디지털 증거 처리 가이드라인

고려대학교 디지털포렌식연구센터

목차

1. 디지털 증거 처리

A. 서론

디지털 포렌식의 주목적은 디지털 증거의 추출과 제출시 법정 유효성을 확보하는 것이다. 또한 디지털 증거는 일반 증거의 속성과는 근본적으로 다른 처리 방법이 요구된다. 원본과 사본의 구분이 불가능하며 일반 증거물에 비해 위·변조가 용의하다. 또한 부주의한 취급으로 인하여 증거력이 훼손될 가능성이 크다. 따라서 디지털 증거 처리 과정의 실수를 최소화하기 위해서 디지털 증거 처리 표준절차 확립과 절차에 대한 교육이 중요하다. 본 디지털 증거 처리 가이드라인은 디지털 증거의 획득, 이송, 수집, 분석에 있어 필요한 절차와 준수 사항을 정한다.

B. 목적

본 문서의 표준 절차는 디지털 증거를 획득, 이송, 수집, 분석에 있어 필요한 절차와 준수사항을 정하는데 목적이 있다.

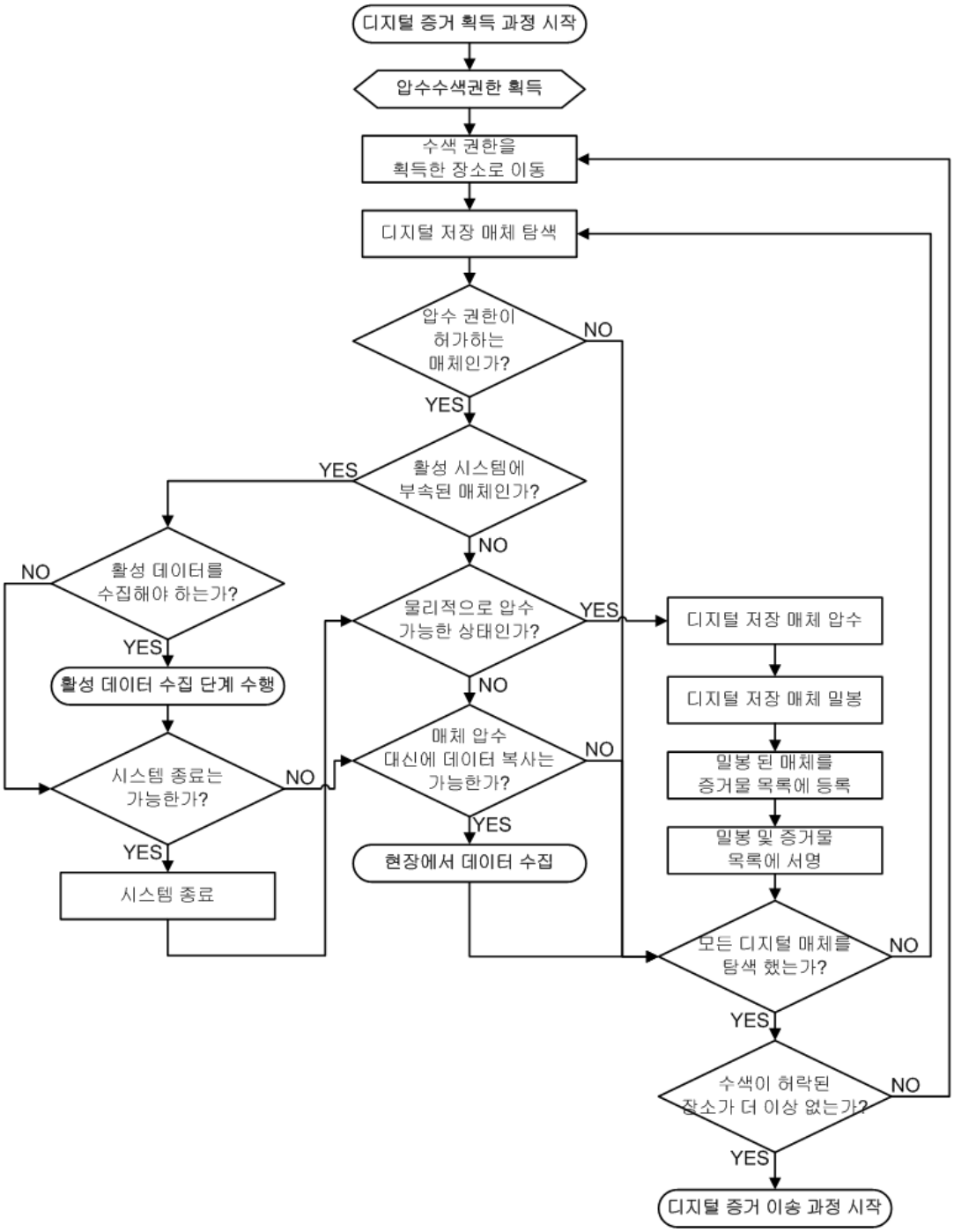
C. 적용범위

이 표준 절차는 디지털 증거를 적법 절차에 따라 수집·분석·보관하는 등(이하 ' 디지털 증거 처리') 디지털 증거 취급과 관련된 각종 조사 행위에 적용된다.

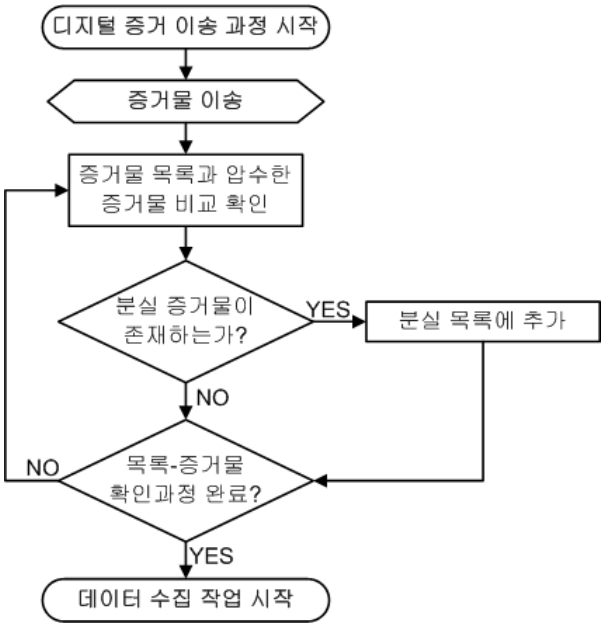
D. 용어 정의

- '디지털 증거'라 함은 컴퓨터 또는 기타 디지털 저장매체에 저장되거나 네트워크를 통해 전송중인 자료로서 조사 및 수사 업무에 필요한 증거자료를 말한다.
- '디지털 증거 분석'이라 함은 컴퓨터 또는 기타 디지털 저장매체에 남아있는 자료에 대한 원본 보존과 사건 관련 증거를 과학적인 절차를 통하여 추출, 검증. 판단하는 조사 및 수사과정을 말한다.
- '휘발성 증거'라 함은 컴퓨터 실행시 일시적으로 메모리 또는 임시파일에 저장되는 증거로 네트워크 접속 상태·프로세스 구동상태·사용중인 파일 내역 등 컴퓨터 종료와 함께 삭제되는 디지털 증거를 말한다.
- '비휘발성 증거'라 함은 컴퓨터 종료 시에도 컴퓨터 또는 기타 디지털 저장매체에 삭제되지 않고 남아있는 디지털 증거를 말한다.
- '기타 디지털 저장매체'라 함은 플로피 디스크, 휴대폰, USB 메모리 등 컴퓨터 하드디스크 외의 디지털 저장매체를 말한다.

2. 디지털 증거의 획득 및 이송 절차



(그림 1) 디지털 증거 획득 과정



(그림 2) 디지털 증거 이송 과정

디지털 증거획득 및 이송 절차는 디지털 정보를 포함하고 있는 매체를 증거로서 확보하고 법적 증거 가치가 훼손되지 않도록 이송하는 과정을 설명하고 있다. 디지털 증거획득은 (그림 1)과 같은 절차를 따르고 획득한 증거 이송 절차는 (그림 2)와 같은 절차를 따른다. 본 절차에서 핵심은 디지털 증거가 법적 효력을 유지해야 한다는 점에 있다. 법적 증거로서의 효력을 유지시키기 위해서는 다음 사항들이 지켜져야만 한다.

- **적법절차의 준수**
  압수·수색권한 혹은 영장이 제한하는 영역 내에서 증거물을 압수해야 한다. 압수·수색권한은 수색범위와 압수 가능한 물건을 제한하고 있다.

- **원본의 안전한 보존**
  증거물이 물리적인 충격에 의해 손상을 입지 않도록 포장에 주의를 기울여야 한다.

- **증거의 무결성 확보**
  증거의 변조·훼손 등이 발생하지 않았음을 입증하기 위해서 증거 획득 과정과 이송 과정에 제 3자 입회인을 두어야 한다.

A. 디지털 증거 획득 절차

I. 준비사항

본 절은 디지털 증거 획득에 앞서 필요한 준비사항에 대해서 설명한다.

- **압수·수색권한(혹은 영장) 획득**
  디지털 포렌식 조사가 민간기관의 의뢰일 경우, 그 기관의 의사결정 기구로부터 디지털 증거를 압수·수색 할 수 있는 권한을 확보한다. 반면에 국가기관으로부터의 의뢰(혹은 명령)일 경우, 법원에 압수·수색영장을 신청 혹은 법원으로부터 명령장을 받는다.

- **증거 수집 및 이송에 필요한 인원 확보**
  수집대상에 대해서 전문지식이 있는 사람들로 수집팀을 구성하거나 상황이 여의치 못하면 적어도 지휘자만은 전문가로 선임해야 한다. 또한 제 3자 입회인을 확보하여 증거 획득 및 이송 절차 과정에 불법 행위가 없었음을 증명할 수 있도록 해야 한다.

- **증거 수집 및 이송에 필요한 장비 확보**
  활성 데이터를 확보하기 위해 사용될 휴대용 컴퓨터와 소프트웨어, 증거 운반용 박스, 증거를 포장할 각종 봉투와 충격흡수소재, 밀봉된 증거물의 무결성을 증명할 특수테이프(Evidence Tape)와 실(Seal), 현장 촬영을 위한 카메라와 캠코더, 분해와 해체를 위한 공구, 서류작성을 위한 각종 서식과 휴대용 프린터 등을 확보해야 한다.

II. 디지털 저장 매체의 종류

본 절은 (그림 1)의 '디지털 저장 매체 탐색' 단계에서 탐색할 디지털 저장 매체의 종류를 설명한다. 또한 압수과정에서 주의해야 할 점을 지적하고 있다.

1. 저장 장치를 포함하고 있는 시스템

가) 컴퓨터

컴퓨터는 개인 사용자가 사용하는 워크스테이션 컴퓨터와 다수의 사용자가 접속해서 사용하는 서버 컴퓨터로 구분된다. 두 종류의 컴퓨터 모두 다수의 하드디스크가 내장되어 있으며 이 하드디스크가 압수수색에서 가장 중요한 대상이다. 일반적으로 컴퓨터에서 하드디스크를 분리하여 디스크만 압수해야 하지만, 레이드(Raid) 시스템을 운영하는 환경의 컴퓨터나 서버의 경우 그 환경이 특수하므로 분석을 위해서는 컴퓨터 자체를 압수해야 한다. 또한 하드디스크 분리 시 그 안의 내용을 자동으로 파괴시키는 구조의 컴퓨터도 고려해야 하기 때문에 가능한 컴퓨터 안의 하드디스크는 컴퓨터 그 자체를 압수하는 것이 바람직하다.

간혹 컴퓨터가 장착하고 있는 CD/DVD 장치 안에 CD나 DVD가 들어있기도 하기 때문에 주의를 해야 한다. 컴퓨터와 이동식 저장 매체는 각각 다른 증거

물로 관리되기 때문이다. 따라서 CD/DVD 장치 외에 이동식 저장 매체를 위한 장치가 더 장착되어 있다면 모두 점검해봐야 할 것이다.

(그림 3) 다양한 형태의 컴퓨터

나) 노트북

수색 현장에서 발견한 노트북은 배터리를 분리시킨 후 노트북 그 자체를 압수하도록 한다. 노트북 역시 컴퓨터 구조가 독특한 경우가 있기 때문에 노트북 하드디스크만 분리하여 압수하기보다는 컴퓨터 자체를 압수하는 것이 좋다. 노트북 역시 이동식 저장 매체를 위한 장치가 장착되어 있기 때문에 삽입되어 있는 매체가 존재하는지 주의를 기울여야 한다. 참고로 노트북의 경우에는 소형 메모리 카드를 위한 장치가 기본적으로 장착되어 있다.

(그림 4) 노트북의 형태

다) 이동전화(Cellular Phone)

이동전화 안에는 플래시 메모리가 내장되어 있으며 평소 이동전화를 사용하며 저장하는 정보는 대부분 이 저장매체 안에 기록된다. 따라서 이동전화 압수 시에는 기기 자체를 압수해야 한다. SIM(Subscriber Identity Module Card)

혹은 USIM(Universal Subscriber Identity Module Card) 메모리 카드를 장착하고 있는 이동전화도 존재하는데 이런 경우 기기와 메모리 카드 각각을 분류해서 압수해야 한다. 최근 3G 휴대폰의 경우 USIM 메모리 카드는 필수적으로 내장되어 있다는 점을 참고한다.

이동전화 압수과정 시 주의해야 할 점이 있는데 무선 신호로 인한 플래시 메모리의 무결성이 훼손되는 것을 방지하기 위해 반드시 전원을 하거나 전파 차단용 봉투나 이동용 전파 차단 장치에 넣어서 압수해야 한다.

(그림 5) 전파 차단 봉투와 장치

라) 개인 휴대용 정보 단말기(PDA)

개인 휴대용 정보 단말기는 내부 저장 장치로 플래시 메모리를 장착하고 있는 작은 컴퓨터이다. 또한 내장된 플래시 메모리 외에 소형 메모리 카드를 삽입해서 사용할 수 있다. 게다가 이동전화와 같은 통신기능이 포함되어 있으면 이를 특별히 스마트 폰(Smart Phone)이라 부른다.

통신기능이 없는 PDA의 경우 소형 메모리 카드가 삽입되어 있는지를 확인한 후 각각을 압수하도록 한다. 스마트 폰의 경우에는 이동전화와 같은 속성을 가지기 때문에 전원을 차단하거나 전파 차단 후 압수를 해야 한다(본 절의 C 항목을 참고한다).

(그림 6) PDA(Personal digital assistant)

마) 디지털 캠코더 & 카메라

디지털 캠코더 및 카메라는 영상 및 사진 정보를 담는 기기로서 포렌식 수사 관점에서 볼 때 컴퓨터의 하드디스크만큼이나 중요한 증거대상이다. 이 기기들은 내부적으로 플래시 메모리를 장착하고 있으나, 실제 영상이나 사진 데이터는 소형 메모리 카드를 통해 저장하고 있다. 따라서 디지털 캠코더와 카메라 기기의 경우 필요하다고 판단되면 압수하도록 하되, 그 안에 삽입되어 있는 메모리 카드는 반드시 분리하여 따로 압수해야 한다.

(그림 7) 디지털 캠코더

바) 휴대용 멀티미디어 플레이어(PMP)

휴대용 멀티미디어 플레이어의 경우 개인 휴대용 정보 단말기(PDA)와 비슷한 개념의 기기이지만 멀티미디어 기능에 있어서 더욱 강력하다. 따라서 PMP 종류에 따라 하드디스크를 저장하고 있는 기기도 존재한다. 따라서 압수 시 PMP 기기 자체를 압수해야 하며 기기에 따로 삽입된 메모리 카드가 있다면 분리하여 또 하나의 증거매체로서 확보해야 한다.

(그림 8) PMP(Portable Media Player)

사) MP3 플레이어

MP3 플레이어는 그 형태가 USB 메모리와 거의 흡사하다. 내장된 플래시 메모리 일부에 작은 운영체제와 미디어 플레이어를 탑재하고 나머지 영역에 음악과 같은 데이터 파일을 저장할 수 있도록 설계되어 있다. 몇몇 MP3 플레이어는 대용량의 데이터 저장을 지원하기 위해서 소형 하드디스크를 탑재하고 있기도 하다. 따라서 MP3 플레이어는 기기 자체를 압수해야 한다.

(그림 9) MP3 플레이어

아) 전자사전

근래 전자사전은 영상 및 음성 파일을 저장 시킬 수 있을 정도의 플래시 메모리가 내장되어 있다. 또한 소형 메모리 카드를 삽입 할 수 있는 장치를 내장하고 있기 때문에 압수의 대상이 된다. 압수 시 메모리 카드가 삽입되어 있는지 확인하고 기기와 메모리카드 각각을 증거로서 획득해야 한다.

(그림 10) 전자 사전

자) 게임 콘솔(Game Console)

Wii, PlayStation, X-Box등의 비디오 게임 콘솔은 자체적으로 하드 디스크를 내장하고 있기 때문에 영상이나 음성 데이터를 저장시킬 수 있다. 게다가 비디오 게임 콘솔을 일반 컴퓨터로 개조해서 사용 가능한 방법도 알려져 있기 때문에 게임 콘솔은 압수해야 하는 대상이다. PSP(PlayStation Portable), NintendoDS등의 휴대용 게임 콘솔도 마찬가지로 플래시 메모리를 내장하고 있으므로 압수대상이 되어야 한다.

(그림 11) Play Station 2

2. 이동식 저장 장치

가) 하드디스크

하드디스크는 컴퓨터의 보조기억장치 중에 하나이다. 일반적으로 컴퓨터에 내장되어 있지만 근래에는 외장형 하드디스크도 많이 사용되고 있다. 가장 많이 사용되는 저장매체이기 때문에 수사관점에서 제 1순위 압수 대상이다. 하드디스크는 자기와 충격에 취약하므로 취급에 주의가 필요하다.

(그림 12) 하드디스크

나) CD / DVD

CD / DVD는 현재 가장 널리 사용되는 보관용 보조기억매체이다. 값이 저렴하고 보관이 용이하기 때문이다. 하드디스크처럼 민감한 보조기억장치는 아니지만 데이터를 저장하고 있는 면이 손상되면 안되므로 취급에 주의를 기울여야 한다. 또한 여러 개가 한묶음으로 있는 경우가 많으나 인수인계시 확인할 수 있게 개별 포장하여야 한다.

다) 플래시 메모리

플래시 메모리는 크게 USB 메모리와 소형 메모리 카드로 구분된다. USB 메모리는 USB 인터페이스 방식을 이용해 데이터를 전송하는 플래시 메모리 기기를 말한다. 근래 휴대용 저장매체로서 각광을 받고 있다. 소형 메모리 카드는 CF, SD, SM, XD, Memory Stick, Micro SD 등으로 구분되며 제조사만의 인터페이스를 이용해 데이터를 전송하는 플래시 메모리 기기이다. 일반적으로 디지털 기기의 저장 매체로서 사용된다.

플래시 메모리는 그 특징상 크기가 매우 작기 때문에 휴대성이 좋으며, 범죄자가 증거물을 쉽게 은닉할 수 있다. 따라서 압수·수색 시 USB 메모리나 소형 메모리 카드를 숨길만한 장소까지 주의를 기울여 수색해야 할 것이다. 또한 리더기도 함께 압수해야 한다.

(그림 13) 소형 메모리 카드

라) 플로피 디스크

플로피디스크는 컴퓨터의 고전적인 보조기억장치 중에 하나이다. 현재는 거의 사용되지 않고 있지만 아직도 광디스크(MO)등은 사용되고 있는 추세이다. 광디스크의 종류로는 잘 알려진 Zip 드라이브와 Jazz 드라이브 등이 존재한다.

