차량 디지털 포렌식에서 타임라인 분석을 위한 안드로이드 기반 오디오 비디오 내비게이션 시스템의 로그 활용

2023 KCC

강해인, 박민수, 조성제, **정지헌**

INDEX

01 서론

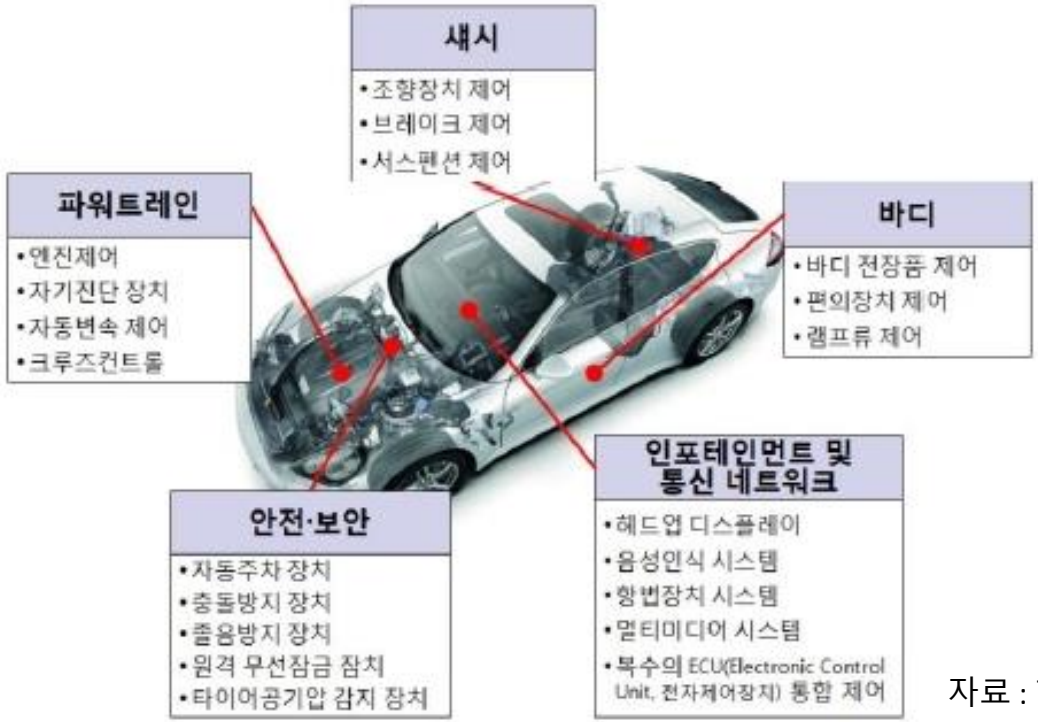
서론

❖ 차량용 인포테인먼트, ‘IVI(in-vehicle infotainment)/AVN(audio video navigation)’의 발전

- 사용자에게 편안하고 안전한 운전 환경과 다양한 엔터테인먼트 서비스를 제공하며 발전함.

❖ 자동차의 전장화로 인하여 차량 내부의 다양한 장치들이 서로 연결되어 작동

- AVN 시스템은 연료 소비량, 차량 상태, 내비게이션 등 차량 운전에 필요한 정보를 보여주기도 함.
  - ✓ 차량 속도, RPM, 엔진 부하, 브레이크 페달의 입력 등의 데이터들이 **AVN 시스템 로그에 저장**될 수 있음.



자료 : 한국전자통신연구원

서론

❖ AVN 시스템은 스마트폰과 연결되어 다양한 애플리케이션 사용 가능

- Android Auto, Apple CarPlay와 같이 폰 프로젝션 서비스를 통해 내비게이션, 음악, 통화 및 문자 메시지, 구글 어시스턴트 애플리케이션을 사용할 수 있음.
- 블루투스 핸즈프리 서비스를 통해 전화 수신 및 발신, 음악 재생 기능을 사용할 수 있음.
  - ✓ 스마트폰을 통한 운전자 행위(내비게이션 사용 기록, 전화번호부 검색, 통화, 음악 재생 등)와 관련된 데이터가 자동차 **AVN 시스템에 저장**될 수 있음.

