

안드로이드 기반 차량 인포테인먼트 시스템에서 로그 데이터에 대한 안티포렌식 기법 분석

단국대학교

운영체제 및 보안 연구실

석사 과정 김선재

<http://secursw.dankook.ac.kr/>

INDEX

1 연구 배경 및 목표

2 포렌식 절차

3 데이터 수집 단계

4 데이터 조사 단계

5 데이터 분석 단계

6 결론 및 향후 연구

01

연구 배경 및 목표

연구 배경 및 목표

✓ 연구 배경

- 차량 인포테인먼트(In-vehicle Infotainment, IVI) 시스템은 차량 운행 중 발생하는 다양한 상태 정보, 사용자 상호작용, 네트워크 연결 기록 등을 로그로 저장
- 다수의 현대 및 기아차는 안드로이드 킷캣(Android KitKat) 기반의 IVI 시스템을 장착
- 킷캣 기반의 IVI 시스템에서 관리하는 일부 로그 데이터에 대해 개인정보보호를 위해서 데이터 마스킹 또는 인코딩 등의 **비식별화(de-identification)** 기법이 적용되며, 이러한 비식별화 기법을 **안티 포렌식(Anti-forensic) 기법의 일종**으로 간주
 - 데이터 은닉
 - 데이터 삭제
 - 데이터 조작
- 안티포렌식 기법이 적용된 상황에서 포렌식 분석의 정확도를 높일 필요가 있음

✓ 본 연구의 목표

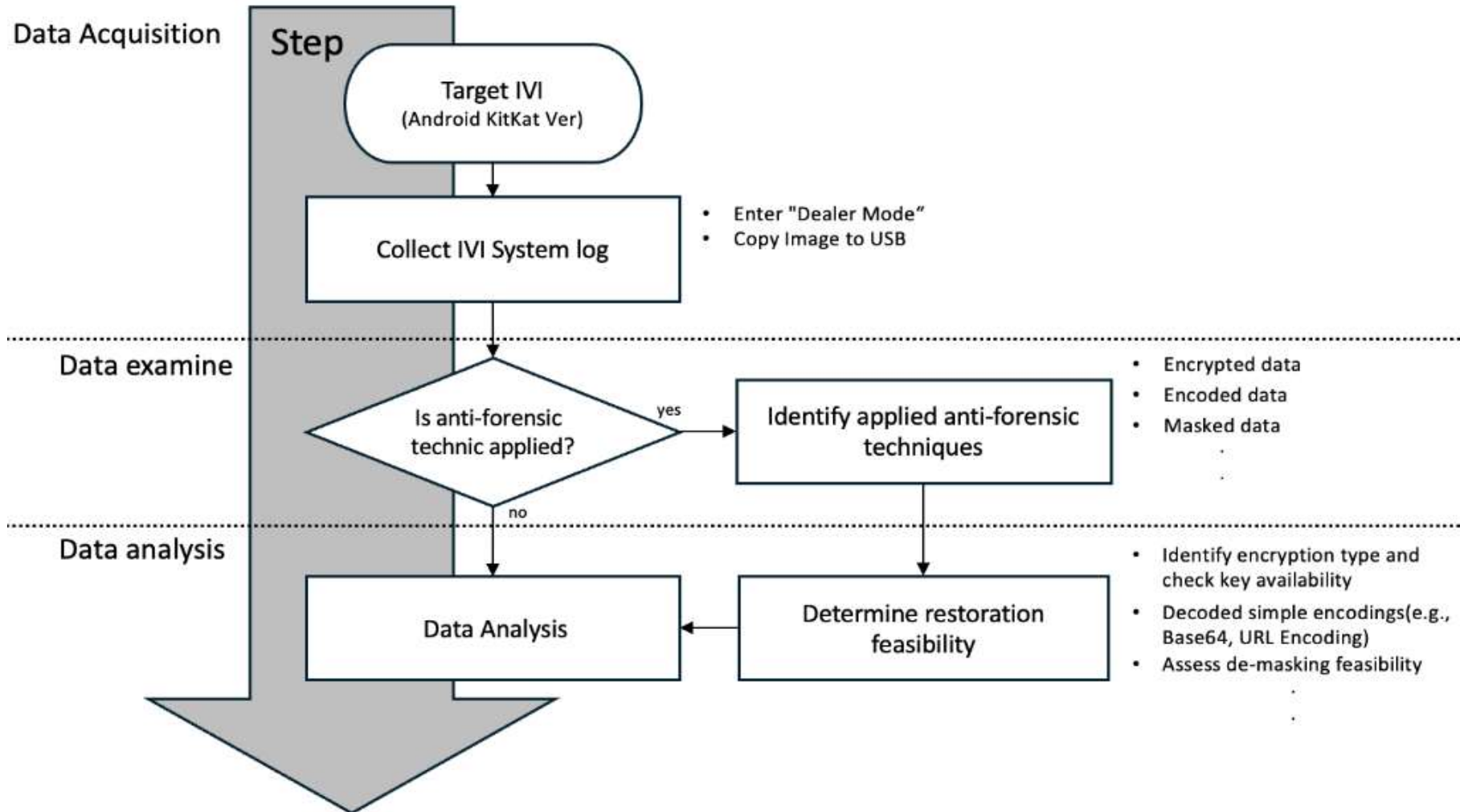
- 현대차 및 기아차에 장착되어 있는 안드로이드 킷캣 기반 IVI 시스템의 로그 데이터를 대상으로, 안티포렌식 기법이 적용된 데이터를 조사 및 분석하는 포렌식 프로세스를 제안

