TTA Standard

정보통신단체표준
TTAS.KO-12.0058

제정일: 2007 년 12 월 26 일

컴퓨터 포렌식 가이드라인

(Computer Forensics Guideline)

TTA 한국정보통신기술협회
Telecommunications Technology Association

정보통신단체표준 제정일 : 2007 년 12 월 26 일
TTAS.KO-12.0058

컴퓨터 포렌식 가이드라인

(Computer Forensics Guideline)

TTA 한국정보통신기술협회
Telecommunications Technology Association

서 문

1. 표준의 목적

본 표준은 컴퓨터나 디지털 기기가 범죄에 직간접적으로 연관되어 있는 경우에 이들로부터 필요한 단서 및 증거를 확보하는 논리적이고 체계화된 절차를 제공함으로써, 최종적으로 확보된 증거가 법적 효력을 갖도록 하는 것을 목적으로 한다.

2. 주요 내용 요약

본 표준은 디지털 증거 처리의 기본 원칙과 절차를 포함한다. 디지털 증거를 획득함에 있어 원본 보존, 디지털 증거의 무결성 보장, 분석 도구의 신뢰성 확보 등 기본 원칙을 정의하고, 디지털 증거 수집을 위한 각 단계별 준수사항을 열거한다. 또한 디지털 증거 처리를 위해 필요한 하드웨어 장비, 소프트웨어 도구 정보를 제공하고, 사전 준비, 디지털 증거물 수집, 증거 분석 등 각 단계별 절차를 제시한다. 하드디스크 상의 정보뿐 아니라 네트워크 사용 정보, 데이터베이스 내의 증거, CCTV 자료 상의 증거 등 각 디지털 증거의 분류에 따른 분석 방법을 상세히 다룬다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 표준은 디지털 증거를 수집, 분석, 보관하는 원칙과 절차를 제공함으로써, 디지털 증거 취급과 관련된 각종 조사 및 수사 행위의 체계화와 표준화를 유도하여 그 결과인 디지털 증거의 신뢰성을 확보할 수 있다.

4. 참조 표준(권고)

4.1 국외표준(권고)

없음

4.2 국내표준

없음

5. 참조표준(권고)과의 비교

5.1 참조표준(권고)과의 관련성

해당사항 없음

5.2 참조한 표준(권고)과 본 표준의 비교표

해당사항 없음

6. 지적재산권 관련사항

2007년 12월 현재까지 본 표준과 관련된 지적재산권은 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
제 1 판	2007. 12. 26	제정

Preface

1. The Purpose of Standard

This standard aims to establish principles and defines standardized procedures on digital evidence collection, analysis, preservation for investigator, researcher and analyzer so that the digital data extract through the procedures defined in this document can be accepted as evidence in the court.

2. The summary of contents

This standard consists of principles and procedures on computer forensics. It presents about preserving of original digital media, guarantee of digital data integrity and tools' reliability are principles of computer forensics. Also, the information of software and hardware tools as well as preparation and procedures of each steps for digital evidence acquisition are included. There are several kinds of digital evidences such as digital documents, internet history, e-mail, network information, data stored in databases, data of CCTV, etc. And they require different procedures, which are contents of this standard as well.

3. Applicable fields of industry and its effect

The principles and standard procedures defined in this document can be applied to investigation and examination related to treating digital evidence. By following the guideline in this standard, the acquired digital evidence will be reliable enough to use as evidence in the court.

4. Reference Standards (Recommendations)

4.1 International Standards (Recommendations)

None

4.2 Domestic Standards

None

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

As of December 2007, any IPRs related to this standard cannot be found

7. The Statement of Conformance Testing and Certification

Not applicable

8. The History of Standard

Edition	Issued date	Contents
The 1st edition	2007. 12. 26	Established

목 차

Contents

컴퓨터 포렌식 가이드라인

Computer Forensics Guideline

1. 개요

범죄 수사에 있어서 컴퓨터와 디지털 기기는 매우 중요한 수사 수단이 될 뿐만 아니라 수사의 대상이 되기도 한다. 그러나 컴퓨터 및 디지털 기기에 저장되어 있는 자료는 생성, 처리, 삭제, 변경, 복사, 전송 등이 매우 용이한 특징을 갖고 있어서, 법정에서 사용할 수 있는 증거가 되기 위해서는 논리적이고 체계적인 분석 방법과 절차가 요구된다. 따라서 본 표준에서는 법적 증거력을 갖는 디지털 증거를 획득하는 일련의 과정에 있어 지켜야 할 원칙 및 따라야 할 절차와 준수사항을 정의한다.

2. 구성 및 범위

본 문서의 구성은 아래와 같다. 먼저 3장에서는 관련 용어 및 약어를 정의하고, 4장에서는 컴퓨터 포렌식의 절차 및 기본 원칙을 기술한다. 5장에서는 컴퓨터 포렌식의 각 단계 별 준수사항을 나열하고, 6장에서는 디지털 증거 획득을 위한 사전 준비 과정을 기술한다. 7장과 8장에서는 각각 디지털 증거물을 수집하는 절차와 수집된 디지털 증거물로부터 디지털 증거를 획득하는 절차를 기술한다. 디스크 데이터 외 다양한 종류의 디지털 증거를 분석하는 과정을 9장에 추가하였다.

본 표준에서 다루는 디지털 증거란 컴퓨터로 접근 가능한 저장장치에 존재하는 디지털 데이터로 한정한다.

3. 정의

3.1. 용어 정의

가. 디지털 증거
: 디지털 형태로 저장되거나 전송되는 증거가치가 있는 정보

나. 디지털 증거 수집
: 디지털 증거를 포함한 디지털 증거물을 획득하고 해당 매체 내의 데이터를 분석하여 사건과 관련된 디지털 증거를 추출하는 과정

* 디지털 증거 획득과 비교했을 때 좀 더 넓은 의미로 디지털 증거물의 수집 및 이송 과정과 디지털 증거 획득 과정을 모두 포함한다.

다. 디지털 증거물

: 디지털 증거, 또는 확보되어야 할 증거와 관련된 잠재적 증거 등을 포함하고 있다고 판단되는 물리적 장치

라. 디지털 증거 획득

: 디지털 증거를 포함한 매체 내의 데이터를 검색 및 분석하여 사건과 관련된 디지털 증거를 추출하는 과정

마. 컴퓨터 포렌식

: 컴퓨터의 접근 인터페이스를 통해 접근 가능한 디지털 데이터 원본 저장소로부터 법적 증거력을 갖도록 디지털 증거를 논리적이며 표준화된 절차와 방법을 통해 수집, 보관, 분석 및 보고하는 과정

바. 휘발성 증거

: 컴퓨터 실행 시 일시적으로 메모리 또는 임시 파일에 저장되는 데이터로 네트워크 접속 상태, 프로세스 구동 상태, 사용 중인 파일 내역 등의 정보를 포함하고 있으며, 컴퓨터 종료와 함께 사라지는 디지털 증거

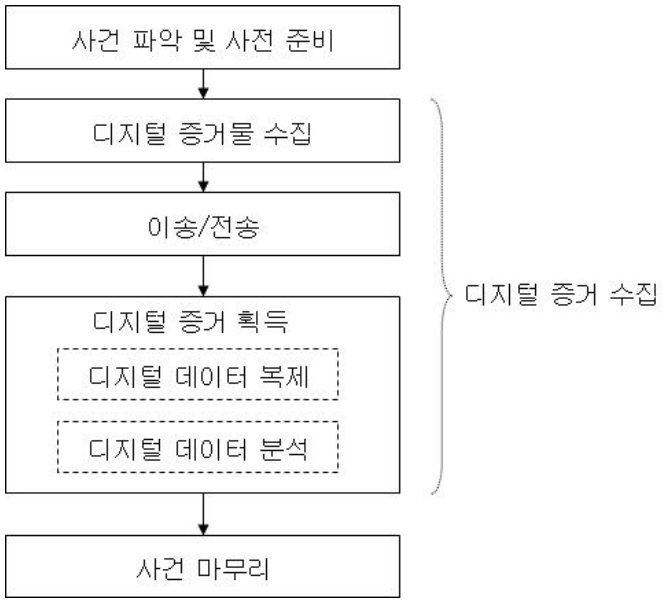
3.2. 약어 정의

ATA	AT-Attachment
BIOS	Basic Input Output System
CCTV	Closed Circuit Television
CD	Compact Disk
DVD	Digital Versatile Disc
IDE	Integrated Drive Electronics
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LCD	Liquid Crystal Display
MAC	Media Access Control
RAID	Redundant Array of Independent Disks
SATA	Serial ATA
SCSI	Small Computer System Interface
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Location
USB	Universal Serial Bus

4. 컴퓨터 포렌식의 절차 및 기본 원칙

4.1. 컴퓨터 포렌식 절차

컴퓨터 포렌식이란 컴퓨터로 접근 가능한 디지털 저장장치 내의 데이터로부터 법적 증거력을 갖도록 디지털 증거를 논리적이며 표준화된 절차와 방법을 통해 수집, 보관, 분석 및 보고하는 과정을 말하며, 그 절차는 아래의 (그림 4-1)에서와 같이 5단계로 구성된다. 먼저, 사건 파악 및 사전 준비를 하고, 현장에 출동하여 디지털 증거를 포함하고 있다고 판단되는 디지털 증거물을 수집한다. 이후 디지털 증거 분석실로 디지털 증거물을 이송하고, 디지털 증거물 내의 디지털 데이터를 분석하여 디지털 증거를 획득한 후, 사건을 마무리한다. 디지털 증거 수집은 디지털 증거물 수집 및 이송, 디지털 증거 획득으로 나뉜다.



(그림 4-1) 컴퓨터 포렌식 절차

사건 파악 및 사전 준비란 범죄의 유형 및 확보하여야 할 정보를 파악하고, 범죄 현장에서 수집 대상을 신속하고 정확하게 효율적으로 획득할 수 있도록 준비하는 과정을 말한다. 증거물 수집 계획 수립, 각 분야의 전문가를 포함한 증거 수집 팀 구성, 필요한 하드웨어 장비 및 소프트웨어 확보 등이 여기에 속한다.

디지털 증거물의 수집 과정은 현장에 도착한 후 현장 상황을 파악하여 디지털 증거가 존재한다고 판단되는 물리적 장치를 확보하는 과정과 해당 증거물을 안전하게 수집하는 과정으로 나뉜다.

디지털 증거 획득은 수집된 디지털 증거물 내의 디지털 데이터를 검색 및 분석하여

사건과 연관된 데이터를 찾아내는 것을 말한다. 디지털 데이터 분석에 앞서 획득된 디지털 증거물 내의 데이터를 보호하기 위해 디지털 데이터 복제가 선행되기도 한다.

