Automotive Crash Data Collection and Analysis: A Log-Based Case Study

MobiSec 2024

Computer Security & OS LAB

Author : Jeehun Jung, Kyoungwon Suh, Seong-Je Cho, Gyunseung Ahn

Presenter : Jiheun Jung

Affiliation : Dankook University

Email : wlgjsjames7224@dankook.ac.kr









Introduction

Introduction

- Adoption of Digital Technology in Modern Vehicles
 - Event Data Recorder (EDR), In-Vehicle Infotainment (IVI) Systems, Telematics, ...
 - GPS navigation, Connecting smartphone to car,

Music streaming, Hands-free calling

- Role and Limitations of EDR
 - Vehicle accident data analysis has predominantly focused on event data recorders (EDRs)
 - Capturing crucial information about the vehicle during a brief period before and after a collision
 - Limitations of Accessing EDR Data
 - It varies across automobile manufacturers
 - Analysis is often restricted by its proprietary formats



[Source : "Security concerns in co-operative intelligent transportation systems" (2017)]







This paper,

- proposes a novel method for analyzing log data of an IVI system to determine the cause of a car accident
 - Vehicle speed, seat belt status, airbag deployment, door status and revolutions per minute(RPM)
- validates the effectiveness of the proposed method:
 - Experiments were conducted using the Hyundai Avante CN7

*Key finding: Log data of an IVI system can be a valuable resource for car accident analysis

- providing reliable legal evidence
- aiding in determining liability for vehicle collision.





Related Work

Related Work

- * "Analyzing driver response in real-world fatal crashes using the event data recorder" (Y. Ahmad et al.)
 - Investigation of 16 accident cases involving passenger cars equipped with EDRs from 2019 to 2021
 - Analysis of driver responses 5 seconds before the collision (braking, acceleration, steering control, etc.)
 - Data extraction using the 'OBD Method' and 'Direct Method'
- "Accident posture reconstruction and analysis of a purposed vehicle event data recorder" (Putra I et al.)
 - Limitations of traditional EDRs: insufficient accident-related data
 - Proposal for advanced event data recorders with more comprehensive data storage
- "Identifying near-miss traffic incidents in event recorder data" (S. Yamamoto et al.)
 - Utilizing EDR data to identify near-miss traffic incidents
 - Developing a predictive model to assess accident likelihood through EDR data analysis







'OBD Method'

'Direct Method'

Related Work

"Practical data acquisition and analysis method for automobile event data recorders forensics" (Lee et al.)

- **Proposing a comprehensive approach** for collecting and analyzing EDR data
- Classified into the 'Canonical Method' and 'Non-Canonical Method'



 STEP2: Identification of the memory in which the EDR data are stored in the ACU. In general, EDR data are stored in an electrically erasable programmable read-only memory (EEPROM).







- * "Validation of EDR data for the purpose of the forensic expertise" (Nouzovský et al.)
 - Evaluate the reliability of EDR data
 - Assessment through comparison with video footage, skid marks, and witness statements
 - Reliable information, but cross-validation with other investigative methods is essential





Forensic Method for car crash investigation

Forensic Method for car crash investigation



ivi system			
Vehicle Model	Hyundai Avante	Acquisition	Sandisk cruzer blade 64gb usb 2.0
IVI Manufacturer	Hyundai Mobis	Acquisition	
OS	Android 4.4.2 (KitKat)		Autopsy 4 20 0
Kernel Version	Linux 3.18.24-tcc	Allalysis	Autopsy 4.20.0