서론

1. IVI 또는 AVN 시스템은 자동차의 전장화로 인하여 수많은 이벤트와 활동을 기록

2. 차량 디지털 포렌식을 위해서 AVN 시스템에 저장된 데이터를 획득하고 분석하는 것은 중요

3. 국내에서 많이 운행 중인 기아 모닝 어반(2020년식) AVN 시스템 로그를 포렌식 조사하여 이벤트 별 로그 데이터를 식별하고 분석

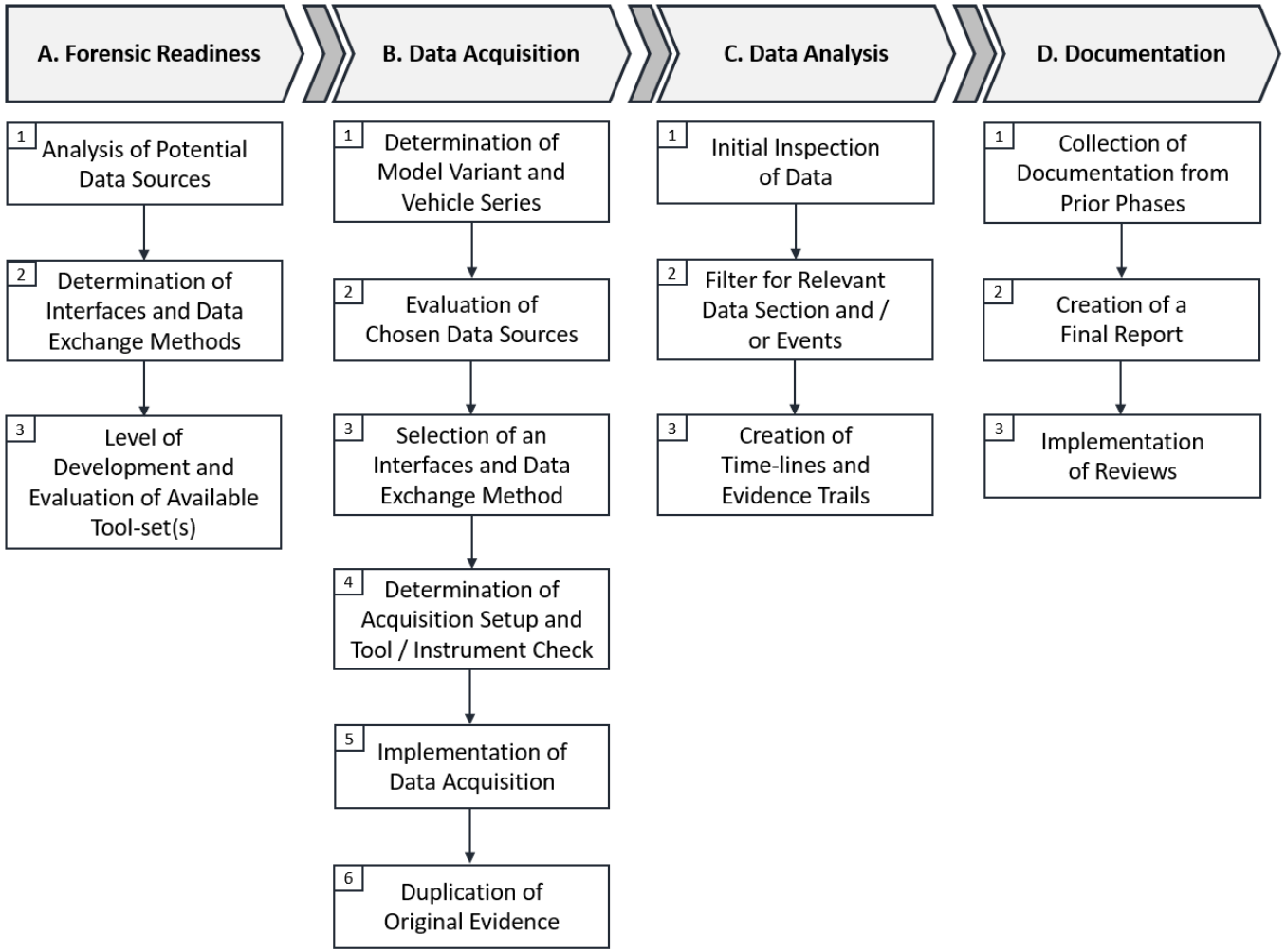
02 관련 연구 및 배경 지식

관련 연구

Forensic Science International: Digital Investigation, 36: 301111, 2021.

❖ A generalized approach to automotive forensics.

- 다양한 차량을 대상으로 서로 다른 환경에서 적용할 수 있는 일반화된 자동차 포렌식 절차 제안



관련 연구

❖ 국내외 자동차 포렌식 연구 동향

동향	국외		국내	
	[1]	[2]	[3][4]	[5]
대상 시스템	Dodge Dart Limited Uconnect 8.4 인포테인먼트 시스템 & Toyota Highlander Limited Toyota Extension Box system 인포테인먼트 시스템	Volkswagen Golf 인포테인먼트 시스템	KIA K5 AVN 시스템 & KIA NIRO EV AVN 시스템	KIA NIRO EV AVN 시스템과 KIA K5 AVN 시스템 (OS : 안드로이드 4.2.2 Jellybean) & KIA All New Morning 시스템과 Hyundai Sonata DN8 시스템 (OS : 안드로이드 4.4.2 Kitkat)
수집 방법	Berla 사의 iVe USB 키트를 사용하여 논리적 추출 진행	Chip-off (물리적 추출) 진행	Android Debug Bridge(ADB) 연결한 후, dd(disk dump) 명령어 수행(논리적 추출)	ADB 연결한 후, dd 명령어 수행(논리적 추출) & Chip-off(물리적 추출) 진행
분석 방법	Berla 사의 iVe software (차량 포렌식 전문 도구) 사용	FTK Imager, Wireshark 사용	X-ways forensics, Autopsy, DB4S, HxD, Epoch Converter, Talmap 사용	Autopsy, DB4S, HxD, Notepad, Talmap, Epoch converter 사용
아티팩트 (artifact)	Devices, Contacts(name, phone number, email), Call logs, Media, Location & Addresses(with latitude and longitude)	Navigation map information	Current Location, Destination, Favorite Location, Last Search Location, Registered Location, connected device list, MAC addr of device, name of device, contacts, call history, call logs	connected device list, MAC address of device, connection time, contacts, call history, call logs, startlog, tracklog, search location, registered locations, home/office address, door open/close info, gear shift state, driving state

관련 연구

[1] Whelan, C. J., Sammons, J., McManus, B., and Fenger, T. W., "Retrieval of infotainment system artifacts from vehicles using iVe," Journal of Applied Digital Evidence, 1(1), 30, 2018.