사건 마무리는 분석 결과 및 기타 정보를 포함한 결과 보고서 작성과 증거 자료의 안전한 보관을 포함한다.

4.1. 컴퓨터 포렌식 기본원칙

디지털 증거는 법정에 제출되는 경우에 증거로서의 가치를 상실하지 않도록 적법한 절차와 수단을 토대로 획득되어야 한다. 명확한 법적 근거가 없는 수집 및 분석 행위는 절차상의 위법성으로 인해 증거 능력 자체에 문제가 생길 수 있다. 또한, 생성, 처리, 삭제, 변경, 복사, 전송 등이 용이하다는 디지털 증거의 취약성으로 인해 원 매체에 저장되어 있는 디지털 정보를 획득하는 과정에서 증거가치 보존을 위한 기술적인 방법들을 동원해야 한다. 더불어 디지털 증거의 또 다른 특성인 매체독립성, 비가시성으로 인해 법정에 제출될 때는 가시적인 형태로 변환되어야 하므로, 변환된 증거가 원본과 동일함을 증명할 수 있는 절차가 필요하다.

컴퓨터 포렌식의 기본 원칙은 아래와 같이 정의된다.

(1) 관련 법규 및 지침에 규정된 일반적인 원칙과 절차를 준수한다.

(2) 수사에 필요한 최소한의 증거 수집을 원칙으로 한다.

(3) 디지털 증거는 기술적, 절차적인 수단을 통해 진정성, 무결성이 보존되어야 한다.

(4) 신뢰성 있는 디지털 증거를 획득하기 위해 도구의 신뢰성이 뒷받침되어야 한다.

(5) 최종적으로 법정에 제출되는 디지털 증거의 원본성이 보장되어야 한다.

5. 컴퓨터 포렌식의 각 단계별 준수사항

본 장에서는 디지털 증거 수집의 각 단계별 준수사항을 나열한다.

5.1. 디지털 증거물 수집 시 준수사항

디지털 증거를 포함한 매체(컴퓨터 본체 또는 경우에 따라 하드디스크 등의 저장 매체)를 수집할 시 준수 사항은 아래와 같다.

가. 어떤 시스템을 수집할 것인지를 목록에서 확인하여 신속 정확하게 수집한다.

나. 하드디스크만 수집할 경우 충격 등으로 인해 증거물에 손상이 가지 않도록 주의한다.

다. 시스템 하드웨어나 네트워크를 파악하고 원본의 손상을 방지한다.

라. 시스템 전원 차단 여부를 먼저 파악하고, 전원이 꺼져 있다고 판단되더라도 화면보호기 작동 여부, 하드디스크 및 모니터 작동여부 등을 파악하여 전원 유무를 재확인한다.
- 화면보호기에 암호설정이 되어 있는 경우 수사관이 사용자 및 관리자에게 비밀번호 질의한다.

마. 전원이 켜져 있는 시스템에 수집해야 할 휘발성 자료가 있을 때 시스템에 피해가 가지 않는 최소한의 범위 내에서 작업을 수행한다.

바. 전원이 켜져 있을 경우 시스템 시간을 확인하는 과정에서 표준시각 정보와 비교해서 정확하게 기록한다.

사. 전원이 켜져 있을 경우 부주의에 의해 시스템 내의 프로그램을 실행시키지 않도록 주의한다.

아. 기타 장치의 종류를 확인하고, 기능이나 용도를 알 수 없는 장치가 있는 경우 사진촬영 등 자료를 확보하고 전문가와 상의한다.

자. 수집관의 전문성이 부족하다고 판단되는 경우 증거물을 조작하지 말고 전문가에게 인계한다.

차. 취급 미숙으로 인해 시스템을 켜는 것 만으로도 데이터를 변경할 수 있으므로 각별히 주의한다.

카. RAID[1] 기능을 지원하는 운영체제의 수가 지속적으로 증가하고 있으며, RAID 시스템으로 구성된 컴퓨터 수집 시에는 다음 사항을 준수한다.

(1) RAID 하드디스크 드라이브 복제본이 있을지라도 RAID 환경을 구성하는 RAID 카드와 프로그램 없이 RAID 환경을 재현하기는 어렵고, 또한 원본과 동일한 업체, 모델, 펌웨어 버전, 용량을 가지고 있지 않을 경우 복사 그 자체도 어려우므로, RAID 환경으로 구성된 컴퓨터 수집 시 세트 전체를 수집한다.

(2) RAID 카드를 사용할 경우, 카드·케이블·하드디스크 드라이브 연결 상태를 기록하고, RAID 카드는 커넥터와 하드디스크 드라이브 사이의 연결정보를 저장하므로, 재설치 시 주의한다.

(3) RAID 관련 프로그램, 케이블, 매뉴얼 등을 함께 수집한다.

타. 휴대용 저장장치는 소형화, 첨단화 및 대용량화 되고 있으므로 다음 사항을 준수한다.

(1) 대상자의 의복을 점검해서 USB 메모리 등 저장장치 소지 여부를 확인한다.

(2) CD-ROM 드라이브 등 구동장치 주변에 또 다른 저장장치가 있는지 조사한다.

(3) 부득이 저장장치에 저장된 내용 조회 및 검색이 필요한 경우 데이터 변조에 주의한다.

5.2. 디지털 증거물 이송 시 주의사항

컴퓨터 및 기타 저장장치는 외부환경에 민감하고 파손되기 쉬우므로 운반 및 이동 시 다음 사항에 주의한다.

가. 컴퓨터 본체

(1) 수집 당시 전원이 켜져 있지 않을 경우 켜지지 않은 상태 그대로 수집

[1] RAID(Redundant Array of Inexpensive Disks)는 여러 개의 하드 디스크에 일부 중복된 데이터를 나눠서 저장하는 기술이다. 데이터를 나누는 다양한 방법이 존재하며, 이 방법들을 레벨이라 하는데, 레벨에 따라 저장장치의 신뢰성을 높이거나 전체적인 성능을 향상시키는 등의 다양한 목적을 만족시킬 수 있다.

및 운반한다.

(2) 하드디스크 등이 물리적인 충격으로부터 보호되도록 완충용 보호 박스를 사용하고, 차량 이동 시는 스피커나 전자파가 나오는 장비 근처에 보관하지 않는다.

(3) 제조일자, 고유번호, 모델 등의 정보를 기록한 후, 모든 드라이브와 본체, 전원코드까지 함께 이송한다.

(4) 수집한 컴퓨터에 외상이 있는 경우, 수집 대상자 및 참관인이 입회한 상태에서 해당 사실을 인지시키고 기록한다.

(5) 수집한 컴퓨터 장비(특히 디스크)에 남아있는 지문 채취가 필요한 경우 과학수사요원에게 통보한다.

- 단, 지문 채취에 사용되는 시약, 분말가루, 테이프 등은 컴퓨터 및 저장장치드라이브 등의 인식에 영향을 미칠 수 있으므로 주의한다.

나. 모니터

완충제를 이용하여 포장한 후, 모니터의 앞면이 차량 뒷좌석의 시트 쪽으로 가도록 위치시키고 벨트로 고정한다. 특히 LCD 모니터 위에는 물건을 올려놓지 않는다.

다. 하드디스크

물리적인 충격이나 전자파의 영향을 받지 않도록 하고, 보호박스를 사용한 개별포장을 원칙으로 한다.

라. 저장장치

(1) 물리적인 충격 및 전자파의 영향을 받지 않도록 하고, 플로피디스크, CD 등은 구부리거나 휘지 않도록 주의한다.

(2) 증거물에 대한 설명을 기재한 인식용 라벨은 저장장치가 들어 있는 가방이나 케이스에 부착하고, 저장장치 표면에 직접 붙이지 않는다.

- CD-R의 표면에 라벨을 붙이면 반사 층에 영향을 주어 오작동을 유발할 수 있다.

5.3. 디지털 증거 획득 시 준수사항

디지털 증거의 획득은 수집된 디지털 매체로부터 대상 데이터를 복제하고 복제된 데이터를 이용하여 검색 및 분석하여 증거 데이터를 획득하는 과정으로 신뢰성 있는 디지털 증거를 확보하기 위해 신뢰성 있는 도구의 사용이 요구된다. 이때 복제된 사본을 복사원본이라고 한다. 데이터 복제 및 분석 도구는 연 1회 이상 신뢰성 검증을 실시하고, 통과된 도구만을 사용하도록 한다. 더불어, 널리 사용되는 전문 증거 분석용 도구를 사용하도록 권장한다.

디지털 증거 획득에 있어 데이터 복제 및 분석 작업을 효율적으로 수행할 수 있는 성능이 우수한 컴퓨터를 사용하고, 데이터 무결성 유지를 위하여 네트워크 접속은 금지한다.

데이터 복제 시에는 반드시 쓰기방지 장치를 이용하여 원본의 변경이 없도록 해야 하며, 이를 확인할 수 있는 암호학적 해쉬 등의 수단을 이용하여 무결성을 확보한다. 이때, 입회인의 서명 날인 등을 이용하여 객관적인 자료를 확보한다.

원본으로부터 수집한 복사원본은 수집하고자 하는 원본 내의 불량섹터를 제외한 모든 섹터를 포함하고 있어야 하며, 오류 없이 정확하게 획득되어야 한다. 여기서 불량섹터를 제외한 모든 섹터를 포함하도록 수집하는 것을 완전한 수집이라 하고, 오류 없이 정확하게 획득하는 것을 정확한 수집이라 한다. 이를 확인하기 위한 수단으로는 복사원본에 대한 해쉬값을 생성한 후 이미 생성된 원본의 해쉬값과 비교하는 방법이 있다. 디지털 증거는 원본의 해쉬값과 동일한 해쉬값을 가진 복사원본을 분석하여 획득하는 것을 원칙으로 한다 단, 신속한 분석을 요하거나 복사원본 생성이 현저히 곤란한 경우는 예외로 한다.

디지털 증거 획득을 위한 데이터 분석 과정에서 원본 및 복사원본의 변경이 발생하지 않아야 한다. 이를 위해 분석대상에 실행 파일이 포함되어 있는 경우는 별도의 운영체제 또는 가상머신에서 실행 및 분석하도록 하여 데이터의 변경을 방지한다. 또한 분석 과정에서 원본 및 복사원본을 이동할 시 책임자, 관리자, 일시, 장소, 사유 등을 관리대장에 기재한다.

