한국SW감정평가학회 학술대회

자동차 관련 디지털 포렌식 연구 동향

강해인, 조성제

단국대학교 소프트웨어학과

컴퓨터보안 및 운영체제 연구실

2023년 5월

목차

- Motivation
- Background
- Android Auto, Apple CarPlay
- Bluetooth HCI Snoop Log-based Forensic Investigation on a Smartphone paired with an Android-based Audio Video Navigation System
- Android-based Audio Video Navigation System Forensics
- Summary

Terminology

- AVN: Audio Video Navigation
- CAN: Controller Area Network
- CDR: Crash Data Retrieval
- ECU: Engine Control Unit
  - also known as Engine Control Module – ECM
- EDR: Event Data Recorder
- IVI: In-Vehicle Infotainment
  - In-Car Entertainment (ICE)
- OBD: On-Board Diagnostics
  - malfunction indicator light (MIL) onboard, diagnostic trouble codes (DTCs)
- RNS: Radio Navigation System

Motivation

- GENIVI alliance, Android Auto, Apple CarPlay 등의 플랫폼 등장으로 다양한 차량이 AI 음성인식 기반 IVI(AVN) 시스템을 지원함.
  - 이들 AVN 시스템이 스마트폰과 연결되어 차량 및 스마트폰에 사용자에 대한 다양한 정보가 저장됨.

- AVN은 영상과 내비게이션 정보를 제공하며 편리한 차량-사용자 인터페이스로 사용됨.
  - 차량의 상태 정보(예를 들어 타이어 공기 부족 등)가 AVN에 수집되어 표시되며, ecall/원격차량관리 등 다양한 무선 통신 서비스가 AVN을 통해서 이루어짐.
  - 점차 내비게이션 기반 스마트 크루즈 콘트롤(Navigation-based Smart Cruise Control) 기술 등이 AVN에 포함되고 있음.
  - 이 기술은 차량 내부의 다양한 ECU들 및 차량 외부의 스마트 교통 인프라와 AVN의 연동을 요구함. AVN은 차세대 자동차의 핵심 제품임.

Motivation

- When a vehicle is involved in a crime scene (e.g., drink driving) or a terrorist attack, ...
  - GPS 정보와 Navigation 정보를 활용하여, (사후에) 도난당한 차량의 이동 경로를 파악할 수 있음

- Vehicles are fast becoming an important source of digital evidence in a criminal investigation.
  - Modern-day vehicles store a range of (digital) information,
    - driving-related data (e.g. recent destinations, favorite locations, routes),
    - personal data (e.g. call logs, contact lists, SMS messages, pictures, and videos), and
    - other communication data (e.g. digital content sent to and from the devices in, or part of, the vehicle, to other “Things” or nodes in a smart vehicle or city network).

Motivation

- 최근 모바일 기기와의 연동을 통한 각종 커넥티드카 서비스가 상용화 되어, 모바일 기기와 자동차가 연결된 상황에 발생한 각종 디지털 데이터에 대한 증거확보에 자동차가 보조역할을 할 수 있는 것으로 확인되고 있음

- 차량은 차량 사고나 범죄 수사에서 중요한 증거를 획득하고 분석하는 매체가 될 수 있음

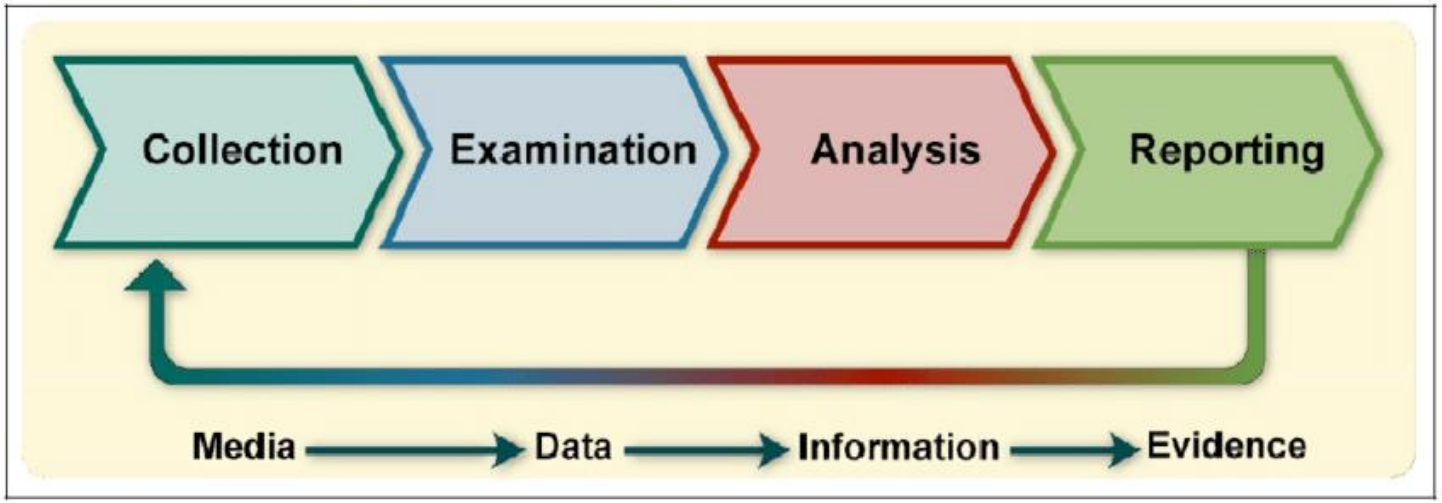
  Vehicular digital forensics, Vehicle digital forensics, Digital vehicle forensics, Automotive forensics

  - Android Auto and Apple CarPlay Forensics
  - Bluetooth HCI Snoop Log
  - Vehicular infotainment forensics
    - AVN은 차량 내부의 포렌식 관련 주요 정보들을 저장함. 따라서 AVN 포렌식이 필요함
  - Telematics
  - Vehicular OBD data
  - …

Background of Digital Forensics

- Digital forensics is the field of forensic science that is concerned with retrieving, storing and analyzing electronic data that can be useful in criminal investigations.
  - This includes information from computers, hard drives, mobile phones and other data storage devices.
  - Digital forensic investigations include the ***identification, preservation, acquisition, verification, analysis,*** and ***reporting of data***.
- In June 2016, the ‘‘Scientific Working Group on Digital Evidence’’ (https://www.swgde.org) published a ‘‘Best practice guide for vehicle infotainment and telematics systems’’ for evidence preservation and evidence handling.

