사이버 범죄 수사 : 초동 수사를 위한 지침

개요

오늘날 컴퓨터와 다른 전자 기기들은 일상 생활의 모든 곳에 다 존재한다. 옛날에는 컴퓨터 한대가 방 전체를 꽉 채우고 있었지만, 요즘에는 컴퓨터가 손바닥만해졌다. 법 집행기관을 도와준 진보된 기술은 범죄자에게도 동일하게 이용되고 있다.

컴퓨터는 범행 도구로 사용될 수도 있고, 범죄의 증거를 포함할 수도 있으며, 심지어는 범죄의 대상이 되기도 한다. 발견되는 디지털 증거의 역할과 특성에 대한 이해, 잠재적인 디지털 증거를 포함하는 범행 장소의 처리 방식, 이러한 상황에 따른 수사 기관의 대응 방식이 중요한 문제가 되었다. 이 지침서는 다양한 범행 장소에서 디지털 증거의 파악, 수집, 보관에 관한 법 집행 기관, 학계, 민간 부문의 축적된 경험을 나타낸다.

디지털 증거에 대한 법집행기관의 대응

법집행기관은 디지털 증거를 처리할 때 관리자, 수사관, 포렌식 조사자, 부서장 모두에게 어떤 역할을 요구한다. 이 문서는 디지털 증거의 최초 처리자를 위한 지침을 제공한다. 최초 처리자는 디지털 증거의 파악, 수집, 보존, 이송, 저장에 대해 책임져야 할 것이다. 오늘날, 이러한 사항은 법집행기관의 거의 모든 구성원에게 해당된다. 관리자는 일상 업무 동안 디지털 기기와 마주칠 것이다. 수사관은 디지털 증거를 직접 수집하거나 수집을 감독할 것이다. 포렌식 조사자는 범행 현장 조사에 도움을 주거나 증거를 조사할 것이다. 부서장은 직원이 디지털 증거를 취급하기에 충분한 훈련을 받고, 적절한 장비를 보유하도록 할 책임이 있다.

디지털 증거를 취급하는 자는 모두 디지털 증거가 훼손되기 쉽다는 것을 명심해야 하며, 증거 수집과 보존에 관련된 원칙과 절차를 이해하여야 한다. 원본 증거를 변경, 손상, 파괴할 가능성이 있는 행동은 법정에서 면밀히 검토될 것이다.

절차는 사이버 범행 현장 조사를 촉진하는 형태이어야 한다. 부서장은 서비스를 제공할 인원과 필요한 예산을 결정하여야 한다. 직원은 기초 교육과 지속적인 기술적 훈련을 받아야만 한다. 종종 특정 사건은 좀더 깊이 있는 전문 기술, 훈련, 장비를 요구할 것이기 때문에 부서장은 이러한 사건에 대처할 방법에 관한 계획을 수립해야 한다. 디지털 증거에 대처해야 하는 요구가 가까운 장래에 증가할 것으로 예견된다. 이러한 요구에 부응하려면 그에 걸맞는 자원의 배정이 필요하다.

디지털 증거의 잠재성

디지털 증거는 수사할 가치가 있는 디지털 기기에 저장되거나 전송되는 정보와 데이터이다. 지문이나 DNA가 증거가 범행 현장에 잠재되어 있는 것처럼 디지털 증거 역시 그렇다.. 그것의 본질적인 특성 때문에 디지털 증거가 있는 물리적 객체에 포함되어 있는 것을 직접

적으로 볼 수는 없다. 증거를 가독성 있게 만들기 위해서는 장비와 소프트웨어가 필요하다. 조사 과정과 그 과정에서의 한계점 등을 설명하기 위해서 증언이 요구될 수 있다.

디지털 증거는 훼손되기 쉬운 속성을 가지고 있다. 부적절하게 취급하거나 조사하면 변경, 손상, 파괴될 수 있다. 이러한 이유 때문에, 디지털 증거의 기록, 수집, 보존, 조사할 때에는 특별한 주의가 있어야 한다. 이러한 조치에 문제가 발생하면 증거를 사용할 수 없게 되거나 부정확한 결론으로 이어질 수 있다. 이 지침서는 디지털 증거의 무결성을 보존하는데 도움을 줄 수 있는 방법을 제시한다.

포렌식 조사 과정

디지털 증거의 특성 때문에 법정에서 채택되기까지 특별한 논란이 있을 것이다. 이러한 법정 논란에 대처하기 위해서는 적합한 포렌식 절차에 따라야 한다. 포렌식 절차는 좀더 세분화할 수 있지만 크게 수집, 조사, 분석, 보고의 네 단계로 이루어진다. 이 지침서는 수집 단계를 집중해서 다루지만 다른 세 단계의 특성과 각 단계에서 해야하는 것을 파악하고 있어야 할 것이다.

수집 단계는 디지털 증거의 검색, 파악, 수집 및 해당 과정의 기록으로 이루어진다. 수집 단계는 특별한 주의를 하지 않으면 사라지는 정보가 있어 실시간으로 해야 하는 경우도 있다.

조사 단계는 증거를 가독성 있게 만들고, 그것의 근원과 중요성을 설명하는 과정이다. 이 과정은 몇 단계로 세분할 수 있다. 우선 전체적인 증거의 내용과 상태를 기록해야 한다. 이러한 사항이 기록된 문서는 모든 당사자가 증거에 포함되어 있는 것을 알 수 있게 한다. 이 과정에는 은닉되거나 모호한 정보의 검색이 포함된다. 모든 정보가 가독성 있는 형태로 변환되면, 가치 있는 것과 없는 것을 분리하는 데이터 축소 과정을 시작한다. 컴퓨터 저장 장치에는 엄청난 양의 정보가 있기 때문에, 이 과정이 조사 단계의 핵심이라 할 수 있다.

조사 단계의 산출물을 사건 관점에서의 중요성과 증거로써 가치 있는지 살펴보는 과정이 분석이다. 포렌식 조사자의 업무인 기술적 검토가 조사인 반면, 분석은 수사팀에서 수행하는 과정이다. 일부 기관에서는 동일인 또는 같은 부서에서 이러한 역할을 둘다 수행할 수 있다.

조사 과정과 의미있는 복구 데이터를 설명한 보고서를 작성함으로써 조사가 종료된다. 조사 일지는 감제 발표(discovery) 또는 증언을 위해 보존되어야만 한다. 조사자는 조사 행위뿐만아니라 조사를 수행할 자격과 조사 절차의 타당성에 대하여 증언할 필요가 있을 수 있다.

서론

이 지침서는 법집행기관과 디지털 증거가 포함된 범죄 현장을 보호하고, 디지털 증거를 파악, 수집, 보존할 책임이 있는 담당자를 위해 작성되었다. 모든 것을 포괄하는 것은 아니며, 단지 디지털 증거를 다룰 때 당면하게 되는 가장 공통된 상황만을 다룬다. 기술이 급속도로 발전하고 있기 때문에 이 지침서에서 제시하는 것은 현재 기술을 반영하여 검토하여야 하며, 실제 적용에서는 상황에 맞게 적절히 대처해야 한다. 모든 범행 현장은 모두 다르기 때문에 이 지침서의 실행 과정에서 초기 대응자/수사관의 판단은 존중되어야 한다. 게다가, 책임이 있는 부서장 또는 특별한 훈련을 받은 지원 인력은 경험 수준, 조건, 가용 장비를 포함하여 환경을 보장함으로써 행동을 조정하여야 한다. 이 지침서는 포렌식 분석을 다루지 않는다. 개별 사건의 환경과 연방, 주, 자치단체의 법/규칙은 이 지침서에 기술된 것과 다른 행동을 요구할 수도 있다.

디지털 증거를 취급할 때에는, 일반적인 포렌식 절차와 원칙이 적용되어야 한다.

- 디지털 증거를 수집하고 보호하는 행위는 증거를 변경시키지 않아야 한다.
- 디지털 증거를 조사하는 자는 이러한 목적을 위해 훈련되어야 한다.
- 디지털 증거의 압수, 조사, 저장, 이송과 관계된 행동은 모두 기록되고, 보존되며, 재검토가 가능해야 한다.

이 지침서는 누가 읽어야 하는가?

- 디지털 증거가 포함될 가능성이 있는 범행 현장 출동자
- 디지털 증거를 포함하는 범행 현장의 처리자
- 이러한 범행 현장의 처리자를 지휘하는 자
- 이러한 범행 현장을 처리하는 조직을 관리하는 자

※ 필요한 기술의 습득과 훈련을 받지 못한 자가 컴퓨터 또는 다른 전자 기기로부터 데이터를 복구하거나 내용을 검색하려고 하지 않아야 하며, 심지어는 키보드에 접촉하거나 마우스를 클릭하지 않아야 한다.