최종적으로 획득된 디지털 증거는 신뢰할 수 있어야 한다. 인가된 증거 분석 도구를 이용한 전문 증거 분석관이라면 누구나 동일한 데이터를 도출할 경우 해당 디지털 증거는 신뢰할 수 있다고 판단된다.

디지털 증거 획득에 있어 분석 과정 및 분석관의 이름, 분석일자, 분석방법에 대해 상세히 기록하며 분석 시 주요 장면은 가급적 사진 또는 비디오로 촬영하여 보관한다.

디지털 증거 획득에 있어서의 기본 원칙은 아래와 같이 요약된다.

가. 데이터 복제 및 분석 도구의 신뢰성을 확보한다.

나. 성능이 우수한 전용 컴퓨터를 사용하고, 네트워크 접속은 금지한다.

다. 데이터 복제 과정에서 원본을 안전하게 보존 하고 무결성을 확보한다.

라. 데이터 복제 과정에서 완전하고 정확한 복사원본을 생성한다.

마. 디지털 데이터 분석 과정에서 원본 및 복사원본을 안전하게 보존하고 무결성을 확보한다.

바. 획득된 디지털 증거의 신뢰성을 확보한다.

사. 디지털 증거 획득 과정을 기록한다.

5.4. 결과 보고서 작성에 따른 준수사항

디지털 증거 획득 후 최종적으로 결과 보고서를 작성하는 과정에서 아래의 준수사항을 따른다.

가. 결과 보고서는 수사관이 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성한다.

나. 결과 보고서는 추정을 배제하고 사실관계를 중심으로 작성한다.

다. 결과 보고서는 객관적 사실, 설명내용, 분석관 의견을 구분하여 작성한다.

라. 증거 발견 방법 및 증거물에 대한 작업 내용은 명확하게 문서화한다.

마. 분석 및 처리 과정을 사진 또는 화면 캡쳐 등으로 기록을 유지한다.

바. 분석에 사용된 하드웨어와 소프트웨어의 정보를 반드시 기록한다.

사. 결과 보고서 작성이 완료되면 분석 담당관의 서명 후, 원본 증거물과 함께 의뢰인에게 송부한다.

아. 결과 보고서는 수정이 불가능한 문서자료 형태로 작성하여, 관련 사건의 재판 종결 시, 또는 공소시효 만료 시까지 증거 보관실에 보관한다.

5.5. 증거자료 관리에 따른 준수사항

사건과 연관된 증거자료의 관리에 있어 아래의 준수사항을 따른다.

가. 온도와 습도 등 기후의 영향을 받지 않으면서 충격과 자기장, 먼지 등으로부터 보호될 수 있는 증거보관실을 설치하여 운영한다.

나. 증거물은 쓰기방지처리가 된 상태로 충격방지용 보관함에 담아 분석이 끝날 때까지 증거보관실에 보관한다.

다. 증거 분석을 위해 생성한 복제본과 분석과정에서 나온 결과물은 반영구적인 저장장치에 저장하여 증거보관실에 보관한다.

라. 증거물 데이터베이스를 구축하여 관리 및 운영한다.

마. 사건 종료 후 관련 분석자료 검색 및 열람을 통해 유사사건 분석 또는 처리에 도움을 제공한다.

바. 증거물의 연계보관성을 보증할 수 있도록 증거물의 입출내역 등을 기록한다.

사. 증거 분석에 사용되는 도구 및 프로그램은 차후 수사 및 재판과정에서 재검증이 필요할 경우를 대비하여 제조사, 제작연도, 업그레이드 버전 별로 구분, 지속적으로 관리 보관한다.

아. 증거보관실 및 증거물에 대한 접근을 통제한다.

6. 디지털 증거물 수집을 위한 사전준비

본 장에서는 사건 현장에서 디지털 증거를 포함하고 있는 매체를 수집하기 위한 사전준비 과정을 다룬다. 디지털 증거물 수집 계획의 수립, 디지털 증거 수집 팀 구성, 수집 및 분석에 필요한 장비 확보 등이 사전준비 과정에 포함된다.

6.1. 디지털 증거물 수집 계획의 수립

디지털 증거물을 수집하는 자는 신속하고 효과적인 수집을 위하여 다음과 같은 사항에 유의하여 증거물 수집 계획을 수립한다.

가. 디지털 증거물 수집과 관련하여 아래와 같은 사항을 사전에 파악하여 둔다.

(1) 컴퓨터 하드웨어, 운영체제, 소프트웨어, 저장장치, 데이터베이스

(2) 네트워크 관련 정보

(3) 시스템 또는 네트워크 책임자나 관리자

(4) 수집해야 할 매체의 개수나 데이터의 분량

나. 수집 및 이송에 필요한 인원과 장비를 파악한다.

다. 디지털 증거물 수집이 법적 테두리에서 수행될 수 있도록 제반 문제점을 검토하고 필요한 서류를 준비한다.

6.2. 디지털 증거 수집 팀 구성

디지털 증거를 수집하기에 앞서 관련 전문가로 구성된 증거 수집 팀을 구성한다.

가. 증거 수집 팀은 사건 조사 담당자, 기술 전문가, 법률 담당자로 구성한다.

(1) 사건 조사 담당자는 수집 방향을 수립하고, 증거 수집 과정을 상세히 기록한 보고서를 작성한다.

(2) 기술 전문가는 운영체제, 데이터베이스, 네트워크, 프로그래밍, 해킹, 악성코드 등 분야별 전문가로 구성하며, 수집을 좌우하는 기술적 한계를 검토한다. 그리고 수집 실행 계획을 만들고, 수집을 담당한다.

(3) 법률 담당자는 증거수집에 따른 법률적 한계를 검토하고, 관련 법규 지침에 규정된 일반적인 원칙과 절차를 따르는지 확인한다.

나. 증거 수집 팀 구성이 완료되면 증거 수집 방법, 범위, 역할 분담, 주의사항에 대한 사전 교육을 실시한다.

다. 대상 시스템에 대해 가능한 한 많은 사전지식을 습득한다.

6.3. 수집장비 확보

디지털 증거 수집을 위해 아래와 같은 하드웨어 장비 및 소프트웨어를 확보한다.

6.3.1. 하드웨어

가. 증거 수집 및 분석용 컴퓨터

- 증거 수집 및 분석용 컴퓨터는 이동 시 충격을 완화하기 위해 보호용 케이스에 보관할 것

나. 증거 수집 및 현장 초동 분석을 위한 휴대용 컴퓨터 및 아래 <표 6-1>과 같은 추가장비 또는 기타 추가장비

<표 6-1> 증거 수집 및 분석을 위한 추가장비

용도	필요장비
인터넷 접속	100Mbps 또는 Gigabit 이더넷 카드, 무선랜(IEEE 802.11bga) 카드 등
주변기기 및 외부장치 연결	USB 2.0 포트, IEEE 1394b 포트, RS-232 시리얼 포트 등
증거보관	대용량 저장장치, 하드디스크 드라이브, CD 등

다. H/W 복제장치

- H/W 복제장치들은 이미징 소프트웨어들처럼 Source Disk와 Destination Disk에 대한 정보 수집 기능, 작업 내용 기록 기능, CRC 및 해쉬값 생성 기능 등 포렌식 기능 등을 갖추고 있음

라. 현장 초동 분석 필요 시 사용할 하드디스크 등 원본 증거의 위·변조 방지를 위한 쓰기방지 장치

- USB, IEEE1394 등과 같은 외부 포트에 연결되어 저장장치에 대한 쓰기 방지 기능 필요
- IDE, SATA, SCSI 등 다양한 저장장치에 대한 쓰기방지 지원 가능

마. 증거 복사원본 보관용 대용량 저장장치

- 증거 원본에 대한 수집이 어려울 경우 증거원본을 복제한 복사원본을 생성하여 저장하기 위한 대용량 디스크
- 복사원본 보관용 디스크는 안전하게 이동 가능한 보호용 케이스 사용
- 보관용 디스크는 기존에 보관되어 있던 자료와 혼동되지 않도록 데이터를 완전 삭제 후 사용

바. 수집된 휘발성 증거 또는 파일 증거 수집을 위해 USB 메모리 등과 같은 외장형 저장장치, 또는 공 CD-R, DVD-R

- 보관용 메모리는 기존에 보관되어 있던 자료와 혼동되지 않도록 내용을 완전 삭제 후 사용

사. 증거 운반 장비

(1) 하드디스크 등 외부충격에 약한 증거물을 위한 스티로폼, 스펀지 등이 내장된 충격완화용 보호박스

(2) 정전기로부터 보호하기 위한 제전용 보호필름

(3) 디스켓, CD 등의 분류와 보관을 위한 투명한 비닐 봉투

(4) 기타 케이블 등 부가적인 증거보관을 위한 수집물품용 박스

아. 다양한 규격의 연결 케이블 및 어댑터 (<표 6-2> 참조)

<표 6-2> 현장 증거 분석에 필요한 케이블 및 어댑터

구분	필요장비
전원 케이블과 어댑터	멀티플러그 종류별 전원케이블 100V to 200V 전원 어댑터
네트워크 케이블	이더넷 다이렉트 케이블 이더넷 크로스 케이블 등
데이터 전송케이블	USB 케이블 IEEE 1394 케이블 시리얼 케이블 패러럴 케이블(프린트 케이블) IDE 80 핀 케이블, IDE 40 핀 케이블 SATA 케이블

	SCSI 케이블 등

자. 분해와 해체를 위한 공구

(1) 장비 분해를 위한 사이즈 별 +/- 드라이버

(2) 케이블 등의 절단을 위한 니퍼, 플라이어 등의 공구

(3) 정전기 방지를 위한 제전용 손목띠

차. 서류 작성을 위한 각종 서식, 휴대용 프린터

카. 현장 촬영을 위한 카메라, 캠코더

6.3.2. 소프트웨어

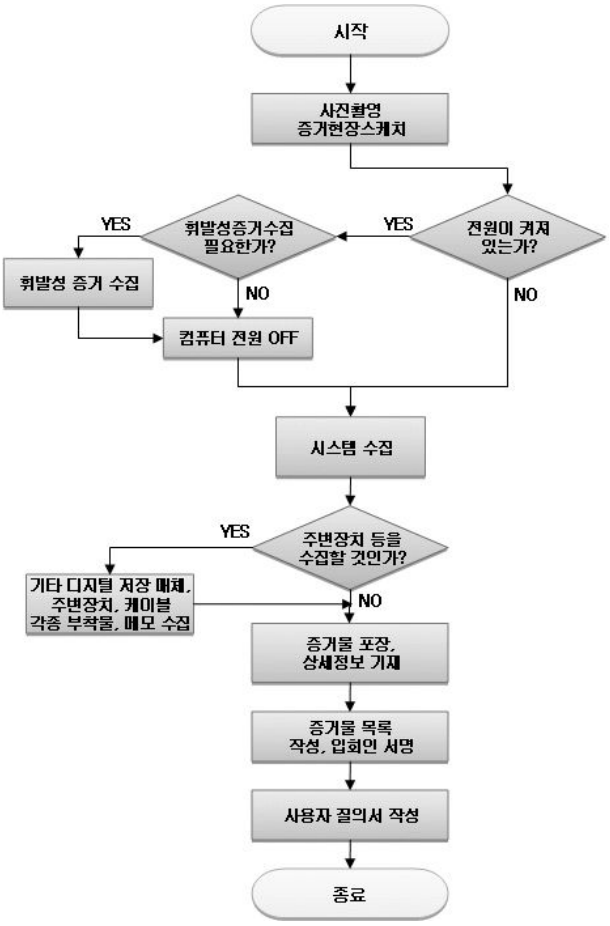
가. 증거 원본에 대한 복사원본을 생성하기 위한 이미지 생성용 소프트웨어

나. 디지털 증거 현장 초동 분석에 필요한 분석 소프트웨어

다. 휘발성 증거 수집을 위한 휘발성 증거 수집 소프트웨어

7. 디지털 증거물 획득 절차

디지털 증거를 포함하고 있는 증거물을 획득하는 절차는 아래 (그림 7-1)과 같다.



