

자동차의 블랙박스를 이용한 실시간 포렌식 자료 생성 연구

박대우*, 서정만**

A Study of Using the Car's Black Box to generate Real-time Forensic Data

Dea-Woo Park *, Jeong-Man Seo**

요 약

본 논문은 유비쿼터스 네트워크의 텔레매틱스 기술을 기반으로 자동차에 장착된 블랙박스에 IPv6에 의한 고유한 주소를 부여한다. 블랙박스는 시동 시에 운전자의 인증을 받아 작동하며, 자동차의 주행기록을 영상신호 처리부와 센서신호 처리부로 분석하여 실시간으로 기록한다. 기록된 자료는 유비쿼터스 네트워크를 통하여 암호화 되어 전송되며 도로변의 기지국 센서들을 통해 끊임없는 위치 추적과 이동성 자료를 생성한다. 이 자료는 교통운영관리 센터의 교통기록 데이터베이스에 IPv6 고유주소로 저장된다. 블랙박스를 장착한 자동차가 교통사고나 범죄에 사용된 경우에, 자동차용 블랙박스에서 회수된 코드와 IPv6주소, 교통기록 데이터베이스에 저장된 자료를 비교하여 검증과 인증을 통해 무결성을 확보한다. 이 포렌식 자료는 법정에서 책임소재와 판단의 증거자료로 인정받아 고도식 정보화사회에 편리하고 안전한 인간생활에 기여하게 될 것이다.

Abstract

This paper is based on the ubiquitous network of telematics technology, equipped with a black box to the car by a unique address given to IPv6. The driver's black box at startup and operation of certification, and the car's driving record handling video signals in real-time sensor signals handling to analyze the records. Through the recorded data is encrypted transmission, and the Ubiquitous network of base stations, roadside sensors through seamless mobility and location tracking data to be generated. This is a file of Transportation Traffic Operations Center as a unique address IPv6 records stored in the database. The car is equipped with a black box used on the road go to criminal cases, the code automotive black boxes recovered from the addresses and IPv6, traffic records stored in a database to compare the data integrity verification and authentication via secure. This material liability in the courtroom and the judge Forensic data are evidence of the recognition as a highly secure, convenient and knowledge in the information society will contribute to human life.

▶ keyword : black box, Forensic, Telematics, Ubiquitous security

• 제1저자 : 박대우

• 접수일 : 2008.1.5, 심사일 : 2008.1.10 심사완료일 : 2008.1.24

* 호서대학교 벤처전문대학원 교수, ** 한국재활복지대학 컴퓨터게임개발과 교수

I. 서론

텔레매틱스(Telematics)는 유비쿼터스(Ubiquitous) 네트워크에서 제공되고 있다. 텔레매틱스는 인공위성을 이용한 위치 확인 시스템(GPS)과 지리정보 시스템(GIS)을 자동차에 부착한 전용단말기를 통해 운전자와 사용자에게 길을 안내하고 실시간으로 교통정보를 알려주는 종합정보 시스템이다. 또한 이동통신이나 PDA 등을 이용하여 자동차와 도로변 기지국장치와 차량 간의 무선통신, 그리고 기지국과 기지국 간의 이동단말 사용자의 끊김없는(Seamless) 네트워크[1]의 실시간 연결을 통해 정보를 제공하여 실시간 모바일 인터넷 서비스 산업과 차량 탑재용 ITS 및 LBS로 발전하고 있다.

자동차와 텔레매틱스 서비스는 사람과 화물에 대한 이동성을 제공하는 교통의 필수 수단으로의 긍정적인 측면 외에, 교통사고나 각종 범죄에 사용되어 인간과 사회에 중대한 피해를 유발시키는 부정적인 측면이 있다. 하지만 자동차의 이동 중에 발생한 교통사고나 범죄에 대한 증거자료가 정확하지 않아, 사고와 피해의 책임소재와 법정에서 책임 판단을 위한 법정 증거자료로서 채택에 어려운 단점[2]이 있어왔다.

비행기는 블랙박스를 이용하여, 사고 당시 비행기의 모든 운행상황인, 속도, 고도, 조종사의 음성 등을 저장하여 사고에 데이터를 분석함으로써 사고 원인을 알아내고, 이 자료를 증거로 하여 법적인 책임 소재를 판단한다.

