안드로이드 젤리빈 기반 오디오 비디오 내비게이션의 로그 데이터 획득 및 분석

WDSC 2023

정욱재, 정지헌, 강해인, 조성제

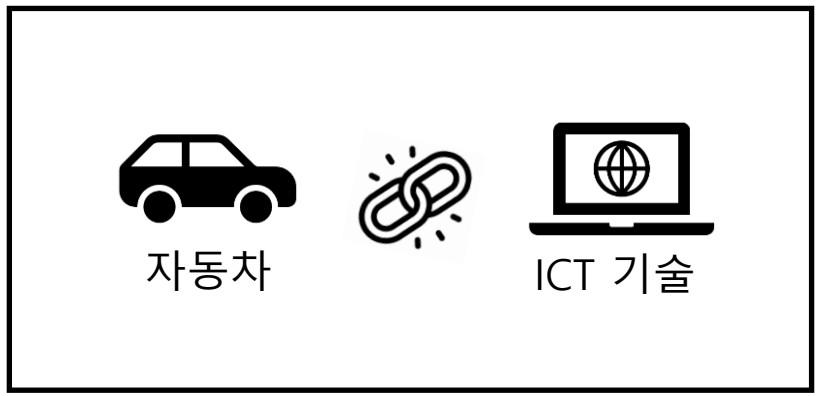
INDEX

01 서론

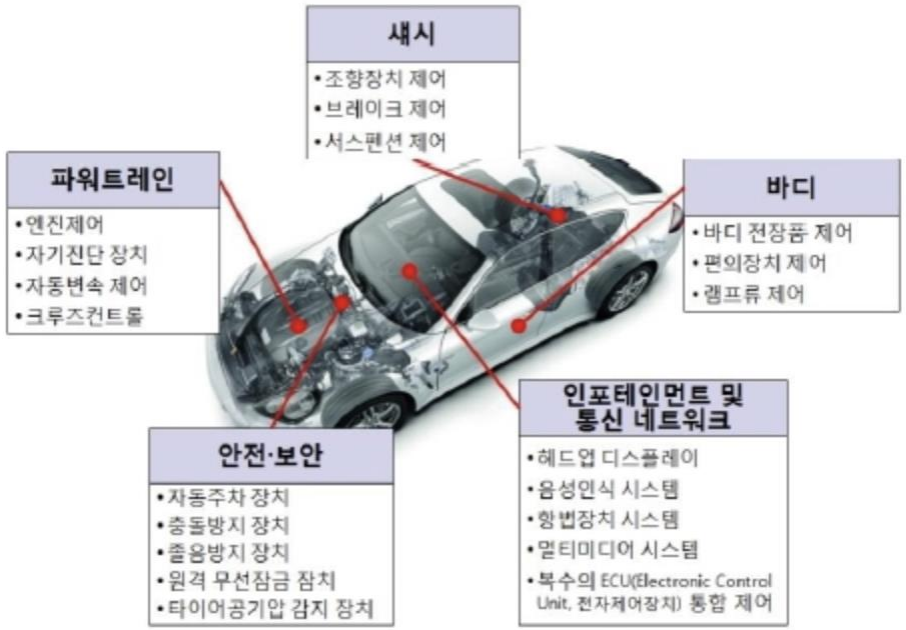
서론

❖ 자동차의 전장화로 자동차와 ICT 기술 융합 가속화

- 자동차에 ICT 기기와 부품의 비중이 증가하고, 자동차 내에서 인터넷을 이용할 수 있어 편의성 증대
- 대표적인 ICT 기기는 AVN(Audio-Video-Navigation)이라고 불리는 인포테인먼트(In–Vehicle Infotainment, IVI) 시스템



