WDSC 논문

2022.08.09

정지헌

INDEX

01

서론

서론

- 차량이 주변 인프라와 상호작용을 통해서 사용자에게 편의성과 안전성 제공
- 이 중 모바일 기기 분야에서 대표적으로 구글의 안드로이드 오토, 애플 카플레이 등이 있다.
- OBD-II를 통해서 차량의 진단정보를 모바일기기 앱에서 확인할 수 있는 서비스 제공
- 최근 차량에 많은 보안사고가 발생하면서 명확한 사

BMW·테슬라·볼보 잇단 급발진 추정사고…'높은 소송의 벽' 재판 관건은 [공포의 질주 下]

- 인포카의 OBD-II 기반 모바일 앱은 차량의 정보를 제공을 통해 사고 원인 규명에 도움을 줄 수 있다.
- 본 논문에서는 사용자 이벤트 기반 시나리오를 구성하고 데이터를 축적하여 앱 포렌식을 하였다.

02

배경지식

OBD-II

- CAN 버스 위에 있는 고수준의 통신 프로토콜
- OBD는 1996년 이후 배출가스 검사를 위해서 미국에서 차량에 탑재하도록 의무화
- 차량 식별 번호, 점화 카운터등 정보를 제공
- 스캐너를 통해서 사용자의 스마트폰에 전달
- 포트의 위치는 차량 왼쪽 대시보드 아래에 위치

인포카 앱

- 자동차 진단 및 관리 서비스를 제공해주는 모바일 앱
- OBD-II 스캐너와 블루투스 또는 와이파이 통신으로 차량정보 전달

https://play.google.com/store/apps/details?id=mureung.obdproject&hl=ko&gl=US

03

인포카 앱 포렌식 과정

인포카 앱 포렌식 과정 (실험환경)

차량	
제조사	현대 자동차
모델	Avante(CN7)
연식	2020
모바일 기기	
모델	Samsung Galaxy S8(SM-G950N)
안드로이드 버전	Android 9.0(Pie)
OBD-II	
OBD-II 스캐너	IO180-OH
인포카 앱 버전	2.24.35

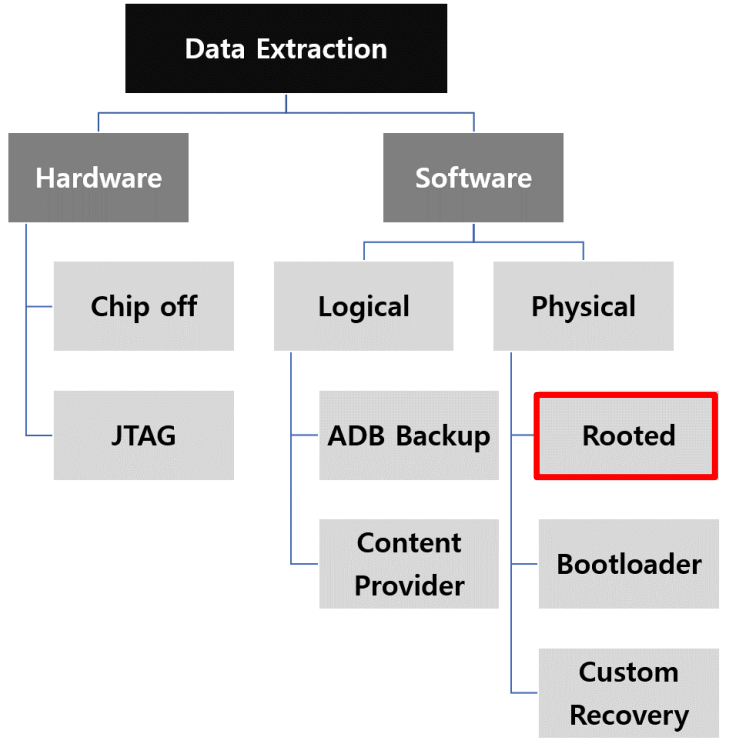
실험 환경

https://www.hyundai.com/kr/ko/brand/heritage/model/avante-history/2020-avante-cn7
https://www.android.com/intl/ko_kr/phones/samsung-galaxy-s8/
https://infocarmobility.com/sub/io180_oh

