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

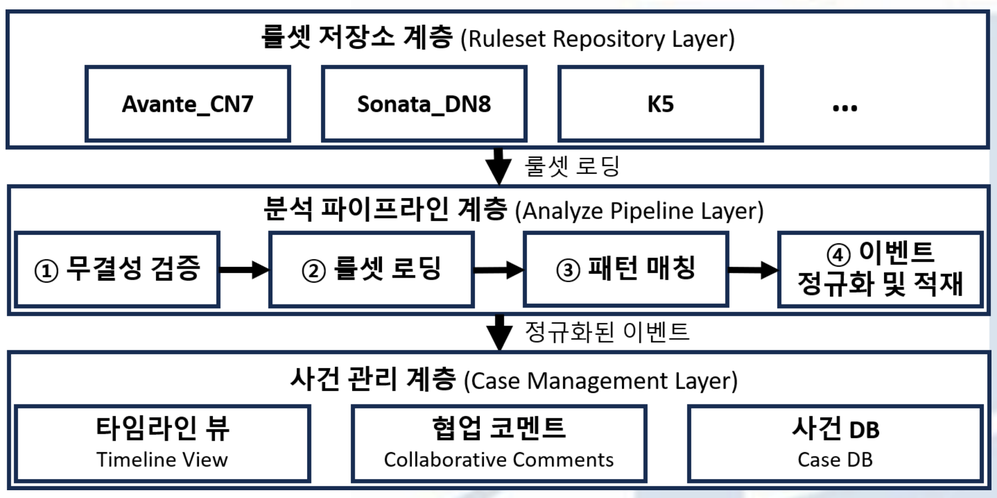
김보겸°[1] · 박수현[2] · 하상우[2] · 조성제[1]
[1]단국대학교 소프트웨어학과, [2]단국대학교 컴퓨터학과
{bogamie, parksh, sangu1115, sjcho}@dankook.ac.kr

1. 서론

- IVI(In-Vehicle Infotainment): 차량 제어·위치·통신 기록을 비휘발성 저장소에 기록 → 교통사고 재구성·운전자 행위 분석의 핵심 증거
- **본 연구의 목표**
  - 국내 차량 포렌식 도구 부재 문제 해결 및 기술 국산화
  - 교차 검증을 위한 Berla iVe 상호 보완적 분석 도구 개발
  - 해시 검증 및 타임라인 가시화로 증거 신뢰성·가독성 향상
  - YAML 기반 룰셋 분리로 차종별 확장성 확보

2. IVI 디지털 포렌식 도구

- **시스템 구조**
  - 룰셋 저장소 계층·분석 파이프라인 계층·사건 관리 계층의 3계층 구조



- **룰셋 저장소 계층**
  - <제조사>/<차종> 디렉터리 구조로 차종별 규칙 분리 보관

  → 분석 파이프라인 수정 없이 추가 룰셋 작성만으로 차종 확장 가능
- **분석 파이프라인 계층**
  - 해시 기반 데이터 변조 여부 검증으로 무결성 확보
  - 분석 과정 중 데이터 조작이 없었음을 증명하여 법적 증거 효력 인정
  - 각 규칙은 로그를 정규화 된 이벤트로 변환하는 5개 필드로 구성

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" → "DoorOpen"
정규화 (normalize)	차종마다 다른 필드 값을 정규화함	event_type: DOOR_OPEN, severity: INFO
요약 (render)	타임라인 요약·상세 문장 생성	"10:23 운전석 문 열림"

- **사건 관리 계층**
  - 타임라인 뷰: 사건 내 이벤트를 시간순으로 정렬해 사건 흐름 가시화
  - 협업 코멘트: 분석가 간 의견 공유·검토로 사건 단위 협업 분석 지원
  - 사건 DB: 추출 이벤트·코멘트를 사건 별로 저장·관리

3. 실험 결과

- **실험 대상 및 분석 범위**
  - 현대 아반떼 CN7PE(7세대) IVI 시스템—Android KitKat 기반
  - 기존 도구: 3개의 로그 파일 종류, 18개의 규칙 수
  - 본 도구: 11개의 로그 파일 종류, 77개의 규칙 수→분석 범위 약 4배
- **처리 성능**
  - 93MB·721개 로그 파일→약 4.2초 내 24,338건 이벤트 추출
  - 추출 이벤트: 차량 정보(차종·VIN·주행거리), 이동 상태, ADAS 동작, 내비게이션 등
- **정규화 후의 표현력**
  - 저수준 로그 표현을 사람이 이해하기 쉬운 표현으로 변환

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 StatusChanged 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

- **추출 신뢰성**
  - 사전 정의된 규칙에 일치하는 이벤트만 정규식으로 추출
  - 추출 결과의 재현성과 정확성 확보
- **타임라인 가시화**
  - 추출 이벤트를 시계열 정렬 → 차량 운행 흐름 직관적 파악

04.11. PM 10:14:32	차량: CN7PE · 주행거리 5803.9km · VIN:**********1315	[Device Information]
04.11. PM 10:14:42	차량 이동: false	[Events]
04.11. PM 10:14:50	차량 이동: true	[Events]
04.11. PM 10:14:59	ADAS · 차로 변경 보조(LCA) 표시등 (값 2)	[Events]
04.11. PM 10:15:03	통신: KT 신호:-64.0dBm	[Events]
04.11. PM 10:15:03	설정된 목적지 주소: 군포시 재궁동	[Navigation Data]
04.11. PM 10:15:17	내비게이션 음성 안내 시작됨	[Navigation Data]

4. 결론

- 차종별 YAML 룰셋·해시 무결성·사건 타임라인 통합 웹 플랫폼 제안
- 현대 아반떼 CN7PE 대상 24,338건 이벤트 자동 추출·가시화
- 분석 파이프라인 수정 없이 YAML 작성만으로 차종 확장
- **한계점**
  - 단일 차종(CN7PE·Android KitKat) 검증에 한정되어, 다양한 제조사·차종·최신 OS로 검증 필요

5. Acknowledgement

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).