법정에서의 디지털 증거:
법 집행과 검사를 위한 지침

서론

신기술의 발전과 확산이 그 기술을 사용할 때 지켜야 하는 사회 윤리 규범과 법률 시스템의 능력을 초과하는 경우가 종종 발생한다. 디지털 증거의 취급이 전형적인 예라 할 수 있다.

비록 컴퓨터가 60년 이상 존재해 왔지만, 기업, 가정, 정부 기관에서 급격히 증가한 것은 1980년대 후반이고, 그 때부터 디지털 증거가 범죄를 해결하고 범죄자를 기소하는데 사용되어왔다.

예를 들면, 수년간 아동 음란물 사건의 증거는 잡지나 전통적인 사진 형태로 발견되었다. 그런데 1990년대 중반에 인터넷으로 변화되었으며, 지금은 디지털 이미지 또는 이러한 이미지의 인쇄물이 아닌 다른 형태의 아동 음란물을 발견하는 경우는 거의 없다.

예전에는 해킹과 같은 "컴퓨터 범죄" 사건에서만 있던 디지털 증거가 현재는 모든 형태의 범죄에서 발견되고 있다. 그렇지만 법집행기관과 사법부는 디지털 증거 사용의 증가로 인해 발생되는 문제에 대처할 준비가 되어 있지 않은 경우가 많다.

일부 판사, 변호사, 배심원은 디지털 증거의 중요성과 신뢰성에 관해 강한 의구심을 가지고 있을 것이다. 재판에서 오해를 방지하기 위하여, 디지털 증거와 관련된 개념은 신중하게 선택한 비유나 시각적인 자료를 동원하여 평이한 용어로 설명해야만 한다.

검사는 수사관이 재판에서 야기되는 혼란의 회피 방법을 알고 있다고 생각하지 말아야 한다. 기술적으로 유능한 수사관이나 조사관은 검사가 증거의 복구와 분석 과정에서 직면하는 문제를 충분히 파악하고 있다고 생각하지 말아야 한다. 검사, 수사관, 조사관은 서로 기술적인 문제에 대한 지식을 공유하고 공판 전략에 대해 논의해야 한다.

법집행기관과 검사를 대상으로 하는 이 보고서는 몇몇 중요한 제약 사항이 있으며, 이 보고서는 오직 지침서일 뿐이다. 첫째로 디지털 증거와 관련된 핵심 논점의 일부를 파악하고 간단히 서술한다. 좀 더 심도 깊은 논의는 이 지침서의 참고문헌과 부록 A를 참조하기 바란다. 둘째로 여기서 논의한 많은 문제들은 재판관할권별로 다른 법률의 지배를 받는다. 세 번째로 이 분야의 법과 기술은 급속도로 발전하고 있다. 마지막으로 이 지침서는 미국 밖에서의 디지털 증거 획득에 대해서는 다루지 않는다.(범죄 수사관들과 검사는 국제 문제청, 미 법무부, 202-514-0000에 자문을 받아야 한다)

제 1 장 수색과 압수에 관한 사항

Ⅰ. 배경

범죄 사건에서 디지털 증거의 수집은 통신과 컴퓨터 산업을 규정하고 디지털 증거의 수집과 사용에 직접적으로 적용되는 법률을 포함하여 다수의 헌법과 법령 조항에 의해 연방이나 주 수준에서 적용된다. 또한 판례와 절차상의 규정도 고려해야 할 필요가 있다.

이 장에서는 국회가 특별 취급할 가치가 있다고 인정한 정보에 대한 접근과 공개에 적용되는 몇 개의 연방 법령에 대하여 논한다. 그것은 Wiretap Act, Pen Register and Trap and Trace Statute, Stored wire and Electronic Communication Act를 포함하는 Eelectronic Communication Privacy Act(ECPA)와 Privacy Protection Act이다. 또한 미국 수정 헌법 제 4조에 적용되는 원칙을 살펴볼 것이다. 이들 법령을 위반하면 증거력의 훼손이나 민사소송의 대상이 될 수 있기 때문에 수사관, 조사관, 검사는 이들 법령에 익숙해야 한다.(다른 연방법 조항과 주법은 이 지침서의 영역 밖이다.)

참고 사항: 수색과 압수 문제에 관한 연방법의 포괄적인 분석은 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)에서 찾을 수 있다.

Ⅱ. Wiretap Act

Wiretap Act는 통신하는 동안 통신 내용을 획득하는 것에 대해 중점적으로 다루고 있다. 통신 내용 획득의 예로는 전화 도청, 대화 내용을 엿듣기 위해 방안에 도청기를 설치하는 것, 해커의 인스턴트 메시지를 가로채는 “sniffer” 소프트웨어를 설치하는 것 등이 있다. Wiretap Act는 또한 가로챈 통신 내용의 공개에도 적용된다.

Wiretap Act은 미국에서 전화선이나 대화 또는 전자 통신의 내용을 가로채는 것을 광범위하게 금지하고 있다. 기본 규정으로 Wiretap Act는 몇 개의 예외조항이 적용되지 않는 한 “전기적, 기계적 또는 다른 장치”를 사용하여 통신에 참여한 사람의 대화 내용을 제 3자가 엿듣는 것을 금지하고 있다.

예외 조항으로 감청을 허가할 수 있는 관할 법원의 명령서 발급이 있다. 명령서 발급을 받기 위해서는 그럴만한 실질적인 가치가 있음을 제시하여야 한다.

Wiretap Act의 위반은 민형사 책임을 져야 할 수 있다. 전화 및 구두 대화의 경우에, 공무원의 Wiretap Act 위반은 증거로서 채택되지 않는 결과를 초래할 수 있다. 법령을 준수하기 위해 최초 결정은 다음 두 가지를 고려하여 내려져야만 한다.

■ 감청하는 통신이 법령에서 정의한 보호 대상 통신 중 하나이다.

■ 제안된 감시가 통신의 “가로채기”에 해당한다.

만약 두 조건에 해당하면, 법적 예외 조항이 감청을 허가하는데 적용될 수 있는지 판단하기 위해 평가가 이루어져야 한다.

참고 사항: 몇몇 주는 연방 법령보다 더 엄격한 Wiretap Act의 변형을 가지고 있다. 연방 공무원에 의해 조사가 수행되지 않는 한 연방 법령은 주법보다 우위에 있지 않다. 주와 지방 자치단체의 법집행기관은 연방의 Wiretap Act 위반이 아니어도, 반드시 해당 주법을 준수해야 한다.

U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005)에서는 고객에게 메시지가 전달되기 전까지 사업자의 램이나 하드 드라이브에 존재하는 이메일을 복사하여 배달해 주는 소프트웨어 사용이 포함되어 있는데, 법정에서 “‘전자 통신’에는 통신 과정에 있는 일시적으로 전자 저장된 데이터도 포함되며, 따라서 그러한 저장 형태인 이메일의 가로채기는 Wiretap Act을 위반한 것이라 판결했다.”

Ⅲ. Pen/Trap statute

Pen Register and Trap and Trace Statute(18 U.S.C. § 3121 et seq.)는 Pen/Trap statute로 알려져 있으며, 통신과 관계된 정보인 송신자 전화번호, 통신경로, 주소지, 수신자 전화번호를 실시간으로 획득할 때 적용되는 법률이다. Wiretap Act와는 다르게 Pen/Trap statute는 통신 내용의 획득에 대해서는 다루지 않으며, 통신에 관한 정보를 대상으로 한다. "pen register"는 외부로 나가는 정보를 기록하는 장치를 뜻하며, “trap and trace"는 내부로 들어오는 정보를 기록하는 장치를 말한다. 예를 들면, pen register는 감시 대상자가 전화를 건 상대방의 번호를 획득하며, 반면 trap-and-trace 장치는 감시 대상자에게 걸려온 상대방 전화번호를 획득한다.

Pen/Trap Statute는 전화와 인터넷 통신에 적용된다. 예를 들면 모든 이메일 통신에는 송신자와 수신자 정보가 있는데, Pen/Trap 장치는 실시간으로 이와 같은 정보를 갈무리한다.

이 법은 예외 조항이 적용되지 않는 한, 전화나 전자 통신 정보를 동의 없이 실시간으로 획득하는 것을 금하고 있다. 예외 조항이 적용되지 않을 때, 법 집행기관은 이 법에서 대상으로 하는 통신 정보를 획득하기 전에 반드시 법원으로부터 Pen/Trap 명령(order)을 받아야만 한다.

참고 사항: 연방의 pen/trap 명령 발급 요청서의 예는 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov /s&smanual2002.htm)에서 찾을 수 있다. 일부 주는 연방 법률보다 더 엄격한 독자적인 Pen/Trap 법을 가지고 있다. 연방 소속의 직원(agent)이 수사하는 경우가 아니라면 연방법이 주법에 우선하지 않는다. 주와 지방 자치단체의 법집행기관은 연방 Pen/Trap 법을 위반하지 않았더라도 반드시 해당 주의 법을 준수해야만 한다.

Ⅳ. Electronic Communications Privacy Act의 저장되어 있는 통신내용에 관한 조항

ECPA의 저장되어 있는 통신 내용에 관한 조항에서는 통신 서비스 사업자의 가입자와 고객의 프라이버시 보호를 규정하고 있다. 이 법은 사업자의 보관 기록물(예 : 과금 정보) 뿐만 아니라 고객이나 가입자를 위해 사업자가 저장하고 있는 파일(예 : 이메일, 업로드한 파일)도 보호한다. 사업자의 유형에 따라, ECPA는 법집행기관이 사업자로부터 고객이나 가입자의 정보를 받기 위해 필요한 법 절차의 유형을 지정하고 있다. 또한 ECPA는 연방, 주, 지방 자치단체를 포함하여 다른 사람에게 공개하는 것을 제한하고 있다. (ECPA의 공개 규정에 대해서는 appendix B를 참고하라.)

ECPA는 법집행기관이 통신 서비스 사업자(예 : 인터넷 서비스 제공자(ISP) 또는 휴대폰 사업자)로부터 고객이나 가입자에 관한 기록을 보려고 할 때 적용된다. 예를 들면, ECPA는 법집행기관이 ISP로부터 고객 이메일의 복사본을 얻으려고 할 때 적용된다. 반면에 법집행기관이 고객의 컴퓨터에서 동일한 이메일을 얻을 때에는 ECPA가 적용되지 않는다.

ECPA에서는 획득하고자 하는 정보 유형에 따라 필요한 법적 요구사항으로 소환장(subpoena), 섹션 2703(d) 하의 법원 명령(court order), 수색 영장(search warrant) 등으로 구분하고 있다. 일반적으로, 정보가 민감해질수록 (가입자 기본 정보보다는 거래정보가 더 민감하고, 통신 내용이 그 보다 더 민감함), 해당 정보를 획득하기 위한 법적 절차도 소환장, 법원명령, 수색영장 순으로 강화된다.

법적 요건이 소환장, 법원 명령, 수색 영장 순으로 강화됨에 따라, 하위 수준에서 획득할 수 있는 정보는 상위 수준에서도 당연히 포함된다. 예를 들면 수색 영장은 가입자의 기

본 정보, 통신 내역 정보 외에 저장되어 있는 통신 내용까지도 접근할 수 있는 권한을 부여한다.

참고 사항: 사업자들은 보유하고 있는 데이터 유형을 지칭하는데 각기 다른 용어를 사용하기 때문에, 가능한 쉽게 정보를 획득하려면 통용되는 용어에 대해 사업자 별로 의견을 들을 것을 권장한다.

A. 소환장: 가입자와 통신 내역

ECPA는 법집행기관이 서비스 사업자로부터 서비스 사업자와의 관계, 기본적인 통신 내역과 같은 고객이나 가입자의 신원에 관한 아래 정보를 획득하려면 소환장을 발부받아야 함을 규정하고 있다.

1. 이름.

2. 주소.

3. 시내와 시외 전화 통화 기록, 또는 통신 시간과 지속 시간에 관한 기록.

4. 시작 날짜를 포함한 서비스의 기간과 사용한 서비스의 유형.

5. 전화나 기계 번호, 또는 임시로 할당된 네트워크 주소와 같은 가입자의 번호 또는 신원.

6. 신용 카드나 은행 계좌 번호와 같은 서비스 사용료의 출처와 수단.

이러한 내역에는 고객과 통신한 사람의 이메일 주소가 드러나는 로깅 정보 또는 친구 목록(buddy lists)과 같이 통신에 관련된 광범위한 기록이 포함되어 있지 않음에 주목하기 바란다.

B. 2703(d)하의 법원 명령: 기타 통신 내용이 아닌 세션 정보

법집행기관이 사업자로부터 다음과 같은 고객이나 가입자의 서비스 사용에 관한 자세한 기록을 획득하려면 18 U.S.C. § 2703(d) 하의 법원 명령을 발부받아야 한다.

1. 가입자가 장기간 방문한 IP 주소를 나타내는 계정 활동 로그.

2. 가입자가 송수신한 다른 사람의 이메일 주소.

3. 친구 목록.

법집행기관은 이동전화 사업자로부터 총 통화시간, 실시간으로 가입자의 휴대폰이 있는 셀에 대한 위치 정보를 보여주는 기록을 얻기 위해 2703(d) 명령을 사용할 수 있다. 이러한 기록은 소환장을 통해서 얻을 수 있는 정보 보다 훨씬 많이 가입자의 시스템 사용에 관한 정보를 제공하지만, 통신의 내용은 포함하지 않는다.

2703(d) 명령은 연방 치안 판사나 수사 대상자의 관할 지방 법원이 발부할 수 있다. 주법에 의해 pen/trap 장치의 사용을 인가하는 명령을 발부할 수 있도록 승인된 주 법원 판사도 2703(d) 명령을 발부할 수 있다. 명령 발부 신청서에는 "얻고자 하는 기록이나 다른 정보가 진행 중인 범죄 수사에 관계가 있고 중요하다고 ..... 믿을 수 있는 합리적인 근거를 보여주는 상세하고 명확한 사실"을 반드시 적시해야만 한다.

참고 사항: 일반적으로 ECPA는 가입자의 신원이나 서비스 사용에 대한 자세한 기록보다는 통신의 내용과 사업자가 저장하고 있는 파일에 대한 프라이버시 보호에 역점을 두고 있다. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations(www.cybercrime.gov/s&smanual2002.htm)은 2703(d) 하의 명령 발급 요청서의 예를 보여주고 있다.

C. 저장되어 있는 통신 내용

ECPA는 고객이나 가입자가 열람한 통신 내용과 열람하지 않은 것을 구별한다. 또한 열람한 통신 내용도 사설 사업자(예 : 직원이나 계약자에게만 제공하는 이메일 서비스 운영주)가 보유한 것과 공공에 서비스를 제공하는 사업자가 보유한 것을 구별한다.

1. 소환장: 사설 사업자가 보유 중인 열람한 통신 내용

ECPA는 서비스 사업자가 이러한 서비스를 공공에 제공할 경우, 고객이나 가입자가 이미 열람했지만 공공 서비스 사업자의 서버에는 남아 있는 통신 내용에만 적용된다.(Ⅳ.C.2 절 참조) 만약 사업자가 이와 같은 서비스를 공공에 제공하지 않는다면 임의로 그러한 정보를 공개하는 사업자의 권리에 대하여 ECPA에 의해 부과된 제약 사항은 없다.

ECPA는 그러한 기록의 공개를 강제하기 위한 특별한 법적 절차나 어떤 주의사항도 요구하지 않는다. 예를 들면, 만약 고용주가 이메일과 계정을 공공이 아닌 고용자에게 제공한다면, 특정 직원이 열람한 이메일을 획득하기 위해 고용자를 강제하는 정부 요청에 대해서는 ECPA가 적용되지 않는다. ECPA가 적용되지 않는 곳에서 그러한 정보를 획득하려면, 전통적인 법적 절차가 유용할 것이다.

참고 사항: 만약 이메일이 고용주의 서버에 남아있고 아직 고용자가 열람하지 않았다면 ECPA가 적용된다. 이러한 사례는 Ⅳ.C.3절에서 논의한다.

2. 통지가 있는 소환장이나 2703(d) 명령: 열람한 통신 내용, 180일 이상 열람하지 않은 통신 내용, 공공 사업자가 보유하고 있는 기타 파일

사업자가 대중에게 서비스를 제공하는 경우, 고객이나 가입자가 열람하였지만 사업자의 통신 서비스 서버에 남아 있는 통신 내용은 ECPA의 적용을 받는다. 이러한 통신 내용에는 고객이 공공 사업자의 시스템 상에 저장한 문서 파일, 사진, 프로그램을 포함한다. ECPA 하에서 이와 같은 사업자는 "원격 컴퓨팅 서비스"로 간주되며 정부에게 통신 내용을 자발적으로 공개하는 것은 금지되어 있다.

법집행기관이 공공 서비스 사업자에게 고객이나 가입자가 열람한 저장되어 있는 통신 내용의 공개를 강제하려면 소환장이나 2703(d) 법원 명령을 발부받아야 한다. 그러나 두 경우 모두 법집행기관은 고객이나 가입자에게 사전에 그러한 요청이 있음을 반드시 통지해야 한다.

ECPA의 다른 규정에서 진행 중인 수사를 위태롭게 하거나 개인의 생명 또는 물리적 안전이 위험해 질 경우, 법집행기관이 고객이나 가입자에게 통지하는 것을 연기할 수 있도록 허용하고 있다. 만약 공공 서비스 사업자에게 열람한 통신 내용의 공개를 강제하는데 소환장을 사용했다면, "소환장의 존재에 대한 통지가 해로운 결과를 초래할 수 있다고 믿을만한 이유가 있음을 관리자의 서명 인증으로 실행되었다는 조건하에서" 법집행기관은 90일 동안 통지를 지연할 수 있다. 만약 2703(d) 명령을 사용했다면, 법집행기관은 명령 요청서의 일부에 통지 지연의 허용을 법원에 요청할 수 있다.

통지 지연 기간이 종료되면, 법집행기관은 반드시 고객이나 가입자에게 통지 지연 이유를 설명하는 서한과 함께 요청서나 진행 과정의 복사본을 반드시 보내야 한다.

또한 법집행기관은 180일 이상 열람되지 않은 채로 서버 상에 남아있는 통신 내용의 공개를 서비스 사업자에게 강제하기 위해 사전 통지가 있는 2703(d) 명령이나 소환장을 사용할 수 있다. 그런데 현실적으로 대부분의 사업자는 열람하지 않은 메시지가 그렇게 오랜 기간 동안 서버에 접근되지 않은 상태로 남아있는 것을 허용하지 않는다.

만약 법집행기관이 수색영장을 사용하거나 통신 내용이 아닌 부가 정보를 찾는다면, 사전 통지가 필요 없다.

참고 사항: Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir.2004)에서, 법원은 고객에게 배달된 후에 ISP 서버에 남아있는 이메일의 복사본은 배달 중인 이메일과 동일하게 ECPA의 보호를 받는다고 판시하였다.

---

3. 수색 영장: 열람하지 않은 통신 내용

음성 메일을 포함하여 180일 이내의 열람되지 않은 통신 내용은 ECPA 하에서 최상

의 보호를 받는다. ECPA는 서비스 사업자가 사설인지 공공인지 상관없이 그러한 통신 내용을 보호한다. 서비스 사업자가 정부에게 열람되지 않은 통신 내용을 자발적으로 공개하는 것은 일반적으로 허용되지 않는다.

예를 들면, ECPA 하에서는 고객에게 보내진 이메일이 고객의 사업자(ISP 또는 고객의 고용주) 서버에 남아 있지만, 고객이 아직 로그인 하지 않았거나 메시지에 접근하지 않았다면 열람되지 않은 것으로 간주한다. 고객이 이메일에 접근했으나 사업자의 서버에 복사본이 남아 있다면 열람한 것으로 판단한다. (1장 Ⅳ.C.1절은 열람된 통신 내용에 대한 좀 더 자세한 지침을 다루고 있다.)

법집행기관이 열람되지 않은 통신내용의 공개를 서비스 사업자에게 강제하려면 2703(a)에 의거한 수색영장을 청구해야 한다. 이 경우, 고객이나 가입자에게 사전 통지할 필요가 없다.

