Transactions of KSAE, Vol. 29, No. 9, pp.855-862 (September, 2021)

pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2021.29.9.855

자동차용 AVN 시스템 디지털 포렌식 분석 사례 및 활용 방안

이 정 환[1)] · 박 현 찬[2)] · 이 지 우[1)] · 전 옥 엽[*1)]

국립과학수사연구원 디지털과[1)] · 전북대학교 컴퓨터공학부[2)]

A Case Study on Using Car AVN System

Jung-Hwan Lee[1)] · Hyunchan Park[2)] · Ji-Woo Lee[1)] · Oc-Yeub Jeon[*1)]

[1)]*Department of Digital Analysis, National Forensic Service, 10 Ipchoon-ro, Wonju-si, Gangwon 26460, Korea*
[2)]*Division of Computer Science and Engineering, Jeonbuk National University, Jeonbuk 54896, Korea*
(Received 30 March 2021 / Revised 24 May 2021 / Accepted 27 May 2021)

Abstract : Since the forensic approach to digital devices began, evidence subject to digital forensics has been steadily increasing. The reason is that general devices are equipped with storage media on their operating systems, and they are becoming the subject of digital forensics. In particular, electronic and autonomous driving performance is rapidly growing in the automotive field. Since these functions are installed, various user convenience functions have been provided. In the automotive field, various parts are becoming electronic; however, the audio, video, and navigation(AVN) system that directly connects with users to exchange data is the most important in the digital forensic field. In this paper, we introduce some examples of data acquisition and analysis of the damaged vehicle AVN system.

Key words : Vehicle forensic(자동차 법과학), AVN System(AVN 시스템), Smart car(지능형 자동차), Built in dash camera(내장 블랙박스), Embedded memory(내장 메모리), Signature carving(시그니쳐 기반 카빙)

1. 서 론

기존 자동차를 대상으로 한 법과학적인 접근은 자동차를 식별할 수 있는 요소(페인트 성분, 타이어 패턴, 손상된 흔적 비교)와 운전자의 신원을 식별할 수 있는 요소(자동차 내부에 남겨져 있는 지문 및 섬유, 운전자 DNA)가 분석 대상[1)]이었다. 하지만, 자동차에 편의성, 안전성을 높이기 위한 전자기기가 장착되기 시작하면서 자동차를 대상으로 한 전자법의학(디지털 포렌식) 기술이 필요하기 시작했다. 우선, 디지털 포렌식을 위해서는 저장매체가 장착된 전자 기기 혹은 저장 매체 자체가 존재하여야 하며, 식별-고립-획득-실험-분석의 순서를 거쳐 범죄 사실을 입증할 수 있는 데이터를 복원 및 분석 하는 과정[2)]이 필요하다. 하지만 최근 들어 자동차에 장착된 전자기기들의 종류 및 역할이 다양해지면서 디지털 포렌식 대상이 되는 장치들이 매년 새로 생겨나고 있지만, 자동차용 전자 모듈은 컴퓨터 포렌식 및 모바일 포렌식과 달리 제조사 혹은 모델마다 하드웨어뿐만 아니라 운용되는 소프트웨어까지 상이하며, 미디어 파일이 DRM (Digital Rights Management)기술로 암호화[3)]되기도 한다. 이러한 이유로 자동차에 장착되어 있는 전자 모듈을 디지털 포렌식하기 위해서는 많은 연구와 시간이 필요하다.

본 논문에서는 자동차용 전자 모듈을 대상으로 디지털 포렌식 기법이 진행 방법을 소개하며, 자동차에 장착된 AVN(Audio, Video, Navigation) 시스템 모듈을 제조사가 공개한 자료에 기반하여 데이터 취득하는 방식과 내장메모리 기반 데이터 취득 하는 방식으로 내장형 블랙박스 영상을 분석한 사례를 소개한다.

2. 관련 연구

자동차에 장착된 전자기기들을 살펴보고 디지털 포렌식 관점에서 어떻게 해석 가능한지 살펴본다.

*Corresponding author, E-mail: yeubjeon@korea.kr

2.1 EDR(Event Data Recorder)

자동차에 장착되어 있는 대표적인 전자기기 장치로는 ACU(Airbag Control Unit)와 연계된 EDR(Event Data Recorder)장치가 있다. EDR은 1990년대 중반, Champ Car 및 Formula One과 같은 경주용 자동차에 장착되기 시작했다. 미국의 경우, NHTSA(National Highway Traffic Safety Administration), 미국 도로교통안전국에 의하여 EDR에 기록되는 데이터의 기록 표준이 설정되었다.[4] 우리나라의 경우 산업표준심의회에 의하여 "자동차용 사고기록장치"(KS R 5076)가 2007년 최초 제정되었다.[5] 일반적으로 EDR은 심각한 사고에서 가장 귀중한 증거로 사용되나 EDR 데이터는 자동차의 충돌에 대비한 에어백 작동과 연계되어 동작하므로, 사고 시점을 기준으로 전후 수 초간 정도의 과거 정보만 확인될 수 있어 사고와 관련된 제한적인 정보만을 확인할 수 있다. EDR에 기록되는 정보로는 속도, 휠 방향, RPM, 브레이크 신호 등이 있다. 또한 EDR은 CDR(Crash Data Retrieval)시스템을 이용하여 데이터를 기록하는데 기록된 데이터를 해석하기 위해서는 제조사에서 제공하는 전용 소프트웨어 혹은 전용 시스템을 이용해야 한다. 특정 제조사의 EDR을 제한적으로 분석한 사례가 있지만[6] 분석한 결과의 정확성을 다시 제조사로부터 확인 받아야 하는 한계점이 있다.

