, 예상 도착 시간 산출..
- 최근 개인정보 보호와 보안의 중요성이 대두되면서, 안드로이드 킷캣 버전(KITKAT Ver) AVN 시스템에 기록되는 로그 데이터 중 민감한 정보는 **마스킹(Masking)**되어 기록
- 개인의 민감한 정보를 보호할 수는 있지만, 디지털포렌식 및 자동차 사고조사 관점에서는 운전자의 정확한 위치 정보와 이동 경로를 파악하는데 어려움

✓ 본 연구의 목표

- 본 연구에서는 2022년형 KIA 3세대 K5 차량에 탑재된 안드로이드 킷캣 버전 기반 AVN 시스템에서 마스킹된 주행 로그 데이터를 분석 및 복원하여 운전자의 주행 경로를 재구성



관련 연구

✓ Kang, Haein, et al.

- 현대 기아 차량의 Android Jellybean 및 KitKat 버전 기반 AVN 시스템을 분석하며, 일부 로그 데이터가 암호화되어 분석이 어렵다는 문제 제기

✓ Yoon, Yejin, et al.

- 기아 차량의 Android Jellybean 기반 AVN 시스템을 대상으로 디지털 포렌식 분석을 수행
- 엔지니어링 모드에서 시스템(System) 로그와 내비(NAVI)로그를 수집하여 운전자의 주행 경로 재구성

✓ Verma, Robin, et al.

- DF.20 프레임워크를 통해 포렌식 과정에서 비마스킹 데이터와 관련된 프라이버시 문제를 해결하는 방안 제시
- 머신러닝을 활용하여 비마스킹된 데이터를 자동 분석 및 처리하며, 디지털 포렌식의 프라이버시와 효율성을 높이는 방법 제시

✓ Stammler, Matthias, et al.

- 차량 통신 시스템에서 발생하는 마스킹 문제를 해결하기 위한 모델과 하드웨어 생성 기법 제안
- 마스킹된 데이터 흐름을 추적하고 의심스러운 정보 흐름을 탐지하는 방법을 통한 차량 네트워크 보안 강화

관련 연구

✓ 관련 연구들과의 차별성

- 기존 연구들은 대부분 비마스킹된 데이터를 활용하거나 마스킹으로 인한 분석의 한계를 강조
- 본 연구는 마스킹된 데이터를 복원하여 주행 경로를 재구성하는 방법론을 제시
- Android KitKat 기반 AVN 시스템의 주행 로그 데이터를 복원함으로써 디지털 포렌식과 자동차 사고 조사의 실효성을 높이는 접근법 제시

데이터 수집 및 분석 방법

✓ 데이터 수집

- AVN 시스템으로부터 로그 데이터를 수집하기 위해, 숨겨진 기능인 **엔지니어링 모드**에 진입
- 해당 모드에 진입 후 USB 포트에 드라이브를 삽입하여 **논리적 추출 방식**으로 AVN의 시스템 로그를 USB로 복사

포렌식 대상 시스템



AVN

차종	KIA 3 rd Generation K5
연식	2022
운영체제	Android 4.4.2(KitKat)
커널 버전	Linux 3.18.24-tcc

