디지털 포렌식 관점에서의 아이나비 내비게이션 사용정보 분석

최 용 석[†] · 서 기 민^{††} · 임 경 수^{†††} · 이 상 진^{††††}

요 약

한국의 내비게이션은 크게 하드웨어와 소프트웨어로 구성되어 있다. 이중 소프트웨어 기반 내비게이션은 외부 저장 매체(ex. SD card)에 저장되어 실행이 된다. 이러한 내비게이션은 운전자의 신속하고 편리한 사용을 위해 자주 가는 장소, 경로 등의 사용자 정보를 외부 저장매체에 저장한다. 이렇게 저장된 파일의 데이터나 시간정보를 분석하여 사용자가 등록한 자주 가는 지점을 통해 집이나 회사의 주소를 확인하여 차량의 실제 소유주와의 관계를 확인할 수 있을 뿐만 아니라 사용자의 알리바이를 입증하는데 이용할 수 있다. 따라서 내비게이션에 저장된 사용자 정보를 분석하는 것은 다양한 범죄를 수사하는데 이용될 수 있어 디지털 포렌식적으로 큰 의미가 있다.

본 논문은 디지털 포렌식 관점에서 내비게이션의 외부 저장 매체에 저장되어 있는 사용자 정보의 분석을 통하여 범죄수사에 있어 이용 가능한 구체적인 정보를 제공한다.

키워드 : 디지털 포렌식, 내비게이션, 아이나비

The Analyst of Inavi Navigation user Information by Digital Forensic

Yongseok Choi[†] · Kimin Seo^{††} · Kyungsoo Lim^{†††} · Sangjin Lee^{††††}

ABSTRACT

The operated type of navigation is composed of hardware or software. The navigation based on software is stored and ran in the external storage(e.g. SD card).

For the convenience of users, Many car navigation systems store user information such as frequently visited place, route, and so on. Those can be used to proving the alibi of users as well as their relationship between the actual owner of the vehicle through data and time information analysis.

Therefore, if it is analyzed datas of navigation, we can get a lot of information such as user's movement, route of car. There are important implications in the digital forensics because it's available for investigating the various crimes.

This paper demonstrates the necessary information in the digital investigation through the analysis of stored data in the navigation.

Keywords : Digital Forensic, Car Navigation System, Inavi

1. 서 론

최근 주 5일제 근무의 시행에 따라 여가 생활의 관심이 증가하고, 임베디드 시스템 기술이 발전함에 따라 텔레매틱스 기술이 보편화되고 있다. 특히 자동차에 GPS 내비게이션 시스템을 별도로 구매하여 설치하는 운전자가 크게 증가

하고 있다. 이러한 GPS 내비게이션 시스템은 운전자의 신속하고 편리한 사용을 위해 자주 가는 장소, 경로 등의 사용자 정보를 내부적으로 저장하고 있다. 이러한 정보를 분석하면 특정 차량의 위치 추적해야 하는 경우 기존의 CCTV만을 이용하는 경우 보다 효율적으로 추적 가능하다. 이처럼 내비게이션 소프트웨어의 사용자 정보 데이터를 통해 수집된 증거는 수사에 있어 다양한 경우에 활용될 수 있다. 저장매체에 기록된 파일의 시간정보를 통해 사용자의 알리바이를 입증하는데 이용할 수 있으며 용의자에게 획득한 차량과 내비게이션으로 부터 사용자의 이동경로 및 최근 도착지를 통해 사건과 관련된 장소나 수색의 범위를 한정할 수 있다[2]. 또한 사용자가 등록한 자주 가는 지점을 통해 저장

※ 본 연구는 한국연구재단을 통해 교육과학기술부의 바이오연구개발사업으로부터 지원받아 수행되었습니다(20090084147)

[†] 준 회 원 : 고려대학교 정보경영공학전문대학원 석사과정

^{††} 정 회 원 : 경찰청 사이버테러대응센터 디지털포렌식 분석관

^{†††} 준 회 원 : 고려대학교 정보경영공학전문대학원 박사과정

^{††††} 종신회원 : 고려대학교 정보경영공학전문대학원 교수

논문접수: 2010년 4월 13일

수 정 일: 1차 210년 5월 25일

심사완료: 2010년 6월 3일

된 집이나 회사의 주소를 확인하여 차량의 실제 소유주와의 관계를 확인할 수 있다.