(그림 14) Zip 드라이브

마) DAT

DAT(Digital Audio Tape)는 오디오 샘플을 전문가 수준의 품질을 유지하면서 디지털 형태로 기록하기 위한 표준매체이다. 하지만 고용량의 보조기억 장치로서 대용량 서버의 백업 테이프로도 사용되고 있다. 모양은 (그림 15)와 같은 작은 테이프와 원형 테이프의 형태 등이 존재한다.

(그림 155) DAT(Digital Audio Tape)

바) 기타

음성자동전화기와 CCTV도 압수해야 한다.

III. 활성 데이터 수집여부 판단

활성 데이터란 작동중인 컴퓨터에서 오직 휘발성 디지털 저장 매체에만 그 정보가 기록되고, (ii)절에서 언급한 비 휘발성 디지털 저장 매체에는 기록되지 않는 디지털 정보를 뜻한다. 활성 데이터는 원본 데이터가 존재하지 않기 때문에 증거력이 떨어지지만 압수한 디지털 저장 매체를 분석하는데 결정적인 도움을 제공 할 수 있기 때문에 필요하다면 반드시 획득해야 한다. 하지만 활성 데이터 수집활동은 디지털 저장 매체 안의 데이터를 소량 변경시키기도 하기 때문에 활성 데이터가 필요 없는 경우에는 피하는 것이 좋다.

활성 데이터를 수집해야 하는지에 대한 판단은 사건을 기준으로 다음과 같은 정보가 필요한지 아닌 지로 결정한다; 활성 시스템에서 동작중인 프로세스 정보, 시스템에 로그인 시도 중인 사용자 정보, 활성 시스템의 네트워크 정보, 시스템이 사용중인 파일들의 리스트 등 활성 시스템을 종료 시켰을 때 사라지는 데이터 모두. 활성 데이터 수집이 결정되면 (그림1)의 흐름대로 활성 데이터 수집 단계를 수행 한 후 계속해서 디지털 증거 획득 절차를 수행한다.

IV. 활성 시스템 종료 방법

활성 시스템의 종료 방법은 크게 두 가지로 구분된다. 하나는 전원 플러그를 차단하는 방법(pulling the plug)이고 다른 하나는 운영체제의 정상적인 종료 과정을 통한 방법이다. 일반적인 워크스테이션의 경우 전자의 방법을 사용하는 반면 서버나 데이터베이스가 운영되고 있는 워크스테이션의 경우에는 후자의 방법을 사용한다. 데이터베이스의 경우 정상적인 종료를 거치지 않으면 많은 데이터가 훼손되기 때문이다. 하지만 정상적인 종료 절차는 운영체제가 활성 상태일 동안 저장되었던 임시 데이터를 지워버리거나 하드디스크를 정리하는 문제가 있다.

전원 플러그를 차단하는 방법은 간단하다. 컴퓨터의 전원을 순간적으로 차단하기만 하면 되기 때문이다. 보통 컴퓨터에서 전력선을 뽑는 과정을 통해서 수행을 하는데 여기서 주의해야 할 점은 반드시 컴퓨터 쪽 코드를 뽑아야 한다는 것이다. 왜냐하면 UPS(Uninterruptible power supply)가 장착된 PC의 경우 벽 쪽 코드를 뽑는다면 바로 UPS가 작동되면서 증거물 컴퓨터의 시스템에 변화를 줄 것이기 때문이다. 컴퓨터의 전원 플러그를 차단 할 때는 항상 컴퓨터 쪽 선을 뽑도록 해야 한다.

정상적인 과정을 통해 컴퓨터의 전원을 종료시킬 때는 종료시킬 시스템의 운영체제가 무엇인지 파악하는 일이 중요하다. 운영체제마다 종료 방법이 조금씩 다르기 때문이다. 또한 DOS, Windows 3.1, Windows 95, Windows NT Workstation, Windows NT Server, Windows 98/ME, Windows 2000, Windows XP, Windows Vista의 경우 일반적인 워크스테이션으로 사용되기 때문에 전원 플러그를 차단하는 방법을 사용하는 것이 권장된다. Windows 2000 Server나 Windows 2003 Server의 경우 대부분 서버나 데이터베이스를 운영하는 워크스테이션으로 사용되기 때문에 정상적인 종료 과정을 통해 시스템을 종료시켜야 한다.

V. 디지털 저장 매체 밀봉

압수한 디지털 저장 매체에 대한 밀봉 목적은 두 가지이다. 첫 번째로 물리적인 충격에 의한 증거 훼손을 막기 위한 목적으로 수행된다. 예를 들어 하드 디스크나 플로피 디스크 등은 충격이나 전자기에 약하기 때문에 정전기 방지 봉투와 충격흡수 소재를 통해 포장해야 할 것이다. 다른 하나는 증거 획득과 이송과정에서 증거물에 대한 위·변조가 없었음을 증명하기 위해서이다. 증거물의 밀봉을 뜯고 증거물을 변조한다거나 훼손시키는 일을 막기 위해서 일반적으로 밀봉전용 특수 테이프(Evidence Tape)와 실(Seal)이 사용된다.

다음은 각 디지털 저장매체 마다 밀봉하는 방법과 주의사항을 나열하고 있다.

- 대형 디지털 기기

  대형 디지털 기기로는 컴퓨터와 노트북 비디오 게임 콘솔 등이 있다. 대형 디지털 기기들의 밀봉 절차는 다음과 같다. 각각 증거물 번호를 부

여 한 후 증거물에 대한 정보가 담긴 이름표(이하 태그)를 붙인다. 그리고 박스와 충격흡수소재를 이용해 견고한 포장을 한다. 오래된 컴퓨터의 경우 종종 케이스가 없거나 일부가 소실된 경우가 있는데 이런 경우 컴퓨터 내부에 손이 닿지 않도록 모든 면을 감싸는 과정도 필요할 것이다. 포장이 완료되면 밀봉전용 특수 테이프로 포장의 모든 면을 둘러쌓음으로써 무결한 상태를 만든다.

- 소형 디지털 기기

  소형 디지털 기기로는 이동전화, PDA, 디지털 캠코더 및 카메라, PMP, MP3 플레이어, 전자 수첩 등을 들 수 있다. 소형 디지털 기기들의 밀봉 절차는 다음과 같다. 각각 증거물 번호를 부여 한 후 태그를 붙인다. 그리고 적절한 크기의 증거물 봉투에 담은 후 특수 테이프(Evidence Tape) 혹은 실(Seal)을 이용해 봉투를 완전 봉한다. 한번 봉한 봉투는 테이프 혹은 실의 손상 없이는 열수 없어야 하며 이들은 복제가 무척 어려워야 한다.

- 이동식 저장장치

  이동식 저장장치는 Hard-Disk, CD/DVD, 플래시 메모리, 플로피 디스크 등을 말한다. 이동식 저장장치를 밀봉 할 때 주의해야 할 점은 아무리 작은 매체라 해도 한 개씩 밀봉전용 봉투에 넣고 밀봉해야 한다는 점이다. 먼저 이동식 저장장치에 증거물 번호를 부여 한 후 태그를 붙인다. 그리고 적절한 크기의 증거물 봉투에 담은 후 특수 테이프(Evidence Tape) 혹은 실(Seal)을 이용해서 밀봉을 완료한다.

  만약 정전기에 약한 매체라면 반드시 정전기방지 봉투를 이용해 먼저 포장을 한 후 밀봉을 해야 한다. 하드디스크와 같이 취급에 주의를 기울여야 하는 매체는 전용 플라스틱 박스에 매체를 담고 특수 테이프로 모든 면을 둘러 쌓음으로써 무결한 상태를 만든다.

VI. 증거물 목록 작성

압수한 디지털 저장 매체들의 목록 작성은 밀봉과정 중에 같이 수행된다. 디지털 저장 매체를 밀봉하기 직전 그 매체에 증거물 번호를 부여하고 목록에 기록한다. 증거물 목록에는 증거물 번호 외에 증거물을 압수한 장소와 증거물의 종류, 제조사, 모델명, 일련번호 등이 기록되어야 한다. 주의할 점은 인수인계를 위해 모든 증거물은 개별적으로 포장하고 목록을 작성해야 한다. 또한 증거물 목록에는 밀봉과정에 입회한 제3자 입회인 서명과 현장을 지휘한 책임자의 서명이 필요하다.

VII. 증거물 서명 절차

밀봉이 완료된 증거물에 서명을 하는 절차는 디지털 저장 매체 밀봉 과정 및 증거물 목록 작성 과정과 함께 수행된다. 증거물에 서명을 하는 이유는 크게 두 가지인데 하나는 밀봉상태가 각 디지털 저장 매체에 적합하고 올바른지에 대한 점검을 위해서이고 다른 하나는 증거물 조작을 방지하기 위해서이다. 봉인의 훼손 후 재봉인을 어렵게 하기 위해서 사람의 서명이 필요한 것이다. 따라서 모든 증거물은 각각 제3자 입회인의 서명이 들어가야 하며 입회인은 각 증거물을 서명하면서 밀봉에 문제가 없는지를 검토해야 한다.

B. 디지털 증거 이송 절차

디지털 증거 이송 절차에서 가장 핵심적인 것은 획득한 증거물의 무결성 유지와 훼손방지이다. 또한 증거물의 누락 및 도난이 없도록 견고하게 포장하는 일 또한 중요하다.

I. 이송 전

디지털 증거 획득 절차가 완료되면 획득한 증거물들을 기록한 증거물 목록이 완성된다. 증거물 수집 팀으로부터 이송 팀으로 증거물들을 전달 할 때 반드시 이 목록과 전달 할 증거물들을 비교 한 후, 누락된 증거물은 없는지 확인해야 한다. 만약 누락된 증거물이 존재한다면 분실목록에 이를 기록해야 한다. 이송 팀은 증거물을 전달받을 때 각 증거물들의 밀봉전용 특수테이프(Evidence Tape)와 실(Seal)의 상태가 이상 없는지에 대해서도 확인을 해야 한다. 만약 특수테이프나 실이 훼손되었다면 해당 증거물은 증거물 목록에서 제외한다.

모든 증거물의 무결성에도 문제가 없다고 판단되면, 이송 책임자는 증거물 목록에 증거물을 무결한 상태로 전달받았다는 서명을 한다. 참고로 모든 확인 과정에서는 제 3자 입회인이 항상 대기하고 있어야 한다. [표 1]은 각 운영체제별로 정상적인 과정을 통해 시스템을 종료하는 방법을 나열하고 있다.

II. 이송 후

획득한 증거물을 분석팀이 대기하고 있는 장소로 이송 완료 후, 가장 먼저 수행해야 할 일은 이송 전과 같다. 증거물 목록과 증거물간의 비교를 통해 이송 과정 중에 누락 및 도난 된 것은 없는지 알아보는 것이다. 만약 증거물 목록에는 존재하지만 증거물은 존재하지 않는다면 해당 증거물은 사라진 것이 된다. 이 경우 해당 증거물을 분실 목록에 기입한다.

이송 전과 같이 각 증거물들의 밀봉전용 특수테이프(Evidence Tape)와 실(Seal)의 상태를 확인 하는 과정 역시 거쳐야 한다. 이 과정을 통해 증거물들이

이송 과정 중 위·변조되었을지도 모르는 상황을 파악할 수 있기 때문이다. 모든 증거물이 무결하다는 것이 확인되면 이 과정을 지켜본 분석팀 책임자는 증거물 목록에 이상 없이 전달받았다는 서명을 한다. 역시 이 서명이 완료될 때까지 제 3자 입회인은 모든 확인 작업에 참여해야 한다.

3. 사건 초기 대응 및 데이터 수집

일반적으로 현장에서 수집해야 할 데이터는 다음과 같다.

- 휘발성 데이터: 시스템이 켜져 있을 경우에만 수집 가능한 데이터
  - ■ 실행 중인 프로세스 목록
  - ■ 실행 중인 서비스 목록
  - ■ 네트워크 연결 정보
  - ■ 공유 파일 사용 정보
  - ■ RAM 데이터
  - ■ 열린 파일 정보

- 비휘발성 데이터: 시스템 종료 시에도 삭제되지 않는 데이터
  - ■ 컴퓨터 본체 및 하드디스크
  - ■ 디지털 저장매체(CD, USB 메모리, 외장형 하드 디스크, 플래쉬 메모리 등)
  - ■ 이벤트 로그
  - ■ 설정 파일(레지스트리 등)
  - ■ 디스크 메타 정보($MFT, FAT 영역 등)

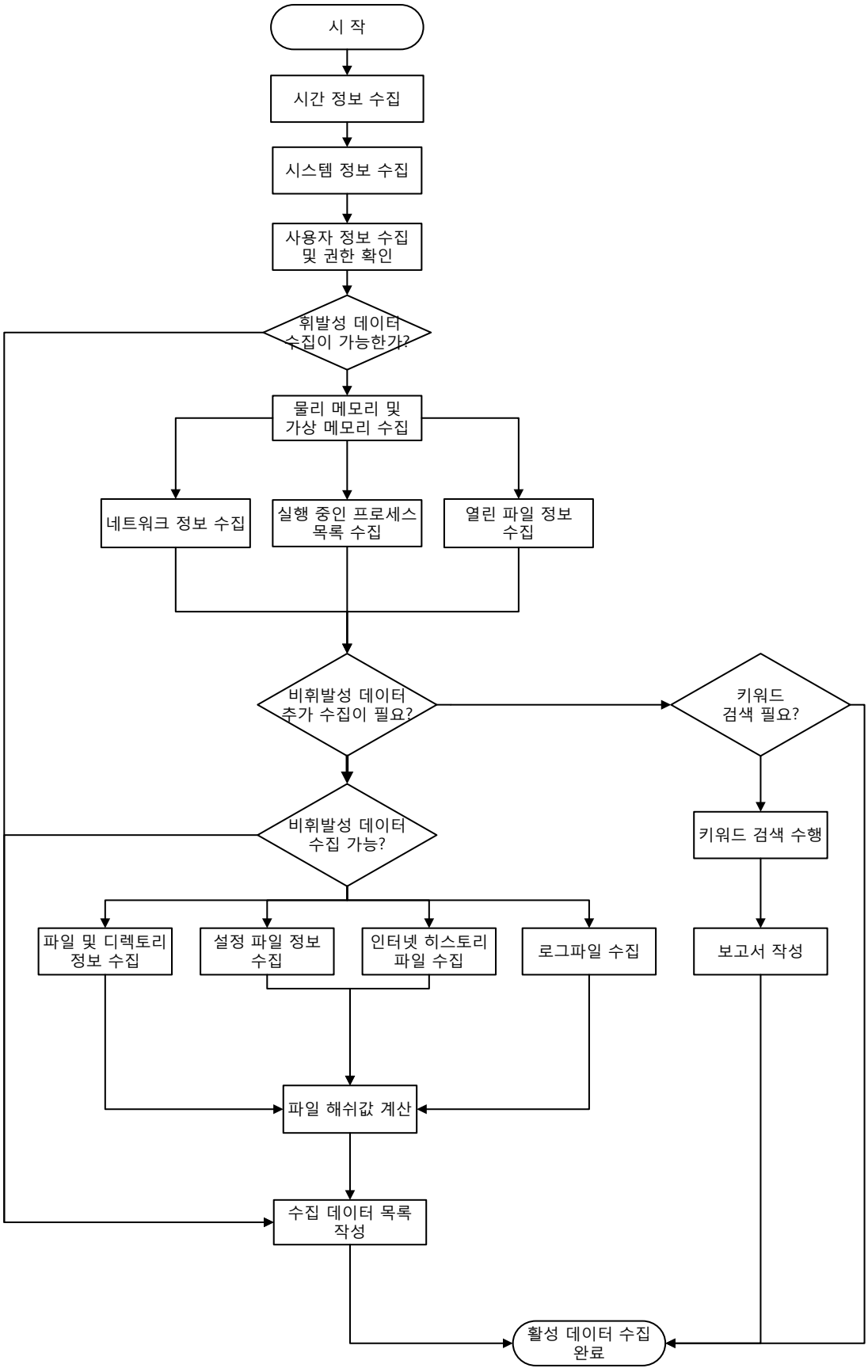
현장의 시스템에 전원이 켜져 있을 때, 상황에 따라 휘발성 데이터를 수집한다.

- 현장의 시스템에 장착된 하드디스크의 용량이 커서 디스크 이미지를 생성하는데 많은 시간이 소요되는 경우
- 침해사고 대응과 같이 RAM 데이터나 네트워크 상태와 같은 정보가 중요한 경우
- 시스템이 루트킷에 감염되어 잘못된 정보를 수집할 가능성이 존재할 경우

하지만 활성 데이터 수집에는 제약사항이 존재하는데, 별도의 하드웨어가 미리 부착되어 있지 않았다면, 수집을 실행하기 위한 도구를 사용해야 하기 때문에 이로 인하여 시스템 메모리를 사용해야 하고, 시스템의 휘발성 데이터를 있는 그대로 수집할 수 없게 된다.

디스크 이미지를 생성하는데 충분한 시간이 없는 경우나 이미지를 생성할 수 없는 환경에 처한 경우, 활성 상태에서 비휘발성 데이터를 선별적으로 수집할 수 있다. 이러한 경우에도 가능한 메타데이터의 훼손을 줄여야 하며, 훼손했을 경우 그 사유를 명시해야 한다.

A. 초기 대응 증거 수집 절차



B. 활성 데이터 수집

I. 시간 정보 수집

수집되는 데이터의 시간 정확성을 보장하기 위해서 시스템의 현재 시간을 수집한다. 시스템의 현재 시간과 실제 시간을 비교하기 위해서 수집된 시간 정보와 정확한 실제 시간 정보와 비교하여 변화를 확인한다. 이때 실제 시간을 알기 위하여 위성에서 휴대전화 시간이나 정확한 시간을 제공해주는 웹 정보를 이용한다.

II. 물리 메모리 및 가상 메모리 수집

물리 메모리는 수시로 변화하고, 이후 데이터 수집 과정에서 변경되기 때문에 활성 데이터 중 가장 먼저 수집해야 한다. 하드디스크에 저장되지 않고 물리 메모리 상에만 존재하는 악성 코드나 이전에 불법적 행위를 수행하면서 남는 흔적들이 존재한다. 수집된 정보는 읽을 수 있는 정보만 추려내는 문자열 추출 과정과 프로세스 관련 정보를 추려내는 과정을 거쳐서 분석을 수행한다. 이때 사용되는 물리 메모리 수집 도구는 반드시 검증된 제품을 사용해야 하며, 수집 후 입회인에게 내용을 설명하고 확인 서명을 받는다.

III. 실행 프로세스 수집

현재 실행 중인 프로세스 정보를 수집하여 의심스럽거나 은닉된 프로세스 정보를 확인한다.

- 이미지 이름
- PID
- 사용자 이름
- 메모리 사용량
- CPU 점유율

하지만 운영체제에서 제공하는 프로세스 매니저만을 이용하여 수집한 경우, 은닉된 프로세스는 탐지하지 못하기 때문에 물리 메모리에서 수집한 프로세스 관련 정보와 함께 분석해야 한다. 물리 메모리에 저장된 프로세스 정보에는 존재하지만, 실행중인 프로세스 정보에는 존재하지 않는 프로세스인 경우에는 다음과 같은 경우가 존재한다.

- 프로세스가 은닉된 경우
- 이전에 실행되었다가 종료된 프로세스

두 경우는 물리 메모리에서 수집한 프로세스 관련 정보에서 프로세스 종료 시간을 검사함으로써 구분할 수 있다. 프로세스 종료 시간이 명시된 경우에는 이전에 실행되었다가 종료된 프로세스라고 판단할 수 있고, Unknown일 경우에 작업 관리자에서 프로세스 정보를 찾을 수 없는 경우는 은닉된 프로세스라고 판단할 수

있다.

