25.08.07

전자증거의 선별압수와 매체압수에 관한 연구

논문 요약을 통한 분석

[BoB_14_디지털포렌식] 논문 분석

Writer : 김민서(8074)

Index

1 서론 2
2 선별압수 및 매체압수 실태 3
2.1 선별압수 및 매체압수 실태 분석 4
3 선별압수의 원칙 6
3.1 선별압수의 원칙 분석 8
4 디지털 포렌식을 위한 매체압수 관련성 확대 필요성 10
4.1 매체압수 관련성 확대 필요성 분석 12
5 모바일에서의 선별압수 14
5.1 모바일에서의 선별압수 분석 16
6 매체 탐색, 선별 과정의 적법절차 18
6.1 매체 탐색, 선별 과정의 적법절차 분석 19
7 결론 21

1 서론

형사소송 절차에서 실체적 진실의 발견은 가장 중심적인 목표로 기능하지만, 이는 피압수자의 기본권, 특히 개인정보와 사생활의 보호와 종종 충돌한다. 디지털 증거는 대용량, 고속성, 다종성, 사적 정보 포함 등 다양한 특성으로 인해, 기존의 일괄 압수 방식으로는 개인의 권리를 과도하게 침해할 가능성이 높다. 따라서 사건과 무관한 정보를 걸러내고, 수사 목적에 부합하는 정보만을 선별하여 수집하는 '선별 압수'의 필요성이 강조된다. 이와 같은 압수 방식은 수사기관이 사건 관련성 있는 정보만을 대상으로 수색, 복사, 저장하는 방식으로, 형사소송법과 헌법상의 기본권 보장을 함께 고려하는 절충점으로 평가된다. 그러나 실무에서는 여전히 '매체 전체의 압수', 즉 일괄적인 물리적 압수 관행이 지속되고 있으며, 이는 개인정보 침해와 무관정보 과잉수집 논란으로 이어지고 있다.

2 선별압수 및 매체압수 실태

제 1 장. 용어정리

본 연구에서 사용하는 '현장'은 압수 수색 영장이 실제로 집행되는 장소, 즉 정보저장매체가 소재한 장소를 의미한다. 관련 문헌에서 일본 판례를 인용하여 일괄압수 제한적 긍정설을 주장하는 경우도 있으나, 일본은 압수 대상을 '정보'가 아닌 '매체'로 간주하기 때문에 이러한 논거는 우리 법 체계와 완전히 부합하지 않는다.

제 2 장. 검찰의 전자증거 압수 실태

검찰은 전자정보 압수 과정에서 저장매체를 반출하면서도 압수조서를 작성하는 등 실무상 일괄 압수와 유사한 방식이 통용되고 있다. 이러한 관행은 법적 개념상 '압수'가 아닐 수 있음에도 불구하고 현실에서는 압수로 처리되는 점에서 이론과 실무의 괴리를 보여준다. 특히 최근에는 하드카피 형식(clone)의 수집은 거의 이루어지지 않고, 대부분 디지털 이미지 방식으로 증거를 수집한다. 대검찰청은 디지털수사망(D-NET)을 통해 디지털 증거를 관리하고 있으며, 매년 압수·수색·분석 현황을 통계로 공표하고 있다. 그러나 해당 통계에서는 PC 와 모바일, 선별압수와 매체압수를 구분하지 않으며, 각각의 수집 방식도 명확히 구분하지 않는다.

검찰의 증거 수집 실태를 구체적으로 살펴보면, PC 의 경우 선별압수가 약 80% 이상을 차지할 정도로 지배적인 방식으로 자리 잡았다. 사건 관련 파일이나 디렉터리만을 선택적으로 복사하는 방식이 일반화되었고, 이는 피압수자의 권리를 일정 부분 보호하는 데 기여하고 있다. 반면 모바일 기기의 경우, 구조적 특성상 파일 단위의 접근이 어렵고, 전체 백업 형태로 수집이 이뤄지기 때문에 매체 전체를 압수하는 방식이 대부분이다. 특히 모바일에서의 '라이브 획득'은 기술적으로는 논리적 수집에 가깝지만, D-NET 시스템에는 물리이미지로 분류되어 등록되기 때문에 결과적으로는 매체압수와 다르지 않다. 이러한 방식은 분석의 용이성이나 법적 증거능력 확보 측면에서는 유리할 수 있으나, 과잉수집과 사생활 침해 우려가 크다는 점에서 문제가 제기된다.

제 3 장. 경찰의 전자증거 압수 실태

경찰 또한 검찰과 유사하게 디지털 증거 수집에서 PC 와 모바일의 구분 없이 자료를 관리하고 있으며, 통계상으로도 선별압수와 매체압수 간의 구체적 비율이나 기준이 명확하게 제시되지 않는다. 경찰 백서나 내부 보고서를 보면 포렌식 전담 인력은 점차 증가하고 있지만, 압수 방식의 실질적 변화는 미비한 것으로 분석된다. 경찰청 산하 사이버안전국이나 각 지방청에서는 디지털 포렌식 전담팀이 운영되고 있으나, 장비의 노후화, 인력의 전문성 부족, 현장 대응 능력의 한계 등으로 인해 실효적인 선별압수는 거의 이뤄지지 않고 있다.

또한 일부 연구에 따르면 경찰은 여전히 모바일 기기나 저장매체를 통째로 압수한 후, 사후적으로 복제본을 분석하는 방식에 의존하고 있으며, 이는 매체압수의 전형적인 사례에

해당한다. ‘원본압수’와 ‘사본압수’라는 표현이 사용되기도 하지만, 실질적으로는 모두 매체 전체를 대상으로 하는 압수라는 점에서 선별압수의 취지와는 거리가 있다. 현장에서 관련성 판단을 할 수 있는 기준과 장비, 법적 지식이 부족한 상황에서 수사관은 법적 안전성을 이유로 일괄압수를 선택할 가능성이 높다. 이에 따라 경찰의 디지털 증거 수집 관행도 사생활 보호보다는 수사 편의에 초점이 맞춰져 있다는 비판이 제기되고 있다.

2.1 선별압수 및 매체압수 실태 분석

상기와 같이 선별압수 원칙은 법적으로는 명시되고 있으나 실무에서의 실효성은 극히 낮다. 특히 모바일 기기의 압수에 있어서는 여전히 매체압수가 지배적이며, 이는 피압수자의 기본권 침해를 야기할 수 있는 구조적 문제로 이어진다. 따라서 향후에는 법적·제도적 보완뿐만 아니라 기술적 지원과 수사관 교육을 병행하여, 선별압수가 실제로 작동할 수 있는 환경을 조성하는 것이 필요하다. 이를 통해 형사절차의 정당성과 증거능력 확보는 물론, 피압수자의 권리 보장이라는 두 가지 목적을 모두 달성할 수 있을 것이다.

선별압수는 '사건 관련성이 있는 정보만을 선택적으로 수집'하는 방식이고, 매체압수는 '저장매체 전체(하드디스크, 스마트폰 등)를 압수하여 사후 분석'하는 방식이다.

표면적으로는 둘 다 합법적 압수 방식처럼 보이지만, 실제로는 압수 대상의 범위·형식·수사권 행사 방식이 전혀 다르며, 법적 판단에 미치는 영향도 근본적으로 상이하다. 선별압수는 기본권 보장 중심, 매체압수는 수사 효율 중심의 방식이며, 압수된 데이터가 미치는 사회적·심리적 충격(사생활 노출 등)도 전혀 다르다.