Analysis of Automotive Crash Data

- Analyzing Log files of the IVI system
 - Files were created or modified after starting driving
 - Telematics.log, eventslogs.log, dumpstate-[date].txt
- Date/Time Description Event Typ 2024-09-05 16 46:24 //og-20240905 164622 ter/./vcrm.log/Error.Log/e File Mod 2024-09-05 16:46:23 //og-20240905,164622.tar//update/dmclient_0.txt 2024-09-05 16:46:22 /log-20240905.164622.tat//telematics.log File Mod 2024-09-05 16:46:22 /log-20240905;164622;tat//micomlog#20240905;16461 2024-09-05 16:46:20 /log-20240905,164622,ter//modem/wrmdll05.log File Mo 🖃 🏥 log-20240905,164622,tar (2) 2024-09-05 15:46:18 /log-20240905.164622.tar/cem_data/log/eventlogs. File Mod 2024-09-05 15:46:17 //oq-20240905.164622.tm/. File Modi ė- 🚺 . (121) 2024-09-05 16:46:17 //og-20240905.164622.tet//LogList.trt File Mod 🗊 📙 backup_data (39) 2024-09-05 15:48:17 /log-20240905.164622.ter//LS_JogFiles File Mor BluetoothLog (1) 2024-09-05 16:46:17 //og-20240905,164622.tar//LS_logFiles/LocationSharing.log File Mo 2024-09-05 16 46 15 //og-20240905,164622,1ar/./dumpstate-20240905,164512.00,txt,g - 📜 databases (2) 2024-09-05 18:46:12 /log-20240905.164622.tat//molgen2.log File Mod history (2) 2024-09-05 16:46:10 /log-20240905,164622.tat//TeleService.to File Mod infox(1) 2024-09-05 16:46:10 //og-20240905.164622.tar/./log_11.txt File Modi D- LS_logFiles (25) 2024-09-05 16 45 18 /log-20240905,164622,tet//micomlog#20240905,164518,txt 🖮 📜 modem (18) 2024-09-05 16:45:15 //og-20240905,164622.tar//LS_JogFiles/LSLog_20240905164515,zip File Mod 2024-09-05 16:45:15 //og-20240905.164622.tet//bluetoothLog File Mo - 🗱 wmmdll00.log.gz (1) 2024-09-05 16:45:15 //log-20240905;164622;ter//bluetoethLog/87_Log_20240905_164515;zip File Mod - 🌆 wmmdll01.log.gz (1) 2024-09-05 16:45:14 //og-20240905.164622.tar//screencep-20240905.164512.00.png - 🌆 wmmdl102,log.gz (1) 2024-09-05 16 45 14 //og-20240905 164622 tar/ /LS_logFiles/LSLog_20240905164515 zip/data/svstem/dropbox/LS_logF File Mod - 10 wmmdl103,log,gz (1) 2024-09-05 16 45 10 /log-20240905,164622, tar//bluetoothLog/BT_Log_20240905_164515,zip/bluetoothLogFiles/bluetoothLogFil 2024-09-05 16:45:06 //og-20240905.164622.ter/./EngMode.log File Mod wmmdll04,log.gz (1) 2024-09-05 16:44:59 //og-20240905;164622;tar//databases/settings.db - 10 wmmdl105,log.gz (1) 2024-09-05 16 44 59 /log-20240905,164622,ter//databases/settings.db-- 🗱 wmmdl106,log.gz (1) 2024-09-05 16:44-52 //og-20240905.164622.tar//bluetoothLog/BT_Log_20240905_16 File Mor - 10 wmmdl107,log.gz (1) 2024-09-05 16:44:32 //og-20240905 164622 tat/./bluetoothLog/BT_Log_20240905_16 File 2024-09-05 16 41 40 /log-20240905 164622 tar//blue to ethLog/BT_Log_20240905_ - 10 wmmdl108,log.gz (1) 2024-09-05 16:40:27 //og-20240905.164622.tat//update/otaclient_0.txt 🏂 telematics,log - 🏥 wmmdl109,log.gz (1) 2024-09-05 16:40:27 //og-20240905.164622.tar//motgenZota.log J recovery (25) 2024-09-05 16 40 16 //og-20240905,164622,tet//history/updatehistory_depth/og 🕭 eventlogs,log 2024-09-05 16:40.16 /log-20240905,164622.ter//history/updatehistory.log TMOS (1) dumpstate=20240905,164512,00,txt 2024-09-05 16 40:15 //og-20240905,164622,tar//update/dmclient_con_0.txt Update (55) 2024-09-05 16:40 13 //o.g-20240905.164622.tar/./infox worm_log (4)
 worm_log (4)
 2024-09-05 16:40-13 //og-20240905,164622,ta///infox/serve dumpstate-20240905.164512.00.txt.gz (1 2024-09-05 16:40:10 //og-20240905.164622.ter/./infox/server/order_2.infox_tw.txt oem_data(1) 024-09-05 16:40:10 /log-20240905.164622.tat//infox/server/order_1.infox_mic

Dividing <u>the log data</u> into six categories

Index	Description	
1	Vehicle Movement	
2	Vehicle Speed	
3	Vehicle Collision	
4	Vehicle Location	
5	Vehicle Assist System	
6	Vehicle Door Status	