따라서 본 논문에서는 유비쿼터스 네트워크에서 텔레매틱스 서비스를 기반으로 자동차에 장착된 블랙박스[3]에 IPv6의 고유한 주소를 부여하고, 자동차와 함께 이동을 할 때, 기지국과 기지국 간의 센서를 통해 Seamless한 위치 추적과 이동성 자료를 기록한다. 그리고 유비쿼터스 네트워크를 통하여, 운영관리 센터의 교통기록 데이터베이스에 고유주소 값으로 실시간으로 기록된다. 기록 정보 DB는 암호화로 저장되고, 블랙박스를 장착한 자동차가 교통사고나, 범죄에 사용된 경우에 자동차용 블랙박스에서 회수된 코드와 IPv6주소 및 네트워크를 통해 운영관리 센터의 교통기록 데이터베이스에 저장된 자료를 비교하여 검증과 인증[4]을 통해 무결성을 확보한다. 이 자료는 법정에서 책임소재와 판단의 증거자료로 무결성을 갖춘 포렌식 자료로 인정받고자 한다.

본 논문의 연구결과가 텔레매틱스 기술과 유비쿼터스 네트워크와 자동차의 블랙박스를 이용한 편리한 운송과 실시간 멀티미디어 정보교환을 통해, 고도지식정보화사회를 통한 편리한 인간 생활을 창조하는데 기여하게 될 것이다.

II. 관련 연구

2.1. 텔레매틱스

텔레매틱스는 그림 1처럼 통신(Telecommunication)과 정보과학(Informatics)의 합성어로서, 자동차를 기반으로 이동통신, 인터넷, 네비게이션 등이 결합된 자동차에서 사용되는 원격정보 서비스이다. 운송수단인 자동차의 이동 중에 운전자가 무선 네트워크를 통해 차량을 원격 진단하고, 무선모뎀을 장착한 컴퓨터로 교통 및 생활정보, 긴급구난 등 각종 정보를 이용할 수 있으며, 쌍방향 전화 메시지와 음성 이메일 및 오디오북을 다운받을 수도 있다.

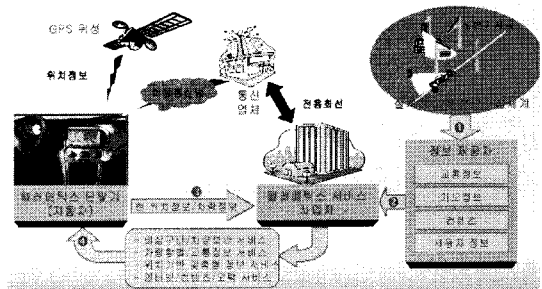


그림 1. 텔레매틱스 개념도
Fig. 1. Telematics key map.

2.2. 자동차 블랙박스의 용도

자동차용 블랙박스는 자동차의 속도, 방향, 브레이크 작동, 자동변속기 제어[5], 안전띠 착용유무 등 데이터의 분석으로 교통사고의 원인을 정확히 판명하며 차량외부 네트워크를 이용하여 교통사고 정보를 경찰, 119구조센터에 자동 통보함으로써 신속한 환자후송, 교통처리 등을 가능케 하는 필수적인 장비이다.

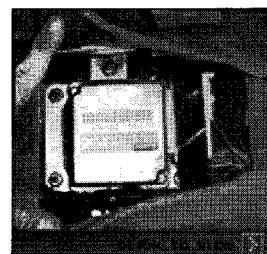


그림 2. 교통사고 자동차의 블랙박스
Fig. 2. Black box in traffic accident car

2.3. 국내 자동차의 블랙박스 장착 현황

국내에서는 2001년 12월 31일자로 도로교통법이 개정되어 40만대 가량의 대형트럭, 버스, 운송사업용 자동차 등은 2002년 7월부터는 운행기록계 설치를 의무화하고, 고장 등으로 사용할 수 없는 경우, 설치하는 하였으나 미작동 등 원래 목적대로 사용하지 아니하는 행위 등에는 범칙금 7만원을 부과하는 한편, 운전자에 대해서는 운전면허 벌점 15점을 부과하고 있다(도로교통법 제48조의 4제 4항, 동법시행규칙 제18조의3)[6]. 현재 우리나라는 1,000여대의 버스 등 상용차량에만 장착되어 이용되고 있다.

산업자원부 기술표준원은 일반 차량에도 블랙박스를 사용할 수 있도록 차량용 블랙박스 국가규격을 2007년 11월 8일 제정 고시하여 자동차의 블랙박스 장착을 기획하고 있다.

2.4. 외국 자동차의 블랙박스 장착 현황

미국 NHTSA[7]는 2007년 6월 발표에서 2008년 9월부터 자동차 제조업체들이 생산하는 모든 차량에 이 장치를 설치하도록 권고한 바 있다. 물론 이 권고안이 의무 사항은 아니지만, 2억대의 경승용차 중 15%가, 그리고 2004년 이후 출시된 승용차의 80%가 블랙박스를 장착하고 있다. 일본의 경우 영업용 차량 4만대, 일반 승용차 2만대 등 6만대의 차량에 블랙박스를 장착함으로써 보편화되는 추세에 있다. 특히 유럽은 2010년부터 모든 차량에 블랙박스를 장착하도록 법률 개정을 하고 있어 2011년부터 4.5톤 이하의 모든 차량에 블랙박스 장착을 의무화하는 것을 추진하고 있다.