모바일 기기의 경우, 그 구조적 특성과 기술적 제약으로 인해 선별압수가 거의 이루어지지 않고 있으며, 사실상 전면적인 매체압수가 이루어지고 있다. 이는 저장장치가 단일 구조로 통합되어 있고, 앱 데이터, 메신저, 사진, 위치기록 등 민감한 정보가 혼재해 있기 때문에 사건 관련성과 무관한 정보가 필연적으로 수집될 수밖에 없는 기술적 구조 때문이다. 또한 루팅, 암호화, 접근제한 등의 장벽도 선별 접근을 어렵게 만든다.

현장 실무에서는 형식적으로는 선별압수를 표방하더라도, 실질적으로는 '이미징 후 선별 분석'이라는 방식으로 매체 전체를 수집하고 분석하는 관행이 여전히 유지되고 있다. 이는 수사기관이 압수 당시 관련성 판단을 하지 않고, 포렌식 분석 단계에서 사건과 관련된 데이터만 골라내면 문제가 없다는 논리로 정당화된다. 그러나 이는 헌법상 과잉금지원칙 및 영장주의에 위배될 수 있으며, 증거능력에도 영향을 줄 수 있는 중대한 문제다.

검찰과 경찰 간의 조직적 차이도 선별압수 실태에 영향을 준다. 검찰은 비교적 체계화된 포렌식 시스템과 전담 인력을 운영하고 있지만, 모바일 수사에서는 여전히 매체압수 중심의 접근을 벗어나지 못하고 있다. 경찰은 장비와 인력, 절차 숙련도에서 지역청별 편차가 크며, 선별 기준 없이 일괄 압수를 택하는 경향이 강하다. 특히 분석 능력 부족으로 원본과 사본의 개념을 혼용하거나, 저장매체 자체를 압수하는 등 위법 소지가 다분한 절차가 반복되고 있다.

기술적으로는 특정 앱의 DB 나 파일만을 추출하는 방식도 가능하지만, 수사기관은 이해 부족, 장비 미비, 법적 리스크 회피 등의 이유로 통째 추출 방식을 여전히 사용하고 있다.

이러한 기술적 후퇴는 결과적으로 사생활 침해 범위를 확대시키고, 피의자뿐 아니라 무관한 제 3 자의 정보까지 과도하게 수집·보관되는 문제로 이어진다.

결론적으로, 현재의 선별압수 실태는 법률상 명시된 원칙과 실무 관행 사이의 괴리가 매우 크며, 이는 수사기관의 증거 수집 방식 전반에 대한 근본적인 재검토를 요구한다. 통계 수치와 기술적 가능성에만 기대는 '형식적 선별'에서 벗어나, 압수의 범위와 절차, 분석 주체와 시기, 증거의 폐기 및 이력 관리 등 실질적 통제를 반영한 구조 개편이 필요하다.

3 선별압수의 원칙

제 1 장. 선별압수 입법

선별압수는 2011 년 형사소송법 개정을 통해 제도화되었으며, 2012 년 1 월 1 일부터 시행되었다. 개정법은 시행 전 사건에도 적용되되, 과거 규정에 따라 행해진 행위의 효력에는 영향을 미치지 않는다고 규정하고 있다. 이로써 디지털 정보의 압수·수색 과정에서도 관련성 있는 정보만을 제한적으로 수집해야 한다는 원칙이 법률적으로 인정되었다. 해당 개정은 영장주의 원칙에 기반을 두고 있으며, 사생활 보호를 위한 최소한의 수단으로 선별적 방식의 수색을 요구하는 방향으로 전환된 것이라 평가된다.

제 2 장. 선별압수 원칙에 관한 영장 변천사

제 1 절. 적정한 압수 절차 모색의 시작

검사가 청구한 압수수색영장은 법원이 아닌 담당 판사가 심사하여 발부하거나 기각한다. 2000 년대 초반부터 법원행정처에서는 압수수색영장 발부 기준을 정비하면서 점차 수사의 범위를 제한적으로 설정하려는 노력이 이루어졌다. 특히 2001 년판 영장실무는 관련성·필요성을 강조하며 전자정보의 특수성을 고려하기 시작한 시기다.

제 2 절. 압수의 방법을 제한하는 영장의 등장

2000 년대 중반부터 영장에 압수 방법을 구체적으로 기재하는 형식이 도입되었다. 예를 들어, 컴퓨터 저장장치가 몰수 대상이 아닌 한, 하드카피 방식이나 출력이 불가능한 경우가 아니면 저장장치 자체를 압수해서는 안 된다는 문구가 들어가게 되었다. 이러한 기재례는 실제 판례에서 반복적으로 등장했으며, 법원이 구체적인 압수 범위를 제한하려는 태도를 보였음을 의미한다.

제 3 절. 관련성 요건을 명시한 영장 별지의 등장

2010 년 이후 개정된 영장 양식에서는 압수 대상 정보의 관련성 요건을 구체적으로 명시하기 시작하였다. 법원은 별지를 통해 관련성 있는 문서, 파일, 데이터의 유형을 상세히 기술하였고, 이를 통해 압수 범위를 명확히 하는 방향으로 제도적 변화가 이루어졌다. 특히 서울중앙지방법원의 사례는 관련성 요건을 강조한 대표적인 판례로 꼽힌다.

제 4 절. 3 단계 선별압수 영장의 본격화

2011 년부터는 세분화된 3 단계 선별압수 모델이 실무에 적용되기 시작하였다. 첫 단계는 현장 수색을 통해 압수 대상이 되는 매체를 특정하고, 둘째는 복사(이미징) 후, 셋째는 관련성 있는 정보를 선별하여 추출하는 절차로 구성되었다. 이 3 단계 방식은 디지털

포렌식의 절차적 정당성을 확보하고, 무관 정보의 과잉 수집을 방지하는 제도적 장치로 기능한다.

제 5 절. 현행 압수 대상 및 방법의 제한

2013 년 이후 발표된 실무자료들은 여전히 새로운 별지를 충분히 소개하지 않는 등, 법원의 실무는 다소 일관되지 않은 측면을 보인다. 다만 형사소송법 개정으로 인해 제 215 조와 제 216 조에서 압수수색의 대상 및 방법에 대한 제한적 해석이 가능해졌으며, 대법원 판결들도 이러한 흐름을 따라가는 모습을 보였다. 예컨대 2015 년, 2014 년 등의 고합 판결에서는 관련 없는 정보까지 포함된 압수에 대해 문제를 제기한 바 있으며, 선별적 접근이 정당화되고 있는 추세다.

제 3 장. 선별압수 원칙화에 대응한 선행 연구들

제 1 절. 모바일 선별압수에 관한 연구의 미흡

모바일 기기에 대한 선별압수 관련 연구는 매우 제한적이다. 기존 연구는 대부분 PC 기반의 선별압수 또는 증거보관 방식에 초점이 맞춰져 있으며, 모바일 환경에서의 선별 기술·법적 쟁점에 대한 탐구는 부족하다.

제 2 절. 수집 도구의 개선에 관한 연구

디지털 증거 추출 도구의 개선을 통해 선별적 수집이 가능해진다는 연구들이 제시되었으며, 특히 현장 상황에서 관련성 있는 정보만을 복사하고 저장할 수 있는 기술적 방안들이 다수 논의되었다. 이 중에는 실시간으로 포렌식 수집을 하면서도 수집된 데이터가 가지는 위치 정보나 바이트 오프셋 등을 활용해 무관 정보를 제외하려는 시도도 있었다.

