이학석사학위논문

참여권 보장을 위한 전자정보 압수·수색 집행 방안에 관한 연구

2016년 2월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공
김 광 호

참여권 보장을 위한 전자정보 압수·수색 집행 방안에 관한 연구

지도교수 이 상 원

이 논문을 이학석사 학위논문으로 제출함

2015년 11월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

김 광 호

김광호의 석사학위논문을 인준함

2016년 1월

위 원 장 이 광 근 (인)

부 위 원 장 이 상 원 (인)

위 원 백 윤 흥 (인)

국 문 초 록

현대인의 일상생활은 컴퓨터, 인터넷, 스마트폰 등의 디지털 기기들을 통해 점차 정보시스템 안으로 들어가 있다. 이런 변화들로 인해 현대인의 생각과 행위가 전자정보로 기록되어 남게 되었다. 기존의 유체물에서는 발견할 수 없었던 방대하고 세세한 정보들이 전자 증거로 사용할 수 있게 된 것이다. 2011년 형사소송법 개정에서는 전자정보를 증거로서 수집하기 위한 “원칙적 선별압수, 예외적 매체압수” 압수방법이 규정되었다. 전자정보의 수집 시 기존 유체물의 압수·수색과는 달리 정보의 대량성으로 인해 혐의사실과 관련 있는 정보뿐만 아니라 그와는 전혀 무관한 정보들이 대량으로 압수될 우려가 있고 피압수자의 사생활 침해를 유발할 수가 있다.

전자정보의 압수·수색 과정에서 범죄와 무관한 막대한 정보가 수집될 수 있으므로, 이로 인한 침해를 방지하기 위한 강력한 사법통제가 요구되고 있다. 형사소송법 제106조에서 관련성에 관한 내용이 추가되었지만 요구되는 사법적 통제가 충분하지 못하고, 전자정보의 구체적인 증거 수집절차도 충분하지 못하다. 지속적으로 전자정보의 증거 수집 절차 등에 대한 입법적 공백에 대해 논의하고 연구하여 체계적이고 구체적인 입법이 시급히 필요하다.

현재 전자정보의 압수·수색 절차에 대한 입법의 미비는 대법원 판례를 통해 입법공백이 일부분 채워지고 있다. 대법원 판례는 전자정보의 ‘압수’ 개념을 기존 압수물과 다르게 ‘저장매체를 반출하여 혐의사실과 관련된 정보를 탐색·복사·출력할 때’까지의 전 과정으로 보고 있고, 압수의 전 과정에 지속적인 피압수자의 참여권 보장을 적법요건으로 제시하여 이를 준수하여야 한다고 판시하였다. 뿐만 아니라 수사기관 사무실에서 저장매체의 전자정보 탐색 과정에서 피압수자의 참여권 미보장, 혐의사실

관련 구분 없는 재복제, 혐의사실과 무관한 정보 출력 등을 중대한 위법 처분으로 판단하고 영장에 기한 압수·수색 전체를 취소하는 판결을 내렸다.

그러나 이 같은 대법원의 전자정보 압수·수색에 대한 적법요건을 실무 현실을 고려하지 않고 기계적으로 해석하였을 경우 수사기관의 전자 증거 수집을 매우 어렵게 하는 결과를 초래할 위험이 있어 실체적 진실 규명을 통한 형사 사법의 정의 실현을 어렵게 할 수 있는 문제점이 있다.

본 논문은 각각의 어려움이 있는 피압수자의 권익보호와 형사 사법 정의 실현이 조화를 이루고자 하는 목표를 가지고 압수·수색 과정별로 어떠한 방식으로 참여권을 보장하여야 하는지에 대해 방안을 제시하였다. 또한 수사기관이 피압수자가 배제된 상태에서 저장매체 내 전자정보에 대한 열람 및 복제나 출력 등을 방지하는 위한 방안으로 저장매체 내 전자정보에 대한 사용 이력 관리 체계 방안을 제안하였다. 이를 위해 전자정보의 특성, 전자정보의 압수·수색 방식, 전자정보의 수집 및 분석 방법을 살펴보고 압수수색 절차에서의 참여권 범위, 참여권 보장 관련 대법원 주요 판례 등을 검토하였다. 이를 통한 궁극적으로는 전자정보의 압수·수색에 있어서 보다 체계적이고 실효성 있는 법규가 형성되는 것에 도움이 g 되기를 바란다.

주요어 : 참여권, 전자정보, 압수수색, 집행

학 번 : 2014-24854

목 차

1. 서론

증거는 형사절차상 사건의 실체적 진실을 발견하고 구체적인 국가의 형벌권을 발동하는데 있어 사건의 진위를 명백히 하기 위한 사실인정의 근거자료로서 중요한 의미를 갖는다. 이러한 증거의 존재형태는 범죄의 태양에 따라 다르나 전통적인 의미에 있어서 증거방법은 유형물로 제한되어 왔다. 그러나 과학기술의 발달로 인하여 첨단정보통신기술을 이용하는 범죄가 증가하면서 과거에는 전혀 예측할 수 없었던 새로운 증거형태가 출현하게 되었는데 그것이 바로 전자 증거이다.[1)]

현대사회는 컴퓨터와 인터넷 등 과학기술의 발달로 각종 전자 증거가 기하급수적으로 증가하고 있다. 실무에서도 과거 진술증거에 의존하던 수사는 피의자, 참고인 등의 비협조 등으로 말미암아 압수수색의 결과로 취득한 전자 증거의 중요성이 더욱 커지고 있다. 즉, 형사절차에서 전자증거의 중요성은 날로 증가하고 있는 것이다.

그럼에도 불구하고 우리 형사소송법은 여전히 물리적 증거만을 주로 예상하여 규정하고 있을 뿐, 기존의 물리적 증거에서는 예상하기 어려웠던 전자정보의 압수·수색 과정에서 참여의 보장 범위, 전자 증거의 증거능력 등과 관련한 법적, 제도적 장치는 아직까지 미비한 상태이다.

한편, 대법원은 전자정보의 압수수색과 관련된 다수의 판례들을 통해 정보저장매체에 대한 압수·수색영장 집행 시 영장에서 인정한 예외적인 사정으로 정보저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우, 전체 과정을 통하여 피압수·수색 당사자나

1) 탁희성, “법정에서 전자 증거의 허용가능성”, 한국전자포렌식학회, 「전자 포렌식 연구」 창간호(2007. 11.), 24쪽.

변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 정보저장매체에 대한 열람·복사 금지 등 압수·수색 대상인 정보저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하다고 천명하였고 압수수색영장 집행의 일부 과정에서 참여권 미보장, 혐의사실 관련 구분 없는 재복제, 혐의사실과 무관한 정보 출력 등을 이유로 전체 압수·수색 처분을 취소하였다.

최근 종근당 사건의 대법원 전원합의체 결정을 보면 법원으로부터 발부받아 집행한 압수·수색 과정 중, 피압수자에게 참여권을 보장하지 않고 혐의사실 관련성에 대한 구분 없이 재복제하는 중대한 위법 처분을 하여 전체 압수·수색이 위법한 것으로 판결됨으로써 수사기관에서는 적지 않은 혼란이 있었다. 이와 같은 혼란이 재발하지 않도록 법 규정과 대법원 판례, 그리고 수사현실을 고려한 전자정보의 압수·수색 절차가 시급히 필요하다고 보인다.

따라서 본 논문은 과학기술의 발달로 인하여 형사절차에서 그 중요성이 크게 증가하고 있는 전자 정보가 기존의 물리적 증거와는 다른 특성을 가지고 있음에 따라 수사기관 실무상 압수수색 절차와 관련하여 검토하고, 수사기관에서의 전자정보 압수·수색 영장 집행 방식을 살펴볼 것이고, 수사실무에서 활용하고 있는 전자정보의 증거 수집 기법인 안티 포렌식 기법들을 조사하여 압수·수색 실무에서 어떤 과정이 있는 지를 알아볼 것이다. 한편, 최근 대법원 전원합의체 결정를 통해 전자정보의 압수·수색 영장 집행 시 참여권 보장과 관련한 경향을 검토한 후 대법원 전원합의체 결정과 수사실무 현실 사이에 발생하는 괴리를 해소하면서 피압수자의 참여권이 보장되는 전자정보의 압수·수색 방안을 제시하였다. 또한 대법원

판례는 수사기관이 압수 현장에서 반출한 저장매체를 피압수자가 배제된 상태에서 열람 및 임의적 복제나 출력을 막기 위한 적절한 조치가 이루어져야 한다고 판시하였다. 이를 위한 방안으로 저장매체 내 전자정보에 대한 사용 이력 관리 체계를 도입하는 것을 제안하였다.

2. 전자정보의 특성

전자증거가 기존의 물리적 증거와는 달리 매체독립성, 비가시·비가독성, 취약성, 대량성, 전문성, 네트워크 관련성 등의 특징을 가지고 있다.[2] 이러한 특성들을 파악하고 그에 따른 문제점을 정리한다.

이와 같은 특성으로 인해 전자정보의 압수수색 절차, 압수한 전자정보의 증거능력 등과 관련하여 기존의 물리적 증거와 달리 취급하여야 할 필요성이 제기된다.[3]

가. 매체독립성

전자정보는 유체물이 아니고 각종 디지털 저장매체에 저장되어 있거나 네트워크를 통하여 전송 중인 정보 그 자체를 말한다. 전자정보는 저장매체와 독립된 정보의 내용이 증거로 되며 이 정보는 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 지니는 것이다.[4]

이러한 특성에 따라 전자정보는 원본과 사본의 구별이 곤란하고, 이에 수사기관은 정보저장매체 원본의 훼손을 방지하기 위해 이미징 사본을 이용하여 전자 정보를 분석하고 이미징 사본에서 출력한 문건을 증거로 제출하고 있다. 위 과정에서 디지털 저장매체 원본과 이미징한 사본의 동일성의 문제가 발생한다.[5]

---

2) 대검찰청, 「검찰수사 실무전범Ⅱ」(2008), 261-264쪽; 손지영.김주석,「디지털 증거의 증거능력 판단에 관한 연구」, 대법원 사법정책연구원(2015), 25-29쪽; 전승수, “형사절차상 전자정보의 압수수색 및 증거능력에 관한 연구”, 서울대학교 박사학위논문(2010), 12-15쪽 등 참조

3) 최성필, “디지털 증거의 증거능력”, 검찰 포털 발표자료

4) 양근원, “형사절차상 전자정보의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위논문(2006), 22쪽; 권양섭 “디지털 증거수집에 관한 연구”, 군산대학교 박사학위 논문(2009), 11쪽.

나. 비가시성, 비가독성

전자 정보는 사람의 육안으로는 식별이 불가능하기 때문에 정보저장 매체를 제시하는 것만으로는 증거가 되는 내용을 확인할 수 없고, 그 내용을 모니터 상에 나타내거나 출력장치를 통해 종이 등으로 인쇄하여 제시하였을 때 비로소 가시성, 가독성이 주어진다.[6)]

전자정보 그 자체는 가시성·가독성이 없는 매체독립적인 정보이므로 법정에 증거로 제출되기 위해서는 가시성·가독성이 있는 형태로 변환하여 제출하게 되는데, 과연 위 출력물을 원본으로 인정할 수 있는가 하는 원본성의 문제가 대두된다.[7)]

다. 취약성(변개 용이성)

물리적 증거의 경우 증거물을 조작하면 조작 흔적이 남게 되므로 조작 여부를 비교적 쉽게 판별할 수 있으나, 전자 정보는 하나의 명령만으로도 수많은 디지털 자료를 삭제하거나 변경시킬 수 있고 자료의 일부만을 쉽게 조작할 수도 있다.[8)] 즉 전자정보는 위·변조 및 삭제가 용이하다는 취약성의 특성이 있다.

따라서 전자정보를 수집할 경우에 수집 이후부터는 전자정보가 변조되지 않았다는 것을 입증할 수 있도록 무결성을 확보하는 절차와 기술이 필요하고,[9)] 여기에서 전자정보의 무결성 문제가 제기된다.[10)]

---

5) 대검찰청, 앞의 책, 262쪽.
6) 양근원, 앞의 논문(각주 3), 23쪽.
7) 대검찰청, 앞의 책, 317쪽.
8) 권양섭, 앞의 논문 12쪽 참조.
9) 탁희성.이상진,「디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보 방안」, 형사정책연구원(2006), 36쪽.

라. 대량성

정보저장매체의 저장기술 발달로 인하여 하나의 매체가 저장할 수 있는 데이터의 양이 상당히 확대되었다. 따라서 방대한 데이터 중 범죄관련성 있는 정보를 선별하는 작업 자체가 용이하지 않다는 문제점을 가진다.

따라서 압수수색 영장의 특정 및 집행 범위와 관련한 문제가 발생하고, 대량의 데이터가 대규모로 저장・전송・처리되는 만큼 저장매체를 압수하여 분석하는데 강력한 성능을 가진 시스템이 필요하고 장기간의 시간과 전문적인 지식이 소요되는 경우가 자주 발생한다.[11] 또한 압수한 전자정보의 검색, 분석 등의 과정에서 장시간이 걸리므로 어느 범위까지 참여권을 보장하여야 하는지에 대한 문제가 제기된다.

마. 전문성

디지털 방식으로 자료를 저장하고 이를 출력하는 데는 많은 컴퓨터 기술과 프로그램이 사용된다. 따라서 저장된 자료가 어떤 소프트웨어를 사용하여 저장되었는지 정확하게 규명하지 않으면 자료에 접근하기조차 어려운 문제가 발생한다. 또한 접근하여 수집된 자료라 할지라도 이를 가독성・가시성 있는 자료로 제시하고 그 내용을 해석하는 데는 해당 분야에 대한 전문적 지식 없이는 불가능한 경우가 많고, 법정에 제시된 최종 산출물이 원본 증거에 대한 정확한 해석인지 검증하는 것도 필요하다.[12]

따라서 전자정보의 수집과 분석에 있어 디지털 포렌식 전문가의 도움이 필수적으로 필요하고, 여기에서 전자정보에 대한 신뢰성 문제가 대두된다.[13]

---

10) 김윤섭,.박상용, “형사증거법상 전자정보의 증거능력”, 형사정책연구 제26권 제2호 (2015), 170쪽.
11) 양근원, 앞의 논문(각주 4), 138쪽
12) 양근원, 앞의 논문(각주 4), 139쪽

바. 네트워크 관련성

정보통신기술의 발달로 현재의 디지털 환경은 수많은 컴퓨터가 상호 연결되어 있는 네트워크 환경을 맞이하고 있으며, 전자 정보는 유무선 네트워크를 통해 시간과 공간, 국경의 벽을 넘어서 저장・전송・처리된다.[14] 또한 전자정보는 단순히 저장매체에 저장되어 있는 경우뿐만 아니라 통신 중에도 수집되어야 하는 경우가 있다.

기본적으로 압수수색은 장소의 개념을 전제로 하고 있는데 반해, 네트워크 환경에서는 장소의 개념이 무의미하다. 국내의 토지관할을 넘어서는 법집행을 어느 정도까지 인정할 것인지가 문제되고, 더욱이 국경을 넘는 경우에는 국가의 주권 문제까지 연관될 수 있다. 또한 본사는 서울에 있지만 지방에 메인 서버를 두고 서울 본사와 지방의 각 지사를 네트워크로 연결하여 중요 자료를 저장・공유하는 경우에, 회사의 전자메일, 회계자료, 영업자료 등을 압수하기 위해서는 압수수색 장소를 본사 외에도 메인 서버의 소재지를 추가로 기재해야 하는 등 압수수색 장소의 특정 문제가 발생한다.[15]

13) 대검찰청, 앞의 책, 263쪽.
14) 탁희성.이상진, 앞의 책, 39쪽 권양섭, 앞의 논문, 15쪽.
15) 권양섭, 앞의 논문 15쪽 이하 참조.

3. 전자정보의 압수·수색과 참여

이번 장에서는 전자정보에 대한 압수수색 방식을 규정과 세부 절차에 대해 확인해 보고 전자정보의 수집 및 분석 기법을 검토하여 수사실무 현실을 살펴보고, 압수수색 절차에서의 참여권 보장에 대한 규정과 대법원의 전자정보 압수수색 관련 판결들의 취지들을 조사하여 전자정보 압수수색 시 참여에 대한 구체적인 사례들을 살펴보고자 한다.

가. 전자정보의 압수수색 방식

1) 수사기관의 전자정보 압수수색 방식

전자 증거의 압수수색 방식은 형사소송법 제106조 제3항과 수사기관 실무상으로 크게 세 가지로 나눌 수 있다.

원칙적인 압수·수색 방식으로 (1) 압수수색 장소(이하 '현장')에서 정보저장매체 등을 수색하고 정보전자매체 내 전자정보를 탐색하여 영장 기재 혐의사실과 관련한 정보만을 선별하고 이를 복사 또는 출력하는 방법이다.

현장에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 (2) 현장에서 저장매체 전체를 이미징하여 복제본을 확보하고 이를 수사기관의 사무실로 가져와 복제본을 이용하여 영장 기재 혐의사실과 관련된 정보를 탐색·선별한 후 이를 출력하는 방법과 (3) 현장에 있는 정보저장매체 자체를 수사기관의

사무실로 가져와 저장매체 전체를 이미징하여 복제본을 확보한 후 정보저장매체 원본은 피압수자에게 반환하고 복제본을 이용하여 영장기재 혐의사실과 관련된 정보를 탐색·선별하여 이를 출력하는 방법이다.

2) 전자정보의 압수·수색 방식별 세부 절차[16)]

위 세 가지 방식에 대한 검찰 수사실무에서의 주요 세부 절차는 디지털 포렌식 수사관의 증거 수집 및 분석 검찰 예규[17)]에 의해 다음과 같다.

(1) 원칙적 방식은 ① 압수·수색 사전 준비 → ② 압수·수색 현장에서 저장매체 등 수색 → ③ 저장매체에서 혐의사실과 관련된 전자정보 탐색 및 선별 → ④ 압수할 전자정보의 해쉬값 생성 → ⑤ 전자정보의 문서 출력 및 파일 복제 → ⑥ 압수 목록 교부와 압수 확인서 작성으로 압수·수색 집행이 종료된다.

예외적 방식으로 (2) 압수·수색 현장에서 저장매체 복제본을 생성하는 경우 ① 압수·수색 사전 준비 → ② 압수·수색 현장에서 저장매체 등 수색 → ③ 저장매체에서 혐의사실과 관련된 전자정보 탐색 → ④ 저장매체 원본에 대한 이미지 파일 및 해쉬값 생성 → ⑤ 이미지 파일 압수 확인서 작성 → ⑥ 디지털수사통합업무관리시스템[18)](이하 '디지털업무시스템')에 이미지 파일 등록 → ⑦ 일선 수사부서에서의 탐색 및 이미지 파일에 대한 분석 → ⑧ 분석 결과 디지털업무시스템에 등록 → ⑨ 수사부서에서의 압수 선별 및 문서 출력, 파일 복제 → ⑩ 압수 목록 교부로 압수·수색 집행이 종료된다.

---

16) 김지홍, "디지털 포렌식 절차 모델에 대한 새로운 접근", 석사학위 논문, 56쪽 참조
17) 대검찰청, "디지털포렌식 수사관의 증거 수집 및 분석 규정" [시행 2015.7.16.] 참조
18) 디지털 증거의 수집 및 분석에 관한 사항과 디지털 증거의 보관에 관한 이력 등을 관리하는 전산시스템을 말한다.

한편, (3) 압수·수색 현장에서 저장매체 복제본을 생성하는 경우 ① 압수·수색 사전 준비 → ② 압수·수색 현장에서 저장매체 등 수색 → ③ 저장매체에서 혐의사실과 관련된 전자정보 탐색 → ④ 압수할 저장매체 원본의 해쉬값 생성 및 압수 확인서 작성 → ⑤ 저장매체 원본 봉인 및 운반 → ⑥ 저장매체 원본 봉인 해제 및 이미지 파일 생성 → ⑦ 디지털업무시스템에 이미지 파일 등록 → ⑧ 일선 수사부서에서의 탐색 및 이미지 파일에 대한 분석 → ⑨ 분석 결과 디지털업무시스템에 등록 → ⑩ 수사부서에서의 압수 선별 및 문서 출력, 파일 복제 → ⑪ 압수 목록 교부로 압수·수색 집행이 종료된다.

나. 전자정보의 수집 및 분석 기법

1) 안티포렌식 대응 기법 분석[19)]

디지털 포렌식은 해킹, 사이버 범죄에서 사용되는 컴퓨터, 노트북, 스마트폰 등의 메모리, 운영체제, 애플리케이션, 네트워크 등에 존재하는 다양한 디지털 증거를 분석하므로써, 사이버 범죄의 추적과 조사에 적극 활용되고 있다. 한편, 디지털 포렌식이 다양한 환경에서 적용되고 보편화 됨에 따라 이에 대한 대응으로 안티 포렌식 도구들이 등장하고 있다. 개인이 자신의 개인정보를 삭제하거나 기업에서 중요 기밀정보를 안전하게 파기함으로서 중요 데이터 보호나 개인정보 보호를 위한 정당한 파괴 행위에 안티포렌식 도구들을 활용하고 있다. 최근에는 추적 및 증거물 획득을 원천적이고 자동화된 방법으로 막아주는 전문 제품들이 등장하고 있으며, 다양한 안티포렌식 기법들이 소개되고 있는 실정이다.

19) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지

특히,예 이들 도구를 활용하여 수사를 방해하기 위한 목적으로 증거가 될 가능성이 있는 데이터를 의도적으로 파괴하는 행위는 엄연히 범법 행위가 된다.

가) 안티 포렌식의 정의[20]

안티포렌식은 “포렌식 도구, 수사 및 수사관의 분석을 방해하기 위한 도구와 기술”로 정의한다. 즉, 디지털 포렌식 기술에 대응하여 자신에게 불리하게 작용될 가능성이 있는 디지털 증거를 훼손하거나 숨기려는 일련의 행위를 의미한다. 데이터 파괴, 데이터 암호화, 데이터 은닉, 데이터 조작, 흔적 최소화 등이 대표적이며, 포괄적으로 디지털 증거의 획득을 방해하는 모든 행위가 포함된다. 가장 일반적인 안티포렌식 행위는 수사관들이 수집할 수 없도록 증거물이 될 수 있는 데이터를 삭제하거나 훼손하는 것인데, 예를 들면 파일을 단순 삭제, 하드디스크의 파티션 삭제나 하드디스크 포맷, 파일 또는 하드디스크 암호화 도구 사용, 파일의 확장자 변경, 웹 브라우저 사용 흔적 삭제 등과 같은 행위가 해당된다.

나) 안티포렌식 기술 분류[21]

안티포렌식 기술은 디지털 증거의 분석을 방해하기 위하여 디지털 증거가 될 수 있는 데이터를 훼손하거나 숨기기 위해 사용하는 모든 방법으로, 사용하는 기법과 세부 내용에 따라 표 1과 같이 분류할 수 있다.

---

20) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지, 2쪽
21) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지, 3쪽

[표 1] 안티포렌식 기술 분류

분류	세부	내용
데이터 파괴	완전삭제	분석을 방해하기 위해 중요 데이터를 삭제하거나 훼손
데이터 은닉	암호화	데이터를 암호화하여 디지털 증거 분석을 방해
	심층암호	특정 파일에 중요 정보를 은닉
데이터 수정	조작	데이터를 수정 또는 조작하여 분석이 어렵도록 처리
흔적 최소화		사용한 안티포렌식 도구나 기법의 흔적을 제거

다) 안티 포렌식 대응 기술 분류[22)]

안티포렌식에 대한 일반적인 대응 방안은 다음과 같다. 첫째, 공격자가 데이터를 접근할 수 있는 장소에 데이터를 저장하는 방법이다. 로그를 남기거나 CD-R 또는 DVD-R 등 한번 기록하면 수정할 수 없는 읽기 전용 매체에 데이터를 저장하는 방법이다. 최근 널리 사용한는 클라우드 컴퓨팅을 활용하는 것도 좋은 방법이다. 둘째, 기존 디지털 포렌식 도구들은 안티포렌식에 대응하기에는 기능이 부족한 것들이 많은데, 이들의 기능을 개선하는 방법이다. 현실적으로 쉽지는 않으나, 새로운 방법들을 적용하여 지속적으로 기능을 개선하여야 한다. 셋째, 안티포렌식에 대응하기 위한 전문 도구들을 새롭게 개발하는 방법이다. 데이터 암호화에 대응하기 위하여 키로거(Keylogger)를 개발하여 설치하거나 네트워크 트래픽 분석을 위하여 스니퍼(Sniffer)를 보강하거나 로그를 활용하여

22) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지, 3쪽

사용자 행위를 모니터링하는 방법이 여기에 속한다. 그러나 이러한 방법은 보수적인 제약 조건이 따르거나 제한적인 환경에서만 적용할 수 있는 단점이 있다. 따라서 안티포렌식에 적극적으로 대응하기 위해서는 안티포렌식 대응 기술(Anti-Anti-Forensics)을 적용해야만 하는데, 안티포렌식 대응 기술은 다음과 같이 분류할 수 있다.

(1) 데이터 복구 방안

삭제한 데이터가 어떤 형태로든 저장매체에 남아 있다면 이론적으로 복구가 가능하지만, 안티포렌식 전용 도구를 이용한 삭제는 일반적으로 복구가 불가능하다. 데이터 복구는 물리적인 복구와 논리적인 복구로 분류할 수 있는데, 물리적인 복구는 저장매체를 파괴하지 않은 경우 복구가 가능하고 이후 논리적인 복구를 수행할 수 있다. 논리적인 복구는 안티포렌식 도구를 이용하여 데이터를 완전삭제하지 않았다면 여러 복구 기법을 동원하여 복구가 가능하다. 단, 데이터 복구율은 저장매체의 상태, 파일 시스템 유형, 데이터 저장방식에 따라 많은 차이가 존재한다.