02

포렌식 절차

포렌식 절차

✓ 안티포렌식 기법이 적용된 로그 데이터 조사 및 분석 절차





03

데이터 수집 단계

데이터 수집 단계

✓ 데이터 수집 방법

- IVI 시스템의 숨겨진 기능인 딜러 모드에 진입
- "Copy Image to USB(USB로 이미지 복사)" 메뉴를 활용하여 시스템 로그 수집
- 물리적 손상 없이 논리적 방식으로 추출



04

데이터 조사 단계

데이터 조사 단계

✔ 안티포렌식 기법이 적용된 데이터

- 본 연구에서 조사한 데이터는 표와 같음
- 마스킹 데이터와 인코딩 데이터 존재

Data type	Artifacts	Filename
Masking	목적지 주소, 목적지 이름, 목적지 위도 경도	LocationSharing.log.#
		bluetoothLofFilter.log.#
	차량 식별 번호(VIN)	LocationSharing.log.#
		mofgen2.log.#
		telematics.log.#
		otaclient_#.txt
	네트워크 접근 디바이스 식별자(NADID)	LocationSharing.log.#
		mofgen2.log.#
Encoding	목적지 설정 시점의 차량 위치 및 목적지명	telematics.log.#



05

데이터 분석 단계

데이터 분석 단계: 주행 경로 재구성

✓ 인코딩 데이터 분석 및 복원(터치스크린으로 목적지 주소를 설정한 경우)

인코딩 된 로그 메시지 - telematics.log.# 파일 분석

07-12 22:06:43.294 - - D [LOS][Navi -> I-BOX] intent action : com.hkmc.telematics.gis.action.REQUEST_CENTER_JSON,
com.hkmc.telematics.gis.extra.SERVICE_TID : , com.hkmc.telematics.gis.extra.HOST : HLOS, com.hkmc.telematics.gis.extra.SERVICE_URI : /gis2/los/hmns,
com.hkmc.telematics.gis.extra.JSON : {

"body" :

"eyJrZXI3b3Jkljoi64Ko7IKw7LyA7J2067iU7Lm07KO87LCo7J6lIiwibG9uIjoxMjcuMTAxNzc3Nzc3Nzc3Nzc3ImxhdCI6MzcuMzU4ODEzODg4ODg4ODksInNvcnQiOiJ
MslmZyb20iOjAsInNpemUjUwLCJyc3BWZXIiOiIyMDI0MDEiLCJ2ZWhpY2xlQ29kZSI6IklDRSIsInZlaGljbGVCCmFuZCI6ImtpYSIsImxhbmd1YWdlIjozLCJyZW1vd
mVDCExpc3QiOiSC1SZXN0YXVYVW50Il19",