제 3 절. 안전한 증거관리 방식에 관한 연구

암호화, 워터마킹, 클러스터 정보 기반 식별 방식 등 다양한 기술이 안전한 증거관리 방안으로 제안되었으며, 이는 정보의 무결성 유지뿐 아니라 무관 정보에 대한 폐기 가능성 확보와도 연결된다.

제 4 절. 암호화하여 제 3 의 기관에 위탁하자는 제안

일부 연구자는 선별 대상이 불명확할 경우, 디지털 증거를 암호화하여 독립된 제 3 기관에 위탁·보관하고, 이후 법원 또는 수사기관이 정당한 절차에 따라 필요한 정보만을 열람하게 하는 모델을 제안하였다. 이는 무관 정보에 대한 과잉 노출을 방지할 수 있는 하나의 대안으로 평가된다.

제 5 절. 무관증거 폐기 방법에 관한 연구

무관증거의 폐기 절차와 무결성 보장을 위해 이중 해시를 활용하는 방법, 디지털 로그와 식별자 추적 방식 등을 도입해야 한다는 제안이 있었다. 폐기 시에는 원본과 폐기 대상의 구분을 명확히 하고, 법적 분쟁이 발생하지 않도록 입증책임을 기술적으로 분산시켜야 한다는 주장도 존재한다.

제 6 절. 원본압수와 선별압수 비교에 대한 연구

일부 연구는 범죄현장성과 관련성 요건을 기준으로, 원본압수가 정당화될 수 있는 경우를 구체적으로 제시하면서, 선별압수와의 구분 기준 및 절차적 보완책 마련을 제안하였다. 이로써 현실적으로 선별이 불가능하거나 기술적으로 제약이 있는 상황에서의 법적 판단 기준이 모색되고 있다.

3.1 선별압수의 원칙 분석

선별압수의 원칙이 법적으로 제도화된 과정과, 영장 실무의 변천, 그리고 현실적인 적용 한계와 대안에 대해 체계적으로 정리하였다. 기술적 수단의 발전, 법적 장치의 개선, 그리고 제도적 실무의 정비가 함께 이루어져야만 선별압수의 원칙이 실효적으로 작동할 수 있음을 보여주고 있다.

선별압수의 원칙은 단순한 수사기법의 하나가 아니라 헌법상 기본권 보호를 실현하기 위한 원칙으로 작동해야 한다. 이는 과잉금지 원칙과 영장주의, 적법절차의 원칙에 뿌리를 두고 있으며, 특히 전자정보처럼 사생활과 인격이 그대로 반영된 데이터를 다룰 때는 관련성 있는 정보만을 제한적으로 압수해야 한다는 요구로 연결된다. 그러나 현재의 형사사법 절차에서 이 원칙은 실질적으로 작동하기 어렵게 설계되어 있다. 법률은 선별압수 원칙을 명시하고 있으나, 수사 현장에서는 이를 구체적으로 실현할 수 있는 절차적 장치와 감독 체계가 마련되어 있지 않다. 법원은 영장별지를 통해 압수 대상의 범위를 제한하려는 시도를 해왔지만, 여전히 관련성 판단은 모호하고 추상적이며, 수사기관의 자의적 판단에 의존하고 있는 것이 현실이다.

특히 '사건과 관련된 정보'라는 판단은 기술적으로도 어렵고, 법적으로도 명확한 기준이 없는 상태에서 사실상 수사기관의 해석에 맡겨지고 있으며, 이는 무관 정보까지 수집될 가능성을 상시적으로 열어놓고 있다. 수사기관은 '전체 매체를 확보한 뒤 사후 분석 과정에서 선별한다'는 논리로 매체 전체의 이미징을 정당화하고 있고, 이는 실질적으로 매체압수와 다를 바 없는 방식이다. 선별이라는 이름 아래 실제로는 무차별적인 데이터 수집이 이루어지고 있는 것이다. 디지털 포렌식 기술이 발전하여 파일 단위, 레코드 단위, 심지어 키워드 단위까지도 특정 정보만 추출할 수 있는 기능이 있음에도 불구하고, 수사기관은 여전히 통째로 이미징한 후 내부 분석을 통해 선별 여부를 판단하고 있으며, 이 과정에 대한 외부 통제는 사실상 부재하다.

선별압수 원칙이 실효성을 갖기 위해서는 관련성 판단을 수사기관이 아닌 중립적인 외부 검토기구나 선별전담팀이 수행해야 하며, 수사담당자와 분석담당자의 인적 분리가

제도화되어야 한다. 또한 탐색 및 선별 과정의 영상 기록, 로그 기록, 피압수자의 이의제기 절차, 무관정보 폐기 기준 등을 명문화하는 실질적 절차 보완이 필요하다. 선별압수는 수사기관의 선택 사항이 아니라, 국가권력이 기본권을 제한하는 행위에 반드시 따라야 할 최소한의 기준이며, 이것이 법률상 명시되었다고 해서 실효적 통제가 이뤄진다고 보아서는 안 된다. 선별압수의 원칙은 선언된 바 있으되, 집행할 수단과 통제 메커니즘이 부재한 이상, 수사기관의 자기합리화 수단으로 오용될 수 있고, 이는 곧 디지털 시대에 가장 위협적인 형태의 인권침해로 작용할 수 있다.

4 디지털 포렌식을 위한 매체압수 관련성 확대 필요성

제 1 장. 디지털 포렌식의 위기

디지털 포렌식은 1999 년부터 2007 년까지를 황금기로 평가하지만, 이후에는 위기 국면에 접어들었다는 진단이 이어지고 있다. 그 배경에는 스토리지의 용량 폭증, 저장장치 종류의 다양화, 암호화 기술 확산, 클라우드 환경의 확대, 운영체제 및 파일 포맷의 복잡화 등 기술적 요소가 있으며, 동시에 법적 규제의 강화도 영향을 미쳤다. 이러한 복합적인 변화는 기존의 포렌식 기법이 더 이상 효과적으로 작동하기 어렵게 만들고 있으며, 수사기관이 기술적·제도적으로 대응하지 않으면 유의미한 증거 확보가 어려워지는 상황에 직면하고 있다.

제 2 장. 선별압수의 실패 요인들

제 1 절. 관련성 요건에 대한 판단의 한계

전자정보 압수 과정에서 가장 핵심적인 기준은 범죄와의 '관련성'인데, 이 요건 자체가 추상적이고 본질적으로 모호하다는 점이 문제로 지적된다. 실제 사례에서도, 객관적으로 유사하거나 동종의 범죄라는 이유만으로 무관한 자료를 함께 압수한 후 증거능력을 부정당하는 경우가 있었다. 이는 수사기관이 주관적 판단이나 포괄적 해석에 기대어 압수 범위를 설정한 결과이며, '기본적 사실관계의 동일성'이라는 법리 기준도 현장에서는 명확히 적용되기 어렵다. 이러한 판단의 한계는 압수 대상이 되는 정보의 성격상 '사전 판단'이 거의 불가능하다는 현실적인 제약과도 연결된다.

