# 안드로이드 젤리빈 기반 오디오 비디오 내비게이션의 로그 데이터 획득 및 분석

정욱재[O1], 정지헌[1], 강해인[2], 조성제[1]
단국대학교 소프트웨어학과[1], 단국대학교 인공지능융합학과[2]
{wookjae, wlgjsjames, hikang, sjcho}@dankook.ac.kr

# Acquisition and Analysis of Log Data in an Android Jelly Bean-based Audio Video Navigation

Wookjae Jeong[O1], Jiheun Jung[1], Haein Kang[2], Seong-je Cho[1]
Department of Software Science, Dankook University[1]
Department of AI-based Convergence, Dankook University[2]

**요 약**

자동차의 전장화로 자동차와 ICT 기술 융합이 가속화되고 있다. 예로, 최신 자동차에 AVN(Audio-Video-Navigation)이라고 불리는 인포테인먼트(In-Vehicle Infotainment, IVI) 시스템을 탑재하여, 내비게이션 기능뿐만 아니라 블루투스를 통한 전화 통화, 음악 재생, 음성 제어 기능 등을 지원한다. 따라서, AVN 시스템에는 최근 목적지와 운행 경로, 운전자가 사용한 기능 및 운전자의 행위 등을 포함한 다양한 정보가 저장되고 있다. 이들 정보 중에서, 시스템적으로 생성·유지되는 로그 데이터는 교통사고 또는 범죄 발생 시 운전자 행위와 사고·범죄 간의 연관성 조사에 활용될 수 있다. 본 논문은, 기아차에 탑재되는 안드로이드 젤리빈 기반 AVN을 대상으로 시나리오 기반 실험을 진행한 후, AVN 시스템에 생성된 로그 데이터를 획득하는 두 가지 방식을 제시한다. 다음으로, 획득한 로그 데이터를 분석하여 획득 방식에 따른 차이점을 설명하고, 로그 데이터에서 운전자 행위 식별이 가능함을 보인다.

## 1. 서 론

자동차의 전장화로 자동차와 ICT 기술 융합이 가속화되면서 자동차에 ICT 기기와 부품의 비중이 증가하고, 자동차 내에서 인터넷을 이용할 수 있어 편의성도 증대되고 있다. 예로, 운전자에게 편리한 기능을 제공해 주는 대표적인 ICT 기기가 AVN(Audio-Video-Navigation)이라고 불리는 인포테인먼트(In-Vehicle Infotainment, IVI) 시스템이다. 최신 AVN은 내비게이션 기능뿐만 아니라 블루투스 통신을 통한 전화 송수신, 음악 재생, 음성 제어 기능 등을 탑재하여 운전자에게 편의성을 제공한다. 특히 블루투스 통신을 통한 모바일 기기와의 연결성 증대는 운전 중 모바일 기기의 기능을 편하게 사용할 수 있게 해 준다 [1]. 자동차 AVN이 다양한 기능을 제공함에 따라, AVN 시스템에는 최근 목적지와 운행 경로, 운전 중에 수신·발신한 통화 목록, 재생한 음악 목록 등과 같은 데이터를 저장하고 있다 [2].

AVN으로 운전자의 편리성이 증가했지만, 주행 중 AVN 조작으로 인한 자동차 사고가 증가하는 부작용이 발생하고 있다 [3]. 만약 운전자가 AVN을 사용하는 중에 자동차 사고가 발생했다고 의심되는 경우라면, 해당 사고의 원인 규명을 위해 AVN과 운전자의 모바일 기기를 포렌식 분석할 수 있다 [4]. 이때, 모바일 기기의 경우 디스크 암호화(disk encryption) 또는 앱 간의 샌드박스 고립화(sandbox isolation)로 포렌식 데이터 획득이 어려울 수 있다 [5]. 이에 반해 자동차 AVN 시스템의 경우, 모바일 기기에 비해 포렌식 데이터 획득이 쉬울 수 있다. 게다가 AVN 시스템이 생성하는 로그 데이터는 운전자가 임의로 수정하는 것이 불가능하다 [6]. 따라서, AVN 시스템에 저장된 로그 데이터를 획득 및 분석하여 운전자 행위 파악이 가능하다면, 자동차 사고와 운전자 행위의 연관성 파악에 도움이 될 것이다.