참고 사항: 사설 사업자는 가입자와 세션 정보, 거래 정보, 저장되어 있는 통신 내용과 파일을 정부나 제삼자에게 자발적으로 공개하여도 ECPA의 위반이 아닐 수 있다. 특정 경우에는 공공 사업자가 자발적으로 정보를 공개하여도 ECPA의 위반이 아닐 수 있다. 연방 법보다 더 엄격한 법을 적용하는 주들도 있다. 연방 직원(agent)이 수사를 하지 않는다면 연방 법이 주 법에 우선하지 않는다. 주나 지방 자치단체의 법집행기관은 연방 법을 위반하지 않는다고 하여도 반드시 소속 주 법을 준수해야 한다.

D. 민사 손해 배상

ECPA의 비헌법적인 위반으로 인한 구제 수단으로 민사 손해 배상이 있다. ECPA를 위반하여 압수된 증거는 폐기되지 않는다.

Ⅴ. 프라이버시 보호법(Privacy Protection Act)

프라이버시 보호법(PPA)(42 U.S.C § 2000aa et seq.)은 언론 공개를 위해 소유하고 있는 자료의 수색이나 압수하려는 법집행기관의 수색 영장 사용을 제한하고 있다. 보호 대상 자료는 “작업 결과물”(저자나 출판사가 작성한 자료)과 “보조 자료”(작업 결과물을 생성하기 위해 사용한 모든 자료)이다.

예를 들면, 온라인 신문을 제작하는 사람이 보유한 인터뷰 노트는 “보조 자료”로 간주되며, 출판된 신문 기사는 “작업 결과물”로 간주된다.

만약 해당 자료가 PPA의 보호 대상이라면, 법집행기관은 그것을 획득하기 위하여 수색영장을 사용할 수 없다.

다음의 경우에는 PPA의 수색 영장 사용 금지조항이 적용되지 않는다.

■ 수색 또는 압수할 자료가 범죄의 수단 또는 결과물이거나 금지품이다.

■ 그러한 자료의 즉각적인 압수가 죽음이나 심각한 상해를 막기 위해 필요하다는 것을 믿을만한 이유가 있어야 한다.

■ 그러한 자료를 소유한 자가 그 자료와 관련하여 범죄를 저질렀거나 저지르고 있다고 믿을만한 합리적인 근거가 있어야 한다.(정부의 특정 정보나 아동 음란물을 소유한 것을 제외한다면, 자료 보유만으로는 범죄를 구성하여 이 예외 조항이 적용되는 경우는 없다.)

만약 범죄 증거가 PPA 보호 대상 자료가 있는 컴퓨터 상에 뒤섞여 있다면, 수색 영장의 적정 범위와 실행에 관한 문제가 발생할 것이다. 최근 사건에서 법원은 PPA 보호 영역을 범죄 혐의가 없는 자로 한정한다고 볼 수 있다. PPA 만 위반하여 압수된 증거는 폐기되지 않을 것이다.

PPA의 위반에 대한 배타적 구제 방법으로 민사 손해 배상이 있다.

참고 사항: 프라이버시 보호법에 관한 더 많은 정보를 원하면 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)를 참조하라.)

Ⅵ. 헌법적인 문제

다른 형태의 증거 수색처럼 디지털 증거에 대한 수색도 연방과 주 헌법의 수색과 압수에 관한 법과 법원 규칙이 적용된다. 봉인된 용기에 있는 것에 대한 전통적인 수정 헌법 제 4 조의 원칙이 디지털 증거에 적용된다.

A. 수정 헌법 제 4 조의 적용

수정 헌법 제 4 조는 무분별한 수색과 압수로부터 개인을 보호한다. 수정 헌법 제 4 조의 보호물에 적용하려면 두 개의 핵심 요건을 고려해야 한다.

■ 정부의 활동과 연관되었는가?

■ 영향을 받는 자가 수색되는 장소나 압수되는 것에 대해 프라이버시의 합당한 기대를 가질 수 있는가?

1. 정부의 활동

대부분의 상황에서 정부의 활동은 정부 직원이 수색하였을 때를 의미한다. 일반적으로 말하면, 수정 헌법 제 4 조의 제한은 정부의 지시에 의하여 수행되지 않는 한, 민간인에 의한 수색에는 적용되지 않는다. 범죄의 증거를 독립적으로 획득한 민간인은 그것을 법집행기관에 제공할 것이다.(법집행기관은 민간인의 수색을 되풀이 할 수 있으나, 그 이상의 수색은 영장이 있어야만 할 수 있다.)

예를 들면, 만약 종업원이 가게에서 수리 중인 컴퓨터에서 금지 파일을 발견하여 법집행기관에 그 정보를 제공한 것은 수정 헌법 제 4 조를 위반한 것이 아니다. 이러한 경우 법집행기관은 종업원이 발견한 것은 무엇이든 조사할 수 있다.

2. 프라이버시의 합당한 기대

수정 헌법 제 4 조는 수색 받는 자가 수색되는 장소나 압수되는 물건에 대해 프라이버시가 보호되고 있다는 실질적인 기대를 할 수 있으며, 그것이 사회에서 합당하다고 인정할만하다고 판단될 때 적용된다.

일부 법원은 컴퓨터를 수정 헌법 제 4 조의 목적을 위한 “봉인된 용기"로 취급한다. 일부 사법 지역에서는 컴퓨터의 하위 디렉토리와 파일의 열람을 봉인된 용기의 개봉과 유사한 것으로 본다.

B. 수정 헌법 제 4 조의 요구 사항 충족

만약 수정 헌법 제 4 조의 수색에 관한 문제와 관련되었다면, 일반적으로 법집행기관은 영장 요건의 예외 사항이 적용되지 않는 한 반드시 영장을 발부받아야 한다.

1. 영장 없는 수색

영장 확보가 필요 없는 잘 알려진 예외가 몇 개 있다. 비록 아래에 있는 것이 모든 경우를 다 열거하는 것은 아니지만, 디지털 증거의 수색과 압수에 적용될 수 있는 공통적인 예외 사항의 예이다.

a. 동의

동의는 수사관에게 효과적인 도구이다. 이것은 로그인 배너, 사용 조건 계약서, 회사 정책 등을 포함하여 많은 곳에서 찾아볼 수 있다. .

(1) 공동으로 사용하는 아파트에서, 한 컴퓨터를 여러 사람이 사용할 수 있다. 한 사용자로부터 동의를 받으면, 컴퓨터에서 그 사람의 개인 영역에 대한 수색은 정당하고, 대부분의 경우 공통으로 사용하는 영역에 대한 수색도 정당하다.

조사관이 패스워드로 보호되는 파일을 열람하려면 추가적인 동의가 필요하다. 또한 대부분의 경우에 부모는 미성년 자녀의 컴퓨터를 수색하는데 동의할 수 있다.

(2) 동의는 당면 문제, 기간, 다른 요소에 의해 제한될 수 있다. 동의는 언제든 철회될 수 있다. (동의서 양식의 예는 appendix C를 참조)

(3) 민간 사업자가 종업원의 작업 컴퓨터에 대한 수색에 동의할 수 있다는 것이 일반적인 규정이다. 이 규정은 고용주가 정부일 때 좀 더 복잡해진다.

참고 사항: 동의 규정에 관해 더 많은 정보를 원한다면 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)를 참고하라.

---

b. 위급 상황

증거의 파괴를 막기 위해 법집행기관은 전자 저장 기기를 압수할 수 있다. 데이터를 손실할 급박한 위험이 있는 경우에, 법집행기관은 그 상황에서 데이터를 보존하기 위한 제한적인 수색을 수행할 수 있다. 위급 상황이 종료되면, 예외 사항도 적용되지 않는다.

c. 체포 상황의 수색

법집행기관의 안전 또는 증거 보존을 위해 체포된 사람에 대한 전면 수색과 체포 현장의 제한적인 수색은 정당화 될 수 있다. 이러한 체포 상황의 수색은 무선 수신 호출기나 휴대폰 같은 체포 대상자가 보유한 전자 저장 기기의 수색을 포함한다.

참고 사항: 비록 체포 상황의 수색이 용의자로부터 발견된 전자 저장 기기의 수색을 허용하지만, 법집행기관의 직원은 증거의 무결성이 유지되도록 주의해야 한다.

---

d. 보관물품 수색

보관물품의 수색에 대한 예외 조항은 수감된 자의 재산을 보호하고 손상이나 분실에 따른 배상을 방지할 의도로 제정되었다. 이러한 예외조항은 법정에서 실제로 다루어지지 않았다. 그래서 보관물품 수색의 예외조항이 법집행기관의 영장 없는 디지털 증거의 접근에 적용될 수 있는지 불확실하다.

e. Plain view doctrine

Plain view doctrine은 전자 증거의 수색과 압수에 관한 몇몇 사례에 적용될 수

있다. Plain view를 적용하려면, 법집행기관은 합법적으로 증거를 관찰할 수 있는 위치에 있어야 하고, 범죄 발생이 명백해야만 한다. 법집행기관의 직원은 디지털 매체에 관한 plain view를 적용할 때, 관할 지역에 따라 다른 형태의 plain view를 준수하도록 조심스럽게 실행해야만 한다.

2. 영장에 준한 수색 및 압수

만약 수정 헌법 제 4 조의 수색에 해당되고 수색 영장이 없어도 되는 예외 조항이 적용되지 않는다면, 법집행기관은 반드시 수색영장을 발부받아야 한다. 일반적으로 다른 수사와 마찬가지로 디지털 증거에 대한 수색 영장의 준비와 집행할 때에도 동일한 영장 규칙이 적용된다. 법집행기관은 전자 증거에 대한 수색 영장의 준비와 집행할 때 다음을 고려해야 한다.

a. 수색 대상 설명

만약 찾고자 하는 증거가 컴퓨터 그 자체(하드웨어가 범죄의 수단, 범죄 결과, 또는 금지품인 경우)이면, 영장은 수색의 목표로서 컴퓨터를 언급해야 한다.

만약 찾고자 하는 증거가 디지털 매체에 저장된 정보이면, 영장은 증거가 무엇인지 설명하고, 저장 형태에 관계없이 압수할 권한을 요청해야 한다. 여기에는 증거를 검색하기 위하여 저장매체를 제어하고 소유할 수 있는 권한의 요청도 포함된다. 검색 범위를 지나치게 제한하는 영장 요청은 피하라.

참고 사항: 영장요청서 문구의 예는 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)를 참조하라.

---

b. 수색 시행

일부 사건의 경우, 전자 저장 기기의 수색은 상당한 기술적 지식을 요할 수 있기 때문에, 수색이 영장의 범위임을 알 수 있게 영장의 복사본을 지참한 적정한 인력이 집행해야 한다.

수색하는 도중, 법집행기관은 시스템이나 데이터에 접근할 수 있게 해주는 키와 패스워드를 발견하는 경우가 있다. 또한 법집행기관은 수색 영장의 범위 밖에서 범죄의 증거를 발견할 수 있다. 이러한 경우, 수색의 범위를 확장하는 별도의 영장 발부를 고려하라.

좀 더 심도 깊은 논의는 2장을 참조하라.

참고 사항: 증거 수집에 관한 문제를 보려면, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)를 참조하라.

a. 합당한 조정

어떤 사건에서는 현장에서 장치를 수색하기 어려울 수 있다. 만약 장치를 다른 곳에서 수색하려면, 법집행기관은 그것의 이동을 정당화시키는 진술서를 영장에 추가할 것을 고려해야 한다.

만약 장치가 수색을 위해 현장 밖으로 이동되었다면, 수색은 알맞은 방법으로 완료되어야 한다. 법집행기관은 용의자나 제 삼자의 합리적 요청을 수용하기 위하여 금지품이 아닌 압수된 데이터, 심지어 범죄 증거와 뒤섞여 있을지라도, 복사본으로 반환할 것을 고려해야 한다.

좀 더 심도 깊은 검토는 2장을 참조하라.

Ⅶ. 특권 또는 지적재산 정보

어떤 경우, 법집행기관은 수색되는 장소에 일반법이나 법률에 특권이 부여된 정보가 포함되어 있을 것으로 예측할 수 있다.(예 : 변호사 사무소, 의료 기관, 성직자) 영장을 제출하고 수색하기 전에, 법집행기관은 관할 지역에 부과된 법적 한계를 파악하고 준수하는지 주의해야 한다. 법집행기관은 다음과 같은 방식으로 해결할 수 있다.

- taint team이나 special master의 사용이나 법원이 인정한 다른 절차를 고려하라.
- 압수되는 매체가 특권 또는 지적재산 정보를 포함하는지에 대해 우선적으로 고려하라.
- 잠재적인 특권 또는 지적재산 정보의 몰수를 피하기 위해 대상으로부터 정보를 압수하기 전에 약정 획득을 고려하라.(appendix D를 보라. “Stipulation Regarding Evidence Returned to the Defendant"에 대한 예)
- taint team에 의한 증거 획득을 피하려면, 수색 영장을 요청할 때 기소팀이 특권 또는 지적 재산 정보에 대한 문제를 취급할 수 있는 지 확인하라.

Ⅷ. 다른 주의 기록물 획득

A. 문제점

종종 주나 지방 자치단체 법집행기관이 획득하기 원하는 기록물을 가지고 있는 ISP가 관할 주가 아닌 경우가 있다. 물론 관할하는 주에 물리적으로 존재하는 타주 실체에 대해서는 서비스를 처리하는 지역 사업 대표나 지정 대리인으로부터 기록물에 대한 관할권을 획득할 수 있다. 외국 사업 실체나 기업으로 등록되어 있으나, 관할하는 주 내에 물리적 실체가 없는 다른 주의 실체에 대해서는 서비스 처리를 위임받은 대리인에게 충분히 관할권을 획득할 수 있을 것이다.

다른 경우, 타주의 제 삼자로부터 증거를 획득하는 데는 다음 두 가지 문제점이 있다.

1. 해당 주의 법은 소환장, 18 U.S.C. 2703(d) 명령, 수색 영장과 같은 강제 집행을 할 수 있는 곳을 해당 주의 영역으로 한정할 것이다. 관할 지역을 제한하는 명확한 법이 없어도, 판사는 관할 지역을 초과하는 집행 영장 발행을 거부할 것이다.

2. 타주의 증거 보유자는 증거가 위치한 주의 외부에서 발행된 집행 영장을 존중하지 않을 것이다. 아주 소수의 주에서만 타주에서 발행된 집행 영장도 자기 주 안에서 발행된 것처럼 자신의 관할 지역 안의 실체가 준수하도록 요구하고 있다. 그래서 집행 영장을 획득할 수 있어도, 종종 타주의 실체는 준수해야 할 법적 의무가 없는 것으로 여긴다. 보통 이와 같은 거부는 ECPA(또는 은행의 경우 Federal and State bank privacy laws) 하의 책임에 대한 두려움 때문이다. 다시 말하면 만약 영장이 합법적인 구속력이 없다면, 공개로 인한 책임으로부터 회사를 보호할 수 없기 때문이다. 그러나 다른 사례에서 이것은 “할 필요가 없다면 하지 않겠다”는 태도로 나타난다.

참고사항: 타주에서 발행된 집행 영장을 자기 주에서 발행된 것과 같이 준수하도록 자기 주 안의 실체에게 요구하는 주는 소수이다.

B. 현재의 선택 방안

타주의 기록물을 획득하기 위한 현재의 선택 방안에 대한 다음의 논의에서, 타주의 기록물을 획득하는 주 절차의 사용이 무효라 하여도 미국 헌법 하에는 증거 폐기 방법이 없음을 명심하라. 부적절하게 압수된 ISP 기록물에 대한 유일한 연방 대책은 ECPA 하의 규정인데, 여기에도 위헌적인 위반 행위에도 폐기하는 방법은 없다. 그러나 주 헌법 또는 법률 규정에 폐기 대책이 있을 수 있다. 다음에서 언급하는 것이 선택 방안이다.

1. 법원 설득

   해당 주에서 주 영역을 넘어서는 집행 영장 발급에 대한 특별한 금지가 없다면, 검찰은 그 지역에 대한 집행 영장을 발행하도록 법원을 설득할 것이다.

a. 그러한 집행 영장의 발행에 대한 특별한 금지가 없다.

b. 수색 영장이 합법적으로 소환장처럼 집행할 수 있도록 인식된 주 판례가 있다.

c. 만약 영장이 합리적인 근거에 의해 소환장처럼 고려할 수 있다면, 자기 주 법원이 타주의 치안 관리인을 지휘할 수 있는지에 대한 문제는 타주의 치안 관리인을 참여시키지 않음으로서 발생하지 않는다.

d. 일부 비평가가 언급한 것처럼, 지방 법원이 타주의 목격자에게 재판 참석을 강제하는 사법권을 가지는 것과 적어도 동일한 정도로 타주에 있는 증거의 획득을 강제하는 사법권이 있다.

타주의 기록물에 대해 영장을 발행하는 법원 권한에 대한 정당성의 확보는 타주의 기록 보유자에서 해당 주의 영장을 송달하거나 팩스를 보내 수색을 수행하라고 법집행기관에 판사가 명령하는 것이다.

2. 증거 보유자 설득

관할 지역을 넘는 수색 영장을 정당하게 발급받은 직원은 영장 수용을 꺼리는 타주의 증거 보유자를 설득할 수 있다. 영장을 발부한 판사를 확신시킨 법집행기관의 동일한 주장을 사용함으로써, 증거 보유자의 납득을 시도할 수 있다. (a) ECPA는 합법적인 수색 영장에 응하여 기록의 생산을 요구하고 있다. (b) 직원은 합법적인 수색 영장을 가지고 있다. 선의의 믿음을 가진 실체는 ECPA에 의거 진행되는 민사 또는 형사 소송에 대해 완벽한 방어를 할 수 있다고 설명할 것이다.

3. 다른 선택 방안에 대한 고려

만약 부장 판사가 관할 지역 밖에 대한 수색 영장 발부를 거부하거나 수령인이 영장 집행을 거절한다면, 법집행기관은 다음과 같은 다른 방안을 고려해야 할 것이다.

a. 재판 소환장.(만약 고발되었다면)

b. 관할 지역이 없는 대배심 또는 수사 소환장

c. Uniform Act to Secure the Attendance of Witnesses From Without a State in Criminal Proceedings(이후론 "Uniform Act"라고 하겠음.)와 같이 함께 사용된 재판 또는 대배심 소환장

소환장은 영장을 집행할 수 없을 때 적용할 수 있다. 대부분의 주는 소환장의 관할 지역을 제한하는 법이 없다. (그리고 Uniform Act의 경우, 이 법을 채용한 주는 타주

의 거주자에게 소환장을 발부할 묵시적 또는 명시적 사법권을 주장한다.)

그러나 소환장의 성공적인 사용은 획득하려는 기록이 ECPA 하에서 D-order 또는 수색 영장과는 달리 소환장에 의해 얻을 수 있는지에 달려 있다.

공판 소환장 또는 대배심 소환장 역시 수색 영장에 대해 수령인이 응하지 않는 것과 같은 문제를 일으킬 수 있다.

Uniform Act는 법의 위력을 충분히 발휘하는 장점이 있다. 판사는 이 법에 의거하여 소환장을 발부할 권한이 있고, 수령인은 반드시 응해야 한다. 그러나 소송 절차는 귀찮고 시간이 많이 소요되며, 재판이 진행되어야 문서를 획득할 수 있다.

4. 영장의 "귀화"

유효하고 집행할 수 있는 영장을 받는 효과적인 방법은 진술서를 준비하여 타 주의 법집행기관에 보내고, 그 주의 법집행기관이 자체적으로 수색 영장을 받도록 그 주의 진술서로 사용하도록 하는 것이다.

이러한 절차를 사용하는 데는 몇 가지 단점이 있다.

- 이것은 타주에 있는 법집행기관의 협조에 달려있다.
- 두 법집행기관의 참여를 요구하기 때문에 부담이 된다.
- 증거를 찾고자 하는 주는 수색이 필요하다는 합리적인 근거에 대해 타 법집행기관의 동의를 받아야 한다.

