

디지털증거 확보체계

이인수*

요약

정보저장매체에 저장된 디지털정보로부터 범죄 단서를 찾고, 법정에서 증거로 제출하기 위한 일련의 활동을 일컫는 디지털 포렌식의 개념과 기법이 국내 수사기관에 도입되어 활용된 지 10여년의 시간이 흘렀다. 그러나 디지털증거라는 새로운 개념의 탄생은 최근까지 정보의 압수대상 여부 논란 등 수사실무에서의 혼란을 초래하고 있다. 기존 증거와 구별되는 디지털 정보의 특성으로 말미암아 증거로 활용함에 있어 필요한 별도의 절차적·기술적 조건이 요구되고 있으나, 과거 규정과 지침만으로는 디지털증거를 취급함에 있어 해석, 처리의 혼선을 가져 왔으며, 아직 명확하고 구체적인 실무 지침과 규정은 마련되지 못하고 있는 실정이다. 디지털증거 확보체계는 이러한 혼선을 최소화하기 위해 디지털증거의 증거능력 유지를 위해 필요한 최소한의 요건을 정의하고, 이를 바탕으로 법정 제출시까지 동일성, 무결성과 이를 증명하기 위한 보관연속성(Chain of Custody) 등을 유지 관리하기 위해 수사기관간에 구축하고 있는 인프라 시스템이다.

본 고에서는 수사기관간의 디지털정보, 디지털증거 처리, 유통, 취급에 있어 문제점을 살펴보고, 이를 보완 개선하기 위한 그간의 노력과 향후 발전방향에 대해 고찰해 보고자 한다.

I. 서론

컴퓨터 및 정보통신기술은 업무환경뿐만 아니라 일상생활에도 많은 변화를 초래하였으며, 정보의 소통과 저장, 보관방식에도 변화를 가져왔다. 대부분의 정보가 디지털형태로 기록, 저장, 소통되고 있으며 범죄관련 정보도 다양한 정보저장매체에 저장되고 있다. 따라서 범죄수사 환경 또한 변화를 요구받고 있다. 이에 수사기관은 자백과 종이서류 중심의 전통적 수사방식에서 증거 재판주의에 따른 법률 환경 변화와 더불어 다양한 정보 저장매체에 저장된 디지털정보로부터 증거를 확보하여 범죄 단서를 찾고 증거능력을 유지하기 위한 새로운 수사기법과 환경에 대한 연구개발과 표준절차 마련 등 대응책 마련에 고심하고 있다.

디지털포렌식은 정보저장매체에 저장된 디지털정보를 바탕으로 정보를 획득, 분석, 결과보고에 이르는 과정으로 수행된다¹⁾. 압수 또는 임의제출 방식으로 획득

된 디지털정보를 증거로 활용하기 위해 증거능력을 유지하고자 하는 별도의 조치와 노력이 필요하게 된다.

우리나라는 2012.1.1. 형사소송법 개정을 통해 제106조 제3항, 제4항에 디지털증거와 관련된 조항이 추가되었으며²⁾, 2015.7.16. 2011모1839 대법원 전원합의체 결정을 계기로 서울중앙지법에서는 전자정보를 압수대상으로 한정하고, 참여권 보장, 무관정보의 삭제, 폐기 의무를 포함한 실무운영 개선방안을 발표하였다³⁾. 최근 2016.5.29.형소법 제313조⁴⁾ 개정으로 디지털증거

1) 각 저장매체나 운영체제 등 디지털정보를 처리, 분석, 취급하는 기술적 특성에 따라 컴퓨터포렌식, 모바일포렌식, 데이터베이스포렌식, 네트워크포렌식 등으로 구분하기도 하나, 이러한 매체중심 기술 특성에 기반한 분류는 기술 환경 변화에 따라 향후 지속적으로 확장, 병합될 것으로 보인다.