표 1. 외국의 자동차 블랙박스를 통한 텔레매틱스 서비스
Table 1. Telematics service through black box of foreign car

자동차업체	통신사업자	서비스 명	서비스 내용
GM	Verzion	OnStar	응급서비스, 원격제어, 경로안내, 도난차량추적, 차량상태 관리
Ford	Sprint	RESCUE	위성라디오방송, 원격진단, 도난추적
Mercedes Benz	AT&T Wireless	TeleAid	주변정보, 자동차 관련정보, 제한된 경로안내
Volvo	Telia	Wireless Car	경로안내, 응급서비스, 교통정보
Toyota	KDDI	Monet	응급서비스, 도난차량 추적
Nissan	NTT Domoco	Compass Link	주변정보, 자동차 관련 정보, 제한된 경로안내

2.5. 자동차 블랙박스 포렌식 자료 채택

뉴욕 법률 저널에 게재된 바에 따르면, 두 명을 차로 친

후 버려두어 사망하게 한 혐의로 기소된 뉴욕 사람 두 명이 재판하는 법정에서 블랙박스에서 추출한 정보가 증거로 사용될 수 있도록 인정한 판례가 있다. 2002년형 시보레 코베트에 설치되어 있던 혐의자들의 차 블랙박스에는 차가 충돌 직전 시속 130마일로 달리고 있었다고 기록되어 있다.

GM은 자동차 블랙박스의 정보를 “▲ 차량 소유자의 동의에 렌터카일 때 임차인의 동의가 있는 경우, ▲ 경찰이나 유사 정부기관의 공식 요청에 응하는 경우, ▲ 법정에서 GM의 변호가 필요한 경우, ▲ 법에 따라 요구되는 경우.”에만 공개하고 있다.

미국 공화당 상원의원 레이 홀름버그(Ray Holmberg)가 제출한 법안(8)은 블랙박스의 데이터는 “▲ 안전 조사나 분석과 관련된 문제를 위해 사용될 때, ▲ 법원의 명령이나 법률에 의해 집행되는 사고 재연과 조사에 필요한 경우.”에만 자동차 소유자를 제외한 다른 사람에 의해 다운로드 될 수 있다’는 것을 분명히 하였다.

또한 컴퓨터 포렌식 자료가 되기 위해서는 블랙박스에서 수집된 데이터라 하더라도 포렌식 소프트웨어의 정확한 동작과정과 평가과정이 필요하다[9]. 이 과정을 거치고 확인된 포렌식 소프트웨어로 블랙박스에서 기록된 자료를 검증할 때에도 테스트의 범위와 실험환경을 명확하게 정의하고 표준 규정에 따라 수행해야 만이 포렌식 자료로서 법정의 판단의 기준이 될 수 있다.

2.6. 국제 및 국내 표준화

텔레매틱스 국제 표준화는 ISO/TC204[10]와 OSGi[11]가 있으며, ISO WG은 WG3 : TICS Database Technology, WG4 : AVI/AEI, WG9 : Integrated Transport Information, Management and Control, WG10 : Traveler and Traffic Information, WG11 : Route Guidance and Navigation System, WG15 : DSRC for TICS Applications, WG16 : Wide Area Communication/Interface and Protocols이고, 차량의 통신부분과 관련 : WG15, WG16, 다른 WG은 텔레매틱스 소프트웨어 측면보다는 콘텐츠 측면의 표준화를 추진 중이다.

OSGi는 OSGi 플랫폼 규격을 개발하기 위한 실무 개발자 모임과 CPEG, VEG, 그리고 MEG의 세 개 그룹으로 구성되어 있고, OSGi가 승인한 우리나라 텔레매틱스의 국제표준안은 “단말 장치 관리 기술, 사용자 정보 관리 기술, 그리고 지불 및 결제”에 관한 것들이다.

블랙박스의 국제표준화는 NHTSA를 중심으로 IEEE P-1616 협의체가 구성되어 있고, UNECE 차량용 블랙박스

의 의무 장착 추진, 차량용 블랙박스 활용 사고 시 자동 통보 체제, eCall도입 추진 및 2010년 EU등록 차량에 대한 eCall장착 의무 장착 및 시스템 구축 을 추진하고 있다. 우리나라에서는 2004년 ISO 국제 표준화 초안 작성, 현재 산업자원부 기술표준원과 TTA를 중심으로 활동하고 있다.

