# USIM 포렌식 툴에 관한 연구†

임재윤[O1], 윤승환[1], 임선희[1], 이옥연[2], 임종인[1]
[1]고려대학교 정보경영공학전문대학원
{limdf, schneeleopard, capsunny, jilim}@korea.ac.kr

[2]국민대학교 자연과학대학 수학과
oyyi@kookmin.ac.kr

# A study for USIM Forensic Tools

Jae-Yoon Lim[O1], Seung-Hwan Yun[1], Sun-Hee Lim[1], Ok-Yeon Yi[2], Jong-In Lim[1]
[1]Graduate School of Information Management and Security, Korea University
[2]Department of Mathematics, Kookmin University

**요 약**

정보 통신기술의 발전으로 단말기와 네트워크에 독립적인 부가서비스를 이용할 수 있는 개방형 가입자 인증 카드인 USIM(Universal Subscriber Identification Module) 카드가 이용되고 있다. 모바일 정보기기의 성능 향상으로 다양한 기능이 추가되고 USIM에 저장된 개인정보의 중요성이 부각되어 범죄 도구로 이용될 가능성이 높아 졌으며, 법정 증거자료로서의 중요성도 증가되었다. 모바일 포렌식은 기존의 데이터 저장장치와는 다른 파일시스템을 가지고 있기 때문에 거기에 맞는 전용 포렌식 툴들이 필요하며, USIM과 관련된 범죄가 일어날 때, 자료의 복구와 빠른 검사를 통해 법적 증거화 시킬 수 있는 USIM 포렌식 툴을 요구한다.

본 논문에서는 USIM의 기본적인 구조와 파일시스템을 분석하고 USIM 포렌식 관점에서 증거화 시킬 수 있는 다양한 유형과 절차들을 알아보고, 현재 사용 중인 USIM 포렌식 툴들에 대해 비교 분석한다.

## 1. 서 론

정보통신 기술의 발전으로 모바일 정보기기인 휴대폰에 사용이 보편화되고 휴대폰의 기능이 다양해지면서 휴대폰이 범죄에 사용될 가능성이 점점 더 높아지고 있다. 모바일 정보기기는 노트북, 휴대폰, MP3, PDA, 네비게이션, 카메라 등의 모든 휴대 가능한 디지털 기기를 의미한다. 모바일 정보기기들에 대한 포렌식을 표현할 때, 'Mobile Forensics'이라고 명칭을 사용하거나 각각의 대상에 따라 'Mobile Phone Forensics' 또는 'Cell Phone Forensics,' 'PDA Forensics' 등의 세부적인 명칭을 사용하고 있다. 모바일 포렌식은 기존의 컴퓨터 포렌식에서 그 대상만 달라지는 것이므로 기존의 컴퓨터 포렌식에 대한 정의를 사용하며 증거에 대한 수집, 추출, 보존, 문서화하여 법정에 제출하는 기본적인 포렌식이라고 정의내릴 수 있다[1].

모바일 포렌식의 대상 중에 하나인 USIM은 대용량 및 다기능의 스마트 기능을 갖추고 있어, 다양한 사용자 요구 충족이 가능한 장점이 있다. 가입자 인증을 통한 통신 기능뿐만 아니라 글로벌 로밍 기능과 신용카드, 뱅킹, 증권거래, 멤버십, 결제 등 다양한 금융기능을 제공한다[2].

† "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행 되었음" (IITA-2007-(C1090-0701-0025))

이에 따라 안전한 신원확인 및 인증 등의 정보보호 특성이 강화되었기 때문에 USIM을 활용한 서비스에 관련된 포렌식의 중요성이 크게 대두 될 것이다. 따라서 본 논문에서는 USIM에 저장되는 데이터들에 대한 디지털 증거화 시킬 수 있는 것들을 추출하기 위해서 기본적인 USIM 구조와 파일시스템과 USIM 포렌식 툴에서 추출할 수 있는 디지털 증거의 유형과 절차에 대해 분석하고, USIM에 관한 데이터 복구와 빠른 검사를 하기 위한 USIM 포렌식 툴들에 대해 비교 분석한다.

## 2. USIM의 개요

### 2.1 USIM의 구조

본 절에서는 USIM에 대한 정의 및 파일시스템 구조에 대하여 간단히 설명한다.