2) 형사소송법 제106조(압수) ③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체" 등"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.> ④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011.7.18.>

3) 2015.7.18. 서울중앙지방법원 보도자료

4) 제313조(진술서등) ② 제1항 본문에도 불구하고 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진

의 진정 성립 인정요건이 새롭게 정의되는 등 디지털증거의 취급, 해석과 관련된 다양한 노력이 이루어지고 있으나, 기존 압수물 관리지침은 물건(유체물)을 중심으로 기술되어 있어 전자정보(디지털증거)의 관리, 처리에 실무적 어려움과 혼선은 여전히 지속되고 있다.

디지털증거는 수사의 성패를 가늠할 정도로 그 중요성이 부각되고 있으나, 프라이버시 침해 가능성 등 다양한 논란의 중심에 서 있다. 실체적 진실발견과 인권보호라는 두 측면에서 균형과 조화를 위한 논의의 축을 기준으로 표준절차와 전문기술을 접목시키고자 노력하고 있으나, 아직 디지털정보의 대량성, 잠재성 등으로 인권 침해 가능성에 따른 균형점을 찾기 위한 명확한 기술적 방안은 제시하고 있지는 못한 실정이다.

이와 더불어 디지털정보의 취약성으로 말미암아 취급과정에서의 부주의는 범죄 증거의 증거능력 훼손과 직결되고, 이는 공소유지에도 심각한 장애요소로 대두되고 있으나⁴⁾, 아직 일선 수사현장에서의 주의와 노력은 부족한 것이 현실이다. 각 수사기관은 이러한 환경 변화에 대응하기 위해 전문 인력 양성, 연구개발 등 다양한 노력을 경주하고 있으나, 예산과 인력 부족 등으로 대응체계 마련이 쉽지 않은 상태이다. 기존 수사 조직의 인력, 절차, 지침, 규정, 운용시스템 등에 대한 변화와 개선을 통해 일선 수사현장에서의 인식 제고, 전문도구 확충 또한 시급히 해결되어야 할 당면 과제이다.

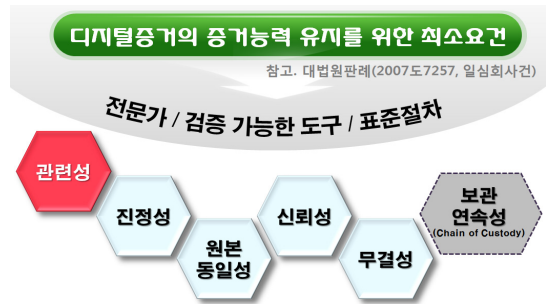
본 고에서는 절차적 측면에서 증거능력 유지를 위해 필요한 최소 요건을 정의하고, 절차관리와 증거관리 측면에서 원본동일성, 무결성, 보관연속성 유지 및 관리방안과 디지털증거데이터팩 표준규격⁵⁾을 소개하고, 이를 기반으로 한 디지털증거 확보체계의 구축현황을 살펴본다.

II. 디지털증거의 증거능력 확보 기본요건

대한민국의 수사기관은 검찰과 사법경찰, 특별사법경찰로 이루어져 있으며, 검사의 지휘에 따라⁶⁾ 사법경찰

술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있을 것을 요한다. <개정 2016.5.29.>

- 4) 서울중앙지법 2014.4.25.선고 2013고합805호 판결
- 5) 디지털증거데이터패키지 KS x 1220
- 6) 형사소송법 제196조(사법경찰관리) ① 수사관, 경무관, 총경, 경정, 경감, 경위는 사법경찰관으로서 모든 수사에 관하여 검사의 지휘를 받는다. ③ 사법경찰관리는 검사의 지휘가 있는 때에는 이에 따라야 한다. 검사의 지



(그림 1) 디지털증거의 증거능력 유지 요건

찰과 특별사법경찰이 수사를 하고, 검사⁷⁾는 사건을 송치 받거나, 직접 수사를 한 후, 검사가 공소제기, 불기소, 또는 이송결정 등을 한다.⁸⁾ 일련의 수사과정에서 확보된 디지털증거는 검찰로 송치되어야 한다.⁹⁾

디지털증거는 압수수색에서 법정제출까지 디지털증거의 처리, 취급에 관한 엄격한 절차관리와 증거의 손상, 훼손방지 등을 위한 관리가 담보될 필요가 있다.