다음은 내비게이션에서 지원하는 기능을 사용함으로써 생성되는 정보 중 디지털 포렌식 수사에 유용한 정보를 분류한 것이다.

• 이동정보

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

최근 목적지 목록, 검색 목록 등의 정보를 통해 용의자가 주로 가는 장소, 행동반경 등을 파악하여 용의자의 행적을 추적할 수 있다. 또한 ‘등록 지점’ 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.

• 시간정보

사용자가 내비게이션을 사용하면 파일이 생성 및 수정되는데 이때 파일의 접근, 생성, 수정시간이 남게 된다. 이때 내비게이션으로부터 획득한 파일의 시간 정보를 분석하면 사건 발생 시간대에 차량의 이동 경로나 방문 장소에 대한 정보를 알 수 있어 용의자의 알리바이를 검증하는데 사용할 수 있다.

현재 국외에서는 TomTom, MAGELLAN과 같은 특정 내비게이션에 관한 연구가 진행 중이다.[11-13] 반면 국내의 경우 제조사 별로 다양한 소프트웨어가 존재하기 때문에 분석의 어려움이 존재하며 사용자 정보 데이터를 디지털 포렌식 관점에서 접근한 연구는 거의 없는 상태이다. 현재 국내에서 내비게이션 소프트웨어를 제조 생산하는 업체가 100개가 넘지만 내비게이션 소프트웨어는 맵피(엠엔소프트)와 아이나비(링크웨어)가 상당수를 차지하고 있다.[10, 16] 또한 두 업체 모두 국내 뿐 아니라 유럽 및 아시아 시장에도 진출하였기 때문에 아이나비나 맵피를 통해 저장되는 사용자 정보를 분석하면 한국뿐만 아니라 다양한 지역에서의 내비게이션에 대해 디지털 포렌식 분석하는데 있어 도움을 줄 수 있다.

기존에 발표한 논문에서는 맵피의 사용자 정보 파일에 대해 중점적으로 분석하였다.[1, 2] 따라서 본 논문에서는 내비게이션 소프트웨어 중 많이 사용되고 있는 아이나비(아이나비 SE 2.0)에서 지원하는 다양한 기능 중에서도 최근 검색 지역 및 경로 정보, 궤적 관리 등의 기능을 통해 남겨지는 사용자의 위치정보를 디지털 포렌식 관점에서 중점적으로 분석한다.

2. 차량항법장치(Car Navigation System, 내비게이션)

2.1 배경지식

내비게이션(Car Navigation System, 차량항법장치)은 현재 위치로부터 목적지까지의 거리 및 교통 상황을 고려하여 선택한 최적의 경로를 안내하는 도로 및 교통정보 제공 시스템이다. 내비게이션은 위성항법시스템의 전파를 받아 현재 위치를 계산하기 위한 수신기(GPS 안테나), 도로 및 경로 정보를 제공하기 위한 전자지도, 도로와 교통 상황을 고려하여 최적 경로를 계산하고 안내하는 소프트웨어, 경로 정보를 화면에 보여주기 위한 정보 단말 및 저장장치 등으로 구성된다.[6]

내비게이션은 차량내의 단말기에 전자지도, GPS, 항법 소프트웨어 등의 기술이 적용된 전자지도상에 운전자의 현재 위치 및 필요시 목적지까지의 최단경로 및 최적경로를 음성으로 안내 받을 수 있을 뿐 아니라 실시간 교통정보를 수신해 쾌적한 운전환경을 제공한다[1].

현재 많이 사용되고 있는 내비게이션은 (그림 1)와 같이 소프트웨어와 하드웨어 부분으로 나눌 수 있다. 하드웨어는 내비게이션을 작동하고 맵과 경로를 사용자에게 제공하기 위한 부분이다.

