TTA Standard

정보통신단체표준
TTAx.xx-xx.xxxx/R1

제정일: 200x 년 xx 월 xx 일
개정일: 200x 년 xx 월 xx 일

휴대폰 포렌식 가이드라인

(Guidelines on Cellular Phone Forensics)

TTA 한국정보통신기술협회
Telecommunications Technology Association

정보통신단체표준(Tab|↔|)
TTAx.xx-xx.xxxx/R1(Tab|↔|)

제정일 : 200x 년 xx 월 xx 일
개정일 : 200x 년 xx 월 xx 일

휴대폰 포렌식 가이드라인

(Guidelines on Cellular Phone Forensics)

TTA 한국정보통신기술협회
Telecommunications Technology Association

서 문

1. 표준의 목적

본 표준은 휴대폰 내에 저장되어 있는 디지털 증거를 수집, 분석, 보관함에 있어 필요한 절차와 준수사항을 정의하는데 목적이 있다.

2. 주요 내용 요약

본 표준의 주요내용은 휴대폰으로부터 수집 가능한 디지털 증거물들을 정의 및 분류하며, 분석 방법 및 보관 방식을 포함한다. 또한 수집, 분석, 보관의 과정이 적법한 절차로 이루어질 수 있도록 표준 가이드라인을 제시한다. 본 표준 가이드라인을 통해 증거물의 무결성을 보장함과 동시에, 적법한 절차를 통해 디지털 증거물을 취급할 수 있는 방안 및 조사 행위를 정립한다. 본 표준에서는 휴대폰으로부터 수집할 수 있는 디지털 증거물은 전자적인 증거 외에, 휴대폰 연결 장비 및 기타 관련 장비들을 포함한다. 이와 함께 디지털 증거물에 대한 보관 방식과 휴대폰 포렌식 도구의 개발 및 발전 방향을 제시한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 표준은 휴대폰에서 디지털 증거를 수집, 분석, 보관하는 원칙과 절차를 제공함으로써, 휴대폰과 관련된 디지털 증거 취급을 다루는 각종 조사 및 수사 행위의 체계화, 표준화를 유도하여, 그 결과인 디지털 증거의 신뢰성을 확보할 수 있도록 한다. 또한 휴대폰의 데이터 수집, 분석용 도구 개발에 활용할 수 있다.

4. 참조 표준(권고)

4.1 국외표준(권고)

- 해당사항 없음

4.2 국내표준

- 해당 사항 없음

5. 참조표준(권고)과의 비교

5.1 참조표준(권고)과의 관련성

- 해당 사항 없음

5.2 참조한 표준(권고)과 본 표준의 비교표

- 해당 사항 없음

6. 지적재산권 관련사항

본 표준과 관련하여 2007 년 6 월 현재까지 확인된 지적재산권 없음.

7. 적합인증 관련사항

7.1 적합인증 대상 여부

- 해당사항 없음.

7.2 시험표준제정여부(해당 시험표준번호)

- 해당사항 없음

8. 표준의 이력

판수	제/개정일	제.개정내역
제1판	2007.00.00	제정

Preface

1. The Purpose of Standard

This standard aims to establish procedure and compliance of digital evidence collection, analysis, preservation for investigator, researcher and analyzer in cellular phones.

2. The summary of contents

This guide defines and classifies digital evidence of cellular devices, and then it suggests analysis procedures and methods of custody. It is proposed guideline which can be guaranteed integrity of evidence and lawful collection, analysis, preservation of digital evidence. This standard defines procedure of digital evidence and activities for investigator, researcher and analyzer. It is collected not only cellular device but also cellular connector and other digital device in this guideline. This guide also suggests collection procedure of digital evidence and digital forensic techniques for preservation.

3. Applicable fields of industry and its effect

This guide provides procedures and principles of acquisition, analysis and preservation of digital evidence for investigation. Examination that is related to treating digital evidence of cellular phones is expected to be standardized and organized. So reliability of digital evidence is ensured. In addition, this guide is able to develop forensic tools for cellular phone to collect and analyze.

4. Reference Standards (Recommendations)

4.1 International Standards (Recommendations)

- Not applicable

4.2 Domestic Standards

- Not Applicable

5. Relationship to Reference Standards(Recommendations)

5.1 The relationship of Reference Standards

- Not applicable

5.2 Differences between Reference Standard(recommendation) and this standard

- Not applicable

6. The Statement of Intellectual Property Rights

- Not applicable

7. The Statement of Conformance Testing and Certification

- Not applicable

8. The History of Standard

Edition	Issued date	Contents
The 1st edition	2007.00.00	Established

목 차

Contents

휴대폰 포렌식 가이드라인

Guidelines on Cellular Phone Forensics

1. 개요

현재 휴대폰 가입자는 2007년 5월말 현재 약 4천 2백만 명에 이른다. 즉 성인 1인당 적어도 한 개의 휴대폰을 소유하고 있음을 의미한다. 휴대폰에는 기본적인 통화기능 외에 문자 메시지(SMS), 카메라, 일정관리 기능 등이 포함되어 있어 상당히 많은 개인 정보를 저장하고 있다. 따라서 휴대폰에 저장되어 있는 데이터에 대한 분석은 수사에 있어 중요한 증거로 활용될 수 있다.

휴대폰 포렌식은 휴대폰에 대해 적법한 기법을 활용하여 저장되어 있는 디지털 데이터의 수집, 분석, 보관을 위한 기술을 의미한다. 최근 휴대폰의 기능이 다양해지고 이에 따라 더 많은 개인 정보가 저장됨으로 인해 휴대폰에 대한 분석의 중요도는 나날이 증가하고 있다. 그러나 휴대폰은 데스크톱 컴퓨터나 노트북 컴퓨터와 달리 운영체제, 파일시스템, 데이터 형식 등과 같은 표준이 존재하지 않는다. 휴대폰의 하드웨어 인터페이스는 현재 표준으로 되어있지만 이는 배터리 충전을 위한 표준이며 PC와의 데이터 전송을 하는 경우에는 제조사와 모델에 따라 개별적인 프로토콜을 이용한다. 따라서 실제 휴대폰에 대한 데이터에 대한 접근이 용이하지 않아 수집 및 분석에 어려움이 있다.

현재 휴대폰에 저장되어 있는 데이터를 수집하기 위한 방법은 크게 물리적 수집방법과 논리적 수집방법으로 구분할 수 있다.

