실무상 디지털증거의 현장압수수색 문제점과 개선방안

김용호* · 이대성**

*성균관대학교 정보통신대학원, 부산가톨릭대학교 컴퓨터공학과**

The problem point and improvement program of the scene confiscation search of digital evidence at practical affairs

Yong-Ho, Kim* · Daesung Lee**

*Graduate school of infomation & Communications, Sungkyunkwan University, cstholic University**

E-mail : porsche0911@paran.com, dslee@cup.ac.kr

요 약

현재 법원에서의 디지털저장매체의 압수방법과 관련하여 형소법 제106조제3항에서 제시하는『원칙적 선별압수, 예외적인 매체압수』방식은 실제의 수사현실을 무시한 것이며, 이것을 준수하여 집행하기에는 압수목적달성에 어려운 점이 많다. 이에 현재의 압수수색방법의 문제점과 새로운 첨단 환경하의 디지털증거의 바람직한 현장 압수수색방법과 개선방안을 제시한다.

ABSTRACT

Currently, under being related with confiscation method of digital store medium from the court of justice, 「the sorting confiscation method of principle, the exceptional medium confiscation method」from in section3 no.106 of the criminal procedure code disregard the actual fields of investigation. What is more, there are many difficulties to execute cases by observing this for the achievement of confiscation purpose.

At this point, I present the problems of the present confiscation search method and the desirable scene confiscation search method and the improvement program under the new technology circumstance.his is an example of ABSTRACT format.

키워드

디지털 포렌식, 증거수집, 선별압수, 압수수색

Ⅰ. 서 론

정보화는 일상생활의 편리함을 가져왔지만, 이러한 문명의 이기가 예전의 아나로그 방식의 범죄에서 첨단범죄의 수단이 되거나 범죄의 대상이 되기도 한다. 이러한 디지털증거를 수단으로 하거나 범죄의 대상으로 하는 범죄의 경우에 압수목적달성을 위해서는 컴퓨터상에 기록된 증거를 적정한 절차를 거쳐 채증하여 무결성과 동일성을 유지된 채 분석되어 분석보고서가 법정에 증거로 제출되어야 한다.

하지만 일상의 편리함을 가져온 첨단 디지털증거는 대용량성, 불가시성·불가독성, 전문성, 익명성, 복제용이성, 전문성 등을 특성으로 하고 있다. 이는 종래 아나로그 방식 압수수색 방법만으로는 압수목적달성을 하기 어려운 경우가 많다. 아니 어떠한 경우에는 불가능하다고 할 수 있다. 따라서 종래의 영장주의 원칙을 고수하면서도 디지털 증거가 갖는 특성에 비추어 영장주의가 수정되어야 한다고 할 수 있다.

이러한 영장기재는 현장의 조사관에게 가이드라인을 제공하고, 행동 준칙에 따른 합리적 판단이었다는 점을 입증케 함으로써 피고인 측의 증거부동의에 대하여 선의의 항변을 가능하게 할 수 있다.

결국 전자적 정보가 갖는 특성에 비추어 영장주의 원칙을 준수하면서도 이익형량의 원칙과 합

리적 판단원칙을 적절히 조화를 이루는 선에서 현장 조사관의 컴퓨터 압수·수색 행동에 대한 위법여부를 판단하는 것이 바람직하다고 생각한다.

II. 수사과정에서의 원본압수금지조항에 대한 문제점

영장의 특정과 관련하여, 정보 자체를 압수할 수 있는 대상으로 하는 입법적 개선이 요구된다. 전자적 정보를 기록하는 저장매체에 대해서는 그 범위를 한정하기 어려울 만큼 영역이 확대되고 있다. 고정적인 하드디스크에서부터 보조장치 기억장치의 일종인 USB 메모리에서 외장하드디스크, CD, 다량의 데이터베이스의 자료, 스마트폰의 정보, 휘발성 증거가 일시적으로 기억된 주변기기까지도 이를 제외할 필요가 없다.