또한, 압수 현장에서는 시간적 압박과 장비의 한계로 인해 판단 여지가 더욱 제한되며, 파일 하나를 열어보는 것조차 메타데이터 변경이라는 리스크를 수반한다. 이처럼 구분 단위가 명확하지 않은 정보 구조, 즉 디렉토리, 파일, 레코드, 섹터, 클러스터 등 다양한 계층이 존재하고, 실제 분석은 해당 계층마다 다르게 접근해야 한다는 점도 실무상 관련성 판단을 어렵게 만든다.

제 2 절. 키워드 검색의 한계에 따른 선별 실패

포렌식 도구에서 핵심으로 사용하는 키워드 검색 방식에도 한계가 존재한다. EnCase 와 CFT 같은 대표 도구에서도, Compound Document File 이나 압축파일, PDF 내부의 텍스트, 다른 언어로 인코딩된 콘텐츠 등은 키워드 검색으로 탐지되지 않는 경우가 많다. 예를 들어, Microsoft Office Open XML 구조는 ZIP 기반이기 때문에 내부 파일을 검색하려면 추가적인 해제가 필요한데, EnCase 는 이를 자동으로 처리하지 못한다.

이외에도 이메일 첨부파일, 특수 문자, 난독화된 문자열, 언어 설정이 바뀐 파일 등은 키워드 검색을 회피할 수 있으며, 이는 안티포렌식 기법이 아니라도 구조적으로 발생할 수 있는 문제다. 파일 속성이 복잡하거나, 사용자가 위장한 파일명이나 위치로 저장한 경우에도 검색이 실패할 가능성이 크다.

제 3 절. 논리이미징의 원리상 포렌식에 부적합

논리이미징은 디지털 증거를 디렉토리 단위 또는 파일 단위로 추출하는 방식으로, 파일 시스템의 구조를 그대로 보존하지 않으며, 클러스터 단위의 메타데이터나 미할당 영역은 수집하지 않는다. 따라서 안티포렌식 탐지, 삭제 파일 복구, 메타데이터 조작 확인 등 핵심 분석 작업이 어려워진다. 예를 들어 NTFS 파일 시스템에서는 MACE(MAC + Entry modified) 값으로 시간 정보를 분석하는데, 논리이미지에는 이러한 값이 누락되거나 변형되어 존재하지 않기 때문에 시각 조작 여부나 변경 로그 추적이 불가능하다.

또한, 논리이미징은 수집 시점에서의 필터링(키워드, 파일 확장자)에 의존하는 경우가 많으며, 이후 포렌식 분석에 필요한 정보가 처음부터 배제되는 결과를 초래할 수 있다. 실무상 dd 또는 EWF 포맷의 물리이미지가 선호되는 이유도 이러한 포렌식 한계를 보완하기 위함이다.

제 3 장. 선별압수 결과에 대한 포렌식 분석의 실패

제 1 절. 아티팩트 분석에 의한 진상규명의 곤란

디지털 포렌식은 단순히 파일 존재 유무를 확인하는 것이 아니라, 사용자의 행위나 의도를 복원하는 데 중점을 둔다. 이를 위해 아티팩트 분석이 이루어지는데, 대표적으로 이벤트 로그, NTUSER.DAT, Jump Lists, Prefetch, 레지스트리 등이 활용된다. 하지만 이러한 데이터는 일부 포맷에서는 수집되지 않거나, 삭제되거나, 논리이미지에는 포함되지 않을 수 있어 진상 규명이 어려워질 수 있다.

제 2 절. 삭제된 파일의 복구 곤란 내지 불가능

삭제된 파일의 복구 여부는 저장장치의 유형에 따라 달라진다. 특히 SSD 는 TRIM 명령어에 따라 삭제된 클러스터가 즉시 초기화되어, 삭제 후 복구가 사실상 불가능하다. HDD 에 비해 복구 가능성이 낮고, 메모리 관리 방식상 잔존 데이터가 금방 사라지기 때문에, 압수 당시의 수집 범위가 진실 규명에 결정적인 영향을 미친다.

제 3 절. 볼륨 섀도우 카피를 활용한 파일 복구의 한계

일부 사건에서는 볼륨 섀도우 복원 지점을 활용해 과거 데이터를 복구하기도 했지만, 이 방식 역시 시스템 설정 여부나 사용자의 행위에 따라 완전히 복원되지 않는 경우가 많다. 예컨대 24,500 여 개의 삭제 파일이 복원되었다는 사법행정권 남용 의혹 사건처럼 일부 사례는 예외적일 뿐, 일반 사건에서는 어렵다는 것이 중론이다.

제 4 절. 완전삭제 도구 사용 흔적의 탐지 곤란

안티포렌식 도구, 예를 들어 SDelete 나 Eraser, 일부 고급 스크립트는 파일 클러스터를 무작위 덮어쓰기 하거나 메타데이터를 조작하여 완전삭제를 수행한다. 이 경우,

논리이미지는 물론이고 물리이미지에서도 흔적 탐지가 어렵다. 특히 NAND Flash 기반의 메모리에서는 wear leveling, garbage collection 등의 내부 처리과정으로 인해 삭제된 흔적조차 남지 않게 된다.

제 5 절. 파일 날짜·시각 변작 탐지의 불가능

NTFS 파일 시스템은 MAC(E) 구조를 통해 파일의 생성, 수정, 접근 시간 정보를 기록하지만, 이를 조작하는 도구들이 존재하며, 심지어 EnCase 나 FTK 에서도 완전히 탐지하지 못하는 경우가 있다. 예컨대 timestomp.exe 같은 도구는 파일의 MFT Entry 를 조작하여 위장된 타임스탬프를 삽입하고, 이를 메타데이터에 남기지 않는다.
논리이미지로는 이러한 변조 여부를 탐지할 수 없다는 것이 치명적인 한계로 작용한다.

제 4 장. 매체압수 또는 관련성 인정 범위 확대 필요성

디지털 포렌식의 실무상 문제와 분석 실패 가능성을 고려할 때, 형식적인 관련성 요건에만 기대어 선별압수만을 고집하기보다는, 필요한 경우 매체 전체를 압수할 수 있도록 요건을 유연하게 재정립할 필요가 있다는 주장이 제기된다. 특히 현장에서 수사관이 충분한 정보 없이 판단하는 것은 구조적으로 불가능하며, 이를 방지하기 위해 영장 별지에 매체압수 가능 여부를 명확히 기재하거나, 관련성 인정 범위를 사후적으로 확장할 수 있는 규정이 필요하다는 의견도 있다.

법원은 이미 일부 판례에서, 피의자의 협조가 없어 관련성 판단이 어려운 경우 매체 전체의 이미징을 허용하고, 이후 관련성 있는 정보만을 사용하도록 한 적이 있다. 이는 압수 당시 선별이 불가능하거나 기술적 제약이 있는 상황에서의 현실적 대안으로 평가되며, 관련성 판단을 압수 이전이 아니라 분석 이후에 판단하도록 하는 방향도 고려되고 있다.

4.1 매체압수 관련성 확대 필요성 분석

결론적으로, 본 장에서는 디지털 포렌식이 직면한 기술적·법적 한계 속에서 선별압수 원칙만으로는 진실 규명과 실효적 수사를 보장하기 어렵다는 점을 지적하고, 매체압수의 허용 범위를 조건부로 확대할 필요성을 제기하였다. 특히 논리이미징과 키워드 검색에 대한 맹신을 지양하고, 물리이미징 및 전체 분석을 기반으로 한 정밀 수사가 필요하다는 점을 강조하고 있다.