- NIST’s 4-phases forensic model

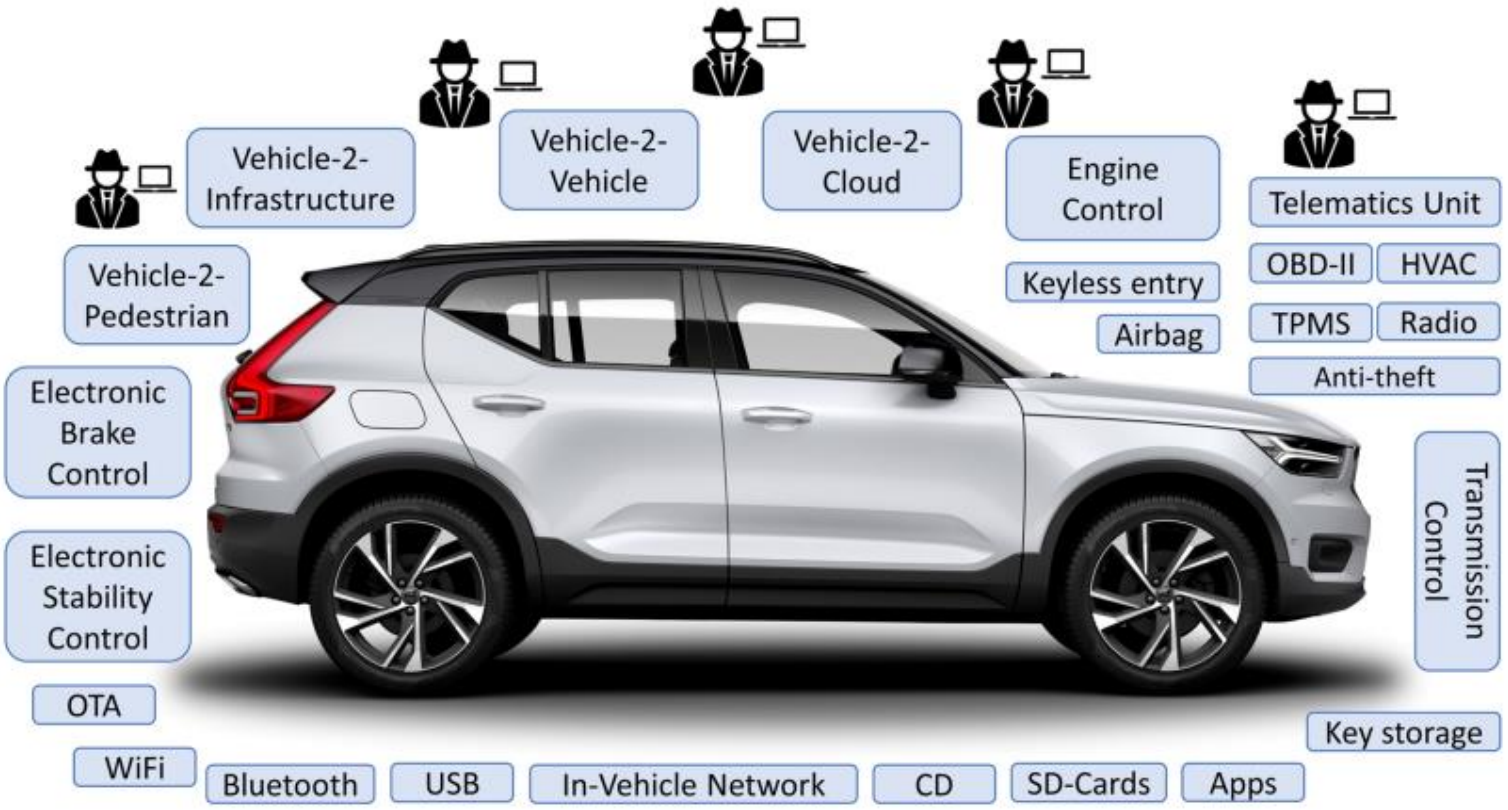


Background of Automotive Digital Forensics

The definition of digital forensics has expanded from involving just computers to include all digital devices that can store, process, or transmit data, a shift that leads to increased complexity.

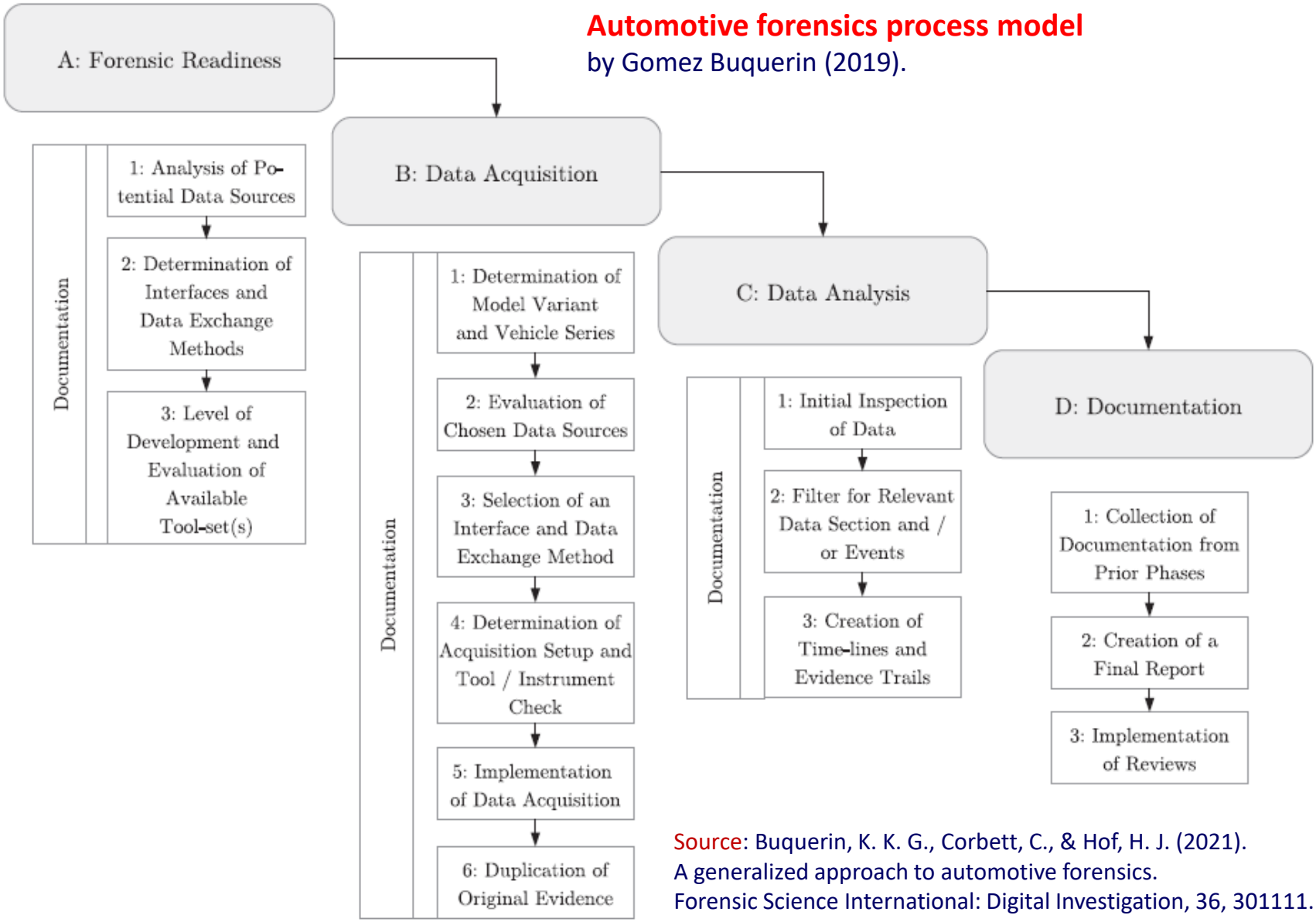
For example, when it comes to vehicles, file formats and OSs differ in ECUs making it challenging to create unified standards and tools; and vehicle IVNs consist of many interconnected devices communicating using different communication protocols.

This figure shows some examples of potential entry points that can be of interest to cyber criminals.



Source:
Strandberg et al., "A systematic literature review on automotive digital forensics: challenges, technical solutions and data collection." IEEE Transactions on Intelligent Vehicles (2022).