우리나라 디지털 증거법의 형성과정을 보면 대부분의 판례법이 대공·선거 등 공안사범에 대한 재판과정에서 형성되었다는 점이다. 디지털증거에 대한 사본 압수 원칙 등 압수수색 방식을 근본적으로 변화시킨 통제 법리도 공안사건을 통해 자리 잡게 되었다는 사실을 쉽게 알아볼 수 있다.2011년 5월 전교조 시국선언 관련 준항고 사건에서 대법원은 전자정보에 대한 압수수색은 혐의사실 관련 부분만을 현장에서 문서 출력하거나 복제하는 방식으로 이루어져야 하고 저장매체의 외부반출은 영장에 명기된 예외적인 때에만 허용된다는 법리를 내놓았다. 그 후 같은 해 7월 국회의 사법개혁 논의를 통해 형사소송법이 개정되어 정보저장매체에 대하여는 제한된 범위 내의 사본압수가 원칙이라는 규정이 신설되기에 이르렀다. 이 외에도 '영남위원회', '일심회' 사건 등에서는 전자정보의 증거능력 인정을 위한 요건, 전문법칙과의 관계 등에 관한 법리가 형성되었다.

위 전교조 사건 결정에서 설시된 법리를 기초로, 최근 영장 발부 시에는 집행 현장에서의 일부복제 원칙, 압수수색 전체 과정에 피압수자 등의 참여권 보장 등을 골자로 하는 집행방법 제한이 부가되고 있다. 법관에 따라서는 피압수자 등이 동의하지 않는 한 저장매체의 외부반출 자체를 금지하는 극단적인 사례도 있었다.

디지털증거의 대량성, 혼재성, 사생활 보호의 필요성 등을 고려하면 이렇게 심하게 통제할 이유도 있다고 생각한다. 하지만, 전자정보에 대한 일부 사본 압수 원칙을 우리처럼 법률 규정과 판례로 명문화하거나 집행기관의 재량영역인 압수수색 방법을 법원이 일일이 제한하는 강력한 통제체제를 외국에서 찾아보기 어렵다. 미국도 2009년에 연방형사소송규칙을 개정하였지만, 영장 유효기간을 10일에서 14일로 연장하고, 압수 이후의 복제·분석은 위 기간에 포함되지 않음을 명백히 하는 등 디지털 증거의 특수성이 가지는 수사 현실에 맞도록 정비하는 추세이며 우리나라처럼 디지털증거로 인한 수사를 원칙적으로 규제 법리는 전세계 어느 나라에서도 찾아보기 힘들다.

사본 압수 원칙을 따르다 보니 법집행 과정인 수사현장에서 많은 차질이 빚어지고 있다. 현장에서 대량의 서버를 압수해야 할 경우 원본을 압수하수 없어서 서버의 다량의 하드 디스크를 복제하느라 며칠간 압수수색이 지속되는 경우도 있다. 이런 경우 압수수색을 집행하는 사람 피 압수자 전부 압수과정에서 서로 지치게 된다. 또 어떤 경우에는 하드디스크를 반출할 수 없어 필요한 부분만 복사하여 분석을 하다 보니 사용자가 임의로 삭제한 삭제파일을 복구할 수 없어 수사에 난항을 겪는 경우도 많다. 하지만 다른 경우에는 삭제파일에서 중요한 수사단서가 나오기도 한다. 복구 부분은 디지털 증거분석에 있어 빠질 수 없는 중요한 부분 중의 하나인데도 불구하고 현장에서 파일의 일부만을 복사한 후 수사를 진행하다가 추가 압수수색의 필요성이 있어 다시나가 보았자 원본 디스크는 이미 폐기되고 없다.

현장에서 검색어를 통한 수색이 쉬운 줄 알지만 실제로 검색을 통해서 파일의 단서를 찾는 경우는 많지 않다. 대부분의 압수수색이 서버인 경우 다량의 자료들이 들어있는 데이터베이스를 압수하게 된다. 물론 이 또한 서버를 통째로 압수해야 하지만 원본압수금지 조항 때문에 디스크를 복제해가지고 오게 된다. 하지만 서버의 특성상 하드디스크를 레이드 형태로 묶어 있을 뿐만아니라, 설령 전부 하드디스크를 복제한다 하다라도 분석실에서 하드디스크이 내용을 100% 원상복구를 하기 쉽지 않다.