III. 자동차 블랙박스와 텔레매틱스 연계시스템

3.1. 자동차 블랙박스 시스템 설계

자동차 블랙박스를 장착하고 자동차가 시동을 하여 엔진이 움직이면, 운전자와 자동차의 정보가 인증되어 블랙박스가 작동하게 된다. 자동차가 움직이면, 그림 3[12]처럼 자동차의 블랙박스는 인공위성과 링크하여 GPS에서 파악된 위치정보와 함께 운전자의 조작정보를 블랙박스에서 기록하여, 암호화되어 도로변의 무선 기지국 사이에서 링크를 통하여 운영관리 센터의 DB에 전송되어 IPv6 고유주소 별로 기록된다.

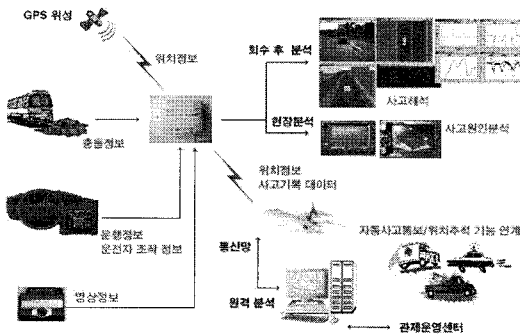


그림 3. 자동차 블랙박스 시스템 설계도
Fig. 3. System design of car black box

3.2. 자동차 블랙박스 작동

그림 4처럼 자동차 블랙박스는 차에 설치된 영상 카메라가 연결된 영상신호 처리부와 차의 부품에 연결되어 반응하는 센서자료를 분석한 신세신호 처리부로 작동되며, 이 자료를 블랙박스에 기록하거나 전송하게 된다.

3.2.1. 사고 감지

사고는 통상적으로 운전석이나 조수석 에어백을 위한 전방 충돌 센서, 측면 에어백 장착 차량은 측면 충돌 센서 등이 사고를 감지하며, 또한 전방 및 측방 가속도 센서를 이용한 충격량 계산방법을 사용한다. 또한 자동감지가 어려운 작은 사

고의 경우는 운전자의 스위치 조작으로 사고감지 기능을 대신 하여 전후 상황의 데이터를 보고 판단 한다.

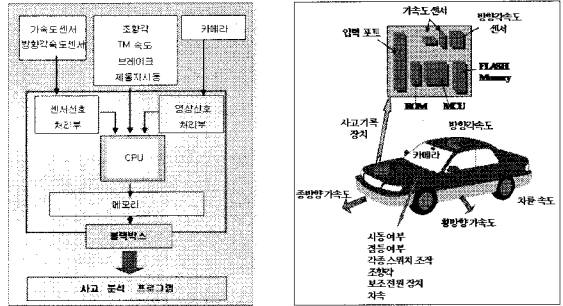


그림 4. 자동차 블랙박스 내부 동작
Fig. 4. Inside action of car black box

3.2.2. 데이터 저장 및 추출

자동차 블랙박스는 그림 5에서 사고 전후의 주행과 관련한 속도, 가속도, 핸들각, 페달 조작 여부, 전조장치의 동작여부 등의 정보를 차에 이미 장착된 센서에서 감지진단모듈[13]을 사용하여 데이터로 저장하고 이를 실시간으로 운영관리 센터의 교통기록 데이터베이스에 저장하도록 전송 하여야 한다.

사고 발생 후, 데이터의 분석을 위한 데이터 추출 시에 전원이 공급되지 않아도 데이터를 보존할 수 있도록 플래시 메모리를 사용한다. 영상데이터를 저장할 때 플래시 메모리는 SRAM, DRAM에 비하여 속도가 느리므로, RAM에 저장한 후 플래시 메모리에 백업을 하고, 영상의 해상도 및 프레임 수를 낮추거나, 압축저장의 방법을 사용한다.

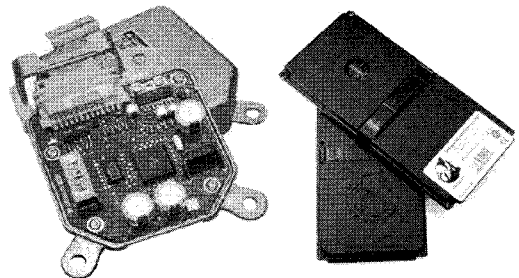


그림 5. 자동차 블랙박스와 저장장치
Fig. 5. Storage on car black box

3.2.3. 데이터 분석

자동차 사고 후, 블랙박스에 저장된 각종 운행 데이터를 사용하여 사고 상황재연 및 분석 또는 운행 행태의 분석을 수행하기 위하여 운영 본부에 데이터 분석 시스템이 요구된다.

