

IVI 엔지니어링 모드를 활용한 차량 로그 데이터 수집 및 디지털 포렌식 분석

2025 한국자동차공학회 춘계학술대회

정지현, 조성제

컴퓨터보안&OS연구실 (CSOS Lab)

INDEX

01

서론

02

IVI 시스템 포렌식 절차

03

결론 및 향후 연구



01

서론

서론

❖ 디지털 포렌식이란?

- 전자적으로 저장된 데이터를 식별, 획득, 처리, 분석 및 보고하는데 중점을 둔 Forensic Science의 한 분야
[ref: INTERPOL | The International Criminal Police Organization]
- 정보의 무결성을 보존하고 데이터에 대한 CoC(Chain of Custody, 증거물 관리의 연속성)을 유지하면서, 데이터의 Identification, collection, examination and analysis에 과학을 적용하는 것
[ref: NIST | National Institute of Standards and Technology]

❖ 디지털 포렌식의 범위 확장

- 컴퓨터, 모바일, 사물인터넷(IoT), **스마트카**



연구 목적

❖ 운전자와 상호작용이 많은 차량용 인포테인먼트 시스템에 축적되는 데이터의 양 증가

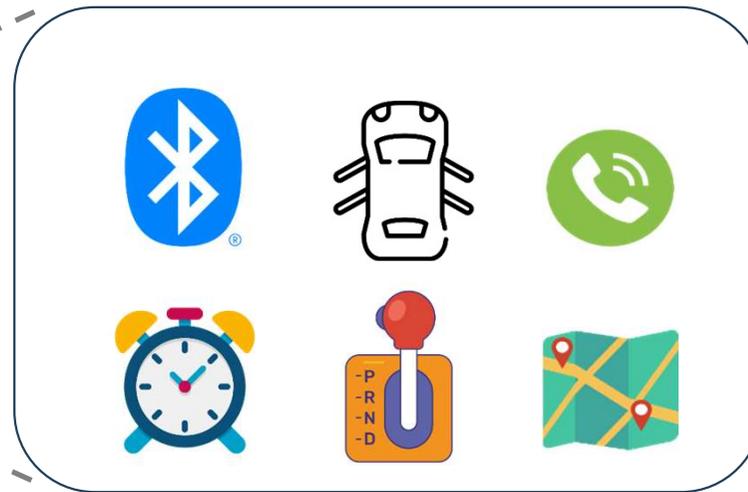
▪ IVI(=In-Vehicle Infotainment), AVN(=Audio Video Navigation)

• 내비게이션, 전화 통화, 음악 재생 등

▪ 차량 상태 정보와 외부 기기와의 상호작용 기록

• 블루투스 연결 이력, 문 개폐 상태, 위치 정보, 기어 변속 등

❖ 차량 인포테인먼트 시스템의 로그 데이터를 기반으로 차량 포렌식 수행



관련 연구 (가능한 강해인의 Applied sciences 논문과 윤예진의 ARES 논문으로 대체)

[1] “차량 디지털 포렌식에서 타임라인 분석을 위한 안드로이드 기반 오디오 비디오 내비게이션 시스템의 로그 활용”

강해인 등, KCC 2023

대상 시스템	KIA Morning Urban AVN 시스템(OS: 안드로이드 4.4.2 KitKat)
수집 방법	딜러 모드 진입 후, 로그 덤프 수행
분석 방법	Autopsy 사용
아티팩트	블루투스 맥 주소, 라디오 채널 명, 팟 캡스트 앱 실행 기록, 전화 연결한 전화번호

[2] “A Preliminary Forensics Analysis of Navigation Records on an Android-based Audio-Video Navigation System”

Seong et al, The 7th International Conference on Next Generation Computing 2021

대상 시스템	KIA Niro EV & KIA K5 AVN 시스템(OS: 안드로이드 4.2.2 Jellybean)
수집 방법	엔지니어링 모드 진입 후, ADB 연결하여 dd 명령어 수행
분석 방법	X-ways forensics, Autopsy, DB4S, HxD, Epoch Converter, Talmap 사용
아티팩트	(최근, 즐겨찾기, 등록된, 마지막으로 검색한) 위치정보, 블루투스 맥 주소, 전화번호부, 전화 기록