초기 내비게이션은 대부분 차량에 장착되어 출시되었으며 맵 데이터는 CD에 저장하고 사용자 정보는 내부 저장매체를 이용하였다. 하지만 현재 내비게이션은 시스템 운영 및 업그레이드의 편리를 위해 관리 소프트웨어와 사용자의 내비게이션 이용정보를 외부저장매체인 SD card에 저장해 놓는다. 따라서 본 논문에서는 특정 소프트웨어를 선택하고 그 소프트웨어에 의해 생성되는 사용자 정보 파일이 저장되어 있는 SD card를 주요 분석 대상으로 선택하였다.[1]

내비게이션을 구성하는 소프트웨어는 사용자에게 경로 검색 및 설정 등을 지원하는 어플리케이션 부분과 그 어플리케이션 부분을 동작하게 하는 운영체제, 그리고 실제 내비게이션에서 보이는 맵 데이터로 구분할 수 있다.

특히 어플리케이션 부분은 사용자에게 UI를 제공하는 부분이며 사용자가 이용한 정보를 저장매체에 저장한다. 따라

(그림 1) 내비게이션 단말기 구성도

〈표 1〉 GPS 내비게이션 시장의 구분

구분	Before Market	After Market
구매형태	차량 출고 시 옵션으로 구매	운전자가 별도로 구매하여 설치
설치형태	고정식(Built-in)	고정형, 혹은 이동형

서 이 어플리케이션이 제공하는 기능과 어떠한 정보를 저장 매체에 저장하는지 분석하면 다양한 범죄 수사에 사용가능한 정보를 획득할 수 있다.[3]

2.2 국내동향

‘2008 CES(The International Consumer Electronics Show)’에서 41년 CES역사상 처음으로 자동차 내장기술(In Vehicle Technology) 전시장에 별도 구성되었을 정도로 미국가전협회(CEA)는 2008년 디지털가전에서의 주요 산업 중 하나이다.

현재 내비게이션 시장은 일본, 유럽과 북미의 3대 시장을 형성하고 있는데 일본의 자동차 내비게이션 사용량은 60%에 달하고 유럽과 미국은 25%에 달하고 있다[7]. 시장 조사업체 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 인기로 힘입어 전체 내비게이션의 출하량이 2012년에는 총 6,510만 개까지 증가될 것이라고 예측하고 있다[9].

국내 내비게이션 시장은 1997년에 GPS를 활용한 내비게이션이 도입된 이후에 내비게이션이 옵션으로 장착돼 나오는 고급 차종이 늘어나면서 이른바 비포시장(Before Market)을 중심으로 형성되었다. 하지만 시장의 성장 한계와 고가의 내비게이션 가격 때문에 초기에는 많이 사용하지 않았으나 2003~2004년을 기점으로 50만원 대 이하의 제품들이 본격적으로 출시되면서 기존 차량에 별도로 내비게이션을 구입하여 설치하는 애프터시장(After Market)이 활성화되기

(그림 2) 내비게이션 연간 판매량 및 보급률[5]

시작했다.

애프터시장이 활성화되면서 국내 내비게이션 판매량은 2004년 20만대에서 2005년 60만대, 2006년 120만대, 2007년 145만대, 2008년 140만대에 이르게 되었으며 내비게이션 장착 누적치는 비포시장까지 포함해 2008년 기준 약 500만 대 이상으로 이는 국토해양부가 발표한 지난해 자동차 누적보급대수 약 1,680만 대의 28.28%에 해당한다.[5]

국내 내비게이션 중 텅크웨어에서 개발한 아이나비는 2000년 PDA용 내비게이션 소프트웨어로 개발되었다. 이후 동일 브랜드로 하드웨어를 동시에 제작하여 판매하고 있으며 내비게이션 하드웨어 부문에서는 약 21%로 1위를 점유하고 있다. 따라서 아이나비의 사용자 정보 파일을 우선적으로 분석하면 범죄수사에 많이 활용될 수 있을 것이다.

3. 아이나비 내비게이션 사용 정보 분석

3.1 환경구성

아이나비 ES200의 저장 매체는 2GB의 SD card이며 아이나비 SE v2.0의 실행파일, 맵 데이터, 사용 정보 등을 담고 있다. 실제 주행을 통해 축적된 사용자 관련 정보를 SD card로부터 이미지를 획득하였으며 포렌식 분석도구인 EnCase 6.13을 이용하여 이미지를 분석하였다.

3.2 단말기 정보

〈표 2〉의 ‘RAM’ 부분에 보면 두 내비게이션이 SD card를 저장매체로 이용하는 것을 확인할 수 있다. 분석에 사용된 내비게이션 외에도 대부분 내비게이션이 시스템 및 맵 데이터를 효율적으로 업그레이드 하기 위해 SD card를 사용하고 있다.