이를 위하여 법적인 요건을 갖춘 인증 후에 다운로드 할 수 있는 검증 시스템을 갖춘다.

3.2.4. 주행 경로

자동차 속도, g-포스(g-force), 브레이크 동작 및 급가속 데이터를 기록하면서 자동차가 지정한 임계치[14]를 초과할 때, 센서가 경고음을 내보낸다. 또한 음주 운전 시에 혈중 알콜 농도 이상의 운전자가 자동차의 동작을 할 수 없도록 하는 모듈을 운전대 앞에 장착하고, 졸음운전 시에 감시 카메라가 운전자 행동을 모니터링하여 눈의 크기, 고개의 떨굼 각도, 운전대에 손의 접촉 여부에 따라, 임계치를 초과할 경우에 경고 후에 자동차의 운행이 중지 되도록 할 수 있다.

3.3. 블랙박스 데이터 텔레매틱스 연계

블랙박스를 장착한 자동차가 주행을 시작 하면서 그림 6처럼 텔레매틱스에 링크된다. 자동차의 운행 시에 GPS에 링크 되어 자동차의 위치 파악을 하게 되며, 주행기록과 영상 정보는 암호화되어 도로변 기지국에 실시간으로 전송된다. 이 정보는 유비쿼터스 네트워크를 통해 교통정보 수집망에 의해 전송되며, 이 정보는 IPv6 주소로 교통운영관리센터에 저장된다.

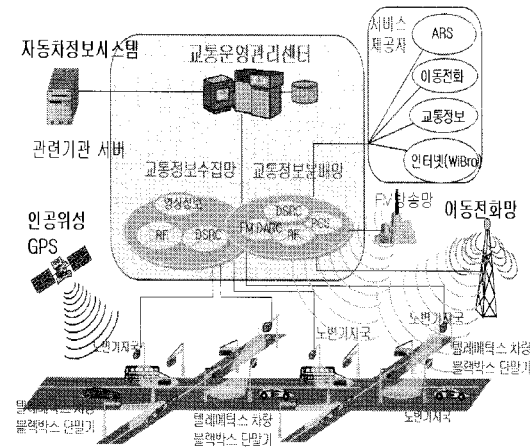


그림 6. 자동차 블랙박스와 텔레매틱스 연계
Fig. 6. Car black box link to Telematics

IV. 블랙박스에서 포렌식 자료 생성

자동차 블랙박스를 통하여 포렌식 자료를 생성하기 위해 자동차에 블랙박스를 장착하고 실험을 하였다. 실험 장비는 HK e-CAR주의 블랙박스[12]인 MOA BOX[12]와 신차 개발용 블랙박스[12], 영상기록 블랙박스[12]를 사용 하였다

으며, 블랙박스를 통해 저장된 자료는 PDA를 통해 교통운영관리센터로 지정된 실험실 서버에 암호화하여 전송하고 기록 저장하는 과정을 실험 하였다.

4.1. 블랙박스에서 운행자료, 영상자료 생성

EF 쏘나타 5인승 승용차에 HK e-CAR주의 블랙박스인 그림 7의 MOA BOX와 신차 개발용 블랙박스, 영상기록 블랙박스 장착하고 작동을 확인한 뒤 실험을 하였다.

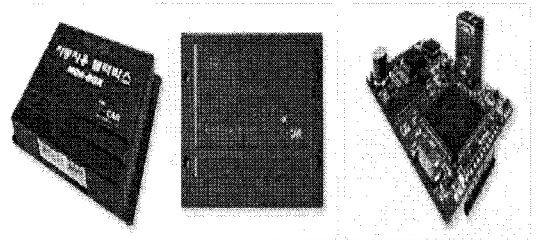


그림 7. 실험에 사용된 자동차 블랙박스 제품
Fig. 7. Car black box product in an experiment

MOA BOX의 주요 기능은 ▲ 사고 자동 인식 기능, ▲ 차량 운행 데이터의 기록 : 차량 운행시간, 운행거리, 최고속도, 평균속도, 급가속, 급제동, 운행 횟수, 시간대별 과속 상황, 공회전, 전조등과 미등의 조작 여부, 위험 운전 여부, ▲ 기록된 운행 데이터의 분석, ▲ 기타 : 자동차사고통보 기능, 긴급구난, 교통 정보 제공 서비스 등을 제공하는 것으로 판단하였다[12].

실험에 사용한 자동차 블랙박스(MOA BOX)의 스펙은 표 2와 같다.

