한국항행학회 논문지 제13권 제5호 2009년 10월

임베디드 포렌식 기술을 활용한 차량용 GPS 항법 장치 분석

Applying Embedded System Forensics to Car GPS Navigation System Analysis

이양선*, 박종혁**, 김수균***

Yang-Sun Lee*, Jong-Hyuk Park** and Soo-Kyun Kim***

요 약

최근 몇 년간 전세계적으로 차량 항법 장치 (Car Navigation System)의 사용이 크게 증가하고 있다. 국내의 CNS 구동 방식은 크게 차량 제조업체에 의해 생산되는 하드웨어 기반과 애프터 마켓을 통해 이용할 수 있는 소프트웨어 기반으로 나눌 수 있다. 이중 소프트웨어 기반 차량항법장치는 외부 저장 매체(ex. SD card)에 저장되어 소프트웨어가 실행되므로 분석이 용이한 장점이 있다. 이러한 소프트웨어 중 하나인 Mappy는 한국에서 가장 많이 사용되는 CNS 소프트웨어로, 신속하고 편리한 사용을 위해 자주 가는 장소, 경로 등의 사용자 정보를 외부 저장매체에 저장한다. 이러한 정보를 디지털 포렌식 관점에서 분석하여 용의자의 행위 추적이나 차량의 이동 정보 분석에 이용될 수 있으며 이렇게 분석된 정보들은 유괴, 살인 등의 다양한 범죄를 수사하는데 이용될 수 있어 큰 시사점을 지닌다. 본 논문은 CNS의 외부 저장매체에 저장되어 있는 정보에 대해 디지털 포렌식 관점에서의 분석을 통해 범죄수사에 있어 구체적으로 이용 가능한 정보를 제공한다.

Abstract

It has increased rapidly use of GPS car navigation system in the last few years worldwide. The type of navigation operation is composed of hardware or software. Navigation based on software is stored in exterior storage(e.g. SD card) and executed. One of many navigation software, Mappy, is used most plentifully in Korea. It stores user information such frequently visited place, route and etc. in exterior storage. If it analyzes the dat of navigation, we gain the information such a suspect's movement, route of car. There are important means in a digital forensic perspective because it's available for investigating the crime such kidnapping, murder and etc.This paper provides the necessary information in digital investigation through the analysis of stored data of navigation in a digital forensic perspective.

Key words : Car Navigation System, Digital Forensics, Embedded Forensics

* 조선대학교 정보통신공학과 BK21네트워크임베디드시스템팀 (Dept. of Information Communication Engineering, Chosun Univ.)
** 서울산업대학교(Dept. of Computer Science and Eng. Seoul National University of Technology)
*** 배재대학교 게임공학과(Dept. of Game Engineering, Paichai University)
· 교신저자 (Corresponding Author) : 김수균
· 투고일자 : 2009년 9월 23일
· 심사(수정)일자 : 2009년 9월 24일 (수정일자 : 2009년 10월 23일)
· 게재일자 : 2009년 10월 30일

I. 서 론

초고속 인터넷 시대를 뛰어넘어 유비쿼터스 시대가 도래함에 따라, 수많은 디지털 장치나 임베디드 시스템이 생활 환경에 넘쳐나고 있다. 임베디드 시스템은 컴퓨터와는 다르게 사전에 정의된 특정한 작업만 할 수 있는 기기나 장비를 말한다. 임베디드 시스템의 종류는 PC를 제외하더라도 일상생활에서 사용되고 있는 TV, 냉장고, 세탁기, 전자레인지 같은 전자 가전제품 뿐 아니라 우리가 가지고 다니는 핸드폰, PDA, 홈 관리 시스템, 홈 네트워크 게이트웨이 장치, 밖으로 살펴보면 교통관리 시스템, 주차 관리 시스템, 홈 관리 시스템, 엘리베이터 시스템, 현금 지급기(ATM), 항공 관제 시스템, 우주선 제어장치, 군사용 제어 장치 등 수 많은 제품들이 우리 생활과 밀접하게 붙어서 도움을 주고 있다.