물리적 수집방법은 플래쉬 메모리의 내용을 직접 수집하는 방법과 JTAG과 같은 표준 인터페이스를 활용하는 방법으로 다시 나눌 수 있다. 휴대폰의 플래쉬 메모리의 내용을 직접 수집하는 방법은 휴대폰의 기판에서 메모리를 떼어 내어 메모리 리더기를 이용하여 수집하는 방법으로 포렌식 관점에서 가장 바람직하다고 할 수 있다. 그러나 휴대폰의 메모리 종류에 따른 별도의 수집 장비를 제작해야 하고 기판에서 메모리를 분리하는 과정이 필요하므로 휴대폰을 손상시킬 수 있다. 따라서 휴대폰이 손상되어 정상 작동을 하지 않는 경우를 제외하고는 사용하기에 어려움이 있다. JTAG과 같은 표준 인터페이스는 휴대폰 제조회사에서 휴대폰을 개발하는 과정에서 사용된다. 표준 하드웨어 인터페이스를 활용하는 방법은 휴대폰의 CPU에 직접 명령을 전송하여 메모리를 전송하도록 한다. 휴대폰의 메모리를 분리할 필요가 없어 손상을 주지 않고 실제 메모리를 이미징 할 수 있으므로 휴대폰의 메모리에 저장된 증거를 수집하기에 가장 바람직한 방법이라 할 수 있다. 그러나 인터페이스에 대한 정보가 공개되어 있지 않고, 제조사와 제품모델에 따른 별도의 케이블을 제작해야 하는 어려움이 있다.

물리적 수집방법은 하드디스크 이미지를 얻는 것과 동일하게 휴대폰의 메모리 이미지를 얻을 수 있으므로 지향되어야 하는 수집방법이다. 그러나 현실적인 적용에 어려움이 있으므로 필요에 따라서는 논리적인 수집 방법이 수반되어야 한다. 논리적인

증거 수집방법은 파일전송 프로토콜을 이용하는 것과 제조사의 PC 소프트웨어를 이용하는 방법으로 구분할 수 있다. 파일전송 프로토콜을 이용하는 방법은 휴대폰에 저장되어 있는 개별파일에 대해 파일전송 명령을 주어 해당 파일을 PC로 다운받는 것이다. 다운받은 파일은 논리적으로 휴대폰의 파일과 동일하며 휴대폰의 종류에 따라 지워진 통화기록, 문자메시지를 얻을 수 있다. 그러나 파일 자체가 삭제되었을 경우 확인을 할 수 없다는 단점이 있다. 마지막으로 제조사의 PC 소프트웨어를 사용하는 방법은 위의 3가지 경우를 활용할 수 없는 경우에 사용되어야 한다. 제조사에 따라 다른 소프트웨어를 이용하여 데이터를 수집하며 제조사 소프트웨어의 데이터 가공방식에 따라 다른 형태의 데이터를 볼 수 있다. 일반적으로 지워진 정보는 알 수 없으나 모든 휴대폰에 대해 사용이 가능하다는 장점이 있다.

본 가이드라인은 휴대폰에 저장되어 있는 증거에 대해 적법한 절차 관계 등을 포함한 수집 기술과 고려사항들을 제시한다. 휴대폰은 음성 통신 및 문자 메시지 이외에도 다양한 기술 및 운영적인 특성을 사용자에게 제공하고 있다. 따라서 휴대폰을 통해 획득할 수 있는 증거에 대해 기술하고, 상황에 따라 수사관이 적절한 기법을 적용할 수 있도록 휴대폰 증거 수집을 위한 사전준비, 초기 대응, 데이터 수집, 조사, 분석 및 보고서 작성 절차에 대해 제시한다. 또한 현재 휴대폰 포렌식을 위한 도구에 대한 기본 명세가 매우 부족하다. 따라서 본 가이드라인에서는 디지털 포렌식의 도구가 갖추고 있는 사항을 포함하여 휴대폰 포렌식을 위한 도구가 갖추어야 할 기본적인 사항들에 대해서 설명한다.

2. 표준의 구성 및 범위

본 가이드라인에서 다루는 휴대폰은 이를 연결하는 전자 장비 및 디지털 증거물 수집 장비를 포함한다. 본 가이드라인은 국내에서 사용하고 있는 CDMA/WCDMA 방식의 휴대폰을 대상으로 하며, 유럽에서 사용되는 GSM 방식에 대해서는 적용되지 않는다.

본 가이드라인은 휴대폰 포렌식을 위한 디지털 증거물을 수집, 분석, 보관하는 표준 절차를 제시하며, 이를 활용할 수 있는 표준 수사 방안 제시를 범위로 한다. 또한 적법한 휴대폰의 분석 방법과 디지털 증거물 수집 방식, 보관 방안을 정립하며, 국내 환경에 적합한 휴대폰 포렌식 수사 가이드라인을 제시한다. 본 가이드라인은 향후 개발될 휴대폰 포렌식 도구에 대한 기본 사양을 제시한다.

3. 정의

3.1 용어 정의

가. 디지털 증거

:휴대폰, 컴퓨터, 기타 디지털 저장매체 등에 저장되어 있는 증거자료로써, 네트워크를 통해 전송 중인 자료를 포함하며, 포렌식 조사 및 수사 업무에 필요한 증거자료.

나. 디지털 증거 분석

:휴대폰, 컴퓨터 등과 같은 디지털 저장매체(네트워크를 통해 전송 중인 자료를 포함)에 남아있는 자료에 대한 원본 보존과 사건 관련 증거를 과학적인 절차를 통하여 추출, 검증, 판단하는 조사 및 수사과정.

다. 휴대폰 포렌식

:휴대폰에 대해 적법한 절차를 수행하여 디지털 증거를 수집하는 기술.

라. 휘발성 증거

:디지털 기기의 실행 시에 일시적으로 메모리 또는 임시파일에 저장되는 증거로써, 네트워크 접속상태, 프로세스 구동상태, 사용 중인 파일 내역 등과 같이 시스템 종료와 함께 사라지는 디지털 증거

마. 비휘발성 증거

:디지털 기기 종료 시에도 저장매체에 삭제되지 않고 남아있는 디지털 증거

바. 기타 디지털 저장매체

:플로피 디스크, 휴대폰, USB, 플래쉬 메모리 등 컴퓨터 하드디스크 외의 디지털 저장매체

3.2 약어

CDMA	Code Division Multiple Access
CPU	Central Process Unit
GSM	Global System for Mobile communication
JTAG	Joint Test Action Group
MSI	Mobile Subscriber Identity
MMS	Multimedia Messaging Service
PC	Personal Computer
PIM	Personal Information Management
PIN	Personal Identification Number
PUK	PIN Unlocking Key
SMS	Short Message Service
USB	Universal Serial Bus
WCDMA	Wideband Code Division Multiple Access

4. 디지털 포렌식 개요

4.1 디지털 포렌식 원칙

범죄 현장에 도착을 하면 우선적으로 실시해야 할 것은 현장보존이다. 각 포렌식 수사 단계마다 안전함이 보장되고 잠재적인 증거에 대한 무결성이 보장되어야 하기 때문에 현장에 대한 보존이 반드시 이루어져야 한다.

