ISSN(Print) : 1976-5304, ISSN(Online) : 2713-931X
https://kdfs.jams.or.kr, DOI : 10.22798/kdfs.2022.16.2.126

경·검 수사권 조정에 따른 디지털증거 인수·인계 과정상 증거능력 유지방안

정 웅 길*, 이 상 진**
고려대학교 디지털포렌식학과 (대학원생)*, 고려대학교 정보보호대학원 (교수)**

Measures to maintain the admissibility of evidence for taking over digital evidence in accordance with the adjustment of the police·prosecution investigation authority

Woongkil Jeong*, Sangjin Lee**
Dept. of Digital Forensics, Korea University (Graduate Student)*
School of Cybersecurity, Korea University (Professor)**

요 약

범죄 해결과 혐의 입증의 핵심 요소로 그 역할이 나날이 증가하고 있는 디지털증거는 위·변조 취약성으로 인해 무결성, 진정성, 관리연속성 등 증거능력 유지가 수사의 성패를 좌우하는 매우 중요한 요소가 되었다. 특히 경찰에게 수사종결권을 부여하는 개정 형사소송법 시행 이후 수사기관간 디지털증거를 송부해야 하는 구조로 수사환경이 변화됨에 따라 디지털증거가 수집 및 분석과정을 거쳐 법정에 제출되기까지 일련의 과정이 명확해야 하고, 이러한 과정이 추적 가능하여야 한다.

과거 검찰은 일명 '별장 성접대 사건'에서 김학의 전 법무부차관을 무혐의 처분하면서 경찰이 관련 증거를 송치하지 않아 동영상 속 인물을 특정할 수 없었다고 주장한 사실이 있다. 수사기관간 송부되는 디지털증거의 수리 기준 및 검증 절차 부재가 재판 결과에 큰 영향을 미친 사례이다. 본 고에서는 현행 디지털증거의 인수·인계 절차 및 문제점을 살펴보고, 이를 해결할 수 있는 자동화된 확인 시스템을 제안해 보고자 한다.

주제어 : 디지털증거 증거능력, 관리연속성, 수사권 조정, 디지털증거 인수·인계, 김학의 사건

ABSTRACT

Digital evidence, whose role is increasing day by day as a key factor in solving crimes and proving charges, has become a very important factor in determining the success or failure of an investigation due to its vulnerability to forgery and falsification. In particular, as the investigation environment has changed to a structure in which digital evidence must be sent between investigative agencies after the enforcement of the revised Criminal Procedure Law, which gives the police the right to terminate the investigation, the sequence of processes from the collection and analysis of digital evidence to submission to the court is clear. and this process should be traceable. In the past, prosecutors have claimed that the person in the video could not be identified because the police did not send relevant evidence while disposing of former Vice Minister of Justice Kim Hak-eui in the 'Villa Sexual Hospitality Case'. The lack of acceptance standards and verification procedures for digital evidence sent between investigative agencies is a case in which the outcome of the trial was greatly affected. In this paper, we will examine the current takeover procedure and problems of digital evidence and propose an automated verification system that can solve them.

Key Words : Admissibility of Digital Evidence, Chain of Custody, Adjustment of Investigation Authority, Takeover and Handover of Digital Evidence, Hak-eui Kim's Case

- Received 21 February 2022, Revised 23 February 2022, Accepted 13 June 2022
- 제1저자(First Author) : Woongkil Jeong (Email : jwk0720@korea.ac.kr)
- 교신저자(Corresponding Author) : Sangjin Lee (Email : sangjin@korea.ac.kr)

Ⅰ. 서 론

1.1 수사권 조정에 따른 수사환경 변화

2020년 2월 4일 개정되어 2021년 1월 1일 시행된 형사소송법(이하 '개정 형사소송법'이라 한다)은 검사의 수사지휘권을 폐지하고, 경찰에게 1차적 수사권과 수사종결권을 부여하였다. 개정 형사소송법 시행으로 경찰이 모든 사건을 검찰에 송치하는 '전건송치주의'에서 사건에 따라 선별적으로 송치하는 '선별송치주의'로 변화되었다. 과거 수사종결권이 없던 경찰은 범죄 혐의 인정 여부와 상관없이 입건된 모든 사건(관리미제사건 제외)은 검찰에 송치하고 관련 서류와 증거물을 송부하였으나, 개정 형사소송법 시행 이후에는 경·검 상호간 관계 서류와 증거물을 송부해야 하는 구조로 변경된 것이다.

경찰이 사건을 검찰에 송치하더라도 보완수사요구를 위해서는 관계 서류 및 증거물을 경찰에 송부하여야 하고, 경찰이 불송치 결정을 하는 경우에도 관계 서류와 증거물을 송부받은 검찰은 90일 이내에 다시 경찰에 반환하여야 한다.[1] 그 외에도 시정조치, 이의신청 같은 제도의 신설은 경·검 상호간 증거물을 송부해야 하는 구조적 변화를 야기하였다.

경찰청 보도자료에 의하면 2021년 6월말 기준 재수사요청은 5,584건(전체 불송치사건 172,857건 대비 3.2%), 시정조치요구는 1,275건 (전체 수사중지사건 39,729건 대비 3.2%), 이의신청건수는 9,878건(전체 불송치결정 172,857건 대비 5.7%)에 이른다.

개정 형사소송법은 검사의 수사 개시 범위도 부패범죄, 경제범죄, 선거범죄, 공직자범죄, 대형참사, 방위사업범죄 등 6대 범죄 및 경찰공무원이 범한 범죄로 한정하였다. 이에 따라 검사의 수사 개시 범위를 벗어나는 사건이 검찰에 접수되는 경우에는 증거물과 함께 사건을 경찰에 이송하여야 한다.[2] 게다가 2022년 5월 3일에는 검찰이 수사를 개시할 수 있는 범죄를 2대 범죄(부패범죄, 경제범죄)로 축소하는 형사소송법 개정안이 국회와 국무회의를 통과하여 2022년 9월 10일 시행될 예정이다. 검찰의 수사개시 범위에서 4대 범죄가 제외됨에 따라 검찰에서 경찰로 이송되는 사건의 수는 더욱 증가할 것으로 보인다.

또한 고위공직자 및 그 가족의 비리를 중점적으로 수사·기소하는 고위공직자범죄수사처(이하 '공수처'라 한다)도 2021년 1월 20일에 출범하였다. 이에 따라 공수처의 범죄수사와 중복되는 다른 수사기관의 범죄수사에 대하여 공수처장이 수사의 진행 정도 및 공정성 논란 등에 비추어 공수처에서 수사하는 것이 적절하다고 판단하여 이첩을 요청하는 경우 경찰을 비롯한 해당 수사기관은 이에 응하여야 한다.[3]

한편 개정 형사소송법은 검·경간 증거물 송부뿐 아니라 경찰서간 이송도 함께 증가시켰다. 그간 경찰은 수사지연 방지 및 사건관계인의 권리보호 등을 이유로 이송을 엄격하게 제한해왔다. 이로 인해 경찰이 송치한 사건 중 일부는 형사소송법상 재판관할과 불일치하여 그간 검사가 관할 있는 검찰청으로 이송하여 수사종결 또는 공소 제기해 왔다. 그러나 개정 형사소송법 이후에는 경찰에 수사종결권이 있기 때문에 원칙적으로 재판관할 있는 검찰청에 사건을 송치해야 한다.

이와 같은 수사환경의 변화 속에서 위·변조에 취약한 디지털증거는 수집 및 분석과정을 거쳐 법정에 제출되기까지 일련의 과정이 명확하고 이러한 과정에 대한 추적이 가능한지, 그리고 증거가 법정에 제출되기까지 변경이나 훼손이 없이 유지되었는지 끊임없이 유의하여야 한다. 또한 컴퓨터 기술의 급속한 발전으로 기존의 텍스트 위주의 사용자 환경이 그래픽, 이미지, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환되고 있으므로 디지털증거 인수·인계 과정상 무결성, 진정성, 관리연속성 등 증거능력은 반드시 유지되어야 한다.

1.2 문제 제기

개정 형사소송법 시행 이후 변화된 수사 환경과 더불어 급속한 정보화는 수사기관에 큰 변화를 요구하고 있다. 하지만 과거 상명하복 관계였던 경·검은 그간 상호 협의가 아닌 일방의 지휘에 따라 수사절차가 진행됨에 따라 디지털증거 관리 또한 기관간 협의에 따른 지침이 부재했던 것이 사실이다. 수사의 성패를 가늠할 정도로 그 중요성이 부각되고 있는 디지털증거에 대해 증거능력을 유지하기 위한 개별 수사기관 내부의 조치뿐만 아니라 수사기관간 표준절차 마련 등 적극적인 대응이 필요한 시점이다. 개정 형사소송법 시행으로 인해 더 이상 개별 수사기관만의 문제로 치부할 수 없게 되었기 때문이다.

1) 검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정 제60조 제1항
2) 검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정 제18조 제3항
3) 고위공직자범죄수사처 설치 및 운영에 관한 법률 제24조 제1항

과거 검찰은 소위 '별장 성접대 사건'에서 김학의 전 법무부 차관을 무혐의 처분하면서 경찰이 관련 증거를 송치하지 않아 동영상 속 인물을 특정할 수 없었다고 주장하였다. 하지만 민갑룡 전 경찰청장은 2019년 3월 국회 행정안전위원회 전체회의에 출석해 검찰의 주장과 다르게 답한 사실이 있다. 당시 김민기 민주당 의원은 "성 접대 의혹과 관련된 동영상의 감정을 위해 국립과학수사연구원에 영상을 의뢰할 때 선명한 영상을 제출하지 않고 흐린 영상을 제출한 이유가 무엇이냐"라고 질문하자, 민 전 청장은 "선명한 영상은 김학의 전 차관인 것을 육안으로도 식별할 수 있어서 의뢰 없이 동일인이라고 결론 내리고 검찰에 송치한 것"이라고 대답했다. 이에 김 전 의원이 수사가 부실했던 것이 아니냐고 지적하자, 민 전 청장은 "많은 문제를 제기했고 법적 항고 절차를 거쳤지만 명확하게 해소가 안 됐다"고 답변했다.