기술 융합 가속화

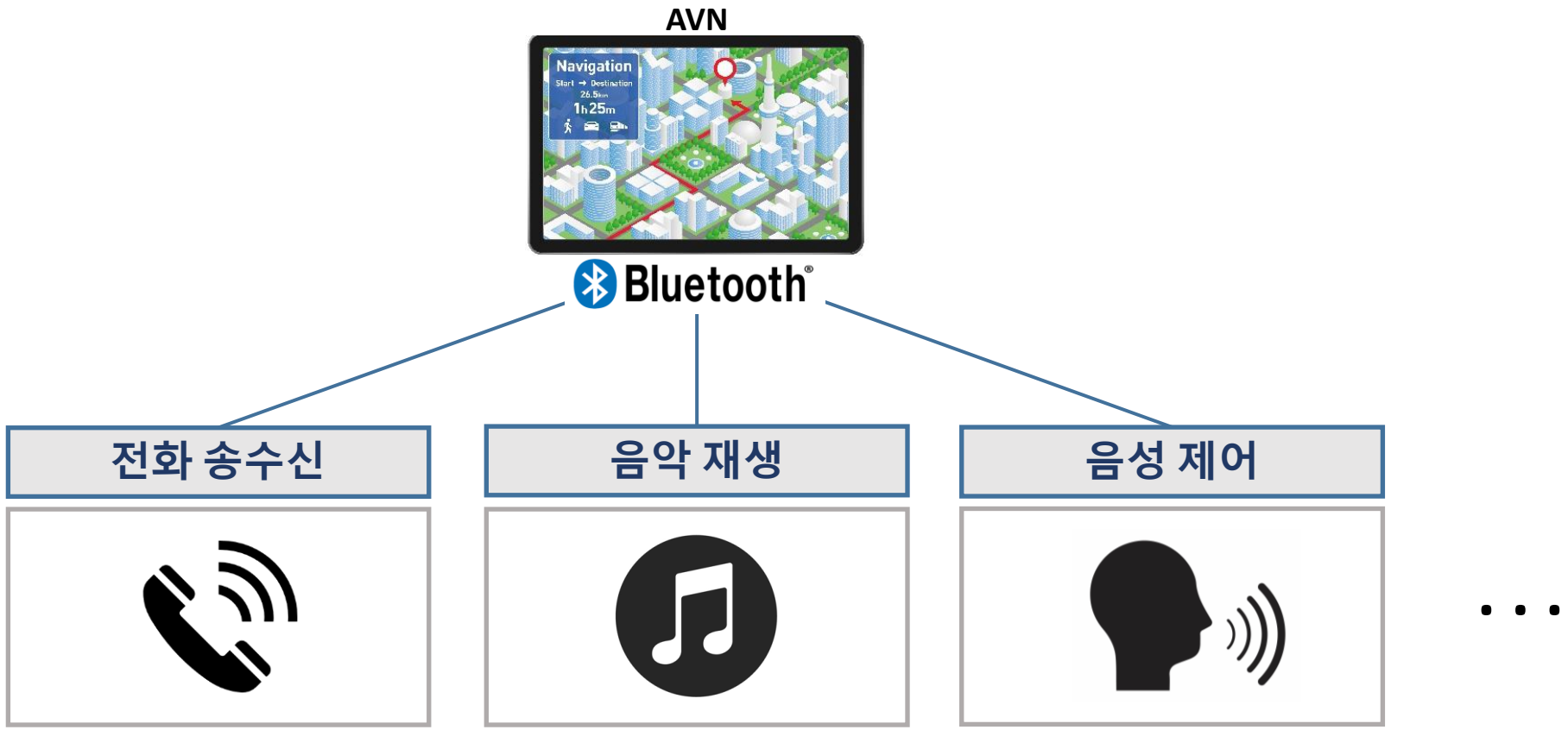


자료 : 한국전자통신연구원

서론

❖ 최신 AVN은 내비게이션 기능 뿐만 아니라 블루투스 기능을 통한 전화 송수신, 음악 재생, 음성 제어 기능 등을 탑재하여 운전자에게 편의성 제공

- 자동차 AVN에 다양한 기능이 추가되면서 AVN 시스템에 최근 목적지와 운행 경로, 운전 중에 수신·발신한 전화 통화, 재생한 음악 목록 등과 관련된 데이터 저장