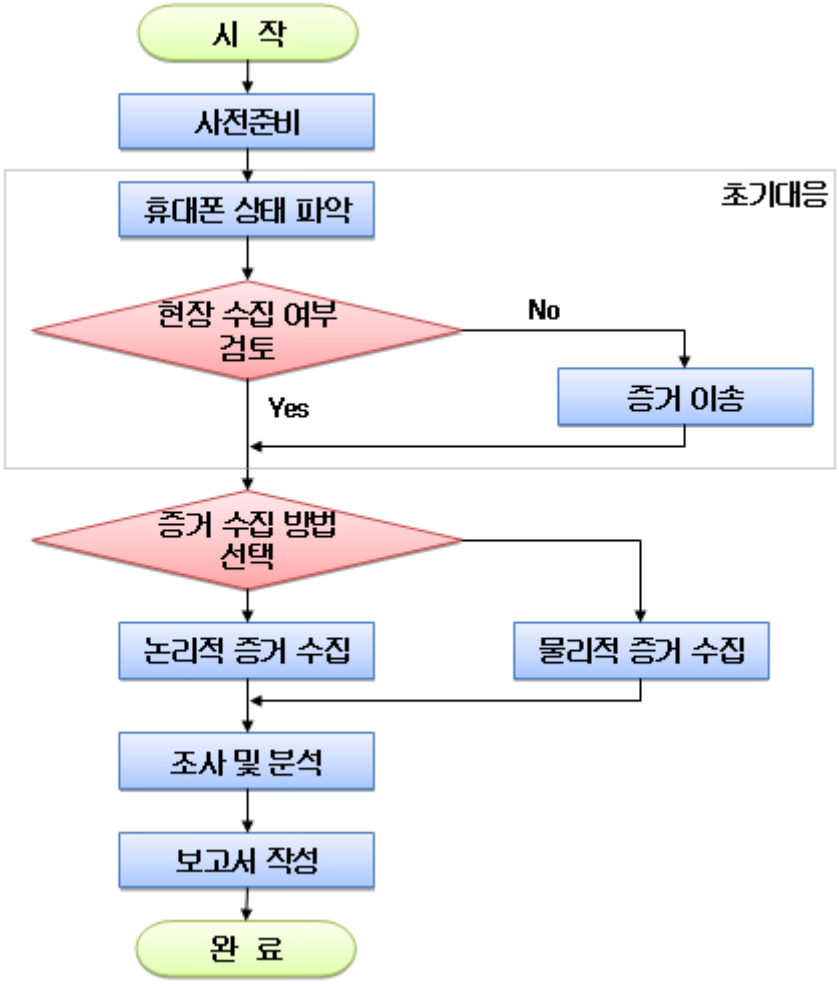
그 다음 현장에 대한 상황과 주요 사항들을 기록으로 남겨야 한다. 현장에 대한 영구적인(불변의) 기록을 남기고 디지털 증거든 일반적인 형태의 증거든 두 측면 모두 정확히 기록되어야 한다. 이후 일반적 형태의 증거와 디지털 증거를 수집하고 법적 효력을 유지할 수 있도록 디지털 증거의 무결성을 훼손하지 않아야 하며, 절차연속성(Chain of Custody)을 유지해야 한다. 수집된 데이터는 증거 포장, 증거 이송, 증거 저장 순으로 처리되며 이 역시 절차연속성을 유지해야 한다.

4.2 디지털 포렌식 수사 단계

포렌식 수사 절차는 수사준비, 증거수집, 증거 보관 및 이송, 증거 분석, 보고서 작성 등의 다양한 단계로 구성되며 각 단계에서 다음 단계로의 절차연속성의 유지는 무엇보다 중요하다. 수사준비 단계에서는 증거의 수집 및 분석을 위한 포렌식 도구의 구비 및 장비 점검을 하여 신속한 수사가 이루어질 수 있도록 하며, 수사관에 대한 교육을 통해 운용가능한 도구를 최대한 활용할 수 있도록 한다. 증거 수집 단계에서는 현장의 사진을 촬영하고, 압수수색 영장이 허용하는 범위에서 하드웨어, 소프트웨어, 보조기억장치 등을 수집한다. 대상 시스템이 활성화 되어 있는 상태일 경우에는 휘발성데이터를 수집한다. 하드디스크와 같은 저장 매체의 경우에는 무결성을 해치지 않도록 주의하여 이미징 작업을 수행하고 추후 변조되지 않았음을 입증하기 위해 해쉬값을 계산하여 저장한다. 증거 보관 및 이송단계에서는 디지털 증거물이 이송 및 보관 과정에서 손상되지 않도록 쓰기 방지 조치를 취하고, 정전기 방지용 팩을 사용하여 외부의 전자기력으로 인한 손상을 예방해야 한다. 증거 분석 단계에서는 상황에 따라 적절한 포렌식 도구를 이용하여 법정에 제출할 디지털 증거를 검색·복구한다. 마지막으로 보고서 작성 단계에서는 보고서를 읽게 되는 법관, 변호사 등 컴퓨터에 대한 지식이 부족한 사람이 보더라도 쉽게 알 수 있는 형태로 작성이 되어야 하며, 증거물 수집, 보관, 분석 등의 과정을 6 하 원칙에 따라 명백하고 객관성 있게 작성되어야 한다.

5. 휴대폰 포렌식 절차

휴대폰 역시 디지털 기기의 하나로써 디지털 포렌식의 절차에서 크게 벗어나지 않는다. 그러나 일반 디지털 기기에 비해 휴대폰의 경우 개인의 생활과 밀접한 관련이 있어 각 세부단계에서 상황에 따른 여러 사항을 고려해야 한다.



(그림 5-1) 휴대폰 포렌식 절차

5.1 사전 준비

사전 준비 단계는 포렌식 수사를 위한 제반 사항에 대한 준비단계이다. 디지털 포렌식에서의 사전 준비 단계와 마찬가지로 도구에 대한 준비 및 수사관에 대한 교육이 이루어져야 한다.

새로운 휴대폰은 제조사마다 경쟁적으로 출시가 되고 있으므로, 새로운 휴대폰의 출시에 맞춰 각각에 대응할 수 있는 도구의 개발이 이루어져야 한다. 또한 기존의 도구에 대한 지속적인 업데이트를 수행해야 한다. 모든 휴대폰에 대한 증거 추출 및 분석을 가능하게 하는 휴대폰 포렌식 도구는 현재 존재하지 않으며, 추후에도 기대하기에 무리가 있다.

휴대폰 포렌식을 위한 도구의 개발에서 무엇보다 증거 수집 도구의 개발이

선행되어야 한다. 증거 수집은 가능하다면 물리적 수집을 우선으로 할 수 있도록 하며, 논리적 수집은 물리적 수집이 어려운 경우에 수행 이루어 질 수 있도록 해야 한다. 물리적 수집에서도 비파괴적 방법인 표준 하드웨어 인터페이스 사용방식이 가능한 도구 개발이 이루어져야 한다. 휴대폰에서 플래쉬 메모리를 분리하여 직접 수집하는 방법은 추후 용의자에게 휴대폰을 돌려주어야 하는 경우 문제의 소지가 발생할 수 있으므로 사용이 제한된다.

