디지털 증거의 포렌식 조사:
법집행기관을 위한 지침

서론

이 지침서는 디지털 증거 조사에 책임이 있는 법집행기관의 직원과 부서장을 대상으로 한다.

이 지침서가 디지털 증거 조사에 대한 모든 사항을 포괄하는 것은 아니며, 디지털 증거를 조사하면서 발생하는 공통적인 상황에 대해서 다룬다. 이것은 법집행기관이 지켜야 하는 강제 사항이 아니며, 각 기관이 독자적인 정책과 절차를 개발하는데 도움을 주기 위한 안내서이다.

기술이 급속도로 발전하고 있기 때문에 이 지침서에서 제시하는 기술과 관행은 현재의 상황에서 최선이라 할 수 있다. 각 사건은 독특한 면이 있으며, 이 지침서에서 제시하는 절차를 실행함에 있어 조사자의 판단이 우선되어야 한다. 개별 사건의 환경과 연방, 주, 자치단체의 법률과 규정 때문에 실제 적용할 때에는 이 지침서에서 제시하는 것과는 다르게 수행할 수도 있다.

디지털 증거를 취급할 때에는 다음과 같은 일반적인 포렌식 원칙과 절차를 따라야 한다.

- 디지털 증거의 보호와 수집 행위는 디지털 증거의 무결성에 영향을 주지 않아야 한다.
- 디지털 증거를 조사하는 자는 이러한 목적을 위해 훈련받아야 한다.
- 디지털 증거의 수집, 조사, 저장, 이송과 관계된 행위는 기록되고, 보존되며, 재검토가 가능해야 한다.

조사자는 모든 과정에 걸쳐 디지털 증거의 조사가 정확하고 편견없이 시행될 필요가 있음을 인지해야 한다.

디지털 증거 처리 방식

평가. 컴퓨터 포렌식 조사자는 취해야 하는 행동을 결정하기 위하여 사건의 범위를 고려하여 디지털 증거를 철저하게 평가해야 한다.

획득. 디지털 증거는 본질적으로 훼손되기 쉬우며, 부적합한 취급이나 조사로 인해 변경, 손상, 파괴될 수도 있다. 조사는 디지털 증거의 복사본을 대상으로 시행하는 것이 최선이다. 원본 증거는 디지털 증거의 무결성을 보호, 보존하는 방식으로 획득되어야 한다.

조사. 조사 과정의 목적은 디지털 증거를 추출하고 분석하는 것이다. 조사는 저장 매체의 데이터 복구를 의미하며, 분석은 특정 포멧에서 복구된 데이터의 논리적 위치와 그 데이터의 내용 파악을 의미한다.

기록과 보고. 증거에 대한 포렌식 처리 과정 전체에 걸쳐 수행된 행위와 관찰은 모두 기록되어야 한다. 이것은 조사 결과 보고서 작성으로 종료될 것이다.

디지털 증거 처리 준비

디지털 증거를 취급하려는 기관은 우선적으로 디지털 증거를 처리할 수 있는 외부 자원에 대해 파악할 것을 권고한다. 이들 자원은 해당 부서의 자원이나 전문 기술로 해결할 수 없는 상황에 유용하다. 또한 각 기관은 연방, 주, 자치 단체의 법률에 맞는 정책과 절차의 개발을 권고한다.

다음의 다섯가지 주제는 컴퓨터 포렌식 조사를 시행하는데 필요한 기본 단계이며, 시행해야 하는 순서를 나타낸다. 비록 기록이 마지막 단계에 있지만 숙련된 조사자는 조사의 전 과정을 통하여 기록이 수행되어야 함을 잘 알고 있을 것이다.

1. 정책과 절차 개발
2. 증거 평가
3. 증거 획득
4. 증거 조사
5. 기록과 보고

이들 각 단계는 후술하는 장에서 상세히 설명할 것이다. 부록에 있는 상세 정보들이 각 장의 내용을 뒷받침될 것이다.

제 1 장 정책 및 절차 개발

원칙 : 컴퓨터 포렌식 부서는 숙련된 인원, 부서장의 지원, 조직 운영을 위한 예산이 필요하다. 이는 조사자를 위한 종합적인 훈련 프로그램의 구축, 견실한 디지털 증거 복구 기술의 보유, 최대한 효율적으로 운영되는 고도화된 부서의 유지 보장 등으로 달성할 수 있다.

절차 : 기관은 컴퓨터 포렌식 부서의 설립과 운영을 위한 정책과 절차를 개발해야 한다.

규정과 절차

■ 업무 명세

운영과 기능 요소를 확립하기 위한 정책과 절차의 개발은 컴퓨터 포렌식 부서를 설치하는 데 있어 중요한 단계이다. 이 작업을 효과적으로 시행하는 방법은 부서의 기능이 첨단기술 범죄 수사, 증거수집 또는 포렌식 분석과 같은 핵심 기능을 포괄하는 업무 명세를 개발하는 것이다.

■ 인원

정책과 절차에는 컴퓨터 포렌식 부서 구성원의 자격 요건이 정의되어야 한다. 이 절에는 직무 설명서, 최소 자격요건, 가동시간, 대기근무 상태, 명령체계, 팀의 구성요소 등이 포함될 것이다.

■ 관리적 고려사항

- **소프트웨어 사용권한** : 컴퓨터 포렌식 부서에서 사용되는 모든 소프트웨어는 기관 또는 부서내의 직원에게 적절히 라이세스가 부여되어야 한다.

- **자원 배정** : 컴퓨터 포렌식 부서를 설치하고 운영하기 위해서는 막대한 자금과 인원이 요구될 것이다. 대부분의 비용은 경상비이며, 매년 예산이 책정되어야 할 것이다. 자원 배정에는 부서가 위치할 시설, 조사자가 사용하는 장비, 소프트웨어와 하드웨어 요구사항, 업그레이드, 훈련, 지속적인 전문 인력 양성 및 유치에 대한 내용이 포함되어야 한다.

- **훈련** : 컴퓨터 포렌식 부서는 숙련되고 능력있는 조사자를 유지하는 것이 무엇보다 중요하다. 이는 특정한 교육을 받은 인력의 채용이나 구성원의 기술을 향상시킴으로써 성취할 수 있다. 컴퓨터 포렌식 분야의 급변하는 특성 때문에, 포괄적이면서 지속적인 교육 계획이 책정된 훈련비 내에서 개발되어야 하며, 예산 책정에 반영되어야 한다. 훈련에는 멘토 프로그램, 현장 연수, 다른 형태의 전문 분야 개발이 포함될 수 있을 것이다.

■ 서비스 요청과 수용 (Service request and intake)

지침서에는 포렌식 서비스 요청 절차와 디지털 증거 조사를 위해 채택된 요청의 수용 절차가 확립되어야 한다. 이러한 지침서의 내용에는 요청서와 수용서 양식, 연락처, 필요한 문서, 채택 기준, 물리적 증거제출을 위한 요구사항이 포함된다. 현장 직원은 서비스 요청과 수용을 위한 정책을 숙지하고 있어야 한다.

■ 사건 관리

일단 포렌식 서비스에 대한 요청이 채택되면, 조사의 우선순위와 배정에 대한 기준이 결정되고 실행되어야 한다. 이 기준은 범죄의 특성, 법정날짜, 기한, 잠재적 희생자, 법적 고려사항, 증거의 휘발성, 이용 가능한 자원 등을 고려하여 결정될 것이다.

■ 증거의 취급과 보관

지침은 증거의 수취, 처리, 기록, 취급에 관한 사항과 조사와 관련된 작업 산출물이 확립되어야 한다. 또란 이 지침은 현 부서의 정책과 일치해야 한다. 그러나 디지털 증거 취급과 보관 기준은 설치된 부서의 정책 보다 엄격할 수도 있다. **주의**: 어린이 포르노그래피와 같이 금지품으로 확인된 증거는 금지품과 관련된 압수 수색 영장 획득과 같은 특별한 방안이 요구될 수 있다.

다른 포렌식 부서에서 하드드라이브의 지문, 키보드에 떨어진 머리카락이나 피부조직, 손으로 직접 쓴 디스크 레이블 또는 인쇄된 것들과 같은 다른 증거를 찾을 수 있음을 명심해야 한다. 이러한 사례에서 보듯이 절차는 증거로써 가치있는 모든 것을 확보할 수 있는 형태로 조사의 순서와 방법이 결정될 수 있도록 개발하여야 한다.

■ 사건 처리

표준 운영 절차(SOPs, Standard operating procedures)는 디지털 증거의 보존과 처리를 위해 개발되어야 한다. SOPs는 포렌식 조사에서 예측하지 못한 상황이 발생하는 개별 환경에 대응할 수 있도록 융통성을 제공하면서 근본적인 조치를 취하는데 충분하게 포괄적이어야 한다.

■ 기술적인 처리 절차의 개발

수립된 절차들은 증거 조사의 기술적인 처리 과정을 제시해야 한다. 절차들은 획득된 결과가 타당하고 독립적으로 재연 가능함을 보증하기 위해 해당 절차의 실행에 앞서 검증되어야 한다. 절차의 개발과 검증의 단계는 문서화되어야 하며 다음을 포함해야 한다.

- 업무 또는 문제 식별
- 가능한 해결 방안 제시
- 알려진 표본을 기반으로 각 해결 방안 검증
- 검증 결과 평가
- 절차 완성

☞ 원본 증거는 절차 개발에 결코 사용되지 않아야 한다.

제 2 장 증거 평가 (Evidence Assessment)

원칙 : 디지털 증거물은 수사 방법을 결정하기 위하여 사건의 범위를 고려하여 철저하게 평가하여야 한다.

절차 : 수색 영장 또는 다른 법적 권한, 사건의 세부항목, 하드웨어 및 소프트웨어의 특성, 잠재적 증거의 수색, 조사해야 하는 증거의 **수집과** 관련된 주위 환경 등에 대한 검토를 통해 철저한 평가를 수행한다.