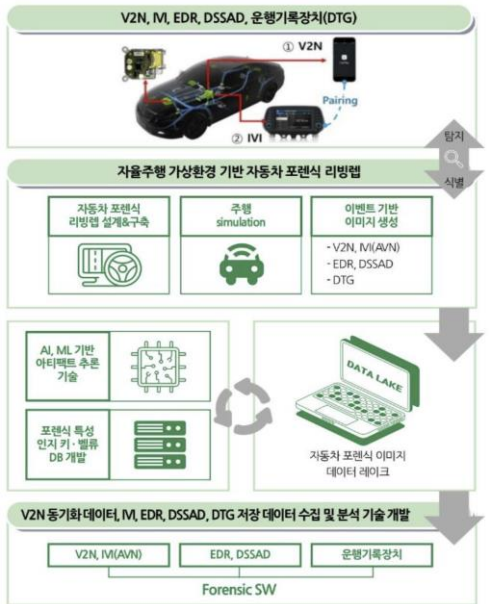
서론

- ❖ AVN으로 운전자의 편리성이 증가했지만, 주행 중 AVN 조작으로 인해 사고가 증가하는 부작용 발생
- ❖ 사고 원인 규명을 위해 AVN과 모바일 기기를 포렌식 분석할 수 있음
  - 모바일 기기의 경우 디스크 암호화 및 샌드박스 고립화로 데이터 획득에 어려움이 있을 수 있음
  - AVN 시스템의 경우 모바일 기기에 비해 포렌식 데이터 획득이 쉬울 수 있음
  - AVN 시스템이 생성하는 로그 데이터의 경우 운전자가 임의로 수정하는 것이 불가능 함
  - 로그 데이터를 획득 및 분석하여 운전자 행위 파악이 가능하면, 자동차 사고와 운전자 행위의 연관성 파악 가능

이투데이 > 사회 > 법조

[진화하는 과학수사]① 휴대폰처럼 자동차도 포렌식 수사한다…대검, 실무 적용

입력 2022-10-19 16:19 | 수정 2022-10-19 16:20



자료 : 자동차 포렌식 기술 구조 (대검찰청)

연구 목표 및 개요

- 기아 Niro EV에 탑재된 안드로이드 젤리빈 기반 AVN을 대상으로 시나리오 기반 실험 진행
- 두 가지 방식을 사용하여 획득한 로그 데이터 분석 진행
- 분석 결과를 토대로 로그 데이터 획득 방식 중 더 효율적인 방식 설명
- 로그 데이터 분석으로 운전자 행위 파악이 가능함을 보임

02 배경지식 및 관련 연구

배경지식

❖ 안드로이드 로깅 시스템

- 애플리케이션 작동 과정에서 발생하는 이벤트와 디바이스 정보 기록
- 애플리케이션 개발 과정에서 오류 수정 작업에 활용되며, 일반적으로 아래의 4개의 메모리(로그) 버퍼에 저장
- 로그는 휘발성 데이터라는 특징이 있으며, 로그 버퍼의 크기는 안드로이드 기기 제조사 및 버전에 따라 다를 수 있지만 기본적으로 256KB 크기를 가짐

메모리 버퍼	설명
main	애플리케이션 이벤트 및 디버깅 메시지
system	시스템에서 생성된 메시지
radio	모바일 기기 신호 및 데이터 통신 메시지
events	시스템 이벤트 관련 메시지

- logcat 명령어를 사용하면 생성된 로그 메시지를 텍스트 형식으로 획득할 수 있음

```
07-09 15:02:36.737 14640 14640 D AbsSettings: getStringInner: from cache AODSettingsDBItem / CLOCK_VERSION = 100000
Timestamp          PID   TID   Level Tag                                  Body
```

관련 연구

❖ Hong, I., Lee, S., "Research on Efficient Live Evidence Analysis System Based on User Activity Using Android Logging System"

- 안드로이드 모바일 기기에서 생생되는 휘발성 데이터와 관련된 연구가 활발하지 않음을 인지
- 안드로이드 모바일 기기의 휘발성 데이터를 획득 및 분석하는 연구 진행
- 사용자 행위를 정의하고 실험을 진행했고, 한 번의 행위에 여러 로그가 생성되는 것을 확인
- 생성된 로그 데이터를 분석하여 사용자 행위를 추적할 수 있음을 보임

❖ Satrya, G. B., Daely, P. T., and Shin, S. Y., "Android forensics analysis: Private chat on social messenger"

- 안드로이드 모바일 기기에서 사용하는 메신저 앱 Telegram, Line, Kakao Talk에서 기능별 대화 시나리오 진행
- 생성되는 아티팩트를 획득하고 분석하여 해당 데이터들이 디지털 증거로 사용될 수 있음을 보임

관련 연구

❖ 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"

- 기아 니로 EV에 탑재된 안드로이드 4.2.2 버전의 AVN 디스크 이미지 파일을 획득하고 분석
- Dirty Cow(CVE-2016-5195) 취약점을 사용해 root 권한 상승 공격을 진행하고, dd 명령어를 사용해 AVN 디스크 이미지 파일 획득

❖ Kang, H., Seong, H., Kim, I., Jeong, W., Cho, S. J., Park, M. K., and Han, S. C., "Android-Based Audio Video Navigation System Forensics: A Case Study"

- dd 명령어를 사용하여 획득한 안드로이드 4.2.2 버전의 AVN 디스크 이미지 파일을 포렌식 분석
- 분석을 통해 이미지 파일 내부에 로그 데이터가 존재함을 확인
- 로그 데이터와 이미지 파일 내부의 블루투스 및 내비게이션 데이터를 통합 분석하여 운전자의 이동 경로 파악