압수방법과 관련하여 형소법 제106조제3항에서 제시하는 「원칙적 선별압수, 예외적인 매체압수」 방식은 실제의 수사현실을 무시한 것이며, 이것을 준수하여 집행하기에는 압수목적달성에 어려운 점이 많다. 기본적으로 정보자체가 압수의 대상이 되는 경우 수사기관에서는 매체 전체를 압수할 필요는 없다. 범죄의 수단이 되거나 몰수의 대상이 되는 경우, 증거인멸우려가 있어 복구할 필요가 있는 경우, 현장에서 방해 등으로 현장에서 관련성을 따져 압수하기에는 사실상 어려운 경우 등에는 저장매체 자체를 압수할 수 있도록 하여야 한다. 당장 개정안을 도출하기 어려우면 당분간 수사기관으로서는 이러한 예외적인 상황을 사전에 법관에게 제시하고, 사법통제를 받아야 할 것이다. 그렇지 않으면 압수목적을 달성할 수 없을 뿐아니라 수사자체가 불가능할 수 있다.

범죄관련 정보와 무관한 정보가 혼재되어 있는 압수물을 분류하고 신속히 반환하도록 할 필요가 있다. 나아가 피압수자로 하여금 환부청구권을 명문화할 필요가 있고, 디지털 증거의 특성에 비추어 저장매체에 기억된 정보 일부를 폐기하는 경우에는 복구가 불가능하도록 암호화하여 매체를 돌려주는 방안도 검토되어야 한다.

또한 우리 현행법은 압수·수색 후 정보주체에 대한 통지와 관련하여 지체없이 통지하도록

요구하면서 구체적인 주체의 범위, 잠정적인 유보 등에 관하여 명확히 하지 않고 있다.

영장의 대상이, 특정 어드레스 소지자의 수신 메일의 일시 보존 파일 내지 백업 파일이 수록된 컴퓨터 또는 기억매체인 경우에는 비교적 특정이 간단한 경우도 있으나 피의자의 사무실 등에 있는 컴퓨터나 기록매체는 현장에 그들 매체가 몇 개나 있는지 사전에 알 수 없는 경우가 많고, 그 중에 과연 어느 매체에 목적하는 데이터가 수록되어 있는지 내용을 보지 않고는 알 수 없는 경우가 많다. 그러한 경우 목적으로 하는 데이터가 수록되어 있을 개연성이 있는 것을 유형적, 개괄적으로 제시하고, 거기에 '본건에 관계가 있는 데이터를 기록했다'고 간주하는 기재를 할 수 밖에 없기 때문에 영장의 조건인 특정성의 요청과 괴리문제가 발생한다.

III. 집행방법을 영장에 기재하는 방법

형사소송규칙 제107조는 압수·수색영장 청구서에 기재하여야 할 사항을 나열하고 있으나 압수·수색에 대한 구체적인 방법에 대하여는 현행법상 요청되고 있지 않다. 이를 현장에서 수색을 종료할 것인지 아니면 일단 캐비넷이나 서류, 컴퓨터 등 용기를 압수 후 제3의 장소에 이전해서 수색할 것인지에 대하여도 아무런 기재가 없다.

사전에 이러한 제3지에로의 장소의 이전, 어떠한 프로그램을 사용하여 수색할 것인가에 대한 구체적 집행방법을 영장에 기재하였다면 법원에서도 사전에 이를 허용한 것이라고 대항할 수 있을 것이다.

이러한 취지에서 미국의 연방대법원도, 특정한 파일을 찾기 위한 컴퓨터 수색 시 수사관들이 겪는 실제적인 어려움을 인정해 왔으며 추가적인 재산에 대한 임시적 압수나 제3의 장소에서 조사를 수행하는 것을 인정하고 있다[1].