데이터 수집 방법



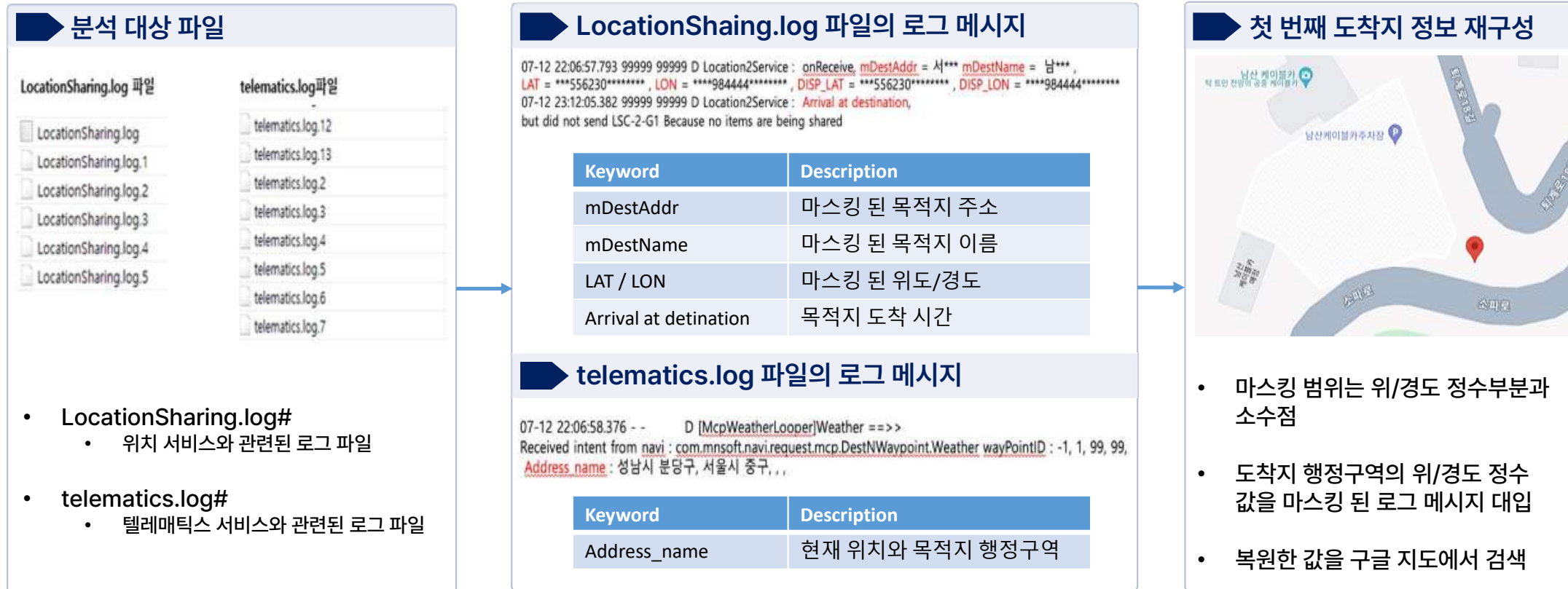
- 숨겨진 기능인 엔지니어링 모드 진입
- USB Copy 메뉴 진입
- Copy to USB에서 Copy Logs to USB Click

논리적 추출

데이터 수집 및 분석 방법

✓ 마스킹 된 데이터 분석 및 복원

- 수집한 로그 데이터는 디지털 포렌식 도구인 Autopsy와 구글 지도를 사용하여 분석



데이터 수집 및 분석 방법

☑ 마스킹 된 데이터 분석 및 복원

▶ 두 번째 도착지 정보 재구성

LocationSharing.log 파일의 로그 메시지

```
07-12 23:20:18.325 99999 99999 D Location2Service: onReceive, mDestAddr = 서*** mDestName = 현***, LAT = ***522069***, LON = ***94085***, DISP_LAT = ***522069***, DISP_LON = ***94085***
07-12 23:41:48.648 99999 99999 D Location2Service: Arrival at destination, but did not send LSC-2-G1 Because no items are being shared
```

telematics.log 파일의 로그 메시지

```
07-12 23:12:18.642 -- D [McpWeatherLooper]Weather ==>> Received intent from navi: com.mnsoft.navi.request.mcp.DestWaypoint.Weather wayPointID: -1, 99, 99, Address_name: 서울시 중구, ...
07-12 23:20:18.874 -- D [McpWeatherLooper]Weather ==>> Received intent from navi: com.mnsoft.navi.request.mcp.DestWaypoint.Weather wayPointID: -1, 1, 99, 99, Address_name: 서울시 용산구, 서울시 영등포구, ...
```