디지털 포렌식 수사에서 매체압수의 관련성을 확대해야 한다는 주장은 단지 수사 편의성만을 위한 것이 아니라, 현재의 선별압수 원칙이 기술적·현실적 한계를 극복하지 못하고 있다는 점에서 비롯된다. 현행 법제는 사건과 관련된 정보만을 압수하도록 요구하지만, 디지털 저장매체의 구조는 이를 전제로 작동하기 어렵다. 예를 들어, 하나의 저장매체에는 사건과 무관한 수많은 정보와 사건 관련 정보가 혼재되어 있으며, 이들을 압수 당시 구분해내는 것은 기술적으로 불가능하거나 고도로 제한된 상황에서만 가능하다. 특히 파일 단위나 앱 단위의 추출이 가능한 경우에도, 해당 데이터가 사건과의 관련성을

갖는지 여부는 압수 시점이 아닌 분석 이후에야 비로소 명확해질 수 있다는 한계가 존재한다. 따라서 수사 초기 단계에서 불명확한 관련성 판단만을 근거로 전체 매체의 압수를 제한한다면, 실질적인 증거 수집의 실패로 이어질 위험이 높다.

또한, 디지털 포렌식은 단순한 파일 복사 수준을 넘어 사용자의 행동 추적, 삭제 파일 복구, 타임라인 분석, 아티팩트 조사 등을 포함하며, 이 과정은 특정 파일이나 폴더만을 대상으로 진행해서는 전체적인 진상을 밝히기 어렵다. 예를 들어, 사용자의 특정 행위를 증명하기 위해서는 로그파일, 캐시, 시스템 이벤트, 미할당 영역의 잔존 데이터 등 광범위한 정보에 대한 통합적 분석이 필요한데, 이는 논리이미징이나 파일 단위 선별압수로는 원천적으로 불가능하다. 특히 안티포렌식 기법이 동원된 경우에는 삭제된 흔적이나 조작된 시간정보가 핵심 단서가 되므로, 물리적인 전체 매체의 분석 없이는 증거 인멸이나 왜곡을 탐지할 수 없다. 이처럼 전체 매체를 확보하지 않고는 분석 자체가 불가능한 상황에서는 압수 당시의 관련성 판단 기준을 완화하고, 분석 후 관련성 있는 부분만을 사용하도록 하는 절차가 더 실효적일 수 있다.

법원 역시 실제 판례에서 피의자의 협조가 없거나 선별이 불가능한 경우 매체 전체의 압수를 허용한 사례가 있으며, 이는 압수 당시의 절대적인 관련성 판단보다는, 수사 현실을 반영한 탄력적인 대응이 필요하다는 점을 보여준다. 특히 저장매체의 암호화, 접근 제한, 비표준 포맷 등으로 인해 수사기관이 사건 관련성을 사전 판단할 수 없는 경우, 전체 매체를 확보한 뒤 포렌식 절차를 통해 점진적으로 범위를 축소하는 방식이 헌법상 비례성 원칙에 더 부합할 수 있다는 견해도 있다. 이는 무차별적 수집을 정당화하는 것이 아니라, 수사기관이 전체 매체를 확보하되, 관련성 없는 정보는 분석에서 배제하고 사후 폐기하며, 그 과정을 명확하게 기록하고 통제하는 전제 아래에서만 정당화될 수 있다.

결국 매체압수의 관련성을 지나치게 협소하게 해석할 경우, 디지털 포렌식의 실효성이 형해화되고, 진실 발견의 기능은 심각하게 훼손될 수 있다. 선별압수 원칙을 무력화하지 않으면서도 실질적인 수사를 가능하게 하기 위해서는, 매체 전체를 압수할 수 있는 법적 공간을 열어두되, 이를 제어할 수 있는 절차적 장치(중립적 필터링, 입회 및 기록 시스템, 분석 후 폐기 명령제도)를 함께 구축하는 것이 현실적 대안이 될 수 있다. 이는 단순한 원칙의 선언이 아니라, 디지털 시대에 걸맞은 수사권 행사와 기본권 보장의 균형점을 재정립하는 것이다.

5 모바일에서의 선별압수

제 1 장. 모바일 매체압수 실태의 문제점

모바일 기기의 압수 과정에서는 PC 와는 다른 구조적 특성과 기술적 제약이 존재하며, 현재 실무에서는 대부분 기기 전체를 물리적으로 압수하는 방식이 채택되고 있다. 이는 기기 내에 저장된 데이터의 범위가 방대하고, 저장 형태가 다층적이며, 사건과 무관한 민감 정보까지 함께 수집되는 문제를 유발한다. 특히 포렌식 수사관들도 모바일의 분석이 어렵다는 점을 인정하고 있으며, 현행 제도나 장비는 특정 앱의 데이터만을 선별하여 수집하기 어려운 상황이다. 이런 상황에서 매체 전체를 압수하는 방식은 사생활 침해 논란과 함께, 법적 정당성 문제로도 이어지고 있다.

제 2 장. 모바일 포렌식의 획득 기술

제 1 절. 획득 기술의 검토

모바일 포렌식에서의 데이터 획득은 크게 하드웨어 방식과 소프트웨어 방식으로 나뉜다. 하드웨어 방식은 물리적인 복사를 수행하는 반면, 소프트웨어 방식은 루팅을 통해 접근 권한을 확보하거나 루팅 없이 앱 기반 접근 방식으로 데이터를 수집한다. 그러나 루팅은 보안 기능을 무력화할 수 있으며, 루팅이 어려운 기기나 최신 기종에서는 접근 자체가 불가능한 경우도 많다. SQLite 데이터베이스를 포함한 모바일 앱의 저장 구조는 매우 복잡하며, 삭제된 레코드의 복구 역시 기술적으로 제한된다.

키워드 검색 기능이나 획득 단위의 세분화 기술은 일부 앱이나 장비에서 제공되지만, 특정 앱 데이터만을 정확히 추출하거나 파일 단위의 선별적 획득이 가능한 경우는 매우 제한적이다. 현실적으로는 전체 앱 데이터를 복사한 뒤, 사후에 관련성 여부를 판단하는 방식이 일반적이다. 일부 논문과 실무 자료는 Content Provider 를 이용해 레코드 단위의 데이터 추출 가능성을 제시하지만, 기술적 난이도와 기기 호환성 문제로 실무 활용은 제한적이다. 또한, 획득 소요시간도 문제가 되며, 대용량 기기의 경우 수 시간이 소요되기도 한다. 이로 인해 현장에서는 '전체 이미지' 방식이 선택될 수밖에 없는 구조적 문제가 존재한다.

제 2 절. MFA 의 이해

MFA(Mobile Forensic Analyzer)는 검찰이 사용 중인 모바일 포렌식 도구로, 라이브획득 모드와 물리획득 모드를 지원한다. 라이브획득 모드에서는 네트워크 연결 없이도 아이디와 비밀번호를 입력하여 현장에서 즉시 데이터 획득이 가능하며, 수집된 데이터는 이후 온라인 접속 시 자동 업로드된다. 그러나 현행 MFA 는 특정 앱의 데이터만을 골라 획득하는 기능이 미비하며, 본 논문은 이러한 기능 개선이 필요하다고 강조한다.