Background



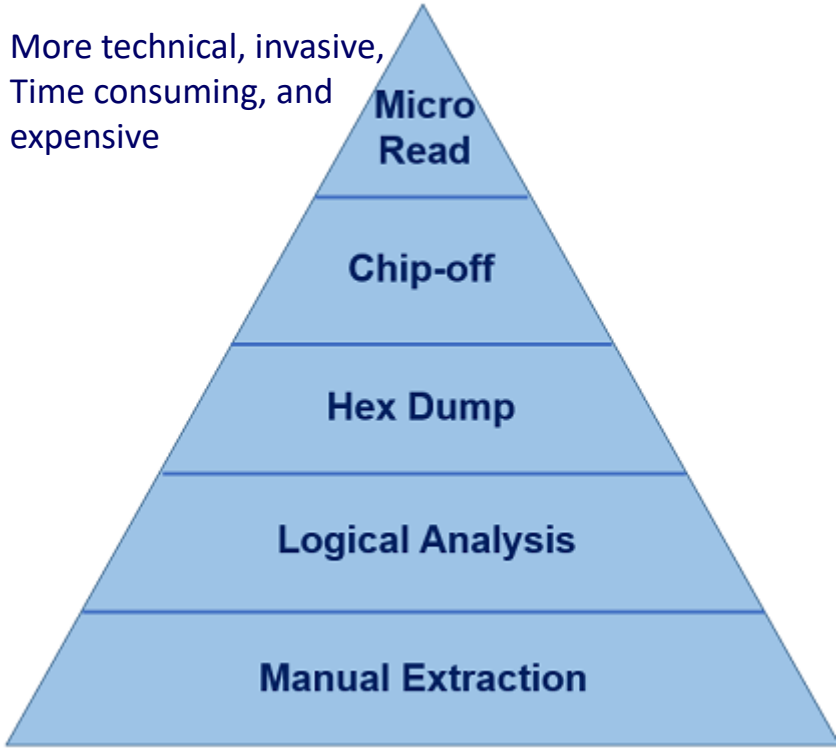
Automotive forensics process model
by Gomez Buquerin (2019).

Source: Buquerin, K. K. G., Corbett, C., & Hof, H. J. (2021). A generalized approach to automotive forensics. Forensic Science International: Digital Investigation, 36, 301111.

Background

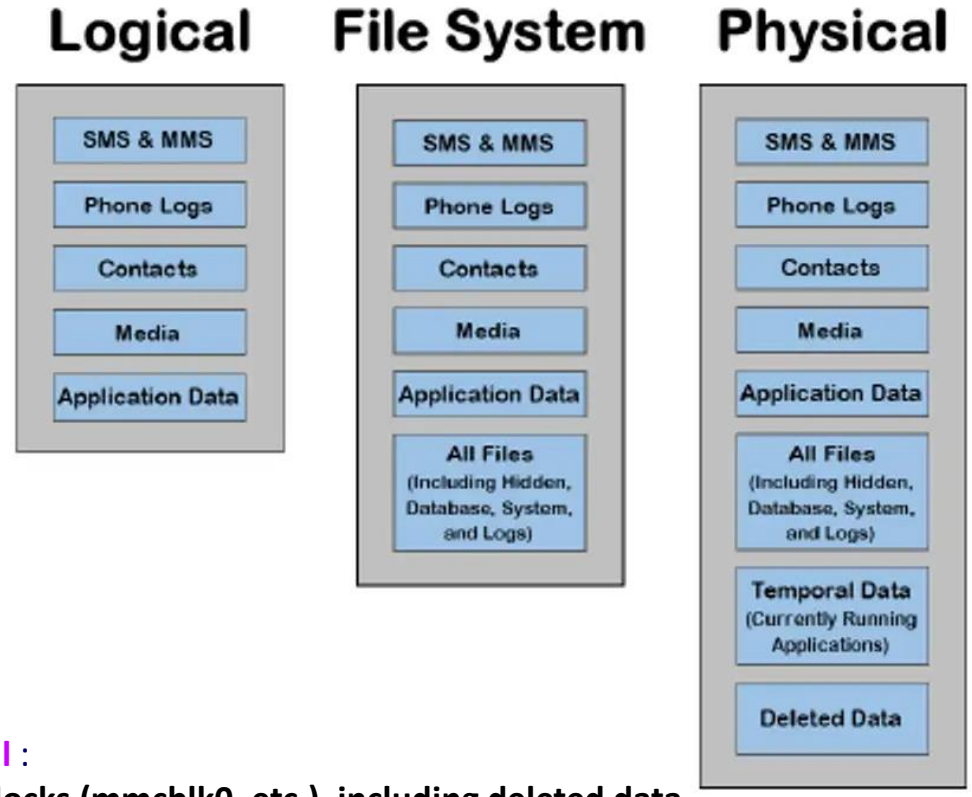
- Data acquisition, Digital evidence extraction scheme

More technical, invasive, Time consuming, and expensive



Source: R. Ayers, S. Brothers, W. Jansen (2014). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. Revision 1.

Source: Methods of Mobile Device Extractions. https://indianlegalsystem.org/methods-of-mobile-device-extractions/



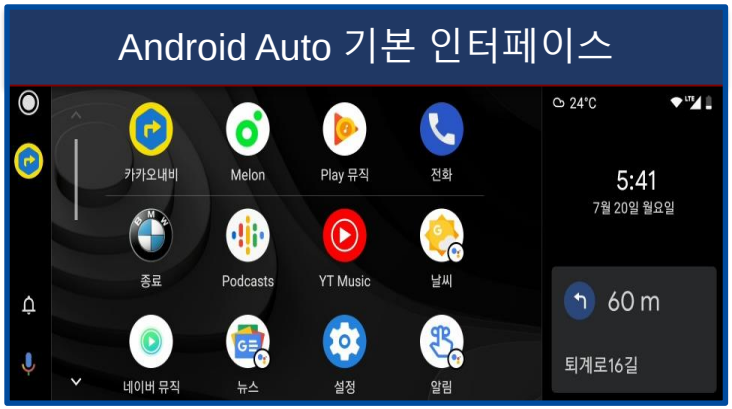
Physical :

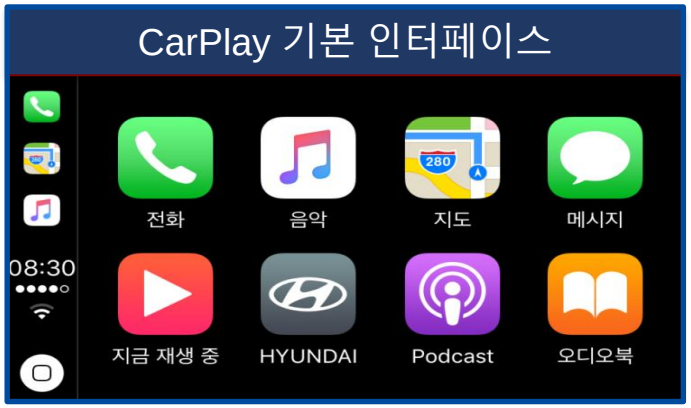
- **All blocks (mmcblk0, etc.), including deleted data.**
- **Recovery/Bootloader & JTAG/Chip-off methods**

Android Auto & Apple CarPlay

Android Auto:

- The hands-free integration of Android devices into a vehicle's in-dash head unit.
- A mobile app developed by Google to mirror features of an Android device, such as a smartphone, on a car's dashboard information and entertainment head unit.





IVI (In-Vehicle Infotainment)

- 차 안에 설치된 장비들이 차량 상태와 길 안내 등 운행과 관련된 정보는 물론이고, 사용자를 위한 엔터테인먼트적인 요소를 함께 제공하는 서비스.
  - a collection of hardware and software in automobiles that provides audio or video entertainment.
- In-car entertainment (ICE)
- AVN, RNS
- As cars are increasingly equipped with Internet connectivity (like Opel Onstar wifi hotspot, BMW ConnectedDrive or Volkswagen Car-net), vehicle infotainment systems are becoming more common and are frequently paired with mobile phones.