〈표 2〉 내비게이션 단말기 정보

Model	아이나비 ES200	XROAD V7 Season2
CPU	AU 1200 500MHz RMI Alchemy	AU 1250 600MHz RMI Alchemy
RAM	SD / MMC card	SD card
Storage	Push -in / Push-out	Push -in / Push-out
GPS	Sirf Star III	Sirf Star III
S/W	아이나비 SE 2.0	Mappy United v5.5
OS	Micosoft Window CE 5.0	Micosoft Window CE 5.0

3.3 주요기능

아이나비SE는 크게 ‘경로검색’, ‘경로관리’, ‘사용자목록’, ‘환경설정’의 4가지 메뉴로 구성되어 있다. 그중 ‘경로검색’을 통해 찾은 지점의 목록, ‘경로관리’에 의해 저장된 경로 및 ‘사용자 목록’에서 저장된 ‘최근목적지’, ‘등록지점’ 등에서 중요 자료를 추출할 수 있다.

3.4 사용자 정보파일

〈표 3〉는 각 저장매체에 저장되는 주요 파일 목록이다.

〈표 3〉 아이나비 주요파일 목록

파일명	파일 내용
GpsPosition	가장 최근의 위치 정보
UserPoint	사용자가 지정한 집의 위치 및 자주 가는 장소
recentgoal	최근 검색 목록
*.inr	사용자가 지정한 경로 저장
routebl	가장 최근에 검색된 경로

아이나비SE는 'iNaviData'라는 단일 폴더 안에 사용자 정보와 관련된 모든 파일이 저장되어 있다. 표에 있는 파일은 사용자가 내비게이션을 사용하면서 생성하거나 수정된 파일이므로 이 파일을 중점적으로 분석해야한다.

3.5 데이터 획득 및 분석

3.5.1 문자 표현 방식

아이나비 SE는 문자열이 (그림 3)과 같이 유니코드로 저장되는 것을 확인할 수 있다.

위와 같이 저장된 데이터의 문자타입을 사전에 확인하면 내비게이션 저장매체에서 추출한 이미지에서 특정 문자열 검색을 효율적으로 할 수 있다.

```

15AC A8B0 EDC5 0000 0000 0000 0000 0000 0000 강남역 . . . .
0000 0000 0000 0000 0000 0000 0000 0000 0000 . . . . .
0000 0000 0000 0000 0100 0000 9068 0200 . . . . .
C22E 0800 1CC1 B8C6 EDC5 0000 0000 0000 0000 □ 서울역 . . .

```

(그림 3) 아이나비 파일의 바이너리 값

3.5.2 아이나비 좌표 값 분석

내비게이션이 GPS 수신기에서 좌표를 받아 현재 사용자의 위치를 맵 데이터에 표시한다. 맵의 맵코드, 아이나비의 아이콘과 같이 각각의 내비게이션 맵에 경로 및 위치를 표시하거나 좌표 정보를 파일에 저장할 때 각 제조사의 내비게이션은 자체적인 인코딩된 GPS 좌표값을 이용한다.

아이나비 내비게이션에서 맵의 특정 지점은 (그림 4)와 같이 x축(0~99999)과 y축(0~99999)의 좌표 값을 가지고 있다.

그리고 아이나비에서 이 좌표 값을 (그림 5)과 같이 'I-CODE'라는 값으로 표기한다.

'I-CODE'는 10자리의 숫자로 표시되며 (그림 5)에서 실선으로 표시된 값이 (그림 4)에서의 x축을 점선으로 표시된 값이 y축을 나타낸다. X1의 자리에 있는 3부터 X5 자리에 있는 8까지 순서대로 나열하면 'I-CODE'의 x축 좌표 값인 36218이 되며 동일한 방법으로 y축 좌표 값은 '67044'가 된다. 그리고 이 값들이 파일에 저장될 때에는 (그림 6)의 체크된 부분과 같이 x축 좌표 값 4바이트(0x4BF8 0200)와 y축 좌표 값 4바이트(0x183F 0800)가 리틀 엔디언 형식으로 저장된다.