사건 평가 (Case assessment)

- 사건 수사관의 요청서에 대한 검토
  - 포렌식 조사 요청에 대한 법적 권한 확인
  - 도움을 받기 위해 완전한 요청서인지 확인 (Appendix D 참고)
  - 절차 연속성의 문서 완성

- 수사관에게 사건에 대한 도움을 주고 포렌식 조사로 밝힐 수 있는 사실과 밝힐 수 없는 사실을 주지시킨다. 수사관과 사건의 사실에 관해 대화할 때, 다음을 고려한다
  - 증거에 대해서 다른 포렌식 분석과정이 필요한지 논의한다. 예를 들어, DNA 분석, 지문, 도구흔적, 흔적, 의심되는 문서 등이 있다.
  - 추가적인 디지털 증거를 획득하기 위한 다른 수사 방법의 적용 가능성을 논의한다. 예를 들어, ISP에 증거 보존 명령, 원격 데이터 저장소 식별, 전자메일 획득 등이 있다.
  - 수사에서 주변기기의 구성 요소와의 연관성 여부를 고려한다. 예를 들어, 위조 또는 사기 사건의 경우 컴퓨터 이외의 장치인 라미네이터(laminator), 위조용 신용카드, 수표책, 스캐너, 프린터 등을 확인하고 아동 포르노 사건일 경우 디지털 카메라를 확인한다.
  - 찾아야 할 잠재적 증거를 결정한다. 예를 들어, 사진, 스프레드시트, 문서, 데이터베이스, 재무기록 등이 있다.
  - 사건과 관련된 추가적인 정보를 결정한다. 예를 들어 별명(aliase), 전자메일 계정, 전자메일 주소, 사용된 ISP, 이름, 네트워크 설정 및 사용자, 시스템 로그, 패스워드, 사용자 이름 등이 있다. 이러한 정보는 **시스템 관리자**, 사용자 및 직원과의 인터뷰를 통해 획득할 수도 있다.
  - 사건에 연루된 사용자의 컴퓨터 사용 능력을 평가한다. 컴퓨터 사용 능력이 높은 사용자의 경우 암호화, 부비트랩, 스테가노그라피와 같은 기술을 통해 증거를 숨기거나 삭제할 가능성이 있다.
  - 조사할 증거에 대한 우선순위를 결정한다.
  - 추가적인 인원이 필요한 지 결정한다.
  - 필요한 장비를 결정한다.

☞ 이러한 평가는 다른 범죄와 관련된 증거를 밝혀낼 수도 있다. 예를 들면 마약 범죄와 관련된 돈세탁 등이 있다.

현장 고려사항 (Onsite considerations)

다음의 내용들은 디지털 증거 조사에 완전한 정보를 제공하는 것은 아니다. 이 내용은 범죄 현장에서 법집행기관이 디지털 증거에 대한 평가를 하기 위한 일반적인 지침서이다. 본 지침과 함께 "Electronic Crime Scene Investigation: A Guide for First Responders"를 참고하라. (http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm)

☞ 현장에서는 각 개인의 안전에 유의해야 한다. 현장 수색전에 주위가 안전하도록 조치를 취해야 한다.

일부 사건 현장에서 조사자는 다음의 사항만을 수행할 수도 있다.

- 컴퓨터의 수와 종류 확인
- 네트워크 연결 유무 판단
- 시스템 관리자 및 사용자와의 인터뷰
- 이동식 저장 장치를 포함한 저장 장치의 종류와 크기 파악 및 기록, 저장매체를 시스템으로부터 분리하는 경우 원래의 위치에 대한 기록
- 현장 이외의 저장소 위치와 원격 컴퓨터의 위치 확인
- 소유하고 있는 소프트웨어 확인
- 현장의 일반적인 상태 측정
- 의심이 가는 운영체제 판단

☞ 외부 자원이 필요한 지와 연락해야 하는 지를 판단하고, 그러한 자원에 연락하기 위한 전화 목록을 작성 및 보관해야 한다.

조사 장소 평가 (Processing location assessment)

조사 수행 장소를 결정하기 위해 증거를 평가한다. 지정된 포렌식 연구실과 같은 통제 가능한 환경이 조사를 완벽하게 하는데 유리하다. 현장에서 조사를 수행해야 하는 경우에는 주위 환경을 충분히 통제해야 한다. 평가에 필요한 고려사항은 다음과 같다.

- 증거 복구를 수행하기 위해 현장에서 필요한 시간
- 장기간의 조사팀 배치와 연관된 보급과 인력 문제
- 장시간 수색이 사업에 미치는 영향

- 현장조사에 대한 경험, 숙련도, 장비, 자원 등의 적합성

법적 고려사항 (Legal considerations)

- 수색에 대한 법적 허용 범위 결정
- 적절한 연방법, 주법, 지역 정책 및 법률에 의거한 가능한 관련 사항 파악
  (Electronic Communication Privacy Act of 1986(ECPA), Cable Communications Policy Act(CCPA), USA PATRIOT ACT of 2001, Privacy Protection Act of 1980(PPA))

☞ 증거가 허가 받은 이외의 장소에 있는 경우, 추가적인 법적 조치를 취해 수색을 계속할 필요가 있는 지 결정해야 한다. 필요하다면 법적 조언을 구해야 한다.

증거 평가 (Evidence assessment)

- 증거의 우선순위를 결정한다. 예를 들어, 일반 배포된 CD와 개인이 작성한 CD가 있는 경우 증거일 가능성이 높은 것은 개인이 작성한 CD가 될 것이다.

  - 증거가 발견된 장소
  - 조사 대상 저장 매체의 안정성
  - 증거 기록 방식의 결정 (사진, 스케치, 노트기록)
  - **전자기적 간섭**이 있을 수 있는 장소인지 평가
  - 증거의 포장, 이송, 저장 후 증거물의 상태를 확인
  - 전원이 계속 공급이 되어야 하는 장치인지 확인

❖ 이 내용은 일반적으로 실제 상황에서 받아들일 수 있는 상황을 기초로 작성되었다. 이외에 필요하다면 조사를 수행하기에 앞서 법적 조언을 미리 구해야 한다. 실제 상황에서는 이 지침외의 대체 방법이 필요할 수 있다. 사건에 대한 철저한 평가는 후속 절차의 기초가 된다.

제 3 장 증거 수집 (Evidence Acquisition)

원칙 : 디지털 증거는 본질적으로 훼손되기 쉬우며, 부적합한 취급이나 조사를 통해 변경, 손상, 파괴될 수도 있다. 이러한 이유로 인해, 증거의 특성을 보존할 수 있도록 사전에 세심한 주의를 기울려야 한다. 이러한 조치가 실패할 때에는 증거를 사용하지 못하게 되거나 부정확한 결과를 초래할 수 있다.

절차 : 증거를 보호하고 보존할 수 있는 방식으로 원본 디지털 증거를 수집한다. 기본 절차는 다음과 같다.

- 해당 기관의 지침에 따라 디지털 증거를 보호한다. 지침이 없다면 'Electronic Crime Scene Investigation: A Guide for First Responders'에서 유용한 정보를 찾을 수 있을 것이다.
  (사이트 - http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm)
- 조사자 시스템의 하드웨어와 소프트웨어에 대한 환경설정을 문서로 기록한다.
- 하드웨어와 소프트웨어를 포함하여 조사자 컴퓨터 시스템의 전반적인 동작 상황을 확인한다.
- 저장 매체에 대한 물리적 접근을 위해 수사대상의 컴퓨터를 분해한다.
  – 전자기장으로부터 장비가 영향을 받지 않도록 유의해야 한다.
- 획득할 필요가 있는 저장 매체를 식별한다. 이들 저장 매체는 내장형, ·외장형 또는 모두일 수 있다.
- 내부에 장착된 저장매체와 하드웨어 환경 설정 상황을 문서로 기록한다.
  – 드라이브 상태 (제작자, 모델, 외형 상태, 크기, 연결선 셋팅, 위치, 드라이브 인터페이스 등)
  – 내부 구성요소 (사운드 카드, 비디오 카드, MAC 어드레스를 포함한 네트워크 카드, PCMCIA 카드 등)
- 데이터의 변조, 손상, 파괴를 막기 위하여 마더 보드 또는 드라이브와 연결된 전원 플러그 또는 데이터 케이블을 제거하여 저장 매체의 연결 상태를 분리한다.
- 아래와 같이 통제된 상태의 부팅을 통해, 용의자 시스템의 환경설정 정보를 확인한다.
  – 기능성 테스트 및 CMOS/BIOS 정보를 확인하기 통제된 부팅을 한다.
    - 부트 시퀀스 (플로피, CD-ROM 드라이브에서 시스템 부트를 수행하기 위해 BIOS 변경이 될 수 있음)
    - 날짜와 시간 정보
    - 패스워드 설정된 전원(Power)
  – 포렌식 부트 디스크와 컴퓨터의 기능성 테스트를 위해 다시 한 번 통제된 상태의 부팅을 수행한다.
    - 전원과 데이터 케이블이 플로피 또는 CD-ROM 드라이브에 올바르게 연결되었는지 확인하고. 저장매체의 데이터 케이블과 전원이 분리된 상태인지 확인한다.
    - 플로피 또는 CD-ROM 드라이브에 포렌식 부트 디스크를 삽입한다. 컴퓨터를 부팅하고 포렌식 부트 디스크로 부터 부팅되는지 확인한다.

– 분리하였던 저장 매체를 다시 연결하고, CMOS/BIOS에서 드라이브 환경 설정 정보를 확인할 수 있도록 세 번째 통제 상태의 부팅을 수행한다.
  • 저장매체로부터 컴퓨터가 부팅이 되지 않도록, 플로피 또는 CD-ROM 드라이브 내에 포렌식 부트 디스크가 존재하는지 확인한다.
  • 드라이브 설정 정보는 대용량 디스크를 위한 Logical Block Addressing (LBA) 방식인지 또는 실린더, 헤드, 섹터(CHS) 방식인지 또는 자동 탐지인지를 포함한다.

▪ 시스템을 종료한다.
▪ 현장에서 가능하면 주요 저장매체를 제거하고, 조사자의 시스템을 사용하여 증거를 획득한다. 조사자의 시스템에 주요 저장 매체를 부착할 시에는 인식될 수 있도록 설정해야한다.
▪ 아래와 같이, 대상 시스템으로부터 저장매체를 제거할 수 없는 예외상황이 발생할 수 있다.
– RAID (Redundant array of inexpensive disks). 디스크를 제거하여 개별적으로 획득하게 되면, 유용한 결과를 산출하지 못할 수 있다.
– Laptop 시스템. 시스템 드라이브에 접근하기 어려울 수 있고, 원 시스템에서 탈착하였을 경우에는 사용하지 못할 수 있다.
– 하드웨어 종속성(레거시 장비). 신 시스템에서 구형 드라이브가 인식되지 못할 수 있다.
– 장비 가용성. 조사자는 필요한 장비에 접근할 수 없는 경우가 있다.
– 네트워크 스토리지. 데이터를 획득하기 위해서는 네트워크 장비가 사용되어야 한다.

디지털 증거를 획득하기 위해서 대상 컴퓨터를 사용할 경우, 시스템에 저장 매체를 다시 연결하고, 수사관의 증거물 저장용 매체(하드드라이브, 테이프 드라이브, CD-RW, MO 등)도 함께 부착한다.

▪ 증거물을 획득할 때, 수사관의 저장 매체가 포렌식 관점에서 무결한 디스크인지 확인해야 한다.

☞ 원본 증거를 보호, 보존하기 위해 가능하다면 쓰기 방지가 설정되어야 한다.

❖ 조사자는 증거를 획득하기 이전에 해쉬 값 또는 CRC 등을 활용하여 원본 증거에 대한 무결성 검증용 데이터 생성을 고려해야 한다. 단, 획득 방식에 따라 이러한 절차가 이미 완료된 경우도 있다.