IV. 네트워크 정보 수집

악성 코드에 의한 의심스러운 연결이 이루어지고 있는지 확인하기 위해 현재 네트워크 연결 상태에 대한 정보를 수집한다. 또한 외부에서 불법적으로 접근하고 있는 공유 폴더에 대한 정보를 수집해야 한다. 이는 사용자의 의도와 관계없이 외부에서 접근하는 공유 폴더에 대한 정보이다. 또한 인터넷 라우팅 테이블 정보를 수집하여 악성코드에 의한 변조가 이루어졌는지를 확인해야 한다.

V. 열린 파일 정보 수집

실제 프로세스가 동작 중일 때, 사용하는 파일들의 정보를 수집해야 한다. 프로세스는 실행하면서 사용하는 파일 정보를 핸들로 관리한다. 따라서 운영체제에서 사용하고 있는 핸들 정보를 수집함으로써 실제 어떤 파일이 사용되고 있는지를 파악할 수 있다.

VI. 시스템 정보 및 각종 설정 정보 수집

1. 운영체제 정보

운영체제 버전이나 서비스팩 버전 별로 조금씩 상이한 분석 기법이 존재한다. 또한 특정 버전에 대한 알려진 취약점 정보를 파악하기 위해 시스템에서 운영되고 있는 운영체제 버전과 서비스팩 버전을 수집해야 한다. 또한 부팅한 시간정보를 파악함으로써 시스템 사용에 대한 시간 추이를 확인할 수 있다. 따라서 수집해야 할 운영체제 정보는 다음과 같다.

- 운영체제 버전
- 운영체제 서비스팩 버전
- 부팅한 시각
- 부팅 후 운영된 시각

2. IP 설정 정보 수집

시스템이 사용하고 있는 네트워크 환경에 대한 정보이다. 이 정보는 운영되고 있는 네트워크 관련 정보를 비롯하여 네트워크 카드 정보, MAC 주소 정보, NETMASK, 게이트웨이 IP 주소, DNS 서버 정보 등이다.

3. 물리 디스크 사용 정보 수집

시스템에서 사용하고 있는 물리 디스크의 대한 정보이다. 이 정보는 물리 디스크의 개수, 디스크의 용량, 파티션 구조, 파일 시스템 종류, 부팅 가능 여부 정보 등을 수집한다.

VII. 사용자 정보 수집

사용자 정보는 사용자가 시스템을 사용한 흔적을 수집한 정보이다. 이 정보를 분석하면 사용자의 시스템 사용 성향 및 사용 이력을 조사할 수 있다. 계정명과 그룹명, 해당 계정 권한을 확인해야 한다. 또한 사용자가 최근에 사용한 문서목록과 자동 시작 프로그램 목록, 최근 실행 명령을 수집하여 사용자의 행동 패턴을 분석하는데 이용할 수 있다.

C. 비휘발성 데이터 수집

전체 디스크 이미지를 생성할 시간적 여유가 없는 경우 필요한 몇 가지 시스템 파일을 수집한 후 해쉬값을 획득하여 증거력을 보전해야 한다. 수집해야 하는 데이터는 다음과 같다.

I. 파일 및 디렉토리 정보 수집

먼저 파일 시스템의 종류를 파악한 후, 해당 파일 시스템에 맞는 방법을 사용하여 조사를 진행한다. 파일 시스템 분석에서는 불법적인 파일 소지 여부, 삭제한 파일 정보, 정보 유출 파일 소지 여부 등을 조사할 수 있다. Windows에서 주로 사용하는 파일 시스템은 FAT 파일 시스템과 NTFS 파일 시스템이 있다. NTFS 파일 시스템일 경우에는 각 파티션에 대한 $MFT 파일을 수집한다. FAT 파일 시스템일 경우에는 FAT 영역의 데이터를 수집한다.

II. 운영체제 설정 파일 수집

각각의 운영체제는 자신의 설정 정보를 파일로 저장하여 관리하는데, 대표적으로 Windows는 시스템의 설정 정보를 레지스트리에 저장한다. 레지스트리는 C:₩WINDOWS₩system32₩config 디렉토리에 다섯 개의 파일로 존재한다.

- Default: 기본 정보를 저장하는 레지스트리 파일
- SAM: 계정 정보를 저장하는 레지스트리 파일
- SECURITY: 보안 관련 정보를 저장하는 레지스트리 파일
- SOFTWARE: 소프트웨어 정보를 저장하는 레지스트리 파일
- system: 시스템 설정 정보를 저장하는 레지스트리 파일

III. 인터넷 히스토리 파일 수집

분석 시스템의 인터넷 사용 기록을 분석함으로써 사용자의 인터넷 사용 이력을 조사할 수 있다. 각각의 웹 브라우저는 프로그램의 설정 정보를 파일에 저장한다. 주로 Microsoft의 Internet Explorer 5, Internet Explorer 6, Internet Explorer 7, Mozilla의 Firefox 2, Firefox 3, Apple Safari, Google Crome 등을 사용한다. 수집해야 할 데이터는 다음과 같다.

- 쿠키 정보: 웹 사이트의 사용자 정보
- 임시 인터넷 파일: 웹 사이트를 출력하기 위한 임시 파일

- 히스토리: 웹 사이트 접속 목록

IV. 로그 파일 수집

1. IIS 로그

IIS는 Internet Information Server의 약자로 Microsoft 사가 개발하고 배포 중이다. 시스템이 서버로 운영되고 있을 때, 많은 경우 IIS를 이용하고 있다. IIS는 운영되면서 생긴 로그를 다음과 같은 파일에 기록한다.

%WinDir%₩System32₩LogFiles

기본적으로 이 로그 파일은 사람이 읽기 쉬운 ASCII 문서 파일로 기록되기 때문에 분석이 용이하다.

2. Windows 로그 파일

Windows는 각종 설정 정보 및 최초 설치 정보를 로그 파일에 기록한다. 수집해야 할 로그 파일은 다음과 같다.

- Setuplog.txt: Windows 설치 로그
- Setupact.log: Windows 설치 로그
- SetupAPI.log: Windows 드라이버 설치 로그
- Drwtsn32.log: 소프트웨어 오류 로그 정보

3. 이벤트 로그 파일

이벤트 로그는 Windows에서 발생하는 여러 종류의 이벤트를 기록한 파일이다. 이벤트 로그는 C:₩WINDOWS₩system32₩config 디렉토리에 세 개의 파일로 존재한다.

- AppEvent.Evt
- SecEvent.Evt
- SysEvent.Evt

V. Hash값 계산

각각 수집된 시스템 파일은 수집 후, 즉시 해쉬 알고리즘을 이용하여 해쉬값을 계산해야 한다. 이 값은 증거 데이터의 무결성을 유지하기 위해 필요하다.

D. 검색

비휘발성 데이터를 복제할 상황이 안되거나, 필요성이 없을 경우, 활성 시스템 상에서 검색을 통한 정보 수집을 진행한다. 이때, 대상 시스템의 타임스탬프가 변경될 가능성이 존재하므로 신중하게 조사를 진행해야 한다. 해당 폴더에 직접 접근하여 파일을 열거나, 운영체제의 검색 기능을 사용한다.

E. 활성 데이터 수사 고려사항

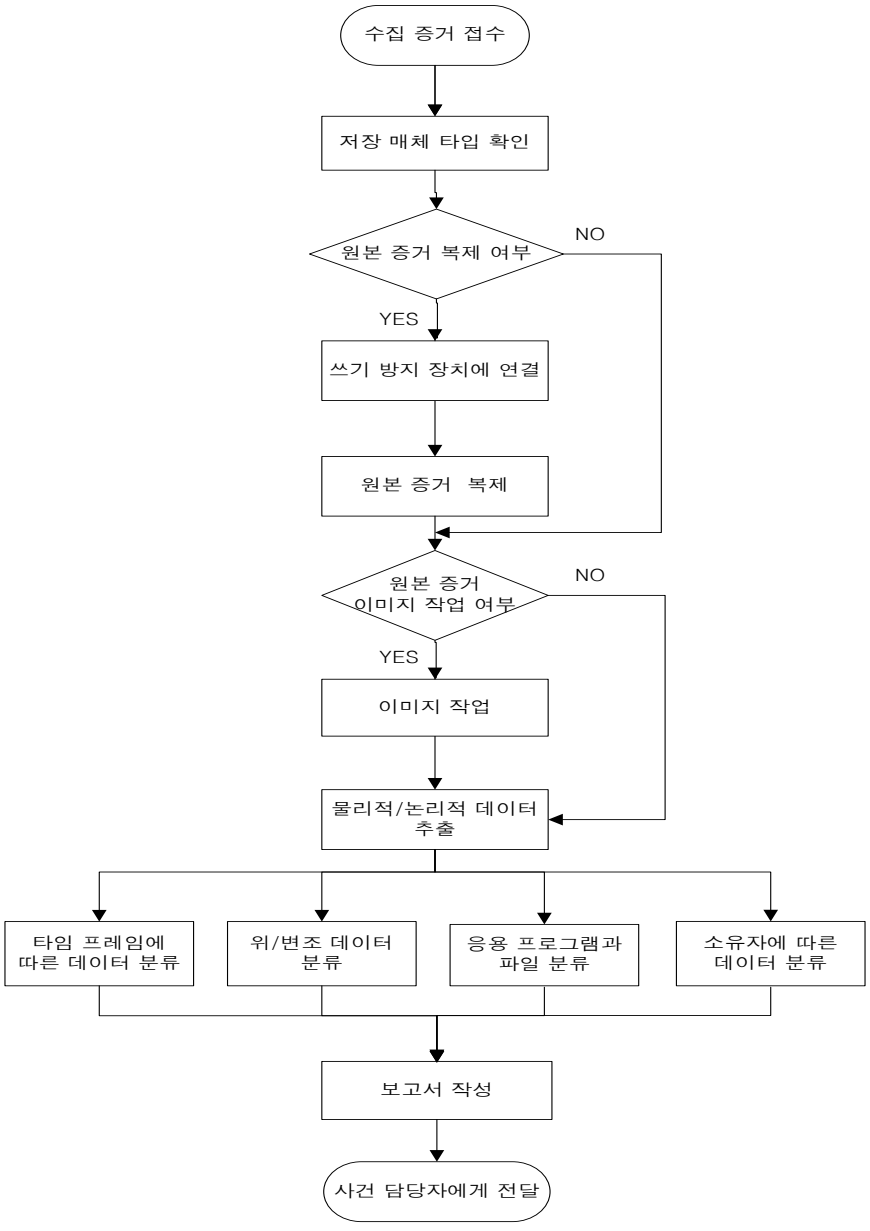
활성 데이터 수사에서 중점적으로 고려되어야 할 사항은 실제 증거 수집 과정에서 시스템을 변경하기 때문에 그 영향을 최소화해야 한다는 것이다. 따라서 믿을 수 있는 검증된 도구를 사용해야 하고, 모든 수집 과정을 기록해 두어야 한다.

다음과 같은 확인사항을 점검하면서 수집을 진행하여야 한다.

- 사용자의 간섭을 최소화 하여 디지털 증거의 수정을 최소화해야 한다.
- 활성 데이터는 휘발성이 높은 것부터 우선적으로 수집해야 한다.
- 우선순위가 중요하지 않거나 비휘발성 데이터인 경우, 전통적인 디지털 증거 수집 방법을 통해서 수집한다.
- 증거 데이터 추출이나 복사는 실제 원본 데이터와 타임스탬프를 변경하지 말아야 한다.
- 활성 데이터 수집 과정의 모든 행위는 기록되어야 한다.
- 수사관이 대상 컴퓨터를 조사하는 과정은 녹화하는 것을 권장하고, 수행한 행위는 기록으로 남겨야 한다.
- 추출된 데이터나 수행된 작업에 대한 기록은 수집 과정이 끝난 후 증거 무결성을 위해서 즉시 해쉬값을 구해야 한다.
- 대상 컴퓨터에서 동작하는 모든 도구는 정상적인 이진파일(the known good binary)임이 검증 된 것만 사용해야 한다. 또한 이 도구들은 최소한의 메모리를 사용하여 실행되어야 한다.

4. 증거 분석 전 준비 단계

디지털 증거의 분석은 조사하여야 할 데이터가 많고, 사건에 따라 조사하여야 할 데이터가 서로 다르므로 많은 시간이 소요될 수 있다. 따라서 데이터 유형에 따라 조사하여야 할 데이터를 분류하고 분류된 데이터를 이용하여 상세 분석을 수행함으로써 신속하고 효율적인 분석이 이루어질 수 있도록 하여야 한다. 디지털 증거 분류를 위해서는 분석 대상 증거물에서 데이터 추출이 선행되어야 한다. 그리고 데이터 추출은 원본 증거물에 대한 무결성을 최대한 유지하면서 수행되어야 한다. <그림 1>은 이송 책임자로부터 디지털 증거를 인계 받은 다음부터 증거 분류까지 일련의 절차를 도식화 한 것이다.



<그림 16> 디지털 증거 분류 과정

A. 증거 추출 전 준비 단계

수집된 증거를 이송 책임자로부터 인계 받고 이상이 없음을 확인하였으면 분석팀은 사건 담당자의 증거 분석 의뢰 내용에 맞게 증거를 분석 하게 된다. 이때 증거물 원본에 대하여 분석을 수행하게 되면 증거물의 무결성에 손상을 줄 수 있으므로 원본과 동일한 분석이 가능하도록 증거물을 복제하여야 하며, 증거 분석의 편의성을 위해 이미지 작업을 수행한다.

I. 증거물 복제

증거물 복제 과정은 원본 증거물을 손상시키지 않는 범위에서 수행되어야 한다. 일반적으로 증거물 복제 과정은 다음 사항들을 준수하여야 한다.

- 원본 증거물의 무결성 유지를 위하여 쓰기방지장치를 사용한다.
- 증거물 복제는 분석용과 보관용을 따로 두어 관리한다.
- 원본 증거물, 분석용 복제 증거물, 보관용 복제 증거물에 대한 해쉬 값을 획득하여 무결성을 유지한다.
- 분석용 복제 증거물과 보관용 복제 증거물에 대한 일련 번호를 기재하고 원본 증거물을 복제하는 일련의 과정을 기록한다.
- 증거물 복제는 입회자가 참석한 가운데 수행되어야 하며, 복제된 증거물과 해쉬 값에 대하여 입회자와 분석 책임자의 서명을 한다.
- 증거물의 복제는 원본 증거물과 동일한 장치에서 수행되어야 하며, 동일한 장치가 없을 경우 원본 증거물과 최대한 비슷하고, 원본 증거물의 모든 기능을 포함하는 장치에서 수행되어야 한다.

II. 이미지 작업

이미지 작업은 분석용 복제 증거물을 이용하여 수행하여야 하며 분석용 복제 증거물을 손상 시키지 않는 범위에서 수행되어야 한다. 이미지 획득 과정은 다음 사항들을 준수하여야 한다.

- 분석용 복제 증거물의 무결성 유지를 위하여 쓰기방지장치를 사용한다.
- 획득한 이미지에 대한 해쉬 값을 획득하여 무결성을 유지한다.
- 이미지 획득은 입회자가 참석한 가운데 수행되어야 하며, 획득한 이미지와 해쉬 값에 대하여 입회자와 분석 책임자의 서명을 한다.

B. 증거 추출 단계

디지털 증거의 추출은 물리적 방법과 논리적 방법으로 나눌 수 있다. 물리적 추출 단계는 파일 시스템과 무관하게 물리적인 장치에서 데이터를 복구하고 식별한다. 논리적 추출 단계는 설치된 운영체제, 파일 시스템, 응용 프로그램에 기반하여 파일과 데이터를 복구하고 식별한다.

I. 물리적 방법

이 단계의 데이터 추출은 장치에 설정되어 있는 파일 시스템과는 무관하게 물리적 수준에서 이루어진다. 여기에는 키워드 검색, 파일 카빙(Carving), 파티션 테이블 추출, 물리적 장치 상의 사용하지 않는 영역 추출 등이 포함될 수 있다.

- 키워드 검색을 수행하여 운영 체제와 파일 시스템이 다루지 않는 데이터를 추출한다.
- 파일 카빙 도구를 사용하여 운영 체제와 파일 시스템이 관리하지 않는 유용한 파일과 데이터를 추출하고 복구한다.
- 파티션 구조 검사를 통하여 현재의 파일 시스템을 식별하고 장치에서 물리적으로 할당된 전체 크기를 결정한다.

II. 논리적 방법

이 단계의 데이터 추출은 드라이브 상의 파일 시스템에 기초하며, 사용 중인 파일, 삭제된 파일, 파일 슬랙, 파일 시스템의 미사용 영역이 포함될 수 있다. 각 단계는 다음을 포함한다.

- 디렉토리 구조, 파일 속성, 파일 이름, 시간과 날짜, 파일 크기, 파일 위치와 같은 특성을 나타내는 파일 시스템의 정보를 추출한다.
- 알려진 해쉬 값과 계산한 해쉬 값 비교를 통해 알려진 파일을 식별하여 제거함으로써 데이터를 축소한다.
- 파일 이름과 확장자, 파일 헤더, 파일 내용, 디스크상의 경로 등을 이용하여 조사에 필요한 파일을 추출한다.
- 삭제된 파일을 복구한다.
- 패스워드로 보호된 데이터, 암호화된 데이터, 압축된 데이터를 추출한다.
- 파일 슬랙에서 데이터를 추출한다.
- 미할당된 영역에서 데이터를 추출한다.

C. 추출 증거 분류 단계

추출 증거 분류는 사건 유형에 따라 분석이 필요한 데이터를 특정 지음으로서 분석을 수행하여야 할 데이터의 양을 줄여 효율적이고 신속한 증거 분석을 가능하게 한다. 분류 방법의 예로 타임프레임(timeframe)에 따른 분류, 위/변조 데이터 분류, 응용 프로그램과 파일 분류, 소유자에 따른 분류 등이 있으며 각각의 분류 방법은 데이터가 서로 중복될 수 있다.

I. 타임프레임에 따른 분류

타임프레임에 따른 분류는 컴퓨터 상에서 사건이 발생한 시점, 사건이 발생한 시기에 컴퓨터를 사용한 자를 결정하는데 유용할 수 있다. 다음과 같은 두 가지 방법을

활용할 수 있다.

- 파일 시스템의 메타정보(마지막 수정 시간, 마지막 접근 시간, 생성 시간, 변경 상태 등)에 포함된 시간과 날짜 정보를 검토하여 수사와 관계된 타임프레임 내에 관심 있는 파일을 분류한다. 이러한 분류 방법의 예로 파일 내용이 마지막으로 변경될 때 설정된 마지막 수정 날짜와 시간의 사용을 들 수 있다.
- 시스템과 응용프로그램의 로그를 확인하여 수사와 관계된 타임프레임 내에 로그를 분류한다. 여기에는 에러 로그, 설치 로그, 네트워크 연결 로그, 보안 로그 등이 있다. 예를 들어 보안 로그의 조사는 사용자가 로그인한 시간을 파악할 수 있다.
  ※ 운영체제에 기록된 시간과 실제 시간의 차이점이 없는지 확인한다.

II. 위/변조 데이터 분류

위/변조 데이터는 컴퓨터 시스템 상에 숨겨질 수 있다. 위/변조 데이터 분류를 위해서는 데이터 탐지와 복구 기술이 필요하다. 대상 시스템에서 위/변조 데이터가 발견되면 사용자가 고의적으로 데이터를 은닉했음으로 수사에 실마리를 제공하는 단서를 획득한 가능성이 높다. 다음과 같은 방법을 활용 할 수 있다.