2.2 ECU(Electronic Control Units)

ECU(Electronic Control Units) 모듈은 다양한 역할(텔레메틱스 시스템, 차체 제어 시스템, Data Storage System for Autonomous Driving(DSSAD), 인포테인먼트 시스템 등)을 수행하고 있으며, 종류에 따라 다양한 전원 방식에 따라 동작한다. 또한 시동이 걸리지 않는 환경에서도 동작하기 때문에 다양한 정보를 저장할 수 있다. SWGDE (Scientific Working Group on Digital Evidence)에서 공개한 문서[7]에 따르면 자동차 문을 열고 닫은 기록, 언제 시동을 켜고 껐는지에 대한 기록이 저장되며, 시동이 꺼지고 내 · 외부 전등이 꺼지고 모든 문이 닫힌 상태에서 60초 후에 전원을 제거해야만 ECU장치들을 손상 없이 보존할 수 있다고 설명하고 있다. 이러한 정보들을 분석하여 자동차 사고뿐만 아니라 자동차를 이용한 범죄 사건을 재구성 할 수 있는 주요 증거로 사용될 수 있다.

2.3 자동차용 인포테인먼트 시스템

다양한 전자 제어 장치 중, 자동차용 인포테인먼트 시스템은 사용자와 가장 가까이에서 상호작용하고 사용자의 상태를 확인할 수 있는 장치다. 특히 스마트 자동차, 자율주행 자동차 기술들이 대중화되면서 많은 데이터를 수집하고 있다.[8] 자동차용 인포테인먼트 시스템은 기능과 역할에 따라 차량 내 여러 위치에 존재할 수 있으며, 여러 인포테인먼트 시스템이 연결되어 다양한 센서에서 받아온 데이터를 가공하고 전달한다. 이러한 정보를 증거로 사용하기 위해서는 보존의 연속성(Chain of custody)이 유지된 환경에서 전자 제어 장치를 다루며 데이터 손상 및 변경이 없는 방법으로 데이터를 획득하여야 한다. 하지만, 전자 제어 장치에 기록된 데이터를 획득 및 분석하기 위해서는 데이터가 어디에 어떻게 기록되어 있는지 분석 전에 확인하여야 하지만, 각 전자 모듈 제조사의 협조 없이는 확인이 어렵다는 한계점이 있다.

2.4 AVN 시스템

최근 자동차에 사용자 다양한 편의 기능을 위해 이기종 분산 시스템을 탑재하고 있으며, 그 중에서도 AVN 시스템은 사용자 인터페이스를 담당하고 있다. 다양한 전자 제어 장치들에서 수집된 데이터가 AVN을 통해서 사용자에게 디스플레이 되고 기록되어 외부 저장 매체 및 내장 메모리에 다양한 기록을 하고 있다. 이러한 다양한 기록은 자동차 사고 및 자동차를 이용한 범죄를 분석 하는데 중요한 증거물로 사용될 수 있으며, 시스템 특성상 위변조가 어렵다.

현재 시중에 상용되는 AVN 시스템은 다양한 운영체제(QNX, Windowns Embedded, Android, VxWorks 등)를 기반으로 데이터를 기록하고 있으며,[3] 공개된 운영체제인 Android를 탑재한 시스템이 최근 많이 출시되고 있다. AVN 시스템에 기록되는 데이터는 통화기록, 연락처, SNS(Social Networking Service)기록, 운행기록, 목적지, 음성명령 기록, 최근 재생한 멀티미디어 데이터 등이 저장된다. 또한, 최근 ADAS(Advanced Driver Assistance System)기술 도입에 따라 운전자 상태, 조향 관련 기록 등과 같은 자동차 내부의 기록과 주변 물체 인식, 도로상태 인식들과 같은 자동차 외부에 관한 기록 등이 저장되며, 자동차용 블랙박스 기능 또한 AVN 시스템에 내장되어 출시됨에 따라 영상 파일들이 저장되고 있다.[9]

2.5 ECU 시스템 분석 연구

자동차에 장착된 전자제어 장치를 분석 하는 연구들은 EDR에 장착된 EEPROM(Electrically Erasable Programmable Read Only Memory)을 대상으로 사고 전 후 수 초간의 데이터를 분석하는 연구들이 진행되어 왔다.[10] 그 후, 차량에 사용자 중심의 전자제어 장치들이 많아지면서, 엔터테인먼트 시스템을 분석한 연구, 텔레메틱스 시스템을 분석한 연구들이 시작되었다.[3,11] 하지만, 본 연구에서는 최근 새롭게 장착되고 있는 AVN 시스템의 영상 저장 시스템을 대상으로 추출 및 분석하여, 영상이 기록되어 있

는 전자제어 장치를 대상으로 범용적으로 적용될 수 있는 영상 복원 기법 적용 사례를 소개 한다.