▪ 쓰기방지 하드웨어가 사용되는 경우
– 쓰기 방지 디바이스를 설치한다.
– 수사관이 제어하는 운영체제를 통해 시스템을 부팅한다.
▪ 쓰기방지 소프트웨어가 사용되는 경우
– 수사관이 제어하는 운영체제를 통해 시스템을 부팅한다.
– 쓰기 방지를 실행한다.
▪ host-protected 데이터 영역을 포함하여 저장 매체의 모든 영역을 확인하기 위해 저장

매체의 구조를 조사한다. 예를 들면 파티션 테이블이 드라이브의 물리적인 구조와 일치하는지와 같은 호스트와 무관한 특정 데이터를 조사한다.

- 드라이브의 시리얼 넘버와 사용자가 접근할 수 있는 호스트의 특정 데이터들을 확보한다.
- 아래와 같은 적절한 소프트웨어 및 하드웨어를 활용하여 조사자의 저장 매체에 주요 증거를 획득한다.
  - Stand-alone 복제 소프트웨어
  - 포렌식 통합 분석 소프트웨어
  - 전용 하드웨어 디바이스
- 원본과 사본의 해쉬값을 비교하거나 섹터 단위로 원본과 사본을 확인함으로써 데이터 획득이 올바르게 되었는지 확인한다.

제 4 장 증거 조사 (Evidence Examination)

원칙 : 일반적인 포렌식 원칙들은 디지털 증거 조사에도 적용된다. 사건과 저장 매체의 종류에 따라 조사 방법이 달라질 수 있다. 디지털 증거 조사자는 각 상황에 대처할 수 있게 훈련받아야 한다.

절차 : 승인된 포렌식 절차에 따라 수집된 데이터에 대해 조사를 수행한다. 가능하면 원본 증거에서 조사가 수행되지 않아야 한다.

이 장에서는 디지털 증거의 추출과 분석에 관하여 논의한다. 추출은 저장 매체의 데이터 복구를 나타낸다. 또한 분석은 복구된 데이터의 내용과 특정 포맷에서 그 데이터의 논리적인 위치의 해석을 말한다. 예를 들어 어떻게 획득하고, 어디에서 추출하고, 무엇을 의미하는지 등을 나타낸다. 제안된 개념은 디지털 증거의 조사를 구조화하고 절차를 개발하는데 있어서 조사자를 도와주기 위한 것이다. 이러한 개념이 모든 것을 포괄하는 것은 아니며, 후술하는 모든 기술이 사건에 사용되지는 않을 것이다. 적합한 접근법을 선택하는 것은 조사자의 재량이다.

증거 조사를 시행할 때에는 다음과 같은 각 단계의 사용을 고려한다.

단계 1. 준비

증거 파일과 데이터를 복구하거나 추출하여 저장할 수 있도록 별도의 매체에 작업 디렉터리를 준비한다.

단계 2. 추출

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

물리적 추출

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

- 전체 하드 디스크에 걸쳐 키워드 검색을 수행하면 운영 체제와 파일 시스템이 다루지 않는 데이터를 추출할 수 있다.
- 전체 하드 디스크에 걸쳐 파일 카빙 도구를 사용하면 운영 체제와 파일 시스템이 관리하지 않는 유용한 파일과 데이터를 추출하고 복구하는데 도움이 될 수 있다.
- 파티션 구조 검사는 현재의 파일 시스템을 식별하고 하디 디스크의 물리적 크기 전체가 할당되었는지 결정할 수 있다.

논리적 추출

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 포함할 수 있다.

- 디렉토리 구조, 파일 속성, 파일 이름, 시간과 날짜, 파일 크기, 파일 위치와 같은 특성을 나타내는 파일 시스템의 정보 추출
- 알려진 해쉬 값과 계산한 해쉬 값 비교를 통해 알려진 파일을 식별하여 제거함으로써 데이터를 축소
- 조사에 적합한 파일의 추출. 이를 성취하기 위하여 파일 이름과 확장자, 파일 헤더, 파일 내용, 디스크상의 경로 등이 사용될 것이다.
- 삭제 파일의 복구
- 패스워드로 보호된, 암호화된, 압축된 데이터의 추출
- 파일 슬랙의 추출
- 비할당된 영역의 추출

단계 3. 추출 데이터의 분석

분석은 사건의 의미를 결정하기 위하여 추출된 데이터를 해석하는 과정이다. 분석 방법의 예로 타임프레임(timeframe), 데이터 은닉, 응용프로그램과 파일, 소유자와 점유자 등이 있다. 분석은 조사 요청서, 디지털 증거의 검색을 위한 법적 권한, 수사 실마리 또는 분석 실마리에 대한 재검토가 필요할 수 있다.

타임프레임 분석

타임프레임 분석은 컴퓨터 시스템 상에서 사건이 발생한 시점, 사건이 발생한 시기에 컴퓨터의 일부를 사용한 자를 결정하는데 유용할 수 있다. 다음과 같은 두 가지 방법을 활용할 수 있다.

- 수사와 관계된 타임프레임 내에 관심있는 파일에 연결된 파일 시스템의 메타정보(마지막 수정 시간, 마지막 접근 시간, 생성 시간, 변경 상태 등)에 포함된 시간과 날짜 정보를 검토한다. 이러한 분석의 예로 파일 내용이 마지막으로 변경될 때 설정된 마지막 수정 날짜와 시간의 사용을 들 수 있다.
- 시스템과 응용프로그램의 로그를 확인한다. 여기에는 에러 로그, 설치 로그, 네트워크 연결 로그, 보안 로그 등이 포함될 것이다. 예를 들면, 보안 로그의 조사는 사용자가 로그인한 시간을 파악할 수 있다.

❖ 운영체제에 기록된 시간과 BIOS에 기록된 시간의 차이점이 없는지 확인하라.

은닉 데이터 분석

데이터는 컴퓨터 시스템 상에 숨길 수 있다. 숨겨진 데이터 분석은 데이터 탐지와 복구뿐만 아니라 지식, 소유자, 의도를 파악할 수도 있다.

- 파일 확장자에 대응하는 파일 헤더를 비교하여 파일의 이상 유무를 판별한다. 불일치하는 파일의 존재는 사용자가 고의적으로 데이터를 은닉했음을 의미할 수도 있다.
- 패스워드로 보호되거나 암호화 또는 압축된 파일의 획득은 인가되지 않은 사용자가 데이터를 숨기려고 시도했음을 나타낼 수 있다. 패스워드 그 자체는 해당 파일의 내용만큼 사건과 관련이 있을 수 있다.
- 스테가노그라피
- HPA (Host-protected area)에 접근한다. HPA에 사용자가 생성한 데이터가 존재하면 데이터를 숨기기 위한 의도라고 판단할 수 있다.

응용 프로그램과 파일 분석

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

- 연관성 및 패턴을 위한 파일 이름 관찰
- 파일 내용 검사
- 운영 체제의 종류와 개수의 식별
- 설치된 응용 프로그램과 파일들의 연관성
- 파일들의 관련성 검토. 예를 들어, 인터넷 히스토리와 캐쉬 파일의 연관성, 이메일 파일과 첨부 파일의 관련성 등이 있다.
- 수사할 가치가 있는지 판단하기 위해 알려지지 않은 파일 타입 식별
- 파일의 저장 위치가 디폴트인지 수정된 위치인지를 판단하기 위해서 드라이브의 파일 구조와 응용프로그램을 위한 사용자 기본 저장 위치를 검사한다.
- 사용자 환경 설정 검사
- 사용자가 응용프로그램을 통해 파일에 추가한 테이터를 포함하여 파일의 메타데이터 분석. 예를 들어, 문서 편집기로 생성한 파일은 파일의 소유자, 마지막 수정 시간, 수정 횟수, 저장되거나 인쇄된 위치의 정보가 포함될 수 있다.

소유자와 점유자

어떤 경우에는 누가 파일을 생성했으며 수정했는지 또는 접근했는지를 식별하는 것이 필수적일 수 있다. 의문가는 데이터의 소유자와 교활한 점유자를 판단하는 것은 중요할 수 있다. 교활한 점유자의 요소는 다음의 항목을 포함하여 앞에서 언급한 분석절차에 의거 조사될 것이다.

- 파일의 소유자와 점유자를 확인하는데 도움이 될 수 있는 특정한 시간대의 사용 내역을 확인한다. (타임프레임 분석)
- 중요한 파일은 디폴트 위치가 아닌 곳에 저장될 수 있다. (예를 들어 사용자가 지정한 “child porn" 이름의 디렉터리) (응용프로그램 및 파일 분석)
- 파일 이름 그 자체가 증거로서 가치가 있을 수 있으며, 파일의 내용을 암시할 수도 있다. (응용프로그램 및 파일 분석)
- 숨겨진 데이터가 있다는 것은 탐지를 피하기 위한 고의적인 시도로 판단할 수 있다. (은닉 데이터 분석)
- 암호화되거나 패스워드로 보호된 파일에 접근할 수 있는 패스워드가 복구되었다면, 그 패스워드 자체가 점유자 또는 소유자를 가리킬 수 있다. (은닉 데이터 분석)
- 파일 내용에 사용자의 특정 정보가 포함됨으로써 소유자 또는 점유자를 판별할 수 있다. (응용프로그램 및 파일 분석)

단계 4. 결론

위와 같은 단계에서 얻어진 결과가 사건의 전말을 설명하기에 충분하지 않을 수 있다. 그러나 각 단계의 결과들에 대한 연관성을 전체적으로 검토하면, 사건에 관하여 좀 더 명확한 윤곽을 제공할 수 있다. 따라서 분석 절차의 마지막 단계는 추출과 분석 결과를 전체적인 관점에서 재검토해야 한다.

제 5 장 기록과 보고

원칙 : 조사자는 디지털 증거분석을 통하여 발견하고 찾아낸 결과에 대해서 완벽하고 정확하게 보고할 책임이 있다. 기록은 조사 과정 전체를 통하여 지속적으로 진행되어야 한다. 디지털 증거 분석 과정 동안 진행된 각 단계를 정확하게 기록하는 것이 중요하다.

절차 : 모든 문서는 완벽하고, 정확하며, 이해할 수 있는 형태로 작성되어야 한다. 결과 보고서는 열람하는 사람들을 위해서 작성되어야 한다.

조사자의 기록

기록물은 조사 과정과 동시에 작성되어야 하고, 기록의 보관은 부서의 정책에 따라야 한다. 다음의 항목들은 문서화 작업을 진행하는 동안 분석자가 고려해야 할 일반적인 사항들이다.

- 담당 수사관이나 담당 검사의 의견을 기록한다.
- 사건 기록에 수색 영장의 복사본을 보존한다.
- 사건 파일에 초기 지원 요청서를 보존한다.
- 절차 연속성 문서의 복사본을 보존한다.
- 완벽한 복제 행위가 허용되기에 충분할 정도로 상세하게 기록한다.
- 메모에는 날짜, 시간, 분석 행위에 대한 결과와 설명을 포함한다.
- 분석과정 중 발생하였던 예외사항과 예외사항을 유발한 행위를 기록한다.
- 네트워크 구조, 인가된 사용자 목록, 사용자 동의, 패스워드 같은 추가적인 정보를 기록한다.
- 법집행기관의 지휘나 조사자에 의해 시스템이나 네트워크에 만들어진 변경사항을 기록한다.
- 운영체제와 관련 소프트웨어 버전과 현재 적용된 패치 사항들을 기록한다.
- 원격 저장소, 원격 사용자의 접근, offsite 백업을 고려하여 범죄 현장에서 획득된 정보들을 기록한다.