특히 차량 GPS 네비게이션 시스템(Car Navigation System, 이하 CNS)은 특히 괄목할 만한 성장으로 두각을 나타내고 있다. 현재 내비게이션 시장은 일본, 유럽과 북미의 3대 시장을 형성하고 있으며, 일본의 자동차 내비게이션 사용량은 60%에 달하고 유럽과 미국은 25%에 달하고 있다. 추가적으로 현재 중국의 자동차 내비게이션 사용률은 2% 이지만 최근 중국의 신차 시장이 세계 2대 판매시장으로 부상한 것을 감안하면 중국내 GPS시장도 함께 부상할 것이다. 시장조사업체 캐너리스(Canalys)에 의하면 2007년 4월부터 6월까지 3개월 동안 전 세계적으로 740만 개의 내비게이션이 출하됐는데, 이는 2006년 같은 기간에 비해 116% 성장한 수치이며, 이 중 미국은 300%로 가장 큰 성장률을 보였다. 또 다른 조사업체 아이서플라이(iSuppli)는 내비게이션의 치솟는 인기에 힘입어 전체 내비게이션의 출하량이 2012년에는 총 6,510만 개까지 증가될 것이라고 예측하고 있다.

임베디드 포렌식은 디지털 포렌식 분야의 한 종류로 ,임베디드 시스템에 대하여 범죄 사건에 필요한 증거를 수집하여 분석할 수 있도록 소프트웨어나 하드웨어적인 방법을 이용하는 조사 방법이다. 최근의 임베디드 시스템의 다양성에 대응하여 학계에서도 활발한 연구를 통해 새로운 범죄 환경에 대응하고 있다. 이처럼 다양한 임베디드 시스템의 등장은 디지털 포렌식 관점에서 중요한 시사점을 지닌다. 개괄적인 임베디드 포렌식 분야는 크게 임베디드 시스템에 대한 데이터 수집 및 증거 획득, 수집한 데이터에 대한 분석, 안티-포렌식 관점에서 발생할 수 있는 데이터 은닉에 대한 탐지/복구 방안 등으로 크게 나눌 수 있다.

안티 포렌식 관점에서의 임베디드 포렌식은 포함된 플래쉬 메모리나 하드디스크와 같은 저장 장치에 대해, 기존 파일시스템이나 운영체제가 사용하는 파티션 외에 사용자가 추가로 파티션을 생성한 다음 여기에 데이터를 은닉하는 방법이 있다. 또한 일반적인 증거 수집 관점에서는 각 임베디드 시스템의 사용 기록이나 시간 정보를 활용한 타임라인 분석 등에 이용하여 정황 증거를 파악할 수 있는 실마리를 제공할 수 있다. 마지막으로 일반적인 개인 컴퓨터나 데스크탑과 동일한 기능을 가진 임베디드 시스템은 리눅스 운영체제를 설치하여 해킹 시스템으로 변경하여 이용될 수 있으므로, 이에 대한 포렌식 분석 및 증거 획득 기술이 필요하다.

국내 CNS 는 차량 제조업체에서 출하 시 설치되어 있는 장치외에, 애프터 마켓을 이용하여 CNS 시스템을 사용하는 이용자가 대부분이다. 국내에 하드웨어를 제조, 판매하는 업체는 100여개가 넘지만, 국내 CNS의 전자지도 소프트웨어 시장의 90% 이상을 차지하는 엠앤소프트(맵피&지니), 팅크웨어(아이나비), 시터스(루센)등 3사의 소프트웨어를 대부분 탑재되어 판매하고 있다.

본 논문에서는 사용자가 가장 많은 앰앤소프트 사의 Mappy 네비게이션 소프트웨어(이하 Mappy)를 분석하여 포렌식 관점에서 중요한 의미를 지니는 데이터의 수집 및 분석에 대하여 설명한다. 특히 기존에 나와 있는 임베디드 포렌식 기술을 활용하여 법정에서의 증거자료로 가치를 지닐 수 있도록 한다. 2장에서는 디지털 포렌식에서 차량 항법 장치의 중요성을, 3장에서는 CNS 장치에 대한다지털 증거 수집 및 분석 방법론을 다룬다. 4장에서는 이러한 방법론을 적용하여 Mappy 네비게이션 소프트웨어의 데이터를 수집 및 분석한다.