휴대폰은 현대인에게 있어 단순 통신 장비가 아닌 생활필수품으로써 사용되고 있다. 따라서 조사를 수행하기 위해 수사관이 휴대폰을 가져가야 하는 경우 휴대폰의 소유자에게 잠재적인 피해를 입힐 수 있다. 따라서 수사기관에서는 휴대폰을 소유자로부터 인계 받아야 되는 경우 대체하여 사용할 수 있는 별도의 기기를 제공할 수 있도록 준비하여야 한다.

5.2 초기 대응

초기 대응 단계는 사건 현장을 보존하고 기록한다. 현장에서 휴대폰을 입수하였을 경우에도 역시 휴대폰에 대한 기본적인 정보를 확인하고 기록하여 차후에 있을 재현에 대비해야 한다.

휴대폰은 일반적으로 개인이 휴대하므로 현장에서 입수하는 경우 외에도 수사과정에서 용의자 및 피해자가 휴대한 상태로 발견될 수도 있다. 이러한 경우 일차적으로 휴대폰 소유자에게 동의를 구해 소유자의 입회 하에 휴대폰에 저장되어 있는 디지털 증거를 물리적으로 수집하고, 소유자의 기명날인 또는 서명을 받아야 한다. 휴대폰의 디지털 증거를 소유자의 동의하에 물리적으로 수집을 한 후에는 소유자에게 휴대폰을 돌려주고 수집된 증거를 이용하여 수사를 진행한다. 이 때 수집된 증거물의 해쉬값을 출력하여 소유자의 서명을 받아 원본으로써 효력을 유지해야 한다. 휴대폰의 조사가 필요하나 휴대폰의 소유자에게 동의를 얻지 못한 경우에는 압수수색 영장을 받아 휴대폰을 압수하여 수사한다. 이 때 휴대폰 소유자의 생활 및 생계에 영향을 미칠 수 있으므로 대체하여 사용할 수 있는 휴대폰을 소유자에게 제공한다. 압수한 휴대폰은 연구실로 이송하여 휴대폰의 디지털 증거를 수집한다.

사건과 관련된 휴대폰을 입수하였을 때 휴대폰의 상태에 따라 초기에 대응하는 방법이 달라져야 한다. 일반적으로 휴대폰을 입수하였을 때 휴대폰의 상태는 정상 상태로 켜져 있는 경우, 휴대폰이 꺼져있는 경우, 파손 또는 침수 등으로 인한 비정상 상태로 구분할 수 있다.

5.2.1 정상 작동을 하고 휴대폰이 켜져 있는 경우

정상 작동을 하고 휴대폰이 켜져 있는 경우 휴대폰 소유자의 동의 여부에 따라 다음과 같이 대응한다.

가. 증거 수집에 대한 소유자의 동의를 얻은 경우

(1) 휴대폰 배터리의 양이 얼마나 남아 있는지를 확인한다.

- o 배터리의 양이 충분하지 않을 경우 배터리를 충전하여 증거 수집 도중 휴대폰이 꺼지는 일을 방지한다.

(2) 휴대폰의 통신을 차단하여 증거 수집을 수행하는 동안에 증거 변화의 가능성을 제거한다.

(3) 휴대폰이 잠금 모드로 설정된 경우에는 휴대폰의 소유자에게 비밀번호를 확인한 후 기록하고 잠금 모드를 해제한다.

(4) 휴대폰의 기본적인 상태(날짜, 시간)을 기록한다.

(5) 물리적 수집의 가능여부를 파악한다.

(6) 물리적 수집이 가능한 경우 즉시 수집을 수행하고, 수집된 증거의 해쉬값에 대해 휴대폰의 소유자로부터 기명날인 또는 서명을 받아 기록한다.
- o 수집이 완료되면 휴대폰은 소유자에게 돌려준다.

(7) 물리적 수집이 불가능 한 경우에는 휴대폰의 연구실 이동을 위한 2차 동의를 요청한다.
- o 휴대폰의 소유자가 2차 동의를 했다면 휴대폰을 통신이 차단된 상태에서 연구실로 이송하고, 휴대폰 소유자에게 사전에 준비되어 있는 휴대폰을 제공한다.
- o 2차 동의를 얻지 못했다면 압수수색 영장을 통해 휴대폰을 입수하고, 동의를 얻지 못한 상황에서의 초기대응 단계로 진행한다.

나. 증거 수집에 대한 소유자의 동의를 얻지 못한 경우

(1) 압수수색 영장을 받아 휴대폰을 입수한다.

(2) 남아있는 배터리 양을 확인하여 부족시 충전한다.

(3) 휴대폰이 잠금 모드로 설정된 경우에는 휴대폰의 소유자에게 비밀번호를 확인한 후 기록하고 잠금 모드를 해제한다.

(4) 휴대폰의 기본적인 상태(날짜, 시간)을 기록한다.

(5) 전자기 차폐 봉투 등을 이용하여 휴대폰의 통신을 차단하고 봉인한다.

(6) 연구실로 봉인된 휴대폰을 이송한다.

5.2.2 휴대폰이 꺼져 있는 경우

가. 증거 수집에 대한 소유자의 동의를 얻은 경우

(1) 휴대폰의 비정상 여부 확인을 위해 휴대폰의 외관을 확인하고 소유자에게 휴대폰이 정상인가를 확인한다.

(2) 휴대폰의 통신을 차단한다.

(3) 휴대폰이 정상으로 판단되는 경우 휴대폰의 전원을 켜서 실제 이상여부를 확인하여 기록한다.

(4) 휴대폰의 작동에 이상이 있는 경우 신속히 배터리를 분리한다.
- o 휴대폰 수집에 대한 2차 동의를 구한다.
- o 휴대폰 소유자가 2차 동의를 한 경우 휴대폰을 봉인하고 연구실로 이송한다.
- o 2차 동의를 얻지 못했다면 압수수색 영장을 통해 휴대폰을 입수하고, 동의를 얻지 못한 상황에서의 초기대응 단계로 진행한다

(5) 휴대폰의 작동에 이상이 없는 경우 정상 휴대폰에 대한 초기 대응 단계를 수행한다.

나. 증거 수집에 대한 소유자의 동의를 얻지 못한 경우

(1) 압수수색 영장을 받아 휴대폰을 입수한다.

(2) 휴대폰의 현재상태를 기록한다.

(3) 휴대폰의 통신을 차단하고, 봉인한다.

(4) 휴대폰을 연구실로 이송한다.