☞ 조사 과정 중에, 증거가 될 수 있는 정보가 현재의 권한 범위 밖에서 발견될 수 있다. 이러한 정보들을 기록하고, 추가적인 수색권한이 필요할 수 있기 때문에 사건 담당자한테 보고한다.

조사자 보고서

이 절은 수사관, 검사, 그 외의 사람에게 제출할 보고서를 준비하는데 필요한 길잡이를 제공한다. 일반적인 권고 사항이 있으며, 각 부서의 정책에는 순서, 내용과 같은 보고서 작성 세부규칙들을 포함하고 있을 것이다.

- 보고서 작성 기관의 확인
- 사건 식별자와 제출번호

- 담당 수사관
- 제출자의 식별
- 접수 날짜
- 보고 날짜
- 일련번호, 제조번호, 모델를 포함하여 조사를 위해 함께 제출된 항목의 설명 목록
- 분석자의 이름과 서명
- 문자열 검색, 그래픽 이미지 검색, 삭제된 파일 복구와 같은 분석할 때 실행하였던 절차들에 대한 간단한 설명
- 결과와 결론

다음의 절은 다른 보고서 형식에서도 유용할 것이다. (부록 A의 보고서 참조)

■ 조사 결과의 요약

이 절은 분석을 위해 제출된 항목에 대해 수행된 조사 결과에 대한 요약으로 구성되어 있다. 요약에 수록된 조사 결과는 보고서의 해당 결과에 관한 절에 세부사항이 설명되어 있어야 한다.

■ 조사 결과에 대한 세부사항

- 요청과 관련된 특정 파일
- 삭제된 파일을 포함하여 조사 결과를 뒷받침하는 다른 파일
- 문자열 검색, 키워드 검색, 문장 검색
- 인터넷과 관련된 증거(웹 사이트 트래픽 분석, 채팅 로그, 캐쉬 파일, 이메일, 뉴스그룹 활동 사항)
- 그래픽 이미지 분석
- 프로그램 등록 날짜가 포함될 수 있는 소유자에 대한 지시자
- 데이터 분석
- 분석 대상과 관련된 프로그램 설명
- 데이터를 은닉하거나 은폐하기 위한 기술(스테가노그라피, 암호화, 숨김 파일 속성, 은닉 파티션, 비정상적인 파일 이름)

■ 보충 자료

증거의 특정 항목 출력물, 증거의 디지털 복사본, 절차 연속성 문서와 같은 보고서에 첨부되는 보충자료를 목록화 한다.

■ 용어 설명

독자가 언급된 기술적인 용어를 이해할 수 있도록 관련 용어에 대한 설명이 보고서에 포함되어야 한다. 용어 정의는 일반적으로 채택하는 자료를 사용하고, 적절한 참고문헌을 제시한다.

부록 A. 사례 분석

사건 분석을 수행할 수 있는 예로 다음의 두 사건을 간략히 살펴보자.

주의사항: 설명하는 사건 시나리오는 교육을 목적으로 가공으로 구성하였으며, 실제 사건과 기소 내용이 유사하다면 그것은 우연히 발생한 것이다. 사건 시나리오에 사용된 이름, 장소는 가상으로 작성된 것으로 실제 장소와 사람과는 아무런 관련이 없다. 여기에서 언급된 상품명, 상표, 제조사 등에 관한 특정 상용제품, 처리과정, 서비스 등은 주 정부 및 지역 정부기관에 의해 추천하거나 선호하는 것이 아니며, 언급된 정보 및 문장 역시 광고를 위한 목적으로 사용할 수 없다.

☑ 사건 개요 1

용의자는 건자재 회사를 소유하고 있다. 용의자는 직원을 시켜 컴퓨터 수리 전문점인 Mom & Pop‘s 에 노트북 모니터의 수리를 의뢰하였다. 노트북 수리가 끝난 후 모니터가 수리가 잘 되었는지 확인하기 위해 Mom & Pop‘s의 Mom은 노트북을 켰으며, Mom & Pop‘s의 수리 절차에 따라 Mom은 “마이크로소프트 윈도우98”의 시작메뉴에서 최근 문서 메뉴로 이동하였고 파일을 열어 확인을 하였다. 이때 Mom은 아동 음란물을 발견하였으며, 즉시 보안관에게 신고하였다. 신고를 받은 보안관은 해당 이미지를 보고 그것이 주정부 법에 위배됨을 확인하였다. 보안관은 노트북에 불법자료가 있음을 근거로 하여 즉시 압수하였다. 이러한 압수 절차는 "Electronic Crime Scene Investigation: A Guide for First Responders"에 입각하여 수행하였다. 노트북은 수사기관의 방침에 따라 증거물로 등록되었고, 추가적인 조사를 위해 수색영장을 발부받았으며, 컴퓨터는 조사를 의뢰하였다.

- 조사목적: 용의자의 아동 음란물 소유 여부 판단. 노트북 사용자가 많을 경우 어려움이 있다.
- 컴퓨터 유형: 노트북, 시리얼번호 123456789
- 운영체제: Microsoft Windows 98
- 혐의사항: 아동 음란물 소지
- 사건담당자: Johnson 수사관
- 사건번호: 012345
- 절차연속성(Chain of custody) : 첨부문서 참조
- 조사장소: 범죄수사반(Criminal investigations unit)
- 사용도구: Disk acquisition Utility, Universal graphic viewer, Command line

⊙ 조사 과정

✓ **증거평가**: 담당 수사관의 디지털 포렌식 조사요청서 검토. 법원으로부터 수색 영장을 발부받았다. 수사관은 아동 음란물, 접근날짜, 컴퓨터 소유자에 관한 모든 정보의 조사를 의뢰하였으며, 포렌식 랩에 조사에 필요한 장비가 있음을 확인하였다.

- ✓ **증거획득**: 하드웨어 환경을 기록하였고, 증거 보호와 보존을 위해 하드디스크의 사본을 생성하였으며, 시간 및 날짜를 포함한 CMOS 정보 기록하였다.

- ✓ **증거조사**: 날짜와 시간을 포함하여 디렉토리와 파일 구조에 대해 기록하였다. 모든 영상파일의 위치를 파악하기 위해 파일헤더 검색을 수행하였고, 영상파일에 대한 검사를 수행하였으며, 아동을 성적으로 표현한 영상파일에 대해서는 증거로 보전하였다. 플로피디스크에 저장된 아동관련 성적의미를 가진 파일의 단축아이콘 파일을 복구하였고, 해당 파일에 대한 최종 접근시간과 날짜는 Mom & Pop'S로 보내기 10일 전임을 확인하였다.

- ✓ **기록과 보고**: 수사관은 조사결과에 대한 보고서를 보고, 용의자에 대한 심문이 필요하다고 판단하였다.

- ✓ **이후수사과정**: Mom&Pop'S로 노트북을 보낸 직원과 면담을 수행하였는데, 해당 직원은 노트북을 사용하지 않았음을 주장하였다. 추가적으로 해당 직원은 용의자가 노트북에 있는 아동 음란물 영상을 자신에게 보여준 적이 있으며, 집에 있는 플로피디스크에 음란물 사진을 보관하고 있다고 말한 적이 있음을 진술하였다.

주 검찰청은 용의자의 집에 대한 수색 영장을 받기 위하여 디지털 증거와 직원의 진술을 설명하였고, 판사는 영장을 발부하였다. 용의자의 집에서 여러 개의 플라티 디스크가 발견되었다. 이 플로피 디스크에 대한 포렌식 조사 결과 용의자가 포함되어 있는 아동음란물이 추가로 발견되었다. 이로 인하여 용의자는 체포되었다.

☑ 사건 개요 1 보고서

저장매체 분석 보고서

수신: County Sheriff's Police
Investigator Johnson
Anytown, USA 01234

제목: 저장매체 분석 보고서
용의자: DOE, JOHN
사건번호: 012345

1. 현재 상태: 조사 종결

2. 조사 결과 요약

- 327개의 아동에 대한 성적 표현물이 복구됨
- 플로피디스크에 있는 파일을 가리키는 단축아이콘 파일을 34개 복구하였는데, 이 파일의 이름은 아동과 관련된 성적 표현을 사용함

3. 분석 대상

- **사건번호**: 012345
- **설 명**: 노트북 컴퓨터 1대(시리얼번호 123456789)

4. 조사 결과 상세 내용

- ABCDE 모델(시리얼번호 3456ABCD)의 하드드라이브에 대한 조사 결과이며, 해당 하드드라이브는 시리얼 번호 123456789인 노트북 컴퓨터(태그번호 012345)에 탑재된 것임

1) 조사한 하드드라이브에는 운영 체제로 Microsoft Windows 98이 설치되었다.

2) 하드드라이브의 디렉토리와 파일목록은 마이크로소프트 엑세스 데이터베이스 TAG012345.MDB 에 저장하였다.

3) C:\JOHN DOE\PERSONAL\FAV PICS\ 디렉토리에서 327개의 아동포르노 영상 발견하였으며, 327개의 파일은 2001년 7월 5일 오후 11시 33분에서 11시 45분 사이에 생성되었다. 326개 파일에 대한 마지막 접근 일자는 2001년 12월 27일이다. 하나의 파일에 대한 최종 접근 날짜는 2002년 1월 6일이다.

4) C:\JOHN DOE\PERSONAL\FAV PICS TO DISK\ 디렉토리에 아동 음란물임을 암시하는 파일명을 가진 플로피디스크에 저장된 파일을 가리키는 34개의 단축아이콘 파일이 저장되어 있다. 34개의 단축아이콘 파일은 2001년 7월 5일 오후 11시 23분에서 11시 57분 사이에 생성되었으며, 34개의 단축아이콘 파일의 최종접근날짜

는 2001년 7월 5일이다.

5) C:\JOHN DOE\LEGAL\ 디렉토리에 5개의 마이크로소프트 워드 문서가 저장되어 있으며, 해당 파일은 용의자의 회사와 관련된 계약서 파일이다.

6) C:\JOHN DOE\JOHN DOE ROOFING\ 디렉토리에는 용의자의 회사 운영에 관련된 문서가 저장되어 있다.

7) 디스크에 사용자가 생성한 파일은 존재하지 않는다.

5. 용어

단축아이콘 파일(Shortcut File): 다른 파일에 연결하기 위해 생성된 파일

6. 제출 문서 및 물품

본 보고서와 보고서 파일을 저장한 CD이다. CD에 저장된 보고서 파일에는 발견된 파일과 디렉토리에 대한 하이퍼링크를 포함하고 있다.