표 2. 실험에 사용된 자동차 블랙박스(MOA BOX) 스펙
Table 2. Car black box(MOA BOX) spec in an experiment

구분	내용
동작 전압	12V, 24V
사이즈	150 X 120 X 30 mm
동작 온도	-30℃ ~ 85℃
보존 온도	-40℃ ~ 105℃
CPU	16 bit
RAM	32 Kbyte
F/ROM	1 Mbyte
영상기능	30 fps
해상도	10 bit
기록 시간	사고 발생 30초전, 사고 발생 15초 후 (30회 총틀까지 기록 할 수 있습니다.)

4.2. 블랙박스에서 자료 전송과 DB 저장

실험용 자동차 블랙박스를 장착하고 USB에 연결된 WiBro 이동단말[15]을 사용한 노트북에서 KTF의 PCMCIA 카드 타입을 WiBro 프로그램이 인스톨된 노트북에 연결하여 WiBro를 통해 실시간 자료 전송이 가능한 것을 확인하고 사용하였다. PDA는 WiBro 기능이 내장되어 있으며, 지상파 DMB가 가능한 이동전화 단말기 형식이다.

▲ 노트북 스펙은 CPU 듀얼코어 2.0GHz, 1GRAM MM, Windows XP, 120GB HDD이다. ▲ PDA의 스펙은 CDMA2000 1x EVDO 방식과 WiBro 802.16e 동시 지원하며, 2G/3G System Soft/Hard Handoff 기능을 가지며, 2.8형 262K Color TFT LCD 채용, 무선인터넷(MagicN) 기능과 E-mail 기능을 지원한다.

자동차 블랙박스를 장착한 차가 주행을 시작하면서 그림 8 처럼 노트북과 PDA의 WiBro는 노변 기지국에 링크된다. 자동차의 운행 시에 PDA의 네비게이션과 GPS 수신기를 통해 실시간으로 자동차의 위치를 파악하여 위치가 정확히 동작됨을 확인 하였다.

자동차의 주행으로 블랙박스를 통해 얻은 주행기록과 영상 정보 및 외부센서 데이터 등의 자료는 PDA를 통해 자료를 확인 하였으며, 노트북에서는 자료를 실시간으로 암호화하여 VPN 기능을 통해 실시간으로 현재의 유무선 네트워크를 통해 전송되었다.

실험실에 설정된 교통운영관리센터 서버에 연결 포트를 설정하고, 방화벽(Firewall)에서 인증을 한 후에 VPN 전송포트를 열어서 자료를 전송 받았고, 자동차 블랙박스 IPv6 주소 디렉토리에 암호화된 자료를 저장하였다.

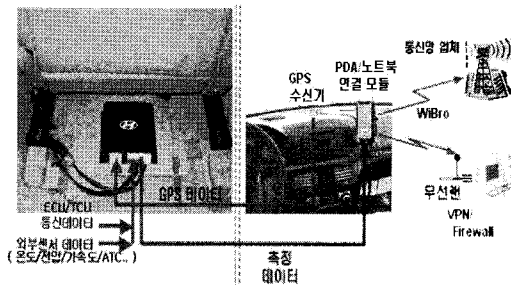


그림 8. 자동차 블랙박스에서 자료 전송 Fig. 8.

4.3. 블랙박스 자료와 DB 자료의 무결성 검증

실험 주행을 마친 자동차에서 블랙박스를 회수하거나, 파손 위험성 전원을 공급하여 기록 자료를 백업 받는데, 현장의 증

거 보증을 위해 블랙박스와 자료저장장치를 봉투에 넣어 밀봉하고 실험실에 가져와 운반 도중에 신뢰성과 무결성이 보존되었음을 확인 한 후에 블랙박스의 저장된 자료를 추출하였다.

실험 차량의 블랙박스에 연결된 노트북과 PDA의 로그 기록과 IPv6 주소를 확인하였다. 그리고 실험실에 설정된 교통운영관리센터의 DB 서버에 IPv6 주소에 저장된 자료를 추출하였다. 블랙박스 회사에서 제공하는 데이터 전송 프로그램을 사용하여 노트북과 PDA에 저장된 데이터를 전송 받았다.

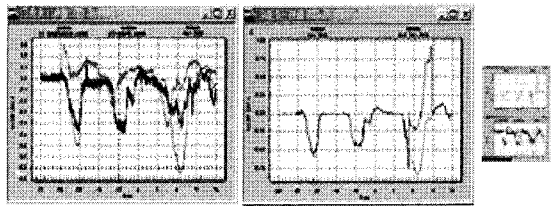


그림 9. 자동차 블랙박스 자료와 PDA에서 전송 자료 Fig. 9. From Car black box data to PDA transmission data

실험 자동차의 블랙박스에서 확인한 자료와 주행기록과 PDA를 통해서 확인한 주행기록이 그림 9처럼 일치하는 것을 확인하였다.