- 파일 확장자에 대응하는 파일 구조를 비교하여 파일의 이상 유무를 판별한다. 불일치하는 파일의 존재는 사용자가 고의적으로 데이터를 은닉했음을 의미할 수도 있다.
- 패스워드로 보호되거나 암호화된 파일의 획득은 사용자가 데이터를 숨기려고 시도했음을 나타낼 수 있다. 또한 패스워드 그 자체는 해당 파일의 내용만큼 사건과 관련이 있을 수 있다.
- 스테가노그라피 탐지 도구를 이용하여 디스크 상에서 스테가노그라피 기술을 이용한 은닉 데이터가 있는지 확인한다.
- HPA(Host-Protected Area)에 접근한다. HPA에 사용자가 생성한 데이터가 존재하면 데이터를 숨기기 위한 의도라고 판단할 수 있다.

III. 응용 프로그램과 파일 분류

식별된 많은 프로그램과 파일들은 사건과 관련된 정보를 포함할 수 있으며, 컴퓨터 시스템의 사양과 사용자의 컴퓨터 사용 수준을 파악할 수 있다. 분류된 결과들은 추가적인 추출과 분석 과정이 필요할 수 있다.

- 파일 이름 관찰을 통하여 응용프로그램과 파일의 연관성 및 패턴을 조사하여 데이터를 분류한다.

- 파일의 확장자를 조사하여 확장자에 따른 통계치를 검사한다.
- 운영 체제의 종류와 개수의 식별을 통하여 동일한 운영체제 내의 데이터를 분류한다.
- 전체 응용프로그램의 종류와 개수를 식별하고 설치된 응용프로그램과 연관된 파일을 분류한다.
- 서로 관련성이 있는 파일들을 분류한다. 예를 들어, 인터넷 히스토리와 캐쉬 파일은 연관성이 있으며, 이메일 파일과 첨부 파일은 서로 연관성이 있다.
- 알려지지 않은 파일 타입을 식별하여 분류한다.
- 파일의 저장 위치가 디폴트인지 수정된 위치인지를 판단하기 위해서 드라이브의 파일 구조와 응용프로그램의 기본 저장 위치를 검사한다.

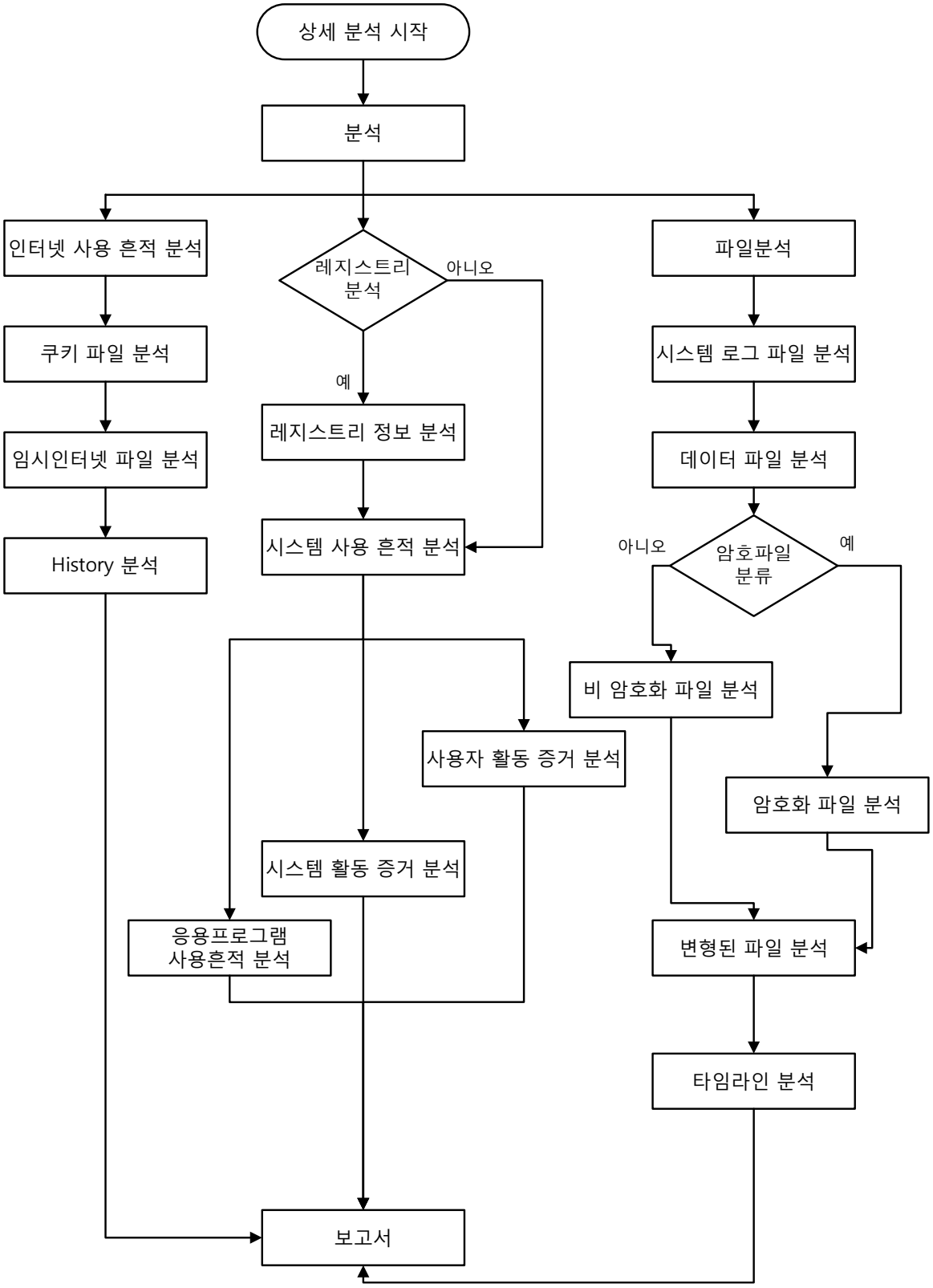
IV. 소유자에 따른 분류

누가 파일을 생성했으며 수정했는지 또는 접근했는지를 식별하는 것은 포렌식 수사에서 필수적으로 조사하여야 할 사항이다. 따라서 의심가는 데이터의 소유자를 판단하는 것은 중요하다. 소유자에 따른 분류 방법은 위의 3가지 방법을 통해 이루어질 수 있다.

- 타임프레임에 따른 분류를 통하여 특정한 시간대의 사용내역을 확인하고 파일의 소유자를 확인하여 분류한다.
- 파일 및 디렉토리의 이름 그 자체는 소유자를 명시할 수 있다.
- 응용프로그램 설치 시 입력한 사용자의 이름을 확인한다.
- 응용프로그램 및 파일 분류를 이용하여 디폴트 위치가 아닌 곳에 저장된 파일을 분류한다. 중요한 파일은 디폴트 위치가 아닌 곳에 저장될 수 있으며 파일 및 디렉토리의 이름은 소유자와 매우 밀접한 관련이 있을 수 있다.
- 암호화되거나 패스워드로 보호된 파일에 접근할 수 있는 패스워드가 복구되었다면, 그 패스워드 자체가 소유자를 가리킬 수 있다.
- 파일 내용에 사용자의 특정 정보가 포함됨으로써 소유자를 판별할 수 있다.

5. 디지털 증거 상세 분석

A. 디지털 증거 상세 분석 절차



B. 인터넷 사용 흔적

I. 개요

웹 브라우저는 인터넷을 사용하기 위한 가장 기본적인 소프트웨어로서 검색, 쇼핑, 통신, 금융, 파일 다운로드, 파일 업로드 등 많은 곳에 사용된다. 웹 브라우저는 대부분의 인터넷 사용 내역을 별도의 파일에 기록한다. 따라서 웹 브라우저 생성 파일을 분석하여 용의자의 웹 브라우저 사용 정보를 조사하면 범죄 행위에 대한 직/간접적 증거를 추출할 수 있다. 또한 최근에는 웹 브라우저의 종류가 다양해지고 있으며 운영체제 종류나 버전에 따라 증거로 사용 가능한 파일들의 위치가 달라지기 때문에 각 운영체제 및 브라우저 간의 차이점을 숙지하고 수사하여야 한다.

II. 인터넷 사용 흔적 증거 수집

Temporary Internet File 폴더는 웹 서버로부터 불러온 임시 파일을 저장하며 Cookies 폴더는 쿠키 파일을, History 폴더는 사용자가 접속한 웹 사이트의 목록을 저장한다. 3곳 모두 index.dat 파일을 통하여 관련 정보를 관리한다. 각각의 index.dat 파일의 구조는 동일 하지만 추출할 수 있는 정보는 서로 다르다. Temporary Internet Files의 index.dat는 임시파일과 웹 메일을 추출할 수 있으며 History의 index.dat는 다운로드 받은 파일의 위치 및 검색어를 추출할 수 있다.

운영 체제	저장 위치
Windows 95/98/Me	₩WINDOWS₩Temporary Internet Files₩Content.IE5 ₩WINDOWS₩Cookies ₩WINDOWS₩History₩History.IE5
Windows NT	₩Winnt₩Profiles₩<사용자 계정 SID>₩Local Setting₩Temporary Internet Files₩Content.IE5 ₩Winnt₩Profiles₩<사용자 계정 SID>₩Cookies ₩Winnt₩Profiles₩<사용자 계정 SID>₩Local Setting₩History₩History.IE5
Windows 2K/XP	₩Documents and Settings₩<사용자 계정 SID>₩Local Settings₩Temporary Internet Files₩Content.IE5₩ ₩Documents and Settings₩<사용자 계정 SID>₩Cookies₩ ₩Document and Settings₩<사용자 계정 SID>₩Local Settings₩History₩History.IE5₩
Windows Vista	₩Users₩username₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5 ₩Users₩username₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5 ₩Users₩username₩AppData₩Roaming₩Microsoft₩Windows₩Cookies

Microsoft Windows 버전에 따른 웹 브라우저 생성 파일 저장 위치

III. 인터넷 사용 흔적 증거 분석

1. Temporary Internet File

Temporary Internet File 폴더는 웹 브라우저의 성능을 높이기 위하여 서버로부터 가져온 임시 파일을 저장하여 놓는다. 이후 같은 서버에서 같은 파일을 가져와야 하는 경우에 저장된 파일을 이용하여 화면에 출력함으로써 속도를 향상시킨다. 구체적으로 Temporary Internet File의 index.dat 파일에서는 저장된 임시파일의 url, 임시파일의 저장위치, 임시파일의 이름, 접속 시간을 확인할 수 있다.

2. History

History 폴더는 사용자가 웹 브라우저를 통해 방문한 URL을 저장한다. 구체적으로 History의 index.dat 파일은 접속한 url, 다운로드 받은 파일, 마지막 방문 시간을 확인할 수 있다. 그리고 이러한 정보를 이용하면 피의자가 어느 시간에 어느 사이트에 방문했는지, 검색 사이트에서 무엇을 검색했는지, 어떤 파일을 다운 받았는지에 대한 정보를 알 수 있다.

3. Cookie

Cookies 폴더는 웹 사이트에서 사용자와 관련된 정보를 사용자의 하드디스크에 저장한다. Cookies 파일의 index.dat 파일에서는 Cookies를 저장하는 사이트의 URL과, 생성 시간, 최근 접근 시간, 정보를 저장하는 쿠키 파일의 이름을 확인할 수 있다. 이를 통해 해당 사이트의 쿠키 파일이름을 확인할 수 있고, 마지막으로 언제 수정되었는지 알 수 있다.

4. 타임라인 분석

용의자는 범죄를 저지르기 전에 관련된 정보를 수집하거나 범죄를 저지른 직후에 상황을 지켜보기 위해서 평소보다 인터넷 사용이 급격한 증가한다. 따라서 인터넷 사용이 평소보다 급격이 증가한 날짜를 중심으로 웹 사용 내역을 분석한다면 신속하고 효율적인 수사가 이루어질 수 있다.

C. 시스템 사용 흔적

I. 개요

하드디스크의 대용량화와 다양한 어플리케이션의 개발로 분석 대상의 정보량과 분석에 따른 시간 비용이 크게 증가하고 있다. Windows 시스템에서는 사용자 정보와 응용 프로그램 및 하드웨어 장치에 맞게 시스템을 구성하는 데 필요한 정보를 레지스트리에 저장한다. 이 레지스트리에는 각 사용자의 프로필, 컴퓨터에 설치된 응용 프로그램과 각 응용 프로그램이 작성할 수 있는 문서 유형, 폴더 및 응용 프로그램 아이콘의 속성 시트 설정, 시스템에 존재하는 하드웨어, 사용되고 있는 포트 등 Windows가 작동 중에 지속적으로 참조하는 정보가 존재하는데 이러한 정보를 우선적으로 분석하여 효율성을 높일 수 있다.

또한 레지스트리에 남는 기록 외에도 운영체제 및 응용 프로그램에 따라 파일형태로 로그나 중요 정보를 남기는 경우도 있으므로 관련 로그가 있으면 주의 깊게 살펴봐야 한다.

II. 시스템 사용 흔적 증거 수집

레지스트리에서 정보를 획득할 때에는 무결성을 보장하면서 Hive 획득하여야만 한다. Hive 파일은 데이터의 백업이 포함된 지원 파일의 집합을 가진 레지스트리의 키, 하위 키 및 값의 그룹이다. 키 값들은 Windows에서 지원하는 regedit.exe를 이용하여 볼 수 있지만 이 프로그램은 단순히 편집 도구이므로 분석에는 적당하지 않다. 또한 Hive 파일내의 몇몇 키 값은 가독성이 떨어지기 때문에 자체 포맷에 대해 포렌식 분석 기능을 제공하는 레지스트리 분석 도구(EnCase, RegAn, FTK)를 이용하여야 한다.

레지스트리 관련 Hive 파일은 C:₩WINDOWS₩system32₩config 폴더에 DEFAULT, SAM, SECURITY, SOFTWARE, SYSTEM의 확장명이 없는 5개의 파일과 C:₩Documents and Settings₩<사용자 계정 SID>₩폴더에 있는 NTUSER.DAT파일이다. 이 파일을 중점적으로 분석하여 사용자 및 시스템의 활동 정보를 분석한다.

III. 사용자 활동 증거 분석

1. 윈도우 설치 정보

현재 설치된 윈도우의 정보를 확인하기 위해서는 레지스트리의 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion에 있는 키 값을 분석하여야 한다. 여기에는 윈도우가 설치된 날짜, 서비스 팩 버전, 설치 폴더, 윈도우 설치 버전 및 빌드 버전, 윈도우 설치 시 입력한 사용자 이름 및 회사이름을 확인할 수 있다.

2. 사용자 계정 정보

사용자 계정 정보는 레지스트리의 HKEY_LOCAL_MACHINE₩SAM₩SAM₩Domains₩Account 하위에 저장되어 있다. 이 위치에는 현재 설치된 시스템에서 만들어진 계정 및 로그인 횟수, 최종 로그인 시간, 최종 암호 변경 시간을 확인할 수 있다. 하지만 이 키 값은 가독성이 떨어지므로 포렌식 분석 전문 도구(EnCase, RegAn, FTK)를 이용하여 분석하여 한다.

3. 실행 명령

사용자가 윈도우 '시작'에서 '실행'을 클릭한 후 그 창에 작성한 명령어 이다. 이 정보는 레지스트리의 HKEY_USERS₩DEFAULT₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RunMRU에서 확인할 수 있다. 이 곳의 정보를 통해 사용자가 실행한 응용프로그램이 무엇인지 확인 가능하다.

4. 검색 키워드

검색 키워드는 사용자가 윈도우 검색 기능 사용시 사용하였던 키워드로 레지스트리의 HKEY_USERS₩<사용자 계정 SID>₩Software₩Microsoft₩Search Assistant₩ACMru에서 정보를 확인할 수 있다. 이 키는 두 개의 하위 키를 가지고 있는데 하나는 전체 또는 일부 파일 이름에서 검색할 경우이고 다른 하나는 파일에 들어있는 문장이나 단어에 대해 검색할 경우이다.

5. 원격데스크톱 연결 정보

사용자가 윈도우에 있는 원격데스크톱 연결 프로그램을 이용하여 접근을 시도한 상대방의 IP 정보를 확인할 수 있다. 이 정보는 HKEY_USERS₩<사용자 계정 SID>₩Software₩Microsoft₩Terminal Server Client₩Default에 저장되어 있다.

6. 최종 접근 폴더

사용자가 설치한 응용프로그램들이 각각 최종 접근한 폴더를 확인할 수 있다. 이 정보는 레지스트리의 HKEY_USERS₩<사용자 계정 SID>₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedMRU에서 확인할 수 있다. 이 정보를 통해 사용자가 응용프로그램을 이용하여 작업한 마지막 파일에 대한 정보를 획득할 수 있다.

7. 최근 실행 파일

레지스트리 HKEY_USERS₩<사용자 계정 SID>₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RecentDocs에 존재하는 값으로 사용자가 최근 실행한 파일에 대한 목록이 저장되어 있다. 이 키 밑에는 각 확장자 별로 하위 폴더가 존재하는데 이 하위 폴더에 분류되어 있어 만약 특정한 확장자에 대해 찾아야 한다면 동일한 하위 폴더를 찾으면 된다.

8. 문서 관련 최근 실행 파일 정보

레지스트리 HKEY_USERS₩<사용자 계정 SID>₩Software에는 설치된 소프트웨어 목록이 각 폴더 별로 존재하는데 몇몇 프로그램은 최근 열었던 문서나 이미지 등의 목록이 존재한다. MS오피스의 경우 Microsoft₩Office₩<version>₩<오피스 프로그램 ex)엑셀, 파워포인트>₩File MRU에 하위키로서 존재한다. 그 외에도 미디어플레이어(Microsoft₩MediaPlayer₩Player₩RecentFileList), 한글(HNC₩Hwp₩<version>₩FileDialog₩Settings₩00020953₩File MRU) 등에도 응용프로그램에서 접근한 파일의 목록을 얻을 수 있다.

IV. 시스템 활동 증거 분석

1. 서비스 및 드라이버 정보

레지스트리 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services에

는 시스템에 설치된 서비스나 드라이버에 대한 정보를 확인할 수 있다. 각각의 서비스와 드라이버는 이 키의 하위폴더로 구성되어 있다. 이 키는 각 서비스나 드라이버의 시작 유형, 실행 파일 경로 등의 정보를 가지고 있다.

2. 네트워크 정보

레지스트리 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services ₩<장치 ID>₩Parameters₩Tcpip에서 네트워크 관련 정보를 획득할 수 있다. 이 폴더는 하위키로 IP주소, 장치 명, 도메인 서버 주소, 게이트웨이 외에도 DHCP 사용 여부, IP할당시간, 만료시간 등을 분석할 수 있다.

3. USB 장치 정보

레지스트리 HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Enum₩USB 와 HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩Enum₩USBSTOR을 통해 시스템에 사용된 USB목록을 확인할 수 있다. 이때 USB저장 장치 외에도 다양한 보조 장치들이 존재하기 때문에 주의 깊게 분류해야 한다. 이 키는 각 USB 장치에 대한 제조사, 시리얼 넘버, 최초 연결시각 등의 정보를 담고 있다.

V. 응용프로그램 활동 증거 분석

1. 설치된 응용프로그램 정보

레지스트리 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows ₩CurrentVersion₩Uninstall에는 시스템에 설치되어 있는 응용프로그램, 윈도우에 업데이트 프로그램 등의 정보를 획득할 수 있다. 이 키는 응용프로그램들이 언제 설치되었는지 또는 어디에 설치되었는지에 대한 정보를 가지고 있다.

2. 응용 프로그램 사용로그

레지스트리 HKEY_USERS₩<사용자 계정 SID>₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist에서는 설치된 응용프로그램사용에 대한 정보를 가지고 있다. 이 키는 파일의 종류, 최종 실행시각, 실행횟수 등의 정보를 가지고 있다.