(그림 7-1) 디지털 증거물 획득 절차

7.1. 사진 촬영 및 현장 스케치

가. 컴퓨터 등 대상물의 앞·뒷면 사진, 주변장치를 포함한 사진을 촬영하고, 전원이 켜져 있는 경우는 모니터 화면을 촬영한다

나. 현장에 있는 수집 대상물의 위치를 상세히 스케치한다.

7.2. 휘발성 증거 수집 및 안전한 전원 차단

수집 대상물의 전원을 확인하고 꺼져 있는 경우 그대로 수집하고, 전원이 켜져 있을 경우 필요에 따라 휘발성 증거를 수집한 후 안전하게 전원을 차단한다.

컴퓨터의 전원을 종료함으로써 소실되는 휘발성 증거에는 실행중인 프로그램이나 프

로세스, 로그인 정보 뿐만 아니라 해킹, 웜·바이러스 등 사건 수사에 중요한 단서가 되는 경우가 많으므로 다음 과정을 통해 휘발성 증거를 수집한다.

가. 증거의 손상을 막기 위해 사건관련자 및 제3자들의 컴퓨터나 전원공급기로의 접근을 차단한다.

나. 모니터의 상태를 확인하고 현재 화면 등을 촬영한다.

다. 시간 정보를 수집한다.

라. 컴퓨터가 네트워크에 연결되어 있는 경우 원격접속을 통한 증거인멸 등을 사전에 차단하기 위하여 다음과 같은 사항을 확인 후 즉시 네트워크 케이블을 분리한다.

(1) 현재 네트워크 연결 상태를 수집한다.

(2) 현재 오픈된 TCP, UDP 포트 정보를 수집한다.

(3) TCP, UDP 포트를 오픈하고 있는 실행파일을 수집한다.

(4) NetBIOS 캐시 정보를 수집한다.

(5) 현재 접속 사용자 정보를 수집한다.

(6) 인터넷 라우팅 테이블을 수집한다.

마. 실행 중인 프로세스 및 서비스 내역을 수집한다.

바. 실행 중인 서비스 내역을 수집한다.

사. 현재 사용 중인 파일 내역을 수집한다.

아. 실행 중인 프로세스의 메모리 내용을 파일에 저장한다.

자. 휘발성 정보가 저장된 파일에 대한 해쉬값을 생성하여 증거물 목록에 기재한다.

전원이 켜져 있는 시스템의 경우 정상적인 종료 절차를 수행하면 임시 데이터가 삭제되므로 이를 방지하기 위해서 컴퓨터의 경우 종료 절차 없이 전원플러그를 강제 분리하여 비정상 종료한다. 상황에 따라 최대 절전 모드 종료와 비정상 종료를 선택해야

하며, 운영체제 별 전원 분리 방법은 아래 <표 7-1>에 기술한 대로 따른다.

<표 7-1> 운영체제 별 전원 분리 방법

운영체제	전원분리방법
DOS	전원 플러그 분리
Windows 3.1	전원 플러그 분리
Windows 9x/ME	전원 플러그 분리
Windows NT	전원 플러그 분리
Windows NT Server	정상 종료 최대절전 모드 전원 플러그 분리
Windows XP/2000 pro	정상종료 최대절전 모드 전원 플러그 분리
Windows 2000/2003 Server	정상 종료 최대절전 모드 전원 플러그 분리
Windows Vista	Bit Locker 해제 후 정상종료 최대절전 모드
Linux	정상 종료
Unix	정상 종료
Macintosh	전원 플러그 분리

비정상 종료는 시스템에 치명적인 손상을 가할 위험이 있다. 최대 절전 모드는 종료될 때 메모리의 데이터를 하드디스크로 옮기고 전원을 바로 차단하여 하드웨어적인 손상을 가하지 않으면서 시스템을 종료한다. 정상 종료 보다 시스템이 변경되는 부분이 극히 미약하기 때문에 서버와 같은 고가의 장비나 시스템일 경우, 또는 상황이 여의치 않을 경우 최대 절전 모드 사용을 고려해 볼 수 있다. 윈도우 시스템의 경우 최대 절전 모드 종료 과정은 아래 <표 7-2>와 같다.

<표 7-2> 윈도우 시스템의 최대 절전 모드 종료

제약사항	1. 전원 사용자 그룹의 구성원 또는 관리자로 로그온 해야 한다. 2. 컴퓨터가 네트워크에 연결되어 있으면 네트워크 정책 설정으로 인해 이 절차를 완료하지 못할 수도 있다.
순서	1. 제어판에서 전원 옵션을 연다. 2. 최대 절전 모드 탭을 클릭한 다음 최대 절전 모드 지원 확인란을 선택한다. (최대 절전 모드 탭이 표시되지 않으면 하드웨어가 이 기능을 지원하지 않는 것이다.) 3. 확인을 클릭하여 전원 옵션 대화 상자를 닫는다. 4. 시스템 종료를 클릭하고, 목록에서 최대 절전 모드를 선택한다.

Windows Vista의 경우 BitLocker로 인하여 기존의 방식에서 몇 가지 추가된 과정이

필요하다. 만약 활성시스템이 관리자 권한으로 로그인 되어 있다면 효율적인 조사를 위하여 활성정보 수집 후 ‘BitLocker 끄기’를 클릭한 후 ‘볼륨암호 해독’을 통하여 BitLocker를 해지한 후 종료하여야 한다. 만약 관리자 계정이 아니라면 앞의 방식으로 BitLocker를 해지할 수 없다. 관리자 계정이 아니면 활성정보 수집 후 BitLocker의 복구키를 찾아 BitLocker를 해지해야 한다. 복구키는 USB 메모리나 하드디스크에 저장하거나, 인쇄물로 출력하는 방식이 있다.

7.3. 시스템 수집

사건과 관련된 증거물로는 컴퓨터 시스템 및 주변 장치가 있다. 컴퓨터 시스템은 본체 수집을 원칙으로 하되, 부득이한 경우 하드디스크만 분리하여 수집한다. 하드디스크를 분리하여 수집할 경우 아래 절차를 따른다.

가. BIOS의 메인 메뉴에서 시스템 시간과 날짜 정보를 확인한다.

나. BIOS 시간과 표준 시간 간의 오차를 확인한 후 기록한다.

다. 컴퓨터 본체에서 하드디스크를 안전하게 분리한다.

컴퓨터 시스템을 수집하기 위해서는 먼저 네트워크 및 전원 케이블을 차단하고 기타 장치들을 분리한다. 단, 연결 포트와 케이블은 차후에 재 연결할 수 있도록 동일 숫자의 라벨을 부착하며, 주변 장치의 경우도 연결 상태를 쉽게 식별 가능하도록 사진 촬영을 하거나 일련번호를 부착한다. 노트북은 전원 어댑터를 분리하기 전에 전원상태 및 대기 모드 등을 확인하고 AC 어댑터를 수집한다.

7.4. 주변 장치 확보

시스템 수집 후 필요에 따라 외장형 디스크, USB 메모리 등 기타 디지털 저장장치와 관련 드라이브, 각종 소프트웨어, 주변장치, 케이블 등을 수집한다. 그리고 컴퓨터 주변에 부착되어 있는 포스트 잇, 메모, Note 각종 기록물들을 수집한다.

7.5. 증거물 포장

입수한 증거물의 이송을 위해 포장을 하고 상세 정보를 기록하여 부착한다. 상세정보의 내용은 사건번호, 수집자, 입회인, 수집일시, 장소, 물품, 제조번호 등이고, 하드디스크만 분리하여 수집하는 경우에는 추가로 BIOS 시간 오차를 기재한다. 하드디스크는 보호박스를 사용하여 개별 포장함을 원칙으로 한다.

7.6. 증거물 확인

증거물 포장을 완료하면 아래의 과정을 통해 수집한 증거물을 확인한다.

가. 수집증명서를 작성하여 입회인에게 교부하고, 입회인으로부터 수집확인서 및 수집증거물 목록에 서명 날인을 받는다.

나. 수집된 휘발성 데이터에 대한 해쉬값을 기록하여 입회인의 서명 날인을 받는다.

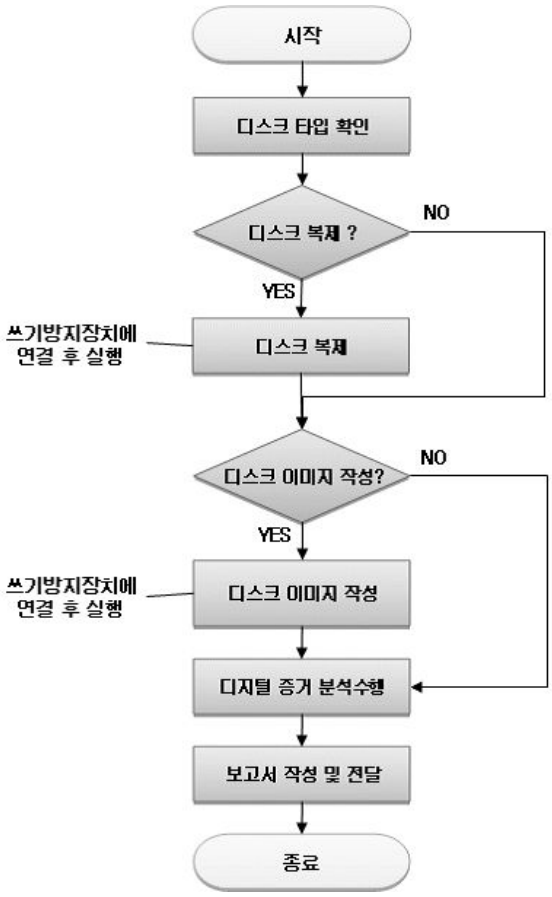
다. 디지털 데이터에 대한 이미지를 생성하였다면, 해당 데이터에 대한 해쉬값을 기록하여 입회인의 서명 날인을 받는다.