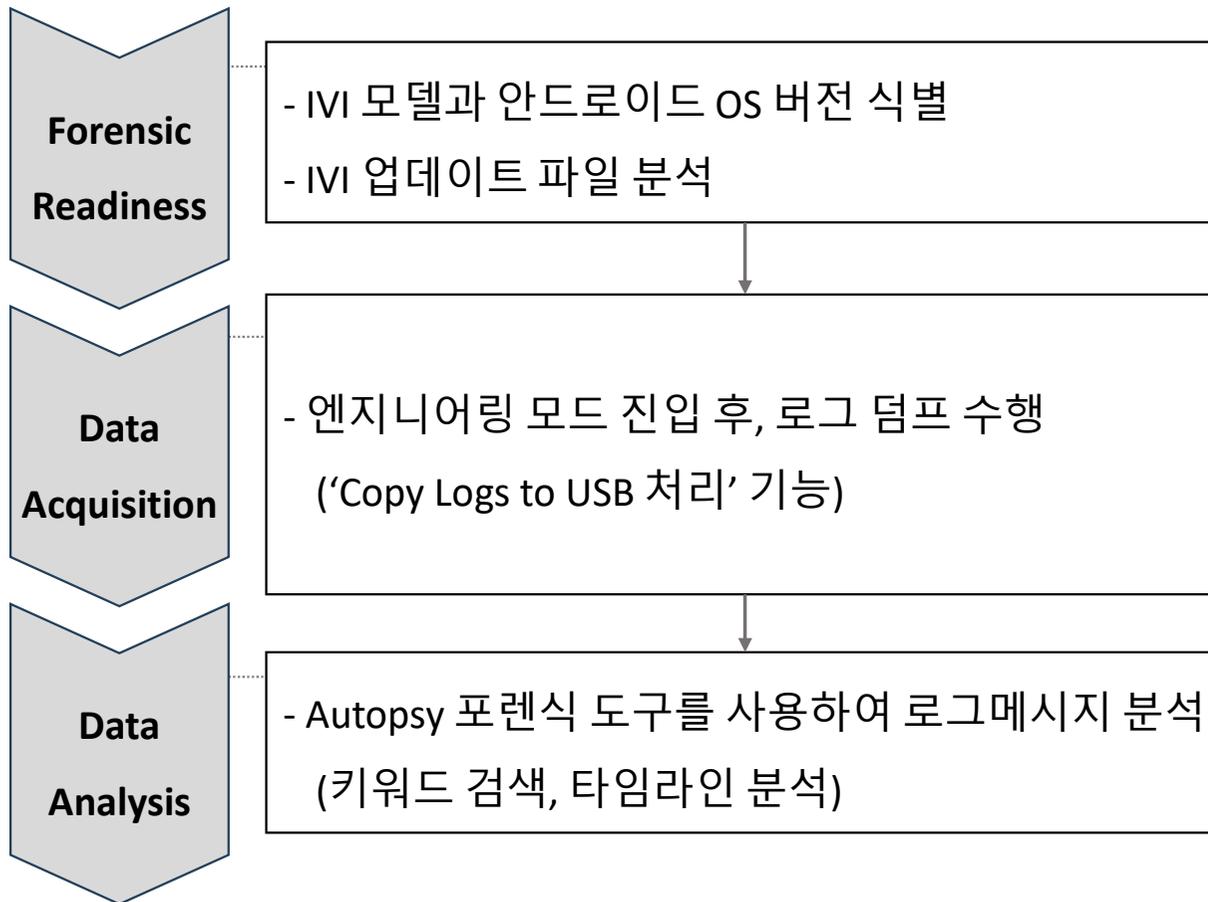


02

IVI 시스템 포렌식 절차

IVI 시스템 포렌식 절차

❖ IVI 시스템 포렌식 절차



IVI 시스템 포렌식 절차

Forensic Readiness

Data Acquisition

Data Analysis

❖ Forensic Readiness

- IVI 모델과 세대 그리고 안드로이드 OS 버전 식별



AVN	
차종	KIA Sorento (2016)
운영체제	Android 2.3.4 (Gingerbread)
세대	표준형 4세대
모델명	AT210C5DG, 15Y 2ND

IVI 시스템 포렌식 절차

Forensic Readiness

Data Acquisition

Data Analysis

❖ Forensic Readiness

- IVI 업데이트 파일 분석

1. SD카드에서 업데이트 이미지 획득

- .fseventsd
- .Spotlight-V100
- .TemporaryItems
- DATA
- swversion
- update
- vr
- All_New_SORENTO_UVO.ver
- HKMC_Navi.apk
- HKMC_Navi_ST4.apk