C. 연방 법률 제정의 제안

형사 사건에서 주 법원이 발행한 제출 명령에 대해 완전한 믿음과 신용을 부여할 것을 각 주에게 요구하는 연방 법률의 제정이 제안되었다. 만약 법률이 제정된다면, 이 법은 타주의 증거 보유자에게 완전히 집행할 수 있는 제출 명령의 발행을 주에 허락하는 국가적인 시스템의 출발점이 된다. 이 법률과 다른 법률 제정에 대한 정보를 얻으려면 www.ecpi-us.org를 방문하라.

그 동안 일부 주는 주 내에 등록되어 있는 타주의 회사에 주내의 소송 절차 서비스를 수용하도록 대리인의 지명을 요구하고, 주내에 설립된 회사에 타주의 법정 절차를 수용하도록 요구하는 방식을 채용했다.

제 2 장 디지털 증거의 무결성, 개시, 공개

조사 전반에 걸친 디지털 증거의 무결성 유지는 전통적인 물리적 또는 문서 증거를 다룰 때 마주치는 것과는 다른 문제가 나타난다. 일부 공통되는 문제는 컴퓨터 망의 복잡성에 의해 더욱 악화된다. 이 지침서는 네트워크 환경으로 인해 초래된 고유의 문제를 다루지 않으며, 단독 사용의 전자 매체로부터 추출된 정보의 무결성을 유지하는 문제를 집중적으로 다룬다.(네트워크 포렌식에 관련된 문헌 목록은 appendix A를 참조하라.)

이 지침서는 압수된 매체에 사건 관련 정보가 있고, 압수된 이후로 매체에 시행된 포렌식 조사가 증거를 변경시키지 않았다고 가정한다. 압수 후의 전통적인 절차연속성의 유지가 필요하지만, 포렌식 조사로부터 획득된 데이터나 증거의 신뢰성을 수립하기엔 충분하지 않다. 절차 연속성(chain of custody)에 추가하여 디지털 증거를 취급하기 위해서는 보조적인 예방 조치가 요구된다.

이 지침서는 전자 기기나 매체로부터 디지털 증거를 복구하는데 포렌식 사회에서 인정받은 도구가 사용되었다고 가정한다. 왜냐하면 데이터를 획득하는데 사용된 절차도 그 자체가 전자적이며, 따라서 증거와 절차 둘 다 법적인 논란이 일어날 수 있기 때문이다. 기계, 응용프로그램, 포렌식 도구를 인증받기 위해 추가적인 전문가 의견이 요구될 수 있다. 제 3장은 이 문제를 상세하게 다룬다.

참고사항: 컴퓨터 포렌식 도구의 정확성을 보증하기 위해 계획된 시험 결과를 보려면 NIJ's Computer Forensic ToolTesting Project Web site (www.ojp.usdoj.gov/nij/topics/ecrime/cftt.htm)를 참조하라.

Ⅰ. 예비 조사

일부 사건의 경우, 디지털 증거가 법집행기관에 확보되기 전에 고의 혹은 우연히 변경될 수 있다. 이것은 법집행기관이 참여하기 전에, 피해자가 범죄를 발견하거나 조사하는 경우에 많이 일어난다. 이 경우 조사를 위해 검찰에 제출된 증거는 절차연속성과 신뢰성을 확보하지 못하면 사용할 수 없게 된다.

참고 사항: 증거를 평가할 때, 컴퓨터가 없는 범죄를 포함하여 범죄 요건을 파악하기 위해 관할 지역의 규정을 참조하라. 만약 사건이 재판까지 간다면, 입증해야만 하는 요소의 점검표를 만들어라. 컴퓨터가 포함된 범죄의 특정 유형에 대한 간단한 질의에 대해서는 이 시리즈의 다른 NIJ 지침서를 참고하라.

증거를 제공하는 사람들에게 물어볼 필요가 있는 질문의 예로 다음과 같은 것이 있다.

■ 모르는 침입자가 범죄를 저질렀거나 또는 부여된 권한을 넘어서 기계나 데이터에 접근한 알려진 사용자를 가리키는 증거는 무엇인가?

■ 데이터를 접근하거나 변경한 시간의 순서가 어찌되는가?

■ 예상되는 피해는 무엇인가?

■ 사건에 책임이 있는 자가 누구인가?

■ 그 사람을 의심하는 이유는 무엇인가?

■ 사업에 영향 받는 것은 무엇인가?

■ 컴퓨터와 시스템이 사업을 운영하는데 필요한가?

■ 사건이 처음 발생한 시간은 언제인가?

■ 언제 사건을 처음 발견했는가?

■ 누가 사건을 조사했는가?

■ 장치에 있는 데이터를 확인, 수집, 보존, 분석하기 위하여 취해진 행동은 무엇인가?

이러한 예비 질의는 사건에서 도출된 증거의 필요한 근거를 검사에게 제공할 것이다. 정보가 증거로 인정되면, 증거의 일치성에 무게 중심이 이동할 것이다. 증거 인정은 첫 번째 장애일 뿐이다. 증거에 대한 신뢰성과 설득력은 사실인정자(trier of fact)에 의해 평가되어야만 할 것이다.

Ⅱ. 데이터의 무결성

디지털 증거의 인정과 설득력이 있기 위하여, 검사는 매체로부터 얻어진 정보가 시민, 피해자, 법집행기관 중 누구로부터 획득되었는지에 관계없이 진실이며, 매체에 있던 원래의 데이터를 정확하게 나타낸다는 것을 법정에서 보여야만 한다.

A. 절차 연속성(chain of custody)

절차 연속성은 물리적인 물품 그 자체와 그것에 관련된 데이터에 관한 것이다. 데이터에 관한 절차 연속성은 물리적 물품에 관한 절차 연속성에 추가돼야 함을 인식하라.

인정된 표준과 포렌식 연구실의 정책, 절차, 기타 지침 등 일반 증거와 전자 증거 둘 다에 대한 절차 연속성 관련 모든 것을 알아야 한다. 준수했는지 또는 일탈이 있었는지 판단하라. 일탈로 인하여 사건 조사에 미치는 영향을 이해하고 그것을 설명할 준비를 하라. 또한 정책, 절차, 기타 지침들이 유동적임을 인지하라. 검찰은 조사가 실행되던 시기에 적용한 방식을 반드시 알아야 한다.

B. 증거 획득과 조사 과정

피해 회사의 직원(예 : 정보 기술 또는 보안 담당 직원)은 법집행기관에 제공하거나 제공할 모든 디지털 증거의 사전 처리에 관련된 일련의 질문을 받아야 한다. 기소 준비나 공판 전략 수립 전에 답변을 듣고 기록하는데 충분한 시간이 주어져야 한다.

그러나 잠재적인 디지털 증거를 취급하였거나 취급한 것으로 생각되는 민간인과 법집행기관 사이에 의도하지 않은 대리인 관계가 성립되지 않도록 주의해야 한다.

이러한 문제에 대해 질의하면, 법집행기관이 사건 조사를 하게 될 때 적정한 디지털 증거 수집을 보장해주는 장점이 있다. 만약 정보를 획득하는데 사용된 초기 절차가 규범에 미치지 못하지만 원래의 매체에 남아 있으면, 법집행기관은 직접 수집할 수 없어도 증거의 구성 요건이 되도록 할 수 있을 것이다.

전통적인 절차 연속성 절차를 지키기 위해, 사건을 조사하는 법집행기관은 도착하기 전에 증거가 어떻게 취급되었는지 알아보기 위하여 다음과 같은 질문을 해야 한다.

1. 법집행기관이 참여하기 전에 수집된 증거의 유형은 무엇인가? 예를 들면, 사이버 스토킹의 경우, 이메일의 인쇄물이 있는가? 전자적인 복사가 가능한가? 헤더 정보가 모두 포함되어 있는가?

2. 증거를 다룬 사람은 누구인가?

    a. 증거를 취급한 사람의 이름과 직무를 기록하라. 증거를 다룬 사람이 한 사람 이상일 수 있음을 명심해야 한다.

    b. 디지털 증거가 조사되면서부터 법집행기관에 제공되기 전까지 그것을 통제한 모든 사람의 신원을 확인하라.

3. 어떻게 디지털 증거를 수집하고 저장했는가?

    a. 디지털 증거를 수집하기 위해 사용한 모든 도구나 방법을 확인하라.

    b. 디지털 증거가 수집되고 난 후에 접근한 사람을 파악하라. 증거에 접근한 모든 자는 절차 연속성의 부분으로 고려해야 한다. 저장된 모든 데이터에 설명을 달아 기

록하라.

4. 증거가 수집된 시기는 언제인가? 수집된 일시를 기록하라. (만약 필요하다면 시간대도 기록) 상세한 기록은 재판의 시작과 설명과정에서 검사와 검찰 측 증인에게 증거 수집을 설명하기 위한 타임라인을 사용할 수 있게 해줄 것이다. 증거 수집은 계속되는 과정임을 명심하라.

5. 증거가 수집되었을 때, 증거가 있는 곳은 어디인가?

   전통적으로 "어디" 라는 질문(예를 들면, 컴퓨터가 어디에서 발견되었는가?)에 추가적으로, 디지털 증거와 관련된 또 다른 문제가 발생할 수 있다. 디지털 증거는 여러 곳에 동시에 존재할 수 있음을 인식하라. (예를 들면 이메일은 보내는 사람의 컴퓨터와 받는 사람의 컴퓨터, 그리고 각각의 ISP에 존재할 수 있다.) 다음 질문을 고려하라.

   ■ 디지털 증거가 존재하는 기계나 장치(일련 번호)의 종류는 무엇인가?

   ■ 기계나 장치에 접근한 사람은 누구인가?

   ■ 기계나 장치를 담당하는 사람은 누구인가?

   ■ 기계나 장치는 공용인가?

   ■ 정보가 네트워크로부터 검색되었는가?

   ■ 패스워드로 보호되는 정보인가?

   ■ 누가 패스워드로 보호된 정보에 접근할 수 있는가?

   ■ 컴퓨터 또는 네트워크와 분리된 곳에 있는 데이터인가?

참고 사항: 범죄 현장 관리에 관해 더 많은 정보를 원하면 Electronic Crime Scene Investigation:A Guide for First Responder (www.ojp.usdoj.gov/nij/pubs-sum/187736.htm)의 NIJ 지침서를 참고하라.

Ⅲ. 사건 기록 작성

A. 문서화

증거를 철저하고 정확하게 기록하는 것은 중요하다. 이것은 이 지침서의 1장과 3장에 논의한 기본 원칙 하에서의 증거 인정과 증거의 설득력을 보장하기 위해 필수적이다. 기록이 잘된 사건은 유죄 판결을 잘 이끌어낼 수 있으며, 중요한 검찰과 법원의 자원을 절약해 준다. 앞 장에서 법집행기관은 압수 전 데이터에 무슨 일이 발생했는지를 기록해서 수집해야 한다는 것을 서술했다. 또한 법집행기관은 데이터에 대해 그들이 취한 행위를 철저히 기록해야 한다. 기록물에는 데이터의 획득, 조사, 저장 단계에서 취한 행동이 포함되어야 한다.

조사 노트 작성에 관하여 다음을 명심해야 한다.

■ 노트의 준비와 보관에 관한 소속 기관의 정책을 준수하라.

■ 보유한 노트와 다른 기록들을 찾을 수 있게 유지하라. 검사가 그것을 재검토할 수 있도록 알려줘야만 한다.

■ 다른 사건의 노트와 섞이지 않도록 하라.

B. 보고서와 추가 자료

1. 상세한 보고서 준비

   보고서의 준비와 발표에 대한 법적 요구 사항은 관할 지역마다 다르고, 또한 민사나 형사 사건에 따라 다르다.

   a. 민사 소송에 관한 연방 규칙의 26번째 조항을 보라.

   b. 형사 소송에 관한 연방 규칙의 16번째 조항을 보라.

참고 사항: 민사 소송에 관한 연방 규칙은 www.law.cornell.edu/rules/frcp/overview.htm 에 있고 형사 소송에 관한 연방 규칙은 www.law.cornell.edu/rules/frcrmp에 있다.

---

2. 만약 증인이 전문가 자격이 있거나 의견을 말할 수 있다면 다음을 제공할 준비를 하라.

   a. 의견에 대한 기본 지식

   b. 증인의 이력서

   c. 증인이 전문가로 인정받았다는 사례. 또한 검사는 증인이 전문가로 신청되었으나 인정되지 않은 사례에 대해서도 인지해야만 한다.

참고사항: 전문가로 인정되지 않은 증인은 법률적인 보고서 작성을 요구하지 않는다. 그러나 적절하게 관련 있는 정보를 기술하지 못하면 기소의 성공에 영향을 줄 수 있다.

Ⅳ. 원본 증거의 반환

전자 증거를 압수당한 자는 조사의 시작 여부와 관계없이 반환을 요구할 것이다. 다음은 발생할 수 있는 문제를 개략적으로 나타내고 있다.

A. 금지품

1. 만약 압수된 데이터가 금지품이면 그 매체의 반환이 합당한 지 고려해야 한다.

2. 만약 법정에서 원본을 피고 측에 제공하지 않는다고 결정했다면, 원본이나 포렌식 복제품에 대한 접근을 피고 측에 허용할 상황이 발생할 수 있다. 우선 피고 측에게 압수된 증거에 대해 적절하게 통제된 접근을 제공할 수 있도록 준비하라.

B. 조건

1. 증거가 반환되었을 때, 진정성, 정확성, 소유권, 전문, 절차 연속성과 같은 잠재적인 논쟁거리에 대비하여 각서를 받아라. 각서는 피고 측으로부터 받아야 함을 기억하라. 피고가 아닌 데이터의 소유자로부터 받은 각서는 피고에게 구속력이 없다.

2. 사업이 진행 중이면 해당 정보를 반환해야 할 필요가 있음을 예상해야 한다. 만약 수색 영장을 통해서 정보가 획득되었다면, 이것을 진술서에 명시하라.

Ⅴ. 피고 측에 증거를 공개할 의무

개시 규칙에는 검찰이 계속적으로 피고 측에게 증거를 제공해야 할 의무가 있음을 규정하고 있다. 게다가 피고 측 변호사는 피고 측 조사관이 분석할 수 있도록 증거에 접근하는 것을 강제할 수 있다.

A. 일반적인 개시

1. 피고 측에게 조사의 편의를 위하여 디지털 증거의 복제본을 제공한다.

   a. 피고 측은 환경에 따라 실제 증거나 이미지, 또는 복사본에 접근할 권리가 있다.

금지품의 접근에 대한 요구에 대처(예 : 보호 명령)할 수 있도록 준비하라.

b. 피고 측은 법집행기관이 제시한 디지털 증거를 조사할 권리가 있다.

(1) 디지털 매체를 조사할 수 있도록 다른 사건의 잔존물이 없는 깨끗한 컴퓨터를 피고 측에게 제공하라.

(2) 디지털 매체를 검토할 수 있는 적정한 공간을 피고 측에게 제공하라.

2. 공공 문서의 보존 기간을 알아야 한다. (주나 연방의 정보 공개법이 정보를 얻기 위한 다른 수단으로 사용될 수 있다는 것을 알아야 한다.)

3. 증거에 대해 작업하고 발견한 모든 조사관을 파악해야 한다.

B. 무죄를 증명하는 자료

검찰은 무죄를 증명하는 자료를 파악, 보존하고, 피고 측에 제공할 의무가 있다. 이러한 의무는 관할 지역에 따라 다양하지만, 최소한 무죄를 증명하는 증거가 공판 전에 발견될 때마다 피고 측이 사용할 수 있게 해야 한다.

검사는 조사관이 잠재적으로 무죄를 증명할 수 있는 증거를 포함하여 관련된 모든 증거를 찾았는지 판단해야 한다. 모든 관련된 증거에 대한 검색과 보고의 실패는, 특히 동일한 매체에 대한 피고 측의 조사에 의해 추가적인 정보가 발견된다면, 조사관의 증언에 대한 신뢰성에 영향을 미칠 수 있다. 조사 절차는 포렌식 회계사가 감사 결론을 내기 위하여 장부나 기록에 시행하는 표본 추출과 유사하게 방대한 양의 전자 증거 조사가 적정하게 이루어지도록 해야 한다.

참고 사항; 증거는 무죄를 증명하는 자료가 파괴되지 않도록, 또는 수집이나 분석 과정에서 무죄를 증명할 자료의 손상 가능성으로 인한 불필요한 논란, 시간 소모, 소송 비용 증가를 피하기 위해 세심하게 다루어야 한다.

제 3 장 공판 준비와 증거 규칙

디지털 증거가 포함된 사건의 기소를 준비할 때 몇 가지 문제를 명심해야 한다. 가장 중요한 점은 디지털 증거의 제출은 전문적이고, 진화하며, 때때로 복잡한 기술의 지식에 익숙할 것을 요구한다는 것이다. 그러므로 조사관과 검사는 필수적으로 다음 부분을 알아야 한다.

■ 일반적인 디지털 증거의 기술적인 기본 동작에 관한 지식을 알아야 한다.

■ 직접 사건 관련 특정한 기술의 세부 사항에 정통해야 한다.

효과적인 공판 준비는 수사 착수부터 시작하기 때문에 사건 전반에 걸쳐 기술적인 능력이 필요하다. 디지털 증거의 수색, 압수, 절차 연속성에 관한 문제는 1 장과 2 장에서 다루었다.

이 장에서는 공판 전 준비의 세 측면에 초점을 맞춘다.

■ 진행된 수사의 범위를 검토할 때, 검사가 고려해야 하는 예비 고려사항

■ 공판 전에 검사, 수사관, 조사관 상호 간의 효과적인 의견 교환

■ 증거 가치 문제(예 : 증거 인정과 전문 법칙)

Ⅰ. 사전 고려사항

이상적으로 디지털 증거가 포함된 사건은 검사, 수사 책임자, 조사관으로 구성된 팀에 의해 진행되어야 한다. 이러한 사건은 종종 특정한 절차와 실질적인 문제가 나타난다.

검사에게 부여된 첫 번째 업무 중 하나는 수사 범위를 재검토하는 것이다. 이와 관련 다음과 같은 몇 가지 중요한 문제가 있다.

A. 사실인정자(trier of fact)가 사건에 대한 추론을 이해할 수 있게 준비하고 제시.

B. 기술적인 부분의 특성을 명확히 함.

1. “첨단 기술” 범죄와 관련된 디지털 증거인가?

2. 첨단 기술 범죄와 관련이 없더라도, 디지털 증거가 사건의 중요한 면인가? 아니면 디지털 증거가 단순히 사건의 설명과 수사에 관련 있는가? (예를 들면, 검사는 전

문가의 증언을 설명하기 위해 컴퓨터 시뮬레이션이나 애니메이션을 사용할 수 있다.)

C. 사건에서 디지털 증거의 출처와 특성을 확인하고, 설명함.

1. 저장 장치가 사건의 증거를 포함하는가? 아니면 그 자체가 증거 혹은 범죄 도구인가?

2. 피해자 또는 조사 대상에서 사용된 하드웨어, 소프트웨어, 운영체제, 시스템 구성은 무엇인가?

3. 증거가 단독 사용의 개인용 컴퓨터에서 발견되었는가? 아니면 네트워크에 연결된 컴퓨터에서 발견되었는가?

D. 디지털 증거의 추가적인 출처를 조사해야 하는지 검토. (예 : 백업파일, 로그 파일)

E. 적용할 수 있는 죄목의 검토.(예 : 아동 음란물 소유 사건에서 유포죄와 관련 있는가?)

Ⅱ. 공판 전 의견 교환

디지털 증거 사건의 조사 단계 동안 팀으로서 일한 것은 물론 검사, 수사관, 조사관은 공판 전에 사건의 발표 계획을 수립하기 위해 회의를 해야 한다. 검사는 다음과 같은 주요 사항을 검토해야 한다.

A. 명확히 해야 할 요소, 분석이 더 필요한 부분, 추가 조사가 필요한 부분이 있는 지 논의해야 한다.

1. 사건 관련 특정 기술에 관해 익숙해져야 한다.

2. 수사관과 조사관의 경험과 자격을 검토해야 한다.

3. 증거의 범위와 한계를 검토해야 한다.

