서울대학교 이학석사 학위 논문

불송치 결정에 따른 디지털증거의 보관 및 관리 방안에 대한 연구

2023년 2월

서울대학교 융합과학기술대학원

수리정보과학과(정보보호 및 디지털포렌식학 전공)

김 영 현

불송치 결정에 따른 디지털증거의 보관 및 관리 방안에 대한 연구

지도교수 이 효 원

이 논문을 이학석사 학위논문으로 제출함

2022년 12월

서울대학교 융합과학기술대학원

수리정보과학과 정보보호 및 디지털포렌식학 전공

김 영 현

김영현의 석사 학위논문을 인준함

2023년 1월

위 원 장 천 정 희 (인)

부위원장 이 효 원 (인)

위 원 전 동 석 (인)

국문초록

형사법적으로 디지털증거는 비가시성・취약성・변조 가능성・복제 용이성・대규모성이라는 취약점으로 인하여 무결성・진정성・동일성・신뢰성・관리 연속성이 담보되어야 법정 증거능력이 부여될 수 있다. 그럼에도 디지털증거는 훼손 가능성이 매우 높음에도 불구하고 CD/DVD/USB 메모리 등의 정보저장매체를 이용하여 수사기록에만 편철하여 보관하는 구태를 벗어나지 못하고 있는 실정이다. 이는 기존 검찰에서 모든 사건에 대한 수사기록을 일괄적으로 송치받아 검찰청 보존계에 보관 및 관리하던 방식에서 개정 형사사법시스템상 경찰과 검찰이 각각 수사기록을 분리하여 보관 및 관리하는 방식으로 변경되어, 항시 디지털증거에 대한 관리 위험성을 내포하고 있음을 부인할 수 없는 상황에 이르렀다고 볼 수 있다.

특히 피의자 또는 참고인 소재불명에 따른 수사중지, 범죄사실과 증거 간 혐의없음・증거불충분・공소권없음 등으로 종결된 경찰의 불송치 수사기록에는 향후 새로운 증거가 발견되거나 사정 변경 등으로 검찰・군검찰에 송치 또는 이송될 가능성이 있는 수사기록상 디지털증거를 수사기록에 편철가능한 CD/DVD/USB메모리 등 정보저장매체에만 보관하여 관리하는 현 실태는 디지털증거 훼손으로 형사사법시스템에 대한 국민의 신뢰를 저버리는 가능성이 존재하는 상황이다. 이에 경찰에서는 이미지 파일 형태로 생성하고 해시값을 확인하는 방식으로 디지털증거 압수를 원칙으로 하는 규정을 신설하여 모든 종류의 디지털증거는 경찰 디지털증거 클라우드 서버(가칭: 폴-클라우드)에 보관함으로써 디지털증거에 대한 무결성・진정성・동일성・신뢰성・관리 연속성이 담보될 수 있도록 한다. 이렇게 보관된 디지털증거 중 불송치 증거는 공소시효 완성 완성되는 해의 익년도까지 보관함을 원칙으로 하되, 후일 송치결정이 이뤄지면, 사법경찰관의 보완수사가 완료되는 해의 다음 해까지만 보존하도록 하는 규정을 신설함으로써 보존기한 경과 시 자동으로 삭제하는 조치를 실시한다. 이는 무한

정 늘어만 가는 서버 데이터 스토리지 구축 비용을 절감할 수 있다는 장점이 있을 것으로 예상하고 지속 가능한 증거 보관 유지할 수 있게 할 것이다.

위와 같이 디지털증거 확보 단계에서부터 다수의 디지털증거를 하나의 이미지(Image) 파일 형태로 보관하고 이를 경찰 디지털증거 클라우드 서버(가칭: 폴-클라우드)에 보관하는 방식으로 변화할 경우, 디지털증거의 비가시성・취약성・변조 가능성・복제 용이성・대규모성이라는 취약점을 극복하고 무결성・진정성・동일성・신뢰성・관리 연속성을 담보하여 궁극적으로 개정 형사사법시스템상 경찰 수사에 대한 국민의 신뢰를 제고할 것이라고 예상한다.

주요어 : 불송치 디지털증거 이미지 폴클라우드
학 번 : 2021-23755

목 차

표 목 차

그 림 목 차

제 1 장 서론

제 1 절 문제 제기

디지털증거는 비가시성・취약성・변조 가능성・복제 용이성・대규모성이라는 취약점으로 인하여 무결성・진정성・동일성・신뢰성・관리 연속성이 담보되어야 법정 증거능력이 부여될 수 있다.

경찰의 디지털증거 확보 시 다수의 디지털증거를 하나의 압축 파일로 작성하고 이에 대한 전자정보 상세목록에 압축 파일에 대한 파일명과 해시값을 피압수자에게 교부하고 있으며, 이와 같이 압수한 디지털증거는 CD/DVD/USB메모리 등의 정보저장매체를 이용하여 수사기록에만 편철하여 보관하는 실정이다. 압축 파일은 디지털포렌식에 대한 이해가 없는 사람도 쉽게 압축 파일 내부의 전자정보를 편집・조작이 가능하므로 디지털증거 보관 및 관리에 취약성이 그대로 노출되어 있다는 문제가 제기된다. 또한 압수된 디지털증거는 CD/DVD/USB메모리 등의 정보저장매체에만 보관하고 있는 실무를 돌이켜보면, 디지털증거가 저장・보관된 유일한 정보저장매체가 물리적으로 훼손될 경우 디지털증거 복구는 요원해진다. 이에 더하여, 수사 또는 공판 과정에서 USB메모리의 일부 엑셀 등 문서파일을 검토하는 과정에서 파일을 열어보는 그 행위 자체만으로도 해시값이 변경되어 디지털증거의 무결성에 심각한 문제가 발생할 수도 있으며, 고의 또는 과실로 USB메모리에 보관된 파일을 삭제할 수도 있게 된다. 국민의 형사사법제도에 대한 신뢰가 언제 어디에서 문제였는지도 밝히지 못한 채 무너질 수 있는 문제가 있음을 제기하지 않을 수 없다.

물론 디지털증거를 수사기록에 편철함으로써 기록 검토 과정에서 바로 확인할 수 있다는 수사 효율성이라는 장점을 부인할 수는 없다. 그러나 수사 효율성이라는 이유로 이에 대한 대비책을 마련하지 않는 것을 당연하다고는 할 수 없다. 형사소송법 개정으로 경찰은 범죄가 성립하는 것으로 판단되면 검찰에 사건을 송치하고, 범죄가 성립하지 않는 등의 사건에 대해서는 검찰에 이를 송치하지 않고 이렇게 조제된 수사기록은 경찰 보

존 창고에 보관을 하게 되는데 이 중에는 피의자 또는 참고인 등이 소재 불명, 국외도피 등으로 처분하는 수사중지 사건 등도 포함되어 있다. 이는 곧 언젠가 소재 발견 등의 사유로 수사가 재기되어 범죄가 성립하는 것으로 판단되어 검찰에 송치할 가능성 역시 존재하고 있다. 예를 들어 피의자 국외도피로 30년 경찰 보존 창고에 잠자고 있던 수사기록이 소재 발견으로 사건을 재기하였는데 최초 수사 당시 확보한 디지털증거가 보관된 DVD 매체가 장기간 보관되면서 물리적 훼손되어 있다면, 이 사건의 피해자는 어디에 호소할 수 있겠는가.

이러한 점을 고려하여 검찰에 송치하는 사건뿐만 아니라 불송치하는 사건의 디지털증거 역시 그 보관 및 관리에 체계적인 접근이 필요함을 제기하는 바이다.

제 2 절 연구의 내용 및 방향

디지털증거에 대한 기술적·법규적 특징을 바탕으로 실무상 디지털증거 보관 및 관리 절차가 관련 법규·판례상 어떤 문제점이 있는지 살펴보고, 이에 대한 해결책과 관련 법제도 개선 방안을 제안한다.

위와 같은 연구 내용 중 중점사항은 수사기록에 편철하여 보관하는 디지털증거 보관 및 관리 방식의 법적·기술적 특징을 기술하고, 이를 극복하기 위해 경찰청 디지털증거 훈령상 디지털증거 수집 시 포렌식 이미지를 생성함을 원칙으로 하고, 이렇게 저장된 디지털증거는 별도 '경찰 디지털증거 클라우드 서버'를 구축하여 관리하고, 범죄혐의 인정되어 송치 시 경찰에서 검찰에 디지털증거를 안전하게 송부하는 대안을 마련하여 디지털증거의 취약성을 극복하고 무결성을 담보하여 법정 증거능력이 인정되도록 그 대안을 마련한다.

제 2 장 불송치결정과 디지털증거의 관리

제 1 절 개정 형사소송법

1. 형사소송법 일부개정 이유

2021년 1월 1일부터 개정 시행된 형사소송법은 경찰과 검찰의 수사권에 일대 변혁을 가져왔다. 기존 모든 수사에 대해 사법경찰관은 검사의 수사지휘를 받는 구조에서 경찰과 검사는 상호 협력의 방향으로 변경되어 시행되었다. 이는 기존 검사가 사법경찰관에게 수사지휘하는 수직적 구조에서 상호 동등한 수사기관으로서 협력하고 수사권이 국민을 위해 민주적이고 효율적으로 행사되도록 하려는 목적에서 개정된 것이라고 개정 이유에서 밝히고 있다.[1)]

변화된 주요 내용을 보면, ①검사와 사법경찰관은 수사, 공소제기 및 공소유지에 관하여 서로 협력하는 관계로 정립한다는 규정, ②경위부터 경무관 등은 사법경찰관으로서 범죄의 혐의가 있다고 사료하는 때에 범인, 범인사실과 증거를 수사한다는 규정, ③검사는 사법경찰관에게 송치사건의 공소제기 여부 결정 또는 공소의 유지에 관하여 필요한 경우 등에 해당하면 사법경찰관에게 보완수사를 요구할 수 있고, 사법경찰관은 정당한 이유가 없는 한 지체 없이 이를 이행하도록 하는 규정으로 변화되었다. 이와 더불어 검사는 사법경찰관에 대한 법령위반 등 사유로 시정조치요구권이 있고, 사법경찰관이 수사한 사건의 혐의가 인정되면 송치결정을, 인정되지 않으면 불송치결정 권한을 부여하여 책임수사를 강화시킨 측면이 있다.

---

1) 형사소송법[시행 2021. 1. 1.] [법률 제16924호, 2020. 2. 4., 일부개정] 【제정·개정이유】 전문

2. 경찰 소속 사법경찰관의 권한 변화

2-1. 수사지휘권 폐지

개정 형사소송법에서 검사의 수사지휘권을 폐지하고, 경찰에게 1차 수사권과 수사종결권을 부여하였다. 개정 전 형사소송법 제195조에는 검사의 수사권에 대해 규정하고 있었지만, 개정 형사소송법 제195조는 검사와 사법경찰관의 관계를 상호 협력의 관계로 규정하고 있다.

제195조(검사의 수사) 검사는 범죄의 혐의 있다고 사료하는 때에는 범인, 범죄사실과 증거를 수사하여야 한다.

<표 1> 형사소송법 개정 전

↓

제195조(검사와 사법경찰관의 관계 등) ① 검사와 사법경찰관은 수사, 공소제기 및 공소유지에 관하여 **서로 협력**하여야 한다. ② 제1항에 따른 수사를 위하여 준수하여야 하는 일반적 수사준칙에 관한 사항은 대통령령으로 정한다.[본조신설 2020. 2. 4.][종전 제195조는 제196조로 이동 <2020. 2. 4.>]

<표 2> 형사소송법 개정 후

개정 전 형사소송법 제196조 제1항에 따라 수사관, 경무관, 총경, 경정, 경감, 경위는 사법경찰관으로서 모든 수사에 관하여 검사의 지휘를 받아야 했었다. 하지만 개정 후 '지휘'라는 항목은 삭제되었고, 이를 대신하여 제197조의2(보완수사요구) 조문이 신설되었다. '보완수사요구'는 송치된 사건에 공소의 유지에 필요한 경우에 사법경찰관에게 말 그대로 보완수사를 요구하는 것이다. 보완수사 요구를 하는 경우에도 관계 서류 및 증거물을 경찰에 송부하여야 한다.

2-2. 사건기록 및 증거물 송부의 변화

검사의 사법경찰관에 대한 시정조치, 사법경찰관의 수사중지, 고소인 등의 이의신청, 경찰 간 이첩 같은 제도의 신설도 검·경 간의 증거물을 송

부해야 하는 구조적인 변화가 생겼다. 개정 형사소송법으로 검·경 간 증거물 송부 변화도 생겼지만, 경찰서 간 이송에도 변화가 생겼다. 그간 경찰은 수사 지연 방지 및 사건관계인의 권리보호 등을 이유로 경찰서 간 이송을 제한해, 검찰로 송치 후 재판관할이 있는 검찰청 간 이송으로 수사를 종결하였다. 그러나 개정 형사소송법 이후에는 경찰에 수사종결권이 있어 원칙적으로 재판관할이 있는 검찰청에 사건을 송치해야 하기 때문에 경찰서 간 관련 서류, 증거물 송부, 즉 경찰서 간 이송도 증가하게 되는 변화가 생겼다.[2)]

3. 사법경찰관의 불송치 권한

개정 형사소송법 시행으로 가장 크게 바뀐 것은 경찰에서 검찰로 송치 방법과 수사지휘권 폐지이다. 먼저 송치 방법에 대해서 살펴보면, 개정 전에는 형사소송법 제196조 4항('사법경찰관은 범죄를 수사한 때에는 관계 서류와 증거물을 지체 없이 검사에게 송부하여야 한다.')에 따라 경찰이 수사한 모든 사건을 검찰에 송치하여야 하는 '전건 송치주의'였다. 하지만 개정 후 형사소송법 제245조의5 제1호 범죄의 혐의가 있다고 인정되는 경우에 검사에게 사건을 송치, 제2호 그 밖의 경우에는 그 이유를 명시한 서면과 함께 관계 서류와 증거물을 지체 없이 검사에게 송부하는 불송치로, 혐의 유무에 따라 선별적으로 송치하는 '선별 송치주의'로 변화하게 되었다.[3)]

2) 정웅길·이상진. (2022). 경 · 검 수사권 조정에 따른 디지털증거 인수 · 인계 과정상 증거능력 유지방안. 디지털포렌식연구, 127.
3) 정웅길·이상진. (2022). 경 · 검 수사권 조정에 따른 디지털증거 인수 · 인계 과정상 증거능력 유지방안. 디지털포렌식연구, 127.

제245조의5(사법경찰관의 사건송치 등) 사법경찰관은 고소·고발 사건을 포함하여 범죄를 수사한 때에는 다음 각 호의 구분에 따른다.

1. 범죄의 혐의가 있다고 인정되는 경우에는 지체 없이 검사에게 사건을 송치하고, 관계 서류와 증거물을 검사에게 송부하여야 한다.
2. 그 밖의 경우에는 그 이유를 명시한 서면과 함께 관계 서류와 증거물을 지체 없이 검사에게 송부하여야 한다. 이 경우 검사는 송부받은 날부터 90일 이내에 사법경찰관에게 반환하여야 한다.[본조신설 2020. 2. 4.]

<표 3> 형사소송법 사건 송치 및 불송치 근거 규정

이와 같이 과거 경찰에서는 수사종결권이 없어 범죄 혐의 유무와 관계없이 입건된 모든 사건은 검찰에 관련 서류와 증거물을 송부하였으나 개정 형사소송법 시행 이후에는 경·검 상호 간 관계 서류와 증거물을 송부해야 하는 구조로 바뀌게 되었고, 이는 경찰이 불송치 결정을 하는 경우에 관계 서류와 증거물을 송부받은 검사는 송부받은 날로부터 90일 이내에 사법경찰관에게 반환하는 구조로 변화하게 된 것이다.

4. 경찰의 불송치 사건 현황

경찰청 보도자료에 의하면, 2021년 6월말 기준 불송치 사건은 172,857건, 수사중지 사건은 39,729건에 이른다. 이와 같은 수사환경의 변화 속에서 위·변조에 취약한 디지털증거는 수집 및 분석 과정을 거쳐 법정에 제출되기까지 과정이 명확하고, 이러한 과정에 대한 추적이 가능한지, 그리고 증거가 법정에 제출되기까지 변경이나 훼손이 없이 유지되었는지도 끊임없이 유의하여야 한다.

[송치 사건] 보완수사요구		[불송치 사건] 재수사요청		[수사중지 사건] 시정조치요구	
'20년	'21년	'20년	'21년	'20년	'21년
4.1%	9.7%	5.0%	3.2%	2.3%	3.2%
18,074명 (440,397명 中)	31,482건 (323,056건 中)	13,148명 (265,597명 中)	5,584건 (172,857건 中)	1,891명 (81,300명 中)	1,275건 (39,729건 中)
5.6%p ↑		1.8%p ↓		0.9%p ↑	

<표 4> 검사의 요구·요청 건수(전년 대비)

즉 검·경 간 디지털증거 인수·인계 과정상 무결성·동일성·진정성·관리 연속성 등의 증거능력 요건이 반드시 유지되어야 한다. 개정 형사소송법 시행 이후 변화된 수사 환경과, 급속하게 변화하는 정보화에 맞게 수사기관도 맞게 변화할 필요가 있다. 디지털증거가 수사의 성패를 가늠할 정도로 중요한 역할을 하고 있는 만큼, 디지털증거의 증거능력을 유지하기 위한 개별 수사기관 내부의 조치뿐만 아니라 수사기관 간 표준절차를 마련하는 등 적극적인 대응이 필요하다.

제 2 절 디지털증거의 특징과 생성

1. 디지털증거 특징

1-1. 디지털증거 정의

1995년 미국, 호주 등 여러 국가의 법집행관계자들을 중심으로 창설된 '컴퓨터증거에 관한 국제조직(IOCE: Imternational Organization on Computer Evidence)은 '디지털증거'를 '이진수 형태로 저장 혹은 전송되는 법정에서 신뢰될 수 있는 정보'라 정의하고 있으며, 미국 법무부 마약수사청(Drug Enforcement Administration: DEA), 연방수사국(Federal Bureau of Investigation : FBI) 등 연방정부 기관의 증거분석 연구소들을 중심으로 구성된 '디지털증거에 관한 과학실무그룹(Scientific Working

Group on Digital Evidence: SWGDE)은 '디지털증거'를 '디지털 형태로 저장되거나 전송되는 증거가치 있는 정보'라 규정하고 있다.[4)]
현재 우리나라에서 디지털증거는 보통 "디지털 형태로 저장되거나 전송되는 범죄 증거로서 가치 있는 정보", "컴퓨터 또는 기타 디지털 저장매체에 저장되거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있는 증거가치가 있는 정보"를 의미하고 있다.

대검찰청 예규인「디지털증거의 수집·분석 및 관리 규정」제3조에서 "디지털증거"란 "범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보"라 정의하고 있으며, 경찰청 훈령인 「디지털 증거의 처리 등에 관한 규칙」제2조에서 "디지털 증거"를 "범죄와 관련하여 증거로서의 가치가 있는 전자정보"라 정의하고 있다. 즉, 디지털증거는 ①정보의 표기 및 저장이나 전달의 형태가 0과 1의 조합인 이진수 방식, 즉 디지털 형태인 정보, ②저장·전송의 매체가 컴퓨터, 스마트폰 등 디지털 정보기기, ③저장 또는 전송되는 정보, ④증거가치가 있는 정보 등 개념적인 요소들을 충족해야 함을 알 수 있다.

1-2. 디지털증거 종류

디지털증거는 저장 상태에 따라 비휘발성 디지털 데이터와 휘발성 디지털 데이터로 분류할 수 있고, 생성과정에 따라 컴퓨터에 저장된 정보와 컴퓨터에 의하여 자동 생성된 정보로 분류할 수 있다. 휘발성 증거는 프로세스, 예약작업, 인터넷 연결 정보, 네트워크 공유 정보, 메모리 정보 등 컴퓨터의 종료 등의 기능으로 인해 쉽게 휘발될 수 있는 정보를 의미하며, 비휘발성 증거는 파일, 파일시스템, 운영체제, 소프트웨어 등 임의적인 삭제 없이는 쉽게 삭제되지 않는 정보를 의미한다. 디지털증거는 일반증거물과 달리 물질로 존재하는 것이 아닌 데이터로서 존재하기 때문에 다음과 같은 특성을 지니고 있다.[5)]

---

4) 양근원, (2006). "형사절차상 디지털증거의 수집과 증거능력에 관한 연구", 경희대학교 박사학위 논문, 20-21.
5) 손지영·김주석, (2015). "디지털 증거의 증거능력 판단에 관한 연구", 사법정책연구원, 37-38.

1-3. 디지털증거의 성격

1-3-1. 비가시성・비가독성・잠재성

디지털 저장매체에 담긴 데이터는 이진수 형태의 전자적인 신호로 존재하므로 육안으로 바로 인식할 수 없고, 그 내용을 파악하기 위해서는 일정한 하드웨어나 소프트웨어로 구성된 변환장치를 사용하여 사람이 인식할 수 있는 형태로 변환해야 한다. 이러한 디지털 정보의 가시성, 가독성 확보 과정은 물리적이 아닌 기술적·논리적인 방법이 동원되어 디지털증거의 증거능력 검토 과정에서 포렌식 도구의 신뢰성이나 분석관의 전문성 검증과 연관된다.[6)]

1-3-2. 취약성

디지털 정보는 수정・삭제・변경・조작이 용이하다. 이 특징은 디지털 정보를 쉽게 가공할 수 있는 장점으로 활용될 수 있지만 증거 측면에서는 위・변조, 증거 인멸의 가능성이 높다는 단점으로 작용한다. 일반 물리적 증거의 경우 쉽게 특성이 변하는 화학물질이나 사라지기 쉬운 미세물질인 경우를 제외하고는 증거가 갑자기 사라지는 경우는 드물다. 또한 증거를 조작하면 조작 흔적 또한 남게 되므로 조작 여부를 비교적 쉽게 판별할 수 있다.[7)]

또한 디지털 정보는 변조와 삭제가 용이하기 때문에 정보의 신뢰성이 쉽게 훼손될 수 있다. 디지털증거에 대한 증거수집, 보존, 분석과정에서 각종 소프트웨어나 장비 등을 사용할 때 인위적 조작을 하게 되거나 의도하지 않더라도 시스템 작동과정에서 시스템 내의 파일들에 변화가 일어나는 경우도 있다.[8)]

---

6) 탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보 방안, 한국형사정책연구원(2006), 35., 손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 26-27.

7) 탁희성·이상진, (2006). 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보 방안, 한국형사정책연구원, 36-37.

8) 양근원, (2006). “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 박사학위 논문, 경희대학교, 22.

1-3-3. 복제용이성・매체독립성

디지털증거는 어떠한 저장매체에 저장되더라도 그 정보가 동일한 경우에 동일한 가치를 지닌다는 의미에서 저장매체와 독립되어 있다. 하드디스크에 저장된 파일을 USB에 복제하여 이 두 개의 파일이 동일한 정보와 해시값을 가지는 경우에 원본 파일과 사본 파일의 구별이 불가능하고, 그 저장매체로부터 독립하여 복제를 통해 이동할 수 있게 된다. 이를 '매체 독립성'이라고 한다. 따라서 수집된 증거가 원본인지, 복사본인지 명확하게 하는 것이 요구되며, 후에 디지털증거에 증거능력을 부여하기 위한 요건인 무결성(진정성) 내지 동일성의 요건 충족 여부를 판단하기 위한 전제로 문제가 되는 것이다.[9)]

1-3-4. 대량성

디지털 시대에서 각종 메신저의 텍스트부터 대용량 멀티미디어 자료까지 대형 기업의 서버와 클라우드에 쌓여가고 있다. 그만큼 정보저장매체의 저장용량이 방대해졌다. 유튜브나 구글에 저장되는 데이터는 그 데이터 크기를 상상하기 어려울 만큼이나 커져만 가고 있다. 일상 생활의 대화는 스마트폰과 컴퓨터로 이뤄지고 있고, 다이어리에 그 일상을 기록하는 사람들의 생활은 스마트폰 다이어리, 캘린더, 메모장이 이를 대신하고 있다. 방대해져만 가는 디지털 시대 데이터는 디지털증거의 대량성이라는 특성이 되었고 그만큼 개인의 사생활과 범죄 관련 데이터는 커져만 가는 형국인 것이다. 이러한 일상 생활의 디지털 정보가 대량성이라는 특징을 가지므로 디지털포렌식 절차에서 범죄와 관련 정보에 한하여 데이터의 선별 압수가 이슈가 되어온 것이다. 물론 피압수자의 인권을 보호한다는 취지도 있지만, 이러한 데이터의 대량성을 반영하여 형사소송법 제106조3항에서 컴퓨터용 디스크 등 정보저장매체에서 압수할 경우, 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다고 규정하게 된 것이다

.

9) 손지영·김주석, (2015). "디지털 증거의 증거능력 판단에 관한 연구", 사법정책연구원, 26.

1-3-5. 휘발성

컴퓨터 또는 스마트폰을 사용하면서 생성된 절대적 양의 데이터는 컴퓨터 메모리 또는 네트워크상에만 일시적으로 존재하는 휘발성을 가진다. 휘발성 데이터는 범행이 계속되는 상황에서 디지털포렌식 분석결과에 대한 결정 시 유의미한 판단의 근거가 될 수 있으므로 디지털증거 수집 과정에서 각별히 유의하도록 해야 한다.

2. 디지털증거의 증거능력 인정 요건

디지털증거는 기존 유체물인 증거물과는 다른 매체독립성, 취약성 등의 특성을 가지고 있다. 그래서 디지털증거가 증거능력을 인정받아 법정에서 증거로 사용하기 위해서는 증거 수집 절차의 적법성 확보뿐만 아니라 진정성・무결성・원본성・신뢰성 등의 문제가 해결되어야 한다.[10]

대법원 판례에서도 “정보저장매체에 저장된 문건 또는 그로부터 출력된 문건을 증거로 사용하기 위해서는 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 수집(압수) 시부터 문건 출력 시까지 변경되지 않았음(무결성)이 담보되어야 하며, 위 문건을 진술증거로 사용하는 경우 그 기재 내용의 진실성에 관하여는 전문법칙이 적용된다”고 언급하고 있다.[11]

2-1. 무결성(Integrity, 동일성)

디지털 증거는 취약성(변조의 용이성) 특성을 가지고 있어, 최초 수집된 증거가 저장된 매체에서 법정에 제출되기까지 변경이나 훼손이 없었다는 점을 입증하여야 한다. 이는 진정성의 문제와도 연관되어 있다. 디지털증거를 처리하는 전과정에서 많은 사람들이 개입하게 되는데, 이 경우 각 절차마다 원본 데이터의 무결성이 그대로 유지되고 있다는 절차적 보증을 해야한다.[12] 이 과정에서 무결성을 검증하기 위해 ‘해시함수’[13]를 사용한

10) 손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 30.

11) 대법원 2013. 6. 13. 2012도16001 판결

다. 이는 신뢰성을 갖는 본래 증거가 관리 과정에서 변경되지 않은 상태를 유지하고 있는지 증명하는 데에 여전히 사용되고 있다.

2-2. 진정성(Authenticity)

진정성은 디지털 증거가 저장·수집 과정에서 오류가 없으며, 특정한 사람의 행위 결과가 정확히 표현되었고, 그로 인해 생성된 자료인 것임이 인정되어야 한다는 것이다. 진정성 구성요소 중 가장 중요한 요소는 기록의 생산 주체, 생산주체에 의한 발신, 생산 시점이다. 무결성은 디지털증거의 수집·관리 등 증거처리의 절차적 측면에 초점이 있다면, 진정성은 최초의 증거와 법정에 제출된 증거가 일치한다는 성질을 밝히는 것이다. 이는 디지털증거가 갖추어야 할 가장 기본적인 요건으로 파악되기도 한다.