Table 1. IVI system used in case studies and connectivity of the IVI system.

Manufacturer	IVI System	Android Auto	Apple CarPlay
BMW	NBT HU EVO	No Support	Wireless
BMW	X5 45e xLine	Wireless	Wireless
Chevrolet	TrailBlazer	Wireless	Wireless
Pioneer	AVH-Z5050BT	Wired	Wireless
Sony	XAV-AX5000	Wired	Wired
TTEC	D5	Wired	No Support
RASPBERRY-PI	Raspberry Pi 3B (Crankshaft)	Wired	No Support
Belsee	Best Aftermarket Auto	Wired	Wired

Source: Shin et al., (2022). Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay. Sensors, 22(19), 7196.

IVI systems

Table 4. IVI systems.

Name	Model	Size of IVI Screen	Voice Assistant	Smart Home	IVI Source	Other Apps
DiLink	BYD Song	14.6	Nuance	√	Local, Bluetooth, USB, Online Apps	rotatable display screen support large game
GUKI	Geely Boyue	12.0	Iflytek	√	Local, Bluetooth, USB, Online Apps	Baidu/Tencent music Baidu, JD, MI smart home
iDrive	BMW 7 Series	7.0	Nuance Iflytek	NaN	Local, Bluetooth, USB, Online Apps	Map, FM radio BMW assistant
Nomi	Nextev ES6	11.3	Iflytek	NaN	Local, Bluetooth, USB,Online Apps	vehicle camera, social fragrance system
XmartOS	Xpeng G3	15.6	AI Speech	√	Local, Bluetooth, USB, Online Apps	In-vehicle camera, audiobook, music
IVI screen: Central control screen (inch)				√: Support Smart Home		

Source: Yu, Zhiyuan, et al. "Internet of vehicle empowered mobile media scenarios: In-vehicle infotainment solutions for the mobility as a service (MaaS)." Sustainability 12.18 (2020): 7448.

EDR (Event Data Recorder)

- a device installed in a motor vehicle to record technical vehicle and occupant information for a brief period of time (seconds, not minutes) before, during and after a crash.

- A number of manufacturers like Volvo and Toyota have install the EDR by default.
- An EDR installed in a vehicle stores more information in the event of a crash than the freeze frame information in ECU.
- The EDR stores information before, during and just after an accident.
- This information contains speed, brake status, seatbelt status and airbag deployment.

Forensic Tool: Berla iVe

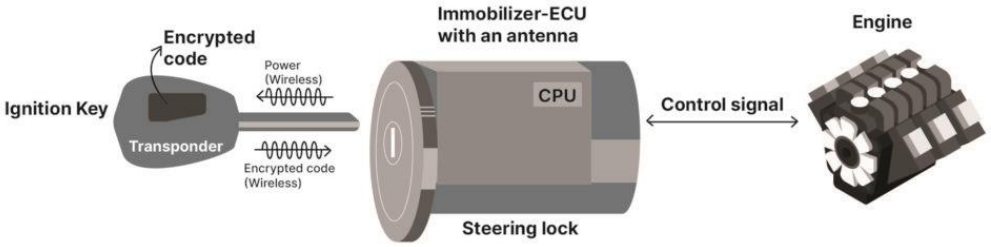
- iVe created by Berla Corporation is a software–hardware tool, designed for evidence acquisition and decoding from infotainment and telematics systems.
- It can extract vehicle information (from installed applications and Wi-Fi connections)
  - serial numbers, part numbers and VIN,
  - user related data like navigation data, information from car kits and user related events (doors open, Wi-Fi and Bluetooth connections, points-of-interest, tracklogs and previous destinations).
- iVe is also able to extract both physical and logical data from the infotainment and telematics units, via the OBD II port, USB connections inside the vehicle, and/or special diagnostics ports on the navigation system.

- iVe only supports a small number of European vehicles like BMW and Volkswagen.
  - in BMW QNX FS, the tool can be used to extract logical information over the OBD II port or the USB port connected to the infotainment system.
  - The support for VxWorks FS appears to be work in the same way. The tool is not able to make a complete physical extraction and is not able to decode the VxWorks FS.

Source: Le-Khac et al. "Smart vehicle forensics: Challenges and case study." Future Generation Computer Systems 109 (2020)

Forensic Tool: Bosch crash data retrieval system

- The Bosch crash data retrieval system is mainly used in crash investigations.
- It extracts data from the EDR by using the OBD II connector or a direct connection to the EDR.
- This tool is not built to extract and decode filesystems, and not surprisingly the tool cannot be used to extract data from immobilizers or ECUs.
  - Immobilizer: (차가 움직이지 못하게 고정하는) 자동차 도난 방지 장치



Other Forensic Tools

Desk-based review of forensic tool support.

File system support	Encase 7.x	Access forensics	Xways 18.x
FAT 12/16/32	×	×	×
exFAT	×	×	×
NTFS	×	×	×
EXT2/3	×	×	×
ReiserFS	×	×	×
UFS 1/2	×		×
AIX	×		
LVM8	×		
FFS	×		
Palm	×		
HFS(+)	×	×	×
CDFS	×	×	×
ISO 9660	×		×
UDF	×		×
DVD	×		
TiVo1/2	×		
ReFS		×	
VxFS (Veritas File system)		×	
TFAT			
Next3®			×
XFS			×

OS & FS of IVI systems

	OS	File System
BMW	QNX	QNX4, QNX6
Ford, Fiat, Nissan, KIA	Windows embedded	FAT, UDFS
Volkswagen	VxWorks	HRFS, DosFS

Encase 7.x does not support any of the filesystems within the QNX OS or the VxWorks.

Accessdata Forensic Toolkit does not appear to have any filesystem support for QNX or VxWorks.

Xways does not support specific filesystems in QNX and VxWorks.

Source: Le-Khac et al. "Smart vehicle forensics: Challenges and case study." Future Generation Computer Systems 109 (2020)

Android Auto,
Apple CarPlay

1. **안드로이드 오토 사용 차량의 포렌식 분석 사례연구**,
정보과학회 컴퓨팅의 실제 논문지,28(5), 2022.05
2. **Forensic Analysis of Apple CarPlay: A case study**,
Communications in Computer and Information Science, Volume 1544, January 2022

Android Auto 포렌식을 위한 실험 환경

실험환경

주행환경

- 자동차 : 2019 팰리세이드
- 휴대전화 : 삼성 갤럭시
- 연결 방식 : USB 포트 이용
- 네비게이션 : 카카오맵
- 운영체제 : Android 5.0.2
- 운영체제 : Android 7.0

분석도구

Autopsy

WinHEX

실제 실험 차량

Android Auto 관련 주요 artifacts

관련 부분	위치	파일명	비고
Gearhead 관련 (Android Auto)	/data/com.google.andoird.projection.gearhead/databases	Carservicedata.db	제조사, 모델, 제조 년도, 블루투스 주소, 연결시간
	/data/com.google.android.projection.gearhead/shared_prefs	App_state_shared_preferences.xml	Android auto 마지막 연결시간
			블루투스 주소(USB)
		Common_user_settings.xml	사용자의 음성입력 및 변환 과정
googlequciksearchbox 관련 (구글 어시스턴트)	/data/com.google.android.googlequicksearchbox/app_session	~~~.binarypb	내비게이션의 마지막 음성
KimGisa 관련 (카카오내비)	/data/com/locnall.KimGisa/Cache	KimGiSa_.mp3	내비게이션 음성 파일
	/data/com.locnall.KimGisa/database	Com.kakao.kinsight.android.~~~.sqlite	Kimgisa관련 session, event, event_history, event_flow.. 등
KakaNavi 관련 (카카오내비)	/media/0/KakaoNaviSDK/Cache	HWD_~~~.cache	경로 중 갈림길 정보
		DSW_~~~.cache	경로 중 지명 정보
기타	/data/com.Samsung.android.oneconnect/database	QcDb.db	핸드폰과 연결했던 devices, timestamp
	/system_de/0/ringtones	Notification_sound_cache	네비게이션이 켜지는 소리