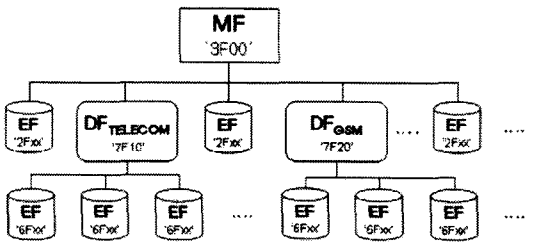
USIM은 스마트카드(Smart Card)의 한 종류로써 ISO 7816-2에 나와 있는 ID-000 규격을 사용하며, 마이크로프로세서(CPU)와 메모리(EEPROM)이외도 운영체제와 필요한 프로그램들이 들어있는 ROM(Read Only Memory)과 마이크로프로세서의 작업공간이라고 할 수 있는 RAM(Random Access Memory)으로 구성된다.

USIM의 규격은 카드리더기와 카드의 물리적인 접촉을 통해 정보를 주고받는 접촉식을 방법을 사용한다. 따라서 접촉식 스마트카드의 규격을 정의하고 있는 ISO/IEC-7816을 비롯한 일련의 규격들은 USIM의 물리적 규격으로 적용되었고 그 중 주요내용은 다음과 같다[3][4].

- ISO/IEC7816-1 : 접점을 가지는 집적회로 카드에 대하여 물리적 특성을 규정
- ISO/IEC7816-2 : COB(Chip On Board) 접점부의 크기와 위치를 규정
- ISO/IEC7816-3 : 접점을 가지는 집적회로 카드에 대하여 전기신호 및 전송프로토콜을 규정
- ISO/IEC7816-4 : 카드와 단말기 또는 시스템 간에 통신을 하기 위한 기본 명령어를 규정
- ISO/IEC7816-5 : 시스템을 개발하는 업체들의 응용 관련 AID(Application Identifier)와 등록번호 RID(Registered application provider Identifier)를 부여 받기 위한 절차 규정
- ISO/IEC7816-6 : IC카드 업체들 간에 응용분야별로 상이한 데이터요소 구현, 호환성 결여 등의 문제점을 보안하기 위한 표준을 규정
- ISO/IEC7816-7 : IC카드 내부의 데이터베이스에 대한 호환 명령어를 규정
- ISO/IEC7816-8 : 보안구조와 관련 명령어에 대한 규정

### 2.2 USIM 파일시스템 구조

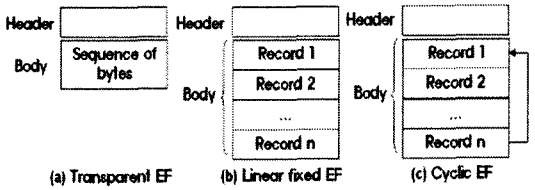
USIM 파일시스템은 계층적 트리구조로 되어있으며, 파일 구조의 루트인 MF(Master File)와 디렉터리 기능 및 다른 데이터파일을 포함하는 DF(Dedicated File)와 파일기능과 데이터를 제공하는 EF(Elementary File)로 구성된다. 기본적으로 위에 설명된 파일 구조들은 2바이트 형식으로 되어있는 파일 ID를 가지고 있으며 파일의 주소를 가리킨다. 또한 파일 ID는 관련 파일이 생성될 때 할당되며 계층구조상 같은 파일 ID를 가질 수 없다.




[그림 1] USIM 파일 구조[5]

DF는 하나의 그룹을 형성하며, 헤더 부분만 가지고 있고 EF는 헤더와 바디부분으로 구성되어 있다. EF는 아래 3가지의 구조를 가지고 있다.

- Transparent EF : 데이터를 포함하는 이진 파일로 구성되어 있다. 모든 데이터의 길이는 헤더에 정의되어 있으며, 이진 명령어들을 통해 파일을 읽고, 쓰고, 수정할 수 있다.
- Linear fixed EF : 레코드 형식으로 구성되어 있으며 데이터 길이가 헤더에 정의되어 있으며, 레코드 명령어들을 통해 파일을 읽고, 쓰고, 수정할 수 있다.
- Cyclic EF : Linear fixed EF와 마찬가지로 레코드 형식으로 구성되어 있으나, 순환적인 구조를 갖고 있는 형식이다. 레코드 명령어들을 통해 파일을 읽고, 쓰고, 수정할 수 있다.