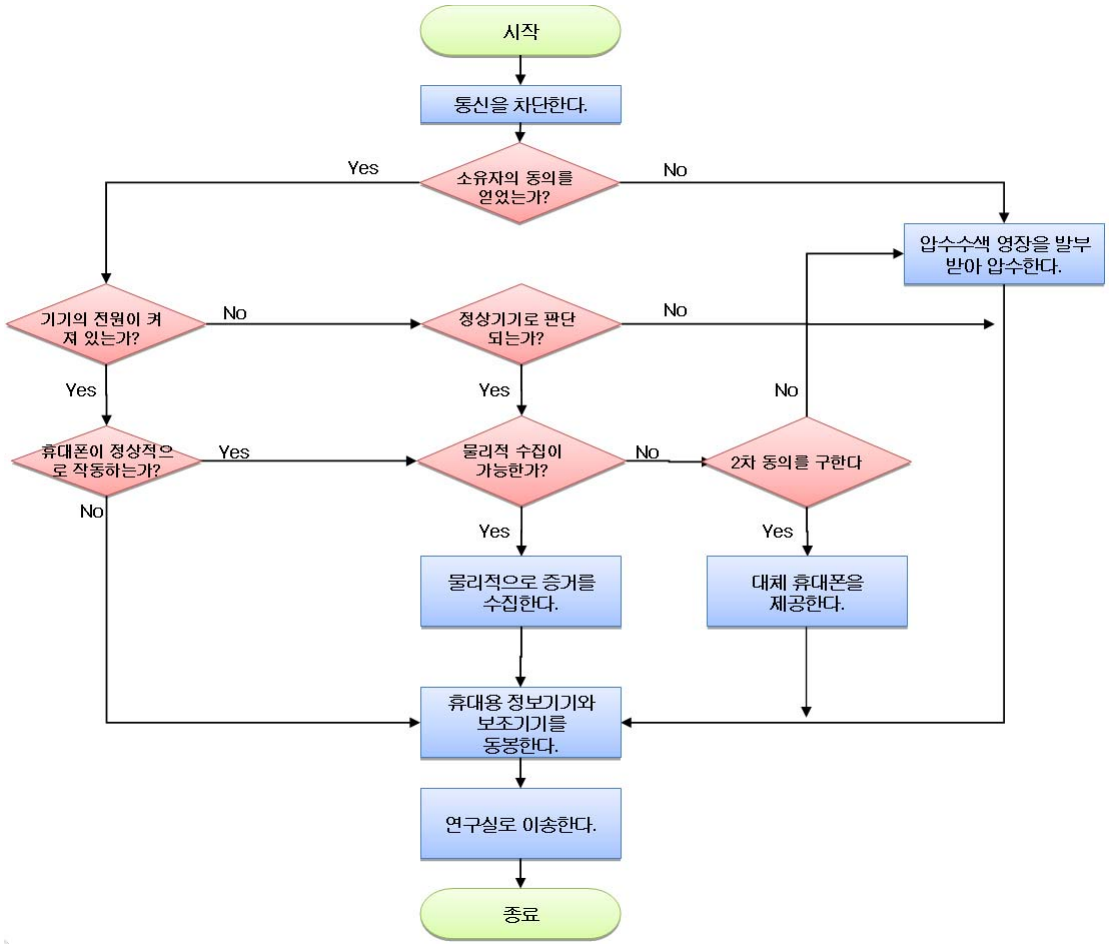
5.2.3 비정상적인 상태로 발견된 경우

비정상적인 상태는 휴대폰의 외관상 파손 또는 파괴가 된 경우와 외관에는 문제가 없으나 작동하지 않는 상태를 포괄한다. 휴대폰이 비정상적인 상태에 있을 경우 초기 대응시 신속히 연구실로의 이송이 필요하다.

(1) 휴대폰 상태를 기록을 한다.

(2) 비정상적인 상태로 발견된 경우 추가 손상을 예방하기 위해 파손방지 처리와 함께 봉인한다.

(3) 봉인된 휴대폰을 연구실로 이송한다.



(그림 5-1) 초기 대응 절차

5.3 증거 수집

증거 수집 단계는 휴대폰에서 디지털 증거를 추출하는 단계로써 증거 수집시 휴대폰의 데이터에 대한 변조가 발생해서는 안된다. 휴대폰의 경우 전원이 켜져있을 때 외부의 신호로 인해 데이터가 변조될 가능성이 높다. 따라서 휴대폰 증거 수집시 외부와의 통신을 차단하여 증거 수집 중에 휴대폰의 데이터가 변조되는 것을 예방해야 한다.

휴대폰의 증거를 수집하기 위해서는 휴대폰의 상태 및 휴대폰에 대한 포렌식 하드웨어, 소프트웨어 도구의 지원에 따라 적합한 수집 방법을 적용해야 한다. 증거 수집 방법은 물리적 방법과 논리적 방법이 존재하며 물리적 방법을 우선하여 적용해야 한다.

5.3.1 증거 수집 방법

증거 수집 방법은 크게 물리적 방법과 논리적 방법으로 구분할 수 있다. 물리적 방법에는 휴대폰에서 플래쉬 메모리를 분리하여 직접 메모리를 읽는 방법과 JTAG과 같은 표준 하드웨어 인터페이스를 이용한 방법이 있다. 논리적 방법에는 휴대폰의 파일전송 프로토콜을 이용하여 휴대폰의 파일을 직접 받는 방법과 제조사의 PC 소프트웨어를 이용한 방법이 있다.

각 증거 수집 방법을 적용하기 전에 다음과 같은 정보를 공통적으로 기록해야 한다.

- o 수집을 수행하는 도구와 버전
- o 휴대폰의 날짜와 실제 시간
- o 추가 외부 메모리의 사용여부

(가) 물리적 수집 방법

물리적 수집 방법은 디지털 포렌식에서의 하드디스크 이미징과 유사하게 휴대폰의 모든 메모리를 Bit-By-Bit로 복사할 수 있다. 따라서 휴대폰 포렌식 수사를 위해 가능하다면 물리적 방법을 이용하여 데이터를 수집해야 한다. 이러한 물리적 방법에는 직접 메모리 접근 방식과 표준 인터페이스를 이용한 CPU 제어 방식이 존재한다.

직접 메모리 접근 방식은 휴대폰을 분해하여 휴대폰 기판에 고정이 되어 있는 메모리를 분리하여 메모리를 포렌식 장비를 통해 데이터를 직접 읽는 방식이다. 표준 하드웨어 인터페이스를 이용한 증거 수집 방법은 휴대폰의 배터리와 작동여부에 영향을 받을 수 있으나 직접 메모리 접근 방식은 영향을 받지 않는다는 장점이 있다. 그러나 휴대폰의 메모리 타입에 따라 포렌식 장비를 별도로 제작해야 하는 단점이 있으며, 직접 메모리 접근 방식을 이용할 경우 휴대폰이 파손되어 추후 사건이 종결되어 휴대폰을 돌려주어야 하는 경우 문제 발생 소지가 있다. 따라서 직접 메모리 접근 방식은 파손되거나 비정상작동을 하는 휴대폰에 대해 한정해서 사용되어야 한다.