파일에 저장된 (그림 6)의 좌표 값을 <표 4>의 수식에 넣고 계산하면 x, y축의 값이 나오고 이 값을 (그림 4)과 같이 나열하면 아이나비 내비게이션에서 확인 가능한 'I-CODE' 값이 나온다. 이렇게 나온 'I-CODE'는 웹에서 맵토피아라는

(그림 4) 아이나비 맵 좌표

(그림 5) I-CODE 표기

```

0E00 0000 0200 0000 78C7 F5AC A5C7 30AE ㅁ . 1 . 인공장기
3CC1 30D1 0000 0000 0000 0000 0000 0000 센터 . . . . .
0000 0000 0000 0000 0000 0000 0000 0000 . . . . .
31C1 81BD 6CAD 2000 48C5 54C5 D9B3 3500 성북구 안암동 5
00AC 0000 0000 0000 0000 0000 0000 0000 가 . . . . .
0000 0000 0000 FFFF 4BF8 0200 183F 0800 . . . . .
0100 0000 3200 3100 3900 2D00 3000 3400 r . 2 1 9 - 0 4

```

(그림 6) 파일에 저장된 I-CODE 값

서비스를 이용하여 쉽게 확인할 수 있다.[17] (그림 7)은 위에서 나온 'I-CODE' 값을 이용하여 맵토피아에서 검색한 위치이다.

이러한 'I-CODE'는 두 지점간의 경로정보를 저장하고 있는 'inr' 파일이나 사용자가 지나온 궤적정보를 저장하고 있는 'locuspos.bin'파일, 내비게이션 최종위치를 저장하고 있는 'GpsPosition.bin'파일 등을 분석하는데 도움이 된다. 또한 아이나비 저장 매체의 이미지 파일만 획득한 경우 또는 획득한 파일의 데이터가 손실되어 아이나비에서 파일을 읽지 못하는 경우 'I-CODE'의 정보를 추출한다면 아이나비나 또는 'I-CODE'를 지원하는 지도서비스에서 지도상의 좌표를 확인할 수 있으며 이 정보를 토대로 사용자가 지나온 경로를 추정할 수 있다.

〈표 4〉 I-CODE변환 식

$$X\text{축 값} = [x / 12] + 14,000$$

$$Y\text{축 값} = [y / 10] + 13,000$$

3.5.3 사용자 정보 파일 분석

3.5.3.1 GpsPosition 파일

'GpsPosition.bin' 파일에는 아이나비 내비게이션이 종료되는 시점의 위치정보가 저장되어 있다. 이 파일은 (그림 8)과 같이 24바이트 크기이며 8바이트 크기의 최종 위치좌표 값이 연속적으로 두 번 저장되어 있는 것을 확인할 수 있다.

이 정보는 내비게이션이 동작 중에 최종 위치좌표 값을 나타내기 때문에 이 파일의 최종 수정시간을 확인하면 해당 시간에 사용자가 어디에 있었는지를 확인할 수 있다.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
20F8	0200	E83E	0800	20F8	0200	E83E	0800	0C00	0000	8700	0000				

3.5.3.2 Locuspos 파일

'Locuspos.bin' 파일은 차량의 이동경로 정보를 가지고 있다. (그림 9)와 같이 처음 10바이트는 이전에 획득한 데이터셋과 동일한 값을 가지고 있으며 33번째 오프셋부터 8바이트씩 좌표 값이 저장된다. 이 파일의 크기는 16032바이트이다. 여기서 헤더 부분의 32바이트를 제외한 16000바이트가 내비게이션의 이동 경로 정보이며 2000개의 좌표 값이 저장된다.

이 파일의 데이터는 실제 차량의 이동 경로를 보여 줌으로써 사용자의 행적을 파악하는데 중요한 정보를 제공한다. 또한 이 파일의 경로 정보와 함께 최종 수정시간을 확인하면 'GpsPosition.bin'보다 상세한 정보를 획득할 수 있다.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
4C	4F	43	55	53	50	4F	53	53	45	00	00	00	00	00	00	LOCUSPOSSE.....
00	00	00	00	01	00	00	00	00	3E	00	00	00	00	07	00	>.....
5F	F8	02	00	C7	3E	08	00	46	F8	02	00	DF	3E	08	00	>.F.....>
31	F8	02	00	FA	3E	08	00	F7	F7	02	00	3C	3F	08	00	1.....>.....<?.....
18	F8	02	00	F0	3E	08	00	F1	F8	02	00	02	3F	08	00	>.A.....?.....

