Forensic Investigation of An Android Jellybean-based Car Audio Video Navigation System

Yejin Yoon, Jeehun Jung, Seong-je Cho

Dept. of Software Science

Dankook University, Yongin-si, Repulic of Korea

INDEX

01 Introduction

Introduction

❖ **Digital Forensic – Car Audio Video Navigation (AVN)**

Modern Vehicle

In-Vehicle Infotainment (**IVI**) system
(also known as **AVN system**)

User Behaviors

Related work

[5] Dawabsheh and Owda (2023), **“In-Vehicles Infotainment System Forensics Case Study”**, *ICIT*

Target System	KIA Sportage 2014’s Android IVI system paired with a Xiaomi phone
Acquisition Method	SD card memory extraction, Wi-Fi connection
Extracted Artifacts	Maps, Calls, Media files (videos, music, images), Email address

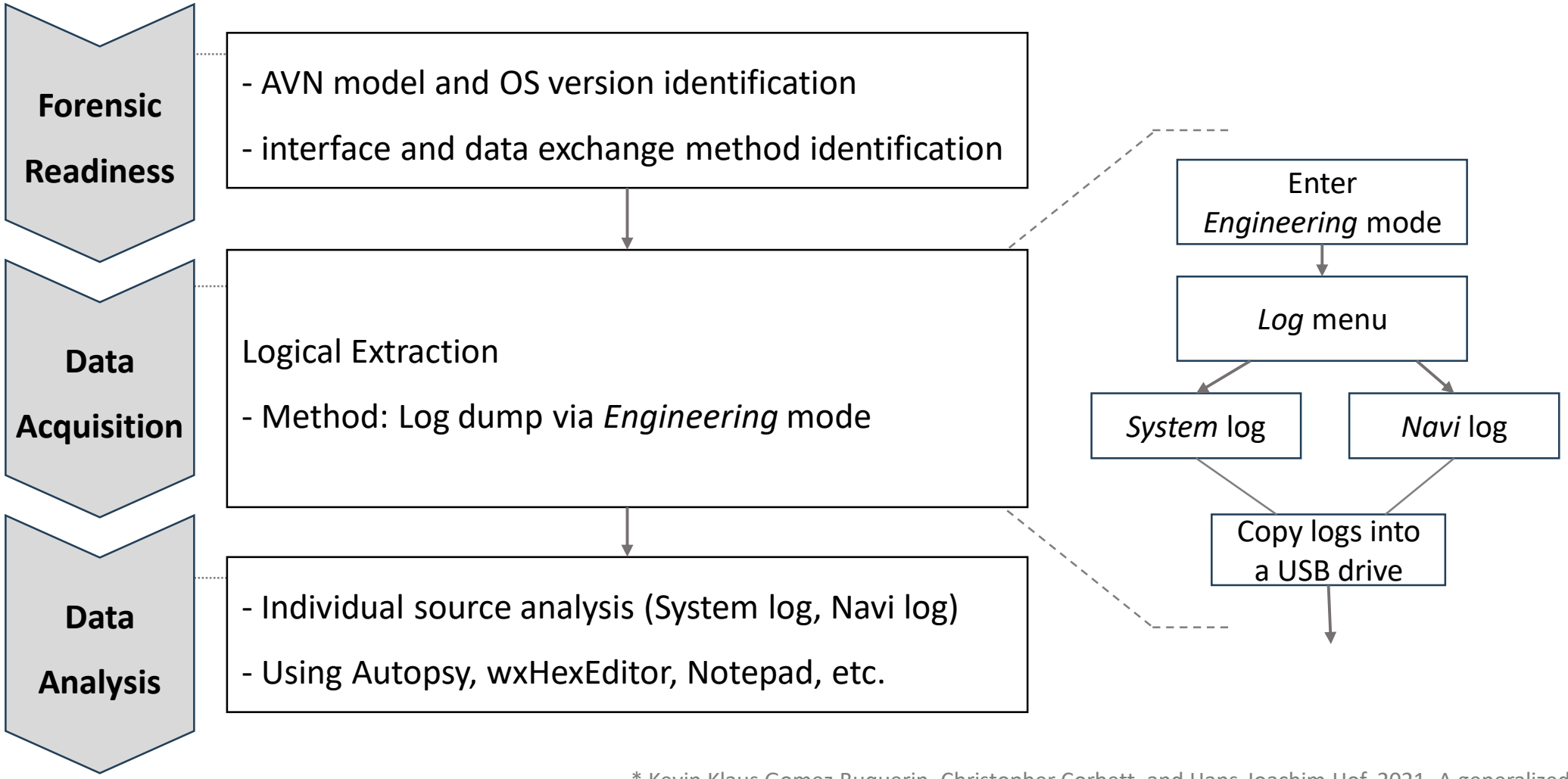
[7] Kang et al. (2023), **“Android-Based Audio Video Navigation System Forensics”**, *Applied Sciences*