2-3. 원본성(Originality)

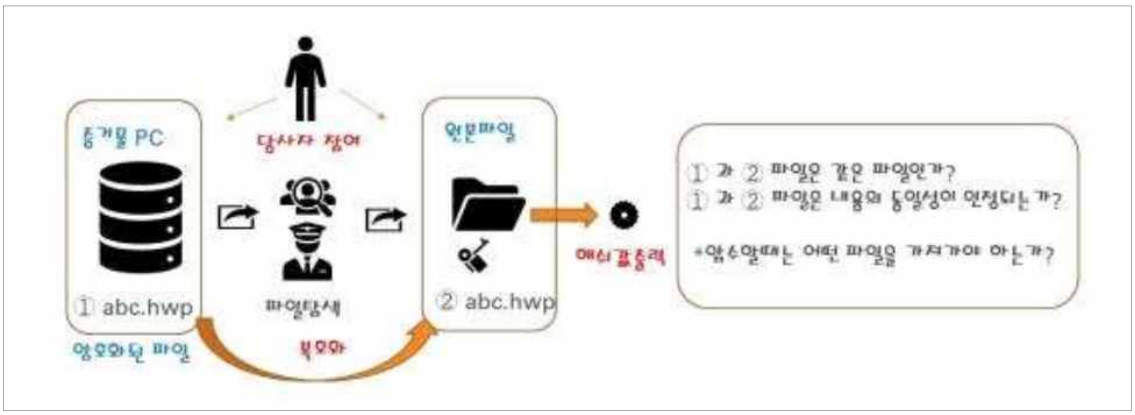
디지털증거의 출력물을 원본으로 인정할 수 있는지 다양한 학설이 있으나, 우리 형사소송법에서는 미국의 최량증거원칙을 채택하고 있지 않으므로 디지털증거의 원본성에 대하여 다툴 실익은 그다지 많지 않다고 보고 있다.[14)]

법원행정처의 법원실무제요에는 “원본(原本)”이란 일정한 사상을 표현하기 위하여 최초에 확정적으로 작성된 문서를 말하고 “사본(寫本)”은 원본을 등사한 문서를 총칭하여 말하는 것으로서, 누가 작성한 것이든, 문서

12) 양근원, (2006). “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위 논문, 20-21.
13) Hash Value: 해시값은 데이터를 고유하게 식별하는 고정 길이의 값으로 해시함수의 결과로 생성된다. 만약 원본에서 조금이라도 변경이 되면 계산되는 해시값이 완전히 달라지기 때문에, 일반적으로 디지털증거의 무결성을 입증하는 수단으로 사용되고 있다.(대검찰청 디지털증거 예규)
14) 손지영·김주석, (2015). 디지털 증거의 증거능력 판단에 관한 연구, 대법원 사법정책연구원, 36.

의 전부이든 일부이든 가리지 아니하고 모두 지칭한다고 정의하고 있다. 특히 “등본(謄本)”은 원본의 기재사항 전부를 그대로 옮겨 기재하고 작성자가 원본과 동일함을 증명한 것이라고 하며, “초본(抄本)”은 원본 내용 중 일부만을 옮겨 기재하고 초본임을 인증한 서면으로서, ‘원본의 존재와 옮겨 기재된 내용을 증명하는 효력’을 갖는다고 설명한다.[15]

원본성과 관련하여 최근에는 카카오톡 또는 텔레그램 메신저 등과 같은 데이터베이스에서 추출한 자료의 일부가 원본인지 여부에 대한 의문이 생길 수 있다. 암호화된 파일의 압수나 휴대전화에서 카카오톡이나 텔레그램 등의 메시지 전자정보를 압수하는 경우가 있는데, 이들 데이터는 기술적인 측면에서 바라보면 암호화된 파일의 경우, 컴퓨터 또는 정보저장매체에 저장된 암호화된 상태 그 파일 자체가 원본이라고 할 수 있다.



<그림 1> 암호화된 파일 압수[16]

그러나 압수하여 가져오는 데이터는 복호화된 전자정보로 기술적 측면에서는 복호화 전과 후의 데이터는 해시값도 다르고 파일의 형식도 다르기 때문에 원본성을 잃었다고 볼 수 있으나, 법적인 측면에서 내용이 동일하기 때문에 원본성을 잃지 않았다고 볼 수도 있게 된다. 이에 대해 형사소송법에서 증거조사 관련 대법원 형사소송규칙에 위임되어 있는바, 현

15) 이주호·이태명, (2020). 디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구.디지털포렌식연구. 252-268.
16) 이주호·이태명, (2020). 디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구.디지털포렌식연구. 252-268.

행 규칙 제134조의7 제1항에서 디지털증거의 제출방법에 대하여 '컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 기억된 문자정보를 증거자료로 하는 경우에는 읽을 수 있도록 출력하여 인증한 등본을 낼 수 있다'고 규정하여 원본성의 문제를 입법적으로 해결하고 있다.[17]

2-4. 신뢰성(Reliability)

대법원 2007. 12. 13. 선고 2007도7257 판결('일심회 사건')에서는 법원에 제출된 디지털증거의 증거능력을 인정받기 위해서는 동일성과 무결성을 그 요건으로 하고, 이를 담보하기 위해서 디지털포렌식 전문가에 의한 신뢰성과 관련하여 디지털포렌식 프로그램인 도구와 절차상 방법의 신뢰성을 원론적 입장에서 밝히고 있다. 다만, 각종 판결에서 디지털포렌식 도구에 대한 신뢰성과 디지털포렌식 전문가에 대한 신뢰성 부분에 대해 위 판결문의 제1심[서울중앙지방법원 2007. 4. 16. 선고 2006고합1365, 1363, 1364, 1366, 1367(각 병합) 판결]에서 EnCase 프로그램을 이용한 검증 절차가 적절한 방법으로 진행된 점 등을 들어 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력, 처리, 출력 각 단계에서의 정확성, 조작자의 전문적 기술능력 등 요건이 구비되었다고 설시하고 있을 뿐 신뢰성에 관해 직접적으로 판단한 사례는 없는 것으로 보인다.[18]

2-5. 관리 연속성(Chain of Custody)

관리 연속성이란 수사기관이 증거를 획득하고 법원에 제출되기까지 모든 관리 과정에서 어떠한 변화 없이 동일하다는 것을 의미한다. 디지털증거의 발견 방법과 처리 방법을 비롯하여 증거와 관련된 모든 사항을 명확히 기술하고 보관·이송 과정에서 인수인계 과정에 대한 기록과 검증이 필요하다. 관리 연속성을 유지하기 위해서는 증거를 발견하고 수집한 사람,

17) 이주호·이태명, (2020). 디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구.디지털포렌식연구. 252-268.
18) 손지영·김주석, (2015). "디지털 증거의 증거능력 판단에 관한 연구", 사법정책연구원, 35-36.

장소, 시간 증거를 취급하고, 조사한 사람, 장소, 시간 증거를 보관하는 사람, 보관 기간, 보관 방식·증거 관리가 변경되었을 때의 이송 방법과 날짜를 기록하는 방법 등이 있다.[19]

관리 연속성을 유지하기 위해서는 증거를 발견하고 수집한 사람·장소·시간·증거를 취급하고 조사한 사람 장소·시간, 증거를 보관하는 사람·보관 기관·보관 방식·증거 관리가 변경되었을 때의 이송 방법과 날짜를 철저히 기록하여 수집된 증거가 적법한 절차에 의해 관리된 증거임을 증명하여 증거능력을 확보하고자 하는 데 그 의미를 갖고 있다. 디지털증거는 물질이 아닌 데이터로서 존재하여, 근본적으로 일반 증거물과는 다른 특성을 지니고 있기 때문에 앞에서 언급한 것을 유의하여 전문가에 의한 특별한 수집·보관·관리가 이루어져야 한다.

3. 디지털포렌식의 정의 및 수집·분석 절차

3-1. 디지털포렌식 정의

디지털증거를 수집・분석하는 과정을 디지털포렌식이라고 하는데 Forensic Magazine(Ken Zatyko, 2007)에서 디지털포렌식을 “적법한 탐색 권한·관리 연속성·수리학적 평가·신뢰있는 도구의 사용·재현 가능성·전문 프레젠테이션이 가능케 하여 디지털증거에 대한 분석이 수반된 컴퓨터공학이 응용된 법적 조사 절차이다”라고 정의하였다.[20]

---

19) 이정인, (2019). ‘디지털증거의 관리연속성과 적법절차의 원리에 관한 연구, 서울대학교 석사학위 논문, 27.

20) Zatyko, Ken; “Commentary: Defining Digital Forensics,” Forensic Magazine, 2 January 2007, www.forensicmag.com/articles/2007/01/commentary-defining-digital-forensics

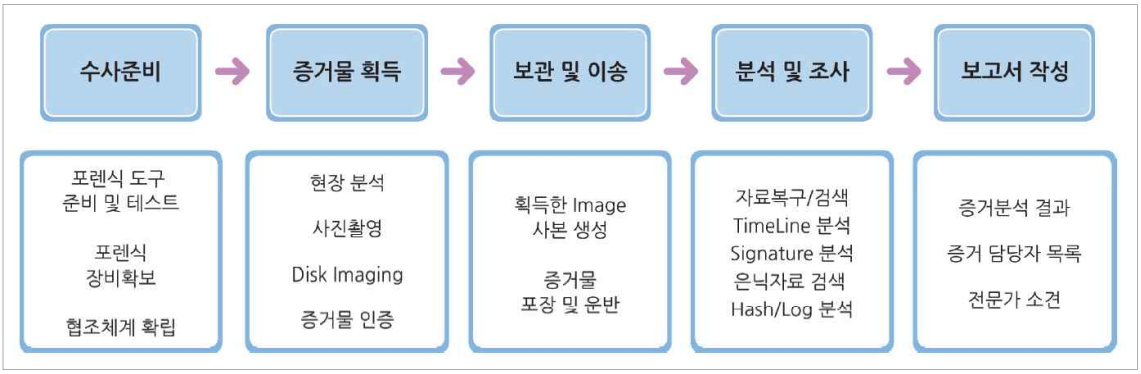
“The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation” (Ken Zatyko, 2007)

<표 5> 디지털포렌식 정의

디지털 데이터가 법정에서 유효한 증거로 인정받기 위해서는 적법한 절차를 거쳐 과학적인 방법으로 데이터를 수집·분석하고 그에 대한 검증과정이 수반되어야 하는데, 이러한 방식으로 각종 디지털 데이터를 조사하여 사건을 규명하는 법과학 분야를 디지털포렌식(Digital Forensic)이라고 한다. 즉 디지털포렌식이란 재판에 사용하기 위해 과학적 기술과 방법으로 디지털 데이터를 수집 → 보존 → 분석 → 보고서 작성 → 증거로 제출하는 행위를 의미하며, 수집·보존·분석되는 디지털 정보기기의 종류에 따라 컴퓨터포렌식, 모바일포렌식, 데이터베이스포렌식 등으로 나뉜다.

3-2. 디지털증거물 수집 및 분석 절차

디지털증거의 수집에서 그 분석하는 과정은 수사준비 → 증거물 획득 → 보관 및 이송 → 분석 및 조사 → 보고서 작성이라는 5단계로 구성된다.



<그림 2> 디지털포렌식 5단계 절차[21]

(1) 수사준비 : 증거 수집과 분석에 관한 계획을 수립하고, 대상 컴퓨터 시스템과 네트워크 현황 등에 관한 정보를 최대한 수집하며, 필요한 경우 관련 분야 전문가의 도움을 받을 수 있도록 한다.

(2) 증거물 획득 : 압수 현장에 있는 컴퓨터 하드웨어, 소프트웨어, USB메모리와 같은 이동식 휴대용 저장매체 등을 키워드를 입력해서 데이터를 선별해 증거물을 획득한다. 선별이 불가능할 경우 매체를 봉인해 획득한다.

(3) 보관 및 이송 : 정보저장매체 등이 물리적인 충격이나 정전기/자기장 전자파 등의 영향을 받지 않도록 주의하고, 증거물 보관실에는 증거물 원본과 사본, 분석 결과물 등을 보존한다.

(4) 분석 및 조사 : 선별된 디지털증거를 이미징하고, 이때 이미징한 사본은 훼손되지 않도록 하며, 해시값을 작성하여 원본과 사본의 동일성을 검증해야 한다.

(5) 보고서 작성 : 객관적 사실과 설명 내용, 분석자의 의견을 구분하여 작성하며, 분석자와 분석 일시, 분석에 사용한 시스템과 도구, 분석 방법 및 분석 결과를 명확하게 기록한다.

---

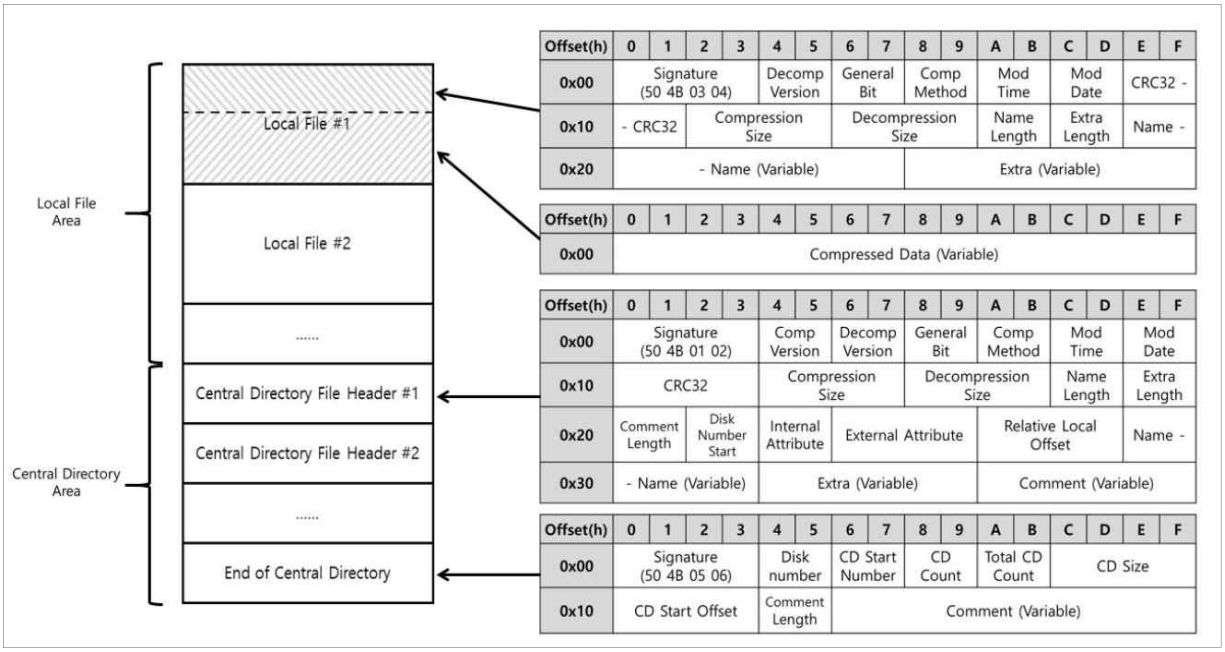
21) 손지영·김주석, (2015). 디지털 증거의 증거능력 판단에 관한 연구, 대법원 사법정책연구원, 46.

4. 디지털증거의 생성

4-1. 압축 파일에 의한 디지털증거 생성

4-1-1. ZIP 파일 구조[22)]

ZIP 파일은 크게 로컬파일(LF) 영역, 센트럴 디렉터리(CD) 영역으로 구분할 수 있다.



<그림 3> ZIP File Format

- 로컬파일(LF) 영역의 구조

로컬 파일 영역은 1개 이상의 로컬 파일로 구성되며, 로컬 파일의 개수는 ZIP파일을 만들 때 사용된 파일의 개수에 의해 결정된다. 로컬 파일은 압축된 파일의 압축 정보와 같은 메타데이터를 저장하고 있는 헤더영역과 Deflate 압축 알고리즘으로 압축된 데이터를 저장하고 있는 데이터 영역으로 구분된다. 로컬 파일의 헤더 영역의 경우 시그니처(Signature)부터 추가설명 길이(Extra length)까지는 0x1E (10진법:

22) 정병준·한재혁·이상진, (2017). 손상된 ZIP 파일 복구 기법, 고려대학교 정보보호대학원, 1109-1110.

30)의 고정된 크기를 가지고 이름(name)과 추가설명(Extra) 부분만 가변적인 길이를 갖는다. 로컬 파일의 데이터 영역의 경우 헤더 바로 뒤에 이어서 나오는 영역으로 압축된 데이터(Compressed Data)가 있다. 이 압축된 데이터는 4GB 미만의 가변크기로 저장된다.

- 센트럴 디렉터리(CD) 영역의 구조

센트럴 디렉터리 영역은 로컬 파일 영역의 뒤에 위치하며, 로컬 파일의 개수와 동일한 개수의 센트럴 디렉터리 파일 헤더와 1개의 엔드 오브 센트럴 디렉터리(EOCD)로 구성되어 있다. 센트럴 디렉터리 파일 헤더들은 로컬 파일들과 일대일로 쌍을 이루고 있고, 각 내부에는 쌍을 이루는 로컬 파일의 위치와 로컬 파일이 저장하고 있는 메타데이터[23]를 포함한 정보를 저장하고 있다. 센트럴 디렉터리 파일 헤더는 시그니처부터 상대 로컬파일 주소까지는 0x2E(10진수: 46)의 고정된 크기를 가지고, 그 뒤에 가변적인 길이의 이름과 추가설명, 주석(Comment)을 갖는다. ZIP파일의 가장 마지막에 위치한 엔드 오브 센트럴 디렉터리에는 압축된 파일의 수, 센트럴 디렉터리영역의 시작 위치 등의 ZIP파일의 메타데이터를 저장하고 있다. 해당 영역은 시그니처부터 주석 길이(Comment Length)까지는 0x16(10진법: 19)의 고정된 크기를 갖고, 가변크기의 주석으로 구성되어 있다.

---

23) 메타데이터(metadata)는 데이터에 관한 구조화된 데이터로, 다른 데이터를 설명해 주는 데이터이다. 여기에는 콘텐츠의 위치와 내용, 작성자에 관한 정보, 권리 조건, 이용 조건, 이용 내력 등이 기록되어 있다. 컴퓨터에서는 보통 메타데이터를 데이터를 표현하기 위한 목적과 데이터를 빨리 찾기 위한 목적으로 사용하고 있다.[네이버 지식백과] 메타데이터 [metadata](두산백과 두피디아, 두산백과)

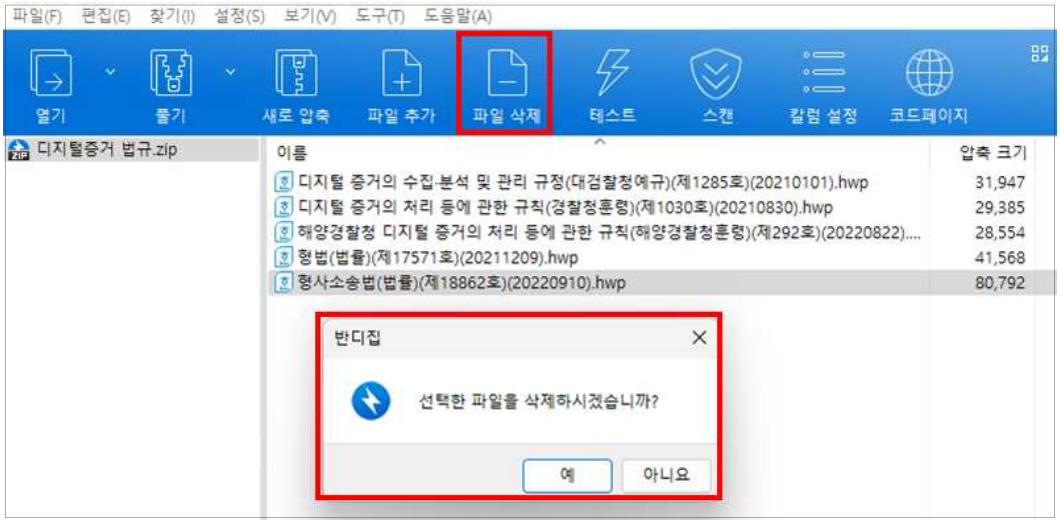
4-1-2. 압축 파일 내부의 메타데이터 보존

경찰의 정보저장매체에 대한 압수·수색 후 압수된 전자정보의 실무상 보관 방법은 일반적으로 압축 파일을 택하고 있다. 가장 많이 사용하는 압축 파일은 PKZIP 형식의 ZIP 확장자 파일이다. ZIP 파일 내부의 압축된 전자정보 파일의 메타데이터에는 파일명, 압축 크기(파일 사이즈), 원본 크기, 파일 종류, 수정한 날짜(Modification), CRC정보, 압축 방식, 암호 설명, 속성정보(Read-only, Hidden), 파일 설명, 부가 정보로 구성된다.

<그림 4> ZIP 압축 파일의 메타데이터 정보

4-1-3. 압축 파일 내부 파일 편집

ZIP 파일의 특징은 압축 파일 내부에 저장된 특정 파일에 대한 삭제 등 편집・조작이 가능하다는 점이다.

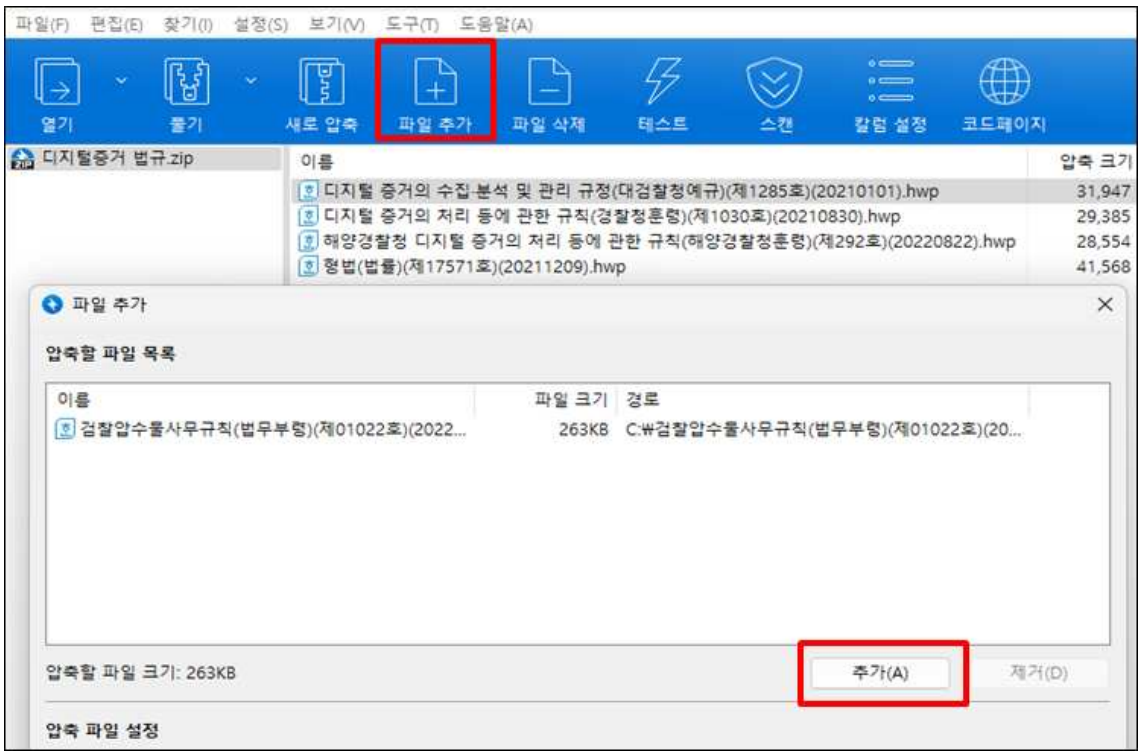


<그림 5> 형사소송법(법률)(제18862호)(20220910).hwp 파일을 삭제하는 모습

위 ZIP 압축 파일에서 특정 파일 [형사소송법(법률)(제18862호)(20220910) .hwp]을 삭제하는 기능을 실행하면, 다음 그림과 같이 파일이 삭제되는 것을 확인할 수 있다.

<그림 6> 형사소송법(법률)(제18862호)(20220910).hwp 파일이 삭제된 모습

ZIP 압축 파일에서 특정 파일[검찰압수물사무규칙(법무부령)(제01022호)(20220207).hwp]을 추가하는 기능을 실행하면, 다음 그림과 같이 압축 파일 내부에 파일이 추가되는 모습을 확인할 수 있다.



<그림 7> 검찰압수물사무규칙(법무부령)(제01022호)(20220207).hwp 파일 추가

위 그림은 ZIP 파일 내부에서 파일 추가 기능을 실행하여 파일을 추가하여 편집하는 모습이고, 아래 그림은 별도 재압축 과정 없이도 압축 파일 내부에서 파일 추가가 완료된 모습이다.

<그림 8> 검찰압수물사무규칙(법무부령)(제01022호)(20220207).hwp 추가 완료

위와 같이 ZIP 형태 등 압축 파일에서는 압축 파일 내부에 보관된 전자정보의 추가·삭제 등 인위적인 편집이 가능하다는 특징이 있다.

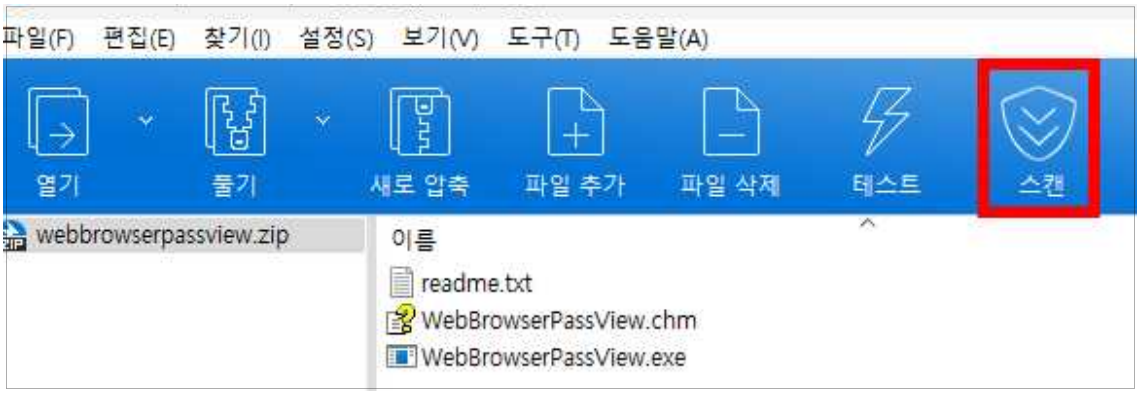
4-1-4. 악성코드 노출의 위험성

압축 파일은 악성코드, 바이러스, 랜섬웨어에 노출되어 있다. 인위적인 편집이 가능하기에 압축 파일 내부에 보관된 전자정보 중 일부는 악성코드 등에 감염되어 디지털증거의 무결성을 담보하기가 어려울 수 있다.

<그림 9> 압축 파일 내부 파일이 악성코드에 의해 차단된 모습

디지털증거는 수집 당시 내용 및 메타데이터를 그대로 유지되어야 그 증거능력이 인정될 수 있고, 이는 복제 당시 해시값과 공판 과정에서 그 전자정보의 해시값의 비교를 통해 임의적 증거 변경이 있었는지 여부를 확인하게 된다. 증거 보관 또는 증거 검토 과정에서 다양한 수사 상황에 노출되므로 악성코드 등에 증거가 오염되는 상황은 무결성 확보에 도움이 되지 않는다.

또한 디지털증거는 문서, 그림 등이 다수를 이루나 위 그림과 같이 실행프로그램이나 설정 파일 등이 그 대상일 수도 있다. 압축 파일 내부에 토로이언 악성코드가 발견되어 윈도우 운영체제의 바이러스 및 위협방지 시스템 설정과 V3 백신 앱에서 이를 발견하고 그 파일이 삭제될 경우 증거는 흔적도 없이 사라질 것이다. 압축 파일 내부 파일들이 변경될 가능성은 압축 파일 응용프로그램에서 확인할 수 있다.