하드웨어 표준인터페이스를 활용하는 물리적 수집 방법은 제조사에서 휴대폰을 디버깅하기 위해 사용하는 방식을 이용한 것이다. 대표적인 표준인터페이스로 JTAG이 존재하며 이를 이용하여 휴대폰의 CPU를 제어함으로써 휴대폰의 메모리를 수집할 수 있다. 하드웨어 표준인터페이스를 활용한 방법은 휴대폰에 대한 파손의 염려가 없어 직접 메모리 접근 방식에 비해 유리하며, 물리적으로 데이터를 획득할 수 있으므로 휴대폰 증거 수집시 가장 우선하여 사용되어야 한다. 그러나 휴대폰이 비정상동작을 하는 경우 수집이 불가능 할 수 있으며, 휴대폰 마다 다른 입력신호의 사용과 CPU의 차이로 인해 휴대폰의 모델에 따른 케이블 제작과정이 필요하여 모든 휴대폰에 적용하는데 어려움이 있다.

(나) 논리적 수집 방법

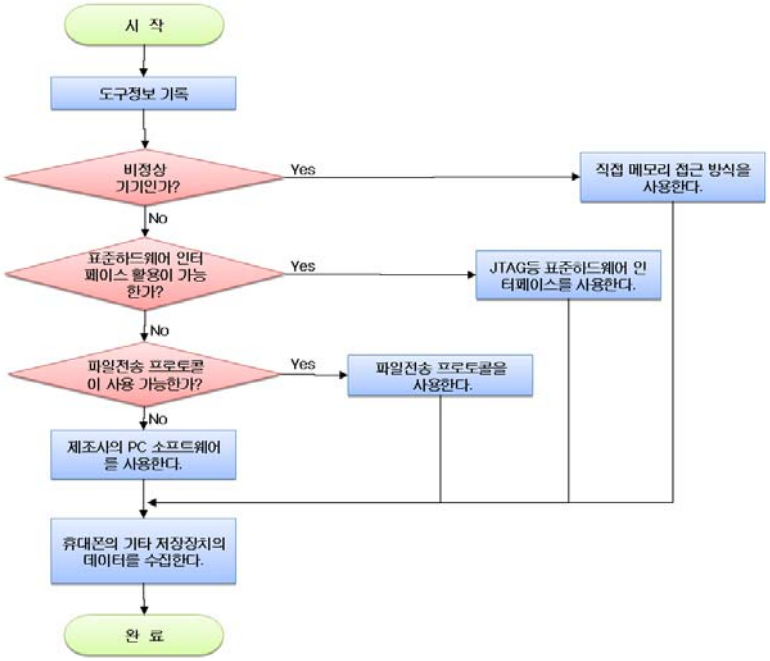
논리적 수집 방법은 하드디스크의 파일을 복사하는 방법과 유사하다. 이러한 논리적 수집 방법에는 휴대폰의 파일전송 프로토콜을 이용하는 방법과 제조사에서 제공하는 PC 소프트웨어를 사용하는 방법이 있다. 논리적 수집 방법은 삭제된 파일이나 미할당 영역의 정보 등을 수집할 수 없으므로 물리적 수집 방법을 적용할 수 없는 경우에 적용하도록 해야 한다.

휴대폰의 파일전송 프로토콜을 이용하는 방법은 휴대폰의 파일을 별도의 가공 없이 직접 전송을 받는 방법으로 휴대폰에 저장된 논리적 파일을 동일하게 복사한다. 따라서 외부로는 삭제되어 보이지 않는 문자메시지, 통화기록과 같은 정보를 플래그를 통해 표시만 하는 휴대폰의 경우 일부 삭제된 내용을 복원할 수 있다는 장점이 있다.

그러나 휴대폰의 모델마다 통신프로토콜이 다르고 OS 버전마다 차이가 있어 모든 휴대폰에 적용하는데 어려움이 있다.

제조사의 PC 소프트웨어를 이용한 방법은 위의 3가지 경우를 모두 사용할 수 없는 경우에 활용되어야 한다. 일반적으로 휴대폰 제조사는 휴대폰과 PC를 연결하여 사용할 수 있도록 소프트웨어를 제작, 배포하고 있다. 따라서 각 제조사에 따른 소프트웨어를 사용하면 모든 휴대폰에 대해 정보를 획득하는 것이 가능하다. 그러나 제조사의 소프트웨어에 따라 휴대폰의 데이터를 가공하여 다르게 보일 수 있으므로 타 방법이 존재하지 않을 경우에만 사용해야 한다.

디지털 포렌식에서는 증거의 무결성에대한 염려로 인해 논리적 복사에 대해서는 증거력이 소멸된 것으로 인정하나, 휴대폰의 경우 증거 수집이 매우 어려운 환경임으로 논리적 방법을 이용한 수집시 각 파일에 대한 모든 해쉬값을 저장하여 무결성을 보장해야 한다.



(그림 5-2) 휴대폰 증거 수집 절차

5.3.2 잠금 단말기

보통 잠금 단말기란 비밀번호 확인 모듈이나 잠금 기능이 활성화된 휴대폰을 말한다. 잠금 단말기에서 데이터를 수집하기 위해서는 수사정보를 활용할 수 있다.

(1) 용의자에게 질의 - 디바이스가 PIN이나 패스워드, 토큰, 어떤 다른 메커니즘으로 보호되어 있다면 초기 심문때 이 정보를 얻기 위해 용의자에게 물어볼 수 있다.

(2) 압수물품 검토 - 패스워드나 PIN이 종이 위에 쓰여진 상태로 남아 있거나 휴대폰과 연결되는 데스크 탑에 남아있거나 지갑과 같은 곳에 남아 있을 수도 있다.

(3) 수동 입력 - 취약한 메커니즘을 사용하고 있는 경우가 있다. 예를 들어 (U)SIM용 휴대폰은 4자리 숫자 PIN을 사용하는데 수사관은 숫자 조합을 이용해 폰을 풀 수 있다.

(4) 서비스 제공자에게 질의 - 휴대폰이 PIN-enabled (U)SIM으로 보호되고 있다면 가입자의 ID는 PIN이 여기 포함될 것이고 서비스 제공자로부터 PUK를 요구하거나 PIN을 초기화 시켜달라고 요구할 수 있다.

5.3.3 휴대폰 외부 저장 장치

메모리 카드와 휴대폰에 연결되는 호스트 컴퓨터 등이 위의 장비에 속한다. 여러 기종의 휴대폰들 중에서 고가의 기종은 일반적으로 여러 종류의 외부 저장 장치를 지원하기 때문에 대용량의 데이터를 저장할 수 있다. 메모리 카드는 대부분 플래쉬 메모리이며, 사용자 파일의 보조 기억장치로 사용되어 중요한 내용의 백업이나 디바이스 복구를 위한 파일들이 저장된다.