(2) 데이터 검색 및 탐지방안

데이터 검색 및 탐지 기술은 하드디스크 및 파일 시스템 기반 조사와 파일 기반 조사로 나눌 수 있다. 첫째, 하드디스크 및 파일 시스템 기반 조사에는 Index 기반 탐색과 Bitwise 방법이 있다. Index 기반 탐색은 포렌식 도구에서 키워드에 의존하여 일반 드라이브, 이미지, 파티션 등의 모든 영역을 검색하는 방법으로, 파일 포맷과는 독립적인 조사가 가능하고 속도가 빠른 장점이 있다. Bitwise 방법은 디스크 내의 섹터나 슬랙 공간

(Slack Space)에서 찾을 수 있는 비 할당 영역에 존재하는 간단한 텍스트나 특정 표현들을 찾는 방법으로, 텍스트 뿐만 아니라 이진수 표현 검색도 가능하지만, 단편화가 심하게 되어 있는 경우 조사가 어렵다.둘째, 파일 기반 조사에는 파일 포맷 분석과 해쉬 검증이 있다. 파일 포맷 분석은 파일 시그니처(Signature)에 의존하여 원하는 대상 검색하는 방법으로, 파일 포맷에 의존하므로 파일의 이름 또는 확장자를 변경하더라도 분석이 가능하다. 해쉬 검증은 해쉬 값을 분석함으로써 해당 파일을 찾는 경우로, 이미 알려진 파일의 해쉬값은 NSRL(National Software Reference Library)의 RDS(Reference Data Set) 해쉬셋에 테이블 형태로 제공하고 있다.

(3) 암호 크래킹 방안

암호 크래킹은 암호화된 데이터의 키를 알아내어 이를 복호화하는 기법으로 암호 알고리즘으로 암호화된 데이터의 키를 무차별 대입하는 경우 많은 시간을 소요한다. 그러나 패스워드 기반 암호 체계를 사용하는 경우 복구를 위해서 크래킹 전용 도구를 사용한 사회공학 공격, 사전 공격(Dictionary Attack), 무차별 대입 공격 등을 사용할 수 있다.

데이터를 암호화할 때 AES, RSA 등 널리 사용되는 표준 암호 알고리즘을 이용하여 암호화하는 경우가 많은데, 일반적으로 이들 표준 암호 알고리즘에서는 권장하는 키 크기(AES는 128/192/256비트, RSA는 1024/2048 비트)와 IV(Initial Vector)를 사용하여 데이터를 암호화한다. 이 경우에 암호화 키와 IV를 안전한 장소에 보관하여 알아낼 수 없다면 암호 크래킹은 사실상 불가능하다. 그러나 로그온 패스워드나 파일 암호화는 대부분 사람의 기억에 의존하여 패스워드 또는 암호화키를 관리하는 경우가 많으므로, 사회공학 공격, 사전 공격 등을 사용하여 크래킹 시간을 충분히

단축할 수 있으며, 필요에 따라 전용 도구를 사용하건 직접 개발하여 암호 크래킹을 수행할 수 있다.

(4) 은닉 데이터 탐지 방안

은닉 데이터 탐지 및 분석 기법은 이미지와 같은 멀티미디어 파일 또는 문서 파일 등에 숨겨 놓은 데이터를 탐지하고 분석하는 방법이다. 대상에 따라 멀티미디어 파일 분석과 문서 파일 분석이 있다. 멀티미디어 파일 분석은 데이터를 이미지/오디오/비디오 파을 등에 암호화해 숨기는 기술인 심층암호(Steganography)를 탐지하는 방법인데, 영상 분석, 색상 분석, 통계 분석 기법을 이용한다. 문석 파일 분석은 오피스 문서 등에서 많이 사용하는 문서 파일에 은닉한 데이터, 악성 코드 등을 탐지하는 방법으로, 포맷 분석, 저장 형식 분석 기법을 이용한다.

은닉된 데이터를 탐지하는 기법으로는 영상 분석, 색상 분석, 통계 분석, 포맷 분석, 저장 형식 분석 등을 이용하여 은닉 데이터를 탐지해내거나 데이터 은닉에 사용될 수 있는 영역을 검사하는 방법을 사용한다.

(5) 물리 메모리 분석 방안

휘발성 메모리 분석은 저장매체를 이용하지 않고 메모리 영역에서만 실행되는 기법과 그 흔적을 탐지하기 위한 방법이다. 이는 물리 메모리 영역은 일반적으로 완전삭제 프로그램의 영향을 받지 않는 것으로 알려져 있기 때문이다.

메모리 관련 항목은 물리 메모리, 페이지 파일, 스왑(Swap) 파일 등이 포함될 수 있고, 구체적인 추출 대상 항목은 운영체제 정보, 프로세스 정보, 네트워크 연결 정보, 로그인 정보, 메모리 내 텍스트 정보 등이 해당한다.

(6) 기타 분석 방안

기타 분석 방법으로는 파일 내부의 시간 정보 분석, 일관선 분석, 연관 관계 분석 방법이 있다. 파일 내부의 시간 정보 분석은 어플리케이션의 의해 저장되는 파일 내부에 저장된 시간 정보를 분석하는 방법이고, 일관성 분석은 파일, 메타데이터, 로그 등의 정보를 활용하여 시간의 연속성에 따른 일관성을 분석하는 것이다. 연관 관계 분석은 확률 및 통계 기법을 적용하여 서로 다른 이벤트 사이의 연관 관계를 이용한 분석 방법이다.

2) 디지털 증거 수집도구별 기능 비교

현재 국내에서 가장 많이 사용되고 있는 현장용 디지털 포렌식 도구의 성능에 대하여 비교하였다. CFT는 검찰에서 주로 사용하는 현장용 디지털 포렌식 도구이고, HERA는 경찰청 수사관이 컴퓨터에 대한 전문지식이 없어도 디지털 포렌식 관련 업무를 수행할 수 있도록 경찰이 자체 개발한 도구이다. Encase Portable의 경우는 미국의 Guidance사가 만든 현장용 디지털 포렌식 도구이다. 아래에서 비교한 버전은 CFT의 경우 2010. 개발된 CFT10, HERA의 경우는 2011. 개발된 프로그램, Encase Portable의 경우는 2012. 버전을 기준으로 비교하였다.[23)]

23) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 37쪽.

[표 2] 현장 디지털 포렌식 도구 기능 비교[24)]

분류	지원항목	CFT	Encase Portable	HERA
파일시스템	NTFS	O	O	O
	FAT	O	O	O
	NFS	X	X	X
	EXT2	X	X	X
	EXT3	X	X	X
	EXT4	X	X	X
	HFSX	X	X	X
	UFS	X	X	X
이미지 읽기	E01	O	X	X
	DD	O	X	X
	DFI	X	X	X
이미지 쓰기	E01	O	O	O
	DD	O	O	O
	DFI	O	O	X
논리이미지	LFI	O	O	X
	TAR	X	X	O
물리 드라이브	HDD	O	O	O
	USB / Memory CARD	X	X	X
	논리 드라이브	O	O	O
정보수집	휘발성 정보 수집	O	O	O
	하드 디스크 분석	O	O	O
	메모리 정보 수집	O	O	O
	레지스트리 정보 수집	O	O	O
	인터넷 히스토리	O	O	O
	클라우드 정보수집	X	X	X
	SNS 정보수집	X	X	X
복구	삭제된 파일	O	O	O
	유실 파일	O	O	O
	비할당 영역 복구	O	X	X
	슬랙 영역 복구	O	X	X
안티포렌식 탐지	완전삭제도구 탐지	X	X	X
	파일 은닉 도구 탐지	O	X	X
	가상 드라이브, 암호화 도구 탐지	X	X	X
검색	키워드 검색, 정규식 검색	O	X	O
	비할당 영역 검색	X	X	X
	슬랙 영역 검색	O	X	X
	HWP/DOC 등 파일 키워드 검색	O	O	O
	파일 이름 검색	O	X	O

24) 임한희. 개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구. 석사학위논문. 2012. 38-39쪽.

분류	지원항목	CFT	Encase Portable	HERA
	파일 타입 검색	O	O	O
	개인 정보 검색	O	X	O
시각화	이미지 갤러리 지원	O	X	X
	문서 미리 보기	O	O	X
	헥사뷰	X	X	X
	텍스트 뷰	O	X	X
	데이터 전환	X	X	X
프로젝트	프로젝트 파일 지원	X	X	X
	북마크	O	X	X
기타	운영체제 정보	O	X	O
	사용자 정보	O	X	O
	이메일 분석	O	O	O
	웹검색	O	X	O
	메신저	X	X	O
	USB 히스토리	O	X	O
	이벤트 로그	O	X	O
	원격 사용 정보	O	X	O
	프로세스 분석	O	O	O
	해시데이터 생성 기능	O	O	O
	증거데이터 목록 출력	O	X	O

위 비교에 따르면, 분석 가능한 파일시스템의 경우 NTFS와 FAT만 지원하고 있고, 안티포렌식 도구 탐지 기능은 CFT가 지원하고 있으나, 완전 삭제 프로그램, 가상 드라이브, 암호화 프로그램, 파일 은닉 프로그램 등 다양한 안티포렌식에 대한 탐지 기능은 부족하다.

그리고 가장 중요한 기능이라고 볼 수 있는 디지털 데이터에 대한 복구 기능, 검색 기능, 유용한 정보 분석 기능이 상호간에 차이가 있고, 그 지원 정도도 다양한 현장 상황에 대응하기에는 부족하여 문제된다.[25]

25) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제37쪽.

다. 압수·수색 절차에서의 참여

1) 압수수색 절차와 참여권 관련 규정

형사소송법은 제121조(영장집행과 당사자의 참여)에서 '검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있다'고 규정하고, 이를 수사기관의 압수에 준용하고 있다(형사소송법 제219조).

압수수색 절차에서 사건관계인인 피고인이나 변호인이 참여하는 것은 공개주의를 원칙으로 하는 법원의 절차에서 사건관계인들이 참여함으로서 절차의 적정한 진행을 도모하고, 절차 과정을 봄으로써 검사는 검사대로 소추를 위한 준비를 하고, 피고인은 피고인대로 방어를 준비할 수 있도록 하는 취지이다.[26]

한편 우리 형사소송법은 피압수자의 압수수색 절차 참여를 별도 조문으로 규정하고 있지는 않으나, 압수수색영장의 집행 절차에 관한 조문들을 종합하면 피압수자로서의 지위에서 참여가 인정될 것이다. 즉 형사소송법은 압수수색영장을 집행하는 때에는 처분을 받는 자에게 영장을 제시하여야 한다고 규정하고(제118조, 제219조), 타인의 주거 등에서 압수수색을 하는 때에는 주거주 등을 참여하게 하여야 한다고 규정하고(제123조 제2항, 제219조), 나아가 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준하는 자에게 교부하여야 한다고 규정하고(제129조, 제219조) 있는 바, 이 규정들을 준수하게 되면 피압수자는 압수절차에 참여하게 될 것이다.[27] 이와 같은 피압수자의 지위에서 참여는 집행을 받는 당사자를 보호하고 영장집행 절차의 적정성을 담보하려는데 그 목적이 있다.[28]

---

26) 백형구 등, 「주석 형사소송법 I 」제4판, 한국사법행정학회(2009), 530쪽.
27) 이완규, "디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 확보 방압", 대검찰청 이프로스 게시판(2015. 8.), 11쪽.

2) 전자정보 압수·수색 관련 대법원 주요 판례

가) 전교조 본부 사무실 압수수색 사건[29]

(1) 전자정보 압수수색 영장의 예외적인 집행에 대한 적법 요건[30]

전자정보에 대한 압수·수색영장을 집행할 때에 집행현장 사정상 원칙적 방식의 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 '반출'하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장기재 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의의 원칙상 당연하다. 그러므로, 범죄혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다. 한편 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이

28) 백형구 등, 앞의 책, 533쪽.
29) 대법원 2011. 5. 26. 자 2009모1190결정 준항고기각결정에 대한 재항고(전국교직원노동조합 본부 사무실 압수수색 사건)
30) 전자정보에 대한 압수·수색영장을 집행할 때 저장매체 자체를 수사기관 사무실 등 외부로 반출할 수 있는 예외적인 경우 및 위 영장 집행이 적법성을 갖추기 위한 요건

인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.

(2) 전교조 본부 사무실의 압수·수색에 대한 준항고[31]

영장의 명시적인 근거 없이 수사기관이 임의로 정한 시점 이후의 접근 파일 일체를 복사하는 방식으로 8,000여개의 파일을 복사한 영장집행은 원칙적으로 압수·수색영장이 허용한 범위를 벗어난 것으로서 위법하다고 볼 여지가 있는데, 압수수색 전 과정에 비추어 볼 때, 수사기관이 영장에 기재된 혐의사실 일시로부터 소급하여 일정시점 이후의 파일들만 복사한 것은 나름대로 대상을 제한하려고 노력한 것으로 보이고, 당사자측도 그 적합성에 대하여 묵시적으로 동의한 것으로 보는 것이 타당하므로, 위 영장집행이 위법하다고 볼 수는 없다.

(3) 대상결정의 취지

위 결정은 전자증거 압수수색에 관하여 '원칙적 선별압수, 예외적 매체압수'원칙을 천명한 리딩케이스로서 관련성 유무를 확인하지 않은 채 일괄복사 한 압수수색은 위법하다고 볼 여지가 있지만, 수사기관의 노력과

31) 수사기관이 전국교직원노동조합 본부 사무실에 대한 압수·수색영장을 집행하면서 방대한 전자정보가 담긴 저장매체 자체를 수사기관 사무실로 가져가 그곳에서 저장매체 내 전자정보파일을 다른 저장매체로 복사하였는데, 이에 대하여 위 조합 등이 준항고를 제기한 사안에서, 위 영장 집행이 위법하다고 볼 수 없다는 이유로 준항고를 기각한 원심의 조치를 수긍한 사례

당사자 측의 묵시적 동의를 이유로 위법하다고 볼 수 없다고 하여 수사기관이 매뉴얼에 따른 압수·수색을 한 경우 선의의 항변이 가능하다는 여지를 남긴 것으로 평가 할 수 있다[32]

나) 통합진보당 내란음모에 관한 사건[33]

(1) 당사자에 대한 참여통지 규정 위반 주장

항소이유로 피고인들에 대한 모든 압수·수색절체에서 당사자에게 미리 영장 집행에 참여할 것을 통지하지 않은 위법이 있다는 것이나, 항소심 재판부는『기록에 의하면, 압수·수색 당시 국정원 수사관들이 사전에 피고인들이나 그 변호인들에게 영장 집행의 일시와 장소를 통지하지 않음은 인정되나, 영장 기재 범죄사실의 죄질이 중하고 위험성도 크며 그 법정형도 무거운 점, 압수 대상물들이 주로 문건 또는 전자정보로서 비교적 은닉이나 인멸이 용이한 점, 이 사건 압수수색 처분을 받는 당사자가 피고인들 본인이었던 점 등을 감안하면, 영장 집행 사실을 미리 통지하였을 경우 증거인멸 우려가 컸다고 보인다. 따라서 이 사건 압수·수색은 '급속을 요하는 때'에 해당하여 형사소송법 제122조 단서가 정한 사전통지의 예외사유에 해당되므로, 이를 위법으로 볼 수 없다.[34]』고 판시하였다.

32) 노명선, '디지털 증거의 압수·수색에 관한 판례 동향과 비교법적 고찰', 형사법의 신동향 통권 제43호(2014.6.) p.145이하
33) 대법원 2015. 1. 22. 선고 2014도10978 / 서울고등법원 2014. 8. 11. 선고 2014노762 / 수원지방법원 2014. 2. 17. 선고 2013고합620, 624(병합), 699(병합), 851(병합)
34) 위 2014노762 판결 p.11이하

(2) 영장 집행절차의 명확성·공정성이 없어 위법하다는 주장

항소이유로 이 사건 각 압수수색 과정에서 사전통지가 생략되는 등 당사자의 참여권이 박탈되었고, 이를 대신할 적법한 참여인의 참여도 없었으며, 절차를 집행한 수사관들이나 입회인들이 증거의 발견 장소나 경위를 밝히지 못하여, 이 사건 압수수색은 절차의 명확성·공정성이 인정되지 않아 위법이 있다는 것이다.

이에 대해 항소심 재판부는『이 사건 압수수색은 일부 절차규정 준수 여부가 문제되는 부분이 있기는 하나, 대부분의 경우 형사소송법과 형사소송규칙이 정한 절차 규정이 준수되었고, 피고인 본인이 참여하거나 형사소송법이 참여하도록 규정한 참여인들이 참여한 상태에서 진행되었다. 위 참여인들은 각 압수수색 과정에서 압수물 선별, 디지털 포렌직, 압수목록 확인 등 과정에 관여하였고, 수사관들의 처분에 이의를 제기하거나 의견을 제시하고 압수수색을 저지하기도 하는 등 실질적이고 충분한 참여권을 행사하였다. 수사관들은 형사소송법이 정한 참여인 이외에도 민간 포렌직 전문가나 경찰관 또는 국회직원 등을 입회시키기도 하였고, 압수수색 전 과정을 영상녹화하기도 하는 등 절차의 적정성을 담보하기 위하여 형사소송법 및 규칙이 정한 것 이상의 조치를 취하기도 하였다. 또한 각 압수수색 과정에서 압수된 물건들은 이 사건 혐의사실이나 피고인들과의 관련성이 인정되거나 무관하다고 단정하기 어려운 것들로서 영장이 허용한 압수의 범위 내의 것들이다. 한편, 변호인의 참여권을 규정한 형사소송법 제121조가 형사소송법 제243조의2와는 달리, 변호인을 반드시 참여하게 하여야 한다고는 규정하고 있지 않은 점, 형사소송법 제122조 단서가 급속을 요하는 때에는 피고인과 변호인에 대한 참여통지를 생략할 수 있도록 규정하고 있는 점 등을 고려할 때, 수사관들이 변호인이 참여하기 전에 피고인에 대한 일부 압수수색절차를 진행하였다고 하더라도 이를 위법하다고 볼 수 없다』고 판시하였다.[35)]

(3) 전자정보 탐색·복제·복구·복호화 과정 참여권 침해 주장

항소이유로 수사관들이 저장매체를 전부 복제하여 압수한 후 해독된 암호로 암호화된 파일을 복호화 하거나 삭제된 파일을 복구하고 영장 기재 범죄 혐의 관련 전자정보를 탐색하여 문서로 출력하는 과정 역시 영장 집행의 일환에 포함된다. 그 과정에서 피고인과 변호인에게 집행 일시·장소를 통지하지 않은 위법이 있다는 것이다.

이에 대해 항소심 재판부는『법이 정한 절차에 따르지 아니하고 수집한 압수물의 증거능력 인정여부를 최종적으로 판단함에 있어서는 실체적 진실규명을 통한 정당한 형벌권 실현도 헌법과 형사소송절차를 통하여 달성하려는 중요한 목표이므로, 형식적으로 보아 정해진 절차를 따르지 아니하고 수집한 증거라는 이유만으로 획일적으로 그 증거의 증거능력을 부정하는 것 역시 헌법과 형사소송법의 이념에 반하므로, 증거 수집과정에서 이루어진 절차 위반행위는 절차 조항의 취지와 위반의 정도, 구체적인 위반 경위와 회피 가능성, 절차 조항이 보호하고자 하는 권리 또는 법익의 성질과 침해 정도 및 피고인과의 관련성, 절차위반행위와 증거수집 사이의 인과관계 등 관련성의 정도, 수사기관의 인식과 의도 등을 전체적·종합적으로 살펴볼 때, 수사기관의 절차 위반 행위가 적법절차의 실질적인 내용을 침해하는 경우에 해당하지 아니하고, 오히려 그 증거의 증거능력을 배제하는 것이 헌법과 형사소송법이 형사소송에 관한 절차조항을 마련하여 적법절차의 원칙과 실체적 진실규명의 조화를 도모하고 이를 통하여 형사사법 정의를 실현하려 한 취지에 반하는 결과를 초래하는 것으로 평가되는 예외적인 경우라면, 법원은 그 증거를 유죄의 증거로 사용할 수 있다고 보아야 한다(대법원 2007. 11. 15. 선고 2007도3061 전원합의체 판결 참조)』고 전제한 뒤, 다음과 같은 사정을 종합하면 이 사건 압수

35) 위 2014노762 판결 p. 12 이하

수색 과정에서 수집된 증거는 복호화 과정 참여권과 관련된 절차 위반에도 불구하고 유죄의 증거로 사용될 수 있는 예외적인 경우에 해당된다고 판단하였다.

① 형사소송법 제121조, 제122조는 피고인 등의 참여권을 보장하고 있고, 집행의 일시·장소를 미리 통지하도록 규정하고 있다. 하지만, 피고인 등을 반드시 참여시켜야 한다고는 규정되어 있지 않으며, 참여권자가 불참의사를 명시하거나 급속을 요하는 때에는 참여통지를 생략할 수 있도록 규정하고 있다. ② 피고인들은 일부 압수수색 과정에는 직접 참여하기도 하였고 직접 참여하지 아니한 압수수색절차에도 피고인들과 관련된 참여인들의 참여가 있었으므로, 추후 수사기관이 압수물에 관하여 영장 기재 범죄혐의 관련 전자정보를 탐색할 것을 예상할 수 있었을 것임에도 이후 수사기관에 압수물 분석과정 등에 대한 참여권 보장을 요청하지는 않았다. ③ 통상적으로 손상된 전자정보 저장매체의 복구나 암호의 해독, 삭제된 파일의 복원 과정 등은 그 성공 가능성을 미리 예측할 수 없고, 그 방법이나 소요시간 등도 가늠하기 어려워 이러한 조치가 수반되는 정보 분석 과정의 경우 피고인 등의 참여권을 완전히 보장하기란 현실적으로 어려움이 있다. ④ 이 사건 수사관들이 피고인과 변호인들에게 복호화 과정의 집행일시와 장소를 사전 통지하지 않은 것은 영장 집행 종료시점에 관하여 나름대로 해석한 결과인 것으로 볼 여지가 있었고, 피고인들과 변호인의 참여를 의도적으로 배제하려 하였던 것으로는 보이지 않는다. ⑤ 압수된 저장매체 중 증거로 제출된 것은 추가적인 정보저장이나 내용의 변경이 불가능한 매체이거나, 객관성이 인정되는 제3자의 서명에 의한 봉인조치에 의해 보존되어 있고, 그 해쉬값도 보존되어 있다. 또한 압수 및 복호화 관련 절차에 참여한 증인들의 증언 등을 통하여 그 보관의 연속성 등이 인정되므로, 수사기관이 분석 과정에서 정보를 훼손하거나 조작을 가할

개연성은 매우 낮아 보이고, 복호화 등 과정에 대한 참여통지 누락이 이 사건 증거수집에 어떠한 영향을 미쳤다고 보이지 않는다.』[36]

이에 대한 상고심에서 대법원도『수사관들이 압수한 디지털 저장매체 원본이나 복제본을 국정원 사무실 등으로 옮긴 후 범죄혐의와 관련된 전자정보를 수집하거나 확보하기 위하여 삭제된 파일을 복구하고 암호화된 파일을 복호화 하는 과정도 전체적으로 압수·수색과정의 일환에 포함되므로 그 과정에서 피고인들과 변호인에게 압수·수색 일시와 장소를 통지하지 아니한 것은 형사소송법 제219조, 제122조 본문, 제121조에 위배되나, 피고인들은 일부 현장 압수·수색 과정에는 직접 참여하기도 하였고, 직접 참여하지 아니한 압수·수색 절차에도 피고인들과 관련된 참여인들의 참여가 있었던 점, 현장에서 압수된 디지털 저장매체들은 제3자의 서명하에 봉인되고 그 해쉬(Hash)값도 보존되어 있어 복호화 과정등에 대한 사전통지 누락이 증거수집에 영향을 미쳤다고 보이지 않는 점 등을 감안하면, 위 압수·수색 과정에서 수집된 디지털 관련 증거들은 유죄 인정의 증거로 사용할 수 있는 예외적인 경우라고 본 원심의 판단은 정당하다고 판시[37]하였다.

36) 위 2014노762 판결 p. 17 이하
37) 위 대법원 2014도10978 전합 판결 p. 17 이하 대법원 2015. 1. 22. 선고 2014도10978

다) 대법원 2011모1839 준항고 인용결정에 대한 재항고

(1) 사건 개요

검사는 갑 회사에 대한 배임혐의로 압수・수색영장(제1영장)을 발부받아 갑 회사 빌딩 내 을 사무실을 압수·수색하였는데 저장매체에 유관정보와 무관정보가 혼재된 것으로 판단하여 갑 회사의 동의하에 저장매체 자체를 봉인하여 반출한 뒤 수사기관 사무실로 반출한 다음 관계자의 참여하에 봉인을 해제하고 전체를 이미징하여 다른 저장매체에 복제하였다.(제1처분)

이미징한 복제본을 외장 하드디스크에 재복제하였고(제2처분), 외장 하드디스크를 탐색하던 중 갑 회사의 별건 범죄혐의 관련 전자정보 등 무관정보를 발견하고 문서로 출력(제3처분)하였다. 제2・3처분 당시에 을 측에 참여기회를 부여하지 아니하였다.

이후 을 측에 참여를 보장하지 않은 채 다른 검사가 별건 정보를 소명자료로 제출하여 압수·수색영장(제2영장)을 발부 받아 외장 하드디스크에서 별전 정보를 탐색·출력하자, 갑 회사는 검찰의 압수처분이 위법하다며 준항고를 제기하였고, 원심은 제1영장의 집행 과정 전체에 당사자의 참여가 보장되지 않았고, 영장 범죄사실과 무관한 전자정보까지 무차별 복제・출력되었음을 이유로 제1, 2, 3처분을 각 취소하는 준항고 인용결정을 하자 검찰이 재항고를 제기하였다.

(2) 결정 요지

(가) 제1 영장에 기한 압수·수색

① 전자정보는 복제가 용이하여 전자정보가 수록된 저장매체 또는 복제본이 압수・수색 과정에서 외부로 반출되면 압수・수색이 종료한

후에도 복제본이 남아 있을 가능성을 배제할 수 없고, 그 경우 혐의사실과 무관한 전자정보가 수사기관에 의해 다른 범죄의 수사의 단서 내지 증거로 위법하게 사용되는 등 새로운 법익침해를 초래할 가능성이 있으므로, 혐의사실 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는 조치가 중요성을 가지게 된다.