[그림 2] EF의 구조

## 3. USIM 포렌식의 분석

사이버 범죄의 수사과정에서 디지털 증거가 과학적인 접근 방법으로 다루어져야 할 필요성이 제기되면서 포렌식 절차에 대한 기본적인 가이드라인 요구되기 시작하였다.

모바일 포렌식의 기본적인 절차는 컴퓨터 포렌식과 유사하지만 각 절차에 대한 내용은 모바일 정보기기의 특성에 맞도록 만들어 졌다.

미국의 NIST에서는 휴대폰 포렌식 대한 가이드라인인 'Guidelines on Cell Phone Forensics'에서 휴대폰 포렌식의 절차를 보존, 수집, 검사, 분석, 보고서 작성의 5단계로 나누고 있다[6].

### 3.1 USIM에 대한 디지털 증거

다양한 유형의 디지털 증거들이 USIM에 나타나는데 이러한 디지털 증거들은 USIM 파일시스템 내의 EF를 통해서 찾아 낼 수 있다.

예를 들어 서비스 관련 정보나 Phonebook, Call Information, 메시지 정보, 위치정보 등을 찾아 낼 수 있다. 이런 기록들은 수사에서 중요한 증거자료가 되기도 한다[7].

#### 3.1.1 서비스 관련 정보

ICCID(Integrated Circuit Card Identification)는 USIM의 시리얼 번호로 총 20digits로 되어있다. ICCID는 USIM에서 PIN(Personal Identification Number) 코드 제공 없이 읽을 수 있으나, 수정은 할 수 없다.

IMSI(International Mobile Subscriber Identifier)는 UMTS도 해당 서비스 가입 시에 이동 단말기에 최대 15digits까지 할당되는 식별 번호로 되어있다. 이 번호는 MCC(Mobile Conuntry Code), MNC(Mobile Network Code), MSIN(Mobile Subscriber Identifier Number)로 구성된다. MCC와 MNC를 이용하여 전세계 UMTS 망에서 유일하게 식별 가능하게 한다. ICCID 및 IMSI는 가입자와 이동통신사 확인하기 위해 사용된다.

#### 3.1.2 Phonebook과 Call Information

ADN(Abbreviated Dialling Numbers) EF는 핸드폰에서 제공되는 단축 전화번호를 의미한다. 이름과 전화번호를 선정하고 단축번호 지정하여 사용할 수 있다. USIM에서는 최대 100개까지 저장할 수 있다.

LND(Last Numbers Dialled) EF는 휴대폰 장치에 의해 불려진 최근 전화번호 목록을 나타낸다. 최근 전화번호는 이름과 전화번호 구성된다. LND는 Cyclic EF이기 때문에 지원되는 레코드에 필드 수가 초과하게 되면 처음 저장된 최근 전화번호 목록에서 삭제되고 그 자리에 새로운 최근 전화번호가 저장된다.

#### 3.1.3 메시지 정보

사용자가 이동 전화 네트워크를 통해 SMS(Short text message)를 다른 사용자에게 보내면 SMSC(Short Message Service Centre)를 통해 전달된다. SMS 메시지 입력할 수 있는 최대 길이는 160자 이다.

EMS(Enhanced Messaging Service)는 간단한 멀티미디어 메시지를 전달할 수 있다. EMS는 SMS메시지의 내용을 확장시킬 수 있는 방법이다.

#### 3.1.4 위치 정보

LOCI(Location Information) EF는 음성 통신을 위한 위치 지역 정보인 LAI(Location Area Informaion)를 포함한다. LAI는 전화를 끊을 때, USIM과 HLR에 위치가 저장되며 HLR 데이터베이스를 분석하면 마지막으로 등록된 위치 정보를 알 수 있다.

### 3.2 휴대폰 포렌식의 절차

#### 3.2.1 증거 보존

수사는 압수수색 영장과 소유자로부터의 승인과 같은 적법한 허가증을 확보하는 것부터 시작된다. 범죄 현장에 있는 디지털 증거물들을 처해있는 상황에 잘 맞게 판단하여 보존되어야만 한다. 예를 들어 휴대폰은 크게 활성 메모리와 비활성 메모리로 구분되어 지는데, 비활성 메모리는 휴대폰 전원 없이도 데이터가 유지되지만 활성 메모리는 휴대폰 전원이 차단되면 저장된 데이터가 모두 손실 된다. 최대한 증거물을 훼손시키지 않으면서 증거를 분석해야 되기 때문에 그 상황에 맞게 보존 되어져야 한다. 만약 증거물을 올바르게 다루지 않는다면, 물리적인 증거가 훼손되어 증거로써의 가치가 손상된다.