3.5.3.3 Recentgoal 파일

'Recentgoal.bin'파일의 정보는 사용자가 특정 지점을 목적으로 설정하기 위해 검색한 단어들의 집합이다. 이 정보를 통해 사용자가 최근에 방문한 지역을 확인할 수 있다. 이 파일에는 최대 20개의 정보가 저장되며 (그림 10)과 같이 8바이트의 좌표 값과 목적지명이 저장되어 있다.

[illegible]

3.5.3.4 UserPoint 파일

'UserPoint.bin'파일에는 사용자의 집이나 자주 가는 곳 등의 정보가 저장되어 있다. 이 파일의 정보를 통해 사용자의 주 생활반경을 추정할 수 있다.

(그림 11)과 같이 처음 5바이트는 이 파일의 헤더 시그니처이다. 8번째 오프셋의 2바이트는 현재 이 파일에 저장되어 있는 자료의 개수를 의미한다. 12번째 오프셋은 이 파일에 저장된 순서를 나타낸다. 그 다음 사용자가 지정한 지점의 이름과 지점의 행정구역 그리고 ‘아이코드’ 정보가 저장되어 있다.

[illegible]

3.5.3.5 Routetbl 파일

'Routetbl.bin' 파일에는 가장 최근에 설정된 경로 정보가 저장되어 있다. 이 파일은 사용자가 경로 설정 시 생성되며 경로 찾기가 종료되면 자동적으로 삭제된다. 삭제가 되더라도 간혹 일부만 복구가 가능하다. 이 정보를 통해 사용자가 맨 마지막으로 이동한 경로를 파악할 수 있다.

(그림 12)와 같이 파일의 3번째 오프셋부터 5바이트는 다른 테스트 이미지의 Routetbl 파일에도 동일한 값을 가지고 있다. 이 값을 이용하여 삭제된 Routetbl 파일을 복구하는데 이용한다. 그 다음 경로의 시작 지점과 목적지점이 저장되어 있다.

확장자가 'inr' 인 파일은 현재 설정된 경로를 저장한 파일로 현재 생성되어 있는 'Routetbl.bin'의 데이터를 저장한 파일이다. 파일의 구조는 'Routetbl.bin' 파일과 동일한 구조로 구성되어 있다.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
CDFB	B08D	3201	0100	0102	0000	0000	B8C7									U r . .
B902	2678	CE00	8BCA	B902	BA79	CE00	FFFF									i 쉼 馬 i
FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF									
FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF									
FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF									현 위치 . .
0000	0000	0000	0000	0000	0000	0000	0000									
0000	0000	0000	0000	0000	0000	0000	0000									
0000	0000	0000	0000	0000	0000	0000	0000									
24B8	00B3	59D5	50AD	15C8	F4BC	F4BC	30B8									고
0000	0000	0000	0000	0000	0000	0000	0000									려
0000	0000	0000	0000	0000	0000	0000	0000									대
0000	0000	0000	0000	0000	0000	0000	0000									학
0000	0000	0000	0000	0000	0000	0000	0000									교
0000	0000	0000	0000	0000	0000	0000	0000									정
0000	0000	0000	0000	0000	0000	0000	0000									보
0000	0000	0000	0000	0000	0000	0000	0000									호
0000	0000	0000	0000	0000	0000	0000	0000									연
0000	0000	0000	0000	0000	0000	0000	0000									구
0000	0000	0000	0000	0000	0000	0000	0000									원
0000	0000	0000	0000	0000	0000	0000	0000									다
0000	0000	0000	0000	0000	0000	0000	0000									지
0000	0000	0000	0000	0000	0000	0000	0000									탈
0000	0000	0000	0000	0000	0000	0000	0000									포

(그림 12) Routetbl.bin의 바이너리 데이터 1

0000	20F8	0200	E83E	0800	2FF8	0200	D53E	.	1	0	1
0800	3AF8	0200	B23E	0800	3FF8	0200	AA3E	.	1	1	1
0800	5FF8	0200	A13E	0800	67F8	0200	9B3E	.	1	0	1
0800	6CF8	0200	953E	0800	75F8	0200	843E	.	1	0	1
0800	84F8	0200	553E	0800	84F8	0200	483E	.	1	0	1

