차량 IVI 로그 분석을 위한 룰셋 기반 디지털 포렌식 도구 설계 및 구현*

김보겸°[1] · 박수현[2] · 하상우[2] · 조성제[1]
[1]단국대학교 소프트웨어학과, [2]단국대학교 컴퓨터학과
{bogamie, parksh, sangu1115, sjcho}@dankook.ac.kr

Design and Implementation of a Rule-based Digital Forensic Tool for Vehicle IVI Log Analysis

Bogyeom Kim°[1] · SuHyeon Park[2] · SangWoo Ha[2] · SeongJe Cho[1]
[1]Dept. of Software Science, Dankook University
[2]Dept. of Computer Science and Engineering, Dankook University

요 약

차량 인포테인먼트(IVI) 시스템은 차량 제어 이벤트, 위치 이력, 통신 기록 등 디지털 포렌식에 활용 가능한 다양한 로그를 생성한다. 그러나 기존 안드로이드 기반 IVI 로그 분석 도구는 차종별 확장성이 낮고, 로그 무결성 검증 기능이 미흡하며, 사건 맥락을 파악할 수 있는 타임라인 가시화 기능이 제한적이다. 본 논문에서는 이러한 한계를 해결하기 위해, 분석 규칙을 YAML 기반 룰셋(YAML Ain't Markup Language-based Rule set)으로 분리하고, 암호학적 해시 기반 무결성 검증 및 사건 단위 타임라인 가시화를 지원하는 IVI 디지털 포렌식 도구를 제안한다. 제안 시스템은 룰셋 저장소, 분석 파이프라인, 사건 관리의 3계층 구조로 구성된다. 이들 중, 로그 분석 파이프라인은 무결성 검증, 룰셋 로딩, 패턴 매칭, 이벤트 정규화 및 적재의 4단계로 구성된다. 현대 아반떼 CN7PE IVI 시스템 로그(약 93MB)를 대상으로 77개의 분석 규칙을 적용한 결과, 721개 파일을 약 4.2초 만에 처리하여 총 24,338건의 이벤트를 자동 추출하고 이를 사건 단위 타임라인으로 가시화할 수 있었다.

1. 서 론

차량 인포테인먼트(In-Vehicle Infotainment, IVI) 시스템은 내비게이션, 스마트폰 연동 등 다양한 기능을 제공하는 동시에, 차량 제어 이벤트, 운전자 위치 이력, 통신 기록과 같은 로그를 비휘발성 저장소에 지속적으로 기록한다. 이러한 로그는 교통사고 재구성과 운전자 행위 분석 등 차량 디지털 포렌식 분야에서 핵심 증거로 활용될 수 있으며, 이에 따라 IVI 로그를 효율적으로 수집·분석하기 위한 기술적 요구가 증가하고 있다[1].

그러나 기존 안드로이드 기반 IVI 로그 분석 방법은 몇 가지 한계를 가진다. 첫째, 분석에 사용되는 정규식 규칙이 도구 내부에 종속적으로 포함되어 있어 차종 또는 제조사 변경 시 확장성이 낮다[2, 3]. 둘째, 분석 대상 로그에 대한 무결성 검증 기능이 부재하여 디지털 증거로서의 신뢰성과 법적 활용 가능성을 충분히 보장하기 어렵다[1, 4]. 셋째, 분석 결과가 주로 CSV 형태로 제공되어 사건의 시간적 흐름과 맥락을 직관적으로 파악하기 어렵다[2, 5].

본 논문에서는 이러한 문제를 해결하기 위해, 분석 규칙을 YAML 기반 룰셋으로 분리하여 차종별 확장성을 확보하고, 로그 수집·분석 단계에서 해시 기반 무결성 검증을 수행하며, 추출된 이벤트를 사건 단위 타임라인으로 가시화해 주는 웹 기반 IVI 디지털 포렌식 도구를 제안한다. 제안 도구는, 룰셋 저장소 계층, 분석 파이프라인 계층, 사건 관리 계층으로 구성되며, 분석 파이프라인은 무결성 검증, 룰셋 로딩, 패턴 매칭, 이벤트 정규화의 단계적 처리 과정을 통해 구조화된 이벤트 데이터를 생성한다. 또한, 현대 아반떼 CN7PE IVI 시스템에서 수집한 로그 데이터를 대상으로 다양한 로그 유형에 대한 분석 규칙을 정의하고 이를 제안 도구에 적용함으로써, IVI 로그 포렌식 분석의 자동화 및 효율성을 실험적으로 검증한다.