#### 3.2.2 증거 수집

데이터 수집은 이미징 절차, 또는 증거물로부터 정보를 추출해 내는 절차라고 할 수 있다.

USIM의 모델명, 운영체제, 그 외의 특징 등의 정보들을 가지고 어떻게 데이터를 추출해 낼 것인지 결정해야 한다. 현재 사용되고 있는 USIM 포렌식 툴들이 모든 USIM을 분석할 수 있는 것이 아니기 때문에 어떤 포렌식 툴을 사용해야 할 지 결정해야 한다.

#### 3.2.3 증거 검사와 분석

USIM 포렌식 툴마다 지원하는 USIM의 모델이 다르기 때문에 수사관은 모델명에 호환되는 툴을 사용하여 USIM을 분석하게 된다.

USIM 포렌식 툴들을 이용하여 휴대폰 안에 들어가 있는 정보들을 분석을 통해 제조사나 모델명, 이동통신사, 제품 특성, IMSI, ICCID와 같은 데이터를 수집해서 분석해야 한다.

#### 3.2.4 증거 제출

모든 포렌식 절차상 일어난 사항들의 세부적인 요약본을 준비해서 제출하게 된다. 생성된 보고서에는 보통 전문가의 이름, 사건 번호, 날짜, 제목, 증거 사건파일에 대한 정보와 세부적인 분석 결과가 포함된다.

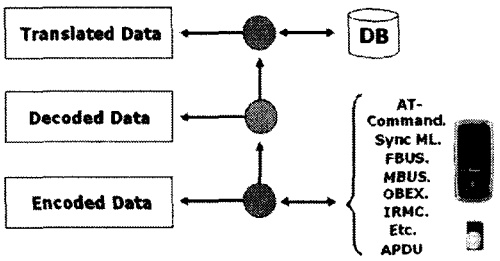
## 4. USIM 포렌식 분석 도구

### 4.1 USIM 포렌식 분석 도구 소개

USIM 포렌식 툴은 휴대폰에 관련된 특정 작업에만 사용되도록 설계되어 있다. USIM 포렌식 툴의 주요 목적은 파일시스템에서 존재하는 디지털 증거를 추출하기 위한 것이다. 증거 취득 외에도 대부분의 USIM 포렌식 툴들은 분석과 보고서 쓸 수 있는 기능을 제공한다. USIM 포렌식 툴에 가장 중요한 특성은 원본 데이터를 변형 없이 완벽하게 추출하는데 있다.

포렌식 툴이 저장장치에서 데이터를 추출하는 방법은 크게 물리적인 방법과 논리적인 방법으로 나누어진다. 물리적인 방법은 메모리 칩 같이 물리적인 저장장치에서 bit-by-bit로 전체 데이터를 복사하는 것을 의미하며, 논리적인 방법은 파일시스템 파티션처럼 논리적인 저장공간에 저장되어 있는 파일이나 디렉터리 같은 데이터를 복사 하는 것을 의미한다[1].

USIM에서 논리적인 방법으로 데이터를 추출하기 위한 대부분의 포렌식 툴들은 아래의 그림 3처럼 동기화 하여 통신하고 디버깅하기 위하여 일반적인 디바이스 프로토콜을 사용한다[6].




[그림 3] 모바일 포렌식 툴의 데이터 처리절차[6]

## 4.2 USIM 포렌식 분석 툴 비교

USIM이 ME(Mobile Equipment)로부터 제거되어 USIM을 읽을 수 있는 적합한 리더기에 삽입되면 외부 장치로부터 보내오는 명령어에 따라서 리셋 작업을 수행하며 리셋 작업의 결과로 USIM의 모델, 제작 회사 등의 정보를 담고 있는 ATR(Answer to Reset) 신호를 외부 장치로 보낸다.

USIM의 데이터를 분석하기 위해서 많은 종류의 포렌식 도구가 사용되고 있지만 이 각각의 분석 도구는 지원하는 대상기기와 기능, 데이터 추출 방법 등이 다르다.