Ⅱ. CNS 시스템의 포렌식 분석 중요성

CNS 소프트웨어에 저장되어 있는 사용자 정보 데이터는 다양한 유형의 범죄 수사에 활용될 수 있다. 특히 용의자로부터 획득한 차량에 CNS 장치가 설치되어 있다면, CNS 소프트웨어로부터 용의자의 이동 경로 및 최근 도착지를 통해 사건 관련 장소나 수색의 범위를 한정할 수 있다. 이렇게 분석된 정보는 유괴나 납치 사건, 테러사건과 같이 사건 관련 장소의 범위를 한정하는데 이용하여 수사에 효과적이고 신속한 대처가 가능하다. 또한 프로파일링 관점에서는 사용자가 저장한 즐겨 찾는 지점들을 통해 주요 행동반경이나 패턴 등을 분석할 수 있다. 저장된 장소 정보를 통해 집이나 회사의 주소를 확인하여 차량의 실제 소유주와 관계를 확인할 수 있다.

다음은 Mappy 에서 지원하는 기능 중에서 디지털 포렌식 수사에 활용 가능한 정보를 나열한 것이다.

● 이동정보

CNS 소프트웨어의 경유구간, 경로설정 등의 기능을 사용하게 되면 특정 출발지에서 목적지까지의 최근 경로 정보가 저장되는데 이 정보에 대한 분석을 통해서 차량의 이동 경로 및 용의자의 이동 패턴 등을 파악할 수 있다. 또한 궤적관리를 통해 사용자의 최근 이동 정보를 자세히 파악할 수 있다.

● 행동패턴

CNS 소프트웨어의 최근 목적지 목록, 검색 목록 등의 정보를 통해 용의자가 주로 가는 장소, 행동반경 등을 파악하여 용의자의 행적을 추적할 수 있다. 또한 '스피드 탐색지 설정' 기능을 제공하는데 이 기능은 실제 차량 소유주가 자신과 밀접한 관계가 있는 집이나 회사 등의 위치 정보를 저장하고 경로 탐색 시 목적지를 쉽게 찾을 수 있게 해주는 기능이다. 이 기능을 통해 용의자의 집이나 회사 등과 같이 밀접한 관계가 있는 주소를 확인할 수 있다.

● 알리바이

CNS에서 저장되는 정보는 크게 두 가지로 분류할 수 있다. 하나는 경로저장을 통해 저장된 경로, 마이포인트와 같이 사용자 본인에 의해 저장되는 정보와 최근검색지명, 경로정보 등과 같이 소프트웨어에서 자동적으로 저장하는 정보가 있다. 따라서 용의자가 일반적인 차량 항법 장치를 사용할 경우, 저장되어 있는 파일에 접근 및 생성, 수정을 하게 된다. 이때 획득한 파일의 시간 정보를 분석하여 사건 발생 시간대에 차량의 이동 경로나 방문 장소 정보를 수집하여 용의자의 알리바이를 검증하는데 도움이 될 수 있다.

그림 1. Mappy United 소프트웨어 실행화면
Fig. 1. Execution of mappy united software

Ⅲ. CNS 장치에 대한 디지털 증거 수집 및 분석 방법론

CNS 소프트웨어인 Mappy는 CNS하드웨어와 결합하여 다양한 기능을 제공한다. 본 논문에서는 CNS에서 디지털 증거 수집의 무결성을 확보하기 위해 Hannay가 제시한 수집절차[1]에 맞춰 진행하였으며 분석절차는 Lim 이 제시한 방법론[3]을 따랐다. 본 논문에서 분석하게 될 소프트웨어는 Mappy United 5.0으로 동일한 제조사에서 개발하여 한국 이외의 지역에서 사용되고 있는 SpeednaviSQ보다 많은 기능을 지원하고 있으나 동일한 회사에서 개발한 소프트웨어이며 현재 SpeednaviSQ의 기능이 Mappy United 5.0 이전의 버전과 유사점이 많기 때문에 SpeednaviSQ의 차후 업데이트 시에는 Mappy United 5.0과 기능적 차이가 없을 것이다.