따라서, 예외적으로 저장매체 또는 복제본을 수사기관 사무실 등으로 옮겨 이를 복제·탐색·출력하는 경우에도 피압수자나 그 변호인에게 참여의 기회를 보장하여 혐의사실과 무관한 전자정보의 복제를 방지하는 적절한 조치가 필요하며, 그러한 조치가 취해지지 않았다면 절차 위반 행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수·수색이 적법하다고 평가할 수 없고(대법원 2011. 5. 26.자 2009모1190결정 등 참조), 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였다 하더라도 달리 볼 것은 아니다.

② 전자정보에 대한 압수·수색 과정에서 이루어진 현장에서의 저장매체 압수·이미징·탐색·복제 및 출력행위 등 수사기관의 처분은 하나의 영장에 의한 압수·수색과정에서 이루어지는 것이므로, 특별한 사정이 없는 한 당해 압수·수색 과정 전체를 하나의 절차로 파악하여 그 과정에서 나타난 위법이 압수·수색 절차 전체를 위법하게 할 정도로 중대한지 여부에 따라 압수·수색 절차 전체를 취소할 것인지를 가려야 할 것이다. 여기서 위법의 중대성은 위반한 절차조항의 취지, 전체과정 중에서 위반 행위가 발생한 과정의 중요도, 그 위반사항에 의한 법익침해 가능성의 경중 등을 종합하여 판단하여야 한다.

③ 제1처분은 저장매체 자체 반출 사유가 인정되고, 저장매체 원본을 조속히 반환하기 위한 목적으로 당사자의 묵시적 동의와 복제과정의 참여가 있었으므로 적법하나, 제2·3처분은 압수·수색의 목적에 해당하는 중요한 과정인데 그 과정에 참여권을 보장하지 않았고, 더구나 혐의사실과 무관한 정보까지 재복제·출력한 점 등 위법의 중대성에 비추어 볼 때, 제1처분까지 압수수색이 적법하다 하더라도 전체적으로 제1영장에 기한 압수·수색 처분은 취소되어야 한다.

(나) 제2영장에 기한 압수수색

전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대해서도 적법하게 압수·수색을 할 수 있으며, 이러한 경우 별도의 압수·수색절차는 최초의 압수·수색절차와 구별되는 별개의 절차이고, 별도 범죄혐의와 관련된 전자정보의 피압수자는 최초의 압수·수색이전부터 해당 전자정보를 관리하고 있던 자라 할 것이므로, 특별한 사정이 없는 한 그 피압수자에게 형사소송법 제219조, 제121조, 제129조에 따라 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피압수자의 이익을 보호하기 위한 적절한 조치가 이루어져야 한다.

그런데, 제2영장 청구 당시 압수할 물건으로 삼은 정보는 제1영장의 피압수자에게 참여의 기회를 부여하지 않은 상태에서 임의로 재복제한 외장하드디스크에 저장된 정보로서 그 자체가 위법한 압수물이어서 앞서 본 별건 정보에 대한 영장청구 요건을 충족하지 못한 것이므로, 비록 제2영장이 발부되었다고 하더라도 그 압수·수색은 영장주의 원칙에 반하는 것으로 위법하다.

3) 판례 분석[38]

소위 종근당 사건의 대법원 2011모1839 결정은 디지털 저장매체의 압수와 이미징 절차에 피압수자가 참여하였다고 하더라도, 더 나아가 그 저장매체에 있는 정보를 탐색·출력하는 과정에도 당사자의 참여가 요구되는가의 문제에 대해, 정보를 탐색·출력하는 과정에 피압수자의 참여가 이루어지지 않은 경우에는 피압수자에게 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수절차가 위법하다는 취지로 해석하고 있는 것으로 풀이된다.

이와 같은 대법원의 해석은 디지털 정보에 대한 압수수색 영장을 집행함에 있어서 현장에서 저장매체 전체를 이미징하여 증거사본을 확보하는 과정과 정보저장매체 자체를 수사기관의 사무실로 가져와 그것을 이미징하여 증거사본을 확보하는 과정, 그리고 이미징 사본에서 영장에 기재된 범죄혐의 관련 정보를 검색하여 해당 부분을 출력하거나 해당 부분의 파일을 복사하는 과정이 모두 전체적으로 압수수색영장의 집행과정에 포함되므로 정보를 검색하거나[39] 출력하는 과정에도 형사소송법 제121조 규정에 따라 피압수자의 참여를 보장하여야 하고, 그 참여권을 보장하지 않는 경우에는 압수절차가 위법하다고 보는 것으로 해석된다.

다만, 대법원은 전자정보의 특성으로 인해 영장 범죄사실과 관련성이 없는 디지털 정보가 수사기관에 의해 다른 범죄의 수사단서 내지 증거로 위법하게 사용되는 등 새로운 법익침해를 초래할 가능성이 있으므로 혐의사실과 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는

38) 최성필, “디지털 증거의 증거능력”, 이프로스 발표자료, 13쪽
39) 대법원은 이와 같은 검색 행위를 ‘탐색’으로 표현하고 있는 바, 용어에 있어 통일을 기하기 위해 이하에서는 탐색으로 표현하기로 한다.

조치가 중요성을 가지게 된다는 전제 하에, 위와 같은 피압수자의 참여권이 절차적으로 보장되어야 한다는 것이므로 결국, 대법원 결정의 주된 취지는 수사기관으로 하여금 영장 범죄사실과 관련성이 없는 정보의 취득을 제한하고자 하는 것에 있다고 할 것이다.

4. 압수·수색 영장 집행 시 참여권 보장 방안

이하에서는 전자정보의 압수·수색과 관련한 대법원 전원합의체 결정과 수사기관의 실무를 조화롭게 해석하여 전자정보의 압수수색 과정에서 절차의 적정성을 보장하는 한편, 실체적 진실을 발견함으로써 형사사법 정의를 실현할 수 있는 피압수자의 참여권 보장 방안을 제시하고자 한다.

구체적 방안으로, 전자정보의 압수수색 집행 과정에서 피압수자나 참여권자에게 참여을 보장하는 방법에 대해 모색해 보고, 해당 참여 보장 방법을 전자정보의 압수수색 영장 집행 각 과정에 적용하고자 실무상 압수수색 집행 과정을 장소별, 그리고 장소 내 각 단계별로 분류하여 시간적 순서로 배열하였다. 그리고 각 단계별로 참여 보장 방법을 적용해 보고자 한다.

가. 피압수자의 참여권 보장 방법

전자정보의 압수수색 영장 집행 과정에서 피압수자나 참여권자(이하 '피압수자'라고 함)에게 참여을 보장하는 방법으로는 압수수색 영장 집행의 장소와 일시를 피압수자가 인지하여 참여의사를 선택할 수 있어야 하며, 참여를 신청할 경우 압수수색 영장 집행 과정에 참여할 수 있어야 할 것이다.

전자정보의 압수수색 집행 과정은 기존 유체물과 달리 시·공간적으로 불연속적이어서 피압수자는 압수수색 집행 과정에 대한 정보를 제공 받아야 참여의사를 선택할 수 있을 것이다.

전자정보의 압수수색 집행 과정은 3장 1절 전자정보의 압수수색 방식

에서 살펴본 봐와 같이 압수수색 장소뿐만 아니라 수사기관 사무실 등 외부에서도 진행되어 공간적으로 불연속적이고, 수사기관 사무실 등 외부에서 이루어지는 압수수색 과정은 저장매체 복사본에 대한 분석 과정 등 여러 과정으로 나누어 볼 수 있는데, 각 과정별 종료시점을 예측하기 힘들고 시간적으로도 장시간 소요된다. 이런 시·공간적 특성으로 인해 피압수자는 압수수색 집행 과정에 대한 정보 부족으로 참여권 행사에 제약이 따른다. 이를 해결하기 위해서는 수사기관에서 압수수색 집행 과정에 대한 정보를 피압수자에게 제공하는 것이 필요하다.

나. 전자정보의 압수수색 집행 각 과정에서의 참여 보장

현재 실무상 대검찰청 예규[40]에 의해 저장매체 원본이 제출되어 압수수색 현장에서 반출되는 경우 피압수자에게 이미징 등 과정에 대한 참관여부를 확인하고 있으며, 이미징 등 과정에 참관을 신청한 경우 참관예정자에게 참관일정을 통지한다. 이때 참관일정은 수사기관 사무실 등 외부에서 압수수색 집행 과정이 시작되는 시점이고, 참관인 입회하에 봉인된 저장매체들의 봉인 해제부터 이미징 작업 수행, 저장매체 복제본 디지털수사통합업무관리시스템 등록을 수행한다. 그러나 그 이후 압수수색 과정들인 저장매체 복제본에 대한 분석 과정이나 정보 탐색 과정 등에 대하여 구체적인 참여 관련 규정은 없는 실정이다.[41]

---

40) 대검 예규 제805호 “디지털포렌식 수사관의 증거 수집 및 분석 규정”, 2015.7.16. 시행

41) 제19조 (정보저장매체 등의 등록 및 책임자등의 참여)

① 제15조 제1항 단서의 압수·수색의 경우 및 제9조 제2항의 분석 의뢰를 받은 경우에는 대상 정보저장매체 등의 봉인을 해제한 후 이에 기억된 정보에 대하여 이미지 파일로 복제하여, 이를 디지털수사통합업무관리시스템에 등록하고, 대상 정보저장매체 등은 재봉인하여 지원요청자에게 인계한다. <개정 2015.7.16.>

② 전항의 경우 책임자 등 참여권자의 요청이 있는 경우 참여를 보장하여야 한다. 책임자 등이 이미징 과정 등에 참여한 경우에는 별지 제5호의 서식에 따라 확인서를 작성토록 한다. <개정 2015.7.16.>

이런 참여 관련 규정이 없는 압수수색 과정들에 대한 진행 정도나 종료 여부 등의 정보가 피압수자에게는 제공될 수 있어야 한다. 저장매체 복제본에 대한 분석 과정에 대한 소요시간은 저장매체의 용량과 활용되는 분석 기법에 따라 매우 상이하고 장시간이 걸리기 때문에 진행 정도를 예측하기가 불가능하므로 분석 과정 이후 압수수색 과정들이 언제 진행이 될지는 진행상황에 따라 다를 것이다. 피압수자가 이미징 등 과정에 참여하더라도 장시간이 걸리고 종료시점이 예측되지 않는 저장매체 복제본의 분석 과정을 참관하기 위해 수사기관 사무실에 계속해서 남아 있는 것은 피압수자도 힘들고 수사기관도 사무실 보안 등의 어려움이 따를 것이다.

이하에서는 전교조 본부 사무실 압수수색 사건[42] 등 전자정보의 압수·수색과 관련한 대법원 판례에서 설시[43]한 압수수색 현장에서나 수사기관 사무실 등 외부에서 전체 과정을 통해 피압수·수색 당사자나 변호인의 계속적인 참여권을 보장하기 위한 적절한 조치에 대하여 장소별, 장소 내 압수수색 과정을 분류하여 각 과정별로 제안해 보려고 한다.

---

42) 대법원 2011. 5. 26. 자 2009모1190결정 준항고기각결정에 대한 재항고(전국교직원노동조합 본부 사무실 압수수색 사건)

43) 대법원 2011.05.26. 자 2009모1190 결정[준항고기각결정에대한재항고]
검사나 사법경찰관이 압수·수색영장을 집행할 때에는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.

1) 압수·수색 현장에서의 참여

압수수색 장소에 있는 정보저장매체 등에서 영장 기재 혐의사실과 관련한 정보를 수색하여 이를 복사 또는 출력할 수 있는 경우에는 압수수색 집행 시작 시 영장 제시를 하여 피압수자는 참여권 행사가 비교적 잘 이루어질 수 있다. 현장에서 혐의사실과 관련 있는 전자정보를 선별할 수 있는 경우에는 피압수자나 참여인은 파일 복사되거나 문서 출력되는 전자정보에 대한 무결성 입증 확인을 하기 위해서도 현장에 있어야 할 것이다.

가) 압수 현장에서의 영장집행에 대한 통지

형사소송법 제121조는 압수수색 영장 집행 시 당사자는 '참여할 수 있다'고 규정하고 있어 당사자의 참여권을 임의적 참여로 규정하고 있으며, 법 제122조는 압수수색영장 집행 시 원칙적으로 사전에 집행의 일시와 장소를 통지하도록 규정하고 있다. 현재 수사실무에서 피압수자에게 영장을 제시하고 집행 과정에 참여할 수 있게 잘 이루어지고 있다고 본다. 대법원 판례 등에서 압수 현장에서의 참여권 보장에 대한 이슈는 없다.

그러나 당사자가 참여하지 아니한다는 의사를 명시한 때나 급속을 요하는 때에는 예외로 한다는 규정도 있다. 당사자가 참여하지 아니한다는 의사를 명시할 때에는 당사자에게 확인를 반드시 받아야 하고 수사실무상 압수의 목적을 달성하기 위해 보안유지가 필요한 경우에는 대법원 판례의 '급속을 요하는 때'라는 해석[44]에 적합해야 할 것이다. 급속을 요하는 경우에도 사후적으로 피압수자의 참여권 보장과 증거의 무결성 확인 절차 등을 하여야 할 것이다.

---

44) 대법원 2012.10.11. 선고 2012도7455판결, '급속을 요하는 때'라는 해석은 압수수색의 실효를 거두기 어려울 경우를 말함

나) 정보 탐색·선별 및 출력·복제 절차에의 참여

대법원 판결에 따르면 압수·수색 집행 전 과정에서 피압수자의 참여를 보장하여야 한다고 설시하였으므로, 디지털포렌식 도구를 활용하여 탐색하고 혐의사실과 관련 있는 전자정보를 선별하여 압수·수색를 종료할 수 있다면 이 탐색·선별 과정에도 피압수자를 참여시켜 영장 집행 과정을 확인하게 하여야 할 것이다.

또한 추후 증거의 무결성 논란을 방지하기 위하여 압수 대상인 전자정보에 대한 문서 출력 및 파일 복사 시에 해쉬값을 생성하여 책임자 등의 확인 서명[45]을 받아야 한다. 정보저장매체의 이미징 복사본이나 정보저장매체 자체를 봉인하여 수사기관 사무실로 운반되는 경우에도 피압수자가 봉인 과정에 참여하여 서명날인을 받아야 할 것이다.

2) 수사기관 사무실에서의 참여권 보장 절차

압수수색 현장의 사정이나 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한하여 예외적으로 저장매체 자체나 저장매체 복사본을 수사기관 사무실 등 외부로 반출하는 방식으로 압수·수색이 가능하다.[46] 이런 방식에서는

45) 대검찰청, 디지털포렌식 수사관의 증거 수집 및 분석 규정, 시행 2015.7.16

46) 대법원 2011.05.26. 자 2009모1190 결정[준항고기각결정에대한재항고]
전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색

저장매체 원본나 복사본을 수사기관 사무실 등에서 탐색·복제·출력 과정에서 참여권 보장 관련 문제가 있을 수 있다.

가) 압수물의 봉인 해제 및 이미징 생성·등록 과정에서의 참여

압수수색 현장에서 정보저장매체 원본이나 복제본이 수사기관 사무실로 옮겨지면 검찰의 경우는 저장매체의 이미지를 디지털수사통합업무관리시스템에 등록하여야 한다.[47] 이를 위해 먼저 압수물의 봉인해제가 필요하다.

피압수자가 봉인해제 및 복제, 이미지 과정에 참여를 신청한 경우 수사기관은 봉인해제 및 복제과정에 피압수자를 입회시키고 복제가 완료되면 복제본의 해쉬값을 생성하여 입회자로부터 확인서에 서명을 받고 저장매체 원본은 피압수자에게 반환하여야 할 것이다. 수사실무상에서 해당 과정들은 전자정보의 무결성을 확보하는 차원에서도 피압수자의 참여가 필요하므로, 참여권 보장과 관련한 문제는 발생하지 않는다.

나) 저장매체 분석을 통한 전자정보의 수집 과정에서의 참여

압수수색 절차에서 사건관계인인 피고인이나 변호인이 참여하는 것은 공개주의를 원칙으로 하는 법원의 절차에서 사건관계인들이 참여함으로서 절차의 적정한 진행을 도모하고, 절차 과정을 봄으로써 검사는 검사대로

영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다.

47) 대검찰청, 디지털포렌식 수사관의 증거 수집 및 분석 규정, 시행 2015.7.16

소추를 위한 준비를 하고, 피고인은 피고인대로 방어를 준비할 수 있도록 하는 취지이다.[48] 피압수자의 지위에서 참여는 집행을 받는 당사자를 보호하고 영장집행 절차의 적정성을 담보하려는데 그 목적이 있다.[49]

한편, 대법원은 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 '반출'하여 영장기재 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보았으며, 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다고 판시[50]하였다. 저장매체 자체나 복제본에 대한 분석 과정도 혐의사실 관련 정보를 탐색하기 전이나 도중에 이루어지므로, 이 과정 또한 압수·수색영장 집행의 일환에 포함된다고 보아야 할 것이다.

수사기관의 입장에서는 피압수자나 사건관계인을 수사기관 사무실에서 전 과정을 참여시키는 것은 여러 어려움이 따를 수 있다. 수사기관의 증거수집 기법들이 노출될 수 있으며, 정보저장매체의 분석 과정에는 상당한 시일이 걸리는데, 피압수자나 사건관계인을 지속적으로 참여시키는 것에 대한 시·공간적인 제약도 있을 것이다.

그럼에도 불구하고, 수사기관은 범죄와 무관한 정보에 관한 피압수자 사생활의 비밀과 자유, 정보에 대한 자기결정권 등에 대한 침해를 방지

48) 백형구 등, 「주석 형사소송법 Ⅰ」제4판, 한국사법행정학회(2009), 530쪽.
49) 백형구 등, 앞의 책, 533쪽.
50) 대법원 2011. 5. 26.자 2009모1190결정

하려고 노력함으로써, 사실인정의 근거가 되는 자료를 발견·수집하는 과정에서 형사사법 정의 실현과 기본권 보장을 위한 적법절차 준수 사이의 조화를 도모하여야 할 것이다.

저장매체에 대한 분석 과정은 안티포렌식 대응 기법에 따라 삭제된 전자정보 복구, 전자정보의 검색 및 탐지를 위한 사전 준비, 암호화된 전자정보 복호화, 전자정보의 은닉 탐지 과정으로 세부화 시킬 수 있다. 이들 세부 과정들은 신뢰성을 담보하기 위해 수사기관에서 자체 개발된 포렌식 도구나 국제적으로 공인된 EnCase 프로그램을 이용하여 수행된다. 포렌식 도구 프로그램이 저장매체의 복제본을 분석하는 시간은 예측하기가 힘들며, 장시간 소요되는 경우도 있다. 이하에서는 각 세부 분석 과정별로 참여권을 어떻게 보장해야 할지 살펴보기로 하자.

(1) 저장매체 내의 삭제된 전자정보 복구 과정

전자정보의 압수·수색 집행에서는 압수·수색 현장에서 반출된 저장매체 내의 삭제된 전자정보에 대한 수색은 반드시 필요한 절차 중 하나일 것이다.[51] 저장매체의 전자정보 복구는 무결성을 위해서 저장매체의 이미지 형태를 이용하여야 한다. 저장매체의 전자정보 복구 실시 여부를 압수물의 봉인 해제 및 저장매체의 이미지 생성 과정 이전에 결정을 하고 해당 과정의 수행 시기는 이미지 생성이 완료된 직후에 전자정보 복구

51) 서울고등법원 2014.08.11. 선고 2014노762 판결[내란음모·국가보안법위반(찬양·고무등)·내란선동]
저장매체 원본이나 복제본으로부터 범죄혐의와 관련된 전자정보를 탐색하여 이를 문서로 출력하거나 파일을 복사하는 과정은 전체적으로 영장 집행의 일환에 포함되고, 이를 위해 저장매체 자체를 복구·복제하거나 삭제된 파일을 복원하고, 암호를 풀어 복호화하는 과정 역시 영장 집행의 일환이다. 따라서 그 과정에 대하여 피고인들과 변호인에게 집행의 일시와 장소를 사전에 통지하지 아니한 것은 형사소송법 제219조, 제122조 본문, 제121조에 위배된다.

과정을 수행하면 될 것이다.

이러한 절차로 진행이 된다면 삭제된 전자정보 복구 과정에서의 참여는 별도의 통보 없이 압수물의 봉인해제와 저장매체의 이미지 생성 과정에서의 참여에 대한 연장선으로 볼 수 있을 것이다.

한편, 전자정보 복구 과정을 통해 복구된 전자정보들에 대한 탐색·출력 과정에서도 피압수자나 사건 관계인에게 참여권이 보장되어야 하므로 집행에 대한 통지를 해야 할 것이다. 저장매체에 대한 분석 과정 이후 탐색·출력 과정이 있을 것으므로, 복구된 전자정보들이 탐색·출력 과정에서 탐색이 이루어지면 복구된 전자정보를 위한 탐색·출력 과정을 위한 별도의 집행에 대한 통지는 필요 없을 것이다.

(2) 전자정보의 검색 및 탐지 사전 준비 과정

전자정보의 검색 및 탐지 과정은 저장매체 내에 있는 수많은 전자정보들을 혐의사실과의 관련성 여부를 확인하는데 중요한 수단이다. 해당 과정은 전자정보를 직접적으로 열람하지 않고 전자정보 내에 포함되어 있는 특정 키워드를 가지는 파일을 검색하거나, 파일의 확장자와 파일 시그니처(Signature)가 불일치하는 경우를 탐지하는 것이다. 이런 전자정보 내의 키워드 검색이나 파일 기반 조사는 검찰에서 개발한 CFT 포렌식 도구나 EnCase 포렌식 도구를 활용하여 수행 가능하며, 사전 준비 과정으로 포렌식 도구들은 압수·수색 현장에서 반출된 저장매체의 복제본을 분석 작업을 수반한다. 이런 사전 준비 후에야 키워드 검색이나 파일 기반 조사가 가능하다.

전자정보 검색 및 탐지 과정의 사전 준비는 반출된 저장매체의 이미지가 생성한 후에 수행하면 된다. 따라서 참여권 보장은 압수물의 봉인해제

및 저장매체의 이미지 생성 과정에서의 참여에 대한 연장선으로 보면 될 것이다. 한편, 전자정보 검색 및 탐지 과정의 실질적인 검색 및 탐지는 전자정보의 탐색·출력 과정에서 이루어진다.

(3) 암호화된 전자정보에 대한 복호화 과정

저장매체 내에서 암호화된 전자정보가 있다면 이 전자정보에는 중요한 정보가 담겨 있을 가능성이 크다고 할 수 있다. 따라서 이 중요한 정보를 혐의사실과의 관련성 여부를 확인하는 것은 압수·수색 집행에 있어서 상당히 중요해 보인다. 먼저 저장매체 내에서 암호화된 전자정보를 파악이 되어야 할 것이다. 그러나 포렌식 도구 프로그램으로 모든 암호화된 파일을 검색하지는 못 하므로 전자정보의 탐색 과정에서 확인되는 암호화된 전자정보를 대상으로 복호화 과정이 진행되어야 할 것이다.

전자정보의 탐색 과정으로 복호화해야 할 전자정보가 확정되면 복호화 프로그램을 수행하기 전에 피압수자나 사건 관계인에게 복호화 과정 집행에 대한 참여 통보를 하여야 할 것이다. 해당 과정의 통보를 하면서 피압수자에게 암호화된 전자정보에 대한 복호화를 요구하여 복호화 과정을 줄이도록 해야 할 것이다.

(4) 전자정보의 은닉 탐지 과정

전자정보 은닉 탐지 과정에서는 이미지, 음성, 동영상 등의 멀티미디어 파일 또는 문서 파일 등에 숨겨 놓은 전자정보를 탐지하고 분석한다. 검찰 포렌식 도구인 CFT을 활용하여 압수·수색 현장에서 반출된 저장매체의 이미지를 분석하고 전자정보의 은닉 여부를 탐지한다. 은닉 탐지

과정은 반출된 저장매체의 이미지가 생성된 이후에 수행하면 될 것이다. 따라서 전자정보 은닉탐지 과정은 압수물 봉인해체 및 저장매체의 이미지 생성 과정 이후 연속적으로 수행하고 은닉탐지 과정에서의 참여도 봉인 해제 및 저장매체의 이미지 생성 과정의 참여에 대한 연장선으로 볼 수 있다.

다) 탐색·출력 과정에서의 참여

앞에서 살펴본 전자정보의 여러 압수·수색 과정들을 통하여 압수물의 대상이 될 수 있는 것들을 최대한 수집할 수 있을 것이다. 탐색·출력 과정은 수집된 전자정보들 중 혐의사실과의 관련성이 있는지 탐색하고 관련성이 있다면 파일 복사나 문서 출력으로 압수 대상을 확정하는 것이다.

한편 앞서 본 전자정보 압수수색과 관련된 대법원의 판례들은 이러한 탐색·출력 절차에도 피압수자를 참여시켜야 한다고 판시하였다.[52]

따라서 수사실무 현실과 대법원이 참여권을 보장하고자 하는 취지, 즉 수사기관으로 하여금 영장 범죄사실과 관련성이 없는 정보의 취득을 제한하고자 하는 취지를 조화롭게 합리적으로 해석하는 것이 중요하다고 본다.[53]

실무상 압수한 정보저장매체의 이미징 사본을 이용하여 영장 범죄사실과

52) 대법원 2015.07.16. 자 2011모1839 전원합의체 결정[준항고인용결정에대한재항고]
저장매체에 대한 압수·수색 과정에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 또는 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)를 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 경우에도, 그와 같은 일련의 과정에서 형사소송법 제219조, 제121조에서 규정하는 피압수·수색 당사자(이하 '피압수자'라 한다)나 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다. 만약 그러한 조치가 취해지지 않았다면 피압수자 측이 참여하지 아니한다는 의사를 명시적으로 표시하였거나 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자 측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수·수색이 적법하다고 평가할 수 없고, 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였다 하더라도 달리 볼 것은 아니다.