'별장 성접대 사건'은 2013년 3월 김학의 대전고검장이 법무부 차관에 내정된 직후 성접대 동영상이 언론에 보도되면서 불거졌다. 당시 경찰이 수사에 착수해 확보한 동영상에는 김 전 차관으로 추정되는 인물이 술을 함께 마시던 여성과 성관계를 하는 장면이 담겨 있었다. 이에 경찰은 해당 사건을 기소 의견으로 서울중앙지검에 송치하였다.

하지만 사건을 맡은 서울중앙지검은 2013년 11월 김학의 전 법무부 차관에 대해 증거가 불충분해 혐의가 없다면서 불기소 결정을 내렸다. 검찰이 김학의 전 차관의 성접대 혐의에 대해 동영상 속 피해자의 신원을 파악할 수 없다는 등의 이유였다. 그러던 중 2014년 7월 동영상 속 피해자가 자신이라고 주장하는 여성이 김 전 차관과 건설업자 윤모씨를 성폭력범죄의처벌등에관한특례법위반(카메라등이용촬영)과 폭력행위등처벌에관한법률위반(상습강요) 등의 혐의로 검찰에 고소했다. 그러나 1차 수사에서 김 전 차관을 무혐의 처분한 검사가 다시 사건을 배당받았고, 2차 수사에서도 동영상 속의 여성과 고소인이 동일 인물인지 확인하기 어렵다면서 다시 무혐의 처분하였다.

이후 '별장 성접대 사건'은 2018년 4월 법무부 검찰과거사위원회의 수사권고로 수사가 재개되었다. 재수사에 나선 검찰은 의혹 제기 6년여만인 2019년 6월 김 전 차관을 기소하였으나 성접대(2006년 9월~2008년 2월까지 13차례) 혐의는 이미 10년의 공소시효를 넘겨 처벌할 수 없는 상황이었다. 이에 검찰은 성접대를 뇌물로 간주해 공소시효가 남은 다른 뇌물 혐의(건설업자 윤모씨가 제공한 1억 3천만원 상당)와 묶어 포괄일죄로 기소하였고, 1심 재판부도 성접대가 이뤄진 역삼동 오피스텔 사진과 성접대 동영상 속 남성이 사실상 김 전 차관이 맞다고 인정하였다.

당시 1심 재판부는 건설업자 윤모씨로부터의 뇌물수수 부분에 대한 판단에서 '성접대 사진(증거순번 225-2,383)' 및 '영상감정결과통보(증거순번 384)의 각 기재 및 영상에 의하면, 피고인이 2006. 10경부터 2007년경까지 여성1과 지속적으로 성관계 또는 성적 접촉을 가질 수 있는 기회를 Y로부터 제공받아 온 사실'을 인정사실로 들었다. 특히 성접대 사진 관련해서는 '이와 관련하여 피고인 및 변호인들은, 해당 사진(이하 '이 사건 사진'이라 한다) 상으로 얼굴이 드러나 있는 남성이 피고인은 아니라면서, 피고인은 이 사건 사진이 촬영된 일시(2007. 11. 13. 21:57경)에 촬영장소(AB 오피스텔)가 아닌 자택에 있었고, 위 사진 상의 남성과 피고인의 가르마 방향이 서로 다른 등으로 위 두 사람은 동일인이 아니라고 주장한다. 위에서 든 증거들을 포함하여, 이 법원이 적법하게 채택하여 조사한 증거들을 토대로 알 수 있는 다음의 사정에 비추어 보면 이 사건 사진 상의 남성은 피고인이라고 봄이 상당하고, 다른 가능성(우연히 다른 사람이 찍혔을 가능성, Y가 피고인과 닮은 대역을 세워 촬영했을 가능성)은 지극히 합리성이 떨어지는 것으로 받아들이기 어렵다.'라고 판단하였고, 이에 대한 근거로 9가지를 기재하였는데 그중에서 사진과 동영상에 대한 직접적 판단이 기재되어 있는 부분은 다음과 같다.

*'② 이 사건 사진 상의 남성과 당일 기사에 실린 피고인의 사진을 비교할 때 피고인의 얼굴형, 이목구비, 머리모양(가르마 방향 제외), 안경 등이 매우 유사하고 이 사건 사진에 합성 등 인위적 조작은 이루어지지 않았다. ⑤ 이 사건 사진파일이 저장된 CD는 2019. 4. 4.에야 DR으로부터 압수되었는데, 위 CD에는 '*AA별장 동영상*'(가르마 방향이 피고인과 동일하며, 피고인의 이름을 따서 파일명을 저장한 것으로 보인다)도 들어있어 동영상의 인물과 이 사건 사진파일의 인물은 같은 인물이라고 봄이 상당하며, 이 사건 사진파일의 보관자, 장소와 등장인물, 행위내용 등이 위 여성1 등의 2013년, 2014년 진술과 같거나 유사하다.'*

하지만 1심 재판부는 성접대 혐의와 포괄일죄로 기소된 뇌물수수 혐의를 무죄로 판단하였고, 성접대 혐의는 공소시효 완성으로 면소 판결하였다. 윤모씨와 관련된 제3자 뇌물(1억원의 채무 면제) 혐의가 무죄가 됨에 따라, 나머지 3천만원과 성접대에 대해서는 공소시효가 지났다는 판단이었다. 뇌물 액수가 1억원 미만인 경우 공소시효가 10년인데, 성접대 관련 뇌물은 2008년 2월까지 받은 것으로 인정됐기 때문이다.

이후 2020년 10월에 선고된 항소심은, 무죄를 선고한 1심을 깨고 일부 혐의(사업가 최모씨가 제공한 4,300만원)만을 유죄로 인정하면서 특정범죄가중처벌법상 뇌물수수 혐의로 기소된 김학의 전 차관에게 징역 2년 6개월과 벌금 500만원, 추징금 4,300만원을 선고하였다. 하지만 항소심에서도 성접대 혐의와 포괄일죄로 기소된 뇌물수수 혐의는 무죄 판단이 유지되어 결국 성접대 혐의는 공소시효에 막혀 면소 판결되었고, 대법원에서도

이 같은 판단이 유지됐다. 대법원은 항소심에서 유죄로 인정된 사안에 대해서 검사의 사전 증인 면담에 의해 증인의 진술에 신빙성이 없다면서 파기환송하면서도, 성접대 혐의에 대해서는 공소시효가 지났다는 이유로 면소 판결한 원심 판단을 그대로 확정하였다.

정리하면 1심 판결에서 성접대 동영상 속 인물이 김 전 차관임이 인정되었음에도 성접대 혐의와 포괄일죄의 관계에 있는, 건설업자 윤모씨가 제공한 뇌물수수 혐의가 무죄로 선고됨에 따라 대법원은 성접대 혐의와 관련해서는 실체적 판단을 하지 않고 공소시효 완성이라는 형식적 판단만 확정하였다. 이는 수사기관간 송부되는 디지털증거의 수리기준 부재가 재판 결과에 큰 영향을 미친 사례로 즉각적인 보완이 필요하다.

1.3 선행연구

이인수는 디지털증거가 확보된 이후 디지털증거데이터팩을 기본단위로 표준화된 절차에 따라 수사기관간에 유통·관리되는 시스템(디지털증거 확보체계)의 구축현황을 조사하였다. 검찰로 송치되는 디지털증거는 검찰과 각 수사기관간의 연계 시스템 부재로 송치 정보를 온라인으로 유통하기 어려워 해당 과정은 검찰 압수계 담당자가 수동으로 식별 입력하고 있는 등 수사 기관간 시스템 연계를 통한 자동화가 시급히 필요한 상태였음을 지적하였다[1].

성혜정은 디지털증거에 대한 무결성을 보장하고 제3자로서 감시자 역할을 하는 독립된 디지털증거 검증기관의 필요성과 그 역할을 제안했다. 수사기관은 제3의 독립된 기관으로부터 증거분석 처리에 대한 신뢰성을 보증받음으로써 공판정에서 객관적이고 과학적인 사실의 존부에 관해 공방을 하는 시간을 절약하고 사건의 쟁점에 빠르게 접근하여 보다 효율적인 재판을 수행하고 집중 심리를 펼치는 데 도움이 될 것이라고 주장하였다[2].

정형상은 압수된 증거 데이터를 디지털 저장매체 관리시스템에서 지원하는 저장매체에 암호화하여 저장하고, 데이터를 복호화할 수 있는 암호화키는 디지털증거관리 서버로 전송하는 방안을 제시하였다. 그리고 수사관이 가상 데스크톱 시스템에 사용자 인증을 통하여 가상머신에 접속하여 디지털증거관리 서버에 저장된 증거 파일을 분석하고, 송치 후 디지털증거관리 서버에 보관된 자료에 대한 접근 통제하여 자료 유출을 방지하는 시스템을 함께 제안하였다[3].

정현희는 형사사법체계에서 디지털증거의 전체적인 흐름도를 그려보고, 처리 과정의 각 단계별 디지털증거에 대한 현행 관리 실태를 확인한 후 관리미제 사건의 장기 보관 문제에 대한 디지털증거 표준화 방안과 함께 향후 대용량화 및 다양화될 디지털증거에 대한 통합 관리의 필요성에 대한 대책으로 '디지털증거 관리시스템'을 제안하였다. 제안 시스템은 경찰이 사건을 검찰에 송치할 때 사건정보, 송치정보 등과 사건 메타정보, 분석 메타정보, 이미지를 디지털증거팩 구성시스템을 통해 입력하고, 국가전송망을 이용하여 검찰에 송치한 후 경·검 KICS 시스템간 데이터를 서로 연동시키는 시스템이다[4].