"service" : "unified-search"

}



디코딩 결과

{"keyword":"남산케이ابل카주차장","lon":127.10177777777777,"lat":37.35881388888889,"sort":3,"from":
"vehicleBrand":"kia","language":3,"removeCpList":["H-Restaurant"]}

목적지 설정 시 운전자의 위치



데이터 분석 단계: 주행 경로 재구성

☑ 마스킹 데이터 분석 및 복원(행정구역 정보 기반 복원)

▶ 분석 대상 파일

LocationSharing.log 파일

- LocationSharing.log
- LocationSharing.log.1
- LocationSharing.log.2
- LocationSharing.log.3
- LocationSharing.log.4
- LocationSharing.log.5

telematics.log 파일

- telematics.log.12
- telematics.log.13
- telematics.log.2
- telematics.log.3
- telematics.log.4
- telematics.log.5
- telematics.log.6
- telematics.log.7

- LocationSharing.log#
 - 위치 서비스와 관련된 로그 파일
- telematics.log#
 - 텔레매틱스 서비스와 관련된 로그 파일

▶ LocationShaing.log 파일의 로그 메시지

```
07-12 22:06:57.793 99999 99999 D Location2Service: onReceive, mDestAddr = 서***, mDestName = 남***,  
LAT = ***556230***, LON = ****984444***, DISP_LAT = ***556230***, DISP_LON = ****984444***  
07-12 23:12:05.382 99999 99999 D Location2Service: Arrival at destination,  
but did not send LSC-2-G1 Because no items are being shared
```

Keyword	Description
mDestAddr	마스킹 된 목적지 주소
mDestName	마스킹 된 목적지 이름
LAT / LON	마스킹 된 위도/경도
Arrival at detination	목적지 도착 시간

▶ telematics.log 파일의 로그 메시지

```
07-12 22:06:58.376 -- D [McpWeatherLooper]Weather ==>>  
Received intent from navi : com.mnsoft.navi.request.mcp.DestNWaypoint.Weather wayPointID : -1, 1, 99, 99,  
Address name : 성남시 분당구, 서울시 중구,,
```

Keyword	Description
Address_name	현재 위치와 목적지 행정구역

▶ 첫 번째 도착지 정보 재구성



- 마스킹 범위는 위/경도 정수부분과 소수점
- 도착지 행정구역의 위/경도 정수 값을 마스킹 된 로그 메시지 대입
- 복원한 값을 구글 지도에서 검색

데이터 분석 단계: 주행 경로 재구성

☑ 마스킹 데이터 분석 및 복원(행정구역 정보 기반 복원)