무엇이 전자 기기인가?

디지털 증거는 전자 기기에 의해서 저장되거나 전송 중인 정보로 수사할 가치가 있는 데이터이다. 이러한 증거는 조사할 목적으로 데이터 또는 그것을 포함하고 있는 물리적 대상을 수집, 저장할 때 획득된다.

디지털 증거는 다음과 같은 특성이 있다.

- 지문 또는 DNA 증거와 유사하게 물리적 대상에 내재해 있다.

- 국경을 넘어가는 것이 아주 쉽고 빠르게 이루어진다.
- 훼손되기 쉬우며, 변경, 손상, 파괴가 요이하다.
- 종종 시간에 민감(time-sensitive)하다. .

범행 현장에서 디지털 증거를 어떻게 취급하는가?

디지털 증거를 수집, 보존, 조사할 때에는 세심한 주의가 필요하다.

범행 현장에서 디지털 증거를 취급할 때는 보통 다음의 절차를 따른다. :

- 증거의 파악과 식별
- 범행 현장의 기록
- 증거의 수집과 보존
- 증거의 포장과 이송

이 지침서에서 제시하는 정보는 다음을 가정한다 :

- 증거를 검색하고 압수하는데 필요한 법적 권한을 획득했다.
- 범행 현장은 안전하게 보호되었고 사진 촬영 또는 스케치나 일지 형태로 기록되었다.
- 필요에 따라 범행 현장을 보호하는 장갑과 같은 장비가 사용된다.

※ 초기 출동자가 디지털 증거를 압수할 때는 매우 세심한 주의가 필요하다. 전자 기기에 저장되어 있는 데이터에 대하여 부적합하게 접근하면 Electronic Communication Privacy Act를 포함하여 연방법을 위반할 수 있다. 추가적인 법적 절차가 필요할 수 있다. 전자 기기에 접근하기 전에 담당 검사의 자문을 받기 바란다. 디지털 증거는 훼손되기 쉽기 때문에 적합한 인원에 의해 조사가 진행되야 한다.

디지털 증거를 취급하기 위한 준비가 되어 있는가?

모든 기관은 담당 지역의 컴퓨터 전문가를 미리 확인할 것을 권고한다. 이들 전문가는 초기 출동자 또는 부서의 기술적 역량으로 처리할 수 없는 상황에 도움을 줄 것이다. 또한 수사 계획은 부서 정책과 연방, 주, 자치단체의 법률을 준용하여 수립할 것을 권고한다. 특히, Privacy Protection Act의 예외 조항으로 기자(대중에게 정보를 알리는 자)가 소유하고 있는 물체를 정부 직원이 검색 또는 압수하는 것은 불법이다. 예를 들면, 뉴스 초안이나 웹 페이지와 같은 수정 헌법 제 1조에 해당하는 물체의 압수는 Privacy Protection Act와 연관되어 있을 것이다.

이 지침서는 다음과 같은 사항에 도움이 될 것이다 :

- 자원에 대한 접근

- 절차의 개발
- 부여된 역할과 임무
- Considering officer safety
- 범행 현장에 출동할 때 보유해야 할 장비와 물품을 파악하고 문서화

제 1 장　전자 기기: 종류와 잠재적 증거

요즈음 사람들이 사용하는 다양한 전자 기기에 디지털 증거가 내재되어 있을 수 있다. 이 장에서는 범행 현장에서 공통적으로 접하는 다양한 유형의 전자 기기를 살펴보고, 각 전자 기기의 간략한 사용 방법을 설명하고자 한다. 추가적으로 각 전자 기기에서 발견될 수 있는 디지털 증거를 설명한다.

※ 많은 전자 기기에는 정보를 유지하려면 배터리 또는 전원 케이블에 의하여 지속적으로 전원을 공급해야 하는 메모리가 탑재되어 있다. 따라서 전원을 차단하거나 배터리가 방전되면 데이터가 쉽게 손실될 수 있다.(참고: 수집 방법을 결정한 후에 필요하다면 복구 기기와 함께 전원 어뎁터나 케이블을 수집하고 보관하라.)

컴퓨터 시스템

설명 : 컴퓨터 시스템은 일반적으로 중앙처리장치(CPU), 데이터 저장 장치, 모니터, 키보드, 마우스로 구성된다. 단독으로 사용될 수도 있고 네트워크에 연결될 수도 있다. 랩탑, 데스크탑, 타워 시스템, 랙(Rack) 마운트 시스템, 미니컴퓨터, 메인프레임 등과 같이 많은 유형의 컴퓨터가 존재한다. 추가적인 설비로 모뎀, 프린터, 스캐너, 도킹 스테이션, 외부 데이터 저장 장치 등이 포함되어 있는 경우가 많다. 예를 들면, 데스크탑은 외부 키보드와 마우스, 케이스, 메인보드, CPU, 저장 장치 등으로 구성된 컴퓨터 시스템이다.

주요 용도 : 문서 작업, 계산, 통신, 그래픽 등을 포함한 모든 형태의 계산 작업과 정보 저장.

잠재적 증거 : 증거는 대부분 하드드라이브와 저장 매체에 저장된 파일에서 발견된다.
구체적인 예는 다음에서 열거한다.

사용자 생성 파일

사용자 생성 파일에는 범죄 조직을 증명할 수 있는 주소록과 데이터베이스 파일, 아동 성학대 관련 정지영상 또는 동영상, 이메일 또는 편지와 같은 범죄자들 간의 통신 내용 등의 범죄 행위의 중요한 증거가 포함되어 있기도 한다. 또한, 마약 거래 목록들은 스프레드시트에서 자주 발견되기도 한다.

- ◆ 주소록
- ◆ 오디오/비디오 파일
- ◆ 달력
- ◆ 데이터베이스 파일
- ◆ 문서 또는 텍스트 파일
- ◆ 이메일 파일
- ◆ 이미지/그래픽 파일
- ◆ 인터넷 북마크/즐겨찾기
- ◆ 스프레드시트 파일

사용자 보호 파일

사용자는 다양한 형태로 증거를 숨길 수 있다. 예를 들면, 사용자들은 그들에게 중요한 데이터를 암호화하거나 패스워드로 보호할 수 있다. 그들은 또한 하드디스크나 다른 파일의 내부에 파일을 숨기거나 범죄 증거 파일의 이름을 고의적으로 내용과 무관하게 부여하기도 한다.

- ◆ 압축 파일
- ◆ 암호 파일
- ◆ 숨김 파일
- ◆ 내용과 무관하게 명명된 파일
- ◆ 패스워드로 보호된 파일
- ◆ 스테가노그라피

한편 증거는 컴퓨터 운영체제의 일반 기능에 의해 생성된 파일이나 데이터 영역에서 발견되기도 한다. 많은 경우, 사용자는 운영 체제가 생성한 데이터를 인식하지 못한다. 패스워드, 인터넷 행위, 그리고 임시 백업 파일들은 종종 복구하고 조사하는 데이터의 예이다.

주의: 파일의 구성 요소에는 생성, 수정, 삭제, 접근 일시와 사용자 이름 또는 식별자, 파일 속성 등과 같은 증거로서 가치 있는 데이터가 있다.

컴퓨터 생성 파일

- ◆ 백업 파일
- ◆ 설정 파일
- ◆ 쿠키 (Cookies)
- ◆ 숨김 파일
- ◆ 히스토리 파일
- ◆ 로그 파일
- ◆ 프린터 스풀 파일
- ◆ 스왑 파일
- ◆ 시스템 파일
- ◆ 임시 파일

다른 데이터 영역

- ◆ Bad clusters
- ◆ 컴퓨터 날짜, 시간, 그리고 패스워드
- ◆ 삭제된 파일
- ◆ 비어있는(free) 공간
- ◆ 숨김 파티션
- ◆ Lost clusters
- ◆ 메타데이터
- ◆ 다른 파티션
- ◆ 예약된 영역
- ◆ 슬랙(slack) 공간
- ◆ 소프트웨어 등록 정보
- ◆ 시스템 영역
- ◆ 미할당된 공간

컴퓨터의 구성요소

중앙처리장치(CPU)

설명 : 종종 "칩"이라고 불리며, 컴퓨터 내부에 있는 마이크로프로세서이다. 마이크로프로세

서는 다른 전자 부품들과 함께 컴퓨터 내부의 회로 기판 위에 위치해 있다.