<그림 10> 반디집에서 악성코드 스캔 기능

현재 가장 많이 사용되고 있는 압축 파일 프로그램인 알집(Alzip), 반디집(Bandizip)에서는 악성코드 등을 스캔해서 감염되었을 경우 이를 치료하는 기능이 제공된다. 압축 파일 응용프로그램에서 스캔 기능을 이용하여 악성코드 등을 치료하면 오염된 파일 자체를 삭제하는 경우도 있고, 단순히 악성코드 자체만 제거하는 경우가 있을 수 있다. 오염된 파일을 삭제하면 증거는 흔적도 없이 사라지는 것이고, 악성코드를 제거하는 방법으로 치료한다면 전자정보 내용이 1비트라도 바뀌게 될 것이고, 결국 압축 파일의 해시값이 변경될 것이다. 이는 해시값이 변경되어 공판 과정에서 아무리 결정적인 디지털증거를 제시되었다고 하더라도 증거능력 요건에 쟁점이 될 수 있고, 결국 디지털증거의 무결성이 깨져서 증거의 신뢰성에 위협이 될 수도 있을 것이다.

4-1-5. 최초 획득 복제한 디지털증거 복원의 한계

압축 파일 응용프로그램을 이용해서 쉽게 전자정보를 검토할 수 있으나 디지털증거 수집 당시의 메타데이터를 복원하기 어려워, 증거능력에 대한 법정 공방 시 검증 및 재현에 한계가 있게 된다. 예를 들어, 위에서 살핀 바와 같이 악성코드에 감염된 파일이 임의로 삭제된 파일이 있을 수 있고, 파일의 수정・변경・접근 일시가 쟁점이 될 수도 있으며, 압수 당시의 파일시스템 환경을 구현해서 특정 매크로 프로그램을 시현할 필요가 있을 수 있다. 압축 파일은 보관의 안정성에 문제가 있고, 메타데이터 복원에도 한계가 있기 때문에 최초 획득 복제한 디지털증거로의 복원에도 한계가 있는 것으로 정리된다.

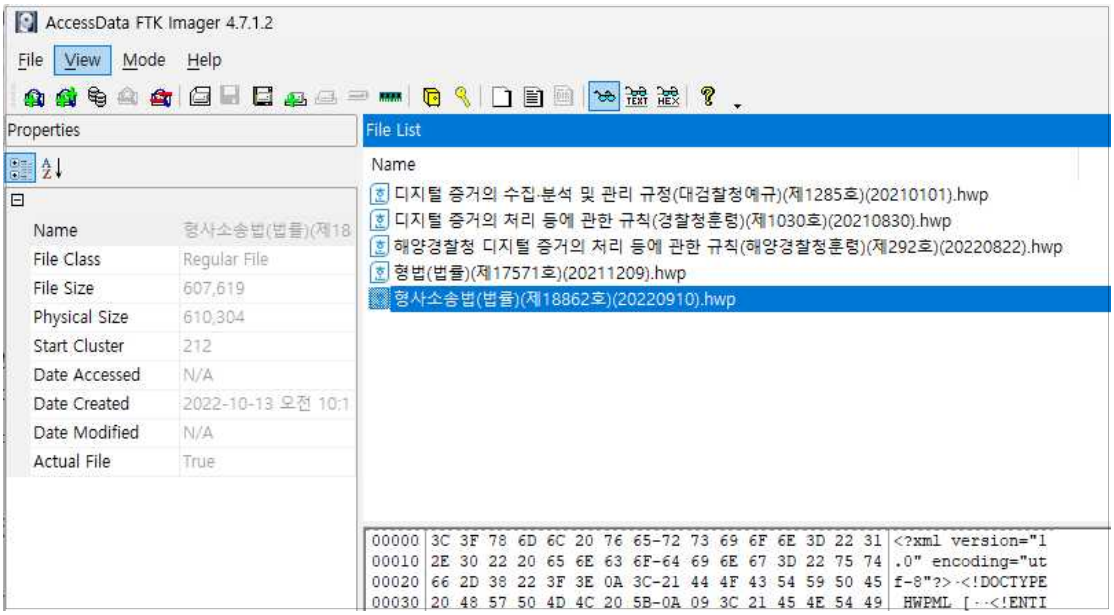
이와 같은 점을 정리하면, 압축 파일은 디지털증거를 보관하기에 ①압축 파일 내부에 보관된 파일의 인위적 개작·편집의 가능성, ②악성코드 및 바이러스 등에 노출의 위험성, ③메타데이터 복원의 한계, ④압수 당시 파일시스템 등 재현 및 검증의 제한에 문제가 있다고 봄이 타당하다.

4-2. 포렌식 이미지에 의한 디지털증거 생성

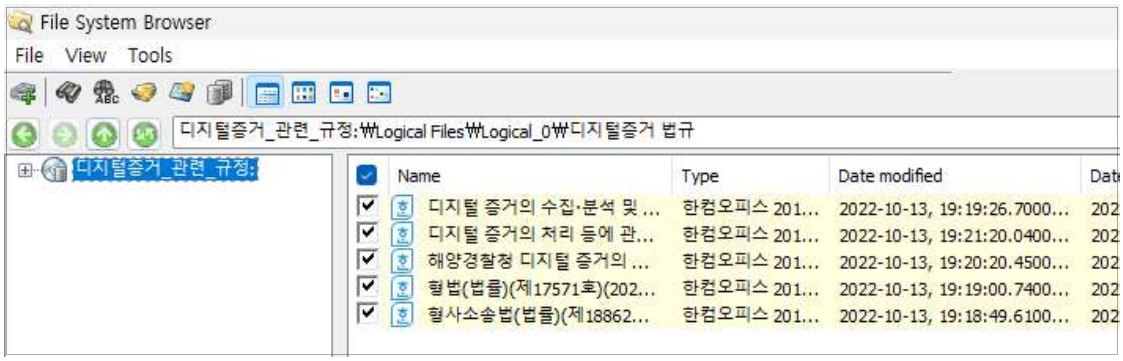
4-2-1. 포렌식 이미지 특징 및 구조

원본 디스크 이미지를 만들기 위해 가장 오랜 기간 무료로 사용된 도구는 UNIX DD유틸리티이다. DD는 Disk Dump의 약어로써 리눅스, BSD, macOS, Unix체계 운영체제에서 제공되는 무료 프로그램으로 디스크 전체, 파티션, 파일 일부 등을 대상으로 일정한 파일시스템을 구성하여 디스크 각 섹터를 비트단위까지 압축하여 저장하는 과정없이 로우레벨(Raw level) 복제를 진행하기 때문에 원본 디스크와 사본 DD이미지가 완전히 동일한 형태의 이미지를 생성하게 된다. 또한 위 운영체제에서 오픈소스 형식으로 무료 제공되고 있으므로 대다수의 디지털포렌식 분석툴에서 기본으로 제공되는 기능으로 사용되고 있다. 이러한 이유로 DD 이미지는 다양한 파일시스템 및 각종 분석툴에서 호환성이 매우 뛰어나며, 이미지 생성 당시 원본 전자정보의 메타데이터까지 완전히 동일하게 복제하기 때문에 실무상 DD 형식의 이미지 파일이 적절히 관리된다는 조건하에 무결성을 담보하고 있는 것으로 본다.

포렌식 이미지 중 DD 이미지 파일에 보관된 전자정보의 메타데이터에는 파일명, 파일 종류, 파일 크기, Modification·Created·Accessed time, 파일 속성 정보(Read-only, Hidden) 등의 정보가 저장되고 이미지 생성 이후에 이미지 내부에 보관된 전자정보를 추출하더라도 이미지 생성 당시 그대로의 메타데이터가 유지된 상태에서 이를 복원하여 추출할 수 있다.

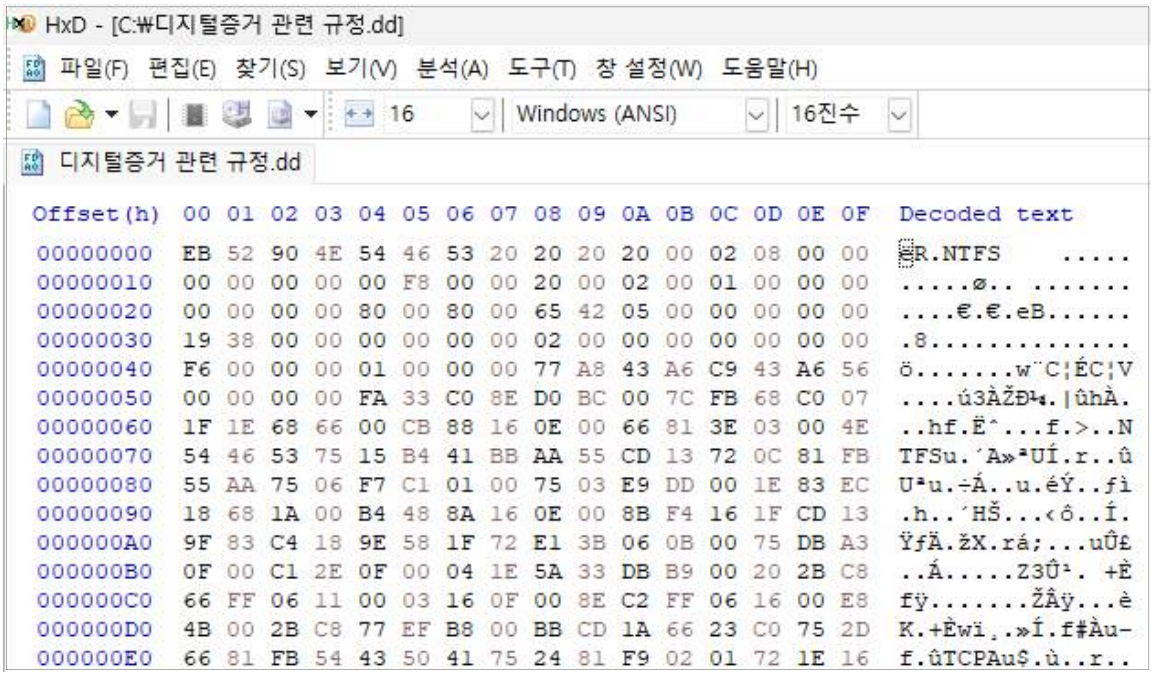


<그림 11> FTK Imager 툴에서 DD 이미지 속성 정보 모습



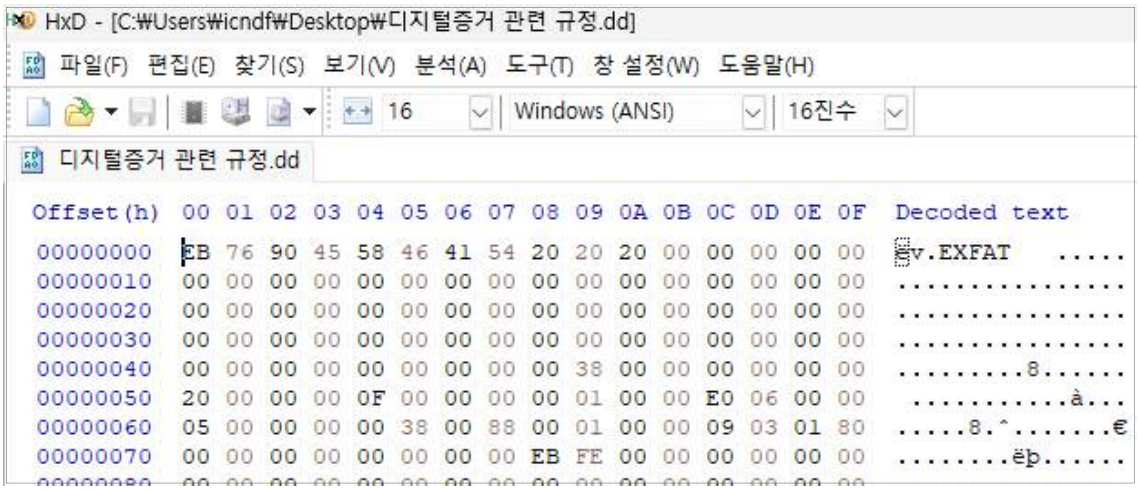
<그림 12> OSForensics 툴에서 DD 이미지 속성 정보 모습

DD 이미지 파일에 대한 구조는 파일시스템 구조별로 다르다. 예를 들어, 다음과 같이 NTFS 파일시스템으로 저장된 DD 이미지 파일의 시그니처 등을 보면, NTFS 파일시스템 구조와 일치한다.



<그림 13> NTFS 파일시스템으로 저장된 DD 이미지 구조

위 NTFS 파일시스템 DD Raw Image에 저장된 파일을 exFAT 파일시스템으로 작성하면 exFAT 파일시스템 구조와 일치한다.



<그림 14> exFAT 파일시스템으로 저장된 DD 이미지 구조

4-2-2. DD 이미지 생성 명령어

```
dd if=/dev/sdc1 of=/dev/sdd1 bs=128K conv=noerror,sync
```

<그림 15> DD 디스크 이미지를 만드는 명령어 예시

리눅스에서 DD 디스크 이미지를 만드는 명령어를 위와 같이 제시하였다. 이는 디지털포렌식 분석 툴에서 디지털증거를 선별하고 최종적으로 수집할 전자정보를 대상으로 이미지를 생성의 방법으로 획득 시 사용할 수 있다. Windows 또는 MacOS에서는 여러 유료 분석 툴이 있기에 이러한 툴을 사용해서 선별하고 이를 이미징하면 되지만, 리눅스에서는 그리 많은 툴이 제공되지 않으므로 운영체제 단위에서 제공되는 DD 명령어를 이용한다면 별도 분석 툴이 없이도 이미징할 수 있게 된다. 여기서 이미징한다는 것은 선별하여 압수의 대상이 되는 정보저장매체 등에 저장된 전자정보를 포렌식 도구를 사용하여 비트열 방식으로 동일하게 복사하여 '포렌식 이미지'를 생성하는 것을 말하는데, 이렇게 생성된 포렌식 이미지는 하나의 파일시스템을 구성하여 비록 파일 1개에 불과한 파일이지만 하나의 하드디스크 드라이브 같은 역할을 하게 되고 메타데이터까지 그대로 복제되므로 이미지 파일에 데이터를 안정적으로 보관이 가능하고 향후 이를 재분석하고 재현・검증에도 유리하다.

위에서 사용한 DD 이미지 생성 명령어를 살펴보면, 먼저 DD 프로그램을 실행할 수 있는 dd를 입력하고, 이후에는 원본 즉, 입력이 되는 데이터를 정하고, 다음으로 복제본 즉, 출력이 될 이미지 파일명을 입력한다. 더불어 하나의 파일시스템을 구성하므로 개별 블록 크기(64KB)를 정하여 이미지를 생성한다. 세부 옵션 내역은 'if=/dev/file'는 입력이 되는 디바이스 파일, 'of=/dev/file'는 출력이 되어 생성되는 이미지 파일, 'bs=64k'는 생성되는 디스크 이미지의 블록 크기를 64K로 설정한 것이고 128K 또는 다른 값으로 대체 가능하다. 'conv=noerror'는 모든 읽기 오류를 무시하고 작업을 수행, 'sync'는 읽기 오류 시 값을 00으로 채우라는 옵션이다.

4-2-3. 포렌식 이미지 생성의 법적 근거

대검찰청 예규 “디지털 증거의 수집·분석 및 관리 규정”에서 ″포렌식 이미지″(이하 ‘이미지 파일’이라고 한다)란 법률적으로 유효한 증거로 사용될 수 있도록 정보저장매체 등에 저장된 전자정보를 포렌식 도구를 사용하여 비트열 방식으로 동일하게 복사하여 생성한 파일로 규정한다. 이는 마치 ‘Image’라는 단어가 거울에 비친 형상과 동일한 모습으로 비치는 것처럼 컴퓨터의 이미지는 정보저장매체 간 데이터를 동일하게 복제하는 것을 의미한다고 볼 수 있다.

검찰 디지털포렌식 실무상 정보저장매체에 대한 압수·수색 후 압수된 전자정보는 일반적으로 DD 논리이미지 형식의 파일 1개를 작성하고 이에 대한 해시값을 생성하여 압수하는 방식을 취하고 있다. 이는 원본데이터로부터 압수한 전자정보 및 그 메타데이터까지 복제하여 원본데이터의 동일성을 유지하고 무결성을 담보하기 위한 하나의 방식으로 인정되고 있다.

4-2-4. 포렌식 이미지에 의한 디지털증거 보관 특징

포렌식 이미지는 exFAT, NTFS 등 파일시스템에 디지털증거를 비트(bit) 단위로 복제하여 이미지를 생성하고 이에 대한 해시값을 계산하여 동일성을 유지한 채 복제되었는지 검증하고 있다.

위와 같이 생성된 포렌식 이미지는 ①디지털포렌식 툴이 아니고서는 접근에 제한이 있고, ②일반적인 디지털포렌식 툴에서는 이미지 내부 파일을 임의로 편집할 수 없다. ③포렌식 이미지 내부에 있는 파일은 외부에서 악성코드 또는 바이러스로부터 안전하게 보호할 수 있고, 더불어 ④이미지 내부에 보관된 디지털증거를 압수 당시 기준으로 재현하여 복원할 때 디지털증거의 메타데이터까지 원본과 완전히 동일하게 복원이 가능하며 ⑤포렌식 이미지를 최초 디지털증거 수집 당시로부터 상당기간 경과한 이후에도 해시값 계산에 의한 검증으로 동일성과 무결성 담보를 위해 완전한 재현·검증이 가능하다는 장점이 있다.

이러한 특징은 디지털포렌식 절차에서 무결성·동일성·신뢰성·관리 연계성을 담보할 수 있는 장점을 지닌 포렌식 이미지를 가장 많이 사용하게 된 것이다.

제 3 절 디지털증거에 관한 법규정과 판례

1. 디지털증거에 관한 법규정

1-1. 형사소송법・대법원 형사소송규칙

형사소송법 및 대법원 형사소송규칙에서는 주로 피압수자의 디지털증거를 무분별하게 압수・수색하지 못하도록 제한을 규정함으로써 피압수자의 권리와 함께 법정 증거능력 및 증거조사 방법 등을 주로 규정하고 있다.

1) 형사소송법

법률에서 디지털증거를 어떻게 보느냐에 따라서 압수조서 및 압수목록의 기재방식이 달라진다. 디지털증거는 물리적 형상이 없어서 CD/DVD/USB메모리/HDD/SSD/SD카드 메모리 등의 정보저장매체로 기재할 수 있지만, 피압수 대상 정보저장매체에서 복제하는 방식으로 압수할 경우 기재 문구가 문제가 된다. 이는 디지털포렌식 분석관이 디지털증거를 생성하는 방식에 따라 그 차이가 있게 마련이다.

제49조(검증 등의 조서) ③압수조서에는 품종, 외형상의 특징과 수량을 기재하여야 한다.

<표 6> 형사소송법 제49조 압수목록상 디지털증거 관련 규정

실무상 검찰에서 압수・수색 영장 집행 과정에서 피압수자에게 교부하는 압수조서 및 압수목록에는 '홍길동의 업무용PC 선별 전자정보 논리이미지' 등 이미지 정보를 기재하고 있다. 경찰은 이와 달리 전자정보(압수물)의 파일명 및 해시값 정보가 포함된 '전자정보 확인서'를 교부하는 방식으로 압수목록을 교부하고 있다.

[별지 제1호 서식]

전자정보 확인서

※ 정보저장매체별 작성

수집종류	[ ] 임의제출 [ ] 압수·수색·검증영장 [ ] 기타			
일시 · 장소	*정보저장매체 원본 · 복제본 반출 후, 경찰관서에서 복제하는 경우 경찰관서 기재*			
정보저장 매체	품 명		모 델 명	
	일련번호		비 고	*시간오차 등*
전자정보 (압수물)	파 일 명	*피의자명_품명.zip*	해시종류	*SHA-1*
	해 시 값	*상세목록에 기재된 전자정보를 하나의 파일로 압축한 파일*		
	※ 전자정보 상세목록에서 제외된 전자정보는 삭제·폐기함			
상세목록	교부방법	[ ] 출력 [ ] 복사 [ ] 전송(e-mail :)		
	파 일 명	*상세목록 파일 정보*	해시종류	*SHA-1*
	해 시 값	*플해시 등으로 생성한 상세목록 파일의 해시값*		
피압수자 (제출자)	구 분 : [ ] 소지자, [ ] 소유자, [ ] 기타( ) 성 명 : 생년월일 : 연락처 :			
참여자	피압수자와의 관계 : *피압수자(제출자)와 참여자가 같은 경우 기재 생략* 성 명 : (인) 생년월일 : 연락처 :			

<그림 16> 경찰청 디지털증거 훈령상 '전자정보 확인서'

1-1) 디지털증거 압수 대상

형사소송법상 디지털증거에 대한 압수의 목적물을 '컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체'로 규정하고 있다. 따라서 디지털증거 압수·수색 시 압수의 목적물은 컴퓨터용 디스크 등 정보저장매체로 봄이 타당하다. 그러나 이는 물리적 형상일 때로 한정하고, 압수의 목적물이 파일 등 전자정보일 경우에는 추상적 형상이므로 물리적 형상을 기재하는 방법과 달리, 형사소송법 제49조에서 품종, 외형상의 특징을 기재해야 한다는 규정에 따라 물리이미지 또는 논리이미지로 기재하거나, 전자정보(압수물) 파일명으로 기재가 가능한 것이다.

1-2) 압수 3단계 원칙

제106조(압수) ③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 “정보저장매체등”이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다. <신설 2011. 7. 18.>

<표 7> 형사소송법 제106조 조문

형사소송법 제106조에서 규정한 바와 같이 디지털증거 압수는 사건과 관련 있는 전자정보에 대한 선별 압수를 원칙으로 하고, 예외적으로 전부 복제 또는 원본 반출 등을 명시하여 디지털증거에 대한 무분별한 압수를 제한하고 있음을 확인할 수 있다.

1-3) 불송치 자료는 열람·등사 대상

형사소송법 제266조의3에서 검사의 공소제기 후 피고인 등은 디지털증거에 대한 열람·등사가 가능함을 규정하여 피고인에 대한 증거개시 제도에 디지털증거를 포함하여 권리를 부여한 것으로 디지털증거 역시 사건관계인의 열람·등사의 대상이고, 이는 수사 중 사건의 열람·등사가 가능하고 경찰이 불송치 결정한 수사기록 역시 열람·등사의 대상이 될 수 있다.

제266조의3(공소제기 후 검사가 보관하고 있는 서류 등의 열람·등사) ①피고인 또는 변호인은 검사에게 공소제기된 사건에 관한 서류 또는 물건(이하 “서류등”이라 한다)의 목록과 공소사실의 인정 또는 양형에 영향을 미칠 수 있는 다음 서류등의 **열람·등사** 또는 서면의 교부를 신청할 수 있다. 다만, 피고인에게 변호인이 있는 경우에는 피고인은 열람만을 신청할 수 있다.
⑥제1항의 서류등은 도면·사진·녹음테이프·비디오테이프·**컴퓨터용 디스크**, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 특수매체를 포함한다. 이 경우 특수매체에 대한 등사는 필요 최소한의 범위에 한한다.
[본조신설 2007. 6. 1.]

<표 8> 형사소송법 제266조의3 조문

1-4) 디지털증거 증거능력 요건

제313조에서 성립의 진정함이 증명되고 특히 신빙할 수 있다는 조건하에 디지털증거의 증거능력이 있으나, 그럼에도 불구하고 디지털포렌식 분석으로 객관적 성립의 진정성이 인정된다면 특히 신빙할 수 있는 상태를 충족하지 않더라도 증거능력이 인정될 수 있다는 증거능력 요건을 규정한다.

제313조(진술서등) ①전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 **컴퓨터용디스크**, 그 밖에 이와 비슷한 **정보저장매체**에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 **성립의 진정함이 증명**된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 그 진술이 **특히 신빙할 수 있는 상태**하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다. <개정 2016. 5. 29.>

② **제1항 본문에도 불구하고** 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 **과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명**되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다. <개정 2016. 5. 29.>

<표 9> 형사소송법 제313조 조문

더불어 제314조에서는 법정 진술할 수 없는 경우에도 특히 신빙할 수 있는 상태하에 디지털증거는 증거능력이 있음을 규정한다.

제314조(증거능력에 대한 예외) 제312조 또는 제313조의 경우에 공판준비 또는 공판기일에 진술을 요하는 자가 사망·질병·외국거주·소재불명 그 밖에 이에 준하는 사유로 인하여 진술할 수 없는 때에는 그 조서 및 그 밖의 서류(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 **컴퓨터용디스크**, 그 밖에 이와 비슷한 **정보저장매체**에 저장된 것을 포함한다)를 증거로 할 수 있다. 다만, 그 진술 또는 작성이 **특히 신빙**할 수 있는 상태하에서 행하여졌음이 증명된 때에 한한다. <개정 2016. 5. 29.>[전문개정 2007. 6. 1.]

<표 10> 형사소송법 제314조 조문

2) 대법원 형사소송규칙

형사소송법 제292조의3에서는 (중략) 컴퓨터용디스크, 그 밖에 정보를 담기 위하여 만들어진 물건으로서 문서가 아닌 증거의 조사에 관하여 필요한 사항은 대법원규칙으로 정한다고 규정하여 디지털증거에 대한 증거조사 방식을 대법원 형사소송규칙에 위임하고 있다.

- 원본 동일성

특히, 형사소송규칙 제134조의7 제1항에서 '정보저장매체(다음부터 이 조문 안에서 이 모두를 "컴퓨터디스크 등"이라 한다)에 기억된 문자정보를 증거자료로 하는 경우에는 읽을 수 있도록 출력하여 인증한 등본을 낼 수 있다.'라고 하고 있는데 이는 원본의 카카오톡 메신저나 텔레그램 메신저의 데이터베이스를 복호화한 결과물이 기술적으로는 원본과 다르나 내용상으로는 원본과 동일성이 인정되므로 증거능력이 인정되는 근거 규정으로 볼 수 있다.[24]

일반적으로 수사기관에서 확보한 디지털증거는 수사보고 형식으로 증거가 되는 부분 또는 전부를 현출하여 이를 법정에서 가시적으로 볼 수 있도록 출력하여 증거로 제출하고 있다. 형사소송규칙 제134조의7에서는 원

24) 이주호·이태명, (2020). 디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구.디지털포렌식연구, 14(3), 252-268.

본과 동일성이 인정되는 디지털증거를 서면으로 출력하여 이를 증거로 제출하고 법정 증거조사를 할 수 있도록 한 근거 규정이 된다.

제134조의8(음성·영상자료 등에 대한 증거조사)에서는 소위 디지털증거 중 멀티미디어(영상 또는 음성) 파일에 대한 증거조사 방법을 규정한 것으로서 제2항은 영상 또는 음성의 녹취 내용 등을 서면으로 제출하고, 제3항에서 멀티미디어 디지털증거에 대해 '녹음·녹화매체 등에 대한 증거조사는 녹음·녹화매체 등을 재생하여 청취 또는 시청하는 방법으로 한다.'라고 규정하여, 멀티미디어 증거는 법정에서 재생하여 시각적·청각적 방식에 의한 증거조사 원칙을 제시하였다.

3) 대통령령「검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정」

대통령령인 수사준칙에서는 법률에서 압수·수색·검증영장 집행을 명시한 형사소송법 제106조를 디지털증거 압수·수색 대상을 범죄사실 관련성의 3단계 원칙(선별 → 전부 복제 반출 → 원본 반출)으로 규정하고, 압수한 디지털증거에 대한 전자정보 상세목록 교부, 목록에 없는 전자정보 삭제·폐기, 피압수자 및 변호인의 압수·수색 참여권 보장, 관련성에 대한 의견진술권, 압수한 디지털증거에 대한 해시값 생성 및 압수 과정 영상 촬영 등으로 디지털증거의 동일성, 무결성 등을 보장하는 내용을 규정하였다.