Mappy에 저장된 정보로는 현재 지정된 경로정보, 궤적 정보, 사용자가 저장한 경로 정보 및 특정 지점, 검색 기록에 관한 정보가 있으며 저장되어 있는 파일

중 위 정보를 저장하고 있는 파일을 대상으로 분석한다. 또한 파일에 저장되어 있는 텍스트 형태는 각 나라별로 차이가 있을 수 있으므로 텍스트 형태 보다는 저장된 정보의 특성에 대해 초점을 맞춰 분석한다.

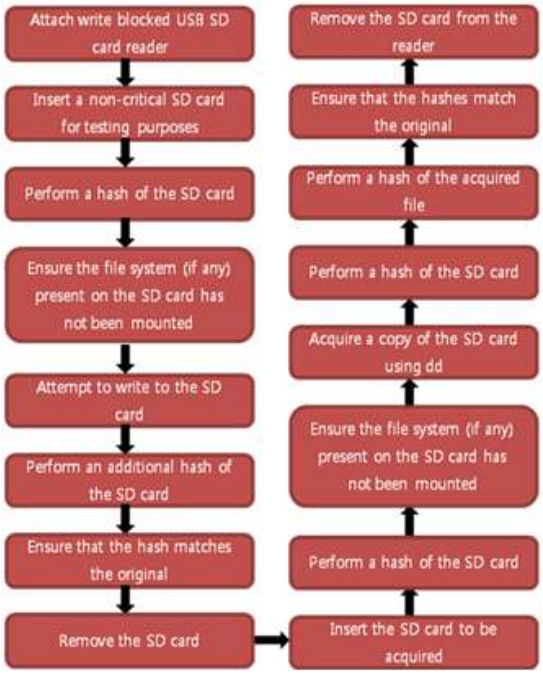

그림 2. CNS 장치에 대한 디지털 증거 수집 절차
Fig. 2. Digital evidence correction procedure in CNS device

3-1 수집 절차

디지털 포렌식의 주목적은 디지털 증거의 추출과 제출시 법정 유효성을 확보하는 것이다. 또한 디지털 증거는 일반 증거의 속성과는 근본적으로 다른 처리 방법이 요구된다[7]. 우선 분석 대상인 SD card의 무결성을 유지를 위한 방법으로 크게 두가지가 있다. 하나는 [그림 3]에 표시 부분을 이용하여 SD card의 쓰기방지장치를 하는 것과 [그림 4]와 같이 쓰기방지 장치가 되어 있는 Write Protect Card Reader를 이용하는 것이다. 이미지 작업은 분석용 복제 증거물을 이용하여 수행하여야 하며 분석용 복제 증거물을 손상시키지 않는 범위에서 수행 되어야 한다. 분석용 복제 증거물의 무결성 유지를 위하여 쓰기방지장치를 사용하고 원본 증거물, 분석용 복제 증거물, 보관용 복제 증거물에 대한 해쉬 값을 획득하여 무결성을 유지한다[7].

Mappy에서 생성된 정보를 획득하기 위해 [그림 2]와 같이Hannay가 제시한 증거 수집 절차에 따라 증거를 수집한다.Mappy United 5.0(이하 Mappy)이 저장되어 있는 SD card(2GB)의 무결성 보존을 위해 쓰기방지장치를 활성화 시키고 AccessData FTK Imager Ver2.4[11]을 이용하여 이미지를 만든다. 실제 분석은 생성된 이미지를 통해 하고 분석시 이용되는 소프트웨어는 EnCase(Ver.4.2)[12] 및 Ultra Edit(ver.14.00)[13], HexWorkshop(ver.5.1)[14]이다.