주요 용도 : 컴퓨터의 모든 산술 연산과 논리 기능들을 수행하고, 컴퓨터의 운영을 통제한다.

잠재적 증거 : 그 자체가 부품 절취, 위조의 증거가 될 수 있다.

메모리

설명 : 컴퓨터 내부에 있는 착탈이 가능한 회로판. 보통 여기에 저장된 정보는 컴퓨터 전원이 꺼질 때 보존되지 않는다.

주요 용도 : 컴퓨터가 동작하는 동안 사용자의 프로그램과 데이터를 저장.

잠재적 증거 : 그 자체가 부품 절취, 위조의 증거가 될 수 있다.

접근 통제 장치

스마트카드, 동글, 생체 인식기

설명 : 스마트카드는 금융 정보, 암호 키나 인증 정보(패스워드), 공개키 인증서, 또는 부가 정보를 저장하며, 마이크로프로세서가 탐재된 손만한 크기의 장치이다. 동글(Dongle)은 스마트카드에 저장하는 정보와 유사한 정보를 담고 있으며, 컴퓨터 포트에 끼울 수 있는 작은 장치이다. 생체 인식기는 컴퓨터 시스템에 접속되는 장치로 지문, 목소리, 망막과 같은 개인의 생체 정보를 인식한다.

주요 용도 : 암호 키와 같이 컴퓨터나 프로그램 또는 기능에 대한 접근을 통제하는데 사용한다.

잠재적 증거 : 카드나 사용자의 식별/인증 정보, 접근 수준, 설정 정보, 허가 정보, 그리고 장비 자체

자동응답기

설명 : 전화기의 한 부분이거나 전화기와 연결된 전자 장치. 자기테이프나 테이프를 사용하는 모델과 디지털 레코딩 시스템을 사용하는 모델이 있다.

주요 용도 : 수신자가 부재중이거나 전화를 받지 않을 때, 발신자가 남기는 음성 메시지를

녹음한다. 보통 수신자가 남긴 메시지가 재생된 후 송신자의 메시지가 녹음된다.

주의 : 배터리는 한정된 수명을 가지고 있기 때문에, 배터리가 방전된다면 데이터는 손실될 수 있다. 그래서 담당 직원들(예를 들면, 증거 보관자, 포렌식 연구실장, 포렌식 조사관)은 배터리에 의해 구동되는 장치인 경우 즉각적인 대응이 필요함을 숙지해야 한다.

잠재적 증거 : 자동응답기는 음성 메시지를 저장하며, 일부 경우에는 메시지가 남겨진 때의 시간 및 날짜 정보를 저장할 수 있다. 또한 다음과 같은 음성 녹음을 포함하고 있기도 한다.

- ◆ 발신자 식별 정보
- ◆ 삭제된 메시지
- ◆ 마지막 수신 번호
- ◆ 메모
- ◆ 전화번호와 이름
- ◆ 테잎

디지털 카메라

설명 : 카메라의 일종으로, 컴퓨터 매체로 이미지와 비디오의 전송이 가능한 변환 하드웨어와 저장 장치가 있는 이미지와 비디오 디지털 녹화 장치.

주요 용도 : 디지털 카메라는 재생 또는 편집하기 위하여 컴퓨터 저장 매체로 전송이 용이한 디지털 형식의 이미지나 비디오를 갈무리한다.

잠재적 증거 :

- ◆ 이미지
- ◆ 탈착되는 카트리지
- ◆ 사운드
- ◆ 시간과 날짜 스탬프
- ◆ 비디오

소형 휴대(Handheld) 장치 (PDA, 전자수첩)

설명 : PDA(Personal Digital Assistant)는 계산, 전화/팩스, 호출(paging), 네트워킹, 또는 다른 기능이 있는 소형 장치이다. 보통 개인 수첩의 용도로 사용된다. 소형 휴대 컴퓨터는 데스크탑 컴퓨터 시스템의 모든 기능과 거의 같다. 디스크 드라이브가 없는 모델도 있지만, 모뎀, 하드 드라이브, 또는 다른 장치들을 연결할 수 있는 PC 카드 슬롯을 가지고 있기도 한다. 그것들은 보통 크래들(받침대)를 통한 접속으로 다른 컴퓨터 시스템과 데이터를 동기화할 수 있는 기능이 있다. 만약 크래들(받침대)이 있다면, 관련된 소형 휴대 장치를 찾도록 한다.

주요 용도 : 휴대용 계산, 저장, 통신 기기로 정보를 저장할 수 있다.

주의 : 배터리는 한정된 수명을 가지고 있기 때문에, 배터리가 방전된다면 데이터는 손실될 수 있다. 그래서 담당 직원들(예를 들면, 증거 보관자, 포렌식 연구실장, 포렌식 조사관)은 배터리에 의해 구동되는 장치인 경우 즉각적인 대응이 필요함을 숙지해야 한다.

잠재적 증거 :

- ◆ 주소록
- ◆ 약속 일정/정보
- ◆ 문서
- ◆ 이메일
- ◆ 메모
- ◆ 패스워드
- ◆ 전화번호부
- ◆ 텍스트 메시지
- ◆ 음성 메시지

하드 드라이브

설명 : 자기적으로 데이터를 저장할 수 있는 물질로 코팅된 정밀한 원판(디스크)이 탑재되어 있는 봉인된 상자 모양의 기기. PC의 내부 뿐만아니라 외장 형태도 있다.

주요 용도 : 컴퓨터 프로그램, 텍스트, 사진, 비디오, 멀티미디어 파일 등과 같은 정보의 저장.

잠재적 증거 : '컴퓨터 시스템' 절의 잠재적 증거를 참조하라.

메모리 카드

설명 : 전원이 차단되어도 정보가 손실되지 않는 탈착이 가능한 전자적 저장 장치이다. 메모리 카드에서 지워진 이미지도 복구가 가능한 경우도 있다. 메모리 카드는 신용카드 크기의 모듈에 수백 개의 이미지를 저장할 수 있다. 컴퓨터, 디지털 카메라, PDA를 포함하여 다양한 전자 장치에서 사용된다. 메모리 카드의 예로 메모리 스틱, 스마트 카드, 플래시 메모리, 플래시 카드 등이 있다.

주요 용도 : 착탈 방식으로 정보의 저장과 전송

잠재적 증거 : '컴퓨터 시스템' 절의 잠재적 증거를 참조하라.

모뎀

설명 : 모뎀, 내장형과 외장형(아날로그, DSL, ISDN, Cable), 무선 모뎀, PC 카드

주요 용도 : 모뎀은 전화선, 무선, 또는 다른 통신 매체를 통해 컴퓨터나 네트워크에 접근을 가능하게 함으로써 전자 통신을 쉽게 하는데 사용된다.

잠재적 증거 : 장치 자체

네트워크 구성요소

LAN 카드 또는 네트워크 인터페이스 카드(NIC)

주의 : 이 구성요소는 컴퓨터 네트워크를 나타낸다. 컴퓨터 시스템 또는 접속 장치를 다루기 전에 5장에 있는 네트워크 시스템 증거에 대한 설명을 참조하라.

설명 : 네트워크 카드, 부속 케이블. 네트워크 카드는 무선일 수 있다.

주요 용도 : LAN/NIC 카드는 컴퓨터를 연결하기 위해 사용된다. 카드는 정보의 교환과 자원의 공유를 가능하게 해준다.

잠재적 증거 : 장치 자체, MAC (Media Access Control) 접근 주소.

라우터, 허브, 스위치

설명 : 이 전자 장치는 컴퓨터 시스템 망에서 사용된다. 라우터, 스위치, 허브는 다른 컴퓨터 또는 네트워크에 연결할 수 있는 방법을 제공한다. 이것들은 종종 여러 케이블이 연결되어 있는 곳에서 파악된다.

주요 용도 : 네트워크를 통한 데이터 분배를 쉽게 하는데 사용된다.

잠재적 증거 : 장치 자체, 또한 라우터의 경우는 설정 파일.

서버

설명 : 서버는 네트워크를 통해 연결되어 있는 다른 컴퓨터에게 특정 서비스를 제공하는 컴퓨터이다. 랩탑을 포함한 어떠한 컴퓨터도 서버로 설정될 수 있다.

주요 용도 : 네트워크를 통한 이메일, 파일 저장, 웹페이지 서비스, 인쇄 서비스와 같은 자원를 공유하는데 사용한다.

잠재적 증거 : '컴퓨터 시스템' 절의 잠재적 증거를 참조하라.