53) 최성필, "디지털 증거의 증거능력", 검찰 포털 발표자료(2015. 9.), 28쪽

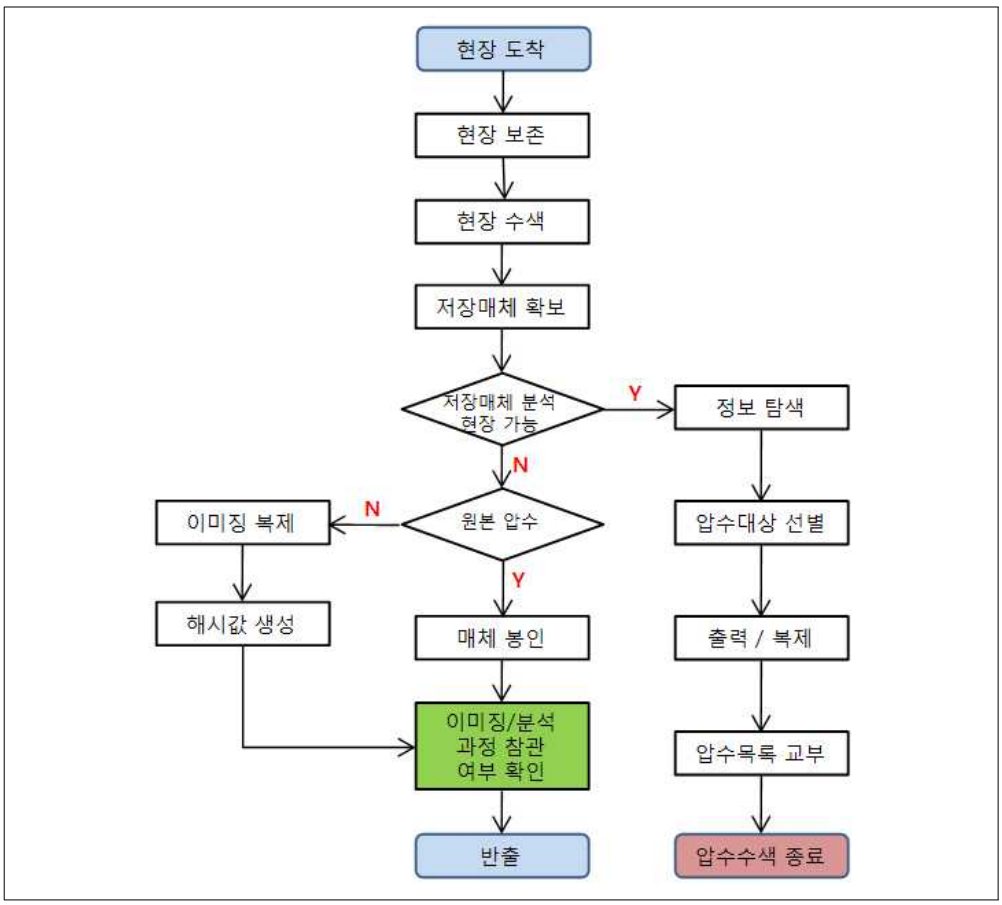
관련성이 있는 정보를 탐색하게 되는데, 전자정보의 대량성으로 인해 주로 키워드 검색을 통해 영장 범죄사실과 관련성이 있다고 생각되는 파일을 추출 내지 선별하고(이하 '선별 절차'라 함), 이렇게 추출된 파일에서 또 다시 영장 범죄사실과 관련된 정보의 내용을 확인한 다음, 이를 증거로 사용하기 위하여 범죄사실과 관련된 해당 정보의 내용을 출력하게 된다.[54]

탐색·출력 절차는 압수·수색 현장에서 반출된 정보저장매체의 봉인 해제 및 이미지 생성 과정에서의 참여와는 불연속적으로 이루어질 가능성이 크다. 저장매체에 대한 분석 과정에는 여러 안티 포렌식 대응 기법들이 포함되어 있고 각각의 세부 분석 과정들의 종료 시점들을 예측하기 어렵기 때문이다. 실제 종근당 사건에서도 이미징 사본을 이용하여 추출된 파일의 내용을 검색하는데 11일이 소요되었다고 한다.

탐색·출력 절차에서의 참여는 피압수자나 참여권자가 소추에 대한 방어를 위해서는 다른 과정보다 그 중요성이 크다. 따라서 피압수자나 참여권자에게 참여권 행사를 보장하기 위해서는 이미징 파일 작성 등 과정에서 불연속적으로 압수수색 집행 과정이 이루어질 경우 수사기관에서 탐색 및 ·출력 과정에 참여를 할 것인지 여부를 확인하여 그 여부를 기록하는 것이 참여권 보장을 위한 적절한 조치를 하였다는 것을 나타낼 수 있을 것이다.

54) 최성필, "디지털 증거의 증거능력", 검찰 포털 발표자료(2015. 9.), 28쪽

다. 전자정보의 압수·수색 절차(안)

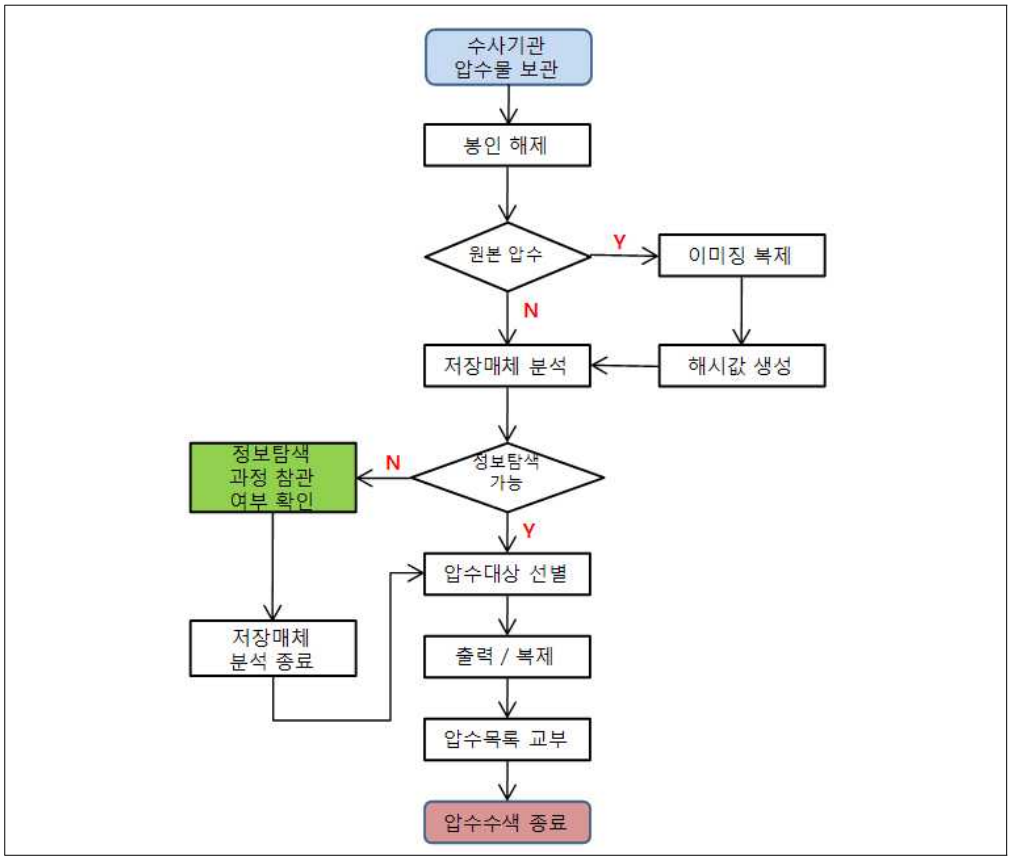


[그림 1] 압수 현장에서의 전자정보 압수·수색 절차(안)

[그림 1]은 현장에서의 전자정보 압수수색 영장 집행 절차를 흐름도로 나타낸 것이다.

압수·수색 영장 집행 전에 피압수자나 사건관계인에게 영장 집행에 대한 사전 통지나 영장 제시를 하여 참여여부를 선택할 수 있도록 해야 할 것이다. 압수·수색 현장에 도착해서는 증거 인멸이나 훼손 등을 방지하기 위해 네트워크 차단 등 압수수색 현장 보존을 위한 조치들을 취하여야 할 것이다. 이런 현장 보존이 되어 있는 상황에서 각종 시스템 및 정보저장매체를 수색하여 저장매체들을 확보하며, 저장매체들에 대하여

분석 과정을 수행한다. 이 과정에서 저장매체 분석의 진행정도나 현장 사정을 살펴보며, 압수 현장에서 압수·수색 집행을 계속 진행할 지를 판단하여 압수수색 집행을 현장에서 마칠 수 있는지를 결정한다. 현장에서 압수수색 집행을 마칠 수 있는 상황이라면 저장매체의 복제본을 생성하고 해당 복제본을 반출하거나 저장매체 자체를 반출할 지를 결정하여야 할 것이다. 압수수색 현장에서 휴대용 전자정보 분석 도구를 이용하여 저장매체 분석이 가능하고 현장 사정들이 압수수색을 진행할 수 있는 상황이라면 피압수자나 참여권자를 압수수색 집행 과정에 참여할 수 있게 하고 정보 탐색 및 출력·복제 작업을 통해 압수 대상을 확정하여 압수수색을 종료한다.



[그림 2] 수사기관 사무실에서의 전자정보 압수·수색 절차(안)

[그림2]와 같이 저장매체 자체나 복제본을 수사기관 사무실 등 외부로 반출한 경우 저장매체 원본에 대한 이미지 파일을 디지털수사통합업무관리시스템에 등록하고 저장매체 복제본에 대한 분석 작업을 수행해야 할 것이다. 이 분석 과정에서 분석 대상이 많거나 요구되는 분석 기법들이 다양할 경우 분석 과정에 필요한 시간은 장시간이며 예측하기 어렵다. 이런 경우 피압수자나 사건관계인을 계속적으로 수사기관에 입회시키기가 보안 등 여러 사정에 어려움이 있으므로 정보탐색 과정에 대한 참관 여부를 확인하여 참관을 신청한 경우 참관 예정 일시를 통보하여 참여권을 보장하는 조치를 취하여야 할 것이다.

저장매체 복제본에 대한 분석 과정이 모두 완료되면 압수 대상을 선별하기 위해서 지금까지 수집된 정보들을 탐색하여 혐의사실과의 관련성 여부를 판별할 것이다. 피압수자나 사건관계인은 전자정보의 탐색 과정을 참여할 수 있고 최종적으로 압수 대상이 선정이 되면 압수 목록을 교부받을 수 있을 것이다.

라. 저장매체 내 전자정보에 대한 사용 이력 관리 방안

1) 도입 배경

대법원 판례[55]는 피압수자가 배제된 상태의 저장매체에 대한 열람을 금지하고 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다고 판시하였다.

이를 위한 조치로서 압수수색 현장에서 반출된 저장매체의 복사본을 디지털수사통합관리시스템에 등록한 이후 저장매체 복사본의 열람 및 복제나 출력 등 사용 이력에 대한 관리를 제안한다.

전자정보가 수록된 저장매체 또는 복제본이 압수・수색 과정에서 외부로 반출되는 경우 저장매체의 복제본이 디지털수사통합관리시스템에 등록이 되는 과정까지는 전자정보의 오·남용 및 임의적인 복제나 복사에 대한 적절한 조치가 이루어지고 있다. 압수·수색 현장에서 수사기관 사무실로 운반 시에는 저장매체 또한 복제본에 대한 훼손을 방지하고 무결성을 유지하기 위해 저장매체 또는 복제본을 반드시 봉인하고, 저장매체나

---

55) 대법원 2011. 5. 26. 자 2009모1190결정 준항고기각결정에 대한 재항고(전국교직원노동조합 본부 사무실 압수수색 사건)
검사나 사법경찰관이 압수·수색영장을 집행할 때에는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.

복제본에 대한 봉인 해제 시에는 수사기관 규정상으로 피압수자의 참여를 보장하고 있다. 그러나 그 이후 압수수색 집행과정(저장매체 복제본 분석 및 정보 탐색 등)에서는 수사기관이 저장매체 복제본을 직접 관리하고 있으며, 저장매체 복제본 분석 과정은 실무상 며칠씩 장시간 소요되고 종료시점을 예상하기 어렵다. 또한 수사기관 내 규정에 피압수자의 참여권 보장이 명시되어 있지 않아 수사기관에서 피압수자를 배제한 상태에서 저장매체 복제본에 대한 열람 및 임의적인 복제나 복사 시도가 이루어질 가능성이 있다. 이에 따라 저장매체 내 전자정보의 사용 이력 체계를 도입하여 수사기관에서 임의적인 열람 및 복사나 출력을 제한하는 조치가 필요할 것이다.

2) 설계 시 고려사항과 실무상 보완해야 할 사항

저장매체 복제본에 대한 사용 이력 관리 체계의 설계는 다음사항을 고려하여야 할 것이다.

- 첫째, 관리 대상을 저장매체 복제본과 저장매체 복제본 내 전자정보로 분류한다.
- 둘째, 저장매체 복제본의 저장위치는 디지털통합수사업무시스템이고 저장매체 복제본 내 전자정보의 저장위치는 수사기관 PC이다.
- 셋째, 저장매체 복제본 내 전자정보에 대한 사용에 대하여 사용자별로 열람, 복제, 출력 등 사용의 구분이 이루어져야 한다.

대검찰청 예규 상 저장매체 복제본은 디지털수사통합업무시스템에 등록되며 등록된 저장매체 복제본 이외의 동일한 저장매체 복제본은 모두 삭제해야 한다. 또한 디지털수사통합업무시스템은 수사기관 직원별로 접근

권한을 설정하여, 저장매체 복제본의 접근이력을 관리하고 있다. 따라서 보완적으로 혐의사실 관련성에 대한 구분 없이 행해지는 저장매체 복제본의 재복제를 금지하는 제도적 조치가 필요하다.

저장매체 복제본 내 전자정보는 디지털통합수사업무시스템에서 파일 단위로 수사기관 직원 PC에 다운로드 되어 열람된다. 디지털통합수사업무시스템에서 저장매체 복제본 내 전자정보를 수사기관 직원 PC에 다운로드한 이력은 로그로서 기록되어 관리가 된다. 하지만 수사기관 직원 PC에 저장된 저장매체 복제본의 전자정보는 열람·복사·출력에 대한 통제 관리가 이루어지지 않고 사용 이력을 확인할 수 없는 문제점이 있다. 수사기관 직원 PC에 저장된 저장매체 복제본의 전자정보에 대한 사용자별 사용 통제 관리와 사용 이력 체계가 필요한 실정이다.

3) 기술적 해결 방안

파일 단위로 수사기관 직원 PC에 저장되는 저장매체 복제본의 전자정보에 대한 열람·복사·출력의 이력 관리 대책으로서 이력 관리 기술구조를 모색하고 이력 관리 기술구조를 구현하는 한 방법으로서 Enterprise DRM[56] 중 Server DRM 기술을 적용하는 방안을 제안한다.

본 논문에서 제안하는 이력 관리 기술구조는 [그림3]와 같이 전자정보의 이력 관리 여부에 따라 관리영역과 비관리영역으로 구분하고 비관리영역에 있는 수사

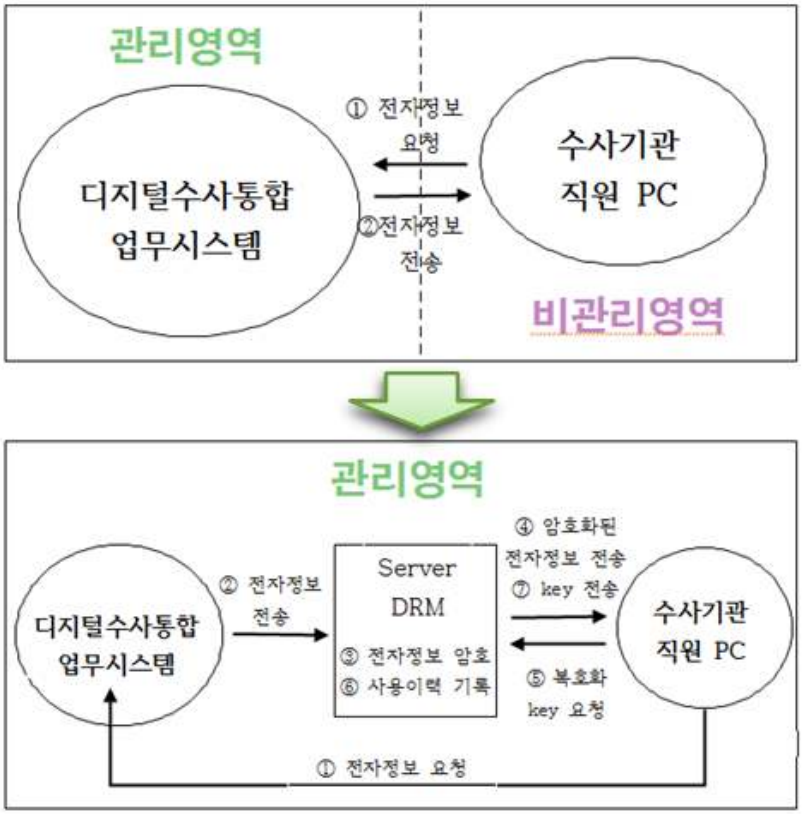
---

56) 조규곤, “Enterprise DRM 구축 방안”, 정보과학회지, 23권 8호, pp.31-32, 2005.8, DRM(Digital Rights Management) 기술은 디지털 콘텐츠의 저작권 보호를 목적으로 개발되었다. 초기 DRM은 콘텐츠의 상거래 시 콘텐츠 보호가 주목적이었지만 현재는 여러 방면에서 응용되고 있다. 상거래 시 콘텐츠의 저작권 보호를 위한 DRM을 Commerce DRM이라고 하고, 기업의 중요한 자산인 문서의 기밀을 효과적으로 지키기 위한 DRM을 Enterprise DRM이라고 부른다.

Enterprise DRM은 기업 내부의 혹은 외부의 합법적 사용자의 고의나 부주의로 인한 정보의 유출을 막는다. 또한 전자문서의 사용내역을 관리할 수 있어, 보안 사고를 예방하고 사고 발생 시에는 전자문서의 사용내역을 조사에 이용할 수 있다. 전자문서 보안 정책으로 DRM을 적용함으로써, 각 전자문서별로 다음과 같은 점을 통제할 수 있다.

- 사용자, 사용 PC, 사용기간, 사용횟수, 오프라인 사용 허용 여부, 사용 이력 수집주기
- 보기, 편집, 인쇄, 암호화 저장, 원본 저장 허용 여부

기관 직원 PC를 Server DRM 기술을 활용하여 관리영역으로 전환하는 것이다.



[그림3] 전자정보 사용 이력 관리 기술 구조

기술구조에 대한 구체적인 설명은 다음과 같다. 수사기관 직원 PC에서 디지털수사통합업무시스템의 사건 관련 저장매체 복제본의 전자정보를 다운로드 요청을 하면 디지털수사통합업무시스템은 해당 전자정보를 Server DRM[57] 시스템에 전송한다. Server DRM 시스템은 전송받은 전자정보를 암호화하여 수사기관 직원 PC에 전송한다. 수사기관 직원 PC에

57) 문진규, "내부정보유출방지를 위한 DRM 적용방법설계", 한국컴퓨터종합학술대회, 2007 전자문서 저장 및 관리의 주체를 기준으로 Enterprise DRM 기술을 세분화 정의한다. 그 중 하나인 Server DRM은 전자문서를 암호화 하는 시점이 사용자 PC에 다운로드 전인 정보시스템 서버 내에서 이루어지며, 전자문서가 사용자 PC에 다운로드된 후에 열람, 인쇄, 저장 등 이용의 권한을 통제하는데 사용된다. Server DRM의 사용자 인증은 별도 인증 없이 정보시스템의 사용자 인증을 활용한다. 문서 관리의 주체는 서버 관리자이다.

서 암호화된 전자정보를 열람하기 위해 복호화 키를 Server DRM 시스템에 요청을 한다. Server DRM 시스템은 사용자 인증 및 권한 확인을 하고 복호화 키를 수사기관 직원 PC에 전송하면서 문서 사용이력을 기록한다.

4) 저장매체의 전자정보에 대한 사용 이력 관리 체계의 기대 효과

수사기관이 저장매체 복제본의 열람 및 복사나 출력 등의 사용 이력을 관리함으로써, 수사기관은 압수·수색 집행 절차의 투명성을 확보하며, 집행 절차에 대한 위법성 논란이 줄어들고 저장매체 복제본에 대한 관리에 경각심을 갖게 되어 사전 및 사후 통제기능이 강화될 것이다.

Server DRM을 적용함으로써, 각 파일별로 열람자, 열람 PC, 열람횟수, 인쇄횟수를 기록할 수 있게 된다. 또한 사용자별로 전자정보의 열람 및 복사나 출력 등 사용에 대한 통제가 가능하여 자료 유출를 방지하는 효과도 있다.

5. 결론

본 논문에서는 형사사법체계에 있어서 날로 중요성이 커지는 전자정보에 대한 압수·수색 영장 집행을 할 경우 피압수자나 사건 관계인에게 참여를 보장하기 위한 방안으로 전자정보의 압수·수색 집행 과정을 공간과 절차별로 나누어 보고 각 절차에서 참여권을 어떻게 보장할 것인지에 대해 제안해 보았다.

2장에서는 수사기관에서 형사소송법 제106조 3항에 따라 압수·수색 영장 집행하는 방식이 크게 3가지로 나뉘며, 각 방식별 세부절차를 확인하였다. 압수·수색의 절차적인 측면과 더불어, 내용적인 측면을 살펴보기 위하여 전자정보의 압수·수색에서 활용되고 있는 전자정보 수집 및 분석 기법을 조사하였고 수사실무에서 활용하는 디지털 포렌식 도구에 대한 기능을 비교·분석한 것도 찾아보았다.

3장에서는 압수·수색 절차에 있어서 피압수자의 참여와 관련한 규정에 대해 살펴보았고 참여권 보장의 취지들을 알아보았다. 그리고 전자정보의 압수수색 집행 과정에서의 참여권 보장 등과 관련한 대법원 주요 판례들을 조사하였다. 전자정보의 압수·수색 집행 시에 수사기관 사무실 등 예외적인 방식의 집행이 가능한 요건, 피압수자의 참여 보장, 혐의사실과의 유관정보에 한정한 문서출력, 파일복제 등 적법절차 및 영장주의의 원칙에 대해 구체적인 사례를 통해 알 수 있었다. 또한 영장 집행 과정 중 발생한 위법한 행위들이 전체과정 중에서의 중요도, 그 위반사항에 의한 법익 침해 가능성의 경중 등을 종합하였을 때 위법의 중대성으로 전제적인 압수·수색 처분이 취소되는 사례도 있었다.

전자정보의 압수·수색영장 집행과 관련하여 살펴본 법 규정, 수사기관에서의 실무 현실, 대법원의 판례 사례을 종합적으로 고려하여 참여권을 보장하는 전자정보의 압수·수색 영장 집행 절차를 제시하였다. 또한 수사기관에서 피압수자를 배제한 상태에서 압수 현장에서 반출한 저장매체 내 전자정보를 열람 및 임의적인 복사나 출력 등을 제한하기 위한 방안으로 저장매체 내 전자정보 사용 이력 관리 체계를 제안하였다. 피압수자 압수·수색 현장에서뿐만 아니라 수사기관 사무실 등 외부에서도 피압수자의 참여 횟수를 최소화하면서도 압수·수색 집행 과정의 대부분에 참여가 되도록 하는 것이 목표이었다. 수사기관에서는 형사소송법 개정으로 과거에 비해 전자정보의 압수·수색에 대한 사전·사후 통제가 가해져 집행에 어려움을 겪고 있다. 수사의 목적을 달성하여 사법 정의를 바로 세우면서 동시에 피압수자의 권리도 보장하는 데에 본 논문이 조금이나마 도움이 되길 바란다.

참 고 문 헌

1. 권양섭 “디지털 증거수집에 관한 연구”, 군산대학교 박사학위 논문(2009)
2. 김윤섭, · 박상용, “형사증거법상 전자정보의 증거능력”, 형사정책연구 제26권 제2호(2015)
3. 김지홍, “디지털 포렌식 절차 모델에 대한 새로운 접근”, 서울대학교 석사학위논문(2015)
4. 노명선, ‘디지털 증거의 압수·수색에 관한 판례 동향과 비교법적 고찰’, 형사법의 신동향 통권 제43호(2014.6.)
5. 문진규, “내부정보유출방지를 위한 DRM 적용방법설계”, 한국컴퓨터종합학술대회, (2007)
6. 백형구 등, 「주석 형사소송법 Ⅰ」 제4판, 한국사법행정학회(2009)
7. 손지영 · 김주석,「디지털 증거의 증거능력 판단에 관한 연구」, 대법원 사법정책연구원(2015)
8. 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지
9. 양근원, “형사절차상 전자정보의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위논문(2006)
10. 이완규, “디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 확보 방안”, 대검찰청 이프로스 게시판(2015. 8.)
11. 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요 요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012)
12. 전승수, “형사절차상 전자정보의 압수수색 및 증거능력에 관한 연구”, 서울대학교 박사학위논문(2010)
13. 조규곤, “Enterprise DRM 구축 방안”, 정보과학회지, 23권 8호(2005. 9.)
14. 최성필, “디지털 증거의 증거능력”, 검찰 포털 발표자료(2015. 9.)
15. 탁희성, “법정에서 전자 증거의 허용가능성”, 한국전자포렌식학회, 「전자 포렌식 연구」 창간호(2007. 11.)

16. 탁희성・이상진,「디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보 방안」, 형사정책연구원(2006)
17. 대검찰청, 「검찰수사 실무전범Ⅱ」(2008)
18. 대검찰청, “디지털포렌식 수사관의 증거 수집 및 분석 규정” [시행 2015.7.16.]