4. 회의 전에 수사관과 조사관이 작성한 보고서를 검토하고, 회의를 진행하면서 불확실한 부분을 명확히 해야 한다.

B. 사건 관련 법률 이론, 범죄 구성 요건, 예상되는 변론을 명확히 하기 위해 수사관과 조사관이 참석한 공판 전 대책 회의를 개최하라.

C. 예상되는 직접 심문과 반대 심문의 범위와 방향을 수사관, 조사관과 함께 검토해야 한다.

D. 디지털 증거의 종류를 식별해야 한다.

디지털 증거의 세 가지 카테고리는 공판 전 회의에서 중요하게 다루어야 할 문제이다 - 배경 증거(background evidence), 실질 증거(substantive evidence), 설명 증거(illustrative evidence). 각 증거의 카테고리는 증인이 전문가로써 증언을 할 수 있는지를 명확히 하기 위해 필요하다.

1. 기술적인 문제에 대한 배경 증거(background evidence)

사건의 기술적인 문제를 사실인정자(trier of fact)가 이해할 수 있게 배경 증거를 제시하라. 다음은 공판 전 회의 동안 점검해야 하는 전술적 질문의 예이다.

a. 조사관은 분석 결과와 관련된 증언 뿐만 아니라 증언에 관한 일반적인 지식에 답할 수 있는가?

b. 논란이 없는 일반적인 기술에 관한 것이 있는가? 만약 그렇다면, 사건에 특정된 증언과 분리하여 협의 하에 초기에 제시할 수 있는가?

c. 법적 논란을 일으키는 기술적 문제를 설명하기 위해 은유나 유추를 사용하는가? 은유를 사용하면 의도하지 않은 결과가 초래될 수 있다.(예 : “용기(containers)”로 컴퓨터 혹은 컴퓨터 파일을 언급하면 수정 헌법 제 4 조가 적용될 수 있다.)

d. 사실인정자(trier of fact)에게 논란이 없는 기술적 용어에 대한 설명서를 제공해야 하는가?

2. 실질 증거(substantive evidence)

실질 증거의 제시는 전술적, 기술적인 검토가 필요하다.

a. 전술적인 고려사항

■ 이메일 메시지와 기타 디지털 증거를 인쇄물로 제시할 것인가? 스크린으로 제시할 것인가?

■ 배심원은 디지털 증거의 인쇄물을 별도의 공간에서 검토할 수 있는가?

■ 관련된 모든 파일을 제출할 것인가? 아니면 특정 사례만 제출할 것인가? 만약 파일을 모두 제출한다면 그것들 모두를 논의할 것인가? 아니면 특정 사례만 논의할 것인가? 어떻게 샘플 파일(예 : 아동 음란물 사건의 파일)을 선택할 것인가?

■ 디지털 증거는 막대한 양의 기록을 포함할 수 있기 때문에 적절하게 요약되어야 할 것이다.

참고사항 : 재판 과정 중에 실시간으로 네트워크에 접근하여 보여 주는 것은 기대할 수 없다. 필요한 경우 동영상으로 녹화하여 법정에서 상영하는 것을 고려하라. 만약 실시간으로 진행하는 설명이 필요하다면, 문제가 발생할 수 있음을 감안하여 주의 깊게 연습하라.

---

b. 기술적인 고려사항

■ 재판 과정 중에 발생할 수 있는 기술적 오류에 대비하라. (예 : 기술 지원 인력 배치, 백업이나 인쇄물 제공)

■ 디지털 증거의 발표를 위한 법정 준비
- 컴퓨터의 기능 확인
- 발표하는데 필요한 장비를 이용할 수 있고 제대로 동작하는지, 콘센트와 전선이 잘 설치되었는지 확인
- 법정 안에 특별한 장치의 설치를 법정 안전요원에게 통지
- 만약 오디오가 설치된다면, 법원 서기에게 통지
- 모니터의 위치와 조명 상태를 고려

■ 증거 설명
- 증거 서류의 복사본 준비
- 적정한 설치 시간 확인
- 대기 모드, 시작 스크린, 사운드, 스크린 보호 상태를 비활성화
- 이전 공판에서 한 증거 설명의 종료 부분 확인
- 참조 증거물을 완벽하게 명시한 법정 기록 생성. 증거 설명에 대한 기록을 특별한 방법으로 할 것을 법정에 요청할 지 고려(예 : 컴퓨터 발표의 비디오 녹화, 스크린 캡처의 인쇄물, CD-ROM)
- 배심원에게 노트와 증거목록 제출
- 배심원이 노트를 요청할 것인지 고려

3. 설명 증거(illustrative evidence)

앞에서 언급한 전술적, 기술적인 문제 이외에 추가적으로 다음과 같은 설명 증거를 제시할 지 고려한다.

a. 매체나 매체의 조합을 통한 발표가 가장 설득력 있을 것이다.

b. 변경할 수 없는 고정된 형태의 애니메이션으로 발표할 것인지 변경된 가정을 반영하여 수정할 수 있는 형태의 애니메이션으로 발표할 것인지 결정한다.

c. 이러한 증거를 공판 전에 공개할 필요가 있는지 결정한다.

E. 공판 전 재정(pretrial rulings)에 대한 고려사항

디지털 증거는 법정에서 익숙하지 않으며, 복잡해 보이기 때문에, 공판 전 회합을 통해 증거 인정(예 : 전문가 증언)과 발표 문제의 해결 방안을 생각해야 한다. 이것은 다음의 목표를 달성하기 위한 것이다.

1. 배심원이 없는 공판에서 처음으로 이러한 문제의 언급을 피한다.

2. 기술 관련 문제에 관해 법정 관계자를 교육한다.

3. 공판에서 증거의 인정을 확실히 한다.

4. 잠재적인 반대 증거를 파악한다.

Ⅲ. 증거에 대한 고려사항

주 법정의 증거 규칙이 관할 지역마다 다를지라도, 많은 주의 증거 규칙이 연방 증거 규칙(Federal Rules of Evidence, FRE)을 모델로 삼고 있다. 주별 검토는 이 지침서의 범위 밖이기 때문에, 이 절은 FRE에 기반하여 설명한다. 검사는 적용해야 하는 해당 지역의 규칙을 참고해야 한다.

참고 사항 : 연방 증거 규칙은 www.law.cornell.edu/rules/fre/overview.html.에서 찾아 볼 수 있다. 연방 증거 규칙에 대한 포괄적인 분석은 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)에 되어 있다.

다른 유형의 증거와 마찬가지로 디지털 증거는 연관성, 진정성, 전문과 같은 문제가 제기될 수 있다. 비록 이러한 문제가 다른 유형의 증거와 동일한 토대 위에서 해소되더라도, 디지털 증거는 특별한 부분이 있음을 명심해야 한다. 디지털 증거 그 자체 뿐만 아니라, 디지털 증거의 제출에는 전문가 증언 및 그와 관련된 증거적 문제가 포함될 수 있다. 비록 증거 인정이 궁극적으로는 검사가 다루어야 할 문제이지만, 증거 인정을 받는

데 필요한 기본 설명에 대해서는 수사관과 조사관이 도와줄 수 있다.

증거의 고려사항은 디지털 증거의 특성과 출처에 영향을 받는다. 이와 관련하여 이 절에서는 다음과 같은 사항을 논의한다.

■ 증거 용어 정의

■ 컴퓨터에 설정되어 있는 실질 증거

■ 컴퓨터가 생성한 실질 증거

■ 재판을 위해 준비된 실질적이고 사례가 되는 컴퓨터로 생성한 증거

■ 전문가 증언

A. 증거에 관한 용어 정의

1. 판사의 자유 재량

판사(trial judge)는 증거의 인정을 판정할 때 광범위한 재량권이 있다. 많은 판사(trial judge)에게 디지털 증거는 익숙하지 않은 영역이기 때문에, 증거 제출자(proponent)는 어떻게 신기술을 증거 규칙에 적용할 수 있는 지에 대해서 알아야 한다.

2. 관련성(증거가 도움을 주는가?)

만약 증거가 사건에 중요한 어떤 사실을 증명하거나 반박하는데 도움이 된다면, 보통은 증거로 인정될 것이다. 특별한 규칙, 법령, 헌법 조항으로 배제되지 않는다면, FRE의 기본 방침은 “모든 관련된 증거는 인정”한다 (FRE 401). “관련 증거”는 “그것이 없었을 경우 보다 큰 확률로 행동으로 인한 결과로써 어떤 사실이 존재할 가능성이 큰 증거”를 의미하는 것으로 광범위하게 정의한다.(FRE 401)

다양한 관련성에 대한 대상 중에 다음 두 가지는 특별히 고려해야 한다.

a. 편견

만약 판사가 심하게 편파적이라고 결정하면 그 관련 증거는 배제될 것이다. 즉, 그것은 “증거적 가치가 불공정한 편견으로 인한 위험성으로 사건을 혼란스럽게 하며, 배심원을 현혹시키거나, 혹은 과도한 연기를 고려함으로써 시간을 낭비하고, 불필요한 중복 증거의 제출을 통하여 실제 보다 중요하게 여기게 하는 것이다.”(FRE 403). 컴퓨터로 생성한 시뮬레이션이나 애니메이션을 증거로 제출하는

것을 고려할 때, 이러한 잠재적 이의 제기의 가능성을 명심해야 한다.

b. 다른 행위

디지털 증거 사건에서 FRE404(b)에 의한 “다른 범죄, 과실, 행위”에 의한 증거로써 이의 제기가 있을 수 있다. 그러나 이러한 증거는 “동기, 기회, 의도, 준비, 계획, 지식, 성격, 실수 또는 사고 가능성의 부재”를 증명하는 것으로 인정될 수 있다.

예를 들어, 아동 음란물 사건은 다양한 불법 행위를 수반하며, 일부는 기소할 수 있는 것이다. 기소할 수 없는 증거는 관련 사실의 지식이 없거나 실수가 아님을 증명하기 위해 인정될 수 있다.

3. 진정성(그것이 말한 그것인가?)

제공된 증거는 증거의 제출자가 주장하는 것임을 입증해야 한다.(FRE 901(a)). 제출자에게 진정성과 부합하지 않는 모든 가능성을 배제시킬 것을 요구하는 것은 아니다. 증거 인정의 규정은 그 증거가 의미하는 것의 합리적 가능성이다.

4. 전문(傳聞)(실제 증언 우선권)

전문에 대한 규정은 법정에서 진술자(declarant)의 증언 태도를 사실인정자(trier of fact)가 관찰하고 반대 심문할 수 있도록 진술한 그 사람이 실제 증언하게 하는 것을 반영한다. 디지털 증거는 때때로 전문 문제를 야기한다. 전문 문제를 검토하는 단순하면서 유용한 프레임워크는 다음과 같다.

a. 전문인가?

(1) 대상이 전문에 대한 핵심 정의에 부합하는가?

“전문”은 진술로 주장하는 문제의 진실을 입증하기 위해 법정 밖에서 진술된 것이다.(FRE 801(c)). 만약 그 진술이 말한 것의 진실을 증명하기 위해 제공된 것이 아니면, 그것은 전문이 아니다. 예를 들어, 신용카드 사기 사건의 기소에서 신용카드 회사의 수집 부서에서 보관한 피고의 계좌와 관련된 컴퓨터 인쇄물은 그 내용의 진실성을 증명하기 위해 제출되었기 때문에 전문에 대한 정의에 부합한다. 반면에 온라인 미성년 교사죄 사건에서, 피해자가 보낸 이메일이 내용의 진실성 보다는 단순히 피고와 피해자 사이의 교류가 있었음을 보여주기 위해 제출되었다면 전문의 정의에 부합하지 않는다. 즉 피고가 이메일을 받았다는 사실과 관련이 있는 것이지 이메일로 말한 것이 아니다.

주장하는 사실의 진실을 증명하기 위해 제공되는 증거인지와는 별도로 전문의

구성요건에 해당되는 “진술”인지에 관한 문제가 있다. 진술은 “(1)구두나 서면, (2) 주장하기 위한 의도로 행한 사람의 행동”으로 정의된다.(FRE 801(a)). 이러한 관점에서 핵심 쟁점은, 아래에서 논의하는 것처럼, 기록이 컴퓨터가 생성한 것인지(진술이 아닐 가능성이 높음), 아니면 컴퓨터에 저장된 것인지(진술로 판단)이다.

(2) 대상이 전문의 정의에 해당할 경우에도, 증거의 규칙에 의거 전문에서 제외될 수 있는가?

FRE는 비록 주장된 사실의 진실성을 증명하기 위해 제공됨에도 불구하고 전문으로 간주하지 않는 몇 개의 카테고리를 특정하고 있다. 공통적인 예외는 “자백(admissions)” 카테고리이다.(FRE 801(d)(2)).

b. 만약 전문이라면, 그럼에도 불구하고 예외 조항에 의해 인정될 수 있는가?

진술이 전문으로 볼 수 있음에도 불구하고 전문 법칙의 다양한 예외에 의해 인정될 수 있다. 디지털 증거와 관련된 공통적인 예외는 아래의 Ⅲ.B.3. 절에서 논의하는 사업 기록 예외조항이다.

B. 컴퓨터에 미리 저장된 실질 증거

1. 실질 증거와 설명 증거, 컴퓨터에 저장된 것과 생성된 것의 구별

a. 실질 증거 대 설명 증거

문서나 법정 증언(live testimony)과 같은 다른 형태의 증거가 있는 사건의 경우, 디지털 증거의 인정에 적용되는 원칙은 대부분 출처, 생성 방법, 제공 목적에 의존한다. 제출 목적 관점에서, “실질 증거”는 그 자체를 증명하는데 도움을 주기 위해 제출된 것인 반면에 “설명 증거”는 그 자체로 무엇인가를 증명하는 것이 아니라 증언을 설명하기 위한 것이다.

예를 들어, 신용카드 사기사건에서 전산화된 은행 기록, 사이버스토킹 사건에서 이메일, 아동 음란물 사건에서 이미지 파일은 모두 실질 증거이다. 각각은 사건의 쟁점을 증명하는데 도움을 주는 실질 증거이다. 반대로 목격자의 증언을 설명하기 위해 사용되는 컴퓨터 애니메이션은 그 자체가 증명을 하는 것이 아니라 관련된 실질 증거(증언)를 지원하기 위해 제공되는 것이다.

b. 컴퓨터 저장물 대 컴퓨터 생성물

컴퓨터 저장 증거는 사람이 생성하여 전자형태로 저장된 문서와 기타 기록물을 말한다. 워드 파일, 이메일, 인터넷 채팅 메시지 등이 그 예이다. 이러한 종류의 증

거는 증거 인정과 전문 문제를 야기한다.

컴퓨터 생성 증거는 컴퓨터 프로그램의 직접적인 출력으로 구성된다. ISP의 로그인 기록, 자동화된 전화 통화 기록, 현금 인출기 영수증 등이 그 예이다. 이러한 기록은 증거 인정 문제는 있지만 사람의 진술 형태가 아니기 때문에 전문으로 간주하지는 않는다.

마지막으로 어떤 기록은 컴퓨터 생성 증거와 저장 기록이 혼합되어 있을 수 있다. 예를 들면 회계 스프레드시트는 사람이 입력한 값과 컴퓨터 프로그램에 의해 생성된 출력이 있다. 그래서 이러한 증거는 두 가지 문제가 모두 존재한다.

다른 증거의 카테고리로 재판 준비를 위한 컴퓨터 생성 증거가 있는데, Ⅲ. D 절에서 논의하는 독특한 문제가 나타난다.

2. 컴퓨터 저장 실질 증거의 인정

앞에서 언급한대로 인정 요건은 단순히 컴퓨터에 저장된 기록이 기소하면서 주장한 것임을 증명해야만 한다는 것이다. 핵심 쟁점은 컴퓨터에 저장된 기록물의 작성자를 확인하고 사건의 본질 측면에서 중요한 변화가 없음을 보이는 것이다. 이 두 가지 관점은 절차 연속성과 2장에서 언급한 기타 정황 증거를 통해 증명할 수 있다. FRE 901의 (b)(1)는 “어떤 문제가 주장된 것이다”라는 것을 “알고 있는 증인의 증언”으로 증거를 인정하는 예이다.

여러 법정에서 증거 인정을 위해 출석한 증인은 증언하는 사실에 관해 직접 알아야 하지만, 의심되는 컴퓨터의 프로그래머일 필요는 없고, 기술적 운영과 유지 관리를 하거나, 입력된 데이터를 보았다면 증언을 인정하고 있다. 예를 들어 피고의 소유물에서 압수한 컴퓨터에 불법 마약 거래에 관한 컴퓨터 저장 기록이 발견되었으면, 컴퓨터를 압수한 수사관(해당 컴퓨터가 피고의 소유물이었고, 마약거래의 다른 증거를 통해 관련된 자가 파일에서 사용하는 이름과 일치함을 증명)과 파일을 복구한 조사관(그 기록이 실제로 해당 컴퓨터에서 발견되었음을 증명)의 증언에 의해서 인정될 수 있다.

일부 사건에서 컴퓨터 저장 기록의 익명성(인터넷 관련 범죄) 때문에, 작성자를 주로 정황 증거로 확인하였다. 예를 들어 인터넷 채팅이 포함된 아동 음란물 사건에서 비밀요원에게 준 정보와 ISP로부터 얻은 정보로 채팅방과 게시물이 연결된 피고의 거주지에서 얻은 증거의 작성자임을 충분히 입증하였다.

FRE에 의거한 디지털 증거의 인정은 종종 간단하고 쉬운 문제이다. 피고는 때때로 컴퓨터 기록이 그가 생성한 후에 변경되었다는 주장을 함으로써 진정성에 대해 이의를 제기한다. 그러한 주장은 컴퓨터 기록이 쉽게 수정될 수 있음을 강조한다. 그러나 증거 인증에 대한 임계치의 “합리적인 가능성”하에서 법정은 일반적으로 특정 증거의

변경 부재로 그러한 주장을 기각하였다. 더욱이 데이터 인정은 필수적이지 않은 데이터는 수정해도 실질적인 데이터는 중요한 변화를 일으키지 않는 조사 소프트웨어를 사용함으로써 배제되지 않을 수 있다. 예를 들어 시간과 날짜의 변경은 주어진 사건의 증거에서 제외되지 않을 수 있다.

변경 가능성과는 별도로 기록의 완전성, 입력 절차, 입력 방법(정확한 데이터 변환)과 같은 문제가 제기될 수 있다. 만약 이러한 문제가 중요한 쟁점이라면, 검찰은 증거를 취급한 자를 증언대에 세울 준비를 해야 한다.

예를 들어 이메일을 인정하기 위한 일반적인 방법은 다음과 같다.

■ 메시지가 생성된 컴퓨터에 지목한 송신자가 주로 접속했다는 증언과 함께, 메시지의 경로에 대한 연속된 추적

■ 이메일의 내용을 작성자가 알고 있음을 언급

■ 이메일의 회신 기능을 사용한 답장. 답장은 송신자의 원 메시지를 포함할 수 있음

■ 이메일을 수신한 후, 송신자는 내용과 일치하는 행동을 한다.

대부분의 경우, 정황 증거와 결합하면 컴퓨터 기록의 작성자와 진정성을 확립할 수 있다.

3. 전문과 컴퓨터 저장 실질 증거

만약 컴퓨터 저장 기록이 사람에 의해 작성된 진술을 포함하고 진술에서 주장하는 사실의 진정성을 증명하기 위해 제공된다면, 검사는 전문법칙을 생각해야 한다. 앞에서 언급했듯이, 만약 진술을 상대편에서 인정하면, FRE801(d)(2)에 의해 전문의 정의에서 벗어나며 예외 조항의 적용이 필요 없게 된다. 또한 진술이 주장한 사실을 증명하기 위해 제공한 것이 아니라면 전문법칙은 적용되지 않는다.