7.7. 사용자 질의서 작성

컴퓨터 사용자를 상대로 컴퓨터의 용도, 설치된 운영체제, 주로 사용하는 응용 프로그램 명, 패스워드가 설정된 프로그램 명, 패스워드 정보 등을 질의 후 기재한다.

8. 디지털 증거 획득 절차

사건 현장에서 획득한 디지털 증거물 내의 데이터를 수집하고 분석하는 디지털 증거 획득 절차는 아래 (그림 8-1)에 나타난 바와 같다.



(그림 8-1) 디지털 증거 획득 절차

8.1. 디스크 타입 확인

가. 증거 분석 담당자는 데이터 수집자와 사전 면담을 실시하여 사건개요, 증거물 수집 과정, 분석의 목적 등을 파악하고 분석 대상 및 범위를 결정한다.

나. 증거 분석 담당자는 증거물의 형태 및 인터페이스를 확인하고, 종류 및 특징에 따라 분석에 필요한 정보 및 기법을 사전에 숙지한다.

8.2. 디스크 복제

디지털 증거물의 복제 여부를 결정하고, 복제하여 분석하고자 할 경우 다음 절차를 따른다.

가. 물리적인 복제를 수행할 경우 동일한 용량의 하드디스크를 준비하고, 동일한 하드디스크가 없을 경우 원본 디지털 증거물보다 용량이 큰 하드디스크를 준비한다.

나. 원본 디지털 증거물에 쓰기방지 장치 연결하여 복제본(복사원본)을 생성한다.

다. 복제 후에는 원본 디지털 증거물과의 동일성 및 무결성 입증을 위해 원본 및 복사원본의 각 해쉬값을 수집, 비교한다.

8.3. 디스크 이미지 작성

디지털 증거물의 디스크 이미지 작성 여부를 결정하고, 디스크 이미지를 작성하고자 할 경우 다음 절차를 따른다.

가. 디스크 이미지 작성에 필요한 용량을 갖는 하드 디스크 또는 기타 저장 장치를 준비한다.

나. 원본 디지털 증거물에 쓰기방지 장치 연결하여 디스크 이미지를 작성한다.

다. 원본 디지털 증거물과의 동일성 및 무결성 입증을 위해 디스크 이미지를 복구한 후 해쉬값을 계산해 원본의 해쉬값과 비교한다.

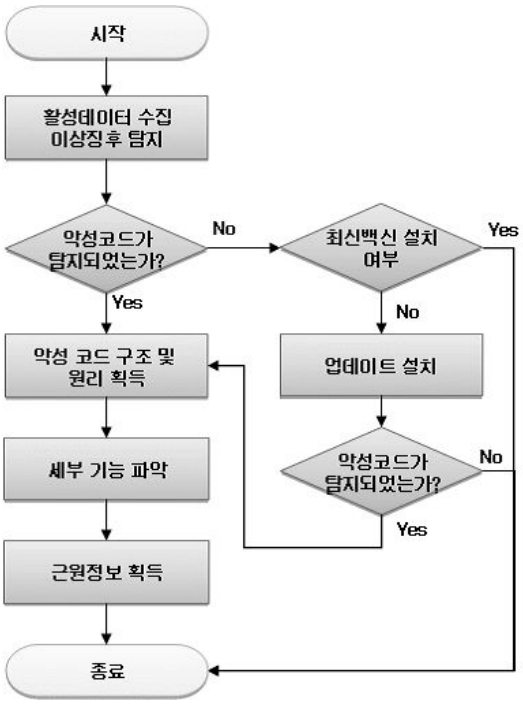
8.4. 디지털 증거 분석 및 보고서 작성

끝으로 디지털 증거를 분석하고, 분석 완료후 분석 결과 및 전반적인 절차와 정보를 기술한 보고서를 작성한다. 보고서는 사건 담당자에게 상세 설명 후 증거물과 함께 전달한다. 디지털 증거 분석은 복제 디스크, 또는 디스크 이미지를 이용하는 것이 일반적이나 여의치 않을 경우 원본 디스크를 직접 이용할 수도 있다. 그러나 이런 경우 원본 디스크의 데이터 변경을 최소화하고 변경 사항에 대한 이해를 하고 있어야 하며, 이러한 사실을 보고서에 포함하여야 한다. 또한 디스크의 분석에 앞서 용의자가 해킹을 당했다고 주장할 것에 대비하여 바이러스나 백도어 등 악성코드 감염 여부를 확인한다.

악성코드, 암호파일 등 특정 데이터에 대한 분석 절차는 아래 절에서 다룬다.

8.5. 악성코드 분석

악성코드 분석 절차는 아래 (그림 8-2)와 같다.



(그림 8-2) 악성코드 분석 절차

가. 실행 프로세스 목록 및 네트워크 상태 정보 등의 활성 데이터를 이용하여 이상징후를 탐지한다.

나. 악성코드가 탐지되지 않은 경우 최신 백신이 설치되었는지 확인하고, 업데이트 후 백신을 이용해 악성 코드를 검사한다.

다. 악성코드가 들어있는 파일의 실행파일구조, 압축된 실행 파일 상태, 메모리를 확인한다.

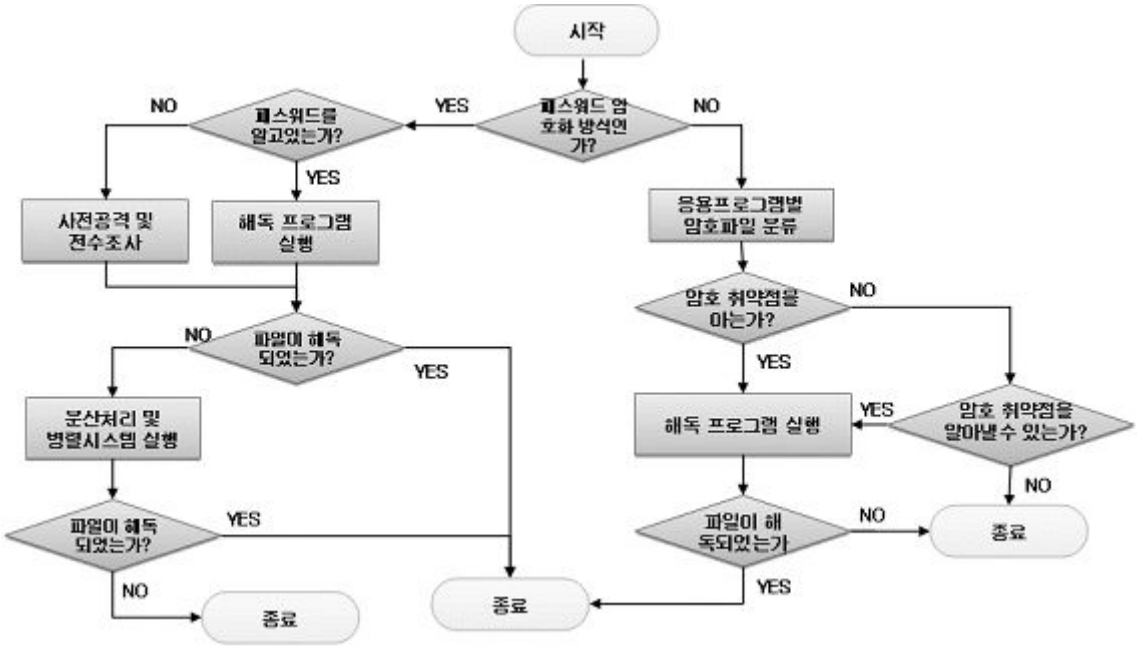
라. 소프트웨어 역공학 기법 등을 사용하여 분석 가능한 구조로 복원하여 기능, 원리 등을 획득한다.

마. 악성 코드의 사용 파일, 메모리 정보 등의 자원 사용 정보를 통해 해당 악성코드의 세부 기능을 파악한다.

바. 전자우편, IP, URL 등의 원격지를 추적할 수 있는 정보를 획득한다.

8.6. 암호파일 해독

수집된 디스크 내에 암호화된 파일이 있을 경우 암호 파일이 사용된 운영체제 또는 응용 프로그램의 종류 및 설정 정보를 파악하고, 해독에 필요한 하드웨어가 있을 경우 해당 하드웨어를 확보한다. 암호화된 자료의 해독 절차는 아래 (그림 8-3)과 같다.



(그림 8-3) 암호화된 자료 해독 절차

가. 패스워드를 이용한 암호 파일인지, 기타 응용 프로그램에서 자동적으로 암호화한 파일인지를 파악한다.

나. 패스워드를 이용한 암호 파일일 경우, 패스워드를 알고 있다면 해독 프로그램을 실행하여 해독하고, 모른다면 전수조사 및 병렬시스템을 이용하여 암호파일을 해독한다.

다. 파일이 해독되었으면 종료하고, 해독되지 않았으며 분산처리 및 병렬시스템 실행을 통해 파일을 해독한다.

라. 기타 응용 프로그램에 의한 암호화 파일일 경우 해당 응용 프로그램을 파악한 후 취약점을 찾아 해독 프로그램을 이용해 파일을 해독한다.