Target Systems	KIA K5 2017, KIA NIRO EV, Hyundai Sonata DN8, KIA All New Morning
Acquisition Method	Chip-off, Hidden menu (Engineering mode)
Extracted Artifacts	System log, Bluetooth data, Navigation app data

02

Forensic Investigation Process and Target System

❖ Digital Forensic Investigation Process



* Kevin Klaus Gomez Buquerin, Christopher Corbett, and Hans-Joachim Hof. 2021. A generalized approach to automotive forensics. Forensic Science International: Digital Investigation 36 (2021), 301111

2. Forensic Investigation Process and Target System

❖ Target System

- **Vehicle Model**: KIA K5 2017
- **AVN**: Compact 5th generation
- **OS**: Android Jellybean (4.2.2)
- **Kernel Version**: Linux 3.1.10

❖ Forensic Tools

- Autopsy
- Notepad
- wxHexEditor
- Epoch Converter

03 Forensic Data Acquistion

3. Forensic Data Acquisition

❖ Forensic Data Acquisition Process

Target AVN → **USB drive**

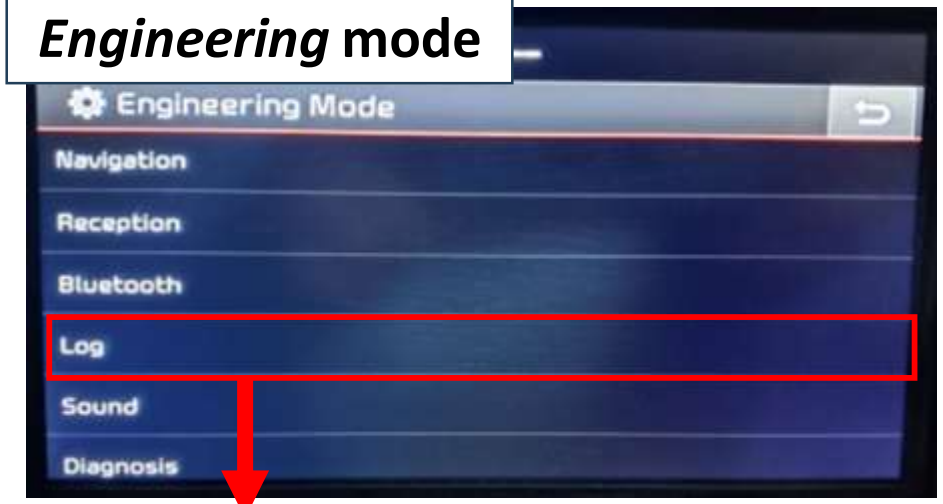
System log data

Navi log data

1. Connect a USB drive to AVN
2. Access *Engineering mode*
3. Go to *Log* menu
4. Copy two logs into USB drive (*System* log / *Navi* log)
5. Two compressed files are copied to USB drive