대통령령인 수사준칙 제41조(전자정보의 압수·수색 또는 검증 방법)에서는 주로 법원의 디지털증거 관련 판례를 반영하여 이를 대통령령으로 규정한 것으로, 디지털증거의 압수를 3단계로 정의한 것이다. 범죄사실과 관련된 디지털증거를 ①선별하여 압수함을 원칙으로 하되, ②압수가 불가능하거나 현저히 곤란한 경우에 전부 복제하여 이를 반출할 수 있고, ③이 역시 불가능할 경우에는 원본 자체를 봉인하여 압수할 수 있음을 규정하였다.

제42조(전자정보의 압수·수색 또는 검증 시 유의사항)에서는 피압수자에게 압수가 종결된 이후 해시값이 포함된 전자정보 상세목록을 교부하면서 이에 포함되지 않은 전자정보를 삭제·폐기하는 근거조항이다. 또한 전자정보 복제 시 해시값을 확인하고, 피압수자 등에게 참여권을 보장하여 전자정보의 사건 관련성에 대한 의견을 제시할 경우 이를 조서에 기재해야 한다. 피압수자 등이 참여 거부 시 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 수행하도록 규정하고 있다.

4) 규칙·예규·훈령

법무부 규칙·행정안전부 규칙, 대검찰청 예규, 경찰청 훈령 등에서는 형사소송법·대법원 형사소송규칙·대통령령 수사준칙 등에서 규정한 피의자 등의 권리와 증거능력에 관한 디지털포렌식 기술적, 수사, 형사 절차에 대한 적법 절차적 내용을 가장 세부적으로 규정하여 디지털포렌식 분석관과 수사관이 상황별로 따라야 할 가장 기본이 되는 원칙을 명시하고 있다.

(1) 대검찰청 예규「디지털 증거의 수집·분석 및 관리 규정」

대검찰청 디지털증거 예규 제3조에서는 디지털포렌식에서 사용하는 전문용어를 정의한다. 이는 주로 학계에서 일반적으로 인정되는 용어로 정의하여 디지털증거 규정의 이해를 돕는 역할을 한다고 볼 수 있다.

수사준칙과 예규, 훈령 등에서 자주 언급되는 용어에 대한 정의를 보면, ①"전자정보"란 정보저장매체등에 기억된 정보를 말한다, ②"디지털증거"란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다, ③"디지털포렌식"이란 디지털 증거를 수집·보존·분석·현출하는 데 적용되는 과학기술 및 절차를 말한다, ④"디지털수사통합업무관리시스템"(이하 '업무관리시스템'이라고 한다)이란 디지털 증거의 수집·분석에 관한 사항과 디지털 증거의 보관·폐기에 관한 이력 등을 관리하는 전산시스템을 말하며, 이는 검찰 실무상 D-NET (Digital Evidence Network)이라 일컫는다, ⑤"정보저장매체등의 복제"란 법률적으

로 유효한 증거로 사용될 수 있도록 수집 대상 정보저장매체등에 저장된 전자정보를 동일하게 파일로 생성하거나, 다른 정보저장매체에 동일하게 저장하는 것을 말한다, ⑥"포렌식 이미지"(이하 '이미지 파일'이라고 한다)란 법률적으로 유효한 증거로 사용될 수 있도록 정보저장매체 등에 저장된 전자정보를 포렌식 도구를 사용하여 비트열 방식으로 동일하게 복사하여 생성한 파일을 말한다, ⑦"증거파일"이란 법률적으로 유효한 증거로 사용될 수 있도록 정보저장매체 등에 저장된 전자정보를 파일 또는 디렉터리 단위로 복사하여 생성한 파일을 말한다고 정의한다.

제4조(적법절차의 준수)에서는 디지털증거는 쉽게 변조할 수 있다는 취약성이 있다는 특징을 고려하여 디지털증거 수집 및 분석의 기본 원칙을 규정한 것으로서 '디지털 증거는 수사에 필요한 범위 내에서 적법한 절차를 엄격히 준수하여 수집·분석 및 관리되어야 한다.'고 규정하고 제5조부터 제8조까지는 각각, 제5조 '원본과의 동일성을 재현하거나 검증하는데 지장이 초래되지 않도록 수집·분석 및 관리되어야 한다', 제6조 '디지털증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다', 제7조 '디지털증거는 디지털포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집·분석 및 관리하여야 한다', 제8조 '최초 수집된 상태 그대로 어떠한 변경도 없이 보관되어야 하고, 이를 위해 보관 주체들 간의 연속적인 승계 절차를 관리하는 등의 조치를 취해야 한다'고 하여 학계에서 인정되고 있는 디지털증거 특징(원본성·동일성·무결성·신뢰성·보관 연속성)을 그대로 반영하여 규정하였다.

특히 대법원 판례에서는 "정보저장매체에 저장된 문건 또는 그로부터 출력된 문건을 증거로 사용하기 위해서는 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 수집(압수)시부터 문건 출력 시까지 변경되지 않았음(무결성)이 담보되어야 한다"고 판시하면서 디지털증거의 무결성 특징을 직접적으로 언급하고 있다.[25]

대법원 판례에서는 영장 발부의 사유로 된 범죄 혐의사실과 무관한 별개의 증거를 압수하였을 경우 이는 원칙적으로 유죄 인정의 증거로 사용할 수 없다. 그러나 압수·수색의 목적이 된 범죄나 이와 관련된 범죄의 경우에는 그 압수·수색의 결과를 유죄의 증거로 사용할 수 있다.
압수·수색영장의 범죄 혐의사실과 관계있는 범죄라는 것은 압수·수색영장에 기재한 혐의사실과 객관적 관련성이 있고 압수·수색영장 대상자와 피의자 사이에 인적 관련성이 있는 범죄를 의미한다. 그중 혐의사실과의 객관적 관련성은 압수·수색영장에 기재된 혐의사실 자체 또는 그와 기본적 사실관계가 동일한 범행과 직접 관련되어 있는 경우는 물론 범행 동기와 경위, 범행 수단과 방법, 범행 시간과 장소 등을 증명하기 위한 간접증거나 정황증거 등으로 사용될 수 있는 경우에도 인정될 수 있다. 이러한 객관적 관련성은 압수·수색영장에 기재된 혐의사실의 내용과 수사의 대상, 수사 경위 등을 종합하여 구체적·개별적 연관관계가 있는 경우에만 인정된다고 보아야 하고, 혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로 객관적 관련성이 있다고 할 것은 아니라고 판시하고 있다.[26]

대법원 판례는 객관적·인적 관련성을 기준으로 영장기재 범죄사실과 디지털증거의 관련성을 판단한다. 이에 대검찰청 디지털증거 예규 제22조(관련성의 판단기준)에서는 대법원 판례에서 판시한 내용에 더해 관련성의 범위를 압수·수색 당시를 기준으로 범죄혐의에 대한 기본적 사실 관계, 동종 유사 범행 또는 정황, 공범 등 인적 관련성, 범행의 동기·목적·양형사유 등 객관적, 인적 관련성을 포함한 디지털증거 뿐만 아니라, 법정에서 디지털증거에 대한 재현·검증·출처증명·정확성 및 신뢰성 입증(아티팩트 등) 등을 포함한 내용까지 압수할 수 있다고 규정하였다. 이는 실무상 영장 기재 범죄사실 뿐만 아니라, 컴퓨터 등 정보저장매체를 사용하면서 시스템상 자동으로 생성되는 시스템 로그파일, USB메모리 등 사용기록, 인터넷 사용 및 검색 내역 등 아티팩트 정보 등이 포함된 디지털증거를 압수할 수 있다는 기술적 내용을 추가하여 기재한 것이다.

---

25) 대법원 2013. 6. 13. 2012도16001 판결
26) 대법원 2017. 1. 25. 선고 2016도13489 판결, 대법원 2017. 12. 5. 선고 2017도13458 판결, 대법원 2020. 2. 13. 선고 2019도14341, 2019전도130 판결

제25조(임의 제출 정보저장매체등에 대한 조치) ① 전자정보가 저장된 정보저장매체등을 임의제출 받는 경우에는 임의제출의 취지와 범위를 확인하여야 한다.

② 정보저장매체등에 저장된 전자정보를 임의 제출하는 것으로서 전자정보에 대한 탐색·복제·출력이 필요한 경우에는 본 장에서 규정한 절차를 준용한다.

<표 11> 대검찰청 디지털증거 예규 제25조 임의제출 규정

제25조(임의 제출 정보저장매체등에 대한 조치)에서는 임의제출에 대해서 규정하고 있는데 이는 대법원 판례에 의하면, 임의제출 역시 압수·수색·검증 절차와 동일한 절차에 의해야 하고, 따라서 수사기관이 전자정보를 담은 매체를 피의자로부터 임의제출 받아 압수하면서 거기에 담긴 정보 중 무엇을 제출하는지 명확히 확인하지 않은 경우, 임의제출의 동기가 된 범죄혐의 사실과 관련되고 이를 증명할 수 있는 최소한의 가치가 있는 정보여야 압수의 대상이 되는데, 범행 동기와 경위, 수단과 방법, 시간과 장소 등에 관한 간접증거나 정황증거로 사용될 수 있는 정보도 그에 포함될 수 있다. 수사기관이 피의자로부터 범죄혐의 사실과 관련된 전자정보와 그렇지 않은 전자정보가 섞인 매체를 임의제출 받아 사무실 등지에서 정보를 탐색·복제·출력하는 경우 피의자나 변호인에게 참여의 기회를 보장하고 압수된 전자정보가 특정된 목록을 교부해야 하나, 그러한 조치를 하지 않았더라도 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피의자의 절차상 권리가 실질적으로 침해되지 않았다면 압수·수색이 위법하다고 볼 것은 아니라고 판시하였다.[27]

다른 대법원 판례에서는 헌법과 형사소송법이 구현하고자 하는 적법절차, 영장주의, 비례의 원칙은 물론, 사생활의 비밀과 자유, 정보에 대한 자기결정권 및 재산권의 보호라는 관점에서 정보저장매체 내 전자정보가 가지는 중요성에 비추어 볼 때, 정보저장매체를 임의제출하는 사람이 정보

27) 대법원 2022. 2. 17., 선고, 2019도4938 판결

저장매체에 담긴 전자정보를 지정하거나 제출 범위를 한정하는 취지로 한 의사표시는 엄격하게 해석하여야 하고, 확인되지 않은 제출자의 의사를 수사기관이 함부로 추단하는 것은 허용될 수 없다. 따라서 수사기관이 제출자의 의사를 쉽게 확인할 수 있음에도 이를 확인하지 않은 채 특정 범죄혐의사실과 관련된 전자정보와 그렇지 않은 전자정보가 혼재된 정보저장매체를 임의제출받은 경우, 그 정보저장매체에 저장된 전자정보 전부가 임의제출되어 압수된 것으로 취급할 수는 없다. 전자정보를 압수하고자 하는 수사기관이 정보저장매체와 거기에 저장된 전자정보를 임의제출의 방식으로 압수할 때, 제출자의 구체적인 제출 범위에 관한 의사를 제대로 확인하지 않는 등의 사유로 인해 임의제출자의 의사에 따른 전자정보 압수의 대상과 범위가 명확하지 않거나 이를 알 수 없는 경우에는 임의제출에 따른 압수의 동기가 된 범죄혐의사실과 관련되고 이를 증명할 수 있는 최소한의 가치가 있는 전자정보에 한하여 압수의 대상이 된다. 이때 범죄혐의사실과 관련된 전자정보에는 범죄혐의사실 그 자체 또는 그와 기본적 사실관계가 동일한 범행과 직접 관련되어 있는 것은 물론 범행 동기와 경위, 범행 수단과 방법, 범행 시간과 장소 등을 증명하기 위한 간접증거나 정황증거 등으로 사용될 수 있는 것도 포함될 수 있다. 다만 그 관련성은 임의제출에 따른 압수의 동기가 된 범죄 혐의사실의 내용과 수사의 대상, 수사의 경위, 임의제출의 과정 등을 종합하여 구체적·개별적 연관관계가 있는 경우에만 인정되고, 범죄혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로 관련성이 있다고 할 것은 아니라고 판시하여 대검찰청 디지털증거 예규 제25조 제1항에서 임의제출의 취지와 범위를 확인하여야 한다는 내용을 재확인하고 있다.[28)]

대검찰청 디지털증거 예규 제27조에서는 선별하여 압수를 원칙으로 하는데 이때 디지털증거 파일명 목록 및 해시값을 확인하고, 이를 피압수자 등에게 교부하면서 압수 절차가 기재된 확인서에 피압수자의 서명을 받으며, 압수 현장에서 선별이 어려울 경우 디지털증거 중 일부만 가선별하고 이렇게 저장한 정보저장매체를 현장 외 장소로 반출할 경우에는 피압수자에게 특정 가능한 범위에서 목록을 작성하여 교부한다.

---

28) 대법원 2022. 1. 27. 선고, 2021도11170 판결

디지털증거 전부 복제 압수하는 제28조(전자정보의 전부 복제 시 조치)에도 선별 압수 때와 동일하게 해시값 확인, 압수 과정 촬영 등으로 디지털증거에 대한 동일성과 무결성을 담보하는 조치를 하고, 이렇게 압수한 정보저장매체 등은 봉투에 봉인지를 붙여 봉인하며 피압수자 등에게 참관 여부 확인서를 받는다. 이때 압수된 전부 복제본 목록을 압수목록에 기재하여 교부하여야 한다.

대검찰청 디지털증거 예규 34조 제3항에서는 '사건과 관련이 있는 전자정보를 파일 형태로 복제하여 압수하는 경우에는 선별된 전자정보에 대한 이미지 파일을 생성하고 그에 대한 해시값을 확인한다.'고 규정하는데 이는 검찰만의 디지털증거 수집 절차의 특징이라고 볼 수 있다. 검찰은 압수한 디지털증거는 압수 이후 법정에서 재현·검증에 용이한 포렌식 이미지를 생성하고 이에 대한 해시값을 계산하는 방법으로 디지털포렌식 절차를 진행한다. 무결성·동일성·진정성·원본성·신뢰성·관리 연속성 등 디지털증거 특징에 대한 일부 법정 공방이 이뤄지고 있으나, 디지털포렌식 절차상 포렌식 이미지를 생성한 사건에서 이러한 공방이 드문 것은 이미지를 생성하고 해시값을 확인하는 절차가 디지털포렌식에 대한 절차적 신뢰성과 적법성을 부여하고 있다고 봄이 상당하기 때문으로 판단된다.

제41조, 제42조에서는 위와 같이 획득한 이미지 파일과 그 추출파일을 디지털수사통합업무관리시스템(D-NET)에 등록하도록 하고 전부이미지에 대해서는 제37조 및 제38조에서 권한이 부여된 사람만 접근이 가능토록 하여 접근을 통제하고 있다.

제53조에서는 디지털증거 폐기 시 유의사항을, 제54조에서는 폐기 대상을 구체적으로 규정하면서, 중요한 증거가 될 경우 폐기의 예외를 규정하였고, 제58조에서는 유죄판결 확정된 디지털증거라도 피고인의 재심청구의 기회 보장을 위해 10년·준영구·영구 등 기간을 지정하여 보존하도록 하는 규정이다.

제54조(폐기대상) ① 다음 각 호에 해당하는 디지털 증거는 본 장에서 규정한 절차에 따라 업무관리시스템에서 폐기한다.

1. 수사 또는 재판 과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우
2. 압수의 원인이 된 사건에 대한 기소·불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우
3. 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우

② 제1항에도 불구하고 다음 각 호의 사유가 있는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다.

1. 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우
2. 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우

제58조 (유죄확정 판결에 대한 특례) ① 유죄판결이 확정된 사건에서 압수된 디지털 증거는 피고인에게 재심청구의 기회를 보장하기 위하여 형이 확정된 때로부터 10년간 보존할 수 있다.

② 판결 확정 이후 당사자의 폐기요청이 있는 경우에는 디지털 증거를 폐기한다. 다만, 유죄의 확정판결을 받은 자가 수인인 경우에는 당사자 전원의 폐기요청이 있을 경우에 폐기한다.

③ 내란죄, 외환죄 등 「검찰보존사무규칙」 제8조제3항에 해당하는 죄의 디지털 증거는 「검찰보존사무규칙」 제8조제3항을 준용하여 영구 또는 준영구로 보존한다.

<표 12> 디지털증거 폐기 대상 및 특례 규정

(2) 경찰청 훈령「디지털 증거의 처리 등에 관한 규칙」

경찰에서 디지털포렌식 절차를 구체적으로 규정한 디지털증거 훈령은 디지털포렌식 분석관 뿐만 아니라 일반 사법경찰관의 업무를 수행하는 경찰관들의 가장 기본이 되는 디지털증거 원칙이다.

제2조에서는 ①항 "전자정보"란 전기적 또는 자기적 방법으로 저장되거나 네트워크 및 유·무선 통신 등을 통해 전송되는 정보를 말한다, ②항 "디지털포렌식"이란 전자정보를 수집·보존·운반·분석·현출·관리하여

범죄사실 규명을 위한 증거로 활용할 수 있도록 하는 과학적인 절차와 기술을 말한다, ③항 "디지털증거"란 범죄와 관련하여 증거로서의 가치가 있는 전자정보를 말한다, ④항 "정보저장매체등"이란 전자정보가 저장된 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체를 말한다, ⑤"정보저장매체등 원본"이란 전자정보 압수·수색·검증을 목적으로 반출의 대상이 된 정보저장매체등을 말한다, ⑥항 "복제본"이란 정보저장매체등에 저장된 전자정보 전부를 하드카피 또는 이미징 등의 기술적 방법으로 별도의 다른 정보저장매체에 저장한 것을 말한다, ⑨항 "디지털포렌식 업무시스템(이하 "업무시스템"이라 한다)"이란 디지털 증거분석 의뢰와 분석결과 회신 등을 포함한 디지털포렌식 업무를 종합적으로 관리하기 위하여 구축된 전산시스템을 말한다고 규정하고 있다.

제5조(디지털 증거 처리의 원칙) 제1항에서는 '디지털 증거는 수집 시부터 수사 종결 시까지 변경 또는 훼손되지 않아야 하며, 정보저장매체등에 저장된 전자정보와 동일성이 유지되어야 한다'고 하여 무결성과 동일성을 규정한 내용이고 제2항에서는 각 단계별 업무처리자 변동 등의 이력이 관리되어야 한다고 하여 관리 연속성을 규정한 것이다.

경찰은 제30조(결과보고서 작성)에서 증거분석관은 분석 종료 시 디지털증거분석 결과보고서를 작성하여야 함을 규정하였다. 이는 검찰에서는 디지털증거업무관리시스템(D-NET)에 디지털증거 등록 완료 후 자동으로 생성되는 (약식)분석결과보고서와 달리, 경찰은 증거분석이 완료되면 모든 사건에 대해 분석보고서를 작성하는 특징이 있다.

제34조에서는 디지털증거 등의 보관에 대해 규정하는데 정보저장매체라는 특징을 반영하여 항온·항습이 되고 보안유지가 가능한 장소에 보관하는 규정이다. 제35조에서는 분석과정에서 생성된 전자정보의 삭제·폐기에 관한 내용을, 제36조에서는 입건 전 조사편철·관리미제사건 등록 사

건의 압수한 전자정보는 공소시효 만료일까지 보관 후 삭제·폐기하고, 이는 관서별 통합 증거물 처분심의위원회의 심의를 거쳐 관련 법령 및 절차에 따라 삭제·폐기함을 규정하였다. 제37조에서는 디지털증거 관리 시 과장급 부서장이 소속 부서의 디지털증거 보관 및 삭제·폐기 등 관리 현황을 정기적으로 점검하고 필요한 조치를 취하여야 한다고 하여 관리 책임자를 지정하는 내용이다.

2. 디지털증거 특징에 관한 증거능력 판례

대법원의 '일심회' 사건 판결문에서 다음과 같이 판시하고 있다. 압수물인 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 압수 시부터 문건 출력시까지 변경되지 않았음이 담보되어야 한다. 특히 디지털 저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다.[29)]

즉, 대법원 판례에서는 디지털증거의 원본 동일성이 인정되고, 무결성이 담보되며, 분석 컴퓨터 및 도구의 신뢰성과 디지털포렌식 분석관의 전문성·정확성이 담보되어야 증거능력을 인정할 수 있다는 조건을 판시한 것이다. 이러한 판례 취지 이후, 수사기관은 디지털증거의 수집·분석·보관·관리 전 단계에 걸쳐 디지털포렌식 기본 원칙을 확립하게 되었고 이는 현재 대검찰청 디지털증거 예규와 경찰청 디지털증거 훈령에 세부 절차와 원칙을 규정하였다.

---

29) 대법원 2007. 12. 13. 선고 2007도7257 판결

또한 위와 같은 판결 이후, 대법원 정책연구용역에서 디지털증거에 대한 압수·수색 개선방안을 제안하였는데, 이는 ①해당 디지털 증거의 출력·복사(선별), ②저장매체 자체의 하드카피 또는 이미징(전부 복제 반출), ③저장매체 자체의 압수(원본 반출)가 있는데, 그중 ①, ②의 방법은 취약성이라는 디지털증거의 특성상 증거수집·보전의 과정에서 동일성·무결성이 특히 문제될 수 있고, ②, ③의 방법은 대량성이라는 디지털증거의 특성상 피압수자의 영업비밀을 침해하거나 사생활의 비밀을 침해할 가능성이 매우 높다. 강제수사의 비례성 원칙에 비추어 원칙적으로 ①의 방법을, 예외적으로 ②, ③의 방법을 순차로 채택하는 것이 옳다고 제안하였고 이는 수사기관의 디지털증거 규정과 수사실무상 <선별→전부 복제 반출→원본 반출> 압수의 3단계 디지털포렌식 기본 절차로 확립되었다.[30]

대법원 판례에서는 압수・수색 과정에서 선별 후 비트열 방식으로 복제하여 생성한 포렌식 이미지를 압수하였다면 압수 절차는 종결된 것이므로 수사기관에서 위 이미지에 대한 탐색・출력・복제 과정에서 피압수자의 참여권이 보장되어야 하는 것은 아니다. 또한 전자문서 등은 성질상 작성자의 서명 혹은 날인이 없을 뿐만 아니라 작성자·관리자의 의도나 특정한 기술에 의하여 내용이 편집·조작될 위험성이 있음을 고려하여, 원본임이 증명되거나 혹은 원본으로부터 복사한 사본일 경우에는 복사 과정에서 편집되는 등 인위적 개작 없이 원본의 내용 그대로 복사된 사본임이 증명되어야만 하고, 그러한 증명이 없는 경우에는 쉽게 증거능력을 인정할 수 없다. 그리고 이러한 전자문서가 인위적 개작 없이 원본 내용을 그대로 복사·출력한 것이라는 사실은 전자문서 파일의 사본이나 출력물의 생성과 전달 및 보관 등의 절차에 관여한 사람의 증언이나 진술, 원본이나 사본 파일 생성 직후의 해시(Hash)값 비교, 전자문서 파일에 대한 검증·감정 결과 등 제반 사정을 종합하여 판단할 수 있다. 이러한 원본 동일성은 증거능력의 요건에 해당하므로 검사가 그 존재에 대하여 구체적으로 주장·증명해야 한다고 판시하였다.[31]

---

30) 이주원, (2012). “디지털 증거에 대한 압수수색제도의 개선”, 166-167.
31) 대법원 2018. 2. 8., 선고, 2017도13263 판결

위와 같은 판례가 나온 배경에는 법정에 제출된 디지털증거의 해시값 변경에 따른 것이다. MS오피스의 엑셀 프로그램 일부 버전에서는 전자문서를 읽어 오는 과정만으로도 그 전자문서의 내용을 변경하지 않더라도 파일의 해시값이 변경되는 특징이 있다. 수사기관의 검사 또는 사법경찰관이 압수한 디지털증거의 내용을 분석·검토하는 과정에서 엑셀 파일을 읽어오면서 해시값이 변경되었고 이는 그대로 CD/DVD 매체에 저장하여 법정에 증거로 제출되었던 것이고, 공판 과정에서 그 해시값 변경이 쟁점이 되어 위와 같은 대법원 판결문이 나오게 된 것이다.

이러한 판결문 사례는 디지털포렌식 절차에서 다음과 같은 교훈을 주게 된다. ①디지털증거의 보관 및 관리 과정에서 CD/DVD/USB메모리 등의 매체 뿐만 아니라 백업 디지털증거 데이터 보관의 중요성, ②디지털증거 압수 단계에서 포렌식 이미지 생성 및 해시값 확인의 중요성이다. 특히, 포렌식 이미지는 원본 데이터로부터 복제할 당시의 메타데이터를 포함한 비활성데이터까지 획득하고 이는 압수가 종결된 이후에도 수사기관에서 추출된 파일의 접근 자체로도 무결성 및 동일성이 훼손되어 해시값이 변경되는 파일이 있더라도 원본에서 복제한 그대로의 디지털증거로 재현이 가능하다는 점 때문에 포렌식 이미지를 생성하여 보관하는 것이 중요하다는 것이다.

3. 디지털증거 압수물 처리에 관한 법규정

대통령령「검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정」제62조(사법경찰관의 사건불송치) 제1항에서 ‘사법경찰관은 법 제245조의5제2호 및 동령 제51조제1항제3호에 따라 불송치 결정을 하는 경우 불송치의 이유를 적은 불송치 결정서와 함께 압수물 총목록, 기록목록 등 관계 서류와 증거물을 검사에게 송부해야 한다.’고 규정한다.

법무부 규칙「검찰압수물사무규칙」제4조(압수물의 수리) 제1항에서 ‘압수물사무담당직원은 경찰서등에서 검사에게 압수물을 송부 또는 인계하려는 경우 사건기록 또는 불송치기록의 ㅋ압수물 총목록 및 압수조서 등과

그 압수물을 대조하여 확인한 후 압제번호를 부여하여 수리한다. 이 경우 환가대금을 수리할 때에는 환가지휘서・견적서・매수서 등 공매관계서류를 추가로 대조・확인해야 한다'고 규정한다.

제56조(불기소처분사건의 압수물환부)에서는 '검사는 불기소처분된 고소・고발사건에 관한 압수물중 중요한 증거가치가 있는 압수물에 관하여는 그 사건에 대한 검찰항고 또는 재정신청 절차가 종료된 후에 압수물 환부 절차를 취하여야 한다'고 하고, 제57조(다른 검찰청에의 이송) 제1항에서는 '검사는 사건을 다른 검찰청의 검사에게 송치하는 경우에 압수물이 운반에 불편하거나 송부하는 것이 적당하지 아니한 때에는 이를 소속검찰청 또는 그 외의 장소에 보관한 상태로 송치할 수 있다'고 규정, 제62조(기소중지처분・참고인중지처분 사건의 압수물처분) 제1항에서 '검사는 기소중지처분 및 참고인중지처분을 하는 사건의 압수물을 공소시효가 완성할 때까지 계속 보관 처분하여야 한다. 이 경우 권리증서와 유가증권등 중요한 압수물을 제외한 서류 또는 위조인장등과 같은 소형의 압수물은 사건기록에 편철하여 보관하게 할 수 있다'고 하여 디지털증거를 보관하는 CD/DVD/USB메모리 등 소형 압수물은 수사기록에 편철할 수 있는 근거 규정으로 본다.

대검찰청 예규「압수 및 압수물 처리지침」을 보면, 제1조에서 불필요한 압수의 방지를 정하여 사법경찰관이 압수를 함에 있어 압수할 필요가 없는 물건 또는 사진, 사본으로 대체가능한 물건 등을 압수하는 경우가 있으니 그러한 사례가 없도록 하고, 제2조에서 압수물 송치의 통제로 사법경찰관이 압수한 물건들 중에는 형사소송법 제130조 내지 제134조에 규정된 보관, 환가, 가환부, 사진촬영 등 절차를 취하는 것이 상당함에도 만연히 송치하는 경우가 있으니 구속영장신청 때 또는 사건송치 때 형사소송법 제219조 단서 소정의 절차를 이행하도록 하여 디지털증거물이 사진촬영이 가능 시 이를 별도 적절한 장소에 보관하고 경위를 기록한 수사보

고 형태로 기록에 편철하고, 제4조에서는 기록에 편철된 문서·물건 등의 압수방법에서 사법경찰관이 압수절차를 취하여야 할 문서·물건 등을 기록에 편철하여 송치한 경우, 동 기록에서 위 문서 등을 빼내어 압수하고 그 자리에는 위 문서 등의 사본 또는 그 경위를 기재한 서면을 편철하도록 하여 기록에 편철하기 부적절한 압수물은 기록에서 떼어 그 경위를 기재한 서류로 대체하도록 한다.