2. 관련 연구

Strandberg 등[1]은 차량 디지털 포렌식 분야의 도전 과제를 제시하고, 데이터 수집·분석 기법을 체계적으로 정리한 문헌을 제시하여 사고·범죄 수사에서 활용될 수 있음을 보였으며, 차종 간 표준화된 분석 절차의 부재를 주요 한계로 지적하였다.

Kang 등[2]은 안드로이드 기반 IVI 시스템의 압축 로그를 대상으로, 도어·GPS·기어 3개 카테고리 18개 메시지에서 이벤트를 추출해 CSV로 출력하는 특정 차종에 종속된 정규식 DB 기반 자동 필터링 도구를 제안하였다.

Shin 등[6]은 Android Auto·Apple CarPlay 환경의 IVI 디지털 포렌식 사례연구를 통해 모바일기기-차량 연결 환경에서 추출·분석 가능한 아티팩트 분류 체계를 정리하였고, 상용 도구인 Berla iVe[7]는 다수 차종에 대한 추출 프로파일을 제공한다. 다만 두

* 본 논문은 2026년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업 지원을 받아 수행되었음 (2024-0-00035). 또한 본 논문은 2026년도 정부(경찰청·과학기술정보통신부)의 재원으로 과학치안진흥센터 미래치안도전기술개발 사업의 지원을 받아 수행된 연구임 (No.RS-2026-25527545).

접근 모두 분석 결과를 사건(case) 단위로 통합 관리·재현하는 워크플로우가 제한적이다.

본 논문에서는, IVI 로그를 분석하는 규칙을 분석 파이프라인과 분리된 YAML 규칙 파일로 관리하여, 해당 파이프라인의 재빌드 없이 차종 확장이 가능하고, 로그 수집·분석 시점의 해시 검증으로 디지털 증거의 무결성을 보장하며, 추출된 이벤트를 사건 단위로 묶어 시간순 타임라인으로 가시화·협업 분석을 지원한다는 점에서 기존 연구와 차별화된다.

3. IVI 디지털 포렌식 도구

제안 시스템은 그림 1과 같이 룰셋 저장소 계층, 분석 파이프라인 계층, 사건 관리 계층의 3계층으로 구성된다. 룰셋 저장소 계층은 차종별 분석 규칙을 외부 파일로 보관하고, 분석 파이프라인 계층은 IVI 로그 파일을 4단계로 나누어 처리해 정규화된 이벤트를 산출하며, 사건 관리 계층은 추출된 이벤트를 사건 단위로 묶어 가시화·협업 분석을 지원한다.

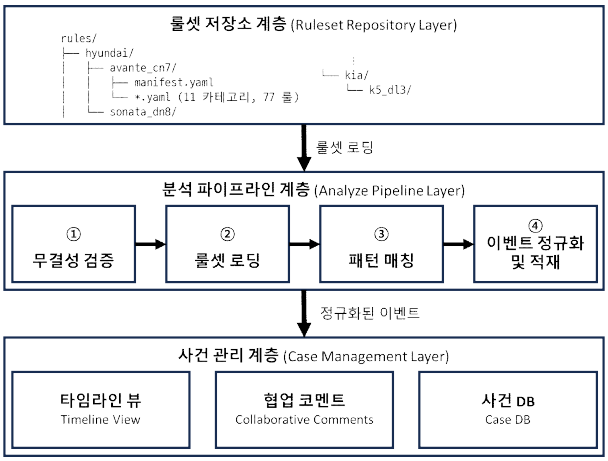

그림 1 제안 시스템의 3계층 구조

3.1 룰셋 저장소 계층

룰셋 저장소 계층은 <제조사>/<차종>/ 디렉터리 구조로 차종별 규칙을 분리하여 보관한다. 각 차종 디렉터리는 차종 정보(제조사·모델명·OS 버전 등)와 어떤 로그 파일에 어떤 규칙 파일을 적용할지 정의한 매니페스트(manifest), 로그 종류별 규칙 파일들로 구성된다(그림 2 참조).

```yaml
manufacturer: "Hyundai"
target_models: "Avante CN7"
version: "Kitkat"
mappings:
  - file_pattern: "telematics"
    rule_file: "telematics.yaml"
  - file_pattern: "eventlogs"
    rule_file: "eventlogs.yaml"
  - file_pattern: "dumpstate"
    rule_file: "dumpstate.yaml"
```

그림 2 매니페스트 구조 예시

개별 규칙 파일은, (i) 해당 로그 종류 전체에 공통으로 적용되는 타임스탬프 패턴, (ii) 코드값을 사람이 읽을 수 있는 라벨로 바꾸기 위한 사전(dictionary), (iii) 규칙 목록으로 구성된다. 각 규칙은 로그 메시지를 차종마다 서로 다른 필드값을 정규화된 이벤트로 변환하기 위해 다음 5개 필드로 구성된다(표 1 참조).