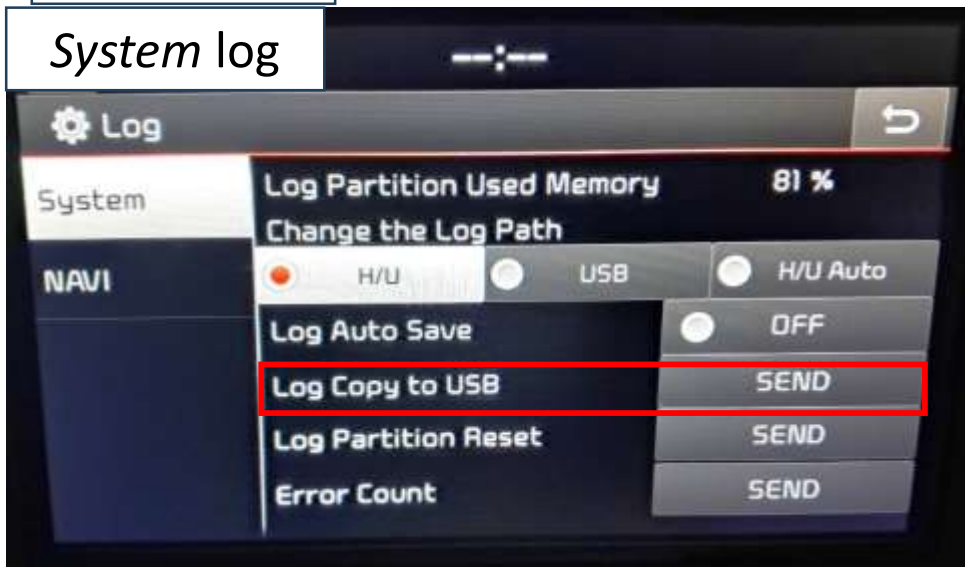
3. Forensic Data Acquisition

***Engineering* mode**

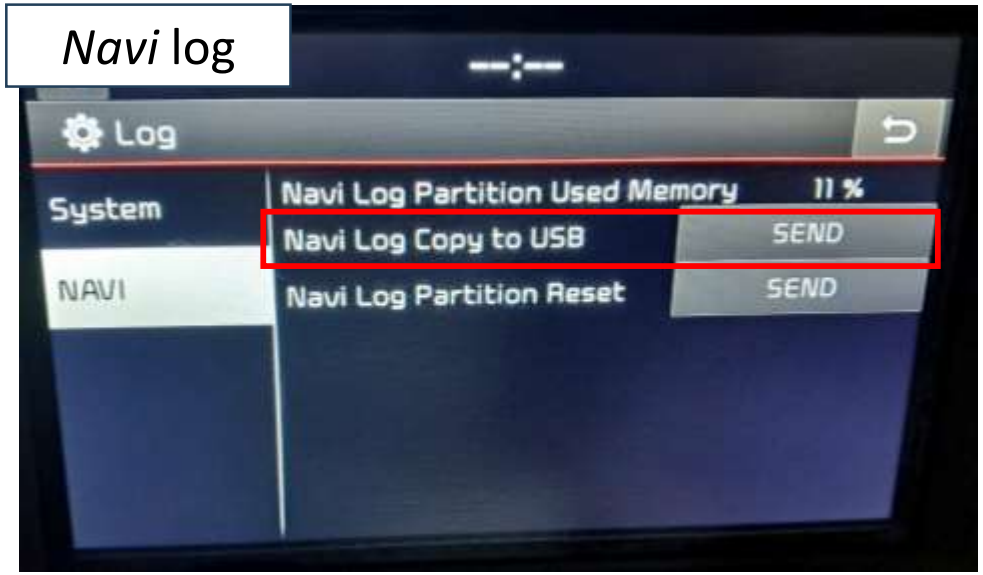


***Log* menu**

System log



Navi log



04 Analysis

❖ Analysis of *System* log

* date : [yyyymmhh]
* time : [hhmmss]