Apple CarPlay 포렌식을 위한 실험 환경

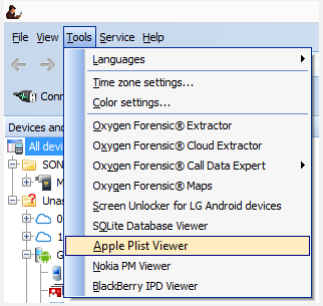
실험환경

주행환경

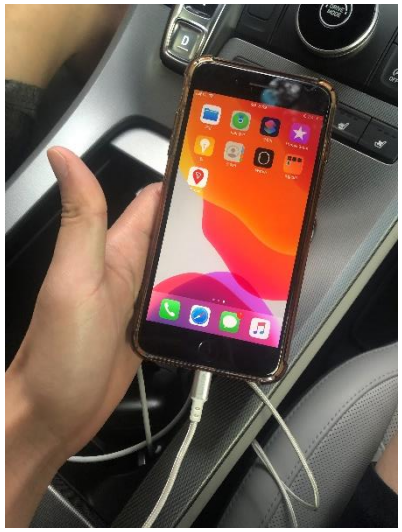
자동차 : 2019 팰리세이드	
휴대전화1 : iPhone 7 Plus	운영체제 : iOS 13.3
연결 방식 : USB 포트 이용	
네비게이션: 지도(아이폰 기본 앱)	네비게이션 : T map

분석도구

mac4n6



DB4S (DB Browser for SQLite)	APOLLO	Plist Viewer



실험 차량과 휴대전화 연결

Apple CarPlay 관련 주요 artifacts

폴더	위치	파일명	비고
/var/root/Library/Caches (차량 정보, 시간 정보)	/locationd	Cache.plist	자동차와의 마지막 USB 연결시간 /분리시간
		Cache_encryptedC.db	차량 탑승, 움직임에 대한 기록 (CarPaly USB 연결과 상관없이 아이폰 내부적으로 처리)
/var/mobile/Library	/Preferences	Com.apple.carplay.plist	자동차명
		Com.apple.celestial.plist	블루투스 정보
		Com.apple.CarplayApp.plist	마지막으로 어플을 실행시킨 시간
	/Springboard	CarDisPlayIconState.plist	자동차 화면상 어플리케이션들의 위치
	/Assistant	PreviousConversation.plist	Siri와의 가장 최근 대화(text형태), 시간 정보 포함
	/CoreDuet/knowledge	KnowledgC.db (음성 입출력 정보, 폰 연결분리 시간)	input/output 오디오에 대한 정보, CarPlay(USB) 연결/분리 시간
/var/mobile/Library	/Caches/com.apple.routined	Cache.sqlite	시간에 따른 휴대폰의 위치 좌표, 속도(m/s) ✓ 차량 연결과 무관하게 저장됨
	/CoreDuet/People	interactionC.db	핸드폰 통화 및 문자 기록
	/SMS	sms.db	메시지를 text 형태로 저장

안드로이드 AVN과 연동된 스마트 폰에서 Bluetooth HCI Snoop Log 기반 포렌식 조사

차량용 안드로이드 AVN과 연동된 모바일 기기의 블루투스 HCI 스눕 로그를 이용한 차량 포렌식 분석용 사용자 행위 파악, 한국차세대컴퓨팅학회 논문지, 2021.10.

Bluetooth HCI Snoop Log

- **Bluetooth HCI Snoop Log**
  - 안드로이드 시스템에서 어플리케이션 개발 중 블루투스 관련 디버깅 을 위한 기능
  - 안드로이드 4.4 (KitKat) 이후 버전에서 개발자 옵션으로 활성화하여 수동으로 Host Controller Interface (HCI)의 패킷을 캡처할 수 있으며, 캡처한 패킷은 RFC 1761 스눕 형식과 유사

- 차량용 AVN과 스마트 폰의 블루투스 연결을 통해 수행 가능한 운전자 행위

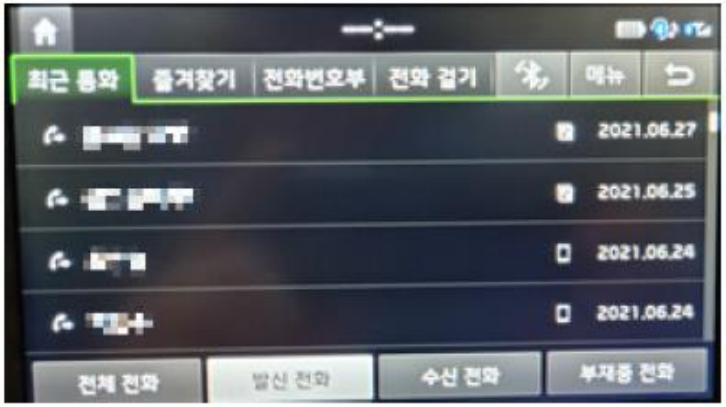
사용자 행위	설명
전화번호부 조회	전화번호부 연동을 통한 모바일 기기의 전화번호부 조회 및 통화 가능
최근 통화목록 조회	최근 통화목록 연동을 통한 조회 및 통화 기능
전화 수신 및 발신	연동된 전화번호부, 최근 통화기록, 다이얼을 통한 통화 발신과 통화 수신 기능
미디어(음악) 재생	모바일 기기에서 재생 가능한 미디어(음악) 재생