MFA 의 분석 단계에서는 수집된 데이터를 기반으로 분석 보고서를 생성할 수 있으며, 내부적으로 SQLite Browser 를 포함하고 있어 앱 데이터베이스 분석이 가능하다. 그러나 증거관리 시스템상 수사팀이 이미징 파일에 접근하지 못하게 되어 있어, 데이터의

동일성을 확보하기 위한 절차가 복잡하고, 디지털 포렌식 수사관이 별도로 데이터를 추출하거나 분석하는 부담이 크다. 포렌식팀이 파일 전체를 수사팀에 전달하면, 수사-분석의 인적 분리 원칙이 무너질 수 있다.

제 3 장. MFA 프로그램 개선방안

현행 MFA 의 기술적 한계를 보완하기 위해 몇 가지 개선 방안이 제시되었다. 첫째, 사후 논리이미징 기능을 추가하여 필요한 경우 사건 종결 이후에도 추가 분석이 가능하도록 해야 한다. 둘째, 획득 단계에서 특정 앱의 데이터베이스 파일만을 선별적으로 추출할 수 있는 기능을 도입해야 한다. 이 경우 관련성 판단 단위를 앱 단위, 파일 단위, 또는 레코드 단위로 세분화할 수 있으며, 사건의 특성에 따라 탄력적으로 적용해야 한다. 셋째, 키워드 검색 결과에 해당하는 데이터만을 선별 추출하는 기능을 통해 불필요한 정보 수집을 줄이고, 피압수자의 권리를 보호할 수 있다. 이는 데이터의 무단 수집에 대한 법적 대응을 예방하는 장치로도 기능할 수 있다.

제 4 장. 모바일 선별압수를 위한 압수절차 개선

제 1 절. 검찰 모바일 압수절차의 개선 방안

검찰 수사관이 현장에서 직접 선별 수집을 시행할 수 있도록 관련 장비와 훈련이 제공되어야 하며, 모바일 선별압수는 추출 방식, 선별 기준, 분석 절차에 따라 크게 세 가지 유형으로 분류된다. MFA 의 기능이 보급되었지만 실제로 수사관들이 이를 적극적으로 활용하지 않는 경우가 많으며, 이는 장비에 대한 이해 부족과 기술적 한계 때문이기도 하다. 디지털 포렌식팀에서도 MFA 보다는 상용 포렌식 도구를 더 선호하는 경향이 있다.

제 2 절. 모바일 압수절차 개선의 장점

모바일 선별압수를 제도화하면, 헌법상 비례성 원칙에 부합하는 압수 방식이 가능해진다. 피압수자 입장에서는 사생활 침해의 범위를 최소화할 수 있으며, 반환까지 걸리는 평균 기간도 단축될 수 있다. 수사기관 입장에서는 불필요한 데이터에 대한 분석 부담이 줄고, 증거의 적법성 논란도 감소할 수 있다. 선별적 압수는 수사 효율성과 인권 보호를 동시에 실현할 수 있는 수단으로 작용한다.

제 5 장. 모바일 매체압수의 적법 여부

제 1 절. 모바일 매체압수가 적법하다는 통념의 극복

일반적으로 모바일 기기를 통째로 압수하는 관행이 적법하다는 인식이 강하나, 헌법재판소와 일부 대법원 판례는 이를 제한적으로 해석하고 있다. 특히 압수 당시 사건과 관련된 정보를 선별할 수 있는 기술이 존재하거나, 피압수자의 협조를 받을 수 있는 경우에는 매체 전체 압수는 위헌 소지가 있다는 입장이 설득력을 얻고 있다.

제 2 절. 파티션 이미지 계속 보유의 위법 여부

모바일 기기의 파티션을 이미징하여 계속 보관하는 행위는 데이터 삭제 요청권, 사생활 보호권, 증거보존의 필요성 사이에서 충돌을 일으킨다. 일부 판례는 이를 위법이라고 판단하였으며, 계속 보유하려면 별도의 법적 근거 또는 법원의 명시적 허가가 필요하다고 보았다. 모바일 데이터의 특성상 일정 기간이 지나면 그 민감성이나 사적 성격이 더욱 부각되므로, 장기 보관에 대해서는 보다 엄격한 기준이 적용되어야 한다.

5.1 모바일에서의 선별압수 분석

모바일 기기의 압수·분석 과정에서 발생하는 기술적 제약과 법적 문제를 종합적으로 검토하고 있으며, 선별압수 원칙을 실질적으로 구현하기 위한 기술적 개선안과 절차적 정비방안을 함께 제시하고 있다. 특히 검찰과 경찰 양측의 실무를 고려한 개선 제안이 균형 있게 다루어졌으며, 모바일 환경에 특화된 선별압수 시스템의 필요성이 강하게 강조되고 있다.

모바일 환경에서의 선별압수는 이론적으로는 가능하나, 실무적으로는 거의 실현되지 않고 있다는 점에서 법제와 기술, 현실 사이의 괴리를 가장 적나라하게 드러낸다. 모바일 기기의 구조는 PC 와 달리 저장매체가 단일화되어 있고, 운영체제 자체가 사용자 데이터, 앱 캐시, 로그, 시스템 설정 등 민감 정보들을 하나의 저장 영역에 통합해 보관한다. 이러한 구조적 특성으로 인해 사건 관련 정보만을 선택적으로 추출한다는 것은 기술적으로도 복잡하고, 법적으로도 과감한 기준 설정이 요구된다. 예를 들어, 카카오톡 대화 내용만을 수집하고자 할 경우에도 해당 앱의 DB, 캐시, 임시 파일, 썸네일 이미지, 전송파일 등 다양한 경로의 정보가 연결되어 있기 때문에, 단순히 하나의 파일만을 추출하는 것으로는 진실 규명이 불가능할 수 있다.

또한 모바일 운영체제는 루팅이나 탈옥 없이 접근할 수 있는 데이터가 제한적이기 때문에, 수사기관은 기기 전체를 포렌식 장비에 연결해 데이터를 추출하는 방식에 의존할 수밖에 없다. 이러한 기술적 한계는 결국 수사기관이 모바일 압수에 있어서 선별이라는 원칙을 사실상 포기하거나, 형식적으로만 선별 기준을 갖추는 데 그치도록 만든다. 실제로 모바일 포렌식에서 이뤄지는 선별은 대부분 추출된 전체 데이터 중 일부를 분석 단계에서 걸러내는 수준이며, 이는 본질적으로 매체압수와 구별되지 않는다. 심지어 모바일 기기 내부의 데이터는 사용자 식별 정보, 위치정보, 금융정보 등 사생활 침해 수준이 PC 보다 훨씬 심각함에도 불구하고, 모바일 압수에는 오히려 더 낮은 수준의 통제가 가해지고 있다는 점은 현행 제도의 구조적 모순을 보여준다.

법원 역시 모바일 압수에 대해서는 판례가 미비하고, 수사기관의 기술적 한계나 현실을 고려하여 폭넓은 압수를 사실상 용인하는 경향이 있다. 이로 인해 모바일 선별압수는 기술적으로 가능함에도 불구하고, 장비의 한계, 수사관의 역량 부족, 법적 통제 장치 미비 등으로 인해 실질적인 구현이 거의 이뤄지지 못하고 있다. 특히 수사관이 모바일 기기를 현장에서 압수할 때, 디지털 수사 장비에 대한 이해 없이 특정 앱이나 데이터만을 선별하여 추출하기란 현실적으로 매우 어렵고, 시간이 오래 걸리며, 추출 결과의 증거능력을 보장하는 데에도 리스크가 따른다. 결과적으로 선별이라는 이름 하에 이루어지는 압수는

대부분 형식적인 수준에 머물며, 모바일이라는 고밀도의 사적 공간에 대한 전면적 침해가 반복되고 있다.