정효정은 대용량 데이터에 대한 효율적인 증거 수집을 위해 사이버 공간 내 주요 웹 기반 서비스를 중심으로, 클라이언트 측면에서의 자동화된 증거 수집 방식을 제안하였고, 제안한 방식을 사용하여 수집한 디지털증거의 법정 제출 시점까지 증거팩을 생성하여 무결성을 보장하는 사이버 공간 내 디지털증거 수집 시스템을 제안하였다[5].

위 논문들은 디지털증거의 관리연속성을 유지하기 위해 디지털증거팩 구성, 디지털증거의 수리과 검증 자동화, 디지털증거가 온라인으로 전송될 수 있도록 수사기관간 IT 인프라 환경 조성 필요성 등에 대해서 공통적으로 언급하고 있으나, 수사단계별 수사기관간 송부되는 디지털증거의 수리 기준 및 검증 절차에 대해 구체적인 방법은 제시하고 있지 않다. 본 연구에서는 현행 디지털증거 인수인계 절차 및 체계에 대해서 살펴보고, 이에 대한 문제점을 해결할 수 있는 자동화된 확인 시스템을 제안하고자 한다.

Ⅱ. 현행 디지털증거 인수·인계 체계

2.1 디지털증거의 라이프사이클(Lifecycle)

사건담당 수사관은 사건 관계인으로부터 디지털증거를 압수하거나 임의제출 받은 후, 경찰청 디지털증거 통합관리시스템을 통해 디지털증거가 저장된 저장매체에 대한 디지털포렌식을 의뢰한다. 의뢰를 받은 증거분석관은 분석의뢰물로부터 디지털증거를 획득·분석한 다음, 저장매체에 저장하여 사건담당 수사관에게 회신하거나 디지털증거 통합관리시스템을 통해 파일로 회신한다. 회신받은 사건담당 경찰관은 선별압수를 진행하고 형사사법정보시스템(Korea Information system of Criminal-justice Services, 이하 'KICS'라 한다)에 압수물로 등재한다. 이후 압수한 디지털증거를 담은 저장매체는 봉인한 후 통합증거관리시스템에서 압수물 바코드를 생성·부착하여 사건 종결시까지 경찰관서별 통합증거물보관실에서 보관된다.

이렇게 수집・분석한 디지털증거는 피의자의 혐의사실이 인정되면 검찰에 송부되고, 사건담당 수사관의 개인 PC 및 저장매체 등에 별로도 보관되어 있는 사건관련 전자정보는 지체없이 삭제・폐기된다.

송부 후 검찰에서도 혐의사실이 인정되면 기소되어 법정에서 사용되고 재판과정에서 법정 전문가 증언이 필요한 경우 재분석 등에 사용될 수 있으며, 피의자(피고인)・변호인의 요청에 따라 열람・등사(복제)되는 경우도 있다[4]. 그리고 재판이 종료되면 증거로서 역할은 마무리되나 재심을 위해 증거보전 청구되기도 한다.

한편 경찰이 수사를 진행하였으나 피의자를 특정할 수 없어 종결할 수 없는 사건은 추가 단서 확보시까지 관리미제사건으로 별도 등록하여 관리할 수 있다. 그리고 조사에 착수한 후 원칙적으로 6개월 이내에 수사절차로 전환하지 않은 사건이 혐의없음, 죄안됨, 공소권없음, 각하 사유에 해당하는 경우에는 불입건 결정(입건 전 조사종결)한다.[4] 관리미제사건 및 불입건 결정 사건에서 수사단서로 사용된 디지털증거는 통합증거물 처분심의위원회를 통해 심의 후 폐기되거나 별도의 저장매체에 담아 공소시효 경과시까지 통합증거물보관실에 보관된다.

2.2 디지털증거 인수·인계 절차 및 문제점

2.2.1 디지털증거 수집 후 보관(관리) 단계

경찰의 통합증거물 관리시스템은 과학적범죄분석시스템(SCAS) 내 증거물과 압수물에 대한 체계적인 관리・감독을 위해 구축된 시스템으로 경찰이 수집한 디지털증거는 압수유형에 따라 압수물・증거물로 구분하여 등록 후 관리된다.

디지털증거를 현장에서 선별압수를 완료하는 경우 압수물로서 관리하고, 현장에서 선별압수가 어려워 원본・복제본을 반출한 경우 압수 완료시까지 임시적으로 증거물로 등록한다. 이후 증거물 바코드를 생성・부착하여 관리하다가, 압수 완료시 압수물로 전환하여 관리한다.

2.2.2 디지털증거 분석의뢰 단계

분석의뢰 수사관은 압수한 디지털증거가 원본인 경우 현장에서 피압수자의 참여권을 보장한 상태에서 봉인 후 분석의뢰해야 하고, 피압수자가 참여하겠다고 하는 경우에는 분석팀과 사전에 분석일시 등을 협의해야 한다.

증거물의 운반은 의뢰자가 직접 운반하는 것이 원칙이고 직접 운반의 방식이 현저히 곤란한 경우 분석의뢰물이 손상되지 않고 운반 이력이 확인될 수 있는 안전한 방법(택배는 현관 앞 배달 등 직접 전달을 하지 않는 경우가 많아 등기를 이용하거나 안심소포 활용 등)으로 운반해야 한다. 운반 시에는 분석의뢰물의 파손, 훼손, 멸실 등에 각별히 유의하고 분석의뢰자, 운반자, 접수자 등을 기록하여 관리연속성(Chain of Custody)을 유지하여야 한다.

분석의뢰물을 전자적 방식으로 전송할 필요가 있는 경우 해시값을 기록하는 등 분석의뢰물의 동일성을 유지하는 조치를 취하고, 디지털증거 통합관리시스템을 통해 분석의뢰물을 전송한다.

증거분석관은 디지털증거 분석의뢰 접수 시 접수일시 등을 기록 관리하고, 분석의뢰물의 종류 및 수량, 봉인 여부 등 상태를 확인하고 촬영하여 관리연속성을 유지하여야 한다. 그리고 제조일자, 고유번호, 모델명 등 분석의뢰물 관련 정보를 비롯하여 최초 수집일시・장소, 해시값도 함께 확인하여야 한다.

2.2.3 디지털증거 획득·분석 단계

분석 의뢰사건의 개요, 분석 목적 및 요청사항 등을 파악한 후 요청사항, 분석의뢰물 유형 및 상태 등을 고려하여 획득·분석의 범위와 방법을 결정한다. 이때 분석의뢰물에 대하여 권한 없는 사람의 접근을 통제하고, 특별한 사유가 있는 경우를 제외하고 증거분석실 출입을 제한함으로써 획득・분석 과정에서 분석의뢰물의 무결성, 관리연속성을 유지하여야 한다.

디지털증거 획득시 부득이한 경우에도 이를 훼손하는 행위를 최소화하고, 그 행위의 사유와 그로 인한 변경사항 및 조치 등을 기록하여 추후 전문가가 신뢰성을 확인할 수 있도록 하여야 한다. 그리고 무결성 유지를 위해 네트워크 접속은 최소화하고, 해시값 기록 및 쓰기방지장치 사용 등의 조치도 행해야 한다.

디지털증거분석은 원본과 동일한 해시값을 가진 복제본을 생성하여 이를 대상으로 수행하여야 한다. 다만, 수사상 긴박한 사정이 있거나 복제본을 생성할 수 없는 불가피한 사정이 있는 경우 원본을 대상으로 분석할 수

4) 경찰청 수사기획과-23347 ('17. 12. 26.) 장기 기획(인지)수사 일몰제 시행 계획

있다. 이 경우 원본이 변경, 훼손되지 않도록 기술적 조치를 취하고 기술적 조치에 관한 사항 및 원본의 변경 여부 등을 분석결과보고서에 기재한다.

아울러 증거분석관은 증거분석 도구(이름과 버전정보 등 상세), 분석일시 및 장소, 분석의뢰물에 대한 접근 이력, 방법론 등에 관한 정보를 기록하여야 한다. 특히 사회적 이목이 집중되는 사건 등 주요 사건의 경우 분석 과정을 반드시 사진 또는 영상으로 촬영하여 보관한다.

한편 시·도경찰청 디지털포렌식계에서는 고도의 기술이나 특정 장비 등이 필요하여 복제본 획득 또는 분석이 어려운 경우, 경찰청 디지털포렌식센터에 디지털증거분석을 재의뢰할 수 있다. 재의뢰 시에도 무결성, 관리 연속성 등이 훼손되지 않도록 증거물 바코드 기록, 담당자 기록 등이 유지되어야 한다.

재의뢰는 디지털증거 통합관리시스템에 분석의뢰 사건을 등록한 후, 분석의뢰물을 봉인 봉투 등으로 봉인하여 재의뢰자(시·도경찰청 증거분석관)가 직접 운반하여야 한다. 직접 운반이 현저히 곤란한 경우 분석의뢰물이 손상되지 않고 운반 이력이 확인될 수 있는 안전한 방법으로 재의뢰할 수 있다. 이때 재의뢰한 분석결과물은 디지털증거 통합관리시스템을 통해 시·도경찰청 디지털포렌식계에 파일로 회신된다.