D. 파일 분석

I. 개요

사용자가 저장하거나 작업한 데이터는 범죄나 사건에 결정적 증거를 제공한다. 따라서 가장 중점적으로 분석이 진행되어야 하며 결과를 도출하는데 있어 주의를 기울여야 한다. Windows 시스템의 경우 다양한 버전이 존재한다. 이때 Windows 시스템이 일반 개인 사용자에 의해 사용되는지 아니면 서버로 사용되는지에 따라 분석하는데 있어 대상의 우선순위가 정해질 것이다. 또한 대용량의 하드디스크에 있는 모든 파일을 조사하는 것은 힘들기 때문에 각 파일들의 키워드나 생성, 수정 및 접근 시간

등을 활용하여 주로 검사하여야 할 대상을 선정하고 검색 범위를 축소하여 분석의 효율성을 높여야 한다. 하드디스크 분석 시 범죄의 유형이나 사건의 내용에 따라 주로 분석해야 할 파일이 정해질 것이다. 만약 회계 부정이나 내부 감사 시에는 주 목적 파일이 문서가 될 것이다. 반면 성 범죄나 스토킹과 같은 사건에는 이미지 파일이 주 분석 파일이 될 것이다. 또한 각 파일의 시간정보는 사용자의 시간대별 행적을 검증할 수 있다. 이 정보는 포렌식 도구(EnCase) 등을 사용하여 분석하기 쉬운 GUI 형태로 확인이 가능하다.

최근에는 이미지나 문서 등의 정상파일에 데이터를 암호화하여 숨기거나 기존정보에 다른 정보를 삽입하여 은닉하는 경우도 존재하기 때문에 특정 사건에 대해서는 의심이가는 파일에 대해 신중히 조사를 해야 할 경우도 있다.

II. 시스템 로그파일

이미지 파일, 문서 파일 외에도 다양한 형태의 파일들이 존재하고 있다. 시스템 로그 등의 파일들은 사용자의 행적 및 패턴을 분석하는데 중요한 정보를 제공한다. 특히 서버로 사용되는 시스템일 경우에는 시스템이나 네트워크 로그를 통해 네트워크 사용자의 접근 여부 및 서비스 기록을 확인이 가능하기 때문에 더욱 중점적으로 분석이 필요할 수도 있다. 또한 특정 파일들은 바이너리 형태로 저장되어 있기 때문에 이것을 쉽게 인지하기 위해 변화하는 도구가 필요하다.

III. 데이터 파일

1. 검색을 통한 분석

파일 및 디랙토리에 대해 확장자나 포함 문자열 등을 이용해 분리하고 정리한다. 이 작업을 통해 중요한 파일이나 특정 확장자에 대해 데이터를 선별할 수 있으며 분석 시 효율성을 높일 수 있다.

2. Browsing을 통한 분석

다양한 항목(시간, 위치, 해쉬값, 삭제 유무, 숨긴 파일) 등에 대해 선택 및 정렬을 통해 파일을 분리한다. 이러한 과정을 통해 데이터 파일을 분석하는데 있어 정확성을 높일 수 있다.

3. Signature 분석

의도적으로 파일 확장자를 변경해 놓은 파일을 간단히 파악할 수 있다. 파일은 내부에 파일의 종류를 나타내는 시그니처를 포함하고 있는데 용의자가 정보를 은닉하기 위해 확장자를 변경했다면, 시그니처와 확장자를 비교함으로써 은닉 대상을 찾을 수 있다.

4. Hash 분석

Hash 분석은 그래픽 파일, 실행 파일 등과 같이 불필요한 변경이 잘 일어나

지 않는 파일에 적용해 봄으로써 시스템 내의 파일이 변경되었는가를 확인할 수 있다. 기존의 알려진 파일과 같은 파일이 존재하는 가를 확인하고 분석 파일에 대해서 해쉬 값을 계산한 후, 미리 준비된 해쉬 값과 비교하여 대상 파일을 검색한다.

5. 타임라인 분석

파일의 수정시간, 생성시간, 삭제시간, 접근시간을 분석하면 컴퓨터에 내장된 자료의 흐름을 판단할 수 있고, 용의자의 알리바이, 사건의 정황을 파악하는데 많은 도움이 된다. 타임라인 분석에 앞서 시스템 시간이나 시간 지역을 체크하여 오류가 없도록 해야 한다.

IV. 암호화된 파일

개인 정보보호의 중요성이 대두되면서 사용자들이 중요한 파일을 암호화하는 경향이 늘어가고 있다. 용의자는 자신에게 불리한 증언을 하지 않을 권리가 있으므로 수사관은 다양한 방법을 이용하여 암호 키나 패스워드를 찾아내야 한다.

V. 이상 파일

비교적 크기가 큰 오디오, 이미지, 영상 파일에 필요한 정보를 암호화하여 하는 스테가노그라피는 육안으로 식별하기 불가능하다. 또한 디지털 포렌식을 회피하기 위한 제품들이 나오고 있기 때문에 파일의 크기가 평균 크기에 비해 차이가 날 경우에는 분석하는데 있어 주의를 기울여야 한다.

6. 데이터 복구

이번 장에서는 용의자가 임의로 은닉했거나 삭제한 데이터에 대해서 복구하는 기법에 대해 살펴본다. 전체적인 데이터 복구 과정은 [그림 1]과 같다.

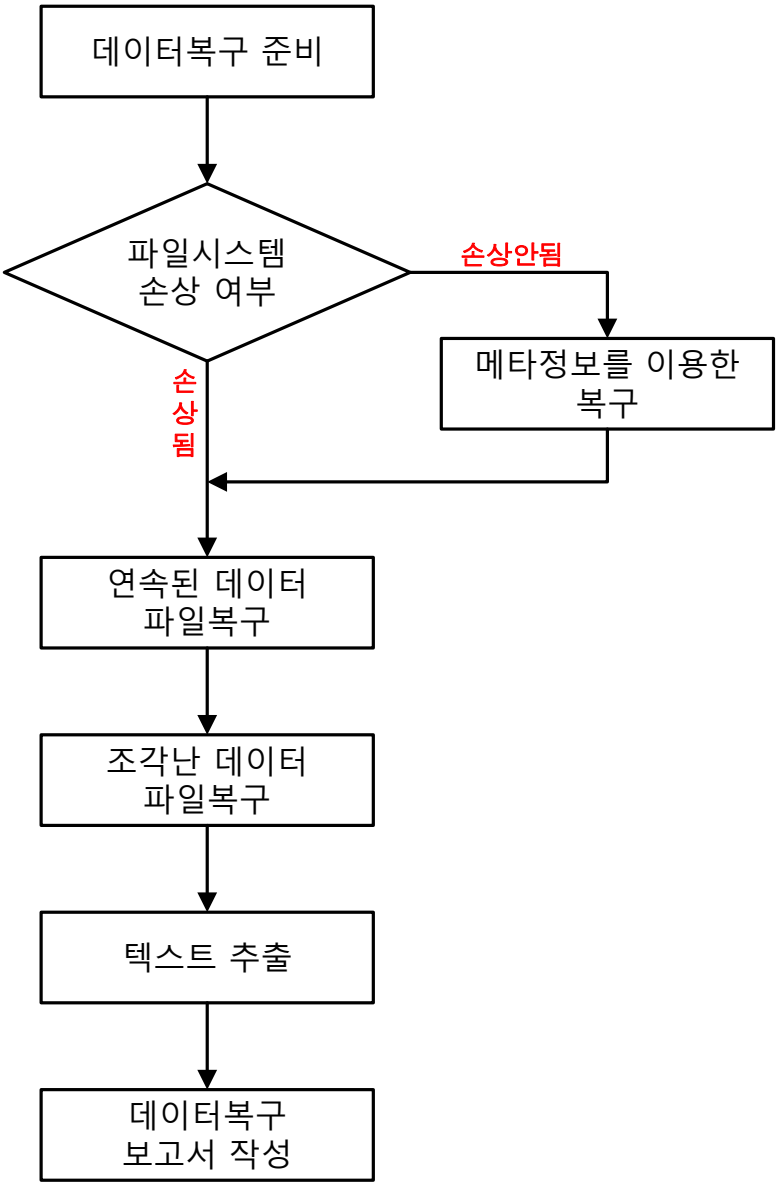


그림 17. 데이터 복구 과정

A. 데이터 복구 준비

데이터 복구 준비 과정은 복구할 데이터의 범위를 설정하고 복구 과정에서 사용할 도구를 준비하는 과정이다.

B. 메타정보를 이용한 복구

데이터 복구에 사용되는 대상이 복제된 하드디스크이거나 디스크이미지의 경우 파일 시스템의 손상여부 판단이 선행되어야 한다. 만약, 파일시스템이 손상되지 않았다면 파일 시스템을 해석하여 이전에 할당되어있는 파일을 빠르고 안전하게 복구할 수 있다. 이와 같이 메타정보를 이용한 복구 방법은 파일시스템이 손상되지 않은 경우 파일시스템 정보를 가지고 데이터를 복구하는 방법이다.

메타정보에는 파일이름, 위치, 크기 등의 정보가 기록된다. 만약, 특정 파일을 찾고자 하는 경우 저장매체 전체 영역을 검색할 필요 없이 쉽게 메타정보를 이용해 접근이 가능하다. 파일이 삭제된 경우에는 메타정보 변경을 통해 파일이 삭제되었음을 표시하여 다른 파일의 메타정보가 기록될 수 있도록 한다. 다른 파일의 메타정보가 기록되기 전에는 이전 파일의 메타정보가 파일시스템에 계속 남아 있게 된다. 따라서 이러한 메타정보를 활용하여 삭제된 파일을 복구할 수 있다. 메타정보를 활용하여 복구한 파일은 비교적 최근에 삭제된 파일들이기 때문에 고의로 삭제한 데이터가 존재할 가능성이 높다. 본 절에서는 윈도우즈(Windows) 파일시스템인 FAT 파일시스템과 NTFS를 대상으로 메타정보를 활용한 데이터 복구 방안에 대해서 살펴본다.

I. FAT 파일시스템의 파일 삭제 및 복구 과정

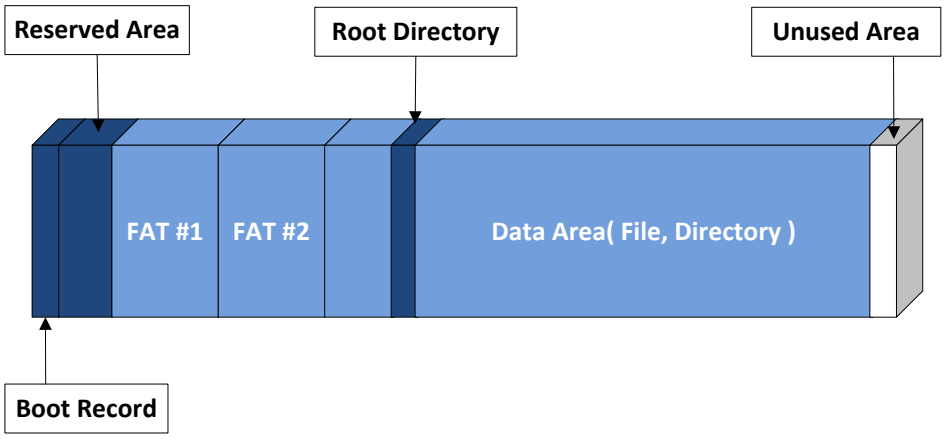


그림 18. FAT 파일시스템 구조

[그림 2]는 FAT 파일시스템의 구조를 보여준다. FAT 파일시스템은 데이터 영역에 파일과 디렉터리에 대한 정보를 기록하고 데이터 영역의 할당 여부를 FAT(File Allocation Table)에 추상화시켜 표현한다. 윈도우즈 시스템은 클러스터(Cluster)라는 논리적인 단위를 사용하여 데이터를 처리하기 때문에 데이터 영역에 기록되는 단위도 클러스터 단위를 따른다. FAT에는 데이터 영역의 클러스터 단위에 대한 할당 여부가 테이블의 형태로 표현되어 있다. FAT는 모든 데이터 영역의 할당 여부를 표현하고 있기 때문에 손상될 경우를 대비하여 [그림 2]와 같이 복사본이 존재한다.

FAT 파일시스템에서 파일의 메타정보는 데이터 영역의 디렉터리 정보를 기록하고 있는 디렉터리 엔트리(Directory Entry)에 기록되어 있다. 파일들은 계층적인 구조를 가지고 있는 디렉터리 내부에 저장되고 해당 파일의 메타정보는 파일이 위치한

디렉터리 엔트리에 저장된다.

1. FAT 파일시스템의 파일 삭제

FAT 파일시스템은 파일을 삭제할 경우 파일이 저장되어 있던 데이터 영역에 해당하는 FAT의 값이 '0x00'으로 초기화된다. '0x00' 값을 가지고 있는 FAT에 대응되는 영역은 빈 영역으로 간주되어 새로운 파일을 저장할 경우 해당 영역을 사용하게 된다. 또한 해당 파일의 정보를 포함하는 디렉터리 엔트리의 첫 바이트가 '0xE5'의 값으로 변경되어 삭제된 파일임을 표시한다. 운영체제는 디렉터리 엔트리의 첫 바이트가 '0xE5' 이거나 '0x00'인 경우에는 빈 파일로 간주하여 처리하지 않는다.

2. FAT 파일시스템의 삭제된 파일 복구

앞서 살펴본 바와 같이 파일을 삭제할 경우 FAT와 디렉터리 엔트리의 첫 바이트 값이 변경된다. 하지만 디렉터리 엔트리의 나머지 메타정보들은 변경되지 않는다. 따라서 디렉터리 엔트리의 첫 바이트가 '0xE5'인 디렉터리 엔트리를 검색하여 해당 메타정보에 기록된 파일의 위치에서 해당 파일의 데이터를 복구할 수 있다. 단, 파일의 데이터가 데이터 영역에 연속으로 기록되어 있지 않다면 FAT의 초기화로 클러스터의 연결정보를 파악할 수 없다.

II. NTFS 의 파일 삭제 및 복구 과정

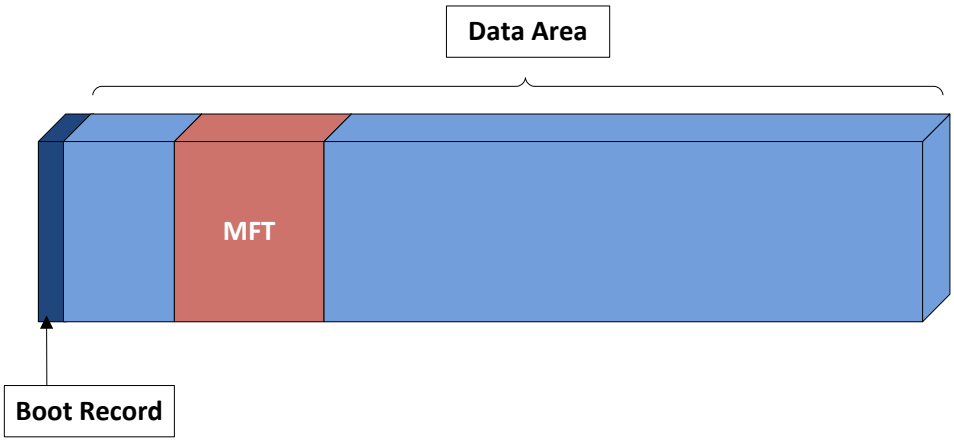


그림 19. NTFS 구조

[그림 3]는 NTFS의 구조를 보여준다. NTFS는 MFT(Mater File Table)이라는 영역을 사용하여 파일들을 관리한다. 하지만 FAT 파일시스템과는 달리 MFT는 위치가 고정적이지 않고 데이터 영역 어느 곳에나 위치한다. NTFS는 MFT 엔트리(Entry)라는 구조를 사용하여 모든 정보를 파일의 형태로 관리한다. MFT 자체도 파일로 보아 MFT 엔트리에 의해 관리된다. 파일은 크기에 따라 하나 이상의 MFT 엔트리를 사용한다.

1. NTFS 의 파일 삭제

MFT에는 파일의 메타정보를 포함한 수많은 MFT 엔트리들이 존재하고 각

MFT 엔트리가 표현하는 데이터는 일정 크기가 넘을 경우 데이터 영역의 특정 클러스터에 저장된다. 파일이 생성, 삭제를 반복할 때마다 MFT 엔트리 또한 생성, 삭제를 반복한다. 하지만 실제로 생성, 삭제를 하는 것이 아니라 MFT 엔트리들의 정보를 저장하고 있는 $MFT 라는 이름의 MFT 엔트리 내에 할당 여부를 비트맵으로 관리한다. 따라서 파일이 삭제될 경우 $MFT의 비트맵 값을 '0x00'으로 변경하여 해당 MFT 엔트리가 사용되지 않음을 표시한다. 이렇게 비트맵 값 '0x00'에 해당되는 MFT 엔트리는 새로운 파일의 정보를 저장하는데 사용될 수 있다.

2. NTFS 의 삭제된 파일 복구

NTFS는 다른 파일시스템보다 삭제된 파일을 복구하기 쉽다. 그 이유는 메타정보를 변경시키지 않고 단지 MFT 엔트리가 사용되지 않음을 표시하기 때문이다. 따라서 삭제된 파일의 복구를 위해서는 $MFT의 비트맵 값이 '0x00'에 해당하는 MFT 엔트리를 검색하여 메타정보를 이용, 해당 데이터를 복구할 수 있다.

C. 연속된 데이터파일 복구

연속된 데이터파일 복구는 파일시스템이 정상적으로 존재할 경우 메타정보를 이용한 복구의 나머지 영역을 대상으로 한다. 또한 파일시스템이 손상되거나 정상적이지 않은 경우에는 전체영역을 대상으로 한다. 연속된 데이터파일 복구는 데이터를 포함한 파일이 물리적인 저장매체에 기록될 때 파일시스템의 제약 아래 데이터가 연속적으로 기록된 경우에 복구하는 방법이다. 연속적으로 기록된 데이터는 파일포맷의 특성을 분석하여 복구가 가능하다. 대표적인 연속적인 데이터 복구 방법으로는 Ram-Slack 복구 방법과 File-Structure 복구 방법이 있다.

I. Ram-Slack 복구

운영체제별로 저장매체의 크기에 따라 파일을 읽고 쓰는 I/O 작업과 파일 Slack을 줄이기 위해 여러 개의 섹터를 묶은 논리적인 데이터단위를 사용한다. 이러한 데이터단위는 운영체제에서 파일을 처리하기 위한 기본 단위가 되며 운영체제에 따라 클러스터(Cluster), 블록(Block)등의 이름을 가진다. 이러한 논리적인 데이터단위는 운영체제가 처리하기 위한 단위이고 실제 물리적인 저장매체는 섹터단위로 읽고 쓴다.