본 논문에서는, 기아 NIRO EV에 탑재된 안드로이드 젤리빈(Jelly Bean) 기반 AVN을 대상으로 시나리오 기반의 실험을 진행하고, 시나리오와 관련된 로그 데이터를 두 가지 방식으로 획득한 후 분석한다. 이후 분석 결과를 토대로 로그 데이터를 획득하는 두 가지 방식 중 더 효율적인 방식을 설명하고, 로그 데이터 분석을 통해 운전자 행위 파악이 가능함을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 안드로이드 로깅 시스템을 설명하고, 안드로이드 기기 포렌식과 관련된 기존 연구를 기술한다. 3장에서는 포렌식 절차와 포렌식 대상 시스템을 기술하고, 4장에서는 시나리오 기반 실험을 통해 생성한 로그 데이터를 획득하는 방식을 기술한다. 5장에서는 획득한 로그 데이터를 분석하고, 6장에서는 분석한 로그 데이터를 정리하고 본 논문에서 발생하는 한계점을 기술한다. 마지막으로 7장에서는 결론과 향후 연구를 기술한다.

## 2. 배경지식 및 관련 연구

### 2.1 배경지식

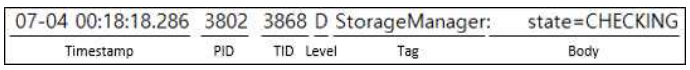
안드로이드 로깅 시스템은 애플리케이션 작동 과정에서 발생하는 이벤트와 디바이스 정보를 기록하는 역할을 한

다. 애플리케이션 개발 과정에서 발생하는 오류를 수정하는 작업에 활용되며, 일반적으로 main, system, radio, events의 4개의 메모리 버퍼(로그 버퍼)에 저장된다. 로그는 휘발성 데이터라는 특징이 있으며, 로그 버퍼의 크기는 안드로이드 기기 제조사 및 버전에 따라 다를 수 있지만 기본적으로 256KB로 설정되어 있다. 각 버퍼에 저장되는 데이터는 표 1과 같다 [7, 8].

**[표 1]. 로그 데이터를 저장하는 4개의 메모리 버퍼**

| 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 있으며 그림 1과 같은 구조를 가지는 것을 확인할 수 있다. 시간 정보를 나타내는 Timestamp, PID, TID, 로그 Level, Tag, 마지막으로 시스템이 수행한 행위를 의미하는 Body로 구성된다 [9].




**[그림 1]. 안드로이드 로그 메시지 및 구조**

### 2.2 관련 연구

Hong 등[10]은 안드로이드 모바일 기기에서 생성되는 휘발성 데이터와 관련된 연구가 활발하지 않음을 인지하고 휘발성 데이터를 획득 및 분석하는 방법을 연구했다. 사용자 행위를 정의하고 실험을 진행했으며, 한 번의 행위에 여러 로그가 생성되는 것을 확인했다. 이후 생성된 로그 데이터를 분석하여 사용자 행위를 추적할 수 있음을 보였다.

Satrya 등[11]은 안드로이드 모바일 기기에서 사용하는 메신저 앱 Telegram, Line, Kakao Talk에서 기능별 대화 시나리오를 진행했다. 이후 생성되는 아티팩트를 획득하고 분석하여 해당 데이터들이 디지털 증거로 사용될 수 있음을 보였다.

Seong 등[12]은 기아 니로 EV에 탑재된 안드로이드 4.2.2 버전의 AVN 디스크 이미지 파일을 획득하고 이를 분석했다. Dirty Cow(CVE-2016-5195) 취약점[13]을 사용해 root 권한 상승 공격을 진행하고, dd 명령어를 사용해 AVN 디스크 이미지 파일을 획득했다.

Kang 등[14]은 dd 명령어를 사용하여 획득한 안드로이드 4.2.2 버전의 AVN 디스크 이미지 파일을 포렌식 분석했다. 분석을 통해 이미지 파일 내부에 로그 데이터가 존재함을 확인했다. 이후, 확인한 로그 데이터와 이미지 파일 내부의 블루투스 및 내비게이션 데이터를 통합 분석하여 운전자의 이동 경로를 파악했다.