IMA D. 조사관 작성자 : (인)
컴퓨터 포렌식 조사관

☑ 사건 개요 2

한 시민이 장물일 것으로 추측되는 물건을 경찰서에 신고했다. 그는 적당한 가격대의 오토바이를 구매하기 위해 관련 인터넷을 검색하던 중, 마음에 드는 광고를 찾았다고 진술하였다. 이 광고는 혼다 오토바이를 저렴한 가격으로 판매하고 있었는데, 판매자와 연락하여 만났을 때, 판매하려는 오토바이가 훔친 물건일 수 있다는 의심을 하게 되었다. 이 정보를 접한 경찰은 차량 절도 수사반(The Auto Theft Unit)에 이첩하였다. 차량 절도 수사반은 오토바이 구입을 하는 것처럼 위장하여 수사를 착수했다. 구매자로 가장한 수사관은 용의자를 만나서 대금을 지불한 후에 오토바이와 권리증서, 등록 카드, 보험 카드를 함께 전달받았다. 용의자는 체포되었고, 용의자가 운행한 차량은 그의 체포와 함께 수색되었다. 수색 도중에 노트북 컴퓨터가 압수되었다. 용의자가 제공한 서류들은 진짜처럼 보였지만, 문서 감정가는 위조된 문서로 판명했다. 차량 절도 수사관은 압수한 노트북 컴퓨터를 조사하기 위하여 컴퓨터 포렌식 랩에 연락을 취했다. 수사관은 컴퓨터를 분석하고, 문서 위조를 위해 사용한 자료와 차량 절도 혐의와 관련된 다른 증거물을 수색하기 위해 수색영장을 발부 받았다. 압수된 노트북 컴퓨터는 분석을 위해 컴퓨터 포렌식 랩에 전달하였다.

- 조사목적: 차량 절도, 사기, 위조, 위조문서 사용, 위조된 차량 등록증 보유 및 이러한 범죄와 관련된 데이터의 저장소로 용의자의 컴퓨터가 사용되었는지 판단.
- 컴퓨터유형: Gateway Solo 9100 노트북 컴퓨터
- 운영체제: Microsoft Windows 98
- 혐의사항: 차량절도, 사기, 위조, 위조문서 사용, 위조된 차량 등록증 소유
- 사건담당자: 차량절도 전담 수사관
- 조사장소: 컴퓨터 포렌식 랩
- 사용도구: Guidance Software EnCase, DiGit, Jasc Software, Quick View Plus, AccessData Password Recovery Toolkit

⊙ 조사 과정

✓ 증거평가

1. 수사관이 제출한 문서를 검토하였다.
   A. 포렌식 랩에서 컴퓨터 조사를 할 수 있는 수색 영장을 발부받았기 때문에 법적 권한이 확립되었다.
   B. 적정한 양식에 의해 절차 연속성 문서가 제대로 작성되었다.
   C. 수사관은 수사 기관의 요구사항과 사건개요를 설명하였고, 키워드 목록과 용의자, 도난 차량, 위조 문서, 인터넷 광고 등에 대한 정보를 제공하였다. 또한 수사관은 위조문서를 촬영한 사진을 함께 제출하였다.

2. 컴퓨터 포렌식 수사관은 사건 담당자와 만나 추가적인 수사 방향과 수사해야 할 잠재적인 증거물에 대하여 토의하였다.

3. 증거 수집이 완료되었다.

A. 증거에 분류표를 부착하고, 촬영하였다.
B. 관련된 서류철을 만들고 사건정보를 포렌식 랩 데이터베이스에 기록하였다.
C. 컴퓨터는 랩의 보관소에 보관하였다.

4. 이 사건에 대한 조사를 컴퓨터 포렌식 수사관에게 할당하였다.

✓ **이미징**

1. 노트북 컴퓨터를 조사하고, 촬영하였다.
A. 하드웨어를 조사하고, 기록하였다.
B. 포렌식 수사의 목적으로 작성된 조사용 부트 디스크를 컴퓨터의 플로피 드라이브에 삽입한다. 컴퓨터의 전원을 공급하고, BIOS 설정 모드로 전환하였다. BIOS 정보를 기록하고, 시스템 시간은 실제 시간과 비교하여 문서에 기입하였다. 컴퓨터 부팅 순서를 확인하고 문서에 기록하였는데, 이미 시스템 부팅순서의 첫 번째가 플로피 드라이브로 설정되어 있음을 확인하였다.
C. BIOS에 대한 정보를 변경시키지 않고, 컴퓨터의 전원을 차단하였다.

2. 노트북 컴퓨터의 하드 드라이브에 대한 이미지를 포함하는 증거물 파일 생성을 위해 EnCase를 사용하였다.
A. 컴퓨터 병렬 포트들을 연결하는 Null 모뎀 케이블을 사용하여 용의자 컴퓨터와 랩 컴퓨터를 연결하였다.
B. 조사용 부트 디스크를 이용하여 DOS 환경으로 노트북 컴퓨터를 부팅하였고, EnCase를 서버 모드로 실행하였다.
C. 저장 매체로 자기광 드리아브가 장착된 랩 컴퓨터를 조사용 부트 디스크를 이용하여 DOS 환경으로 부팅하였다. EnCase는 서버 모드에서 실행되었고 노트북 컴퓨터를 위한 증거 파일이 획득되었고 자기광 디스크에 저장되었다.
D. 이미징 절차가 완성되었을 때, 컴퓨터를 종료시켰다.
i. 조사 대상인 노트북 컴퓨터는 포렌식 랩의 보관소로 반환하였다.
ii. EnCase 증거 파일이 저장된 자기광 디스크를 쓰기방지로 설정하고 증거물에 접근하였다.

✓ **증거조사**

1. 포렌식 랩 컴퓨터의 운영체제를 Windows 98로 설치하고, Windows 용 EnCase, 기타 포렌식 도구를 준비하였다.

2. 노트북 컴퓨터에서 수집한 EnCase 증거 파일을 포렌식 랩 컴퓨터의 하드 디스크에 복사하였다.

3. 새로운 EnCase 사건 파일을 생성하고, 노트북에서 수집한 증거 파일을 Encase로 조사하였다.
A. 삭제된 파일을 EnCase를 이용하여 복구하였다.

B. 파일 이름, 일시, 물리적/논리적 크기, 경로 등을 포함하는 파일 데이터를 기록하였다.
C. 수사관이 제공한 사건 개요를 기반으로 키워드 검색을 수행하였다. 모든 검색 결과를 확인하였다.
D. 그림 파일을 열어 확인하였다.
E. HTML 파일을 열어 확인하였다.
F. 데이터 파일을 열어 확인하였으며, 패스워드 보호된 암호 파일 두 개가 발견되었다.
G. 미할당 영역과 슬랙 공간을 검색하였다.
H. 증거로 가치가 있거나 수사의 실마리가 될 수 있는 파일을 Encase 증거 파일로부터 복구/복사하였고, CD에 복사하였다.

4. Encase 증거 파일로부터 미할당된 클러스터를 복구하여 미국 국방성에서 제시된 기준에 의거 깨끗하게 초기화된 하드 디스크에 복사하였다. 그 후, 미할당 영역에서 이미지를 추출하기 위해 DiGit 도구를 사용하였는데, 8,476개의 이미지가 추출되었다.

5. 패스워드로 보호된 파일은 1.44MB 플로피 디스크에 복구/복사하였다. 패스워드 검색을 위해 AccessData Password Recovery Toolkit을 실행하였고, 두 파일 모두 패스워드를 복구하였다. 해당 패스워드를 이용하여 실제 데이터를 확인하였다.

✓ **조사결과**

노트북 컴퓨터를 조사한 결과, 176개의 파일이 증거로서 가치가 있거나 추가적인 조사가 필요한 것으로 판명되었다.

1. 용의자의 이름 및 개인정보, 위조문서에 포함된 내용, 스캔한 임금 대장, 회사명, 지불 보증 수표, 훔친 항목을 설명하는 내용, 개조한 오토바이 대한 설명 등이 포함된 59개의 문서 파일

2. 임금 대장, 기업명, 지불 보증 수표, 미국 화폐, 차량 권리증, 등록카드, 조지아주 및 기타 주의 운전 면허증 양식, 여러 회사의 보험카드, 컴퓨터를 구입하기 위해 컴퓨터 회사에 지급할 수 있는 $25,000에서 $40,000에 이르는 위조된 보증수표 등을 나타내는 해상도가 높은 38개의 이미지 파일

3. Hotmail, Yahoo 이메일과 개조한 오토바이, 기타 차량들, 주요 브랜드의 노트북 컴퓨터에 대한 비밀 광고가 포함된 63개의 HTML 파일. 여기에는 개조한 오토바이의 구매에 관심있는 사람과 용의자 사이에 주고받은 이메일, 노프북 컴퓨터 판매에 관심있는 컴퓨터 업체와 용의자 사이에 주고받은 이메일 등이 포함됨

4. 미할당 영역에서 미국 화폐를 스캔한 이미지 및 여러 단계의 위조 수표 등이 포함

된 14개의 이미지 파일 복원

5. 패스워드로 보호된 두 개의 암호 파일
   i. 성명, 주소, 생일, 신용카드번호, 은행 계좌번호, 만료일, 당좌예금 정보, 기타 정보 등 여러 명의 개인신상 정보들이 기록되어 있는 WordPerfect 문서이며, 페스워드는 nomoresecrets 임
   ii. 개조한 오토바이의 차량 권리증이 저장된 MS Word 문서이며, 패스워드는 HELLO임

✓ **문서화**

1. 포렌식 보고서 - 모든 행위, 절차, 조사 결과가 상세히 기록된 보고서로 포렌식 랩 사건 철에 보관되었다.
2. 경찰 보고서 - 조사하였던 증거물, 사용한 기법, 조사결과를 설명한 보고서로 사건 담당자에게 제출하였다.
3. 조사 결과물 - 증거로 가치 있거나 추가 수사가 필요한 데이터와 파일이 포함된 CD. 원본은 포렌식 랩 사건 철에 보관하였으며, 복사본은 사건 담당자와 검사에게 제출하였다.

✓ **요약**

컴퓨터 분석을 통해 조사된 정보를 기반으로 몇 개의 새로운 수사 방향을 제시하였다.

☞ 패스워드로 보호된 Word 문서에 나열된 피해자들과 연락한 결과, 피해자들은 지난 여름에 같은 도시에서 모두 용의자와 접촉하였음을 알게 되었다.

☞ 용의자 컴퓨터에서 발견된 위조 수표에서 드러난 컴퓨터 회사에 확인한 결과, 컴퓨터 구매에 사용되었으며, 구입한 컴퓨터가 용의자에게 전달된 바, 해당 컴퓨터는 수사 대상이 되었다. 컴퓨터 회사에서 제공한 모델번호와 시리얼번호는 용의자의 컴퓨터에서 발견된 Hotmail과 Yahoo의 비밀 광고와 일치하였다.

☞ 용의자 컴퓨터에서 발견된 여러 개의 위조 수표는 이미 수사 대상이었다.

☞ 복구된 다른 차량에 관한 정보는 추가적으로 도난 차량임이 밝혀졌다.