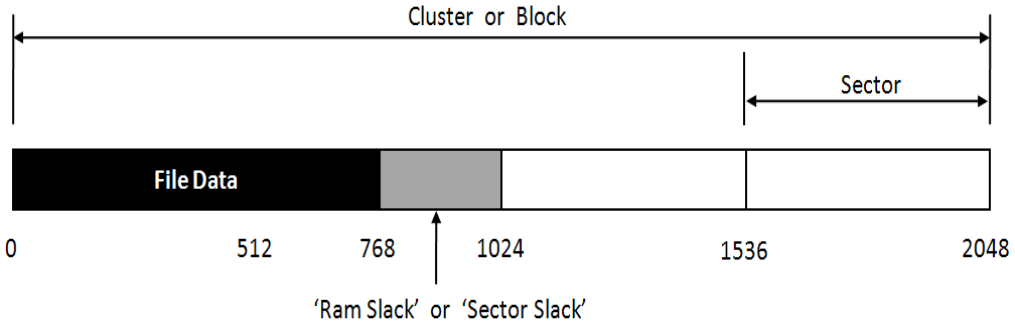


그림 20. Ram-Slack

Ram-Slack은 RAM에 상주하던 데이터가 저장매체에 저장될 때 섹터단위로 처리되는 특성 때문에 발생하는 것으로 Sector Slack이라고도 한다. 만일 [그림 4]와 같이 운영체제의 논리적인 데이터단위가 2K 바이트이고 실제 파일 크기가 768 바이트인 경우 섹터단위로 처리되므로 두 번째 섹터의 마지막 256 바이트가 Ram-Slack이 된다. Ram-Slack은 운영체제와 파일시스템 API에 의해 항상 0x00으로 채워지는데 Ram-Slack 카빙 기법은 이러한 특성을 이용한다. 전통적인 파일카빙 기법은 파일 포맷별로 고유하게 가지고 있는 시그니쳐(Signature)를 이용하는 것이다. 시그니쳐는 파일의 처음에 오는 헤더(Header) 시그니쳐와 파일의 끝에 오는 푸터(Footer) 시그니쳐가 있다. 파일 포맷별로 헤더와 푸터 시그니쳐가 모두 존재하는 경우도 있고 헤더 시그니쳐만 존재하는 경우도 있다.

Ram-Slack 카빙 기법은 헤더와 푸터 시그니쳐가 모두 존재하는 포맷을 대상으로 적용할 수 있는 방법이다. 파일의 끝을 나타내는 푸터 시그니쳐 이후에는 Ram-Slack이 발생하기 때문에 해당 영역이 0x00 값을 가지고 있는지 확인해 볼 수 있다. Ram-Slack의 특성을 이용하지 않고 푸터 시그니쳐만으로 파일의 끝을 판단하게 되면 푸터 시그니쳐 값이 파일의 데이터영역에도 존재할 수 있기 때문에 많은 false-positive가 발생하게 된다. Ram-Slack 카빙 기법은 푸터 시그니쳐를 찾는 과정이 선행되어야 하므로 평균적인 크기가 큰 파일 포맷은 적합하지 않다.

II. File-Structure 복구

File-Structure 카빙 기법은 푸터 시그니쳐가 존재하지 않거나 파일데이터 내에 여러 개의 시그니쳐가 존재하는 경우에 효과적인 방법이다. 대부분의 파일포맷은 데이터 표현을 위해 고유한 구조를 가지고 있다. 따라서 해당 포맷에 적합한 구조를 가지고 있어야 해당 소프트웨어를 통해 내용을 확인할 수 있다. File-Structure 카빙 기법은 파일의 구조를 분석하는 기법으로 파일크기 획득 방법과 파일구조 검증 방법으로 나눌 수 있다.

1. 파일크기 획득

대부분의 파일은 해당 데이터 표현을 위해 파일의 앞부분에 파일구조체가 위치한다. 파일구조체 내부에는 파일시스템의 파일메타정보와 유사하게 해당 파일의 크기, 형식 등의 정보가 포함된 메타정보가 저장된다. 파일크기 획득 방법은 파일

구조체 내부에서 파일크기 정보를 획득하여 카빙하는 방법이다. 파일의 시작위치와 파일크기에 대한 정보를 알고 있다면 쉽게 해당 파일을 카빙할 수 있다.

하지만 단순히 파일의 시작위치와 파일크기 정보만을 가지고 카빙하게 되면 문제점이 발생한다. 파일의 데이터영역에도 파일의 시작위치를 나타내는 헤더 시그니쳐 값이 올 수 있기 때문이다. 이 경우 많은 false-positive가 발생하게 된다. 따라서 파일크기 획득 방법은 파일구조체가 올바른 형식을 갖추고 있는지 검증한 후 이루어져야 한다. 파일구조체에는 항상 고정된 값을 가지거나 일정한 범위의 값을 가지는 필드가 존재하게 되는데 이를 검증하여 해당 시그니쳐가 실제 파일의 시작인지를 확인해야 한다. 파일크기 획득 방법은 평균적인 파일 크기가 큰 포맷의 경우에 푸터 시그니쳐를 찾는 작업이 필요 없기 때문에 효과적이다.

2. 파일구조 검증

대부분 파일구조체는 고정된 형태를 가지는 파일의 경우에 사용된다. 문서파일과 같이 빈번한 수정이 이루어지는 경우에는 해당 데이터표현을 위해 고유한 계층구조를 사용한다. 파일구조 검증은 이러한 계층 구조를 검증하여 카빙하는 방법이다. Microsoft 복합문서나 압축 파일 등은 계층적인 파일구조를 갖추고 있고 각 계층마다 고유한 시그니쳐를 가지고 있다. 따라서 파일의 시작위치를 찾은 후 계층구조를 검증하여 올바른 구조를 갖추고 있다면 정상적인 파일이라고 판단할 수 있다. 하지만 모든 구조를 검증하기 위해서는 많은 시간이 필요하고 이러한 시간은 전체적인 파일 카빙 속도에 나쁜 영향을 미치게 된다. 따라서 구조 검증은 카빙된 파일 내용을 소프트웨어로 확인가능하고 속도에 큰 영향을 미치지 않는 범위에서 이루어져야 한다.

D. 조각난 데이터 파일 복구

조각난 데이터 파일 복구는 데이터가 물리적인 저장매체에 저장될 때 파일시스템의 특성 하에서 조각나 저장된 경우에 복구하는 방법이다. 조각난 데이터 복구는 조각난 데이터 자체가 의미가 있는 경우에 복구하는 방법과 조각난 파일 조각을 서로 결합하여 하나의 완전한 파일을 생성하여 복구하는 방법으로 나누어진다.

E. 텍스트 추출

텍스트 추출은 물리적인 저장매체의 전체영역에서 연속적 또는 조각난 데이터를 복구한 나머지 영역을 대상으로 의미 있는 텍스트를 추출하는 방법이다. 일반적으로 텍스트 파일의 데이터는 특정한 파일포맷이 존재하는 것이 아니라 텍스트의 집합으로 구성되어 있다. 따라서 앞선 연속적 또는 조각난 데이터 복구 후에 텍스트 영역을 추출하게 되면 정상적인 텍스트 파일과 조각난 파일에서의 텍스트 부분을 효과적으로 추출할 수 있다.

F. 데이터 복구 보고서 작성

앞선 데이터 복구 과정을 마쳤다면 효과적인 분석이 이루어질 수 있도록 보고서 작

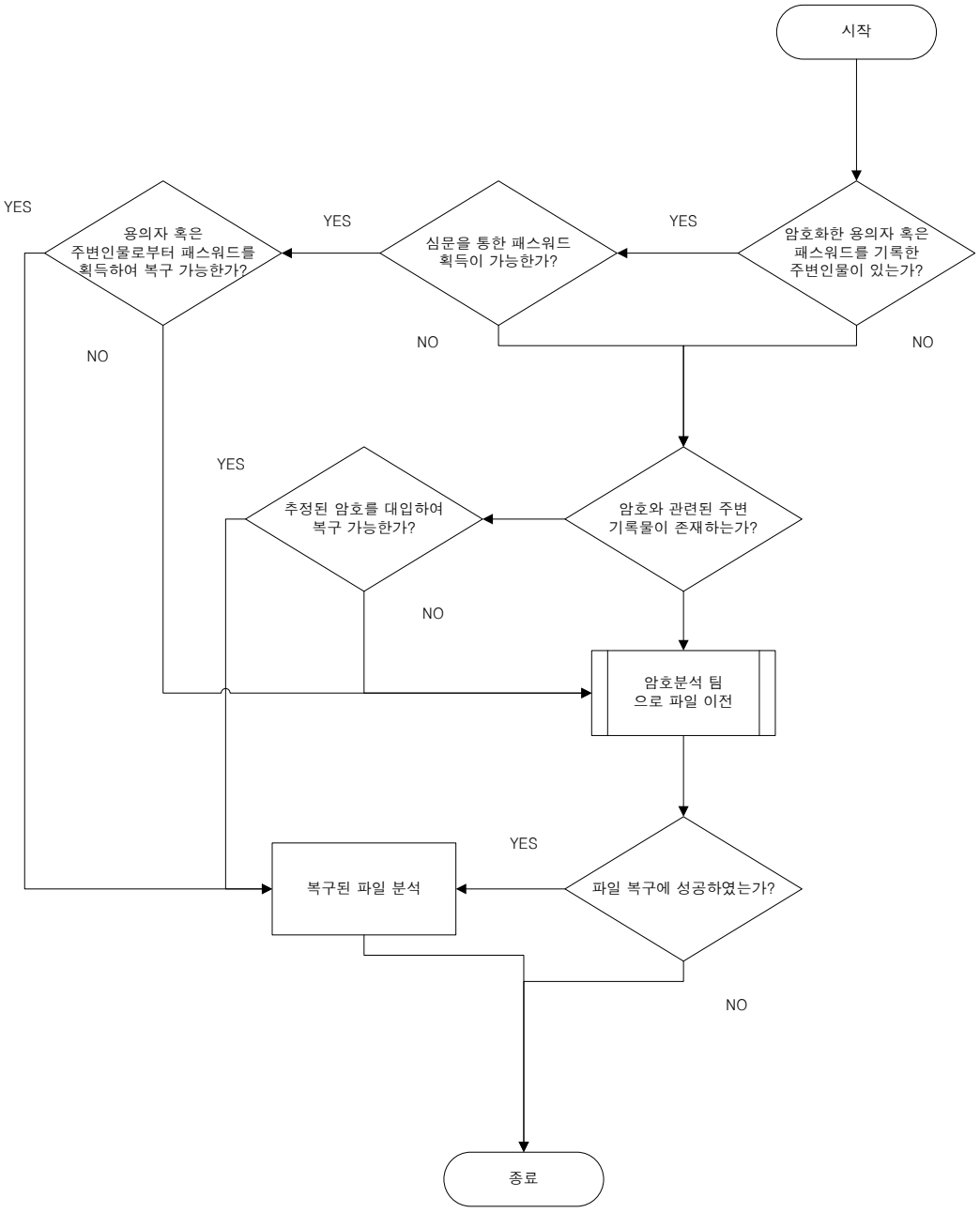
성이 이루어져야 한다. 다음은 데이터 복구 보고서의 예를 보여준다.

7. 암호 파일 분석

파일분석과정에서 암호파일에 대한 분석 시 수사관에 의해 기본적으로 수행될 수 있는 패스워드 획득 절차 및 암호파일전담지원 팀에 의한 패스워드 획득 절차를 서술하고자 한다.

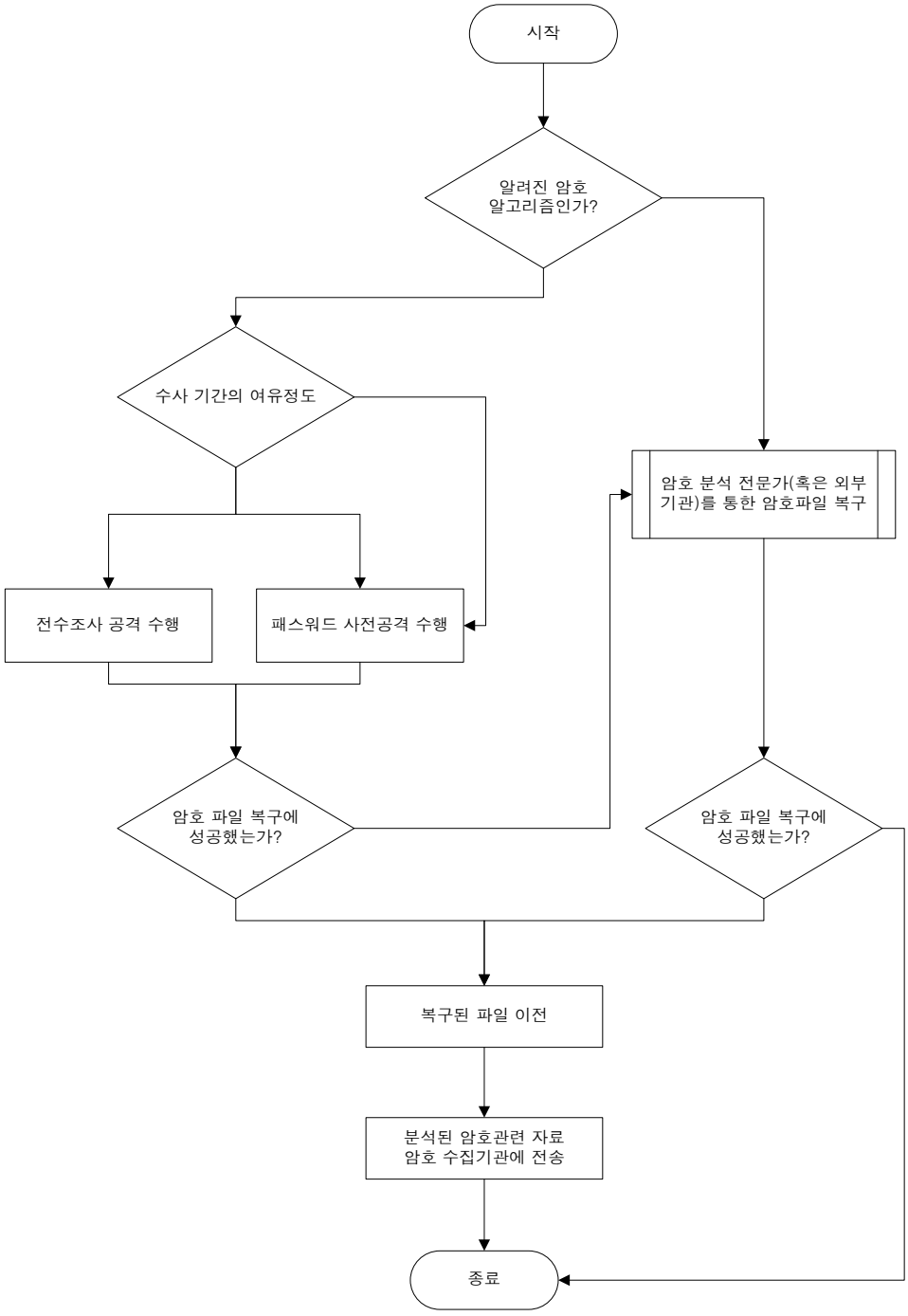
A. 수사관에 의한 복구 절차

수사관에 의해서 수행될 수 있는 패스워드 복구 절차는 다음과 같다. 용의자 및 주변인물, 용의자의 주변 기록물에 의해 복호화 하는 방법과 암호파일전담지원 팀에 파일을 이전하여 복구하는 방법이 있다.



B. 암호파일전담지원 팀의 복구절차

암호파일의 복구를 위하여 파일의 암호에 사용되는 알고리즘이 이미 알려진 것인지 알아본다. 만약 알려지지 않은 알고리즘일 경우 암호 분석 전문가를 통하여 파일을 복구하도록 한다. 알려진 알고리즘일 경우 수사기간을 고려한다. 수사기간이 전수조사가 가능한 시간대에 있다면 전수조사 공격과 사전 공격을 동시에 수행하여 먼저 발견되는 패스워드를 통해 파일을 복구한다.



I. 패스워드 복구

알려진 암호 알고리즘의 경우 패스워드가 맞는지 대입하여 결과를 알려주는 자동화된 도구가 존재한다. 패스워드 공격에는 크게 두 가지로 나누어 볼 수 있다.

1. 전수조사 공격

전수조사 공격 방법은 사용 가능한 패스워드의 모든 경우의 수를 대입하는 방법으로써 컴퓨터에 의해 자동화 될지라도 패스워드의 길이가 길어지면 복구 시간이 기하 급수적으로 늘어나므로 패스워드 검색의 효율성이 떨어진다.

2. 패스워드 사전공격

패스워드를 알아내기 위한 사전 공격은 사전에 있는 단어를 순차적으로 입력하는 것이다. 단어를 그대로 입력할 뿐 아니라, 대문자와 소문자를 뒤섞기도 하고, 단어에 숫자를 첨부하기도 하는 등의 처리도 병행하면서 공격할 수 있다. 수십만 개의 단어가 수록되어 있는 사전을 컴퓨터에 자동 처리시킴으로써 단시간에 모든 단어를 입력할 수 있기 때문에 사전공격은 기본적인 패스워드 탐색의 수법으로 이용된다.

C. 패스워드 사전 생성 매커니즘

위에서 언급한 암호파일 접근 방법 중 가장 효율적이고 실질적인 방법은 패스워드 사전을 생성하여 공격하는 방법이다. 이를 위해서 패스워드 사전 생성을 위한 매커니즘을 소개하고자 한다. 기본적인 사전 생성 기능으로써 특수문자 포함여부, 문자 반복사용 여부, 패스워드 최소 길이 선택 등은 수사관의 목적에 맞게 적용하여 생성할 수 있어야 한다.

I. 범용 사전

가장 일반적인 방법으로 기존에 나와있는 용어, 국어, 영어 사전 등 일반 사전을 우선순위를 적용하여 단어를 토큰화 하여 사전을 생성한다. 범용사전의 효율성을 높이기 위해서는 다양한 분야의 사전파일의 획득하는 것이 중요하다. 예를 들어 인명사전, 한글사전, 영어사전, 비속어사전, 채팅용어사전, 법률용어사전, 의학용어사전 등에서 추출된 토큰은 일반적으로 패스워드로 사용될 만한 문자를 포함하고 있으므로 사전 구성 시 이점을 적용할 수 있다.

II. 용의자에 대한 프로파일

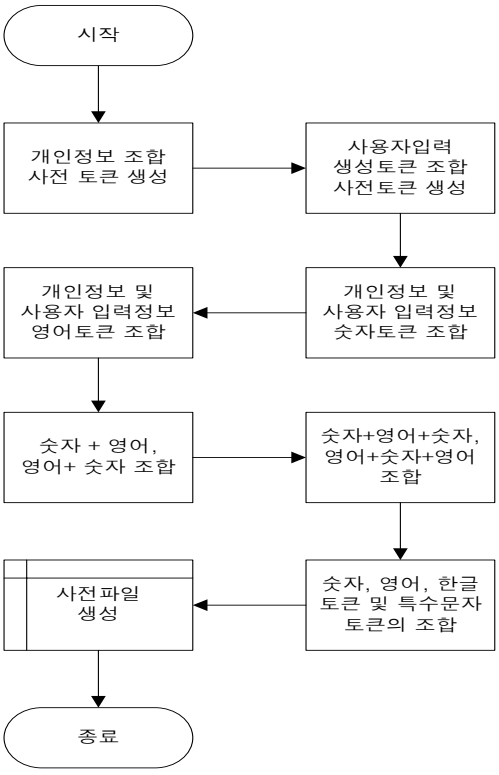
암호파일의 패스워드 추측을 위해 용의자 개인의 정보를 활용하여 사전의 생성이 가능하다. 예를 들어 용의자 이름, 주민등록 번호, 전화번호, 핸드폰 번호, 차량번호, 학번, 군번, 생년월일, 친구이름, 친구 또는 친척, 가족과 관련된 정보 등 용의자와 관련된 정보의 조합을 통해 패스워드 사전 생성이 가능하다.