2.2.4 디지털증거 분석 후 수사관 회신 단계

증거분석관이 보고서 최종 승인 후 분석의뢰 수사관에게 보고서와 분석결과물을 회신하면 사건담당 수사관은 선별압수를 해야 한다. 수사관이 저장매체로 회신받은 때에는 선별압수를 진행할 사본을 생성한 후, 분석결과물을 증거물로 등록·입고 관리하고, 디지털증거 통합관리시스템으로 분석결과물을 파일로 회신받은 때에는 파일사본만 생성하여 선별압수 진행한다. 이때 디지털증거 통합관리시스템의 분석결과물 삭제(폐기) 시점이 2021년 11월 15일부터 기존 4주에서 2주로 변경되어, 파일 보관기간인 2주 이내에 처리하여야 한다.

선별압수한 전자정보는 USB, 하드디스크 등 별도의 저장매체에 담아 KICS에 압수물로 등재하고 저장매체는 압수물 봉투 또는 디지털증거물 봉인 봉투에 넣어 봉인한 후 관리시스템에서 압수물 바코드를 생성·부착한다.

2.2.5 검찰 송부 단계

경찰은 관리미제 및 입건 전 조사종결(구 내사종결) 건을 제외하고 수사 후 관계서류와 증거물을 검사에게 송부한다. 이때 디지털증거는 원본 저장매체 자체 또는 사본 저장매체에 디지털증거를 복제하여 송부한다.

디지털증거를 포함한 모든 증거물(압수물)은 일반적으로 담당 수사관이 KICS상 사건종결 처리 후 수사지원팀에 제출하면, 수사지원팀 송부 담당자가 이를 취합하여 검찰청 사건과에 인계한다. 이때 송부 담당자는 검찰청 압수물 담당자로부터 '사건 인계부'에 확인 서명 또는 날인을 받아 부책(보존기간 3년)으로 관리한다.

사건인계부의 중요성은, 지난 2015년 부산의 모 경찰서에서 수사지원팀 송부 담당자가 송치단계에서의 압수물 관리가 미흡한 점을 악용, 압수금품 3,200만원을 횡령한 사건이 발생하면서 인식되기 시작했다. 당시 경찰은 수사관 비리방지에만 초점을 두었고, 검찰도 여러 기관 송치사건을 담당자 1명이 처리하는 등 송치단계에서의 사건압수물 관리가 미흡하였다.[5)]

경찰은 이 사건 이후로 '송치단계 사건·압수물 관리체계 강화 계획'을 수립하여 사건인계부에 '압수물 유무'가 추가로 자동입력되도록 조치하였다. 이에 따라 사건 인계부에는 사건번호·결정·결정일·송치번호·피의자·죄명·발송일시·압수물 유무 등이 자동입력된다. 다만 송치 사건에 대한 사건 인계부는 모든 항목이 자동입력되나, 불송치·수사중지 사건에 대한 사건 인계부는 발송일시만 입력되지 않으므로 검찰청에 서류 및 증거물을 인계하는 '실제시간'을 수기로 기재하여야 한다. 그리고 사건 인계부도 KICS 양식이 아닌 관서별 자체양식의 사용을 금지시켰고, 사건인계부에 수사지원팀장 확인란도 추가하였다.

한편 디지털증거를 송부받은 수사기관은 관리연속성 확보를 위해 단순 수리가 아닌 개별 파일의 해시값 확인을 하여야 한다. 그러나 검찰 사건과 압수물 담당자는 증거물 인수시, 압수목록상 증거물 존재 여부만 확인하고, 개별 파일의 해시값은 확인하지 않는다. 증거물 존재 여부도 개별 파일의 존재 여부가 아닌 디지털증거가 저장된 저장매체의 존재 여부만 확인할 뿐이다.

즉, 압수물(증거물) 인수 시점에 디지털증거의 목록과 실제 데이터의 존재 여부를 비교·확인하는 절차가 없다. 개별 증거 파일에 대한 해시값 확인 누락은 곧 관리연속성의 흠결을 의미하므로 이를 보완하기 위해서는 경찰과 검찰 사이에 디지털증거의 수리와 검증을 자동화 해주는 시스템을 구축할 필요가 있다.

5) 현재 광주지검의 경우에도 압수물 관리를 2명이 하고 있으나, 1명은 몰수보전·처분·관보·촉탁 등의 업무를 처리하고 있고, 사실상 1명이 압수물 수리, 반환, 건의 업무를 처리하고 있다.

2.2.6 경찰서간 이송 단계

경찰의 이송은 필수적인 유형과 임의적인 유형으로 분류된다. 먼저 필수적 이송 유형으로는 사건 관할이 없거나 다른 기관의 소관 사항으로 경찰의 수사사항이 아닌 경우와 법령에서 다른 기관에 이송의무를 부여한 경우로서, 공수처법 제24조 제1항(공수처 이첩요청) 및 제25조 제2항(검사의 고위공직자범죄) 등이 이에 해당한다.

임의적 이송 유형으로는 다른 경찰관서나 기관에서 수사 중인 사건과 병합처리하는 것으로 이송받을 기관과 협의된 경우와 해당 경찰관서에서 수사하는 것이 부적당한 경우가 이에 해당한다.

수사관이 KICS와 연계된 타 경찰관서나 검찰에 이송하는 경우에는 KICS상 사건이송서를 작성하고 별도 공문 작성 없이 KICS에서 이송처리 후 관련 서류 및 증거물을 등기로 발송한다. KICS와 연계되지 않은 군부대, 특사경 등 타기관 이송하는 경우에는 해당 기관에 온나라 서비스(On-nara service)[6]를 통해 공문 작성·발송하고 KICS상 이송처리(공문번호 기재) 후, 관련 서류 및 증거물을 등기 발송한다.

한편 경찰의 디지털증거 관리(저장 및 보관)는 온라인이 아닌 과학적범죄분석시스템(SCAS)의 통합증거물관리시스템에 증거물로 등록 후 바코드 발급하여 증거물 보관실에 보관하는 방법으로 이루어지고 있다. 따라서 이송시에도 온라인이 아닌 디지털증거가 보관된 저장매체를 등기로 발송해야 하는 구조라서 해당 저장매체의 분실 및 훼손 가능성이 존재한다.

한편 '디지털증거의 처리등에 관한 규칙'상 경찰관은 사건을 이송한 경우 수사과정에서 생성한 디지털증거의 복사본을 지체 없이 삭제·폐기하여야 한다. 그런데 이송 받은 담당수사관이 착오 또는 처리지연으로 이송 과정에서 디지털증거가 분실 및 훼손된 사실을 뒤늦게 확인한 경우 이미 삭제·폐기된 디지털증거는 복구할 방법이 없으므로 이에 대한 보완도 필요하다.

2.2.7 검찰에서 경찰로의 이첩(반환) 단계

사건 이첩(반환)시, 관계 서류 및 증거물을 반환하는 기관이 인계받는 기관으로 직접 가져다주어 전달하여야 하는 것이 원칙이다. 그러나 경·검간에는 송부담당 경찰관이 검찰청을 방문했을 때 그 시점에 송부대기 중인 서류와 증거물을 가져올 수 있도록 하여 예외적으로 협조하고 있다. 검찰서류 수령을 위해 송부담당 경찰관이 부당하게 장시간 대기하지 않고 송부 준비되어 있는 서류만 가져오는 방식이다. 이는 1개 검찰청에 대응하는 경찰서가 다수라는 측면을 고려한 것이다.

이에 따라 송부담당 경찰관이 압수물 (가)환부 등 처리 문제로 검찰청 사건과를 방문하면, 보완수사요구·재수사요청 사건기록과 함께 관련 증거물을 인수하고, 검찰청에서 요구하는 인수부에 확인서명 또는 날인한 후, 인수부 사본을 부책으로 관리하고 있다.

이때 송부담당 경찰관이 관계 서류와 증거물을 가져오는 행위 자체는 사실행위이며, 경찰수사규칙 제9조[7]의 접수에는 해당하지 않는다. 송부담당 경찰관이 검찰 요청시 검찰청에 비치 중인 수령확인서, 인계서, 대장 등에 서명 가능하나, 이는 접수가 아니며 단순히 서류를 인계·인수하였다는 확인 차원에 불과하다. 동 규칙 제9조에 따라 경찰관서로 서류를 가져온 후 경찰관서 내 사건기록 담당직원이 접수여부를 별도로 판단하게 되고, 보완이 필요한 경우 보완을 요구하는 등 필요한 조치를 취할 수 있기 때문이다. 그런데 문제는 사건기록 담당직원이 접수 여부를 판단할 때 검찰청에 디지털증거를 인계하는 경우와 마찬가지로 인수한 개별 파일에 대한 해시값을 확인하는 절차를 규정하고 있지 않다는 점이다.

한편 검찰사건사무규칙도 경찰수사규칙과 마찬가지로 해시값 확인에 대해서는 구체적으로 언급하고 있지 않다. 검찰사건사무규칙 제7조에서, '사건사무 담당직원이 기록을 접수했을 때에는 기록 송부관서가 제시하는 접수기록부 등에 접수일시 및 접수자의 직급 및 성명 등을 기재하여 압수물이 있는 경우에는 이를 압수물 사무 담당직원에게 인계하여 압수물 수리절차를 취하게 해야 한다.'고 규정하고 있고, 검찰압수물사무규칙 제4조는 '압수물 사무 담당직원은 경찰서등에서 검사에게 압수물을 송부 또는 인계하려는 경우 사건기록 또는 불송치 기록의 압수물 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 규정하고 있을 뿐이다.

6) 정부 부처와 지방자치단체 공무원이 문서결제 등을 위해 사용하는 정부 업무시스템으로 행정안전부가 운영하고 있는 범정부적인 전자정부 시스템

7) 사건기록 담당직원은 사건 기록과 증거물을 반환받은 때에는 관계 서류 등이 법령에 따라 작성·편철됐는지를 점검하고, 이를 접수한 경우에는 접수대장에 접수일시, 검사 또는 검찰청 직원의 성명을 기재하고, 검사 또는 검찰청 직원이 제시하는 접수기록부에 접수일시와 접수자의 직급 및 서명을 기재한다.