- Extracted file: dropbox_[date].[time].tar

File		
dropbox_[date].[time].tar		
Path	**File Paths**	**Description**
/data	…/dump@######_dumpstate.txt	Info. of Smartphone connected through Bluetooth
/ivilog	…/trace_log.txt.#.	User behaviors (Music and Radio playback; Info. of Smartphone connected through Bluetooth
	…/SYSTEM_BOOT@######_[epochtime].txt	AVN booting time
	…/infobigdata.everylog.json	User behaviors (Bluetooth audio playback, Destination info, location info.)
	…/infobigdata.snapshot.json	User behaviors (Bluetooth audio playback, Destination info, location info.)
	…/Standard_Log.dat	Location at the specific time, Info. of Smartphone connected through Bluetooth

❖ Analysis of *System* log

* date : [yyyymmhh]
* time : [hhmmss]

- Extracted file: dropbox_[date].[time].tar - **infobigdata.everylog.json**

Category	Description
ccs	-
PhoneProejction	-
bt	Blutooth audio play (songTitle, songArtist, songAlbum, playingTime)
navi	The location, speed, destination name, and GPS information at the time of route deviation, route guidance interruption, or route guidance termination
System	accOn/OffTime, ignOnTime
vr	-
vi	Video camera
ux	-
av	Radio information(Frequency, station name, dateTime), DMB

❖ Analysis of *Navi* log

* date : [yyyymmhh]
* time : [hhmmss]

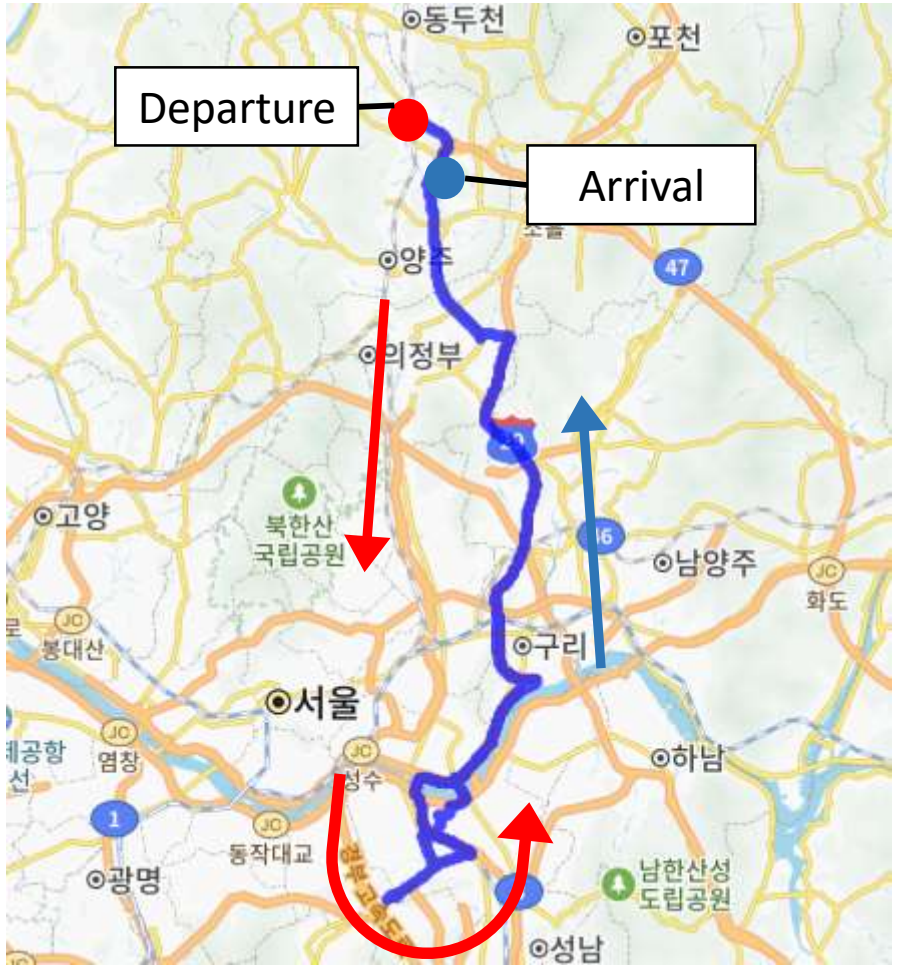
- Extracted file: NaviLog_[date].[time].tar