▶ 비마스킹 된 로그 메시지

```
07-12 23:21:27.318 -- D [CMM]VI-185 wdWStatus: 2 1 1 1 37.55266944 126.9822805 0 202
```



```
07-12 23:31:29.577 -- D [CMM]VI-185 wdWStatus: 1 1 1 1 37.53836944 126.9871027 0 255
```



✓ 비마스킹 된 현재 위치 로그는 복원한 주행 경로가 맞는지 검증에 필요

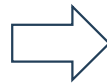
데이터 수집 및 분석 방법

☑ 마스킹 된 데이터 분석 및 복원

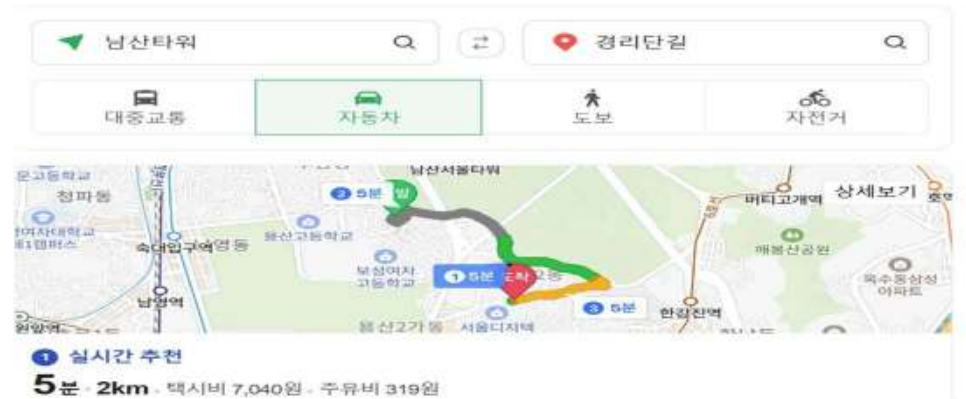
복원된 운전자 주행 경로



- 22 : 06경 성남시 분당구에서 출발
- 11 : 12경 남산케이블카주차장 도착
- 11 : 20경 서울 한강 파라다이스로 출발
- 11 : 31경 이태원 경리단길 지남
- 23 : 41경 서울 한강 파라다이스 도착



이동 시간 검증



결론

✓ 마스킹된 위도 및 경도 데이터 복원

- 로그 데이터의 패턴 분석과 시간적 상관관계 분석을 통한 마스킹된 데이터 복원

✓ 주행 경로 재구성

- 복원된 데이터를 기반으로 운전자의 실제 주행 경로를 시각적으로 재구성하여 디지털 포렌식 작업의 실효성 증가

✓ 디지털 포렌식 활용 가능성 증대

- 본 연구는 차량 사고 조사 혹은 범죄자의 주행 경로 조사와 같은 차량 디지털 포렌식 작업에서 마스킹된 데이터 문제를 해결하는 새로운 접근법 제시

향후 연구 방향

✓ 로그 분석 자동화

- 머신러닝 및 AI 기반 자동화 기술을 활용하여 로그 분석 및 복원 과정 효율화
- 분석 시간 단축과 데이터 복원 정확성 향상

✓ 다양한 차량 모델에 대한 확장 연구

- 다양한 차량 모델 및 AVN 시스템에서 로그 데이터를 수집 및 분석하여 연구 방법론의 일반화
- 각 차량 모델에서 발생하는 로그 데이터의 차이를 비교하여 복원 기법의 적용 가능성 확장

✓ 비마스킹 데이터 기록 조건 분석

- 일부 비마스킹된 데이터가 기록되는 조건과 주기를 규명하여 더 정밀한 주행 경로 복원
- 특정 트리거와 로그 메시지 출력 간의 상관관계를 분석하여 데이터 복원 과정 정밀화

Thank you

- Q&A -