1. Vehicle Movement data

./telematics.log

• True: started moving

• False: stopped moving

2. Vehicle Speed data

./dumpstate-[date].txt

A. Current vehicle speed

- B. Current speed from the system
- C. Changes in the vehicle's speed

Time	File	logmessage
09-05 16:44:14	./telematics.log	[EngineIdleAlarmTask] Vehicle Movement Status Changed to true
09-05 16:44:14	./telematics.log	[EngineIdleAlarmTask] ADM ON: false Gear in Parking: false Vehicle Moving: true mPwrAutoOffTimer: -1 Validity Status: false

	Time	File	logmessage
Α	09-05 16:44:09	./dumpstate-[date].txt	SystemService: [SystemService.getVehicleSpeed] speed: 0 , called by 1400
В	$09-05 \ 16:44:14$	$./dumpstate\-[date].txt$	SystemService: SYS_SPEED_M: 12
С	09-05 16:44:14	$./dumpstate\-[date].txt$	SystemService: Vehicle Speed Changed to : ${\bf 12}$
	09-05 16:44:14	./dumpstate-[date].txt	UsageLoggingService: onVehicleSpeedChanged - speed: ${f 12}$

3. Data related to Vehicle Collision

- ./dumpstate-[date].txt
- Collision occurred
- Presence of passengers
- Seatbelt usage
- Rollover sensor activation
- Transmission position
- Engine Oil temperature
- RPM
- Airbag deployment status
- Parking brake activation.

Time	File	logmessage
09-05 16:44:55	./dumpstate-[date].txt	TAS_HS : iBox CrashPos_F_First:0 CrashPos_F_Full:0 CrashPos_Driver:0 CrashPos_Passenger:0 OccupancyDr:1 OccupancyPa:0 SeatBeltDr:0 SeatBeltPs:0 SeatBeltRrCtr:1 SeatBeltRrRt:1 SeatBeltRrLft:1 RolloverSensor:1 TransmissionPos:5 EngineTemperature:87.75 EngineTemperatureUnit:0 Rpm:796 AirbagsDeployed:1 ParkBreak:1



4. Vehicle Location data

- ./telematics.log, ./dumpstate-[date].txt
- 'Address_name' filed

Share this location

Directions from here

Directions to here What's here? Search nearby

Add a missing place Add your business

Report a data problem Measure distance

Print

Latitude and Longitude are masked

.

0

0

0

Lat:***580222** Lon:****876086*

37.66044, 126.9205

Your location

Deogyang-gu

09-05 16:40:17	telematics log	[McpWeatherLooper]Weather == Received intent from payi : com mpsoft payi request mcp
	toromaticonog	DestNWaypoint.Weather wayPointID : -1, 99, 99, 99, Address_name : Deogyang-gu , Goyang-si , , , ,
09-05 16:43:34	telematics.log	[CMM][2]LastGps Lat: ***580222** Lon: ****876086 type:0 GMTTime:20240905074334 LocalTime:20240905164334 Head:235
09-05 16:45:12	./dumpstate-[date].tx	DUMP OF SERVICE location: Last Known Locations: gps: Location[gps $37.579692,126.875139$] acc=6 accH=0 accV=0 accP=0 odoS=1 gyroS=1 t back=0 modocount=0 gpstatus=1 drstatus=1 accelstatus=0 angle=0 t= 2012107079000 tv=0 et= $+12m4s781ms$ alt=0.0 vel=0.0 bear= 235.83252 gnssSpeed=0.0 gnssHeading=0.0 Bundle[satellites=0, DREHPE= 8.543833]]
ude: 37.58022 itude: 127.87	22** '6086*	Decedeoksan ro Deedeoksan ro Og-05 16:45.12 Arrival points Gayango Gyel NGGI DO SEOUL

Computer Security & OS LAB

DONGSAN-DONG 동산동

Vehicle Assist System data 5.

- ./telematics.log
- Status of TCS (Traction Control System)
- Status of LKA (Lane Keeping Assist) system
- status of the LDWS (Lane Departure Warning Syster
- 0: No issues
- Positive: issues

Vehicle Door Status data 6.