(그림 13) Routetbl.bin의 바이너리 데이터 2

3.6 삭제된 파일 추출 및 분석

일반적으로 라이브 데이터뿐만 아니라 포렌식 도구를 사용하여 비 할당 영역이나 파일의 슬랙 부분에서 추출해낼 수 있는 정보는 상당히 많다.[3] 내비게이션에도 사용자 정보가 저장되어 있는 파일을 소프트웨어가 삭제할 하였어도 저장매체인 SD card에는 삭제된 데이터가 남아있게 된다. 본 논문에서는 위와 같이 삭제된 데이터를 EnCase 및 Hex Workshop을 이용하여 확인하였다.

3.6.1 Locuspos 파일

위에서 설명한 바와 같이 Locuspos 파일은 차량의 이동 경로 정보를 가지고 있다. (그림 14), (그림 15)는 주행 후 Locuspos 파일의 변화를 보여준다. 두 그림에서 상단에 있는 바이너리는 주행 전에 추출한 Locuspos 파일이며 하단은 약간의 주행 후 추출한 Locuspos 파일이다.

(그림 14)에서는 주행 후 33번째 오프셋부터 8바이트 세 개의 좌표 값이 삭제된 것을 확인할 수 있다. (그림 15)에서는 주행 후 세 개의 좌표 값이 추가된 것을 확인할 수 있다.

주행 전후의 저장매체 이미지 비교 분석 결과 Locuspos 파일의 크기는 16,032바이트로 항상 고정이고 주행 후 저장매체에서 Locuspos 파일의 위치 주소가 바뀌는 것을 확인하였다.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
4C4F	4355	5350	4F53	5345	0000	0000	0000									0123456789ABCDEF
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000	0100	0000	A03E	0000	D007	0000									儼 . . .
0300	0700	0300	0700													L . . .
0300	0700	D711	0300	C4E5	0700											8E L . .
B811	0300	B1E5	0700	9911	0300	9FE5	0700									8E L . .
0000	0000															

(그림 14) 비할당 영역에서 복원한 Locuspos.bin 파일(상)과 현재 Locuspos.bin 파일(하)

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
4DF9	0200	7B3E	0800	33F9	0200	923E	0800									儼 . . .
16F9	0200	A63E	0800	F5F8	0200	B53E	0800									儼 . . .
CEF8	0200	B73E	0800	23F8	0200	123F	0800									儼 . . .
1BF8	0200	323F	0800	1AF8	0200	533F	0800									儼 . . .
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
F5F8	0200	B53E	0800	CEF8	0200	B73E	0800									儼 . . .
23F8	0200	123F	0800	1BF8	0200	323F	0800									儼 . . .
1AF8	0200	533F	0800	4EF8	0200	713F	0800									儼 . . .
6CF8	0200	5D3F	0800	86F8	0200	483F	0800									儼 . . .

(그림 15) 비할당 영역에서 복원한 Locuspos.bin 파일 하단(상)과 현재 Locuspos.bin 파일 하단(하)

Address	i6	Length	i6	Length	i6
00001000	10	0A			
00006000	10	0A			
0000B000	10	0A			
00010000	10	0A			
00015000	10	0A			
0001A000	10	0A			
0001F000	10	0A			
00024000	10	0A			
00029000	10	0A			

(그림 16) 비할당 영역에서의 Locuspos.bin 헤더 시그니처 검색 결과

이번에는 비할당 영역에 존재하는 Locuspos 파일을 추출하기 위해 이미지에서 비할당영역만을 추출하여 Locuspos 파일의 헤더 시그니처를 검색하였다.

그 다음 검색된 시그니처 주소를 기반으로 각각 16,032바이트 씩 추출하여 파일로 만들고 상호 대조작업을 통해 최대한 동일한 정보를 가지고 있는 Locuspos 파일별로 (그림 17)과 같이 결합을 시켰다. 위에서 언급한 바와 같이 Locuspos

(그림 17) 비할당 영역에서 복원한 Locuspos.bin의 결합

로 이제는 단순히 길만 안내하는 내비게이션은 찾아보기 힘들뿐 아니라 하이패스 장치 및 차량용 블랙박스 기능을 탑재한 내비게이션이 출시되고 있을 정도로 기능의 향상뿐 아니라 IT장비로서의 중요성도 점차 늘어나고 있다. 따라서 이제는 단순히 내비게이션에 대한 사용자 정보 분석 외에도 차량용 블랙박스 및 하이패스에 관한 정보에도 주의를 기울여야 한다.