(1) 수사관은 메모리 카드를 압수하기 위해서, 메모리 카드의 인터페이스 및 종류를 상세하고 면밀하게 검색한다.

(2) 이동식 저장 매체를 통해 미디어 리더기 등을 사용하여 내부에 존재하는 데이터를 수집한다.

(3) 필요하다면 디지털 포렌식 수사 시 사용되는 이미징 작업을 수행한다.

(4) 메모리 카드에 있는 데이터는 개인용 호스트 컴퓨터에도 존재할 가능성이 있다.

전통적인 컴퓨터 포렌식 도구로 용의자 호스트 시스템의 하드 드라이브에서 증거를 수집하고 조사하며 증거를 복구한다.

5.4 휴대폰 포장, 운송 및 보관

(1) 휴대폰을 압수한 수사관은 증거 가방에 휴대폰을 넣고 봉인한 후 꼬리표를 붙인다.

(2) 휴대폰을 압수한 사람은 반드시 서명을 하고 날짜를 기록해 절차 연속성을 유지한다.

(3) 휴대폰은 안전하게 보관되어야 하며 증거가 보관 용기에 있을 때 우연히 버튼이 눌러지는 상황을 방지해야 한다. 견고한 운송용기를 특별히 제조하여 이러한 목적에 사용하도록 권고한다.

(4) 휴대폰을 옮길 때 전자파 차단 기능이 있는 가방을 사용하여 전자파 신호로부터

영향을 받지 않도록 해야 한다.

(5) 외부로부터 독립적인 전원 충전기가 연결되어 휴대폰이 운반되는 과정에 휴대폰의 배터리가 방전되지 않도록 해야 한다.

(6) 디지털 증거는 망가지기 쉽고 또한 쉽게 손상되기 때문에, 휴대폰이 운송될 때 조심스럽게 다루어야 하고 충격이나 부러짐, 극한의 온도를 피해 적절히 운송해야 한다.

(7) 데이터 휘발성이 큰 스마트 폰은, 즉시 디지털 포렌식 분석실로 옮겨야 하며, 증거의 절차 연속성은 필히 유지되어야 한다.

(8) 증거 저장 설비는 적절한 항온 항습을 유지해야 한다.

모든 증거는 컨테이너 안에 봉인되어야 하고, 안전한 장소에서 보관되어야 한다.

5.5 조사 및 분석

조사 및 분석 단계는 과학적인 방법으로 디지털 증거를 면밀히 살펴 법정에 제출할 수 있는 상태로 만들어 주는 단계로 수집한 증거를 복사하는 것으로부터 시작된다. 수집한 증거들을 토대로 사건과 직접적으로 관련이 있는 증거를 추출하게 되는데 예를 들어, 피해자가 살해당하기 전에 찍힌 사진을 용의자의 휴대폰에서 복구할 수 있었다거나 협박 문자를 복구할 수 있었다면 이것은 명백히 유죄를 판가름할 수 있는 증거가 될 수 있다. 다음은 분석 과정을 나타낸다.

(1) 추출된 휴대폰 데이터 복사본 및 증거 파일의 해쉬값 비교 확인

(2) 휘발성 정보를 획득하였을 경우 메모리, 프로세스, 사용 파일 등의 자원 사용을 분석하여 종료 전 사용됐던 기능 및 상황을 인지

(3) 휴대폰 증거 파일을 복사 및 복제하고 종류에 따른 분석 프로그램 실행

(4) 분석을 통해 전화번호, 주소, 메모, 스케줄 등의 기록 및 삭제된 기록, 시간과 관련된 정보들을 목적에 맞게 획득

(5) 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록

조사 및 분석 단계에서는 눈에 보이는 증거이든 감춰져 있는 증거이든 그 증거를 찾아내어 유.무죄를 증명할 수 있는 기반을 마련하는 단계이다. 조사 및 분석 단계에서 포렌식 전문가가 살펴보아야 할 휴대폰 내 정보는 아래와 같다.

✓ 가입자와 장치 ID ✓ 날짜, 시간, 언어 및 설정 정보 ✓ 전화번호 목록 정보 ✓ 스케줄 정보 ✓ 문자메시지 ✓ 발신, 송신, 부재 중 전화 정보	✓ 전자 메일, MMS ✓ 사진 ✓ 오디오 & 비디오 기록 ✓ 녹음 기록 ✓ 메모 ✓ 위치 정보

휴대폰의 증거를 분석할 때에는 휴대폰에서 제공하는 파일들뿐만 아니라 외부로부터 유입되는 파일, 즉, 사용자가 생성하는 사진, 동영상 같은 파일과 다운로드 받는 컨텐츠 등을 함께 분석해야 한다. 그리고 압수한 휴대폰에 대해서 통신사로부터 통화기록 및 가입자 정보를 얻어내고 그 데이터도 함께 분석해야 할 필요성이 있다. 왜냐하면 휴대폰의 사용 정보는 통신사에서 일부 저장하고 있으며, 이를 이용하면 알리바이를 증명할 수 있는 가능성이 많기 때문이다.

통화 기록은 전화 송수신 및 SMS 같은 송수신 정보를 의미한다. 통신사는 국제회선의 게이트웨이, 통화정보, 통화음성 등을 기록으로 남기기도 한다. 이런 기록 내용과 형식이 서비스 제공자마다 달라도 가입자 정보나 초기 통화, 발신 통화, 중복 전화 같은 장치 확인에 필요한 정보들은 기본적으로 저장된다.

통화 기록은 수사 협조와 수색 영장 등을 통해 통신사로부터 획득할 수 있다. 통화 기록뿐만 아니라 가입자의 정보 또한 요청할 수 있으며, 이것은 수사에 있어서 유용한 정보이다. 시스템의 DB는 대부분 아래와 같은 고객 정보를 저장하고 있다.

- ✓ 고객 이름 및 주소
- ✓ 계약자 (거래자) 이름 및 주소
- ✓ 실 사용자 이름 및 주소
- ✓ 전화번호
- ✓ 가입자 번호(MSI)
- ✓ 통화요금제
- ✓ 허용 서비스

5.6 보고서 작성

5.6.1 결과보고서 작성 및 준수사항

(1) 결과보고서는 조사자가 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성한다. 또한 작성자는 결과보고서에 서명하고 작성내용에 대해 책임을 진다.

(2) 결과보고서는 추정을 배제하고 사실관계를 중심으로 작성한다.

(3) 결과보고서는 객관적 사실, 설명내용, 분석자 의견을 구분하여 작성한다.

(4) 증거 발견방법 및 증거물에 대한 작업 내용은 명확하게 문서화한다.

(5) 분석 및 처리과정을 사진 또는 화면 캡쳐 등으로 기록을 유지한다.

(6) 분석에 사용된 하드웨어와 소프트웨어의 정보를 반드시 기록한다.