## 3. 안드로이드 기반 자동차 AVN에 대한 디지털 포렌식

### 3.1 디지털 포렌식 절차

본 논문의 디지털 포렌식 절차는 데이터 획득과 데이터 분석 과정으로 구성된다. 데이터를 획득하는 방법은 전자 현미경을 통해 플래시 메모리의 게이트를 물리적으로 관찰하는 Micro Read, 플래시 메모리를 물리적으로 제거하여 데이터를 획득하는 Chip-off, 기기에 플래셔 박스와 컴퓨터를 연결하고 플래셔 박스를 사용하여 진단 모드로 전환한 후, 데이터를 획득하는 Hex Dumping, PCB 기판의 인터페이스에 선을 연결하여 데이터를 획득하는 JTAG(Joint Test Action Group), 기기와 컴퓨터를 유·무선으로 연결하고 컴퓨터 명령어를 사용하여 데이터를 획득하는 논리적 추출(logical extraction), 기기를 직접 조작하여 내부에 저장된 데이터를 확인하는 수동 추출(manual extraction) 방식으로 구분할 수 있다 [15].

우리는 로그 버퍼에 존재하는 로그 데이터를 획득하는 과정과 디스크 내부에 존재하는 로그 데이터를 획득하기 위해서 디스크 이미지 파일을 획득하는 과정을 진행했다. 이는 기기와 컴퓨터를 유선으로 연결하고, 컴퓨터 명령어를 통해 데이터를 획득하는 논리적 추출 방식이다.

데이터 획득이 완료되면 데이터를 분석하는 과정을 진행한다. 로그 버퍼에서 획득한 로그 데이터의 경우 텍스트 형태로 존재하기 때문에, 메모장에서 로그 데이터를 직접 분석했다. 획득한 디스크 이미지 파일의 경우 직접 분석하는 것이 어렵기 때문에, 전문 포렌식 도구인 Autopsy를 사용하여 분석했다.

### 3.2 디지털 포렌식 대상 시스템

본 논문의 디지털 포렌식 대상 시스템은 국내 차량에 탑재되는 안드로이드 젤리빈 기반 AVN이다. 실험을 위해서 AVN 시스템과 국내 제조사의 안드로이드 모바일 기기를 블루투스 기능으로 연동했다. 본 논문에서 사용한 AVN 시스템과 모바일 기기의 사양은 표 2와 같다.

**[표 2]. 대상 AVN 시스템 및 모바일 기기**

| **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 |

AVN 내부에 운전자 행위와 관련된 로그 데이터를 생성하기 위해서 시나리오 기반의 실험을 진행했다. 주행 중 운전자가 수행할 수 있는 행위를 선별하고 표 3과 같은 시나리오를 작성했다. 실험을 진행하면서 시간 정보를 기록하고 이를 토대로 로그 데이터 분석을 진행했다.

[표 3]. 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 |

## 4. 안드로이드 AVN의 로그 데이터 획득

안드로이드 기기가 생성하는 로그 데이터는 메인 메모리의 로그 버퍼에도 존재하지만, 디스크 내부에도 존재한다 [14]. 따라서 로그 버퍼에 존재하는 로그 데이터를 획득하는 logcat 명령어와 디스크 전체 데이터를 획득하는 dd 명령어를 사용하여 로그 데이터를 획득했다.

표 2의 AVN을 대상으로 데이터를 획득하기 위해서는 AVN 시스템의 엔지니어링 모드(engineering mode)에 접근하여 USB 디버깅 설정을 활성화해야 한다 [12]. USB 디버깅을 활성화하면 ADB(Android Debug Bridge)[16]를 사용해 logcat 명령어와 dd 명령어 사용이 가능하다.

### 4.1 logcat 명령어를 사용한 로그 버퍼 데이터 획득

자동차 AVN 시스템에 존재하는 로그 버퍼의 로그 데이터를 획득하기 위해서 USB 디버깅이 활성화된 AVN을 PC와 연결하고 logcat 명령어를 사용했다. 로그 데이터 획득은 AVN에 존재하는 4개의 버퍼를 대상으로 진행했으며, 시간 정보가 획득되지 않는 것을 발견하여 '-v time' 조건을 통해 시간 정보를 포함한 로그 데이터를 획득했다. 또한 아래의 명령어와 같이 tee 명령어[17]를 사용하여 로그 버퍼에 존재하는 로그 데이터를 실시간으로 획득했다.

```
> adb logcat -v time -b [buffer 이름] |tee [buffer 이름].log
```