그림 3. SD 플래쉬 메모리에 쓰기방지 설정
Fig. 3. Write protect of SD flash memory

그림 4. 쓰기방지 기능을 지원하는 플래쉬 메모리 리더기
Fig. 4. Flash Memory reader system for supporting write protect

3-2 분석 절차

Mappy 의 사용자 정보가 저장되어 있는 SD card로부터 무결성이 보장된 증거를 수집한 후 증거 분석을 시작하여야 한다. [그림 5]은 Lim이 제시한 디지털 증거 분석 절차 방안이다. 본 논문에서는 디지털 증거 분석을 수행할 때 위 논문을 바탕으로 분석을 진행하였다. 수집된 Mappy이미지로부터 디렉토리 구조 및 각 디렉토리 내의 파일을 파악하고 각 파일의 포멧과 어떠한 정보를 가지고 있는지 분석한다. [그림 5]에서는 로그 파일 및 메타데이터의 분석을 권고하고 있지만 Mappy에서는 로그파일과 메타데이터를

생성 및 관리하지 않기 때문에 두 과정은 생략한다. 각 파일의 MAC 타임을 분석하여 시스템 사용 정보 및 시간에 따른 사용자의 알리바이를 확인할 수 있다.

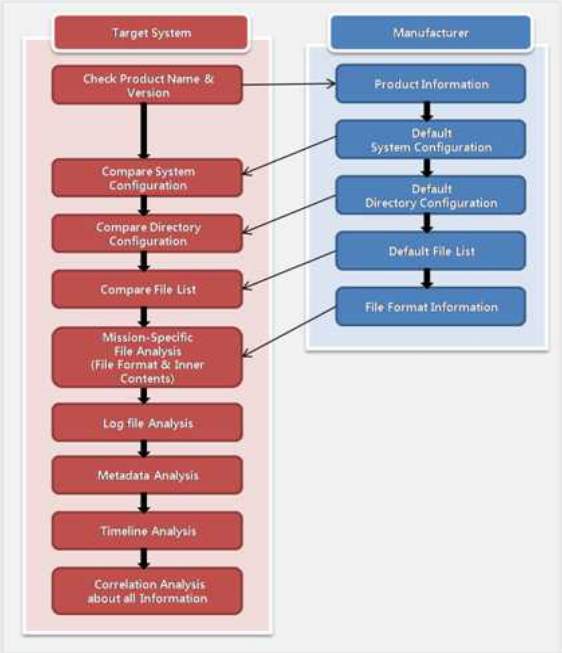

그림 5. 임베디드 시스템에 대한 증거 분석 절차
Fig. 5. Evidence analysis procedure in Embedded system

Ⅳ. Mappy Software 분석

4-1 파일시스템, 디렉토리 분석

Mappy에 사용되는 SD card는 기본적으로 FAT32 파일시스템을 사용하며 한 섹터당 크기는 512Byte이다. Mappy를 이용하는 사용자는 크게 두 개의 파일을 생석하거나 삭제하는데 하나는 두 지점의 경로를 나타내는 rp5파일이고, 다른 하나는 특정 위치의 이름을 나타내는 mpt파일이다. rp5파일 중 current.rp5파일은 현재 사용자가 지정해 놓은 두 지점간의 경로를 표현하는 파일이며 사용자가 목적지에 도착할 경우 자동적으로 경로가 삭제되고 경로에서 이탈했을 경우 현재 위치를 기준으로 재 탐색을 하게 된다. 이때, 이 파일의 생성시간이 변하게 되며 이와 같은 경우 기존 파일에 덮어쓰기가 되지 않고 새로 생성된다는 것을 확인하였다. 또한, 기존 파일의 메타정보는 새로운 파일의 메타정보로 변경된다.

4-1 파일 종류와 분석

Mappy 는 맵 정보가 저장되어 있는 디렉토리(MapData)와 사용자 정보가 저장되어 있는 디렉토리(UserData)로 나누어져 있다. 다음에 나오는 [표1]은 UserData 디렉토리 내에 존재하는 하위 디렉토리와 파일을 보여준다.