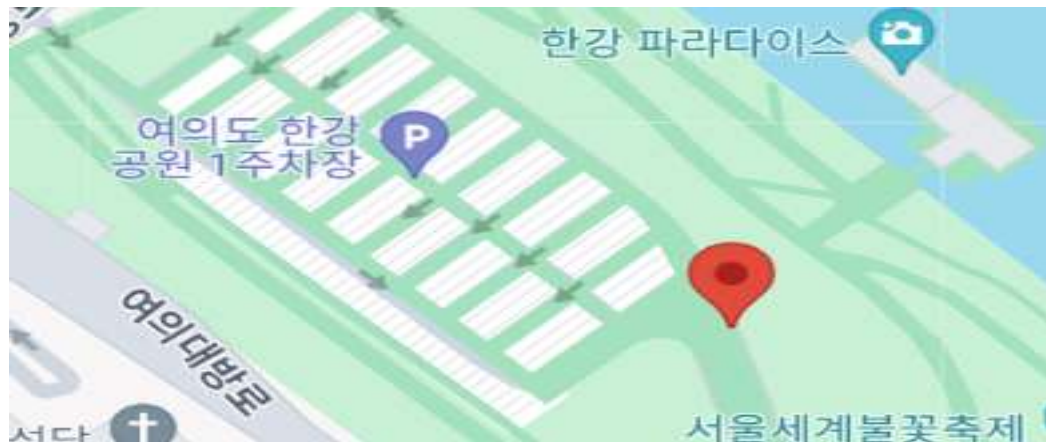
▶ 두 번째 도착지 정보 재구성

❖ LocationSharing.log파일 분석

```
07-12 23:20:18.325 99999 99999 D Location2Service : onReceive, mDestAddr = 서*** mDestName = 한***, LAT = ***522069*****, LON = ***94085*****, DISP_LAT = ***522069*****, DISP_LON = ***94085*****
```