- ✓ IVI 시스템의 SD 맵 슬롯에 삽입된 SD 카드 식별
- ✓ SD 카드로부터 업데이트 이미지 파일 획득

2. 파일 시스템 이미지 추출 및 탐색

```

$ file system.img
system.img: Linux rev 1.0 ext4 filesystem data, UUID=53542e55-4d2e-4535-3336-2e0000000000, volume name "SYS.KR.181209" (extents) (large files)

$ 7z x system.img -o./extracted_system.img
7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=C.UTF-8 Threads:20 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 313524224 bytes (299 MiB)

Extracting archive: system.img
--
Path = system.img
Type = Ext
Physical Size = 313524224
Cluster Size = 4096
Free Space = 59887616
Host OS = Linux
Revision = 1
inode Size = 256
Code Page = UTF-8
Label = SYS.KR.181209
ID = 53542E554D2E45353362E000000000
Characteristics = HAS_JOURNAL RESIZE_INODE
Incompatible Features = FILETYPE EXTENTS
ReadOnly-compatible Features = SPARSE_SUPER LARGE_FILE

Everything is Ok

Folders: 57
Files: 778
Size: 24633491
Compressed: 313524224
    
```

- ✓ 이미지 파일 내에서 파일 시스템 이미지를 식별
- ✓ 7z 명령어를 사용하여 추출 및 마운트

3. Setting.dex 파일 리버싱 및 분석

```

public void onCreate(Bundle savedInstanceState) {
    View v = inflater.inflate(R.layout.storage_memory, ViewGroup.LayoutParams.MATCH_PARENT, true);
    this.findViewById(R.id.right_door_for_engineering_mode);
    this.findViewById(R.id.right_door_for_engineering_mode);
    this.findViewById(R.id.right_door_for_engineering_mode);
    public boolean onTouch(View v, MotionEvent event) {
        if (event.getAction() == MotionEvent.ACTION_DOWN) {
            if (StorageMemoryFragment.this.mLeftDoorKnockCount == 0) {
                CountdownTimer unused = StorageMemoryFragment.this.timerForEngineeringMode = new CountdownTimer(3000, 1000) {
                    public void onFinish() {
                        int unused = StorageMemoryFragment.this.mLeftDoorKnockCount + 1;
                        boolean unused2 = StorageMemoryFragment.this.mLeftDoorOpen = true;
                    }
                };
                return true;
            }
            this.mRightDoorForEngineeringMode.setOnTouchListener(new View.OnTouchListener() {
                public boolean onTouch(View v, MotionEvent event) {
                    if (event.getAction() == MotionEvent.ACTION_DOWN) {
                        if (StorageMemoryFragment.this.mLeftDoorOpen) {
                            Intent i = new Intent("android.intent.action.MAIN");
                            i.setClassName("com.hmc.system.app.engineering", "com.hmc.system.app.engineering.EngineeringModeMainActivity");
                            StorageMemoryFragment.this.startActivity(i);
                        }
                    }
                }
            });
            boolean unused = StorageMemoryFragment.this.timerForEngineeringMode.cancel();
            int unused2 = StorageMemoryFragment.this.mLeftDoorKnockCount + 1;
            return true;
        }
    }
}
    
```

- 1. 왼쪽 도어 3초 이내에 5번 클릭
- 2. 오른쪽 도어를 1번 터치
- 3. 엔지니어링 모드 활성화

- ✓ Settings.odex 파일을 역공학 도구를 통해 디컴파일
- ✓ 내부 코드를 분석하여 엔지니어링 모드의 진입 조건 및 작동 흐름을 확인

IVI 시스템 포렌식 절차

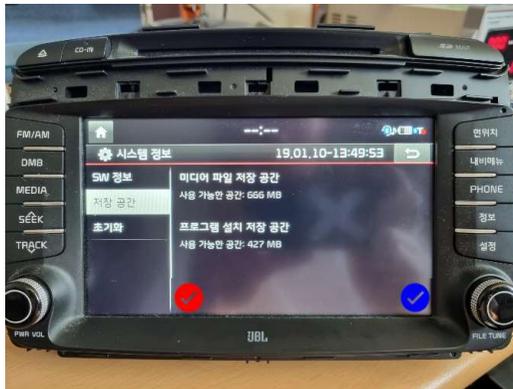
Forensic Readiness

Data Acquisition

Data Analysis

❖ Data Acquisition

1. 엔지니어링 메뉴로 진입
(시스템 정보/저장공간 화면 진입 -> 왼쪽 도어 지점 *번 클릭 후, 오른쪽 도어 지점 *번 터치)
2. 'USB Copy' 메뉴 선택
3. USB 포트에 USB 저장매체 삽입 후, 'Copy Logs to USB 처리' 기능 선택