☞ 위조문서와 훔친 차량의 판매에 관하여 수색 영장에서 지정한 특정 정보는 용의자의 컴퓨터에서 복구되었다.

✓ **결론**

용의자는 결국 모든 죄를 인정하였고 현재 수감 중이다.

☑ 사건 개요 2 보고서

주립 경찰서
컴퓨터 범죄수사반
컴퓨터 포렌식 랩
7155-C Columbia Gateway Drive
Columbia, MD 21046
(410) 290-0000

1999년 4월 19일

포렌식 조사과정 기록 조사관: **SGT.David B. Smith (5555)**
포렌식 사건번호: **99-03-333-A**

조사 요청자:	TFC. Brian Jones 주립 경찰 차량 절도 수사반 (310-288-8433)
혐의 내용:	차량 절도 및 위조
사건번호:	01-39-00333

수신일:	1999년 3월 19일
조사개시일:	1999년 3월 24일
조사완료일:	1999년 4월 19일

포렌식 조사 시간:	40 시간
운영체제:	Microsoft Windows 98
파일시스템:	FAT32
분석데이터 크기:	7,782MB

증거물: Gateway Solo 9100 노트북 컴퓨터, 시리얼번호555-Z3025-00-002-0433

조사 일지:
1999년 3월 24일

16시 00분

- 원본 디지털 증거를 CCU Property Room 으로부터 인계받음
- 증거 목록 작성, 이름표 부착 후 MSP Form 67에 명시되어 있는 증거로 분류
- 절차 연속성 양식에 나열된 모든 증거를 대조함

16시 20분

- Gateway Solo 9100 노트북 조사

- 초기 컴퓨터 증거 처리 양식(Initial Computer Evidence Processing Form) 작성(첨부 문서 참조)
- 컴퓨터에 하나의 고정디스크 존재
- 드라이브(원본 디지털 증거 번호 hdd01)를 보기 위해 노트북 케이스를 열지 않음
- 노트북의 플로피 드라이브에 조사용 부트디스크 삽입 후 노트북을 동작시킴
- F1 버튼을 눌러 Setup 환경 실행
- 다음과 같이 바이오스가 설정되어 있었음

주립 경찰 - 컴퓨터 포렌식 연구실
포렌식 보고서 - 랩 사건 번호 99-03-333-A

BIOS	시스템 날짜	시스템 시간	메모리	부팅 순서
Award 4.5 pg	3/24/1999	16:30:03	128MB	플로피드라이브 하드드라이브
	실제 날짜 3/24/1999	실제 시간 16:30:08	CPU Intel PII 300	

EnCase(1.998)(DOS Version 7.10)

물리 디스크 : 1개					논리 볼륨 : 1개				
Disk 0 Size 7.6GB CHS 7480:16:63					LP	LABEL	SYSTEM	FREE	SIZE
Lock	Code	Type	Sector	Size	C0	NONAME	FAT32	5.5GB	7.6GB
80	0B	FAT32	16,000,740	7.6GB					

En.exe 파일을 포렌식 랩 컴퓨터에서 실행하여 다음과 같은 EnCase 보고서 획득

EnCase(1.998)(DOS Version 7.10)

물리 디스크 : 1개					논리 볼륨 : 1개				
Disk 0 Size 7.6GB CHS 7480:16:63					LP	LABEL	SYSTEM	FREE	SIZE
Lock	Code	Type	Sector	Size	C0	NONAME	FAT32	5.5GB	7.6GB
80	0B	FAT32	16,000,740	7.6GB					

17시 50분

- 압축된 형태의 증거 파일 획득 시작
- 파일 명 및 경로: F:\hdd01
- 사건번호: 01-39-00333
- 조사관: Sgt. David B. Smith
- 증거번호: 99-03-333-A
- 요약: 555-Z3025-00-002-0433

1999년 3월 25일

09시 00분

- EnCase의 이미징 결과보고 내용 : "An evidence file for drive 0 was successfully created ... Elapsed Time 11:14:00, 7.6GB read, 0 errors, 11:14:00 elapsed, 0:00:00 remaining"

09시 10분

- 랩 컴퓨터의 EnCase 종료 후 "A:/prompt" 상태로 돌아감
- 컴퓨터 전원을 내린 후 증거 파일이 저장된 소니 MO 디스크를 MO 드라이브에서 제거하여 쓰기방지 상태로 설정하고 증거물 보관소로 이동(placed into evidence)
- 주립 경찰의 절차 연속성 서류를 작성

1999년 3월 30일

14시 00분

- 랩의 Gateway GX-450XL 컴퓨터는 AHA 2940UW SCSI 어뎁터 카드로 연결된 소니 MO 드라이브를 장착하고 있음
- 조사용 부트디스크를 A: 드라이브에 삽입 후 시스템을"A:\prompt"로 부팅
- DOS의 copy 명령을 이용하여 소니 MO 디스크의 F:에 있는 Encase 증거파일을 하드디스크의 E: 로 복사
- 파일복사 성공 후 컴퓨터를 끄고 Sony MO 디스크는 증거보관소로 보냄

1999년 4월 1일

08시 00분

- 랩의 Gateway GX-450XL 컴퓨터를 Microsoft Windows 98로 부팅
- Window 98 용 EnCase(버전 1.999) 시작
- EnCase에서 새로운 case 파일을 생성하고 99-03-33-A로 명명함
- 획득한 이미지 파일을 사건에 추가한 후 EnCase 파일의 무결성을 확인함.

09시 00분

- EnCase에서 case 파일에 포함된 데이터 논리분석을 시작

10시 00분

- 랩 컴퓨터 Gateway GX-450XML의 I: 드라이브를 와이핑 도구를 이용하여 완전 삭제를 실행
- 해당 드라이브는 미 국방부에서 추천하고 있는 방식(DoD 5200.28-STD)을 준수
- 증거 파일의 미할당 클러스터와 슬랙공간의 데이터를 I: 드라이브로 복사
- 복사된 파일은 7개의 폴더에 나누어 저장되었으며, 각 폴더는 최대 1MB의 크기를 가짐
- 총 5,944MB에서 575개 파일이 복사됨

12시 20분

- NCIS DIgit(버전 1.08) 실행.
- 증거 파일에서 I: 드라이브로 복사된 파일 조사
- 미할당 클러스터와 슬랙 공간에서 복사된 5,944MB 크기의 파일을 7개의 일괄 처리과정으로 분석함

미할당 공간에서의 파일 추출내역

DIGit® (Version 1.08)

Batch	HITS	Jpg	Bmp	Gif	Tif	Pcx	HTML	Word8	Total Megs Examined
1	5,378	197	82	4,908	11	16	66	98	1,048
2	2,499	53	48	2,258	14	3	76	47	1,048
3	599	0	6	550	4	6	11	22	1,048
4	0	0	0	0	0	0	0	0	1,048
5	0	0	0	0	0	0	0	0	1,048
6	0	0	0	0	0	0	0	0	704
7	0	0	0	0	0	0	0	0	512 bytes
Total	8,476	250	136	7,716	29	25	153	167	5,944MB

추출된 그래픽 파일은 Digit view Plus로 확인

1999년 4월 4일

09시 30분

- DIGit를 이용하여 추출된 미할당 공간의 그래픽 파일과 HTML파일 조사 계속

10시 00분

- 전체 case 파일을 대상으로 EnCase 1.999를 이용하여 키워드 검색 수행
- 발견된 모든 결과를 조사하고 증거가치가 있는 데이터 추출

Search 1: Keyword: honda Hits: 433

1999년 4월 5일

07시 00분

- DIGit를 이용하여 추출된 HTML 파일에 대한 조사 계속

13시 54분

- 전체 case 파일을 대상으로 EnCase 1.999를 이용하여 키워드 검색 수행
- 발견된 모든 결과를 조사하고 증거가치가 있는 데이터 추출

Search 2:	**Keyword:**	**99985 (Case)**	**Hits:**	**0**
		999886(Case)		**1**
		ZDF-3333 (Case)		**0**
		39347618		**0**
		virginia		**212**
		georgia		**333**
		certificate of title		**0**
Search 3:	**Keyword:**	**motorcycle**	**Hits:**	**1,696**

1999년 4월 6일

08시 00분

- 전체 case 파일을 대상으로 EnCase 1.999를 이용하여 키워드 검색 수행
- 발견된 모든 결과를 조사하고 증거가치가 있는 데이터 추출

Search 4:	**Keywords:**	**suzuki gsxr**	**Hits:**	**2**
Search 5:	**Keyword:**	**brandell**	**Hits:**	**125**
Search 6:	**Keywords:**	**jh2sc3307wm20333**	**Hits:**	**5**
		..#..####..######(Grep)		**0**
Search 7:	**Keyword:**	**Jn8hd17y5nw011333**	**Hits:**	**0**

1999년 4월 7일

08시 00분

- 검색 결과에 대한 조사 계속

13시 33분

- 전체 case 파일을 대상으로 EnCase 1.999를 이용하여 키워드 검색 수행
- 발견된 모든 결과를 조사하고 증거가치가 있는 데이터 추출

Search 8:	**Keywords:**	**9998##(Grep)**	**Hits:**	**5**
		hotmail		**19,465**
		chyma		**27,453**
		suzuki		**20**

1999년 4월 19일

07시 00분

- 증거 이미지 파일에 대한 개별 조사 계속

09시 00분

- 포렌식 조사 완료
- EnCase 키워드 검색과 NCIS DIGit에서 개별 파일 조사를 통해 발견된 문서파일, 그림파일, HTML파일과 부분문자열에 대한 위치를 저장
- 키워드 검색 결과는 EnCase 보고서에 포함
- 수사에 도움을 줄 것으로 판단되는 파일을 분류하여 북마크함
- 발견된 정보와 관련된 파일은 EnCase case 파일에서 복구/복사함

조사 결과

노트북 컴퓨터의 분석 결과 증거로써 가치가 있을 것으로 판단되거나 수사에 도움을 줄 수 있는 176개 파일을 복구하였으며 그 내용은 다음과 같다.

1. 용의자의 이름과 개인정보가 저장된 문서를 포함하여 총 59개의 문서
   - 위조문서에 포함된 내용
   - 스캔한 급료 지불 명부, 회사명, 지불 보증 수표
   - 도난 물품에 대해 설명하거나 관련된 내용
   - 개조한 오토바이를 설명한 내용

2. 급료 지불 명부, 회사명, 지불보증수표에 대한 고해상도 그림파일 총 38개
   - 지폐
   - 차량 모델명
   - 등록 카드(Registration cards)
   - Georgia와 다른 주에 대한 운전면허증 템플릿
   - 여러 보험 회사 카드(insurance cards)
   - 노트북 구입을 위한 $25,000~$40,000의 위조된 지불보증수표
   - 대부분의 파일은 스캔이 된 형태임

3. Hotmail과 Yahoo 이메일을 포함한 총 63개의 HTML 파일이 있었으며 개조한 오토바이 및 다른 차량과 몇 종류의 노트북 컴퓨터에 대한 비밀 광고도 포함되어 있음
   - 용의자와 개조한 오토바이의 구입에 관심있는 사람 사이의 이메일 문자열
   - 용의자와 노트북 컴퓨터를 판매하고자 한 회사 사이의 이메일

4. 미할당 공간의 파일복원(Carving)을 통해 여러 단계의 수표와 미국 지폐(U.S currency)를 스캔한 파일 14개 복원

5. 2개의 패스워드로 보호된 암호 파일
   - 성명, 주소, 생일, 신용카드, 은행 계좌번호, 만료일, 수표계좌 정보 및 다른 개인 정보의 목록이 저장된 WordPerfect 문서(암호 : nomoresecrets)
   - 개조한 오토바이에 대한 정보를 저장하고 있는 마이크로소프트 워드 문서(암호 : HELLO)

상기 열거된 파일의 복사본을 저장한 CD를 제작하였고, 이는 컴퓨터 포렌식 랩 사건철에 보관될 것이다. CD의 사본은 라벨을 붙여 수사관에게 전달되었다.