3. 자동차에 대한 데이터 획득 방법

자동차를 대상으로 디지털 증거물을 획득하기 위해서 Fig. 1과 같이 인터폴 디지털 증거물 분석 가이드라인의 모바일 포렌식 데이터 획득 단계를 고려하여 진행할 수 있다.[12)]

Fig. 1 Process of mobile forensic data acquisition

3.1 저장매체 식별

첫 번째, 전자 모듈에 장착되어 있는 저장매체를 먼저 파악해야 한다. 자동차에 장착되는 저장매체는 RAM (Random Access Memory), EPROM(Erasable Programmable Read Only Memory), HDD(Hard Disk Drive), SSD(Solid State Drive), MicroSDHC, eMMC(embedded Multi-Media Card), UFS(Universal Flash Storage)등 다양하며, 저장매체의 종류에 따라 무결성을 유지하며 획득 하는 방법에 차이가 있다. 또한 저장매체의 외부에 기록된 저장용량, 제조사, 모델, 시리얼 번호 등과 같은 다양한 정보를 확인할 수 있다. 최근 출시되는 자동차의 저장매체는 충격에 강하며, 응답속도가 빠른 eMMC나 UFS 메모리를 많이 사용하고 있다.

3.2 고립 환경 구축

두 번째, 디지털 포렌식과정에서 데이터 획득 전 포렌식 대상이 되는 기기가 네트워크로 연결되어 해당 데이터가 손상되지 않도록 방지하기 위한 단계이다. 자동차에 장착된 모듈들은 다양한 네트워크 통신(WiFi, Celluar, Bluetooth, IoT망 등)과 모듈간의 통신이 발생하기 때문에 전자 모듈과 저장 매체를 분리하는 과정이 필요하며, 전자 모듈을 자동차에서 분리할 수 없는 경우에는 외부 네트워크와 연결될 수 있는 포트와 통신 칩을 분리하여야 한다. 만약 위와 같이 연결된 포트도 분리할 수 없다면, 외부 전파를 차단할 수 있는 공간이나 전파 방해 장치를 이용하여야 한다.

3.3 데이터 추출

세 번째, 고립된 환경을 구축한 후 데이터 추출 단계를 진행 한다. 전자 모듈에 장착된 저장매체가 착탈식으로 되어 있는 경우 분리하여 쓰기방지 장치를 이용하여 데이터를 획득한다. 만약 저장 매체가 모듈 회로에 온보드 되어 있는 경우 JTAG(Joint Test Action Group), Chip-Off 방식으로 저장매체의 데이터를 획득한다. 만약 저장 매체에 배드 섹터나 배드 클러스터를 발견하면 추출과정에서 ECC(Error Correcting Code)를 통해 논리적으로 복원 하거나 배드 영역을 제외하는 과정을 거친다. 한편, 전자 모듈 제작사가 데이터를 추출할 수 있는 방법을 공개한 경우, OBD Ⅱ포트, USB 포트, 진단 포트 등을 통해 공개된 방법을 통해 데이터를 추출할 수 있다. 자동차 사고의 특성상 전자 모듈이 불에 타거나, 침수되거나, 충격으로 망가졌을 경우에는 저장매체를 분리하여 물리적 복원 후 데이터를 추출하여야 한다.

3.4 검증, 문서화

네 번째 단계로 논리적/물리적으로 추출된 데이터를 교차 검증 한다. 데이터 추출 과정에서 대상이 되는 미디어 매체 데이터의 해시값과 추출된 후에 이미징된 데이터의 해시값을 비교하여 데이터 추출이 정상적으로 이루어 졌는지 검증한다. 마지막 단계로 데이터 획득 과정, 획득 시간, 추출된 데이터의 해시값을 문서화한다.

4. CASE: AVN 시스템에 저장된 블랙박스 영상 복원 및 분석

2020년 기아자동차 K7(YG)에 장착된 전자 모듈 중 AVN 모듈의 일종인 Fig. 2의 영상기록시스템(DVRS)장치를 대상으로 디지털 포렌식 방법으로 분석을 진행하였다. 본 연구에서 진행한 영상 기록 시스템은 2019년 이후 출시된 현대, 기아, 제네시스 차량에 옵션 및 패키지 형태로 장착이 가능하고,[13-15)] 본 연구에서 진행된 추출-분석 방법은 빌트인 캠 형태로 동작하는 시스템에 대해서 범용적으로 적용될 수 있다.