☑ : 왼쪽 도어 지점

☑ : 오른쪽 도어 지점



USB drive

IVI 시스템 포렌식 절차

Forensic Readiness

Data Acquisition

Data Analysis

❖ Data Analysis

- 위치 관련 로그, 차량 이벤트 관련 로그, 시간 조작 관련 로그, 전화 관련 로그, 블루투스 연결 관련 로그

File	Tag	Info
tombstone_*	<ul style="list-style-type: none"> • GpsLocationProvider 	위도/경도
system_app_anr@*.txt	<ul style="list-style-type: none"> • Location_Manager • [CMM] initLastGpsDetail 	차량 문(후드, 트렁크) 개폐 또는 잠금 상태
SYSTEM_TOMBSTONE@*.txt	<ul style="list-style-type: none"> • TAS_BODY 	기어 상태
system_app_crash@*.txt	<ul style="list-style-type: none"> • System.out • BluetoothPbapClientService 	에어백 상태
Logcatdump.txt.*	<ul style="list-style-type: none"> • BluetoothPbapManager • CallLogProvider 	연료 경고등
Dumpstate- YYYYMMDD.HHMMSS.txt	<ul style="list-style-type: none"> • BTM • SynergyAndroid 	시간 조작 관련 로그
telematics.log.*	<ul style="list-style-type: none"> • BluetoothService • [CP]_DipoObserverService 	전화번호부 삭제 및 동기화 이력
SET_USER_TIME@NNNNNNNN.txt	<ul style="list-style-type: none"> • StatusBarPolicy • AllMenu • ApplicationMenu • SynergyAndroid 	통화 정보(이름, 전화번호, 통화유형:수신/발신, 통화 시간 및 날짜) 블루투스 연결/해제 상태 블루투스 MAC 주소

IVI 시스템 포렌식 절차

❖ Data Analysis

Forensic Readiness

Data Acquisition

Data Analysis

File	Tag	Info
tombstone_*	GpsLocationProvider, [CMM] initLastGpsDetail	위도/경도
	TAS_BODY	차량 문(후드, 트렁크) 열림/닫힘 상태, 잠금 상태
system_app_anr@*.txt	GpsLocationProvider, Location_Manager, [CMM] initLastGpsDetail	위도/경도
	TAS_BODY	차량 문(후드, 트렁크) 열림/닫힘 상태, 잠금 상태
SYSTEM_TOMBSTONE@*.txt	GpsLocationProvider, Location_Manager, [CMM] initLastGpsDetail	위도/경도
	TAS_BODY	차량 문(후드, 트렁크) 열림/닫힘 상태, 잠금 상태
system_app_crash@*.txt	Location_Manager	위도/경도
	TAS_BODY	차량 문(후드, 트렁크) 열림/닫힘 상태, 잠금 상태
Logcatdump.txt.*		
Dumpstate-YYYYMMDD.HHMMSS.txt		
telematics.log.*	GpsLocationProvider, Location_Manager, [CMM] initLastGpsDetail	
SYSTEM_TOMBSTONE@*.txt		
system_app_anr@*.txt		



03

결론 및 향후 연구

결론

- ❖ IVI 시스템의 로그 파일을 수집/분석하여 차량 및 탑승자 관련 정보를 파악 할 수 있음
 - 차량의 위치, 통화 정보, 이벤트 정보(문 개폐 상태, 기어 상태, 에어백 상태 등), 시간 조작 행위, 앱 실행 기록 등

- ❖ 차량 범죄 또는 충돌 사고 발생 시에
 - 차량의 이동 경로, 공모자 여부, 통화 이력 등을 파악 가능
 - 사고 시의 운전자 행위 재구성 가능

- ❖ IVI 시스템에서 ADB 디버깅 모드 활성화 방안 연구
 - ADB를 통한 데이터 수집 방법

Acknowledgement

이 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(no. 2021R1A2C2012574),

또한

2024년도 산업통상자원부 및 한국산업기술진흥원(KIAT)의 연구비 지원에 의해 수행된 연구임(No. P0023522)

Q&A