03 안드로이드 기반 자동차 AVN에 대한 디지털 포렌식

디지털 포렌식 절차

❖ 데이터 획득과 데이터 분석 과정으로 구성

- 데이터 획득 방식
  - Micro Read : 전자 현미경으로 플래시 메모리의 게이트를 물리적으로 관찰
  - Chip-off : 기기의 플래시 메모리를 물리적으로 제거하여 데이터 획득
  - Hex Dumping : 기기를 플래셔 박스와 PC에 연결하고 플래셔 박스의 진단 모드를 사용하여 데이터 획득
  - JTAG : PCB 기판의 JTAG 인터페이스에 선을 연결하여 데이터 획득
  - 논리적 추출(logical extraction) : 기기와 컴퓨터를 유무선으로 연결하고 명령어를 사용하여 데이터 획득
  - 수동 추출(manual extraction) : 기기를 직접 조작하여 내부에 저장된 데이터 확인

데이터 획득 방식

자료 : "Guidelines on Mobile Device Forensics", NIST SP

- 본 논문에서는 논리적 추출 방식을 사용하여 로그 데이터 획득

- 획득한 데이터는 메모장과 전문 포렌식 도구인 Autopsy를 사용하여 분석

디지털 포렌식 대상 시스템

❖ 안드로이드 기반 AVN과 안드로이드 모바일 기기를 블루투스로 연동

AVN	
차종	KIA NIRO EV (2018)
제조사	KIA motors
운영체제	Android 4.2.2 (Jelly Bean)
커널 버전	3.1.10-tcc
Mobile device	
기기명	Samsung Galaxy S8
운영체제	Android 9.0

디지털 포렌식 대상 시스템

❖ 로그 데이터 생성

- AVN 내부에 운전자 행위와 관련된 로그 데이터를 생성하기 위해 시나리오 기반 실험 진행
- 주행 중 운전자가 수행할 수 있는 행위를 선별하고 시나리오 구성
- 실험을 진행하면서 시간 정보를 기록하고, 기록한 정보를 토대로 로그 데이터 분석 진행

[주요 이벤트 생성 시나리오]

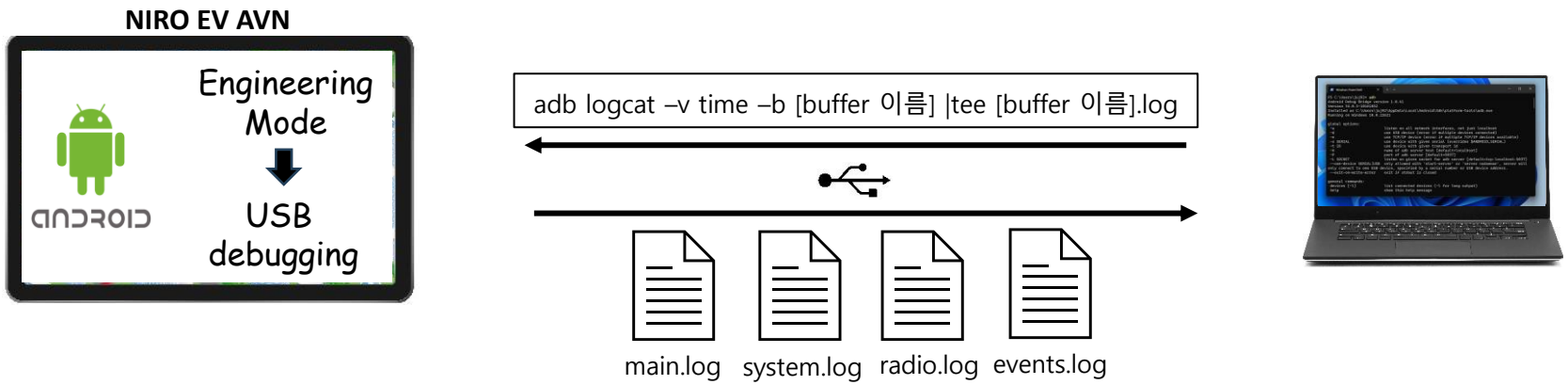
시간	시나리오
23:47	AVN과 모바일 기기 연동
23:48	전화 수신
23:48	음악 재생
23:48	전화 발신
23:49	메시지 회신
23:49	연동 해제