[표 1] USIM 포렌식 툴 기능비교

| 도구 | 대상 기기 | 기능 |
|---|---|---|
| Cell Seizure | - TDMA, CDMA, GSM 휴대폰<br>- SIMs, USIMs | 추출, 분석, 보고서 |
| GSM.XRY | - GSM, CDMA 휴대폰<br>- SIMs, USIMs | 추출, 분석, 보고서 |
| MobilEdit | - GSM 휴대폰<br>- SIMs | 추출, 분석, 보고서 |
| TULP 2G | - GSM 휴대폰<br>- SIMs | 추출, 보고서 |
| Forensic Card Reader | - SIMs | 추출, 보고서 |
| ForensicSIM | - SIMs, USIMs | 추출, 분석, 보고서 |
| SIMCon | - SIMs, USIMs | 추출, 분석, 보고서 |
| SIMIS | - SIMs, USIMs | 추출, 분석, 보고서 |

## 4.3 USIM 데이터의 추출

데이터를 추출하는 단계는 증거물의 정보를 확인하여 휴대폰 단말기의 USIM에서 데이터를 추출하는 단계이다. 데이터를 추출하거나 검사 및 분석하는 과정에서 증거물에 내용이 훼손되거나 수정될 경우 증거로써 가치가 없어지기 때문에 주의해야한다. 데이터 추출하는 과정은 다음과 같다.

### 4.3.1 USIM 카드 데이터 추출을 위한 준비

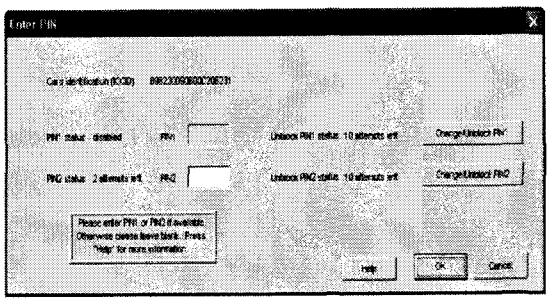
기본적인 USIM 포렌식 툴들은 연결 장치 종류가 크게 적외선, 블루투스, 케이블을 이용해서 PC와 연결한다. PC와 연결시키기 위한 장치 종류를 선택하고 거기에 맞는 드라이브를 설치한다.

### 4.3.2 USIM 포렌식 툴 선택

USIM 데이터를 추출하는데 필요한 툴을 선택해야 한다. 표 1에서 언급한 종류 중 본 절에서는 SIMCon이라는 툴을 이용하여 USIM 데이터를 추출 하도록 한다. SIMCon은 오직 SIM 카드와 USIM을 포렌식 하기 위해 만들어진 툴이다. SIMCon의 기능으로써 디지털 증거 추출, 분석, 보고서작성 등을 할 수 있다.

### 4.3.3 USIM을 PC에 연결

SIMCon 포렌식 툴과 호환되는 리더기를 이용하여 USIM에 데이터를 읽어온다. SIMCon 포렌식 툴을 실행시키면 아래와 같은 화면이 나온다.



[그림 4] PIN 입력

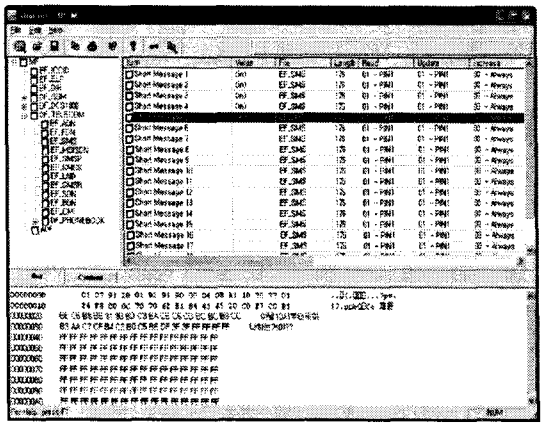
SIMCon 포렌식 툴에 실행 화면을 보면 USIM에 ICCID가 20digits로 표시되고 PIN 코드를 넣을 수 있는 에디터박스가 나온다. PIN 코드는 PIN1과 PIN2로 나누어져 있으며 PIN1은 패스워드가 걸려 있지 않는 상태이고 PIN2는 패스워드가 걸려 있는 상태이다.

PIN2에 패스워드를 2회 이상 틀리게 되면 USIM에 접근이 불가능해 지고 차단된다. PUK(Personal Unblocking Key) 코드는 PIN 코드로 인해 차단된

USIM을 풀어주는 역할을 하며 새로운 PIN 설정을 할 때도 사용된다. PUK1과 PUK2는 패스워드 입력 값을 10번 실패 하게 되면 USIM은 영구적으로 차단되어 재 사용하지 못하게 된다.