[2] Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K., and Choo, K.-K. R.. "Smart vehicle forensics: Challenges and case study." Future Generation Computer Systems, 109: 500-510, 2020.

[3] Seong, H., Lee, K., Han, S., Park, M., and Cho, S. J., "A Preliminary Forensics Analysis of Navigation Records on an Android-based Audio-Video Navigation System," The 7th International conference on Next Generation Computing (ICNGC 2021). 2021.

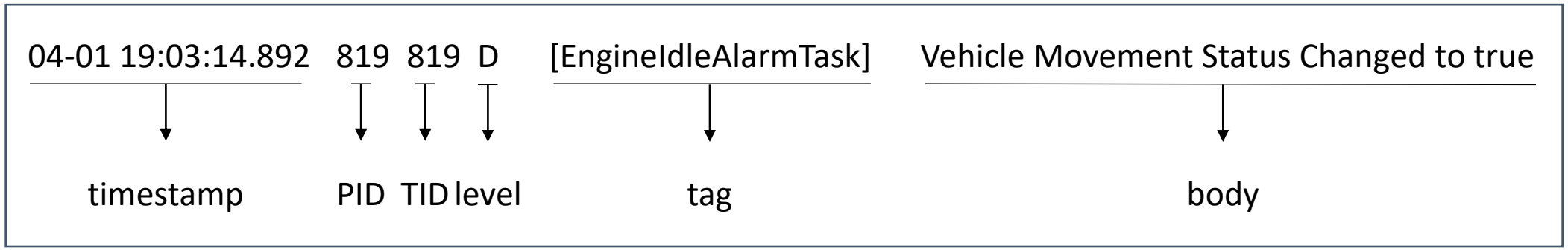
[4] Lee, K., Seong, H., Kang, H., Cho, S. J., Han, H., and Suh, K., "A Forensic Data Analysis of a Bluetooth Device paired with an Android-based Audio Video Navigation System," The 7th International conference on Next Generation Computing (ICNGC 2021). 2021

[5] Kang, H., Seong, H., Kim, I., Jeong, W., Cho, S.J., Park, M., Han, S., "Android-Based Audio Video Navigation System Forensics: A Case Study. Applied Sciences," Applied Sciences, 13(10): 6176, 2023

배경지식

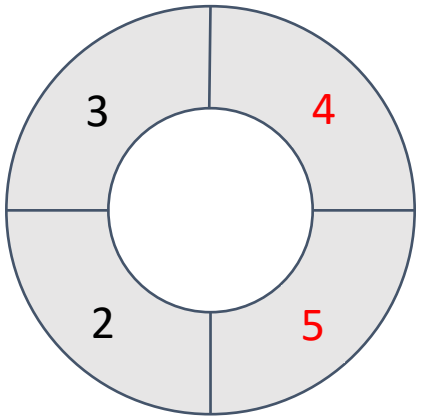
❖ 안드로이드 로깅 시스템

- 안드로이드 기반 AVN 시스템에서 logcat 명령어 입력하면 로그 메시지를 검색할 수 있음.



- 로그 메시지는 아래의 네 가지 메모리 버퍼에 저장되고 생성되는 메시지가 많아 버퍼 크기를 초과하면, 가장 오래된 로그 메시지부터 덮어쓰게되는 링 버퍼 구조임.

Buffer	Description
main	메인 앱 로그
event	시스템에서 발생하는 이벤트 정보를 위한 로그
radio	이동통신망 접속 관련 로그
system	안드로이드 플랫폼 내부의 하위 레벨 시스템 메시지와 디버깅을 위한 로그



03 실험 환경 및 분석 방법

실험 환경

❖ 실험 환경

블루투스 연결

USB 연결

AVN	
차종	KIA Morning Urban (2020)
운영체제	Android 4.4.2 (Kitkat)
스마트폰	
기기 명	iphone 12 pro
운영체제	iOS 14.1
제조사	Apple