- ./oem data/log/eventlogs.log, ./telematics.log
- 1: Door opened
- 0: Door closed

		[CAN] temp =0 mTroubleDiagMilLamp.CF_Lkas_Ldws SysState=0
09-05 16:45	:58 ./telematics.log	[CAN] temp =0 mTroubleDiagMilLamp.TCS_LAMP=1
em)		[CAN] temp =0 mTroubleDiagMilLamp.CF_LKA_Symbol State=4
		[CAN] temp =0 mTroubleDiagMilLamp.CF_Lkas_Ldws SysState=15
Time	File	logmessage
09-05 16:43:48	./oem_data/log/eve	entlogs.log ivi_welcome_driver_door_opened:
	./telematics.log	[RVP]notiDoorChange() prevDoor : 0 , curDoor : 1

logmessage

State=0

[CAN] temp =0 mTroubleDiagMilLamp.TCS_LAMP=0

[CAN] temp =0 mTroubleDiagMilLamp.CF_LKA_Symbol

[EngineIdleAlarmTask] Driver Door Open

[EngineIdleAlarmTask] IGN ON: true Parking Gear ON: true Driver Door Open:

Status Changed to true

true Service Status: true

Time

09-05 16:44:15

File

./telematics.log

5. Vehicle Door Status data

- ./oem data/log/eventlogs.log, ./telematics.log
- 1: Door opened
- 0: Door closed

Time	File	logmessage	
09-05 16:43:48	$./oem_data/log/eventlogs.log$	ivi_welcome_driver_door_opened:1	
./telematics.log		[RVP]notiDoorChange() prevDoor : 0 , curDoor : 1	
		[EngineIdleAlarmTask] Driver Door Open Status Changed to true	
		[EngineIdleAlarmTask] IGN ON: true Parking Gear ON: true Driver Door Open: true Service Status: true	

6. Vehicle Assist System data

- ./telematics.log
- Status of TCS (Traction Control System)
- Status of LKA (Lane Keeping Assist) system
- status of the LDWS (Lane Departure Warning System)
- 0: No issues
- Positive: issues

Time	File	logmessage
09-05 16:44:15	./telematics.log	[CAN] temp =0 mTroubleDiagMilLamp.TCS_LAMP= :0
		[CAN] temp =0 mTroubleDiagMilLamp.CF_LKA_Symbol State=0
		[CAN] temp =0 mTroubleDiagMilLamp.CF_Lkas_Ldws SysState=0
09-05 16:45:58	./telematics.log	$[CAN] temp = 0 mTroubleDiagMilLamp.TCS_LAMP = 1$
		[CAN] temp =0 mTroubleDiagMilLamp.CF_LKA_Symbol State=4
		[CAN] temp =0 mTroubleDiagMilLamp.CF_Lkas_Ldws SysState=15





Discussion

Discussion

Timeline that reconstructs the driver's actions

- Vehicle's location information
- Estimation of Driver's behavior
- Vehicle's condition
- Estimating the time of the accident (09-05 16:44:21)

- Some limitations
 - Considering to a specific car model
 - Needed to enter Engineering mode

Time	\mathbf{Event}	Description	
09-05 16:40:17.2	Vahiala location information	Deogyang-gu, Goyang-si	
09-05 16:43:34.4	- venicle location information	Latitude: ***580222**, Longitude: ****876086*	
09-05 16:43.48.1	Driver's door	Open	
09-05 16:43:57.7	- Driver's door	Close	
09-05 16:44:09.2	Vehicle speed	$0 \mathrm{km/h}$	
09-05 16:44:14.6	Vehicle start Ve	hicle Collision	$12 \mathrm{km/h}$
$09-05\ 16:44:21.4$	Vakielo groad		$64 { m km/h}$
$09-05 \ 16:44:21.6$	- venicie speed	29km/h	
09-05 16:44:37.6	Vehicle stop	0km/h	
09-05 16:44:55.8	Vehicle status	AirbagsDeployed, RPM 796	
09-05 16:45:12.1	Vehicle location information	Latitude: 37.579692, Longitude: 126.875139	

Automotive crash timeline





Conclusion and future work

Conclusion

- A new method for collecting and analyzing log data from IVI systems for vehicle accident investigations
 - It can help determine the cause of car crashes
- Critical data related to car accident could be obtained without relying on manufacturer-specific tools
 - Date type: vehicle speed, vehicle assist system data, vehicle movement, airbag deployment,
 - The data can be used to complement EDR data

Future work

- Our method should be extended to a wider range of vehicle models
- Automated tools are needed for efficient analysis







Presenter : Jeehun Jung E-mail :: wlgjsjames7224@dankook.ac.kr