Fig. 2 Drive video record system in K7

4.1 데이터 획득

4.1.1 분석 대상 매체 식별

영상기록 시스템(Drive video record system)은 제조사[14]에 따르면 AVN 시스템과 연동되어 컨트롤 및 영상 재생이 가능하다. 입력 장치로는 전방/후방 카메라, CAN 통신 포트 등이 있으며 출력 장치로는 AVN 장치와 연결된 화면 출력 단자, 영상을 다운로드 받을 수 있는 USB 단자 등이 Fig. 3과 같이 존재한다.[14] 또한 보조 배터리 장착 시 배터리 전원과는 별개의 전원 장치로 동작이 가능하다.

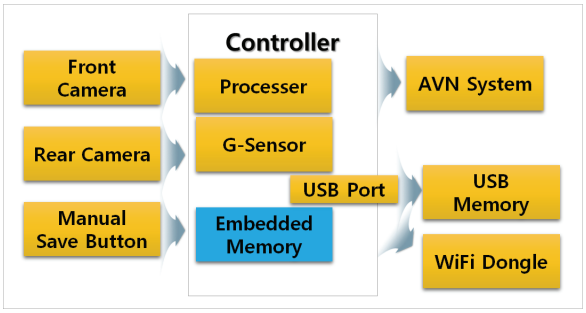

Fig. 3 DVRS system diagram[14]

4.1.2 고립 환경 구축

영상기록 시스템(Drive video record system)은 AVN 시스템 및 카메라 모듈들과 연결되어 증거물이 되는 영상을 삭제 및 덮어쓰기 될 가능성이 있기 때문에 장착되어 있는 연결 포트를 모두 제거 한다. 이때 USB 포트에 WiFi 연결 동글이 장착되어 있다면 함께 제거 한 후 데이터 획득을 진행하여야 한다.

4.1.3 AVN 데이터 추출

영상기록 시스템(Drive video record system)의 저장 매체를 확인하기 위해 분해하여 내부 회로를 확인한 결과 Fig. 4와 같이 eMMC(embedded Multimedia Card) 메모리가 온보드된 형태로 발견 되었다. 메모리 외관에 표기된 라벨 정보를 확인한 결과, 해당 메모리는 삼성전자에서 제작한 eMMC 메모리이며, 모델명은 “KLMCG8GESD-B04Q”으로 세부적인 규격은 Table 1과 같이 확인되었다. 해당 eMMC 메모리카드의 데이터를 추출하기 위한 방법은 세 가지 방식이 있다.

1) 첫 번째로는 정상적으로 시동이 켜지는 경우, 영상기록 시스템과 연동된 AVN 시스템의 화면으로 원하는 영상을 선택하여 USB 단자를 이용하여 영상 데이터를 추출하는 방법이 있지만, 자동차가 손상되어 정상적으로 전원을 연결할 수 없거나 AVN 시스템을 정상적으로 연결할 수 없는 경우 사용할 수 없다.

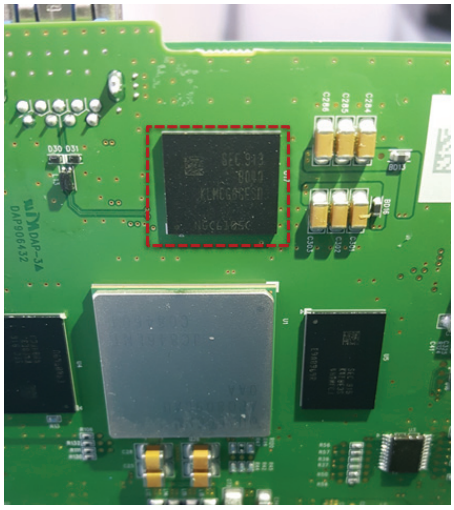

Fig. 4 eMMC memory on DVRS system

Table 1 KLMCG8GESD-B04Q specifications[16]

Type	Value
Version	eMMC5.1
Voltage	1.8/3.3 V
Density	64 GB
Interface	HS400
Temp.	-40 ~ 105 °C

2) 두 번째 정상적으로 전원을 연결할 수 없거나 AVN 시스템에 연결되지 않았을 경우, 제조사에서 제공하는 영상 비상다운로드 방식[14]으로 데이터를 획득하는 방법이다. 영상 기록 시스템의 메인 커넥트는 배터리 전원 및 접지, 앞/뒤 카메라 모듈 전원 공급 및 접지, CAN 통신, ACC 및 IGN 입력 등의 역할을 하고 있다. 하지만 Fig. 5와 같이 메인 커넥터에 특정 시간동안 특정 핀에 전원을 입력 하면 영상 비상 다운로드 모드로 동작 시킬 수 있으며, 연결된 USB 포트로 영상 데이터를 추출할 수 있다.