참 고 문 헌

- [1] 최용석, 임경수, 이상진, “디지털 포렌식 관점에서의 차량 항법 장치 분석”, 디지털포렌식연구, pp.1-15, 6월, 2009년.
- [2] 최용석, 임경수, 이상진, “디지털 포렌식 관점에서의 GPS 내비게이션 사용자정보 분석”, 제2회 안티포렌식 기술대응 워크샵, pp.51-56, 8월, 2008년.
- [3] Beverley Nutter, “Pinpointing TomTom location records_A forensic analysis,” Digital Investigation, In Press, Corrected Proof, Available online 26 June, 2008.
- [4] Peter Hannay, A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System, A Research in Progress, 5th Australian Digital Forensics Conference, pp.195-198, December, 2007.
- [5] Mid-Small Cap Brief & Note 2009년 07월 available at :http://flink.hi-ib.com/upload/R_C21/2009/07/%5B28072103%5Dt.pdf
- [6] 전황수, 신돌석, “국내외 내비게이션 시장 및 업체 동향”, 주간 기술동향 통권 1324호, 2007년 11월.
- [7] 내비게이션 시장전망 available at : <http://www.computertimes.co.kr/news/articleView.html?idxno=3490>
- [8] KISTI, “아시아 지역, 내비게이션 단말기 이용 활성화 전망”, 글로벌동향브리핑(GTB), 2008년 04월.
- [9] 美 내비게이션시장, 폭발적 성장 available at : http://www.globalwindow.org/wps/portal/gw2/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4238LYASYGZq6kRhiJgixIH1vfV-P_NxU_QD9gtzQiHJHR0UAQ7UvqA!//delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNEIVRS82X0VfOFBF?nID=6_E_8K8&cID=6_E_8K8
- [10] 박철우, 양희동, “인터넷을 이용한 사용자 혁신: 자동차 내비게이션”, Information System Review 11권, 2009년 2월.
- [11] gpsforensics.org available at : <http://www.gpsforensics.org/>
- [12] satnavforensics available at : <http://www.satnavforensics.com/>
- [13] forensicavigation available at : <http://www.forensicnavigation.com/>
- [14] 아이나비 available at : <http://www.inavi.com>
- [15] 아이나비 ES200 available at : http://www.inavi.com/_Menu/Product/prod_es200_Spec.asp
- [16] 내비게이션 맵, 2장 5중으로 춘추전국시대 available at : <http://kr.aving.net/news/view.php?articleId=83340>
- [17] 아이나비 지도 서비스 available at : http://www.maptopia.com/_Menu/Map/MapMain.asp?InfoIndex=13

최 용 석

e-mail : cyseoks@korea.ac.kr

2008년 세종대학교 컴퓨터소프트웨어학과 (학사)

2008년~현 재 고려대학교 정보경영공학 전문대학원 석사과정

관심분야: 디지털 포렌식, 모바일 포렌식, 데이터베이스포렌식

서 기 민

e-mail : enseo@police.go.kr

2006년 고려대학교 수학전공(이학사)

2009년 고려대학교 정보경영공학전문대학원 정보보호전공(석사)

2009년~현 재 경찰청 사이버테러대응센터 디지털포렌식 분석관

관심분야: 디지털 포렌식, 포렌식 어카운팅, 임베디드포렌식, IT 감사

임 경 수

e-mail : proneer@gmail.com

2006년 부경대학교 컴퓨터멀티미디어공학 (공학사)

2009년 고려대학교 정보경영공학전문대학원 정보보호전공(석사)

2008년~현 재 고려대학교 정보경영공학 전문대학원 박사과정

관심분야: 디지털 포렌식, 디지털 증거수집 프레임워크 설계, 정보보호

이 상 진

e-mail : sangjin@korea.ac.kr

1987년 고려대학교 수학과(학사)

1989년 고려대학교 수학과(이학석사)

1994년 고려대학교 수학과(이학박사)

1989년~1999년 ETRI 연구원

1999년~현 재 고려대학교 정보경영공학 전문대학원 교수

관심분야: 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수