따라서 우리도 컴퓨터에 대한 압수·수색 영장 청구서에는, 만일 수사관들이 관련된 증거를 확보하기 위해서 피의자의 주거지나 목적물 소재지 이외의 장소에서 수색을 수행하고 컴퓨터를 압수할 필요가 있을 경우, 그러한 가능성에 대한 설명과 충분한 근거를 기재하고, 컴퓨터를 수색하거나 분석하는 Tool과 사용할 기술, 컴퓨터 하드웨어 자체가 불법 물품이나 범죄의 도구이기 때문에 하드웨어를 압수한 경우 사후 수색을 필요로 하는 사유 등을 기재하도록 하는 방법을 새롭게 검토할 필요가 있다.

통신비밀보호법 제6조 제4항[2]이 통신제한조치 허가장 청구서에 구체적인 방법을 기재하도록 하는 것도 이와 같은 취지라고 해석할 수 있다. 입법적 검토가 요구된다. 다음은 바람직한 형사소송절차에 의한 정보저장매체 압수수색절차(안)의 내용이다.

IV. 정보저장매체 등의 압수절차(안)

형사소송법은 압수의 목적물이 컴퓨터용 디스크, 그 밖의 이와 비슷한 정보저장매체(이하 '정보저장매체'등이라 한다)인 경우

- 우선적으로, '범위를 정해 출력물이나 복제물을 압수'하도록 한다.
- 예외적으로, 현장 상황을 고려하여 선별적 판단이 현저히 불가능하거나 곤란할 때 정보저장매체 등을 압수할 수 있도록 규정하고 있다.

동 규정은 대법원의 판례(대결 2011. 5. 26. 자 2009모1190)의 입장을 반영하여 개정한 것으로 당분간 법률의 개정이나 판례의 변경은 어려울 것으로 보인다. 이러한 상황 하에서 각 수사기관은 위 법률의 취지에 충실하게 정보저장매체 등의 압수·수색 절차를 제정하여 시행할 수밖에 없을 것이다.

본 절차는 집행 현장에서 컴퓨터 등 정보저장매체로부터 디지털증거를 수집하는 과정에서 준수하여야 할 기본적 사항을 정함으로써 적절절차를 준수하면서 압수·수색을 통한 실체적 진실의 발견에 기여하고, 동시에 피 처분자의 프라이버시 등 기본적인 인권을 보호하기 위한 표준(안)의 제공을 그 목적으로 한다.

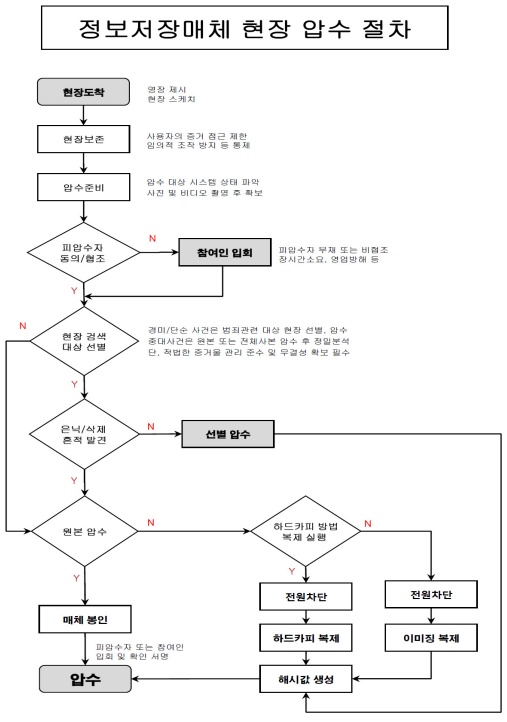

그림 1. 정보저장매체 현장압수절차(안)

4.1 사전 준비

가. 정보저장매체 등을 압수·수색·검증하거나 전자정보를 수집하고자 할 경우에는 사전에 다음 사항을 확인하고 계획을 수립한다.

1) 사건 개요, 압수·수색 장소 및 대상

2) 압수·수색대상 정보처리시스템의 유형과 규모

3) 압수·수색대상 현장 네트워크의 구성 형태

4) 기타 정보저장매체의 보유 현황 등

나. 압수목적 달성을 위해 사건의 성질에 따라 대상 범위 선정, 원본 또는 사본 전체, 출력물과 복사물 등 선별 압수의 필요성을 다음과 같이 명확하게 구분하여 영장을 청구한다.