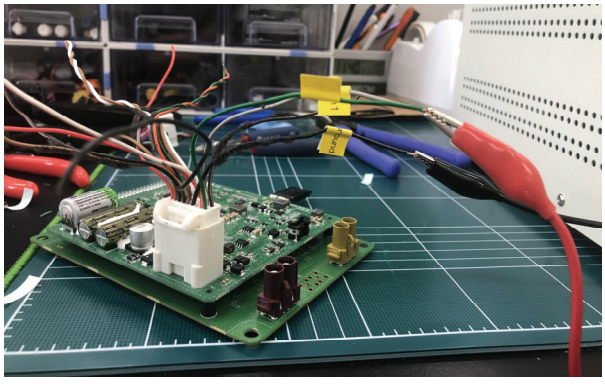

Fig. 5 Emergency download method on DVRS

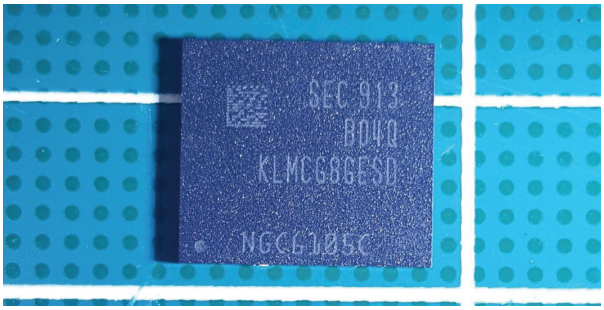

Fig. 6 Chip-off on DVRS system

3) 마지막 방법은 온보드 되어 있는 메모리를 분리 하는 방법(Chip-off)이다. 이 방법은 회로 손상 및 USB 단자 손상 등으로 비상다운로드 방법을 사용 할 수 없는 경우 Fig. 6과 같이 물리적으로 eMMC 메모리를 분리하는 방법이다. 이 방법을 이용하면 메모리 전체영역의 데이터를 획득할 수 있다는 장점이 있지만, 메모리 분리 과정에서 손상될 수 있다는 단점을 가지고 있다.

4.2 취득 방법에 따른 데이터 형태

본 논문에서는 제조사의 비상다운로드 방식과 메모리 분리 방식을 이용하여 데이터를 취득 후 분석하였다.

4.2.1 비상 다운로드 모드 추출 데이터

제조사에서 제공한 비상 다운로드 방식으로 USB 포트로 연결된 메모리로 추출된 데이터는 제조사 매뉴얼에 따라 상위 디렉토리에 하나의 로그 텍스트 파일과 하나의 폴더가 생성된 것이 확인되었다. 제조사 매뉴얼[14] 따르면 로그 텍스트 파일은 네 가지 형태로 기록되는 것이 확인되었다. 첫 번째, USB단자에 저장매체가 완료 전 제거되었을 때, 두 번째, 저장매체에 파일을 정상적으로 생성하지 못했을 때, 세 번째, USB 저장매체의 용량이 다운로드 받을 데이터의 용량보다 작을 때, 마지막으로 정상적으로 다운이 완료되었을 때 로그 기록을 남긴다. 본 논문에서 진행된 방식은 다운로드가 정상적으로 완료되어 밀리 초 단위로 기록된 시간정보와 “Download completed”로그가 기록된 것이 확인되었다. 최상위 폴더에 기록된 폴더명은 차명이 기록되며 그 하위 폴더에는 다운로드 시작 시점의 시간 정보가 초 단위로 기록되어 있었다. 한편, 영상 기록시스템이 분리 되어도 회로에 장착된 배터리로 시간 정보가 현재 시간을 기록할 수 있을 것으로 추정된다.

초 단위로 기록된 폴더의 하위 폴더에는 Table 2와 같이 세 개의 폴더에 영상 데이터가 각각 저장되어 있으며, 각 폴더는 일반 주행 시, 주행 시 충격 이벤트 발생시, 저장 버튼을 눌렀을 때의 상황에 따라 각기 다른 영상을 저장하고 있다. 전체 동영상 파일 중 가장 마지막에 기록된 영상 파일은 “1.Drive_Normal”폴더에 저장되어 있는 것으로 보아 영상 파일은 해당 영상 기록 시스템은 일반적으로 “1.Drive_Normal”폴더에 영상을 기록하고 난 후, 보드에 장착된 G-Sensor 값이 일정 수준 이상으로 기록될 시점의 앞 뒤 10초가량의 영상데이터를 “2.Drive_Crash_Event” 폴더에 기록하는 것으로 추정된다.

Table 2 Extracted files using emergency download

Folder name	Num. of files	Capacity
1.Drive_Normal	360	15.6 GB
2.Drive_Crash_Event	80	1.18 GB
5.Switch_Event	6	90.5 MB

또한, 비상다운로드 모드로 추출된 데이터양이 약 16.7 GB이며, 제조사에서 제시한 파일 최대 용량 28 GB인 것을 고려할 때, 녹화된 활성 데이터만을 추출할 수 있는 것으로 추정된다.