표 1 개별 규칙 파일을 구성하는 5개 필드

필드	역할	산출물
패턴 매칭 (pattern)	정규식에 통과되는 로그만 걸러냄	(?P<code>0x[0-9A-F]+)과 매칭되는 로그
추출 (extract)	로그 메시지에서 의미있는 이벤트 추출	시각=10:23:45, 코드=0x1A, 위치=운전석
해석 (interpret)	이벤트를 사람이 읽을 수 있는 언어로 변환	code: "0x1A" → "Door Open"
정규화 (normalize)	차종마다 다른 필드값을 정규화함	event_type: DOOR_OPEN, severity: INFO
요약 (render)	타임라인 요약·상세 문장 생성	"10:23 운전석 문 열림"

3.2. 분석 파이프라인 계층

분석 파이프라인 계층은 다음 4단계로 구성된다. 먼저 무결성 검증 단계에서 로그 획득 시 생성한 해시값과 도구가 계산한 해시값을 비교해 파일 변조 여부를 검증하며, 이를 통해 수집 시점과 분석 시점의 로그 동일성·무결성을 확인한다. 검증을 통과한 파일만 다음 단계로 진입하게 하여, chain of custody 기록과 결합될 때 분석 결과의 신뢰성과 법적 증거 수용 가능성을 보완할 수 있다.

룰셋 로딩 단계에서는 사용자가 지정한 차종에 해당하는 매니페스트와 규칙 파일들을 메모리에 적재한다. 패턴 매칭 단계에서 압축 로그 파일을 풀어 각 로그 파일을 매핑된 규칙 파일에 분배하고 표 1의 패턴·추출 필드를 적용한다. 마지막으로 이벤트 정규화 및 적재 단계에서, 표 1의 해석·정규화·요약 필드를 차례로 적용하여 정규화된 이벤트를 생성하고, 이를 사건 식별자와 함께 데이터베이스에 적재한다.

3.3. 사건 관리 계층

사건 관리 계층은, 분석 파이프라인 계층에서 산출된 정규화된 이벤트를 사건 단위로 통합 관리하며, 타임라인 뷰, 협업 코멘트, 사건 DB의 세 가지 구성 요소를 갖는다. 타임라인 뷰는 사건에 속한 이벤트를 시간순으로 정렬해 분석가가 사건 흐름을 직관적으로 파악할 수 있도록 가시화한다. 협업 코멘트는 각 이벤트에 분석가가 의견을 남기고 다른 분석가가 이를 검토할 수 있게 하여 사건 단위 협업 분석을 지원한다. 사건 DB는 추출된 이벤트와 분석가가 남긴 코멘트를 사건 식별자로 묶어 영속 보관한다.

4. 실험 및 평가

본 실험은 현대 아반떼 CN7PE(7세대 아반떼) 차량의 IVI 시스템에서 딜러 모드 (Dealer Mode)를 통해 추출한 약 93MB 용량의 압축 로그 파일을 사용하여 수행하였다(표 2 참조).

표 2 실험 대상 로그 데이터 정보

항목	값
차종	현대 Avante CN7PE
HU 플랫폼	wp_daudioplus_cn7pe_kr
AVN 펌웨어	CN7PE.KOR.0000.V036.001.251023
Android 버전	4.4.2 (KitKat, SDK 19)

4.1. 정의된 정규식 규칙 개수

대상 차량의 로그를 분석하여 11개의 로그 파일 종류에 대하여 총 77개의 규칙을 정의하였다(표 3 참조). 선행 연구[2]에서는 도어·GPS·기어 3개의 로그 파일 종류에 한정되어 18개의 정규식 패턴만을 정의한 반면, 본 논문에서는 텔레매틱스·부팅·블루투스 등을 포함한 11개 로그 파일 종류로 분석 범위를 확장하였다.