III. 특정 파일에서 문자열을 통한 패스워드 사전추출

파일에서 추출된 문자열의 사전생성은 몇 가지 측면에서 의미를 가질 수 있다. 첫 번째로 시스템상에서 관리하는 memory의 덤프파일 혹은 page 파일 등은 Live 상태에서 용의자가 암호화를 위해 사용한 패스워드의 저장 가능성이 존재한다. 그러므로 이러한 파일에 대한 문자열을 추출하여 패스워드 사전을 생성할 수 있다. 두 번째로 용의자가 작성한 것으로 추측되는 파일에는 위에서 언급한 용의자와 관련된 정보를 포함할 가능성이 있다. 특히 이력서, 신상기록, 자기 소개서 등의 문서파일은 용의자의 신상정보를 포함하고 있으므로 문자열 추출을 활용한 사전생성이 가능하다. 세 번째로 용의자가 작성한 것으로 의심되는 파일의 경우 용의자가 평소 문서작성시 사용하는 단어선택 및 문자 패턴 등을 포함할 가능성이 있으므로 이점 역시 문자열 추출을 통한 사전 생성이 가능하다.

IV. 패스워드 처리 및 조합

위의 세 가지에서 나온 사전의 토큰은 별도의 패스워드 처리과정을 거쳐야 한다. 암호파일의 패스워드가 영문자로 되어 있기 때문에 한글의 경우 영문 타자로의 변환이 필요하며 병합과정에서 발생하는 중복을 제거해야 한다. 또한 각각의 토큰을 조합해 패스워드 사전을 생성한다.



8. 디지털 증거 수집 – 모바일 기기(Mobile Devices)

A. 개요

디지털 범죄 수사에서는 컴퓨터 이외에 많은 디지털 기기들이 존재한다. 이러한 기기들은 디지털 정보를 저장하는 저장 매체를 갖추고 있으며, 저장된 정보 중에는 직·간접적으로 범죄와 관련이 있는 정보가 존재한다.

모바일 기기는 정보통신 기술(IT)을 이용한 이동성과 정보 처리 및 저장 능력을 갖춘 매체를 말한다. 정보통신 기술(IT)이 발전함에 따라 다양한 모바일 기기들이 생겨나고 있다. 그 중에 대표적인 모바일 기기는 생활필수품이 되어버린 휴대폰이다. 최초 휴대폰은 음성통화를 목적으로 만들어졌지만, 최근 디지털 컨버전스(Digital Convergence)화가 진행됨에 따라 휴대폰에 다양한 기능들이 통합되고 있다. 이렇게 휴대폰이 사용자에게 다양한 기능을 제공함에 따라 사용자와 관련된 많은 정보를 담게 된다. 이러한 대표적인 모바일 기기인 휴대폰을 대상으로 디지털 포렌식 수사에서의 범죄와 관련된 모바일 기기 취급 방안을 제시한다.

본 절에서는 디지털 범죄와 관련된 디지털 매체 가운데 모바일 기기에 저장되어 있는 디지털 증거 수집 및 분석, 보고에 관한 기본 원칙과 절차를 다룬다.

본 절의 주요 내용은 최근 소형화, 다양화, 대용량화되고 있는 모바일 기기의 종류와 특성을 파악하고, 현행 증거법에서 중요시되는 증거의 정확성 및 신뢰성을 고려하여 모바일 기기에서의 증거 수집 및 분석, 보고에 필요한 항목 및 세부 절차를 포함한다.

B. 모바일 기기 증거 수집

모바일 기기는 휴대폰, PDA, 디지털 카메라 등 다양한 종류의 기기들을 포함한다. 이렇게 다양한 모바일 기기들의 종류와 특성을 파악하고, 그에 따른 디지털 증거로서의 모바일 기기 취급 방안을 제시한다.

I. 모바일 기기 종류

모바일 기기는 사용 목적에 따라 휴대폰, PDA, 노트북, PMP, 디지털 카메라, MP3 플레이어, 게임기, 네비게이션 등이 있으며, 이동 및 휴대 가능한 기기를 모두 포함한다.

<대표적인 모바일 기기>

II. 모바일 기기 특징

모바일 기기는 이름에서 알 수 있듯이 이동성 및 휴대성을 고려해 만들어진 디지털 기기이다. 기능성으로는 정보를 저장하고 처리할 수 있는 기능과 무선 네트워크 기능을 갖추고 있으며, 대부분 소형화를 위해 플래시 메모리를 저장 매체로 사용하고 있다.

III. 모바일 기기 취급 시 고려 사항

모바일 기기는 대부분 소형화되어 물리적 충격에 상대적으로 약하며, 대부분 무선 네트워크가 구성되어 있어 무선 신호에 영향을 받을 수 있으므로 취급 시 유의해야 한다.

따라서 사건 현장에서 모바일 기기 취급 시에는 일반 유선 네트워크를 사용하는 컴퓨터와 달리 무선 네트워크로 인한 데이터 추가 및 변경 등의 무결성 훼손에 대한 고려가 필요하다. 상세한 고려 사항은 증거 수집 및 이송, 보관 시 유의 사항에서 제시한다.

C. 증거 수집/분석 항목 및 절차

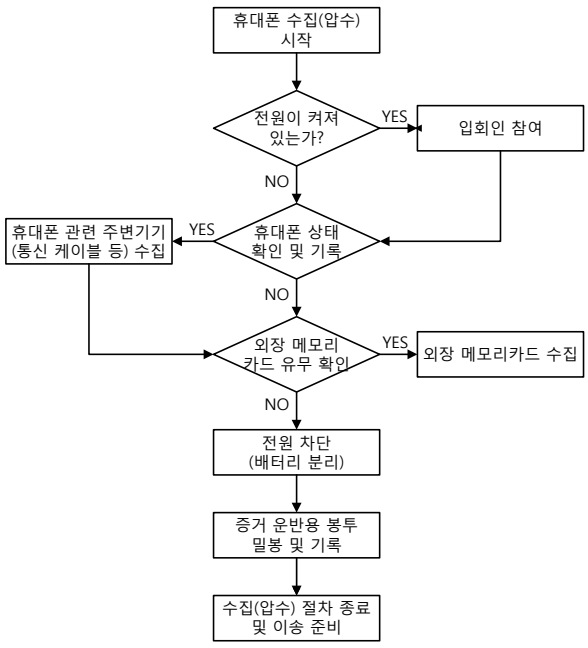
I. 현장에서의 증거 수집(압수)

1. 증거 수집(압수) 절차

범죄 현장에서 디지털 증거로서 휴대폰을 수집(압수)하는 절차는 일반적인 디지털 포렌식에서의 절차와 크게 다르지 않으며, 세부적인 단계에서 약간의 차이가 있다.

휴대폰 증거 수집의 첫 번째 과정은 휴대폰의 전원 상태 확인이다. 우선 전원이 켜진 상태라면 전원을 차단하기 전에 휴대폰의 사용자나 입회인과 함께 현재 상태를 확인하고 휴대폰 액정에 나타나는 정보(시간, 문구, 배경사진 등)를 기록하고, 압수 당시의 휴대폰 상태를 사진으로 찍는다. 이후 무선 신호로 인한 무결성이 훼손되는 것을 방지하기 위해 전원을 차단한다.

휴대폰의 전원을 차단한 후 사전 준비한 증거 운반용 봉투나 장치에 넣고, 봉투 겉 표지 등에 압수수색 집행 기관, 압수수색 대상, 인적 사항 등의 과정에 대한 세부사항을 기재하도록 한다. 또한 컴퓨터와의 통신 여부를 확인하고 통신 케이블, 통신 프로그램, 외장형 메모리 등도 같이 수집(압수)하고 그에 대한 내용을 기재하도록 한다.



<휴대폰 수집(압수) 절차>

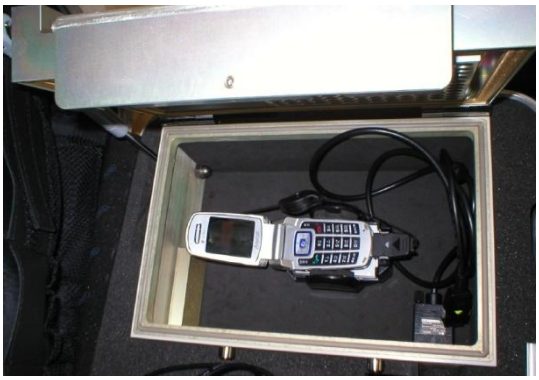
2. 증거 수집(압수) 시 유의사항

전원이 켜진 휴대폰은 장소의 제약을 거의 받지 않고 무선 신호에 의해 데이터의 추가 및 변경 가능성이 높다. 따라서 휴대폰 증거물은 반드시 전파 차단용 봉투나 이동용 전파 차단 장치 등에 넣고 밀봉하여 증거의 무결성이 훼손되지 않도록 한다.

또한 증거 수집(압수) 시 모든 과정에 대한 사항을 기록하도록 한다.

※ 전파 차단용 봉투 : 내부(충격 방지용 버블 보호막), 외부(전파 차단용 모직(구리•니켈 도금 실크 메시 소재))

※ 이동용 전파 차단 장치 : 충격 방지와 전파 차단 목적의 증거 이송 장치



<전파 차단용 봉투와 장치>

II. 증거 이송

1. 증거 이송 절차

범죄 현장에서 수집된 휴대폰은 전파 차단용 봉투나 가방에 넣고 밀봉한 상태로 증거 조사 및 분석을 위한 증거 분석실로 이송한다.

2. 증거 이송 시 유의사항

휴대폰과 같은 모바일 기기는 물리적인 충격에 상대적으로 약하므로, 이송 간 충격이 발생하지 않도록 유의해야 한다.

III. 증거 자료 추출 및 보관

휴대폰은 주파수 사용방식에 따라 크게 CDMA(Code Division Multiple Access) 방식과 GSM(Global System for Mobile communication) 방식으로 나뉜다. GSM 방식은 유럽 표준으로 유럽 및 기타 지역에서 광범위하게 사용되고 있으며, GSM 방식을 사용하는 휴대폰은 데이터를 (U)SIM 카드에 저장한다. CDMA 방식은 우리나라를 포함해 일본, 중국, 미국 일부, 동남아 일부 등에서 사용되고 있으며, 휴대폰 데이터를 플래시 메모리에 저장한다.

따라서 우리나라에서 사용하는 CDMA 방식을 기반으로 휴대폰 증거 자료 추출 및 분석 방법을 제시한다.

1. 증거 자료 추출 방법

휴대폰 증거 분석을 위해서는 휴대폰의 보조 기억장치로 사용되는 플래시 메모리의 데이터를 추출하여야 한다. 휴대폰 데이터 접근 방법은 크게 물리적, 논리적 방법으로 구분된다.

가) 물리적 접근 방법

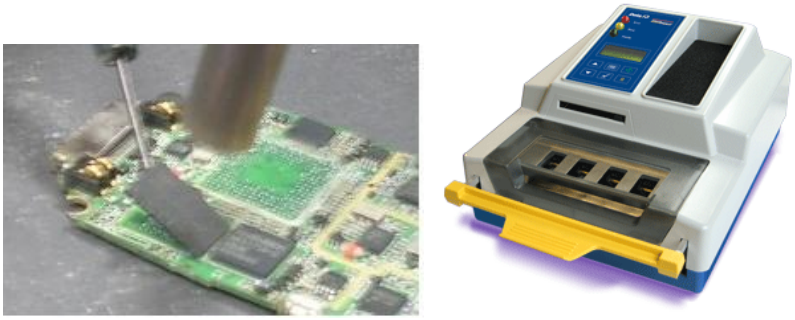
① JTAG(Joint Test Action Group)

JTAG 은 임베디드 시스템 개발 시 디버깅을 위한 장비로 휴대폰 인쇄회로기판(PCB)에 숨겨져 있는 JTAG 핀을 찾아 JTAG 에뮬레이터와 연결하여 전체 물리 메모리를 bit 단위로 접근하여 모든 플래시 메모리 영역을 덤프한다. 따라서 플래시 메모리에 저장되어 있는 삭제된 데이터들도 복구가 가능하다.

<JTAG 을 이용한 물리적 접근>

② 플래시 메모리 리더기

플래시 메모리 리더기는 인쇄회로기판(PCB)에서 물리적으로 분리된 플래시 메모리를 읽어 전체 물리 메모리를 덤프한다. JTAG 과 마찬가지로 삭제된 데이터들도 복구가 가능하다. 하지만 플래시 메모리를 물리적으로 분리해야 하는 문제점과 플래시 메모리를 프로그램 하기 위해 제작된 장치이기 때문에 법정에서 무결성 문제가 대두될 수 있는 문제점이 있다.



<플래시 메모리 리더기를 이용한 물리적 접근>

나) 논리적 접근 방법

논리적 데이터 추출 방법은 휴대폰과 PC 가 통신 프로토콜을 이용하여 동기화되어 프로토콜에 명시된 명령어로 데이터를 추출하는 방법이다. 하지만 논리적 데이터 추출 방법은 일반적인 컴퓨터 하드디스크 복제 방법과 달리 휴대폰 주파수 사용방식 및 제조사, 기종에 따라 추출 방식이 다르기 때문에 범용적인 추출 도구는 존재하지 않는다.

<휴대폰-PC 통신 프로토콜을 이용한 논리적 접근>

현재 국내의 CDMA 휴대폰에 적용 가능한 알려진 도구들은 다음 표와 같다.

도구	기능	설명
QPST	수집	Qualcomm CDMA 프로그램 도구, 데이터 추출
EasyCDMA	수집, 뷰어	파일시스템 뷰어, 데이터 추출•삽입
BitPim	수집, 뷰어, 분석	공개용, 파일시스템 뷰어, 데이터 추출•삽입, 분석
Final Mobile Forensics	수집, 뷰어, 리포팅	파일시스템 뷰어, 데이터 추출
Mobile Forensic Toolkit	수집, 뷰어, 분석	파일시스템 및 데이터 추출, 분석

2. 증거 보관 방법

휴대폰 플래시 메모리로부터 데이터를 추출한 후에는 증거 수집(압수) 절차에서와 같이 전원을 차단한 후 전파 차단용 봉투나 장치에 넣고, 밀봉 일시 및 조사 사항, 인적 사항 등을 기재하도록 한다. 또한 직사광선이나 물리적 충격으로부터 안전한 증거 보관소에 휴대폰 증거물을 보관하도록 한다.

3. 증거 무결성 보장

휴대폰 플래시 메모리로부터 획득한 데이터(덤프) 파일은 분석 간 추가 및 변경, 삭제 등의 여부를 판단할 수 있도록 분석 전·후의 해쉬 값을 비교해 증거의 무결성을 검증하도록 한다.

IV. 증거 분석

1. 휴대폰 분석 항목 및 방법

가) 분석 항목

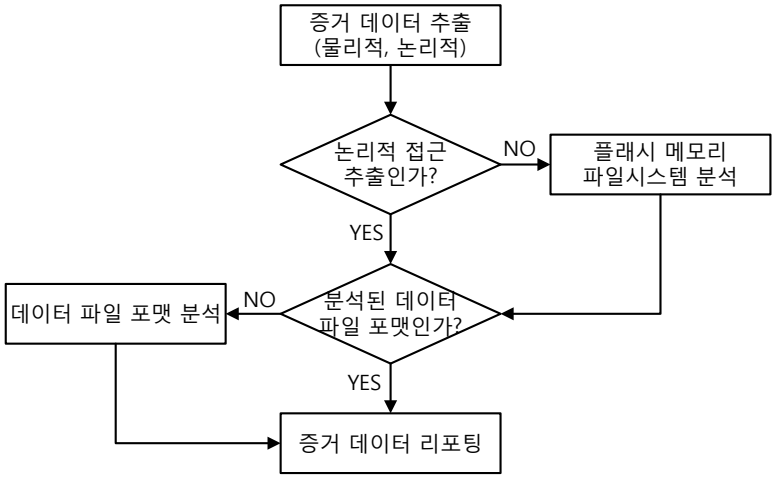
휴대폰 데이터에서 사건의 직접적인 증거나 사건의 실마리를 제공하는 간접적인 증거로 사용될 수 있는 분석 대상 데이터는 다음 표와 같다.

데이터	항목
수신 문자메시지(SMS)	수신 일시, 송신자 전화번호, 문자내용
발신 문자메시지(SMS)	발신 일시, 수신자 전화번호, 문자내용
임시저장 문자메시지(SMS)	저장 일시, 수신자 전화번호, 문자내용
최근 통화 기록(Call History)	통화종류, 송수신자 전화번호, 통화시간
전화번호부(PhoneBook)	저장된 이름, 전화번호, 단축번호, 그룹
일정(Schedule)	일정 일시, 일정내용
메모(Memo)	메모 일시, 메모내용
사진(Photo)	사진 콘텐츠, 사진 촬영 정보
멀티미디어(Multimedia)	동영상, 음성 메모, 음악 등
휴대폰 전자일련번호(ESN)	제조사 식별 코드, 기기 일련 번호
휴대폰 비밀번호	※ 휴대폰 잠금 해제

나) 분석 방법

휴대폰 데이터 분석 방법은 데이터 추출 방식에 따라 크게 2 가지로 구분된다. 논리적으로 데이터를 추출하였을 경우, 각 데이터를 분석하기 위해서는 각 데이터 파일 포맷을 분석해야 한다. 하지만 이러한 대부분의 데이터 파일은 제조사와 기종에 따라서 서로 다른 파일 포맷을 사용한다.

물리적으로 데이터를 추출하였을 경우에는 플래시 메모리에서 사용한 파일시스템을 알아야 한다. 현재 휴대폰 플래시 메모리에서 사용하고 있는 파일시스템으로는 EFS, EFS2, TFS4 등이 있으며, 이러한 파일시스템은 공개되어 있지 않아 분석에 어려움이 따른다. 또한 각 제조사마다 이러한 파일시스템을 변형하여 사용하고 있어 파일시스템도 휴대폰 제조사 및 기종에 따른 분석이 필요하다. 이러한 파일시스템 분석 후 데이터 파일 포맷의 분석도 필요하다.



<증거 데이터 분석 절차>

다) 데이터 복구 방법

물리적으로 증거 데이터를 추출하였을 경우에는 전체 플래시 메모리 상에 남아있는 삭제된 데이터의 복구가 가능하다. 삭제된 데이터의 복구를 위해서는 플래시 메모리에서의 파일시스템 분석이 선행되어야 한다.

2. 기타 모바일 기기

휴대폰 이외에 다양한 모바일 기기가 존재하며, 이러한 모바일 기기 또한 증거 수집 대상이 될 수 있다. 또한 증거 수집 시 휴대폰 증거와 같은 절차를 따를 수 있다.

- 개인 휴대용 정보 단말기(PDA, Personal Digital Assistant)
- 휴대용 멀티미디어 플레이어(PMP, Portable Multimedia Player)
- 노트북
- 디지털 카메라
- MP3 플레이어
- 게임기
- 네비게이터(Navigator)

D. 결과 보고서 작성

결과 보고서는 범죄 수사가 결론에 도달하고 각 단계 별로 결과를 낼 때마다의 기록을 모아 상세한 결과물을 도출하는 절차이다.

I. 보고서 작성 요령

결과 보고서는 수사관 및 분석관 등의 모든 행동과 관찰, 기록이 정확히 유지되어야 하고 각 단계의 결과와 완벽히 일치해야 그 결과를 증거로 인정받을 수 있게 된다.

또한 조사자가 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성한다. 작성자는 결과 보고서에 서명하고 작성 내용에 대해 책임을 진다.