4.4. 포렌식 자료 생성

포렌식 자료를 생성하기 위해 실험용 자동차의 블랙박스의 IPv6 주소를 확인하고, 그림 10처럼 Cain을 통해 출발지와 목적지의 IP 주소를 확인하여 주소가 일치됨을 확인 하였다. 이 주소를 토대로 하여 실험실에 설정된 교통운영관리센터 DB 서버에 암호화된 자료를 복호화 하여 실험용 자동차의 블랙박스의 IPv6 주소를 확인하여 IP 주소가 일치함을 확인하였다. 이로써 동일 IP 주소에서 출발하여 목적지가 같은 동일 자료임을 확인하였다.

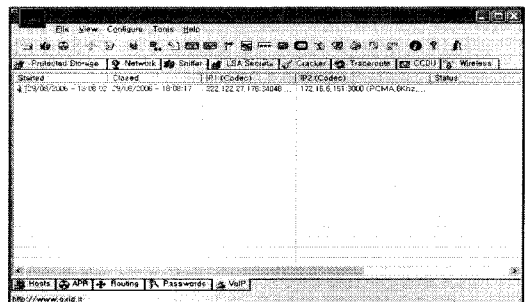


그림 10. Cain에서 IP주소 확인 Fig. 10. Confirmation IP address in Cain

포렌식 자료의 내용에 관한 무결성 검증을 위해 실험용 자동차의 블랙박스 및 실험용 자동차 안의 노트북에 저장된 주행기록과 영상 정보 및 외부센서 데이터와 위치 파악 데이터를 추출하였다. 그림 11처럼 Ethereal을 통해 출발지와 목적지의 IP 주소를 확인하여 주소가 일치됨을 확인하였다.

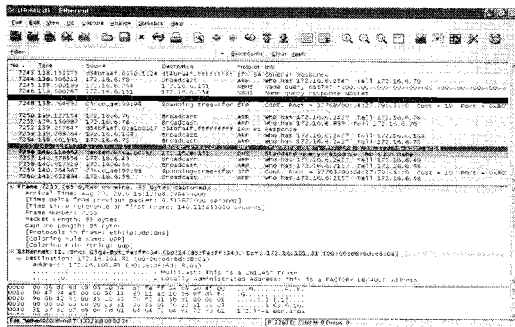


그림 11. Ethereal에서 자료 패킷 무결성 확인
Fig. 11. Data packet integrity confirmation in Ethereal

실험실에 설정된 교통운영관리센터 DB 서버에 암호화된 자료를 복호화 하여 저장된 주행기록과 영상 정보 및 외부센서 데이터와 위치 파악 데이터를 추출하였다.

실험용 자동차의 블랙박스 및 실험용 자동차 안의 노트북에 저장된 주행기록과 영상 정보 및 외부센서 데이터와 위치 파악 데이터는 실험실에 설정된 교통운영관리센터 DB 서버의 자료와 일치함을 확인하였다.

검증 확인 결과, IPv6 주소의 일치, 위치 파악 정보 일치, 주행기록 일치, 영상저장 정보 일치를 확인하여 '이상없음'이라는 무결성 보고서를 작성하였다. 그리고 각각의 데이터에 대한 무결성 확인에서도 '원본과 대조하여 동일함'의 결론을 내어 무결성을 검증하였다.

이상의 실험과정을 거쳐 실험에서 밝혀진 자동차 블랙박스와 블랙박스에서 암호화되어 실시간으로 전송되어 교통운영관리센터 DB 서버에 저장된 기록 자료의 내용은 범정의 증거로서, 채택될 수 있는 포렌식 자료로서 인정되었다.

V. 결론

본 논문에서는 유비쿼터스 네트워크의 텔레메틱스 기술을 기반으로 자동차에 장착된 블랙박스에 IPv6에 의한 고유한 주소를 부여하도록 설계하였다.

자동차에 장착된 블랙박스는 시동 시에 인증을 받아 작동

하며, 영상신호 처리부와 센서신호 처리부는 차가 이동을 할 때 실시간으로 주행기록과 영상기록을 한다. 기록된 자료는 차량이 움직이는 도로변의 WiBro 기지국과 기지국 간의 센서를 통해 끊임없는 위치 추적과 이동성 자료를 생성하고 암호화 되어 유비쿼터스 네트워크를 통하여 실시간으로 전송된다.

교통운영관리 센터의 교통기록 데이터베이스 서버에서는 방화벽의 인증을 받은 포트로부터 VPN 터널링 기법으로 안전하게 IPv6 고유주소의 디렉토리에 저장된다.