4.2.2 메모리 분리 추출 데이터

영상기록 시스템의 온보드 되어있는 메모리에서 분리하여 추출된 eMMC 메모리에서 추출된 데이터의 전체 용량은 약 64.3 GB로 메모리 사양에서 확인되는 용량(64 GB)[16]과 유사한 용량의 데이터가 추출되었다. 추출된 데이터는 57개의 파티션 정보로 분류되며, 각 파티션 정보는 다양한 역할(백업, 복구, 캐시, 시스템, 유저 데이터, 부트, 비디오, 업데이트 등)을 하는 공간으로 분리 되어 있었다. 그 중에서 “ALLPART”영역은 약 32 GB로 가장 큰 데이터 영역을 차지하고 있었고, 해당 영역을 파일시스템 단위로 분석 한 결과, 메모리 분리로 추출된 파티션 57개의 영역 중 자신의 파티션 정보를 제외한 56 파티션 정보가 기록되어 있었다. 더욱이 메모리 분리된 56개의 파티션 정보와 “ALLPART”영역에서 파일시스템으로 분석된 56개의 파티션 정보의 각 볼륨별 해시값을 비교 하였을 때 모두 같은 것으로 보아 데이터 안전성 및 보안성을 높이기 위해 eMMC 메모리에서 미러링된 데이터로 추정된다.

4.3 취득 방법 별 데이터 분석 결과

4.3.1 비상 다운로드 모드 추출 데이터

비상 다운로드 모드로 추출된 영상 파일은 총 446개이며, 영상 파일은 Table 3과 같이 확장자 MP4파일로 전방/후방채널이 분리되어 저장되며 파일 이름에 시간정보가 기록되어 있었다.

Table 3 Example of extracted MP4 files

Folder name	Example of file name
1.Drive_Normal	NOR_20201001_134148_F.mp4
	NOR_20201001_134148_R.mp4
	...
2.Drive_Crash_Event	EVT_20201025_153258_F.mp4
	EVT_20201025_153258_R.mp4
	...
5.Switch_Event	NOM_20201011_131303_F.mp4
	NOM_20201011_131303_R.mp4
	...

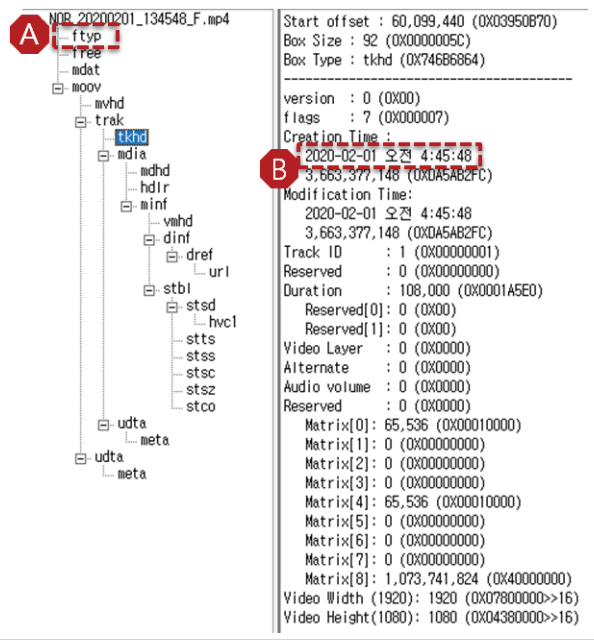

Fig. 7 Front channel video file by emergency download

추출된 확장자 “MP4”동영상 파일을 분석한 결과, 전방 채널 영상 파일은 해상도 1920×1080, 프레임 레이트 30 fps이며, 음성 채널 정보는 포함되어있지 않고, 후방 채널 영상 파일은 해상도 1280×720, 프레임 레이트 30 fps이며, 음성 채널 정보는 포함되어 있지 않았다.

추출된 MP4 파일은 Fig. 7A와 같이 FTYP(File Type Box)구조[17]로 영상이 기록되어 있었다. 또한 Fig. 7B와 같이 tkhd(Track header box)에 시간정보가 기록되어 있었다. FTYP 구조 안에 기록된 메타 정보의 시간 정보는 파일 이름에 기록된 시간정보와 9시간 차이가 나는 것으로 보아 메타 정보에 기록된 시간 정보가 UTC(Coordinated Universal Time) 기준으로 기록된 것으로 추정된다.

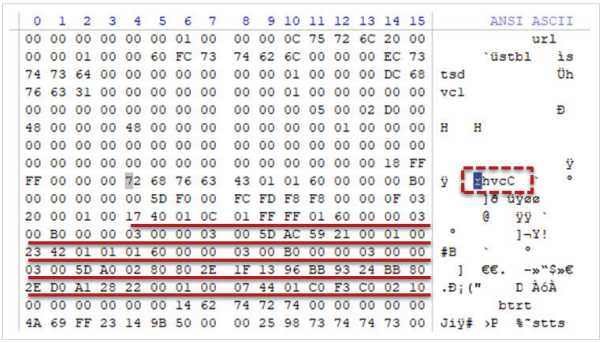

Fig. 8 Information of H.265 encoding parameter

또한 추출된 동영상 파일은 Fig. 8과 같이 파일 구조 정보에 “hvcc”가 기록되어 있어, 추출된 동영상 파일은 H.265코덱[18]으로 인코딩되어 있음을 확인할 수 있다. 또한 Fig. 8과 같이 H.265코덱의 인코딩 정보인 SPS(Sequence Parameter Set), PPS(Picture Parameter Set), VPS(Video Parameter Set)정보가 기록되어 있다.