II. 보고서 세부 항목

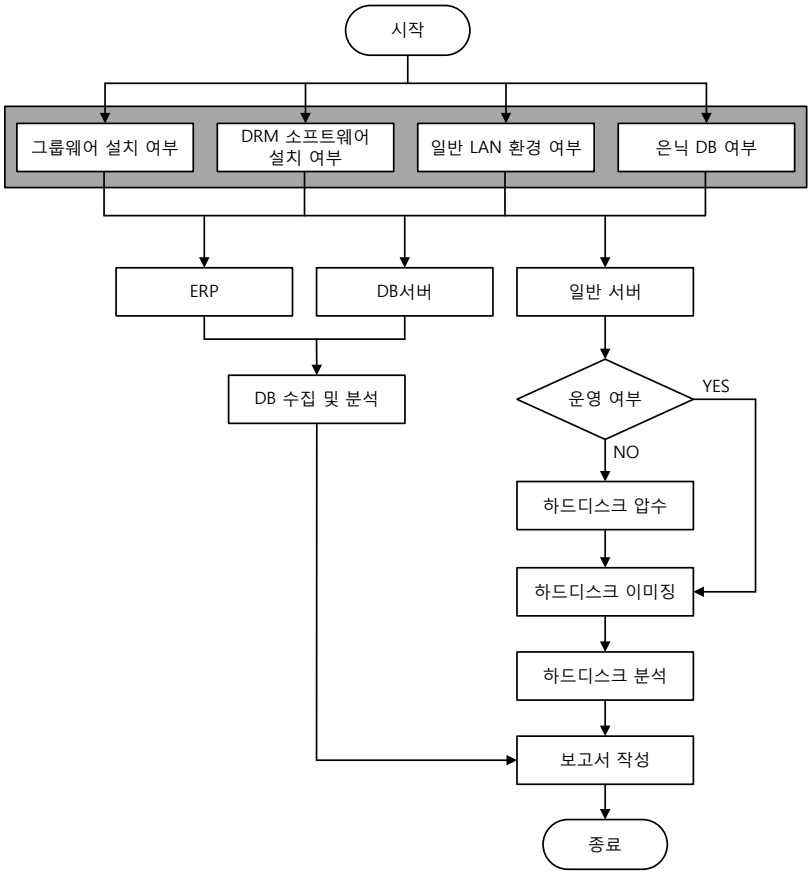
결과 보고서에 포함되어야 할 항목은 다음과 같다

- 사건(Case) 및 보고서 번호
- 증거 수집 일시, 보고서 작성 일시
- 수사 및 분석관, 보고서 작성자의 신분과 서명
- 휴대폰의 기본 정보(일련 번호, 제조사, 기종, 전화번호 등)
- 조사 및 분석에 사용된 장비 및 환경
- 각 절차에 대한 개략적 설명
- 사진 및 인쇄물 등과 같은 첨부 자료
- 추출 및 분석된 증거 데이터의 상세 설명
- 분석 결과 및 결론

9. 사건 유형별 디지털 포렌식 수사 절차

이번 장에서는 본 문서에서 제시한 디지털 증거 수집 가이드라인을 기반으로 총 6가지의 사건을 유형별로 분석하는 절차를 살펴보고자 한다.

A. 기업부정

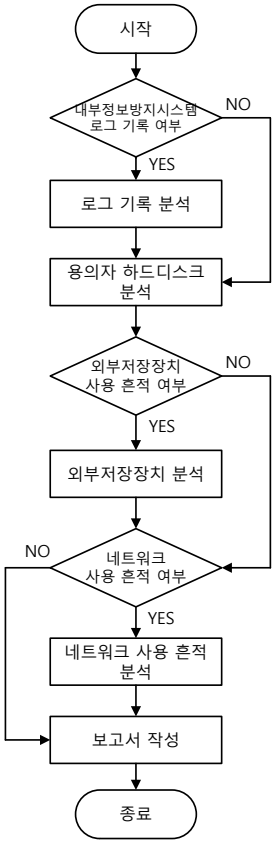


기업부정은 해당 기업의 규모와 실제 관리하고 있는 데이터의 정도에 따라 수사 과정을 다르게 진행해야 한다. 우선 그룹웨어 및 DRM 소프트웨어 설치 여부, 일반 LAN 환경, 은닉 DB 여부와 같이 기업의 전산 환경을 파악하여 조사한 뒤, 데이터 관리 방법에 따라 데이터 및 기업 내 결제, 승인 등의 트랜잭션까지 관리하는 ERP, 데이터 관리를 위해 별도로 구축한 DB서버, 컴퓨터 내 설치된 회계관리 소프트웨어로 관리하는 일반서버로 나누어 수사한다. ERP 시스템은 내부적으로 DB 서버를 사용하므로 이 시스템은 DB 서버와 동일하게 DB 수집 및 분석으로 수사를 진행한다.

일반 서버의 경우 별도의 시스템을 구축, 운영하는 것이 아니라 회계관리 기능을 제공하는 소프트웨어를 설치한 뒤 이를 통해 데이터를 관리하기 때문에 서버의 운영 여부에 따라 장착된 하드디스크를 압수 혹은 현장에서 생성한 디스크 이미지로 하드디스크 분석을 수행해야 한다. 분석 과정에서는 실제 데이터 변조가 일어난 시간을 추적할 수 있는 시간정보, 각 파일의 고유한 시그니처와 실제 파일의 확장자를 비교하여 임의로 확

장자가 변경된 파일 유무를 중점적으로 살펴본다.

B. 기밀정보 유출



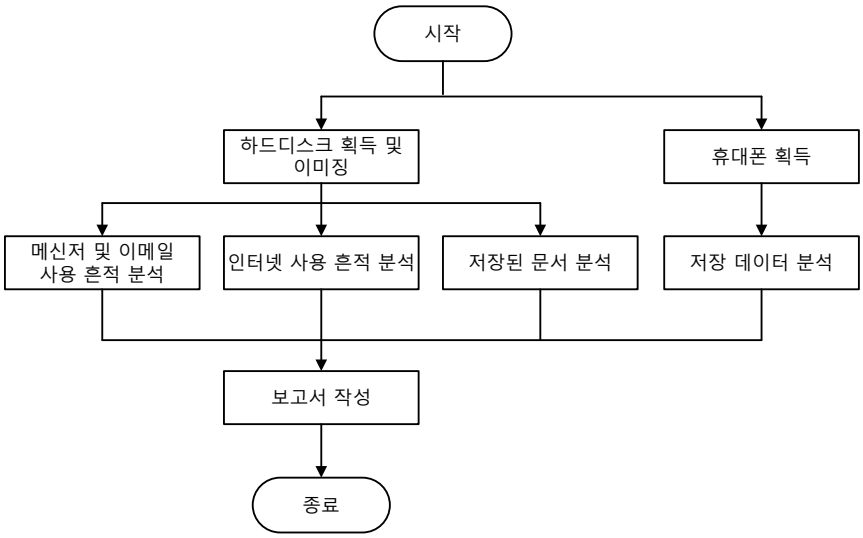
기밀정보 유출은 크게 네트워크를 통한 제 3자의 침입이 일어난 경우와 내부자에 의해 고의적으로 일어난 경우로 나누어 볼 있으며, 이는 시스템 사용 흔적 및 네트워크 사용 흔적을 모두 수집, 분석해야 한다. 본 문서에서는 내부 보안팀의 접근에 의한 기밀정보 유출에 대해 살펴본다.

먼저 기업 내부 보안 팀에서 용의자를 판단해야 한다. 특히 사전에 불량한 행동이나 의심스러운 행동을 했던 사람을 대상으로 수사를 진행해야 한다. 내부적으로 별도 운영하고 있는 내부정보방지시스템이 존재하는 경우에는 해당 시스템의 로그 기록을 통해 기밀 정보를 변경 혹은 불법 접근한 사람이 있었는지, 그리고 용의선상에 있는 사람이 사용했던 흔적을 조사한다. 이 단계에서 내부 조사가 일어난다는 사실이 알려지면 증거 인멸 가능성이 있다는 점에 유의한다.

이후 용의자를 대상으로 컴퓨터 포렌식 수사를 진행하며 특히 메신저, 메일, 웹하드 등 네트워크를 통해 기밀 정보를 유출할 수 있다는 점을 고려한다. 또한 확인 기밀정보에 접근이 가능한 내부자가 데이터를 이동하기 위해서는 USB와 같이 별도의 저장장치를 사용하는 것이 일반적이라는 점을 감안하여 외부저장장치의 탈, 부착 여부를 확인한다. 이는 특정 레지스트리 키 값, setupapi.log 파일 등의 분석을 통해 확인이 가능하다. 만약

용의자가 획득한 기밀정보 관련 파일을 실제로 유출하지 않았다고 주장할 경우, 해당 파일의 시간정보 분석, 메타데이터 분석 등을 통한 파일 사용 여부로 판단한다.

C. 살인 및 자살



살인 사건은 용의자의 증거가 명백하다면 포렌식 수사는 필요하지 않다. 여기서는 계획적인 살인에 대해서 다루도록 한다.

우선 사건 용의자를 파악 해야 한다. 개인인지 조직 범죄인지 판단하는 것이 중요하다. 그리고 사건 발생 전후의 최근 용의자 행동정보를 파악해야 한다. 이러한 용의자 행동정보는 컴퓨터뿐만 아니라 용의자가 사용하는 다양한 디지털 기기를 통해서 입증할 수 있기 때문에 우선 수집 가능한 디지털 기기의 목록을 확인해야 하며, 본 문서에서는 이러한 기기로 휴대폰과 CCTV를 선택하였다.

휴대폰은 사건 발생 직후 통화 내역 및 직접 저장한 일정, 메모 등의 데이터를 중심으로 분석하면 사건과 연관된 인물과 용의자의 동선파악이 가능하다. 만약 휴대폰 사용 기록이 없는 경우, 용의자가 의도적으로 삭제했을 수 있다는 점을 감안하여 휴대폰 데이터 수집 도구와 전용 분석 프로그램을 통해 삭제 데이터 유무를 판단, 이를 복구하여 분석하는 과정을 진행하여야 한다.

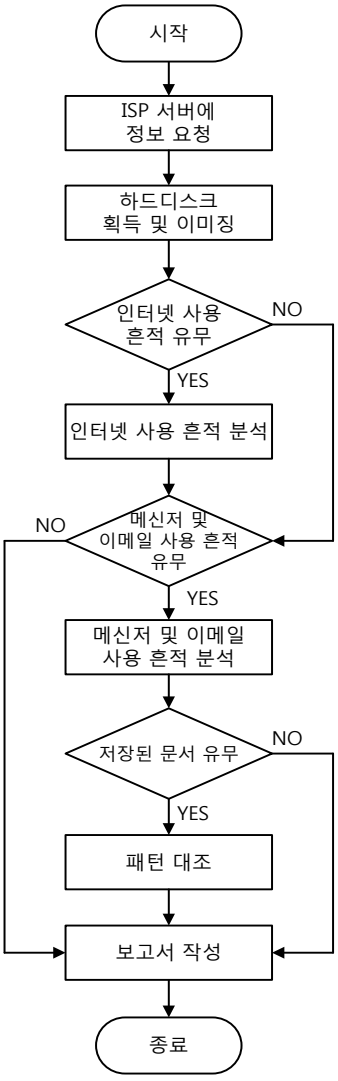
만약 사건 발생 장소에 CCTV가 설치되어 있다면 당시 촬영된 영상을 증거로 활용할 수 있다. CCTV도 컴퓨터의 하드디스크와 마찬가지로 저장장치의 이미징이나 복제 저장 장치를 통해 분석이 가능하다. 이러한 경우, CCTV 증거의 복사본 및 증거 파일의 해쉬값을 생성하고, 수집 시 작성된 문서에 기재된 값과 반드시 비교해야 한다. 필요에 따라 삭제된 동영상을 복구해야 하는 경우도 발생하는데, 이 때에는 파일 시스템 또는 동영상 저장 방식에 따라 복구한다. 이렇게 수집한 동영상 파일은 CCTV 분석 프로그램이나 관련 응용 프로그램을 이용한 분석 과정을 통해 사건 시점에 용의자가 해당 장소에 있었는지 여부를 판별하는 데 사용된다.

마지막으로 용의자가 사용한 컴퓨터를 분석해야 한다. 인터넷 사용 흔적과 사용자의

사용 문서를 통해 증거 분석을 해야 한다. 관련된 증거 수집과 분석이 끝나면 분석 내용을 보고서로 작성한 후 형사사건 수사절차를 진행한다.

자살의 경우 정확한 사인 및 타살 여부를 확인하기 위해 디지털 증거 분석이 필요하다. 일반적으로 자살을 결심한 사람은 인터넷을 통해 관련 정보를 얻거나, 죽음에 관한 글을 작성하는 경우가 많다. 따라서 인터넷 사용 흔적 분석으로 자살 관련 단어의 검색여부 및 미니홈피, 블로그 등 개인 홈페이지에 게시한 자살을 암시하는 글, 그리고 인터넷 동호회 형태의 자살 모임 가입 유무 등을 발견할 수 있다. 또한 워드프로세서를 이용하여 작성한 유서 혹은 그간 작성한 일기와 같이 문서로 자살 관련 흔적이 남아있을 수 있기 때문에 최근 사용한 문서를 중심으로 하드디스크 내 저장된 문서를 유심히 살펴보아야 한다. 이외에도 사용했던 휴대폰의 통화내역, 문자, 저장된 일정이나 메모 등으로 자살의 원인 파악이 가능할 수 있다.

D. 명예훼손 및 허위사실 유포



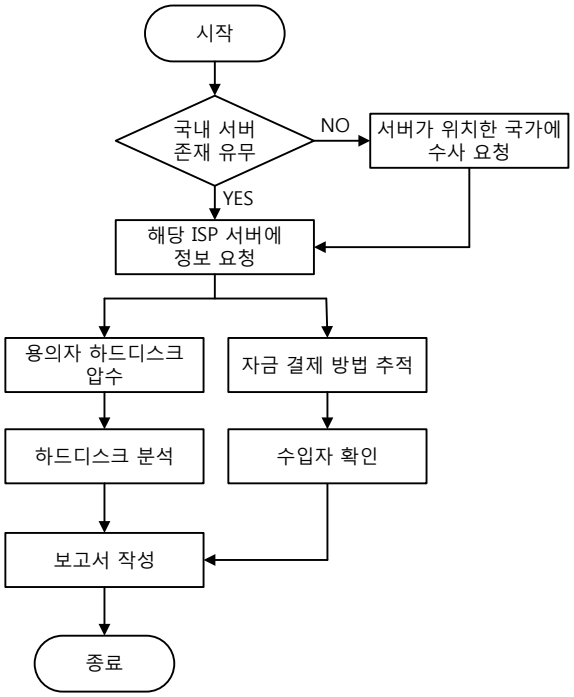
명예훼손 및 허위사실 유포는 민사사건에 속하며, 이는 명예훼손을 당한 당사자가 직접 고소, 고발해야 하는 친고죄로 경찰, 검찰의 조사 후 해당 유포자가 처벌된다.

수사를 위해 우선 해당 ISP에 협조 요청을 해야 한다. 그래서 해당 용의자의 IP 주소 등 용의자를 판단할 수 있는 정보를 얻어야 한다. 이렇게 용의자의 정보를 확인한 후 반복적이고 지속적인 역추적 과정을 해야 한다. 특히 네트워크 사용, 로그 정보를 확인해야 한다.

그리고 용의자의 컴퓨터를 압수해서 사건과 관련된 정보를 확인해야 한다. 악성 댓글 등 인터넷을 통한 허위사실 유포로 인해 명예훼손이 일어난 경우, 해당 웹 사이트에 글이 게시된 시간과 근접한 때에 방문한 웹 페이지 및 로그인 기록과 같이 인터넷 사용 시 남게 되는 흔적으로 유포자의 행위 유추가 가능하다. 또한 메신저 및 이메일 사용흔적에서 사건의 단서를 포착할 수 있다. 이 때 유포자의 컴퓨터에 저장된 문서 중 직접 작성한 것으로 보이는 문서를 이용하여 실제 명예훼손 관련 게시글과 유사한지 문장 패턴을 대조해본다. 이렇듯 텍스트 기반의 글 이외에 임의로 조작된 합성사진 혹은 음성파일, 동영상 파일이 첨부된 무단 게재 게시물이 발견된 경우에는 유포자의 하드디스크에 저장되어 있는지 존재 여부를 확인해야 한다. 그리고 모바일 기기, 외부저장장치의 사용 여부를 확인해야 한다.

마지막으로 이러한 결과를 보고서로 작성, 제출하고, 민사사건 수사 절차를 진행하게 된다.

E. 음란물 배포 및 인터넷 도박



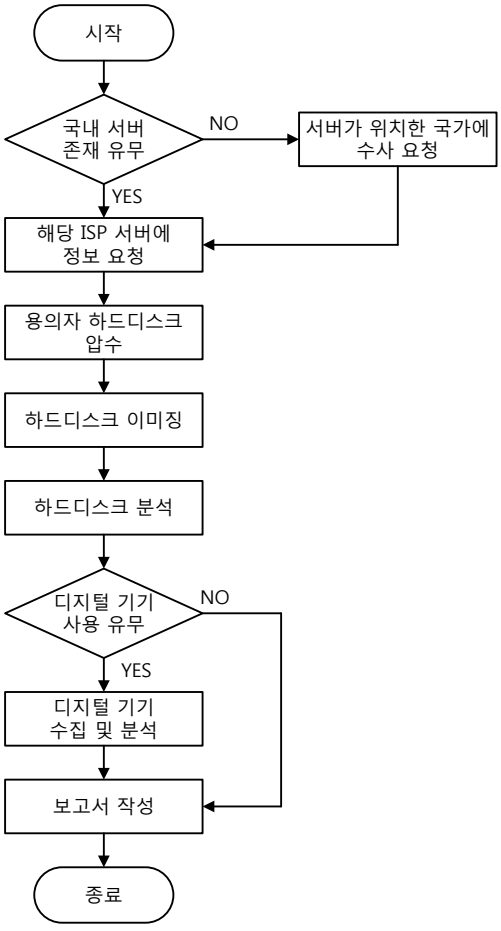
음란물 배포 및 인터넷 도박 사건은 크게 해당 서비스의 제공자와 이용자로 나누어

수사를 진행해야 한다.

먼저 서비스를 이용할 수 있는 서버의 위치와 현재 서버에 접속 중인 이용자에 대한 정보 수집 단계가 필요하다. 그리고 이 단계에서는 실제 이러한 서비스를 제공하고 있는 인물의 정보를 파악하는 것이 가장 중요하다. 수사권이 닿지 않는 제3국에 개설된 서버의 경우 복합적인 수사를 진행해야 하며, 국내 P2P나 웹 공유사이트, 웹하드를 이용하여 배포했을 경우에는 ISP 서버로부터 용의자에 관한 정보를 수집한다. 서비스가 제공중인 서버 확인 후에는 자금 결제 방법을 추적해야 한다. 이를 추적하면 실제 음란물 배포를 통한 수익자를 알 수 있기 때문이다.

앞서 살펴본 과정으로 서비스를 제공한 용의자 관련 정보가 수집되면, 실제 배포한 원본 및 복사본 데이터를 수집해야 한다. 우선 배포된 자료와 동일한 파일을 파일 메타데이터의 시그니처 검색이나 키워드 검색 등의 방법으로 찾는다. 다음으로 음란물과 불법 복제에 사용된 응용프로그램 및 장치를 수집한다. 특히 디지털 사진의 경우, 촬영에 사용된 디지털 카메라 정보 및 촬영 시간 등이 존재하기 때문에 원본과의 대조가 용이하다고 볼 수 있다.

F. 저작권 침해 (불법 소프트웨어)



불법 소프트웨어 이용 등 저작권 침해 사건이 일어난 경우, 먼저 해당 소프트웨어를 사용한 흔적을 찾아야 한다. 이는 용의자가 특정 웹하드에 파일을 업로드한 적이 있는지, 그리고 하드디스크에 해당 소프트웨어가 존재하는지 그 여부로 판별할 수 있다. 소프트웨어 사용 여부는 실행횟수, 실행일자 등을 통해 확인이 가능하다. 만약 소프트웨어가 설치되어 있지 않다면, 사용 후 삭제한 경우를 의심하여 레지스트리 분석 등을 통해 삭제 여부를 확인한다.