인포카 앱 포렌식 과정 (실험환경)

❖ 데이터 획득 방법

- 하드웨어 기반 획득
  - Chip-off : 스마트폰의 PCB에서 플래시 메모리의 데이터를 복제하여 획득
  - JTAG : 스마트폰의 PCB에서 JTAG 인터페이스를 연결하여 데이터를 획득
- 소프트웨어 기반 획득 (논리적)
  - ADB Back up : 안드로이드에서 내장된 백업기능을 활용
  - Content Provider : 안드로이드 앱 간에 데이터 공유하는 기술 활용
- 소프트웨어 기반 획득 (물리적)
- 본 논문에서는 루팅을 이용한 기법을 사용



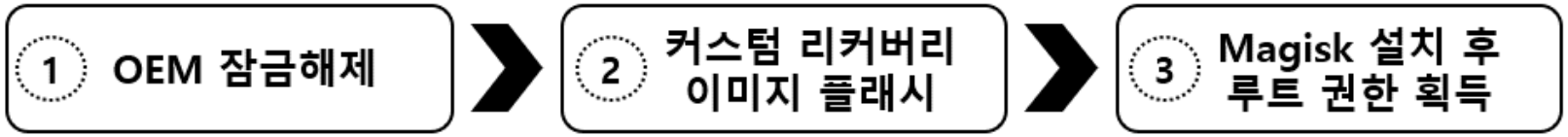
최재원, 김승주, 모바일 포렌식 증거 수집방안 연구: 제조사 백업 앱 기반 데이터 획득 기법, 정보보호학회논문지, 28권, 1호, pp. 95-110, 2018

인포카 앱 포렌식 과정 (시나리오 구성)

Time	Function	Event	OBD Scanner
17:19	Power on	차량 시동 On	
17:20	Blutooth Connection	블루투스로 인포카 앱과 연동	OBD-II 포트와 연결
17:23	Drive	주행 시작	
17:38	Power off	차량 시동 Off	OBD-II 포트에서 제거하지 않음
17:39	Power on	차량 시동 On	
17:39	Blutooth Connection	블루투스로 인포카 앱과 연동	OBD-II 포트와 연결
17:40	Drive	주행 시작	
17:54	Power off	차량 시동 Off	
17:55			OBD-II 포트에서 제거

- 사용자 이벤트 기반 시나리오 설계
- 차량 시동 ON/OFF, 주행시작/종료, OBD연결 위주로 작성

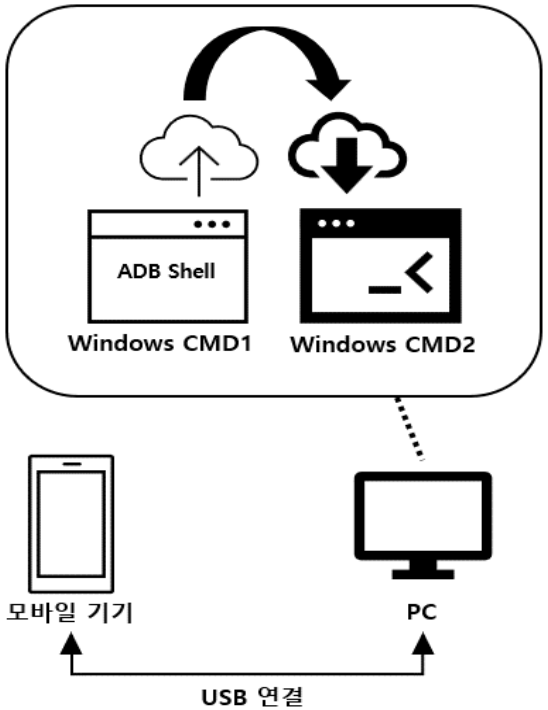
인포카 앱 데이터 획득



❖ 모바일기기의 루팅 진행 과정

- 모바일 기기 OEM잠금 해제
- Odin을 사용하여 TWRP에서 받은 사용자 정의 복구 모드 이미지 플래시
- Twrp진입하여 설치 기능을 통해 Magisk설치
- Magisk앱에서 루팅 수행