강제수사 또는 임의수사로 확보된 디지털증거는 수사의 결정적 단서가 되는 경우가 많으며, 이러한 디지털증거의 증거능력 유지는 수사 성패 및 공소 유지의 매우 중요한 요소로 대두되고 있다. 즉, 디지털정보의 특성에 따른 요건 이외도 법적 요건 충족을 위해 원본동일성, 무결성, 보관연속성(Chain of Custody), 진정성, 관련성, 신뢰성, 적법성 등 다양한 조건을 충족시키기 위한 노력이 수반되어야 한다.

수사기관은 증거능력 유지를 위해 각 요건을 충족시키고 해당 요건이 법정 제출까지 유지되도록 관리하여야 하며, 확보과정, 송치과정, 이후의 취급과정 등 전 과정에서 요구되는 기술적, 절차적인 매우 까다로운 절차와 요건을 충족시키도록 노력하여야 하고, 증거능력이 훼손되지 않도록 별도의 세심한 주의와 조치를 마련하여야 한다.¹⁰⁾

위에 관한 구체적 사항은 대통령령으로 정한다.

- 7) 형사소송법 제195조(검사의 수사) 검사는 범죄의 혐의 있다고 사료되는 때에는 범인, 범죄사실과 증거를 수사하여야 한다.
- 8) 형사소송법 제246조(국가소추주의) 공소는 검사가 제기하여 수행한다.
- 9) 형사소송법 제196조(사법경찰관리) ② 사법경찰관은 범죄의 혐의가 있다고 인식하는 때에는 범인, 범죄사실과 증거에 관하여 수사를 개시·진행하여야 한다. ④ 사법경찰관은 범죄를 수사한 때에는 관계 서류와 증거물을 지체 없이 검사에게 송부하여야 한다.
- 10) 형사소송법 제131조(주의사항) 압수물에 대하여는 그

지금까지 대부분의 연구와 논의는 디지털증거 자체의 특성에 기인한 요건을 기준으로 개별 수사기관내에서의 디지털증거 취급시 대응방안에 대해서만 고찰되어 온 것이 사실이다. 기관내의 실무 규정, 지침의 부족, 부재와 더불어 개별 수사기관내에서만 문제로 국한됨으로써 수사기관간 디지털증거 송치과정 및 이후의 관리, 취급, 처분 과정 등 전체 생명주기에 대한 관리에서는 심각한 공백이 발생하고 있다.

Ⅲ. 디지털증거의 취급 및 관리 현황

지난 시간 디지털증거가 압수물인가? 아닌가? 라는 논란 속에 있었다¹¹⁾. 그로 인한 실무적 혼선은 디지털증거를 취급하는 다양한 과정에서 노출되어 디지털증거 관리의 공백을 초래하였다. 그러나 최근 법원은 2015년 8월 실무지침을 통해 전자정보를 압수대상으로 명시함으로써 저장매체가 아닌 디지털증거를 압수물로 취급되고 관리하도록 요구하고 있다¹²⁾.

최근 디지털증거의 압수수색, 증거분석 등 관련업무가 폭증하고 있으며, 각 수사기관은 현실에 따라 자체적으로 조직 정비 및 도구 확보, 연구개발 등 대책마련에 고심하고 있다. 2012년 검찰은 디지털포렌식유관기관 협의체를 구성하여 수사기관간의 디지털증거 수집 기법 및 유의사항 공유, 최신 기술동향 및 우수사례 공유 등을 추진하고 있다.



(그림 2) 디지털증거 처리 절차

3.1. 현장에서의 조치 및 디지털증거 확보

디지털정보의 압수는 출력 또는 복제를 원칙으로 하

상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 한다.