판례자료

대법원 2011. 5. 26. 자 2009모1190
대법원 2012.10.11. 선고 2012도7455
수원지방법원 2014. 2. 17. 선고 2013고합620, 624, 699, 851
서울고등법원 2014. 8. 11. 선고 2014노762
대법원 2015. 1. 22. 선고 2014도10978

이학석사학위논문

참여권 보장을 위한 전자정보 압수·수색 집행 방안에 관한 연구

2016년 2월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공
김 광 호

참여권 보장을 위한 전자정보 압수·수색 집행 방안에 관한 연구

지도교수 이 상 원

이 논문을 이학석사 학위논문으로 제출함

2015년 11월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

김 광 호

김광호의 석사학위논문을 인준함

2016년 1월

위 원 장 이 광 근 (인)

부 위 원 장 이 상 원 (인)

위 원 백 윤 흥 (인)

국 문 초 록

현대인의 일상생활은 컴퓨터, 인터넷, 스마트폰 등의 디지털 기기들을 통해 점차 정보시스템 안으로 들어가 있다. 이런 변화들로 인해 현대인의 생각과 행위가 전자정보로 기록되어 남게 되었다. 기존의 유체물에서는 발견할 수 없었던 방대하고 세세한 정보들이 전자 증거로 사용할 수 있게 된 것이다. 2011년 형사소송법 개정에서는 전자정보를 증거로서 수집하기 위한 “원칙적 선별압수, 예외적 매체압수” 압수방법이 규정되었다. 전자정보의 수집 시 기존 유체물의 압수·수색과는 달리 정보의 대량성으로 인해 혐의사실과 관련 있는 정보뿐만 아니라 그와는 전혀 무관한 정보들이 대량으로 압수될 우려가 있고 피압수자의 사생활 침해를 유발할 수가 있다.

전자정보의 압수·수색 과정에서 범죄와 무관한 막대한 정보가 수집될 수 있으므로, 이로 인한 침해를 방지하기 위한 강력한 사법통제가 요구되고 있다. 형사소송법 제106조에서 관련성에 관한 내용이 추가되었지만 요구되는 사법적 통제가 충분하지 못하고, 전자정보의 구체적인 증거 수집절차도 충분하지 못하다. 지속적으로 전자정보의 증거 수집 절차 등에 대한 입법적 공백에 대해 논의하고 연구하여 체계적이고 구체적인 입법이 시급히 필요하다.

현재 전자정보의 압수·수색 절차에 대한 입법의 미비는 대법원 판례를 통해 입법공백이 일부분 채워지고 있다. 대법원 판례는 전자정보의 ‘압수’ 개념을 기존 압수물과 다르게 ‘저장매체를 반출하여 혐의사실과 관련된 정보를 탐색·복사·출력할 때’까지의 전 과정으로 보고 있고, 압수의 전 과정에 지속적인 피압수자의 참여권 보장을 적법요건으로 제시하여 이를 준수하여야 한다고 판시하였다. 뿐만 아니라 수사기관 사무실에서 저장매체의 전자정보 탐색 과정에서 피압수자의 참여권 미보장, 혐의사실

관련 구분 없는 재복제, 혐의사실과 무관한 정보 출력 등을 중대한 위법 처분으로 판단하고 영장에 기한 압수·수색 전체를 취소하는 판결을 내렸다.

그러나 이 같은 대법원의 전자정보 압수·수색에 대한 적법요건을 실무 현실을 고려하지 않고 기계적으로 해석하였을 경우 수사기관의 전자 증거 수집을 매우 어렵게 하는 결과를 초래할 위험이 있어 실체적 진실 규명을 통한 형사 사법의 정의 실현을 어렵게 할 수 있는 문제점이 있다.

본 논문은 각각의 어려움이 있는 피압수자의 권익보호와 형사 사법 정의 실현이 조화를 이루고자 하는 목표를 가지고 압수·수색 과정별로 어떠한 방식으로 참여권을 보장하여야 하는지에 대해 방안을 제시하였다. 또한 수사기관이 피압수자가 배제된 상태에서 저장매체 내 전자정보에 대한 열람 및 복제나 출력 등을 방지하는 위한 방안으로 저장매체 내 전자정보에 대한 사용 이력 관리 체계 방안을 제안하였다. 이를 위해 전자정보의 특성, 전자정보의 압수·수색 방식, 전자정보의 수집 및 분석 방법을 살펴보고 압수수색 절차에서의 참여권 범위, 참여권 보장 관련 대법원 주요 판례 등을 검토하였다. 이를 통한 궁극적으로는 전자정보의 압수·수색에 있어서 보다 체계적이고 실효성 있는 법규가 형성되는 것에 도움이 g 되기를 바란다.

주요어 : 참여권, 전자정보, 압수수색, 집행

학 번 : 2014-24854

목 차

1. 서론

증거는 형사절차상 사건의 실체적 진실을 발견하고 구체적인 국가의 형벌권을 발동하는데 있어 사건의 진위를 명백히 하기 위한 사실인정의 근거자료로서 중요한 의미를 갖는다. 이러한 증거의 존재형태는 범죄의 태양에 따라 다르나 전통적인 의미에 있어서 증거방법은 유형물로 제한되어 왔다. 그러나 과학기술의 발달로 인하여 첨단정보통신기술을 이용하는 범죄가 증가하면서 과거에는 전혀 예측할 수 없었던 새로운 증거형태가 출현하게 되었는데 그것이 바로 전자 증거이다.[1)]

현대사회는 컴퓨터와 인터넷 등 과학기술의 발달로 각종 전자 증거가 기하급수적으로 증가하고 있다. 실무에서도 과거 진술증거에 의존하던 수사는 피의자, 참고인 등의 비협조 등으로 말미암아 압수수색의 결과로 취득한 전자 증거의 중요성이 더욱 커지고 있다. 즉, 형사절차에서 전자증거의 중요성은 날로 증가하고 있는 것이다.

그럼에도 불구하고 우리 형사소송법은 여전히 물리적 증거만을 주로 예상하여 규정하고 있을 뿐, 기존의 물리적 증거에서는 예상하기 어려웠던 전자정보의 압수·수색 과정에서 참여의 보장 범위, 전자 증거의 증거능력 등과 관련한 법적, 제도적 장치는 아직까지 미비한 상태이다.

한편, 대법원은 전자정보의 압수수색과 관련된 다수의 판례들을 통해 정보저장매체에 대한 압수·수색영장 집행 시 영장에서 인정한 예외적인 사정으로 정보저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우, 전체 과정을 통하여 피압수·수색 당사자나

1) 탁희성, “법정에서 전자 증거의 허용가능성”, 한국전자포렌식학회, 「전자 포렌식 연구」 창간호(2007. 11.), 24쪽.

변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 정보저장매체에 대한 열람·복사 금지 등 압수·수색 대상인 정보저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하다고 천명하였고 압수수색영장 집행의 일부 과정에서 참여권 미보장, 혐의사실 관련 구분 없는 재복제, 혐의사실과 무관한 정보 출력 등을 이유로 전체 압수·수색 처분을 취소하였다.

최근 종근당 사건의 대법원 전원합의체 결정을 보면 법원으로부터 발부받아 집행한 압수·수색 과정 중, 피압수자에게 참여권을 보장하지 않고 혐의사실 관련성에 대한 구분 없이 재복제하는 중대한 위법 처분을 하여 전체 압수·수색이 위법한 것으로 판결됨으로써 수사기관에서는 적지 않은 혼란이 있었다. 이와 같은 혼란이 재발하지 않도록 법 규정과 대법원 판례, 그리고 수사현실을 고려한 전자정보의 압수·수색 절차가 시급히 필요하다고 보인다.

따라서 본 논문은 과학기술의 발달로 인하여 형사절차에서 그 중요성이 크게 증가하고 있는 전자 정보가 기존의 물리적 증거와는 다른 특성을 가지고 있음에 따라 수사기관 실무상 압수수색 절차와 관련하여 검토하고, 수사기관에서의 전자정보 압수·수색 영장 집행 방식을 살펴볼 것이고, 수사실무에서 활용하고 있는 전자정보의 증거 수집 기법인 안티 포렌식 기법들을 조사하여 압수·수색 실무에서 어떤 과정이 있는 지를 알아볼 것이다. 한편, 최근 대법원 전원합의체 결정를 통해 전자정보의 압수·수색 영장 집행 시 참여권 보장과 관련한 경향을 검토한 후 대법원 전원합의체 결정과 수사실무 현실 사이에 발생하는 괴리를 해소하면서 피압수자의 참여권이 보장되는 전자정보의 압수·수색 방안을 제시하였다. 또한 대법원

판례는 수사기관이 압수 현장에서 반출한 저장매체를 피압수자가 배제된 상태에서 열람 및 임의적 복제나 출력을 막기 위한 적절한 조치가 이루어져야 한다고 판시하였다. 이를 위한 방안으로 저장매체 내 전자정보에 대한 사용 이력 관리 체계를 도입하는 것을 제안하였다.

2. 전자정보의 특성

전자증거가 기존의 물리적 증거와는 달리 매체독립성, 비가시·비가독성, 취약성, 대량성, 전문성, 네트워크 관련성 등의 특징을 가지고 있다.[2] 이러한 특성들을 파악하고 그에 따른 문제점을 정리한다.

이와 같은 특성으로 인해 전자정보의 압수수색 절차, 압수한 전자정보의 증거능력 등과 관련하여 기존의 물리적 증거와 달리 취급하여야 할 필요성이 제기된다.[3]

가. 매체독립성

전자정보는 유체물이 아니고 각종 디지털 저장매체에 저장되어 있거나 네트워크를 통하여 전송 중인 정보 그 자체를 말한다. 전자정보는 저장매체와 독립된 정보의 내용이 증거로 되며 이 정보는 값이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 지니는 것이다.[4]

이러한 특성에 따라 전자정보는 원본과 사본의 구별이 곤란하고, 이에 수사기관은 정보저장매체 원본의 훼손을 방지하기 위해 이미징 사본을 이용하여 전자 정보를 분석하고 이미징 사본에서 출력한 문건을 증거로 제출하고 있다. 위 과정에서 디지털 저장매체 원본과 이미징한 사본의 동일성의 문제가 발생한다.[5]

---

2) 대검찰청, 「검찰수사 실무전범Ⅱ」(2008), 261-264쪽; 손지영.김주석,「디지털 증거의 증거능력 판단에 관한 연구」, 대법원 사법정책연구원(2015), 25-29쪽; 전승수, “형사절차상 전자정보의 압수수색 및 증거능력에 관한 연구”, 서울대학교 박사학위논문(2010), 12-15쪽 등 참조

3) 최성필, “디지털 증거의 증거능력”, 검찰 포털 발표자료

4) 양근원, “형사절차상 전자정보의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위논문(2006), 22쪽; 권양섭 “디지털 증거수집에 관한 연구”, 군산대학교 박사학위 논문(2009), 11쪽.

나. 비가시성, 비가독성

전자 정보는 사람의 육안으로는 식별이 불가능하기 때문에 정보저장 매체를 제시하는 것만으로는 증거가 되는 내용을 확인할 수 없고, 그 내용을 모니터 상에 나타내거나 출력장치를 통해 종이 등으로 인쇄하여 제시하였을 때 비로소 가시성, 가독성이 주어진다.[6)]

전자정보 그 자체는 가시성·가독성이 없는 매체독립적인 정보이므로 법정에 증거로 제출되기 위해서는 가시성·가독성이 있는 형태로 변환하여 제출하게 되는데, 과연 위 출력물을 원본으로 인정할 수 있는가 하는 원본성의 문제가 대두된다.[7)]

다. 취약성(변개 용이성)

물리적 증거의 경우 증거물을 조작하면 조작 흔적이 남게 되므로 조작 여부를 비교적 쉽게 판별할 수 있으나, 전자 정보는 하나의 명령만으로도 수많은 디지털 자료를 삭제하거나 변경시킬 수 있고 자료의 일부만을 쉽게 조작할 수도 있다.[8)] 즉 전자정보는 위·변조 및 삭제가 용이하다는 취약성의 특성이 있다.

따라서 전자정보를 수집할 경우에 수집 이후부터는 전자정보가 변조되지 않았다는 것을 입증할 수 있도록 무결성을 확보하는 절차와 기술이 필요하고,[9)] 여기에서 전자정보의 무결성 문제가 제기된다.[10)]

---

5) 대검찰청, 앞의 책, 262쪽.
6) 양근원, 앞의 논문(각주 3), 23쪽.
7) 대검찰청, 앞의 책, 317쪽.
8) 권양섭, 앞의 논문 12쪽 참조.
9) 탁희성.이상진,「디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보 방안」, 형사정책연구원(2006), 36쪽.

라. 대량성

정보저장매체의 저장기술 발달로 인하여 하나의 매체가 저장할 수 있는 데이터의 양이 상당히 확대되었다. 따라서 방대한 데이터 중 범죄관련성 있는 정보를 선별하는 작업 자체가 용이하지 않다는 문제점을 가진다.

따라서 압수수색 영장의 특정 및 집행 범위와 관련한 문제가 발생하고, 대량의 데이터가 대규모로 저장・전송・처리되는 만큼 저장매체를 압수하여 분석하는데 강력한 성능을 가진 시스템이 필요하고 장기간의 시간과 전문적인 지식이 소요되는 경우가 자주 발생한다.[11] 또한 압수한 전자정보의 검색, 분석 등의 과정에서 장시간이 걸리므로 어느 범위까지 참여권을 보장하여야 하는지에 대한 문제가 제기된다.

마. 전문성

디지털 방식으로 자료를 저장하고 이를 출력하는 데는 많은 컴퓨터 기술과 프로그램이 사용된다. 따라서 저장된 자료가 어떤 소프트웨어를 사용하여 저장되었는지 정확하게 규명하지 않으면 자료에 접근하기조차 어려운 문제가 발생한다. 또한 접근하여 수집된 자료라 할지라도 이를 가독성・가시성 있는 자료로 제시하고 그 내용을 해석하는 데는 해당 분야에 대한 전문적 지식 없이는 불가능한 경우가 많고, 법정에 제시된 최종 산출물이 원본 증거에 대한 정확한 해석인지 검증하는 것도 필요하다.[12]

따라서 전자정보의 수집과 분석에 있어 디지털 포렌식 전문가의 도움이 필수적으로 필요하고, 여기에서 전자정보에 대한 신뢰성 문제가 대두된다.[13]

---

10) 김윤섭,.박상용, “형사증거법상 전자정보의 증거능력”, 형사정책연구 제26권 제2호 (2015), 170쪽.
11) 양근원, 앞의 논문(각주 4), 138쪽
12) 양근원, 앞의 논문(각주 4), 139쪽

바. 네트워크 관련성

정보통신기술의 발달로 현재의 디지털 환경은 수많은 컴퓨터가 상호 연결되어 있는 네트워크 환경을 맞이하고 있으며, 전자 정보는 유무선 네트워크를 통해 시간과 공간, 국경의 벽을 넘어서 저장・전송・처리된다.[14] 또한 전자정보는 단순히 저장매체에 저장되어 있는 경우뿐만 아니라 통신 중에도 수집되어야 하는 경우가 있다.

기본적으로 압수수색은 장소의 개념을 전제로 하고 있는데 반해, 네트워크 환경에서는 장소의 개념이 무의미하다. 국내의 토지관할을 넘어서는 법집행을 어느 정도까지 인정할 것인지가 문제되고, 더욱이 국경을 넘는 경우에는 국가의 주권 문제까지 연관될 수 있다. 또한 본사는 서울에 있지만 지방에 메인 서버를 두고 서울 본사와 지방의 각 지사를 네트워크로 연결하여 중요 자료를 저장・공유하는 경우에, 회사의 전자메일, 회계자료, 영업자료 등을 압수하기 위해서는 압수수색 장소를 본사 외에도 메인 서버의 소재지를 추가로 기재해야 하는 등 압수수색 장소의 특정 문제가 발생한다.[15]

13) 대검찰청, 앞의 책, 263쪽.
14) 탁희성.이상진, 앞의 책, 39쪽 권양섭, 앞의 논문, 15쪽.
15) 권양섭, 앞의 논문 15쪽 이하 참조.

3. 전자정보의 압수·수색과 참여

이번 장에서는 전자정보에 대한 압수수색 방식을 규정과 세부 절차에 대해 확인해 보고 전자정보의 수집 및 분석 기법을 검토하여 수사실무 현실을 살펴보고, 압수수색 절차에서의 참여권 보장에 대한 규정과 대법원의 전자정보 압수수색 관련 판결들의 취지들을 조사하여 전자정보 압수수색 시 참여에 대한 구체적인 사례들을 살펴보고자 한다.

가. 전자정보의 압수수색 방식

1) 수사기관의 전자정보 압수수색 방식

전자 증거의 압수수색 방식은 형사소송법 제106조 제3항과 수사기관 실무상으로 크게 세 가지로 나눌 수 있다.

원칙적인 압수·수색 방식으로 (1) 압수수색 장소(이하 '현장')에서 정보저장매체 등을 수색하고 정보전자매체 내 전자정보를 탐색하여 영장 기재 혐의사실과 관련한 정보만을 선별하고 이를 복사 또는 출력하는 방법이다.

현장에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 (2) 현장에서 저장매체 전체를 이미징하여 복제본을 확보하고 이를 수사기관의 사무실로 가져와 복제본을 이용하여 영장 기재 혐의사실과 관련된 정보를 탐색·선별한 후 이를 출력하는 방법과 (3) 현장에 있는 정보저장매체 자체를 수사기관의

사무실로 가져와 저장매체 전체를 이미징하여 복제본을 확보한 후 정보저장매체 원본은 피압수자에게 반환하고 복제본을 이용하여 영장기재 혐의사실과 관련된 정보를 탐색·선별하여 이를 출력하는 방법이다.

2) 전자정보의 압수·수색 방식별 세부 절차[16)]

위 세 가지 방식에 대한 검찰 수사실무에서의 주요 세부 절차는 디지털 포렌식 수사관의 증거 수집 및 분석 검찰 예규[17)]에 의해 다음과 같다.

(1) 원칙적 방식은 ① 압수·수색 사전 준비 → ② 압수·수색 현장에서 저장매체 등 수색 → ③ 저장매체에서 혐의사실과 관련된 전자정보 탐색 및 선별 → ④ 압수할 전자정보의 해쉬값 생성 → ⑤ 전자정보의 문서 출력 및 파일 복제 → ⑥ 압수 목록 교부와 압수 확인서 작성으로 압수·수색 집행이 종료된다.

예외적 방식으로 (2) 압수·수색 현장에서 저장매체 복제본을 생성하는 경우 ① 압수·수색 사전 준비 → ② 압수·수색 현장에서 저장매체 등 수색 → ③ 저장매체에서 혐의사실과 관련된 전자정보 탐색 → ④ 저장매체 원본에 대한 이미지 파일 및 해쉬값 생성 → ⑤ 이미지 파일 압수 확인서 작성 → ⑥ 디지털수사통합업무관리시스템[18)](이하 '디지털업무시스템')에 이미지 파일 등록 → ⑦ 일선 수사부서에서의 탐색 및 이미지 파일에 대한 분석 → ⑧ 분석 결과 디지털업무시스템에 등록 → ⑨ 수사부서에서의 압수 선별 및 문서 출력, 파일 복제 → ⑩ 압수 목록 교부로 압수·수색 집행이 종료된다.

---

16) 김지홍, "디지털 포렌식 절차 모델에 대한 새로운 접근", 석사학위 논문, 56쪽 참조
17) 대검찰청, "디지털포렌식 수사관의 증거 수집 및 분석 규정" [시행 2015.7.16.] 참조
18) 디지털 증거의 수집 및 분석에 관한 사항과 디지털 증거의 보관에 관한 이력 등을 관리하는 전산시스템을 말한다.

한편, (3) 압수·수색 현장에서 저장매체 복제본을 생성하는 경우 ① 압수·수색 사전 준비 → ② 압수·수색 현장에서 저장매체 등 수색 → ③ 저장매체에서 혐의사실과 관련된 전자정보 탐색 → ④ 압수할 저장매체 원본의 해쉬값 생성 및 압수 확인서 작성 → ⑤ 저장매체 원본 봉인 및 운반 → ⑥ 저장매체 원본 봉인 해제 및 이미지 파일 생성 → ⑦ 디지털업무시스템에 이미지 파일 등록 → ⑧ 일선 수사부서에서의 탐색 및 이미지 파일에 대한 분석 → ⑨ 분석 결과 디지털업무시스템에 등록 → ⑩ 수사부서에서의 압수 선별 및 문서 출력, 파일 복제 → ⑪ 압수 목록 교부로 압수·수색 집행이 종료된다.

나. 전자정보의 수집 및 분석 기법

1) 안티포렌식 대응 기법 분석[19)]

디지털 포렌식은 해킹, 사이버 범죄에서 사용되는 컴퓨터, 노트북, 스마트폰 등의 메모리, 운영체제, 애플리케이션, 네트워크 등에 존재하는 다양한 디지털 증거를 분석하므로써, 사이버 범죄의 추적과 조사에 적극 활용되고 있다. 한편, 디지털 포렌식이 다양한 환경에서 적용되고 보편화 됨에 따라 이에 대한 대응으로 안티 포렌식 도구들이 등장하고 있다. 개인이 자신의 개인정보를 삭제하거나 기업에서 중요 기밀정보를 안전하게 파기함으로서 중요 데이터 보호나 개인정보 보호를 위한 정당한 파괴 행위에 안티포렌식 도구들을 활용하고 있다. 최근에는 추적 및 증거물 획득을 원천적이고 자동화된 방법으로 막아주는 전문 제품들이 등장하고 있으며, 다양한 안티포렌식 기법들이 소개되고 있는 실정이다.

19) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지

특히,예 이들 도구를 활용하여 수사를 방해하기 위한 목적으로 증거가 될 가능성이 있는 데이터를 의도적으로 파괴하는 행위는 엄연히 범법 행위가 된다.

가) 안티 포렌식의 정의[20]

안티포렌식은 “포렌식 도구, 수사 및 수사관의 분석을 방해하기 위한 도구와 기술”로 정의한다. 즉, 디지털 포렌식 기술에 대응하여 자신에게 불리하게 작용될 가능성이 있는 디지털 증거를 훼손하거나 숨기려는 일련의 행위를 의미한다. 데이터 파괴, 데이터 암호화, 데이터 은닉, 데이터 조작, 흔적 최소화 등이 대표적이며, 포괄적으로 디지털 증거의 획득을 방해하는 모든 행위가 포함된다. 가장 일반적인 안티포렌식 행위는 수사관들이 수집할 수 없도록 증거물이 될 수 있는 데이터를 삭제하거나 훼손하는 것인데, 예를 들면 파일을 단순 삭제, 하드디스크의 파티션 삭제나 하드디스크 포맷, 파일 또는 하드디스크 암호화 도구 사용, 파일의 확장자 변경, 웹 브라우저 사용 흔적 삭제 등과 같은 행위가 해당된다.

나) 안티포렌식 기술 분류[21]

안티포렌식 기술은 디지털 증거의 분석을 방해하기 위하여 디지털 증거가 될 수 있는 데이터를 훼손하거나 숨기기 위해 사용하는 모든 방법으로, 사용하는 기법과 세부 내용에 따라 표 1과 같이 분류할 수 있다.

---

20) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지, 2쪽
21) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지, 3쪽

[표 1] 안티포렌식 기술 분류

분류	세부	내용
데이터 파괴	완전삭제	분석을 방해하기 위해 중요 데이터를 삭제하거나 훼손
데이터 은닉	암호화	데이터를 암호화하여 디지털 증거 분석을 방해
	심층암호	특정 파일에 중요 정보를 은닉
데이터 수정	조작	데이터를 수정 또는 조작하여 분석이 어렵도록 처리
흔적 최소화		사용한 안티포렌식 도구나 기법의 흔적을 제거

다) 안티 포렌식 대응 기술 분류[22)]

안티포렌식에 대한 일반적인 대응 방안은 다음과 같다. 첫째, 공격자가 데이터를 접근할 수 있는 장소에 데이터를 저장하는 방법이다. 로그를 남기거나 CD-R 또는 DVD-R 등 한번 기록하면 수정할 수 없는 읽기 전용 매체에 데이터를 저장하는 방법이다. 최근 널리 사용한는 클라우드 컴퓨팅을 활용하는 것도 좋은 방법이다. 둘째, 기존 디지털 포렌식 도구들은 안티포렌식에 대응하기에는 기능이 부족한 것들이 많은데, 이들의 기능을 개선하는 방법이다. 현실적으로 쉽지는 않으나, 새로운 방법들을 적용하여 지속적으로 기능을 개선하여야 한다. 셋째, 안티포렌식에 대응하기 위한 전문 도구들을 새롭게 개발하는 방법이다. 데이터 암호화에 대응하기 위하여 키로거(Keylogger)를 개발하여 설치하거나 네트워크 트래픽 분석을 위하여 스니퍼(Sniffer)를 보강하거나 로그를 활용하여

22) 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지, 3쪽

사용자 행위를 모니터링하는 방법이 여기에 속한다. 그러나 이러한 방법은 보수적인 제약 조건이 따르거나 제한적인 환경에서만 적용할 수 있는 단점이 있다. 따라서 안티포렌식에 적극적으로 대응하기 위해서는 안티포렌식 대응 기술(Anti-Anti-Forensics)을 적용해야만 하는데, 안티포렌식 대응 기술은 다음과 같이 분류할 수 있다.

(1) 데이터 복구 방안

삭제한 데이터가 어떤 형태로든 저장매체에 남아 있다면 이론적으로 복구가 가능하지만, 안티포렌식 전용 도구를 이용한 삭제는 일반적으로 복구가 불가능하다. 데이터 복구는 물리적인 복구와 논리적인 복구로 분류할 수 있는데, 물리적인 복구는 저장매체를 파괴하지 않은 경우 복구가 가능하고 이후 논리적인 복구를 수행할 수 있다. 논리적인 복구는 안티포렌식 도구를 이용하여 데이터를 완전삭제하지 않았다면 여러 복구 기법을 동원하여 복구가 가능하다. 단, 데이터 복구율은 저장매체의 상태, 파일 시스템 유형, 데이터 저장방식에 따라 많은 차이가 존재한다.