Ⅲ. 디지털증거 송치표준화

3.1 경·검의 디지털증거 관리시스템

검찰은 디지털증거의 안정적 취급·관리를 위해 디지털수사지원 인프라시스템(Digital Investigation Network, 이하 'D-NET'이라 한다)을 구축하여 디지털수사 지원업무 절차의 관리, 디지털증거의 관리 및 분석 등을 수행하고 있다. 디지털증거의 관리에 있어서는 획득에서 제출까지 전단계의 모든 업무단계별로 일선청과 디지털포렌식팀간의 업무 담당자, 책임자를 기록 관리하고 있으며, 등록된 디지털증거는 별도의 생명주기 관리정책에 따라 보관·폐기하고 있다 [1].

경찰도 디지털증거 통합관리시스템을 구축하여 현장지원요청, 증거분석의뢰를 할 수 있고, 부가적으로 현장소통방 등 커뮤니티 및 가이드/매뉴얼 등을 통해 업무소통 및 업무지식의 습득 및 공유할 수도 있다.

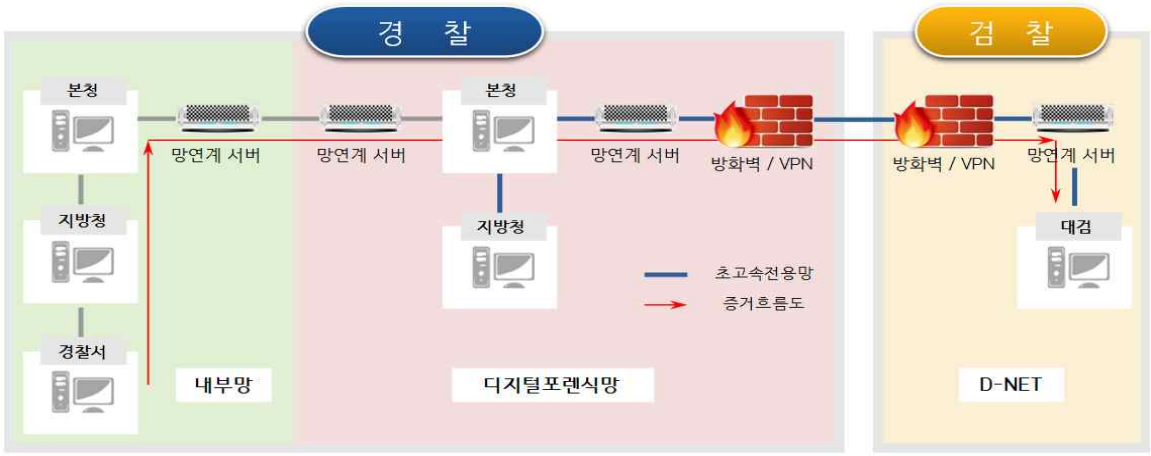
하지만 검찰이 디지털증거를 PC 또는 저장매체에 저장하여 보관하지 않고 D-NET을 통해 온라인으로 관리하는데 반해, 경찰은 디지털증거 통합관리시스템을 주로 현장지원요청 및 증거분석의뢰(접수 및 회신)시에 사용하고, 디지털증거 관리(저장 및 보관)는 온라인이 아닌 통합증거물관리시스템에 증거물로 등록 후 바코드 발급하여 경찰관서별 '증거물 보관실'에 보관하는 방식을 활용하고 있다.

한편 디지털증거 분석의뢰한 획득 이미지(분석결과물 최대 용량은 의뢰사건당 200GB로 제한)는 다운로드를 위해 최대 2주(2021년 11월 15일부터 기존 4주에서 2주로 변경) 동안 저장하고 있으나, 2주 경과시 자동 삭제된다. 그리고 수사관이 다운로드 받으면(회신완료)시에는 2주가 경과되지 않았더라도 7일 후 삭제되고, 7일 이내에도 수사관이 직접 삭제할 수 있다.

3.2 디지털증거 송치표준화 시범실시 결과

경찰은 법원의 엄격한 디지털증거의 증거능력 요구에 대응할 수 있는 무결성 및 관리 연속성을 확보하기 위해 지난 2015년부터 일부 경찰관서를 대상으로 '디지털증거 송치표준화'를 시범실시하고 있다. '디지털증거 송치표준화'는 사건송치시 디지털증거 및 관련 정보를 증거팩 형태로 온라인 전송 또는 지정된 저장매체를 활용하여 송부하는 것이다. 2015년 1차 시범실시의 경우 대전 5개 경찰서를 대상으로 하였고, 2017년부터 현재까지 실시하고 있는 2차 시범실시의 경우 서울 북부지검으로 송치되는 서울 7개 경찰서 및 대전 5개 경찰서를 대상으로 하고 있다. 증거팩은 디지털증거와 관련정보를 표준화하여 저장한 꾸러미 파일로 필수정보(사건정보, 디지털증거정보)와 선택정보(추가정보)로 구성된다. 사건정보는 사건번호, 송치번호, 소속기관, 피의자명 등이고, 디지털증거 정보는 증거파일, 압수담당자명, 압수일시·장소, 피압수자명, 압수물정보(매체명, 제조사, 모델, 일련번호), 해시값 등이며, 추가정보는 참여정보(참여일시, 참여인명), 분석보고서, 압수과정 촬영파일 등이다. 다만 저용량(20GB↓) 증거파일의 경우 온라인으로 검찰시스템에 직접 저장되나, 대용량(20GB↑) 증거파일의 경우에는 저장매체별 관리되고 서버에 저장되지는 않는다.

〈Figure 1〉 Digital evidence storage medium (RDX) and device



〈Figure 2〉 Flowchart of digital evidence online transmission

하지만 '디지털증거 송치표준화' 중 온라인으로 전송된 사건은 2019년 한 해 동안 19건에 불과했다. 실제 디지털증거를 송부하는 각 수사관의 호응을 얻지 못한 결과다. 비록 사건번호, 접수번호, 소속기관명, 소속부서명 등은 디지털포렌식포털에서 자동 연계되지만, 담당 수사관이 증거팩을 구성하기 위해서는 디지털증거팩(DEP) 구성프로그램을 활용하여 피의자명, 송치번호, 송치 검찰청 등을 추가 입력해야 하고 각 저장매체별로 송치할 파일을 일일이 추가해야 하는 문제가 있기 때문이다. 그리고 파일 첨부는 최대 3,000개 내외 가능하나, 팩 구성 및 전송속도를 고려하여 100개 미만으로 유지를 권장하고 있어 파일의 개수가 많은 경우에는 가능한 압축하여 100개 미만으로 만들어야 한다. 이처럼 증거팩을 구성하는 방식이 기존 오프라인 증거송치 방법보다 절차가 복잡하였고, 담당 검사도 기존 방법으로 송부를 요구하는 사례도 많았다.

증거팩 구성·저장 및 온라인 전송에 걸리는 시간도 문제였다. 경찰청 내부자료인 디지털증거 송치표준화 관련 실무매뉴얼에 의하면, RDX (외부 충격에 강하고, 용량은 1TB 또는 2TB이며, 물리적 쓰기방지가 가능한 저장매체)에 저장된 증거파일을 PC로 저장(증거팩 구성·저장)하는 경우 USB 3.0 포트 기준으로 1G → 약 10초, 10G → 약 1분 40초, 20G → 약 3분 20초, 100G → 약 14분, 1TB → 약 2시간 20분, 2TB → 약 4시간 40분 소요됐고, 온라인 전송하는 경우 1G → 약 4분 50초, 10G → 약 45분, 20G → 약 1시간 30분 소요됐다.

이에 따라 경찰청은 송치 증거가 20GB 이하인 경우 저장매체를 이용하지 않아도 되는 장점이 있기에 시범관서에 한해 계속 사용할 방침이나, 현 상태에서는 현장 활용도가 낮아 전국관서로 확대 실시는 검토하고 있지 않다.

〈Table 1〉 The number of cases using standardized transmission

The number of cases		2019 year	
total cases	storage medium (RDX)	983	306
	online transfer		19
the standardized rate of transmission		33.0%	

3.3 블록체인 기반 디지털증거 관리시스템

앞서 설명한 바와 같이 경찰은 '디지털증거 송치표준화'를 통해 디지털증거를 자동 검증하는 프로세스를 구축하여 관리연속성을 확보하려고 시도하였다. 그러나 이를 실무적으로 활용하지 못하였고, 그 대안으로 블록체인을 활용한 방안이 거론되고 있다.

최복용·함용욱은 확보한 디지털증거의 데이터 원본에서 추출한 해시값, 등록 등록자 ID, 등록 시간, 증거정보 등 등록 데이터를 블록체인 네트워크에 연결된 모든 컴퓨터(노드)에 전파하는 방법으로 위·변조를 차단함으로써 디지털증거의 무결성을 보장하는 방안을 제안하였다 [6] .

실제로 경찰은 2020년 블록체인 기반 디지털증거 관리시스템 구축 시범사업의 일환으로 블록체인 기반 디지털증거 이력관리 플랫폼을 개발하여 현재 시범운영 중에 있다. 이 플랫폼은 경찰의 디지털증거 수집 프로그램인 '폴-해시앱'과 연동함으로써 무결성 보장과 신뢰성 강화를 추진하고 있다. 폴-해시 앱으로 전자정보확인서 생성시 블록체인에 파일명, 해시값, 파일생성 시간을 기록하는 방법이다. 향후 디지털포렌식포털의 고도화사업이 완료되면 디지털증거별로 사건 이력, 해시값, 생성시각 등 일부 메타데이터가 저장되어 관리될 예정이다. 더 나아가 블록체인 서버를 검찰과 법원에도 설치한다면 디지털증거의 무결성 및 관리연속성을 한층 더 확보할 수 있을 것이다.