- 11) 제106조(압수) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. <개정 2011.7.18.> * 현 형사소송법에서는 정보가 압수물에 포함되는 지에 대한 명확한 규정이 존재하고 있지 않다.
- 12) 2015.7.18. 서울중앙지방법원 보도자료

고 있다. 복제의 경우, 현장에서 사건 관련성 정보(유관 정보)를 선별한 후, 원본 디지털정보와 사본 디지털정보를 대상으로 암호학적 해시함수로 각각의 해시값을 계산하고 상호 비교한 후, 원본동일성 검증을 거쳐 해당 해시값이 기록된 확인서에 참관인의 서명을 받은 후, 압수된 전자정보의 상세목록을 교부한다. 예외적으로 원본 저장매체를 압수한 경우에는 저장매체를 봉인하고 압수목록을 교부하며, 디지털포렌식 업무담당부서로 이송하여 이해 당사자의 참관 하에 봉인을 해제하고 유관 정보를 선별 추출하는 복제를 통한 전자정보 압수 절차를 따른다.

암호학적 해시함수는 무결성 유지와 원본동일성 유지의 중요한 기술적 요소로 활용되고 있으며, 현재 가장 비용 효율적이고 안전한 방법으로 인식되고 활용되고 있다. 과거 원본성은 유체물인 매체를 중심으로 정의되고 있었으나, 디지털증거측면에서는 매체독립성 등의 특성으로 정보의 원본성과 진정성 입증에 필요하다. 또한 디지털 정보는 변조가 용이한 특성으로 압수시점부터의 변개, 조작 등의 논란에 휩싸일 수 있다. 따라서 봉인 또는 해시값을 받는 것은 디지털증거의 증거능력 유지의 시작점이고 가장 중요한 절차 중 하나이다. 참관이 이루어지지 못하는 상황에서는 저장매체의 봉인해제, 재봉인 과정 등을 녹화하거나 사진 촬영 등을 통해 기록을 남겨 두고 있다.

이 후 법정 제출까지의 무결성 보장을 위해 획득시 동일성 확인에 사용된 해시값을 보존하고, 디지털증거 획득과정의 해시값과 법정 제출된 디지털증거의 해시값을 비교하여 제출된 디지털증거와 확보된 이후 디지털증거가 수사과정에서 변경되지 않았음을 즉, 동일, 무결함을 증명한다. 또한 혹 발생할 수 있는 디지털증거의 훼손 가능성에 대한 대비책 마련 필요에 따라 확보된 디지털증거의 획득(압수수색 또는 임의제출)에서 법정 제출시까지 각 단계에서의 담당자, 책임자를 명확히 기록 관리하여 사후 검증이 가능하도록 관리하여야 한다. 즉, 보관연속성 또한 증거능력 유지에 필요한 중요한 요소 중 하나이다.

디지털증거의 경우, 현장에서의 조치, 처리 미흡은 수사 전 과정의 노력을 수포로 만드는 결과를 초래하므로 각별히 주의할 필요가 있다. 디지털포렌식의 과정은 전문도구를 통해 수행된다. 따라서 검증된 전문 도구가 필요하다. 최근 전문도구가 일반인도 쉽게 사용할 수 있

도록 개발되고 있어 디지털포렌식 기본소양 교육, 도구 사용교육 등을 통해 일반수사관도 직접 디지털증거를 확보하는 방안 등을 마련하여 디지털포렌식의 일반화에 따른 인력의 배치와 효율적 활용에 대한 재해석이 필요한 시점이다. 즉, 단순 파일의 압수와 처리과정은 고도의 전문성이 필요하다고 볼 수 없으며, 로그분석, 메타 정보 분석, 안티포렌식 대응 등 피의자의 행위를 분석하는 영역 등에 국한하여 전문 인력을 활용하는 등 인력 운영의 다변화가 필요하다.