표 1. 디렉토리 및 파일 목록
Table 1. Directory and file list

디렉토리/파일명	저장된 정보
./current.rp5	현재 저장되어 있는 경로
./ MyMappy/*.*	사용자 검색한 정보 및 설정 파일
./ MyPoint/위치명.mpt	사용자가 저장한 특정 위치 정보
./ Route/출발지-목적지.rp5	사용자가 저장한 출발지와 목적지간의 경로정보
./ Trace/GPS YYYY-MM-DD Time.pnt	사용자의 궤적 정보

UserData디렉토리 내에는 총8개의 디렉토리가 존재하지만 사용자가 저장한 정보를 가지고 있는 폴더는 CNS소프트웨어의 설정 정보 및 검색 정보를 가지고 있는 MyMappy 디렉토리, 특정 위치에 대해 사용자가 저장한 파일이 있는 MyPoint 디렉토리, 출발지와 목적지간의 경로정보가 저장되어 있는 Route 디렉토리 그리고 사용자가 이동한 궤적이 저장되어 있는 Trace 디렉토리까지 실제 수사에 이용할 수 있는 정보가 있는 디렉토리는 총 4개의 디렉토리로 분류할 수 있다. UserData 디렉토리 내에 있는 파일은 두지점간의 경로정보가 있는 rp5파일, 특정 위치 정보가 있는 mp5파일, 사용자 차량의 궤적 정보가 있는 pnt파일, 사용자의 집이나 회사 등 자주가는 곳의 정보가 저장되어 있는 dat파일, 그리고 사용자가 검색한 이름이 들어가 있는 bin파일까지 확장자 별로 총 5개의 종류로 나눌 수 있다. 본 논문에서는 먼저 사용자가 즐겨찾기로 추가한 지점을 나타내는 mpt 파일에 대한 분석 결과를 설명한다.

확장자가 mpt인 파일은 MyPoint 디렉토리 안에 존재하는 파일로 사용자가 저장한 특정 지역의 정보가

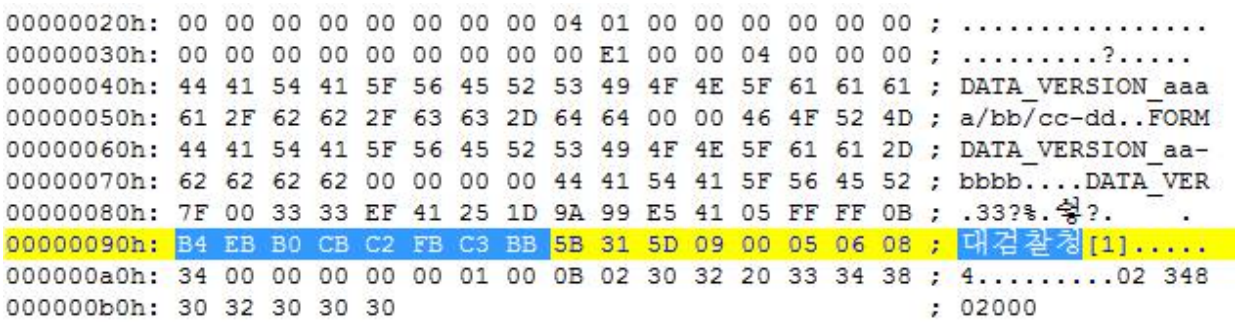

그림 9. Ulatra Edit를 이용한 mpt 파일의 헥사 코드
Fig. 6. Hexa code of mpt file using Ulatra Edit

저장되어 있다. [그림9]는 mpt파일내에 저장되어 있는 값이다. offset 0x90부터 특정 지역의 이름이 저장되고 그 이후에 전화번호 등과 같은 상세 정보가 저장된다. 대부분의 파일이 저장되어 있는 지역 이름으로 파일명이 생성되지만 사용자가 임의로 바꿀 수 있는 만큼 파일명만 보고 판단할 경우 오탐 가능성이 있다.