4.3.2 메모리 분리 추출 데이터

메모리 분리 방식으로 추출된 56개의 파티션을 분석한 결과, 다양한 파일시스템(FAT16, EXT4, TrueFFS)으로 구성되어 있었다. 파티션에서 데이터를 추출하기 위해 Signature Carving[19] 방식으로 데이터를 추출한 결과, JPEG, MP4, DB 형태의 파일들이 발견되었다. JPEG 구조로 추출된 사진 파일은 해상도 640×480 사이즈이고, EXIF(Exchangeable Image File Format)메타 데이터는 발견되지 않았으며, Fig. 9와 같이 전방/후방 채널 영상의 썸네일 사진 파일로 추정된다.

DB 형식으로 추출된 파일은 Fig. 10과 같이 SQLlite 포맷[20]의 형태로 데이터를 기록하고 있으며, 추출된 데이

Fig. 9 Example of JPEG files by signature carving

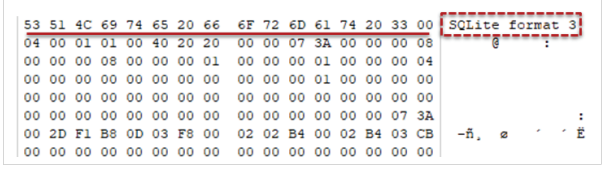

Fig. 10 Example of DB files by signature carving

name	type	fullpath	thumb	exist
NOM_20191210_024205	5	null	null	1
NOM_20200111_111748	5	null	null	1
NOM_20200111_131303	5	null	null	1
EVT_20200125_152038	2	null	null	1
EVT_20200125_153258	2	null	null	1
EVT_20200125_230126	2	null	null	1
EVT_20200126_015341	2	null	null	1
EVT_20200126_235424	2	null	null	1
EVT_20200127_191017	2	null	null	1
EVT_20200127_222015	2	null	null	1
EVT_20200128_000003	2	null	null	1

Fig. 11 Example of DB files by signature carving

Table 4 Compare of total play time by each method

Method	Total play time
Emergency download method	6 h 12 m 15 s
Chip-off (Signature carving)	2 h 50 m 56 s
Chip-off (Frame based carving)	7 h 48 m 47 s

터베이스 일부에서는 Fig. 11과 같이 파일명, 저장경로, 썸네일 사진의 유무, 삭제 유무에 대한 기록이 저장되어 있는 것으로 추정된다.

FTYP 구조로 추출된 동영상 파일은 512개로 확인되나, 그중 파일 파편화 되어 있지 않으며 정상적으로 재생되는 파일은 230개로 확인 되었다. 비상 다운로드 방식으로 추출된 파일 446개와 메모리 분리 후 Signature carving 방식으로 추출된 재생 가능한 동영상 파일 230개의 총 재생 시간은 Table 4와 같이 비상다운로드 방식이 약 3시간 20분 더 많이 재생되는 차이가 발생하였다. 그 이유로는 Signature carving 방식으로 추출된 동영상 파일 중 절반 이상이 파편화되어 있기 때문에 정상적으로 재생되지 않은 것으로 확인된다.

동영상 파일을 프레임 단위로 복원 가능한 기법[21]으로 동영상 파일이 기록되어 있는 파티션을 대상으로 복원을 진행하였다. 전체 영역에서 H.265코덱으로 인코딩된 프레임은 인터 프레임과 인트라 프레임을 합쳐 843,810개의 영상 프레임으로 확인되었다. 비상다운로드 방식으로 추출된 동영상의 FPS(Frame Per Sec)값인 30 fps로 계산 한 결과 전체 영역의 재생 시간은 7시간 48분 47초인 것으로 확인되었다. 그 이유는 메모리에 삭제된 영상 파일이 메모리에 남아 있을 경우와 메모리 캐시 영역 및 파일 슬랙 영역에 영상 파일이 남아 있기 때문이다. 따라서 프레임 단위로 추출된 영상 프레임의 총 재생 시간이 비상다운로드 방식 및 Signature carving한 방법보다 재생 시간이 긴 것으로 확인된다.