행정안정부령「경찰수사규칙」제64조(압수조서 등)에서는 수사준칙 제42조제2항 후단에 따른 삭제・폐기・반환 확인서는 별지 제69호서식에 따르고, 압수목록 교부서에 삭제・폐기 또는 반환했다는 내용을 포함시켜 교부하는 경우에는 삭제・폐기・반환 확인서를 교부하지 않을 수 있다고 규정하였다.

제108조(불송치 결정) ① 불송치 결정의 주문(主文)은 다음과 같이 한다.

1. **혐의없음**
   가. 혐의없음(범죄인정안됨): 피의사실이 범죄를 구성하지 않거나 범죄가 인정되지 않는 경우
   나. 혐의없음(증거불충분): 피의사실을 인정할 만한 충분한 증거가 없는 경우
2. **죄가안됨**: 피의사실이 범죄구성요건에 해당하나 법률상 범죄의 성립을 조각하는 사유가 있어 범죄를 구성하지 않는 경우(수사준칙 제51조제3항제1호는 제외한다)
3. **공소권없음**
   가. 형을 면제한다고 법률에서 규정한 경우
   나. 판결이나 이에 준하는 법원의 재판・명령이 확정된 경우
   다. 통고처분이 이행된 경우
   라. 사면이 있는 경우
   마. 공소시효가 완성된 경우
   바. 범죄 후 법령의 개정・폐지로 형이 폐지된 경우
   사. 「소년법」, 「가정폭력범죄의 처벌 등에 관한 특례법」, 「성매매알선 등 행위의 처벌에 관한 법률」 또는 「아동학대범죄의 처벌 등에 관한 특례법」에 따른 보호처분이 확정된 경우(보호처분이 취소되어 검찰에 송치된 경우는 제외한다)
   아. 동일사건에 대하여 재판이 진행 중인 경우(수사준칙 제51조제3항제2호

는 제외한다)
자. 피의자에 대하여 재판권이 없는 경우
차. 친고죄에서 고소가 없거나 고소가 무효 또는 취소된 경우
카. 공무원의 고발이 있어야 공소를 제기할 수 있는 죄에서 고발이 없거나 고발이 무효 또는 취소된 경우
타. 반의사불벌죄(피해자의 명시한 의사에 반하여 공소를 제기할 수 없는 범죄를 말한다)에서 처벌을 희망하지 않는 의사표시가 있거나 처벌을 희망하는 의사표시가 철회된 경우, 「부정수표 단속법」에 따른 수표회수, 「교통사고처리 특례법」에 따른 보험가입 등 법률에서 정한 처벌을 희망하지 않는 의사표시에 준하는 사실이 있는 경우
파. 동일사건에 대하여 공소가 취소되고 다른 중요한 증거가 발견되지 않은 경우
하. 피의자가 사망하거나 피의자인 법인이 존속하지 않게 된 경우
4. **각하**: 고소·고발로 수리한 사건에서 다음 각 목의 어느 하나에 해당하는 사유가 있는 경우
가. 고소인 또는 고발인의 진술이나 고소장 또는 고발장에 따라 제1호부터 제3호까지의 규정에 따른 사유에 해당함이 명백하여 더 이상 수사를 진행할 필요가 없다고 판단되는 경우
나. 동일사건에 대하여 사법경찰관의 불송치 또는 검사의 불기소가 있었던 사실을 발견한 경우에 새로운 증거 등이 없어 다시 수사해도 동일하게 결정될 것이 명백하다고 판단되는 경우
다. 고소인·고발인이 출석요구에 응하지 않거나 소재불명이 되어 고소인·고발인에 대한 진술을 청취할 수 없고, 제출된 증거 및 관련자 등의 진술에 의해서도 수사를 진행할 필요성이 없다고 판단되는 경우
라. 고발이 진위 여부가 불분명한 언론 보도나 인터넷 등 정보통신망의 게시물, 익명의 제보, 고발 내용과 직접적인 관련이 없는 제3자로부터의 전문(傳聞)이나 풍문 또는 고발인의 추측만을 근거로 한 경우 등으로서 수사를 개시할 만한 구체적인 사유나 정황이 충분하지 않은 경우

<표 13> 행정안전부령 경찰수사규칙

위 규칙 제108조에서 경찰청 소속 사법경찰관은 혐의없음, 죄가안됨, 공소권없음, 각하 등의 사유로 불송치 결정할 수 있는 근거규정을 두고 있는데, 본 논문에서 다루고 있는 불송치 결정에 따른 디지털증거 보관 및 관리의 근거가 된다.

4. 디지털증거 불송치 결정에 관한 법규정

디지털증거는 형사소송법 제49조에서 압수조서에 품종, 외형상의 특징을 기재하도록 되어 있는바 정보저장매체가 목적물일 경우 물리적 형상인 HDD/SSD/USB메모리 등을 기재하고, 추상적 형상인 물리이미지 또는 논리이미지일 경우 물리이미지, 논리이미지 또는 전자정보 파일로 기재한다. 법률 제106조 및 수사준칙 제41조에서는 압수 3단계(선별 - 전부복제 반출 - 원본 반출) 원칙하에 전자정보를 수집하도록 하였다. 형사소송법 제266조의3에서 디지털증거를 열람·등사 대상으로 하였고, 이는 불송치 디지털증거 역시 이에 포함될 수 있는 것이다.

디지털증거 증거능력 요건을 살펴보면, 디지털포렌식 등 과학적인 분석으로 객관적 성립의 진정성이 인정된다면 특별히 신빙할 수 있는 상태가 불비하더라도 증거로서 인정된다고 본다. 대법원 형사소송규칙에서 정보저장매체 디지털증거는 원본의 카카오톡, 텔레그램 메신저 등 암호화된 데이터베이스 전자정보를 복호화 후 결과물이 원본과 동일성이 인정되면 증거능력이 인정되고, 이는 규칙 제134조에서 디지털증거 내용을 서면으로 출력하여 법정 증거로 제출할 수 있게 된다.

수사준칙 제42조에서 전자정보 상세목록에 포함되지 않는 전자정보는 삭제·폐기하도록 하였고, 검찰 디지털증거 예규 및 경찰청 디지털증거 훈령에서 이와 동일한 내용으로 규정하였다.

대검찰청 디지털증거 예규에서는 디지털증거 관련 용어를 정의하고, 객관적·인적 관련성에 대한 조건하에서 정황부터 디지털증거 재현·검증·정확성·신뢰성을 입증하는 자료까지 관련성이 있는 것으로 해석한다. 특히 검찰에서는 법정 재현·검증을 위해 반드시 포렌식 이미지를 생성하고 해시값을 확인하여 무결성·동일성·진정성·원본성·신뢰성·관리 연속성 담보에 사용되도록 하였고, 디지털증거수사망에서 보관·관리하고 사건 종결 또는 재판 확정 시까지 이를 보관하다가 폐기하나 재심의 청구 등의 이유로 10년·준영구·영구 보존이 가능한 이유를 규정하였다.

경찰 디지털증거 훈령에서는 디지털증거 정의와 함께 디지털증거의 수집부터 수사 종결 시까지 변경 또는 훼손되지 않고 동일성이 인정되도록 보관 및 관리하도록 하였다. 제35조에서는 전자정보 상세목록에 없는 전자정보는 삭제·폐기하도록 하고 제36조에서는 공소시효 만료일까지 보존하도록 세부적으로 규정하였다.

검찰 압수물사무규칙에서는 불송치기록은 압수물 총목록, 압수조서를 같이 송부하며, 검찰에서 수리 시 압수물을 대조하여 수리하도록 하는 내용을 규정하였다. 대검찰청 예규인 압수 및 압수물 처리지침에서는 사법경찰관이 압수를 하면서 영장 신청 또는 사건송치 때 디지털증거물을 사진촬영 가능 시 별도 장소에 보관하고 그 경위를 기록한 수사보고로 기록에 편철하며, 기록 편철이 부적절 시 기록에서 떼어내 그 경위를 기재한 서류로 대체하도록 하여 수사기록에 CD/DVD/USB메모리에 편철 보관하거나 부적절 시 별도 보관하고 경위를 수사보고로 기재하여 기록에 편철하도록 하였다.

경찰에서 사건 수사 결과, 혐의없음·죄가안됨·공소권없음·각하 시 불송치 결정하도록 하고, 이는 향후 증거관계 또는 상황의 변경으로 재수사의 경우를 대비하여 최소한 공소시효 완성 전까지는 사법경찰관의 수사기록 및 디지털증거 보관의 책임있는 보관·관리의 주체가 된다고 해석할 것이다.

제 3 장 디지털증거의 수집과 관리

제 1 절 검찰 디지털증거 수집 및 관리

1. 디지털증거 수집 절차

1-1. 압수・수색 현장에서 디지털증거 수집

압수・수색 현장에서 디지털증거 수집은 주임검사 등이 대검찰청 디지털수사과에 압수・수색을 요청하고 관할 거점청 디지털포렌식팀에 디지털포렌식 전문수사관을 배치하고 필요 시 다른 거점청 디지털포렌식 전문수사관을 추가 배치한다. 대검찰청 디지털증거 예규상 검찰의 디지털증거 압수・수색 시 반드시 디지털포렌식 전문수사관에 의해서만 압수・수색이 이뤄지는 점이다.

제14조(전자정보의 압수・수색・검증 실시자) 전자정보의 압수・수색・검증은 디지털포렌식 수사관이 하여야 한다. 다만, 부득이한 사유가 있는 경우에는 포렌식 도구 교육 등 제11조 제1항에서 정한 디지털포렌식 관련 교육을 이수한 검찰공무원으로 하여금 디지털포렌식 업무를 수행하게 할 수 있다.

<표 14> 대검찰청 디지털증거 예규 제14조 규정

자격 요건은 3개월 이상 디지털포렌식 수사 실무를 수행한 자 중에서 "디지털포렌식 전문가 양성과정"의 교육을 이수한 자 또는 국내・외 컴퓨터 관련 교육과정을 이수한 자로서 디지털포렌식 관련 지식이 충분하다고 인정되는 자로 제한하고 있다. 이는 압수・수색 현장에서 역시 전문교육을 이수한 자로 제한하여 디지털증거의 취약성과 그 특징을 감안하여 증거능력을 갖춘 증거 수집을 수행하기 위한 정책적 고려에서 나온 산물로 보인다.

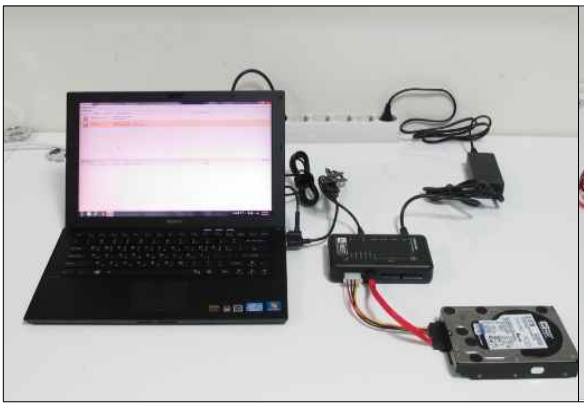
압수・수색 현장에서 디지털포렌식 전문수사관은 주임검사 등으로부터 ①사건과 관련된 디지털 증거의 구별에 필요한 검색어(인물, 대상 등), 검색기간, 파일명, 확장자 등 선별 관련 정보, ②그밖에 수집할 디지털 증거의 대상 및 범위 등을 정하는데 필요하다고 인정되는 자료 및 정보(대검

찰청 디지털증거 예규 제16조 제1항)를 제공받아 각종 정보저장매체(PC, 노트북 등)에서 피압수자 참관하에 전자정보에 대한 탐색·선별·논리이미지 생성 등의 절차로 디지털증거를 수집한다.

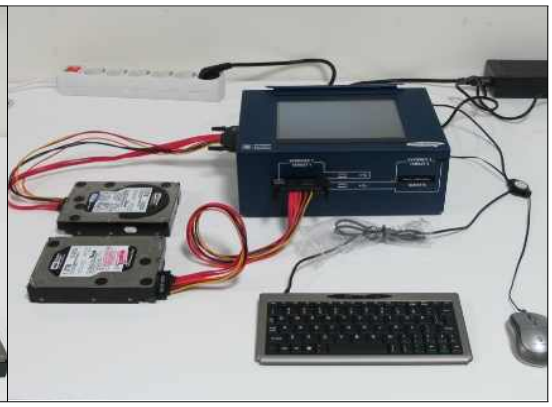
영장 제시 → 대상자 매체 특정 → 선별 압수 가능 여부 → 전자정보 의견진술 보장 → 압수목록 교부 등 관련 디지털증거 수집 절차는 '압수·수색·검증 현장에서 전자정보 수집 흐름도'에서 확인할 수 있다. 특히 흐름도에서는 ①선별 ②전부 복제 이미징 반출 ③원본 반출 등의 압수의 3단계 원칙을 명확히 제시한다.

현장에서 전자정보에 대한 선별 압수가 불가능하거나 현저히 곤란한 사유가 있을 경우 현장 압수의 3단계 절차 중 2단계인 정보저장매체 전부 복제 이미징으로 물리이미지를 생성하여 이를 반출한다. 반출 사유로는 ① 파일 암호화 등으로 인해 범위를 정한 출력·복제가 불가능한 경우, ② 안티포렌식 등 범죄혐의와 개연성이 있는 디지털정보가 조작 또는 삭제된 정황이 발견된 경우, ③ 정보저장매체등에 저장되어 있는 정보가 방대하여 현장에서 출력·복제 방식으로 압수하는데 많은 시간이 소요되어 피압수자의 사생활의 평온이나 영업 활동을 침해할 우려가 있는 경우, ④ 정보저장매체등이 사이버범죄 및 새로운 유형의 첨단범죄에 이용되는 등 수사 또는 공소의 제기 및 유지를 위하여 정보저장매체등에 기억된 디지털 증거의 종합적인 분석이 필요한 경우, ⑤ DB시스템이나 RAID시스템 등과 같이 분석 대상 시스템과 동일한 시스템을 구축하여 분석해야 하는 경우 등이 있을 수 있다.[32]

32) 대검찰청 디지털증거 예규 별지 13호 전자정보 압수·수색·검증 안내문



<그림 17> 이미지 파일 생성 과정



<그림 18> 디스크 복제 과정[33]

현장에서 선별 또는 전부 복제본 압수가 모두 불가능하거나 현저히 곤란한 경우에는 현장 압수의 3단계 방법 중 3단계인 정보저장매체의 원본을 반출한다. 이때 원본 반출 사유는 ①정보저장매체등이 물리적으로 손상된 경우, ②정보저장매체등에 암호가 걸려 있고 피압수자등이 협조하지 않는 경우, ③현장에서 복제·출력할 수 있는 장비나 도구가 개발되어 있지 않거나 준비에 장시간이 소요되는 경우, ④현장에 전력 공급이 원활하지 않은 경우, ⑤피압수자가 위력을 행사하여 정상적인 압수·수색 집행이 불가능한 경우, ⑥전자정보의 전부 복제 반출을 위한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우, ⑦ 정보저장매체 등 또는 동 매체에 기억된 전자정보가 몰수대상인 경우 등이 있을 수 있다.[34]

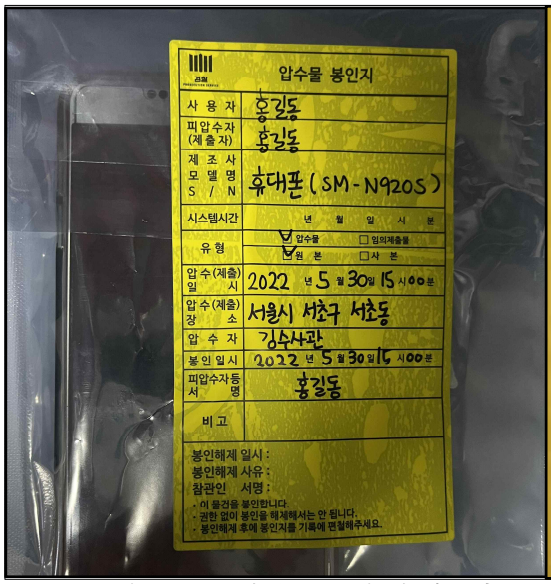
피압수자 등의 협조에도 불구하고 스마트폰, 태블릿, 아이패드 등 모바일정보기기에 대해서는 ①일반적으로 사용하는 윈도우 등 운영체제가 달라서 데이터의 획득 및 분석 과정이 상이하고, ②제조사 및 모델마다 그 방식이 다르고, ③현장에서 획득 및 분석에 사용하는 고가의 장비 및 분석 툴을 구비하기 어렵다는 사유로 정보저장매체 원본을 반출하고 있다.

---

33) http://forensic-proof.com/archives/3613

34) 대검찰청 예규, "디지털 증거의 수집·분석 및 관리 규정" 별지 13호 전자정보 압수·수색·검증 안내문

원본 정보저장매체를 반출할 경우 '압수물 봉인지' 및 '정전기방지 봉투'를 이용하여 원본 매체를 봉인하고 '충격방지봉투'에 안전하게 보관한다.



<그림 19> 압수물 봉인지 및 정전기방지 봉투

<그림 20> 충격방지봉투

1-2. 현장 외 디지털증거 수집 절차

압수 3단계 중 현장에서 전부 복제본 또는 원본 정보저장매체 반출 후 디지털포렌식팀 분석실에서 진행하는 디지털증거 수집 절차이다.

현장에서 수집한 전부 복제본 또는 원본 매체는 대검찰청 디지털증거 업무관리시스템(D-NET)상 관할 거점청에 증거분석을 요청하고 참관여부 확인서와 전부 복제본 또는 원본 매체를 송부한다.

피압수자가 참관하기로 한 경우에는 피압수자가 참여한 상태에서, 그렇지 않는 경우에는 신뢰성과 전문성을 담보하는 상당한 방법으로 전자정보를 탐색·분석하여야 한다. 전부 복제본 또는 원본 매체에 대한 봉인 해제는 참관인이 있을 경우 봉인지에 서명을 받고 그렇지 않을 경우에는 참관인 서명 없이 봉인을 해제하되 디지털포렌식 절차상 무결성 및 신뢰성을 담보하기 위하여 봉인 해제 전 과정은 다음 그림과 같이 비디오 촬영을 하고 있다.

봉인 해제 후에는 디지털포렌식 분석 툴을 사용하여 대상 매체에 대한 획득·분석·탐색·선별 등의 절차로 최종 압수되는 선별 디지털증거를 논리이미징하여 이를 압수한다. 선별 후 절차는 압수 현장에서 진행되는 디지털증거 수집 절차와 동일하다.

기존에 없던 '전자정보의 삭제·폐기 또는 반환' 절차가 수사준칙으로 제정되었다. 검사 또는 사법경찰관은 선별 압수된 디지털증거를 대상으로 전자정보 상세목록을 생성하고 이를 피압수자에게 교부해야 한다. 이때 상세목록에 포함되지 않을 전자정보가 있는 경우에는 해당 전자정보를 지체 없이 삭제 또는 폐기하거나 반환해야 하고, 이 경우 삭제·폐기 또는 반환확인서를 작성하여 피압수자등에게 교부해야 한다.[35]

전자정보 상세목록 교부와 삭제·폐기 또는 반환확인서 작성 과정은 수사준칙에 따라 시행되고 있는데, 이는 사건과 무관한 파일들이 부수적으로 수사기관의 분석용 PC 등에 저장되고 있어, 피압수자에게 교부한 전자정보 상세목록에 포함되지 않은 전자정보는 반드시 삭제·폐기함으로써 피압수자 등의 인권을 보호하는 데 그 목적이 있다고 할 수 있다. 여기서 전자정보 상세목록에 포함되지 않은 전자정보는 삭제할 의무가 발생하는데 상세목록에 전부 복제 이미지 및 선별된 이미지의 파일명과 해시값 정보가 포함되지 않을 경우 수사기관의 이미지 보관의 근거가 없어지고, 디지털포렌식 절차상 신뢰에 영향을 미치므로 이 점 유의해야 한다.

35) 대통령령, "검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정" 제42조 제2항

2. 디지털증거의 보관・관리 및 폐기

2-1. 디지털증거 보관 및 관리

검찰에서 디지털증거를 보관・관리하는 방법은 다음의 '디지털증거 보관 및 관리 흐름도'에서 확인할 수 있다. 주임검사 등의 요청으로 압수 또는 임의제출로 수집된 디지털증거는 디지털증거업무관리시스템(D-NET)에 의해 보관・관리된다.

이는 일종의 클라우드 서버로 광범위한 디지털증거를 주임검사 등의 수사기록에 CD/DVD 또는 USB메모리 등에만 보관하기에는 증거가 안정적으로 보관된다고 보기 어렵게 된다. 그래서 서버에 디지털증거를 안전하게 보관함으로써 공판 과정 등에서 디지털증거에 대한 무결성・신뢰성 등을 담보할 수 있게 되는 것이다.

주임검사 등은 디지털증거업무관리시스템(이하 'D-NET'이라고 함)에서 디지털증거를 압수물로 수리하게 됨으로써 D-NET에서는 압수물 수리에 따른 압수조서(디지털증거)와 디지털증거 보관확인서가 자동으로 작성된다. 서버단의 정보저장매체상 정보로 남는 디지털증거의 특성에 맞춰 별도 실물이 없더라도 압수물의 경위를 담고 있는 '디지털증거 보관 확인서'가 실물을 대신하는 것이다.

D-NET에 보관된 디지털증거물을 관리하는 디지털증거 관리담당자는 디지털 증거의 보관의 연속성이 유지될 수 있도록 디지털 증거의 승계과정에서 등록된 기록, 사진, 영상 등은 관리하여야 하며, 권한 없이 디지털 증거에 접근하지 못하도록 업무관리시스템 상 디지털 증거에 대한 접근 로그를 생성·관리하여야 한다.[36]

---

36) 대검찰청 예규, "디지털 증거의 수집·분석 및 관리 규정" 제52조

대검찰청 과학수사부 디지털수사과

디지털증거 보관 확인서

피의자 홍길동에 대한 서울중앙지검 2022형제10000호(2022요청3500호) 사건에 관하여 대검찰청 국가디지털포렌식센터(NDFC)에 보관되어 있는 디지털증거는 다음과 같습니다.

순번	디지털증거명	용량	등록일시	담당(분석수사관)	보관 증거번호	비고
1	홍길동의 업무 PC 논리이미지	5.2GB	2022. 10. 1.	검찰주사보 김길동	2022증거3500_1	
2	홍길동의 휴대폰(AA-A8) 논리이미지	20.1GB	2022. 10. 1.	검찰주사보 김길동	2022증거3500_2	

위와 같이 디지털증거가 보관되어 있음을 확인합니다.

2022. 10. 1.

디지털증거 관리책임자
대검찰청 디지털수사과장

<그림 21> 디지털증거 보관 확인서(디지털증거)

■ 검찰사건사무규칙 [별지 제60호서식]

압 수 조 서(디지털증거)

피의자 홍길동에 대한 절도 피의사건에 관하여 2022년 10월 1일 10시 00분경 서울시 서초구에서 검사 김○○ 검찰주사보 김○○을 참여하게 하고 아래 경위와 같이 물건을 압수하다.

①증제번호	②물건명	③특기사항					④비고
		수량 등	홍길동의 업무PC 논리이미지 1개(5.2GB)				
		압수이유	물수대상	□ 범죄행위에 제공되었거나 제공하려고 한 물건 □ 범죄행위로 생겼거나 취득한 물건 □ 위 대가로 취득한 물건			
			□ 장 물				
			□ 기타 압수가 필요한 이유( )				
		발견·압수 경위	2022요청3500호에 근거하여 정보저장매체에서 범죄사실과 관련 있는 전자정보를 추출하여 이를 압수하다.				
		소지자(제출자)	성명	홍길동	주민등록번호	000000-0000000	
			주소	서울시 서초구	전화번호	02-3480-0000	
		소유자	성명		주민등록번호		
			주소		전화번호		
		■ 소유권 포기 □ 환부 요구					
		수량 등	홍길동의 휴대폰 논리이미지 1개(20.1GB)				
			□ 범죄행위에 제공되었거나 제공하려고 한 물건				

<그림 22> 압수조서(디지털증거)

2-2. 디지털증거의 폐기

D-NET 보관 디지털증거는 대검 디지털증거 예규상 ① 수사 또는 재판 과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우, ② 압수의 원인이 된 사건에 대한 기소·불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우, ③ 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우 폐기한다(대검 예규 제54조 제1항).

그러나 위와 대상에 해당함에도 ㉠ 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우, ㉡ 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우, ㉢ 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다(대검 예규 제54조 제2항). 또한 유죄판결이 확정된 사건 중에서도 피고인의 재심청구의 기회를 보장하기 위하여 형이 확정된 때로부터 10년간 보존할 수 있고, 판결 확정 이후 당사자의 폐기요청이 있는 경우에 디지털증거를 폐기한다. 유죄의 확정판결을 받은 자가 수인일 경우 당사자 전원의 폐기 요청이 있을 경우에 폐기한다. 그 외 내란죄, 외환죄 등 「검찰보존사무규칙」 제8조 제3항에 해당하는 죄의 디지털증거는 「검찰보존사무규칙」 제8조 제3항을 준용하여 영구 또는 준영구로 보존한다.

‘디지털증거 폐기 절차 흐름도’는 대검찰청 디지털증거 예규 제54조 제1항, 제2항 및 검찰보존사무규칙」제8조 제3항에 따른 폐기 절차를 착오가 없도록 구체적으로 명시하였다.

구체적 폐기 절차는 주임검사(없는 경우 그 승계 검사) 또는 압수전담검사의 요청으로 폐기 절차는 개시한다(대검 예규 제56조). 주임검사 또는 압수전담 검사는 폐기대상 디지털 증거에 대하여 폐기촉탁지휘를 하고, 폐기촉탁지휘를 받은 압수물담당직원은 KICS의 압수물관리시스템을 통하

여 대검찰청 과학수사부 디지털수사과장에게 해당 디지털증거에 대한 폐기를 요청한다. 디지털수사과장은 폐기를 요청 받은 디지털증거를 지체 없이 폐기하고 별지 제12호 서식의 '디지털 증거 폐기(촉탁) 회보서'를 업무관리시스템을 통하여 입력하는 방법으로 작성하여 압수물담당직원에게 회보한다.[37]

제 2 절 경찰 디지털증거 수집 및 관리 현황

1. 디지털증거 수집 및 관리

1-1. 디지털증거 수집

경찰은 인력구조 상 분석관이 직접 현장에서 압수·수색에 참여할 수 없어, 일선 수사관이 디지털 증거의 압수·수색에 관한 기본적인 지식과 기술을 훈련 받아 디지털증거를 압수·수색을 수행하고, 분석은 증거분석관들이 담당하고 있다.[38]

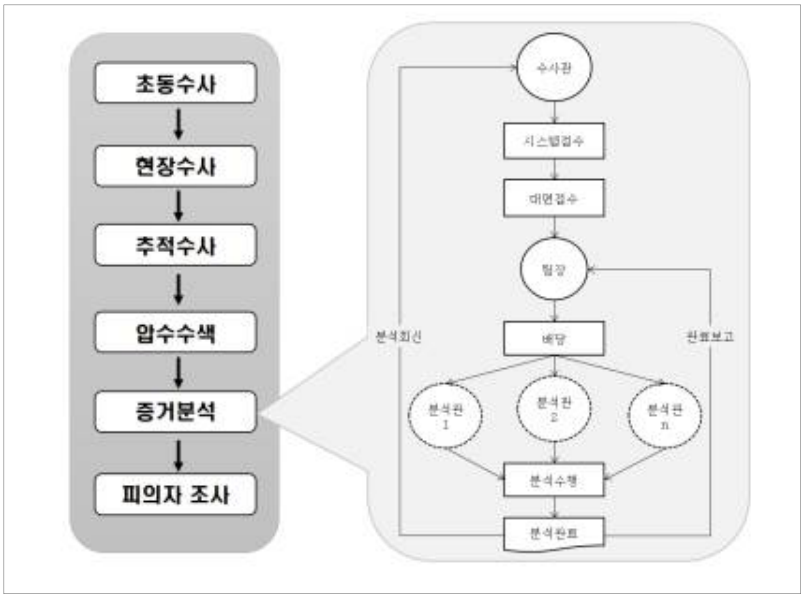
디지털증거를 현장에서 선별 압수 완료하는 경우, 압수물로 관리하고, 현장에서 복제본 또는 원본을 반출할 경우 압수 완료 시까지 임시적으로 증거물로 등록한다. 이후 증거물 바코드를 생성·부착하여 관리하다가, 압수가 종결되면 압수물로 전환하여 관리하고 있다.[39]

1-2. 디지털증거물 분석 의뢰

사법경찰관은 압수한 디지털증거가 원본인 경우 현장에서 피압수자의 참여권을 보장한 상태에서 봉인 후 분석 의뢰하고, 피압수자가 참여하겠다고 하는 경우에는 디지털포렌식 분석팀과 사전에 분석 일시와 장소를 협의하여 의뢰한다.