V. 결론 및 향후 연구

이 논문은 CNS소프트웨어인 Mappy United 5.5을 대상으로 디지털 증거 수집 및 분석 절차를 제시한다. 이러한 절차를 바탕으로 사용자 정보 파일의 특징에 대해 분석하였다. 이 분석을 통해서 CNS는 대부분 자주 가는 장소, 경로 정보 등의 사용 정보를 내부적으로 저장하고 있다는 것을 확인하였으며, 이러한 정보들은 용의자의 행위 추적이나 차량의 이동 정보 분석에 이용될 수 있다. 또한 유괴, 살인 등의 범죄수사에 있어 다양하게 사용될 수 있어 범죄 수사에 중요한 증거 자료로 활용되거나 또한 각각의 데이터 파일의 시간정보를 이용하여 용의자의 알리바이 검증에 이용될 수 있다.

감사의 글

이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (KRF-2008-331-D00580).

참 고 문 헌

[1] Peter Hannay, "A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System – A Research in Progress", *5thAustralian Digital Forensics Conference,* 2007, pp195~198

[2] Beverley Nutter, “Pinpointing TomTom location records: A forensic analysis” *Digital Investigation, Volume 5,* Issues 1-2, September 2008, Pages 10-18

[3] Kyung-Soo Lim and Sangjin Lee, “A methodology for Forensic analysis of Embedded Systems”, *FGCN,* vol. 2, pp.283-286, 2008 Second International Conference on Future Generation Communication and Networking, 2008

[4] 美 내비게이션시장, 폭발적 성장 URL: http://www.globalwindow.org/

[5] 차량용 내비게이션 시장전망 URL: http://www.computertimes.co.kr/news/articleView.html?idxno=3490

[6] KISTI, “아시아 지역, 내비게이션 단말기 이용 활성화 전망”, *글로벌동향브리핑* (GTB), 2008.

[7] 디지털증거 처리 가이드라인, URL : http://cist.korea.ac.kr/~forensic/forensic/dfguideline.php

[8] Write Protect Card Reader, URL: http://www.ics-iq.com/index.cfm/action/product.show/id_product/8207ed2b-2720-49fe-a5df-4b66d3d58fa4/id_category/f1ed34dc-a34d-4088-9784-eb9e011a

7b38
[9] M&Software, Mappy United, URL: http://www.mappy.co.kr/
[10] M&Software, SpeednaviSQ, URL: http://www.speednavi.com/
[11] AccessData, FTK Imager, URL: http://www.accessdata.com
[12] Guidance Software, EnCase Tranning Edition, URL: www.guidancesoftware.com
[13] Ultra Edit, URL: http://www.ultraedit.com
[14] HexWorkshop, URL: http://www.hexworkshop.com

이 양 선(李洋先)

2001년 2월 : 동신대학교 전기전자공학과(공학사)
2003년 2월 : 동신대학교 대학원 전기전자공학과(공학석사)
2007년 2월 : 목원대학교 대학원 IT공학과(공학박사)
2007년 2월 ~ 2009년 9월 : (주)휴메이트 기술연구소 기획팀장
2009년 10월 ~ 현 재 : 조선대학교 정보통신공학부 연구교수
관심분야 : 무선통신시스템, Wireless USN, ITS

박 종 혁(朴鍾爀)

2001년 2월 : 순천향대학교 컴퓨터공학부(공학사)
2003년 2월 : 고려대학교 정보보호대학원 공학과(공학석사)
2007년 2월 : 고려대학교 정보보호대학원 공학과(공학박사)
2002년 12월 ~ 2007년 7월 : (주)한화에스엔씨 기술연구소 선임연구원
2007년 9월 ~ 2009년8월 : 경남대학교 컴퓨터공학부 전임강사
2009년 9월~ 현재 : 서울산업대학교 컴퓨터공학부 조교수
관심분야 : 디지털포렌식, 접근제어, 멀티미디어 보안 및 서비스, 유비쿼터스 컴퓨팅

김 수 균(金修均)

2006년 2월 : 고려대학교 컴퓨터공학과 (이학박사)
2006년 3월 ~ 2008년 2월 : 삼성전자 통신연구소 책임연구원
2008년 3월~현재 : 배재대학교 게임공학과 전임강사
관심분야 : 디지털포렌식, 멀티미디어, 가상현실