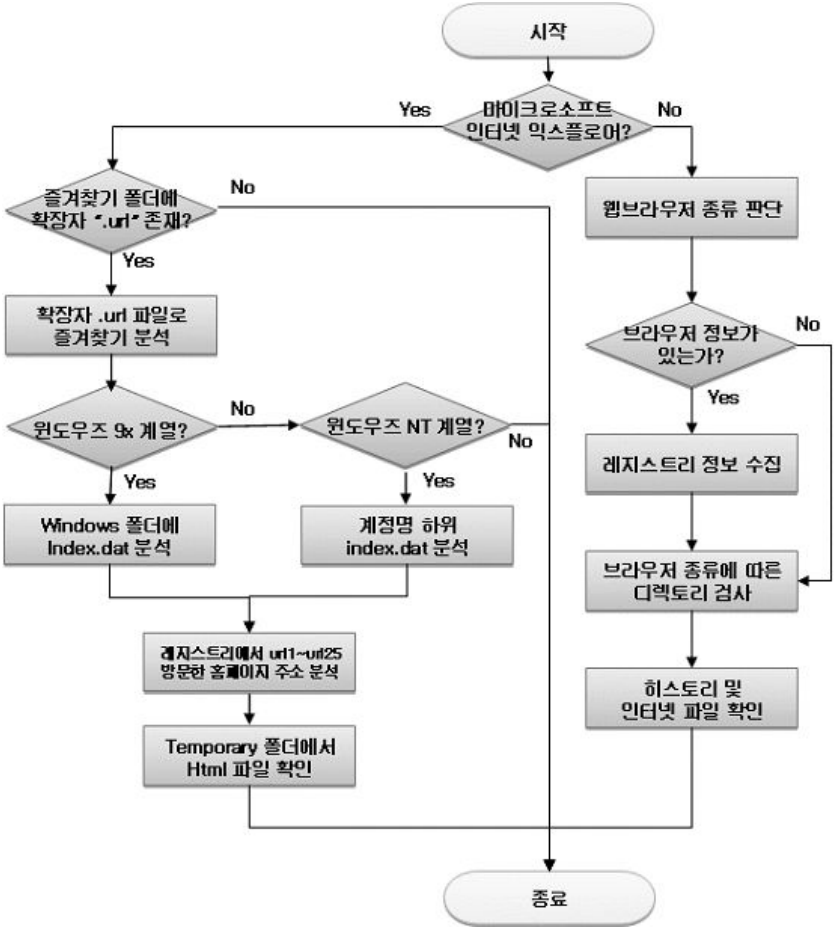
마. 암호 증거를 해독하는 방법이 알려져 있지 않은 경우 응용 프로그램 및 암호 증거를 암호화 패턴 검사, 역공학 기법 등의 방법으로 분석한다.

바. 암호파일의 경우 항상 해독이 가능하진 않으므로 해독하지 못하였을 경우 그

에 대한 보고서를 작성하여 제출한다.

8.7. 인터넷 사용 증거 분석

용의자의 컴퓨터에서 인터넷 사용과 관련된 정보가 존재할 경우 아래 (그림 8-4)의 절차를 이용해 접속한 주소지를 획득한다.



(그림 8-4) 인터넷 사용 증거 분석 절차

위 그림에 나열된 절차에서처럼 사용된 운영체제 및 웹 브라우저 환경에 따른 적절한 방법을 통해 인터넷 접속 정보를 파악한 뒤 접속 시간 등을 확인하여 용도에 맞는 정보를 획득한다. 해당 웹사이트의 관리자의 동의를 받아 사건과 관련된 데이터를 획득한다.

가. 웹브라우저의 종류를 파악해 마이크로소프트 인터넷 익스플로어일 경우 즐겨찾기 폴더 내 확장자 “.url”인 파일을 이용해 즐겨 찾기를 분석한다.

나. 운영 체제가 윈도우 9x 계열일 경우 Windows 폴더 내의 index.dat를 분석하고 NT 계열일 경우 각 계정 내 폴터에서 index.dat 파일을 분석한다.

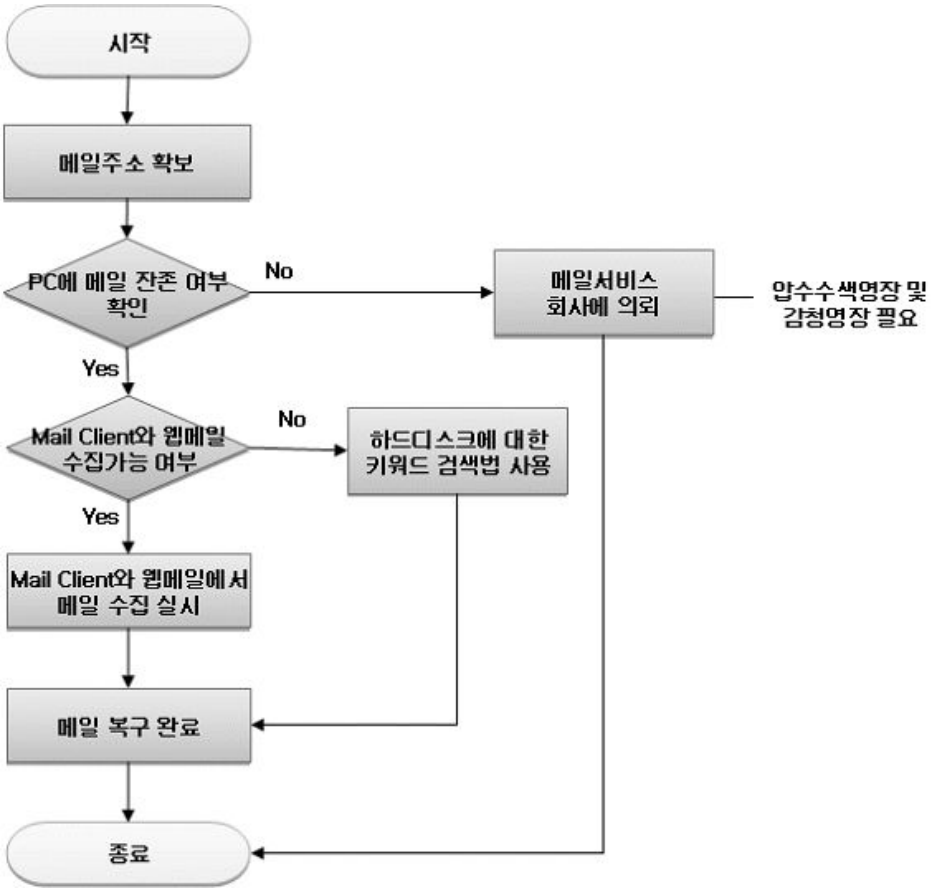
다. 레지스트리에서 방문한 홈페이지 주소를 분석하고 Temporary 폴더에서 Html 파일을 확인한다.

라. 사용된 웹브라우저가 인터넷 익스플로어가 아니라면 웹브라우저 정보를 파악하고 레지스트리 정보를 수집한 후 웹브라우저 종류에 따라 해당 디렉토리를 검사하여 히스토리 및 관련 인터넷 파일을 확인한다.

8.8. 전자우편 분석

전자우편과 관련된 증거를 획득하기 위해 디스크 및 메일 서버로부터 관련된 데이터를 획득 한 후 분석하는 과정을 거친다.

전자우편과 관련된 증거 자료 수집 절차는 아래 (그림 8-5)와 같다.



(그림 8-5) 전자우편 증거 수집 절차

가. 사용된 운영체제 및 전자우편의 종류 및 설정 정보를 확인한다.

나. 운영 중인 전자우편 서버에서 수집해야 할 경우 운영자에게 문의하여 관리자

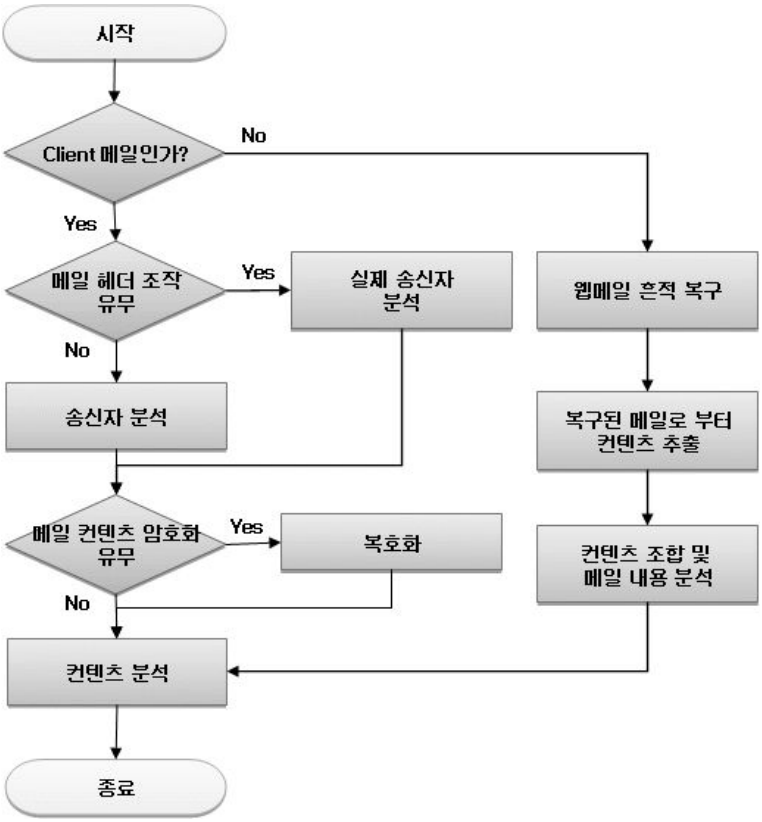
계정을 획득한다.

다. 전자우편의 우편함 파일과 주소록 파일을 확인 및 수집한다.

라. PC에 존재하는 데이터로 웹메일 수집이 가능한 경우 웹메일을 수집한다.

마. 전자우편 서버에서 전자우편 파일만을 수집하였을 경우 수집된 전자우편의 복사본 또는 저장한 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관한다.

수집된 전자우편과 관련된 증거의 분석 절차는 아래 (그림 8-6)과 같다.



(그림 8-6) 전자우편 증거 분석 절차

가. 전자우편 증거의 종류에 따른 전자우편 프로그램을 구축하고 증거 파일을 복사 및 복제한다.

나. 메일 헤더의 조작 유무를 확인하고 조작되었을 시 실제 헤더를 복구하여 송수신자를 분석한다.

다. 메일 컨텐츠가 암호화 되어 있을 경우 암호파일 해독 절차를 거쳐 복호화한다.