컴퓨터 저장 기록의 가장 일반적인 전문증거 예외 조항은 사업 기록 예외 조항이다(FRE 803(6)). 이러한 예외 조항의 적용을 위한 근거를 설정하기 위해서, 검사는 정보의 출처, 작성 방법과 환경이 믿을만한지 입증할 준비를 해야 한다. 다음과 같은 방법으로 입증할 수 있을 것이다.

a. 기록이 저장된 컴퓨터 장비(하드웨어와 소프트웨어)는 표준형 또는 믿을만한 것으로 인정된다.

b. 데이터는 정상적인 업무 형태로 입력되었거나 기록된 이벤트 발생 시간이 인정할 만한 업무 시간 근처이다.

c. 근거가 되는 기록의 출처뿐만 아니라 작성 시간과 방법이 기록을 신뢰할 수 있게 해주며, 따라서 증거 인정이 합당하다.

기록 관리자 또는 작성 방법에 익숙한 자의 증언을 통해 이러한 근거를 확립할 수 있는데, 증언하는 자가 기록에 포함된 사실을 직접적으로 알지 못하고 소프트웨어나 하드웨어의 기술적 측면에 익숙하지 않아도 된다. 더욱 더 신뢰할 수 있도록 검사는 다음을 보여 줄 수 있다.

■ 데이터에 대한 회사 의존도

■ 데이터 기입의 정확성에 대한 확인 노력

■ 저장되어 있는 동안 데이터의 변경이나 손실 예방 노력

■ 출력 데이터의 무결성을 위한 정책

증거 인정을 위한 요건과 전문법칙의 사업 기록 예외조항 적용을 위한 요건은 상당 부분 중첩된다. 진정성에 관해 앞에서 말한 것처럼 합당한 근거가 제시된다면, 컴퓨터의 인쇄물 또는 기록 그 자체가 일부 부정확하다는 주장이 반드시 증거의 무효화를 초래하지는 않는다. 사업 기록이 종이에 기록된 사건과 유사하게, 일부 오류의 존재는 기록의 인정 여부가 아니라 중요도에 영향을 준다. 또한 소송만을 위해 작성된 기록은 신뢰할 수 없다는 이의 제기가 있을 수 있어도 해당 데이터에 적용되는 것이지 기록의 인쇄물에 적용되는 것이 아님을 주목하라. 따라서 소송을 위한 인쇄물의 준비는 해당 데이터가 정상적인 사업 활동 하에서 기입되고 저장된 것이라면 신뢰성을 감소시키지 않는다.

예를 들어 피고가 파산 처리 기간에 재산을 은닉하고 파산된 회사의 기록을 파기하거나 은닉한 죄로 기소되었다고 하자. 이 경우 법정에서는 경리직원이 입력한 재고 목록, 임금 대장, 기타 회계기록이 포함된 회사의 일반 원장에 대한 컴퓨터 인쇄물은 증거로 당연히 인정될 것이다. 증거 인정을 받기 위해서 검사는 경리 직원에게 현재의 기준으로 데이터가 입력되었고, 인쇄물이 데이터를 정확히 나타내고 있으며, 매월 일상 업무로 작성되었다는 증언을 받아야 한다. 또한 데이터가 정확한 지 정규적으로 확인했으며 사용된 시스템이 산업계의 표준이라는 것에 대해서도 증언을 받아야 한다.

참고 사항 : 다른 기록들처럼 컴퓨터 저장 기록은 여러 단계의 전문이 포함될 수 있다. 데이터 기입 행위는 FRE 801(a)에 의한 법정 외부의 “진술”이지만, 그 결과는 앞에서 언급한 FRE 803(6)에 의한 일반적인 업무 활동으로 유지된 기록이다. 또한 입력된 기본 데이터는 전문인 “진술”로 볼 수 있으며, 전문의 예외 또는 면제로 인정되어야만 한다.

---

4. 컴퓨터 저장 실질 증거의 인쇄물

a. 원본의 요건, 최선 증거(best evidence) 규칙

예외 조항이 적용되지 않는 한, 내용 증명을 하려는 자가 제시하는 원본 필기물, 기록물, 사진에는 소위 “최선 증거(best evidence)” 규칙의 적용이 요구된다.(FRE 1002)

비록 컴퓨터 저장 기록의 인쇄물이 기술적으로 원본처럼(원본 데이터는 0과 1의 비트열이기 때문에) 보이지 않는다고 해도 인쇄물이 데이터를 정확하게 나타낸다면 최선 증거 규칙에 문제가 되지 않는다. 일반적으로 사용되고 실용성의 요구에 의해서, “만약 데이터가 컴퓨터 또는 유사한 매체에 저장되어 있는 경우, 인쇄물 또는 눈으로 읽을 수 있는 형태의 출력이 그 데이터를 정확히 나타내면, 그것은 ‘원본’이다.”라고 FRE는 규정하고 있다 (FRE 1001(3)). 이 원칙은 복제 원본(duplicate originals)이 외견 상 일치되지 않아도(예 : 폰트나 여백이 다름) 적용된다.

b. 요약

FRE 1006 하에서, 만약 필기물, 기록물, 사진의 양이 방대하여 법정에서 내용을 쉽게 조사할 수 없다면, 원본 또는 복제본을 상대 측에서 검토 또는 복사할 수 있다는 조건하에서 차트, 요약, 추정의 형태로 제시할 수 있다. 컴퓨터 기록의 인쇄물은 그 기록의 데이터 요약으로 항상 취급되는 것은 아니다.

그러나 디지털 증거의 양이 너무 많으면 편의성을 위해 데이터 요약이 필요하다. 예를 들어 대형 사기사건에서 전산화된 송장의 요약은 FRE 1006의 제한 조건에 부합하면 인정된다.

일부 주는 훨씬 자세하게 최선 증거 규칙을 다룬 법률이 있다.(예 : California Evidence Code, sections 1521 through 1523)

C. 컴퓨터에 의해서 생성된 실질 증거

일부 컴퓨터 기록은 사람이 생성했다기 보다는 컴퓨터 프로그램에 의해 자체적으로 생성되며 단순히 전자적 형태로 저장된다. 이러한 관점에서, “컴퓨터 생성(computer generated)”은 인쇄물 보다는 기록 그 자체를 의미한다. (많은 법정에서 해당 기록이 사람이 입력한 데이터인지 컴퓨터 알고리즘이 생성한 것인지 구별하지 않고 컴퓨터 인쇄물을 컴퓨터가 생성한 것으로 막연히 언급할 수 있음에 주의하라.) 컴퓨터 생성 기록의 예로 자동 전화 통신 기록, ISP 로그 기록, 자동 현금 인출기 기록 등이 있다.

일부 법정에서 모든 디지털 증거가 유사한 것이 아님을 인식하기 시작했지만, 증거 제출자는 컴퓨터 저장 증거와 컴퓨터 생성 증거의 차이점을 알고 있어야 한다. 올바르게 고려되면, 컴퓨터 생성 증거는 인정 문제는 있으나 전문 문제는 없다. 그럼에도 불구하고 일부 법정은 컴퓨터 생성 증거를 전문 법칙에 계속해서 적용하고 있다. 실제적으로는 증거 인정과 사업 기록 예외조항에 대한 근거 확립이 중첩되기 때문에 이러한 구별이 공판 과정에서는 큰 차이로 나타나지 않는다.

1. 컴퓨터 생성 실질 증거의 인정

컴퓨터 생성 기록은 사람이 입력한 것이 아니라 컴퓨터 프로그램이 직접 만들었기 때문에, 증거 인정 문제에 기록 작성자의 확인이 필요 없다. 대신 증거 인정의 관심사는 처리 과정과 출력 기능의 신뢰성이다. 특별히 이런 관심사에 대한 타당성은 FRE 901(b)(9)에 의거한 것인데, “결과를 생성하기 위해 사용한 프로세스와 시스템을 설명한 증거와 그 프로세스와 시스템이 정확한 결과를 산출함을 입증”함으로써 진정성이 확보된다.

2. 전문과 컴퓨터 생성 실질 증거

컴퓨터 프로그램이 생성한 기록은 전문으로 간주되지 않는다. 이것은 FRE 801(a)에 의한 “진술”의 정의에 부합하지 않기 때문이다. 사실 그것은 “구두나 서면 형태”도 아니고 “주장하는 자의 행위”도 아니다. 더욱이 FRE 801(b)는 “진술한 자”를 “주장자(declarant)"로 정의한다. 일부 컴퓨터 생성 기록은 사람의 진술 형태로 보일 수 있다. 읽지 않은 이메일의 존재를 알리는 “You've got mail”과 같은 프롬프트가 그 예인데, 이것은 단지 컴퓨터 프로그램의 자동 출력문일 뿐이다.

전문 법칙에 대한 이론적 근거는 ‘법정 증언을 통해서 사실인정자(trier of fact)에 의한 증인의 태도 관찰과 반대 심문을 함으로써 사람의 주장을 검증하려는 것’이기 때문에 사람에 의해서 만들어지지 않은 증거는 전문법칙이 적용되지 않는다. 그래서 법정에서 오랫동안 인정된 음주 측정 기기와 과속 탐지 장치의 출력, 냄새에 반응하는 경찰견의 행동과 같은 증거는 진정성 문제는 있으나 전문은 아니다.

또한 일부 법정은 컴퓨터 생성 기록을 전문이 아니라고 판단하였다. 이러한 구별을 인식하지 못한 지역도 사업 기록 예외조항을 적용할 수 있는 적정한 근거가 제시된다면 그러한 증거를 인정하는 추세이다. 예를 들면, 개방된 ATM 내의 컴퓨터 생성 기록이 FRE 901(b)(9)에서 의도한 진정성 입증 요건처럼 비록 기록 관리자가 기록을 생성한 프로그램의 정확성과 기능에 대해 잘 알지 못해도, 기록 관리자에 의한 증언에 기반한 사업 기록 예외 조항을 적용하여 증거로 인정되었다.

D. 공판을 위해 준비한 컴퓨터 생성 실질 및 설명 증거

1. 증거의 종류

앞에서 언급한 디지털 증거의 두 종류인 컴퓨터 저장 기록과 컴퓨터 생성 기록은 수사 착수 전에 어떠한 형태로 존재한 것이다. 그 형태는 디지털일 것이며. 따라서 그 증거는 수사와 공판을 위해 인쇄되었을 것이다. 그러나 원 데이터는 이미 존재하고 있는 것이다. 이러한 관점에서 디지털 실질 증거는 지문, 생체 샘플, 위조화폐, 살인 무기와 같은 다른 실질 증거와 유사하다.

다른 종류의 증거로 공판을 위해 준비한 것이 있다. 이들 중 일부는 실질 증거라기 보다는 설명 증거이다. 일반적인 예로 목격자의 증언을 설명하기 위한 건물의 도면이 있다. 이러한 도면은 그 자체로는 아무 것도 증명하지 못하며, 단지 증언을 설명하기 위해 사용된다.

수사와 공판을 위해 준비하는 다른 종류의 증거 중에는 증인의 증언과 별개로 무엇인가를 증명하는 실질 증거도 있다. 사건 현장의 사진이 그 예이다. 이러한 증거는 “사실(real)”이라기 보다는 “사실을 설명하는(demonstrative)” 것이다. 이것은 그 자체가 기소하게 된 거래나 사건과 관련된 것이 아니라 그것을 설명하기 위한 것이다.

비슷하게, 공판을 위해 준비한 컴퓨터 생성 증거 역시 설명 증거 또는 실질 증거가 될 수 있다. 빌딩의 복도 도면(강도의 목격자와 범인의 위치를 보여주기 위함), 기소하는 사건의 요약, 혹은 전문가 증언의 요점과 같이 이미 배포한 이미지를 컴퓨터를 사용하여 보여 줄 수 있다.

실질 증거로 사용되는 컴퓨터 생성 정지 영상의 예로 사건 현장 또는 범인의 디지털 사진이 있다. 또한 인쇄된 이미지는 수작업으로 하는 확대나 하이라이트 같은 강조나 효과를 위한 컴퓨터 화면에 있는 정지 영상의 조작도 허용된다. 심지어 컴퓨터 기술은 동영상 발표도 가능하게 해준다.

예를 들어 포렌식 병리학자가 사체를 관통한 총알의 궤도를 설명하기 위해 애니메이션을 사용했다고 하자. 개인적인 상해 사건을 묘사하는 “day-in-the-life”처럼 생생한 묘사를 위해 소송 관계자에게 비디오 테이프 기술을 허용하는 것과 동일하게 컴퓨터 기술은 사건의 정교한 “재현(re-creations)”과 컴퓨터 시뮬레이션을 위해 현재 허용된다.

2. 증거 관련 문제

a. 적절성

공판을 위해 컴퓨터 생성 증거와 관련된 주요한 적절성은 FRE 403에 있는데, 불공정한 편견, 문제를 혼란스럽게 하는 것, 배심원을 현혹시키는 것 등에 근거하여 증거를 배재시킬 수 있도록 판사(trial judge)에게 광범위한 재량권을 부여하고 있다. 예를 들면, 컴퓨터 생성 증거물, 특히 재구성한 애니메이션 혹은 시뮬레이션은

사실인정자(trier of fact)에게 강한 인상을 심어 줄 수 있기 때문에 과도한 편견을 유발할 위험이 있다. 판사(trial judge)가 FRE 403의 반대 조항(objection) 위에서 컴퓨터 생성 증거물을 인정했다면, 배심원에게 증거물을 허용한 취지에 관해서는 제한적인 설명을 할 수 있다.

b. 심문 방법

직접 심문을 진행하는 정상적인 방법은 증인에게 유도 심문을 피하면서 자세히 묻는 것이다. 공판정에서 컴퓨터 생성 증거물을 사용하는 변호사는 증인을 유도하거나 장황한 설명을 한다는 이의 제기를 피하기 위해 적합한 근거를 확립하고, 증인에게 적합한 질의를 하기 위해 세심한 주의를 해야 한다. 컴퓨터 생성 증거에 음성 해설이 포함되어 있다면 이러한 우려가 발생할 가능성이 크다.

c. 증거 인정과 다른 기본적인 문제

증인의 증언을 설명하기 위해 사용하는 이미지는 쉽게 인정받을 수 있는데, 이미지는 개인적인 지식에 기반하여 나타내고자 하는 것을 공정하고 정확하게 묘사한다는 증인의 증언만 요구한다. 범죄 현장 사진으로 제출된 디지털 사진은 변조 가능성이 제기되지 않는다면 전통적인 사진처럼 일반적으로 인정된다. 예를 들면, 디지털 사진의 화질을 높이는 것은 인정문제를 일으킬 수 있다. 전문가 증언이 수반된 재구성과 시뮬레이션은 그러한 증거의 입증 중지를 수락하기 위하여 전문가 증거 그 자체(III E. 절 참조)와 동일한 근거를 요구한다. 또한 입력과 출력 변수가 올바르다는 증언이 필요할 것이다. 예를 들면, 시뮬레이션은 비행기사고와 자동차 사고를 표현하기 위해 민사사건에 공통적으로 사용된다. 이러한 사건의 인정 문제는 시뮬레이션이 기반하고 있는 수학적 모델의 과학적 유효성과 실제 사건에 대응되는 입력 데이터의 범위(정확성과 안정성 관점)에 초점이 맞추어진다.

d. 전문(hearsay)

(1) 전문인가?

공판을 위해 준비한 컴퓨터 생성 증거는 증거의 성격과 제출 취지에 따라 전문 문제를 발생할 수 있다. 건물의 복도 도면이나 권총 그림과 같이 단순히 증인의 증언을 설명하기 위해 사용하는 컴퓨터 증거는 주장한 문제의 진실이나 무엇인가를 증명하기 위해 제시하지 않는다. 그것은 단지 증인의 증언을 설명하기 위해 제공한다. 따라서 이러한 컴퓨터 증거는 전문이 아니다. 범죄 현장의 실체를 증명하기 위해 제공하는 디지털 사진은 “진술”이 아니라 기계의 직접적인 출력이다.

반면에 재구성과 시뮬레이션은 증인의 증언 이상이며, 따라서 목격자의 법정 증언과는 분리된 실질 증거로 구성된다. 만약 입력 데이터와 시뮬레이션의 기반이 되는 가정을 포함하여 시뮬레이션이 법정외 진술에 기반했다면, 전문 문제가 발생한

다.

(2) 예외조항의 적용이 가능한가?

만약 컴퓨터 생성 증거물이 전문으로 간주되면, 그것의 제출자는 적용할 수 있는 예외조항이나 전문법칙의 다른 방법을 찾아야 한다.

몇몇 예외조항은 입력 데이터에 적용할 수 있다. 예를 들어 측정은 FRE 803(1)에 의해서 "present sense impression"로 간주할 수 있다. 다른 데이터는 FRE 803(6) 하의 사업 기록으로 적격한 지 검증되거나 FRE 803(8) 하의 공공기록으로 적격한 지 검증되어야 한다. (그러나 공공기록은 형사 소송 절차에서 중요한 제한을 받는다.) 입력 데이터가 이러한 예외 조항에 적합해도, 전문법칙은 프로그램 실행과 출력 기능에 여전히 적용될 것이다.

또한 증거물 제출자는 몇 개의 한계를 조건으로 하는 FRE 807 하의 "residual exception"를 호소할 수 있다. 제출자는 "진술"이 중요한 사실의 증거이고, 합리적인 노력을 통해 제출할 수 있는 다른 증거보다 그 사실을 더 잘 입증하며, 증거의 인정이 증거 규칙과 정의 측면에서 적합함을 보여야만 한다. 또한 FRE 807은 통지 요건(notice requirement)을 만족해야 한다.

공판을 위해 준비한 컴퓨터 애니메이션이나 시뮬레이션의 제출자는 전문가의 의견 진술(opinion testimony)에 기반하여 FRE 703 하의 증거 인정을 추구할 것이다. 그러나 FRE 703에 대해 2000년 개정된 법률에서는 전문가에 의존하지 않고는 허용될 수 없는 정보에 대한 인정이 제한됨을 주목하라. 이제 이러한 증거는 법정에서 "전문가 의견을 평가하여 배심원을 도와주는 입증 가치가 편견에 의한 영향보다 중요하다"는 것을 발견하지 못하면 기각된다.

E. 전문가 의견 진술(opinion testimony)

전문가 의견의 사용은 다음과 같은 세 단계 접근 방식을 요구한다.

■ 전문가 의견이 요구되는 문제 파악 (4장 III.A 절에서 논의)

■ 적격한 전문가 파악 (4장 III.C 절에서 논의)

■ 적격한 전문가가 허용된 방법을 사용하는지 확인 (이 절에서 논의)

두 개의 중요한 판정법이 전문가 의견의 인정 여부를 좌우한다. 하나는 Frye test(Frye v. United States, 54 App. D.C> 46, 293 F. 1013(1923))이고, 다른 하나는 Daubert test(Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993))이다.

참고사항 : 전문가 의견 진술의 인정은 공판 전 회의(pretrial)에 이의 제기를 받을 수 있다. 검사와 전문가는 공판을 준비하는 것만큼 공판 전 회의(pretrial)의 이의제기에도 세심하게 준비해야 한다.

1. Daubert 판정법은 연방법원에서 적용된다.

Daubert 판정법은 연방법원이나 많은 주법원에서 바탕이 되는 과학적 기술의 신뢰성과 적정성에 기반한 전문가 의견 진술의 인정을 판사(trial judge)가 결정하게 함으로써 Frye 판정법을 대체하였다. 미국 대법원은 사실인정자(trier of fact)에게 과학적 전문가 의견 진술이 유용한 지를 다음으로 확인할 것을 제안했다. (1) 과학적 기술이 검증될 수 있고 검증되었다. (2) 기술이 자세한 검토와 공개를 위해 제안되었다. (3) 알려지거나 가능성 있는 오류율이 있다. (4) 관련된 과학 단체에 의해 널리 인정된 기술이다.

법원은 이 기준을 엄격하게 적용하지도 않고 모두 요구하지도 않음으로써 Daubert 사건과 후속 사건들을 해결했다. Daubert 판결은 “쓰레기 과학”의 인정을 억제하고 신뢰할 수 있는 과학적, 기술적 포렌식 기술의 개발을 촉진하도록 법원(trial court)이 “게이트키퍼”처럼 행동하도록 미국 대법원이 제안하는 것으로 여겨진다. Daubert 사건과 후속 사건에 기반한 전문가 의견 진술의 인정에 적용되는 FRE의 7항이 최근에 변경되었다. Kumho Tire Co., Ltd v. Carmichael(526 U.S.137(1999))에서 과학 분야로 엄격하게 제한되던 것을 기술 분야로 확장 적용하였다.