---

37) 대검찰청 예규, "디지털 증거의 수집·분석 및 관리 규정" 제57조
38) 장진, (2021). 수사과정에서 확보한 디지털증거 관리 방안 연구, 23.
39) 정웅길·이상진, (2022). 검·경 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지 방안, 130.



<그림 23> 범죄수사와 디지털포렌식 업무절차[40]

분석의뢰 수사관은 분석의뢰물을 봉인 후 직접 운반이 원칙이나[41], 직접 운반이 현저히 곤란한 경우에는 분석 의뢰물이 훼손되지 않고 운반 이력이 확인될 수 있는 안전한 방법으로 의뢰할 수 있다.

분석의뢰물을 전자적 방식으로 전송할 필요가 있는 경우에는 동일성·무결성을 유지하는 해시값을 기록하는 등 조치를 취하고 디지털증거 통합관리시스템을 통해 분석 의뢰물을 전송한다.[42]

1-3. 디지털증거 분석 및 보관, 관리

1-3-1. 디지털증거 분석

경찰청 훈령인 「디지털 증거의 처리등에 관한 규칙」에서 디지털증거 수집 시 분석 의뢰사건의 개요, 분석 목적 및 요청사항 등을 파악한 후 요청사항, 분석 의뢰물 유형 및 상태 등을 고려하여 획득·분석의 범위와

40) 신지호·최낙범, (2016). 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구, 경찰, 242.
41) 경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제23조 제1항
42) 경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제23조 제2항

방법을 결정한다. 이때 분석 의뢰물에 대해 권한 없는 사람의 접근을 통제하고, 특별한 사유가 있는 경우를 제외하고는 증거분석실 출입을 제한하여 획득·분석 과정에서 분석의뢰물의 무결성과 관리연속성을 유지해야 한다.

분석을 마친 후 분석관은 분석의뢰 수사관에게 보고서와 분석결과물을 회신하고, 이에 수사관은 선별 압수를 해야 한다. 이때 디지털증거 통합관리시스템의 분석결과물 보관기간은 2주이므로, 2주 이내에 처리를 마쳐야 한다.

1-3-2. 디지털증거 보관 및 관리

선별 압수한 전자정보는 USB, 하드디스크 등 저장매체에 옮긴 뒤 KICS(형사사법포털사이트)에 압수물로 등록하고, 저장매체는 압수물봉투 등에 넣어 봉인 후 관리시스템에서 압수물을 바코드를 생성해 부착하여 관리한다.[43]

증거분석을 통해 획득한 전자정보는 항온·항습·무정전·정전기차단시스템이 설치된 장소에 보관함을 원칙으로 하며, 이 경우 열람제한설정, 보관장소 출입제한 등 보안유지에 필요한 조치를 병행하여야 한다.[44]

1-3-3. 포렌식 이미지 생성 규정 미비

경찰청 디지털증거 훈령에서는 포렌식 이미지를 작성에 관한 규정이 없다. 전자정보 상세목록은 작성하나 별도 이미지를 생성하지 않기에 경찰 실무상 압수된 디지털증거 파일은 ZIP 형태로 압축하여 해시값을 생성하여 피압수자에게 교부하는 절차를 취하고 있다. 이렇게 수집된 디지털증거는 수사기록의 CD/DVD/USB메모리 등으로 편철하여 보관하고 있다. 그래서 디지털증거의 수사기록에 편철된 정보저장매체 외에는 백업 디지털증거가 존재하지 않는다.

---

43) 정웅길·이상진, (2022). 검·경 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지 방안, 131.
44) 경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제34조

1-4. 디지털증거의 폐기

1-4-1. 경찰 디지털증거 폐기

증거분석관은 분석을 의뢰한 경찰관에게 분석결과물을 회신한 때에는 해당 분석과정에서 생성된 전자정보를 지체 없이 삭제·폐기하여야 하며, 분석을 받은 경찰관은 사건 이송·송치 시 경찰관 개인 컴퓨터·저장매체 등에 보관되어 있는 디지털 증거의 복사본은 지체 없이 삭제·폐기 하여야 한다.[45]

입건 전 조사편철·관리미제사건의 경우에는 압수를 계속할 필요가 있는 경우 해당 사건의 공소시효 만료일까지 보관 후 삭제·폐기하며, 압수를 계속할 필요가 없다고 인정되는 경우 삭제·폐기 하여야 한다.[46]

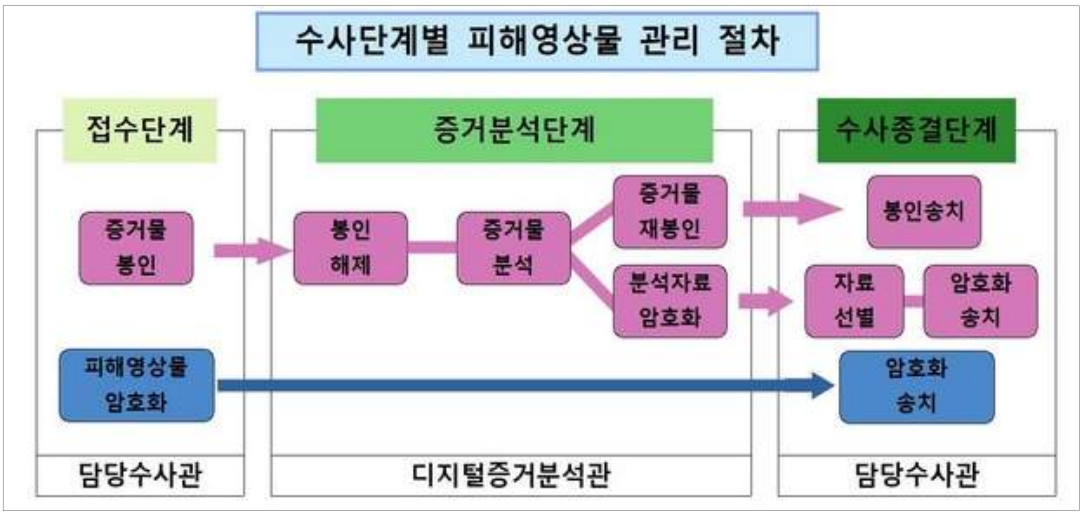
1-4-2. 불송치·수사중지 등 처리 절차 규정 미비

경찰청 디지털증거 훈령에는 새로 생긴 절차인 불송치·수사중지 등 검찰에서 경찰로 기록이 반환되었을 때 디지털증거물 처리 절차에 대한 규정이 없다. 경찰에서는 사건이 종결되었다고 판단하여 디지틀증거물을 폐기할 수 있고, 보관성에 취약한 CD, USB등 저장매체에 보관하게 되면 디지털증거물이 손상되어 항후 수사가 재개될 경우 문제가 생길 수 있다.

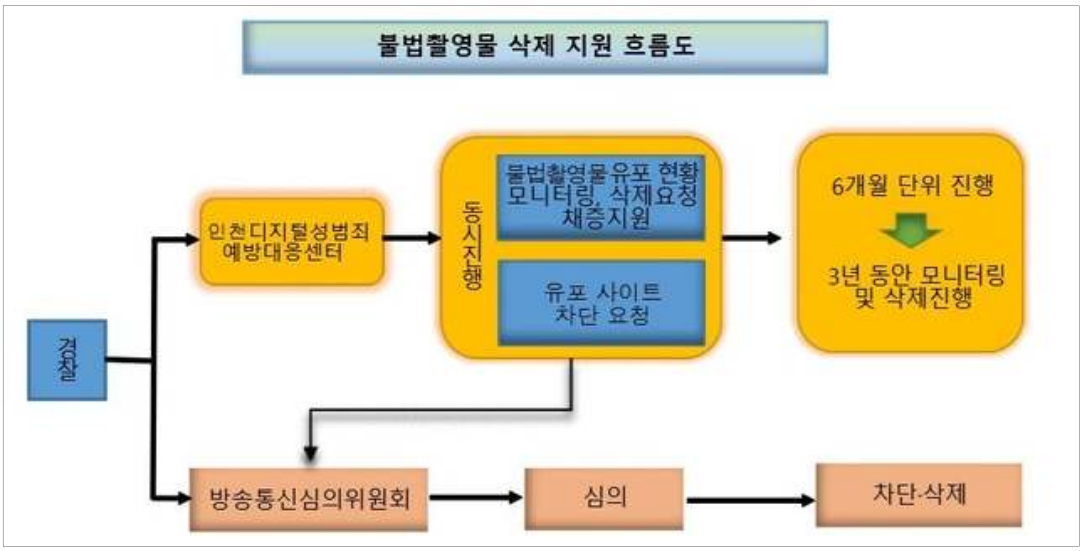
---

45) 경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제35조
46) 경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제36조

1-4-3. 인천경찰청 디지털성범죄 피해영상물 관리 체계[47]



<그림 24> 수사단계별 피해영상물 관리 절차



<그림 25> 불법촬영물 삭제 지원 흐름도

인천경찰청은 디지털 성범죄 피해영상물 관리 절차를 시행하여 디지털 성범죄 피해자에 대해 보호·지원 체계를 갖추고 있다. 인천경찰청 디지털 증거분석관으로 현장 지원반을 구성해 관련 사건에 대한 압수·수색을 24

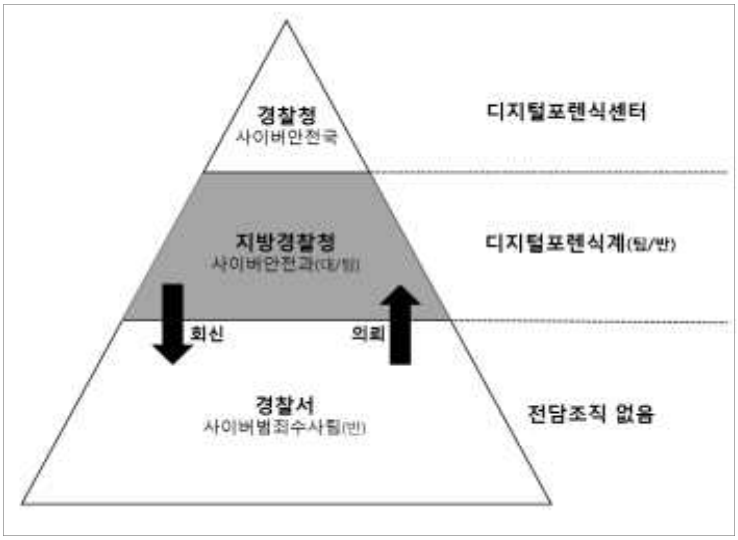
47) 인천경찰청 보도자료, 인천경찰청 디지털성범죄 피해자 보호·지원 강화, 2021. 9. 5.

시간 지원하고 확보한 증거물은 즉시 증거분석을 실시하는 제도이다. 피해 영상물로 신고되면 방송통신심의위원회를 통해 삭제·차단하고, 이러한 영상물의 재유포를 막기 위해 경찰과 인천디지털성범죄예방대응센터가 사후 모니터링을 통해 추가 삭제 삭제 조치한다. 영상물은 동성 수사관이 피해자와 함께 확인하도록 하고, 수사 사건이 검찰에 송치될 때까지 관련 증거는 모두 암호화해 보관한다.

2. 디지털포렌식 운영 및 제도 현황

2-1. 디지털포렌식 운영 현황

경찰은 인력구조상 분석관이 직접 현장에서 압수·수색에 참여할 수 없어, 일선 수사관이 디지털 증거의 압수·수색에 관한 기본적인 지식과 기술을 훈련받아 디지털증거를 압수·수색을 수행하고, 분석은 경찰청 및 지방청 디지털포렌식센터 증거분석관이 담당하고 있다.



<그림 26> 경찰의 디지털포렌식 조직[48]

2020년 기준, 경찰의 디지털포렌식 분석 건수는 6만 3,000건에 이르며, 2017년 기준 3만 4541건에서 3년 사이 2배가량 급증한 것으로 나타난다.

48) 신지호·최낙범, (2016). 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구, 240.

(단위 : 건)

구 분	소계	컴퓨터기기 (PC,노트북 등)	디지털기기 (CCTV,네비)	모바일기기 (스마트폰,휴대폰)	파일/기타 (해킹,암호,DB 등)
'10년	6,247	3,864	276	1,611	496
'11년	7,388	3,356	479	3,352	201
'12년	10,426	3,830	393	5,870	333
'13년	11,200	3,138	483	7,332	247
'14년	14,899	3,079	510	10,656	654
'15년	24,295	3,357	712	19,526	700
'16년	32,281	3,923	794	26,408	1,156
'17년	36,060	4,198	867	30,238	757
'18년	45,103	6,239	1,065	36,986	813
'19년	56,440	7,295	1,412	46,551	1,182
'20년	63,935	9,113	1,557	52,479	786

<표 15> 경찰 디지털증거 분석현황 2010-2020(경찰청 정보공개자료)

국내에서 발생하는 다수의 형사 사건에서 디지털포렌식을 통한 증거분석 요청은 지속적으로 증가하고 있으나, 실무상 증거분석을 담당할 수 있는 인력은 많이 부족하다.

(단위: 명)

총계	본청	서울	부산	대구	인천	광주	대전	울산	경기남부	경기북부	강원	충북	충남	전북	전남	경북	경남	제주
221	40	33	17	10	9	7	5	5	32	8	5	5	8	8	7	7	10	5

<표 16> 경찰 디지털포렌식 인력 현황(2020. 12. 31. 기준)[49]

49) 경찰청, 2021년 경찰백서, 206

경찰청 통계에 따르면 전국적으로 디지털포렌식 분석관이 평균 1인당 약 290건을 분석하였으며, 청별로는 경북청이 1인당 501.3건, 서울청 428.7건, 경기남부청 395.1건으로 나타났다. 스마트폰 등 모바일기기가 범죄의 주요 수단이나 증거가 되면서, 수사 과정에서 디지털포렌식 분석의 역할이 점점 더 커지고 있다.[50]

2-2. 경찰청 디지털포렌식 자문위원 제도

경찰청은 디지털포렌식 전문가 20명을 제3기 디지털포렌식 자문위원으로 위촉하여 2년의 임기로 활동한다. 자문위원은 교수・국책연구기관 연구원・변호사 등 외부 전문가로 구성되며, 기술 분야와 법률·인권분야로 나눠 디지털 증거분석 절차의 공정성과 신뢰성을 확보할 방안에 관해 경찰에 의견을 제시하는 역할 한다. 디지털포렌식 자문위원 제도는 2018년 디지털포렌식 증거분석 등의 신뢰성과 공정성 확보를 위해 시행되어 제1기는 지방청 분과위원을 포함한 94명의 전문가로 구성돼 '증거의 처리 등에 관한 규칙' 개정안 등 모두 45회 자문활동을 했고, 2020년 제2기는 20명 규모로 압축돼 경찰청 위원으로만 구성해 운영하면서 분석관 법정증언 법률 검토 등 총 24회의 자문활동을 수행하였다.[51]

제 3 절 디지털증거 송부 및 그 문제점

1. 수사기관 내부 디지털증거 송부

1-1. 경찰 - 경찰 간 송부

경찰에서 수집한 디지털증거는 CD/DVD/USB메모리/외장HDD 등 정보저장매체에 보관하고 있다. 경찰서 간 사건 이송 시 첨부되는 디지털증거물은 정보저장매체를 직접 수사기록에 편철하여 인계하거나 별도 등기 등을 활용하여 전송되고 있다. 형사사법정보시스템(KICS)에 디지털증거를 첨부파일로 등록할 수 있으나, 용량제한이 있어 활용도가 높지 않고, 수사

50) http://www.koit.co.kr/news/articleView.html?idxno=89644
51) 경찰청 보도자료, 경찰청 제3기 디지털포렌식 자문위원 위촉, 2022. 10. 25.

서류 작성에 대한 보조적 수단에 불과하며, 경찰의 과학적범죄분석시스템(SCAS)의 통합증거물관리시스템은 증거물 바코드를 발급하거나, 디지털 증거 분석의뢰를 위한 전송체계지, 경찰 전체의 디지털증거물 전송체계라고는 볼 수 없다.[52]

경찰청 훈령 '디지털증거의 처리등에 관한 규칙'상 사건을 이송한 경우 수사과정에서 생성한 디지털 증거의 복사본은 지체 없이 삭제·폐기되어야 하는데, 이송 받은 담당 수사관이 착오 또는 처리지연으로 이송 과정에서 저장매체·디지털증거가 분실 및 훼손된 사실을 뒤늦게 확인한 경우에는 이미 삭제·폐기된 디지털증거는 복구할 방법이 없어 문제가 발생할 수도 있다.[53]

1-2. 검찰 - 검찰 간 송부

대검찰청은 형사사법정보시스템과 별도로 디지털증거업무관리시스템(D-NET)을 구축하여 전국 검찰청의 모든 디지털증거를 중앙 서버로 전송하여 관리하고 있다. 그래서 검찰청 간 사건 이송을 할 때 첨부되는 디지털증거는 별도 물리적 송부 없이 디지털증거업무관리시스템(D-NET) 내에서 담당 주임검사 등에게 접근권한을 변경하는 방식으로 이송되고 있다.[54]

2. 수사기관 외부 디지털증거 송부

2-1. 경찰 - 검찰 간 송부

경찰은 관리 미제 및 입건 전 조사편철(구 내사) 종결 건을 제외하고 수사서류와 증거물을 송부하여야 한다. 이때 원본 정보저장매체 자체 또는 사본 정보저장매체에 디지털증거를 복제하여 송부한다. 경찰에서 형사

52) 김일권·김기범. (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 184.
53) 정웅길·이상진. (2022). 경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안. 디지털포렌식연구, 132.
54) 김일권·김기범. (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 184.

사법정보시스템에 디지털증거를 첨부하였다고 하더라도 검찰 형사사법정보시스템에는 전송되지 않는다. 그렇기 때문에 경찰에서 송치할 때, 디지털증거를 출력하여 수사기록에 편철하거나, 정보저장매체에 저장한 다음 수사기록에 묶어 검찰에 사건을 송부하고 있다.[55]

경찰에서 검찰로 디지털증거물이 송부되었을 때 관리 연속성 확보를 위해 개별 파일의 해시값을 확인하는 등 절차를 거쳐야 하지만, 검찰에서는 증거물인 저장매체의 존재 여부만 확인하고 있다. 또한 경찰에서 송부된 디지털증거에 대해서는 검찰에서 별도로 디지털증거업무관리시스템(D-NET)에 등록하지 않는다.

2-2 검찰 - 경찰 간 송부

검찰에서 경찰로 수사기록 반환 시(수사중지, 불송치, 보완수사 등은 반환하는 절차 있음을 각주로), 사건 송부 담당 경찰관이 검찰청에서 관계서류와 증거물을 인수하고 있다. 이때도 검찰청에 디지털증거를 인계하는 경우와 마찬가지로 증거물인 정보저장매체의 존재 여부만 확인할 뿐, 인수한 개별 파일에 대한 해시값을 확인하는 절차를 규정하고 있지는 않고 있다.[56]

3. 디지털증거 송부에 관한 문제점[57]

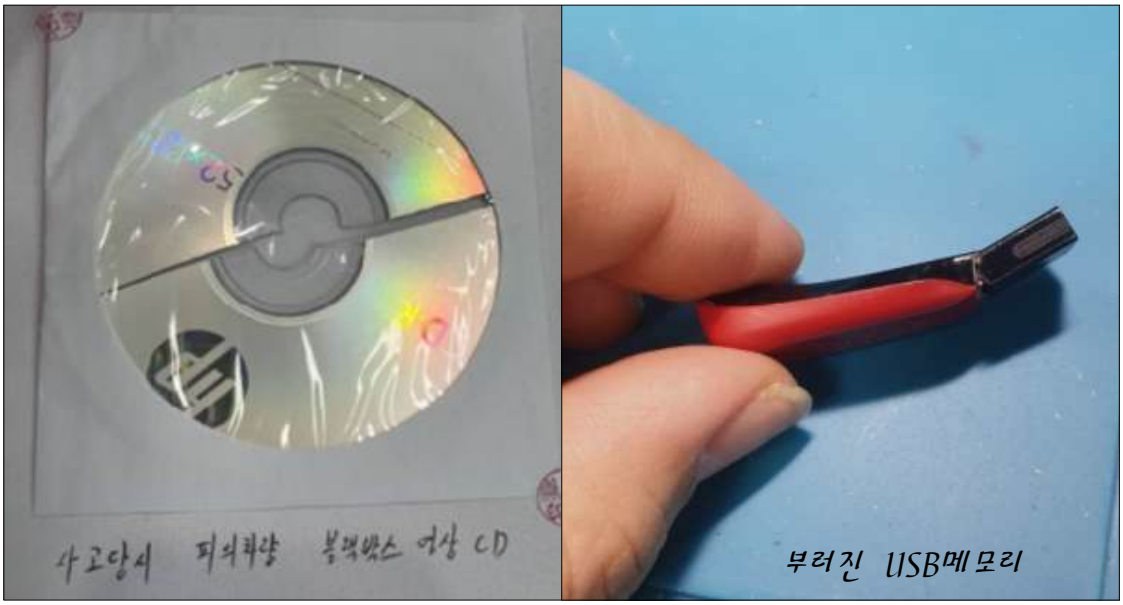
위와 같이 검찰 디지털증거 예규 및 경찰청 디지털증거 훈령에 디지털증거에 대한 수집・분석・보관・관리 등의 절차에만 언급하고 있을 뿐, 형사사법기관 간 디지털증거물 전송 방식에 대한 내용은 확인되지 않는다. 그래서 디지털증거물을 정보저장매체에 보관해 기록 편철 또는 출력하여 송부하고 있어 많은 문제점이 발생하고 있다.

---

55) 김일권·김기범. (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 185.
56) 정웅길·이상진. (2022). 경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안. 디지털포렌식연구, 132.
57) 김일권·김기범, (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 186.

첫째, 복사·복제가 잦아져 디지털증거에 대한 정보통제가 어려워지고 있다. 수사 - 송치 - 보완수사-송치-공소제기여부결정 - 공소제기 - 공판 - 형 집행 등 형사소송 전체 과정을 통해 다수의 업무PC에 디지털증거가 저장 될 수 있어 정보통제가 어렵고 디지털증거 유출 가능성이 높으며, 음란물·국가기밀 등 보안이 중요한 증거도 실행·복사·복제 과정에서 유출 가능성이 높아질 수 있다.

둘째, 디지털증거의 손망실·훼손이 우려된다. 형사사법기관 간 송부하는 과정에서 손망실·훼손이 발생할 수 있으며, 시간이 경과할 수록 정보저장매체의 내구성이 떨어져 보관의 문제가 발생한다.



<그림 27> 송부 과정상 물리적 손상된 디지털증거 정보저장매체

위 그림과 같이 디지털증거 송부 과정에서 정보저장매체 자체가 손상되어 디지털증거물 자체가 사라지는 사례도 발생하고 있다.

셋째, 불송치 결정에 대한 이의신청 기한을 별도로 규정하고 있지 아니하다. 이는 사법경찰관의 불송치 결정에 대해 수년이 경과한 후에나 사건이 재기되는 절차를 진행할 때 최초 수집한 디지털증거물이 훼손되어 혐의유무 판단에 커다란 문제가 될 수 있다.

경찰청 훈령인 「디지털증거의 처리 등에 관한 규칙」 제35조 제3항에 의하면 “경찰관은 사건을 이송 또는 송치한 경우 수사 과정에서 생성한 디지털증거의 복사본을 지체 없이 삭제·폐기하여야 한다”고 규정하고 있다. 같은 규칙 제36조에 의하면 “입건 전 조사편철(구 내사편철)·관리미제 사건에 등록한 사건에서 압수한 전자정보는 압수를 계속할 필요가 있는 경우 해당 사건의 공소시효 만료일까지 보관 후 삭제·폐기하고, 압수를 계속할 필요가 없다고 인정되는 경우 삭제·폐기한다”고 규정하고 있다. 그런데 형사소송법이 개정되면서 새로 생긴 절차인 불송치 결정에 대한 디지털증거 보관·삭제·폐기 규정은 없으며, 이의신청, 재수사요청, 시정조치 요구 시 디지털증거의 보관・삭제・폐기 관련 규정도 존재하지 않고 이의신청 기한이 없다는 이유로, 경찰은 불송치 결정으로 사건이 종결된 것으로 간주하고, 디지털증거를 삭제·폐기하였다가 수사 재개 시 증거로 사용하지 못하는 문제가 발생하는 것이다.[58]

넷째, 디지털증거를 단순 출력만 하고 포렌식 이미지 생성 및 해시값을 확인하는 등의 절차가 없을 경우, 출력으로 인한 증거의 소실이 발생할 수 있다. 문서 또는 멀티미디어 전자정보의 특정 부분을 선별하여 이를 출력할 경우 파일의 속성값인 메타데이터가 사라지기 때문에 증거로서 활용가치가 떨어질 수 있기 때문이다.

다섯째, 관리 연계성(Chain of custody) 입증이 어렵다. 형사사법기관 간 정보저장매체에 대한 입·출고, 보관, 송부, 작동 여부 등 각 단계마다 기록을 유지하여야 하는데, 수사와 공판 과정에서 봉인・봉인해제・재봉인이 반복적으로 일어나고, 많은 소송관계인들이 직・간접적으로 개입하게 되어 관리 연계성에 대한 입증 부담이 계속 커지고 있다.

58) 정웅길·이상진, (2022). 경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안. 디지털포렌식연구, 136.

제 4 장 디지털증거의 보관 및 관리 방안

제 1 절 디지털증거 포렌식 이미지 생성과 보존

1. 포렌식 이미지 생성 및 보존의 필요성

디지털증거의 성격에서 비가시성・비가독성・잠재성으로 인하여 0과 1로 구성되어 있어 내용을 파악하기 위해서는 일정한 하드웨어나 소프트웨어로 구성된 변환장치를 사용하여야 사람이 인식할 수 있게 된다. 취약성으로 인하여 디지털증거의 수정・삭제・변경・조작이 용이하고 또한 증거 보존 과정에서도 시스템 내의 파일들에 변화가 일어날 수도 있게 된다. 이에 더하여 복제용이성・매체독립성 때문에 원본과 사본에 대한 구별이 불가능할 수도 있다. 이와 같은 디지털증거의 성격 때문에 무결성・신뢰성・동일성・진정성이라는 일정한 증거능력 요건을 충족하였다는 전제하에 디지털증거는 증거로서 가치를 가지는 법정 증거가 되는 것이다. 대법원은 '대법원 2007. 12. 13. 선고 2007도7257 판결'(소위 일심회 사건)이나 '대법원 2013. 7. 26. 선고 2013도2511 판결'(소위 왕재산 사건)에서 무결성・동일성 인정 여부로 디지털증거의 증거능력 유무를 판단하였던 것이다.