04 안드로이드 AVN의 로그 데이터 획득

logcat 명령어를 사용한 로그 버퍼 데이터 획득

❖ 로그 버퍼 데이터 획득 과정

1. 시나리오 기반 실험 종료 후 AVN 시스템의 "엔지니어링 모드(Engineering Mode)" 진입
2. Android Setting 메뉴에서 "USB 디버깅" 활성화
3. USB 케이블을 사용하여 PC와 AVN 시스템 연결
4. PowerShell에서 logcat 명령어를 사용하여 로그 버퍼에 생성되는 로그 데이터 실시간 획득
   - AVN에 존재하는 main, system, radio, events 버퍼를 대상으로 데이터 획득
   - 로그 데이터는 텍스트 형식으로 획득 가능



dd 명령어를 사용한 디스크 이미지 파일 획득

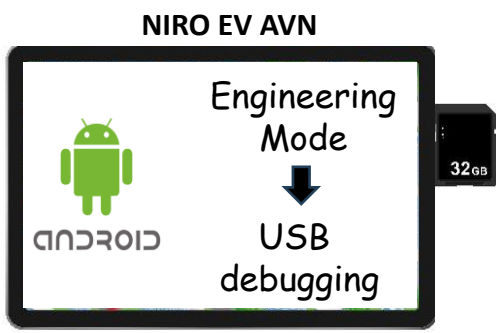
❖ 디스크 이미지 파일 획득 과정

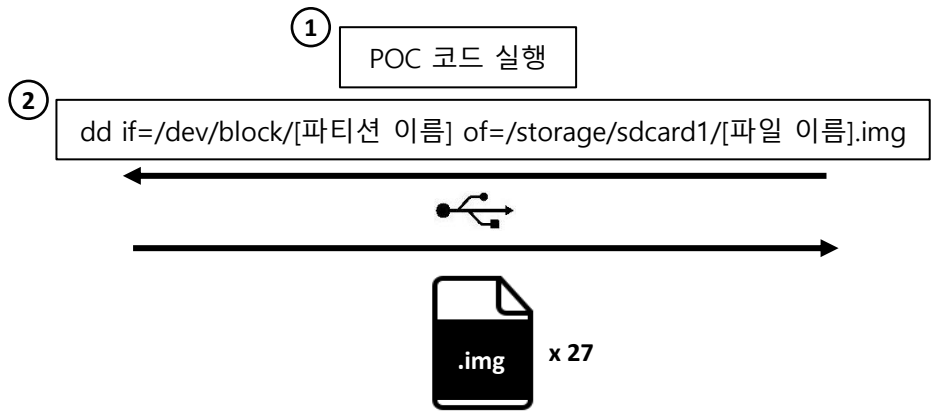
1. "USB 디버깅"이 활성화된 AVN 시스템을 USB 케이블로 PC와 연결
2. PC에 Dirty Cow 취약점 POC 코드 설치
3. POC 코드를 실행하여 AVN 내부에 권한 상승 공격 파일 설치
4. AVN 시스템의 shell에서 생성된 파일을 확인하고 권한 상승 공격 진행
5. dd 명령어를 사용하여 디스크 이미지 파일 획득
   - cat /proc/partitions 명령어로 확인 가능한 파티션을 대상으로 명령어 사용 (mmcblk0 영역)
   - sd 카드에 저장된 이미지 파일 획득

```
shell@android:/data $ cat /proc/partitions
major minor  #blocks  name

179        0    7634944 mmcblk0
179        1      20480 mmcblk0p1
179        2     665600 mmcblk0p2
179        3    1758927 mmcblk0p3
179        4          1 mmcblk0p4
179        5     153600 mmcblk0p5
179        6      20480 mmcblk0p6
179        7       5120 mmcblk0p7
179        8       5120 mmcblk0p8
179        9       1024 mmcblk0p9
179       10       1024 mmcblk0p10
179       11     262144 mmcblk0p11
179       12      20480 mmcblk0p12
179       13     665600 mmcblk0p13
179       14      20480 mmcblk0p14
179       15     102400 mmcblk0p15
259        0     102400 mmcblk0p16
259        1     262144 mmcblk0p17
259        2    2097152 mmcblk0p18
259        3     870400 mmcblk0p19
259        4     153600 mmcblk0p20
259        5     102400 mmcblk0p21
259        6     262144 mmcblk0p22
259        7      81904 mmcblk0p23
179       32       8192 mmcblk0boot1
179       16       8192 mmcblk0boot0
179       48   31276032 mmcblk1
179       49   31271936 mmcblk1p1
253       31     122880 wrs_ss0p0
253       30     139264 wrs_ss0p1
```