이러한 문제는 기술의 부재보다는 통제 메커니즘의 부재에서 기인하는 측면이 크며, 모바일 기기의 구조적 특수성을 감안한 절차적 대안이 마련되지 않는 이상, 선별압수는 선언에 그칠 수밖에 없다. 선별적 추출을 실질화하기 위해서는 앱 단위의 접근 권한 설정, 데이터베이스 단위 추출 기능, 메타데이터 기반 필터링 기능 등 기술적 개선과 함께, 수사단계에서의 입회 절차, 추출로그 관리, 사후적 관련성 판단 구조 같은 제도적 장치가 병행되어야 한다. 또한 모바일 포렌식 장비의 표준화, 수사관에 대한 기술 교육 강화, 분석 인력과 압수 인력의 역할 분리 등 조직적 대응도 필요하다. 모바일 기기는 가장 민감한 사생활이 집중된 장치이기에, 선별압수의 원칙은 다른 어떤 매체보다도 강하게 실현되어야 하지만, 현재는 가장 후진적인 방식으로 처리되고 있는 것이 현실이다. 이를 개선하기 위한 접근은 단지 수사 효율성의 문제가 아니라, 디지털 시대의 헌법적 수사권 행사 기준을 다시 설정하는 작업이다.

6 매체 탐색, 선별 과정의 적법절차

제 1 장. 매체 탐색, 선별의 적법 요건

디지털 정보에 대한 압수수색 절차에서 '탐색'과 '선별'은 본질적으로 수색 또는 검증의 일환으로 보아야 하며, 이는 단순한 부수행위가 아니라 독립적인 절차로서 법적 정당성이 요구된다. 대법원은 여러 판결을 통해, 탐색과 선별은 영장에 근거한 적법한 절차 하에서만 이루어져야 하며, 피압수자의 참여권 보장이 필수적이라는 입장을 일관되게 유지해왔다. 특히 전교조 재항고 사건(2009 도 1190 결정) 이후부터 이러한 원칙이 보다 명확히 확인되었다. 이에 따라 수사기관은 탐색·선별 과정에서도 영장 범위 내의 적법성과 절차적 통제를 충실히 따라야 하며, 이 과정이 수사기관 자의적으로 이루어질 경우 위법수집증거가 될 수 있다는 점이 강조되고 있다.

제 2 장. 참여권 보장 방법의 고도화

피압수자의 참여권은 단순히 형식적인 절차가 아니라, 증거의 적법성과 신뢰성을 확보하기 위한 핵심적인 요소로 간주된다. 그러나 실무상 참여권이 충분히 보장되지 못하는 경우가 많으며, 디지털 증거의 특수성을 고려할 때 참여권 행사 방식도 시대에 맞게 변화되어야 한다. 예를 들어, 수사관의 작업 화면을 동영상으로 캡처하거나 로깅하는 기술, 또는 가상머신에서 분석 작업을 수행한 후 이미지 파일을 보존하는 방식 등이 제안되고 있다. 또, 원격 데스크탑 공유, 화상회의 참관, 입회인 제도 활성화 등의 방법도 현실적인 대안으로 논의된다.

이러한 고도화 방안은 단순히 수사기관의 자율적 판단에 맡기기보다는, 제도화하여 명문화해야 실효성이 있다. 동시에 피압수자의 권리를 보장하는 과정은 수사기관의 신뢰성 회복과도 직결되며, 객관적이고 공정한 증거 수집 과정을 통해 법적 분쟁을 줄이는 효과도 가져올 수 있다.

제 3 장. 피압수자의 이의제기권과 수사기관의 대응 의무

피압수자는 수사기관의 압수수색 및 선별 분석 과정에 대해 이의를 제기할 수 있어야 하며, 수사기관은 그러한 이의 제기에 대해 합리적으로 대응할 법적 의무가 있다. 하지만 현재 법률에는 이의제기권이 명시적으로 규정되어 있지 않고, 실무적으로도 적극적으로 보장되지 않는 경우가 많다. 예컨대, 피압수자가 무관한 정보의 삭제나 폐기를 요구할 수 있는 법적 권한이 불분명한 상황에서, 수사기관은 그러한 요청을 무시하거나 법적 근거 없이 거부하기도 한다. 이에 대해 학계와 실무에서는 무관 정보 삭제 요구권을 명문화하고, 수사기관은 이에 대한 합리적·신속한 조치 의무를 부담해야 한다는 입장이 점점 확산되고 있다.

제 4 장. 전자증거 관리의 철저 및 관리이력의 공개

디지털 증거의 적법성을 보장하려면 수집된 증거의 보관·삭제·활용에 대한 관리 체계를 철저히 갖추는 것이 필수다. 수사기관은 증거 이미지를 완전히 삭제하고, 접근 권한을 엄격하게 설정하며, 접근 및 조작 이력을 로그로 남기는 등의 절차를 통해 증거의 무결성과 정당성을 확보해야 한다. 특히 증거로 수집된 파일이 복제되거나 복사될 경우, 해시값 검증이나 수색과정의 영상 기록 등을 통해 원본과 동일성 여부를 입증해야 한다. 또한 수사기관 내부의 시스템(D-NET 등)에 등록된 이미지를 제외한 다른 이미지 파일은 자동으로 삭제되도록 설정하거나, 삭제 여부를 명확하게 기록하는 기능도 필요하다.

제 5 장. 선별 담당자와 수사 담당자의 인적 분리

수사기관 내에서 증거를 선별하고 분석하는 사람과 이를 활용하여 수사를 진행하는 사람 간의 역할 분리를 명확히 하는 제도적 장치도 필요하다. 이는 미국 연방 판례인 CDT(Comprehensive Drug Testing) 사건에서도 강조된 원칙으로, 수사권 남용과 사생활 침해를 방지하기 위해서는 중립적 선별 담당자 제도가 실무에 도입되어야 한다. 실제로 일부 연구자들은 '인적 분리'를 전제로 선별 분석 시스템이나 조직 운영 구조의 개편을 제안하고 있으며, 국내에서도 관련 논의가 점차 활발해지고 있다. 분석 담당자와 수사 담당자가 동일한 인물일 경우, 증거의 관련성 판단에 주관이 개입될 위험이 커지고, 위법한 정보 수집으로 이어질 수 있다는 문제의식에서 출발한 것이다.

이러한 인적 분리를 제도화할 경우, 수사기관 내의 내부 통제 체계가 강화되고, 적법절차 위반 논란을 사전에 차단할 수 있으며, 증거로서의 신뢰성도 함께 확보할 수 있다.

6.1 매체 탐색, 선별 과정의 적법절차 분석

전자정보 압수 과정에서 탐색과 선별이라는 독립 행위의 적법성을 확보하기 위한 제도적, 기술적, 절차적 조건들을 종합적으로 분석하였다. 특히 피압수자의 참여권 보장과 이의제기권, 그리고 수사기관의 적극적 대응책 마련이 핵심적으로 강조되었으며, 디지털 시대의 수사절차가 가져야 할 공정성과 투명성 확보를 위한 다양한 대안이 함께 제시되었다.