디지털증거 생성에 관하여 검토하면서 압축 파일은 디지털증거를 보관하기에 ①압축 파일 내부에 보관된 파일의 인위적 개작・편집의 가능성, ②악성코드 및 바이러스 등에 노출의 위험성, ③메타데이터 복원의 한계, ④압수 당시 파일시스템 등 재현 및 검증에 한계가 있음을 살펴보았다.

이와 달리, 포렌식 이미지는 ①디지털포렌식 툴이 아니고서는 접근에 제한이 있고, ②일반적인 디지털포렌식 툴에서는 이미지 내부 파일을 임의로 편집할 수 없으며, ③포렌식 이미지 내부에 있는 파일은 외부에서 악성코드 또는 바이러스로부터 안전하게 보호할 수 있고, ④이미지 내부에 보관된 디지털증거를 압수 당시 기준으로 재현하여 복원할 때 디지털증거의 메타데이터까지 원본과 완전히 동일하게 복원이 가능하여 ⑤포렌식 이미지를 최초 디지털증거 수집 당시로부터 상당기간 경과한 이후에도

해시값 계산에 의한 검증으로 동일성과 무결성 담보를 위한 완전한 재현·검증이 가능하다는 장점이 있음을 확인하였다.

특히 디지털증거 증거능력 요건 중 진정성은 디지털증거의 수집에서 보존까지를 다루는 문제이고, 무결성 또는 동일성은 디지털증거 수집과 보존을 포함하여 이를 분석하고, 법정에 제출하는 등 전 과정에 걸친 문제로 파악되어야 하는 관점[59]에서 보면, 디지털증거가 컴퓨터 기술에 의하여 내용이 편집·조작될 위험성이 있는 등 그 취약성이 드러나므로 디지털포렌식 전 과정에 걸쳐 무결성·신뢰성·동일성·진정성 등을 담보하는 절차를 요구하게 되었다. 이와 같은 사정을 반영하여 경찰에서 최초 디지털증거 수집 시 현재처럼 압수된 전자정보 파일들을 한 개의 압축파일로 묶어 생성하는 것은 디지털증거 증거능력 요건에 부적합하므로 전문적인 디지털포렌식 분석툴을 사용하여 포렌식 이미지를 생성하는 것이 필요하다.

경찰은 전자문서인 디지털증거를 CD/DVD/USB메모리 등의 매체에만 보관하면서 주임검사 또는 사법경찰관이 전자문서를 엑셀 프로그램으로 열어보는 그 자체만으로도 그 해시값이 변경되어 이러한 전자문서 파일이 그대로 법정에 제출되면서 무결성·동일성을 담보하지 못한 점을 이유로 고등법원에 사건을 파기환송한 사례에서 살펴보았듯 피압수자에게 교부한 전자정보 상세목록상 해시값과 동일한 전자정보로 재현이 가능한 포렌식 이미지 생성이 반드시 필요하다는 것을 깨닫게 하는 것이라고 볼 수 있다.

2. 포렌식 이미지 생성 방안

2-1. 경찰 디지털증거 수집 시 포렌식 이미지 미생성 이유

경찰은 실무상 압수·수색 현장에 대한 디지털포렌식 지원 인력의 한계로 수사를 담당하는 수사관이 컴퓨터 등 정보저장매체를 대상으로 직접 탐색·선별함으로써 디지털증거를 수집하고 있는 실정이다. 더불어 디지털증거 수집에 활용되고 있는 분석툴은 경찰 내부적으로 제작한 툴을 사

59) 양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 박사학위논문, 경희대학교(2006), 217.

용하고 이렇게 수집된 전자정보를 1개의 압축파일을 생성하고 이에 대한 해시값을 계산하여 피압수자에게 교부하는 방식을 채택하고 있다. 전문적인 교육훈련을 받고 경험이 축적된 디지털포렌식 전문가 한 두 명이 압수·수색 현장에서 현장지원을 하고 있는 현재 관행의 한계에서는 디지털포렌식 전문가에 의한 디지털증거 수집의 신뢰성을 확보하기에 어려움이 있을 것이다. 또한 압축파일로 생성한 압수 전자정보는 전문 분석툴을 사용하였는지 그 분석 도구에 대한 신뢰성에 의문을 제기하지 않을 수 없다.

위와 같이 명시한 바와 같이 경찰이 디지털증거 수집 시 포렌식 이미지를 생성하지 않는 이유를 정리해보면, ①경찰청 디지털증거 훈령에서 디지털증거 압수 시 각 개별 파일의 파일명과 해시값을 전자정보 상세목록에 기재하여 피압수자에게 교부하도록 하는 규정은 있으나, 포렌식 이미지를 생성해야 하는 규정의 미비 때문이다. ②경찰 디지털포렌식 인력 풀의 한계로 압수 현장에서 컴퓨터 등 정보저장매체에 대한 압수·수색은 사건을 담당하는 수사관이 직접 수행하는 현실에 있다. ③경찰에서 디지털증거 수집에 사용하는 분석툴이 포렌식 이미징을 정상적으로 수행하기 어렵고 그만큼 신뢰도가 낮기 때문으로 보인다. ④공판을 수행하지 않는 경찰 특성상 공판에서 디지털증거 재현·검증을 수행하는 경우가 적기 때문에 포렌식 이미지 생성의 필요성에 대한 인식이 부족하다는 점 때문이다.

2-2. 포렌식 이미지 생성에 의한 디지털증거 수집 방안

디지털포렌식 전문가에 대한 신뢰성, 디지털포렌식 분석툴에 대한 신뢰성 같은 문제를 해결하는 방안은 다음과 같다.

첫째, 경찰 디지털포렌식 인력 풀을 대거 확보하여 디지털포렌식 전문가에 의한 디지털포렌식 압수·수색을 실시하거나, 현직 경찰관을 대상으로 일정 기간 의무적으로 디지털포렌식 분석툴 사용에 대한 교육훈련을 실시하여 자격을 부여하고 이렇게 자격이 부여된 경찰관에 한하여 디지털포렌식 압수·수색 업무를 수행할 수 있도록 하는 것이다.

둘째, 포렌식 이미지를 생성할 수 있는 전문적인 분석툴을 사용하여 전자정보를 탐색·선별하고, 이에 대한 포렌식 이미지를 생성한다. 검찰 등 공공기관에서 사용하면서 그 신뢰성이 법원 판례에서 인정된 CFT 분석툴을 사용하거나, 최근 검찰 등에서 주로 사용하고 있는 DFT 툴을 사용할 수도 있고, 포렌식 이미지 생성이 가능한 상용 분석툴을 사용하는 것이다.

셋째, 포렌식 이미지 생성에 의해 디지털증거를 확보한 뒤 송치 또는 불송치 등 수사 종결 과정에서도 포렌식 이미지를 적극 보존하는 것이다. 수사관의 판단에 따라 증거로 사용하기로 한 파일만을 대상으로 하드카피로 출력하고 압수·수색 과정에서 확보한 전자정보가 잘 보존되지 않는 경우가 많기 때문이다. 디지털증거에 대한 압수조서를 작성 시 포렌식 이미지를 대상으로 하여 실물에 대한 압수와 동일시하여 디지털증거가 누락되지 않도록 하여야 할 것이다.

제 2 절 디지털증거 보관 전용 클라우드 서버의 구축

1. 디지털증거 보관 클라우드 서버 구축

1-1. 불송치 디지털증거의 불완전성

경찰 수사 사건은 사건 처분 결과에 상관없이 디지털증거는 불완전한 상태에 처해진다. 사건을 검찰에 송치 결정 시에는 디지털증거는 송치받은 검찰청으로 수사기록과 함께 송부되고, 이송결정 시에는 다른 경찰서·수사기관·군검찰·군사경찰 등으로 송부된다. 송치 또는 이송 결정은 현재 수사가 완결된 상태에서 송부되므로 그나마 디지털증거에 대한 훼손 가능성이 낮겠지만, 불송치 디지털증거는 경찰서 기록 창고에 보관되고, 언제든 이의신청 또는 피의자·참고인의 소재발견 등으로 사건이 재기되어 재수사 되어 검찰에 송치될 수 있는 등 그 지위는 불완전한 상태일 수밖에 없다. 불송치 상태 기록 창고에 보관 중에도 정보저장매체에 저장된 디지털증거는 물리적 훼손 가능성과 자기장에 의한 손망실 가능성

이 있고, 컴퓨터로 정보저장매체를 접속하는 과정에서 실수로 삭제·편집·개작 등의 가능성이 존재하는 것이다.

경찰은 수사실무에서 디지털증거는 CD/DVD/USB메모리 등 매체에 저장하여 이를 A4 크기 용지의 수사기록에 편철하여 보관하고 있다. 이는 경찰·검찰·수사기관·법원 등에 수사기록이 송치·불송치·이송·이첩·영장청구·열람등사 등 다양한 사유로 정보저장매체 자체가 물리적으로 훼손될 가능성이 높고 사법경찰관·검사·판사 등이 기록 검토 중에 의도치 않게 전자정보 자체가 삭제 또는 훼손의 가능성이 존재하게 되는 것이다. 이는 곧 비가시성, 취약성, 변조 가능성, 복제 용이성 등의 디지털증거의 특성이 그대로 노출되는 문제점을 초래하게 된다. 만약 디지털증거가 유일하게 CD 매체 1장에 보관되었는데, 이러한 CD 매체에 물리적 훼손이 발생할 경우 수사기관은 신뢰를 잃을 것이고, 결국 이러한 일이 반복된다면 국가 형사사법시스템에 대한 신뢰가 온전히 유지되기 어려울 것이다. CD 매체에 대한 물리적 훼손을 예방하기는 어려우나, 물리적 훼손에도 불구하고 별도 장소에서 완전히 동일한 백업 디지털증거 데이터가 보관·관리되고 있다면 신뢰를 잃을 가능성은 거의 없게 될 것이다.

형사 사건의 98%를 경찰 단계에서 수사개시하고 있을 뿐만 아니라 개정 형사사법시스템상 일부 사건에 대해서도 경찰에서 수사 개시하는 현실을 고려한다면, 경찰 단계에서 피해자·고소인·고발인·참고인·피의자로부터 확보한 디지털증거는 경찰 외 기관으로 적게는 수 회에서 많게는 수십 회 정도가 이동하게 되므로 디지털증거가 보관된 정보저장매체에 대한 훼손가능성을 염두에 두고 신뢰성을 확보할 방안을 찾아야 한다.

1-2. 디지털증거 보관 클라우드(가칭: Pol-Cloud) 서버 구축 방안

불송치 디지털증거의 불완전성에 따른 배경에서 예기치 못한 손망실 상황을 예방할 수 있는 가장 좋은 방법은 경찰 디지털증거 보관 및 관리 전용 클라우드 서버를 구축하는 것이다. 경찰 디지털증거를 클라우드에 보관 및 관리하는 방안은 몇 차례 연구된 사례가 있다.

특히 정웅길·이상진의 “경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안”에서 클라우드 DaaS 도입에 따른 디지털증거 관리시스템을 구축하여야 한다고 하였다. 디지털증거는 네트워크를 통해 송부하는 것이 시대적 흐름이자 관리 연속성 등 디지털증거의 증거능력을 유지할 수 있는 방법이다. 디지털증거를 시스템에 저장할 수 있는 용량, 전송속도 등 문제를 해결할 수 있는 가장 좋은 방법은 클라우드 시스템을 활용하는 것이다. 현재 행정안전부는 고비용의 물리적 망분리 방식에서 서버 가상화 방식의 클라우드 DaaS(Datacenter as a Service, 서비스로의 데이터센터) 형태로 전환 준비 중이다. DaaS는 ‘연속성’. ‘경제성’. ‘보안성’. ‘관리 편의성’ 등 특징을 가지고 있다.. DaaS는 기업의 업무망을 중앙의 가상화된 서버에 조성하여, 직원 개인 PC에 화면만 전송하는 기술로, 개인의 접속 단말은 보안에 취약할지라도, 중앙 업무망에는 영향을 받지 않아 보안성에 강하다. 향후 업무망 PC에서 클라우드 DaaS를 이용해 인터넷을 이용할 수 있는 시스템이 구축된다면, 디지털증거 수집 단계부터 디지털증거에 대한 보안성과 무결성이 담보될 수 있어 증거능력이 유지될 수 있으며, 디지털증거 송치표준화의 큰 걸림돌인 저장용량 및 전송속도 문제도 해결될 수 있을 것이다. 그리고 일반 행정 업무와 달리 경찰 업무는 보안상 민간 클라우드의 활용이 어려울 수 있으니, 국가정보자원관리원 내에 경찰청 전용 클라우드존 구성을 추진할 필요가 있다고 언급하였다.

디지털증거 수집 시부터 클라우드 서버에 보관하는 가장 대표적인 곳은 대검찰청 디지털수사통합업무관리시스템(이하 'D-NET')으로 볼 수 있다. 이는 대검찰청 디지털증거 예규 제41조에 따라 포렌식 이미지 생성 등의 방법으로 압수·수색을 종료한 디지털포렌식 수사관이 포렌식 이미지, 그 추출파일, 해시값, 전자정보 상세목록 등을 D-NET에 등록하는 절차이다.

제41조(현장에서 압수한 디지털 증거의 등록) ① 디지털포렌식 수사관은 지원을 종료하고 복귀한 후 지체 없이 제20조제1항에 따라 압수한 디지털 증거(이미지 파일, 증거파일을 포함한다)와 그 해시값을 업무관리시스템에 등록한다. ② 제1항의 경우 현장에서 압수목록 이외에 전자정보 상세목록을 교부한 때에는 그 전자정보 상세목록을 업무관리시스템에 등록한다.

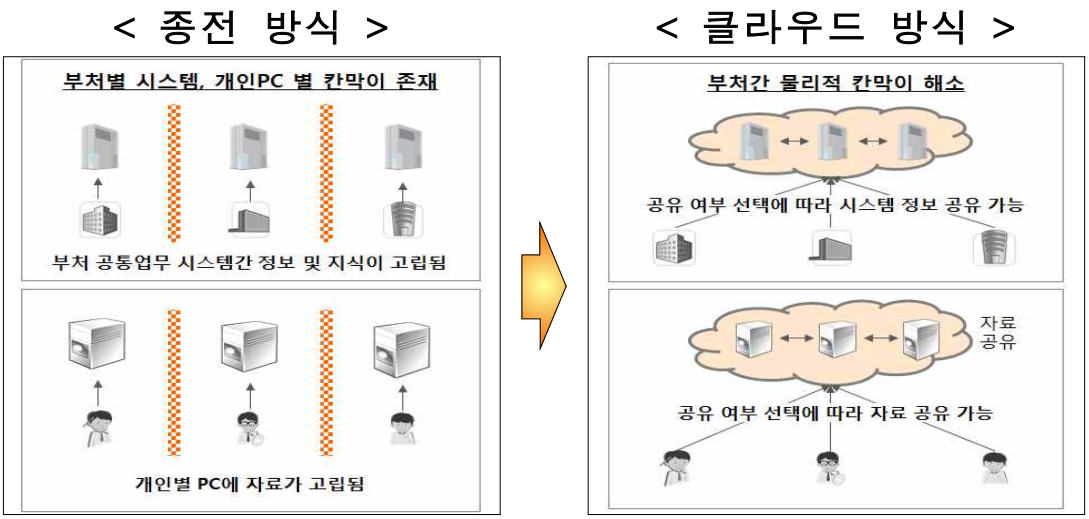
<표 17> 대검찰청 예규 제41조 D-NET에 디지털증거 등록

검찰의 D-NET 서버에 디지털증거를 등록하고 이를 보관·관리하는 방식은 디지털증거를 보다 더 안전하게 유지 관리할 수 있고 디지털증거의 증거능력 요건인 무결성에서 진정성을 담보하는 데까지 그 장점이 유지될 수 있다. 가령 공판에 디지털증거 제출이 필요할 경우 검찰 디지털증거 보관·관리에서 살핀 바와 같이 서버에 보관되면서 자동으로 생성된 압수조서, 디지털증거 보관확인서만을 사건기록에 편철하면 되고, 공판정에서 디지털증거에 대한 제출을 명령할 경우에는 대상 디지털증거를 대상으로 보관확인서에 대한 증거번호를 확인하고, 검찰 지휘 결재권자 및 인권보호관의 검토를 거쳐 대검찰청 디지털수사과장으로부터 권한을 승인받아 디지털증거를 별도 정보저장매체에 보존하여 이를 법정에 제출할 수 있게 된다. 대검찰청 D-NET뿐만 아니라 수사실무상 직접 증거로 사용하는 경우에는 증거로 제출할 전자정보는 별도 CD/DVD/USB메모리 등으로 보존하여 이를 법정에 제출하고 있는데 이러한 수사실무상 관행은 D-NET과 사건기록에 편철 보관하는 방식은 증거보관의 이중화는 디지털증거 보관 및 관리의 합리적 방안이라고 볼 수 있다.

검찰에서 D-NET을 통하여 디지털증거를 체계적으로 보관·관리하는 점을 벤치마킹하여 볼 때 정웅길·이상진의 “경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안”에서 경찰의 디지털증거를 클라우드 디지털증거 관리시스템을 구축하여 보관·관리하는 방식은 매우 합리적이라고 볼 수 있다. 다만, 대검찰청의 클라우드 서버를 구축하는 방식은 다양하나, 개인정보가 응축되어 있고, 기업의 비밀 또는 국가안보에 관한 전자정보가 응축되어 구성되는 디지털증거 특성을 반영하면, 경찰에서 검찰 또는 다른 수사기관 등으로 인계·인수 과정에 보안성을 확보하는 방안이 매우 중요하다. 이에 보안성 유지라는 목적을 고려하면 경찰 디지털증거를 논스톱으로 대검찰청 D-NET에 송신하기에는 기술적 한계가 있다. D-NET은 외부 네트워크와 단절된 검찰 내부 인트라넷 구조이기 때문이다. 그렇다고 D-NET을 인터넷과 연결하기에는 보안 취약성이 생기기 때문에 사실상 불가능하고, 경찰로부터 송부받은 디지털증거 보관을 위해 별도 서버를 구축하기에는 D-NET의 이중화로 경제성과 업무효율성이 있어 보이지도 않아 보인다.

그런데 국가기관 간 정보통신업무는 온나라 시스템을 활용하는 인트라넷 구조이고, 행정안전부에서 2018년부터 클라우드 온-나라 시스템 고도화 사업에 따라 각 기관이 생산하는 보고서, 문서 등을 클라우드에 통합 저장·활용하는 방식으로 기관 간 협업과 소통이 가능한 구조[60]이기 때문에 이를 디지털증거 보관 및 관리에 활용하는 것이 합리적이라 볼 수 있다.

60) 행정안전부 보도자료 2018. 4. 26. 정부 클라우드 온-나라 확산으로 혁신 기틀 마련 - 행안부, 24개 기관 클라우드 기반 온-나라 시스템 전환 완료 -

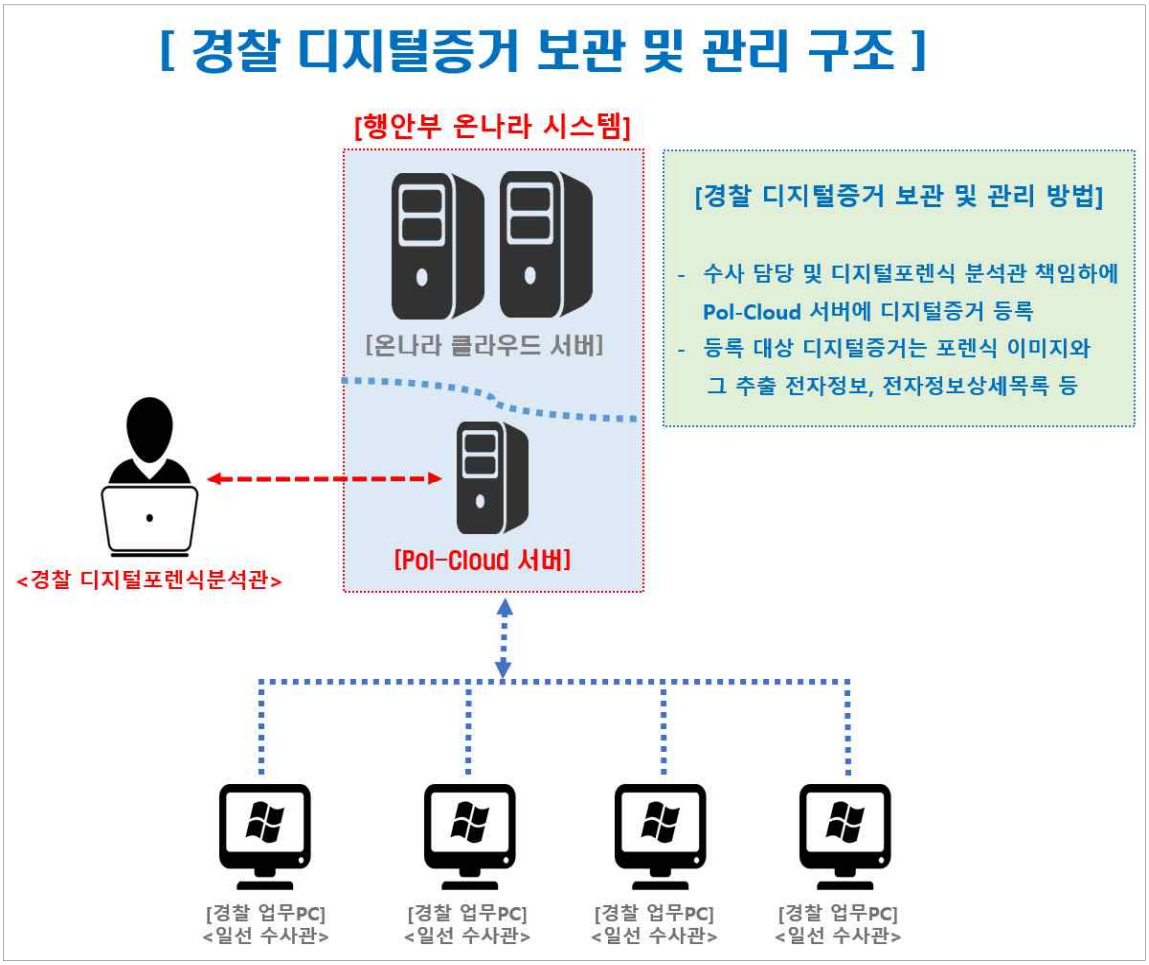


<그림 28> 행정안전부 클라우드 온-나라 고도화 사업 구조[61]

이는 경찰 디지털증거를 행정안전부 온나라 클라우드 서버의 일부를 경찰디지털증거업무관리시스템(이하 'Pol-Cloud 서버')으로 사용하는 것이다. 행정안전부에서 기존 구축된 온나라 클라우드 서버에 Pol-Cloud 서버라는 명칭으로 추가하기 때문에 경제성이라는 이점이 있을 뿐 아니라 다음과 같은 점에서 매우 활용가치가 높다고 볼 수 있다.

첫째, 온나라 시스템은 국가기관 어디서든 인증된 업무PC로 접속이 가능하다. 둘째, 온나라 클라우드망은 인터넷과 분리되어 있으므로 보안 취약성이 낮다. 디지털증거 인계·인수 과정은 국가기관 간 보안성·네트워크 연계성이 중요하기 때문에 이러한 점을 반영하여 경찰-검찰 간 인계·인수 방안을 설계하는 것도 필요하다고 보기 때문이다.

61) 행정안전부 보도자료 2018. 4. 26.(주 60)



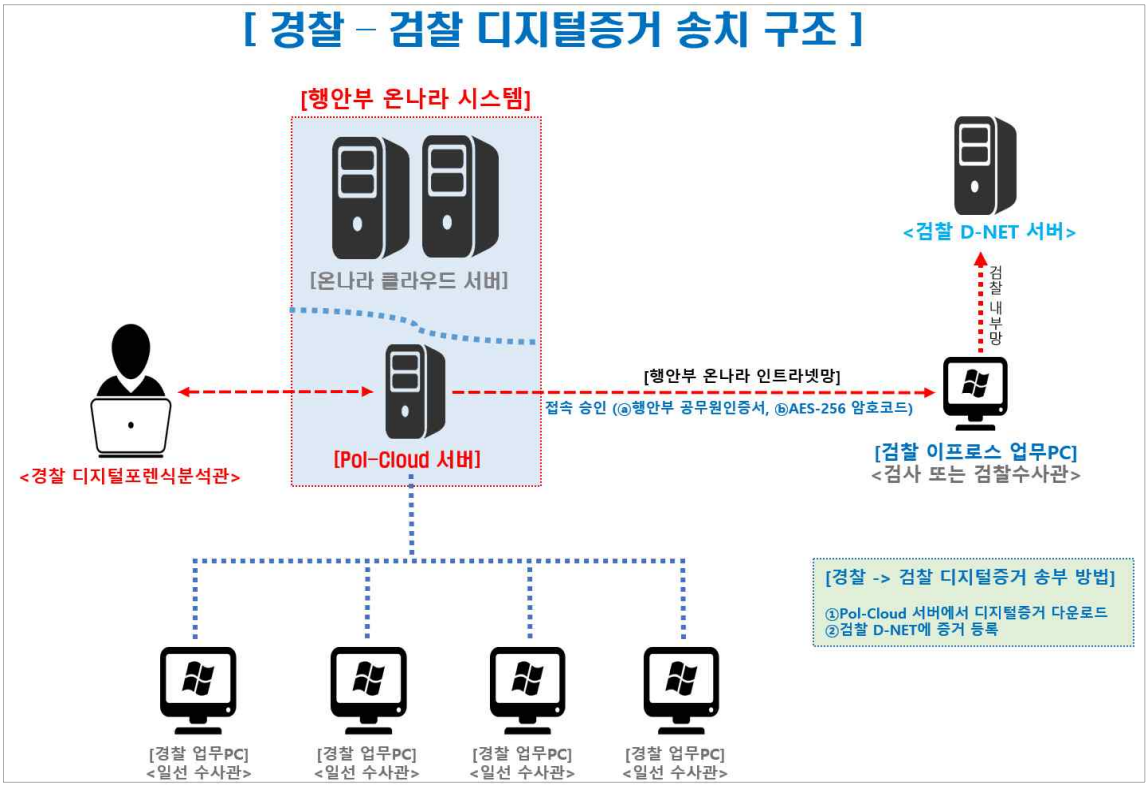
<그림 29> 경찰 디지털증거 보관 및 관리 구조

위와 같이 디지털증거 증거능력 요건을 살펴보았는바, <그림 29>와 같이 경찰 디지털증거 보관 및 관리 구조를 제안한다. 이는 경찰 수사 담당 및 디지털포렌식 분석관 책임하에 수사 과정에서 확보한 디지털증거를 Pol-Cloud 서버에 등록하는 것이다. 특히 그 등록 대상은 디지털포렌식 압수·수색 과정에서 확보한 포렌식 이미지와 그 추출 전자정보, 전자정보 상세목록 등을 포함한다. 송치 여부는 최종 수사가 종결된 이후의 문제로 수사 과정에서는 이를 정확히 예상하기란 어려운 일이므로 송치 여부를 불문하고 위와 같은 방식으로 Pol-Cloud 서버에 디지털증거를 보관하도록 하여야 한다.

2. 불송치 사건 송치 시 디지털증거 관리

경찰에서 불송치 사건을 재기하여 사건을 검찰에 송치할 경우, 경찰 디지털증거를 행정안전부 온나라 클라우드 서버의 일부인 Pol-Cloud 서버에 보관 중이므로 비교적 간단히 행안부 온나라 인트라넷망을 통해 디지털증거 송치가 가능하다. 경찰과 검찰은 모두 온나라 클라우드 서버에 접속 가능한 인트라넷을 사용하고 있기에 보안 취약성이 낮고 행정안전부의 공무원인증서를 통해 사용자 인증이 가능하고, 수사기록과 형사사법정보시스템(KICS)을 활용하여 AES-256[62] 암호화 코드를 생성하여 이를 입력하는 방법으로 인증도 간편하기 때문이다. 이렇게 인증받아 경찰로부터 송부받은 디지털증거를 검사는 검찰 내부망을 통해 검찰 D-NET에 디지털증거 등록도 가능하기 때문에 경찰-검찰 간 별도 서버 시스템과 네트워크를 갖추지 않고도 디지털증거 송치 체계를 갖출 수 있는 것이다.