실험 환경

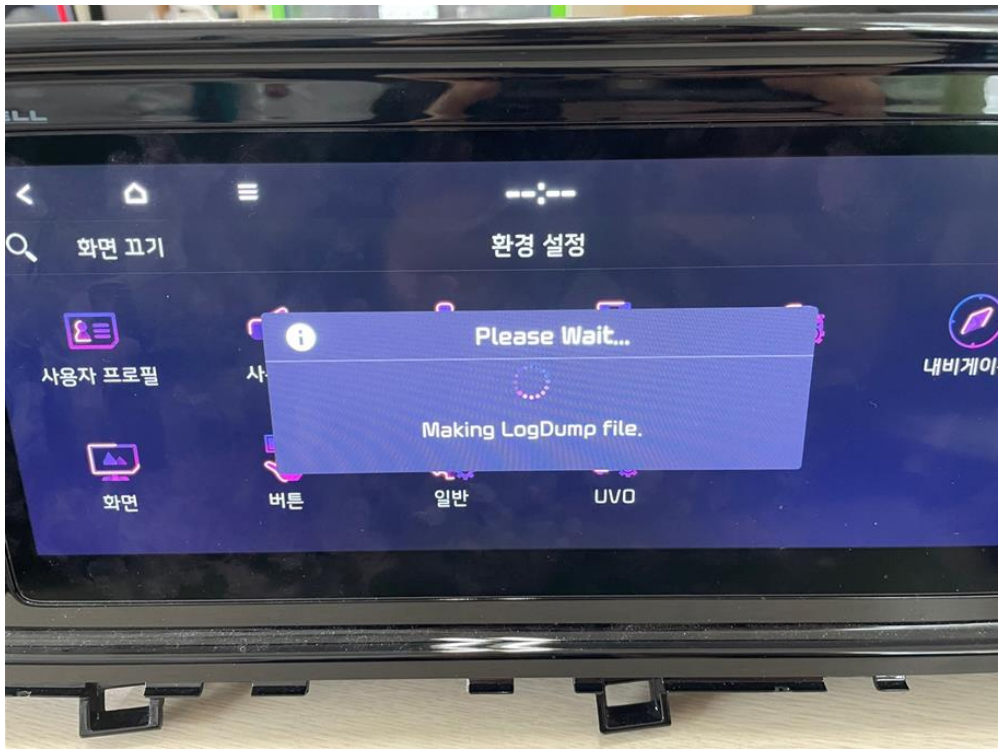
❖ 실험을 위해 발생시킨 주요 이벤트 및 타임라인

Time	Description
19:11	시동 켜기
19:16	블루투스 연결
19:16	스마트폰에서 AVN 시스템에 대한 권한 허용
19:20	메시지 수신
19:20	메시지 회신
19:21	목적지 설정
19:22	출발
19:30	기어 변경
19:32	라디오 앱 실행(채널 : SBS 파워 FM)
19:35	음악 재생
19:36	문 열기 및 닫기
19:41	팟캐스트 앱 실행
19:42	전화 발신
19:44	AVN 시스템에서 로그 덤프를 통한 데이터 수집

수집 · 분석 방법

❖ 데이터 수집

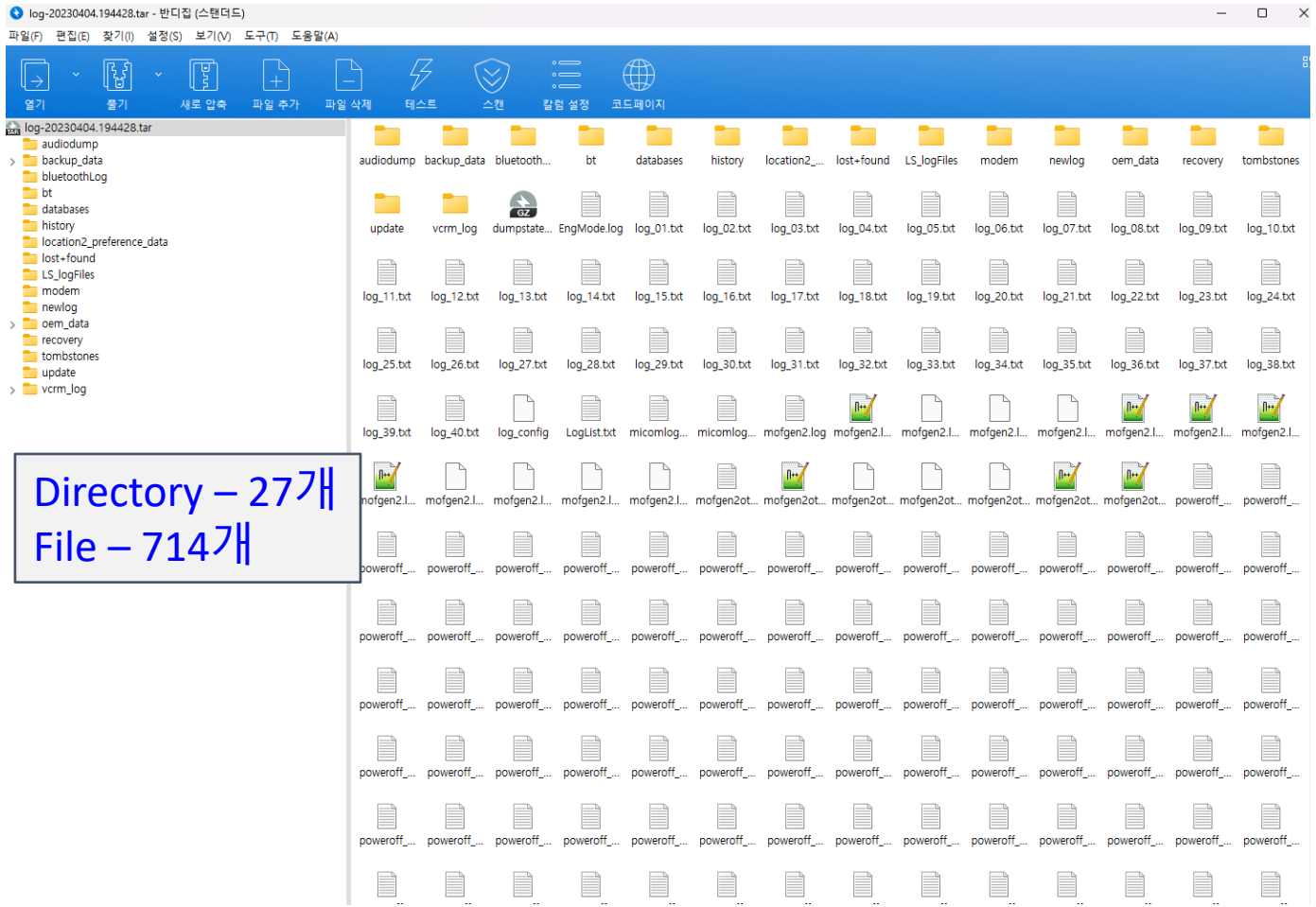
- 시나리오 기반 주행을 마친 다음 AVN 시스템의 '딜러 모드(Dealer mode)'로 진입함.
- USB 포트에 드라이브를 삽입한 후, Copy image to USB 버튼을 터치함.