AVN과 모바일 기기 간 블루투스 기반 사용자 행위

(1) 연락처 접근 허용에 따른 AVN으로 전화번호부 다운로드

(2) AVN에서의 전화번호부 조회

(3) 연락처 접근 허용에 따른 AVN으로 최근 통화목록 다운로드



(4) AVN에서의 최근 통화목록 조회

(5) AVN상에서 다이얼을 통한 통화 발신 기능

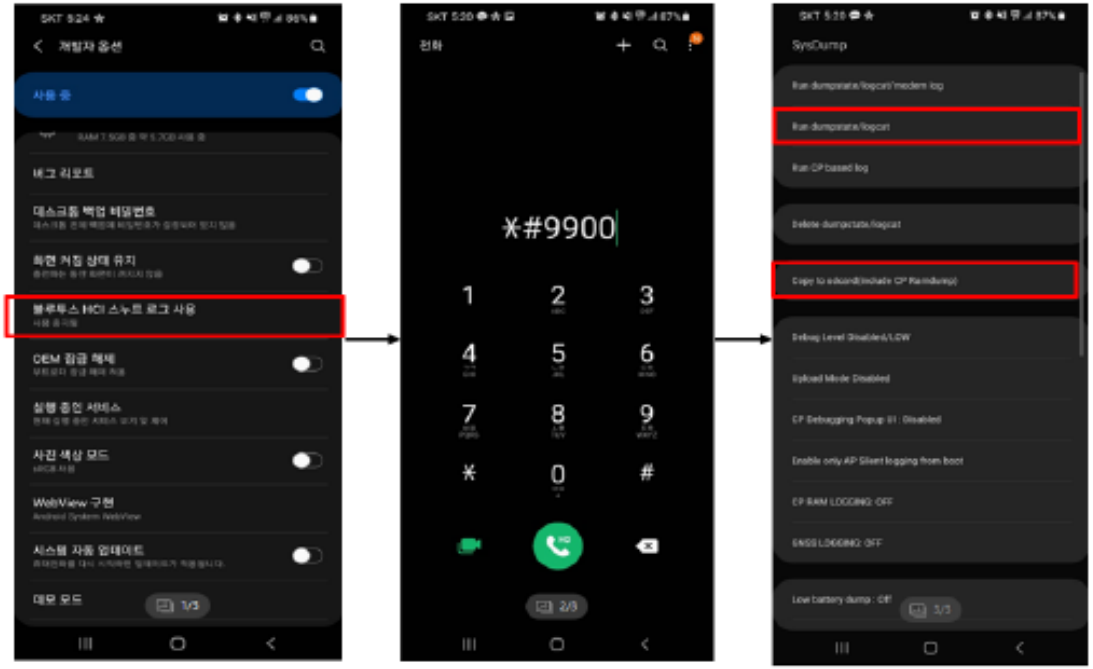
(6) AVN을 통한 미디어(음악) 재생

실험 환경 및 패킷 수집

실험 환경

AVN (19)	
차종(연식)	KIA K5(2015)
제조사	현대모비스(주)
운영체제	Android 4.4.2
지원 블루투스 규격	3.0
지원 프로파일	핸즈프리(1.6), A2DP(1.2), AVRCP(1.4), PBAP(1.0)
송신출력	0.125mW
채널 수	79개
모바일 기기 (휴대전화)	
기기명	Samsung Galaxy S21
운영체제	Android 11
블루투스 버전	5.0

- Wireshark 사용

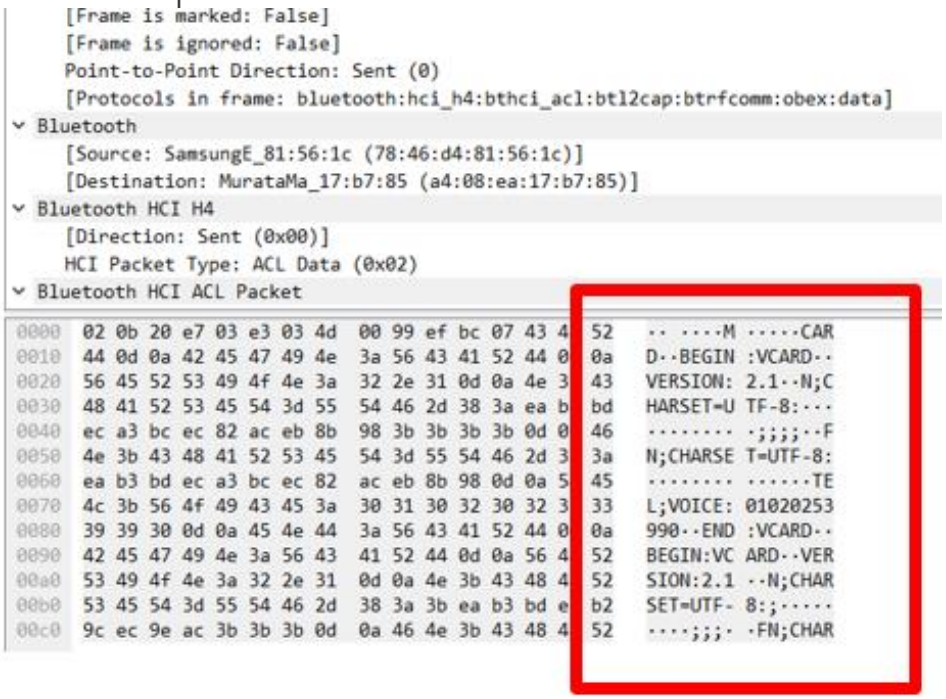


모바일 기기의 블루투스 패킷 획득 과정

블루투스 패킷 분석

전화번호부 연동 시에 나타나는 주요 블루투스 패킷 데이터

Src	Dst	Prt	Info
K5	S21	SDP	Rcvd Service Search Attribute Request : Phonebook Access Server Attribute Range(0x0000~0xFFFF)...**1)**
S21	K5	OBEX	Sent Success - Phone Book Ac Profile ...**2)**
K5	S21	OBEX	Rcvd Get final "telecom/pb.vcf"...
S21	K5	OBEX	Sent Success ..**4)**
K5	S21	OBEX	Rcvd Get final "SIM1/pb.vcf"...**5)**
S21	K5	OBEX	Sent Success ...**6)**
S21	K5	OBEX	Sent OBEX fragment ...**7)**
S21	K5	OBEX	Sent OBEX fragment ...**8)**
S21	K5	OBEX	Sent OBEX fragment ...**9)**



Wireshark 상에서 확인 가능한 전화번호부 전송데이터

패킷 분석을 통한 운전자 행위 재구성

1. 최초로 K5 장치와 Galaxy S21 장치가 요청을 주고받은 패킷으로 해당 시점인 6월 28일 14시 46분 39초경, 차량에 탑승하여 모바일 기기와 차량 AVN을 블루투스로 연결하였거나, 이 전에 탑승하여 모바일 기기와 차량 AVN을 블루투스로 연동하였음
2. 이후 K5 장치와 Galaxy S21 장치의 이벤트에 의해 생성된 패킷 분석. 해당 패킷은 미디어(음악) 재생 관련을 위해 요청에 대한 응답 패킷임. 이를 통해 6월28일 14시 46분 43초경, 차량에 탑승하여 AVN과 모바일 기기를 블루투스로 연동한 후 4초 뒤, 차량 AVN을 통해 연동된 모바일 기기의 미디어(음악)를 재생하고자 했음.
3. 이후, 약 0.5초 뒤 연동된 모바일 기기의 미디어(음악)가 재생되었음.
4. 전화번호부 조회를 위한 전화번호부 동기화 요청 패킷을 분석. 이를 통해 6월 28일 14시 46분 45초경 AVN과 모바일 기기의 전화번호부가 연동되었음을 알 수 있으며, 만약 해당 연동 상황이 최초 연동 상황이라면 해당 시각은 사용자가 모바일 기기에 나타난 전화 번호부 접근 요청을 수락한 시각으로 볼 수 있음.
5. 진행 중인 통화 관련 이벤트에 의한 패킷 분석. Galaxy S21 장치에서 K5 장치로 보낸 CLCC 명령의 해석과 시간정보를 통해 6월 28일 14시 52분 28초 경 010000000000000 이라는 그룹을 지정해 놓지 않은 수신자에게서 온 음성 수신 전화가 걸려 왔음.
6. 통화 관련 패킷 뒤에 미디어(음악)를 재생하는 요청 분석. 이를 통해, 통화가 종료되어 차량의 음향 장치로 재생되는 서비스의 종류가 바뀌었음을 유추. 즉, 6월 28일 14시 53분 31초경 통화가 종료되고 연동된 모바일 기기의 미디어(음악)가 다시 재생되었음. 이는 실제 실험에 사용된 모바일 기기상에서 통화 기록에 서 14시 52분부터 약 1분 가량의 통화가 있었음을 확인