❖ telematics_log.txt 파일 분석

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

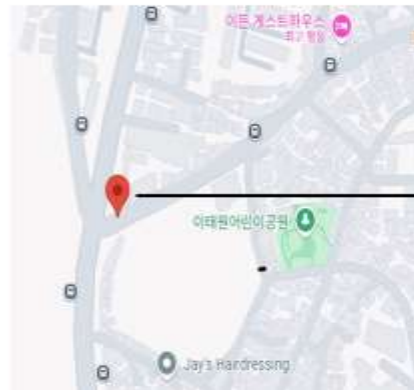


▶ 비마스킹 된 로그 메시지

```
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

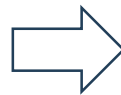
데이터 분석 단계: 주행 경로 재구성

☑ 마스킹 데이터 분석 및 복원(행정구역 정보 기반 복원)

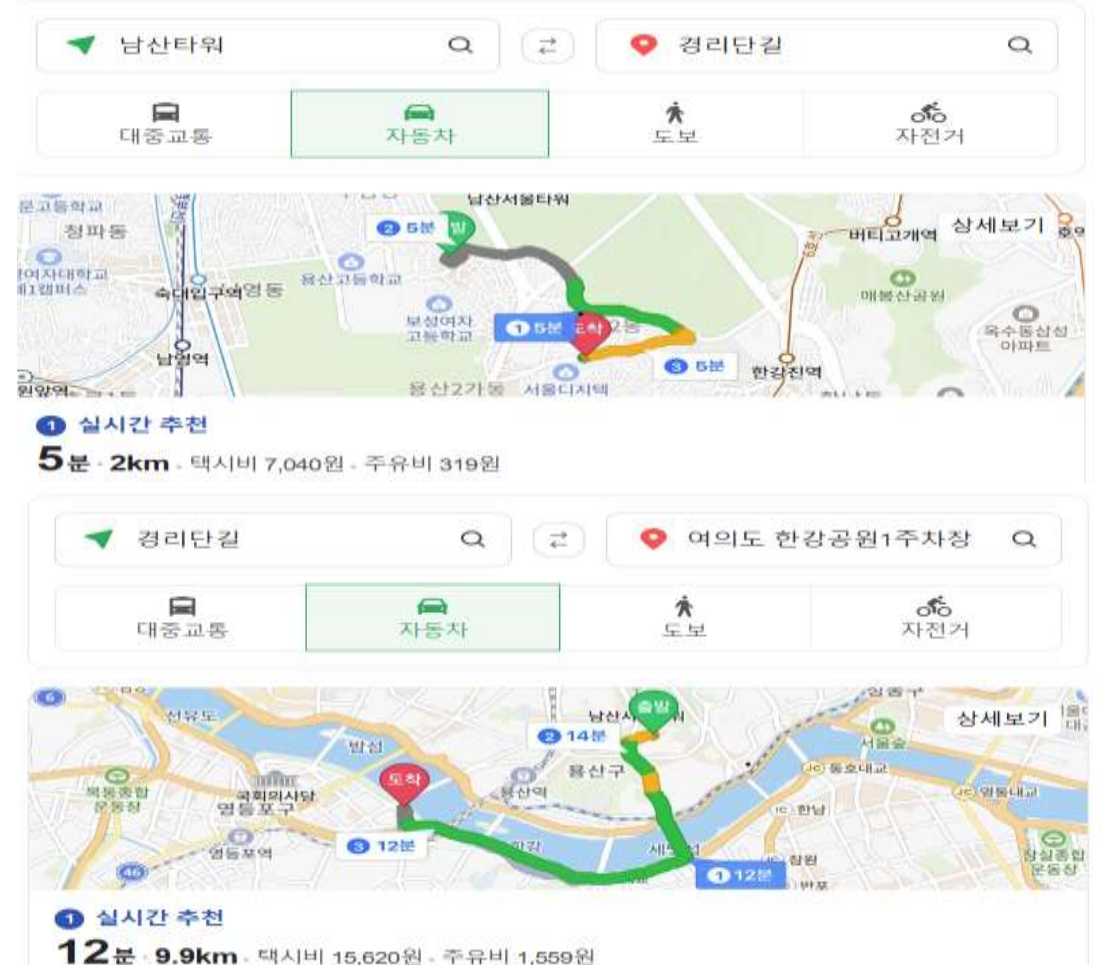
복원된 운전자 주행 경로



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



이동 시간 검증



데이터 분석 단계: 주행 경로 재구성

마스킹 데이터 분석 및 복원(음성 데이터 기반 복원)

VR_ENGINE_START.dat 파일 분석

TIMA RESULT :: 보정역 복지 센터:
TIMA REQUIRED RESULT TIME:: 002s 814ms
ENGINE RESULT :: 보정역 복지 센터_9999

음성으로 입력한 목적지

ENGINE PARAMETER :: LH_FX_PARAM_START_ENABLE:: 1 | LH_FX_PARAM_SENSITIVITY:: 50 | LH_FX_PARAM_ABSOLUTE_THRESHOLD:: -2000 | LH_FX_PARAM_MINSPEECH:: 60 | LH_FX_PARAM_TSILENCE:: 500 | LH_FX_PARAM_AGC:: 0 | LH_FX_PARAM_FARTALK:: 1 | LH_FX_PARAM_TSILENCE:: 0 | LH_FX_PARAM_TIMEOUT_SPEECH:: 0 | LH_FX_PARAM_EVENT_TIMER:: 0 | LH_FX_PARAM_KNOWN_SPEAKER_CHANGES:: 1 | LH_FX_PARAM_FIX_WARPFACOR:: 6 |
ENGINE SNR :: 5067

BT STATUS :: 0xf93d5b3f (CONNECTED/UPDATED)
[1] G: F:내 이름 ^
[2] G:정연수, F: ^
[3] G:testHuman_1, F: ^
[4] G:안균승, F: ^
[5] G: F:내 이름 ^

핸드폰 연락처 이름

TALK START TIME :: 2024 11-21 19:07:04
PROMPT START TIME :: 2024 11-21 19:07:05

음성 명령 기능 활성화 시간

BEEP START TIME ::
MIC OPEN TIME ::
MIC DIALOG ID :: 56
BARGEIN FLAG :: 0
SOFTWARE VERSION :: CN7.KOR.S5W_M.V034.001.240821^CN7.KOR.301.240423.MICOM.D^KOR.17.47.49.000.511.0
OUTSIDE INFO ::