➢ 안드로이드 4.4.2 Kitkat 버전의 AVN 시스템의 로그를 대상으로 논리적 추출 진행하였음.

수집 · 분석 방법

❖ 데이터 수집

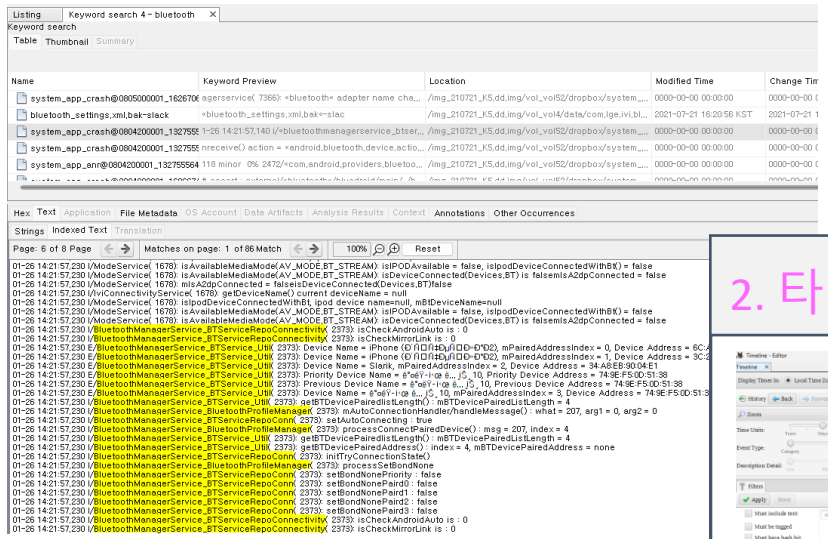


수집 · 분석 방법

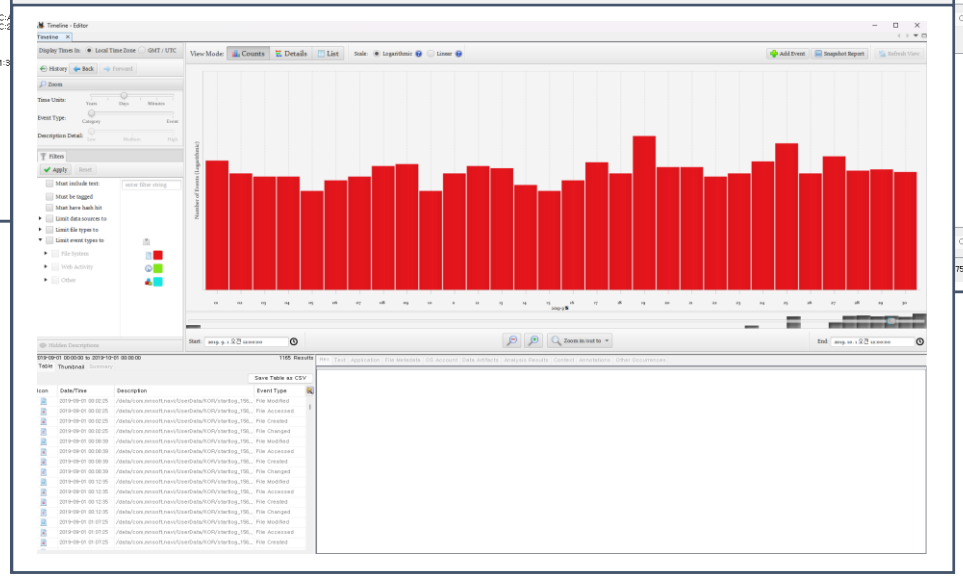
❖ 데이터 분석

- 대표적인 디지털 포렌식 도구인 Autopsy를 활용하여 로그 데이터를 분석함

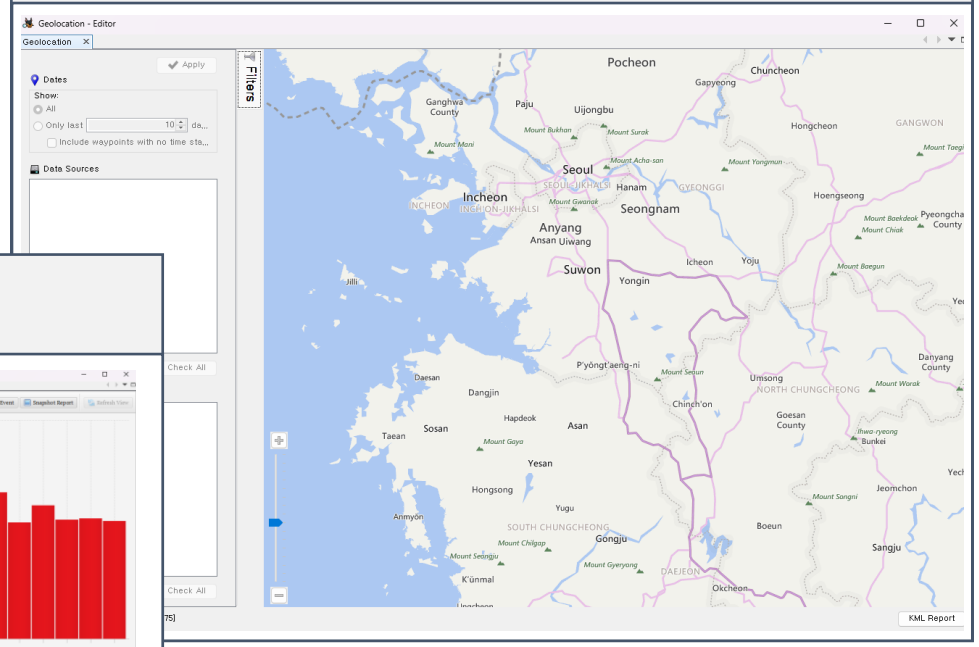
1. 키워드 검색(keyword search)