안드로이드 기반 AVN 시스템 포렌식

- **A Forensic Data Analysis of a Bluetooth Device paired with an Android-based Audio Video Navigation System,** ICNGC, 2021
- **A Preliminary Forensics Analysis of Navigation Records on an Android-based Audio-Video Navigation System,** ICNGC, 2021.
- **Android-based Audio Video Navigation System Forensics: A Case Study**, Submitted to Applied Science (March 30, 2023)

Target AVN systems

TABLE I. KIA NIRO EV AVN'S SPECIFICATION

Manufacturer	LG Electronics
OS	Android 4.2.2(Jelly Bean)
File System	Ext4
Vehicle	KIA NIRO EV
Processor	ARM v7
Chipset	Telechips TCC893x_EVM
Kernel	3.1.10-tcc

TABLE I. KIA K5 AVN'S SPECIFICATION

Manufacturer	LG Electronics
OS	Android 4.2.2 (Jelly bean)
File System	Ext4
Vehicle	Kia K5(2015)
Processor	ARM v7
Chipset	Telechips TCC893x
Kernel version	3.1.10-tcc

Vehicle model	AVN model	Android version	Linux kernel	File system	eMMC chip
Kia K5 (2015)	LG Electronics LAN5020KKJF	4.2.2 Jellybean	3.1.10	ext4	Micron MTFC4GACA AAM-4M IT(32GB)
Kia NIRO EV (2018)	LG Electronics IA88431DELE	4.2.2 Jellybean	3.1.10	ext4	Micron MTFC4GACA JCN-4M IT(32GB)
Hyundai Sonata DN8 (2019)	Hyundai MOVIS 96560L1070SS	4.4.2 KitKat	3.18.24	ext4	Samsung KLMCG8G ESD-B03Q (64GB)
Kia All New Morning (2020)	LG Electronics 965601Y000MB2	4.4.2 KitKat	3.18.24	ext4	Samsung KLM4G1FE PD-B031 (64GB)

Forensic Tools

TABLE II. FORENSIC TOOLS USED FOR ANALYSIS

	Tool Name	Use of Tool
1	X-ways Forensics	Image Analyzing
2	DB4S	DB file Analyzing
3	HxD	Binary file Analyzing
4	Epoch converter	Convert Epoch time
5	Talmap(former:Smartmap)	Check GPS coordinates

- **X-Ways Forensics** : a computer forensic examiner. Its functionality is similar to EnCase and FTK, but it does not support some functions such as network connection analysis or remote capture.
- **DB4S (DB Browser for SQLite)** : a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite.
- **HxD** : fast hex editor which, additionally to raw disk editing and modifying of main memory (RAM), handles files of any size.
- **TalMap** : TalMap Series는 지리정보 (지도, 도면, 속성, 위치, 객체)를 검색하는 Tool

Forensic Tools

Tool	Description	Use
Autopsy	a free and open source hard drive investigation tool	to analyze hard drive image of AVN's internal partition
ADB (Android Debug Bridge)	a debugging tool for Android-based devices that connects PC with Android device	to enter AVN system and identify disk partitions
dd (disk dump)	a command-line utility that convert and copy (device) files	to image and copy AVN's internal partition to SD card
DB4S (DB Browser for SQLite)	a tool for manipulating SQLite-compatible database files	to identify tables and fields and search for keywords in datadbase files
HxD	a hex editor that edits binary files	to analyze binary files generated by navigation software with file extension of .dat or .bin
Notepad	a simple text editor that edits various types of text files including HTML and XML and supports various encodings	to read and analyze log files
Talmap	a Korean navigation software	to convert Talmap's coordination information to GPS infromation
Epoch converter	a simple program that converts Unix epoch to human readable date & time	to convert epoch found in file names to local time (KST)

Primary Artifacts on AVN

Artifacts	File Location
Bluetooth Logs (Bluetooth History)	/data/data/com.android.provider.bluetooth
Media Play from USB	/data/data/com.android.providers.media
DMB History	/data/data/com.lge.ivi.dmb
Navigation Logs	/data/data/com.mnsoft.navi

- 블루투스 이용 기록
- USB 음악 재생 기록
- DBM 시청 관련 기록
- 내비게이션 이용 기록

/data/data/com.android.providers.Bluetooth/databases/*.db
(1차 분석)

Location and File name	Name of DB Table	Attribute
/databases/BTSetup.db	BTDevList	Address
/databases/BTContacts.db	Switch_index	dev# _name
/databases/BTFavorites.db	Switch_index	dev# _na
/databases/BTCallHistory.db	Switch_index	dev# _na

블루투스 이용 기록

- **MAC address of the mobile devices (최대 5 개 기기의 MAC 주소)**
- **device name**
- **phone book (BTContacts.db)**
- **recent call history (최근 통화 기록)**

BTSetup.db의 BTDevList table
AVN에 연결된 모바일 기기들의 정보

Table BTDevList 5 entries Page 1 of 1 Export to CSV

_id	devname	address	status	a2dp_st...	avrcp_s...	priority
62	iPhone ([redacted])	6C:AB:31:[redacted]	0	0	0	0
63	iPhone ([redacted])	3C:2E:FF:[redacted]	0	0	0	0
65	[redacted]	34:A8:EB:[redacted]	0	0	0	0
66	갤럭시 노트 10	74:9E:F5:[redacted]	0	0	0	0
68	[redacted]의 Galaxy S21	78:46:D4:[redacted]	2	2	0	1

Primary Artifacts on AVN

AVN 시스템에서 분석한 블루투스 이용 기록

/data/data/com.android.providers.Bluetooth/databases/*.db (2차 분석)

File Name	Table	Attribute	Artifact
BTSetup.db	BTDevList	devname	device name
		address	MAC
	Switch_Index	dev#_name	MAC
BTContacts.db	Switch_Index	dev#_name	MAC
	Dev#Contacts	name	given name
		fname	family name
		num#	phone number
BTCallHistory.db	Switch_Index	dev#_name	MAC
	Dev#CallHistory	type	dialed | received | missed
		name	name
		fname	fname
		number	phone number
		tel_type	[cell, home, other]
		date_time	call date

- BTSetup.db의 BTDevList 테이블 : 연동된 모바일 기기의 명칭, MAC 주소
- BTContacts.db : 연동된 모바일 기기의 전화번호부
- BTCallHistory.db : 연동된 모바일 기기의 최근 통화 기록

Primary Artifacts on AVN

연결 기기의 전화번호부: /data/…/databases/BTContacts.db

테이블(T): Dev5Contacts — 모든 열에서 필터링

	_id	vcard_version	storage	name	fname	num1_type	num1
	필터	필터	필터	필터	필터	필터	필터
1	21980	2.1	0	[illegible]	[illegible]	CELL	0102[illegible]
2	21981	2.1	0	[illegible]	[illegible]	CELL	0107[illegible]
3	21982	2.1	0	[illegible]	[illegible]	CELL	0102[illegible]
4	21983	2.1	0	[illegible]	[illegible]	CELL	0103[illegible]
5	21984	2.1	0	[illegible]	[illegible]	CELL	0104[illegible]
6	21985	2.1	0	[illegible]	[illegible]	CELL	0105[illegible]
7	21986	2.1	0	[illegible]	[illegible]	CELL	0109[illegible]
8	21987	2.1	0	[illegible]	[illegible]	OTHER	0102[illegible]
9	21988	2.1	0	[illegible]	[illegible]	CELL	0102[illegible]
10	21989	2.1	0	[illegible]	[illegible]	OTHER	0318[illegible]