네트워크 케이블과 커넥터

설명 : 네트워크 케이블은 색, 굵기, 모양이 다를 수 있으며, 연결하는 장치별로 다른 커넥터가 있다.

주요 용도 : 컴퓨터 네트워크의 각 구성요소들을 연결한다.

잠재적 증거 : 장치 자체

무선 호출 수신기 (Pager)

설명 : 휘발성 증거(전화번호, 음성 메일, 이메일)를 담고 있는 손에 쥘만한 크기의 휴대용 전자 장치. 휴대폰과 PDA도 무선 호출 수신 장치의 기능이 있다.

주요 용도 : 전자 메시지, 숫자(전화번호 등)과 알파벳(텍스트, 이메일 등을 포함)을 송수신

주의 : 배터리는 한정된 수명을 가지고 있기 때문에, 배터리가 방전된다면 데이터는 손실될 수 있다. 그래서 담당 직원들(예를 들면, 증거 보관자, 포렌식 연구실장, 포렌식 조사관)은 배터리에 의해 구동되는 장치인 경우 즉각적인 대응이 필요함을 숙지해야 한다.

잠재적인 증거 :

- ◆ 주소 정보
- ◆ 이메일
- ◆ 전화 번호
- ◆ 텍스트 메시지
- ◆ 음성 메시지

프린터

설명 : 케이블(시리얼, 패러럴, USB, Firewire) 또는 적외선 포트를 통해 컴퓨터에 연결되는 레이저, 잉크젯 등의 다양한 인쇄 시스템을 지칭한다. 일부 모델은 인쇄하는 동안 컴퓨터로부터 여러 페이지 문서를 수신하여 저장하는 메모리 버퍼가 있으며, 하드드라이브를 가지고 있는 경우도 있다.

주요 용도 : 컴퓨터에 있는 텍스트, 이미지 등을 종이로 인쇄한다.

잠재적 증거 : 프린터는 사용 기록, 시간과 날짜 정보를 유지하는 경우가 있으며, 네트워크에 연결되었다면 네트워크 식별 정보가 저장될 수 있다. 추가적으로 각 프린터를 식별하기 위한 유일한 특정 정보가 존재할 수 있다.

- ◆ 문서
- ◆ 하드 드라이브
- ◆ 잉크 카트리지
- ◆ 네트워크 식별자/정보
- ◆ 잉크롤러 상의 인화된 이미지
- ◆ 시간과 날짜 스탬프
- ◆ 사용자별 사용 기록

이동 저장 장치와 매체

설명 : 전자, 자기, 또는 디지털 정보를 저장하기 위한 매체 (예를 들면, 플로피 디스크, CD, DVD, 카트리지, 테이프).

주요 용도 : 컴퓨터 프로그램, 텍스트, 사진, 비디오, 멀티미디어 파일 등을 저장할 수 있는 휴대용 장치

새로운 형태의 저장 장치와 매체들이 자주 출시되며, 여기에 예로 든 것은 일부임을 염두에 두기 바란다.

잠재적 증거 : '컴퓨터 시스템' 절의 잠재적 증거를 참조하라.

스캐너

설명 : 종이 문서를 스캔하여 파일로 변환하여 컴퓨터로 송신하는 광학 장치.

주요 용도 : 문서, 사진 등을 컴퓨터에서 열람, 조작하거나 전송할 수 있도록 전자 파일로 변환한다.

잠재적 증거 : 장치 자체가 증거가 될 수 있다. 스캐너의 보유는 불법 행위 (예를 들면, 아동 음란물, 위조 수표, 위폐, 위조 신분증 등)를 증명하는데 일조한다. 추가적으로, 스캐너 유리의 얼룩과 같은 결함은 문서를 처리하는데 사용된 스캐너를 특정할 수 있게 해준다.

전화

설명 : 무전기, 또는 무선전화기, 또는 통신로에 직접 연결된 것. 내부 배터리, 전원 플러그,

또는 전화 시스템으로부터 직접 전원을 받아 작동한다.

주요 용도 : 전화통신선, 무선 전송, 셀룰러 시스템, 또는 두 개 이상의 조합으로 두 기계간의 양방향 통신에 사용. 정보를 저장할 수 있는 전화도 있다.

주의 : 배터리는 한정된 수명을 가지고 있기 때문에, 배터리가 방전된다면 데이터는 손실될 수 있다. 그래서 담당 직원들(예를 들면, 증거 보관자, 포렌식 연구실장, 포렌식 조사관)은 배터리에 의해 구동되는 장치인 경우 즉각적인 대응이 필요함을 숙지해야 한다.

잠재적 증거 : 많은 전화기들은 이름과 전화번호, 그리고 발신자 식별 정보를 저장할 수 있다. 게다가, 휴대폰은 약속 일정을 저장하고, 전자 메일과 쪽지를 받으며, 음성 녹음기와 같은 기능을 수행할 수도 있다.

- ◆ 약속 일정/정보
- ◆ 발신자 식별 정보
- ◆ 전자 시리얼 번호
- ◆ 이메일
- ◆ 메모
- ◆ 패스워드
- ◆ 전화번호부
- ◆ 텍스트 메시지
- ◆ 음성 메일
- ◆ 웹 브라우저

기타 전자 장치

범죄 현장에서 발견되는 전자 장비의 종류는 매우 많아서 모두 열거하는 것은 어렵다. 그러나 일반적이지 않은 장비들 중에 우수한 수사 정보나 증거의 원천이 되는 경우가 많이 있다. 예를 들면, 신용카드 정보수집기(Skimmer), 휴대폰 복제 장비, 발신자 ID 기계, 오디오 녹음기, 웹 TV 등이 있다. 팩스, 복사기, 복합기 중에는 내부 저장 장치를 가지고 있는 경우가 있는데 그 중에서 증거가치가 있는 정보를 담고 있을 수 있다.

강조사항 : 이런 형태의 증거에 대해 조사하려면 수색 영장이 필요하다. 서론의 마지막 부분을 참조하라.

복사기

어떤 복사기는 사용자 접근 기록과 복사 이력을 유지한다. 스캔 후 프린트 기능을 가진 복사기들은 문서를 메모리에 한번 스캔한 후에 인쇄를 진행한다.

잠재적 증거 :

- ◆ 문서
- ◆ 시간과 날짜 스탬프
- ◆ 사용자 이용 기록

신용카드 정보수집기 (Skimmers)

신용카드 정보수집기는 플라스틱 카드 상의 자기띠에 담겨진 정보를 읽는데 사용된다.

잠재적 증거 : 자기띠의 트랙에는 다음과 같은 카드소지자 정보가 담겨 있다.

- ◆ 카드 만기일
- ◆ 신용카드 번호
- ◆ 사용자의 주소
- ◆ 사용자의 이름

전자 시계

어떤 전자 시계들은 디지털 메시지를 저장하는 무선 호출 수신기(Pager)와 같은 기능을 하는 것이 있다. 그것들은 주소록, 약속 일정, 이메일, 그리고 노트와 같은 추가적인 정보가 저장되어 있을 수 있다. 어떤 전자 시계는 컴퓨터와 정보를 송수신하는 기능을 가지고 있다.

잠재적 증거 :

- ◆ 주소록
- ◆ 약속 일정
- ◆ 이메일
- ◆ 노트
- ◆ 전화번호

팩스

팩스는 미리 입력된 전화번호와 송수신 문서의 이력을 저장할 수 있다. 게다가, 어떤 것들은 메모리를 가지고 있어 여러 장의 문서를 스캔한 후 송신하고, 수신된 정보를 메모리에 저장했다가 나중에 출력하는 기능이 있다. 심지어는 송수신되는 수백 쪽의 문서를 저장할 수 있다.

잠재적 증거 :

- ◆ 문서
- ◆ 필름 카트리지
- ◆ 전화번호
- ◆ 송수신 기록

위성 항법 장치 (GPS)

위성 항법 장치는 목적지 정보와 중간 지점, 그리고 경로를 통해 이전에 이동한 정보를 제공할 수 있다. 어떤 것들은 이동 기록을 포함하여 이전 목적지를 자동으로 저장한다.

잠재적 증거 :

◆ 집
◆ 이전 목적지
◆ 이동 기록
◆ 중간 지점 좌표
◆ 중간 지점 명칭

제 2 장　수사 도구와 장비

원칙 : 디지털 증거를 수집하기 위해서는 특별한 도구와 장비가 필요하다. 기술이 진보하면 필요한 도구와 장비도 변해야 한다.

정책 : 디지털 증거의 분류 및 기록, 차단, 추출, 포장, 이송에 필요한 도구와 장비에 접근할 수 있어야 한다.