3.2. 수사기관내에서의 처리

[처리, 송치, 수리단계]

압수 또는 임의제출된 디지털증거는 각 기관의 상향에 따라 새로운 별도의 관리시스템을 통해 관리하거나, 기존 관리시스템 내의 일부로 관리되고 있다. 기존 관리시스템에 의한 처리는 무체물인 디지털증거를 관리하는데 한계가 있고 필요 정보의 누락 등이 발생할 수 있어 별도의 관리시스템 구축을 통해 디지털증거의 보관 연속성 유지 등의 조치가 시급한 상태이다.

압수된 디지털증거는 압수조서와 압수물 총목록과 함께 검찰로 송치된다. 이때 원본 저장매체 자체를 송치하거나 사본 저장매체에 디지털증거를 복제하여 송치하기도 하나, 디지털정보의 출력물이 기록물에만 편철되고, 디지털증거는 송치되지 않는 경우도 있다. 기록물에 편철된 출력물의 경우 원본 동일성, 무결성 등의 논란과 압수물의 처분에서 환부 등에 있어 곤란한 문제에 봉착된다. 송치되는 디지털증거는 수리기준 부재로 기재 누락 및 입력 오류뿐만 아니라 압수물총목록과 압수조서간의 기재목록이 달라 압수물 수리가 거부되는 등 일선의 혼선이 가중되고 있으며, 원본 저장매체, 사본 저장매체의 식별조차 제대로 이루어지지 못하고 있다. 송치사건의 경우, 동일성, 무결성 등 디지털증거의 증거능력을 유지하기 위한 절차 미비나 전문도구 사용률이 극히 저조하여 법정에서 증거능력이 부정되는 사례 또한 발생되고 있으며, 사경, 특사경 및 일선검찰청의 담당자에 따라 처리방식 또한 상이한 상태이다. 2014년 11월 디지털증거를 취급함에 있어 사본 증거와 관련 부가정보를 하나의 데이터 셋으로 묶어주는 디지털증거데이터패키지 기술규격을 국가표준(KS X 1220)으로 제정하여 표준 형태로 관리할 수 있는 기반을 만들고 있으나, 현

장의 인식부족과 업무부담 등의 이유로 널리 확산되고 있지 못한 실정이다. 따라서 디지털증거의 송치 지침 및 과거 유체물 중심의 압수조서, 압수물 총목록 기재 방식 등을 표준화하고, 디지털증거의 압수물 송치 및 관리체계가 시급히 개선되어야 한다.

[보관, 열람, 대출단계]

수리 시 원본 저장매체, 사본 저장매체 식별이 제대로 안 된 상태이므로 열람 및 대출 등 디지털증거에 대한 접근이 필요한 경우 오처리로 인한 증거능력 훼손 가능성이 상존하며, 일반압수물로 분류, 보관되어 보관상태 또한 취약한 상태이다. 특히, 원본 저장매체의 경우, 쓰기방지 등 디지털증거를 별도 조치없이 열람하게 되면 증거로써의 가치를 상실할 수 있으며, 정보저장매체의 경우 빛, 온도, 습기, 충격 등에 취약하여 보관환경이 열악할 경우 매체손상으로 수록된 정보 훼손가능성도 상존한다.

[압수물 처분단계]

원본, 사본 저장매체의 구분 부재 등으로 사본 저장매체의 경우 저장매체가 수사기관 소유인 경우가 대부분이나, 수리 시 저장매체의 소유정보가 정확히 기록되지 않아 디지털증거 처분 시 디지털증거의 소유자인 피압수자에게 저장매체가 환부되는 경우 등도 발생되고 있다. 또한 몰수 되지 않은 디지털증거의 환부는 어떻게 이루어져야 하는가에 대한 실무적 해석과 어려움도 발생되고 있다.