AVN 파티션 정보



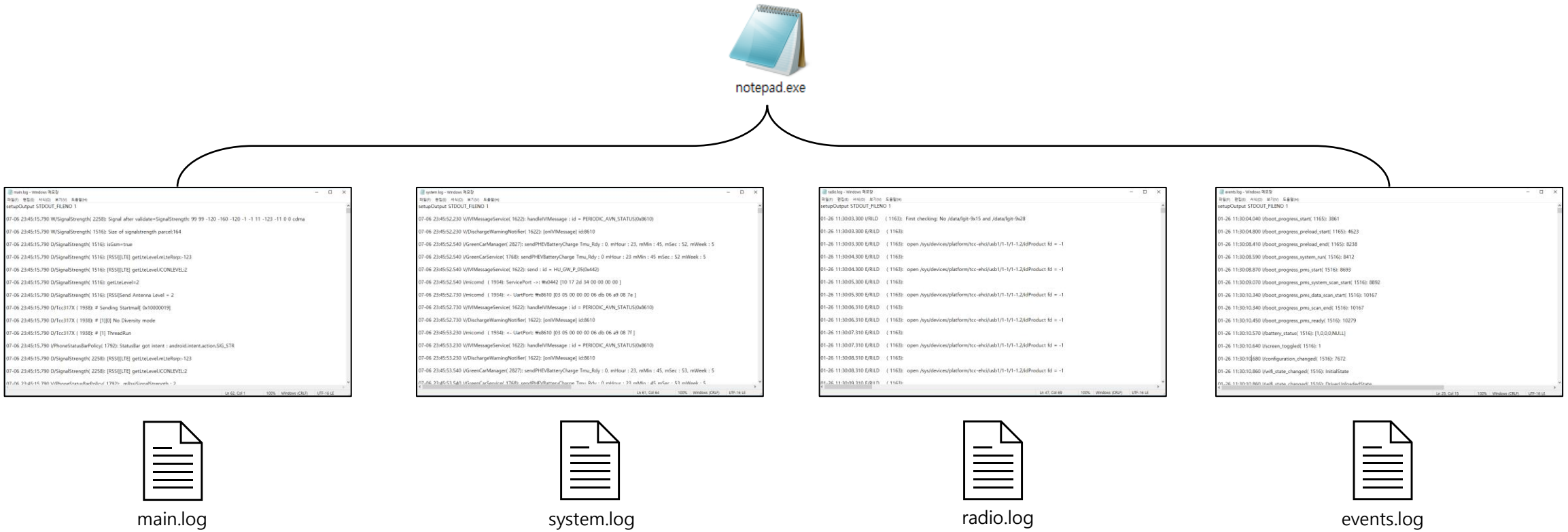


05 안드로이드 AVN의 로그 데이터 분석

로그 버퍼 데이터 분석

❖ 텍스트 형식으로 생성된 로그 파일 분석

- 메모장을 사용하여 생성된 로그 데이터 파일 분석
- 시나리오 실험 중 기록한 시간 정보를 토대로 로그 데이터 분석



로그 버퍼 데이터 분석

❖ 분석 결과

- main, system, events 버퍼에서 운전자 행위와 관련된 로그 데이터 발견
- main 버퍼의 경우 body 부분에 운전자 행위와 관련된 정보가 구체적으로 존재
- system 버퍼에는 main 버퍼 만큼 구체적인 정보가 남지 않지만 body 부분을 확인하여 운전자 행위 추측 가능
- events 버퍼의 경우 body 부분에 운전자 행위와 관련된 구체적인 정보가 기록되지 않아 tag 정보와 통합 분석하여 운전자 행위 파악 가능

[AVN 시스템의 음악 재생 관련 로그 데이터]

버퍼	tag	body	행위
main	BTMedia_BTstreamingMainActivity	bt_PlayBTStream : avrcp_Play =========> normal	음악 재생
	BTMedia_BTStreamControl	sTitle = 스티커 사진, sArtist = 21학번, sAlbum = 스티커 사진	
events	am_resume_activity	[0,1109983784,14,com.lge.ivi.btmedia/.BTstreamingMainActivity]	
main	BTMedia_BTstreamingMainActivity	onPause	재생 중지
events	am_pause_activity	[0,1109983784,com.lge.ivi.btmedia/.BTstreamingMainActivity]	
system	ModeService	onActivitySwitching() appType = MEDIA	화면 전환
	OsdService	[onTopAppTypeChanged] MEDIA -> OTHER	