### 4.2 dd 명령어를 사용한 디스크 이미지 파일 획득

자동차 AVN 시스템의 디스크 내부에 존재하는 로그 데이터를 획득하기 위해서 디스크 이미지 파일을 획득했다. 이 과정은 루트 권한이 필요하며, 우리는 리눅스 커널 취약점인 Dirty Cow(CVE-2016-5195)[13]를 이용한 루트 권한 상승 공격을 진행했다. 먼저, USB 디버깅이 활성화된 AVN과 PC를 USB 케이블로 연결하고, PoC(Proof of Concept) 코드[18]를 사용하여 루트 권한 상승 공격에 사용되는 실행 파일을 AVN 내부에 생성한다. 이후 'adb shell' 명령어를 통해 AVN의 shell에 접근하고, 생성된 'run-as' 실행 파일을 사용해 루트 권한 상승 공격을 진행한다. 루트 권한을 확보하면 dd 명령어를 사용하여 디스크 이미지 파일을 획득할 수 있다 [12]. 본 논문에서는 그림 2에서 확인할 수 있는 모든 디스크 파티션을 대상으로 디스크 이미지 파일 획득을 진행했다.

```
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
```

[그림 2]. AVN 파티션 정보

## 5. 안드로이드 AVN의 로그 데이터 분석

본 절에서는 4절에서 획득한 로그 데이터를 분석한다. 획득한 로그 데이터는 실험 중 기록한 시간 정보를 기반으로 분석했으며, 텍스트 형식의 로그 데이터는 메모장을 사용해 분석하고, 디스크 이미지 파일은 Autopsy를 사용해 분석했다.

### 5.1 로그 버퍼 데이터 분석

logcat으로 획득한 로그 데이터를 분석한 결과, 안드로이드 모바일 기기와 같이 AVN에도 main, system, radio. events 버퍼가 존재함을 확인했다. 이중 radio 버퍼의 로그 데이터에는 AVN과 모바일 기기 사이의 SIM 카드 정보 교환과 관련된 로그만이 존재한다. 운전자 행위와 관련된 정보는 main, system, events 버퍼에 존재한다.

표 4는 시나리오와 관련된 로그 데이터 중 음악 재생과 관련된 로그 데이터를 정리한 표이다. 먼저 main 버퍼에서 발견한 로그 데이터는 body 부분에 운전자 행위와 관련된 구체적인 정보가 존재한다. body 부분의 'avrcp_Play'을 통해 음악 재생을 시작했음을 알 수 있고, 재생한 음악 이름과 아티스트 이름도 확인할 수 있다. 재생 중지의 경우는 'onPause'를 통해 쉽게 확인할 수 있다.

system 버퍼의 경우 main 버퍼의 로그 데이터만큼 구체적인 정보를 가지고 있지 않다. 하지만 body 부분 확인을 통해 운전자 행위 추측이 가능하다. body 부분의 'onActivitySwitching() appType = MEDIA'을 통해 음악 재생 화면으로 이동했음을 알 수 있다. 또한 '[onTopAppTypeChanged] MEDIA -> OTHER'를 통해 음악 재생 화면에서 다른 화면으로 이동했음을 알 수 있다.

마지막으로 events 버퍼의 경우 로그 데이터의 body 부분만을 확인해서는 운전자의 행위 파악이 어렵다. 이는 tag 정보를 추가로 확인하여 해결할 수 있다. body 부분의 'BTstreamingMainActivity' 클래스와 tag 부분의 'am_resume_activity'와 'am_pause_activity'를 통해 음악 재생 및 중지 여부를 확인할 수 있다.