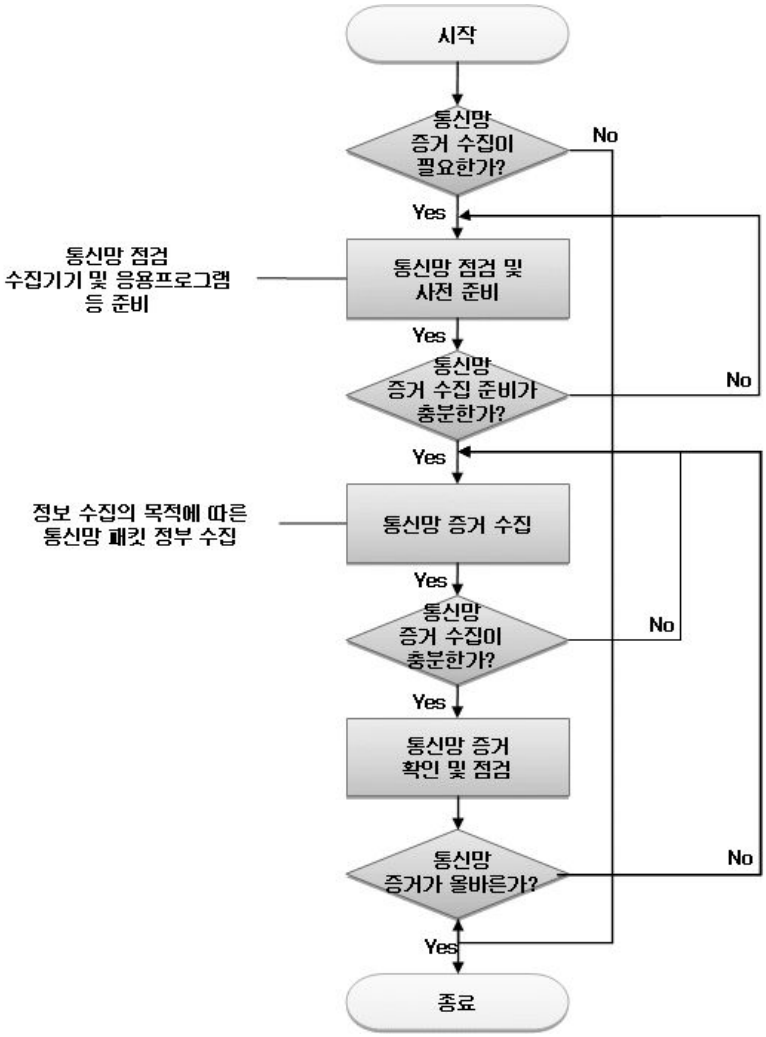
라. 획득된 컨텐츠로부터 IP 주소, 송신자, 수신자, 내용, 경로, 첨부 파일 등을 목적에 맞게 분석한다.

9. 디지털 증거의 종류별 분석 절차

9.1. 네트워크

9.1.1. 네트워크 증거 수집

네트워크 증거 수집 절차는 아래 (그림 9-1)과 같다.



(그림 9-1) 네트워크 증거 수집 절차

가. 네트워크 증거를 수집하기 위한 호스트 및 서버 등과 가까운 곳에 탭 장비를 설치한다.

나. 네트워크 장비의 탭 장비에 노트북 및 증거수집 기기에 연결한다.

다. 노트북 및 증거수집 기기에 수집 목적에 맞는 입력 값을 설정하고 실행한다.

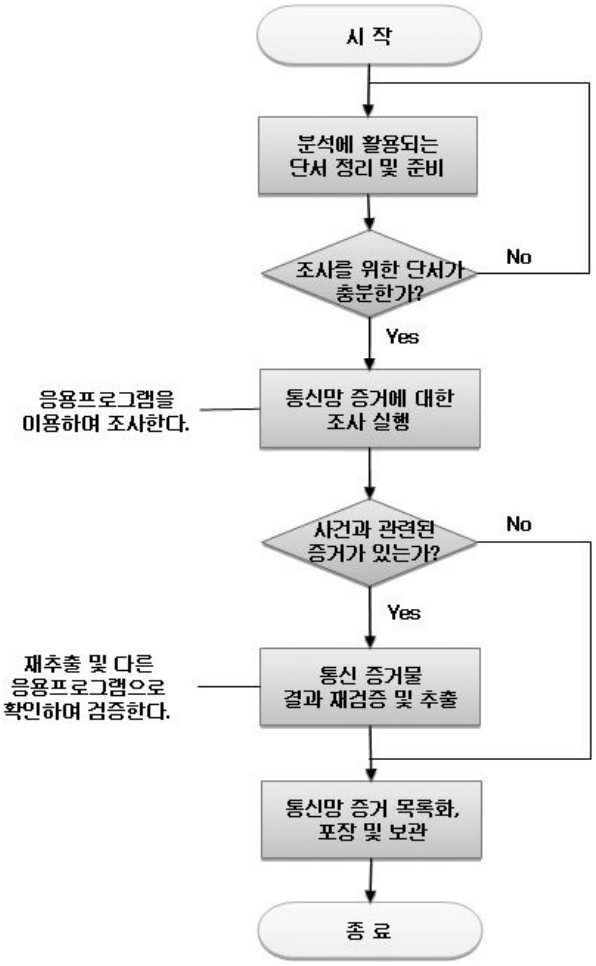
라. 수집 프로그램의 출력이 있을 경우 지속적으로 수집 상태를 확인한다.

마. 목표하는 네트워크 정보가 수집되었거나 목표하는 시간 또는 용량에 도달하였을 경우 수집을 종료한다.

바. 수집된 네트워크 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관한다.

9.1.2. 네트워크 증거 분석

네트워크 증거 분석 절차는 아래 (그림 9-2)와 같다.



(그림 9-2) 네트워크 증거 분석 절차

가. 수집된 통신망 증거 파일의 해쉬값을 생성하고 수집 시 작성된 문서에 기재된 값과 비교한다.

나. 네트워크 증거 파일을 복사 및 복제하고 분석 프로그램을 실행한다.

다. 목적에 맞게 용의 IP 주소, 용의 MAC 주소, 피해 IP 주소, 피해 MAC 주소, 포트 번호 등의 초점을 맞춰 프로그램을 설정하고 분석을 실행한다.

라. 분석을 통해 IP 주소, MAC 주소, 서비스, 기능, 원리 및 내용 등을 목적에 맞게 획득한다.

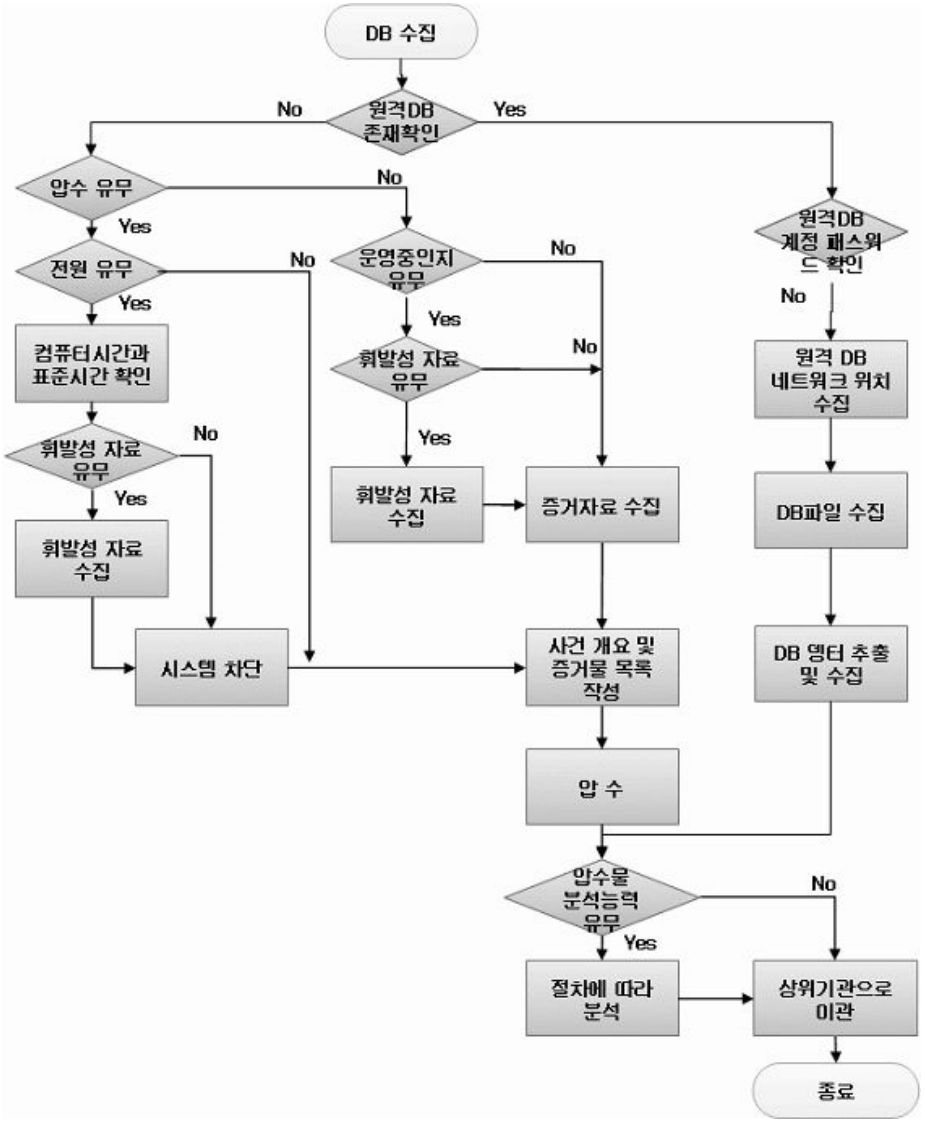
마. 네트워크 증거 분석의 분석자, 분석 과정, 분석 결과 등 세부 사항을 빠짐없이 기록한다.

9.2. 데이터베이스

데이터베이스를 포함하고 있을 시스템의 경우 시스템의 수집과 분석 경우, 데이터베이스 증거를 먼저 수집한 후 분석한다.

9.2.1. 데이터베이스 증거 수집

데이터베이스와 관련된 디지털 증거의 수집 절차는 아래 (그림 9-3)과 같다.



(그림 9-3) 데이터베이스 증거 수집 절차

가. 수집할 데이터베이스를 포함한 시스템원격 데이터베이스가 존재하는지 확인하고 존재하지 않을 경우 운영체제 및 데이터베이스의 종류 및 설정 정보를 확인한다.

나. 접속 프로그램을 사용하여 데이터베이스에 접속한 후 메모리, 사용자 정보,

자원사용 정보 등의 휘발성 정보를 수집한다.

다. 데이터베이스 서버를 수집할 경우 서버 프로그램 종료 후 운영체제를 정상 종료한다.