62)AES(Advanced Encryption Standard, 고급 암호화 표준)는 미국 표준 기술연구소(NIST)에 의해 제청된 대칭키 방식의 암호 저장 기술로써, 데이터 블록의 길이가 128bit이며, 키의 길이가 128bit, 192bit, 256bit 3가지인 알고리즘이다. 키의 길이가 길수록 암호화 과정에서 경우의 수가 많아지므로 보안 강도가 높습니다. AES-256bit는 알파벳, 전각, 기호, 특수문자 등 PC에서 사용 가능한 모든 입력 방식을 암호로 사용할 수 있다.([네이버 지식백과] AES-256bit)



<그림 30> 경찰 - 검찰 디지털증거 송치 구조

경찰의 디지털증거 보관 및 관리를 위해 <그림 30>과 같이 '경찰 - 검찰 디지털증거 송치 구조'를 제안한다. 이는 경찰 내부적으로는 온나라 클라우드의 일부인 Pol-Cloud 서버를 이용해 업무PC에서 디지털증거를 보관 및 관리하는 것이고, 경찰 외부적으로는 검찰에 송치할 경우를 상정해 국가기관에서 사용하는 온나라 인트라넷망을 통해 디지털증거를 검찰에 송부하는 구조인 것이다.

예를 들어, 경찰이 Pol-Cloud 서버에 보관하고 있는 불송치 사건의 디지털증거 사건에서 피의자 소재발견으로 사건 재기 후 수사가 종결되고 이를 기소의견으로 검찰에 송치 시 이를 송치받는 검사는 1차적으로 이프로스 업무PC에서 인트라넷 내부망을 통해 온나라 클라우드의 Pol-Cloud 서버에 공무원 인증서 비밀번호를 통해 접속하고, 2차적으로 수사기록 및 형사사법시스템(KICS)에서 확인된 AES-256으로 암호화된 암호코드를 Pol-Cloud 서버에 입력하여 디지털증거를 다운로드 후 이를 바로 대검찰청 D-NET에 등록하는 방식인 것이다.

검찰에서 온나라 인트라넷 내부망을 행안부 공무원인증서로 접속하고, 수사기록 및 KICS에서 확인된 AES-256 암호코드를 입력하여 접속하는 보안단계는 디지털증거에 대한 보안성 유지를 위해 필요하다. 더불어 이렇게 확보한 디지털증거를 대검찰청 D-NET에 등록하는 단계는 향후 법정 제출여지가 높은 디지털증거에 대한 무결성과 진정성을 담보하고 별도로 수사기록에 정보저장매체에 보관된 디지털증거의 훼손 가능성을 대비하는 차원에서도 필요하다.

경찰에서 검찰에 송치 완료 후의 디지털증거에 관해 살펴본다. 불송치에 따른 디지털증거 관리는 온전히 경찰 사무에 해당한다. 그러나 송치결정이 이뤄진 때에는 상황이 완전히 달라진다. 사법경찰관이 검사에게 사건을 송치할 경우 검사의 보완수사요구로 수사기록이 사법경찰관에게 반환되는 때를 제외하고는 사실상 사법경찰관의 수사권한은 종결되는 것이나 마찬가지이다. 그러나 이때도 검사가 사법경찰관에게 보완수사요구를 통해 사건 일부 사항에 대한 사법경찰관의 검토 및 수사재개가 있을 수 있고, 검사의 공소제기 등으로 다양한 사유가 발생할 수도 있으므로 디지털증거에 대한 보관 및 관리는 일정기간 동안은 불완전한 상황이기 마련이다.

경찰 송치 처분이 있더라도 검사의 요구에 의한 사법경찰관의 보완수사 과정에서도 디지털증거가 필요한 상황이므로 사법경찰관이 송치 결정한 날로부터 보완수사요구에 의한 수사 기간 동안만큼은 경찰이 디지털증거를 보관할 필요가 있다. 보완수사가 종결되면서부터는 온전히 검사에게 수사 및 공소제기여부를 결정하는 권한이 있으므로 송치가 완료된 후 일정 기간 후에는 경찰에서 보관 중인 디지털증거는 삭제·폐기하는 것이 타당하다.

결국 경찰의 송치 결정 처분이 완료하고, 검사가 사건 관련 디지털증거를 Pol-Cloud 서버에서 송부받은 때로부터 6개월의 경과기간을 두고, 사

건 담당 경찰이 특별히 송치 결정한 디지털증거를 계속하여 보관한다는 조치를 취하지 아니하면 경찰 Pol-Cloud 서버에 보관 중인 디지털증거는 자동으로 삭제·폐기하도록 하여야 한다.

이와 같이 송치 결정된 디지털증거에 대해 삭제·폐기가 필요한 이유는 경찰 클라우드 서버 운영관리에 관한 경제성도 고려하여야 하기 때문이다. 경찰 디지털증거 분석 통계에 의하면 2018년 45,103건, 2019년 56,440건, 2022년 63,935건으로 확인되고 디지털증거 분석 건수와 그 보관 및 관리할 디지털증거 용량은 기하급수적으로 증가하고 있으므로 경찰 단계에서 사건이 종결되었고, 검찰 D-NET에 송부가 완료되어 이중 보관된 디지털증거에 대해서만큼은 삭제·폐기하는 것이 반드시 필요한 것이다.

제 3 절 관련 법제도의 개선

1. 포렌식 이미지 생성에 관한 규정 신설

1-1. 포렌식 이미지 생성 및 해시값 확인 원칙

경찰청 디지털증거 훈령에는 이미지 생성에 관한 규정이 없다. 그러나 위에서 살펴본 바와 같이 사건과 관련 있는 전자정보 자체를 별다른 조치 없이 단순 복제하는 방식으로 압수할 경우 그 보관 및 관리에 디지털증거 훼손 가능성이 존재한다. 실무상 수행되는 바와 같이 전자정보 묶음 방식의 압축(ZIP) 파일 형태로 보관 시 디지털증거에 대한 인위적인 편집이 가능하고 악성코드 공격에 취약하게 된다. 이러한 점을 고려하여 현재까지는 비교적 무결성·진정성·동일성·신뢰성·관리 연속성 등을 담보하도록 사건과 관련 있는 디지털증거를 이미지(Image) 파일 형태로 생성하고 이에 대한 해시값을 확인하는 방식으로 증거를 보관하고 관리함이 타당하다. 따라서 이러한 점을 고려하여 경찰청 디지털증거 훈령상 사건과 관련 있는 디지털증거 압수 시 포렌식 이미지(Image)를 생성하고 이에 대한 해시값을 확인하여 압수함을 원칙으로 하는 규정을 신설하는 것이다.

위와 같이 대법원 판결 사례에서 살펴보았듯 디지털증거의 재현·검증뿐만 아니라 디지털포렌식 무결성과 신뢰성을 담보하기 위해 다음과 같이 디지털증거에 대한 포렌식 이미지 생성을 원칙으로 하는 규정 신설이 필요하다.

제00조(포렌식 이미지 생성에 의한 압수) ①범죄사실 관련 디지털증거는 포렌식 이미지(Image)를 생성하고 이에 대한 해시값을 확인하여 압수한다. ②제1항과 같이 포렌식 이미지 생성에 의한 방법으로는 디지털증거를 수집하기에 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우 디지털증거에 대한 무결성·진정성·동일성·신뢰성·관리 연속성 등을 고려하여 범죄사실 관련 전자정보 자체 및 그 해시값을 확인하여 압수하거나 기타 전자정보 묶음 방식의 압축파일 형태 등으로 압수할 수 있다. ③제1항 내지 제2항에 의해 압수된 디지털증거의 목록과 해시값이 기재된 전자정보 상세목록을 작성하여 이를 피압수자에게 교부한다.

<표 18> 포렌식 이미지 생성에 의한 압수 원칙 신설 규정 제안

이미지 생성 및 해시값 확인에 의한 디지털증거를 수집하는 것을 원칙으로 하고, 현재의 경찰 실무와 현장의 다양한 상황을 고려하여 예외적으로 디지털포렌식 분석관 및 사법경찰관리의 판단하에 전자정보 자체(해시값 확인 포함) 또는 압축 파일(해시값 확인 포함)에 의한 압수를 수행하는 것이다.

1-2. 예외적으로 다른 방법으로 보관 방법 규정

포렌식 이미지를 모든 경우에 생성하기 어려울 수 있다. 이런 경우에는 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 곤란한 경우, 디지털증거에 대한 무결성·진정성·동일성·신뢰성·관리 연속성 등을 고려하여 전자정보 자체 및 그 해시값을 확인하여 압수하거나 기타 전자정보 묶음 방식의 압축 파일 형태 등으로 압수할 수 있다는 예외 규정을 둘 수 있다. 이는 디지털포렌식 분석관 또는 담당 수사관의 현장 상황 판단하에 수행하게 함으로써, 까다로운 규정 때문에 압수의 목적을 달성하지 못하는 상황이 발생하지 않도록 함이다.

2. 경찰 디지털증거 폴클라우드 서버 보관 규정 신설

2-1. 디지털증거 폴클라우드 서버에 보관

경찰은 디지털증거 훈령에 디지털증거는 폴클라우드 서버에 보관함을 원칙으로 하는 규정 신설 제안한다. 특히 서버에 증거 등록 시 포렌식 이미지, 그 추출 전자정보, 전자정보 상세목록 등을 등록하도록 하는 것이다.

제00조(압수한 디지털증거 등록) ①사법경찰관리 또는 디지털포렌식 분석관은 압수한 디지털증거(포렌식 이미지, 관련 추출 증거파일을 포함한다)와 그 해시값을 경찰 디지털증거 업무관리시스템(이하 'Pol-Cloud 서버'라 한다)에 등록한다. ②제1항에서 등록한 디지털증거에 대한 전자정보 상세목록과 이와 관련된 전자정보를 Pol-Cloud 서버에 등록한다.

<표 19> 디지털증거 폴클라우드 서버 등록 신설 규정 제안

2-2. 경찰 - 검찰 디지털증거 송치 방법 규정 신설

경찰이 사건을 검사에게 송치하기로 결정한 경우, 온나라 클라우드의 Pol-Cloud 서버에 보관 중인 디지털증거를 검사에게 온나라 인트라넷망을 통하여 송부한다. 이때 사건을 송치받은 검사는 1차적으로 행정안전부 공무원인증서 로그인을 통하여 인증을 받고, 2차적으로 수사기록 및 형사사법정보시스템(KICS)에서 AES-256 암호화 코드를 확인하고 이를 Pol-Cloud 서버에 접속 인증을 받아 송부한다.

제00조(경찰-검찰 디지털증거 송부 방법) ①사건 담당 사법경찰관은 검사에게 사건을 송치할 경우 디지털증거는 Pol-Cloud 서버에서 온나라 인트라넷망을 통하여 보안에 유의하여 송부한다. ②제1항과 같이 사건을 송치받은 검사는 1차적으로 행정안전부 공무원인증서에 의한 방법으로 인증을 받고, 2차적으로 수사기록 및 형사사법정보시스템(KICS)에서 AES-256 암호화 코드를 확인하는 방식으로 Pol-Cloud 서버에 접속 인증을 받도록 하여 디지털증거를 송부한다.

<표 20> 디지털증거 송치 방법 신설 규정 제안

2-3. 디지털증거 보관・삭제・폐기 기간 규정 신설

불송치 및 송치 시별로 보관 기간, 삭제・폐기 원칙, 보관 특례 사항 등을 구체적으로 규정할 필요가 있다. 경찰 단계 불송치는 개정 형사소송법 시행 전에는 검찰 단계에서 불기소에 해당하는 처분과 그 유사성이 있으나, 고소인・피해자 등의 이의신청이나 검사의 위법・부당성에 대한 판단으로 송치될 가능성이 존재한다. 특히 이의신청 기간은 법률상 별도로 규정하고 있지 않아 공소시효가 완성되기까지는 언제든 송치가 가능한 상황이다. 또한 피의자 또는 참고인의 소재불명에 따른 수사중지의 경우, 수년에서 수십 년이 경과하여 소재가 발견될 경우가 있고 이는 사건이 재기되어 기소의견으로 검찰에 송치될 가능성이 매우 높다는 특징이 있다. 더불어 불송치 디지털증거는 수사중지, 공소권없음, 혐의없음 등 다양한 이유로 불송치하고 있으나 다른 수사기관, 특별검사 또는 법원 등에서 문서송부촉탁, 열람・등사, 다른 사건에서 피해자 진술 확보, 기타 공익적 필요에 의한 증거상 가치로 불송치되어 경찰 보존 창고에서 잠자고 있다고 하여 그 증거가치가 완전히 사라졌다고 보기에도 어렵다는 특징이 있다.

불송치된 디지털증거는 수사기록과 동일하거나 그 이상의 보존 기간을 설정함이 타당한 것으로 보이는데, 검찰 디지털증거 예규에 따르면 검찰 디지털증거업무관리시스템(D-NET)에 보존된 디지털증거는 공소시효 완성 시까지 보존하나, 구체적이고 다양한 사유로 10년, 준영구, 영구 기간 보존의 근거를 마련하고 있는 점에 비춰보면, 경찰의 불송치 디지털증거 역시 이에 준하여 보존함이 타당하다.

경찰의 불송치 수사기록이 공소시효 완성 시를 기준으로 보존기간을 설정하기 때문에 디지털증거 역시 공소시효 완성 시를 기준으로 함이 타당하나, 국외도피 및 공범의 공판으로 인한 공소시효 완성 기간 계산에 착오가 있을 수 있다는 점을 고려하여 수사기록 폐기 후 1년의 경과 기간을 두어 디지털증거를 삭제・폐기하는 것이 필요하며, 이 역시 매년 수사기록 데이터베이스와 디지털증거 데이터베이스 간 보존 상태를 비교 후 삭제・폐기한다면 착오에 의한 폐기될 가능성은 현저히 낮아질 것으로 판단된다.

제00조(불송치 사건의 디지털증거의 삭제·폐기) ①불송치 사건의 디지털증거는 수사기록이 폐기된 해에서 1년의 경과 기간을 두고 일괄 삭제·폐기한다. 디지털증거에 대한 삭제·폐기를 담당하는 직원은 디지털증거 삭제·폐기 전에 해당 사건기록 데이터베이스와 디지털증거의 데이터베이스 간 보존상태를 비교하여 삭제·폐기하여 착오에 의한 삭제·폐기가 되지 않도록 주의한다.

<표 21> 불송치 디지털증거 삭제·폐기 신설 규정 제안

위와 같이 정기적으로 디지털증거를 삭제·폐기하는 주요한 이유는 사건처분 시 피압수자 등의 인권보호를 위함에도 있지만, 경찰이 절대 다수의 사건을 수사개시하고 있어 지속적인 클라우드 서버 증축이 필요하게 되므로, 서버 증축의 경제성을 고려하지 않을 수 없기 때문이다.

디지털증거 보관 클라우드 서버 구축 항목에서 보완수사 기간 등을 고려하여 사건 송치 시 디지털증거 보관 기간은 6개월이 타당한 것으로 보았으므로 송치 후 6개월간 보관하고 그 이후는 삭제하는 규정을 신설한다.

제00조(송치 사건의 디지털증거의 삭제·폐기) ①송치 사건의 디지털증거는 경찰의 송치 결정 처분이 완료하고, 송치받은 검사가 사건 관련 디지털증거를 Pol-Cloud 서버로부터 송부받은 때로부터 6개월의 경과기간을 두고 Pol-Cloud 서버에서 자동으로 삭제·폐기한다, 다만, 사건 담당 사법경찰관리가 송치결정한 디지털증거를 특별히 계속하여 보관하는 조치를 취하면 그 필요 기간까지 보관하고 이후 삭제·폐기한다.

<표 22> 송치 사건의 디지털증거 삭제·폐기 신설 규정 제안

제 5 장 결론

2022. 10. 15. 카카오(포털 및 인터넷 정보매개 서비스업) 데이터 센터에 불이 나면서 대부분의 플랫폼 서비스가 마비되고, 국민 대부분의 생활이 마비되는 등 디지털 기기는 우리 일상생활에서 떼려야 뗄 수 없는 존재가 되었다. 디지털 기기를 일상에서 만연하게 사용함에 따라 디지털 정보는 과거부터 현재까지 데이터가 저장되고, 기기에 저장된 메시지, 사진, 위치 정보 등 디지털 정보는 형사소송법상 증거 활용에 매우 중요한 단서 역할을 하고 있다.

과거에는 대부분의 증거물은 유체물인 것에 반해 현재는 대부분의 증거물은 디지털 기기에 저장되어 있는 디지털 정보로, 디지털 포렌식이 없으면 사건이 해결되지 않을 정도로 중요한 절차가 되었다.

디지털증거물은 기존 유체물인 증거물과는 달리 비가시성·비가독성·잠재성·취약성·복제용이성·매체독립성·대량성·휘발성 등 취약한 성질을 가지고 있으므로, 디지털증거가 증거능력을 인정받아 법정에서 증거로 사용하기 위해서는 증거 수집 절차의 적법성 확보뿐만 아니라 진정성·무결성·원본성·신뢰성·관리연속성 등이 담보되어야 한다.

현재 경찰은 수사실무상 디지털증거물은 압축 파일로 디지털증거를 확보하고 보관하므로, ①압축 파일 내부에 보관된 파일의 인위적 개작·편집의 가능성, ②악성코드 및 바이러스 등에 노출의 위험성, ③메타데이터 복원의 한계, ④압수 당시 파일시스템 등 재현 및 검증에 한계가 있음을 확인하였다.

이와 달리, 포렌식 이미지는 ①디지털포렌식 툴이 아니고서는 접근에 제한이 있고, ②일반적인 디지털포렌식 툴에서는 이미지 내부 파일을 임의로 편집할 수 없으며, ③포렌식 이미지 내부에 있는 파일은 외부에서 악

성코드 또는 바이러스로부터 안전하게 보호할 수 있고, ④이미지 내부에 보관된 디지털증거를 압수 당시 기준으로 재현하여 복원할 때 디지털증거의 메타데이터까지 원본과 완전히 동일하게 복원이 가능하여 ⑤포렌식 이미지를 최초 디지털증거 수집 당시로부터 상당기간 경과한 이후에도 해시값 계산에 의한 검증으로 동일성과 무결성 담보를 위한 완전한 재현·검증이 가능하다는 장점이 있음을 확인하였다.

2021. 1. 1. 형사소송법 개정으로 '불송치'라는 경찰에 수사종결권을 부여하는 새로운 절차가 생겼다. 소재불명에 따른 수사중지, 증거부족 등에 따라 사건이 송치되지 않음으로써 기록과 증거물을 경찰에서 보관하게 되는 큰 변화가 생겼다. 하지만 경찰의 결정에 불복하는 '이의신청' 절차도 함께 신설되었는데, 이는 이의신청 기간이 별도로 명시되어 있지 않아 언제든 사건이 재개되어 검찰에 송치될 수 있다.

하지만 경찰 수사실무상 디지털증거는 CD·DVD 등 저장매체 등에 저장하여 수사기록에만 편철하여 보관하고 있다. 이는 기관 간 기록 이동 시 저장매체가 물리적으로 훼손될 가능성이 높고, 기록 검토 중에 의도치 않게 전자정보가 훼손될 가능성이 존재한다. 이는 디지털증거의 취약한 특성이 그대로 노출되는 문제점을 확인할 수 있다.

저장매체에 대한 물리적 훼손을 예방과 경찰 수사과정에서 처분은 예상하기 어려우므로, 송치·불송치를 불문하고 경찰은 수사 담당 및 디지털포렌식 분석관 책임 하에 디지털포렌식 압수·수색 과정에서 확보한 포렌식 이미지와 그 추출 전자정보 상세목록 등의 디지털증거를 폴클라우드 서버에 등록하여 디지털증거물을 보관·관리하도록 하여야 한다. 이렇게 별도 장소에 완전한 동일한 백업 디지털증거 데이터가 보관·관리되고 있다면 훼손에 따른 디지털증거 신뢰성을 잃을 가능성은 거의 없을 것이다.

경찰 클라우드 서버 운영관리에 관한 경제성, 그리고 피압수자의 인권보장을 위해서 송치 완료된 사건, 공소시효 완성된 사건 등의 불필요한

디지털증거는 삭제·폐기가 필요하다. 경찰의 불송치 수사기록이 공소시효 완성 시를 기준으로 보존기간을 설정하기 때문에, 디지털증거도 공소시효 완성 시를 기준으로 폐기를 함이 타당하다. 하지만 공소시효 완성 기간 계산에 착오가 있을 수 있으므로 수사기록 폐기 후 1년의 경과 기간을 두어 삭제·폐기하되, 매년 수사기록 데이터베이스와 디지털증거 데이터베이스 간 보존 상태를 비교 후 삭제·폐기한다면 착오에 의한 폐기될 가능성은 현저히 낮아질 것으로 판단된다.

위와 같은 디지털포렌식 절차는 포렌식 이미지 생성, 경찰 디지털증거 Pol-Cloud 서버 보관 및 관리, 디지털증거 보관・삭제・폐기 기간을 규정하여 법제를 완비한다면 경찰 디지털증거의 무결성・신뢰성・동일성・진정성・관리 연속성 등을 담보하기에 충분하리라 판단한다.

참 고 문 헌

형사소송법[시행 2021. 1. 1.] [법률 제16924호, 2020. 2. 4., 일부개정] 【제정·개정 이유】 전문

정웅길·이상진. (2022). 경 · 검 수사권 조정에 따른 디지털증거 인수 · 인계 과정상 증거능력 유지방안. 디지털포렌식연구, 127.

양근원, (2006). “형사절차상 디지털증거의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위 논문, 20-21.

손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 37-38.

탁희성·이상진, 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보 방안, 한국형사정책연구원(2006), 35., 손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 26-27.

탁희성·이상진, (2006). 디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보 방안, 한국형사정책연구원, 36-37.

양근원, (2006). “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 박사학위 논문, 경희대학교, 22.

손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 26.

손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 30.

대법원 2013. 6. 13. 2012도16001 판결

양근원, (2006). “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위 논문, 20-21.

손지영·김주석, (2015). 디지털 증거의 증거능력 판단에 관한 연구, 대법원 사법정책연구원, 36.

이주호·이태명, (2020). 디지털증거의 선별압수에 따른 원본성 및 동일성 증명에 관한 연구.디지털포렌식연구. 252-268.

손지영·김주석, (2015). “디지털 증거의 증거능력 판단에 관한 연구”, 사법정책연구원, 35-36.

이정인, (2019). ‘디지털증거의 관리연속성과 적법절차의 원리에 관한 연구, 서울대학교 석사학위 논문, 27.

Zatyko, Ken; “Commentary: Defining Digital Forensics,” Forensic Magazine, 2 January 2007, www.forensicmag.com/articles/2007/01/commentary-defining-digital-forensics

손지영·김주석, (2015). 디지털 증거의 증거능력 판단에 관한 연구, 대법원 사법정책연구원, 46.
정병준·한재혁·이상진, (2017). 손상된 ZIP 파일 복구 기법, 고려대학교 정보보호대학원, 1109-1110.
대법원 2013. 6. 13. 2012도16001 판결
대법원 2017. 1. 25. 선고 2016도13489 판결
대법원 2017. 12. 5. 선고 2017도13458 판결
대법원 2020. 2. 13. 선고 2019도14341, 2019전도130 판결
대법원 2022. 2. 17., 선고, 2019도4938 판결
대법원 2022. 1. 27. 선고, 2021도11170 판결
대검찰청 디지털증거 예규 별지 13호 전자정보 압수・수색・검증 안내문
http://forensic-proof.com/archives/3613
대검찰청 예규, “디지털 증거의 수집·분석 및 관리 규정” 별지 13호 전자정보 압수・수색・검증 안내문
대통령령, “검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정” 제42조 제2항
대검찰청 예규, “디지털 증거의 수집·분석 및 관리 규정” 제52조
대검찰청 예규, “디지털 증거의 수집·분석 및 관리 규정” 제57조
장진, (2021). 수사과정에서 확보한 디지털증거 관리 방안 연구, 23.
정웅길·이상진, (2022). 검·경 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지 방안, 130.
신지호·최낙범, (2016). 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구, 경찰, 242.
경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제23조 제1항
경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제23조 제2항
정웅길·이상진, (2022). 검·경 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지 방안, 131.
경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제34조
경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제35조
경찰청 훈령, “디지털증거의 처리 등에 관한 규칙” 제36조
인천경찰청 보도자료, 인천경찰청 디지털성범죄 피해자 보호・지원 강화, 2021. 9. 5.
신지호·최낙범, (2016). 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구, 240.
경찰청, 2021년 경찰백서, 206
http://www.koit.co.kr/news/articleView.html?idxno=89644
경찰청 보도자료, 경찰청 제3기 디지털포렌식 자문위원 위촉, 2022. 10. 25.
김일권·김기범. (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연

구, 184.
정웅길·이상진. (2022). 경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안. 디지털포렌식연구, 132.
김일권·김기범. (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 184.
김일권·김기범. (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 185.
정웅길·이상진. (2022). 경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안. 디지털포렌식연구, 132.
김일권·김기범, (2017). 형사사법기관의 디지털증거전송체계 도입방안. 형사정책연구, 186.
정웅길·이상진, (2022). 경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안. 디지털포렌식연구, 136.
양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 박사학위 논문, 경희대학교(2006), 217.
행정안전부 보도자료 2018. 4. 26. 정부 클라우드 온-나라 확산으로 혁신 기틀 마련 - 행안부, 24개 기관 클라우드 기반 온-나라 시스템 전환 완료 -
행정안전부 보도자료 2018. 4. 26.(주 60)

Abstract

A Study on the Storage and Management of the Digital Evidence by the Police disposition of the Non-indictment opinion

Kim, Younghyun
Department of Mathematical
Information Science
The Graduate School
Seoul National University

Under criminal law, digital evidence can be granted legal evidence only when integrity, authenticity, identity, reliability, and management continuity are guaranteed due to weaknesses such as invisibility, vulnerability, modulation, ease of replication, and large scale. Nevertheless, despite the high possibility of damage to digital evidence, it has not gotten out of the old convention in which digital evidence is kept on the investigation

paper files with the storage media such as CD/DVD/USB memory. This has changed from the method of the storing the criminal investigation paper files to the prosecutor's office preservation department to the method of separately between the police and prosecutor storing and managing the investigation paper files, which cannot be denied that there is a risk of managing the stored digital evidence.

In particular, the police's disposition of the Non-indictment opinion, which are closed due to suspension of investigation due to unknown whereabouts of suspects or witnesses, lack of evidence, lack of sufficient evidence, or lack of right to indict, lost the public's trust in the criminal evidence system if the digital evidence is damaged. Accordingly, I suggest that the police shall establish a new regulation that requires the seizure of digital evidence in the form of forensic image files and check hash values to ensure integrity, authenticity, identity, reliability, and management continuity of digital evidence by storing all kinds of digital evidence in the police digital evidence cloud server (tentative name: Pol-Cloud). In principle, the digital evidence of the Police's disposition of the Non-indictment opinion should be kept until the next year when the statute of limitations is completed, but if a decision to send the investigation paper files to the prosecutor's office with the indictment opinion is made later, a new regulation is established to preserve it until the next year when the judicial police officer's supplementary investigation is completed. This will

enable sustainable evidence retention in anticipation of the advantage of reducing the ever-increasing cost of deploying server data storage.

If digital evidence is stored in one forensic image file from the stage of gathering the digital evidence as above and managed to a police digital evidence cloud server (tentative name: Pol-Cloud), it is expected for police to overcome the weaknesses of digital evidence, and ultimately enhance the police's trust in integrity, integrity, identity, reliability, and continuity.

keywords : Police disposition of the Non-indictment opinion, Digital evidence, forensic image, Pol-Cloud
Student Number : 202123755