절차 : 디지털 증거를 수집하는데 필요한 장비를 획득할 수 있도록 계획을 수립해야 한다. 필요한 도구와 장비는 분류 및 기록, 수집, 포장, 이송의 각 단계에 적합해야 한다.

툴 킷

해당 부서는 범행 현장을 처리하는 일반적인 도구를 보유해야 한다. (예. 카메라, 메모지, 스케치북, 증거 분류 양식, 범행 현장 차단용 테잎, 표시장치) 디지털 증거가 포함된 법행 현장에서 사용될 수 있는 추가적인 항목은 다음과 같다.

문서 작성 도구

◆ Cable tags
◆ 지워지지 않는 표시
◆ 스티커

시스템 분해 도구

다양한 크기와 여러 유형의 자성이 없는 물품
◆ 일자형과 십자형 드라이버
◆ 너트 드라이버
◆ 롱-노즈 집게
◆ Secure-bit 드라이버
◆ 소형 핀셋
◆ 특수용 십자 드라이버 (제조자가 별도로 제공한 물품, 예. 컴팩, 매킨토시)
◆ 표준 집게
◆ 성형 너트 드라이버
◆ 선 절단기

포장과 이송용 물품

◆ 정전기 방지 포장지
◆ 정전기 방지 버블랩(뽁뽁이)
◆ 케이블 타이
◆ 증거 가방
◆ 증거 테잎
◆ 포장용 물품 (스티로폼과 같은 정전기를 발생할 수 있는 물품은 제외)
◆ 포장용 테잎
◆ 다양한 크기의 튼튼한 박스

기타 물품

해당 부서의 툴 킷에 포함될 수 있는 항목들은 다음과 같다.
◆ 장갑
◆ 손수레
◆ 큰 고무줄
◆ 도움을 받을 수 있는 곳의 전화번호 목록
◆ 돋보기
◆ 인쇄용지
◆ 압수용 디스크
◆ 손전등
◆ 미사용 플로피 디스크($3^{1}/_{2}$ 과 $5^{1}/_{4}$ 인치)

재 3 장 현장 보존과 평가

원칙 : 최초의 현장 출동자는 모든 사람의 안전을 확인하고 전통적인 증거와 디지털 증거 모두의 무결성을 보호하기 위한 조치를 취해야 한다.

정책 : 모든 행위는 해당 부서의 정책과 연방, 주, 자치단체의 법률을 준용해야 한다. (추가적인 자료는 부록 B를 참조하라.)

절차 : 현장과 현장에 있는 모든 사람에 대한 안전 조치를 한 후, 최초 출동자는 전통적(물리적인) 또는 전자적인 형태의 잠재적 증거를 시각적으로 확인하고, 소멸되기 쉬운 증거가 존재하는지 파악해야 한다. 최초 출동자는 현장을 평가하고 수색 계획을 수립해야 한다.

현장 보존과 평가

◆ 범행 현장의 안전 조치에 대한 법률 정책에 따라야 한다. 여기에는 증거가 수집될 수 있는 장소에서 모든 사람들을 내보냈는 지 확인하는 과정이 포함된다. 이 때 모든 전자 장치의 상태가 변경되지 않아야 한다. 즉, **전원이 있으면 있는 상태로 없으면 없는 상태로 유지해야 한다.**

◆ 물리적 또는 전자적으로 소멸되기 쉬운 데이터를 보호하라. 소멸되기 쉬운 데이터는 무선 호출 수신기, 전화 ID 박스, 전자 수첩, 휴대폰, 기타 비슷한 장치에서 발견될 것이다. 최초 출동자는 소멸되기 쉬운 데이터가 포함된 장치가 있으면 즉시 보호 조치를 하고, 기록 및 촬영해야 함을 명심해야 한다.

◆ 모뎀이나 전화 ID 박스와 같이 전화선과 연결된 장치를 파악하라. 파악된 것을 기록하고, 전화선과 분리하며 가능하다면 해당 장치 보다는 전화선에 라벨을 붙여라. 또한 LAN/이더넷 통신을 위한 다른 통신선이 있을 수 있다. 이러한 경우에는 적합한 직원이나 전문가의 자문을 받아라.

※ 키보드, 컴퓨터 마우스, 디스크, CD, 또는 기타 부품들은 지문 또는 기타 보존해야 할 물리적 증거가 있을 수 있다. 지문 채취 과정에 사용하는 화학 약품은 장비와 데이터에 피해를 줄 수 있다. 그러므로, 지문 채취는 디지털 증거 복구가 완료된 후에 진행해야 한다.

예비 심문

◆ 현장에서 목격자, 당사자, 기타 등과 같이 모든 사람들을 파악하고 분리하며, 시간별로 그들의 위치를 기록하라.

◆ 부서 정책과 적용해야 하는 법률을 준용해서 다음과 같이 개별적인 정보를 획득하라.

  ◇ 현장에서 발견된 전자 장치의 사용자와 담당자 뿐만 아니라, 패스워드(아래 참조), 사용자 명, 인터넷 서비스 제공자

- 시스템, 소프트웨어, 또는 데이터에 접근하고자 할 때 요구되는 모든 패스워드. (한 사람이 여러 개의 패스워드를 가질 수 있다. 예. BIOS, 시스템 로그인, 네트워크 또는 ISP, 응용프로그램 파일, 암호용 패스워드, 이메일, 엑세스 토큰, 스케쥴러, 또는 접속자 목록)
- 시스템의 목적
- 고유의 보안 체계 또는 파괴 장치
- 외부 데이터 저장 장치
- 시스템에 설치된 하드웨어 또는 소프트웨어에 관련된 문서

제 4 장 범행 현장의 기록

원칙 : 범행 현장에 대한 기록은 영구적으로 보존할 수 있는 문서 형태로 생성한다. 문서 작업은 수사 전 과정 동안 진행된다. 컴퓨터, 저장 매체, 기타 전자 장치, 전통적인 증거의 위치와 상태를 정확하게 기록하는 것이 중요하다.

정책 : 범행 현장의 기록은 부서 정책과 연방, 주, 자치단체의 법률을 준용하여 생성하고 유지해야 한다.

절차 : 범행 현장은 상세하게 기록해야 한다.

물리적인 현장의 최초 기록

◆ 마우스의 위치와 기타 관계되는 주변기기들의 위치(예. 컴퓨터 왼쪽에 있는 마우스는 왼손잡이 사용자임을 알려준다.)와 같은 물리적인 현장 상태를 관찰하고 기록한다.
◆ 컴퓨터의 전원 상태(켜짐, 꺼짐, 절전 모드)를 포함하여 컴퓨터 시스템의 상태와 위치를 기록한다. 대부분의 컴퓨터는 컴퓨터가 동작 중인지 알려주는 표시등을 가지고 있다. 비슷하게, 팬 소음이 들린다면 시스템은 아마도 켜져 있을 것이다. 더군다나 컴퓨터 시스템이 따뜻하다면 이는 시스템이 켜져 있거나 최근에 꺼졌다는 것을 나타낸다.
◆ 수거하지 않을 관련된 주변기기를 확인하고 기록하라.
◆ 최초 출동자가 목격한 상태의 가시적인 기록을 만들기 위해 현장 전체를 촬영하라. 가능하다면, 범행 현장 전체를 포괄하기 위해 360도 전방위를 기록하라.
◆ 컴퓨터의 전면과 모니터 스크린, 기타 다른 주변기기를 촬영하라. 또한 모니터 스크린에 무엇이 나타나는지 기록하라. 실행 중인 프로그램은 녹화를 하거나 모니터 스크린의 활동에 관한 상세히 기록해야 할 것이다.

주의 : 시스템이 작동하고 있는 동안 컴퓨터 시스템을 이동시키면 시스템 데이터의 변화를 가져올 수 있다. 그러므로 5 장에서 설명할 것처럼 시스템을 안전하게 다운시킬 때까지 이동하지 말아야 한다.

◆ 증거를 수집하는 동안, 시스템에 관한 추가적인 내용을 기록해야 할 것이다.

제 5 장 증거 수집

강조사항 : 디지털 증거가 포함된 범행 현장에서 증거의 검색과 수집은 수색 영장이 있어야 할 것이다. 서론의 마지막 부분을 참고하라.