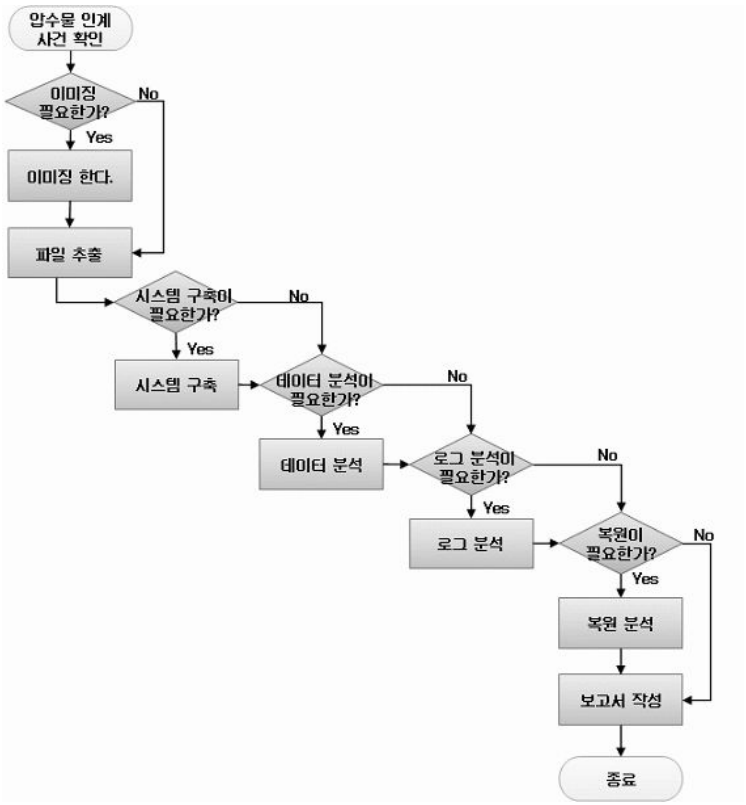
라. 목적하는 자료만을 수집할 경우 데이터베이스 또는 운영체제 명령어를 사용하여 자료를 수집 및 복사한다.

마. 데이터베이스 운영자 또는 개발자가 있을 경우 데이터베이스 설계 개념, 사용 목적 및 방법, 추가적인 백업 데이터 여부를 조사한다.

바. 수집된 데이터베이스의 복사본 또는 저장한 증거 파일의 해쉬값을 계산, 기록, 확인 후 보관한다.

9.2.2. 데이터베이스 증거 분석

수집된 데이터베이스 정보의 분석 절차는 아래 (그림 9-4)와 같다.



(그림 9-4) 데이터베이스 증거 분석 절차

가. 수집된 데이터베이스 복사본 및 증거 파일의 해쉬값을 생성하고 수집 시 작

성된 문서에 기재된 값과 비교한다.

나. 데이터베이스의 휘발성 정보를 획득하였을 경우 메모리, 프로세스, 사용 파일 등의 자원 사용을 분석하여 사용됐던 기능 및 상황을 파악한다.

다. 데이터베이스 증거에 맞는 운영체제 및 데이터베이스 프로그램을 구축하고 증거 파일을 복사 및 복제한다.

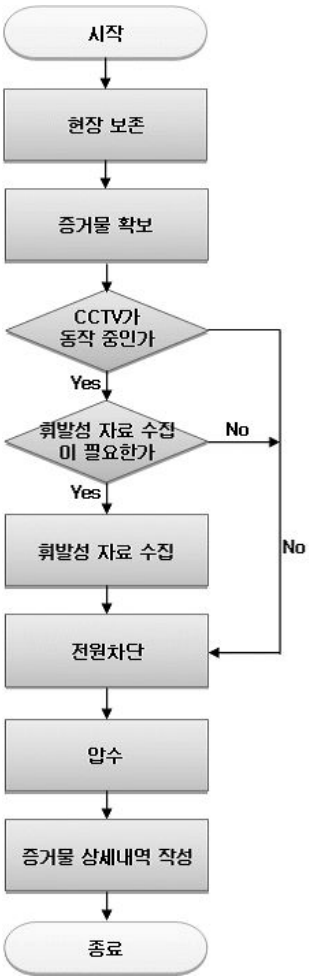
라. 데이터베이스 접속 프로그램 및 로그 분석 프로그램을 사용하여 자료 구조, 자료 관계, 접속자, 사용 내역, 자료 복구 등을 목적에 맞게 실행하고 증거를 획득한다.

마. 데이터베이스 분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록한다.

9.3. CCTV

9.3.1. CCTV 증거자료 수집

CCTV에 저장된 디지털 데이터를 수집하는 과정은 아래 (그림 9-5)와 같다.



(그림 9-5) CCTV 데이터 수집 절차

가. 사용된 운영체제 및 멀티미디어 증거의 종류, 설정 정보를 확인한다.

나. CCTV의 회사명 및 제품 정보를 확인하고 자료가 저장되는 컴퓨터의 통신 및 전원을 차단한다.

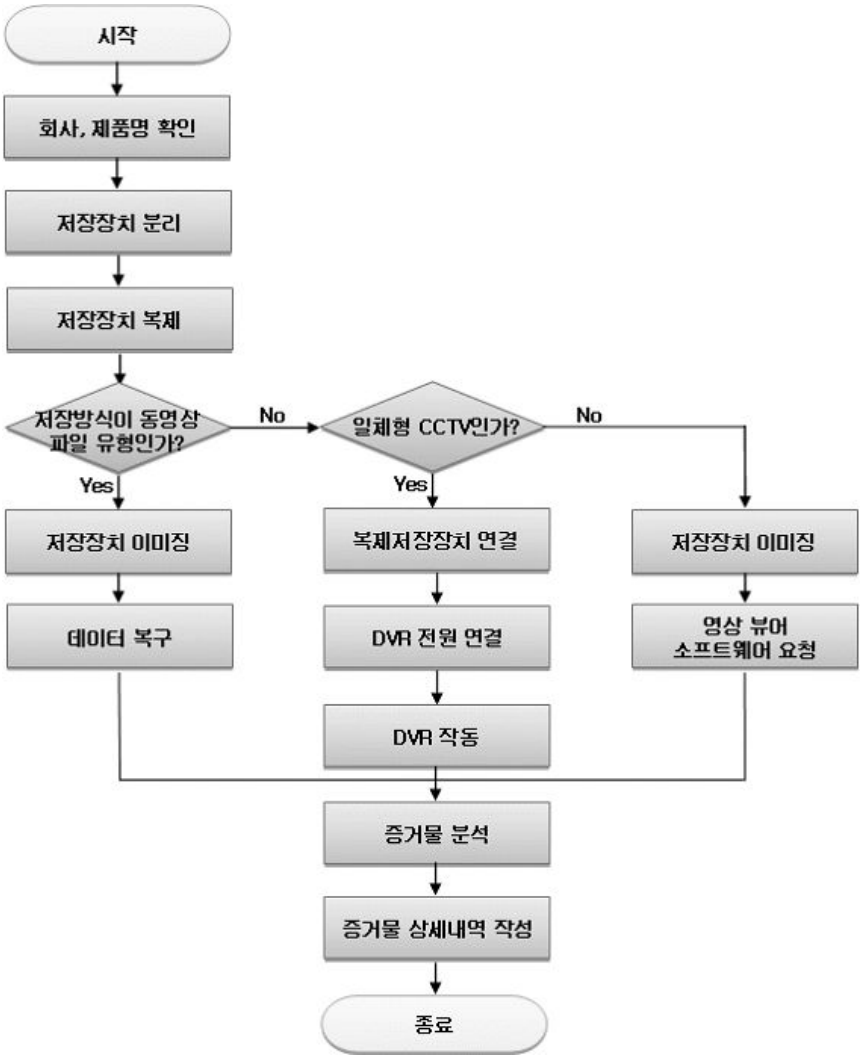
다. 운영 중인 CCTV에서 증거를 수집해야 할 경우 설정 파일 및 동영상 파일을 수집한다.

라. CCTV 제품을 동작할 때 필요한 하드웨어를 수집한다.

마. CCTV 자료가 저장되는 저장장치 또는 수집된 파일들의 해쉬값을 계산, 기록, 확인 후 보관한다.

9.3.2. CCTV 증거 분석

수집된 CCTV 데이터를 이용한 증거 분석 과정은 아래 (그림 9-6)과 같다.



(그림 9-6) CCTV 증거 분석 절차

가. 수집된 CCTV 증거의 복사본 및 증거 파일의 해쉬값을 생성하고 수집 시 작성된 문서에 기재된 값과 비교한다.

나. CCTV 증거의 종류에 따른 분석 프로그램을 구축하고 증거 파일을 복사 및 복제한다.

다. 삭제된 동영상 파일을 복구할 경우 파일 시스템 또는 동영상 저장 방식에 따라 복구한다.

라. CCTV 분석 프로그램 및 응용 프로그램을 사용하여 사용 파일 및 동영상 파일을 분석한다.

마. 설정 정보, 동영상 내용 등을 분석하여 사용 시간대, 수사와 관련된 동영상 존재 여부 및 내용 확인 등을 목적에 맞게 분석하고 증거를 획득한다.

바. CCTV 분석의 분석자, 분석 과정, 분석 결과 등의 세부 사항을 빠짐없이 기록한다.

표준작성 공헌자

표준 번호 : TTAS.KO-12.0058

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	ETRI
표준 초안 제출	이석희	PG102 위원	016-860-5964 gosky7@korea.ac.kr	고려대학교
	길연희	PG102 위원	042-860-1031 yhgil@etri.re.kr	ETRI
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	ETRI
	은성경	PG102 부의장	042-860-5741 skun@etri.re.kr	ETRI
	홍도원	PG102 위원	042-860-6147 dwhong@etri.re.kr	ETRI
	인재형	PG102 참관자	02-3438-6600 injazz@finaldata.com	파이널데이터
	원유재	PG102 의장	02-405-5360 yjwon@kisa.or.kr	KISA
		외 프로젝트그룹 위원		
표준안 심의	정교일	공통기반 기술위원회 의장	kyoil@etri.re.kr	ETRI
	김응배	공통기반 기술위원회 부의장	ebkim@etri.re.kr	ETRI
	원유재	공통기반 기술위원회 부의장	02-405-5360 yjwon@kisa.or.kr	KISA
	이필중	공통기반 기술위원회 부의장	054-279-2232 pjl@postech.ac.kr	포항공대

		외 공통기반 기술위원회 의장		
사무국 담당	김 선	팀 장	031-724-0080 skim@tta.or.kr	TTA
	오흥룡	과 장	031-724-0083 hroh@tta.or.kr	TTA

정보통신단체표준

컴퓨터 포렌식 가이드라인
(Computer Forensics Guideline)

발행인 : 김원식
발행처 : 한국정보통신기술협회
463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0114, Fax : 031-724-0119
발행일 : 2007.12