File		
NaviLog_[date].[time].tar		
Path	**File Paths**	**Description**
/ivilog	…/infobigdata.everylog.json	User behaviors (Bluetooth audio playback, Destination info, location info.)
	…/infobigdata.snapshot.json	User behaviors (Bluetooth audio playback, Destination info, location info.)
	…/Standard_Log.dat	Location at the specific time, Info. of Smartphone connected through Bluetooth
/KOR	/USERPOI/#.muj	User's registered place names (place name, addresses, latitude, longitude)
	/USERRECENT/#.muj	The most recent search term, destination address, phone number, latitude, longitude, and administrative code
	/GPSTrack.dat	GPS records (latitude, longitude, and administrative code)
	/Last_Route_Info	Last search term and GPS coordinates of the most recent destination
	/startlog_[epochtime].txt	AVN booting time

❖ Analysis of *Navi* log

- Extracted file: NaviLog_[date].[time].tar – **GPSTrack.dat**

* date : [yyyymmhh]
* time : [hhmmss]



05 Discussion

❖ Data Artifacts extracted from Each *Log* Menu

System Log

◆ Extracted File: *dropbox_[date].[time].tar*

- **Information on smartphones connected to the AVN via Bluetooth**
- **User behaviors**: music, radio playback, destination info and location info etc.
- **AVN booting time**
- **Calling status of smartphone**

Navi Log

◆ Extracted File: *NaviLog_[date].[time].tar*

- **Information on smartphones connected to the AVN via Bluetooth**
- **User behaviors**: music, radio playback, destination info and location info etc.
- **AVN booting time**
- **User-registered Data**: place names, last search term, destination address, latitude and longitude etc.
- **GPS records**: latitude, longitude, and administrative code

5. Discussion

❖ Digital Forensics on an Android-based AVN system

System Log

Navi Log

Collect and Analyze log files → "User Behavior " Identification

❖ Comparison with Previous Study

	Previous study [7]	This study
Data Acquisition	*Chip-off*, *Engineering mode*	*Engineering mode*
Rooting required	Need to root target device	No need to root target device
Analysis	*System* Log	*System* Log and *Navi* Log

5. Discussion

Limitations

- **Lack of Generalization**:

  investigation on only the AVN system of KIA K5 2017 (Android OS 4.2.2 Jellybean)

- **Lack of Automation**
- **Privacy issues**: Two logs include personal information

Future Work

- **Generalization**: Analyzing other AVN systems with the latest Android versions
- **Event Scenario-based Experiment**: To track how useful artifacts are generated and stored
- **Automation of the Forensic Process:** Development of AVN system forensics tool

06 Conclusions

6. Conclusion & Future Work

Conclusions

- **Vehicle forensic investigation on Android-base AVN system** :
  - Efficient data collection: System log and Navi log via engineering mode
  - Effective Analysis **:** Obtaining new artifacts from Navi log

Q & A

Forensic Investigation of An Android Jellybean-based Car Audio Video Navigation System

Keywords: Vehicle forensics, Audio Video Navigation, System log, Navigation log

Yejin Yoon / yoon17710@dankook.ac.kr

Seong-je Cho / sjcho@dankook.ac.kr