[표 4]. AVN 시스템의 음악 재생 관련 로그 데이터

| 버퍼 | tag | body | 행위 |
|---|---|---|---|
| main | BTMedia_BTstreaming MainActivity | bt_PlayBTStream : avrcp_Play ========> normal | 음악 재생 |
| | BTMedia_BTStream Control | sTitle = 스티커 사진, sArtist = 21학번, sAlbum = 스티커 사진 | |
| events | am_resume_activity | [0,1109983784,14,com.lge.ivi.btmedia/.BTstreamingMainActivity] | |
| main | BTMedia_BTstreaming MainActivity | 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 | |

[표 5]. 디스크 이미지 파일에서 확인한 운전자 행위 로그 데이터

| tag | body | 행위 |
|---|---|---|
| BluetoothProfileManager | After HFP Connected, BT Device Name : Galaxy S8 | 기기 연동 |
| | onBluetoothDeviceACLDisconnected, LinkDown Reason : By HeadUnit | 연동 해제 |

### 5.2 디스크 이미지 파일 내부의 로그 데이터 분석

획득한 디스크 이미지 파일을 분석한 결과 그림 2의 디스크 파티션 중 'mmcblk0p16'와 'mmcblk0p21' 파티션에서 로그 데이터를 발견할 수 있었다. mmcblk0p21 파티션에는 차량에 탑재된 텔레매틱스 시스템과 관련된 로그 데이터와 커널 로그 데이터가 존재한다. 시나리오 기반의 운전자 행위와 관련된 로그 데이터는 mmcblk0p16 파티션의 'trace_log.txt.*[숫자]' 형태의 파일에 존재한다. 해당 파일에는 AVN 음향 설정과 관련된 로그 데이터와 시나리오 행위와 관련된 로그 데이터가 존재한다. 그러나 시나리오 행위와 관련된 로그 데이터에서는 표 5와 같이 기기 연동 및 해제와 관련된 정보와 실험에서 사용한 모바일 기기의 이름만을 확인할 수 있었다. 또한, logcat을 통해 획득한 로그 데이터와는 다르게 버퍼 정보가 존재하지 않았다.

모든 디스크 파티션을 분석했지만, logcat으로 확인할 수 있는 버퍼들의 데이터는 발견할 수 없었다. 이는 logcat으로 획득할 수 있는 로그 버퍼 데이터가 디스크 내부에 저장되지 않음을 의미한다. 그리고 디스크 내부에 존재하는 로그 데이터만을 단독으로 분석하는 경우 운전자 행위를 파악하는 것에 제한이 있다는 것을 보여준다.

## 6. 논의 및 한계점

본 논문에서는 기아 NIRO EV (2018) AVN 시스템의 로그 데이터를 두 가지 방식을 사용하여 획득하고 분석을 진행했다. 첫 번째로, logcat 명령어를 사용해 main, system, radio, events 버퍼를 대상으로 로그 데이터를 획득했으며, 분석을 통해 main, system, events 버퍼에서 운전자 행위와 관련된 로그 데이터를 확인할 수 있었다. 특히 main 버퍼에서 운전자 행위와 관련된 로그 데이터가 구체적으로 생성됨을 알 수 있었다.

두 번째로, dd 명령어를 사용해 디스크 이미지 파일을 획득하고, 내부에 존재하는 로그 데이터를 분석했다. 디스크 이미지 파일의 경우 2개의 파티션에서 로그 데이터를 확인할 수 있었으며, 그중 mmcblk0p16 파티션에서 AVN과 모바일 기기 간의 연동 및 해제 정보만을 확인할 수 있었다. 로그 데이터 획득 방식에 따라 확인할 수 있는 운전자 행위 관련 로그 데이터는 표 6과 같이 정리할 수 있다. 이를 통해 logcat 명령어를 사용하여 로그 데이터를 획득하는 방식이 운전자 행위를 파악하는데 더 효율적임을 알 수 있다.

본 논문에서는 로그 데이터를 획득했지만, 안드로이드 AVN의 로그 데이터 획득 과정에는 한계점이 존재한다. 먼저, 분석 대상 시스템의 로그 데이터는 휘발성 데이터라는 특징으로 인해 전원이 꺼진 AVN의 경우 운전자 행위와 관련된 로그 데이터를 획득할 수 없다. 또한, 로그 버퍼 크기를 초과하는 로그 데이터가 생성되면 가장 오래된 데이터부터 덮어씌워지는 문제가 있다. 마지막으로 본 논문에서 사용한 로그 데이터 획득 방식은 엔지니어링 모드에 접근할 수 있고, USB 디버깅 활성화가 가능한 기기에서만 사용할 수 있다.