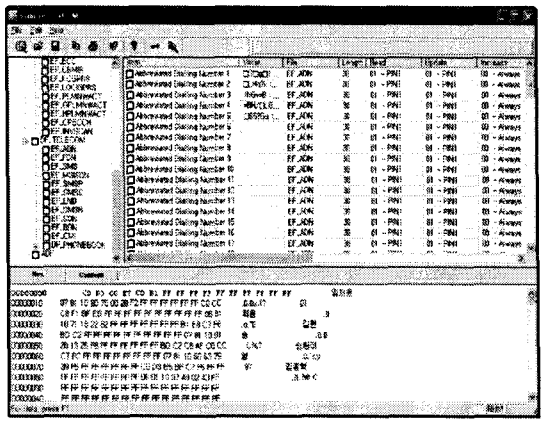
PIN 코드를 입력하여 USIM과의 인증이 완료 되면 USIM안에 있는 약 80개에 파일들이 그림 5와 같이 트리구조로 나타낸다.

80개정도 되는 USIM 파일 중에서 앞에 언급된 USIM에 대한 디지털 증거가 될 수 있는 SMS, ADN, LOCI 부분에 대해 분석한다.



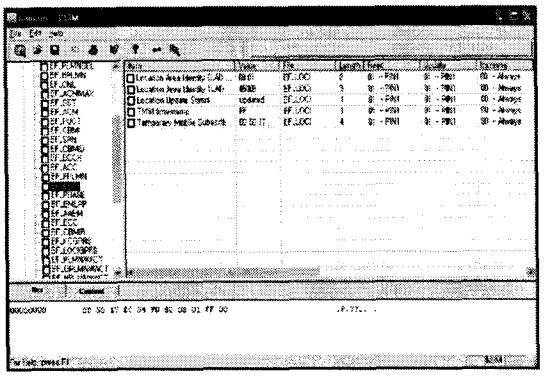
[그림 5] USIM 파일시스템 내용(SMS)

그림 5에는 분석된 USIM 파일시스템 중에 EF_SMS의 내용을 살펴보았다. SIMCon 포렌식 툴은 지워진 SMS도 복구 시킬 수 있다. 또한 송수신된 SMS 메시지가 볼 수 있고 하나의 메시지를 클릭하면 SMS 메시지에 대한 상세한 내용과 송수신된 시간과 전화번호까지 알 수 있다. 또한 EF_SMS의 데이터내용을 핵사 값으로도 볼 수 있다.



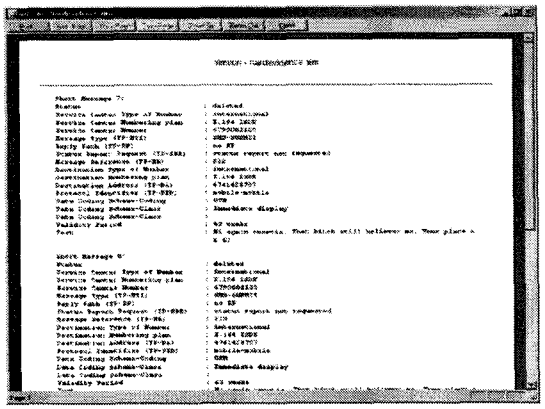
[그림 6] USIM 파일시스템 내용(ADN)

그림 6에는 분석된 USIM 파일시스템 중에 EF_ADN의 내용을 살펴보았다. EF_ADN은 USIM에 지정된 단축 전화번호이다. 위에 그림 6을 보면 단축번호 1번부터 5번까지 입력되어 있는 것을 볼 수 있다. 단축번호를 클릭하게 되면 저장된 사람의 이름과 전화번호를 볼 수 있다.



[그림 7] 위치 정보 내용

그림 7에는 분석된 USIM 파일시스템 중에 EF_LOCI에 내용을 살펴보았다. EF_LOCI안에 들어가는 LAI에 대한 자세한 코드 정보와 TMSI(Temporary Mobile Subscriber Identity)값과 TMSI timestamp 값을 알 수 있었고 마지막 전화를 끊었을 때에 위치 정보도 알아낼 수 있다.



[그림 8] 보고서 결과물[8]

그림 8에서는 사용자가 원하는 디지털 증거 자료들을 결과물 형식으로 만든 것이다.