```
def make_wav_format(pcm_data:bytes, ch:int) -> bytes:
    """
    pcm_data를 통해서 wav 헤더를 만들고 wav 형식으로 저장
    :param pcm_data: pcm bytes
    :param ch: 채널 수
    :return wav: wave bytes
    """
    waves = []
    waves.append(struct.pack('<4s', b'RIFF'))
    waves.append(struct.pack('I', 1))
    waves.append(struct.pack('4s', b'WAVE'))
    waves.append(struct.pack('4s', b'fmt '))
    waves.append(struct.pack('I', 16))
    # audio_format, channel_cnt, sample_rate, bytes_rate(sr*blockalign:초당 바이트수), block_align, bps
    if ch == 2:
        waves.append(struct.pack('HHIIHH', 1, 2, 16000, 64000, 4, 16))
    else:
        waves.append(struct.pack('HHIIHH', 1, 1, 16000, 32000, 2, 16))
    waves.append(struct.pack('<4s', b'data'))
    waves.append(struct.pack('I', len(pcm_data)))
    waves.append(pcm_data)
    waves[1] = struct.pack('I', sum(len(w) for w in waves[2:]))
    return b''.join(waves)

import struct
import pathlib

pcm_bytes = pathlib.Path(r"C:\Users\qpslx\Desktop\VR_ENGINE_START_12.pcm").read_bytes()
wav_bytes = make_wav_format(pcm_bytes, 1)
with open('sample2.wav', 'wb') as file:
    file.write(wav_bytes)
```

/Error_Log/error_vr/VR_ENGINE_START.pcm



Python code로 파일 변환

/Error_Log/error_vr/VR_ENGINE_START.wav



데이터 분석 단계: 블루투스 통신 데이터

✔ 마스킹 된 상대방 전화번호 및 이름

- bluetoothLogFile.log 파일에는 IVI 시스템과 블루투스로 연결된 휴대전화의 활동 기록이 저장
- 전화 시, 상대방 이름과 전화번호 항목이 동일 파일 내에 마스킹된 값과 비마스킹된 값이 혼재된 형태로 저장
- 일부 항목이 그대로 노출된 채 저장된 점은 비식별화 처리의 일관성 부족 또는 기술적 불완전성을 의미

Filename	Artifacts	Log Message
bluetoothLofFilter.log	Caller Name	11-21 19:11 IUpdateCallerNameToCluster 2 , name = 홍길동
	Masked Caller Name	11-21 19:11 callerinfo name--->홍***
	Caller Number	11-21 19:11 [BTHF] IUpdateCallerNameToCluster 2 , number = 01012345678
	Masked Caller Number	11-21 19:11 Incoming number 0101234***

데이터 분석 단계: 차량 정보 데이터

✓ 마스킹 된 VIN, NADID

- 차량식별번호(VIN)과 네트워크 접근 디바이스(NADID)는 단일 파일이 아닌 복수의 로그 파일에 걸쳐 서로 다른 형식으로 기록
- 파일 간 정보를 결합하면 마스킹된 값의 일부를 식별할 수 있는 형태로 나타남
- VIN 구조상 제조사/차체형상/안전장치 등 식별 패턴을 통해 KMHLL41EPU**3515와 같은 형태로 원래 값을 상당 부분 복원할 수 있는 가능성 존재

Filename	Artifacts	Log Message
LocationSharing.log.#	VIN	VIN: *****3515
mofgen2.log.#		VIN: *****3515
telematics.log.#		VIN: *****3515
otaclient_#.txt		VIN:KMHLL**EPU*****
LocationSharing.log.#	NADID	NADID : [*****]
mofgen2.log.#		NADID : [*****2619]



06

결론 및 향후 연구

결론 및 향후 연구

✓ 결론

- 안드로이드 기반 IVI 시스템에서는 개인정보보호를 위해 일부 데이터에 비식별화 기법이 적용됨
- 분석 결과, 적용된 비식별화 기법은 상대적으로 낮은 수준의 보안성으로 평가됨
- 비식별화 된 데이터임에도 불구하고 일부 정보가 추론 또는 복원이 가능

✓ 향후 연구 방향

- 다양한 차량 모델 및 시스템 버전을 대상으로 비식별화 기법의 수준을 정량적으로 평가할 예정
- IVI 로그 데이터의 실시간 수집 및 처리 환경을 고려한 현장 적용 가능한 도구 개발

Q&A

Thank you !

컴퓨터보안 및 OS 연구실
rlatjswo0824@dankook.ac.kr

<http://securesw.dankook.ac.kr/>