표 3 현대 아반떼 CN7PE 로그 파일 종류별 정의 규칙 수

로그 파일 종류	규칙 수	로그 파일 종류	규칙 수
telematics	22	setGps	3
eventlogs	15	systemBoot	3
micomBoot	13	locationsharing	3
bluetoothLogFilter	6	driveSession	2
teleService	6	dumpstate	2
-	-	mofgen	2
합계			77

4.2. 분석 결과

분석 파이프라인은 721개 파일로 구성된 압축 로그 파일을 약 4.2초 만에 처리하여 총 24,338건의 이벤트를 추출하였다. 추출된 이벤트에는 차량 식별 정보(차종·VIN·주행거리), 차량 이동 상태, ADAS 동작 로그, 내비게이션 정보 등이 포함되었으며, 타임라인 뷰에서 시계열로 정렬되어 차량 운행 흐름을 직관적으로 파악할 수 있도록 가시화하였다(그림 3 참조).

그림 3 추출된 이벤트의 시간순 타임라인 UI 예시

표 4는 원본 IVI 로그와 제안 도구의 정규화 표현을 비교한 예시이다. 기존 로그는 필드명, 시스템 메시지, CAN 신호명이 혼재되어 의미 해석이 어렵지만, 제안 도구는 이를 차량 식별 정보, 이동 상태, ADAS 상태 신호 등 의미 단위 이벤트로 변환한다. 이를 통해 원본 로그의 신호 코드에 대한 의존도를 낮추고, 사건 타임라인에서 차량 상태와 운행 흐름을 직관적으로 파악할 수 있다.

표 4 기존 원본 로그와 제안 도구의 정규화 표현 비교

원본 로그	데이터 유형	정규화 표현
{VehicleName:CN7PE}, {RunDistance:5803.9}, {VIN:…1315} …	차량/시스템 정보	차량 식별: CN7PE · 주행거리 5803.9km · VIN:…1315
Vehicle Movement Status Changed to true/false	차량 이동 상태	차량 이동 시작/멈춤 이벤트
[CAN] CF_Lca_Stat_LAMP=2	CAN 기반 ADAS 상태 신호	ADAS·차로 변경 보조(LCA) 표시등 동작

5. 결 론

본 논문에서는 차량 IVI 로그 분석을 위해 차종별 YAML 룰셋 관리, 로그 분석 시 해시 검증 기반 무결성 보장, 사건 단위 협업 분석을 지원하는 통합 웹 플랫폼을 제안하였다. 현대 아반떼 CN7PE 양산 펌웨어를 대상으로 총 24,338건의 이벤트를 자동 추출하고 시간순 타임라인으로 가시화하였다.

단일 차종(현대 아반떼 CN7PE의 Android 4.4.2 기반 IVI)에 대해 실험 및 검증을 수행하였지만, 분석 파이프라인 수정 없이 외부 YAML 작성만으로 차종 확장이 가능하다는 점에서 신규 차종 대응의 진입 장벽을 낮출 수 있다. 향후, 차량의 IVI 시스템과 연동한 운전자 모바일 단말 로그(통화·메시지·위치 등)를 결합한 통합 타임라인 구축과 다양한 제조사·차종으로의 룰셋 확장 등의 연구를 수행할 계획이다.

참고 문헌

[1] K. Strandberg, N. Nowdehi, T. Olovsson, "A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection," IEEE Transactions on Intelligent Vehicles, vol. 8, no. 2, pp. 1350-1367, 2023.

[2] H. Kang, J. Jung, S. Cho, M. Park, J. Choi, S. Cho, "A Filtering Tool for Efficiently Analyzing Log Data of Android-based In-Vehicle Infotainment Systems," The 9th International Conference on Next Generation Computing, pp. 207-210, 2023.

[3] C. C.-C. Cheng, C. Shi, N. Z. Gong, Y. Guan, "LogExtractor: Extracting digital evidence from android log messages via string and taint analysis," Forensic Science International: Digital Investigation, vol. 37, pp. 301193, 2021.

[4] I. Ismail, K. A. Z. A. Ariffin, "Open Source Tools for Digital Forensic Investigation: Capability, Reliability, Transparency and Legal Requirements," KSII Transactions on Internet and Information Systems, vol. 18, no. 9, pp. 2692-2716, 2024.

[5] H. Kang, H. Seong, I. Kim, W. Jeong, S.-J. Cho, M. Park, S. Han, "Android-Based Audio Video Navigation System Forensics: A Case Study," Applied Sciences, vol. 13, no. 10, pp. 6176, 2023.

[6] Y. Shin, S. Kim, W. Jo, T. Shon, "Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay," Sensors, vol. 22, no. 19, pp. 7196, 2022.

[7] Berla Corporation, "Berla iVe," 2026, [Online]. Available: https://berla.co/.