(2) 데이터 검색 및 탐지방안

데이터 검색 및 탐지 기술은 하드디스크 및 파일 시스템 기반 조사와 파일 기반 조사로 나눌 수 있다. 첫째, 하드디스크 및 파일 시스템 기반 조사에는 Index 기반 탐색과 Bitwise 방법이 있다. Index 기반 탐색은 포렌식 도구에서 키워드에 의존하여 일반 드라이브, 이미지, 파티션 등의 모든 영역을 검색하는 방법으로, 파일 포맷과는 독립적인 조사가 가능하고 속도가 빠른 장점이 있다. Bitwise 방법은 디스크 내의 섹터나 슬랙 공간

(Slack Space)에서 찾을 수 있는 비 할당 영역에 존재하는 간단한 텍스트나 특정 표현들을 찾는 방법으로, 텍스트 뿐만 아니라 이진수 표현 검색도 가능하지만, 단편화가 심하게 되어 있는 경우 조사가 어렵다.둘째, 파일 기반 조사에는 파일 포맷 분석과 해쉬 검증이 있다. 파일 포맷 분석은 파일 시그니처(Signature)에 의존하여 원하는 대상 검색하는 방법으로, 파일 포맷에 의존하므로 파일의 이름 또는 확장자를 변경하더라도 분석이 가능하다. 해쉬 검증은 해쉬 값을 분석함으로써 해당 파일을 찾는 경우로, 이미 알려진 파일의 해쉬값은 NSRL(National Software Reference Library)의 RDS(Reference Data Set) 해쉬셋에 테이블 형태로 제공하고 있다.

(3) 암호 크래킹 방안

암호 크래킹은 암호화된 데이터의 키를 알아내어 이를 복호화하는 기법으로 암호 알고리즘으로 암호화된 데이터의 키를 무차별 대입하는 경우 많은 시간을 소요한다. 그러나 패스워드 기반 암호 체계를 사용하는 경우 복구를 위해서 크래킹 전용 도구를 사용한 사회공학 공격, 사전 공격(Dictionary Attack), 무차별 대입 공격 등을 사용할 수 있다.

데이터를 암호화할 때 AES, RSA 등 널리 사용되는 표준 암호 알고리즘을 이용하여 암호화하는 경우가 많은데, 일반적으로 이들 표준 암호 알고리즘에서는 권장하는 키 크기(AES는 128/192/256비트, RSA는 1024/2048 비트)와 IV(Initial Vector)를 사용하여 데이터를 암호화한다. 이 경우에 암호화 키와 IV를 안전한 장소에 보관하여 알아낼 수 없다면 암호 크래킹은 사실상 불가능하다. 그러나 로그온 패스워드나 파일 암호화는 대부분 사람의 기억에 의존하여 패스워드 또는 암호화키를 관리하는 경우가 많으므로, 사회공학 공격, 사전 공격 등을 사용하여 크래킹 시간을 충분히

단축할 수 있으며, 필요에 따라 전용 도구를 사용하건 직접 개발하여 암호 크래킹을 수행할 수 있다.

(4) 은닉 데이터 탐지 방안

은닉 데이터 탐지 및 분석 기법은 이미지와 같은 멀티미디어 파일 또는 문서 파일 등에 숨겨 놓은 데이터를 탐지하고 분석하는 방법이다. 대상에 따라 멀티미디어 파일 분석과 문서 파일 분석이 있다. 멀티미디어 파일 분석은 데이터를 이미지/오디오/비디오 파을 등에 암호화해 숨기는 기술인 심층암호(Steganography)를 탐지하는 방법인데, 영상 분석, 색상 분석, 통계 분석 기법을 이용한다. 문석 파일 분석은 오피스 문서 등에서 많이 사용하는 문서 파일에 은닉한 데이터, 악성 코드 등을 탐지하는 방법으로, 포맷 분석, 저장 형식 분석 기법을 이용한다.

은닉된 데이터를 탐지하는 기법으로는 영상 분석, 색상 분석, 통계 분석, 포맷 분석, 저장 형식 분석 등을 이용하여 은닉 데이터를 탐지해내거나 데이터 은닉에 사용될 수 있는 영역을 검사하는 방법을 사용한다.

(5) 물리 메모리 분석 방안

휘발성 메모리 분석은 저장매체를 이용하지 않고 메모리 영역에서만 실행되는 기법과 그 흔적을 탐지하기 위한 방법이다. 이는 물리 메모리 영역은 일반적으로 완전삭제 프로그램의 영향을 받지 않는 것으로 알려져 있기 때문이다.

메모리 관련 항목은 물리 메모리, 페이지 파일, 스왑(Swap) 파일 등이 포함될 수 있고, 구체적인 추출 대상 항목은 운영체제 정보, 프로세스 정보, 네트워크 연결 정보, 로그인 정보, 메모리 내 텍스트 정보 등이 해당한다.

(6) 기타 분석 방안

기타 분석 방법으로는 파일 내부의 시간 정보 분석, 일관선 분석, 연관 관계 분석 방법이 있다. 파일 내부의 시간 정보 분석은 어플리케이션의 의해 저장되는 파일 내부에 저장된 시간 정보를 분석하는 방법이고, 일관성 분석은 파일, 메타데이터, 로그 등의 정보를 활용하여 시간의 연속성에 따른 일관성을 분석하는 것이다. 연관 관계 분석은 확률 및 통계 기법을 적용하여 서로 다른 이벤트 사이의 연관 관계를 이용한 분석 방법이다.

2) 디지털 증거 수집도구별 기능 비교

현재 국내에서 가장 많이 사용되고 있는 현장용 디지털 포렌식 도구의 성능에 대하여 비교하였다. CFT는 검찰에서 주로 사용하는 현장용 디지털 포렌식 도구이고, HERA는 경찰청 수사관이 컴퓨터에 대한 전문지식이 없어도 디지털 포렌식 관련 업무를 수행할 수 있도록 경찰이 자체 개발한 도구이다. Encase Portable의 경우는 미국의 Guidance사가 만든 현장용 디지털 포렌식 도구이다. 아래에서 비교한 버전은 CFT의 경우 2010. 개발된 CFT10, HERA의 경우는 2011. 개발된 프로그램, Encase Portable의 경우는 2012. 버전을 기준으로 비교하였다.[23)]

23) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 37쪽.

[표 2] 현장 디지털 포렌식 도구 기능 비교[24)]

분류	지원항목	CFT	Encase Portable	HERA
파일시스템	NTFS	O	O	O
	FAT	O	O	O
	NFS	X	X	X
	EXT2	X	X	X
	EXT3	X	X	X
	EXT4	X	X	X
	HFSX	X	X	X
	UFS	X	X	X
이미지 읽기	E01	O	X	X
	DD	O	X	X
	DFI	X	X	X
이미지 쓰기	E01	O	O	O
	DD	O	O	O
	DFI	O	O	X
논리이미지	LFI	O	O	X
	TAR	X	X	O
물리 드라이브	HDD	O	O	O
	USB / Memory CARD	X	X	X
	논리 드라이브	O	O	O
정보수집	휘발성 정보 수집	O	O	O
	하드 디스크 분석	O	O	O
	메모리 정보 수집	O	O	O
	레지스트리 정보 수집	O	O	O
	인터넷 히스토리	O	O	O
	클라우드 정보수집	X	X	X
	SNS 정보수집	X	X	X
복구	삭제된 파일	O	O	O
	유실 파일	O	O	O
	비할당 영역 복구	O	X	X
	슬랙 영역 복구	O	X	X
안티포렌식 탐지	완전삭제도구 탐지	X	X	X
	파일 은닉 도구 탐지	O	X	X
	가상 드라이브, 암호화 도구 탐지	X	X	X
검색	키워드 검색, 정규식 검색	O	X	O
	비할당 영역 검색	X	X	X
	슬랙 영역 검색	O	X	X
	HWP/DOC 등 파일 키워드 검색	O	O	O
	파일 이름 검색	O	X	O

24) 임한희. 개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구. 석사학위논문. 2012. 38-39쪽.

분류	지원항목	CFT	Encase Portable	HERA
	파일 타입 검색	O	O	O
	개인 정보 검색	O	X	O
시각화	이미지 갤러리 지원	O	X	X
	문서 미리 보기	O	O	X
	헥사뷰	X	X	X
	텍스트 뷰	O	X	X
	데이터 전환	X	X	X
프로젝트	프로젝트 파일 지원	X	X	X
	북마크	O	X	X
기타	운영체제 정보	O	X	O
	사용자 정보	O	X	O
	이메일 분석	O	O	O
	웹검색	O	X	O
	메신저	X	X	O
	USB 히스토리	O	X	O
	이벤트 로그	O	X	O
	원격 사용 정보	O	X	O
	프로세스 분석	O	O	O
	해시데이터 생성 기능	O	O	O
	증거데이터 목록 출력	O	X	O

위 비교에 따르면, 분석 가능한 파일시스템의 경우 NTFS와 FAT만 지원하고 있고, 안티포렌식 도구 탐지 기능은 CFT가 지원하고 있으나, 완전 삭제 프로그램, 가상 드라이브, 암호화 프로그램, 파일 은닉 프로그램 등 다양한 안티포렌식에 대한 탐지 기능은 부족하다.

그리고 가장 중요한 기능이라고 볼 수 있는 디지털 데이터에 대한 복구 기능, 검색 기능, 유용한 정보 분석 기능이 상호간에 차이가 있고, 그 지원 정도도 다양한 현장 상황에 대응하기에는 부족하여 문제된다.[25]

25) 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012), 제37쪽.

다. 압수·수색 절차에서의 참여

1) 압수수색 절차와 참여권 관련 규정

형사소송법은 제121조(영장집행과 당사자의 참여)에서 '검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있다'고 규정하고, 이를 수사기관의 압수에 준용하고 있다(형사소송법 제219조).

압수수색 절차에서 사건관계인인 피고인이나 변호인이 참여하는 것은 공개주의를 원칙으로 하는 법원의 절차에서 사건관계인들이 참여함으로서 절차의 적정한 진행을 도모하고, 절차 과정을 봄으로써 검사는 검사대로 소추를 위한 준비를 하고, 피고인은 피고인대로 방어를 준비할 수 있도록 하는 취지이다.[26]

한편 우리 형사소송법은 피압수자의 압수수색 절차 참여를 별도 조문으로 규정하고 있지는 않으나, 압수수색영장의 집행 절차에 관한 조문들을 종합하면 피압수자로서의 지위에서 참여가 인정될 것이다. 즉 형사소송법은 압수수색영장을 집행하는 때에는 처분을 받는 자에게 영장을 제시하여야 한다고 규정하고(제118조, 제219조), 타인의 주거 등에서 압수수색을 하는 때에는 주거주 등을 참여하게 하여야 한다고 규정하고(제123조 제2항, 제219조), 나아가 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준하는 자에게 교부하여야 한다고 규정하고(제129조, 제219조) 있는 바, 이 규정들을 준수하게 되면 피압수자는 압수절차에 참여하게 될 것이다.[27] 이와 같은 피압수자의 지위에서 참여는 집행을 받는 당사자를 보호하고 영장집행 절차의 적정성을 담보하려는데 그 목적이 있다.[28]

---

26) 백형구 등, 「주석 형사소송법 I 」제4판, 한국사법행정학회(2009), 530쪽.
27) 이완규, "디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 확보 방압", 대검찰청 이프로스 게시판(2015. 8.), 11쪽.

2) 전자정보 압수·수색 관련 대법원 주요 판례

가) 전교조 본부 사무실 압수수색 사건[29]

(1) 전자정보 압수수색 영장의 예외적인 집행에 대한 적법 요건[30]

전자정보에 대한 압수·수색영장을 집행할 때에 집행현장 사정상 원칙적 방식의 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 '반출'하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장기재 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의의 원칙상 당연하다. 그러므로, 범죄혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다. 한편 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이

28) 백형구 등, 앞의 책, 533쪽.
29) 대법원 2011. 5. 26. 자 2009모1190결정 준항고기각결정에 대한 재항고(전국교직원노동조합 본부 사무실 압수수색 사건)
30) 전자정보에 대한 압수·수색영장을 집행할 때 저장매체 자체를 수사기관 사무실 등 외부로 반출할 수 있는 예외적인 경우 및 위 영장 집행이 적법성을 갖추기 위한 요건

인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.

(2) 전교조 본부 사무실의 압수·수색에 대한 준항고[31]

영장의 명시적인 근거 없이 수사기관이 임의로 정한 시점 이후의 접근 파일 일체를 복사하는 방식으로 8,000여개의 파일을 복사한 영장집행은 원칙적으로 압수·수색영장이 허용한 범위를 벗어난 것으로서 위법하다고 볼 여지가 있는데, 압수수색 전 과정에 비추어 볼 때, 수사기관이 영장에 기재된 혐의사실 일시로부터 소급하여 일정시점 이후의 파일들만 복사한 것은 나름대로 대상을 제한하려고 노력한 것으로 보이고, 당사자측도 그 적합성에 대하여 묵시적으로 동의한 것으로 보는 것이 타당하므로, 위 영장집행이 위법하다고 볼 수는 없다.

(3) 대상결정의 취지

위 결정은 전자증거 압수수색에 관하여 '원칙적 선별압수, 예외적 매체압수'원칙을 천명한 리딩케이스로서 관련성 유무를 확인하지 않은 채 일괄복사 한 압수수색은 위법하다고 볼 여지가 있지만, 수사기관의 노력과

31) 수사기관이 전국교직원노동조합 본부 사무실에 대한 압수·수색영장을 집행하면서 방대한 전자정보가 담긴 저장매체 자체를 수사기관 사무실로 가져가 그곳에서 저장매체 내 전자정보파일을 다른 저장매체로 복사하였는데, 이에 대하여 위 조합 등이 준항고를 제기한 사안에서, 위 영장 집행이 위법하다고 볼 수 없다는 이유로 준항고를 기각한 원심의 조치를 수긍한 사례

당사자 측의 묵시적 동의를 이유로 위법하다고 볼 수 없다고 하여 수사기관이 매뉴얼에 따른 압수·수색을 한 경우 선의의 항변이 가능하다는 여지를 남긴 것으로 평가 할 수 있다[32]

나) 통합진보당 내란음모에 관한 사건[33]

(1) 당사자에 대한 참여통지 규정 위반 주장

항소이유로 피고인들에 대한 모든 압수·수색절체에서 당사자에게 미리 영장 집행에 참여할 것을 통지하지 않은 위법이 있다는 것이나, 항소심 재판부는『기록에 의하면, 압수·수색 당시 국정원 수사관들이 사전에 피고인들이나 그 변호인들에게 영장 집행의 일시와 장소를 통지하지 않음은 인정되나, 영장 기재 범죄사실의 죄질이 중하고 위험성도 크며 그 법정형도 무거운 점, 압수 대상물들이 주로 문건 또는 전자정보로서 비교적 은닉이나 인멸이 용이한 점, 이 사건 압수수색 처분을 받는 당사자가 피고인들 본인이었던 점 등을 감안하면, 영장 집행 사실을 미리 통지하였을 경우 증거인멸 우려가 컸다고 보인다. 따라서 이 사건 압수·수색은 '급속을 요하는 때'에 해당하여 형사소송법 제122조 단서가 정한 사전통지의 예외사유에 해당되므로, 이를 위법으로 볼 수 없다.[34]』고 판시하였다.

32) 노명선, '디지털 증거의 압수·수색에 관한 판례 동향과 비교법적 고찰', 형사법의 신동향 통권 제43호(2014.6.) p.145이하
33) 대법원 2015. 1. 22. 선고 2014도10978 / 서울고등법원 2014. 8. 11. 선고 2014노762 / 수원지방법원 2014. 2. 17. 선고 2013고합620, 624(병합), 699(병합), 851(병합)
34) 위 2014노762 판결 p.11이하

(2) 영장 집행절차의 명확성·공정성이 없어 위법하다는 주장

항소이유로 이 사건 각 압수수색 과정에서 사전통지가 생략되는 등 당사자의 참여권이 박탈되었고, 이를 대신할 적법한 참여인의 참여도 없었으며, 절차를 집행한 수사관들이나 입회인들이 증거의 발견 장소나 경위를 밝히지 못하여, 이 사건 압수수색은 절차의 명확성·공정성이 인정되지 않아 위법이 있다는 것이다.

이에 대해 항소심 재판부는『이 사건 압수수색은 일부 절차규정 준수 여부가 문제되는 부분이 있기는 하나, 대부분의 경우 형사소송법과 형사소송규칙이 정한 절차 규정이 준수되었고, 피고인 본인이 참여하거나 형사소송법이 참여하도록 규정한 참여인들이 참여한 상태에서 진행되었다. 위 참여인들은 각 압수수색 과정에서 압수물 선별, 디지털 포렌직, 압수목록 확인 등 과정에 관여하였고, 수사관들의 처분에 이의를 제기하거나 의견을 제시하고 압수수색을 저지하기도 하는 등 실질적이고 충분한 참여권을 행사하였다. 수사관들은 형사소송법이 정한 참여인 이외에도 민간 포렌직 전문가나 경찰관 또는 국회직원 등을 입회시키기도 하였고, 압수수색 전 과정을 영상녹화하기도 하는 등 절차의 적정성을 담보하기 위하여 형사소송법 및 규칙이 정한 것 이상의 조치를 취하기도 하였다. 또한 각 압수수색 과정에서 압수된 물건들은 이 사건 혐의사실이나 피고인들과의 관련성이 인정되거나 무관하다고 단정하기 어려운 것들로서 영장이 허용한 압수의 범위 내의 것들이다. 한편, 변호인의 참여권을 규정한 형사소송법 제121조가 형사소송법 제243조의2와는 달리, 변호인을 반드시 참여하게 하여야 한다고는 규정하고 있지 않은 점, 형사소송법 제122조 단서가 급속을 요하는 때에는 피고인과 변호인에 대한 참여통지를 생략할 수 있도록 규정하고 있는 점 등을 고려할 때, 수사관들이 변호인이 참여하기 전에 피고인에 대한 일부 압수수색절차를 진행하였다고 하더라도 이를 위법하다고 볼 수 없다』고 판시하였다.[35)]

(3) 전자정보 탐색·복제·복구·복호화 과정 참여권 침해 주장

항소이유로 수사관들이 저장매체를 전부 복제하여 압수한 후 해독된 암호로 암호화된 파일을 복호화 하거나 삭제된 파일을 복구하고 영장 기재 범죄 혐의 관련 전자정보를 탐색하여 문서로 출력하는 과정 역시 영장 집행의 일환에 포함된다. 그 과정에서 피고인과 변호인에게 집행 일시·장소를 통지하지 않은 위법이 있다는 것이다.

이에 대해 항소심 재판부는『법이 정한 절차에 따르지 아니하고 수집한 압수물의 증거능력 인정여부를 최종적으로 판단함에 있어서는 실체적 진실규명을 통한 정당한 형벌권 실현도 헌법과 형사소송절차를 통하여 달성하려는 중요한 목표이므로, 형식적으로 보아 정해진 절차를 따르지 아니하고 수집한 증거라는 이유만으로 획일적으로 그 증거의 증거능력을 부정하는 것 역시 헌법과 형사소송법의 이념에 반하므로, 증거 수집과정에서 이루어진 절차 위반행위는 절차 조항의 취지와 위반의 정도, 구체적인 위반 경위와 회피 가능성, 절차 조항이 보호하고자 하는 권리 또는 법익의 성질과 침해 정도 및 피고인과의 관련성, 절차위반행위와 증거수집 사이의 인과관계 등 관련성의 정도, 수사기관의 인식과 의도 등을 전체적·종합적으로 살펴볼 때, 수사기관의 절차 위반 행위가 적법절차의 실질적인 내용을 침해하는 경우에 해당하지 아니하고, 오히려 그 증거의 증거능력을 배제하는 것이 헌법과 형사소송법이 형사소송에 관한 절차조항을 마련하여 적법절차의 원칙과 실체적 진실규명의 조화를 도모하고 이를 통하여 형사사법 정의를 실현하려 한 취지에 반하는 결과를 초래하는 것으로 평가되는 예외적인 경우라면, 법원은 그 증거를 유죄의 증거로 사용할 수 있다고 보아야 한다(대법원 2007. 11. 15. 선고 2007도3061 전원합의체 판결 참조)』고 전제한 뒤, 다음과 같은 사정을 종합하면 이 사건 압수

35) 위 2014노762 판결 p. 12 이하

수색 과정에서 수집된 증거는 복호화 과정 참여권과 관련된 절차 위반에도 불구하고 유죄의 증거로 사용될 수 있는 예외적인 경우에 해당된다고 판단하였다.

① 형사소송법 제121조, 제122조는 피고인 등의 참여권을 보장하고 있고, 집행의 일시·장소를 미리 통지하도록 규정하고 있다. 하지만, 피고인 등을 반드시 참여시켜야 한다고는 규정되어 있지 않으며, 참여권자가 불참의사를 명시하거나 급속을 요하는 때에는 참여통지를 생략할 수 있도록 규정하고 있다. ② 피고인들은 일부 압수수색 과정에는 직접 참여하기도 하였고 직접 참여하지 아니한 압수수색절차에도 피고인들과 관련된 참여인들의 참여가 있었으므로, 추후 수사기관이 압수물에 관하여 영장 기재 범죄혐의 관련 전자정보를 탐색할 것을 예상할 수 있었을 것임에도 이후 수사기관에 압수물 분석과정 등에 대한 참여권 보장을 요청하지는 않았다. ③ 통상적으로 손상된 전자정보 저장매체의 복구나 암호의 해독, 삭제된 파일의 복원 과정 등은 그 성공 가능성을 미리 예측할 수 없고, 그 방법이나 소요시간 등도 가늠하기 어려워 이러한 조치가 수반되는 정보 분석 과정의 경우 피고인 등의 참여권을 완전히 보장하기란 현실적으로 어려움이 있다. ④ 이 사건 수사관들이 피고인과 변호인들에게 복호화 과정의 집행일시와 장소를 사전 통지하지 않은 것은 영장 집행 종료시점에 관하여 나름대로 해석한 결과인 것으로 볼 여지가 있었고, 피고인들과 변호인의 참여를 의도적으로 배제하려 하였던 것으로는 보이지 않는다. ⑤ 압수된 저장매체 중 증거로 제출된 것은 추가적인 정보저장이나 내용의 변경이 불가능한 매체이거나, 객관성이 인정되는 제3자의 서명에 의한 봉인조치에 의해 보존되어 있고, 그 해쉬값도 보존되어 있다. 또한 압수 및 복호화 관련 절차에 참여한 증인들의 증언 등을 통하여 그 보관의 연속성 등이 인정되므로, 수사기관이 분석 과정에서 정보를 훼손하거나 조작을 가할

개연성은 매우 낮아 보이고, 복호화 등 과정에 대한 참여통지 누락이 이 사건 증거수집에 어떠한 영향을 미쳤다고 보이지 않는다.』[36]

이에 대한 상고심에서 대법원도『수사관들이 압수한 디지털 저장매체 원본이나 복제본을 국정원 사무실 등으로 옮긴 후 범죄혐의와 관련된 전자정보를 수집하거나 확보하기 위하여 삭제된 파일을 복구하고 암호화된 파일을 복호화 하는 과정도 전체적으로 압수·수색과정의 일환에 포함되므로 그 과정에서 피고인들과 변호인에게 압수·수색 일시와 장소를 통지하지 아니한 것은 형사소송법 제219조, 제122조 본문, 제121조에 위배되나, 피고인들은 일부 현장 압수·수색 과정에는 직접 참여하기도 하였고, 직접 참여하지 아니한 압수·수색 절차에도 피고인들과 관련된 참여인들의 참여가 있었던 점, 현장에서 압수된 디지털 저장매체들은 제3자의 서명하에 봉인되고 그 해쉬(Hash)값도 보존되어 있어 복호화 과정등에 대한 사전통지 누락이 증거수집에 영향을 미쳤다고 보이지 않는 점 등을 감안하면, 위 압수·수색 과정에서 수집된 디지털 관련 증거들은 유죄 인정의 증거로 사용할 수 있는 예외적인 경우라고 본 원심의 판단은 정당하다고 판시[37]하였다.

36) 위 2014노762 판결 p. 17 이하
37) 위 대법원 2014도10978 전합 판결 p. 17 이하 대법원 2015. 1. 22. 선고 2014도10978

다) 대법원 2011모1839 준항고 인용결정에 대한 재항고

(1) 사건 개요

검사는 갑 회사에 대한 배임혐의로 압수・수색영장(제1영장)을 발부받아 갑 회사 빌딩 내 을 사무실을 압수·수색하였는데 저장매체에 유관정보와 무관정보가 혼재된 것으로 판단하여 갑 회사의 동의하에 저장매체 자체를 봉인하여 반출한 뒤 수사기관 사무실로 반출한 다음 관계자의 참여하에 봉인을 해제하고 전체를 이미징하여 다른 저장매체에 복제하였다.(제1처분)

이미징한 복제본을 외장 하드디스크에 재복제하였고(제2처분), 외장 하드디스크를 탐색하던 중 갑 회사의 별건 범죄혐의 관련 전자정보 등 무관정보를 발견하고 문서로 출력(제3처분)하였다. 제2・3처분 당시에 을 측에 참여기회를 부여하지 아니하였다.

이후 을 측에 참여를 보장하지 않은 채 다른 검사가 별건 정보를 소명자료로 제출하여 압수·수색영장(제2영장)을 발부 받아 외장 하드디스크에서 별전 정보를 탐색·출력하자, 갑 회사는 검찰의 압수처분이 위법하다며 준항고를 제기하였고, 원심은 제1영장의 집행 과정 전체에 당사자의 참여가 보장되지 않았고, 영장 범죄사실과 무관한 전자정보까지 무차별 복제・출력되었음을 이유로 제1, 2, 3처분을 각 취소하는 준항고 인용결정을 하자 검찰이 재항고를 제기하였다.

(2) 결정 요지

(가) 제1 영장에 기한 압수·수색

① 전자정보는 복제가 용이하여 전자정보가 수록된 저장매체 또는 복제본이 압수・수색 과정에서 외부로 반출되면 압수・수색이 종료한

후에도 복제본이 남아 있을 가능성을 배제할 수 없고, 그 경우 혐의사실과 무관한 전자정보가 수사기관에 의해 다른 범죄의 수사의 단서 내지 증거로 위법하게 사용되는 등 새로운 법익침해를 초래할 가능성이 있으므로, 혐의사실 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는 조치가 중요성을 가지게 된다.