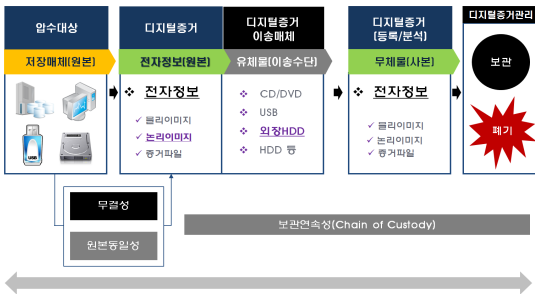
IV. 수사기관의 현황

검찰은 디지털포렌식 업무를 담당하는 별도의 조직을 구성 운영하고 있으며, 디지털증거의 안정적 취급, 관리를 위해 디지털수사지원 인프라시스템(D-NET, Digital Investigation Network, 디지털수사망)을 구축하여 디지털수사 지원업무 절차의 관리, 디지털증거의 관리, 디지털증거 분석 등을 수행하고 있다.

디지털증거의 관리에 있어서는 획득에서 제출 전단계의 모든 업무단계별로 일선청과 디지털포렌식팀간의 업무 담당자, 책임자를 기록 관리하고 있으며, 등록된 디지털증거는 별도의 생명주기 관리정책에 따라 보관, 폐기하고 있다.



(그림 3) 디지털수사망 시스템 구성



(그림 4) 검찰 디지털증거 취급현황



(그림 5) 경찰, 특사경 디지털증거 취급현황

경찰 및 일부 특사경에서도 디지털포렌식을 담당할 전문조직 또는 인력을 설치 운영 중에 있으나, 검찰과 마찬가지로 폭증하는 디지털포렌식 수요를 감당할 전문 인력과 예산의 부족 등의 문제로 어려움을 겪고 있는 실정이다. 또한 일선의 디지털증거에 대한 인식부족 등으로 증거능력 유지에 필요한 절차나 필수 정보를 미기재하는 일이 발생되고 있으며, 디지털증거를 기록물에만 편철하거나 디지털증거의 송치 자체가 누락되는 등의 문제가 발생되고 있다. 더욱이 몰수물이 아닌에도 원본 저장매체를 압수하여 검찰로 송치하는 등 실무적 혼선이 지속되고 있다.

이에 정보 즉, 디지털증거에 대한 압수물 관련 규정, 지침¹³⁾을 정비하고 디지털증거의 관리, 취급, 처분의 공백을 시급히 보완할 필요가 있다.

V. 디지털증거확보체계

디지털증거확보체계는 협의로 디지털정보의 처리, 취급 절차를 정의하고, 최소한의 기술적, 절차적 표준규격을 통해 증거능력의 훼손을 최소화하는 시스템을 말하며, 광의로 디지털포렌식을 통한 수사 활동을 위해 필요한 연구개발, 교육 등 환경 변화에 따른 기술적 한계, 전문역량의 한계를 극복하여 인권보호와 실제적 진실발견의 균형을 위해 수행하는 제반 활동을 지원하기 위한 디지털수사 지원체계를 말한다.

본고에서는 협의의 디지털증거확보체계를 대상으로 현황을 살펴본다.

5.1. 디지털증거확보체계 구축현황

디지털증거확보체계는 디지털증거가 확보된 이후 디지털증거데이터팩을 기본단위로 표준화된 절차에 따라 디지털증거가 유통 관리될 수 있도록 구축하고 있는 시스템이다.

2012년 시범시스템 구축을 기점으로 검찰과 각 기관 연계를 추진하고 있으며, 각 기관의 특성에 맞는 실무적 고려를 통하여 7개 기관과 연계 구축하였다. 2016년에 추가적으로 5개 기관과 연계 구축 예정이다.

5.2. 디지털증거데이터팩의 구성

디지털증거데이터팩은 ‘디지털증거’를 중심으로 증거 자체와 증거와 관련이 있는 정보를 담도록 설계되었다. 포함된 디지털증거의 원본 동일성과 신뢰성을 입증하기 위한 정보와 채증정보 등이 기록되며 디지털증거 관련 결과보고서를 포함한다. 디지털증거데이터팩은 기관간 유통시 디지털증거와 해당 증거에 가해진 행위를 모두 기록 관리함으로써 효율적 디지털증거의 관리가 가능하도록 설계하였다. 이 과정에서 송신기관에서는 송신이력, 그리고 수신기관에서는 수신이력을 디지털증거데이터팩에 추가하게 된다. 디지털증거데이터팩을 취급하는 또 다른 기관에서 새로운 증거를 입수하거나 기존 증거물에서 파생된 증거물을 관리하기 위해 디지털증거데이터팩을 업데이트하는 경우 업데이트가 가능하