원칙 : 다른 증거와 마찬가지로 컴퓨터 증거는 증거적 가치가 보존되도록 세심하게 취급해야만 한다. 이는 도구나 장치의 물리적 무결성과 직접적으로 관련 있을 뿐만 아니라 내재되어 잇는 디지털 데이터도 관련 있다. 그러므로 특정한 유형의 컴퓨터 증거의 특수한 형태의 수집, 포장, 이송을 요구한다. 정전기, 자석, 라디오송신기, 그 외 다른 장치에서 생기는 전자기장에 의해서 쉽게 손상이나 변경될 수 있는 데이터를 보호하기 위한 조치가 취해져야 한다.

정책 : 디지털 증거는 해당 부서의 지침에 따라서 수집해야 한다. 소속 조직에서 디지털 증거 수집을 위한 지침이 없는 경우에는 다음의 절차를 참고하기 바란다.

주의 : 증거 수집을 하기 전에 3장과 4장에서 설명한 것처럼 증거의 위치 파악과 관련 내용을 기록해야 한다. 족적, 생체, 지문과 같은 존재할 가능성이 있는 다른 유형의 증거도 파악해야 한다. 증거 수집과 관련된 소속 기관의 정책을 따라야 한다. **지문 채취를 위한 화학약품의 사용과 같은 증거에 손상을 주는 행위는 디지털 증거의 복구가 완료된 후에 해야 한다.**

비디지털 증거

비디지털증거의 복구가 사이버 범죄의 수사에서 중요할 수 있다. 그러한 증거가 복구, 보존되도록 적합한 주의를 기울려야 한다. 디지털 증거에 대한 후속 조사와 관련된 대상이 여러 형태로 존재할 수 있기 때문에(예: 출력한 패스워드나 필기한 메모, 필기 자국이 있는 메모지장, 하드웨어와 소프트웨어의 매뉴얼, 일정표, 책자, 텍스트 또는 그림 형태의 출력물, 사진), 추후 분석을 위해 안전하게 보존해야 한다. 이러한 물품은 대부분은 컴퓨터 또는 관련된 하드웨어의 근처에 있다. 모든 증거는 해당 부서의 정책에 준해서 파악되고, 보호되며, 보존되어야 한다.

독립형 또는 랩탑 컴퓨터 증거

주의 : 여러 대의 컴퓨터는 하나의 컴퓨터 네트워크를 암시할 수 있다. 마찬가지로 회사의 컴퓨터는 보통 네트워크에 연결되어 있다. 이러한 상황에서 효과적으로 증거를 복구하고 잠재적인 민사적 책임을 경감시키기 위해서는 시스템에 관한 특별한 지식이 필요하다. 컴퓨터 네트워크가 있다면, 소속 부서의 컴퓨터 포렌식 전문가나 도움을 주기로

한 외부의 전문가에게 연락해야 한다. 복잡한 환경의 컴퓨터 시스템은 이 장의 후반부에서 설명한다.

독립형 개인용 컴퓨터는 다른 컴퓨터 또는 네트워크에 연결되지 않은 컴퓨터를 말한다. 독립형 컴퓨터는 데스크탑이나 랩탑일 것이다.

랩탑 컴퓨터는 컴퓨터, 모니터, 키보드, 마우스가 통합되어 이동할 수 있는 형태로 구성된다. 랩탑 컴퓨터는 다른 컴퓨터와 달리 배터리나 전원에 의해서 전력이 공급될 수 있다. 그러므로 독립형 컴퓨터의 전원 차단 절차에 추가적으로 배터리 제거가 요구된다.

만약 컴퓨터가 동작 중이면, 현재 상태를 기록하고, 부서의 전문가나 외부 자문가를 호출하라. 만약 내외부 전문가에게 연락할 수 없으면, 다음의 절차를 따라야 한다.

절차 :

3장에서 언급한데로 현장에 대한 안전 조치를 취한 후, 그리고 증거의 가치가 있는 데이터가 변경될 가능성이 있는 어떠한 행동을 취하기 전에, 아래의 모든 단계를 숙지하라.

a. 취한 모든 행동과 그 행동으로 인하여 발생한 모니터, 컴퓨터, 프린터, 주변기기의 변화를 노트로 기록하라.

b. 모니터를 관찰해서 꺼졌는지 켜졌는지 화면 보호 모드인지 판단하라. 그리고 적용할 후속 조치를 결정하고, 각 상황에 맞는 조치를 취하라.

상황 1 : 모니터는 켜져 있고, 동작 중이며 화면을 볼 수 있다.

1. 스크린을 사진 찍고, 화면에 나타난 정보를 기록한다.
2. 단계 c를 실행한다.

상황 2 : 모니터는 켜져 있고, 스크린이 절전모드 또는 화면보호모드의 동작화면을 볼 수 있다.

1. 버튼 입력 없이 조심스럽게 마우스를 움직인다. 그러면 스크린이 변하고, 작업창 또는 패스워드를 요청할 것이다.
2. 만약 마우스를 움직여도 스크린이 변하지 않으면, **어떠한 키 입력이나 마우스 입력을 하지 말아야 한다.**
3. 스크린을 촬영하고, 화면에 나타난 정보를 기록하라.
4. 단계 c를 실행한다.

상황 3 : 모니터가 꺼져 있다.

1. 꺼진 상태를 기록하라.
2. 모니터를 켜고, 만약 모니터 상태가 앞에서 말한 상황 1,2처럼 나온다면 그에 맞는 과정을 실행한다.

c. 컴퓨터 전원의 상태(켜짐, 꺼짐, 절전모드)와 상관없이, 컴퓨터로부터 전원 공급 케이블를 제거하라. 벽전원은 예외로 한다. 만약 랩탑이면 전원 코드에 추가하여 배터리 팩을 제거하라. 배터리는 시스템의 전원 차단을 위해 제거한다. 일부 랩탑은 플로피 드라이브 및 CD 드라이브를 위해서 보조 배터리를 가지고 있다. 이러한 가능성을 조사하고, 그 배터리도 제거하라.

d. 전화 모뎀, 케이블, ISDN, DSL 같은 외부로 연결되어 있는지 확인하라. 만약 전화로 연결되어 있다면, 전화번호를 파악하라.

e. 잠재적 증거의 손상을 피하기 위해, 들어 있는 플로피 디스크를 분리하고, 디스크 별로 라벨을 붙여서 포장하라. 가능하다면 압수용 디스크나 공 플로피 디스크를 삽입하라. CD를 제거하거나 CD 드라이브를 조작하지마라.

f. 모든 드라이브 슬롯과 전원 커넥터에 테이프를 붙여라.

g. 제조사, 모델, 시리얼 번호를 기록하라.

h. 컴퓨터의 연결선과 관련된 케이블을 촬영하고, 구성도를 그려라.

i. 나중에 정확하게 재조합하기 위해서 주변장치 연결선를 포함하여 모든 커넥터와 케이블에 라벨을 붙여 분류하라. 사용되지 않은 포트는 "미사용"과 같은 라벨을 붙여라. 다른 저장매체를 파악하기 위하여 랩탑의 연결부를 파악하라.

j. 소속 부서의 절차에 따라서 증거를 증거 분류하고 기록하라.

k. 만약 이송이 필요하다면, 깨지기 쉬운 물품을 포장하듯이 각 장치를 포장하라.(6장 참조)

복잡한 환경의 컴퓨터

사무실 환경은 종종 여러 대의 컴퓨터가 서로 연결되어 있거나 중앙 서버에 연결되어 있다. 네트워크에 연결되어 컴퓨터 시스템이 있는 범행 현장의 보존과 처리는 특별한 문제를 야기시키며 특히 부적절한 종료는 데이터를 파괴할 수 있다. 이것은 증거를 손상시킬 수 있으며, 심각한 민사적인 책임을 초래할 수 있다. 알려져 있는 비즈니스 환경의 범죄 행위를 조사할 때에는 우선적으로 컴퓨터 네트워크의 존재를 가정하여 계획을 수립해야 하며, 가능하다면 적합한 전문가의 도움을 받도록 한다. 컴퓨터 네트워크가 가정이나 유사한 환경에도

존재할 수 있음을 주목해야 한다.

다양한 운영 체제와 다른 종료 절차를 요구하는 복잡한 하드웨어 구성의 가능성은 본 지침의 영역을 넘어서는 것으로 별도의 네트워크 범행 현장 처리 지침이 필요하다. 그러나 컴퓨터 네트워크를 인식하고 파악하는 것은 상당히 중요하며, 그러한 상황에서는 전문가의 도움을 받아야 할 것이다.