[표 6]. 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 |

## 7. 결론 및 향후 연구

본 논문에서는 기아 NIRO EV 차량에 장착된 안드로이드 젤리빈 기반의 AVN 시스템을 대상으로, 로그 버퍼에

생성되는 로그 데이터와 디스크 내부에 저장된 로그 데이터를 분석하여 시나리오 기반의 운전자 행위 파악 가능 여부를 확인했다. 분석 결과, logcat으로 획득한 로그 데이터에는 시나리오와 관련된 모든 정보가 포함되어 있었으며, 운전자 행위를 파악할 수 있었다. 하지만, dd를 통해 획득한 디스크 이미지 파일 내부의 로그 데이터에서는 기기 연동과 연동 해제와 관련된 정보만을 발견할 수 있었다. 이를 통해 logcat 명령어를 사용하여 로그 데이터를 획득하는 방식이 시나리오 기반의 운전자 행위를 파악할 수 있음을 보였고, 디스크 이미지 파일을 획득하는 방식보다 더 효율적임을 보였다. 또한, AVN 로그 데이터를 획득한다면 운전자 행위 파악이 가능해 운전자 행위와 자동차 사고의 연관성 조사에 도움이 될 수 있음을 보였다.

향후, 본 논문에서 획득한 로그 데이터를 검증하기 위해 모바일 기기의 로그 데이터와 AVN의 로그 데이터를 비교 분석할 예정이다. 또한, 실험 과정을 통해 획득한 로그 데이터를 활용하여 효과적으로 AVN 로그 데이터를 분석할 수 있는 환경을 구축하기 위한 연구를 진행할 예정이다.

## ACKNOWLEDGEMENT

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 실험 시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발).

## 참고 문헌

[1] [車전장 빅뱅]① 자동차와 ICT의 '만남과 대결'…지각변동 진원지 전장기술, ChosunBiz, 2017.01.04.
[2] Le-Khac, N. -A., Jacobs, D., Nijhoff, J., Bertens, K., and Choo, K. -K. R., "Smart vehicle forensics: Challenges and case study", Future Generation Computer Systems, Vol.109, pp. 500 - 510, Aug. 2020.
[3] 주행중 네비게이션 조작 "사고위험 아찔", 전북연합신문, 2015.04.13.
[4] [진화하는 과학수사]① 휴대폰처럼 자동차도 포렌식 수사한다…대검, 실무 적용, 이투데이, 2022.10.19.
[5] Android security features, [Online]. Available: https://source.android.com/docs/security/features
[6] Chuvakin, A. A., Schmidt, K. J., and Phillips, C., "Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management", [Online]. Available: https://usermanual.wiki/Document/Logging20and20Log20Management20The20Authoritative20Guide20to20Undeanagement2020Anton20Chuvakin202620Kevin20Schmidt202620Chris20P.1447316472/view
[7] Logcat command-line tool, [Online]. Available: https://developer.android.com/studio/command-line/logcat
[8] Levin, J., "Android Internals: a Confectioner's Cookbook: Volume 1: the Power User's View", [Online]. Available: https://wikileaks.org/ciav7p1/cms/files/AIvI-M-RL1.pdf
[9] View logs with Logcat, [Online]. Available: https://developer.android.com/studio/debug/logcat
[10] Hong, I., Lee, S., "Research on Efficient Live Evidence Analysis System Based on User Activity Using Android Logging System", Korea Institute Of Information Security And Cryptology, Vol. 22, No. 1, pp. 67-80, Feb. 2012.
[11] Satrya, G. B., Daely, P. T., and Shin, S. Y., "Android forensics analysis: Private chat on social messenger", 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), July 2016.
[12] 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", The 7th International conference on Next Generation Computing 2021 (ICNGC 2021), Nov. 2021.
[13] CVE-2016-5195, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-5195
[14] 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", Applied Sciences, 13(10), 6176, May 2023.
[15] Ayers, R., Brothers, S., and Jansen, W., "Guidelines on Mobile Device Forensics", Special Publication (NIST SP) 800-101 Rev 1, 2014.
[16] ADB, [Online]. Available: https://developer.android.com/studio/command-line/adb
[17] Microsoft.PowerShell.Utility/Tee-Object, [Online]. Available: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/tee-object?view=powershell-7.3
[18] Kernel_exploitation/CVE-2016-5195, [Online]. Available: https://github.com/timwr/CVE-2016-5195/tree/47461529aa629433fea956b44dab487d4486b629