1) 현장에서 범죄와 관련된 증거를 신속하게 획득할 가능성이 높고, 선별하여 압수하더라도 시비가 없을 것으로 평가 되는 경미·단순사건은 현장 검색 후 범죄 관련 압수대상 선별 압수한다.

2) 현장 선별과 분석에 장시간이 소요되거나 범죄와 관련된 파일이 상당부분 삭제된 흔적이 있거나 증거인멸의 가능성이 높은 경우, 또는 압수대상 디지털매체 전체에 대한 정밀분석이 필요한 '강력범죄, 첨단범죄, 산업보안, 테러·안보·보안범죄 등'사건은 원본 또는 전체사본을 압수 후 사후 범죄와 관련성이 없는 것으로 확인된 부분은 신속하게 반환하거나 폐기처분 한다.

3) 정보저장매체 등 그 자체가 밀수품, 증거물, 도구 혹은 범죄의 결과물인 경우에는 원칙적으로 매체원본을 압수

※ 불법자료를 전송하고, 저장하는데 사용하는 가정용 개인 컴퓨터는 그 자체 범죄의 도구로 평가하여 하드디스크를 압수 할 수 있다[3].

4.2 현장 압수

가. 영장에 따라 전자정보를 저장하고 있는 정보저장 매체를 수색하고 현장 무결성을 유지하며 압수대상을 선별한다.

나. 선별한 정보저장 매체의 전자정보의 압수방법은 압수 상황에 따라 다음과 같이 구분하여 진행한다.

1) 압수 영장에 따라 단순·경미사건은 압수대상 매체를 현장에서 수색 검증 후 혐의사실과 관련된 전자정보만을 문서로 출력하거나 수사기관이 휴대한 저장매체에 복사하여 압수한다.

2) 집행 현장에서 압수목적 달성을 위한 전체 검색·선별에 장시간이 소요되고, 정보저장매체의 비할당공간에 대한 정밀 분석이 필요한 첨단범죄, 산업보안·기밀유출, 강력범죄, 테러·안보관련 범죄 등의 경우에는 원본압수 또는 하드카피·이미징 실행한다.

3) 집행 현장에서 저장매체의 복제가 불가능하거나 현저히 곤란할 때(피압수자의 비협조 또는 협조하지 않는 경우, 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견되는 경우, 출력·복사에 의한 집행이 피압수자의 영업이나 사생활의 평온을 저해하는 경우, 기타 이와 준하는 경우) 피압수자 또는 참여인의 입회하에 저장매체의 원본을 봉인하여 압수한다.

4) 정보저장매체 등 그 자체가 밀수품, 증거물, 범죄의 도구 혹은 그 결과물인 경우에는 원칙적으로 매체원본을 압수한다

다. 피압수자 또는 참여인을 입회시키고 수색한 결과물이 대상 정보처리시스템의 자료로서 검색된 것임을 확인시킨 후 다음의 내용 작성하여 입회인의 확인서명을 받는다.

1) 압수·수색·검증 착수 시작과 종료시간

2) 정보처리시스템의 종류와 구성

3) 정보처리시스템의 고유번호(가능한 경우)

4) 검색·하드카피·이미징 도구와 방법

5) 압수 디지털 자료에 대한 해시 값(Hash Value)

4.3 무결성 확보를 위한 단계별 요령

가. 기본원칙

1) 디지털 증거의 무결성 유지를 위해 정보저장매체 등을 압수·수색·검증하거나 전자정보를 수집·분석할 때에는 정보저장매체 또는 전자정보를 수집한 때로부터 법정에 증거로 제출할 때까지 변경 또는 훼손되지 않도록 무결성을 유지하여야 하고 그 과정을 기록하여 수사기록에 첨부한다.

2) 압수 현장에 따라 발생하는 여러 가지 상황은 수사목적 달성 및 인권보호를 위한 적절한 방법으로 조치를 취한 후 정보처리시스템과 정보자료의 압수·수색·검증을 실시하고, 그 과정을 기록하여 첨부한다.