18시 00분 포렌식 조사 완료

부록 B. 용어 정리

획득(Acquisition) : 디지털 증거를 복제하고, 복사하고, 이미징 작업을 하는 과정

분석(Analysis) : 사건의 증거가 될 중요 요소들을 조사하는 것

BIOS : Basic Input Output System. 컴퓨터의 운영체제 구동과 하드웨어 장치(모니터, 키보드, 프린트, 디스크 드라이브)와의 연결에 필요한 설정을 위해 ROM에 저장된 설정 값

CD-RW : Compact Disk-ReWritable. 쓰기, 사제가 가능한 CD

CMOS : Complementary metal oxide semiconductor. BIOS 설정 정보를 저장하는데 사용되는 칩 종류

압축파일(Compressed file) : 디스크 공간을 절약하기 위하여 압축 알고리즘을 사용하여 파일의 크기를 작게 만든 파일. 파일을 압축하면 압축이 푸리기 전까지는 대부분의 프로그램에서 읽을 수 없다. 일반적인 압축 도구는 PKZIP이며 확장자가 .zip이다.

복사(Copy) : 전기적 저장 매체와 상관없이 원본 물리적 데상에 포함되어 있는 정보를 정확하게 재생산하는 행위. 내용은 유지하지만 재생산 과정 중에 속성 정보는 변경될 수 있다.

삭제된 파일(Deleted file) : 용의자가 컴퓨터에 범죄와 관련된 파일이 있다는 것을 알면, 증거 인멸을 위하여 해당 파일을 삭제할 것이다. 대부분의 컴퓨터 사용자들은 정확히 삭제된 줄 알지만, 파일이 삭제되는 방식에 따라서 많은 경우 포렌식 조사자가 원본 파일의 일부나 전부를 복구할 수 있다.

디지털 증거(Digital Evidence) : 법적 효력이 있는 바이너리 형태로 저장되거나 전송된 정보

복제(Duplicate) : 디지털 저장 장치(하드디스크, Cd-ROM, 플래쉬 메모리 등) 상에 있는 원본 데이터와 정확하게 똑같이 재생산하는 과정. 파일의 내용과 속성이 정확하게 복사됨

전자기 간섭(Electromagnetic interference) : 전기/전자 장비의 성능으 떨어뜨리거나 방해하는 전자기 교란

암호화(Encryption) : 특정 사람만이 평문을 확인할 수 있도록 암호문으로 바꾸는 암호 기술 절차

조사(Examination) : 분석에 적합하도록 증거를 읽고 판독할 수 있도록 만드는 기술적 검토. 특정한 데이터의 존재 유무를 판단하기 위해 증거에 행하는 시험.

비정상 파일 이름(File name anomaly) : 헤더와 확장자 불일치. 파일 이름과 내용이 불일치

파일 슬랙(File slack) : 파일이 할당된 메모리 공간에서 파일의 논리적 끝과 할당 영역 끝 사이의 공간

파일 구조(File structure) : 응용 프로그램이 파일 내용을 저장하는 방식

파일 시스템(File system) : 운영체제가 디스크 드라이브 상에서 파일을 추적 관리하는 방식

포렌식적 초기화(Forensically clean) : 디지털 저장매체를 사용하기 전에 잔여 데이터가 없게 완벽히 삭제하고, 바이러스 검사와 검증을 수행하는 것

해쉬작업(Hashing) : 수학적 알고리즘을 사용하여 해당 데이터를 나타내는 숫자 정보를 생산하는 과정

HPA 영역(Host protected area) : ATA4 이후 버전에 정의된 기술적인 스펙에 부합되도록 IDE 디스크 상에 설정될 수 있는 영역. 만약 파일시스템에서 사용하는 가장 높은 주소(Max address)가 실제 가장 높은 주소(native Max address)보다 작게 나타난다면, HPA 영역이 존재하는 것으로 판단할 수 있다.

IDE : Intergrated drive eletronics. 일반적으로 저장 장치와 연결하는 데이터 전송 인터페이스의 유형

이미지(Image): 디지털 저장 장치(CD-ROM, 하드디스크, 플로피 디스크, 플래쉬 메모리 등)에 존재하는 모든 데이터의 정확한 디지털 표현물. 내용과 속성을 유지하며, CRC, 해쉬 값, 감사 정보와 같은 메타 데이터도 포함할 수 있음

인터넷 서비스 제공자(ISP) : Internet service provider. 개인이나 회사들에게 인터넷 접속서비스, 웹사이트 구축 및 웹호스팅 서비스 등을 제공하는 회사.

Mac address : Media Access control address. 네트워크 인터페이스 카드를 식별하기 위해 제조사에서 부여한 번호

MO : Magneto-optical. 개인 컴퓨터의 파일을 백업하기 위해서 전자기, 광학 기술을 사용하는 드라이브

네트워크 : 정보와 자원을 공유하기 위하여 연결된 컴퓨터 집합체

원본증거(Original evidence): 압수 시점의 물리적 아이템과 그와 관련된 데이터

패스워드 보호(Password protected) : 많은 소프트웨어 프로그램은 패스워드를 사용한 파일 보호 기능을 가지고 있다. 패스워드 보호의 한 유형은 “접근 거부”라는 용어로도 사용된다. 이러한 방법이 사용된다면, 데이터는 디스크 상에 일반적으로 제공되지만 패스워드가 입력되지 않는다면 소프트웨어는 파일을 열어서 사용자에게 보여주지 않는다. 포렌식 조사자는 이러한 패스워드 검증을 우회하거나 통과해야할 경우가 종종 있다.

보존 명령(Preservation order) : 개인이나 회사에게 잠재적인 증거의 보존을 명령하는 문서.

소유권이 있는 소프트웨어 (Proprietary software): 개인이나 회사가 소유하고 있고, 라이센스가 필요한 소프트웨어.

이동형 매체(removable media): 데이터를 저장하고 쉽게 제거할 수 있는 장치(플로피 디스크, CD, DVD, USB disk 등)

SCSI : Samll Computer System Interface. 데이터 통신 인터페이스 형태

스테가노그라피(steganography) : 메시지가 전송되고 있다는 사실을 숨기는 기술로써 내용을 숨기기 위해 은닉 채널이나 보이지 않는 잉크를 사용하는 것과 매우 유사한 기술로 이미지 및 오디오 파일과 같은 다양한 디지털 매체를 통해 메시지를 숨겨 전송하는 것을 말한다.

시스템 관리자(System Administrator): 컴퓨터 시스템을 관리할 권한이 있는 자. 관리자는 시스템에 빠른 속도로 접속이 가능하며, sysop, sysadmin, system operator로 불리기도 한다.

비할당영역(unallocated space): 파일 시스템 안에서 실제 파일이 할당되지 않은 영역

쓰기방지보호(Write protection) : 디스크나 다른 저장 매체에 데이터가 쓰이는 것을 방지하는 하드웨어 또는 소프트웨어 방법

부록 C. 양식 예

컴퓨터 증거 작업표

사건 번호 : _____ 제출 번호 : _____
랩 번호: _____ 관리 번호 : _____

컴퓨터 정보

제조사 : _____ 모델 : _____
일련 번호 : _____
조사관 정보 : _____

컴퓨터 유형 : 개인용 컴퓨터 ☐ 노트북 ☐ 기타 : _____
컴퓨터 상태 : 정 상 ☐ 손상됨 ☐ (참고사항 참조)
하드 디스크 수 : _____ 3.5″ 플로피 디스크 ☐ 5.25″ 플로피 디스크 ☐

모뎀 ☐ 네트워크 카드 ☐ 테이프 저장장치 ☐ 테이프 저장 장치 유형 : _____

100MB ZIP 디스크 ☐ 250MB ZIP 디스크 ☐ CD 읽기 가능 ☐ CD 읽기/쓰기 가능 ☐

DVD ☐ 기타 : _____

CMOS 정보	사용 불가능 ☐

비밀번호 설정 여부 : 예 ☐ 아니오 ☐ 비밀번호 : _____

현재 시각 : _____ 오전 ☐ 오후 ☐ 현재 날짜 : ___/__/__

CMOS 시각 : _____ 오전 ☐ 오후 ☐ CMOS 날짜 : ___/__/__

1번 하드 디스크 CMOS 설정	자동 ☐

용량 : _____ 실린더 수 : _____ 헤드 수 : _____ 섹터 수 : ____

모드 : LBA ☐ NORMAL ☐ Auto ☐ Legacy CHS ☐

2번 하드 디스크 CMOS 설정	자동 ☐

용량 : _____ 실린더 수 : _____ 헤드 수 : _____ 섹터 수 : ____

모드 : LBA ☐ NORMAL ☐ Auto ☐ Legacy CHS ☐

해당 컴퓨터의 부가 물품

부가 번호	유형	발견 장소

참고 사항

Hard Drive 증거 작업계획표

사건 번호: _____ 체출 번호: _____

랩 번호: _____ 관리 번호: _____

Hard Drive #1 레이블 정보 [사용 불가능☐] Hard Drive #2 레이블 정보 [사용 불가능☐]

제조사: _____ 모델: _____ 시리얼번호: _____ 용량: _____ 실린더: _____ 헤드 : _____ 섹터: _____ 컨트롤러 버전수정 _____ IDE ☐ 50 Pin SCSI ☐ 68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐	제조사: _____ 모델: _____ 시리얼번호: _____ 용량: _____ 실린더: _____ 헤드 : _____ 섹터: _____ 컨트롤러 버전수정 _____ IDE ☐ 50 Pin SCSI ☐ 68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐
Jumper: Master ☐ Slave ☐ Cable Select ☐ Undetermined ☐	Jumper: Master ☐ Slave ☐ Cable Select ☐ Undetermined ☐

Hard Drive #1 파라미터 정보

DOS FDISK ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

용량: _____ 실린더: _____ 헤드: _____ 섹터: _____

LBA Addressable 섹터: _____ 포맷된 드라이브 용량: _____

볼륨레이블: _____

파티션

이름:	부트가능?	시작:	끝:	파일시스템유형:
	☐			
	☐			
	☐			
	☐			

Hard Drive #2 파라미터 정보

DOS FDISK ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

용량: _____ 실린더: _____ 헤드: _____ 섹터: _____

LBA Addressable 섹터: _____ 포맷된 드라이브 용량: _____

볼륨 레이블: _____

이름:	부트가능?	시작:	끝:	파일시스템유형:
	☐			
	☐			
	☐			
	☐			

이미지 보관 정보

보관 방법: Direct to Tape ☐ NTBackup ☐ Tar ☐ Other:*_____ 압축 여부?☐

사용한 백업 방법에 대한 적당한 워크시트를 첨부하시오.