만약 “(1) 증언이 충분한 사실이나 데이터에 기반하고, (2) 증언이 신뢰할 수 있는 원칙이나 방법의 결과이며, (3) 증인이 사건을 위해 신뢰할 수 있게 그 원칙이나 방법을 적용했다면” 기술적인 전문가 의견 진술은 2000년에 수정된 FRE 702하에서 인정된다.

참고사항 : 전문가 의견 진술에 관련된 법은 계속적으로 개정되고 있다. 하급 법원에 의해서 수많은 요소가 Daubert 판정법의 4가지 요소에 추가되었다. A Guide to Forensic Testimony: The Art Practice of Providing Testimony as an Expert Technical Witness 의 61쪽에 나열된 것을 참조하라.

2. 많은 주에서 여전히 Frye 판정법을 사용하고 있다.

Frye 판정법은 만약 기술이 관련 과학 단체에서 널리 받아들여졌다면, 법정에서 인정될 수 있는 과학적 기술로 허용하는 것이다. 컬럼비아 특별 순회 재판구의 항소법원(The Court of Appeals for the District of Columbia Circuit)에서 Frye 판정법에 대해 다음과 같이 언급하였다. “법원은 잘 알려진 과학적 원리나 발견으로부터 연역된 전문가 증언을 계속해서 인정할 것이다. 그러나 연역된 것은 그것이 속한 분야에서 일반적으로 승인(general acceptance)되었음이 충분하게 확증되어야만 한다.”

(Daubert 판정법에서, 일반적인 승인(general acceptance)은 법원에서 고려해야 할 몇 가지 요소 중 하나임을 주목하라.)

조사관이 디지털 매체의 조사에서 새로운 소프트웨어나 예전 소프트웨어의 업데이트 버전을 사용하면, 그 소프트웨어에 대해 Frye나 Daubert 판정법에 근거한 이의 제기를 당할 수 있다. 조사 기술이 발전함에 따라, 전문가 증인이 증거와 사실에 관한 의견을 연역함에 따라, 법원에서 신뢰할 수 있고 적정함을 인정받기 위해 "그 연역으로부터 도출된 것은 충분히 확증되어야만 한다."

참고사항 : 4장 I, Ⅱ 절에서 언급한 것처럼 기술과 다른 전문 지식에 의존한 방법이 증거를 찾거나 파악하는데 사용되었을지라도, 그 방법에 근거한 전문가 의견이 없다면, 그 방법은 Daubert 또는 Frye의 규정에 부합하지 않는다. 게다가 컴퓨터 프로그램의 출력(예 : ATM 기록)에서 도출된 증거라는 사실만으로는 그 증거가 과학적 증거에 대한 요건을 만족한다는 것을 의미하지 않는다.

제 4 장 디지털 증거의 발표

디지털 증거가 포함된 재판은 두가지 기본적인 측면에서 일반 재판과 다르다. 첫째로, 디지털 증거의 인정과 관련된 법적 문제가 거의 항상 발생할 것이다. 이에 관한 문제는 3장 “공판 준비와 증거 규칙”에서 논의하였다. 둘째로, 디지털 증거에 대한 검사의 설명에는 복잡하거나 익숙하지 않은 용어, 문제, 개념이 수반될 것이다. 그러므로 초기 진술에서 공판동안 언급될 디지털 증거에 대한 용어와 유형을 배심원이 알 수 있도록 설명해야 한다. 면밀한 사건 발표 계획과 디지털 증거의 사용 방식은 성공적인 재판 결과의 필수적인 요소이다.

이 장은 디지털 증거가 수반된 사건의 성공적인 발표 방법에 대한 지침이다.

Ⅰ. 청중에 대한 교육

사건이 복잡하면, 소송 과정의 모든 단계에서 판사와 배심원 모두를 교육시켜라.

■ 공판 전 청문회 (Daubert 또는 Frye의 판정법에 따른 이의 신청을 포함)

■ 배심원 선정

■ 초기 변론(opening statement)

■ 증인의 증언

■ 반론 (both in making and answering them)

■ 최후 변론(Closing argument)

청중이 최소한의 능력을 보유하도록 하거나 이해시키는 것이 중요하지만, 그들을 전문가로 만들려고 시도하지 말아야 한다. 일반적인 기소 원칙은 단순하게 유지하는 것이다. 이는 본질적으로 복잡한 사건의 발표에서도 여전히 유효한 말이다.

Ⅱ. 입증 또는 반박하기 위해 무엇이 필요한가?

모든 사건은 죄목에 해당되는 요소 별로 설득력 있는 증거의 제시를 위해 각 죄목의 요소에 대한 세밀한 조사를 요구한다. 디지털 증거 사건들은 종종 증거에 대한 합당한 해석을 통해 배제할 수 있거나 배제해야만 하는 것에 대한 검사의 결정을 요구한다. 고려

해야할 핵심 질문은 다음과 같다.

■ 모든 합리적인 대안 해석을 반박할 수 있는가?

■ 모든 대안 해석을 반박할 필요가 있는가?

A. 기술적인 이상

일부 사례에서, 증거에 관한 특별한 이상 현상에 대해서 완벽하거나 충분한 해석을 하지 못하는 경우가 있다. 어떤 경우에는 컴퓨터 프로그래머 또는 전자 공학자에 의해서 이상 현상을 설명하기 위해 필요한 비용이 엄청나게 많아 현실적으로 조사하지 못할 수도 있다.

컴퓨터와 운영체제가 점점 복잡해짐에 따라, 대부분의 네트워크 관리자와 컴퓨터 유지보수 직원들은 가장 자주 발생하는 문제를 해결하는 것으로 자신의 직무를 한정한다. 컴퓨터 전문가는 컴퓨터에 의해 저장되거나 처리되는 정보의 유효성에 대한 의심 없이 설명하기 힘든 “버그” 또는 “결함”의 존재를 받아들인다.

B. 대안에 대한 반박

검사가 반박해야 하는 대상은 관련된 문제와 그것이 사건의 다른 부분에 미치는 중요도에 따라 선정한다.

아동 음란물 소지와 같은 사건처럼 결정적인 요소가 대상 음란물에 대해 알고 있는 지에 관한 것일 때, 검사는 피고가 알지 못한 상태에서 피고의 컴퓨터에 그 음란물이 저장되었다는 변론에 반박하기 위한 준비를 해야 한다. 그러나 검찰은 불합리한 대안에 대해서는 반박할 필요가 있다. (예 : 전원의 서지가 컴퓨터상에 아동 음란물을 나타나게 했다.)

C. 적시성

변론에 대한 반박 시기가 중요하다. 예를 들면, 컴퓨터 상의 콘텐츠에 대한 피고의 인지 여부가 결정적이라면, 검찰 측 최초 변론(case-in-chief)에서 설명하기 보다는 반대 심문 또는 재반박을 통해 피고에게 증거를 제공하고 그 문제를 먼저 제기하도록 한 후 피고 측의 주장을 반박하는 것이 현명하다. 종종 배심원은 변호사가 문제를 제기하고 검사가 반박하는 것보다 검찰이 제기한 문제를 훨씬 중요하게 생각하고 검사에게 더 높은 기준을 요구한다.

Ⅲ. 전문가 증인과 기술적인 증거

A. 기술적인 전문가 증인의 필요 여부 결정

복잡한 기술과 디지털 증거에 대한 광범위한 조사가 수반된 사건에서 전문가 증인의 채택 여부는 중요한 결정이다. 여기서 전문가 증인은 특별한 교육, 지식, 경험이 있는 자를 말한다.

증인이 의견을 제시한다고 하면, 반드시 적격한 전문가이어야 한다. 일부 사건에서, 증인이 의견을 제시하지 않는다면, 전문가 자격에 대한 검증 없이 복잡한 문제에 증언할 수 있다. 또한 판사들은 의견을 제시하는 증인에 관해 각기 다른 기준을 가지고 있으며, 기술적인 증언을 할 경우, 전문가 자격을 요구할 수 있다.

디지털 증거를 수반한 많은 사건에서, 현장 수사관 또는 조사관은 디지털 증거가 어떻게 발견되었는지 증언할 수 있다. 비록 조사관이 전문 기술과 기교를 사용할지라도, 그와 관련된 재판에서의 문제는 해당 증거의 발견 방식이 아니라, 해당 증거가 용의자의 컴퓨터 상에 존재했는지 여부이다.

전문가가 기술적 또는 다른 특별한 지식에 따른 기법에 근거한 의견을 제시하지 않는다면, 비록 그러한 지식이 증거를 찾고 확인하는데 사용되었을지라도, 그 기법은 3장에서 논의한 Daubert 또는 Frye 규정에 부합하지 않는다. 예를 들면, 금속 탐지기는 범죄 현장에서 소모된 탄약통을 찾는데 사용되지만, 금속 탐지기의 기술은 검증할 필요가 없다. 한번 탄약통이 발견되면, 수사는 탄약통에 집중된다. 디지털 증거를 수반한 사건도 이와 유사하다.

B. 기술적인 사실 증언과 전문가 의견 증언의 효과적인 사용

비록 위의 예와 같이 금속 탐지기를 사용한 탄약통이나 탄환의 발견 방식에 대한 전문가의 설명이 필요 없어도, 발사화기와 toolmark 조사에서는 특정 탄환의 강선 흔적이 용의자의 무기로부터 발사된 탄환과 일치되는 지에 대해 적격한 전문가의 의견이 요구될 것이다. 유사하게 디지털 증거 사건에서도 간혹 전문가 의견 증언이 필요하다.

C. 적격한 기술 전문가 단체 파악

비록 디지털 증거 조사에 대한 전문가가 다른 인정된 분야의 화려한 권위는 부족하다고 할지라도, 그럼에도 불구하고 충분한 자격이 있을 수 있다. 사실상, 실무에 기반한 능력이 학위나 잘 알려진 전문가 그룹의 회원이라는 자격 보다 우수할 수 있다. 전문가 자격이 무엇이든지 간에, 전문가로써 증언하는 문제에 관한 지식과 이해를 설명할 준비를 하라. 수사를 도와주고 재판에서 증언할 검찰 측 전문가를 선택할 때, 파악된 전문가 단체에 관련 분야의 전문 기술이 존재하는지, 전문가 후보가 그 단체에서 어떻게 평가되는지 판단해야 한다.

D. 사건의 쟁점과 유용한 증거 조사에 대한 법적 한계에 대한 설명

검사는 증거 규칙과 절차가 증거 인정, discoverability, 전문가 관찰과 결론의 유용성에 어떤 영향을 주는 지를 전문가가 이해하고 있는지 확인해야 한다.

전문가는 검찰의 증거 분석과 재판을 진행하는 것보다 사법 거래(plea bargain)가 좀 더 적합한 지 결정하는데 도움을 줄 것이다.

E. Daubert gatekeeping challenge 대처 계획

검찰은 Daubert 또는 Frye 이의 제기 회의를 위하여 미리 증인을 준비해야 한다.(상세한 것은 3장 참조) 비록 이러한 유형의 이의 제기가 보통은 공판 전(pretrial)에 있지만, 증거 인정과 신뢰성 문제로 재판 과정 중에도 발생할 수 있다.

F. 재판을 위한 증인 준비

디지털 증거에 관해 증언할 증인을 준비시키는 것은 일반 사건에 대한 것 뿐만 아니라 특별한 문제점도 고려할 필요가 있다. 다음은 명심해야 할 사항을 열거한 것이다.

1. 직접 심문을 위한 준비

   a. 전문가는 소송의 전 과정에서 객관적인 역할을 유지하고 진상조사자(factfinder)를 도와야 한다.

   b. 검사는 모든 관련 자료(예 : 경찰 보고서, 포렌식 기록물, 공판 기록, 변론 자료)의 사본을 증인에게 제공해야 한다.

   c. 검사는 자격과 증언을 검증하는 공판 전 청문회(예 : a Daubert hearing)에 대비하기 위해 증인을 준비해야 한다. 또한 배심원 앞에서 그의 자격, 의견, 의견에 대한 이유에 대해 증언하게 될 것임을 상기시켜야 한다.

   d. 검사는 증인에게 피고 측이 접촉해 보면 알려 줄 것을 요청해야 한다.

   e. 검사는 직접 심문에서 증언을 간단하게, 이해할 수 있게, 관심을 끌 수 있게 준비하도록 증인에게 권하여야 한다. 아마도 “이야기체(storytelling)”로 말하는 것이 도움이 될 것이다.

   f. 검사는 증인에게 직접 심문 과정에서 받게 될 질문을 알려줘야 한다. 증인은 사용할 전시물, 필요한 시청각 장비, 증언의 근거가 되는 책자나 논문 등을 검사에게 말해야 한다.

g. 증인은 증언 준비를 위해 사용한 또는 증언 과정에서 사용할 모든 자료가 피고 측에게 제공된다는 것을 알아야 한다.

h. 증인은 모든 기술 용어와 약어를 쉽게 설명해야 한다. 예를 들면, “나는 MD5 해쉬 알고리즘을 포렌식 이미지에 적용하였고, 그 해쉬 값은 변경되지 않았습니다. 이것은 복사본에 있는 모든 파일이 원본에 있는 해당 파일과 일치한다는 것을 의미합니다.”

i. 증인은 받은 질문에 대해 변호사가 아니라 배심원에 직접 증언해야 한다.

j. 검사는 증인에게 판사가 증언의 범위와 성격을 제한할 수 있다는 것을 설명해야 한다. 증인은 예심 법정(trial court)에서 설정된 한계 내에서 증언해야 할 것이다.

k. 검찰의 일원으로 활동한 수사관도 객관적인 태도로 증언해야만 한다. 편파적으로 보이는 것을 방지하려면, 증인은 증언하는 동안 자신의 몸짓, 음성의 크기, 얼굴 표정 등을 포함하여 자신의 전체적인 태도를 인식해야 한다.

2. 반대 심문을 위한 준비

a. 증인은 반대 심문에 대해 절대로 호전적이지 않아야 한다. 호전적 태도는 배심원과 소원해지며 증언의 효과를 약화시킨다.

b. 증인은 “증언이 자신에 관한 것이 아니라 증거에 관한 것이다.”라는 것을 염두에 두어야 한다.

c. 변호사는 유도 심문성 질의를 하면서 반대 심문 과정을 제어할 것이다. 질문에 대한 답변을 피하거나 피하는 것으로 보이지 마라. 증인은 질문이 암시하고 있는 것(implied question)에 대해서가 아니라 묻는 질문(asked question)에 답변해야 한다. 다음은 그 예이다.

변호사 : “증인은 증거보관실에 예약하고 3일 후에 컴퓨터를 받은 것이 사실입니까?”

증언자 : 네

또는

증언자 : “예, 원하시면 이유를 설명하겠습니다.”

하지만 다음처럼 하지 마라

증언자 : “나는 휴가갈 예정이었고, 그 부서는 시간외 근무에 대한 허가를 거부하였다, 그리고 ... ”

d. 증인은 절대로 변호사와 맞서려고 하지 마라. 증인의 태도는 직접 심문과 반대 심문 과정에서 동일해야 한다. 증인이 피고라기보다는 재판 중이라고 느껴진다면 변호사와 맞서려고 하는 징후이다. 증인은 재판 전에 검사가 재심문 과정에서 보다 많은 질문에 답할 기회를 줄 것임을 상기해야 한다. 만약 검사와 증인이 함께 일했다면, 검사는 반대 심문 이후에 어떻게 진행하는 것이 최선인지 알아야 한다.

3. 반박 준비

가끔 피고는 정부가 제공한 디지털 증거를 다루기 위해 자신의 증인을 요청하기도 한다. 이러한 증인은 최고로 능력 있는 전문가일 것이다. 일부의 경우에는, 관련된 모든 데이터에 접근하지 못한 적법한 포렌식 업무의 전문가일 것이다. 또는 포렌식 실무 경험이 없는 “직업적(professional)” 피고 측 증인일 수 있다. 피고 측 증인이 증언한 후에, 검찰 측 증인은 증언 내용을 반박하기 위해 소환될 것이다. 이러한 것을 재판 전에 예상하고 대비해야 한다.

Ⅳ. 컴퓨터 범죄 재판에서 자주 발생하는 문제

비록 각각의 디지털 증거 사건이 서로 다르지만, 일부 공통적인 문제가 범죄 죄목의 기본 요소와 컴퓨터 및 컴퓨터 망의 특성 둘 다에서 발생한다.

A. 신원 확인(Identity)

디지털 증거로 범죄가 피고의 컴퓨터에서 저질러졌다는 것을 보일 수 있어도, 검찰은 그 컴퓨터와 피고를 직접 연결할 필요가 있다. 다음을 포함하여 몇 가지 방법을 통하여 컴퓨터에서 발견된 증거와 피고를 직접적으로 연결할 수 있다.

1. 자백 또는 시인

2. 정황(예 : 피고는 컴퓨터가 있었던 곳의 유일한 거주자이고, 하드웨어 또는 소프트웨어의 사용자로 등록됨)

3. 피고만이 알고 있는 컴퓨터 상의 실질 정보

4. 콘텐츠 분석 : 증거의 문법, 맞춤법, 또는 다른 특성과 피고가 작성한 문건 사이의 특징적인 유사성이 존재

B. 인지

일부 사건에서, 컴퓨터 상의 디지털 증거를 피고가 인지하고 있음을 보여야 한다. 예를 들면, 아동 음란물 소지 사건에서 공통되는 변론 중 하나는 피고가 컴퓨터에 있는 이미지를 알지 못했다고 주장하는 것이다. 이 같은 주장은 종종 다음과 같이 반박할 수 있다.

1. 발견된 이미지의 개수

2. 디렉토리 구조. 사진들이 논리적으로 관련된 디렉토리에 있는가? (예 : C:₩Pictures ₩young₩girls₩sex)

3. 파일명. 파일명이 유일하고, 파일의 내용을 정확하게 나타내고 있는가? (예 : 8yrold.jpg, baby.jpg)

4. 가입한 뉴스 그룹이나 인터넷 활동 이력과 같은 아동 음란물에 관해 피고가 관심을 갖고 있다는 컴퓨터 상의 다른 징후

C. 사건 발생 일지

파일의 타임스탬프는 피고와 컴퓨터, 컴퓨터와 범죄를 연결하는 강력한 증거가 될 수 있다. 그럼에도 불구하고 시간과 날짜 스탬프는 다음과 같은 한계가 있다.

■ 스탬프의 정확도는 컴퓨터 내부 시계의 정확성에 의존한다.

■ 특정 시간대(time zone)와 연결되어 있다

■ 쉽게 조작할 수 있다.

시간과 날짜 스탬프의 정확도는 다음을 포함하여 여러 방법으로 보일 수 있다.

1. **오프셋의 일관성.** 파일이 일관되게 특정 크기의 시간이나 날짜만큼 사용되지 않았는가?(예 : 항상 1 시간 또는 2 일간 끄기) 만약 그렇다면, 시간과 날짜는 정확한 일시를 나타내며, 오프셋에 의해 파일의 일시를 조정할 수 있다는 주장은 설득력이 있다.

2. **내부 파일의 정확도.** 파일의 일시가 해당 파일의 내용과 일치하는가? 예를 들면, 편지 파일의 날짜 스탬프와 편지의 서두에 있는 날짜가 일치하는가?

3. **이메일 헤더의 일자와 시스템에서 부여한 시간 및 날짜 스탬프의 비교.** 이메일을 개별 파일로 저장하거나 한 파일에 복사하는 이메일 시스템에서 이메일 헤더의 일시 정

보와 파일에 부여된 시스템의 시간과 날짜 스탬프가 일치하는가?

4. **알려진 일시와 시스템 일시의 비교.** 알려진 일시에 피해자의 컴퓨터에서 다운로드된 파일이 있는가? 용의자의 컴퓨터에 있는 그 파일의 시간과 날짜 스탬프가 알려진 일시와 일치하는가?