연결 기기의 최신 통화기록: /data/…/databases/BTCallHistory.db의 Dev#[index]CallHistory table

테이블(T): Dev5CallHistory — 모든 열에서 필터링

	_id	vcard_version	storage	type	name	fname	nickname	tel_type	number	date_time
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	9341	2.1	0	DIALED	NULL	건[illegible]	NULL	CELL	010276[illegible]	20210728150928
2	9342	2.1	0	DIALED	NULL	박[illegible]	NULL	CELL	01046[illegible]	20210728130845
3	9343	2.1	0	DIALED	NULL	아[illegible]	NULL	CELL	01083[illegible]	20210727131619
4	9344	2.1	0	DIALED	NULL	김[illegible]	NULL	CELL	010220[illegible]	20210723223934
5	9345	2.1	0	DIALED	NULL	울[illegible]	NULL	OTHER	+8210[illegible]	20210720223557
6	9346	2.1	0	DIALED	NULL	김[illegible]	NULL	CELL	010801[illegible]	20210719141839
7	9347	2.1	0	DIALED	NULL	김[illegible]	NULL	CELL	010801[illegible]	20210719135439
8	9348	2.1	0	DIALED	NULL	울[illegible]	NULL	OTHER	010270[illegible]	20210715163516
9	9349	2.1	0	DIALED	NULL		NULL	OTHER	050710[illegible]	20210714104956
10	9350	2.1	0	DIALED	NULL	울[illegible]	NULL	OTHER	010276[illegible]	20210710223230

Primary Artifacts on AVN

내비게이션 이용 기록: /data/data/com.mnsoft.navi/**database/Navi_vr.db** → 14개 table을 포함

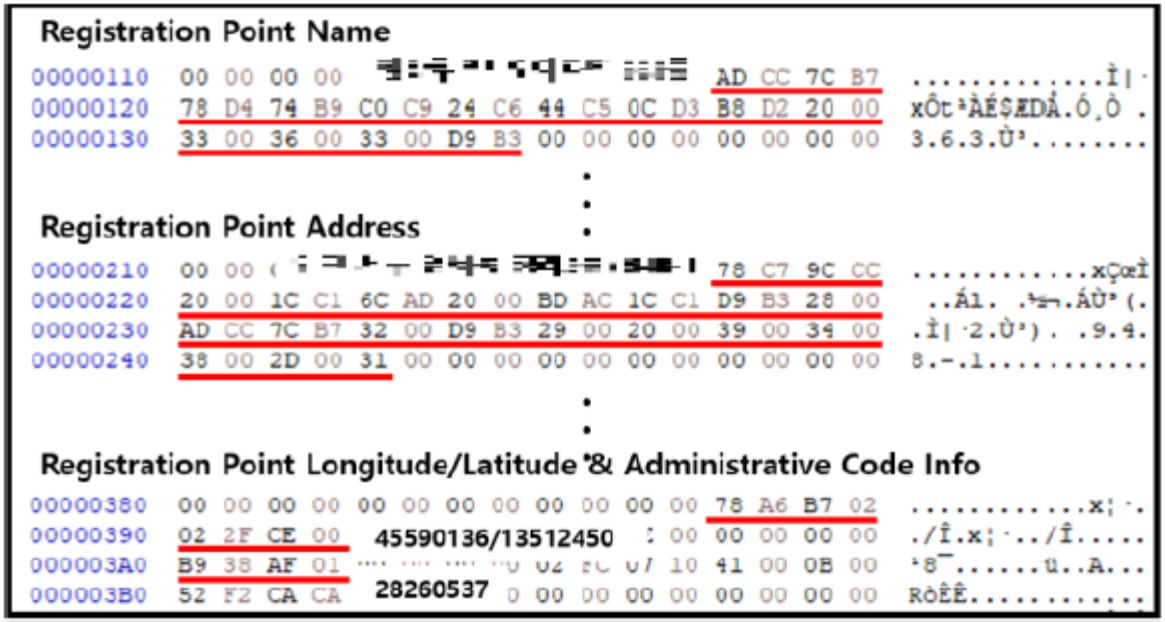
14개 테이블 중에서 몇 테이블만 정보 유지

- **CurrentLoc_Table** : (latitude, longitude), the name of the place and the code for administrative district of the last location. [마지막 위치 이름, 행정동 번호]
- **Destination_Table** : the information of the last destination search including search keyword, address, phone number, distance from starting point and destination and estimated time required. [검색어, 검색지 주소, 검색지 경도/위도 정보, 검색지 전화번호, 출발지에서 목적지까지 예상 소요시간, 등]
- **MemoryPoint_Table** : 즐겨찾기 저장 이름, 즐겨찾기 저장 주소
- **RegisPntSpecial_Table** : 등록 위치(주소), 등록 위치 전화번호, 등록치 경도/위도, 등록 위치 순서
- **NonSearch_Table** : 검색어, 검색지 주소, 검색지 전화번호, 목적지까지 거리, 검색지 경도/위도 정보 등

	Table Name	Existence of data
1	CurrentLoc_Table	O
2	Destination_Table	O
3	MemoryPoint_Table	O
4	NaviMenu_ButtonState_Table	X
5	NaviVersion	X
6	NonSearch_Table	O
7	RegistPnt_G1_Table	X
8	RegistPnt_G2_Table	X
9	RegistPnt_G3_Table	X
10	RegistPnt_SectorName_Table	X
11	RegistPnt_Special_Table	O
12	Search_Table	X
13	State_Table	X
14	android_metadata	X

Primary Artifacts on AVN

- An example to analyze “registered points” (내비게이션 상 등록 위치) using HxD.
  - It shows the contents of binary file that contains ‘special registered points’ information.
- Since the target AVN system embeds a Korean navigation software TalMap, it supports Korean language, which means a character is encoded using 2 bytes.
- We identified the name of registered point, address, longitude/latitude, and code for administrative district.



.muf 라는 이진파일을 분석하여 파악한 등록 위치 관련 정보

Summary

Requirements and Security Properties on Vehicle Forensics

- A forensic investigation requires trust in the chain of events, such as the logical order of braking, acceleration, and steering.
  - Digital forensics has strong dependencies on information security to ensure trustable data.

- Forensics investigation includes the following basic steps
  1. ***Identification***. What is the reason for the incident? What data is relevant, and where is the data stored? What resources, e.g., tools and subject matter experts, are needed?
  2. ***Preservation***. How can we preserve integrity during data collection? Can the devices be turned off without losing data? Can data be remotely changed or erased?
  3. ***Acquisition and verification***. How can we extract the data (e.g., creating images and performing live acquisition)? How can we validate the authenticity of the data (e.g., with signatures and hashes)?
  4. ***Analysis***. What type of information is relevant to assess?
  5. ***Reporting***. How can we document all parts of the forensic investigation process?

Source: Strandberg et al., "A systematic literature review on automotive digital forensics: challenges, technical solutions and data collection." IEEE Transactions on Intelligent Vehicles (2022).

Future Research Agenda

1. Extending the research to other car makes and models.
   - Such examinations will potentially allow the digital forensic community to be better equipped in digital investigations of vehicles.

2. Continue the research on the forensic acquisition and analysis of GPS, maps, VoIP, IM apps, and other integrated components in a vehicle.
   - OBD-II, Telematics, Other AVN apps

3. Research on the automated real time acquisition of target vehicle or intercepting stream based on their IP address or other unique information.
   - Hence, there may be a need to design tools or interfaces that allow live forensic investigations.

4. Integrating forensic readiness in the design of future vehicles, a term coined forensic-by-design.
   - This will facilitate future forensic investigations of such vehicles.

Source: Le-Khac et al. "Smart vehicle forensics: Challenges and case study." Future Generation Computer Systems 109 (2020)

Acknowledgment

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)

Thank You !

Q&A