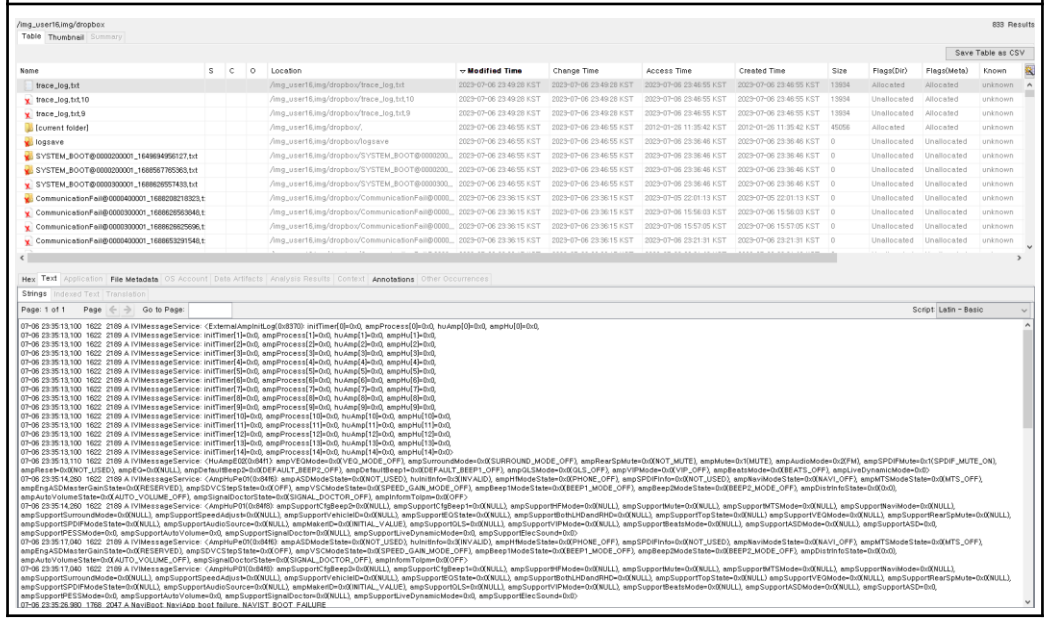
디스크 이미지 파일 내부의 로그 데이터 분석

❖ 디스크 이미지 파일 분석

- 포렌식 도구인 Autopsy를 사용하여 분석 진행
- 파티션 중 ‘mmcblk0p16’와 ‘mmcblk0p21’에서 로그 데이터 발견

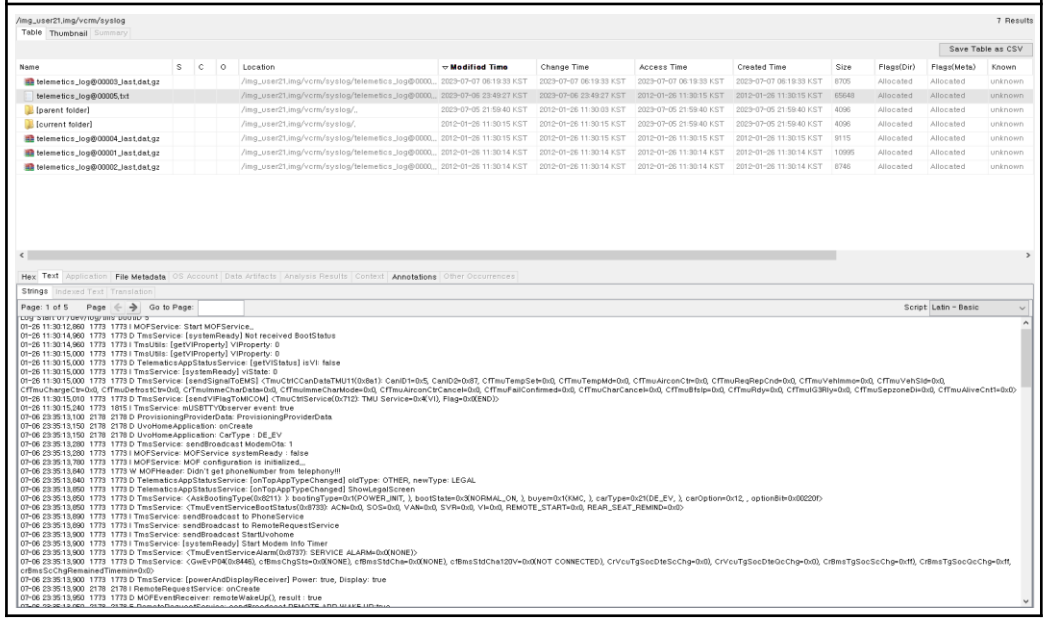
.img

mmcblk0p16 파티션



.img

mmcblk0p21 파티션



디스크 이미지 파일 내부의 로그 데이터 분석

❖ 분석 결과

- mmcblk0p21에 존재하는 로그 데이터는 텔레매틱스 시스템 및 커널과 관련된 로그 데이터
- mmcblk0p16의 'trace_log.txt.* [숫자]' 형태의 파일에 운전자 행위와 관련된 로그 데이터 존재
  - AVN 음향 설정 관련 데이터와 기기 연동 및 해제 정보만 존재하는 것을 확인 (버퍼 정보 확인 불가)
- logcat으로 획득한 로그 버퍼 데이터와 관련된 정보는 존재하지 않음
  - 메모리 버퍼에서 생성되는 로그 데이터는 디스크에 저장되지 않는 것으로 추정됨
  - 디스크 이미지 파일에 존재하는 로그 데이터를 단독으로 분석하는 것은 운전자 행위를 파악하는 것에는 제한이 있음

[디스크 이미지 파일에서 확인한 운전자 행위 로그 데이터]

timestamp	tag	body	행위
07-06 23:47:34.500	BluetoothProfileManager	After HFP Connected, BT Device Name : Galaxy S8	기기 연동
07-06 23:49:28.310		onBluetoothDeviceACLDisconnected, LinkDown Reason : By HeadUnit	연동 해제

06 논의 및 한계점

논의

❖ 기아 NIRO EV (2018)에 탑재되는 AVN 시스템의 로그 데이터를 획득하고 분석

- logcat 명령어를 사용하여 main, system, radio, events 버퍼를 대상으로 로그 데이터를 획득