테이프 형태: DAT 24 ☐ DAT 40 ☐ DLT ☐* Other*: Number Used:

플랫폼 분석 정보

운영체제: DOS ☐ Windows ☐ Mac ☐ *nix ☐ Other: _____

버전: _____

분석 S/W: I-Look ☐ EnCase ☐ Dos Utilities ☐ *nix Utilities ☐ Other:*

버전:

수행한 복구 작업(복사/이미지)이 유효한가?	예 ☐ 아니오 ☐

기타 사용한 유틸리티 목록

이 름	버 전	목 적

분석 마일스톤

마일스톤	설명	확인
안티-바이러스 스캐닝		
모든 파일 리스트 획득(메타데이터 포함)		
사용자/로그온 사용자/ISP 계정 등 확인		
파일 시스템 브라우징		
키워드/문자열 탐색		
웹/전자메일 헤더 복구		
미사용 영역/슬랙 공간의 복구 및 검사		
Swap 영역 검사		
삭제된 파일의 복구		
Execute Program as Needed		
전자메일/채팅 내용 복구 및 검사		
패스워드 크랙		

이동식 저장장치 워크시트

사건 번호: _____ 체출 번호: _____

랩 번호: _____ 관리 번호: _____

저장 장치 종류 및 수량

종류	용량	수량	종류	용량	수량	종류	용량	수량
USB 플래시 메모리			DVD			CD		
Jazz 드라이브			ZIP 드라이브			Magneto-Optical		
디스켓			Tape			Other		

점검표

증거물 번호	우선순위 (Triage)	복 제 (Duplicate)	탐 색 (Browse)	복 구 (Unerase)	키워드 검색 (Keyword Search)
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

조사자 **날짜** 감독관 날짜

_____ _____ _____ _____

증거물 번호	우선순위	복제	탐색	복구	키워드 검색
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

부록 D. 포렌식 조사 요청서 예

예 1: 지역 컴퓨터 포렌식 랩

4455 Genesee Street, Cheektowaga, NY 14225

포렌식 분석 요청서

사건 정보:		**랩 사건 번호:**
제출인/ID#:	날짜:	의뢰자 사건번호 #:
의뢰 기관:	서비스: **현장 랩 기술**	사건명:
기관 소유 표 #:	용의자 성명:	
사건 담당자:	전화번호:	
DDA/AUSA Assigned:	전화번호:	
압수 날짜:	사건/범죄 형태:	
압수 장소:	공판 날짜:	
소재지 #:	필요한 데이터 분석:	
구금된 용의자: **예/아니오**	증거 반환 예정일:	
관련된 마약: **예/아니오**	예상 컴퓨터 수:	
압수 형태:(Circle) **수색영장 보호관찰 집행유예 동의 Admin 연방대배심 기타:**		
이 증거가 다른 사람에 의해 사전에 검토 또는 접근된 적이 있습니까?(설명)		
당신은 증거에 포함되어 있는 특별한 정보를 알고 있습니까?(설명)		
당신은 증거에 대하여 표준 사건과 관련된 문자열 검색을 원합니까? **예/아니오** (관련된 영역에 체크) **아동 음란물 마약 회계부정 인터넷범죄 강탈 기타:**		

서비스 요청:(현장 조사에 대한 요청은 적어도 2일 간의 행정 절차가 필요함)

예 2 : DoD Computer Forensics Laboratory (DCFL) Intake Form

기관의 심볼 문구

Department of the air force

(Form has been edited)
(USE YOUR OWN LETTER HEAD)
MEMORANDUM FOR RECORD DoD Computer Forensics Laboratory

- 12 June 2000

수신: DoD Computer Forensics Laboratory (DCFL)
911 Elkridge Landing Road, Suite 300
Linthicum, MD 21090
발신: Self-Explanatory
제목: 포렌식 매체 분석 요청 (수사 번호)
NOTE: 굵은 글씨로 적혀진 항목은 남겨두고 설명부분은 삭제하라. 항목에 해당하는 정보가 없다면 N/A 또는 모름(unknown)이라고 작성한다.

1. ***용의자의 성명: 성명을 모른다면, "현재 불명"이라고 작성한다.

2. ***우선순위: 공표 사실, 우선 관심사, 공판 날짜와 같은 사항과 관련되어 앞으로 진행될 수사에 관한 사항이 있다면 설명하라.

3. 분류: 공개-비밀-특정 보호 조치와 같은 분류하고 적절히 표시하라.

4. ***사건 담당자 : 수사책임자를 의미하며. 협력 수사를 진행하고 있다면, 선임기관의 지휘자를 기입한다. 상세한 주소와 소속을 제공하라.

5. ***사건 개요 : 사건에 대한 상황과 내용, 배경에 대해서 간략하게 작성한다. 분석관에게 도움이 될만한 정보들을 기술하여, 좀 더 우수한 조사가 진행될 수 있도록 한다.

6. ***분석할 ITEM: (증거가 아니라면, 사실 내용을 기술한다.)
NOTE: 모든 질문에 대답하는 것이 아니라, 분석해야 할 ITEM을 목록화해야 한다. 증거 목록은 모든 ITEM을 식별할 수 있도록 작성되어야 한다. 그 예는 다음과 같다.

Tag #'s Description
Tag # XX Western Digital Caviar 31600 Hard Drive, Serial #: WT2891586134 taken from AST Computer Serial # 186AUZ022348.
Tag # XX Fujitsu M1636TAU Hard Drive, Serial #: 08613105, Size: 1226MB.

Tag # XX Gateway 2000, 386/33 MHz, Serial #: 302557386-330XC. Computer System with a Western Digital 125 MB internal hard drive, a Seagate 107 MB internal hard drive, internal 3.5-inch high-density floppy drive, one internal 5.25-inch floppy drive, internal sound card. Gateway 2000 101 Keyboard, Serial #: 9208572226f7. Computer Mouse Device, Serial #: 850753.

Tag # XX 198 each 3.5-inch floppy diskettes 1 each 5.25-inch floppy diskettes

7. ***지원 요청: (세부적인 특정 요구사항들을 기입.)

예) **Computer Media**

Extract all system logs, graphic files, text, documents, etc.
Examine file system for modification to operating system software or configuration.
Examine file system for back doors, check for setuid and setgid files.
Examine file system for any sign of a sniffer program.
Extract data from this 8-mm tape and convert to readable format, cut to CD.
Backup hard drives and place backup on a CD, tape, or other format.
Analyze for deleted files and restore deleted files, cut findings to CD.
If possible, correlate sexually explicit images to the Internet history file.
Extract sexually explicit images from logical, slack space, free space, cut to CD.
Extract all pertinent text files of a sexual nature.
Provide an analysis report and cut all findings to CD (specify).
Conduct string search on physical level of media (provide list of words).

8. 부가데이터: (예: 패스워드, 키워드 목록, 운영체제, 별명, 컴퓨터 형태, 네트워크 정보, IP 주소 등 분석에 도움이 되는 내용)
NOTE: 네트워크 침입 탐지 로그나 다른 형태의 침입 탐지 로그(ASIM log, 스니퍼 로그)가 현재 수사에 관련되어 있다면, 제공되어야 한다. 이러한 데이터가 조사를 좀 더 낳은 방향으로 할 수 있으며, 분석에 필요한 적절한 항목을 선별할 수 있다.

NOTE: 조사자는 요청한 특정 작업만을 수행할 것이다. 명시하지 않은 작업은 수행하지 않는다. 명확한 항목만 있다면, DCFL은 확인하기 위해 연락할 것이다. 자세하게 정보가 제공될 수록 세밀한 분석이 수행될 것이다.

NOTE: 필요하다면, 요청서 작성을 위해 컴퓨터 전문가에게 도움을 요청하라.

9. ***권한: 요청한 검색을 시행하는데 필요한 법률적인 내용을 기입하라. 일반적으로 다음의 세 가지 사항으로 분류할 수 있다.

1. 수색 영장, 군 수색 허가

2. 동의서
    - ■ DoD Banner.
    - ■ 개인이나 단체의 동의
    - ■ 책임자가 서명한 동의서
    - ■ 매체를 수색할 수 있는 권한을 증명할 수 있는 문서
    - ■ 구두 동의에 대한 메모
3. 제출된 매체는 개인정보 보호에 대한 권리를 가질수 없다는 것을 공식적인 메모

10. ***다른 문서들 : 요청자는 그 조직에서 자주 사용되는 문서 형식을 제공한다. (ACISS 보고서 복사본, Army Form 66, or Navy ALS, etc.)

11. 정보 제공: 특정한 정보가 있다면 DCFLdp 알려주기 바란다.

12. ***POC is: 요청자의 연락처를 기록한다. 정확한 신원정보를 기입한다.
SA Jane Doe, AFOSI Detachment 999 at DSN: 123–1234 or Commercial: (123) 123–1234.

NOTE: 필요한 정보가 모두 제공되지 않는다면, 요청된 분석은 모든 정보가 제공될 때까지 잠시 중단될 것이다.

예 3 : Department of Maryland State Police Coumputer Forensic Lab.

디지털 포렌식 연구실 전화 : 82-2-3290-4293 팩스 : 82-2-928-9109

조사 요청서

제출일:				MSP Complaint Conrol #:	
기관:	주소		County	기관 사건번호 #:	
수사관:	ID:	E-Mail주소		전화:	
입수장소:			압수 일시:	압수기관 #:	
사건명:	이름		성별 M/F	나이:	전화 :
Crime:	사건 발생일:	Date Charge Filed		재판일시:	재판장소:
사건 담당자:			주소:		전화:

압수형태 : 영장청구, 사전 동의, 행정처리, 연방배심

컴퓨터 수:	
사전에 증거 데이터에 접근한 적이 있는가? 예 아니오	
제출된 증거에 포함된 특별한 정보를 알고 있는가? 예 아니오	
제출된 증거 데이터 간에 관련된 정보를 알고 있는가? 예 아니오	

□ 긴급 요구 사항

의뢰서 수신일:	이름:	전화#:	소요시간:
요청사유 :			

의뢰 내용

지시사항

□ 조사요청서를 준비하시오.
□ 모든 요구 사항을 기술하시오.
□ 절차 연속성을 위한 문서를 첨부하시오.
□ 수사와 관련된 모든 개인 정보를 기입하시오.

LabCase #:	감정 수락 일시: 접수자:	Case 중요도: 1 2 3 4 5 선정인 :

번역 : 고려대학교 포렌식 연구실