2. 타임라인 분석(timeline analysis)



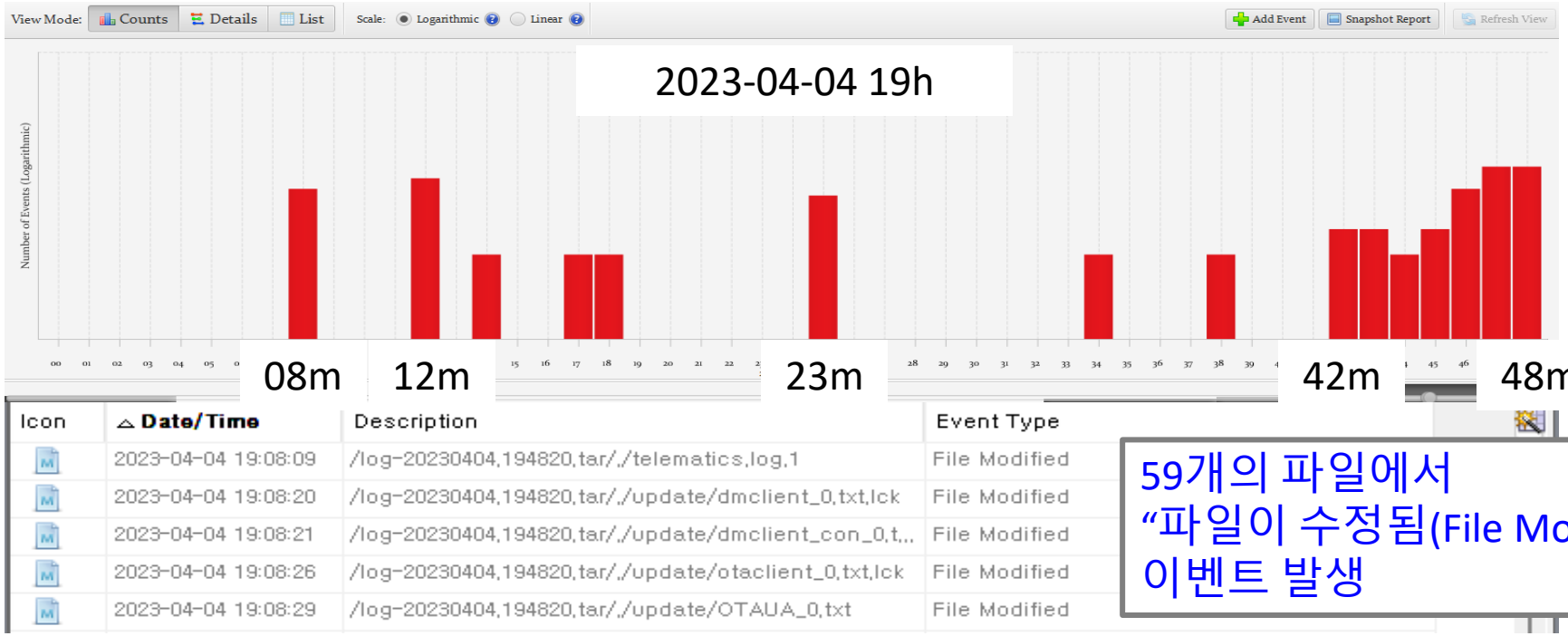
3. 지리적 위치 표시(show geolocation)



04 분석 결과

분석 결과

❖ Autopsy의 타임라인 생성 기능을 활용하여 714개의 파일 중 중요한 파일을 필터링



✓ 하나의 파일에 저장된 수많은 로그 메시지를 라인별로 분석해주지 않기 때문에, 차량 이벤트(블루투스 연결, 앱 실행, 전화 발신 등)를 식별하는 모습은 보이지 않았음.