5. **네트워크로 연결된 컴퓨터.** 많은 네트워크에서 클라이언트가 로그온할 때 클라이언트의 내부 시계가 자동으로 업데이트된다. 네트워크에 클라이언트 컴퓨터가 연결되었는가? 클라이언트 컴퓨터 내의 시계가 네트워크를 통해 자동으로 업데이트 되는가?

6. **파일 생성 시간 및 날짜 패턴.** 동일한 일시에 생성된 파일의 집합이 있는가? 상대 일시(즉, 동일한 시간에 모두 생성됨)가 생성된 절대 일시 보다 중요할 수 있다.

7. **실험.** 용의자의 하드웨어에 원본 드라이브를 교체한 후, 파일을 생성하고 변경하라. 불일치되는 부분을 관찰하고, 증거 파일과 비교하라.

참고 사항 : 컴퓨터 범죄 수사에 대한 자세한 내용은 이 시리즈의 다른 지침서를 참조하라.:

■ *Electronic Crime Scene Investigation: A Guide for First Responders* (www.ojp.usdoj.gov/nij/pubs-sum/187736.htm).

■ *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (www.ojp.usdoj.gov/nij/pubs-sum/199408.htm).

■ *Investigations Involving the Internet and Computer Networks* (www.ojp.usdoj.gov/nij/pubs-sum/210798.htm).

Ⅴ. 배심원 선정

검사는 복잡하거나 고도의 기술적인 증거의 용인이 필요한 컴퓨터 범죄 사건에 최선의 배심원이 구성되도록 신중하게 고려해야 한다. 수사관은 적절한 질문서 개발과 배심원단의 구성과 소환된 개별 배심원의 검토를 위해 검사를 도울 수 있다.

목표는 기술 전문가를 배심원으로 선택하는 것이 아니라, 공판 과정 중에 발표해야만 하는 기술적 증언을 이해할 정도로 컴퓨터 사용에 충분한 경험이 있는 적어도 소수의 사람을 찾는 것이다. 이상적으로는 사건 설명 이후 협의 과정 중에 일부 배심원이 다른 배심원에게 증거에 대한 이해를 돕는 것이다.

A. 배심원 선정

사건에 따라, 배심원 예비 심문 중에 잠재적인 배심원에 대한 중요한 정보를 다음과 같은 질문에 대한 답으로부터 수집할 수 있다.

1. 컴퓨터 모니터나 프로젝션 스크린의 자료를 검토하기 어려운 시각적인 장애가 있는가?

2. 컴퓨터에 대한 지식과 경험 수준은 어느 정도인가?

3. 디지털 증거에 대한 감각이 있는가?

4. 기소된 특정 범죄에 관해 강력한 견해가 있는가?

5. 컴퓨터 범죄의 피해자, 특히 비즈니스 피해자에 대해 일부 과실이 있는 것으로 보는가?

6. 배심원의 지식과 인터넷, 이메일, 기타 사건 관련 컴퓨터의 특정 측면에 대한 경험 수준이 얼마인가?

7. 기소한 것과 유사한 범죄의 피해를 입은 배심원이 있는가?

8. 배심원들이 자신의 컴퓨터에 사용하는 보안 수단은 무엇인가?

9. 침해 사건에서, 네트워크로 연결된 컴퓨터의 위험에 대한 생각과 프라이버시에 대한 견해는 무엇인가?

B. 배심원 풀에서 컴퓨터 전문가에 대한 특별 고려사항

컴퓨터 전문가가 배심원으로 선택될 필요는 없다. 배심원에 컴퓨터 전문가가 있는 것은 의료 관련 증언에 의사가 배심원으로 있는 것과 유사하다. 의사가 복잡한 의료 개념을 설명할 수 있는 것처럼, 컴퓨터 전문가도 동료 배심원에게 정보 기술의 문제를 명확하게 설명할 수 있을 것이다. 그러나 배심원으로 있는 의사가 검찰에게 기소 사건을 과도하게 증명할 것을 요구하고 중요하지 않은 문제에 대해 반박하는 것처럼, 컴퓨터 전문가도 제시된 증거를 자신의 지식으로 대체하고 포렌식 조사 및 분석에 관한 심의 과정을 주도할 수도 있다.

Ⅵ. 복잡하고 기술적인 문제의 발표

다음은 복잡한 디지털 증거 또는 복잡한 사건을 설명하는데 유용한 방법에 관한 것이다.

A. 기술적인 용어와 개념을 배심원이 이해할 수 있도록 정의

일반적인 개념을 설명하기 위해 유사한 비유를 사용하라. 예를 들면, 이메일을 엽서 보내는 것으로 비유하고, 메일 박스를 한 우체국의 우편함에서 수신자가 있는 우체국을 거친 후 수신자의 우편함으로 전달되는 것으로 설명할 수 있다. 그러나 디지털 세계는 실세계와 다르기 때문에, 비유가 효과적이지 않을 수 있음을 주의해야 한다. 비유를 하게 되면, 실세계 상황이 왜곡되어서 결국 비현실적이 될 수도 있다. 결과적으로 비유하고자 했던 익숙한 상황이 익숙하지 않게 될 수 있다.

더욱이 비유의 사용은 예기치 못한 법적 결과를 초래할 수 있다. 예를 들면, 판례에 근거한 비유는 디지털 증거에 대해 부적합한 법적 제약을 가져올 수 있다.

예를 들어, P2P 파일 공유를 전통적인 도서관으로 비교한 경우를 생각해 보자.

■ 각 책은 무제한 공급된다.

■ 책을 반환할 필요가 없다.

■ 도서관 이용자는 자신의 책을 도서관에 가져다 놓을 수 있다.

■ 도서관 이용자는 대출한 책을 가질 수 있고, 자신의 도서관에 비치해 다른 이용자가 이용할 수 있다.

P2P 파일 공유를 익숙한 도서관에 빗대어 정확히 설명하려던 노력이 이상하고 생소한 도서관을 창출하게 되었다. 비유에 필요한 특성을 추가하면 의도한 유사성을 약화시켜서 궁극적으로는 그 자체를 말한 것 외에는 소득이 없을 수 있다.

B. 복잡한 시스템 또는 개념을 설명하기 위한 사진, 그림, 그래프 사용

C. 초기 변론(opening statement)과 후속 증인의 증언을 통해 배심원의 지식 개발

1. 배심원에게 단순한 개념을 소개하고, 그러한 개념을 자세히 설명하여 이해시킨 후 좀 더 복잡한 문제로 이동하라.

2. 가능하다면, 배심원 예비 심문(voir dire)에서 파악된 배심원이 익숙한 또는 사용한 기술과 사건에 있는 기술을 연결시켜라.

D. 발표를 위한 기술적 도구 재검토

사용할 발표 도구에 관한 결정은 많은 요소에 의해 좌우되지만, 가장 중요한 것은 발표 도구의 숙달 정도와 적정한 발표 준비와 검증에 필요한 시간이다. 그러나 배심원이 젊거나 도구에 기반한 발표에 익숙하면, 시청각적, 멀티미디어적인 발표를 기대할 수 있음을 명심해야 한다.

발표 도구를 사용한다면, 다음의 사항을 명심하라.

1. 컴퓨터가 아니라 증인 및 배심원과 대화하라. 이것이 재판의 모든 단계에서 지켜져야 하겠지만, 배심원과 직접적으로 대화하는 최초, 최후 변론에서 가장 중요하다.

   a. 가능하다면 컴퓨터를 조작해 주는 사람을 준비하라.

   b. 컴퓨터 모니터가 아닌 배심원을 바라봐라.

2. 슬라이드의 의도에 따라, 슬라이드에 있는 정보를 직접 사용하지 않을 때에는 스크린을 어둡게 처리하라.

   a. 재판 중에 오랜 시간 동안 스크린에 발표물을 띄워 놓을 것을 고려하라.

      (1) 배심원이나 증인이 시간이 지남에 따라 발표물을 언급할 수 있다는 것은 중요하다.

      (2) 발표물의 지속적인 디스플레이는 반대하지 않는 감정적인 효과를 유발할 수 있다.

   b. 최후 변론 또는 기타 시간에 배심원이 검찰과 증인이 말한 것에 집중하도록 스크린을 어둡게 하라.

3. 단순히 사용할 수 있기 때문이 아니라 특정 목적을 위해 발표 소프트웨어를 사용하라. 다음이 그 예이다.

   a. 그래픽, 애니메이션, 특수 효과를 보여주는데 적합한 소프트웨어 (연관성 있는 내용인지 확인)

   b. 복잡한 발표에서 구성을 보여주거나 유지

   c. 드라마틱한 효과

d. 시각적 효과 이용

e. 배심원의 주의를 집중

f. 한마디 한마디씩 증거를 보여 주는 것이 효과적일 때 (예 : 배심원에게 이메일의 내용을 읽어주어야 하는 경우)

4. 틀린 방법으로 발표 소프트웨어를 사용하지 마라.

a. 단순히 화면에 있는 것만을 읽지 마라.

b. 최후 변론의 요점 정리를 위해 발표 소프트웨어를 사용하지 마라.

c. 다음의 경우를 제외하곤 글이 많은 슬라이드를 사용하지 마라.

(1) 배심원이 해당 문장을 읽을 필요가 있는 경우

(2) 문장에 핵심 사항이 있는 경우

d. 배심원이 읽을 틈도 없이 슬라이드를 빠르게 넘기거나 일부를 숨기지 마라. 모의 디지털 증거 재판에서 배심원들은 변호사가 문서의 일부만 밝게 하고 나머지는 어둡게 하거나 화면상에서 문서를 빠르게 깜박이게 하면 무엇인가 감추려 한다는 의심을 표현한다.

5. 기본 발표 원칙을 지켜라.(항상 예외는 존재)

a. 개요와 내용에서 일관성을 유지하라.

b. 슬라이드 당 10초 이상, 100초 이하의 시간을 할애하라. (만약 슬라이드 중간에 대화할 필요가 있다면 화면을 어둡게 하라.)

c. 스크린에 보이는 색상을 이용하라. (컴퓨터 모니터에 보이는 색상이 스크린에 제대로 나타날 것으로 생각하지 마라.) 어떤 연구에 의하면 약간 어두운 조명에서 진한 파랑 배경에 밝은 파랑 글자색이 가장 읽기 쉽다고 한다.

d. 충분히 큰 글자체 사용

e. 복잡하거나 색상이 다양하거나 또는 글자체가 독특한 슬라이드를 사용하지 마라.

Ⅶ. 최후 변론

A. 일반적인 주의사항

최후 변론을 준비할 때 기억해야 할 핵심 사항은 다음과 같다.

1. 사건의 주제 요약

   a. 초기 변론에서 명확히 말한 사건의 주제를 최후 변론에서 다시 한 번 언급한다.

   b. 최후 변론에서 모두 발언과 종료 발언을 가져라. 발언된 말 중에 처음과 마지막 단어가 가장 많이 기억된다.

   c. 우선 배심원이 기억해야 하는 것이 무엇인지 인지하라.

2. 배심원에 대한 설명을 생각

   a. 핵심 부분에서 배심원에 대한 설명과 주장을 연결하라.

   b. 교육 과정 중에 증명하지 않고 언급한 것을 배심원에게 정확히 말하라.

3. 최후 변론의 “비수(thrus)” 결정

   a. 최후 변론의 주요 목적 중 하나는 복잡하게 보이는 것을 단순하고 명확하게 만드는 것이다.

   b. 끝내면서 어떻게 감동을 주어야 하는가?

   c. 범죄의 중요성을 강조한다.

   d. 변호인 측 변론의 취약점을 공격한다.

4. 다음의 질문에 답함으로써 피고 측 주장에 대처할 방식을 결정

   a. 피고 측 주장에 답변해야 하는 것은 무엇이며, 배심원의 검토 과정 중에 제공해야 하는 유리한 정보는 무엇인가?

   b. 피고 측 주장에 모두 응답해야 하는가? 아니면 가장 관련 있는 것만 중점적으로 다룰 것인가?

   c. 관련 없다고 생각되는 피고 측 주장을 어떻게 취급할 것인가? 무시하는가, 관련이

없다고 배심원에게 말한 것인가, 또는 관련성 없음을 설명하여 기각시킬 것인가?

d. 관련 없는 주장을 단지 언급함으로써 주의를 끌었는가?

e. 관련 없는 주장을 짧게 언급함으로써 피고 측 주장이 약해졌는가?

5. 반박 결정

a. 안건에 따라야 하는가? 피고 측 주장에 하나씩 대응하라.

b. 피고 측 주장에 적절히 대응하기 위한 주제 별 반박을 준비하는데 충분한 시간이 있는가?

c. 안건에 따라 진행된다면, 피고 측 주장을 무시하지 마라.

d. 건건이 대응할 때조차도 주장의 마지막에 검찰 측 주제로 복귀할 수 있는 부분을 준비하라.

B. 디지털 증거 사건에서 최후 변론을 할 때 기억해야 할 핵심 사항

1. 비디지털 증거를 보강해 주도록 디지털 증거를 제시한다.

2. 사건의 더 복잡한 문제와 증거 재검토

a. 배심원은 증거를 이해하기 위해 기술에 정통할 필요가 없음을 상기하라.

b. “증인의 교육”이 올바르게 수행되었다면, 검사가 부연 설명할 필요는 없을 것이다.

3. 배심원이 새로 익힌 기술적 지식 관점에서 핵심 증거의 중요성을 설명하고 명확하지 않은 것을 연결하라.

4. 배심원이 상당한 컴퓨터 지식 또는 경험을 가지고 있다면, 최후 변론 동안에 설명된 중요한 증거와 배심원을 연결하라.

a. 배심원이 설명에 동의하는지 판단하라.

b. 배심원이 설명에 동의하는 것 같다면, 기술적 설명을 완벽히 이해하지 못한 다른 배심원이 동료 배심원에게 설명을 요청할 수 있게 말할 것을 고려하라.

제 5 장 적용 사례 : 아동 음란물 사건

아동 음란물과 아동 성적 착취 사진과 영상(집합적으로 “이미지”)을 소지한 자들은 인터넷의 가장 어두운 측면에 해당된다. 아동 음란물 사건을 수사하고 기소할 때, 필연적으로 피고가 사용한 컴퓨터에서 발견된 이미지는 증거만이 아니라 수사의 실마리가 된다.

그러한 사람들 다수가 아동 음란물 수집가이고, 그들의 컴퓨터와 디지털 저장 매체에서 보통 수백 개 또는 심지어 수천 개의 이미지들이 발견된다. 일부 이미지들의 출처나 대상 아동들의 신원에 대한 정보는 수사가 진행되는 동안 확인된다. 그러나 일부 이미지들은 슬프게도 전 세계 수많은 익명의 아동 피해자들 사진이 한 범죄자에서 다음 범죄자에게 계속해서 전달된다는 것을 보여준다.

그들 중 일부는 컴퓨터에 아동 음란물을 소지하는 것을 넘어서, 그러한 행위를 시도하거나 실제로 물리적인 성폭행이나 아동 학대와 같은 행위를 저지른다. 아동에 대한 물리적인 행위가 포함된 사건의 증거에 대한 논의는 이 지침서의 범위 밖이다.

아동 음란물 수사에는 종종 기술, 컴퓨터, 인터넷에 대한 지식이 많은 사람이 참여한다. 그들은 예를 들면 웹 사이트, 파일 공유, 이메일, 버디 리스트, 패스워드로 보호된 파일, 또는 암호 등을 사용하여, 전 세계의 다른 수집가와 이미지를 거래한다.

이러한 인터넷의 하위 문화에 대한 기초적인 이해를 하는 그 곳의 회원인 자가 수사관과 검사에게 특정 사건을 검토하고 기소할 수 있게 상황을 잘 이해할 수 있도록 도와 줄 것이다. 음란물 사건의 경험이나 특별한 훈련을 받은 법집행기관 수사관뿐만 아니라 ‘실종 및 착취 아동을 위한 국립 센터’와 같은 수사 자원이 검사에게 많은 도움을 줄 것이다.

Ⅰ. 고려사항 : 수사 단서와 포렌식 증거

컴퓨터 장비를 사용하거나 수리하는 동안 컴퓨터나 저장 매체에 아동 음란물이 있다는 것을 알게 된 제 3자가 법집행기관에 고발하여 아동 음란물 수사를 시작하는 경우가 많다. 또는 아동을 대상으로 하는 범죄자를 겨냥한 비밀 온라인 수사의 부산물인 경우도 있다. 용의자가 비밀 요원에게 아동 이미지를 보내는 경우가 있다. 어떤 경우에는 수사관이 용의자의 컴퓨터와 매체를 압수한 후, 후속 포렌식 조사에서 아동 이미지가 발견될 수도 있다. 시작이 무엇이든, 컴퓨터 사용 환경과 피고에 대한 상세한 배경에 대한 후속 수사는 재판에서 결정적인 증거를 제공할 것이다.

검찰의 시각에서, 이런 사건들은 발견된 이미지가 전부는 아니다. 피고나 컴퓨터에 접근한 다른 사람들의 사용 습관을 밝혀내는 광범위한 포렌식 조사와 분석은 이미지의 소유와 묘사된 것에 대한 인식을 입증하는데 도움을 줄 것이다. 이 때문에, 포렌식 조사관은 재판에서 중요한 증인이 될 것이다.

포렌식 조사는 전부는 아니지만 다음과 같은 증거로 사건을 기소할 수 있게 해 줄 것이다.

■ 인터넷 브라우저 히스토리와 입력된 URL.

■ 가입한 웹 사이트

■ 이메일 내용

■ 파일 공유 및 P2P 소프트웨어, 사용 히스토리, 사용 흔적

■ 인스턴트 메시지

■ 친구 목록(buddy lists)

■ 파일과 연관된 시간/날짜 스탬프

■ 폴더와 디렉토리 구조 (즉, 이미지나 데이터의 “경로”)

■ 대화명(screen names), 이메일 주소, 온라인 신원

■ 원격이나 외부의 파일 저장 위치 (물리적이나 가상적)

■ 로그온-로그오프 내역

■ 인터넷 서비스 제공자(ISP) 정보

■ 아동 취미에 관련된 금융이나 다른 개인 정보

■ 유죄가 되는 이미지의 **메타데이터**

후속 수사로 전부는 아니지만 다음과 같이 재판에 유용한 증거를 찾을 것이다.

■ 이미지들이 신원을 증명할 수 있는 아동들로부터 나온 것인지의 여부 (예를 들면, 실종 및 착취 아동을 위한 국립 센터 또는 미국 출입국 및 세관에 의해 관리되는 데이터베이스)

■ 이미지에 나타난 아동의 실제 신원에 관한 증인의 법정 증언

■ 피고가 다양한 대화명이나 신원으로 인터넷(예 : 웹 사이트, 뉴스 그룹, 게시판 서비스)에 게시한 기록이 있는 지 여부

■ 이메일 계정의 ISP 계정 정보를 통한 신원 확인 또는 관련 주소

Ⅱ. 고려사항 : 기소

아동 이미지 사건에서 검사의 중요한 기소 결정은 후속 재판에 상당한 영향을 끼칠 것이다. 기소 결정에 대한 실제적인 접근 방식은 최소한 합법적이거나 증거 가치에 이의 제기할 수 있는 이미지(예 : 비디오나 스틸 이미지, 알려진 피해자 시리즈, 미상 아동의 연령 판단 근거, 보여진 행동의 성격, 얼굴과 신체의 다른 부분의 전시 형태, 이미지의 배경)와 배심원에서 가장 큰 충격을 줄 수 있는 이미지에 근거할 것이다.

그래서 아동 음란물 사건의 검사는 많은 이미지들 중에서 기소 근거로 사용하는 것을 결정하기 때문에, 실체적인 면과 전술적인 면 모두를 고려하여 결정할 것이다.

A. 실체적인 고려사항

■ 이미지들이 아동 음란물이나 음란물로 정의한 법에 부합하는가?

■ 발견된 이미지 중 어느 것과 어느 정도를 기소의 근거로 사용할 것인가?

■ 적절하게 피고의 관련성을 입증할 증거가 있는가? 예를 들면, 피고의 집이나 직장의 컴퓨터에서 발견된 이미지인가? 또는 그것들이 CD-ROM이나 플래시 메모리 드라이브와 같은 외부 매체에서 발견되었는지 그리고 그 매체들은 어디서 발견되었는가?