- main, system, events 버퍼에 운전자 행위와 관련된 로그 데이터가 존재하며, main 버퍼에 운전자 행위와 관련된 로그가 구체적으로 생성됨을 확인
- dd 명령어를 사용하여 획득한 디스크 이미지 파일은 2개의 파티션에서 로그 데이터를 확인했으며, mmcblk0p16 파티션에서 AVN과 모바일 기기 간의 연동 및 해제 정보만을 발견

❖ logcat 명령어를 사용하여 로그 데이터를 획득하는 방식이 운전자 행위를 파악하는데 더 효율적임을 알 수 있음

[운전자 행위 데이터 확인 가능 여부]

행위	로그 버퍼	디스크 이미지
기기 연동	o	o
전화 수신	o	x
음악 재생	o	x
전화 발신	o	x
메시지 회신	o	x
연동 해제	o	o

한계점

- ❖ 로그는 휘발성 데이터라는 특징으로 인해 기기의 전원이 꺼지면 운전자 행위와 관련된 로그 데이터를 획득할 수 없음
- ❖ 로그 버퍼 크기를 초과하는 로그가 생성되면 가장 오래된 로그 데이터부터 덮어씌워지는 문제가 있음
- ❖ 본 논문에서 사용한 로그 데이터 획득 방식은 엔지니어링 모드에서 접근할 수 있고, USB 디버깅 활성화가 가능한 기기에서만 사용할 수 있음

엔지니어링 모드 진입

USB 디버깅 활성화

07 결론 및 향후 연구

결론 및 향후 연구

❖ 결론

- logcat으로 획득한 로그 데이터에 시나리오와 관련된 모든 정보가 포함되어 있었고, 운전자 행위 파악이 가능함
- dd를 통해 획득한 디스크 이미지 파일 내부의 로그 데이터에는 기기 연동과 연동 해제와 관련된 정보만이 존재함
- logcat 명령어를 사용하여 로그 데이터를 획득하는 방식을 사용하면 시나리오 기반의 운전자 행위를 파악할 수 있고, 디스크 이미지 파일을 획득하는 방식보다 더 효율적임
- AVN 로그 데이터를 획득할 수 있다면 운전자 행위를 파악하여 자동차 사고와의 연관성 조사에 도움이 될 수 있음

❖ 향후 연구

- 획득한 로그 데이터 검증을 위해 실험에 사용한 모바일 기기의 로그 데이터와 AVN 로그 데이터 비교 분석
- 실험을 통해 획득한 로그 데이터를 활용하여 효과적으로 로그 데이터를 분석할 수 있는 환경 구축

Q&A