따라서, 예외적으로 저장매체 또는 복제본을 수사기관 사무실 등으로 옮겨 이를 복제·탐색·출력하는 경우에도 피압수자나 그 변호인에게 참여의 기회를 보장하여 혐의사실과 무관한 전자정보의 복제를 방지하는 적절한 조치가 필요하며, 그러한 조치가 취해지지 않았다면 절차 위반 행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수·수색이 적법하다고 평가할 수 없고(대법원 2011. 5. 26.자 2009모1190결정 등 참조), 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였다 하더라도 달리 볼 것은 아니다.

② 전자정보에 대한 압수·수색 과정에서 이루어진 현장에서의 저장매체 압수·이미징·탐색·복제 및 출력행위 등 수사기관의 처분은 하나의 영장에 의한 압수·수색과정에서 이루어지는 것이므로, 특별한 사정이 없는 한 당해 압수·수색 과정 전체를 하나의 절차로 파악하여 그 과정에서 나타난 위법이 압수·수색 절차 전체를 위법하게 할 정도로 중대한지 여부에 따라 압수·수색 절차 전체를 취소할 것인지를 가려야 할 것이다. 여기서 위법의 중대성은 위반한 절차조항의 취지, 전체과정 중에서 위반 행위가 발생한 과정의 중요도, 그 위반사항에 의한 법익침해 가능성의 경중 등을 종합하여 판단하여야 한다.

③ 제1처분은 저장매체 자체 반출 사유가 인정되고, 저장매체 원본을 조속히 반환하기 위한 목적으로 당사자의 묵시적 동의와 복제과정의 참여가 있었으므로 적법하나, 제2·3처분은 압수·수색의 목적에 해당하는 중요한 과정인데 그 과정에 참여권을 보장하지 않았고, 더구나 혐의사실과 무관한 정보까지 재복제·출력한 점 등 위법의 중대성에 비추어 볼 때, 제1처분까지 압수수색이 적법하다 하더라도 전체적으로 제1영장에 기한 압수·수색 처분은 취소되어야 한다.

(나) 제2영장에 기한 압수수색

전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대해서도 적법하게 압수·수색을 할 수 있으며, 이러한 경우 별도의 압수·수색절차는 최초의 압수·수색절차와 구별되는 별개의 절차이고, 별도 범죄혐의와 관련된 전자정보의 피압수자는 최초의 압수·수색이전부터 해당 전자정보를 관리하고 있던 자라 할 것이므로, 특별한 사정이 없는 한 그 피압수자에게 형사소송법 제219조, 제121조, 제129조에 따라 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피압수자의 이익을 보호하기 위한 적절한 조치가 이루어져야 한다.

그런데, 제2영장 청구 당시 압수할 물건으로 삼은 정보는 제1영장의 피압수자에게 참여의 기회를 부여하지 않은 상태에서 임의로 재복제한 외장하드디스크에 저장된 정보로서 그 자체가 위법한 압수물이어서 앞서 본 별건 정보에 대한 영장청구 요건을 충족하지 못한 것이므로, 비록 제2영장이 발부되었다고 하더라도 그 압수·수색은 영장주의 원칙에 반하는 것으로 위법하다.

3) 판례 분석[38]

소위 종근당 사건의 대법원 2011모1839 결정은 디지털 저장매체의 압수와 이미징 절차에 피압수자가 참여하였다고 하더라도, 더 나아가 그 저장매체에 있는 정보를 탐색·출력하는 과정에도 당사자의 참여가 요구되는가의 문제에 대해, 정보를 탐색·출력하는 과정에 피압수자의 참여가 이루어지지 않은 경우에는 피압수자에게 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수절차가 위법하다는 취지로 해석하고 있는 것으로 풀이된다.

이와 같은 대법원의 해석은 디지털 정보에 대한 압수수색 영장을 집행함에 있어서 현장에서 저장매체 전체를 이미징하여 증거사본을 확보하는 과정과 정보저장매체 자체를 수사기관의 사무실로 가져와 그것을 이미징하여 증거사본을 확보하는 과정, 그리고 이미징 사본에서 영장에 기재된 범죄혐의 관련 정보를 검색하여 해당 부분을 출력하거나 해당 부분의 파일을 복사하는 과정이 모두 전체적으로 압수수색영장의 집행과정에 포함되므로 정보를 검색하거나[39] 출력하는 과정에도 형사소송법 제121조 규정에 따라 피압수자의 참여를 보장하여야 하고, 그 참여권을 보장하지 않는 경우에는 압수절차가 위법하다고 보는 것으로 해석된다.

다만, 대법원은 전자정보의 특성으로 인해 영장 범죄사실과 관련성이 없는 디지털 정보가 수사기관에 의해 다른 범죄의 수사단서 내지 증거로 위법하게 사용되는 등 새로운 법익침해를 초래할 가능성이 있으므로 혐의사실과 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는

38) 최성필, “디지털 증거의 증거능력”, 이프로스 발표자료, 13쪽
39) 대법원은 이와 같은 검색 행위를 ‘탐색’으로 표현하고 있는 바, 용어에 있어 통일을 기하기 위해 이하에서는 탐색으로 표현하기로 한다.

조치가 중요성을 가지게 된다는 전제 하에, 위와 같은 피압수자의 참여권이 절차적으로 보장되어야 한다는 것이므로 결국, 대법원 결정의 주된 취지는 수사기관으로 하여금 영장 범죄사실과 관련성이 없는 정보의 취득을 제한하고자 하는 것에 있다고 할 것이다.

4. 압수·수색 영장 집행 시 참여권 보장 방안

이하에서는 전자정보의 압수·수색과 관련한 대법원 전원합의체 결정과 수사기관의 실무를 조화롭게 해석하여 전자정보의 압수수색 과정에서 절차의 적정성을 보장하는 한편, 실체적 진실을 발견함으로써 형사사법 정의를 실현할 수 있는 피압수자의 참여권 보장 방안을 제시하고자 한다.

구체적 방안으로, 전자정보의 압수수색 집행 과정에서 피압수자나 참여권자에게 참여을 보장하는 방법에 대해 모색해 보고, 해당 참여 보장 방법을 전자정보의 압수수색 영장 집행 각 과정에 적용하고자 실무상 압수수색 집행 과정을 장소별, 그리고 장소 내 각 단계별로 분류하여 시간적 순서로 배열하였다. 그리고 각 단계별로 참여 보장 방법을 적용해 보고자 한다.

가. 피압수자의 참여권 보장 방법

전자정보의 압수수색 영장 집행 과정에서 피압수자나 참여권자(이하 '피압수자'라고 함)에게 참여을 보장하는 방법으로는 압수수색 영장 집행의 장소와 일시를 피압수자가 인지하여 참여의사를 선택할 수 있어야 하며, 참여를 신청할 경우 압수수색 영장 집행 과정에 참여할 수 있어야 할 것이다.

전자정보의 압수수색 집행 과정은 기존 유체물과 달리 시·공간적으로 불연속적이어서 피압수자는 압수수색 집행 과정에 대한 정보를 제공 받아야 참여의사를 선택할 수 있을 것이다.

전자정보의 압수수색 집행 과정은 3장 1절 전자정보의 압수수색 방식

에서 살펴본 봐와 같이 압수수색 장소뿐만 아니라 수사기관 사무실 등 외부에서도 진행되어 공간적으로 불연속적이고, 수사기관 사무실 등 외부에서 이루어지는 압수수색 과정은 저장매체 복사본에 대한 분석 과정 등 여러 과정으로 나누어 볼 수 있는데, 각 과정별 종료시점을 예측하기 힘들고 시간적으로도 장시간 소요된다. 이런 시·공간적 특성으로 인해 피압수자는 압수수색 집행 과정에 대한 정보 부족으로 참여권 행사에 제약이 따른다. 이를 해결하기 위해서는 수사기관에서 압수수색 집행 과정에 대한 정보를 피압수자에게 제공하는 것이 필요하다.

나. 전자정보의 압수수색 집행 각 과정에서의 참여 보장

현재 실무상 대검찰청 예규[40]에 의해 저장매체 원본이 제출되어 압수수색 현장에서 반출되는 경우 피압수자에게 이미징 등 과정에 대한 참관여부를 확인하고 있으며, 이미징 등 과정에 참관을 신청한 경우 참관예정자에게 참관일정을 통지한다. 이때 참관일정은 수사기관 사무실 등 외부에서 압수수색 집행 과정이 시작되는 시점이고, 참관인 입회하에 봉인된 저장매체들의 봉인 해제부터 이미징 작업 수행, 저장매체 복제본 디지털수사통합업무관리시스템 등록을 수행한다. 그러나 그 이후 압수수색 과정들인 저장매체 복제본에 대한 분석 과정이나 정보 탐색 과정 등에 대하여 구체적인 참여 관련 규정은 없는 실정이다.[41]

---

40) 대검 예규 제805호 “디지털포렌식 수사관의 증거 수집 및 분석 규정”, 2015.7.16. 시행

41) 제19조 (정보저장매체 등의 등록 및 책임자등의 참여)

① 제15조 제1항 단서의 압수·수색의 경우 및 제9조 제2항의 분석 의뢰를 받은 경우에는 대상 정보저장매체 등의 봉인을 해제한 후 이에 기억된 정보에 대하여 이미지 파일로 복제하여, 이를 디지털수사통합업무관리시스템에 등록하고, 대상 정보저장매체 등은 재봉인하여 지원요청자에게 인계한다. <개정 2015.7.16.>

② 전항의 경우 책임자 등 참여권자의 요청이 있는 경우 참여를 보장하여야 한다. 책임자 등이 이미징 과정 등에 참여한 경우에는 별지 제5호의 서식에 따라 확인서를 작성토록 한다. <개정 2015.7.16.>

이런 참여 관련 규정이 없는 압수수색 과정들에 대한 진행 정도나 종료 여부 등의 정보가 피압수자에게는 제공될 수 있어야 한다. 저장매체 복제본에 대한 분석 과정에 대한 소요시간은 저장매체의 용량과 활용되는 분석 기법에 따라 매우 상이하고 장시간이 걸리기 때문에 진행 정도를 예측하기가 불가능하므로 분석 과정 이후 압수수색 과정들이 언제 진행이 될지는 진행상황에 따라 다를 것이다. 피압수자가 이미징 등 과정에 참여하더라도 장시간이 걸리고 종료시점이 예측되지 않는 저장매체 복제본의 분석 과정을 참관하기 위해 수사기관 사무실에 계속해서 남아 있는 것은 피압수자도 힘들고 수사기관도 사무실 보안 등의 어려움이 따를 것이다.

이하에서는 전교조 본부 사무실 압수수색 사건[42] 등 전자정보의 압수·수색과 관련한 대법원 판례에서 설시[43]한 압수수색 현장에서나 수사기관 사무실 등 외부에서 전체 과정을 통해 피압수·수색 당사자나 변호인의 계속적인 참여권을 보장하기 위한 적절한 조치에 대하여 장소별, 장소 내 압수수색 과정을 분류하여 각 과정별로 제안해 보려고 한다.

---

42) 대법원 2011. 5. 26. 자 2009모1190결정 준항고기각결정에 대한 재항고(전국교직원노동조합 본부 사무실 압수수색 사건)

43) 대법원 2011.05.26. 자 2009모1190 결정[준항고기각결정에대한재항고]
검사나 사법경찰관이 압수·수색영장을 집행할 때에는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.

1) 압수·수색 현장에서의 참여

압수수색 장소에 있는 정보저장매체 등에서 영장 기재 혐의사실과 관련한 정보를 수색하여 이를 복사 또는 출력할 수 있는 경우에는 압수수색 집행 시작 시 영장 제시를 하여 피압수자는 참여권 행사가 비교적 잘 이루어질 수 있다. 현장에서 혐의사실과 관련 있는 전자정보를 선별할 수 있는 경우에는 피압수자나 참여인은 파일 복사되거나 문서 출력되는 전자정보에 대한 무결성 입증 확인을 하기 위해서도 현장에 있어야 할 것이다.

가) 압수 현장에서의 영장집행에 대한 통지

형사소송법 제121조는 압수수색 영장 집행 시 당사자는 '참여할 수 있다'고 규정하고 있어 당사자의 참여권을 임의적 참여로 규정하고 있으며, 법 제122조는 압수수색영장 집행 시 원칙적으로 사전에 집행의 일시와 장소를 통지하도록 규정하고 있다. 현재 수사실무에서 피압수자에게 영장을 제시하고 집행 과정에 참여할 수 있게 잘 이루어지고 있다고 본다. 대법원 판례 등에서 압수 현장에서의 참여권 보장에 대한 이슈는 없다.

그러나 당사자가 참여하지 아니한다는 의사를 명시한 때나 급속을 요하는 때에는 예외로 한다는 규정도 있다. 당사자가 참여하지 아니한다는 의사를 명시할 때에는 당사자에게 확인를 반드시 받아야 하고 수사실무상 압수의 목적을 달성하기 위해 보안유지가 필요한 경우에는 대법원 판례의 '급속을 요하는 때'라는 해석[44]에 적합해야 할 것이다. 급속을 요하는 경우에도 사후적으로 피압수자의 참여권 보장과 증거의 무결성 확인 절차 등을 하여야 할 것이다.

---

44) 대법원 2012.10.11. 선고 2012도7455판결, '급속을 요하는 때'라는 해석은 압수수색의 실효를 거두기 어려울 경우를 말함

나) 정보 탐색·선별 및 출력·복제 절차에의 참여

대법원 판결에 따르면 압수·수색 집행 전 과정에서 피압수자의 참여를 보장하여야 한다고 설시하였으므로, 디지털포렌식 도구를 활용하여 탐색하고 혐의사실과 관련 있는 전자정보를 선별하여 압수·수색를 종료할 수 있다면 이 탐색·선별 과정에도 피압수자를 참여시켜 영장 집행 과정을 확인하게 하여야 할 것이다.

또한 추후 증거의 무결성 논란을 방지하기 위하여 압수 대상인 전자정보에 대한 문서 출력 및 파일 복사 시에 해쉬값을 생성하여 책임자 등의 확인 서명[45]을 받아야 한다. 정보저장매체의 이미징 복사본이나 정보저장매체 자체를 봉인하여 수사기관 사무실로 운반되는 경우에도 피압수자가 봉인 과정에 참여하여 서명날인을 받아야 할 것이다.

2) 수사기관 사무실에서의 참여권 보장 절차

압수수색 현장의 사정이나 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한하여 예외적으로 저장매체 자체나 저장매체 복사본을 수사기관 사무실 등 외부로 반출하는 방식으로 압수·수색이 가능하다.[46] 이런 방식에서는

45) 대검찰청, 디지털포렌식 수사관의 증거 수집 및 분석 규정, 시행 2015.7.16

46) 대법원 2011.05.26. 자 2009모1190 결정[준항고기각결정에대한재항고]
전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색

저장매체 원본나 복사본을 수사기관 사무실 등에서 탐색·복제·출력 과정에서 참여권 보장 관련 문제가 있을 수 있다.

가) 압수물의 봉인 해제 및 이미징 생성·등록 과정에서의 참여

압수수색 현장에서 정보저장매체 원본이나 복제본이 수사기관 사무실로 옮겨지면 검찰의 경우는 저장매체의 이미지를 디지털수사통합업무관리시스템에 등록하여야 한다.[47] 이를 위해 먼저 압수물의 봉인해제가 필요하다.

피압수자가 봉인해제 및 복제, 이미지 과정에 참여를 신청한 경우 수사기관은 봉인해제 및 복제과정에 피압수자를 입회시키고 복제가 완료되면 복제본의 해쉬값을 생성하여 입회자로부터 확인서에 서명을 받고 저장매체 원본은 피압수자에게 반환하여야 할 것이다. 수사실무상에서 해당 과정들은 전자정보의 무결성을 확보하는 차원에서도 피압수자의 참여가 필요하므로, 참여권 보장과 관련한 문제는 발생하지 않는다.

나) 저장매체 분석을 통한 전자정보의 수집 과정에서의 참여

압수수색 절차에서 사건관계인인 피고인이나 변호인이 참여하는 것은 공개주의를 원칙으로 하는 법원의 절차에서 사건관계인들이 참여함으로서 절차의 적정한 진행을 도모하고, 절차 과정을 봄으로써 검사는 검사대로

영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다.

47) 대검찰청, 디지털포렌식 수사관의 증거 수집 및 분석 규정, 시행 2015.7.16

소추를 위한 준비를 하고, 피고인은 피고인대로 방어를 준비할 수 있도록 하는 취지이다.[48] 피압수자의 지위에서 참여는 집행을 받는 당사자를 보호하고 영장집행 절차의 적정성을 담보하려는데 그 목적이 있다.[49]

한편, 대법원은 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 '반출'하여 영장기재 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보았으며, 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다고 판시[50]하였다. 저장매체 자체나 복제본에 대한 분석 과정도 혐의사실 관련 정보를 탐색하기 전이나 도중에 이루어지므로, 이 과정 또한 압수·수색영장 집행의 일환에 포함된다고 보아야 할 것이다.

수사기관의 입장에서는 피압수자나 사건관계인을 수사기관 사무실에서 전 과정을 참여시키는 것은 여러 어려움이 따를 수 있다. 수사기관의 증거수집 기법들이 노출될 수 있으며, 정보저장매체의 분석 과정에는 상당한 시일이 걸리는데, 피압수자나 사건관계인을 지속적으로 참여시키는 것에 대한 시·공간적인 제약도 있을 것이다.

그럼에도 불구하고, 수사기관은 범죄와 무관한 정보에 관한 피압수자 사생활의 비밀과 자유, 정보에 대한 자기결정권 등에 대한 침해를 방지

48) 백형구 등, 「주석 형사소송법 Ⅰ」제4판, 한국사법행정학회(2009), 530쪽.
49) 백형구 등, 앞의 책, 533쪽.
50) 대법원 2011. 5. 26.자 2009모1190결정

하려고 노력함으로써, 사실인정의 근거가 되는 자료를 발견·수집하는 과정에서 형사사법 정의 실현과 기본권 보장을 위한 적법절차 준수 사이의 조화를 도모하여야 할 것이다.

저장매체에 대한 분석 과정은 안티포렌식 대응 기법에 따라 삭제된 전자정보 복구, 전자정보의 검색 및 탐지를 위한 사전 준비, 암호화된 전자정보 복호화, 전자정보의 은닉 탐지 과정으로 세부화 시킬 수 있다. 이들 세부 과정들은 신뢰성을 담보하기 위해 수사기관에서 자체 개발된 포렌식 도구나 국제적으로 공인된 EnCase 프로그램을 이용하여 수행된다. 포렌식 도구 프로그램이 저장매체의 복제본을 분석하는 시간은 예측하기가 힘들며, 장시간 소요되는 경우도 있다. 이하에서는 각 세부 분석 과정별로 참여권을 어떻게 보장해야 할지 살펴보기로 하자.

(1) 저장매체 내의 삭제된 전자정보 복구 과정

전자정보의 압수·수색 집행에서는 압수·수색 현장에서 반출된 저장매체 내의 삭제된 전자정보에 대한 수색은 반드시 필요한 절차 중 하나일 것이다.[51] 저장매체의 전자정보 복구는 무결성을 위해서 저장매체의 이미지 형태를 이용하여야 한다. 저장매체의 전자정보 복구 실시 여부를 압수물의 봉인 해제 및 저장매체의 이미지 생성 과정 이전에 결정을 하고 해당 과정의 수행 시기는 이미지 생성이 완료된 직후에 전자정보 복구

51) 서울고등법원 2014.08.11. 선고 2014노762 판결[내란음모·국가보안법위반(찬양·고무등)·내란선동]
저장매체 원본이나 복제본으로부터 범죄혐의와 관련된 전자정보를 탐색하여 이를 문서로 출력하거나 파일을 복사하는 과정은 전체적으로 영장 집행의 일환에 포함되고, 이를 위해 저장매체 자체를 복구·복제하거나 삭제된 파일을 복원하고, 암호를 풀어 복호화하는 과정 역시 영장 집행의 일환이다. 따라서 그 과정에 대하여 피고인들과 변호인에게 집행의 일시와 장소를 사전에 통지하지 아니한 것은 형사소송법 제219조, 제122조 본문, 제121조에 위배된다.

과정을 수행하면 될 것이다.

이러한 절차로 진행이 된다면 삭제된 전자정보 복구 과정에서의 참여는 별도의 통보 없이 압수물의 봉인해제와 저장매체의 이미지 생성 과정에서의 참여에 대한 연장선으로 볼 수 있을 것이다.

한편, 전자정보 복구 과정을 통해 복구된 전자정보들에 대한 탐색·출력 과정에서도 피압수자나 사건 관계인에게 참여권이 보장되어야 하므로 집행에 대한 통지를 해야 할 것이다. 저장매체에 대한 분석 과정 이후 탐색·출력 과정이 있을 것으므로, 복구된 전자정보들이 탐색·출력 과정에서 탐색이 이루어지면 복구된 전자정보를 위한 탐색·출력 과정을 위한 별도의 집행에 대한 통지는 필요 없을 것이다.

(2) 전자정보의 검색 및 탐지 사전 준비 과정

전자정보의 검색 및 탐지 과정은 저장매체 내에 있는 수많은 전자정보들을 혐의사실과의 관련성 여부를 확인하는데 중요한 수단이다. 해당 과정은 전자정보를 직접적으로 열람하지 않고 전자정보 내에 포함되어 있는 특정 키워드를 가지는 파일을 검색하거나, 파일의 확장자와 파일 시그니처(Signature)가 불일치하는 경우를 탐지하는 것이다. 이런 전자정보 내의 키워드 검색이나 파일 기반 조사는 검찰에서 개발한 CFT 포렌식 도구나 EnCase 포렌식 도구를 활용하여 수행 가능하며, 사전 준비 과정으로 포렌식 도구들은 압수·수색 현장에서 반출된 저장매체의 복제본을 분석 작업을 수반한다. 이런 사전 준비 후에야 키워드 검색이나 파일 기반 조사가 가능하다.

전자정보 검색 및 탐지 과정의 사전 준비는 반출된 저장매체의 이미지가 생성한 후에 수행하면 된다. 따라서 참여권 보장은 압수물의 봉인해제

및 저장매체의 이미지 생성 과정에서의 참여에 대한 연장선으로 보면 될 것이다. 한편, 전자정보 검색 및 탐지 과정의 실질적인 검색 및 탐지는 전자정보의 탐색·출력 과정에서 이루어진다.

(3) 암호화된 전자정보에 대한 복호화 과정

저장매체 내에서 암호화된 전자정보가 있다면 이 전자정보에는 중요한 정보가 담겨 있을 가능성이 크다고 할 수 있다. 따라서 이 중요한 정보를 혐의사실과의 관련성 여부를 확인하는 것은 압수·수색 집행에 있어서 상당히 중요해 보인다. 먼저 저장매체 내에서 암호화된 전자정보를 파악이 되어야 할 것이다. 그러나 포렌식 도구 프로그램으로 모든 암호화된 파일을 검색하지는 못 하므로 전자정보의 탐색 과정에서 확인되는 암호화된 전자정보를 대상으로 복호화 과정이 진행되어야 할 것이다.

전자정보의 탐색 과정으로 복호화해야 할 전자정보가 확정되면 복호화 프로그램을 수행하기 전에 피압수자나 사건 관계인에게 복호화 과정 집행에 대한 참여 통보를 하여야 할 것이다. 해당 과정의 통보를 하면서 피압수자에게 암호화된 전자정보에 대한 복호화를 요구하여 복호화 과정을 줄이도록 해야 할 것이다.

(4) 전자정보의 은닉 탐지 과정

전자정보 은닉 탐지 과정에서는 이미지, 음성, 동영상 등의 멀티미디어 파일 또는 문서 파일 등에 숨겨 놓은 전자정보를 탐지하고 분석한다. 검찰 포렌식 도구인 CFT을 활용하여 압수·수색 현장에서 반출된 저장매체의 이미지를 분석하고 전자정보의 은닉 여부를 탐지한다. 은닉 탐지

과정은 반출된 저장매체의 이미지가 생성된 이후에 수행하면 될 것이다. 따라서 전자정보 은닉탐지 과정은 압수물 봉인해체 및 저장매체의 이미지 생성 과정 이후 연속적으로 수행하고 은닉탐지 과정에서의 참여도 봉인 해제 및 저장매체의 이미지 생성 과정의 참여에 대한 연장선으로 볼 수 있다.

다) 탐색·출력 과정에서의 참여

앞에서 살펴본 전자정보의 여러 압수·수색 과정들을 통하여 압수물의 대상이 될 수 있는 것들을 최대한 수집할 수 있을 것이다. 탐색·출력 과정은 수집된 전자정보들 중 혐의사실과의 관련성이 있는지 탐색하고 관련성이 있다면 파일 복사나 문서 출력으로 압수 대상을 확정하는 것이다.

한편 앞서 본 전자정보 압수수색과 관련된 대법원의 판례들은 이러한 탐색·출력 절차에도 피압수자를 참여시켜야 한다고 판시하였다.[52]

따라서 수사실무 현실과 대법원이 참여권을 보장하고자 하는 취지, 즉 수사기관으로 하여금 영장 범죄사실과 관련성이 없는 정보의 취득을 제한하고자 하는 취지를 조화롭게 합리적으로 해석하는 것이 중요하다고 본다.[53]

실무상 압수한 정보저장매체의 이미징 사본을 이용하여 영장 범죄사실과

52) 대법원 2015.07.16. 자 2011모1839 전원합의체 결정[준항고인용결정에대한재항고]
저장매체에 대한 압수·수색 과정에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 또는 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)를 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 경우에도, 그와 같은 일련의 과정에서 형사소송법 제219조, 제121조에서 규정하는 피압수·수색 당사자(이하 '피압수자'라 한다)나 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다. 만약 그러한 조치가 취해지지 않았다면 피압수자 측이 참여하지 아니한다는 의사를 명시적으로 표시하였거나 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자 측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수·수색이 적법하다고 평가할 수 없고, 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였다 하더라도 달리 볼 것은 아니다.