사용자가 USIM 파일시스템을 선택하여 필요한 부분만 프린터가 할 수 있고 USIM의 모든 종류에 관한 파일시스템도 프린터 할 수 있다. 또한 필요한 파일들을 추출하여 엑셀 파일로 저장할 수 있다.

결과 보고서는 제출용 디지털 증거로 사용될 수 있다.

### 4.4 증거 복구

저장되는 USIM의 모든 자료에는 잠재적으로 증거상 가치가 있을지도 모른다. 일반적으로 USIM 포렌식 툴들은 USIM에 들어 있는 모든 데이터를 복구할 수 있는 것은 아니다. 복구가 가능한 데이터도 포렌식 툴에 따라 다르다. 표 2에서는 복구 가능한 리스트와 USIM 포렌식 툴들을 나타내고 있으며, 복구 가능한 리스트는 O으로 표시 하였다.

[표 2] 데이터 복구 적용범위[7]

| | Cell Seizure | GSM XRY | Mobiledit | TULP 2G | FCR | Forensic USIM | USIMCon | USIMIS |
|---|---|---|---|---|---|---|---|---|
| IMSI | O | O | O | O | O | O | O | O |
| ICCID | O | O | O | O | O | O | O | O |
| MSISDN | O | O | | O | O | O | O | O |
| SDN | O | | | O | | O | O | O |
| SPN | O | | | O | | O | O | O |
| Phase | O | O | O | | | O | O | O |
| ADN | O | O | O | O | O | O | O | O |
| LND | O | O | O | O | O | O | O | O |
| SMS/EMS<br>• Read/Unread<br>• Deleted | O<br>O | O<br>O | O | O<br>O | O | O<br>O | O<br>O | O<br>O |
| LOCI | O | O | | O | O | O | O | O |
| GPRSLOCI | O | | | | | O | O | O |

## 5. 결론

휴대폰의 사용이 보편화되고 기능이 다양화 되면서 휴대폰이 범죄에 사용될 가능성이 높아지고 있다. 휴대폰 안에 들어가는 USIM은 사용자와 이동통신사에 관련된 중요한 데이터를 가지고 있어 범죄에 악용될 가능성이 높다. 그래서 거기에 따른 별도의 모바일 포렌식이 연구되어야 한다. 기존의 모바일 포렌식 툴들의 문제점은 USIM 파일시스템을 핵사 코드로 읽어 왔을 때 문자 부분에 대한 내용이 깨져 보여 데이터 식별에 어려움이 따르고, 또한 PIN 코드를 넣어 SMS나 ADN 등에 데이터들을 임의적으로 수정할 수 있어 거기에 따른 무결성 문제 대해서도 생각해 봐야 될 것이다. 또한 모바일 포렌식 툴들마다 지원하는 휴대폰의 모델들이 다르고 새로운 휴대폰 모델들이 계속 출시되기 때문에 모두 지원 가능한 툴들에 대한 연구가 필요하다.

본 논문은 USIM에 대한 기본적인 구조와 파일시스템을 분석하고 USIM에 대한 모바일 포렌식 관점에서의 절차와 디지털 포렌식 증거가 될 수 있는 USIM 데이터를 설명하였다. 또한 그 데이터를 분석할 수 있는 USIM 포렌식 툴들에 대한 기능들을 비교 분석 하였다.

## 참고문헌


[1] 이경민, "모바일 포렌식을 위한 CDMA 휴대폰의 데이터 추출 및 분석에 관한 硏究," 동국대학교, 2006.

[2] 김민석, "USIM 카드," LG주간경제, 2007.

[3] 인선준, "SIM, UIM과 USIM," 제83호 TTA저널 2002.

[4] ISO. Identification Cards - Integrated Circuit Card with Contacts, "http://www.cardwerk.com/smmartcards/smartcard_standard_ISO7816.aspx"

[5] ETSI TS 100 977 : "Digital cellular telecommunications system(Phase 2+) Specification of the Subscriber Identity Module - Mobile Equipment(SIM-ME) Interface (3GPP TS 11.11 version 8.14.0 Release 1999)," Technical Specification), 2007.

[6] Wayne Jansen and Rick Ayers, "Guidelines on Cell Phone Forensics," NIST, Draft Special Publication 800-101, 2006.

[7] Wayne Jansen and Rick Ayers, "Forensic Software Tools for Cell Phone Subscriber Identity Modules," Computer Sercurity Division - 893, 2006.

[8] SIMCon, "http://www.simcon.no"