■ 기소 조항은 어떻게 구성할 것인가?

- 이미지에 따라

- 사건에 따라 (예 : 다운로드 일시)

- 저장 매체에 따라 (예 : 디스켓, 하드 드라이브, thumb drive, CD, DVD)

■ 얼마나 많은 조항으로 기소할 것인가? 관할 지역 법이 개별 조항의 나열을 허용하는가? 또는 다중성 또는 중복성 문제가 있는가?

■ 증거는 이미지가 실제 아동을 나타냈다는 것을 입증하는가?

■ 소지만 한 사건인가 또는 배포나 선전한 증거가 있는가?

■ 사건이 완결된 범죄와 달리 시도한 것만으로도 기소되어야 하는가?

B. 전술적인 고려사항

■ 어떻게 사건을 과도한 형량 없이 배심원에게 최대의 영향을 주어 기소하여야 하는가?

■ 기소되지 않은 이미지와 다른 관련된 데이터가 신원 확인, 의도, 인지, 소유권, 통제, 실수나 과실의 부재 등에 대한 증거로 인정될 수 있는가?

- 피고가 컴퓨터를 통해서 연락하는 유사한 취미가 있는 자들의 대규모 모임과 연결되어 있다는 증거가 있는가?

- 피고가 수집가 이상의 존재라는 것을 암시하는 증거가 있는가? (예를 들면, 피고에 의한 실제로 물리적 성폭행이나 학대를 당한 미상의 아동 피해자에 대한 증거)

- 피고와 관련된 성향을 증명하는 다른 증거(예 : 성적 지향 잡지나 비디오 테이프, 인터넷 검색 엔진 히스토리, 외설적인 의류)가 발견되었는가?

- 컴퓨터와 컴퓨터 기술에 관한 피고의 지식 수준에 관한 증거로는 무엇이 있는가?

- 피고가 컴퓨터나 매체 상에 이미지를 보관했다는 것을 보여주는 증거로는 무엇이 있는가?

■ 비디오 이미지들은 좀 더 명확하게 불법행위의 요소를 입증할 수 있다.

■ 선택된 이미지들이 기소된 불법 행위를 적절하게 나타내는가? (예를 들면, 이미지가 성행위를 직접 나타내는가? 아니면 단지 성행위를 암시하는 것인가?)

■ 얼굴이 보이는가?

■ 선택된 이미지들의 개수와 성격이 범죄 요소와 관련된 가능한 변론에 대처하기에 타당한가? (예를 들면, 10개의 이미지가 변경되었다고 주장하는 것보다 100개의 이미지가 변경되었다고 주장하는 것이 훨씬 어렵다. 다른 고려사항으로 수많은 다른 이미지에 같은 아동이 나타나는지 여부일 수 있다.)

참고사항 : 특별한 고려사항으로 대배심원 절차에 영향을 주는 것이 있다. 관할 지역의 절차는 다양하지만, 판례는 대배심원에게 이미지를 설명하는 것보다 보여 주는 것이 최선의 방법이라는 것을 암시한다. 대배심원과 재판에 제출되는 이미지들(또는 이미지에 대한 설명) 사이의 차이는 사건에 치명적일 수 있다.

Ⅲ. 고려사항 : 배심원 선택

아동 음란물 사건에서 죄과와 증거는 큰 견해 차이가 있을 수 있기 때문에, 배심원 선택 과정은 중요하다. 일부 진보적인 배심원은 아동 음란물을 문화적으로 수용할 수 있거나 피해자가 없는 범죄로 인식할 수도 있다. 게다가, 미래의 많은 배심원들은 컴퓨터 기술과 포렌식 증거를 이해하지 못할 수도 있다. 언어, 컴퓨터, 인터넷, 그리고 연방, 주, 또는 지방 정부 법규에 관해 탐구하는 태도로 디지털 증거를 믿을 수 있는 배심원을 선택해야 한다. 마지막으로 아동 음란물 사건에 접할 준비가 된 배심원인지 확인해야 한다.

Ⅳ. 고려사항 : 재판

아동 음란물 사건의 재판에서 검사는 법정에서 (공개 재판인 경우는 다른 참석자를 포함해서) 배심원에게 공개되고 검토되는 증거물을 어떻게 통제할 것이지 생각해야 한다:

■ 이미지들이 개별적으로 또는 다른 방법으로 인쇄되는가?

■ 각 배심원을 위한 복사본과 더불어 판사와 판결 기록원을 위한 복사본이 있는가?

■ 이미지들이 컴퓨터나 프로젝터를 통해 배심원에게 디스플레이 되는가?

■ 공개 법정에서 증거를 제시하면서 방청인에게 보이거나 혹은 보이지 않게 적절한 통제를 할 수 있는가?

■ 이미지들이 상소 심리를 위해 어떻게 보존할 것인가?

이러한 고려사항에는 이미지가 제시될 때의 형식과 크기뿐만 아니라 배심원 협의실에서의 취급 방식까지도 포함된다. 또한 검사는 원본과의 관련성, 크기를 고려해야 한다.

Ashcroft v. Free Speech Coalition, 122 S. Ct. 1389 (2002) 사건(아동에 대한 노골적인 성적 이미지에 대한 연방 법의 금지조항은 헌법적으로 오직 “실제” 아동을 대상으로 한 이미지에 대해서만 적용될 수 있다는 판결)에 대한 미국 대법원의 결정 이후, 대부분의 법정은 이미지 검토를 결정하기 위해 사실인정자(trier of fact)가 사실에 입각해 질문하도록 단순하게 문제를 규정함으로써 Ashcroft 판결에 대응하고 있다. 그러나, 소수의 법정에선 검찰에게 이미지 그 자체와 이미지에 나타난 아동들이 컴퓨터에 의해 생성된 것이 아니라 실재 인물임을 확언하는 증거의 제출을 요구하고 있다. 만약 이런 관점의 증거가 요구되면, 훈련된 수사관, 의료인, 디지털 이미지 기술자, 또는 (“알려진” 시리즈를 통해) 아동의 실제 신원을 증언할 수 있는 수사관, 디지털 이미지 기술 출현 이전에 존재한 이미지임을 입증할 수 있는 자 등이 가능한 증인일 것이다.

참고사항 : 이 분야의 많은 사람들이 미래의 어느 시점에서는 실제 아동들의 이미지와 컴퓨터로만 생성된 아동 이미지를 구별하는 것은 아주 어려운 문제로 증거 입증의 장애가 될 것이라고 예상하고 있다.

또한 법정별로 입증해야만 하는 아동의 나이가 다양하다. 대부분 법정들은 이미지에 근거하여 결정할 사실인정권자(trier of fact)가 사실에 입각한 질문을 하도록 단순하게 문제를 규정한다. 그러나 소수의 법정은 검사에게 이미지 그 자체와 이미지에 나타난 아동의 나이를 확언하는 증거의 제출을 요구한다. 만약 법정이 나이에 대한 특정 증거를 요구한다면, 경험이 풍부하거나 훈련받은 의료인(예를 들면, 소아과 의사나 간호사)을 이용할 수 있다.

Ⅴ. 만장일치

만장일치 요구사항은 지방자체 단체의 규정에 따라 다양하다. 만약 여러 이미지들이 단일 기소조항의 근거를 형성한다면, 배심 재판에서 특별 평결 양식을 제공할 필요가 있거나 그렇지 않으면 배심원이 만장일치로 이미지들이 법을 위반한 것으로 결정하고 평결에서 이러한 이미지들을 명확하게 확인한다는 것을 보장할 필요가 있다.

Ⅵ. 고려사항 : 피고 측에 의한 개시

아동 음란물은 금지품이기 때문에, 적절한 통제와 처리, 접근 제한은 항상 고려되어야 한다. 피고 측 개시 과정 동안 법적 보호 명령(judicial protective order)이나 각서(stipulaion)의 사용을 강력히 권고한다. 사건이 종결되었을 때, 금지품을 반환하면서 검찰은 디지털 와이핑(wiping)이나 파괴하는 적정한 절차를 시행해야 한다.

부록 B. ECPA의 공개 규정

	자발적인 공개가 허용되었는가?		강제적인 공개 메커니즘	
	공개 사업자	**사설 사업자**	**공개 사업자**	**사설 사업자**
기본 가입자, 세션, 과금 정보	§2702(c) 예외 적용이 아니면 국가에 불가 [§2702(a)(3)]	허용됨 [§2702(a)(3)]	소환장, 2703(d) 명령, 수색 영장 [§2703(c)(2)]	소환장, 2703(d) 명령, 수색 영장 [§2703(c)(2)]
다른 처리내역과 계정 기록	§2702(c) 예외 적용이 아니면 국가에 불가 [§2702(a)(3)]	허용됨 [§2702(a)(3)]	2703(d) 명령, 수색 영장 [§2703(c)(1)]	2703(d) 명령, 수색 영장 [§2703(c)(1)]
사업자 또는 다른 저장 파일로 남겨진 접근한 통신 (열람한 이메일과 음성 메일)	§2702(b) 예외 적용이 아니면 허용 불가 [§2702(a)(2)]	허용됨 [§2702(a)(2)]	통지가 있는 소환장, 통지가 있는 2703(d) 명령, 수색 영장 [§2703(b)]	소환장; ECPA는 적용되지 않음 [§2711(2)]
이메일과 음성 메일(180일 이상 전자 저장소에 있었던)을 포함한 열람되지 않은 통신	§2702(b) 예외 적용이 아니면 허용 불가 [§2702(a)(1)]	허용됨 [§2702(a)(1)]	통지가 있는 소환장, 통지가 있는 2703(d) 명령, 수색 영장 [§2703(a, b)]	통지가 있는 소환장, 통지가 있는 2703(d) 명령, 수색 영장 [§2703(a, b)]
180일 이내의 열람되지 않은 이메일과 음성 메일을 포함한 통신	§2702(b) 예외 적용이 아니면 허용 불가 [§2702(a)(1)]	허용됨 [§2702(a)(1)]	수색 영장 [§2703(a)]	수색 영장 [§2703(a)]

주의: 이러한 조항들의 법정 해석은 다를 수 있다.

부록 C. 동의(허가)서 양식 예

예 1: 수색 동의서

(미국 메인 주 컴퓨터 범죄 담당 기구의 수색 허가 양식을 번안함)

나는 _____ 기관의 모든 직원과 법집행기관의 담당관 _____에게 다음에 명시한 항목에 대한 수색을 동의 및 허용한다.

나는 다음에 기술된 항목에 대한 접근, 소유, 감사, 조사, 수색할 수 있는 권한과 능력을 가지고 있음을 분명히 확인한다.

나는 다음에 기술된 항목에 대한 수색을 거부할 권리를 가지고 있다는 것을 알고 있다. 나는 어떠한 위협, 강요, 계약이나 권유 때문이 아닌, 나 자신의 자유 의지에 따른 행위로서 자발적으로 이 수색에 대해 동의한다. 나는 더욱이 이 동의서에 서명하기 위한 강요나 권유하는 위협이나 계약 등이 없었음을 확인한다.

나는 다음에 기술된 항목들의 수색에 의해 발견된 어떠한 항목, 이미지, 문서, 기타 다른 증거들이 법정에서 증거로 사용될 수 있음을 알고 있다.

수색 대상(설명, 등록 번호 등):

_____

_____

_____

_____

_____

_____

_____

이 양식에 서명함으로써, 나는 이 문서의 전체적인 내용들을 읽고 이해했음을 확인한다.

이름 : (인) 날짜 :

담당관 이름 (인) 날짜 :

예 2: 수색 허가서

나 _____는 _____에 의해 다음과 같은 장소, 차량, 물품에 대한 수색에 동의한다.

집/사업장 주소
1.) _____ 2.) _____
_____ _____
_____ _____

이 동의는 위에서 명시한 사항에 딸린 모든 마당, 주차장, 차고, 별채, 저장소, 헛간, 쓰레기통, 편지함도 포함한다.

차량
제조사/모델 _____
년도/면허증 _____

제조사/모델 _____
년도/면허증 _____

나는 이 동의가 적합한 도구와 기술을 이용하여 조사할 수 있는 안전한 시설로 모든 컴퓨터, 하드 드라이브, 기타 전자 저장 매체(CD, DVD, 플로피 디스크, Zip® 디스크, Jaz® 카트리지, 스마트 미디어 카드, 컴팩트 플래시, 메모리 스틱 등)의 이동을 허가한다는 것을 알고 있다.

이름 : (인) 날짜 :

담당관 이름 (인) 날짜 :

예 3: 추가 수색 허가서

나의 동의로 압수된 컴퓨터, 하드 드라이브, 그리고 다른 전자 저장 매체의 수색을 하는 _____의 담당자나, 다른 지방, 주 또는 연방 법집행기관의 직원들에 협조하기 위해, 나는 다음과 같은 정보를 제공한다.

스크린 세이버 / BIOS 패스워드

다른 패스워드 / 사용자명

프로그램 / 서비스	사용자명	패스워드

암호화 키

공개키	개인키

서명 :

예 4: 추가 수색 허가서

(인터넷 서비스 제공자 / 웹 기반 이메일)

나, _____는 _____ 의 담당자나 다른 지방, 주, 또는 연방 법집행기관의 직원이 나의 인터넷 서비스 제공자나 웹 기반 이메일 제공자에 의해 저장된 모든 폴더(송신, 수신, 휴지통 등)안에 있는 모든 전자 메일에 관한 내용들을 접근, 열람, 다운로드, 인쇄, 복사하는 것에 동의한다. 이 수색에 협조하면서, 나는 자유롭고 자발적인 의사로 다음과 같은 계정명, 사용자명, 그리고 패스워드를 제공한다.

인터넷 서비스 제공자	사용자명	패스워드

이 허가는 열람, 다운로드, 복사, 인쇄 목적에 대한 접근을 단 한 번으로 제한되며, 아래에 적혀진 날짜와 시간의 48시간 후에 만료된다.

_____	_____	_____
서명	날짜	시간
_____	_____	_____
증거 / 법 집행 담당자	날짜	시간

부록 D. 피고에게 반환되는 증거에 관한 각서

판사 _____가 _____일자에 서명한 수색 영장 #_____에 의해 인가된 기록물이나 다른 증거의 압수 수색을 신속히 처리하기 위하여, 또한 _____의 정상적인 전산 업무에 대한 방해를 최소화 하기 위하여 _____와 첨부된 물품명세서에 나열된 기록물, 장비, 증거에 적용되는 다음 조항을 약정한다.

_____는 _____일자에 만들어진 포렌식 복사본이나 백업이 완전하고 그 날짜에 수색된 시스템 전체 내용의 완벽하고 정확한 복사본이라는 것에 만족한다.

_____는 백업/포렌식 복사본에서 복사, 인쇄, 도출된 모든 기록의 정확성, 신뢰성, 또는 출처에 어떠한 이의도 제기하지 않을 것이다.

_____는 백업/포렌식 복사본에서 복사, 인쇄, 도출된 모든 기록에 대한 최선 증거, 진정성, 또는 근거에 대한 이의 제기를 철회한다.

부록 E. 용어

에이전트(Agent): 디지털 증거를 포함한 형사 및 민사 사건에 사법관할권(jurisdiction)이 있는 기관의 이해관계를 위해 일하는 사람. 대부분의 사법관할권과 환경에서 에이전트는 법집행기관의 직원일 것이다. 그러나 에이전트는 형사 및 민사 사건의 수사를 하는 자를 위해 일하는 적당한 자격의 민간인일 수도 있다.

친구 목록(Buddy list): 개인 컴퓨터나 휴대 전화에서 "인스턴트 메시징"을 하는 대화 상대자들의 대화명 모음,

복사(Copy (v.)): 전자 저장 장치와 무관하게(예 : 논리적 파일 복사), 본래의 물리적인 물건에 포함된 정보를 정확하게 재생산하는 것. 재생산 과정 중에 내용(컨텐츠)은 유지하지만, 속성은 변할 수 있다.

디지털 증거(Digital evidence): 법정에서 신뢰할 수 있는 이진 형태로 저장되거나 전송된 정보.

기록물(Documentation): 범죄 현장, 복구된 증거, 현장 수색과정에서 취해진 행동을 상세히 기록한 필기 노트, 오디오 테이프, 비디오 테이프, 인쇄된 형태, 사진.

복제(Duplicate): 디지털 저장 장치(예 : 하드 드라이브, CD-ROM, 플래시 메모리, 플로피 디스크, Zip®, Jaz®)에 포함된 모든 데이터의 정확한 디지털 재생산. 내용(컨텐츠)과 속성(예 : 비트 스트림, 비트 복사, 그리고 섹터 덤프)이 유지된다.

디지털 증거 복제(Duplicate digital evidence): 원 물리적인 대상에 포함된 모든 데이터 객체의 정확한 디지털 재생산.

ECPA: 이 지침서에서는 Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq. 의 저장된 통신 장을 지칭함.

전자 기기(Electronic device): 전자 작용 원리로 작동하는 기기.

전자 증거(Electronic evidence): 전자 기기에 의해 저장되거나 전송되는 수사할 가치가 있는 정보와 데이터.

암호화(Encryption): 데이터의 정당한 수신자를 제외한 모든 사람이 읽지 못하도록 평문을 암호문으로 변환하는 암호 기술을 사용하는 모든 과정.

최초 출동자(First responder): 현장에 도착하여 초기 대응을 하는 법집행기관 직원이나 다른 공공안전 직원.

FRE: 연방 증거 규정.

High-technology crime: 컴퓨터 범죄, 컴퓨터 관련 범죄, 인터넷 관련 범죄를 포함한 컴퓨터 기술이 사용된 범죄.

ISP: 인터넷 서비스 제공자. ISP는 가입자에게 인터넷에 접근할 수 있게 해주는 기관이다. 소규모 ISP들은 모뎀과 ISDN(Integrated Services Digital Network)를 통하여 서비스를 제공하는 반면, 대규모 ISP들은 전용선(예 : T1, T1의 분할)을 제공한다.

메타데이터(Metadata): 데이터에 관한 데이터.

네트워크(Network): 정보와 자원을 공유하기 위해 서로 연결된 컴퓨터 그룹.

서버(Server): 네트워크를 통해 연결된 다른 컴퓨터에게 특정 서비스를 제공하는 컴퓨터.

스니퍼(Sniffer): 네트워크 패킷을 감시하고 패스워드, 신용카드 번호, 기타 등을 포함한 데이터를 가로채기 위해 사용될 수 있는 소프트웨어.

Special master: 증거적(evidentiary)으로나 증언 특권(testimonial previlege)으로 보호해야 할 파일, 데이터 또는 다른 증거들이 포함된 사건에서 파일, 데이터 또는 다른 증거를 보호해야 하는지(수사관에게 공개되지 않음) 아니면 보호하지 않아도 되는 지(수사관에게 공개됨)를 결정함으로써 판사를 돕는 준 사법 역할을 하는 법원에서 지정한 독립 개인

Taint team (or privilege team): 사건 수사팀이나 기소 팀에 공개되기 전에 증거적(evidentiary)으로나 증언 특권(testimonial privilege)으로 보호해야 할 파일, 데이터 또는 다른 증거인지 결정하기 위해 사건에 독자적으로 참여하여 피고 측을 위해 일하는 정부 수사관과 변호사. 논란의 여지가 있는 피고 측에서 제기한 특권에 관한 주장이 있는 사건에서, Taint team과 피고는 수사팀이나 기소 팀의 구성원 없이 기밀 방식으로 그 문제를 법원에 가져올 수 있다. Taint team의 구성원은 “윤리적 벽(ethical wall)”에 의해 사건 수사와 기소팀으로부터 독립되어 있고 법정 외에는 업무에 대한 논의가 금지되어 있다.

사실인정자(Trier of fact): 법정 사건에서 사실을 결정하는 자. 배심 재판에서는 배심원이 Trier of fact이다. 배심원이 없을 때(종종 “bench trial"이나 ”trial to the court"라고 불림)는 판사가 Trier of fact이다. 배심이 있든 없든 간에 사건에서 법으로 판단하는 것은 판사가 한다.

URL: Universal Resource Locator.