Ⅳ. 수사종결 방식에 따른 디지털증거 관리

4.1 불송치 결정시 증거능력 확보방안

경찰 수사결과, 범죄혐의가 인정되어 검찰에 사건을 송치하면 관련 디지털증거는 검찰에 송부되어 D-NET에 저장된 후 보관·삭제·폐기의 일련 과정을 거친다. 하지만 수사권 조정 등으로 수사종결 방식에 따라 경찰이 자체적으로 디지털증거를 보관·삭제·폐기해야 하는 경우가 발생한다. 경찰이 불송치 결정시 그 이유를 명시한 서면과 함께 관계 서류와 증거물을 지체 없이 검사에게 송부하여야 하지만, 검토 후 90일 이내에 반환받기 때문이다.

경찰청훈령인 디지털증거의 처리등에 관한 규칙 제35조 제3항에 의하면, "경찰관은 사건을 이송 또는 송치한 경우 수사과정에서 생성한 디지털증거의 복사본을 지체 없이 삭제·폐기하여야 한다"고 규정하고 있다. 그리고 동 규칙 제36조에 의하면 "입건 전 조사편철(구 내사편철)·관리미제사건 등록한 사건의 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 경찰이 불송치 결정한 경우 디지털증거 보관·삭제·폐기 규정은 확인할 수 없다. 아울러 경찰의 불송치 결정에 대한 통제 수단인 이의신청, 재수사요청, 시정조치 요구시에도 디지털증거 보관·삭제·폐기 관련 규정을 확인할 수 없다.

특히 이의신청은 기한이 없어 사실상 공소시효의 기간까지 이의신청이 가능하므로 경찰의 입장에서는 사건이 종결되었다고 간주하고 디지털증거를 삭제·폐기하였다가 수사가 재개될 경우 혐의 입증이 어려운 경우가 발생할 수 있다. 그리고 불송치 결정사건은 사실상 처분이 완료된 건으로 디지털증거를 보관할 이유가 없고, 보관시 별건 수사 이용 우려 및 개인 사생활 침해 등의 문제가 발생될 수 있다.

따라서 이의신청 기한을 무제한으로 두지 않고 검사의 사건기록 검토 기간(90일)에 맞추어 불송치결정 통지를 받은 날로부터 90일 이내로 한정하고, 해당기간 동안에는 디지털증거의 증거능력이 철저히 유지되도록 보관하는 방식으로 개선할 필요가 있다.

4.2 관리미제 편철시 증거능력 확보방안

경찰은 수사 단서를 찾지 못해 수사를 잠정 중단할 필요가 있는 경우 관리미제사건으로 등록한다. 이때 CCTV·블랙박스 영상자료 등 수사단서로 활용했던 디지털증거는 형사소송법 제218조의2 제1항에 따라 압수를 계속할 필요가 없다고 인정되는 경우 압수물의 소유자, 소지자, 보관자 또는 제출인에게 환부 조치하거나 폐기 처분한다. 그 외에는 관리미제 등록된 사건의 중한 죄에 해당하는 공소시효 만료일까지 디지털증거를 보관하여야 하고, 별도의 저장매체에 담아 증거물 보관실에 보관하는 등 증거의 무결성과 보안 유지에 필요한 조치를 병행하여야 한다.

이처럼 CCTV·블랙박스 영상자료 등 디지털증거는 증거물 보관실에 보관하여야 함에도 일부 수사관들은 CD 또는 USB 등 별도의 저장매체에 담아 사건기록에 첨부하고 있고, 해시값도 확보하지 않은 경우도 있다. 비록 사건기록을 별도의 기록물 창고에 보관하기는 하나 분실, 손상 및 위·변조의 위험에 바로 노출되기 때문에 디지털증거, 해시값, 메타데이터 등을 하나의 증거팩으로 구성하여 저장매체에 저장한 후 공소시효 만료일까지 통합증거물 보관소에 보관하는 방식으로 개선할 필요가 있다.

관리미제사건의 디지털증거에 대해서는 필요시 피압수자에게 환부하고 그렇지 않을 경우 장기보관을 하는데, 디지털증거의 장기보관의 경우 국가기록물의 장기보관 문제와 비교하여 생각해 볼 수 있을 것으로 보인다[7]. 국가전자기록물은 진본성·무결성을 보장하고 장기간 안전하게 보존하기 위해 전자기록물 원본·문서보존포맷·메

타데이터·전자서명을 하나의 패키지로 구성한 포맷으로 보관하고 있는데, 이러한 국가전자기록물 장기보관 포맷을 관리미제사건 관련 디지털증거 보관에 적용할 필요가 있다[8]. 또한 증거분석 시스템의 경우 분석 관련 도구, 운영체제, 분석에 필요한 전용 프로그램 등의 보관 및 분석정보 구성을 위한 시스템도 구축하도록 하면서, 디지털증거 보관 시스템과 연계할 수 있도록 설계해야 한다[4].

4.3 수사중지 결정시 증거능력 확보방안

2021년 제정된 검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정(대통령령)에 따라 경찰의 결정 중 하나로 수사중지 제도가 신설되었다. 이에 따라 기존에는 기소중지 의견으로 송치되던 사건기록이 이제는 검찰에 송부하되 다시 경찰에 반환되는 형식으로 변경되었다. 수사중지 결정 기록과 디지털증거는 수사중지 결정 후 7일 이내 검찰에 송부하되, 30일 이내 반환된다.

수사중지 결정은 송치 결정과는 별개의 개념으로 '송치시 수사과정에서 생성한 디지털증거의 복사본을 삭제·폐기하여야 한다'는 디지털증거의 처리등에 관한 규칙 제35조 제3항 규정이 적용되지 않는다. 그리고 수사중지 결정은, 범죄 혐의는 있으나 피의자를 추적할 단서가 없어서 잠정 수사를 중지할 필요가 있거나, 피의자 또는 참고인의 소재불명 등으로 수사를 계속하기 어려운 경우에 처리하는 것이므로 수사단서에 활용된 CCTV·블랙박스 영상자료 등 디지털증거를 삭제·폐기해서는 안 된다. CCTV·블랙박스 영상자료의 화질 등 문제로 당시 피의자를 특정하지 못하였을 뿐, 피의자 검거 후 혐의 입증자료로는 충분히 활용할 수 있기 때문이다.

그러나 수사중지 결정 건에 대한 디지털증거를 어떻게 처리할 것인지는 규정상 명시되어 있지 않다. 일부 수사관들은 디지털증거를 CD 또는 USB 등 저장매체에 담아 사건기록에 첨부하거나 개인 PC에 보관하다가 피의자 검거시 활용하고 있다. 따라서 수사중지 결정건의 경우도 디지털증거는 위에서 제안한 증거팩을 구성하여 보관하여야 증거능력을 유지할 수 있을 것이다.

4.4 입건 전 조사종결시 증거능력 확보방안

입건 전 조사종결된 사건(구 내사종결 사건)에 대해서는 경찰 자체적으로 분기에 1회씩 종결의 적정성 여부에 대해서 정기 점검하고 점검 결과를 경찰수사심의위원회에 상정해야 한다. 경찰수사심의위원회는 입건 전 조사종결된 건이라고 하더라도 필요에 따라 재수사를 의결하기도 한다.

아울러 입건 전 조사종결된 건은 불송치 결정 사건이 아니므로 이의신청의 대상은 아니나, 각 시·도경찰청 수사심의계에 심의신청을 할 수 있다. 심의신청을 받은 수사심의계에서는 경찰 수사절차 또는 결과의 적정성(적법성)이 침해되었는지 여부를 조사하고, 조사결과에 따라 경찰서에 보완·재수사를 지시하기도 한다.

경찰수사의 완결성을 확보한다는 취지에서 심의신청 또한 이의신청과 마찬가지로 신청기한이 별도로 규정되지 않아 언제든지 신청할 수 있다. 그런데 앞서 살펴본 바와 같이 입건 전 조사종결 사건의 압수한 전자정보는 압수를 계속할 필요가 있는 경우 해당 사건의 공소시효 만료일까지 보관 후 삭제·폐기하고, 압수를 계속할 필요가 없다고 인정되는 경우 삭제·폐기해야 한다.

비록 압수한 전자정보의 삭제·폐기는 디지털증거의 처리등에 관한 규칙 제36조에 따라 관서별 통합 증거물 처분심의위원회를 통해 심의 후 처분 가능하나, 보존의 필요성이 없다고 의결되어 관련 전자정보가 삭제·폐기된 이후에 심의신청되는 경우가 발생할 수 있다. 반대로 압수한 전자정보를 보존할 필요성이 없음에도 수사기관이 향후 별건 수사에 활용하기 위해 일부러 공소시효 만료일까지 보관하고자 시도할 수 있다. 경찰의 통합증거물 관리지침상 통합 증거물 처분심의위원회 구성원은 위원장(수사과장) 포함 위원 4인 이상으로 구성되고 구성원 중 1명이라도 반대의견이 있는 경우는 삭제·폐기가 불가하지만, 처분 대상 통합 증거물이 있는 수사부서에서 1인 이상이 구성원으로 반드시 참여토록 하여 담당 수사부서의 의견이 관철되기 쉬운 구조적 문제를 안고 있기 때문이다.

따라서 무제한의 심의신청 기한을 종결 후 1년 정도로 한정하되, 해당 기한까지는 위에서 언급한 증거팩을 구성하여 디지털증거의 증거능력을 철저히 유지할 필요가 있다. 압수를 계속할 필요가 없다고 인정되는 증거도 증거팩을 구성해야 하는지에 대한 이견도 있을 수 있으나, 압수한 전자정보의 보존 필요성에 대한 명확한 기준이 부재하고 이를 구체적으로 설정하기도 어렵기 때문에 모든 증거에 대해서 증거팩을 구성할 필요가 있다.