✓ 본 연구에서 **차량 이벤트를 식별하기 위해 수많은 로그 메시지를 개별적으로 추가 분석함.**

분석 결과

❖ dumpstate_[date].[time].txt (하나의 파일)에서 로그 메시지

실험을 위해 발생시킨 주요 이벤트 중 차례대로

1. 블루투스 연결, 2. 라디오 재생, 3. 주차 기어로 설정하고 문 열기, 4. 팟캐스트 앱 실행, 5. 전화 발신 로그에 대해 정리

Buffer	Idx	log message			
		timestamp	level	tag	body
main	1	0404-19:16:53.010	I	bt-hci	BD_ADDR of remote : d8-de-XX-XX-XX-XX
	2	0404-19:32:55.340	D	HKMC_RadioGE_v2209	[RadioUtils] : SetStationName()- StationName : SBS 파워FM [수도권]
	3	0404-19:36:54.200	I	System.out	[EngineIdleAlarmTask] IGN ON: true Parking Gear ON: true Driver Door Open: true Service Status: true
system	4	0404-19:41:23.720	I	CarPlay_	04-04 19:41:23.720 880 1935 I CarPlay_: [ag] ==========> analyze Playback String : AppName is 팟캐스트
	5	0404-19:42:01.830	D	ClusterService	updateCallStatusForPrivateMode:status = 4, number=01012345678, name = 홍길동, mode=115, numberForHUD=01012345678, nameForHUD=홍길동

분석 결과

❖ 시스템 로그를 통한 운전자 행위 재구성

1. 4월 4일 19시 16분 53초에 AVN 시스템은 d8-de-XX-XX-XX 인 MAC 주소를 가진 모바일 기기와 블루투스로 연동하였다.
2. 19시 32분 55초에 차량 탑승자는 라디오 SBS 파워 FM[수도권] 채널을 켰다.
3. 19시 36분 54초에 주차 기어로 설정하고 차량 문을 열었다.
4. 19시 41분 23초에 스마트폰의 팟캐스트 앱을 실행했다.
5. 19시 42분 01초에 010-1234-5678 번호를 가진 사용자와 전화하였다.

분석 결과

❖ 주요 이벤트를 식별한 후, 중요 키워드를 추출

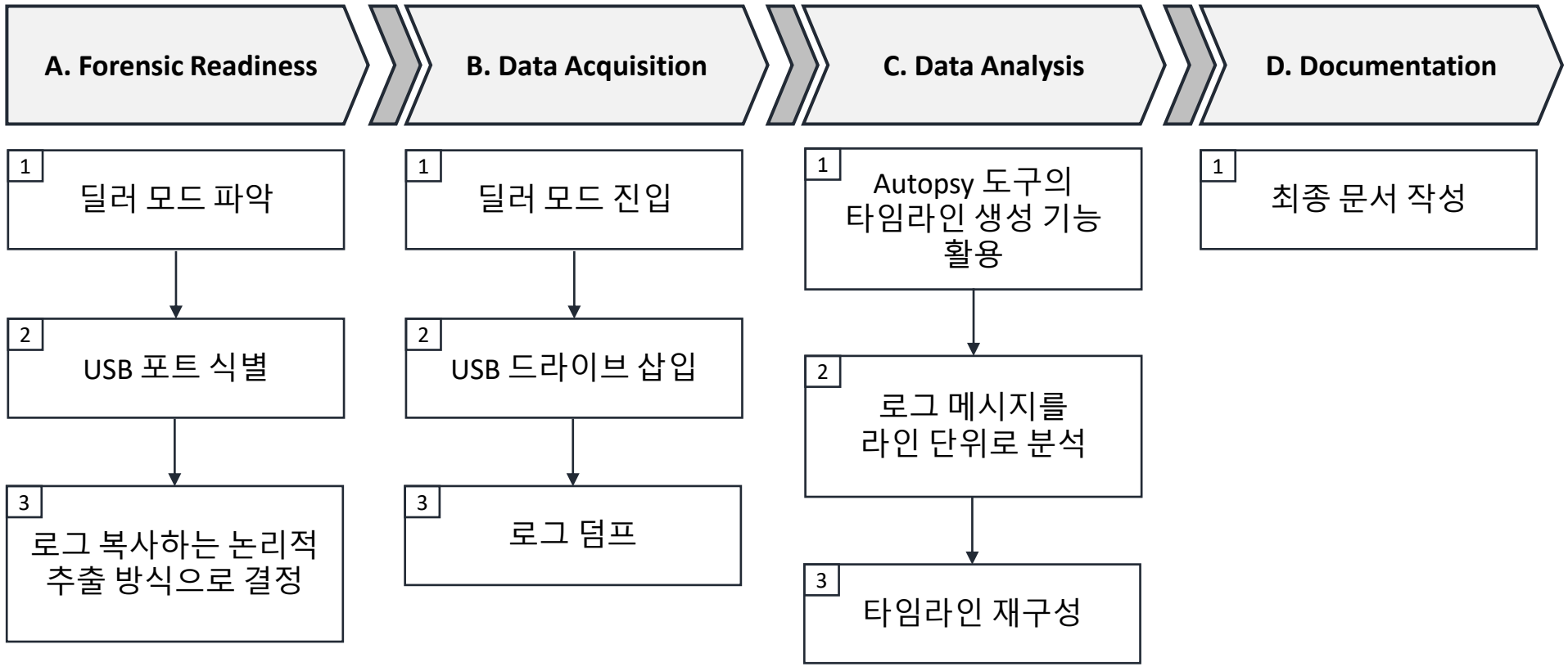
✓ bt-hci, BD_ADDR of remote, Radio Utils, EngileIdleAlarmTask, Cluster Service 등을 파악