(7) 결과보고서 작성이 완료되면 분석담당관 서명 후, 원본 증거물과 함께 의뢰인에게 송부한다.

결과보고서는 수정이 불가능한 문서자료 형태로 부본을 작성하여, 관련 사건의 재판 종결시 또는 공소시효 만료시까지 증거보관실에 보관한다.

5.6.2 결과 보고서에 포함되어야 할 내용

(1) 보고서 번호, 사건 번호와 제출물 번호

(2) 사건 조사자, 제출자 신분

(3) 수령한 날짜, 보고서의 날짜(보고일)

(4) 휴대폰의 시리얼 번호, 제작, 모델을 포함한 아이템의 설명 기록 리스트

(5) 조사관의 신분과 서명

(6) 조사에 사용된 장비와 환경

(7) 조사 각 단계에 대해서 간단한 설명 (검색 단어, 그래픽 이미지 검색, 지워진 파일 복구)

(8) 증거의 독특한 아이템의 인쇄물, 증거의 디지털 복사본, 절차 연속성 문서

(9) 추출한 증거의 자세한 내용
- ✓ 사건과 관련된 특정 파일
- ✓ 지워진 파일과 같은 복구 증거를 지원하는 다른 파일들
- ✓ 인터넷 관련 증거
- ✓ 그래픽 이미지 분석
- ✓ 데이터 분석

✓ 조사된 아이템에서 관련된 프로그램 기술

(10) 보고서 결론

6. 휴대폰 포렌식 도구 개발 방향

휴대폰의 모델과 제조사를 알게 되면 매뉴얼을 찾을 수 있고 그로부터 정보를 획득할 수 있다. 검색 엔진에 모델 번호를 입력해 검색하면 그 디바이스에 대한 상당히 많은 정보를 얻을 수 있다. 제조사의 웹사이트 역시 좋은 정보 출처가 될 것이다. 앞서 언급했듯이 압수한 휴대폰에 따라서 포렌식 도구를 선택해야 한다. 아래 언급되는 사항은 휴대폰 포렌식 도구가 만족해야 할 기본적인 사항이다.

o 편의성 - 수사관에게 쉽게 이해할 수 있는 형태로 데이터를 표현하는가?

o 포괄성 - 조사자가 유/무죄를 입증하기 위해 모든 데이터를 표현할 수 있는가?

o 정확성 - 도구의 결과가 실증가능하고 알려진 에러율의 범위내에서 동작하는가?

o 일관성 - 같은 명령과 입력 데이터가 주어졌을 때 도구가 항상 같은 결과를 도출하는가?

o 검증가능성 - 중간 번역물과 발표결과로 나타나는 결과물의 정확성을 확신할 수 있는가?

휴대폰 포렌식 도구는 크게 수집도구와 분석도구로 구분을 할 수 있다. 각 도구는 위의 기본사항을 모두 만족할 수 있는 형태로 제작이 되어야 한다.

수집도구의 경우 휴대폰의 다양성과 짧은 생명 주기로 인해 빠른 업그레이드가 필요하며 가능하면 물리적 수집이 가능할 수 있도록 제작이 되어야 한다. 수사관이 휴대폰의 증거를 수집하는데 편리한 인터페이스를 제공해야 하며 다양한 휴대폰에 적용할 수 있는 방향으로 개발이 되어야 한다. 또한 수집시 발생할 수 있는 예외사항에 대한 기록을 할 수 있어야 하고 증거물에 대한 무결성을 제공해야 한다. 수집도구는 크게 물리적 방법과 논리적 방법으로 구분할 수 있다. 물리적인 데이터 획득 시에는 지워진 파일이나 할당되지 않은 영역의 데이터로 나타낼 수 있다는 장점을 지닌다. 논리적인 획득 방법을 적용할 경우에는 이해하기 쉬운 구조를 제공하며 제조사의 소프트웨어를 사용할 경우 이미 가공되어 누구나 알아볼 수 있는 형태로 제공이 된다는 장점이 있다. 휴대폰으로부터 데이터를 획득하는 도구는 근본적으로 물리적 획득을 수행해야 한다. 그러나 현재 이러한 수집방법에 대한 연구 및 개발이 미비하고, 획득한 이미지에 대한 분석 방법에 대한 개발 역시 미비하다.

따라서 논리적 수집도구를 개발 할 때에는 증거물의 무결성에 대해 무엇보다 고려해야 한다. 모든 파일에 대한 해쉬값을 저장하여 법정 증거로 채택되는데 있어 무리가 없도록

지원해야 한다.

분석도구는 휴대폰의 주요 데이터를 특성에 맞도록 조사관에게 표현해야 하며 휴대폰의 다양한 파일을 쉽게 표현할 수 있어야 한다. 또한 조사과정에서 수행한 데이터의 복원, 복구 과정등을 검증할 수 있도록 해야 한다. 조사관이 쉽게 증거를 조사할 수 있도록 검색 및 필터링 기능을 포함해야 한다. 휴대폰은 일차적으로 통신장비이므로 여러 용의자로부터 입수한 다양한 휴대폰 증거를 입력으로 활용하여 휴대폰 간의 관계를 파악할 수 있도록 해야 한다.

휴대폰용 수사 소프트웨어는 PC용 수사 소프트웨어와는 차이점이 존재한다. PC가 일반적인 용도로 설계된 반면 휴대폰은 좀더 특별한 용도로, 미리 결정된 업무를 수행하기 위한 용도로 설계해야한다. 휴대폰의 짧은 생명 주기에 맞춰 휴대폰 포렌식 도구 또한 빠르게 업그레이드되어야 한다.

표준작성 공헌자

표준 번호 : TTAx.xx-xx.xxxx/R1

이 표준의 제.개정 및 발간을 위해 아래와 같이 여러분들이 공헌하였습니다.

구분	성명	위원회 및 직위	연락처	소속사
과제 제안	길연희	PG102 - 위원	042-860-1031 yhgil@etri.re.kr	한국전자통신연구원
표준 초안 제출	이석희	PG102 - 위원	016-860-5964 gosky7@korea.ac.kr	고려대학교
표준 초안 검토 및 작성	이석희	PG102 - 위원	02-3290-4276 gosky7@korea.ac.kr	고려대학교
	이상진	PG102 - 위원	02-3290-4893 sangjin@korea.ac.kr	고려대학교
	길연희	PG102 - 위원	042-860-1031 yhgil@etri.re.kr	한국전자통신연구원
	은성경	PG102 - 부의장	042-860-5741 skun@etri.re.kr	한국전자통신연구원
	홍도원	PG102 - 위원	042-860-6147 dwhong@etri.re.kr	한국전자통신연구원
표준안 심의				
사무국 담당				

정보통신(영문)단체표준

TTA 표준 작성 샘플
(Example for Writing on TTA Standard)

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0114, Fax : 031-724-0019
발행일 : 200x.xx