나. 압수, 수색 요령

1) 정보저장매체 등을 압수·수색·검증하거나 전자정보를 수집하는 현장에서 복제·분석을 실시하는 경우에는 쓰기방지 기능이 포함된 기기를 사용하는 등으로 자료가 변경 또는 훼손되지 않도록 주의한다.

2) 압수대상 정보저장 매체는 식별 값을 특정할 수 있도록 기록하고 불가능할 경우 촬영, 시리얼확인(콘트롤러, 볼륨시리얼 등) 등 향후 증명을 위한 적절한 조치 수행한다.

다. 이송, 보관요령

1) 전자정보가 저장된 정보저장매체 등을 운반 또는 보관할 경우에는 정전기차단, 충격방지 등의 조치를 취하여 해당 기기 등이 파손되거나 저장된 디지털 자료가 손상되지 않도록 관리한다.

2) 장기간 보관의 경우 디지털 증거보관 케이스에 넣고, 습기 등을 차단하는 등의 조치를 취하고, 복사본을 만들어 둠으로써 손상에 대비하여야 한다.

3) 배터리에 의해 구동되는 장치에 대해서는 이미징을 하는 등의 즉각적인 대응조치가 필요하다.

4.4 기타 유의사항

가. 정보저장매체 등을 압수·수색·검증하거나 전자정보를 수집하는 현장에서 사용자가 대상 정보시스템의 전원과 운영장치에 대한 전원차단, 강제 종료 등 임의적 조작 행위 방지를 위한 통제한다.

나. 압수·수색·검증 대상 정보처리시스템이 네

트워크에 연결되어 있고 압수·수색대상자가 네트워크로 접속하여 저장된 자료를 임의로 삭제할 우려가 있을 경우에는 네트워크 연결 케이블을 차단한다.

Ⅴ. 결 론

최근 디지털 증거 압수수색의 문제점과 개선방안에 대한 문제점을 지적하는 사례들이 늘고 있다. 디지털 증거 압수수색 절차를 두고 법원과 학계는 디지털 증거가 개인 사생활을 침해할 우려가 있는 만큼 영장 발부 기준을 엄격히 해야 한다고 주장하고 있고, 검찰을 비롯한 수사기관 입장에선 수사 인원 부족과 예기치 못한 상황 그리고 디지털자료의 방대한 점 때문에 이를 감안해야 한다고 서로들 자신의 입장에서 주장하고 있다.

물론 이러한 주장은 수사과정에서 충분히 있을 일어날 수 있는 상황이고, 개인적사생활 보호측면에서는 그렇게 주장할 여지도 있다. 하지만, "현행 압수수색 규정은 그 대상을 증거물 또는 물건으로 규정하고 있을 뿐만아니라 디지털 증거라고 해서 그것이 범죄의 증거임에도 불구하고 이를 압수할 수 없는 상황을 만들어 수사가 중단되거나 아예 수사를 하지 못하는 상황이 발생되어서는 안된다고 판단된다. "디지털 증거물을 처리하는 전문인력 부족으로 현장에서 수많은 디지털 기기 등을 일일이 검색해 볼 수 없는 상황이다. 압수수색 과정에서 수사기관이 우선 수색을 하고, 추후 문제 발생시 법원에서 분쟁을 조정할 수 있도록 해야 하는 것이 옳은 판단이라고 생각된다.

우리나라의 형사소송법상 증거는 원본을 압수수색하는 것이 원칙으로 하고 있고, 디지털 증거는 소유자가 현장에서 쉽게 위변조하기에 용이하다. 이러한 문제점을 야기하는 만큼 디지털 저장매체를 압수하는 하는 것이 현실에 맞다고 할 수 있다. 그렇기 때문에 그동안 문제가 될 수 있는 부분이 많은 압수절차에 새롭게 압수절차를 제안 시행하여 실제 압수 현장에서 문제가 될 수 있는 부분이 말끔히 해소 되었으면 하는 바람이다.

참고문헌

[1] United States v. Hay, 231 F.3d 630, 634, 9th. Cir., 2000

[2] 통신비밀보호법 제6조4

[3] (Davis v. Gracey, 111 F. 3d 1472, 1480(10th Cir. 1997)