매체 탐색과 선별 과정의 적법절차는 단순히 압수 이후의 기술적 문제로 치부되어서는 안 되며, 헌법상 적법절차 원칙과 직접적으로 연결되는 독립적 절차로 인식되어야 한다. 전자정보 수색은 특성상 압수 이후에도 상당한 범위의 탐색과 분석이 필요하기 때문에, 초기의 압수·수색이 정당했다고 하더라도 이후의 선별 과정이 자의적으로 이루어질 경우 전체 절차가 위법이 될 수 있다. 그러나 현재의 제도 구조에서는 이 선별 분석 단계가 명확한 법적 통제를 받지 않으며, 대부분 수사기관 내부의 실무 관행과 기술적 판단에 따라 이루어지고 있다. 이는 전통적인 수색·압수 개념에서는 상정되지 않았던 '지연된 수색' 혹은 '후속적 압수'라는 새로운 차원의 권력 행사로, 형식적으로는 압수가 끝났더라도 실질적으로는 반복적 수색이 계속되는 셈이다.

문제는 이러한 탐색·선별 과정에 대해 별도의 영장이 발부되지 않더라도 정당한 절차로 간주되는 관행이 존재하며, 피압수자의 참여권 또한 이 시점부터 사실상 배제된다는

점이다. 즉, 탐색이 시작되는 순간부터 분석이 종료될 때까지 수사기관이 일방적으로 정보를 열람하고 판단하며 선별하는 구조가 정착되어 있고, 이는 외부 통제를 받지 않는 폐쇄적 절차로 작동하고 있다. 또한 선별 과정에서 무관 정보가 수사팀에 그대로 전달되거나, 사건과 무관하다는 이유로 폐기되지 않고 별도의 내부 데이터베이스에 보관되는 경우도 있어, 개인 정보의 2 차적 침해 가능성도 배제할 수 없다. 이는 헌법이 보장하는 자기정보통제권이나 정보주체의 사적 영역 보호 개념에 정면으로 충돌하는 문제이며, 절차의 실효성 확보가 불가능한 구조적 허점을 의미한다.

더불어 탐색과 선별의 정당성을 담보하기 위해서는 기술적인 투명성 확보도 필수적이다. 단순히 수사관의 기억이나 설명에 의존하는 것이 아니라, 디지털 포렌식 장비의 사용 이력을 자동으로 기록하는 로그 기능, 탐색 화면의 영상 기록 저장, 명시적인 추출 파일 목록 보존 등, 행위 자체에 대한 증명이 가능한 시스템이 요구된다. 그러나 국내 현실에서는 이러한 기술적 장치들이 일부 고가의 장비에만 탑재되어 있거나, 사용자가 임의로 비활성화할 수 있는 구조로 되어 있어, 사실상 통제력 확보에 실패하고 있다. 수사기관이 내부적으로 선별 작업을 수행하고, 그 결과만 법원에 제출하거나 피압수자에게 통지하는 방식은 절차적 정당성을 외양만 유지한 채 실질적 통제는 모두 회피하는 편의적 구조이다.

이와 같은 탐색·선별 절차가 적법하려면, 단순히 영장 범위 내 수집이라는 논리를 넘어, 사후적 탐색 및 분석까지도 포함하는 적법성 심사 구조가 필요하다. 구체적으로는 탐색·선별 자체를 독립된 수색 행위로 보고 별도의 통제 기준을 마련하거나, 그 과정에 대한 실시간 기록과 피압수자의 이의제기권을 실질적으로 보장하는 절차가 설계되어야 한다. 탐색의 순간부터 사건 관련성이 없는 정보는 즉시 폐기하거나 접근 제한을 걸어야 하며, 분석 이후에도 관련성이 없다고 판단된 정보는 자동 삭제되도록 기술과 절차가 연동되어야 한다. 그럼에도 불구하고 현재는 압수만 영장 통제를 받고, 탐색·분석은 사실상 사법적 통제 바깥에서 작동한다는 점에서 심각한 적법절차 침해가 구조적으로 발생하고 있는 것이다. 요컨대, 매체 탐색과 선별 분석은 더 이상 압수의 부속 절차가 아니라, 별도의 권력 행위로 보아야 하며, 이에 상응하는 법적 통제와 투명성 확보 조치를 동반하지 않는다면, 전자정보 수사의 합헌성과 정당성은 근본적으로 위협받을 수 있다.

7 결론

본 논문은 전자정보 압수·수색이라는 복잡하고 민감한 절차에서 '선별압수'라는 원칙이 왜 필요한지, 그리고 그 원칙이 실무에 어떻게 구현되고 있으며 어떤 한계를 드러내는지를 포괄적으로 다루었다. 특히 매체압수 관행이 아직도 광범위하게 존재하는 현실 속에서, 무관한 정보의 과잉수집 문제와 사생활 침해, 기본권 침해의 위험성은 매우 심각한 사안으로 지적된다. 이러한 문제의식은 헌법상 과잉금지 원칙 및 영장주의의 본질과도 밀접히 연관된다.

현행 형사소송법은 선별압수의 원칙을 명문으로 도입하였고, 법원의 영장 실무 또한 과거에 비해 발전하였지만, 여전히 추상적이거나 형식적 수준에 머무르고 있는 측면이 많다. 수사기관이 실제 압수·수색 단계에서 관련성 없는 정보까지 포함한 자료를 수집하는 경우, 이는 곧바로 위법수집 논란으로 이어질 수 있고, 증거능력의 문제뿐 아니라 국가권력의 남용이라는 법적·윤리적 비판을 피할 수 없게 된다.

특히 디지털 포렌식 환경에서는 탐색과정 자체가 압수에 준하는 법적 효과를 발생시키기 때문에, 이 과정에서도 엄격한 절차적 통제가 요구된다. 탐색과 선별은 수사기관의 내부 판단이나 기술적 편의에 따라 이루어져서는 안 되며, 헌법과 형사소송법이 정한 원칙에 따라 반드시 영장에 근거한 범위 내에서 수행되어야 한다. 이에 따라 디지털 증거 수집과정에서 피압수자의 참여권을 보장하는 절차, 무관 증거의 삭제와 폐기를 위한 시스템, 그리고 작업기록의 영상화·로깅 등 절차적 투명성을 확보하는 방안이 구체적으로 제도화될 필요가 있다.

또한 미국의 CDT 판례에서 제시된 것처럼, 디지털 포렌식 과정에서 수사기관의 역할을 분리하여 수사관이 직접 관련성 판단을 하지 못하도록 하는 '인적 분리 원칙'도 도입이 필요하다. 이러한 구조는 중립성을 확보하고, 무관 정보가 수사과정에서 무단 활용되는 것을 방지하며, 결과적으로는 적법절차의 실효성을 높이는 장치가 된다.

결국 디지털 시대의 형사절차는 단순히 정보를 수집하는 기술적 행위가 아니라, 헌법이 보장한 기본권과 직결되는 정치적·법적 행위로 이해되어야 한다. 따라서 전자정보 압수 과정에서의 '선별'은 단지 실무의 선택이 아닌, 법률이 요구하는 최소한의 기준이며, 이를 정교하게 실현할 수 있도록 제도와 장비, 인력의 전반적 정비가 요구된다. 이를 통해 수사 효율성과 인권 보호를 동시에 달성할 수 있으며, 디지털 포렌식의 정당성과 사회적 수용성 역시 함께 확보될 수 있을 것이다.