Ⅴ. 디지털증거 인수·인계 체계 제안

5.1 디지털증거 통합관리시스템 고도화

2020년 8월 수사부터 재판, 집행까지 모든 형사절차가 전자적으로 진행되는 「형사사법절차에서의 전자문서 이용 등에 관한 법률」 제정안이 입법예고 되었고, 현재 2024년 완성을 목표로 「차세대 형사사법정보시스템(KICS) 구축사업」도 병행 중이다. 이러한 형사사법절차의 전자화를 대비한 디지털증거 통합관리시스템이 디지털증거 분석의뢰 접수·회신의 창구를 넘어, 수사 전반에 걸쳐 디지털증거를 종합적으로 관리할 수 있도록 구현할 필요가 있다. 이를 위해서는 '디지털증거 통합관리시스템 자체' 또는 '이와 연계된 프로그램'에서 디지털증거에 대한 선별압수를 진행해야 하고, 압수대상 디지털증거는 송치 시점까지 증거관리시스템에 보관하다가 KICS와 연계하여 전자적 송치로 무결성 및 관리연속성을 보강하여야 한다.

즉, 분석결과물을 회신받아 수사관 PC에서 선별압수를 진행하는 방식에서 디지털증거 통합관리시스템 자체 내지 이와 연계된 프로그램에서 선별 압수하는 방식으로 변경하여야 한다. 그리고 분석결과물을 수사관의 PC에 보관하는 방식에서 통합증거물관리시스템에 보관하는 방식으로 변경하고, USB 등 저장매체에 저장하여 송부하는 방식에서 네트워크를 통해 송부하는 방식으로 변경하여야 한다.

5.2 클라우드 DaaS 도입에 따른 디지털증거 관리

위에서 살펴본 디지털증거 송치표준화 시범사업은 일선 수사관들의 호응이 기대에 미치지 않아 전국으로 확대되지 못하였다. 하지만 결국은 네트워크를 통해 디지털증거를 송부하는 것이 시대적 흐름이자 관리연속성 등 디지털증거의 증거능력을 유지할 수 있는 방법이다. 하지만 아무리 좋은 시스템을 구축하더라도 이를 활용하는 사람에게 업무 부담이 가중된다면 무용지물이다. 일선 수사관들의 호응을 얻기 위해서 해결해야 할 문제는 결국 저장용량 및 전송속도의 문제이고, 이를 해결할 수 있는 가장 좋은 방법은 클라우드 시스템을 활용하는 것이다.

때마침 경찰을 비롯한 행정안전부는 고비용의 물리적 망분리 방식에서 서버 가상화 방식의 클라우드 DaaS(Datacenter as a Service, 서비스로의 데이터센터) 형태로 전환을 준비 중이다. 원격근무나 재택근무가 일상화되면 현재의 망분리 정책이 더 이상 유효하지 않다는 판단에서다. 정부의 기존 물리적 망분리 정책은 해킹 위협이 상당히 줄어드나 업무를 위해 두 가지 망과 내외부 메일을 연동해 쓰면서 오히려 해킹의 표적이 된다는 지적이 있기 때문이다.

DaaS는 보안에 강하고, 화면만 가상화되면 PC화면이든 스마트폰이든 상관없어 재택근무가 가능하다. 어느 기기에서건 로그인만 하면 작업하던 화면을 불러올 수 있다. 따라서 향후 업무망 PC에서 클라우드 DaaS를 이용해 인터넷을 이용할 수 있는 시스템이 구축된다면 디지털증거 송치표준화의 가장 큰 걸림돌인 저장용량 및 전송속도 문제도 해결될 수 있을 것으로 보인다. 아울러 디지털증거 수집 단계부터 디지털증거에 대한 보안성과 무결성이 담보될 수 있어 증거능력이 한층 더 유지될 수 있는 환경이 조성될 것이다.

다만 Daas를 도입하더라도 초대용량 디지털증거의 경우에는 포렌식 및 증거검토를 위해 데이터센터로부터 반복 전송받게 되는 상황이 발생하여 큰 부담으로 작용할 수 있으므로 초대용량 디지털증거는 저장매체를 이용하는 방식으로 보완할 필요도 있다. 그리고 일반 행정 업무와 달리 경찰 업무는 보안상 불가피하게 민간 클라우드의 활용이 어려울 수 있으므로 국가정보자원관리원 내에 경찰청 전용 클라우드존 구성을 추진할 필요도 있다.

5.3 클라우드 기반 영상제보 및 관리시스템 구축

경찰은 국민의 자발적 참여와 협력을 통한 목격자 제보 정보를 활용하기 위해 지난 2015년부터 국민과 함께하는 '스마트 국민제보' 서비스(위치 및 영상 기반의 국민제보 시스템)를 시행하고 있다. 이 시스템에는 뺑소니 등 교통사고 및 사회적 이슈 범죄의 사건·사고에 대한 정보들이 축적되어 있다. 특히 영상과 사진에 세부정보(위반일시, 장소 등)가 자동 표기되어 디지털증거로 활용할 수 있다.

그러나 이 시스템은 교통위반행위에 대한 사실을 형사 기관에 알리는 신고는 활성화되었으나, 교통사고 및 형사사건에 대해 목격한 정보를 제공하는 제보의 경우 그 활용도가 낮다는 문제점을 갖고 있다. 지난 2017년 6월 기준으로 신고는 441,546건이나 제보는 9건에 불과했다 [9] .

이는 시스템에 업로드 가능한 파일용량이 90MB로 제한되고, 제보하기 위해 별도의 회원가입(홈페이지)이나

본인 인증(앱)이 필요하기 때문으로 보인다. 범죄 현장에 있던 시민들이 자신의 신변노출에 대한 우려와 증언 및 휴대전화 제출의 부담감으로 자료 제출을 기피하기 마련이다.

'스마트 국민제보 시스템'을 개선하여 활성화시키려면 저장서버의 증설로 시스템에 업로드할 수 있는 파일용량을 대폭 늘리고, 제보자의 신변노출에 대한 우려를 불식시키기 위해 별도의 회원가입이나 본인인증 제도를 폐지해야 한다. 다만 회원가입이나 본인인증이 없어도 제출되는 이미지를 디지털증거로 사용하기 위해서는 이미지와 함께 메타데이터를 저장하여야 한다. 시간 정보, 위치 정보 등 메타데이터의 저장은 딥페이크 영상과 같이 디지털증거 위·변조 후 이루어질 수 있는 무고나 허위제보도 예방하는 효과도 있다.

제보의 익명성을 보장하면 사회적 이목이 집중되는 중요 사건의 증거자료 수집에도 큰 도움이 될 것이다. 언론 등을 통해 자료 등록 주소(URL) 또는 이와 연동된 QR코드를 공개함으로써 신변노출을 우려하는 제보자들을 상대로 적극적인 제보를 유도할 수 있다.

그리고 경찰이 익명의 제보자가 아닌 특정된 수사대상자 또는 목격자 등으로부터 핸드폰에 저장된 영상 등을 임의제출 받고자 하는 경우에도 다음과 같은 절차를 활용하면 임의성과 무결성을 확보할 수 있을 것이다. 사진이나 비디오 장면을 업로드하기 위해 클릭할 수 있는 URL을 문자메시지나 SNS 등을 통해 상대방에게 제공하고, 상대방이 직접 사이트에서 자료를 등록한 다음 경찰관이 이를 확인하는 프로세스다.

최근에는 가정용 CCTV 및 차량용 블랙박스 녹화영상을 기기 자체에 저장하지 않고, 서버에 저장함으로써 서비스 이용자가 해당 영상을 실시간 확인할 수 있고, 일정 기간 보관도 해주는 서비스를 제공하는 제품이 출시되었다. 이 경우 서비스 이용자가 서버에서 녹화영상을 다운받은 후 위 프로세스를 활용하여 경찰에 증거로 제공한다면 과거 '원세훈 전 국정원장 자택 방화사건'과 같이 CCTV가 증거로 채택되지 않는 일은 더 이상 벌어지지 않을 것이다.

스마트 국민제보 시스템이 위와 같은 프로세스를 제공할 수 있도록 업데이트되고, 제출된 디지털증거의 해시값 등을 인증하는 기능도 포함된 클라우드 서비스가 구축된다면 디지털증거의 증거능력은 한층 더 확보할 수 있을 것이다. 또한 해당 프로세스 활용으로 강제수사로서 제출 명령 제도의 도입도 고려해 볼 수 있을 것이다.

한편 경찰은 여러 형태의 자체 이동형 영상기기를 활용해서 디지털증거를 확보하고 있다. 불법 집회·시위 현장이나 압수수색 현장에서 디지털 카메라로 채증하는 것을 비롯해 최근에는 웨어러블 폴리스캠, 112 순찰차 캠, 순찰용 드론 등을 활용하고자 시도하고 있다. 다만 112순찰차 캠은 2019년 10월 영상을 저장하지 않고 실시간 관제에만 사용하는 조건으로 제한적 허용되었고, 순찰에 드론을 활용하는 것은 개인정보침해 우려가 있어 불허된 사례(시흥경찰서)가 있다. 불법 집회·시위 현장이나 압수수색 현장이 아닌 장소에서 경찰이 자체 이동형 영상기기로 채증하는 경우 영장 없이 기본권을 제한하는 강제수사가 될 수 있으므로 이에 대한 법률적 근거 마련이 필요한 시점이다.