53) 최성필, "디지털 증거의 증거능력", 검찰 포털 발표자료(2015. 9.), 28쪽

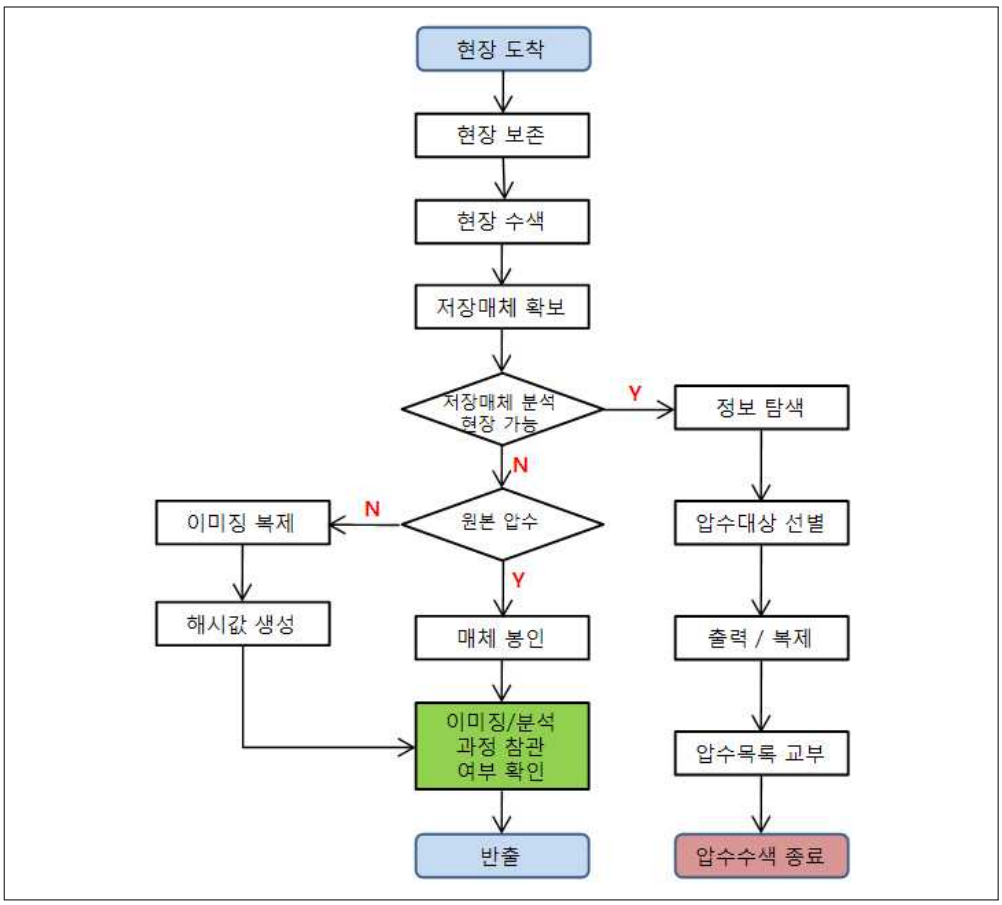
관련성이 있는 정보를 탐색하게 되는데, 전자정보의 대량성으로 인해 주로 키워드 검색을 통해 영장 범죄사실과 관련성이 있다고 생각되는 파일을 추출 내지 선별하고(이하 '선별 절차'라 함), 이렇게 추출된 파일에서 또 다시 영장 범죄사실과 관련된 정보의 내용을 확인한 다음, 이를 증거로 사용하기 위하여 범죄사실과 관련된 해당 정보의 내용을 출력하게 된다.[54]

탐색·출력 절차는 압수·수색 현장에서 반출된 정보저장매체의 봉인 해제 및 이미지 생성 과정에서의 참여와는 불연속적으로 이루어질 가능성이 크다. 저장매체에 대한 분석 과정에는 여러 안티 포렌식 대응 기법들이 포함되어 있고 각각의 세부 분석 과정들의 종료 시점들을 예측하기 어렵기 때문이다. 실제 종근당 사건에서도 이미징 사본을 이용하여 추출된 파일의 내용을 검색하는데 11일이 소요되었다고 한다.

탐색·출력 절차에서의 참여는 피압수자나 참여권자가 소추에 대한 방어를 위해서는 다른 과정보다 그 중요성이 크다. 따라서 피압수자나 참여권자에게 참여권 행사를 보장하기 위해서는 이미징 파일 작성 등 과정에서 불연속적으로 압수수색 집행 과정이 이루어질 경우 수사기관에서 탐색 및 ·출력 과정에 참여를 할 것인지 여부를 확인하여 그 여부를 기록하는 것이 참여권 보장을 위한 적절한 조치를 하였다는 것을 나타낼 수 있을 것이다.

54) 최성필, "디지털 증거의 증거능력", 검찰 포털 발표자료(2015. 9.), 28쪽

다. 전자정보의 압수·수색 절차(안)

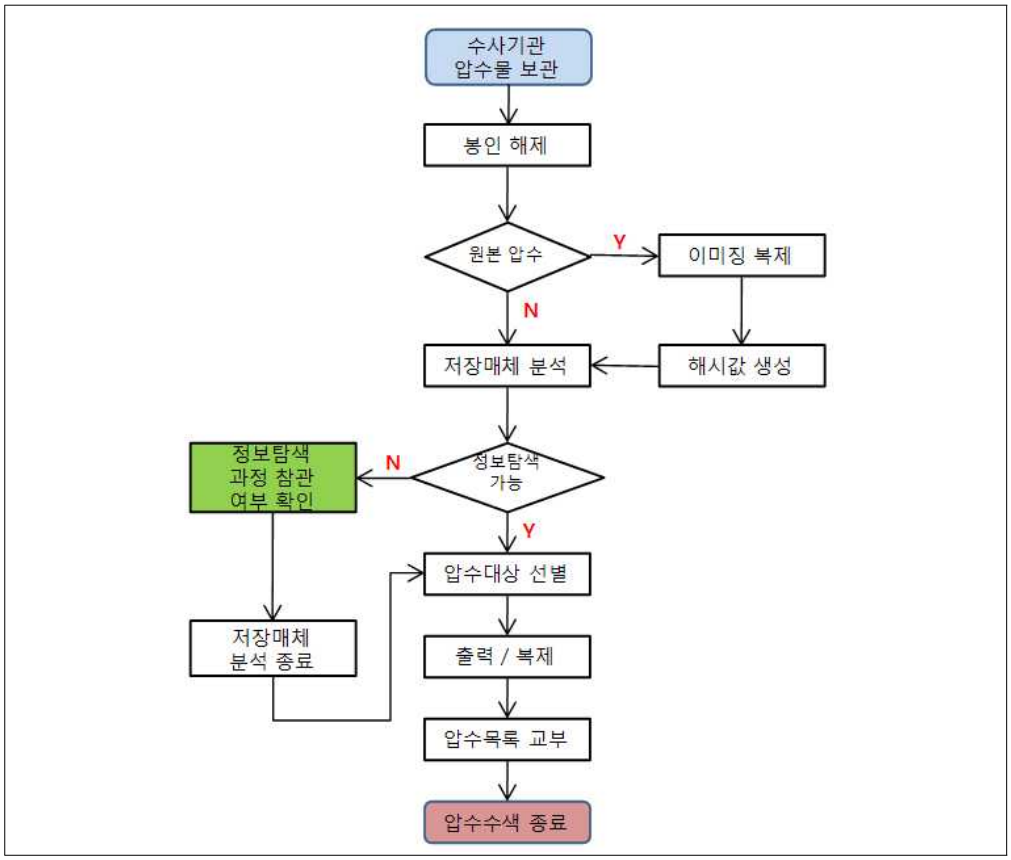


[그림 1] 압수 현장에서의 전자정보 압수·수색 절차(안)

[그림 1]은 현장에서의 전자정보 압수수색 영장 집행 절차를 흐름도로 나타낸 것이다.

압수·수색 영장 집행 전에 피압수자나 사건관계인에게 영장 집행에 대한 사전 통지나 영장 제시를 하여 참여여부를 선택할 수 있도록 해야 할 것이다. 압수·수색 현장에 도착해서는 증거 인멸이나 훼손 등을 방지하기 위해 네트워크 차단 등 압수수색 현장 보존을 위한 조치들을 취하여야 할 것이다. 이런 현장 보존이 되어 있는 상황에서 각종 시스템 및 정보저장매체를 수색하여 저장매체들을 확보하며, 저장매체들에 대하여

분석 과정을 수행한다. 이 과정에서 저장매체 분석의 진행정도나 현장 사정을 살펴보며, 압수 현장에서 압수·수색 집행을 계속 진행할 지를 판단하여 압수수색 집행을 현장에서 마칠 수 있는지를 결정한다. 현장에서 압수수색 집행을 마칠 수 있는 상황이라면 저장매체의 복제본을 생성하고 해당 복제본을 반출하거나 저장매체 자체를 반출할 지를 결정하여야 할 것이다. 압수수색 현장에서 휴대용 전자정보 분석 도구를 이용하여 저장매체 분석이 가능하고 현장 사정들이 압수수색을 진행할 수 있는 상황이라면 피압수자나 참여권자를 압수수색 집행 과정에 참여할 수 있게 하고 정보 탐색 및 출력·복제 작업을 통해 압수 대상을 확정하여 압수수색을 종료한다.



[그림 2] 수사기관 사무실에서의 전자정보 압수·수색 절차(안)

[그림2]와 같이 저장매체 자체나 복제본을 수사기관 사무실 등 외부로 반출한 경우 저장매체 원본에 대한 이미지 파일을 디지털수사통합업무관리시스템에 등록하고 저장매체 복제본에 대한 분석 작업을 수행해야 할 것이다. 이 분석 과정에서 분석 대상이 많거나 요구되는 분석 기법들이 다양할 경우 분석 과정에 필요한 시간은 장시간이며 예측하기 어렵다. 이런 경우 피압수자나 사건관계인을 계속적으로 수사기관에 입회시키기가 보안 등 여러 사정에 어려움이 있으므로 정보탐색 과정에 대한 참관 여부를 확인하여 참관을 신청한 경우 참관 예정 일시를 통보하여 참여권을 보장하는 조치를 취하여야 할 것이다.

저장매체 복제본에 대한 분석 과정이 모두 완료되면 압수 대상을 선별하기 위해서 지금까지 수집된 정보들을 탐색하여 혐의사실과의 관련성 여부를 판별할 것이다. 피압수자나 사건관계인은 전자정보의 탐색 과정을 참여할 수 있고 최종적으로 압수 대상이 선정이 되면 압수 목록을 교부받을 수 있을 것이다.

라. 저장매체 내 전자정보에 대한 사용 이력 관리 방안

1) 도입 배경

대법원 판례[55]는 피압수자가 배제된 상태의 저장매체에 대한 열람을 금지하고 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다고 판시하였다.

이를 위한 조치로서 압수수색 현장에서 반출된 저장매체의 복사본을 디지털수사통합관리시스템에 등록한 이후 저장매체 복사본의 열람 및 복제나 출력 등 사용 이력에 대한 관리를 제안한다.

전자정보가 수록된 저장매체 또는 복제본이 압수・수색 과정에서 외부로 반출되는 경우 저장매체의 복제본이 디지털수사통합관리시스템에 등록이 되는 과정까지는 전자정보의 오·남용 및 임의적인 복제나 복사에 대한 적절한 조치가 이루어지고 있다. 압수·수색 현장에서 수사기관 사무실로 운반 시에는 저장매체 또한 복제본에 대한 훼손을 방지하고 무결성을 유지하기 위해 저장매체 또는 복제본을 반드시 봉인하고, 저장매체나

---

55) 대법원 2011. 5. 26. 자 2009모1190결정 준항고기각결정에 대한 재항고(전국교직원노동조합 본부 사무실 압수수색 사건)
검사나 사법경찰관이 압수·수색영장을 집행할 때에는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.

복제본에 대한 봉인 해제 시에는 수사기관 규정상으로 피압수자의 참여를 보장하고 있다. 그러나 그 이후 압수수색 집행과정(저장매체 복제본 분석 및 정보 탐색 등)에서는 수사기관이 저장매체 복제본을 직접 관리하고 있으며, 저장매체 복제본 분석 과정은 실무상 며칠씩 장시간 소요되고 종료시점을 예상하기 어렵다. 또한 수사기관 내 규정에 피압수자의 참여권 보장이 명시되어 있지 않아 수사기관에서 피압수자를 배제한 상태에서 저장매체 복제본에 대한 열람 및 임의적인 복제나 복사 시도가 이루어질 가능성이 있다. 이에 따라 저장매체 내 전자정보의 사용 이력 체계를 도입하여 수사기관에서 임의적인 열람 및 복사나 출력을 제한하는 조치가 필요할 것이다.

2) 설계 시 고려사항과 실무상 보완해야 할 사항

저장매체 복제본에 대한 사용 이력 관리 체계의 설계는 다음사항을 고려하여야 할 것이다.

- 첫째, 관리 대상을 저장매체 복제본과 저장매체 복제본 내 전자정보로 분류한다.
- 둘째, 저장매체 복제본의 저장위치는 디지털통합수사업무시스템이고 저장매체 복제본 내 전자정보의 저장위치는 수사기관 PC이다.
- 셋째, 저장매체 복제본 내 전자정보에 대한 사용에 대하여 사용자별로 열람, 복제, 출력 등 사용의 구분이 이루어져야 한다.

대검찰청 예규 상 저장매체 복제본은 디지털수사통합업무시스템에 등록되며 등록된 저장매체 복제본 이외의 동일한 저장매체 복제본은 모두 삭제해야 한다. 또한 디지털수사통합업무시스템은 수사기관 직원별로 접근

권한을 설정하여, 저장매체 복제본의 접근이력을 관리하고 있다. 따라서 보완적으로 혐의사실 관련성에 대한 구분 없이 행해지는 저장매체 복제본의 재복제를 금지하는 제도적 조치가 필요하다.

저장매체 복제본 내 전자정보는 디지털통합수사업무시스템에서 파일 단위로 수사기관 직원 PC에 다운로드 되어 열람된다. 디지털통합수사업무시스템에서 저장매체 복제본 내 전자정보를 수사기관 직원 PC에 다운로드한 이력은 로그로서 기록되어 관리가 된다. 하지만 수사기관 직원 PC에 저장된 저장매체 복제본의 전자정보는 열람·복사·출력에 대한 통제 관리가 이루어지지 않고 사용 이력을 확인할 수 없는 문제점이 있다. 수사기관 직원 PC에 저장된 저장매체 복제본의 전자정보에 대한 사용자별 사용 통제 관리와 사용 이력 체계가 필요한 실정이다.

3) 기술적 해결 방안

파일 단위로 수사기관 직원 PC에 저장되는 저장매체 복제본의 전자정보에 대한 열람·복사·출력의 이력 관리 대책으로서 이력 관리 기술구조를 모색하고 이력 관리 기술구조를 구현하는 한 방법으로서 Enterprise DRM[56] 중 Server DRM 기술을 적용하는 방안을 제안한다.

본 논문에서 제안하는 이력 관리 기술구조는 [그림3]와 같이 전자정보의 이력 관리 여부에 따라 관리영역과 비관리영역으로 구분하고 비관리영역에 있는 수사

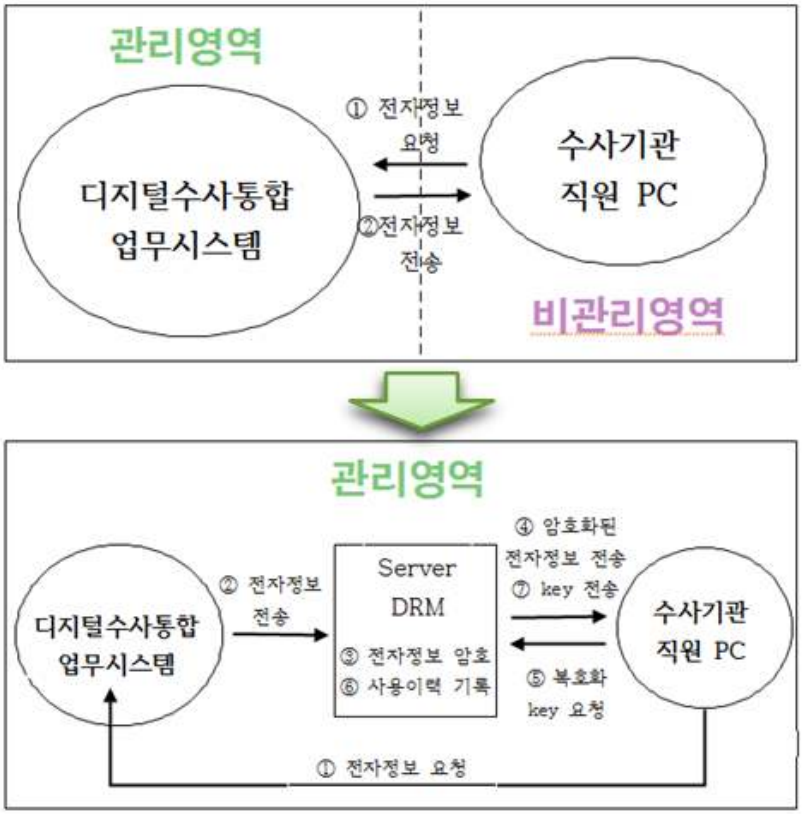
---

56) 조규곤, “Enterprise DRM 구축 방안”, 정보과학회지, 23권 8호, pp.31-32, 2005.8, DRM(Digital Rights Management) 기술은 디지털 콘텐츠의 저작권 보호를 목적으로 개발되었다. 초기 DRM은 콘텐츠의 상거래 시 콘텐츠 보호가 주목적이었지만 현재는 여러 방면에서 응용되고 있다. 상거래 시 콘텐츠의 저작권 보호를 위한 DRM을 Commerce DRM이라고 하고, 기업의 중요한 자산인 문서의 기밀을 효과적으로 지키기 위한 DRM을 Enterprise DRM이라고 부른다.

Enterprise DRM은 기업 내부의 혹은 외부의 합법적 사용자의 고의나 부주의로 인한 정보의 유출을 막는다. 또한 전자문서의 사용내역을 관리할 수 있어, 보안 사고를 예방하고 사고 발생 시에는 전자문서의 사용내역을 조사에 이용할 수 있다. 전자문서 보안 정책으로 DRM을 적용함으로써, 각 전자문서별로 다음과 같은 점을 통제할 수 있다.

- 사용자, 사용 PC, 사용기간, 사용횟수, 오프라인 사용 허용 여부, 사용 이력 수집주기
- 보기, 편집, 인쇄, 암호화 저장, 원본 저장 허용 여부

기관 직원 PC를 Server DRM 기술을 활용하여 관리영역으로 전환하는 것이다.



[그림3] 전자정보 사용 이력 관리 기술 구조

기술구조에 대한 구체적인 설명은 다음과 같다. 수사기관 직원 PC에서 디지털수사통합업무시스템의 사건 관련 저장매체 복제본의 전자정보를 다운로드 요청을 하면 디지털수사통합업무시스템은 해당 전자정보를 Server DRM[57] 시스템에 전송한다. Server DRM 시스템은 전송받은 전자정보를 암호화하여 수사기관 직원 PC에 전송한다. 수사기관 직원 PC에

57) 문진규, "내부정보유출방지를 위한 DRM 적용방법설계", 한국컴퓨터종합학술대회, 2007 전자문서 저장 및 관리의 주체를 기준으로 Enterprise DRM 기술을 세분화 정의한다. 그 중 하나인 Server DRM은 전자문서를 암호화 하는 시점이 사용자 PC에 다운로드 전인 정보시스템 서버 내에서 이루어지며, 전자문서가 사용자 PC에 다운로드된 후에 열람, 인쇄, 저장 등 이용의 권한을 통제하는데 사용된다. Server DRM의 사용자 인증은 별도 인증 없이 정보시스템의 사용자 인증을 활용한다. 문서 관리의 주체는 서버 관리자이다.

서 암호화된 전자정보를 열람하기 위해 복호화 키를 Server DRM 시스템에 요청을 한다. Server DRM 시스템은 사용자 인증 및 권한 확인을 하고 복호화 키를 수사기관 직원 PC에 전송하면서 문서 사용이력을 기록한다.

4) 저장매체의 전자정보에 대한 사용 이력 관리 체계의 기대 효과

수사기관이 저장매체 복제본의 열람 및 복사나 출력 등의 사용 이력을 관리함으로써, 수사기관은 압수·수색 집행 절차의 투명성을 확보하며, 집행 절차에 대한 위법성 논란이 줄어들고 저장매체 복제본에 대한 관리에 경각심을 갖게 되어 사전 및 사후 통제기능이 강화될 것이다.

Server DRM을 적용함으로써, 각 파일별로 열람자, 열람 PC, 열람횟수, 인쇄횟수를 기록할 수 있게 된다. 또한 사용자별로 전자정보의 열람 및 복사나 출력 등 사용에 대한 통제가 가능하여 자료 유출를 방지하는 효과도 있다.

5. 결론

본 논문에서는 형사사법체계에 있어서 날로 중요성이 커지는 전자정보에 대한 압수·수색 영장 집행을 할 경우 피압수자나 사건 관계인에게 참여를 보장하기 위한 방안으로 전자정보의 압수·수색 집행 과정을 공간과 절차별로 나누어 보고 각 절차에서 참여권을 어떻게 보장할 것인지에 대해 제안해 보았다.

2장에서는 수사기관에서 형사소송법 제106조 3항에 따라 압수·수색 영장 집행하는 방식이 크게 3가지로 나뉘며, 각 방식별 세부절차를 확인하였다. 압수·수색의 절차적인 측면과 더불어, 내용적인 측면을 살펴보기 위하여 전자정보의 압수·수색에서 활용되고 있는 전자정보 수집 및 분석 기법을 조사하였고 수사실무에서 활용하는 디지털 포렌식 도구에 대한 기능을 비교·분석한 것도 찾아보았다.

3장에서는 압수·수색 절차에 있어서 피압수자의 참여와 관련한 규정에 대해 살펴보았고 참여권 보장의 취지들을 알아보았다. 그리고 전자정보의 압수수색 집행 과정에서의 참여권 보장 등과 관련한 대법원 주요 판례들을 조사하였다. 전자정보의 압수·수색 집행 시에 수사기관 사무실 등 예외적인 방식의 집행이 가능한 요건, 피압수자의 참여 보장, 혐의사실과의 유관정보에 한정한 문서출력, 파일복제 등 적법절차 및 영장주의의 원칙에 대해 구체적인 사례를 통해 알 수 있었다. 또한 영장 집행 과정 중 발생한 위법한 행위들이 전체과정 중에서의 중요도, 그 위반사항에 의한 법익 침해 가능성의 경중 등을 종합하였을 때 위법의 중대성으로 전제적인 압수·수색 처분이 취소되는 사례도 있었다.

전자정보의 압수·수색영장 집행과 관련하여 살펴본 법 규정, 수사기관에서의 실무 현실, 대법원의 판례 사례을 종합적으로 고려하여 참여권을 보장하는 전자정보의 압수·수색 영장 집행 절차를 제시하였다. 또한 수사기관에서 피압수자를 배제한 상태에서 압수 현장에서 반출한 저장매체 내 전자정보를 열람 및 임의적인 복사나 출력 등을 제한하기 위한 방안으로 저장매체 내 전자정보 사용 이력 관리 체계를 제안하였다. 피압수자 압수·수색 현장에서뿐만 아니라 수사기관 사무실 등 외부에서도 피압수자의 참여 횟수를 최소화하면서도 압수·수색 집행 과정의 대부분에 참여가 되도록 하는 것이 목표이었다. 수사기관에서는 형사소송법 개정으로 과거에 비해 전자정보의 압수·수색에 대한 사전·사후 통제가 가해져 집행에 어려움을 겪고 있다. 수사의 목적을 달성하여 사법 정의를 바로 세우면서 동시에 피압수자의 권리도 보장하는 데에 본 논문이 조금이나마 도움이 되길 바란다.

참 고 문 헌

1. 권양섭 “디지털 증거수집에 관한 연구”, 군산대학교 박사학위 논문(2009)
2. 김윤섭, · 박상용, “형사증거법상 전자정보의 증거능력”, 형사정책연구 제26권 제2호(2015)
3. 김지홍, “디지털 포렌식 절차 모델에 대한 새로운 접근”, 서울대학교 석사학위논문(2015)
4. 노명선, ‘디지털 증거의 압수·수색에 관한 판례 동향과 비교법적 고찰’, 형사법의 신동향 통권 제43호(2014.6.)
5. 문진규, “내부정보유출방지를 위한 DRM 적용방법설계”, 한국컴퓨터종합학술대회, (2007)
6. 백형구 등, 「주석 형사소송법 Ⅰ」 제4판, 한국사법행정학회(2009)
7. 손지영 · 김주석,「디지털 증거의 증거능력 판단에 관한 연구」, 대법원 사법정책연구원(2015)
8. 신원, “안티포렌식 기법 분석을 통한 안티포렌식 대응 방안”, 보안공학연구논문지
9. 양근원, “형사절차상 전자정보의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위논문(2006)
10. 이완규, “디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 확보 방안”, 대검찰청 이프로스 게시판(2015. 8.)
11. 임한희, “개정된 형사소송법에 적합한 현장 디지털 증거 추출도구 필요 요건에 관한 연구”, 고려대학교 정보보호대학원 석사학위논문(2012)
12. 전승수, “형사절차상 전자정보의 압수수색 및 증거능력에 관한 연구”, 서울대학교 박사학위논문(2010)
13. 조규곤, “Enterprise DRM 구축 방안”, 정보과학회지, 23권 8호(2005. 9.)
14. 최성필, “디지털 증거의 증거능력”, 검찰 포털 발표자료(2015. 9.)
15. 탁희성, “법정에서 전자 증거의 허용가능성”, 한국전자포렌식학회, 「전자 포렌식 연구」 창간호(2007. 11.)

16. 탁희성・이상진,「디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보 방안」, 형사정책연구원(2006)
17. 대검찰청, 「검찰수사 실무전범Ⅱ」(2008)
18. 대검찰청, “디지털포렌식 수사관의 증거 수집 및 분석 규정” [시행 2015.7.16.]

판례자료

대법원 2011. 5. 26. 자 2009모1190
대법원 2012.10.11. 선고 2012도7455
수원지방법원 2014. 2. 17. 선고 2013고합620, 624, 699, 851
서울고등법원 2014. 8. 11. 선고 2014노762
대법원 2015. 1. 22. 선고 2014도10978