13) 검찰사건사무규칙, 형사소송규칙, 검찰압수물사무규칙, 압수및압수물처리지침, 디지털증거수집 및 분석규정 등

[표 1] 디지털증거데이터팩 설계 철학

항 목	의 미
디지털 증거중심	증거에 가해지는 모든 행위를 하나의 디지털증거데이터팩에서 관리
육하원칙	누가(누구에게), 언제, 어디서, 무엇을, 어떻게, 왜
관리단위	1 사건 → 1 디지털증거데이터팩
디지털 증거 데이터팩 구성요소	디지털 증거 (N개) + 채증 (M개) + 보고서 (L개) * 다수의 디지털 증거에 대해 하나의 채증 정보 존재 가능
원활한 유통	디지털증거를 취급하는 모든 기관에서 원활한 사용 (증거팩 생성, 수정, 송수신 등)이 가능해야 함
이력 관리	증거팩에 가해지는 모든 행위를 이력 정보로 관리

며, 이러한 모든 변화 내역은 이력 정보로 관리하여 보관연속성을 입증할 수 있도록 했다.

디지털증거의 흐름에서 생성, 업데이트된 디지털증거데이터팩은 미래를 고려하여 최종적으로 사법기관에 제출할 수 있도록 설계하였다. 이 과정에서도 송수신 이력이 추가되어 디지털증거데이터팩의 흐름을 관리할 수 있으며, 사법기관에서는 제출된 디지털증거데이터팩을 바탕으로 디지털증거의 원본동일성, 무결성, 신뢰성 그리고 보관연속성을 확인하고 증거 능력을 판단할 수 있어서 사법 절차를 효율적으로 수행할 수 있다.

모든 사법 절차가 마무리되면, 수집된 디지털 증거에 대한 환부 및 폐기절차가 수행된다. 폐기 과정에서 수집된 디지털증거 전체 또는 일부 불필요한 항목은 삭제할

수 있으며, 마찬가지로 불필요한 채증 및 보고서 정보도 증거능력의 훼손 없이 삭제가 가능하다. 이와 같은 삭제 행위도 이력정보로 추가하여 보관연속성을 입증할 수 있도록 하였다.

5.3. 디지털증거데이터팩 표준 추진 경과

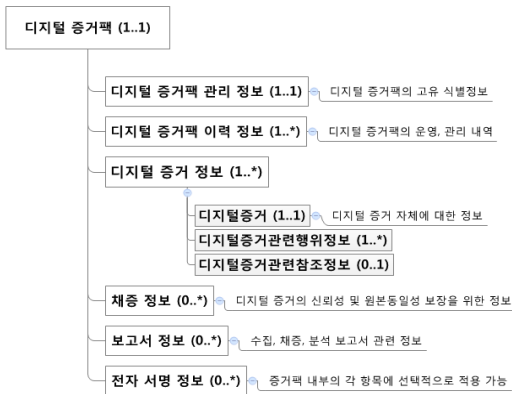
디지털증거데이터팩은 2013년 6월에 포럼을 구성하여 초안을 만들었고 2차례의 공청회를 거쳐 2014년 11월에 표준으로 KS 표준으로 고시되었다.