이와 함께 경찰에 의한 영상의 오·남용 및 위·변조 우려를 불식시켜야 한다. 수사기관은 형사소송의 한 당사자이며 또한 피의자 및 피고인의 이익을 보호하는 공익의 대표자로서의 객관의무를 가진다고는 하나 항상 이를 성실히 이행할 것이라고 확신하기는 현실적으로 어렵다. 이는 증거처리에 있어서도 마찬가지로 모든 사건에 대해 공정한 증거처리를 하였음을 보장하기는 현실적으로 불가능하다고 할 수 있다. 악의적인 사용자가 저장매체 저장매체 원본과 사본에 자유롭게 접근할 수 있는 경우 디지털증거의 위·변조를 방어할 수 없으며, 수사기관에서 제시한 증거의 무결성을 수사기관 자체에서 증명한다는 것이 모순이라는 지적도 있다 [2] . 따라서 클라우드를 기반으로 한 범용 영상관리시스템을 구축함으로써 경찰이 이동형 영상 기기로부터 직접 추출하여 임의로 변경·편집한 영상은 증거물로 활용할 수 없도록 하여야 한다.

국립과학수사연구원에서 2015년부터 개발하여 관리하고 있는 디지털증거 인증 서비스(DAS)를 활용할 수도 있다. 그간 일부 수사기관(경찰청 보안국, 국가정보원 등)에서 사용되고 있지만, 국립과학수사연구원에서의 DAS ID 발급 문제 등으로 인하여 아직 전 수사기관에서 활용되지 않고 있다[10]. DAS는 주기적으로 대한민국 전자관보에 해시값을 공개함으로써 객관성과 신뢰성을 높게 유지하고 있고, 현장에서 수집한 디지털증거의 해시값을 포함한 메타데이터도 함께 전송함으로써 법정에서 무결성을 인정받기 훨씬 수월하다. 따라서 이동형 영상기기에 DAS 앱을 설치하거나 캡처 프로그램에 로그인할 수 있는 기능을 구현 후 활용한다면 디지털증거의 위·변조 여부 등 무결성 입증 문제를 해결할 수 있을 것이다.

5.4 클라우드 시스템 구축 전, 과도기적 해결방안

디지털증거의 증거능력을 유지하기 위해 클라우드 시스템이 도입될 필요가 있으나, 이를 구축하기 위해서는 예산 문제 및 추가 연구 필요 등으로 도입까지 상당한 시일이 필요할 것으로 보인다. 그래서 클라우드 시스템

이 구축되기 전까지 과도기적인 해결방안을 제안하고자 한다.

첫 번째가 '에스크로(escrow)'를 활용하는 방안이다. 이는 디지털증거 수신기관이 해시값을 구하고 일치 여부를 확인할 때까지 자체 통합증거물 보관소에 보관하는 방식이다. 수신기관이 송부된 디지털증거의 해시값 일치 여부를 확인하면 송부기관에게 '에스크로(escrow)' 서비스에 의해 자동 통보되고, 그 이후 파기 절차를 진행하면 된다. 이 방법은 많은 예산이 필요한 제3의 공인인증기관을 설립하지 않아도 이미 설치되어 있는 기관별 통합증거물 보관소를 활용할 수 있다는 장점도 있다.

두 번째로 제안하는 방안은, 경찰이 디지털증거를 검찰에 송부하여 검찰청 사건과에서 수리하는 즉시 현장에서 검찰의 D-NET에 일괄 등록하고 확인서를 발급해주면 경찰이 해당 증거를 파기하는 방식이다. 다만 경찰은 아직 검찰의 D-NET과 같은 성격의 디지털증거 관리(저장 및 보관)시스템이 구축되지 않아 검찰에서 경찰로 송부되는 디지털증거에 대해서는 대안이 될 수 없다는 한계가 있다.

한편 시범실시 중인 디지털증거송치표준화 사업도 20G를 초과하는 대용량의 디지털증거를 송부할 때는 온라인 전송이 불가하다는 측면에서 오프라인 방식의 확인서 작성도 여전히 의미가 있다. 이 경우 확인서는 단순 수리가 아닌 해당 디지털증거의 해시값을 검증 후 인수하였음을 인증하여야 한다. 단, 이를 위해서는 디지털증거 송부시 인계 현장에서 해시값을 검증하는 시간을 효과적으로 단축시켜야 하는데, 의외로 간단하게 해결할 수 있다. 바로 압축을 통해서 하나의 파일로 생성 후 해시값을 계산하는 것이다. 압수시 먼저 개별 전자정보의 해시값을 확인하고 선별파일을 피압수자별로 구분하여 압축한 후, 압축한 파일의 해시값도 함께 확인한다면 동일성과 무결성을 확보할 수 있다. 피압수자가 많다면 이를 다시 하나의 파일로 압축해도 무방하다.

이를 정리하면, 송부기관은 개별 파일 및 압축 파일의 해시값을 각각 추출·등록한 후 송부하고 수신기관은 1개의 압축파일에 대해서만 확인하면 되므로 확인서 작성 방식의 최대 걸림돌인 검증 시간을 줄일 수 있을 것이다.

이때 선별파일을 압축한 파일의 해시값을 검증하더라도 개별 파일의 해시값을 검증하지 않으면 동일성이 부정되므로 유의해야 한다. 이와 관련 대법원은 지난 2017년 8월 2일 "이 사건 사실확인서에는 이 사건 USB 이미지 파일의 전체 해시값만이 기재되어 있을 뿐 이미징을 한 이 사건 USB 내 개별 파일에 대한 해시값은 기재되어 있지 않으므로, 이 사건 사실확인서를 가지고 이 사건 판매심사 파일과 이 사건 USB 내 원본 파일과의 개별 해시값을 상호 비교할 수도 없다."고 판결(대판 2017도13263)하였다.

Ⅵ. 결 론

현대인의 하루는 디지털 기기로 시작해서 디지털 기기로 끝난다고 해도 과언이 아닐 만큼 디지털 기기의 활용도는 날로 증가하고 있다. 범죄 수사에 있어서 스마트폰에 저장된 대화내용, 사진, 동영상, 위치 정보 등을 통해 범죄를 해결하고, 사건 해결의 단서를 발견하는 등 디지털증거는 범죄 해결의 핵심 역할을 수행하고 있다. 과거에는 유체물 형태의 범행도구 확보가 범죄해결의 성패를 좌우했다면, 최근에는 디지털증거를 얼마나 신속히 확보하였는지, 디지털증거를 어떻게 수집하고 관리하여 법정에서 동일성과 무결성, 관리연속성을 입증할 수 있는지가 범죄해결과 혐의 입증에 핵심요소로 강조되고 있다. 즉, 디지털증거의 증거능력 유지는 수사의 성패 및 공소 유지의 매우 중요한 요소로 자리 잡았다.

본 고에서는 데이터 위·변조에 취약한 디지털증거가 수집 및 분석과정을 거쳐 법정에 제출되기까지 증거능력을 유지하기 위해 현행 디지털증거의 인수인계 절차 및 문제점을 살펴보고, 이를 해결할 수 있는 자동화된 확인 시스템을 제안하였다.

개정 형사소송법 시행 및 정보화의 새로운 패러다임 변화 속에서 디지털증거의 확보보다 더 중요한 증거능력 유지를 위해 수사기관간 협업을 통해 디지털증거 송부시 해시값 자동 검증 시스템이 빠른 시일 내에 구축되어야 한다. 이로써 증거물 분실(?)로 인한 혐의를 입증하지 못한 '제2의 김학의 사건'이 발생하는 일이 없어질 것이고, 국가 수사 체계에 대한 국민의 신뢰도도 향상될 것이다.

참 고 문 헌 (References)

〔1〕 In-soo Lee, "Digital Evidence Securing System", Korea Institute Of Information Security And Cryptology 26(5), pp. 37-43, 2016.
〔2〕 Hye-jeong Seong, Hye-Jeong Yoo, "A Study on the Authority for Verifying Digital Evidence Independent of Judical Procedure", The Korean Institute of Information Technology, pp. 224, 2014.
〔3〕 Hyung-sang Jeong, Sang-jin Lee, "Digital Evidence Information Leakage and Prevention Measures", Police Science Institute, 35(2), pp 103-131, 2021.
〔4〕 Hyun-hee Jung, "Management from the Perspective of the Life Cycle of Digital Evidence", Journal of Digital Forensics 10(1), pp. 1-20, 2016.
〔5〕 Hyo-jeong Jeong, "A Study on Digital Evidence Collection System in Cyberspace", Journal of the Korean Institute of Information Security & Cryptology, 28(4), pp.869-878, 2018)
〔6〕 Bok-yong Choi · Yeong-ug Ham, "A Study on Ways to Reinforce Integrity of Digital Evidence Using Blockchain", Police Science Institute 30(3), pp. 295-318, 2016.
〔7〕 Hye-ran Suh, "Developing a Reference Model of Korean Recordkeeping System for Integrated Information Resources Management", Korean Soceity for Library and Information Science, 38(4), pp.302-326, 2006
〔8〕 Tea-shik Shon, "Research on advanced electronic record management technology using digital forensics", Journal of the Korean Institute of Information Security and Cryptology, 23(2), pp.273-277, 2013)
〔9〕 Sang-yeon Yoon, "Criminal Environment Risk Index Development Study", Responsible Research Report, pp.75, 2017
〔10〕 Jung-Won Shin, "A Study on the Usefulness of Digital Evidence Authentication System", New trends in forensic science, 11(4), 111-161, 2021

저 자 소 개

정 웅 길 (Woongkil Jeong)
준회원

2004년 3월 : 경찰대학 행정학과 졸업
2020년 9월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 디지털 포렌식, 정보보호 등

이 상 진 (Sangjin Lee)
평생회원

1989년 10월 ~ 1999년 2월 : 한국전자통신연구원 선임연구원
1999년 3월 ~ 2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월 ~ 현재 : 고려대학교 정보보호대학원 교수
2017년 3월 ~ 현재 : 고려대학교 정보보호대학원 원장
관심분야 : 대칭키 암호, 정보은닉 이론, 디지털 포렌식