5. 결론 및 향후 연구

본 논문에서는 기존 디지털 포렌식 기술들을 자동차에 장착된 전자 기기를 대상으로 식별, 고립, 획득, 실험, 분석하는 방법과 AVN 시스템과 같이 사용자와 직접 연결되어 데이터를 수집 저장하는 장치들에 대해 디지털 포렌식한 사례를 소개하였다. 본 연구에서 소개한 AVN 시스템에 장착된 영상 기록 장치 사례에서는 데이터 획득 방법에 따라 획득 가능한 데이터 용량과 형태가 달라질 수 있음을 보였고, 그에 따라 분석된 결과 또한 다름을 알 수 있었다. 또한 제조사에서 공개한 상세한 매뉴얼과 데이터 추출 방법이 있는 경우, 보다 명확한 사고원인 파악이 가능함을 확인하였다. 앞으로 자동차에 장착된 전자기기들은 더욱 다양해질 것이며, 모바일 포렌식과 같이 수사를 위해서 필수적으로 자동차 포렌식을 해야 되는 시대에 직면함에 따라 자동차에 장착된 다양한 전자기기들을 대상으로 한 디지털 포렌식 연구를 진행할 필요가 있다.

후 기

이 논문은 행정안전부 주관 국립과학수사연구원 중장기과학수사감정기법연구개발(R&D) 사업의 지원을 받아 수행한 연구임(NFS2021DTB02).

References

1) T. Zou, M. Cai, R. Du and J. Liu, “Analyzing the Uncertainty of Simulation Results in Accident Reconstruction with Response Surface Methodology,” Forensic Science International, Vol.216, Nos.1-3, pp.49-60, 2012.
2) D. L. Watson and A. Jones, Digital Forensics Processing and Procedures Meeting the Requirements of ISO 17020, ISO17025, ISO 27001 and Best Practice Requirements, Elsevier, MA, 2013.
3) N. A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens and K. K. R. Choo, “Smart Vehicle Forensics: Challenges and Case Study,” Future Generation Computer Systems, Vol.109, pp.500-510, 2020.
4) J. S. Daily, N. Singleton, E. Downing and G. W. Manes, “The Forensics Aspects of Event Data Recorders,” Journal of Digital Forensics, Security and Law, Vol.3, No.3, pp.29-42, 2008.
5) Korean Agency for Technology and Standards, Accident Data Recording Systems for Road Vehicles, KS R 5076, 2019.
6) S. H. Lim, J. C. Park, J. H. Kim, W. T. Oh, J. H. Choi and J. J. Park, “Analysis of Multi-Car

Rear-End and Chain Reaction Collision Using EDR," Transactions of KSAE, Vol.27, No.2, pp.101-108, 2019.
7) K. A. Jackson Jr., Infotainment and Telematic Systems Challenges Effecting Vehicle Forensic Law Enforcement Capabilities. Ph.D. Dissertation, Utica College, 2020.
8) K. S. Han, "Optimized Speed and Gearshift Trajectories Planning for Autonomous Electric Vehicles," Transactions of KSAE, Vol.28, No.10, pp.669-676, 2020.
9) G. De La Torre, P. Rad and K. K. R. Choo, "Driverless Vehicle Security: Challenges and Future Research Opportunities," Future Generation Computer Systems, Vol.108, pp.1092-1111, 2020.
10) H. Mansor, K. Markantonakis, R. N. Akram, K. Mayes and I. Gurulian, "Log Your Car: The Non-invasive Vehicle Forensics," IEEE Trustcom/BigDataSE/ISPA, pp.974-982, 2016.
11) C. J. Whelan, J. Sammons, B. McManus and T. W. Fenger, "Retrieval of Infotainment System Artifacts from Vehicles Using iVe," Journal of Applied Digital Evidence, Vol.1, No.1, pp.30-45, 2018.
12) P. Reedy, "Interpol Review of Digital Evidence 2016-2019," Forensic Science International: Synergy, Vol.2, pp.489-520, 2020.
13) KIA Motors, K7, https://www.kia.com/kr/vehicles/k7/features.html, 2021.
14) KIA Motors, Global Service Way Technical Information, https://gsw.kia.com/kmc/login.tiles, Last accessed 2021-08-25.
15) Hyundai Motors, Hyundai Service Network, https://gsw.hyundai.com/hmc/login.tiles, Last accessed 2021-08-25.
16) Samsung Electronics, eMMC, https://www.samsung.com/semiconductor/estorage/emmc/KLMCG8GESD-B04Q/, Last accessed 2021-03-26.
17) T. Gloe, A. Fischer and M. Kirchner, "Forensic Analysis of Video File Formats," Digital Investigation, Vol.11, pp.S68-S76, 2014.
18) G. J. Sullivan, J. R. Ohm, W. J. Han and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard," IEEE Transactions on Circuits and Systems for Video Technology, Vol.22, No.12, pp.1649-1668, 2012.
19) D. Povar and V. K. Bhadran, "Forensic Data Carving," International Conference on Digital Forensics and Cyber Crime, Springer, Berlin, Heidelberg, pp.137-148, 2010.
20) S. Nemetz, S. Schmitt and F. Freiling, "A Standardized Corpus for SQLite Database Forensics," Digital Investigation, Vol.24, pp.S121-S130, 2018.
21) G. H. Na, K. S. Shim, K. W. Moon, S. G. Kong, E. S. Kim and J. Lee, "Frame-based Recovery of Corrupted Video Files Using Video Codec Specifications," IEEE Transactions on Image Processing, Vol.23, No.2, pp.517-526, 2013.