인포카 앱 데이터 획득



❖ 디스크 덤프 과정

- 모바일 기기와 PC연결후 PC에서 ADB쉘 접근
- Busybox 앱 모바일기기에 설치
- /data 파티션의 마운트 정보 확인
- PC와 모바일 기기 사이에서 TCP 소켓 통신을 가능하게 해준다.
- /data 파티션을 PC에 이미징

인포카 앱 데이터 분석

/data/mureung.obdproject /databases/	설명
WMI.db	World Manufacturer Identification의 약자로 차량의 제조업체에 대한 정보가 존재
STD_OBD2_PID.db	암호화로 추정됨
PROFILE.db	암호화로 추정됨
InfoCar.db	운전자의 주행정보와 개인정보 차량정보가 저장된다.
DTC.db	Diagnostic Trouble Code의 약자로 차량의 진단 코드명이 존재

- /data/mureung.obdproject/databases/의 db파일
- 차 사고와 가장 연관된 DB는 Infocar.db
- STD_OBD2_PID.db PROFILE.db
  - Autopsy 도구의 기능을 통해 엔트로피값 8에 근접
- WMI.db DTC.db
  - 인포카 앱에서 이미 만들어 놓은 데이터

인포카 앱 데이터 분석(USERINFO 테이블)

Table USERINFO 1 entries Page 1 of 1 Export to CSV

userName	userEmail	carName	carMaker	carYear	carModel	carFuelT...	allDistan...	avrFuel...	obdSN	drvFinishTime
정지현	csosdusrntlf2738@gmail.com	cn7	현대	2020	아반떼	Gasoline	40,500614	8,671122	66:1E:11:09:01:0D	20220714175507

Time	Function	Event	OBD Scanner
17:19	Power on	차량 시동 On	
17:20	Blutooth Connection	블루투스로 인포카 앱과 연동	OBD-II 포트와 연결
17:23	Drive	주행 시작	
17:38	Power off	차량 시동 Off	OBD-II 포트에서 제거하지 않음
17:39	Power on	차량 시동 On	
17:39	Blutooth Connection	블루투스로 인포카 앱과 연동	OBD-II 포트와 연결
17:40	Drive	주행 시작	
17:54	Power off	차량 시동 Off	
17:55			OBD-II 포트에서 제거

- 사용자 이름, 이메일, 차량 연식, 차량 모델명 등
  - 인포카 첫 사용시 등록한 기본정보와 차량정보

- OBD-II 스캐너 블루투스 MAC주소, 마지막으로 차량을 사용한 시간저장
  - 마지막으로 차량을 사용한 시간 = drvFinishTime
  - “20220714175507” => YYYYMMDDHHMMSS
  - 시나리오시간정보에서 OBD-II 스캐너 제거와 매칭

인포카 앱 데이터 분석(DRVREC 테이블)

Table DRVREC 4 entries Page 1 of 1 Export to CSV

_id	drvValue	userSN	drvKey	drvIsHid...	drvStartTime	drvFinishTime	drvLatitude	drvLongitu...	drvAddress
1	22070601	1	9874806	0	20220706155615	20220706163752	37,361026	127,1194287	대한민국 경기도 성남시 분당구 정자동 202
2	22063001	1	9681908	0	20220630154426	20220630161410	37,381182	127,1230882	대한민국 성남시 서현고등학교
3	22071401	1	9929943	0	20220714151436	20220714161115	37,3244442	127,1260347	대한민국 경기도 용인시 수지구 죽전1동 1338-5
4	22071402	1	null	0	20220714172026	20220714175507	37,3235212	127,1242471	대한민국 경기도 용인시 수지구 죽전1동 147

- 차량의 운행 관련 정보가주로 저장
  - 운행시작/종료시간, 총 주행거리, 도착지점과 출발지점, 연비, 평균주행속도
- drvAddress = 도착지점, drvStartAddress = 출발지점

인포카 앱 데이터 분석(SRCREC 테이블)