컴퓨터 네트워크의 존재 가능성을 나타내는 표시

◆ 여러 대의 컴퓨터 시스템 존재
◆ 허브와 같은 중앙장치 및 컴퓨터가 작동하고 있으면서 왼쪽 사진과 같은 케이블과 커넥터의 존재
◆ 현장에 있었던 사람 혹은 정보제공자에게 받은 정보
◆ 1 장에서 말한 네트워크 부품 존재

다른 전자 장치와 주변기기의 증거

아래에 나열된 목록과 같은 전자 장치는 범죄 행위와 관련된 잠재적 증거를 포함하고 있을 수 있다. 긴급 상황이 아니라면, 장치는 작동되지 않을 것이다. 장치에 있는 정보에 접근할 필요가 있다면, 정보의 정당성을 유지하기 위해 장치의 조작에 관련된 모든 행위를 기록해야 한다. 아래에 나열된 많은 물품은 적절하게 취급하지 않으면 손상될 수 있는 데이터를 포함하고 있을 수 있다. 이들 장치에 대한 상세한 정보는 1 장을 참조하라.

컴퓨터 주변장치를 포함한 다른 전자 장치의 예

◆ 오디오 레코더
◆ 자동 응답기
◆ 케이블
◆ 송신자 신원 보증 장치
◆ 휴대폰
◆ 칩(칩과 같은 부품이 많이 발견되면 칩 도둑의 표시일 수 있음)
◆ 복사기
◆ Databank/Organizer digital
◆ 디지털 카메라(정지 또는 비디오)
◆ 동글 또는 소프트웨어 보호를 위한 하드웨어(키)
◆ 드라이브 복제기
◆ 외장 드라이브
◆ 플래시 메모리 카드
◆ 플로피, 디스켓, CD-ROM
◆ GPS 장치
◆ 무선 호출 수신기
◆ PDA/전자수첩
◆ PCMCIA 카드
◆ 프린터(인쇄 중이면 종료될까지 기다림)
◆ 이동 미디어 장치
◆ 스캐너(필름, flatbed, 시계 등)
◆ 스마트 카드/ 보안 ID 토큰
◆ 전화(스피드 다이얼러등 포함)
◆ VCR

◆ 팩스

◆ 무선 접속 포인트

주의 : 이동 매체를 압수했을 때는, 그 매체를 생성하는 관련 장치도 압수해야 한다.(예 : Zip®, Jaz®, ORB, Clik!™™, Syquest, LS-120에 맞는 테이프 드라이브, 카트리지 드라이브)

제 6 장 포장, 이송, 보관

원리 : 이 과정에서 취한 행동으로 인하여 컴퓨터나 다른 매체에 저장된 데이터가 수정되거나, 파괴되지 않아야 하며, 또다른 데이터가 추가되어서도 안된다. 컴퓨터는 온도, 습도, 물리적인 충격, 정전기, 자성 물체 등에 민감하게 반응하는 손상되기 쉬운 전자 장치이다. 그래서, 디지털 증거를 포장, 이송, 보관할 때에는 각별히 조심해야 한다. 디지털 증거의 절차 연속성을 유지하기 위해서는 포장, 이송, 보관 과정을 기록해야 한다.

정책 : 디지털 증거가 변경, 손실, 물리적 손상, 데이터의 파괴되지 않게 포장, 이송, 보관 과정에서 따라야 하는 적절한 절차가 수립되어야 한다.

포장 절차 :

a. 수집된 모든 디지털 증거는 적절히 기록 및 라벨을 붙이고, 포장 전에 목록화가 되어야 한다.
b. 잠복되어 있거나 흔적이 있는 증거에 각별한 주의를 기울이고, 그것을 보존하는 조치를 취해야 한다.
c. 자기 매체는 종이나 정전기 방지 플라스틱 가방으로 정전기 방지 포장을 해야 한다.
d. 디스켓, CD-ROM, 테이프와 같은 컴퓨터 매체들이 접히거나, 구부러지거나, 긁히지 않게 해야 한다.
e. 증거가 담긴 모든 용기는 적절한 라벨을 붙여 분류한다.

주의 : 만약 여러 컴퓨터 시스템이 수집되었다면, 발견되었을 때와 동일하게 재조립될 수 있도록 각 시스템마다 라벨을 붙여 분류한다. (예를 들면, 시스템 A-마우스, 키보드, 모니터, 본체; 시스템 B-마우스, 키보드, 모니터, 본체)

이송 절차 :

a. 디지털 증거는 자성을 띤 물체로부터 멀리 떨어져야 한다. 라디오 송신기, 스피커 자석, 열선이 있는 의자 등은 디지털 증거를 손상시킬 수 있는 항목들의 예이다.
b. 디지털 증거를 오랜 시간동안 자동차에서 보관하는 것은 피해야 한다. 과도한 열기와 냉기, 또는 습도는 디지털 증거를 손상시킬 수 있다.
c. 안전한 용기에 포장되지 않은 컴퓨터와 다른 물품들은 자동차 내에서 충격과 과도한 진동에 안전하게 유지될 수 있어야 한다. 예를 들면, 컴퓨터는 자동차 바닥에 싣고, 모니터는 스크린을 아래로 하여 의자에 놓고 안전벨트로 보호한다.
d. 이송되는 증거 모두가 절차 연속성이 유지되게 한다.

보관 절차

a. 증거는 소속 부서의 정책에 따라 목록화되어야 한다.

b. 증거는 극단적인 온도와 습도로부터 안전한 곳에 보관되어야 한다. 또한 자기장, 습기, 먼지, 기타 해로운 입자나 오염 물질로부터 보호되어야 한다.

주의 : 날짜, 시간, 시스템 설정과 같은 잠재적 증거들이 장기간 보관으로 인하여 손실될 수 있음을 인지해야 한다. 배터리는 한정된 수명을 가지고 있기 때문에, 배터리가 방전된다면 데이터는 손실될 수 있다. 그래서 담당 직원들(예를 들면, 증거 보관자, 연구실장, 포렌식 조사관)은 배터리에 의해 구동되는 장치에 대한 즉각적인 대응의 필요성을 알아야 한다.

제 7 장 범죄 유형에 따른 포렌식 조사

다음에 제시되는 내용은 부서장/수사관들이 특정 범죄 유형과 관련하여 공동적인 포렌식 조사 결과물을 파악하는데 도움이 될 것이다. 또한 수행해야 하는 조사 범위를 결정하는데 도움이 될 것이다.(이 정보는 이 장의 마지막에 표로 제시되어 있다.)

경매사기(온라인)

- ◆ 온라인 경매 사이트의 계좌정보
- ◆ 회계/경리 소프트웨어와 관련된 데이터 파일
- ◆ 주소록
- ◆ 일정표
- ◆ 채팅 로그
- ◆ 고객정보/신용카드 데이터
- ◆ 데이터 베이스
- ◆ 디지털 카메라 소프트웨어
- ◆ 이메일/메모/편지
- ◆ 재무/재산 기록
- ◆ 그림 파일
- ◆ 인터넷 접속 기록
- ◆ 인터넷 브라우져의 히스토리/캐쉬 파일
- ◆ 온라인 금융 기관 접속 소프트웨어
- ◆ 증명서의 기록 및 서류
- ◆ 전화 기록

아동학대

- ◆ 채팅 로그
- ◆ 날짜 및 시간 기록
- ◆ 디지털 카메라 소프트웨어
- ◆ 이메일/메모/편지
- ◆ 게임
- ◆ 이미지
- ◆ 인터넷 사용 로그
- ◆ 동영상 파일
- ◆ 이미지를 구분하기 위해 사용자가 생성한 디렉토리와 파일명
- ◆ 그래픽 편집, 뷰어 프로그램

컴퓨터 침입

- ◆ 주소록
- ◆ 설정파일
- ◆ 이메일/메모/편지
- ◆ 실행 프로그램
- ◆ 인터넷 사용 로그
- ◆ 인터넷 relay 채팅 로그
- ◆ 소스코드
- ◆ 텍스트 파일(사용자 이름, 패스워드)
- ◆ IP 주소, 사용자 이름

살인

- ◆ 주소록
- ◆ 일기
- ◆ 이메일/메모/편지
- ◆ 금융/자산 기록
- ◆ 이미지
- ◆ 인터넷 사용 로그
- ◆ 법적 문서, 유언
- ◆ 의료 기록
- ◆ 통화 기록

가정폭력

- ◆ 주소록
- ◆ 일기
- ◆ 이메일/메모/편지
- ◆ 금융/자산 기록
- ◆ 의료 기록
- ◆ 통화 기록

경제사기(온라인 사기, 위조사기 포함)