Buffer	log message			
	timestamp	level	tag	body
main	0404-19:16:53.010	I	bt-hci	BD_ADDR of remote : d8-de-XX-XX-XX-XX
	0404-19:32:55.340	D	HKMC_RadioGE_v2209	[RadioUtils] : SetStationName()-StationName : SBS 파워FM [수도권]
	0404-19:36:54.200	I	System.out	[EngineIdleAlarmTask] IGN ON: true Parking Gear ON: true Driver Door Open: true Service Status: true
system	0404-19:41:23.720	I	CarPlay_	04-04 19:41:23.720 880 1935 I CarPlay_: [ag] ==========> analyze Playback String : AppName is 팟캐스트
	0404-19:42:01.830	D	ClusterService	updateCallStatusForPrivateMode:status = 4, number=01012345678, name = 홍길동, mode=115, numberForHUD=01012345678, nameForHUD=홍길동

05 결론 및 향후 연구

결론

❖ 기아 모닝 어반(2020년식) 차량의 AVN 시스템을 대상으로 로그 데이터를 수집하고 분석



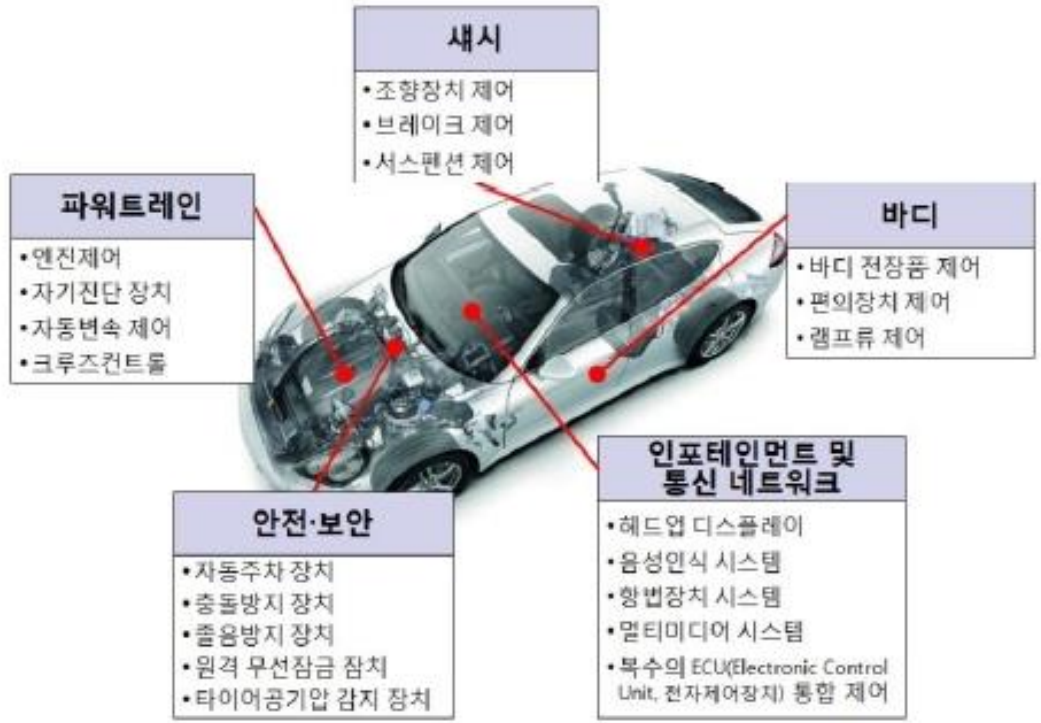
향후 연구

❖ 다양한 차량 제조업체와 모델에서 포렌식 조사를 수행하여 대상 범위를 확장

- 차량 디지털 포렌식 조사에서 중요한 키워드를 다양한 차량에서 식별할 예정
- 식별한 결과를 토대로 좀 더 세부적이면서 구체적인 타임라인을 구성

❖ 다양한 이벤트에 생성 및 저장되는 데이터에 대한 수집 및 분석에 대한 연구를 계속적으로 진행

- 파워트레인, 섀시, 바디 시스템에서 생성되는 데이터
  - **User data, safety-related data, security-related data**
- 내비게이션, GPS 시스템에서 생성되는 데이터
  - **location information with latitude, longitude**
- 차량 진단과 관련하여 생성되는 데이터
  - **OBD-II 통신**
  - **Infocar, Toque Pro 와 같은 차량 진단용 앱**



Acknowledgement

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

또한

2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2022-0-01022, 이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발).

Q&A