Table SRCREC 5342 entries Page 34 of 54 Export to CSV

_id	srcValue	userSN	realTime	srcLatit...	srcLong...	srcSpeed	srcRPM	srcAPS	srcTPS	srcRPS
3328	22071401	1	20220714161111	37,3244442	127,12603...	0,0	0,0	14,90196	14,509804	0,0
3329	22071401	1	20220714161112	37,3244442	127,12603...	0,0	0,0	14,90196	14,509804	0,0
3330	22071401	1	20220714161113	37,3244442	127,12603...	0,0	0,0	14,90196	14,509804	0,0
3331	22071401	1	20220714161114	37,3244442	127,12603...	0,0	0,0	14,90196	14,509804	0,0
3332	22071402	1	20220714172026	0,0	0,0	0,0	704,0	14,90196	0,0	0,0
3333	22071402	1	20220714172027	0,0	0,0	0,0	704,0	14,90196	0,0	0,0
3513	22071402	1	20220714172327	0,0	0,0	0,0	700,0	14,90196	14,509804	0,0
3514	22071402	1	20220714172328	0,0	0,0	0,0	700,0	14,90196	14,509804	0,0
3515	22071402	1	20220714172329	0,0	0,0	0,0	676,5	14,90196	14,509804	0,0
3516	22071402	1	20220714172330	37,2395975	127,178017	2,0	676,5	14,90196	14,509804	0,0
3517	22071402	1	20220714172331	37,2395841	127,178023	2,0	676,5	14,90196	14,509804	0,0

Time	Function	Event	OBD Scanner
17:19	Power on	차량 시동 On	
17:20	Blutooth Connection	블루투스로 인포카 앱과 연동	OBD-II 포트와 연결
17:23	Drive	주행 시작	
17:38	Power off	차량 시동 Off	OBD-II 포트에서 제거하지 않음
17:39	Power on	차량 시동 On	
17:39	Blutooth Connection	블루투스로 인포카 앱과 연동	OBD-II 포트와 연결
17:40	Drive	주행 시작	
17:54	Power off	차량 시동 Off	
17:55			OBD-II 포트에서 제거

- 차량의 실시간 진단 데이터 저장
  - RPM(Revolutions per Minute), APS(Accelerator pedal position sensor), TPS(Throttle position sensor), RPS(Revolutions Per Second)
- RPM, APS, TPS, RPS등의 속성정보가 1초단위로 저장

- 위도, 경도 데이터는 차량이 움직인 시점부터 저장
  - 위도, 경도를 제외하고는 OBD연결시점부터 데이터가 저장

실험(분석)

❖ 분석 방법

- Autopsy 포렌식 도구 사용

- 시나리오의 타임라인과 영상정보를 활용하여 인포카 앱의 시간정보와 매칭

04

논의

논의

- 허욱이 진행한 방식:
  - 로그파일을 통해 db파일 재구성
  - 테이블 속성정보 간단한 설명
- 본 논문에서 진행한 방식:
  - 루팅을 통한 데이터 베이스분석
  - 사용자 행위 시나리오 기반 데이터 축적
  - 사용자 행위와 비교하여 데이터 분석

테이블 명	데이터
USERINFO	사용자 이름, 이메일, 차량 연식, 차량 모델명, 사용하는 연료 등
DRVREC	운행 시작/종료 시각, 총 주행거리, 도착지점과 출발지점, 연비, 평균 주행속도 등
SRCREC	RPM, APS, TPS, RPS, 위/경도 등

Infocar.db 테이블 및 데이터

05

결론 및 향후 연구

결론 및 향후 연구

❖ 본 논문에 대한 설명

- 사용자 이벤트 기반 시나리오를 설계하여 데이터를 축적
- 모바일 기기 루팅을 통해 인포카 앱 데이터 획득
- 포렌식 도구인 Autopsy를 사용하여 시나리오 타임라인과 비교하여 분석
- 데이터의 명확한 의미 파악
- 사용자의 동선 및 행위를 재구성 가능

❖ 한계점

- 최신 모델인 경우 루팅이 불가능

❖ 향후 연구

- 획득한 데이터를 통해 시나리오 이벤트 기반 추가적인 분석 진행

Q&A