주행기록과 영상기록이 저장된 정보는 IPv6 주소별로 저장되고, 블랙박스를 장착한 자동차가 교통사고나 범죄에 사용된 경우에, 자동차용 블랙박스에서 회수된 코드와 IP 주소, 데이터베이스에 저장된 교통기록 등의 자료를 비교하여 검증과 인증을 통해 무결성을 확보한다.

검증된 자료는 무결성을 갖춘 '원본과 대조하여 동일함'의 결론을 내어 포렌식 자료로서 인정되어, 법정에서 책임소재와 판단의 증거자료로 사용되어 고도지식정보사회에 편리한 인간의 생활에 기여하게 될 것이다.

향후 연구에서는, 실제 자동차의 사고 시에 블랙박스와 교통운영관리센터에서 생성되는 주행기록과 영상기록이 실시간으로 분석되면서, 사고에 대한 긴급구조 상황에서 신속한 구조 활동에 적용 될 수 있고, 또한 포렌식 자료가 법적 책임의 판단뿐만 아니라, 사고의 피해를 최소화하면서 예방할 수 있는 능력을 갖추는 고도전문지능화 포렌식 자료의 생성과 현장에서의 적용에 관한 연구가 필요하다.

참고문헌

- [1] 박대우, 박종진, 전문석, "이동단말사용자의 이동패턴 모델 평가에 관한 연구", 제27권 12B호, 한국통신학회논문지, pp1114-1120, 2002, 12.
- [2] Luoma, V. "Forensics and electronic discovery: The new management challenge". Computers & Security, 25(2), pp91-96, 2006.
- [2] 박대우, 임승린, "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구." 한국컴퓨터정보학회논문지, 제11권 제2호, pp44-50, 2006, 5.
- [3] Kowalick, Thomas M, Fatal Exit, The Automotive Black Box Debate, John Wiley and Sons, 2005.
- [4] 김정관, 한명철, 홍금식, 클러치의 독립구동에 의한 자동

변속기의 변속제어. 한국자동차공학회논문집 제8권 제4호, pp. 68~84, 2000. 7.

[4] NHTSA. <http://www.nhtsa.dot.gov> 2007. 11.

[5] 도로교통법시행규칙. 법제처 종합법령정보센터. <http://www.klaw.go.kr/CNT2/LawContent/MCNT2Right.jsp?lawseq=78726> 2008. 1.

[6] Tom Wilsdon. Jill Slay. Validation of Forensic Computing Software Utilizing Black Box Testing Techniques. SCISSEC & Edith Cowan University. 2006.

[7] Ray Holmberg. ROCKY ROAD FOR CAR 'BLACK BOXES' http://www.news.com/Rocky-road-for-car-black-boxes/2009-1041_3-5604449.html CNET News.com, March 9, 2005.

[8] ISO/TC204-Intelligent Transport Systems. http://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/ISO_TC_204_Transport_information_and_control_systems.pdf?nodeid=1166991&vernum=0 2007. 12.

[9] OSGi Technology. http://www.osgi.org/osgi_technology/index.asp?section=2#Standard_Services 2007. 12.

[10] 블랙박스, 신차개발용블랙박스, 영상기록블랙박스-제품 소개. <http://www.hke-car.com/> 2007. 11.

[11] Deawoo Park. "A study about dynamic intelligent network security systems to decrease by malicious traffic". International Journal of Computer Science and Network Security, V.6.N.9B. pp193-199. Sep. 2006.

[12] 박대우, 임승린. "WiBro에서 공격 이동단말에 대한 역추적기법 연구". 한국컴퓨터정보학회 논문지, 제12권 제3호, pp175-184, 2007. 7.

저자 소개



박 대 우

1998년 숭실대학교 컴퓨터학과 (공학석사)
 2004년 숭실대학교 컴퓨터학과 (공학박사)
 2000년 매직캐슬정보통신 연구소 소장,
 부사장
 2004년 숭실대학원 정보과학대학원 정보
 보안학과 겸임교수
 2006년 정보보호진흥원(KISA)
 선임연구원
 2007년 호서대학교 벤처전문대학원
 조교수
 <관심분야> 정보보호, 유비쿼터스 네트워크
 및 보안, Cyber Reality,
 보안 시스템, CERT/CC,
 Forensic, VoIP 보안, 이동통신
 및 WiBro 보안



서 정 만

2003년 충북대학교 컴퓨터공학과
 (공학박사)
 2002년~현재 한국재활복지 대학
 컴퓨터게임개발과 교수
 <관심분야> 데이터베이스, 게임프로그래밍,
 실시간처리