[표 2] 디지털증거데이터팩 표준 추진경과

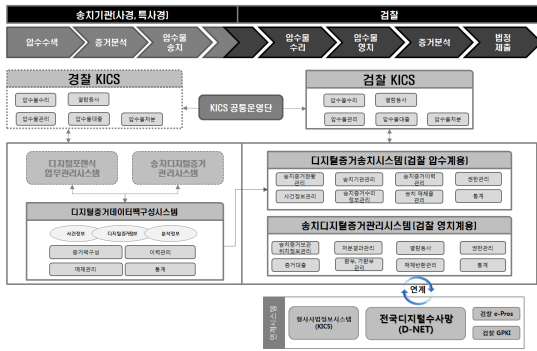
추진일자	추진 내용
'13.06 ~ '13.12	- 디지털포렌식표준화 포럼 구성 (산.학.연.관 전문가 16명) - 표준(안) 수립 및 1차 공청회
'14.6.12	- 국가기술표준원에 표준(안) 자료 제출
'14.7.18	- 전문위원회 서면 검토
~'14.7.31	- 전문위원 검토내용 반영 및 추가 검토내역 작성 - 디지털증거데이터팩 최종본 제출 (7.31)
~'14.9.30	- 예고고시
'14.9.20	- 2차 공청회
'14.10월말	- 전문위원회 최종(서면) 검토
'14.11.11	- 기술심의위원회 개최 및 평가
'14.11.28	- KS 표준 고시(표준번호: KS X 1220, 고시번호: 2014-0782)

5.4. 디지털증거 처리 및 취급 절차

디지털증거데이터팩으로 구성되어 검찰로 송치되는 디지털증거는 압수물 수리시 일반압수물로 분류하고, 상세분류에서 ‘컴퓨터 등 기타’를 선택하여 디지털증거를 분류한다. 이후 원본 저장매체, 사본 저장매체 여부를 식별하고, 원본 저장매체 유형을 구분한다. 검찰과 각 수사기관간의 연계 시스템 부재로 송치 정보를 온라인으로 유통하기 어려워 해당 과정은 검찰 압수계 담당자가 수동으로 식별 입력하고 있다. 따라서 수사 기관간 시스템 연계를 통한 자동화가 시급히 필요한 상태이다. 해당정보 입력의 정확성과 편의성 개선을 위해 디지털 증거를 온라인으로 유통 가능한 수사 기관간은 디지털



[그림 6] 디지털증거데이터팩 구조도



(그림 7) 디지털증거확보체계 논리 구조도

증거의 수리와 검증을 자동화 할 필요가 있으며, 네트워크 대역폭 등의 확장을 통해 디지털증거가 온라인으로 유통될 수 있는 환경 구축 또한 필요한 상태이다.

VI. 결 론

디지털정보로부터 출발한 디지털증거의 증거능력을 유지하고자 하는 수사기관의 그간의 변화 노력과 시스템의 개선방안에 대해 살펴보았다. 새로운 패러다임의 변화 속에서 디지털증거의 확보와 증거능력을 유지하기 위한 형사사법 체계의 정비와 수사기관간의 협업을 통하여 형사사법 인프라를 개선하고 안정적 형사사법 체계를 구현하기 위한 노력이 필요한 시점이다.

참 고 문 헌

- [1] 탁희성, “전자증거에 관한 연구, 압수·수색과 증거능력을 중심으로, 이화여자대학교 박사학위논문, 2004
- [2] 이숙연, “형사소송에서의 디지털증거의 취급과 증거능력”, 고려대학교 박사학위논문, 2010
- [3] 전승수, “형사절차상 디지털 증거의 합수수색 및 증거능력에 관한 연구”, 서울대학교 박사학위논문 2011.
- [4] 디지털증거데이터패키지 표준 KS X 1220, 2014
- [5] 서울중앙지법 2014.4.25.선고 2013고합805호 판결
- [6] 서울중앙지법 보도자료, 2015.7.18.

<저자소개>



이 인 수 (Lee Insoo)
정회원

1992년 2월 : 연세대학교 수학과 졸업
1994년 2월 : 연세대학교 수학과 이
학석사

2005년 8월 : 고려대학교 수학과 이
학박사

1996년 12월~2000년 5월 : 한국정
보보호센터 연구원

2000년 6월~2007년 12월 : 쥬비씨큐어 암호기술연구소장
2007년 12월~현재 : 대검찰청 디지털수사와 검찰사무관
관심분야 : 암호학, 디지털포렌식, 정보보호