- ◆ 주소록
- ◆ 일정표
- ◆ 수표, 현금, 어음 이미지
- ◆ 신용카드 스키머
- ◆ 고객 정보/신용카드 정보
- ◆ 데이터베이스
- ◆ 이메일/메모/편지
- ◆ 위조 금융 거래 양식
- ◆ 위조 신분증
- ◆ 금융/자산 기록
- ◆ 서명 이미지
- ◆ 인터넷 사용 로그
- ◆ 온라인 금융 기관 접속 소프트웨어

이메일을 통한 협박/희롱/스토킹

- ◆ 주소록
- ◆ 일기
- ◆ 이메일/메모/편지
- ◆ 금융/자산 기록
- ◆ 이미지
- ◆ 인터넷 사용 로그
- ◆ 법률 문서
- ◆ 통화기록
- ◆ 희생자 배경 조사물

갈취

- ◆ 날짜 및 시간 기록
- ◆ 이메일/메모/편지
- ◆ 로그인 기록
- ◆ 인터넷 사용 로그
- ◆ 임시 인터넷 파일
- ◆ 사용자 이름

도박

- ◆ 주소록
- ◆ 일정
- ◆ 고객 데이터베이스와 사용자 기록
- ◆ 고객 정보/신용카드 데이터
- ◆ 전자화폐
- ◆ 이메일/메모/편지
- ◆ 금융/자산 기록
- ◆ 도박꾼 사진
- ◆ 인터넷 사용 로그
- ◆ 온라인 금융 기관 접속 소프트웨어
- ◆ 스포츠 베팅 통계

명의 도용

- ◆ 하드웨어, 소프트웨어 툴
  - ◈ 배경막
  - ◈ 신용카드생성기
  - ◈ 신용카드 reader/writer
  - ◈ 디지털 카메라
  - ◈ 스캐너
- ◆ 협상 도구
  - ◈ 업무용 수표
  - ◈ 자기앞 수표
  - ◈ 위조지폐
  - ◈ 신용카드 번호
  - ◈ 위조 법정문서
  - ◈ 위조 증여 증명서
  - ◈ 위조 대출 문서
  - ◈ 위조 판매 영수증
  - ◈ 우편환
  - ◈ 가계 수표
  - ◈ 주식 양도 문서
  - ◈ 여행자 수표
  - ◈ 차량 양도 문서
- ◆ 명의도용과 관련된 인터넷 사용 기록
  - ◈ 이메일과 뉴스그룹 개제글
  - ◈ 삭제된 문서
  - ◈ 온라인 주문서
  - ◈ 온라인 거래 정보
  - ◈ 시스템 파일과 파일 슬랙
  - ◈ 위조 사이트 사용 로그
- ◆ **신분증 서식**
  - ◈ 생일 증명서
  - ◈ 체크카드
  - ◈ 증명사진을 위한 디지털 사진이미지
  - ◈ 운전면허증
  - ◈ 전자서명
  - ◈ 허위 차량 등록증
  - ◈ 자동차 보험 증명서
  - ◈ 스캔된 서명
  - ◈ 사회 보장 카드

마약

◆ 주소록
◆ 일정표
◆ 데이터베이스
◆ 약품 영수증
◆ 이메일/메모/편지
◆ 위조 신분증
◆ 금융/자산 기록
◆ 인터넷 사용 로그
◆ 처방전 이미지

매춘

◆ 주소록
◆ 바이오그래피
◆ 일정표
◆ 고객 데이터 베이스/ 기록
◆ 이메일/메모/편지
◆ 위조신분증
◆ 금융/자산 기록
◆ 인터넷 사용 로그
◆ 의료 기록
◆ WWW 광고

소프트웨어 불법 복제

◆ 채팅 로그
◆ 이메일/메모/편지
◆ 소프트웨어 증명서의 이미지 파일
◆ 인터넷 사용로그
◆ 소프트웨어 크래킹 정보와 유틸리티
◆ 소프트웨어를 분류하기 위해 사용자가 생성한 디렉토리와 파일명
◆ 시리얼 번호

물리적 현장에서 복제품과 포장용 물품을 찾아라.

전화 사기

◆ 복제 소프트웨어
◆ 고객 데이터베이스/ 기록
◆ ESN/MIN 기록
◆ 이메일/메모/편지
◆ 금융/자산 기록
◆ 공짜 전화 사용법 매뉴얼
◆ 인터넷 사용로그
◆ 전화 기록

다음의 정보를 수집할 수 있다면 포렌식 조사를 위해 기록해야 한다.

◆ 사건 요약
◆ IP 주소
◆키워드 모록
◆ 닉네임
◆ 패스워드
◆ 연락처
◆ 참고 문서
◆ 범죄 유형

	성범죄		사람간의범죄			사기/기타 금융 범죄								
	아동학대	매춘	살인	가정폭력	이메일협박희롱스토킹	경매사기	컴퓨터침입	경제사기	갈취	도박	명의도용	마약	소프트웨어불법복제	전화사기
일반 정보														
데이터베이스		✓				✓		✓		✓		✓		
이메일/노트/편지	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
금융/자산 기록		✓	✓	✓	✓	✓		✓		✓		✓		✓
의료 기록		✓	✓	✓										
전화기록			✓	✓	✓	✓								✓
상세정보														
계좌데이터						✓								
회계/경리 소프트웨어						✓								
주소록		✓	✓	✓	✓	✓	✓	✓		✓		✓		
배경막											✓			
바이오그래피			✓											
생일증명서											✓			
일정표		✓				✓		✓		✓		✓		
채팅 로그	✓					✓							✓	
수표 화폐 어음 이미지								✓			✓			
체크카드											✓			
복제 소프트웨어														✓
설정파일							✓							
위조화폐											✓			
신용카드생성기											✓			
신용카드 번호											✓			
신용카드 reader/writer											✓			

	성범죄		사람간의범죄			사기/기타 금융 범죄								
	아동학대	매춘	살인	가정폭력	이메일협박희롱스토킹	경매사기	컴퓨터침입	경제사기	갈취	도박	명의도용	마약	소프트웨어불법복제	전화사기
신용카드 스키머								✓						
고객데이터베이스/기록		✓								✓				✓
고객정보/신용카드 데이터						✓		✓		✓				
날짜 시간정보	✓								✓					
일기			✓	✓	✓									
디지털 카메라/소프트웨어/이미지	✓					✓					✓			
운전면허증											✓			
약품 영수증												✓		
전자화폐										✓				
전자서명											✓			
지워진 인터넷 문서											✓			
ESN/MIN 기록														✓
실행 프로그램							✓							
위조 금융 거래 양식								✓						
위조신분증		✓						✓				✓		
위조법정문서											✓			
위조 증여 증명서											✓			
위조 대출문서											✓			
위조 판매 영수증											✓			

	성범죄		사람간의범죄			사기/기타 금융 범죄								
	아동학대	매춘	살인	가정폭력	이메일협박희롱스토킹	경매사기	컴퓨터침입	경제사기	갈취	도박	명의도용	마약	소프트웨어불법복제	전화사기
위조 차량 등록증											✓			
게임		✓												
그래픽 편집 뷰어 소프트웨어	✓													
로그 기록										✓				
공짜전화를 사용할 수 있는 매뉴얼														✓
이미지	✓		✓		✓	✓								
서명 이미지								✓						
소프트웨어 증명서 이미지 파일													✓	
이미지 플레이어										✓				
인터넷 사용 로그	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓
인터넷 브라우져 기록/캐시파일						✓								
IP주소/사용자 이름							✓							
IRC 채팅 로그							✓							
법률문서, 유언장			✓		✓									
동영상 파일	✓													
온라인 금융 기관 접속 프로그램						✓		✓		✓				

	성범죄		사람간의범죄			사기/기타 금융 범죄								
	아동학대	매춘	살인	가정폭력	이메일협박희롱스토킹	경매사기	컴퓨터침입	경제사기	갈취	도박	명의도용	마약	소프트웨어불법복제	전화사기
온라인 주문 거래 정보											✓			
처방전 이미지												✓		
증명서의 기록물/문서						✓								
스캐너/스캔된 서명											✓			
시리얼 번호													✓	
사회보장카드											✓			
소프트웨어 크래킹 정보, 유틸리티													✓	
소스코드							✓							
스포츠 배팅 통계										✓				
주식거래문서											✓			
시스템 파일 파일 slack											✓			
임시 인터넷 파일									✓					
사용자 이름							✓		✓					
상용소프트웨어 분류를 위한 사용자 생성 디렉토리와 파일명													✓	
이미지 파일 분류용 디렉토리와 파일명	✓													
차량보험과											✓			

이전 문서														
희생자 뒷조사물					✓									
위조사이트 접속 내역											✓			
웹페이지 광고		✓												